kaspersky

卡巴斯基安全管理中心 14.2 Windows

© 2026 AO Kaspersky Lab

目錄

- 卡巴斯基安全管理中心 14.2 說明
- 新增內容
- 卡巴斯基安全管理中心 14.2
  - 基本概念
    - 管理伺服器
    - 管理伺服器階層
    - 虛擬管理伺服器
    - 行動裝置伺服器
    - 網頁伺服器
    - 網路代理
    - 管理群組
    - 受管理裝置
    - 未配置的裝置
    - 管理員工作站
    - 管理外掛程式
    - 管理 Web 外掛程式
    - 政策
    - 政策設定檔
    - 工作
    - 工作範圍
    - 本機應用程式設定與政策的關係
    - 發佈點
    - 連線閘道
  - 關於卡巴斯基安全管理中心
    - 硬體和軟體需求
      - 管理伺服器要求
      - 網頁主控台要求
      - 行動伺服器要求
      - 管理主控台要求
      - 網路代理要求
    - 相容的卡巴斯基應用程式和解決方案
    - 卡巴斯基安全管理中心 14.2 的產品授權與功能
    - 關於管理伺服器和卡巴斯基安全管理中心網頁主控台的相容性
    - 卡巴斯基安全管理中心比較：基於 Windows 與基於 Linux
    - 關於 卡巴斯基安全管理中心雲端主控台
  - 架構
  - 主要安裝情境
  - 卡巴斯基安全管理中心使用的連接埠
  - 用於卡巴斯基安全管理中心的憑證
    - 關於卡巴斯基安全管理中心憑證
    - 關於管理伺服器憑證
    - 卡巴斯基安全管理中心中使用的自訂憑證要求
    - 情境：指定自訂管理伺服器憑證

使用 klsetsrvcert 公用程式替換管理伺服器憑證
使用 klmover 公用程式將網路代理連線到管理伺服器
重新發行網頁伺服器憑證
資料流量和連接埠使用的 schema
LAN 中的管理伺服器和受管理裝置
LAN 的主管理伺服器和兩個從屬管理伺服器
管理伺服器位於 LAN、受管理裝置位於網際網路、反向代理使用中
管理伺服器位於 LAN、受管理裝置位於網際網路、連線閘道器使用中
管理伺服器位於 DMZ、受管理裝置位於網際網路
與卡巴斯基安全管理中心元件和安全應用程式的互動：更多資訊
互動模式中的慣例
管理伺服器和 DBMS
管理伺服器和管理主控台
管理伺服器和用戶端裝置：管理安全應用程式
透過發佈點在用戶端裝置上升級軟體
管理伺服器階層：主管理伺服器和從屬管理伺服器
DMZ 中帶有從屬管理伺服器的管理伺服器階層
管理伺服器、網段連線閘道和用戶端裝置
管理伺服器和 DMZ 中的兩台裝置：連線閘道和用戶端裝置
管理伺服器和卡巴斯基安全管理中心 網頁主控台
啟動和管理行動裝置上的安全應用程式
佈署最佳實踐
硬化指南
管理伺服器佈署
連線安全
帳戶和身分驗證
對管理伺服器防護的管理
管理用戶端裝置防護
配置受管理應用程式的防護
管理伺服器維護
事件傳輸到協力廠商系統
佈署準備
排程卡巴斯基安全管理中心佈署
佈署防毒軟體的標準流程
在組織網路中計畫卡巴斯基安全管理中心佈署的資訊
選取企業防護結構
卡巴斯基安全管理中心的標準設定
標準配置：單一辦公室
標準配置：由自己管理員執行的幾個大規模辦公室
標準配置：多個小遠端辦公室
選取 DBMS
設定 MariaDB x64 伺服器以與卡巴斯基安全管理中心 14.2 一起使用
設定 MySQL x64 伺服器以與卡巴斯基安全管理中心 14.2 一起使用
設定 PostgreSQL 或 Postgres Pro 伺服器與卡巴斯基安全管理中心 14.2 搭配使用
使用 Kaspersky Endpoint Security for Android 管理行動裝置
提供到管理伺服器的網際網路存取
網際網路存取：本機網路上的管理伺服器

網際網路存取：DMZ 中的管理伺服器
網際網路存取：DMZ 中作為連線閘道的網路代理
關於發佈點
增加 klnagent 服務的檔案描述符限制
計算發佈點的數量和配置
管理伺服器階層
虛擬管理伺服器
卡巴斯基安全管理中心的限制資訊
網路負載
病毒防護的初始佈署
病毒資料庫的原始更新
使用戶端與管理伺服器同步
病毒資料庫額外更新
利用管理伺服器對用戶端事件的處理
24 小時流量
準備行動裝置管理
Exchange 行動裝置伺服器
如何佈署 Exchange 行動裝置伺服器
佈署 Exchange 行動裝置伺服器所需的權限
Exchange ActiveSync 服務帳戶
iOS MDM 伺服器
標準配置：DMZ 中的 Kaspersky Device Management for iOS
標準配置：組織本機網路中的 iOS MDM 伺服器
使用 Kaspersky Endpoint Security for Android 管理行動裝置
管理伺服器效能資訊
連線到管理伺服器的限制
管理伺服器效能測試報告
KSN 代理伺服器效能測試結果
用於與外部服務交互的網路設定
佈署網路代理和安全應用程式
初始化佈署
配置安裝程式
安裝套件
MSI 內容和轉換檔案
使用應用程式遠端安裝的協力廠商工具佈署
卡巴斯基安全管理中心的遠端安裝工作相關資訊
透過擷取和複製裝置映像來佈署
磁碟機映像錯誤複製
使用 Microsoft Windows 群組政策佈署
透過卡巴斯基安全管理中心遠端安裝工作的強制佈署
執行卡巴斯基安全管理中心建立的獨立安裝套件
手動安裝應用程式的選項
建立 MST 檔案
在安裝有網路代理的裝置上遠端安裝應用程式
在遠端安裝工作中管理裝置重新啟動
安全應用程式安裝套件上的資料庫更新
在卡巴斯基安全管理中心中使用工具遠端安裝應用程式以便在受管理裝置上執行相關可執行檔

監控佈署
配置安裝程式
一般資訊
在靜默模式下安裝（帶有回應檔案）
在靜默模式下安裝（沒有回應檔案）
透過 setup.exe 的部分安裝配置
管理伺服器安裝參數
網路代理安裝參數
虛擬基礎架構
降低虛擬機負載的竅門
對動態虛擬機的支援
對虛擬機複製的支援
對網路代理裝置檔案系統回溯的支援
本機安裝應用程式
網路代理的本機安裝
使用靜默模式安裝網路代理
以靜默模式安裝適用於 Linux 的網路代理（搭配回應檔案）
以互動模式安裝 Linux 網路代理
準備在封閉軟體環境模式下執行 Astra Linux 的裝置以安裝網路代理
本機安裝應用程式管理外掛程式
以靜默模式安裝應用程式
使用獨立安裝套件安裝應用程式
網路代理安裝套件設定
檢視隱私政策
佈署行動裝置管理系統
透過 Exchange ActiveSync 協定佈署管理系統
安裝 Exchange ActiveSync 行動裝置伺服器
連線行動裝置到 Exchange 行動裝置伺服器
設定 Internet Information Services Web 伺服器
Exchange 行動裝置伺服器的本機安裝
Exchange 行動裝置伺服器的遠端安裝
使用 iOS MDM 協定佈署管理系統
安裝 iOS MDM 伺服器
在靜默模式安裝 iOS MDM 伺服器
iOS MDM 伺服器佈署方案
簡易佈署方案
涉及 Kerberos constrained delegation (KCD) 的佈署方案
接收 APN 憑證
續約 APN 憑證
配置備用 iOS MDM 伺服器憑證
安裝 APN 憑證到 iOS MDM 伺服器
配置到 Apple 推送通知服務的存取
在行動裝置上發佈和安裝共用憑證
新增 KES 裝置到受管理裝置清單
將 KES 裝置連線至管理伺服器
直接連線裝置到管理伺服器
連線 KES 裝置到 Kerberos constrained delegation (KCD) 伺服器的方案

使用 Firebase Cloud Messaging
與公共金鑰基礎架構整合
卡巴斯基安全管理中心網頁伺服器
卡巴斯基安全管理中心的安裝
準備安裝
使用 DBMS 的帳戶
設定與 SQL Server 搭配使用的帳戶（Windows 身分驗證）
設定與 SQL Server 搭配使用的帳戶（SQL Server 身分驗證）
設定帳戶以搭配使用 MySQL 和 MariaDB
在 MySQL 或 MariaDB DBMS 中將資料從共享表空間移動到每個表格一個檔案的表空間
設定帳戶以搭配使用 PostgreSQL 和 Postgres Pro
情境：驗證 Microsoft SQL Server
管理伺服器安裝建議
在失敗轉移叢集上為管理伺服器服務建立帳戶
定義共用資料夾
使用管理伺服器工具透過 Active Directory 群組政策遠端安裝
透過傳送 UNC 路徑到獨立安裝套件遠端安裝
使用管理伺服器共用資料夾更新
安裝作業系統映像
指定管理伺服器位址
標準安裝
步驟 1。檢視產品授權協議和隱私政策
步驟 2。選取安裝方式
步驟 3。安裝卡巴斯基安全管理中心網頁主控台
步驟 4。選擇網路大小
步驟 5。選取一個資料庫
步驟 6。設定 SQL Server
步驟 7。選取身分驗證模式
步驟 8。在硬碟磁碟機上解壓縮並安裝檔案
自訂安裝
步驟 1。檢視產品授權協議和隱私政策
步驟 2。選取安裝方式
步驟 3。選取要安裝的元件
步驟 4。安裝卡巴斯基安全管理中心網頁主控台
步驟 5。選擇網路大小
步驟 6。選取一個資料庫
步驟 7。設定 SQL Server
步驟 8。選取身分驗證模式
步驟 9。選取帳戶以啟動管理伺服器
步驟 10。選取帳戶以執行卡巴斯基安全管理中心服務
步驟 11。選取共用資料夾
步驟 12。設定與管理伺服器的連線
步驟 13。定義管理伺服器位址
步驟 14。指定行動裝置連線到管理伺服器的位址
步驟 15。選取應用程式管理外掛程式
步驟 16。在硬碟磁碟機上解壓縮並安裝檔案
部署卡巴斯基安全管理中心容錯移轉叢集

情境：部署卡巴斯基安全管理中心容錯移轉叢集
關於卡巴斯基安全管理中心容錯移轉叢集
為卡巴斯基安全管理中心容錯移轉叢集準備檔案伺服器
為卡巴斯基安全管理中心容錯移轉叢集準備節點
在卡巴斯基安全管理中心容錯移轉叢集節點上安裝卡巴斯基安全管理中心
手動啟動和停止叢集節點
在 Windows 伺服器容錯移轉叢集上安裝管理伺服器
步驟 1。檢視產品授權協議和隱私政策
步驟 2。選取叢集上的安裝類型
步驟 3。指定虛擬管理伺服器的名稱
步驟 4。指定虛擬管理伺服器的網路詳細資訊
步驟 5。指定叢集群組
步驟 6。選取一個叢集資料儲存空間
步驟 7。指定用於遠端安裝的帳戶
步驟 8。選取要安裝的元件
步驟 9。選擇網路大小
步驟 10。選取一個資料庫
步驟 11。設定 SQL Server
步驟 12。選取身分驗證模式
步驟 13。選取帳戶以啟動管理伺服器
步驟 14。選取帳戶以執行卡巴斯基安全管理中心服務
步驟 15。選取共用資料夾
步驟 16。設定與管理伺服器的連線
步驟 17。定義管理伺服器位址
步驟 18。指定行動裝置連線到管理伺服器的位址
步驟 19。在硬碟磁碟機上解壓縮並安裝檔案
在靜默模式下安裝管理伺服器
在管理員的電腦上安裝管理主控台
卡巴斯基安全管理中心安裝後系統的變化
移除程式
關於升級卡巴斯基安全管理中心
情境：升級卡巴斯基安全管理中心和受管理安全應用程式
從先前版本升級卡巴斯基安全管理中心
在卡巴斯基安全管理中心容錯移轉叢集節點上升級卡巴斯基安全管理中心
卡巴斯基安全管理中心的初始化配置
硬化指南
管理伺服器快速啟動精靈
關於快速啟動精靈
開始管理伺服器快速設定精靈
步驟 1。設定代理伺服器
步驟 2。選取應用程式啟動方式
步驟 3。選取防護範圍和作業系統
步驟 4。為受管理應用程式選取外掛程式
步驟 5。下載分發套件並建立安裝套件
步驟 6。設定卡巴斯基安全網路使用
步驟 7。設定電子郵件通知
步驟 8。配置更新管理

步驟 9。建立初始防護設定
步驟 10。連線行動裝置
步驟 11。下載更新
步驟 12。裝置發現
步驟 13。關閉快速啟動精靈
設定管理主控台與管理伺服器的連線
設定管理伺服器的網際網路存取設定
連線漫遊裝置
情境：透過連線閘道連線辦公室外的裝置
情境：通過 DMZ 中的從屬管理伺服器連線漫遊裝置
關於連線辦公室外的裝置
將外部桌上型裝置連線到管理伺服器
關於漫遊使用者的連線設定檔
為漫遊使用者建立連線設定檔
關於將網路代理切換到其他管理伺服器
依據網路位置建立網路代理轉換規則
使用 TLS 的加密通信
事件通知
設定事件通知
測試通知
透過執行可執行檔顯示的事件通知
設定介面
發現網路裝置
情境：發現網路裝置
未配置的裝置
裝置發現
Windows 網路輪詢
Active Directory 輪詢
IP 範圍輪詢
Zeroconf 輪詢
使用視窗網域。瀏覽和變更網域設定
為未配置的裝置配置保留規則
使用 IP 範圍
建立 IP 範圍
瀏覽和變更 IP 範圍設定
使用 Active Directory 群組。檢視與修改群組設定
建立將裝置自動移至管理群組的規則
在用戶端裝置上使用 VDI 動態模式
在網路代理安裝套件的內容中啟用 VDI 動態模式
搜尋啟用 VDI 的裝置
將啟用 VDI 的裝置移至管理群組
設備清查
關於新增裝置的資訊
設定用於定義企業裝置的標準
配置自訂欄位
產品授權
超出了產品授權限制事件

關於產品授權
關於產品授權
關於最終使用者產品授權協議
關於產品授權憑證
關於產品授權金鑰
關於金鑰檔案
關於訂購
關於啟動碼
撤銷最終使用者產品授權協議的許可
關於資料提供
卡巴斯基安全管理中心產品授權選項
卡巴斯基安全管理中心和受管理應用程式的產品授權功能
Kaspersky 應用程式。集中佈署
取代協力廠商安全應用程式
使用遠端軟體安裝工作安裝應用程式
安裝應用程式到所選裝置
在管理群組中的用戶端裝置上安裝應用程式
透過 Active Directory 群組政策安裝應用程式
在從屬管理伺服器上安裝應用程式
使用遠端安裝精靈安裝應用程式
檢視防護佈署報告
使用管理外掛程式
應用程式的遠端移除
在管理群組中，替用戶端裝置遠端移除應用程式
從所選裝置中遠端移除應用程式
使用安裝套件
建立安裝套件
建立獨立安裝套件
建立自訂安裝套件
檢視與編輯自訂安裝套件的內容
從 Kaspersky Security Center 分發套件獲取網路代理安裝套件
分發安裝套件至從屬管理伺服器
透過發佈點分發安裝套件
將應用程式佈署結果傳回至卡巴斯基安全管理中心
定義安裝套件的 KSN 代理伺服器位址
接收最新的應用程式版本
準備好用於遠端安裝的 Windows 裝置
準備 Linux 裝置並在 Linux 裝置上遠端安裝網路代理
準備一部執行 SUSE Linux Enterprise Server 15 的裝置以安裝網路代理
準備 macOS 裝置以遠端安裝網路代理
Kaspersky 應用程式：產品授權和啟動
受管理應用程式的產品授權
檢視使用中產品授權金鑰的相關資訊
新增產品授權金鑰到管理伺服器儲存區
新增管理伺服器產品授權金鑰
移除管理伺服器產品授權金鑰
佈署產品授權金鑰到用戶端裝置

- 自動分發產品授權金鑰
- 建立和瀏覽產品授權金鑰使用報告
- 檢視有關應用程式產品授權金鑰的資訊
- 匯出產品授權金鑰檔案

配置網路防護

- 情境：配置網路防護
- 政策設定和傳播：以裝置為中心的方法
- 關於以裝置為中心和以使用者為中心的安全管理方法
- Kaspersky Endpoint Security 政策的手動設定
  - 在進階威脅防護區域配置政策
  - 在關鍵威脅防護部分配置政策
  - 在一般設定部分配置政策
  - 在事件配置區域配置政策
- Kaspersky Endpoint Security 更新群組工作的手動設定
- Kaspersky Endpoint Security 裝置掃描群組工作的手動設定
- 排程「尋找弱點和所需更新」工作
- 更新安裝和弱點修復群組工作的手動設定
- 設定事件儲存區中的最大事件數量
- 設定修復弱點資訊的最長儲存期間
- 管理工作
  - 建立工作
  - 建立管理伺服器工作
  - 為特定裝置建立工作
  - 建立本機工作
  - 在嵌套群組工作台中顯示繼承的群組工作
  - 在工作啟動前自動開啟裝置
  - 在工作結束後自動關閉裝置
  - 限制工作執行時間
  - 匯出工作
  - 匯入工作
  - 轉換工作
  - 手動啟動和停止工作
  - 手動暫停和繼續工作
  - 監視工作執行
  - 檢視儲存在管理伺服器中的工作執行結果
  - 設定工作執行結果資訊的篩選條件
  - 修改工作。回溯變更
  - 比較工作
  - 啟動工作的帳戶
  - 匯出工作執行歷程記錄
  - 變更工作密碼精靈
    - 步驟 1。指定憑證
    - 步驟 2。選取要採取的動作
    - 步驟 3。檢視結果
- 在虛擬管理伺服器上建立您所需要的管理群組
- 政策和政策設定檔
  - 政策層級，使用政策設定檔

政策層次結構
政策設定檔
政策設定繼承
管理政策
建立政策
在子群組中顯示繼承的政策
啟動政策
在出現病毒爆發事件時自動啟用政策
套用漫遊政策
修改政策回溯變更
檢視政策發佈狀態圖表
比較政策
刪除政策
複製政策
匯出政策
匯入政策
轉換政策
管理政策設定檔
管理政策設定檔
建立政策設定檔
修改政策設定檔
刪除政策設定檔
建立政策設定檔啟動規則
裝置移動規則
克隆裝置移動規則
軟體分類
安裝應用程式到用戶端組織裝置的先決條件
檢視和編輯本機應用程式設定
更新卡巴斯基安全管理中心和受管理應用程式
情境：定期更新 Kaspersky 資料庫與應用程式
關於更新 Kaspersky 資料庫、軟體模組和應用程式
關於使用 diff 檔案更新 Kaspersky 資料庫和軟體模組
啟用下載 diff 檔案功能
建立管理伺服器的「將更新下載至儲存區」工作
建立"將更新下載至發佈點儲存區"工作
設定管理伺服器的「將更新下載至儲存區」工作
驗證已下載的更新
設定測試政策和輔助工作
瀏覽已下載的更新
在裝置上自動安裝 Kaspersky Endpoint Security 更新
行動模式更新下載
啟用和停用行動模式更新下載
卡巴斯基安全管理中心元件的自動更新和修補程式
啟用和停用卡巴斯基安全管理中心元件的自動更新和修補程式
自動發佈更新
自動將更新發佈至用戶端裝置
將更新自動發佈至從屬管理伺服器

自動分配發佈點
手動為裝置指派發佈點
從發佈點清單刪除裝置
透過發佈點下載更新
從儲存區刪除軟體更新
為叢集模式中的 Kaspersky 應用程式安裝修補程式
管理用戶端裝置上的協力廠商應用程式
安裝協力廠商軟體更新
情境：更新協力廠商軟體
檢視對於協力廠商應用程式可用的更新資訊
批准和拒絕軟體更新
使用管理伺服器從 Windows 更新同步更新
步驟 1。定義是否減少流量
步驟 2。應用程式
步驟 3。更新類別
步驟 4。更新語言
步驟 5。選取帳戶以移動工作
步驟 6。設定工作啟動排程
步驟 7。定義工作名稱
步驟 8。完成工作建立
手動在裝置上安裝更新
在網路代理政策中設定 Windows 更新
修復協力廠商軟體弱點
情境：尋找與修復協力廠商軟體弱點
關於尋找與修復軟體弱點
檢視軟體弱點資訊
檢視受管理裝置的弱點統計資料
掃描應用程式以尋找弱點
修復應用程式中的弱點
修復隔離網路中的弱點
情境：修復隔離網路中的協力廠商軟體弱點
關於修復隔離網路中的協力廠商軟體弱點
配置具有網際網路存取權限的管理伺服器以修復隔離網路中的弱點
配置隔離管理伺服器以修復隔離網路中的弱點
在隔離網路中傳輸修補程式和安裝更新
停用在隔離網路中傳輸修補程式和安裝更新的選項
忽略軟體弱點
選取適用於協力廠商軟體中弱點的使用者修復項目
更新安裝規則
應用程式群組
取得並檢視儲存在用戶端裝置上的可執行檔清單
使用「應用程式控制」來管理可執行檔
為 Kaspersky Endpoint Security for Windows 政策建立應用程式類別
建立含有手動新增內容的應用程式類別
建立應用程式類別以包含來自所選裝置的可執行檔
建立應用程式類別以包含來自特定資料夾的可執行檔
新增事件相關的可執行檔到應用程式類別

- 設定應用程式在用戶端裝置上的啟動管理
- 檢視可執行檔的啟動規則與分析結果
- 檢視已安裝的應用程式登錄資料
- 變更軟體清查開始時間
- 關於協力廠商應用程式的產品授權金鑰管理
- 建立授權的應用程式群組
- 管理應用程式群組的產品授權金鑰
- 可執行檔儲存區
- 檢視關於可執行檔的資訊

監控和報告

- 方案：監控和報告
- 在管理主控台中監控交通信號燈和記錄的事件
- 使用報告、統計和通知
  - 搭配報告一起使用
    - 建立報告範本
    - 檢視和編輯報告範本內容
    - 報告範本中的延伸篩選格式
      - 轉換篩選至延伸格式
      - 設定延伸的篩選
    - 建立和瀏覽報告
    - 儲存報告
    - 建立報告傳送工作
      - 步驟 1。選取工作類型
      - 步驟 2。選取報告類型
      - 步驟 3。對報告的操作
      - 步驟 4。選取帳戶以移動工作
      - 步驟 5。設定工作排程
      - 步驟 6。定義工作名稱
      - 步驟 7。完成工作建立
  - 管理統計資訊
  - 設定事件通知
  - 為 SMTP 伺服器建立憑證
  - 事件分類
    - 檢視事件分類
    - 自訂事件分類
    - 建立事件分類
    - 將事件分類匯出至文字檔案
    - 從分類中刪除事件
    - 根據使用者請求新增應用程式到排除
  - 裝置分類
    - 檢視裝置分類
    - 配置裝置分類
    - 匯出裝置分類設定到檔案
    - 建立裝置分類
    - 依據匯入的設定建立裝置分類
    - 在分類中從管理群組中刪除裝置
- 監控應用程式的安裝與移除

- 卡巴斯基安全管理中心元件的事件
  - 事件類型描述的資料結構
  - 管理伺服器事件
    - 管理伺服器緊急事件
    - 管理伺服器功能失效事件
    - 管理伺服器警告事件
    - 管理伺服器資訊事件
  - 網路代理事件
    - 網路代理功能失效事件
    - 網路代理警告事件
    - 網路代理資訊事件
  - iOS MDM 伺服器事件
    - iOS MDM 伺服器功能失效事件
    - iOS MDM 伺服器警告事件
    - iOS MDM 伺服器資訊事件
  - Exchange 行動裝置伺服器事件
    - Exchange 行動裝置伺服器功能失效事件
    - Exchange 行動裝置伺服器資訊事件
- 封鎖頻繁事件
  - 關於封鎖頻發事件
  - 管理頻發事件封鎖
  - 移除對頻發事件的封鎖
  - 將軟體弱點匯出至檔案中
- 管控變更虛擬機的狀態
- 使用系統登錄檔中的資訊監控病毒防護狀態
- 當裝置顯示不活動時檢視和配置操作
- 停用卡巴斯基公告

發佈點和連線閘道器的調整

- 發佈點的標準配置：單一辦公室
- 發佈點的標準配置：多個小遠端辦公室
- 手動指派受管理裝置作為發佈點使用
- 在非警戒區將 Linux 裝置連線為閘道
- 透過連線閘道將 Linux 裝置連線到管理伺服器
- 在 DMZ 中新增連線閘道作為發佈點
- 自動分配發佈點
- 在選取用作發佈點的裝置上本機安裝網路代理
- 使用發佈點作為連線閘道
- 將 IP 範圍新增至分發點輪詢的範圍清單中
- 使用發佈點作為推送伺服器

其他日常工作

- 管理管理伺服器
  - 建立管理伺服器階層：新增次要管理伺服器
  - 連線至管理伺服器及在管理伺服器之間轉換
  - 透過網際網路連線至管理伺服器的條件
  - 到管理伺服器的加密連線
    - 當裝置連線時驗證管理伺服器
    - 在管理主控台連線期間的管理伺服器身分驗證

- 配置連線到管理伺服器的 IP 位址允許清單
- 使用 klscflag 公用程式關閉連接埠 13291
- 從管理伺服器斷開連線
- 將管理伺服器新增至主控台樹狀目錄
- 從主控台樹狀目錄中刪除管理伺服器
- 將虛擬管理伺服器新增至主控台樹狀目錄
- 變更管理伺服器服務帳戶。公用程式工具 klsrvswch
- 變更 DBMS 憑證
- 使用管理伺服器節點解決問題
- 檢視和修改管理伺服器的設定
  - 調整管理伺服器的一般設定
  - 管理主控台介面設定
  - 在管理伺服器上的事件處理和儲存
  - 檢視連線到管理伺服器的記錄
  - 控制病毒爆發
  - 限制流量
  - 設定網頁伺服器
  - 管理內部使用者
- 管理伺服器設定的備份和還原
  - 使用檔案系統快照降低備份時間
  - 管理伺服器裝置不可操作
  - 管理伺服器設定或資料庫被損壞
- 備份複製和管理伺服器資料還原
  - 備份管理伺服器資料工作
  - 資料備份和還原公用程式 (klbackup)
  - 互動模式下的資料備份和還原
  - 靜默模式下的資料備份和還原
  - 使用 klbackup 公用程式切換在另一個管理伺服器的管理下的受管理裝置
  - 使用 MySQL 或 MariaDB 時備份和還原管理伺服器資料
- 將管理伺服器移動至其他裝置
- 避免多個管理伺服器之間的衝突
- 兩步驟驗證
  - 關於雙步驟驗證
  - 情境：為所有使用者配置雙步驟驗證
  - 對您自己的帳戶啟用雙步驟驗證（基於 MMC）
  - 對所有使用者啟用雙步驟驗證（基於 MMC）
  - 對使用者帳戶停用雙步驟驗證（基於 MMC）
  - 對所有使用者停用要求的雙步驟驗證（基於 MMC）
  - 從雙步驟驗證中排除帳戶（基於 MMC）
  - 編輯安全碼簽發者的名稱（基於 MMC）
  - 為您自己的帳戶配置兩步驟驗證（基於 MMC）
- 變更管理伺服器共用資料夾

對管理群組進行管理

- 建立管理群組
- 移動管理群組
- 刪除管理群組
- 自動建立管理群組架構

- 將應用程式自動安裝到管理群組中的裝置
- 管理用戶端裝置
  - 將用戶端裝置連線至管理伺服器
  - 將用戶端裝置手動連線至管理伺服器。Klmover 公用程式
  - 要建立用戶端裝置與管理伺服器之間的通道連線
  - 用戶端裝置的遠端桌面連線
    - 連線到 Windows 用戶端裝置
    - 連線到 macOS 用戶端裝置
  - 透過 Windows 桌面共用連線到用戶端裝置
  - 設定重新啟動用戶端裝置
  - 稽核在遠端用戶端裝置上執行的操作
  - 檢查用戶端裝置與管理伺服器之間的連線
    - 自動檢查用戶端裝置與管理伺服器之間的連線
    - 手動檢查用戶端裝置與管理伺服器之間的連線。Klnagchk 公用程式
    - 關於檢查裝置和管理伺服器之間的連線時間
  - 在管理伺服器上識別用戶端裝置
  - 將裝置移動至管理群組
  - 變更用戶端裝置的管理伺服器
  - 將透過連線閘道連線到管理伺服器的裝置移至另一台管理伺服器
  - 叢集和伺服器陣列
  - 遠端開啟、關閉和重新啟動用戶端裝置
  - 關於使用受管理裝置和管理伺服器之間的持續連線
  - 關於強制同步
  - 關於連線排程
  - 傳送訊息到裝置使用者
  - 管理 Kaspersky Security for Virtualization
  - 設定裝置狀態轉換
  - 標記裝置和檢視分配的標籤
    - 自動裝置標記
    - 檢視和設定分配到裝置的標籤
  - 用戶端裝置的遠端診斷。卡巴斯基安全管理中心遠端診斷公用程式
    - 使用遠端診斷公用程式連線至用戶端裝置
    - 為應用程式建立記憶體傾印檔案
    - 啟用和關閉偵錯，下載偵錯檔案
    - 下載應用程式設定
    - 下載事件記錄
    - 下載多個診斷資訊項目
    - 進行診斷並下載診斷結果
    - 啟動、停止和重新啟動應用程式
  - UEFI 防護裝置
  - 受管理裝置設定
  - 一般政策設定
  - 網路代理政策設定
- 管理使用者帳戶
  - 使用使用者帳戶
  - 新增內部使用者帳戶
  - 編輯內部使用者帳戶

變更允許的密碼輸入嘗試次數
設定內部使用者名稱的唯一性檢查
新增安全群組
新增使用者到群組
設定應用程式功能的存取權限。角色型存取控制
存取管理伺服器及其物件的權限
應用程式功能的存取權
預先定義的使用者角色
新增使用者角色
為使用者或安全群組分配角色
分配權限到使用者和群組
傳輸使用者角色到從屬管理伺服器
指派使用者作為裝置所有者
將資訊傳送給使用者
檢視使用者的行動裝置清單
為使用者安裝憑證
檢視發佈給使用者的憑證清單
關於虛擬管理伺服器的管理員
遠端佈署作業系統和應用程式
建立作業系統映像
安裝作業系統映像
設定 KSN 代理伺服器位址
新增 Windows Preinstallation Environment (WinPE) 的驅動程式
將驅動程式新增至作業系統安裝套件
設定 sysprep.exe 公用程式
佈署作業系統至新聯網的裝置
佈署作業系統至用戶端裝置
建立應用程式安裝套件
為應用程式安裝套件發佈憑證
安裝應用程式到用戶端裝置
管理物件修訂
檢視修訂歷程區域
比較物件修訂
為物件修訂和已刪除物件資訊設定儲存期限
檢視物件修訂
儲存物件修訂到檔案
回溯變更
新增修訂敘述
物件刪除
刪除物件
檢視關於已刪除物件的資訊
從已刪除物件清單永久刪除物件
行動裝置管理
情境：行動裝置管理佈署
關於管理 EAS 和 iOS MDM 裝置的群組政策
啟用行動裝置管理
修改行動裝置管理設定

停用行動裝置管理
使用行動裝置指令
行動裝置管理的指令
使用 Firebase Cloud Messaging
傳送指令
檢視指令記錄中的指令狀態
使用行動裝置的憑證
啟動憑證安裝精靈
步驟 1。選取憑證類型
步驟 2。選取裝置類型
步驟 3。選取使用者
步驟 4。選取憑證來源
步驟 5。為憑證指派標籤
步驟 6。指定憑證發佈設定
步驟 7。選取使用者通知方法
步驟 8。產生憑證
設定憑證發佈規則
與公共金鑰基礎架構整合
啟用支援 Kerberos Constrained Delegation
新增 iOS 行動裝置到受管理裝置清單
新增 Android 行動裝置到受管理裝置清單
管理 Exchange ActiveSync 行動裝置
新增管理設定檔
刪除管理設定檔
處理 Exchange ActiveSync 政策
配置掃描範圍
使用 EAS 裝置
檢視有關 EAS 裝置的資訊
將 EAS 裝置斷開管理
使用者管理 Exchange ActiveSync 行動裝置的權限
管理 iOS MDM 裝置
透過憑證籤署 iOS MDM 設定檔
新增設定檔
將設定檔安裝至裝置
從裝置中刪除設定檔
透過發佈設定檔連結來新增新裝置
透過由管理員安裝設定檔來新增新裝置
新增 provisioning 設定檔
將 provisioning 設定檔安裝至裝置
從裝置中刪除 provisioning 設定檔
新增受管應用程式
在行動裝置上安裝應用程式
將應用程式從裝置上移除
在 iOS MDM 行動裝置上設定漫遊
檢視有關 iOS MDM 裝置的資訊
將 iOS MDM 裝置斷開管理
傳送指令到裝置

檢查所傳送指令的執行狀態
管理 KES 裝置
建立 KES 裝置行動應用程式套件
啟用 KES 裝置的憑證式驗證
檢視有關 KES 裝置的資訊
將 KES 裝置斷開管理
資料加密與防護
檢視加密裝置的清單
檢視加密事件清單
將加密事件清單匯出到文字檔案中
建立和檢視加密報告
在管理伺服器之間傳輸加密金鑰
資料儲存區
將儲存區物件清單匯出到文字檔案中
安裝套件
儲存區中檔案的主狀態
智慧培訓模式中的規則觸發
檢視使用適應性異常控制規則執行的偵測清單
從適應性異常控制規則新增排除
步驟 1。選取應用程式
步驟 2。選取政策
步驟 3。執行政策
隔離區和備份區
啟用儲存區檔案遠端管理
檢視儲存區的檔案內容
從儲存區刪除檔案
從儲存區還原檔案
將儲存區中的檔案儲存到磁碟
掃描隔離區中的檔案
活動威脅
解毒未處理檔案
將未處理的檔案儲存到磁碟
從「主動威脅」資料夾中刪除檔案
卡巴斯基安全網路 (KSN)
關於 KSN
設定到卡巴斯基安全網路的存取
啟用和停用 KSN
檢視接受的 KSN 聲明
檢視 KSN 代理伺服器統計資訊
接受更新的 KSN 聲明
使用卡巴斯基安全網路獲得增強防護
檢查發佈點是否作為 KSN 代理伺服器運作
在線上說明和離線說明之間切換
匯出到 SIEM 系統的事件
設定事件匯出到 SIEM 系統
在您開始之前
卡巴斯基安全管理中心中的事件

關於事件匯出
配置在 SIEM 系統中的事件匯出
標記事件，將其以 Syslog 格式匯出到 SIEM 系統
關於標記事件並將其以 Syslog 格式匯出到 SIEM 系統
將 Kaspersky 應用程式的事件標記為以 Syslog 格式匯出
標記一般事件，將其以 Syslog 格式匯出
關於使用 Syslog 格式匯出事件
使用 CEF 和 LEEF 格式匯出事件
將事件轉換為 CEF 或 LEEF 格式
配置卡巴斯基安全管理中心以將事件匯出到 SIEM 系統
直接從資料庫匯出事件
使用 klsql2 實用程式執行 SQL 查詢
klsql2 實用程式中的 SQL 查詢例子
檢視卡巴斯基安全管理中心資料庫名稱
檢視匯出結果
使用 SNMP 將統計資訊發送到協力廠商應用程式
設定 SNMP 服務以與卡巴斯基安全管理中心結合使用
SNMP 代理和物件識別碼
從物件識別碼取得字串計數器名稱
SNMP 的物件識別碼值
故障排除
使用雲端環境
關於使用雲端環境
情境：在雲端環境中佈署
在雲端環境中佈署卡巴斯基安全管理中心的先決條件
雲端環境中管理伺服器的硬體要求
雲端環境中的產品授權選項
在雲端環境中工作的資料庫選項
使用 Amazon Web Services 雲端環境
關於使用 Amazon Web Services 雲端環境
為 Amazon EC2 實例建立 IAM 角色和 IAM 使用者帳戶
確保卡巴斯基安全管理中心管理伺服器具有使用 AWS 的權限
為管理伺服器建立 IAM 角色
建立 IAM 使用者帳戶以使用卡巴斯基安全管理中心
為安裝應用程式到 Amazon EC2 實例建立 IAM 角色
使用 Amazon RDS
建立 Amazon RDS 實例
為 Amazon RDS 實例建立選項群組
修改選項群組
為 IAM 角色修改權限以使用 Amazon RDS 資料庫實例
為資料庫準備 Amazon S3 bucket
遷移資料庫到 Amazon RDS
工作在 Microsoft Azure 雲端環境
關於使用 Microsoft Azure
建立訂購、應用程式 ID 和密碼
分配角色到 Azure 應用程式 ID
在 Microsoft Azure 中佈署管理伺服器並選取資料庫

使用 Azure SQL
建立 Azure 儲存帳戶
建立 Azure SQL 資料庫和 SQL Server
遷移資料庫到 Azure SQL
在 Google Cloud 中使用
建立客戶電子郵件，專案 ID 和私密金鑰
使用 Google Cloud SQL for MySQL 實例
在雲端環境中準備必要的用戶端裝置以使用卡巴斯基安全管理中心
建立設定雲端環境所需的安裝套件
設定雲端環境
關於設定雲端環境精靈
步驟 1。選取應用程式啟動方式
步驟 2。選取雲端環境
步驟 3。在雲端環境中授權
步驟 4。配置與雲端的同步並選取後續操作
步驟 5。在雲端環境中配置卡巴斯基安全網路
步驟 6。在雲端環境中配置電子郵件通知
步驟 7。建立雲端環境保護的初始配置
步驟 8。選取安裝過程中必須重啟操作系統時的動作（針對雲端環境）
步驟 9。透過管理伺服器接收更新
檢查設定
雲端裝置群組
網路區段投票
為雲端區段輪詢新增連線
為雲端區段輪詢刪除連線
配置輪詢排程
安裝應用程式到雲端環境中的裝置
檢視雲端裝置內容
與雲端同步
卡巴斯基安全管理中心在 Yandex.Cloud 中的佈署
附錄
進階功能
卡巴斯基安全管理中心自動化作業。klakaut 公用程式
自訂工具
網路代理磁碟克隆模式
準備已安裝網路代理的參照裝置以建立作業系統映像
配置從檔案完整性監控接收訊息
管理伺服器維護
存取公用 DNS 伺服器
使用者通知方法視窗
“一般”區域
裝置分類視窗
定義新物件名稱視窗
“應用程式類別”區域
使用管理介面的功能
主控台樹狀目錄
如何在工作台中更新資料

- 如何瀏覽主控台樹狀目錄
- 如何在工作台開啟物件內容視窗
- 如何在工作台中選取一群組物件
- 如何在工作台中變更表列集
- 參考資訊
- 上下文功能表指令
- 受管理裝置清單。列敘述
- 裝置、工作和政策的狀態
- 管理主控台上的檔案狀態圖示
- 搜尋和匯出資料
- 尋找裝置
- 裝置搜尋設定
- 在字串變數中使用遮罩
- 在搜尋欄位使用規則運算式
- 從對話方塊匯出清單
- 工作設定
- 一般工作設定
- "將更新下載至管理伺服器儲存區"工作設定
- 「將更新下載至發佈點儲存區」工作設定
- 「弱點掃描和所需更新」工作設定
- 「安裝所需更新並修復弱點」工作設定
- 子網路全域清單
- 新增子網路到子網路全域清單
- 在子網路全域清單中檢視和修改子網路內容
- Windows、macOS 和 Linux 網路代理的使用：比較
- 按作業系統比較網路代理設定

卡巴斯基安全管理中心網頁主控台

- 關於卡巴斯基安全管理中心網頁主控台
- 卡巴斯基安全管理中心網頁主控台的硬體和軟體需求
- 卡巴斯基安全管理中心管理伺服器佈署圖表和卡巴斯基安全管理中心網頁主控台
- 卡巴斯基安全管理中心 網頁主控台使用的連接埠
- 情境：卡巴斯基安全管理中心網頁主控台的安裝和初始化設定
- 安裝
- 安裝卡巴斯基安全管理中心網頁主控台
- 安裝卡巴斯基安全管理中心 網頁主控台到 Linux 平台
- 安裝卡巴斯基安全管理中心網頁主控台到 Linux 平台
- 卡巴斯基安全管理中心網頁主控台安裝參數
- 安裝連線到安裝在容錯移轉叢集節點上的管理伺服器的卡巴斯基安全管理中心網頁主控台
- 升級卡巴斯基安全管理中心網頁主控台
- 用於卡巴斯基安全管理中心網頁主控台的憑證
- 取代卡巴斯基安全管理中心網頁主控台憑證
- 在卡巴斯基安全管理中心網頁主控台中，為受信任的管理伺服器指定憑證
- 將 PFX 憑證轉換為 PEM 格式
- 從 Kaspersky Security Center Windows 進行移轉
- 移轉至卡巴斯基安全管理中心雲端主控台
- 遷移到 Kaspersky Next XDR Expert
- 移轉到卡巴斯基安全管理中心 Linux

透過使用移轉精靈移轉到卡巴斯基安全管理中心 Linux
從卡巴斯基安全管理中心 Windows 匯出群組物件
將匯出的檔案匯入到卡巴斯基安全管理中心 Linux
將受管理裝置切換到卡巴斯基安全管理中心 Linux 的管理之下
使用管理伺服器資料備份遷移到卡巴斯基安全管理中心 Linux
登入到卡巴斯基安全管理中心網頁主控台並登出
在卡巴斯基安全管理中心網頁主控台中的身分和存取管理器
關於身分和存取管理器
啟用身分和存取管理器：情境
在卡巴斯基安全管理中心 網頁主控台中配置身分和存取管理器
在卡巴斯基安全管理中心網頁主控台中註冊 Kaspersky Industrial CyberSecurity for Networks 應用程式
身分和存取管理器的權杖存留期和授權逾時
下載和分發 IAM 憑證
停用身分和存取管理器
使用 NTLM 和 Kerberos 通訊協定設定網域身分驗證
設定管理伺服器
配置卡巴斯基安全管理中心 網頁主控台到管理伺服器的連線
配置管理伺服器連線事件記錄
設定管理伺服器網際網路存取設定
設定事件儲存區中的最大事件數量
UEFI 防護裝置連線設定
建立管理伺服器階層：新增次要管理伺服器
檢視從屬管理伺服器清單
刪除管理伺服器階層
管理伺服器維護
設定介面
管理虛擬管理伺服器
建立虛擬管理伺服器
啓用和停用虛擬管理伺服器
為虛擬管理伺服器指派管理員
變更用戶端裝置的管理伺服器
刪除虛擬管理伺服器
啟用帳戶防護以防止未經授權的修改
兩步驟驗證
關於雙步驟驗證
為所有使用者配置兩步驟驗證
對您自己的帳戶啟用雙步驟驗證（網頁主控台）
對所有使用者啟用要求的雙步驟驗證（網頁主控台）
對使用者帳戶停用雙步驟驗證（網頁主控台）
對所有使用者停用要求的雙步驟驗證（網頁主控台）
從雙步驟驗證中排除帳戶
產生新的金鑰
編輯安全碼簽發者的名稱（網頁主控台）
對您自己的帳戶停用雙步驟驗證（網頁主控台）
備份複製和管理伺服器資料還原
重新發佈卡巴斯基安全管理中心網頁主控台憑證
建立資料備份工作

- 將管理伺服器移動至其他裝置
- 使用 klscmodchk 和 integrity_checker 實用程式檢查模組的完整性

卡巴斯基安全管理中心網頁主控台初始設定

- 快速啟動精靈（卡巴斯基安全管理中心網頁主控台）
  - 步驟 1：指定網際網路連線設定
  - 步驟 2。下載所需的更新
  - 步驟 3。選擇要防護的資產
  - 步驟 4。在解決方案中選取加密方式
  - 步驟 5。為受管理應用程式配置外掛程式安裝
  - 步驟 6。下載分發套件並建立安裝套件
  - 步驟 7。設定卡巴斯基安全網路
  - 步驟 8。選取應用程式啟動方式
  - 步驟 9。指定協力廠商更新管理設定
  - 步驟 10。建立基本的網路保護設定
  - 步驟 11。設定電子郵件通知
  - 步驟 12。執行網路輪詢
  - 步驟 13。關閉快速啟動精靈
- 連線漫遊裝置
  - 情境：透過連線閘道連線辦公室外的裝置
  - 情境：通過 DMZ 中的從屬管理伺服器連線漫遊裝置
  - 關於連線辦公室外的裝置
  - 將外部桌上型裝置連線到管理伺服器
  - 關於漫遊使用者的連線設定檔
  - 為漫遊使用者建立連線設定檔
  - 關於將網路代理切換到其他管理伺服器
  - 依據網路位置建立網路代理轉換規則

防護佈署精靈

- 步驟 1。開始防護佈署精靈
- 步驟 2。選取安裝套件
- 步驟 3。選取金鑰檔案或啟動碼的發佈方式
- 步驟 4。選取網路代理版本
- 步驟 5。選取裝置
- 步驟 6。指定遠端安裝工作設定
- 步驟 7。重新啟動管理
- 步驟 8。安裝前移除不相容的應用程式
- 步驟 9。移動裝置到受管理裝置
- 步驟 10。選取存取裝置的帳戶
- 步驟 11。啟動安裝

透過卡巴斯基安全管理中心網頁主控台佈署 Kaspersky 應用程式

- 情境：透過卡巴斯基安全管理中心網頁主控台佈署 Kaspersky 應用程式
- 獲取 Kaspersky 應用程式外掛程式
- 下載和建立 Kaspersky 應用程式的安裝套件
- 變更自訂安裝套件資料大小限制
- 為 Kaspersky 應用程式下載分發套件
- 檢查 Kaspersky Endpoint Security 已成功部署
- 建立獨立安裝套件
- 檢視獨立安裝套件清單

- 建立自訂安裝套件
- 分發安裝套件至從屬管理伺服器
- 使用遠端軟體安裝工作安裝應用程式
  - 遠端安裝應用程式
  - 透過 Active Directory 群組政策安裝應用程式
  - 在從屬管理伺服器上安裝應用程式
- 指定在 Unix 裝置上進行遠端安裝的設定
- 啟動和停止卡巴斯基應用程式
- 行動裝置管理
- 取代協力廠商安全應用程式

發現網路裝置

- 情境：發現網路裝置
- 裝置發現
  - Windows 網路輪詢
  - Active Directory 輪詢
  - IP 範圍輪詢
  - 新增和修改 IP 範圍
  - Zeroconf 輪詢
  - 為未配置的裝置配置保留規則

Kaspersky 應用程式：產品授權和啟動

- 受管理應用程式的產品授權
- 新增產品授權金鑰到管理伺服器儲存區
- 佈署產品授權金鑰到用戶端裝置
- 自動分發產品授權金鑰
- 檢視使用中產品授權金鑰的相關資訊
- 從儲存區移除產品授權金鑰
- 撤銷最終使用者產品授權協議的許可
- 續約 Kaspersky 應用程式的產品授權
- 使用卡巴斯基市場選擇卡巴斯基商業解決方案

配置網路防護

- 情境：配置網路防護
- 關於以裝置為中心和以使用者為中心的安全管理方法
- 政策設定和傳播：以裝置為中心的方法
- 政策設定和傳播：以使用者為中心的方法
- 網路代理政策設定
- Kaspersky Endpoint Security 政策的手動設定
  - 設定卡巴斯基安全網路
  - 檢查受防火牆防護的網路清單
  - 停用網路磁碟機掃描
  - 從管理伺服器記憶體中排除軟體詳細資訊
  - 在工作站上設定對 Kaspersky Endpoint Security for Windows 介面的存取
  - 在管理伺服器資料庫中儲存重要的政策事件
- Kaspersky Endpoint Security 更新群組工作的手動設定
- 授予離線存取權限給受裝置控制封鎖的外部裝置
- 遠端移除應用程式或軟體更新
- 回溯物件到先前修訂
- 工作

- 關於工作
- 關於工作範圍
- 建立工作
- 手動啟動工作
- 檢視工作清單
- 一般工作設定
- 匯出工作
- 匯入工作
- 啟動變更工作密碼精靈
  - 步驟 1。指定憑證
  - 步驟 2。選取要採取的動作
  - 步驟 3。檢視結果

管理用戶端裝置

- 受管理裝置設定
- 建立管理群組
- 將裝置手動新增至管理群組
- 將裝置手動移動至管理群組
- 建立裝置移動規則
- 複製裝置移動規則
- 裝置移動規則的條件
- 當裝置顯示不活動時檢視和配置操作
- 關於裝置狀態
- 設定裝置狀態轉換
- 用戶端裝置的遠端桌面連線
- 透過 Windows 桌面共用連線到用戶端裝置
- 裝置分類
  - 從裝置分類中檢視裝置清單
  - 建立裝置分類
  - 配置裝置分類
  - 從裝置分類中匯出裝置清單
  - 在分類中從管理群組中刪除裝置
- 裝置標籤
  - 裝置標籤
  - 建立裝置標籤
  - 重命名裝置標籤
  - 刪除裝置標籤
  - 檢視分配了標籤的裝置
  - 檢視分配到裝置的標籤
  - 手動標記裝置
  - 從裝置上刪除分配的標籤
  - 檢視自動標記裝置規則
  - 編輯自動標記裝置規則
  - 建立自動標記裝置規則
  - 為自動標記裝置執行規則
  - 刪除自動標記裝置規則
  - 使用 klscflag 公用程式管理裝置標籤

政策和政策設定檔

- 關於政策和政策設定檔
- 關於鎖定和已鎖定的設定
- 政策繼承和政策設定檔
  - 政策層次結構
  - 政策層次結構中的政策設定檔
  - 如何在受管理裝置上實作設定
- 管理政策
  - 檢視政策清單
  - 建立政策
  - 修改政策
  - 一般政策設定
  - 啟用和停用政策繼承選項
  - 複製政策
  - 移動政策
  - 匯出政策
  - 匯入政策
  - 檢視政策發佈狀態圖表
  - 刪除政策
- 管理政策設定檔
  - 檢視政策設定檔
  - 變更政策設定檔優先順序
  - 建立政策設定檔
  - 修改政策設定檔
  - 複製政策設定檔
  - 建立政策設定檔啟動規則
  - 刪除政策設定檔

資料加密與防護

- 檢視加密磁碟機的清單
- 檢視加密事件清單
- 建立和檢視加密報告
- 以離線模式授予加密磁碟機的存取權限

使用者和使用者角色

- 關於用於角色
- 檢視使用者帳戶和工作階段
- 設定應用程式功能的存取權限。角色型存取控制
  - 應用程式功能的存取權
  - 預先定義的使用者角色
  - 為特定物件分配存取權限
  - 分配存取權限給使用者和安全群組
- 新增內部使用者帳戶
- 建立安全群組
- 編輯內部使用者帳戶
- 編輯安全群組
- 新增使用者帳戶到內部群組
- 指派使用者作為裝置所有者
- 刪除使用者或安全群組
- 建立使用者角色

編輯使用者角色
編輯使用者角色範圍
刪除使用者角色
關聯政策設定檔到角色
傳輸使用者角色到從屬管理伺服器
在卡巴斯基安全管理中心網頁主控台中管理物件
新增修訂敘述
物件刪除
卡巴斯基安全網路 (KSN)
關於 KSN
設定對 KSN 的存取
啟用和停用 KSN
檢視接受的 KSN 聲明
接受更新的 KSN 聲明
檢查發佈點是否作為 KSN 代理伺服器運作
更新 Kaspersky 資料庫和應用程式
情境：定期更新 Kaspersky 資料庫與應用程式
關於更新 Kaspersky 資料庫、軟體模組和應用程式
建立「將更新下載至管理伺服器儲存區」工作
驗證已下載的更新
建立"將更新下載至發佈點儲存區"工作
啟用和停用卡巴斯基安全管理中心元件的自動更新和修補程式
自動安裝 Kaspersky Endpoint Security for Windows 的更新
批准和拒絕軟體更新
更新管理伺服器
啟用和停用行動模式更新下載
在離線裝置上更新 Kaspersky 資料庫和軟體模組
備份和還原 Web 外掛程式
發佈點和連線閘道器的調整
發佈點的標準配置：單一辦公室
發佈點的標準配置：多個小遠端辦公室
關於分配發佈點
自動分配發佈點
手動分配發佈點
修改管理群組的發佈點清單
強制同步
啟用推送伺服器
管理用戶端裝置上的協力廠商應用程式
關於協力廠商應用程式
安裝協力廠商軟體更新
安裝協力廠商軟體更新
建立「弱點掃描和所需更新」工作
「弱點掃描和所需更新」工作設定
建立「安裝必要更新並修復弱點」工作
新增安裝更新的規則
建立「安裝 Windows Update 更新」工作
檢視可用協力廠商軟體更新的資訊

- 將可用軟體更新清單匯出至檔案
- 核准與拒絕協力廠商軟體更新
- 建立執行 Windows Update 同步的工作
- 自動更新協力廠商應用程式
- 情境：更新協力廠商軟體
- 修復協力廠商軟體弱點
  - 情境：尋找與修復協力廠商軟體弱點
  - 關於尋找與修復軟體弱點
  - 修復協力廠商軟體弱點
  - 建立修復弱點工作
  - 建立「安裝必要更新並修復弱點」工作
  - 新增安裝更新的規則
  - 選取適用於協力廠商軟體中弱點的使用者修復項目
  - 檢視在所有受管理裝置上偵測到的軟體弱點
  - 檢視在受管理裝置上偵測到的軟體弱點的資訊
  - 檢視受管理裝置的弱點統計資料
  - 將軟體弱點匯出至檔案中
  - 忽略軟體弱點
- 管理用戶端裝置上的應用程式執行
  - 使用「應用程式控制」來管理可執行檔
  - 應用程式控制模式和類別
  - 取得並檢視安裝在用戶端裝置的應用程式清單
  - 取得並檢視儲存在用戶端裝置上的可執行檔清單
  - 建立含有手動新增內容的應用程式類別
  - 建立應用程式類別以包含來自所選裝置的可執行檔
  - 建立應用程式類別以包含來自所選資料夾的可執行檔
  - 檢視應用程式類別清單
  - 在 Kaspersky Endpoint Security for Windows 政策配置應用程式控制
  - 新增事件相關的可執行檔到應用程式類別
- 從卡巴斯基資料庫建立協力廠商應用程式的安裝套件
- 從卡巴斯基資料庫檢視和修改協力廠商應用程式的安裝套件設定
- Kaspersky 資料庫協力廠商應用程式的安裝套件設定
- 應用程式標籤
  - 建立應用程式標籤
  - 重命名應用程式標籤
  - 分配標籤到應用程式
  - 從應用程式上刪除分配的標籤
  - 刪除應用程式標籤

監控和報告

- 方案：監控和報告
- 關於監控和報告的類型
- 儀表板和小部件
  - 使用儀表板
  - 新增小部件到儀表板
  - 從儀表板隱藏小部件
  - 移動儀表板上的小部件
  - 變更部件尺寸或樣子

- 變更部件設定
- 關於“僅儀表板”模式
- 配置“僅儀表板”模式
- 報告
  - 使用報告
  - 建立報告範本
  - 檢視和編輯報告範本內容
  - 匯出報告到檔案
  - 生成和瀏覽報告
  - 建立報告傳送工作
  - 刪除報告範本
- 事件和事件分類
  - 關於卡巴斯基安全管理中心事件
  - 使用事件分類
    - 建立事件分類
    - 編輯事件分類
    - 檢視事件分類清單
    - 刪除事件分類
  - 檢視事件詳情
  - 匯出事件到檔案
  - 匯出事件到 SIEM 系統
    - 設定事件匯出到 SIEM 系統
    - 在您開始之前
    - 關於事件匯出
    - 配置在 SIEM 系統中的事件匯出
    - 標記事件，將其以 Syslog 格式匯出到 SIEM 系統
      - 關於標記事件並將其以 Syslog 格式匯出到 SIEM 系統
      - 將 Kaspersky 應用程式的事件標記為以 Syslog 格式匯出
      - 標記一般事件，將其以 Syslog 格式匯出
    - 使用 CEF 和 LEEF 格式匯出事件
    - 關於使用 Syslog 格式匯出事件
    - 配置卡巴斯基安全管理中心以將事件匯出到 SIEM 系統
    - 直接從資料庫匯出事件
      - 使用 klsql2 實用程式執行 SQL 查詢
      - klsql2 實用程式中的 SQL 查詢例子
      - 檢視卡巴斯基安全管理中心資料庫名稱
    - 檢視匯出結果
  - 從事件檢視物件歷程
  - 刪除事件
  - 設定事件儲存期限
  - 卡巴斯基安全管理中心元件的事件
    - 事件類型描述的資料結構
    - 管理伺服器事件
      - 管理伺服器緊急事件
      - 管理伺服器功能失效事件
      - 管理伺服器警告事件
      - 管理伺服器資訊事件

網路代理事件
網路代理功能失效事件
網路代理警告事件
網路代理資訊事件
iOS MDM 伺服器事件
iOS MDM 伺服器功能失效事件
iOS MDM 伺服器警告事件
iOS MDM 伺服器資訊事件
Exchange 行動裝置伺服器事件
Exchange 行動裝置伺服器功能失效事件
Exchange 行動裝置伺服器資訊事件
封鎖頻繁事件
關於封鎖頻發事件
管理頻發事件封鎖
移除對頻發事件的封鎖
從 Kaspersky Security for Microsoft Exchange Server 接收事件
通知和裝置狀態
使用通知
檢視螢幕通知
關於裝置狀態
設定裝置狀態轉換
配置通知傳送
透過執行可執行檔顯示的事件通知
卡巴斯基公告
關於卡巴斯基公告
指定卡巴斯基公告設定
停用卡巴斯基公告
檢視有關威脅偵測的資訊
從隔離和備份下載和刪除檔案
從隔離和備份下載檔案
卡巴斯基安全管理中心網頁主控台活動記錄
卡巴斯基安全管理中心和其他解決方案之間的整合
配置到 KATA / KEDR 網頁主控台的存取
建立背景連線
在雲端環境中搭配卡巴斯基安全管理中心網頁主控台使用
卡巴斯基安全管理中心網頁主控台中的雲端環境設定
步驟 1。檢查需要的外掛程式和安裝套件
步驟 2。許可應用程式
步驟 3。選取雲端環境與授權
步驟 4。區段輪詢，設定與雲端的同步並選取後續操作
步驟 5。選擇一個應用程式來為其建立政策和工作
步驟 6。設定適用於卡巴斯基安全管理中心的卡巴斯基安全網路
步驟 7。建立初始保護設定
透過卡巴斯基安全管理中心網頁主控台進行網路區段輪詢
為雲端區段輪詢新增連線
為雲端區段輪詢刪除連線
透過卡巴斯基安全管理中心網頁主控台設定輪詢排程

透過卡巴斯基安全管理中心 網頁主控台檢視雲端區段輪詢結果
透過卡巴斯基安全管理中心 網頁主控台檢視雲端裝置內容
與雲端同步：設定移動規則
將應用程式遠端安裝到 Azure 虛擬機
使用雲端 DBMS建立管理伺服器資料的備份工作
用戶端裝置的遠端診斷
開啟遠端診斷視窗
啟用與停用應用程式偵錯
下載應用程式偵錯檔案
刪除偵錯檔案
下載應用程式設定
下載事件記錄
啟動、停止、重新啟動應用程式
執行卡巴斯基安全管理中心網路代理的遠端診斷並下載結果
在用戶端裝置執行應用程式
為應用程式建立記憶體傾印檔案
變更卡巴斯基安全管理中心網頁主控台介面的語言
API 參考手冊
服務供應商最佳實踐
排程卡巴斯基安全管理中心佈署
提供到管理伺服器的網際網路存取
卡巴斯基安全管理中心標準設定
關於發佈點
管理伺服器階層
虛擬管理伺服器
使用 Kaspersky Endpoint Security for Android 管理行動裝置
佈署和初始化設定
管理伺服器安裝建議
在失敗轉移叢集上為管理伺服器服務建立帳戶
選取 DBMS
指定管理伺服器位址
在用戶端組織網路中設定防護
Kaspersky Endpoint Security 政策的手動設定
在進階威脅防護區域配置政策
在關鍵威脅防護部分配置政策
在一般設定部分配置政策
在事件配置區域配置政策
Kaspersky Endpoint Security 更新群組工作的手動設定
Kaspersky Endpoint Security 裝置掃描群組工作的手動設定
排程「尋找弱點和所需更新」工作
更新安裝和弱點修復群組工作的手動設定
建立管理群組結構和分配發佈點
標準 MSP 用戶端設定：單一辦公室
標準 MSP 用戶端設定：多個小遠端辦公室
政策層級，使用政策設定檔
政策層次結構
政策設定檔

工作
裝置移動規則
軟體分類
關於多租戶應用程式
管理伺服器設定的備份和還原
管理伺服器裝置不可操作
管理伺服器設定或資料庫被損壞
佈署網路代理和安全應用程式
初始化佈署
配置安裝程式
安裝套件
MSI 內容和轉換檔案
使用應用程式遠端安裝的協力廠商工具佈署
卡巴斯基安全管理中心中遠端安裝工作的一般資訊
使用 Microsoft Windows 群組政策佈署
透過卡巴斯基安全管理中心遠端安裝工作的強制佈署
執行卡巴斯基安全管理中心建立的獨立安裝套件
手動安裝應用程式的選項
建立 MST 檔案
在安裝有網路代理的裝置上遠端安裝應用程式
在遠端安裝工作中管理裝置重新啟動
病毒防護應用程式安裝套件上的資料庫更新
刪除不相容的協力廠商安全應用程式
使用命令提示字元刪除受密碼防護的網路代理
在卡巴斯基安全管理中心中使用工具遠端安裝應用程式以便在受管理裝置上執行相關可執行檔
監控佈署
配置安裝程式
一般資訊
在靜默模式下安裝（帶有回應檔案）
在靜默模式下安裝（沒有回應檔案）
透過 setup.exe 的部分安裝配置
管理伺服器安裝參數
網路代理安裝參數
虛擬基礎架構
降低虛擬機負載的竅門
對動態虛擬機的支援
對虛擬機複製的支援
對網路代理裝置檔案系統回溯的支援
關於漫遊使用者的連線設定檔
佈署行動裝置管理功能
將 KES 裝置連線至管理伺服器
直接連線裝置到管理伺服器
連線 KES 裝置到 Kerberos constrained delegation (KCD) 伺服器的方案
使用 Firebase Cloud Messaging
與公共金鑰基礎架構整合
卡巴斯基安全管理中心網頁伺服器
其他日常工作

在管理主控台中監控交通信號燈和記錄的事件
遠端存取受管理裝置
使用"不要中斷與管理伺服器的連線"選項在受管理裝置和管理伺服器之間提供持續連線
關於檢查裝置和管理伺服器之間的連線時間
關於強制同步
關於通道
度量手冊
關於本手冊
卡巴斯基安全管理中心的限制資訊
管理伺服器計算
管理伺服器的硬體資源計算
DBMS 和管理伺服器的硬體需求
資料庫空間計算
磁碟空間計算（使用或不使用弱點和修補程式管理功能）
計算管理伺服器的數量和配置
將動態虛擬機連線到卡巴斯基安全管理中心時的建議事項
發佈點和連線閘道的計算
發佈點需求
計算發佈點的數量和配置
連線閘道數量計算
工作和政策事件資訊的記錄
特別考慮和特定工作的最佳化設定
裝置發現頻率
管理伺服器資料備份工作和管理伺服器維護工作
更新 Kaspersky Endpoint Security 的群組工作
清查工作
管理伺服器和受防護裝置間的網路負載詳情
不同方案下的流量消耗
24 小時平均流量使用
聯絡技術支援
如何取得技術支援
透過 Kaspersky CompanyAccount 取得技術支援
取得管理伺服器的傾印檔案
有關程式的資訊來源
詞彙表
Amazon EC2 實例
Amazon 系統映像 (AMI)
Android 裝置
AWS Application Program Interface (AWS API)
AWS IAM 存取金鑰
AWS 管理主控台
EAS 裝置
Exchange 行動裝置伺服器
HTTPS
IAM 使用者
IAM 角色
iOS MDM 伺服器

iOS MDM 裝置
iOS MDM 設定檔
JavaScript
Kaspersky 更新伺服器
KES 裝置
Provisioning 設定檔
SSL
UEFI 防護裝置
Windows Server 更新服務 (WSUS)
不相容應用程式
中間人攻擊
事件儲存區
事件嚴重等級
修補程式重要等級
備份資料夾
內部使用者
共用憑證
卡巴斯基安全管理中心操作員
卡巴斯基安全管理中心管理員
卡巴斯基安全管理中心系統健康驗證程式 (SHV)
卡巴斯基安全管理中心網頁伺服器
卡巴斯基安全網路 (KSN)
卡巴斯基私有安全網路 (KPSN)
受管理裝置
可用更新
安裝套件
工作
工作設定
廣播網域
弱點
強制安裝
應用程式商店
手動安裝
指定裝置的工作
授權檔案
授權的應用程式群組
政策
啟動產品授權
更新
服務供應商管理員
本機安裝
本機工作
歸屬管理伺服器
產品授權期限
用戶端管理員
病毒活動臨界值
病毒爆發

病毒資料庫
病毒防護服務供應商
發佈點
直接應用程式管理
程式設定
管理主控台
管理伺服器
管理伺服器憑證
管理伺服器用戶端（用戶端裝置）
管理伺服器資料備份
管理員工作站
管理員權限
管理外掛程式
管理群組
網路代理
網路位置辨識 (NLA)
網路病毒防護
網路防護狀態
群組工作
虛擬管理伺服器
行動裝置伺服器
裝置所有者
角色群組
設定檔
設定檔
身分和存取管理 (IAM)
身分驗證代理
輕量級 Nagent（LWNGT）
連線閘道
遠端安裝
還原
還原管理伺服器資料
防護狀態
附加（或備用）產品授權金鑰
隔離區域 (DMZ)
集中式應用程式管理
雲端環境
有關協力廠商代碼的資訊
商標聲明
已知問題

卡巴斯基安全管理中心 14.2 說明

	**新增內容** 在最新應用程式版本中的新增內容。		**配置網路防護** 管理組織的安全。
	**硬體和軟體需求** 檢查支援什麼作業系統和應用程式版本。		**Kaspersky 應用程式。更新資料庫和軟體模組** 維持防護系統的可靠性。
	**佈署和初始化設定** 計畫資源使用、安裝管理伺服器、安裝網路代理和安全應用程式到用戶端裝置，以及整理裝置到管理群組。		**監控和報告** 檢視您的基礎架構、防護狀態和統計資訊。
	**發現網路裝置** 發現您組織網路中的現有裝置和新裝置。		**取代協力廠商安全應用程式** 學習移除不相容應用程式的方法。
	**Kaspersky 應用程式。集中佈署** 佈署 Kaspersky 應用程式。		**發佈點和連線閘道器的調整** 配置發佈點。
	**從先前版本升級卡巴斯基安全管理中心** 從先前版本升級至卡巴斯基安全管理中心 14.2。		**服務供應商的最佳實務（僅限線上說明）** 學習如何佈署、配置和使用應用程式的建議，以及解決應用程式操作中的典型問題的方法。
	**Kaspersky 應用程式。產品授權和啟動** 幾步啟動 Kaspersky 應用程式。		**規模指南（僅限線上說明）** 要在不同的條件下最佳化效能，需要考慮網路裝置數量、網路拓撲和您需要的卡巴斯基安全管理中心功能集。
	**匯出事件到 SIEM 系統** 配置將事件匯出到 SIEM 系統以進行分析。		**弱點和修補程式管理** 尋找和修復協力廠商軟體中的弱點。
	**使用雲端環境** 在雲端環境中佈署卡巴斯基安全管理中心：Amazon Web Services™、Microsoft Azure™、Google™ Cloud Platform。		**Frequently Asked Questions（僅限英語）** 查找有關如何解決常見問題的說明。
	**Kaspersky Endpoint Security for Business 快速入門指南** 開始使用 Kaspersky Endpoint Security for Business：安裝和配置此解決方案。您還可以查看卡巴斯基安全管理中心的功能比較，以選擇最合適的網路安全管理方式。		

新增內容

卡巴斯基安全管理中心 14.2

卡巴斯基安全管理中心 14.2 有幾項新功能和改善事項：

- 一個新的硬化指南已發佈。我們強烈建議您仔細閱讀指南並按照安全建議設定卡巴斯基安全管理中心和您的網路基礎架構。

  另外，請安裝卡巴斯基安全管理中心的最新更新。此更新包括基礎架構防護功能，例如使用者帳戶的雙步驗證和其他改進。

- 現在會自動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，則應用程式使用公用 DNS。

- 虛擬管理伺服器上的使用者權限可隨時獨立於主管理伺服器之外進行設定。此外，您可以為主伺服器使用者分配管理虛擬伺服器的權限。

- 卡巴斯基安全管理中心現在支援搭配使用以下 DBMS：

  - PostgreSQL 13.x
  - PostgreSQL 14.x
  - Postgres Pro 13.x（所有版本）
  - Postgres Pro 14.x（所有版本）
  - MariaDB 10.1, 10.4, 10.5

- 您可以使用卡巴斯基安全管理中心網頁主控台，將政策和工作匯出到一個檔案，接著將政策和工作匯入到卡巴斯基安全管理中心 Windows 或卡巴斯基安全管理中心 Linux。

- 以下工作已移除**不使用代理伺服器**選項：

  - *將更新下載至管理伺服器儲存區*
  - *將更新下載至發佈點儲存區*

- 如要在雲端環境中保護用戶端裝置，您可以部署 Kaspersky Endpoint Security for Windows 而不是 Kaspersky Security for Windows Server。此功能現在 Kaspersky Endpoint Security 12.0 for Windows 發佈後可用。

- 使用加密金鑰現在受**一般功能**：**加密金鑰管理**功能區域的存取權限限制。如果卡巴斯基安全管理中心使用者擁有**讀取**權限，他們現在可以匯出加密金鑰；如果他們擁有**寫入**權限，他們可以匯入加密金鑰。

卡巴斯基安全管理中心 14

卡巴斯基安全管理中心 14 有幾項新功能和改善事項：

- 您可以安裝更新並修復隔離網路中的協力廠商軟體的弱點（Microsoft 軟體除外）。此類網路包括管理伺服器和無法存取網際網路的受管理裝置。要修復此類網路中的弱點，您需要使用具有網際網路存取權限的管理伺服器下載所需的更新，然後將修補程式傳輸到隔離的管理伺服器。

- 已為 macOS 裝置新增了漫遊使用者的連線設定檔。透過使用連線設定檔，您可以為 macOS 裝置上的網路代理配置連線到相同或不同管理伺服器的規則，具體取決於裝置位置。

- 網路代理現在可以安裝在執行 Microsoft Windows 10 IoT 企業版的裝置上。

- 在**威脅報告**中，您現在可以過濾威脅清單以僅檢視 Cloud Sandbox 偵測到的威脅。

- 卡巴斯基安全中心現在支援使用 Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 作為受管理應用程式。

卡巴斯基安全管理中心網頁主控台有幾項新功能和改善事項：

- 您可以為不管理網路但希望在卡巴斯基安全管理中心中檢視網路防護統計資訊的員工（例如，高級經理）配置僅儀表板模式。當使用者啟用此模式時，只會顯示一個含有一組預先定義小工具的儀表板。因此，他或她可以監控小工具中指定的統計資訊，例如，所有受管理裝置的防護狀態、最近檢測到的威脅數量或網路中最常見的威脅清單。

- 卡巴斯基安全管理中心網頁主控台現在支援 Kaspersky Security for iOS 為安全應用程式。

- 在工作屬性中，您可以指定是否要將工作套用到子群組和從屬管理伺服器（包括虛擬伺服器）。

- 卡巴斯基安全中心現在支援使用 Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 作為受管理應用程式。

卡巴斯基安全管理中心 13.2

卡巴斯基安全管理中心 13.2 有幾項新功能和改善事項：

- 您現在可以在以下新作業系統上安裝管理伺服器、管理主控台、卡巴斯基安全管理中心 13.2 網頁主控台和網路代理（請參閱軟體要求瞭解詳細資訊）：

  - Microsoft Windows 11
  - Microsoft Windows 10 21H2（2021 年 10 月更新）
  - Windows Server 2022

- 您可以使用 MySQL 8.0 作為資料庫。

- 您可以在卡巴斯基安全管理中心容錯移轉叢集上部署卡巴斯基安全管理中心，使卡巴斯基安全管理中心具備高可用性。

- 卡巴斯基安全管理中心現在可以使用 IPv6 位址和 IPv4 位址。管理伺服器可以輪詢具有 IPv6 位址的裝置的網路。

卡巴斯基安全管理中心 13.2 網頁主控台有幾項新功能和改善事項：

- 現在，您可以透過卡巴斯基安全管理中心 13.2 網頁主控台管理執行 Android 的行動裝置。
- Kaspersky 市場作為新功能表部分提供：您可以透過卡巴斯基安全管理中心 13.2 網頁主控台搜尋 Kaspersky 應用程式。
- 卡巴斯基安全管理中心現在支援以下 Kaspersky 應用程式：
  - Kaspersky Endpoint Detection and Response Optimum 2.0
  - Kaspersky Sandbox 2.0
  - Kaspersky Industrial CyberSecurity for Networks 3.1

卡巴斯基安全管理中心 13.1

卡巴斯基安全管理中心 13.1 有幾項新功能和改善事項：

- 與 SIEM 系統的整合已獲得改進。您現在可以透過加密通道 (TLS) 將事件匯出到 SIEM 系統。該功能可用於卡巴斯基安全管理中心網頁主控台和基於 MMC 的管理主控台。
- 您現在可以將管理伺服器的修補程式作為分發套件接收，您可以將其用於未來更新到更高版本。
- 新的區段**警示**，已針對 Kaspersky Endpoint Detection and Response Optimum 新增到卡巴斯基安全管理中心 13.1 網頁主控台。還新增了幾個新小工具，用於處理 Kaspersky Endpoint Detection and Response Optimum 偵測到的威脅。
- 在卡巴斯基安全管理中心 13.1 網頁主控台，您現在可以收到關於 Kaspersky 應用程式授權到期的通知。
- 卡巴斯基安全管理中心 13.1 網頁主控台的響應時間已縮短。

卡巴斯基安全管理中心 13

下列功能已新增至卡巴斯基安全管理中心 13 網頁主控台：

- 實作了兩步驟驗證。您可以啟用兩步驟驗證，以減少未授權存取卡巴斯基安全管理中心 13 網頁主控台的風險。
- 透過使用 NTLM 和 Kerberos 通訊協定（單點登入）實作網域身分驗證。單一登入功能允許 Windows 使用者在卡巴斯基安全管理中心 13 網頁主控台中啟用安全身分驗證，而無需在公司網路上重新輸入密碼。
- 現在，您可以設定外掛程式以與 Kaspersky Managed Detection and Response 一起使用。您可以使用此整合來查看事件並管理工作站。
- 現在，您可以在管理伺服器的安裝精靈中為卡巴斯基安全管理中心 13 網頁主控台指定設定。
- 顯示有關更新和修補程式的新版本通知。您可以立即安裝更新，也可以稍後安裝。現在，您可以透過卡巴斯基安全管理中心 13 網頁主控台為管理伺服器安裝修補程式。
- 使用資料表時，現在可以指定資料欄的順序和寬度，對資料進行排序並指定頁面大小。
- 現在，您可以透過按一下其名稱來開啟任何報告。

- 卡巴斯基安全管理中心 13 網頁主控台現已提供韓語版本。

- 卡巴斯基公告中有新的區段，可在**監控和報告**功能表取得。此區段會提供您卡巴斯基安全管理中心版本和受管理裝置上安裝的受管理應用程式相關資訊，讓您隨時了解最新資訊。卡巴斯基安全管理中心會透過刪除過時的公告並新增資訊來定期更新此區段中的資訊。但是，您可以根據需要停用 Kaspersky 公告。

- 更改使用者帳戶的設定後，實作了其他身分驗證。您可以啟用以防護使用者帳戶免遭未授權的修改。如果啟用此選項，則修改使用者帳戶設定需要具有修改權限的使用者授權。

卡巴斯基安全管理中心 13 新增了以下功能：

- 實作了兩步驟驗證。您可以啟用兩步驟驗證，以減少未授權存取管理主控台的風險。如果啟用此選項，則修改使用者帳戶設定需要具有修改權限的使用者授權。您現在可以為 KES 裝置啟用或停用兩步驟驗證。

- 您可以透過 HTTP 將訊息傳送到管理伺服器。管理伺服器 OpenAPI 的參考手冊 和 Python 資料庫現已推出。

- 您可以簽發備用憑證以在 iOS MDM 設定檔中使用，藉此確保在 iOS MDM 伺服器憑證到期後無縫切換受管理的 iOS 裝置。

- 多租戶應用程式資料夾不再顯示在管理主控台中。

卡巴斯基安全管理中心 14.2

該部分提供了卡巴斯基安全管理中心 14.2 資訊。

Online Help 中提供的資訊可能會與應用程式中隨附的文件資訊不同，在此情況下，Online Help 中的資訊為最新資訊。您可點選應用程式介面的連結，或文件中 Online Help 連結以繼續前往 Online Help。Online Help 可能會在沒有事先通知的情況下更新。如有必要，您可以在線上說明和離線說明間切換。

基本概念

本章節解釋關於卡巴斯基安全管理中心的基本概念。

管理伺服器

使用卡巴斯基安全管理中心元件可遠端管理用戶端裝置上安裝的 Kaspersky 應用程式。

安裝了管理伺服器元件的裝置將被稱作*管理伺服器*（也稱作*伺服器*）。管理伺服器必須被防護，包括實體防護，以防範非授權的存取。

管理伺服器在安裝的裝置上為系統服務，且擁有以下內容：

- 名稱為"卡巴斯基安全管理中心管理伺服器"
- 設定隨作業系統啟動而自動啟動
- 具有**LocalSystem**帳戶或在安裝管理伺服器過程中所選取的使用者帳戶

管理伺服器會執行下列功能：

- 儲存管理群組結構
- 儲存關於用戶端裝置設定的資訊
- 應用程式分發套件的儲存結構
- 將應用程式遠端安裝至用戶端裝置和遠端移除應用程式
- 更新 Kaspersky 應用程式的程式資料庫和軟體模組
- 管理用戶端裝置上的政策和工作
- 儲存有關用戶端裝置上已發生事件的資訊
- 產生有關 Kaspersky 應用程式操作的報告

- 向用戶端裝置佈署授權金鑰並儲存授權金鑰資訊
- 有關工作處理程序的通知轉發（例如在用戶端裝置上偵測到病毒）

在應用程式介面命名管理伺服器

在基於 MMC 的管理主控台和卡巴斯基安全管理中心 網頁主控台介面中，管理伺服器可以擁有以下名稱：

- 管理伺服器的裝置名稱，例如："*裝置名稱*"或"管理伺服器：*裝置名稱*"。
- 管理伺服器裝置的 IP 位址，例如："*IP 位址*"或"管理伺服器：*IP 位址*"。
- 從屬管理伺服器和虛擬管理伺服器具有在將虛擬或從屬管理伺服器連線到主管理伺服器時指定的自訂名稱。
- 如果您使用安裝在 Linux 裝置上的卡巴斯基安全管理中心 網頁主控台，則該應用程式將顯示您在回應檔案中指定為受信任的管理伺服器名稱。

使用管理主控台或卡巴斯基安全管理中心 網頁主控台連線到管理伺服器。

管理伺服器階層

您可以按照階層架構排列管理伺服器。在該層次結構的不同階層等級上，每個管理伺服器都可以擁有多個次要管理伺服器（稱為*次要伺服器*）。次要伺服器的階層等級不受限制。主要管理伺服器的管理群組將會包括所有次要管理伺服器的用戶端裝置。因而，實體隔離的區域網路或不同網段，可使用不同台的管理伺服器進行管理，最後再由一台主要伺服器去管理其他管理伺服器。

*虛擬管理伺服器*是次要管理伺服器的一個特例。

要做到管理伺服器的樹狀結構，請做到以下幾點：

- 降低管理伺服器的負載（與為整個網路安裝單一的管理伺服器比較）。
- 安裝多台的好處還可以減少內網的流量以及簡化遠端辦公室的工作流量。您不必在主要管理伺服器和所有網路裝置（例如，它們可能位於不同地區）之間建立連線。只需在每個地區或網段中安裝次要管理伺服器，由次要伺服器管理各自的裝置，再由次要伺服器和主要伺服器之間建立專屬連線來同步資訊。
- 可由各地區或網段的管理員管理各自的從屬伺服器以分擔工作量。用於集中管理和監控用戶端防護安全狀態的所有功能仍然可正常使用。
- 由服務提供商使用卡巴斯基安全管理中心。服務提供商只需安裝卡巴斯基安全管理中心和卡巴斯基安全管理中心 網頁主控台。為了管理各種組織的大量用戶端裝置，服務提供商向管理伺服器階級新增從屬管理伺服器（包括虛擬伺服器）。

管理群組階層架構中所包括的用戶端裝置都只能連線到一個管理伺服器。您必須獨立監控裝置到管理伺服器的連線。使用這些功能可以在不同伺服器的管理群組中搜尋裝置。

虛擬管理伺服器

虛擬管理伺服器（以下也稱作*虛擬伺服器*）是卡巴斯基安全管理中心的一個元件，用於管理用戶端封鎖網路的病毒防護系統。

虛擬管理伺服器是特殊的從屬管理伺服器，與實體的管理伺服器相比，它具有以下限制：

- 只能在主管理伺服器上建立虛擬管理伺服器。
- 虛擬管理伺服器在其操作中使用主管理伺服器資料庫。虛擬管理伺服器不支援資料備份和還原工作，以及更新掃描和下載工作。
- 虛擬伺服器無法建立從屬管理伺服器（包括虛擬伺服器）。

另外虛擬管理伺服器具有以下限制：

- 在虛擬管理伺服器內容視窗中，能調整的區域是有限的。
- 若要在虛擬管理伺服器管理的用戶端裝置上遠端安裝 Kaspersky 應用程式，您必須確保已在其中一台用戶端裝置上安裝網路代理，以確保與虛擬管理伺服器的通訊。在第一次連線到虛擬管理伺服器時，該裝置會被自動分配為發佈點，並充當用戶端裝置與虛擬管理伺服器的連線閘道。
- 虛擬伺服器只能透過發佈點進行網路輪詢。
- 若要重新啟動有問題的虛擬伺服器，卡巴斯基安全管理中心需要重新啟動主管理伺服器及所有虛擬管理伺服器。
- 在虛擬伺服器上建立的使用者在管理伺服器上無法被分配到角色。

虛擬伺服器的管理員應擁有自己所管理的虛擬伺服器全部權限。

行動裝置伺服器

*行動裝置伺服器*是卡巴斯基安全管理中心的一個元件，它可以提供對行動裝置的存取，並且允許透過管理主控台來管理它們。行動裝置伺服器接收行動裝置的相關資訊並且儲存其設定檔。

我們提供了兩種行動裝置伺服器：

- Exchange 行動裝置伺服器。安裝至已安裝 Microsoft Exchange 伺服器的裝置，並且允許從 Microsoft Exchange 伺服器擷取資料並將其傳送給管理伺服器。行動裝置伺服器是用來管理支援 Exchange ActiveSync 協定的行動裝置。
- iOS MDM 伺服器。此行動裝置伺服器用於管理支援 Apple® Push Notifications 服務 (APNs) 的行動裝置。

卡巴斯基安全管理中心的行動裝置伺服器允許您管理以下物件：

- 單個行動裝置。
- 多個行動裝置。
- 多個行動裝置同時連結到叢集伺服器上。行動裝置連線到一個叢集伺服器時，在管理主控台中此叢集伺服器將顯示其為一個單一的行動裝置伺服器。

網頁伺服器

卡巴斯基安全管理中心*網頁伺服器*（以下簡稱"*網頁伺服器*"），是卡巴斯基安全管理中心的一個元件，與管理伺服器一同安裝。網頁伺服器用於透過網路傳輸獨立安裝套件、iOS MDM 設定檔、以及共用資料夾的檔案。

當您建立獨立安裝套件時，它會自動發佈在網頁伺服器上。已建立獨立安裝套件清單中將會顯示獨立安裝套件的下載連結。必要時，您可以取消發佈獨立安裝套件或在網頁伺服器上重新發佈。

當您為使用者的行動裝置建立 iOS MDM 設定檔時，它會自動發佈在網頁伺服器上。發佈的設定檔在成功安裝到使用者行動裝置後自動從網頁伺服器刪除。

共用資料夾專用於儲存透過管理伺服器所管理的所有裝置使用者的資訊。如果使用者無法直接存取共用資料夾，他/她可以透過網頁伺服器獲取共用資料夾的資訊。

要透過網頁伺服器為使用者提供共用資料夾的資訊，管理員需要在共用資料夾中建立一個名為 public 的子資料夾並將訊息複製至此。

資訊傳輸連結的語法請按以下格式：

`https://<網頁伺服器名稱>:<HTTPS 連接埠>/public/<物件>`

其中：

- `<Web Server name>`為卡巴斯基安全管理中心網頁伺服器的名稱。
- `<HTTPS port>`為由管理員定義的網頁伺服器 HTTPS 連接埠。HTTPS 連接埠可在管理伺服器內容視窗的**網頁伺服器**區域中設定。預設埠號為 8061。
- `<object>`是使用者可以存取的檔案或子資料夾。

管理員可以以任意方式例如電子郵件等方式將新連結傳送給使用者。

透過點擊連結，使用者可將所需資訊下載至本機裝置。

網路代理

管理伺服器和裝置之間的互動由卡巴斯基安全管理中心的*網路代理*元件執行。網路代理必須安裝在所有使用卡巴斯基安全管理中心來管理 Kaspersky 應用程式的裝置上。

網路代理作為系統服務安裝在裝置上，且具有以下內容：

- 名稱為"卡巴斯基安全管理中心網路代理"
- 設定隨作業系統啟動而自動啟動
- 使用 LocalSystem 帳戶

安裝了網路代理的裝置被稱為*受管理裝置*或*裝置*。

您可以在 Windows、Linux 或 Mac 裝置上安裝網路代理。您可以透過以下方式獲得元件：

- 管理伺服器儲存中的安裝套件（您必須安裝了管理伺服器）
- Kaspersky Web 伺服器上的安裝套件

您不必在安裝管理伺服器的裝置上安裝網路代理，因為網路代理的伺服器版本隨管理伺服器一同自動安裝。

網路代理啟動的處理程序名稱叫 *klnagent.exe*。

網路代理同步管理伺服器的受管理裝置。我們建議您設定同步間隔（也叫*心跳*）為每 10,000 台受管理裝置 15 分鐘。

管理群組

管理群組（以下簡稱*群組*）是受管理裝置的邏輯集合，根據某一特徵組合在一起以便作為卡巴斯基安全管理中心的一個單元來統一管理。

管理群組內的所有受管理裝置都被配置以做如下事情：

- 使用共同的應用程式設定（您可以在群組政策中指定）。
- 透過建立具有指定設定的群組工作，為所有應用程式使用共同的操作模式。群組工作的例子包括建立和安裝公用安裝套件、更新程式資料庫和模組、自訂掃描裝置和啟用即時防護。

受管理裝置只能屬於一個管理群組。

您可以建立管理伺服器和群組的層級。單個層次結構等級可以包括次要和虛擬管理伺服器、群組和受管理裝置。您可以從一個群組移動裝置到其他群組，而不做實體移動。例如，如果企業員工的職位從會計變更為開發者，您可以將該員工的裝置從會計管理群組移動到開發者管理群組。然後，該裝置將自動接收開發者所需的應用程式設定。

受管理裝置

*受管理裝置*是已安裝網路代理且執行 Windows、Linux 或 macOS 的裝置，或是已安裝卡巴斯基安全應用程式的行動裝置。您可以透過裝置上安裝的應用程式的工作和政策來管理此類裝置。您也可以從受管理裝置接收報告。

您可以讓非行動管理的裝置作為發佈點和連線閘道執行。

裝置僅可以被一個管理伺服器管理。一個管理伺服器可以管理最多 100,000 部裝置，包含行動裝置。

未配置的裝置

*未配置的裝置*是網路中未被包含在任何管理群組中的裝置。您可以在未配置裝置上執行一些操作，例如，移動它們到管理群組或在其上安裝應用程式。

當在您的網路中發現新裝置時，該裝置轉到"**未配置的裝置**"管理群組。您可以設定規則以便裝置在被發現後被自動移動到其他管理群組。

管理員工作站

*管理員工作站*是安裝管理主控台或用於開啟卡巴斯基安全管理中心 網頁主控台的裝置。管理員可以使用這些裝置來遠端集中管理用戶端裝置上安裝的 Kaspersky 應用程式。

在裝置上安裝管理主控台後，系統會顯示其圖示，允許您啟動管理主控台。您可在**開始 → 程式 → 卡巴斯基安全管理中心**功能表中找到。

管理主控台的數量不受限制。在任何管理員的工作站電腦上，都可以同時管理網路中多台管理伺服器。您可以使用管理主控台連線至網路中任何層級（實體或虛擬）的管理伺服器。

您可以將管理員的工作站移動至管理群組節點中的用戶端裝置。

在任何管理伺服器的管理群組中，單一裝置可以當做用戶端裝置、管理伺服器或管理主控台。

管理外掛程式

Kaspersky 應用程式會使用名為*管理外掛程式*的專屬元件透過管理主控台管理。可透過卡巴斯基安全管理中心管理的每個 Kaspersky 應用程式都會包含管理外掛程式。

使用應用程式管理外掛程式，可以在管理主控台中執行以下操作：

- 建立和編輯應用程式政策和工作以及應用程式工作的設定。
- 取得關於應用程式工作和應用程式事件的資訊，以及從用戶端裝置接收的應用程式操作統計資訊。

您可以從卡巴斯基技術支援網頁下載管理外掛程式。

管理 Web 外掛程式

一個特殊元件—*管理 Web 外掛程式*—用於使用卡巴斯基安全管理中心網頁主控台對 Kaspersky 軟體進行遠端管理。在下方，管理 Web 外掛程式又稱為*管理外掛程式*。管理外掛程式是卡巴斯基安全管理中心網頁主控台與特定 Kaspersky 應用程式間的介面。使用管理外掛程式，您可以配置應用程式工作和政策。

您可以從卡巴斯基技術支援網頁下載管理 Web 外掛程式。

管理外掛程式提供以下：

- 建立並編輯應用程式工作和設定的介面
- 建立和編輯政策和政策設定檔以便遠端和集中配置 Kaspersky 應用程式和裝置的介面
- 應用程式事件傳輸
- 卡巴斯基安全管理中心網頁主控台顯示應用程式的操作資料和事件，以及從用戶端裝置轉發的統計資訊

政策

*政策*是一組套用於管理群組及其子群組的卡巴斯基應用程式設定。您可以在管理群組的裝置上安裝多個 Kaspersky 應用程式。卡巴斯基安全管理中心為管理群組中的每個卡巴斯基應用程式提供單一政策。政策會有下列其中一種狀態（請見下表）：

政策狀態

狀態	敘述
活動	套用至裝置的目前政策。每個管理群組中的 Kaspersky 應用程式只能啟用一個政策。裝置將為卡巴斯基應用程式套用活動政策的設定值。
不啟用	目前未將政策套用至裝置。
漫遊	如果選取該選項，政策將在裝置離開企業網路時變為啟用狀態。

政策會根據以下規則執行：

- 您可以為單個應用程式配置擁有不同值的多個政策。
- 對於目前應用程式只有一個政策可以處於啟用狀態。
- 您可在特定事件發生時啟動非作用中的政策。例如，這代表您可以在病毒爆發時定義更加嚴謹的病毒防護設定。
- 政策可以有子政策。

通常，您可以將政策作為緊急情況 (例如病毒攻擊) 的準備。例如，如果有透過快閃記憶體磁碟機的攻擊，則可以啟動阻止存取快閃記憶體磁碟機的政策。在這種情況下，目前的啟用政策將自動變為非啟用狀態。

為了防止維護多個政策，例如，當不同場合僅假設變更多個設定時，您可以使用政策設定檔。

*政策設定檔*是政策設定值的已命名子集，用於替換政策的設定值。政策設定檔會影響受管理裝置上有效的設定形式。*有效設定*是目前應用於裝置的一組政策設定，政策設定檔設定和本機應用程式設定。

政策設定檔會根據以下規則執行：

- 當特定的啟動條件發生時，政策設定檔會生效。
- 政策設定檔包含與政策設定不同的設定值。
- 政策設定檔的啟動會變更受管理裝置的有效設定。
- 政策可以包含最多 100 個設定檔。

政策設定檔

有時候有必要為不同的管理群組建立單一政策的若干實例；您也可能想要集中修改這些政策的設定。這些實例實例可能僅有一兩處設定不同。例如，企業中所有的會計工作在相同政策下 — 但是進階會計被允許使用快閃記憶體磁碟機，而初級會計不被允許。此種情況下，僅透過管理群組層級套用政策到裝置可能不方便。

要說明您避免建立單一政策的不同實例，卡巴斯基安全管理中心可讓您建立*政策設定檔*。政策設定檔用於在單一管理群組中的裝置在不同政策設定下執行時。

政策設定檔是政策設定的命名子集。子集會連同政策一起分發至目標裝置，並根據名為*設定檔啟動條件*的特別條件來作為輔助政策。設定檔僅包含與「基本」政策不同的設定，並在受管理裝置上活動。設定檔的啟動將修改在裝置上最初活動的"基本"政策的設定。修改的設定將使用已在設定檔中指定的值。

工作

卡巴斯基安全管理中心透過建立和執行*工作*來管理裝置上安裝的 Kaspersky 應用程式。安裝、啟用和停用應用程式、掃描檔案、更新病毒資料庫和軟體模組以及應用程式的其他行為均需要使用工作來完成。

特定應用程式的工作僅在安裝了該應用程式的管理外掛程式時可以被建立。

工作可以在管理伺服器和裝置上執行。

以下工作管理伺服器上執行：

- 自動發佈報告
- 將更新下載至管理伺服器儲存區
- 備份管理伺服器資料
- 資料庫維護
- Windows Update 同步
- 建立以一個作業系統 (OS) 映像為參照裝置的安裝套件

以下類型的工作在裝置上執行：

- *本機工作* — 在特定裝置上執行的工作。

  本機工作可以被管理員透過管理主控台工具修改，或者被遠端裝置使用者修改（例如，透過安全應用程式介面）。如果本機工作同時被管理員和受管理裝置使用者修改，管理員的修改將生效，因為其具有更高優先順序。

- *群組工作* — 在特定裝置上執行的工作。

  除非在工作內容中指定了其他項目，群組工作也影響所選群組的所有子群組。群組工作也影響（可選）佈署在其群組或子群組的連線到從屬和虛擬管理伺服器的裝置。

- *全域工作* — 選取指定裝置來執行的工作，與裝置屬於哪個管理群組無關。

您可以為每個應用程式建立任意數量群組工作、全域工作或本機工作。

您可以修改工作設定、檢視工作進度、複製、匯出、匯入和刪除工作。

只有當裝置上應用程式被執行，建立之工作才會執行。

工作結果會儲存在 Microsoft Windows 事件記錄和卡巴斯基安全管理中心的事件記錄中，這兩個記錄會集中儲存在管理伺服器上，以及本機儲存在每個裝置上。

請勿在工作設定中包含私密資料。例如，避免指定網域管理員密碼。

工作範圍

*工作範圍*是執行工作的裝置集合。範圍的類型包括以下：

- 對於*本機工作*，範圍是裝置本身。
- 對於*管理伺服器工作*，範圍是管理伺服器。
- 對於*群組工作*，範圍是包含在群組中的裝置清單。

當建立*全域工作*時，您可以使用以下方法指定範圍：

- 手動指定特定裝置。

  您可以使用 IP 位址（或 IP 範圍）、NetBIOS 名稱或 DNS 名稱作為該裝置的位址。

- 從包含有要新增的裝置位址的 TXT 檔案來匯入裝置清單（每一個電腦位址必須單獨一行）。

  如果透過檔案匯入裝置清單或手動建立裝置清單，且如果裝置是以名稱定義，則清單可以只包含其資訊已被輸入到管理伺服器資料庫中的裝置。而且，資訊必須在裝置被連線或裝置發現中輸入。

- 指定裝置分類。

  後續，工作範圍隨著包含在分類中的裝置集的變更而變更。裝置分類可以基於裝置內容（包含安裝在裝置上的軟體）建立，也可以基於分配到裝置的標籤來建立。裝置分類是指定工作範圍的最靈活的方法。

  裝置分類的工作總是按管理伺服器排程執行。這些工作無法執行在缺少管理伺服器連線的裝置上。使用其他方法指定範圍的工作直接執行在裝置上，且因此不取決於到管理伺服器的裝置連線。

  裝置分類的工作不會按裝置本機時間執行；相反，它們將按照管理伺服器本機時間執行。使用其他方法指定範圍的工作以裝置本機時間執行。

本機應用程式設定與政策的關係

您可以使用政策為群組中的所有裝置設定完全相同的應用程式設定值。

政策指定的設定值可針對群組中的個別裝置使用本機應用程式設定重新定義。但本機只能調整政策中允許修改的設定項目，即為解鎖的項目。

應用程式在用戶端裝置上使用的設定的值由政策設定的鎖定（🔒）位置確定：

- 如果政策內容項目被鎖定，則所有用戶端裝置的設定值與政策中定義設定相同。
- 如果政策內容項目被「解鎖」，則應用程式將使用用戶端裝置的本機設定值，而不是政策中指定的值。您可以在本機應用程式設定中自行調整設定值。

用戶端裝置上執行工作時，應用程式以兩種不同的方式決定使用的設定：

- 如果沒有將設定項目鎖定以避免政策變更，則使用本機應用程式設定。
- 如果鎖定設定項目以避免修改，則使用群組政策設定。

需統一本機應用程式設定但又需要"解鎖"，需先"鎖定"並確定用戶端接收後再"解鎖"。

發佈點

發佈點（先前為更新代理）是安裝了網路代理的裝置，用於更新發佈、應用程式遠端安裝和網路裝置資訊檢索。發佈點加速更新發佈並釋放管理伺服器資源。

安裝在作為發佈點的裝置上的網路代理的功能和用例因作業系統而異。

發佈點可執行以下功能：

- 將從管理伺服器接收到的檔案發佈到群組中的用戶端裝置（包括透過 UDP 進行多點傳送進行發佈）。

  可被發佈點傳輸的檔案清單包括：

  - Kaspersky 資料庫和軟體模組更新
  - 協力廠商軟體更新
  - 安裝套件
  - 將管理伺服器作為 WSUS 伺服器使用時的 Windows 更新

  更新可以從管理伺服器接收，或者從 Kaspersky 更新伺服器獲取。如果後者，必須為發佈點建立更新工作。執行 macOS 的發佈點裝置無法從 Kaspersky 更新伺服器下載更新。

  若一或多個執行 macOS 的裝置位於 *下載更新至發佈點儲存區* 工作範圍內，該工作會以 *失敗* 狀態完成，即使工作已在所有 Windows 裝置上成功完成。

- 使用 UDP 透過多點傳送發佈政策和群組工作。
- 用作管理群組中的裝置與管理伺服器的連線閘道。

  如果群組中的受管理裝置與管理伺服器之間的直接連線無法建立，則發佈點可用作此群組的管理伺服器連線閘道。在這種情況下，受管理裝置將連線到閘道，連線閘道又連線到管理伺服器。

  用作連線閘道的發佈點的可用性不會封鎖受管理裝置與管理伺服器之間的直接連線。如果連線閘道不可用，但在技術上可與管理伺服器進行直接連線，則受管理裝置將直接連線到管理伺服器。

- 輪詢網路以偵測新裝置並更新現有裝置的資訊。發佈點套用與管理伺服器相同的裝置發現方法。

- 使用發佈點作業系統的工具，執行協力廠商軟體和卡巴斯基應用程式的遠端安裝。請注意，發佈點可以在沒有網路代理的用戶端裝置上執行安裝。

  此功能允許將網路代理的安裝套件遠端傳輸到位於管理伺服器無直接存取權限的網路上的用戶端裝置。

- 作為代理伺服器參與卡巴斯基安全網路 (KSN)。

  您可以在發佈點端啟用 KSN 代理伺服器以使裝置作為 KSN 代理伺服器。此種情況下，KSN 代理服務 (ksnproxy) 會在裝置上執行。

檔案透過 HTTP（如果啟用了 SSL 連線，則透過 HTTPS）從管理伺服器傳輸到發佈點。使用 HTTP 或 HTTPS 促成更高效能，相比透過流量的 SOAP。

安裝有網路代理的裝置可以被手動（透過管理員）或自動（透過管理伺服器）分配發佈點。指定管理群組的發佈點完整清單顯示在發佈點清單的報告中。

發佈點的範圍是管理員將其分配到其中的管理群組，以及其所有階層等級的子群組。如果已在管理群組的階層中分配幾個發佈點，則受管理裝置的網路代理會連線在階層上最近的發佈點。

網路位置也可以是發佈點範圍。網路位置用於手動建立裝置集，發佈點可在其上發佈更新。網路位置可以被執行 Windows 作業系統的裝置決定。

如果發佈點被管理伺服器自動分配，它透過廣播網域分配，而不是透過管理群組。此情況發生在所有廣播網域已知時。網路代理在相同的子網路與其他網路代理交換資訊並傳送給管理伺服器它的其他網路代理的資訊。管理伺服器可以用此資訊透過廣播網域分組網路代理。在管理群組中超過 70% 的網路代理被輪詢後，廣播網域對管理伺服器已知。管理伺服器每兩小時輪詢一次廣播網域。發佈點透過廣播網域分配後，就無法透過管理群組重新分配。

若管理員會手動指派發佈點，則可將其指派至管理群組或網路位置。

帶有活動連線設定檔的網路代理不參與廣播網域偵測。

卡巴斯基安全管理中心為每個網路代理分配不同於其他位址的單獨的 IP 多點傳送位址。這允許您避免由於 IP 重疊引起的網路超載。

當兩個或更多發佈點分配在單獨的網路區域或單獨的管理群組，其中一個會變成活動發佈點，其餘的變成備用發佈點。活動發佈點直接從管理伺服器下載更新和安裝套件，備用發佈點只從活動發佈點接收更新。此種情況下，檔案從管理伺服器下載一次，然後在發佈點之間發佈。如果因為任何原因活動發佈點不可用，其中一個備用發佈點將變成活動的。管理伺服器自動分配發佈點作為備用。

發佈點狀態（*活動* / *備用*）會連帶核取方塊一起顯示在 klnagchk 報告中。

一個發佈點需要至少 4 GB 的可用磁碟空間。如果發佈點的磁碟剩餘空間少於 2 GB，卡巴斯基安全管理中心建立嚴重等級為*警告*的事件。事件將被發佈在裝置內容中，在**事件註記**區域。

在分配為發佈點的裝置上執行遠端安裝工作需要更多可用磁碟空間。剩餘磁碟空間磁區必須超過安裝套件的總大小。

在分配為發佈點的裝置上執行任何更新（修補）工作和修復弱點工作需要另外的可用磁碟空間。剩餘磁碟空間磁區必須是至少兩倍的要安裝修補程式的總大小。

作為發佈點的裝置必須被防護，包括實體防護，以防範非授權的存取。

連線閘道

*連線閘道*是一種以特殊模式執行的網路代理。連線閘道接受來自其他網路代理的連線，並透過其自身與伺服器的連線將它們透過通道傳送到管理伺服器。與普通的網路代理不同，連線閘道會等待來自管理伺服器的連線，而不是建立與管理伺服器的連線。

連線閘道最多可以接收來自 10,000 台裝置的連線。

您可以使用兩個選項來使用連線閘道：

- 我們建議您在非警戒區 (DMZ) 中安裝連線閘道。對於在辦公室外的裝置上安裝的其他網路代理，您需要透過連線閘道專門設定與管理伺服器的連線。

  連線閘道不以任何方式修改或處理從網路代理傳輸到管理伺服器的資料。此外，它不會將此資料寫入任何緩衝區，因此不能接受來自網路代理的資料，以後再將其轉發給管理伺服器。如果網路代理嘗試透過連線閘道連線到管理伺服器，但是連線閘道無法連線到管理伺服器，則網路代理會認為這是無法存取的管理伺服器。所有資料均保留在網路代理上（不在連線閘道上）。

  連線閘道無法透過另一個連線閘道連線到管理伺服器。這意味著網路代理不能同時作為連線閘道，且不能使用連線閘道連線到管理伺服器。

  所有連線閘道都包含在管理伺服器內容的發佈點清單中。

- 您也可以在網路內使用連線閘道。例如，自動分配的發佈點也將成為其自身範圍內的連線閘道。但是，在內部網路中，連線閘道無法提供可觀的效益。它們減少了管理伺服器接收到的網路連線數量，但是沒有減少傳入資料的數量。即使沒有連線閘道，所有裝置仍可以連線到管理伺服器。

關於卡巴斯基安全管理中心

本節說明卡巴斯基安全管理中心的用途、其主要功能特色和元件、以及購買卡巴斯基安全管理中心的方式。

Online Help 中提供的資訊可能會與應用程式中隨附的文件資訊不同，在此情況下，Online Help 中的資訊為最新資訊。您可點選應用程式介面的連結，或文件中 Online Help 連結以繼續前往 Online Help。Online Help 可能會在沒有事先通知的情況下更新。如有必要，您可以在線上說明和離線說明間切換。

卡巴斯基安全管理中心是設計用來在區域網路中集中執行基本的管理和維護工作。提供關於組織的網路安全等級的詳盡資訊予管理員存取；及准許設定使用 Kaspersky 應用程式建置的防護元件。

卡巴斯基安全管理中心是一款主要供公司網路管理員和廣泛組織中負責裝置防護員工使用的應用程式。

使用卡巴斯基安全管理中心您可以做到：

- 建立虛擬管理伺服器以確保遠端辦公室或用戶端組織架構網路的病毒防護。

  *用戶端群組架構*是指由服務提供者確保病毒防護的一種群組架構。

- 建立一個管理群組層級結構以整體的形式管理一組選定的用戶端裝置。

- 管理基於 Kaspersky 程式構建的病毒防護系統。

- 建立作業系統的映像，並透過網路佈署到用戶端裝置上，以及遠端安裝和移除 Kaspersky 程式與協力廠商程式。

- 遠端允許管理與安裝 Kaspersky 與協力廠商程式至用戶端。安裝更新，尋找和修復弱點。
- 將 Kaspersky 應用程式的產品授權金鑰集中分發給用戶端裝置、監控其使用情況，以及續約產品授權。
- 接收關於程式和裝置執行的統計資訊和報告。
- 接收有關 Kaspersky 程式操作中緊急事件的通知。
- 管理行動裝置。
- 管理儲存在裝置硬碟磁碟機和卸除式磁碟機上的資訊的加密處理，以及使用者對加密資料的存取。
- 執行連線至內部網路的硬體儲存區。
- 集中管理被安全應用程式移動到隔離區或備份區中的檔案，以及安全應用程式已經推遲處理的檔案。

您可以透過 Kaspersky （例如，https://www.kaspersky.com.tw ）或其合作夥伴公司購買卡巴斯基安全管理中心。

如果透過 Kaspersky 購買卡巴斯基安全管理中心，您可以從我們的網站複製應用程式。付款成功後，將會透過電子郵件傳送您產品所需要的應用程式啟動碼。

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

硬體和軟體需求

- 管理伺服器要求
- 網頁主控台要求
- 行動伺服器要求
- 管理主控台要求
- 網路代理要求

管理伺服器要求

最小硬體條件：

- CPU 的作業頻率為 1 GHz 或更高。64 位元作業系統，CPU 最低頻率 1.4 GHz。
- RAM：4 GB。
- 可用磁碟空間：10 GB。當使用弱點和修補程式管理時，至少需要 100 GB 可用磁碟空間。

對於在雲端環境中的佈署，對管理伺服器和資料庫伺服器的要求會與對物理管理伺服器的要求相同（視要管理的裝置數量而定）。

軟體需求：

- Microsoft® Data Access Components (MDAC) 2.8
- Microsoft Windows® DAC 6.0
- Microsoft Windows Installer 4.5

支援以下作業系統：

- Windows Server 2008 R2 Standard Service Pack 1 和更高版本 64 位元
- Windows Server 2012 Server Core 64 位元
- Windows Server 2012 Datacenter 64 位元
- Windows Server 2012 Essentials 64 位元
- Windows Server 2012 Foundation 64 位元
- Windows Server 2012 Standard 64 位元
- Windows Server 2012 R2 Server Core 64 位元
- Windows Server 2012 R2 Datacenter 64 位元
- Windows Server 2012 R2 Essentials 64 位元
- Windows Server 2012 R2 Foundation 64 位元
- Windows Server 2012 R2 Standard 64 位元
- Windows Server 2016 Datacenter (LTSB) 64 位元
- Windows Server 2016 Standard (LTSB) 64 位元
- Windows Server 2016 Server Core（安裝選項）(LTSB) 64 位元
- Windows Server 2019 Standard 64 位元
- Windows Server 2019 Datacenter 64 位元
- Windows Server 2019 Core 64 位元
- Windows Server 2022 Standard 64 位元
- Windows Server 2022 Datacenter 64 位元
- Windows Server 2022 Core 64 位元
- Windows Storage Server 2012 64 位元
- Windows Storage Server 2012 R2 64 位元

- Windows Storage Server 2016 64 位元
- Windows Storage Server 2019 64 位元

支援以下虛擬平台：

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware Workstation 16 Pro
- Microsoft Hyper-V Server 2012 64 位元
- Microsoft Hyper-V Server 2012 R2 64 位元
- Microsoft Hyper-V Server 2016 64 位元
- Microsoft Hyper-V Server 2019 64 位元
- Microsoft Hyper-V Server 2022 64 位元
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 17
- Oracle VM VirtualBox 6.x

支援以下資料庫伺服器（可以安裝在不同的裝置上）：

- Microsoft SQL Server 2012 Express 64 位元具有限制
- Microsoft SQL Server 2014 Express 64 位元具有限制
- Microsoft SQL Server 2016 Express 64 位元具有限制
- Microsoft SQL Server 2017 Express 64 位元具有限制
- Microsoft SQL Server 2019 Express 64 位元具有限制
- Microsoft SQL Server 2014（所有版本）64 位元
- Microsoft SQL Server 2016（所有版本）64 位元
- Microsoft SQL Server 2017（所有版本），Windows 64 位元
- Microsoft SQL Server 2017（所有版本），Linux 64 位元
- Microsoft SQL Server 2019（所有版本），Windows 64 位元（需要額外動作）
- Microsoft SQL Server 2019（所有版本），Linux 64 位元（需要額外動作）
- Microsoft Azure SQL 資料庫

- 所在 Amazon RDS 和 Microsoft Azure 雲端平台支援的 SQL Server 版本
- MySQL 5.7 社區 32 位元/64 位元
- MySQL 標準版 8.0（8.0.20 及更高版本）32 位元/64 位元
- MySQL 企業版 8.0（8.0.20 及更高版本）32 位元/64 位元
- MariaDB 10.1（組建編號 10.1.30 及以上）32 位元/64 位元
- MariaDB 10.3（組建編號 10.3.22 及以上）32 位元/64 位元
- MariaDB 10.4（組建編號 10.4.26 及以上）32 位元/64 位元
- MariaDB 10.5（組建編號 10.5.27 及以上）32 位元/64 位元
- MariaDB Galera Cluster 10.3 32 位元/64 位元，搭配 InnoDB 儲存引擎
- PostgreSQL 13.x 64 位元
- PostgreSQL 14.x 64 位元
- Postgres Pro 13.x（所有版本）
- Postgres Pro 14.x（所有版本）

有關詳細資訊和限制，請參閱以下主題：選擇 DBMS。

> 建議您使用 MariaDB 10.3.22；若您使用舊版，執行 Windows 更新工作可能需耗費超過一天的時間。

SIEM 和其他資訊管理系統：

- HP (Micro Focus) ArcSight ESM 7.0
- IBM QRadar 7.3
- Splunk 7.1

網頁主控台要求

卡巴斯基安全管理中心網頁主控台伺服器

最小硬體條件：

- CPU：4 核心，作業頻率 2.5 GHz
- RAM：8 GB
- 可用磁碟空間：40 GB

卡巴斯基安全管理中心網頁主控台伺服器支援的作業係統

作業系統。Microsoft Windows（僅 64 位元版本）：	Windows Server 2012 Server Core Windows Server 2012 Datacenter Windows Server 2012 Essentials Windows Server 2012 Foundation Windows Server 2012 Standard Windows Server 2012 R2 Server Core Windows Server 2012 R2 Datacenter Windows Server 2012 R2 Essentials Windows Server 2012 R2 Foundation Windows Server 2012 R2 Standard Windows Server 2016 Datacenter (LTSB) Windows Server 2016 Standard (LTSB) Windows Server 2016 Server Core（安裝選項）(LTSB) Windows Server 2019 Standard Windows Server 2019 Datacenter Windows Server 2019 Core Windows Server 2022 Standard Windows Server 2022 Datacenter Windows Server 2022 Core Windows Storage Server 2012 Windows Storage Server 2012 R2 Windows Storage Server 2016 Windows Storage Server 2019
作業系統。Linux（僅 64 位元版本）	Debian GNU/Linux 9.x (Stretch) Debian GNU/Linux 10.x (Buster) Debian GNU/Linux 11.x (Bullseye) Ubuntu Server 18.04 LTS (Bionic Beaver) Ubuntu Server 20.04 LTS (Focal Fossa) Ubuntu Server 22.04 LTS (Jammy Jellyfish) CentOS 7.x Red Hat Enterprise Linux Server 7.x Red Hat Enterprise Linux Server 8.x Red Hat Enterprise Linux Server 9.x SUSE Linux Enterprise Server 12（所有服務套件） SUSE Linux Enterprise Server 15（所有服務套件） Astra Linux 特別版 RUSB.10015-01（操作更新 1.6） Astra Linux 特別版 RUSB.10015-01（操作更新 1.7） Astra Linux 通用版 2.12

	ALT Server 9.2 ALT Server 10 ALT 8 SP Server (LKNV.11100-01) ALT 8 SP Server (LKNV.11100-02) ALT 8 SP Server (LKNV.11100-03) Oracle Linux 7 Oracle Linux 8 Oracle Linux 9 RED OS 7.3 Server RED OS 7.3 認證版 基於內核的虛擬機（卡巴斯基安全管理中心網頁主控台伺服器支援的所有 Linux 作業系統）

用戶端裝置

對於用戶端裝置，卡巴斯基安全管理中心網頁主控台的使用僅需要一個瀏覽器。

最小螢幕解析度為 1366x768 像素。

裝置的硬體和軟體需求和卡巴斯基安全管理中心網頁主控台所使用的瀏覽器的需求是相同的。

瀏覽器：

- Mozilla Firefox 延伸程式支援版本 91.8.0 或更高版本（91.8.0 於 2022 年 4 月 5 日發布）
- Google Chrome 100.0.4896.88 或更高版本（官方版本）
- Microsoft Edge 100 或更高版本
- macOS 的 Safari 15

行動伺服器要求

iOS 行動裝置管理 (iOS MDM) 伺服器

硬體需求：

- CPU 的作業頻率為 1 GHz 或更高。64 位元作業系統，CPU 最低頻率 1.4 GHz。
- RAM：2 GB。
- 可用磁碟空間：2 GB。

軟體需求：Microsoft Windows（支援的 Windows 版本視管理伺服器需求定義）。

Exchange 行動裝置伺服器

Exchange 行動裝置伺服器的所有軟體和硬體需求包含在 Microsoft Exchange Server 的系統需求中。

支援與 Microsoft Exchange Server 2007、Microsoft Exchange Server 2010 及 Microsoft Exchange Server 2013 的相容。

管理主控台要求

硬體需求：

- CPU 的作業頻率為 1 GHz 或更高。64 位元作業系統，CPU 最低頻率 1.4 GHz。
- RAM：512MB。
- 可用磁碟空間：1 GB。

軟體需求：

- Microsoft Windows 作業系統（支援的作業系統版本視管理伺服器的需求而定），以下作業系統除外：
  - Windows Server 2012 Server Core 64 位元
  - Windows Server 2012 R2 Server Core 64 位元
  - Windows Server 2016 Server Core（安裝選項）(LTSB) 64 位元
  - Windows Server 2019 Core 64 位元
  - Windows Server 2022 Core 64 位元
- Microsoft Management Console 2.0
- Microsoft Windows Installer 4.5
- 在以下系統執行的 Microsoft Internet Explorer 10.0：
  - Microsoft Windows Server 2008 R2 Service Pack 1
  - Microsoft Windows Server 2012
  - Microsoft Windows Server 2012 R2
  - Microsoft Windows 7 Service Pack 1
  - Microsoft Windows 8
  - Microsoft Windows 8.1
  - Microsoft Windows 10

- 在以下系統執行的 Microsoft Internet Explorer 11.0：
  - Microsoft Windows Server 2012 R2
  - Microsoft Windows Server 2012 R2（Service Pack 1）
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2019
  - Microsoft Windows 7 Service Pack 1
  - Microsoft Windows 8.1
  - Microsoft Windows 10
- 在 Microsoft Windows 10 上執行的 Microsoft Edge

網路代理要求

最小硬體條件：

- CPU 的作業頻率為 1 GHz 或更高。64 位元作業系統，CPU 最低頻率 1.4 GHz。
- RAM：512MB。
- 可用磁碟空間：1 GB。

弱點和修補程式管理的最低硬體需求：

- 執行頻率為 1.4 GHz 或更高的 CPU。需要 64 位元作業系統。
- RAM：8 GB。
- 可用磁碟空間：1 GB。

針對基於 Linux 的裝置的軟體要求：必須安裝 Perl 語言解譯器 5.10 或更高版本。

作業系統。Microsoft Windows	Microsoft Windows Embedded POSReady 2009 with latest Service Pack 32 位元 Microsoft Windows Embedded POSReady 7 32 位元/64 位元 Microsoft Windows Embedded 7 Standard (Service Pack 1) 32 位元/64 位元 Microsoft Windows Embedded 8 Standard 32 位元/64 位元 Microsoft Windows Embedded 8.1 Industry Pro 32 位元/64 位元 Microsoft Windows Embedded 8.1 Industry Enterprise 32 位元/64 位元 Microsoft Windows Embedded 8.1 Industry Update 32 位元/64 位元 Microsoft Windows 10 Enterprise 2015 LTSB 32 位元 /64 位元 Microsoft Windows 10 Enterprise 2016 LTSB 32 位元 /64 位元 Microsoft Windows 10 IoT Enterprise 2015 LTSB 32 位元 /64 位元 Microsoft Windows 10 IoT Enterprise 2016 LTSB 32 位元 /64 位元 Microsoft Windows 10 Enterprise 2019 LTSC 32 位元 /64 位元 Microsoft Windows 10 IoT 企業版 1703 32 位元 / 64 位元 Microsoft Windows 10 IoT 企業版 1709 32 位元/64 位元 Microsoft Windows 10 IoT 企業版 1803 32 位元 / 64 位元 Microsoft Windows 10 IoT 企業版 1809 32 位元 / 64 位元 Microsoft Windows 10 20H2 IoT 企業版 32 位元/64 位元 Microsoft Windows 10 21H2 IoT 企業版 32 位元 / 64 位元 Microsoft Windows 10 IoT 企業版 32 位元/64 位元 Microsoft Windows 10 IoT 企業版 1909 32 位元 / 64 位元 Microsoft Windows 10 IoT 企業版 LTSC 2021 32 位元/64 位元 Microsoft Windows 10 IoT 企業版 1607 32 位元 / 64 位元 Microsoft Windows 10 家用版 RS3（Fall Creators Update，v1709）32 位元/64 位元 Microsoft Windows 10 專業版 RS3（Fall Creators Update，v1709）32 位元/64 位元 Microsoft Windows 10 工作站專業版 RS3（Fall Creators Update，v1709）32 位元/64 位元 Microsoft Windows 10 企業版 RS3（Fall Creators Update，v1709）32 位元/64 位元 Microsoft Windows 10 教育版 RS3（Fall Creators Update，v1709）32 位元/64 位元 Microsoft Windows 10 家用版 RS4（2018 年 4 月更新，17134）32 位元/64 位元 Microsoft Windows 10 專業版 RS4（2018 年 4 月更新，17134）32 位元/64 位元 Microsoft Windows 10 工作站專業版 RS4（2018 年 4 月更新，17134）32 位元/64 位元 Microsoft Windows 10 企業版 RS4（2018 年 4 月更新，17134）32 位元/64 位元 Microsoft Windows 10 教育版 RS4（2018 年 4 月更新，17134）32 位元/64 位元 Microsoft Windows 10 家用版 RS5（2018 年 10 月）32 位元/64 位元 Microsoft Windows 10 專業版 RS5（2018 年 10 月）32 位元/64 位元 Microsoft Windows 10 工作站專業版 RS5（2018 年 10 月）32 位元/64 位元 Microsoft Windows 10 企業版 RS5（2018 年 10 月）32 位元/64 位元 Microsoft Windows 10 教育版 RS5（2018 年 10 月）32 位元/64 位元 Microsoft Windows 10 家庭版 19H1 32 位元 / 64 位元 Microsoft Windows 10 專業版 19H1 32 位元/64 位元 Microsoft Windows 10 工作站專業版 19H1 32 位元/64 位元 Microsoft Windows 10 企業版 19H1 32 位元/64 位元 Microsoft Windows 10 教育版 19H1 32 位元/64 位元 Microsoft Windows 10 教育版 19H2 32 位元 / 64 位元 Microsoft Windows 10 專業版 19H2 32 位元/64 位元 Microsoft Windows 10 Pro for Workstations 19H2 32 位元 / 64 位元 Microsoft Windows 10 Enterprise 19H2 32 位元 / 64 位元 Microsoft Windows 10 Education 19H2 32 位元 / 64 位元 Microsoft Windows 10 家用版 20H1（2020 年 5 月更新）32 位元/64 位元 Microsoft Windows 10 專業版 20H1（2020 年 5 月更新）32 位元/64 位元 Microsoft Windows 10 企業版 20H1（2020 年 5 月更新）32 位元/64 位元 Microsoft Windows 10 教育版 20H1（2020 年 5 月更新）32 位元/64 位元 Microsoft Windows 10 家用版 20H2（2020 年 10 月更新）32 位元/64 位元 Microsoft Windows 10 專業版 20H2（2020 年 10 月更新）32 位元/64 位元 Microsoft Windows 10 企業版 20H2（2020 年 10 月更新）32 位元/64 位元 Microsoft Windows 10 教育版 20H2（2020 年 10 月更新）32 位元/64 位元

Microsoft Windows 10 家用版 21H1（2021 年 5 月更新）32 位元/64 位元
Microsoft Windows 10 專業版 21H1（2021 年 5 月更新）32 位元/64 位元
Microsoft Windows 10 企業版 21H1（2021 年 5 月更新）32 位元/64 位元
Microsoft Windows 10 教育版 21H1（2021 年 5 月更新）32 位元/64 位元
Microsoft Windows 10 家用版 21H2（2021 年 10 月更新）32 位元/64 位元
Microsoft Windows 10 專業版 21H2（2021 年 10 月更新）32 位元/64 位元
Microsoft Windows 10 企業版 21H2（2021 年 10 月更新）32 位元/64 位元
Microsoft Windows 10 教育版 21H2（2021 年 10 月更新）32 位元/64 位元
Microsoft Windows 10 家用版 22H2（2023 年 10 月更新）32 位元/64 位元
Microsoft Windows 10 專業版 22H2（2023 年 10 月更新）32 位元/64 位元
Microsoft Windows 10 企業版 22H2（2023 年 10 月更新）32 位元/64 位元
Microsoft Windows 10 教育版 22H2（2023 年 10 月更新）32 位元/64 位元
Microsoft Windows 11 家用版 64 位元
Microsoft Windows 11 專業版 64 位元
Microsoft Windows 11 企業版 64 位元
Microsoft Windows 11 教育版 64 位元
Microsoft Windows 11 22H2
Microsoft Windows 8.1 專業版 32 位元/64 位元
Microsoft Windows 8.1 企業版 32 位元/64 位元
Microsoft Windows 8 專業版 32 位元/64 位元
Microsoft Windows 8 Enterprise 32 位元 / 64 位元
Microsoft Windows 7 專業版（Service Pack 1 和更高版本）32 位元/64 位元
Microsoft Windows 7 專業版/旗艦版（Service Pack 1 和更高版本）32 位元/64 位元
Microsoft Windows 7 家用基本版/進階版（Service Pack 1 和更高版本）32 位元/64 位元
Microsoft Windows XP Professional Service Pack 32 位元/64 位元（僅受網路代理版本 10.5.1781 支持，您可以透過技術支援請求該版本）
Microsoft Windows XP Professional Service Pack 3 及更高版本 32 位元（受網路代理版本 14.0.0.20023 支援）
適用於嵌入式系統的 Microsoft Windows XP Professional Service Pack 3 32 位元（受網路代理版本 14.0.0.20023 支援）
Windows Small Business Server 2011 Essentials 64 位元
Windows Small Business Server 2011 Premium Add-on 64 位元
Windows Small Business Server 2011 Standard 64 位元
Windows MultiPoint™ Server 2011 Standard/Premium 64 位元
Windows MultiPoint™ Server 2012 Standard/Premium 64 位元
Windows Server 2003 SP1 32 位元/64 位元（僅受網路代理版本 10.5.1781 支援）
Windows Server 2003 SP2 標準版/企業版 32 位元/64 位元（僅受網路代理版本 10.5.1781 支援）
Windows Server 2003 R2 標準版/企業版 SP2 32 位元/64 位元（僅受網路代理版本 10.5.1781 支援）
Windows Server 2008 Foundation (Service Pack 2) 32 位元/64 位元
Windows Server 2008 Service Pack 2（所有版本）32 位元/64 位元
Windows Server 2008 R2 Datacenter（Service Pack 1 和更高版本）64 位元
Windows Server 2008 R2 Enterprise（Service Pack 1 和更高版本）64 位元
Windows Server 2008 R2 Foundation（Service Pack 1 和更高版本）64 位元
Windows Server 2008 R2 內核模式（Service Pack 1 和更高版本）64 位元
Windows Server 2008 R2 Standard Service Pack 1 和更高版本 64 位元
Windows Server 2008 R2 Service Pack 1（所有版本）64 位元
Windows Server 2012 Server Core 64 位元
Windows Server 2012 Datacenter 64 位元
Windows Server 2012 Essentials 64 位元
Windows Server 2012 Foundation 64 位元
Windows Server 2012 Standard 64 位元
Windows Server 2012 R2 Server Core 64 位元
Windows Server 2012 R2 Datacenter 64 位元
Windows Server 2012 R2 Essentials 64 位元
Windows Server 2012 R2 Foundation 64 位元
Windows Server 2012 R2 Standard 64 位元
Windows Server 2016 Datacenter (LTSB) 64 位元

	Windows Server 2016 Standard (LTSB) 64 位元 Windows Server 2016 Server Core（安裝選項）(LTSB) 64 位元 Windows Server 2019 Standard 64 位元 Windows Server 2019 Datacenter 64 位元 Windows Server 2019 Core 64 位元 Windows Server 2022 Standard 64 位元 Windows Server 2022 Datacenter 64 位元 Windows Server 2022 Core 64 位元 Windows Storage Server 2012 64 位元 Windows Storage Server 2012 R2 64 位元 Windows Storage Server 2016 64 位元 Windows Storage Server 2019 64 位元
作業系統。Linux	Debian GNU / Linux 9.x (Stretch) 32 位元 / 64 位元 Debian GNU/Linux 10.x (Buster) 32 位元 / 64 位元 Debian GNU/Linux 11.x (Bullseye) 32 位元 / 64 位元 Ubuntu Server 18.04 LTS (Bionic Beaver) 32 位元 / 64 位元 Ubuntu Server 20.04 LTS (Focal Fossa) 32 位元/64 位元 Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64 位元 Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32 位元 / 64 位元 Ubuntu Desktop 20.04 LTS (Focal Fossa) 32 位元/64 位元 Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 位元 CentOS 7.x 64 位元 CentOS 7.x ARM 64 位元 Red Hat Enterprise Linux Server 6.x 32 位元/64 位元 Red Hat Enterprise Linux Server 7.x 64 位元 Red Hat Enterprise Linux Server 8.x 64 位元 Red Hat Enterprise Linux Server 9.x 64 位元 SUSE Linux Enterprise Server 12（所有服務套件）64 位元 SUSE Linux Enterprise Server 15（所有服務套件）64 位元 SUSE Linux Enterprise Desktop 15（所有服務套件）64 位元 SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM 64 位元 openSUSE 15 64 位元 EulerOS 2.0 SP8 ARM Pardus OS 19.1 64 位元 Astra Linux 通用版（操作更新 2.12）64 位元 Astra Linux 特別版 RUSB.10015-01（操作更新 1.6）64 位元 Astra Linux 特別版 RUSB.10015-01（操作更新 1.7）64 位元 Astra Linux 特別版 RUSB.10152-02（操作更新 4.7）ARM 64 位元 ALT Server 9.2 64 位元 ALT Server 10 64 位元 ALT Workstation 9.2 32 位元/64 位元 ALT Workstation 10 32 位元/64 位元 ALT 8 SP Server (LKNV.11100-01) 64 位元 ALT 8 SP Server (LKNV.11100-02) 64 位元 ALT 8 SP Server (LKNV.11100-03) 64 位元 ALT 8 SP Workstation (LKNV.11100-01) 32 位元/64 位元 ALT 8 SP Workstation (LKNV.11100-02) 32 位元/64 位元 ALT 8 SP Workstation (LKNV.11100-03) 32 位元/64 位元 Mageia 4 32 位元 Oracle Linux 7 64 位元 Oracle Linux 8 64 位元 Oracle Linux 9 64 位元 Linux Mint 19.x 32 位元 Linux Mint 20.x 64 位元 AlterOS 7.5 及更高版本 64 位元 GosLinux IC6 64 位元

	RED OS 7.3 Server 64 位元 RED OS 7.3 Certified Edition 64 位元 ROSA COBALT 7.9 64 位元 ROSA CHROME 12 64 位元 Lotos (Linux 核心版本 4.19.50, DE: MATE) 64 位元
作業系統。macOS	有關受支援的作業系統清單，請參閱Kaspersky Endpoint Security for Mac 說明。

對於網路代理，還支援 Apple Silicon (M1) 架構以及 Intel。

支援以下虛擬平台：

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware Workstation 16 Pro
- Microsoft Hyper-V Server 2012 64 位元
- Microsoft Hyper-V Server 2012 R2 64 位元
- Microsoft Hyper-V Server 2016 64 位元
- Microsoft Hyper-V Server 2019 64 位元
- Microsoft Hyper-V Server 2022 64 位元
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- 基於內核的虛擬機（網絡代理支援的所有 Linux 作業系統）

在執行 Windows 10 RS4 或 RS5 版本的裝置上，卡巴斯基安全管理中心可能無法在啟用了大小寫敏感的資料夾中偵測到一些弱點。

在執行 Windows 7、Windows Server 2008、Windows Server 2008 R2 或 Windows Small Business Server 2011 Premium Add-on 的裝置上安裝網路代理程式之前，請先確保已安裝適用於 Windows 作業系統的安全性更新 KB3063858（適用於 Windows 7 的安全更新 (KB3063858)，適用於基於 x64 的系統的 Windows 7 的安全更新 (KB3063858)，適用於 Windows Server 2008 的安全更新 (KB3063858)，適用於 Windows Server 2008 x64 版的安全更新 (KB3063858)，適用於 Windows Server 2008 R2 x64 版的安全更新 (KB3063858)。

在 Microsoft Windows XP，網路代理可能錯誤執行一些操作。

您只能在 Microsoft Windows XP 中安裝或更新適用於 Windows XP 的網路代理。支援的作業系統清單中列出了受支援的 Microsoft Windows XP 版本及其對應的網路代理版本。您可以從此頁面下載適用於 Microsoft Windows XP 的網頁代理所需版本。

我們建議您安裝與卡巴斯基安全管理中心相同或更新版本的 Linux 網路代理。

卡巴斯基安全管理中心完全支援相同或更新版本的網路代理。

適用於 macOS 的網路代理與適用於此作業系統的卡巴斯基安全應用程式一起提供。

相容的卡巴斯基應用程式和解決方案

卡巴斯基安全管理中心支援集中佈署和管理目前受支援的所有卡巴斯基應用程式和解決方案。下表顯示了基於 MMC 的管理主控台和卡巴斯基安全管理中心 網頁主控台支援的卡巴斯基應用程式和解決方案。要了解應用程式和解決方案的版本，請參閱產品支援生命週期網頁。

由卡巴斯基安全管理中心網頁主控台支援的卡巴斯基應用程式和解決方案清單

卡巴斯基應用程式或解決方案的名稱	受基於 MMC 的管理主控台支援	受卡巴斯基安全管理中心 網頁主控台支援
對於工作站		
Kaspersky Endpoint Security for Windows	✓	✓
Kaspersky Endpoint Security for Linux	✓	✓
Kaspersky Endpoint Security for Linux Elbrus Edition	✓	✓
Kaspersky Endpoint Security for Mac	✓	✓
Kaspersky Endpoint Agent	✓	✓
Kaspersky Embedded Systems Security for Windows	✓	✓
Kaspersky Embedded Systems Security for Linux	—	✓
對於工業解決方案		
Kaspersky Industrial CyberSecurity for Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Linux Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Networks（不支援集中佈署）	✓	✓
對於行動裝置		
Kaspersky Endpoint Security for Android	✓	✓
Kaspersky Security for iOS	—	✓
對於檔案伺服器		
Kaspersky Security for Windows Server	✓	✓
Kaspersky Endpoint Security for Windows	✓	✓
Kaspersky Endpoint Security for Linux	✓	✓
對於虛擬環境		
Kaspersky Security for Virtualization Light Agent	✓	✓
Kaspersky Security for Virtualization Agentless	✓	—
對於郵件和協作伺服器		
Kaspersky Security for Linux Mail Server	✓	—
Kaspersky Security for Microsoft Exchange Servers	✓	—

卡巴斯基應用程式或解決方案的名稱	受基於 MMC 的管理主控台支援	受卡巴斯基安全管理中心 網頁主控台支援
對於目的攻擊的偵測		
Kaspersky Sandbox Server	—	✓
Kaspersky Endpoint Detection and Response Optimum	—	✓
Kaspersky Managed Detection and Response	—	✓
對於 KasperskyOS 裝置		
Kaspersky IoT Secure Gateway	—	✓
Kaspersky Thin Client	—	✓

卡巴斯基安全管理中心 14.2 的產品授權與功能

卡巴斯基安全管理中心需要具有以下功能的產品授權。

下表顯示了卡巴斯基安全管理中心的功能涵蓋了哪些產品授權。

若要啟用卡巴斯基安全管理中心的功能，您必須透過新增管理伺服器產品授權金鑰來啟動管理伺服器。

> 您必須為每個管理伺服器手動新增產品授權金鑰。

產品授權與卡巴斯基安全管理中心產品授權

卡巴斯基安全管理中心的功能	Kaspersky 弱點和修補程式管理	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security for Business	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise	Kaspersky EDR Optimum
弱點評估	✓	✓	✓	✓	✓	✓	✓
修補程式管理	✓	—	✓	✓	—	✓	✓
角色型存取控制	✓	✓	✓	✓	✓	✓	✓
作業系統和應用程式的安裝	✓	—	✓	✓	—	✓	✓
行動裝置管理（即對使用者 iOS 和 Android 裝置的管理）	✓	✓	✓	✓	—	—	✓
適用於 AWS、Microsoft Azure 或 Google Cloud 等雲端環境工作的設定雲端環境	—	—	—	—	✓	✓	—
匯出事件到 SIEM 系統：Syslog	✓	✓	✓	✓	✓	✓	✓
將事件匯出到 SIEM 系統：IBM 的 QRadar 和 Micro Focus 的 ArcSight	✓	✓	✓	✓	✓	✓	✓

關於管理伺服器和卡巴斯基安全管理中心網頁主控台的相容性

我們建議您使用最新版本的卡巴斯基安全管理中心管理伺服器和卡巴斯基安全管理中心網頁主控台；否則，卡巴斯基安全管理中心的功能將受到限制。

您可以獨立安裝和升級卡巴斯基安全管理中心管理伺服器和卡巴斯基安全管理中心網頁主控台。在此情況下，您應該確保已安裝的卡巴斯基安全管理中心網頁主控台的版本與您要連線的管理伺服器版本相容：

- Kaspersky Security Center 14.2 Windows 中包含的網頁主控台支援以下版本的 Kaspersky Security Center 管理伺服器：14.2、14 和 13.2。
- Kaspersky Security Center 14.2 Windows 中包含的管理伺服器支援以下版本的 Kaspersky Security Center 網頁主控台：Windows 14.2、14 和 13.2，Linux 15。

卡巴斯基安全管理中心比較：基於 Windows 與基於 Linux

卡巴斯基為兩個平台（Windows 和 Linux）提供卡巴斯基安全管理中心作為內部部署解決方案。在基於 Windows 的解決方案中，您將管理伺服器安裝在 Windows 裝置上，而基於 Linux 的解決方案具有旨在安裝在 Linux 裝置上的管理伺服器版本。此線上說明包含有關卡巴斯基安全管理中心 Windows 的資訊。有關基於 Linux 的解決方案的詳細資訊，請參閱卡巴斯基安全管理中心 Linux 線上說明。

下表可讓您比較卡巴斯基安全管理中心作為基於 Windows 的解決方案和基於 Linux 的解決方案的主要功能。

卡巴斯基安全管理中心作為基於 Windows 的解決方案和基於 Linux 的解決方案的功能比較

功能或內容	卡巴斯基安全管理中心 14.2	
	基於 Windows 的解決方案	基於 Linux 的解決方案
管理伺服器地點	內部部署	內部部署
資料庫管理系統 (DBMS) 地點	內部部署	內部部署
在其上安裝管理伺服器的作業系統	Windows	Linux
管理主控台類型	內部部署和基於 Web	基於 Web
在其上安裝基於 Web 的管理主控台的作業系統	Windows 或 Linux	Linux
管理伺服器階層	✓	✓
管理群組階層	✓	✓
網路輪詢	✓	✓ （僅按 IP 範圍）
受管理裝置的最大數量	100,000	20,000
對受 Windows、macOS 和 Linux 管理的裝置的防護	✓	✓ （僅保護 Linux 和 Windows 裝置）
對行動裝置的防護	✓	–
對虛擬機的防護	✓	–
對公有雲端基礎結構的防護	✓	–
以裝置為中心的安全管理	✓	✓
以使用者為中心的安全管理	✓	✓
應用程式政策	✓	✓

功能或內容	卡巴斯基安全管理中心 14.2	
	基於 Windows 的解決方案	基於 Linux 的解決方案
卡巴斯基應用程式的工作	✓	✓
卡巴斯基安全網路	✓	✓
KSN 代理	✓	✓
卡巴斯基私有安全網路	✓	✓
卡巴斯基應用程式產品授權金鑰的集中部署	✓	✓
自動更新病毒資料庫	✓	✓
支援虛擬管理伺服器	✓	✓
安裝協力廠商軟體更新和修復協力廠商軟體弱點	✓	– （僅透過使用遠端安裝工作）
有關發生在受管理裝置上的事件的通知	✓	✓
建立和管理使用者帳戶	✓	✓
使用網域身分驗證登入主控台	✓	–
與 SIEM 系統整合	✓	✓ （僅通過使用 syslog）
監控政策和工作狀態	✓	✓
部署卡巴斯基安全管理中心容錯移轉叢集	✓	✓
在 Windows 伺服器容錯移轉叢集上安裝管理伺服器	✓	–
使用 SNMP 將管理伺服器統計資訊傳送到協力廠商應用程式	✓	–
用戶端裝置的遠端診斷	✓	–
用戶端裝置的桌面遠端連線	✓	–
管理物件修訂	✓	–
自動更新卡巴斯基應用程式	✓	–
佈署作業系統至用戶端裝置	✓	–
用於發布安裝套件和其他檔案的網頁伺服器	✓	–
檢視和使用 Kaspersky Endpoint Detection and Response Optimum 偵測到的警報	✓	–
將管理伺服器用作 WSUS 伺服器	✓	–
與 Kaspersky Managed Detection and Response 整合	✓	–
自適應異常控制支援	✓	–
支援管理群組中的叢集和伺服器陣列	✓ （僅限基於 MMC 的管理主控台）	–
管理協力廠商產品授權	✓	–

關於 卡巴斯基安全管理中心雲端主控台

使用卡巴斯基安全管理中心為本機應用程式意味著，您需在本機裝置上安裝卡巴斯基安全管理中心（包括管理伺服器），並透過以 Microsoft Management Console 為基礎的管理主控台（僅在卡巴斯基安全管理中心 Windows 中可用）或卡巴斯基安全管理中心網頁主控台來管理網路安全系統。

不過，您可以將卡巴斯基安全管理中心作為雲端服務使用。在此情況下，卡巴斯基安全管理中心將由卡巴斯基專家為您在雲端環境中安裝並維護，卡巴斯基可以讓您以服務的方式存取管理伺服器。您可以透過以雲端為基礎名為 卡巴斯基安全管理中心雲端主控台 的管理主控台來管理網路安全系統。此主控台的介面與卡巴斯基安全管理中心網頁主控台類似。

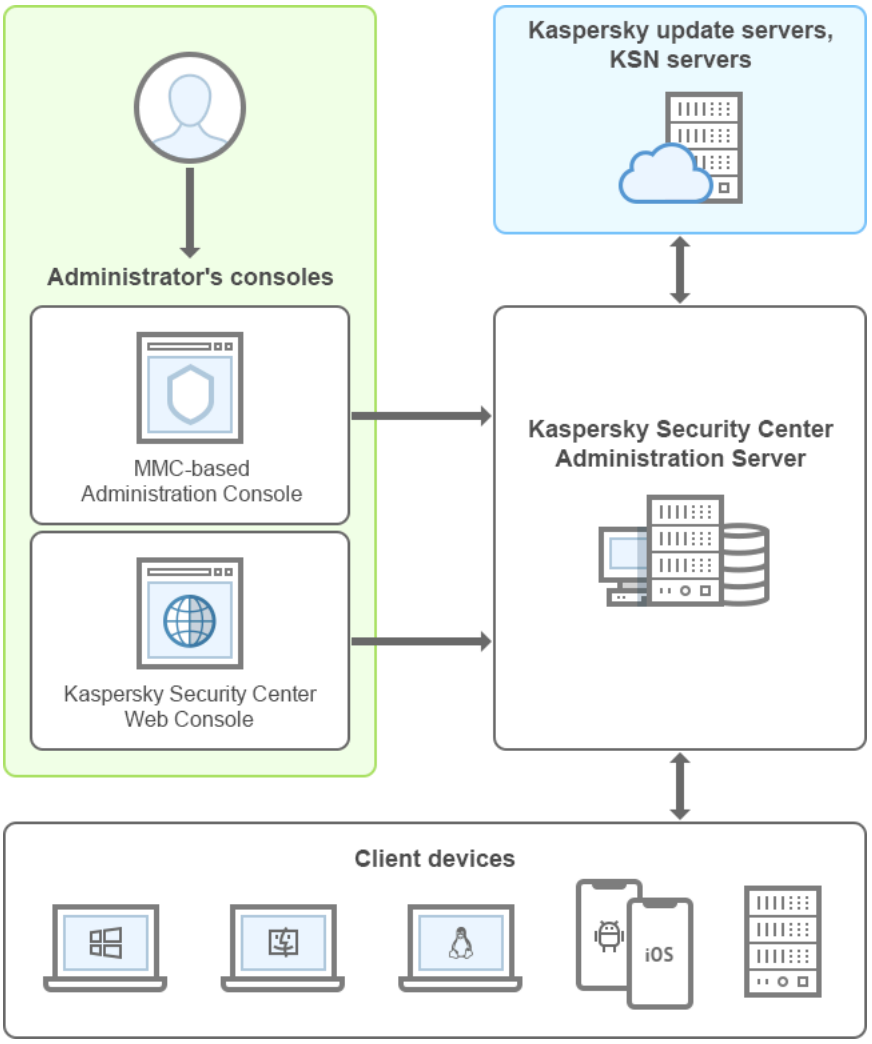
卡巴斯基安全管理中心雲端主控台 的介面和說明文件以下列語言提供：

- 英語
- 法語
- 德語
- 意大利語
- 日語
- 葡萄牙語（巴西）
- 俄語
- 簡體中文
- 西班牙語
- 西班牙語（南美）
- 繁體中文

關於卡巴斯基安全管理中心雲端主控台及其功能的更多資訊請見卡巴斯基安全管理中心雲端主控台文檔和 Kaspersky Endpoint Security for Business 文檔。

架構

該部分提供了對卡巴斯基安全管理中心元件和其互動的敘述。



卡巴斯基安全管理中心架構

卡巴斯基安全管理中心含有以下主要部件：

- *管理主控台*（簡稱*主控台*）。為管理伺服器的管理服務與網路代理之間，提供人性化的使用者介面。管理主控台使用 Microsoft Management Console (MMC) 作為操作介面。使用管理主控台可以透過網際網路連線到管理伺服器。
- *卡巴斯基安全管理中心網頁主控台*。提供 Web 介面以建立和維護由卡巴斯基安全管理中心管理的用戶端組織網路的防護系統。
- *卡巴斯基安全管理中心管理伺服器*（也稱為*伺服器*）。集中管理群組織網路中所安裝應用程式的資訊儲存，並包含如何管理這些應用程式的資訊。
- *Kaspersky 更新伺服器*。Kaspersky 應用程式可以從 Kaspersky 的 HTTP(S) 伺服器下載資料庫和程式模組更新。

- *KSN 伺服器*。包含 Kaspersky 資料庫存取權限的伺服器，其中有持續更新的檔案、網路資源和軟體等信譽資訊。卡巴斯基安全網路確保在遇到未知威脅時 Kaspersky 應用程式能夠做出更快速的回應，提高某些防護元件的效能並降低誤報的可能性。

- *用戶端裝置*。客戶公司的裝置受卡巴斯基安全管理中心保護。每個需要防護的裝置都必須安裝一個 Kaspersky 安全應用程式。

主要安裝情境

該情境允許您佈署管理伺服器以及安裝網路代理和安全應用程式到網路裝置。您可以使用該情境更好的檢視應用程式和安裝應用程式。

卡巴斯基安全管理中心的安裝套件括以下步驟：

1. 準備工作

2. 在管理伺服器裝置上安裝卡巴斯基安全管理中心和 Kaspersky 安全應用程式

3. 在用戶端裝置上集中式佈署 Kaspersky 安全應用程式

在其它「說明」區段會說明佈署卡巴斯基安全管理中心到雲端環境和為服務提供者佈署卡巴斯基安全管理中心。

建議您分配至少一小時用於管理伺服器安裝和至少一個工作日用於完成情境。我們也建議您在將作為卡巴斯基安全管理中心管理伺服器的電腦上安裝安全應用程式，例如 Kaspersky Security for Windows Server 或 Kaspersky Endpoint Security。

情境完成時會以下列方式在組織網路中佈署防護：

- 系統將為管理伺服器安裝 DBMS。

- 系統將會安裝卡巴斯基安全管理中心管理伺服器。

- 系統將會建立所有所需的政策和工作；系統將會指定政策和工作的預設設定。

- 受管理裝置上將安裝安全應用程式（例如，Kaspersky Endpoint Security for Windows）和網路代理。

- 系統會建立管理群組（可能組合成階層）。

- 如有必要，將會佈署行動裝置防護。

- 如有必要，將會分配發佈點。

卡巴斯基安全管理中心安裝分步驟進行：

準備工作

1 **獲取必要檔案**

確保您擁有卡巴斯基安全管理中心的產品授權金鑰（啟動碼）或 Kaspersky Security 應用程式的產品授權金鑰（啟動碼）。

解壓縮從供應商處收到的檔案。此封存包含授權金鑰（金鑰檔案），啟動碼，以及可以透過每個授權金鑰啟動的 Kaspersky 應用程式清單。

如果您想先試用卡巴斯基安全管理中心，則可以在 Kaspersky 網站取得 30 天的免費試用版。

有關卡巴斯基安全管理中心中未包含的 Kaspersky Security 應用程式產品授權的詳細資訊，您可以參考這些應用程式的文件。

2 選取組織防護結構

找到更多卡巴斯基安全管理中心元件。選取最適合您組織的防護結構和網路配置。基於網路配置和通訊管道的輸送量，定義要使用的管理伺服器數量以及如何在您的辦公室間分發它們（如果您的組織執行分散式網路）。

要在不同的操作條件下獲取和維持最佳化執行，請考慮網路裝置數量、網路拓撲和您需要的卡巴斯基安全管理中心功能集（更多詳情，請參考卡巴斯基安全管理中心層級手冊）。

定義是否管理伺服器階層將被用於您的組織。為此，您必須評估您的情況是否適合用單一管理伺服器覆蓋所有用戶端裝置，或者是否有必要建立一個管理伺服器階層。您可能必須建立一個對應於您要防護的組織的組織結構的管理伺服器階層。

如果您必須確保行動裝置的防護，請執行所有設定 Exchange 行動裝置伺服器和 iOS MDM 伺服器所需的先決操作。

確保您選為管理伺服器以及安裝管理主控台的裝置滿足所有的硬體和軟體需求。

3 準備使用自訂憑證

如果組織的金鑰基礎結構 (PKI) 要求您使用由特定憑證頒發機構 (CA) 頒發的自訂憑證，請準備這些憑證並確保它們滿足所有要求。

4 準備卡巴斯基安全管理中心產品授權

如果您排程使用帶有與 SIEM 系統整合的行動裝置管理和/或弱點和修補程式管理系統支援的卡巴斯基安全管理中心版本，請確保您有應用程式產品授權金鑰檔案或啟動碼。

5 準備受管理安全應用程式的產品授權

在防護佈署過程中，您將必須提供 Kaspersky 要透過卡巴斯基安全管理中心管理之應用程式的啟動金鑰（請參閱可管理安全應用程式清單）。對於任何安全應用程式的產品授權詳情，參見此應用程式的文件。

6 選取管理伺服器和 DBMS 的硬體配置

計畫 DBMS 和管理伺服器硬體配置，需要考慮您網路裝置的數量。

7 選取 DBMS

當選取 DBMS 時注意要由該管理伺服器覆蓋的受管理裝置數量。如果您的網路包含少於 10,000 台裝置且您不計畫增加該數字，您可以選取免費 DBMS，例如 SQL Express 或 MySQL，並將其安裝到管理伺服器裝置。另外，您可以選擇 MariaDB DBMS，它最多可以管理 20000 台裝置。如果您的網路包含多於 10,000 台裝置（或如果您計畫延伸您的網路到該數量的裝置），我們建議您選取付費 SQL DBMS 並將其安裝到專用裝置。付費 DBMS 可以用於多個管理伺服器，但免費 DBMS 僅可以用於一個。

如果您選取 SQL Server DBMS，請注意您可以將儲存在資料庫中的資料遷移到 MySQL、MariaDB 或 Azure SQL DBMS。要執行遷移，請備份您的資料並將其還原到新的 DBMS 中。

8 安裝 DBMS 並建立資料庫

找到更多使用 DBMS 的帳戶詳情並安裝您的 DBMS。

安裝之前選擇支援的 DBMS。例如，您可以選取 PostgreSQL、Postgres Pro、Microsoft SQL Server、MySQL 或 MariaDB。

對於如何安裝所選 DBMS 的資訊，請參考其文件。

如要安裝 MariaDB、MySQL、PostgreSQL 或 Postgres Pro，請使用建議的設定以確保 DBMS 正常運行。

寫下並儲存 DBMS 設定，因為您將在管理伺服器安裝時需要它們。這些設定包括 SQL Server 名稱、連線 SQL Server 的埠號、存取 SQL Server 的帳戶名稱和密碼。

如果您決定安裝 PostgreSQL 或 Postgres Pro DBMS，請務必為超級使用者指定密碼。如未指定密碼，管理伺服器可能無法連線到資料庫。

預設下，卡巴斯基安全管理中心安裝程式建立管理伺服器資訊儲存資料庫，但是您可以取消建立該資料庫並使用其他資料庫。此種情況下，確保資料庫已被建立，您知道它的名稱，管理伺服器將再次存取該資料庫的帳戶具有 db_owner 角色。

如果必要，聯絡您的 DBMS 管理員獲取更多資訊。

9. **設定連接埠**

確保所有必要的連接埠都開啟以便與您選取的安全結構對應的各元件間進行互動。

如果您必須提供網際網路存取給管理伺服器，依據網路設定配置連接埠並指定連線設定。

10. **檢查帳戶**

確保您具有所有在裝置上成功安裝卡巴斯基安全管理中心管理伺服器和後續防護佈署所需的本機管理員權限。安裝網路代理到這些裝置上時需要用戶端裝置上的本機管理員權限。安裝網路代理後，您可以使用它遠端安裝應用程式到裝置，而不使用帶有裝置管理員權限的帳戶。

預設下，在用於安裝管理伺服器的裝置上，卡巴斯基安全管理中心安裝程式建立執行管理伺服器和卡巴斯基安全管理中心服務的本機帳戶：

- KL-AK-*：管理伺服器服務帳戶
- NT Service/KSC*：管理伺服器輪詢的其他服務帳戶
- KlPxeUser：作業系統佈署帳戶

您可以不必為管理伺服器服務和其他服務建立帳戶。您使用您的現有帳戶，例如網域帳戶，如果您計畫安裝管理伺服器到容錯移轉叢集，或者由於其他原因計畫使用網域帳戶而不是本機帳戶。此種情況下，確保執行管理伺服器和卡巴斯基安全管理中心服務的帳戶被建立，且具有存取 DBMS 所需的所有權限。（如果您計畫透過卡巴斯基安全管理中心進一步佈署作業系統到裝置，不要結束建立帳戶。）

在管理伺服器裝置上安裝卡巴斯基安全管理中心和 Kaspersky 安全應用程式

1. **為安全應用程式安裝管理伺服器、管理主控台、卡巴斯基安全管理中心網頁主控台和管理外掛程式**

從 Kaspersky 網站 下載卡巴斯基安全管理中心。您可下載完整套件，或是只下載網頁主控台或管理主控台。

安裝管理伺服器到所選裝置（或多個裝置，如果您計畫使用多個管理伺服器）。您可以選取管理伺服器標準或自訂安裝。管理主控台將同管理伺服器一起安裝。建議將管理伺服器安裝在專用伺服器上而不是網域控制器上。

標準安裝用在您要嘗試卡巴斯基安全管理中心並在網路中的小區域測試其操作的時候。在標準安裝期間，您僅設定資料庫。您還可以僅安裝 Kaspersky 應用程式的管理外掛程式的預設集合。如果您有過使用卡巴斯基安全管理中心的經驗，因此您可以在標準安裝後指定所有相關設定，您也可以使用標準安裝。

自訂安裝允許您修改卡巴斯基安全管理中心設定，例如共用資料夾路徑、帳戶和連線管理伺服器的連接埠，以及資料庫設定。自訂安裝允許您指定安裝哪些 Kaspersky 管理外掛程式。如果必要，您可以在靜默模式啟動自訂安裝。

管理主控台和網路代理的伺服器版本與管理伺服器一起安裝。您也可以在安裝過程中選取安裝卡巴斯基安全管理中心網頁主控台。

如果您想，安裝管理主控台和/或卡巴斯基安全管理中心網頁主控台到管理員的工作站以透過網路管理管理伺服器。

2. **初始化設定和產品授權**

當管理伺服器安裝完成後，在第一次連線至管理伺服器時，快速啟動精靈自動開始。依據現有需求指定管理伺服器初始化設定。在初始化配置步驟，精靈使用預設設定建立防護佈署所需的政策和工作。然而，預設設定可能少於您組織需要的最優設定。如果必要，您可以編輯政策和工作設定（在用戶端組織網路中設定防護、情境：設定網路防護）。

如果您排程使用基本功能意外的功能，請授權應用程式。您可以在快速啟動精靈的某步驟做該操作。

3 檢查管理伺服器安裝是否成功

當所有先前步驟完成後，管理伺服器被安裝並準備使用。

確保管理主控台正在執行且您可以透過管理主控台連線到管理伺服器。而且，確保管理伺服器中可使用「將更新下載至管理伺服器儲存區」的工作（在主控台樹狀目錄的**工作**資料夾），以及 Kaspersky Endpoint Security 政策是可用的（在主控台樹狀目錄的**政策**資料夾）。

當檢查完成時，繼續以下步驟。

在用戶端裝置上集中式佈署 Kaspersky 安全應用程式

1 發現網路裝置

該步驟是快速啟動精靈的一部分。您也可以手動啟動裝置發現。卡巴斯基安全管理中心接收網路中偵測到的所有裝置的位址和名稱。然後您可以使用卡巴斯基安全管理中心在偵測到的裝置上安裝 Kaspersky 應用程式和其他供應商的軟體。卡巴斯基安全管理中心定期啟動裝置發現，這意味著如果任何新實例出現在網路，它們將被自動偵測。

2 安裝網路代理和安全應用程式到網路裝置

將防護功能（在用戶端組織網路中設定防護、情境：設定網路防護）佈署到組織網路，則需要在裝置發現期間管理伺服器偵測到的裝置上安裝網路代理和安全應用程式（例如，Kaspersky Endpoint Security）。

安全應用程式防護裝置以防病毒和/或其他威脅程式。網路代理確保裝置和管理伺服器之間的通訊。網路代理設定預設被自動配置。

如有需要，您可以靜默模式搭配回應檔案或不搭配回應檔案來安裝網路代理。

在您開始安裝網路代理和安全應用程式到網路裝置之前，確保這些裝置是可存取的（即開啟）。您可以在虛擬機和物理裝置上安裝網路代理。

安全應用程式和網路代理可以被遠端或本機安裝。

遠端安裝 – 使用防護佈署精靈，您可以遠端安裝安全應用程式（例如 Kaspersky Endpoint Security for Windows）和網路代理到組織網路管理伺服器發現的裝置。通常，遠端安裝工作成功佈署防護到大多數網路裝置。然而，它可能在一些裝置上回傳錯誤，如果，例如裝置被關閉或由於其他原因無法存取。此種情況下，我們建議您手動連線到裝置並使用本機安裝。

本機安裝用於不能使用遠端安裝工作佈署防護的網路裝置。要安裝防護到此類裝置，建立獨立安裝套件以便在這些裝置本機執行。

有關 Linux 和 macOS 作業系統裝置的網路代理安裝說明，請分別參閱 Kaspersky Endpoint Security for Linux 和 Kaspersky Endpoint Security for Mac 的相關文件。雖然我們認為 Linux 和 macOS 作業系統裝置比 Windows 作業系統裝置的弱點少，但建議您也在這類裝置上安裝安全應用程式。

安裝後，確保安全應用程式被安裝到了受管理裝置。執行 Kaspersky 軟體版本報告並檢視結果。

3 佈署產品授權金鑰到用戶端裝置

佈署產品授權金鑰到用戶端裝置以在這些裝置上啟動受管理安全應用程式。

4 設定行動裝置防護

該步驟是快速啟動精靈的一部分。

若您想要管理企業行動裝置，採取必要準備步驟並佈署行動裝置管理。

5 建立管理群組架構

在一些情況下，最方便的佈署防護到網路裝置的方式需要您分割整個裝置池到管理群組，依據組織結構。您可以建立移動規則以在群組間分發裝置，或者您可以手動分發裝置。您可以為管理群組分配群組工作，定義政策範圍並分配發佈點。

確保所有受管理裝置被正確分配到適當的管理群組，且網路中不再有未配置的裝置。

6 分配發佈點

卡巴斯基安全中心指派分佈點自動指派給管理組，但您可以根據需要手動指派它們。我們建議您在大規模網路中使用發佈點以降低管理伺服器負載，以及在具有分散式結構的網路中提供管理伺服器透過窄通道存取裝置（或裝置群組）。您可以使用執行 Linux 的裝置作為發佈點，也可以使用執行 Windows 的裝置。

卡巴斯基安全管理中心使用的連接埠

下表顯示了管理伺服器和用戶端裝置使用的預設連接埠。如果需要，您可以變更每個預設的埠號。

如果您安裝管理伺服器和資料庫到不同裝置，您必須使資料庫所在裝置的必要連接埠可用（例如，連接埠 3306 用於 MySQL Server、連接埠 1433 用於 Microsoft SQL Server，或連接埠 5432 用於 PostgreSQL 和 Postgres Pro）。請參閱 DBMS 文件以取得相關資訊。

管理伺服器使用的連接埠

埠號	開啟連接埠的處理程序名稱	協定	連接埠目的	範圍
8060	klcsweb	TCP	傳輸發佈的安裝套件到用戶端裝置	發佈安裝套件。 您可以在管理主控台或卡巴斯基安全管理中心網頁主控台中，管理伺服器內容視窗的**網頁伺服器**區段中變更預設埠號。 該連接埠是可選的。出於安全原因，我們建議使用 8061 TCP 連接埠。
8061	klcsweb	TCP (TLS)	傳輸發佈的安裝套件到用戶端裝置	發佈安裝套件。 您可以在管理主控台或卡巴斯基安全管理中心網頁主控台中，管理伺服器內容視窗的**網頁伺服器**區段中變更預設埠號。
13000	klserver	TCP (TLS)	從網路代理和從屬管理伺服器接收連線；也用於在從屬管理伺服器上從主管理伺服器接收連線（例如，如果從屬管理伺服器在 DMZ 中）	管理用戶端裝置和從屬管理伺服器。 設定連線的連接埠時，您可以更改用於從網路代理接收連接的預設埠號；在管理主控台或卡巴斯基安全管理中心網頁主控台中建立管理伺服器的階層時，您可以更改用於從從屬管理伺服器接收連接的預設埠號。
13000	klserver	UDP	接收從網路代理關閉的裝置的資訊	管理用戶端裝置。 您可以在管理主控台或卡巴斯基安全管理中心網頁主控台中的網路代理政策設置中更改預設埠號。
13291	klserver	TCP (TLS)	接收從管理主控台到管理伺服器的連線	管理管理伺服器。 您可以在管理主控台中的管理伺服器內容視窗中更改預設埠號。
13299	klserver	TCP (TLS)	接收從卡巴斯基安全管理中心網頁主控台到管理伺服器的連線；接收透過 OpenAPI 到管理伺服器的連線	卡巴斯基安全管理中心網頁主控台，OpenAPI。 您可以在管理伺服器內容視窗中變更預設連接埠號（**管理伺服器連線設定** 部分 → **連線連接埠**子部分），或者在管理主控台中或在卡巴斯基安全管理中心網頁主控台中建立管理伺服器的階層時變更。
14000	klserver	TCP	接收從網路代理的連線	管理用戶端裝置。 在安裝卡巴斯基安全管理中心期間配置連線連接埠時，或將用戶端裝置手動連接到管理伺服器時，您可以更改預設埠號。 該連接埠是可選的。出於安全原因，我們建議使用 1300 TCP 連接埠。
13111（僅在裝置上執行 KSN 代理服務時）	ksnproxy	TCP	接收從受管理裝置到 KSN 代理伺服器的請求	KSN 代理伺服器。 您可以在管理伺服器內容視窗中變更預設埠號。

埠號	開啟連接埠的處理程序名稱	協定	連接埠目的	範圍
15111（僅在裝置上執行 KSN 代理服務時）	ksnproxy	UDP	接收從受管理裝置到 KSN 代理伺服器的請求	KSN 代理伺服器。 您可以在管理伺服器內容視窗中變更預設埠號。
17000	klactprx	TCP (TLS)	接收從受管理裝置的應用程式啟動連線（除了從行動裝置）	非行動裝置用來透過啟動碼啟動卡巴斯基應用程式的啟動代理伺服器。 您可以在管理伺服器內容視窗中更改預設埠號。
17100（僅當您管理行動裝置時）	klactprx	TCP (TLS)	接收從行動裝置的應用程式啟動連線	行動裝置啟動代理伺服器。 您可以在管理伺服器內容視窗中更改預設埠號。
19170	klserver	HTTPS (TLS)	使用 klsctunnel 公用程式將通道與受管理裝置連線	使用卡巴斯基安全管理中心網頁主控台遠端連線受管理裝置。 您只能在管理主控台的管理伺服器屬性視窗中變更預設連接埠號（**管理伺服器連線設定**部分 →**連線連接埠**子部分 →**為卡巴斯基安全管理中心網頁主控台開啟遠端桌面協定連接埠**選項）。
13292（僅當您管理行動裝置時）	klserver	TCP (TLS)	接收從行動裝置的連線	行動裝置管理。 您可以在管理主控台或卡巴斯基安全管理中心網頁主控台的管理伺服器內容視窗中更改預設埠號。
13294（僅當您管理行動裝置時）	klserver	TCP (TLS)	接收從 UEFI 防護裝置的連線	管理 UEFI 防護用戶端裝置。 您可以在連線行動裝置時變更預設連接埠號，或稍後在管理伺服器內容視窗（**管理伺服器連線設定** 部分 → **連線連接埠**子部分）的管理主控台中或在卡巴斯基安全管理中心網頁主控台中變更。
13296	klserver	TCP (TLS)	發布 Prometheus 的卡巴斯基安全管理中心指標	發布卡巴斯基安全管理中心指標，Prometheus 將進一步取得這些指標。 您可以透過以下連結檢視指標：https://<server_address>:13296/metrics。在 <server_address>，指定您的管理伺服器的 IP 位址或網域名稱。 您可以在管理主控台中的管理伺服器內容視窗中更改預設埠號。
30522, 30523（localhost 介面上的連接埠）	klnagent	TCP	使用 FileTransferBridge 元件從管理伺服器接收 卡巴斯基應用程式更新	接收卡巴斯基應用程式更新的管理伺服器裝置。

下表顯示了 iOS MDM 伺服器使用的連接埠（僅在您管理行動裝置時）。

iOS MDM 伺服器使用的連接埠

埠號	開啟連接埠的處理程序名稱	協定	連接埠目的	範圍
443	kliosmdmservicesrv	TCP (TLS)	接收從 iOS 行動裝置的連線	行動裝置管理。 您可以在安裝 iOS MDM 伺服器時更改預設埠號。

下表顯示了卡巴斯基安全管理中心網頁主控台伺服器使用的連接埠。它可以是安裝了管理伺服器的同一裝置，也可以是其他裝置。

卡巴斯基安全管理中心網頁主控台伺服器使用的連接埠

埠號	開啟連接埠的處理程序名稱	協定	連接埠目的	範圍
8080	Node.js：伺服器端 JavaScript	TCP (TLS)	接收從瀏覽器到卡巴斯基安全管理中心網頁主控台的連線	卡巴斯基安全管理中心網頁主控台。 在執行 Windows 或 Linux 平台的裝置上安裝卡巴斯基安全管理中心網頁主控台時，可以更改預設埠號。若在 Linux ALT 作業系統上安裝卡巴斯基安全管理中心網頁主控台，必須指定 8080 以外的連接埠號，因為作業系統使用的連接埠是 8080。

下表顯示了在安裝了網路代理的受管理裝置上使用的連接埠。

網路代理使用的連接埠

埠號	開啟連接埠的處理程序名稱	協定	連接埠目的	範圍
15000	klnagent	UDP	管理從管理伺服器或者發佈點傳至網路代理的訊號	管理用戶端裝置。 您可以在管理主控台或卡巴斯基安全管理中心網頁主控台中的網路代理政策設置中更改預設埠號。
15000	klnagent	UDP 廣播	取得在相同廣播網域中其他網路代理的資料（資料之後會傳送至管理伺服器）	傳送更新和安裝套件。
15001	klnagent	UDP	從發佈點接收多點傳送請求（如果正在使用）	從發佈點接收更新和安裝套件。 您可以在管理主控台中或在卡巴斯基安全管理中心網頁主控台中的發佈點內容視窗中更改預設埠號。
30522, 30523（localhost 介面上的連接埠）	klnagent	TCP	使用 FileTransferBridge 元件從管理伺服器接收 卡巴斯基應用程式更新	從被指定為資料庫更新來源的管理伺服器接收卡巴斯基應用程式更新的受管理裝置。
161	klnagent	SNMP	監控和發現連網裝置。	裝置的可發現性。

請注意，klnagent 處理程序還可以從端點作業系統的動態連接埠範圍請求空閒連接埠。這些連接埠由作業系統自動分配給 klnagent 處理程序，所以 klnagent 處理程序可以使用一些已經被其他軟體使用的連接埠。如果 klnagent 處理程序影響軟體運行，請變更此軟體中的連接埠設定，或變更作業系統中的預設動態連接埠範圍以排除受影響軟體使用的連接埠。

另請注意，有關卡巴斯基安全管理中心與協力廠商軟體的相容性的建議僅供參考，可能不適用於新版本的協力廠商軟體。所描述的配置連接埠的建議基於技術支援人員的經驗和我們的最佳實踐。

下表顯示在安裝了網路代理作為發佈點的受管理裝置上使用的連接埠。除了網路代理使用的連接埠外，列出的連接埠在發佈點裝置上使用（請參見上表）。

作為發佈點之網路代理所用的連接埠

埠號	開啟連接埠的處理程序名稱	協定	連接埠目的	範圍
13000	klnagent	TCP (TLS)	當發佈點充當DMZ 中的連線閘道時，從網路代理和卡巴斯基安全管理中心接收連線。如果安裝了管理伺服器的裝置被指定為發佈點，則預設使用連接埠 13001（而不是 13000）進行 SSL 連線。	管理用戶端裝置、傳送更新和安裝套件。 詳細資訊請參見以下主題：管理伺服器、網段中的連線閘道和用戶端裝置。 您可以在管理主控台中或在卡巴斯基安全管理中心網頁主控台中的發佈點內容視窗中更改預設埠號。
13111（僅在裝置上執行 KSN 代理服務時）	ksnproxy	TCP	接收從受管理裝置到 KSN 代理伺服器的請求	KSN 代理伺服器。 您可以在管理主控台中或在卡巴斯基安全管理中心網頁主控台中的發佈點內容視窗中更改預設埠號。
15111（僅在裝置上執行 KSN 代理服務時）	ksnproxy	UDP	接收從受管理裝置到 KSN 代理伺服器的請求	KSN 代理伺服器。 您可以在管理主控台中或在卡巴斯基安全管理中心網頁主控台中的發佈點內容視窗中更改預設埠號。
17111（僅在裝置上執行 KSN 代理服務時）	ksnproxy	HTTPS	接收從受管理裝置到 KSN 代理伺服器的請求	KSN 代理伺服器。 您可以在管理主控台中或在卡巴斯基安全管理中心網頁主控台中的發佈點內容視窗中更改預設埠號。
13295（僅當您將發佈點用作推送伺服器時）	klnagent	TCP (TLS)	接收用戶端裝置的連線	推送伺服器。 您可以在管理主控台中或在卡巴斯基安全管理中心網頁主控台中的發佈點內容視窗中更改預設埠號。

用於卡巴斯基安全管理中心的憑證

本節包含有關卡巴斯基安全管理中心憑證的資訊並描述如何為管理伺服器頒發自訂憑證。

關於卡巴斯基安全管理中心憑證

卡巴斯基安全管理中心使用以下類型的憑證來啟用應用程式元件之間的安全互動：

- 管理伺服器憑證
- 行動憑證
- iOS MDM 伺服器憑證
- 卡巴斯基安全管理中心網頁伺服器憑證
- 卡巴斯基安全管理中心網頁主控台憑證

預設情況下，卡巴斯基安全管理中心使用自我簽署憑證（即由卡巴斯基安全管理中心本身頒發的憑證），但是您可以用自訂憑證加以替換，以更好地滿足組織網路的要求並符合安全標準。在管理伺服器驗證自訂憑證是否滿足所有適用要求之後，該憑證將承擔與自我簽署憑證相同的功能範圍。唯一的區別是自訂憑證在到期後不會自動重新發行。您可以透過 klsetsrvcert 公用程式或透過管理主控台中的「管理伺服器屬性」區段將憑證替換為自訂憑證，具體視憑證類型而定。使用 klsetsrvcert 實用程式時，您需要使用以下值之一指定憑證類型：

- C—適用於連接埠 13000 和 13291 的常見憑證。
- CR—適用於連接埠 13000 和 13291 的預留憑證。
- M—適用於連接埠 13292 的行動憑證。
- MR—適用於連接埠 13292 的行動預留憑證。
- MCA—適用於自動產生使用者憑證的行動憑證機構。

> 您無需下載 klsetsrvcert 公用程式。它包含在卡巴斯基安全管理中心分發套件中。公用程式與以前的卡巴斯基安全管理中心版本不相容。

任何管理伺服器憑證的最長有效期不得超過 397 天。

管理伺服器憑證

管理伺服器的驗證以及管理伺服器和受管理裝置上的網路代理間、或主管理伺服器和從屬管理伺服器之間的安全互動時，需要管理伺服器憑證。首次將管理主控台連線到管理伺服器時，系統將提示您確認當前使用的管理伺服器憑證。每次更換管理伺服器憑證時，每次重新安裝管理伺服器後，以及將從屬管理伺服器連線到主管理伺服器時，都需要進行此類確認。該憑證稱為通用憑證 ("C")。

安裝管理伺服器元件時會自動建立通用（“C”）憑證。憑證由兩部分組成：

- klserver.cer 檔；預設情況下，它位於安裝管理伺服器元件的裝置上的 C:\ProgramData\KasperskyLab\adminkit\1093\cert 資料夾中。
- 金鑰位於 Windows 受防護的儲存中。

此外，還存在一個通用預留（「CR」）憑證。卡巴斯基安全管理中心會在通用憑證到期前 90 天自動產生此憑證。公用預留憑證隨後會用來無縫替換管理伺服器憑證。當公用憑證即將到期時，公用預留憑證會用來維持與安裝在受管理裝置上網路代理實例的連線。為此，通用預留憑證會在舊的通用憑證到期前 24 小時自動變為新的通用憑證。

您也可以與其他管理伺服器設置獨立的備份管理伺服器憑證，以在將管理伺服器從一部裝置移至另一部裝置時不會遺失資料。

行動憑證

在行動裝置上對管理伺服器進行驗證需要行動憑證（「M」）。您可以在「快速啟動精靈」的專用步驟上配置使用行動憑證。

此外還有行動預留（「MR」）憑證：該憑證會用來無縫替換行動憑證。當行動憑證即將到期時，將使用行動備用憑證來維護與安裝在受管理行動裝置上的網路代理實例的連線。為此，行動備用憑證會在舊的行動憑證到期前 24 小時自動變為新的行動憑證。

不支援自動重新頒發行動憑證。我們建議您在現有憑證即將到期時指定新的行動憑證。如果行動憑證過期且未指定儲備行動憑證，則管理伺服器與安裝在受管理行動裝置上的網路代理實例之間的連線將丟失。在這種情況下，要重新連線受管理行動裝置，您必須指定新的行動憑證並在每個受管理行動裝置上重新安裝 Kaspersky Security for Mobile。

如果連線情境要求在行動裝置上使用用戶端憑證（涉及雙向 SSL 驗證的連線），則可以透過用於自動產生的使用者憑證（「MCA」）的憑證機構來產生那些憑證。此外，快速啟動精靈使您可以開始使用由其他憑證機構發行的自訂用戶端憑證，而與組織的網域公用金鑰基礎架構 (PKI) 整合，可讓您透過網域憑證機構發佈用戶端憑證。

iOS MDM 伺服器憑證

在執行 iOS 作業系統的行動裝置上對管理伺服器進行驗證時，需要 iOS MDM 伺服器憑證。透過不涉及網路代理的 Apple 行動裝置管理 (MDM) 通訊協定執行與這些裝置的互動。而是在每部裝置上安裝特殊的 iOS MDM 設定檔，其中包含用戶端憑證，以確保雙向 SSL 驗證。

此外，快速啟動精靈使您可以開始使用由其他憑證機構發行的自訂用戶端憑證，而與組織的網域公用金鑰基礎架構 (PKI) 整合，可讓您透過網域憑證機構發佈用戶端憑證。

當您下載那些 iOS MDM 設定檔時，用戶端憑證會傳輸到 iOS 裝置。iOS MDM 伺服器用戶端憑證對於每個受管理 iOS 裝置都是唯一的。您將透過自動產生的使用者憑證（「MCA」）的憑證機構產生所有 iOS MDM 伺服器用戶端憑證。

卡巴斯基安全管理中心網頁伺服器憑證

卡巴斯基安全管理中心網頁伺服器（以下簡稱 Web 伺服器）是卡巴斯基安全管理中心管理伺服器的元件，使用特殊類型的憑證。發佈此網路代理安裝套件（隨後將其下載到受管理裝置）以及發佈 iOS MDM 設定檔，iOS 應用程式和 Kaspersky Security for Mobile 安裝套件都需要此憑證。基於此用途，網頁伺服器可以使用各種憑證。

如果停用行動裝置支援，則網頁伺服器會按優先等級使用以下憑證之一：

1. 您透過管理主控台手動指定的自訂網頁伺服器憑證
2. 通用管理伺服器憑證 ("C")

如果啟用行動裝置支援，則網頁伺服器會按優先等級使用以下憑證之一：

1. 您透過管理主控台手動指定的自訂網頁伺服器憑證
2. 自訂行動憑證
3. 自我簽署行動憑證（「M」）
4. 通用管理伺服器憑證 ("C")

卡巴斯基安全管理中心網頁主控台憑證

卡巴斯基安全管理中心網頁主控台（以下簡稱「網頁主控台」）的伺服器有自己的憑證。當您開啟網站時，瀏覽器會驗證您的連線是否可信。網頁主控台憑證允許您對網頁主控台進行身分驗證，並被用於加密瀏覽器和網頁主控台之間的流量。

當您開啟網頁主控台時，瀏覽器會通知您與網頁主控台的連線不是私有，並且網頁主控台憑證無效。出現此警告是因為網頁主控台憑證為自簽名並由卡巴斯基安全管理中心自動產生。要刪除此警告，您可以執行以下操作之一：

- 用自訂憑證替代網頁主控台憑證（建議選項）。建立一個在您的基礎架構中受信任且滿足自訂憑證的要求的憑證。
- 將網頁主控台憑證新增到受信任的瀏覽器憑證清單中。我們建議您僅在無法建立自訂憑證時使用此選項。

關於管理伺服器憑證

以下兩項操作都是根據*管理伺服器憑證*來執行的：連線期間管理主控台進行的管理伺服器身分驗證以及與裝置的資料交換。此憑證還用於在主管理伺服器連線到從屬管理伺服器時的身分驗證。

由 Kaspersky 發佈的憑證

管理伺服器憑證是在安裝管理伺服器元件時自動產生的，並儲存在 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert 資料夾中。

如果管理伺服器憑證是由管理伺服器版本 12.2 或更早版本產生的，則該憑證的有效期為五年。否則，憑證有效期不得超過 397 天。在目前憑證到期前 90 天，新憑證會傳輸到管理伺服器。然後，新憑證在到期日期一天前自動取代目前憑證。用戶端裝置上的所有網路代理被自動設定以驗證管理伺服器新憑證。

自訂憑證

如有必要，您可以為管理伺服器分配協力廠商憑證。例如，為了更好的整合您企業的現有 PKI 或為了憑證欄位的自訂設定，這可能是必要的。

任何管理伺服器憑證的最長有效期不得超過 397 天。

當取代憑證時，所有先前透過 SSL 連線到管理伺服器的網路代理將遺失它們的連線，並將返回「管理伺服器身分驗證錯誤」。要消除該錯誤，您將必須在憑證取代後還原連線。

如果遺失了管理伺服器憑證，要想還原憑證，就只能重新安裝管理伺服器元件，然後還原資料。

如果您在不同的瀏覽器中開啟卡巴斯基安全管理中心網頁主控台並在管理伺服器屬性視窗中下載管理伺服器憑證檔案，則下載的檔案具有不同名稱。

卡巴斯基安全管理中心中使用的自訂憑證要求

下表顯示了為卡巴斯基安全管理中心的不同元件指定的自訂憑證的要求。

卡巴斯基安全管理中心憑證要求

憑證類型	要求	註解
一般憑證，一般備用憑證（「C」、「CR」）	最小金鑰長度：2048。 基本限制： • 路徑長度限制：無 金鑰使用情況： • 電子簽名 • 憑證籤名 • 金鑰加密 • CRL 簽署 延伸金鑰使用（選填）：伺服器身分驗證、用戶端身分驗證。	延伸金鑰使用參數為選填。 路徑長度限制值可以有別於「無」，但不能小於「1」。
移動憑證、移動備用憑證（「M」、「MR」）	最小金鑰長度：2048。 基本限制： • CA：真 • 路徑長度限制：無 金鑰使用情況： • 電子簽名 • 憑證籤名 • 金鑰加密 • CRL 簽署 延伸金鑰使用（選填）：伺服器身分驗證。	延伸金鑰使用參數為選填。 如果一般憑證的「路徑長度限制」值不小於「1」，則「路徑長度限制值」可能與「無」不同。

憑證類型	要求	註解
自動產生之使用者憑證（「MCA」）的憑證 CA	最小金鑰長度：2048。 基本限制： • CA：真 • 路徑長度限制：無 金鑰使用情況： • 電子簽名 • 憑證簽名 • 金鑰加密 • CRL 簽署 延伸金鑰使用（選填）：伺服器身分驗證、用戶端身分驗證。	延伸金鑰使用參數為選填。 如果一般憑證的「路徑長度限制」值不小於「1」，則「路徑長度限制值」可能與「無」不同。
網頁伺服器憑證	延伸金鑰使用：伺服器身分驗證。 從中指定憑證的 PKCS # 12/PEM 容器會包括整個公共金鑰鏈。 出現憑證的主題替代名稱 (SAN)；也就是說，`subjectAltName` 欄位值有效。 該憑證符合瀏覽器對伺服器憑證施加的有效要求，以及 CA/瀏覽器論壇 的目前基準要求。	–
卡巴斯基安全管理中心網頁主控台憑證	從中指定憑證的 PEM 容器會包括整個公共金鑰鏈。 出現憑證的主題替代名稱 (SAN)；也就是說，`subjectAltName` 欄位值有效。 該憑證符合瀏覽器對伺服器憑證的有效要求，以及 CA/瀏覽器論壇 的目前基準要求。	卡巴斯基安全管理中心網頁主控台不支援加密憑證。

情境：指定自訂管理伺服器憑證

例如，您可以分配自訂管理伺服器憑證以便更好地與企業的現有公鑰基礎結構 (PKI) 進行整合，或自訂配置憑證欄位。最好在安裝管理伺服器後，快速啟動精靈完成之前立即取代憑證。

任何管理伺服器憑證的最長有效期不得超過 397 天。

先決條件

必須滿足以下條件：

- 新憑證必須以 PKCS#12 格式建立（例如，透過組織的 PKI）。
- 對於新憑證，必須滿足下表中列出的要求。

  在下表中，請注意要求“CA: true”，這表示新憑證必須由受信任的憑證授權單位 (CA) 頒發。具有要求"CA: true"的新憑證必須包含整個信任鏈和私密金鑰，該私密金鑰必須儲存在副檔名為 pfx 或 p12 的檔案中。

管理伺服器憑證的要求

憑證類型	要求
一般憑證，一般備用憑證（「C」、「CR」）	最小金鑰長度：2048。 基本限制： • 路徑長度限制：無 路徑長度限制值可以有別於「無」，但不能小於「1」。 金鑰使用情況： • 電子簽名 • 憑證簽名 • 金鑰加密 • CRL 簽署 延伸金鑰使用 (EKU)：伺服器身分驗證和用戶端身分驗證。EKU 可選，但如果您的憑證包含它，則必須在 EKU 中指定伺服器和用戶端身分驗證資料。
移動憑證、移動備用憑證（「M」、「MR」）	最小金鑰長度：2048。 基本限制： • CA：真 • 路徑長度限制：無 如果一般憑證的「路徑長度限制值不小於 1」，則「路徑長度限制值」可以是與「無」不同的整數。 金鑰使用情況： • 電子簽名 • 憑證簽名 • 金鑰加密 • CRL 簽署 延伸金鑰使用 (EKU)：伺服器身分驗證。EKU 可選，但如果您的憑證包含它，則必須在 EKU 中指定伺服器身分驗證資料。
自動產生之使用者憑證（「MCA」）的憑證 CA	最小金鑰長度：2048。 基本限制： • CA：真 • 路徑長度限制：無 如果一般憑證的「路徑長度限制值不小於 1」，則「路徑長度限制值」可以是與「無」不同的整數。 金鑰使用情況： • 電子簽名 • 憑證簽名 • 金鑰加密 • CRL 簽署 延伸金鑰使用 (EKU)：用戶端身分驗證。EKU 可選，但如果您的憑證包含它，則必須在 EKU 中指定用戶端身分驗證資料。

公共 CA 頒發的憑證沒有憑證簽名權限。要使用此類憑證，請確保您在網路中的發佈點或連線閘道上安裝了

網路代理版本 13 或更高版本。否則，您將無法在沒有簽名權限的情況下使用憑證。

階段

指定管理伺服器憑證分階段進行：

1. **替換管理伺服器憑證**

   為此使用指令行 klsetsrvcert utility。

2. **指定新憑證和還原網路代理與管理伺服器的連線**

   當憑證被取代時，所有先前透過 SSL 連線到管理伺服器的網路代理會遺失它們的連線，並返回「管理伺服器身分驗證錯誤」。要指定新憑證和還原連線，使用 klmover 公用程式。

3. **在卡巴斯基安全管理中心網頁主控台的設定中指定新憑證**

   更換憑證後，請在卡巴斯基安全管理中心網頁主控台的設定中指定憑證。否則，卡巴斯基安全管理中心網頁主控台將無法連線到管理伺服器。

結果

當您結束情境時，管理伺服器憑證被取代，且伺服器得到受管理裝置上的網路代理的身分驗證。

使用 klsetsrvcert 公用程式替換管理伺服器憑證

要取代管理伺服器憑證：

在命令列下，執行以下公用程式：

```
klsetsrvcert [-t <憑證類型> {-i <新憑證路徑> [-p <密碼>] [-o <參數>] | -g < dns 名稱>}]
[ - f <取代時間> ] [-r <根憑證> ] [ - l <日誌檔案路徑> ]
```

您無需下載 klsetsrvcert 公用程式。它包含在卡巴斯基安全管理中心分發套件中。它與以前的卡巴斯基安全管理中心版本不相容。

下表列出了 klsetsrvcert 公用程式參數的說明。

klsetsrvcert 實用工具參數值

參數	參數值
`-t <憑證類型>`	要取代的憑證類型。<憑證類型>參數可能的值： • `C` – 取代連接埠 13000 和 13291 的普通憑證。 • `CR` – 取代連接埠 13000 和 13291 的普通預留憑證。 • `M`—在連接埠 13292 取代行動裝置憑證。 • `MR`—取代連接埠 13292 的行動預留憑證。 • `MCA`—適用於自動產生使用者憑證的行動憑證授權機構。
`-f <取代時間>`	變更憑證的時間排程，使用格式「DD-MM-YYYY hh:mm」（適用於連接埠 13000 和 13291）。 如果要在通用憑證到期前使用備用通用憑證取代通用憑證，請使用此參數。 指定受管理裝置必須與新憑證上的管理伺服器同步的時間。

參數	參數值
`-i <新憑證路徑>`	帶有 PKCS#12 格式憑證和私密金鑰的容器（帶有副檔名 .p12 或 .pfx 的檔案）。
`-p <密碼>`	用於防護 p12 容器的密碼。 憑證和私密金鑰儲存在容器中，因此需要密碼才能使用容器解密檔案。
`-o <驗證參數>`	憑證驗證參數（以冒號區隔）。 要在沒有簽名權限的情況下使用自訂憑證，請在 klsetsrvcert 公用程式中指定 `-o NoCA`。這對於公共 CA 頒發的憑證很有用。 若要變更憑證類型 C 或 CR 的加密金鑰長度，請在 klsetsrvcert 實用程式中指定 `-o RsaKeyLen:<金鑰長度>`，其中 `<金鑰長度>` 參數是所需的金鑰長度值。否則，將使用目前的憑證金鑰長度。
`-g <dns 名稱>`	新憑證將為指定 DNS 名稱建立。
`-r <根憑證>`	信任的根憑證授權機構清單，格式 PEM。
`-l <日誌檔案路徑>`	結果輸入檔案。預設下，輸出被重新定向到標準輸出流。

例如，要指定自訂管理伺服器憑證，使用以下指令：

```
klsetsrvcert -t C -i <新憑證路徑> -p <密碼> -o NoCA
```

憑證被取代後，所有透過 SSL 連線到管理伺服器的網路代理都會失去連線。要還原它，請使用指令行 klmover utility。

為避免丟失網路代理連線，請使用以下指令：

1. 安裝新憑證：

   ```
   klsetsrvcert.exe -t CR -i <新憑證路徑> -p <密碼> -o NoCA
   ```

2. 指定套用新憑證的日期：

   ```
   klsetsrvcert.exe -f "DD-MM-YYYY hh:mm"
   ```

其中，“`DD-MM-YYYY hh:mm`”是比目前日期晚 3-4 週的日期。將憑證變更為備份憑證的時間偏移將允許將新憑證分發給所有網路代理。

使用 klmover 公用程式將網路代理連線到管理伺服器

使用命令列 klsetsrvcert 公用程式替換管理伺服器憑證後，您需要在網路代理和管理伺服器之間建立 SSL 連線，因為連線已斷開。

要指定新管理伺服器憑證並還原連線：

在命令列下，執行以下公用程式：

```
klmover [-address <伺服器位址>] [-pn <埠號>] [-ps <SSL 埠號>] [-nossl] [-cert <憑證檔案的路徑>]
```

執行該公用程式需要管理員權限。

當網路代理安裝在用戶端裝置上時，此公用程式會自動複製到網路代理安裝資料夾。

如果在**網路代理政策設定使用解除安裝密碼**使用解除安裝密碼選項且使用的網路代理版本為 15，則 klmover 公用程式需要對應的密碼。您可以使用位於網路代理安裝資料夾中的 klcsngtgui 公用程式來檢查網路代理版本。

對於透過連線閘道連線到管理伺服器的用戶端裝置，您不能使用 klmover 實用程式。對於這樣的裝置，您必須重新設定網路代理或重新安裝網路代理並指定連線閘道。

下表列出了 klmover 公用程式參數的說明。

Klmover 公用程式參數值

參數	參數值
`-address <伺服器位址>`	用於連線的管理伺服器的位址。 您可以指定 IP 位址、NetBIOS 名稱或 DNS 名稱。
`-pn <連接埠號>`	用來建立與管理伺服器非加密連線的埠號。 預設埠號為 14000。
`-ps <SSL 連接埠號>`	使用 SSL 與管理伺服器建立加密連線時使用的 SSL 埠號。 預設埠號為 13000。
`-nossl`	使用非加密方式連線管理伺服器。 如果未使用該鍵值，網路代理將透過使用加密的 SSL 協定連線至管理伺服器。
`-cert <憑證檔案的路徑>`	存取管理伺服器時使用指定的憑證檔案作為身分驗證。
`-virtserv`	虛擬管理伺服器名稱。
`-cloningmode`	網路代理磁碟克隆模式。 使用以下參數之一配置磁碟克隆模式： • `-cloningmode`—請求磁碟克隆模式的狀態。 • `-cloningmode 1`—啟用磁碟克隆模式。 • `-cloningmode 0`—停用磁碟克隆模式。
`-nauninstpwd <密碼>`	使用此參數指定網路代理解除安裝密碼。 該參數不是必需的。

例如，要將網路代理連線到管理伺服器，請執行以下指令：

```
klmover  -address kscserver.mycompany.com -logfile klmover.log
```

重新發行網頁伺服器憑證

發佈之後要下載到受管理裝置的網路代理安裝套件，以及發佈 iOS MDM 設定檔、iOS 應用程式和 Kaspersky Endpoint Security for Mobile 安裝套件，都需要卡巴斯基安全管理中心使用的網頁伺服器憑證。根據目前的應用程式配置，各種憑證都可以用作網頁伺服器憑證（如需詳細資訊，請參閱關於卡巴斯基安全管理中心憑證）。

在開始升級應用程式之前，您可能需要重新頒發網頁伺服器憑證以滿足組織的特定安全要求或保持受管理裝置的連續連線。卡巴斯基安全管理中心提供了兩種重新發佈網頁伺服器憑證的方式；兩種方法之間的選擇取決於您是否透過行動協議（即透過使用行動憑證）連線和管理行動裝置。

如果您從未將自己的自訂憑證指定為網頁伺服器憑證，在"管理伺服器"內容視窗的"**網頁伺服器**"區段中，行動憑證會作為網頁伺服器憑證。在這種情況下，透過重新發佈行動協議本身來執行網頁伺服器憑證的重新發佈。

若要在沒有透過行動協議管理行動裝置時重新發佈網頁伺服器憑證，請執行以下操作：

1. 在主控台樹狀結構中，右擊相關管理伺服器的名稱，然後在內容功能表中選取**內容**。
2. 在開啟的"管理伺服器"內容視窗中左側的頁籤，選取**管理伺服器連線設定**區段。
3. 在裝置清單中，選取**憑證**子區段。
4. 如果您打算繼續使用卡巴斯基安全管理中心頒發的憑證，請執行以下操作：
   a. 在右窗格中的**管理伺服器的行動裝置身分驗證**群組設定，選取**透過管理伺服器發佈的憑證**選項，然後點擊**重新發佈**按鈕。
   b. 在開啟的**重新發佈憑證**視窗中設定的**連線位址**和**啟動條款**群組，選取相關選項並點擊**確定**。
   c. 在確認視窗中，點擊**是**。

   或者，如果您打算使用自己的自訂憑證，請執行以下操作：

   a. 檢查您的自訂憑證是否符合卡巴斯基安全管理中心的要求以及 Apple 對受信任憑證的要求。如有必要，請修改憑證。
   b. 選取**其他憑證**選項並點擊**瀏覽**按鈕。
   c. 在開啟的**憑證**視窗中的**憑證類型**欄位選取憑證類型，然後指定憑證位置和設定：
      - 如果您已選擇**PKCS#12 容器**，請點擊**瀏覽**旁邊的按鈕**憑證檔案**欄位並在硬碟上指定憑證檔案。如果憑證檔案受密碼防護，請在**密碼（如果有）**欄位。
      - 如果您已選取**X.509 憑證**，點擊**瀏覽**旁邊的按鈕**私密金鑰(.prk 、.pem)**欄位並在硬碟上指定私密金鑰。如果私密金鑰受密碼防護，請在**密碼（如果有）**欄位中輸入密碼。然後點擊**公開金鑰 (.cer)**旁邊的**瀏覽**按鈕，並在硬碟上指定私密金鑰。
   d. 在 **憑證**視窗中，點擊**確定**。
   e. 在確認視窗中，點擊**是**。

   重新發佈行動憑證以用作網頁伺服器憑證。

若要在透過行動協議管理任何行動裝置時重新發行網頁伺服器憑證，請執行以下操作：

1. 產生自訂憑證，並為卡巴斯基安全管理中心中的使用做好準備。檢查您的自訂憑證是否符合卡巴斯基安全管理中心的要求以及 Apple 對受信任憑證的要求。如有必要，請修改憑證。

   您可以使用 kliossrvcertgen.exe 實用程式來產生憑證。

2. 在主控台樹狀結構中，右擊相關管理伺服器的名稱，然後在內容功能表中選取**內容**。

3. 在開啟的"管理伺服器"內容視窗中左側的頁籤，選取**網頁伺服器**區段。

4. 在**透過 HTTPS**功能表中，選取**指定其他憑證**選項。

5. 在**透過 HTTPS**功能表，點擊**變更**按鈕。

6. 在開啟的**憑證**視窗中的**憑證類型**欄位內選取憑證的類型：

   - 如果您已選擇**PKCS#12 容器**，請點擊**瀏覽**旁邊的按鈕**憑證檔案**欄位並在硬碟上指定憑證檔案。如果憑證檔案受密碼防護，請在**密碼（如果有）**欄位。
   - 如果您已選取**X.509 憑證**，點擊**瀏覽**旁邊的按鈕**私密金鑰(.prk 、.pem)**欄位並在硬碟上指定私密金鑰。如果私密金鑰受密碼防護，請在**密碼（如果有）**欄位中輸入密碼。然後點擊**公開金鑰 (.cer)**旁邊的**瀏覽**按鈕，並在硬碟上指定私密金鑰。

7. 在 **憑證**視窗中，點擊**確定**。

8. 如有必要，在“管理伺服器內容”視窗中的**網頁伺服器 HTTPS 連接埠**欄位更改網頁伺服器的 HTTPS 埠號。點擊“**確定**”。

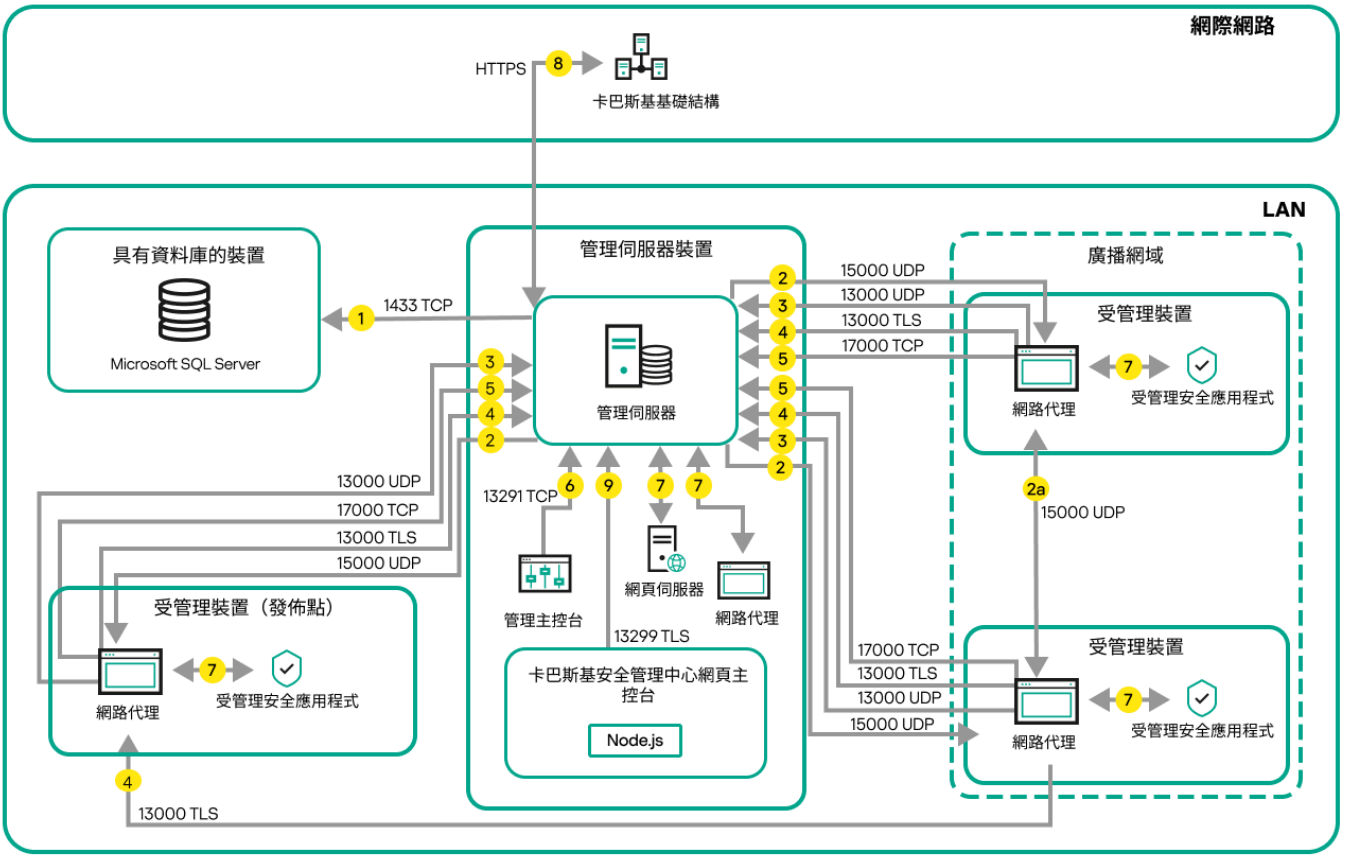
   重新發佈網頁伺服器憑證。

資料流量和連接埠使用的 schema

該部分提供了卡巴斯基安全管理中心元件、受管理安全應用程式和不同配置下的外部伺服器之間的資料流量 schema。結構描述提供了必須可在本機裝置上使用的連接埠號。

LAN 中的管理伺服器和受管理裝置

下圖顯示卡巴斯基安全管理中心僅在區域網路（LAN）中被佈署時的資料流量。



區域網路（LAN）中的管理伺服器和受管理裝置

該圖片顯示了受管理裝置連線到管理伺服器的不同方式：直接或透過發佈點。發佈點降低發佈更新時管理伺服器的負載並最佳化網路流量。然而，發佈點僅在受管理裝置數量足夠大時才被需要。如果受管理裝置數量較小，所有受管理裝置可以從管理伺服器直接接收更新。

箭頭表示流量的開始：每個箭頭從發起連線的裝置指向"回答"請求的裝置。連接埠號和用於資料傳輸的協定名稱被提供。每個箭頭都有數字標籤，對應的資料流量詳情是：

1. 管理伺服器傳送資料到資料庫。如果您安裝管理伺服器和資料庫到不同裝置，您必須使資料庫所在裝置的必要連接埠可用（例如，連接埠 3306 用於 MySQL 伺服器，或連接埠 1433 用於 Microsoft SQL Server）。請參閱 DBMS 文件以取得相關資訊。

2. 來自管理伺服器的通信請求被傳輸到所有非行動受管理裝置，透過 UDP 連接埠 15000。

   網路代理會在一個廣播網域中傳送要求給彼此。資料之後會傳送至管理伺服器並用來定義廣播網域的限制，以及發佈點的自動分配（若已啟用此選項）。

   如果管理伺服器無法直接存取受管理裝置，則不會直接傳送從管理伺服器到這些裝置的通信請求。

3. 受管理裝置關閉的資訊透過 UDP 連接埠 13000 被從網路代理傳輸到管理伺服器。

4. 管理伺服器透過 TLS 連接埠 13000 從網路代理和從屬管理伺服器接收連線。

   如果您使用卡巴斯基安全管理中心的早期版本，您網路中的管理伺服器可以透過非 TLS 連接埠 14000 從網路代理接收連線。卡巴斯基安全管理中心也支援透過連接埠 14000 連線網路代理，儘管使用 TLS 連接埠 13000 是被建議的。

   > 發佈點在早期卡巴斯基安全管理中心版本中被叫做更新代理。

5. 受管理裝置（除了行動裝置）透過 TCP 連接埠 17000 請求啟動。如果裝置自己擁有網際網路連線，則不必要；此種情況下，裝置直接透過網際網路傳送資料到 Kaspersky 伺服器。

6. 基於 MMC 的管理主控台透過連接埠 13291 傳送資料到管理伺服器。（管理主控台可以安裝在相同或不同裝置。）

7. 單一裝置交換本機流量的應用程式（在管理伺服器或受管理裝置之一）。不需要開啟任何外部連接埠。

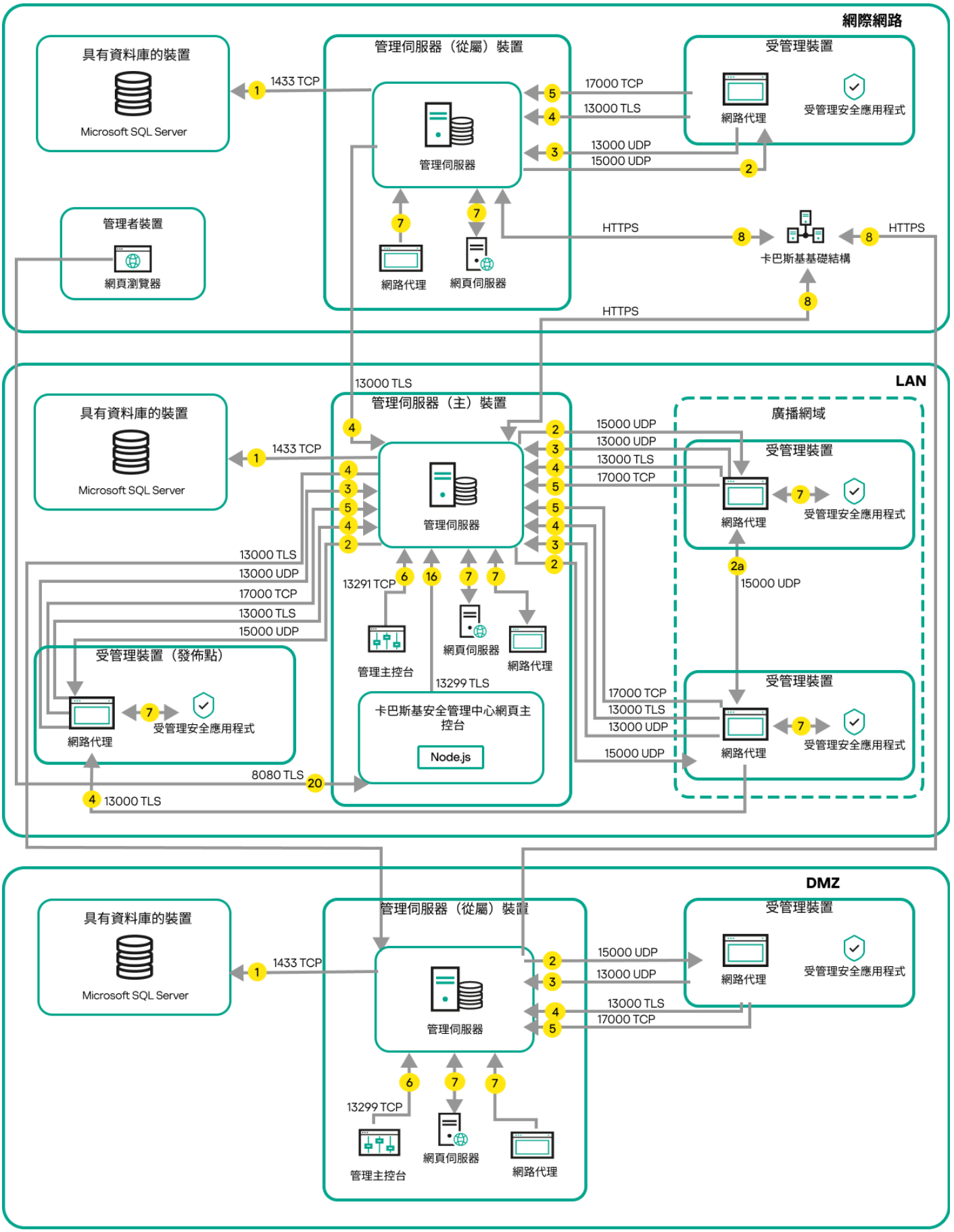
8. 從管理伺服器到 Kaspersky 伺服器的資料（例如 KSN 資料或產品授權資訊）和從 Kaspersky 伺服器到管理伺服器的資料（例如應用程式更新和病毒資料庫更新）使用 HTTPS 協定傳輸。

   如果您不想讓您的管理伺服器擁有網際網路連線，您必須手動管理該資料。

9. 卡巴斯基安全管理中心網頁主控台伺服器透過 TLS 連接埠 13299 傳送資料到管理伺服器，該管理伺服器可能被安裝到相同或不同裝置。

LAN 的主管理伺服器和兩個從屬管理伺服器

下圖顯示管理伺服器階層：主管理伺服器位於區域網路 (LAN)。一個從屬管理伺服器位於 DMZ；另一個從屬管理伺服器位於網際網路。



管理伺服器階層：主管理伺服器和兩個從屬管理伺服器

箭頭表示流量的開始：每個箭頭從發起連線的裝置指向"回答"請求的裝置。連接埠號和用於資料傳輸的協定名稱被提供。每個箭頭都有數字標籤，對應的資料流量詳情是：

1. 管理伺服器傳送資料到資料庫。如果您安裝管理伺服器和資料庫到不同裝置，您必須使資料庫所在裝置的必要連接埠可用（例如，連接埠 3306 用於 MySQL 伺服器，或連接埠 1433 用於 Microsoft SQL Server）。請參閱 DBMS 文件以取得相關資訊。

2. 來自管理伺服器的通信請求被傳輸到所有非行動受管理裝置，透過 UDP 連接埠 15000。

   網路代理會在一個廣播網域中傳送要求給彼此。資料之後會傳送至管理伺服器並用來定義廣播網域的限制，以及發佈點的自動分配（若已啟用此選項）。

   如果管理伺服器無法直接存取受管理裝置，則不會直接傳送從管理伺服器到這些裝置的通信請求。

3. 受管理裝置關閉的資訊透過 UDP 連接埠 13000 被從網路代理傳輸到管理伺服器。

4. 管理伺服器透過 TLS 連接埠 13000 從網路代理和從屬管理伺服器接收連線。

   如果您使用卡巴斯基安全管理中心的早期版本，您網路中的管理伺服器可以透過非 TLS 連接埠 14000 從網路代理接收連線。卡巴斯基安全管理中心也支援透過連接埠 14000 連線網路代理，儘管使用 TLS 連接埠 13000 是被建議的。

   > 發佈點在早期卡巴斯基安全管理中心版本中被叫做更新代理。

5. 受管理裝置（除了行動裝置）透過 TCP 連接埠 17000 請求啟動。如果裝置自己擁有網際網路連線，則不必要；此種情況下，裝置直接透過網際網路傳送資料到 Kaspersky 伺服器。

6. 基於 MMC 的管理主控台透過連接埠 13291 傳送資料到管理伺服器。（管理主控台可以安裝在相同或不同裝置。）

7. 單一裝置交換本機流量的應用程式（在管理伺服器或受管理裝置之一）。不需要開啟任何外部連接埠。

8. 從管理伺服器到 Kaspersky 伺服器的資料（例如 KSN 資料或產品授權資訊）和從 Kaspersky 伺服器到管理伺服器的資料（例如應用程式更新和病毒資料庫更新）使用 HTTPS 協定傳輸。

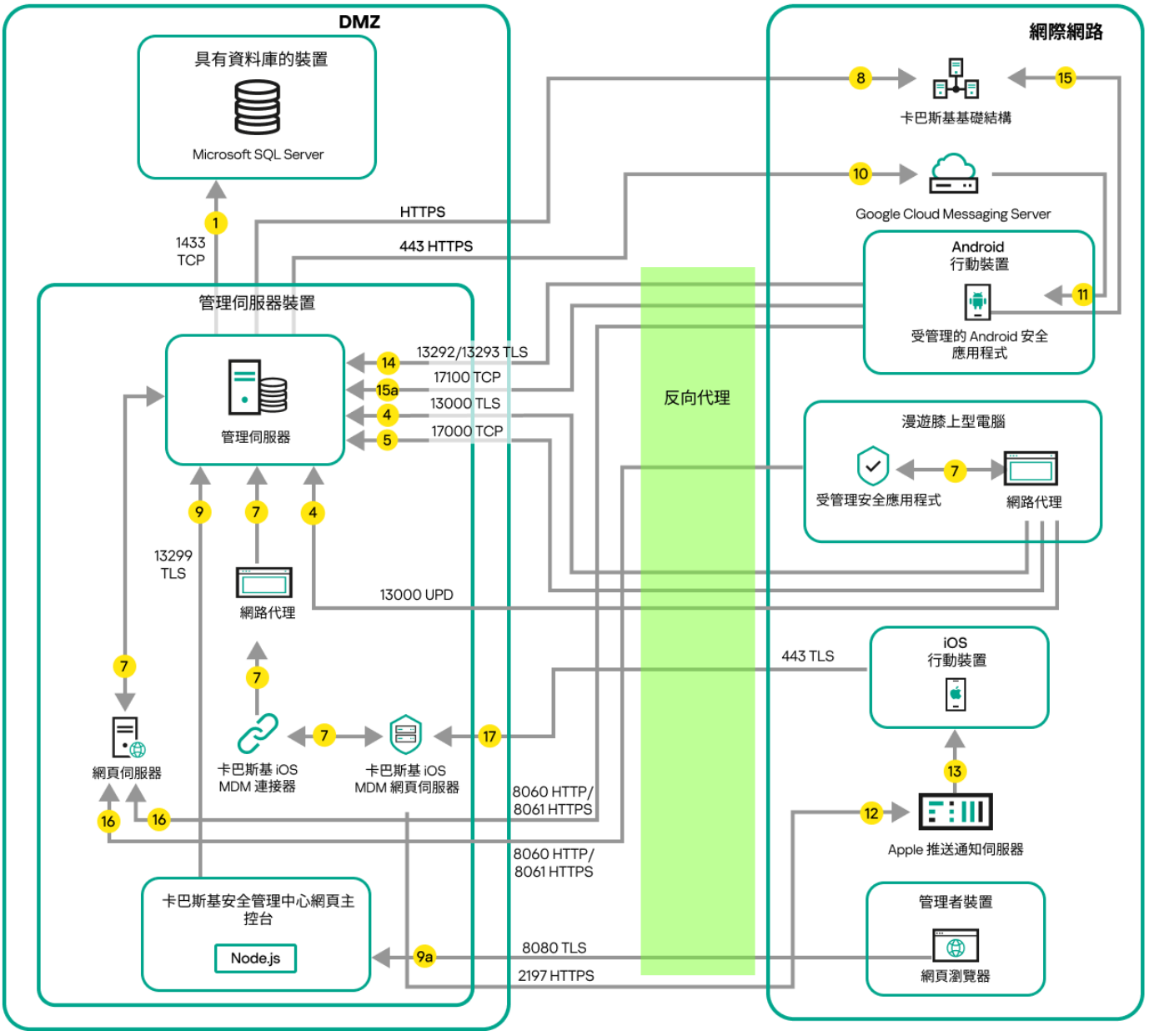
   如果您不想讓您的管理伺服器擁有網際網路連線，您必須手動管理該資料。

9. 卡巴斯基安全管理中心 網頁主控台伺服器透過 TLS 連接埠 13299 傳送資料到管理伺服器，該管理伺服器可能被安裝到相同或不同裝置。

   9a.來自 Web 瀏覽器（安裝在管理員的其他裝置）的流量透過 TLS 連接埠 8080 傳輸到卡巴斯基安全管理中心 網頁主控台伺服器。卡巴斯基安全管理中心 網頁主控台伺服器可以安裝到管理伺服器或其他裝置。

管理伺服器位於 LAN、受管理裝置位於網際網路、反向代理使用中

下圖顯示管理伺服器處於區域網路中且受管理裝置（包括行動裝置）都在網際網路中時的資料流量。在此圖中，您選擇的反向代理正在使用中。請參考應應用程式的文件瞭解詳情。



管理伺服器位於區域網路；受管理裝置透過反向代理連線到管理伺服器

如果您不想讓行動裝置直接連線到管理伺服器，且不想在 DMZ 中分配連線閘道器，則該佈署方案被建議。

箭頭表示流量的開始：每個箭頭從發起連線的裝置指向"回答"請求的裝置。連接埠號和用於資料傳輸的協定名稱被提供。每個箭頭都有數字標籤，對應的資料流量詳情是：

1. 管理伺服器傳送資料到資料庫。如果您安裝管理伺服器和資料庫到不同裝置，您必須使資料庫所在裝置的必要連接埠可用（例如，連接埠 3306 用於 MySQL 伺服器，或連接埠 1433 用於 Microsoft SQL Server）。請參閱 DBMS 文件以取得相關資訊。

2. 來自管理伺服器的通信請求被傳輸到所有非行動受管理裝置，透過 UDP 連接埠 15000。

   網路代理會在一個廣播網域中傳送要求給彼此。資料之後會傳送至管理伺服器並用來定義廣播網域的限制，以及發佈點的自動分配（若已啟用此選項）。

   如果管理伺服器無法直接存取受管理裝置，則不會直接傳送從管理伺服器到這些裝置的通信請求。

3. 受管理裝置關閉的資訊透過 UDP 連接埠 13000 被從網路代理傳輸到管理伺服器。

4. 管理伺服器透過 TLS 連接埠 13000 從網路代理和從屬管理伺服器接收連線。

   如果您使用卡巴斯基安全管理中心的早期版本，您網路中的管理伺服器可以透過非 TLS 連接埠 14000 從網路代理接收連線。卡巴斯基安全管理中心也支援透過連接埠 14000 連線網路代理，儘管使用 TLS 連接埠 13000 是被建議的。

   > 發佈點在早期卡巴斯基安全管理中心版本中被叫做更新代理。

5. 受管理裝置（除了行動裝置）透過 TCP 連接埠 17000 請求啟動。如果裝置自己擁有網際網路連線，則不必要；此種情況下，裝置直接透過網際網路傳送資料到 Kaspersky 伺服器。

6. 基於 MMC 的管理主控台透過連接埠 13291 傳送資料到管理伺服器。（管理主控台可以安裝在相同或不同裝置。）

7. 單一裝置交換本機流量的應用程式（在管理伺服器或受管理裝置之一）。不需要開啟任何外部連接埠。

8. 從管理伺服器到 Kaspersky 伺服器的資料（例如 KSN 資料或產品授權資訊）和從 Kaspersky 伺服器到管理伺服器的資料（例如應用程式更新和病毒資料庫更新）使用 HTTPS 協定傳輸。

   如果您不想讓您的管理伺服器擁有網際網路連線，您必須手動管理該資料。

9. 卡巴斯基安全管理中心 網頁主控台伺服器透過 TLS 連接埠 13299 傳送資料到管理伺服器，該管理伺服器可能被安裝到相同或不同裝置。

   9a.來自 Web 瀏覽器（安裝在管理員的其他裝置）的流量透過 TLS 連接埠 8080 傳輸到卡巴斯基安全管理中心 網頁主控台伺服器。卡巴斯基安全管理中心 網頁主控台伺服器可以安裝到管理伺服器或其他裝置。

10. 僅對 Android 行動裝置：來自管理伺服器的資料被傳輸到 Google 伺服器。該連線用於通知 Android 行動裝置他們需要連線到管理伺服器。然後推送通知被傳送到行動裝置。

11. 僅對 Android 行動裝置：來自 Google 伺服器的推送通知被傳送到行動裝置。該連線用於通知行動裝置他們需要連線到管理伺服器。

12. 僅對 iOS 行動裝置：來自 iOS MDM 伺服器的資料被傳送到 Apple 推送通知伺服器。然後推送通知被傳送到行動裝置。

13. 僅對 iOS 行動裝置：推送通知從 App 伺服器被傳送到行動裝置。該連線用於通知 iOS 行動裝置他們需要連線到管理伺服器。

14. 僅對行動裝置：來自受管理應用程式的資料透過 TLS 連接埠 13292 / 13293 被傳輸到管理伺服器（或連線閘道器）— 直接或透過反向代理。

15. 僅對行動裝置：來自行動裝置的資料被傳輸到 Kaspersky 基礎架構。

    如果行動裝置沒有網際網路存取，資料透過連接埠 17100 傳送到管理伺服器，然後管理伺服器將其傳送到 Kaspersky 基礎架構；然而，該方案很少被套用。

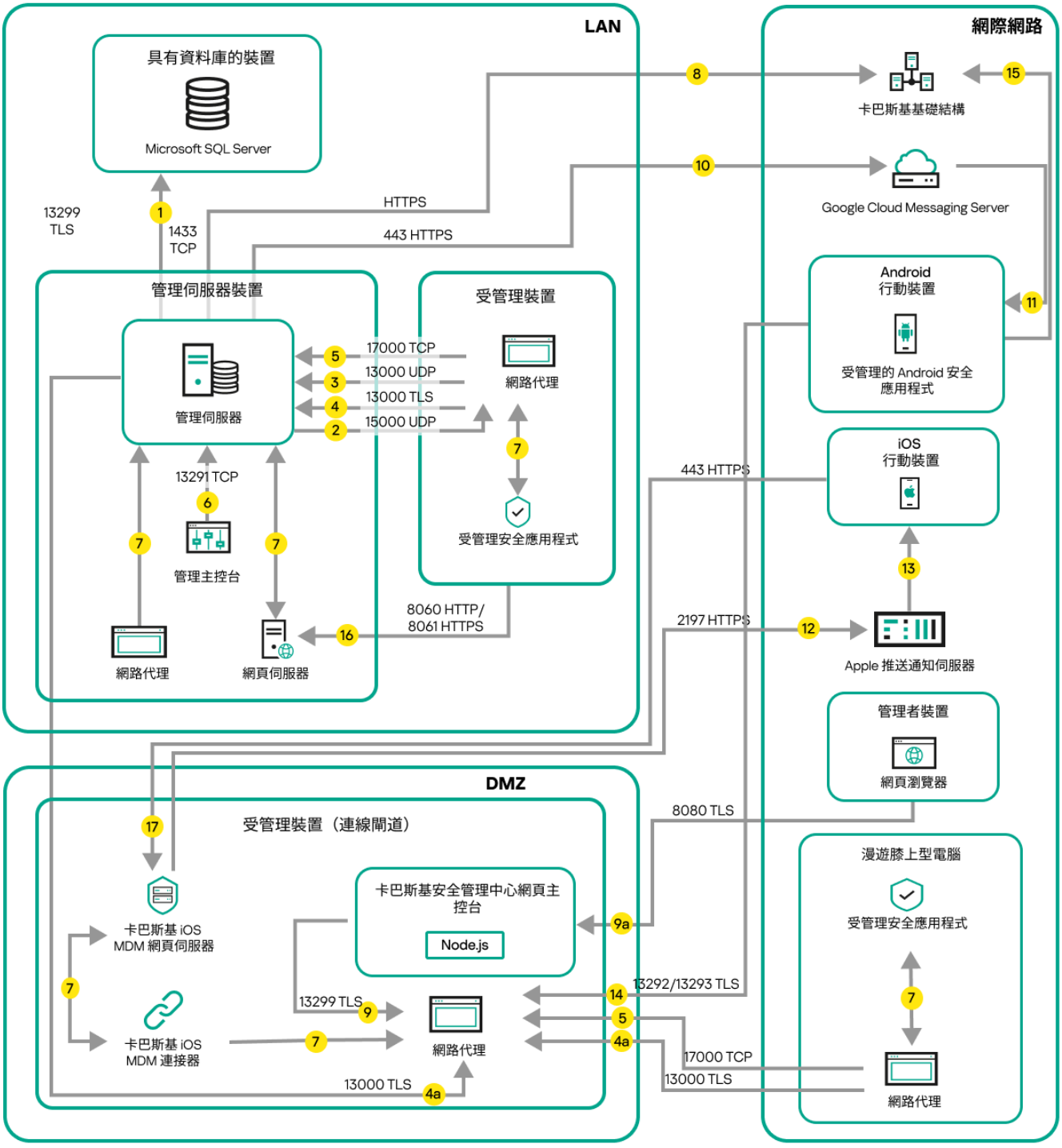
16. 來自受管理裝置，包括行動裝置的包請求被傳輸到 Web 伺服器，該伺服器位於管理伺服器所在裝置。

17. 僅對 iOS 行動裝置：來自行動裝置的資料透過 TLS 連接埠 443 傳輸到 iOS MDM 伺服器，該伺服器位於管理伺服器裝置或連線閘道。

管理伺服器位於 LAN、受管理裝置位於網際網路、連線閘道器使用中

下圖顯示管理伺服器處於區域網路中且受管理裝置（包括行動裝置）都在網際網路中時的資料流量。連線閘道使用中。

如果您不想讓行動裝置直接連線到管理伺服器，且不想使用反向代理或企業防火牆，則建議該佈署方案。



受管理行動裝置透過連線閘道器連線到管理伺服器

在該圖中，受管理裝置透過 DMZ 中的連線閘道器連線到管理伺服器。未使用反向代理或企業防火牆。

箭頭表示流量的開始：每個箭頭從發起連線的裝置指向"回答"請求的裝置。連接埠號和用於資料傳輸的協定名稱被提供。每個箭頭都有數字標籤，對應的資料流量詳情是：

1. 管理伺服器傳送資料到資料庫。如果您安裝管理伺服器和資料庫到不同裝置，您必須使資料庫所在裝置的必要連接埠可用（例如，連接埠 3306 用於 MySQL 伺服器，或連接埠 1433 用於 Microsoft SQL Server）。請參閱 DBMS 文件以取得相關資訊。

2. 來自管理伺服器的通信請求被傳輸到所有非行動受管理裝置，透過 UDP 連接埠 15000。

   網路代理會在一個廣播網域中傳送要求給彼此。資料之後會傳送至管理伺服器並用來定義廣播網域的限制，以及發佈點的自動分配（若已啟用此選項）。

   如果管理伺服器無法直接存取受管理裝置，則不會直接傳送從管理伺服器到這些裝置的通信請求。

3. 受管理裝置關閉的資訊透過 UDP 連接埠 13000 被從網路代理傳輸到管理伺服器。

4. 管理伺服器透過 TLS 連接埠 13000 從網路代理和從屬管理伺服器接收連線。

   如果您使用卡巴斯基安全管理中心的早期版本，您網路中的管理伺服器可以透過非 TLS 連接埠 14000 從網路代理接收連線。卡巴斯基安全管理中心也支援透過連接埠 14000 連線網路代理，儘管使用 TLS 連接埠 13000 是被建議的。

   > 發佈點在早期卡巴斯基安全管理中心版本中被叫做更新代理。

   4a.如果 DMZ 中有一個連線閘道，則此連線閘道還會透過 TLS 連接埠 13000 從管理伺服器接收連線。由於 DMZ 中的連線閘道無法存取管理伺服器的連接埠，因此管理伺服器會建立並維護與連線閘道的永久訊號連線。訊號連線不會用於資料傳輸，僅會用於向網路互動傳送邀請。當連線閘道需要連線到伺服器時，它將透過此訊號連線通知伺服器，然後伺服器建立資料傳輸所需的連線。

   漫遊裝置也會透過 TLS 連接埠 13000 連線到連線閘道。

5. 受管理裝置（除了行動裝置）透過 TCP 連接埠 17000 請求啟動。如果裝置自己擁有網際網路連線，則不必要；此種情況下，裝置直接透過網際網路傳送資料到 Kaspersky 伺服器。

6. 基於 MMC 的管理主控台透過連接埠 13291 傳送資料到管理伺服器。（管理主控台可以安裝在相同或不同裝置。）

7. 單一裝置交換本機流量的應用程式（在管理伺服器或受管理裝置之一）。不需要開啟任何外部連接埠。

8. 從管理伺服器到 Kaspersky 伺服器的資料（例如 KSN 資料或產品授權資訊）和從 Kaspersky 伺服器到管理伺服器的資料（例如應用程式更新和病毒資料庫更新）使用 HTTPS 協定傳輸。

   如果您不想讓您的管理伺服器擁有網際網路連線，您必須手動管理該資料。

9. 卡巴斯基安全管理中心 網頁主控台伺服器透過 TLS 連接埠 13299 傳送資料到管理伺服器，該管理伺服器可能被安裝到相同或不同裝置。

   9a.來自 Web 瀏覽器（安裝在管理員的其他裝置）的流量透過 TLS 連接埠 8080 傳輸到卡巴斯基安全管理中心 網頁主控台伺服器。卡巴斯基安全管理中心 網頁主控台伺服器可以安裝到管理伺服器或其他裝置。

10. 僅對 Android 行動裝置：來自管理伺服器的資料被傳輸到 Google 伺服器。該連線用於通知 Android 行動裝置他們需要連線到管理伺服器。然後推送通知被傳送到行動裝置。

11. 僅對 Android 行動裝置：來自 Google 伺服器的推送通知被傳送到行動裝置。該連線用於通知行動裝置他們需要連線到管理伺服器。

12. 僅對 iOS 行動裝置：來自 iOS MDM 伺服器的資料被傳送到 Apple 推送通知伺服器。然後推送通知被傳送到行動裝置。

13. 僅對 iOS 行動裝置：推送通知從 App 伺服器被傳送到行動裝置。該連線用於通知 iOS 行動裝置他們需要連線到管理伺服器。

14. 僅對行動裝置：來自受管理應用程式的資料透過 TLS 連接埠 13292 / 13293 被傳輸到管理伺服器（或連線閘道器）— 直接或透過反向代理。

15. 僅對行動裝置：來自行動裝置的資料被傳輸到 Kaspersky 基礎架構。

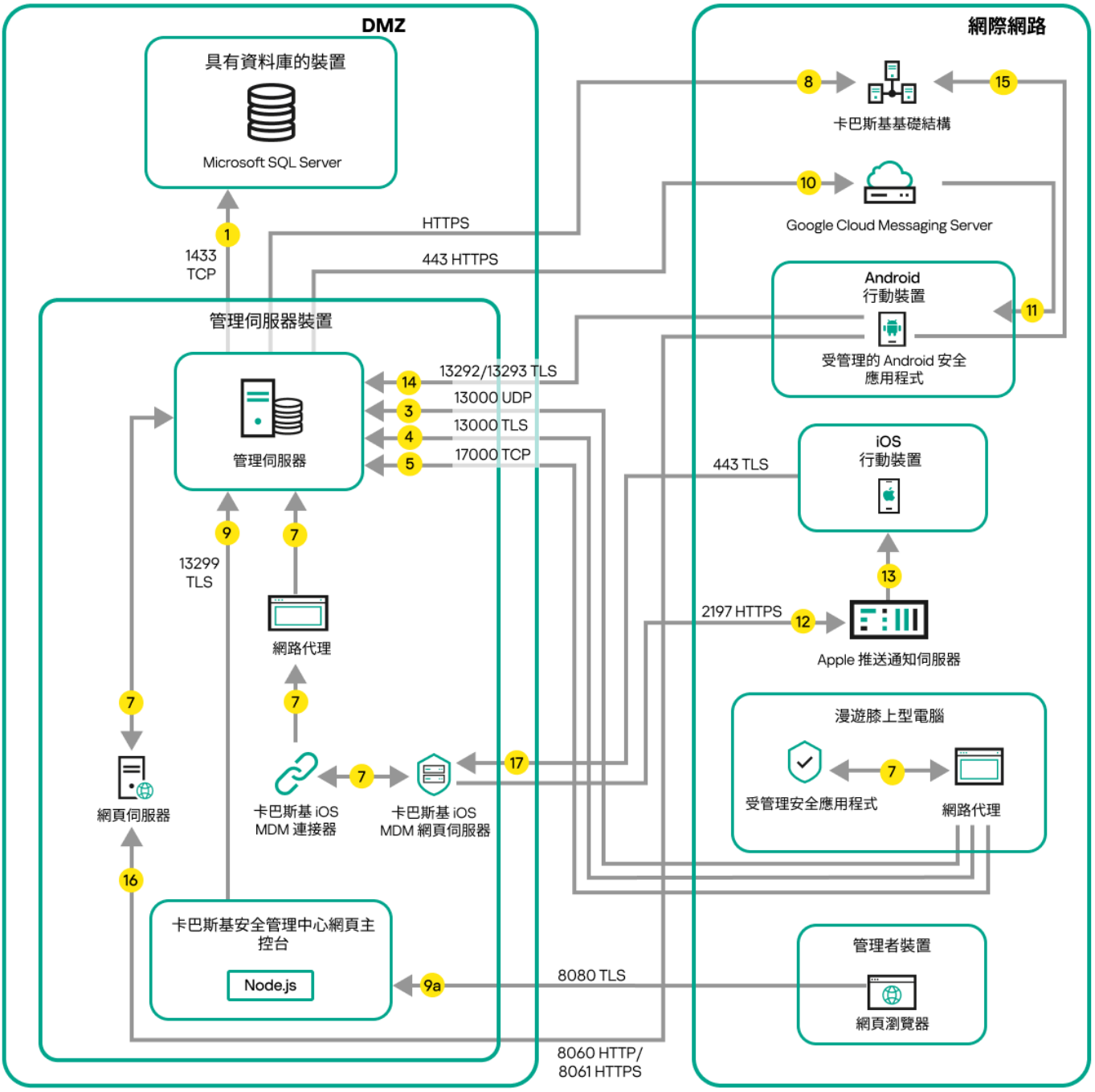
    如果行動裝置沒有網際網路存取，資料透過連接埠 17100 傳送到管理伺服器，然後管理伺服器將其傳送到 Kaspersky 基礎架構；然而，該方案很少被套用。

16. 來自受管理裝置，包括行動裝置的包請求被傳輸到 Web 伺服器，該伺服器位於管理伺服器所在裝置。

17. 僅對 iOS 行動裝置：來自行動裝置的資料透過 TLS 連接埠 443 傳輸到 iOS MDM 伺服器，該伺服器位於管理伺服器裝置或連線閘道。

管理伺服器位於 DMZ、受管理裝置位於網際網路

下圖顯示管理伺服器處於 DMZ 中且受管理裝置，包括行動裝置，都在網際網路中時的資料流量。



管理伺服器位於 DMZ、受管理行動裝置位於網際網路

在該影像中，未使用連線閘道器：行動裝置直接連線到管理伺服器。

箭頭表示流量的開始：每個箭頭從發起連線的裝置指向"回答"請求的裝置。連接埠號和用於資料傳輸的協定名稱被提供。每個箭頭都有數字標籤，對應的資料流量詳情是：

1. 管理伺服器傳送資料到資料庫。如果您安裝管理伺服器和資料庫到不同裝置，您必須使資料庫所在裝置的必要連接埠可用（例如，連接埠 3306 用於 MySQL 伺服器，或連接埠 1433 用於 Microsoft SQL Server）。請參閱 DBMS 文件以取得相關資訊。

2. 來自管理伺服器的通信請求被傳輸到所有非行動受管理裝置，透過 UDP 連接埠 15000。

   網路代理會在一個廣播網域中傳送要求給彼此。資料之後會傳送至管理伺服器並用來定義廣播網域的限制，以及發佈點的自動分配（若已啟用此選項）。

   如果管理伺服器無法直接存取受管理裝置，則不會直接傳送從管理伺服器到這些裝置的通信請求。

3. 受管理裝置關閉的資訊透過 UDP 連接埠 13000 被從網路代理傳輸到管理伺服器。

4. 管理伺服器透過 TLS 連接埠 13000 從網路代理和從屬管理伺服器接收連線。

   如果您使用卡巴斯基安全管理中心的早期版本，您網路中的管理伺服器可以透過非 TLS 連接埠 14000 從網路代理接收連線。卡巴斯基安全管理中心也支援透過連接埠 14000 連線網路代理，儘管使用 TLS 連接埠 13000 是被建議的。

   > 發佈點在早期卡巴斯基安全管理中心版本中被叫做更新代理。

5. 受管理裝置（除了行動裝置）透過 TCP 連接埠 17000 請求啟動。如果裝置自己擁有網際網路連線，則不必要；此種情況下，裝置直接透過網際網路傳送資料到 Kaspersky 伺服器。

6. 基於 MMC 的管理主控台透過連接埠 13291 傳送資料到管理伺服器。（管理主控台可以安裝在相同或不同裝置。）

7. 單一裝置交換本機流量的應用程式（在管理伺服器或受管理裝置之一）。不需要開啟任何外部連接埠。

8. 從管理伺服器到 Kaspersky 伺服器的資料（例如 KSN 資料或產品授權資訊）和從 Kaspersky 伺服器到管理伺服器的資料（例如應用程式更新和病毒資料庫更新）使用 HTTPS 協定傳輸。

   如果您不想讓您的管理伺服器擁有網際網路連線，您必須手動管理該資料。

9. 卡巴斯基安全管理中心 網頁主控台伺服器透過 TLS 連接埠 13299 傳送資料到管理伺服器，該管理伺服器可能被安裝到相同或不同裝置。

   9a.來自 Web 瀏覽器（安裝在管理員的其他裝置）的流量透過 TLS 連接埠 8080 傳輸到卡巴斯基安全管理中心 網頁主控台伺服器。卡巴斯基安全管理中心 網頁主控台伺服器可以安裝到管理伺服器或其他裝置。

10. 僅對 Android 行動裝置：來自管理伺服器的資料被傳輸到 Google 伺服器。該連線用於通知 Android 行動裝置他們需要連線到管理伺服器。然後推送通知被傳送到行動裝置。

11. 僅對 Android 行動裝置：來自 Google 伺服器的推送通知被傳送到行動裝置。該連線用於通知行動裝置他們需要連線到管理伺服器。

12. 僅對 iOS 行動裝置：來自 iOS MDM 伺服器的資料被傳送到 Apple 推送通知伺服器。然後推送通知被傳送到行動裝置。

13. 僅對 iOS 行動裝置：推送通知從 App 伺服器被傳送到行動裝置。該連線用於通知 iOS 行動裝置他們需要連線到管理伺服器。

14. 僅對行動裝置：來自受管理應用程式的資料透過 TLS 連接埠 13292 / 13293 被傳輸到管理伺服器（或連線閘道器）— 直接或透過反向代理。

15. 僅對行動裝置：來自行動裝置的資料被傳輸到 Kaspersky 基礎架構。

    如果行動裝置沒有網際網路存取，資料透過連接埠 17100 傳送到管理伺服器，然後管理伺服器將其傳送到 Kaspersky 基礎架構；然而，該方案很少被套用。

16. 來自受管理裝置，包括行動裝置的包請求被傳輸到 Web 伺服器，該伺服器位於管理伺服器所在裝置。

17. 僅對 iOS 行動裝置：來自行動裝置的資料透過 TLS 連接埠 443 傳輸到 iOS MDM 伺服器，該伺服器位於管理伺服器裝置或連線閘道。

與卡巴斯基安全管理中心元件和安全應用程式的互動：更多資訊

該部分提供了與卡巴斯基安全管理中心元件和受管理安全應用程式互動的方案。方案提供了必須可用的埠號和開啟這些連接埠的處理程序名稱。

互動模式中的慣例

下表提供了方案中使用的轉換。

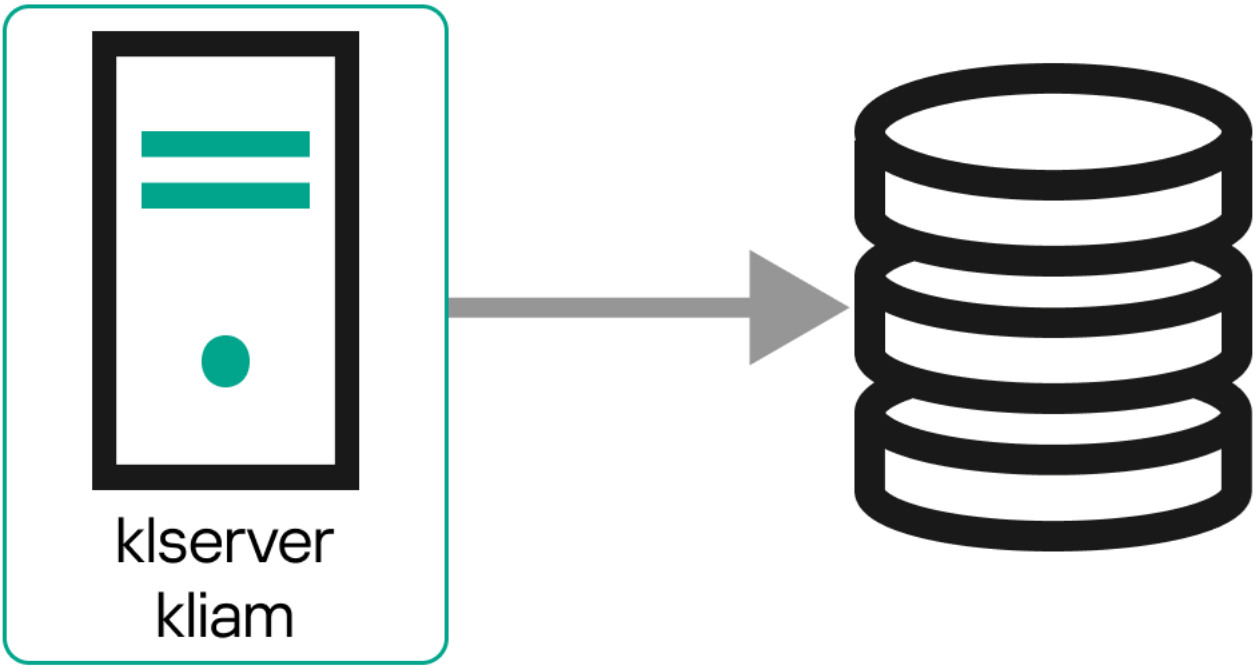
文件說明

圖示	含義
	管理伺服器
	從屬管理伺服器
	DBMS
	用戶端裝置（安裝了網路代理和 Kaspersky Endpoint Security 系列應用程式，或卡巴斯基安全管理中心可以管理的其他應用程式）
	連線閘道
	發佈點
	安裝了 Kaspersky Security for Mobile 的行動用戶端裝置

	使用者裝置上的瀏覽器
	執行在裝置和開啟連接埠的處理程序
	連接埠和其號碼
	TCP 流量（箭頭方向顯示流量方向）
	UDP 流量（箭頭方向顯示流量方向）
	COM 調用
	DBMS 傳輸
	DMZ 邊界

管理伺服器和 DBMS

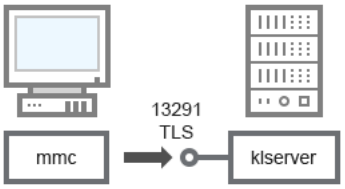
管理伺服器資料登入 SQL Server、MySQL 或 MariaDB 資料庫。



管理伺服器和 DBMS

如果您安裝管理伺服器和資料庫到不同裝置，您必須使資料庫所在裝置的必要連接埠可用（例如，連接埠 3306 用於 MySQL 伺服器，或連接埠 1433 用於 Microsoft SQL Server）。請參閱 DBMS 文件以取得相關資訊。

管理伺服器和管理主控台



管理伺服器和管理主控台

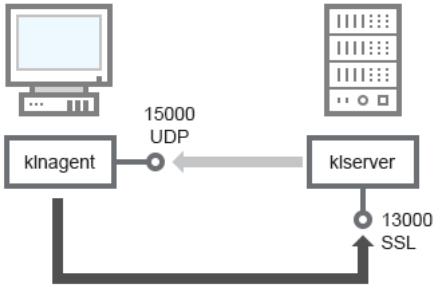
對於方法敘述，參見下表。

管理伺服器和管理主控台（流量）

裝置	埠號	開啟連接埠的處理程序名稱	協定	TLS	連接埠目的
管理伺服器	13291	klserver	TCP	是	從管理主控台接收連線

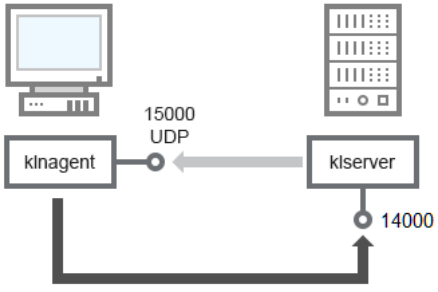
管理伺服器和用戶端裝置：管理安全應用程式

管理伺服器透過 SSL 連接埠 13000 從網路代理接收連線（參見下圖）。



管理伺服器和用戶端裝置：管理安全應用程式、透過連接埠 13000 連線（建議）

如果您使用卡巴斯基安全管理中心的早期版本，您網路中的管理伺服器可以透過非 SSL 連接埠 14000 從網路代理接收連線（參見下圖）。卡巴斯基安全管理中心 14.2 也支援透過連接埠 14000 連線網路代理，儘管使用 SSL 連接埠 13000 是被建議的。



管理伺服器和用戶端裝置：管理安全應用程式、透過連接埠 14000 連線（低安全級）

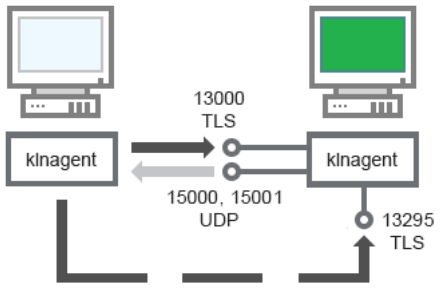
為了澄清方案，參見下圖。

管理伺服器和用戶端裝置：管理安全應用程式（流量）

裝置	埠號	開啟連接埠的處理程序名稱	協定	TLS（僅對 TCP）	連接埠目的
網路代理	15000	klnagent	UDP	Null	網路代理多點傳送
管理伺服器	13000	klserver	TCP	是	接收從網路代理的連線
管理伺服器	14000	klserver	TCP	否	接收從網路代理的連線

透過發佈點在用戶端裝置上升級軟體

用戶端裝置透過連接埠 13000 連線到發佈點，如果您將發佈點作為推送伺服器，也透過連接埠 13295；發佈點會透過連接埠 15000 多點傳送到網路代理（見下圖）。更新和安裝套件通過連接埠 15001 從發佈點接收。



透過發佈點在用戶端裝置上升級軟體

對於方法敘述，參見下表。

透過發佈點升級軟體（流量）

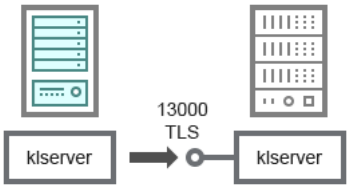
裝置	埠號	開啟連接埠的處理程序名稱	協定	TLS（僅對 TCP）	連接埠目的
網路代理	15000	klnagent	UDP	Null	網路代理多點傳送
網路代理	15001	klnagent	UDP	Null	從發佈點接收更新和安裝套件
發佈點	13000	klnagent	TCP	是	接收從網路代理的連線
發佈點	13295	klnagent	TCP	是	接收來自用戶端裝置的連線（伺服器推送）

管理伺服器階層：主管理伺服器和從屬管理伺服器

方案（參見下圖）顯示了如何使用連接埠 13000 確保層級中管理伺服器之間的互動。

當組合兩個管理伺服器到一個層級，確保連接埠 13291 在兩個管理伺服器上都可以存取。透過連接埠 13291 連線管理主控台到管理伺服器。

此後，當管理伺服器組合到層級時，您將可以使用連線到主管理伺服器的管理主控台管理兩個管理伺服器。因此，主管理伺服器連接埠 13291 的可存取性是僅有的前提。



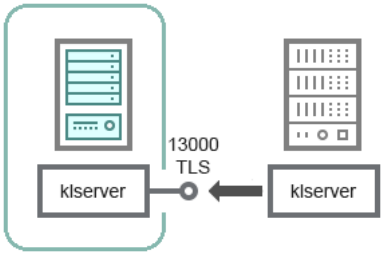
管理伺服器階層：主管理伺服器和從屬管理伺服器

對於方法敘述，參見下表。

管理伺服器階層（流量）

裝置	埠號	開啟連接埠的處理程序名稱	協定	TLS	連接埠目的
主管理伺服器	13000	klserver	TCP	是	從從屬管理伺服器接收連線

DMZ 中帶有從屬管理伺服器的管理伺服器階層



DMZ 中帶有從屬管理伺服器的管理伺服器階層

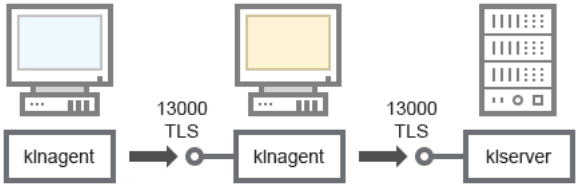
方案顯示了管理伺服器階層，其中 DMZ 中的從屬管理伺服器從主管理伺服器接收連線（請參閱下表）。當組合兩個管理伺服器到一個層級，確保連接埠 13291 在兩個管理伺服器上都可以存取。透過連接埠 13291 連線管理主控台到管理伺服器。

此後，當管理伺服器組合到層級時，您將可以使用連線到主管理伺服器的管理主控台管理兩個管理伺服器。因此，主管理伺服器連接埠 13291 的可存取性是僅有的前提。

DMZ 中帶有從屬管理伺服器的管理伺服器階層（流量）

裝置	埠號	開啟連接埠的處理程序名稱	協定	TLS	連接埠目的
從屬管理伺服器	13000	klserver	TCP	是	從主管理伺服器接收連線

管理伺服器、網段連線閘道和用戶端裝置



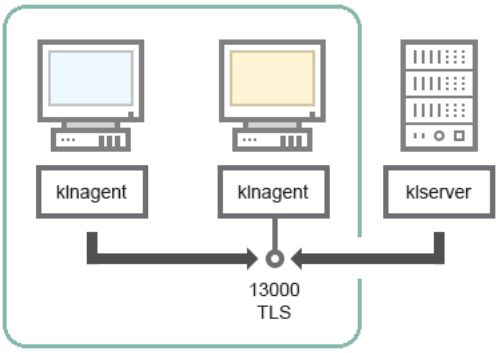
管理伺服器、網段連線閘道和用戶端裝置

對於方法敘述，參見下表。

管理伺服器、網段連線閘道和用戶端裝置（流量）

裝置	埠號	開啟連接埠的處理程序名稱	協定	TLS	連接埠目的
管理伺服器	13000	klserver	TCP	是	接收從網路代理的連線
網路代理	13000	klnagent	TCP	是	接收從網路代理的連線

管理伺服器和 DMZ 中的兩台裝置：連線閘道和用戶端裝置



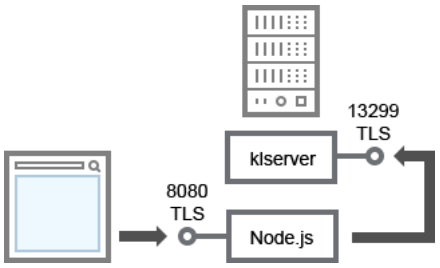
帶有連線閘道的管理伺服器和 DMZ 中的用戶端裝置

對於方法敘述，參見下表。

帶有網段連線閘道的管理伺服器和用戶端裝置（流量）

裝置	埠號	開啟連接埠的處理程序名稱	協定	TLS	連接埠目的
網路代理	13000	klnagent	TCP	是	接收從網路代理的連線

管理伺服器和卡巴斯基安全管理中心網頁主控台



管理伺服器和卡巴斯基安全管理中心 網頁主控台

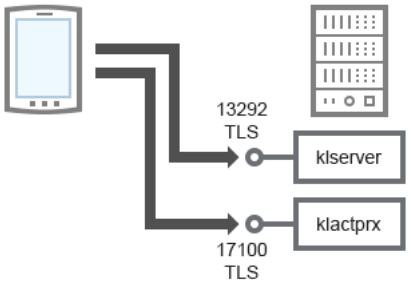
對於方法敘述，參見下表。

管理伺服器和卡巴斯基安全管理中心 網頁主控台（流量）

裝置	埠號	開啟連接埠的處理程序名稱	協定	TLS	連接埠目的
管理伺服器	13299	klserver	TCP	是	接收透過 OpenAPI 從卡巴斯基安全管理中心 網頁主控台到管理伺服器的連線
卡巴斯基安全管理中心 網頁主控台伺服器或管理伺服器	8080	Node.js：伺服器端 JavaScript	TCP	是	從卡巴斯基安全管理中心 網頁主控台接收連線

卡巴斯基安全管理中心 網頁主控台可以安裝到管理伺服器或其他裝置。

啟動和管理行動裝置上的安全應用程式



啟動和管理行動裝置上的安全應用程式

對於方法敘述，參見下表。

啟動和管理行動裝置上的安全應用程式（流量）

裝置	埠號	開啟連接埠的處理程序名稱	協定	TLS	連接埠目的
管理伺服器	13292	klserver	TCP	是	接收從管理主控台到管理伺服器的連線
管理伺服器	17100	klactprx	TCP	是	接收從行動裝置的應用程式啟動連線

佈署最佳實踐

卡巴斯基安全管理中心是一個分發的應用程式。卡巴斯基安全管理中心包含以下應用程式：

- 管理伺服器 — 核心元件，設計用於管理組織裝置和在 DBMS 中整理資料。
- 管理主控台 — 管理員基本工具。管理主控台與管理伺服器一起出貨，但是它也可以被單獨安裝在一個或幾個由管理員執行的裝置上。
- 網路代理 — 設計用於管理安裝在裝置上的安全應用程式，同時取得裝置資訊並傳輸該資訊到管理伺服器。網路代理安裝在組織裝置上。

卡巴斯基安全管理中心在組織網路上的佈署執行如下：

- 管理伺服器的安裝
- 管理員裝置上管理主控台的安裝
- 網路代理和企業裝置上安全應用程式的安裝

硬化指南

卡巴斯基安全管理中心是設計用來在區域網路中集中執行基本的管理和維護工作。該應用程式使管理員可以存取有關組織網路安全級別的詳細資訊。卡巴斯基安全管理中心允許您配置使用卡巴斯基應用程式構建的所有防護元件。

卡巴斯基安全管理中心管理伺服器擁有對用戶端裝置防護管理的完全存取權限，是組織安全系統中最重要的元件。因此，管理伺服器需要增加防護方法。

在設定之前，請使用管理伺服器資料備份工作或 klbackup 公用程式建立卡巴斯基安全管理中心管理伺服器備份副本並將其儲存在安全位置。

硬化指南描述了配置卡巴斯基安全管理中心及其元件的建議和功能，旨在降低其危害的風險。

硬化指南包含以下資訊：

- 選擇管理伺服器架構
- 設定與管理伺服器的安全連線
- 設定帳戶來存取管理伺服器
- 對管理伺服器防護的管理
- 管理用戶端裝置防護
- 配置受管理應用程式的防護
- 管理伺服器維護
- 將資訊傳輸到協力廠商應用程式
- 第三方資訊系統安全建議

管理伺服器佈署

管理伺服器架構

一般來說，集中式管理架構的選擇取決於受防護裝置的位置、相鄰網路的存取、資料庫更新的交付方案等。

在架構開發的初始階段，我們建議熟悉卡巴斯基安全管理中心元件和他們之間的互動，以及資料流量和連接埠使用方案。

基於此資訊，您可以形成一個架構，指定：

- 管理伺服器位置和網路連線
- 管理員工作區的組織和連線到管理伺服器的方法
- 網路代理及防護軟體的佈署方法
- 使用發佈點
- 使用虛擬管理伺服器
- 使用管理伺服器階層

- 病毒資料庫更新方案
- 其他資訊流

為管理伺服器安裝選擇裝置

我們建議您在組織基礎結構中的專用伺服器上安裝管理伺服器。如果伺服器上沒有安裝其他協力廠商軟體，您可以根據卡巴斯基安全管理中心的要求配置安全設定，無需依賴協力廠商軟體的要求。

您可以在物理伺服器或虛擬伺服器上佈署管理伺服器。請確保選定裝置滿足硬體和軟體要求。

管理伺服器地點

由管理伺服器管理的裝置可以位於如下位置：

- 在區域網路 (LAN) 上
- 在網際網路上
- 在隔離區域 (DMZ)

同時，管理伺服器也可以位於不同的區隔：工業區隔、企業區隔和 DMZ 區隔。

如果您使用卡巴斯基安全管理中心來管理隔離網段的防護，我們建議將管理伺服器佈署在隔離區域 (DMZ) 的一個區隔中。這使您可以組織適當的網路分段並最大程度地減少流向受防護分段的流量，同時保持完整的管理功能和更新交付。

限制在網域控制器、終端伺服器或使用者裝置上佈署管理伺服器

我們強烈不建議在網域控制器、終端伺服器或使用者裝置上安裝管理伺服器。

我們建議您提供網路關鍵節點的功能分離。這種方法允許您在節點出現故障或受到危害時保持不同系統的可操作性。同時，您可以為每個節點建立不同的安全政策。

例如，通常套用於網域控制器的安全限制會顯著降低管理伺服器的效能，並導致無法使用管理伺服器的某些功能。如果入侵者獲得對網域控制器的特權存取，Active Directory 網域服務 (AD DS) 資料庫可以被修改、損壞或銷毀。此外，所有由 Active Directory 管理的系統和帳戶都可能受到危害。

用於安裝和執行管理伺服器的帳戶

我們建議在本機管理員帳戶下執行管理伺服器安裝，以避免使用域帳戶存取管理伺服器資料庫。所需帳戶及其權限集合取決於所選的 DBMS 類型、DBMS 位置和管理伺服器資料庫建立方法。

在安裝卡巴斯基安全管理中心期間，程式將自動建立 KLAdmins 和 KLOperators 群組。這些群組被授予連線至管理伺服器和處理管理伺服器物件的權限。

依據安裝卡巴斯基安全管理中心時使用的帳戶類型，系統會建立如下所示的 KLAdmins 和 KLOperators 群組：

- 如果應用程式是在網域內包含的使用者帳戶下安裝的，則系統會在包含管理伺服器的網域內和管理伺服器上同時建立這些群組。
- 如果應用程式是在系統帳戶下安裝的，則系統僅會在管理伺服器裝置上建立這些群組。

為了避免在網域中建立 KLAdmins 和 KLOperators 群組並因此**向管理伺服器裝置外的帳戶提供管理管理伺服器的權限**，我們建議在本機帳戶下安裝卡巴斯基安全管理中心。

在管理伺服器安裝期間，選取用於啟動管理伺服器作為服務的帳戶。預設情況下，應用程式會建立一個名為 KL-AK-* 的本機帳戶，管理伺服器服務（klserver 服務）將在該帳戶下執行。

如有必要，管理伺服器服務可以在所選帳戶下執行。此帳戶必須被授予存取 DBMS 所需的權限。出於安全原因，請使用非特權帳戶來執行管理伺服器服務。

為避免使用不正確的帳戶設定，我們建議自動產生賬戶。

從網域中排除管理伺服器

如果您使用管理伺服器來防護高重要性係統的裝置群組，我們不建議將管理伺服器裝置包含在網域中。這可讓您區分卡巴斯基安全管理中心管理權限並防止在網域帳戶受到危害的情況下存取管理伺服器。

請考慮到，如果您在工作群組中包含的裝置上安裝管理伺服器，則以下使用管理伺服器的場景將無法使用：

- 使用卡巴斯基安全管理中心容錯移轉叢集
- 使用Windows Server 容錯移轉叢集
- 在單獨的裝置上使用 SQL Server for Windows

  只有當管理伺服器和 SQL Server 包含在同一個網域或者受信任網域中時，您才可以在單獨的裝置上使用 SQL Server for Windows。如果管理伺服器、SQL Server 和用於備份的 UNC 共用位於一個工作群組中，則無法在 SQL Server 和共用之間安全地設定存取和讀寫權限。
- 使用管理伺服器工具透過 Active Directory 群組政策遠端安裝

如果您需要斷開管理伺服器與 Active Directory 網域的連線，請按照下列主題中所述的步驟操作：如何變更卡巴斯基安全管理中心的名稱。

如果需要在工作群組中包含的裝置上安裝管理伺服器，您可以使用卡巴斯基安全管理中心 Linux 而不是卡巴斯基安全管理中心 Windows。

連線安全

TLS 的使用

我們建議禁止與管理伺服器的不安全連線。例如，您可以在管理伺服器設定中禁止使用 HTTP 的連線。

請注意，預設情況下，管理伺服器的幾個 HTTP 連接埠是關閉的。其餘連接埠用於管理伺服器 Web 伺服器 (8060)。此連接埠可能受管理伺服器裝置的防火牆設定限制。

嚴格的 TLS 設定

建議使用 1.2 及以後版本的 TLS 協定，限製或禁止不安全的加密演算法。

您可以設定管理伺服器使用的加密協定 (TLS)。請注意，在發布管理伺服器版本時，加密協定設定會得到預設配置以確保安全的資料傳輸。

禁止使用 Windows 帳戶進行遠端身分驗證

您可以使用 LP_RestrictRemoteOsAuth 標誌來禁止來自遠端位址的 SSPI 連線。此標誌允許您禁止使用本機或網域 Windows 帳戶在管理伺服器上進行遠端身分驗證。

將 LP_RestrictRemoteOsAuth 標誌切換為禁止來自遠端位址的連線模式：

1. 使用管理員權限執行 Windows 命令提示符，然後將目前目錄變更為包含 klscflag 公用程式的目錄。klscflag 公用程式位於安裝管理伺服器的資料夾中。預設安裝路徑：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
2. 在命令列中執行以下命令以指定 LP_RestrictRemoteOsAuth 標誌的值：

   ```
   klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_RestrictRemoteOsAuth -t d -v 1
   ```

3. 重新啟動管理伺服器服務。

如果通過安裝在管理伺服器裝置上的卡巴斯基安全管理中心網頁主控台或管理主控台執行遠端身分驗證，則 LP_RestrictRemoteOsAuth 標誌不起作用。

限制存取管理伺服器資料庫

我們建議限制存取管理伺服器資料庫。例如，只允許從管理伺服器裝置進行存取。這會降低管理伺服器資料庫因已知弱點而受到損害的可能性。

您可以根據所用資料庫的操作說明配置參數，也可以在防火牆上提供關閉的連接埠。

驗證 Microsoft SQL Server

如果卡巴斯基安全管理中心使用 Microsoft SQL Server 作為 DBMS，有必要防護傳輸到資料庫或從資料庫傳輸到的卡巴斯基安全管理中心資料以及儲存在資料庫中的資料免遭未經授權的存取。為此，您必須提供卡巴斯基安全管理中心和 SQL Server 之間的安全通信。提供安全通訊的最可靠方式是安裝卡巴斯基安全管理中心與 SQL Server 在相同的裝置並對這兩個應用程式使用共用的記憶體機制。在所有情況下，建議您使用 SSL/TLS 憑證來驗證 SQL Server 實例。

通常，管理伺服器可以透過下列提供者尋址 SQL Server：

- 使用 TCP/IP 或命名管道的 SQLOLEDB

  此提供者被安裝到 Windows 作業系統中並預設使用。

- 使用 TCP/IP、命名管道或共用記憶體的 MSOLEDBSQL

  如果想使用這個提供者，您必須將其安裝 在具有管理伺服器的裝置上，然後將全域環境變數 `KLDBADO_UseMSOLEDBSQL` 的值設為 `1`。

- 使用 TCP/IP、命名管道或共用記憶體的 MSOLEDBSQL19

  如果想使用這個提供者，您必須將其安裝 在具有管理伺服器的裝置上，然後將全域環境變數 `KLDBADO_UseMSOLEDBSQL` 的值設為 `1`，將全域環境變數 `KLDBADO_ProviderName` 的值設為 `MSOLEDBSQL19`。

此外，在使用 TCP/IP、命名管道或共用記憶體之前，請確保已啟用所需協定。

與外部 DBMS 的安全性互動

如果在安裝管理伺服器（外部 DBMS）期間在單獨的裝置上安裝 DBMS，我們建議設定參數以與此 DBMS 進行安全性互動和驗證。如需有關設定 SSL 驗證的更多資訊，請參閱驗證 PostgreSQL 伺服器和情境：驗證 MySQL 伺服器。

配置連線到管理伺服器的 IP 位址允許清單

預設情況下，卡巴斯基安全管理中心使用者可以從任何安裝了基於 MMC 的管理主控台、卡巴斯基安全管理中心網頁主控台或OpenAPI 應用程式的裝置登入卡巴斯基安全管理中心。您可以配置管理伺服器，以便使用者只能從具有允許 IP 位址的裝置連線到它。例如，如果入侵者嘗試透過安裝在未包含在允許清單中的裝置上的卡巴斯基安全管理中心網頁主控台伺服器連線到卡巴斯基安全管理中心，他或她將無法登入卡巴斯基安全管理中心。

設定連線到卡巴斯基安全管理中心網頁主控台的 IP 位址允許清單

預設情況下，卡巴斯基安全管理中心使用者可以從任何裝置連線到卡巴斯基安全管理中心網頁主控台。在安裝了卡巴斯基安全管理中心網頁主控台的裝置上，您必須設定防火牆（內建於作業系統或第三方防火牆中），以便操作員只能從允許的 IP 位址連線到卡巴斯基安全管理中心網頁主控台。

輪詢期間與網域控制器的連線安全性

管理伺服器或 Linux 發佈點透過 LDAPS 連線到網域控制器以輪詢網域。預設連線時不會要求執行憑證驗證。若要強制執行憑證驗證，請將 `KLNAG_LDAP_TLS_REQCERT` 標誌設為 1。此外，您可以使用 `KLNAG_LDAP_SSL_CACERT` 標誌指定憑證授權單位 (CA) 的自訂路徑來存取憑證鏈。

帳戶和身分驗證

在執行以下步驟之前，請使用管理伺服器資料備份工作或 klbackup 公用程式建立卡巴斯基安全管理中心管理伺服器備份副本並將其儲存在安全位置。

通過管理伺服器使用雙步驟驗證

卡巴斯基安全管理中心為卡巴斯基安全管理中心網頁主控台和管理主控台的使用者提供雙步驟驗證，基於 RFC 6238 標準（TOTP：基於時間的一次性密碼演算法）。

為帳戶啟用雙步驟驗證後，每次登入到卡巴斯基安全管理中心網頁主控台或管理主控台時，都將輸入使用者名稱、密碼和其他一次性安全碼。如果您對帳戶使用網域身分驗證，則只需輸入其他一次性使用的安全碼。若要接收一次性使用的安全碼，您必須在電腦或行動裝置上安裝身份驗證器應用程式。

有支援 RFC 6238 標準的軟體和硬體驗證器（權杖）。例如，軟體驗證器包括 Google Authenticator、Microsoft Authenticator、FreeOTP。

我們強烈建議不要在與管理伺服器建立連線的同一台裝置上安裝驗證器應用程式。您可以在行動裝置上安裝驗證器應用程式。

對作業系統使用雙重身分驗證

我們建議使用權杖、智慧卡或其他方法（如果可能）在管理伺服器裝置上用多重要素身分驗證 (MFA) 進行身分驗證。

禁止儲存管理員密碼

如果您使用管理主控台，我們不建議在管理伺服器連線對話方塊中儲存管理員密碼。

如果您使用卡巴斯基安全管理中心網頁主控台，我們不建議在使用者裝置上安裝的瀏覽器中儲存管理員密碼。

內部使用者帳戶的身分驗證

預設情況下，管理伺服器內部使用者帳戶的密碼必須遵守以下規則：

- 密碼必須是 8 到 256 位字元長度。
- 密碼必須包含以下組中三組的字元：
  - 大寫字母 (A-Z)
  - 小寫字母 (a-z)
  - 數字 (0-9)
  - 特殊字元 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- 密碼不可以包含任何空白、Unicode 字元或 "." 和「@」的組合，並且「@」前不可有「.」。

依預設，可輸入密碼的嘗試次數上限為 10 次。您可以變更允許的密碼輸入嘗試次數。

卡巴斯基安全管理中心使用者可以輸入無效的密碼有限次數。達到限制後，使用者帳戶被鎖定一小時。

管理伺服器的專用管理群組

我們建議為管理伺服器建立一個專門的管理群組。授予該群組特殊存取權限並為其建立特殊安全政策。

為避免故意降低管理伺服器的安全級別，我們建議限制可以管理專用管理群組的帳戶清單。

KLAdmins 和 KLOperators 群組

在安裝卡巴斯基安全管理中心期間，程式將自動建立 KLAdmins 和 KLOperators 群組。KLAdmins 群組被授予所有存取權限。KLOperators 群組僅被授予讀取和執行權限。授予 KLAdmins 群組的權限被**鎖定**。

您可以使用作業系統的標準管理工具檢視 KLAdmins 和 KLOperators 群組，並對這些群組進行變更。

在製定使用管理伺服器的規範時，有必要確定資訊安全專家是否需要完全存取權限（並包含在 KLAdmins 群組中）以執行標準工作。

大多數基本的管理工作可以在公司部門（或同一部門的不同員工）之間分配，因此也可以在不同的賬戶之間分配。您還可以在卡巴斯基安全管理中心中設定管理組訪問差異。因此，可能會出現這樣一種情況，KLAdmins 群組帳戶下的授權將出現異常，並可能被視為事件。

如果卡巴斯基安全管理中心安裝在系統帳戶下，則僅在管理伺服器裝置上建立群組。在這種情況下，我們建議確保只有在安裝卡巴斯基安全管理中心期間建立的項目才包含在該群組中。我們不建議將任何群組新增到在卡巴斯基安全管理中心安裝期間自動建立的 KLAdmins 群組（本機和/或網域）。您還應該限制變更該群組的權限。KLAdmins 群組必須僅包含一個非特權帳戶。

如果安裝是在網域使用者帳戶下執行的，則會在管理伺服器和包含管理伺服器的網域中建立群組 KLAdmins 和 KLOperators。建議使用類似的方法，例如本機帳戶安裝。

限制主要管理員角色成員資格

我們建議限制主管理員角色成員資格。

預設情況下，在管理伺服器安裝之後，主要管理員角色會被分配給本機管理員群組和建立的 KLAdmins 群組。它對管理有用，但從安全的角度來看它至關重要，因為主要管理員角色具有廣泛的權限，應嚴格規範向使用者分配此角色。

本機管理員可以從具有卡巴斯基安全管理中心管理員權限的使用者清單中排除。主要管理員角色不能從 KLAdmins 群組中刪除。您可以在 KLAdmins 群組中包含將用於管理管理伺服器的帳戶。

如果您使用網域驗證，我們建議在卡巴斯基安全管理中心中限制網域管理員帳戶的權限。預設情況下，這些帳戶具有主要管理員角色。此外，網域管理員可以將其帳戶包含在 KLAdmins 群組中以獲得主要管理員角色。為避免這種情況，您可以在卡巴斯基安全管理中心安全設定中新增 Domain Admins 組，然後為其定義禁止規則。這些規則必須優先於允許的規則。

您還可以使用預先定義的使用者角色，它們具有一組已配置的權限。

設定應用程式功能的存取權限

我們建議為每個使用者或群組靈活配置對卡巴斯基安全管理中心的功能的存取權限。

基於角色的存取控制可讓您使用一群組預先定義的權限建立標準使用者角色並根據使用者的職責範圍將這些角色分配給使用者。

基於角色的存取控制模型的主要優點：

- 易於管理
- 角色階層
- 最少特權方法
- 職責分離

您可以根據職位為某些員工分配內建角色，或建立全新的角色。

在配置角色時，需要注意與變更管理伺服器裝置防護狀態和遠端安裝協力廠商軟體相關的權限：

- 對管理群組進行管理。
- 管理伺服器操作。
- 遠端安裝。
- 變更用於儲存事件和傳送通知的參數。
  此權限允許您設定當事件發生時在管理伺服器裝置上執行指令碼或可執行模組的通知。

為遠端安裝應用程式使用單獨的帳戶

除了存取權限的基本區分外，我們建議限制所有帳戶（主要管理員或其他專用帳戶除外）的應用程式遠端安裝。

我們建議為遠端安裝應用程式使用單獨的帳戶。你可以分配角色或者權限給單獨帳戶。

保護 Windows 特權存取

我們建議考慮 Microsoft 關於提供特權存取安全性的建議。要檢視這些建議，請轉到保護特權存取文章。

建議的重點之一是特權存取工作站 (PAW) 的實施。

使用受管理服務帳戶 (MSA) 或群組受管理服務帳戶 (gMSA) 執行管理伺服器服務

Active Directory 有一種特殊類型的帳戶用於安全地執行服務，稱為群組受管理服務帳戶 (MSA/gMSA)。卡巴斯基安全管理中心支援受管理服務帳戶 (MSA) 和受群組管理的服務帳戶 (gMSA)。如果這些帳戶類型在您的網域中被使用，您可以選取它們之一作為管理伺服器服務帳戶。

定期稽核所有使用者和使用者的操作

我們建議對管理伺服器裝置上的所有使用者進行定期稽核。這使您能夠應對與裝置可能受到危害相關的某些類型的安全威脅。

另外，您還可以追蹤使用者的操作，例如連線到管理伺服器和斷開連線、連線到管理伺服器時發生錯誤以及物件修改（適用於支援修訂管理的物件）。

對管理伺服器防護的管理

選擇管理伺服器防護軟體

根據管理伺服器佈署的類型和一般防護策略，選擇防護管理伺服器裝置的應用程式。

如果您在專用裝置上佈署管理伺服器，我們建議選擇 Kaspersky Endpoint Security 應用程式來防護管理伺服器裝置。這可讓您套用所有可用技術來防護管理伺服器裝置，包括行為分析模組。

如果管理伺服器安裝在基礎結構的裝置上並且之前曾用於其他工作，我們建議考慮以下防護軟體：

- Kaspersky Industrial CyberSecurity for Nodes。我們建議在包含在產業網路中的裝置上安裝此應用程式。Kaspersky Industrial CyberSecurity for Nodes 是一個應用程式，具有與各種工業軟體製造商的相容性憑證。
- 推薦的安全解決方案。如果管理伺服器安裝在裝有其他軟體的裝置上，我們建議考慮該軟體供應商對安全解決方案相容性的建議（可能已經有選擇安全解決方案的建議，您可能需要配置信任區域）。

為防護應用程式建立單獨的安全政策

我們建議您為防護管理伺服器裝置的應用程式建立單獨的安全政策。此政策必須不同於用戶端裝置的安全政策。這可讓您為管理伺服器指定最合適的安全設定，而不會影響其他裝置的防護級別。

我們建議將裝置分組，然後將管理伺服器裝置放入一個單獨的群組中，您可以為其建立特殊的安全政策。

防護模組

如果與管理伺服器安裝在同一裝置上的協力廠商軟體供應商沒有特別建議，我們建議啟動並配置所有可用的防護模組（在檢查這些防護模組的運行一段時間後）。

配置管理伺服器裝置的防火牆

在管理伺服器裝置上，我們建議將防火牆配置為限制裝置數量，管理員可以從這些裝置通過管理主控台或卡巴斯基安全管理中心網頁主控台連線到管理伺服器。

預設情況下，管理伺服器使用連接埠 13291 從管理主控台接收連線，使用連接埠 13299 從卡巴斯基安全管理中心網頁主控台接收連線。我們建議限制可以使用這些連接埠管理管理伺服器的裝置數量。

管理用戶端裝置防護

限制將產品授權金鑰新增到安裝套件

安裝套件儲存在管理伺服器共用資料夾的 Packages 子資料夾中。如果將產品授權金鑰新增到安裝套件，則產品授權金鑰可能會洩露，因為對安裝套件的儲存區啟用了共用讀取存取權限。

為避免洩露產品授權金鑰，我們不建議將產品授權金鑰新增到安裝套件中。

我們推薦使用將產品授權金鑰自動發佈到受管理裝置，通過受管理應用程式的新增產品授權金鑰工作進行佈署，並手動將啟動碼或金鑰檔案新增到裝置。

在管理群組之間移動裝置的自動規則

我們建議限制使用自動規則在管理群組之間行動裝置。

如果您使用自動規則移動裝置，這可能會導致政策的傳播，這些政策為移動的裝置提供比重新定位前的裝置更多的權限。

此外，將用戶端裝置移動到另一個管理群組可能會導致政策設定的傳播。這些政策設定可能不適合發佈給訪客和不受信任的裝置。

此建議不適用於將裝置一次性初始分配給管理群組。

發佈點和連線閘道的安全要求

安裝了網路代理的裝置可以充當發佈點並執行以下功能：

- 將從管理伺服器收到的更新和安裝套件發佈到群組內的用戶端裝置。
- 在用戶端裝置上執行協力廠商軟體和卡巴斯基應用程式的遠端安裝。
- 輪詢網路以偵測新裝置並更新現有裝置的資訊。發佈點可以使用與管理伺服器相同的裝置偵測方法。

在組織的網路上放置發佈點用於：

- 降低管理伺服器負載
- 流量最佳化
- 提供管理伺服器到網路中難以到達的裝置的存取

考慮到可用功能，我們建議防護充當發佈點的裝置免受任何類型的未經授權存取（包括物理存取）。

限制自動分配發佈點

為了簡化管理並保持網路的可操作性，我們建議使用自動分配發佈點。但是，對於產業網路和小型網路，我們建議您避免自動分配發佈點，因為（例如）用於推送遠端安裝工作的帳戶的私人資訊可以被通過作業系統轉移到發佈點。

對於產業網路和小型網路，您可以手動分配裝置作為發佈點。

您還可以檢視發佈點活動報告。

對卡巴斯基安全管理中心使用者裝置的安全要求

卡巴斯基安全管理中心使用者的裝置必須套用特殊的安全要求。我們建議防護這些裝置免受任何類型未經授權的存取（包括實體存取）：

卡巴斯基安全管理中心使用者裝置包括以下內容：

- 使用者使用瀏覽器從其連線到卡巴斯基安全管理中心網頁主控台的裝置。
- 使用者使用基於 MMC 的管理主控台從其連線到卡巴斯基安全管理中心的裝置。
- 透過 OpenAPI 與管理伺服器互動的應用程式從其連線到卡巴斯基安全管理中心的裝置。

對於安裝了卡巴斯基安全管理中心網頁主控台的裝置的安全要求

安裝了卡巴斯基安全管理中心網頁主控台的裝置用於管理卡巴斯基安全管理中心，因此必須對這些裝置的安全性套用特殊要求。我們建議防護這些裝置免受任何類型未經授權的存取（包括實體存取）。

配置受管理應用程式的防護

受管理應用程式政策

我們建議為使用的每種類型的應用程式和卡巴斯基安全管理中心元件（網路代理、Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Agent 等）建立一個政策。此政策必須套用於所有受管理裝置（根管理群組）或根據配置的移動規則受管理裝置將自動移動到其中的單獨群組。

指定用於停用防護和解除安裝應用程式的密碼

為防止入侵者停用卡巴斯基安全應用程式，我們強烈推薦啟用密碼防護以停用卡巴斯基安全應用程式的防護和解除安裝。例如，您可以為 Kaspersky Endpoint Security for Windows、Kaspersky Security for Windows Servers、網路代理和其他卡巴斯基應用程式設定密碼。啟用密碼防護後，我們建議通過關閉"鎖"來鎖定這些設定。

指定將用戶端裝置手動連線到管理伺服器（klmover 公用程式）的密碼

klmover 公用程式允許您手動將用戶端裝置連線到管理伺服器。用戶端裝置上安裝網路代理時，此公用程式將同樣被複製到網路代理安裝節點。

為了防止入侵者將裝置移出管理伺服器的控制，我們強烈建議執行 klmover 公用程式時啟用密碼防護。要啟用密碼防護，請在**網路代理政策設定使用解除安裝密碼**使用卸載密碼選項。

klmover 公用程式需要本機管理員權限。對於沒有本機管理員權限操作的裝置，可以忽略為了執行 klmover 公用程式的密碼防護。

使用解除安裝密碼也會啟用 Cleaner 工具 (cleaner.exe) 的密碼防護。

使用卡巴斯基安全網路

在受管理應用程式的所有政策和管理伺服器內容中，我們建議啟用卡巴斯基安全網路 (KSN) 和接受 KSN 聲明。更新或升級管理伺服器時，您可以接受更新後的 KSN 聲明。在某些情況下，當法律或其他法規禁止使用雲端服務時，您可以停用 KSN。

定期掃描受管理裝置

對於所有裝置群組，我們建議建立一個定期執行完整裝置掃描的工作。

發現新裝置

我們建議正確配置裝置發現設定：設定與 Active Directory 的整合，並指定用於發現新裝置的 IP 位址範圍。

出於安全目的，您可以使用包含所有新裝置的預設管理群組和影響該群組的預設政策。

選取共用資料夾

如果您在執行 Windows 的裝置上佈署管理伺服器並選擇現有的共用資料夾（例如，用於放置安裝套件和儲存更新的資料庫的資料夾），我們建議確保向 Everyone 群組授予讀取權限，和向 KLAdmins 群組授予寫入權限。

管理伺服器維護

備份複製管理伺服器資料

資料備份允許您在不丟失資料的情況下還原管理伺服器資料。

預設情況下，資料備份工作在管理伺服器安裝後自動建立並定期執行，將備份儲存在適當的目錄中。
資料備份工作的設定可以變更如下：

- 備份頻率增加
- 指定儲存副本的特殊目錄
- 變更備份副本的密碼

如果您將備份副本儲存在不同於預設目錄的特殊目錄中，我們建議限制該目錄的存取控制清單 (ACL)。管理伺服器帳戶和管理伺服器資料庫的帳戶必須具有此目錄的寫入權限。

管理伺服器維護

管理伺服器維護允許您降低資料庫容積，提高程式的執行和操作可靠性。我們建議您至少每週維護一次管理伺服器。

管理伺服器維護透過專用工作執行。應用程式會在維護管理伺服器時執行以下操作：

- 檢查資料庫是否有錯誤
- 重組資料庫索引
- 更新資料庫統計資訊
- 收縮資料庫（如果必要）

安裝作業系統更新和協力廠商軟體更新

我們強烈建議您定期為管理伺服器裝置上的作業系統和協力廠商軟體安裝軟體更新。

用戶端裝置不需要持續連線到管理伺服器，因此在安裝更新後重新啟動管理伺服器裝置是安全的。管理伺服器宕機期間在用戶端裝置上註冊的所有事件都會在連線還原後傳送給它。

事件傳輸到協力廠商系統

監控和報告

為了及時回應安全事件，我們建議配置監控和報告功能。

匯出到 SIEM 系統的事件

為了在重大損害發生之前快速偵測事件，我們建議使用 SIEM 系統中的事件匯出。

稽核事件的電子郵件通知

卡巴斯基安全管理中心允許您接收受管理裝置上安裝的管理伺服器和其他 Kaspersky 應用程式的操作事件資訊。為了及時回應緊急情況，我們建議配置管理伺服器以傳送有關其發布的稽核事件、關鍵事件、故障事件和警告的通知。

由於這些事件是系統內事件，因此可以預期它們的數量很少，這非常適用於郵件。

佈署準備

該部分敘述了在佈署卡巴斯基安全管理中心之前必須採取的操作。

排程卡巴斯基安全管理中心佈署

本節資訊說明根據以下標準，在組織網路中佈署卡巴斯基安全管理中心元件的最方便選項：

- 裝置總數
- 在組織或地理上拆分的單元（本機辦公室、分支）
- 由狹窄通道連線的網路拆分網路
- 需要管理伺服器的網際網路存取權限

佈署防毒軟體的標準流程

本章節將介紹在企業網路中使用卡巴斯基安全管理中心標準的佈署病毒防護。

系統必須防止任何非授權的存取。我們建議您為您的作業系統安裝所有可用更新，然後再安裝應用程式到您的裝置並實體防護管理伺服器和發佈點。

您可以使用卡巴斯基安全管理中心佈署防護系統到企業網路，透過以下佈署方案：

- 使用下列方法其中之一，透過卡巴斯基安全管理中心佈署防毒軟體：
  - 透過管理主控台
  - 透過卡巴斯基安全管理中心 網頁主控台

  Kaspersky 應用程式自動安裝在用戶端裝置上，並透過卡巴斯基安全管理中心自動連線到管理伺服器。

  標準的佈署流程是透過管理主控台來佈署防毒軟體。使用卡巴斯基安全管理中心 網頁主控台可以在瀏覽器上進行佈署卡巴斯基應用程式。

- 使用在卡巴斯基安全管理中心建立的獨立安裝套件手動佈署防護系統。

  手動在用戶端裝置和管理員工作站中安裝 Kaspersky 應用程式；在安裝網路代理時指定用戶端裝置與管理伺服器的連線設定。

  該佈署方法建議在遠端安裝不可用時使用。

卡巴斯基安全管理中心可讓您使用 Microsoft Active Directory® 群組政策佈署您的防護系統。

在組織網路中計畫卡巴斯基安全管理中心佈署的資訊

一個管理伺服器可以支援最多 100,000 台裝置。如果組織網路中的裝置總數超過 100,000，必須在網路中佈署多個管理伺服器，並合併到一個方便集中管理的層級。

如果組織包含大規模有各自管理員的遠端本機辦公室（分支），則適合在這些辦公室佈署管理伺服器。否則，應將此類辦公室視為透過低速通道通訊起來的獨立網路，請參閱「標準配置：由自己管理員執行的幾個大規模辦公室」一節。

當使用由狹窄通道連線的拆分網路時，可以分配一個或幾個網路代理作為發佈點來節省流量（參見發佈點數量計算表格）。這種情況下，一個拆分網路中的所有裝置都從此本機更新中心上獲取更新。實際發佈點可以從管理伺服器（預設情景）和網際網路上的 Kaspersky 伺服器下載更新，參見"標準配置：多個小遠端辦公室"。

"卡巴斯基安全管理中心標準配置"部分提供了卡巴斯基安全管理中心標準配置的詳細敘述。當排程佈署時，根據組織架構選取最合適的標準配置。

在佈署排程階段，必須考慮到特別憑證 X.509 到管理伺服器的分配。X.509 憑證到管理伺服器的分配可能用在以下情況（部分清單）：

- 透過 SSL 終端代理或使用反向代理檢查安全通訊端層 (SSL)
- 與組織公共金鑰基礎架構 (PKI) 的整合

- 在憑證欄位中指定所需值
- 提供所需的憑證加密長度

選取企業防護結構

組織防護結構的選取根據以下因素進行定義：

- 環境的網路拓樸。
- 環境架構。
- 公司負責資訊人員數目，以及它們的職責。
- 可用於分配以便防護管理元件的硬體資源。
- 網路環境可分配給防護元件的承載量。
- 在組織網路中執行關鍵管理操作的時間限制。關鍵管理操作，包括分發病毒資料庫和修改用戶端裝置的政策。

當選取防護架構時，建議先確認集中防護系統可用的網路和硬體資源。

要分析網路和硬體的結構，建議進行以下流程：

1. 確認要佈署防毒軟體電腦上的網路設定：
   - 網段的數量。
   - 網段之間連線速度。
   - 每個網段受管理裝置的數量。
   - 可供防護操作所使用的網路承載量。
2. 進行重要的受管理裝置防護期間，能被允許的最長執行時間。
3. 分析來自步驟 1 和步驟 2 的資訊以及來自管理系統負載測試的資料。請您依照上述分析結果，來回答以下問題：
   - 是否可以用單一管理伺服器服務所有用戶端，或者需要管理伺服器階層？
   - 需要哪種管理伺服器硬體配置以便用在項目 2 中指定的時間限制內處理所有用戶端？
   - 是否需要使用發佈點來減少通信通道的負載？

根據您上述問題的答案，您可以得到結果來選取最符合您的環境的管理架構。

在您的網路環境下，您可以選取以下其中之一的標準架構：

- 單一管理伺服器。將所有用戶端裝置連線至單個管理伺服器。管理伺服器充當發佈點。
- 一個包含發佈點的管理伺服器。將所有用戶端裝置連線至單個管理伺服器。某些聯網的用戶端裝置作為發佈點執行。

- 管理伺服器階層。每個網段都分配了單獨的管理伺服器，作為管理伺服器一般階層式架構的一部分。主管理伺服器充當發佈點。
- 包含發佈點的管理伺服器階層。每個網段都分配了單獨的管理伺服器，作為管理伺服器一般階層式架構的一部分。某些聯網的用戶端裝置作為發佈點執行。

卡巴斯基安全管理中心的標準設定

該部分描述了以下用於組織網路中的卡巴斯基安全管理中心元件佈署的標準配置：

- 單一辦公室
- 幾個大規模辦公室，被地理拆分並由自己的管理員執行
- 多個小辦公室，被地理拆分

標準配置：單一辦公室

可以在組織網路佈署一個或幾個管理伺服器。管理伺服器數量可以基於可用硬體或受管理裝置總數來選取。

一個管理伺服器可以支援最多 100,000 台裝置。您必須考慮今後增加受管理裝置的數量的可能性：最好連線較少裝置到單一管理伺服器。

管理伺服器可以被佈署在內部網路或 DMZ，這取決於是否需要對管理伺服器的網際網路連線。

如果使用了多個伺服器，建議您合併它們到一個層級。使用管理伺服器階層允許您避免冗餘政策和工作、處理整個受管理裝置，使它們看起來是被單一管理伺服器管理，意即搜尋裝置、建立裝置分類和建立報告。

標準配置：由自己管理員執行的幾個大規模辦公室

若組織有些在地理位置上獨立的大規模辦公室，您必須考慮在各辦公室佈署管理伺服器的選項。每間辦公室可佈署一或多部管理伺服器，視可用用戶端裝置與硬體數量而定。此種情況下，每個辦公室可以被視為"標準配置：單一辦公室"。為了方便管理，建議將所有管理伺服器組合在階層中（多層級為佳）。

如果一些員工帶著裝置（膝上型電腦）在辦公室之間移動，請在網路代理政策中建立網路代理連線設定檔。網路代理連線設定檔僅支援用於 Windows 和 macOS 裝置。

標準配置：多個小遠端辦公室

此標準配置為透過網際網路聯絡總部的總部辦公室與許多遠端小型辦公室提供服務。每個遠端辦公室都可能位於 Network Address Translation (NAT) 之外，例如，兩個遠端辦公室之間無法建立連線，因為它們被隔離在外。

總部辦公室必須佈署一個管理伺服器，且必須分配一或多個發佈點到所有其他辦公室。如果辦公室透過網際網路連線，為發佈點建立*將更新下載到發佈點儲存區*工作會是比較實用的作法，這樣它們將從 Kaspersky 伺服器、本機或者網路資料夾而不是從管理伺服器直接下載更新。

如果遠端辦公室的一些裝置不能直接存取管理伺服器（例如，到管理伺服器的存取是透過網際網路提供但是一些裝置沒有網際網路連線），發佈點必須被轉換到連線閘道模式。此種情況下，遠端辦公室裝置上的網路代理將被透過閘道而不是直接連線到管理伺服器，為了後期同步。

作為管理伺服器，很可能無法輪詢遠端辦公室網路，最好把該功能轉給發佈點。

管理伺服器將無法傳送通知到遠端辦公室 NAT 以外的受管理裝置的連接埠 15000 UDP。要解決此問題，您可在作為發佈點的裝置內容中啟用持續連線到管理伺服器模式（**不斷開與管理伺服器的連線**核取方塊）。如果發佈點總數不超過 300 則該模式可用。使用推送伺服器以確保受管理裝置和管理伺服器之間存在持續連線。有關詳細資訊，請參閱以下主題：使用分發點作為推送伺服器。

選取 DBMS

當選取管理伺服器使用的資料庫管理系統 (DBMS) 時，您必須考慮到被管理伺服器覆寫的裝置數量。

下表列出了有效 DBMS 選項，以及對它們使用的建議和限制。

對 DBMS 的建議和限制

DBMS	建議和限制
SQL Server Express Edition 2012 或後續版本	如果您打算為少於 10,000 台裝置執行單個管理伺服器，請使用此 DBMS。 建議停用軟體清查工作並停用（在 Kaspersky Endpoint Security 政策設定中）管理伺服器對已啟動應用程序的通知。 您可以限制事件儲存庫中事件的最大數量，以防止資料庫外溢。 有關詳細資訊，請參閱以下主題：資料庫空間的計算。 SQL Server Express Edition DBMS 被管理伺服器和其他應用程式同時使用是被嚴格禁止的。 **執行 Windows Update 同步**工作不支援 Microsoft SQL Express 資料庫。
本機 SQL Server 版本，而不是 Express 2014 或後續版本	沒有限制。
遠端 SQL Server 版本，而不是 Express 2014 或後續版本	僅在兩台裝置都在相同 Windows® 網域中時可用；如果網域不同，必須在它們之間建立雙向信任關係。
本機或遠端 MySQL 5.5、5.6 或 5.7（MySQL 版本 5.5.1、5.5.2、5.5.3、5.5.4 和 5.5.5 不再被支援）。	如果您打算為少於 10,000 台裝置執行單個管理伺服器，請使用此 DBMS。 建議停用軟體清查工作並停用（在 Kaspersky Endpoint Security 政策設定中）管理伺服器對已啟動應用程序的通知。有關詳細資訊，請參閱以下主題：資料庫空間的計算。
本機或遠端 MySQL 8.0.20 或更新版本	如果您打算為少於 50,000 台裝置執行單個管理伺服器，請使用此 DBMS。 建議停用軟體清查工作並停用（在 Kaspersky Endpoint Security 政策設定中）管理伺服器對已啟動應用程序的通知。有關詳細資訊，請參閱以下主題：資料庫空間的計算。
本機或遠端 MariaDB（參見受支援的版本）	如果您打算為少於 20,000 台裝置執行單個管理伺服器，請使用此 DBMS。 建議停用軟體清查工作並停用（在 Kaspersky Endpoint Security 政策設定中）管理伺服器對已啟動應用程序的通知。有關詳細資訊，請參閱以下主題：資料庫空間的計算。
PostgreSQL、Postgres Pro（查看支援的版本）	如果您打算為少於 50,000 台裝置執行單個管理伺服器，請使這些 DBMS 之一。 建議停用軟體清查工作並停用（在 Kaspersky Endpoint Security 政策設定中）管理伺服器對已啟動應用程序的通知。有關詳細資訊，請參閱以下主題：資料庫空間的計算。

如果您使用 PostgreSQL、MariaDB 或 MySQL DBMS，**事件**頁簽可能會顯示所選用戶端裝置的不完整事件清單。當 DBMS 儲存大量事件時，就會發生這種情況。您可以執行下列任一操作來增加顯示的事件數目：

- 刪除不必要的事件。
- 減少不必要事件的儲存期限。

若要查看裝置的管理伺服器上記錄的事件的完整清單，請使用報告。

若您使用 SQL Server 2019 作為 DBMS，且沒有累積修補 CU12 或更新版本，您必須在安裝卡巴斯基安全管理中心後執行以下項目：

1. 使用 SQL Management Studio 連線至 SQL Server。
2. 請執行以下指令 (若您為資料庫選擇不同名稱，請使用開名稱而非 KAV)：

   ```
   USE KAV
   GO
   ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
   GO
   ```

3. 請重新啟動 SQL Server 2019 服務。

否則，使用 SQL Server 2019 可能造成錯誤，例如「資源集區『內部』的系統記憶體不足，無法執行此查詢。」

設定 MariaDB x64 伺服器以與卡巴斯基安全管理中心 14.2 一起使用

若要成功設定 MariaDB x64 伺服器以與卡巴斯基安全管理中心搭配使用，您必須使用本文中指定的伺服器參數之外的預設伺服器參數。

卡巴斯基安全管理中心 14.2 支援 MariaDB DBMS。如需有關支援的 MariaDB 版本的更多資訊，請參閱硬體和軟體需求一節說明。

如果您將 MariaDB DBMS 用於 Kaspersky Security Center，請啟用對 InnoDB 與 MEMORY 儲存以及 UTF-8 與 UCS-2 編碼的支援。

my.ini 檔案的建議設定

要設定 my.ini 檔案：

1. 在文字編輯器中開啟 my.ini 檔案。

2. 將以下行新增到 my.ini 檔案的 `[mysqld]` 部分：

```
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=< 實際值必須不得少於預期 KAV 資料庫大小的 80% >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
sql_mode="STRICT_TRANS_TABLES,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION"
```

`innodb_buffer_pool_size` 的值必須不少於預期之 KAV 資料庫大小的 80%。請注意，指定的記憶體是在伺服器啟動時分配的。如果資料庫大小小於指定的緩衝區大小，則只分配所需的記憶體。如果您使用 MariaDB 10.4.3 或更早版本，所分配記憶體的實際大小約比指定的緩衝大小大 10%。

建議使用參數值 `innodb_flush_log_at_trx_commit=0`，因為值 1 或 2 會對 MariaDB 的執行速度產生負面影響。確保`innodb_file_per_table`參數設定為`1`。

對於 MariaDB 10.1，另外在 [mysqld] 區域中輸入以下內容：

```
innodb_file_format='Barracuda'
innodb_default_row_format=dynamic
innodb_large_prefix=1
```

對於 MariaDB 10.6，另外在 [mysqld] 區域中輸入以下內容：

```
optimizer_prune_level=0
optimizer_search_depth=8
```

預設情況下，會啟用 `join_cache_incremental`、`join_cache_hashed` 和 `join_cache_bka` 最佳化程式附加元件。如果未啟用這些附加元件，則必須啟用它們。

要檢查是否啟用了最佳化程式附加元件：

1. 在 MariaDB 用戶端主控台中，執行以下命令：

   ```
   SELECT @@optimizer_switch;
   ```

2. 檢查其輸出是否包含以下幾行：

   ```
   join_cache_incremental=on
   join_cache_hashed=on
   join_cache_bka=on
   ```

   如果存在這幾行並on了這些值，則會啟用最佳化程式附加元件。

   如果這幾行不見了或其值為 `off`，請執行以下幾點：

   1. 在文字編輯器中開啟 my.ini 檔案。

   2. 將以下行新增到 my.ini 檔案的 `[mysqld]` 部分：

      ```
      optimizer_switch='join_cache_incremental=on'
      optimizer_switch='join_cache_hashed=on'
      optimizer_switch='join_cache_bka=on'
      ```

隨即會啟用 `join_cache_incremental`、`join_cache_hash` 和 `join_cache_bka` 附加元件。

設定 MySQL x64 伺服器以與卡巴斯基安全管理中心 14.2 一起使用

若要成功設定 MySQL x64 伺服器以與卡巴斯基安全管理中心搭配使用，您必須使用本文中指定的伺服器參數之外的預設伺服器參數。

如果您將 MySQL DBMS 用於 Kaspersky Security Center，請啟用對 InnoDB 與 MEMORY 儲存以及 UTF-8 與 UCS-2 編碼的支援。

my.ini 檔案的建議設定

要設定 my.ini 檔案：

1. 在文字編輯器中開啟 my.ini 檔案。

2. 將以下行新增到 my.ini 檔案的 `[mysqld]` 部分：

```
sort_buffer_size=10M
join_buffer_size=20M
tmp_table_size=600M
max_heap_table_size=600M
key_buffer_size=200M
innodb_buffer_pool_size=<實際值必須不得少於預期 KAV 資料庫大小的 80%>
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0 (i多數情況下，伺服器會使用小型交易)
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

請注意，在 `innodb_buffer_pool_size` 值中指定的記憶體在伺服器啟動時予以分配。如果資料庫大小小於指定的緩衝區大小，則只分配所需的記憶體。所分配記憶體的實際大小約比指定的緩衝大小大 10%。請參閱 MySQL 文件 以取得詳細資訊。

建議使用參數值 `innodb_flush_log_at_trx_commit = 0`，因為值「1」或「2」會對 MySQL 的執行速度產生負面影響。確保`innodb_file_per_table`參數設定為`1`。

設定 PostgreSQL 或 Postgres Pro 伺服器與卡巴斯基安全管理中心 14.2 搭配使用

若要成功設定 PostgreSQL 或 Postgres Pro 伺服器以與卡巴斯基安全管理中心搭配使用，您必須使用本文中指定的伺服器參數之外的預設伺服器參數。

卡巴斯基安全管理中心 14.2 支援 PostgreSQL 和 Postgres Pro DBMS。如果您使用這些 DBMS 之一，請考慮設定 DBMS 伺服器參數以最佳化 DBMS 與卡巴斯基安全管理中心一起運作。

設定檔的預設路徑是：`C:\Program Files\PostgreSQL\<版本>\data\postgresql.conf`

PostgreSQL 和 Postgres Pro 的建議參數：

- `shared_buffers` = DBMS 安裝所在裝置的 RAM 值的 25%

  如果 RAM 小於 1 GB，則保留預設值。

- `max_stack_depth = 2MB`

- `temp_buffers = 24MB`

- `work_mem = 16MB`

- `max_connections = 151`

- `max_parallel_workers_per_gather = 0`
- `maintenance_work_mem = 128MB`

確保`standard_conforming_strings`參數設定為其預設值on。更新 postgresql.conf 檔案後重新載入配置或重新啟動伺服器。請參閱PostgreSQL 文件以取得詳細資訊。

有關 PostgreSQL 和 Postgres Pro 伺服器參數以及如何指定它們的詳細資訊，請參閱相應的 DBMS 文件。

有關如何為 PostgreSQL 和 Postgres Pro 建立和配置帳戶的詳細資訊，請參閱以下主題： 設定帳戶以搭配使用 PostgreSQL 和 Postgres Pro。

使用 Kaspersky Endpoint Security for Android 管理行動裝置

安裝了 Kaspersky Endpoint Security for Android™ 的行動裝置（也叫 KES 裝置）透過管理伺服器管理。卡巴斯基安全管理中心支援以下管理 KES 裝置的功能：

- 將行動裝置處理為用戶端裝置：
  - 管理群組中的成員關係
  - 監控，例如檢視狀態、事件和報告
  - 修改本機設定和為 Kaspersky Endpoint Security for Android 分配政策
- 以集中模式傳送指令
- 遠端安裝行動應用程式套件

管理伺服器透過 TLS、TCP 連接埠 13292 管理 KES 裝置。

提供到管理伺服器的網際網路存取

以下情況需要到管理伺服器的網際網路存取：

- 定期更新 Kaspersky 資料庫、軟體模組和應用程式
- 更新協力廠商軟體

  預設情況下，管理伺服器不需要網際網路連線即可在受管理裝置上安裝 Microsoft 軟體更新。例如，受管理裝置可以直接從 Microsoft Update 伺服器下載 Microsoft 軟體更新，也可以從具有組織網路中佈署的 Microsoft Windows Server Update Services (WSUS) 的 Windows Server 下載 Microsoft 軟體更新。在以下情況下，您必須將管理伺服器連線到網際網路：
  - 將管理伺服器作為 WSUS 伺服器使用
  - 安裝 Microsoft 軟體以外協力廠商軟體的更新

- 修復協力廠商軟體弱點

  管理伺服器需要網際網路連線才能執行以下工作：

  - 列出針對 Microsoft 軟體弱點的建議修補程式。該清單由卡巴斯基專家建立並定期更新。
  - 修復非 Microsoft 軟體的協力廠商軟體中的弱點。
- 管理漫遊使用者的裝置（攜帶式電腦）
- 在遠端辦公室管理裝置
- 與位於遠端辦公室的主或從屬管理伺服器互動
- 管理行動裝置

該部分敘述了透過網際網路提供到管理伺服器的存取的典型方法。著眼於提供到管理伺服器的網際網路存取的每種情況都可能需要一個管理伺服器專用憑證。

網際網路存取：本機網路上的管理伺服器

如果管理伺服器位於組織內部網路，您可能希望管理伺服器的 TCP 連接埠 13000 可以從外部存取。若需行動裝置管理，您可能需要使連接埠 13292 TCP 可供存取。

網際網路存取：DMZ 中的管理伺服器

如果管理伺服器位於組織網路的 DMZ，它不能存取組織內部網路。因此，以下限制被套用：

- 管理伺服器無法偵測新裝置。
- 管理伺服器無法透過在組織內部網路裝置上強制安裝來執行網路代理初始化佈署。

這僅套用到網路代理初始化安裝上。任何網路代理的後續升級或安全應用程式安裝可以被管理伺服器執行。同時，網路代理的初始化佈署可以用其他方法執行，例如，透過 Microsoft® Active Directory® 群組政策。

- 管理伺服器無法透過連接埠 15000 UDP 傳送通知到受管理裝置，該連接埠不是卡巴斯基安全管理中心功能的關鍵連接埠。
- 管理伺服器無法輪詢 Active Directory。然而，Active Directory 輪詢結果在大多數方案下不需要。

如果上述限制被視為關鍵，它們可以透過使用組織網路的發佈點進行刪除：

- 要在沒有網路代理的裝置上執行初始化佈署，您首先要在其中一台裝置上安裝網路代理，然後給它分配發佈點狀態。結果，在其他裝置上的網路代理初始化安裝將透過該發佈點由管理伺服器執行。
- 要在組織網路中偵測新裝置並輪詢 Active Directory，您必須在其中一個發佈點上啟用相關的裝置發現方法。

要確保將通知成功傳送到組織網路上受管理裝置的連接埠 15000 UDP，您必須使用發佈點覆寫整個網路。在配置分佈點的內容中，選取**不斷開與管理伺服器的連線**核取方塊。因此，管理伺服器會建立一個到發佈點的持續連線，這些代理將能夠傳送通知到組織內部網路中裝置上的連接埠 15000 UDP（可以是 IPv4 或者 Ipv6 網路）。

網際網路存取：DMZ 中作為連線閘道的網路代理

管理伺服器可以位於組織內部網路，在其網路的 DMZ 中，可以有一個以連線閘道執行帶有反向連線（管理伺服器建立到網路代理的連線）的網路代理裝置。此種情況下，以下條件必須被滿足以確保網際網路存取：

- 網路代理必須安裝在該 DMZ 中的裝置。當您安裝網路代理時，請在安裝精靈**連線閘道**視窗中選取**使用網路代理作為 DMZ 連線閘道**。
- 您必須將安裝了連線閘道的裝置新增為發佈點。當您新增連線閘道時，在**新增發佈點**視窗中，選取**選取→按地址在 DMZ 中新增連線閘道**選項。
- 若要使用網際網路連線將外部桌上型裝置連線到管理伺服器，必須修正網路代理的安裝套件。在已建立安裝套件的屬性中，選取**進階→透過使用連線閘道連線到管理伺服器**選項，然後指定新建立的連線閘道。

對於 DMZ 中的連線閘道，管理伺服器建立與管理伺服器憑證一同簽署的憑證。如果管理員決定分配自訂憑證到管理伺服器，它必須在連線閘道在 DMZ 中被建立之前完成。

如果一些員工使用可以連線到管理伺服器的攜帶式電腦，最好在網路代理政策中為網路代理建立交換規則。

關於發佈點

已安裝網路代理裝置可以作為發佈點使用。在該模式中，網路代理可以執行以下功能：

- 派送更新（可以從管理伺服器獲取，或者從 Kaspersky 更新伺服器獲取）。在後者的案例中，您必須為作為發佈點的裝置建立*將更新下載到發佈點儲存區工作*：
  - 安裝軟體（包括網路代理初始化佈署）到其他裝置。
  - 輪詢網路以偵測新裝置並更新現有裝置的資訊。發佈點套用與管理伺服器相同的裝置發現方法。

在組織網路中佈署發佈點有以下好處：

- 降低管理伺服器負載。
- 最佳化流量。
- 提供管理伺服器到組織網路中難以到達的裝置的存取。NAT 以外發佈點的可用性（與管理伺服器有關）允許管理伺服器執行以下操作：
  - 在 IPv4 或 IPv6 網路上透過 UDP 傳送通知到裝置
  - 輪詢 IPv4 或 Ipv6 網路
  - 執行初始化佈署
  - 作為推送伺服器使用

為每個管理群組分配發佈點。在此情況下，發佈點的範圍包括管理群組和其所有子群組中的所有裝置。然而，作為發佈點的裝置可能不包含在它被分配的管理群組。

您可以讓發佈點作為連線閘道工作。在此情況下，發佈點範圍內的裝置會透過閘道，而不是直接連線到管理伺服器。不允許在網路代理和管理伺服器裝置之間建立直接連線時，此模式十分實用。

如果您使用基於 Linux 的裝置作為發佈點，我們強烈建議增加 klnagent 服務的檔案描述符限制，因為如果發佈點的範圍包括許多裝置，則預設可以開啟的最大檔案數可能還不夠。

增加 klnagent 服務的檔案描述符限制

如果基於 Linux 的發佈點的範圍包括許多裝置，則可開啟的檔案（檔案描述符）的預設限制可能不夠。為了避免這種情況，您可以增加 klnagent 服務的檔案描述符的限制。

要增加 klnagent 服務的檔案描述符限制：

1. 在充當發佈點的基於 Linux 的裝置上，開啟 `/lib/systemd/system/klnagent64.service` 檔案，然後在 `[Service]` 部分的 `LimitNOFILE` 參數中指定檔案描述符的硬限制和軟限制：

   `LimitNOFILE=< 軟資源限制 >:< 硬資源限制 >`

   例如，`LimitNOFILE=32768:131072`。請注意，檔案描述符的軟限制必須小於或等於硬限制。

2. 執行以下命令以確保參數指定正確：

   `systemd-analyze verify klnagent64.service`

   如果參數指定不正確，此命令可能會輸出下列錯誤之一：

   - `/lib/systemd/system/klnagent64.service:11: Failed to parse resource value, ignoring: 32768:13107`

     如果發生此錯誤，則 `LimitNOFILE` 行中的符號指定不正確。您必須檢查並更正輸入的行。

   - `/lib/systemd/system/klnagent64.service:11: Soft resource limit chosen higher than hard limit, ignoring: 32768:13107`

     如果發生此錯誤，則表示您輸入的檔案描述符的軟限制大於硬限制。您必須檢查輸入的行並確保檔案描述符的軟限制小於或等於硬限制。

3. 執行以下命令重新載入系統處理程序：

   `systemctl daemon-reload`

4. 執行以下命令重新啟動網路代理服務：

   `systemctl restart klnagent`

5. 執行以下命令以確保指定的參數得到正確套用：

   `less /proc/< nagent process id >/limits`

   其中 `< nagent process id >` 參數是網路代理處理程序的標識符。您可以執行以下命令來取得標識符：

   `ps -ax | grep klnagent`

對於基於 Linux 的發佈點，可以開啟的檔案的限制得到增加。

計算發佈點的數量和配置

網路包含越多的用戶端裝置，就需要越多的發佈點。我們建議您停用發佈點的自動分配。當發佈點的自動分配被啟用時，如果用戶端裝置數量很大，管理伺服器就分配發佈點並定義其配置。

使用單獨分配的發佈點

如果您計畫使用特定裝置作為發佈點（就是，單獨分配的伺服器），您可以不使用發佈點的自動分配。此種情況下，確保您要分配為發佈點的裝置具有足夠的剩餘磁碟空間磁區，不定期關閉，且停用了睡眠模式。

網路中基於網路裝置數量被專門分配的包含單一網段的發佈點的數量

網段中的用戶端裝置的數量	發佈點數量
少於 300	0（不分配發佈點）
大於 300	可接受：(N/10,000 + 1)，建議：(N/5000 + 2)，N 是網路裝置數量

網路中基於網路裝置數量被專門分配的包含多個網段的發佈點的數量

每個網段中的用戶端裝置的數量	發佈點數量
少於 10	0（不分配發佈點）
10–100	1
大於 100	可接受：(N/10000 + 1)，建議：(N/5000 + 2)，N 是網路裝置數量

使用標準用戶端裝置（工作站）作為發佈點

如果您計畫使用標準用戶端裝置（就是，工作站）作為發佈點，我們建議您按照所示分配發佈點（參見下表），以便避免通信管道和管理伺服器超載。

網路中基於網路裝置數量作為發佈點工作的包含單一網段的工作站的數量

網段中的用戶端裝置的數量	發佈點數量
少於 300	0（不分配發佈點）
大於 300	(N/300 + 1)，N 是網路裝置數量；至少有三台發佈點

網路中基於網路裝置數量作為發佈點工作的包含多個網段的工作站的數量

每個網段中的用戶端裝置的數量	發佈點數量
少於 10	0（不分配發佈點）
10–30	1
31–300	2
大於 300	(N/300 + 1)，N 是網路裝置數量；至少有三台發佈點

如果裝置被關閉（或由於某些原因不可用），其範圍內的受管理裝置可以存取管理伺服器以更新。

管理伺服器階層

一個 MSP 可能執行多個管理伺服器。可能不方便管理幾個不同的管理伺服器，因此可以應用階層結構。兩個管理伺服器的"主要/從屬"組態提供了以下選項：

- 一個從屬管理伺服器從主管理伺服器繼承政策和工作，這防止了重複設定。
- 主管理伺服器上的裝置分類可以包含從屬管理伺服器的裝置。
- 主管理伺服器的報告可以包含從屬管理伺服器的資料（包括詳細資訊）。

主管理伺服器僅會從上列選項範圍內的非虛擬從屬管理伺服器收到資料。此限制之所以不適用於虛擬管理伺服器，是因為虛擬管理伺服器與其主管理伺服器共用一個資料庫。

虛擬管理伺服器

基於實體管理伺服器，可以建立多個虛擬管理伺服器，它們與從屬管理伺服器相似。相比於基於存取控制清單 (ACLs) 的任意存取模式，虛擬管理伺服器模式功能更強大並且提供更高度隔離。除了適用於含政策與工作的已配置裝置的管理群組專屬結構外，各虛擬伺服器會具備其自己未配置的裝置的群組、自己的報告集、選取的裝置和事件、安裝套件、移動規則等。虛擬管理伺服器的功能範圍可由服務供應商 (xSP) 以及有複雜工作流程與無數管理員的大規模組織同時使用，以充分發揮隔離客戶的目的。

虛擬管理伺服器與從屬管理伺服器非常相似，但是有以下不同點：

- 虛擬管理伺服器缺少多數全域設定和自己的 TCP 連接埠。
- 虛擬管理伺服器沒有從屬管理伺服器。
- 虛擬管理伺服器沒有其他虛擬管理伺服器。
- 實體管理伺服器可以檢視它所有虛擬管理伺服器的裝置、群組、事件和受管理裝置上的物件（隔離區項目、應用程式登錄資料等等）。
- 虛擬管理伺服器僅可以掃描連線了發佈點的網路。

卡巴斯基安全管理中心的限制資訊

下表顯示卡巴斯基安全管理中心目前版本的限制。

卡巴斯基安全管理中心的限制

限制類型	參數值
每個管理伺服器的最大受管理裝置數量	100,000
選取**不斷開與管理伺服器的連線**選項時的裝置數量上限。	300
管理群組最大數量	10,000
要儲存的事件的最大數量	45,000,000
政策的最大數量	2000
工作的最大數量	2000
Active Directory 物件的最大總數（組織單元 (OU) 和使用者帳戶、裝置和安全群組）	1,000,000
政策中設定檔的最大數量	100
單一主管理伺服器的從屬管理伺服器的最大數量	500
虛擬管理伺服器的最大數量	500
單一發佈點可以覆蓋的最大裝置數量（發佈點僅可以覆蓋非行動裝置）	10,000
可以使用單一連線閘道的最大裝置數量	10,000，包括行動裝置
每個管理伺服器的最大行動裝置數量	100,000 減去固定的受管理裝置數量

網路負載

本章節介紹在關鍵管理操作期間，用戶端裝置與管理伺服器交換的網路流量。

網路流量主要的來源是來自於以下的狀況所產生：

- 病毒防護的初始佈署
- 病毒資料庫的原始更新
- 用戶端裝置與管理伺服器同步
- 定期排程的病毒資料庫更新
- 利用管理伺服器對用戶端裝置上事件的處理

病毒防護的初始佈署

本章節提供關於網路代理和 Kaspersky Endpoint Security for Windows 安裝到用戶端裝置之後的流量值的相關資訊（請參閱下表）。

網路代理被強制安裝，當安裝所需檔案被管理伺服器複製到用戶端裝置上的共用資料夾時。安裝後，網路代理使用到管理伺服器的連線收回 Kaspersky Endpoint Security for Windows 的分發套件。

流量

情景	網路代理安裝在單一裝置上	在單一用戶端裝置上安裝 Kaspersky Endpoint Security for Windows（資料庫已更新）	網路代理與 Kaspersky Endpoint Security for Windows 一起安裝
從用戶端裝置到管理伺服器的流量，KB	1638.4	7843.84	9707.52
管理伺服器到用戶端裝置的流量，KB	69,990.4	259,317.76	329,318.4
總流量（對單一用戶端裝置而言），KB	71,628.8	267,161.6	339,025.92

網路代理被安裝至用戶端裝置後，管理群組中的一個裝置可以被指派為發佈點。這將會在發佈安裝套件發揮其用途。在此範例中，初始佈署病毒防護的流量隨著是否使用 IP 多點傳送而顯著變化。

如果使用多點傳送 IP 傳輸，安裝套件將會同時傳送給管理群組中的裝置。因此，總網路流量將會下降 N 倍，其中 N 為代表管理群組的裝置總數量。如果不使用 IP 多點傳送，總流量等同于安裝套件從管理伺服器下載的情況。但是，下載的來源會是發佈點，並不是管理伺服器。

病毒資料庫的原始更新

病毒資料庫在初始更新的流量率（當在用戶端裝置上首次啟資料庫更新工作時）如下：

- 從用戶端裝置到管理伺服器的流量：1.8 MB。
- 從管理伺服器到用戶端裝置的流量：113 MB。
- 總流量（對單一用戶端裝置而言）：114 MB。

資料可能會依據目前病毒資料庫版本而有細微差別。

使用戶端與管理伺服器同步

此情況敘述當用戶端裝置與管理伺服器有密集的資料同步的狀況下。用戶端裝置以管理員定義的間隔與管理伺服器相連。管理伺服器將比較用戶端裝置與管理伺服器的資料、記錄用戶端裝置最近一次連線資料庫的資訊以及同步資料。

在一個基本的管理規則下，用戶端電腦連線到管理伺服器的流量（請參考下表）。表中資料可能會依據目前病毒資料庫版本而有細微差別。

流量

情景	從用戶端裝置到管理伺服器的流量，KB	管理伺服器到用戶端裝置的流量，KB	總流量（對單一用戶端裝置而言），KB
初次同步在預先更新威脅資料庫的用戶端裝置的流量	699.44	568.42	1267.86
初次同步在更新威脅資料庫之後的用戶端裝置的流量	735.8	4474.88	5210.68
用戶端裝置與管理伺服器同步時，並無變動的同步資料的流量	11.99	6.73	18.72
在變更群組政策設定後，同步的流量	9.79	11.39	21.18
在變更群組工作設定後，同步的流量	11.27	11.72	22.99
使用強制同步，並無變動的同步資料的流量	77.59	99.45	177.04

在管理群組中是否選用 IP 多點傳送，其總體流量差異相當大。如果選用了 IP 多點群播，總流量將下降大約 N 倍，N 代表管理群組中執行的裝置數量。

按照如下情況指定在更新資料庫之前和之後的初始同步的流量:

- 安裝網路代理和安全應用程式到用戶端裝置
- 移動用戶端裝置到管理群組
- 套用預設建立的群組政策和工作到用戶端裝置

該表標示在修改 Kaspersky Endpoint Security 政策設定中包括防護設定時的流量速率。其他政策設定的資料可能與該表中顯示的資料不同。

病毒資料庫額外更新

上次更新 20 小時後病毒資料庫進行增量更新時的流量比率如下：

- 從用戶端裝置到管理伺服器的流量：169 KB。
- 從管理伺服器到用戶端裝置的流量：16 MB。
- 總流量（對單一用戶端裝置而言）：16.3 MB。

表中資料可能會依據目前病毒資料庫版本而有細微差別。

在管理群組中是否選用 IP 多點傳送，其總體流量差異相當大。如果選用了 IP 多點群播，總流量將下降大約 N 倍，N 代表管理群組中執行的裝置數量。

利用管理伺服器對用戶端事件的處理

本章節提供當用戶端裝置遇到“偵測到病毒”事件，並且隨後將此事件傳送到管理伺服器並註冊到資料庫中時的流量值的相關資訊（請參考下表）。

流量

情景	發生「偵測到病毒」事件時傳送至管理伺服器的資料傳輸	發生九次「偵測到病毒」事件時傳送至管理伺服器的資料傳輸
從用戶端裝置到管理伺服器的流量，KB	49.66	64.05
管理伺服器到用戶端裝置的流量，KB	28.64	31.97
總流量（對單一用戶端裝置而言），KB	78.3	96.02

該表中的資料可能依據病毒防護程式的目前版本和在其政策中定義的在管理伺服器資料庫中註冊的事件而略有差異。

24 小時流量

本章節提供若您未進行任何管理動作（用戶端裝置和管理伺服器上沒有任何資料變動）24 小時的流量比率的資訊（請參閱下表）。

表中資料敘述了標準安裝卡巴斯基安全管理中心並完成快速設定精靈後的網路條件。用戶端裝置與管理伺服器同步的週期為 20 分鐘一次，更新每一小時下載到管理伺服器儲存區一次。

處於閒置狀態的每 24 小時流量率

流量	參數值
從用戶端裝置到管理伺服器的流量，KB	3235.84
管理伺服器到用戶端裝置的流量，KB	64,378.88
總流量（對單一用戶端裝置而言），KB	67,614.72

準備行動裝置管理

此部分提供下列資訊：

- 關於透過 Exchange ActiveSync 協定管理行動裝置的 Exchange 行動裝置伺服器
- 關於用於透過在 iOS 裝置上安裝專用 iOS MDM 設定檔來管理它們的 iOS MDM 伺服器
- 關於安裝了 Kaspersky Endpoint Security for Android 的行動裝置的管理

Exchange 行動裝置伺服器

Exchange 行動裝置伺服器允許您使用 Exchange ActiveSync 協定（EAS 裝置）管理連線到管理伺服器的行動裝置。

如何佈署 Exchange 行動裝置伺服器

如果有用戶端存取伺服器陣列中的多個 Exchange 伺服器被佈署到組織，Microsoft Exchange 行動裝置伺服器必須被安裝到陣列中的每個伺服器。**叢集模式**選項必須在 Exchange 行動裝置伺服器部署精靈中啟用。此種情況下，陣列中伺服器上安裝的 Exchange 行動裝置伺服器實例集被稱作 Exchange 行動裝置伺服器叢集。

如果 Exchange 伺服器的用戶端存取伺服器陣列未被佈署到組織，Microsoft Exchange 行動裝置伺服器必須被安裝在具有用戶端存取的 Microsoft Exchange 伺服器上。在此情況下，**標準模式**選項必須在 Exchange 行動裝置伺服器安裝精靈中啟用。

與 Exchange 行動裝置伺服器一起，網路代理也必須安裝在裝置上；它說明將 Exchange 行動裝置伺服器與卡巴斯基安全管理中心進行整合。

Exchange 行動裝置伺服器的預設掃描範圍是目前所在 Active Directory 網域。佈署 Exchange 行動裝置伺服器到安裝了 Microsoft Exchange Server（版本 2010, 2013）的伺服器上允許您延伸掃描範圍以包含整個網域樹系到 Exchange 行動裝置伺服器（參見"設定掃描範圍"部分）。掃描中所需的資訊包括 Microsoft Exchange 伺服器使用者帳戶、Exchange ActiveSync 政策和透過 Exchange ActiveSync 協定連線到 Microsoft Exchange Server 的使用者行動裝置。

如果實例在由單一管理伺服器管理的**標準模式**執行，則不能在一個單一網域安裝多個 Exchange 行動裝置伺服器的實例。在單一 Active Directory 網域樹系中，如果實例在包含了整個網域的延伸掃描範圍的**標準模式**執行，或它們連線到單一管理伺服器，則不能在一個單一網域安裝多個 Exchange 行動裝置伺服器實例（或多個 Exchange 行動裝置伺服器叢集）。

佈署 Exchange 行動裝置伺服器所需的權限

在 Exchange Server（2010、2013）上佈署 Microsoft Exchange 行動裝置伺服器需要網域管理員權限和組織管理角色。在 Exchange Server (2007) 上佈署 Microsoft Exchange 行動裝置伺服器需要網域管理員權限和 Exchange Organization Administrators 安全群組成員關係。

Exchange ActiveSync 服務帳戶

當安裝了 Exchange 行動裝置伺服器被安裝後，帳戶在 Active Directory 裡自動建立：

- 在 Microsoft Exchange Server (2010, 2013) 上：帶有 KLMDM 角色群組角色的 KLMDM4ExchAdmin***** 帳戶。
- 在 Microsoft Exchange Server (2007) 上：KLMDM4ExchAdmin***** 帳戶，它是 KLMDM 安全群組成員。

Exchange 行動裝置伺服器在此帳戶下執行。

如果您要取消帳戶的自動產生，您需要建立具有以下權限的自訂帳戶：

- 當使用 Microsoft Exchange Server (2010, 2013) 時，帳戶必須被分配允許執行以下 cmdlets 的角色：
  - Get-CASMailbox
  - Set-CASMailbox
  - Remove-ActiveSyncDevice
  - Clear-ActiveSyncDevice
  - Get-ActiveSyncDeviceStatistics
  - Get-AcceptedDomain
  - Set-AdServerSettings
  - Get-ActiveSyncMailboxPolicy
  - New-ActiveSyncMailboxPolicy
  - Set-ActiveSyncMailboxPolicy
  - Remove-ActiveSyncMailboxPolicy
- 當使用 Microsoft Exchange Server (2007) 時，帳戶必須被授予到 Active Directory 物件的存取權限（參見下表）。

到 Active Directory 物件的存取權限

權限	物件	Cmdlet
完全	執行緒 "CN=Mobile Mailbox Policies,CN=< 組織名稱 >,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=< 網域名稱 >"	`Add-ADPermission -User < 使用者或群組名稱 > -Identity "CN=Mobile Mailbox Policies,CN=< 組織名稱 >,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=< 網域名稱 >" -InheritanceType All -AccessRight GenericAll`
讀取	執行緒 "CN=< 組織名稱 >,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=< 網域名稱 >"	`Add-ADPermission -User < 使用者或群組名稱 > -Identity "CN=< 組織名稱 >,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=< 網域名稱 >" -InheritanceType All -AccessRight GenericRead`
讀/寫	Active Directory 物件的 msExchMobileMailboxPolicyLink 和 msExchOmaAdminWirelessEnable 內容	`Add-ADPermission -User < 使用者或群組名稱 > -Identity "DC=< 網域名稱 >" -InheritanceType All -AccessRight ReadProperty,WriteProperty -Properties msExchMobileMailboxPolicyLink, msExchOmaAdminWirelessEnable`
延伸權限 ms-Exch-Store-Active	Exchange 伺服器信箱儲存區，執行緒 "CN=Databases,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=< 組織名稱 >,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=< 網域名稱 >"	`Get-MailboxDatabase | Add-ADPermission -User < 使用者或群組名稱 > -ExtendedRights ms-Exch-Store-Admin`

iOS MDM 伺服器

iOS MDM 伺服器允許您透過在 iOS 裝置上安裝專用 iOS MDM 設定檔來管理它們。它支援以下功能：

- 裝置鎖定
- 密碼重設
- 資料抹除
- 安裝和移除應用
- 使用帶有進階設定（例如 VPN 設定、電子郵件設定、Wi-Fi 設定、攝影鏡頭設定、憑證設定等等）的 iOS MDM 設定檔

iOS MDM 伺服器是一個 Web 服務，它透過 TLS 連接埠（預設下，連接埠 443）從行動裝置接收傳入連線，它被卡巴斯基安全管理中心使用網路代理進行管理。網路代理安裝在佈署了 iOS MDM 伺服器的裝置本機。

當佈署 iOS MDM 伺服器時，管理員必須執行以下操作：

- 提供網路代理到管理伺服器的存取
- 提供連線裝置到 iOS MDM 伺服器的 TCP 連接埠的存取

該部分涉及 iOS MDM 伺服器的兩個標準配置。

標準配置：DMZ 中的 Kaspersky Device Management for iOS

iOS MDM 伺服器位於組織本機網路的 DMZ 中，並提供網際網路存取。該方法的一個特殊功能就是當 iOS MDM Web 服務從網際網路被裝置存取時，將不會出現問題。

因為 iOS MDM 伺服器的管理需要網路代理安裝在本機，您必須確保網路代理與管理伺服器的互動。您可以使用下列可用方法之一進行確保：

- 透過行動管理伺服器到 DMZ。
- 透過使用連線閘道：
  a. 在佈署了 iOS MDM 伺服器的裝置上，透過連線閘道連線網路代理到管理伺服器。
  b. 在佈署了 iOS MDM 伺服器的裝置上，分配網路代理作為連線閘道。

標準配置：組織本機網路中的 iOS MDM 伺服器

iOS MDM 伺服器位於組織內部網路。必須啟用連接埠 443（預設連接埠）以進行外部存取，例如，透過在支援 Kerberos 約束委派的反向代理上發布 iOS MDM Web 服務。

任何標準配置都需要 iOS MDM 伺服器（範圍 17.0.0.0/8）透過 TCP 連接埠 2197 存取 Apple Web 服務。該連接埠用於透過名為 APNs 的專用服務通知裝置新指令。

使用 Kaspersky Endpoint Security for Android 管理行動裝置

安裝了 Kaspersky Endpoint Security for Android™ 的行動裝置（也叫 KES 裝置）透過管理伺服器管理。卡巴斯基安全管理中心支援以下管理 KES 裝置的功能：

- 將行動裝置處理為用戶端裝置：
  - 管理群組中的成員關係
  - 監控，例如檢視狀態、事件和報告
  - 修改本機設定和為 Kaspersky Endpoint Security for Android 分配政策
- 以集中模式傳送指令
- 遠端安裝行動應用程式套件

管理伺服器透過 TLS、TCP 連接埠 13292 管理 KES 裝置。

管理伺服器效能資訊

本章節顯示了不同硬體設定的管理伺服器效能測試的結果，以及連線受管理裝置到管理伺服器的限制。

連線到管理伺服器的限制

管理伺服器支援對 100,000 台裝置的管理，而不降低效能。

不降低效能而連線到管理伺服器的限制：

- 一個管理伺服器可以支援最多 500 台虛擬管理伺服器。
- 主管理伺服器同時支援的連線數不多於 1000 個。
- 虛擬管理伺服器同時支援不多於 1000 個連線。

管理伺服器效能測試報告

此測試結果為在固定的時間間隔內，管理伺服器能同步裝置的最大數量。您可以使用此資訊來選擇在電腦網路上部署病毒防護的方案。

具有以下硬體設定的裝置（參見下表）用於測試：

管理伺服器硬體設定

參數	參數值
CPU	Intel Xeon CPU E5630, clock speed of 2.53 GHz, 2 socket, 8 cores, 16 logical processors
RAM	26 GB

參數	參數值
硬碟磁碟機	IBM ServeRAID M5014 SCSI Disk Device, 487 GB
作業系統	Microsoft Windows Server 2019 標準版，版本 10.0.17763，內部版本 17763
網路	QLogic BCM5709C 千兆以太網（NDIS VBD 用戶端）

SQL Server 伺服器裝置硬體設定

參數	參數值
CPU	Intel Xeon CPU X5570，時脈速度 2.93 Ghz，2 個通訊端，8 個核心，16 個邏輯處理器
RAM	32 GB
硬碟磁碟機	Adaptec 陣列 SCSI 磁碟機裝置，2047 GB
作業系統	Microsoft Windows Server 2019 標準版，版本 10.0.17763，內部版本 17763
網路	Intel 82576 Gigabit

管理伺服器支援建立 500 個虛擬管理伺服器。

同步間隔是每 10,000 部受管理裝置 15 分鐘（請參閱下表）。

管理伺服器負載測試概要結果

同步間隔（分鐘）	受管理裝置數量
15	10,000
30	20,000
45	30,000
60	40,000
75	50,000
90	60,000
105	70,000
120	80,000
135	90,000
150	100,000

如果您的管理伺服器使用 MySQL 或 SQL Express 資料庫，建議您管理的裝置在 10000 台以下。對於 MariaDB 資料庫管理系統，建議的最大受管理裝置數量為 20000。

KSN 代理伺服器效能測試結果

如果您的企業網路包含大量用戶端裝置且它們使用管理伺服器作為 KSN 代理伺服器，管理伺服器硬體必須滿足特定需求才可以處理來自用戶端裝置的請求。您可以使用以下測試結果評估您網路中的管理伺服器負載，並分配硬體資源以提供 KSN 代理伺服器的正常功能。

下表顯示了管理伺服器和 SQL Server 的硬體設定。此設定用於測試。

管理伺服器硬體設定

參數	參數值
CPU	Intel Xeon CPU E5450，時脈速度 3.00 GHz，2 個通訊端，8 個核心，16 個邏輯處理器
RAM	32 GB
作業系統	Microsoft Windows Server 2016 Standard

SQL 伺服器硬體設定

參數	參數值
CPU	Intel Xeon CPU E5450，時脈速度 3.00 GHz，2 個通訊端，8 個核心，16 個邏輯處理器
RAM	32 GB
作業系統	Microsoft Windows Server 2019 Standard

下表顯示測試結果。

KSN 代理伺服器效能測試結果摘要

參數	參數值
每秒處理的最大請求數	4914
最大 CPU 使用	36%

用於與外部服務交互的網路設定

卡巴斯基安全管理中心使用以下網路設定與外部服務交互。

網路設定

網路設定	位址	敘述
連接埠：443 協定：HTTPS	activation-v2.kaspersky.com	應用程式啟動。
連接埠：443 協定：HTTPS	https://s00.upd.kaspersky.com https://s01.upd.kaspersky.com https://s02.upd.kaspersky.com https://s03.upd.kaspersky.com https://s04.upd.kaspersky.com https://s05.upd.kaspersky.com https://s06.upd.kaspersky.com https://s07.upd.kaspersky.com https://s08.upd.kaspersky.com https://s09.upd.kaspersky.com https://s10.upd.kaspersky.com https://s11.upd.kaspersky.com https://s12.upd.kaspersky.com https://s13.upd.kaspersky.com https://s14.upd.kaspersky.com https://s15.upd.kaspersky.com https://s16.upd.kaspersky.com https://s17.upd.kaspersky.com https://s18.upd.kaspersky.com https://s19.upd.kaspersky.com https://cm.k.kaspersky-labs.com	更新 Kaspersky 資料庫、軟體模組和應用程式。

網路設定	位址	敘述
連接埠： 443 協定： HTTPS	https://downloads.upd.kaspersky.com	• 更新 Kaspersky 資料庫、軟體模組和應用程式。 • 檢查卡巴斯基伺服器是否可存取。 在下載卡巴斯基資料庫和軟體模組之前，卡巴斯基安全管理中心會檢查卡巴斯基伺服器是否可以存取。如果無法使用系統 DNS 存取伺服器，則應用程式使用公用 DNS 伺服器。
連接埠： 80 協定： HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	更新 Kaspersky 資料庫、軟體模組和應用程式。
連接埠： 443 協定： HTTPS	ds.kaspersky.com dc1.ksn.kaspersky-labs.com dc1-file.ksn.kaspersky-labs.com dc1-pp.ksn.kaspersky-labs.com dc1-st.ksn.kaspersky-labs.com	使用卡巴斯基安全網路。

網路設定	位址	敘述
連接埠： 443、1443 協定： HTTPS	ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com	使用卡巴斯基安全網路。
協定： HTTPS	click.kaspersky.com redirect.kaspersky.com	開啟介面中的連接。
連接埠： 80 協定： HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	這些伺服器是公鑰基礎設施 (PKI) 的一部分，是驗證卡巴斯基數位簽章憑證有效性狀態所必需的。CRL 是已撤銷憑證的清單。OCSP 可讓您即時請求特定憑證的狀態。這些伺服器有助於確保與數位憑證互動的安全性並防止可能的攻擊。
連接埠： 443 協定： HTTPS	https://ipm-klca.kaspersky.com	行銷公告。

為了讓卡巴斯基安全管理中心與外部服務正確交互，請考慮以下建議：
- 組織的網路裝置和代理伺服器上的連接埠 443 和 1443 必須允許未加密的網路流量。
- 當管理伺服器與卡巴斯基更新伺服器和卡巴斯基安全網路伺服器交互時，必須避免通過憑證替換劫持網路流量（ MITM 攻擊 ）。

要使用 klscflag 公用程式透過 HTTP 或 HTTPS 協定下載更新：

1. 使用管理員權限執行 Windows 命令提示符，然後將目前目錄變更為包含 klscflag 公用程式的目錄。klscflag 公用程式位於安裝管理伺服器的資料夾中。預設安裝路徑：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. 如果您想透過 HTTP 協定下載更新，請執行以下命令之一：

   - 在安裝了管理伺服器的裝置上：

     ```
     klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
     ```

   - 在發佈點上：

     ```
     klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
     ```

   如果您想透過 HTTPS 協定下載更新，請執行以下命令之一：

   - 在安裝了管理伺服器的裝置上：

     ```
     klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
     ```

   - 在發佈點上：

     ```
     klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
     ```

佈署網路代理和安全應用程式

要管理組織裝置，您必須在其上安裝網路代理。佈署分發的卡巴斯基安全管理中心到組織裝置通常開始於在其上安裝網路代理。

在 Microsoft Windows XP 中，網路代理可能錯誤執行以下操作：直接從 Kaspersky 伺服器（作為發佈點）下載更新；作為 KSN 代理伺服器（作為發佈點）；偵測協力廠商弱點（如果弱點和修補程式管理被使用）。

初始化佈署

要管理組織中的裝置，您必須在每台裝置上都安裝網路代理。

可以透過以下方式在執行 Windows 的受管理裝置上安裝網路代理：

- 使用應用程式遠端安裝的協力廠商工具。
- 透過克隆帶有作業系統和網路代理的管理員硬碟磁碟機映像，透過使用卡巴斯基安全管理中心提供的工具處理磁碟映像或透過使用協力廠商工具。
- 對於 Windows 群組政策，透過使用標準 Windows 群組政策管理工具、或在自動模式下，透過卡巴斯基安全管理中心遠端安裝工作的專用選項。
- 在強制模式下，透過卡巴斯基安全管理中心的遠端安裝工作使用作業系統資源。
- 透過程式裝置使用者連結到卡巴斯基安全管理中心生成的獨立安裝套件。獨立安裝套件是包含所選應用程式分發套件的定義了設定的可執行模組集合。
- 在裝置上手動執行應用程式安裝程式。

可以透過以下方式在執行 Linux 的受管理裝置上初始安裝網路代理：

- 透過 SSH 連線到受管理裝置並執行遠端安裝工作。
- 透過在受管理裝置上執行套件安裝。

可以透過以下方式在執行 macOS 的受管理裝置上初始安裝網路代理：

- 透過 macOS 發佈點執行遠端安裝工作。
- 透過將裝置使用者連結傳送到卡巴斯基安全管理中心產生的獨立套件。獨立套件是包含所選應用程式分發套件且具有預定義設定的可執行模組。

在裝置上安裝網路代理後，您可以透過該網路代理在裝置上執行卡巴斯基應用程式的遠端安裝。要安裝的應用程式分發套件透過網路代理和管理伺服器之間的通訊管道，與管理員定義的安裝設定一併傳輸。若要轉移分發套件，您可使用轉發分發節點，也就是發佈點、多點傳送等。

當選取用於佈署應用程式到受管理網路的方法和政策時，您必須考慮很多因素（部分清單）：

- 組織網路的配置。
- 裝置總數。
- 組織網路的裝置存在情況、不是任何 Active Directory 網域成員；在這些裝置上具有管理員權限的統一帳戶的存在情況。
- 管理伺服器和裝置通道的容量。
- 管理伺服器和遠端子網路之間的通訊類型以及這些子網路中的網路通道容量。
- 部署開始時在遠端裝置上套用的安全設定。這些參數允許建立與受管理裝置的遠端連線並開始安裝。

配置安裝程式

在開始佈署 Kaspersky 應用程式到網路之前，您必須指定安裝設定，就是在應用程式安裝過程中定義的設定。當安裝網路代理時，您應該指定最小值、連線管理伺服器的位址，也可能需要一些進階設定。取決於您選取的安裝方法，您可以用不同方法定義設定。最簡單的方法（在所選裝置上的手動互動式安裝），所有相關設定可以透過安裝程式使用者介面進行定義。

該定義設定的方法不適用於在裝置群組上的應用程式靜默安裝。通常情況下，管理員必須集中指定設定值；這些值可能隨後用於在所選網路裝置上的靜默安裝。

安裝套件

定義應用程式安裝設定的第一個和主要的方法是通用的，因此適用於所有安裝方法，用卡巴斯基安全管理中心工具和多數協力廠商工具。該方法包括在卡巴斯基安全管理中心中建立應用程式安裝套件。

安裝套件使用以下方法產生：

- 基於包含的*敘述符*（帶有 .kud 副檔名的包含了安裝和結果分析規則以及其他資訊的檔案）從指定的分發套件自動產生
- 來自安裝程式的可執行檔或來自原生格式（.msi、.deb、.rpm）的安裝程式，適用於標准或受支援的應用程式

產生的安裝套件以子資料夾和檔案層級組織。除了原始分發套件，安裝套件包含可編輯設定（包含安裝程式設定和是否在安裝結束時重新啟動作業系統等處理規則）以及小的輔助模組。

單獨支援的應用程式的安裝設定值可以在建立安裝套件時在管理主控台的使用者介面定義。當透過卡巴斯基安全管理中心工具執行遠端應用程式安裝時，安裝套件被傳送到裝置，因此執行應用程式安裝程式使得所有管理員定義的設定對該應用程式可用。當使用協力廠商工具安裝 Kaspersky 應用程式時，您僅需要確保裝置上整個安裝套件的可用性，即是分發套件和其設定的可用性。安裝套件被卡巴斯基安全管理中心建立和儲存在共用資料夾下的專用資料夾。

不在安裝套件參數中顯示授權帳戶的任何細節。

如須在透過協力廠商工具佈署之前對 Kaspersky 應用程式使用此配置方法的說明，請參閱「使用 Microsoft Windows 群組政策佈署」。

在卡巴斯基安全管理中心安裝之後，一些安裝套件被自動產生；它們可用於安裝並包含網路代理和 Microsoft Windows 安全應用程式套件。

儘管應用程式的產品授權金鑰可在安裝套件內容中設定，建議您避免此產品授權分發方法，因為這樣很容易就獲取對安裝套件的讀取權限。您應該使用自動分發的產品授權金鑰或產品授權金鑰來安裝工作。

MSI 內容和轉換檔案

另一個在 Windows 平台上配置安裝的方法是定義 MSI 內容和轉換檔案。該方法可以被套用到以下情況：

- 當透過 Windows 群組政策安裝時，透過使用一般 Microsoft 工具或其他協力廠商工具處理 Windows 群組政策。
- 當使用旨在處理 Microsoft Installer 格式的安裝程式的協力廠商工具安裝應用程式時。

使用應用程式遠端安裝的協力廠商工具佈署

當任何應用程式遠端安裝工具（例如 Microsoft System Center）都在組織中可用時，可以使用這些工具進行初始化佈署。

必須執行以下操作：

- 選取能最好配合佈署工具的配置應用程式的方法。
- 定義用於同步安裝套件設定修改（透過管理主控台介面）和所選的用於從安裝套件資料佈署應用程式的協力廠商工具的操作的裝置。
- 當從共用資料夾執行安裝時，您必須確保該檔案資源具有足夠容量。

卡巴斯基安全管理中心的遠端安裝工作相關資訊

卡巴斯基安全管理中心提供了遠端安裝應用程式的不同裝置，它們作為遠端安裝工作實現（強制安裝、複製磁碟機映像安裝、透過 Microsoft Windows 群組政策安裝）。您可以為指定管理群組、特定裝置或選擇的裝置建立遠端安裝工作（此類工作顯示在管理主控台的**工作**資料夾中）。當建立工作時，您可以選取安裝套件（網路代理和/或其他應用程式的安裝套件）以用此工作安裝，並指定定義遠端安裝方法的設定。此外，您可以使用遠端安裝精靈，基於遠端安裝工作和結果監控。

管理群組的工作影響指定群組的裝置和所有管理群組子群組的裝置。如果工作中啟用了相應設定，工作包含了群組和其任何子群組中的從屬管理伺服器裝置。

指定裝置的工作在每一次執行時根據分類內容重新整理用戶端裝置清單。如果分類包含連線到從屬管理伺服器的裝置，工作也將在那些裝置上執行。對於那些設定的詳情和安裝方法請參見以下。

若要確保遠端安裝工作在連線到從屬管理伺服器的裝置上成功操作，您必須使用轉發工作提前轉發您工作使用的安裝套件到對應的從屬管理伺服器。

透過擷取和複製裝置映像來佈署

如果您需要安裝網路代理到必須安裝（或重新安裝）作業系統和其他軟體的裝置，您可以使用擷取和複製裝置裝置映像。

若要透過擷取和複製硬碟來執行佈署，請執行以下操作：

1. 建立安裝了作業系統和相關軟體的參考裝置，包含網路代理和安全應用程式。
2. 在裝置上擷取參考映像並透過卡巴斯基安全管理中心專用工作分發該映像到新裝置。

   要擷取和安裝磁碟映像，您可以使用組織網可用協力廠商工具，或者卡巴斯基安全管理中心提供的功能（在弱點和修補程式管理產品授權下）。

當從參考映像佈署裝置時，如果您使用任何協力廠商工具處理磁碟映像，您必須刪除卡巴斯基安全管理中心用以識別受管理裝置的資訊。否則，管理伺服器將不能正確區分透過複製相同映像建立的裝置。

當使用卡巴斯基安全管理中心工具擷取磁碟映像時，該問題被自動解決。

使用協力廠商工具複製磁碟映像

當應用協力廠商工具擷取安裝了網路代理的裝置映像時，使用以下方法之一：

- 建議方法。在參照裝置上安裝網路代理時，會在網路代理服務第一次執行之前擷取裝置映像（因為識別裝置的獨一資訊在網路代理第一次連線到管理伺服器時建立）。之後，直到完成映像擷取作業前，建議您避免執行網路代理服務。
- 在參考裝置上，停止網路代理服務並使用 -dupfix 參數執行 klmover 公用程式。公用程式 klmover 包含在網路代理安裝套件中。在映像擷取操作完成之前請避免任何網路代理服務的執行。
- 請確保 klmover 將使用 -dupfix 參數執行（強制需求）在目的裝置網路代理服務第一次執行之前，在映像佈署後的作業系統第一次啟動時。實用程式 klmover 包含在網路代理安裝套件中。
- 使用網路代理磁碟克隆模式。

如果磁碟機映像被錯誤地複製，則可以解決此問題。

您還可以捕獲未安裝網路代理的裝置的映像。為此，在目標裝置上執行映像部署，然後部署網路代理。如果使用此方法，請使用裝置中的獨立安裝套件提供對網路資料夾的存取權限。

磁碟機映像錯誤複製

如果網路代理磁碟機映像不遵照以下佈署規則複製，一些裝置可能以一個單獨的圖示在管理主控台一起顯示並不斷變換名稱。

您可以使用下列可用方法之一解決該問題：

- 移除網路代理

  該方法最可靠。您必須在錯誤複製映像的裝置上移除網路代理，使用協力廠商工具，然後再次安裝。網路代理無法透過卡巴斯基安全管理中心工具移除，因為管理伺服器工具無法區分錯誤裝置（它們都在管理主控台分享相同的圖示）。

- 使用 "-dupfix" 參數執行 klmover 公用程式

  使用協力廠商工具執行 klmover 公用程式，在網路代理安裝資料夾，使用 "-dupfix" 參數 (klmover -dupfix) 在錯誤（從映像錯誤複製）裝置上執行一次。您無法使用卡巴斯基安全管理中心工具執行公用程式，因為管理伺服器工具無法區分錯誤裝置（它們都在管理主控台分享相同的圖示）。

  然後在您執行公用程式之前刪除顯示錯誤裝置的圖示。

- 最佳化規則以偵測錯誤複製的裝置。

  該方法僅適用於版本 10 Service Pack 1 或更新的管理伺服器和網路代理。

  必須最佳化偵測錯誤複製的網路代理的規則，以便變更裝置 NetBIOS 名稱導致這些網路代理的自動"修復"（假設所有複製的裝置擁有相同的 NetBIOS 名稱）。

  在管理伺服器裝置上，您必須匯入以下顯示的 reg 檔案到登錄檔，然後重新啟動管理伺服器服務。

  - 如果 32-bit 作業系統安裝在管理伺服器裝置：

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

  - 如果 64-bit 作業系統安裝在管理伺服器裝置：

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

使用 Microsoft Windows 群組政策佈署

建議您透過 Microsoft Windows 群組政策執行網路代理初始化佈署，如果滿足以下條件：

- 該裝置是 Active Directory 網域中的成員。
- 佈署方案允許您在開始佈署網路代理到裝置之前，等待下一次目的裝置例行重新啟動（或者您可以強制 Windows 群組政策套用到這些裝置）。

該佈署方案包含以下：

- Microsoft Installer 格式的應用程式分發套件（MSI 套件）位於共用資料夾（目的裝置的 LocalSystem 帳戶對該資料夾具有讀權限）。
- 在 Active Directory 群組政策中，安裝物件被建立用於分發套件。

- 安裝範圍透過指定組織單元 (OU) 和/或安全群組設定，包含目的裝置。
- 目的裝置下一次登入到網域中時（裝置使用者登入到系統之前），所有已安裝的應用程式被檢查。如果未找到應用程式，分發套件從指定在政策中的資源中下載，然後被安裝。

該佈署方案的一個好處就是被分配的應用程式在目的裝置的作業系統正在載入時被安裝，甚至在使用者登入到系統之前。即便有帶有足夠權限的使用者移除了該應用程式，它也將在作業系統下一次重新啟動時被重新安裝。該佈署方案的劣勢是管理員對群組政策所做的變更在裝置重新啟動之前將不會生效（如果不涉及附加工具）。

您可以使用群組政策安裝網路代理和其他應用程式，如果它們的安裝程式是 Windows Installer 格式。

當選取該佈署方案後，您必須評估在應用 Windows 群組政策後，從中複製檔案到裝置的檔案資源負載。

透過卡巴斯基安全管理中心遠端安裝工作處理 Microsoft Windows 政策

透過 Microsoft Windows 群組政策安裝應用程式的最簡單方法，就是在卡巴斯基安全管理中心遠端安裝工作的內容中選取**在 Active Directory 群組政策中指定安裝套件的安裝**選項。此種情況下，您在執行工作時，管理伺服器自動執行以下操作：

- 在 Microsoft Windows 群組政策中建立所需物件。
- 建立專用安全群組，包含目的裝置到這些群組，並為它們分配所選應用程式的安裝。安全群組集將在每一次工作執行時更新，與執行時的裝置輪詢一致。

要使該功能可操作，在工作內容中，指定對 Active Directory 群組政策有寫權限的帳戶。

如果您要透過相同工作安裝網路代理和其他應用程式，選取**在 Active Directory 群組政策中指定安裝套件的安裝**選項將導致應用程式只會針對網路代理在 Active Directory 政策中建立安裝物件。工作中所選的第二個應用程式將透過網路代理工具被安裝，網路代理一旦安裝在裝置就開始安裝。如果您要透過 Windows 群組政策安裝網路代理之外的應用程式，您必須僅為該應用套裝程式建立安裝工作（沒有網路代理封包）。不是每個應用程式都可以使用 Microsoft Windows 群組政策安裝。要尋找此能力，您可以參考安裝應用程式的方法資訊。

如果所需的物件透過卡巴斯基安全管理中心工具被建立在群組政策，卡巴斯基安全管理中心的共用資料夾將被用於安裝套件來源。當排程佈署時，您必須將權衡該資料夾的讀取速度和裝置數量以及要安裝的分發套件大小。最好將卡巴斯基安全管理中心的共用資料夾位於高效能專用檔案儲存區。

除了使用方便，透過卡巴斯基安全管理中心自動建立 Windows 群組政策還有如下好處：當排程網路代理安裝時，您可以輕鬆指定安裝完成後裝置要被自動移動到的卡巴斯基安全管理中心管理群組。您可以在新工作精靈或遠端安裝工作視窗設定中指定該群組。

當透過卡巴斯基安全管理中心處理 Windows 群組政策時，您可以透過建立安全群組為群組政策物件指定裝置。卡巴斯基安全管理中心同步安全群組內容與工作中裝置的目前集。當使用其他工具處理群組政策時，您可以將群組政策物件與所選的 Active Directory OU 直接關聯。

透過 Microsoft Windows 政策獨立安裝應用程式

管理員可以用自己名義在 Windows 群組政策中建立安裝所需的物件。此種情況下，他/她可以提供儲存在卡巴斯基安全管理中心共用資料夾中的套件連結，或者上傳這些套件到專用檔案伺服器並提供相關連結。

可能有以下安裝方案：

- 管理員建立安裝套件並在管理主控台設定其內容。群組政策物件提供卡巴斯基安全管理中心共用資料夾中的套件的 MSI 檔案的連結。
- 管理員建立安裝套件並在管理主控台設定其內容。然後管理員複製卡巴斯基安全管理中心共用資料夾中整個 EXEC 子資料夾到組織專用檔案資源的資料夾。群組政策物件提供組織專用檔案資源子資料夾中的套件的 MSI 檔案的連結。
- 管理員從網際網路下載應用程式分發套件（包括網路代理封包）並將其上傳到組織專用檔案資源。群組政策物件提供組織專用檔案資源子資料夾中的套件的 MSI 檔案的連結。安裝設定透過配置 MSI 內容或透過配置 MST 轉換檔案來定義。

透過卡巴斯基安全管理中心遠端安裝工作的強制佈署

若要執行網路代理或其他應用程式的初始部署，您可以使用卡巴斯基安全管理中心的遠端安裝工作強制安裝選定的安裝套件，前提是每個裝置都有一個具有本機管理員權限的使用者帳戶。

強制安裝也可以在裝置無法被管理伺服器直接存取時套用：例如，裝置在隔離網路中，或者裝置在本機網路但管理伺服器在 DMZ。

在初始部署的情況下，不會安裝網路代理。因此，在遠端安裝工作的設定中，您無法選擇使用網路代理進行應用程式安裝所需的檔案分發。您只能透過管理伺服器或發佈點選擇使用作業系統資源來分發檔案。

管理伺服器服務必須在對目標裝置具有管理權限的帳戶下執行。或者，您可以在遠端安裝工作的設定中指定有權存取 admin$ share 的帳戶。

> 預設情況下，遠端安裝工作被使用執行管理伺服器的帳戶的憑證套用到裝置。需要澄清的是，這是用於存取 admin$ share 的帳戶，而不是執行遠端安裝工作的帳戶。安裝在 LocalSystem 帳戶下進行。

您可以明確指定目的裝置（使用清單），透過選取它們所屬的卡巴斯基安全管理中心管理群組，或透過基於指定標準建立裝置分類。安裝開始時間定義在工作排程中。如果工作內容中啟用了**執行略過的工作**，工作可以在裝置開啟時立即執行，或裝置被移動到目的管理群組時立即執行。

強制安裝套件包括傳送安裝套件到目的裝置、隨後複製檔案到每個目的裝置的 admin$ 資源，和在這些裝置上遠端註冊支援服務。傳送安裝套件到目的裝置透過卡巴斯基安全管理中心的網路互動功能執行。以下條件必須在此種情況下被滿足：

- 目的裝置可從管理伺服器端或分發點端存取。
- 目的裝置的名稱解析在網路中正常運作。
- 裝置上的管理分享 (admin$) 保持啟用。

- 目標裝置上正在執行以下系統服務：
  - 伺服器 (LanmanServer)
    預設情況下，該服務正在執行。
  - DCOM 伺服器處理程序啟動器 (DcomLaunch)
  - RPC Endpoint Mapper (RpcEptMapper)
  - 遠端過程呼叫 (RpcS)
- 目標裝置上開啟了連接埠 TCP 445，以便透過 Windows 管理工具啟用遠端存取。

  TCP 139、UDP 137 和 UDP 138 由舊協定使用，目前應用程式不再需要。

  防火牆上必須允許動態出站存取連接埠，以便實現從管理伺服器和發佈點到目標裝置的連線。
- 在部署網路代理期間，Active Directory 網域政策安全性設定被允許提供 NTLM 協定的操作。
- 在執行 Microsoft Windows XP 的目的裝置上，簡單檔案共用模式被停用。
- 在目標裝置上，存取共用和安全模型被設定為*經典 - 本機使用者以自己的身分進行身分驗證*。它絕不可能是*僅限訪客 - 本機使用者以訪客身分進行身分驗證*。
- 目的裝置是網域成員，或帶有管理員權限的統一帳戶提前在目的裝置上被建立。

若要將網路代理或其他應用程式成功部署到未加入 Windows Server 2003 或更高版本 Active Directory 網域的裝置，必須在該裝置上停用遠端 UAC。遠端 UAC 是阻止本機管理帳戶存取 admin$ 的原因之一，這對於強制部署網路代理或其他應用程式必不可少。停用遠端 UAC 不會影響本機 UAC。

在未配置到任何卡巴斯基安全管理中心管理群組的新裝置上進行安裝時，您可以開啟遠端安裝工作內容並指定網路代理安裝後裝置要移動到的管理群組。

當建立群組工作時，記住每個群組工作都影響所選群組的潛逃群組中的所有裝置。因此，您必須避免在子群組中的重複安裝工作。

建立強制安裝應用程式工作的一種簡化方法是自動安裝。為此，您必須開啟管理群組內容，開啟安裝套件清單，然後選取必須在該群組中的裝置上安裝的套件。結果，所選安裝套件將被自動安裝在該群組和其所有子群組中的所有裝置上。套件被安裝的時間間隔取決於網路吞吐量和網路裝置總數。

為了減少傳送安裝套件到目的裝置期間管理伺服器的負載，您可以在安裝工作中選擇透過發佈點安裝。注意，該安裝方法給作為發佈點的裝置增加了大量負載。因此，建議您選擇符合發佈點要求的裝置。如果您使用發佈點，必須確保它們存在於託管目的裝置的每個隔離子網路中。

使用發佈點作為本機安裝中心也可以用在與管理伺服器具有窄通道通訊的子網路裝置上的安裝，此時子網路中的通道頻寬很高。

資料夾 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit 所在分區的磁碟剩餘空間必須超過所安裝應用程式的分發套件的總大小的好幾倍。

執行卡巴斯基安全管理中心建立的獨立安裝套件

以上敘述的網路代理和其他應用程式的初始化佈署方法無法總被實現，因為不可能滿足所有可套用條件。此種情況下，您可以透過卡巴斯基安全管理中心建立通用可執行檔，叫做*獨立安裝套件*，使用管理員準備的帶有相關安裝設定的安裝套件。獨立安裝套件儲存在卡巴斯基安全管理中心共用資料夾。

您可以使用卡巴斯基安全管理中心來給所選使用者傳送包含該共用資料夾檔案連結的電子郵件，提示他們執行該檔案（在互動模式或靜默模式）。您可以附加獨立安裝套件到電子郵件，然後傳送它到對卡巴斯基安全管理中心共用資料夾沒有存取權限的裝置使用者。管理員也可以複製獨立安裝套件到卸除式磁碟機，將其傳送到相關裝置然後稍後執行。

您可以從網路代理套件或其他應用程式套件建立獨立安裝套件（例如，安全應用程式）。如果獨立安裝套件從網路代理和其他應用程式建立，安裝和網路代理一起啟動。

當建立帶有網路代理的獨立安裝套件時，您可以指定當網路代理安裝完成時，新裝置（未配置到任何管理群組的裝置）將被自動移動到的管理群組。

獨立安裝套件可以在互動模式下執行（預設），顯示應用程式安裝結果，或者可以執行在靜默模式（以參數 "-s" 執行）。靜默模式可以用在從指令碼安裝，例如作業系統映像佈署後要執行的指令碼。靜默模式安裝的結果決定與處理程序返回程式碼。

單機版 Linux 網路代理具有來自 nmap 實用程式的可選相依性。如果 nmap 實用程式缺失或早於版本 6.0，則 Broadcast DHCP Discover 不受支援。

手動安裝應用程式的選項

管理員或資深使用者可以在互動模式下手動安裝應用程式。他們可以使用原始分發套件或從其他建立並儲存在卡巴斯基安全管理中心共用資料夾的安裝套件。預設下，安裝程式在互動模式下執行並提示使用者所需的設定值。然而，當使用參數 "-s" 從安裝套件根目錄執行 setup.exe 處理程序時，安裝程式將執行在靜默模式，使用配置安裝套件時定義的設定。

當從儲存在卡巴斯基安全管理中心共用資料夾的安裝套件的根目錄執行 setup.exe 時，套件先被複製到暫時資料夾，然後應用程式安裝程式將從本機資料夾執行。

建立 MST 檔案

若要轉換 MSI 套件的內容並將自訂設定套用到現有 MSI 檔案，您必須建立 MST 格式的轉換檔案。為此，請使用 Windows SDK 中包含的 Orca.exe 編輯器。

若要建立 MST 檔案：

1. 執行 Orca.exe 編輯器。
2. 轉到**檔案**頁簽，然後在功能表中點擊**開啟**。
3. 選擇 Kaspersky Network Agent.msi 檔案。
4. 轉到**轉換**頁簽，然後在功能表中選擇**新建轉換**。

5. 在**「表格」**列中，選擇**「屬性」**並寫入以下值：

   - *EULA=1*
   - *SERVERADDRESS=<管理伺服器位址>*

   點擊**儲存**按鈕。

6. 轉到**轉換**頁簽，然後在功能表中選擇**產生轉換**。

7. 在開啟的視窗中，指定您建立的轉換檔案的名稱，然後點擊**儲存**按鈕。

MST 檔案已儲存。

在安裝有網路代理的裝置上遠端安裝應用程式

如果連線到主管理伺服器（或任何其從屬管理伺服器）的可操作網路代理被安裝到裝置，您可以升級該裝置上的網路代理，以及透過網路代理安裝、升級或移除支援的應用程式。

您可在遠端安裝工作的內容中，啟用**使用網路代理**選項。

如果選取此選項，具有管理員定義的安裝設定的安裝套件將被透過網路代理和管理伺服器之間的通訊頻道傳輸到目標裝置。

要最佳化管理伺服器負載和最小化管理伺服器和裝置之間的流量，最實用的方法是為每個遠端網路或每個多點群播網域分配發佈點（請參閱「管理發佈點」一節和「建立管理群組結構和分配發佈點」一節）。此種情況下，安裝套件和安裝設定透過發佈點從管理伺服器分發到目的裝置。

而且，您可以使用發佈點來多點群播傳送安裝套件，這將允許您在佈署應用程式時顯著降低網路流量。

當透過網路代理和管理伺服器之間的通訊渠道傳輸安裝套件到目的裝置時，所有準備傳輸的安裝套件都將被快取在 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer 資料夾。當使用多個不同類型的大安裝套件並涉及大量發佈點時，該資料夾的大小將顯著增長。

檔案不能從 FTServer 資料夾手動刪除。當原始安裝套件被刪除時，對應資料將被自動從 FTServer 資料夾刪除。

發佈點接收的資料儲存在資料夾 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp。

檔案不能從 $FTCITmp 資料夾手動刪除。使用該資料夾資料的工作完成後，該資料夾的內容將被永久刪除。

因為安裝套件從中轉儲存區以最佳化傳輸的格式透過管理伺服器與網路代理之間的通訊渠道進行分發，原始資料夾裡的安裝套件不允許變更。這些變更將不會被管理伺服器自動註冊。如果您需要手動修改安裝套件的檔案（儘管建議您避免此方案），您必須在管理主控台編輯安裝套件的任何設定。在管理主控台編輯安裝套件的設定導致管理伺服器在目的裝置傳輸快取中更新安裝套件映像。

在遠端安裝工作中管理裝置重新啟動

裝置經常需要在完成應用程式遠端安裝時重新啟動（尤其在 Windows）。

如果您使用卡巴斯基安全管理中心遠端安裝工作，在新工作精靈或所建立工作的內容視窗（**作業系統重新啟動**區域），您可以選取 Windows 裝置需要重新啟動時的操作：

- **不重新啟動裝置**。此種情況下，自動重新啟動不會執行。要完成安裝，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊將被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的安裝工作。

- **重新啟動裝置**。此種情況下，如果完成安裝需要重新啟動，裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的安裝工作。

- **提示使用者操作**。此種情況下，用戶端裝置上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。**提示使用者操作**最適用於使用者需要選取最合適重新啟動時間的工作站。

安全應用程式安裝套件上的資料庫更新

開始防護佈署之前，您必須注意要隨安全應用程式的分發套件一起更新病毒資料庫（包括模組和自動修補程式）。最好在開始佈署之前更新應用程式安裝套件中的資料庫（例如，透過使用所選安裝套件上下文功能表中的相關指令）。這將減少目的裝置在完成防護佈署後所需的重新啟動次數。

在卡巴斯基安全管理中心中使用工具遠端安裝應用程式以便在受管理裝置上執行相關可執行檔

使用新安裝套件精靈，您可以選取任何可執行檔並為其定義命令列設定。為此，您可以新增所選檔案或整個檔案所在資料夾到安裝套件。然後，您必須建立遠端安裝工作並選取所建立的安裝套件。

當工作正在執行時，帶有命令列所定義設定的指定可執行檔將在目的裝置上執行。

如果您使用 Microsoft Windows Installer (MSI) 格式的安裝程式，卡巴斯基安全管理中心使用標準工具分析安裝結果。

如果有弱點和修補程式管理產品授權可用，卡巴斯基安全管理中心（當為任何企業環境中支援的應用程式建立安裝套件時）也使用安裝和安裝結果分析規則。

否則，可執行檔的預設工作將等待執行中處理程序和所有子處理程序的完成。在所有執行中處理程序完成後，工作將被成功完成，不管初始處理程序的返回碼是什麼。若要變更此工作的這種行為，在建立工作之前，您必須手動修改卡巴斯基安全中心在新建的安裝套件及其子資料夾中產生的 .kpd 檔案。

.kpd 檔案使用 ASCII 編碼。 .kud 檔案使用 Unicode 編碼。

對於不需要等待執行中處理程序完成的工作，設定 [SetupProcessResult] 區域的等待設定的值為 0：

```
[SetupProcessResult]
Wait=0
```

對於僅需要等待 Windows 執行中處理程序，而不是所有子處理程序完成的工作，設定 [SetupProcessResult] 區域的 WaitJob 設定值為 0，例如：

```
[SetupProcessResult]
```

```
WaitJob=0
```

若要工作根據正在執行的處理程序的返回代碼成功完成或者返回錯誤，請建立一個儲存錯誤代碼到檔案的 .bat 檔案，例如：

```
echo [ResponseResult] > setup.log
echo ResultCode=2 >> setup.log
exit 0
```

然後修改卡巴斯基安全管理中心在新建立的安裝套件的資料夾中產生的 .kud 檔案：

```
[SetupMainResult]
File=setup.log
Section=ResponseResult
Value=ResultCode
[SetupMainResult_SuccessCodes]
0=安裝成功完成。
[SetupMainResult_ErrorCodes]
1=安裝指令碼錯誤
2=自訂錯誤
```

此種情況下，任何非清單中的返回碼都會導致返回錯誤。

要在工作成功完成或工作結果錯誤中顯示註釋，在 [SetupProcessResult_SuccessCodes] 和 [SetupProcessResult_ErrorCodes] 區域根據處理程序返回碼輸入錯誤的簡短敘述，例如：

```
[SetupProcessResult_SuccessCodes]
0=安裝成功完成
3010=需要重新啟動以完成安裝
[SetupProcessResult_ErrorCodes]
1602=安裝被使用者取消
1603=安裝過程中出現致命錯誤
```

要使用卡巴斯基安全管理中心工具管理裝置重新啟動（如果需要重新啟動以完成操作），列出暗示重新啟動的處理程序返回碼，在 [SetupProcessResult_NeedReboot] 區域：

```
[SetupProcessResult_NeedReboot]
3010=
```

監控佈署

要監控卡巴斯基安全管理中心佈署和確保安全應用程式和網路代理成功安裝在受管理裝置，您必須在**佈署**區域檢查信號燈。該信號燈位於管理主控台主視窗的管理伺服器節點工作區。信號燈反映了目前佈署狀態。安裝了網路代理和安全應用程式的裝置數量顯示在信號燈旁邊。當任何安裝工作正在執行時，您可以監控它們的處理程序。如果有任何安裝錯誤發生會顯示錯誤數量。您可以透過按連結檢視錯誤詳情。

在**受管理裝置**資料夾的工作區的**群組**頁籤，您也可以使用佈署圖表。圖表反映了佈署處理程序，顯示沒有網路代理、帶有網路代理或帶有網路代理和安全應用程式的裝置數量。

若需更多佈署處理程序（或者特定安裝工作的操作）的詳情，開啟相關遠端安裝工作的結果視窗：點擊工作並在上下文功能表中選取**結果**。視窗顯示了兩個清單：上面一個包含裝置上的工作狀態，下面一個包含從上面清單中選取的裝置上的工作事件。

佈署錯誤的資訊被新增到管理伺服器上的卡巴斯基事件記錄。在**事件**頁籤，也可透過管理伺服器節點中的相關事件分類取得錯誤資訊。

配置安裝程式

該部分提供了卡巴斯基安全管理中心安裝程式檔案和安裝設定的資訊，以及如何在靜默模式安裝管理伺服器和網路代理的建議。

一般資訊

卡巴斯基安全管理中心 14.2 元件（管理伺服器、網路代理和管理主控台）的安裝程式根據 Windows Installer 技術建立。MSI 套件是安裝程式的核心。該格式的套件允許使用 Windows Installer 的所有好處：可量測性、修補程式系統可用性、轉換系統、透過協力廠商解決方案集中安裝以及在作業系統中透明註冊。

在靜默模式下安裝（帶有回應檔案）

管理伺服器和網路代理安裝程式可以使用回應檔案工作 (ss_install.xml)，其中整合了不需要使用者參與的靜默模式安裝參數。ss_install.xml 檔案位於與 MSI 套件相同的資料夾；在靜默模式安裝時被自動使用。您可以使用指令行鍵 "/s" 啟用靜默安裝模式。

一個大概例子執行如下：

```
setup.exe /s
```

在靜默模式中啟動安裝程式之前，請閱讀最終使用者產品授權協議 (EULA)。如果卡巴斯基安全管理中心分發套件不包含帶有 EULA 文字的 TXT 檔案，您可以從卡巴斯基網站下載此檔案。

ss_install.xml 檔案卡巴斯基安全管理中心安裝程式參數的內部格式的實例。分發套件包含帶有預設參數的 ss_install.xml 檔案。

請不要手動修改 ss_install.xml 檔案。該檔案可以透過卡巴斯基安全管理中心工具修改，當在管理主控台編輯安裝套件參數時。

如要修改管理伺服器安裝的回應檔案，請執行以下操作：

1. 開啟卡巴斯基安全管理中心分發套件。如果您是使用完整的套件 EXE 檔案，然後將其解壓縮。
2. 從伺服器資料夾中，開啟命令列，然後執行以下命令：
   ```
   setup.exe /r ss_install.xml
   ```
   卡巴斯基安全管理中心安裝程式啟動。
3. 按照精靈的步驟設定卡巴斯基安全管理中心安裝。

當您完成精靈時，回應檔案會根據您指定的新設定自動修改。

在靜默模式下安裝（沒有回應檔案）

您可以使用單獨 .msi 套件安裝網路代理，以標準方法指定 MSI 內容的值。該方案允許網路代理使用群組政策安裝。

請勿重新命名安裝套件 Kaspersky Network Agent.msi。重新命名此套件可能會在網路代理的未來更新期間導致安裝錯誤。

要避免透過 MSI 套件內容定義的參數與回應檔案中定義的參數衝突，您可以透過設定內容 `DONT_USE_ANSWER_FILE=1` 來停用回應檔案。MSI 檔案位於卡巴斯基安全管理中心分發套件，此項目位於 Packages\NetAgent\exec 資料夾中。一個帶有 .msi 套件的網路代理安裝程式執行例子如下。

在靜默模式中安裝網路代理需要接受最終使用者產品授權協議的條款。只有在您已完整閱讀、瞭解和接受最終使用者產品授權協議的條款，才使用 `EULA=1` 參數。

```
示例：
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1
```

您也可以透過提前準備回應檔案（帶有 .mst 副檔名）來定義 msi 套件的安裝參數。該指令顯示如下：

```
例如：
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

您可以在單一命令列中指定幾個回應檔案。

如果要使用 Windows 安裝程式升級網路代理，請執行下列命令：

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

透過 setup.exe 的部分安裝配置

當透過 setup.exe 執行應用程式安裝時，您可以新增 MSI 任何內容的值到 MSI 套件。

該指令顯示如下：

```
例如：
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

管理伺服器安裝參數

下表敘述了安裝管理伺服器時您可以配置的 MSI 內容。所有參數都是可選的，除了 EULA 和隱私政策。

MSI 內容	敘述	可用值
EULA	是否接受授權協議的條款（必需）。	• 1—我已完整閱讀、瞭解和接受最終使用者產品授權協議的條款。 • 其它值或未指定 – 表示我不接受產品授權協議的條款（將不會執行安裝）。
隱私政策	是否接受隱私政策條款（必需）。	• 1—我瞭解並同意將我的資料進行處理和傳輸(包括向第三國)，如所述於隱私權政策。我確認已完整閱讀並理解隱私權政策。 • 其它值或未指定 – 表示我不接受隱私政策的條款（將不會執行安裝）。
INSTALLATIONMODETYPE	管理伺服器的安裝類型	• 標準 • 自訂
INSTALLDIR	應用程式的安裝資料夾	字串值。
ADDLOCAL	要安裝的元件清單（以逗號分隔）	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. 管理伺服器安裝正常執行的最小元件清單： `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	網路的大小	• NRT_1_100 — 1 to 100 台裝置。 • NRT_100_1000 — 101 到 1000 台裝置。 • NRT_GREATER_1000 —多於 1,000 部裝置。
SRV_ACCOUNT_TYPE	指定操作管理伺服器服務的使用者的方法	• SrvAccountDefault —將自動建立使用者帳戶。 • SrvAccountUser —手動定義使用者帳戶。
SERVERACCOUNTNAME	服務使用者名稱	字串值。
SERVERACCOUNTPWD	服務使用者密碼	字串值。
DBTYPE	資料庫類型	• MySQL – 將使用 MySQL 或 MariaDB 資料庫。 • MSSQL – 將使用 Microsoft SQL Server (SQL Express) 資料庫。
MYSQLSERVERNAME	MySQL Server 或 MariaDB 伺服器完整名稱	字串值。
MYSQLSERVERPORT	連線到 MySQL 或 MariaDB 伺服器連接埠號碼	數值。
MYSQLDBNAME	MySQL 或 MariaDB 伺服器資料庫的名稱	字串值。
MYSQLACCOUNTNAME	連線到 MySQL 或 MariaDB 伺服器資料庫的使用者名稱	字串值。
MYSQLACCOUNTPWD	連線到 MySQL 或 MariaDB 伺服器資料庫的使用者密碼	字串值。
MSSQLCONNECTIONTYPE	MSSQL 資料庫使用類型	• InstallMSSEE – 從套件安裝 • ChooseExisting – 使用已安裝伺服器
MSSQLSERVERNAME	SQL Server 實例的完整名稱	字串值。
MSSQLDBNAME	SQL Server 資料庫名稱	字串值。
MSSQLAUTHTYPE	連線到 SQL Server 的身分驗證方法	• Windows • SQLServer
MSSQLACCOUNTNAME	以 SQLServer 模式連線到 SQL Server 的使用者名稱	字串值。

MSI 內容	敘述	可用值
MSSQLACCOUNTPWD	以 SQLServer 模式連線到 SQL Server 的使用者密碼	字串值。

CREATE_SHARE_TYPE	指定共用資料夾的方法	• Create – 建立新共用資料夾。此種情況下，必須定義以下內容：
		  • SHARELOCALPATH – 本機資料夾路徑
		  • SHAREFOLDERNAME – 資料夾網路名稱
		• Null – EXISTSHAREFOLDERNAME 必須被正確指定

EXISTSHAREFOLDERNAME	現有共用資料夾的完整路徑	字串值。
SERVERPORT	連線至管理伺服器的埠號	數值。
SERVERSSLPORT	建立到管理伺服器的 SSL 連線的埠號	數值。
SERVERADDRESS	管理伺服器位址	字串值。
SERVERCERT2048BITS	管理伺服器憑證金鑰長度（位元）	• 1 – 管理伺服器憑證的金鑰長度為 2048 位元。 • 0 – 管理伺服器憑證的金鑰長度為 1024 位元。 • 如果未指定值，管理伺服器憑證的金鑰長度為 2048 位元。
MOBILESERVERADDRESS	連線行動裝置的管理伺服器位址；如果未選取 MobileSupport 元件則略過	字串值。

網路代理安裝參數

下表敘述了安裝網路代理時您可以配置的 MSI 內容。所有參數都是可選的，除了 EULA 和伺服器位址。

靜默模式下安裝網路代理的參數

MSI 內容	敘述	可用值
EULA	設定是否接受授權協議的條款	• 1—我確認我已完整閱讀、理解並接受此最終使用者產品授權協議的條款和條件。 • 0—表示我不接受產品授權協議的條款（將不會執行安裝）。 • 沒有值—表示我不接受產品授權協議的條款（將不會執行安裝）。
DONT_USE_ANSWER_FILE	從回應檔案讀取安裝設定	• 1—不使用。 • 其他值或沒有值 – 讀取。
INSTALLDIR	網路代理的安裝資料夾路徑	字串值。
SERVERADDRESS	管理伺服器位址（必需）	字串值。
SERVERPORT	連線管理伺服器的埠號	數值。
SERVERSSLPORT	使用 SSL 協定加密連線到管理伺服器的埠號	數值。
USESSL	是否使用 SSL 連線	• 1 – 使用。 • 其它值或未指定 – 不使用。
OPENUDPPORT	是否開啟 UDP 連接埠	• 1 – 開啟。 • 其它值或未指定 – 不開啟。
UDPPORT	UDP 埠號	數值。

MSI 內容	敘述	可用值
USEPROXY	是否使用代理伺服器。 出於相容性目的，不建議在網路代理安裝套件設定中指定代理連線設定。	• 1 – 使用。 • 其它值或未指定 – 不使用。
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	連線到 Proxy 伺服器的 Proxy 位址和埠號	字串值。
PROXYLOGIN	連線代理伺服器的帳戶	字串值。
PROXYPASSWORD	用於連線至代理伺服器的帳戶密碼（請勿在安裝套件的參數中指定權限帳戶的任何詳細資訊）。	字串值。
GATEWAYMODE	連線閘道使用模式	• 0 – 不使用連線閘道。 • 1 – 使用該網路代理作為連線閘道。 • 2 – 使用連線閘道連線到管理伺服器。
GATEWAYADDRESS	連線閘道位址	字串值。
CERTSELECTION	接收憑證的方法	• GetOnFirstConnection – 從管理伺服器接收憑證。 • GetExistent – 如果選中此選項則選取現有憑證，必須指定 CERTFILE 內容。
CERTFILE	憑證檔案路徑	字串值。
VMVDI	啟用虛擬桌面基礎架構 (VDI) 的動態模式	• 1 – 啟用。 • 0 – 不啟用。 • 沒有值 – 不啟用。
VMOPTIMIZE	網路代理設定是否最適用於 hypervisor	• 1 – 啟用。 • 0 – 不啟用。 • 沒有值 – 不啟用。
LAUNCHPROGRAM	安裝後是否啟動網路代理服務。如果 VMVDI=1，則忽略該參數	• 1 – 啟動。 • 其他值或沒有值 – 不啟動。
NAGENTTAGS	網路代理標籤（具有比回應檔案中標籤高的優先順序）	字串值。

虛擬基礎架構

卡巴斯基安全管理中心支援虛擬機的使用。您可以將網路代理和安全應用程式安裝在每台虛擬機器，以及在 hypervisor 級別的虛擬機器防護。在第一種情況下，您可以使用標準安全應用程式或 Kaspersky Security for Virtualization Light Agent 來防護您的虛擬機器。在第二種情況下，您可以使用 Kaspersky Security for Virtualization Agentless。

卡巴斯基安全管理中心支援將虛擬機器回溯到其以前的狀態。

降低虛擬機負載的竅門

當安裝網路代理到虛擬機時，建議您停用一些對虛擬機沒有用的卡巴斯基安全管理中心功能。

當在虛擬機或虛擬機範本上安裝網路代理時，我們建議執行以下操作：

- 如果您正執行遠端安裝，在網路代理安裝套件的內容視窗（在**進階**下），選取**最佳化 VDI 設定**選項。
- 如果您正透過精靈在互動式介面上執行，在精靈視窗，選中**為虛擬架構最佳化網路代理設定**選項。

選中這些選項將改變網路代理設定，因此以下功能保持預設被停用（在套用政策之前）：

- 獲取已安裝軟體的資訊
- 獲取硬體資訊
- 獲取偵測到的弱點資訊
- 獲取需要更新的資訊

通常，這些功能對於虛擬機不必要，因為它們使用統一軟體和虛擬硬體。

停用該功能是不可逆的。如果需要任何被停用的功能，您可以透過網路代理政策啟用它，或透過網路代理本機設定。網路代理本機設定透過管理主控台中相關裝置的上下文功能表可用。

對動態虛擬機的支援

卡巴斯基安全管理中心支援動態虛擬機。如果虛擬架構佈署在組織網路，動態（暫時）虛擬機可以被用在特定情況。動態虛擬機基於管理員提供的範本以獨立名稱建立。使用者工作在虛擬機一定時間，然後關閉虛擬機後，該虛擬機將被從虛擬架構刪除。如果卡巴斯基安全管理中心被佈署在組織網路，安裝了網路代理的虛擬機將被新增到管理伺服器資料庫。在您關閉虛擬機後，對應的項目必須從管理伺服器資料庫中刪除。

要自動刪除虛擬機項目，當安裝網路代理到範本或動態虛擬機時，選取**啟用 VDI 動態模式**選項：

- 對於遠端安裝–在網路代理安裝套件的內容視窗（**進階**區段）
- 對於互動式安裝 – 在網路代理安裝精靈中

> 當安裝網路代理到實體裝置時，不要選取**啟用 VDI 動態模式**選項。

如果您要在刪除虛擬機後將動態虛擬機的事件儲存在管理伺服器一段時間，那麼，在管理伺服器內容視窗，在**事件儲存區**區域，選取**裝置被刪除後儲存事件**選項並指定事件的最大儲存期限（天）。

> 我們不建議在動態虛擬機上啟用加密磁碟機。

對虛擬機複製的支援

複製安裝了網路代理的虛擬機或從安裝了網路代理的範本建立虛擬機，和擷取和複製硬碟磁碟機映像的網路代理佈署相同。因此，一般情況下，當複製虛擬機時，您需要執行與透過複製磁碟映像佈署網路代理時相同的操作。

然而，以下敘述的兩種情況展示了自動偵測複製的網路代理。由於以上原因，您不必執行"透過擷取和複製裝置磁碟映像佈署"中敘述的複雜操作：

- 安裝網路代理時勾選**啟用 VDI 動態模式**選項：在每次重新啟動作業系統後，系統會將此虛擬機視為新裝置，無論此虛擬機是否為複製的虛擬機。
- 以下 hypervisors 之一被使用：VMware™, HyperV®, 或 Xen®：網路代理透過變更的虛擬硬體 ID 偵測虛擬機的複製。

虛擬硬體變更分析並不絕對可靠。在廣泛套用該方法之前，您必須在小組虛擬機上測試您組織中使用的目前 hypervisor 版本。

對網路代理裝置檔案系統回溯的支援

卡巴斯基安全管理中心是一個分發的應用程式。在安裝了網路代理的裝置上回溯檔案系統到先前狀態將導致資料不同步和卡巴斯基安全管理中心功能不正常。

檔案系統（或一部分）可以在以下情況下回溯：

- 當複製硬體磁碟機映像時。
- 當透過虛擬架構還原虛擬機狀態時。
- 當從備份副本或還原點還原資料時。

安裝了網路代理的裝置上的協力廠商軟體影響 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ 資料夾的情景僅是卡巴斯基安全管理中心的關鍵情景。因此，如果可能，您必須總是從還原處理程序中排除該資料夾。

因此一些組織的工作規則提供了對裝置檔案系統的回溯，對安裝了網路代理的裝置的檔案系統回溯的支援被新增到了卡巴斯基安全管理中心，從版本 10 Maintenance Release 1 開始（管理伺服器和網路代理必須是版本 10 Maintenance Release 1 或更新）。當偵測到時，這些裝置被自動連線到管理伺服器，帶有完整資料清除和完整同步。

預設下，對檔案系統回溯偵測的支援在卡巴斯基安全管理中心 14.2 中被啟用。

盡量不要回溯網路代理裝置的 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ 資料夾，因為完整資料的重新同步需要大量資源。

系統狀態回溯在管理伺服器裝置上是不允許的。管理伺服器使用的資料庫的回溯也是不允許的。

您可以僅可以使用標準的 klbackup 公用程式從備份副本還原管理伺服器狀態。

本機安裝應用程式

本章節提供了本機裝置安裝應用程式的流程。

要在所選用戶端裝置上，本機上安裝軟體，您必須擁有此裝置上的管理員權限。

要在所選用戶端裝置上本機安裝應用程式：

1. 在用戶端裝置上安裝網路代理，並且設定網路代理與管理伺服器的連線。

2. 依照這些軟體的手冊在本機上安裝這些軟體。

3. 為每個管理員工作站安裝的應用程式安裝管理外掛程式。

卡巴斯基安全管理中心也支援使用獨立安裝套件在本機上進行安裝應用程式。卡巴斯基安全管理中心不支援所有 Kaspersky 應用程式 的安裝。

網路代理的本機安裝

要在裝置上本機安裝網路代理：

1. 在裝置上，執行從網際網路下載的分發套件中的 setup.exe 檔案。有關詳細信息，請參閱以下主題：從卡巴斯基安全管理中心分發工具包獲取網絡代理安裝套件。

   將開啟 Kaspersky 應用程式選取安裝的提示視窗。

2. 在應用程式分類視窗中，點擊**僅安裝卡巴斯基安全管理中心 14.2 網路代理**連結以啟動網路代理安裝精靈。遵照精靈的說明。

   a. **管理伺服器**

   連接埠

   指定管理伺服器用於接收來自網絡代理的連線的非 SSL 連接埠。

   默認情況下，此選項設定為 14000。

   UDP 連接埠

   指定管理伺服器用於接收來自網絡代理的連線的 SSL 連接埠。

   默認情況下，此選項設定為 13000。

   使用 SSL 連線到管理伺服器

   如果啟用此選項，則使用 SSL 通訊協定透過安全連接埠連線管理伺服器。

   預設情況下已啟用該選項。

   允許網路代理程式開啟 UDP 連接埠

   如果啟用此選項，安裝程式會自動開啟管理伺服器使用的連接埠來管理用戶端裝置並接收有關它的資訊。

   預設情況下已啟用該選項。

   UDP 連接埠

   允許您配置管理伺服器用於管理用戶端裝置並接收有關它的資訊的連接埠。

   預設情況下，此選項設定為 15000。

   b. **代理伺服器設定**

使用代理伺服器

如果啟用此選項，您可以指定代理伺服器身分驗證的憑據。

我們建議您指定僅具有代理伺服器身分驗證所需的最低權限的帳戶的憑據。

預設情況下已停用該選項。

位址

連接埠

帳戶

建立連線代理伺服器的帳戶的使用者名稱。

我們建議您指定僅具有代理伺服器身分驗證所需的最低權限的帳戶的憑據。

密碼

建立連線代理伺服器的帳戶的密碼。

我們建議您指定僅具有代理伺服器身分驗證所需的最低權限的帳戶的憑據。

c. **連線閘道**

不使用連線閘道

使用網路代理作為 DMZ 連線閘道

選擇該選項以使用網路代理作為隔離區 (DMZ) 中的連線閘道，以連線到管理伺服器，與之通訊，以及在資料傳輸過程中保持網路代理上的資料安全。

透過使用連線閘道連線到管理伺服器

選擇此選項，然後指定將充當連線閘道的裝置。

d. **管理伺服器憑證**

e. **代理標籤**

f. **進階設定**

對未定義狀態的元件自動安裝可套用更新和修補程式

我們建議保持此選項啟用。您可以清除此選項以停用卡巴斯基安全管理中心的自動更新和修補。管理員可以稍後使用政策重新啟用自動更新和修補。

預設情況下已停用該選項。

啟用網路代理服務防護

如果啟用該選項，則網路代理被安裝到受管理裝置之後，沒有所需權限元件無法被移除或重新設定。網路代理服務無法被停止。此選項對網域控制器沒有影響。

啟用此選項可防護以本機管理員權限操作的工作站上的網路代理。

預設情況下已停用該選項。

啟用 VDI 動態模式

如果啟用此選項，虛擬機上安裝的網路代理的虛擬桌面基礎架構 (VDI) 動態模式將會啟用。

預設情況下已停用該選項。

最佳化虛擬基礎架構的卡巴斯基安全管理中心網路代理設定。停用弱點掃描以及應用程式和軟體清查。您可以透過網絡代理政策編輯當前設定。

如果啟用此選項，在網路代理設定中將停用以下功能：

- 獲取已安裝軟體的資訊
- 獲取硬體資訊
- 獲取偵測到的弱點資訊
- 獲取需要更新的資訊

預設情況下已停用該選項。

g. **啟動應用程式**

安裝精靈完成後，網路代理被安裝在裝置。

您可以檢視卡巴斯基安全管理中心網路代理服務的內容，您也可以使用標準的 Microsoft Windows 工具（電腦管理\服務）來啟動、停止或監控網路代理活動。

使用靜默模式安裝網路代理

網路代理可以使用靜默模式進行安裝，即沒有安裝設定的互動輸入。靜默安裝會使用網路代理的 Windows 安裝套件 (MSI)。MSI 檔案位於卡巴斯基安全管理中心分發套件，此項目位於 Packages\NetAgent\exec 資料夾中。

請勿重新命名安裝套件 Kaspersky Network Agent.msi。重新命名此套件可能會在網路代理的未來更新期間導致安裝錯誤。

僅可以靜默模式從 MSI 套件安裝網路代理，不支援以互動模式從 MSI 套件進行安裝。

要在靜默模式下將網路代理安裝至本機裝置：

1. 閱讀最終使用者產品授權協議。只有在您理解並接受最終使用者產品授權協議的條款時，才使用以下命令。
2. 執行指令

   ```
   msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters>
   ```

   這裡 `setup_parameters` 是一系列參數，其各自的值用空格隔開 (`PROP1=PROP1VAL PROP2=PROP2VAL`)。

   在參數清單中，您必須包含 `EULA=1`。否則網路代理不會被安裝。

若要對卡巴斯基安全管理中心以及遠端裝置上的網路代理使用標準連線設定，請執行命令：

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` 是寫入記錄的金鑰。該日誌是在網路代理安裝期間建立的，並儲存在 C:\windows\temp\nag_inst.log 中。

除了 nag_inst.log 之外，應用程式還會建立 $klssinstlib.log 檔案，其中包含安裝日誌。此檔案儲存在 %windir%\temp or %temp% 資料夾中。為了進行故障排除，您或 Kaspersky 技術支援專家可能同時需要兩個日誌檔案—nag_inst.log 和 $klssinstlib.log。

若需額外指定連線至管理伺服器的連接埠，請執行命令：

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

參數 `SERVERPORT` 會對應連線至管理伺服器的埠號。

網路代理安裝參數區域的表列出了在靜默模式下安裝網路代理時可用到的參數名稱和可能的值。

如果要使用 Windows 安裝程式升級網路代理，請執行下列命令：

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

以靜默模式安裝適用於 Linux 的網路代理（搭配回應檔案）

您可在 Linux 裝置上使用回應檔案設定檔安裝網路代理，此檔案內含自訂的安裝參數：變數與其各自的值。使用此回應檔案可讓您以靜默模式執行安裝，意即使用者無須參與。

若要以靜默模式安裝適用於 Linux 的網路代理：

1. 為 Linux 裝置做好遠端安裝的準備。透過任何適用的套件管理系統下載並建立遠端安裝套件，例如使用網路代理的 .deb 或 .rpm 套件。

2. 如果您想在裝有 SUSE Linux Enterprise Server 15 作業系統的裝置上安裝網路代理，請首先安裝 insserv-compat 套件配置網路代理。

3. 閱讀最終使用者產品授權協議。只有在您理解並接受最終使用者產品授權協議的條款時，才遵循以下步驟操作。

4. 建立應答檔案（TXT 格式）。將採取 VARIABLE_NAME=variable_value 格式的變數清單（個別列於單獨字行）加入至回應檔案。

   正確使用回應檔案，您必須在其中包含三個必要變數的最小集合：

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   您也可新增任何選用變數來使用您遠端安裝更特定的變數。下表列出可包含在回應檔案中的所有變數：

   回應檔案的變數會作為以靜默模式安裝網路代理的參數使用。

回應檔案的變數會作為以靜默模式安裝網路代理的參數使用。

變數名稱	必要	敘述	可能的值
KLNAGENT_SERVER	是	包含管理伺服器名稱，以完全合格的網域名稱 (FQDN) 或 IP 位址呈現。	DNS 名稱或 IP 位址。
KLNAGENT_AUTOINSTALL	是	定義是否啟用靜默的安裝模式。	1—啟用靜默模式；使用者在安裝期間未收到要採取任何行動的提示。 其他—停用靜默模式；使用者可能會在安裝期間收到要採取行動的提示。
EULA_ACCEPTED	是	定義使用者是否接受網路代理的最終使用者產品授權協議 (EULA)；遺失時，可解讀為未接受 EULA。	1—本人確認已完全閱讀、理解並接受本最終使用者授權協議的條款和條件。 其他值或未指定 — 表示我不接受產品授權協議的條款（將不會執行安裝）。
KLNAGENT_PROXY_USE	否	定義與管理伺服器的連線是否會使用代理設定。預設值是 0。	1—使用代理設定。 其他—未使用代理設定。
KLNAGENT_PROXY_ADDR	否	定義用來與管理伺服器連線的代理伺服器位址。	DNS 名稱或 IP 位址。
KLNAGENT_PROXY_LOGIN	否	定義用來登入代理伺服器的使用者名稱。	任何現有的使用者名稱。
KLNAGENT_PROXY_PASSWORD	否	定義用來登入代理伺服器的使用者密碼。	作業系統中密碼格式允許使用的任何英數字元集。
KLNAGENT_VM_VDI	否	定義網路代理是否已安裝在建立動態虛擬機器的映像檔。	1—網路代理會安裝在映像擋上，這在之後會用來建立動態虛擬機器。 其他—安裝期間沒有使用映像檔。
KLNAGENT_VM_OPTIMIZE	否	定義網路代理設定是否最適用於 hypervisor。	1—網路代理的預設本機設定已修改，以使其最佳運用 hypervisor。
KLNAGENT_TAGS	否	列出指派給網路代理實例的標籤。	由分號區隔的一或多個標籤名稱。
KLNAGENT_UDP_PORT	否	定義由網路代理使用的 UDP 連接埠。預設值是 15000。	任何現有的埠號。
KLNAGENT_PORT	否	定義網路代理使用的非 TLS 連接埠。預設值是 14000。	任何現有的埠號。
KLNAGENT_SSLPORT	否	定義網路代理使用的 TLS 連接埠。預設值是 13000。	任何現有的埠號。
KLNAGENT_USESSL	否	定義連線是否使用傳輸層安全 (TLS)。	1（預設）—使用 TLS。 其他—不使用 TLS。
KLNAGENT_GW_MODE	否	定義是否使用連線閘道。	1（預設）—不修改目前設定（在初次呼叫中，不指定任何連線閘道）。 2—不使用任何連線閘道。 3—使用連線閘道。 4—網路代理實例會在隔離區域 (DMZ) 作為連線閘道使用。
KLNAGENT_GW_新增RESS	否	定義連線閘道的位址。僅在 KLNAGENT_GW_MODE=3 時適用該值。	DNS 名稱或 IP 位址。

5. 執行網路代理安裝。KLAUTOANSWERS 環境變數指定應答檔案的路徑，並傳遞給安裝指令。執行以下指令：

- 要將網路代理從 RPM 套件安裝到 32 位元作業系統，請執行以下命令：
  `sudo KLAUTOANSWERS=<應答檔案路徑> yum install ./klnagent-<內部版本編號>.i386.rpm`
- 要將網路代理從 RPM 套件安裝到 64 位元作業系統，請執行以下命令：
  `sudo KLAUTOANSWERS=<應答檔案路徑> yum install ./klnagent64-<內部版本號>.x86_64.rpm`
- 要將網路代理從 RPM 套件安裝到 Arm 架構的 64 位元作業系統，請執行以下命令：
  `sudo KLAUTOANSWERS=<應答檔案路徑> yum install ./klnagent64-<內部版本號>.aarch64.rpm`
- 要將網路代理從 DEB 套件安裝到 32 位元作業系統，請執行以下命令：
  `sudo KLAUTOANSWERS=<應答檔案路徑> apt install ./klnagent_<內部版本號>_i386.deb`
- 要將網路代理從 DEB 套件安裝到 64 位元作業系統，請執行以下命令：
  `sudo KLAUTOANSWERS=<應答檔案路徑> apt install ./klnagent64_<內部版本號>_amd64.deb`
- 要將網路代理從 DEB 套件安裝到 Arm 架構的 64 位元作業系統，請執行以下命令：
  `sudo KLAUTOANSWERS=<應答檔案路徑> apt install ./klnagent64_<內部版本號>_arm64.deb`

根據作業系統配置，您也可以使用 rpm、dpkg 或 dnf 套件管理器來安裝網路代理。

Linux 的網路代理安裝會以靜默模式啟動；使用者在程序期間不會收到採取任何動作的提示。

以互動模式安裝 Linux 網路代理

本文旨在說明如何透過逐步指定安裝參數的方式，以互動模式在 Linux 裝置上安裝網路代理。相對的，您也可以使用回應檔案，即內含一組自訂安裝參數（變數及其相關值）的文字檔。使用此回應檔案可讓您以靜默模式執行安裝，亦即使用者無須參與。

以互動模式安裝網路代理：

1. 執行網路代理安裝。根據您的 Linux 版本，執行以下命令之一：
   - 要將網路代理從 RPM 套件安裝到 32 位元作業系統，請執行以下命令：
     `# yum -i klnagent-<版本編號>.i386.rpm`
   - 要將網路代理從 RPM 套件安裝到 64 位元作業系統，請執行以下命令：
     `# yum -i klnagent64-<版本編號>.x86_64.rpm`
   - 要將網路代理從 RPM 套件安裝到 Arm 架構的 64 位元作業系統，請執行以下命令：
     `# yum -i klnagent64-<版本編號>.aarch64.rpm`
   - 要將網路代理從 DEB 套件安裝到 32 位元作業系統，請執行以下命令：
     `# apt install ./klnagent_<版本編號>_i386.deb`
   - 要將網路代理從 DEB 套件安裝到 64 位元作業系統，請執行以下命令：
     `# apt install ./klnagent64_<版本編號>_amd64.deb`
   - 要將網路代理從 DEB 套件安裝到 Arm 架構的 64 位元作業系統，請執行以下命令：
     `# apt install ./klnagent64_<版本編號>_arm64.deb`
2. 執行網路代理組態：
   `# /opt/kaspersky/klnagent64/bin/setup/postinstall.pl`

3. 閱讀最終使用者產品授權協議 (EULA)。文字顯示在命令行視窗中。按空格鍵檢視下一個文字段。然後在出現提示時，輸入以下值之一：

   - 輸入 `y`（如果您理解並接受 EULA 的條款）。
   - 輸入 `n`（如果您不接受 EULA 的條款）。若要使用網路代理，您必須接受 EULA 的條款。
   - 輸入 `r` 再次顯示 EULA。

4. 輸入管理伺服器 DNS 名稱或 IP 位址。
5. 輸入管理伺服器連接埠號。預設情況下使用連接埠 14000。
6. 輸入管理伺服器 SSL 連接埠號。預設情況下使用連接埠 13000。
7. 如果想對網路代理和管理伺服器之間的流量使用 SSL 加密，請輸入 `y`。否則，輸入 `n`。
8. 使用下列方式之一設定網路代理：

   - `[1]`：不設定連線閘道。
     您的裝置不會充當連線閘道，也不會透過連線閘道連接到管理伺服器。
   - `[2]`：不使用連線閘道。
     您的裝置將不會透過連線閘道連接到管理伺服器。
   - `[3]`：使用連線閘道連接到伺服器。
     您的裝置將透過連線閘道連接到管理伺服器。
   - `[4]`：用作連線閘道。
     您的裝置將充當連線閘道。

網路代理安裝在 Linux 裝置上。

準備在封閉軟體環境模式下執行 Astra Linux 的裝置以安裝網路代理

在封閉軟體環境模式下執行 Astra Linux 的裝置上安裝網路代理之前，您必須執行兩個準備過程：下面說明中的一個和適用於任何 Linux 裝置的一般準備步驟。

> 在具有 root 權限的帳戶下執行本指令中提供的命令。

準備在封閉軟件環境模式下執行 Astra Linux 的裝置以安裝網路代理：

1. 開啟 `/etc/digsig/digsig_initramfs.conf` 檔案，然後指定以下設定：

   ```
   DIGSIG_ELF_MODE=1
   ```

2. 在指令行中，執行以下指令來安裝相容套件：

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

3. 為應用程式金鑰建立一個目錄：

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. 將應用程式金鑰 /opt/kaspersky/klnagent64/share/kaspersky_astra_pub_key.gpg 放在上一步建立的目錄中：

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   如果卡巴斯基安全管理中心分發套件不包含 kaspersky_astra_pub_key.gpg 應用程式金鑰，您可以點擊以下連接下載：https: //media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg。

5. 更新 RAM 瓷碟：

   ```
   update-initramfs -u -k all
   ```

   重新啟動系統。

Linux 裝置已準備好安裝網路代理。您可以遠端、以互動模式或靜默模式安裝網路代理。

本機安裝應用程式管理外掛程式

若要安裝應用程式管理外掛程式：

在已安裝管理主控台的裝置上執行 klcfginst.exe 可執行檔案，這會包含在應用程式分發套件中。

klcfginst.exe 包含在可透過卡巴斯基安全管理中心管理的所有應用程式裡。安裝過程將由安裝精靈全自動安裝，您無須進行任何手動設定。

以靜默模式安裝應用程式

若要使用靜默模式安裝應用程式，請執行以下操作：

1. 開啟卡巴斯基安全管理中心的應用程式主視窗。
2. 在主控台樹狀目錄的**遠端安裝**資料夾中的**安裝套件**子資料夾，選取相關應用程式的安裝套件，或者為該應用程式建立新安裝套件。

   安裝套件將存放在管理伺服器上的共用資料夾中的"安裝套件服務"資料夾中。個別的套件將會存放在個別的資料夾。

3. 您可以透過以下方式開啟該資料夾：

   - 透過將相關安裝套件對應的資料夾從管理伺服器複製到用戶端裝置。然後在用戶端裝置上開啟複製的資料夾。
   - 透過從用戶端裝置開啟對應於管理伺服器預安裝套件的分享資料夾。

   若共用資料夾位於已安裝 Microsoft Windows Vista 的裝置，您需為**使用者帳戶控制：在管理員核准模式中執行所有管理員**的設定配置**已停用**的值（**開始 → 主控台 → 管理 → 本機安全性原則 → 安全性設定**）。

4. 依照您選取的應用程式，執行以下步驟：

   - 對於 Kaspersky Anti-Virus for Windows Workstations、Kaspersky Anti-Virus for Windows Servers 和卡巴斯基安全管理中心，開啟 exec 子資料夾並用 /s 參數執行可執行檔（帶 .exe 副檔名的檔案）。
   - 對於其他 Kaspersky 應用程式，請在開啟的資料夾中，以 /s 參數執行可執行檔（帶 .exe 副檔名的檔案）。

   使用 `EULA=1` 和 `PRIVACYPOLICY=1` 參數執行可執行檔，代表您完全閱讀、理解並接受最終使用者產品授權協議和隱私權政策的各自條款。您也知道您的資料將受到處理與傳輸（包含傳送至第三國家/地區），如隱私政策所述。產品授權協議和隱私政策的文字檔案包含在卡巴斯基安全管理中心分發套件中。必須接受授權協議和隱私政策的條款才能安裝應用程式或升級上一版本應用程式。

使用獨立安裝套件安裝應用程式

卡巴斯基安全管理中心允許您為應用程式建立獨立安裝套件。獨立安裝套件是可位於網頁伺服器、由電子郵件傳送或已其他方式傳輸至用戶端裝置的可執行檔案。收到的檔案可以在本機用戶端裝置上執行，並且安裝程式不包含卡巴斯基安全管理中心。

單機版 Linux 網路代理具有來自 nmap 實用程式的可選相依性。如果 nmap 實用程式缺失或早於版本 6.0，則 Broadcast DHCP Discover 不受支援。

要使用獨立安裝套件安裝應用程式：

1. 連線到必要的管理伺服器。
2. 在主控台樹狀目錄**遠端安裝**資料夾中，選取**安裝套件**子資料夾。
3. 在安裝套件的畫面中，選取您需要的軟體。
4. 您可以透過以下方式之一，來建立獨立安裝套件：

   - 透過在安裝套件的上下文功能表中選取**建立獨立安裝套件**。
   - 透過點擊在安裝套件的工作區**建立獨立安裝套件**連結。

   獨立安裝套件建立精靈啟動。遵照精靈的說明。

   在精靈的最後一個步驟當中，您可以選取一個方法來將獨立安裝套件傳送到用戶端裝置上。

5. 將獨立安裝套件傳送到用戶端裝置上。
6. 在用戶端裝置上執行獨立安裝套件。

在執行完成獨立安裝套件後，您所指定的應用程式將會安裝在此台裝置上。

當您建立獨立安裝套件時，它會自動發佈在網頁伺服器上。已建立獨立安裝套件清單中將會顯示獨立安裝套件的下載連結。您可以取消發佈選取的獨立安裝套件，也可以重新在網頁伺服器上發佈。預設情況下，使用連接埠 8060 下載獨立安裝套件。

網路代理安裝套件設定

要設定網路代理安裝套件：

1. 在主控台樹狀目錄**遠端安裝**資料夾中，選取**安裝套件**子資料夾。

   遠端安裝資料夾預設是**進階**資料夾的子資料夾。

2. 在網路代理安裝套件的右鍵，選取**內容**。

   「網路代理安裝套件」內容視窗將開啟。

一般

一般區域顯示有關安裝套件的一般資訊：

- 安裝套件名稱
- 為其建立該安裝套件的應用程式的名稱和版本
- 安裝套件大小
- 安裝套件建立日期
- 安裝套件資料夾的路徑

設定

本區域顯示為確保網路代理在安裝後就能正確工作所需的設定。該區域的設定僅在執行 Windows 的裝置上可用。

在**目的資料夾**設定群組，您可以選取安裝網路代理的用戶端裝置。

- **安裝到預設資料夾**

  如果選取該選項，網路代理將安裝在 <磁碟機>:\Program Files\Kaspersky Lab\NetworkAgent folder 資料夾中。如果該資料夾不存在，系統會自動建立。

  預設情況下已選定此選項。

- **安裝到指定資料夾**

  如果選取該選項，則網路代理將安裝到輸入欄位中指定的資料夾中。

在以下設定群組中，您可以設定網路代理遠端移除工作的密碼：

- **使用解除安裝密碼**

  如果啟用此核取方塊，透過按一下**修改**按鈕，您可以輸入移除密碼（僅對執行 Windows 的裝置上的網路代理可用）。

  預設情況下已停用該選項。

- **狀態**

  密碼狀態：**密碼已設定**或**密碼沒有設定**。

  預設情況下，該密碼未指定。

- **防護網路代理服務免遭非授權的移除或終止，並防止設定變更**

  如果啟用該選項，則網路代理被安裝到受管理裝置之後，沒有所需權限元件無法被移除或重新設定。網路代理服務無法被停止。此選項對網域控制器沒有影響。

  啟用此選項可防護以本機管理員權限操作的工作站上的網路代理。

  預設情況下已停用該選項。

- **對未定義狀態的元件自動安裝可套用更新和修補程式**

  如果啟用此選項，將自動安裝管理伺服器、網路代理、管理主控台、Exchange 行動裝置伺服器和 iOS MDM 伺服器適用的所有已下載更新和修補程式。

  如果停用此選項，所有下載的更新和修補程式僅在您變更其狀態到*已批准*後被更新。帶有*未定義*狀態的更新和修補程式將不被安裝。

  預設情況下已啟用該選項。

連線

在該區域中，您可以配置網路代理至管理伺服器的連線。要建立連線，您可以使用 SSL 或 UDP 通訊協定。要配置連線，請指定以下設定：

- **管理伺服器**

  安裝了管理伺服器的裝置位址。

- **連接埠**

  用於連線的埠號。

- **SSL 連接埠**

  用於透過 SSL 協定的連線的埠號。

- **使用伺服器憑證**

  如果該核取方塊被選中，網路代理存取管理伺服器的身分驗證將使用您可以透過按一下**瀏覽**按鈕指定的憑證檔案。

  如果停用此選項，憑證檔案將在網路代理第一次連線到**伺服器位址**欄位指定的位址時從管理伺服器接收。

  我們不建議停用此選項，因為網路代理在連線到管理伺服器時自動接收管理伺服器憑證被認為是不安全的。

  預設情況下已選取此方塊。

- **使用 SSL**

  如果啟用此選項，則使用 SSL 通訊協定透過安全連接埠連線管理伺服器。

  預設情況下已停用該選項。我們建議您不要停用此選項，以便您的連線保持安全。

- **使用 UDP 連接埠**

  如果啟用此選項，網路代理將透過 UDP 連接埠連線至管理伺服器。這將允許管理用戶端裝置並接收有關它們的資訊。

  在安裝了網路代理的受管理裝置上必須開啟 UDP 連接埠。因此，我們建議您不要停用此選項。

  預設情況下已啟用該選項。

- **UDP 連接埠號**

  在該欄位中，可以指定使用 UDP 協定連線管理伺服器到網路代理的連接埠。

  預設 UDP 連接埠 15000。

- **在 Microsoft Windows 防火牆中開啟網路代理連接埠**

  如果啟用此選項，網路代理使用的連接埠將被新增到 Microsoft Windows 防火牆排除項目清單中。

  預設情況下已啟用該選項。

- **使用代理伺服器**

  如果啟用此選項，請指定代理伺服器參數：

  - **代理伺服器位址**
  - **代理伺服器連接埠**

  如果您的代理伺服器需要身分驗證，請啟用**代理伺服器身分驗證**選項並指定與代理伺服器建立連線的帳戶的**使用者名稱**和**密碼**。我們建議您指定僅具有代理伺服器身分驗證所需的最低權限的帳戶的憑據。

出於相容性目的，不建議在網路代理安裝套件設定中指定代理連線設定。

進階

在**進階**部分，您可以配置如何使用連線閘道。為此，您可以進行以下操作：

- 使用網路代理作為非警戒區 (DMZ) 中的連線閘道，以連線到管理伺服器，與之通訊，以及在資料傳輸過程中保持網路代理上的資料安全。
- 透過使用連線閘道連線到管理伺服器以減少與管理伺服器的連線數量。在這種情況下，請在**連線閘道位址**中輸入將充當連線閘道的裝置位址。
- 如果您的網路包含虛擬機，請配置虛擬桌面基礎架構 (VDI) 的連線。為此，進行以下操作：
  - **啟用 VDI 動態模式**

    如果啟用此選項，虛擬機上安裝的網路代理的虛擬桌面基礎架構 (VDI) 動態模式將會啟用。

    預設情況下已停用該選項。
  - **最佳化 VDI 設定**

    如果啟用此選項，在網路代理設定中將停用以下功能：
    - 獲取已安裝軟體的資訊
    - 獲取硬體資訊
    - 獲取偵測到的弱點資訊
    - 獲取需要更新的資訊

    預設情況下已停用該選項。

附加元件

在該區域，您可以為網路代理同時安裝選取附加元件。

標籤

標籤區域顯示網路代理安裝後，可以被新增到用戶端裝置的關鍵字清單。您可以在清單中新增和刪除標籤以及重命名它們。

如果標籤旁的核取方塊被選中，該標籤在網路代理安裝過程中被自動新增到受管理裝置。

如果標籤旁的核取方塊被清空，該標籤在網路代理安裝過程中不被自動新增到受管理裝置。您可以手動新增該標籤到裝置。

當從清單中刪除標籤時，它被自動從所有新增了該標籤的裝置上刪除。

變更歷程

在該區域，您可以檢視安裝套件修訂歷程。您可以比較修訂、檢視修訂、儲存修訂到檔案和新增/編輯修訂敘述。

對特別作業系統可用的網路代理安裝套件設定在下表中給出。

內容區域	Windows	Mac	Linux
一般	✓	✓	✓
設定	✓	—	—
連線	✓	✓ （除了**在 Microsoft Windows 防火牆中開啟網路代理連接埠**和**僅使用自動偵測代理伺服器**選項）	✓ （除了**在 Microsoft Windows 防火牆中開啟網路代理連接埠**和**僅使用自動偵測代理伺服器**選項）
進階	✓	✓	✓
附加元件	✓	✓	✓
標籤	✓	✓ （自動標記規則除外）	✓ （自動標記規則除外）
變更歷程	✓	✓	✓

檢視隱私政策。

您可在 https://www.kaspersky.com/products-and-services-privacy-policy 線上取得隱私政策；您也可以取得離線版本。例如，在安裝網路代理之前，您可以閱讀隱私政策。

若要離線檢視隱私政策：

1. 啟動卡巴斯基安全管理中心安裝程式。
2. 在安裝程式視窗中，前往**擷取安裝軟體套件**連結。
3. 在開啟的清單中，選取卡巴斯基安全管理中心網路代理，然後點擊**下一步**。

privacy_policy.txt 檔案會顯示在裝置上，在您指定的資料夾中的 NetAgent 子資料夾內。

佈署行動裝置管理系統

本章節敘述如何使用 Exchange ActiveSync，iOS MDM，以及 Kaspersky Endpoint Security 協定佈署行動裝置管理系統。

透過 Exchange ActiveSync 協定佈署管理系統

卡巴斯基安全管理中心允許您管理透過 Exchange ActiveSync 協定連線至管理伺服器的行動裝置。Exchange ActiveSync (EAS) 行動裝置已連線到 Exchange 行動裝置伺服器並受管理伺服器管理。

以下作業系統支援 Exchange ActiveSync 協定：

- Windows Phone® 8
- Windows Phone 8.1
- Windows 10 Mobile

- Android
- iOS

Exchange ActiveSync 裝置管理設定集的內容取決于其行動裝置執行的作業系統。有關 Exchange ActiveSync 對應不同作業系統支援度的詳細資訊，請參閱隨附的系統文件。

透過 Exchange ActiveSync 協定佈署管理系統包含以下步驟：

1. 管理員將 Exchange 行動裝置伺服器安裝在所選的用戶端裝置上。
2. 管理員在管理主控台上建立管理設定檔，用於管理 EAS 裝置，並將設定檔新增到 Exchange ActiveSync 使用者的信箱中。

   *Exchange ActiveSync 行動裝置管理設定檔*是 Microsoft Exchange 伺服器上用於管理 Exchange ActiveSync 行動裝置的 ActiveSync 政策。只能將一個 EAS 裝置管理設定檔分配給 Microsoft Exchange 信箱。

   使用者的行動 EAS 裝置連線到他們的 Exchange 信箱。任何管理設定檔都在行動裝置上施加一些限制。

安裝 Exchange ActiveSync 行動裝置伺服器

Exchange 行動裝置伺服器被安裝在安裝了 Microsoft Exchange 伺服器的用戶端裝置上。建議您在分配了用戶端存取角色的 Exchange 伺服器上安裝 Microsoft Exchange 行動裝置伺服器。如果同一網域中有多個帶有用戶端存取伺服器角色的 Exchange 伺服器都合並在陣列中，建議在此叢集模式陣列中每一個 Microsoft Exchange 伺服器上都安裝 Microsoft Exchange 行動裝置伺服器。

要在本機裝置上安裝 Exchange 行動裝置伺服器：

1. 執行 setup.exe 可執行檔。

   將開啟 Kaspersky 應用程式選取安裝的提示視窗。

2. 在程式選取視窗，點擊**安裝 Exchange 行動裝置伺服器**連結執行 Exchange 行動裝置伺服器安裝精靈。

3. 在**安裝設定**視窗選取 Exchange 行動裝置伺服器的安裝類型。

   - 若要使用預設安裝 Exchange 行動裝置伺服器，請選取"**標準安裝**"並點擊"**下一步**"。
   - 要手動定義 Exchange 行動裝置伺服器的安裝設定，選取**自訂安裝**並點擊**下一步**。然後請執行以下操作：

     a. 在**目的資料夾**視窗選取目的資料夾。預設資料夾為 <磁碟機>:\Program Files\Kaspersky Lab\Mobile Device Management for Exchange.。如果這個資料夾不存在，安裝精靈將會自動的產生此資料夾。您可以使用**瀏覽**按鈕變更目的資料夾。

     b. 在**安裝模式**視窗選取 Exchange 行動裝置伺服器安裝類型：一般模式或叢集模式。

     c. 在**選取帳戶**視窗選取用於管理行動裝置的帳戶：

        - **自動建立帳戶與角色群組**。將自動建立帳戶。
        - **指定帳戶**。需要手動指定帳戶。點擊**瀏覽**按鈕，選取使用者帳戶並指定密碼。選取的使用者所屬的群組必須具有透過 ActiveSync 管理行動裝置的權限。

     d. 在 **IIS 設定**視窗，啟用或停用網際網路資訊服務 (IIS) web 伺服器內容的自動設定。

        如果您禁止了 IIS 內容的自動配置，請在 Microsoft PowerShell 虛擬目錄的 IIS 設定中手動啟用 "Windows 身分認證"機制。如果停用了"Windows 身分驗證"機制，Exchange 行動裝置伺服器將不能正常運作。關於設定 IIS 的更多資訊請參閱 IIS 檔案。

     e. 點擊"**下一步**"。

4. 在開啟的視窗中，驗證 Exchange 行動裝置伺服器安裝內容，然後點擊**安裝**。

   當精靈完成後，Exchange 行動裝置伺服器即安裝在本機裝置上了。Exchange 行動裝置伺服器將顯示在主控台樹狀目錄中"**行動裝置管理**"資料夾下。

連線行動裝置到 Exchange 行動裝置伺服器

在任何行動裝置連線之前，您必須設定 Microsoft Exchange 伺服器以允許裝置透過 ActiveSync 協定同步。

要將行動裝置連線到 Exchange 行動裝置伺服器，使用者透過使用 ActiveSync 從行動裝置連線到他或她的 Microsoft Exchange 信箱。連線時，使用者必須在 ActiveSync 用戶端指定連線設定，如電子郵件信箱和信箱密碼。

連線至 Microsoft Exchange 伺服器的使用者行動裝置會顯示在**行動裝置**子資料夾中，此資料夾位於主控台樹狀目錄的**行動裝置管理**資料夾內。

當 Exchange ActiveSync 行動裝置連線到 Exchange 行動裝置伺服器後，管理員可以管理所連線的 Exchange ActiveSync 行動裝置。

設定 Internet Information Services Web 伺服器

當使用 Microsoft Exchange Server（版本 2010 和 2013）時，您必須在 Internet Information Services (IIS) Web 伺服器設定中啟動 Windows PowerShell™ 的 Windows 身分驗證裝置。如果在 Exchange 行動裝置伺服器部署精靈中選取了**自動組態 Microsoft 網際網路資訊服務 (IIS)**選項（預設選項），則會自動啟動該身分驗證機制。

否則，您將必須自己啟動身分驗證裝置。

要手動為 PowerShell 虛擬目錄啟動 Windows 身分驗證裝置：

1. 在 Internet Information Services (IIS) 管理主控台，開啟 PowerShell 虛擬目錄內容。
2. 轉到**身分驗證**區域。
3. 選取 **Microsoft Windows 身分驗證**，然後按一下**啟用**按鈕。
4. 開啟**進階設定**。
5. 選取**啟用 Kernel-mode 身分驗證**選項。
6. 在**延伸防護**下拉清單，選取**必要**。

當使用 Microsoft Exchange Server 2007 時，IIS Web 伺服器不需要設定。

Exchange 行動裝置伺服器的本機安裝

對於 Exchange 行動裝置伺服器的本機安裝，管理員必須執行以下操作：

1. 從卡巴斯基安全管理中心分發套件複製 \Server\Packages\MDM4Exchange\ 資料夾的內容到用戶端裝置。
2. 執行 setup.exe 可執行檔。

本機安裝套件含兩種安裝：

- 標準安裝是不需要管理員定義任何設定的簡單安裝；在多數情況下被建議。
- 延伸安裝是需要管理員定義以下設定的安裝：
  - Exchange 行動裝置伺服器安裝路徑。
  - Exchange 行動裝置伺服器操作模式：標準模式或叢集模式。
  - 指定帳戶以用來執行 Exchange 行動裝置伺服器的可能性。
  - 啟用/停用 IIS Web 伺服器自動配置。

Exchange 行動裝置伺服器佈署精靈必須在具有所有必要權限的帳戶下執行。

Exchange 行動裝置伺服器的遠端安裝

如要設定 Exchange 行動裝置伺服器的遠端安裝，管理員必須執行以下操作：

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**遠端安裝**資料夾，接著選取**安裝套件**子資料夾。
2. 在**安裝套件**子資料夾，開啟 **Exchange 行動裝置伺服器外掛程式**套件的內容。
3. 轉到**設定**區域。
   該區域包含與用於應用程式本機安裝的設定相同的設定。

配置遠端安裝後，您可以開始安裝 Exchange 行動裝置伺服器。

如要安裝 Exchange 行動裝置伺服器，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**遠端安裝**資料夾，接著選取**安裝套件**子資料夾。
2. 在**安裝套件**子資料夾，選取 **Exchange 行動裝置伺服器外掛程式**套件。
3. 在套件的上下文功能表中，選取**安裝應用程式**。
4. 在開啟的遠端安裝精靈中，選取裝置（或為在叢集中安裝選取多個裝置）。
5. 在**在指定的帳戶下執行程式安裝精靈**欄位，指定在遠端裝置上執行應用程式安裝的帳戶。

   帳戶必須具有所需權限。

使用 iOS MDM 協定佈署管理系統

卡巴斯基安全管理中心可讓您管理執行 iOS 的行動裝置。iOS MDM 行動裝置是已連線至 iOS MDM 伺服器並且受到管理伺服器管理的 iOS 行動裝置。

行動裝置透過以下步驟連線到 iOS MDM 伺服器：

1. 管理員安裝 iOS MDM 伺服器。
2. 管理員獲得 Apple 推播通知服務 (APNs) 憑證（接收 APNs 憑證，https://support.kaspersky.com/help/KSMM/4.1/en-US/64900.htm ）。

   APNs 憑證可讓管理伺服器連線至 APNs 伺服器來傳送派送通知至 iOS MDM 裝置。
3. 管理員安裝 APNs 憑證到 iOS MDM 伺服器。
4. 管理員為 iOS 行動裝置的使用者建立 iOS MDM 設定檔。

   iOS MDM 設定檔包含將 iOS 行動裝置連線至管理伺服器的相關設定。

安裝 iOS MDM 設定檔並且在 iOS MDM 裝置已與管理伺服器同步後，裝置會顯示在**行動裝置**資料夾中，它是在主控台樹狀目錄中**行動裝置管理**資料夾的子資料夾。

安裝 iOS MDM 伺服器

要在本機裝置上安裝 iOS MDM 伺服器：

1. 執行 setup.exe 可執行檔。

   將開啟 Kaspersky 應用程式選取安裝的提示視窗。

   在程式選取視窗，點擊**安裝 iOS MDM 伺服器**連結執行 iOS MDM 伺服器安裝精靈。
2. 安裝精靈會請您選取安裝的資料夾位置。

   預設目的資料夾為 <磁碟機>:\Program Files\Kaspersky\Mobile Device Management for iOS。如果這個資料夾不存在，安裝精靈將會自動的產生此資料夾。您可以使用**瀏覽**按鈕變更目的資料夾。

3. 在精靈的**指定連線 iOS MDM 伺服器的設定**視窗中的**連線 iOS MDM 服務的外部連接埠**欄位，指定用於將行動裝置連線至 iOS MDM 服務的外部連接埠。

   行動裝置使用外部連接埠 5223 與 APN 伺服器進行通訊。確保在防火牆中連接埠 5223 被開啟，連線位址範圍為 17.0.0.0/8。

   連接埠 443 預設用於連線到 iOS MDM 伺服器。如果連接埠 443 已經由另一個服務或應用程式使用，它可以被其他連接埠取代，例如，連接埠 9443。

   iOS MDM 伺服器使用外部連接埠 2197 將通知傳送到 APNs 伺服器。

   APNs 伺服器執行在負載均衡模式。行動裝置不總是連線到相同的 IP 位址接收通知。位址範圍 17.0.0.0/8 是為 Apple 留的，這就是為什麼建議在防火牆設定中指定整個範圍為允許範圍。

4. 如果您想為程式元件設定互動連接埠，請選定**手動設定本機連接埠**選項，並指定以下設定的值：

   - **連線到網路代理的連接埠**。在此欄位中，指定用於將 iOS MDM 服務連線到網路代理的連接埠。預設埠號為 9799。
   - **連線到 iOS MDM 服務的本機連接埠**。在此欄位中，指定用於將網路代理連線到 iOS MDM 服務的本機連接埠。預設埠號為 9899。

   > 我們建議使用以上的預設值。

5. 在精靈的**行動裝置伺服器外部位址**視窗中的**遠端連線到行動裝置伺服器的網址**欄位，指定要安裝 iOS MDM 伺服器的用戶端裝置。

   此位址將用於連線受管理行動裝置到 iOS MDM 服務。此用戶端裝置必須是可以讓 iOS MDM 裝置連線到的。

   您可用以下任意方式指定用戶端裝置位址：

   - 裝置 FQDN（例如 mdm.example.com）
   - 裝置 NetBIOS 名稱

   > 您無需在位址區段新增 URL 格式或埠號：這些值會自動新增。

當精靈完成時，iOS MDM 伺服器被安裝到用戶端裝置。iOS MDM 伺服器顯示在主控台樹狀目錄“**行動裝置管理**”資料夾中。

在靜默模式安裝 iOS MDM 伺服器

卡巴斯基安全管理中心允許您在靜默模式下安裝 iOS MDM 伺服器到本機裝置，即沒有安裝設定的互動輸入。

要在靜默模式下安裝 iOS MDM 伺服器到本機裝置：

1. 閱讀最終使用者產品授權協議。只有在您理解並接受最終使用者產品授權協議的條款時，才使用以下命令。

2. 執行以下指令：

   ```
   .\exec\setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 <安裝參數>"
   ```

   其中"安裝參數"是一系列設定，其各自的值用空格隔開 (PROP1=PROP1VAL PROP2=PROP2VAL)。setup.exe 檔案位於伺服器資料夾，它是卡巴斯基安全管理中心分發套件的一部分。

以下清單列出了在靜默模式下安裝 iOS MDM 伺服器時可使用的參數名稱和可能的值。參數可以按任何順序指定。

參數名稱	參數敘述	可用值
EULA	是否接受最終使用者產品授權協議條款。該參數是必須的。	• 1 – 我已完整閱讀、瞭解和接受最終使用者產品授權協議的條款。 • 其它值或未指定 – 表示我不接受產品授權協議的條款（將不會執行安裝）。
DONT_USE_ANSWER_FILE	是否在 iOS MDM 伺服器安裝設定中使用 XML 檔案。 XML 檔案包含在安裝套件或儲存在管理伺服器。您不必指定檔案的額外路徑。 該參數是必須的。	• 1–不使用 XML 參數檔案。 • 其它值，或未定義值–使用 XML 參數檔案。
INSTALLDIR	iOS MDM 伺服器安裝資料夾。 該參數是可選的。	字串值，例如 `INSTALLDIR=\"C:\install\"`
CONNECTORPORT	連線 iOS MDM 服務到網路代理的本機連接埠。 預設埠號為 9799。 該參數是可選的。	數值。
LOCALSERVERPORT	連線網路代理到 iOS MDM 服務的本機連接埠。 預設埠號為 9899。 該參數是可選的。	數值。
EXTERNALSERVERPORT	連線裝置到 iOS MDM 伺服器的連接埠。 預設埠號為 443。 該參數是可選的。	數值。
EXTERNAL_SERVER_URL	要安裝 iOS MDM 伺服器的用戶端裝置的外部位址。此位址將用於連線受管理行動裝置到 iOS MDM 服務。此用戶端裝置必須可用於透過 iOS MDM 連線。 位址不能包含網址和埠號，因為這些值將被自動新增。 該參數是可選的。	• 裝置 FQDN（例如 mdm.example.com） • 裝置 NetBIOS 名稱 • 裝置 IP 位址
WORKFOLDER	iOS MDM 伺服器工作資料夾。 如果未指定工作資料夾，資料將被寫入預設資料夾。 該參數是可選的。	字串值，例如 `WORKFOLDER=\"C:\work\"`
MTNCY	多個虛擬伺服器使用 iOS MDM 伺服器。 該參數是可選的。	• 1–iOS MDM 伺服器將被多個虛擬管理伺服器使用。 • 其它值，或未定義值–iOS MDM 伺服器將不被多個虛擬管理伺服器使用。

例如：

```
\exec\setup.exe /s /v"EULA=1 DONT_USE_ANSWER_FILE=1 EXTERNALSERVERPORT=9443 EXTERNAL_SERVER_URL=\"www.test-mdm.com\""
```

iOS MDM 伺服器安裝參數在安裝 iOS MDM 伺服器部分給出。

iOS MDM 伺服器佈署方案

要安裝的 iOS MDM 伺服器副本數量可以基於可用硬體或所覆蓋的行動裝置總數來選取。

記住，對於單一 Kaspersky Device Management for iOS 的安裝所建議的最大行動裝置數量是 50,000。為了降低負載，裝置輪詢可以在幾個安裝了 iOS MDM 的伺服器上分發。

iOS MDM 裝置的身分驗證透過使用者憑證執行（任何安裝在裝置上的設定檔都包含裝置所有者的憑證）。因此，iOS MDM 伺服器佈署擁有兩個佈署方案：

- 簡易方案
- 涉及 Kerberos constrained delegation (KCD) 的佈署方案

簡易佈署方案

當在簡易方案下佈署 iOS MDM 伺服器時，行動裝置直接連線到 iOS MDM Web 服務。此種情況下，管理伺服器發佈的使用者憑證僅可以被套用與裝置身分驗證。與公共金鑰基礎架構 (PKI) 的整合對使用者憑證不可用。

涉及 Kerberos constrained delegation (KCD) 的佈署方案

若要使用具有 Kerberos 約束委派 (KCD) 的部署方案，必須符合下列要求：

- 管理伺服器和 iOS MDM 伺服器位於組織的內部網路上。
- 正在使用支援 KCD 的反向代理。

此佈署方案提供以下內容：

- 與支援 KCD 的反向代理整合
- 使用 KCD 對行動裝置做身分驗證
- 與 PKI 整合以套用使用者憑證

當使用該佈署方案時，您必須做以下操作：

- 在管理主控台，在 iOS MDM Web 服務設定中，選取**確認與 Kerberos Constrained Delegation 相容**核取方塊。
- 作為 iOS MDM Web 服務的憑證，指定當 iOS MDM Web 服務發佈在反向代理上時定義的自訂憑證。
- iOS 裝置的使用者憑證必須由網域中的 Certificate Authority (CA) 發佈。如果網域包含多個根 CAs，使用者憑證必須由當 iOS MDM Web 服務發佈在反向代理上時指定的 CA 發佈。

  您可以透過以下方法確保使用者憑證與 CA 發佈需求相容：

  - 在新 iOS MDM 設定檔精靈和憑證安裝精靈中指定使用者憑證。
  - 將管理伺服器與網域的 PKI 整合並在憑證發佈規則中定義對應的設定：

    1. 在主控台樹狀目錄中，延伸**行動裝置管理**資料夾並選擇**憑證**子資料夾。
    2. 在**憑證**資料夾中點擊**配置憑證發佈規則**按鈕，開啟**憑證發佈規則**視窗。
    3. 在**與 PKI 整合**區域，配置與公共金鑰基礎架構的整合。
    4. 在**行動憑證發佈**區域，指定憑證來源。

以下是使用以下假定設定 Kerberos Constrained Delegation (KCD) 的例子：

- iOS MDM Web 服務正執行在連接埠 443。
- 具有反向代理的裝置的名稱是firewall.mydom.local。
- iOS MDM Web 服務裝置名稱是 iosmdm.mydom.local。
- iOS MDM Web 服務的外部發佈名稱是 iosmdm.mydom.global。

http/iosmdm.mydom.local 的服務主體名稱

在網域中，您必須為 iOS MDM Web 服務裝置註冊服務主體名稱 (SPN) (iosmdm.mydom.local)：

```
setspn -a http/iosmdm.mydom.local iosmdm
```

配置具有反向代理的裝置的網域內容 (firewall.mydom.local)

要授權流量，信任反向代理裝置 (tmg.mydom.local) 到由 SPN 定義的服務 (http/iosmdm.mydom.local)。

要信任反向代理裝置 (tmg.mydom.local) 到由 SPN 定義的服務 (http/iosmdm.mydom.local)，管理員必須執行以下操作：

1. 在名稱為「Active Directory 使用者和電腦」的 Microsoft Management Console 中，選取安裝了反向代理的裝置 (firewall.mydom.local)。
2. 在裝置內容視窗，在**授權**頁籤，設定**信任此電腦到指定服務的授權**轉換鍵到**使用任何身分驗證協議**。
3. 新增 SPN (http/iosmdm.mydom.local) 到**該帳戶可以展示已授權憑證的服務**清單。

已發佈 Web 服務的特殊（自訂）憑證 (iosmdm.mydom.global)

您必須在 FQDN iosmdm.mydom.global 上為 iOS MDM Web 服務發佈特殊（自訂）憑證，並在管理主控台的 iOS MDM Web 服務設定中指定它取代預設憑證。

請注意憑證容器（帶有 p12 或 .pfx 副檔名的檔案）必須也包含根憑證鏈（公共金鑰）。

在反向代理上發佈 iOS MDM Web 服務

在反向代理上，對於從行動裝置到 iosmdm.mydom.global 連接埠 443 的流量，您必須在 SPN (http/iosmdm.mydom.local) 上配置 KCD，使用為 FQDN (iosmdm.mydom.global) 發佈的憑證。請注意，正發佈和已發佈的 Web 服務必須共用相同的伺服器憑證。

接收 APN 憑證

如果您已經有 APNs 憑證，請考慮續約它而不是建立一個新的。當您將現有的 APNs 憑證替換為新建立的憑證時，管理伺服器將失去對當前連線的 iOS 行動裝置的管理能力。

當在 APNs 憑證精靈第一步中建立憑證簽署請求 (CSR)，其私密金鑰將儲存在您裝置的記憶體中。因此，所有的精靈步驟必須在應用程式的單次工作階段中完成。

要安裝 APN 憑證，請執行以下操作：

1. 在主控台樹狀目錄**行動裝置管理**資料夾中，選取**行動裝置伺服器**子資料夾。
2. 在**行動裝置伺服器**資料夾的工作區中，選取 iOS MDM 伺服器。
3. 在 iOS MDM 伺服器的上下文功能表中，選取**"內容"**。
   這將開啟 iOS MDM 伺服器的"內容"視窗。
4. 在 iOS MDM 伺服器的"內容"視窗中，選取**"憑證"**區域。
5. 在**憑證**區域的**Apple 推送通知憑證**設定群組中，點擊**請求新憑證**按鈕。
   接收 APNs 憑證精靈啟動，**請求新憑證**視窗隨即開啟。
6. 建立憑證簽章請求 (CSR)。若要完成此項目，請執行以下操作：
   a. 點擊**"建立 CSR"**按鈕。
   b. 在開啟的**"建立 CSR"**視窗中，指定一個請求名稱，包含公司和部門的名稱、您所在的城市、區域和國家。
   c. 點擊**"儲存"**按鈕，並指定儲存您的 CSR 的檔案名稱。

   憑證的私密金鑰將儲存在裝置的記憶體中。
7. 使用您的 CompanyAccount 傳送已建立的帶有符號的 CSR 檔案到 Kaspersky。

   > 僅當您在 CompanyAccount 入口網站上上傳了允許使用行動裝置管理的金鑰，您的 CSR 的簽章才可使用。

   在您的線上請求處理程序中，您將收到由 Kaspersky 簽章的 CSR 檔案。

8. 使用隨機的 Apple ID 將簽章的 CSR 檔案傳送至 Apple Inc. 網站。

> 我們建議您避免使用個人的 Apple ID。可建立一個專用 Apple ID 作為企業 ID。在您建立完 Apple ID 後，請連線至公司的信箱。（不要連線到員工的信箱）。

您的 CSR 經由 Apple Inc. 處理後，您將收到 APNs 憑證的公開金鑰。儲存檔案至磁碟。

9. 連同產生 CSR 時建立的私密金鑰一起匯出 APNs 憑證檔案，格式為 PFX。若要這麼做：

   a. 在**需要新的 APNs 憑證**視窗中，點擊**完成 CSR**按鈕。

   b. 在**"開啟"**視窗中，選取從 Apple Inc.（由於 CSR 處理）收到的包含憑證公開金鑰的檔案，然後點擊**"開啟"**視窗。

      憑證匯出處理程序將開始。

   c. 在下一個視窗中，輸入私密金鑰密碼並點擊**確定**。

      該密碼將被用於在 iOS MDM 伺服器上的 APNs 憑證安裝。

   d. 在**儲存 APNs 憑證**視窗，指定 APNs 憑證檔案名稱，選擇資料夾並點擊**儲存**。

憑證的私密金鑰和公開金鑰會組合起來，APNs 憑證將儲存為 PFX 格式。此後，您可以安裝 APNs 憑證到 iOS MDM 伺服器。

續約 APN 憑證

要續約 APN 憑證，請執行以下操作：

1. 在主控台樹狀目錄**行動裝置管理**資料夾中，選取**行動裝置伺服器**子資料夾。
2. 在**行動裝置伺服器**資料夾的工作區中，選取 iOS MDM 伺服器。
3. 在 iOS MDM 伺服器的上下文功能表中，選取**"內容"**。
   這將開啟 iOS MDM 伺服器的"內容"視窗。
4. 在 iOS MDM 伺服器的"內容"視窗中，選取**"憑證"**區域。
5. 在**憑證**區域的**Apple 推送通知憑證**設定群組中，點擊**續約**按鈕。
   APNs 憑證續約精靈啟動，**續約 APNs 憑證**視窗隨即開啟。
6. 建立憑證簽章請求 (CSR)。若要完成此項目，請執行以下操作：

   a. 點擊**"建立 CSR"**按鈕。

   b. 在開啟的**"建立 CSR"**視窗中，指定一個請求名稱，包含公司和部門的名稱、您所在的城市、區域和國家。

   c. 點擊**"儲存"**按鈕，並指定儲存您的 CSR 的檔案名稱。

   憑證的私密金鑰將儲存在裝置的記憶體中。

7. 使用您的 CompanyAccount 傳送已建立的帶有符號的 CSR 檔案到 Kaspersky。

   僅當您在 CompanyAccount 入口網站上上傳了允許使用行動裝置管理的金鑰，您的 CSR 的簽章才可使用。

   在您的線上請求處理程序中，您將收到由 Kaspersky 簽章的 CSR 檔案。

8. 使用隨機的 Apple ID 將簽章的 CSR 檔案傳送至 Apple Inc. 網站。

   我們建議您避免使用個人的 Apple ID。可建立一個專用 Apple ID 作為企業 ID。在您建立完 Apple ID 後，請連線至公司的信箱。（不要連線到員工的信箱）。

   您的 CSR 經由 Apple Inc. 處理後，您將收到 APNs 憑證的公開金鑰。儲存檔案至磁碟。

9. 請求憑證的公共金鑰。若要完成此項目，請執行以下操作：

   a. 轉到蘋果推送憑證入口。要登入到入口，使用在憑證初始化請求時接收到的 Apple ID。

   b. 在憑證清單中，選取其中的 APSP 名稱與 iOS MDM 伺服器使用的憑證 APSP 名稱相符的憑證（格式為"APSP: <號碼>"），並點擊**續約**按鈕。

      APNs 憑證被續約。

   c. 儲存在入口上建立的憑證。

10. 連同產生 CSR 時建立的私密金鑰一起匯出 APNs 憑證檔案，格式為 PFX。若要完成此項目，請執行以下操作：

    a. 在**續約 APNs 憑證**視窗中，點擊**完成 CSR**按鈕。

    b. 在**開啟**視窗，選取從 Apple Inc. 的 CSR 中收到的憑證公開金鑰檔案，並點擊**開啟**視窗。

       將開始進行憑證匯出。

    c. 在下一個視窗中，輸入私密金鑰密碼並點擊**確定**。

       該密碼將被用於在 iOS MDM 伺服器上的 APNs 憑證安裝。

    d. 在開啟的**續約 APNs 憑證**視窗，指定 APNs 憑證檔案名稱，選取資料夾並點擊**儲存**。

憑證的私密金鑰和公開金鑰會組合起來，APNs 憑證將儲存為 PFX 格式。

配置備用 iOS MDM 伺服器憑證

iOS MDM 伺服器功能使您可以簽發預留憑證。此憑證旨在用於 iOS MDM 設定檔中，以確保在 iOS MDM 伺服器憑證過期後無縫切換受管理的 iOS 裝置。

如果您的 iOS MDM 伺服器使用 Kaspersky 簽發的預設憑證，則可以在 iOS MDM 伺服器憑證過期之前簽發預留憑證（或將您自己的自訂憑證指定為預留憑證）。預設情況下，iOS MDM 伺服器憑證到期前 60 天會自動簽發預留憑證。保留的 iOS MDM 伺服器憑證在 iOS MDM 伺服器憑證到期後立即成為主憑證。透過配置組態設定檔將公共金鑰分發給所有受管理裝置，因此您不必手動傳輸它。

要簽發 iOS MDM 伺服器預留憑證或指定自訂預留憑證，請執行以下操作：

1. 在主控台樹狀目錄中的**行動裝置管理**資料夾，選取**行動裝置伺服器**子資料夾。
2. 在「行動裝置伺服器」清單中，選取相關的 iOS MDM 伺服器，然後在右窗格中點擊**配置 iOS MDM 伺服器**按鈕。
3. 在開啟的iOS MDM 伺服器設定視窗中，選取**憑證**區段。
4. 在**預留憑證**區段，執行以下其中一種操作：
   - 如果您打算繼續使用自簽名憑證（意即由 Kaspersky 簽發的憑證）：
     a. 點擊**發佈**按鈕。
     b. 在**啟動日期**開啟的視窗中，選取兩個日期中必須套用預留憑證的日期之一：
        - 如果要在目前憑證到期時套用預留憑證，請選取**目前憑證到期時**選項。
        - 如果要在目前憑證過期之前套用預留憑證，請選取**指定期間後（天）**選項。在此選項旁邊的輸入欄位中，指定預留憑證必須取代目前憑證的期限。

       > 您指定的預留憑證有效期不能超過目前 iOS MDM 伺服器憑證的有效期。

     c. 點擊**確定**按鈕。

     iOS MDM 伺服器憑證已簽發。
   - 如果您打算使用由憑證簽發機構簽發的自訂憑證，請執行以下操作：
     a. 點擊**新增**按鈕。
     b. 在開啟的「檔案總管」視窗中，以 PEM、PFX 或 P12 格式指定憑證檔案，該憑證檔案儲存在裝置中，然後按一下**開啟**按鈕。

     您的自訂憑證被指定為預留的 iOS MDM 伺服器憑證。

您已指定了預留的 iOS MDM 伺服器憑證。預留憑證的詳細資訊會顯示在設定的**預留憑證**區塊中（憑證名稱、簽發者名稱、到期日期以及必須套用預留憑證的日期（若有））。

安裝 APN 憑證到 iOS MDM 伺服器

收到 APNs 憑證後，您必須將其安裝至 iOS MDM 伺服器。

要安裝 APNs 憑證到 iOS MDM 伺服器：

1. 在主控台樹狀目錄**行動裝置管理**資料夾中，選取**行動裝置伺服器**子資料夾。
2. 在**行動裝置伺服器**資料夾的工作區中，選取 iOS MDM 伺服器。
3. 在 iOS MDM 伺服器的上下文功能表中，選取"**內容**"。
   這將開啟 iOS MDM 伺服器的"內容"視窗。

4. 在 iOS MDM 伺服器的“內容”視窗中，選取**“憑證”**區域。

5. 在**憑證**區域的**Apple 推送通知憑證**設定群組中，點擊**安裝**按鈕。

6. 選取包含 APNs 憑證的 PFX 檔案。

7. 輸入在匯出 APNs 憑證時指定的私有金鑰密碼。

APNs 憑證將安裝在 iOS MDM 伺服器上。憑證詳情將在**“憑證”**區域的 iOS MDM 伺服器內容視窗中顯示。

配置到 Apple 推送通知服務的存取

要確保 iOS MDM Web 服務的正常功能和行動裝置到管理員指令的回應，您需要在 iOS MDM 伺服器設定中指定 Apple 推送通知服務憑證（也叫 APN 憑證）。

與 Apple 推送通知（也叫 APN）的互動中，iOS MDM Web 服務透過連接埠 2197（傳送）連線到 api.push.apple.com 的外部位址。因此，iOS MDM Web 服務請求存取到連接埠 TCP 2197 的 17.0.0.0/8 位址範圍。從 iOS 裝置端存取到連接埠 TCP 5223 的 17.0.0.0/8 位址範圍。

如果您要透過代理伺服器從 iOS MDM Web 服務存取到 APN，您必須在安裝了 iOS MDM Web 服務的裝置上執行以下操作：

1. 新增以下字串到登錄檔：

   - 對於 32 位元作業系統：

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<代理主機名稱>"
"ApnProxyPort"="<代理連接埠>"
"ApnProxyLogin"="<代理登入名稱>"
"ApnProxyPwd"="<代理密碼>"
```

   - 對於 64 位元作業系統：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<代理主機名稱>"
"ApnProxyPort"="<代理連接埠>"
"ApnProxyLogin"="<代理登入名稱>"
"ApnProxyPwd"="<代理密碼>"
```

2. 重新啟動 iOS MDM Web 服務。

在行動裝置上發佈和安裝共用憑證

要發佈共用憑證給使用者:

1. 在主控台樹狀目錄中的**“使用者帳戶”**資料夾中，選取使用者帳戶。

2. 在使用者帳戶的上下文功能表中，選取**安裝憑證**。

啟動憑證安裝精靈。遵照精靈的說明。

當精靈完成時，憑證將被建立並且新增到使用者的憑證清單中。

使用者將下載已發佈的憑證，以及包含 iOS MDM 設定檔的安裝套件。

行動裝置連線到 iOS MDM 伺服器後，iOS MDM 設定檔的設定將套用到使用者裝置。管理員能夠在連線後管理該裝置。

連線至 iOS MDM 伺服器的使用者行動裝置會顯示在主控台樹狀目錄中**行動裝置管理**資料夾內的**行動裝置**子資料夾。

新增 KES 裝置到受管理裝置清單

要使用 Google Play™ 連結新增 KES 裝置到受管理裝置清單：

1. 在主控台樹狀目錄中，選取**使用者帳戶**資料夾。

   依預設，**使用者帳戶**資料夾是**進階**資料夾的子資料夾。

2. 選取您要將其行動裝置新增到受管理裝置清單的使用者帳戶。

3. 在使用者帳戶的上下文功能表中，選取**新增行動裝置**。

   新行動裝置連線精靈啟動。在精靈的**憑證來源**視窗，您必須指定建立管理伺服器用以識別裝置的共用憑證的方法。您可以使用下列可用方法之一指定一個共用憑證：

   - 自動建立共用憑證，透過管理伺服器工具，然後傳送憑證到裝置。
   - 指定共用憑證檔案。

4. 在精靈的**裝置類型**視窗，選取**到 Google Play 的連結**。

5. 在精靈的**使用者通知方式**視窗，定義憑證建立的行動裝置使用者通知設定（透過 SMS 訊息、透過郵件或在精靈完成時顯示資訊）。

6. 在精靈的憑證資訊視窗，點擊**完成**按鈕關閉精靈。

精靈結束操作後，一個連結和 QR 代碼將被傳送到使用者行動裝置從而允許使用者從 Google Play 下載 Kaspersky Endpoint Security。使用者透過使用連結或掃描 QR 代碼轉到 Google Play。此後，裝置作業系統會提示使用者接受 Kaspersky Endpoint Security for Android 安裝。Kaspersky Endpoint Security for Android 下載並安裝後，行動裝置連線到管理伺服器並下載共用憑證。在行動裝置安裝憑證後，裝置會顯示在**行動裝置**資料夾中，它在主控台樹狀目錄是**行動裝置管理**資料夾的子資料夾。

如果 Kaspersky Endpoint Security for Android 先前已經被安裝到行動裝置，使用者必須自己從管理員處接收並輸入連線管理伺服器的設定。定義了連線裝置後，行動裝置連線到管理伺服器。管理員為裝置發佈共用憑證並傳送給使用者帶有憑證下載登入名稱和密碼的郵件訊息或 SMS 訊息。使用者下載並安裝共用憑證。在行動裝置安裝憑證後，裝置會顯示在**行動裝置**資料夾中，它在主控台樹狀目錄是**行動裝置管理**資料夾的子資料夾。此種情況下，Kaspersky Endpoint Security for Android 不被下載和再次安裝。

將 KES 裝置連線至管理伺服器

根據連線裝置到管理伺服器的方法，對 KES 裝置 Kaspersky Device Management for iOS 有兩個佈署方案：

- 直接連線裝置到管理伺服器來佈署的方案
- 涉及支援 Kerberos 約束委派的反向代理的部署方案

直接連線裝置到管理伺服器

KES 裝置可以直接連線到管理伺服器的連接埠 13292。

根據使用的身分驗證方法，連線 KES 裝置到管理伺服器有兩個選項：

- 使用使用者憑證連線裝置
- 不用使用者憑證連線裝置

運用使用者憑證連線裝置

當連線帶有使用者憑證的裝置時，裝置與透過管理伺服器工具被分配憑證的使用者帳戶相關聯。

此種情況下，雙向 SSL 身分驗證（雙向認證）將被使用。管理伺服器和裝置都將使用憑證認證。

不用使用者憑證連線裝置

當連線沒有使用者憑證的裝置時，裝置不與任何管理伺服器上的使用者帳戶關聯。然而，當裝置接收任何憑證時，裝置將與透過管理伺服器工具被分配憑證的使用者相關聯。

當連線裝置到管理伺服器時，將套用單向 SSL 身分驗證，這意味著僅管理伺服器使用憑證進行身分驗證。裝置獲取使用者憑證後，身分驗證類型將變更為雙向 SSL 身分驗證（雙向 SSL 身分驗證，共有身分驗證）。

連線 KES 裝置到 Kerberos constrained delegation (KCD) 伺服器的方案

連線 KES 裝置到 Kerberos constrained delegation (KCD) 管理伺服器的方案包括如下：

- 與支援 KCD 的反向代理整合。
- 將 Kerberos Constrained Delegation (KCD) 用於行動裝置身分驗證。
- 與公共金鑰基礎架構 (PKI) 整合以套用使用者憑證。

當使用該連線方案時，請注意以下幾點：

- 連線 KES 裝置到反向代理的類型必須是"雙向 SSL 身分驗證"，就是，裝置必須透過先前使用者憑證連線到反向代理。為此，您不要整合使用者憑證到 Kaspersky Endpoint Security for Android 安裝套件。該 KES 套件必須由裝置指定的管理伺服器建立。
- 您必須指定特定（自訂）憑證，而不是行動協定的預設伺服器憑證：
  1. 在管理伺服器的內容視窗，在**設定**區域，選取**為行動裝置開啟連接埠**核取方塊，然後在下拉清單中選取**新增憑證**。
  2. 在開啟的視窗中，指定當到行動協定的存取點被發佈在管理伺服器時設定在反向代理上的憑證。
- KES 裝置的使用者憑證必須由網域中的 Certificate Authority (CA) 發佈。記住，如果網域包含多個多個根 CA，使用者憑證必須被該 CA 發佈，這已設定在反向代理發佈中。

  您可以透過以下方法確保使用者憑證與上述需求相容：
  - 在新增安裝套件精靈和憑證安裝精靈中指定使用者憑證。
  - 將管理伺服器與網域的 PKI 整合並在憑證發佈規則中定義對應的設定：
    1. 在主控台樹狀目錄中，延伸**行動裝置管理**資料夾並選擇**憑證**子資料夾。
    2. 在**憑證**資料夾中點擊**配置憑證發佈規則**按鈕，開啟**憑證發佈規則**視窗。
    3. 在**與 PKI 整合**區域，配置與公共金鑰基礎架構的整合。
    4. 在**行動憑證發佈**區域，指定憑證來源。

以下是使用以下假定設定 Kerberos Constrained Delegation (KCD) 的例子：

- 管理伺服器到行動協定的存取點被設定成連接埠 13292。
- 具有反向代理的裝置的名稱是firewall.mydom.local。
- 管理伺服器裝置名稱是 ksc.mydom.local。
- 存取點到行動協定的外部發佈位址是 kes4mob.mydom.global。

管理伺服器網域帳戶

您必須建立執行管理伺服器服務的網域帳戶（例如，KSCMobileSrvcUsr）。您可以在安裝管理伺服器或使用 klsrvswch 公用程式時指定管理伺服器服務帳戶。klsrvswch 公用程式位於管理伺服器安裝資料夾。預設安裝路徑：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

網域帳戶必須由以下原因指定：

- KES 裝置管理功能是管理伺服器的一部分。
- 要確保 Kerberos Constrained Delegation (KCD) 的正常功能，接收端（例如，管理伺服器）必須執行在網域帳戶下。

http/kes4mob.mydom.local 的服務主體名稱

在網域中，在 KSCMobileSrvcUsr 帳戶下，新增 SPN 以在管理伺服器裝置的連接埠 13292 發佈行動協議服務。對於管理伺服器裝置 kes4mob.mydom.local，將是如下：

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

配置具有反向代理的裝置的網域內容 (firewall.mydom.local)

要授權流量，您必須信任反向代理裝置 (firewall.mydom.local) 到由 SPN 定義的服務 (http/kes4mob.mydom.local:13292)。

要信任反向代理裝置到由 SPN 定義的服務 (http/kes4mob.mydom.local:13292)，管理員必須執行以下操作：

1. 在名稱為「Active Directory 使用者和電腦」的 Microsoft Management Console 中，選取安裝了反向代理的裝置 (firewall.mydom.local)。
2. 在裝置內容視窗，在**授權**頁籤，設定**信任此電腦到指定服務的授權**轉換鍵到**使用任何身分驗證協議**。
3. 在**該帳戶可以展示已授權憑證的服務**清單，新增 SPN http/kes4mob.mydom.local:13292。

要發佈的特定（自訂）憑證 (kes4mob.mydom.global)

要發佈管理伺服器行動協議，您必須發佈一個 FQDN kes4mob.mydom.global 特定（自訂）憑證並在管理主控台中管理伺服器的行動協議設定中指定它以代替預設伺服器憑證。為此，在管理伺服器的內容視窗，在**設定**區域，選取**為行動裝置開啟連接埠**核取方塊，然後在下拉清單中選取**新增憑證**。

請注意伺服器憑證容器（帶有 .p12 或 .pfx 副檔名的檔案）必須也包含根憑證鏈（公共金鑰）。

配置在反向代理上發布

在反向代理上，對於從行動裝置到連接埠 kes4mob.mydom.global 連接埠 13292 的流量，您必須在 SPN (http/kes4mob.mydom.local:13292) 上配置 KCD，使用為 FQND kes4mob.mydom.global 發佈的憑證。請注意，正發佈和已發佈的存取點（管理伺服器連接埠 13292）必須共用相同的伺服器憑證。

使用 Firebase Cloud Messaging

為了確保及時將指令交付到 Android 作業系統管理的 KES 裝置上，卡巴斯基安全管理中心使用推送通知機制。推播通知透過 Firebase Cloud Messaging（以下簡稱 FCM）在 KES 裝置和管理伺服器之間交換。在卡巴斯基安全管理中心管理主控台中，可以指定 Firebase Cloud Messaging 的設定從而將 KES 裝置連線到服務。

若要擷取 Firebase Cloud Messaging 的設定，您必須有 Google 帳戶。

要啟用對 FCM 的使用：

1. 在管理主控台中，選取**行動裝置管理** 節點以及**行動裝置**資料夾。
2. 在**行動裝置**的上下文功能表中，選取**內容**。
3. 在資料夾內容中，選取**Google Firebase Cloud Messaging 設定**區域。

4. 在**傳送者 ID**欄位中，指定 FCM 寄件者 ID。

5. 在**私密金鑰檔案（JSON 格式）**欄位中，選擇私鑰檔案。

在下次同步管理伺服器時，由 Android 作業系統管理的 KES 裝置將被連線到 Firebase Cloud Messaging。

透過點擊**重設設定**按鈕，您可以編輯 Firebase Cloud Messaging 的設定。

當您切換到其他 Firebase 項目時，您需要等待 10 分鐘 FCM 才能還原。

FCM 服務在以下位址範圍內執行：

- 從 KES 裝置端，需要對以下位址的連接埠 443 (HTTPS)、5228 (HTTPS)、5229 (HTTPS) 和 5230 (HTTPS) 的存取：
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - Google's ASN 15169 中列出的所有 IP 位址
- 從管理伺服器端，需要對以下位址的連接埠 443 (HTTPS) 的存取：
  - fcm.googleapis.com
  - Google's ASN 15169 中列出的所有 IP 位址

如果將代理伺服器設定（**進階 / 設定網際網路存取**）指定在管理主控台的管理伺服器內容中，系統會將其將用來與 FCM 互動。

設定 FCM：獲取寄件者 ID 和私鑰檔案

要設定 FCM：

1. 在 Google 入口註冊。
2. 前往Firebase 主控台。
3. 執行以下操作之一：
   - 若要建立新項目，請按一下**建立項目**並按照螢幕上的指示進行操作。
   - 開啟現有項目。
4. 點擊齒輪圖示並選擇**項目設定**。
   項目設定視窗將開啟。
5. 選擇**Cloud Messaging**頁簽。
6. 從**Firebase Cloud Messaging API (V1)**部分的**寄件者 ID**欄位中檢索相關寄件者 ID。

7. 選擇**服務帳戶**頁簽，然後按一下**產生新私鑰**。

8. 在開啟的視窗中，按一下**產生金鑰**以產生並下載私鑰檔案。

Firebase Cloud Messaging 現已配置。

與公共金鑰基礎架構整合

與公共金鑰基礎架構 (PKI) 整合旨在管理伺服器對網域使用者憑證的發佈。

管理員可以在管理主控台中為使用者分配網域憑證。這可以使用以下方法完成：

- 在憑證建立精靈中，從檔案將特別（自訂）憑證指派給使用者。
- 執行與 PKI 的整合並分配 PKI 以作為制定類型憑證或所有類型憑證的憑證來源。

與 PKI 整合的設定可在 **行動裝置管理 / 憑證**資料夾中取得，方法是點擊**與公共金鑰基礎架構整合**連結。

用於網域使用者憑證發佈的與 PKI 整合的一般原則

在管理主控台的**行動裝置管理 / 憑證**資料夾工作區中點擊**與公共金鑰基礎架構整合**連結，以指定管理伺服器用來透過網域 CA（這指的是執行 PKI 整合的帳戶）發佈網域使用者憑證的網域帳戶。

請注意以下：

- 與 PKI 整合的設定允許您為所有類型的憑證指定預設範本。請注意，憑證發佈規則（可在**行動裝置管理 / 憑證**資料夾工作區點擊**配置憑證發佈規則**按鈕取得）可讓您為每種類型的憑證指定各自的範本。
- 特殊 Enrollment Agent (EA) 憑證必須安裝在管理伺服器裝置，在與 PKI 整合的帳戶的憑證儲存區中。Enrollment Agent (EA) 憑證由網域 CA (Certificate Authority) 管理員發佈。

與 PKI 整合的帳戶必須滿足以下標準：

- 它是網域使用者。
- 它是發起與 PKI 的整合的管理伺服器裝置本機管理員。
- 它具有*作為服務登入*的權限。
- 管理伺服器裝置必須在此帳戶下執行至少一次以建立永久使用者設定檔。

卡巴斯基安全管理中心網頁伺服器

卡巴斯基安全管理中心網頁伺服器（以下簡稱"網頁伺服器"）是卡巴斯基安全管理中心的一個元件。網頁伺服器用於發佈獨立安裝套件、行動裝置獨立安裝套件、iOS MDM 設定檔、以及共用資料夾的檔案。

所建立的 iOS MDM 設定檔和安裝套件被自動發佈在網頁伺服器並在第一次下載後被刪除。管理員可以以任意方式例如電子郵件等方式將新連結傳送給使用者。

透過點擊連結，使用者可將所需資訊下載至行動裝置。

如果需要網頁伺服器的 fine-tuning，管理主控台網頁伺服器內容提供為 HTTP (8060) 和 HTTPS (8061) 變更連接埠。除了變更連接埠，您可以為 HTTPS 取代伺服器憑證並為 HTTP 變更網頁伺服器的 FQDN。

卡巴斯基安全管理中心的安裝

本章節敘述了卡巴斯基安全管理中心元件的安裝。如果您只想在一台裝置上本機安裝應用程式，可以使用兩種安裝選項：

- **標準**。此選項用在您要嘗試卡巴斯基安全管理中心並在網路中的小區域測試其操作的時候。在標準安裝期間，您僅設定資料庫。您還可以僅安裝 Kaspersky 應用程式的管理外掛程式的預設集合。如果您有過使用卡巴斯基安全管理中心的經驗，因此您可以在標準安裝後指定所有相關設定，您也可以使用標準安裝。

- **自訂**。自訂安裝允許您修改卡巴斯基安全管理中心設定，例如共用資料夾路徑、帳戶和連線管理伺服器的連接埠，以及資料庫設定。自訂安裝允許您指定安裝哪些 Kaspersky 管理外掛程式。如果必要，您可以在靜默模式啟動自訂安裝。

如果網路中至少已安裝一台管理伺服器，您可以透過遠端安裝工作使用強制安裝方式將伺服器安裝到同一網路中的其他裝置上。當建立遠端安裝工作時，您應該使用管理伺服器安裝套件：ksc_<version_number>.<build number>_full_<localization language>.exe。

如果您要安裝全功能卡巴斯基安全管理中心元件，或升級目前版本到這些元件，請使用此套件。

如果您想部署卡巴斯基安全管理中心容錯移轉叢集，您需要在叢集的所有節點上安裝卡巴斯基安全管理中心。

準備安裝

在啟動安裝之前執行以下操作。

- **檢查硬體和軟體要求**

  確保裝置的硬體和軟體滿足管理伺服器和管理主控台的需求。

- **選擇並安裝資料庫管理系統 (DBMS)**

  卡巴斯基安全管理中心將其資訊儲存在由 DBMS 管理的資料庫中。在卡巴斯基安全管理中心之前在網路上安裝 DBMS（詳細了解如何選擇 DBMS）。如果您決定安裝 PostgreSQL 或 Postgres Pro DBMS，請為超級使用者指定密碼。如未指定密碼，管理伺服器可能無法連線到資料庫。

  建議將管理伺服器安裝在專用伺服器上而不是網域控制器上。然而，若在作為唯讀網域控制器 (RODC) 的伺服器上安裝卡巴斯基安全管理中心，則不得在相同裝置上安裝 Microsoft SQL Server (SQL Express)。在此情況下，建議您遠端安裝 Microsoft SQL Server (SQL Express)（在不同裝置上），如果需要本機安裝 DBMS，則使用 MySQL、MariaDB 或 PostgreSQL。

- **為管理伺服器、網路代理和管理主控台準備資料夾**

  管理伺服器、網路代理和管理主控台應該安裝在停用了大小寫敏感的資料夾。此外，主管理伺服器共用資料夾和卡巴斯基安全管理中心隱藏資料夾 (%ALLUSERSPROFILE%\KasperskyLab\adminkit) 也必須停用大小寫敏感。

- **刪除舊的網路代理**

網路代理的伺服器版本會連同管理伺服器一起安裝在裝置上。管理伺服器不能與不同版本的管理伺服器的網路代理安裝在同一台電腦上。如果裝置已經安裝了不同版本的管理伺服器版本網路代理，請先移除它並且重新啟動管理伺服器。網路代理的伺服器版本詳見安裝卡巴斯基安全管理中心後系統的變化。

- **檢查帳戶**

  安裝卡巴斯基安全管理中心時，您必須要提供此台裝置上的管理員權限才能正常的安裝卡巴斯基安全管理中心。

  卡巴斯基安全管理中心支援受管理服務帳戶和受群組管理的服務帳戶。如果在您的網域中使用了這些類型的帳戶，並且您想指定其中一個作為管理伺服器服務的帳戶，則要先將帳戶安裝在要安裝管理伺服器的同一裝置上。如需在本機裝置上安裝受管理服務帳戶的詳細資訊，請參閱正式的 Microsoft 文件。

使用 DBMS 的帳戶

要安裝管理伺服器並使其運作，您需要一個用於執行管理伺服器安裝程式（以下簡稱「安裝程式」）的 Windows 帳戶、一個用於啟動管理伺服器服務的 Windows 帳戶，以及一個用於存取 DBMS 的內部 DBMS 帳戶。您可以建立新帳戶或使用現有帳戶。所有這些帳戶都需要特定的權限。所需的一組帳戶及其權限取決於以下標準：

- DBMS 類型：
  - Microsoft SQL Server（使用 Windows 身分驗證或 SQL Server 身分驗證）
  - MySQL 或 MariaDB
  - PostgreSQL 或 Postgres Pro
- DBMS 位置：
  - **本機 DBMS**。*本機 DBMS* 是安裝在管理伺服器裝置的 DBMS。
  - **遠端 DBMS**。*遠端 DBMS* 是安裝在其他裝置上的 DBMS。
- 管理伺服器資料庫的建立方法：
  - **自動**。在安裝管理伺服器的過程中，您可以使用安裝程式自動建立一個管理伺服器資料庫（以下簡稱「伺服器資料庫」）。
  - **手動**。您可以使用協力廠商應用程式（例如 SQL Server Management Studio）或指令碼來建立一個空資料庫。之後，您可以在管理伺服器安裝期間，將此資料庫指定為伺服器資料庫。

為帳戶授予權利和權限時，請遵循最小權限原則。也就是說，授予的權限應該僅足以執行所需的動作。

下表提供有關在安裝和啟動管理伺服器之前，應授予帳戶的系統權限和 DBMS 權限資訊。

使用 Windows 身分驗證的 Microsoft SQL Server

如果選擇 SQL Server 作為 DBMS，則可以使用 Windows 身分驗證來存取 SQL Server。為用於執行安裝程式的 Windows 帳戶和用於啟動管理伺服器服務的 Windows 帳戶設定系統權限。在 SQL Server 上，為這兩個 Windows 帳戶建立登入資訊。根據伺服器資料庫的建立方法，如下表所述，將所需的 SQL Server 權限授予這些帳戶。有關如何設定帳戶權限的更多資訊，請參閱設定帳戶以搭配 SQL Server 使用（Windows 身分驗證）。

DBMS：使用 Windows 身分驗證的 Microsoft SQL Server（包含 Express 版本）

	自動建立資料庫（由安裝程式進行）	手動建立資料庫（由管理員進行）
執行安裝程式的帳戶	• 遠端 DBMS：只有安裝 DBMS 的遠端裝置的網域帳戶。 • 本機 DBMS：本機管理員帳戶或網域帳戶。	• 遠端 DBMS：只有安裝 DBMS 的遠端裝置的網域帳戶。 • 本機 DBMS：本機管理員帳戶或網域帳戶。

執行安裝程式的帳戶權限	• 系統權限：本機管理員權限。
	• SQL Server 權限：
	  • 伺服器層級角色：sysadmin。
		• 系統權限：本機管理員權限。
		• SQL Server 權限：
		  • 伺服器層級角色：public。
		  • 伺服器資料庫的資料庫角色成員資格：db_owner，公有。
		  • 伺服器資料庫的預設方案：dbo。

管理伺服器服務帳戶	• 遠端 DBMS：只有安裝 DBMS 的遠端裝置的網域帳戶。
	• 本機 DBMS：
	  • 由管理員選擇的 Windows 帳戶。
	  • 安裝程式自動建立的 KL-AK-* 格式帳戶。
		• 遠端 DBMS：只有安裝 DBMS 的遠端裝置的網域帳戶。
		• 本機 DBMS：
		  • 由管理員選擇的 Windows 帳戶。
		  • 安裝程式自動建立的 KL-AK-* 格式帳戶（在這種情況下，我們不建議您產生 KL-AK-* 帳戶）。

管理伺服器服務帳戶權限	• 系統權限：安裝程式指派的所需權限。
	• SQL Server 權限：安裝程式指配的所需權限。
		• 系統權限：安裝程式指派的所需權限。
		• SQL Server 權限：
		  • 伺服器層級角色：public。
		  • 伺服器資料庫的資料庫角色成員資格：db_owner，公有。
		  • 伺服器資料庫的預設方案：dbo。

使用 SQL Server 身分驗證的 Microsoft SQL Server

如果選擇 SQL Server 作為 DBMS，則可以使用 SQL Server 身分驗證來存取 SQL Server。為用於執行安裝程式的 Windows 帳戶和用於啟動管理伺服器服務的 Windows 帳戶設定系統權限。在 SQL Server 上，建立一個含密碼的登入資訊以用於身分驗證。然後，將下表中列出的所需權限授予此 SQL Server 帳戶。有關如何設定帳戶權限的更多資訊，請參閱設定帳戶以搭配 SQL Server 使用（SQL Server 身分驗證）。

DBMS：使用 SQL Server 身分驗證的 Microsoft SQL Server（包含 Express 版本）

	自動建立資料庫（由安裝程式進行）	手動建立資料庫（由管理員進行）
執行安裝程式的帳戶	• 遠端 DBMS：只有安裝 DBMS 的遠端裝置的網域帳戶。 • 本機 DBMS：本機管理員帳戶或網域帳戶。	• 遠端 DBMS：只有安裝 DBMS 的遠端裝置的網域帳戶。 • 本機 DBMS：本機管理員帳戶或網域帳戶。
執行安裝程式的帳戶權限	系統權限：本機管理員權限。	系統權限：本機管理員權限。

管理伺服器服務帳戶	• 遠端 DBMS：只有安裝 DBMS 的遠端裝置的網域帳戶。
	• 本機 DBMS：
	  • 由管理員選擇的 Windows 帳戶。
	  • 安裝程式自動建立的 KL-AK-* 格式帳戶。
		• 遠端 DBMS：只有安裝 DBMS 的遠端裝置的網域帳戶。
		• 本機 DBMS：
		  • 管理員選擇的 Windows 使用者帳戶。
		  • 安裝程式自動建立的 KL-AK-* 格式帳戶。

	自動建立資料庫（由安裝程式進行）	手動建立資料庫（由管理員進行）
管理伺服器服務帳戶權限	系統權限：安裝程式指派的所需權限。	系統權限：安裝程式指派的所需權限。

用於 SQL Server 身分驗證的登入權限	建立資料庫和安裝管理伺服器所需的 SQL Server 權限：
	• 伺服器層級角色：public。
	• *主*資料庫的資料庫角色成員資格：db_owner。
	• *主*資料庫的預設方案：dbo。
	• 權限：
	  • CONNECT ANY DATABASE
	  • CONNECT SQL
	  • CREATE ANY DATABASE
	  • VIEW ANY DATABASE
	  • VIEW SERVER STATE（如果啟用了 **Always On**選項）
	搭配管理伺服器使用所需的 SQL Server 權限：
	• 伺服器層級角色：public。
	• 伺服器資料庫的資料庫角色成員資格：db_owner。
	• 伺服器資料庫的預設方案：dbo。
	• 權限：
	  • CONNECT SQL
	  • VIEW ANY DATABASE
	  • VIEW SERVER STATE（如果啟用了 **Always On**選項）
	  • VIEW ANY DEFINITION
		SQL Server 權限：
		• 伺服器層級角色：public。
		• 伺服器資料庫的資料庫角色成員資格：db_owner。
		• 伺服器資料庫的預設方案：dbo。
		• 權限：
		  • CONNECT SQL
		  • VIEW ANY DATABASE
		  • VIEW ANY DEFINITION

設定用於復原管理伺服器資料的 SQL Server 權限

如要從備份中還原管理伺服器資料，請使用安裝管理伺服器所用的 Windows 帳戶執行 klbackup 公用程式。在啟動 klbackup 公用程式之前，請在 SQL Server 上，將該權限授予與此 Windows 帳戶關聯的 SQL Server 登入名稱。SQL Server 權限會因管理伺服器版本而異。對於 14.2 或更高版本的管理伺服器，您可以授予 sysadmin 伺服器層級角色或 dbcreator 伺服器層級角色。

用於復原管理伺服器資料庫的 SQL Server 權限

14.2 或更高版本的管理伺服器	其他版本的管理伺服器

• SQL Server 權限：
  • 伺服器層級角色：dbcreator。
• 權限：
  • VIEW ANY DEFINITION
在啟動 klbackup 公用程式之前，請指定 KLSRV_SKIP_ADJUSTING_DBMS_ACCESS 伺服器旗標。使用管理員權限執行 Windows 命令提示符，然後將目前目錄變更為包含 klscflag 公用程式的目錄。klscflag 公用程式位於安裝管理伺服器的資料夾中。預設安裝路徑：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.此後，在命令行中執行以下命令：
`klscflag.exe -fset -pv klserver -n KLSRV_SKIP_ADJUSTING_DBMS_ACCESS -t d -v 1`	

MySQL 和 MariaDB

如果您選擇 MySQL 或 MariaDB 作為 DBMS，請建立一個 DBMS 內部帳戶，並將下表列出的所需權限授予該帳戶。安裝程式和管理伺服器服務會使用這個內部 DBMS 帳戶來存取 DBMS。請注意，資料庫建立方法不影響所需的一組權限。有關如何設定帳戶權限的更多資訊，請參閱設定帳戶以搭配 MySQL 和 MariaDB 使用。

DBMS：MySQL 和 MariaDB

	自動或手動建立資料庫
執行安裝程式的帳戶	• 遠端 DBMS：只有已安裝 DBMS 的遠端裝置的網域帳戶。 • 本機 DBMS：本機管理員帳戶或網域帳戶。
執行安裝程式的帳戶權限	系統權限：本機管理員權限。

管理伺服器服務帳戶	• 遠端 DBMS：只有已安裝 DBMS 的遠端裝置的網域帳戶。
	• 本機 DBMS：
	  • 由管理員選擇的 Windows 帳戶。
	  • 安裝程式自動建立的 KL-AK-* 格式帳戶。

管理伺服器服務帳戶權限	系統權限：安裝程式指派的所需權限。
DBMS 內部帳戶的權限	方案權限： • 管理伺服器資料庫：ALL（不包括 GRANT OPTION）。 • 系統方案（mysql 和 sys）：SELECT、SHOW VIEW。 • sys.table_exists 儲存的處理程序：EXECUTE（如果您使用 MariaDB 10.5 或更早版本作為 DBMS，則無需授予 EXECUTE 權限）。 所有方案的全域權限：PROCESS、SUPER。

有關如何將資料從共享表空間移動到每個表一個檔案的表空間的詳細資訊，請參閱在 MySQL 和 MariaDB DBMS 中將資料從共享表空間移動到每個表一個檔案的表空間。

設定用於復原管理伺服器資料的權限

您授予內部 DBMS 帳戶的權限足以從備份中還原管理伺服器資料。如要開始還原，請使用安裝管理伺服器所用的 Windows 帳戶執行 klbackup 公用程式。

PostgreSQL 或 Postgres Pro

如果您選擇 PostgreSQL 或 Postgres Pro 作為 DBMS，則可以使用 *Postgres* 使用者 (預設的 Postgres 角色) 或建立一個新的 Postgres 角色（以下簡稱「角色」）來存取 DBMS。根據伺服器資料庫的建立方法，如下表所述，將所需的權限授予角色。有關如何設定角色權限的更多資訊，請參閱設定帳戶以搭配 PostgreSQL 或 Postgres Pro 使用。

DBMS：PostgreSQL 或 Postgres Pro

	自動建立資料庫	手動建立資料庫
執行安裝程式的帳戶	• 遠端 DBMS：只有已安裝 DBMS 的遠端裝置的網域帳戶。 • 本機 DBMS：本機管理員帳戶或網域帳戶。	• 遠端 DBMS：只有已安裝 DBMS 的遠端裝置的網域帳戶。 • 本機 DBMS：本機管理員帳戶或網域帳戶。
執行安裝程式的帳戶權限	系統權限：本機管理員權限。	系統權限：本機管理員權限。

管理伺服器服務帳戶	• 遠端 DBMS：只有已安裝 DBMS 的遠端裝置的網域帳戶。
	• 本機 DBMS：
	  • 由管理員選擇的 Windows 帳戶。
	  • 安裝程式自動建立的 KL-AK-* 格式帳戶。
			• 遠端 DBMS：只有已安裝 DBMS 的遠端裝置的網域帳戶。
			• 本機 DBMS：
			  • 由管理員選擇的 Windows 帳戶。
			  • 安裝程式自動建立的 KL-AK-* 格式帳戶。

管理伺服器服務帳戶權限	系統權限：安裝程式指派的所需權限。		系統權限：安裝程式指派的所需權限。
Postgres 角色的權限	*Postgres* 使用者不需要額外的權限。	新角色的權限： `CREATEDB`。	對於新角色： • 管理伺服器資料庫的權限：`ALL`。 • 公用方案中所有表格的權限：`ALL`。 • 公用方案中所有序列的權限：`ALL`。

設定用於復原管理伺服器資料的權限

如要從備份中還原管理伺服器資料，請使用安裝管理伺服器所用的 Windows 帳戶執行 klbackup 公用程式。請注意，用於存取 DBMS 的 Postgres 角色必須具有管理伺服器資料庫的擁有者權限。

設定與 SQL Server 搭配使用的帳戶（Windows 身分驗證）

先決條件

在為帳戶指派權限之前，請執行以下操作：

1. 確保您以本機管理員帳戶登入系統。
2. 安裝搭配使用 SQL Server 的環境。
3. 確保您有一個 Windows 帳戶，以便用它來安裝管理伺服器。
4. 確保您有一個 Windows 帳戶，以便用它來啟動管理伺服器服務。
5. 在 SQL Server 上，為用於執行 Administration Server 安裝程式（以下簡稱「安裝程式」）的 Windows 帳戶建立一個登入資訊。此外，還要為啟動管理伺服器服務所用的 Windows 帳戶建立一個登入資訊。

如果您使用 SQL Server Management Studio，請在登入屬性視窗的**一般**頁面，選取 **Windows 身分驗證**選項。

如果要在位於不同 Windows 域中的裝置上安裝管理伺服器和 SQL Server，請注意這些域必須具有雙向信任關係以確保管理伺服器的正確操作，包括執行工作和套用政策。有關使用各種 DBMS 所需的帳戶和帳戶權限的資訊，請參閱 使用 DBMS 的帳戶。

設定帳戶以安裝管理伺服器（自動建立管理伺服器資料庫）

要為管理伺服器安裝設定帳戶：

1. 在 SQL Server 上，將 sysadmin 伺服器層級角色指派給用於執行安裝程式的 Windows 帳戶的登入名稱。
2. 使用執行安裝程式所用的 Windows 帳戶登入系統。
3. 執行管理伺服器安裝程式。

   管理伺服器設定精靈啟動。遵照精靈的說明。
4. 選取管理伺服器的自訂安裝選項。
5. 選取 Microsoft SQL Server 作為 DBMS 來儲存管理伺服器資料庫。
6. 選取 Microsoft Windows 身分驗證模式，以透過 Windows 帳戶在管理伺服器和 SQL Server 之間建立連線。
7. 指定用於啟動管理伺服器服務的 Windows 帳戶。

   您可以選取之前為其建立了 SQL Server 登入名稱的 Windows 使用者帳戶。或者，您可以使用安裝程式自動建立 KL-AK-* 格式的新 Windows 帳戶。在這種情況下，安裝程式會自動為此帳戶建立一個 SQL Server 登入資訊。無論選擇何種帳戶，安裝程式都會將所需的系統權限和 SQL Server 權限指派給管理伺服器服務帳戶。

安裝完成後，將建立伺服器資料庫，並將所有必需的系統權限和 SQL Server 權限指派給管理伺服器服務帳戶。管理伺服器可以使用了。

設定帳戶以安裝管理伺服器（手動建立管理伺服器資料庫）

要為管理伺服器安裝設定帳戶：

1. 在 SQL Server 上，建立一個空資料庫。此資料庫將用作管理伺服器資料庫（以下簡稱「伺服器資料庫」）。
2. 對於為 Windows 帳戶建立的兩個 SQL Server 登入名稱，指定公共伺服器層級角色，然後設定對應到建立的資料庫：
   - 伺服器層級角色：public
   - 資料庫角色成員：db_owner、public
   - 預設方案：dbo
3. 使用執行安裝程式所用的 Windows 帳戶登入系統。
4. 執行管理伺服器安裝程式。

   管理伺服器設定精靈啟動。遵照精靈的說明。
5. 選取管理伺服器的自訂安裝選項。
6. 選取 Microsoft SQL Server 作為 DBMS 來儲存管理伺服器資料庫。
7. 將建立的資料庫名稱指定為管理伺服器資料庫名稱。

8. 選取 Microsoft Windows 身分驗證模式，以透過 Windows 帳戶在管理伺服器和 SQL Server 之間建立連線。

9. 指定用於啟動管理伺服器服務的 Windows 帳戶。

   您可以選取之前已為其建立了 SQL Server 登入名稱並設定登入權限的 Windows 使用者帳戶。

我們不建議您自動建立 KL-AK-* 格式的新 Windows 帳戶。在這種情況下，安裝程式會建立一個您尚未為其建立和設定 SQL Server 帳戶的新 Windows 帳戶。管理伺服器無法使用此帳戶啟動管理伺服器服務。如果需要建立 KL-AK-* Windows 帳戶，請不要在安裝後啟動管理主控台。請改為執行以下操作：

1. 停止 kladminserver 服務。

2. 在 SQL Server 上，為建立的 KL-AK-* Windows 帳戶建立一個 SQL Server 登入名稱。

3. 授予此 SQL Server 登入權限並設定對應到建立的資料庫：

   - 伺服器層級角色：public
   - 資料庫角色成員：db_owner、public
   - 預設方案：dbo

4. 重新啟動 kladminserver 服務，然後執行管理主控台。

安裝完成後，管理伺服器將使用建立的資料庫來儲存伺服器資料。管理伺服器可以使用了。

設定與 SQL Server 搭配使用的帳戶（SQL Server 身分驗證）

先決條件

在為帳戶指派權限之前，請執行以下操作：

1. 確保您以本機管理員帳戶登入系統。

2. 安裝搭配使用 SQL Server 的環境。

3. 確保您有一個 Windows 帳戶，以便用它來安裝管理伺服器。

4. 確保您有一個 Windows 帳戶，以便用它來啟動管理伺服器服務。

5. 在 SQL Server 上，啟用 SQL Server 身分驗證模式。

   如果您使用 SQL Server Management Studio，請在 SQL Server 屬性視窗中的**安全**頁面，選取 **SQL Server 和 Windows 身分驗證模式**選項。

6. 在 SQL Server 上，建立一個有密碼的登入資訊。管理伺服器安裝程式（以下簡稱「安裝程式」）和管理伺服器服務將使用此 SQL Server 帳戶存取 SQL Server。

   如果您使用 SQL Server Management Studio，在登入屬性視窗的**一般**頁面，選取 **SQL 伺服器身分驗證**選項。

如果要在位於不同 Windows 網域中的裝置上安裝 Administration Server 和 SQL Server，請注意這些域必須具有雙向信任關係以確保 Administration Server 的正確操作，包括執行工作和套用政策。有關使用各種 DBMS 所需的帳戶和帳戶權限的資訊，請參閱 使用 DBMS 的帳戶。

設定帳戶以安裝管理伺服器（自動建立管理伺服器資料庫）

要為管理伺服器安裝設定帳戶：

1. 在 SQL Server 上，將 SQL Server 帳戶對應到預設的*主*資料庫。*主*資料庫是管理伺服器資料庫（以下簡稱「伺服器資料庫」）的範本。*主*資料庫會用於對應，直到安裝程式建立伺服器資料庫為止。授予 SQL Server 帳戶以下權利和權限：
   - 伺服器層級角色：public
   - *主*資料庫的資料庫角色成員資格：db_owner
   - *主*資料庫的預設方案：dbo
   - 權限：
     - CONNECT ANY DATABASE
     - CONNECT SQL
     - CREATE ANY DATABASE
     - VIEW ANY DATABASE
2. 使用執行安裝程式所用的 Windows 帳戶登入系統。
3. 執行安裝程式。

   管理伺服器設定精靈啟動。遵照精靈的說明。
4. 選取管理伺服器的自訂安裝選項。
5. 選取 Microsoft SQL Server 作為 DBMS 來儲存管理伺服器資料庫。
6. 指定管理伺服器資料庫名稱。
7. 選取 SQL Server 身分驗證模式，以透過建立的 SQL Server 帳戶在管理伺服器與 SQL Server 之間建立連線。接著，指定 SQL Server 帳戶憑證。
8. 指定用於啟動管理伺服器服務的 Windows 帳戶。

   您可以選取現有的 Windows 使用者帳戶或使用安裝程式建立 KL-AK-* 格式的新 Windows 帳戶。無論選擇何種帳戶，安裝程式都會將所需的系統權限指派給管理伺服器服務帳戶。

安裝完成後，將建立伺服器資料庫，並將所有必需的系統權限指派給管理伺服器服務帳戶。管理伺服器可以使用了。

您可以取消對應到*主*資料庫，因為安裝程式已經建立了一個伺服器資料庫，並在管理伺服器安裝期間已設定對應到該資料庫。

由於自動建立資料庫需要比正常使用管理伺服器更多的權限，您可以撤銷一些權限。在 SQL Server 上，選取 SQL Server 帳戶，然後授予以下使用管理伺服器的權限：

- 伺服器層級角色：public
- 伺服器資料庫的資料庫角色成員資格：db_owner

- 伺服器資料庫的預設方案：dbo
- 權限：
  - CONNECT SQL
  - VIEW ANY DATABASE

設定帳戶以安裝管理伺服器（手動建立管理伺服器資料庫）

要為管理伺服器安裝設定帳戶：

1. 在 SQL Server 上，建立一個空資料庫。該資料庫將用作管理伺服器資料庫。
2. 在 SQL Server 上，授予 SQL Server 帳戶以下權利和權限：
   - 伺服器層級角色：public。
   - 已建立資料庫的資料庫角色成員資格：db_owner。
   - 已建立資料庫的預設方案：dbo。
   - 權限：
     - CONNECT SQL
     - VIEW ANY DATABASE
3. 使用執行安裝程式所用的 Windows 帳戶登入系統。
4. 執行安裝程式。

   管理伺服器設定精靈啟動。遵照精靈的說明。
5. 選取管理伺服器的自訂安裝選項。
6. 選取 Microsoft SQL Server 作為 DBMS 來儲存管理伺服器資料庫。
7. 將建立的資料庫名稱指定為管理伺服器資料庫名稱。
8. 選取 SQL Server 身分驗證模式，以透過建立的 SQL Server 帳戶在管理伺服器與 SQL Server 之間建立連線。接著，指定 SQL Server 帳戶憑證。
9. 指定用於啟動管理伺服器服務的 Windows 帳戶。

   您可以選取現有的 Windows 使用者帳戶或使用安裝程式建立 KL-AK-* 格式的新 Windows 帳戶。無論選擇何種帳戶，安裝程式都會將所需的系統權限指派給管理伺服器服務帳戶。

安裝完成後，管理伺服器將使用建立的資料庫來儲存管理伺服器資料。所有必需的系統權限都被指派給管理伺服器服務帳戶。管理伺服器可以使用了。

設定帳戶以搭配使用 MySQL 和 MariaDB

先決條件

在為帳戶指派權限之前，請執行以下操作：

1. 確保您以本機管理員帳戶登入系統。
2. 安裝搭配使用 MySQL 或 MariaDB 的環境。
3. 確保您有一個 Windows 帳戶，以便用它來安裝管理伺服器。
4. 確保您有一個 Windows 帳戶，以便用它來啟動管理伺服器服務。

設定帳戶來安裝管理伺服器

要為管理伺服器安裝設定帳戶：

1. 在安裝 DBMS 時建立的根帳戶下執行搭配使用 MySQL 或 MariaDB 的環境。
2. 建立一個含密碼的內部 DBMS 帳戶。管理伺服器安裝程式（以下簡稱「安裝程式」）和管理伺服器服務將使用此內部 DBMS 帳戶存取 DBMS。授予此帳戶以下權限：
   - 方案權限：
     - 管理伺服器資料庫：ALL（不包括 `GRANT OPTION`）
     - 系統方案（mysql 和 sys）：`SELECT`、`SHOW VIEW`
     - sys.table_exists 預存程序：`EXECUTE`
   - 所有方案的全域權限：`PROCESS`、`SUPER`

   要建立內部 DBMS 帳戶並授予此帳戶所需的權限，請執行以下指令碼（在此指令碼中，DBMS 登入名稱是 *KSCAdmin*，管理伺服器資料庫名稱為 *kav*）：

   ```
   /* Create a user named KSCAdmin */
   CREATE USER 'KSCAdmin'
   /* Specify a password for KSCAdmin */
   IDENTIFIED BY '< 密碼 >';
   ```

   如果您使用 MySQL 8.0 或更早版本作為 DBMS，請注意這些版本不支援“快取 SHA2 密碼”身分驗證。將預設身分驗證從“快取 SHA2 密碼”變更為“MySQL 本機密碼”：

   - 要建立使用“MySQL本機密碼”認證的 DBMS 帳戶，執行以下命令：

     ```
     CREATE USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '< 密碼 >';
     ```

   - 要變更現有 DBMS 帳戶的身分驗證，請執行以下命令：

     ```
     ALTER USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '< 密碼 >';
     ```

   ```
   /* Grant privileges to KSCAdmin */
   GRANT USAGE ON *.* TO 'KSCAdmin';
   GRANT ALL ON kav.* TO 'KSCAdmin';
   GRANT SELECT, SHOW VIEW ON mysql.* TO 'KSCAdmin';
   GRANT SELECT, SHOW VIEW ON sys.* TO 'KSCAdmin';
   GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin';
   GRANT PROCESS ON *.* TO 'KSCAdmin';
   GRANT SUPER ON *.* TO 'KSCAdmin';
   ```

   > 如果您使用 MariaDB 10.5 或更早版本作為 DBMS，則無需授予 EXECUTE 權限。在這種情況下，從指令碼中排除以下命令：`GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin'`。

3. 要檢視授予 DBMS 帳戶的權限清單，請執行以下指令碼：

   ```
   SHOW grants for 'KSCAdmin';
   ```

4. 要手動建立管理伺服器資料庫，請執行以下指令碼（在此指令碼中，管理伺服器資料庫名稱為 *kav*）：

   ```
   CREATE DATABASE kav
   DEFAULT CHARACTER SET ascii
   DEFAULT COLLATE ascii_general_ci;
   ```

   使用您在建立 DBMS 帳戶的指令碼中指定的相同資料庫名稱。

5. 使用執行安裝程式所用的 Windows 帳戶登入系統。

6. 執行安裝程式。

   管理伺服器設定精靈啟動。遵照精靈的說明。

7. 選取管理伺服器的自訂安裝選項。

8. 選擇 MySQL 或 MariaDB 作為 DBMS來儲存管理伺服器資料庫。

9. 指定管理伺服器資料庫名稱。使用您在指令碼中指定的相同資料庫名稱。

10. 指定您透過指令碼建立的 DBMS 帳戶的憑證。

11. 指定用於啟動管理伺服器服務的 Windows 帳戶。

    您可以選擇現有的 Windows 使用者帳戶或使用安裝程式自動建立 KL-AK-* 格式的新 Windows 帳戶。無論選擇何種帳戶，安裝程式都會將所需的系統權限指派給管理伺服器服務帳戶。

安裝完成後，將建立管理伺服器資料庫，然後管理伺服器就可以使用了。

在 MySQL 或 MariaDB DBMS 中將資料從共享表空間移動到每個表格一個檔案的表空間

對於 MySQL 和 MariaDB DBMS，您可以透過以下方式儲存資料：

- 作為共享表空間，當所有使用者資料庫的資料都儲存在單一檔案中（通常在`ibdata1`檔案中）時。
- 作為每個表格一個檔案的表空間，當為每個表建立一個單獨的資料空間作為單獨的檔案時。

使用共享表空間會增加表空間碎片的風險。由於無法執行`SHRINK`操作，共用表空間中的一個檔案可能會佔用約 90% 的磁碟空間。這會對磁碟子系統的效能產生負面影響。因此，選擇每個表格一個檔案的表空間很有用。

本文介紹如何將資料從共享表空間移動到每個表格一個檔案的表空間。如果其他應用程式也使用 MySQL 或 MariaDB DBMS，則您必須將這些應用程式的資料庫移至每個表格一個檔案的表空間。

我們建議您僅在使用管理伺服器的 MySQL 或 MariaDB DBMS 時才執行此程序。
將資料從共享表空間移動到每個表格一個檔案的表空間可能會增加磁碟子系統的負載。

先決條件

在開始之前，請確保：

- 您透過執行資料備份工作或klbackup 公用程式建立了管理伺服器資料的備份副本。
- 您建立了其他應用程式的備份副本，這些應用程式的資料庫由 MySQL 或 MariaDB DBMS（如有）管理。
- 在安裝了 DBMS 的裝置上，在具有資料庫的分割區中，有可用磁碟空間。

所需磁碟空間是目前資料庫總大小（ `ibdata1`檔案的目前大小）的 150%。

過程

若要將資料從共享表空間移動到每個表格一個檔案的表空間：

1. 停止卡巴斯基安全管理中心管理伺服器服務和其他使用您要為其執行此程序的 DBMS 實例的應用程式。

2. 根據 DBMS 版本，以超級使用者身分登入您的 DBMS，然後在任何方便的應用程式中執行 `fix_tablespace.sql` 指令碼。

   您可以透過點擊這些連接來檢視 `fix_tablespace.sql` 指令碼：

   檢視適用於 MySQL 5.7 和 MariaDB 10.1+ 的指令碼

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;

    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';'
);
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;

        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

檢視適用於 MySQL 8.0+ 的指令碼

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;

    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';'
);
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;

        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` TABLESPACE =
innodb_file_per_table;' );
        PREPARE stmt2 FROM @`strSQL`;
        EXECUTE stmt2;
        DEALLOCATE PREPARE stmt2;

        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

您不得停止指令碼執行。
如果沒有發生 DBMS 錯誤，但您終止了指令碼執行，請再次執行指令碼，或停止執行此程序的步驟，重新啟動 DBMS 服務，然後從備份中還原管理伺服器資料。

3. 在 my.cnf 檔案的 `[mysqld]` 部分中，將 `innodb_file_per_table` 參數設為 `1`。
4. 重新啟動 MySQL 或 MariaDB 服務。
5. 啟動卡巴斯基安全管理中心管理伺服器服務。

資料被從共享表空間移動到每個表格一個檔案的表空間。

設定帳戶以搭配使用 PostgreSQL 和 Postgres Pro

先決條件

在為帳戶指派權限之前，請執行以下操作：

1. 確保您以本機管理員帳戶登入系統。
2. 安裝搭配使用 PostgreSQL 和 Postgres Pro 的環境。

3. 設定 PostgreSQL 或 Postgres Pro 伺服器與卡巴斯基安全管理中心 14.2 搭配使用。

4. 確保您有一個 Windows 帳戶，以便用它來安裝管理伺服器。

5. 確保您有一個 Windows 帳戶，以便用它來啟動管理伺服器服務。

設定帳戶以安裝管理伺服器（自動建立管理伺服器資料庫）

要為管理伺服器安裝設定帳戶：

1. 執行搭配使用 PostgreSQL 和 Postgres Pro 的環境。

2. 選擇一個 Postgres 角色來存取 DBMS。您可以使用以下角色之一：

   - *Postgres* 使用者（預設的 Postgres 角色）。

     如果使用 *Postgres* 使用者，則不需要授予該使用者額外的權限。

   - 一個新的 Postgres 角色。

     如果你想使用一個新的 Postgres 角色，請建立這個角色，然後授予它 CREATEDB 權限。為此，請執行以下指令碼（在此指令碼中，角色是 *KSCAdmin*）：

     ```
     CREATE USER "KSCAdmin" WITH PASSWORD '<密碼>' CREATEDB;
     ```

     建立的角色將用作管理伺服器資料庫（以下簡稱「伺服器資料庫」）的所有者。

3. 使用執行管理伺服器安裝程式（以下簡稱「安裝程式」）所用的 Windows 帳戶登入系統。

4. 執行安裝程式。

   管理伺服器設定精靈啟動。遵照精靈的說明。

5. 選取管理伺服器的自訂安裝選項。

6. 選擇 PostgreSQL 或 Postgres Pro 作為 DBMS 來儲存管理伺服器資料庫。

7. 指定伺服器資料庫名稱。安裝程式將自動建立伺服器資料庫。

8. 指定 Postgres 角色的憑證。

9. 指定用於啟動管理伺服器服務的 Windows 帳戶。

   您可以選擇現有的 Windows 使用者帳戶或使用安裝程式自動建立 KL-AK-* 格式的新 Windows 帳戶。無論選擇何種帳戶，安裝程式都會將所需的系統權限指派給管理伺服器服務帳戶。

安裝完成後，將自動地建立伺服器資料庫，然後管理伺服器就可以使用了。

設定帳戶以安裝管理伺服器（手動建立管理伺服器資料庫）

要為管理伺服器安裝設定帳戶：

1. 執行搭配使用 Postgres 的環境。

2. 用 *Postgres*資料庫中的*Postgres*使用者登入。

3. 建立一個新的 Postgres 角色（在此範例中，該角色是 *KSCAdmin*）：

   ```
   CREATE USER "KSCAdmin" WITH PASSWORD '<密碼>';
   ```

4. 建立管理伺服器資料庫（在此範例中，管理伺服器資料庫名稱為 *kav*）：

   ```
   CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";
   ```

   > 如果出現「新編碼 (UTF8) 與範本資料庫的編碼不相容」錯誤，請使用以下命令建立資料庫：
   > `CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin" TEMPLATE template0;`
   > ，而不是使用：
   > `CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";`

5. 授予該角色對管理伺服器資料庫的所有權限。

   ```
   GRANT ALL PRIVILEGES ON DATABASE "KAV" TO "KSCAdmin";
   ```

   > 確保該角色對管理伺服器資料庫具有預設的 CONNECT 和 TEMPORARY 權限。

6. 為建立的 Postgres 角色授予以下權限：

   - 公用方案中所有表格的權限：ALL
   - 公用方案中所有序列的權限：ALL

   為此，請以伺服器資料庫中的 *Postgres* 使用者登入，然後執行以下指令碼（在這個指令碼中，角色是 *KSCAdmin*）：

   ```
   GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "KSCAdmin";
   GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "KSCAdmin";
   ```

7. 使用執行安裝程式所用的 Windows 帳戶登入系統。

8. 執行管理伺服器安裝程式。

   管理伺服器設定精靈啟動。遵照精靈的說明。

9. 選取管理伺服器的自訂安裝選項。

10. 選擇 PostgreSQL 或 Postgres Pro 作為 DBMS 來儲存管理伺服器資料庫。

11. 指定伺服器資料庫名稱。使用您在指令碼中指定的相同資料庫名稱。請注意，資料庫名稱區分大小寫。

12. 指定 Postgres 角色的憑證。

13. 指定用於啟動管理伺服器服務的 Windows 帳戶。

    您可以選擇現有的 Windows 使用者帳戶或使用安裝程式自動建立 KL-AK-* 格式的新 Windows 帳戶。無論選擇何種帳戶，安裝程式都會將所需的系統權限指派給管理伺服器服務帳戶。

安裝完成後，管理伺服器將使用建立的資料庫來儲存管理伺服器資料。管理伺服器可以使用了。

情境：驗證 Microsoft SQL Server

本節資訊僅適用於卡巴斯基安全管理中心使用 Microsoft SQL Server 作為資料庫管理系統的配置。

若要防護卡巴斯基安全管理中心資料移轉至或來自的資料庫，以及儲存於從未授權存取權限之資料庫的資料，您必須保障卡巴斯基安全管理中心與 SQL Server 間的通訊。提供安全通訊的最可靠方式是安裝卡巴斯基安全管理中心與 SQL Server 在相同的裝置並對這兩個應用程式使用共用的記憶體機制。在所有情況下，建議您使用 SSL 或 TLS 憑證來驗證 SQL Server 實例。您可使用來自信任的憑證授權單位 (CA) 或自簽發憑證。建議您使用來自信任 CA 的憑證，因為自簽發憑證僅提供有限防護。

SQL Server 驗證會分階段進行：

1. **根據憑證需求產生適用於 SQL Server 的自簽發 SSL 或 TLS 憑證**

   若您已有 SQL Server 的憑證，請略過此步驟。

   SSL 憑證僅適用於早於 2016 (13.x) 的 SQL Server 版本。在 SQL Server 2016 (13.x) 和更新版本中，請使用 TLS 憑證。

   例如，若要產生 TLS 憑證，請輸入 PowerShell 中的以下命令：

   ```
   New-SelfSignedCertificate -DnsName SQL_HOST_NAME -CertStoreLocation cert:\LocalMachine
   -KeySpec KeyExchange
   ```

   在命令中，若網域中包含主機，您必須取代 SQL_HOST_NAME 改為輸入 SQL Server 主機名稱，若網域未納入主機，請輸入主機*完全合格的網域名稱* (FQDN)。相同名稱—主機名稱或 FQDN—必須在管理伺服器安裝精靈指定為 SQL Server 實例名稱。

2. **在 SQL Server 實例新增憑證**

   請視平台在哪個 SQL Server 上執行參閱此階段的指示說明。請參閱正式文件以取得詳細資訊：

   - Windows
   - Linux
   - Amazon Relational Database Service
   - Windows Azure

   若要在容錯移轉叢集上使用憑證，您必須在容錯移轉叢集的各個節點安裝憑證。如需詳細資訊，請參閱 Microsoft 檔案。

3. **指派服務帳戶權限**

   確保服務帳戶在哪個 SQL Server 服務下執行並擁有存取私密金鑰的完整控制權限。如需詳細資訊，請參閱 Microsoft 檔案。

4. **將憑證新增至卡巴斯基安全管理中心的信任憑證清單**

   在管理伺服器裝置上，將憑證新增至信任的憑證清單。如需詳細資訊，請參閱 Microsoft 檔案。

5. **啟用 SQL Server 實例與卡巴斯基安全管理中心間的加密連線**

在管理伺服器裝置上，將環境變數 KLDBADO_UseEncryption 設定值為 1。例如，在 Windows Server 2012 R2 中，您可在**系統內容視窗**按一下**進階**頁籤的**環境變數**來變更環境變數。新增變數，並將其命名為 KLDBADO_UseEncryption，之後設定值為 1。

6. **使用 TLS 1.2 通訊協定的其他配置**

   若您使用 TLS 1.2 通訊協定，請額外進行以下事項：

   - 確保 SQL Server 安裝版本為 64 位元應用程式。
   - 在管理伺服器裝置上安裝 Microsoft OLE DB 驅動程式。如需詳細資訊, 請參閱 Microsoft 檔案。
   - 在管理伺服器裝置上，將環境變數 KLDBADO_UseMSOLEDBSQL 的值設為 1。例如，在 Windows Server 2012 R2 中，您可在**系統內容視窗**按一下**進階**頁籤的**環境變數**來變更環境變數。新增變數，並將其命名為 KLDBADO_UseMSOLEDBSQL，之後設定值為 1。

     如果 OLE DB 驅動程式版本為 19 或更高版本，還需設定值 MSOLEDBSQL19 為環境變數 KLDBADO_ProviderName。

7. **在 SQL Server 已命名實例上使用 TCP/IP 通訊協定**

   若您使用已命名的 SQL Server 實例，請額外啟用 TCP/IP 通訊協定並將 TCP/IP 埠號指派給 SQL Server Database Engine。當您在管理伺服器安裝精靈中設定 SQL Server 連線時，請在 **SQL Server 實例名稱**欄位中指定 SQL Server 主機名稱與埠號。

管理伺服器安裝建議

該部分包含了如何安裝管理伺服器的建議。該部分還提供了使用管理伺服器上的共用資料夾以便佈署網路代理到用戶端裝置的情境。

在失敗轉移叢集上為管理伺服器服務建立帳戶

預設下，安裝程式自動為管理伺服器服務建立非特權帳戶。該行為對於在一般裝置上安裝管理伺服器來說是最方便的。

然而，在失敗轉移的叢集上安裝管理伺服器需要不同的方案：

1. 為管理伺服器服務建立非特權網域帳戶，並把它們作為以 KLAdmins 為名稱的全域網域安全群組的成員。
2. 在管理伺服器安裝程式中，指定為服務建立的網域帳戶。

定義共用資料夾

當安裝管理伺服器時，您可以指定共用資料夾位置。您也可以在安裝後，在管理伺服器內容中指定共用資料夾位置。依預設會將共用資料夾建立在管理伺服器的所在裝置（對**每個人**子群組具有讀取權限）。然而，在一些情況下（例如高負載或需要從隔離網路存取），最好放置共用資料夾到專用檔案資源。

共用資料夾在網路代理佈署中偶爾使用。

共用資料夾必須停用大小寫敏感。

使用管理伺服器工具透過 Active Directory 群組政策遠端安裝

如果目的裝置位於 Windows 網域（沒有工作群組）中，初始化佈署（安裝網路代理和安全應用程式到未被管理的裝置）必須透過 Active Directory 群組政策執行。佈署使用卡巴斯基安全管理中心遠端安裝標準工作執行。如果網路規模較大，最好放置共用資料夾到專用檔案資源以便降低管理伺服器裝置磁碟子系統的負載。

透過傳送 UNC 路徑到獨立安裝套件遠端安裝

如果組織網路裝置使用者具有本機管理員權限，另一個初始化佈署方法就是建立一個獨立網路代理安裝套件（或者一個與安全應用程式一起的"連結的"網路代理安裝套件）。在您建立獨立安裝套件後，傳送給使用者一個位於共用資料夾中的安裝套件的連結。當使用者點擊連結時安裝開始。

使用管理伺服器共用資料夾更新

在病毒更新工作中，您可以配置從管理伺服器共用資料夾更新。如果工作被分配了大量裝置，最好放置共用資料夾到專用檔案資源。

安裝作業系統映像

作業系統映像總是透過共用資料夾安裝：裝置從共用資料夾讀取作業系統映像。如果映像佈署被分配了大量組織裝置，最好放置共用資料夾到專用檔案資源。

指定管理伺服器位址

安裝管理伺服器時，您可以指定管理伺服器的位址。該位址將用作建立網路代理安裝套件時的預設位址。

作為管理伺服器位址，您可以指定以下內容：

- 管理伺服器的 NetBIOS 名稱（預設指定）
- 管理伺服器的完整網域名稱 (FQDN)（如果組織網路上的網域名稱系統 (DNS) 已配置且運行正常）
- 外部位址（如果管理伺服器安裝在隔離區域 (DMZ) 中）

此後，您將可以透過使用管理主控台工具變更管理伺服器位址；此位址將不會在所建立的網路代理安裝套件中自動變更。

標準安裝

標準安裝是使用應用程式檔案預設路徑的管理伺服器安裝，安裝預設外掛程式集，不啟用行動裝置管理。

要在本機裝置上安裝卡巴斯基安全管理中心管理伺服器：

執行 ksc_<版本號>.<組建編號>_full_<中文化語言>.exe 可執行檔。

將開啟 Kaspersky 應用程式選取安裝的提示視窗。在應用程式選取視窗，按一下**安裝卡巴斯基安全管理中心管理伺服器**連結，來啟動管理伺服器安裝精靈。遵照精靈的說明。

步驟 1：檢視產品授權協議和隱私政策

在安裝精靈的此步驟，您必須閱讀您與 Kaspersky 之間的授權協議以及隱私政策。

您也可以從卡巴斯基安全管理中心分發套件中的應用程式管理外掛程式檢視授權協議和隱私政策。

請仔細閱讀產品授權協議和隱私政策。如果您同意產品授權協議和隱私政策的所有條款，請選中相應的核取方塊進行確認。

在您選取兩個核取方塊後，您裝置上的應用程式安裝將繼續。

如果您不同意此產品授權協議或隱私政策，請按一下**取消**按鈕，取消安裝。

步驟 2：選取安裝方式

在安裝類型選取視窗，選取**標準**。

標準安裝用在您要嘗試卡巴斯基安全管理中心並在企業網路中的小區域測試其操作的時候。在標準安裝期間，您僅設定資料庫。您不指定任何管理伺服器設定：它們的預設值被使用。標準安裝不允許您選取要安裝的管理外掛程式；僅預設的外掛程式集被安裝。在標準安裝期間，不建立行動裝置安裝套件。然而，您可以稍後在管理主控台建立它們。

步驟 3：安裝卡巴斯基安全管理中心網頁主控台

該步驟僅在您使用 64 位元作業系統時顯示。否則，該步驟不被顯示，因為卡巴斯基安全管理中心網頁主控台不工作在 32 位元作業系統下。

預設將同時安裝卡巴斯基安全管理中心網頁主控台和 MMC 型管理主控台。

如果僅要安裝卡巴斯基安全管理中心網頁主控台，請執行以下操作：

1. 選取**僅安裝這一項**。
2. 在下拉清單中選擇**網頁型主控台**。

管理伺服器安裝完成後，將自動開始安裝卡巴斯基安全管理中心網頁主控台。

如果只想安裝 MMC 型管理主控台，請執行以下操作：

1. 選取**僅安裝這一項**。
2. 在下拉清單中選擇 **MMC 型主控台**。

步驟 4：選擇網路大小

指定要安裝卡巴斯基安全管理中心的網路的大小。精靈會根據網路上的裝置數量設定應用程式介面的安裝設定和外觀以求相符。

下表列出了在不同的網路規模下應用程式安裝設定和應用程式介面外觀的不同。

依據選取的網路規模所設定的內容區別

設定	1–100 台受管理裝置	101–1000 台受管理裝置	1001 到 5000 台受管理裝置	多於 5000 台受管理裝置
顯示從屬和虛擬管理伺服器的節點，以及與從屬和虛擬管理伺服器相關的所有設定（僅在基於 MMC 的管理主控台中可用）	不適用	不適用	適用	適用
在管理伺服器和管理群組的屬性視窗中顯示**安全性**部分（僅在基於 MMC 的管理主控台中可用）	不適用	不適用	適用	適用
用戶端裝置的更新工作的隨機啟動時間	不適用	以 5 分鐘為間隔	以 10 分鐘為間隔	以 10 分鐘為間隔

如果您的管理伺服器使用 MySQL 5.7 或 SQL Express 資料庫，建議您管理的裝置在 10,000 台以下。對於 MariaDB 資料庫管理系統，建議的最大受管理裝置數量為 20000。

步驟 5：選取一個資料庫

在精靈的此步驟中，選取以下資料庫管理系統 (DBMS) 之一，將其用於儲存管理伺服器資料庫：

- **Microsoft SQL Server 或者 SQL Server Express**
- **MySQL 或者 MariaDB**
- **PostgreSQL 或者 Postgres Pro**

建議將管理伺服器安裝在專用伺服器上而不是網域控制器上。然而，若在作為唯讀網域控制器 (RODC) 的伺服器上安裝卡巴斯基安全管理中心，則不得在相同裝置上安裝 Microsoft SQL Server (SQL Express)。在此情況下，建議您遠端安裝 Microsoft SQL Server (SQL Express)（在不同裝置上），如果需要本機安裝 DBMS，則使用 MySQL、MariaDB 或 PostgreSQL。

管理伺服器資料庫結構提供在 klakdb.chm 檔案，它位於卡巴斯基安全管理中心安裝資料夾。Kaspersky 入口網站也以壓縮格式提供這個檔案：klakdb.zip。

步驟 6：設定 SQL Server

在精靈的此步驟中，請根據您選取的資料庫管理系統 (DBMS)，指定以下連線設定：

- 若您已在先前步驟選取**Microsoft SQL Server 或者 SQL Server Express**：
  - 在**SQL Server 實例名稱**欄位，指定網路中的 SQL Server 名稱。要檢視網路上的所有 SQL Server 清單，請點擊**瀏覽**按鈕。預設情況下該欄位為空。

    若您透過自訂連接埠連線 SQL Server，請連同 SQL Server 主機名稱一起指定埠號並用逗號區隔，例如：

    ```
    SQL_Server_host_name,1433
    ```

    若您要透過憑證保障管理伺服器與 SQL Server 的通訊，請在**SQL Server 實例名稱**欄位中指定與在產生憑證時使用的相同主機名稱。若您使用已命名的 SQL Server 名稱，請連同 SQL Server 主機名稱一起指定埠號並用逗號區隔，例如：

    ```
    SQL_Server_name,1433
    ```

    若您在相同主機上使用數個 SQL Server 實例，請額外以反斜線區隔來指定實例名稱，例如：

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

    如果企業網路上的 SQL Server 啟用了 Always On 功能，請在**SQL Server 實例名稱**欄位中指定可用性群組接聽程式的名稱。請注意，當 Always On 功能啟用時，管理伺服器僅支援同步提交可用性模式。
  - 在**資料庫名稱**欄位中，指定被建立用來儲存管理伺服器資料的 DBMS 的名稱。預設值是 *KAV*。

  如果此階段您要在正安裝卡巴斯基安全管理中心的裝置上安裝 SQL Server，您必須終止安裝卡巴斯基安全管理中心，並在 SQL Server 安裝完成後重新啟動卡巴斯基安全管理中心的安裝。支援的 SQL Server 版本在系統需求中列出。

  如果您要在遠端裝置上安裝 SQL Server，您無須取消卡巴斯基安全管理中心的安裝精靈。安裝 SQL Server，並恢復執行卡巴斯基安全管理中心的安裝。
- 若您已在先前步驟中選取**MySQL 或者 MariaDB**：
  - 在**SQL Server 實例名稱**欄位，指定 SQL Server 實例名稱。預設下，名稱是要安裝卡巴斯基安全管理中心的裝置的 IP 位址。
  - 在**連接埠**欄位中，指定管理伺服器連線到 DBMS 的連接埠。預設埠號為 3306。
  - 在**資料庫名稱**欄位中，指定被建立用來儲存管理伺服器資料的 DBMS 的名稱。預設值是 *KAV*。
- 若您已在先前步驟中選取 **PostgreSQL 或者 Postgres Pro**：
  - 在**PostgreSQL 或者 Postgres Pro 伺服器**欄位，指定 DBMS 實例名稱。預設下，名稱是要安裝卡巴斯基安全管理中心的裝置的 IP 位址。
  - 在**連接埠**欄位中，指定管理伺服器連線到 DBMS 的連接埠。預設埠號為 5432。
  - 在**資料庫名稱**欄位中，指定被建立用來儲存管理伺服器資料的 DBMS 的名稱。預設值是 *KAV*。

步驟 7：選取身分驗證模式

決定管理伺服器連線到資料庫管理系統 (DBMS) 時將使用的身分驗證模式。

依據您選取的 DBMS，您可以選取以下其中之一的身分驗證模式：

- 對於 SQL Express 或 Microsoft SQL Server，請選取以下選項之一：
  - **Microsoft Windows 身分驗證模式**。使用啟動管理伺服器的帳戶來驗證權限。
  - **SQL Server 身分驗證模式**。如果您選取此選項，將會使用您指定的帳戶進行驗證。填寫**"帳戶"**、**"密碼"**欄位。

    要檢視輸入的密碼，點擊並按住**顯示**按鈕。

  對於兩個身分驗證模式，應用程式檢查資料庫是否可用。如果資料庫不可用，則顯示錯誤訊息，且您必須提供正確的憑證。

  如果您的管理伺服器資料庫是存放在別台裝置上，並且管理伺服器的帳戶無法存取該資料庫伺服器，您必須使用 SQL Server 身分驗證模式。SQL Server 身分驗證模式來進行安裝及升級您的管理伺服器。這種情況可能會發生在資料庫伺服器不在網域當中，或您指定的管理伺服器帳戶為「LocalSystem」帳戶。

- 若為 MySQL、MariaDB、PostgreSQL 或 Postgres Pro，請指定帳戶和密碼。

步驟 8：在硬碟磁碟機上解壓縮並安裝檔案

在您安裝完成卡巴斯基安全管理中心，並且都設定完畢了之後，可以在硬碟磁碟機上安裝檔案。

如果安裝需要其他程式，安裝精靈在開始安裝卡巴斯基安全管理中心之前，在**"正在安裝系統所需之相依套件"**頁面中通知您。所需程式將在您點選**"下一步"**按鈕後自動安裝。

在最後一頁，您可以選取啟動哪個主控台以使用卡巴斯基安全管理中心：

- **啟動基於 MMC 的管理主控台**
- **啟動卡巴斯基安全管理中心網頁主控台**

  此選項僅在您在先前步驟中選取了安裝卡巴斯基安全管理中心 網頁主控台時可用。

您也可以點擊**完成**以關閉精靈而不使用卡巴斯基安全管理中心。您可以稍後隨時開始使用。

在管理主控台或者卡巴斯基安全管理中心 網頁主控台第一次啟動時，您可以執行應用程式初始化設定。

安裝精靈完成後，以下程式元件便會安裝在作業系統所在的硬碟磁碟機：

- 管理伺服器（包含了管理伺服器版本的網路代理）
- 基於 Microsoft Management Console 的管理主控台
- 卡巴斯基安全管理中心 網頁主控台（如果您選取安裝）
- 應用程式管理外掛程式在分發套件中可用

另外，Microsoft Windows Installer 4.5 如果先前未安裝，則將被安裝。

自訂安裝

自訂安裝是指在管理伺服器安裝過程中您可以選取要安裝的元件並指定應用程式被安裝到的資料夾。

使用該安裝類型，您可以設定資料庫和管理伺服器，以及安裝不包含在標準安裝中的元件或眾多 Kaspersky 安全應用程式的管理外掛程式。您也可以啟用行動裝置管理。

要在本機裝置上安裝卡巴斯基安全管理中心管理伺服器：

執行 ksc_<版本號>.<組建編號>_full_<中文化語言>.exe 可執行檔。

將開啟 Kaspersky 應用程式選取安裝的提示視窗。在應用程式選取視窗，按一下**安裝卡巴斯基安全管理中心管理伺服器**連結，來啟動管理伺服器安裝精靈。遵照精靈的說明。

步驟 1：檢視產品授權協議和隱私政策

在安裝精靈的此步驟，您必須閱讀您與 Kaspersky 之間的授權協議以及隱私政策。

您也可以從卡巴斯基安全管理中心分發套件中的應用程式管理外掛程式檢視授權協議和隱私政策。

請仔細閱讀產品授權協議和隱私政策。如果您同意產品授權協議和隱私政策的所有條款，請選中相應的核取方塊進行確認。

在您選取兩個核取方塊後，您裝置上的應用程式安裝將繼續。

如果您不同意此產品授權協議或隱私政策，請按一下**取消**按鈕，取消安裝。

步驟 2：選取安裝方式

在安裝類型選取視窗，選取**自訂**。

自訂安裝允許您修改卡巴斯基安全管理中心設定，例如共用資料夾路徑、帳戶和連線管理伺服器的連接埠，以及資料庫設定。自訂安裝允許您指定安裝哪些 Kaspersky 管理外掛程式。在自訂安裝期間，您可以透過啟用相關選項為行動裝置建立安裝套件。

步驟 3：選取要安裝的元件

選取您要安裝的卡巴斯基安全管理中心管理伺服器的元件：

- **行動裝置管理**。如果您要在卡巴斯基安全管理中心安裝精靈執行時為行動裝置建立安裝套件，則選取此核取方塊。您也可以在管理伺服器安裝後，使用管理主控台工具手動建立行動裝置安裝套件。
- **SNMP 代理**。此元件可透過 SNMP 協定接收管理伺服器上的統計資訊。此元件僅在有安裝 SNMP 的裝置上運作。

  在卡巴斯基安全管理中心安裝後，.mib 檔案將存放於程式安裝目錄下的 SNMP 子資料夾。

網路代理和管理主控台並不會在元件清單中顯示。這些元件是必要元件，安裝程式將會自動安裝它們。

在此步驟中，您需要指定管理伺服器的安裝資料夾位置。依預設會將元件安裝在 <磁碟機>:\Program Files\Kaspersky Lab\Kaspersky Security Center。如果資料夾不存在，則會在安裝過程中自動建立。您可以使用**瀏覽**按鈕變更目的資料夾。

步驟 4：安裝卡巴斯基安全管理中心網頁主控台

該步驟僅在您使用 64 位元作業系統時顯示。否則，該步驟不被顯示，因為卡巴斯基安全管理中心網頁主控台不工作在 32 位元作業系統下。

預設將同時安裝卡巴斯基安全管理中心網頁主控台和 MMC 型管理主控台。

如果僅要安裝卡巴斯基安全管理中心網頁主控台，請執行以下操作：

1. 選取**僅安裝這一項**。
2. 在下拉清單中選擇**網頁型主控台**。

管理伺服器安裝完成後，將自動開始安裝卡巴斯基安全管理中心網頁主控台。

如果只想安裝 MMC 型管理主控台，請執行以下操作：

1. 選取**僅安裝這一項**。
2. 在下拉清單中選擇 **MMC 型主控台**。

步驟 5：選擇網路大小

指定要安裝卡巴斯基安全管理中心的網路的大小。精靈會根據網路上的裝置數量設定應用程式介面的安裝設定和外觀以求相符。

下表列出了在不同的網路規模下應用程式安裝設定和應用程式介面外觀的不同。

依據選取的網路規模所設定的內容區別

設定	1–100 台受管理裝置	101–1000 台受管理裝置	1001 到 5000 台受管理裝置	多於 5000 台受管理裝置
顯示從屬和虛擬管理伺服器的節點，以及與從屬和虛擬管理伺服器相關的所有設定（僅在基於 MMC 的管理主控台中可用）	不適用	不適用	適用	適用
在管理伺服器和管理群組的屬性視窗中顯示**安全性**部分（僅在基於 MMC 的管理主控台中可用）	不適用	不適用	適用	適用
用戶端裝置的更新工作的隨機啟動時間	不適用	以 5 分鐘為間隔	以 10 分鐘為間隔	以 10 分鐘為間隔

如果您的管理伺服器使用 MySQL 5.7 或 SQL Express 資料庫，建議您管理的裝置在 10,000 台以下。對於 MariaDB 資料庫管理系統，建議的最大受管理裝置數量為 20000。

步驟 6：選取一個資料庫

在精靈的此步驟中，選取以下資料庫管理系統 (DBMS) 之一，將其用於儲存管理伺服器資料庫：

- **Microsoft SQL Server 或者 SQL Server Express**
- **MySQL 或者 MariaDB**
- **PostgreSQL 或者 Postgres Pro**

建議將管理伺服器安裝在專用伺服器上而不是網域控制器上。然而，若在作為唯讀網域控制器 (RODC) 的伺服器上安裝卡巴斯基安全管理中心，則不得在相同裝置上安裝 Microsoft SQL Server (SQL Express)。在此情況下，建議您遠端安裝 Microsoft SQL Server (SQL Express)（在不同裝置上），如果需要本機安裝 DBMS，則使用 MySQL、MariaDB 或 PostgreSQL。

管理伺服器資料庫結構提供在 klakdb.chm 檔案，它位於卡巴斯基安全管理中心安裝資料夾。Kaspersky 入口網站也以壓縮格式提供這個檔案：klakdb.zip。

步驟 7：設定 SQL Server

在精靈的此步驟中，請根據您選取的資料庫管理系統 (DBMS)，指定以下連線設定：

- 若您已在先前步驟選取**Microsoft SQL Server 或者 SQL Server Express**：
  - 在**SQL Server 實例名稱**欄位，指定網路中的 SQL Server 名稱。要檢視網路上的所有 SQL Server 清單，請點擊**瀏覽**按鈕。預設情況下該欄位為空。

    若您透過自訂連接埠連線 SQL Server，請連同 SQL Server 主機名稱一起指定埠號並用逗號區隔，例如：

    ```
    SQL_Server_host_name,1433
    ```

    若您要透過憑證保障管理伺服器與 SQL Server 的通訊，請在**SQL Server 實例名稱**欄位中指定與在產生憑證時使用的相同主機名稱。若您使用已命名的 SQL Server 名稱，請連同 SQL Server 主機名稱一起指定埠號並用逗號區隔，例如：

    ```
    SQL_Server_name,1433
    ```

    若您在相同主機上使用數個 SQL Server 實例，請額外以反斜線區隔來指定實例名稱，例如：

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

    如果企業網路上的 SQL Server 啟用了 Always On 功能，請在**SQL Server 實例名稱**欄位中指定可用性群組接聽程式的名稱。請注意，當 Always On 功能啟用時，管理伺服器僅支援同步提交可用性模式。
  - 在**資料庫名稱**欄位中，指定被建立用來儲存管理伺服器資料的 DBMS 的名稱。預設值是 *KAV*。

  如果此階段您要在正安裝卡巴斯基安全管理中心的裝置上安裝 SQL Server，您必須終止安裝卡巴斯基安全管理中心，並在 SQL Server 安裝完成後重新啟動卡巴斯基安全管理中心的安裝。支援的 SQL Server 版本在系統需求中列出。

  如果您要在遠端裝置上安裝 SQL Server，您無須取消卡巴斯基安全管理中心的安裝精靈。安裝 SQL Server，並恢復執行卡巴斯基安全管理中心的安裝。
- 若您已在先前步驟中選取**MySQL 或者 MariaDB**：
  - 在**SQL Server 實例名稱**欄位，指定 SQL Server 實例名稱。預設下，名稱是要安裝卡巴斯基安全管理中心的裝置的 IP 位址。
  - 在**連接埠**欄位中，指定管理伺服器連線到 DBMS 的連接埠。預設埠號為 3306。
  - 在**資料庫名稱**欄位中，指定被建立用來儲存管理伺服器資料的 DBMS 的名稱。預設值是 *KAV*。
- 若您已在先前步驟中選取 **PostgreSQL 或者 Postgres Pro**：
  - 在**PostgreSQL 或者 Postgres Pro 伺服器**欄位，指定 DBMS 實例名稱。預設下，名稱是要安裝卡巴斯基安全管理中心的裝置的 IP 位址。
  - 在**連接埠**欄位中，指定管理伺服器連線到 DBMS 的連接埠。預設埠號為 5432。
  - 在**資料庫名稱**欄位中，指定被建立用來儲存管理伺服器資料的 DBMS 的名稱。預設值是 *KAV*。

步驟 8：選取身分驗證模式

決定管理伺服器連線到資料庫管理系統 (DBMS) 時將使用的身分驗證模式。

依據您選取的 DBMS，您可以選取以下其中之一的身分驗證模式：

- 對於 SQL Express 或 Microsoft SQL Server，請選取以下選項之一：
  - **Microsoft Windows 身分驗證模式**。使用啟動管理伺服器的帳戶來驗證權限。
  - **SQL Server 身分驗證模式**。如果您選取此選項，將會使用您指定的帳戶進行驗證。填寫**"帳戶"**、**"密碼"**欄位。

    要檢視輸入的密碼，點擊並按住**顯示**按鈕。

  對於兩個身分驗證模式，應用程式檢查資料庫是否可用。如果資料庫不可用，則顯示錯誤訊息，且您必須提供正確的憑證。

  如果您的管理伺服器資料庫是存放在別台裝置上，並且管理伺服器的帳戶無法存取該資料庫伺服器，您必須使用 SQL Server 身分驗證模式。SQL Server 身分驗證模式來進行安裝及升級您的管理伺服器。這種情況可能會發生在資料庫伺服器不在網域當中，或您指定的管理伺服器帳戶為「LocalSystem」帳戶。

- 若為 MySQL、MariaDB、PostgreSQL 或 Postgres Pro，請指定帳戶和密碼。

步驟 9：選取帳戶以啟動管理伺服器

選取用於啟動管理伺服器作為服務的帳戶。

- **自動產生帳戶**。應用程式會建立名為 KL-AK-* 的帳戶，kladminserver 服務會在該帳戶下執行。

  如果您排程將共用資料夾和 DBMS 放置在管理伺服器所在裝置。

- **選取帳戶**。管理伺服器服務 (kladminserver) 將在您選取的帳戶下執行。

  如果您計畫使用其他裝置上任何版本的 SQL Server 實例（包括 SQL Express）作為 DBMS，且/或您計畫在其他裝置放置共用資料夾，您必須選取網域帳戶。

  卡巴斯基安全管理中心支援受管理服務帳戶 (MSA) 和受群組管理的服務帳戶 (gMSA)。如果這些帳戶類型在您的網域中被使用，您可以選取它們之一作為管理伺服器服務帳戶。

  在指定 MSA 或 gMSA 之前，您必須將帳戶安裝在要安裝管理伺服器的同一裝置上。如果尚未安裝該帳戶，請取消管理伺服器安裝，在安裝該帳戶後，再重新啟動管理伺服器安裝。如需在本機裝置上安裝受管理服務帳戶的詳細資訊，請參閱正式的 Microsoft 文件。

  若要指定 MSA 或 gMSA：

  1. 按一下**瀏覽**按鈕。
  2. 在開啟的視窗中，按一下**物件類型**按鈕。
  3. 選取**服務帳戶**類型並點擊**確定**。
  4. 選取相關帳戶並按一下**確定**。

您選取的帳戶必須有不同的權限，取決於您排程使用的 DBMS。

出於安全原因，請不要分配權限狀態到您執行管理伺服器的帳戶。

管理伺服器帳戶以後不能變更。您需要重新安裝故障移轉叢集以使用另一個管理伺服器帳戶。

步驟 10：選取帳戶以執行卡巴斯基安全管理中心服務

在裝置上選取即將執行卡巴斯基安全管理中心服務的帳戶：

- **自動產生帳戶**。卡巴斯基安全管理中心在 kladmins 群組的裝置上建立名為 KlScSvc 的本機帳戶。卡巴斯基安全管理中心服務將在已建立的帳戶下執行。
- **選取帳戶**。卡巴斯基安全管理中心服務將執行在您選取的帳戶下。

  您將必須選取網域帳戶，如果您要儲存報告到不同裝置的資料夾，或基於您組織的安全政策。如果您安裝管理伺服器到失敗轉移叢集，您也可能必須選取網域帳戶。

出於安全原因，請不要分配權限狀態到您執行服務的帳戶。

KSN 代理服務 (ksnproxy)、Kaspersky 啟動代理服務 (klactprx) 和 Kaspersky 身分驗證入口服務 (klwebsrv) 將在所選帳戶下執行。

步驟 11：選取共用資料夾

在此步驟中，安裝精靈將請您指定共用資料夾的目錄和名稱：

- 儲存遠端安裝程式所需的檔案（這些檔案會在建立安裝套件過程中複製到管理伺服器）。
- 儲存管理伺服器從網際網路上下載的更新檔案。

檔案分享的權限會是所有的使用者（僅有讀取的權限）。

您可以選取以下選項其中之一：

- **建立共用資料夾**。建立一個新的資料夾。在文字方塊中，指定資料夾路徑。
- **選取現有共用資料夾**。選取一個已有的共用資料夾。

此共用資料夾可以是此裝置上（正在安裝卡巴斯基安全管理中心的裝置），或是企業網路環境中的任何一台裝置上的共用資料夾。您可以點擊**"瀏覽"**按鈕來選取共用資料夾或請您在下方的欄位中，手動輸入共用資料夾的 UNC 路徑（例如：\\server\Share）。

在預設的情況下，安裝精靈會替您在卡巴斯基安全管理中心的目錄下，自動建立一個共用名稱為 KLSHARE 的本機資料夾。

如果需要，您可以稍後定義共用資料夾。

步驟 12：設定與管理伺服器的連線

設定與管理伺服器的連線：

- **連接埠**

  用於連線至管理伺服器的埠號。

  預設埠號為 14000。

- **SSL 連接埠**

  用於安全地連線至管理伺服器的安全通訊端層 (SSL) 埠號。

  預設埠號為 13000。

- **加密金鑰長度**

  選取加密金鑰長度：1024 bit 或 2048 bit。

  1024-bit 加密金鑰少量佔用 CPU，但它被認為是過時的，因為由於技術說明，它無法提供可靠的加密。而且，現有硬體可能與 1024-bit 金鑰的 SSL 憑證不相容。

  2048-bit 加密金鑰滿足所有加密標準。然而，使用 2048-bit 加密金鑰可能增加 CPU 負載。

  依預設會選取 **2048 bit（最大安全）**。

您也可以稍後變更連線到管理伺服器的參數，如下所示：

- 您也可以在管理伺服器屬性的**連線連接埠**部分中變更連接埠和 SSL 連接埠號。有關管理伺服器連接埠的更多資訊，請參閱卡巴斯基安全管理中心使用的連接埠。
- 當使用 klsetsrvcert 公用程式取代管理伺服器憑證時，您可以使用 `-o RsaKeyLen:<金鑰長度>` 參數來變更加密金鑰長度。

步驟 13：定義管理伺服器位址

請用下列方式之一指定管理伺服器位址：

- **DNS 網域名稱**。如果網路包含 DNS 伺服器且用戶端裝置可以使用它來接收管理伺服器位址，則您可以使用此方法。
- **NetBIOS 名稱**。如果用戶端裝置使用 NetBIOS 協定接收管理伺服器位址，或者網路中可使用 WINS 伺服器，則您可以使用此方法。
- **IP 位址**。如果管理伺服器擁有將來不會變更的靜態 IP 位址，則您可以使用此方法。

如果您在卡巴斯基安全管理中心容錯移轉叢集的主動節點上安裝卡巴斯基安全管理中心，並且在準備叢集節點時建立了一個從屬網路介面卡，請指定此介面卡的 IP 位址。否則，請輸入您使用的協力廠商負載均衡器的 IP 位址。

步驟 14：指定行動裝置連線到管理伺服器的位址

如果選取了安裝“行動裝置管理”元件，則安裝精靈會出現這一步。

在**行動裝置連線的位址**視窗中，指定管理伺服器外部位址以連線本機網路之外的行動裝置。您可以指定管理伺服器的 IP 位址或網域名稱系統 (DNS)。

步驟 15：選取應用程式管理外掛程式

選取需要與卡巴斯基安全管理中心一起安裝的程式管理外掛程式。

為了搜尋方便，外掛程式被根據安全物件類型分成了群組。

步驟 16：在硬碟磁碟機上解壓縮並安裝檔案

在您安裝完成卡巴斯基安全管理中心，並且都設定完畢了之後，可以在硬碟磁碟機上安裝檔案。

如果安裝需要其他程式，安裝精靈在開始安裝卡巴斯基安全管理中心之前，在“**正在安裝系統所需之相依套件**”頁面中通知您。所需程式將在您點選“**下一步**”按鈕後自動安裝。

在最後一頁，您可以選取啟動哪個主控台以使用卡巴斯基安全管理中心：

- **啟動基於 MMC 的管理主控台**
- **啟動卡巴斯基安全管理中心網頁主控台**
  此選項僅在您在先前步驟中選取了安裝卡巴斯基安全管理中心 網頁主控台時可用。

您也可以點擊**完成**以關閉精靈而不使用卡巴斯基安全管理中心。您可以稍後隨時開始使用。

在管理主控台或者卡巴斯基安全管理中心 網頁主控台第一次啟動時，您可以執行應用程式初始化設定。

部署卡巴斯基安全管理中心容錯移轉叢集

本節包含關於卡巴斯基安全管理中心容錯移轉叢集的一般資訊，以及有關在您的網路中準備和部署卡巴斯基安全管理中心容錯移轉叢集的指示。

情境：部署卡巴斯基安全管理中心容錯移轉叢集

卡巴斯基安全管理中心容錯移轉叢集提供卡巴斯基安全管理中心的高可用性，並在出現故障時最大限度地減少管理伺服器的停機時間。容錯移轉叢集基於安裝在兩台電腦上的兩個相同的卡巴斯基安全管理中心例項。其中一個例項用作主動節點，另一個例項用作被動節點。主動節點負責管理用戶端裝置的防護，而被動節點則準備在主動節點出現故障時承擔主動節點的所有功能。當發生故障時，被動節點變為主動節點，主動節點變為被動節點。

先決條件

您擁有滿足容錯移轉叢集要求的硬體。

階段

Kaspersky 應用程式佈署分步驟進行：

1. **為卡巴斯基安全管理中心服務建立帳戶**

   建立一個新的網域群組（在此狀況中為此群組使用名稱「KLAdmins」），然後在兩個節點和檔案伺服器上向該群組授予本機管理員權限。然後建立兩個新的網域使用者帳戶（在此狀況下，為這些帳戶使用名稱「ksc」和「rightless」），並將這些帳戶新增到 KLAdmins 網域群組。

   將要安裝卡巴斯基安全管理中心的使用者帳戶新增至之前建立的 KLAdmins 網域群組。

2. **檔案伺服器準備**

   準備檔案伺服器作為卡巴斯基安全管理中心容錯移轉叢集的一個元件。確保檔案伺服器滿足硬體和軟體要求，為卡巴斯基安全管理中心資料建立兩個共用資料夾，並配置存取共用資料夾的權限。

   說明：為卡巴斯基安全管理中心容錯移轉叢集準備檔案伺服器

3. **準備主動和被動節點**

   準備兩台具有相同硬體和軟體的裝置作為主動節點和被動節點。

   說明：為卡巴斯基安全管理中心容錯移轉叢集準備節點

4. **資料庫管理系統 (DBMS) 安裝**

   選取任何一個受支援的 DBMS，然後在專用裝置上安裝 DBMS。對於如何安裝 DBMS 的資訊，請參考其文件。

5. **卡巴斯基安全管理中心安裝**

   在兩個節點上以容錯移轉叢集模式安裝卡巴斯基安全管理中心。您必須先在想要其成為主動主機的裝置上安裝卡巴斯基安全管理中心，然後再將其安裝在被動主機上。

   您必須在不是叢集節點的單獨裝置上安裝卡巴斯基安全管理中心網頁主控台。

   說明：在卡巴斯基安全管理中心容錯移轉叢集節點上安裝卡巴斯基安全管理中心

6. **測試容錯移轉叢集**

   檢查您是否正確配置了容錯移轉叢集以及它是否正常工作。例如，您可以在主動節點上停止卡巴斯基安全管理中心服務之一：kladminserver、klnagent、ksnproxy、klactprx 或 klwebsrv。服務停止後，防護管理必須自動切換到被動節點。

結果

卡巴斯基安全管理中心容錯移轉叢集已部署。請熟悉導致主動節點和被動節點之間切換的事件。

關於卡巴斯基安全管理中心容錯移轉叢集

卡巴斯基安全管理中心容錯移轉叢集提供卡巴斯基安全管理中心的高可用性，並在出現故障時最大限度地減少管理伺服器的停機時間。容錯移轉叢集基於安裝在兩台電腦上的兩個相同的卡巴斯基安全管理中心例項。其中一個例項用作主動節點，另一個例項用作被動節點。主動節點負責管理用戶端裝置的防護，而被動節點則準備在主動節點出現故障時承擔主動節點的所有功能。當發生故障時，被動節點變為主動節點，主動節點變為被動節點。

使用容錯移轉叢集不會影響基於規模指南的計算。

使用卡巴斯基事件記錄功能進行故障排除。

切換條件

如果主動節點上發生以下任何事件，容錯移轉叢集會將用戶端裝置的防護管理從主動節點切換到被動節點：

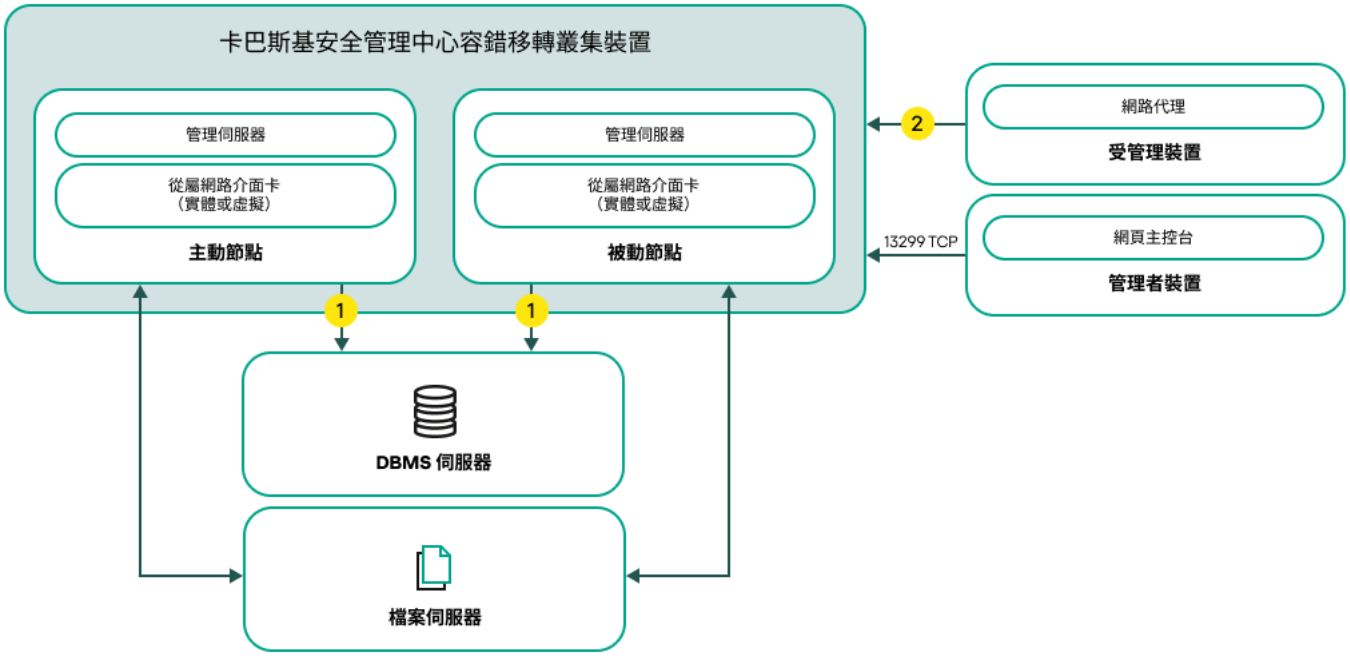
- 主動節點由於軟體或者硬體故障而損壞。
- 主動節點因為維護活動被暫時停止。
- 至少一項卡巴斯基安全管理中心服務（或處理程序）失敗或被使用者故意終止。卡巴斯基安全管理中心服務如下：kladminserver、klnagent、klactprx 和 klwebsrv。
- 主動節點與檔案伺服器上的儲存之間的網路連線被中斷或終止。

卡巴斯基安全管理中心容錯移轉叢集會自動管理所有卡巴斯基安全管理中心服務。請勿手動重啟服務。

部署方案

您可以選擇以下方案之一來部署卡巴斯基安全管理中心容錯移轉叢集：

- 使用從屬網路介面卡的方案。
- 使用協力廠商負載均衡器的方案。

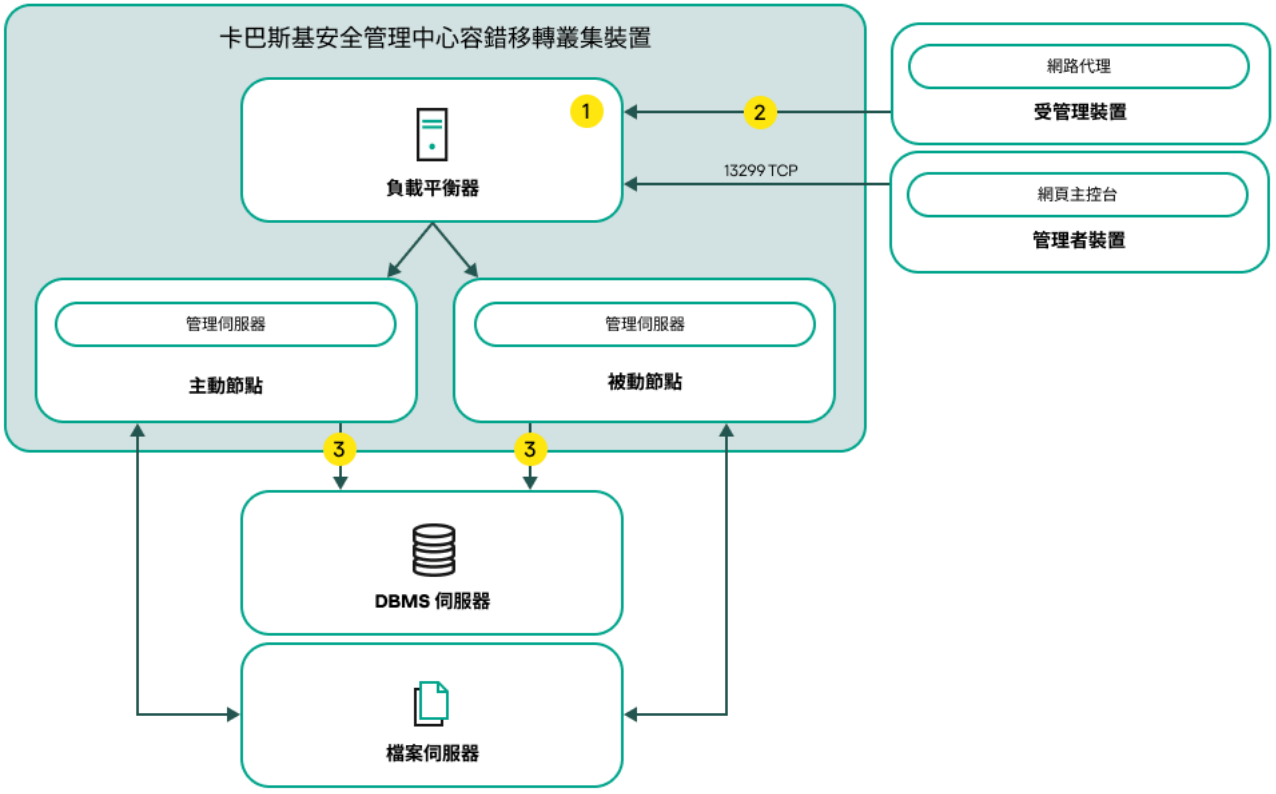


使用從屬網路介面卡的方案

方案圖例：

1 管理伺服器傳送資料到資料庫。在資料庫所在裝置上開啟必要的連接埠，例如MySQL Server 為 3306 連接埠，Microsoft SQL Server 為 1433 連接埠。請參閱 DBMS 文件以取得相關資訊。

2 在受管理裝置上，開啟以下連接埠：TCP 13000、UDP 13000 和 TCP 17000。



使用協力廠商負載均衡器的方案

方案圖例：

1 在負載均衡器裝置上，開啟所有管理伺服器連接埠：TCP 13000、UDP 13000、TCP 13299 和 TCP 17000。

> 如果想使用 klakaut 實用程式進行自動化，您還必須開啟 TCP 13291 連接埠。

2 在受管理裝置上，開啟以下連接埠：TCP 13000、UDP 13000 和 TCP 17000。

3 管理伺服器傳送資料到資料庫。在資料庫所在裝置上開啟必要的連接埠，例如MySQL Server 為 3306 連接埠，Microsoft SQL Server 為 1433 連接埠。請參閱 DBMS 文件以取得相關資訊。

為卡巴斯基安全管理中心容錯移轉叢集準備檔案伺服器

檔案伺服器是卡巴斯基安全管理中心容錯移轉叢集的一個必需元件 。

要準備檔案伺服器：

1. 確保檔案伺服器滿足硬體和軟體要求。
2. 確保檔案伺服器和兩個節點（主動和被動）包含在同一個網域中，或者檔案伺服器是網域控制器。

3. 在檔案伺服器上，建立兩個共用資料夾。其中之一用於保存有關容錯移轉叢集狀態的資訊。另一個用於儲存卡巴斯基安全管理中心的資料和設定。您將在配置卡巴斯基安全管理中心的安裝時指定共用資料夾的路徑。

4. 為以下使用者帳戶和群組授予對建立的共用資料夾的完全存取權限（共用權限和 NTFS 權限）：

   - 網域群組 KLAdmins。
   - 使用者帳戶 $<node1>和 $<node2>。這裡，<node1> 和 <node2> 分別是主動節點和被動節點的裝置名稱。

檔案伺服器已準備就緒。若要部署卡巴斯基安全管理中心容錯移轉叢集，請按照此情境中的進一步說明進行操作。

為卡巴斯基安全管理中心容錯移轉叢集準備節點

準備兩台裝置作為卡巴斯基安全管理中心容錯移轉叢集的主動節點和被動節點。

要為卡巴斯基安全管理中心容錯移轉叢集準備節點：

1. 確保您有兩台滿足硬體和軟體需求的裝置。這些裝置將充當容錯移轉叢集的主動節點和被動節點。

2. 確保檔案伺服器和兩個節點都包含在同一個網域中。

3. 執行以下操作之一：

   - 在每個節點上，配置一個從屬網路介面卡。

     從屬網路介面卡可以是實體的，也可以是虛擬的。如果要使用實體網路介面卡，請使用標準作業系統工具連接並配置它。如果要使用虛擬網路介面卡，請使用協力廠商軟體建立它。

     確保滿足以下條件：

     - 從屬網路介面卡被停用。

       您可以建立處於停用狀態的從屬網路介面卡或在建立後停用它們。

     - 兩個節點上的從屬網路介面卡具有相同的 IP 位址。

   - 使用協力廠商負載均衡器。例如，您可以使用 nginx 伺服器。在這種情況下，請執行以下操作：

     a. 提供一台安裝了 nginx 的基於 Linux 的專用裝置。

     b. 配置負載均衡。設定主動節點為主伺服器，被動節點為備份伺服器。

     c. 在 nginx 伺服器上，開啟所有管理伺服器連接埠：TCP 13000、UDP 13000、TCP 13299 和 TCP 17000。

     > 如果想使用 klakaut 實用程式進行自動化，您還必須開啟 TCP 13291 連接埠。

4. 重新啟動節點和檔案伺服器。

5. 對應您在檔案伺服器準備步驟期間建立的兩個共用資料夾到每個節點。您必須將共用資料夾對應為網路磁碟機。對應資料夾時，您可以選擇任何空的磁碟機字母。要存取共用資料夾，請使用您在情境的第 1 步中建立的使用者帳戶的憑據。

節點已準備就緒。若要部署卡巴斯基安全管理中心容錯移轉叢集，請按照情境中的進一步說明進行操作。

在卡巴斯基安全管理中心容錯移轉叢集節點上安裝卡巴斯基安全管理中心

卡巴斯基安全管理中心分別安裝在卡巴斯基安全管理中心容錯移轉叢集的兩個節點上。首先，在主動節點上安裝應用程式，然後在被動節點上安裝應用程式。安裝時，您可以選擇哪個節點是主動節點，哪個節點是被動節點。

只有來自 KLAdmins 網域群組的使用者才能在每個節點上安裝卡巴斯基安全管理中心。

要在卡巴斯基安全管理中心容錯移轉叢集的主動節點上安裝卡巴斯基安全管理中心：

1. 執行 ksc_14.2_<組建編號>_full_<語言>.exe 可執行檔。

   一個視窗將開啟，提示您選擇要安裝的 Kaspersky 應用程式。在應用程式選取視窗，按一下**安裝卡巴斯基安全管理中心管理伺服器**連結，來啟動管理伺服器安裝精靈。遵照精靈的說明。

2. 請仔細閱讀產品授權協議和隱私政策。如果您同意產品授權協議和隱私政策的所有條款，在**我確認我已完整閱讀、理解並接受**部分選取以下核取方塊：

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

   在您選取兩個核取方塊後，您裝置上的應用程式安裝將繼續。

   如果您不同意此產品授權協議或隱私政策，請按一下**取消**按鈕，取消安裝。

3. 選擇 **卡巴斯基容錯移轉叢集的主要節點** 在主動節點上安裝應用程式。

4. 在**共用資料夾**視窗，執行以下操作：

   - 在 **狀態共用** 和 **資料共用** 欄位，指定您在準備期間在檔案伺服器上建立的共用資料夾的路徑。
   - 在 **狀態共用磁碟機** 和 **資料共用磁碟機** 欄位，選擇您在節點準備期間將共用資料夾對應到的網路磁碟機。
   - 選擇叢集連線模式：透過從屬網路介面卡或協力廠商負載均衡器。

5. 執行其它自訂安裝步驟，從第 3 步開始。

   在第 13 步，如果您在準備叢集節點時已建立了一個介面卡，請指定從屬網路介面卡的 IP 位址。否則，請輸入您使用的協力廠商負載均衡器的 IP 位址。

卡巴斯基安全管理中心安裝在主動節點上。

要在卡巴斯基安全管理中心容錯移轉叢集的被動節點上安裝卡巴斯基安全管理中心：

1. 執行 ksc_14.2_<組建編號>_full_<語言>.exe 可執行檔。

   一個視窗將開啟，提示您選擇要安裝的 Kaspersky 應用程式。在應用程式選取視窗，按一下**安裝卡巴斯基安全管理中心管理伺服器**連結，來啟動管理伺服器安裝精靈。遵照精靈的說明。

2. 請仔細閱讀產品授權協議和隱私政策。如果您同意產品授權協議和隱私政策的所有條款，在**我確認我已完整閱讀、理解並接受**部分選取以下核取方塊：

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

   在您選取兩個核取方塊後，您裝置上的應用程式安裝將繼續。

   如果您不同意此產品授權協議或隱私政策，請按一下**取消**按鈕，取消安裝。

3. 選擇 **卡巴斯基容錯移轉叢集的次要節點** 在被動節點上安裝應用程式。

4. 在 **共用資料夾** 視窗的 **狀態共用** 欄位，指定共用資料夾的路徑，其中包含您在準備期間在檔案伺服器上建立的叢集狀態有關資訊。

5. 點擊**安裝**按鈕。安裝完成後，點擊 **完成** 按鈕。

卡巴斯基安全管理中心安裝在被動節點上。現在，您可以測試卡巴斯基安全管理中心容錯移轉叢集，以確保您正確配置了它並且叢集工作正常。

手動啟動和停止叢集節點

您可能需要停止整個卡巴斯基安全管理中心容錯移轉叢集或臨時分離叢集的一個節點進行維護。如果是這種情況，請按照此節中的說明進行操作。請勿嘗試透過任何其他方式啟動或停止與容錯移轉叢集相關的服務或處理程序。這可能會導致資料丟失。

啟動和停止整個容錯移轉叢集以進行維護

若要啟動或停止整個容錯移轉叢集：

1. 在啟動節點上，轉到<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。

2. 開啟命令行，然後執行以下命令之一：

   - 若要停止叢集，請執行：`klfoc -stopcluster --stp klfoc`
   - 若要啟動叢集，請執行：`klfoc -startcluster --stp klfoc`

   容錯移轉叢集的啟動或停止取決於您執行的命令。

維護節點之一

若要維護節點之一：

1. 在啟動節點上，使用`klfoc -stopcluster --stp klfoc`命令停止容錯移轉叢集。
2. 在想要維護的節點上，轉到<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。
3. 開啟命令行，然後透過執行`detach_node.cmd`命令將節點從叢集中分離。
4. 在啟動節點上，使用`klfoc -startcluster --stp klfoc`命令啟動容錯移轉叢集。
5. 執行維護活動。
6. 在啟動節點上，使用`klfoc -stopcluster --stp klfoc`命令停止容錯移轉叢集。
7. 在被維護的節點上，轉到<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center。
8. 開啟命令行，然後透過執行`attach_node.cmd`命令將節點附著到叢集。
9. 在啟動節點上，使用`klfoc -startcluster --stp klfoc`命令啟動容錯移轉叢集。

該節點得到維護並被附著到容錯移轉叢集。

在 Windows 伺服器容錯移轉叢集上安裝管理伺服器

在容錯移轉叢集上安裝管理伺服器的過程不同於在獨立裝置上進行標準安裝和自訂安裝的過程。

在包含叢集的公用資料儲存節點上執行本節中所述過程。

要在叢集上安裝卡巴斯基安全管理中心管理伺服器：

執行 ksc_<版本號>.<組建編號>_full_<中文化語言>.exe 可執行檔。

將開啟 Kaspersky 應用程式選取安裝的提示視窗。在應用程式選取視窗，按一下**安裝卡巴斯基安全管理中心管理伺服器**連結，來啟動管理伺服器安裝精靈。遵照精靈的說明。

步驟 1：檢視產品授權協議和隱私政策

在安裝精靈的此步驟，您必須閱讀您與 Kaspersky 之間的授權協議以及隱私政策。

您也可以從卡巴斯基安全管理中心分發套件中的應用程式管理外掛程式檢視授權協議和隱私政策。

請仔細閱讀產品授權協議和隱私政策。如果您同意產品授權協議和隱私政策的所有條款，請選中相應的核取方塊進行確認。

在您選取兩個核取方塊後，您裝置上的應用程式安裝將繼續。

如果您不同意此產品授權協議或隱私政策，請按一下**取消**按鈕，取消安裝。

步驟 2：選取叢集上的安裝類型

選取叢集上的安裝類型：

- **叢集（安裝在所有叢集節點上）**

  這是推薦的選項。如果選取此選項，則管理伺服器將同時安裝在叢集的所有節點上。

  > 在"選擇要安裝的管理主控台"步驟中，您需要選擇將安裝在目前叢集節點上的主控台。如果僅在叢集節點上安裝主控台，萬一節點出現故障，您將無法存取管理伺服器。建議您在此步驟中，選取基於 MMC 的主控台在所有叢集節點上進行安裝。安裝管理伺服器後，在不是叢集節點的單獨裝置上安裝卡巴斯基安全管理中心網頁主控台。這可讓您在叢集節點出現故障時使用卡巴斯基安全管理中心網頁主控台來管理管理伺服器。

- **本機（僅在此裝置上安裝）**

  如果選取此選項，則管理伺服器將僅安裝在目前節點上，就像安裝在獨立伺服器上一樣，並且管理伺服器將無法當作支援叢集的應用程式使用。例如，如果管理伺服器不需要容錯移轉功能，則可能要選取此選項以節省共用儲存空間。如果目前節點發生故障，則必須在另一個節點上安裝管理伺服器，然後從備份中還原管理伺服器的狀態。

從安裝方法選擇步驟開始，其他步驟與使用標準或自訂安裝方法時相同。

步驟 3：指定虛擬管理伺服器的名稱

指定新的虛擬管理伺服器的網路名稱。您將能夠使用該名稱將管理主控台或卡巴斯基安全管理中心 網頁主控台連線到管理伺服器。

您指定的名稱必須與叢集名稱不同。

步驟 4：指定虛擬管理伺服器的網路詳細資訊

要指定新的虛擬管理伺服器實例的網路詳細資訊，請執行以下操作：

1. 在**要使用的網路**中，選取目前叢集節點所連線的網域網路。
2. 做以下之一：
   - 如果在所選網路中使用 DHCP 分配 IP 位址，請選取"**使用 DHCP**"選項。
   - 如果在所選網路中未使用 DHCP，請指定所需的 IP 位址。

     您指定的 IP 位址必須與叢集 IP 位址不同。
3. 點擊**新增**以套用指定的設定。

您將能夠使用自動分配的 IP 位址或指定的 IP 位址將管理主控台或卡巴斯基安全管理中心網頁主控台連線到管理伺服器。

步驟 5：指定叢集群組

叢集群組是一種特殊的容錯移轉叢集角色，其中包含所有節點的公用資源。您有兩種選擇：

- 建立一個新的叢集群組。

  在大多數情況下，建議使用此選項。新的叢集群組將包含與管理伺服器實例相關的所有公共資源。

- 選取一個現有的叢集群組。

  如果要使用已經與現有叢集群組關聯的公共資源，請選取此選項。例如，如果要使用與現有叢集群組關聯的儲存，並且新叢集群組沒有其他可用儲存，則可能要使用此選項。

步驟 6：選取一個叢集資料儲存空間

選取叢集資料儲存空間：

1. 在**"可用的儲存區"中**，選取將要安裝虛擬虛擬管理伺服器實例公共資源的資料儲存空間。
2. 如果所選資料儲存空間包含多個磁區，請在**磁碟上的"可用"部分**下，選取所需的磁區。
3. 在**"安裝路徑"中**，輸入公共資料儲存空間上虛擬管理伺服器實例的資源將安裝的路徑。

已選擇資料儲存空間。

步驟 7：指定用於遠端安裝的帳戶

指定將在叢集的被動節點上進行遠端安裝虛擬管理伺服器實例的使用者名稱和密碼。

您指定的帳戶必須被授予叢集所有節點上的管理權限。

步驟 8：選取要安裝的元件

選取您要安裝的卡巴斯基安全管理中心管理伺服器的元件：

- **行動裝置管理**。如果您要在卡巴斯基安全管理中心安裝精靈執行時為行動裝置建立安裝套件，則選取此核取方塊。您也可以在管理伺服器安裝後，使用管理主控台工具手動建立行動裝置安裝套件。
- **SNMP 代理**。此元件可透過 SNMP 協定接收管理伺服器上的統計資訊。此元件僅在有安裝 SNMP 的裝置上運作。

  在卡巴斯基安全管理中心安裝後，.mib 檔案將存放於程式安裝目錄下的 SNMP 子資料夾。

網路代理和管理主控台並不會在元件清單中顯示。這些元件是必要元件，安裝程式將會自動安裝它們。

在此步驟中，您需要指定管理伺服器的安裝資料夾位置。依預設會將元件安裝在 <磁碟機>:\Program Files\Kaspersky Lab\Kaspersky Security Center。如果資料夾不存在，則會在安裝過程中自動建立。您可以使用**瀏覽**按鈕變更目的資料夾。

步驟 9：選擇網路大小

指定要安裝卡巴斯基安全管理中心的網路的大小。精靈會根據網路上的裝置數量設定應用程式介面的安裝設定和外觀以求相符。

下表列出了在不同的網路規模下應用程式安裝設定和應用程式介面外觀的不同。

依據選取的網路規模所設定的內容區別

設定	1–100 台受管理裝置	101–1000 台受管理裝置	1001 到 5000 台受管理裝置	多於 5000 台受管理裝置
顯示從屬和虛擬管理伺服器的節點，以及與從屬和虛擬管理伺服器相關的所有設定（僅在基於 MMC 的管理主控台中可用）	不適用	不適用	適用	適用
在管理伺服器和管理群組的屬性視窗中顯示**安全性**部分（僅在基於 MMC 的管理主控台中可用）	不適用	不適用	適用	適用
用戶端裝置的更新工作的隨機啟動時間	不適用	以 5 分鐘為間隔	以 10 分鐘為間隔	以 10 分鐘為間隔

如果您的管理伺服器使用 MySQL 5.7 或 SQL Express 資料庫，建議您管理的裝置在 10,000 台以下。對於 MariaDB 資料庫管理系統，建議的最大受管理裝置數量為 20000。

步驟 10：選取一個資料庫

在精靈的此步驟中，選取以下資料庫管理系統 (DBMS) 之一，將其用於儲存管理伺服器資料庫：

- **Microsoft SQL Server 或者 SQL Server Express**
- **MySQL 或者 MariaDB**
- **PostgreSQL 或者 Postgres Pro**

建議將管理伺服器安裝在專用伺服器上而不是網域控制器上。然而，若在作為唯讀網域控制器 (RODC) 的伺服器上安裝卡巴斯基安全管理中心，則不得在相同裝置上安裝 Microsoft SQL Server (SQL Express)。在此情況下，建議您遠端安裝 Microsoft SQL Server (SQL Express)（在不同裝置上），如果需要本機安裝 DBMS，則使用 MySQL、MariaDB 或 PostgreSQL。

管理伺服器資料庫結構提供在 klakdb.chm 檔案，它位於卡巴斯基安全管理中心安裝資料夾。Kaspersky 入口網站也以壓縮格式提供這個檔案：klakdb.zip。

步驟 11：設定 SQL Server

在精靈的此步驟中，請根據您選取的資料庫管理系統 (DBMS)，指定以下連線設定：

- 若您已在先前步驟選取**Microsoft SQL Server 或者 SQL Server Express**：
  - 在**SQL Server 實例名稱**欄位，指定網路中的 SQL Server 名稱。要檢視網路上的所有 SQL Server 清單，請點擊**瀏覽**按鈕。預設情況下該欄位為空。

    若您透過自訂連接埠連線 SQL Server，請連同 SQL Server 主機名稱一起指定埠號並用逗號區隔，例如：

    ```
    SQL_Server_host_name,1433
    ```

    若您要透過憑證保障管理伺服器與 SQL Server 的通訊，請在**SQL Server 實例名稱**欄位中指定與在產生憑證時使用的相同主機名稱。若您使用已命名的 SQL Server 名稱，請連同 SQL Server 主機名稱一起指定埠號並用逗號區隔，例如：

    ```
    SQL_Server_name,1433
    ```

    若您在相同主機上使用數個 SQL Server 實例，請額外以反斜線區隔來指定實例名稱，例如：

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

    如果企業網路上的 SQL Server 啟用了 Always On 功能，請在**SQL Server 實例名稱**欄位中指定可用性群組接聽程式的名稱。請注意，當 Always On 功能啟用時，管理伺服器僅支援同步提交可用性模式。
  - 在**資料庫名稱**欄位中，指定被建立用來儲存管理伺服器資料的 DBMS 的名稱。預設值是 *KAV*。

  如果此階段您要在正安裝卡巴斯基安全管理中心的裝置上安裝 SQL Server，您必須終止安裝卡巴斯基安全管理中心，並在 SQL Server 安裝完成後重新啟動卡巴斯基安全管理中心的安裝。支援的 SQL Server 版本在系統需求中列出。

  如果您要在遠端裝置上安裝 SQL Server，您無須取消卡巴斯基安全管理中心的安裝精靈。安裝 SQL Server，並恢復執行卡巴斯基安全管理中心的安裝。
- 若您已在先前步驟中選取**MySQL 或者 MariaDB**：
  - 在**SQL Server 實例名稱**欄位，指定 SQL Server 實例名稱。預設下，名稱是要安裝卡巴斯基安全管理中心的裝置的 IP 位址。
  - 在**連接埠**欄位中，指定管理伺服器連線到 DBMS 的連接埠。預設埠號為 3306。
  - 在**資料庫名稱**欄位中，指定被建立用來儲存管理伺服器資料的 DBMS 的名稱。預設值是 *KAV*。
- 若您已在先前步驟中選取 **PostgreSQL 或者 Postgres Pro**：
  - 在**PostgreSQL 或者 Postgres Pro 伺服器**欄位，指定 DBMS 實例名稱。預設下，名稱是要安裝卡巴斯基安全管理中心的裝置的 IP 位址。
  - 在**連接埠**欄位中，指定管理伺服器連線到 DBMS 的連接埠。預設埠號為 5432。

在**資料庫名稱**欄位中，指定被建立用來儲存管理伺服器資料的 DBMS 的名稱。預設值是 *KAV*。

步驟 12：選取身分驗證模式

決定管理伺服器連線到資料庫管理系統 (DBMS) 時將使用的身分驗證模式。

依據您選取的 DBMS，您可以選取以下其中之一的身分驗證模式：

- 對於 SQL Express 或 Microsoft SQL Server，請選取以下選項之一：
  - **Microsoft Windows 身分驗證模式**。使用啟動管理伺服器的帳戶來驗證權限。
  - **SQL Server 身分驗證模式**。如果您選取此選項，將會使用您指定的帳戶進行驗證。填寫**"帳戶"**、**"密碼"**欄位。

    要檢視輸入的密碼，點擊並按住**顯示**按鈕。

  對於兩個身分驗證模式，應用程式檢查資料庫是否可用。如果資料庫不可用，則顯示錯誤訊息，且您必須提供正確的憑證。

  如果您的管理伺服器資料庫是存放在別台裝置上，並且管理伺服器的帳戶無法存取該資料庫伺服器，您必須使用 SQL Server 身分驗證模式。SQL Server 身分驗證模式來進行安裝及升級您的管理伺服器。這種情況可能會發生在資料庫伺服器不在網域當中，或您指定的管理伺服器帳戶為「LocalSystem」帳戶。

若為 MySQL、MariaDB、PostgreSQL 或 Postgres Pro，請指定帳戶和密碼。

步驟 13：選取帳戶以啟動管理伺服器

選取用於啟動管理伺服器作為服務的帳戶。

- **自動產生帳戶**。應用程式會建立名為 KL-AK-* 的帳戶，kladminserver 服務會在該帳戶下執行。

  如果您排程將共用資料夾和 DBMS 放置在管理伺服器所在裝置。

- **選取帳戶**。管理伺服器服務 (kladminserver) 將在您選取的帳戶下執行。

  如果您計畫使用其他裝置上任何版本的 SQL Server 實例（包括 SQL Express）作為 DBMS，且/或您計畫在其他裝置放置共用資料夾，您必須選取網域帳戶。

  卡巴斯基安全管理中心支援受管理服務帳戶 (MSA) 和受群組管理的服務帳戶 (gMSA)。如果這些帳戶類型在您的網域中被使用，您可以選取它們之一作為管理伺服器服務帳戶。

  在指定 MSA 或 gMSA 之前，您必須將帳戶安裝在要安裝管理伺服器的同一裝置上。如果尚未安裝該帳戶，請取消管理伺服器安裝，在安裝該帳戶後，再重新啟動管理伺服器安裝。如需在本機裝置上安裝受管理服務帳戶的詳細資訊，請參閱正式的 Microsoft 文件。

  若要指定 MSA 或 gMSA：

  1. 按一下**瀏覽**按鈕。
  2. 在開啟的視窗中，按一下**物件類型**按鈕。
  3. 選取**服務帳戶**類型並點擊**確定**。
  4. 選取相關帳戶並按一下**確定**。

您選取的帳戶必須有不同的權限，取決於您排程使用的 DBMS。

出於安全原因，請不要分配權限狀態到您執行管理伺服器的帳戶。

管理伺服器帳戶以後不能變更。您需要重新安裝故障移轉叢集以使用另一個管理伺服器帳戶。

步驟 14：選取帳戶以執行卡巴斯基安全管理中心服務

在裝置上選取即將執行卡巴斯基安全管理中心服務的帳戶：

- **自動產生帳戶**。卡巴斯基安全管理中心在 kladmins 群組的裝置上建立名為 KlScSvc 的本機帳戶。卡巴斯基安全管理中心服務將在已建立的帳戶下執行。
- **選取帳戶**。卡巴斯基安全管理中心服務將執行在您選取的帳戶下。

  您將必須選取網域帳戶，如果您要儲存報告到不同裝置的資料夾，或基於您組織的安全政策。如果您安裝管理伺服器到失敗轉移叢集，您也可能必須選取網域帳戶。

出於安全原因，請不要分配權限狀態到您執行服務的帳戶。

KSN 代理服務 (ksnproxy)、Kaspersky 啟動代理服務 (klactprx) 和 Kaspersky 身分驗證入口服務 (klwebsrv) 將在所選帳戶下執行。

步驟 15：選取共用資料夾

在此步驟中，安裝精靈將請您指定共用資料夾的目錄和名稱：

- 儲存遠端安裝程式所需的檔案（這些檔案會在建立安裝套件過程中複製到管理伺服器）。
- 儲存管理伺服器從網際網路上下載的更新檔案。

檔案分享的權限會是所有的使用者（僅有讀取的權限）。

您可以選取以下選項其中之一：

- **建立共用資料夾**。建立一個新的資料夾。在文字方塊中，指定資料夾路徑。
- **選取現有共用資料夾**。選取一個已有的共用資料夾。

此共用資料夾可以是此裝置上（正在安裝卡巴斯基安全管理中心的裝置），或是企業網路環境中的任何一台裝置上的共用資料夾。您可以點擊**"瀏覽"**按鈕來選取共用資料夾或請您在下方的欄位中，手動輸入共用資料夾的 UNC 路徑（例如：\\server\Share）。

在預設的情況下，安裝精靈會替您在卡巴斯基安全管理中心的目錄下，自動建立一個共用名稱為 KLSHARE 的本機資料夾。

如果需要，您可以稍後定義共用資料夾。

步驟 16：設定與管理伺服器的連線

設定與管理伺服器的連線：

- **連接埠**

  用於連線至管理伺服器的埠號。

  預設埠號為 14000。

- **SSL 連接埠**

  用於安全地連線至管理伺服器的安全通訊端層 (SSL) 埠號。

  預設埠號為 13000。

- **加密金鑰長度**

  選取加密金鑰長度：1024 bit 或 2048 bit。

  1024-bit 加密金鑰少量佔用 CPU，但它被認為是過時的，因為由於技術說明，它無法提供可靠的加密。而且，現有硬體可能與 1024-bit 金鑰的 SSL 憑證不相容。

  2048-bit 加密金鑰滿足所有加密標準。然而，使用 2048-bit 加密金鑰可能增加 CPU 負載。

  依預設會選取 **2048 bit（最大安全）**。

您也可以稍後變更連線到管理伺服器的參數，如下所示：

- 您也可以在管理伺服器屬性的**連線連接埠**部分中變更連接埠和 SSL 連接埠號。有關管理伺服器連接埠的更多資訊，請參閱卡巴斯基安全管理中心使用的連接埠。
- 當使用 klsetsrvcert 公用程式取代管理伺服器憑證時，您可以使用 `-o RsaKeyLen:<金鑰長度>` 參數來變更加密金鑰長度。

步驟 17：定義管理伺服器位址

指定管理伺服器位址。您可以選取以下選項之一：

- **DNS 網域名稱**。如果網路包含 DNS 伺服器且用戶端裝置可以使用它來接收管理伺服器位址，則您可以使用此方法。
- **NetBIOS 名稱**。如果用戶端裝置使用 NetBIOS 協定接收管理伺服器位址，或者網路中可使用 WINS 伺服器，則您可以使用此方法。
- **IP 位址**。如果管理伺服器擁有將來不會變更的靜態 IP 位址，則您可以使用此方法。

步驟 18：指定行動裝置連線到管理伺服器的位址

如果選取了安裝“行動裝置管理”元件，則安裝精靈會出現這一步。

在**行動裝置連線的位址**視窗中，指定管理伺服器外部位址以連線本機網路之外的行動裝置。您可以指定管理伺服器的 IP 位址或網域名稱系統 (DNS)。

步驟 19：在硬碟磁碟機上解壓縮並安裝檔案

在您安裝完成卡巴斯基安全管理中心，並且都設定完畢了之後，可以在硬碟磁碟機上安裝檔案。

如果安裝需要其他程式，安裝精靈在開始安裝卡巴斯基安全管理中心之前，在“**正在安裝系統所需之相依套件**”頁面中通知您。所需程式將在您點選“**下一步**”按鈕後自動安裝。

在最後一頁，您可以選取啟動哪個主控台以使用卡巴斯基安全管理中心：

- **啟動基於 MMC 的管理主控台**
- **啟動卡巴斯基安全管理中心網頁主控台**
  此選項僅在您在先前步驟中選取了安裝卡巴斯基安全管理中心 網頁主控台時可用。

您也可以點擊**完成**以關閉精靈而不使用卡巴斯基安全管理中心。您可以稍後隨時開始使用。

在管理主控台或者卡巴斯基安全管理中心 網頁主控台第一次啟動時，您可以執行應用程式初始化設定。

在靜默模式下安裝管理伺服器

管理伺服器可以使用靜默模式進行安裝，即沒有安裝設定的互動輸入。

要在靜默模式下將管理伺服器安裝至本機裝置：

1. 閱讀最終使用者產品授權協議。只有在您理解並接受最終使用者產品授權協議的條款時，才使用以下命令。
2. 閱讀隱私政策。只有在您理解並同意您的資料將受到處理與傳輸（包含傳送至第三國家/地區）（如隱私政策所述）時，才使用以下命令。
3. 執行指令

```
setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 PRIVACYPOLICY=1 <setup_parameters>"
```

這裡「安裝參數」是一系列參數，其各自的值用空格隔開 (PARAM1=PARAM1VAL PARAM2=PARAM2VAL)。setup.exe 檔案位於伺服器資料夾，它是卡巴斯基安全管理中心分發套件的一部分。

以下清單列出了在靜默模式下安裝管理伺服器時可使用的參數名稱和可能的值。

靜默模式下安裝管理伺服器的參數

參數名稱	參數敘述	可用值
EULA	設定是否接受授權協議的條款。	• 1 – 我已完整閱讀、瞭解和接受最終使用者產品授權協議的條款。 • 其它值或未指定 – 表示我不接受產品授權協議的條款（將不會執行安裝）。
隱私政策	接受隱私政策條款。	• 1 – 我瞭解並同意將我的資料進行處理和傳輸(包括向第三國)，如所述於隱私權政策。我確認已完整閱讀並理解隱私權政策。 • 其它值或未指定 – 表示我不接受隱私政策的條款（將不會執行安裝）。
INSTALLATIONMODETYPE	管理伺服器的安裝類型。	• Standard – 標準安裝。 • Custom – 自訂安裝。
INSTALLDIR	管理伺服器的安裝資料夾路徑。	字串值。
ADDLOCAL	要安裝的管理伺服器元件清單（以逗號隔開）。	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. 管理伺服器安裝正常執行的最小元件清單： `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`。
NETRANGETYPE	網路規模（網路中裝置的數量）。	• NRT_1_100 — 1 to 100 台裝置。 • NRT_100_1000 — 101 到 1000 台裝置。 • NRT_GREATER_1000 —多於 1,000 部裝置。
SRV_ACCOUNT_TYPE	指定管理伺服器作為服務執行時帳戶使用的模式。	• SrvAccountDefault – 自動建立帳戶。 • SrvAccountUser – 手動指定帳戶。此種情況下，您必須指定 `SERVERACCOUNTNAME` 和 `SERVERACCOUNTPWD` 參數的值。
SERVERACCOUNTNAME	管理伺服器作為服務執行時使用的帳戶的名稱。如果 SRV_ACCOUNT_TYPE=SrvAccountUser，您必須為參數指定值。	字串值。
SERVERACCOUNTPWD	用於啟動管理伺服器作為服務的帳戶密碼。如果 SRV_ACCOUNT_TYPE=SrvAccountUser，您必須為參數指定值。	字串值。
SERVERCER	管理伺服器憑證金鑰長度（位元）。	• 1 – 管理伺服器憑證的金鑰長度為 2048 位元。 • 未指定值 – 管理伺服器憑證金鑰長度為 1024 位元。
DBTYPE	為儲存管理伺服器資料庫而建立的資料庫類型。 這是必要參數。	• MySQL – 將使用 MySQL 或 MariaDB 資料庫。此種情況下，您必須指定 `MYSQLSERVERNAME`、`MYSQLSERVERPORT`、`MYSQLDBNAME`、`MYSQLACCOUNTNAME` 和 `MYSQLACCOUNTPWD` 參數的值。 • MSSQL – 將使用 Microsoft SQL Server (SQL Express) 資料庫。此種情況下，您必須指定 `MSSQLSERVERNAME`、`MSSQLDBNAME` 和 `MSSQLAUTHTYPE` 參數的值。 • POSTGRES – 將使用 PostgreSQL 或 Postgres Pro 資料庫。此種情況下，您必須指定 `POSTGRESSERVERNAME`、`POSTGRESSERVERPORT`、`POSTGRESDBNAME`、`POSTGRESACCOUNTNAME` 和 `POSTGRESACCOUNTPWD` 參數的值。
MYSQLSERVERNAME	SQL Server 完整名稱。如果 DBTYPE=MySQL，您必須為參數指定值。	字串值。
MYSQLSERVERPORT	連線至 SQL Server 的埠號。如果 DBTYPE=MySQL，您必須為參數指定值。	數值。

參數名稱	參數敘述	可用值
MYSQLDBNAME	為儲存管理伺服器資料庫而建立的資料庫名稱。如果 DBTYPE=MySQL，您必須為參數指定值。	字串值。
MYSQLACCOUNTNAME	連線到資料庫的帳戶名稱。如果 DBTYPE=MySQL，您必須為參數指定值。	字串值。
MYSQLACCOUNTPWD	連線到資料庫的帳戶密碼。如果 DBTYPE=MySQL，您必須為參數指定值。	字串值。
MSSQLSERVERNAME	SQL Server 完整名稱。如果 DBTYPE=MSSQL，您必須為參數指定值。	字串值。
MSSQLDBNAME	資料庫名稱。如果 DBTYPE=MSSQL，您必須為參數指定值。	字串值。
MSSQLAUTHTYPE	連線到 SQL Server 的授權類型。如果 DBTYPE=MSSQL，您必須為參數指定值。	• Windows – Microsoft Windows 身分驗證模式。 • SQLServer – SQL Server 身分驗證模式。此種情況下，您必須指定 `MSSQLACCOUNTNAME` 和 `MSSQLACCOUNTPWD` 參數的值。
MSSQLACCOUNTNAME	連線至 SQL Server 的帳戶名稱。如果 MSSQLAUTHTYPE=SQLServer，您必須為參數指定值。	字串值。
MSSQLACCOUNTPWD	連線至 SQL Server 的帳戶密碼。如果 MSSQLAUTHTYPE=SQLServer，您必須為參數指定值。	字串值。
CREATE_SHARE_TYPE	指定共用資料夾的方法。	• Create – 建立新共用資料夾。此種情況下，您必須指定 `SHARELOCALPATH` 和 `SHAREFOLDERNAME` 參數的值。 • ChooseExisting – 選取現有資料夾。此種情況下，您必須指定 `EXISTSHAREFOLDERNAME` 參數的值。
SHARELOCALPATH	本機資料夾完整路徑。您必須指定參數值，如果 CREATE_SHARE_TYPE=Create	字串值。
SHAREFOLDERNAME	共用資料夾網路名稱。如果 CREATE_SHARE_TYPE=Create，您必須為參數指定值。	字串值。
EXISTSHAREFOLDERNAME	現有共用資料夾的完整路徑。 如果 CREATE_SHARE_TYPE=ChooseExisting，您必須為參數指定值。	字串值。
SERVERPORT	連線至管理伺服器的埠號。	數值。
SERVERSSLPORT	使用 SSL 協定加密連線到管理伺服器的埠號。	數值。
SERVERADDRESS	管理伺服器位址。	字串值。
MOBILESERVERADDRESS	指定行動裝置連線到管理伺服器的位址。	字串值。

有關管理伺服器安裝設定的詳細敘述，請參閱「自訂安裝」部分。

在管理員的電腦上安裝管理主控台

您可以在管理員的電腦上，安裝管理主控台。如此可以透過網路來連線到管理伺服器進行管理。

在管理員的電腦上安裝管理主控台：

1. 執行 setup.exe 可執行檔。

   將開啟 Kaspersky 應用程式選取安裝的提示視窗。

2. 在應用程式選取視窗，按一下**僅安裝卡巴斯基安全管理中心管理主控台**連結，來執行管理主控台安裝精靈。遵照精靈的說明。

3. 安裝精靈會請您選取安裝的資料夾位置。在預設的情況下，目的資料夾將為<系統磁區>:\Program Files\Kaspersky Lab\Kaspersky Security Center Console。如果這個資料夾不存在，安裝精靈將會自動的產生此資料夾。您可以使用**瀏覽**按鈕變更目的資料夾。

4. 在安裝精靈的最後一頁，按一下**開始**按鈕來啟動管理主控台的安裝。

當精靈完成後，管理主控台將會安裝在管理員工作站上。

在處於靜默模式中管理員的電腦上安裝管理主控台：

1. 閱讀最終使用者產品授權協議。只有在您理解並接受最終使用者產品授權協議的條款時，才使用以下命令。

2. 在卡巴斯基安全管理中心發佈套件的 `Distrib\Console` 資料夾中，使用以下命令執行 setup.exe 檔案：

   ```
   setup.exe /s /v"EULA=1"
   ```

   如果要與管理主控台一起從 `Distrib\Console\Plugins` 資料夾安裝所有管理外掛程式，請執行以下命令：

   ```
   setup.exe /s /v"EULA=1" /pALL
   ```

   如果要指定要從 `Distrib\Console\Plugins` 資料夾與管理主控台一起安裝的管理外掛程式，請在「/p」金鑰後指定外掛程式，並用分號分隔：

   ```
   setup.exe /s /v"EULA=1" /pP1;P2;P3
   ```

   其中 `P1`、`P2`、`P3` 是與 `Distrib\Console\Plugins` 資料夾中的外掛程式資料夾名稱相對應的外掛程式名稱。例如：

   ```
   setup.exe /s /v"EULA=1" /pKES4Mac;KESS;MDM4IOS
   ```

管理主控台和管理外掛程式（如果有）將安裝在管理員的工作站上。

在您安裝完管理主控台之後，您必須將主控台連線到管理伺服器上。為此，請執行管理主控台，然後在開啟的視窗中，指定裝有管理伺服器的裝置名稱或 IP 位址，以及輸入連線的帳戶密碼。在連線成功之後，您就可以在您的電腦上，連線到管理伺服器進行防毒軟體的管理。

您可以使用標準的 Microsoft Windows 新增/移除工具移除管理主控台。

卡巴斯基安全管理中心安裝後系統的變化

管理主控台圖示

在裝置上安裝管理主控台後，系統會顯示其圖示，允許您啟動管理主控台。您可以在**開始 → 程式 → 卡巴斯基安全管理中心**功能表中找到管理主控台。

管理伺服器和網路代理服務

管理伺服器和網路代理將會以服務的型態安裝在您的裝置，您可以參考下列清單的說明。此表還包含了在其他服務的內容。

卡巴斯基安全管理中心服務內容

元件	服務名稱	顯示的服務名稱	帳戶
管理伺服器	kladminserver	卡巴斯基安全管理中心管理伺服器	安裝過程中，使用者定義的或專用的 KL-AK-* 格式的帳戶被建立
網路代理	klnagent	卡巴斯基安全管理中心網路代理	本機系統
存取卡巴斯基安全管理中心網頁主控台和管理群組織內網的網頁伺服器	klwebsrv	Kaspersky 網路論壇	專用非授權 KlScSvc 帳戶
啟動代理伺服器	klactprx	Kaspersky 的啟動代理伺服器	專用非授權 KlScSvc 帳戶
KSN 代理伺服器	ksnproxy	卡巴斯基安全網路代理伺服器	專用非授權 KlScSvc 帳戶

如果您在 Kaspersky Security Center 容錯移轉叢集節點上安裝 Kaspersky Security Center，klfocsvc_klfoc 服務將變得可用。klnagent_klfoc 和 klfocsvc_klfoc 服務在本機系統帳戶下執行。kladminserver_klfoc 服務必須在「ksc」帳戶下執行，其他服務在「rightless」帳戶下執行。必須將「ksc」和「rightless」帳戶新增至具有本機管理員權限的 KLAdmins 群組。為了卡巴斯基安全管理中心正常運作，您必須僅使用「ksc」和「rightless」帳戶來執行服務。我們不建議使用具有相同權限的其他帳戶。下表包含在 Kaspersky Security Center 容錯移轉叢集上安裝管理伺服器後，裝置上會套用的服務內容。

安裝在 Kaspersky Security 中的 Kaspersky Security Center 服務的內容

元件	服務名稱	顯示的服務名稱	帳戶
管理伺服器	kladminserver_klfoc	卡巴斯基安全管理中心管理伺服器	ksc
網路代理	klnagent_klfoc	卡巴斯基安全管理中心網路代理	本機系統
存取卡巴斯基安全管理中心網頁主控台和管理群組織內網的網頁伺服器	klwebsrv_klfoc	Kaspersky 網路論壇	rightless
啟動代理伺服器	klactprx_klfoc	Kaspersky 啟動代理伺服器	rightless
KSN 代理伺服器	ksnproxy_klfoc	卡巴斯基安全網路代理伺服器	rightless
Kaspersky Security Center 容錯移轉叢集	klfocsvc_klfoc	Kaspersky Security Center 容錯移轉叢集	本機系統

卡巴斯基安全管理中心網頁主控台服務

如果您在裝置上安裝卡巴斯基安全管理中心網頁主控台，則會部署以下服務（請參閱下表）：

卡巴斯基安全管理中心網頁主控台服務

顯示的服務名稱	帳戶
卡巴斯基安全管理中心服務網頁主控台	NT Service/KSCSvcWebConsole
卡巴斯基安全管理中心網頁主控台	網路服務
卡巴斯基安全管理中心產品外掛程式伺服器	NT Service/KSCWebConsolePlugin

卡巴斯基安全管理中心網頁主控台管理服務	本機系統
卡巴斯基安全管理中心網頁主控台訊息佇列	NT Service/KSCWebConsoleMessageQueue

網路代理伺服器版本

管理伺服器版本的網路代理將會連同管理伺服器一起安裝在裝置上。管理伺服器版本的網路代理是管理伺服器的一部分元件，他只能與管理伺服器一同安裝或移除，而且他只與安裝管理伺服器的電腦有作用。設定網路代理到管理伺服器的連線不是必須的步驟：設定會透過程式功能進行實施，因為這些元件已安裝在同一裝置中。管理伺服器版本的網路代理安裝的內容和功能與一般版本的網路代理相同，並且具有相同的功能。此版本由管理群組（該管理群組要包含管理伺服器的用戶端裝置）的政策管理。對於伺服器版本的網路代理，除了「變更卡巴斯基管理伺服器」的工作不適用於此版本外，其餘所有的工作都是用於管理伺服器版本的網路代理。

網路代理無法被安裝到已經安裝了管理伺服器的裝置。

您可以檢視管理伺服器、網路代理的各項服務的內容，也可以使用標準的 Microsoft Windows 管理工具監控其操作：Computer management\Services。有關 Kaspersky 管理伺服器服務活動的資訊已註冊，並儲存在 Microsoft Windows 系統記錄中，而且是在安裝管理伺服器的裝置上的一個單獨的卡巴斯基事件記錄分支中。

我們建議您不要手動開始和停止服務，且不要在服務設定中修改服務帳戶。如果必要，您可以使用 klsrvswch 公用程式修改管理伺服器服務帳戶。請注意，您必須使用用於安裝管理伺服器的具有管理員權限的帳戶在管理伺服器裝置上啟動 klsrvswch 公用程式。

使用者帳戶和安全群組

管理伺服器安裝程式預設建立以下帳戶：

- KL-AK-*：管理伺服器服務帳戶
- KlScSvc：管理伺服器輪詢的其他服務帳戶
- KlPxeUser：作業系統佈署帳戶

如果您在執行安裝程式時為管理伺服器服務和其他服務選取其他帳戶，指定的帳戶被使用。

在安裝管理伺服器完成之後，系統會自動建立 KLAdmins 和 KLOperators 這兩個本機安全群組，並隨附他們各自的權限集。

建議不要在網域控制器上安裝管理伺服器；但若您在網域控制器上安裝管理伺服器，則必須使用網域管理員權限啟動安裝程式。在此情況下，安裝程式會自動建立稱為 KLAdmins 和 KLOperators 的網域安全性群組。若您在不是網域控制器的裝置上安裝管理伺服器，必須改用本機管理員權限啟動安裝程式。在此情況下，安裝程式會自動建立稱為 KLAdmins 和 KLOperators 的本機安全性群組。

配置郵件通知時，您需要在郵件伺服器上建立一個用於 ESMTP 驗證的帳戶。

移除程式

您可以使用標準的 Microsoft Windows 新增/移除工具移除卡巴斯基安全管理中心。移除精靈將移除此台裝置上的所有的程式元件（包含外掛程式）。該精靈使您的預設瀏覽器開啟帶有投票的網頁，您可以在其中告訴我們您選擇停止使用卡巴斯基安全管理中心的原因。如果您在移除精靈的過程中選取刪除共用資料夾 (KLSHARE)，則可以在所有相關工作完成後手動將其刪除。

移除應用程式後，它的一些檔案可能保持在系統暫時資料夾。

應用程式移除工作建立精靈會建議您儲存管理伺服器的備份副本。

當應用程式從 Microsoft Windows 7 和 Microsoft Windows 2008 移除時，系統可能會提前終止應用程式移除工作建立精靈。您可以透過關閉系統中的使用者帳戶控制 (UAC) 並重新啟動應用程式移除來避免。

關於升級卡巴斯基安全管理中心

本節包含如何從先前版本升級卡巴斯基安全管理中心的資訊。您可以不同方式升級卡巴斯基安全管理中心，具體取決於卡巴斯基安全管理中心安裝在本機還是卡巴斯基安全管理中心容錯移轉叢集節點上。

升級期間，DBMS 被管理伺服器和其他應用程式同時使用是被嚴格禁止的。

從先前版本升級卡巴斯基安全管理中心時，所有已安裝的受支援卡巴斯基應用程式的外掛程式都會得到保留。會自動升級管理伺服器外掛程式和網路代理外掛程式（適用於管理主控台和卡巴斯基安全管理中心 網頁主控台）。

情景：升級卡巴斯基安全管理中心和受管理安全應用程式

該部分敘述卡巴斯基安全管理中心和受管理安全應用程式升級的主要方案。

卡巴斯基安全管理中心和受管理安全應用程式升級分步驟進行：

1. **檢查硬體和軟體要求**

   確保您的硬體滿足要求並安裝所需的更新。

2. **排程資源**

   評估您的資料庫會佔用多少磁碟空間。確保您有足夠磁碟空間儲存管理伺服器設定和資料庫的備份副本。

3. **獲取卡巴斯基安全管理中心的安裝檔案**

   獲取目前版本卡巴斯基安全管理中心的可執行檔並儲存它到作為管理伺服器的裝置。閱讀您要使用的卡巴斯基安全管理中心版本的發佈說明。

4. **建立先前版本的備份副本**

   使用資料備份和還原實用工具建立管理伺服器資料的備份副本。您還可以建立備份工作。

建議匯出已安裝外掛程式的清單。

5. **執行安裝程式**

   執行卡巴斯基安全管理中心最新版本的可執行檔。當執行檔案時，指定您有備份副本並指定其位置。您的資料將從備份被還原。

6. **升級受管理應用程式**

   如果有新版本可用，您可以升級應用程式。閱讀支援的 Kaspersky 應用程式清單並確保您的卡巴斯基安全管理中心版本與該應用程式相容。然後按照發佈說明的敘述執行應用程式升級。

結果

升級方案完成後，確保管理伺服器新版本已成功安裝到 Microsoft Management Console。點擊**說明 → 關於卡巴斯基安全管理中心**。版本被顯示。

要確保您正在卡巴斯基安全管理中心 網頁主控台中使用管理伺服器的新版本，在螢幕上方點擊管理伺服器名稱旁邊的設定圖示（ ）。在開啟的管理伺服器內容視窗中的**一般**頁籤，選取**一般**區段。版本被顯示。

如果您需要還原管理伺服器資料，請按照以下主題中描述的步驟操作：互動模式下的資料備份和還原。

如果您升級受管理安全應用程式，確保它被正確安裝在受管理裝置。對於更多資訊，請參考該應用程式的文件。

從先前版本升級卡巴斯基安全管理中心

以下主題描述了建議的升級準備步驟：升級卡巴斯基安全管理中心和受管理安全應用程式。

您可以安裝版本 14.2 的管理伺服器到安裝了早期版本管理伺服器的裝置（從版本 11 (11.0.0.1131b) 開始）。當升級至版本 14.2 時，上一管理伺服器版本的所有資料和設定都將被保留下來。

如果在管理伺服器安裝過程中發生問題，您可以重新安裝先前的管理伺服器版本，並利用升級前所建立的備份資料還原回去。

如果網路中至少已成功安裝一台新版管理伺服器，則您可以用使用管理伺服器安裝套件的遠端安裝工作升級網路上的其他管理伺服器。

如果您部署了卡巴斯基安全管理中心容錯移轉叢集，您也可以在它的節點上升級卡巴斯基安全管理中心。

要升級早期版本的管理伺服器到版本 14.2：

1. 對版本 14.2 執行 ksc_14.2_<組建編號>_full_<語言>.exe 安裝檔案（您可從卡巴斯基網站下載此檔案）。
2. 在開啟的視窗中，點擊**安裝卡巴斯基安全管理中心 14.2**連結啟動管理伺服器安裝精靈。遵照精靈的說明。

3. 讀取產品授權協議和隱私政策。如果您同意產品授權協議和隱私政策的所有條款，在**我確認我已完整閱讀、理解並接受**部分選取以下核取方塊：

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

   在您選取兩個核取方塊後，您裝置上的應用程式安裝將繼續。安裝精靈提示您建立早期版本管理伺服器資料的備份。

   卡巴斯基安全管理中心支援從用舊版本的管理伺服器建立的備份還原資料。

4. 如果要建立管理伺服器資料的備份，請在開啟的**管理伺服器備份**視窗中指定此點。

   備份由 klbackup 公用程式建立。此公用程式包含在分發套件中，位於卡巴斯基安全管理中心安裝資料夾的 Root 目錄下。

5. 按照安裝精靈安裝管理伺服器版本 14.2。

   若訊息表示卡巴斯基安全管理中心網頁主控台伺服器忙碌中，請在精靈視窗中點擊**略過**。

   我們建議您避免終止安裝精靈。在管理伺服器安裝階段取消升級會導致卡巴斯基安全管理中心的升級版本失敗。

6. 對於安裝了更早版本網路代理的裝置，為新版本的網路代理建立和執行遠端安裝工作。

   我們建議您將 Linux 網路代理升級到與卡巴斯基安全管理中心相同的版本。

   在完成遠端佈署工作之後，網路代理的版本將會更新。

   在基於 Linux 的資產上執行以下命令以刪除不再需要的依賴項：

   - 對於基於 Debian 的資產，執行以下命令之一：
     - `apt-get -y autoremove`
     - `apt -y autoremove`
   - 對於基於 RPM 的資產，執行以下命令之一：
     - `dnf autoremove`
     - `yum autoremove`

在卡巴斯基安全管理中心容錯移轉叢集節點上升級卡巴斯基安全管理中心

您可以在已安裝舊版（從版本 13.2 開始）管理伺服器的每個卡巴斯基安全管理中心容錯移轉叢集節點上安裝管理伺服器版本 14.2。當升級至版本 14.2 時，上一管理伺服器版本的所有資料和設定都將被保留下來。

如果之前在裝置上本機安裝了卡巴斯基安全管理中心，您也可以在這些裝置上升級卡巴斯基安全管理中心。

若要在卡巴斯基安全管理中心容錯移轉叢集節點上升級卡巴斯基安全管理中心：

1. 在叢集的活躍節點上執行以下操作：

   a. 執行 ksc_14.2_<組建編號>_full_<語言>.exe 可執行檔。

   一個視窗將開啟，提示您選取要升級的卡巴斯基應用程式。按一下安**安裝卡巴斯基安全管理中心管理伺服器**連結來啟動管理伺服器安裝精靈。請按照精靈的步驟進行操作。

   b. 讀取產品授權協議和隱私政策。如果您同意產品授權協議和隱私政策的所有條款，在**我確認我已完整閱讀、理解並接受**部分選取以下核取方塊：

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

   勾選兩個核取方塊以繼續安裝。

   如果不接受產品授權協議或隱私政策，請按一下**取消**按鈕取消升級。

2. 在卡巴斯基安全管理中心容錯移轉叢集的被動節點上，執行與在主動節點上相同的操作。

3. 啟動叢集。

從結果來看，您已在卡巴斯基安全管理中心容錯移轉叢集節點上安裝了最新版本的管理伺服器。

卡巴斯基安全管理中心的初始化配置

該部分敘述了安裝卡巴斯基安全管理中心後，要執行初始設定必須採取的操作。

硬化指南

硬化指南專為安裝管理卡巴斯基安全管理中心的專業人員，以及為使用卡巴斯基安全管理中心的企業提供技術支援的人員而設計。

硬化指南描述了配置卡巴斯基安全管理中心及其元件的建議和功能，旨在降低其危害的風險。

在設定之前，請使用管理伺服器資料備份工作或 klbackup 公用程式建立卡巴斯基安全管理中心管理伺服器備份副本並將其儲存在安全位置。

硬化指南包括以下資訊：

- 選擇管理伺服器架構
- 設定與管理伺服器的安全連線
- 設定帳戶來存取管理伺服器
- 管理管理伺服器和用戶端裝置的防護
- 配置受管理應用程式的防護
- 管理伺服器維護
- 將資訊傳輸到協力廠商應用程式

在您開始使用管理伺服器之前，卡巴斯基安全管理中心會提示您閱讀硬化指南的簡要版本。

請注意，您確認已閱讀硬化指南後才能使用管理伺服器。

要閱讀硬化指南：

1. 開啟管理主控台或卡巴斯基安全管理中心網頁主控台，然後登入主控台。主控台會檢查您是否確認閱讀了目前版本的硬化指南。

   如果您尚未閱讀硬化指南，則一個視窗會開啟並顯示它的簡要版本。

2. 執行以下操作之一：

   - 如果想要以文字文件形式檢視強化指南的簡要版本，請點擊**在新視窗中開啟**連結。
   - 如果想要檢視完整版本的強化指南，請點擊**在線上幫助中開啟強化指南**連結。

3. 閱讀強化指南後，選取**我確認我已完全閱讀並理解強化指南**核取方塊，然後點擊**同意**按鈕。

   現在，您可以使用管理伺服器。

當新版本的硬化指南出現時，卡巴斯基安全中心將提示您閱讀它。

管理伺服器快速啟動精靈

本節提供了管理伺服器快速啟動精靈的資訊。

關於快速啟動精靈

本節提供了管理伺服器快速啟動精靈的資訊。

管理伺服器快速啟動精靈可讓您建立最少的必要工作與政策、調整最少設定、下載與安裝適用於 Kaspersky 應用程式的外掛程式，以及建立受管理 Kaspersky 應用程式的安裝套件。當精靈執行時，您可以對應用程式做以下變更：

- 下載並安裝適用於受管理應用程式的外掛程式。快速設定精靈完成作業後，安裝的管理外掛程式清單會顯示在管理伺服器內容視窗中的**進階 → 有關已安裝應用程式管理外掛程式的詳情**區域。
- 建立受管理 Kaspersky 應用程式的安裝套件。快速啟動精靈完成作業後，適用於 Windows 和受管理 Kaspersky 應用程式網路代理的安裝套件會顯示在**管理伺服器 → 進階 → 遠端安裝 → 安裝套件**清單。
- 新增可自動佈署至管理群組內的裝置的金鑰檔案或啟動碼。快速設定精靈完成作業後，產品授權金鑰資訊會顯示在管理伺服器內容視窗中的**Administration Server → Kaspersky Licenses** list and in the **產品授權金鑰**區段。
- 設定與卡巴斯基安全網路 (KSN) 的互動。
- 為管理伺服器和受管理應用程式的操作事件通知設定郵件傳送設定（成功的通知傳送需要訊息服務在管理伺服器和所有接收端裝置上執行）。快速設定精靈完成作業後，電子郵件通知設定會顯示在管理伺服器內容視窗中的**通知**區域。
- 調整裝置上安裝的應用程式的更新設定和修復弱點設定。
- 為工作站和伺服器建立防護政策，以及為受管理裝置階層的最上層群組建立惡意軟體掃描工作、更新下載工作和資料備份工作。快速啟動精靈完成作業後，建立的工作會顯示在**管理伺服器 → 工作**清單中，對應受管理應用程式外掛程式的政策會顯示在**管理伺服器 → 政策**清單中。

快速啟動精靈會為受管理應用程式建立政策，例如 Kaspersky Endpoint Security for Windows，除非已為**受管理裝置**群組建立此類政策。若**受管理裝置**群組中不存在相同名稱的工作，則快速啟動精靈會建立工作。

在管理主控台中，卡巴斯基安全管理中心會在您初次啟動後自動提示您執行快速啟動精靈。您還可以在任意時刻手動啟動快速啟動精靈。

開始管理伺服器快速設定精靈

在安裝管理伺服器後，在第一次連線時，應用程式自動提示您執行快速啟動精靈。您還可以在任意時刻手動啟動快速啟動精靈。

要手動啟動快速啟動精靈：

1. 在主控台樹狀目錄中，選取**管理伺服器**節點。
2. 在節點的上下文功能表中，選取**所有工作 → 管理伺服器快速啟動精靈**。

   精靈提示您執行管理伺服器初始化設定。遵照精靈的說明。

若您再次啟動快速設定精靈，則先前執行精靈時所建立的工作和政策無法重新建立。

步驟 1：設定代理伺服器

指定管理伺服器的網際網路存取設定。您必須設定網際網路存取權限，才能使用卡巴斯基安全網路並下載卡巴斯基安全管理中心病毒資料庫和受管理卡巴斯基應用程式的更新。

如果您要在連線到網際網路時使用代理伺服器，選取**使用代理伺服器**選項。如果選取此選項，可將欄位用於輸入設定。為代理伺服器連線指定以下設定：

- **位址**

  卡巴斯基安全管理中心用於連線到網際網路的代理伺服器位址。

- **連接埠號**

  將建立卡巴斯基安全管理中心代理伺服器連線的埠號。

- **略過本機位址的代理伺服器**

  將不會使用代理伺服器連線本機網路的裝置。

- **代理伺服器身分驗證**

  如果選取該方塊，您可以在輸入欄位中為代理伺服器身分驗證指定憑證。

  如果選取**使用代理伺服器**核取方塊，則可使用該輸入欄位。

- **使用者名稱**

  用來建立前往 Proxy 伺服器之連線的使用者帳戶（若選取了**代理伺服器身分驗證**核取方塊，則此欄位可用）。

- **密碼**

  其帳戶用來建立 Proxy 伺服器連線的使用者所設定的密碼（若選取了**代理伺服器身分驗證**核取方塊，則此欄位可用）。

  若要檢視輸入的密碼，依您所需的時間長度點擊並按住**顯示**按鈕。

您可以稍後設定網際網路存取，單獨從速啟動精靈執行。

步驟 2：選取應用程式啟動方式

選取以下其中一個卡巴斯基安全管理中心啟動選項：

- **透過插入您的啟動碼**

  *啟動碼*是一串由 20 個字元數字組成的唯一序列。您可以輸入啟動碼來新增一個金鑰來啟動卡巴斯基安全管理中心。您會透過您在購買卡巴斯基安全管理中心後指定的電子郵件地址收到啟動碼。

  若要使用啟動碼啟動應用程式，您需要網際網路來建立與 Kaspersky 啟動伺服器的連線。

  若您已選取此啟動選項，就能啟用**自動分發產品授權金鑰到受管理裝置**選項。

  若啟用此選項，授權金鑰將會自動佈署至受管理裝置。

  若停用此選項，您可以稍後在管理主控台樹狀目錄的 **Kaspersky** 產品授權節點中，將產品授權金鑰佈署至受管理裝置。

  如果因為某些原因透過插入啟動碼進行啟動失敗，您可以透過指定金鑰檔案來啟動應用程式。

- **透過指定金鑰檔案**

  *金鑰檔案*是 Kaspersky 提供的 .key 副檔名的檔案。金鑰檔案被用來啟動應用程式。

  金鑰檔案的取得方法請參閱關於金鑰檔案章節。

  若使用金鑰檔案啟動程式，您無需連線至 Kaspersky 啟動伺服器。

  若您已選取此啟動選項，就能啟用**自動分發產品授權金鑰到受管理裝置**選項。

  若啟用此選項，授權金鑰將會自動佈署至受管理裝置。

  若停用此選項，您可以稍後在管理主控台樹狀目錄的 **Kaspersky** 產品授權節點中，將產品授權金鑰佈署至受管理裝置。

- **透過高推遲應用程式啟動**

  應用程式將使用基本功能操作，沒有行動裝置管理也沒有弱點和修補程式管理。

如果您選取延遲啟動應用程式，您可以稍後在任意時刻新增產品授權金鑰。

步驟 3：選取防護範圍和作業系統

選取您網路中使用的防護區域和作業系統。當您選取這些選項，您就在 Kaspersky 伺服器上指定了應用程式管理外掛程式的篩選和分發套件，您可下載此程式以在網路中的用戶端裝置上安裝。選取選項：

- **地區**

  您可選取以下防護範圍：

  - **工作站**。若您要在網路中防護工作站，請選取此選項。依預設會選定此選項。
  - **檔案伺服器和儲存**。若要防護網路中的檔案伺服器，請選取此選項。
  - **行動裝置**。若要防護公司或公司員工擁有的行動裝置，請選取此選項。若您選取此選項，但您未透過行動裝置管理功能提供授權，則會出現一則訊息，告知您透過行動裝置管理功能提供授權的必要性。若您沒有提供授權，則您無法使用行動裝置功能。
  - **虛擬化**。若您要防護網路中的虛擬機，請選取此選項。
  - **Kaspersky 垃圾郵件防護**。若要防護組織中的郵件伺服器不要受到垃圾郵件、詐騙和惡意郵件攻擊，請選取此選項。

- **作業系統**

  您可以選取以下平台：

  - Microsoft Windows
  - Linux
  - macOS
  - Android
  - 其他

  有關受支援的作業系統的資訊，請參閱硬體和軟體需求。

您可以稍後從可用套件清單中選擇卡巴斯基應用程式套件，單獨從快速啟動精靈執行。為了簡化搜尋所需套件的作業，您可以使用以下條件篩選可用套件清單：

- 保護區域
- 所下載軟體的類型（分發套件、公用程式、外掛程式或 Web 外掛程式）
- 卡巴斯基應用程式的版本
- 卡巴斯基應用程式的本地化語言

步驟 4：為受管理應用程式選取外掛程式

選取要安裝且適用於受管理應用程式的外掛程式。系統會顯示 Kaspersky 伺服器上的外掛程式清單。會根據在精靈的上一步選取的選項篩選清單。依預設，完整清單包含所有語言的外掛程式。若要僅顯示特定語言的外掛程式，請從**顯示管理主控台中文化語言或**下拉清單選取語言。外掛程式清單包含以下欄：

- **應用程式名稱**

  您在先前步驟中已選取的外掛程式會依存在保護範圍和平台中，系統會選取這些程式。

- **應用程式版本**

  清單包含放在 Kaspersky 伺服器中所有版本的外掛程式。依預設會選取最新版本的外掛程式。

- **本地化語言**

  依預設，外掛程式的本地化語言會由您在安裝時選取的卡巴斯基安全管理中心語言來決定。您可在**顯示管理主控台中文化語言或**下拉清單指定其他語言。

選取外掛程式後，其安裝程式會自動在獨立視窗中啟動。若要安裝一些外掛程式，您必須接受 EULA 條款。閱讀 EULA 條款，選取**我接受產品授權協議的條款**選項並點擊**安裝**按鈕。若您不接受 EULA 條款，則不會安裝外掛程式。

安裝完成後，請關閉安裝視窗。

您也可以稍後選擇管理外掛程式，不需透過快速啟動精靈。

步驟 5：下載分發套件並建立安裝套件

Kaspersky Endpoint Security for Windows 包含適用於儲存在用戶端裝置上資訊的加密工具。若要下載符合您組織需要的 Kaspersky Endpoint Security for Windows 分發套件，請諮詢組織用戶端裝置所在的國家或地區的法務部門。

在**加密類型**視窗，選取以下加密類型之一：

- 強加密 (AES256)。此加密類型會使用 256 位元的金鑰長度。
- 簡單加密 (AES56)。此加密類型會使用 56 位元的金鑰長度。

只有在您選取了 **工作站**作為防護範圍並選取了**Microsoft Windows**作為平台時，才會顯示**加密類型**視窗。

選取加密類型後，會顯示兩種類型的分發套件清單。清單中會選取有所選加密類型的分發套件。分發套件語言會對應卡巴斯基安全管理中心語言。若適用於卡巴斯基安全管理中心的 Kaspersky Endpoint Security for Windows 分發套件不存在該語言，則會選取英文版分發套件。

在清單中，您可透過**顯示管理主控台中文化語言或**下拉式清單選取分發套件語言。

受管理應用程式的發佈，可能需要安裝卡巴斯基安全管理中心特定的最低版本。

在清單中，您可選取任何加密類型的分發套件，與您在**加密類型**視窗中選取的不同。為 Kaspersky Endpoint Security for Windows 選取分發套件後，請對應元件和平台下載分發套件，之後啟動。您可在**下載狀態**欄中監控下載進度。快速啟動精靈完成作業後，適用於 Windows 和受管理 Kaspersky 應用程式網路代理的安裝套件會顯示在**管理伺服器 → 進階 → 遠端安裝 → 安裝套件**清單。

若要完成下載某些分發套件，您必須接受 EULA。當您點擊**同意**按鈕時，顯示 EULA 條款。若要繼續至精靈的下個步驟，您必須接受 EULA 的條款與條件，以及 Kaspersky 隱私政策的條款與條件。選取 EULA 和 Kaspersky 隱私政策旁的選項，並點擊**全部同意**按鈕。若您不接受條款與條件，系統會取消套件的下載程序。

接受 EULA 與 Kaspersky Privacy 隱私政策的條款與條件後，會繼續分發套件下載程序。下載完成時，會顯示**已建立安裝套件**狀態。之後您可以使用安裝套件在用戶端裝置上佈署 Kaspersky 應用程式。

您可以手動建立安裝套件，單獨從快速啟動精靈執行。轉到管理主控台樹狀目錄中的**管理伺服器→進階→遠端安裝→ 安裝套件**。

步驟 6：設定卡巴斯基安全網路使用

您可以取得卡巴斯基安全網路的信譽資料庫存取權限，確保在遇到未知威脅時 Kaspersky 應用程式能夠做出更快速的回應，提高某些防護元件的效能並降低誤報的風險。

請閱讀顯示在視窗中的 KSN 聲明。指定設定以轉發卡巴斯基安全管理中心操作資訊到卡巴斯基安全網路知識庫。您可以選取以下其中一個方法：

- **我同意使用卡巴斯基安全網路**

  安裝在用戶端裝置上的卡巴斯基安全管理中心與受管理應用程式會自動傳輸其作業詳情至卡巴斯基安全網路。參與卡巴斯基安全網路確保了包含病毒和其他威脅的資料庫的快速更新，該資料庫確保了對緊急安全威脅的快速回應。

- **我不同意使用卡巴斯基安全網路**

  卡巴斯基安全管理中心和受管理應用程式將不會提供資訊至卡巴斯基安全網路。

  若您選取此選項，則會停用卡巴斯基安全網路。

若您已下載 Kaspersky Endpoint Security for Windows 外掛程式，則會顯示 KSN 聲明，包括適用卡巴斯基安全管理中心的 KSN 聲明和適用 Kaspersky Endpoint Security for Windows 的 KSN 聲明。適用其他受管理 Kaspersky 應用程式（並且已下載其外掛程式）的 KSN 聲明會顯示在獨立的視窗中，您必須分別接受（或不接受）每個聲明。

您也可以稍後在管理主控台的管理伺服器內容視窗中，設定管理伺服器到卡巴斯基安全網路 (KSN) 的存取。

步驟 7：設定電子郵件通知

設定 Kaspersky 應用程式在受管理裝置上操作時傳送已註冊事件的相關通知。這些設定將作為管理伺服器的預設設定使用。

要配置發生在 Kaspersky 應用程式上的事件的通知傳送，使用以下設定：

- **收件者（電子郵件信箱）**

  應用程式將給其傳送通知的使用者的郵件位址。您可以輸入一個或更多位址；如果您輸入多個位址，使用分號分隔。

- **SMTP 伺服器**

  您組織郵件伺服器的位址。

  如果您輸入多個位址，使用分號分隔。您可以使用以下參數：

  - IPv4 或 IPv6 位址
  - 裝置的 Windows 網路名稱（NetBIOS 名稱）
  - SMTP 伺服器的 DNS 名稱

- **SMTP 伺服器連接埠**

  SMTP 伺服器的通訊埠號。如果您使用多部 SMTP 伺服器，則會透過指定的通訊連接埠與它們建立連線。預設埠號為 25。

- **使用 ESMTP 身分驗證**

  啟用 ESMTP 身分驗證支援。當選取了該核取方塊時，您可以在**使用者名稱**和**密碼**欄位指定 ESMTP 身分驗證設定。預設情況下已清空此方塊。

- **設定**

  指定下列設定：

  - **主旨**（電子郵件的主旨）
  - **寄件者電子郵件地址**
  - **SMTP 伺服器的 TLS 設定**

  您可以為 SMTP 伺服器指定 TLS 設定：

  您可以停用 TLS 的使用，如果 SMTP 伺服器支援此協議，則使用 TLS，或者您可以強制僅使用 TLS。如果您選取僅使用 TLS，請指定用於驗證 SMTP 伺服器的憑證，並選取是要透過任何版本的 TLS，還是僅透過 TLS 1.2 或更高版本啟用通訊。此外，如果您選取僅使用 TLS，您可以為 SMTP 伺服器上的用戶端身分驗證指定憑證。

  - 瀏覽 SMTP 伺服器憑證檔案：

  您可以從受信任的憑證頒發機構接收帶有憑證清單的檔案，然後將該檔案上傳到管理伺服器。卡巴斯基安全管理中心會檢查 SMTP 伺服器的憑證是否也由受信任的憑證頒發機構簽署。如果未從受信任的憑證頒發機構收到 SMTP 伺服器的憑證，卡巴斯基安全管理中心將無法連線到 SMTP 伺服器。

  - 瀏覽用戶端憑證檔案：

  您可以使用從任何來源（例如，從任何受信任的憑證頒發機構）收到的憑證。您必須使用以下憑證類型之一指定憑證及其私密金鑰：

  - X-509 憑證：

  指定一個含有憑證的檔案和一個含有私密金鑰的檔案。這些檔案的上傳順序不拘。當同時上傳兩個檔案時，請指定用於解密私密金鑰的密碼。如果私密金鑰未加密，則密碼可以為空值。

  - pkcs12 容器：

  您必須上傳包含憑證及其私密金鑰的單一檔案。載入檔案後，您必須指定用於解碼私密金鑰的密碼。如果未編碼私密金鑰未編碼，則密碼可以為空值。

您可以透過點擊**傳送測試訊息**按鈕測試新郵件通知設定。

您也可以稍後設定事件通知，不需透過快速啟動精靈。

步驟 8：配置更新管理

設定管理用戶端裝置上安裝的更新的設定。

只有當您提供有弱點和修補程式管理選項的產品授權金鑰時，才可配置這些設定。

在設定的**搜尋並安裝更新**群組中，您可以選取卡巴斯基安全管理中心更新搜尋和安裝的模式：

- **搜尋所需更新**

  如果您沒有*弱點掃描和所需更新*工作，系統會自動建立該工作。

  預設情況下已選取此選項。

- **尋找與安裝需要的更新**

  若您沒有，系統會自動建立*弱點掃描和所需更新*和*安裝所需更新並修復弱點*的工作。

在設定的**Windows Server Update Services**群組中，您可以選取更新同步來源：

- **使用網域政策中定義的更新來源**

  用戶端裝置將會根據網域政策設定下載 Windows Update 更新。若您沒有，會自動建立網路代理政策。

- **使用管理伺服器作為 WSUS 伺服器**

  用戶端裝置將會從管理伺服器下載 Windows Update 更新。若您沒有，會自動建立*執行 Windows Update 同步*工作和網路代理政策。

您可以從快速啟動精靈單獨建立*尋找弱點和所需更新*和*安裝所需更新並修復弱點*工作。若要使用管理伺服器作為 WSUS 伺服器，請建立*執行 Windows Update 同步*工作，然後選取網路代理政策中的**使用管理伺服器作為 WSUS 伺服器**選項。

步驟 9：建立初始防護設定

設定初始化防護視窗顯示自動建立的政策和工作清單。系統會建立以下政策與工作：

- 卡巴斯基安全管理中心網路代理政策
- 受管理 Kaspersky 應用程式（之前已安裝管理外掛程式）的政策
- 管理伺服器維護工作
- 備份管理伺服器資料工作
- 將更新下載至管理伺服器儲存區工作
- 弱點掃描和所需更新工作
- 安裝更新工作

等待政策和工作完成建立，然後轉到精靈的下一步。

若您已下載並安裝適用於 Kaspersky Endpoint Security for Windows 10 Service Pack 1 與最高至 11.0.1 的更新版本的外掛程式，在建立政策與工作期間，系統會開啟一個視窗供您初始設定 Kaspersky Endpoint Security for Windows 的信任區域。應用程式將提示您新增被 Kaspersky 驗證過的供應商到信任網域，以便從掃描中排除他們的應用程式以防止它們被自動封鎖。您可透過在主控台樹狀目錄中選取以下項目以立即建立建議的排除項目或在之後建立排除項目清單：**政策** → Kaspersky Endpoint Security 內容功能表 → **進階威脅防護** → **信賴的區域** → **設定** → **新增**。掃描排除項目清單在使用應用程式的任意時刻都可以編輯。

管理員可使用 Kaspersky Endpoint Security for Windows 中整合的工具執行信任網域操作。關於如何執行操作的詳細說明和加密功能的詳細資訊，請參閱 Kaspersky Endpoint Security for Windows Online Help。

要完成信任網域的初始設定並返回精靈，按一下**確定**。

點擊**"下一步"**。該按鈕在所有政策和工作被建立後可用。

您也可以稍後建立所需的工作和政策，不需透過快速啟動精靈。

步驟 10：連線行動裝置

如果您先前在精靈設定中選取啟用**行動裝置**防護範圍，請指定受管理組織中企業行動裝置的連線設定。如果您不啟用**行動裝置**防護範圍，系統會略過該步驟。

在精靈的此步驟中，您可以進行以下操作：

- 設定行動裝置連線連接埠：
- 設定管理伺服器身分驗證
- 建立或管理憑證
- 設定一般憑證的發佈、自動更新和加密
- 為行動裝置建立移動規則

要設定行動裝置連線連接埠：

1. 點擊**行動裝置連線**欄位右方的**設定**按鈕。
2. 在下拉清單中，選取**配置連接埠**。
   管理伺服器內容視窗隨即開啟，顯示**附加連接埠**區域。

3. 在**附加連接埠**區域中，您可以指定行動裝置連線設定：

- **啟動代理伺服器的 SSL 連接埠**

  SSL 埠號，以將 Kaspersky Endpoint Security for Windows 連線到 Kaspersky 的啟動伺服器。
  預設埠號為 17000。

- **為行動裝置開啟連接埠**

  行動裝置連線到產品授權伺服器的連接埠被開啟。您可以在以下欄位定義埠號和其他設定。
  預設情況下已啟用該選項。

- **行動裝置同步連接埠**

  行動裝置連線到管理伺服器並與其交換資料的埠號。預設埠號為 13292。
  如果連接埠 13292 被用於其他目的，您可以分配其他連接埠。

- **行動裝置啟動連接埠**

  用於將 Kaspersky Endpoint Security for Android 連線到 Kaspersky 啟動伺服器的連接埠。
  預設埠號為 17100。

- **開啟 UEFI 防護裝置和 KasperskyOS 裝置的連接埠**

  UEFI 防護裝置可以連線到管理伺服器。

- **UEFI 防護裝置和 KasperskyOS 裝置的連接埠**

  若啟用**開啟 UEFI 防護裝置和 KasperskyOS 裝置的連接埠**選項則可變更埠號。預設埠號為 13294。

- **開啟 Prometheus 的連接埠**

  Prometheus 提取請求連接埠。預設埠號為 13296。

4. 點擊**確定**以儲存變更並返回到快速啟動精靈。

您將必須設定管理伺服器的行動裝置身分驗證和行動裝置的管理伺服器身分驗證。如有需要，您可以稍後設定身分驗證，不需透過快速設定精靈設定。

要設定管理伺服器的行動裝置身分驗證：

1. 點擊**行動裝置連線**欄位右方的**設定**按鈕。
2. 在下拉式清單中，選取**配置身分驗證**。

   管理伺服器內容視窗隨即開啟，顯示**憑證**區段。
3. 在設定的**管理伺服器的行動裝置身分驗證**群組選取行動裝置驗證選項，並在**管理伺服器的 UEFI 防護裝置身分驗證**設定群組選取 UEFI 防護裝置的驗證選項。

   當管理伺服器與用戶端裝置交換資料時，它透過使用憑證來驗證。

   預設下，管理伺服器使用管理伺服器安裝過程中建立的憑證。如果您想，您可以新增新憑證。

要新增新憑證（可選）：

1. 選取**其他憑證**。

   瀏覽按鈕隨即顯示。
2. 點擊**瀏覽**按鈕。
3. 在開啟的視窗，指定憑證設定：

   - **憑證類型**

     在該下拉清單中，您可以選取憑證類型：

     - **X.509 憑證**.如果選取此選項，您應該指定憑證的私密金鑰和開放的憑證：
       - **私密金鑰(.prk 、.pem)**。在此欄位點擊**瀏覽**按鈕，以指定 PKCS #8 (*.prk) 格式的憑證私密金鑰。
       - **公開金鑰 (.cer)**。在此欄位點擊**瀏覽**按鈕，以指定 PEM (*.cer) 格式的公開金鑰。
     - **PKCS#12 容器**。如果您選取了此選項，則可以透過點擊**瀏覽**按鈕並填寫**憑證檔案**欄位來指定 P12 或 PFX 格式的憑證檔案。

   - 啟動時間：
     - **立即**

       在您點擊**確定**後目前憑證將由新憑證立即取代。

       先前連線的行動裝置將不能連線到管理伺服器。
     - **該時間段到期後，天數**

       如果選中該選項，將生成備用憑證。在指定天數後目前憑證將被新憑證代替。備用憑證的有效日期會顯示在**憑證**區域。

       建議您事先規劃重新發佈事宜。在指定的期限到期之前，必須將儲稅券下載到行動裝置。目前憑證由新憑證取代後，先前連線且沒有保留憑證的行動裝置將不能連線到管理伺服器。
4. 點擊**內容**按鈕以檢視選取的管理伺服器憑證設定。

要透過管理伺服器重新發佈憑證：

1. 選擇**透過管理伺服器發佈的憑證**。
2. 點擊**重新發佈**按鈕。
3. 在開啟的視窗，指定以下設定：
   - 連線位址：
     - **使用舊連線位址**

       行動裝置要連線的管理伺服器位址將保持不變。

       預設情況下已選取此選項。
     - **變更連線位址到**

       如果您要讓行動裝置連線到其他位址，在該欄位指定相關位址。

       如果行動裝置連線位址被變更，必須發佈新的憑證。舊的憑證將在所連線的行動裝置上不可用。先前連線的裝置將不能連線到管理伺服器，因此將不再可管理。
   - 啟動時間：
     - **立即**

       在您點擊**確定**後目前憑證將由新憑證立即取代。

       先前連線的行動裝置將不能連線到管理伺服器。
     - **該時間段到期後，天數**

       如果選中該選項，將生成備用憑證。在指定天數後目前憑證將被新憑證代替。備用憑證的有效日期會顯示在**憑證**區域。

       建議您事先規劃重新發佈事宜。在指定的期限到期之前，必須將儲稅券下載到行動裝置。目前憑證由新憑證取代後，先前連線且沒有保留憑證的行動裝置將不能連線到管理伺服器。
4. 點擊**確定**以儲存變更並返回**憑證**視窗。
5. 點擊**確定**以儲存變更並返回到快速啟動精靈。

要設定用於由管理伺服器識別行動裝置的一般類型憑證的發佈、自動更新和加密：

1. 點擊**行動裝置身分驗證**欄位右方的**設定**按鈕。

   開啟的**憑證發佈規則**視窗中顯示**行動憑證發佈**區域。

2. 如果必要，在**發佈設定**區域指定以下設定：

   - **憑證生命週期，天**

     憑證生命週期（天）。預設的憑證生命週期是 365 天。此時間段到期後，行動裝置將不能連線到管理伺服器。

   - **憑證來源**

     為行動裝置選取一般類型來源：憑證由管理伺服器發佈，或被手動指定。

     如果與公共金鑰基礎架構 (PKI) 的整合已在**與 PKI 整合**區域設定，則您可以修改憑證範本。此種情況下，以下範本分類欄位可用：

   - **預設範本**

     使用由外部憑證來源發佈的憑證 – 憑證中心 – 在預設範本下。

     預設情況下已選定此選項。

   - **其他範本**

     選取用於發佈憑證的範本。您可在該域中指定憑證範本。**重新整理清單**按鈕可更新憑證範本的清單。

3. 如果必要，在**自動更新設定**區域為憑證的自動發佈指定以下設定：

   - **當憑證剩餘此天數時續約**

     目前憑證到期前管理伺服器應當發佈新憑證的剩餘天數。例如，如果欄位值為 4，管理員伺服器會在目前憑證到期的前 4 天發佈新的憑證。預設值是 7。

   - **如果可能，自動重新發佈憑證**

     選擇此選項可自動重新發佈憑證，天數為**當憑證剩餘此天數時續約**欄位中指定的天數。如果憑證是手動定義的，則無法自動續約，並且啟用的選項將不起作用。

     預設情況下已停用該選項。

   憑證由認證中心自動重新發佈。

4. 如有必要，請在**密碼防護**設定區域，指定在安裝過程中解密憑證的設定。

   選取**在憑證安裝過程中提示密碼**選項，以在憑證被安裝到行動裝置上時提示使用者輸入密碼。密碼僅用一次 — 在安裝憑證到行動裝置時。

   憑證將透過管理伺服器自動產生並傳送到您指定的電子郵件信箱。您可以指定使用者的電子郵件信箱，或您自己的電子郵件信箱，如果您要使用其他方法轉發密碼到使用者。

   您可以使用捲軸在憑證解密密碼中指定字元數。

   需要密碼提示選項，例如，以在獨立 Kaspersky Endpoint Security for Android 安裝套件中防護共用憑證。密碼防護將防止入侵者透過從卡巴斯基安全管理中心網頁伺服器竊取獨立安裝套件獲取到共用憑證的存取。

   如果該選項被停用，憑證在安裝過程中被自動解密，且使用者不被提示密碼。預設情況下已停用該選項。

5. 點擊**確定**以儲存變更並返回快速啟動精靈視窗。

   點擊**取消**按鈕以返回快速啟動精靈而不儲存任何變更。

要啟用移動行動裝置到您選取的管理群組的功能，

在**行動裝置自動移動**欄位中，選取**為行動裝置建立移動規則**選項。

如果選取了**為行動裝置建立移動規則**選項，應用程式自動建立移動規則以移動執行 Android 和 iOS 的裝置到**受管理裝置**群組：

- 安裝了 Kaspersky Endpoint Security for Android 和行動憑證的 Android 作業系統
- iOS 作業系統上有安裝共用憑證的 iOS MDM 設定檔

如果此規則已經存在，應用程式不再建立它。

預設情況下已停用該選項。

Kaspersky 不再支援 Kaspersky Safe Browser。

步驟 11：下載更新

卡巴斯基安全管理中心病毒資料庫的更新和受管理 Kaspersky 應用程式的更新會由系統自動下載。更新會從 Kaspersky 伺服器下載。

要從快速啟動精靈中單獨下載更新，請建立和設定「*將更新下載至管理伺服器儲存區*」工作。

步驟 12：裝置發現

網路輪詢視窗顯示由管理伺服器執行的網路輪詢狀態的資訊。

您可以檢視由管理伺服器偵測到的網路裝置並透過點擊視窗下部的連結接收關於**裝置發現**視窗的說明。

您可以稍後輪詢您的網路，單獨從快速啟動精靈這行。使用管理主控台配置 Windows 網域、Active Directory、IP 範圍和IPv6 網絡 的輪詢。

步驟 13：關閉快速啟動精靈

在「快速啟動精靈」完成視窗中，如果您想自動安裝病毒防護應用程式和/或網路代理到您的網路裝置，請選取**執行遠端安裝精靈**選項。

要完成精靈，請點擊**完成**按鈕。

設定管理主控台與管理伺服器的連線

管理主控台是透過 SSL 連接埠 TCP 13291 連線至管理伺服器。klakaut 自動化物件可使用相同的連接埠。

連接埠 TCP 14000 僅可以用於連線管理主控台、發佈點、從屬管理伺服器和 klakaut 自動化物件，以及用於從用戶端裝置接收資料。

通常，SSL 連接埠 TCP 13000 僅可以由網路代理、從屬管理伺服器和 DMZ 中的主管理伺服器使用。在一些情況下，管理主控台可能需要透過 SSL 連接埠 13000 連線：

- 如果將單一的 SSL 連接埠用於管理主控台和其他活動（從用戶端裝置接收資料、連線發佈點、連線從屬管理伺服器）。
- 如果 klakaut 自動化物件未直接連線到管理伺服器，而是透過 DMZ 中的發佈點。

要允許透過連接埠 13000 的管理主控台連線：

1. 開啟安裝了管理伺服器的裝置的登錄檔（例如，在**開始 → 執行**功能表使用 regedit 指令）。
2. 轉至以下分支：
   - 對於 32 位元系統：
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - 對於 64 位元系統：
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. 對於 LP_ConsoleMustUsePort13291 (DWORD) 鍵，設定 00000000 值。
   該鍵指定的預設值是 1。
4. 重新啟動管理伺服器服務。

結果，您將可以透過連接埠 13000 連線管理主控台到管理伺服器。

設定管理伺服器的網際網路存取設定

您必須設定網際網路存取權限，才能使用卡巴斯基安全網路並下載卡巴斯基安全管理中心病毒資料庫和受管理卡巴斯基應用程式的更新。

指定管理伺服器的網際網路存取設定：

1. 在主控台樹狀目錄中，選取**管理伺服器**節點。
2. 在管理伺服器的上下文功能表中，選取**內容**。
3. 在管理伺服器視窗中，轉到**進階** → **設定網際網路存取**。
4. 如果您要在連線到網際網路時使用代理伺服器，選取**使用代理伺服器**選項。如果選取此選項，可將欄位用於輸入設定。為代理伺服器連線指定以下設定：

   - **位址**

     卡巴斯基安全管理中心用於連線到網際網路的代理伺服器位址。

   - **連接埠號**

     將建立卡巴斯基安全管理中心代理伺服器連線的埠號。

   - **略過本機位址的代理伺服器**

     將不會使用代理伺服器連線本機網路的裝置。

   - **代理伺服器身分驗證**

     如果選取該方塊，您可以在輸入欄位中為代理伺服器身分驗證指定憑證。

     如果選取**使用代理伺服器**核取方塊，則可使用該輸入欄位。

   - **使用者名稱**

     用來建立前往 Proxy 伺服器之連線的使用者帳戶（若選取了**代理伺服器身分驗證**核取方塊，則此欄位可用）。

   - **密碼**

     其帳戶用來建立 Proxy 伺服器連線的使用者所設定的密碼（若選取了**代理伺服器身分驗證**核取方塊，則此欄位可用）。

     若要檢視輸入的密碼，依您所需的時間長度點擊並按住**顯示**按鈕。

您還可以使用快速啟動精靈設定網際網路存取。

連線漫遊裝置

本節說明如何將漫遊裝置（即位於主網路外的受管理裝置）連線到管理伺服器。

情境：透過連線閘道連線辦公室外的裝置

此方案說明如何將位於主網路外的受管理裝置連線到管理伺服器。

先決條件

該情境需有以下先決條件：

- 非警戒區域 (DMZ) 會在組織的網路中組織。
- 卡巴斯基安全管理中心管理伺服器已佈署在公司網路上。

階段

此情境分階段進行：

1. **在 DMZ 中選取用戶端裝置**

   此裝置將作為連線閘道使用。您選取的裝置必須滿足連線閘道的要求。

2. **以連線閘道角色安裝網路代理**

   我們建議您使用本機安裝在所選裝置上安裝網路代理。

   預設情況下，安裝檔案位於：\\<伺服器名稱>\KLSHARE\PkgInst\NetAgent_<版本編號>

   在網路代理安裝精靈的**連線閘道**視窗中，選取**使用網路代理作為 DMZ 連線閘道**。此模式同時啟動連線閘道角色，並通知網路代理等待來自管理伺服器的連線，而不是建立與管理伺服器的連線。

   或者，您可以在 Linux 裝置上安裝網路代理並將網路代理設定為連線閘道使用，但是要注意在 Linux 裝置上執行的網路代理限制清單。

3. **允許連線閘道上防火牆中的連線**

   為確保管理伺服器實際上可以連線到 DMZ 中的連線閘道，請允許連線到管理伺服器和連線閘道間所有防火牆中的 TCP 連接埠 13000。

   如果連線閘道在網際網路上沒有真實 IP 地址，而是位於網路位址轉換 (NAT) 後面，請配置規則以透過 NAT 轉發連線。

4. **建立外部裝置的管理群組**

   在**受管理裝置**群組下建立新群組。此新群組將包含外部受管理裝置。

5. **將連線閘道連到管理伺服器**

   您配置的連線閘道正在等待來自管理伺服器的連線。但是，管理伺服器未在受管理裝置中列出具有連線閘道的裝置。這是因為連線閘道尚未嘗試建立與管理伺服器的連線。因此，您需要一個特殊程序來確保管理伺服器啟動到連線閘道的連線。

   請執行下列操作：

   1. 將連線閘道新增為發佈點。
   2. 將連線閘道從**未配置的裝置**群組移動到您為外部裝置建立的群組。

   連線閘道已連線並配置。

6. **將外部桌上型裝置連線到管理伺服器**

   通常，外部桌上型裝置不會在週邊環境中移動。因此，在安裝網路代理時，需要配置它們以透過閘道連線到管理伺服器。

7. **設定外部桌上型裝置的更新**

   如果將安全應用程式的更新設定為從管理伺服器下載，則外部裝置將透過連線閘道下載更新。這有兩個缺點：

   - 這是不必要的流量，會佔用公司的網際網路通訊頻道的頻寬。
   - 這不一定是獲取更新的最快方法。對於外部裝置來說，從卡巴斯基更新伺服器接收更新可能會更便宜、更快捷。

   請執行下列操作：

   1. 將所有外部裝置移至您先前建立的單獨管理群組。
   2. 從更新工作中排除具有外部裝置的群組。
   3. 使用外部裝置為該群組建立單獨的更新工作。

8. **將行動的筆記型電腦連線到管理伺服器**

   行動的筆記型電腦有時位於網路內部，而其他時間位於網路外部。為了有效管理，您需要根據其位置以不同的方式連線到管理伺服器。為了有效利用流量，他們還需要根據所在位置從不同來源接收更新。

   您需要為漫遊使用者配置規則：連線設定檔和網路位置描述。每個規則都根據其位置定義了行動筆記型電腦必須連線到的管理伺服器實例，以及必須從中接收更新的管理伺服器實例。

情境：通過 DMZ 中的從屬管理伺服器連線漫遊裝置

如果要將位於主網路外的受管理裝置連線到管理伺服器，可以使用位於隔離區 (DMZ) 中的從屬管理伺服器來實現。

先決條件

在您開始之前，確保您已做了如下：

- DMZ 會在組織的網路中組織。
- 卡巴斯基安全管理中心管理伺服器已佈署在組織的內部網路上。

階段

此情境分階段進行：

1. **在 DMZ 中選取用戶端裝置**

   在 DMZ 中，選擇將用作從屬管理伺服器的用戶端裝置。

2. **安裝卡巴斯基安全管理中心管理伺服器**

   在此用戶端裝置上安裝卡巴斯基安全管理中心管理伺服器。

3. **建立管理伺服器階層**

如果將從屬管理伺服器放置在 DMZ 中，則從屬管理伺服器必須接收來自主管理伺服器的連線。為此，可以新增新管理伺服器作為從屬管理伺服器，以便主管理伺服器透過連接埠 13000 連線到從屬管理伺服器。當組合兩個管理伺服器到一個層級，確保連接埠 13291 在兩個管理伺服器上都可以存取。管理主控台透過連接埠 13291 連線到管理伺服器。

4. **將不在辦公室的受管理裝置連線到從屬管理伺服器。**

   您可以將不在辦公室的裝置連線到 DMZ 中的管理伺服器，其連線方式與在管理伺服器和位於主網路中的受管理裝置之間建立連線的方式相同。不在辦公室的受管理裝置通過連線埠 13000 發起連線。

關於連線辦公室外的裝置

部分受管理裝置永遠位在主網路之外（例如，地區分公司中的裝置；資訊站、ATM 和安裝在各個銷售點的終端機；員工居家辦公的裝置）。有些裝置不時在外圍移動（例如，存取地區分公司或客戶辦公室的使用者筆記型電腦）。

您仍然需要監控和管理漫遊裝置受保護的情況，接收其保護狀態的實際資訊，並使裝置上的安全應用程式保持最新狀態。這是必要措施，因為如果這樣的裝置在遠離主網路時受到威脅，一旦它們連到主網路，就可能成為傳播威脅的平台。要將辦公室外的裝置連線到管理伺服器，可以使用兩種方法：

- 非警戒區 (DMZ) 中的連線閘道

  請參閱資料流量方案：LAN 上的管理伺服器、網際網路上的受管理裝置、正在使用的連線閘道

- DMZ 中的管理伺服器

  請參閱資料流量方案：DMZ 中的管理伺服器、網際網路上的受管理裝置。

DMZ 中的連線閘道

將辦公室外的裝置連線到管理伺服器的推薦方法是在組織的網路中組織 DMZ，並在 DMZ 中安裝連線閘道。外部裝置將連線到連線閘道，網路內部的管理伺服器將透過連線閘道啟動與裝置的連線。

與其他方法相比，此方法更安全：

- 您不需要從網路外部開啟對管理伺服器的存取。
- 受損的連線閘道不會對網路裝置的安全構成高風險。連線閘道本身實際上並不管理任何東西，也不會建立任何連線。

而且，連線閘道不需要很多硬體資源。

但是，此方法的設定過程較為複雜：

- 若要使裝置作為 DMZ 中的連線閘道，您需要安裝網路代理並以特定方式將其連線到管理伺服器。
- 在所有情況下，您將無法使用相同的位址連線到管理伺服器。從週邊以外，您不僅需要使用其他位址（連線閘道位址），還需要使用其他連線模式：透過連線閘道。
- 您還需要為不同位置的筆記型電腦定義不同的連線設定。

要將連線閘道新增到先前配置的網路：

1. 以連線閘道模式安裝網路代理。

2. 在要連線到新增的連線閘道的裝置上重新安裝網路代理。

DMZ 中的管理伺服器

另一種方法是在 DMZ 中安裝一個管理伺服器。

此配置不如其他方法安全。在這種情況下，要管理外部筆記型電腦，管理伺服器必須接受來自網際網路上任何位址的連線。它仍然將管理內部網路中的所有裝置，但會透過 DMZ 進行管理。因此，儘管發生此類事件的可能性很小，但有風險的伺服器可能會造成巨大的損失。

如果 DMZ 中的管理伺服器不管理內部網路中的裝置，則風險將大大降低。例如，服務提供商可以使用這種設定來管理客戶的裝置。

在以下情況下，您可能要使用此方法：

- 如果您熟悉安裝和配置管理伺服器，並且不想執行其他過程來安裝和設定連線閘道。
- 如果您需要管理更多裝置。管理伺服器的最大容量為 100,000 台裝置，而連線閘道最多可支援 10,000 台裝置。

此解決方案也可能有困難：

- 管理伺服器需要更多的硬體資源和一個資料庫。
- 有關裝置的資訊將儲存在兩個不相關的資料庫中（用於網路內的管理伺服器，另一個用於 DMZ 中的資料庫），這使監控變得複雜。
- 若要管理所有裝置，則需要將管理伺服器連線到一個階層中，使得監控和管理變得複雜。從屬管理伺服器執行個體對管理群組的可能架構施加了限制。您必須決定如何以及將哪些工作和政策分配給從屬管理伺服器執行個體。
- 配置外部裝置以從外部使用 DMZ 中的管理伺服器並從內部使用主管理伺服器，並不比僅設定它們透過閘道使用條件式連線簡單。
- 高安全風險。受到破壞的管理伺服器實例可以更輕鬆地破壞其受管理的筆記型電腦。如果發生這種情況，駭客只需要等待其中一台筆記本電腦返回公司網路，即可繼續對區域網路展開攻擊。

將外部桌上型裝置連線到管理伺服器

永遠位在主網路之外的桌上型裝置（例如，地區分公司中的裝置；資訊站、ATM 和安裝在各個銷售點的終端機；員工居家辦公的裝置）不能直接連線到管理伺服器。它們必須透過安裝在非軍事區 (DMZ) 中的連線閘道連線到管理伺服器。在這些裝置上安裝網路代理時，將進行此設定。

要將外部桌上型裝置連線到管理伺服器，請執行以下操作：

1. 為網路代理建立一個新的安裝套件。
2. 開啟已建立的安裝套件屬性，轉到**進階**部分，然後選取**透過使用連線閘道連線到管理伺服器**選項。

   透過使用連線閘道連線到管理伺服器設定與**使用網路代理作為 DMZ 連線閘道**設定不相容。您不能同時啟用這兩個設定。

3. 在**連線閘道位址**中，指定連線閘道的公共位址。

   如果連線閘道位於網路位址轉換 (NAT) 後面並且沒有自己的公用位址，請配置 NAT 閘道規則以將連線從公用位址轉發到連線閘道的內部位址。

4. 建立以已建立安裝套件為基礎的獨立安裝套件。
5. 透過電子方式或在卸除式磁碟機上將獨立安裝套件傳輸至目標裝置。
6. 從獨立安裝套件安裝網路代理。

外部桌上型裝置已連線到管理伺服器。

關於漫遊使用者的連線設定檔

可攜式電腦（也叫"裝置"）的漫遊使用者需要變更連線到管理伺服器的方法或者根據目前裝置在企業網路中的位置在管理伺服器之間進行轉換。

連線設定檔僅支援執行 Windows 和 macOS 的裝置。

使用單一管理伺服器的不同位址

網路代理裝置從組織網路或內部網可以連線到管理伺服器。該情況可能需要網路代理使用不同的位址以連線到管理伺服器：對於網際網路連線的外部管理伺服器位址和對於內部網路連線的內部管理伺服器位址。

為此，您必須新增設定檔（為了從網際網路連線到管理伺服器）到網路代理政策。在政策內容中新增設定檔（**連線**區域，**連線設定檔**子區域）。在建立設定檔視窗中，您必須停用**僅用來接收更新**選項並選取**在此設定檔中同步連線設定和管理伺服器設定**選項。如果您使用連線閘道存取管理伺服器（例如，在"網際網路存取：DMZ 中作為連線閘道的網路代理"部分敘述的卡巴斯基安全管理中心設定中），您必須在連線設定檔的對應欄位指定連線閘道位址。

根據目前網路在管理伺服器之間進行轉換

如果組織有帶有多個管理伺服器的多個辦公室，並且一些網路代理裝置在期間進行移動，您需要網路代理連線到裝置所在的本機網路中的管理伺服器。

此種情況下，您必須為每個辦公室在網路代理政策內容中建立連線管理伺服器的設定檔，除了歸屬管理伺服器所在的主辦公室。您必須在連線設定檔中指定管理伺服器位址，並啟用或停用**僅用來接收更新**選項：

- 在使用本機伺服器下載更新時，如果您需要網路代理與歸屬管理伺服器同步，則選中此選項。
- 如果網路代理必須被本機管理伺服器完全管理，則停用此選項。

此後，您必須設定轉換到新建立的設定檔的條件：每個辦公室至少一個條件，除了歸屬辦公室。每個條件的目的包括辦公室網路環境項目的偵測。如果條件是真，對應設定檔被啟動。如果沒有條件是真，網路代理轉換到歸屬管理伺服器。

為漫遊使用者建立連線設定檔

管理伺服器連線設定檔僅在執行 Windows 和 macOS 的裝置上可用。

若要為漫遊使用者建立網路代理連線至管理伺服器的連線設定檔，請執行以下操作：

1. 在主控台樹狀目錄中，為您要建立設定檔以連線網路代理到管理伺服器的用戶端裝置選取一個管理群組。
2. 執行以下操作之一：
   - 如果您要為群組中的所有裝置建立連線設定檔，請在群組工作區的**政策**標籤中選取網路代理政策。開啟所選政策的內容視窗。
   - 如果您要為群組中的裝置建立連線設定檔，請在群組工作區中的**裝置**標籤選取該裝置，並執行以下操作：
     a. 開啟所選裝置的內容視窗。
     b. 在裝置內容視窗的**應用程式**區域中，選取網路代理。
     c. 開啟網路代理內容視窗。
3. 在內容視窗的 **連線**區域中，選取**連線設定檔**子區域。
4. 在**管理伺服器連線設定檔**設定群組中，點擊**新增**按鈕。

   預設下，連線設定檔清單包含<離線模式>和<歸屬管理伺服器>設定檔。您不能編輯或刪除設定檔。

   <離線模式>設定檔不指定任何伺服器以連線。因此，網路代理，當切換到該設定檔時，當用戶端裝置上的應用程式工作在漫遊政策下時不試圖連線到任何管理伺服器。如果裝置與網路斷開連線，可以使用<離線模式>設定檔。

   <歸屬管理伺服器>設定檔指定在網路代理安裝過程中選取的管理伺服器的連線。當裝置在外部網路中執行了一段時間後重新連線到管理伺服器時，<歸屬管理伺服器>設定檔被套用。

5. 在開啟的**新設定檔**視窗中，配置連線設定檔：

- **設定檔名稱**

  在該輸入欄位中，您可以檢視或變更連線設定檔名稱。

- **管理伺服器**

  用戶端裝置在設定檔啟動期間必須連線的管理伺服器位址。

- **連接埠**

  用於連線的埠號。

- **SSL 連接埠**

  使用 SSL 協定時的埠號。

- **使用 SSL**

  如果啟用此選項，則使用 SSL 協定透過安全埠建立連線。
  預設情況下已啟用該選項。我們建議您不要停用此選項，以便您的連線保持安全。

- 點擊**設定透過代理伺服器的連線**連結以透過代理伺服器設定連線。如果您要在連線到網際網路時使用代理伺服器，選取**使用代理伺服器**選項。如果選取此選項，可將欄位用於輸入設定。為代理伺服器連線指定以下設定：

  - **代理伺服器位址**

    卡巴斯基安全管理中心用於連線到網際網路的代理伺服器位址。

  - **連接埠號**

    將建立卡巴斯基安全管理中心代理伺服器連線的埠號。

  - **代理伺服器身分驗證**

    如果選取該方塊，您可以在輸入欄位中為代理伺服器身分驗證指定憑證。
    如果選取**使用代理伺服器**核取方塊，則可使用該輸入欄位。

  - **使用者名稱**（如果選取**代理伺服器身分驗證**選項，則可使用該欄位）

    用來建立前往 Proxy 伺服器之連線的使用者帳戶（若選取了**代理伺服器身分驗證**核取方塊，則此欄位可用）。

  - **密碼**如果選取**代理伺服器身分驗證**選項，則可使用該欄位）

其帳戶用來建立 Proxy 伺服器連線的使用者所設定的密碼（若選取了**代理伺服器身分驗證**核取方塊，則此欄位可用）。

若要檢視輸入的密碼，依您所需的時間長度點擊並按住**顯示**按鈕。

- **連線閘道設定**

  透過用戶端裝置連線至管理伺服器的閘道位址。

- **啟用漫遊模式**

  如果啟用此選項，則在透過該設定檔連線的情況下，用戶端裝置上安裝的應用程式將使用漫遊模式裝置的政策設定檔，以及漫遊政策。如果沒有為應用程式定義漫遊政策，則使用啟動政策。

  如果停用此選項，則應用程式將使用已啟動的政策。

  預設情況下已停用該選項。

- **僅用來接收更新**

  如果啟用此選項，則該設定檔將僅被用戶端裝置上安裝的應用程式用來下載更新。對於其他操作，程式將使用在網路代理安裝過程中定義的初始連線設定連線管理伺服器。

  預設情況下已啟用該選項。

- **在此設定檔中同步連線設定和管理伺服器設定**

  如果停用此選項，網路代理將使用設定檔屬性中指定的設定連線至管理伺服器。

  如果停用此選項，網路代理將使用安裝期間已指定的原始設定連線至管理伺服器。

  如果停用**僅用來接收更新**選項，則此選項可用。

  預設情況下已停用該選項。

6. 選取**當管理伺服器不可用時啟用漫遊模式**選項，允許用戶端裝置上安裝的應用程式在在不可使用管理伺服器進行的任何離線嘗試時，以漫遊模式使用政策設定檔和漫遊政策。如果沒有為應用程式定義漫遊政策，則使用啟動政策。

程式將為漫遊使用者建立一個用於將網路代理連線至管理伺服器的設定檔。當使用此設定檔將網路代理連線至管理伺服器後，用戶端裝置上安裝的應用程式將使用漫遊模式裝置的政策，或漫遊政策。

關於將網路代理切換到其他管理伺服器

網路代理連線至管理伺服器的初始設定在安裝網路代理時定義。要將網路代理切換到其他管理伺服器，您可以使用切換規則。僅執行 Windows 或 macOS 的裝置上安裝的網路代理支援此功能。

切換規則可以在變更以下網路參數時觸發：

- 預設閘道位址。
- Dynamic Host Configuration Protocol (DHCP) 伺服器的 IP 位址。
- 子網路的 DNS 後置詞。

- 網路 DNS 伺服器的 IP 位址。
- Windows 網域可存取性。此參數僅適用於執行 Windows 的裝置。
- 子網路位址和遮罩。
- 網路 WINS 伺服器的 IP 位址。此參數僅適用於執行 Windows 的裝置。
- 用戶端裝置的 DNS 或 NetBIOS 名稱。
- SSL 連線位址可存取性。

如果建立了將網路代理轉換至其他管理伺服器的規則，網路代理將以下列方式回應網路參數的變更：

- 如果網路設定符合已建立的規則之一，網路代理將連線至該規則中指定的管理伺服器。如果該規則中已經啟用漫遊轉換政策，用戶端裝置上的應用程式將轉換至漫遊政策。
- 如果未套用任何規則，網路代理將回溯至安裝過程中指定的管理伺服器連線預設設定。用戶端裝置上安裝的應用程式將回溯至活動政策。
- 如果無法存取管理伺服器，網路代理將使用使用者漫遊政策。

網路代理只會在網路代理政策設定中的**當管理伺服器不可用時啟用漫遊模式**選項啟用時才會切換至漫遊政策。

網路代理連線至管理伺服器的設定儲存在連線設定檔中。在連線設定檔中，您可以建立將用戶端裝置轉換至漫遊政策的規則，並可對設定檔進行設定，使其僅可用於下載更新。

依據網路位置建立網路代理轉換規則

根據網路位置切換網路代理僅在執行 Windows 和 macOS 的裝置上可用。

若要建立一個當網路設定改變時將網路代理從一個管理伺服器轉換至另一個的規則，請執行以下操作：

1. 在主控台樹狀目錄中，為要透過網路位置敘述建立網路代理轉換規則的裝置選取一個管理群組。
2. 執行以下操作之一：
   - 如果您要為群組中的所有裝置建立規則，請在群組工作區的**政策**頁籤中選取一個網路代理政策。開啟所選政策的內容視窗。
   - 如果您要為從群組中選取的裝置建立規則，請前往群組工作區，在**裝置**頁籤選取裝置，然後執行以下操作：
     a. 開啟所選裝置的內容視窗。
     b. 在裝置內容視窗的**應用程式**區域中，選取網路代理。
     c. 開啟網路代理內容視窗。
3. 在開啟的**內容**視窗中，在**連線**區域中，選取**連線設定檔**子區域。

4. 在**網路位置設定**區域，點擊**新增**按鈕。

5. 在開啟的**新敘述**視窗中，設定網路位置敘述和轉換規則。指定以下網路位置敘述設定：

   - **網路位置敘述名稱**

     網路位置敘述名稱不能超過 255 字元或包含特殊字元，例如 ("*<>?\/:|)。

   - **使用連線設定檔**

     在該下拉清單中，您可以指定網路代理用於連線至管理伺服器的連線設定檔。該設定檔將在網路位置敘述條件被滿足時使用。連線設定檔包含網路代理連線到管理伺服器的設定；它還定義了用戶端裝置轉換到漫遊政策的時間。設定檔僅用於下載更新。

6. 在**轉換條件**區域中，點擊**新增**按鈕建立網路位置敘述條件清單。

   使用邏輯運算子 AND 可組合規則中的條件。要基於網路位置敘述觸發切換規則，必須滿足所有規則切換條件。

7. 在下拉清單中，選取與用戶端裝置連線到的網路特徵變化相對應的值：

   - **預設連線閘道位址**—主要網路閘道的位址已變更。
   - **DHCP 伺服器位址**—網路 Dynamic Host Configuration Protocol (DHCP) 伺服器的 IP 位址已變更。
   - **DNS 網域**—子網路的 DNS 後置詞已變更。
   - **DNS 伺服器位址**—網路 DNS 伺服器的 IP 位址已變更。
   - **Windows 網域可存取性（僅限 Windows）**—可變更用戶端裝置連線到的 Windows 網域的狀態。僅對執行 Windows 的裝置使用此設定。
   - **子網路**—可變更子網路位址和遮罩。
   - **WINS 伺服器位址（僅限 Windows）**—網路 WINS 伺服器的 IP 位址已變更。僅對執行 Windows 的裝置使用此設定。
   - **名稱可解析性** — 用戶端裝置的 DNS 或 NetBIOS 名稱已更改。
   - **SSL 連線位址可存取性**—用戶端裝置可以或無法（取決於您選取的選項）與指定伺服器（名稱：連接埠）建立 SSL 連線。對於每個伺服器，您還可以指定 SSL 憑證。在這種情況下，除了檢查 SSL 連線的功能之外，網路代理還會驗證伺服器憑證。如果憑證不相符，則連線會失敗。連線頻率為每分鐘一次。

8. 在開啟的視窗中，指定網路代理轉換到其他管理伺服器的條件值。視窗的名稱取決於先前步驟中選取的值。指定轉換條件的以下設定：

- **參數值**

  在該欄位中，您可以為所建立的條件新增一個或多個值。

- **至少符合清單中的一個參數值**

  如果選中該選項，只要符合**參數值**清單中指定的任何值就會滿足條件。

  預設情況下已選定此選項。

- **不符合清單中的任意參數值**

  如果選中該選項，**參數值**清單中不存在條件的值，則滿足條件。

9. 在**新敘述**視窗，選取**敘述已啟用**選項來啟用新網路位置的敘述。

會建立網路位置敘述的新切換規則；當滿足其條件時，網路代理將使用此規則指定的設定檔連線至管理伺服器。

系統將依據它們在清單中出現的順序檢視是否有與網路佈局相比對的網路位置敘述。如果某個網路有多個比對的敘述，將使用第一個。您可以使用**向上**按鈕 ( ) 和**向下**按鈕 ( ) 變更清單中的規則順序。

使用 TLS 的加密通信

要修復您組織企業網路中的弱點，您可以使用 TLS 協定啟用流量加密。您可以在管理伺服器和 iOS MDM 伺服器上啟用 TLS 加密協定和受支持的密碼套裝。卡巴斯基安全管理中心支援 TLS 協定版本 1.0、1.1 和 1.2。您可以選取所需的加密協定和加密套裝。

卡巴斯基安全管理中心使用自簽發憑證。不需要 iOS 裝置的附加設定。您也可以使用您自己的憑證。Kaspersky 專家建議使用由受信任憑證當局發佈的憑證。

要在管理伺服器上設定允許的加密協議和加密套件：

1. 使用管理員權限執行 Windows 命令提示符，然後將目前目錄變更為包含 klscflag 公用程式的目錄。klscflag 公用程式位於安裝管理伺服器的資料夾中。預設安裝路徑：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. 使用 SrvUseStrictSslSettings 旗標在管理伺服器上設定允許的加密協議和加密套件。請在 Windows 命令提示符下輸入以下命令：

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <值> -t d
   ```

   指定 SrvUseStrictSslSettings 旗標的<value>參數：

   - 4 — 僅啟用 TLS 1.2 協定。此外，還啟用了具有 TLS_RSA_WITH_AES_256_GCM_SHA384 的密碼套裝（需要該密碼套裝才能向後相容卡巴斯基安全管理中心 11）。這是預設值。

     TLS 1.2 協定支援的密碼套裝：

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - AES256-GCM-SHA384（具有 TLS_RSA_WITH_AES_256_GCM_SHA384 的密碼套裝）
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

   - 5 — 僅啟用 TLS 1.2 協定。對於 TLS 1.2 協定，下面列出的特定密碼套裝受支援。

     TLS 1.2 協定支援的密碼套裝：

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

   我們不建議使用 0、1、2 或 3 作為 SrvUseStrictSslSettings 標誌的參數值。這些參數值對應於不安全的 TLS 協定版本（TLS 1.0 和 TLS 1.1 協定）和不安全的密碼套裝，僅用於向後相容早期的卡巴斯基安全管理中心版本。

3. 重新啟動以下卡巴斯基安全管理中心 14.2 服務：

   - 管理伺服器
   - 網頁伺服器

- 啟動代理

iOS MDM 伺服器

iOS 裝置和 iOS MDM 伺服器之間的連線預設被加密。

要在 iOS MDM 伺服器上設定允許的加密協議和加密套件：

1. 開啟安裝了 iOS MDM 伺服器的用戶端裝置的登錄檔（例如，在**開始** → **執行**功能表使用 regedit 指令）。
2. 轉至以下分支：
   - 對於 32 位元系統：
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Cor
   - 對於 64 位元系統：
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSI
3. 建立名為 `StrictSslSettings` 的鍵。
4. 指定 `DWORD` 作為鍵類型。
5. 設定鍵值：
   - 2 — 啟用 TLS 1.0、TLS 1.1 和 TLS 1.2 協定。
   - 3 — 僅啟用 TLS 1.2 協定（預設值）。
6. 重新啟動卡巴斯基安全管理中心 iOS MDM 伺服器服務。

事件通知

該部分敘述如何選取方法傳送關於用戶端裝置上的事件的管理員通知，以及如何配置事件通知設定。

它也敘述了如何使用 Eicar 測試病毒測試事件通知的分發。

設定事件通知

卡巴斯基安全管理中心允許您設定將用戶端裝置上發生的事件通知管理員的方法，並允許您設定通知：

- 電子郵件。當發生事件時，程式將向指定的電子郵件信箱傳送通知。您可以編輯通知文字。
- SMS。當發生事件時，程式將向指定的電話號碼傳送通知。您可以配置 SMS 通知以便透過郵件閘道傳送。
- 可執行檔。當裝置上發生事件時，將在管理員工作站上啟動該可執行檔。管理員可以透過該可執行檔接收已發生事件參數。

要設定關於用戶端電腦上已發生事件的通知，請執行以下操作：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。
2. 在節點工作區中，選取**事件**頁籤。
3. 點擊**配置通知和事件匯出**連結並在下拉清單中選取**配置通知**值。
   這會開啟**內容：事件**視窗。

4. 在**通知**區域，選取通知方法（透過郵件、SMS或者執行可執行檔）並定義通知設定：

- **電子郵件**

電子郵件頁籤允許您透過電子郵件配置事件通知。

在**收件者（電子郵件信箱）**欄位，指定應用程式傳送通知的電子郵件信箱。您可以在該欄位指定多個位址，以分號分隔。

在 **SMTP 伺服器**欄位，指定郵件伺服器位址，以分號分隔。您可以使用以下參數：

- IPv4 或 IPv6 位址
- 裝置的 Windows 網路名稱（NetBIOS 名稱）
- SMTP 伺服器的 DNS 名稱

在 **SMTP 伺服器連接埠**欄位，指定 SMTP 伺服器通訊埠號。預設埠號為 25。

如果您啟用**使用 DNS MX 尋找**選項，您可以將 IP 位址的多個 MX 記錄用於 SMTP 伺服器的相同 DNS 名稱。相同 DNS 名稱可能有幾個 MX 記錄，具有不同的接收電子郵件的優先次序。管理伺服器嘗試按 MX 記錄優先次序向 SMTP 伺服器傳送電子郵件通知。預設情況下已停用該選項。

如果您啟用**使用 DNS MX 尋找**選項並且不啟用 TLS 設定的使用，我們建議您使用伺服器裝置上的 DNSSEC 設定作為傳送電子郵件通知的額外防護措施。

按一下**設定**用於定義其他通知設定的連結：

- 主旨名稱（電子郵件的主旨名稱）
- 寄件者電子郵件地址
- ESMTP 身分驗證設定

如果為 SMTP 伺服器啟用了 ESMTP 身分驗證選項，則必須在 SMTP 伺服器上指定帳戶進行身分驗證。

- SMTP 伺服器的 TLS 設定：
  - **請勿使用 TLS**

    如果您想停用電子郵件訊息加密，您可以選取此選項。

  - **如果 SMTP 伺服器支援，請使用 TLS**

    如果要使用 TLS 連線到 SMTP 伺服器，則可以選取此選項。如果 SMTP 伺服器不支援 TLS，管理伺服器將不使用 TLS 連線 SMTP 伺服器。

  - **始終使用 TLS，檢查伺服器憑證的有效性**

    如果要使用 TLS 身分驗證設定，則可以選取此選項。如果 SMTP 伺服器不支援 TLS，管理伺服器將無法連線 SMTP 伺服器。

我們建議您使用此選項以更好地防護與 SMTP 伺服器的連線。如果選取此選項，則可以為 TLS 連線設定身分驗證設定。

如果您選擇"**始終使用 TLS，檢查伺服器憑證的有效性**"值，則可以指定用於驗證 SMTP 伺服器的憑證，並選取是要透過任何版本的 TLS，還是僅透過 TLS 1.2 或更高版本啟用通訊。此外，您可以指定在 SMTP 伺服器上進行用戶端身分驗證的憑證。

您可以為 SMTP 伺服器指定 TLS 設定：

- 瀏覽 SMTP 伺服器憑證檔案：

您可以從受信任的憑證頒發機構接收帶有憑證清單的檔案，然後將該檔案上傳到管理伺服器。卡巴斯基安全管理中心會檢查 SMTP 伺服器的憑證是否也由受信任的憑證頒發機構簽署。如果未從受信任的憑證頒發機構收到 SMTP 伺服器的憑證，卡巴斯基安全管理中心將無法連線到 SMTP 伺服器。

- 瀏覽用戶端憑證檔案：

您可以使用從任何來源（例如，從任何受信任的憑證頒發機構）收到的憑證。您必須使用以下憑證類型之一指定憑證及其私密金鑰：

- X-509 憑證：

您必須指定一個帶有憑證的檔案和一個帶有私密金鑰的檔案。這兩個檔案互不相依，檔案的載入順序並不重要。當同時載入兩個檔案時，您必須指定用於解碼私密金鑰的密碼。如果未編碼私密金鑰未編碼，則密碼可以為空值。

- pkcs12 容器：

您必須上傳包含憑證及其私密金鑰的單一檔案。載入檔案後，您必須指定用於解碼私密金鑰的密碼。如果未編碼私密金鑰未編碼，則密碼可以為空值。

通知訊息欄位包含事件發生時應用程式傳送的事件資訊標準文字。該文字包含替代參數，例如事件名稱、裝置名稱和網域名稱。您可以新增有事件相關詳情的其他更新替代參數來編輯訊息文字。替代參數的清單可點擊欄位右方的按鈕取得。

如果通知文字包含百分號 (%) 字元，您必須指定兩次以允許訊息傳送。範例，“CPU 負載是 100%%”。

點擊**設定通知限制數**連結指定應用程式在指定時段內可以傳送的最大通知數量。

按一下**傳送測試訊息**按鈕以檢查您是否已正確配置通知。該應用程式應向您指定的電子郵件位址傳送測試通知。

- SMS

SMS 頁籤可讓您設定將各種事件的 SMS 通知傳到手機。SMS 訊息透過郵件閘道傳送。

在**收件者（電子郵件信箱）**欄位，指定應用程式傳送通知的電子郵件信箱。您可以在該欄位指定多個位址，以分號分隔。通知將被傳送到指定郵件信箱關聯的電話號碼。

在 **SMTP 伺服器**欄位，指定郵件伺服器位址，以分號分隔。您可以使用以下參數：

- IPv4 或 IPv6 位址
- 裝置的 Windows 網路名稱（NetBIOS 名稱）
- SMTP 伺服器的 DNS 名稱

在 **SMTP 伺服器連接埠**欄位，指定 SMTP 伺服器通訊埠號。預設埠號為 25。

按一下**設定**用於定義其他通知設定的連結：

- 主旨名稱（電子郵件的主旨名稱）
- 寄件者電子郵件地址
- ESMTP 身分驗證設定

如有必要，如果 SMTP 伺服器啟用了 ESMTP 身分驗證選項，您可以在 SMTP 伺服器上指定一個帳戶進行身分驗證。

- 適用於 SMTP 伺服器的 TLS 設定

您可以停用 TLS 的使用，如果 SMTP 伺服器支援此協議，則使用 TLS，或者您可以強制僅使用 TLS。如果您選取僅使用 TLS，您可以指定用於驗證 SMTP 伺服器的憑證，並選取是要透過任何版本的 TLS，還是僅透過 TLS 1.2 或更高版本啟用通訊。此外，如果您選取僅使用 TLS，您可以為 SMTP 伺服器上的用戶端身分驗證指定憑證。

- 瀏覽 SMTP 伺服器憑證檔案

您可以從受信任的憑證頒發機構接收帶有憑證清單的檔案，然後將該檔案上傳到卡巴斯基安全管理中心。卡巴斯基安全管理中心會檢查 SMTP 伺服器的憑證是否也由受信任的憑證頒發機構簽署。如果未從受信任的憑證頒發機構收到 SMTP 伺服器的憑證，卡巴斯基安全管理中心將無法連線到 SMTP 伺服器。

您必須上傳包含憑證及其私密金鑰的單一檔案。載入檔案後，您必須指定用於解碼私密金鑰的密碼。如果私密金鑰未編碼，則密碼可以為空值。**通知訊息**欄位包含標準文字，其中包含有關事件發生時應用程式傳送的事件的資訊。該文字包含替代參數，例如事件名稱、裝置名稱和網域名稱。您可以新增有事件相關詳情的其他更新替代參數來編輯訊息文字。替代參數的清單可點擊欄位右方的按鈕取得。

如果通知文字包含百分號 (%) 字元，您必須指定兩次以允許訊息傳送。範例，“CPU 負載是 100%%”。

按一下**設定通知限制數**連結以指定應用程式在指定時間段可以傳送的最大通知數量（通知數量 / 分鐘數）。

點擊**“傳送測試訊息”**按鈕檢查您是否正確配置了通知。該應用程式應向您指定的收件人傳送測試通知。

- **要執行的可執行檔**

如果選取該通知方法，您可以在輸入欄位指定事件發生時要啟動的應用程式。

點擊**設定通知限制數**連結允許您指定應用程式在指定時間段可以傳送的最大通知數量（通知數量 / 分鐘數）。

點擊**傳送測試訊息**按鈕允許您檢查您是否正確配置了通知：應用程式傳送測試通知到您指定的郵件信箱。

5. 在**通知訊息**欄位中，輸入事件發生時程式要傳送的文字。

   您可以使用文字欄位右邊的下拉清單來新增事件詳情的替代設定（例如，事件敘述、發生事件等等）。

   如果通知文字包含 % 字元，您必須指定兩次以允許訊息傳送。範例，“CPU 負載是 100%”。

6. 點擊**傳送測試訊息**按鈕以檢查通知是否已成功設定。

   程式傳送測試通知到指定使用者。

7. 點擊**確定**儲存變更。

經過調整的通知設定將應用於用戶端裝置上發生的所有事件。

您可在管理伺服器設定、隱私設定或應用程式設定的**事件配置**區域覆寫特定事件的通知設定。

測試通知

為了檢查事件通知是否可以傳送,程式將在用戶端裝置上使用 Eicar 測試“病毒偵”測通知。

要驗證事件通知的傳送，請執行以下操作：

1. 停止用戶端裝置上的即時檔案系統防護工作，將 EICAR 測試“病毒”複製到用戶端裝置。現在重新啟用檔案系統的即時防護。

2. 為管理群組中的用戶端裝置或指定裝置執行掃描工作，包括帶有 EICAR“病毒”的裝置。

   如果掃描工作設定正確，會偵測到測試“病毒”。如果通知設定正確，您將收到偵測到病毒的通知。

   在**管理伺服器**節點工作區的**事件**頁籤，**最近事件**分類會顯示偵測到的「病毒」記錄。

EICAR 測試“病毒”不包含任何危害您裝置的代碼。不過，多數廠商的安全應用程式都將該檔案視為病毒。您可以從 EICAR 官方網站 下載該測試“病毒”。

透過執行可執行檔顯示的事件通知

卡巴斯基安全管理中心可透過執行可執行檔將用戶端裝置上發生的事件通知管理員。可執行檔必須包含另外一個可執行檔，而後者具有要轉發給管理員的事件的佔位符（請參見下表）。

敘述事件的佔位符

佔位符	佔位符敘述
%SEVERITY%	事件嚴重等級。可能的值： • **資訊** • **警告** • **錯誤** • **緊急**
%COMPUTER%	發生事件的裝置的名稱。 裝置名稱的最大長度為 256 個字元。
%DOMAIN%	發生事件的裝置的網域名稱。

佔位符	佔位符敘述
%EVENT%	事件類型的名稱。 事件類型名稱的最大長度為 50 個字元。
%DESCR%	事件敘述。 敘述的最大長度為 1000 個字元。
%RISE_TIME%	事件建立時間。
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	工作名稱。 工作名稱的最大長度為 100 個字元。
%KL_PRODUCT%	應用程式名稱。
%KL_VERSION%	應用程式版本號。
%KLCSAK_EVENT_SEVERITY_NUM%	事件嚴重性編號。可能的值： • 1—**資訊** • 2—**警告** • 3—**錯誤** • 4—**緊急**
%HOST_IP%	發生事件的裝置的 IP 位址。
%HOST_CONN_IP%	發生事件的裝置的連線 IP。

例如：
事件通知由某個可執行檔（例如，script1.bat）發出，在該可執行檔中，將啟動具有 %COMPUTER% 佔位符的另一個可執行檔（例如，script2.bat）。當發生事件時，將在管理員的裝置上執行 script1.bat 檔案，而該檔案隨後執行具有 %COMPUTER% 佔位符的 script2.bat 檔案。管理員將接收到發生事件的裝置的名稱。

設定介面

您可設定卡巴斯基安全管理中心介面：

- 根據使用的功能，顯示並隱藏主控台樹狀目錄、工作空間以及物件的內容視窗（資料夾、區段）。
- 顯示和隱藏主視窗的元素（例如主控台樹狀目錄或標準選單，例如**操作**和**檢視**）。

若要根據目前使用的功能集設定卡巴斯基安全管理中心介面：

1. 在主控台樹狀目錄中，選取**管理伺服器**節點。
2. 在主應用程式視窗的選單列，選取**檢視 → 配置介面**。

3. 在開啟的**配置介面**視窗中，使用以下核取方塊設定介面元素的顯示：

- **顯示弱點和修補程式管理**

  若已選取此核取方塊，則**遠端安裝**資料夾會顯示**佈署裝置映像**子資料夾，以及**儲存區**資料夾會顯示**硬體**子資料夾。

  若未完成快速啟動精靈，依預設會取消選取此核取方塊。完成快速啟動精靈後，依預設會選取此核取方塊。

  如果停用此選項，即使您擁有**系統管理產品授權，建立 RDP 連線**「建立 RDP 工作階段」**Windows 共用桌面**「Windows 桌面共用」也將無法使用。

- **顯示資料加密與防護**

  若啟用此選項，主控台樹狀目錄會顯示**資料加密與防護**資料夾。

  預設情況下已啟用該選項。

- **顯示端點控制設定**

  若啟用此選項，以下子區段會顯示在 Kaspersky Endpoint Security for Windows 政策內容視窗的**安全控制**區段：

  - **應用程式控制**
  - **裝置控制**
  - **Web 控制**
  - **自適應異常控制**

  若停用此選項，這些指定的子區段不會顯示在**安全控制**區段。

  預設情況下已啟用該選項。

- **顯示行動裝置管理**

  若啟用此選項，則可使用**行動裝置管理**功能。若重新啟動應用程式，主控台樹狀目錄會顯示**行動裝置**資料夾。

  預設情況下已啟用該選項。

- **顯示從屬管理伺服器**

  若選取該核取方塊，主控台樹狀目錄會顯示管理群組中從屬與虛擬管理伺服器。與從屬與虛擬管理伺服器連線的功能—例如，建立從屬管理伺服器遠端安裝應用程式的工作—可以該方式提供使用。

  預設情況下已清空此方塊。

- **顯示安全設定區段**

若啟用此選項，**安全性**區段會顯示在管理伺服器、管理群組與其他物件的內容視窗。此選項可讓您提供使用者與使用者群組使用物件的自訂權限。

預設情況下已停用該選項。

4. 點擊**"確定"**。

若要套用部分變更，您需關閉主應用程式視窗並再次將其開啟。

若要設定在主應用程式視窗的元素顯示：

1. 在主應用程式視窗的選單列中，選取**檢視 → 配置**。
2. 在開啟的**配置檢視**視窗中，設定使用核取方塊的主視窗元素顯示。
3. 點擊**"確定"**。

發現網路裝置

該部分敘述了安裝卡巴斯基安全管理中心後必須採取的操作。

情境：發現網路裝置

您必須在安裝安全應用程式之前執行裝置發現。管理伺服器接收有關已發現裝置的資訊，並允許您通過政策管理這些裝置。需要定期進行網路輪詢以更新網路中可用裝置的清單。

在開始網路輪詢之前，請確保已啟用 SMB 協定。否則，卡巴斯基安全管理中心將無法發現輪詢網路中的裝置。要啟用 SMB 協定，請按照您的作業系統的說明進行操作。

網路裝置探索按以下階段進行：

1. **探索裝置**

   快速啟動精靈透過初始裝置發現指引您，並幫助您尋找網路裝置，例如電腦、平板電腦和行動電話。您也可以手動執行裝置發現。

2. **設定排程輪詢**

   決定您要定期使用哪些輪詢類型。啟用所需的類型並設定輪詢排程。您可以參考網路輪詢頻率建議。

3. **設定規則以新增發現的裝置到管理群組（可選）**

   如果新裝置出現在您的網路，它們會在常規輪詢中被發現並被自動包含在**未配置的裝置**群組。您可以設定裝置移動規則以自動分配裝置到**受管理裝置**群組。您也可以設定保留規則。

   如果跳過步驟 3，新發現的裝置將被分配給**未配置的裝置**群組。如果您想，您可以手動移動這些裝置到**受管理裝置**群組。如果您手動移動這些裝置到**受管理裝置**群組，您可以分析每部裝置的資訊，並決定您是否要移動它到管理群組以及移動到具體哪個群組。

結果

完成情境可以導致如下：

- 卡巴斯基安全管理中心管理伺服器發現網路中的裝置並提供您它們的資訊。
- 未來輪詢被設定並根據指定的排程工作。
- 新發現的裝置按照配置的規則進行排列。（或者，如果未配置規則，裝置將保留在**未配置的裝置**群組中）。

未配置的裝置

本章節介紹如何管理企業網路中未包含在管理群組中的裝置。

裝置發現

該部分敘述了卡巴斯基安全管理中心中可用的裝置發現類型並給出使用每種類型的資訊。

管理伺服器透過一般輪詢接收網路結構資訊和網路裝置資訊。資訊被記錄到管理伺服器資料庫。管理伺服器可使用下列類型的輪詢：

- **Windows 網路輪詢**。管理伺服器可以執行兩種 Windows 網路輪詢：快速和完整。在快速輪詢過程中，管理伺服器只會從所有網域和工作群組中裝置的 NetBIOS 名稱清單獲取資訊。在完整輪詢中，需要每台用戶端裝置的更多資訊，例如作業系統名稱、IP 位址、DNS 名稱和 NetBIOS 名稱。預設下，快速和完整輪詢都被啟用。Windows 網路輪詢可能發現裝置失敗，例如，如果連接埠 UDP 137、UDP 138、TCP 139 在路由器上或被防火牆關閉。
- **Active Directory 輪詢**。管理伺服器接收 Active Directory 單元結構以及 Active Directory 群組中裝置的 DNS 名稱的資訊。預設情況下已啟用該輪詢類型。如果您使用 Active Directory，我們建議您使用 Active Directory 輪詢；否則，管理伺服器不發現任何裝置。如果您使用 Active Directory 但是一些網路裝置不列為成員，這些裝置無法透過 Active Directory 輪詢發現。
- **IP 範圍輪詢**。管理伺服器將使用 ICMP 封包或 NBNS 通訊協定輪詢指定的 IP 範圍，並收集 IP 範圍內裝置上的一組完整資料。預設情況下已停用該輪詢類型。如果您使用 Windows 網路輪詢和/或 Active Directory 輪詢，不建議您使用該輪詢類型。
- **Zeroconf 輪詢**。透過使用零配置網路（也稱為*零配置*）輪詢 IPv6 網路的發佈點。預設情況下已停用該輪詢類型。如果發佈點執行 Linux，您可以使用 Zeroconf 輪詢。

如果您設定和啟用了裝置移動規則，新發現的裝置會自動包含在**受管理裝置**群組中。如果未啟用移動規則，新發現的裝置被自動包含在**未配置的裝置**群組。

您可以為每種類型修改裝置發現設定。例如，您可能想要修改輪詢排程或者設定是否輪詢整個 Active Directory 樹系還是僅指定網域。

在開始網路輪詢之前，請確保已啟用 SMB 協定。否則，卡巴斯基安全管理中心將無法發現輪詢網路中的裝置。要啟用 SMB 協定，請按照您的作業系統的說明進行操作。

Windows 網路輪詢

關於 Windows 網路輪詢

在快速輪詢過程中，管理伺服器只會從所有網域和工作群組中裝置的 NetBIOS 名稱清單獲取資訊。在完整輪詢中，以下資訊被從每個用戶端裝置請求：

- 作業系統名稱
- IP 位址
- DNS 名稱
- NetBIOS 名稱

快速輪詢和完整輪詢都需要以下：

- 連接埠 UDP 137/138、TCP 139、UDP 445、TCP 445 必須在網路中可用。
- SMB 協定已啟用。
- 必須使用 Microsoft Computer Browser 服務，且主瀏覽器電腦必須在管理伺服器上啟用。
- 必須使用 Microsoft Computer Browser 服務，且主瀏覽器電腦必須在用戶端裝置上啟用。
    - 至少一台裝置上，如果網路裝置數量不超過 32。
    - 對每 32 台網路裝置至少一台裝置上。

完整輪詢僅在快速輪詢至少執行了一次時可以執行。

檢視和修改 Windows 網路輪詢設定

要修改 Windows 網路輪詢的設定，請執行以下操作：

1. 在主控台樹狀目錄中的**裝置發現**資料夾，選取**網域** 子資料夾。

   透過點擊**立即輪詢**按鈕，您可從**未配置的裝置**資料夾繼續前往**裝置發現**資料夾。

   在**網域**子資料夾的工作區中會顯示裝置清單。

2. 點擊**立即輪詢**。

   網域內容視窗將開啟。如果您想，修改 Windows 網路輪詢設定：

   - **啟用 Windows 網路輪詢**

     預設情況下已選取此選項。如果您不想執行 Windows 網路輪詢（例如，如果您認為 Active Directory 輪詢已足夠），您可以清空該選項。

   - **設定快速輪詢排程**

預設期間是 15 分鐘。

在快速輪詢過程中，管理伺服器只會從所有網域和工作群組中裝置的 NetBIOS 名稱清單獲取資訊。

下次輪詢接收的資料取代舊資料。

有以下輪詢排程選項可用：

- **每 N 天**

  輪詢定期執行，按照指定天數間隔，從指定的日期和時間開始。

  預設下，輪詢每天執行一次，從目前系統日期和時間開始。

- **每 N 分鐘**

  輪詢定期執行，按照指定分鐘間隔，從指定的時間開始。

  預設下，輪詢每五分鐘執行一次，從目前系統時間開始。

- **按每星期中的指定日**

  輪詢定期執行，在指定星期的指定時間。

  預設下，輪詢會每週五下午 6:00:00 執行。

- **每個月在所選週的指定天**

  輪詢定期執行，在指定月日的指定時間。

  預設下，未選取月日；預設啟動時間是 6:00:00 P.M.。

- **執行錯過的工作**

  如果在排程輪詢期間管理伺服器被切換掉或不可用，管理伺服器可以在切換回來後立即啟動輪詢，或者等待下次排程輪詢。

  如果啟用該選項，管理伺服器在它切換回來後立即啟動輪詢。

  如果停用該選項，管理伺服器等待下一次排程輪詢。

  預設情況下已啟用該選項。

- **設定完整輪詢排程**

預設間隔是一小時。下次輪詢接收的資料取代舊資料。

有以下輪詢排程選項可用：

- **每 N 天**

  輪詢定期執行，按照指定天數間隔，從指定的日期和時間開始。

  預設下，輪詢每天執行一次，從目前系統日期和時間開始。

- **每 N 分鐘**

  輪詢定期執行，按照指定分鐘間隔，從指定的時間開始。

  預設下，輪詢每五分鐘執行一次，從目前系統時間開始。

- **按每星期中的指定日**

  輪詢定期執行，在指定星期的指定時間。

  預設下，輪詢會每週五下午 6:00:00 執行。

- **每個月在所選週的指定天**

  輪詢定期執行，在指定月日的指定時間。

  預設下，未選取月日；預設啟動時間是 6:00:00 P.M.。

- **執行錯過的工作**

  如果在排程輪詢期間管理伺服器被切換掉或不可用，管理伺服器可以在切換回來後立即啟動輪詢，或者等待下次排程輪詢。

  如果啟用該選項，管理伺服器在它切換回來後立即啟動輪詢。

  如果停用該選項，管理伺服器等待下一次排程輪詢。

  預設情況下已啟用該選項。

如果您要立即執行輪詢，點擊**立即輪詢**。兩種輪詢將啟動。

在虛擬管理伺服器上，可以在**裝置發現**區域中發佈點的內容視窗中檢視和編輯輪詢 Windows 網路的設定。

Active Directory 輪詢

如果您使用 Active Directory 則使用 Active Directory 輪詢；否則，建議使用其他類型的輪詢。如果您使用 Active Directory 但是一些網路裝置不列為成員，這些裝置無法透過 Active Directory 輪詢發現。

無論後續輪詢的結果為何，Active Directory 輪詢結果都會儲存在管理伺服器上 30 天。

在開始網路輪詢之前，請確保已啟用 SMB 協定。否則，卡巴斯基安全管理中心將無法發現輪詢網路中的裝置。要啟用 SMB 協定，請按照您的作業系統的說明進行操作。

瀏覽和修改 Active Directory 輪詢設定

要檢視和修改 Active Directory 群組的輪詢設定，請執行以下操作：

1. 在主控台樹狀目錄中的**裝置發現**資料夾中，選取**Active Directory**子資料夾。

   或者，您可透過點擊**立即輪詢**按鈕從**未配置的裝置**資料夾輪詢至**裝置發現**資料夾。

2. 點擊**設定輪詢**。

   Active Directory 內容視窗開啟。如果您想，修改 Active Directory 輪詢設定：

   - **啟用 Active Directory 輪詢**

     預設情況下已選取此選項。然而，如果您不使用 Active Directory，輪詢不獲取任何結果。此種情況下，您可以清空該選項。

   - **設定輪詢排程**

預設間隔是一小時。

有以下輪詢排程選項可用：

- **每 N 天**

  輪詢定期執行，按照指定天數間隔，從指定的日期和時間開始。

  預設下，輪詢每天執行一次，從目前系統日期和時間開始。

- **每 N 分鐘**

  輪詢定期執行，按照指定分鐘間隔，從指定的時間開始。

  預設下，輪詢每五分鐘執行一次，從目前系統時間開始。

- **按每星期中的指定日**

  輪詢定期執行，在指定星期的指定時間。

  預設下，輪詢會每週五下午 6:00:00 執行。

- **每個月在所選週的指定天**

  輪詢定期執行，在指定月日的指定時間。

  預設下，未選取月日；預設啟動時間是 6:00:00 P.M.。

- **執行錯過的工作**

  如果在排程輪詢期間管理伺服器被切換掉或不可用，管理伺服器可以在切換回來後立即啟動輪詢，或者等待下次排程輪詢。

  如果啟用該選項，管理伺服器在它切換回來後立即啟動輪詢。

  如果停用該選項，管理伺服器等待下一次排程輪詢。

  預設情況下已啟用該選項。

- **進階**

您可以選取要輪詢的 Active Directory 網域：

- 卡巴斯基安全管理中心所屬的 Active Directory 網域
- 卡巴斯基安全管理中心所屬的網域樹系。
- Active Directory 網域的指定清單。
  如果您選取該選項，您可以新增域到輪詢範圍：
  - 點擊**"新增"**按鈕。
  - 在對應的欄位，指定網域控制站位址、存取它的帳戶名稱和密碼。
  - 按一下**確定**以儲存變更。

  您可以在清單上選取網域控制站位址並按一下**修改**或**移除**按鈕以修改或移除它。
- 按一下**確定**以儲存變更。

如果您要立即執行輪詢，請點擊**立即輪詢**按鈕。

在虛擬管理伺服器上，您可以在**裝置發現**區域中，於發佈點的內容視窗內，檢視和編輯輪詢 Windows 網路的設定。

IP 範圍輪詢

管理伺服器將使用 ICMP 封包或 NBNS 通訊協定輪詢指定的 IP 範圍，並收集 IP 範圍內裝置上的一組完整資料。預設情況下已停用該輪詢類型。

對於 Microsoft Active Directory 或 Samba 網域控制器內的所有基於 Linux 的主機，請在`netbios name`檔案中指定`workgroup` 和 `/etc/samba/smb.conf`參數。否則，輪詢結果可能包含重複的主機。

在開始網路輪詢之前，請確保已啟用 SMB 協定。否則，卡巴斯基安全管理中心將無法發現輪詢網路中的裝置。要啟用 SMB 協定，請按照您的作業系統的說明進行操作。

瀏覽和修改 IP 範圍輪詢設定

要檢視和修改 IP 範圍群組的輪詢設定，請執行以下操作：

1. 在主控台樹狀目錄中的**裝置發現**資料夾，選取**IP 範圍**子資料夾。

   透過點擊**立即輪詢**按鈕，從**未配置的裝置**資料夾繼續前往**裝置發現**資料夾。

2. 如果您要前往，請在 **IP 範圍**子資料夾點擊**新增子網路**來新增輪詢的 IP 範圍，然後點擊**確定**。

3. 點擊**設定輪詢**。

   IP 範圍內容視窗將開啟。如果您想，您可以修改 IP 範圍輪詢的設定：

   - **啟用 IP 範圍輪詢**

     預設情況下不選中該選項。如果您使用 Windows 網路輪詢和/或 Active Directory 輪詢，不建議您使用該輪詢類型。

   - **設定輪詢排程**

預設期間是 420 分鐘。下次輪詢接收的資料取代舊資料。

有以下輪詢排程選項可用：

- **每 N 天**

  輪詢定期執行，按照指定天數間隔，從指定的日期和時間開始。

  預設下，輪詢每天執行一次，從目前系統日期和時間開始。

- **每 N 分鐘**

  輪詢定期執行，按照指定分鐘間隔，從指定的時間開始。

  預設下，輪詢每五分鐘執行一次，從目前系統時間開始。

- **按每星期中的指定日**

  輪詢定期執行，在指定星期的指定時間。

  預設下，輪詢會每週五下午 6:00:00 執行。

- **每個月在所選週的指定天**

  輪詢定期執行，在指定月日的指定時間。

  預設下，未選取月日；預設啟動時間是 6:00:00 P.M.。

- **執行錯過的工作**

  如果在排程輪詢期間管理伺服器被切換掉或不可用，管理伺服器可以在切換回來後立即啟動輪詢，或者等待下次排程輪詢。

  如果啟用該選項，管理伺服器在它切換回來後立即啟動輪詢。

  如果停用該選項，管理伺服器等待下一次排程輪詢。

  預設情況下已啟用該選項。

如果您要立即執行輪詢，點擊**立即輪詢**。此按鈕僅在您選取**啟用 IP 範圍輪詢**時可用。

在虛擬管理伺服器上，您可在發佈點內容視窗的**裝置發現**區域中檢視並編輯 IP 範圍輪詢的設定。在輪詢 IP 範圍期間發現的用戶端電腦會顯示在虛擬管理伺服器的**網域**資料夾中。

Zeroconf 輪詢

僅基於 Linux 的分發點支援此輪詢類型。

分發點可以輪詢具有 IPv6 位址的裝置的網路。在這種情況下，不會指定 IP 範圍，分發點將使用以下零配置網路（稱為“*零配置*”）輪詢整個網路 。要開始使用 Zeroconf，您必須在分發點上安裝 avahi-browse 公用程式。

要啟用 Zeroconf 輪詢：

1. 在主控台樹狀目錄中的**裝置發現**資料夾，選取**IP 範圍**子資料夾。
   透過點擊**立即輪詢**按鈕，從**未配置的裝置**資料夾繼續前往**裝置發現**資料夾。
2. 點擊**設定輪詢**。
3. 在開啟的 IP 範圍內容視窗中，選擇 **啟用輪詢與 Zeroconf 技術**。

之後，分發點開始輪詢您的網路。在這種情況下，指定的 IP 範圍將被忽略。

使用視窗網域。瀏覽和變更網域設定

要修改網域設定，請執行以下操作：

1. 在主控台樹狀目錄中的**裝置發現**資料夾，選取**網域** 子資料夾。
2. 以下列方式之一選取一個網域並開啟其內容視窗：
   - 從網域的上下文功能表中選取**"內容"**。
   - 透過點擊**顯示群組內容**連結。

內容：<網域名稱>視窗將開啟，您可以在其中設定所選網域。

為未配置的裝置配置保留規則

Windows 網路輪詢完成後，發現的裝置被放置到"未配置的裝置"管理群組的子群組。該管理群組可以在**進階 → 裝置發現 → 網域**中取得。**網域**資料夾是父群組。它包含以對應域為名稱的子群組和在網路輪詢過程中發現的工作群組。父群組可能也包含行動裝置管理群組。您可以為父群組和每個子群組配置未配置的裝置的保留規則。保留規則不取決於網路輪詢設定並在網路輪詢被停用時也工作。

要為未配置的裝置設定保留規則：

1. 在主控台樹狀目錄中的**裝置發現**資料夾，進行以下其中一個操作：

   - 若要配置父群組設定，右擊**網域**子資料夾並選取**內容**。
     父群組內容視窗將開啟。
   - 要設定子群組設定，右擊其名稱並選取**內容**。
     子群組內容視窗將開啟。

2. 在**裝置**區域，指定以下設定：

   - **若裝置未活動超過下列天數，則從群組刪除裝置**

     如果啟用該選項，您可以指定從組中自動移除裝置的時間間隔。預設下，該選項也被分發到子群組。
     預設時間間隔為 7 天。
     預設情況下已啟用該選項。

   - **從父群組繼承**

     如果啟用該選項，裝置在目前群組的保留期從父群組繼承且無法被變更。
     該選項僅對子群組可用。
     預設情況下已啟用該選項。

   - **強制子群組繼承**

     該設定值將被分發到子群組，但在子群組的內容中這些設定被鎖定。
     預設情況下已停用該選項。

您的變更已儲存並套用。

使用 IP 範圍

您可以自訂現有的 IP 範圍並建立新子網路。

建立 IP 範圍

要建立 IP 範圍，請執行以下操作：

1. 在主控台樹狀目錄中的**裝置發現**資料夾，選取**IP 範圍**子資料夾。
2. 從資料夾的上下文功能表中，選取**新增 → IP 範圍**。
3. 在開啟的**新 IP 範圍**視窗中自訂新的 IP 範圍。

新的 IP 範圍將顯示在 **IP 範圍**資料夾中。

瀏覽和變更 IP 範圍設定

要修改 IP 範圍設定，請執行以下操作：

1. 在主控台樹狀目錄中的**裝置發現**資料夾，選取**IP 範圍**子資料夾。
2. 以下列方式之一選取一個 IP 範圍並開啟其內容視窗：
   - 從 IP 範圍的右鍵功能表中選取"**內容**"。
   - 透過點擊**顯示群組內容**連結。

   系統將開啟"**內容：<IP 範圍名稱>**"視窗，您可以在該視窗中設定選定的 IP 範圍的內容。

使用 Active Directory 群組。檢視與修改群組設定

要修改 Active Directory 群組設定，請執行以下操作：

1. 在主控台樹狀目錄中的**裝置發現**資料夾中，選取**Active Directory**子資料夾。
2. 透過以下方式之一選取一個 Active Directory 群組並開啟其內容視窗：
   - 從 IP 範圍的右鍵功能表中選取"**內容**"。
   - 透過點擊**顯示群組內容**連結。

   系統將開啟**內容：<Active Directory 群組名稱>**視窗，在其中可以設定選定的 Active Directory 群組。

建立將裝置自動移至管理群組的規則

您可以配置將在網路輪詢中發現的裝置自動移至管理群組。

要設定將裝置自動移至管理群組的規則：

1. 在主控台樹狀目錄中，選取**未配置的裝置**資料夾。
2. 在此資料夾的工作區，點擊**配置規則**連結。

   這會開啟**內容: 未配置的裝置** 視窗。在**移動裝置**區域，配置自動行動裝置至管理群組的規則。

清單中的第一個適用規則（從清單的頂部到底部）將套用於裝置。

在用戶端裝置上使用 VDI 動態模式

虛擬基礎架構可以使用動態虛擬機佈署企業網路。卡巴斯基安全管理中心偵測到動態虛擬機和他們在管理伺服器資料庫的附加資訊。使用者使用完動態虛擬機後，這些虛擬機將從虛擬架構中移除。動態虛擬機記錄將儲存在管理伺服器資料庫中。並且，動態虛擬機將不會在管理主控台顯示。

為了防止不存在的虛擬機被儲存，卡巴斯基安全管理中心支援動態模式的 Virtual Desktop Infrastructure (VDI)。管理員可在要安裝於臨時虛擬機的網路代理安裝套件內容中啟用 VDI 動態模式協助。

當動態虛擬機被停用，網路代理通知管理伺服器該虛擬機已被停用。虛擬機被成功停用，它將從連線到管理伺服器的裝置清單中被移除。如果虛擬機被停用錯誤，網路代理沒有傳送停用虛擬機的通知到管理伺服器，使用備份方案。使用這個方案，和管理伺服器嘗試同步三次未成功後，虛擬機將從連線管理伺服器的裝置清單中移除。

在網路代理安裝套件的內容中啟用 VDI 動態模式

要啟用 VDI 動態模式，請執行以下操作：

1. 在主控台樹狀目錄**遠端安裝**資料夾中，選取**安裝套件**子資料夾。
2. 在網路代理安裝套件的右鍵，選取"**內容**"。
   內容：卡巴斯基安全管理中心網路代理視窗將開啟。
3. 在**內容：卡巴斯基安全管理中心網路代理**視窗中，選取**進階**區域。
4. 在**進階**區段上選取**啟用 VDI 動態模式**選項。

要安裝網路代理的裝置將成為 VDI 的一部分。

搜尋啟用 VDI 的裝置

要尋找構成 VDI 的未指派的裝置：

1. 在**未配置的裝置**的上下文功能表中選取**搜尋**。
   若要查看屬於虛擬桌面基礎結構的所有裝置的清單，請從**搜尋**資料夾的上下文功能表中選擇**管理伺服器**。
2. 在**搜尋**視窗的**虛擬機**頁簽上，在**是**設定群組中選擇**虛擬桌面基礎架構的一部分**。
3. 點擊 **立即尋找**按鈕。

將顯示屬於虛擬桌面基礎架構的未指派的裝置清單。

將啟用 VDI 的裝置移至管理群組

要將啟用 VDI 的裝置移至管理群組，請執行以下操作：

1. 在**未配置的裝置**資料夾的工作區中，點擊**配置規則**。
   該**未配置的裝置**資料夾的內容視窗將開啟。
2. 在**未配置的裝置**資料夾的**移動裝置**區域中，點擊**新增**按鈕。
   新規則 視窗隨即開啟。
3. 在**新規則**視窗中，選取**虛擬機**區域。
4. 在 **這是一台虛擬機**下拉清單中，選取**是**。

將會建立移動裝置到管理群組的規則。

設備清查

您用於庫存設備的硬體清單（**儲存區 → 硬體**）以兩種方式填入：自動和手動。在每次網路輪詢後，所有偵測到的裝置會自動新增至清單：不過，若您不想輪詢網路，也可以手動新增裝置。您可以手動將其他裝置新增至清單，例如路由器、印表機或裝置硬體。

在裝置的內容視窗，您可以檢視和編輯有關該裝置的詳細資訊。

硬體清單含有以下裝置類型：

- 電腦
- 行動裝置
- 網路裝置
- 虛擬裝置
- OEM 元件
- 電腦週邊裝置
- 已連接裝置
- VoIP 電話
- 網路儲存區

管理員可以將"*企業裝置*"內容分配給所偵測到的裝置。內容設定項目，可以手動指定裝置的內容，或者管理員可以指定內容後，進行自動派送。在此方式下，系統將按裝置類型分配"*企業裝置*"內容。

卡巴斯基安全管理中心允許註銷裝置。為此，請選取裝置內容中的**裝置已記錄**選項。此後，刪除的裝置將不會顯示在裝置清單。

管理員可以在**硬體**資料夾管理可編程邏輯控制 (PLC)。管理 PLC 清單的詳細資訊提供在 *Kaspersky Industrial CyberSecurity for Nodes 使用者手冊*。

關於新增裝置的資訊

若要新增網路上新裝置資訊，請執行以下操作：

1. 在主控台樹狀目錄**儲存區**資料夾中，選取**硬體**子資料夾。
2. 在**硬體**資料夾中，點擊**新增裝置**按鈕以開啟**新裝置**視窗。
   新裝置視窗隨即開啟。
3. 在**新裝置**視窗中，從**類型**下列清單中選取您要新增的裝置類型。
4. 點擊**確定**。
   裝置內容視窗中將開啟**一般**區域。
5. 在**一般**區域中使用裝置資料填寫輸入欄位。**一般**區域將顯示以下設定：
   - **企業裝置**。如果您希望將"*企業*"內容分配給該裝置，請選取該方塊。您可以使用該內容搜尋**硬體**資料夾中的裝置。
   - **裝置已記錄**。如果您不希望此裝置顯示在**硬體**資料夾中的裝置清單中，請選取此方塊。
6. 點擊"**套用**"。

新裝置將顯示在**硬體**資料夾的工作區中。

設定用於定義企業裝置的標準

若要設定偵測企業裝置的標準，請執行以下操作：

1. 在主控台樹狀目錄**儲存區**資料夾中，選取**硬體**子資料夾。
2. 在**硬體**資料夾的工作區中，點擊**附加操作**按鈕並在下拉式清單中選取**設定企業裝置規則**。
   "硬體內容"視窗開啟。
3. 在硬體內容視窗中**企業裝置**區域中選取將*企業*內容分配給該裝置的方法：
   - **為裝置手動設定"企業"裝置內容**。在裝置內容視窗的***General***區域中手動將一般內容分配給該裝置。
   - **為裝置自動設定"企業"裝置內容**。在設定的**透過裝置類型**區塊中指定程式自動為其分配*企業*內容的裝置類型。

     此選項僅影響透過網路輪詢新增的裝置。對於手動心中的裝置，手動設定*企業*內容。
4. 點擊"**確定**"。

企業裝置的偵測標準得到配置。

配置自訂欄位

要設定裝置的自訂欄位：

1. 在主控台樹狀目錄**儲存區**資料夾中，選取**硬體**子資料夾。
2. 在**硬體**資料夾的工作區中，點擊**附加操作**按鈕並在下拉式清單中選取**設定自訂資料欄位**。

   "硬體內容"視窗開啟。
3. 在硬體內容視窗中，選取**自訂欄位**區域並點擊**新增**按鈕。

   新增欄位視窗將開啟。
4. 在**新增欄位**視窗，指定將顯示在硬體內容中的自訂欄位名稱。

   您可以使用獨立名稱建立多個自訂欄位。
5. 點擊"**確定**"。

新增的自訂欄位會顯示在硬體內容的**自訂欄位**區域。您可以使用自訂欄位提供裝置的特別資訊。例如，這可以是硬體的內部訂購號。

產品授權

本節提供關於卡巴斯基安全管理中心 14.2 產品授權的一般概念資訊。

超出了產品授權限制事件

卡巴斯基安全管理中心允許您獲取用戶端裝置上安裝的 Kaspersky 應用程式的產品授權達到限制的事件資訊。

產品授權達到限制的此類事件的重要級別依據以下規則定義：

- 如果目前使用單一產品授權的單元的數量達到該產品授權所覆蓋的單元總數的 90% 和 100% 之間，事件等級就是**資訊**重要等級。
- 如果目前使用單一產品授權的單元的數量達到該產品授權所覆蓋的單元總數的 100% 和 110% 之間，事件等級就是**警告**重要等級。
- 如果目前使用單一產品授權的單元的數量超過該產品授權所覆蓋的單元總數的 110%，事件等級就是**緊急事件**重要級別。

關於產品授權

本部分包含有關透過卡巴斯基安全管理中心管理的 Kaspersky 應用程式產品授權資訊。

關於產品授權

*產品授權*是根據簽章的產品授權條約（最終使用者產品授權協議）條款授予在有限時間內使用卡巴斯基安全管理中心的權限。

服務範圍和有效期取決於用於根據其使用該應用程式的產品授權。

我們提供下列授權類型：

- *試用*

  用於試用此程式的免費產品授權。試用版產品授權通常擁有較短的有效期。

  試用版產品授權到期後，卡巴斯基安全管理中心的所有功能都會被停用。要繼續使用程式，您需要獲得正式版的產品授權。

  您只能在試用產品授權下使用該應用程式一個試用期。

- *正式*

  付費產品授權。

  當正式產品授權到期時，應用程式的主要功能將被停用。要繼續使用卡巴斯基安全管理中心，您必須續約您的正式產品授權。正式產品授權過期後，您將無法繼續使用該應用程式，必須將其從裝置中刪除。

  我們建議在產品授權到期之前進行續約，以確保防護不受中斷，抵禦所有安全威脅。

關於最終使用者產品授權協議

最終使用者產品授權協議（產品授權協議或 EULA）是您和 AO Kaspersky Lab 之間具有約束力的合作協議，其中規定了您使用該程式應遵守的條款。

在您開始使用應用程式之前請仔細閱讀產品授權協議。

卡巴斯基安全管理中心與其元件（如網路代理）有其各自的 EULA。

您可使用以下方式，檢視卡巴斯基安全管理中心最終使用者產品授權協議的條款：

- 在卡巴斯基安全管理中心安裝期間。
- 如果閱讀包含在卡巴斯基安全管理中心分發套件的 license.txt 文件。
- 如果閱讀在卡巴斯基安全管理中心安裝資料夾的 license.txt 文件。
- 透過從卡巴斯基網站下載 license.txt 檔案。

您可使用以下方式，檢視 Windows 版網路代理、Mac 版網路代理、Linux 版網路代理的最終使用者產品授權協議條款：

- 從 Kaspersky Web 伺服器下載網路代理分發套件期間。
- 安裝 Windows 版網路代理、Mac 版網路代理、或 Linux 版網路代理期間。
- 透過閱讀包含在 Windows 版網路代理、Mac 版網路代理、或 Linux 版網路代理分發套件的 license.txt 文件。
- 透過閱讀在 Windows 版網路代理、Mac 版網路代理、或 Linux 版網路代理安裝資料夾的 license.txt 文件。
- 透過從卡巴斯基網站下載 license.txt 檔案。

當您安裝程式時同意最終使用者產品授權協議，表示您接受最終使用者產品授權協議的條款。如果您不接受產品授權協議中的條款，將取消應用程式安裝且不再使用應用程式。

關於產品授權憑證

*產品授權憑證*是隨著您收到的一個金鑰檔案和啟動碼一起的檔案。

產品授權憑證提供以下的產品授權資訊：

- 產品授權 ID 或訂單號
- 授予產品授權的使用者資訊
- 可以使用提供的產品授權啟動的應用程式資訊
- 產品授權單元的數量限制（例如，在該產品授權下，裝置上的應用程式可以被使用）
- 產品授權期限的開始日期
- 產品授權到期日期或產品授權期限
- 產品授權類型

關於產品授權金鑰

*產品授權金鑰*由一系列字母數字組成，您可以依據最終使是用者產品授權協議的條款使用它們啟動並使用程式。產品授權金鑰由 Kaspersky 專家產生。

您可以使用下面的方法新增一個產品授權金鑰到應用程式：透過套用*金鑰檔案*或輸入*啟動碼*。為程式新增金鑰後，將在程式介面中顯示該產品授權金鑰的唯一字母數字序列。

如果違反產品授權協議的條款，Kaspersky 可能會封鎖產品授權金鑰。如果金鑰已被封鎖，要使用程式，您需要新增另外一個金鑰。

產品授權金鑰可以是啟用或備用的金鑰（或預留）。

*啟動產品授權金鑰*是應用程式目前使用的產品授權金鑰。啟動產品授權金鑰可以被新增為正式產品授權。應用程式只能擁有一個啟動產品授權金鑰。

*備用（或預留）產品授權金鑰*是允許使用者使用應用程式，但是目前未使用的產品授權金鑰。與目前產品授權金鑰相關聯的產品授權到期時，備用產品授權金鑰將自動成為目前產品授權金鑰。只有在新增啟動產品授權金鑰之後，才可以新增備用產品授權金鑰。

試用產品授權金鑰僅可以被當作啟動產品授權金鑰新增。試用產品授權金鑰不可以被當作備用產品授權金鑰新增。

關於金鑰檔案

*金鑰檔案*是 Kaspersky 提供的 .key 副檔名的檔案。金鑰檔案設計用於透過新增產品授權金鑰啟動應用程式。

在購買卡巴斯基安全管理中心或預定試用版本的卡巴斯基安全管理中心後，您透過您指定的郵件位址可以收到金鑰檔案。

您不需要連線到 Kaspersky 啟動伺服器以使用金鑰檔案啟動應用程式。

如果金鑰檔案被意外刪除，您可以還原它。您可能需要金鑰檔案來註冊 Kaspersky CompanyAccount。

若要還原您的金鑰檔案，執行下面任何的操作：

- 聯絡產品授權銷售商。
- 使用您有效的啟動碼，透過卡巴斯基網站接收金鑰檔案。
- 從其他管理伺服器匯出產品授權金鑰檔案。

關於訂購

*卡巴斯基安全管理中心訂購*是在所選設定（訂購到期時間、受防護裝置數量）下使用程式的訂購。您可以和您的服務供應商（例如，網際網路供應商）註冊您的卡巴斯基安全管理中心訂購。訂購可以自動或手動續約，您也可以取消訂購。

訂購可以是限期的（例如，一年）或不限期的。如果要在限期訂購後繼續使用卡巴斯基安全管理中心，您必須續約訂購。無限制訂購如果已經預付給服務提供商了，則會在到期日自動續約。

當受限制訂購到期時，可為您提供一個使產品繼續工作的寬限期以便您及時續約。寬限期的可用性和期限由服務供應商提供。

要在訂購下使用卡巴斯基安全管理中心，您必須套用從服務供應商收到的啟動碼。

您僅可以在訂購到期後或者取消訂購後為卡巴斯基安全管理中心申請不同的啟動碼。

取決於服務供應商，訂購管理可能的操作也會不同。服務供應商可以不提供訂購寬限期，因此程式會失去它的功能。

訂購啟動碼無法用於啟動卡巴斯基安全管理中心的早期版本。

在訂購下使用應用程式時，卡巴斯基安全管理中心在指定時間間隔自動嘗試存取啟動伺服器，直到訂購到期。這將確保有關訂購的資訊與啟動伺服器同步。如果無法存取使用系統 DNS 的伺服器，則應用程式使用公用 DNS 伺服器。您可以在服務提供商網站續約您的訂購。

您可以手動更新有關訂購的資訊，無需等待卡巴斯基安全管理中心存取啟動伺服器。例如，當您變更訂購設定時，這可能很有用。

要手動更新訂購資訊：

1. 在主控台樹狀目錄中，選取**卡巴斯基產品授權**資料夾。
2. 點擊**「其他動作」**，然後從下拉清單中選擇**「將訂購設定與授權伺服器同步」**。

有關訂購的資訊在啟動伺服器上得到更新。

關於啟動碼

*啟動碼*是一串由 20 個字元數字組成的唯一序列。您可以輸入啟動碼來新增一個產品授權金鑰來啟動卡巴斯基安全管理中心。在購買卡巴斯基安全管理中心或預定試用版本的卡巴斯基安全管理中心後，透過您指定的郵件信箱可以收到啟動碼。

若要使用啟動碼啟動應用程式，您需要網際網路來建立與 Kaspersky 啟動伺服器的連線。如果無法使用系統 DNS 存取伺服器，則應用程式使用公用 DNS 伺服器。

當程式被啟動碼啟動後，程式有時傳送有規律的請求到 Kaspersky 啟動伺服器，以便檢查目前產品授權金鑰狀態。您必須提供給程式網際網路連線以使其能夠傳送請求。

如果您在安裝應用程式後丟失了啟動碼，請聯繫從其購買產品授權的卡巴斯基合作夥伴。

> 您不能使用金鑰檔案來啟動受管理的應用程式，僅接受以啟動碼啟動受管理的應用程式。

撤銷最終使用者產品授權協議的許可

若您決定停止保護用戶端裝置，您可取消安裝受管理的 Kaspersky 應用程式，並撤銷這些應用程式的最終使用者產品授權協議 (EULA)。

若要撤銷 Kaspersky 受管理應用程式的 EULA：

1. 在主控台樹狀目錄中，選擇**管理伺服器 → 進階 → 已接受的 EULA**。
   會顯示在建立安裝套件時、在無縫安裝更新時或在佈署 Kaspersky Security for Mobile 時接受的 EULA 清單。
2. 在清單中，選取您要撤銷協議的 EULA。
   您可以檢視 EULA 的下列內容：
   - 接受 EULA 的日期。
   - 接受 EULA 的使用者名稱。
   - 前往 EULA 條款的連結。
   - 與 EULA 相關的物件清單：安裝套件名稱、無縫更新名稱、行動應用程式名稱。

3. 按一下**撤銷 EULA** 按鈕。

   在開啟的視窗中，會告知您必須解除安裝對應至 EULA 的 Kaspersky 應用程式。

4. 按一下按鈕以確認撤銷。

   卡巴斯基安全管理中心會檢查安裝套件（對應至您要撤銷其 EULA 的 Kaspersky 受管理應用程式）是否已刪除。

   您僅可撤銷受管理 Kaspersky 應用程式的 EULA，其安裝套件會遭到刪除。

EULA 已撤銷。這不會顯示在**管理伺服器 → 進階 → 已接受的 EULA** 區域的 EULA 清單中。您無法使用其 EULA 已被您撤銷的 Kaspersky 應用程式防護用戶端裝置。

關於資料提供

傳輸至第三方的資料

若使用軟體的行動裝置管理功能，則為了透過推播通知機制，將命令及時傳遞至執行 Android 作業系統的裝置，會使用 Google Firebase Cloud Messaging 服務。若使用者已設定 Google Firebase Cloud Messaging服務的使用方式，代表使用者接受以自動模式向 Google Firebase Cloud Messaging 服務提供下列資訊：Kaspersky Endpoint Security for Android 應用程式的安裝 ID（推播通知必須傳送至該應用程式）。

若要封鎖與向 Google Firebase Cloud Messaging 服務交換資訊，則使用者必須將 Google Firebase Cloud Messaging服務的使用設定復原至而原廠值。

若使用軟體的行動裝置管理功能，則為了透過推播通知機制，將命令及時傳遞至執行 iOS 作業系統的裝置，會使用 Apple 推播通知服務（APNs）。若使用者已在 iOS MDM 伺服器上安裝 APNs 憑證、已透過 iOS 行動裝置對軟體的連線設定集合建立 iOS MDM 設定檔，並且已在行動裝置上安裝此設定檔，代表使用者同意以自動模式向 APNs 提供下列資訊：

- 權杖—裝置的推播權杖。伺服器在向裝置傳送推播通知時使用此權杖。
- PushMagic—必須在推播通知中納入的字串。字串值由裝置產生。

本機處理的資料

卡巴斯基安全管理中心是設計用來在區域網路中集中執行基本的管理和維護工作。卡巴斯基安全管理中心提供關於組織的網路安全等級的詳盡資訊予管理員存取；卡巴斯基安全管理中心可讓管理員根據 Kaspersky 應用程式設定所有防護元件。卡巴斯基安全管理中心執行以下主要功能：

- 在組織的網路中偵測裝置及其使用者
- 建立裝置管理的管理群組階層
- 在裝置上安裝卡巴斯基應用程式
- 管理已安裝應用程式的設定和工作
- 管理 Kaspersky 和協力廠商應用程式的更新，並尋找和修正弱點
- 在裝置上啟動 Kaspersky 應用程式
- 管理使用者帳戶

- 檢視卡巴斯基應用程式在裝置上的操作相關資訊
- 檢視報告

若要執行其主要功能，卡巴斯基安全管理中心可以接收、儲存和處理下列資訊：

- 組織網路中的裝置相關資訊，在 Active Directory 網路或 Windows 網路中作為裝置發現結果來接收，或透過掃描 IP 間隔來接收。管理伺服器獨立取得資料或接收來自網路代理的資料。
- Active Directory 組織單位、網域、使用者和群組的相關資訊，在 Active Directory 網路中作為裝置發現結果來接收。管理伺服器獨立取得資料或接收來自網路代理的資料。
- 受管理裝置的詳細資料。網路代理將下列資料從裝置傳輸至管理伺服器。使用者在管理主控台介面或卡巴斯基安全管理中心 網頁主控台介面中輸入裝置的顯示名稱和說明：
  - 裝置識別所需的受管理裝置及其元件的技術規格：裝置顯示名稱和說明、Windows 網域名稱和類型、Windows 環境中的裝置名稱、DNS 網域和 DNS 名稱、IPv4 位址、IPv6 位址、網路位置、MAC 位址、作業系統類型、裝置是否為虛擬機以及 hypervisor 類型、以及裝置是否為屬於 VDI 的動態虛擬機。
  - 稽核受管理裝置以及決定特定修補程式和更新是否適用時所需的受管理裝置及其元件的其他規格：Windows 更新代理 (WUA) 狀態、作業系統架構、作業系統供應商、作業系統組建編號、作業系統發行 ID、作業系統位置資料夾，如果裝置是虛擬機器—虛擬機器類型；管理裝置的虛擬管理伺服器名稱；雲端裝置資料（雲端區域、VPC、雲端可用區、雲端子網路、雲端安置區）。
  - 受管理裝置的動作詳細資訊：上次更新的日期和時間、網路中上次顯示裝置的時間、重新啟動等待狀態以及裝置開啟時間。
  - 裝置使用者帳戶和其工作階段的詳情。
- 若裝置是發佈點，也包括發佈點操作統計資料。網路代理將資料從裝置傳輸至管理伺服器。
- 使用者在管理主控台或卡巴斯基安全管理中心 網頁主控台中輸入的發佈點設定。
- 將行動裝置連線到管理伺服器所需的資料：憑證、行動連線連接埠、管理伺服器連線位址。使用者在管理主控台或卡巴斯基安全管理中心 網頁主控台中輸入資料。
- 使用 Exchange ActiveSync 協定傳輸的行動裝置詳情。下列資料從行動裝置傳輸至管理伺服器：
  - 裝置識別所需的行動裝置和其元件的技術規格：裝置名稱、型號、作業系統名稱、IMEI 編號和電話號碼。
  - 行動裝置和其元件的說明：裝置管理狀態、SMS 支援、傳送 SMS 訊息的權限、FCM 支援、使用者指令支援、作業系統儲存資料夾和裝置名稱。
  - 行動裝置動作詳情：裝置位置（透過定位指令）、上一次同步時間、上一次連線到管理伺服器時間和同步支援詳情。

- 使用 iOS MDM 協定傳輸的行動裝置詳情。下列資料從行動裝置傳輸至管理伺服器：
  - 用於裝置識別的行動裝置和其元件的技術說明：裝置名稱、模組、作業系統名稱和組建編號、裝置型號、IMEI 編號、UDID、MEID、序號、記憶體、數據機固件版本、藍牙 MAC 位址、Wi-Fi MAC 位址和 SIM 卡詳情（作為 SIM 卡 ID 一部分的 ICCID）。
  - 受管理裝置使用的行動網路詳情：行動網路類型、目前使用的行動網路名稱、家庭行動網路名稱、行動網路操作員設定版本、語音漫遊和資料漫遊狀態、家用網路國家代碼、居住國代碼、目前使用的網路國家代碼和加密等級。
  - 行動裝置的安全設定：密碼使用和其與政策設定的遵從、設定檔清單和用於安裝協力廠商應用程式的 provisioning 設定檔。
  - 與管理伺服器的上一次同步日期和裝置管理狀態。
- 安裝到裝置的 Kaspersky 應用程式詳情。受管理應用程式透過網路代理將資料從裝置傳輸至管理伺服器：
  - 安裝在受管理裝置上的 Kaspersky 應用程式設定：Kaspersky 應用程式名稱和版本、狀態、即時防護狀態、上次裝置掃描日期和時間、威脅偵測數量、物件解毒失敗數量、應用程式元件的可用性和狀態、病毒資料庫的上次更新時間和版本、Kaspersky 應用程式設定和工作的詳情、關於作用中和備用產品授權金鑰的資訊、應用程式安裝日期和 ID。
  - 應用程式操作統計資訊：受管理裝置上的 Kaspersky 應用程式元件狀態變更相關事件和應用程式元件發起的工作效能相關事件。
  - Kaspersky 應用程式定義的裝置狀態。
  - Kaspersky 應用程式指派的標記。
  - Kaspersky 應用程式的已安裝和適用更新的設定。
- 來自卡巴斯基安全管理中心元件和 Kaspersky 受管理應用程式的事件中包含的資料。網路代理將資料從裝置傳輸至管理伺服器。
- 將卡巴斯基安全管理中心與 SIEM 系統整合以進行事件匯出所需的資料。使用者在管理主控台或卡巴斯基安全管理中心 網頁主控台中輸入資料。
- 存在於政策和政策設定檔中的卡巴斯基安全管理中心元件和 Kaspersky 受管理應用程式的設定。使用者在管理主控台或卡巴斯基安全管理中心 網頁主控台介面中輸入資料。
- 卡巴斯基安全管理中心元件和 Kaspersky 受管理應用程式的工作設定。使用者在管理主控台或卡巴斯基安全管理中心 網頁主控台介面中輸入資料。
- 弱點和修補程式管理功能處理的資料。網路代理將下列資料從裝置傳輸至管理伺服器：
  - 安裝在受管理裝置（應用程式登錄資料）的應用程式和修補程式的詳細資訊。
  - 受管理裝置上偵測到的硬體相關資訊（硬體登錄資料）。
  - 在受管理裝置上偵測到的協力廠商軟體中的弱點詳細資訊。
  - 安裝在受管理裝置上的協力廠商應用程式的可用更新詳細資訊。
  - WSUS 功能找到的 Microsoft 更新詳細資訊。
  - WSUS 功能找到且必須安裝在裝置上的 Microsoft 更新清單。

- 在隔離的管理伺服器上下載更新以修復託管裝置上的第三方軟體弱點所需的資料。使用者使用管理伺服器 klscflag 實用程式輸入和傳輸資料。

- 卡巴斯基安全中心在雲端環境（Amazon Web Services、Microsoft Azure、Google Cloud、Yandex Cloud）中工作所需的資料。使用者在管理主控台或卡巴斯基安全管理中心 網頁主控台中輸入資料。

- 應用程式使用者類別。使用者在管理主控台或卡巴斯基安全管理中心 網頁主控台介面中輸入資料。

- 受管理裝置上偵測到的應用程式控制功能使用的可執行檔詳細資料。使用者在管理主控台或卡巴斯基安全管理中心 網頁主控台介面中輸入資料。相應應用程式的說明檔案中提供了完整資料清單。

- 置於備份中的檔案詳細資訊。受管理應用程式透過網路代理將資料從裝置傳輸至管理伺服器。相應應用程式的說明檔案中提供了完整資料清單。

- 置於隔離中的檔案詳細資訊。受管理應用程式透過網路代理將資料從裝置傳輸至管理伺服器。相應應用程式的說明檔案中提供了完整資料清單。

- Kaspersky 專家為了詳細分析而要求的檔案詳細資訊。受管理應用程式透過網路代理將資料從裝置傳輸至管理伺服器。相應應用程式的說明檔案中提供了完整資料清單。

- 狀態和觸發自適應異常控制規則的詳細資訊。受管理應用程式透過網路代理將資料從裝置傳輸至管理伺服器。相應應用程式的說明檔案中提供了完整資料清單。

- 安裝或連線至受管理裝置並且由裝置控制功能偵測到的外部裝置的詳細資訊（記憶體單位、資訊傳輸工具、資訊實體工具和連線匯流排）。受管理應用程式透過網路代理將資料從裝置傳輸至管理伺服器。相應應用程式的說明檔案中提供了完整資料清單。

- 關於加密裝置和加密狀態的資訊。受管理應用程式透過網路代理將資料從裝置傳輸至管理伺服器。

- 使用 Kaspersky 應用程式的資料加密功能執行的裝置上的資料加密錯誤詳細資訊。受管理應用程式透過網路代理將資料從裝置傳輸至管理伺服器。相應應用程式的說明檔案中提供了完整資料清單。

- 受管理可程式設計邏輯控制器 (PLC) 清單。受管理應用程式透過網路代理將資料從裝置傳輸至管理伺服器。相應應用程式的說明檔案中提供了完整資料清單。

- 建立威脅開發鏈所需的資料。受管理應用程式透過網路代理將資料從裝置傳輸至管理伺服器。相應應用程式的說明檔案中提供了完整資料清單。

- 卡巴斯基安全管理中心與 Kaspersky Managed Detection and Response 服務整合（必須為卡巴斯基安全管理中心 網頁主控台安裝專用外掛程式）所需的資料：整合啟動權杖、整合權杖和使用者工作階段權杖。使用者在卡巴斯基安全管理中心 網頁主控台介面中輸入資料。Kaspersky MDR 服務透過專用外掛程式傳輸整合權杖和使用者工作階段權杖。

- 輸入的啟動碼或指定金鑰檔案的詳細資訊。使用者在管理主控台或卡巴斯基安全管理中心 網頁主控台介面中輸入資料。

- 使用者帳戶：名稱、描述、全名、電子郵件地址、主要電話號碼、密碼、管理伺服器產生的金鑰，以及用於兩步驟驗證的一次性密碼。使用者在管理主控台或卡巴斯基安全管理中心 網頁主控台介面中輸入資料。

- 識別和存取管理器為了進行集中式身分驗證和為了給與卡巴斯基安全管理中心集成的 Kaspersky 應用程式提供單點登錄 (SSO) 所需的資料：識別和存取管理器的安裝和配置設定，識別和存取管理器使用者工作階段，識別和存取管理器權杖，用戶端應用程式狀態和資源伺服器狀態。使用者在管理主控台或卡巴斯基安全管理中心 網頁主控台介面中輸入資料。

- 管理物件的修訂歷史記錄。使用者在管理主控台或卡巴斯基安全管理中心 網頁主控台介面中輸入資料。

- 已刪除之管理物件的登錄資料。使用者在管理主控台或卡巴斯基安全管理中心 網頁主控台介面中輸入資料。
- 從檔案建立的安裝套件以及安裝設定。使用者在管理主控台或卡巴斯基安全管理中心 網頁主控台介面中輸入資料。
- 在卡巴斯基安全管理中心 網頁主控台中顯示來自 Kaspersky 公告所需的資料。使用者在管理主控台或卡巴斯基安全管理中心 網頁主控台介面中輸入資料。
- 卡巴斯基安全管理中心 網頁主控台中受管理應用程式的外掛程式執行所需的資料，並在其日常操作期間由外掛程式儲存在管理伺服器資料庫中。相應應用程式的說明檔案中提供了描述和提供資料的方式。
- 卡巴斯基安全管理中心 網頁主控台使用者設定：當地語系化和介面佈景主題、監控面板顯示設定、通知狀態相關資訊（已讀 / 未讀）、試算表資料行狀態（顯示 / 隱藏）、訓練模式進度。使用者在卡巴斯基安全管理中心 網頁主控台介面中輸入資料。
- 卡巴斯基安全管理中心元件的卡巴斯基事件記錄和 Kaspersky 受管理應用程式。卡巴斯基事件記錄儲存在各裝置上，從未傳輸至管理伺服器。
- 與受管理裝置和卡巴斯基安全管理中心元件的安全連線憑證。使用者在管理主控台或卡巴斯基安全管理中心網頁主控台介面中輸入資料。
- 卡巴斯基安全管理中心在雲端環境（例如 Amazon Web Services (AWS)、Microsoft Azure、Google Cloud 和 Yandex.Cloud）中執行所需的資料。管理伺服器從其執行所在的虛擬機器接收資料。
- 使用者接受與 Kaspersky 法律通訊協定條款和條件的相關資訊。
- 使用者在以下元件中輸入的管理伺服器資料：
  - 管理主控台
  - 卡巴斯基安全管理中心網頁主控台
  - 使用 klscflag 實用程式時的命令行終端
  - 透過 klakaut 自動化物件和卡巴斯基安全管理中心 OpenAPI 與管理伺服器互動的元件
- 使用者在管理主控台或卡巴斯基安全管理中心 網頁主控台介面中輸入的任何資料。

若套用下列方法之一，以上列出的資料可出現在卡巴斯基安全管理中心：

- 使用者在以下元件的介面中輸入資料：
  - 管理主控台
  - 卡巴斯基安全管理中心網頁主控台
  - 使用 klscflag 實用程式時的命令行終端
  - 透過 klakaut 自動化物件和卡巴斯基安全管理中心 OpenAPI 與管理伺服器互動的元件
- 網路代理自動接收來自裝置的資料並傳輸至管理伺服器。
- 網路代理接收 Kaspersky 受管理應用程式擷取的資料並傳輸至管理伺服器。相應應用程式的說明檔案中提供了 Kaspersky 受管理應用程式處理的資料清單。

- 管理伺服器可獨立取得有關連網裝置的資訊或從充當發佈點的網路代理接收資訊。
- 使用 Exchange ActiveSync 或 iOS MDM 通訊協定，將資料從行動裝置傳輸至管理伺服器。

列出的資料儲存在管理伺服器資料庫。使用者名稱和密碼以加密格式儲存。

上列所有資料只能透過卡巴斯基安全管理中心元件的傾印檔案、偵錯檔案或記錄檔案傳輸至 Kaspersky，包含安裝程式和實用程式建立的記錄檔案。

卡巴斯基安全管理中心元件的傾印檔案、偵錯檔案和記錄檔案包含管理伺服器、網路代理、管理主控台、iOS MDM 伺服器、Exchange 行動裝置伺服器和卡巴斯基安全管理中心 網頁主控台的隨機資料。這些檔案可能包含個人與敏感性資料。傾印檔案、偵錯檔案和記錄檔案以非加密形式儲存在裝置。傾印檔案、偵錯檔案和記錄檔案不會自動傳輸到 Kaspersky；然而，管理員可以在技術支援要求下手動傳輸資料到 Kaspersky 以便解決卡巴斯基安全管理中心的操作問題。

依照管理主控台或卡巴斯基安全管理中心 網頁主控台中的連線進行操作，即表示使用者同意自動傳輸以下資料：

- 卡巴斯基安全管理中心代碼
- 卡巴斯基安全管理中心版本
- 卡巴斯基安全管理中心當地語係化
- 產品授權 ID
- 產品授權類型
- 產品授權是否是透過合作夥伴購買的

透過每個連接提供的資料清單取決於連接的目的和位置。

Kaspersky 以匿名形式使用已接收的資料，並且僅用於一般統計用途。摘要統計資料會從原本接收的資訊中自動產生，其中不包含任何個人或機密資料。新資料累積後，就會抹除先前的資料（一年一次）。摘要統計資料會無限期儲存。

Kaspersky 防護接收到的符合法律和相應 Kaspersky 規則的任何資訊。資料會透過安全的通道傳輸。

卡巴斯基安全管理中心產品授權選項

卡巴斯基安全管理中心 可以在以下模式下工作：

- **無產品授權（基本功能）**

  卡巴斯基安全管理中心 在應用程式啟動之前或商業產品授權到期之後以這種模式工作。在管理主控台的基本功能支援下的卡巴斯基安全管理中心作為防護企業網路的 Kaspersky 應用程式的一部分被傳送。您也可以從 Kaspersky 網站下載。

- **商業執照**

  如果您需要管理主控台基本功能中未包含的其他功能，則必須購買商業產品授權。

  在「管理伺服器」屬性視窗中新增授權金鑰時，請確保新增允許使用卡巴斯基安全管理中心的授權金鑰。您可以在 Kaspersky 網站上找到此資訊。每個解決方案網頁均包含此解決方案中包含的應用程式清單。管理伺服器可接受不受支援的產品授權金鑰，例如 Kaspersky Endpoint Security Cloud 的產品授權金鑰，但此類產品授權金鑰除了管理主控台的基本功能外，不提供任何新功能。

功能或內容	卡巴斯基安全管理中心作業模式	
	無產品授權	商業執照
管理主控台的基本功能 提供以下功能選項： • 建立用於管理遠端辦公室網路或用戶端組織網路的虛擬管理伺服器。 • 建立一個管理群組層級結構，作為一個單一實體管理特定裝置。 • 遠端安裝應用程式。 • 對安裝在用戶端裝置上的應用程式的集中配置。 • 控制群組的病毒防護狀態。 • 管理使用者角色。 • 擷取統計資料和應用程式執行報告，以及緊急事件通知。 • 集中式管理被延遲處理的檔案或被移至隔離區或備份區的檔案。 • 加密和資料防護管理。 • 檢視和編輯現有的已授權的應用程式群組。 • 手動檢視和編輯網路偵測到的硬體裝置清單。 • 檢視可用於遠端安裝的作業系統映像檔的清單。	✓	✓
弱點和修補程式管理：基本功能 以下工作不需要正式產品授權： • *弱點掃描和所需更新*工作 透過此工作，卡巴斯基安全管理中心會收到已偵測弱點清單，與安裝在受管理裝置上協力廠商軟體必要更新的清單。 • *安裝 Windows Update 更新*工作 此工作只能用於安裝 Windows Update 更新。要使用此工作，您必須在工作設定中手動指定所需的更新。 • *修復弱點*工作 *修復弱點*工作會使用適用於 Microsoft 軟體的建議修復項目，以及適用於協力廠商軟體的使用者修復項目。若要使用此工作，您必須為工作設定中的弱點手動指定使用者修復項目。	✓	✓

功能或內容	卡巴斯基安全管理中心作業模式	
	無產品授權	商業執照
弱點和修補程式管理：進階功能 提供以下功能選項： • 根據您定義的規則，遠端安裝軟體更新並自動修復弱點。 • 使用管理伺服器作為 Windows 伺服器更新服務 (WSUS) 伺服器，以集中模式和設定頻率為裝置上的 Windows 更新服務提供更新。	–	✓
基於 MMC 的管理主控台中的行動裝置管理功能 「行動裝置管理」功能設計用於管理 Exchange ActiveSync (EAS) 和 iOS MDM 行動裝置。 以下功能適用於 Exchange ActiveSync 行動裝置： • 新增受卡巴斯基安全管理中心管理的新裝置。 • 管理行動裝置的身分配置和編輯，並套用設定到行動裝置端信箱。 • 設定行動裝置（郵件同步，應用程式使用，使用者密碼，資料加密，連線卸除式磁碟機）。 • 安裝行動裝置憑證。 以下功能適用於管理 iOS MDM 裝置： • 添加受 Kaspersky Security Center 管理的新裝置。 • 管理行動裝置的設定配置和編輯，並套用設定到行動裝置。 • 透過 App Store® 或使用清單檔案 (.plist) 在行動裝置上安裝應用程式。 • 鎖定行動裝置，重新設定行動裝置密碼，從行動裝置中刪除所有資料。 以下功能適用於管理 iOS MDM 裝置： • 添加受 Kaspersky Security Center 管理的新裝置。 • 通過政策管理 Kaspersky Endpoint Security for Android。 此外，行動裝置管理功能支援對應協定的執行指令。 行動裝置管理功能是依行動裝置為管理單位。當管理行動裝置伺服器，連線到行動裝置便可開始進行管控。	–	✓（必須將產品授權金鑰新增到管理伺服器內容中。）

功能或內容	卡巴斯基安全管理中心作業模式	
	無產品授權	商業執照
卡巴斯基安全管理中心網頁主控台中的雲端環境設定 卡巴斯基安全管理中心網頁主控台 為您提供以下功能來管理 Android 和 iOS 行動裝置： • 新增受卡巴斯基安全管理中心管理的新裝置。 • 通過政策管理 Kaspersky Endpoint Security for Android 和 Kaspersky Security for iOS。 • 通過相關協定向行動裝置發送命令並執行命令。	–	✓（必須在每個行動裝置上新增產品授權金鑰。）
系統管理 提供以下功能選項： • 作業系統和應用程式的安裝。 卡巴斯基安全管理中心允許您建立作業系統映像，以及將其佈署在網路用戶端裝置上，也可以執行遠端安裝 Kaspersky 或其他供應商的應用程式。您可以從裝置轉換可擷取的作業系統映像到管理伺服器。作業系統映像儲存在管理伺服器的一個專屬資料夾中。參考裝置的作業系統映像被捕獲並透過安裝套件建立工作建立。您可透過網路佈署映像，在沒有作業系統的裝置上安裝作業系統。在這種情況下將使用名為 Preboot eXecution Environment (PXE) 的技術。 • 管理已授權應用程式群組。 • 透過名為遠端桌面連線的 Microsoft® Windows® 元件遠端連線到使用者端裝置的權限。 • 透過 Windows 桌面共用遠端到用戶端裝置。 • 透過**卡巴斯基遠端桌面連線檢視器**進行遠端連線。	–	✓

功能或內容	卡巴斯基安全管理中心作業模式	
	無產品授權	商業執照
與雲端環境整合 卡巴斯基安全管理中心不僅工作在預置裝置上，也提供特殊功能以使用雲端環境，如雲端環境設定精靈。卡巴斯基安全管理中心可透過下列虛擬機運作： • Amazon EC2 實例 • Microsoft Azure 虛擬機 • Google 雲端虛擬機實例 • 對於虛擬機	–	✓
將事件匯出到 SIEM 系統：使用 Syslog 協定 使用 Syslog 協定，您可以轉發發生在卡巴斯基安全管理中心管理伺服器上和受管理裝置上安裝的 Kaspersky 應用程式中的任意事件。Syslog 協定是標準訊息記錄協定。您可以用它匯出事件到任何 SIEM 系統。	✓	✓

卡巴斯基安全管理中心和受管理應用程式的產品授權功能

管理伺服器和受管理應用程式的產品授權涉及以下方面：

- 您可新增產品授權金鑰或有效啟動碼至管理伺服器，以啟動弱點和修補程式管理、行動裝置管理或與 SIEM 系統整合。卡巴斯基安全管理中心的某些功能只能根據使用的金鑰檔案或新增到管理伺服器的有效啟動碼來存取。
- 您可以為受管理應用程式新增多個啟動碼和金鑰檔案到管理伺服器儲存區。

關於卡巴斯基安全管理中心產品授權

如果您使用金鑰檔案啟動授權功能（例如，行動裝置管理），但是您也想使用其他授權功能（例如，弱點和修補程式管理），您必須從您的服務提供者購買金鑰檔案以啟動這兩個功能，且您必須使用該金鑰檔案啟動管理伺服器。

受管理應用程式的產品授權功能

對於受管理應用程式的授權，啟動碼或金鑰檔案可以被自動佈署或使用其他任何便捷方法。您可運用以下方法來佈署啟動碼或金鑰檔案：

- 自動佈署

  > 如果您使用不同的受管理應用程式且您必須佈署特定金鑰檔案或啟動碼到裝置，請選取其他方法佈署啟動碼或金鑰檔案。

  卡巴斯基安全管理中心允許您自動佈署可用產品授權金鑰到裝置。例如，三個產品授權金鑰被儲存在管理伺服器儲存區。您已為所有三個產品授權金鑰選取**自動分發產品授權金鑰到受管理裝置**核取方塊。Kaspersky 安全應用程式—例如，Kaspersky Endpoint Security for Windows—被安裝到組織裝置。發現必須佈署產品授權金鑰的新裝置。例如，應用程式會決定儲存區中可套用到裝置的兩個產品授權金鑰：產品授權金鑰 *Key_1*和產品授權金鑰 *Key_2*。這些產品授權金鑰之一被佈署到裝置。此種情況下，無法預見兩個產品授權金鑰中的哪個將被佈署到裝置，因為自動佈署產品授權金鑰不提供給任何管理員活動。

  當佈署產品授權金鑰時，裝置為該產品授權金鑰重新計算。您必須確保佈署產品授權金鑰的裝置數量不超過產品授權限制。如果裝置數量超過產品授權限制，所有不被產品授權覆蓋的裝置將被分配*緊急狀態*。

- 新增金鑰檔案或啟動碼至受管理應用程式安裝套件

  如果您使用安裝套件安裝受管理應用程式，您可以在該安裝套件中或在應用程式政策中指定啟動碼或金鑰檔案。產品授權金鑰將在下一次裝置與管理伺服器同步時被佈署到受管理裝置。

- 透過為受管理應用程式新增產品授權金鑰工作佈署

  如果您選擇為受管理應用程式新增產品授權金鑰工作，您可以選取要佈署到裝置的產品授權金鑰，並以任何便捷方法選取裝置—例如，選取管理群組或裝置分類。

- 手動新增啟動碼或金鑰檔案至裝置

Kaspersky 應用程式。集中佈署

該部分敘述了遠端安裝 Kaspersky 應用程式和從網路裝置移除它們的方法。

> 在用戶端裝置上佈署應用程式之前，請確保用戶端裝置的硬體和軟體滿足相應的需求。

網路代理是一個提供用戶端裝置和管理伺服器連線的元件。因此，網路代理必須安裝到每一台要進行管理的裝置上。管理伺服器的裝置僅能使用管理伺服器版本的網路代理。該版本包括在管理伺服器中，與管理伺服器一同安裝以及一同移除。所以您不需要再額外安裝網路代理在此裝置上。

網路代理與一般的軟體一樣，您可以利用遠端或是本機進行安裝。在您透過管理主控台進行遠端安裝安全應用程式的時候，您可以將網路代理連同安全應用程式一起安裝。

網路代理根據相應的 Kaspersky 應用程式不同而不同。在某些情況下，網路代理僅能在本機進行安裝。（有關詳細資訊，請參閱其應用程式的手冊）。您僅必須安裝網路代理到用戶端裝置一次。

Kaspersky 應用程式 使用管理外掛程式透過管理主控台管理。因此，要透過卡巴斯基安全管理中心存取應用程式管理介面，必須在管理員工作站上安裝相應管理外掛程式。

您可以在管理員工作站的卡巴斯基安全管理中心主視窗執行應用程式遠端安裝。

要進行遠端軟體佈署，您必須先建立一個遠端軟體安裝的工作。

您建立的遠端軟體安裝的工作，將會依照您指定的排程進行。您可以手動停止工作，來中斷安裝過程。

如果應用程式的遠端安裝傳回錯誤，請確保滿足裝置準備要求。

您可以使用佈署報告來偵錯 Kaspersky 程式的遠端安裝進度。

關於卡巴斯基安全管理中心列出的應用程式的管理的詳細資訊，請參閱其相對應的文件。

取代協力廠商安全應用程式

透過卡巴斯基安全管理中心進行 Kaspersky 安全應用程式的安裝可能需要移除與正在安裝的應用程式不相容的協力廠商軟體。卡巴斯基安全管理中心提供幾種移除協力廠商應用程式的方法。

透過使用安裝程式移除不相容應用程式

該選項僅在基於 Microsoft 管理主控台的管理主控台可用。

移除不相容應用程式的安裝程式方法被各種應用程式支援。如果在該安全應用程式安裝套件的內容視窗中選取（**不相容的應用程式**區域）**自動解除安裝不相容的應用程式**選項，在安裝安全應用程式之前，會自動移除所有不相容的應用程式。

當配置應用程式遠端安裝時移除不相容應用程式

您可以在配置安全應用程式遠端安裝時，啟用**自動解除安裝不相容的應用程式**選項。在基於 Microsoft Management Console (MMC) 的管理主控台，該選項在遠端安裝精靈可用。在卡巴斯基安全管理中心網頁主控台，您可以在防護佈署精靈中找到該選項。當該選項被啟用時，卡巴斯基安全管理中心在安裝安全應用程式到受管理裝置之前移除不相容的應用程式。

說明：

- 管理主控台：使用0遠端安裝精靈移除不相容的應用程式
- 卡巴斯基安全管理中心網頁主控台：安裝前移除不相容的應用程式

透過專用工作移除不相容的應用程式

要移除不相容的應用程式，使用**遠端移除應用程式**工作。該工作應該在安全應用程式安裝工作執行之前執行在裝置。例如，在安裝工作中，您可以選取**在完成其它工作時**作為排程類型，其中其他工作為**遠端解除安裝應用程式**。

該移除方法在安全應用程式無法正確移除不相容應用程式時是很有用的。

管理主控台的操作說明：建立工作。

使用遠端軟體安裝工作安裝應用程式

卡巴斯基安全管理中心允許您遠端安裝應用程式到裝置，使用遠端安裝工作。那些工作透過專門精靈被建立被分配到裝置。要更快和更便捷地分配工作，您可以在精靈視窗中指定裝置（最多 1000 台裝置），使用以下方式之一：

- **選取管理伺服器偵測到的網路裝置**。此種情況下，工作被分配到指定裝置。特定裝置可以包含管理群組的裝置和未配置的裝置。
- **手動指定裝置位址或從清單匯入位址**。您可以指定您要為其分配工作的裝置的 NetBIOS 名稱、DNS 名稱、IP 位址和 IP 子網路。
- **分配工作到裝置分類**。此種情況下，工作被分配到先前建立的分類中的裝置。您可以指定預先定義的分類或您所建立的自訂分類。
- **分配工作到管理群組**。此種情況下，工作被分配到先前建立的管理群組中的裝置。

為避免在未安裝網路代理的用戶端裝置上安裝應用程式時可能出現的問題，您必須按照透過卡巴斯基安全管理中心的遠端安裝工作強制部署中所述進行操作。

安裝應用程式到所選裝置

要安裝應用程式到所選裝置：

1. 在主控台樹狀目錄中，選取**工作**資料夾。
2. 點擊**建立工作**按鈕，執行工作建立。

   新工作精靈啟動。遵照精靈的說明。

   在新增工作精靈的**選取工作類型**視窗的**卡巴斯基安全管理中心管理伺服器**節點中，選取**遠端安裝應用程式**作為工作類型。

   新工作精靈將建立一個在特定裝置上遠端安裝所選應用程式的工作。新建立的工作顯示在**工作**資料夾工作區。
3. 您可以手動執行此工作，或依照您指定的排程進行工作。

遠端安裝工作完成時，所選應用程式將安裝在所選裝置上。

在管理群組中的用戶端裝置上安裝應用程式

要在管理群組中的用戶端裝置上安裝應用程式：

1. 連線控制相關管理群組的管理伺服器。
2. 在主控台樹狀目錄中選取您的管理群組。
3. 在群組工作區中，選取**工作**頁籤。

4. 點擊**建立工作**按鈕，執行工作建立。

   新工作精靈啟動。遵照精靈的說明。

   在新增工作精靈的**選取工作類型**視窗的**卡巴斯基安全管理中心管理伺服器**節點中，選取**遠端安裝應用程式**作為工作類型。

   新工作精靈將建立一個遠端安裝所選應用程式的群組工作。新工作將顯示在**工作**頁籤的管理群組區域中。

5. 您可以手動執行此工作，或依照您指定的排程進行工作。

遠端安裝工作完成時，所選應用程式將安裝在管理群組中的用戶端裝置上。

透過 Active Directory 群組政策安裝應用程式

卡巴斯基安全管理中心可以讓您在受管理裝置上使用 Active Directory 群組政策安裝 Kaspersky 應用程式。

> 您必須連同安裝套件中的網路代理一起安裝，才使用 Active Directory 的群組政策進行安裝應用程式。

使用 Active Directory 的群組政策安裝應用程式，請執行以下操作：

1. 使用遠端安裝精靈開始配置應用程式安裝。
2. 在「遠端安裝精靈」的**定義遠端安裝工作設定**視窗中，選取**在 Active Directory 群組政策中指定安裝套件的安裝**選項。
3. 在遠端安裝精靈的**選取帳戶以存取裝置**視窗，選取**需要帳戶（不使用網路代理）**選項。
4. 在安裝了卡巴斯基安全管理中心的裝置上新增帶有管理員權限的帳戶或包含在「群組政策建立器所有者」網域群組的帳戶。

5. 將權限授予所選帳戶：

   a. 轉到**控制面板→管理工具**，然後開啟**群組政策管理**。

   b. 按一下具有所需網域的節點。

   c. 按一下**委派**區段。

   d. 在**權限**下拉功能表中，選取**連結 GPOs**。

   e. 按一下**新增**。

   f. 在開啟的**選取使用者、電腦或群組**視窗中，選取所需的帳戶。

   g. 按一下**確定**關閉**選取使用者、電腦或群組**視窗。

   h. 在**群組和使用者**清單中，選取剛剛新增的帳戶，然後按一下**進階 → 進階**。

   i. 在**權限項目**清單中，按兩下剛剛新增的帳戶。

   j. 授予以下權限：

      - **建立群組物件**
      - **刪除群組物件**
      - **建立群組政策容器物件**
      - **刪除群組政策容器物件**

   k. 按一下**確定**儲存變更。

6. 按照精靈的說明定義其他設定。

7. 手動執行建立的遠端安裝工作，或等待排程啟動。

啟動該工作之後，將會進行遠端安裝的流程：

1. 工作執行時，以下的物件將會建立在指定裝置上的網域中：

   - 名稱 **Kaspersky_AK{GUID}** 下的群組政策物件 (GPO)。
   - 對應於 GPO 的安全群組。該安全群組包含工作覆蓋的用戶端裝置。安全群組的內容定義了 GPO 的範圍。

2. 在這種情況下，卡巴斯基安全管理中心會直接從程式名為 KLSHARE 的共用網路資料夾在用戶端裝置上安裝程式。在卡巴斯基安全管理中心的安裝資料夾中，系統將建立一個輔助子資料夾，其中包含安裝應用程式所需的 .msi 檔案。

3. 當新裝置新增到此工作範圍內時，這些新電腦將會在下個工作啟動時，自動加入到安全性群組。如果在工作排程中選定**執行略過的工作**選項，則裝置將立即加入安全群組。

4. 當從工作範圍中刪除了裝置，在下個工作啟動時，將會將其安全性群組中刪除。

5. 當您從 Active Directory 中刪除了此工作，GPO、連至 GPO 的連結，還有安全性群組都會刪除。

如果您要透過 Active Directory 安裝其他的程式，您可以手動的進行調整這些設定。例如，這可能會發生在以下狀況：

- 當病毒防護管理員沒有權限進行更動網域中的 Active Directory 時
- 原始安裝套件必須儲存在單獨的網路資源上時
- 當需要將 GPO 連結到特定的 Active Directory 單元時

在 Active Directory 中有以下情況，可使用下列另一種安裝方式：

- 如果直接從卡巴斯基安全管理中心共用資料夾進行安裝，您必須在 GPO 屬性中為所需應用程式指定 .msi 檔案（位於安裝套件的 exec 子資料夾中）。
- 如果必須將安裝套件放置在其他網路資源上，您必須將整個 exec 資料夾的內容複製過去，因為除了副檔名為 .msi 的檔案外，該資料夾還包含建立安裝套件時建立的設定檔。要安裝與該程式相關聯的產品授權金鑰，請將金鑰檔案一起複製到該資料夾中。

在從屬管理伺服器上安裝應用程式

在從屬管理伺服器上安裝應用程式：

1. 與控制相關從屬管理伺服器的管理伺服器建立連線。
2. 請您確定每台從屬管理伺服器都必須有要安裝的應用程式套件。如果任何從屬伺服器缺少安裝套件，請使用安裝套件發佈工作。
3. 透過以下方式，建立在從屬管理伺服器安裝應用程式的工作：
   - 如果要為所選管理群組中的從屬管理伺服器建立工作，請為該群組建立遠端安裝群組工作。
   - 如果您要為特定從屬管理伺服器建立工作，請為特定裝置建立遠端安裝工作。

   佈署工作建立精靈啟動，來指導您建立遠端安裝工作。遵照精靈的說明。

   在新建工作精靈中**選取工作類型**視窗內的**卡巴斯基安全管理中心管理伺服器**區域中，開啟**進階**資料夾，然後選取**將應用程式遠端安裝到從屬管理伺服器**作為工作類型。

   新工作精靈將建立遠端安裝所選應用程式到特定的從屬管理伺服器的工作。
4. 您可以手動執行此工作，或依照您指定的排程進行工作。

遠端安裝工作完成時，所選應用程式將安裝在特定的從屬管理伺服器上。

使用遠端安裝精靈安裝應用程式

要安裝 Kaspersky 應用程式，您可以使用遠端安裝精靈。遠端安裝精靈允許使用特別建立的安裝套件或直接從分發套件來遠端安裝應用程式。

若您要在未安裝網路代理的裝置上正確進行遠端安裝，您必須開啟以下的連接埠：TCP 139 和 445；UDP 137 和 138。預設的情況下，網域中所有裝置將自動被開啟這些連接埠。如果發生網路錯誤，請參閱卡巴斯基安全管理中心知識庫。

要使用遠端安裝精靈來安裝應用程式到所選裝置：

1. 在主控台樹狀目錄中，找到**遠端安裝**資料夾並選取**安裝套件**子資料夾。
2. 在該資料夾的工作區，選取您要安裝的應用程式的安裝套件。
3. 在安裝套件的上下文功能表中，選取**安裝應用程式**。
   遠端安裝精靈開始。
4. 在**選取需要安裝的裝置**視窗中，您可以建立將安裝應用程式的裝置清單：

   - **安裝到受管理裝置群組**

     如果選取該選項，程式將為該裝置群組建立遠端安裝工作。

   - **選取需要安裝的裝置**

     如果選取該選項，程式將為指定的裝置建立遠端安裝工作。這些指定裝置可以包含受管理的裝置和未配置的裝置。

5. 在**定義遠端安裝工作設定**視窗，指定應用程式遠端安裝設定。

在**強制下載安裝套件**設定群組中，指定如何將安裝應用程式所需的檔案分發到用戶端裝置中：

- **使用網路代理**

  如果啟用此選項，安裝套件透過安裝在裝置上的網路代理傳送到用戶端裝置。

  如果停用此選項，則會使用用戶端裝置的作業系統工具傳送安裝套件。

  如果已指派工作給安裝了網路代理的裝置，建議您選取該核取方塊。

  預設情況下已啟用該選項。

- **透過管理伺服器使用作業系統資源**

  如果啟用此選項，檔案將使用用戶端裝置的作業系統工具透過管理伺服器傳輸到用戶端裝置。如果使用者端裝置上未安裝網路代理，但是使用者端裝置與管理伺服器在同一網路，則您可以啟用此選項。

  預設情況下已啟用該選項。

- **透過發佈點使用作業系統資源**

  如果啟用此選項，安裝套件使用作業系統工具透過發佈點傳送到用戶端裝置。如果網路中存在不止一個發佈點，那麼您可以選取本選項。

  如果選取**使用網路代理**方塊，僅在網路代理工具不可用時才透過作業系統工具傳送檔案。

  預設情況下，已經為虛擬管理伺服器上建立的遠端安裝工作選取該選項。

- **安裝嘗試次數**

  如果，執行遠端安裝工作時，卡巴斯基安全管理中心安裝應用程式到受管理裝置失敗超過指定次數，卡巴斯基安全管理中心停止傳送安裝套件到該受管理裝置且不再在該裝置上啟動安裝程式。

  嘗試安裝的次數選項允許您節省受管理裝置資源，以及減少流量（移除、MSI 檔案執行和錯誤訊息）。

  重複的工作啟動嘗試可能提示裝置具有妨礙安裝的問題。管理員應該在指定安裝嘗試次數內解決該問題（例如，透過分配足夠磁碟空間、移除不相容的應用程式或修改妨礙安裝的其他應用程式設定）並重新啟動工作（手動或按排程）。

  如果安裝始終未完成，問題被視為無法解決且後續工作啟動被認為是不必要的資源和流量浪費。

  當工作被建立時，嘗試次數被設定為 `0`。返回錯誤的安裝程式的每次執行都增加計數。

  如果指定的嘗試次數被超過且裝置已準備好應用程式安裝，您可以增加嘗試安裝的次數 參數的值並啟動工作以安裝應用程式。或者，您可以建立新的遠端安裝工作。

定義由其他管理伺服器管理的用戶端裝置做什麼：

- **在所有裝置上安裝**

  應用程式將被安裝到由其他管理伺服器管理的裝置。

  預設情況下已選取此選項。如果您在網路中只有一個管理伺服器，您不必變更該設定。

- **僅安裝到透過該管理伺服器管理的裝置**

  應用程式將僅被安裝到由該管理伺服器管理的裝置。如果您在網路中有多個管理伺服器且需要避免它們之間的衝突，請選取該選項。

定義附加設定：

- **如果已經安裝應用程式則不再重新安裝**

  如果啟用此選項，則如果選定的應用程式已安裝到該用戶端裝置上，將不再重新安裝它。
  如果停用此選項，系統仍將安裝應用程式。
  預設情況下已啟用該選項。

- **在 Active Directory 群組政策中指定安裝套件的安裝**

  如果選取此方塊，安裝套件會使用 Active Directory 的群組政策安裝。
  如果選取網路代理安裝套件，則該方塊可用。
  預設情況下已停用該選項。

6. 在**選取產品授權金鑰**視窗中，選取產品授權金鑰和分發方法：

- **不將產品授權金鑰放置到安裝套件(建議)**

  金鑰被自動分發到所相容的所有裝置：
  - 如果自動分發在金鑰內容中啟用。
  - 如果已建立**新增金鑰**。

- **將產品授權金鑰放置到安裝套件**

  金鑰與安裝套件一起被分發到裝置。

  我們不建議您使用該方法分發金鑰，因為共用讀取存取權限已被啟用到安裝套件儲存區。

如果安裝套件不包含產品授權金鑰，則會顯示**選取金鑰**視窗。
如果安裝套件包含產品授權金鑰，則會顯示**產品授權金鑰內容**視窗，其中含有產品授權金鑰詳情。

7. 在**選取作業系統重新啟動選項**視窗，指定安裝應用程式時需要重新啟動作業系統時裝置是否被重新啟動：

- **不重新啟動裝置**

  如果選取該選項，安全應用程式安裝後裝置不被重新啟動。

- **重新啟動裝置**

  如果選取該選項，安全應用程式安裝後裝置將被重新啟動。

- **提示使用者操作**

  如果選中該選項，則在安裝安全應用程式後，會向使用者顯示通知，告知使用者需要重新啟動裝置。使用「**修改**」連結，您可以修改文字訊息、訊息顯示期限和自動重新啟動時間。

  預設情況下已選定此選項。

- **強制關閉已鎖定連線的應用程式**

  如果啟用此選項，鎖定裝置上的應用程式在重新啟動前被強制關閉。

  預設情況下已停用該選項。

8. 在**選取帳戶以存取裝置**視窗，您可以新增用於啟動遠端安裝工作的帳戶：

   - **不需要帳戶（網路代理已安裝）**

     如果該選項被選中，您不是必須指定一個帳戶，並在該帳戶下執行程式的安裝。將使用執行管理伺服器服務的帳戶執行該工作。

     如果網路代理未安裝在用戶端裝置，則此選項無法使用。

   - **需要帳戶（不使用網路代理）**

     如果您為其分配遠端安裝工作的裝置上未安裝網路代理，請選取此選項。在這種情況下，您可以指定使用者帳戶或 SSH 憑證來安裝應用程式。

     - **本機帳戶**。如果選取此選項，請指定用於執行應用程式安裝程式的使用者帳戶。點擊**新增**按鈕，選擇**本機帳戶**，然後指定使用者帳戶憑據。

       您可以根據情況指定多個帳戶，例如，沒有一個帳戶在分配工作的所有裝置上擁有全部所需權限時。在此情況下，已新增的所有帳戶會用於從上到下按順序執行該工作。

     - **SSH 憑證**。如果要在 Linux 用戶端裝置上安裝應用程式，您可以指定 SSH 憑證而不是指定使用者帳戶。按一下**新增**按鈕，選擇**SSH 憑證**，然後指定憑證的私鑰和公鑰。

       如要產生私密金鑰，您可以使用 ssh-keygen 公用程式。請注意，卡巴斯基安全管理中心支援 PEM 格式的私密金鑰，但 ssh-keygen 公用程式預設為產生 OPENSSH 格式的 SSH 金鑰。卡巴斯基安全管理中心不支援 OPENSSH 格式。要以支援的 PEM 格式建立私密金鑰，請在 ssh-keygen 命令中加入 -m PEM 選項。例如：

       ```
       ssh-keygen -m PEM -t rsa -b 4096 -C "< 使用者電子郵件 >"
       ```

9. 在**開始安裝**視窗點擊**下一步**按鈕，以在所選裝置上建立和啟動遠端安裝工作。

   若**開始安裝**視窗已選取**在遠端安裝精靈完成後不執行工作**選項，遠端安裝工作將不會啟動。您可以稍後手動執行此工作。對應於應用程式安裝套件名稱的工作名稱：**<安裝套件名稱>的安裝**。

要使用遠端安裝精靈來安裝應用程式到管理群組裝置：

1. 連線控制相關管理群組的管理伺服器。
2. 在主控台樹狀目錄中選取您的管理群組。
3. 在該群組的工作區中，點擊**執行操作**按鈕並在下拉清單中選取**安裝應用程式**。

   這將會啟動遠端安裝精靈。遵照精靈的說明。

4. 在此精靈的最後一步，按**下一步**，建立並啟動在所選裝置上的遠端佈署工作。

當遠端安裝精靈完成後，卡巴斯基安全管理中心執行以下操作：

- 為軟體安裝程式，建立一個安裝套件（如果安裝套件先前並沒有被建立）。安裝套件位於**遠端安裝**資料夾的**安裝套件**子資料夾中，名稱會對應應用程式的名稱和版本。您可以使用這些套件進行遠端安裝。
- 您可以為您指定的裝置或是管理群組，建立並啟動遠端安裝工作。新建立的遠端安裝工作會儲存在**工作**資料夾中，或新增至為管理群組建立的工作中。您可以稍後手動執行此工作。對應於應用程式安裝套件名稱的工作名稱：**<安裝套件名稱>的安裝**。

檢視防護佈署報告

您可以使用"防護佈署報告"來監控網路防護佈署的進度。

要檢視防護佈署報告：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。
2. 在節點的工作區中，選取**報告**標籤。
3. 在**報告**資料夾中，選取名為**防護佈署報告**的報告範本。

工作區會顯示報告，其中包含所有聯網裝置防護佈署的資訊。

您可以建立新的防護佈署報告，並制定該報告中要包含的資料類型：

- 用於管理群組
- 用於特別裝置
- 用於裝置分類
- 用於所有裝置

如果安全應用程式被安裝並且即時防護被啟用，卡巴斯基安全管理中心認定防護已被佈署在裝置。

使用管理外掛程式

Kaspersky 應用程式使用管理外掛程式透過管理主控台管理。可透過卡巴斯基安全管理中心管理的每個 Kaspersky 應用程式都會包含管理外掛程式。使用應用程式管理外掛程式，可以在管理主控台中執行以下操作：

- 建立和編輯應用程式政策和工作以及應用程式工作的設定。
- 取得關於應用程式工作和應用程式事件的資訊，以及從用戶端裝置接收的應用程式操作統計資訊。

查看已安裝外掛程式清單及其版本：

1. 在管理主控台樹狀圖中，以滑鼠右鍵按一下**管理伺服器<Server_name>**，然後選擇**內容**。
2. 點擊**進階 → 有關已安裝應用程式管理外掛程式的詳情**。

   已安裝的管理外掛程式及其版本的清單顯示在右側窗格中。

您可以在卡巴斯基安全管理中心初始設定期間執行管理伺服器快速啟動精靈時安裝受管理應用程式的外掛程式。此外，您也可以手動安裝管理外掛程式。

手動安裝管理管理外掛程式：

1. 從卡巴斯基技術支援網頁下載卡巴斯基應用程式的管理外掛程式和所需版本（例如 Kaspersky Endpoint Security for Windows 12.3）。
2. 如果管理主控台正在執行，請將其關閉。
3. 解壓縮下載的外掛程式檔案並執行 klcfginst.msi 或 klcfginst.exe 檔案。請按照安裝精靈的步驟進行操作。
4. 安裝完成後，請執行管理主控台並確保外掛程式顯示在已安裝外掛程式清單中，如上一流程所述。

在安裝支援受管理應用程式快速啟動精靈的管理外掛程式後執行管理主控台時，該精靈會自動啟動。您可以按照受管理應用程式快速啟動精靈的步驟來建立預設的卡巴斯基應用程式政策和工作。只有當您在初始外掛程式安裝後或將管理外掛程式更新至與尚未建立工作和政策的卡巴斯基應用程式的其他版本相容的版本後執行管理主控台時，精靈才會自動啟動。您也可以手動啟動受管理應用程式快速啟動精靈。

要手動啟動受管理應用程式快速啟動精靈：

1. 在主控台樹狀目錄中，選取**管理伺服器**節點。
2. 在管理伺服器節點的上下文功能表中，選取**所有工作 → 受管理應用程式快速啟動精靈**。
3. 受管理應用程式快速啟動精靈啟動。依照精靈步驟建立預設的卡巴斯基應用程式政策和工作。

若要刪除管理外掛程式：

1. 如果管理主控台正在執行，請將其關閉。
2. 開啟 Windows 登錄檔編輯程式。
3. 找到以下金鑰：
   - 32 位元系統：`HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\28\Plugins`。
   - 64 位元系統：`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\28\Plugins`。

   此金鑰包含已安裝的管理外掛程式。對於每個外掛程式，`DisplayName` 值包含外掛程式名稱，`UninstallString` 值包含解除安裝外掛程式的命令。

4. 找到要解除安裝的外掛程式的金鑰，並將其`UninstallString`值複製到剪貼簿。

5. 將值貼到命令字串中並使用系統管理員權限來執行它。

管理外掛程式版本不得早於卡巴斯基受管理應用程式版本。如果您更新裝置上的卡巴斯基應用程式，則必須安裝相同版本的管理外掛程式。

當您開啟在早期版本的外掛程式中建立的政策時，系統將要求您接受卡巴斯基安全網路聲明。

當您解除安裝卡巴斯基安全管理中心網頁主控台時，所有管理外掛程式也會被解除安裝。

如果您在高於受管理應用程式版本的外掛程式版本中開啟並儲存政策，則政策將被更新，並且您將無法在早期版本的外掛程式中開啟它。

應用程式的遠端移除

卡巴斯基安全管理中心允許您從裝置遠端移除應用程式，透過遠端移除工作。那些工作透過專門精靈被建立被分配到裝置。要更快和更便捷地分配工作到裝置，您可以在精靈視窗中指定裝置，使用以下方式之一：

- **選取管理伺服器偵測到的網路裝置**。此種情況下，工作被分配到指定裝置。特定裝置可以包含管理群組的裝置和未配置的裝置。
- **手動指定裝置位址或從清單匯入位址**。您可以指定您要為其分配工作的裝置的 NetBIOS 名稱、DNS 名稱、IP 位址和 IP 子網路。
- **分配工作到裝置分類**。此種情況下，工作被分配到先前建立的分類中的裝置。您可以指定預先定義的分類或您所建立的自訂分類。
- **分配工作到管理群組**。此種情況下，工作被分配到先前建立的管理群組中的裝置。

遠端移除問題

當執行遠端移除協力廠商應用程式時，管理員可能會遇到警告說，“遠端解除安裝已在該裝置上完成，但有警告：要移除的應用程式未安裝。”該問題通常發生在要移除的應用程式僅為目前已登入的單個使用者所安裝時。如果使用者未登入，此類應用程式將不可見，無法進行遠端移除。

該行為與同一裝置上供多個使用者使用的應用程式不同，在後一種情況下，應用程式全球可見，可供裝置的所有使用者存取。

在卡巴斯基安全管理中心內，應用程式登錄檔演算法處理供單個使用者使用的應用程式和供多個使用者使用的應用程式的方式不同：

- 供多個使用者使用的應用程式在已安裝應用程式的即時、最新清單中進行維護。
- 供單個使用者使用的應用程式使用快取機制進行監控。

  如果使用者在應用程式偵測時登入過，卡巴斯基安全管理中心會快取關於該使用者的應用程式的資訊。即時使用者隨後登出，卡巴斯基安全管理中心也會根據快取資料繼續將這些應用程式顯示為已安裝，雖然他們不再在裝置上可見或者可存取。

該差異可能導致卡巴斯基安全管理中心根據快取資料將應用程式辨識為已安裝但是應用程式移除工作失敗，因為當使用者登出時應用程式不可存取。

預設情況下，快取應用程式資料的生命周期設為 30 天。管理員可以修改此設定以縮短快取持續時間，從而盡量減少裝置上顯示的資料和實際應用程式可見性之間的差異。

若要將快取生命周期調整到1小時（3600 秒鐘），請在管理伺服器上執行以下指令：

```
klscflag -fset -pv klserver -n KLNAG_INV_PERUSER_APPS_CACHE_NONACTIVE_SIDS_LIFETIME_SEC
-t d -v 3600
```

執行此指令後，請重啟管理伺服器以便變更生效。

有關已安裝應用程式的資訊來源

網路代理從以下登錄機碼提取關於安裝在 Windows 裝置上的軟體的資訊：

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

  包含關於為所有使用者安裝的應用程式的資訊。
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

  包含關於為所有使用者安裝的應用程式的資訊。
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall

  包含關於為目前使用者安裝的應用程式的資訊。
- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall

  包含關於為特定使用者安裝的應用程式的資訊。

在管理群組中，替用戶端裝置遠端移除應用程式

要在管理群組中，替用戶端裝置遠端移除應用程式：

1. 連線控制相關管理群組的管理伺服器。
2. 在主控台樹狀目錄中選取您的管理群組。
3. 在群組工作區中，選取**工作**頁籤。

4. 點擊**新工作**按鈕，執行工作建立。

   新工作精靈啟動。遵照精靈的說明。

   在新工作精靈的**選取工作類型**視窗中的**卡巴斯基安全管理中心管理伺服器**節點，選取 **進階**資料夾的**遠端解除安裝應用程式**作為工作類型。

   新工作精靈將會建立遠端移除所選應用程式的群組工作。新工作將顯示在**工作**頁籤的管理群組區域中。

5. 您可以手動執行此工作，或依照您指定的排程進行工作。

在此工作結束之後，您所指定的應用程式，將會從此群組的裝置中移除。

從所選裝置中遠端移除應用程式

要從所選裝置中遠端移除應用程式：

1. 在主控台樹狀目錄中，選取**工作**資料夾。

2. 透過點擊**新工作**執行工作。

   新工作精靈啟動。遵照精靈的說明。

   在新工作精靈的**選取工作類型**視窗中的**卡巴斯基安全管理中心管理伺服器**節點，選取 **進階**資料夾的**遠端解除安裝應用程式**作為工作類型。

   新工作精靈將建立一個從特定裝置上遠端移除所選應用程式的工作。新建立的工作顯示在**工作**資料夾工作區。

3. 您可以手動執行此工作，或依照您指定的排程進行工作。

遠端移除工作完成時，所選應用程式從所選裝置上移除。

使用安裝套件

當您建立遠端安裝工作時，系統會使用安裝套件中的參數進行遠端安裝。

安裝套件可能包含金鑰檔案。我們建議您避免共用對包含金鑰檔案的安裝套件的存取。

您可以在日後的相同安裝過程，重複的使用它。

由管理伺服器建立的安裝套件被移至主控台樹狀結構，且放置在**遠端安裝**資料夾下的**安裝套件**子資料夾中。安裝套件儲存於管理伺服器的共用資料夾下的「Packages」子資料夾中。

如果需要，您可以按照**刪除物件安裝套件**安裝套件子資料夾中刪除安裝套件。

請勿手動變更共用資料夾中安裝套件的內容。如果需要，您可以建立安裝套件的副本，進行必要的更改，並建立新的安裝工作。

建立安裝套件

本文介紹建立以下類型的安裝套件的過程：

- 卡巴斯基應用程式的安裝套件
- 被指定的可執行檔的安裝套件
- 卡巴斯基資料庫中應用程式的安裝套件

您不需要手動建立安裝套件以遠端安裝網路代理。系統會在卡巴斯基安全管理中心的安裝期間自動建立此項目並儲存於**安裝套件**資料夾中。如果用於遠端安裝網路代理的安裝套件已經被刪除了，您可以透過在卡巴斯基安全管理中心分發套件的"NetAgent"資料夾中選取"nagent.kud"檔案來重新建立安裝套件。

要建立安裝套件：

1. 連線到必要的管理伺服器。
2. 在主控台樹狀目錄中，選取**進階 → 遠端安裝 → 安裝套件**。
3. 以下列方式之一開始建立新的安裝套件：
   - 右鍵點選**安裝套件**資料夾，然後從上下文選單中選擇**新建→安裝套件**。
   - 右鍵點選安裝套件清單的空白區域，然後從上下文選單中選擇**建立 → 安裝套件**。
   - 在安裝套件清單管理區域，點擊**建立安裝套件**。

   新套件精靈啟動。
4. 透過點擊對應的圖示選擇以下安裝套件類型之一：
   - 卡巴斯基應用程式的安裝套件。
   - 被指定的可執行檔的安裝套件。
   - 卡巴斯基資料庫中應用程式的安裝套件。
5. 指定要建立的安裝套件名稱。
   您可以指定任何名稱。

6. 透過以下方式之一選擇要為其建立安裝套件的應用程式或可執行檔：

   - 按一下**瀏覽**按鈕，然後在標準 Windows**開啟**視窗中選擇位於可用磁碟上所需應用程式的分發套件。

     如果您選擇為卡巴斯基應用程式或指定的可執行檔建立安裝套件，則此選項適用。

   - 按一下**瀏覽**按鈕，在**選擇應用程式**視窗中選擇所需應用程式的分發套件。

     如果您選擇從卡巴斯基資料庫為應用程式建立安裝套件，則此選項適用。

   如果您要為管理伺服器建立安裝套件，請選擇 sc.kud 檔案。sc.kud 檔案位於卡巴斯基安全管理中心分發套件的根資料夾中。

   不在安裝套件參數中顯示授權帳戶的任何細節。

7. 審閱最終使用者產品授權協議和隱私權政策。

   為應用程式建立安裝套件時，您可能會被提示檢視並接受該應用程式的最終使用者授權協議和隱私權政策。

   閱讀這兩份文件。如果您同意產品授權協議和隱私權政策的所有條款，請選中相應的核取方塊接受他們。

   應用程式安裝將在您的裝置上繼續，安裝套件建立將還原。

   如果建立 Kaspersky Endpoint Security for Mac 的安裝套件，您可以選取最終使用者產品授權協議和隱私政策的語言。

8. 如有必要，請啟用系統元件自動安裝。

   如果要從卡巴斯基資料庫為應用程式建立安裝套件，則可以啟用必要係統元件的自動安裝。新安裝套件精靈將顯示指定程式所有的系統元件清單。任何時候都可以在安裝套件內容中存取此清單。

   如果您要建立修補程式安裝套件，則該清單包含部署此修補程式所需的所有系統元件。

9. 點擊**完成**按鈕完成套件建立過程。

一旦新套件精靈執行完畢，新的安裝套件將顯示在主控台樹狀目錄的**安裝套件**資料夾的工作區中。

建立獨立安裝套件

貴組織中您與裝置使用者可使用獨立安裝套件在裝置上手動安裝應用程式。

獨立安裝套件是可執行檔 (installer.exe)，您可將其儲存在網頁伺服器或共用資料夾，或以其他方式傳輸至用戶端裝置。您也能透過電子郵件將連結傳送至獨立安裝套件。在用戶端裝置上，使用者會本機執行已接收檔案而不透過卡巴斯基安全管理中心以安裝應用程式。

請確保未獲授權的人員無法取得獨立安裝套件。

您可以為 Kaspersky 應用程式和 Windows、macOS 和 Linux 平台的協力廠商應用程式建立獨立安裝套件。若要建立協力廠商的應用程式獨立安裝套件，您必須先建立自訂安裝套件。

建立獨立安裝套件的來源是在管理伺服器建立的清單中的安裝套件。

若要建立獨立安裝套件：

1. 在主控台樹狀目錄上，選取**管理伺服器 → 進階 → 遠端安裝 → 安裝套件**。

   系統會顯示可在管理伺服器使用的安裝套件清單。

2. 在安裝套件清單中，選取您要建立獨立安裝套件的安裝套件。

3. 在上下文功能表中，選取**建立獨立安裝套件**。

   獨立安裝套件建立精靈啟動。使用**下一步**按鈕進行精靈。

4. 在精靈的第一頁上，如果您已為 Kaspersky 應用程式選取了安裝套件，並且要與所選應用程式一起安裝網路代理，請確保**網路代理與該應用程式一同安裝**選項已啟用。

   預設情況下已啟用該選項。若您不確認裝置是否安裝網路代理，建議啟用此選項。若網路代理已在裝置上安裝，在安裝含網路代理的獨立安裝套件後，網路代理將會更新至新版本。

   若您停用此選項，網路代理將不會安裝在裝置上，且裝置不會受到管理。

   若管理伺服器已存在所選應用程式的獨立安裝套件，精靈會告知您此資訊。在此情況下，您必須選取以下其中一個動作：

   - **建立獨立安裝套件**。若您要針對新應用程式版本建立獨立安裝套件，並同時希望保留針對先前應用程式版本建立的獨立安裝套件，請選取此選項。新獨立安裝套件會放在另一個資料夾中。
   - **使用存在的獨立安裝套件**。若要使用現有獨立安裝套件，請選取此選項。建立套件的程序將不會啟動。
   - **重新建立存在的獨立安裝套件**。如果您要再次針對相同應用程式建立獨立安裝套件，請選取此選項。獨立安裝套件會放在相同資料夾。

5. 在精靈的下一頁上，請選取**將未配置的裝置移動到此群組**選項並指定您要在網路代理安裝後移動用戶端裝置的管理群組。

   依預設，裝置會移至**受管理裝置**群組。

   若您在網路代理安裝後不要移動用戶端裝置至任何管理群組，請選取**不移動裝置**選項。

6. 在精靈下一頁上，當獨立安裝套件建立程序完成後，會顯示獨立套件建立的結果和獨立安裝套件的路徑。

   您可按一下連結並執行以下任一項目：

   - 開啟有獨立安裝套件的資料夾。
   - 以電子郵件傳送連結至建立的獨立安裝套件。若要執行此動作，您必須啟動電子郵件應用程式。
   - 在網站上發佈連結的範例 HTML 程式碼。系統會在與 TXT 格式相關的應用程式中建立和開啟 TXT 檔案。在檔案中會顯示有屬性的 <a> HTML 標籤。

7. 在精靈的下一頁中，若您要開啟獨立安裝套件清單，啟用**開啟獨立安裝套件清單**選項。

8. 按一下**完成**按鈕。

   獨立安裝套件建立精靈會關閉。

系統會在管理伺服器共用資料夾的 Pkglnst 子資料夾建立和放置獨立安裝套件。您可透過點擊在安裝套件清單上的**檢視獨立安裝套件清單**按鈕檢視獨立安裝套件的清單。

建立自訂安裝套件

您可使用自訂安裝套件進行以下操作：

- 在用戶端裝置安裝應用程式（如文字編輯器），例如以工作方式為依據。
- 建立獨立安裝套件。

自訂安裝套件是有一組檔案的資料夾。建立自訂安裝套件的來源是*封存檔案*。封存檔案內含檔案或必須包含在自訂安裝套件的檔案。建立自訂安裝套件，您可指定命令行參數，例如在靜默模式中安裝應用程式。

若要建立應用程式安裝套件：

1. 在主控台樹狀目錄上，選取**管理伺服器 → 進階 → 遠端安裝 → 安裝套件**。

   系統會顯示可在管理伺服器使用的安裝套件清單。

2. 在安裝套件清單上，點擊**建立安裝套件** 按鈕。

   新套件精靈啟動。使用**下一步**按鈕進行精靈。

3. 在精靈的第一個頁面中，選取**為指定的可執行檔建立安裝套件**。

4. 在精靈的次頁中指定自訂安裝套件名稱。

5. 在精靈的次頁上點擊**瀏覽**按鈕，並在標準版 Windows **開啟**視窗，選擇位於可用磁碟機上的封存檔案以建立自訂安裝套件。

   您可以上傳 ZIP、CAB、TAR 或 TAR.GZ 封存。您無法從 SFX（自行解壓封存）檔案來建立安裝套件。

   檔案會下載至卡巴斯基安全管理中心管理伺服器。

6. 在精靈的次頁中，指定可執行檔的命令行參數。

   您可指定命令行參數以靜默模式從安裝應用程式來安裝套件。您可選擇指定命令行參數。

   如有需要，請指定以下選項：

   - **複製整個資料夾至安裝套件**

     如果可執行檔伴隨應用程式安裝所需的附加檔案，則選擇該選項。在您啟用該選項之前，確保所有所需檔案都儲存在相同資料夾。如果啟用該選項，應用程式新增資料夾的全部內容，包括指定的可執行檔，到安裝套件。

   - **對被卡巴斯基安全管理中心辨識的應用程式轉換設定到建議值**

     如果指定應用程式的資訊被包含在 Kaspersky 資料庫，應用程式將以建議設定安裝。

     如果您在**可執行檔命令列**欄位中資料了參數，它們被使用建議設定重寫。

     預設情況下已啟用該選項。

     Kaspersky 資料庫由 Kaspersky 分析家建立和維護。對於每個新增到資料庫的應用程式，Kaspersky 分析家定義最優的安裝設定。設定被定義以確保成功將應用程式遠端安裝到用戶端裝置。當您執行將更新下載至管理伺服器儲存庫工作時，資料庫在管理伺服器上被自動更新。

   系統會啟動建立自訂安裝套件的程序。

   精靈會通知您程序已完成。

   若未建立自訂安裝套件，系統會顯示適合訊息。

7. 點擊**完成**按鈕以關閉精靈。

您建立的安裝套件會下載至管理伺服器共用資料夾的套件子資料夾。下載後，安裝套件會在自訂安裝套件清單中顯示。

在管理伺服器上的安裝套件清單，您可檢視並編輯自訂安裝套件內容。

檢視與編輯自訂安裝套件的內容

建立自訂安裝套件後，您可檢視安裝套件的一般資訊，並在內容視窗中指定安裝設定。

若要檢視和編輯自訂安裝套件的內容：

1. 在主控台樹狀目錄上，選取**管理伺服器 → 進階 → 遠端安裝 → 安裝套件**。

   系統會顯示可在管理伺服器使用的安裝套件清單。

2. 在安裝套件的上下文功能表中，選取**內容**。

   所選安裝套件的內容視窗開啟。

3. 檢視以下資訊：

- 安裝套件名稱
- 封裝在自訂安裝套件的應用程式名稱
- 應用程式版本
- 安裝套件建立日期
- 前往管理伺服器自訂安裝套件的路徑
- 可執行檔指令行

4. 指定下列設定：

- 安裝套件名稱
- **安裝所需的一般系統元件**

  如果啟用該選項，在安裝更新之前，應用程式自動安裝所需的所有一般系統元件（先決條件）。例如，這些先決條件可以是作業系統更新。

  如果停用該選項，您可能必須手動安裝先決條件。

  預設情況下已停用該選項。

  此選項僅在卡巴斯基安全管理中心可識別新增至安裝套件的應用程式時可用。

- **可執行檔命令列**

  如果應用程式需要更多參數以進行靜默安裝，在該欄位指定它們。參考供應商文件以獲取詳情。

  您也可以輸入其他參數。

  此選項僅在套件不是在 Kaspersky 應用程式建立時可用。

5. 點擊**確定**或**套用**按鈕以儲存變更（如有）。

新設定已儲存。

從卡巴斯基安全管理中心分發套件獲取網路代理安裝套件

您可以從從卡巴斯基安全管理中心分發套件獲取網路代理安裝套件，而無需安裝卡巴斯基安全管理中心。然後您可以使用安裝套件在用戶端裝置上安裝網路代理。

要從卡巴斯基安全管理中心分發套件獲取網路代理安裝套件:

1. 從卡巴斯基安全管理中心分發套件執行 ksc <版本號>.<內部版本號>_full_<中文化語言>.exe 可執行檔。
2. 在開啟的視窗中，點擊**抽取安裝套件**連接。

3. 在安裝套件清單中，選中網路代理安裝套件旁邊的核取方塊，然後點擊**下一步**按鈕。

4. 如有必要，點擊**瀏覽**按鈕變更顯示的資料夾以解壓縮安裝套件。

5. 按一下**抽取**按鈕。
   應用程式將解開網路代理安裝套件。

6. 過程完成後，按一下**關閉**按鈕。

網路代理安裝套件被解開到選定的資料夾。

您可以用以下方法之一使用安裝套件來安裝網路代理：

- 本機，透過執行解開資料夾的 setup.exe 檔案
- 透過靜默安裝
- 透過使用 Microsoft Windows 群組政策

分發安裝套件至從屬管理伺服器

若要分發安裝套件至從屬管理伺服器：

1. 與控制相關從屬管理伺服器的管理伺服器建立連線。

2. 使用以下其中一種方式，建立向從屬管理伺服器發佈安裝套件的工作：

   - 如果您要管理群組中的從屬管理伺服器建立發佈套件工作，您可以在群組工作中建立此工作。
   - 如果您要為指定的從屬管理伺服器建立發佈套件的工作，您可以在指定裝置工作中建立該工作。

   新工作精靈啟動。遵照精靈的說明。
   在新工作精靈的**選取工作類型**視窗中的**卡巴斯基安全管理中心管理伺服器**節點，選取 **進階**資料夾的**Distribute installation package**作為工作類型。
   新工作精靈將會建立發佈所選安裝套件到特定從屬管理伺服器的工作。

3. 您可以手動執行此工作，或等候工作設定中指定的排程將其啟動。

所選安裝套件將會複製到指定的從屬管理伺服器上。

透過發佈點分發安裝套件

您可以使用發佈點，在管理群組內發佈安裝套件。

當從管理伺服器收到安裝套件後，發佈點將利用 IP 群播分發，自動發佈套件給其用戶端裝置。管理群組中安裝套件的 IP 多點傳送僅發生一次。如果發佈的過程中，用戶端裝置與公司網路中斷連線，當安裝工作啟動時，網路代理將自動從發佈點的裝置上下載安裝套件進行安裝。

將應用程式佈署結果傳回至卡巴斯基安全管理中心

在您建立了應用程式安裝套件後，您可以對其進行設定以便所有應用程式安裝結果的診斷資訊都會被傳回至卡巴斯基安全管理中心。對於 Kaspersky 應用程式安裝套件，程式安裝結果的傳輸或診斷資訊預設已被設定，無需多餘的設定。

要為安裝到卡巴斯基安全管理中心的應用程式設定診斷資訊：

1. 導航至由卡巴斯基安全管理中心為所選應用程式建立的安裝套件資料夾。您可以在安裝卡巴斯基安全管理中心時指定的共用資料夾中找到該資料夾。

2. 開啟副檔名為 .kpd 或 .kud 的檔案進行編輯（比如在 Microsoft Windows Notepad 編輯器中編輯）。

   此檔案的格式與一般的 .ini 檔案格式相同。

3. 在檔案中新增以下行列：

   ```
   [SetupProcessResult]
   Wait=1
   ```

   此指令設定卡巴斯基安全管理中心等待安裝套件要建立的應用程式設定完畢並分析安裝程式的回傳值。如果您要關閉其回傳診斷資料，您可以把值設為 0。

4. 新增成功安裝的回傳值。若要新增此功能，請新增以下行列到該檔案中：

   ```
   [SetupProcessResult_SuccessCodes]
   <return code>=[<description>]
   <return code 1>=[<description>]
   ...
   ```

   > 中括號包含了可選的值。

   命令列的語法：

   - `<return code>`。安裝程式所對應的任何數字。回傳值的數字是任意的。
   - `<description>`。安裝結果的文字說明。您可忽略此說明。

5. 新增安裝失敗的回傳值的說明。若要新增此功能，請新增以下行列到該檔案中：

   ```
   [SetupProcessResult_ErrorCodes]
   <return code>=[<description>]
   <return code 1>=[<description>]
   ...
   ```

   此語法與成功安裝的回傳值語法相同。

6. 儲存所有變更，關閉 .kpd 或 .kud 檔案。

關於使用者定義的應用程式的安裝結果將儲存在卡巴斯基安全管理中心的記錄中，並將顯示在事件清單、報告和工作記錄中。

定義安裝套件的 KSN 代理伺服器位址

如果管理伺服器的位址或域發生變化，您可以為安裝套件定義 KSN 代理伺服器位址。

若要為安裝套件定義 KSN 代理伺服器位址：

1. 在主控台樹狀目錄中，在**遠端安裝**資料夾，按兩下**安裝套件**子資料夾。
2. 在開啟的功能表中，選取**內容**。
3. 在開啟的內容視窗中，選取**一般**子區段。
4. 在內容視窗的**一般**子區段中，輸入 KSN 代理伺服器的位址。

安裝套件會預設使用這個位址。

接收最新的應用程式版本

卡巴斯基安全管理中心允許您接收儲存在 Kaspersky 伺服器上的最新企業應用程式版本。

要從 Kaspersky 接收企業應用程式的最新版本：

1. 執行以下操作之一：

   - 在主控台樹狀目錄中，選取節點及所需管理伺服器的名稱，確認選取**監控**頁籤，然後在**佈署**區域中按一下**有 Kaspersky 應用程式的新版本可用**連結。

     當管理伺服器在 Kaspersky 伺服器找到新版本企業應用程式時可顯示**有 Kaspersky 應用程式的新版本可用**連結。

   - 在主控台樹狀目錄中，選取**進階 → 遠端安裝 → 安裝套件**，然後在工作區中按一下**附加操作**，並從下拉式清單中選取**檢視 Kaspersky 應用程式的目前版本**。

   會顯示 Kaspersky 應用程式目前版本的清單。

2. 您可以篩選 Kaspersky 應用程式清單，藉此簡化對所需應用程式的搜尋。
   在**最新應用程式版本**視窗的頂部，點擊**篩選器**連接以按以下條件篩選應用程式清單：

   - **元件**。使用此標準，可按照您網路上正在使用的保護區域篩選 Kaspersky 應用程式清單。
   - **已下載軟體的類型**。使用此標準，可按照應用程式類型篩選 Kaspersky 應用程式清單。
   - **要顯示的軟體產品和更新**。使用此標準，可按照特定版本顯示可用的卡巴斯基應用程式。
   - **軟體和更新的顯示語言**。使用此標準，可顯示具有特定本地化語言的 Kaspersky 應用程式。

   點擊**套用**按鈕套用選定的篩選器。

3. 在清單中選取您所需要的應用程式。

4. 透過點選在**分發套件網址**中的連結下載應用程式分發套件。

> 受管理應用程式的更新可能需要安裝卡巴斯基安全管理中心特定的最低版本。如果此版本晚於目前版本，則顯示這些更新，但無法核准。同樣，在升級卡巴斯基安全管理中心之前，無法從此類更新中建立安裝軟體套件。提示您將卡巴斯基安全管理中心執行個體升級到所需的最低版本。

如果所選應用程式的**下載應用程式並建立安裝套件**按鈕顯示，您可以點選這個按鈕來下載應用程式分發套件並自動建立安裝套件。卡巴斯基安全管理中心下載應用程式分發套件到管理伺服器，儲存於安裝卡巴斯基安全管理中心時指定的共用資料夾下。自動建立的安裝套件顯示在主控台樹狀目錄**遠端安裝**資料夾的**安裝套件**子資料夾中。

之後**最新應用程式版本**視窗關閉，**有 Kaspersky 應用程式的新版本可用**連結會從**佈署**區段中消失。

您可以為新版本應用程式建立安裝套件，並在主控台樹狀目錄的**遠端安裝**資料夾的**安裝套件**子資料夾中管理新建立的安裝套件。

您也可點擊**安裝套件**資料夾工作區的**檢視 Kaspersky 應用程式的目前版本**連結來開啟**最新應用程式版本**視窗。

準備好用於遠端安裝的 Windows 裝置

遠端安裝應用程式到用戶端裝置時可能會因下列原因發生錯誤：

- 安裝的工作已經成功在此裝置上執行。
  在此狀況下，工作無須再重複執行。
- 工作開始後，裝置被關閉。
  在此情況下，開啟裝置，然後重新啟動工作。
- 用戶端的網路代理與管理伺服器並無連線。
  要確定問題原因，請使用用戶端裝置的遠端診斷實用程式 (klactgui)。
- 如果網路代理未安裝在裝置上，遠端安裝過程中可能會發生以下狀況：
  - 用戶端裝置已啟用**停用檔案簡易共用**。
  - 用戶端裝置上未執行伺服器服務。
  - 用戶端裝置上的所需連接埠被關閉。
  - 用來執行該工作的帳戶權限不足。

  為避免在未安裝網路代理的用戶端裝置上安裝應用程式時可能出現的問題，您必須按照透過卡巴斯基安全管理中心的遠端安裝工作強制部署中所述進行操作。

> 之前，riprep 公用程式用來為裝置準備遠端安裝。現在，這被認為是過時的作業系統配置方法。不建議在比 Windows XP 和 Windows Server 2003 R2 更新的作業系統上使用 riprep 公用程式。

準備 Linux 裝置並在 Linux 裝置上遠端安裝網路代理

網路代理安裝套件括兩個步驟：

- Linux 裝置準備
- 網路代理遠端安裝

Linux 裝置準備

要準備執行 Linux 的裝置以遠端安裝網路代理：

1. 確保您要在上面安裝 Network Agent for Linux 的裝置執行受支援的 Linux 版本。
2. 使用應用程式介面或從卡巴斯基網站下載網路代理安裝套件。
3. 確保目標 Linux 裝置上已安裝下列軟體：
   - Sudo（對於 Ubuntu 10.04，Sudo 版本為 1.7.2p1 或者更高）
   - Perl 語言解譯器 5.10 或更高版本
4. 測試裝置配置：
   a. 檢查是否您可以透過 SSH 用戶端（例如 PuTTY）連線到裝置。
   如果您無法連線到裝置，開啟檔案 `/etc/ssh/sshd_config` 並確保以下設定具有以下相關值：
   ```
   PasswordAuthentication no
   ChallengeResponseAuthentication yes
   ```
   > 如果您可以毫無問題地連線到裝置，請不要修改 /etc/ssh/sshd_config 檔案；否則在執行遠端安裝工作時可能會遇到 SSH 認證失敗的情況。
   儲存檔案（如果必要）並使用 `sudo service ssh restart` 命令來重新啟動 SSH 服務。
   b. 停用要連線裝置的使用者帳戶的 sudo 密碼。
   c. 使用 sudo 的 `visudo` 指令開啟 sudoers 設定檔。
   在開啟的檔案中，新增以下行到檔案結尾：<使用者名稱> `ALL = (ALL) NOPASSWD: ALL`。此種情況下，< 使用者名稱 >是用於透過 SSH 進行裝置連線的使用者帳戶。如果您使用的是 Astra Linux 作業系統，請在 /etc/sudoers 檔案的最後一行新增以下文字：`%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`
   d. 儲存並關閉 sudoers 檔案。
   e. 透過 SSH 再次連線裝置並確保 Sudo 服務不提示您輸入密碼；您可以使用 `sudo whoami` 指令來操作。

5. 開啟 `/etc/systemd/logind.conf` 檔案，接著執行以下操作之一：

   - 指定 no 為 KillUserProcesses 設定的值：`KillUserProcesses=no`。
   - 對於 KillExcludeUsers 設定，請輸入執行遠端安裝之帳戶的使用者名稱，例如：`KillExcludeUsers=root`。

   如果目標裝置正在執行 Astra Linux，在 `/home/<` 使用者名稱 `>/.bashrc` 檔案中新增 `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` 子串，其中 `<` 使用者名稱 `>` 是用於使用 SSH 進行裝置連線的使用者帳戶。

   若要套用變更的設定，請重新啟動 Linux 裝置或執行以下命令：

   ```
   $ sudo systemctl restart systemd-logind.service
   ```

6. 如果您想在裝有 SUSE Linux Enterprise Server 15 作業系統的裝置上安裝網路代理，請首先安裝 insserv-compat 套件配置網路代理。

7. 如果要在封閉軟體環境模式下執行 Astra Linux 作業系統的裝置上安裝網路代理，請執行額外的步驟來準備 Astra Linux 裝置。

8. 如果要在作業系統為 RED OS 7.3.4 或更高版本或者 MSVSPHERE 9.2 或更高版本的裝置上安裝網路代理，請安裝 libxcrypt-compat 套件以便網路代理正確運作。

網路代理遠端安裝

要在 Linux 裝置上遠端安裝網路代理：

1. 下載並建立安裝套件：

   a. 在裝置上安裝之前，請確保該安裝套件安裝了所有的先決條件（程式和庫）。

   您可以自己檢視每個安裝套件的先決條件，使用 Linux 分發套件的實用工具。有關更多公用程式的詳情，請參閱您的作業系統文件。

   b. 要建立遠端安裝套件，使用以下檔案：

   - klnagent.kpd
   - akinstall.sh
   - 網路代理的 .deb 或 .rpm 套件

2. 使用以下設定建立遠端安裝工作：

   - 在新工作精靈的**設定**頁面，選取**透過管理伺服器使用作業系統資源**核取方塊。清空所有其他核取方塊。
   - 在**選取要執行此工作的帳戶**頁面，請指定透過 SSH 進行裝置連線的使用者帳戶設定。

3. 執行遠端安裝工作。使用 `su` 指令的選項保存環境：`-m, -p, --preserve-environment`。

準備一部執行 SUSE Linux Enterprise Server 15 的裝置以安裝網路代理

要在裝有 SUSE Linux Enterprise Server 15 作業系統的裝置上安裝網路代理，

在安裝網路代理之前，執行以下指令：

```
$ sudo zypper install insserv-compat
```

這使您能夠安裝 insserv-compat 套件並正確配置網路代理。

執行 `rpm -q insserv-compat` 指令來檢查套件是否已經安裝。

如果您的網路包含大量執行 SUSE Linux Enterprise Server 15 的裝置，您可以使用用來配置和管理公司基礎結構的特殊軟體。透過使用此軟體，您可以一次在所有必要的裝置上自動安裝 insserv-compat 套件。例如，您可以使用 Puppet、Ansible、Chef，或者製作自己的指令碼 — 使用任何方便的方法。

如果裝置沒有 SUSE Linux Enterprise 的 GPG 簽名金鑰，您可能會遇到以下警告：`Package header is not signed!` 選擇 `i` 選項略過警告。

除了安裝 insserv-compat 套件外，請確保您已完全準備好 Linux 裝置。之後，部署和安裝網路代理。

準備 macOS 裝置以遠端安裝網路代理

要準備執行 macOS 的裝置以遠端安裝網路代理：

1. 確保目的 macOS 裝置上安裝了 sudo。
2. 測試裝置配置：
   a. 確保用戶端裝置上已開啟連接埠 22。若要開啟，請在**系統偏好設定**開啟**共用**窗格，然後確認已勾選**遠端登入**核取方塊。

      您只能透過連接埠 22 經由 Secure Shell (SSH) 連線到用戶端裝置。您不能更改連接埠號。

      您可以使用 `ssh <device_name>` 命令，遠端登入 macOS 裝置。在**共用**窗格中，您可以使用**允許存取**選項，設定可以存取 macOS 裝置的使用者範圍。

   b. 停用要連線裝置的使用者帳戶的 sudo 密碼。

      在終端中使用 `sudo visudo` 指令開啟 sudoers 設定檔。在您開啟的檔案中，於 使用者權限指定 項目中指定下列內容：`username ALL = (ALL) NOPASSWD: ALL`。此種情況下，`username` 代表透過 SSH 進行裝置連線的使用者帳戶。

   c. 儲存並關閉 sudoers 檔案。

   d. 透過 SSH 再次連線裝置並確保 Sudo 服務不提示您輸入密碼；您可以使用 `sudo whoami` 指令來操作。

3. 下載並建立安裝套件：

   a. 使用下列其中一種方法下載網路代理安裝套件：

      - 在主控台樹狀目錄中，開啟**遠端安裝 → 安裝套件**的內容功能表，然後選取**顯示最新應用程式版本**以從可用的套件中進行選擇
      - 從技術支援網站 https://support.kaspersky.com/ 下載相關的網路代理版本
      - 請技術支援專家提供安裝套件

   b. 要建立遠端安裝套件，使用以下檔案：

      - klnagent.kud
      - install.sh
      - klnagentmac.dmg

4. 使用以下設定建立遠端安裝工作：

   - 在新工作精靈的**設定**頁面，選取**透過管理伺服器使用作業系統資源**核取方塊。清空所有其他核取方塊。
   - 在**選取要執行此工作的帳戶**頁面，請指定透過 SSH 進行裝置連線的使用者帳戶設定來執行工作。

用戶端裝置已準備就緒，可供您透過自行建立的對應工作來遠端安裝網路代理。

Kaspersky 應用程式：產品授權和啟動

本章節說明使用受管理的 Kaspersky 應用程式產品授權金鑰的卡巴斯基安全管理中心功能。

卡巴斯基安全管理中心使您可以集中為用戶端裝置上的 Kaspersky 應用程式分發產品授權金鑰、監控其使用情況，以及續約產品授權。

使用卡巴斯基安全管理中心新增產品授權金鑰時，該金鑰的設定會儲存在管理伺服器上。應用程式會根據該資訊產生一份產品授權金鑰使用情況的報告，並通知管理員產品授權金鑰內容中指定的產品授權期滿日期，以及是否違反此限制。您可以在管理伺服器設定內配置產品授權金鑰使用情況的通知。

受管理應用程式的產品授權

安裝到受管理裝置上的 Kaspersky 應用程式必須透過套用產品金鑰檔案或啟動碼到每個應用程式而被授權。金鑰檔案或啟動碼可以按以下方法佈署：

- 自動佈署
- 受管理應用程式安裝套件
- 受管理應用程式的「*新增產品授權金鑰*」工作
- 受管理應用程式的手動啟動

您可以透過上面列出的任何方法新增啟動或備用產品授權金鑰。卡巴斯基應用程式當前使用一個啟動金鑰並儲存一個備用金鑰以在啟動金鑰到期後套用。您為其新增產品授權金鑰的應用程式定義該金鑰是啟動還是備用金鑰。金鑰定義不依賴於您用於新增產品授權金鑰的方法。

自動佈署

如果您使用不同的受管理應用程式且您必須佈署特定金鑰檔案或啟動碼到裝置，請選取其他方法佈署啟動碼或金鑰檔案。

卡巴斯基安全管理中心允許您自動佈署可用產品授權金鑰到裝置。例如，三個產品授權金鑰被儲存在管理伺服器儲存區。您已為所有三個產品授權金鑰選取**自動分發產品授權金鑰到受管理裝置**核取方塊。Kaspersky 安全應用程式—例如，Kaspersky Endpoint Security for Windows—被安裝到組織裝置。發現必須佈署產品授權金鑰的新裝置。應用程式決定，例如，儲存區中的兩個產品授權金鑰可以被佈署到裝置：產品授權金鑰 *Key_1*和產品授權金鑰 *Key_2*。這些產品授權金鑰之一被佈署到裝置。此種情況下，無法預見兩個產品授權金鑰中的哪個將被佈署到裝置，因為自動佈署產品授權金鑰不提供給任何管理員活動。

當佈署產品授權金鑰時，裝置為該產品授權金鑰重新計算。您必須確保佈署產品授權金鑰的裝置數量不超過產品授權限制。如果裝置數量超過產品授權限制，所有不被產品授權覆蓋的裝置將被分配緊急狀態。

佈署之前，您必須新增產品授權金鑰或啟動碼到管理伺服器儲存區。

說明：

- 管理主控台：
  - 新增產品授權金鑰到管理伺服器儲存區
  - 自動分發產品授權金鑰

  或
- 卡巴斯基安全管理中心網頁主控台：
  - 新增產品授權金鑰到管理伺服器儲存區
  - 自動分發產品授權金鑰

請注意，在以下情況下，自動分發的產品授權金鑰可能不會顯示在虛擬管理伺服器儲存庫中：

- 產品授權金鑰對於應用程式無效。
- 虛擬管理伺服器沒有受管理裝置。
- 產品授權金鑰已用於由另一個虛擬管理伺服器管理的裝置，並且已達到裝置數量限制。

新增金鑰檔案或啟動碼至受管理應用程式安裝套件

對於安全應用程式，該選項不被建議。新增至安裝套件的產品授權金鑰或啟動碼可能會有安全風險。

如果您使用安裝套件安裝受管理應用程式，您可以在該安裝套件中或在應用程式政策中指定啟動碼或金鑰檔案。產品授權金鑰將在下一次裝置與管理伺服器同步時被佈署到受管理裝置。

說明：

- 管理主控台：
  - 建立安裝套件
  - 安裝應用程式到用戶端裝置

  或
- 卡巴斯基安全管理中心網頁主控台：新增產品授權金鑰到安裝套件

透過為受管理應用程式新增產品授權金鑰工作佈署。

如果您選擇為受管理應用程式*新增產品授權金鑰*工作，您可以選取要佈署到裝置的產品授權金鑰，並以任何便捷方法選取裝置—例如，選取管理群組或裝置分類。

佈署之前，您必須新增產品授權金鑰或啟動碼到管理伺服器儲存區。

說明：

- 管理主控台：
  - 新增產品授權金鑰到管理伺服器儲存區
  - 佈署產品授權金鑰到用戶端裝置

  或
- 卡巴斯基安全管理中心網頁主控台：
  - 新增產品授權金鑰到管理伺服器儲存區
  - 佈署產品授權金鑰到用戶端裝置

手動新增啟動碼或金鑰檔案至裝置

您可以啟動本機安裝的 Kaspersky 應用程式，透過使用應用程式介面提供的工具。請參考已安裝應用程式的文件。

檢視使用中產品授權金鑰的相關資訊

要檢視使用中產品授權金鑰的相關資訊，

在主控台樹狀目錄中，選取**Kaspersky 產品授權**資料夾。

資料夾工作區將顯示用戶端裝置上使用的產品授權金鑰清單。

產品授權金鑰旁邊會顯示一個圖示，指示使用類型：

-  – 已從連線至管理伺服器的用戶端裝置上收到產品授權金鑰的相關資訊。該產品授權金鑰檔案儲存在管理伺服器之外。
-  —授權檔案儲存在管理伺服器儲存區中。已停用該產品授權金鑰的自動分發。
-  —授權檔案儲存在管理伺服器儲存區中。已啟用該產品授權金鑰的自動分發。

您可透過開啟用戶端裝置內容視窗的**應用程式** 區域，檢視用來啟動用戶端裝置應用程式的產品授權金鑰的資訊。

要定義虛擬管理伺服器產品授權金鑰的即時設定，管理伺服器每天至少傳送一次請求到 Kaspersky 啟動伺服器。如果無法使用系統 DNS 存取伺服器，則應用程式使用公用 DNS 伺服器。

如果產品授權金鑰從用戶端裝置收到，則無法將其作為檔案匯出。

新增產品授權金鑰到管理伺服器儲存區

要新增產品授權金鑰到管理伺服器儲存區：

1. 在主控台樹狀目錄中，選取**Kaspersky 產品授權**資料夾。
2. 使用以下方法之一啟動產品授權金鑰的新增工作：
   - 透過從產品授權金鑰上下文功能表中，選取**新增啟動碼或金鑰檔案**。
   - 在產品授權金鑰清單的工作區中，點擊**新增啟動碼或金鑰檔案**連結。
   - 點擊**新增啟動碼或金鑰檔案**按鈕。

   新增產品授權金鑰精靈啟動。
3. 選擇如何啟動管理伺服器：使用啟動碼或使用金鑰檔案。
4. 指定您的啟動碼或金鑰檔案。
5. 如果您想立即在網路上分發相關的產品授權金鑰，請選擇**自動分發產品授權金鑰到受管理裝置**選項。如果不選擇此選項，您可以之後手動分發產品授權金鑰。

結果，金鑰檔案下載，新增產品授權金鑰精靈完成。您現在可以在卡巴斯基產品授權清單中看到新增的產品授權金鑰。

新增管理伺服器產品授權金鑰

要新增管理伺服器產品授權金鑰：

1. 在管理伺服器的上下文功能表中，選取**內容**。
2. 在開啟的管理伺服器內容視窗中，選取**產品授權金鑰**區段。
3. 在**「啟動產品授權金鑰」**區段中，按一下**「編輯」**按鈕。
4. 在開啟的視窗中，按一下**「新增」**按鈕新增產品授權金鑰。
   新增產品授權金鑰精靈啟動。

精靈完成後，您可以根據相應的產品授權檢查管理主控台中是否顯示了這些功能。

移除管理伺服器產品授權金鑰

要移除管理伺服器產品授權金鑰：

1. 在管理伺服器的上下文功能表中，選取**內容**。
2. 在開啟的管理伺服器內容視窗中，選取**產品授權金鑰**區段。
3. 透過點擊**移除**按鈕來移除產品授權金鑰。

過會移除產品授權金鑰。

若已新增備用產品授權金鑰，備用產品授權金鑰會在移除先前啟用的產品授權金鑰後，自動成為啟動產品授權金鑰。

管理伺服器的目前產品授權金鑰被移除後，弱點和修補程式管理和行動裝置管理功能將不可用。您可以再次新增一個已移除的產品授權金鑰或新增一個新產品授權金鑰。

佈署產品授權金鑰到用戶端裝置

卡巴斯基安全管理中心允許您使用*產品授權金鑰發佈*工作將產品授權金鑰發佈至用戶端裝置。

部署前，請新增產品授權金鑰到管理伺服器儲存區。

要將產品授權金鑰分發至用戶端裝置，請執行以下操作：

1. 在主控台樹狀目錄中，選取**Kaspersky 產品授權**資料夾。
2. 在產品授權金鑰清單的工作區，點擊**自動分發產品授權金鑰到受管理裝置**按鈕。
   應用程式啟動工作建立精靈會啟動。使用**下一步**按鈕進行精靈。

3. 在應用程式清單中，選取您要為其建立工作的應用程式。

4. 在精靈的**「新增金鑰」**步驟中，使用下列選項之一新增產品授權金鑰：

   - 選擇**啟動碼**選項以從卡巴斯基安全管理中心儲存區新增啟動碼。

     點擊**選取**。在開啟的視窗中，選擇啟動碼，然後按一下**確定** 。

   - 選擇**金鑰檔案或金鑰**選項，然後執行以下操作：

     a. 點擊**選取**。

     b. 在上下文功能表中，選擇以下選項之一：

     - **資料夾中的金鑰檔案**。

       在開啟的視窗中，從您的裝置中選擇金鑰檔案，然後按一下**開啟**。

     - **來自卡巴斯基安全管理中心儲存區的金鑰**。

       在開啟的視窗中，從卡巴斯基安全管理中心儲存區中選擇金鑰，然後按一下**確定**。

5. 如果要取代作用中產品授權金鑰，請清除預設的**用作備用金鑰**核取方塊。

   例如，當組織發生變化並且裝置上需要另一個組織的金鑰時，或者重新頒發了金鑰、新產品授權早於目前的產品授權到期時，就需要這樣做。為了避免錯誤，您必須清除**用作備用金鑰**核取方塊。

   如果您想了解有關將產品授權金鑰新增到卡巴斯基安全管理中心 Windows 時可能出現的問題及其解決方法的更多資訊，請參閱卡巴斯基安全管理中心知識庫。

6. 檢查產品授權金鑰資訊，然後點擊**下一步**。

7. 在精靈的此步驟中，選擇要向其指派新增金鑰工作的裝置。您可以使用下列可用方法之一指定裝置（最多 1000 個裝置）：

   - **選取管理伺服器偵測到的網路裝置**。此種情況下，工作被分配到指定裝置。特定裝置可以包含管理群組的裝置和未配置的裝置。

   - **手動指定裝置位址或從清單匯入位址**。您可以指定您要為其分配工作的裝置的 NetBIOS 名稱、DNS 名稱、IP 位址和 IP 子網路。

   - **分配工作到裝置分類**。此種情況下，工作被分配到先前建立的分類中的裝置。您可以指定預先定義的分類或您所建立的自訂分類。

   - **分配工作到管理群組**。此種情況下，工作被分配到先前建立的管理群組中的裝置。

8. 在精靈的**設定工作排程**步驟，為啟動工作建立排程：

- **排程開始**:
  - **一次**

    此工作在指定的日期和時間（預設情況下，在建立工作的當天）執行一次。

  - **手動**

    工作不自動執行。您僅可以手動啟動。

    預設情況下已選定此選項。

  - **當新更新下載至儲存區時**

    工作會在更新下載至儲存區時執行。例如，您可能希望使用此排程進行「尋找弱點和必要更新」工作。

  - **在偵測到病毒爆發時**

    工作在發生*病毒爆發*事件後執行。選取將監控病毒爆發的應用程式類型。有下列應用程式類型可用：
    - 病毒防護工作站和檔案伺服器
    - 用於週邊防護的防毒軟體
    - 用於郵件伺服器的防毒軟體

    預設情況下選定所有應用程式類型。

    您可能想根據報告病毒爆發的安全應用程式類型執行不同的工作。此種情況下，刪除您不需要的應用程式類型選項。

  - **在完成其它工作時**

    目前工作在其他工作完成後啟動。您可以選取先前工作如何結束（成功或帶有錯誤）以觸發目前工作的啟動。例如，您可能想使用***Turn on the device***選項執行開啟裝置工作，完成後，請執行*惡意軟體掃描*工作。只有當這兩項工作都被分配給相同的裝置時，此參數才會有作用。

- **執行錯過的工作**

  該選項決定在工作要啟動時用戶端裝置在網路中不可見時工作的行為。

  如果啟用該選項，系統將在下一次在用戶端裝置上執行 Kaspersky 應用程式時嘗試啟動工作。如果工作排程是**手動**、**一次**或**立即**，裝置在網路中可見或包含在工作範圍後，工作會立即啟動。

  如果停用此選項，則僅限排程的工作會在用戶端裝置上執行。若為**手動**、**一次**與**立即**排程，工作僅會在網路上顯示的用戶端裝置上執行。例如，您可能想為消耗資源的工作停用該選項，您僅想在業餘時間執行該工作。

  預設情況下已停用該選項。

- **使用工作啟動自動隨機延遲**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動，即是，*分佈式工作啟動*。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  當工作被建立時，根據工作中包含用戶端裝置的數量，分發啟動時間被自動計算。然後，工作總是在計算的開始時間啟動。然後當工作設定被編輯或者工作被手動啟動時，計算的工作啟動時間值被變更。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

- **使用工作啟動隨機延遲間隔（分鐘）**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

  預設情況下已停用該選項。預設時間間隔為一分鐘。

9. 在精靈的**定義工作名稱**步驟中，指定工作的名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。

10. 在精靈的**完成工作建立**步驟，點擊**完成**按鈕關閉精靈。

    如果您想讓工作在精靈完成時立即啟動，選取**精靈完成時執行工作**核取方塊。

使用**應用程式啟動工作建立精靈**所建立的工作，是用來在主控台樹狀目錄的**工作**資料夾中儲存特定裝置的工作。

您也可以使用工作建立精靈為管理群組和用戶端裝置建立群組或本機產品授權金鑰發佈工作。

自動分發產品授權金鑰

如果金鑰位於管理伺服器上的產品授權金鑰儲存區中，則卡巴斯基安全管理中心允許將這些產品授權金鑰自動發佈至受管理裝置。自動分配產品授權金鑰不適用於**未配置的裝置**資料夾中的裝置。

要將產品授權金鑰自動分發至受管理裝置，請執行以下操作：

1. 在主控台樹狀目錄中，選取**Kaspersky 產品授權**資料夾。

2. 在資料夾的工作台，選取您要自動發佈到裝置的產品授權金鑰。

3. 使用以下方法之一開啟選定產品授權金鑰的內容視窗：

   - 透過從產品授權金鑰上下文功能表中選取**"內容"**。

   - 在所選產品授權金鑰的資訊框中，點擊**檢視產品授權金鑰內容**連結。

4. 在開啟的產品授權金鑰內容視窗中，選取**自動分發的產品授權金鑰**核取方塊。關閉產品授權金鑰內容視窗。

   產品授權金鑰將被自動分發到所有相容的裝置。

產品授權金鑰發佈是使用網路代理執行的。沒有為應用程式建立產品授權金鑰發佈工作。

在自動分發產品授權金鑰過程中，系統會考慮產品授權對裝置數量的限制。（授權限制會在產品授權金鑰的內容中設定。）若達授權限制，則會自動停止分發此裝置上的產品授權金鑰。

虛擬管理伺服器會自動從其儲存區和管理伺服器的儲存區中分發產品授權金鑰。我們建議您：

- 使用*新增產品授權金鑰*工作以選擇必須部署到裝置的產品授權金鑰。
- 避免在虛擬管理伺服器設定中停用**允許從該虛擬管理伺服器自動佈署產品授權金鑰到它的裝置**選項。否則，虛擬管理伺服器將不會向裝置分發產品授權金鑰，包括管理伺服器儲存區中的產品授權金鑰。

如果您在產品授權金鑰內容視窗中選擇**自動分發的產品授權金鑰**核取方塊，產品授權金鑰會立即在您的網路上分發。如果不選擇此選項，您可以之後手動分發產品授權金鑰。

建立和瀏覽產品授權金鑰使用報告

要在用戶端裝置上建立產品授權金鑰使用情況報告：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。
2. 在節點的工作區中，選取**報告**標籤。
3. 選取名為**產品授權金鑰使用報告**的報告範本，或者建立相同類型的報告範本。

產品授權金鑰使用報告的工作區會顯示用戶端裝置中，使用的啟動和備用產品授權金鑰的相關資訊。報告也包含使用產品授權金鑰的裝置和產品授權金鑰內容中指定的限制的相關資訊。

檢視有關應用程式產品授權金鑰的資訊

要了解在為 Kaspersky 應用程式使用哪些產品授權金鑰：

1. 在卡巴斯基安全管理中心主控台樹狀目錄，選取**受管理裝置**節點並轉到**裝置**頁籤。
2. 右鍵開啟相關裝置的上下文功能表並選取**內容**。
3. 在開啟的裝置內容視窗中，選取**應用程式**區域。
4. 在出現的應用程式清單中，選取您希望檢視其產品授權的應用程式，然後點擊**內容**按鈕。
5. 在開啟的應用程式內容視窗中，選取"**產品授權金鑰**"區段。

   該資訊將顯示在此區段的工作區中。

匯出產品授權金鑰檔案

如果您的產品授權金鑰被意外刪除但您想要還原它，您可以從其他管理伺服器匯出產品授權金鑰檔案。

若要匯出產品授權金鑰檔案，您必須在**匯出金鑰檔案：金鑰管理**功能區中具有**一般功能**權限。

如果產品授權金鑰從用戶端裝置收到，則無法將其匯出。

若要匯出產品授權金鑰：

1. 在主控台樹狀目錄中，選取**Kaspersky 產品授權**資料夾。
2. 在清單中，選擇要匯出為檔案的產品授權金鑰。
3. 在開啟的資訊框中，按一下**匯出金鑰檔案**連結。
4. 在開啟的視窗中，指定要儲存產品授權金鑰檔案的資料夾的路徑，然後指定檔案名稱。之後，按一下**儲存**。

   產品授權金鑰檔案將以 .key 格式被匯出到所選資料夾。

如果您匯出的產品授權金鑰檔案已作為啟動碼新增到管理伺服器儲存區，並且您想要將匯出的產品授權金鑰檔案新增至另一台管理伺服器的儲存區，則必須將其新增為啟動碼，而不是金鑰檔案。否則，就會發生錯誤。您必須在任何方便的文字編輯器中開啟匯出的產品授權金鑰檔案，然後複製啟動碼。

配置網路防護

本節包含有關政策和工作的手動配置、使用者角色、建構管理群組結構和工作階層的資訊。

情境：配置網路防護

快速啟動精靈會建立含預設設定的政策與工作。這些設定可能對組織來說並不是最佳設定，甚至不被允許。因此，建議您微調這些政策與工作，並在您網路有需求時，建立其他政策與工作。

先決條件

在您開始之前，確保您已做了如下：

- 已安裝卡巴斯基安全管理中心管理伺服器
- 已安裝卡巴斯基安全管理中心網頁主控台（選用）

- 完成卡巴斯基安全管理中心主安裝情境
- 完成快速設定精靈，或在**受管理裝置**管理群組手動建立以下政策和工作：
  - Kaspersky Endpoint Security 政策
  - 更新 Kaspersky Endpoint Security 的群組工作
  - 網路代理政策
  - *尋找弱點和必要更新*工作

設定要以階段進行的網路防護：

1. **設定和傳播 Kaspersky 應用程式政策和政策設定檔**

   要為安裝在受管理裝置上的 Kaspersky 應用程式配置和傳播設定，您可以使用兩種不同的安全管理方法—以裝置為中心或以使用者為中心。這兩種方法也可以被合併。要實現以裝置為中心的安全管理，您可以使用提供在基於 Microsoft Management Console 的管理主控台或卡巴斯基安全管理中心網頁主控台的工具。以使用者為中心的安全管理僅可以透過卡巴斯基安全管理中心網頁主控台實現。

2. **配置工作以遠端管理 Kaspersky 應用程式**

   檢查使用快速啟動精靈建立的工作並調整它們，如有必要。

   說明：

   - 管理主控台：
     - 為 Kaspersky Endpoint Security 設定群組工作
     - 排程「尋找弱點和所需更新」工作
   - 卡巴斯基安全管理中心網頁主控台：
     - 為 Kaspersky Endpoint Security 設定群組工作
     - 「尋找弱點和所需更新」工作設定

   如果必要，建立附加工作以管理安裝在用戶端裝置上的 Kaspersky 應用程式。

3. **評估和限制資料庫上的事件負載**

   受管應用程式操作相關的事件資訊將被從用戶端電腦上傳輸並記錄至管理伺服器資料庫。要降低管理伺服器負載，評估和限制可以儲存在資料庫的最大事件數量。

   說明：

   - 管理主控台：設定事件最大數量
   - 卡巴斯基安全管理中心網頁主控台：設定事件最大數量

結果

當您完成該情境時，您將透過配置 Kaspersky 應用程式、工作和管理伺服器接收的事件來防護您的網路：

- Kaspersky 應用程式會根據政策與政策設定檔設定。
- 應用程式會透過一組工作管理。
- 儲存在資料庫的事件數量上限已設定。

當網路防護配置完成時，您可以繼續配置 Kaspersky 資料庫和應用程式的一般更新。

有關如何配置針對 Kaspersky Sandbox 偵測到的威脅的自動回應的詳細資訊，請參閱 Kaspersky Sandbox 2.0 線上說明。

政策設定和傳播：以裝置為中心的方法

當您完成該方案後，應用程式將在所有受管理裝置上被設定，與您定義的應用程式政策和政策設定檔一致。

先決條件

開始前，請確保您已安裝了卡巴斯基安全管理中心管理伺服器和卡巴斯基安全管理中心網頁主控台（選用）。如果您安裝了卡巴斯基安全管理中心網頁主控台，您可能也想考慮以使用者為中心的安全管理作為以裝置為中心的安全管理的備選或附加選項。

階段

以裝置為中心的 Kaspersky 應用程式管理情境包含以下步驟：

1. **管理應用程式政策**

   透過為每個應用程式建立政策來配置安裝在受管理裝置上的 Kaspersky 應用程式設定。政策集將被傳播到用戶端裝置。

   當您在快速啟動精靈配置您網路的防護時，卡巴斯基安全管理中心會為以下應用程式建立預設政策。

   - Kaspersky Endpoint Security for Windows—適用於 Windows 用戶端裝置
   - Kaspersky Endpoint Security for Linux—適用於 Linux 用戶端裝置

   如果您透過使用該精靈完成了設定過程，您不必為該應用程式建立新政策。轉到 Kaspersky Endpoint Security 政策的手動設定。

   如果您有幾個管理伺服器和/或管理群組的層級結構，次要管理伺服器和子管理伺服器預設從主要管理伺服器繼承政策。您可以強制子群組和從屬管理伺服器的繼承以防止上流政策設定的修改。如果您僅要一部分設定被強制繼承，您可以在上游政策中鎖定它們。剩餘未鎖定的設定將可以在下流政策中修改。建立的政策層級將允許您有效管理管理群組中的裝置。

   說明：

   - 管理主控台：建立政策
   - 卡巴斯基安全管理中心網頁主控台：建立政策

2. **建立政策設定檔（可選）**

   如果您想讓單一管理群組中的裝置在不同政策設定下執行，為這些裝置建立政策設定檔。政策設定檔是政策設定的命名子集。子集會連同政策一起分發至目標裝置，並根據名為*設定檔啟動條件*的特別條件來作為輔助政策。設定檔僅包含與「基本」政策不同的設定，並在受管理裝置上活動。

   透過使用設定檔啟動條件您可以應用不同的政策設定檔，例如，到特定單元中的裝置或到 Active Directory 安全群組，具有特別硬體設定或被特別標籤標記。使用標籤篩選滿足特別標準的裝置。例如，您可以建立叫做 *Windows* 的標籤，使用該標籤標記所有執行 Windows 作業系統的裝置，然後指定該標籤作為政策設定檔啟動條件。結果，安裝在所有 Windows 裝置上的 Kaspersky 應用程式將被使用它們自己的政策設定檔管理。

   說明：

   - 管理主控台：
     - 建立政策設定檔
     - 建立政策設定檔啟動規則
   - 卡巴斯基安全管理中心網頁主控台：
     - 建立政策設定檔
     - 建立政策設定檔啟動規則

3. **傳播政策和政策設定檔到受管理裝置**

   預設情況下，管理伺服器每 15 分鐘自動與受管理裝置同步一次。您可以避免自動同步並透過使用強制同步指令手動執行同步。在您建立或更改政策或政策設定檔之後，系統也會強制同步。同步過程中，新的或變更的政策和政策設定檔被傳播到受管理裝置。

   如果您使用卡巴斯基安全管理中心網頁主控台，您可以檢查政策和政策設定檔是否被傳送到裝置。卡巴斯基安全管理中心在裝置內容中指定傳送日期和時間。

   說明：

   - 管理主控台：強制同步
   - 卡巴斯基安全管理中心網頁主控台：強制同步

結果

當以裝置為中心的情境完成時，Kaspersky 應用程式根據指定的設定被設定並透過政策層級傳播。

設定的應用程式政策和政策設定檔將被自動應用到新增到管理群組的新裝置。

關於以裝置為中心和以使用者為中心的安全管理方法

您可以從裝置功能的立場和從使用者角色的立場管理安全設定。第一種方法叫做*以裝置為中心的安全管理*，第二種叫做*以使用者為中心的安全管理*。要應用不同的應用程式設定到不同的裝置，您可以使用兩種方法的任意或組合。要實現以裝置為中心的安全管理，您可以使用提供在基於 Microsoft Management Console 的管理主控台或卡巴斯基安全管理中心網頁主控台的工具。以使用者為中心的安全管理僅可以透過卡巴斯基安全管理中心網頁主控台實現。

裝置特定安全性管理可讓您根據裝置特定的功能，套用不同的安全應用程式設定至受管理裝置。例如，您可套用不同設定至分配在不同管理群組中的裝置。您也可在 Active Directory 根據裝置使用量或其硬體規格來區分裝置。

以使用者為中心的安全性管理可讓您套用不同安全應用程式設定至不同的使用者角色。您可建立一些使用者角色，將適當的使用者角色指派給每位使用者，並將不同的應用程式設定定義至不同角色使用者擁有的裝置。例如，您可能要應用不同的應用程式設定到會計和人力資源 (HR) 人員的裝置。結果，當實現了以使用者為中心的安全管理時，每個部門—財務部門和人事部門—具有自己的 Kaspersky 應用程式設定配置。設定配置定義了哪些應用程式設定可以被使用者變更以及哪些被強制設定並被管理員鎖定。

透過使用以使用者為中心的安全管理，您可以應用特別應用程式設定到單個使用者。這可能用在員工在公司有獨一角色或您要監控與個別人的裝置相關的安全事故時。取決於該員工在公司的角色，您可以延伸或限制該員工變更應用程式設定的權限。例如，您可能要延伸在本機辦公室管理用戶端裝置的系統管理員的權限。

您也可以組合以裝置為中心的安全管理和以使用者為中心的安全管理方法。例如，您可以為每個管理群組設定特別的應用程式政策，然後為一個或幾個使用者角色建立政策設定檔。在此情況下，政策和政策設定檔會按照以下優先順序加以套用：

1. 為以裝置為中心的安全管理建立的政策被應用。
2. 政策設定檔會根據政策設定檔優先順序內容加以修改。
3. 政策被與使用者角色關聯的政策設定檔修改。

Kaspersky Endpoint Security 政策的手動設定

該部分提供了如何配置 Kaspersky Endpoint Security 政策的建議，該政策由快速設定精靈建立。您可以在政策屬性窗口中執行設置。

當編輯設定時，請記住您必須點擊相關設定之上的鎖圖示以便允許在工作站上使用該值。

在進階威脅防護區域配置政策

對於該區域設定的完整敘述，請參考 Kaspersky Endpoint Security for Windows 文件。

在**進階威脅防護**區域中，您可設定 Kaspersky Endpoint Security for Windows 如何使用卡巴斯基安全網路。您也可設定 Kaspersky Endpoint Security for Windows 模組，例如行為偵測、弱點利用防禦、主機入侵防禦和補救引擎。

在**卡巴斯基安全網路**子區域，建議您啟用使用**卡巴斯基安全網路**選項。使用該功能有助於重新分發和最佳化網路流量。如果**卡巴斯基安全網路**選項已停用，您可以啟用直接使用 KSN 伺服器。

在關鍵威脅防護部分配置政策

對於該區域設定的完整敘述，請參考 Kaspersky Endpoint Security for Windows 文件。

在政策內容視窗的**關鍵威脅防護**區段，我們建議您在**防火牆**和**檔案威脅防護**子區段中指定額外設定。

防火牆子區段包含的設定可讓您控制用戶端裝置上應用程式的網路活動。用戶端裝置使用指派了以下狀態之一的網路：公用、本機或受信任。根據網路狀態，Kaspersky Endpoint Security 可以允許或拒絕裝置上的網路活動。將新網路新增至您的組織時，您必須為其指派適當的網路狀態。例如，如果用戶端裝置是筆記型電腦，我們建議此裝置使用公用或受信任的網路，因為筆記型電腦不一定永遠都連線到本機網路。在**防火牆**子區段，您可以檢查是否正確將狀態指派給組織中使用的網路。

要檢視網路清單：

1. 在政策內容中，前往**關鍵威脅防護 → 防火牆**。
2. 在**可用網路**區域中，按一下**設定**按鈕。
3. 在開啟的**防火牆**視窗中，前往**網路**頁籤檢視網路清單。

在**檔案威脅防護**子區段中，您可以停用網路磁碟機掃描。掃描網路磁碟機會顯著提高網路磁碟機負載。在檔案伺服器上執行間接掃描更方便。

要停用網路磁碟機掃描：

1. 在政策內容中，前往**關鍵威脅防護 → 檔案威脅防護**。
2. 在**安全等級**區域中，按一下**設定**按鈕。
3. 在開啟的**檔案威脅防護**視窗中，在**一般**頁籤，清空**所有網路磁碟機**核取方塊。

在一般設定部分配置政策

對於該區域設定的完整敘述，請參考 Kaspersky Endpoint Security for Windows 文件。

在政策內容視窗的**一般設定**區段中，我們建議在**報告和儲存**和**介面**子區段中指定額外設定。

在**報告和儲存**子區段中，前往**到管理伺服器的資料傳輸**區段。**關於已啟動的應用程式**核取方塊指定管理伺服器資料庫是否儲存網路裝置上所有軟體模組的所有版本資訊。如果選取此核取方塊，所儲存的資訊可能需要使用卡巴斯基安全管理中心資料庫上的大量磁碟空間（數十 GB）。如果在最上層政策中選取了**關於已啟動的應用程式**核取方塊，請取消勾選。

如果管理主控台以集中模式管理組織網路上的威脅防護，請停用工作站上 Kaspersky Endpoint Security for Windows 使用者介面的顯示。為此，在**介面**子區段中，前往**使用者互動**區段，然後勾選**不顯示使用者介面**選項。

如要在工作站上啟用密碼防護，請在**介面**子區段中，前往**密碼防護**區段，點擊**設定**按鈕，然後選取**啟用密碼防護**核取方塊。

在事件配置區域配置政策

在**事件配置**區域，您應該停用儲存任何事件到管理伺服器，除了以下事件：

- 在**緊急**頁籤：
  - *應用程式自動執行已停用*
  - *存取被拒絕*
  - *已禁止應用程式啟動*
  - *無法解毒*
  - *違反了最終使用者產品授權協議*
  - *無法載入加密模組*
  - *不能同時執行兩項工作*
  - *偵測到活動威脅。應該啟動進階解毒技術*
  - *偵測到網路攻擊*
  - *未更新所有元件*
  - *啟動錯誤*
  - *啟用攜帶模式時出錯*
  - *與卡巴斯基安全管理中心互動時發生錯誤*
  - *停用攜帶模式時出錯*
  - *變更應用程式元件時出錯*
  - *套用檔案加密/解密規則時出錯*
  - *無法套用政策*
  - *處理程序已終止*
  - *網路活動已封鎖*
- 在**功能失效**頁籤上：*工作設定無效，未套用設定*

- 在**警告**頁籤：
  - *自我防護被停用*
  - *備用金鑰不正確*
  - *使用者選擇了結束加密政策*
- 在**資訊**頁籤：*禁止應用程式在測試模式下啟動*

Kaspersky Endpoint Security 更新群組工作的手動設定

Kaspersky Endpoint Security 版本 10 與更新版本最佳與建議的排程選項為**當新更新下載至儲存區時**，以及選取**使用工作啟動自動隨機延遲**核取方塊。

Kaspersky Endpoint Security 裝置掃描群組工作的手動設定

快速設定精靈建立掃描裝置的群組工作。預設下，工作被分配**在星期五下午 7:00 執行**排程，並且不選取**執行錯過的工作**核取方塊。

這意味著如果組織中的裝置在星期五關閉，例如在下午 6:30，裝置掃描工作將永遠不會被執行。您必須基於組織的工作規則為該工作設定最方便的排程。

排程「尋找弱點和所需更新」工作

快速設定精靈為網路代理建立*尋找弱點和所需更新*工作。預設下，工作被分配**在星期二下午 7:00 執行**排程，並且**執行略過的工作**核取方塊被選中。

如果組織的工作規則要在此時關閉所有裝置，*尋找弱點和所需更新*工作將在裝置再次開啟時執行，也就是，在星期三早晨。此活動可能不是必須的，因為弱點掃描可能增加 CPU 和磁碟子系統負載。您必須根據組織的工作規則為該工作設定最方便的排程。

更新安裝和弱點修復群組工作的手動設定

該快速設定精靈為網路代理建立更新安裝和弱點修復群組工作。預設下，工作被設定在每天 01:00 AM 執行，並且不會啟用**執行略過的工作**選項。

如果組織工作規則整夜關閉所有裝置，則更新安裝將永遠不會執行。您必須基於組織的工作規則為弱點掃描工作設定最方便的排程。值得注意的是，更新的安裝可能需要重新啟動裝置。

設定事件儲存區中的最大事件數量

在管理伺服器內容視窗的**事件儲存區**區域中，您可以透過限制事件記錄數和儲存期限來編輯管理伺服器資料庫的事件儲存設定。當您指定事件最大數時，應用程式計算用於指定數目的儲存空間的大概大小。您可以使用該大概計算來評估您在磁碟上是否具有足夠空間以避免資料庫溢出。管理伺服器資料庫的預設容量是 400,000 個事件。最大建議的資料庫容量是 45,000,000 個事件。

應用程式每 10 分鐘檢查一次資料庫。如果事件數達到指定的最大值加 10,000，應用程式將刪除最舊的事件，以便僅保留指定的最大事件數。

若管理伺服器刪除舊事件，則無法儲存新事件到資料庫。在此時間段內，拒絕事件的資訊被寫入卡巴斯基事件記錄。新事件被列隊，然後在刪除操作後被儲存到資料庫。

要限制儲存在管理伺服器事件儲存區中的事件的數量：

1. 右擊管理伺服器，然後選取**內容**。

   管理伺服器內容視窗將開啟。

2. 在**事件儲存區**區域的工作區，指定儲存在資料庫中事件的數量上限。

3. 點擊**確定**。

此外，您可以更改任何工作的設定，以儲存與工作進度相關的事件，或者只儲存工作執行結果。為此，您將降低資料庫中的事件數量，提高與資料庫中事件表分析相關之情境的執行速度，並降低緊急事件被大數量事件覆寫的風險。

設定修復弱點資訊的最長儲存期間

若要在資料庫中設定已在受管理裝置上修復的弱點的資訊的最長儲存期間：

1. 右擊管理伺服器，然後選取**內容**。

   管理伺服器內容視窗將開啟。

2. 在"**事件儲存區**"區段的工作區中，指定資料庫中修復弱點資訊的最長儲存期間。

   預設情況下，儲存期間為 90 天。

3. 點擊**確定**。

修復弱點資訊的最長儲存期間為指定天數。之後，管理伺服器維護工作將從資料庫中刪除過時的資訊。

管理工作

卡巴斯基安全管理中心透過建立和執行不同工作來管理裝置上安裝的應用程式。安裝、啟用和停用應用程式、掃描檔案、更新病毒資料庫和軟體模組以及應用程式的其他行為均需要使用工作來完成。

工作又被細分為以下類型：

- *群組工作*。在群組中的全部裝置共同執行的工作。
- *管理伺服器工作*。管理伺服器所需執行的工作。
- *指定裝置的工作*。選取指定裝置來執行的工作，與裝置屬於哪個群組無關。
- *本機工作*。在特定裝置上執行的工作。

如果應用程式的管理外掛程式未安裝在管理主控台上，只能建立應用程式工作。

您可以透過以下方式之一來建立工作的裝置清單（最多 1000 個裝置）：

- 透過選取管理伺服器發現的網路裝置。
- 透過手動指定裝置清單。您可以使用 IP 位址（或 IP 範圍）、NetBIOS 名稱或 DNS 名稱作為該裝置的位址。
- 透過包含有要新增的裝置位址的 .txt 檔案來匯入裝置清單（每一個電腦位址必須單獨一行）。

  如果透過檔案匯入或手動建立裝置清單，且裝置是以名稱定義，則清單可以只包含其資訊已在裝置連線或裝置發現中輸入到管理伺服器資料庫中的裝置。

您可以為每個應用程式建立任意數量群組工作、指定裝置的工作或本機工作。

在網路代理與管理伺服器連線時，裝置上安裝的應用程式將與卡巴斯基安全管理中心資料庫交換工作資訊。

您可以修改工作設定、檢視工作進度、複製、匯出、匯入和刪除工作。

只有當建立工作的應用程式執行時，裝置才會啟動工作。當應用程式未執行時，則取消所有執行的工作。

已完成工作結果儲存在 Microsoft Windows 和卡巴斯基安全管理中心的事件記錄中，既集中在管理伺服器上，又位於每個裝置上。

請勿在工作設定中包含私密資料。例如，避免指定網域管理員密碼。

管理支援多承租的應用程式的工作詳情

支援多承租的應用程式的群組工作根據管理伺服器和用戶端裝置層級被套用到應用程式。建立工作的虛擬管理伺服器必須處於安裝應用程式的用戶端裝置的相同或更低管理群組。

在對應於工作執行結果的事件中，服務提供者管理員可以看到執行工作的裝置的資訊。相對地，租戶管理會顯示在**多租戶節點**。

建立工作

在管理主控台，您可以在管理群組資料夾直接建立工作，也可以在**工作**資料夾的工作區建立。

要在管理群組資料夾建立工作：

1. 在主控台樹狀目錄中，選取您要為其建立工作的管理群組。
2. 在群組工作區中，選取**工作**頁籤。
3. 點擊**建立工作**按鈕，執行工作建立。

   新工作精靈啟動。遵照精靈的說明。

*要在**工作**資料夾的工作區建立工作：*

1. 在主控台樹狀目錄中，選取**工作**資料夾。
2. 點擊**完成**按鈕，執行工作建立。

   新工作精靈啟動。遵照精靈的說明。

請勿在工作設定中包含私密資料。例如，避免指定網域管理員密碼。

建立管理伺服器工作

管理伺服器可執行的工作如下：

- 傳送報告
- 將更新下載至管理伺服器儲存區
- 備份管理伺服器資料
- 管理伺服器維護
- 執行 Windows Update 同步
- 基於參考裝置作業系統映像建立安裝套件
- 遠端安裝應用程式
- 遠端解除安裝應用程式
- 發佈安裝套件
- 將應用程式遠端安裝到從屬管理伺服器

虛擬管理伺服器，可提供報告和建立作業系統映像安裝套件。虛擬管理伺服器的儲存區節點下的更新，將顯示已下載至主管理伺服器的更新。虛擬管理伺服器的資料備份與主管理伺服器的資料備份一起進行。

要建立管理伺服器工作：

1. 在主控台樹狀目錄中，選取**工作**資料夾。
2. 透過下列方式開始建立工作：
   - 在主控台樹狀目錄的 **工作** 資料夾右鍵功能表中選取**新增 → 工作**。
   - 透過點擊在**工作**資料夾工作區的**建立工作**按鈕。

新工作精靈啟動。遵照精靈的說明。

將更新下載至管理伺服器儲存區、執行 Windows 更新同步工作、管理伺服器維護和*備份管理伺服器資料*工作只能建立一次。如果已為管理伺服器建立了*將更新下載至管理伺服器儲存區*、*管理伺服器維護*、*備份管理伺服器資料*和執行 *Windows Update 同步*工作，則它們將不會顯示在新工作精靈的工作類型選取視窗中。

為特定裝置建立工作

在卡巴斯基安全管理中心中您可以為指定裝置建立工作。加入組合的裝置可以被包含在各種管理群組中，也可以被排除在外。卡巴斯基安全管理中心能夠為特定裝置執行以下主要工作：

- 遠端安裝應用程式
- 將訊息傳送至使用者
- 變更管理伺服器
- 受管理裝置
- 驗證更新
- 分發安裝套件
- 將應用程式遠端安裝到從屬管理伺服器
- 遠端移除應用程式

要為特定裝置建立工作：

1. 在主控台樹狀目錄中，選取**工作**資料夾。
2. 透過下列方式開始建立工作：
   - 在主控台樹狀目錄的**工作**資料夾上下文功能表中，選取**新增 → 工作**。
   - 透過點擊在**工作**資料夾工作區的**建立工作**按鈕。

新工作精靈啟動。遵照精靈的說明。

建立本機工作

要為裝置建立本機工作，請執行以下操作：

1. 在包含該裝置的群組的工作區中，選取**裝置**頁籤。
2. 在**裝置**頁籤的物件清單中，選取要為其建立本機工作的裝置。
3. 使用下列方式之一為所選裝置建立工作：
   - 透過點擊**執行操作**按鈕並在下拉清單中選取**建立工作**。
   - 點擊在裝置的工作區中的**建立工作**連結。
   - 使用以下裝置內容：
     a. 在裝置的上下文功能表中，選取**內容**。
     b. 在開啟的裝置內容視窗中，選取**工作**區域，然後點擊**新增**。

新工作精靈啟動。遵照精靈的說明。

您可以在相應的 Kaspersky 應用程式手冊中找到詳細說明如何建立本機工作。

在嵌套群組工作台中顯示繼承的群組工作

要啟用在嵌套群組的工作台中顯示繼承的群組工作功能，請執行以下操作：

1. 在嵌套群組工作區中選取**工作**頁籤。
2. 在**工作**頁籤的工作區，點擊**顯示繼承的工作**按鈕。

繼承的工作將顯示在帶有以下圖示的工作列清單中：

-  —如果它們從主管理伺服器上建立的群組中繼承。
-  —如果它們從頂級群組繼承。

如果啟用了繼承模式，繼承的工作只能在原來建立的群組中進行編輯。繼承的工作無法在繼承此工作的群組中進行編輯。

在工作啟動前自動開啟裝置

卡巴斯基安全管理中心不會在關閉的裝置上執行工作。您可以使用網路喚醒功能將卡巴斯基安全管理中心配置為在開始工作之前自動開啟這些裝置。

要設定開始工作之前自動開啟裝置，請執行以下操作：

1. 在工作內容視窗中，選取**排程**區段。
2. 要在裝置上配置操作，請點擊**進階**連接。
3. 在開啟的**進階**視窗中，選取**透過使用 Wake-On-LAN 功能在啟動工作之前開啟裝置（分鐘）**核取方塊，然後指定時間區段（分鐘）。

結果，在開始工作前的指定分鐘數內，卡巴斯基安全管理中心會使用網路喚醒功能開啟裝置並在其上加載作業系統。工作完成後，如果裝置使用者未登入系統，裝置會被自動關閉。請注意，卡巴斯基安全管理中心僅自動關閉使用網路喚醒功能開啟的裝置。

卡巴斯基安全管理中心只能在支援網路喚醒 (WoL) 標準的裝置上自動啟動作業系統。

在工作結束後自動關閉裝置

卡巴斯基安全管理中心允許您用這種方法配置工作，以便其所分發的裝置在工作完成後自動關閉。

要在工作結束後自動關閉裝置：

1. 在工作內容視窗中，選取**排程**區段。
2. 點擊**進階**連結以開啟視窗設定裝置操作。
3. 在開啟的**進階**視窗中，選取**完成工作後關閉裝置**核取方塊。

限制工作執行時間

要限制工作在裝置上執行的時間：

1. 在工作內容視窗中，選取**排程**區段。
2. 點擊**進階**，開啟用於設定用戶端裝置操作的視窗。
3. 在開啟的**進階**視窗中，選取**停止工作，若時間超過（分鐘）**核取方塊並指定時間區段（分鐘）。

   如果超過特定時間間隔，裝置上工作還未完成的話，卡巴斯基安全管理中心將自動停止該工作。

匯出工作

您可以將群組工作和指定裝置的工作匯出至檔案。管理伺服器工作不供匯出。

要匯出工作，請執行以下操作：

1. 從工作的上下文功能表中，選取**所有工作 → 匯出**。
2. 在開啟的"**另存為**"視窗中，指定檔案的名稱和路徑。
3. 按一下**儲存**按鈕。

本機使用者的權限無法被匯出。

匯入工作

您可以匯入群組工作和指定裝置的工作。管理伺服器工作無法匯入。

要匯入工作，請執行以下操作：

1. 選取必須匯入工作的清單：
   - 如果您希望將工作匯入到群組工作清單中，請在相關群組的工作區中選取**工作**頁籤。
   - 如果您希望將工作匯入到指定裝置的工作清單中，請從主控台樹狀目錄中選取**工作**資料夾。
2. 使用下列方式之一匯入工作：
   - 從工作清單的上下文功能表中，選取**所有工作 → 匯入**。
   - 在工作清單管理區塊中，點擊**從檔案匯入工作**連結。
3. 在開啟的視窗中，指定您要匯入的工作檔案及路徑。
4. 按一下**開啟**按鈕。

   工作顯示在工作清單。

如果新匯入的工作與現有工作的名稱相同，則匯入工作的名稱將加上 **(<next sequence number>)** 索引，例如：**(1)**、**(2)**。

轉換工作

卡巴斯基安全管理中心可將以前版本的 Kaspersky 應用程式的工作轉換為最新版本的工作。

可轉換以下應用程式的工作：

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4
- Kaspersky Endpoint Security 8 for Windows
- Kaspersky Endpoint Security 10 for Windows

若要轉換工作，請執行以下操作：

1. 在主控台樹狀目錄中，選取您希望為其轉換工作的管理伺服器。
2. 在管理伺服器的上下文功能表選取**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啟動。遵照精靈的說明。

精靈完成作業後會建立新工作，此工作會沿用先前應用程式版本使用的政策設定。

手動啟動和停止工作

您可以使用以下任一方法手動啟動和停止工作：在工作的右鍵功能表中，或在已分配工作的用戶端裝置的內容視窗中。

> 只有KLAdmins 群組中包含的使用者能從裝置的上下文功能表啟動群組工作。

從上下文功能表或工作的內容視窗啟動或停止工作：

1. 在工作的物件清單中，選取一個工作。
2. 使用下列方式之一開始或停止工作：
   - 透過在裝置的上下文功能表中選取**開始 → 停止**。
   - 透過點擊工作內容視窗中**一般**區域的**開始**或**停止**。

從上下文功能表或用戶端裝置的內容視窗啟動或停止工作：

1. 在裝置清單中，選取一個裝置。
2. 使用下列方式之一開始或停止工作：
   - 透過在裝置的上下文功能表中選取**所有工作 → 執行工作**。從工作清單選取相關工作。
     為其分配工作的裝置清單將更換為所選裝置。工作啟動。
   - 透過點擊裝置內容視窗中**工作**區域的啟動按鈕（  ）或停止按鈕（  ）。

手動暫停和繼續工作

要手動暫停和繼續工作，請執行以下操作：

1. 在工作的物件清單中，選取一個工作。
2. 使用下列方法之一暫停或繼續工作：
   - 透過在工作的上下文功能表中選取**暫停** 或 **繼續**。
   - 透過在工作內容視窗中選取**一般**區域，並點擊**暫停**或**繼續**。

監視工作執行

要監視工作執行，

在工作內容視窗中，選取**一般**區域。

一般區域的中間部份顯示了目前工作狀態。

檢視儲存在管理伺服器中的工作執行結果

卡巴斯基安全管理中心允許您檢視群組工作、指定裝置的工作和管理伺服器工作的執行結果。但無法瀏覽本機工作的執行結果。

要檢視工作結果：

1. 在工作內容視窗中，選取**一般**區域。
2. 點擊**結果**連結開啟**工作結果**視窗。

設定工作執行結果資訊的篩選條件

卡巴斯基安全管理中心允許您篩選群組工作、指定裝置的工作以及管理伺服器工作的執行結果。但無法篩選本機工作。

要設定工作執行結果的資訊篩選，請執行以下操作：

1. 在工作內容視窗中，選取**一般**區域。
2. 點擊**結果**連結開啟**工作結果**視窗。

   視窗上方的表格包含為其分配工作的所有裝置清單。視窗下方的表格顯示選取裝置執行的工作結果。

3. 點擊相關表格，開啟上下文功能表並選取**篩選器**。

4. 在開啟的**設定篩選器**視窗中的**事件**、**裝置**與**時間**區域設定篩選器。點擊**確定**。

工作結果視窗將顯示符合篩檢條件指定設定的資訊。

修改工作。回溯變更

要修改工作：

1. 在主控台樹狀目錄中，選取**工作**資料夾。

2. 在**工作**資料夾的工作區，選取一個工作並使用上下文功能表前往工作內容視窗。

3. 做相關變更。

> 在**工作範圍排除項目**區域，您可以設定不應用工作的子群組清單。

4. 點擊"**套用**"。

對工作所做的變更將儲存在工作內容中，在**變更歷程**區域。

如果必要，您可以回溯對工作所做的變更。

要回溯對工作所做的變更：

1. 在主控台樹狀目錄中，選取**工作**資料夾。

2. 選取必須回溯變更的工作，使用上下文功能表轉到工作內容資料夾。

3. 在工作內容視窗中，選取**變更歷程**區域。

4. 在工作修訂清單中，選取您要回溯的修訂號。

5. 點擊**進階**按鈕並在下拉清單中選取**回溯**。

比較工作

您可以比較相同類型的工作：例如，您可以比較兩個惡意軟體掃描工作，但是您無法比較惡意軟體掃描工作和更新安裝工作。比較之後，您收到工作設定相同點和不同點報告。您可以列印工作比較報告或者儲存為檔案。當公司中不同的規則被分配給相同類型的不同工作時，您可能需要工作比較。例如，財務部門的惡意軟體掃描工作僅掃描本機磁碟和他們的裝置，然而銷售部門由於要與客戶聯絡，他們的惡意軟體掃描工作需要掃描本機硬碟和電子郵件。您不必檢視所有工作設定以找出不同點；您可以簡單地使用比較。

> 您僅可以比較相同類型的工作。

> 工作僅可以成對比較。

您可以用以下方法之一比較工作：透過選取一個工作並與另一個比較，或者透過從工作清單中比較任意兩個工作。

要選取一個工作並與另一個進行比較：

1. 在主控台樹狀目錄中，選取**工作**資料夾。
2. 在**工作**資料夾的工作區，選取您要與另一個進行比較的工作。
3. 從工作的上下文功能表中，選取**所有工作 → 與其他工作比對**。
4. 在**選取一個工作**視窗，選取要比較的工作。
5. 點擊**確定**。

   一個 HTML 格式的比較兩個工作的報告被顯示。

要從工作清單比較兩個工作：

1. 在主控台樹狀目錄中，選取**工作**資料夾。
2. 在**工作**資料夾的工作清單中，使用 **Shift** 或 **Ctrl** 鍵選取兩個相同類型的工作。
3. 在上下文功能表中，選取**比較**。

   一個 HTML 格式的比較所選工作的報告被顯示。

當工作被比較時，如果密碼不同，星號 (******) 被顯示在工作比較報告。

如果密碼在工作內容中被變更，星號 (******) 被顯示在修訂比較報告。

啟動工作的帳戶

您可以指定在哪個帳戶下執行工作。

例如，要執行自訂掃描工作，您必須具有對要掃描物件的存取權限；要執行更新工作，您需要具有授權代理伺服器使用者權限。為執行工作指定帳戶的機會可避免使用者執行沒有必需存取權限的工作時自訂掃描工作和更新工作出現問題。

執行遠端安裝/移除工作期間，系統會使用指定的帳戶將安裝或移除應用程式所需的檔案下載到用戶端裝置，以防網路代理未安裝或不可用。如果網路代理已安裝並且可用，則會依據工作設定使用帳戶，使用 Microsoft Windows 實用程式僅從共用資料夾中提供檔案。在這種情況下，帳戶必須在裝置上擁有以下權限：

- 遠端啟動應用程式的權限。
- 使用 Admin$ 資源的權限。
- *作為服務登入*的權限。

如果檔案由網路代理提供給裝置，則不會使用帳戶。所有檔案複製和安裝操作便會由**網路代理**（**本機系統帳戶**）執行。

匯出工作執行歷程記錄

如果遇到任何工作問題，您可能需要調查潛在原因。為此，您可以匯出和進一步分析工作執行歷程記錄。

要匯出工作執行歷程記錄：

1. 在裝置上的目錄中建立一個空的 TXT 檔案。
   工作執行歷程記錄將被匯出到此檔案中。
2. 開啟工作結果視窗。
3. 在工作結果視窗的上方，選擇正在經歷問題的裝置。
4. 在工作結果視窗的下方（其中顯示所選裝置的執行歷程記錄），選擇一個或多個事件。
   若要選擇多個事件，請使用**Shift** 或 **Ctrl**鍵。
5. 右鍵點擊所選事件，開啟上下文功能表並選取**匯出**。
   事件匯出精靈啟動。
6. 在精靈的**匯出檔案**步驟，點擊**瀏覽**按鈕，然後選擇您已建立用來匯出工作執行歷程記錄的 TXT 檔案。
   如果只想要匯出選定事件，請啟用選項**只匯出選取的事件**。
   如果想要匯出整個工作執行歷程記錄（所有事件），必須停用 **只匯出選取的事件** 。
7. 點擊**下一步**按鈕。
8. 在精靈的**匯出格式**步驟，啟用以下選項之一：
   - **匯出以定位點分隔的 Unicode 文字**
     如果匯出的資料包括多種語言的特殊字元和符號，且您需要確保當包含匯出資料的 TXT 檔案在不同應用程式中開啟時所有字元得到準確保留，請啟用此選項。
   - **匯出以定位點分隔的文字**
     如果您想要維護與可能不支援 Unicode 的舊系統或者應用程式的相容性，請啟用此選項。
9. 點擊**下一步**按鈕以完成精靈。

工作執行歷程記錄被匯出到所選 TXT 檔案。

變更工作密碼精靈

對於非本機工作，您可在指定必須在其下執行工作的帳戶。您可在建立工作期間或在現有工作的內容中指定帳戶。若根據組織安全指示使用指定帳戶，這些指示可能不實需要變更帳戶密碼。當帳戶密碼過期且您設定了新密碼，工作將無法啟動直到您在工作內容中指定新的有效密碼。

變更工作密碼精靈可讓您自動在指定帳戶的所有工作中以新密碼取代密碼。或者，您可在各工作的內容中手動進行。

若要啟動變更工作密碼精靈：

1. 在主控台樹狀目錄中，選取**工作**節點。
2. 在此節點的上下文功能表中，選取**變更工作密碼精靈**。

遵照精靈的說明。

步驟 1：指定憑證

在**帳戶**與**密碼**欄位中，指定您系統中目前有效的新憑證（例如在Active Directory）。當您切換至精靈的下一步時，卡巴斯基安全管理中心會檢查指定帳戶名稱是否符合各個非本機內容中的帳戶名稱。若帳戶名稱相符，則工作內容中的密碼將自動取代為新的。

若您填寫**舊密碼（可選）**欄位，卡巴斯基安全管理中心僅會對已找到帳戶名稱與密碼的工作取代密碼。取代會自動執行。在所有其他情況下，您必須選擇進行精靈的下個步驟。

步驟 2：選取要採取的動作

若您未在精靈的第一步指定舊密碼或指定的舊密碼與工作中的密碼不符，您需要對已找到的工作選擇要採取的動作。

對於有*需要批准*的各個工作，請決定您是否要在工作內容中移除密碼，或用新的加以取代。若您選擇移除密碼，系統會切換工作以在預設帳戶下執行。

步驟 3：檢視結果

在精靈的最後步驟中，檢視各個已找到工作的結果。要完成精靈，請點擊**完成**按鈕。

在虛擬管理伺服器上建立您所需要的管理群組

建立虛擬管理伺服器後，它將預設包含名為"**受管理裝置**"的群組。

在虛擬管理伺服器下建立子群組的方式與實體管理伺服器建立子群組的方式和流程都是相同的。

> 您不能在虛擬管理伺服器下新增虛擬管理伺服器和從屬管理伺服器。這是由於虛擬管理伺服器的限制。

政策和政策設定檔

在卡巴斯基安全管理中心網頁主控台中，您可以為 Kaspersky 應用程式 建立政策。該部分描述了政策和政策設定檔，並提供建立和修改它們的說明。

政策層級，使用政策設定檔

本章節提供關於如何套用政策到管理群組裝置的資訊。此外，還提供有關政策設定檔的資訊。

政策層級

在卡巴斯基安全管理中心，您使用政策來定義一個單一設定集到多個裝置。例如，應用程式 P 的政策範圍，為管理群組 G 定義，包含安裝了應用程式 P 的佈署在群組 G 和其子群組的受管理裝置，除了在內容中清空了**從父群組繼承**核取方塊的子群組。

政策透過設定旁邊的鎖頭圖示（ ）不同於本機設定。如果一個設定（或設定群組）在政策內容中被鎖定，您必須首先在建立有效設定時使用該設定（或設定群組），其次，必須將設定或設定群組寫入 downstream 政策。

在裝置上建立有效設定可以如此敘述：所有未鎖定的設定值必須來自政策，然後被本機設定覆蓋，然後結果集被來自政策的鎖定設定的值覆蓋。

相同應用程式的政策透過管理群組層級互相影響：來自 upstream 政策的鎖定設定覆蓋來自 downstream 政策的相同設定。

漫遊使用者有特殊政策。該政策在裝置切換到漫遊模式時在裝置上生效。漫遊使用者的政策不透過管理群組層級影響其他政策。

政策設定檔

僅透過管理群組層級套用政策到裝置可能在許多環境下不方便。有必要建立單一政策的幾個實例，這些實例對於不同的管理群組在一兩個設定上有所不同，可以在將來同步這些政策的內容。

為了幫助您避免此類問題，卡巴斯基安全管理中心支援*政策設定檔*。政策設定檔是政策設定的命名子集。子集會連同政策一起分發至目標裝置，並根據名為*設定檔啟動條件*的特別條件來作為輔助政策。設定檔僅包含與「基本」政策不同的設定，並在用戶端裝置（電腦或行動裝置）上活動。啟動設定檔會變更設定檔啟動之前已在電腦上活動的政策設定。這些設定將使用已在設定檔中指定的值。

以下限制被施加在政策設定檔：

- 政策可以包含最多 100 個設定檔。
- 政策設定檔不能包含其他設定檔。
- 政策設定檔不能包含通知設定。

設定檔內容

政策設定檔包含以下組成部分：

- 名稱。帶有相同名稱的設定檔透過管理群組層級互相影響。
- 政策設定子集。不同於包含所有設定的政策，設定檔僅包含實際所需的設定（鎖定設定）。

- 啟動條件是裝置內容的邏輯表達。設定檔僅在設定檔啟動條件為真是活動（補充政策）。在其他所有情況，設定檔是非啟動和略過的。以下裝置內容可以被包含在邏輯表達：
  - 漫遊模式狀態。
  - 網路環境內容 – 用於網路代理連線的活動規則名稱。
  - 裝置上指定標籤的出現和消失。
  - 裝置在 Active Directory 組織單元 (OU) 上的分配：明確（裝置在指定 OU 中），或不明確（裝置是 OU，以嵌套級別包含在指定 OU）。
  - 裝置在 Active Directory 安全群組中的資格（明確或不明確）。
  - Active Directory 安全群組中裝置所有者的成員關係（明確或不明確）。
- 設定檔停用核取方塊。被停用的設定檔總是被略過，並且它們的啟動條件不被驗證。
- 設定檔優先順序。不同設定檔的啟動條件是獨立的，因此幾個設定檔可以一起啟動。如果活動設定檔包含設定的非重疊集合，將不會發生問題。然而，如果兩個活動設定檔包含不同的相同設定的值，將發生歧義。該歧義可以透過政策優先順序避免：歧義變數的值將來自高優先順序的設定檔（在設定檔清單中評級較高）。

政策透過層級互相影響時的設定檔行為

帶有相同名稱的設定檔根據政策合併規則合併到一起。upstream 政策的設定檔比 downstream 政策的設定檔擁有更高優先順序。如果編輯設定在 upstream 政策中被禁止（鎖定），downstream 政策使用 upstream 政策的設定檔啟動條件。如果編輯設定在 upstream 政策中被允許，downstream 政策的設定檔啟動條件被使用。

由於政策設定檔可能在啟動條件中包含**裝置已離線**內容，因此設定檔會完全取代漫遊使用者的政策功能，即此功能將不再受到支援。

漫遊使用者的政策可能包含設定檔，但是它們設定檔僅可以在裝置轉換到漫遊模式後啟動。

政策設定繼承

已為管理群組指定政策。政策設定可以是*繼承的*，即是在其所在管理群組的子群組被接收。因此，父群組政策也叫*父政策*。

您可以啟用或停用繼承的兩個選項：**從父群組政策中繼承設定**和**強制繼承子政策設定**：

- 如果您對子政策啟用**從父政策繼承設定**，並在父政策中鎖定一些設定，那麼您無法為子群組變更這些設定。然而，您可以變更在父政策中未鎖定的設定。
- 如果您對子政策停用**從父政策繼承設定**，那麼您可以變更子群組中的所有設定，即便一些設定在父政策中是鎖定的。
- 如果您為父群組啟用**強制繼承子政策設定**，這將為每個子群組啟用**從父政策繼承設定**。此種情況下，您無法為任何子政策停用該選項。所有在父政策中被鎖定的設定被強制繼承到子群組，且您無法在子群組中變更這些設定。
- 在**受管理裝置**群組的政策中，**從父政策繼承設定**不影響任何設定，因為**受管理裝置**群組沒有任何上游群組，因此不繼承任何政策。

預設下，**從父群組政策中繼承設定**選項已為新政策啟用。

如果一個政策具有設定檔，所有子政策都繼承這些設定檔。

管理政策

用戶端裝置上安裝的應用程式設定值是透過定義政策集中管理的。

為管理群組中的應用程式所建立政策將顯示在工作區中的**政策**頁籤上。在每個政策前面會顯示一個狀態的圖示。

政策被刪除後，在應用程式繼續依照政策中的設定工作。這些設定隨後可以被手動變更。

政策將按如下方式套用：如果某個裝置正在執行駐留工作（即時防護工作），它們將使用新的設定值保持執行。所有已執行的排程工作（掃描，病毒資料庫更新）均保持執行，且設定值不變。下次，它們將使用新設定值執行。

帶有多項支援的應用程式的政策被繼承到更低級別管理群組以及更高等級管理群組：政策被傳播到所有安裝了應用程式的用戶端裝置。

如果管理伺服器有階層架構，從屬管理伺服器將從主管理伺服器接收政策，然後將其發佈至用戶端裝置。啟用繼承後，則可以在主管理伺服器上修改政策設定。而從屬管理伺服器上的政策也跟著一並被修改。

如果主從管理伺服器之間的連線中斷，從屬管理伺服器上的政策依然有效不會消失。當主從管理伺服器重新連線後，主要伺服器已調整過的政策將立即套用到從屬管理伺服器。

如果停用繼承，您可以獨立修改從屬管理伺服器上的政策設定，不受主管理伺服器的影響。

如果管理伺服器和用戶端裝置之間的連線中斷，用戶端裝置將使用漫遊政策（如果定義）的政策，或者繼續使用原來的政策設定，直至連線被重新建立。

政策分配至從屬管理伺服器的結果將顯示在主管理伺服器主控台的「政策內容」視窗。

向用戶端裝置分發政策的結果將顯示在所連線的管理伺服器的政策內容視窗中。

> 不在政策設定中使用私人資料。例如，避免指定網域管理員密碼。

建立政策

在管理主控台中，您可以在管理群組資料夾直接建立政策，或在**政策**資料夾的工作區。

在管理群組資料夾建立政策：

1. 在主控台樹狀目錄中，選取您要為其建立政策的管理伺服器。
2. 在群組的工作區中，選取**政策**頁籤。
3. 透過點擊**新政策**按鈕執行新政策精靈。

   新政策精靈啟動。遵照精靈的說明。

*要在**政策**資料夾的工作區建立政策：*

1. 在主控台樹狀目錄中，選取**政策**資料夾。
2. 透過點擊**新政策**按鈕執行新政策精靈。

   新政策精靈啟動。遵照精靈的說明。

您可以為此群組中的一個應用程式建立多個政策，但一次只能啟用一個政策。當您建立新的政策時，先前的啟用的政策將變為停用狀態。

建立政策時，您可以匯入先前應用程式設定檔。而未被先前應用程式設定檔所定義的設定將使用預設值。您可以在政策建立後變更。

不在政策設定中使用私人資料。例如，避免指定網域管理員密碼。

在政策套用後變更的 Kaspersky 程式設定將在其各自手冊中詳細介紹。

在政策被建立後，被鎖定的設定（標記了鎖頭圖示（ ））即在用戶端裝置上生效，無論先前為應用程式指定了什麼設定。

在子群組中顯示繼承的政策

要為子群組啟用顯示繼承政策，請執行以下操作：

1. 在主控台樹狀目錄中，選取需顯示其所繼承政策的群組。
2. 在所選群組的工作區中，選取**政策**頁籤。
3. 在政策清單的上下文功能表中，選取"**檢視 → 繼承的政策**"。

   繼承的政策會顯示在帶有以下圖示的政策清單中：

- —如果它們從主管理伺服器上建立的群組中繼承。
- —如果它們從頂級群組繼承。

  當啟用設定繼承模式後，繼承的政策只能在建立此政策的群組中修改。在繼承此政策的群組，無法修改此政策。

啟動政策

要為所選群組啟用政策，請執行以下操作：

1. 在此群組的工作區中的**政策**頁籤，選取必須啟動的政策。
2. 要啟用此政策，請執行下列操作之一：
   - 在政策的上下文功能表中，選取**啟用政策**。
   - 在政策內容視窗中，開啟**一般** 區域並從**政策狀態**設定群組選取**啟用政策**。

該政策即對所選管理群組啟動了。

政策套用大量用戶端裝置後，管理伺服器的負載和網路流量在一段時間內會顯著增加。

在出現病毒爆發事件時自動啟用政策

要使政策在出現病毒爆發事件時自動啟用，請執行以下操作：

1. 在管理伺服器內容視窗中，開啟**病毒爆發**區域。
2. 點擊**配置在病毒爆發事件發生時要啟動的政策**連結以開啟**啟動政策**視窗，並新增政策至已選取要在病毒爆發時啟動的政策清單。

如果政策在*病毒爆發*事件中啟動，您僅可以使用手動模式返回到先前政策。

套用漫遊政策

當裝置與企業網路斷開時，漫遊政策將生效。

若要套用漫遊政策：

在政策內容視窗中，開啟**一般**區域並在**政策狀態**設定群組中選取**漫遊政策**。

漫遊政策被套用到從企業網路斷開的裝置。

修改政策回溯變更

要修改政策：

1. 在主控台樹狀目錄中，選取**政策**資料夾。
2. 在**政策**資料夾的工作區，選取一個政策並使用上下文功能表轉到政策內容視窗。

3. 做相關變更。

4. 點擊**"套用"**。

   在**變更歷程**區域對政策所做的變更將儲存在政策內容中。

如果必要，您可以回溯對政策所做的變更。

要回溯對政策所做的變更：

1. 在主控台樹狀目錄中，選取**政策**資料夾。

2. 選取需要回溯變更的政策，使用上下文功能表轉到政策內容資料夾。

3. 在政策內容視窗中，選取**變更歷程**區段。

4. 在政策修訂清單中，選取您要回溯的修訂號。

5. 點擊**進階**按鈕並在下拉清單中選取**回溯**。

檢視政策發佈狀態圖表

在卡巴斯基安全管理中心中，您可以檢視每個裝置上政策執行的結果。

要檢視每個裝置上的政策發佈狀態：

1. 在群組的工作區中，在**政策**頁簽上選擇要查看其分發狀態的政策。
   右窗格中的圖表顯示政策執行的概述。

2. 點擊**詳細資訊**。
   政策強制執行結果視窗開啟。
   您可以匯出政策執行結果為 CSV 或 TXT 檔案。

比較政策

您可以為單個受管理應用程式比較兩個政策。比較之後，您收到政策設定相同點和不同點報告。例如，您可能在不同辦公室的不同管理員為單個受管理應用程式建立了多個政策時，或者在單個頂級政策被所有本機辦公室繼承並修改時必須比較這些政策。您可以用以下方法之一比較政策：透過選取一個政策並與另一個比較，或者透過從政策清單中比較任意兩個政策。

> 您只能比較修訂歷史記錄中具有目前修訂的政策。

要將政策與另一個進行比較：

1. 在主控台樹狀目錄中，選取**政策**資料夾。

2. 在**政策**資料夾的工作區中，選取您要比較的另一個政策。

3. 在政策的上下文功能表中，選擇**與其他政策比較**。

4. 在**選取政策**視窗中，選取要比較的政策。

5. 點擊**確定**。

一個把相同應用程式的兩個政策相比較的 HTML 格式的報告被顯示。

要從政策清單比較兩個政策：

1. 在**政策**資料夾的政策清單中，使用 **Shift** 或 **Ctrl** 鍵為單一受管理應用程式選取政策。

2. 在上下文功能表中，選取**比較**。

一個把相同應用程式的兩個政策相比較的 HTML 格式的報告被顯示。

比較 Kaspersky Endpoint Security for Windows 政策設定的報告還提供政策設定檔比較詳情。您可以最小化政策設定檔比較結果。要最小化，點擊區域名稱旁的箭頭圖示 ( )。

刪除政策

要刪除政策，請執行以下操作：

1. 在管理群組工作區中，在**政策**頁籤上選取需要刪除的政策。

2. 以下列方式之一刪除政策：

   - 在政策的上下文功能表中，選取**刪除**。
   - 在所選政策的資訊框中，點擊**刪除政策**連結。

複製政策

要複製政策，請執行以下操作：

1. 在必要群組的工作區中的**政策**標籤中選取一個政策。

2. 在政策的上下文功能表中，選取**複製**。

3. 在主控台樹狀目錄中，選取您要貼上該政策的群組。

   您可以複製政策到群組中。

4. 在所選群組政策清單的上下文功能表中，在**政策**標籤選取**貼上**。

系統會將所有政策設定連同政策一起複製並套用到目的群組的裝置上。如果在同一群組內複製和貼上政策，政策名稱後會自動新增 **(<下一個序號>)** 索引，例如 **(1)**、**(2)**。

活動政策在其被複製至目的群組時，複製的政策將為停用的狀態。如有需要您可以將其啟用。

匯出政策

要匯出政策，請執行以下操作：

1. 以下列方式之一匯出政策：
   - 透過在政策的上下文功能表中選取**所有工作 → 匯出**。
   - 在所選政策的資訊框中，點擊**匯出政策到檔案**連結。
2. 在開啟的"**另存為**"視窗中，指定政策檔案的名稱和路徑。按一下**儲存**按鈕。

匯入政策

要匯入政策，請執行以下操作：

1. 在相關群組工作區的**政策**頁籤中，選取下列政策匯入方法之一：
   - 透過在政策清單的上下文功能表中選取**所有工作 → 匯入**。
   - 在政策清單的管理區塊中，按一下**從檔案匯入政策**連結。
2. 在開啟的視窗中，指定您要匯入的政策檔案及路徑。按一下**開啟**按鈕。

匯入的政策會顯示在政策清單中。政策的設定和設定檔也會一併匯入。無論匯出期間選取的政策狀態如何，匯入的政策都處於非使用中狀態。您可以在政策內容中變更政策狀態。

> 如果新匯入政策的名稱與現有政策的名稱相同，則匯入政策的名稱將加上 **(<next sequence number>)** 索引，例如：**(1)**、**(2)**。

轉換政策

卡巴斯基安全管理中心可將舊版受管理卡巴斯基應用程式的政策轉換為同一應用程式的最新版本的政策。轉換後的政策會保留更新之前指定的當前管理員設定，並包括來自最新版本應用程式的新設定。如果將政策轉換為受管理卡巴斯基應用程式的最新版本，則您無法在安裝了早期版本應用程式外掛程式的管理伺服器上開啟該政策。卡巴斯基應用程式的管理外掛程式可判斷這些應用程式的政策是否可以轉換。有關為每個受支援的卡巴斯基應用程式轉換政策的資訊，請參閱下列相關說明：

- **適用於工作站的卡巴斯基應用程式：**
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Linux Elbrus Edition
  - Kaspersky Endpoint Security for Mac
  - Kaspersky Endpoint Agent
  - Kaspersky Embedded Systems Security for Windows
- **Kaspersky Industrial CyberSecurity:**
  - Kaspersky Industrial CyberSecurity for Nodes
  - Kaspersky Industrial CyberSecurity for Linux Nodes
  - Kaspersky Industrial CyberSecurity for Networks（不支援集中佈署）
- **適用於行動裝置的卡巴斯基應用程式：**
  - Kaspersky Endpoint Security for Android
  - Kaspersky Security for iOS
- **適用於檔案伺服器的卡巴斯基應用程式：**
  - Kaspersky Security for Windows Server
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Endpoint Security for Linux
- **適用於虛擬機的卡巴斯基應用程式：**
  - Kaspersky Security for Virtualization Light Agent
  - Kaspersky Security for Virtualization Agentless

- **適用於郵件系統和 SharePoint/協作伺服器的卡巴斯基應用程式：**
  - Kaspersky Security for Linux Mail Server
  - Kaspersky Security for Microsoft Exchange Servers
- **適用於偵測鎖定式攻擊的卡巴斯基應用程式：**
  - Kaspersky Sandbox
  - Kaspersky Endpoint Detection and Response Optimum
  - Kaspersky Managed Detection and Response
- **適用於 KasperskyOS 裝置的卡巴斯基應用程式：**
  - Kaspersky IoT Secure Gateway
  - Kaspersky Security Management Suite（Kaspersky Thin Client 外掛程式）

若要轉換政策，請執行以下操作：

1. 在主控台樹狀目錄中，選取您希望為其轉換政策的管理伺服器。
2. 在管理伺服器的上下文功能表選取**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啟動。遵照精靈的說明。

精靈完成後會建立新政策，此政策會沿用當前管理員的政策設定和最新版本卡巴斯基應用程式的新設定。

管理政策設定檔

本節說明管理政策設定檔，並提供查看政策設定檔、更改政策設定檔優先等級、建立政策設定檔、修改政策設定檔、複製政策設定檔、建立政策設定檔啟動規則，以及刪除政策設定檔的資訊。

管理政策設定檔

政策設定檔是政策的一組命名設定集合，當裝置狀態滿足特定啟動規則時，它會在用戶端裝置（電腦或行動裝置）上啟動。啟動設定檔會變更設定檔啟動之前已在電腦上活動的政策設定。這些設定將使用已在設定檔中指定的值。

政策設定檔用於單一管理群組中的裝置在不同政策設定下執行。例如，可能發生管理群組中的一些裝置的政策設定必須被變更的情況。這種情況下，您可以為該政策配置政策設定檔，這允許您編輯管理群組中所選裝置的政策設定。例如，政策禁止在「使用者」管理群組的所有裝置上執行 GPS 導航軟體。GPS 導航軟體僅在「使用者」管理群組中的單個裝置上是必須的——該裝置屬於所僱傭的導遊。您可以標記該裝置為「導遊」並重新設定政策設定檔，以便它僅允許 GPS 軟體在標記為「導遊」的裝置上執行，同時保持所有剩餘政策設定。這種情況下，如果標記為「導遊」的裝置出現在「使用者」管理群組，它將被允許執行 GPS 導航軟體。執行 GPS 導航軟體仍將在「使用者」管理群組的其他裝置上被禁止，除非它們也被標記為「導遊」。

設定檔僅被以下政策支援：

- Kaspersky Endpoint Security for Windows 的政策
- Kaspersky Endpoint Security for Mac 的政策
- Kaspersky Mobile Device Management 外掛程式版本 10 Service Pack 1 到版本 10 Service Pack 3 Maintenance Release 1 的政策
- Kaspersky Device Management for iOS 外掛程式政策
- Kaspersky Security for Virtualization 5.1 Light Agent for Windows 的政策
- Kaspersky Security for Virtualization 5.1 Light Agent for Linux 的政策

政策設定檔簡化了政策套用的用戶端裝置的管理：

- 政策設定檔設定可能不同於政策設定。
- 您無需維護和手動套用單一政策中，僅數項設定不同的多個實例。
- 您無需為漫遊使用者單獨分配政策。
- 您可以匯出和匯入政策設定檔，以及基於現有政策設定檔建立新的政策設定檔。
- 一個政策可以擁有多個活動政策設定檔。僅滿足裝置上啟動規則的設定檔才能套用到該裝置。
- 設定檔服從政策層級。一個繼承政策包括所有高等級政策的設定檔。

設定檔的優先權

為政策建立的設定檔優先以名稱遞減排列。例如，如果在清單中設定檔 X 比設定檔 Y 更高，則 X 比後者具有更高優先順序。多個設定檔可以同時套用到一個裝置。如果設定值在不同設定檔中有變化，最高優先順序設定檔中的值將被套用到該裝置。

設定檔啟動規則

當啟動規則觸發時，政策設定檔在用戶端裝置上啟動。*啟動規則*是個條件集合，當滿足時，則在裝置上開啟政策設定檔。啟動規則可以包含以下條件：

- 用戶端裝置的網路代理用一組指定的連線參數連線管理伺服器，例如伺服器位址，埠號，等。
- 用戶端裝置已離線。
- 已為用戶端裝置分配了指定標籤。
- 用戶端裝置被顯性（裝置立即位於所選單元）或隱性）裝置位於嵌套單元）放置於 Active Directory 特定單元，裝置或其所有者位於 Active Directory® 安全群組。
- 用戶端裝置屬於指定擁有者，或者裝置所有者包含在卡巴斯基安全管理中心的安全群組裡。
- 用戶端裝置所有者被分配了特殊角色。

管理群組層級結構中的政策

如果您正在低級別管理群組中建立政策，該新政策繼承高級別群組中活動政策的所有設定檔。相同名稱的設定檔被刪除。高級別群組的政策設定檔擁有更高的優先順序。例如，在管理群組 *A* 中，政策 *P(A)* 具有設定檔 *X1*、*X2* 和 *X3*（按優先權降序排列）。在管理群組 *A* 的子群組管理群組 *B* 中，政策 *P(B)* 會使用設定檔 *X2*、*X4*、*X5* 建立。然後系統將使用政策 *P(A)* 來修改 *P(B)*，這樣政策 *P(B)* 中的設定檔清單將顯示如下：*X1*、*X2*、*X3*、*X4*、*X5*（以遞減優先順序排列）。設定檔 *X2* 的優先順序會依照政策 *P(B)* 設定檔 *X2* 和政策 *P(A)*. 設定檔 *X2* 的初始狀態來決定。在政策 *P(B)* 被建立後，政策 *P(A)* 不再顯示在子群組 *B*。

每次您啟動網路代理，啟用和停用行動模式，或編輯為用戶端裝置分配的標籤清單時，將會重新評估活動政策。例如，RAM 大小在裝置上增加，從而啟動擁有大 RAM 的裝置上的政策設定檔。

政策設定檔的內容和限制

設定檔具有以下內容：

- 停用政策的設定檔對用戶端裝置沒有任何影響。
- 如果政策被設定為**漫遊政策**狀態，只有在裝置從企業網路斷開連線時才會套用該政策設定檔。
- 設定檔不支援對可執行檔的存取的靜態分析。
- 政策設定檔無法包含事件通知的任何設定。
- 如果裝置使用 UDP 連接埠 15000 連線至管理伺服器，則在為裝置分配標籤後，會在 1 分鐘內啟動對應的政策設定檔。
- 當您建立政策設定檔啟動規則時，您可以為網路代理連線到管理伺服器使用規則。

建立政策設定檔

設定檔建立僅可供以下應用程式政策使用：

- Kaspersky Endpoint Security 10 Service Pack 1 for Windows 或更新版本
- Kaspersky Endpoint Security 10 Service Pack 1 for Mac
- Kaspersky Mobile Device Management 外掛程式版本 10 Service Pack 1 到版本 10 Service Pack 3 Maintenance Release 1
- Kaspersky Device Management for iOS 外掛程式
- Kaspersky Security for Virtualization 5.1 Light Agent for Windows and Linux

要建立政策設定檔：

1. 在主控台樹狀目錄中，選取您要為其建立政策設定檔的管理群組。
2. 在所選群組的工作區中，選取**政策**頁籤。
3. 選取政策並使用上下文功能表轉換到政策內容視窗。

4. 開啟政策內容視窗中的**政策設定檔**區域並點擊**新增**按鈕。

   新政策設定檔精靈啟動。

5. 在精靈的**政策設定檔名稱**視窗，指定以下內容：

   a. 政策設定檔的名稱

      設定檔名稱不能包括 100 個以上字元。

   b. 政策設定檔狀態（*已啟用*或*已停用*）

      我們建議您僅在完成了政策設定檔啟動條件後建立和啟動不活動的政策設定檔。

6. 選取**關閉新政策設定檔精靈後，轉到政策設定檔啟動規則的配置**核取方塊以啟動新政策設定檔啟動規則精靈。請遵循精靈的步驟進行操作。

7. 在政策設定檔內容視窗中編輯政策設定檔設定，以您請求的方式。

8. 透過點擊**確定**儲存變更。

   設定檔被儲存。設定檔將在滿足啟動條件的裝置上啟動。

您可以為單個政策建立多個設定檔。已為政策建立的設定檔會顯示在**政策設定檔**區域中的政策內容中。您可以修改政策設定檔並變更設定檔優先順序，以及刪除設定檔。

修改政策設定檔

編輯政策設定檔的設定

只有 Kaspersky Endpoint Security for Windows 的政策才支援編輯政策設定檔。

修改政策設定檔：

1. 在主控台樹狀目錄中，選取必須為其修改政策設定檔的管理群組。

2. 在群組的工作區中，選取**政策**頁籤。

3. 選取政策並使用上下文功能表轉換到政策內容視窗。

4. 開啟政策內容的**政策設定檔**區域。

   此部分包含已為政策建立的設定檔的清單。設定檔按照它們的優先權顯示在該清單中。

5. 選取政策設定檔並點擊**內容**按鈕。

6. 在內容視窗中設定設定檔：

   - 如有需要，請在**一般**區域中變更設定檔名稱，並使用**啟用設定檔**方塊來啟用或停用設定檔。
   - 在**啟動規則**區域中，編輯設定檔啟動規則。
   - 在相應的區域中編輯政策設定。

7. 點擊**確定**。

您已變更的設定將在裝置與管理伺服器同步之後生效（如果政策設定檔處於活動狀態），或在啟動規則觸發後生效（如果政策設定檔處於非活動狀態）。

變更政策設定檔的優先權

政策設定檔的優先權決定了設定檔在用戶端裝置上的啟動順序。如果為不同政策設定檔設定了相同啟動規則，則會使用優先權。

範例：已經建立了以下兩個政策設定檔：*設定檔 1*和*設定檔 2*，它們的差異是某一個設定分別使用各自的值（*值 1*和*值 2*）。*設定檔 1*的優先權高於*設定檔 2*。此外，還有一些設定檔，它們的優先權低於*設定檔 2*。這些設定檔的啟動規則是相同的。

當啟動規則觸發時，*設定檔 1*將被啟動。裝置上的設定將使用*值 1*。如果您刪除了*設定檔 1*，則*設定檔 2*將有最高的優先權，因此設定將使用*值 2*。

在政策設定檔清單上，設定檔按照它們各自的優先權顯示。優先權最高的設定檔排列在最前。您可使用向上箭頭 和向下箭頭 按鈕變更設定檔的優先順序。

刪除政策設定檔

要刪除政策設定檔：

1. 在主控台樹狀目錄中，選取您要為其刪除政策設定檔的管理群組。
2. 在所選群組的工作區中，選取**政策**頁籤。
3. 選取政策並使用上下文功能表轉換到政策內容視窗。
4. 開啟 Kaspersky Endpoint Security 的政策內容中的**政策設定檔**區域。
5. 選取您要刪除的政策設定檔並點擊 **刪除**按鈕。

政策設定檔將被刪除。活動狀態將傳遞到在裝置上觸發的啟動規則的另一個政策設定檔，或者傳遞到政策。

建立政策設定檔啟動規則

要建立政策設定檔啟動規則：

1. 在主控台樹狀目錄中，選取您要為其建立政策設定檔啟動規則的管理群組。
2. 在群組的工作區中，選取**政策**頁籤。
3. 選取政策並使用上下文功能表轉換到政策內容視窗。
4. 選取政策內容視窗中的**政策設定檔**區域。
5. 選取您需要建立啟動規則的政策設定檔，點擊**內容**按鈕。

   “政策設定檔”視窗開啟。

   如果政策設定檔清單為空，您可以建立政策設定檔。

6. 選取**啟動規則**區域並點擊**新增**按鈕。

   政策設定檔啟動規則精靈開啟。

7. 在**政策設定檔啟動規則**視窗中，選取啟動您要建立的政策設定檔時，一定會影響到該設定檔條件旁的核取方塊：

   - **政策設定檔啟動一般規則**

     選取該核取方塊依據裝置行動模式狀態設定裝置上的政策設定檔啟動規則、連線管理伺服器規則和分配給裝置的標記。

   - **Active Directory 使用規則**

     選取該核取方塊依據裝置在 Active Directory 組織單元中的出現或者裝置在 Active Directory 安全性群組中的成員關係設定裝置上的政策設定檔啟動規則。

   - **特殊裝置擁有者規則**

     選取該核取方塊依據裝置擁有者設定裝置上的政策設定檔啟動規則。

   - **硬體說明書規則**

     選取該核取方塊依據記憶體和邏輯處理器數量設定裝置上的政策設定檔啟動規則。

   精靈的附加頁面數量取決於您在第一步選取的設定。您可以稍後修改政策設定檔啟動規則。

8. 在**一般條件**視窗，指定以下設定：

- 在**裝置已離線**欄位中，在下拉清單指定裝置在網路中出現的條件：
  - **是**

    裝置在外部網路，管理伺服器不可用。

  - **否**

    裝置位於網路上，因此管理伺服器可供使用。

  - **未選取值**

    將不套用標準。

- 在**裝置位於指定的網路位置**欄位中，如果管理伺服器連線規則已在裝置上執行/未在裝置上執行，請使用下拉清單來設定政策設定檔的啟動：
  - **已執行 / 未執行**

    政策設定檔啟動條件（規則是否被執行）。

  - **規則名稱**

    用於連線到管理伺服器的裝置網路位置敘述，它的條件必須被滿足（或不滿足）以便啟動政策設定檔。

    用於連線到管理伺服器的裝置網路位置敘述可以在網路代理轉換規則中被建立或設定。

如果選取**政策設定檔啟動一般規則**的核取方塊，則會顯示**一般條件**視窗。

9. 在**使用標籤的條件**視窗，指定以下設定：

- **標籤清單**

  在標籤清單中，透過選中與相應標籤對應的方塊，可以指定政策設定檔中的裝置包含規則。

  您可以透過清單上方的欄位新增新標籤到清單，並點擊**新增**按鈕。

  政策設定檔包含具有選定標籤的裝置。如果清除方塊，則將不套用該標準。預設情況下已清除這些方塊。

- **套用到沒有指定標籤的裝置**

  如果您必須轉換您的標籤選項則啟用此選項。

  如果啟用此選項，政策設定檔將包含未帶有所選標籤的敘述的裝置。如果停用該選項，則不套用標準。

  預設情況下已停用該選項。

如果選取**政策設定檔啟動一般規則**核取方塊，則會顯示**使用標籤的條件**視窗。

10. 在**使用 Active Directory 的條件**視窗中，指定以下設定：

- **裝置所有者列入 Active Directory 安全群組**

  如果啟用此選項，當裝置屬於指定的安全群組或指定安全群組的子群組時，裝置上的政策設定檔被啟動。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

- **裝置列入 Active Directory 安全群組**

  如果選取此核取方塊，則會在裝置上啟動政策設定檔。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

- **在 Active Directory 組織單元中的裝置分配**

  如果啟用此選項，包含在指定 Active Directory 組織單元 (OU) 中的裝置上的政策設定檔將會啟動。如果停用此選項，則不套用設定檔啟動標準。

  預設情況下已停用該選項。

如果選中**Active Directory 使用規則**核取方塊，則會顯示**使用 Active Directory 的條件**視窗。

11. 在**使用裝置所有者的條件**視窗中，指定以下設定：

- **裝置所有者**

  啟用此選項依據裝置所有者在其上設定和啟用設定檔啟動規則。在此方塊下的下拉清單，你可以選取設定檔啟動標準：

  - 裝置屬於指定的擁有者（“=”符號）。
  - 裝置不屬於指定的擁有者（“#”符號）。

    如果啟用該選項，設定檔根據配置的標準在裝置上啟動。啟用此選項時，您可以指定裝置所有者。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

- **裝置所有者包含在內部安全群組**

  啟用此選項以卡巴斯基安全管理中心內部安全群組的資格在裝置上設定和啟用設定檔啟動規則。在此方塊下的下拉清單，你可以選取設定檔啟動標準：

  - 裝置所有者是指定安全群組的成員（“=”符號）。
  - 裝置所有者不是指定安全群組的成員（“#”符號）。

    如果啟用該選項，設定檔根據配置的標準在裝置上啟動。您可以指定卡巴斯基安全管理中心的安全性群組。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

- **由裝置所有者特定角色啟動政策設定檔**

  選取該選項以在裝置上根據所有者角色配置和啟用設定檔啟動規則。從現有角色清單手動新增角色。

  如果啟用該選項，設定檔根據配置的標準在裝置上啟動。

如果選取**特殊裝置擁有者規則**核取方塊，則會顯示**使用裝置所有者的條件**視窗。

12. 在**使用裝置說明的條件**視窗中，指定以下設定：

- **記憶體大小 (MB)**

  啟用此選項透過裝置上可用 RAM 容量在裝置上設定和啟用設定檔啟動規則。在此方塊下的下拉清單，你可以選取設定檔啟動標準：

  - 該裝置記憶體大小小於指定值（"<" 符號）。
  - 該裝置記憶體大小大於指定值（">" 符號）。

  如果啟用該選項，設定檔根據配置的標準在裝置上啟動。您可以指定裝置上的 RAM 容量。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

- **邏輯處理器數量**

  啟用此選項透過裝置上邏輯處理器數量在裝置上設定和啟用設定檔啟動規則。在此方塊下的下拉清單，你可以選取設定檔啟動標準：

  - 裝置上邏輯處理器數量少於或等於指定值（“<”符號）。
  - 裝置上邏輯處理器數量大於或等於指定值（“>”符號）。

  如果啟用該選項，設定檔根據配置的標準在裝置上啟動。您可以指定裝置上的邏輯處理器數量。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

如果選中**硬體說明書規則**核取方塊，則會顯示**使用裝置說明的條件**視窗。

13. 在**政策設定檔啟動規則名稱**視窗中的**規則名稱**欄位，指定規則的名稱。

設定檔將被儲存。當觸發啟動規則時，將在裝置上啟動該設定檔。

針對顯示在**啟動規則**區域中政策設定檔內容的設定檔，所建立的政策設定檔啟動規則。您可以修改或刪除任何政策設定檔啟動規則。

多個啟動規則可以被一起觸發。

裝置移動規則

我們建議您將裝置設定為透過*裝置移動規則*自動分配到管理群組。裝置移動規則由三個主要部分組成：名稱、執行條件（裝置內容邏輯表達）和目的管理群組。如果裝置內容滿足規則執行條件，則規則移動裝置到目的管理群組。

所有裝置移動規則都有優先順序。管理伺服器會檢查裝置屬性是否滿足每條規則的執行條件（遞增優先順序）。如果裝置內容滿足某條規則的執行條件，裝置被移動到目的群組，至此規則處理在該裝置上完成。如果裝置內容滿足多個規則的條件，裝置被移動到具有高優先順序的規則的目的群組。

裝置移動規則可以被間接建立。例如，在安裝套件或遠端安裝工作的內容中，您可以指定安裝網路代理後裝置必須被移動到的管理群組。而且，裝置移動規則可以被卡巴斯基安全管理中心管理員明確建立，在移動規則清單。清單位於管理主控台，在**未配置的裝置**群組內容中。

預設下，裝置移動規則用於裝置到管理群組的一次性初始分配。規則僅會移動**未配置的裝置**群組的裝置一次。一旦該規則移動裝置，該規則不會再次移動該裝置，即便您把裝置手動放回**未配置的裝置**群組也一樣。這是應用移動規則的建議方法。

您可以移動已經被分配的裝置到一些管理群組。要這麼做，請在規則的內容中，不要勾選**僅移動不屬於任何管理群組的裝置**核取方塊。

應用移動規則到已經分配到一些管理群組中的裝置會顯著增加管理伺服器負載。

僅移動不屬於任何管理群組的裝置"核取方塊在自動建立的移動規則的屬性中被鎖定。當您新增*遠端安裝應用程式*工作或建立獨立安裝套件時，會建立此類規則。

您可以建立重複影響單一裝置的移動規則。

我們強烈建議您避免從一個群組重複移動單一裝置到另一個群組（例如，為了套用特別政策到該裝置，執行特別群組工作，或者透過特別發佈點更新裝置）。

此類情境不被支援，因為它們顯著增加了管理伺服器負載和網路流量。這些情境也與卡巴斯基安全管理中心的操作原則衝突（尤其在存取權限、事件和報告方面）。必須找到其他解決方案，例如，透過使用政策設定檔、裝置分類的工作、根據標準方案分配網路代理。

克隆裝置移動規則

當您必須建立多個帶有相似設定的裝置移動規則時，您可以克隆現有規則然後變更所克隆規則的設定。例如，當您必須具有幾個帶有不同 IP 範圍和目的群組的相似的裝置移動規則時，這是有用的。

要克隆裝置移動規則：

1. 開啟主應用程式視窗。
2. 在 **未配置的裝置** 資料夾中，點擊**配置規則**。

   內容：未配置的裝置視窗開啟。
3. 在**移動裝置**區域中，選取您要複製的裝置移動規則。
4. 點擊**複製規則**。

   所選裝置移動規則的克隆將被新增到清單的結尾。

新規則以停用狀態被建立。您可以在任何時候編輯和啟用規則。

軟體分類

監控應用程式執行的主要工具是 *Kaspersky 類別*（也叫 *KL 類別*）。KL 類別說明卡巴斯基安全管理中心管理員簡化軟體分類和減少到受管理裝置的流量。

使用者類別必須僅對無法被分類成現有 KL 類別的應用程式建立（例如，對於自訂軟體）。基於應用程式安裝套件 (MSI) 或帶有安裝套件的資料夾建立的使用者類別。

如果有未透過 KL 類別分類的大軟體集可用，最好建立一個自動更新的類別。每次對包含分發套件的資料夾進行修改時，可執行檔的核對總和將被自動新增到該類別。

不要為資料夾 My Documents、%windir%、%ProgramFiles% 和 %ProgramFiles(x86)% 建立自動更新的軟體類別。在這些資料夾的檔案輪詢受頻繁變更的影響，這將導致增加管理伺服器負載和網路流量。您必須為軟體集建立專用資料夾並定期新增新項目。

安裝應用程式到用戶端組織裝置的先決條件

在用戶端組織的裝置上遠端安裝應用程式與在企業內遠端安裝的步驟相同。

要安裝應用程式到用戶端網路環境下的裝置，應執行下列操作：

- 在進行佈署應用程式到用戶端裝置前，您必須要先安裝網路代理。

  當透過卡巴斯基安全管理中心的服務供應商配置網路代理安裝套件時，應在安裝套件的內容視窗中調整下列設定：

  - 在**連線**區域中的**管理伺服器**字串，指定相同虛擬管理伺服器的位址，此位址已在發佈點本機安裝網路代理時指定。
  - 在**進階**區域中，選取**透過使用連線閘道連線到管理伺服器**核取方塊。在**連線閘道位址**字串，指定發佈點位址。您可以使用裝置 IP 位址或 Windows 網路中的裝置名稱。

- 選取**"透過發佈點使用作業系統資源"**作為網路代理安裝套件的下載方法。您可以選取以下下載方法：
  - 如果使用遠端安裝工作來安裝應用程式，您可以以兩種方式之一來指定下載方法：
    - 在**"設定"**視窗中，建立遠端安裝工作
    - 在遠端安裝工作的內容視窗，透過**"設定"**區域
  - 如果使用遠端安裝精靈來安裝應用程式，您可以在此精靈的**"設定"**視窗中選取下載方法。
- 由發佈點用於驗證的帳戶應該擁有在所有用戶端裝置上存取管理資源的權限。

檢視和編輯本機應用程式設定

卡巴斯基安全管理中心允許您使用管理主控台在裝置上管理本機應用程式設定。

*本機應用程式設定*是指裝置上的應用程式的設定。您可以使用卡巴斯基安全管理中心為管理群組中的裝置指定本機應用程式設定。

關於 Kaspersky 程式設定的詳細說明，請參閱相關手冊。

要檢視或修改應用程式的本機設定，請執行以下操作：

1. 在相關裝置所在的群組工作區中，選取**裝置**頁籤。
2. 在裝置內容視窗的**應用程式**區域中，選取相關的應用程式。
3. 點兩下滑鼠應用程式名稱或點擊**內容**按鈕，以開啟程式內容視窗。

以上操作將在開啟所選程式的本機設定視窗，您可以檢視並編輯這些設定。

您可以修改未被群組政策禁止修改的設定值（例如：未在政策中以鎖頭圖示（🔒）標記的設定）。

更新卡巴斯基安全管理中心和受管理應用程式

該部分敘述了更新卡巴斯基安全管理中心和受管理應用程式的步驟。

情境：定期更新 Kaspersky 資料庫與應用程式

該部分提供了定期更新 Kaspersky 資料庫、軟體模組和應用程式的情境。完成設定網路防護情境後，您必須維持防護系統的可靠性，確保管理伺服器和受管理裝置受到多種威脅的防護，包含病毒、網路攻擊與釣魚攻擊。

網路防護透過更新以下內容保持最新：

- 卡巴斯基資料庫和軟體模組
- 已安裝的 Kaspersky 應用程式，包括卡巴斯基安全管理中心元件和安全應用程式

當您完成此情境，您可確保以下事項：

- 您的網路被最近的 Kaspersky 軟體防護，包括卡巴斯基安全管理中心元件和安全應用程式。
- 對網路安全關鍵的病毒資料庫和其他 Kaspersky 資料庫保持最新。

先決條件

受管理裝置必須有與管理伺服器的連線。若沒有連線，請考慮手動更新 Kaspersky 資料庫、軟體模組與應用程式，或直接從 Kaspersky 更新伺服器更新。

管理伺服器必須具有到網際網路的連線。

在您開始之前，確保您已做了如下：

1. 根據透過卡巴斯基安全管理中心網頁主控台佈署 Kaspersky 應用程式的情境佈署 Kaspersky 安全應用程式到受管理裝置。
2. 建立了配置了所有所需政策、政策設定檔和工作，根據網路防護配置情境。
3. 分配了適當數量的發佈點，與受管理裝置和網路拓撲一致。

更新 Kaspersky 資料庫和應用程式分步驟進行：

1 選取更新方案

您可使用多種方案為卡巴斯基安全管理中心元件和安全應用程式安裝更新。選取一個或多個滿足您網路需求的方案。

2 建立管理伺服器的「將更新下載至儲存區」工作

該工作由卡巴斯基安全管理中心快速啟動精靈自動建立。如果您未執行精靈，立即建立工作。

需要該工作以從 Kaspersky 更新伺服器下載更新到管理伺服器儲存區，以及為卡巴斯基安全管理中心更新 Kaspersky 資料庫和軟體模組。更新被下載後，它們可以被傳播到受管理裝置。

如果您的網路被分配了發佈點，更新被從管理伺服器儲存區自動下載到發佈點儲存區。此種情況下，發佈點所在範圍的受管理裝置從發佈點儲存區下載更新，而不是從管理伺服器儲存區。

說明：

- 管理主控台：建立管理伺服器的「將更新下載至儲存區」工作
- 卡巴斯基安全管理中心網頁主控台：建立管理伺服器的「將更新下載至儲存區」工作

3 建立「將更新下載至發佈點儲存區」工作（可選）

預設下，更新被從管理伺服器下載到發佈點。您可以配置卡巴斯基安全管理中心直接從 Kaspersky 更新伺服器下載更新到發佈點。您可以下載到發佈點儲存區，例如，如果管理伺服器和發佈點之間的流量比發佈點和 Kaspersky 更新伺服器之間的流量貴，或者如果您的管理伺服器沒有網際網路存取。

當您的網路獲得指派的發佈點並且建立了*將更新下載至發佈點儲存區*工作後，發佈點會從 Kaspersky 更新伺服器下載更新，而非管理伺服器儲存區。

說明：

- 管理主控台：建立「將更新下載至發佈點儲存區」工作
- 卡巴斯基安全管理中心網頁主控台：建立「將更新下載至發佈點儲存區」工作

4 配置發佈點

當您的網路有指派的發佈點時，請確保**佈署更新**選項已在所有必要發佈點中啟用。當該選項對發佈點停用時，包含在發佈點範圍中的裝置從管理伺服器儲存區下載更新。

若您要受管理裝置僅從發佈點接收更新，請啟用網路代理政策的**僅透過發佈點分發檔案**選項。

5 使用行動模式更新下載或 diff 檔案最佳化更新程序（選用）

您可以透過使用行動模式更新下載（預設啟用）或使用 diff 檔案最佳化更新過程。對於每個網路段，您必須選取應用哪個功能，因為它們無法同時工作。

當行動模式更新下載被啟用時，一旦更新被下載到管理伺服器儲存區，在安全應用程式請求更新之前，網路代理就下載所需更新到受管理裝置。這確保了更新過程的可靠性。若要使用此功能，請啟用網路代理政策中的**提前從管理伺服器下載更新和病毒資料庫（建議）**選項。

如果您不使用行動模式更新下載，您透過使用 diff 檔案最佳化管理伺服器和受管理裝置之間的流量。當該功能被啟用時，管理伺服器或發佈點下載 diff 檔案，而不是整個 Kaspersky 資料庫或軟體模組檔案。diff 檔案敘述了資料庫或軟體模組的檔案的兩個版本之間的差異。因此，diff 檔案比整個檔案佔用更少的空間。這導致降低管理伺服器之間或發佈點和受管理裝置之間的流量。若要使用此功能，請啟用*將更新下載至管理伺服器儲存區*工作和/或*將更新下載至發佈點儲存區*工作內容中的**下載差異檔案**選項。

說明：

- 使用 diff 檔案更新 Kaspersky 資料庫和軟體模組
- 管理主控台：啟用和停用行動模式更新下載
- 卡巴斯基安全管理中心網頁主控台：啟用和停用行動模式更新下載

6 驗證已下載的更新（可選）

安裝下載的更新之前，您可以透過*更新驗證*工作驗證更新。該工作按順序執行透過測試裝置集的設定來配置的裝置更新工作和惡意軟體掃描工作。獲取工作結果時，管理伺服器開始或封鎖更新傳播到剩餘裝置。

*更新驗證*工作可作為「*將更新下載至管理伺服器儲存區*」工作的一部分執行。在「*將更新下載至管理伺服器儲存區*」工作的內容中，啟用管理主控台中的**發佈前驗證更新**選項，或卡巴斯基安全管理中心網頁主控台的**執行更新驗證**選項。

說明：

- 管理主控台：驗證下載的更新
- 卡巴斯基安全管理中心網頁主控台：驗證下載的更新

7 批准和拒絕軟體更新

預設下，下載的軟體更新具有*未定義*狀態。您可以變更狀態到*已批准*或*已拒絕*。批准的更新總是被安裝。如果更新需要檢視和接受最終使用者產品授權協議的條款，您需要先接受它們。此後，更新可以被傳播到受管理裝置。未定義的更新僅可以被安裝到網路代理和其他卡巴斯基安全管理中心元件，與網路代理政策設定一致。您設定了*已拒絕*狀態的更新將不被安裝到裝置。若先前安裝了安全應用程式的拒絕更新，卡巴斯基安全管理中心會嘗試從所有裝置解除安裝該更新。卡巴斯基安全管理中心元件更新無法被移除。

說明：

- 管理主控台：批准和拒絕軟體更新
- 卡巴斯基安全管理中心網頁主控台：批准和拒絕軟體更新

8 配置卡巴斯基安全管理中心元件的更新和修補程式的自動安裝

下載的網路代理更新和修補程式以及其他卡巴斯基安全管理中心元件被自動安裝。若您在網路代理內容中保持啟用**對未定義狀態的元件自動安裝可套用更新和修補程式**選項，則所有更新都會在下載至儲存區後自動安裝（或數個儲存區）。如果停用此選項，被下載和標注為*未定義*狀態的 Kaspersky 修補程式將僅在您改變其狀態為*已批准*是被安裝。

說明：

- 管理主控台：啟用和停用卡巴斯基安全管理中心元件的自動更新和修補程式
- 卡巴斯基安全管理中心網頁主控台：啟用和停用卡巴斯基安全管理中心元件的自動更新和修補程式

9 為管理伺服器安裝更新

管理伺服器軟體更新不取決於更新狀態。這些更新不會自動安裝，必須由管理員在管理主控台的**監控**頁籤（**管理伺服器** <伺服器名稱> → **監控**）或卡巴斯基安全管理中心網頁主控台中的**通知**區段（**監控和報告** → **通知**）進行初步核准。此後，管理員必須明確執行更新安裝。

10 為安全應用程式配置更新的自動安裝

為受管理應用程式建立*更新*工作，以提供對應用程式、軟體模組和 Kaspersky 資料庫（包括病毒資料庫）的及時更新。為了確保定期更新，建議您在配置工作排程時選取**當新更新下載至儲存區時**選項。

如果您的網路包括僅支援 IPv6 的裝置，並且您想要定期更新安裝在這些裝置上的安全應用程式，請確保管理伺服器（不早於 13.2 版）和網路代理（不早於 13.2 版）安裝在受管理裝置上。

預設下，Kaspersky Endpoint Security for Windows 和 Kaspersky Endpoint Security for Linux 的更新在您變更更新狀態到*已批准*後被安裝。您可以在*更新*工作中變更更新設定。

如果更新需要檢視和接受最終使用者產品授權協議的條款，您需要先接受它們。此後，更新可以被傳播到受管理裝置。

說明：

- 管理主控台：在裝置上自動安裝 Kaspersky Endpoint Security 更新
- 卡巴斯基安全管理中心網頁主控台：在裝置上自動安裝 Kaspersky Endpoint Security 更新

結果

當情境完成時，卡巴斯基安全管理中心被配置在更新被下載至管理伺服器儲存區或發佈點儲存區時更新 Kaspersky 資料庫和已安裝的 Kaspersky 應用程式。您然後可以繼續監控網路狀態。

關於更新 Kaspersky 資料庫、軟體模組和應用程式

為了確保管理伺服器和受管理裝置的防護是最新的，您必須提供以下內容的定期更新：

- 卡巴斯基資料庫和軟體模組

  在下載卡巴斯基資料庫和軟體模組之前，卡巴斯基安全管理中心會檢查卡巴斯基伺服器是否可以存取。如果無法使用系統 DNS 存取伺服器，則應用程式使用公用 DNS 伺服器。這是為了確保更新病毒資料庫並維護受管裝置的安全級別。

- 已安裝的 Kaspersky 應用程式，包括卡巴斯基安全管理中心元件和安全應用程式

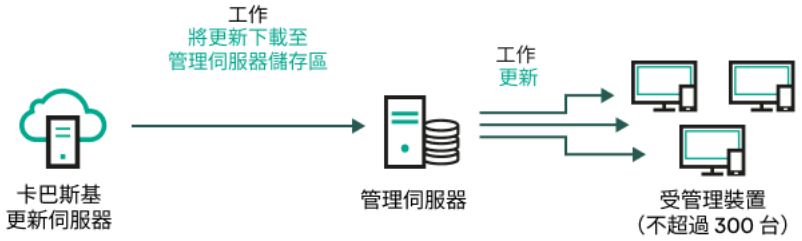
取決於您網路的配置，您可以使用以下方案來下載和分發所需更新到受管理裝置：

- 通過使用單個工作：*將更新下載至管理伺服器儲存區*
- 透過使用兩個工作：
  - *將更新下載至管理伺服器儲存區*工作
  - *將更新下載至發佈點儲存區*工作
- 透過本機資料夾、共用資料夾或 FTP 伺服器手動。

- 直接從卡巴斯基更新伺服器到受管理裝置上的 Kaspersky Endpoint Security
- 如果管理伺服器沒有網際網路連線，則透過本機或網路資料夾

使用將更新下載至管理伺服器儲存區工作

在此方案中，卡巴斯基安全管理中心會透過*將更新下載至管理伺服器儲存區*工作下載更新。在單一網段包含少於 300 台受管理裝置或每個網段包含少於 10 台受管理裝置的小網路中，更新直接從管理伺服器儲存區被分發到受管理裝置（參見下圖）。

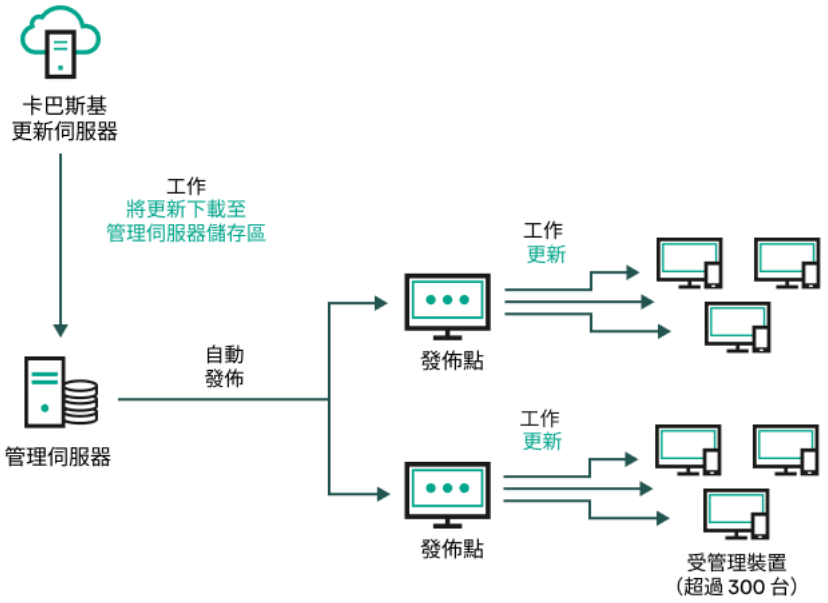


使用將更新下載至管理伺服器儲存區工作在沒有發佈點狀態下更新

預設下，管理伺服器與 Kaspersky 更新伺服器通訊並使用 HTTPS 協定下載更新。您可以配置管理伺服器使用 HTTP 協定，而不是 HTTPS。

如果您的網路中單一網段包含多於 300 台受管理裝置或每個網段包含多於 9 台受管理裝置，我們建議您使用發佈點傳播更新到受管理裝置（參見下圖）。發佈點降低管理伺服器負載並最佳化管理伺服器和受管理裝置之間的流量。您可以計算數字並配置您網路所需的發佈點。

此種方案中，更新被從管理伺服器儲存區自動下載到發佈點儲存區。發佈點所在範圍的受管理裝置從發佈點儲存區下載更新，而不是從管理伺服器儲存區。



使用將更新下載至管理伺服器儲存區工作在有發佈點狀態下更新

當*將更新下載至管理伺服器儲存區*當工作完成時，系統會將以下更新下載至管理伺服器儲存區：

- Kaspersky 資料庫和卡巴斯基安全管理中心軟體模組

  這些更新被自動安裝。

- Kaspersky 資料庫和受管理裝置上安全應用程式的軟體模組

  這些更新透過 Kaspersky Endpoint Security for Windows 更新工作安裝。

- 管理伺服器更新

  這些更新不被自動安裝。管理員必須明確批准和執行更新安裝。

  需要本機管理員權限以安裝修補程式到管理伺服器。

- 卡巴斯基安全管理中心模組更新

  預設下，這些更新被自動安裝。您可以在網路代理政策中變更設定。

- 安全應用程式更新

  預設情況下，Kaspersky Endpoint Security for Windows 僅安裝您批准的更新。（您可以透過管理主控台或者透過卡巴斯基安全管理中心網頁主控台批准更新）。更新透過*更新*工作安裝且可以在工作內容中被配置。

*將更新下載至管理伺服器儲存區*工作在虛擬管理伺服器上不可用。虛擬管理伺服器的儲存區節點下的更新，將顯示已下載至主管理伺服器的更新。

您可以配置在測試裝置集上進行更新的操作和錯誤驗證。如果驗證成功，更新被分發到其他受管理裝置。

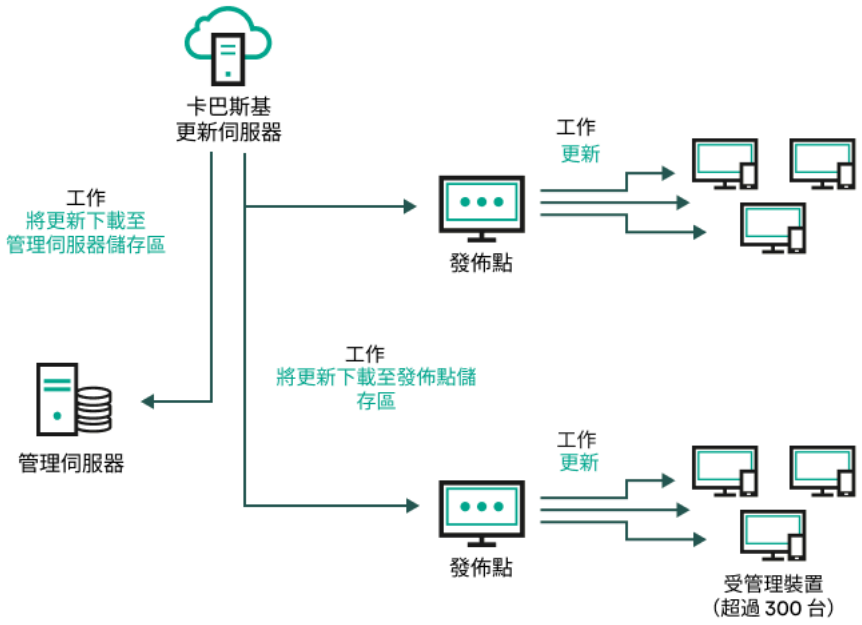
每個 Kaspersky 應用程式都從管理伺服器請求所需更新。管理伺服器集合這些更新並僅下載應用程式請求的更新。這確保了相同更新不被下載多次，且不必要更新不被下載。當執行*將更新下載至管理伺服器儲存區*工作時，管理伺服器自動傳送以下資訊到 Kaspersky 更新伺服器以便確保相關版本的 Kaspersky 資料庫和軟體模組的下載：

- 應用程式 ID 和版本
- 應用程式安裝 ID
- 啟動金鑰 ID
- 「*將更新下載至管理伺服器儲存區*」工作執行 ID

傳輸的資訊均不含個人詳情或其他機密資訊。AO Kaspersky Lab 依照法律需求防護資訊。

使用兩個工作：將更新下載至管理伺服器儲存區工作與將更新下載至發佈點儲存區工作

您可以直接從 Kaspersky 更新伺服器下載更新到發佈點儲存區，而不是從管理伺服器儲存區，然後分發更新到受管理裝置（參見下圖）。您可以下載到發佈點儲存區，例如，如果管理伺服器和發佈點之間的流量比發佈點和 Kaspersky 更新伺服器之間的流量貴，或者如果您的管理伺服器沒有網際網路存取。



使用將更新下載至管理伺服器儲存區工作與將更新下載至發佈點儲存區工作更新

預設下，管理伺服器和發佈點與 Kaspersky 更新伺服器通訊並使用 HTTPS 協定下載更新。您可以配置管理伺服器和/或發佈點使用 HTTP 協定，而不是 HTTPS。

若要實現該方案，請在*將更新下載至管理伺服器儲存區*工作外再建立*將更新下載至發佈點儲存區*工作。此後，發佈點將從 Kaspersky 更新伺服器下載更新，而不是從管理伺服器儲存區。

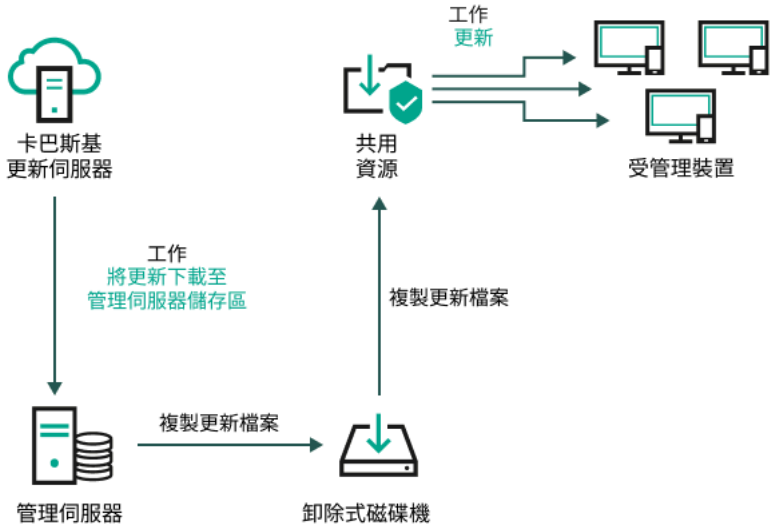
執行 macOS 的發佈點裝置無法從 Kaspersky 更新伺服器下載更新。

若一或多個執行 macOS 的裝置位於*下載更新至發佈點儲存區*工作範圍內，該工作會以*失敗*狀態完成，即使工作已在所有 Windows 裝置上成功完成。

此方案也需要*將更新下載至管理伺服器儲存區*工作，因為該工作被用於下載 Kaspersky 資料庫和卡巴斯基安全管理中心軟體模組。

透過本機資料夾、共用資料夾或 FTP 伺服器手動。

如果裝置未連線到管理伺服器，您可以使用本機資料夾或共用資料夾作為更新 Kaspersky 資料庫、軟體模組和應用程式的更新來源。在此方案中，您需要從管理伺服器儲存區複製所需更新到卸除式磁碟機，然後複製更新到在 Kaspersky Endpoint Security 設定中指定的本機資料夾或共用資料夾（參見下圖）。



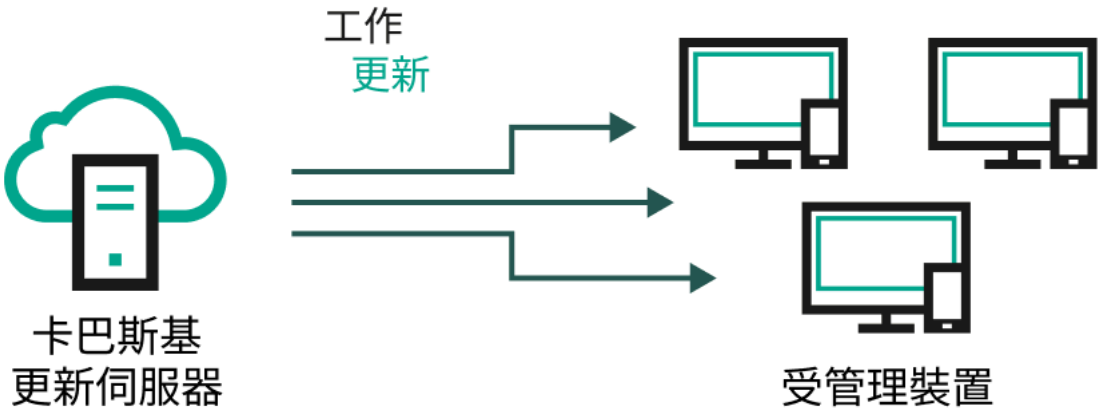
透過本機資料夾、共用資料夾或 FTP 伺服器更新

有關 Kaspersky Endpoint Security 更新來源的更多資訊，請參閱以下說明：

- Kaspersky Endpoint Security for Windows 說明
- Kaspersky Endpoint Security for Linux 說明

直接從卡巴斯基更新伺服器到受管理裝置上的 Kaspersky Endpoint Security

在受管理裝置上，您可以配置 Kaspersky Endpoint Security 直接從卡巴斯基更新伺服器接收更新（參見下圖）。



直接從卡巴斯基更新伺服器更新安全應用程式

在此方案中，安全應用程式不使用卡巴斯基安全管理中心提供的儲存區。要直接從 Kaspersky 更新伺服器接收更新，在安全應用程式介面中指定 Kaspersky 更新伺服器作為更新來源。有關這些設定的詳細資訊，請參閱以下說明：

- Kaspersky Endpoint Security for Windows 說明
- Kaspersky Endpoint Security for Linux 說明

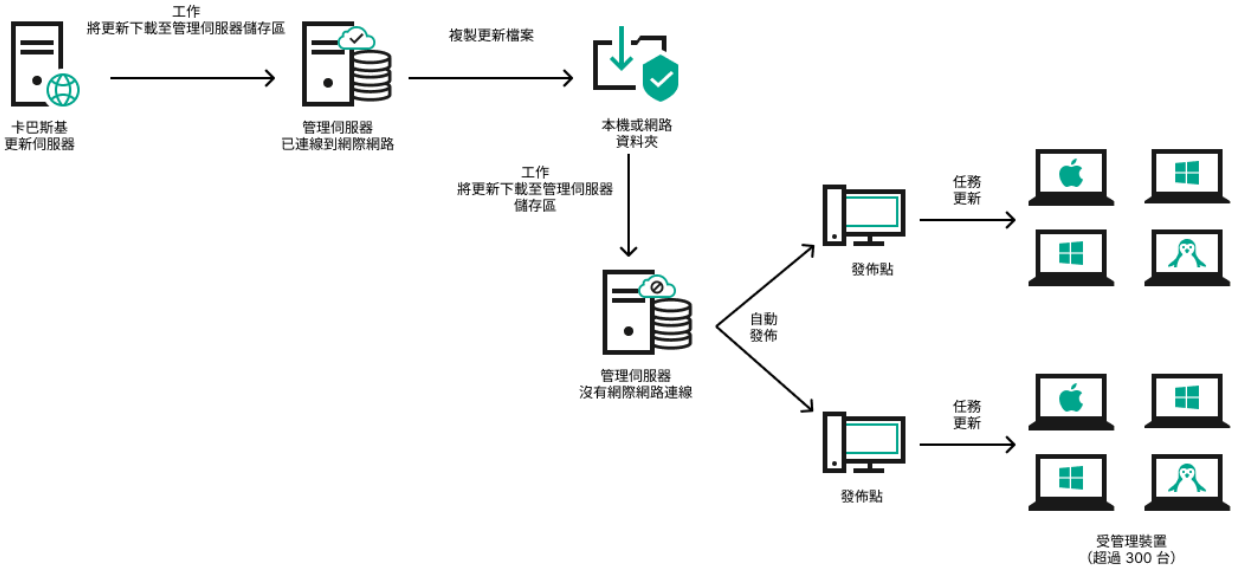
如果管理伺服器沒有網際網路連線，則透過本機或網路資料夾

如果管理伺服器沒有網際網路連線，您可以配置*將更新下載至管理伺服器儲存區*本機或網路資料夾下載更新。在這種情況下，您必須不時將所需的更新檔案複製到指定的資料夾中。例如，您可以從以下來源之一複制所需的更新檔案：

- 具有網際網路連線的管理伺服器（參見下圖）

  因為管理伺服器只下載安全應用程式請求的更新，所以管理伺服器管理的安全應用程式集合（一個有網際網路連線，一個沒有網際網路連線）必須比對。

  如果您用於下載更新的管理伺服器版本為 13.2 或更早，請開啟*將更新下載至管理伺服器儲存區*工作，然後啟用**使用舊配置下載更新**選項。



如果管理伺服器沒有網際網路連線，則透過本機或網路資料夾更新

- Kaspersky Update Utility

  由於此公用程式使用舊方案下載更新，請開啟*將更新下載至管理伺服器儲存區*工作的內容，然後啟用**使用舊配置下載更新**選項。

關於使用 diff 檔案更新 Kaspersky 資料庫和軟體模組

當卡巴斯基安全管理中心從 Kaspersky 更新伺服器下載更新時，它透過使用 diff 檔案最佳化流量。您也可以對從網路中其他裝置（管理伺服器、發佈點和用戶端裝置）獲取更新的裝置啟用對 diff 檔案的使用。

關於下載 diff 檔案功能

diff 檔案敘述了資料庫或軟體模組的檔案的兩個版本之間的差異。使用 diff 檔案節省您公司網路內的流量，因為 diff 檔案相比資料庫和軟體模組的完整檔案佔據更少的空間。如果對管理伺服器或發佈點啟用 *下載 diff 檔案*功能，diff 檔案被儲存到該管理伺服器或發佈點。結果，從該管理伺服器或發佈點獲取更新的裝置可以使用儲存的 diff 檔案更新它們的資料庫和軟體模組。

要最佳化對 diff 檔案的使用，我們建議您根據管理伺服器或發佈點的更新排程同步從管理伺服器或更新代理獲取更新的的裝置的更新排程。然而，即便裝置更新頻率小於從其獲取更新的管理伺服器或發佈點，流量也被節省。

下載 diff 檔案功能僅可以在版本 11 之後的管理伺服器和發佈點上啟用。若在早期版本的管理伺服器和發佈點上儲存 diff 檔案，請將它們升級至版本 11 或更新版本。

下載 diff 檔案功能與移動模式更新下載不相容。這意味著使用移動模式更新下載的網路代理即便在傳送更新到這些網路代理的管理伺服器或發佈點上啟用了下載 diff 檔案功能，也不下載 diff 檔案。

發佈點不對 diff 檔案的自動分發使用 IP 多點傳送。

啟用下載 diff 檔案功能

先決條件

方案的先決條件是：

- 管理伺服器和發佈點會升級到版本 11 或更新版本。
- 移動模式更新下載在網路代理政策設定中被停用。

階段

1. **在管理伺服器上啟用功能。**

   在將更新下載至管理伺服器儲存區設定中啟用該功能。

2. **為發佈點啟用該功能**

   對透過“將更新下載至發佈點儲存區”工作接收更新的發佈點啟用該功能。

   接著啟用對從管理伺服器接收更新的發佈點啟用該功能。

   該功能會在網路代理政策設定中，以及管理伺服器內容的**發佈點**區段中（如果您手動分配發佈點，而且要覆寫政策設定時）啟用。

要檢查下載 diff 檔案功能是否被成功啟用，您可以在執行方案之前和之後分別測試內部流量。

建立管理伺服器的「將更新下載至儲存區」工作

管理伺服器儲存區的「*將更新下載至管理伺服器儲存區*」工作會由卡巴斯基安全管理中心快速設定精靈自動建立。您僅可建立一個「*將更新下載至管理伺服器儲存區*」的工作。因此，若要建立「*將更新下載至管理伺服器儲存區*」工作，必須先在管理伺服器工作清單中移除此工作。

要建立「將更新下載至管理伺服器儲存區」工作：

1. 在主控台樹狀目錄中，選取**工作**資料夾。
2. 透過下列方式開始建立工作：
   - 在主控台樹狀目錄**工作**的物件上下文功能表中，選取**新增 → 工作**。
   - 在**工作**資料夾工作區中，選擇**建立工作**按鈕。

   新工作精靈啟動。遵照精靈的說明。
3. 在精靈的**選取工作類型**頁面，選取**將更新下載至管理伺服器儲存區**。

4. **在精靈的設定**頁面，指定以下工作設定：

- **更新來源**

  可使用以下資源作為管理伺服器的更新來源：

  - 卡巴斯基更新伺服器

    Kaspersky 應用程式可以從 Kaspersky 的 HTTP(S) 伺服器下載資料庫和程式模組更新。預設下，管理伺服器與 Kaspersky 更新伺服器通訊並使用 HTTPS 協定下載更新。您可以配置管理伺服器使用 HTTP 協定，而不是 HTTPS。

    預設選取。

  - 主管理伺服器

    該資源套用到為從屬或虛擬管理伺服器建立的工作。

  - 本機或網路資料夾

    包含最新更新的本機或網路資料夾。網路資料夾可以是 FTP 或 HTTP 伺服器，或者 SMB 共用。如果網路資料夾需要身分驗證，則僅支援 SMB 通訊協定。在選取本機資料夾時，您必須在安裝了管理伺服器的裝置上指定一個資料夾。

    更新來源所使用的 FTP 或 HTTP 伺服器或網路資料夾必須包含比對 Kaspersky 更新伺服器所建立的結構的資料夾結構（帶有更新）。

- **其他設定**：

  - **強制執行從屬管理伺服器的更新**

    如果啟用該選項，當新更新下載後管理伺服器立刻在從屬管理伺服器上啟動更新工作。更新工作透過使用在從屬管理伺服器上的工作屬性中配置的更新來源來啟動。

    如果停用此選項，從屬管理伺服器上的更新工作將根據排程啟動。

    預設情況下已停用該選項。

  - **複製下載的更新至其他資料夾**

    管理伺服器接收更新後，它複製它們到指定資料夾。如果您想要在您的網路上手動管理更新的分發，則使用該選項。

    例如，您可能要在以下情況下使用該選項：您組織的網路包含幾個獨立子網路，且每個子網路的裝置不能存取其他子網路。然而，所有子網路中的裝置都可以存取通用網路共用。此種情況下，您在子網路之一設定管理伺服器從 Kaspersky 更新伺服器下載更新，啟用該選項，然後指定該網路共用。對於其他管理伺服器的「將更新下載至儲存區」工作中，指定與更新來源相同的網路共用。

    預設情況下已停用該選項。

    - **除非複製完成，否則不強制更新裝置和從屬管理伺服器**

下載更新到用戶端裝置和從屬管理伺服器工作僅在這些更新從主更新資料夾被複製到附加更新資料夾後才啟動。

如果用戶端裝置和從屬管理伺服器從附加網路資料夾下載更新，則必須啟用該選項。

預設情況下已停用該選項。

- **使用舊配置下載更新**

  從版本 14 開始，卡巴斯基安全管理中心使用新方案下載資料庫和軟體模組的更新。對於使用新方案下載更新的應用程式，更新來源必須包含具有與新方案相容的中繼資料的更新檔案。如果更新來源包含的更新檔案的中繼資料僅與舊方案相容，請啟用**使用舊配置下載更新**選項。否則，更新下載工作將失敗。

  例如，當本機或網路資料夾被指定為更新來源並且此資料夾中的更新檔案由以下應用程式之一下載時，您必須啟用此選項：

  - Kaspersky Update Utility

    此公用程式使用舊方案下載更新。

  - 卡巴斯基安全管理中心 13.2 或更早版本

    例如，您的管理伺服器 1 沒有網際網路連線。在這種情況下，您可以使用具有網際網路連線的管理伺服器 2 下載更新，然後將更新放置到本機或網路資料夾以將其用作管理伺服器 1 的更新來源。如果管理伺服器 2 的版本為 13.2 或更早，請啟用管理伺服器 1 的工作中的**使用舊配置下載更新**選項。

  預設情況下已停用該選項。

5. 在**設定工作排程**精靈頁面，您可以為啟動工作建立排程。如果必要，指定以下設定：

- **排程開始：**

  選取工作執行排程並設定所選排程。

  - **每 N 小時**

    工作定期執行，按照指定小時數間隔，從指定的日期和時間開始。

    預設下，工作每 6 小時執行一次，從目前系統日期和時間開始。

  - **每 N 天**

    工作定期執行，按照指定天數間隔。此外，您可指定第一個工作執行的日期與時間。這些額外選項會在您建立的工作受到應用程式支援時可用。

    預設下，工作每天執行一次，從目前系統日期和時間開始。

  - **每 N 星期**

    工作定期執行，按照指定星期數間隔，從指定的星期和時間開始。

    預設下，工作每星期一於目前系統時間執行一次。

  - **每 N 分鐘**

    工作定期執行，按照指定分鐘數間隔，從工作建立日期的指定時間開始。

    預設下，工作每 30 分鐘執行一次，從目前系統時間開始。

  - **每天（不支援日光節約時間）**

    工作定期執行，按照指定天數間隔。排程不支援日光節約時間 (DST)。這意味著在夏令時開始和結束時當時鐘向前或向後撥動一小時時，實際工作啟動時間不變更。

    我們不建議您使用該排程。它用於向後相容卡巴斯基安全管理中心。

    預設下，工作每天於目前系統時間執行一次。

  - **每週**

    工作每週在指定星期和指定時間執行。

  - **按每星期中的指定日**

    工作定期執行，在每周指定日期的指定時間。

    預設下，工作每週五 6:00:00 P.M. 執行。

  - **每月**

工作定期執行，在指定月日的指定時間。

在缺少指定日的月份，工作在最後一天執行。

預設下，工作在每月的第一天執行，在目前系統時間。

- **手動**

  工作不自動執行。您僅可以手動啟動。

  預設情況下已選定此選項。

- **每個月在所選週的指定天**

  工作定期在指定月日的指定時間執行。

  預設情況下，不選取一個月中的任何一天。預設開始時間為 18:00。

- **在偵測到病毒爆發時**

  工作在發生*病毒爆發*事件後執行。選取將監控病毒爆發的應用程式類型。有下列應用程式類型可用：

  - 病毒防護工作站和檔案伺服器
  - 用於週邊防護的防毒軟體
  - 用於郵件伺服器的防毒軟體

  預設情況下選定所有應用程式類型。

  您可能想根據報告病毒爆發的安全應用程式類型執行不同的工作。此種情況下，刪除您不需要的應用程式類型選項。

- **在完成其它工作時**

  目前工作在其他工作完成後啟動。您可以選取先前工作如何結束（成功或帶有錯誤）以觸發目前工作的啟動。例如，您可能想使用***Turn on the device***選項執行開啟裝置工作，完成後，請執行*惡意軟體掃描*工作。只有當這兩項工作都被分配給相同的裝置時，此參數才會有作用。

- **執行錯過的工作**

  該選項決定在工作要啟動時用戶端裝置在網路中不可見時工作的行為。

  如果啟用該選項，系統將在下一次在用戶端裝置上執行 Kaspersky 應用程式時嘗試啟動工作。如果工作排程是**手動**、**一次**或**立即**，裝置在網路中可見或包含在工作範圍後，工作會立即啟動。

  如果停用此選項，則僅限排程的工作會在用戶端裝置上執行。若為**手動**、**一次**與**立即**排程，工作僅會在網路上顯示的用戶端裝置上執行。例如，您可能想為消耗資源的工作停用該選項，您僅想在業餘時間執行該工作。

  預設情況下已停用該選項。

- **使用工作啟動自動隨機延遲**

如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動，即是，*分佈式工作啟動*。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

當工作被建立時，根據工作中包含用戶端裝置的數量，分發啟動時間被自動計算。然後，工作總是在計算的開始時間啟動。然後當工作設定被編輯或者工作被手動啟動時，計算的工作啟動時間值被變更。

如果該選項被停用，工作依據排程在用戶端裝置上啟動。

- **使用工作啟動隨機延遲間隔（分鐘）**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

  預設情況下已停用該選項。預設時間間隔為一分鐘。

6. 在**定義工作名稱**精靈頁面，指定您正在建立的工作名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。
7. 在精靈的**完成工作建立**頁面，點擊**完成**按鈕關閉精靈。

   如果您想讓工作在精靈完成時立即啟動，選取**精靈完成時執行工作**核取方塊。

精靈結束後，**將更新下載至管理伺服器儲存區**出現在工作區的管理伺服器工作清單。

除了您在工作建立過程中指定的設定，您還可以變更所建立工作的其他屬性。

當管理伺服器執行「*將更新下載至管理伺服器儲存區*」工作時，資料庫和軟體模組更新將從更新來源下載並儲存在管理伺服器共用資料夾中。如果您為管理群組建立此工作，它將僅被套用到包含在指定管理群組中的網路代理。

這些更新將從管理伺服器共用資料夾分發至用戶端裝置和從屬管理伺服器。

建立「將更新下載至發佈點儲存區」工作

執行 macOS 的發佈點裝置無法從 Kaspersky 更新伺服器下載更新。

若一或多個執行 macOS 的裝置位於*下載更新至發佈點儲存區*工作範圍內，該工作會以*失敗*狀態完成，即使工作已在所有 Windows 裝置上成功完成。

您可以為管理群組建立*將更新下載至發佈點儲存區*工作。該工作將為包含在指定管理群組中的發佈點執行。

您可以使用該工作，例如，如果管理伺服器和發佈點之間的流量比發佈點和 Kaspersky 更新伺服器之間的流量貴，或者如果您的管理伺服器沒有網際網路存取。如果發佈點使用代理伺服器連線到網際網路，則必須在網路代理政策中指定相應的設定。

您可以為所選管理群組建立「將更新下載至發佈點儲存區」工作：

1. 在主控台樹狀目錄中，選取**工作**資料夾。
2. 在此資料夾的工作區，點擊**新工作**按鈕。

   新工作精靈啟動。遵照精靈的說明。
3. 在精靈的**選取工作類型**頁面，選取**卡巴斯基安全管理中心管理伺服器**節點，展開**進階**資料夾，然後選取**將更新下載至發佈點儲存區**工作。
4. **在精靈的設定**頁面，指定以下工作設定：

   - **更新來源**

     以下資源可作為發佈點的更新來源：

     - Kaspersky 更新伺服器

       Kaspersky 應用程式可以從 Kaspersky 的 HTTP(S) 伺服器下載資料庫和程式模組更新。

       預設情況下已選取此選項。

     - 本機或網路資料夾

       包含最新更新的本機或網路資料夾。網路資料夾可以是 FTP 或 HTTP 伺服器，或者 SMB 共用。如果網路資料夾需要身分驗證，則僅支援 SMB 通訊協定。在選取本機資料夾時，您必須在安裝了管理伺服器的裝置上指定一個資料夾。

       更新來源所使用的 FTP 或 HTTP 伺服器或網路資料夾必須包含比對 Kaspersky 更新伺服器所建立的結構的資料夾結構（帶有更新）。

   - **更新儲存資料夾**

     用於儲存已儲存更新的指定資料夾的路徑。您可以將指定的資料夾路徑複製到剪貼簿。您不能變更群組工作的指定資料夾的路徑。

   - **使用舊配置下載更新**

     從版本 14 開始，卡巴斯基安全管理中心使用新方案下載資料庫和軟體模組的更新。對於使用新方案下載更新的應用程式，更新來源必須包含具有與新方案相容的中繼資料的更新檔案。如果更新來源包含的更新檔案的中繼資料僅與舊方案相容，請啟用 **使用舊配置下載更新**選項。否則，更新下載工作將失敗。

     例如，當本機或網路資料夾被指定為更新來源並且此資料夾中的更新檔案由以下應用程式之一下載時，您必須啟用此選項：

     - Kaspersky Update Utility

       此公用程式使用舊方案下載更新。

     - 卡巴斯基安全管理中心 13.2 或更早版本

       例如，發佈點被配置為從本機或網路資料夾獲取更新。在這種情況下，您可以使用具有網際網路連線的管理伺服器下載更新，然後將更新放在發佈點上的本機資料夾中。如果管理伺服器的版本為 13.2 或更早，請啟用*將更新下載到發佈點的儲存區*工作中的**使用舊配置下載更新**選項。

     預設情況下已停用該選項。

5. 在精靈的**選取管理群組**頁面，點擊**瀏覽**並選取要套用工作的管理群組。

6. 在**設定工作排程**精靈頁面，您可以為啟動工作建立排程。如果必要，指定以下設定：

- **排程開始：**

  選取工作執行排程並設定所選排程。

  - **每 N 小時**

    工作定期執行，按照指定小時數間隔，從指定的日期和時間開始。

    預設下，工作每 6 小時執行一次，從目前系統日期和時間開始。

  - **每 N 天**

    工作定期執行，按照指定天數間隔。此外，您可指定第一個工作執行的日期與時間。這些額外選項會在您建立的工作受到應用程式支援時可用。

    預設下，工作每天執行一次，從目前系統日期和時間開始。

  - **每 N 星期**

    工作定期執行，按照指定星期數間隔，從指定的星期和時間開始。

    預設下，工作每星期一於目前系統時間執行一次。

  - **每 N 分鐘**

    工作定期執行，按照指定分鐘數間隔，從工作建立日期的指定時間開始。

    預設下，工作每 30 分鐘執行一次，從目前系統時間開始。

  - **每天（不支援日光節約時間）**

    工作定期執行，按照指定天數間隔。排程不支援日光節約時間 (DST)。這意味著在夏令時開始和結束時當時鐘向前或向後撥動一小時時，實際工作啟動時間不變更。

    我們不建議您使用該排程。它用於向後相容卡巴斯基安全管理中心。

    預設下，工作每天於目前系統時間執行一次。

  - **每週**

    工作每週在指定星期和指定時間執行。

  - **按每星期中的指定日**

    工作定期執行，在每周指定日期的指定時間。

    預設下，工作每週五 6:00:00 P.M. 執行。

  - **每月**

工作定期執行，在指定月日的指定時間。

在缺少指定日的月份，工作在最後一天執行。

預設下，工作在每月的第一天執行，在目前系統時間。

- **手動**

  工作不自動執行。您僅可以手動啟動。

  預設情況下已選定此選項。

- **每個月在所選週的指定天**

  工作定期在指定月日的指定時間執行。

  預設情況下，不選取一個月中的任何一天。預設開始時間為 18:00。

- **在偵測到病毒爆發時**

  工作在發生*病毒爆發*事件後執行。選取將監控病毒爆發的應用程式類型。有下列應用程式類型可用：

  - 病毒防護工作站和檔案伺服器
  - 用於週邊防護的防毒軟體
  - 用於郵件伺服器的防毒軟體

  預設情況下選定所有應用程式類型。

  您可能想根據報告病毒爆發的安全應用程式類型執行不同的工作。此種情況下，刪除您不需要的應用程式類型選項。

- **在完成其它工作時**

  目前工作在其他工作完成後啟動。您可以選取先前工作如何結束（成功或帶有錯誤）以觸發目前工作的啟動。例如，您可能想使用***Turn on the device***選項執行開啟裝置工作，完成後，請執行*惡意軟體掃描*工作。只有當這兩項工作都被分配給相同的裝置時，此參數才會有作用。

- **執行錯過的工作**

  該選項決定在工作要啟動時用戶端裝置在網路中不可見時工作的行為。

  如果啟用該選項，系統將在下一次在用戶端裝置上執行 Kaspersky 應用程式時嘗試啟動工作。如果工作排程是**手動**、**一次**或**立即**，裝置在網路中可見或包含在工作範圍後，工作會立即啟動。

  如果停用此選項，則僅限排程的工作會在用戶端裝置上執行。若為**手動**、**一次**與**立即**排程，工作僅會在網路上顯示的用戶端裝置上執行。例如，您可能想為消耗資源的工作停用該選項，您僅想在業餘時間執行該工作。

  預設情況下已停用該選項。

- **使用工作啟動自動隨機延遲**

如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動，即是，*分佈式工作啟動*。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

當工作被建立時，根據工作中包含用戶端裝置的數量，分發啟動時間被自動計算。然後，工作總是在計算的開始時間啟動。然後當工作設定被編輯或者工作被手動啟動時，計算的工作啟動時間值被變更。

如果該選項被停用，工作依據排程在用戶端裝置上啟動。

- **使用工作啟動隨機延遲間隔（分鐘）**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

  預設情況下已停用該選項。預設時間間隔為一分鐘。

7. 在**定義工作名稱**精靈頁面，指定您正在建立的工作名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。
8. 在精靈的**完成工作建立**頁面，點擊**完成**按鈕關閉精靈。

   如果您想讓工作在精靈完成時立即啟動，選取**精靈完成時執行工作**核取方塊。

當精靈完成操作時，**將更新下載至發佈點儲存區**會出現在目標管理群組主控台**工作**工作區的網路代理工作清單。

除了您在工作建立過程中指定的設定，您還可以變更所建立工作的其他屬性。

當*將更新下載至發佈點儲存區*工作執行時，資料庫和軟體模組更新從更新來源下載並儲存在共用資料夾。下載的更新將僅被包含在指定管理群組的發佈點和沒有更新下載工作的更新代理使用。

在管理伺服器內容視窗的**區域**視窗選取**發佈點**。在各發佈點內容的**更新來源**區域，您可指定更新來源（**從管理伺服器接收**或**使用強制更新下載工作**）。手動或自動分配的發佈點預設會選取**從管理伺服器接收**。這些發佈點將使用*將更新下載至發佈點儲存區*工作的結果。

每個發佈點的內容指定了為單個發佈點設定的網路資料夾。資料夾名稱可能依據不同發佈點而變化。因為這個原因，如果工作是為群組裝置建立，我們不建議您在工作內容中變更網路資料夾。

如果您要建立裝置的本機工作，可以在*將更新下載至發佈點儲存區*工作的內容中以更新變更網路資料夾。

設定管理伺服器的「將更新下載至儲存區」工作

要設定管理伺服器的"將更新下載至儲存區"工作：

1. 在**工作**主控台樹狀目錄資料夾的工作區，在工作清單中選取**將更新下載至管理伺服器儲存區**工作。
2. 以下列方式之一開啟工作內容視窗：
   - 透過從工作的上下文功能表中，選取**內容**。
   - 在所選檔案的資訊框中，點擊**設定工作**連結。

"*將更新下載至管理伺服器儲存區*"工作內容視窗將開啟。在此視窗中您可以調整更新下載至管理伺服器儲存區。

驗證已下載的更新

安裝更新到受管理裝置之前，您可以先透過*更新驗證*工作檢查更新。*更新驗證*工作會自動作為 *將更新下載至管理伺服器儲存區*工作的一部分執行。管理伺服器從更新來源下載更新、將其儲存在臨時儲存區並執行*更新驗證*工作。如果工作成功完成，更新將從臨時儲存區複製到管理伺服器共用資料夾（<卡巴斯基安全管理中心安裝資料夾>\Share\Updates）。它們被分發到所有以該管理伺服器為更新來源的用戶端裝置。

如果*更新驗證*工作的結果顯示位於臨時儲存區中的更新是錯誤的，或*更新驗證*工作發生錯誤，這些更新不會被複製到共用資料夾。管理伺服器保留之前的更新集。此外，有**當新更新下載至儲存區時**排程類型的工作也不會啟動。若新更新的掃描成功完成，這些操作會在*將更新下載至管理伺服器儲存區*工作下次啟動時執行。

如果在一台或多台測試裝置上出現以下情況，那麼更新就被認為是無效的：

- 發生了更新工作錯誤。
- 安全應用程式的即時防護狀態在套用更新後變更。
- 執行自訂掃描工作過程中發現一個被感染的物件。
- Kaspersky 程式出現執行階段錯誤。

如果在任何測試裝置上未出現以上情況，則此更新集就被認為是有效的，*更新驗證*工作被認為已成功完成。

在開始建立*更新驗證*工作之前 ，執行先決條件：

1. 用幾個測試裝置建立管理群組。您將需要該群組來驗證其更新。

   我們建議使用網路中防護最可靠、應用程式設定最常用的裝置作為測試裝置。這種方法提高了掃描期間病毒偵測的品質和概率，將誤報的風險降至最低。如果在測試裝置上偵測到病毒，*更新驗證*工作將被判定為不成功。

2. 為卡巴斯基安全管理中心支援的應用程式（例如 Kaspersky Endpoint Security for Windows 或 Kaspersky Security for Windows Server）建立*更新*和*惡意軟體掃描*工作。當建立*更新*和*惡意軟體掃描*工作時，指定測試裝置的管理群組。

   *更新驗證*工作將在測試裝置上順序執行*更新*和*惡意軟體掃描*工作以檢查所有更新是否有效。此外，在建立*更新驗證*工作時，您需要指定*更新*和*惡意軟體掃描*工作。

3. 建立*將更新下載至管理伺服器儲存區*工作。

要讓卡巴斯基安全管理中心將更新發佈至用戶端裝置前對下載的更新進行驗證，請執行以下操作：

1. 在**工作**資料夾工作區的工作清單中，選取「*將更新下載至管理伺服器儲存區*」工作。
2. 以下列方式之一開啟工作內容視窗：
   - 透過從工作的上下文功能表中，選取**內容**。
   - 在所選工作的資訊框中，按一下**設定工作**連結。
3. 如果存在*更新驗證*工作，請點擊**瀏覽**按鈕。在開啟的視窗中，在測試裝置的管理群組中選取*更新驗證*工作。

4. 如果您之前沒有建立*更新驗證*工作，請點擊**建立**按鈕。
   以上操作將執行*更新驗證*工作精靈。遵照精靈的說明。

5. 點擊**OK**關閉*將更新下載至管理伺服器儲存區*工作的內容視窗。

自動更新驗證被啟用。現在，您可以執行*將更新下載至管理伺服器儲存區*工作，它將從更新驗證開始。

設定測試政策和輔助工作

在建立*更新驗證*工作時，管理伺服器將建立測試政策、測試更新及掃描工作。

測試更新和掃描工作可能需要一些時間。這些工作在*更新驗證*工作執行時執行。在執行"*將更新下載至儲存區*"工作時，執行"*更新驗證*"工作。"*將更新下載至儲存區*"工作的持續時間也包含測試更新和掃描工作。

您可以變更測試政策和輔助群組工作的設定。

要變更測試政策和輔助工作的設定，請執行以下操作：

1. 在主控台樹狀目錄中，選取要為其建立*更新驗證*工作的群組。
2. 在此群組的工作台中，選取以下標籤之一：
   - **政策**，如果您希望編輯測試政策設定。
   - **工作**，如果您希望變更輔助工作設定。
3. 在標籤工作台中選取您希望變更其設定的政策或工作。
4. 以下列方式之一開啟政策（工作）內容視窗：
   - 從政策（工作）的上下文功能表中，選取**內容**。
   - 在所選政策（工作）的資訊框中，點擊**設定政策**（**設定工作**）連結。

要正確驗證更新，請在修改測試政策和輔助工作時設定以下限制：

- 在輔助工作設定中：
  - 將所有嚴重性等級為**"緊急事件"**和**"功能失效"**的工作儲存在管理伺服器。管理伺服器將使用這些類型的事件來分析應用程式執行狀況。
  - 使用管理伺服器作為更新來源。
  - 指定工作排程類型：**手動**。
- 在測試政策設定中：
  - 停用 iChecker 和 iSwift 掃描加速技術（**基本威脅防護 → 檔案威脅防護 → 設定 → 其他 → 掃描技術**）。
  - 選擇對受感染物件的操作：**解毒；解毒失敗則刪除/解毒；解毒失敗則**封鎖**/封鎖**。（**關鍵威脅防護→檔案威脅防護→偵測到威脅後的操作**）。
- 在測試政策和工作設定中：

  如果安裝軟體模組更新後需要重新啟動電腦，必須立即執行。如果裝置沒有重新啟動，則無法測試此類型的更新。對於一些需要重新啟動的應用程式更新安裝，重新啟動可能停用，或設定為需提示使用者確認。應在測試政策和工作設定中停用這些限制。

瀏覽已下載的更新

要檢視已下載的更新，

在主控台樹狀目錄的**儲存區**資料夾中，選擇**Kaspersky 資料庫和軟體模組更新**子資料夾。

Kaspersky 資料庫和軟體模組更新資料夾的工作區中將顯示管理伺服器中儲存的更新清單。

在裝置上自動安裝 Kaspersky Endpoint Security 更新

您可以在用戶端裝置上設定 Kaspersky Endpoint Security 自動更新資料庫和軟體模組。

要在裝置上設定下載和自動安裝 Kaspersky Endpoint Security 更新：

1. 在主控台樹狀目錄中，選取**工作**資料夾。
2. 透過以下方式建立**更新**工作:
   - 在主控台樹狀目錄的**工作**資料夾上下文功能表中，選取**新增 → 工作**。
   - 透過點擊在**工作**資料夾工作區的**新工作**按鈕。

   新工作精靈啟動。遵照精靈的說明。
3. 在精靈的**選取工作類型**頁面，選取 **Kaspersky Endpoint Security** 作為工作類型，然後選取**更新**作為工作子類型。

4. 遵照剩餘的精靈說明。

   精靈完成後，Kaspersky Endpoint Security 更新工作將被建立。新建立的工作顯示在**工作**資料夾工作區的工作清單。

5. 在**工作**資料夾的工作區域，選取您已建立的更新工作。

6. 從工作的上下文功能表中，選取**內容**。

7. 在開啟的工作內容視窗中，在 **區域**視窗選取**選項**。

   在**選項**區域，您可以定義本機或行動模式的更新工作設定：

   - **本機模式更新設定**：連線會在裝置和管理伺服器之間建立。
   - **行動模式更新設定**：卡巴斯基安全管理中心與裝置間不會建立連線（例如裝置未與網際網路連線時）。

8. 點擊**設定**按鈕選取更新來源。

9. 選取**下載應用程式模組更新**選項，更新應用程式資料庫同時下載和安裝應用程式模組。

   如果選定該核取方塊，Kaspersky Endpoint Security 在執行更新工作時，通知使用者有可用的軟體模組更新並且更新套件包含軟體模組更新。設定更新模組的使用：

   - **安裝嚴重與經批准的更新**。如果軟體模組有任何更新，Kaspersky Endpoint Security 自動安裝*關鍵*狀態的更新；其餘的更新會在您批准後安裝。
   - **僅安裝批准的更新**。如果軟體模組有任何更新，Kaspersky Endpoint Security 在安裝批准後安裝它們；它們將被透過程式介面或透過卡巴斯基安全管理中心本機安裝。

   如果軟體模組更新需要審查並接受產品授權協議的隱私政策，程式將在使用者接受最終使用者產品授權協議的條款和隱私政策後安裝更新。

10. 選取**複製更新到資料夾**選項，程式將已下載的更新儲存到透過點擊**瀏覽**按鈕指定的資料夾。

11. 點擊"**確定**"。

更新工作在執行時，程式傳送請求到 Kaspersky 更新伺服器。

一些更新需要安裝最新版本的管理外掛程式。

行動模式更新下載

受管裝置上的網路代理有時可能不會連線到管理伺服器來接收更新。例如，網路代理可能安裝在有時沒有網路連線的筆記型電腦上。而且，管理員可能會限制裝置連線到網路的時間。此種情況下，安裝了網路代理的裝置無法按照現有排程從管理伺服器接收更新。如果您已經使用網路代理設定了受管應用程式的更新（例如 Kaspersky Endpoint Security），每個更新都請求連線到管理伺服器。如果網路代理和管理伺服器之間沒有建立連線，則無法更新。您可以設定網路代理和管理伺服器之間的連線，以便網路代理在指定的時間段連線到管理伺服器。最壞的情況是，如果指定的時間段內沒有網路連線可用，資料庫將不會被更新。除此之外，如果多個受管應用程式同時嘗試存取管理伺服器以接收更新，可能會發生問題。此種情況下，管理伺服器可能停止回應（類似 DDoS 攻擊）。

為了避免上述問題，受管理應用程式的行動模式更新和模組的下載在卡巴斯基安全管理中心中實現。該模式提供裝置以分發更新，無論是否有管理伺服器通訊管道無法存取導致的臨時問題。該模式也降低管理伺服器負載。

行動模式更新下載如何工作

當管理伺服器接收更新時，它通知網路代理（安裝網路代理的裝置）將用於受管理應用程式的更新。當網路代理接收更新的資訊後，它提前從管理伺服器下載相關檔案。在第一次連線網路代理時，管理伺服器發起更新下載。網路代理下載所有更新到用戶端裝置後，更新對該裝置上的應用程式可用。

當用戶端裝置上的受管理應用程式嘗試存取網路代理以更新時，該網路代理檢查其是否具有所有所需的更新。如果在受管理應用程式請求更新之前 25 小時內，更新已從管理伺服器收到，則網路代理不連線到管理伺服器，而是從本機快取提供更新給受管理應用程式。當網路代理提供更新到用戶端裝置上的應用程式時，可能不會建立到管理伺服器的連線，但是更新不需要連線。

要在管理伺服器上發佈負載，裝置上的網路代理在管理伺服器指定的時間段連線到管理伺服器並隨機下載更新。該時間段取決於安裝了下載更新的網路代理的裝置的數量和更新的大小。要降低管理伺服器負載，您可以使用網路代理作為發佈點。

如果更新下載的行動模式被停用，更新根據更新下載工作的排程被分發。

預設下，行動模式更新下載已啟用。

行動模式更新下載僅受管理裝置才可使用，受管理應用程式擷取更新的工作會將**當新更新下載至儲存區時**選為排程類型。對於其他受管理裝置，以即時模式從管理伺服器接收更新的方案被使用。

如果將受管理應用程式設定為不從管理伺服器接收更新，而是改為從 Kaspersky 伺服器或網路資料夾接收，以及更新下載工作選取了**當新更新下載至儲存區時**作為排程類型時，建議您使用相關管理群組的代理伺服器政策設定停用行動模式更新下載。

啟用和停用行動模式更新下載

我們建議您避免停用行動模式更新下載。停用它可能導致更新傳送到裝置失敗。特殊情況下，Kaspersky 技術支援專家可能建議您清空**提前從管理伺服器下載更新和病毒資料庫**核取方塊。然後，您將必須確保接收 Kaspersky 應用程式更新的工作被設定。

要為管理群組啟用或停用行動模式更新下載：

1. 在主控台樹狀目錄中，選取您要啟用行動模式更新下載的管理群組。
2. 在群組工作區中，開啟**政策**頁籤。
3. 在**政策**頁籤，選取網路代理政策。
4. 在政策的上下文功能表中，選取**內容**。

   開啟網路代理政策內容視窗。
5. 在工作內容視窗中，選取**管理修補程式和更新**區域。
6. 選取或不要選取**提前從管理伺服器下載更新和病毒資料庫（建議）**核取方塊以啟用或停用更新下載的離線模式。

   預設下，行動模式更新下載已啟用。

這樣便啟用或停用了行動模式更新下載。

卡巴斯基安全管理中心元件的自動更新和修補程式

預設下，任何下載的更新和修補程式都會自動安裝於以下應用程式元件：

- Windows 網路輪詢
- 管理主控台
- Exchange 行動裝置伺服器
- iOS MDM 伺服器

卡巴斯基安全管理中心元件的自動更新和修補程式僅對 Windows 裝置可用。您可以停用這些元件的自動更新和修補程式。此種情況下，下載的任何更新和修補程式將在您改變其狀態到*已批准*後被安裝。帶有*未定義*狀態的更新和修補程式將不被安裝。

啟用和停用卡巴斯基安全管理中心元件的自動更新和修補程式

在裝置上安裝網路代理時，自動安裝卡巴斯基安全管理中心元件更新和修補程式被預設啟用。您可以在網路代理安裝過程中停用它，或稍後使用政策停用。

要在裝置上本機安裝網路代理時停用卡巴斯基安全管理中心元件自動更新和修補程式：

1. 在裝置上啟動網路代理本機安裝。
2. 在**進階設定**步驟，清空**自動安裝元件的未定義狀態的可應用更新和修補程式**核取方塊。
3. 遵照精靈的說明。

停用了卡巴斯基安全管理中心元件自動更新和修補程式的網路代理將被安裝在裝置。您可以稍後使用政策啟用自動更新和修補程式。

要在透過安裝套件安裝網路代理到裝置時停用卡巴斯基安全管理中心元件自動更新和修補程式：

1. 在主控台樹狀目錄中，選取**遠端安裝 → 安裝套件**資料夾。
2. 在卡巴斯基安全管理中心**網路代理<版本號>**套件，選取**內容**。
3. 在安裝套件內容中的**設定**區域不要選取**對未定義狀態的元件自動安裝可套用更新和修補程式**核取方塊。

停用了卡巴斯基安全管理中心元件自動更新和修補程式的網路代理將被從該封包安裝。您可以稍後使用政策啟用自動更新和修補程式。

如果在網路代理安裝到裝置時選取（清空）了該核取方塊，您可以後續啟用（或停用）使用網路代理政策自動更新。

要使用網路代理政策啟用或停用卡巴斯基安全管理中心元件的自動更新和修補程式：

1. 在主控台樹狀目錄中，選取您要啟用或停用自動更新和修補程式管理群組。
2. 在群組工作區中，開啟**政策**頁籤。
3. 在**政策**頁籤，選取網路代理政策。
4. 在政策的上下文功能表中，選取**內容**。
   開啟網路代理政策內容視窗。
5. 在工作內容視窗中，選取**管理修補程式和更新**區域。
6. 選取或不要選取**對未定義狀態的元件自動安裝可套用更新和修補程式**核取方塊以啟用或停用自動更新和修補。
7. 為該核取方塊設定鎖。

該政策將被應用到所選裝置，且卡巴斯基安全管理中心元件自動更新和修補程式將在這些裝置上被啟用（停用）。

自動發佈更新

卡巴斯基安全管理中心允許在用戶端裝置和從屬管理伺服器上自動分發並安裝更新。

自動將更新發佈至用戶端裝置

要在更新下載至管理伺服器儲存區之後立即自動發佈所選應用程式更新到用戶端裝置，請執行以下操作：

1. 連線至管理該用戶端裝置的管理伺服器。
2. 以下列方式之一為所選用戶端裝置建立更新工作：
   - 如果要將更新分發至屬於所選管理群組的用戶端裝置，請建立選定群組的工作。
   - 如果要將更新分發至屬於不同管理群組或不屬於任何管理群組的用戶端裝置，請建立指定裝置的工作。

   新工作精靈啟動。按照說明執行以下操作：
   a. 在**"工作類型"**精靈視窗中，在所需應用程式節點內選取更新工作。

      根據您為其建立更新工作的應用程式，顯示在**"工作類型"**視窗的更新工作名稱將有所不同。關於所選 Kaspersky 程式的更新工作名稱詳細資訊，請參閱對應手冊。

   b. 在**"排程"**精靈視窗中，在**"排程開始"**欄位中，選取**"當新更新下載至儲存區時"**。

新建的更新分發工作將在每次更新被下載到管理伺服器儲存區時在選定裝置上啟動。

若已為所選裝置建立必要應用程式的更新分配工作，請在工作內容視窗的**排程**區域中，在**排程的啟動**欄位選取**下載新更新至儲存區時**作為啟動選項。

將更新自動發佈至從屬管理伺服器

若要在更新下載至主管理伺服器儲存區之後立即發佈到從屬管理伺服器，請執行以下操作：

1. 在主控台樹狀目錄的主管理伺服器節點中，選取**工作**資料夾。
2. 在工作區的工作清單，選取管理伺服器的"將更新下載至管理伺服器儲存區"工作。
3. 以下列方式開啟所選工作的"**設定**"：
   - 透過從工作的上下文功能表中，選取"**內容**"。
   - 透過在所選工作的資訊框中點擊**編輯設定**連結。
4. 在工作內容視窗的"**設定**"區域，選取"**其他設定**"子區域，點擊"**設定**"連結。
5. 在開啟的**其他設定**視窗中，選取**強制從屬管理伺服器更新**方塊。
6. 在管理伺服器更新下載工作的設定中，在工作內容視窗**設定**標籤中，選取**強制從屬管理伺服器更新**方塊。

當主伺服器擷取到更新後，不論排程為何，從屬管理伺服器上的更新下載工作均會自動啟動。

主管理伺服器根據安裝在從屬管理伺服器上的應用程式更新病毒資料庫。不需要在主管理伺服器上安裝額外的外掛程式和建立安裝套件。

自動分配發佈點

我們建議您自動分配發佈點。然後卡巴斯基安全管理中心將自行選取哪個裝置要被分配為發佈點。

要自動分配發佈點：

1. 開啟主應用程式視窗。
2. 在主控台樹狀目錄中，選取您要為其自動指派發佈點的節點及管理伺服器名稱。
3. 在管理伺服器的上下文功能表中，按一下"**內容**"。
4. 在管理伺服器內容視窗的**區域**視窗選取**發佈點**。
5. 在視窗右側選取**自動分配發佈點**選項。

> 如果自動指派裝置作為發佈點被啟用，您無法手動配置發佈點，也不能編輯發佈點清單。

6. 點擊"**確定**"。

管理伺服器便自動指派和配置發佈點。

手動為裝置指派發佈點

卡巴斯基安全管理中心允許您指定裝置作為發佈點。

我們建議您自動分配發佈點。此種情況下，卡巴斯基安全管理中心將自行選取哪個裝置要被分配為發佈點。然後，如果您由於一些原因必須不自動分配發佈點（例如，如果您要使用單獨分配的伺服器），您可以在計算數量和配置後手動分配發佈點。

作為發佈點的裝置必須被防護，包括實體防護，以防範非授權的存取。

要手動指派裝置作為發佈點：

1. 在主控台樹狀目錄中，選取**管理伺服器**節點。
2. 在管理伺服器的上下文功能表中，選取**內容**。
3. 在管理伺服器內容視窗中，選取**發佈點**區域並點擊**新增**按鈕。若已選取**手動分配發佈點**則可使用此按鈕。

   新增發佈點視窗將開啟。
4. 在**新增發佈點**視窗，執行以下操作：

   a. 選取作為發佈點的裝置（選取管理群組，或指定裝置 IP 位址）。選取裝置時，請牢記發佈點的操作功能以及裝置作為發佈點的需求。

   b. 指定發佈點將向其分發更新的裝置。您可以指定管理群組或者網路位置敘述。
5. 點擊**確定**。

   您新增的發佈點將顯示在**發佈點**區域的發佈點清單。

6. 在清單中選取新增的發佈點並按一下**內容**按鈕來開啟內容視窗。

7. 在內容視窗中配置發佈點：

- **一般**區域中包含用於設定發佈點與用戶端裝置的互動設定。

  - **SSL 連接埠**

    用戶端裝置與發佈點之間，使用 SSL 進行安全連線的 SSL 埠號。

    預設情況下使用連接埠 13000。

  - **使用多點傳送**

    如果啟用此選項，程式會使用 IP 多點傳送，在群組中的各用戶端裝置上自動發佈安裝套件。

    IP 多點傳送會減少從安裝套件安裝應用程式至一組用戶端裝置的時間，但當您安裝應用程式至單一用戶端裝置時安裝時間會增加。

  - **IP 多點傳送位址**

    用於多點傳送的 IP 位址。您可以定義範圍是 224.0.0.0 – 239.255.255.255 的 IP 位址

    依預設，卡巴斯基安全管理中心會在指定範圍內自動指派唯一 IP 多點傳送位址。

  - **IP 多點傳輸連接埠號**

    IP 多點傳輸的埠號。

    預設情況下，埠號指定為 15001。如果執行管理伺服器的裝置指定為發佈點，連接埠 13001 預設用於 SSL 連線。

  - **佈署更新**

    更新被從以下來源分發到受管理裝置：

    - 此發佈點（如果啟用此選項）。
    - 其他發佈點、管理伺服器或卡巴斯基更新伺服器（如果停用此選項）。

    使用發佈點來佈署更新可以節省流量，因為您減少了下載次數。此外，您可以減輕管理伺服器上的負載並在發佈點之間重新定位負載。您可以計算網路的發佈點數量以最佳化流量和負載。

    如果停用此選項，管理伺服器上的更新下載和負載數量可能會增加。預設情況下已啟用該選項。

  - **佈署安裝套件**

安裝套件被從以下來源分發到受管理裝置：

- 此發佈點（如果啟用此選項）。
- 其他發佈點、管理伺服器或卡巴斯基更新伺服器（如果停用此選項）。

使用發佈點來佈署安裝套件可以節省流量，因為您減少了下載次數。此外，您可以減輕管理伺服器上的負載並在發佈點之間重新定位負載。您可以計算網路的發佈點數量以最佳化流量和負載。

如果停用此選項，管理伺服器上的安裝套件下載和負載數量可能會增加。預設情況下已啟用該選項。

- **將此發佈點用作推送伺服器**

在卡巴斯基安全管理中心中，發佈點可以用作透過移動協議管理的裝置的推送伺服器。例如，如果您希望能夠對 KasperskyOS 裝置與管理伺服器進行強制同步，則必須啟用推送伺服器。推送伺服器與啟用推送伺服器的發佈點具有相同的受管理裝置範圍。如果為相同管理群組指派了多個發佈點，則可以在每個發佈點上啟用推送伺服器。在這種情況下，管理伺服器會平衡發佈點之間的負載。

如果您管理安裝了 KasperskyOS 的裝置，或計劃這樣做，您必須使用發佈點作為推送伺服器。如果您想向用戶端裝置傳送推送通知，您還可以使用發佈點作為推送伺服器。

- **推送伺服器連接埠**

用戶端裝置將用於連線發佈點上的連接埠。預設情況下使用連接埠 13295。

- 在**範圍**區域中，指定發佈點將發佈更新的範圍（管理群組和/或網路定位）。
- 在 **KSN 代理**區域，您可以設定應用程式使用發佈點，以從受管理裝置轉發 KSN 請求。
  - **在發佈點端啟用 KSN 代理**

KSN 代理服務執行在用作發佈點的裝置上。使用該功能重新分發和最佳化網路流量。

發佈點傳送列在卡巴斯基安全網路聲明中的統計資訊到 Kaspersky。依預設，KSN 聲明位於 %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula。

預設情況下已停用該選項。啟用該選項僅在**使用管理伺服器作為代理伺服器**和**我同意使用卡巴斯基安全網路**選項在管理伺服器內容視窗中被啟用時起作用。

您可以指派活動被動叢集節點到發佈點並在該節點上啟用 KSN 代理伺服器。

  - **轉發 KSN 請求到管理伺服器**

發佈點從受管理裝置轉發 KSN 請求到管理伺服器。

預設情況下已啟用該選項。

  - **透過網際網路直接存取 KSN 雲端 / 私有 KSN**

發佈點從受管理裝置轉發 KSN 請求到 KSN 雲端或私有 KSN。在發佈點上自行產生的 KSN 要求頁會直接傳送至 KSN 雲端或私有 KSN。

已安裝網路代理版本 11（或更早版本）的發佈點無法直接存取私有 KSN。若要重新設定發佈點傳送 KSN 要求至私有 KSN，請為各發佈點啟用 **轉發 KSN 請求到管理伺服器**選項。

已安裝網路代理版本 12（或更新版本）的發佈點可直接存取私有 KSN。

- **當連線到私有 KSN 時略過代理伺服器設定**

  若您已在發佈點內容或網路代理政策中設定代理伺服器設定，但您的網路架構要求您直接使用私有 KSN，請啟用此選項。否則，從受管理應用程式的請求無法到達私有 KSN。

  如果您選擇**透過網際網路直接存取 KSN 雲端 / 私有 KSN**選項，則此選項可用。

- **TCP 連接埠**

  受管理裝置將用於連線到 KSN 代理伺服器的 TCP 埠號。預設埠號為 13111。

- **UDP 連接埠**

  如果需要網路代理透過 UDP 連接埠連線到管理伺服器，啟用**使用 UDP 連接埠**選項，並指定 **UDP 連接埠號**。預設情況下已啟用該選項。連線到管理伺服器的預設 UDP 連接埠是 15000。

- 在**裝置發現**區域，根據發佈點設定視窗 Windows 網域、Active Directory 和 IP 範圍的輪詢。

  - **Windows 網域**

    您可以啟用 Windows 網域裝置發現並為發現設定排程。

  - **Active Directory**

    您可以啟用 Active Directory 網域網路輪詢並為輪詢設定排程。

    如果您使用 Windows 發佈點，則可以選擇以下選項之一：

    - **輪詢目前 Active Directory 網域**。
    - **輪詢 Active Directory 網域樹系**。
    - **僅輪詢所選 Active Directory 網域**。如果您選取該選項，新增一個或更多 Active Directory 網域到清單。

    如果您使用安裝了網路代理版本 15 的 Linux 發佈點，則只能輪詢為其指定位址和使用者憑據的 Active Directory 網域。目前 Active Directory 網域和 Active Directory 網域樹系的輪詢不可用。

  - **IP 範圍**

您可以為 IPv4 範圍和 IPv6 網路啟用裝置發現。

如果啟用**啟用範圍輪詢**核取方塊，您可以新增掃已描範圍並為其設定排程。您可以新增 IP 範圍到已掃描範圍清單。

如果啟用**使用 Zeroconf 來輪詢 IPv6 網路**選項，發佈點將使用零配置網路（也稱為"*Zeroconf*"）自動輪詢 IPv6 網路。在這種情況下，指定的 IP 範圍將被忽略，因為發佈點會輪詢整個網路。如果發佈點執行 Linux，則**使用 Zeroconf 來輪詢 IPv6 網路**選項可用。要使用 Zeroconf Ipv6 輪詢，您必須在發佈點上安裝 avahi-browse 公用程式。

- 在**進階**區域中，指定發佈點必須用來儲存發佈資料的資料夾。
  - **使用預設資料夾**

    如果您選取此選項，應用程式使用發佈點上的網路代理安裝資料夾。

  - **使用指定資料夾**

    如果您選取該選項，則可以在下面的欄位中指定該資料夾的路徑。它可以是發佈點上的本機資料夾，也可以是企業網路上任何裝置的資料夾。

    發佈點上用於執行網路代理的帳戶必須具有對指定資料夾的存取權限以進行讀寫操作。

所選裝置作為發佈點執行。

僅執行 Windows 作業系統的裝置可以定義網路位置。網路位置無法定義在執行其他作業系統的裝置上。

從發佈點清單刪除裝置

要從發佈點清單刪除裝置：

1. 在主控台樹狀目錄中，選取**管理伺服器**節點。
2. 在管理伺服器的上下文功能表中，選取**內容**。
3. 在管理伺服器內容視窗的**發佈點**區域，選取作為發佈點的裝置，接著點擊**刪除**按鈕。

裝置將從發佈點清單刪除並將停止發佈點操作。

如果裝置被管理伺服器自動指定，則它無法從發佈點清單刪除。

透過發佈點下載更新

卡巴斯基安全管理中心允許發佈點從管理伺服器、Kaspersky 伺服器或本機網路資料夾接收更新。

如果您不需要指定更新來源，我們建議您使用管理群組的*將更新下載到發佈點的儲存庫*工作。有關詳細資訊，請參閱以下主題：建立將更新下載到發佈點的儲存庫工作。

要為發佈點設定更新下載：

1. 在主控台樹狀目錄中，選取**管理伺服器**節點。
2. 在管理伺服器的上下文功能表中，選取**內容**。
3. 在管理伺服器內容視窗的**發佈點**區域中，選取要透過其傳送更新到群組中用戶端裝置的發佈點。
4. 點擊**內容**按鈕以開啟所選發佈點的內容視窗。
5. 在發佈點內容視窗中，選取**更新來源**區域。
6. 為發佈點選取更新來源：
   - 要允許發佈點從管理伺服器自動接收更新，選取**從管理伺服器接收**：
     - **下載 diff 檔案**

       該選項啟用下載 diff 檔案功能。

       預設情況下已啟用該選項。
   - 若要透過工作允許發佈點接收更新，請選取**使用強制更新下載工作**：
     - 如果裝置上已存在此工作，點擊**瀏覽**按鈕，並在出現的清單中選取該工作。
     - 如果裝置上不存在此工作，點擊**新工作**按鈕以建立工作。新工作精靈啟動。遵照精靈的說明。

     "將更新下載至發佈點儲存區"工作是個本機工作。您必須為每個做為發佈點的裝置建立一個新的工作。

發佈點將從指定的更新來源接收更新。

從儲存區刪除軟體更新

要從管理伺服器儲存區刪除軟體更新：

1. 在主控台樹狀目錄的**進階** → **應用程式管理**資料夾中，選取**軟體更新**子資料夾。
2. 在**軟體更新**資料夾的工作區中，選取要刪除的更新。
3. 在更新的上下文功能表中，選取**刪除更新檔案**。

軟體更新將被從管理伺服器儲存區刪除。

為叢集模式中的 Kaspersky 應用程式安裝修補程式

卡巴斯基安全管理中心僅支援為叢集模式中的 Kaspersky 應用程式手動安裝修補程式。

要為 Kaspersky 應用程式安裝修補程式：

1. 現在修補程式到叢集的每個節點。
2. 在活動節點運行修補程式安裝。
3. 等待修補程式成功安裝。
4. 在所有叢集的子節點上執行修補程式。
   如果您從命令列執行修補程式，使用 `-CLUSTER_SECONDARY_NODE` 鍵。
   修補程式被安裝到叢集的所有節點。
5. 手動執行 Kaspersky 叢集服務。

叢集的每個節點作為安裝了網路代理的裝置顯示在管理主控台。

關於已安裝修補程式的資訊，請參閱**軟體更新**資料夾或者 Kaspersky 應用程式軟體模組更新版本報告。

管理用戶端裝置上的協力廠商應用程式

卡巴斯基安全管理中心允許您管理安裝在用戶端裝置上的 Kaspersky 或其他供應商的程式。

管理員可以操作以下功能：

- 基於指定的標準建立應用程式類別。
- 建立應用程式類別管理規則。
- 管理裝置上的應用程式執行。
- 執行清單、維護裝置上安裝軟體的登錄檔。
- 修復安裝在裝置上軟體的弱點。
- 安裝 Windows Update 和其他軟體製造商的更新到裝置。
- 為授權的應用程式群組監控產品授權金鑰的使用。

安裝協力廠商軟體更新

卡巴斯基安全管理中心允許您管理安裝在用戶端裝置上的軟體更新，並透過安裝所需更新來修復 Microsoft 應用程式和其他軟體廠商的產品中的弱點。

卡巴斯基安全管理中心透過更新搜尋工作搜尋更新和下載他們到更新儲存。完成更新的搜尋之後，應用程式為管理員提供了可用的更新和弱點的應用程式，並可使用這些更新資源。

Microsoft Windows 的可用更新透過 Windows Update 服務提供。管理伺服器可以被用作 Windows Server Update Services (WSUS) 伺服器。要使用管理伺服器作為 WSUS 伺服器，您應該設定和 Windows Update 的更新同步。在您設定了和 Windows Update 的資料同步後，管理伺服器以集中模式和設定的頻率在裝置上更新到 Windows Update 服務。

您也可以透過網路代理政策管理軟體更新。若要完成上述工作，您應使用政策建立精靈建立一個網路代理政策，並在對應的新建政策精靈視窗設定軟體更新。

管理員可在**應用程式管理**資料夾包含的**軟體更新**子資料夾中檢視可用更新的清單。該資料夾包含了管理伺服器擷取的可以被發佈到裝置的 Microsoft 應用程式和其他軟體廠商產品的更新清單。在檢視可用的更新資訊後，管理員可以將它們安裝到裝置。

卡巴斯基安全管理中心透過移除先前的應用程式並安裝新應用程式來更新應用程式。

在受管理裝置上更新協力廠商應用程式或修復協力廠商應用程式中的弱點時，可能需要使用者互動。例如，若協力廠商應用程式目前開啟，可能會提示使用者關閉協力廠商應用程式。

確保在主管理伺服器和從屬管理伺服器的 **設定介面** 視窗中中啟用了**顯示弱點和修補程式管理**選項。否則，更新搜尋工作將僅處理 WSUS 更新。

出於安全原因，卡巴斯基技術會自動掃描您使用弱點和修補程式管理功能安裝的任何協力廠商軟體更新以查找惡意軟體。這些技術用於自動檢查檔案，包括病毒掃描、靜態分析、動態分析、沙箱環境中的行為分析和機器學習。

卡巴斯基專家不會對可以使用弱點和修補程式管理功能安裝的協力廠商軟體更新進行手動分析。此外，卡巴斯基專家不會在此類更新中搜尋弱點（已知或未知）或未記錄的功能，也不會對上述段落中指定的更新以外的其他類型的更新進行分析。

在安裝更新到所有裝置前，您可以執行測試安裝，以確保安裝更新不會造成任何裝置出現應用程式故障。

情境：更新協力廠商軟體

本節提供在用戶端裝置安裝更新協力廠商軟體的情境。協力廠商軟體包含來自 Microsoft 和其他軟體廠商的應用程式。Microsoft 應用程式的更新會由 Windows Update 服務提供。

先決條件

管理伺服器必須連線到網際網路才能安裝除了 Microsoft 軟體之外的協力廠商軟體更新。

預設情況下，管理伺服器不需要網際網路連線即可在受管理裝置上安裝 Microsoft 軟體更新。例如，受管理裝置可以直接從 Microsoft Update 伺服器下載 Microsoft 軟體更新，也可以從具有組織網路中佈署的 Microsoft Windows Server Update Services (WSUS) 的 Windows Server 下載 Microsoft 軟體更新。將管理伺服器用作 WSUS 伺服器時，必須將管理伺服器連線到網際網路。

階段

更新協力廠商軟體採分階段進行：

1 搜尋所需更新

若要尋找受管理裝置必要的協力廠商軟體更新，請執行*弱點掃描和所需更新*工作。完成此工作時，卡巴斯基安全管理中心會收到偵測到的弱點清單，以及安裝於您在工作內容指定裝置上已安裝軟體需要的更新。

*弱點掃描和所需更新*工作會由管理伺服器快速設定精靈自動建立。若您未執行該精靈，請建立工作或立即執行快速啟動精靈。

說明：

- 管理主控台：掃描應用程式是否有弱點，排程尋找弱點和所需更新的工作
- 卡巴斯基安全管理中心網頁主控台：建立弱點掃描和所需更新工作、尋找弱點和所需更新的工作設定

2 分析已知更新清單

檢視**軟體更新**清單並決定要安裝的更新。若要檢視各更新的詳細資訊，請按一下清單中的更新名稱。對於清單中的各個更新，您也可檢視用戶端裝置上更新的統計資料。

說明：

- 管理主控台：檢視可用更新資訊
- 卡巴斯基安全管理中心網頁主控台：檢視可用協力廠商軟體更新的資訊

3 配置更新的安裝

當卡巴斯基安全管理中心收到協力廠商軟體更新清單時，您可使用*安裝必要更新並修復弱點*工作或*安裝 Windows Update 更新*，以在用戶端裝置安裝這些更新。建立其中一種這類工作。您可在**工作**頁籤或使用**軟體更新**清單建立這類工作。

*安裝所需更新並修復弱點*工作用來安裝 Microsoft 應用程式的更新，包括由 Windows Update 服務提供的更新，以及其他廠商軟體的更新。請注意，只有當您有弱點和修補程式管理功能的授權時，才可建立此工作。

*安裝 Windows Update 更新*工作不需要產品授權，但僅可用來安裝 Windows Update 更新。

若要安裝一些軟體更新，您必須接受安裝軟體的最終使用者產品授權協議 (EULA)。若您拒絕 EULA，則無法安裝該軟體更新。

您可依排程啟動更新安裝工作。指定工作排誠實，請確保更新安裝工作會在*弱點掃描和所需更新*工作完成後啟動。

說明：

- 管理主控台：修復應用程式中的弱點、檢視可用更新的資訊
- 卡巴斯基安全管理中心網頁主控台：建立安裝必要更新並修復弱點工作、建立並安裝 Windows Update 更新工作、檢視可用協力廠商軟體更新的資訊

4 排程工作

為確定更新清單永遠處於最新狀態，請排程*弱點掃描和所需更新*工作以不時自動執行。依預設，*弱點掃描和所需更新*工作設定為手動啟動。

若您已建立*安裝必要更新並修正弱點*工作，您可排程此工作與*弱點掃描和所需更新*工作的執行頻率相同或更少。排程*安裝 Windows Update 更新*工作時，請注意對於此工作，您必須在每次啟動此工作時定義更新清單。

排程工作時，請確定更新安裝工作會在*弱點掃描和所需更新*工作完成後啟動。

5 核准和拒絕軟體更新（選用）

若您已建立安裝必要更新並修復弱點工作，您可在工作內容中，指定更新安裝的規則。若您已建立安裝 Windows Update 更新工作，請略過此步驟。

對於各規則，您可定義更新來根據更新狀態進行安裝：*未定義*、*已核准*或*已拒絕*。例如，您可能要針對伺服器建立特定工作，並針對此工作設定規則，以允許僅安裝 Windows Update 更新，以及僅安裝有*已核准*狀態的更新。針對您要安裝的這些更新手動設定*已核准*狀態後。在此情況下，處於*未定義*或*已拒絕*狀態的 Windows Update 更新將不會安裝到您在工作中指定的伺服器。

對於少量更新而言，使用*已批准*狀態來管理更新安裝非常有效。若要安裝多個更新，請使用可在*安裝所需的更新和修復漏洞*工作中配置的規則。建議您僅為那些不符合規則中指定條件的特定更新設定*已批准*狀態。當您手動批准大量更新時，管理伺服器的效能下降，這可能導致伺服器過載。

預設下，下載的軟體更新具有*未定義*狀態。您可在**軟體更新**清單（**操作 → 修補程式管理 → 軟體更新**）變更狀態至*已核准*或*已拒絕*。

說明：

- 管理主控台：批准和拒絕軟體更新
- 卡巴斯基安全管理中心網頁主控台：批准和拒絕協力廠商軟體更新

6. **配置管理伺服器作為 Windows Server 更新服務 (WSUS) 伺服器（選用）運作**

   依預設，Windows Update 更新會從 Microsoft 伺服器下載至受管理裝置。您可變更此設定以使用管理伺服器作為 WSUS 伺服器。在此情況下，管理伺服器會以特定頻率將更新資料與 Windows Update 同步，並以集中模式提供更新給在網路裝置的 Windows Update。

   若要使用管理伺服器作為 WSUS 伺服器，您可建立執行 Windows Update 同步工作，並選取網路代理政策中的**使用管理伺服器作為 WSUS 伺服器**核取方塊。

   說明：

   - 管理主控台：從 Windows Update 透過管理伺服器同步更新、在網路代理政策中配置 Windows 更新
   - 卡巴斯基安全管理中心網頁主控台：建立執行 Windows Update 同步工作

7. **執行更新安裝工作**

   啟動*安裝所需更新並修復弱點*工作或*安裝 Windows Update 更新*工作。啟動這類工作時，更新會自動下載並安裝至受管理裝置。工作完成後，請確保工作清單出現*已成功完成*狀態。

8. **建立協力廠商軟體更新安裝結果的報告（選用）**

   若要檢視更新安裝的詳細統計，請建立**協力廠商軟體更新安裝結果報告**。

   說明：

   - 管理主控台：建立與檢視報告
   - 卡巴斯基安全管理中心網頁主控台：產生與檢視報告

結果

若已建立並設定*安裝所需更新並修復弱點*工作，更新會自動安裝在受管理裝置。系統會將新更新下載至管理伺服器儲存區，卡巴斯基安全管理中心會檢查更新是否符合更新規則中指定的條件。系統會將符合條件的所有新更新在下次工作執行時安裝。

若已建立*安裝 Windows Update 更新*工作，則系統僅會*安裝 Windows Update 更新*工作屬性中指定的這類更新。未來若要安裝下載至管理伺服器儲存區的新更新，您必須新增必要更新至現有工作的更新清單，或建立新*安裝 Windows Update 更新*工作。

檢視對於協力廠商應用程式可用的更新資訊

若要檢視安裝在用戶端裝置之協力廠商應用程式的可用更新清單，

在主控台樹狀目錄的**進階 → 應用程式管理**資料夾中，選取**軟體更新**子資料夾。

在該資料夾的工作台中，您可以檢視裝置上安裝應用程式的可用更新清單。

要檢視更新的內容，

在**軟體更新**資料夾的工作區中，從更新的上下文功能表中選取**內容**。

在更新的內容視窗中可以檢視以下資訊：

- 在**一般**部分，您可以檢視**更新批准狀態**：
  - **未定義** - 更新在更新清單中可用，但未獲准安裝。
  - **已批准**– 更新在更新清單中可用並已獲准安裝。
  - **已拒絕**– 更新被拒絕安裝。
- 在**內容**部分，您可以檢視**已自動安裝**欄位的值：
  - 如果"*安裝所需更新並修復弱點*"工作可以為應用程式安裝更新，則顯示 **自動地** 值。該工作會從協力廠商軟體供應商提供的網址自動安裝新的更新。
  - 如果卡巴斯基安裝管理中心無法自動安裝應用程式更新，則顯示**手動**值。您可以手動安裝更新。

  已自動安裝 欄位不對 Windows 應用程式更新顯示。

- 需要更新的用戶端裝置的清單。
- 需要安裝更新之前安裝的系統元件清單（先決條件）（如果有的話）。
- 更新將修復的軟體弱點。

批准和拒絕軟體更新

更新安裝工作的設定可能需要對要安裝的更新進行批准。您可以批准必須安裝的更新並拒絕不能安裝的更新。

例如，您可能想先在測試環境中檢查更新安裝以確保它們不干預裝置操作，僅在這之後允許安裝這些更新到用戶端裝置。

對於少量更新而言，使用*已批准*狀態來管理協力廠商更新安裝非常有效。若要安裝多個協力廠商更新，請使用可在*安裝所需的更新和修復漏洞*工作中配置的規則。建議您僅為那些不符合規則中指定條件的特定更新設定*已批准*狀態。當您手動批准大量更新時，管理伺服器的效能下降，這可能導致伺服器過載。

要批准或拒絕一個或幾個更新：

1. 在主控台樹狀目錄中，選取**進階 → 應用程式管理 → 軟體更新**節點。
2. 在**軟體更新**資料夾的工作區，點擊右上角的**重新整理**按鈕。更新清單顯示。
3. 選取您要批准或拒絕的更新。
   所選物件的資訊框出現在工作區的右側。
4. 在**更新批准狀態**下拉清單，選取**已批准**以批准所選更新或**已拒絕**以拒絕所選更新。
   預設值是**未定義**。

您設定了**已批准**狀態的更新會放置在安裝佇列。

您設定了**已拒絕**狀態的更新會從先前將其安裝的裝置上移除（如果可能）。而且，它們將來也不會被安裝到其他裝置。

Kaspersky 應用程式的一些更是無法被移除。如果您為其設定了**已拒絕**狀態，卡巴斯基安全管理中心將不會從先前將其安裝的裝置上移除這些更新。然而，這些更新將來也不會被安裝到其他裝置。如果 Kaspersky 應用程式更新無法被移除，該內容顯示在更新內容視窗，在 **區域**視窗選取**一般**，在工作區中，內容將出現在**安裝需求**下方。如果您為協力廠商軟體更新設定了**已拒絕**狀態，則已計畫但未安裝這些更新的裝置將不會安裝這些更新。更新將保持在已將其安裝的裝置上。如果您必須刪除它們，您可以在本機手動刪除它們。

使用管理伺服器從 Windows 更新同步更新

若您已在快速啟動精靈的**更新管理設定**視窗選取**使用管理伺服器作為 WSUS 伺服器**，則會自動建立 Windows Update 同步工作。您可以執行**工作**資料夾中的工作。Microsoft 軟體更新功能必須在**執行 Windows Update 同步**同步工作完成後才能開始作業。

Microsoft 軟件更新可能超過 10 GB。確保管理伺服器資料庫能夠容納此類容量；否則，**執行 Windows Update 同步**工作將失敗。**執行 Windows Update 同步**工作不支援 Microsoft SQL Express 資料庫。

執行 Windows Update 同步作業僅會從 Microsoft 伺服器下載中繼資料。如果網路不使用 WSUS 伺服器，例如每個用戶端裝置都從外部伺服器獨立下載 Microsoft 更新。

若要建立使用管理伺服器同步 Windows 更新，請執行以下操作：

1. 在主控台樹狀目錄的**進階 → 應用程式管理**資料夾中，選取**軟體更新**子資料夾。
2. 點擊**附加操作**按鈕並在下拉清單選取 **配置 Windows Update 同步**。
   精靈建立的**執行 Windows Update 同步**工作會顯示在**工作**資料夾。
   Windows Update Center 資料擷取工作建立精靈啟動。遵照精靈的說明。

您還可以透過在**工作**資料夾中點擊**建立工作**來建立 Windows Update 同步工作。

Microsoft 定期從公司伺服器刪除過期更新，以便目前更新數量總是介於 200,000 和 300,000 之間。為了減少磁碟空間使用和資料庫大小，卡巴斯基安全管理中心會刪除不再顯示於 Microsoft 更新伺服器上的過期更新。

執行**執行 Windows Update 同步**工作時，應用程式會從 Microsoft 更新伺服器收到目前更新清單。下一步，卡巴斯基安全管理中心編輯過期更新清單。在下次啟動**弱點掃描和所需更新**工作時，卡巴斯基安全管理中心會篩選所有過期更新並為其設定刪除時間。在下次啟動**執行 Windows Update 同步**工作時，所有 30 天前篩選出的過期更新都會被刪除。卡巴斯基安全管理中心也檢查刪除了 180 天以上的過期更新，並刪除更早的更新。

當**執行 Windows Update 同步**工作完成且過期更新被刪除時，資料庫可能仍會在 %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles 檔案中保留刪除的更新的雜湊碼和對應檔案（如果已早期下載這些項目）。您可以執行**管理伺服器維護**工作以從資料庫和對應檔案中刪除這些過期的記錄。

步驟 1：定義是否減少流量

在卡巴斯基安全管理中心與 Microsoft Windows Update Servers 同步更新時，所有檔案的資訊被儲存在管理伺服器資料庫。所有更新所需的檔案也在與 Windows 更新代理的互動過程中被下載到磁碟機。特別地，卡巴斯基安全管理中心儲存快速更新檔案的資訊到資料庫並在必要時下載它們。下載快速更新檔案導致磁碟機空間的減少。

為了避免磁碟空間減少以及流量降低，請取消選取所有**下載快速安裝檔案**的核取方塊。

若已選取此選項，快速更新檔案會在執行工作時下載。預設情況下未選定此選項。

步驟 2：應用程式

在該區域中，您可以選取為哪些應用程式下載更新。

如果清空**所有應用程式**核取方塊，更新將為所有現有應用程式以及可能在將來發佈的應用程式下載。

預設情況下已選取此**所有應用程式**核取方塊。

步驟 3：更新類別

在該區域中，您可以選取將哪些類別的更新下載到管理伺服器。

如果選取**所有類別**核取方塊，更新將為所有現有更新類別以及可能在將來出現的類別下載。

預設情況下已選取此**所有類別**核取方塊。

步驟 4：更新語言

在該視窗中，您可以定義將哪些語言的更新下載到管理伺服器。選取以下選項之一以下載更新的中文化語言：

- **下載包含新語言在內的所有語言**

  如果選定了該方塊，所有可用的更新中文化語言都將被下載至管理伺服器。預設情況下已選定此選項。

- **下載選取語言**

  如果選定了該方塊，您可以從更新的中文化語言清單中進行選取以便下載到管理伺服器中。

步驟 5：選取帳戶以移動工作

在**選取要執行此工作的帳戶**視窗，您可以指定在執行工作時使用哪些帳戶。您可以選取以下其中一個方法：

- **預設帳戶**

  在與執行該工作的應用程式相同的帳戶下執行該工作。
  預設情況下已選定此選項。

- **指定帳戶**

  填寫**帳戶**與**密碼**欄位以指定工作要在其下執行的帳戶詳情。帳戶必須對此工作有足夠的權限。

  - **帳戶**

    執行該工作的帳戶。

  - **密碼**

    工作執行時使用的帳戶的密碼。

步驟 6：設定工作啟動排程

在**設定工作排程**精靈頁面，您可以為工作啟動建立排程。如果必要，指定以下設定：

- **排程開始：**

  選取工作執行排程並設定所選排程。

  - **每 N 小時**

    工作定期執行，按照指定小時數間隔，從指定的日期和時間開始。

    預設下，工作每 6 小時執行一次，從目前系統日期和時間開始。

  - **每 N 天**

    工作定期執行，按照指定天數間隔。此外，您可指定第一個工作執行的日期與時間。這些額外選項會在您建立的工作受到應用程式支援時可用。

    預設下，工作每天執行一次，從目前系統日期和時間開始。

  - **每 N 星期**

    工作定期執行，按照指定星期數間隔，從指定的星期和時間開始。

    預設下，工作每星期一於目前系統時間執行一次。

  - **每 N 分鐘**

    工作定期執行，按照指定分鐘數間隔，從工作建立日期的指定時間開始。

    預設下，工作每 30 分鐘執行一次，從目前系統時間開始。

  - **每天（不支援日光節約時間）**

    工作定期執行，按照指定天數間隔。排程不支援日光節約時間 (DST)。這意味著在夏令時開始和結束時當時鐘向前或向後撥動一小時時，實際工作啟動時間不變更。

    我們不建議您使用該排程。它用於向後相容卡巴斯基安全管理中心。

    預設下，工作每天於目前系統時間執行一次。

  - **每週**

    工作每週在指定星期和指定時間執行。

  - **按每星期中的指定日**

    工作定期執行，在每周指定日期的指定時間。

    預設下，工作每週五 6:00:00 P.M. 執行。

- **每月**

  工作定期執行，在指定月日的指定時間。
  在缺少指定日的月份，工作在最後一天執行。
  預設下，工作在每月的第一天執行，在目前系統時間。

- **手動**

  工作不自動執行。您僅可以手動啟動。

  預設情況下已選定此選項。

- **一次**

  此工作在指定的日期和時間（預設情況下，在建立工作的當天）執行一次。

- **每個月在所選週的指定天**

  工作定期在指定月日的指定時間執行。
  預設情況下，不選取一個月中的任何一天。預設開始時間為 18:00。

- **在偵測到病毒爆發時**

  工作在發生*病毒爆發*事件後執行。選取將監控病毒爆發的應用程式類型。有下列應用程式類型可用：
  - 病毒防護工作站和檔案伺服器
  - 用於週邊防護的防毒軟體
  - 用於郵件伺服器的防毒軟體

  預設情況下選定所有應用程式類型。
  您可能想根據報告病毒爆發的安全應用程式類型執行不同的工作。此種情況下，刪除您不需要的應用程式類型選項。

- **在完成其它工作時**

  目前工作在其他工作完成後啟動。您可以選取先前工作如何結束（成功或帶有錯誤）以觸發目前工作的啟動。例如，您可能想使用***Turn on the device***選項執行開啟裝置工作，完成後，請執行*惡意軟體掃描*工作。只有當這兩項工作都被分配給相同的裝置時，此參數才會有作用。

- **執行錯過的工作**

該選項決定在工作要啟動時用戶端裝置在網路中不可見時工作的行為。

如果啟用該選項，系統將在下一次在用戶端裝置上執行 Kaspersky 應用程式時嘗試啟動工作。如果工作排程是**手動**、**一次**或**立即**，裝置在網路中可見或包含在工作範圍後，工作會立即啟動。

如果停用此選項，則僅限排程的工作會在用戶端裝置上執行。若為**手動**、**一次**與**立即**排程，工作僅會在網路上顯示的用戶端裝置上執行。例如，您可能想為消耗資源的工作停用該選項，您僅想在業餘時間執行該工作。

預設情況下已停用該選項。

- **使用工作啟動自動隨機延遲**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動，即是，*分佈式工作啟動*。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  當工作被建立時，根據工作中包含用戶端裝置的數量，分發啟動時間被自動計算。然後，工作總是在計算的開始時間啟動。然後當工作設定被編輯或者工作被手動啟動時，計算的工作啟動時間值被變更。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

- **使用工作啟動隨機延遲間隔（分鐘）**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

  預設情況下已停用該選項。預設時間間隔為一分鐘。

步驟 7：定義工作名稱

在**定義工作名稱**視窗，指定您正在建立的規則名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元（ **"*<>?\:|** ）。預設值為*執行 Windows Update 同步*。

步驟 8：完成工作建立

在**完成工作建立**視窗，點擊**完成**按鈕以完成精靈。

如果您想讓工作在精靈完成時立即啟動，選取**精靈完成時執行工作**核取方塊。

新建立的 Windows 更新同步工作將顯示在主控台樹狀目錄中**工作**資料夾的工作清單。

手動在裝置上安裝更新

若您已在快速設定精靈的**更新管理設定**頁面選取**尋找與安裝需要的更新**，則會自動建立*安裝必要的更新與修正弱點*工作。您可在**工作**頁籤的**受管理裝置**資料夾執行或停止工作。

如果您已經在快速啟動精靈中選取**搜尋必要更新**，則可以透過*安裝必要更新並修復弱點*工作將軟體更新安裝至用戶端裝置。

您可以做以下任意：

- 建立更新安裝工作。
- 新增安裝更新到現有更新安裝工作的規則。
- 在現有更新安裝工作的設定中，配置更新的測試安裝。

在受管理裝置上更新協力廠商應用程式或修復協力廠商應用程式中的弱點時，可能需要使用者互動。例如，若協力廠商應用程式目前開啟，可能會提示使用者關閉協力廠商應用程式。

透過建立安裝工作安裝更新

您可以做以下任意：

- 建立特定更新安裝工作。
- 選取更新並建立它和相似更新的安裝工作。

要安裝特定更新：

1. 在主控台樹狀目錄的**進階 → 應用程式管理**資料夾中，選取**軟體更新**子資料夾。
2. 在工作區，選取您要安裝的更新。
3. 做以下任意：
   - 右擊清單中一個選擇的更新，然後選取**安裝更新 → 新工作**。
   - 在所選更新的資訊框中，點擊**安裝更新（建立工作）**連結。
4. 在顯示的提示中做出安裝所有先前應用程式更新的選取。如果您同意在安裝所選更新需要時安裝連續的應用程式版本，按一下**是**。如果您要直接更新應用程式而不安裝連續版本，按一下**否**。如果安裝所選更新不能不安裝先前版本的應用程式，應用程式更新失敗。

   更新安裝和弱點修復工作建立精靈啟動。遵照精靈的說明。

5. 在精靈的**選取作業系統重新啟動選項**頁面上，選取用戶端裝置的作業系統在操作後必須被重新啟動時的操作：

- **不重新啟動裝置**

  用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

- **重新啟動裝置**

  如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

- **提示使用者操作**

  用戶端裝置螢幕上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。該選項適用於使用者必須可以選取最方便的時間進行重新啟動的工作站。

  預設情況下已選定此選項。

  - **重複提示間隔（分鐘）**

    如果啟用該選項，應用程式以指定頻率提示使用者重新啟動作業系統。

    預設情況下已啟用該選項。預設間隔是 5 分鐘。可用值介於 1 和 1440 分鐘之間。

    如果停用該選項，提示僅顯示一次。

  - **在該時間後重新啟動（分鐘）**

    提示使用者之後，應用程式在指定時間間隔後強制作業系統重新啟動。

    預設情況下已啟用該選項。預設延時是 30 分鐘。可用值介於 1 和 1440 分鐘之間。

- **強制關閉已鎖定連線的應用程式**

  執行應用程式可能會阻止用戶端裝置重新啟動。例如，如果文件在文書處理應用程式中編輯且未儲存，應用程式不會允許裝置重新啟動。

  如果啟用該選項，鎖定裝置上的此類應用程式在裝置重新啟動前被強制關閉。結果，使用者可能遺失他們未儲存的變更。

  如果停用該選項，鎖定裝置不被重新啟動。此裝置上的工作狀態表示裝置需要重新啟動。使用者必須手動關閉所有執行在鎖定裝置上的應用程式並重新啟動這些裝置。

  預設情況下已停用該選項。

6. 在**設定工作排程**精靈頁面，您可以為啟動工作建立排程。如果必要，指定以下設定：

- **排程開始：**

  選取工作執行排程並設定所選排程。

  - **每 N 小時**

    工作定期執行，按照指定小時數間隔，從指定的日期和時間開始。

    預設下，工作每 6 小時執行一次，從目前系統日期和時間開始。

  - **每 N 天**

    工作定期執行，按照指定天數間隔。此外，您可指定第一個工作執行的日期與時間。這些額外選項會在您建立的工作受到應用程式支援時可用。

    預設下，工作每天執行一次，從目前系統日期和時間開始。

  - **每 N 星期**

    工作定期執行，按照指定星期數間隔，從指定的星期和時間開始。

    預設下，工作每星期一於目前系統時間執行一次。

  - **每 N 分鐘**

    工作定期執行，按照指定分鐘數間隔，從工作建立日期的指定時間開始。

    預設下，工作每 30 分鐘執行一次，從目前系統時間開始。

  - **每天（不支援日光節約時間）**

    工作定期執行，按照指定天數間隔。排程不支援日光節約時間 (DST)。這意味著在夏令時開始和結束時當時鐘向前或向後撥動一小時時，實際工作啟動時間不變更。

    我們不建議您使用該排程。它用於向後相容卡巴斯基安全管理中心。

    預設下，工作每天於目前系統時間執行一次。

  - **每週**

    工作每週在指定星期和指定時間執行。

  - **按每星期中的指定日**

    工作定期執行，在每周指定日期的指定時間。

    預設下，工作每週五 6:00:00 P.M. 執行。

  - **每月**

工作定期執行，在指定月日的指定時間。

在缺少指定日的月份，工作在最後一天執行。

預設下，工作在每月的第一天執行，在目前系統時間。

- **手動**

  工作不自動執行。您僅可以手動啟動。

  預設情況下已選定此選項。

- **每個月在所選週的指定天**

  工作定期在指定月日的指定時間執行。

  預設情況下，不選取一個月中的任何一天。預設開始時間為 18:00。

- **在偵測到病毒爆發時**

  工作在發生*病毒爆發*事件後執行。選取將監控病毒爆發的應用程式類型。有下列應用程式類型可用：

  - 病毒防護工作站和檔案伺服器
  - 用於週邊防護的防毒軟體
  - 用於郵件伺服器的防毒軟體

  預設情況下選定所有應用程式類型。

  您可能想根據報告病毒爆發的安全應用程式類型執行不同的工作。此種情況下，刪除您不需要的應用程式類型選項。

- **在完成其它工作時**

  目前工作在其他工作完成後啟動。您可以選取先前工作如何結束（成功或帶有錯誤）以觸發目前工作的啟動。例如，您可能想使用***Turn on the device***選項執行開啟裝置工作，完成後，請執行*惡意軟體掃描*工作。只有當這兩項工作都被分配給相同的裝置時，此參數才會有作用。

- **執行錯過的工作**

  該選項決定在工作要啟動時用戶端裝置在網路中不可見時工作的行為。

  如果啟用該選項，系統將在下一次在用戶端裝置上執行 Kaspersky 應用程式時嘗試啟動工作。如果工作排程是**手動**、**一次**或**立即**，裝置在網路中可見或包含在工作範圍後，工作會立即啟動。

  如果停用此選項，則僅限排程的工作會在用戶端裝置上執行。若為**手動**、**一次**與**立即**排程，工作僅會在網路上顯示的用戶端裝置上執行。例如，您可能想為消耗資源的工作停用該選項，您僅想在業餘時間執行該工作。

  預設情況下已停用該選項。

- **使用工作啟動自動隨機延遲**

如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動，即是，*分佈式工作啟動*。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

當工作被建立時，根據工作中包含用戶端裝置的數量，分發啟動時間被自動計算。然後，工作總是在計算的開始時間啟動。然後當工作設定被編輯或者工作被手動啟動時，計算的工作啟動時間值被變更。

如果該選項被停用，工作依據排程在用戶端裝置上啟動。

- **使用工作啟動隨機延遲間隔（分鐘）**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

  預設情況下已停用該選項。預設時間間隔為一分鐘。

7. 在**定義工作名稱**精靈頁面，指定您正在建立的工作名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。

8. 在精靈的**完成工作建立**頁面，點擊**完成**按鈕關閉精靈。

   如果您想讓工作在精靈完成時立即啟動，選取**精靈完成時執行工作**核取方塊。

精靈完成操作後，**安裝所需更新並修復弱點**將顯示在**工作**資料夾中。

您可以在「*安裝所需更新並修復弱點*」工作內容中啟用在安裝更新前先自動安裝系統元件（先決條件）。若啟用此選項，所有必需的系統元件都會在安裝更新前為您進行更新。可在元件的內容清單中檢視到相關的更新項目。

在「*安裝所需更新並修復弱點*」工作內容中，您可以允許安裝能夠將程式更新至新版本的更新。

如果工作設定提供了安裝協力廠商更新的規則，管理伺服器從供應商網站下載所有相關更新。更新儲存到管理伺服器儲存區，然後分發並安裝在可套用的裝置。

如果工作設定提供了安裝 Microsoft 更新的規則並且管理伺服器作為 WSUS 伺服器，管理伺服器下載所有更新到儲存區並發佈它們到受管理裝置。如果網路不使用 WSUS 伺服器，例如每個用戶端裝置都從外部伺服器獨立下載 Microsoft 更新。

要安裝特定和相似更新：

1. 在主控台樹狀目錄的**進階 → 應用程式管理**資料夾中，選取**軟體更新**子資料夾。

2. 在工作區中，選取您要安裝的更新。

3. 點擊**執行更新安裝精靈**按鈕。

   更新安裝精靈開始。

   更新安裝精靈功能僅在弱點和修補程式管理產品授權下可用。

   遵照精靈的說明。

4. 在**搜尋現有的更新安裝工作**頁面上，指定以下設定：

- **搜尋安裝該更新的工作**

  如果啟用該選項，更新安裝精靈搜尋安裝所選更新的現有工作。

  如果停用該選項或搜尋未擷取到可應用工作，更新安裝精靈提示您為安裝更新建立規則或工作。

  預設情況下已啟用該選項。

- **批准更新安裝**

  所選更新將被批准安裝。如果一些應用的更新安裝規則僅允許安裝批准的更新，啟用該選項。

  預設情況下已停用該選項。

5. 如果您選取搜尋現有更新安裝工作或搜尋擷取到一些工作，您可以檢視這些工作的內容或手動啟動它們。不需要進一步操作。

   或者，請點擊**新的更新安裝工作**按鈕。

6. 選取安裝規則類型以新增到新工作，然後按一下**結束**按鈕。

7. 在顯示的提示中做出安裝所有先前應用程式更新的選取。如果您同意在安裝所選更新需要時安裝連續的應用程式版本，按一下**是**。如果您要直接更新應用程式而不安裝連續版本，按一下**否**。如果安裝所選更新不能不安裝先前版本的應用程式，應用程式更新失敗。

   更新安裝和弱點修復工作建立精靈啟動。遵照精靈的說明。

8. 在精靈的**選取作業系統重新啟動選項**頁面上，選取用戶端裝置的作業系統在操作後必須被重新啟動時的操作：

- **不重新啟動裝置**

  用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

- **重新啟動裝置**

  如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

- **提示使用者操作**

  用戶端裝置螢幕上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。該選項適用於使用者必須可以選取最方便的時間進行重新啟動的工作站。

  預設情況下已選定此選項。

  - **重複提示間隔（分鐘）**

    如果啟用該選項，應用程式以指定頻率提示使用者重新啟動作業系統。

    預設情況下已啟用該選項。預設間隔是 5 分鐘。可用值介於 1 和 1440 分鐘之間。

    如果停用該選項，提示僅顯示一次。

  - **在該時間後重新啟動（分鐘）**

    提示使用者之後，應用程式在指定時間間隔後強制作業系統重新啟動。

    預設情況下已啟用該選項。預設延時是 30 分鐘。可用值介於 1 和 1440 分鐘之間。

- **強制關閉已鎖定連線的應用程式**

  執行應用程式可能會阻止用戶端裝置重新啟動。例如，如果文件在文書處理應用程式中編輯且未儲存，應用程式不會允許裝置重新啟動。

  如果啟用該選項，鎖定裝置上的此類應用程式在裝置重新啟動前被強制關閉。結果，使用者可能遺失他們未儲存的變更。

  如果停用該選項，鎖定裝置不被重新啟動。此裝置上的工作狀態表示裝置需要重新啟動。使用者必須手動關閉所有執行在鎖定裝置上的應用程式並重新啟動這些裝置。

  預設情況下已停用該選項。

9. 在精靈的**選取要對其分配工作的裝置**頁面上，選取以下其中一個選項：

- **選取管理伺服器偵測到的網路裝置**

  工作被分配到指定裝置。特定裝置可以包含管理群組的裝置和未配置的裝置。

  例如，您可能要在安裝網路代理到未配置的裝置的工作中使用該選項。

- **手動指定裝置位址或從清單匯入位址**

  您可以指定您要為其分配工作的裝置的 NetBIOS 名稱、DNS 名稱、IP 位址和 IP 子網路。

  您可能要使用該選項以對特定子網路執行工作。例如，您可能要安裝特定應用程式到會計裝置，或者掃描疑似被感染子網路中的裝置。

- **分配工作到裝置分類**

  該工作被分配到裝置選項中的裝置。您可以指定其中一個現有選項。

  例如，您可能要使用該選項在特定作業系統版本的裝置上執行工作。

- **分配工作到管理群組**

  工作被分配到包含在管理群組中的裝置。您可以指定其中一個現有群組或者建立新群組。

  例如，您可能要使用該選項執行傳送訊息到使用者工作，如果訊息針對包含在特定管理群組中的裝置。

  如果工作被指派給管理群組，則工作屬性視窗中不會顯示**安全**標籤，因為群組工作受其所套用的群組的安全設定的約束。

10. 在**設定工作排程**精靈頁面，您可以為啟動工作建立排程。如果必要，指定以下設定：

- **排程開始：**

  選取工作執行排程並設定所選排程。

  - **每 N 小時**

    工作定期執行，按照指定小時數間隔，從指定的日期和時間開始。

    預設下，工作每 6 小時執行一次，從目前系統日期和時間開始。

  - **每 N 天**

    工作定期執行，按照指定天數間隔。此外，您可指定第一個工作執行的日期與時間。這些額外選項會在您建立的工作受到應用程式支援時可用。

    預設下，工作每天執行一次，從目前系統日期和時間開始。

  - **每 N 星期**

    工作定期執行，按照指定星期數間隔，從指定的星期和時間開始。

    預設下，工作每星期一於目前系統時間執行一次。

  - **每 N 分鐘**

    工作定期執行，按照指定分鐘數間隔，從工作建立日期的指定時間開始。

    預設下，工作每 30 分鐘執行一次，從目前系統時間開始。

  - **每天（不支援日光節約時間）**

    工作定期執行，按照指定天數間隔。排程不支援日光節約時間 (DST)。這意味著在夏令時開始和結束時當時鐘向前或向後撥動一小時時，實際工作啟動時間不變更。

    我們不建議您使用該排程。它用於向後相容卡巴斯基安全管理中心。

    預設下，工作每天於目前系統時間執行一次。

  - **每週**

    工作每週在指定星期和指定時間執行。

  - **按每星期中的指定日**

    工作定期執行，在每周指定日期的指定時間。

    預設下，工作每週五 6:00:00 P.M. 執行。

  - **每月**

工作定期執行，在指定月日的指定時間。

在缺少指定日的月份，工作在最後一天執行。

預設下，工作在每月的第一天執行，在目前系統時間。

- **手動**（預設選取）

  工作不自動執行。您僅可以手動啟動。

  預設情況下已選定此選項。

- **每個月在所選週的指定天**

  工作定期在指定月日的指定時間執行。

  預設情況下，不選取一個月中的任何一天。預設開始時間為 18:00。

- **在偵測到病毒爆發時**

  工作在發生*病毒爆發*事件後執行。選取將監控病毒爆發的應用程式類型。有下列應用程式類型可用：

  - 病毒防護工作站和檔案伺服器
  - 用於週邊防護的防毒軟體
  - 用於郵件伺服器的防毒軟體

  預設情況下選定所有應用程式類型。

  您可能想根據報告病毒爆發的安全應用程式類型執行不同的工作。此種情況下，刪除您不需要的應用程式類型選項。

- **在完成其它工作時**

  目前工作在其他工作完成後啟動。您可以選取先前工作如何結束（成功或帶有錯誤）以觸發目前工作的啟動。例如，您可能想使用***Turn on the device***選項執行開啟裝置工作，完成後，請執行*惡意軟體掃描*工作。只有當這兩項工作都被分配給相同的裝置時，此參數才會有作用。

- **執行錯過的工作**

  該選項決定在工作要啟動時用戶端裝置在網路中不可見時工作的行為。

  如果啟用該選項，系統將在下一次在用戶端裝置上執行 Kaspersky 應用程式時嘗試啟動工作。如果工作排程是**手動**、**一次**或**立即**，裝置在網路中可見或包含在工作範圍後，工作會立即啟動。

  如果停用此選項，則僅限排程的工作會在用戶端裝置上執行。若為**手動**、**一次**與**立即**排程，工作僅會在網路上顯示的用戶端裝置上執行。例如，您可能想為消耗資源的工作停用該選項，您僅想在業餘時間執行該工作。

  預設情況下已停用該選項。

- **使用工作啟動隨機延遲間隔（分鐘）**

如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動，即是，*分佈式工作啟動*。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

當工作被建立時，根據工作中包含用戶端裝置的數量，分發啟動時間被自動計算。然後，工作總是在計算的開始時間啟動。然後當工作設定被編輯或者工作被手動啟動時，計算的工作啟動時間值被變更。

如果該選項被停用，工作依據排程在用戶端裝置上啟動。

- **使用工作啟動隨機延遲間隔（分鐘）**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

  預設情況下已停用該選項。預設時間間隔為一分鐘。

11. 在**定義工作名稱**精靈頁面，指定您正在建立的工作名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。
12. 在精靈的**完成工作建立**頁面，點擊**完成**按鈕關閉精靈。

    如果您想讓工作在精靈完成時立即啟動，選取**精靈完成時執行工作**核取方塊。

    當精靈結束後，系統將建立**安裝所需更新並修復弱點**工作，並顯示在**工作**資料夾中。

    除了您在工作建立過程中指定的設定，您還可以變更所建立工作的其他屬性。

升級到新版本的應用程式，可能會導致相關的應用程式在裝置上發生錯誤。

透過新增規則到現有安裝工作來安裝更新

要透過新增規則到現有安裝工作來安裝更新：

1. 在主控台樹狀目錄的**進階 → 應用程式管理**資料夾中，選取**軟體更新**子資料夾。
2. 在工作區中，選取您要安裝的更新。
3. 點擊**執行更新安裝精靈**按鈕。

   更新安裝精靈開始。

   更新安裝精靈功能僅在弱點和修補程式管理產品授權下可用。

   遵照精靈的說明。

4. 在**搜尋現有的更新安裝工作**頁面上，指定以下設定：

   - **搜尋安裝該更新的工作**

     如果啟用該選項，更新安裝精靈搜尋安裝所選更新的現有工作。

     如果停用該選項或搜尋未擷取到可應用工作，更新安裝精靈提示您為安裝更新建立規則或工作。

     預設情況下已啟用該選項。

   - **批准更新安裝**

     所選更新將被批准安裝。如果一些應用的更新安裝規則僅允許安裝批准的更新，啟用該選項。

     預設情況下已停用該選項。

5. 如果您選取搜尋現有更新安裝工作或搜尋擷取到一些工作，您可以檢視這些工作的內容或手動啟動它們。不需要進一步操作。

   或者，請點擊**新增更新安裝規則**按鈕。

6. 選取您要新增規則的工作，然後點擊**新增規則**按鈕。

   而且，你您可以檢視現有工作的屬性，手動啟動它們，或者建立新工作。

7. 選取規則類型以新增到所選工作，然後按一下**結束**按鈕。

8. 在顯示的提示中做出安裝所有先前應用程式更新的選取。如果您同意在安裝所選更新需要時安裝連續的應用程式版本，按一下**是**。如果您要直接更新應用程式而不安裝連續版本，按一下**否**。如果安裝所選更新不能不安裝先前版本的應用程式，應用程式更新失敗。

更新安裝新規則被新增到現有**安裝所需更新並修復弱點**工作。

配置更新的測試安裝

若要設定更新的測試安裝，請執行以下操作：

1. 在主控台樹狀目錄中，在**工作**頁籤的**受管理裝置**資料夾選取**安裝必要更新並修正弱點** 工作。

2. 從工作的上下文功能表中，選取**內容**。

   安裝所需更新並修復弱點工作的內容視窗將開啟。

3. 在該工作的內容視窗中的**測試安裝**區域中，選取其中一個可用選項：

   - **不掃描**。如果您不希望執行更新的測試安裝，請選取該選項。
   - **在選定裝置上執行掃描**。如果要在指定裝置上測試更新安裝，請選取此選項。點擊**新增**按鈕，然後選取您需要執行測試更新安裝的裝置。
   - **在指定群組中的裝置上執行掃描**。如果要在一組電腦上測試更新安裝，請選取此選項。在**指定測試群組**欄位中，指定您要在其上執行測試更新安裝的一組裝置。
   - **在指定百分比的裝置上執行掃描**。如果要在一部分裝置上測試更新安裝，請選取此選項。在**所有目標裝置中測試裝置的百分比**欄位中，指定您要在其上執行更新測試安裝的裝置比例。

4. 選取除**不掃描**以外的任意選項，在**決定是否繼續進行安裝的所需時間（小時）**欄位中指定從更新安裝測試到開始將更新安裝到所有裝置上必須間隔的小時數。

在網路代理政策中設定 Windows 更新

若要在網路代理政策中設定 Windows 更新，請執行以下操作：

1. 在主控台樹狀目錄中，選取**受管理裝置**。
2. 在工作區中，選取**政策**頁籤。
3. 選取網路代理政策。
4. 在政策的上下文功能表中，選取**內容**。

   網路代理政策的內容視窗隨即開啟。
5. 在**區域**視窗中，選取**軟體更新和弱點**。
6. 選取**使用管理伺服器作為 WSUS 伺服器**核取方塊以將 Windows 更新下載到管理伺服器，並透過網路代理發佈在用戶端裝置上。

   如果未選擇此選項，Windows 更新不會被下載到管理伺服器。此種情況下，用戶端裝置直接從 Microsoft 伺服器接收 Windows 更新。

7. 選取使用者可以透過使用 Windows Update 手動安裝到裝置的更新集。

在執行 Windows 10 的裝置上，如果 Windows Update 已為裝置找到更新，您在**允許使用者管理 Windows Update 更新安裝**下選取的新選項將僅在發現的更新被安裝後才被套用。

在下拉清單中選取項目：

- **允許使用者安裝所有可套用 Windows Update 更新**

  使用者可以安裝所有可套用到他們裝置的 Microsoft Windows Update 更新。

  如果您不希望干預更新安裝，請選取該選項。

  當使用者手動安裝 Microsoft Windows Update 更新時，更新可能從 Microsoft 伺服器下載，而不是從管理伺服器。如果管理伺服器還未下載這些更新，這是可能的。從 Microsoft 伺服器下載更新導致額外流量。

- **僅允許使用者安裝批准的 Windows Update 更新**

  使用者可以安裝所有可應用到他們裝置的和您批准的 Microsoft Windows Update 更新。

  例如，您可能想先在測試環境中檢查更新安裝以確保它們不干預裝置操作，僅在這之後允許安裝這些批准的更新到用戶端裝置。

  當使用者手動安裝 Microsoft Windows Update 更新時，更新可能從 Microsoft 伺服器下載，而不是從管理伺服器。如果管理伺服器還未下載這些更新，這是可能的。從 Microsoft 伺服器下載更新導致額外流量。

- **不允許使用者安裝 Windows Update 更新**

  使用者無法在他們的裝置上手動安裝 Microsoft Windows Update 更新。所有可套用更新根據您的設定而安裝。

  如果您想要集中管理更新的安裝則選則此選項。

  例如，您可以想最佳化更新排程以便網路不超載。您可以計畫稍後更新，以便它們不干預使用者工作。

8. 選取 Windows 更新搜尋模式：

- **主動**

  如果選中該選項，管理伺服器支援使用網路代理在用戶端裝置上從 Windows 更新代理傳送請求至更新來源：Windows 更新伺服器（或簡稱為 WSUS）。然後，網路代理會將從 Windows 更新代理接收到的資訊傳送給管理伺服器。

  只有選取*弱點掃描和所需更新*工作的**連線更新伺服器更新資料**選項時，此選項才會發揮效力。

  預設情況下已選定此選項。

- **被動**

  如果您選定該選項，網路代理將從上次同步更新來源之後定期從 Windows 更新代理將所擷取更新的資訊傳遞給管理伺服器。如果 Windows 更新代理沒有執行與更新來源同步，在管理伺服器上的更新資訊就不再是最新的。

  若要從更新來源的記憶體快取獲得更新，請選取此選項。

- **已停用**

  如果選中該選項，管理伺服器不會請求任何有關更新的資訊。

  若您要在本機裝置先測試更新，請選取此選項。

9. 若要掃描執行可執行檔時是否存在弱點，請選取**當執行可執行檔時掃描其弱點**選項。

10. 確保為您更改的所有設定鎖定編輯。否則，更改不適用。

11. 點擊"**套用**"。

修復協力廠商軟體弱點

本節說明卡巴斯基安全管理中心如何修復受管理裝置上已安裝軟體的弱點。

情境：尋找與修復協力廠商軟體弱點

本節說明在執行 Windows 的受管理裝置上尋找與修復弱點的情境。您可在作業系統與協力廠商軟體（包含 Microsoft 軟體）中尋找並修復軟體弱點。

先決條件

- 系統會將卡巴斯基安全管理中心佈署在您的組織中。
- 您組織中有執行 Windows 的受管理裝置。
- 管理伺服器需要網際網路連線才能執行以下工作：
  - 列出針對 Microsoft 軟體弱點的建議修補程式。該清單由卡巴斯基專家建立並定期更新。
  - 修復 Microsoft 軟體以外的協力廠商軟體中的漏洞。

階段

分階段尋找並修復軟體弱點：

1. **受管理裝置中已安裝軟體的掃描弱點**

   若要在受管理裝置已安裝軟體中尋找弱點，請執行*弱點掃描和所需更新*工作。完成此工作時，卡巴斯基安全管理中心會收到偵測到的弱點清單，以及安裝於您在工作內容指定裝置上已安裝軟體需要的更新。

   *弱點掃描和所需更新*工作會由卡巴斯基安全管理中心快速啟動精靈自動建立。如果您未執行精靈，請立即將其啟動或手動建立工作。

   說明：

   - 管理主控台：掃描應用程式是否有弱點，排程尋找弱點和所需更新的工作
   - 卡巴斯基安全管理中心網頁主控台：建立弱點掃描和所需更新工作、尋找弱點和所需更新的工作設定

2. **分析偵測到的軟體弱點清單**

   檢視**軟體弱點**清單並決定要修復的弱點。若要檢視各弱點的詳細資訊，請按一下清單中的弱點名稱。對於清單中的各個，您也可檢視受管理裝置上弱點的統計資料。

   說明：

   - 管理主控台：檢視關於軟體弱點的資訊、檢視受管理裝置上弱點的統計資料
   - 卡巴斯基安全管理中心網頁主控台：檢視關於軟體弱點的資訊、檢視受管理裝置上弱點的統計資料

3. **設定弱點修復**

   偵測到軟體弱點時，您可使用*安裝所需更新並修復弱點*工作或*修復弱點*工作修復受管理裝置上的軟體弱點。

   *安裝所需更新並修復弱點*工作會用來更新與修復協力廠商軟體中的弱點，包含安裝在受管理裝置上的 Microsoft 軟體。此工作可讓您根據特定規則安裝多項更新並修復多個弱點。請注意，只有當您有弱點和修補程式管理功能的授權時，才可建立此工作。為了修復軟體弱點，*安裝所需更新並修復弱點*工作會使用建議的軟體更新。

   *修復弱點*工作不需要弱點與修補程式管理功能的授權選項。若要使用此工作，您必須為列於工作設定中協力廠商軟體清單的弱點指定軟體使用者修復項目。*修復弱點*工作會使用適用於 Microsoft 軟體的建議修復項目，以及適用於協力廠商軟體的使用者修復項目。

   您可啟動弱點修復精靈，精靈會自動建立以下其中一種這類工作或您可手動建立其中一種這類工作。

   說明：

   - 管理主控台：選取適用於協力廠商軟體中弱點的使用者修復項目、修復應用程式中的弱點

- 卡巴斯基安全管理中心網頁主控台：選取適用於協力廠商軟體中弱點的使用者修復項目、修復協力廠商軟體中的弱點、建立安裝必要的更新並修復弱點工作

4. **排程工作**

   為確定弱點清單永遠處於最新狀態，請排程*弱點掃描和所需更新*工作以不時自動執行。建議平均頻率為每週一次。

   若您已建立*安裝所需更新並修復弱點*工作，您可排程與*弱點掃描和所需更新*工作的執行頻率相同會更少。排程*修復弱點*工作時，請注意，您必須在每次開始工作時，選擇 Microsoft 軟體的修復項目或指定協力廠商軟體的使用者修復項目。

   排程工作時，請確定修復弱點的工作會在*弱點掃描和所需更新*工作完成後啟動。

5. **忽略軟體弱點（選用）**

   如有需要，您可忽略所有受管理裝置，或僅忽略已選受管理裝置上要修復的軟體弱點。

   說明：

   - 管理主控台：忽略軟體弱點
   - 卡巴斯基安全管理中心網頁主控台：忽略軟體弱點

6. **執行修復弱點工作**

   啟動*安裝必要更新並修復弱點*工作或修復*弱點*工作。工作完成時，請確保工作清單出現*已成功完成*狀態。

7. **建立修復軟體弱點的結果報告（選用）**

   若要檢視弱點修復的詳細統計資料，請產生弱點報告。報告會顯示未修復之軟體弱點的資訊。您已知道如何在組織中尋找與修復協力廠商軟體中的弱點（包含 Microsoft 軟體）。

   說明：

   - 管理主控台：建立與檢視報告
   - 卡巴斯基安全管理中心網頁主控台：產生與檢視報告

8. **檢查尋找與修復協力廠商軟體中的弱點的配置**

   請確保您已完成以下項目：

   - 取得並檢閱受管理裝置上軟體弱點的清單
   - 忽略軟體弱點（如有需要）
   - 設定修復弱點的工作
   - 排程在之後啟動的工作以尋找並修復軟體弱點
   - 檢查修復軟體弱點工作是否執行

結果

若您已建立並設定*安裝所需更新並修復弱點*工作，弱點會自動在受管理裝置上修復。當工作執行時，會將可用軟體更新的清單與工作設定中指定的規則建立關聯。符合規則中條件的所有軟體更新都將會下載至管理伺服器儲存區，且安裝以修復軟體弱點。

若您已建立*修復弱點*工作，僅 Microsoft 軟體中的軟體弱點會被修復。

關於尋找與修復軟體弱點

卡巴斯基安全管理中心會在執行 Microsoft Windows 系列作業系統的受管理裝置上偵測並修復軟體弱點。作業系統和協力廠商軟體（包含 Microsoft 軟體）會偵測弱點。

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

尋找軟體弱點

為了尋找軟體弱點，卡巴斯基安全管理中心會使用來自已知弱點資料庫的特徵。此資料庫會由 Kaspersky 專家建立。資料庫會包含弱點的資訊，例如弱點敘述、弱點偵測日期、弱點嚴重等級。您可以在 Kaspersky 網站上搜尋軟體弱點詳情。

卡巴斯基安全管理中心會使用*弱點掃描和所需更新*工作尋找軟體弱點。

在某些情況下，可以使用下列任一方法修復 Microsoft Windows 作業系統中偵測到的弱點：

- 安裝作業系統更新。
- 將作業系統升級到較新版本（例如，從 Windows 10 升級到 Windows 11）。

在這種情況下，卡巴斯基安全管理中心顯示相同弱點的兩個項目。

修復軟體弱點

為了修復軟體弱點，卡巴斯基安全管理中心會使用由軟體供應上提供的軟體更新。執行以下工作後，系統會下載軟體更新中繼資料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*。此工作是為了 Kaspersky 與協力廠商軟體下載更新中繼資料。該工作由卡巴斯基安全管理中心快速啟動精靈自動建立。您只能手動建立將更新下載至管理伺服器儲存區工作。
- *執行 Windows Update 同步*。此工作是為了下載 Microsoft 軟體的更新中繼資料。

修復弱點的軟體更新可使用完整分發套件或修補程式代表。修復軟體弱點的軟體更新又稱為*修復項目*。*建議的修復項目*是指由 Kaspersky 專家建議安裝的項目。*使用者修復項目*是指由使用者手動指定安裝的項目。若要安裝使用者修復項目，您需建立包含此修復項目的安裝套件。

若您有具備弱點和修補程式管理功能的卡巴斯基安全管理中心授權，若要修復軟體弱點，您可使用*安裝所需更新並修復弱點*工作。此工作會安裝建議的修復項目來自動修復多個弱點。針對此工作，您可手動設定特定規則來修復多個弱點。

若您沒有具備弱點和修補程式管理功能的卡巴斯基安全管理中心授權，若要修復軟體弱點，您可使用*修復弱點*工作。透過使用此工作，您可透過安裝適用於 Microsoft 軟體的建議修復項目，以及適用於其他協力廠商軟體的使用者修復項目來修復弱點。

出於安全原因，卡巴斯基技術會自動掃描您使用弱點和修補程式管理功能安裝的任何協力廠商軟體更新以查找惡意軟體。這些技術用於自動檢查檔案，包括病毒掃描、靜態分析、動態分析、沙箱環境中的行為分析和機器學習。

卡巴斯基專家不會對可以使用弱點和修補程式管理功能安裝的協力廠商軟體更新進行手動分析。此外，卡巴斯基專家不會在此類更新中搜尋弱點（已知或未知）或未記錄的功能，也不會對上述段落中指定的更新以外的其他類型的更新進行分析。

在受管理裝置上更新協力廠商應用程式或修復協力廠商應用程式中的弱點時，可能需要使用者互動。例如，若協力廠商應用程式目前開啟，可能會提示使用者關閉協力廠商應用程式。

若要修復一些軟體弱點，您必須接受安裝軟體的最終使用者產品授權協議 (EULA)（若系統要求您接受 EULA）。若您拒絕 EULA，則無法修復軟體弱點。

檢視軟體弱點資訊

要檢視用戶端裝置上偵測的弱點清單，

在主控台樹狀目錄的 **進階 → 應用程式管理**資料夾中，選取**軟體弱點**子資料夾。

此頁會顯示受管理裝置中偵測到的應用程式弱點清單。

若要取得應用程式弱點資訊，

從該弱點的上下文功能表中選取**內容**。

在應用程式弱點內容項目中，將顯示以下資訊：

- 所偵測到的弱點所在的應用程式。
- 偵測到裝置上的弱點清單。
- 弱點是否已經被修補的資訊。

若要檢視關於所有弱點報告，

在**軟體弱點**資料夾中，點擊**檢視弱點報告**連結。

系統將會建立裝置上所安裝應用程式中關於弱點的報告。您可以透過開啟**報告**頁籤，在相關管理伺服器名稱的節點檢視此報告。

檢視受管理裝置的弱點統計資料

您可檢視受管理裝置上各軟體弱點的統計資料。統計資料會以圖表顯示。圖表會顯示裝置數量搭配以下狀態：

- *已忽略：<裝置數量>*。若您在弱點內容中手動設定選項以忽略弱點，則會配置此狀態。
- *已修復：<裝置數量>*。若修復弱點的工作完成，則會指派此狀態。
- *修復已排程：<裝置數量>*。若您已建立工作修復弱點，但該工作尚未執行，則會指派此狀態。

- *修補程式已套用：<裝置數量>*。若您已手動選取軟體更新來修復弱點，但此更新的軟體尚未修復弱點，則會指派此狀態。

- *需要修復：<裝置數量>*。如果弱點僅在某些受管理裝置上得到修復，並且需要在更多受管理裝置上修復弱點，則會指派此狀態。

若要檢視受管理裝置的弱點統計資料：

1. 在主控台樹狀目錄的 **進階 → 應用程式管理**資料夾中，選取**軟體弱點**子資料夾。

   此頁會顯示受管理裝置中偵測到的應用程式弱點清單。

2. 選取您要檢視統計資料的弱點。

   在使用選取的物件區塊中，會顯示弱點狀態的圖表。按一下狀態會開啟裝置清單，其中會顯示有所選狀態弱點的裝置。

掃描應用程式以尋找弱點

如果您使用了快速設定精靈設定了應用程式，系統將自動建立*弱點掃描*工作。您可在**受管理裝置**資料夾的**工作**頁籤檢視工作。

若要建立一個在用戶端裝置上安裝的應用程式弱點掃描工作，請執行以下操：

1. 在主控台樹狀目錄中選取 **進階 → 應用程式管理**，接著選取**軟體弱點**子資料夾。

2. 在工作區中選取**附加操作 → 設定弱點掃描**。

   如果弱點掃描工作已經存在則會顯示**受管理裝置**資料夾的**工作**頁籤，並選取現有工作。否則，尋找弱點和所需更新工作建立精靈將啟動。遵照精靈的說明。

3. 在**選取工作類型**視窗，選取**尋找弱點掃描和必要更新**。

4. **在精靈的設定**頁面，指定以下工作設定：

- **搜尋 Microsoft 列出的弱點和更新**

  搜尋弱點與更新時，卡巴斯基安全管理中心會使用適用 Microsoft 更新的資訊（來自 Microsoft 更新來源），這些更新都是當下可取得的資訊。

  例如，如果您對 Microsoft 更新和協力廠商應用程式更新有不同設定與不同工作，您可能會需要停用此選項。

  預設情況下已啟用該選項。

  有關可選 Microsoft Windows 更新的資訊未被傳送至管理伺服器。

  - **連線更新伺服器更新資料**

    受管理裝置上的 Windows Update 代理程式會連線至 Microsoft 更新來源。以下伺服器會以 Microsoft 更新來源運作：

    - 卡巴斯基安全管理中心管理伺服器（請參閱網路代理政策的設定）
    - 具備 Microsoft Windows Server Update Services (WSUS) 的 Windows 伺服器會佈署在貴組織的網路中
    - Microsoft Updates 伺服器

    如果啟用該選項，受管理裝置上的 Windows Update 代理程式會連線至 Microsoft 更新來源，以重新整理可應用的 Microsoft Windows Update 資訊。

    若停用此選項，受管理裝置上的 Windows Update 代理程式會使用適用 Microsoft Windows 更新的資訊，此資訊先前從 Microsoft 更新來源取得。

    到 Microsoft 更新來源的連線可能消耗資源。若您的其他工作或網路代理政策內容中的**軟體更新和弱點**區域設定一般連線至此更新來源，您可能需要停用此選項。若您不要停用此選項，為了降低伺服器過載，您可設定工作排程來隨機使工作在 360 分鐘內延遲啟動。

    預設情況下已啟用該選項。

    網路代理政策設定的以下選項組合會定義取得更新的模式：

    - 僅當在**尋找弱點和所需更新連線更新伺服器更新資料工作的屬性中**啟用了*連線到更新伺服器以更新資料弱點掃描和所需更新選項*並且**Windows Update 搜尋模式**選項在網路代理政策的設定中被設定為**主動**時，受管理裝置上的 Windows 更新代理才會連線到更新伺服器以獲取更新。
    - 如果在執行*弱點掃描*工作時不需要網路代理來啟動與 Microsoft Windows 更新來源的連線並下載更新，則可以將**Windows Update 搜尋模式**選項設為**被動**，同時**連線更新伺服器更新資料**選項必須保持啟用狀態。這可讓您節省資源並使用先前收到的 Windows 更新來掃描弱點。如果您設定以不同方式接收 Microsoft Windows 更新，則可以使用被動模式。如果未以其他方式設定接收 Microsoft Windows 更新，請勿將**Windows Update 搜尋模式**選項設為**被動**，因為在這種情況下，將永遠不會收到有關更新的資訊。
    - 無論**連線更新伺服器更新資料**選項是何狀態（啟用還是停用），只要 **Windows Update 搜尋模式**選項被設定為**已停用**，卡巴斯基安全管理中心便不會請求任何更新資訊。

- **搜尋 Kaspersky 列出的第三方弱點和更新**

如果啟用該選項，卡巴斯基安全管理中心在 Windows 登錄檔和**指定檔案系統中應用程式進階搜尋的路徑**下指定的資料夾中搜尋弱點和協力廠商應用程式所需更新（由非 Kaspersky 和 Microsoft 軟體供應商製作的應用程式）。支援的協力廠商應用程式的完整清單由 Kaspersky 管理。

如果停用該選項，卡巴斯基安全管理中心不為協力廠商應用程式尋找弱點和所需更新。例如，如果您有帶有不同 Microsoft Windows 更新和協力廠商應用程式更新設定的不同工作，您可能想要停用該選項。

預設情況下已啟用該選項。

- **指定檔案系統中應用程式進階搜尋的路徑**

卡巴斯基安全管理中心搜尋需要修復弱點和安裝更新的協力廠商應用程式。您可以使用系統變數。

指定應用程式安裝資料夾。預設下，清單包含大多數應用程式所安裝的系統資料夾。

- **啟用進階診斷**

如果啟用該功能，即便寫入偵錯檔案在卡巴斯基安全管理中心遠端診斷公用程式中對網路代理停用，網路代理也寫入偵錯檔案。偵錯輪流寫入兩個檔案中；兩個檔案的最大大小由**進階診斷檔案的最大大小 (MB)**值決定。當兩個檔案都滿時，網路代理再次開始寫入它們。帶有偵錯的檔案儲存在 %WINDIR%\Temp 資料夾。這些檔案在遠端診斷公用程式中可以被存取，您可以在那裡下載或刪除它們。

如果停用該功能，網路代理根據卡巴斯基安全管理中心遠端診斷公用程式中的設定寫入偵錯。沒有附加偵錯被寫入。

當建立工作時，您不必啟用進階診斷。您可能想要使用該功能，如果，例如，工作在一些裝置上失敗且您想要在另一個工作執行期間獲取額外資訊。

預設情況下已停用該選項。

- **進階診斷檔案的最大大小 (MB)**

預設值是 100 MB，可用值介於 1 MB 和 2,048 MB 之間。當您所傳送的進階診斷檔案資訊不足以定位問題時，您可能被 Kaspersky 技術支援專家需求變更預設值。

5. 在**設定工作排程**精靈頁面，您可以為啟動工作建立排程。如果必要，指定以下設定：

- **排程開始：**

  選取工作執行排程並設定所選排程。

  - **每 N 小時**

    工作定期執行，按照指定小時數間隔，從指定的日期和時間開始。

    預設下，工作每 6 小時執行一次，從目前系統日期和時間開始。

  - **每 N 天**

    工作定期執行，按照指定天數間隔。此外，您可指定第一個工作執行的日期與時間。這些額外選項會在您建立的工作受到應用程式支援時可用。

    預設下，工作每天執行一次，從目前系統日期和時間開始。

  - **每 N 星期**

    工作定期執行，按照指定星期數間隔，從指定的星期和時間開始。

    預設下，工作每星期一於目前系統時間執行一次。

  - **每 N 分鐘**

    工作定期執行，按照指定分鐘數間隔，從工作建立日期的指定時間開始。

    預設下，工作每 30 分鐘執行一次，從目前系統時間開始。

  - **每天（不支援日光節約時間）**

    工作定期執行，按照指定天數間隔。排程不支援日光節約時間 (DST)。這意味著在夏令時開始和結束時當時鐘向前或向後撥動一小時時，實際工作啟動時間不變更。

    我們不建議您使用該排程。它用於向後相容卡巴斯基安全管理中心。

    預設下，工作每天於目前系統時間執行一次。

  - **每週**

    工作每週在指定星期和指定時間執行。

  - **按每星期中的指定日**

    工作定期執行，在每周指定日期的指定時間。

    預設下，工作每週五 6:00:00 P.M. 執行。

  - **每月**

工作定期執行，在指定月日的指定時間。

在缺少指定日的月份，工作在最後一天執行。

預設下，工作在每月的第一天執行，在目前系統時間。

- **手動**

  工作不自動執行。您僅可以手動啟動。

  預設情況下已選定此選項。

- **每個月在所選週的指定天**

  工作定期在指定月日的指定時間執行。

  預設情況下，不選取一個月中的任何一天。預設開始時間為 18:00。

- **當新更新下載至儲存區時**

  工作會在更新下載至儲存區時執行。例如，您可能希望使用此排程進行「尋找弱點和必要更新」工作。

- **在偵測到病毒爆發時**

  工作在發生*病毒爆發*事件後執行。選取將監控病毒爆發的應用程式類型。有下列應用程式類型可用：

  - 病毒防護工作站和檔案伺服器
  - 用於週邊防護的防毒軟體
  - 用於郵件伺服器的防毒軟體

  預設情況下選定所有應用程式類型。

  您可能想根據報告病毒爆發的安全應用程式類型執行不同的工作。此種情況下，刪除您不需要的應用程式類型選項。

- **在完成其它工作時**

  目前工作在其他工作完成後啟動。您可以選取先前工作如何結束（成功或帶有錯誤）以觸發目前工作的啟動。例如，您可能想使用***Turn on the device***選項執行開啟裝置工作，完成後，請執行*惡意軟體掃描*工作。只有當這兩項工作都被分配給相同的裝置時，此參數才會有作用。

- **執行錯過的工作**

該選項決定在工作要啟動時用戶端裝置在網路中不可見時工作的行為。

如果啟用該選項，系統將在下一次在用戶端裝置上執行 Kaspersky 應用程式時嘗試啟動工作。如果工作排程是**手動**、**一次**或**立即**，裝置在網路中可見或包含在工作範圍後，工作會立即啟動。

如果停用此選項，則僅限排程的工作會在用戶端裝置上執行。若為**手動**、**一次**與**立即**排程，工作僅會在網路上顯示的用戶端裝置上執行。例如，您可能想為消耗資源的工作停用該選項，您僅想在業餘時間執行該工作。

預設情況下已停用該選項。

- **使用工作啟動自動隨機延遲**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動，即是，*分佈式工作啟動*。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  當工作被建立時，根據工作中包含用戶端裝置的數量，分發啟動時間被自動計算。然後，工作總是在計算的開始時間啟動。然後當工作設定被編輯或者工作被手動啟動時，計算的工作啟動時間值被變更。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

- **使用工作啟動隨機延遲間隔（分鐘）**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

  預設情況下已停用該選項。預設時間間隔為一分鐘。

6. 在**定義工作名稱**精靈頁面，指定您正在建立的工作名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。

7. 在精靈的**完成工作建立**頁面，點擊**完成**按鈕關閉精靈。

   如果您想讓工作在精靈完成時立即啟動，選取**精靈完成時執行工作**核取方塊。

   在精靈完成作業後，「**尋找弱點掃描與必要更新**」的工作會在**受管理裝置**資料夾**工作**頁籤中的工作清單中顯示。

   除了您在工作建立過程中指定的設定，您還可以變更所建立工作的其他屬性。

當「*尋找弱點和所需更新*」工作完成後，管理伺服器顯示裝置上應用程式中發現的弱點清單；它還顯示用來修復弱點的所有軟體更新。

如果您遇到 0x80240033「Windows 更新代理錯誤 80240033（「無法下載產品授權條款」）」，您可以透過 Windows 登錄資料解決此問題。

當您先後執行兩個工作 – 停用了**下載快速安裝檔案**的*執行 Windows 更新同步工作*，和*尋找弱點和所需更新工作*時，管理伺服器不顯示所需軟體更新清單。為了檢視所需軟體更新清單，您必須再次執行*尋找弱點和所需更新*工作。

網路代理從 Windows 更新或管理伺服器（如果管理伺服器作為 WSUS 伺服器）接收任何可用的 Windows 更新和其他 Microsoft 產品更新的資訊。在應用程式開啟時和每次用戶端裝置上的*尋找弱點和所需更新*工作啟動時，資訊被傳輸。

修復應用程式中的弱點

若您已在快速設定精靈的**更新管理設定**頁面選取**尋找與安裝需要的更新**，則會自動建立*安裝必要的更新與修正弱點*工作。該工作將顯示在**工作**頁籤中**受管理裝置**資料夾的工作區。

否則，您可以做以下任意：

- 建立工作以透過安裝可用更新來修復弱點。
- 新增弱點修復規則到現有弱點修復工作。

在受管理裝置上更新協力廠商應用程式或修復協力廠商應用程式中的弱點時，可能需要使用者互動。例如，若協力廠商應用程式目前開啟，可能會提示使用者關閉協力廠商應用程式。

透過建立弱點修復工作來修復弱點

您可以做以下任意：

- 建立工作以修復多個滿足特定規則的弱點。
- 選取弱點並建立修復它和相似弱點的工作。

要修復滿足特定規則的弱點：

1. 在主控台樹狀目錄中，選取要修復弱點的裝置上的管理伺服器。
2. 在程式主視窗的**檢視**功能表，選取**設定介面**。
3. 在開啟的視窗中，選中**顯示弱點和修補程式管理**核取方塊，然後點擊**確定**。
4. 在帶有程式訊息的視窗，點擊**確定**。
5. 重新啟動管理主控台，使變更生效。
6. 在主控台樹狀目錄中，選擇**受管理裝置**資料夾。
7. 在工作區中，選取**工作**標籤。
8. 點擊**建立工作**按鈕以執行新工作精靈。遵照精靈的說明。
9. 在精靈的**選取工作類型**視窗中，選取**安裝所需更新並修復弱點**。

   如果沒有顯示該工作，請檢查您的帳戶是否具有**系統管理**：**弱點和修補程式管理**功能區域的**讀取**、**修改**和**執行**權限。如果沒有這些存取權限，您就不能建立及設定*安裝所需更新並修復弱點*的工作。

10. **在精靈的設定**頁面，指定以下工作設定：

- **指定安裝更新規則**

  這些規則被套用到用戶端裝置上的更新安裝。如果規則未被指定，工作無可執行。對於使用規則操作的資訊，請參考更新安裝規則。

- **在裝置重新啟動或關閉時開始安裝**

  如果啟用該選項，更新在裝置被重新啟動或關閉時安裝。否則，更新根據排程安裝。

  如果安裝更新可能影響裝置效能則使用該選項。

  預設情況下已停用該選項。

- **安裝所需的一般系統元件**

  如果啟用該選項，在安裝更新之前，應用程式自動安裝所需的所有一般系統元件（先決條件）。例如，這些先決條件可以是作業系統更新。

  如果停用該選項，您可能必須手動安裝先決條件。

  預設情況下已停用該選項。

- **更新過程中允許安裝新的應用程式版本**

  如果啟用該**選項**，如果更新導致軟體應用程式新版本的安裝，更新將被允許。

  如果停用該選項，軟體不被升級。您可以稍後手動或透過其他工作安裝軟體的新版本。例如，如果公司基礎架構不被新軟體版本支援，或者如果您想要在測試基礎架構中檢查升級，您可能使用該選項。

  預設情況下已啟用該選項。

  升級應用程式可能導致安裝在用戶端裝置上的獨立應用程式功能異常。

- **下載更新到裝置而不安裝**

  如果啟用該選項，應用程式下載更新到裝置但是不自動安裝它們。您可以稍後手動安裝下載的更新。

  Microsoft 更新被下載到系統 Windows 儲存。協力廠商應用程式更新（由非 Kaspersky 和 Microsoft 軟體供應商製作的應用程式）會下載到在**下載更新資料夾**欄位指定的資料夾。

  如果停用該選項，更新被自動安裝到裝置。

  預設情況下已停用該選項。

  - **下載更新資料夾**

    該資料夾用於下載協力廠商應用程式（由非 Kaspersky 和 Microsoft 軟體供應商製作的應用程式）更新。

- **啟用進階診斷**

如果啟用該功能，即便寫入偵錯檔案在卡巴斯基安全管理中心遠端診斷公用程式中對網路代理停用，網路代理也寫入偵錯檔案。偵錯輪流寫入兩個檔案中；兩個檔案的最大大小由**進階診斷檔案的最大大小 (MB)**值決定。當兩個檔案都滿時，網路代理再次開始寫入它們。帶有偵錯的檔案儲存在 %WINDIR%\Temp 資料夾。這些檔案在遠端診斷公用程式中可以被存取，您可以在那裡下載或刪除它們。

如果停用該功能，網路代理根據卡巴斯基安全管理中心遠端診斷公用程式中的設定寫入偵錯。沒有附加偵錯被寫入。

當建立工作時，您不必啟用進階診斷。您可能想要使用該功能，如果，例如，工作在一些裝置上失敗且您想要在另一個工作執行期間獲取額外資訊。

預設情況下已停用該選項。

- **進階診斷檔案的最大大小 (MB)**

  預設值是 100 MB，可用值介於 1 MB 和 2,048 MB 之間。當您所傳送的進階診斷檔案資訊不足以定位問題時，您可能被 Kaspersky 技術支援專家需求變更預設值。

11. 在精靈的**選取作業系統重新啟動選項**頁面上，選取用戶端裝置的作業系統在操作後必須被重新啟動時的操作：

- **不重新啟動裝置**

  用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

- **重新啟動裝置**

  如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

- **提示使用者操作**

  用戶端裝置螢幕上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。該選項適用於使用者必須可以選取最方便的時間進行重新啟動的工作站。

  預設情況下已選定此選項。

  - **重複提示間隔（分鐘）**

    如果啟用該選項，應用程式以指定頻率提示使用者重新啟動作業系統。

    預設情況下已啟用該選項。預設間隔是 5 分鐘。可用值介於 1 和 1440 分鐘之間。

    如果停用該選項，提示僅顯示一次。

  - **在該時間後重新啟動（分鐘）**

    提示使用者之後，應用程式在指定時間間隔後強制作業系統重新啟動。

    預設情況下已啟用該選項。預設延時是 30 分鐘。可用值介於 1 和 1440 分鐘之間。

- **強制關閉已鎖定連線的應用程式**

  執行應用程式可能會阻止用戶端裝置重新啟動。例如，如果文件在文書處理應用程式中編輯且未儲存，應用程式不會允許裝置重新啟動。

  如果啟用該選項，鎖定裝置上的此類應用程式在裝置重新啟動前被強制關閉。結果，使用者可能遺失他們未儲存的變更。

  如果停用該選項，鎖定裝置不被重新啟動。此裝置上的工作狀態表示裝置需要重新啟動。使用者必須手動關閉所有執行在鎖定裝置上的應用程式並重新啟動這些裝置。

  預設情況下已停用該選項。

12. 在**設定工作排程**精靈頁面，您可以為啟動工作建立排程。如果必要，指定以下設定：

- **排程開始：**

  選取工作執行排程並設定所選排程。

  - **每 N 小時**

    工作定期執行，按照指定小時數間隔，從指定的日期和時間開始。

    預設下，工作每 6 小時執行一次，從目前系統日期和時間開始。

  - **每 N 天**

    工作定期執行，按照指定天數間隔。此外，您可指定第一個工作執行的日期與時間。這些額外選項會在您建立的工作受到應用程式支援時可用。

    預設下，工作每天執行一次，從目前系統日期和時間開始。

  - **每 N 星期**

    工作定期執行，按照指定星期數間隔，從指定的星期和時間開始。

    預設下，工作每星期一於目前系統時間執行一次。

  - **每 N 分鐘**

    工作定期執行，按照指定分鐘數間隔，從工作建立日期的指定時間開始。

    預設下，工作每 30 分鐘執行一次，從目前系統時間開始。

  - **每天（不支援日光節約時間）**

    工作定期執行，按照指定天數間隔。排程不支援日光節約時間 (DST)。這意味著在夏令時開始和結束時當時鐘向前或向後撥動一小時時，實際工作啟動時間不變更。

    我們不建議您使用該排程。它用於向後相容卡巴斯基安全管理中心。

    預設下，工作每天於目前系統時間執行一次。

  - **每週**

    工作每週在指定星期和指定時間執行。

  - **按每星期中的指定日**

    工作定期執行，在每周指定日期的指定時間。

    預設下，工作每週五 6:00:00 P.M. 執行。

  - **每月**

工作定期執行，在指定月日的指定時間。

在缺少指定日的月份，工作在最後一天執行。

預設下，工作在每月的第一天執行，在目前系統時間。

- **手動**

  工作不自動執行。您僅可以手動啟動。

  預設情況下已選定此選項。

- **每個月在所選週的指定天**

  工作定期在指定月日的指定時間執行。

  預設情況下，不選取一個月中的任何一天。預設開始時間為 18:00。

- **在偵測到病毒爆發時**

  工作在發生*病毒爆發*事件後執行。選取將監控病毒爆發的應用程式類型。有下列應用程式類型可用：

  - 病毒防護工作站和檔案伺服器
  - 用於週邊防護的防毒軟體
  - 用於郵件伺服器的防毒軟體

  預設情況下選定所有應用程式類型。

  您可能想根據報告病毒爆發的安全應用程式類型執行不同的工作。此種情況下，刪除您不需要的應用程式類型選項。

- **在完成其它工作時**

  目前工作在其他工作完成後啟動。您可以選取先前工作如何結束（成功或帶有錯誤）以觸發目前工作的啟動。例如，您可能想使用***Turn on the device***選項執行開啟裝置工作，完成後，請執行*惡意軟體掃描*工作。只有當這兩項工作都被分配給相同的裝置時，此參數才會有作用。

- **執行錯過的工作**

  該選項決定在工作要啟動時用戶端裝置在網路中不可見時工作的行為。

  如果啟用該選項，系統將在下一次在用戶端裝置上執行 Kaspersky 應用程式時嘗試啟動工作。如果工作排程是**手動**、**一次**或**立即**，裝置在網路中可見或包含在工作範圍後，工作會立即啟動。

  如果停用此選項，則僅限排程的工作會在用戶端裝置上執行。若為**手動**、**一次**與**立即**排程，工作僅會在網路上顯示的用戶端裝置上執行。例如，您可能想為消耗資源的工作停用該選項，您僅想在業餘時間執行該工作。

  預設情況下已停用該選項。

- **使用工作啟動自動隨機延遲**

如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動，即是，*分佈式工作啟動*。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

當工作被建立時，根據工作中包含用戶端裝置的數量，分發啟動時間被自動計算。然後，工作總是在計算的開始時間啟動。然後當工作設定被編輯或者工作被手動啟動時，計算的工作啟動時間值被變更。

如果該選項被停用，工作依據排程在用戶端裝置上啟動。

- **使用工作啟動隨機延遲間隔（分鐘）**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

  預設情況下已停用該選項。預設時間間隔為一分鐘。

13. 在**定義工作名稱**精靈頁面，指定您正在建立的工作名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。

14. 在精靈的**完成工作建立**頁面，點擊**完成**按鈕關閉精靈。

    如果您想讓工作在精靈完成時立即啟動，選取**精靈完成時執行工作**核取方塊。

等待精靈完成操作後，系統將建立**安裝所需更新並修復弱點**工作，並顯示在**工作**資料夾中。

除了您在工作建立過程中指定的設定，您還可以變更所建立工作的其他屬性。

若工作結果包含 0x80240033「Windows 更新代理錯誤 80240033（「無法下載產品授權條款」）」錯誤，您可以透過 Windows 登錄資料解決此問題。

要修復特定弱點和相似弱點：

1. 在主控台樹狀目錄的 **進階 → 應用程式管理**資料夾中，選取**軟體弱點**子資料夾。

2. 選取您要修復的弱點。

3. 點擊**執行修復弱點精靈**按鈕。

   弱點修復精靈啟動。

   弱點修復精靈功能僅在弱點和修補程式管理產品授權下可用。

   遵照精靈的說明。

4. 在**搜尋現有的修復弱點工作**視窗中，指定以下參數：

   - **僅顯示修復此弱點的工作**

     如果啟用該選項，弱點修復精靈搜尋修復所選弱點的現有工作。

     如果停用該選項或搜尋未擷取到可應用工作，弱點修復精靈提示您為修復弱點建立規則或工作。

     預設情況下已啟用該選項。

   - **批准修復該弱點的更新**

     修復弱點的更新將被批准安裝。如果一些應用的更新安裝規則僅允許安裝批准的更新，請啟用該選項。

     預設情況下已停用該選項。

5. 如果您選取搜尋現有弱點修復工作或搜尋擷取到一些工作，您可以檢視這些工作的屬性或手動啟動它們。不需要進一步操作。

   否則，點擊**新修復弱點工作**按鈕。

6. 選取修復弱點規則類型以新增到新工作，然後按一下**結束**按鈕。

7. 在顯示的提示中做出安裝所有先前應用程式更新的選取。如果您同意在安裝所選更新需要時安裝連續的應用程式版本，按一下**是**。如果您要直接更新應用程式而不安裝連續版本，按一下**否**。如果安裝所選更新不能不安裝先前版本的應用程式，應用程式更新失敗。

   更新安裝和弱點修復工作建立精靈啟動。遵照精靈的說明。

8. 在精靈的**選取作業系統重新啟動選項**頁面上，選取用戶端裝置的作業系統在操作後必須被重新啟動時的操作：

- **不重新啟動裝置**

  用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

- **重新啟動裝置**

  如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

- **提示使用者操作**

  用戶端裝置螢幕上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。該選項適用於使用者必須可以選取最方便的時間進行重新啟動的工作站。

  預設情況下已選定此選項。

  - **重複提示間隔（分鐘）**

    如果啟用該選項，應用程式以指定頻率提示使用者重新啟動作業系統。

    預設情況下已啟用該選項。預設間隔是 5 分鐘。可用值介於 1 和 1440 分鐘之間。

    如果停用該選項，提示僅顯示一次。

  - **在該時間後重新啟動（分鐘）**

    提示使用者之後，應用程式在指定時間間隔後強制作業系統重新啟動。

    預設情況下已啟用該選項。預設延時是 30 分鐘。可用值介於 1 和 1440 分鐘之間。

- **強制關閉已鎖定連線的應用程式**

  執行應用程式可能會阻止用戶端裝置重新啟動。例如，如果文件在文書處理應用程式中編輯且未儲存，應用程式不會允許裝置重新啟動。

  如果啟用該選項，鎖定裝置上的此類應用程式在裝置重新啟動前被強制關閉。結果，使用者可能遺失他們未儲存的變更。

  如果停用該選項，鎖定裝置不被重新啟動。此裝置上的工作狀態表示裝置需要重新啟動。使用者必須手動關閉所有執行在鎖定裝置上的應用程式並重新啟動這些裝置。

  預設情況下已停用該選項。

9. 在精靈的**選取要對其分配工作的裝置**頁面上，選取以下其中一個選項：

- **選取管理伺服器偵測到的網路裝置**

  工作被分配到指定裝置。特定裝置可以包含管理群組的裝置和未配置的裝置。

  例如，您可能要在安裝網路代理到未配置的裝置的工作中使用該選項。

- **手動指定裝置位址或從清單匯入位址**

  您可以指定您要為其分配工作的裝置的 NetBIOS 名稱、DNS 名稱、IP 位址和 IP 子網路。

  您可能要使用該選項以對特定子網路執行工作。例如，您可能要安裝特定應用程式到會計裝置，或者掃描疑似被感染子網路中的裝置。

- **分配工作到裝置分類**

  該工作被分配到裝置選項中的裝置。您可以指定其中一個現有選項。

  例如，您可能要使用該選項在特定作業系統版本的裝置上執行工作。

- **分配工作到管理群組**

  工作被分配到包含在管理群組中的裝置。您可以指定其中一個現有群組或者建立新群組。

  例如，您可能要使用該選項執行傳送訊息到使用者工作，如果訊息針對包含在特定管理群組中的裝置。

  如果工作被指派給管理群組，則工作屬性視窗中不會顯示**安全**標籤，因為群組工作受其所套用的群組的安全設定的約束。

10. 在**設定工作排程**精靈頁面，您可以為啟動工作建立排程。如果必要，指定以下設定：

- **排程開始：**

  選取工作執行排程並設定所選排程。

  - **每 N 小時**

    工作定期執行，按照指定小時數間隔，從指定的日期和時間開始。

    預設下，工作每 6 小時執行一次，從目前系統日期和時間開始。

  - **每 N 天**

    工作定期執行，按照指定天數間隔。此外，您可指定第一個工作執行的日期與時間。這些額外選項會在您建立的工作受到應用程式支援時可用。

    預設下，工作每天執行一次，從目前系統日期和時間開始。

  - **每 N 星期**

    工作定期執行，按照指定星期數間隔，從指定的星期和時間開始。

    預設下，工作每星期一於目前系統時間執行一次。

  - **每 N 分鐘**

    工作定期執行，按照指定分鐘數間隔，從工作建立日期的指定時間開始。

    預設下，工作每 30 分鐘執行一次，從目前系統時間開始。

  - **每天（不支援日光節約時間）**

    工作定期執行，按照指定天數間隔。排程不支援日光節約時間 (DST)。這意味著在夏令時開始和結束時當時鐘向前或向後撥動一小時時，實際工作啟動時間不變更。

    我們不建議您使用該排程。它用於向後相容卡巴斯基安全管理中心。

    預設下，工作每天於目前系統時間執行一次。

  - **每週**

    工作每週在指定星期和指定時間執行。

  - **按每星期中的指定日**

    工作定期執行，在每周指定日期的指定時間。

    預設下，工作每週五 6:00:00 P.M. 執行。

  - **每月**

工作定期執行，在指定月日的指定時間。

在缺少指定日的月份，工作在最後一天執行。

預設下，工作在每月的第一天執行，在目前系統時間。

- **手動**

  工作不自動執行。您僅可以手動啟動。

  預設情況下已選定此選項。

- **每個月在所選週的指定天**

  工作定期在指定月日的指定時間執行。

  預設情況下，不選取一個月中的任何一天。預設開始時間為 18:00。

- **在偵測到病毒爆發時**

  工作在發生*病毒爆發*事件後執行。選取將監控病毒爆發的應用程式類型。有下列應用程式類型可用：

  - 病毒防護工作站和檔案伺服器
  - 用於週邊防護的防毒軟體
  - 用於郵件伺服器的防毒軟體

  預設情況下選定所有應用程式類型。

  您可能想根據報告病毒爆發的安全應用程式類型執行不同的工作。此種情況下，刪除您不需要的應用程式類型選項。

- **在完成其它工作時**

  目前工作在其他工作完成後啟動。您可以選取先前工作如何結束（成功或帶有錯誤）以觸發目前工作的啟動。例如，您可能想使用***Turn on the device***選項執行開啟裝置工作，完成後，請執行*惡意軟體掃描*工作。只有當這兩項工作都被分配給相同的裝置時，此參數才會有作用。

- **執行錯過的工作**

  該選項決定在工作要啟動時用戶端裝置在網路中不可見時工作的行為。

  如果啟用該選項，系統將在下一次在用戶端裝置上執行 Kaspersky 應用程式時嘗試啟動工作。如果工作排程是**手動**、**一次**或**立即**，裝置在網路中可見或包含在工作範圍後，工作會立即啟動。

  如果停用此選項，則僅限排程的工作會在用戶端裝置上執行。若為**手動**、**一次**與**立即**排程，工作僅會在網路上顯示的用戶端裝置上執行。例如，您可能想為消耗資源的工作停用該選項，您僅想在業餘時間執行該工作。

  預設情況下已停用該選項。

- **使用工作啟動自動隨機延遲**

如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動，即是，*分佈式工作啟動*。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

當工作被建立時，根據工作中包含用戶端裝置的數量，分發啟動時間被自動計算。然後，工作總是在計算的開始時間啟動。然後當工作設定被編輯或者工作被手動啟動時，計算的工作啟動時間值被變更。

如果該選項被停用，工作依據排程在用戶端裝置上啟動。

- **使用工作啟動隨機延遲間隔（分鐘）**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

  預設情況下已停用該選項。預設時間間隔為一分鐘。

11. 在**定義工作名稱**精靈頁面，指定您正在建立的工作名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。

12. 在精靈的**完成工作建立**頁面，點擊**完成**按鈕關閉精靈。

    如果您想讓工作在精靈完成時立即啟動，選取**精靈完成時執行工作**核取方塊。

當精靈完成後，系統將建立**安裝所需更新並修復弱點**工作，並顯示在**工作**資料夾中。

除了您在工作建立過程中指定的設定，您還可以變更所建立工作的其他屬性。

透過新增規則到現有弱點修復工作來修復弱點

要透過新增規則到現有弱點修復工作來修復弱點：

1. 在主控台樹狀目錄的 **進階 → 應用程式管理**資料夾中，選取**軟體弱點**子資料夾。

2. 選取您要修復的弱點。

3. 點擊**執行修復弱點精靈**按鈕。

   弱點修復精靈啟動。

   弱點修復精靈功能僅在弱點和修補程式管理產品授權下可用。

   遵照精靈的說明。

4. 在**搜尋現有的修復弱點工作**視窗中，指定以下參數：

   - **僅顯示修復此弱點的工作**

     如果啟用該選項，弱點修復精靈搜尋修復所選弱點的現有工作。

     如果停用該選項或搜尋未擷取到可應用工作，弱點修復精靈提示您為修復弱點建立規則或工作。

     預設情況下已啟用該選項。

   - **批准修復該弱點的更新**

     修復弱點的更新將被批准安裝。如果一些應用的更新安裝規則僅允許安裝批准的更新，請啟用該選項。

     預設情況下已停用該選項。

5. 如果您選取搜尋現有弱點修復工作或搜尋擷取到一些工作，您可以檢視這些工作的屬性或手動啟動它們。不需要進一步操作。

   否則，點擊**新增修復弱點規則到現有工作**按鈕。

6. 選取您要新增規則的工作，然後點擊**新增規則**按鈕。

   而且，你您可以檢視現有工作的屬性，手動啟動它們，或者建立新工作。

7. 選取要新增到所選工作的規則類型，然後按一下**結束**按鈕。

8. 在顯示的提示中做出安裝所有先前應用程式更新的選取。如果您同意在安裝所選更新需要時安裝連續的應用程式版本，按一下**是**。如果您要直接更新應用程式而不安裝連續版本，按一下**否**。如果安裝所選更新不能不安裝先前版本的應用程式，應用程式更新失敗。

弱點修復新規則被新增到現有**安裝所需更新並修復弱點**工作。

修復隔離網路中的弱點

本節介紹您可以採取哪些步驟來修復連線到無法存取網際網路的管理伺服器的受管理裝置上的協力廠商軟體弱點。

情境：修復隔離網路中的協力廠商軟體弱點

您可以安裝更新並修復安裝在隔離網路中受管理裝置上的協力廠商軟體的弱點。此類網路包括管理伺服器和連線到它們但無法存取網際網路的受管理裝置。要修復此類網路中的弱點，您需要一個連線到網際網路的管理伺服器。然後，您將能夠使用具有網際網路存取權限的管理伺服器下載修補程式（所需更新），然後將修補程式傳輸到獨立的管理伺服器。

您可以下載軟體供應商發布的協力廠商軟體更新，但無法使用卡巴斯基安全管理中心下載獨立管理伺服器上的 Microsoft 軟體更新。

要了解在隔離網路中修復弱點的過程是如何工作的，請參閱此處理程序的描述和方案。

先決條件

在開始之前，請執行以下操作：

1. 分配一台裝置用於連線到網際網路和下載修補程式。該裝置將被視為具有網際網路存取權限的管理伺服器。
2. 安裝卡巴斯基安全管理中心（不早於版本 14）在以下裝置上：
   - 分配的裝置，將充當具有網際網路存取權限的管理伺服器
   - 隔離裝置，將充當與網際網路隔離的管理伺服器（以下稱為隔離管理伺服器）
3. 確保每個管理伺服器都有足夠的磁碟空間用於下載和儲存更新和修補程式。

階段

在隔離管理伺服器的受管理裝置上安裝更新和修復協力廠商軟體弱點具有以下階段：

1. **配置具有網際網路存取權限的管理伺服器**

   準備具有網際網路存取權限的管理伺服器以處理所需協力廠商軟體更新的請求和下載修補程式。

2. **配置隔離管理伺服器**

   準備隔離管理伺服器以便他們可以定期形成所需更新的清單和處理具有網際網路存取的管理伺服器下載的修補程式。配置後，隔離管理伺服器不再嘗試從網際網路下載修補程式。相反，他們會透過修補程式獲取更新。

3. **在隔離的管理伺服器上傳輸修補程式和安裝更新**

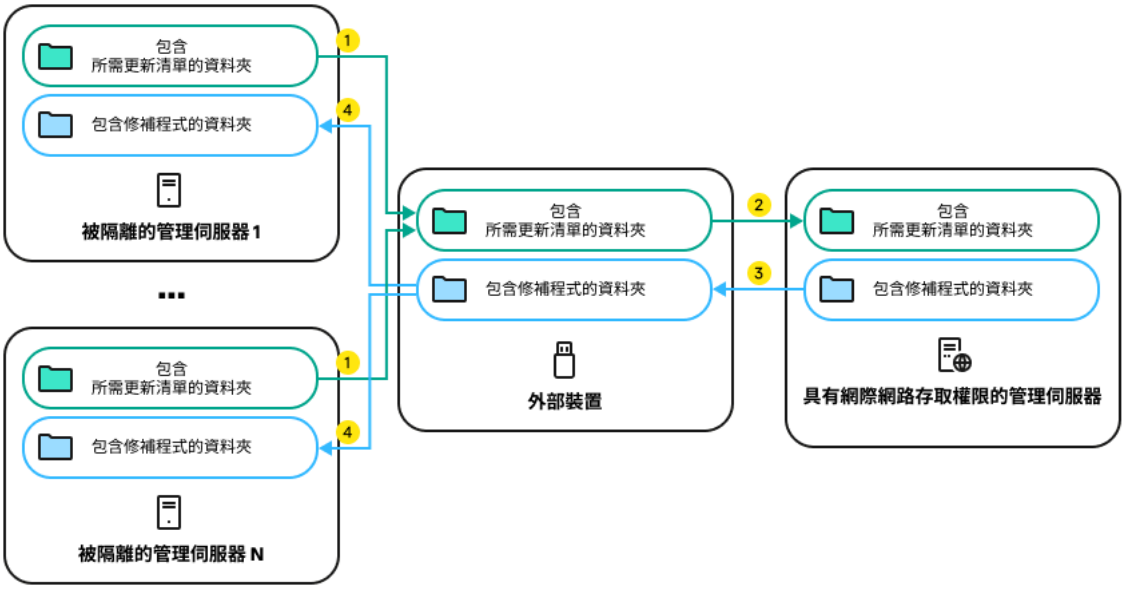
   完成管理伺服器配置後，您可以在具有網際網路存取權限的管理伺服器和隔離管理伺服器之間傳輸所需的更新清單和修補程式。接下來，修補程式的更新將透過使用*安裝所需更新並修復弱點*工作安裝在受管理裝置上。

結果

因此，協力廠商軟體更新被傳輸到隔離管理伺服器並使用卡巴斯基安全管理中心安裝在連線的受管理裝置上。配置管理伺服器一次就足夠了，之後您可以根據需要隨時獲取更新，例如每天一次或多次。

關於修復隔離網路中的協力廠商軟體弱點

修復隔離網路中的協力廠商軟體弱點的過程如圖所示，在下面描述。您可以定期重複此過程。



在具有網際網路存取權限的管理伺服器和隔離的管理伺服器之間傳輸修補程式和所需更新清單的過程

每個與網際網路隔離的管理伺服器（以下稱為隔離的管理伺服器）都會產生一個更新清單，這些更新需要安裝在連線到該管理伺服器的受管裝置上。所需更新清單儲存在特定資料夾中，並提供一組二進位檔案。每個檔案有一個名稱，其中包含具有所需更新的修補程式的 ID。結果，清單中的每個檔案都指向一個特定的修補程式。

透過使用外部裝置，您可以將所需更新的清單從隔離的管理伺服器傳輸到分配的具有網際網路存取權限的管理伺服器。之後，分配的管理伺服器會從網際網路下載修補程式並將它們放在單獨的資料夾中。

當所有修補程式已下載並位於它們的特殊資料夾中時，將這些修補程式移動到您從中獲取所需更新清單的每個隔離的管理伺服器。將修補程式儲存到在隔離的管理伺服器上專門為它們建立的資料夾中。結果，*安裝所需更新並修復弱點*工作將在隔離的管理伺服器的受管裝置上執行修補程式並安裝更新。

配置具有網際網路存取權限的管理伺服器以修復隔離網路中的弱點

若要準備在隔離網路中修復弱點並傳輸修補程式，首先配置一台可以存取網際網路的管理伺服器，然後配置獨立的管理伺服器。

要配置具有網際網路存取權限的管理伺服器：

1. 在安裝了管理伺服器的磁碟上建立兩個資料夾：
   - 所需更新清單的資料夾
   - 修補程式資料夾

   您可以隨意命名這些資料夾。
2. 使用作業系統的標準管理工具，在建立的資料夾中將修改存取權限授予 KLAdmins。

3. 使用 klscflag 公用程式將路徑寫入管理伺服器內容中的資料夾。

   使用管理員權限執行 Windows 命令提示符，然後將目前目錄變更為包含 klscflag 公用程式的目錄。klscflag 公用程式位於安裝管理伺服器的資料夾中。預設安裝路徑：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

4. 請在 Windows 命令提示符下輸入以下命令：

   - 若要設定修補程式資料夾的路徑：
     `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<資料夾路徑>"`
   - 若要為所需更新清單設定資料夾的路徑：
     `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<資料夾路徑>"`

   示例：`klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "C:\<資料夾，針對修補程式>"`

5. 如果必要，使用 klscflag 實用程式指定管理伺服器檢查新修補程式請求的頻率：
   `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <以秒為單位的值>`

   預設值是 120 秒。

   示例：`klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 150`

6. 建立*弱點掃描和所需更新*工作以取得有關受管理上安裝的協力廠商軟體的修補程式資訊，然後設定工作排程。

7. 建立*修復弱點*工作，指定用於修復弱點的協力廠商軟體的修補程式，然後設定工作排程。

   如果您希望它們在工作排程中指定的時間之前執行，請手動執行。工作啟動的順序很重要。完成*修復弱點*工作後，必須執行*弱點掃描和所需更新*工作。

8. 重新啟動管理伺服器服務。

現在，可以存取網際網路的管理伺服器已準備好下載更新並將更新傳輸到獨立的管理伺服器。在開始修復弱點之前，配置獨立的管理伺服器。

配置隔離管理伺服器以修復隔離網路中的弱點

完成配置具有網際網路存取權限的管理伺服器後，準備好網路中的每個隔離管理伺服器，這樣您就可以在連線到隔離管理伺服器的受管理裝置上修復弱點並安裝更新。

要配置隔離的管理伺服器，請在每個管理伺服器上執行以下操作：

1. 啟動一個用於弱點和修補程式管理 (VAPM) 功能的產品授權金鑰。

2. 在安裝了管理伺服器的磁碟上建立兩個資料夾：

   - 將顯示所需更新清單的資料夾
   - 修補程式資料夾

   您可以隨意命名這些資料夾。

3. 使用作業系統的標準管理工具，在建立的資料夾中將*修改*權限授予 KLAdmins。

4. 使用 klscflag 公用程式將路徑寫入管理伺服器內容中的資料夾。

   使用管理員權限執行 Windows 命令提示符，然後將目前目錄變更為包含 klscflag 公用程式的目錄。klscflag 公用程式位於安裝管理伺服器的資料夾中。預設安裝路徑：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

5. 請在 Windows 命令提示符下輸入以下命令：

   - 若要設定修補程式資料夾的路徑：
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v “<資料夾路徑>"`
   - 若要為所需更新清單設定資料夾的路徑：
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<資料夾路徑>"`

   示例：`klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "C:\<資料夾，針對修補程式>"`

6. 如果必要，使用 klscflag 實用程式指定隔離管理伺服器檢查新修補程式的頻率：
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <以秒為單位的值>`

   預設值是 120 秒。

   示例：`klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 150`

7. 如果必要，使用 klscflag 實用程式計算修補程式的 SHA256 雜湊：
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1`

   如果輸入此命令，您可以確保修補程式在傳輸到隔離管理伺服器期間未被修改，並且您已收到包含所需更新的正確修補程式。

   預設情況下，卡巴斯基安全管理中心不計算修補程式的 SHA256 雜湊。如果啟用此選項，則在隔離的管理伺服器收到修補程式後，卡巴斯基安全管理中心會計算其雜湊並將獲取的值與儲存在管理伺服器資料庫中的雜湊進行比較。如果計算出的雜湊與資料庫中的雜湊不符合，則會發生錯誤，您必須替代不正確的修補程式。

8. 建立*弱點掃描和所需更新*工作以取得有關受管理上安裝的協力廠商軟體的修補程式資訊，然後設定工作排程。

9. 建立*修復弱點*工作，指定用於修復弱點的協力廠商軟體的修補程式，然後設定工作排程。

   如果您希望它們在工作排程中指定的時間之前執行，請手動執行。工作啟動的順序很重要。完成*修復弱點*工作後，必須執行*弱點掃描和所需更新*工作。

10. 重新啟動管理伺服器服務。

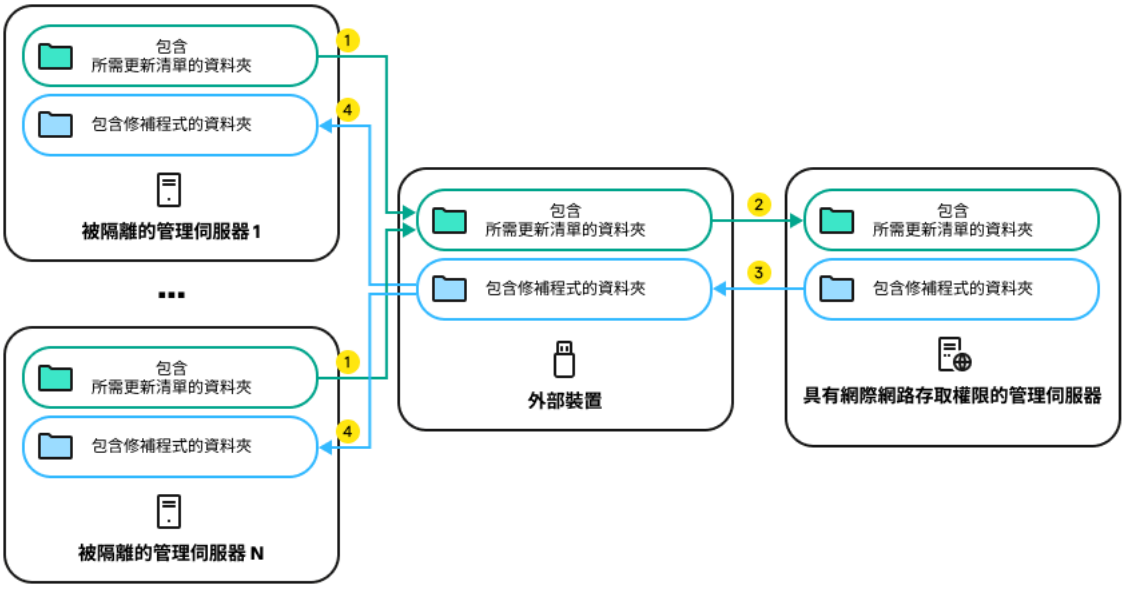
配置完所有管理伺服器後，您可以移動修補程式和所需更新清單，並修復隔離網路中受管理裝置上的協力廠商軟體弱點。

在隔離網路中傳輸修補程式和安裝更新

完成配置管理伺服器後，您可以將包含所需更新的修補程式從具有網際網路存取權限的管理伺服器傳輸到隔離的管理伺服器。您可以根據需要傳輸和安裝更新，例如每天一次或多次。

您需要一個外部裝置（例如，卸除式磁碟機）來在管理伺服器之間傳輸修補程式和所需更新的清單。因此，請確保外部裝置具有足夠的磁碟空間用於下載和儲存修補程式。

傳輸修補程式和所需更新清單的過程如圖所示，描述如下：



在具有網際網路存取權限的管理伺服器和隔離的管理伺服器之間傳輸修補程式和所需更新清單的過程

要在連線到隔離管理伺服器的受管理裝置上安裝更新和修復弱點：

1. 如果*安裝所需更新並修復弱點*工作尚未執行，請啟動之。
2. 將外部裝置連線到任何隔離的管理伺服器。
3. 在外部裝置上建立兩個資料夾：一個用於所需更新清單，一個用於修補程式。您可以隨意命名這些資料夾。

   如果您之前建立了這些資料夾，請清除它們。
4. 從每個隔離的管理伺服器複製所需更新清單，並將此清單粘貼到外部裝置上所需更新清單的資料夾中。

   結果，您將從所有隔離的管理伺服器獲取的所有清單合併到一個資料夾中。此資料夾應包含二進位檔，其中包含所有隔離管理伺服器所需的修補程式的 ID。
5. 將外部裝置連線到具有網際網路存取權限管理伺服器。
6. 從外部裝置複製所需更新清單，並將此清單粘貼到具有網際網路存取權限的管理伺服器上所需更新清單的資料夾中。

   所有需要的修補程式程序都會自動從網際網路下載到管理伺服器上的修補程式的資料夾。這可能需要幾個小時。
7. 確保下載了所有必需的修補程式。為此，您可以進行以下操作之一：

   - 檢查具有網際網路存取權限的管理伺服器上的修補程式資料夾。所需更新清單中指定的所有修補程式都應下載到必要的資料夾中。如果需要少量修補程式，這會更方便。
   - 準備一個特殊的指令碼，例如，一個 shell 指令碼。如果您獲得大量修補程式，則很難自行檢查是否已下載所有修補程式。在這種情況下，最好自動化檢查。
8. 從具有網際網路存取權限的管理伺服器複製修補程式並將它們粘貼到外部裝置上的相應資料夾中。
9. 將修補程式傳送到每個隔離的管理伺服器。將修補程式放入它們的特定資料夾中。

因此，每個隔離的管理伺服器都會建立一個實際的更新清單，連線到當前管理伺服器的受管理裝置需要這些更新。在具有網際網路存取權限的管理伺服器收到所需更新清單後，管理伺服器會從網際網路下載修補程式。當這些修補程式出現在隔離的管理伺服器上時，*安裝所需更新並修復弱點*工作將處理修補程式。因此，更新被安裝在受管理裝置上，協力廠商軟體弱點得到修復。

當*安裝所需更新並修復弱點*工作正在執行的時候，請不要重新啟動管理伺服器裝置，也不要執行*備份管理伺服器資料*工作（它也會導致重新啟動）。結果，*安裝所需更新並修復弱點*工作被中斷，沒有安裝更新。在這種情況下，您必須手動重新啟動此工作或等待工作按照配置的排程啟動。

停用在隔離網路中傳輸修補程式和安裝更新的選項

您可以在隔離的伺服器行停用傳輸修補程式，例如，如果您決定將一個或多個管理伺服器從一個隔離網路中取出。因此，您可以減少修補程式的數量和下載它們的時間。

要停用在隔離的管理伺服器上傳輸修補程式的選項：

1. 如果要使所有管理伺服器脫離隔離狀態，請在具有網際網路存取權限的管理伺服器的屬性中，刪除修補程式資料夾的路徑和所需更新的清單。如果您想將一些管理伺服器保留在隔離網路中，請略過此步驟。

   使用管理員權限執行 Windows 命令提示符，然後將目前目錄變更為包含 klscflag 公用程式的目錄。klscflag 公用程式位於安裝管理伺服器的資料夾中。預設安裝路徑：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   請在命令提示符下輸入以下命令：

   - 若要刪除修補程式資料夾的路徑：
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""
     ```
   - 若要為所需更新清單刪除資料夾的路徑：
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""
     ```

2. 如果您刪除了此管理伺服器上資料夾的路徑，請重新啟動管理伺服器服務。

3. 在要解除獨立的每個管理伺服器的內容中，刪除修補程式資料夾的路徑和所需更新的清單。

   使用管理員權限在 Windows 命令提示符處輸入以下指令：

   - 若要刪除修補程式資料夾的路徑：
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""
     ```
   - 若要為所需更新清單刪除資料夾的路徑：
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""
     ```

4. 重新啟動已刪除資料夾路徑的每個管理伺服器的服務。

因此，如果您重新配置了具有網際網路存取權限的管理伺服器，您將不再透過卡巴斯基安全管理中心接收修補程式。如果您只重新配置了某些獨立的管理伺服器（例如，將其中一些從孤立網路中取出），您將只獲得剩餘的獨立管理伺服器的修補程式。

如果您想在將來開始修復停用的獨立管理伺服器上的弱點，您必須再次配置這些管理伺服器和管理伺服器以存取網際網路。

忽略軟體弱點

您可忽略要修復的軟體弱點。忽略軟體弱點的原因可能如下：

- 您認為軟體弱點對您組織不緊急。
- 您瞭解軟體弱點修復會損壞需弱點修復之軟體的相關資料。
- 您確定軟體弱點對您組織網路並不危險，因為您使用其他措施防護您的受管理裝置。

您可在所有受管理裝置或僅在選取的受管理裝置忽略軟體弱點。

若要在所有受管理裝置上忽略軟體弱點：

1. 在主控台樹狀目錄的 **進階 → 應用程式管理**資料夾中，選取**軟體弱點**子資料夾。
   資料夾的工作區中將顯示在裝置上的網路代理偵測到的應用程式弱點清單。
2. 選取您要忽略的弱點。
3. 從該弱點的上下文功能表中選取**內容**。
   弱點的內容視窗隨即開啟。
4. 在**一般**區段上選取**略過弱點**選項。
5. 點擊**確定**。
   系統會關閉軟體弱點內容視窗。

軟體弱點會在所有受管理裝置遭到忽略。

若要在選取的受管理裝置忽略軟體弱點：

1. 在開啟選取的受管理裝置內容視窗並選取**軟體弱點**區域。
2. 選取軟體弱點。
3. 忽略選取的弱點。

軟體弱點會在選取的裝置上遭到忽略。

忽略的軟體弱點在完成*修復弱點*工作或*安裝所需更新並修復弱點*工作將不會修復。您可從弱點清單使用篩選器排除忽略的軟體弱點。

選取適用於協力廠商軟體中弱點的使用者修復項目

若要使用*修復弱點*工作，您必須手動指定軟體更新來修復列於工作設定中協力廠商軟體清單中的弱點。*修復弱點*工作會使用適用於 Microsoft 軟體的建議修復項目，以及適用於其他協力廠商軟體的使用者修復項目。*使用者修復項目*是管理員手動指定安裝用來修復適用於弱點的軟體更新。

若要在協力廠商軟體中選取適用於弱點的使用者修復項目：

1. 在主控台樹狀目錄的 **進階 → 應用程式管理**資料夾中，選取**軟體弱點**子資料夾。

   資料夾的工作區中將顯示在裝置上的網路代理偵測到的應用程式弱點清單。

2. 選取您要針對的弱點指定使用者修復項目。

3. 從該弱點的上下文功能表中選取**內容**。

   弱點的內容視窗隨即開啟。

4. 在**使用者修復和其他修復**區段，點擊**新增**按鈕。

   系統會顯示可用安裝套件清單。顯示的安裝套件清單會對應**遠端安裝 → 安裝套件**清單。若您未建立內含適用於所選弱點之使用者修復項目的安裝套件，您可啟動新安裝套件精靈以立即建立套件。

5. 在協力廠商軟體中，選取內含適用於弱點之使用者修復項目的安裝套件（或套件）。

6. 點擊**確定**。

系統會指定包含適用於軟體弱點之使用者修復項目的安裝套件。當啟動*修復弱點*工作時，系統會安裝安裝套件並修復軟體弱點。

更新安裝規則

當在應用程式中修復弱點時，您必須指定更新安裝規則。這些規則決定要安裝的更新和要修復的弱點。

精確設定取決於您是否建立了 Microsoft 應用程式、協力廠商應用程式（由非 Kaspersky 和 Microsoft 軟體供應商製作的應用程式）、或所有應用程式的更新的規則。當建立 Microsoft 應用程式或協力廠商應用程式規則時，您可以選取特定的應用程式和您要安裝更新的應用程式版本。當建立所有應用程式的規則時，您可以選取您要安裝的特定更新和您要透過安裝更新而修復的弱點。

要為所有應用程式更新建立規則：

1. 在新工作精靈的**設定**頁面上，點擊**新增**按鈕。

   規則建立精靈開始。遵照精靈的說明。

2. 在**規則類型**頁面上，選取**所有更新的規則**。

3. 在**一般標準**頁面，使用下拉清單指定以下設定：

- **要安裝的更新集**

  選取必須在用戶端裝置上安裝的更新：

  - **僅安裝批准的更新**。這僅安裝批准的更新。
  - **安裝所有更新（除了拒絕的）**。這安裝帶有*已批准*或*未定義*批准狀態的更新。
  - **安裝所有更新（包含拒絕的）**。這安裝所有更新，無論什麼批准狀態。警惕選取該選項。例如，如果您想要在測試基礎架構中檢查一些被拒絕的更新的安裝，使用該選項。

- **修復弱點的時機為嚴重等級大於或等於**

  有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

  如果啟用該選項，更新僅修復 Kaspersky 設定的安全等級等於或高於清單中選定的值（**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

  如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

  預設情況下已停用該選項。

4. 在**更新**頁面，選取要安裝的更新：

- **安裝所有合適的更新**

  安裝滿足在精靈中**一般標準**頁面指定標準的所有軟體更新。預設選取。

- **僅安裝清單中的更新**

  僅安裝您從清單中手動選取的軟體更新。該清單包含所有可用軟體更新。

  例如，您可能想要在以下情況下選取特定更新：要在測試環境中檢查它們的安裝、要僅更新嚴重應用程式、或者要僅更新特定應用程式。

  - **自動安裝所選更新安裝時需要的所有先前應用程式更新**

    如果在安裝所選更新需要時，您同意安裝暫時應用程式版本，保持該選項被啟用。

    如果停用該選項，僅選定的應用程式版本被安裝。如果您想直截了當地更新應用程式，而不嘗試安裝增量版本，請停用該選項。如果安裝所選更新不能不安裝先前版本的應用程式，應用程式更新失敗。

    例如，您在裝置上安裝了應用程式的版本 3，您想更新它到版本 5，但是該應用程式的版本 5 僅可以在版本 4 之上安裝。如果啟用該選項，軟體先安裝版本 4，然後安裝版本 5。如果停用該選項，軟體更新應用程式失敗。

    預設情況下已啟用該選項。

5. 在**弱點**頁面，選取將由安裝所選更新修復的弱點。

- **修復所有符合其他標準的弱點**

  修復滿足在精靈中**一般標準**頁面指定標準的所有弱點。預設選取。

- **僅修復清單中的弱點**

  僅修復您手動從清單中選取的弱點。清單包含所有偵測到的弱點。

  例如，您可能想要在以下情況下選取特定弱點：要在測試環境中檢查它們的修復、要僅修復嚴重應用程式中的弱點、或者要僅修復特定應用程式中的弱點。

6. 在**名稱**頁面，指定您正在建立的規則名稱。您可以稍後在所建立工作的內容視窗的**設定**區域變更該名稱。

規則建立精靈完成操作後會建立新規則，並顯示在新工作精靈的**指定安裝更新規則**欄位中。

要為 Microsoft 應用程式更新建立規則：

1. 在新工作精靈的**設定**頁面上，點擊**新增**按鈕。

   規則建立精靈開始。遵照精靈的說明。

2. 在**規則類型**頁面上，選擇**Windows Update 的規則**。

3. 在**一般標準**頁面中，指定以下設定：

- **要安裝的更新集**

  選取必須在用戶端裝置上安裝的更新：

  - **僅安裝批准的更新**。這僅安裝批准的更新。
  - **安裝所有更新（除了拒絕的）**。這安裝帶有*已批准*或*未定義*批准狀態的更新。
  - **安裝所有更新（包含拒絕的）**。這安裝所有更新，無論什麼批准狀態。警惕選取該選項。例如，如果您想要在測試基礎架構中檢查一些被拒絕的更新的安裝，使用該選項。

- **修復弱點的時機為嚴重等級大於或等於**

  有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

  如果啟用該選項，更新僅修復 Kaspersky 設定的安全等級等於或高於清單中選定的值（**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

  如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

  預設情況下已停用該選項。

- **修復弱點的時機為 MSRC 嚴重等級大於**

  有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

  如果啟用該選項，更新僅修復 Microsoft Security Response Center (MSRC) 設定的安全等級等於或高於清單中選定的值（**低**、**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

  如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

  預設情況下已停用該選項。

4. 在**應用程式**頁面，選取您要安裝更新的應用程式和應用程式版本。預設情況下選定所有應用程式。

5. 在**更新類別**頁面，選取要安裝的更新類別。這些類別與 Microsoft Update Catalog 中的類別相同。預設情況下選定所有類別。

6. 在**名稱**頁面，指定您正在建立的規則名稱。您可以稍後在所建立工作的內容視窗的**設定**區域變更該名稱。

規則建立精靈完成操作後會建立新規則，並顯示在新工作精靈的**指定安裝更新規則**欄位中。

要為協力廠商應用程式更新建立規則：

1. 在新工作精靈的**設定**頁面上，點擊**新增**按鈕。

   規則建立精靈開始。遵照精靈的說明。

2. 在**規則類型**頁面上，選擇**協力廠商更新的規則**。

3. 在**一般標準**頁面中，指定以下設定：

- **要安裝的更新集**

  選取必須在用戶端裝置上安裝的更新：

  - **僅安裝批准的更新**。這僅安裝批准的更新。
  - **安裝所有更新（除了拒絕的）**。這安裝帶有*已批准*或*未定義*批准狀態的更新。
  - **安裝所有更新（包含拒絕的）**。這安裝所有更新，無論什麼批准狀態。警惕選取該選項。例如，如果您想要在測試基礎架構中檢查一些被拒絕的更新的安裝，使用該選項。

- **修復弱點的時機為嚴重等級大於或等於**

  有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

  如果啟用該選項，更新僅修復 Kaspersky 設定的安全等級等於或高於清單中選定的值（**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

  如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

  預設情況下已停用該選項。

4. 在**應用程式**頁面，選取您要安裝更新的應用程式和應用程式版本。預設情況下選定所有應用程式。

5. 在**名稱**頁面，指定您正在建立的規則名稱。您可以稍後在所建立工作的內容視窗的**設定**區域變更該名稱。

規則建立精靈完成操作後會建立新規則，並顯示在新工作精靈的**指定安裝更新規則**欄位中。

應用程式群組

本章節將說明如何管理裝置上安裝的應用程式群組。

建立應用程式類別

卡巴斯基安全管理中心允許建立裝置上所安裝應用程式的類別。

您可以透過以下方式建立應用程式類別：

- 管理員指定某個資料夾，所選類別中包含的可執行檔將存放在該資料夾中。
- 管理員可以指定一台裝置，包含可執行檔的程式類別。
- 管理員可設定所選類別中的應用程式，建立應用程式類別。

當建立應用程式類別時，管理員可以設定該應用程式類別的規則。定義應用程式類別中的規則。例如，您可以封鎖或允許啟動某個類別中包括的應用程式的啟動。

管理裝置上的應用程式執行

卡巴斯基安全管理中心允許您以允許名單模式管理應用程式在裝置上的啟動。詳情請參考 Kaspersky Endpoint Security for Windows Online Help。在「允許清單」模式中時，您只可以在所選裝置上啟動所選類別中包括的應用程式。管理員可以檢視已套用到每個裝置上的應用程式啟動規則的統計分析。

清查裝置上所安裝的軟體

Kaspersky Security Center 可讓您清查 Windows 與 Linux 裝置上安裝了哪些軟體。網路代理將擷取所有裝置上安裝的應用程式的資料。在清查期間擷取到的資訊將顯示在**應用程式登錄資料**資料夾的工作區中。管理員可以檢視任何應用程式的詳細資訊，包括它的版本和製造商。

從單個裝置接收的可執行檔數量不能超過 150,000。達到此限制，卡巴斯基安全管理中心無法接收任何新檔案。

管理已授權應用程式群組

卡巴斯基安全管理中心允許您建立已授權應用程式群組。管理員可設定授權應用程式群組的規則。管理員可以為授權應用程式群組指定以下標準：

- 應用程式名稱
- 應用程式版本
- 製造商
- 應用程式標籤

符合一個或多個標準的應用程式，會自動包含在同一群組。若要建立一個已授權應用程式群組，您必須設定至少一個將應用程式包括在此類群組中的標準。

每個授權的應用程式群組有其自己的產品授權金鑰。已授權應用程式群組的產品授權金鑰會定義此群組中應用程式允許安裝的最大數量。如果安裝數量已超過設定的產品授權金鑰限制，會將該事件記錄在管理伺服器。管理員可以指定產品授權金鑰的到期日。當到期日屆滿時，該事件將會記錄在管理伺服器上。

檢視關於可執行檔的資訊

卡巴斯基安全管理中心將擷取裝置上安裝作業系統以來執行過的可執行檔的相關資訊。可執行檔的資訊將顯示在**可執行檔**資料夾工作區中的應用程式主視窗。

取得並檢視儲存在用戶端裝置上的可執行檔清單

您可以透過以下方式之一獲取儲存在用戶端裝置上的可執行檔清單：

- 在 Kaspersky Endpoint Security 政策中啟用應用程式啟動通知。
- 建立清查工作。

在 Kaspersky Endpoint Security 政策中啟用應用程式啟動通知

要啟用有關應用程式啟動的通知：

1. 開啟 Kaspersky Endpoint Security 政策設定，然後轉至**一般設定 → 報告和儲存**。
2. 在**到管理伺服器的資料傳輸**設定群組中，選擇**關於啟動的應用程式**核取方塊，然後保存變更。

當使用者嘗試啟動可執行檔時，關於這些檔案的資訊將被新增到用戶端裝置上的可執行檔清單中。Kaspersky Endpoint Security 會將該資訊傳送到網路代理，然後網路代理會將其傳送到管理伺服器。

建立清查工作

清查可執行檔的功能可用於以下應用程式：

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux 版本 11.2 和以上版本
- Kaspersky Security for Virtualization 4.0 Light Agent 和更高版本

您可以在獲取已安裝應用程式的資訊時降低資料庫的負載。為了節省空間，請在安裝了標準軟體集合的參考裝置上執行清查工作。建議的裝置數量是 1-3。

當使用以下資料庫時，我們強烈不建議執行清查工作：MySQL、PostgreSQL、SQL Server Express Edition、MariaDB（所有版本）。

要在用戶端裝置上為可執行檔建立清查工作：

1. 在主控台樹狀目錄中，選取**工作**資料夾。
2. 在**工作**資料夾工作區中，點擊**新工作**按鈕。

   新工作精靈啟動。
3. 在精靈的**選取工作類型**視窗，選取**Kaspersky Endpoint Security**作為工作類型，然後選取**清查**作為工作子類型，並點擊**下一步**。
4. 遵照剩餘的精靈說明。

在新工作精靈完成後，**清單**工作隨即建立且設定。如有需要，您可變更已建立工作的設定。新建立的工作會顯示在工作清單。如有需要，您可變更已建立工作的設定。

關於清查工作的詳細說明，請參考以下說明：

- Kaspersky Endpoint Security for Windows 說明
- Kaspersky Endpoint Security for Linux 說明
- Kaspersky Security for Virtualization Light Agent

執行**清單**工作後，會形成儲存在受管理裝置的可執行檔清單，您可檢視該清單。

清查期間可偵測以下格式的可執行檔（取決於您在清查工作內容中選擇的選項）：MZ、COM、PE、NE、SYS、CMD、BAT、PS1、JS、VBS、REG、MSI、CPL、DLL、JAR 和 HTML。

檢視受管理裝置上儲存的可執行檔清單

要檢視儲存在用戶端裝置的可執行檔清單：

在主控台樹狀目錄中，轉至**進階 → 應用程式管理 → 可執行檔**。

如有必要，您可以將可執行檔從受管理裝置傳送到安裝了管理主控台的裝置。

若要傳送可執行檔：

1. 在主控台樹狀目錄中，轉至**進階 → 應用程式管理 → 可執行檔**。
2. 點擊您想要傳送到安裝了管理主控台的裝置的可執行檔連接。
3. 在開啟的視窗中，轉至**裝置**區域，然後選擇要從其傳送可執行檔的受管理裝置的核取方塊。

   在傳送可執行檔之前，請確保受管理裝置與管理伺服器有直接連線，方法是選擇**不斷開與管理伺服器的連線**核取方塊。

4. 點擊**傳送**按鈕，選擇目的資料夾，然後點擊**OK**。

所選可執行檔將被下載，以便進一步傳送到安裝有管理主控台的裝置。

使用「應用程式控制」來管理可執行檔

您可以使用「應用程式控制」元件來允許或阻止使用者裝置上可執行檔的啟動。「應用程式控制」元件支援基於 Windows 和 Linux 的作業系統。

對於基於 Linux 的作業系統，從 Kaspersky Endpoint Security 11.2 for Linux 開始可以使用應用程式控制元件。此元件也可供 Kaspersky Embedded Systems Security for Windows 3.0 或更高版本使用。

先決條件

- 系統會將卡巴斯基安全管理中心佈署在您的組織中。
- Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Linux 的政策已建立並處於使用中狀態。

階段

應用程式控制使用情境分階段進行：

1. **形成和檢視用戶端裝置上可執行檔的清單**

   此階段可提供您受管理裝置上有哪些可執行檔的資訊。檢視可執行檔清單，並將其與允許和禁止的可執行檔清單比較。對可執行檔使用的限制可能與您組織中的資訊安全政策相關。

   說明：

   - 管理主控台：可執行檔清單
   - 卡巴斯基安全管理中心網頁主控台：取得並檢視儲存在用戶端裝置的可執行檔清單

2. **為組織中使用的可執行檔建立類別**

   分析受管理裝置上儲存的可執行檔清單。基於分析為可執行檔建立類別。建議您建立涵蓋組織中使用的可執行檔標準集的「工作應用程式」類別。若不同的安全群組在其工作中使用各自的可執行檔集，則可針對各安全群組建立獨立的應用程式類別。

   說明：

   - 建立含手動新增屬性的應用程式類別、建立含所選裝置可執行檔的應用程式類別、建立含特定資料夾之可執行檔的應用程式類別。
   - 卡巴斯基安全管理中心網頁主控台：建立含手動新增內容的應用程式類別、建立含所選裝置可執行檔的應用程式類別、建立含特定資料夾之可執行檔的應用程式類別。

3. **在 Kaspersky Endpoint Security 政策設定應用程式控制**

   使用您在先前階段已建立的類別在 Kaspersky Endpoint Security 政策中設定應用程式控制元件。

   說明：

   - 管理主控台：設定應用程式在用戶端裝置上的啟動管理
   - 卡巴斯基安全管理中心網頁主控台：在 Kaspersky Endpoint Security for Windows 政策配置應用程式控制項目

4. **在測試模式中開啟應用程式控制元件**

   若要確定應用程式控制規則沒有封鎖使用者工作所需的可執行檔，建議啟用應用程式控制規則測試，並在建立新規則後分析其運作。啟用測試後，Kaspersky Endpoint Security for Windows 不會封鎖應用程式控制規則封鎖啟動的可執行檔，但會改為傳送有關其啟動的資訊至管理伺服器。

   測試應用程式控制規則時，建議執行以下動作：

   - 決定測試期間。測試期間可從數日到兩個月。
   - 檢查因應用程式控制作業產生的測試事件。

   卡巴斯基安全管理中心網頁主控台操作說明：在 Kaspersky Endpoint Security for Windows 政策中設定應用程式控制元件。遵循此指示並在組態程序中啟用**測試模式**選項。

5. **變更應用程式控制元件的類別設定**

   如有必要，請變更應用程式控制設定。根據測試結果，您可於包含手動新增內容的類別中，新增與「應用程式控制」元件事件相關的可執行檔。

   說明：

- 管理主控台：新增事件相關的可執行檔到應用程式類別
- 卡巴斯基安全管理中心網頁主控台：新增事件相關可執行檔至應用程式類別

6. **在操作模式套用應用程式控制規則**

   測試應用程式控制規則且完成類別組態後，您可在操作模式中套用應用程式控制規則。

   卡巴斯基安全管理中心網頁主控台操作說明：在 Kaspersky Endpoint Security for Windows 政策中設定應用程式控制元件。請遵循此指示，並在組態程式中停用**測試模式**選項。

7. **確認應用程式控制組態**

   請確保您已完成以下項目：

   - 為可執行檔建立類別。
   - 使用類別設定「應用程式控制」。
   - 在操作模式中套用應用程式控制規則。

結果

當情境完成時，受管理裝置上的可執行檔啟動會受到控制。使用者僅可啟動組織中允許的這些可執行檔，不可啟動被禁止的可執行檔。

如需有關應用程式控制的詳細資訊，請參閱以下說明主題：

- Kaspersky Endpoint Security for Windows 線上說明
- Kaspersky Endpoint Security for Linux 線上說明
- Kaspersky Security for Virtualization Light Agent
- Kaspersky Embedded Systems Security for Windows 說明
- Kaspersky Embedded Systems Security for Linux 說明

為 Kaspersky Endpoint Security for Windows 政策建立應用程式類別

您可以從**應用程式類別**資料夾和 Kaspersky Endpoint Security for Windows 政策的**內容**視窗為 Kaspersky Endpoint Security for Windows 政策建立應用程式類別。

*要從**應用程式類別**資料夾為 Kaspersky Endpoint Security 政策建立應用程式類別：*

1. 在主控台樹狀目錄中，選取**進階 → 應用程式管理 → 應用程式類別**。
2. 在**應用程式類別**資料夾工作區中，選擇**新類別**按鈕。

   新類別精靈啟動。

3. 在**類別類型**頁面上，選取使用者類別類型：

   - **含有手動新增內容的類別**。指定用於分配可執行檔到到所建立類別的標準。
   - **包含來自所選服務的可執行檔的類別**。指定其可執行檔將被自動分配到類別的裝置。
   - **包含來自特定資料夾的可執行檔的類別**。指定其可執行檔將被自動分配到類別的資料夾。

4. 遵照精靈的說明。

   當精靈結束時，自訂應用程式類別被建立。您可以在**應用程式類別**資料夾的工作區中，使用類別清單檢視新建立的類別。

如果要將應用程式類別匯出到 KLC 檔案，請右鍵點擊該類別的名稱，在選單中選擇**匯出** ，然後在開啟的視窗中指定檔案名稱並按一下**儲存**。

您也可以從**政策**資料夾建立應用程式類別。

*要從 Kaspersky Endpoint Security for Windows 政策的**內容**視窗建立應用程式類別：*

1. 在主控台樹狀目錄中，選取**政策**資料夾。
2. 在**政策**資料夾的工作區中，選取您要為其建立類別的 Kaspersky Endpoint Security 政策。
3. 右擊並選取**內容**。
4. 在開啟的**內容**視窗中，在左側**區域**視窗選取**安全控制 → 應用程式控制**。
5. 在**應用程式控制**區域，在**控制模式**和**操作**下拉清單選取允許清單和拒絕清單，然後點擊**新增**按鈕。
   包含類別清單的**應用程式控制規則**視窗開啟。
6. 點擊**"新增"**按鈕。
7. 輸入新政策名稱並點擊**確定**。
   新類別精靈啟動。
8. 在**類別類型**頁面上，選取使用者類別類型：

   - **含有手動新增內容的類別**。指定用於分配可執行檔到到所建立類別的標準。
   - **包含來自所選服務的可執行檔的類別**。指定其可執行檔將被自動分配到類別的裝置。
   - **包含來自特定資料夾的可執行檔的類別**。指定其可執行檔將被自動分配到類別的資料夾。

9. 遵照精靈的說明。

   當精靈結束時，自訂應用程式類別被建立。您可以在類別清單檢視新建立的類別。

應用程式類別被包含在 Kaspersky Endpoint Security for Windows 中的應用程式控制元件使用。應用程式控制允許管理員對用戶端裝置上的應用程式啟動施加限制—例如，限制某指定類別的應用程式的啟動。

建立含有手動新增內容的應用程式類別

您可指定一組準則作為可執行檔的範本，這些範本是您希望在組織中允許或封鎖的啟動範本。根據對應該準則的可執行檔，您可建立應用程式類別並在應用程式控制元件組態中加以使用。

要建立含有手動新增內容的應用程式類別：

1. 在主控台樹狀目錄中的**進階 → 應用程式管理**資料夾，選取**應用程式類別**子資料夾。
2. 點擊**新類別**按鈕。

   新類別精靈啟動。使用**下一步**按鈕進行精靈。
3. 在**類別類型**精靈頁面，選取**帶有手動新增內容的類別**作為使用者類別類型。
4. 在**輸入應用程式類別名稱**精靈頁面上，輸入新的應用程式類別名稱。
5. 在**設定在類別中納入應用程式的條件**頁面，點擊**新增**按鈕。

6. 在下拉清單，指定相關設定：

- **從可執行檔清單**

  如果選中此選項，可以使用用戶端裝置上的可執行檔清單來選取應用程式並將其新增到類別。

- **從檔案內容**

  如果選中此選項，您可以指定將要新增到自訂應用程式類別的可執行檔的詳細資料。

- **資料夾內檔案數位簽章**

  指定用戶端裝置上包含可執行檔的資料夾。包含在指定資料夾的可執行檔中的檔案內容將被傳送到管理伺服器。包含相同檔案內容的可執行檔將被新增到自訂應用程式類別。

- **資料夾內檔案的總和檢查碼**

  如果選中了此選項，您可以在用戶端裝置上選取或建立資料夾。在指定資料夾裡檔案的 MD5 雜湊將被傳送到管理伺服器。和指定資料夾裡的檔具有相同雜湊的應用程式被新增到自訂應用程式類別。

- **資料夾中的檔案憑證**

  如果選中此選項，則可以在用戶端指定包含了用憑證簽章的可執行檔的資料夾。可執行檔的憑證被讀取並新增到類別的條件中。已按照指定的憑證簽章的可執行檔將被新增到使用者類別。

- **MSI 安裝檔案的檔案內容**

  如果選中此選項，作為新增應用程式到使用者類別的一個條件，您可以指定 MSI 安裝程式的檔。應用程式安裝程式的檔案內容將被傳送到管理伺服器。與指定的 MSI 安裝程式具有相同檔案內容的應用程式被新增到自訂應用程式類別。

- **應用程式 MSI 安裝檔案的核對總和**

  如果選中此選項，作為新增應用程式到使用者類別的一個條件，您可以指定 MSI 安裝程式的檔。應用程式安裝程式的雜湊將被傳送到管理伺服器。MSI 安裝程式檔案雜湊與指定雜湊相同的應用程式被新增到使用者應用程式分類。

- **從 KL 類別**

  如果選中此選項，作為新增應用程式到使用者類別的條件，您可以為應用程式指定 Kaspersky 類別。來自指定 Kaspersky 類別的應用程式將被新增到自訂應用程式類別。

- **指定應用程式路徑（支援遮罩）**

  如果選中此選項，您可以指定包含要新增到使用者應用程式類別的可執行檔的用戶端裝置上的檔案或資料夾路徑。您可以使用正規表示式，例如*C:\path_to_exe**，例如：*C:\Program Files\Internet Explorer**。

- **從儲存區選取憑證**

  如果選中此選項，則可以指定來自儲存空間的憑證。類別條件僅符合指定憑證簽署的可執行檔。

- **磁碟機類型**

  如果選中此選項，您可以指定應用程式在其上執行的媒體類型（任意裝置或行動裝置）。在所選驅動類型上執行的應用程式被新增到使用者應用程式類別。

7. 在**建立應用程式類別**精靈頁面上，點擊**完成**按鈕。

卡巴斯基安全管理中心僅處理數位簽章檔案的中繼資料。不能基於沒有數位簽章的檔案建立類別。

當精靈完成時，使用者應用程式類別被建立，帶有手動新增的內容。您可以在**應用程式類別**資料夾的工作台使用分類清單檢視新建立的類別。

如果要將應用程式類別匯出到 KLC 檔案，請右鍵點擊該類別的名稱，在選單中選擇**匯出** ，然後在開啟的視窗中指定檔案名稱並按一下**儲存**。

建立應用程式類別以包含來自所選裝置的可執行檔

您可從選取的裝置使用可執行檔作為您希望允許或封鎖的可執行檔範本。根據選取裝置的可執行檔，您可建立應用程式類別並在應用程式控制元件組態中加以使用。

若要從裝置檢索可執行檔清單：

1. 確保 Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Linux 的政策已建立並處於使用中狀態。在政策中啟用應用程式控制元件。
2. 取得儲存在用戶端裝置上的可執行檔清單。

若要建立應用程式類別以包含來自所選裝置的可執行檔：

1. 在主控台樹狀目錄中的**進階 → 應用程式管理**資料夾，選取**應用程式類別**子資料夾。
2. 點擊**新類別**按鈕。

   新類別精靈啟動。使用**下一步**按鈕進行精靈。
3. 在**類別類型**精靈頁面，選擇**包括來自所選裝置的可執行檔的類別**作為使用者類別類型。
4. 在**輸入應用程式類別名稱**精靈頁面上，輸入新的應用程式類別名稱。
5. 在**設定**精靈頁面上，點擊**新增**按鈕。
6. 選取一部裝置，或其中的可執行檔將用來建立應用程式類別的裝置。

7. 指定下列設定：

- **雜湊值計算方法**

  取決於您網路裝置上安裝的安全應用程式版本，您必須為此類別中的檔案選取卡巴斯基安全管理中心使用的雜湊值演算法。有關由雜湊函數計算的雜湊值的資訊儲存在管理伺服器資料庫中。

  SHA256 是密碼雜湊函數：未在其演算法中找到弱點，因此是現今公認最可靠的加密功能。Kaspersky Endpoint Security 10 Service Pack 2 for Windows 和更新版本支援 SHA256 計算。計算 MD5 雜湊被所有 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 的早期版本支援。

  為該類別中的檔案選取任意卡巴斯基安全管理中心使用的雜湊值演算法選項：

  - 如果您網路上安裝的所有安全應用程式實例都是 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更高版本，請選取 **SHA-256** 核取方塊。對於 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 早期版本，我們不建議您新增根據可執行檔 SHA256 雜湊為標準建立的類別。這將導致安全應用程式操作失敗。此種情況下，您可以為類別中的檔案使用 MD5 加密演算法。

  - 如果您的網路上安裝了 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 之前的任何版本，請選取**MD5 雜湊值**。對於 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本，您無法新增基於可執行檔的 MD5 總和檢查碼的條件所建立的類別。此種情況下，您可以為類別中的檔案使用 SHA256 加密演算法。

  如果您網路上的不同裝置同時使用早期和更新版本的 Kaspersky Endpoint Security 10，請選取 **SHA-256** 核取方塊和 **MD5 雜湊值** 核取方塊。

  依預設，系統將選取**為該類別中的檔案計算 SHA256（由 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本支援）**核取方塊。

  為該類別中的檔案計算 MD5（在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 更早版本中支援）核取方塊被預設清空。

- **與管理伺服器儲存區同步資料**

  選取此選項，若您希望管理伺服器定期在指定資料夾（或資料夾）檢查變更。

  預設情況下已停用該選項。

  若您啟用此選項，請指定時段（小時）以檢查指定資料夾（或資料夾）中的變更。依預設，掃描間隔為 24 小時。

8. 在**篩選器**精靈頁面中，指定以下設定：

- **檔案類型**

  在此區段內，您可指定用來建立應用程式類別的檔案類型。

  所有檔案。所有檔案都會在建立類別時納入考量。預設情況下已選定此選項。

  僅應用程式類別之外的檔案。僅應用程式類別外的檔案會在建立類別時納入考量。

- **資料夾**

  在此區段中，您可要指定已選取裝置中要用來建立應用程式類別的資料夾。

  所有資料夾。所有資料夾都會納入建立類別的考量。預設情況下已選定此選項。

  指定資料夾。僅指定的資料夾會納入建立類別的考量。若您選取此選項，您必須指定連至資料夾的路徑。

9. 在**建立應用程式類別**精靈頁面上，點擊**完成**按鈕。

當精靈完成時，使用者應用程式類別被建立。您可以在**應用程式類別**資料夾的工作台使用分類清單檢視新建立的類別。

如果要將應用程式類別匯出到 KLC 檔案，請右鍵點擊該類別的名稱，在選單中選擇**匯出** ，然後在開啟的視窗中指定檔案名稱並按一下**儲存**。

建立應用程式類別以包含來自特定資料夾的可執行檔

您可從選取的資料夾使用可執行檔，將其作為組織中允許或封鎖的標準。以所選資料夾的可執行檔為依據，您可建立應用程式類別並在應用程式控制元件組態中加以使用。

若要建立應用程式類別以包含來自特定資料夾的可執行檔：

1. 在主控台樹狀目錄中的**進階 → 應用程式管理**資料夾，選取**應用程式類別**子資料夾。
2. 點擊**新類別**按鈕。

   新類別精靈啟動。使用**下一步**按鈕進行精靈。
3. 在**類別類型**精靈頁面，選擇**包括來自特定資料夾的可執行檔的類別**作為使用者類別類型。
4. 在**輸入應用程式類別名稱**精靈頁面上，輸入新的應用程式類別名稱。
5. 在**儲存區資料夾**精靈頁面上，點擊**瀏覽**按鈕。
6. 指定其可執行檔案將用於建立應用程式類別的資料夾。

7. 定義下列設定：

- **包含動態連結程式庫 (DLL) 到該類別**

  應用程式類別包含動態連結程式庫（DLL 格式的檔案），應用程式控制元件記錄系統中執行的此類庫的操作。包含 DLL 檔案到類別可能降低卡巴斯基安全管理中心的效能。

  預設情況下已清空此方塊。

- **包含指令碼到該類別**

  應用程式類別包含指令碼資料，指令碼不被 Web 威脅防護封鎖。包含指令碼資料到類別可能降低卡巴斯基安全管理中心的效能。

  預設情況下已清空此方塊。

- **雜湊值計算演算法**：**為該類別中的檔案計算 SHA-256（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）**

  取決於您網路裝置上安裝的安全應用程式版本，您必須為此類別中的檔案選取卡巴斯基安全管理中心使用的雜湊值演算法。有關由雜湊函數計算的雜湊值的資訊儲存在管理伺服器資料庫中。

  SHA256 是密碼雜湊函數：未在其演算法中找到弱點，因此是現今公認最可靠的加密功能。Kaspersky Endpoint Security 10 Service Pack 2 for Windows 和更新版本支援 SHA256 計算。計算 MD5 雜湊被所有 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 的早期版本支援。

  為該類別中的檔案選取任意卡巴斯基安全管理中心使用的雜湊值演算法選項：

  - 如果您網路上安裝的所有安全應用程式實例都是 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更高版本，請選取 **SHA-256** 核取方塊。對於 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 早期版本，我們不建議您新增根據可執行檔 SHA256 雜湊為標準建立的類別。這將導致安全應用程式操作失敗。此種情況下，您可以為類別中的檔案使用 MD5 加密演算法。

  - 如果您的網路上安裝了 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 之前的任何版本，請選取**MD5 雜湊值**。對於 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本，您無法新增基於可執行檔的 MD5 總和檢查碼的條件所建立的類別。此種情況下，您可以為類別中的檔案使用 SHA256 加密演算法。

  如果您網路上的不同裝置同時使用早期和更新版本的 Kaspersky Endpoint Security 10，請選取 **SHA-256** 核取方塊和 **MD5 雜湊值** 核取方塊。

  依預設，系統將選取**為該類別中的檔案計算 SHA256（由 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本支援）**核取方塊。

  為該類別中的檔案計算 MD5（在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 更早版本中支援）核取方塊被預設清空。

- **強制掃描資料夾以尋找變更**

  如果啟用此選項，應用程式會定期檢查「類別屬性新增」資料夾的任何變化。您可以在該方塊旁的輸入欄位中指定檢查頻率（小時）。預設情況下，強制檢查的時間間隔為 24 小時。

  如果停用此選項，應用程式不會強制檢查資料夾。如果檔案被修改、新增或刪除，伺服器會嘗試存取這些檔案。

  預設情況下已停用該選項。

8. 在**建立應用程式類別**精靈頁面上，點擊**完成**按鈕。

當精靈完成時，使用者應用程式類別被建立。您可以在**應用程式類別**資料夾的工作台使用分類清單檢視新建立的類別。

如果要將應用程式類別匯出到 KLC 檔案，請右鍵點擊該類別的名稱，在選單中選擇**匯出** ，然後在開啟的視窗中指定檔案名稱並按一下**儲存**。

新增事件相關的可執行檔到應用程式類別

您可以新增**應用程式啟動被禁止**和**測試模式中的應用程式啟動被禁止**事件相關的可執行檔到現有手動新增內容的應用程式類別，或新應用程式類別。

要新增應用程式控制事件相關的可執行檔到應用程式類別：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。
2. 在節點工作區中，選取**事件**頁籤。
3. 在**事件**標籤選取所需事件。
4. 在所選事件之一的上下文功能表中，選取"**新增到類別**"。

5. 在開啟的**對事件相關可執行檔所採取的操作**視窗，指定相關設定：

   您可以選取以下之一：

- **新增到新的應用程式類別**

  如果您需要建立新的應用程式類別，請選取此選項。

  點擊**確定**按鈕以開始新類別精靈。當精靈完成時，帶有指定設定的類別被建立。

  預設情況下未選定此選項。

- **新增到現有應用程式類別**

  如果您需要新增規則到現有應用程式類別則選取該選項。在應用程式類別清單中選取相關類別。

  預設情況下已選取此選項。

在**規則類型**區域，選取以下設定之一：

- **新增到類別**

  如果您需要新增規則到應用程式類別的條件則選取該選項。

  預設情況下已選取此選項。

- **新增到排除的規則**

  如果您需要新增規則到應用程式類別的排除則規則中，請選取此選項。

在**檔案資訊類型**區域，選取以下設定之一：

- **憑證詳情（或無憑證檔案的 SHA256 雜湊）**

  檔案可能使用憑證簽署。多個檔案可能使用相同的憑證簽署。例如，相同應用程式的不同版本可能使用相同的憑證簽署，或者相同供應商的多個不同應用程式可能使用相同憑證簽署。當您選取憑證時，應用程式的多個版本或相同供應商的多個應用程式可能組成一個類別。

  每個檔案都有其獨特的 SHA256 雜湊函數。當您選取 SHA256 雜湊函數時，僅一個對應的檔案（例如定義的應用程式版本）組成類別。

  如果您要在類別規則中新增可執行檔的憑證詳情（或無憑證檔案的 SHA256 雜湊），請選取此選項。

  預設情況下已選定此選項。

- **憑證詳情（無憑證檔案將被略過）**

  檔案可能使用憑證簽署。多個檔案可能使用相同的憑證簽署。例如，相同應用程式的不同版本可能使用相同的憑證簽署，或者相同供應商的多個不同應用程式可能使用相同憑證簽署。當您選取憑證時，應用程式的多個版本或相同供應商的多個應用程式可能組成一個類別。

  如果您要新增可執行檔的憑證詳情到類別規則，請選取此選項。如果可執行檔沒有憑證，該檔案將被略過。該檔案的資訊將不被新增到類別。

- **僅 SHA256（將略過無雜湊的檔案）**

每個檔案都有其獨特的 SHA256 雜湊函數。當您選取 SHA256 雜湊函數時，僅一個對應的檔案（例如定義的應用程式版本）組成類別。

如果您要僅新增可執行檔的 SHA256 雜湊函數詳情，請選取此選項。

- **僅 MD5（僅對 Kaspersky Endpoint Security 10 Service Pack 1 版本）。**

  每個檔案都有單獨的 MD5 雜湊。當您選取 MD5 雜湊時，僅一個對應的檔案，例如，定義的應用程式版本，組成類別。

  如果您要僅新增可執行檔的 MD5 雜湊詳情，請選取此選項。MD5 雜湊碼計算功能被 Kaspersky Endpoint Security 10 Service Pack 1 for Windows 和所有早期版本支援。

6. 點擊**"確定"**。

設定應用程式在用戶端裝置上的啟動管理

應用程式類別允許您最佳化在裝置上執行的應用程式的管理。您可以建立應用程式類別並為政策設定應用程式控制，因此只有指定類別的應用程式將在套用政策的裝置上啟動。例如，您建立了包含 *Application_1* 和 *Application_2* 的類別。在您新增該類別到政策後，僅兩個應用程式被允許在套用政策的裝置上啟動：*Application_1* 和 *Application_2*。如果一個使用者試圖啟動不在類別內的應用程式，例如 *Application_3*，該應用程式從啟動中被封鎖。使用者被提示 *Application_3* 被封鎖啟動，根據應用程式控制規則。您可以基於不同標準從特定資料夾建立自動新增內容類別。此種情況下，檔案被從指定資料夾自動新增到類別。應用程式可執行檔被複製到指定資料夾並被自動處理；它們的度量資料被新增到類別。

若要設定應用程式在用戶端裝置上的啟動管理，請執行以下步驟：

1. 在主控台樹狀目錄**進階 → 應用程式管理**資料夾中，選取**應用程式類別**子資料夾。

2. 在**應用程式類別**資料夾的工作台中，建立啟動應用程式時您要管理的應用程式的類別。

3. 在**受管理裝置**資料夾中的**政策**頁籤中點擊**新政策**按鈕來建立 Kaspersky Endpoint Security for Windows 的新政策，並按照安裝精靈的說明進行操作。

   如果此類政策已經存在，您可以略過此步驟。您可以透過設定應用程式啟動管理的政策，指定設定應用程式類別。新建立的政策顯示在**政策**標籤的**受管理裝置**資料夾。

4. 從 Kaspersky Endpoint Security for Windows 政策的上下文功能表中選取**內容**。

   將會開啟 Kaspersky Endpoint Security for Windows 政策的內容視窗。

5. 在 Kaspersky Endpoint Security for Windows 政策內容視窗中，在**安全控制 → 應用程式控制**區域選取**應用程式控制**核取方塊。

6. 點擊**"新增"**按鈕。

   應用程式控制規則視窗將啟動。

7. 在“**應用程式控制規則**”視窗內，在“**類別**”下拉清單中選取要套用的應用程式啟動控制規則。為所選應用程式類別配置啟動規則。

   對於 Kaspersky Endpoint Security 10 Service Pack 2 和更新版本，如果類別基於可執行檔的 MD5 雜湊而建立則不被顯示。

   對於 Kaspersky Endpoint Security 10 Service Pack 2 早期版本，我們不建議您新增根據可執行檔 SHA256 雜湊為標準建立的類別。這可能導致應用程式失敗。

   設定控制的詳細步驟提供在 Kaspersky Endpoint Security for Windows Online Help。

8. 點擊“**確定**”。

應用程式將在根據您建立的規則的指定類別的裝置上執行。新建立的規則將顯示在 Kaspersky Endpoint Security for Windows 政策內容視窗中的**應用程式控制**區域中。

檢視可執行檔的啟動規則與分析結果

要檢視關於停止使用者執行的可執行檔資訊：

1. 在主控台樹狀目錄**受管理裝置**資料夾中，選取**政策**頁籤。
2. 從 Kaspersky Endpoint Security for Windows 政策的上下文功能表中選取**內容**。

   應用程式政策的內容視窗開啟。
3. 在**區域**視窗，選取**安全控制**，然後選取**應用程式控制**子區域。
4. 點擊**靜態分析**按鈕。

   存取權限分析清單視窗開啟。在視窗左側，基於 Active Directory 資料的使用者清單被顯示。
5. 從上下文功能表選取使用者。

   視窗右側部分顯示分配給該使用者的應用程式類別。
6. 若要檢視停止使用者可執行檔，在**存取權限分析清單**視窗點擊**檢視檔案**按鈕。

   顯示禁止的可執行檔清單的視窗開啟。
7. 若要檢視某類別的可執行檔清單，請選取一個程式類別並點擊**在類別中檢視檔案**按鈕。

   這將開啟視窗顯示包含在應用程式類別中的可執行檔清單。

檢視已安裝的應用程式登錄資料

卡巴斯基安全管理中心清查所有安裝在受管理裝置上的軟體。

網路代理會將安裝在 Windows 或 Linux 裝置上的應用程式彙整成清單，然後將此清單傳送給管理伺服器。對於 Windows 用戶端裝置，網路代理從 Windows 登錄接收有關已安裝應用程式的大部分資訊。對於 Linux 用戶端裝置，套件管理工具會向網路代理提供有關已安裝應用程式的資訊。

要檢視用戶端裝置上安裝的應用程式登錄機碼，

在主控台樹狀目錄**進階** → **應用程式管理**資料夾中，選取**應用程式登錄資料**子資料夾。

應用程式登錄資料資料夾的工作區顯示安裝到用戶端裝置和管理伺服器上的應用程式清單。

您可以透過開啟其上下文功能表並選取**內容**來檢視應用程式詳情。應用程式內容視窗會開啟，其中顯示應用程式的一般資訊以及裝置上可執行檔和已安裝的應用程式清單。

在清單中任意應用程式的上下文功能表中，您可以：

- 新增該應用程式到已安裝的應用程式。
- 分配標籤給應用程式。
- 匯出應用程式清單到 CSV 檔案或 TXT 檔案。
- 檢視應用程式內容，例如，供應商名稱、版本號、可執行檔清單、安裝了該應用程式的裝置清單、可用軟體更新清單或偵測到的軟體弱點清單。

要檢視符合指定的應用程式規則，可以使用**應用程式登錄資料**資料夾的工作區中的篩選欄位。

在所選裝置的內容視窗的**應用程式登錄資料**區域中，您可以檢視安裝在裝置上的應用程式清單。

建立已安裝的應用程式報告

在**應用程式登錄資料**中，您也可以點擊**檢視已安裝的應用程式報告**按鈕產生包含已安裝的應用程式的詳細統計資訊的報告，包括安裝了每個應用程式的裝置數量。在**已安裝的應用程式報告**頁面中開啟的報告包含 Kaspersky 應用程式和協力廠商軟體的資訊。如果您僅想要安裝在用戶端裝置上的 Kaspersky 應用程式的資訊，在**概要**清單，選擇 AO Kaspersky Lab。

有關從屬和虛擬管理伺服器連線到裝置上安裝的 Kaspersky 程式和協力廠商軟體的資訊，也會收集和儲存在主管理伺服器的應用程式註冊清單中。在您從從屬和虛擬管理伺服器新增資料後，點擊**檢視已安裝的應用程式報告**按鈕，並在開啟的**已安裝的應用程式報告**頁面檢視該資訊。

要從從屬和虛擬管理伺服器新增資訊到已安裝的應用程式報告：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。
2. 在節點的工作區中，選取**報告**標籤。
3. 在**報告**頁面上，選取**已安裝的應用程式報告**。
4. 從該報告的上下文功能表中選取**內容**。
   內容：已安裝的應用程式報告 視窗隨即開啟。
5. 在**管理伺服器階層**區域中，選取**包含來自從屬和虛擬管理伺服器的資料**核取方塊。
6. 點擊**確定**。

   從屬和虛擬管理伺服器的資訊會被包含在**已安裝的應用程式報告**。

變更軟體清查開始時間

卡巴斯基安全管理中心清查所有安裝在 Windows 的受管用戶端裝置上的軟體。

網路代理編輯安裝在裝置上的應用程式清單，並把該清單傳給管理伺服器。網路代理從 Windows 登錄機碼自動接收已安裝應用程式的資訊。

要儲存裝置資源，網路代理預設在服務啟動後 10 分鐘便開始接收已安裝應用程式的資訊。

要變更網路代理服務在裝置上執行後軟體清查開始的時間：

1. 開啟安裝網路代理的裝置的系統登錄檔（例如，在本機**開始 → 執行**功能表中使用 regedit 指令）。
2. 轉至以下分支：
   - 對於 32 位元系統：
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags
   - 對於 64 位元系統：
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\NagentF
3. 對於 KLINV_INV_COLLECTOR_START_DELAY_SEC 登錄機碼，設定所需的值。
   預設值是 600 秒。
4. 重新啟動網路代理服務。

網路代理服務執行後的軟體清查開始時間已變更。

關於協力廠商應用程式的產品授權金鑰管理

卡巴斯基安全管理中心可讓您追蹤受管理裝置上已安裝協力廠商應用程式產品授權金鑰的使用情況。可以追蹤產品授權金鑰使用情況的應用程式清單來自應用程式登錄資料。對於每個產品授權金鑰，您可以指定並追蹤違反以下限制的情況：

- 可以使用此產品授權金鑰安裝應用程式的裝置數量上限
- 產品授權金鑰的到期日期

卡巴斯基安全管理中心不會檢查您是否指定了真實產品授權金鑰。您只能追蹤您指定的限制。如果違反了您對產品授權金鑰施加的限制之一，則管理伺服器將註冊一個資訊性、警告或功能失效事件。

產品授權金鑰會綁定到應用程式群組。應用程式群組是根據一或多個條件組合的一組協力廠商應用程式。您可以透過應用程式的名稱、版本、供應商和標籤來定義應用程式。如果滿足至少一個條件，則系統會將一個應用程式新增到群組中。對於每個應用程式群組，您可以綁定多個產品授權金鑰，但是每個產品授權金鑰只能綁定到一個應用程式群組。

還有一個工具可以用來追蹤產品授權金鑰的使用情況，那就是授權應用程式群組的狀態報告。此報告提供已授權應用程式群組最新狀態的資訊，包括：

- 每個應用程式群組上產品授權金鑰的安裝數量
- 使用中的產品授權金鑰數和空閒的產品授權金鑰
- 安裝在受管理裝置上已授權應用程式的詳細清單

協力廠商應用程式的產品授權金鑰管理工具位於**協力廠商產品授權使用**子資料夾（**進階 → 應用程式管理 → 協力廠商產品授權使用**）。在此子資料夾中，您可以建立應用程式群組、新增產品授權金鑰並產生已授權應用程式群組狀態的報告。

只有在**配置介面**視窗中啟用了弱點和修補程式管理選項，協力廠商應用程式的產品授權金鑰管理工具才可使用。

建立授權的應用程式群組

要建立授權的應用程式群組：

1. 在主控台樹狀目錄**進階 → 應用程式管理**資料夾中，選取**協力廠商產品授權使用**子資料夾。
2. 點擊**新增已授權應用程式群組**按鈕以執行新增已授權應用程式群組精靈。
   新增已授權應用程式群組精靈啟動。
3. 在**有關已授權應用程式群組的詳情**步驟上，指定要包括在應用程式群組中的應用程式：
   - **已授權應用程式群組的名稱**
   - **跟蹤違規限制**

     如果違反了您對應用程式群組的授權金鑰施加的限制之一，則管理伺服器將註冊一個資訊性、警告或功能失效事件：
     - 資訊性事件：**已授權應用程式群組之一的安裝即將超過限制（已經使用 95% 以上）**
     - 警告事件：**其中一個已授權應用程式群組總數即將超過最大安裝數量**
     - 功能失效事件：**其中一個已授權應用程式群組已超過最大安裝數量**
       滿足指定條件時，事件僅會註冊一次。下次事件發生時，只有在安裝數量恢復到正常水準後，該事件才能再次註冊。一個事件每小時最多只能註冊一次。
   - **將偵測到的應用程式新增至已授權應用程式群組的標準**

     指定條件以定義要包含在應用程式群組中的應用程式。您可以透過應用程式的名稱、版本、供應商和標籤來定義應用程式。您必須至少指定一個條件。如果滿足至少一個條件，則系統會將一個應用程式新增到群組中。
4. 在**輸入現存產品授權金鑰的資料**步驟，指定要追蹤的授權金鑰。選取**如果授權超過上限，功能將會被限制**選項，然後新增授權金鑰：
   a. 點擊**"新增"**按鈕。
   b. 選取您要新增的授權金鑰並點擊**確定**按鈕。如果未列出所需的授權金鑰，請點擊**新增**按鈕，然後指定授權金鑰屬性。
5. 在**新增已授權應用程式群組**步驟上，點擊**完成**按鈕。

精靈完成後會建立已授權應用程式群組並顯示在**協力廠商產品授權使用**資料夾中。

管理應用程式群組的產品授權金鑰

若要建立應用程式群組的產品授權金鑰：

1. 在主控台樹狀目錄**進階 → 應用程式管理**資料夾中，選取**協力廠商產品授權使用**子資料夾。
2. 在**協力廠商產品授權使用**資料夾的工作區中，點擊**管理已授權應用程式的產品授權金鑰**按鈕。
   已授權應用程式的產品授權金鑰管理視窗開啟。
3. 在**已授權應用程式的產品授權金鑰管理**視窗，點擊**新增**按鈕。
   產品授權金鑰視窗隨即開啟。
4. 在**產品授權金鑰**視窗中指定產品授權金鑰的內容，產品授權金鑰限制將受授權應用程式管控。
   - **名稱**。產品授權金鑰名稱。
   - **備註**。關於所選產品授權金鑰的備註。
   - **最大電腦數**。可以使用此產品授權金鑰安裝應用程式的裝置數量上限。
   - **到期**。產品授權金鑰的到期日期。

   建立的產品授權金鑰顯示在**已授權應用程式的產品授權金鑰管理**視窗中。

要套用產品授權金鑰到授權的應用程式群組：

1. 在主控台樹狀目錄**進階 → 應用程式管理**資料夾中，選取**協力廠商產品授權使用**子資料夾。
2. 在**協力廠商產品授權使用**資料夾中，選取您要套用產品授權金鑰的已授權應用程式群組。
3. 在授權應用程式群組的上下文功能表中選取**內容**。
   這將開啟授權應用程式群組的"內容"視窗。
4. 在授權應用程式群組的內容視窗中，在**產品授權金鑰**區域中選取**如果授權超過上限，功能將會被限制**。
5. 點擊"**新增**"按鈕。
   選取產品授權金鑰視窗隨即開啟。
6. 在**選取產品授權金鑰**視窗中，選取您要套用至已授權應用程式群組的產品授權金鑰。
7. 點擊"**確定**"。

   產品授權金鑰中指定的對授權應用程式群組施加的限制，將套用到所選的授權應用程式群組。

可執行檔儲存區

您可取得儲存在受管理裝置上的可執行檔清單。若要清查可執行檔，您必須建立清查工作。

清查可執行檔的功能可用於以下應用程式：

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization 4.0 Light Agent 和更高版本

從單個裝置接收的可執行檔數量不能超過 150,000。達到此限制，卡巴斯基安全管理中心無法接收任何新檔案。

在開始之前，請在 Kaspersky Endpoint Security 政策和網路代理政策中啟用有關應用程式啟動的通知，以便您可以將資料傳輸到管理伺服器。

要啟用有關應用程式啟動的通知：

- 開啟 Kaspersky Endpoint Security 政策設定並執行以下操作：
  1. 轉到**"一般設定 → 報告和儲存"**。
  2. 在**"將資料傳輸到管理伺服器"**部分，選擇**"關於已啟動的應用程式"**核取方塊。
  3. 儲存您的變更。
- 開啟網路代理政策設定並執行以下操作：
  1. 轉到**儲存區**區域。
  2. 選中**已安裝應用程式詳情**核取方塊。
  3. 儲存您的變更。

要在用戶端裝置上為可執行檔建立清查工作：

1. 在主控台樹狀目錄中，選取**工作**資料夾。
2. 在**工作**資料夾工作區中，點擊**新工作**按鈕。

   新工作精靈啟動。
3. 在精靈的**選取工作類型**視窗，選取**Kaspersky Endpoint Security**作為工作類型，然後選取**清查**作為工作子類型，並點擊**下一步**。
4. 遵照剩餘的精靈說明。

   精靈完成後，Kaspersky Endpoint Security 的清查工作已建立。新建立的工作顯示在**工作**資料夾工作區的工作清單。

清查過程中在裝置上偵測到的可執行檔清單將顯示在**可執行檔**資料夾的工作區。

清查過程中，應用程式偵測以下格式的可執行檔：MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR 和 HTML 檔案。

檢視關於可執行檔的資訊

要檢視用戶端裝置上偵測到的所有可執行檔的資訊清單，

在主控台樹狀目錄**應用程式管理**資料夾中，選取**可執行檔**子資料夾。

可執行檔資料夾工作區會顯示在裝置上執行過或者在執行 Kaspersky Endpoint Security for Windows 的掃描可執行檔工作時，偵測到的可執行檔清單。

要檢視符合指定標準的可執行檔的詳細資訊，您可以使用篩選。

要檢視可執行檔的內容，

從檔案的上下文功能表中，選取"**內容**"。

開啟選定可執行檔的內容視窗可取得此可執行檔的相關資訊，也能夠找到執行此檔案的裝置清單。

監控和報告

該部分敘述了卡巴斯基安全管理中心的監控和報告功能。這些功能給您一個基礎架構、防護狀態和統計資訊的總覽。

在卡巴斯基安全管理中心佈署之後或操作過程中，您可以配置監控和報告以適應您的需要。

- **信號燈**

  管理主控台允許您透過檢查信號燈快速評估目前卡巴斯基安全管理中心狀態和受管理裝置。

- **統計**

  防護系統和受管理裝置狀態的統計資訊顯示在可以自訂的資訊視窗中。

- **報告**

  報告功能允許您獲取您組織網路的詳細安全數字資訊、儲存該資訊到檔案、透過郵件傳送它和列印它。

- **事件**

  事件選項提供從管理伺服器資料庫中選取的事件的命名集合的螢幕視圖。這些事件集會根據以下類別分組：

  - 依嚴重等級—**緊急事件**、**功能失效**、**警告**和**資訊事件**
  - 依時間—**最近事件**
  - 依類型—**使用者請求**和**稽核事件**

您可以基於卡巴斯基安全管理中心網頁主控台介面上可以配置的設定，建立和檢視使用者定義的事件選項。

方案：監控和報告

該部分提供在卡巴斯基安全管理中心中配置監控和報告功能的方案。

先決條件

在組織網路中佈署卡巴斯基安全管理中心後，您可開始監控此程式並對其功能運作產生報告。

階段

組織網路中的監控和報告分步驟進行：

1. **設定裝置狀態轉換**

   根據特定條件，熟悉定義指派裝置狀態的設定。透過變更這些設定，您可以變更帶有*緊急*或*警告*嚴重等級的事件數量。

   在設定裝置狀態的切換時，請確認新設定與組織的資訊安全政策未衝突，並且您能夠及時對組織網路中的重要安全事件做出反應。

2. **配置用戶端裝置上的事件通知**

   根據組織的需求，設定用戶端裝置上的事件通知（透過郵件、簡訊或執行可執行檔）。

3. **變更安全網路對病毒爆發事件的回應**

   要調整網路對新事件的回應，您可以在管理伺服器屬性中變更特定的閾值。您也可以建立要啟動的更嚴格政策，或者建立要在事件發生時執行的工作。

4. **管理統計資訊**

   根據組織的需求設定統計資訊的顯示方式。

5. **檢視您組織網路的安全狀態**

   要查看組織網路的安全狀態，可以執行以下任一操作：

   - 在工作區中的**管理伺服器**節點上的**統計**標籤，開啟**防護狀態**第二層標籤（頁面），然後查看**即時防護狀態**資訊視窗
   - 產生並檢閱**防護狀態報告**
   - 產生並檢閱**錯誤報告**

6. **定位不被防護的用戶端裝置**

   要找到不受保護的用戶端裝置，請前往**管理伺服器**節點上的**統計**標籤，開啟**防護狀態**第二層標籤（頁面），然後查看**網路中新裝置的偵測記錄**資訊視窗。您也可以產生並檢閱**防護佈署報告**。

7. **檢查用戶端裝置防護**

   要檢查用戶端裝置的防護情況，請前往**管理伺服器**節點上的**統計**標籤，開啟**佈署** 或者**威脅統計資料**第二層標籤（頁面），然後查看相關的資訊視窗。您也可以啟動並檢閱**緊急事件**事件分類。

8. **評估和限制資料庫上的事件負載**

受管應用程式操作相關的事件資訊將被從用戶端電腦上傳輸並記錄至管理伺服器資料庫。要降低管理伺服器負載，評估和限制可以儲存在資料庫的最大事件數量。

要評估資料庫上的事件負載，請計算資料庫空間。您也可以限制最大事件數以避免資料庫溢出。

9. **檢視產品授權資訊**

要查看產品授權資訊，請前往**管理伺服器**節點上的**統計**標籤，開啟**佈署** 第二層標籤（頁面），然後查看**產品授權金鑰使用**資訊視窗。您也可以產生並檢閱**產品授權金鑰使用報告**。

結果

完成方案後，您被通知您組織網路的防護，因此可以為進一步防護排程操作。

在管理控制台中監控交通信號燈和記錄的事件

管理主控台允許您透過檢查信號燈快速評估目前卡巴斯基安全管理中心狀態和受管理裝置。信號燈會顯示在**管理伺服器**節點的工作區，此工作區位於**監控**標籤上。頁籤提供了帶有信號燈的六個資訊面板。信號燈是面板左側的彩色欄。每個帶有信號燈的面板對應於卡巴斯基安全管理中心的特定功能範圍（參見下表）。

管理主控台中信號燈覆蓋的範圍

面板名稱	信號燈範圍
佈署	在組織網路裝置上安裝網路代理和安全應用程式
管理方案	管理群組結構。網路掃描。裝置移動規則
防護設定	安全應用程式功能：防護狀態、惡意軟體掃描
更新	更新和修補程式
監控	防護狀態
管理伺服器	管理伺服器功能和屬性

每個信號燈可以變換四種顏色（參見下表）。信號燈的顏色取決於卡巴斯基安全管理中心的目前狀態和記錄的事件。

信號燈的顏色碼

狀態	信號燈顏色	信號燈顏色意義
資訊	綠色	不需要管理員介入。
警告	黃色	需要管理員介入。
緊急	紅色	發生了嚴重問題。需要管理員介入以解決。
資訊	淡藍色	與受管理裝置的潛在或實際威脅無關的事件被記錄。

管理員的目標是，保持**監控**標籤上所有資訊視窗的信號燈都是綠燈。

資訊面板還顯示影響紅綠燈和 Kaspersky Security Center 狀態的記錄事件（見下表）。

信號燈顏色	事件類型顯示名稱	事件類型	敘述
紅色	**%1 台裝置上的產品授權已到期**	IDS_AK_STATUS_LIC_EXPAIRED	當商業授權到期時，會發生此類事件。 卡巴斯基安全管理中心每天會檢查一次產品授權是否接近到期日。 當商業授權到期時，卡巴斯基安全管理中心僅提供基本功能。 要繼續使用卡巴斯基安全管理中心，您必須續約您的正式產品授權。
紅色	**安全應用程式沒有執行：%1 台裝置**	IDS_AK_STATUS_AV_NOT_RUNNING	當安裝在裝置上的安全應用程式未運行時，會發生此類事件。 確保 Kaspersky Endpoint Security 正在裝置上運行。
紅色	**已停用防護：%1 台裝置**	IDS_AK_STATUS_RTP_NOT_RUNNING	當裝置上的安全應用程式被停用的時間比指定時間間隔，會發生此類事件。 檢查即時防護現狀在裝置上並確保啟用了您需要的所有保護組件。
紅色	**在裝置上偵測到軟體弱點**	IDS_AK_STATUS_VULNERABILITIES_FOUND	當*查找漏洞和所需的更新*工作在裝置上安裝的應用程式偵測到具有指定嚴重級別的漏洞，會發生此類事件。 管理員可在**Application management**資料夾包含的**Software updates**子資料夾中檢視可用更新的清單。該資料夾包含了管理伺服器擷取的可以被發佈到裝置的 Microsoft 應用程式和其他軟體廠商產品的更新清單。 查看有關可用更新的資訊後，在裝置上安裝更新。
紅色	**管理伺服器上註冊了緊急事件**	IDS_AK_STATUS_EVENTS_OCCURED	當偵測到管理伺服器緊急事件，會發生此類事件。 檢查儲存在管理伺服器上的事件列表，然後將緊急事件一一修復。
紅色	**管理伺服器上記錄了錯誤事件**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	當在管理伺服器端記錄意外錯誤時，會發生此類事件。 檢查儲存在管理伺服器上的事件列表，然後一一修復錯誤。
紅色	**失去與 %1 台裝置的連線**	IDS_AK_STATUS_ADM_LOST_CONTROL1	當管理伺服器和裝置之間的連接遺失時，會發生此類事件。 查看斷開連接的裝置列表並嘗試重新連接它們。
紅色	**%1 台裝置已長時間未連線到管理伺服器**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	當由於裝置關閉，裝置在指定時間間隔內未連線到管理伺服器，會發生此類事件。 確保裝置已打開並且網路代理正在運行。
紅色	**有 %1 台裝置的狀態異常**	IDS_AK_STATUS_HOST_NOT_OK	當連接到管理伺服器的裝置 *OK* 狀態變更為*緊急*或者*警告*，會發生此類事件。 您可以使用以下方法解決問題 Kaspersky Security Center 遠程診斷實用程序。
紅色	**資料庫過期： %1 台裝置**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	當裝置上的防毒資料庫未在指定時間間隔內更新時，會發生此類事件。 按照說明進行操作更新卡巴斯基資料庫。

信號燈顏色	事件類型顯示名稱	事件類型	敘述
紅色	**Windows Update 更新檢查長時間沒有執行的裝置：%1**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	當「*執行 Windows 更新同步*」工作在指定時間間隔內未執行，會發生此類事件。 按照說明進行操作 將來自 Windows Update 的更新與管理伺服器同步。
紅色	**卡巴斯基安全管理中心的 %1 個外掛程式必須安裝**	IDS_AK_STATUS_PLUGINS_REQUIRED2	當您需要為 Kaspersky應用程式安裝附加外掛程式時，會發生此類事件。 下載並安裝卡巴斯基應用程式所需的管理外掛程式 卡巴斯基技術支援網頁。
紅色	**在 %1 台裝置上偵測到活動威脅。**	IDS_AK_STATUS_NONCURED_FOUND	當在受管理裝置上偵測到活動威脅時，就會發生此類事件。 檢視有關偵測到的威脅的資訊，然後按照建議進行操作。
紅色	**工作 %1 已完成但存在錯誤**	IDS_AK_STATUS_TASK_FAILED	當工作執行完成但出現錯誤時，會發生此類事件。 檢查工作的屬性，然後重新配置工作。
紅色	**偵測到大量病毒：%1 台裝置**	IDS_AK_STATUS_TOO_MANY_THREATS	當在受管理裝置上偵測到病毒時，就會發生此類事件。 檢視有關偵測到的病毒的資訊，然後按照建議進行操作。
紅色	**病毒爆發**	IDS_AK_STATUS_VIRUS_OUTBREAK	當短時間內在若干受管理裝置上偵測到的惡意物件數量超過上限值時，該類型的事件發生。 檢視有關偵測到的威脅的資訊，然後按照建議進行操作。
紅色	**儲存區中的資料庫已長時間未更新**	IDS_AK_STATUS_UPD_SERVER_NOT_UPTODATE	當裝置上的防毒資料庫兩天未更新時，會發生此類事件。 檢查防毒資料庫的更新頻率，然後更新防毒資料庫。
黃色	**儲存區中的資料庫已長時間未更新**	IDS_AK_STATUS_UPD_SERVER_NOT_UPTODATE	當裝置上的防毒資料庫超過一天但少於兩天未更新時，就會發生此類事件。 檢查防毒資料庫的更新頻率，然後更新防毒資料庫。
黃色	**裝置上偵測到 NetBIOS 名稱衝突**	IDS_AK_STATUS_ADM_NAME_CONFLICT	當裝置具有相同的 NetBIOS 名稱時，就會發生此類事件。 重命名裝置。
黃色	**在 %s 台裝置上，資料加密已轉換到裝置狀態偵測標準中指定的狀態**	IDS_AK_STATUS_ENCRYPTION_FAULTS_FOUND	當在受管理裝置上資料加密失敗時，就會發生此類事件。
黃色	**產品授權 %1 還有 %2 天到期**	IDS_AK_STATUS_LIC_EXPAIRING	當裝置上的產品授權在指定天數內到期時，就會發生此類事件。 要繼續使用卡巴斯基安全管理中心，您必須續約您的正式產品授權。
黃色	**安裝了網路代理的未配置的裝置：%1**	IDS_AK_STATUS_NAGENTS_IN_UNASSIGNED	當網路上發現新裝置時，就會發生此類事件。 將具有網路代理程式的裝置移至受管理裝置群組。
黃色	**重新啟動之前，%1 裝置上的網路代理無法執行。上一次，此狀態為 %2**	IDS_AK_STATUS_NAGENTS_NOT_RUNNING_UNTIL_REBOOT	當網路代理未在裝置上執行時，會發生此類事件。 重新啟動裝置。

信號燈顏色	事件類型顯示名稱	事件類型	敘述
黃色	**偵測到的檔案必須傳送至 Kaspersky 以供進一步分析**	IDS_AK_STATUS_NEW_APS_FILE_APPEARED	當偵測到可能感染病毒的檔案並將其移至隔離區時，就會發生此類事件。 將檔案傳送給卡巴斯基進行進一步分析。
黃色	**受管理裝置：%1。安全應用程式安裝在：%2 台裝置**	IDS_AK_STATUS_NO_AV	當 Kaspersky Endpoint Security 未安裝在所有受管理裝置上時，會發生此類事件。 在所有受管理裝置上安裝 Kaspersky Endpoint Security。
黃色	**安裝工作 %1 已在 %2 台裝置上成功完成；%3 台裝置需要重新啟動**	IDS_AK_STATUS_RI_NEED_REBOOT	當 Kaspersky Endpoint Security 剛安裝在受管理裝置上時，會發生此類事件。 安裝 Kaspersky Endpoint Security 後重新啟動裝置。
黃色	**惡意軟體掃描已長時間未執行：%1 台裝置**	IDS_AK_STATUS_SCAN_LATE	當您需要在受管理裝置上執行惡意軟體掃描時，會發生此類事件。 執行病毒掃描。
黃色	**偵測到軟體弱點的裝置：%1**	IDS_AK_STATUS_VULNERABLE_HOSTS_FOUND	當在受管理裝置上偵測到弱點時，就會發生此類事件。 檢視有關偵測到的弱點的資訊並修復它們。
綠色	**受管理裝置：%3。偵測到未分配的裝置：%1**	IDS_AK_STATUS_ADM_OK1	當在管理群組中偵測到新裝置時，會發生此類事件。
綠色	**安全應用程式被安裝在所有受管理的裝置**	IDS_AK_STATUS_DEPLOYMENT_OK	當 Kaspersky Endpoint Security 安裝在所有受管理裝置上時，會發生此類事件。
綠色	**卡巴斯基安全管理中心正在正常執行**	IDS_AK_STATUS_GENERAL_OK	當卡巴斯基安全管理中心正常運作時，會發生此類事件。
綠色	**沒有安裝即時防護程式**	IDS_AK_STATUS_RTP_NA	當受管理裝置上未安裝病毒防護應用程式時，會發生此類事件。
綠色	**防護已啟用**	IDS_AK_STATUS_RTP_OK	當在受管理裝置上啟用即時防護時，會發生此類事件。
綠色	**安全應用程式未安裝**	IDS_AK_STATUS_SCAN_NA	當受管理裝置上未安裝病毒防護應用程式時，會發生此類事件。
綠色	**惡意軟體掃描正依照排程執行**	IDS_AK_STATUS_SCAN_OK	當*惡意軟體掃描*工作按排程執行時，會發生此類事件。
綠色	**上次更新更新儲存區的時間：%1**	IDS_AK_STATUS_UPD_OK	更新儲存庫進行更新時會發生此類事件。
淡藍色	**儲存區中的資料庫已長時間未更新**	IDS_AK_STATUS_UPD_SERVER_NOT_UPTODATE	當防毒資料庫在白天更新時，就會發生此類事件。
淡藍色	**接受的卡巴斯基安全網路聲明已過時**	IDS_AK_STATUS_ACCEPTED_KSN_AGREEMENT_OBSOLETE	當卡巴斯基安全網路聲明過期時，就會發生此類事件。
淡藍色	**卡巴斯基軟體更新尚未得到批准**	IDS_AK_STATUS_APPLICABLE_KL_PATCHES_NOT_APPROVED	當管理員尚未批准受管理卡巴斯基應用程式的適用修補程式時，就會發生此類事件。
淡藍色	**Kaspersky 應用程式更新已被取消**	IDS_AK_STATUS_APPLICABLE_KL_PATCHES_REVOKED	當管理員尚未拒絕已撤銷的修補程式時，就會發生此類事件。
淡藍色	**Kaspersky 行動軟體的最終使用者產品授權協議未被接受**	IDS_AK_STATUS_KL_MOBILE_EULAS_NOT_ACCEPTED	當管理員尚未接受卡巴斯基行動軟體的最終使用者產品授權協議時，就會發生此類事件。

信號燈顏色	事件類型顯示名稱	事件類型	敘述
淡藍色	**Kaspersky 軟體更新的最終使用者產品授權協議未被接受**	IDS_AK_STATUS_KL_PATCHES_EULAS_NOT_ACCEPTED	當管理員尚未接受卡巴斯基軟體更新的最終使用者產品授權協議時，就會發生此類事件。
淡藍色	**關於卡巴斯基軟體更新的卡巴斯基安全網路聲明尚未被接受**	IDS_AK_STATUS_KL_PATCHES_KSN_AGREEMENTS_NOT_ACCEPTED	當管理員尚未接受卡巴斯基軟體更新的卡巴斯基安全網路聲明時，就會發生此類事件。
淡藍色	**您必須接受產品授權協議以安裝更新**	IDS_AK_STATUS_NEED_ACCEPT_EULA	當有新的更新可供安裝但管理員尚未接受產品授權協議時，會發生此類事件。
淡藍色	**Kaspersky 應用程式的新版本已可用**	IDS_AK_STATUS_NEW_DISTRIBUTIVES_AVAILABLE	當新版本的卡巴斯基應用程式可在受管理裝置上安裝時，就會發生此類事件。
淡藍色	**有卡巴斯基安全管理中心元件更新可用**	IDS_AK_STATUS_NEW_KSC_VERSIONS_AVAILABLE	當卡巴斯基安全管理中心元件有可用更新時，會發生此類事件。
淡藍色	**有 Kaspersky 應用程式更新可用**	IDS_AK_STATUS_NEW_VERSIONS_AVAILABLE	當卡巴斯基應用程式有可用更新時，就會發生此類事件。
淡藍色	**應用程式安裝工作 %1 已在 %2 台裝置上成功完成，在 %3 台裝置上失敗**	IDS_AK_STATUS_RI_FAILED	當*應用程式安裝*工作僅在指定集區中的某些裝置上安裝軟體時，會發生此類事件。
淡藍色	**執行佈署工作 - %1 (%2%%)**	IDS_AK_STATUS_RI_RUNNING	當部署工作在受管理裝置上執行時，會發生此類事件。
淡藍色	**在 %1 台裝置上從未執行過完整掃描**	IDS_AK_STATUS_SCAN_NOT_SCANNED	當從未對指定數量的裝置執行完整掃描時，會發生此類事件。
淡藍色	**正在執行更新下載工作（進度：%1%%）**	IDS_AK_STATUS_UPD_SRV_UPDATE_IN_PROGRESS	當下載更新工作在受管理裝置上執行時，會發生此類事件。

使用報告、統計和通知

本章節將介紹如何使用卡巴斯基安全管理中心中的報告和統計，以及如何設定管理伺服器通知。

搭配報告一起使用

卡巴斯基安全管理中心的報告包含受管理裝置狀態的資訊。報告根據管理伺服器上儲存的資訊產生。您可以為以下類型的物件建立報告：

- 為根據指定設定建立的裝置分類。
- 為管理群組。
- 為不同管理群組的特定裝置。
- 為網路中所有裝置（可用於防護佈署報告）。

程式有標準報告範本分類。也可以建立自訂報告範本。報告將顯示在應用程式主視窗，主控台樹狀目錄的"**管理伺服器**"節點。

建立報告範本

要建立報告範本，請執行以下操作：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。
2. 在節點的工作區中，選取**報告**標籤。
3. 點擊**新增報告範本**按鈕。

   程式將啟動“新報告範本精靈”。遵照精靈的說明。

當精靈完成後，新建的報告範本將被新增至主控台樹狀目錄的**管理伺服器**資料夾中。您可以建立和瀏覽此範本的報告。

檢視和編輯報告範本內容

您可以檢視和編輯報告範本的基本內容，例如，報告範本名稱或顯示在報告中的欄位。

要檢視和編輯報告範本內容：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。
2. 在節點的工作區中，選取**報告**標籤。
3. 在報告範本清單，選取所需報告範本。

4. 在所選報告範本的上下文功能表中選取**內容**.。

   另外，您可以先生成報告，然後點擊**開啟報告範本內容**按鈕或**設定報告欄位**按鈕。

5. 在開啟的視窗中，編輯報告範本內容。每個報告的內容可能僅包含若干以下敘述的部分。

   - **一般**區域：

     - 報告範本名稱

     - **顯示項目的最大數量**

       如果啟用該選項，顯示在表格中的帶有詳細報告資料的項目數量不會超過指定值。

       報告項目首先根據指定在報告範本內容的**欄位 → 詳細資料欄位**區域的規則被儲存，然後僅第一個結果項目被儲存。帶有詳細報告資料的表頭展示顯示的項目數量和比對其他報告範本設定的可用項目總數。

       如果停用該選項，帶有詳細報告資料的表顯示所有可用項目。我們不建議您停用該選項。限制顯示的報告項目數量會降低資料庫管理系統 (DBMS) 負載，也會降低產生和匯出報告所需的時間。一些報告包含太多項目。如果是這樣，您可能難於閱讀和分析所有。而且，您的裝置可能在產生此報告時記憶體不夠，進而您將無法檢視報告。

       預設情況下已啟用該選項。預設值是 1000。

     - **列印版本**

       報告輸出被最佳化以用於列印：在一些值之間被新增空格以方便閱讀。

       預設情況下已啟用該選項。

   - **欄位**區域。

     選取在報告中要顯示的欄位，和欄位順序，並設定報告資訊是否被儲存和按照欄位篩選。

   - **時間間隔**區域。

     修改報告間隔。有以下可用值：

     - 在兩個指定日期之間

     - 從指定日期到報告建立日期

     - 從報告建立日期減去指定天數

   - **群組**、**裝置分類**或**裝置**區域。

     變更建立報告的用戶端裝置集。僅其中一個區域可能被展示，取決於報告範本建立過程中指定的設定。

   - **設定**部分。

     變更報告設定。精確設定集合取決於特定報告。

   - **安全性**區域。**從管理伺服器繼承設定**

如果啟用該選項，報告的安全設定從管理伺服器繼承。

如果停用該選項，您可以配置報告的安全設定。您可以分配角色到使用者或使用者群組或分配權限到使用者或使用者群組，如報告中所套用。

預設情況下已啟用該選項。

若在介面設定視窗中選取**顯示安全設定區域**核取方塊，則可使用**安全性**區域。

- **管理伺服器階層** 區域：
  - **包含來自從屬和虛擬管理伺服器的資料**

    如果啟用該選項，報告包含屬於建立範本的管理伺服器的從屬和虛擬管理伺服器的資訊。

    如果您要僅從目前管理伺服器檢視資料，停用該選項。

    預設情況下已啟用該選項。

  - **嵌套等級**

    報告包含位於目前管理伺服器下小於或等於指定巢狀等級的從屬和虛擬管理伺服器的資料。

    預設值是1。如果您必須從樹中位於低等級的從屬管理伺服器接收資訊，您可能要變更該值。

  - **資料等待間隔（分鐘）**

    在產生報告之前，建立報告範本的管理伺服器等待從屬管理伺服器的資料指定分鐘數。如果在該時間段後未從從屬管理伺服器接收到資料，報告依然執行。除了實際資料，報告也顯示從快取接收的資料（如果**從屬管理伺服器的記憶體暫存資料**選項被啟用）或 **N/A**（不可用）。

    預設值是 5 分鐘。

  - **從屬管理伺服器的快取資料**

    從屬管理伺服器定期傳輸資料到建立報告範本的管理伺服器。傳輸的資料儲存在快取。

    如果在產生報告時目前管理伺服器無法從從屬管理伺服器接收資料，報告顯示從快取接收的資料。資料傳輸到快取的日期也被顯示。

    啟用該選項允許您檢視從屬管理伺服器資訊，即便即時資料無法被獲取。然而，所顯示資料可能過期。

    預設情況下已停用該選項。

  - **記憶體緩衝區更新頻率（小時）**

    從屬管理伺服器會在一定間隔時間傳輸資料到建立報告範本的管理伺服器。您可以以小時為單位指定此期間。如果指定值是 0 小時，資料僅會在產生報告時被傳輸。

    預設值是 0。

  - **從從屬管理伺服器傳輸詳細資訊**

在產生的報告中，帶有詳細報告資料的表格包含建立報告範本的管理伺服器的從屬管理伺服器的資料。

啟用該選項會減慢報告產生並增加管理伺服器之間的流量。然而，您可以在一個報告中檢視所有資料。

除了啟用該選項，您可能想分析詳細報告資料以偵測故障從屬管理伺服器，然後僅為該故障管理伺服器產生相同報告。

預設情況下已停用該選項。

報告範本中的延伸篩選格式

In Kaspersky Security Center 14.2, you can apply the extended filter format to a report template.延伸篩選格式會比預設是提供更多彈性。您可使用一組篩選建立複雜的篩選條件，這將會在報告建立期間根據 OR 邏輯運算子套用至報告，如下所示：

Filter[1](Field[1] AND Field[2]...AND Field[n]) OR Filter[2](Field[1] AND Field[2]...AND Field[n]) OR...Filter[n](Field[1] AND Field[2]...AND Field[n])

此外，透過延伸篩選格式，您可在篩選中對特定欄位以相對時間格式中設定時間間隔（例如，使用「針對前 N 天」條件）。以報告範本類型為依據的時間間隔條件設定與可得性。

轉換篩選至延伸格式

報告範本的延伸篩選格式僅在卡巴斯基安全管理中心 12 與更新版本中受到支援。將預設篩選轉換至延伸格式後，報告範本會無法與網路中安裝先前版本卡巴斯基安全管理中心的管理伺服器相容。從這些管理伺服器傳來的資訊將無法供報告使用。

若要轉換報告範本預設篩選至延伸格式：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。
2. 在節點的工作區中，選取**報告**標籤。
3. 在報告範本清單，選取所需報告範本。
4. 在所選報告範本的上下文功能表中選取**內容**.。
5. 在開啟的"工作內容"視窗中，選取**欄位**區域。
6. 在**詳細資料欄位**頁籤點擊**轉換篩選**連結。
7. 在開啟的視窗中，點擊**確定**按鈕。

   報告範本的延伸篩選格式轉換一經套用後即無法還原。若您意外點擊**轉換篩選**，您可點擊報告範本內容視窗的**取消**按鈕來取消變更。

8. 若要套用變更，請點擊**確定**按鈕以關閉報告範本內容視窗。

   報告範本內容視窗再次開啟時，會顯示新的可用**篩選器**區域。在此區域，您可設定延伸的篩選。

設定延伸的篩選

若要在報告範本內容中設定延伸篩選：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。
2. 在節點的工作區中，選取**報告**標籤。
3. 在報告範本清單中，選取先前轉換為延伸篩選格式的報告範本。
4. 在所選報告範本的上下文功能表中選取**內容**.。
5. 在開啟的「屬性」視窗中，選取**篩選器**區段。

   若報告範本先前未轉換至延伸篩選格式，則不會顯示**篩選器**區域。

   在報告範本內容視窗的**篩選器**區域，您可檢閱並修改套用至報告的篩選清單。清單中的各個篩選都有獨立名稱，且代表報告中對應欄位的一組篩選。
6. 以下列方式之一開啟篩選設定視窗：
   - 若要建立新篩選，請點擊**新增**按鈕。
   - 若要修改現有篩選，請選取必要篩選並點擊**修改**按鈕。
7. 在開啟的視窗中，選取並指定篩選必要欄位的值。
8. 點擊**確定**按鈕以儲存變更並關閉視窗。

   若要建立新篩選，您必須先在**篩選名稱**欄位中指定篩選名稱再點擊**確定**按鈕。
9. 點擊**確定**按鈕以關閉報告範本內容視窗。

   系統會設定報告範本中的延伸篩選。現在您可使用此報告範本建立報告。

建立和瀏覽報告

要建立和瀏覽報告，請執行以下操作：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。
2. 在節點的工作區中，選取**報告**標籤。
3. 在報告範本清單中，點兩下您需要的報告範本。

   所選範本的報告被顯示。

此報告將顯示下列資料：

- 報告名稱和類型、簡要說明和報告時間區段，以及該報告為哪個裝置群組產生的相關資訊。
- 圖表顯示最有代表性的報告資料。
- 帶有計算好的報告指示器的加固表格。
- 帶有詳細報告資料的表格。

儲存報告

要儲存產生的報告，請執行以下操作：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。
2. 在節點的工作區中，選取**報告**標籤。
3. 在報告範本清單中，選取您需要的報告範本。
4. 在所選報告範本的上下文功能表中選取**儲存**。

   程式將啟動報告儲存精靈。遵照精靈的說明。

精靈結束後，程式將開啟您儲存報告文件的節點。

當您將報告作為 XLS 檔案儲存時，所有相關映像（例如標誌和資料包）都會被儲存為單獨的檔案。

建立報告傳送工作

報告可以被傳送。卡巴斯基安全管理中心中的報告傳送由提供報告工作完成。

要建立單個報告傳送工作，請執行以下操作：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。
2. 在節點的工作區中，選取**報告**標籤。
3. 在報告範本清單中，選取您需要的報告範本。
4. 在所選報告範本的上下文功能表中選取**傳送報告**。

   報告傳送工作建立精靈啟動。遵照精靈的說明。

要建立多個報告的傳送工作，請執行以下操作：

1. 在主控台樹狀目錄的必要管理伺服器名稱節點下，選取**工作**資料夾。
2. 在**工作**資料夾工作區中，選擇**建立工作**按鈕。

   新工作精靈啟動。遵照精靈的說明。

   新建立的報告傳送工作會顯示在主控台樹狀目錄的**工作**資料夾。

如果在卡巴斯基安全管理中心安裝期間指定了電子郵件設定，程式將會自動建立傳送報告工作。

步驟 1：選取工作類型

在**選取工作類型**視窗的工作清單中，選取**傳送報告**作為工作類型。

點擊**下一步**以繼續到下一步。

步驟 2：選取報告類型

在**選取報告類型**視窗的工作建立範本清單，選取報告類型。

點擊**下一步**以繼續到下一步。

步驟 3：對報告的操作

在**套用到報告的操作**視窗中，指定以下設定：

- **透過郵件傳送報告**

  如果啟用此選項，應用程式會用郵件傳送建立的報告。

  您可以點擊**"郵件通知設定"**連結，設定透過電子郵件傳送的報告。如果啟用此選項，則該連結可用。

  如果停用此選項，應用程式會將報告儲存到指定資料夾。

  預設情況下已停用該選項。

- **儲存報告到共用資料夾**

  如果啟用此選項，應用程式會儲存報告到此方塊下指定的資料夾。要儲存報告到共用資料夾，指定資料夾的 UNC 路徑。此種情況下，在**選取要執行此工作的帳戶**視窗，您必須指定使用者帳戶和密碼以存取該資料夾。

  如果停用此選項，應用程式不會儲存報告到資料夾，而是用郵件傳送。

  預設情況下已停用該選項。

- **覆蓋相同類型的舊報告**

  如果啟用此選項，每次工作啟動時的新報告檔案，會覆蓋之前工作啟動時儲存在報告資料夾中的檔案。

  如果停用此選項，則將不會覆蓋報告檔案。每次工作啟動時，新的報告檔案都將儲存在報告資料夾中。

  如果選取**儲存報告到資料夾**，則會顯示該核取方塊。

  預設情況下已停用該選項。

- **指定帳戶以存取共用資料夾**

  如果啟用此選項，您可以指定儲存報告到資料夾的帳戶。如果共用資料夾的 UNC 路徑被指定為**套用到報告的操作**視窗的**儲存報告到資料夾**設定，您必須指定使用者帳戶和密碼以存取該資料夾。

  如果停用此選項，報告被儲存在管理員的資料夾。

  如果選取**儲存報告到資料夾**，則會顯示該核取方塊。

  預設情況下已停用該選項。

當您將報告作為 XLS 檔案儲存或者傳送時，所有相關映像（例如標誌和資料包）都會被儲存為單獨的檔案。

點擊**下一步**以繼續到下一步。

步驟 4：選取帳戶以移動工作

在**選取要執行此工作的帳戶**視窗，您可以指定在執行工作時使用哪些帳戶。您可以選取以下其中一個方法：

- **預設帳戶**

  在與執行該工作的應用程式相同的帳戶下執行該工作。
  預設情況下已選定此選項。

- **指定帳戶**

  填寫**帳戶**與**密碼**欄位以指定工作要在其下執行的帳戶詳情。帳戶必須對此工作有足夠的權限。

  - **帳戶**

    執行該工作的帳戶。

  - **密碼**

    工作執行時使用的帳戶的密碼。

點擊**下一步**以繼續到下一步。

步驟 5：設定工作排程

在**設定工作排程**精靈頁面，您可以為工作啟動建立排程。如果必要，定義以下設定：

- **排程開始：**

  選取工作執行排程並設定所選排程。

  - **每 N 小時**

    工作定期執行，按照指定小時數間隔，從指定的日期和時間開始。

    預設下，工作每 6 小時執行一次，從目前系統日期和時間開始。

  - **每 N 天**

    工作定期執行，按照指定天數間隔。此外，您可指定第一個工作執行的日期與時間。這些額外選項會在您建立的工作受到應用程式支援時可用。

    預設下，工作每天執行一次，從目前系統日期和時間開始。

  - **每 N 星期**

    工作定期執行，按照指定星期數間隔，從指定的星期和時間開始。

    預設下，工作每星期一於目前系統時間執行一次。

  - **每 N 分鐘**

    工作定期執行，按照指定分鐘數間隔，從工作建立日期的指定時間開始。

    預設下，工作每 30 分鐘執行一次，從目前系統時間開始。

  - **每天（不支援日光節約時間）**

    工作定期執行，按照指定天數間隔。排程不支援日光節約時間 (DST)。這意味著在夏令時開始和結束時當時鐘向前或向後撥動一小時時，實際工作啟動時間不變更。

    我們不建議您使用該排程。它用於向後相容卡巴斯基安全管理中心。

    預設下，工作每天於目前系統時間執行一次。

  - **每週**

    工作每週在指定星期和指定時間執行。

  - **按每星期中的指定日**

    工作定期執行，在每周指定日期的指定時間。

    預設下，工作每週五 6:00:00 P.M. 執行。

  - **每月**

工作定期執行，在指定月日的指定時間。

在缺少指定日的月份，工作在最後一天執行。

預設下，工作在每月的第一天執行，在目前系統時間。

- **手動**

  工作不自動執行。您僅可以手動啟動。

  預設情況下已選定此選項。

- **每個月在所選週的指定天**

  工作定期在指定月日的指定時間執行。

  預設情況下，不選取一個月中的任何一天。預設開始時間為 18:00。

- **在偵測到病毒爆發時**

  工作在發生*病毒爆發*事件後執行。選取將監控病毒爆發的應用程式類型。有下列應用程式類型可用：

  - 病毒防護工作站和檔案伺服器
  - 用於週邊防護的防毒軟體
  - 用於郵件伺服器的防毒軟體

  預設情況下選定所有應用程式類型。

  您可能想根據報告病毒爆發的安全應用程式類型執行不同的工作。此種情況下，刪除您不需要的應用程式類型選項。

- **在完成其它工作時**

  目前工作在其他工作完成後啟動。您可以選取先前工作如何結束（成功或帶有錯誤）以觸發目前工作的啟動。例如，您可能想使用***Turn on the device***選項執行開啟裝置工作，完成後，請執行*惡意軟體掃描*工作。只有當這兩項工作都被分配給相同的裝置時，此參數才會有作用。

- **執行錯過的工作**

  該選項決定在工作要啟動時用戶端裝置在網路中不可見時工作的行為。

  如果啟用該選項，系統將在下一次在用戶端裝置上執行 Kaspersky 應用程式時嘗試啟動工作。如果工作排程是**手動**、**一次**或**立即**，裝置在網路中可見或包含在工作範圍後，工作會立即啟動。

  如果停用此選項，則僅限排程的工作會在用戶端裝置上執行。若為**手動**、**一次**與**立即**排程，工作僅會在網路上顯示的用戶端裝置上執行。例如，您可能想為消耗資源的工作停用該選項，您僅想在業餘時間執行該工作。

  預設情況下已停用該選項。

- **使用工作啟動自動隨機延遲**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動，即是，*分佈式工作啟動*。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  當工作被建立時，根據工作中包含用戶端裝置的數量，分發啟動時間被自動計算。然後，工作總是在計算的開始時間啟動。然後當工作設定被編輯或者工作被手動啟動時，計算的工作啟動時間值被變更。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

- **使用工作啟動隨機延遲間隔（分鐘）**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

  預設情況下已停用該選項。預設時間間隔為一分鐘。

步驟 6：定義工作名稱

在**定義工作名稱**視窗，指定您正在建立的規則名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元（ `"*<>?\:|` ）。

點擊**下一步**以繼續到下一步。

步驟 7：完成工作建立

在**完成工作建立**視窗，點擊**完成**按鈕以完成精靈。

如果您想讓工作在精靈完成時立即啟動，選取**精靈完成時執行工作**核取方塊。

管理統計資訊

防護系統和受管理裝置狀態的統計資訊顯示在可以自訂的資訊視窗中。統計資訊顯示在**管理伺服器**節點工作區的**統計**頁籤中。該標籤包含一些第二級標籤（頁面）。每個選項頁面顯示統計資訊視窗，以及企業新聞和 Kaspersky 的其他材料的連結。統計資訊以表格或圖表（圓餅圖或柱狀圖）的形式顯示在資訊視窗。應用程式執行時，資訊視窗中的資訊實時更新，顯示防護應用程式的目前狀態。

您可以變更**統計**頁籤上的二級選項頁面設定，每頁的資訊視窗數量，以及資訊視窗中的資訊顯示模式。

*若要在**統計**頁籤新增資訊視窗二級頁籤：*

1. 在**統計**頁籤的右上角，點擊**自訂檢視**檢視按鈕。

   統計資訊內容視窗開啟。該視窗包含目前顯示在**統計**頁籤的選項頁面清單。在該視窗，您可以變更標籤上頁面的顯示順序，新增和刪除頁面，透過點擊**內容**按鈕轉到頁面內容設定。

2. 點擊**新增**按鈕。

   這將開啟新頁面的內容視窗。

3. 設定新頁面：

   - 在**一般**區域，指定頁面名稱。
   - 在**資訊視窗**區域，點擊**新增**按鈕新增顯示在頁面的資訊視窗。

     點擊**資訊視窗**區域的**內容**按鈕來設定您新增的資訊視窗內容：名稱、類型和圖表顯示、用於構建圖表的資料。

4. 點擊**確定**。

帶有您所新增的資訊視窗的選項頁面出現在**統計**頁籤。點擊設定圖示（ ⚙ ）迅速轉換到頁面設定或所選資訊視窗。

設定事件通知

卡巴斯基安全管理中心允許您設定將用戶端裝置上發生的事件通知管理員的方法，並允許您設定通知：

- 電子郵件。當發生事件時，程式將向指定的電子郵件信箱傳送通知。您可以編輯通知文字。
- SMS。當發生事件時，程式將向指定的電話號碼傳送通知。您可以配置 SMS 通知以便透過郵件閘道傳送。
- 可執行檔。當裝置上發生事件時，將在管理員工作站上啟動該可執行檔。管理員可以透過該可執行檔接收已發生事件參數。

要設定關於用戶端電腦上已發生事件的通知，請執行以下操作：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。
2. 在節點工作區中，選取**事件**頁籤。
3. 點擊**配置通知和事件匯出**連結並在下拉清單中選取**配置通知**值。

   這會開啟**內容：事件**視窗。

4. 在**通知**區域，選取通知方法（透過郵件、SMS或者執行可執行檔）並定義通知設定：

- **電子郵件**

電子郵件頁籤允許您透過電子郵件配置事件通知。

在**收件者（電子郵件信箱）**欄位，指定應用程式傳送通知的電子郵件信箱。您可以在該欄位指定多個位址，以分號分隔。

在 **SMTP 伺服器**欄位，指定郵件伺服器位址，以分號分隔。您可以使用以下參數：

- IPv4 或 IPv6 位址
- 裝置的 Windows 網路名稱（NetBIOS 名稱）
- SMTP 伺服器的 DNS 名稱

在 **SMTP 伺服器連接埠**欄位，指定 SMTP 伺服器通訊埠號。預設埠號為 25。

如果您啟用**使用 DNS MX 尋找**選項，您可以將 IP 位址的多個 MX 記錄用於 SMTP 伺服器的相同 DNS 名稱。相同 DNS 名稱可能有幾個 MX 記錄，具有不同的接收電子郵件的優先次序。管理伺服器嘗試按 MX 記錄優先次序向 SMTP 伺服器傳送電子郵件通知。預設情況下已停用該選項。

如果您啟用**使用 DNS MX 尋找**選項並且不啟用 TLS 設定的使用，我們建議您使用伺服器裝置上的 DNSSEC 設定作為傳送電子郵件通知的額外防護措施。

按一下**設定**用於定義其他通知設定的連結：

- 主旨名稱（電子郵件的主旨名稱）
- 寄件者電子郵件地址
- ESMTP 身分驗證設定

如果為 SMTP 伺服器啟用了 ESMTP 身分驗證選項，則必須在 SMTP 伺服器上指定帳戶進行身分驗證。

- SMTP 伺服器的 TLS 設定：
  - **請勿使用 TLS**

    如果您想停用電子郵件訊息加密，您可以選取此選項。

  - **如果 SMTP 伺服器支援，請使用 TLS**

    如果要使用 TLS 連線到 SMTP 伺服器，則可以選取此選項。如果 SMTP 伺服器不支援 TLS，管理伺服器將不使用 TLS 連線 SMTP 伺服器。

  - **始終使用 TLS，檢查伺服器憑證的有效性**

    如果要使用 TLS 身分驗證設定，則可以選取此選項。如果 SMTP 伺服器不支援 TLS，管理伺服器將無法連線 SMTP 伺服器。

我們建議您使用此選項以更好地防護與 SMTP 伺服器的連線。如果選取此選項，則可以為 TLS 連線設定身分驗證設定。

如果您選擇"**始終使用 TLS，檢查伺服器憑證的有效性**"值，則可以指定用於驗證 SMTP 伺服器的憑證，並選取是要透過任何版本的 TLS，還是僅透過 TLS 1.2 或更高版本啟用通訊。此外，您可以指定在 SMTP 伺服器上進行用戶端身分驗證的憑證。

您可以為 SMTP 伺服器指定 TLS 設定：

- 瀏覽 SMTP 伺服器憑證檔案：

您可以從受信任的憑證頒發機構接收帶有憑證清單的檔案，然後將該檔案上傳到管理伺服器。卡巴斯基安全管理中心會檢查 SMTP 伺服器的憑證是否也由受信任的憑證頒發機構簽署。如果未從受信任的憑證頒發機構收到 SMTP 伺服器的憑證，卡巴斯基安全管理中心將無法連線到 SMTP 伺服器。

- 瀏覽用戶端憑證檔案：

您可以使用從任何來源（例如，從任何受信任的憑證頒發機構）收到的憑證。您必須使用以下憑證類型之一指定憑證及其私密金鑰：

- X-509 憑證：

您必須指定一個帶有憑證的檔案和一個帶有私密金鑰的檔案。這兩個檔案互不相依，檔案的載入順序並不重要。當同時載入兩個檔案時，您必須指定用於解碼私密金鑰的密碼。如果未編碼私密金鑰未編碼，則密碼可以為空值。

- pkcs12 容器：

您必須上傳包含憑證及其私密金鑰的單一檔案。載入檔案後，您必須指定用於解碼私密金鑰的密碼。如果未編碼私密金鑰未編碼，則密碼可以為空值。

通知訊息欄位包含事件發生時應用程式傳送的事件資訊標準文字。該文字包含替代參數，例如事件名稱、裝置名稱和網域名稱。您可以新增有事件相關詳情的其他更新替代參數來編輯訊息文字。替代參數的清單可點擊欄位右方的按鈕取得。

如果通知文字包含百分號 (%) 字元，您必須指定兩次以允許訊息傳送。範例，“CPU 負載是 100%%”。

點擊**設定通知限制數**連結指定應用程式在指定時段內可以傳送的最大通知數量。

按一下**傳送測試訊息**按鈕以檢查您是否已正確配置通知。該應用程式應向您指定的電子郵件位址傳送測試通知。

- SMS

SMS 頁籤可讓您設定將各種事件的 SMS 通知傳到手機。SMS 訊息透過郵件閘道傳送。

在**收件者（電子郵件信箱）**欄位，指定應用程式傳送通知的電子郵件信箱。您可以在該欄位指定多個位址，以分號分隔。通知將被傳送到指定郵件信箱關聯的電話號碼。

在 **SMTP 伺服器**欄位，指定郵件伺服器位址，以分號分隔。您可以使用以下參數：

- IPv4 或 IPv6 位址
- 裝置的 Windows 網路名稱（NetBIOS 名稱）
- SMTP 伺服器的 DNS 名稱

在 **SMTP 伺服器連接埠**欄位，指定 SMTP 伺服器通訊埠號。預設埠號為 25。

按一下**設定**用於定義其他通知設定的連結：

- 主旨名稱（電子郵件的主旨名稱）
- 寄件者電子郵件地址
- ESMTP 身分驗證設定

如有必要，如果 SMTP 伺服器啟用了 ESMTP 身分驗證選項，您可以在 SMTP 伺服器上指定一個帳戶進行身分驗證。

- 適用於 SMTP 伺服器的 TLS 設定

您可以停用 TLS 的使用，如果 SMTP 伺服器支援此協議，則使用 TLS，或者您可以強制僅使用 TLS。如果您選取僅使用 TLS，您可以指定用於驗證 SMTP 伺服器的憑證，並選取是要透過任何版本的 TLS，還是僅透過 TLS 1.2 或更高版本啟用通訊。此外，如果您選取僅使用 TLS，您可以為 SMTP 伺服器上的用戶端身分驗證指定憑證。

- 瀏覽 SMTP 伺服器憑證檔案

您可以從受信任的憑證頒發機構接收帶有憑證清單的檔案，然後將該檔案上傳到卡巴斯基安全管理中心。卡巴斯基安全管理中心會檢查 SMTP 伺服器的憑證是否也由受信任的憑證頒發機構簽署。如果未從受信任的憑證頒發機構收到 SMTP 伺服器的憑證，卡巴斯基安全管理中心將無法連線到 SMTP 伺服器。

您必須上傳包含憑證及其私密金鑰的單一檔案。載入檔案後，您必須指定用於解碼私密金鑰的密碼。如果私密金鑰未編碼，則密碼可以為空值。**通知訊息**欄位包含標準文字，其中包含有關事件發生時應用程式傳送的事件的資訊。該文字包含替代參數，例如事件名稱、裝置名稱和網域名稱。您可以新增有事件相關詳情的其他更新替代參數來編輯訊息文字。替代參數的清單可點擊欄位右方的按鈕取得。

如果通知文字包含百分號 (%) 字元，您必須指定兩次以允許訊息傳送。範例，“CPU 負載是 100%%”。

按一下**設定通知限制數**連結以指定應用程式在指定時間段可以傳送的最大通知數量（通知數量 / 分鐘數）。

點擊**“傳送測試訊息”**按鈕檢查您是否正確配置了通知。該應用程式應向您指定的收件人傳送測試通知。

- **要執行的可執行檔**

如果選取該通知方法，您可以在輸入欄位指定事件發生時要啟動的應用程式。

點擊**設定通知限制數**連結允許您指定應用程式在指定時間段可以傳送的最大通知數量（通知數量 / 分鐘數）。

點擊**傳送測試訊息**按鈕允許您檢查您是否正確配置了通知：應用程式傳送測試通知到您指定的郵件信箱。

5. 在**通知訊息**欄位中，輸入事件發生時程式要傳送的文字。
   您可以使用文字欄位右邊的下拉清單來新增事件詳情的替代設定（例如，事件敘述、發生事件等等）。

   如果通知文字包含 % 字元，您必須指定兩次以允許訊息傳送。範例，“CPU 負載是 100%%”。

6. 點擊**傳送測試訊息**按鈕以檢查通知是否已成功設定。
   程式傳送測試通知到指定使用者。

7. 點擊**確定**儲存變更。

經過調整的通知設定將應用於用戶端裝置上發生的所有事件。

您可在管理伺服器設定、隱私設定或應用程式設定的**事件配置**區域覆寫特定事件的通知設定。

為 SMTP 伺服器建立憑證

要為 SMTP 伺服器建立憑證：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。
2. 在節點工作區中，選取**事件**頁籤。
3. 點擊**配置通知和事件匯出**連結並在下拉清單中選取**配置通知**值。
   “事件內容”視窗開啟。
4. 在**電子郵件**頁籤，點擊**設定**連結以開啟**設定**視窗。
5. 在**設定**視窗，點擊**指定憑證**連結以開啟**簽章憑證**視窗。
6. 在**簽章憑證**視窗，點擊**瀏覽**按鈕。
   憑證視窗隨即開啟。
7. 在**憑證類型**下拉清單，選取憑證的公有類型或私有憑證類型：
   - 如果選取了私有類型憑證（**PKCS#12 容器**），指定憑證檔案和密碼。
   - 如果選取了公有類型憑證（**X.509 憑證**）：
     a. 指定私有金鑰檔案（帶有 *.prk 或 *.pem 副檔名的檔案）。
     b. 指定私有金鑰密碼。
     c. 指定公共金鑰檔案（帶有 *.cer 副檔名）。
8. 點擊**確定**。

SMTP 伺服器憑證被發佈。

事件分類

卡巴斯基安全管理中心和受管應用程式的操作事件資訊儲存在管理伺服器資料庫和 Microsoft Windows 系統記錄。您可以在管理伺服器資料庫中**管理伺服器**節點的**事件**頁籤上檢視資訊。

事件頁籤的資訊會以事件分類清單形式表示。每個分類僅包含特殊類型的事件。例如，“裝置狀態是緊急”分類僅包含裝置狀態變成“緊急”的記錄。安裝應用程式後，**事件**頁籤會包含一些標準事件分類。您可以建立附加事件分類或者將事件資訊匯出為檔案。

檢視事件分類

要檢視事件分類，請執行以下操作：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。
2. 在節點工作區中，選取**事件**頁籤。
3. 在**事件分類**下拉清單中，選取相關的事件分類。

   如果您想要該分類的事件永久顯示在工作區，點擊分類旁邊的星星按鈕（ ☆ ）。

管理伺服器中所選取的事件清單將顯示在工作區中。

您可以在事件清單中將資訊排序，採用遞增或者遞減。

自訂事件分類

要自訂事件分類，請執行以下操作：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。
2. 在節點工作區中，選取**事件**頁籤。
3. 在**事件**頁籤中開啟相關事件分類。
4. 點擊**分類內容**按鈕。

您可以在隨後開啟的事件分類內容視窗中設定事件分類。

建立事件分類

要建立事件分類，請執行以下操作：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。
2. 在節點工作區中，選取**事件**頁籤。

3. 點擊**建立新分類**按鈕。

4. 在開啟的**新事件分類**視窗中，輸入新分類的名稱，然後點擊**確定**。

   您所指定名稱的分類建立於**事件分類**下拉清單中。

預設情況下，所建立的事件分類將包含管理伺服器中儲存的所有事件。要讓分類中僅顯示您需要的事件，您必須自訂該分類。

將事件分類匯出至文字檔案

要將事件分類匯出至文字檔案，請執行以下操作：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。

2. 在節點工作區中，選取**事件**頁籤。

3. 點擊**匯入/匯出**按鈕。

4. 在下拉式清單中，選擇**匯出事件到檔案**。

   事件匯出精靈啟動。遵照精靈的說明。

從分類中刪除事件

要從分類中刪除事件：

1. 在主控台樹狀目錄中，選取具有相關管理伺服器名稱的節點。

2. 在節點工作區中，選取**事件**頁籤。

3. 使用滑鼠、**Shift** 或 **Ctrl** 鍵選取要刪除的事件。

4. 以下列方式之一刪除所選事件：

   - 透過在所選事件的上下文功能表中，選取**刪除**。

     如果您在上下文功能表中選取**刪除所有**項目，則無論您的事件分類項目為何，所有顯示的事件都將從分類項目中刪除。

   - 如果選取了一個事件，點擊**刪除事件**連結；如果選取了多個事件，點擊**刪除事件**連結。

   所選事件被刪除。

根據使用者請求新增應用程式到排除

當您收到使用者請求解鎖被錯誤封鎖的應用程式時，您可以從這些應用程式的自適應安全規則建立排除。此後，應用程式將不會在使用者裝置上被封鎖。您可以在管理伺服器的**監控**頁籤追蹤使用者要求的數量。

要根據使用者請求新增被 Kaspersky Endpoint Security 封鎖的應用程式到排除：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。
2. 在節點工作區中，選取**事件**頁籤。
3. 在**事件分類**下拉清單中，選取**使用者請求**。
4. 以滑鼠右鍵按一下包含您要新增到排除的應用程式的一個使用者請求（或多個使用者請求），然後選取**新增排除**。

   這啟動新增排除精靈。遵循其說明。

所選應用程式將在下一次用戶端裝置與管理伺服器同步時，從**智慧培訓狀態中的規則觸發**清單（在主控台樹狀目錄的**儲存區**下）中排除，且將不再出現在清單中。

裝置分類

裝置狀態的資訊會顯示在主控台樹狀目錄的**裝置分類**資料夾。

裝置分類資料夾中的資訊會顯示為裝置分類清單。每個分類包含滿足特定條件的裝置。例如，**處於"緊急"狀態的裝置**分類僅包含帶有*緊急*狀態的裝置。安裝應用程式後，**裝置分類**資料夾將包含一些標準分類。您可以建立其他（自訂）裝置分類，將分類項目匯出至檔案，或使用從其他檔案匯入的設定來建立分類項目。

檢視裝置分類

若要檢視裝置分類：

1. 在主控台樹狀目錄中，選取**裝置分類**資料夾。
2. 在該資料夾工作區的**此分類的裝置**清單中，選取相關的裝置分類項目。
3. 點擊**執行分類**按鈕。
4. 點擊**分類結果**頁籤。

工作台將顯示分類中所設定標準的裝置清單。

您可以在裝置清單的任何欄中以遞減或遞增進行排序。

配置裝置分類

要配置裝置分類：

1. 在主控台樹狀目錄中，選取**裝置分類**資料夾。
2. 在工作區中點擊**分類**頁籤，然後點擊使用者分類清單中的相關裝置分類。
3. 點擊**分類內容**按鈕。

4. 在開啟的內容視窗，指定以下設定：

   - 一般分類內容。
   - 包含裝置到該分類必須滿足的條件。您可以在選取條件名稱並點擊**內容**按鈕後設定條件。
   - 安全設定。

5. 點擊**確定**。

裝置被套用並儲存。

以下是分配裝置到分類的條件敘述。多個條件使用 OR 邏輯運算子組合在一起：分類範圍將包含至少符合列出的一個條件的裝置。

一般

在**一般**區域，您可以變更分類條件的名稱，指定是否必須倒轉條件：

反轉分類條件

預設情況下已停用該選項。

如果啟用此選項，指定的分類條件將倒轉。此分類將包含所有不符合該條件的裝置。

以下範例展示了反轉工作的邏輯：

- **條件**：您的裝置上安裝了 Linux 類型且內部版本號為 00.0.000 的作業系統。
- **反轉條件**：您的裝置上安裝了非 Linux 類型且內部版本號為 00.0.000 的作業系統，這等價於：
  安裝了非 Linux 類型或內部版本號非 00.0.000 的作業系統。

因此，分類將包括安裝了 Windows 類型且內部版本號為 00.0.000 的裝置，或安裝了 Linux 類型但內部版本號不為 00.0.000 的裝置。

網路

在**網路**區域，您可以指定依據網路資料裝置納入分類的標準：

- **裝置名稱或 IP 位址**

  裝置的 Windows 網路名稱（NetBIOS 名稱），或者 IPv4 或 IPv6 位址。

- **Windows 網域**

  顯示指定的 Windows 網域中包括的所有裝置。

- **管理群組**

  顯示指定的管理群組中包括的裝置。

- **敘述**

  裝置內容視窗中的文字：在**一般**區域的**敘述**欄位。
  您可以使用以下特徵說明**敘述**欄位中的文字：

  - 在單詞中：

    - *****。用任意數量的字元更換任何字串。

    例如：
    要敘述單詞 **Server** 或 **Server's**，您可以輸入 **Server***。

    - **?**。更換任意單個字元。

    例如：
    要敘述單詞 **Window** 或 **Windows**，您可以輸入 **Windo?**。
    星號 (*****) 或問號 (**?**) 不能用於查詢中的第一個字元。

  - 要尋找多個單詞：

    - 空格。顯示所有在其敘述中包含列出的任何單詞的裝置。

    例如：
    要尋找在其敘述中包含**從屬**或**虛擬**單詞的短語，您可以在查詢中包含**從屬虛擬**等字。

    - **+**。當單詞帶有加號前綴時，所有搜尋結果都將包含該單詞。

    例如：
    要搜尋同時包含**從屬**和**虛擬**的短語，請輸入**+從屬+虛擬**查詢。

    - **-**。當單詞帶有減號前綴時，所有搜尋結果都不包含該單詞。

    例如：
    要尋找包含**從屬**但不包含**虛擬**的短語，請輸入**+從屬-虛擬**查詢。

    - **「<某些文字>」**。引號中圍繞的文字必須存在文字中。

    例如：
    要尋找包含**從屬伺服器**單詞群組合的短語，您可以在查詢中輸入**「從屬伺服器」**。

- **IP 範圍**

  如果啟用此選項，您可以輸入應該包括相關裝置的 IP 範圍的初始和最終 IP 位址。
  預設情況下已停用該選項。

標籤

在**標籤**區域中，您可以根據先前新增到受管理裝置的敘述的關鍵字（標籤）設定將裝置納入分類的標準：

- **如果有至少一個指定的標籤符合則套用**

  如果啟用此選項，搜尋結果將顯示包含帶有所選標籤的敘述的裝置。

  如果停用此選項，搜尋結果將僅顯示包含帶有所有標籤的敘述的裝置。

  預設情況下已停用該選項。

- **必須包含標籤**

  如果選取了該選項，搜尋結果將顯示帶有包含了所選標籤的敘述的裝置。要尋找裝置，您可以使用星號，它表示任何字元長度的字串。

  預設情況下已選定此選項。

- **必須排除標籤**

  如果選取了該選項，搜尋結果將顯示不帶有包含了所選標籤的敘述的裝置。要尋找裝置，您可以使用星號，它表示任何字元長度的字串。

Active Directory

在**Active Directory**區域，您可以根據 Active Directory 資料設定將裝置納入分類的標準：

- **裝置在 Active Directory 組織單元中**

  如果啟用此選項，選取範圍將包括輸入欄位中指定的 Active Directory 單元中的裝置。

  預設情況下已停用該選項。

- **包括子組織單元**

  如果啟用此選項，選取範圍將包括指定 Active Directory 組織單元的所有子組織單元中的裝置。

  預設情況下已停用該選項。

- **該裝置是 Active Directory 群組成員**

  如果啟用此選項，選取範圍將包括輸入欄位中指定的 Active Directory 群組中的裝置。

  預設情況下已停用該選項。

網路活動

在**網路活動**區域，您可以根據網路活動指定將裝置納入分類的標準：

- **該裝置是發佈點**

  在下拉清單中，可設定執行搜尋時在分類中包括裝置的標準：
  - **是**。選取範圍將包括充當發佈點的裝置。
  - **否**。分類不包含作為發佈點的裝置。
  - **未選取值**。將不套用標準。

- **不斷開與管理伺服器的連線**

  在下拉清單中，可設定執行搜尋時在分類中包括裝置的標準：
  - **已啟用**。分類將包含已選取**不斷開與管理伺服器的連線**核取方塊的裝置。
  - **已停用**。分類將包含未選取**不斷開與管理伺服器的連線**核取方塊的裝置。
  - **未選取值**。將不套用標準。

- **連線設定檔已轉換**

  在下拉清單中，可設定執行搜尋時在分類中包括裝置的標準：
  - **是**。該分類將包含連線設定檔轉換後連線到管理伺服器的裝置。
  - **否**。該分類將不包含連線設定檔轉換後連線到管理伺服器的裝置。
  - **未選取值**。將不套用標準。

- **上一次連線到管理伺服器**

  您可使用此方塊設定按上一次連線到管理伺服器的時間搜尋裝置的標準。

  如果選取該方塊，則在輸入欄位中，您可以指定在用戶端裝置上安裝的網路代理和管理伺服器之間建立上一次連線的時間間隔（日期和時間）。選取將包括位於指定間隔的裝置。

  如果清除此方塊，則將不會套用標準。

  預設情況下已清空此方塊。

- **網路輪詢時偵測到新裝置**

  搜尋最近幾天透過網路輪詢偵測到的新裝置。

  如果選取此核取方塊，分類將只包括在**偵測週期（天）**欄位中指定的天數內透過裝置發現偵測到的新裝置。

  如果停用此選項，分類將包括透過裝置發現偵測到的所有裝置。

  預設情況下已停用該選項。

- **裝置可見**

  在下拉清單中，可設定執行搜尋時在分類中包括裝置的標準：

  - **是**。程式在分類中包括網路中目前可見的裝置。
  - **否**。應用程式在分類中包括網路中目前不顯示的裝置。
  - **未選取值**。將不套用標準。

應用程式

在**應用程式**區域中，您可以根據所選的受管理應用程式設定將裝置納入分類的標準：

- **應用程式名稱**

  在下拉清單中，可設定按 Kaspersky 應用程式名稱執行搜尋時在分類中包括裝置的標準。

  清單僅提供管理員工作站上已安裝管理外掛程式的應用程式的名稱。

  如果未選取任何應用程式，則將不會套用該標準。

- **應用程式版本**

  在輸入欄位，可設定按 Kaspersky 應用程式版本號執行搜尋時在分類中包括裝置的標準。

  如果未指定版本號，則將不會套用該標準。

- **重大更新名稱**

  在輸入欄位中，可設定按應用程式名稱或更新套件編號執行搜尋時在分類中包括裝置的標準。

  如果欄位留空，則將不會套用該標準。

- **上一次模組更新**

  您可以使用此選項來設定按這些裝置上安裝的程式模組上次更新的時間搜尋裝置的標準。

  如果選中此方塊，則您可以在輸入欄位中指定執行這些裝置上安裝的程式模組的上一次更新的時間間隔（日期和時間）。

  如果清除此方塊，則將不會套用標準。

  預設情況下已清空此方塊。

- **裝置透過卡巴斯基安全管理中心管理**

  在該下拉清單，您可以包含透過卡巴斯基安全管理中心管理的裝置到分類：
  - **是**。應用程式包含透過卡巴斯基安全管理中心管理的裝置。
  - **否**。若裝置不透過卡巴斯基安全管理中心管理，則應用程式會將其包含在分類中。
  - **未選取值**。將不套用標準。

- **安全應用程式已安裝**

  在該下拉清單，您可以包含已安裝安全應用程式的裝置到分類：
  - **是**。應用程式包含安裝了安全應用程式的裝置到分類。
  - **否**。應用程式會在分類中包含未安裝安全應用程式的裝置。
  - **未選取值**。將不套用標準。

作業系統

在**作業系統**區域，您可以根據作業系統指定將裝置納入分類的標準。

- **作業系統版本**

  如果選中該方塊，您可以從清單中選取一個作業系統。安裝了指定作業系統的裝置會包含在搜尋結果中。

- **作業系統 bit 大小**

  在該下拉清單中可選取作業系統的架構，這將決定將移動規則套用到裝置（**未知**、**x86**、**AMD64** 或 **IA64**）的方式。預設情況下，不選取清單中的任何選項，這樣就不會對作業系統的架構進行定義。

- **作業系統服務套件版本**

  在該欄位中，可以指定作業系統的更新套件版本（採用 *X.Y* 格式），這將決定將移動規則套用到裝置的方式。預設情況下，不指定版本值。

- **作業系統版本**

  該設定僅套用到 Windows 作業系統。

  作業系統版本號。您可以指定所選作業系統是否必須具有相等、更早或更晚的版本號。您也可以設定對所有版本號的搜尋，除了指定的值。

- **作業系統發佈 ID**

  該設定僅套用到 Windows 作業系統。

  作業系統發佈 ID。您可以指定所選作業系統是否必須具有相等、更早或更晚的發佈 ID。您也可以設定對所有發佈 ID 的搜尋，除了指定的值。

裝置狀態

在**裝置狀態**區域，您可以根據受管理應用程式的裝置狀態的敘述設定將裝置納入分類的標準：

- **裝置狀態**

  在該下拉清單中，您可以選取下列裝置狀態之一：*確定*、*緊急*或*警告*。

- **裝置狀態敘述**

  在此欄位中，您可以選取條件旁邊的核取方塊，若滿足這些條件，程式會為裝置分配下列狀態之一：*確定*、*緊急*或*警告*。

- **應用程式定義的裝置狀態**

  您可以在該下拉清單中選取即時防護狀態。具有指定即時防護狀態的裝置將被包括在選取範圍中。

防護元件

在**防護元件**區域，您可以根據防護狀態設定將裝置納入分類的標準：

- **資料庫發佈日期**

  如果啟用此選項，您可以按病毒資料庫發佈日期搜尋用戶端裝置。在該輸入欄位中，您可以設定執行搜尋的時間間隔。

  預設情況下已停用該選項。

- **上一次掃描**

  如果啟用此選項，您可以按上次惡意軟體掃描時間來搜尋用戶端裝置。在該輸入欄位中，您可以指定執行上一次惡意軟體掃描的時段。

  預設情況下已停用該選項。

- **偵測到的威脅總數**

  如果啟用此選項，您可以依據發現的病毒數量來搜尋用戶端裝置。在輸入欄位中，您可以設定發現病毒總數的上限值和下限值。

  預設情況下已停用該選項。

應用程式登錄資料

在**應用程式登錄資料**區域，您可以根據已安裝的應用程式設定搜尋裝置的標準：

- **應用程式名稱**

  在該下拉清單中，您可以選取應用程式。安裝有指定應用程式的裝置將包括在選取範圍中。

- **應用程式版本**

  在該輸入欄位中，您可以指定選定應用程式的版本。

- **供應商**

  在該下拉清單中，您可以選取已安裝應用程式的生產商。

- **應用程式狀態**

  在該下拉清單中，您可以選取應用程式的狀態（*已安裝*、*未安裝*）。已安裝或未安裝指定應用程式的裝置，取決於所選狀態，將被包含在分類。

- **根據更新尋找**

  如果啟用此選項，則搜尋操作將使用相關裝置內應用程式更新的有關資訊來執行。選取核取方塊後，**應用程式名稱**、**應用程式版本**與**應用程式狀態**欄位會各自變成**更新名稱**、**更新版本**和**狀態**。

  預設情況下已停用該選項。

- **不相容的安全應用程式名稱**

  在該下拉清單中，您可以選取協力廠商安全應用程式。在搜尋過程中，安裝有指定程式的裝置將包括在選取範圍中。

- **應用程式標籤**

  在該下拉清單中，您可以選取應用程式標籤。所有安裝了敘述中帶有所選標籤的應用程式的裝置都被包含在裝置分類。

- **套用到沒有指定標籤的裝置**

  如果啟用此選項，分類將包含未帶有所選標籤的敘述的裝置。

  如果停用該選項，則不套用標準。

  預設情況下已停用該選項。

硬體登錄資料

在**硬體登錄資料**區域，您可以根據所安裝的硬體設定將裝置納入分類的標準：

- **裝置**

  在該下拉清單中，您可以選取單元類型。所有帶有該單元的裝置被包含在搜尋結果。

  該欄位支援完整文字搜尋。

- **供應商**

  在該下拉清單中，您可以選取單元生產商的名稱。所有帶有該單元的裝置被包含在搜尋結果。

  該欄位支援完整文字搜尋。

- **裝置名稱**

  在 Windows 網路中的裝置名稱。具有指定名稱的裝置將包括在該分類中。

- **敘述**

  裝置或硬體單元的敘述。帶有該欄位中指定的敘述的裝置將包括在分類範圍內。

  可在裝置的內容視窗輸入任何格式的裝置敘述。該欄位支援完整文字搜尋。

- **裝置製造商**

  裝置製造商的名稱。被指定生產商製造的裝置將包括在分類範圍內。

  您可以在裝置的內容視窗中輸入製造商的名稱。

- **序號**

  帶該欄位中指定序號的所有硬體裝置將包括在該分類中。

- **清單號**

  帶有該欄位中指定的清單編號的裝置將包括在選取範圍內。

- **使用者**

  該欄位中指定使用者的所有硬體裝置都將包括在該分類中。

- **位置**

  裝置或硬體單元的位置（例如，在總部或分公司）。在該欄位中指定的位置佈署的電腦或其他裝置將包括在該分類中。

  您可以在該裝置的內容視窗中以任何格式敘述裝置的位置。

- **CPU 頻率 (MHz)**

  CPU 的頻率範圍。CPU 與這些輸入欄位（含）中頻率範圍比對的裝置將包括在分類範圍內。

- **虛擬 CPU 核心**

  CPU 中虛擬內核的數量範圍。CPU 與這些輸入欄位（含）中範圍比對的裝置將包括在分類範圍內。

- **硬碟磁區 (GB)**

  裝置硬碟容量值的範圍。硬碟與這些輸入欄位（含）中範圍比對的裝置將包括在分類範圍內。

- **記憶體大小 (MB)**

  裝置 RAM 大小的值的範圍。RAM 與這些輸入欄位（含）中範圍比對的裝置將包括在分類範圍內。

虛擬機

在**虛擬機**區域中，您可以根據它們是否是虛擬機或虛擬桌面基礎架構 (VDI) 的一部分來指定將裝置納入分類的標準：

- **這是一台虛擬機**

  在此下拉清單中，您可以選取以下選項：
  - **不重要**。
  - **否**。尋找不是虛擬機的裝置。
  - **是**。搜尋虛擬機裝置。

- **虛擬機類型**

  在該下拉清單中，您可以選取虛擬機製造商。
  若在**這是一台虛擬機**下清單中選取**是**或**不重要**值，則可使用此下拉清單。

- **虛擬桌面基礎架構的一部分**

  在此下拉清單中，您可以選取以下選項：
  - **不重要**。
  - **否**。尋找不是虛擬桌面基礎架構一部分的裝置。
  - **是**。搜尋屬於虛擬桌面基礎架構 (VDI) 一部分的裝置。

弱點與更新

在**弱點與更新**區域，您可以根據 Windows 更新來源指定將裝置納入分類的標準：

WUA 已轉換到管理伺服器

您可以在下拉清單中選取以下搜尋選項之一：
- **是**。如果選中該選項，搜尋結果會包含從管理伺服器收到 Windows Update 更新的裝置。
- **否**。如果選中該選項，結果會包含從其他來源收到 Windows Update 更新的裝置。

使用者

在**使用者**區域中，您可以根據登入到作業系統的使用者帳戶設定將裝置納入分類的標準。

- **最後一次登入系統的使用者**

  如果啟用此選項，按一下**瀏覽**按鈕可以指定使用者帳戶。搜尋結果包含其上一次登入使用者為指定使用者的裝置。

- **登入系統至少一次的使用者**

  如果啟用此選項，按一下**瀏覽**按鈕可以指定使用者帳戶。搜尋結果包含指定使用者至少登入一次的裝置。

影響受管理應用程式狀態的問題

在**影響受管理應用程式狀態的問題**區域，您可以根據由受管理應用程式偵測到的可能問題清單指定將裝置納入分類的標準。如果至少一個您選取的問題存在於裝置，裝置將被包含到分類。當您選取幾個應用程式的問題時，您可以選取在所有清單中自動選取該問題。

裝置狀態敘述

您可以選取受管理應用程式狀態敘述的核取方塊；接收這些狀態時，裝置將被包含在分類。當您選取幾個應用程式的狀態時，您可以選取在所有清單中自動選取該狀態。

受管理應用程式元件的狀態

在**受管理應用程式元件的狀態**區域中，您可以根據受管理應用程式元件狀態設定將裝置納入分類的標準：

- **資料洩漏防護狀態**

  根據資料外洩防護的狀態搜尋裝置（*裝置上無資料*, *已停止*, *正在啟動*, *已暫停*, *執行中*, *失敗*）。

- **協作伺服器防護狀態**

  根據伺服器協作防護狀態搜尋裝置（*裝置上無資料*, *已停止*、*正在啟動*、*已暫停*, *執行中*、*失敗*）。

- **郵件伺服器的病毒防護狀態**

  根據郵件伺服器防護狀態搜尋裝置（*裝置上無資料*、*已停止*、*正在啟動*、*已暫停*、*執行中*、*失敗*）。

- **端點感應器狀態**

  根據端點感應器元件狀態搜尋裝置（*裝置上無資料*、*已停止*、*正在啟動*、*已暫停*、*執行中失敗*）。

加密

加密演算法

進階加密標準 (AES) 對稱區塊編碼器演算法。在下拉清單中，您可以選取加密金鑰大小（56-bit、128-bit、192-bit 或 256-bit）。

可用值：*AES56*、*AES128*、*AES192* 和 *AES256*。

雲端區段

在**雲端區段**區域中，您可以根據相關雲端區段設定將裝置納入分類的標準：

- **裝置在雲端區段中**

  如果啟用此選項，您可以按一下**瀏覽**按鈕可以指定要搜尋的區段。

  如果啟用**包含子物件**選項，則搜尋會在指定區段的所有子物件上執行。

  搜尋結果僅包含所選段的裝置。

- **使用 API 發現的裝置**

  在下拉清單，您可以選取裝置是否由 API 工具偵測：

  - **AWS**。裝置使用 AWS API 發現，就是，裝置在 AWS 雲端環境中。
  - **Azure**。裝置使用 Azure API 發現，就是，裝置在 Azure 雲端環境中。
  - **Google Cloud**。裝置被使用 Google API 發現，即裝置一定在 Google 雲端環境中。
  - **否**。系統無法用 AWS、Azure 或 Google API 偵測裝置，意即裝置在雲端環境外或在雲端環境中，但無法使用 API 加以偵測。
  - **沒有值**。這項條件不適用。

應用程式元件

該區域包含了在管理主控台中安裝了管理外掛程式的這些應用程式的元件清單。

在**應用程式元件**區域中，您可以根據所選應用程式元件的狀態和版本編號指定將裝置納入分類的標準：

- **狀態**

  根據應用程式傳送到管理伺服器的元件狀態搜尋裝置。您可以選取以下狀態之一：*裝置上無資料*、*已停止*、*正在啟動*、*已暫停*、*執行中*、*故障*或*未安裝*。如果安裝在受管理裝置上的應用程式的所選元件具有指定狀態，裝置被包含到裝置分類。

  由應用程式傳送的狀態：

  - *正在啟動* - 元件處於初始化處理程序中。
  - *執行中* - 元件被啟用且在正常工作。
  - *已暫停* - 元件被暫停，例如，在使用者在受管理應用程式上停止了防護後。
  - *故障* - 元件操作中發生錯誤。
  - *已停止* - 元件被停用且不在工作。
  - *未安裝* - 當設定應用程式自訂安裝時，使用者未選取該元件以安裝。

  不同於其他狀態，*裝置上無資料*狀態不由應用程式傳送。該選項顯示應用程式沒有所選元件狀態的資訊。例如，這可能發生在所選元件不屬於任何在裝置上安裝的應用程式時，或裝置關閉時。

- **版本**

  根據您在清單中選取的版本號搜尋裝置。您可以輸入版本號，例如 `3.4.1.0`，然後指定所選元件是否必須具有相同、更早或更新版本。您也可以設定對所有版本的搜尋，除了指定的值。

匯出裝置分類設定到檔案

要將裝置分類設定匯出至文字檔案，請執行以下操作：

1. 在主控台樹狀目錄中，選取**裝置分類**資料夾。
2. 在工作區中點擊**分類**頁籤，然後點擊使用者分類清單中的相關裝置分類。

   設定僅可從使用者建立的裝置分類中匯出。

3. 點擊**執行分類**按鈕。
4. 在**分類結果**頁籤，點擊**匯出設定**按鈕。
5. 在開啟的**"另存為"**視窗中，指定匯出設定的儲存名稱和路徑後點擊**"儲存"**按鈕。

   匯出設定將會儲存在指定路徑。

建立裝置分類

要建立裝置分類，請執行以下操作：

1. 在主控台樹狀目錄中，選取**裝置分類**資料夾。
2. 在該資料夾的工作區，點擊**進階**並在下拉清單中選取**建立新分類**。
3. 在開啟的**新裝置分類**視窗中，輸入新分類的名稱，然後點擊**確定**。

在主控台樹狀目錄中的**裝置分類**資料夾中，將出現您輸入名稱命名的新資料夾。預設情況下，新裝置分類將包含在其建立此分類的管理伺服器上的管理群組中的所有裝置。要讓分類只顯示您特別感興趣的裝置，透過點擊**分類內容**按鈕設定分類。

依據匯入的設定建立裝置分類

要使用匯入的設定建立裝置分類，請執行以下操作：

1. 在主控台樹狀目錄中，選取**裝置分類**資料夾。
2. 在該資料夾的工作區中，點擊**進階**按鈕並在下拉清單中選取**從檔案匯入分類**。
3. 在開啟的視窗中，指定您要匯入分類設定的檔案路徑。按一下**開啟**按鈕。

新分類輸入會建立在**裝置分類**資料夾。新分類的設定從您指定的檔案中被匯入。

如果名稱是**新分類**的分類已經存在於**裝置分類**資料夾，格式為 **(<下一個序號>)** 的索引會被新增到建立的分類名稱中，範例：**(1)**、**(2)**。

在分類中從管理群組中刪除裝置

在使用裝置分類時，你可以直接從管理群組中刪除裝置，而不是轉換到包含這些裝置的管理群組。

要從管理群組刪除裝置，請執行以下操作：

1. 在主控台樹狀目錄中，選取**裝置分類**資料夾。
2. 使用“**Shift**”或“**Ctrl**”鍵選取您希望刪除的裝置。
3. 以下列方式之一從管理群組中刪除所選裝置：
   - 在任何所選裝置的上下文功能表中，選取**刪除**。
   - 點擊**執行操作**按鈕並在下拉式清單中選取**從群組中刪除**。

所選裝置即從對應管理群組中刪除。

監控應用程式的安裝與移除

您可監控特定應用程式在受管理裝置的安裝與移除，例如特定瀏覽器。若要使用此功能，您可從應用程式登錄資料新增應用程式至監控的應用程式清單。安裝或移除監控的應用程式時，網路代理會發佈個別事件：**已安裝監控的應用程式**或**已解除安裝監控的應用程式**。您可使用事件分類或報告來監控這些事件。

只有在這些事件儲存在管理伺服器資料庫中時您才可加以監控。

若要將應用程式新增至監控的應用程式清單：

1. 在主控台樹狀目錄**進階 → 應用程式管理**資料夾中，選取**應用程式登錄資料**子資料夾。
2. 在顯示的應用程式清單上，點擊**顯示應用程式登錄資料內容視窗**按鈕。
3. 在顯示的**監控的應用程式**視窗中，點擊**新增**按鈕。
4. 在顯示的**選取應用程式名稱**視窗中，從應用程式登錄資料選取您要監控安裝與移除的應用程式。
5. 在**選取應用程式名稱**設定群組中，點擊**確定**按鈕。

當您設定了監控的應用程式清單，且監控的應用程式已在您組織的受管理裝置上安裝或移除，您可使用最近事件事件分類各自監控事件。

卡巴斯基安全管理中心元件的事件

每個 Kaspersky 元件都擁有自己的事件類型集。該區域列出出現在卡巴斯基安全管理中心管理伺服器、網路代理、iOS MDM 伺服器和 Exchange 行動裝置伺服器的事件類型。Kaspersky 應用程式中發生的事件類型不在此區域列出。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。對於管理伺服器，您還可以在管理伺服器屬性中檢視和設定事件清單。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

事件類型描述的資料結構

對於每個事件類型，它的顯示名稱、ID、字母碼、描述和預設儲存期限被提供。

- **事件類型顯示名稱**。該文字當您配置事件時和它們發生時被顯示在卡巴斯基安全管理中心中。
- **事件類型 ID**。該數碼在您使用協力廠商工具分析事件時使用。
- **事件類型**（字母碼）。該代碼用於您使用卡巴斯基安全管理中心資料庫中提供的公共視圖瀏覽和處理事件時以及事件被匯出到 SIEM 系統時。

- **敘述**。該文字包含事件發生的情況以及此種情況下您可以做的事。
- **預設儲存期限**。這是事件儲存在管理伺服器資料庫的天數，顯示在管理伺服器事件清單中。該時間段之後，事件被刪除。如果事件儲存期限值是 0，此類事件被偵測但不顯示在管理伺服器事件清單。如果您設定了儲存此類事件到作業系統事件記錄，您可以在那裡找到它們。

  您可以變更事件儲存期限：

  - 管理主控台：設定事件儲存期限
  - 卡巴斯基安全管理中心網頁主控台：設定事件儲存期限

其他資料可能包含以下欄位：

- **event_id**：資料庫中獨特的事件編號，由系統自動產生與指派；請勿與**事件類型 ID** 混淆。
- **Task_id**：造成事件發生的工作 ID（如有）
- **severity**：其中一個以下嚴重等級（以嚴重等級的遞增順序排列）：

  0) 無效的嚴重等級

  1) 資訊

  2) 警告

  3) 錯誤

  4) 緊急

管理伺服器事件

該部分包含管理伺服器相關事件資訊。

管理伺服器緊急事件

下表顯示具有**緊急**重要等級的卡巴斯基安全管理中心管理伺服器事件類型。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。對於管理伺服器，您還可以在管理伺服器屬性中檢視和設定事件清單。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

如果您在管理主控台的管理伺服器內容視窗中指定了連接埠，**卡巴斯基安全管理中心會發布其指標**和關鍵事件，以供 Prometheus（一個用於監控和警報的系統）取得。Prometheus 取得指標和關鍵事件，然後為每個事件產生警報。

// KL.KSC.Common—Kaspersky Security Center common counters

"xdr_klserver_errors", "counter", "klserver errors"

"xdr_klserver_api_calls_time", "counter", "klserver api calls time"

// KL.KSC.Transport—Transport counters set

"ksc_Transport__Number_of_all_connections", "counter", "number of all connections"

"ksc_Transport__Number_of_all_nagent_connection", "counter", "number of all Network Agent connection"

"ksc_Transport__Number_of_controlled_nagent_connections", "counter", "number of controlled Network Agent connections"

"ksc_Transport__Total_active_hosts_count", "gauge", "total active devices count"

"ksc_Transport__Number_of_pings_processed", "counter", "number of pings processed"

"ksc_Transport__Number_of_pings_rejected", "counter", "number of pings rejected"

"ksc_Transport__Number_of_ping_processing_errors", "counter", "number of ping processing errors"

"ksc_Transport__Number_of_TCP_connections_accepted", "counter", "number of TCP connections accepted"

"ksc_Transport__Number_of_failed_TCP_connections", "counter", "number of failed TCP connections"

"ksc_Transport__Bytes_sent_by_TCP", "counter", "bytes sent by TCP"

"ksc_Transport__Bytes_received_by_TCP", "counter", "bytes received by TCP"

"ksc_Transport__Number_of_GetNextFileChunk_requests", "counter", "number of GetNextFileChunk requests"

"ksc_Transport__Number_of_GetNextFileChunk_rejected", "counter", "number of GetNextFileChunk rejected"

"ksc_Transport__Bytes_transmitted_through_GetNextFileChunk", "counter", "bytes transmitted through GetNextFileChunk"

// KL.KSC.Events—Events delivery counters set

"ksc_Events__Number_of_event_bulks_processed", "counter", "number of event bulks processed"

"ksc_Events__Number_of_event_bulks_rejected", "counter", "number of event bulks rejected"

"ksc_Events__Number_of_event_bulks_processing_errors", "counter", "number of event bulks processing errors"

"ksc_Events__Number_of_event_bulks_processing_just_now", "gauge", "number of event bulks processing just now"

"ksc_Events__Number_of_events_processed", "counter", "number of events processed"

"ksc_Events__Number_of_events_rejected", "counter", "number of events rejected"

"ksc_Events__Number_of_events_processing_errors", "counter", "number of events processing errors"

"ksc_Events__Number_of_events_processing_just_now", "gauge", "number of events processing just now"

// KL.KSC.Resources—Kaspersky Security Center resources usage

"ksc_Resources__CPU_time_in_user_mode", "counter", "CPU time in user mode"

"ksc_Resources__CPU_time_in_kernel_mode", "counter", "CPU time in kernel mode"

"ksc_Resources__PID_of_klserver_process", "gauge", "process ID of klserver"

"ksc_Resources__PID_of_klnagent_process", "gauge", "process ID of klnagent"

"ksc_Resources__Available_disk_user_quota_for_server_data", "gauge", "available disk user quota for server data"

"ksc_Resources__Available_disk_user_quota_for_packages", "gauge", "available disk user quota for packages"

"ksc_Resources__Current_OpenAPI_threads_count", "counter", "current OpenAPI threads count"

"ksc_Resources__Maximum_OpenAPI_threads_count", "counter", "maximum OpenAPI threads count"

// KL.KSC.NLST

// KL.KSC.NLST.Trans.Common—List of server transactions

"ksc_NLST__Common__Current_transactions_count", "gauge", "current transactions count"

"ksc_NLST__Common__Transactions_queue_ful", "gauge", "transactions queue full"

"ksc_NLST__Common__Transactions_queue_near_to_ful", "gauge", "transactions queue near to full"

// KL.KSC.NLST.InvAppCtrlLink—Application Control link

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvSoft—Software Inventory

"ksc_NLST__Software_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Software_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Software_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Software_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Software_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Software_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Software_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Software_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Software_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvHard—Hardware Inventory

"ksc_NLST__Hardware_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Hardware_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Hardware_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Hardware_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Hardware_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Hardware_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Hardware_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Hardware_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Hardware_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DevCtrl—Device Control

"ksc_NLST__Device_control__items_changed", "gauge", "items changed"

"ksc_NLST__Device_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_control__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDM—Mobile Device Management

"ksc_NLST__Mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__Mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDMmails—Device management emails

"ksc_NLST__Device_management_emails__items_changed", "gauge", "items changed"

"ksc_NLST__Device_management_emails__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_management_emails__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_management_emails__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_management_emails__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_management_emails__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_management_emails__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_management_emails__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_management_emails__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AppCtrl—Application Control

"ksc_NLST__Application_control__items_changed", "gauge", "items changed"

"ksc_NLST__Application_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_control__transactions_in_queue", "gauge", "transactions in queue"

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DPEErrors—Data protection errors

"ksc_NLST__Data_protection_errors__items_changed", "gauge", "items changed"

"ksc_NLST__Data_protection_errors__items_deleted", "gauge", "items deleted"

"ksc_NLST__Data_protection_errors__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Data_protection_errors__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Data_protection_errors__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Data_protection_errors__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Data_protection_errors__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Data_protection_errors__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Data_protection_errors__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.iOsMDM—iOS Mobile Device Management

"ksc_NLST__iOS_mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__iOS_mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__iOS_mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__iOS_mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__iOS_mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__iOS_mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__iOS_mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Vapm—Vulnerability assessment and patch management

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment_and_patch_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment_and_patch_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Va—Vulnerability assessment

"ksc_NLST__Vulnerability_assesment__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.VM—Virtual machines

"ksc_NLST__Virtual_machines__items_changed", "gauge", "items changed"

"ksc_NLST__Virtual_machines__items_deleted", "gauge", "items deleted"

"ksc_NLST__Virtual_machines__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Virtual_machines__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Virtual_machines__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Virtual_machines__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Virtual_machines__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Virtual_machines__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Virtual_machines__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.WUS—Windows Update

"ksc_NLST__Windows_update__items_changed", "gauge", "items changed"

"ksc_NLST__Windows_update__items_deleted", "gauge", "items deleted"

"ksc_NLST__Windows_update__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Windows_update__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Windows_update__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Windows_update__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Windows_update__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Windows_update__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Windows_update__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.CIP_PLC—CIP PLC

"ksc_NLST__CIP_PLC__items_changed", "gauge", "items changed"

"ksc_NLST__CIP_PLC__items_deleted", "gauge", "items deleted"

"ksc_NLST__CIP_PLC__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__CIP_PLC__change_item_operations", "gauge", "change item operations"

"ksc_NLST__CIP_PLC__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__CIP_PLC__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__CIP_PLC__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__CIP_PLC__list_is_pending", "gauge", "list is pending"

"ksc_NLST__CIP_PLC__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.NagentNetScan—Network Agent Network Scan

"ksc_NLST__Network_scan__items_changed", "gauge", "items changed"

"ksc_NLST__Network_scan__items_deleted", "gauge", "items deleted"

"ksc_NLST__Network_scan__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Network_scan__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Network_scan__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Network_scan__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Network_scan__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Network_scan__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Network_scan__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AS—Adaptive Security

"ksc_NLST__Adaptive_security__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.ASS—Adaptive Security State

"ksc_NLST__Adaptive_security_state__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security_state__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security_state__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security_state__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security_state__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security_state__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security_state__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security_state__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security_state__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.KillChain—Kill Chain

"ksc_NLST__Kill_chain__items_changed", "gauge", "items changed"

"ksc_NLST__Kill_chain__items_deleted", "gauge", "items deleted"

"ksc_NLST__Kill_chain__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Kill_chain__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Kill_chain__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Kill_chain__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Kill_chain__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Kill_chain__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Kill_chain__transactions_in_queue", "gauge", "transactions in queue"

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
已超過產品授權數量限制	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	每天一次，卡巴斯基安全管理中心 Linux 檢查是否超過產品授權限制。 當管理伺服器發現安裝在用戶端裝置上的 Kaspersky 應用程式超過了產品授權限制，以及由單一產品授權覆寫的目前使用的產品授權單元數量超過了該產品授權覆寫的單元總數的 110%，則該類型的事件發生。 即便當該事件發生時，用戶端裝置是被防護的。 您可以透過以下方式回應事件： • 檢視受管理裝置清單。刪除不在使用的裝置。 • 為更多裝置提供產品授權（新增有效的啟動碼或金鑰檔案至管理伺服器）。 卡巴斯基安全管理中心決定當產品授權限制被超過時產生事件的規則。	180 天
病毒爆發	26（對於檔案威脅防護）	GNRL_EV_VIRUS_OUTBREAK	當短時間內在若干受管理裝置上偵測到的惡意物件數量超過上限值時，該類型的事件發生。 您可以透過以下方式回應事件： • 您可以在管理伺服器內容中配置上限值。 • 您也可以建立嚴格政策以便被啟動，或者建立工作以便在事件發生時執行。	180 天
病毒爆發	27（對於郵件威脅防護）	GNRL_EV_VIRUS_OUTBREAK	當短時間內在若干受管理裝置上偵測到的惡意物件數量超過上限值時，該類型的事件發生。 您可以透過以下方式回應事件： • 您可以在管理伺服器內容中配置上限值。 • 您也可以建立嚴格政策以便被啟動，或者建立工作以便在事件發生時執行。	180 天
病毒爆發	28（對於防火牆）	GNRL_EV_VIRUS_OUTBREAK	當短時間內在若干受管理裝置上偵測到的惡意物件數量超過上限值時，該類型的事件發生。 您可以透過以下方式回應事件： • 您可以在管理伺服器內容中配置上限值。 • 您也可以建立嚴格政策以便被啟動，或者建立工作以便在事件發生時執行。	180 天
裝置已失去管理	4111	KLSRV_HOST_OUT_CONTROL	如果受管理裝置在網路中可見，但一定時間未連線到管理伺服器，則該類型的事件發生。 找到什麼封鎖了裝置上網路代理的正常功能。可能的原因包括網路問題和從裝置移除網路代理。	180 天
裝置狀態為"緊急"	4113	KLSRV_HOST_STATUS_CRITICAL	當受管理裝置被分配緊急狀態時，該類型的事件發生。您可設定裝置狀態要變更為緊急的條件。	180 天
金鑰檔案已新增到黑名單	4124	KLSRV_LICENSE_BLACKLISTED	當 Kaspersky 已新增您使用的啟動碼或金鑰檔案到拒絕清單時，會發生該類型的事件。 聯絡技術支援獲得更多詳情。	180 天
受限功能模式	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	當卡巴斯基安全管理中心開始用基本功能操作，沒有"弱點和修補程式管理"和"行動裝置管理"功能時，該類型的事件發生。 以下是事件發生的原因和正確回應： • 產品授權期限已到期。提供授權以使用卡巴斯基安全管理中心的完整功能模式（新增有效的啟動碼或金鑰檔案到管理伺服器）。 • 管理伺服器管理比產品授權限制更多的裝置。從管理伺服器的管理群組移動裝置到其他管理伺服器的管理群組（如果其他管理伺服器的產品授權限制允許）。	180 天

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
產品授權即將到期	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	當接近商業授權到期日時，就會發生此類事件。 卡巴斯基安全管理中心每天會檢查一次產品授權是否接近到期日。此類事件會在產品授權到期日期前 30 天、15 天、5 天和 1 天發布。您不能變更天數。如果管理伺服器在許可證到期日期前的指定日期關閉，則事件將在第二天發布。 當商業授權到期時，卡巴斯基安全管理中心僅提供基本功能。 您可以透過以下方式回應事件： • 請確保將備用產品授權金鑰新增到管理伺服器。 • 如果您使用訂購方案，請確保續訂該方案。無限制訂購如果已經預付給服務提供商了，則會在到期日自動續約。	180 天
憑證已到期	4132	KLSRV_CERTIFICATE_EXPIRED	當行動裝置上的用戶端憑證過期時，就會發生此類事件。	180 天
Kaspersky 軟體模組更新已撤銷	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	如果無縫更新被 Kaspersky 技術專家撤銷（這些更新顯示*已撤銷*狀態）；例如，它們必須被更新到新版本，則該類型的事件發生。該事件涉及卡巴斯基安全管理中心修補程式且不涉及 Kaspersky 受管理應用程式模組。事件提供無縫更新未被安裝的原因。	180 天

管理伺服器功能失效事件

下表顯示有**功能失效**重要等級的卡巴斯基安全管理中心管理伺服器事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。對於管理伺服器，您還可以在管理伺服器屬性中檢視和設定事件清單。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

管理伺服器功能失效事件

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
執行時錯誤	4125	KLSRV_RUNTIME_ERROR	由於未知問題，該類型的事件發生。 多數情況下，這些是 DBMS 問題、網路問題和其他軟體和硬體問題。 事件詳情可以在事件描述中找到。	180 天
其中一個已授權應用程式群組已超過最大安裝數量	4126	KLSRV_INVLICPROD_EXCEDED	管理伺服器定期產生該類型的事件（每小時）。如果在卡巴斯基安全管理中心中，您管理協力廠商應用程式的授權金鑰，以及如果安裝數量超過了協力廠商應用程式授權金鑰設定的限制，則會發生該類型的事件。 您可以透過以下方式回應事件： • 檢視受管理裝置清單。從未使用協力廠商應用程式的裝置上移除該應用程式。 • 為更多裝置使用協力廠商產品授權。 您可以使用已授權應用程式群組的功能管理協力廠商應用程式的產品授權金鑰。這是一組由滿足您所設標準的協力廠商應用程式組成的授權應用程式群組。	180 天
輪詢雲端區段失敗	4143	KLSRV_KLCLOUD_SCAN_ERROR	當管理伺服器無法在雲端環境中輪詢網路區段時，將發生此類事件。讀取事件敘述中的詳細資訊，並據此做出回應。	未儲存

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
將更新複製到指定資料夾失敗	4123	KLSRV_UPD_REPL_FAIL	當軟體更新被複製到附加分享資料夾時，該類型的事件發生。 您可以透過以下方式回應事件： • 檢查用於獲取資料夾存取的使用者帳戶是否具有寫權限。 • 檢查資料夾的使用者名稱和 / 或金鑰是否變更。 • 檢查網際網路連線，因為它可能是事件原因。遵照指示更新資料庫和軟體模組。	180 天
沒有剩餘硬碟空間	4107	KLSRV_DISK_FULL	當安裝管理伺服器的裝置磁碟空間不足時，就會發生此類事件。 釋出裝置上的磁碟空間。	180 天
共用資料夾無法使用	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	如果管理伺服器共用資料夾不可用，則該類型的事件發生。 您可以透過以下方式回應事件： • 檢查管理伺服器（共用資料夾所在位置）是否已開啟並可用。 • 檢查資料夾的使用者名稱和 / 或金鑰是否變更。 • 檢查網路連線。	180 天
管理伺服器資料庫無法使用	4109	KLSRV_DATABASE_UNAVAILABLE	如果管理伺服器資料庫不可用則該類型的事件發生。 您可以透過以下方式回應事件： • 檢查安裝了 SQL Server 的遠端伺服器是否可用。 • 檢視 DBMS 記錄以發現管理伺服器資料庫不可用的原因。例如，因為維護，安裝了 SQL Server 的遠端伺服器可能不可用。	180 天
管理伺服器資料庫空間不足	4110	KLSRV_DATABASE_FULL	當管理伺服器資料庫沒有剩餘空間時，該類型的事件發生。 當管理伺服器的資料庫達到其容量，以及當不可能再往資料庫記錄時，管理伺服器不工作。 以下是根據您使用的 DBMS，該事件的原因，以及到該事件的正確回應： • 您使用 SQL Server Express 版本 DBMS： 在 SQL Server Express 文件中，檢查您使用版本的資料庫大小限制。可能您的管理伺服器資料庫已超過了資料庫大小限制。 限制儲存在管理伺服器資料庫的事件數量。 在管理伺服器資料庫中有太多由應用程式控制元件傳送的事件。您可以變更關於管理伺服器資料庫中應用程式事件儲存的 Kaspersky Endpoint Security for Windows 政策設定。 • 您使用 DBMS 而不是 SQL Server Express Edition： 不限制儲存在管理伺服器資料庫的事件數量。 降低儲存在管理伺服器資料庫的事件數量。 在 DBMS 選項處檢視資訊。	180 天

管理伺服器警告事件

下表顯示具有**警告**重要等級的卡巴斯基安全管理中心管理伺服器事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。對於管理伺服器，您還可以在管理伺服器屬性中檢視和設定事件清單。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
已偵測到頻繁事件		KLSRV_EVENT_SPAM_EVENTS_DETECTED	當管理伺服器在受管理裝置上偵測到頻繁發生的事件時，就會發生這種類型的事件。有關詳細資訊，請參閱以下部分： 阻止頻繁事件。	90 天
已超過產品授權數量限制	4098	KLSRV_EV_LICENSE_CHECK_100_110	每天一次，卡巴斯基安全管理中心 Linux 檢查是否超過產品授權限制。 當管理伺服器發現安裝在用戶端裝置上的 Kaspersky 應用程式超過了產品授權限制，以及由單一產品授權覆寫的目前使用的產品授權單元數量達到了該產品授權覆寫的單元總數的 100% 到 110%，則該類型的事件發生。 即便當該事件發生時，用戶端裝置是被防護的。 您可以透過以下方式回應事件： • 檢視受管理裝置清單。刪除不在使用的裝置。 • 為更多裝置提供產品授權（新增有效的啟動碼或金鑰檔案至管理伺服器）。 卡巴斯基安全管理中心決定當產品授權限制被超過時產生事件的規則。	90 天
裝置在網路上已長時間沒有活動	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	當受管理裝置顯示閒置狀態時，有時會發生該類型的事件。 最常在停用受管理裝置時發生。 您可以透過以下方式回應事件： • 要從受管理裝置清單中手動刪除裝置。 • 指定系統使用管理主控台或使用卡巴斯基安全管理中心網頁主控台建立**裝置在網路上已長時間沒有活動**事件後的時間間隔。 • 指定使用管理主控台或卡巴斯基安全管理中心網頁主控台將裝置自動從群組中刪除的時間間隔。	90 天
裝置名稱衝突	4102	KLSRV_EVENT_HOSTS_CONFLICT	當管理伺服器將兩個或更多受管理裝置視為單一裝置時，會發生此類事件。 當複製的硬碟用在受管理裝置上進行軟體佈署，並且沒有將網路代理切換到參考裝置上的專用磁碟複製模式時，通常會發生這種情況。 為避免此問題，請在複製該裝置硬碟之前將網路代理切換到參考裝置上的磁碟複製模式。	90 天
裝置狀態為“警告”	4114	KLSRV_HOST_STATUS_WARNING	當受管理裝置被分配*警告*狀態時，該類型的事件發生。您可設定裝置狀態要變更為*警告*的條件。	90 天
其中一個已授權應用程式群組總數即將超過最大安裝數量	4127	KLSRV_INVLICPROD_FILLED	當已授權應用程式群組中包含的協力廠商應用程式的安裝數量達到產品授權金鑰屬性中指定之最大允許值的 90% 時，將發生此類事件。 您可以透過以下方式回應事件： • 如果某些受管理裝置上未使用協力廠商應用程式，請從這些裝置上刪除該應用程式。 • 如果您預計協力廠商應用程式的安裝數量將在不久的將來超過允許的最大值，請考慮預先獲取更多裝置的協力廠商授權。 您可以使用已授權應用程式群組的功能管理協力廠商應用程式的產品授權金鑰。	90 天
憑證已被請求	4133	KLSRV_CERTIFICATE_REQUESTED	當無法自動重新發佈行動裝置管理憑證時，將發生此類事件。 以下可能是事件的原因和適當的回應： • 對憑證啟動了自動重新簽發，但憑證的**如果可能，自動重新發佈憑證**選項已停用。這可能是由於建立憑證期間發生的錯誤。可能需要手動重新發佈憑證。 • 如果您使用與公開金鑰基礎架構的整合，則可能是由於缺少適用於與 PKI 整合和發佈憑證之帳戶的 SAM-Account-Name 屬性。檢視帳戶屬性。	90 天

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
憑證已刪除	4134	KLSRV_CERTIFICATE_REMOVED	當管理員為行動裝置管理移除任何類型的憑證（一般、郵件、VPN）時，會發生此類事件。 移除憑證後，透過此憑證連線的行動裝置將無法連線到管理伺服器。 在調查與行動裝置管理相關的故障時，此事件可能會有所幫助。	90 天
憑證將到期	6128	ServerCertificateExpiresSoon	當行動裝置和 UEFI 裝置的管理伺服器憑證過期時，會發生此類事件。 您需要更新過期的憑證。	90 天
APNs 憑證已到期	4135	KLSRV_APN_CERTIFICATE_EXPIRED	當 APNs 憑證過期時，會發生此類事件。 您需要手動續訂 APNs 憑證並將其安裝在 iOS MDM 伺服器上。	未儲存
APNs 憑證即將到期	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	當 APNs 憑證剩餘時間不足 14 天時，就會發生此類事件。 當 APNs 憑證到期時，您需要手動續訂 APNs 憑證並將其安裝在 iOS MDM 伺服器上。 建議您在到期日之前安排續訂 APNs 憑證。	未儲存
傳送 FCM 訊息到行動裝置失敗	4138	KLSRV_GCM_DEVICE_ERROR	當行動裝置管理被配置使用 Firebase Cloud Messaging (FCM) 連線到具有 Android 作業系統的受管理行動裝置並且 FCM 伺服器無法處理從管理伺服器收到的某些要求時，會發生此類事件。這意味著某些受管理行動裝置將不會收到推送通知。 讀取事件事件敘述詳細資訊中的 HTTP 程式碼，並據此做出回應。如需從 FCM 伺服器接收到的 HTTP 程式碼以及相關錯誤的詳細資訊，請參閱 Firebase 服務文件（請參閱「下游訊息錯誤回應程式碼」一章）。	90 天
傳送 FCM 訊息到 FCM 伺服器時發生 HTTP 錯誤	4139	KLSRV_GCM_HTTP_ERROR	當行動裝置管理被配置使用 Firebase Cloud Messaging (FCM) 連線到具有 Android 作業系統的受管理行動裝置並且 FCM 伺服器透過 200 (OK) 以外的 HTTP 程式碼還原管理伺服器的要求時，會發生此類事件。 以下可能是事件的原因和適當的回應： • FCM 伺服器端出現問題。讀取事件事件敘述詳細資訊中的 HTTP 程式碼，並據此做出回應。如需從 FCM 伺服器接收到的 HTTP 程式碼以及相關錯誤的詳細資訊，請參閱 Firebase 服務文件（請參閱「下游訊息錯誤回應程式碼」一章）。 • 代理伺服器端的問題（如果使用代理伺服器）。讀取事件事件敘述詳細資訊中的 HTTP 程式碼，並據此做出回應。	90 天
傳送 FCM 訊息到 FCM 伺服器失敗	4140	KLSRV_GCM_GENERAL_ERROR	使用 Firebase Cloud Messaging HTTP 通訊協定時，由於管理伺服器端發生意外錯誤，因此會發生此類事件。 讀取事件敘述中的詳細資訊，並據此做出回應。 如果您自己找不到問題的解決方案，建議您與卡巴斯基技術支援聯絡。	90 天
硬碟剩餘空間少	4105	KLSRV_NO_SPACE_ON_VOLUMES	當安裝管理伺服器的裝置硬碟空間不足時，就會發生此類事件。 釋出裝置上的磁碟空間。	90 天

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
管理伺服器資料庫的剩餘空間少	4106	KLSRV_NO_SPACE_IN_DATABASE	如果管理伺服器資料庫受限制則該類型的事件發生。如果您不糾正情況，管理伺服器資料庫就將達到其容量且管理伺服器將不工作。 以下是根據您使用的 DBMS，該事件的原因，以及到該事件的正確回應。 您使用 SQL Server Express 版本 DBMS： • 在 SQL Server Express 文件中，檢查您使用版本的資料庫大小限制。可能您的管理伺服器資料庫即將超過資料庫大小限制。 • 限制儲存在管理伺服器資料庫的事件數量。 • 在管理伺服器資料庫中有太多由應用程式控制元件傳送的事件。您可以變更關於管理伺服器資料庫中應用程式事件儲存的 Kaspersky Endpoint Security for Windows 政策設定。 您使用 DBMS 而不是 SQL Server Express Edition： • 不限制儲存在管理伺服器資料庫的事件數量 • 降低儲存在管理伺服器資料庫的事件數量 在 DBMS 選項處檢視資訊。	90 天
連到從屬管理伺服器的連線已中斷	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	當與次要管理伺服器的連線中斷時，會發生此類事件。 在安裝了次要管理伺服器的裝置上讀取卡巴斯基事件記錄，並據此做出回應。	90 天
連到主管理伺服器的連線已中斷	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	當與主要管理伺服器的連線中斷時，會發生此類事件。 在安裝了主要管理伺服器的裝置上讀取卡巴斯基事件記錄，並據此做出回應。	90 天
已註冊 Kaspersky 軟體模組的新更新	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	當管理伺服器為需要批准安裝的受管理裝置上安裝的 Kaspersky 軟體註冊新更新時，將發生此類事件。 使用管理主控台或卡巴斯基安全管理中心網頁主控台核准或拒絕更新。	90 天
超過資料庫中的事件數量限制，刪除事件開始	4145	KLSRV_EVP_DB_TRUNCATING	當從管理伺服器資料庫刪除舊事件在管理伺服器資料庫達到容量後開始時，該類型的事件發生。 您可以透過以下方式回應事件： • 變更儲存在管理伺服器資料庫的事件數量上限 • 降低儲存在管理伺服器資料庫的事件數量	未儲存
超過資料庫中的事件數量限制，事件已被刪除	4146	KLSRV_EVP_DB_TRUNCATED	當從管理伺服器資料庫刪除舊事件在管理伺服器資料庫達到容量後完成時，該類型的事件發生。 您可以透過以下方式回應事件： • 變更允許儲存在管理伺服器資料庫的事件數量上限 • 降低儲存在管理伺服器資料庫的事件數量	未儲存
自動簽發憑證失敗		KLSRV_CERTIFICATE_AUTO_ISSUE_ERROR	如果為行動裝置（在行動協定下執行的裝置）建立用戶端憑證時發生錯誤，則會發生此事件。	90 天

管理伺服器資訊事件

下表顯示具有 **資訊**重要等級的卡巴斯基安全管理中心管理伺服器事件。

管理伺服器資訊事件

事件類型顯示名稱	事件類型 ID	事件類型	預設儲存期限	評論
產品授權金鑰的 90% 已經使用	4097	KLSRV_EV_LICENSE_CHECK_90	30 天	
已偵測到新裝置	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 天	

事件類型顯示名稱	事件類型 ID	事件類型	預設儲存期限	評論
裝置已被自動新增到群組	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 天	
裝置已從群組中刪除：長時間在網路中不活動	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 天	
已授權應用程式群組之一的安裝即將超過限制（已經使用 95% 以上）	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 天	
找到了要傳送至 Kaspersky 以分析的檔案	4131	KLSRV_APS_FILE_APPEARED	30 天	
此行動裝置上的 FCM 實例 ID 已被變更	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 天	
更新被成功複製至指定的資料夾	4122	KLSRV_UPD_REPL_OK	30 天	
連到從屬管理伺服器的連線已建立	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 天	
連到主管理伺服器的連線已建立	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 天	
資料庫已更新	4144	KLSRV_UPD_BASES_UPDATED	30 天	
稽核：到管理伺服器的連線已建立	4147	KLAUD_EV_SERVERCONNECT	30 天	
稽核：物件已修改	4148	KLAUD_EV_OBJECTMODIFY	30 天	此事件追蹤以下物件的變更： • 管理群組 • 安全群組 • 使用者 • 套件 • 工作 • 政策 • 伺服器 • 虛擬伺服器
稽核：物件狀態已修改	4150	KLAUD_EV_TASK_STATE_CHANGED	30 天	例如，當工作因錯誤而失敗時會發生此事件。
稽核：群組設定已修改	4149	KLAUD_EV_ADMGROUP_CHANGED	30 天	
稽核：連到管理伺服器的連線已終止	4151	KLAUD_EV_SERVERDISCONNECT	30 天	
稽核：物件內容已修改	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 天	此事件追蹤以下屬性的變更： • 使用者 • 產品授權 • 伺服器 • 虛擬伺服器
稽核：使用者權限已修改	4153	KLAUD_EV_OBJECTACLMODIFIED	30 天	

事件類型顯示名稱	事件類型 ID	事件類型	預設儲存期限	評論
稽核：加密金鑰已從管理伺服器匯入或者匯出	5100	KLAUD_EV_DPEKEYSEXPORT	30 天	
憑證已成功自動簽發		KLSRV_CERTIFICATE_AUTO_ISSUED	30 天	當成功建立行動裝置（在行動協定下執行的裝置）的憑證時，會發生此事件。 只有在針對行動裝置和 UEFI 裝置的管理伺服器行動憑證執行與該事件對應的操作時，該事件才會由管理伺服器自動發佈並顯示在管理主控台中。

網路代理事件

該部分包含網路代理相關事件資訊。

網路代理功能失效事件

下表顯示具有**功能失效**嚴重等級的卡巴斯基安全管理中心網路代理事件類型。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

網路代理功能失效事件

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
更新安裝錯誤	7702	KLNAG_EV_PATCH_INSTALL_ERROR	如果卡巴斯基安全管理中心元件自動更新和修補程式未成功，則該類型的事件發生。事件不包含受管理的 Kaspersky 應用程式的更新。 閱讀事件描述。管理伺服器上的 Windows 問題可能是該事件的原因。如果描述提到 Windows 配置的任何問題，解決該問題。	30 天
安裝協力廠商軟體更新失敗	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	如果"弱點和修補程式管理"和"行動裝置管理"功能正在使用且協力廠商軟體更新未成功，則該類型的事件發生。 檢查到協力廠商軟體的連結是否合法。閱讀事件描述。	30 天
安裝 Windows Update 更新失敗	7717	KLNAG_EV_WUA_INSTALL_ERROR	如果 Windows 更新未成功，則該類型的事件發生。在網路代理政策中配置 Windows 更新。 閱讀事件描述。在 Microsoft 知識庫中尋找錯誤。如果您無法自己解決問題，請聯絡 Microsoft 技術支援。	30 天

網路代理警告事件

下表顯示具有**警告**嚴重等級的卡巴斯基安全管理中心網路代理事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

網路代理警告事件

事件類型顯示名稱	事件類型 ID	事件類型	預設儲存期限
在安裝軟體模組更新期間返回了警告	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 天
協力廠商軟體更新安裝已完成但存在警告	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 天

事件類型顯示名稱	事件類型 ID	事件類型	預設儲存期限
協力廠商軟體更新已延時	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 天
發生了事件	549	GNRL_EV_APP_INCIDENT_OCCURED	30 天
KSN 代理已啟動。檢查 KSN 可用性失敗	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 天

網路代理資訊事件

下表顯示具有**資訊**嚴重等級的卡巴斯基安全管理中心網路代理事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

網路代理資訊事件

事件類型顯示名稱	事件類型 ID	事件類型	預設儲存期限
軟體模組更新已成功安裝	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 天
軟體模組更新安裝已啟動	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 天
應用程式已安裝	7703	KLNAG_EV_INV_APP_INSTALLED	30 天
應用程式已解除安裝	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 天
已安裝監控的應用程式	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 天
已解除安裝監控的應用程式	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 天
已安裝協力廠商應用程式	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 天
已新增裝置	7708	KLNAG_EV_DEVICE_ARRIVAL	30 天
裝置已被刪除	7709	KLNAG_EV_DEVICE_REMOVE	30 天
已偵測到新裝置	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 天
裝置已被授權	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 天
Windows 共用桌面：檔案已讀取	7712	KLUSRLOG_EV_FILE_READ	30 天
Windows 共用桌面：檔案已修改	7713	KLUSRLOG_EV_FILE_MODIFIED	30 天
Windows 共用桌面：應用程式已啟動	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 天
Windows 共用桌面：已啟動	7715	KLUSRLOG_EV_WDS_BEGIN	30 天
Windows 共用桌面：已停止	7716	KLUSRLOG_EV_WDS_END	30 天
協力廠商軟體更新已成功安裝	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 天
協力廠商軟體更新安裝已開始	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 天
KSN 代理已啟動。KSN 可用性檢查已成功完成	7719	KSNPROXY_STARTED_CON_CHK_OK	30 天
KSN 代理已停止	7720	KSNPROXY_STOPPED	30 天

iOS MDM 伺服器事件

該部分包含 iOS MDM 伺服器相關事件資訊。

iOS MDM 伺服器功能失效事件

下表顯示有**功能失效**嚴重等級的卡巴斯基安全管理中心 iOS MDM 伺服器事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

iOS MDM 伺服器功能失效事件

事件類型顯示名稱	事件類型	預設儲存期限
請求設定檔清單失敗	設定檔清單_指令_失敗	30 天
安裝設定檔失敗	安裝設定檔_指令_失敗	30 天
刪除設定檔失敗	刪除設定檔_指令_失敗	30 天
請求 provisioning 設定檔清單失敗	PROVISIONING 設定檔清單_指令_失敗	30 天
安裝 provisioning 設定檔失敗	安裝 PROVISIONING 設定檔_指令_失敗	30 天
刪除 provisioning 設定檔失敗	刪除 PROVISIONING 設定檔_指令_失敗	30 天
請求數位憑證清單失敗	憑證清單_指令_失敗	30 天
請求已安裝應用程式清單失敗	已安裝應用程式清單_指令_失敗	30 天
請求行動裝置一般資訊失敗	裝置資訊_指令_失敗	30 天
請求安全資訊失敗	安全資訊_指令_失敗	30 天
鎖定行動裝置失敗	裝置鎖_指令_失敗	30 天
重設密碼失敗	清除密碼_指令_失敗	30 天
從行動裝置抹除資料失敗	抹除裝置_指令_失敗	30 天
安裝應用失敗	安裝應用程式_指令_失敗	30 天
為應用設定兌換碼失敗	應用兌換碼_指令_失敗	30 天
請求受管理應用清單失敗	受管理應用程式清單_指令_失敗	30 天
刪除受管理應用失敗	移除應用程式_指令_失敗	30 天
漫遊設定已被拒絕	設定漫遊設定_指令_失敗	30 天
應用操作中發生錯誤	產品_失敗	30 天
指令結果包含無效資料	畸形_指令	30 天
傳送推送通知失敗	傳送_推送_通知_失敗	30 天
傳送指令失敗	傳送_指令_失敗	30 天
未找到裝置	裝置_未_發現	30 天

iOS MDM 伺服器警告事件

下表顯示有**警告**嚴重等級的卡巴斯基安全管理中心 iOS MDM 伺服器事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

iOS MDM 伺服器警告事件

事件類型顯示名稱	事件類型	預設儲存期限
偵測到連線鎖定行動裝置的企圖	不活動_裝置_嘗試_已連線	30 天
設定檔已被刪除	MDM_設定檔_已_被刪除	30 天
偵測到重新使用用戶端憑證的企圖	用戶端_憑證_已_在_使用	30 天
偵測到不活動裝置	發現_不活動_裝置	30 天
兌換碼已請求	需要_兌換_碼	30 天
設定檔已被包含到從裝置刪除的政策	UMDM_設定檔_已_被刪除	30 天

iOS MDM 伺服器資訊事件

下表顯示有**資訊**嚴重等級的卡巴斯基安全管理中心 iOS MDM 伺服器事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

iOS MDM 伺服器資訊事件

事件類型顯示名稱	事件類型	預設儲存期限
新行動裝置已被連線	新_裝置_已連線	30 天
設定檔清單已被成功請求	設定檔清單_指令_成功	30 天
設定檔已被成功安裝	安裝設定檔_指令_成功	30 天
設定檔已被成功刪除	刪除設定檔_指令_成功	30 天
Provisioning 設定檔清單已被成功請求	PROVISIONING 設定檔清單_指令_成功	30 天
Provisioning 設定檔已被成功安裝	安裝 PROVISIONING 設定檔_指令_成功	30 天
Provisioning 設定檔已被成功刪除	刪除 PROVISIONING 設定檔_指令_成功	30 天
數位憑證清單已被成功請求	憑證清單_指令_成功	30 天
已安裝應用程式清單已被成功請求	已安裝應用程式清單_指令_成功	30 天
行動裝置一般資訊已被成功請求	裝置資訊_指令_成功	30 天
安全資訊已被成功請求	安全資訊_指令_成功	30 天
行動裝置已被成功鎖定	裝置鎖_指令_成功	30 天
密碼已被成功重設	清除密碼_指令_成功	30 天
資料已被從行動裝置成功抹除	抹除裝置_指令_成功	30 天
應用已被成功安裝	安裝應用程式_指令_成功	30 天
兌換碼已為應用成功設定	應用兌換碼_指令_成功	30 天
受管理應用清單已被成功請求	受管理應用程式清單_指令_成功	30 天
受管理應用已被成功刪除	刪除應用程式_指令_成功	30 天
漫遊設定已被成功應用	設定漫遊設定_指令_成功	30 天

Exchange 行動裝置伺服器事件

該部分包含 Exchange 行動裝置伺服器相關事件資訊。

Exchange 行動裝置伺服器功能失效事件

下表顯示具有**功能失效**嚴重等級的卡巴斯基安全管理中心 Exchange 行動裝置伺服器事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

Exchange 行動裝置伺服器功能失效事件

事件類型顯示名稱	事件類型	預設儲存期限
從行動裝置抹除資料失敗	抹除_失敗	30 天
無法刪除行動裝置連線到郵箱的資訊	裝置_刪除_失敗	30 天
應用 ActiveSync 政策到郵箱失敗	政策_套用_失敗	30 天
應用程式操作錯誤	產品_失敗	30 天
修改 ActiveSync 功能狀態失敗	變更_活動_同步_狀態_失敗	30 天

Exchange 行動裝置伺服器資訊事件

下表顯示具有**資訊**嚴重等級的卡巴斯基安全管理中心 Exchange 行動裝置伺服器事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

Exchange 行動裝置伺服器資訊事件

事件類型顯示名稱	事件類型	預設儲存期限
已連線新行動裝置	新_裝置_已連線	30 天
資料已被從行動裝置成功抹除	抹除_成功	30 天

封鎖頻發事件

本節資訊說明管理頻發事件封鎖、刪除對頻發事件封鎖，以及將頻發事件清單匯出至檔案。

關於封鎖頻發事件

安裝在單個或多個受管理裝置上的受管理應用程式（例如，Kaspersky Endpoint Security for Windows）可以將許多相同類型的事件傳送到管理伺服器。接收頻繁的事件可能會使管理伺服器資料庫超載並覆寫其他事件。當所有接收到的事件數超過資料庫的指定限制時，管理伺服器將開始封鎖最頻繁的事件。

管理伺服器會封鎖自動接收頻發事件。您不能自己封鎖頻發事件，也不能選擇要封鎖的事件。

如果您想了解某個事件是否被封鎖，可以查看該事件是否存在於管理伺服器內容的**封鎖頻繁事件**區域中。在封鎖的事件中，您可以進行以下操作：

- 如果要封鎖覆寫資料庫，則可以繼續封鎖接收此類事件。
- 例如，如果要查找將頻發事件傳送到管理伺服器的原因，則可以取消封鎖頻發事件並繼續接收此類事件。
- 如果要繼續接收頻發事件直到再次被封鎖，可以從封鎖頻發事件中刪除。

管理頻發事件封鎖

管理伺服器自動封鎖接收頻發事件，但是您可以停止封鎖並繼續接收頻發事件。您還可以封鎖接收以前取消封鎖的頻繁事件。

若要管理頻發的事件封鎖：

1. 在卡巴斯基安全管理中心主控台樹狀目錄中，開啟**管理伺服器**資料夾的右鍵選單並選取**內容**。
2. 在「管理伺服器屬性」視窗中，前往**區段**窗格，然後選取**封鎖頻繁事件**。
3. 在**封鎖頻繁事件**區段中：
   - 選取**事件類型**您想要封鎖接收之事件的選項。
   - 取消選取**事件類型**您想要繼續接收之事件的選項。
4. 點擊**套用**按鈕。
5. 點擊**確定**按鈕。

管理伺服器收到您取消選取該選項**事件類型**的頻發事件，並封鎖接收您選取了該選項**事件類型**的頻發事件。

移除對頻發事件的封鎖

您可以刪除對頻發事件的封鎖並開始接收它們，直到管理伺服器再次封鎖此類頻發事件為止。

要消除對頻發事件的封鎖，請執行以下操作：

1. 在卡巴斯基安全管理中心主控台樹狀目錄中，開啟**管理伺服器**資料夾的右鍵選單並選取**內容**。
2. 在「管理伺服器屬性」視窗中，前往**區段**窗格，然後選取**封鎖頻繁事件**。
3. 在**封鎖頻繁事件**區段中，點擊要刪除其封鎖事件的頻發事件所在的資料列。
4. 點擊**刪除**按鈕。

頻發事件將從頻發事件清單中刪除。管理伺服器將接收此類型的事件。

將軟體弱點匯出至檔案中

若要將頻發事件清單匯出到檔案中，請執行以下操作：

1. 在卡巴斯基安全管理中心主控台樹狀目錄中，開啟**管理伺服器**資料夾的右鍵選單並選取**內容**。
2. 在「管理伺服器屬性」視窗中，前往**區段**窗格，然後選取**封鎖頻繁事件**。
3. 點擊**匯出至檔案**按鈕。

4. 在開啟的**儲存為**視窗中，指定您要儲存清單的檔案路徑。

5. 按一下**儲存**按鈕。

頻發事件清單上的所有記錄都會匯出到檔案中。

管控變更虛擬機的狀態

管理伺服器儲存關於受管理裝置的狀態資訊，例如硬體註冊和已安裝程式的清單，和受管理應用程式的設定、工作和政策。如果虛擬機作為受管理裝置，使用者可以隨時使用先前建立的虛擬機映像功能還原其狀態。這會造成管理伺服器上的虛擬機狀態資訊不準確。

例如，管理員已在 12:00 P.M. 於管理伺服器上建立防護政策，此政策會在12:01 P.M. 於 VM_1 虛擬機啟動。在 12:30 P.M. 時，虛擬機 VM_1 的使用者會透過在 11:00 A.M. 建立的快照模式還原以變更其狀態。防護政策會停止在虛擬機上執行。但是，管理伺服器上會儲存此保護政策繼續在 VM_1 上生效的錯誤資訊。

卡巴斯基安全管理中心允許您監控在虛擬機狀態上的所有變更。

當於每台裝置同步後，管理伺服器會產成一個獨一無二的 ID，將其儲存在裝置和管理伺服器。在啟動下次同步前，管理伺服器會比較兩端的 ID 值。如果 ID 值不比對，則管理伺服器會認為虛擬機已經從映像還原。管理伺服器會重設在此虛擬機上啟動的所有政策和工作設定，並向其傳送最新的政策和群組工作。

使用系統登錄檔中的資訊監控病毒防護狀態

若要使用網路代理記錄的資訊監控用戶端裝置的病毒防護狀態，請根據裝置的系統：

- 在執行 Windows 的裝置：

  1. 開啟用戶端裝置的系統登錄檔（例如，在本機**開始 → 執行**功能表中使用 regedit 指令）。

  2. 轉至以下分支：

     - 對於 32 位元系統：

       HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\Statistics\AVState

     - 對於 64 位元系統：

       HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\Stati

     系統登錄檔將顯示用戶端裝置病毒防護狀態的資訊。

- 在執行 Linux 的裝置：

  - 資訊會包含在獨立的文字檔中，各類型資料一個檔案，位於 /var/opt/kaspersky/klnagent/1103/1.0.0.0/Statistics/AVState/。

- 在執行 macOS 的裝置：

  - 資訊會包含在獨立的文字檔中，各類型資料一個檔案，位於 /Library/Application Support/Kaspersky Lab/klnagent/Data/1103/1.0.0.0/Statistics/AVState/。

病毒防護狀態對應於下表中所述的鍵。

鍵（資料類型）	參數值	敘述
Protection_LastConnected (REG_SZ)	DD-MM-YYYY HH-MM-SS	上次連線至管理伺服器的時間和日期（UTC 格式）
Protection_AdmServer (REG_SZ)	IP、DNS 名稱或 NetBIOS 名稱	管理裝置的管理伺服器的名稱
Protection_NagentVersion (REG_SZ)	a.b.c.d	安裝在裝置上的網路代理版本號
Protection_NagentFullVersion (REG_SZ)	a.b.c.d (patch1; patch2; ...; patchN)	安裝在裝置上網路代理版本的完整編號（具備修補程式）
Protection_HostId (REG_SZ)	裝置 ID	裝置 ID
Protection_DynamicVM (REG_DWORD)	0 — 否 1 — 是	網路代理以動態 VDI 模式安裝
Protection_AvInstalled (REG_DWORD)	0 — 否 1 — 是	安全應用程式會安裝在裝置
Protection_AvRunning (REG_DWORD)	0 — 否 1 — 是	即時防護已在裝置上啟用
Protection_HasRtp (REG_DWORD)	0 — 否 1 — 是	已安裝即時防護元件
Protection_RtpState (REG_DWORD)	即時防護狀態：	
	0	未知
	1	已停用
	2	已暫停
	3	正在啟動
	4	已啟用
	5	啟用高防護層級（最高防護）
	6	啟用低防護層級（最高速度）
	7	啟用預設（建議）設定
	8	啟用自訂設定
	9	操作失敗
Protection_LastFscan (REG_SZ)	DD-MM-YYYY HH-MM-SS	上次完整掃描時間和日期（UTC 格式）
Protection_BasesDate (REG_SZ)	DD-MM-YYYY HH-MM-SS	程式資料庫發佈時間和日期（UTC 格式）

當裝置顯示不活動時檢視和配置操作

如果組中的用戶端裝置不活動，您可以獲取關於它的通知。您也可以自動刪除此類裝置。

要在組中裝置顯示不活動時檢視或設定操作：

1. 在主控台樹狀目錄，右擊所請求的管理群組名稱。
2. 在右鍵選單中，選取**內容**。
   這將開啟管理群組內容視窗。
3. 在「**內容**」視窗中，前往**裝置**區域。

4. 如果需要，啟用或停用以下選項：

- **若裝置未活動超過下列天數，則通知管理員**

  如果啟用該選項，管理員接收不活動裝置的通知。您可以指定**裝置在網路上已長時間沒有活動**事件被建立的時間間隔。預設時間間隔為 7 天。

  預設情況下已啟用該選項。

- **若裝置未活動超過下列天數，則從群組刪除裝置**

  如果啟用該選項，您可以指定從組中自動移除裝置的時間間隔。預設時間間隔為 60 天。

  預設情況下已啟用該選項。

- **從父群組繼承**

  該區域的設定將從包含用戶端裝置的父群組繼承。如果啟用此選項，**網路中的裝置活動**下的設定會禁止任何變更。

  該選項僅在管理群組擁有父群組時可用。

  預設情況下已啟用該選項。

- **強制子群組繼承**

  該設定值將被分發到子群組，但在子群組的內容中這些設定被鎖定。

  預設情況下已停用該選項。

5. 點擊**確定**。

您的變更已儲存並套用。

停用卡巴斯基公告

在卡巴斯基安全管理中心網頁主控台的Kaspersky 公告區段（**監控和報告 → Kaspersky 公告**），透過提供與您的卡巴斯基安全管理中心版本和受管理裝置上安裝的受管理應用程式相關資訊，讓您隨時了解最新資訊。如果您不想接收卡巴斯基公告，則可以停用此功能。

卡巴斯基公告包括兩種類型的資訊：與安全相關的公告和行銷公告。您可以分別停用每種類型的公告。

停用與安全性有關的公告：

1. 在主控台樹狀目錄中，選取要為其停用相關安全公告的管理伺服器。
2. 右擊並在出現的上下文功能表中選取**內容**。
3. 在開啟之管理伺服器內容視窗中的**卡巴斯基公告**區段，選取**啟用卡巴斯基安全管理中心網頁主控台中的卡巴斯基公告顯示**選項。
4. 點擊**"確定"**。

卡巴斯基的公告已停用。

預設情況下，會停用行銷公告。僅在啟用卡巴斯基安全網路 (KSN) 的情況下，您才會收到行銷公告。您可以透過停用 KSN 來停用此類型的公告。

發佈點和連線閘道器的調整

卡巴斯基安全管理中心中的管理群組結構執行以下功能：

- 設定政策範圍

  套用相關設定到裝置有另一種方式，透過使用*政策設定檔*。在此情況下，您可以設定有標籤的政策範圍、在 Active Directory 組織單元中的裝置位置、或Active Directory 安全群組的成員關係。

- 設定群組工作範圍

  還有一個不基於管理群組層級定義群組工作範圍的方法：使用裝置分類的工作和特定裝置的工作。

- 設定裝置、虛擬管理伺服器和次要管理伺服器的存取權限

- 分配發佈點

當建立管理群組結構時，您必須考慮到組織網路的拓撲以便最優分配發佈點。發佈點的最優分發允許您在企業網路中儲存流量。

根據組織圖表和網路拓撲，以下標準配置可以被套用到管理群組結構：

- 單一辦公室

- 多個小遠端分辦公室

作為發佈點的裝置必須被防護，包括實體防護，以防範非授權的存取。

發佈點的標準配置：單一辦公室

在標準「單一辦公室」配置中，所有裝置都在組織網路上，因此它們能看見彼此。組織網路可能包含幾部分（網路或網段），由窄通道連線。

有以下構建管理群組結構的方法：

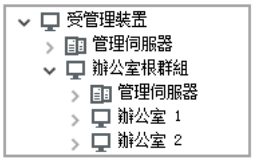
- 構建管理群組結構涉及到網路拓撲。管理群組結構可能不精確反映網路拓撲。網路各部分之間以及特定管理群組相互比對。您可以使用發佈點自動分配或手動分配它們。

- 不考慮網路拓撲而構建管理群組結構。在此情況下，您必須停用發佈點自動分配，然後為網路中每個部分的根管理群組（例如**受管理裝置**群組）分配一或多個裝置作為發佈點。所有發佈點將處於相同等級，並將掌控組織網路中所有裝置的相同範圍。此種情況下，每個網路代理將連線到具有最小路由的發佈點。發佈點的路由可以使用 tracert 公用程式偵錯。

發佈點的標準配置：多個小遠端辦公室

該標準配置用於一定數量的小型遠端辦公室，您可透過網際網路與總部通訊。每個遠端辦公室都位於 NAT 之外，就是說，從一個遠端辦公室到另一個遠端辦公室的連線是不可能的，因為辦公室是彼此隔離的。

配置必須在管理群組中體現：必須為每個遠端辦公室建立各自的管理群組（下圖中的群組**辦公室 1**和**辦公室 2**）。



遠端辦公室包含在管理群組結構

您必須指定一或多個發佈點給一間辦公室的每個對應管理群組。發佈點必須是遠端辦公室中具有足夠剩餘磁碟空間的裝置。佈署在**辦公室 1**群組的裝置，例如，將存取分配到**辦公室 1**管理群組的發佈點。

如果一些使用者在辦公室之間移動他們的攜帶式電腦，您必須在遠端辦公室選取兩個或更多裝置（除了現有的發佈點）並分配它們作為等級管理群組的發佈點（上圖中**辦公室根群組**）。

例如：攜帶式電腦佈署在**辦公室 1**管理群組，然後被移動到對應於**辦公室 2** 管理群組的辦公室。在移動攜帶式電腦後，網路代理試圖存取分配到**辦公室 1**群組的發佈點，但是那些發佈點不可用。然後，網路代理開始嘗試存取分配到**辦公室根群組**的發佈點。因為遠端辦公室是彼此隔離的，嘗試存取分配到**辦公室根群組**管理群組的發佈點僅在網路代理嘗試存取**辦公室 2** 群組中的發佈點時才會成功。就是說，攜帶式電腦將保持在原始辦公室對應的管理群組，但是將使用它當時所在辦公室的發佈點。

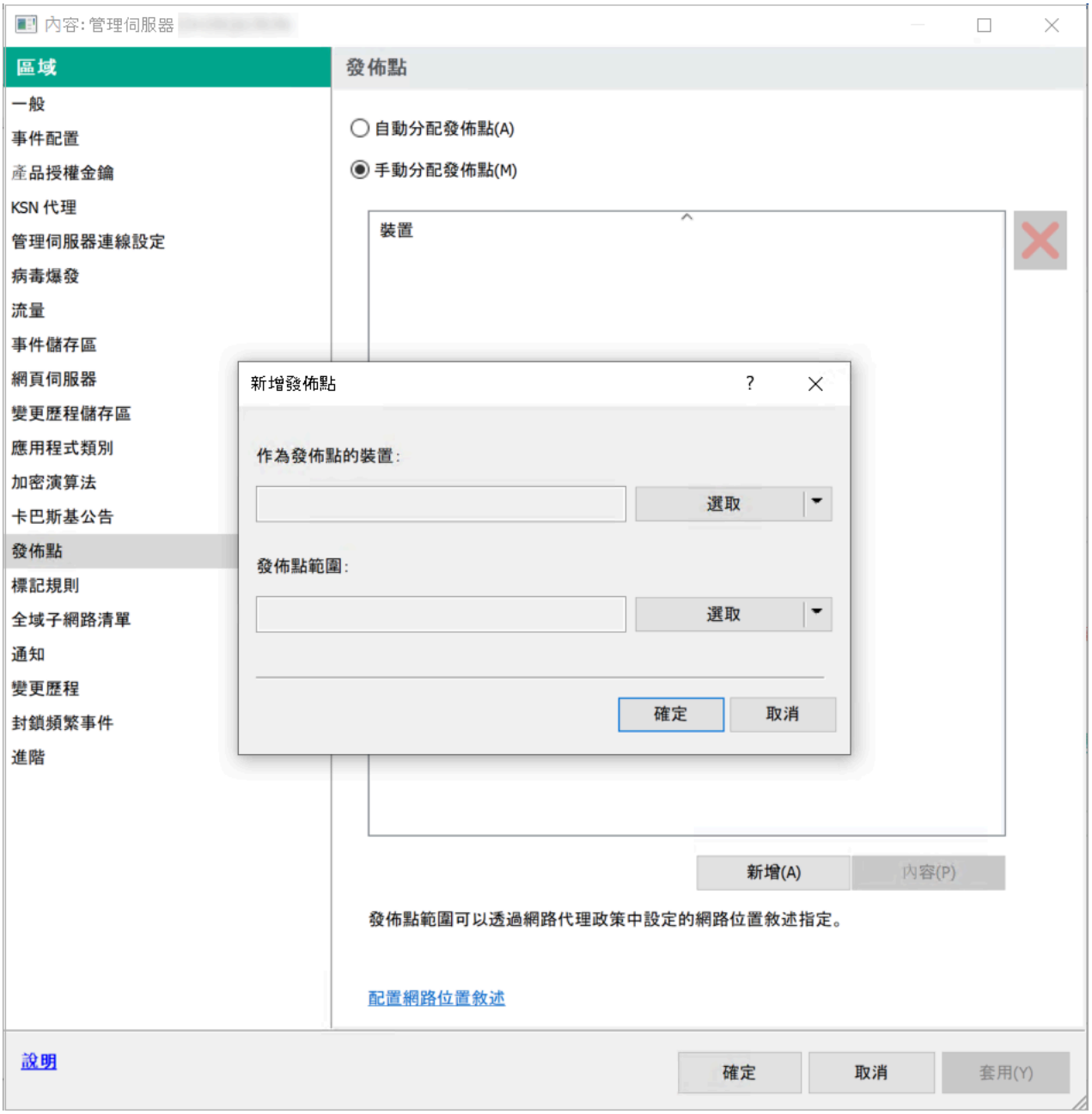
手動指派受管理裝置作為發佈點使用

您可以指定一部裝置作為某個管理群組的發佈點，並在管理主控台中將其配置為連線閘道。

要分配裝置作為管理群組的發佈點：

1. 在主控台樹狀目錄中，選取**管理伺服器**節點。
2. 在管理伺服器的上下文功能表中，選取**內容**。
3. 在管理伺服器內容視窗，選取**發佈點**區域。
4. 在視窗右側選取**手動分配發佈點**選項。

5. 點擊**新增**按鈕。



手動分配發佈點

這會開啟**新增發佈點**視窗。

6. 在**新增發佈點**視窗，執行以下操作：

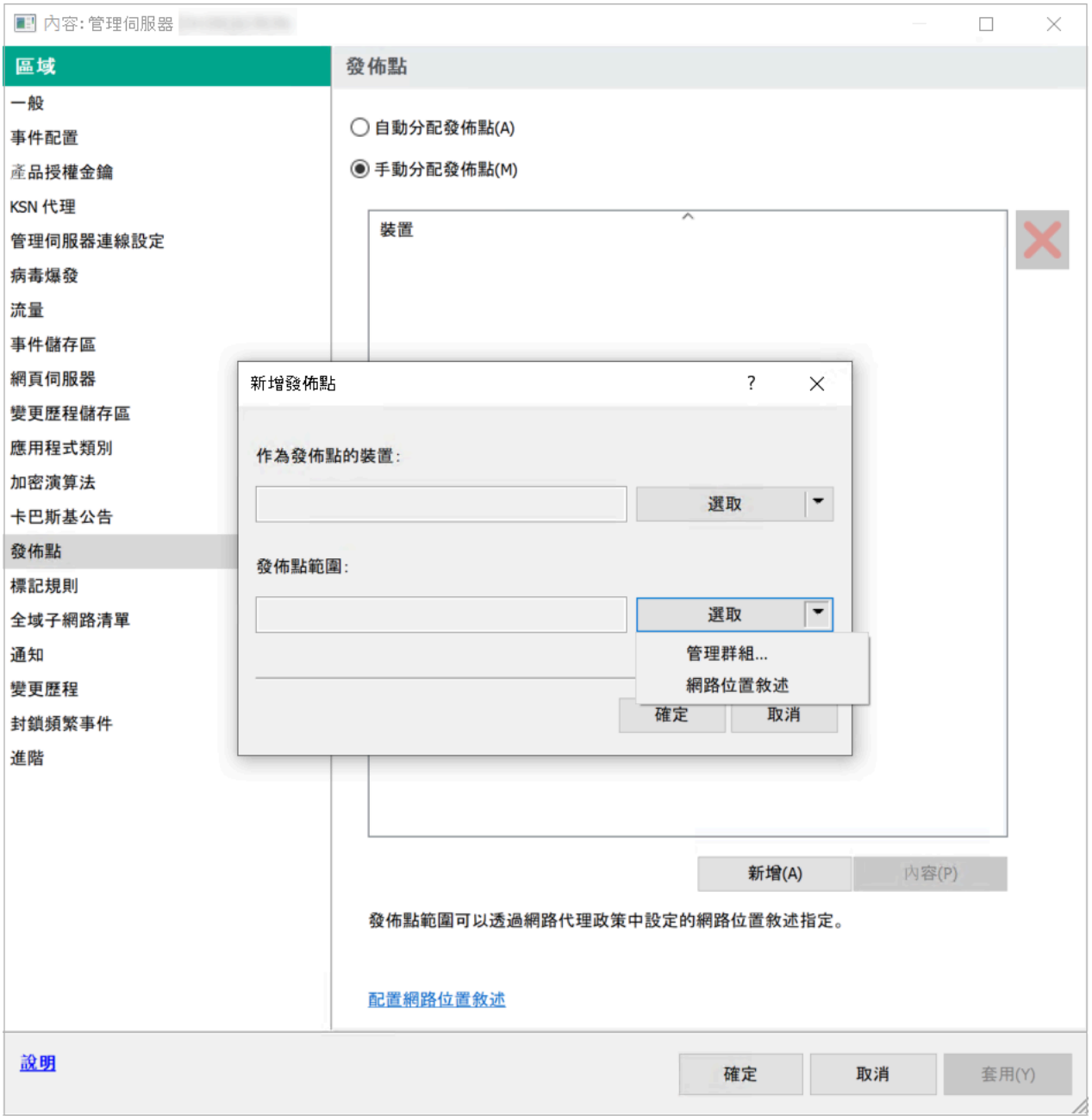
a. 在**作為發佈點裝置使用**下，點擊在**選取**拆分按鈕上的向下箭頭（ ），然後選取**從群組新增裝置**選項。

b. 在開啟的**選取裝置**視窗中，選取要作為發佈點使用裝置。

c. 在**發佈點範圍下**，按一下在**選取**拆分按鈕上的向下箭頭。

d. 指定發佈點將向其分發更新的裝置。您可以指定管理群組或者網路位置敘述。

e. 點擊**確定**以關閉**新增發佈點**視窗。



選取發佈點範圍

您新增的發佈點將顯示在**發佈點**區域的發佈點清單。

安裝有網路代理並連線到虛擬伺服器的第一台裝置將自動指定為發佈點，並配置為連線閘道。

在非警戒區將 Linux 裝置連線為閘道

要將 Linux 裝置連線為非警戒區 (DMZ) 中的閘道，請執行以下操作：

1. 在 Linux 裝置上下載並安裝網路代理。
2. 執行安裝後指令碼並遵循主指令碼以設定本機環境組態。在命令提示字元下，執行以下命令：

```
$ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
```

3. 在要求網路代理模式的步驟中，選擇**作為連線閘道使用**選項。

4. 在 MMC 型管理主控台的管理伺服器的上下文功能表中，選取**內容**。

5. 在開啟的"管理伺服器內容"視窗中，選取**發佈點**區域。

6. 在開啟的**發佈點**視窗中，在視窗的右側：

   a. 選取**手動分配發佈點**選項。

   b. 點擊**新增**按鈕。

   這會開啟**新增發佈點**視窗。

7. 在**新增發佈點**視窗，執行以下操作：

   a. 在**裝置作為發佈點使用**下，按一下在**選取**拆分按鈕上的向下箭頭（ ），然後選取**透過位址新增 DMZ 中的連線閘道**選項。

   b. 在**發佈點範圍下**，按一下在**選取**拆分按鈕上的向下箭頭 。

   c. 指定發佈點將向其分發更新的裝置。您可以指定一個管理群組。

   d. 點擊**確定**以關閉**新增發佈點**視窗。

8. 您新增的發佈點將顯示在**發佈點**區域的發佈點清單。

9. 執行 klnagchk，檢查是否已成功配置到卡巴斯基安全管理中心的連線。在命令提示字元下執行：
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```

10. 在主功能表中，轉到卡巴斯基安全管理中心並找到裝置。

11. 在開啟的視窗中，按一下<裝置名稱>。

12. 在下拉清單中，選取**移至群組**連結。

13. 在開啟的**選取群組**視窗中，按一下**發佈點**連結。

14. 點擊"**確定**"。

15. 透過在命令提示字元下執行以下命令，在 Linux 用戶端上重新啟動網路代理服務：
    ```
    $ sudo /opt/kaspersky/klnagent64/bin/klnagchk -restart
    ```

將 Linux 裝置作為 DMZ 中的閘道連線已完成。

之後，您可以通過配置的連線閘道將 Linux 裝置連線到管理伺服器。僅在完成主要安裝方案後才執行這些過程。

透過連線閘道將 Linux 裝置連線到管理伺服器

連線閘道允許您將用戶端裝置從隔離區 (DMZ) 連線到管理伺服器。基於 Windows和Linux 的裝置可以充當連線閘道。連線並配置連線閘道後，您可以使用此閘道將 Linux 裝置連線到管理伺服器。僅在完成主要安裝方案後才執行以下過程。

若要透過連線閘道將 Linux 裝置連線到管理伺服器，請在此裝置上執行以下操作：

1. 在 Linux 裝置上下載並安裝網路代理。

2. 透過在命令提示字元執行以下命令來執行網路代理安裝後指令碼：
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. 在要求網路代理模式的步驟中，選擇**使用連線閘道連線伺服器**選項，並輸入連線閘道位址。

4. 透過在命令提示字元下使用以下命令，檢查與卡巴斯基安全管理中心和連線閘道的連線：
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```
   連線閘道的位址會顯示在輸出中。

透過連線閘道將 Linux 裝置連線到管理伺服器的操作完成。您可以使用此裝置更新遠端安裝應用程式的發佈，以及擷取有關網路連線裝置的資訊。

在 DMZ 中新增連線閘道作為發佈點

連線閘道會等待來自管理伺服器的連線，而不是建立與管理伺服器的連線。這代表將連線閘道安裝在 DMZ 中的裝置後，管理伺服器不會在受管理裝置中列出該裝置。因此，您需要一個特殊程序來確保管理伺服器啟動到連線閘道的連線。

若要新增以連線閘道作為發佈點的裝置：

1. 在主控台樹狀目錄中，選取**管理伺服器**節點。

2. 在管理伺服器的上下文功能表中，選取**內容**。

3. 在管理伺服器內容視窗，選取**發佈點**區域。

4. 在視窗右側選取**手動分配發佈點**選項。

5. 點擊**新增**按鈕。
   這會開啟**新增發佈點**視窗。

6. 在**新增發佈點**視窗，執行以下操作：

   a. 在**作為發佈點裝置使用**下，點擊在**選取**拆分按鈕上的向下箭頭（ ）， 然後選取**按位址新增 DMZ 連線閘道**選項。

   b. 在開啟的**輸入連線閘道位址**視窗中，輸入連線閘道的 IP 位址（如果可以透過名稱存取連線閘道，則輸入名稱）。

   c. 在**發佈點範圍下**，按一下在**選取**拆分按鈕上的向下箭頭 。

   d. 指定發佈點將向其分發更新的裝置。您可以指定管理群組或者網路位置敘述。
      建議您為外部受管理裝置建立單獨的群組。

在您執行這些動作後，發佈點清單會包含名為**連線閘道臨時項目的新項目**。

管理伺服器幾乎立即嘗試以您指定的位址連線到連線閘道。如果成功，則項目名稱將更改為連線閘道裝置的名稱。此程序大約需要 5 分鐘。

在將連線閘道的臨時項目轉換為命名項目時，該連線閘道也會出現在**未配置的裝置**群組中。

要將連線閘道新增到先前配置的網路，請在要連線到新增的連線閘道的裝置上重新安裝網路代理。

自動分配發佈點

我們建議您自動分配發佈點。然後卡巴斯基安全管理中心將自行選取哪個裝置要被分配為發佈點。

要自動分配發佈點：

1. 開啟主應用程式視窗。
2. 在主控台樹狀目錄中，選取您要為其自動指派發佈點的節點及管理伺服器名稱。
3. 在管理伺服器的上下文功能表中，按一下**"內容"**。
4. 在管理伺服器內容視窗的**區域**視窗選取**發佈點**。
5. 在視窗右側選取**自動分配發佈點**選項。

   如果自動指派裝置作為發佈點被啟用，您無法手動配置發佈點，也不能編輯發佈點清單。

6. 點擊**"確定"**。

管理伺服器便自動指派和配置發佈點。

在選取用作發佈點的裝置上本機安裝網路代理

要允許發佈點選取的裝置與虛擬管理伺服器直接通信，然後作為連線閘道，網路代理必須安裝在該裝置。

在充當發佈點的裝置上本機安裝網路代理的過程與在任何網路裝置上本機安裝網路代理的過程相同。

要將裝置選為發佈點，下列條件必須滿足：

- 在本機安裝網路代理時，在安裝精靈**管理伺服器**視窗的**伺服器位址**指定管理裝置的虛擬管理伺服器的位址。您可以使用裝置 IP 位址或 Windows 網路中的裝置名稱。

  虛擬管理伺服器位址使用下列格式：<虛擬伺服器所屬實體伺服器的絕對位址>/<虛擬管理伺服器的名稱>。

- 因此作為連線閘道的角色，請您在這台裝置上，開啟連接埠以與管理伺服器通訊。

當帶有指定設定的網路代理安裝在裝置上後，卡巴斯基安全管理中心將自動執行下列操作：

- 將此裝置包含在虛擬管理伺服器的**受管理裝置**群組中。
- 將此裝置指定為虛擬管理伺服器的**受管理裝置**群組的發佈點。

您有必要並足以在指定為組織網路**受管理裝置**群組發佈點的裝置上本機安裝網路代理。您可以將網路代理遠端安裝在充當嵌套管理群組中的發佈點的裝置上。為此，請使用**受管理裝置**群組的發佈點作為連線閘道。

使用發佈點作為連線閘道

如果管理伺服器在隔離區 (DMZ) 以外，則該區域的網路代理無法連線管理伺服器。

連線具有網路代理的管理伺服器時，可使用發佈點作為連線閘道。發佈點開啟到管理伺服器的連接埠用以建立連線。當管理伺服器啟動時，它連線到一個發佈點並在整個連線期間維持該連線。

收到管理完全的信號後，發佈點會向網路代理傳送 UDP 信號，以便執行連線到管理伺服器。網路代理收到該信號後會連線到發佈點，這會在網路代理和管理伺服器之間傳輸資訊。資訊交換可以透過 IPv4 或 IPv6 網路進行。

我們建議您使用特殊分配的裝置作為連線閘道並使用該連線閘道覆蓋最多 10,000 台用戶端裝置（包括行動裝置）。

要將連線閘道新增到先前配置的網路：

1. 以連線閘道模式安裝網路代理。
2. 在要連線到新增的連線閘道的裝置上重新安裝網路代理。

將 IP 範圍新增至分發點輪詢的範圍清單中

您可以新增 IP 範圍到發佈點輪詢的範圍清單。

要新增 IP 範圍到已輪詢範圍清單：

1. 在主控台樹狀目錄中，選取**管理伺服器**節點。
2. 在節點的上下文功能表中，選取“**內容**”。
3. 在開啟的“管理伺服器內容”視窗中，選取**發佈點**區域。
4. 在清單中，選取必要的發佈點並按一下**內容**。
5. 在開啟的分發點內容視窗的左側**區域**窗格中，選取**裝置發現 → IP 範圍**。
6. 選中**啟用範圍輪詢**核取方塊。

7. 點擊**新增**按鈕。

   新增按鈕僅在您選取**啟用範圍輪詢**核取方塊時發揮作用。

   IP 範圍視窗將開啟。

8. 在**IP 範圍**視窗，輸入新 IP 範圍名稱（預設名稱是「新範圍」）。

9. 點擊**新增**按鈕。

10. 執行以下操作之一：

    - 使用開始和結束 IP 位址指定 IP 範圍。
    - 使用位址和子網路遮罩指定 IP 範圍。
    - 點擊**瀏覽**並從子網路全域清單中選取子網路。

11. 點擊**確定**。

12. 點擊**確定**以新增有指定名稱的新範圍。

    新範圍將出現在已輪詢的範圍清單中。

使用發佈點作為推送伺服器

在卡巴斯基安全管理中心中，發佈點可以作為透過移動通訊協定管理之裝置和受網路代理管理之裝置的推送伺服器。例如，如果您希望能夠對 KasperskyOS 裝置與管理伺服器進行強制同步，則必須啟用推送伺服器。推送伺服器與啟用推送伺服器的發佈點具有相同的受管理裝置範圍。如果為相同管理群組指派了多個發佈點，則可以在每個發佈點上啟用推送伺服器。在這種情況下，管理伺服器會平衡發佈點之間的負載。

推送伺服器支援負載最多 50,000 個同時連線。

您可能希望將發佈點用作推送伺服器，以確保受管理裝置和管理伺服器之間存在持續連線。某些操作需要持續連線，例如執行和停止本機工作、接收受管理應用程式的統計資訊或建立隧道。如果使用發佈點作為推送伺服器，則不必在受管理裝置上使用**不要中斷與管理伺服器的連線**選項或將封包傳送到網路代理的 UDP 連接埠。

若要將發佈點用作推送伺服器：

1. 在主控台樹狀目錄中，選取**管理伺服器**節點。

2. 在節點的上下文功能表中，選取"**內容**"。

3. 在開啟的"管理伺服器內容"視窗中，選取**發佈點**區域。

4. 在清單中，選取必要的發佈點並按一下**內容**。

5. 在開啟的發佈點內容視窗中，在左邊的**區域**窗格的**一般**區域中，選取**將此發佈點用作推送伺服器**選項。

6. 指定推送伺服器連接埠號，即用戶端裝置將用於連線的發佈點上的連接埠。

   預設情況下使用連接埠 13295。

7. 按一下**確定**按鈕以關閉管理伺服器屬性視窗。

8. 開啟網路代理政策設定視窗。

9. 在**連線**區段，前往**網路** 子區段。

10. 在**網路**子區段中，選取**使用發佈點強制連線到管理伺服器**選項。

11. 按一下**確定**按鈕以離開視窗。

該發佈點將開始作為 KSN 代理伺服器。它現在可以向用戶端裝置傳送推送通知。

如果您管理安裝了 KasperskyOS 的裝置，或計劃這樣做，您必須使用發佈點作為推送伺服器。如果您想向用戶端裝置傳送推送通知，您還可以使用發佈點作為推送伺服器。

其他日常工作

該部分提供佈署卡巴斯基安全管理中心的一般使用建議。

管理管理伺服器

本章節提供有關使用管理伺服器和如何設定它們的資訊。

建立管理伺服器階層：新增次要管理伺服器

您可以新增管理伺服器作為從屬管理伺服器，進而建立「主要/從屬」層級。無論要作為從屬管理伺服器使用的伺服器是否可以透過管理主控台連線，您都可以新增從屬管理伺服器。

當組合兩個管理伺服器到一個層級，確保連接埠 13291 在兩個管理伺服器上都可以存取。連接埠 13291 用以接收從管理主控台到管理伺服器的連線。

連線新管理伺服器以作為主管理伺服器的從屬伺服器。

您可以透過連線其到主管理伺服器的連接埠 13000 來新增管理伺服器作為從屬伺服器。您將需要一個安裝了管理主控台的裝置，其 TCP 連接埠 13291 可以被兩個管理伺服器存取：假定的主管理伺服器和從屬管理伺服器。

若要新增可以透過管理主控台連線的管理伺服器作為從屬伺服器：

1. 確保未來主管理伺服器的連接埠 13000 可用於從從屬管理伺服器接收連線。

2. 使用管理主控台連線到假定的主管理伺服器。

3. 選取您要新增從屬管理伺服器連線到的管理群組。

4. 在選定群組節點的**管理伺服器**工作區中，點擊**新增從屬管理伺服器**連結。

   新增從屬管理伺服器精靈啟動。

5. 在精靈的第一步（輸入正在新增到群組的管理伺服器位址），輸入假定從屬管理伺服器的網路名稱。

6. 遵照精靈的說明。

「主要/從屬」層級被建立。主管理伺服器將從從屬管理伺服器接收連線。

如果您沒有裝置安裝了管理主控台，且 TCP 連接埠 13291 可以在兩個管理伺服器上存取（如果，例如，假定從屬管理伺服器位於遠端辦公室且該辦公室的系統管理員出於安全原因無法開啟到連接埠 13291 的網際網路存取），您將仍可以新增從屬管理伺服器。

若要新增不能透過管理主控台連線的管理伺服器作為從屬伺服器：

1. 確保假定的主管理伺服器連接埠 13000 可用於來自從屬管理伺服器的連線。

2. 將假定主管理伺服器憑證寫入外部裝置，例如快閃記憶體磁碟機，或將其傳送到管理伺服器所在的遠端辦公室系統管理員。

   管理伺服器憑證位於相同的管理伺服器，在 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer。

3. 將假定從屬管理伺服器的憑證寫入外部裝置，例如隨身碟。如果假定從屬管理伺服器位於遠端辦公室，聯絡該辦公室的系統管理員以提醒他/她傳送憑證給您。

   管理伺服器憑證位於相同的管理伺服器，在 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer。

4. 使用管理主控台連線到假定的主管理伺服器。

5. 選取您要新增從屬管理伺服器連線到的管理群組。

6. 在**管理伺服器**節點的工作區中，點擊**新增從屬管理伺服器**連結。

   新增從屬管理伺服器精靈啟動。

7. 在精靈的第一步（輸入位址），將**從屬管理伺服器位址（可選）**欄位留空。

8. 在**從屬管理伺服器憑證檔案**視窗點擊**瀏覽**按鈕，並選取已儲存的從屬管理伺服器憑證檔案。

9. 當精靈完成後，使用管理主控台的不同執行個體連線到假定從屬管理伺服器。如果管理伺服器位於遠端辦公室，聯絡該辦公室的系統管理員以提醒他/她連線到假定從屬管理伺服器並執行進一步操作。

10. 在**管理伺服器**節點的上下文功能表中，選取**內容**。

11. 在管理伺服器內容中，轉到**進階**區域的**管理伺服器階層**子區域。

12. 選取**此管理伺服器是階層中的從屬伺服器**核取方塊。

    輸入欄位可用於資料輸入和編輯。

13. 在**主管理伺服器位址**欄位，輸入未來主管理伺服器的網路名稱。

14. 透過點擊**瀏覽**按鈕選取先前已儲存且帶有假定主管理伺服器憑證的檔案。

15. 點擊**確定**。

「主要/從屬」層級被建立。您可以透過管理主控台連線到從屬管理伺服器。主管理伺服器將從從屬管理伺服器接收連線。

連線主管理伺服器到從屬管理伺服器

您可以新增新管理伺服器作為從屬，以便主管理伺服器透過連接埠 13000 連線到從屬管理伺服器。例如，如果您放置從屬管理伺服器到 DMZ 中時，該選項可用。

您將需要一個安裝了管理主控台的裝置，其 TCP 連接埠 13291 可以被兩個管理伺服器存取：假定的主管理伺服器和從屬管理伺服器。

要新增新管理伺服器作為從屬並透過連接埠 13000 連線主管理伺服器：

1. 確保假定從屬管理伺服器的連接埠 13000 可用於從假定主管理伺服器接收連線。
2. 使用管理主控台連線到假定的主管理伺服器。
3. 選取您要新增從屬管理伺服器連線到的管理群組。
4. 在相關管理群組節點的**管理伺服器**工作區中，點擊**新增從屬管理伺服器**連結。

   新增從屬管理伺服器精靈啟動。
5. 在精靈的第一步（輸入正在新增到群組的管理伺服器位址），輸入假定從屬管理伺服器的網路名稱，並選取**將主管理伺服器連線到 DMZ 中的從屬管理伺服器**核取方塊。
6. 如果您透過代理伺服器連線到假定從屬管理伺服器，在精靈的第一步選取**使用代理伺服器**核取方塊並指定連線設定。
7. 遵照精靈的說明。

管理伺服器階層被建立。主管理伺服器將由從屬管理伺服器接收連線。

連線至管理伺服器及在管理伺服器之間轉換

開啟卡巴斯基安全管理中心後，它將嘗試連線至管理伺服器。如果網路中有多個管理伺服器，則程式會連線卡巴斯基安全管理中心上一次正常連線的管理伺服器。

如果程式在安裝後第一次執行，則它會嘗試連線至卡巴斯基安全管理中心安裝過程中指定的管理伺服器。

在成功建立與管理伺服器的連線後，此管理伺服器的架構將顯示在主控台樹狀目錄中。

如果已經將多個管理伺服器新增至主控台樹狀目錄，您可以在它們之間進行轉換。

管理主控台用於每個管理伺服器。在第一次連線到新管理伺服器之前，確保從管理主控台接收連線的連接埠 13291 被開啟，以及所有用於管理伺服器和其他卡巴斯基安全管理中心元件間互動的剩餘連接埠。

要轉換到其他管理伺服器，請執行以下操作：

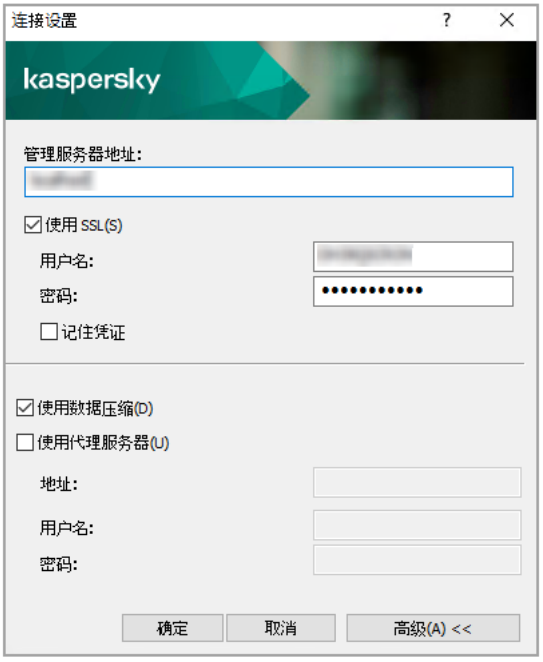
1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。
2. 在該節點的上下文功能表，選取**連線至管理伺服器**。

3. 在開啟的**連線設定**視窗中的**管理伺服器位址**欄位中，輸入您要連線的管理伺服器的名稱。您可以指定一個 IP 位址或 Windows 網路中裝置的名稱作為管理伺服器的名稱。您可點擊**"進階"**按鈕設定與管理伺服器的連線（請參閱下圖）。

   要透過與預設連接埠不同的埠號連線至管理伺服器，請在**管理伺服器位址**欄位中以 <管理伺服器名稱>:<連接埠> 格式輸入值。

   若要連線到虛擬管理伺服器，請在**管理伺服器位址**欄位中以 <管理伺服器位址>/<虛擬伺服器名稱> 格式輸入值。

   沒有**"讀取"**權限的帳戶將會被管理伺服器拒絕存取。



連線至管理伺服器

4. 點擊**"確定"**可完成在伺服器之間的轉換。

連線管理伺服器之後，程式會將其他管理伺服器節點更新在主控台樹狀目錄中。

透過網際網路連線至管理伺服器的條件

如果管理伺服器位於企業網路外部，則用戶端裝置需使用網際網路與其連線。

要透過網際網路將裝置連線至管理伺服器，需符合以下條件：

- 遠端管理伺服器應該有外部 IP 位址，且連接埠 13000 應該保持開啟狀態（為了連線網路代理）。我們建議您也開啟 UDP 連接埠 13000（為了接收裝置關閉通知）。
- 在裝置上安裝網路代理。
- 在裝置上安裝網路代理時，您應該指定遠端管理伺服器的外部 IP 位址。如果使用安裝套件進行安裝，則應該在安裝套件內容的**設定**區域中手動指定外部 IP 位址。
- 若要使用遠端管理伺服器來管理裝置的應用程式和工作，在**一般**區域中該裝置的內容視窗中，選取**不斷開與管理伺服器的連線**方塊。選中該方塊之後，請等待管理伺服器與遠端裝置同步。與管理伺服器保持連線的用戶端裝置的數量不得超過 300。

要提高遠端管理伺服器工作即時性，您可以在裝置上開啟連接埠 15000。在這個情況下，要執行工作，管理伺服器將透過連接埠 15000 向網路代理傳送一個專用封包至用戶端，而不是等待與裝置的同步。

到管理伺服器的加密連線

您可以使用 TLS（傳輸層安全）協定來進行用戶端裝置與管理伺服器的資料交換，以及管理主控台與管理伺服器的連線。TLS 協定能夠將傳輸資料加密並防止其在傳輸過程中被篡改。TLS 協定以互動雙方的身分驗證為基礎，並使用公用金鑰進行資料加密。

當裝置連線時驗證管理伺服器

在用戶端裝置首次連線管理伺服器時，裝置上的網路代理將下載管理伺服器憑證副本並將其儲存在本機。

如果您在裝置本機安裝網路代理，您可以手動選取管理伺服器憑證。

下載的憑證將用於之後驗證連線管理伺服器權限。

在之後的連線中，網路代理將在每次裝置與管理伺服器連線時檢查管理伺服器憑證，並將其與本機的備份憑證進行比較。如果檢查不一致，管理伺服器將封鎖裝置的存取。

在管理主控台連線期間的管理伺服器身分驗證

在當管理主控台第一次連線管理伺服器時，管理主控台將下載管理伺服器憑證並將其儲存在管理主控台。之後每次管理主控台連線管理伺服器時，均使用其驗證管理伺服器。

如果管理伺服器憑證與儲存在管理員工作站中的副本不符，管理主控台將提示您驗證與指定名稱的管理伺服器之間連線的選取，並下載新的憑證。使用再次下載憑證並建立連線後，管理主控台將下載新管理伺服器憑證，並在將來用其驗證管理伺服器。

配置連線到管理伺服器的 IP 位址允許清單

預設情況下，使用者可以用任何可以開啟卡巴斯基安全管理中心網頁主控台（以下簡稱「網頁主控台」）或安裝了基於 MMC 的管理主控台的裝置登入卡巴斯基安全管理中心。但是，您可以配置管理伺服器，以便使用者只能從具有允許 IP 位址的裝置連線到它。在這種情況下，即使入侵者竊取了卡巴斯基安全管理中心帳戶，他或她也將無法登入卡巴斯基安全管理中心，因為入侵者裝置的 IP 位址不在允許清單中。

當使用者登入卡巴斯基安全管理中心或執行透過卡巴斯基安全中心 OpenAPI 與管理伺服器互動的應用程式時，IP 位址會得到驗證。此時，使用者的裝置嘗試與管理伺服器建立連線。如果裝置的 IP 位址不在允許清單中，則會發生身分驗證錯誤，KLAUD_EV_SERVERCONNECT 事件會通知您尚未建立與管理伺服器的連線。

IP 位址允許清單的要求

僅當以下應用程式嘗試連線到管理伺服器時才會驗證 IP 位址：

- 網頁主控台伺服器

  如果您在一台裝置上登入網頁主控台，而網頁主控台伺服器安裝在另一台裝置上，您可以使用作業系統的標準方式在安裝網頁主控台伺服器的裝置上配置防火牆。然後，如果有人嘗試登入網頁主控台，防火牆將有助於防止入侵者乾擾。

- 管理主控台
- 透過 klakaut 自動化物件與管理伺服器互動的應用程式
- 透過 OpenAPI（例如 Kaspersky Anti Targeted Attack Platform 或 Kaspersky Security for Virtualization）與管理伺服器互動的應用程式

因此，請指定安裝了上述應用程式的裝置的位址。

您可以設定 IPv4 和 IPv6 位址。您不能指定 IP 位址的範圍。

如何建立 IP 位址的允許清單

如果您之前沒有設定允許清單，請按照以下說明進行操作。

若要建立 IP 位址允許清單以登入卡巴斯基安全管理中心：

1. 在管理伺服器裝置上，在具有管理員權限的帳戶下執行命令提示符。
2. 將當前目錄變更為卡巴斯基安全管理中心安裝資料夾（通常為 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center）。
3. 使用管理員權限輸入以下命令：
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP 位址>" -t s`

   指定滿足上述要求的 IP 位址。多個 IP 位址必須用分號隔開。

   如何只允許一台裝置連線到管理伺服器的示例：

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s`

   如何允許多個裝置連線到管理伺服器的示例：

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 198.51.100.0; 203.0.113.0" -t s`
4. 重新啟動管理伺服器服務。

您可以在管理伺服器上的卡巴斯基事件記錄中查看是否已成功配置 IP 位址的允許清單。

如何變更 IP 位址的允許清單

您可以像第一次建立產品授權清單時那樣變更它。為此，請執行相同命令並指定一個新的允許清單：

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP 位址>" -t
s
```

如果要從允許清單中刪除某些 IP 位址，請重寫它。例如，您的允許清單包括以下 IP 位址：192.0.2.0; 198.51.100.0; 203.0.113.0。您想要刪除 198.51.100.0 IP 位址。為此，請在命令提示字元下輸入以下命令：

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0;
203.0.113.0" -t s
```

不要忘記重新啟動管理伺服器服務。

如何重置已配置的 IP 位址允許清單

要重置已配置的 IP 位址允許清單：

1. 使用管理員權限在命令提示符處輸入以下指令：
   ```
   klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s
   ```
2. 重新啟動管理伺服器服務。

之後，不再驗證 IP 位址。

使用 klscflag 實用程式關閉連接埠 13291

管理伺服器上的連接埠 13291 用於接收來自管理主控台的連線。預設情況下此連接埠已開啟。如果不想要使用基於 MMC 的管理主控台或 klakaut 實用程式，可以使用 klscflag 實用程式關閉此連接埠。此實用程式可變更 KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN 參數的值。

要關閉連接埠 13291：

1. 使用管理員權限執行 Windows 命令提示符，然後將目前目錄變更為包含 klscflag 公用程式的目錄。klscflag 公用程式位於安裝管理伺服器的資料夾中。預設安裝路徑：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
2. 在命令行中執行以下命令：
   ```
   klscflag -ssvset -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv false -
   svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
   ```
3. 重新啟動卡巴斯基安全管理中心管理伺服器服務。

   連接埠 13291 已關閉。

要檢查 13291 連接埠是否已成功關閉：

在命令行中執行以下命令：

```
klscflag -ssvget -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -
ss "|ss_type = \"SS_SETTINGS\";"
```

此命令將返回以下結果：

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)false
```

`false`值表示連接埠已關閉。否則，系統將顯示`true`值。

從管理伺服器斷開連線

要與管理伺服器中斷連線，請執行以下操作：

1. 在主控台樹狀目錄中，選取與想要斷開連線的管理伺服器相對應的節點。
2. 在節點的上下文功能表中，選取**中斷與管理伺服器的連線**.。

將管理伺服器新增至主控台樹狀目錄

要將管理伺服器新增至主控台樹狀目錄，請執行以下操作：

1. 在卡巴斯基安全管理中心主視窗，在主控台樹狀目錄選取**卡巴斯基安全管理中心**節點。
2. 在該節點的上下文功能表，選取**建立 → 管理伺服器**。

   程式將在主控台樹狀目錄中建立名稱為“**管理伺服器- <裝置名稱>（未連線）**”的節點，您可以從該節點連線至安裝在網路中的任何管理伺服器。

從主控台樹狀目錄中刪除管理伺服器

要從主控台樹狀目錄中刪除管理伺服器，請執行以下操作：

1. 在主控台樹狀目錄中，選取要刪除的管理伺服器節點。
2. 在該節點的上下文功能表中，選取“**刪除**”。

將虛擬管理伺服器新增至主控台樹狀目錄

要將虛擬管理伺服器新增至主控台樹狀目錄，請執行以下操作：

1. 在主控台樹狀目錄中，選取您要為其建立虛擬管理伺服器的管理伺服器節點。
2. 在管理伺服器節點，選取**管理伺服器**資料夾。
3. 在**管理伺服器**資料夾的工作區中，點擊**新增虛擬管理伺服器**連結。

   此操作將啟動“新建虛擬管理伺服器”精靈。
4. 在**虛擬管理伺服器名稱**視窗，指定要建立的虛擬管理伺服器名稱。

   虛擬管理伺服器名稱不能包含多於 255 個字元並且不能包括任何特殊字元 ("*<>?\:|)。

5. 在**輸入裝置到虛擬管理伺服器的連線位址**視窗中指定裝置連線位址

   虛擬管理伺服器的連線位址是裝置透過其連線到伺服器的網路位址。連線位址有兩部分：實體管理伺服器的網路位址和虛擬管理伺服器的名稱，以斜線分割。虛擬管理伺服器名稱將被自動附加。指定的位址將被用於虛擬管理伺服器網路代理安裝套件的預設位址。

6. 在**建立虛擬管理伺服器的管理員帳戶**視窗中，從清單分配使用者作為虛擬伺服器管理員，或透過點擊**建立**按鈕新增管理員帳戶。

   您可以指定多個帳戶。

名為**管理伺服器 <虛擬管理伺服器名稱>** 的節點被建立在主控台樹狀目錄。

變更管理伺服器服務帳戶。實用程式工具 klsrvswch

如果您需要變更在安裝卡巴斯基安全管理中心時設定的管理伺服器服務帳戶，您可以使用一個名稱為 klsrvswch 的實用程式，它設計用來變更管理伺服器帳戶。

安裝卡巴斯基安全管理中心後，此實用程式將自動複製到程式安裝的資料夾中。

執行此實用程式的次數不受限制。

您必須使用用於安裝管理伺服器的具有管理員權限的帳戶在管理伺服器裝置上啟動 klsrvswch 公用程式。

klsrvswch 實用程式允許您變更帳戶類型。例如，如果您使用本機帳戶，您可以將其變更到網域帳戶或受管理裝置帳戶（反之亦然）。klsrvswch 實用程式不允許您將帳戶類型變更為群組受管理服務帳戶 (gMSA)。

Windows Vista 和後續 Windows 版本不允許對管理伺服器使用 LocalSystem 帳戶。在這些 Windows 版本中，**LocalSystem 帳戶**選項不被啟動。

要變更管理伺服器服務帳戶到網域帳戶，請執行以下操作：

1. 從卡巴斯基安全管理中心的安裝節點執行 klsrvswch 實用程式。預設安裝路徑：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   此操作會啟動修改管理伺服器服務帳戶精靈模式。遵照精靈的說明。

2. 在**管理伺服器服務帳戶**視窗，選取 **LocalSystem 帳戶**。

在精靈結束操作後，管理伺服器服務的帳戶將被變更。管理伺服器服務將在"*LocalSystem 帳戶*"下執行並使用其憑證。

卡巴斯基安全管理中心要正常執行，執行管理伺服器服務的帳戶應擁有存取管理伺服器資料庫的管理員權限。

要變更管理伺服器服務帳戶到使用者帳戶或受管理服務帳戶：

1. 從卡巴斯基安全管理中心的安裝節點執行 klsrvswch 實用程式。預設安裝路徑：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   此操作會啟動修改管理伺服器服務帳戶精靈模式。遵照精靈的說明。

2. 在**管理伺服器服務帳戶**視窗，選取**自訂帳戶**。

3. 點擊"**立即搜尋**"按鈕。

   "**選取**"視窗將開啟。

4. 在**選取使用者**視窗，點擊**物件類型**按鈕。

5. 在物件類型清單，選取**使用者**（如果您想要使用者帳戶）或**服務帳戶**（如果您想要受管理服務帳戶）並點擊**確定**。

6. 在物件名稱清單，輸入帳戶名稱，或者名稱的一部分，並點擊**檢查名稱**。

7. 在比對名稱清單，選取必要的名稱，然後點擊**確定**。

8. 若您在**帳戶密碼**中選取**服務帳戶**，請將**密碼**和**確認密碼**欄位留白。如果您選取了**使用者**，輸入使用者新密碼並確認。

管理伺服器服務帳戶將被變更到您選取的帳戶。

在預先假定的使用 Windows 工具對使用者帳戶進行身分驗證的模式下使用 Microsoft SQL Server 時，應該授予其存取資料庫的權限。使用者帳戶需要有卡巴斯基安全管理中心資料庫所有者的權限。預設情況下是使用 dbo 模式。

變更 DBMS 憑證

您可能需要變更 DBMS 憑證，例如，基於安全目的而執行的憑證變更。

若要使用 klsrvswch.exe 在 Windows 環境中變更 DBMS 憑證，請執行以下操作：

1. 從卡巴斯基安全管理中心的安裝資料夾執行 klsrvswch 實用程式。預設安裝路徑：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   您必須使用用於安裝管理伺服器的具有管理員權限的帳戶在管理伺服器裝置上啟動 klsrvswch 公用程式。

2. 點擊精靈的**下一步**按鈕，直到達到**變更 DBMS 存取憑證**步驟。

3. 在精靈的**變更 DBMS 存取憑證**步驟中，您可以執行以下操作：

> 如果使用 WIndows 驗證，則會跳過精靈的**變更 DBMS 存取憑證**步驟。

- 選擇**套用新憑證**選項。
- 在**帳戶**欄位中指定新的帳戶名。
- 在**密碼**欄位中為帳戶指定新密碼。
- 在**確認密碼**欄位中指定新密碼。

> 您應該指定 DBMS 中存在之帳戶的憑證。

4. 點擊**下一步**按鈕。

精靈完成後，將更改 DBMS 憑證。

klsrvswch 公用程式只能用於變更 SQL 驗證的帳戶密碼。不支援變更授權方式。若要變更授權方法，請重新安裝管理伺服器並指定所需的設定。

使用管理伺服器節點解決問題

管理主控台左側面板的主控台樹狀目錄包含管理伺服器節點。您可以任意多的管理伺服器到主控台樹狀目錄。

主控台樹狀目錄中的管理伺服器節點清單透過 Microsoft 管理主控台儲存在 .msc 檔案的陰影副本中。該檔案的陰影副本位於管理主控台裝置的 %USERPROFILE%\AppData\Roaming\Microsoft\MMC\ 資料夾。對於每個管理伺服器節點，檔案包含以下資訊：

- 管理伺服器位址
- 埠號
- 是否使用 TLS

  該參數取決於用於連線管理主控台到管理伺服器的埠號。
- 使用者名稱
- 管理伺服器憑證

故障解決

當管理主控台連線管理伺服器時，本機儲存的憑證與管理伺服器憑證相比較。如果憑證不比對，管理主控台產生錯誤。例如，憑證不比對可能發生在您取代管理伺服器憑證時。此種情況下，在主控台重新建立管理伺服器節點。

要重新建立建立管理伺服器節點：

1. 關閉卡巴斯基安全管理中心管理主控台視窗。
2. 刪除位於 %USERPROFILE%\AppData\Roaming\Microsoft\MMC\ 的卡巴斯基安全管理中心 14.2 檔案。
3. 執行卡巴斯基安全管理中心管理主控台。
   您將被提示連線到管理伺服器並接受現有憑證。
4. 執行以下操作之一：
   - 透過點擊**是**按鈕接受現有憑證。
   - 要指定您的憑證，點擊**否**按鈕，然後瀏覽到用於驗證管理伺服器的憑證檔案。

憑證問題被解決。您可以使用管理主控台連線到管理伺服器。

檢視和修改管理伺服器的設定

您可以在管理伺服器的內容視窗中調整其設定。

要開啟"內容：管理伺服器"視窗，

請在主控台樹狀目錄中管理伺服器節點的上下文功能表中選取**內容**。

調整管理伺服器的一般設定

您可以在管理伺服器內容視窗的**一般**、**管理伺服器連線設定**、**事件儲存區**和**安全性**中調整管理伺服器的一般設定。

如果**安全性**區域的顯示在管理主控台介面上被停用，它不會顯示在管理伺服器內容視窗。

*要在管理主控台啟用**安全性**區域的顯示：*

1. 在主控台樹狀目錄中，選取您需要的管理伺服器。
2. 在程式主視窗的**檢視**功能表，選取**設定介面**。
3. 在開啟的**設定介面**視窗，選取**顯示安全設定區域**核取方塊並點擊**確定**。
4. 在帶有程式訊息的視窗，點擊**確定**。

安全性區域將顯示在管理伺服器內容視窗。

管理主控台介面設定

您可調整要顯示的管理主控台介面設定，或隱藏與以下功能相關的使用者頁面控制：

- 弱點和修補程式管理
- 資料加密與防護
- 端點控制設定
- 行動裝置管理
- 從屬管理伺服器
- 安全設定區域

若億設定管理主控台介面設定：

1. 在主控台樹狀目錄中，選取您需要的管理伺服器。
2. 在程式主視窗的**檢視**功能表，選取**設定介面**。
3. 在開啟的**設定介面**視窗，選取您要顯示功能的核取方塊並點擊**確定**。
4. 在帶有程式訊息的視窗，點擊**確定**。

選取功能將顯示在管理主控台介面中。

在管理伺服器上的事件處理和儲存

應用程式和受管理裝置操作期間發生的事件的有關資訊儲存在管理伺服器資料庫中。每個事件都歸屬於特定類型和安全等級（*緊急事件*、*功能失效*、*警告*或*資訊*）。基於事件發生的條件，程式可以分配不同的安全等級到相同類型的事件。

您可以在管理伺服器內容視窗的**事件配置**區域檢視分配給事件的類型和安全等級。在**事件配置**區域，您也可以設定管理伺服器對每個事件的處理：

- 在管理伺服器以及裝置作業系統和管理伺服器事件記錄中註冊事件。
- 通知管理員事件的方法（例如，SMS 或者郵件訊息）。

在管理伺服器內容視窗的**事件儲存區**區域中，您可以透過限制事件記錄數和儲存期限來編輯管理伺服器資料庫的事件儲存設定。當您指定事件最大數時，應用程式計算用於指定數目的儲存空間的大概大小。您可以使用該大概計算來評估您在磁碟上是否具有足夠空間以避免資料庫溢出。管理伺服器資料庫的預設容量是 400,000 個事件。最大建議的資料庫容量是 45,000,000 個事件。

應用程式每 10 分鐘檢查一次資料庫。如果事件數達到指定的最大值加 10,000，應用程式將刪除最舊的事件，以便僅保留指定的最大事件數。

若管理伺服器刪除舊事件，則無法儲存新事件到資料庫。在此時間段內，拒絕事件的資訊被寫入卡巴斯基事件記錄。新事件被列隊，然後在刪除操作後被儲存到資料庫。

您可以更改任何工作的設定，以儲存與工作進度相關的事件，或者只儲存工作執行結果。為此，您將降低資料庫中的事件數量，提高與資料庫中事件表分析相關之情境的執行速度，並降低緊急事件被大數量事件覆寫的風險。

檢視連線到管理伺服器的記錄

操作期間的連線歷程和到管理伺服器的連線嘗試可以被儲存到檔案。檔案中的資訊不只允許您追蹤您的網路基礎架構中的連線，還有對管理伺服器的非授權存取嘗試。

要記錄連線管理伺服器事件：

1. 在主控台樹狀目錄中，選取您要為其啟用連線事件記錄的管理伺服器。
2. 在管理伺服器的上下文功能表中，選取**內容**。
3. 在開啟的內容視窗中，在**管理伺服器連線設定**區域中，選取**連線連接埠**子區域。
4. 啟用**記錄管理伺服器連線事件**選項。
5. 點擊**確定**按鈕以關閉管理伺服器內容視窗。

所有連入管理伺服器的後續事件、身分驗證結果和 SSL 錯誤將被儲存到 %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog。

控制病毒爆發

卡巴斯基安全管理中心可快速處理病毒爆發*威脅*。透過監控裝置上的病毒活動可以執行病毒爆發威脅評估。

您可以設定病毒爆發威脅和採取行動的評估規則；若要這麼做，請使用管理伺服器內容視窗的**病毒爆發**。

您可在管理伺服器內容視窗的**事件配置**區段（在*病毒爆發*事件內容視窗中），指定*病毒爆發*事件的通知程序。

安全應用程式作業期間若偵測到*已偵測惡意物件*事件時會產生*病毒爆發*事件。因此，您必須儲存管理伺服器上所有的*偵測到惡意物件*事件的資訊，從而識別病毒爆發。

您可以在安全應用程式的政策中指定用於儲存關於"*偵測到惡意物件*"事件資訊的設定。

在計算*偵測到惡意物件*事件的數量時，程式將僅計算來自主管理伺服器的裝置的資訊。對於來自從屬管理伺服器的資訊將不予以計算。對於每個從屬伺服器，程式都將單獨配置*病毒爆發*事件設定。

限制流量

為減少網路中的流量，程式提供相對應的選項，以便限制從指定的 IP 範圍和 IP 子網路向管理伺服器傳送資料的流量。

您可以在管理伺服器內容視窗的**流量**區域中建立和設定流量限制規則。

要建立流量限制規則：

1. 在主控台樹狀目錄中，選取您要為其建立流量限制規則的管理伺服器節點。
2. 在管理伺服器的上下文功能表中，選取**內容**。
3. 在"管理伺服器內容"視窗中，選取**流量**區域。
4. 點擊**新增**按鈕。
5. 在**新規則**視窗，指定以下設定：

   在**限制流量的 IP 範圍**區域中，您可以選取用於定義限制資料傳送速度的子網路或範圍的方法，然後為選定的方法輸入設定值。您可以選取以下方法之一：

   - **使用位址和網路遮罩指定範圍**

     流量基於子網路設定被限制。指定子網路位址和子網路遮罩以定義限制流量的範圍。

     您也可以點擊**瀏覽**以從子網路全域清單新增子網路。

   - **使用開始和結束位址指定範圍**

     流量基於 IP 位址範圍被限制。在**起始**和**結束**輸入欄位指定 IP 位址範圍。

     預設情況下已選取此選項。

   在**流量限制**區域，您可以調整資料傳輸率的以下限制設定：

   - **時間間隔**

     將要實施流量限制的時間段。您可以在輸入欄位中指定時間間隔界限。

   - **限制(KB/S)**

     管理伺服器的傳入和傳出資料的最大傳輸速度。流量限制將在"**時間間隔**"欄位中指定的時間間隔內實施。

   - **限制剩餘時間的流量(KB/S)**

     程式將不僅在"**時間間隔**"欄位中指定的時間間隔內限制流量，在其它時間也同樣。

     預設情況下已清空此方塊。該欄位的值可能與**限制(KB/S)**欄位的值不比對。

首先，流量限制規則影響檔案傳輸。這些規則不套用到管理伺服器和網路代理以及主要與從屬管理伺服器之間的同步產生的流量。

設定網頁伺服器

網頁伺服器用於發佈獨立安裝套件、iOS MDM 設定檔、以及共用資料夾的檔案。

您可以定義網頁伺服器連線至管理伺服器的設定，也可在管理伺服器內容視窗**網頁伺服器**區域設定網頁伺服器憑證。

管理內部使用者

*內部使用者*的帳戶可用於管理虛擬管理伺服器。卡巴斯基安全管理中心授權應用程式的內部使用者擁有真實使用者的所有權限。

只能在卡巴斯基安全管理中心內建立和使用內部使用者帳戶。內部使用者的資料不會傳送到作業系統上。卡巴斯基安全管理中心將驗證內部使用者。

您可在主控台樹狀目錄中的**使用者帳戶**資料夾設定內部使用者帳戶。

管理伺服器設定的備份和還原

管理伺服器設定和其資料庫的備份透過備份工作和 klbackup 公用程式執行。備份副本包括與管理伺服器有關的所有主要設定和物件，例如憑證、用於加密受管理裝置上磁碟機的主金鑰、各種產品授權的金鑰、管理群組的結構及其所有內容、工作、政策等。使用備份副本，您可以盡快還原管理伺服器的運行，這需要花費十幾分鐘到幾個小時的時間。

如果沒有備份副本可用，失敗可能導致憑證和管理伺服器設定的不可挽回的損失。這將導致要重新開始配置卡巴斯基安全管理中心，並在組織網路上重新執行網路代理初始化佈署。所有受管理裝置驅動程式加密金鑰也將遺失，導致 Kaspersky Endpoint Security 裝置上不可挽回的加密資料遺失。因此，不要略過使用標準備份工作對管理伺服器做一般備份。

快速啟動精靈為管理伺服器設定建立備份工作，並設定成每日在 4:00 AM 執行。備份副本預設儲存在 %ALLUSERSPROFILE%\Application Data\KasperskySC 資料夾。

如果安裝在其他裝置上的 Microsoft SQL Server 實例被用作 DBMS，您必須透過指定 UNC 路徑修改備份工作，這可以透過管理伺服器服務和 SQL Server 服務寫入，作為儲存備份副本的資料夾。這個需求來自 Microsoft SQL Server DBMS 備份的特殊功能。

如果一個本機 Microsoft SQL Server 執行個體被作為 DBMS 使用，建議您儲存備份副本到專用媒介，以便保證它們的安全。

因為備份副本包含重要資料，備份工作和 klbackup 公用程式用於備份副本密碼防護。預設下，備份工作使用空密碼建立。您必須在備份工作內容中設定密碼。略過該需求將導致管理伺服器憑證所有金鑰、產品授權金鑰和受管理裝置驅動程式加密金鑰保持未加密。

除了一般備份，您必須在每個顯著變更之前建立備份副本，包括管理伺服器升級和修補程式的安裝。

如果您使用 Microsoft SQL Server 作為 DBMS，則可以最小化備份副本的大小。如要最小化備份副本的大小，請啟用 SQL Server 設定中的**壓縮備份**選項。

從備份副本的還原使用管理伺服器上剛剛安裝的與建立的備份副本具有相同或更新版本的公用程式 klbackup 來執行。

欲執行還原的管理伺服器實例，必須使用相同類型（例如，相同的 SQL Server 或 MariaDB）和相同或更新版本的 DBMS。管理伺服器版本可以相同（帶有相同或更新修補程式）或更新。

這部分敘述了還原管理伺服器設定和物件的標準情境。

使用檔案系統快照降低備份時間

在卡巴斯基安全管理中心 14.2，管理伺服器備份的空閒時間相比早期版本被降低。而且，**使用檔案系統快照以備份資料**功能被新增到工作設定。該功能透過使用 klbackup 實用工具提供附加空間降低，這將在備份過程中增加磁碟的磁區影副本（這將花費幾秒鐘）並同時複製資料庫（這花費最多幾分鐘）。當 klbackup 建立磁碟磁區影副本和資料庫副本時，實用程式再次使管理伺服器可連線。

您僅可以在滿足這兩個條件時使用檔案系統快照功能：

- 管理伺服器共用資料夾和 %ALLUSERSPROFILE%\KasperskyLab 資料夾位於相同邏輯磁碟以及管理伺服器本機。
- %ALLUSERSPROFILE%\KasperskyLab 資料夾不包含任何手動建立的符號連結。

如果任何條件都不能滿足，則不使用該功能。此種情況下，應用程式在建立檔案系統快照時將回傳錯誤訊息。

要使用功能，您必須擁有授予了建立 %ALLUSERSPROFILE% 所在邏輯磁碟的快照的權限的帳戶。注意，管理伺服器服務帳戶沒有此權限。

要使用檔案系統快照功能以便降低備份時間：

1. 在**工作**區域，選取備份工作。
2. 在右鍵選單中，選取**內容**。
3. 在開啟的"工作內容"視窗中，選取"**設定**"區域。
4. 選取**使用檔案系統快照以備份資料**核取方塊。
5. 在**使用者名稱**和**密碼**欄位，輸入具有建立 %ALLUSERSPROFILE% 所在邏輯磁碟的快照的權限的帳戶的名稱和密碼。
6. 點擊"**套用**"。

在備份工作的後續啟動中，klbackup 實用程式將建立檔案系統快照，以便在工作執行中降低管理伺服器空閒時間。

管理伺服器裝置不可操作

如果管理伺服器裝置由於失敗而不可操作，建議您執行以下操作：

- 新管理伺服器必須分配相同的位址：NetBIOS 名稱、FQDN 或靜態 IP（取決於佈署網路代理時的設定）。
- 安裝管理伺服器，使用相同類型、相同版本（或更新）的 DBMS。您可以安裝帶有相同（或更新）修補程式的相同（或更新）版本的伺服器。安裝後，不要透過精靈執行初始化安裝。
- 在**開始**功能表，執行 klbackup 公用程式並執行還原。

管理伺服器設定或資料庫被損壞

如果管理伺服器由於設定或資料庫損壞（例如斷電）而不可操作，建議您使用以下還原方案：

1. 掃描被損壞裝置上的檔案系統。
2. 移除管理伺服器的不可操作版本。
3. 重新安裝管理伺服器，使用相同類型、相同版本（或更新）的 DBMS。您可以安裝帶有相同（或更新）修補程式的相同（或更新）版本的伺服器。安裝後，不要透過精靈執行初始化安裝。
4. 在**開始**功能表，執行 klbackup 公用程式並執行還原。

禁止用除了透過 klbackup 公用程式的其他方法還原管理伺服器。

任何試圖透過協力廠商軟體還原管理伺服器的操作都將不可避免地導致卡巴斯基安全管理中心分發節點上的資料的不一致和應用程式操作不正常。

備份複製和管理伺服器資料還原

資料備份允許您將管理伺服器從一台裝置上轉移至其他裝置且無資料遺失。將管理伺服器從一台裝置上轉移至其他裝置或者將其轉換為新版本卡巴斯基安全管理中心時，您可以使用備份還原資料。此外，您也可以使用資料備份將管理伺服器資料從卡巴斯基安全管理中心 Windows 移動到卡巴斯基安全管理中心 Linux 管理下（不支援將資料從卡巴斯基安全管理中心 Linux 移至卡巴斯基安全管理中心 Windows）。

請注意，已安裝的管理外掛程式沒有備份。從備份副本還原管理伺服器資料後，您需要下載並重新安裝受管應用程式的外掛程式。

備份管理伺服器資料之前，請檢查管理群組中是否新增了虛擬管理伺服器。如果新增了虛擬管理伺服器，請確保在備份之前為該虛擬管理伺服器分配了管理員。備份後，您將無法授予管理員對虛擬管理伺服器的存取權限。請注意，如果管理員帳戶憑據丟失，您將無法向虛擬管理員伺服器分配新管理員。

您可以使用以下方式之一建立管理伺服器資料備份：

- 透過使用管理主控台建立並執行資料備份工作。
- 透過在已安裝管理伺服器的裝置上執行 klbackup 公用程式。該公用程式包含在卡巴斯基安全管理中心分發套件。管理伺服器安裝完畢後，該公用程式位於程式安裝時指定資料夾的根目錄中。

以下資料儲存在管理伺服器的備份副本中：

- 管理伺服器資料庫（政策、工作、應用程式設定、管理伺服器上儲存的事件）。
- 有關管理群組和用戶端裝置的架構的設定資訊。

- 用於遠端安裝的應用程式分發套件的儲存。
- 管理伺服器憑證。

只用使用 klbackup 公用程式才能進行管理伺服器還原。

備份管理伺服器資料工作

建立備份管理伺服器資料工作

備份工作是管理伺服器工作；它透過快速啟動精靈建立。如果由快速啟動精靈建立的備份工作被刪除，您可以手動建立備份工作。

若要建立管理伺服器資料備份工作：

1. 在主控台樹狀目錄中，選取**工作**資料夾。
2. 透過下列方式開始建立工作：
   - 在主控台樹狀目錄的**工作**資料夾上下文功能表中，選取**新增 → 工作**。
   - 點擊工作區中的**建立工作**按鈕。

   新工作精靈啟動。遵照精靈的說明。在該精靈的**選取工作類型**視窗中，選取名為**備份管理伺服器資料**的工作類型。

備份管理伺服器資料工作只能建立單份副本。如果已經為管理伺服器建立了管理伺服器資料備份工作，它不會顯示在管理伺服器備份工作建立精靈的工作類型選取視窗中。

配置備份管理伺服器資料工作

建立備份工作後，您可以配置工作設定。

若要設定管理伺服器資料備份工作：

1. 在主控台樹狀目錄中，選取**工作**資料夾。
2. 在**備份管理伺服器資料**工作的上下文功能表中，選取**內容**。

   *管理伺服器資料備份*工作的內容視窗將開啟。以下功能可用：

- **一般**

  在**一般**部分中，您可以指定工作名稱、檢視工作建立日期、最後命令日期、工作啟動狀態和工作結果。
- **通知**

  在**通知**部分，您可以指定與工作執行結果相關的事件的儲存設定，以及配置有關工作執行結果的通知。

- **排程**

  在**排程**部分中，您可以指定工作啟動排程。

- **目的**

  在**目的**部分中，您可以指定將儲存管理伺服器資料備份副本的資料夾路徑。

- **設定**

  在**設定**部分，您可以根據需要設定備份防護密碼和備份副本數量。

  您也可以建立儲存 %ALLUSERSPROFILE%資料夾的邏輯磁碟的磁碟區副本並複製管理伺服器資料庫。為此，您必須啟用**使用檔案系統快照以備份資料**選項，然後指定有權建立快照的帳戶的名稱和密碼。

- **安全性**

  在**安全性**部分中，您可以授予使用者和群組在管理伺服器上執行操作的權限。如果啟用**從管理伺服器繼承設定**選項，則工作的安全設定將從管理伺服器繼承。

  如果停用該選項，您可以配置工作的安全設定。您可以分配角色到使用者或使用者群組或分配權限到使用者或使用者群組，如工作中所套用。

  預設啟用**從管理伺服器繼承設定**選項。

- **變更歷程**

  在**變更歷程**部分，您可以追蹤工作修改情況。您每次儲存工作變更時，修訂被建立。

資料備份和還原實用程式 (klbackup)

您可以使用卡巴斯基安全管理中心發佈套件中隨附的 klbackup 公用程式複製管理伺服器資料以作備份和將來還原之用。

klbackup 公用程式可用以下兩種模式執行：

- 互動
- 靜默

互動模式下的資料備份和還原

透過使用 klbackup 公用程式以互動模式建立的備份副本還原管理伺服器資料可能會出現錯誤。如果您已經安裝了管理伺服器修補程式 14.2.0.48079-pf5，然後在停用**遷移資料庫**選項的情況下使用 klbackup 公用程式建立備份副本，則在還原此副本時會發生錯誤（對於除 MySQL 和 MariaDB 之外的所有 DBMS）。如果您已安裝管理伺服器修補程式 14.2.0.26967-pf5，並且想要建立備份副本而不遷移到另一個 DBMS，請使用資料備份工作或從命令列執行 klbackup 公用程式。

若要以互動模式建立管理伺服器資料備份，請執行以下操作：

1. 執行位於卡巴斯基安全管理中心安裝資料夾的 klbackup 實用程式。

   這樣將啟動備份和還原精靈。

2. 在精靈的第一個視窗中，選取**執行管理伺服器資料備份**。

   如果您選取**僅還原或備份管理伺服器憑證**選項，將只儲存管理伺服器憑證和私鑰的備份副本。當您執行從卡巴斯基安全管理中心 Windows 管理伺服器到卡巴斯基安全管理中心 Linux 管理伺服器的遷移時，備份管理伺服器憑證和私鑰可能會有用。此外，您也可以在卡巴斯基安全管理中心 Windows 管理伺服器之間遷移受管理裝置。有關詳細資訊，請參閱使用 klbackup 公用程式切換在另一個管理伺服器的管理下的受管理裝置。

   點擊**"下一步"**。

3. 在精靈的下一個視窗中，指定以下選項：

   - **備份目的地資料夾**
   - **移轉資料庫**

     如果您目前將管理伺服器資料儲存在 Microsoft SQL Server 資料庫中，並且需要將其移轉到下列資料庫之一，請啟用此選項：MySQL 或 MariaDB、PostgreSQL 或 Postgres Pro、Azure SQL。預設情況下已停用該選項。

     - **遷移到 MySQL/MariaDB 格式**

       如果您目前使用 SQL Server 作為管理伺服器的 DBMS，並且希望將資料從 SQL Server 遷移到 MySQL 或 MariaDB DBMS，請啟用此選項。卡巴斯基安全管理中心將建立一個與 MySQL 和 MariaDB 相容的備份。之後，您可以將資料從備份還原到 MySQL 或 MariaDB。

     - **遷移到 Postgres**

       如果您目前使用 SQL Server 作為管理伺服器的 DBMS，並且希望將資料從 SQL Server 遷移到 PostgreSQL 或 Postgres Pro DBMS，請啟用此選項。卡巴斯基安全管理中心將建立一個與 PostgreSQL 或 Postgres Pro 相容的備份。之後，您可以將資料從備份還原到 PostgreSQL 或 Postgres Pro。

       只有當您安裝了管理伺服器的修補程式 14.2.0.26967-pf5 以支援遷移到 PostgreSQL 和 Postgres Pro 時，此選項才可用。如果您使用基於卡巴斯基安全管理中心 Windows 14.2 的Kaspersky Secure Mobility Management，請使用修補程式14.2.0.48079-pf5。聯絡卡巴斯基技術支援以取得此修補程式。

     - **移轉到 Azure 格式**

       如果您目前使用 SQL Server 作為管理伺服器的 DBMS，並且希望將資料從 SQL Server 遷移到 Azure SQL DBMS，請啟用此選項。卡巴斯基安全管理中心將建立一個與 Azure SQL 相容的備份。之後，您可以將資料從備份還原到 Azure SQL。

   - **將目前日期和時間包含在備份目的資料夾名稱裡**
   - **備份密碼**

4. 點擊“**下一步**”按鈕，開始備份。

5. 如果您在雲端環境（例如 Amazon Web Services (AWS) 或 Microsoft Azure）使用資料庫，請在**登入到線上儲存**視窗填入以下欄位：

   - 對於 AWS：

     - **S3 bucket 名稱**

       您為備份建立的 S3 bucket 名稱。

     - **存取金鑰 ID**

       當您建立了 IAM 使用者帳戶以使用 S3 bucket 儲存實例時，您接收到金鑰 ID（數字字母序列）。

       如果您在 S3 bucket 上選取了 RDS 資料庫則該欄位可用。

     - **金鑰**

       您建立 IAM 使用者帳戶時接收到的帶有存取金鑰 ID 的金鑰。

       金鑰的字元顯示為星號。在您開始輸入金鑰後，**顯示**按鈕被顯示。按一下並按住該按鈕一定時間以檢視輸入的字元。

       如果您選取了 AWS IAM 存取金鑰來授權而不是 IAM 角色，該欄位可用。

   - 對於 Microsoft Azure：

     - **Azure 儲存帳戶名稱**

       您建立了 Azure 儲存帳戶名稱以使用卡巴斯基安全管理中心。

     - **Azure 訂購 ID**

       您在 Azure 網站建立了該訂購。

     - **Azure 密碼**

       當您建立應用程式 ID 時您收到應用程式 ID 的密碼。

       密碼的字元顯示為星號。在您開始輸入密碼後，**顯示**按鈕可用。按一下並按住該按鈕以檢視您輸入的字元。

     - **Azure 應用程式 ID**

       您在 Azure 網站建立了該應用程式 ID。

       您僅可以提供一個 Azure 應用程式 ID 用於輪詢和其他目的。如果您要輪詢其他 Azure 段，您必須先刪除現有 Azure 連線。

     - **Azure SQL Server 名稱**

名稱和資源群組在您的 Azure SQL Server 內容中可用。

- **Azure SQL Server 資源群組**

  名稱和資源群組在您的 Azure SQL Server 內容中可用。

- **Azure 儲存存取金鑰**

  在您的儲存帳戶內容中可用，在存取金鑰區域。您可以使用任何金鑰（key1 或 key2）。

若要以互動模式還原管理伺服器資料，請執行以下操作：

1. 執行位於卡巴斯基安全管理中心安裝資料夾的 klbackup 實用程式。使用與安裝管理伺服器時相同的帳戶啟動 klbackup 實用程式。我們建議您在新安裝的管理伺服器上執行該公用程式。

   這樣將啟動備份和還原精靈。

2. 在精靈的第一個視窗中，選取**還原管理伺服器資料**，然後點擊**下一步**。

   如果您選取**僅還原或備份管理伺服器憑證**選項，將只還原管理伺服器憑證和私鑰。

   當您在非活動故障轉移群集節點上執行 klbackup 公用程式時，您會被提示選擇下列選項之一：指定管理伺服器憑證或自動從管理伺服器擷取資料。

3. 在精靈的**還原設定**視窗中：

   - 指定包含管理伺服器資料備份副本的資料夾。

     如果您在例如 AWS 或 Azure 的雲端環境中工作，指定儲存位址。此外，確保該檔案名稱為 backup.zip。

   - 指定資料備份中輸入的密碼。

     在還原資料時，您必須指定在備份過程中輸入的密碼。如果某個共用資料夾的路徑在備份工作完成後發生變更，請檢查使用還原資料工作的操作（還原工作和遠端安裝工作）。必要時，編輯這些工作的設定。當從備份檔案還原資料時，沒有人可以存取管理伺服器的共用資料夾。啟動 klbackup 實用程式所使用的帳戶必須對該共用資料夾具有完全存取權限。

4. 點擊"**下一步**"按鈕，還原資料。

靜默模式下的資料備份和還原

若要以靜默模式建立備份副本或還原管理伺服器資料，

在已安裝管理伺服器的裝置上，利用命令列和所需金鑰集執行 klbackup 公用程式。

使用 klbackup 公用程式時，網路代理標誌不會被還原。您需要手動設定網路代理標誌。

公用程式的命令列語法：

```
klbackup -path <備份路徑> [-linux_path <SQL Server 備份路徑>][-node_cert <憑證路徑>] [-
logfile <日誌檔案>] [-use_ts]|[-restore] [-password <密碼>] [-cert_only] [-online] [-
migrate postgres]
```

如果在 klbackup 公用程式的命令列中沒有指定密碼，該公用程式將提示您輸入密碼。

參數敘述：

- `-path <backup path>` — 在備份資料夾中儲存資訊或使用備份資料夾中的資料進行還原（必填參數）。

  資料庫伺服器帳戶和 klbackup 公用程式需要獲得變更備份資料夾中資料的權限。

- `-linux_path <SQL Server 備份路徑>` — Linux 上存放 SQL Server 備份資料的資料夾在本機上的路徑。

  資料庫伺服器帳戶和 klbackup 公用程式需要獲得變更 SQL Server 備份資料夾中資料的權限。

- `-node_cert <憑證路徑>` — 在還原後設定非作用中的容錯移轉叢集節點時，所用的伺服器憑證檔案。如果未設定，將自動從伺服器擷取。

  當您在非活動故障轉移群集節點上執行 klbackup 公用程式時，請使用此金鑰指定伺服器憑證的路徑。

- `-logfile <log file>` — 儲存關於管理伺服器資料備份和還原的報告。

- `-use_ts`—儲存資料時，將資訊複製到備份資料夾，複製到`klbackup` 中以 `YYYY-MM-DD # HH-MM-SS`格式命名的子資料夾，其中包括目前日期和操作時間 (UTC)。如果未指定鍵，資訊將儲存在備份資料夾的根目錄。

  當您嘗試將資訊儲存至已儲存備份副本的資料夾時，系統會回傳錯誤訊息。不會更新任何資訊。

  `-use_ts` 鍵允許您維護管理伺服器資料壓縮檔案。例如，如果 `-path` 鍵指明資料夾 `C:\KLBackups`，資料夾 `klbackup 2022/6/19 # 11-30-18`，那麼程式將儲存管理伺服器截止 2022 年 6 月 19 日 11:30:18 AM. 的狀態資訊。例如，如果 -path 鍵指明資料夾 C:\KLBackups，資料夾 klbackup 2022/6/19 # 11-30-18，那麼程式將儲存管理伺服器截止 2022 年 6 月 19 日 11:30:18 AM. 的狀態資訊。

- `-restore`—還原管理伺服器資料。系統將基於備份資料夾內包含的資訊執行資料還原。如果沒有可用的金鑰，資料會備份在備份資料夾內。

- `-password <密碼>`—用於保護敏感資料的密碼。

  忘記的密碼無法被還原。沒有密碼要求。密碼長度不受限制，並且無長度（無密碼）也是可能的。

  在還原資料時，您必須指定在備份過程中輸入的密碼。如果某個共用資料夾的路徑在備份工作完成後發生變更，請檢查使用還原資料工作的操作（還原工作和遠端安裝工作）。必要時，編輯這些工作的設定。當從備份檔案還原資料時，沒有人可以存取管理伺服器的共用資料夾。啟動 klbackup 公用程式所使用的帳戶必須對該共用資料夾具有完全存取權限。我們建議您在新安裝的管理伺服器上執行該公用程式。

- `-online`—透過建立卷快照來備份管理伺服器資料以最小化管理伺服器的離線時間。當您使用實用程式恢複資料時，該選項被略過。

- `-migrate postgres`—建立儲存在與 PostgreSQL 和 Postgres Pro 相容的 SQL Server 資料庫中的備份管理伺服器資料。您可以將備份中的資料還原到 PostgreSQL 或 Postgres Pro。當您使用管理伺服器資料備份執行向卡巴斯基安全管理中心 Linux 的遷移時使用此旗標。

  只有當您為管理伺服器安裝了修補程式 14.2.0.26967-pf5 以支援遷移到 PostgreSQL 和Postgres Pro，此選項才可用。如果您使用基於卡巴斯基安全管理中心 14.2 Windows 的Kaspersky Secure Mobility Management，請使用修補程式 14.2.0.48079-pf5。聯絡卡巴斯基技術支援以取得所需的修補程式。

使用 klbackup 公用程式切換在另一個管理伺服器的管理下的受管理裝置

klbackup 公用程式可讓您切換在另一個管理伺服器管理下的受管理裝置。執行遷移時，您可以使用 klbackup 公用程式將卡巴斯基安全管理中心 Windows 管理伺服器變更為卡巴斯基安全管理中心 Linux 管理伺服器。此外，您也可以在卡巴斯基安全管理中心 Windows 管理伺服器之間遷移受管理裝置。

要使用 klbackup 公用程式將受管理裝置切換到另一個管理伺服器的管理下：

1. 在先前的裝置上，使用 klbackup 實用程式介面建立管理伺服器憑證和私鑰的備份副本。

   執行位於卡巴斯基安全管理中心安裝資料夾中的 klbackup 公用程式，然後使用**僅還原或備份管理伺服器憑證**選項建立備份。

2. 在之前的裝置上，中斷管理伺服器與網路的連線。

3. 使用另一個管理伺服器將相同的位址分配給裝置。

   可以為新管理伺服器指派 NetBIOS 名稱、FQDN 和靜態 IP 位址。這取決於部署網路代理時在網路代理安裝套件中設定的管理伺服器位址。或者，您可以使用確定網路代理連線到管理伺服器的連線位址（您可以使用 klnagchk 公用程式在受管理裝置上取得此位址）。

4. 在具有另一個管理伺服器的裝置上，從備份副本還原管理伺服器憑證和私鑰。

   您可以使用下列方法之一還原備份副本：

   - 使用 klbackup 實用程式介面（僅適用於卡巴斯基安全管理中心 Windows 管理伺服器）

     執行 klbackup 公用程式，然後使用**僅還原或備份管理伺服器憑證**選項還原備份。

   - 透過使用命令提示符（適用於卡巴斯基安全管理中心 Windows 和卡巴斯基安全管理中心 Linux 管理伺服器版本 15.1 或更高版本）

     從命令列使用 `-cert_only` 金鑰執行 klbackup 公用程式，以還原管理伺服器憑證和私鑰的備份副本：

     `klbackup -path <管理伺服器憑證備份副本的路徑> -restore -cert_only`

受管理裝置被置於另一個管理伺服器的管理之下。您可以轉至此管理伺服器並確保受管理裝置在網路中可見，並且網路代理已安裝並在其上執行（***可見***、**可見**和**網路代理已安裝**列中的網路代理正在執行值）。

使用 MySQL 或 MariaDB 時備份和還原管理伺服器資料

您可以使用資料備份將管理伺服器資料從卡巴斯基安全管理中心 Windows 遷移到卡巴斯基安全管理中心 Linux 的管理下。使用管理伺服器資料備份進行遷移僅支援從任何受支援的卡巴斯基安全管理中心 Windows 版本遷移到卡巴斯基安全管理中心 Linux 15.2 或更高版本。

如果您使用 MySQL 或 MariaDB 作為卡巴斯基安全管理中心 Windows 和卡巴斯基安全管理中心 Linux 的 DBMS，則目前 DBMS 和新 DBMS 的 `lower_case_table_names` 參數必須相符。否則，管理伺服器資料將無法正確遷移。

在卡巴斯基安全管理中心 Windows 上備份管理伺服器資料之前，請檢查 `lower_case_table_names` 參數值。如果先前安裝 DBMS 時沒有指定該參數，則使用預設參數值。Windows 的 `lower_case_table_names` 參數的預設值為 `1`。

在為卡巴斯基安全管理中心 Linux 安裝 MySQL 或 MariaDB 時，請使用MySQL 網站上的說明將 `lower_case_table_names` 參數設定為與 Windows 中該參數指定的值相同的值。如果不指定該參數，則使用預設參數值。對於基於 Linux 的作業系統，`lower_case_table_names` 參數的預設值與 Windows 的預設值不同。

如果要安裝 MySQL 8.0，可能無法依照該說明指定 `lower_case_table_names` 參數。這種情況下，您必須先安裝 MySQL 5.7，使用說明指定 `lower_case_table_names` 參數，然後將 MySQL 5.7 升級到 MySQL 8.0。如果 `lower_case_table_names` 參數與目前 DBMS 和新 DBMS 不匹配，則管理伺服器資料將無法被正確復原。

將管理伺服器移動至其他裝置

如果您需要在新裝置上使用管理伺服器，您可以通過以下方式之一移動它：

- 將管理伺服器和資料庫伺服器移至新裝置（資料庫伺服器可以與管理伺服器一起安裝在新裝置上，也可以安裝在其他裝置上）。
- 將資料庫伺服器保留在以前的裝置上，僅將管理伺服器移動到新裝置上。

將管理伺服器移動至新裝置：

1. 在之前的裝置上，建立管理伺服器資料的備份。

   為此，您可以透過管理主控台執行資料備份工作或執行 klbackup 公用程式。

   > 如果您目前使用 SQL Server 作為管理伺服器的 DBMS，則可以將資料從 SQL Server 遷移到 MySQL 或 MariaDB DBMS。若要這麼做，請執行互動模式下的 klbackup 公用程式來建立資料備份。在備份和還原精靈的**備份設定**視窗中啟用**遷移到 MySQL/MariaDB 格式**選項。卡巴斯基安全管理中心將建立一個與 MySQL 和 MariaDB 相容的備份。之後，您可以將資料從備份還原到 MySQL 或 MariaDB。

   > 如果您想要將資料從 SQL Server 遷移到 Azure SQL DBMS，也可以啟用**移轉到 Azure 格式**選項。

2. 在之前的裝置上，中斷管理伺服器與網路的連線。

3. 選擇要在上面安裝管理伺服器的新裝置。確保所選裝置上的硬體和軟體符合管理伺服器、管理主控台和網路代理的要求。另外，檢查一下管理伺服器上使用的連接埠是否可用。

4. 為新裝置分配相同的位址。

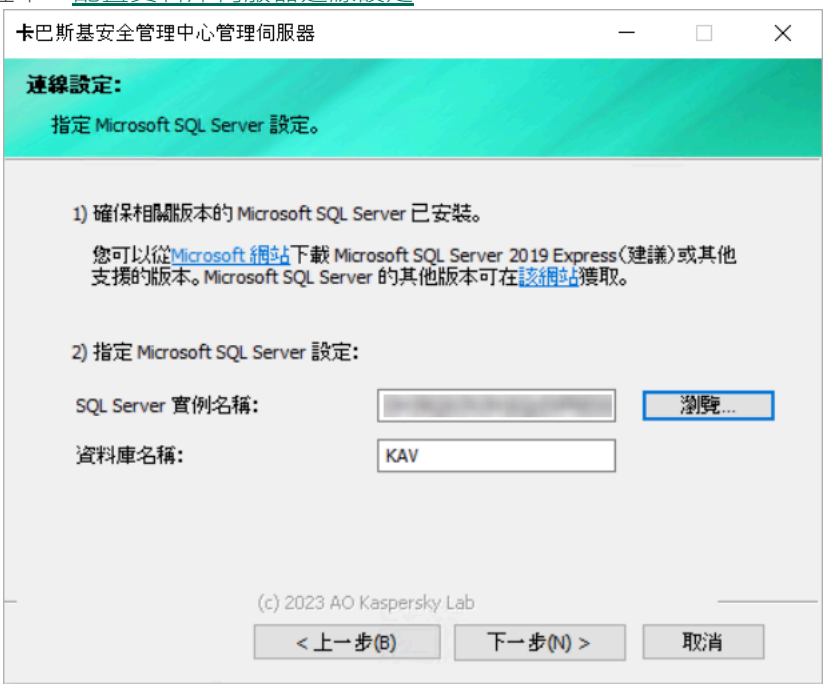
   可以為新管理伺服器指派 NetBIOS 名稱、FQDN 和靜態 IP 位址。這取決於部署網路代理時在網路代理安裝套件中設定的管理伺服器位址。或者，您可以使用確定網路代理連線到管理伺服器的連線位址（您可以使用 klnagchk 公用程式在受管理裝置上取得此位址）。

5. 如有需要，在其他裝置上，安裝管理伺服器將使用的資料庫管理系統 (DBMS)。

   資料庫可以與管理伺服器一起安裝在新裝置上，也可以安裝在其他裝置上。確保該裝置符合硬體和軟體要求。選擇 DBMS 時，請考慮管理伺服器涵蓋的裝置數量。

6. 在新裝置上執行管理伺服器安裝。

7. 在管理伺服器安裝過程中，配置資料庫伺服器連線設定。



Microsoft SQL Server 的連線設定視窗範例

根據所需放置資料庫伺服器的位置，執行以下操作之一：

- **將資料庫伺服器保留在先前裝置上**

  1. 點擊**SQL Server 實例名稱**欄位旁邊的**瀏覽**按鈕，然後在出現的清單中選擇之前的裝置名稱。
     請注意，先前裝置必須可用於連線新的管理伺服器。
  2. 在**資料庫名稱**欄位中輸入以前的資料庫名稱。

- **將資料庫伺服器移至另一個裝置**

  1. 點擊**瀏覽**欄位旁邊的**SQL Server 實例名稱**按鈕，然後在出現的清單中選擇裝置名稱。
  2. 在**資料庫名稱**欄位中輸入新資料庫名稱。
     請注意，新資料庫名稱必須與先前裝置中的資料庫名稱相符。資料庫的名稱必須相同，才能使用管理伺服器備份。預設資料庫名稱是 *KAV*。

8. 安裝完成後，使用 klbackup 公用程式在新裝置上還原管理伺服器資料。

   如果您在舊裝置和新裝置上使用 SQL Server 作為 DBMS，請注意新裝置上安裝的 SQL Server 版本必須與舊裝置上安裝的 SQL Server 版本相同或更高。否則，您將無法在新裝置上還原管理伺服器資料。

9. 開啟管理主控台，並連線到管理伺服器。

10. 驗證所有受管理裝置都已連線到管理伺服器。

11. 從之前的裝置中解除安裝管理伺服器和資料庫伺服器。

您也可以使用卡巴斯基安全管理中心網頁主控台，將管理伺服器和資料庫伺服器移至另一台裝置。

避免多個管理伺服器之間的衝突

如果您的網路中有多於一個管理伺服器，它們可以看到相同的用戶端裝置。例如，這可能會導致管理伺服器安裝另一個管理伺服器已經安裝的應用程式，以及其他衝突。為了防止應用程式被安裝在由另一台管理伺服器管理的裝置上，您必須在**僅安裝到透過該管理伺服器管理的裝置遠端安裝應用程式**_工作屬性中啟用遠端安裝應用程式僅在透過此管理伺服器管理的裝置上安裝_選項。

如果啟用**僅安裝到透過該管理伺服器管理的裝置**選項，然後執行_遠端安裝應用程式_工作，則會執行檢查以確定裝置是否由另一台管理伺服器管理。對於由另一台管理伺服器管理的裝置，**由不同管理伺服器管理**屬性值將設定為`true`。_遠端安裝應用程式_工作將不會被套用於這些裝置。

由不同管理伺服器管理屬性值顯示在**受管理裝置由不同管理伺服器管理未指派的裝置**清單中的由不同管理伺服器管理列中。

您也可以使用**由不同管理伺服器管理**內容作為以下目的的標準：

- 搜尋裝置
- 裝置分類
- 裝置移動規則
- 自動標記規則

若要重設"由不同管理伺服器管理"屬性：

1. 在卡巴斯基安全管理中心網頁主控台的主功能表中，前往**發現和佈署 → 未配置的裝置**。
2. 選擇所需的裝置，然後按一下**清空"由不同管理伺服器管理"核取方塊**按鈕。

由不同管理伺服器管理屬性被重設。

兩步驟驗證

本節介紹如何使用兩步驟驗證來減少未授權存取管理主控台或卡巴斯基安全管理中心 網頁主控台的風險。

關於雙步驟驗證

為帳戶啟用雙步驟驗證後，除了使用者名稱和密碼外，還需要一次性安全代碼才能登入網頁主控台或卡巴斯基安全管理中心網頁主控台。啟用網域身分驗證後，使用者只需輸入一次性安全碼即可。

要使用雙步驟驗證，請在行動裝置或電腦上安裝可產生一次性安全碼的身份驗證器應用程式。您可以使用任何支援基於時間的一次性密碼演算法 (TOTP) 的應用程式，例如：

- Google Authenticator
- Microsoft Authenticator

- Bitrix24 OTP
- Yandex Key
- Avanpost 驗證器
- Aladdin 2FA

要檢查卡巴斯基安全管理中心是否支援您要使用的身分驗證器應用程式，請為所有使用者或特定使用者啟用雙步驟驗證。

其中步驟之一建議您指定由身分驗證器應用程式產生的安全代碼。如果成功，則卡巴斯基安全管理中心支援所選的身分驗證器。

我們強烈建議您將秘密金鑰或 QR 碼儲存在安全的地方。如果您遺失了行動裝置，這有助於您復原對卡巴斯基安全管理中心網頁主控台的存取。

為了確保使用卡巴斯基安全管理中心，您可以為自己的帳戶啟用雙步驟驗證，並為所有使用者啟用雙步驟驗證。

您可以從雙步驟驗證中排除帳戶。對於無法接收身分驗證安全碼的服務帳戶，這可能是必需的。

規則和限制

為了能夠為所有使用者啟動雙步驟驗證並為特定使用者停用雙步驟驗證：

- 確保您的帳戶在**一般功能：使用者權限**功能區域中有修改物件 ACL 權限。
- 對帳戶啟用雙步驟驗證。

為了能夠為所有使用者停用雙步驟驗證：

- 確保您的帳戶在**一般功能：使用者權限**功能區域中有修改物件 ACL 權限。
- 使用雙步驟驗證登入卡巴斯基安全管理中心網頁主控台。

如果在卡巴斯基安全管理中心管理伺服器 13 或者更高版本上為使用者帳戶啟用了雙步驟驗證，則該使用者將無法登入卡巴斯基安全管理中心網頁主控台版本 12、12.1 或 12.2。

重新發布金鑰

任何使用者都可以重新發布用於雙步驟驗證的金鑰。當使用者使用重新發布的秘密金鑰登入到管理伺服器時，新的秘密金鑰將為使用者帳戶進行儲存。如果使用者輸入錯誤的新秘密金鑰，新秘密金鑰將不會得到儲存，當前秘密金鑰仍然有效。

安全碼具有名為*簽發者名稱*的識別碼。安全碼簽發者名稱用作驗證應用程式中管理伺服器的識別碼。安全碼簽發者名稱的預設值與管理伺服器的名稱相同。您可以變更安全碼簽發者名稱的名稱。如果變更了安全碼簽發者名稱，則必須簽發新的金鑰並將其傳遞給驗證應用程式。

情境：為所有使用者配置雙步驟驗證

此情境說明如何為所有使用者啟用雙步驟驗證，以及如何從雙步驟驗證中排除使用者帳戶。如果在為其他使用者啟用帳戶前未啟用帳戶的雙步驟驗證，則應用程式會先開啟用於為帳戶啟用雙步驟驗證的視窗。此情境還說明如何為您自己的帳戶啟用雙步驟驗證。

如果您為帳戶啟用了雙步驟驗證，則可以進入為所有使用者啟用雙步驟驗證的階段。

先決條件

開始之前：

- 確保您的使用者帳戶具有**一般功能：使用者權限**功能區域的修改物件 ACL 權限，用於修改其他使用者帳戶的安全設定。
- 確保管理伺服器的其他使用者在其裝置上安裝驗證應用程式。

階段

為所有使用者啟用雙步驟驗證將分階段進行：

1. **在裝置上安裝驗證應用程式**

   您可以安裝任何支援基於時間的一次性密碼演算法 (TOTP) 的應用程式，例如：

   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP
   - Yandex Key
   - Avanpost 驗證器
   - Aladdin 2FA

   要檢查卡巴斯基安全管理中心是否支援您要使用的身分驗證器應用程式，請為所有使用者或特定使用者啟用雙步驟驗證。

   其中步驟之一建議您指定由身分驗證器應用程式產生的安全代碼。如果成功，則卡巴斯基安全管理中心支援所選的身分驗證器。

   我們強烈建議不要在與管理伺服器建立連線的同一台裝置上安裝驗證器應用程式。

2. **將驗證應用程式時間與安裝了管理伺服器的裝置時間同步**

   透過使用外部時間來源，確保具有身分驗證器應用程式的裝置上的時間和具有管理伺服器的裝置上的時間與 UTC 同步。否則，雙步驟驗證的認證和啟動過程中可能會出現失敗。

3. **對您的帳戶啟用雙步驟驗證，並為您的帳戶接收金鑰**

說明：

- 對於 MMC 型管理主控台：對您自己的帳戶啟用雙步驟驗證
- 對於卡巴斯基安全管理中心網頁主控台：對您自己的帳戶啟用雙步驟驗證

為帳戶啟用雙步驟驗證後，您可以為所有使用者啟用雙步驟驗證。

4. **對所有使用者啟用雙步驟驗證**

   啟用了雙步驟驗證的使用者必須使用它登入管理伺服器。

   說明：

   - 對於 MMC 型管理主控台：對所有使用者啟用雙步驟驗證
   - 對於卡巴斯基安全管理中心網頁主控台：對所有使用者啟用雙步驟驗證

5. **編輯安全碼簽發者的名稱**

   如果您有多個具有相似名稱的管理伺服器，則可能必須更改安全碼簽發者的名稱，以便更進一步識別不同的管理伺服器。

   說明：

   - 對於 MMC 型管理主控台：編輯安全碼簽發者的名稱
   - 對於卡巴斯基安全管理中心網頁主控台：編輯安全碼簽發者的名稱

6. **排除不需要啟用兩步驟驗證的使用者帳戶**

   如有需要，您可以從雙步驟驗證中排除使用者。具有被排除帳戶的使用者不必使用雙步驟驗證即可登入管理伺服器。

   說明：

   - 對於 MMC 型管理主控台：從雙步驟驗證中排除帳戶
   - 對於卡巴斯基安全管理中心網頁主控台：從雙步驟驗證中排除帳戶

7. **為您自己的帳戶配置兩步驟驗證**

   如果使用者未被排除在雙步驟驗證之外，並且尚未為其帳戶配置雙步驟驗證，則他們需要在登入卡巴斯基安全管理中心時開啟的視窗中進行配置。否則，他們將無法按照其權限存取管理伺服器。

   說明：

   - 對於 MMC 型管理主控台：為您自己的帳戶配置雙步驟驗證
   - 對於卡巴斯基安全管理中心網頁主控台：為您自己的帳戶配置雙步驟驗證

結果

完成此情境後：

- 對帳戶啟用雙步驟驗證。
- 為管理伺服器的所有使用者帳戶啟用了雙步驟驗證，但已排除的使用者帳戶除外。

對您自己的帳戶啟用雙步驟驗證（基於 MMC）

在為帳戶啟用雙步驟驗證之前，請確保在行動裝置上安裝了身份驗證器應用程式。驗證應用程式中設定的時間必須與管理伺服器的時間同步。

若要對帳戶啟用兩步驟驗證，請執行以下操作：

1. 在卡巴斯基安全管理中心主控台樹狀目錄中，開啟**管理伺服器**資料夾的右鍵選單並選取**內容**。
2. 在「管理伺服器屬性」視窗中，轉到**區段**窗格，然後選取**進階**，然後選取**兩步驟驗證**。
3. 在**兩步驟驗證**區段中，點擊**設定**按鈕。

   如果您的帳戶已啟用兩步驟驗證，按一下**設定**按鈕將重設金鑰，以便您可以重新配置兩步驟驗證。

   在開啟的兩步驟驗證屬性視窗中，顯示金鑰。
4. 在驗證應用程式中輸入金鑰以接收一次性安全代碼。您可以在身份驗證器應用程式中手動指定秘密金鑰，也可以使用行動裝置上的身份驗證器應用程式掃描 QR 碼。
5. 指定由驗證應用程式產生的安全代碼，然後點擊**確定**按鈕關閉兩步驟驗證屬性視窗。
6. 點擊**套用**按鈕。
7. 點擊**確定**按鈕。

您自己的帳戶已啟用兩步驟驗證。

對所有使用者啟用雙步驟驗證（基於 MMC）

如果您的帳戶具有**一般功能：使用者權限**功能區域中的修改物件 ACL 權限，並且您透過雙步驟驗證進行了身分驗證，則可以為管理伺服器的所有使用者啟用雙步驟驗證。

若要為多個使用者啟用或停用雙步驟驗證，請執行以下操作：

1. 在卡巴斯基安全管理中心主控台樹狀目錄中，開啟**管理伺服器**資料夾的右鍵選單並選取**內容**。
2. 在管理伺服器內容視窗的**區段**視窗，選取**進階**之後選取**兩步驟驗證**。
3. 點擊**設為必要**按鈕可為所有使用者啟用兩步驟驗證。

4. 如果未啟用帳戶的雙步驟驗證，則該應用程式將開啟一個視窗，以為您自己的帳戶啟用雙步驟驗證。

   a. 在驗證應用程式中輸入金鑰以接收一次性安全代碼。您可以在驗證應用程式中手動指定秘密金鑰，也可以使用行動裝置上的驗證應用程式掃描 QR 碼以接收一次性安全碼。

   b. 指定由驗證應用程式產生的安全代碼，然後點擊**確定**按鈕關閉兩步驟驗證屬性視窗。

5. 在**兩步驟驗證**區段中，點擊**套用**按鈕，然後點擊**確定**按鈕。

為所有使用者啟用了雙步驟驗證。從現在開始，除了其帳戶被排除在雙步驟驗證之外的使用者之外，管理伺服器的所有使用者（包括在啟用此選項後新增的使用者）都必須為其帳戶配置雙步驟驗證。

對使用者帳戶停用雙步驟驗證（基於 MMC）

若要停用使用者帳戶的兩步驟驗證，請執行以下操作：

1. 在卡巴斯基安全管理中心主控台樹狀目錄中，開啟**管理伺服器**資料夾的右鍵選單並選取**內容**。
2. 在管理伺服器內容視窗的**區段**視窗，選取**進階**之後選取**兩步驟驗證**。
3. 在**兩步驟驗證**區段中，點擊**停用**按鈕。
4. 點擊**套用**按鈕。
5. 點擊**確定**按鈕。

您的帳戶已停用兩步驟驗證。

您可以停用其他使用者帳戶的兩步驟驗證。這樣可以在使用者遺失或損壞行動裝置的情況下提供保護。

> 您必須具有**一般功能：使用者權限**功能區域中的修改物件 ACL 權限，並且您透過雙步驟驗證進行了身分驗證，才可以為另一個使用者帳戶停用雙步驟驗證。按照以下步驟操作，您也可以為自己的帳戶停用兩步驟驗證。

若要停用使用者帳戶的兩步驟驗證，請執行以下操作：

1. 在主控台樹狀目錄中，選取**使用者帳戶**資料夾。

   使用者帳戶資料夾預設是**進階**資料夾的子資料夾。

2. 在工作區中，按兩下要停用兩步驟驗證的使用者帳戶。

   對於已啟用雙步驟驗證的所有使用者帳戶，**需要 2FA**列設定為**是**。

3. 在開啟的**屬性：<使用者名稱>**視窗中，選取**兩步驟驗證**區段。
4. 在**兩步驟驗證**區段中，選取以下選項：
   - 如果要為所有使用者啟用兩步驟驗證，請點擊**停用**按鈕。
   - 如果您要從兩步驟驗證中排除此使用者帳戶，請選取**使用者僅可使用使用者名稱和密碼通過驗證**選項。
5. 點擊**套用**按鈕。
6. 點擊**確定**按鈕。

使用者帳戶的兩步驟驗證已停用。

如果想為無法使用雙步驟驗證登入管理主控台的使用者恢復存取權限，請為此使用者帳戶停用雙步驟驗證，然後如上文所述，在**雙步驟驗證使用者僅可使用使用者名稱和密碼通過驗證**User can pass authentication by using user name and password only選項。之後，以停用了雙步驟驗證的使用者帳戶登入管理主控台，然後再次啟用驗證。

對所有使用者停用要求的雙步驟驗證（基於 MMC）

如果您具有**一般功能：使用者權限**功能區域中的修改物件 ACL 權限，並且透過雙步驟驗證進行身分驗證，則可以對管理伺服器的所有使用者停用要求的雙步驟驗證。

若要為所有使用者啟用和停用雙步驟驗證：

1. 在卡巴斯基安全管理中心主控台樹狀目錄中，開啟**管理伺服器**資料夾的右鍵選單並選取**內容**。
2. 在管理伺服器內容視窗的**區段**視窗，選取**進階**之後選取**兩步驟驗證**。
3. 點擊**設為選用**按鈕可為所有使用者停用兩步驟驗證。
4. 點擊**兩步驟驗證**區段中**的應用**按鈕。
5. 點擊**兩步驟驗證**區段中的**確定**按鈕。

所有使用者均停用雙步驟驗證。為所有使用者停用雙步驟驗證並不適用於先前單獨啟用雙步驟驗證的特定帳戶。

從雙步驟驗證中排除帳戶（基於 MMC）

如果您的帳戶具有**一般功能：使用者權限**功能區域中的修改物件 ACL 權限，則可以從兩步驟驗證中排除該帳戶。

如果將使用者帳戶排除在兩步驟驗證之外，則該使用者可以登入管理主控台或者卡巴斯基安全管理中心 網頁主控台，而無需使用兩步驟驗證。

對於在身分驗證期間無法通過安全碼驗證的服務帳戶，可能有必要從雙步驟驗證中排除帳戶。

若要從兩步驟驗證中排除使用者帳戶，請執行以下操作：

1. 如果要排除 Active Directory 帳戶，請執行 Active Directory 輪詢以重新整理管理伺服器使用者清單。
2. 在主控台樹狀目錄中，選取**使用者帳戶**資料夾。
   使用者帳戶資料夾預設是**進階**資料夾的子資料夾。
3. 在工作區中，按兩下要從兩步驟驗證中排除的使用者帳戶
4. 在開啟的**屬性：<使用者名稱>**視窗中，選取**兩步驟驗證**區段。

5. 在開啟的區段中，選取**使用者僅可使用使用者名稱和密碼通過驗證**選項。

6. 在**兩步驟驗證**區段中，點擊**套用**按鈕，然後點擊**確定**按鈕。

此使用者帳戶不包括在兩步驟驗證中。您可以在使用者帳戶清單中檢查排除的帳戶。

編輯安全碼簽發者的名稱（基於 MMC）

您可以為不同的管理伺服器使用多個識別碼（這稱為簽發者）。您可以更改安全碼簽發者的名稱以防萬一，例如，管理伺服器已經為另一台管理伺服器使用了類似的安全碼簽發者名稱。預設情況下，安全碼簽發者的名稱與管理伺服器的名稱相同。

變更安全碼簽發者名稱後，您必須重新簽發新的金鑰並將其傳遞給驗證應用程式。

若要指定安全碼簽發者的新名稱，請執行以下操作：

1. 在卡巴斯基安全管理中心主控台樹狀目錄中，開啟**管理伺服器**資料夾的右鍵選單並選取**內容**。

2. 在管理伺服器內容視窗的**區段**視窗，選取**進階**之後選取**兩步驟驗證**。

3. 在**安全碼簽發者**欄位指定新安全碼簽發者名稱。

4. 點擊**兩步驟驗證**區段中**的應用**按鈕。

5. 點擊**兩步驟驗證**區段中的**確定**按鈕。

為管理伺服器指定了新的安全碼簽發者名稱。

為您自己的帳戶配置兩步驟驗證（基於 MMC）

啟用雙步驟驗證後首次登入卡巴斯基安全管理中心時，為您自己的帳戶配置雙步驟驗證的視窗將開啟。

在為帳戶配置雙步驟驗證之前，請確保在行動裝置上安裝了身份驗證器應用程式。透過使用外部時間來源，確保具有身分驗證器應用程式的裝置上的時間和具有管理伺服器的裝置上的時間與 UTC 同步。

若要對帳戶配置雙步驟驗證，請執行以下操作：

1. 使用行動裝置上的身份驗證器應用程式產生一次性安全碼。要這麼做，請執行以下操作之一：

   - 在身分驗證器應用程式中手動輸入安全碼。
   - 使用身分驗證器應用程式掃描 QR 代碼。

   一個安全碼將顯示在行動裝置上。

2. 在**設定兩步驟驗證**視窗中，指定由身分驗證器應用程式產生的安全碼，然後點擊**確定**按鈕。

   對帳戶配置雙步驟驗證。您可以根據您的權限存取管理伺服器。

變更管理伺服器共用資料夾

管理伺服器共用資料夾是在安裝管理伺服器期間指定的。您可以在安裝後在管理伺服器屬性中變更共用資料夾位置。

要變更共用資料夾：

1. 建立網路共用資料夾並配置共用和資料夾結構的權限，以允許**Everyone**子群組擁有完全控制權限。
2. 在卡巴斯基安全管理中心主控台樹狀目錄中，開啟**"管理伺服器"管理伺服器"內容"**。
3. 在管理伺服器內容視窗的**區域**窗格中，選取**進階**，然後選擇**管理伺服器共用資料夾**。
4. 在**管理伺服器共用資料夾**區域中，點擊**變更**按鈕。
5. 選取要用作共用資料夾的資料夾。
6. 點擊**確定**按鈕以關閉管理伺服器內容視窗。
7. 為選取作為共用資料夾的資料夾分配對 **Everyone** 子群組的讀取權限。

對管理群組進行管理

本章節提供關於如何對管理群組進行管理的資訊。

您可以對管理群組採取以下操作：

- 新增任何數量任何階層的管理群組架構。
- 新增裝置到管理群組。
- 透過將單個裝置和整個群組移至其他群組，以改變管理群組的階層架構。
- 從管理群組中刪除子群組和裝置。
- 將從屬伺服器和虛擬管理伺服器新增至管理群組。
- 將裝置從管理伺服器的管理群組移至其他伺服器的管理群組。
- 定義將哪些 Kaspersky 程式自動安裝到包括在群組中的裝置。

對於要管理的群組（或對於這些群組屬於的管理伺服器），若您在**管理群組管理**的管理區域中有**修改**權限，您可執行這些操作。

建立管理群組

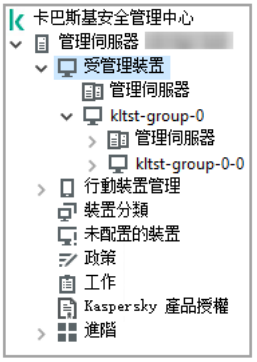
管理群組層次結構是在卡巴斯基安全管理中心程式主視窗的**"受管理裝置"**節點中建立的。管理群組以節點形式顯示在主控台樹狀目錄中（參閱下圖）。

安裝卡巴斯基安全管理中心之後，**受管理裝置**節點只包含空的**管理伺服器**節點。

介面設定決定了**管理伺服器**節點是否出現在主控台樹狀目錄中。若要顯示此資料夾，在功能表選取**檢視 → 設定介面**，然後在開啟的**設定介面**視窗中選取**顯示從屬管理伺服器**核取方塊。

當建立管理群組階層架構時，可以將裝置和子群組新增到**受管理裝置**節點中，也可以新增嵌套群組。您可以將從屬和虛擬管理伺服器新增到**管理伺服器**資料夾。

與**受管理裝置**資料夾一樣，每個初始建立的群組都是僅包含空的**管理伺服器**資料夾，用於處理該群組中的從屬和虛擬管理伺服器。關於該群組的政策和工作的資訊，以及有關該群組所包含裝置的資訊，都會在選項卡上顯示，並在該群組的工作區中具有對應名稱。



檢視管理群組階層架構

要建立管理群組，請執行以下操作：

1. 在主控台樹狀目錄中，展開**受管理裝置**資料夾。
2. 如果您想要建立現有管理群組的子群組，請在**受管理裝置**節點中選取與該群組對應的子節點，該節點應該包括新的管理群組。

   如果您想建立一個新的最高階層管理群組，您可以略過此步驟。
3. 您可以透過下列方式之一進行新增群組的動作：
   - 使用上下文功能表中的**建立 → 群組**命令。
   - 點擊在主應用程式視窗工作區的**裝置**頁籤中的**新群組**按鈕。
4. 在開啟的**"群組名稱"**視窗中輸入群組名稱，然後點擊**"確定"**。

   主控台樹狀目錄將顯示帶有指定名稱的新管理群組資料夾。

程式允許基於 Active Directory 的架構或域網架構建立管理群組結構。您也可以從文字檔案建立群組架構。

要建立管理群組的架構：

1. 在主控台樹狀目錄中，選擇**受管理裝置**資料夾。
2. 從**受管理裝置**資料夾的上下文功能表中，選取**所有工作 → 新群組結構**。

   新管理群組架構精靈啟動。遵照精靈的說明。

移動管理群組

您可以在群組階層架構內移動子群組。

移動群組會連同其下所有子群組、從屬管理伺服器、裝置、群組政策和工作一起移動。程式會將移動群組的所有階層架構及設定放在新位置下。

群組名稱必須在該階層架構的一個級別內唯一。如果在您要移動群組至其他群組時，而其他群組內已有相同名稱的群組，則應該變更要移動群組的名稱。如果尚未變更要移動的群組的名稱，則在移動此群組後，系統將向其名稱新增一個 **(<下一個序號>)** 格式的索引，例如：**(1)**、**(2)**。

您不能重新命名**"受管理裝置"**群組，因為它是管理主控台內建的主要群組。

要將群組移至主控台樹狀目錄的其他群組，請執行以下操作：

1. 在主控台樹狀目錄中選取要移動的群組。
2. 執行以下操作之一：
   - 透過使用上下文功能表移動群組：
     1. 在此群組的上下文功能表中選取**剪下**。
     2. 從您要向其中移動選定群組的上下文功能表中選取**"貼上"**。
   - 使用主程式功能表移動群組：
     a. 在主功能表中選取**操作 → 剪下**。
     b. 在主控台樹狀目錄中選取您必須向其中移動選定群組的管理群組。
     c. 在程式主視窗最上方的功能表中選取**"操作 → 貼上"**。
   - 使用滑鼠將群組拖曳至其他群組。

刪除管理群組

如果群組內不含從屬管理伺服器、子群組或用戶端裝置，並且沒有為其建立任何群組工作或政策，則可以刪除此群組。

在刪除群組之前，您必須先從此群組中刪除所有從屬管理伺服器、子群組和用戶端裝置。

要刪除群組，請執行以下操作：

1. 在主控台樹狀目錄中選取您的管理群組。
2. 執行以下操作之一：
   - 在此群組的上下文功能表中選取**"刪除"**。
   - 在程式主視窗最上方的功能表中選取**"操作 → 刪除"**。
   - 按 **DELETE** 鍵。

自動建立管理群組架構

卡巴斯基安全管理中心允許您使用群組層級建立精靈來建立管理群組的架構。

此精靈依據以下方式建立管理群組的架構：

- Windows 網域和工作群組的架構
- "Active Directory"群組的架構
- 管理員手動建立的文字檔的內容

當文字被產生時，以下需求必須被滿足：

- 每個群組的名稱必須使用 ENTER 鍵換行。空白行將被略過。

  例如：
  Office 1
  Office 2
  Office 3
  將在目標群組中建立三個相同階層的子群組。

- 建立子群組必須使用反斜線符號（/）。

  例如：
  Office 1/Division 1/Department 1/Group 1
  程式將在目標群組中建立四個階層的子群組。

- 要建立相同階層架構的多個子群組，您必須輸入"群組的絕對路徑"。

  例如：
  Office 1/Division 1/Department 1
  Office 2/Division 1/Department 1
  Office 1/Division 3/Department 1
  Office 1/Division 4/Department 1
  程式將在目標群組第一個階層中建立 Office 1 子群組；而 Office 1 子群組下又包含四個相同階層的子群組："Division 1"、"Division 2"、"Division 3"和"Division 4"。最後這四個子群組的每個群組下都會有"Department 1"子群組。

透過精靈建立管理群組層級不影響網路完整性：不更換現有群組，而新增新群組。用戶端裝置不能兩次被包含在管理群組，因為裝置在移動到管理群組時已從**未配置的裝置**群組刪除。

如果在建立管理群組結構時，由於某些原因（被關閉或從網路斷開）未將裝置包含在**未配置的裝置**群組，該裝置將會自動移動到管理群組。您可以在此精靈完成後將用戶端裝置手動新增至管理群組。

要進行自動建立群組架構，請執行以下操作：

1. 在主控台樹狀目錄中選取**受管理裝置**資料夾。
2. 從**受管理裝置**資料夾的上下文功能表中，選取**所有工作 → 新群組結構**。

   新管理群組架構精靈啟動。遵照精靈的說明。

將應用程式自動安裝到管理群組中的裝置

您可以指定必須使用哪些安裝套件以自動遠端安裝卡巴斯基應用程式到管理群組中的用戶端裝置。

要配置自動安裝應用程式在管理群組中的裝置上：

1. 在主控台樹狀目錄中，選定要執行此功能的群組。
2. 於該群組的節點，按上下文功能表選取內容。
3. 在**區域**面板，選取**自動安裝**，然後在工作區選取要安裝到裝置上的應用程式的安裝套件。
4. 點擊**確定**。

   群組工作被建立。這些工作將在新用戶端裝置加入管理群組的時候立即在裝置上執行。

如果自動安裝選定不同版本的軟體建置一個軟體套裝，程式將只會建立最新版本的軟體進行安裝。

管理用戶端裝置

本部分包含用戶端裝置的工作資訊。

將用戶端裝置連線至管理伺服器

用戶端裝置和管理伺服器之間的連線透過安裝在用戶端裝置上的網路代理建立。

當用戶端裝置連線至管理伺服器時，將執行以下操作：

- 自動同步資料：
  - 安裝在用戶端裝置上的應用程式清單同步。
  - 同步政策、應用程式設定、工作和工作設定。
- 依照管理伺服器擷取有關應用程式狀態、工作執行和應用程式操作統計資料的最新資訊。
- 將事件資訊傳送至管理伺服器進行處理。

依據網路代理設定，定期同步資料（例如，每 15 分鐘）。您可以自訂連線的時間間隔。

一旦有任何事件發生，其資訊將被立即傳送至管理伺服器。

如果管理伺服器位於企業網路外部，則用戶端裝置需使用網際網路與其連線。

要透過網際網路將裝置連線至管理伺服器，需符合以下條件：

- 遠端管理伺服器應該有外部 IP 位址，且連接埠 13000 應該保持開啟狀態（為了連線網路代理）。我們建議您也開啟 UDP 連接埠 13000（為了接收裝置關閉通知）。
- 在裝置上安裝網路代理。
- 在裝置上安裝網路代理時，您應該指定遠端管理伺服器的外部 IP 位址。如果使用安裝套件進行安裝，則應該在安裝套件內容的**設定**區域中手動指定外部 IP 位址。
- 若要使用遠端管理伺服器來管理裝置的應用程式和工作，在**一般**區域中該裝置的內容視窗中，選取**不斷開與管理伺服器的連線**方塊。選中該方塊之後，請等待管理伺服器與遠端裝置同步。與管理伺服器保持連線的用戶端裝置的數量不得超過 300。

要提高遠端管理伺服器工作即時性，您可以在裝置上開啟連接埠 15000。在這個情況下，要執行工作，管理伺服器將透過連接埠 15000 向網路代理傳送一個專用封包至用戶端，而不是等待與裝置的同步。

卡巴斯基安全管理中心允許您調整用戶端裝置和管理伺服器之間的連線，使得當所有操作均完成後，仍然保持連線狀態。當需要立即監控應用程式狀態並且因某種原因（例如，連線被防火牆阻擋，不允許開啟用戶端裝置上的連接埠，無法知道用戶端 IP 位址等）管理伺服器無法建立與用戶端電腦的連線時，不中斷與管理伺服器連線是非常重要的。您可以在裝置內容視窗的**一般**區域，建立用戶端裝置和管理伺服器的不間斷連線。

我們建議您和最重要的裝置建立不間斷連線。管理伺服器維護的最大同時連線數被限制到 300。

在手動同步時，系統將使用輔助連線方法，該連線將由管理伺服器發起。在用戶端裝置上開始連線前，您必須開啟 UDP 連接埠。此時管理伺服器將向用戶端裝置的 UDP 連接埠發起連線要求。而收到回應即表示用戶端電腦憑證透過驗證。如果管理伺服器憑證與儲存在用戶端裝置的憑證副本相符，則連線被建立。

手動同步同樣用於取得應用程式狀態、工作執行以及應用程式執行統計的最新資訊。

將用戶端裝置手動連線至管理伺服器。Klmover 公用程式

如果您需要手動將用戶端裝置連線至管理伺服器，您可在用戶端裝置上使用 klmover 公用程式。

用戶端裝置上安裝網路代理時，此公用程式將同樣被複製到網路代理安裝節點。

要使用 klmover 公用程式手動將用戶端裝置連線至管理伺服器：

在裝置上，使用指令提示字元 (CMD) 啟動 klmover 公用程式。

使用指令提示字元時，klmover 公用程式可以執行以下操作（依據當時使用的指令）：

- 將網路代理連線至指定的管理伺服器；
- 將執行結果記錄在事件記錄檔案中或顯示在螢幕上。

對於透過連線閘道連線到管理伺服器的用戶端裝置，您不能使用 klmover 實用程式。對於這樣的裝置，您必須重新設定網路代理或重新安裝網路代理並指定連線閘道。

公用程式的命令列語法：

```
klmover [-logfile <檔案名稱>] [-address <伺服器位址>] [-pn <連接埠號>] [-ps <SSL 連接埠號>] [-nossl] [-cert <憑證檔案的路徑>] [-silent] [-dupfix] [-virtserv] [-cloningmode]
```

執行該公用程式需要管理員權限。

參數敘述：

- `-logfile <檔案名稱>`—將指令執行結果記錄到記錄檔案中。

  預設情況下，資訊將被儲存在標準輸出流中 (stdout)。如果未使用此參數，執行結果和錯誤訊息將顯示在螢幕上。

- `-address <伺服器位址>`—指定連線的管理伺服器的位址。

  您可以使用裝置的 IP 位址、NetBIOS 名稱或 DNS 名稱為指定位址。

- `-pn <埠號>`—用來建立與管理伺服器非加密連線的埠號。

  預設埠號為 14000。

- `-ps <SSL 埠號>`—使用 SSL 與管理伺服器建立加密連線時使用的 SSL 埠號。

  預設埠號為 13000。

- `-nossl`—使用非加密方式連線管理伺服器。

  如果未使用該鍵值，網路代理將透過使用加密的 SSL 協定連線至管理伺服器。

- `-cert <憑證檔案的路徑>`—存取管理伺服器時使用指定的憑證檔案作為身分驗證。

  預設情況下，如果未使用此參數，網路代理將在第一次連線管理伺服器時接收憑證。

- `-silent`—在靜默模式執行公用程式。

  當指令作動成功時，該指令程式將會登入相關資訊在使用者系統註冊資料中。

- `-dupfix`—如果網路代理不是使用一般方式（帶分發套件）安裝，則使用該鍵值 - 範例：透過從 ISO 磁碟映像還原安裝的。

- `-virtserv`—虛擬管理伺服器的名稱。
- `-cloningmode`—網路代理磁碟克隆模式。
  使用以下參數之一配置磁碟克隆模式：
  - `-cloningmode`—請求磁碟克隆模式的狀態。
  - `-cloningmode 1`—啟用磁碟克隆模式。
  - `-cloningmode 0`—停用磁碟克隆模式。
- `-nauninstpwd <`密碼`>`—此金鑰用於指定網路代理解除安裝密碼。
  該金鑰不是必需的。

例如，要將網路代理連線到管理伺服器，請執行以下指令：

```
klmover  -address kscserver.mycompany.com -logfile klmover.log
```

要建立用戶端裝置與管理伺服器之間的通道連線

卡巴斯基安全管理中心允許透過管理伺服器的從管理主控台的 TCP 連線通道，然後透過網路代理到受管理裝置上的指定連接埠。通道設計用於連線安裝管理主控台的裝置上的用戶端應用程式到受管理裝置上的 TCP 連接埠—如果管理主控台和目的裝置之間沒有直接連線可用。

例如，通道用於連線到遠端桌面，可以連線到已存在連線，也可以建立一個新的遠端連線。

通道也可以使用外部工具啟用。例如，管理員可以執行 putty 公用程式、VNC 用戶端和其他工具。

如果用於連線到管理伺服器的連接埠在裝置上不可用，則需要遠端用戶端裝置和管理伺服器之間的連線隧道。在以下情況下裝置連接埠可能無法使用：

- 遠端裝置使用 NAT 機制連線到本機網路。
- 遠端裝置是本機網路管理伺服器的一部分，但是它的連接埠已被防火牆關閉。

檢查用戶端裝置與管理伺服器之間的連線通道：

1. 在主控台樹狀目錄中選取包括該用戶端裝置的群組資料夾。
2. 在**裝置**頁籤上選取該裝置。
3. 在裝置的上下文功能表中，選取**所有工作 → 連線通道**。
4. 在開啟的**連線通道**視窗建立通道。

用戶端裝置的遠端桌面連線

管理員可以在安裝網路代理的用戶端裝置上使用遠端桌面連線。

如果裝置的 TCP 和 UDP 連接埠關閉，也可透過網路代理遠端連線至用戶端裝置。在與裝置建立連線後，管理員會獲取對此裝置上儲存資訊的完全存取權限，以便他或她可以管理其上安裝的應用程式。

本節說明如何透過網路代理建立到 Windows 用戶端裝置和 macOS 用戶端裝置的連線。

連線到 Windows 用戶端裝置

您可使用以下方式之一建立與 Windows 用戶端裝置的遠端連線：

- 透過使用名為「遠端桌面連線」的標準 Microsoft Windows 元件。

  根據標準 Windows 公用程式 mstsc.exe 的設定建立遠端桌面的連線。

- 透過使用 Windows 桌面共用技術。

使用遠端桌面連線來連線到 Windows 用戶端裝置

在使用者不知道的情況下遠端連線到使用者目前的桌面。一旦管理員連線上，裝置使用者將在沒有提前通知的情況下中斷連線。

要透過遠端桌面連線元件連線到用戶端裝置的桌面：

1. 在管理主控台樹狀目錄中，選取您需要獲取存取權限的裝置。
2. 在裝置的上下文功能表中，請選取**所有工作 → 連線到裝置 → 新 RDP 連線**。

   標準 Windows 實用工具 mstsc.exe 將啟動，這有助於與遠端桌面建立連線。
3. 按照公用程式對話框中顯示的說明操作。

與裝置建立連線後，您將能在 Microsoft Windows 的遠端連線視窗中使用桌面。

使用 Windows 桌面共用連線到用戶端裝置：

當連線到遠端桌面的現有連線時，裝置上的連線使用者會收到來自管理員的連線請求。卡巴斯基安全管理中心建立的報告中不會儲存有關裝置上的遠端操作及其結果的任何資訊。

管理員可以連線至用戶端裝置上的現有連線而不會斷開此連線中的使用者。在此情況下，裝置上的管理員和使用者連線將桌面共用存取。

管理員可以在遠端用戶端裝置上設定使用者活動稽核。稽核期間，應用程式會儲存用戶端裝置上管理員開啟和/或修改過的檔案資訊。

使用 Windows 桌面共用連線到用戶端裝置必須符合以下需求：

- 管理員工作站電腦系統環境必須是 Microsoft Windows Vista 或以上版本。管理伺服器裝置作業系統的類型對透過 Windows 桌面共用進行連線沒有限制。

  若要檢查 Windows 桌面共用功能是否隨附於您的 Windows 版本中，請確保 Windows 登錄檔中包含 CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} 機碼。
- 用戶端裝置安裝了 Microsoft Windows Vista 或更新版本。
- 卡巴斯基安全管理中心已安裝弱點和修補程式管理產品授權。

若要透過 Windows 桌面共用連線到用戶端裝置的桌面：

1. 在管理主控台樹狀目錄中，選取您需要獲取存取權限的裝置。
2. 在裝置的上下文功能表中，選取**所有工作 → 連線到裝置 → Windows 共用桌面**。
3. 在開啟的**選取遠端桌面連線**視窗中，選取您想要連線的用戶端裝置。
   如果與裝置成功建立連線，裝置的桌面將會顯示在 **卡巴斯基遠端桌面連線檢視器**視窗中。
4. 若要開始與裝置互動，請在 **卡巴斯基遠端桌面連線檢視器**視窗的主功能表中選取**操作 → 互動模式**。

卡巴斯基遠端桌面連線檢視器公用程式需要商業產品授權。

連線到 macOS 用戶端裝置

管理員可以使用虛擬網路計算 (VNC) 系統連線到 macOS 裝置。

透過安裝在管理伺服器裝置上的 VNC 用戶端建立與遠端桌面的連線。VNC 用戶端將鍵盤和滑鼠控制權從用戶端裝置切換到管理員。

當管理員連線到遠端桌面時，使用者不會收到來自管理員的通知或連線請求。管理員可以連線至用戶端裝置上的現有連線而不會斷開此連線中的使用者。

要透過 VNC 用戶端連線到用戶端 macOS 裝置的桌面，必須符合以下條件：

- VNC 用戶端安裝在管理伺服器裝置上。
- 用戶端裝置允許遠端登入和遠端管理。
- 使用者已在 macOS 作業系統的**分享**設定中，允許管理員存取用戶端裝置。

要透過虛擬網路運算系統連線到用戶端裝置的桌面：

1. 在管理主控台樹狀目錄中，選取您需要獲取存取權限的裝置。
2. 在裝置的上下文功能表中，選取**所有工作 → 連線通道**。
3. 在開啟的**連線通道**視窗中，執行以下操作：
   a. 在**1. 網路連接埠**區域，指定需要連線的裝置的網路連接埠號。
      預設情況下使用連接埠 5900。
   b. 在**2. 通道**區域，點擊**建立通道**按鈕。
   c. 在**3. 網路設定**區域，點擊**複製** 按鈕。
4. 開啟 VNC 用戶端並將複製的網路屬性貼到文字欄位中。按 **Enter**。
5. 在開啟的視窗，檢視憑證詳細資料。如果您同意使用該憑證，請按一下**是**按鈕。
6. 在**身分驗證**視窗，指定用戶端裝置的憑證，然後按一下**確定**。

透過 Windows 桌面共用連線到用戶端裝置

若要透過 Windows 桌面共用連線至裝置，請執行以下操作：

1. 在主控台樹狀目錄的**裝置**資料夾中，選取**受管理裝置**嵌套資料夾。

   該資料夾的工作台顯示裝置清單。

2. 在您要連線的裝置的上下文功能表中，選取**連線到裝置 → Windows 共用桌面**。

   選取遠端桌面連線視窗開啟。

3. 在**選取遠端桌面連線**視窗中選取使用者連線至裝置的桌面連線。

4. 點擊**"確定"**。

   裝置被連線。

設定重新啟動用戶端裝置

當使用、安裝或移除卡巴斯基安全管理中心時，您必須重新啟動裝置。您僅可以對 Windows 裝置指定重新啟動設定。

配置用戶端裝置的重新啟動:

1. 在主控台樹狀目錄中，選取必須為其設定重新啟動的管理群組。

2. 在群組的工作區中，選取**政策**頁籤。

3. 在工作區，在政策清單中選取卡巴斯基安全管理中心網路代理的政策，然後在政策的上下文功能表中選取**"內容"**。

4. 在政策內容視窗中，選取**重新啟動管理**區段。

5. 如果需要重新啟動裝置，選取必須執行的操作：

   - 選取**不要重新啟動作業系統**以封鎖自動重新啟動。
   - 選取**如果必要，自動重新啟動作業系統**以允許自動重新啟動。
   - 選取**提示使用者操作**啟用提示使用者允許重新啟動。

   您可以透過選取對應的核取方塊和選值框中的時間來指定重新啟動請求的頻率，強制重新啟動和強制關閉裝置上連線的程式。

6. 點擊**確定**儲存變更並且關閉政策內容視窗。

   裝置的重新啟動將被設定。

稽核在遠端用戶端裝置上執行的操作

程式允許對管理員在遠端 Windows 用戶端裝置上的操作啟用審核。稽核期間，應用程式儲存有關裝置上管理員開啟和/或修改過的檔案資訊。當符合以下條件時，管理員可使用操作稽核：

- 弱點和修補程式管理授權使用中。
- 管理員有權啟動共用存取遠端裝置的桌面。

啟用稽核在遠端用戶端電腦上執行的操作：

1. 在主控台樹狀目錄中，選取應該為其設定管理員操作稽核的管理群組。
2. 在群組的工作區中，選取**政策**頁籤。
3. 選取卡巴斯基安全管理中心網路代理的政策，然後在政策的上下文功能表中選取**內容**。
4. 在政策內容視窗中，選擇**Windows 共用桌面**區段。
5. 選擇**啟用稽核**核取方塊。
6. 在**讀取時要監控的檔案遮罩**和**修改時要監控的檔案遮罩**清單中，在稽核期間必須監控動作的應用程式上新增檔案遮罩。

   預設情況下，應用程式監控對副檔名為 txt、rtf、doc、xls、docx、xlsx、odt 和 pdf 的檔案執行的操作。
7. 點擊**確定**儲存變更並且關閉政策內容視窗。

因此，設定了管理員在桌面共用存取遠端裝置上的操作稽核。

遠端裝置上的管理員操作是被一一記錄下來的：

- 在遠端裝置的事件記錄中。
- 在遠端裝置上網路代理資料夾中副檔名為 syslog 的檔案中（例如：C:\ProgramData\KasperskyLab\adminkit\1103\logs）。
- 在卡巴斯基安全管理中心事件資料庫中。

檢查用戶端裝置與管理伺服器之間的連線

卡巴斯基安全管理中心允許您手動或自動檢查用戶端裝置與管理伺服器之間的連線。

偵測連線由管理伺服器執行。手動檢查連線在用戶端裝置上執行。

自動檢查用戶端裝置與管理伺服器之間的連線

若要執行偵測用戶端裝置與管理伺服器的連線，請執行以下操作：

1. 在主控台樹狀目錄中選取包括該裝置的管理群組。
2. 在管理群組工作區中的**裝置**頁籤選取裝置。
3. 在裝置的上下文功能表中，選取**偵測裝置可用性**。

這將開啟包含裝置可用性資訊的視窗。

手動檢查用戶端裝置與管理伺服器之間的連線。Klnagchk 公用程式

您可以透過使用 klnagchk 公用程式手動檢查連線和取得用戶端裝置與管理伺服器之間的連線設定資訊。klnagchk 公用程式位於網路代理的安裝資料夾。

使用指令提示字元時，klnagchk 公用程式可以執行以下操作（依據當時使用的指令）：

- 顯示或記錄用以連線裝置上網路代理到管理伺服器的設定值。
- 將網路代理統計資料（自上次啟動以來）和公用程式執行結果記錄在事件記錄檔案中或者顯示在螢幕上。
- 嘗試建立網路代理和管理伺服器之間的連線。

  如果連線嘗試失敗，公用程式將傳送 ICMP 封包檢查管理伺服器的裝置狀態。

要使用 klnagchk 公用程式檢查用戶端裝置和管理伺服器之間的連線，請執行以下操作：

在安裝了網路代理的裝置上，使用本機管理員帳戶從命令列啟動 klnagchk 公用程式。

公用程式的命令列語法：

```
klnagchk [-logfile <檔案名稱>] [-sp] [-savecert <憑證檔案的路徑>] [-restart][-sendhb]
```

參數敘述：

- `-logfile <檔案名稱>`—將網路代理和管理伺服器之間連線設定值和公用程式操作結果記錄到記錄檔案中。

  預設情況下，資訊將被儲存在標準輸出流中 (stdout)。如果未使用此參數，設定、執行結果和錯誤訊息將顯示在螢幕上。
- `-sp`—在代理伺服器顯示用於使用者驗證的密碼。

  如果是透過代理伺服器與管理伺服器建立連線，則需使用此金鑰。
- `-savecert <檔案名稱>` – 在指定指定檔案中儲存用於存取管理伺服器的憑證。
- `-restart`—公用程式執行完成後啟動網路代理。
- `-sendhb`—啟動網路代理與管理伺服器的同步。

啟動後，klnagchk 公用程式將存取網路代理的設定檔並顯示連線參數。這些參數是在網路代理安裝期間和網路代理政策設定中指定的：

- `Current device`—用戶端裝置的 Windows 網路名稱。
- `Network Agent version`—安裝在裝置上網路代理版本的完整編號（具備修補程式）
- `Administration Server address`—管理伺服器的位址。
- `Use SSL`—指示連線到管理伺服器時是否使用安全連線的參數。

  可能的值：

  - 0 — 不使用安全連線。
  - 1— 使用安全連線。
- `Compress traffic`—指示用戶端裝置和管理伺服器之間的流量是否被壓縮的參數。
- `Numbers of the Administration Server SSL ports`—使用安全連線時與管理伺服器通訊的有效連接埠數。
- `Numbers of the Administration Server ports`—使用普通連線時與管理伺服器通訊的有效連接埠號碼。
- `Use proxy server`—指示是否使用代理伺服器的參數。

  可能的值：

  - 0 — 不使用代理伺服器。
  - 1— 使用代理伺服器。
- `Address`—代理伺服器的位址和連接埠，以冒號分隔。僅當使用代理伺服器時才會顯示此參數。
- `User name`—存取代理伺服器的使用者名稱。僅當使用代理伺服器時才會顯示此參數。
- `Password`—存取代理伺服器的密碼。僅當使用代理伺服器時才會顯示此參數。若要顯示代理伺服器密碼，您需要在命令中使用`sp`金鑰。
- `Administration Server certificate`—指示用戶端裝置是否具有管理伺服器憑證的參數。例如，如果網路代理從未成功連線到管理伺服器，則憑證可能不存在。

  可能的值：

  - `not installed`—用戶端裝置沒有管理伺服器憑證。
  - `available`—用戶端裝置具有管理伺服器憑證。
- `Open UDP port`—指示網路代理是否使用 UDP 連接埠從管理伺服器接收同步請求的參數。

  可能的值：

  - 0 — UDP 連接埠已關閉，無法接收來自管理伺服器的同步請求。
  - 1— UDP 連接埠已開啟，用來接收來自管理伺服器的同步請求。
- `Numbers of UDP ports`—網路代理可以使用的 UDP 連接埠數。

- `Location name`—裝置的網路位置。
- `State of network location`—指示用戶端裝置是否可以從一個管理伺服器連線設定檔切換到另一個的參數。

  可能的值：

  - `Enabled`—可以為用戶端裝置切換管理伺服器連線設定檔。
  - `Disabled`—無法為用戶端裝置切換管理伺服器連線設定檔。
- `Profile to use`—管理伺服器的連線設定檔。
- `Condition`—用戶端裝置連線到的網路的 IP 位址和子網路遮罩。
- `Synchronization interval (min)`—同步之間的標準間隔。
- `Connection timeout (in seconds)`—連線逾時。
- `Send / receive timeout (in seconds)`—讀寫操作的連線逾時。
- `Device ID`—網路中的裝置識別碼。`Device ID`在特定管理伺服器管理的用戶端裝置中是唯一的。
- `Locations of connection gateways`—用於透過連線閘道將用戶端裝置連線到管理伺服器的參數。
- `Location of distribution points`—用於透過發佈點將用戶端裝置連線到管理伺服器的參數。
- `Connection with server`—指示連線閘道是否與管理伺服器持續連線的參數。此參數僅在用戶端裝置充當連線閘道時顯示。

  可能的值：

  - `active`—連接閘道與管理伺服器保持持續連線。
  - `inactive`—連線閘道沒有與管理伺服器的持續連線。
- `Connection with server through connection gateway`—指示是否正確建立透過連線閘道與管理伺服器的連線的參數。此參數僅在用戶端裝置充當連線閘道時顯示。

  可能的值：

  - `active`—透過連線閘道與管理伺服器的連線已正確建立。
  - `inactive`— 透過連線閘道與管理伺服器的連線未正確建立。

此外，klnagchk 公用程式輸出可以包含以下行之一：

- `Administration Server is installed on this device`—klnagchk 公用程式在管理伺服器裝置上執行。
- `This device has been assigned a connection gateway but is not yet registered on Administration Server` — klnagchk 公用程式在安裝了網路代理的裝置上以連線閘道模式執行。配置的連線閘道正在等待來自管理伺服器的連線，但管理伺服器未在受管理裝置中列出該裝置。您需要確保管理伺服器啟動到連線閘道的連線。
- `This device is a connection gateway`— klnagchk 公用程式在充當連線閘道的裝置上執行。
- `Acts as a distribution point`— klnagchk 公用程式在充當發佈點的裝置上執行。

klnagchk 公用程式檢查網路代理服務的狀態。如果該服務未執行，則公用程式將停止。如果服務正在執行，則公用程式會顯示以下連線統計資料：

- `Total number of synchronization requests`—嘗試將用戶端裝置連線到管理伺服器的次數。
- `The number of successful synchronization request`—將用戶端裝置連線到管理伺服器的成功嘗試次數。
- `Total number of synchronizations`—嘗試將用戶端裝置設定與管理伺服器設定同步的次數。
- `The number of successful synchronizations`—嘗試將用戶端裝置設定與管理伺服器同步的成功次數。
- `Date/time of the last request for synchronization`—上次連線的日期和時間。

在分析管理伺服器和網路代理之間的連線時，您需要使用`Total number of synchronization requests`和`The number of successful synchronization request`參數。只有當管理伺服器設定發生變更（例如，新增工作或修改政策設定）時，用戶端裝置設定才會與管理伺服器設定同步。否則，`Total number of synchronizations`和`The number of successful synchronizations`參數值保持不變。

有關如何解決網路代理連線到管理伺服器問題的更多資訊，請參閱卡巴斯基安全管理中心常見問題解答。

關於檢查裝置和管理伺服器之間的連線時間

在關閉裝置時，網路代理通知管理伺服器該事件。在裝置顯示為已關閉的管理主控台。然而，網路代理無法通知管理伺服器所有此類事件。因此，管理伺服器會定期分析每台裝置的**連線至管理伺服器**內容（內容值會顯示在管理主控台，在裝置內容中的**一般**區域），並將它與網路代理目前設定中的同步間隔相比較。如果一台裝置在超過三次成功的同步間隔後未回應，該裝置被標記為已關閉。

在管理伺服器上識別用戶端裝置

用戶端裝置是基於它們的名稱識別的。在所有連線到管理伺服器的裝置中，裝置的名稱是唯一的。

當輪詢 Windows 網路並發現新電腦時，或者當裝置上安裝的網路代理第一次連線管理伺服器時，系統都將會把裝置名稱傳至管理伺服器。預設情況下，此名稱與裝置在 Windows 網路中的名稱（NetBIOS 名稱）相同。如果某裝置的名稱已經存在於管理伺服器中，新的裝置將在其名稱後面依順序加入序號，範例：**<Name>-1**、**<Name>-2**。在該名稱下，裝置被新增到管理群組。

將裝置移動至管理群組

您可以將管理群組中的裝置移動至另一個群組，前提是您必須在**管理群組管理**區域中對來源與目標管理群組（或是對於這些群組屬於的管理伺服器）具有**修改**權限。

要把一台或多台裝置新增至一個選定的管理群組中，請執行以下操作：

1. 在主控台樹狀目錄中，展開**受管理裝置**資料夾。
2. 在**受管理裝置**資料夾，選取對應包含用戶端裝置的群組的子資料夾。
   如果要將裝置包含到**受管理裝置**群組中，則可以略過此步驟。
3. 在所選取的群組的工作區中，選取**裝置**頁籤，使用下列方式之一將裝置包含到管理群組：
   - 透過在裝置清單的資訊方塊中，點擊**將裝置移動至群組**連結以將裝置新增到群組中。
   - 透過在裝置清單的上下文功能表中選取**建立 → 裝置**。

   行動裝置精靈啟動。按照說明進行操作，選取任一方式將裝置移動到群組中，建立該群組中包括的裝置清單。

   如果手動建立裝置清單，則可以使用 IP 位址（或 IP 範圍）、NetBIOS 名稱或 DNS 名稱作為裝置的位址。您可以在連線裝置或裝置發現後手動將那些其資訊已經新增至管理伺服器資料庫的裝置移動至清單中。

   要從檔案匯入裝置清單，請指定含有新增裝置位址的資訊清單檔案（TXT 檔案）。每個位址必須個別指定。

該精靈完成後，管理群組中將包括選定的裝置，並在管理伺服器產生的裝置清單中顯示其名稱。

> 將裝置從**未配置的裝置**資料夾中拖曳到管理群組資料夾後即可將其移動至選定管理群組。

變更用戶端裝置的管理伺服器

您可以使用"*變更管理伺服器*"工作來變更用戶端裝置連線的管理伺服器。

要變更用戶端裝置連線的管理伺服器：

1. 在主控台樹狀目錄中，選取**工作**資料夾。
2. 在此資料夾的工作區，點擊**新工作**按鈕。
   新工作精靈啟動。使用**下一步**按鈕進行精靈。
3. 在精靈的**選取工作類型**步驟，選擇**卡巴斯基安全管理中心管理伺服器**節點，展開**進階**資料夾，然後選擇**變更管理伺服器**工作。
4. 在開啟的視窗中，按一下**確定**按鈕確認您同意變更用戶端裝置管理伺服器的條款。

5. 在精靈的**設定**步驟，選擇您想要用來管理所選裝置的管理伺服器：

- **變更到另一個主管理伺服器**

  若要將用戶端裝置移至另一台主管理伺服器，請指定下列管理伺服器連線設定：

  1. 在**管理伺服器**欄位中，指定新的主管理伺服器的位址。
  2. 在**連接埠**欄位中，指定要連線到管理伺服器的連接埠號碼。
     預設埠號為 14000。
  3. 在**SSL 連接埠**欄位中，指定主管理伺服器上的 SSL 連接埠號。
     預設埠號為 13000。
  4. 如果有必要，請選取**使用代理伺服器**核取方塊。
     如果此核取方塊被清除，則使用直接連線將裝置連線到管理伺服器。
     如果此核取方塊被選取，請指定代理伺服器參數：
     - **代理伺服器位址**
     - **代理伺服器連接埠**

     如果您的代理伺服器需要身分驗證，請在**使用者名稱** 和 **密碼**欄位中指定與代理伺服器建立連線的帳戶的憑據。我們建議您指定僅具有代理伺服器身分驗證所需的最低權限的帳戶的憑據。
  5. 如果有必要，請上傳新的管理伺服器憑證。

- **變更到該主伺服器上的另一個虛擬伺服器**

  選擇此選項可以將用戶端裝置移至目前主管理伺服器上的虛擬管理伺服器。為此，在**虛擬管理伺服器名稱**欄位中指定必要的虛擬管理伺服器的名稱。

如有必要，請指定重新啟動網路代理之前的等待時間。

6. 在精靈的這一步，選擇要對其指派工作的裝置：

- **選取管理伺服器偵測到的網路裝置**。此種情況下，工作被分配到指定裝置。特定裝置可以包含管理群組的裝置和未配置的裝置。
- **手動指定裝置位址或從清單匯入位址**。您可以指定您要為其分配工作的裝置的 NetBIOS 名稱、DNS 名稱、IP 位址和 IP 子網路。
- **分配工作到裝置分類**。此種情況下，工作被分配到先前建立的分類中的裝置。您可以指定預先定義的分類或您所建立的自訂分類。
- **分配工作到管理群組**。此種情況下，工作被分配到先前建立的管理群組中的裝置。

7. 在精靈的**選取要執行此工作的帳戶**步驟中，指定帳戶設定：

- **預設帳戶**

  在與執行該工作的應用程式相同的帳戶下執行該工作。
  預設情況下已選定此選項。

- **指定帳戶**

  填寫**帳戶**與**密碼**欄位以指定工作要在其下執行的帳戶詳情。帳戶必須對此工作有足夠的權限。

  - **帳戶**

    執行該工作的帳戶。

  - **密碼**

    工作執行時使用的帳戶的密碼。

8. 在精靈的**設定工作排程**步驟，您可以為啟動工作建立排程。如果必要，指定以下設定：

- **排程開始：**

  選取工作執行排程並設定所選排程。

  - **每天（不支援日光節約時間）**

    工作定期執行，按照指定天數間隔。排程不支援日光節約時間 (DST)。這意味著在夏令時開始和結束時當時鐘向前或向後撥動一小時時，實際工作啟動時間不變更。

    我們不建議您使用該排程。它用於向後相容卡巴斯基安全管理中心。

    預設下，工作每天於目前系統時間執行一次。

  - **按每星期中的指定日**

    工作定期執行，在每周指定日期的指定時間。

    預設下，工作每週五 6:00:00 P.M. 執行。

  - **每月**

    工作定期執行，在指定月日的指定時間。

    在缺少指定日的月份，工作在最後一天執行。

    預設下，工作在每月的第一天執行，在目前系統時間。

  - **一次**

    此工作在指定的日期和時間（預設情況下，在建立工作的當天）執行一次。

  - **手動**

    工作不自動執行。您僅可以手動啟動。

    預設情況下已選定此選項。

  - **立即**

    當裝置在網路上可見或當裝置被納入工作範圍後，工作會立即執行。

- **執行錯過的工作**

該選項決定在工作要啟動時用戶端裝置在網路中不可見時工作的行為。

如果啟用該選項，系統將在下一次在用戶端裝置上執行 Kaspersky 應用程式時嘗試啟動工作。如果工作排程是**手動**、**一次**或**立即**，裝置在網路中可見或包含在工作範圍後，工作會立即啟動。

如果停用此選項，則僅限排程的工作會在用戶端裝置上執行。若為**手動**、**一次**與**立即**排程，工作僅會在網路上顯示的用戶端裝置上執行。例如，您可能想為消耗資源的工作停用該選項，您僅想在業餘時間執行該工作。

預設情況下已停用該選項。

- **使用工作啟動自動隨機延遲**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動，即是，*分佈式工作啟動*。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  當工作被建立時，根據工作中包含用戶端裝置的數量，分發啟動時間被自動計算。然後，工作總是在計算的開始時間啟動。然後當工作設定被編輯或者工作被手動啟動時，計算的工作啟動時間值被變更。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

- **使用工作啟動隨機延遲間隔（分鐘）**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

  預設情況下已停用該選項。預設時間間隔為一分鐘。

9. 在精靈的此步驟中，指定您正在建立的工作的名稱。

10. 在精靈的**完成工作建立**步驟，點擊**完成**按鈕結束精靈。

    如果您想讓工作在精靈完成時立即啟動，選取**精靈完成時執行工作**核取方塊。

在工作完成後，為其建立工作的用戶端裝置將被工作設定中指定的管理伺服器管理。

如果管理伺服器支援加密和資料防護，並且您正在建立*變更管理伺服器*工作，將顯示警告。警告聲明如果有加密資料儲存在裝置，在新伺服器開始管理裝置之後，使用者將僅可以存取他之前使用過的加密資料。在其他情況下，將無法存取加密資料。如需不會提供加密資料存取權限的情況詳細說明，請參閱 Kaspersky Endpoint Security for Windows 說明。

將透過連線閘道連線到管理伺服器的裝置移至另一台管理伺服器

您可以將透過連線閘道連線到管理伺服器的裝置移至另一台管理伺服器。例如，如果您安裝另一個版本的管理伺服器並且不想在裝置上重新安裝網路代理（因為這可能非常耗時），則可能需要執行此操作。

操作說明中所述的命令必須在具有管理員權限的帳戶下在用戶端裝置上執行。

若要將透過連線閘道連線的裝置移至另一台管理伺服器：

1. 通過 `-address <伺服器位址>` 參數執行klmover 實用程式，切換到新的管理伺服器。
2. 執行`klnagchk -nagwait -tl 4`命令。
3. 執行以下命令設定新的連線閘道：
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_mode -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"`
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_loc -sv "<gateway_ip_or_name>" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`
     在此，`gateway_ip_or_name`是可從網際網路存取的連線閘道的位址。
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_ssl_port -sv 13000 -svt INT_T -ss "|ss_type = \"SS_SETTINGS\";"`
     `13000`是連線閘道正在偵聽的 TCP 連接埠號。
4. 執行`klnagchk -restart -tl 4`指令啟動網路代理服務。

裝置被移動到新的管理伺服器並透過新的連線閘道進行連線。

叢集和伺服器陣列

卡巴斯基安全管理中心支援叢集技術。如果網路代理向管理伺服器傳送資訊確認組成伺服器陣列的用戶端裝置上已安裝該應用程式，則該用戶端裝置就成為一個叢集節點。叢集將作為單個物件新增在主控台樹狀目錄的**受管理裝置**資料夾中，並帶有伺服器圖示（  ）。

可以區分叢集的一些常見功能：

- 叢集及其任何節點始終在同一管理群組中。
- 如果管理員嘗試移動叢集節點，則該節點會移回其原始位置。
- 如果管理員嘗試將叢集移至其他群組，則其所有節點隨之一起移動。

遠端開啟、關閉和重新啟動用戶端裝置

卡巴斯基安全管理中心允許您遠端管理用戶端裝置：開機、關機和重新啟動。

要遠端管理用戶端裝置：

1. 連線至管理裝置的管理伺服器。
2. 使用以下方法之一建立裝置管理工作：
   - 如果您要對所選管理群組中的裝置進行開啟、關閉或重新啟動操作，請建立選定群組的工作。
   - 如需對各管理群組或非群組內的裝置執行開啟、關閉或重新啟動操作，請建立指定裝置的工作。

   新工作精靈啟動。遵照精靈的說明。在新增工作精靈的**選取工作類型**視窗中，選取**卡巴斯基安全管理中心**節點，開啟**進階**資料夾，選取**管理裝置**工作。
3. 執行建立的工作。

工作完成後，選定裝置將執行所選命令（開啟、關閉或重新啟動）。

關於使用受管理裝置和管理伺服器之間的持續連線

預設下，卡巴斯基安全管理中心不提供受管理裝置和管理伺服器之間的持續連線。受管理裝置上的網路代理定期建立連線並與管理伺服器同步。這些同步工作階段之間的間隔在網路代理的政策中定義，預設為 15 分鐘。如果需要早期同步（例如，為了強制套用政策），管理伺服器會傳送一個簽章的網路封包到連接埠 UDP 15000 上的網路代理。管理伺服器可以透過 IPv4 或 IPv6 網路傳送此封包。）如果由於任何原因在管理伺服器和受管理設定之間無法建立 UDP 連線，同步將在下次網路代理和管理伺服器一般連線時執行。

但是，如果沒有網路代理和管理伺服器之間的早期連線，則無法執行某些操作。這些操作包括執行和停止本機工作、接收受管理應用程式的統計以及建立隧道。要使這些操作成為可能，您必須在受管理裝置上啟用 **不斷開與管理伺服器的連線** 選項。

關於強制同步

儘管卡巴斯基安全管理中心自動為受管理裝置同步狀態、設定、工作和政策，一些情況下，管理員需要準確知道是否同步已經在指定裝置上執行。

在管理主控台受管理裝置的上下文功能表中，**所有工作**功能表包含**強制同步**命令。當卡巴斯基安全管理中心 14.2 執行該指令時，管理伺服器試圖連線到裝置。如果該嘗試成功，強制同步將被執行。否則，同步將僅在網路代理與管理伺服器的下一次排程連線後被強制。

關於連線排程

在網路代理內容視窗，在**連線**區域的**連線排程**子區域，您可以指定網路代理傳送資料到管理伺服器的時間間隔。

必要時連線。如果選中此選項，當網路代理需要傳送資料到管理伺服器時連線才被建立。

在指定時間間隔連線。如果選中此選項，網路代理在指定時間連線到管理伺服器。您可以新增若干個連線時間段。

傳送訊息到裝置使用者

要傳送訊息到裝置使用者：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。
2. 以下列方式之一，為裝置使用者建立訊息傳送工作：
   - 如果要向屬於所選管理群組的裝置使用者傳送訊息，請建立所選群組工作。
   - 如果要向屬於不同管理群組或不屬於任何管理群組的裝置使用者傳送訊息，請建立指定裝置的工作。

   新工作精靈啟動。遵照精靈的說明。
3. 在新工作精靈的工作類型視窗中，選取**卡巴斯基安全管理中心管理伺服器**節點，開啟**進階**資料夾，選取**將訊息傳送至使用者**工作。傳送訊息到使用者工作僅對 Windows 裝置可用。您也可在**使用者帳戶**資料夾中，透過使用者的上下文功能表傳送訊息。
4. 執行建立的工作。

工作完成後，建立的訊息將傳送至選定裝置的使用者。傳送訊息到使用者工作僅對 Windows 裝置可用。您也可在**使用者帳戶**資料夾中，透過使用者的上下文功能表傳送訊息。

管理 Kaspersky Security for Virtualization

卡巴斯基安全管理中心支援將虛擬機連線到管理伺服器的功能。虛擬機受 Kaspersky Security for Virtualization 的防護。如需詳細資訊，請參閱此應用程式的說明文件。

設定裝置狀態轉換

您可變更條件以為裝置配置*緊急*或*警告*狀態。

要啟用變更裝置狀態到緊急：

1. 使用下列方式之一開啟內容視窗：
   - 在**政策**資料夾，在管理伺服器政策的上下文功能表中，選取**內容**。
   - 在管理群組的右鍵選單中選取**內容**。
2. 在開啟的**內容**視窗中，在**區域**視窗選取**裝置狀態**。
3. 在工作區，在**若指定以下條件，則設為"緊急"** 區域，從清單中選取條件核取方塊。

> 然而，您可以變更在父政策中未鎖定的設定。

4. 點兩下所選條件的名稱，然後在開啟的視窗中設定該條件所需的值。

   您無法為以下條件設定值：安全應用程式未安裝、安裝了不相容的應用程式、偵測到軟體弱點、行動裝置設定與政策不同、偵測到未處理的事件、應用程式定義的裝置狀態、裝置已失去管理、安全應用程式沒有執行、 產品授權已到期。

   對於**需要重新啟動**條件，可以指定重新啟動的原因。建議您選取清單中所有原因旁邊的核取方塊。

5. 點擊**確定**。

未滿足特定條件時，系統會為受管理裝置配置*緊急*狀態。

要啟用變更裝置狀態到警告：

1. 使用下列方式之一開啟內容視窗：

   - 在**政策**資料夾，在管理伺服器政策的上下文功能表中，選取**內容**。
   - 在管理群組的右鍵選單中選取**內容**。

2. 在開啟的**內容**視窗中，在**區域**視窗選取**裝置狀態**。

3. 在工作區，在**若指定以下條件，則設為"警告"**區域，從清單中選取條件核取方塊。

   然而，您可以變更在父政策中未鎖定的設定。

4. 點兩下所選條件的名稱，然後在開啟的視窗中設定該條件所需的值。

   您無法為以下條件設定值：安全應用程式未安裝、安裝了不相容的應用程式、偵測到軟體弱點、行動裝置設定與政策不同、偵測到未處理的事件、應用程式定義的裝置狀態、裝置已失去管理、安全應用程式沒有執行、 產品授權已到期。

   對於**需要重新啟動**條件，可以指定重新啟動的原因。建議您選取清單中所有原因旁邊的核取方塊。

5. 點擊**確定**。

未滿足特定條件時，系統會為受管理裝置配置*警告*狀態。

標記裝置和檢視分配的標籤

卡巴斯基安全管理中心允許您標記裝置。*標籤*是裝置 ID，可以用於分組、敘述或查找裝置。分配到裝置的標籤可以用於建立分類、尋找裝置以及分發裝置到管理群組。

您可以手動或自動標記裝置。在裝置內容中手動標記裝置；當您必須標記單個裝置時，您可以使用手動標記。自動標記由管理伺服器利用指定標記規則來執行。

在管理伺服器內容中，您可以給由此管理伺服器管理的裝置設定自動標記。當指定條件被滿足時，裝置被自動標記。單個規則對應於每個標記。規則應用到裝置網路內容、作業系統、裝置上安裝的應用程式以及其他裝置內容。例如，您可以設定規則以分配 *Win* 標籤到執行 Windows 的所有裝置。然後，您可以在建立裝置分類時使用該標籤；這將說明您整理所有執行 Windows 的裝置，並給它們分配工作。

您也可以使用標籤作為政策設定檔在受管理裝置上的啟動條件，以便僅在帶有特殊標籤的裝置上應用特殊政策設定檔。例如，如果被標記為 *Courier* 的裝置出現在*使用者*管理群組，且透過標記 *Courier* 對政策設定檔的啟動被啟用，則為*使用者*群組建立的政策將不套用到該裝置 – 但是政策設定檔的設定檔將被套用。政策設定檔可以允許該裝置啟動一些被政策封鎖執行的應用程式。

您可以建立多個標記規則。如果您建立了多個標記規則且規則對應的條件同時被滿足，單個裝置可以被分配多個標籤。您可以在裝置內容中檢視所有分配的標籤清單。每個標記規則可以被啟用或停用。如果規則被啟用，它被套用到由管理伺服器管理的裝置。如果您目前不使用規則，但今後可能需要，您不用刪除它；您只要不勾選**啟用規則**核取方塊即可。在此情況下會停用規則；在再次選取**啟用規則**核取方塊前，此政策都不會執行。如果您必須從標記規則清單臨時排除規則然後以後再次包含它，您可能需要停用規則而不刪除。

自動裝置標記

您可以在管理伺服器“內容”視窗中建立和編輯自動標記規則。

要自動標記裝置：

1. 在主控台樹狀目錄中，選取您要為其指定標記規則的管理伺服器節點。
2. 在管理伺服器的上下文功能表中，選取**內容**。
3. 在管理伺服器內容視窗中，選取**標記規則**區域。
4. 在**標記規則**區段，點擊**新增** 按鈕。
   新規則 視窗隨即開啟。
5. 在**新規則**視窗，設定規則的一般設定：
   - 指定規則名稱。
     規則名稱不能包含多於 255 個字元並且不能包括任何特殊字元（例如 `"*<>?\:|` ）。
   - 使用**啟用規則**方塊啟用或停用規則。
     預設情況下已選取此**啟用規則**核取方塊。
   - 在**標籤**欄位中，輸入頁籤名稱。
     規則名稱不能包含多於 255 個字元並且不能包括任何特殊字元（ `"*<>?\:|` ）。
6. 在**條件**區域，點擊**新增**按鈕來新增條件，或點擊**內容**按鈕編輯現有條件。
   新自動標記規則條件精靈視窗開啟。
7. 在**標籤分配條件**視窗，選取影響標記的條件的核取方塊。您可以選取多個條件。

8. 依據您選取的標記條件，精靈將顯示設定對應條件的視窗。設定依據以下條件的規則觸發：

   - **裝置使用或與特定網路的關聯**—裝置網路內容，例如 Windows 網路中的裝置名稱，和裝置是否屬於網域或 IP 範圍。

     如果為您用於卡巴斯基安全管理中心的資料庫設定了區分大小寫的排序規則，請在指定裝置 DNS 名稱時保持大小寫。否則，自動標記規則將不起作用。

   - **使用 Active Directory**—裝置在 Active Directory 組織單元中的出現和裝置在 Active Directory 群組中的成員關係。

   - **特定應用程式**—網路代理在裝置上的出現，和作業系統類型、版本和架構。

   - **虛擬機**—裝置是否屬於指定類型的虛擬機。

   - **應用程式登錄資料中的應用程式已安裝**—裝置上不同供應商應用程式的出現。

9. 設定條件後，為其輸入名稱，然後關閉精靈。

   如果必要，您可以為一個規則設定多個條件。此種情況下，在滿足至少一個條件時，標籤將被分配到裝置。您新增的條件將顯示在規則內容視窗中。

10. 在**新規則**視窗點擊**確定**，並在管理伺服器內容視窗點擊**確定**。

所建立的規則被強加到被所選管理伺服器管理的裝置。如果裝置的設定滿足規則條件，標籤被分配到裝置。

檢視和設定分配到裝置的標籤

您可以檢視分配到裝置的所有標籤的清單，以及在裝置內容視窗中繼續設定自動標記規則。

要檢視和設定分配到裝置的標籤：

1. 在主控台樹狀目錄中，開啟**受管理裝置**資料夾。
2. 在**受管理裝置**資料夾的工作台，選取您要檢視所分配的標籤的裝置。
3. 在行動裝置的上下文功能表中，選取"**內容**"。
4. 在裝置內容視窗中，選取**標籤**區域。

   分配到所選裝置的標籤清單被顯示，以及標籤被分配的方式：手動或依據規則。

5. 如果必要，請執行以下操作之一：

   - 要繼續設定標記規則，點擊**設定自動標記規則**連結（僅對 Windows 可用）。
   - 要重新命名標籤，選取該標籤並點擊**重新命名**按鈕。
   - 要刪除標籤，選取該標籤並點擊**刪除**按鈕。
   - 要手動新增標籤，在**標籤**區域下方的欄位中輸入標籤，並點擊**新增**按鈕。

6. 點擊**套用**按鈕，如果您對**標籤**區域做了變更，以便變更生效。
7. 點擊"**確定**"。

如果您在裝置內容中刪除或重新命名一個標籤，該變更不影響到管理伺服器內容中定義的標記規則。變更將僅套用到修改了內容的裝置。

用戶端裝置的遠端診斷。卡巴斯基安全管理中心遠端診斷公用程式

卡巴斯基安全管理中心遠端診斷實用程式（以下稱為遠端診斷實用程式）可在用戶端裝置上執行下列操作：

- 啟用和關閉偵錯、變更偵錯等級、下載偵錯檔案。
- 下載系統資訊和應用程式設定。
- 下載事件記錄。
- 為應用程式建立記憶體傾印檔案。
- 開始進行診斷並下載診斷報告。
- 啟動和停止應用程式。

您可以使用從用戶端裝置下載的事件記錄和診斷報告以自行定位問題。同時，Kaspersky 技術支援專家可能讓您從用戶端裝置下載偵錯檔案、記憶體傾印檔案、事件記錄和診斷報告以便讓 Kaspersky 進一步分析。

遠端診斷實用程式將隨管理主控台一起自動安裝在裝置上。

使用遠端診斷公用程式連線至用戶端裝置

要使用遠端診斷公用程式連線至用戶端裝置，請執行以下操作：

1. 在主控台樹狀目錄中選取任意管理群組。
2. 在工作區的**裝置**頁籤中，從任何裝置的上下文功能表中選取**自訂工具 → 遠端診斷**。
   系統將開啟遠端診斷公用程式的主視窗。
3. 在遠端診斷公用程式主視窗的第一個欄位中指定您希望用來連線裝置的工具：
   - **使用 Microsoft Windows 網路存取**。
   - **使用管理伺服器存取**。

4. 如果您在公用程式主視窗的第一個欄位中選取**使用 Microsoft Windows 網路存取**，請執行以下操作：

- 在**裝置**欄位，指定您要連線的裝置位址
  您可以使用 IP 位址、NetBIOS 名稱或 DNS 名稱作為裝置位址。
  預設值是使用了公用程式的裝置的上下文功能表上顯示的位址。
- 指定連線到該裝置的帳戶：
  - **使用目前使用者連線**（預設選取）。以目前的使用者帳戶連線。
  - **使用提供的使用者名和密碼來連線**。以提供的使用者帳戶連線。需提供帳戶的"**使用者名稱**"和"**密碼**"。

  只有使用裝置的本機管理員帳戶才可連線到裝置。

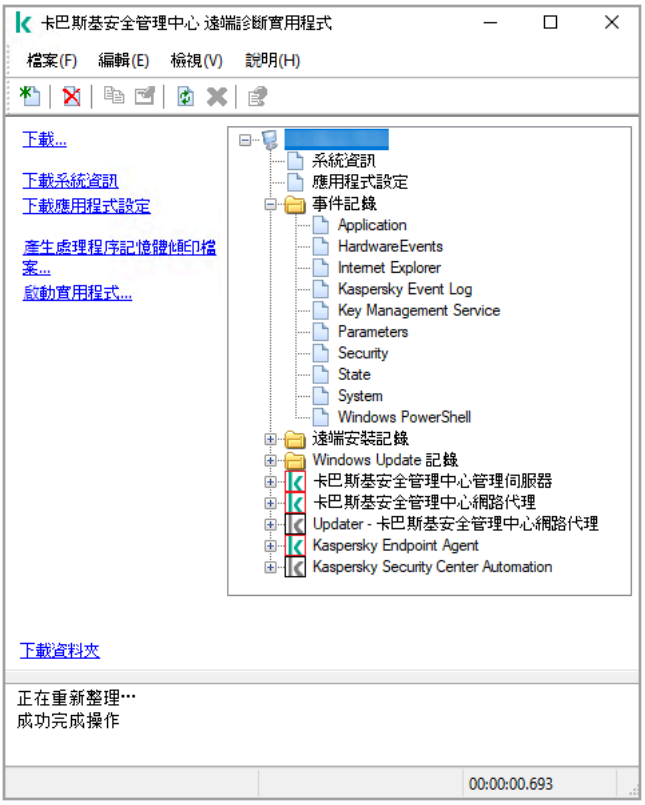
5. 如果您在公用程式主視窗的第一個欄位中選取**使用管理伺服器存取**，請執行以下操作：

- 在**管理伺服器**欄位中輸入您要連線裝置的管理伺服器位址。
  您可以使用 IP 位址、NetBIOS 名稱或 DNS 名稱作為伺服器位址。
  預設值為目前執行公用程式的管理伺服器位址。
- 如有必要，請選取**使用 SSL**、**壓縮資料流量**和**屬於從屬管理伺服器的裝置**核取方塊。
  如果選取了**屬於從屬管理伺服器的裝置**核取方塊，您可以在**屬於從屬管理伺服器的裝置**欄位中填寫從屬管理伺服器的名稱，並透過點擊**瀏覽**按鈕管理該裝置。

6. 若要連線裝置，請點擊**登入**按鈕。

如果您的帳戶啟用了兩步驟驗證，您必須使用兩步驟驗證授權。

這將開啟對裝置進行遠端診斷的視窗（請參閱下圖）。視窗左側包含裝置遠端診斷操作連結。視窗右側包含公用程式管理的裝置物件樹狀目錄。視窗底部顯示公用程式執行狀態。



遠端診斷公用程式。遠端裝置診斷視窗

遠端診斷公用程式把從裝置上下載的檔案儲存在執行此程式的裝置桌面上。

為應用程式建立記憶體傾印檔案

應用程式傾印檔案允許您檢視某個時間點在用戶端裝置上執行的應用程式的參數。該檔案還包含有關為應用程式加載的模組的資訊。

不支援獲取來自 Linux 裝置的傾印。

若要透過遠端診斷獲取傾印，請使用 kldumper 公用程式。該公用程式旨在應技術支援專家的要求獲取卡巴斯基應用程式處理程序的傾印。卡巴斯基安全管理中心知識庫中提供了有關使用 kldumper 公用程式的要求的詳細資訊。

要為應用程式建立傾印檔案：

1. 在**受管理裝置**資料夾的工作區中，在**裝置**頁簽上，開啟所需裝置的右鍵功能表，然後選擇**自訂工具→遠端診斷**。

   卡巴斯基安全管理中心遠端診斷實用程式視窗開啟。

2. 將遠端診斷公用程式連線至用戶端裝置。

   這將開啟對裝置進行遠端診斷的視窗。

3. 在視窗的左側，按一下**"產生處理程序記憶體傾印檔案**連結。

4. 在開啟的**正在產生處理程序記憶體傾印檔案**視窗中，指定要為其產生傾印檔案的應用程式的可執行檔。

5. 點擊**確定**按鈕。

包含指定應用程式的傾印檔案的存檔被下載。

如果指定的應用程式未在用戶端裝置上執行，則下載的存檔中包含的「結果」資料夾將為空。

如果指定的應用程式正在執行，但下載失敗並出現錯誤，或下載的存檔中包含的「結果」資料夾為空，請參閱卡巴斯基安全管理中心知識庫。

啟用和關閉偵錯，下載偵錯檔案

要在遠端裝置上啟用偵錯：

1. 執行遠端診斷實用程式並連線至必要裝置。

2. 在裝置的物件樹狀目錄中，選取您要啟用偵錯的應用程式。

只有當裝置與管理伺服器連線時，才能為具有自我防護功能的應用程式啟用和停用偵錯。

如果您想要啟用網路代理偵錯，您也可以透過建立安裝所需更新並修復弱點工作來實現。此種情況下，在網路代理偵錯已在遠端診斷實用程式中被停用時，網路代理依然會寫入偵錯資訊。

3. 要啟用偵錯：

   a. 在遠端診斷實用程式視窗左側，點擊**啟用偵錯**。

   b. 在開啟的**選取偵錯等級**視窗中，建議您保留設定的預設值。當需要時，技術支援專家將指導您設定過程。下列設定可用：

   - **偵錯等級**

     偵錯等級定義偵錯檔案包含的詳情資料量。

   - **基於循環的偵錯**（僅 Kaspersky Endpoint Security 可以使用）

     應用程式覆蓋偵錯資訊以防止偵錯檔案過量增長。指定用於儲存偵錯資訊的檔案最大數量，以及每個檔案的最大大小。如果寫入了最大數量的最大大小的偵錯檔案，最舊的檔案被刪除以便新偵錯檔案可以被寫入。

   c. 點擊**"確定"**。

4. 對於 Kaspersky Endpoint Security，技術支援專家可能需求您對系統效能資訊啟用 Xperf 偵錯。

   要啟用 Xperf 偵錯：

   a. 在遠端診斷實用程式視窗左側，點擊**啟用 Xperf 偵錯**。

   b. 在開啟的**選取偵錯等級**視窗中，根據技術支援專家的請求，選取以下偵錯等級之一：

   - **輕度等級**

     該類型的偵錯檔案包含系統最少量資訊。

     預設情況下已選定此選項。

   - **深度等級**

     相比於*輕度*類型的偵錯檔案，該類型的偵錯檔案包含更多詳細資訊，且可能在*輕度*類型偵錯檔案不足以評估效能時被技術支援專家需求。*深度*偵錯檔案包含關於系統的硬體、作業系統、應用程式的啟動和結束處理程序清單、用於效能評估的事件和來自 Windows System Assessment 工具的事件的技術資訊。

   c. 選取以下偵錯類型之一：

   - **基本類型**

     偵錯資訊在 Kaspersky Endpoint Security 應用程式執行期間被接收。

     預設情況下已選定此選項。

   - **重新啟動時類型**

     偵錯資訊在作業系統從受管理裝置上啟動時接收。該偵錯類型在影響系統效能的問題發生時，在裝置被開啟後和 Kaspersky Endpoint Security 啟動之前有效。

d. 系統可能要求您啟用**基於循環的偵錯**選項，以防止偵錯檔案的過量增長。然後指定偵錯檔案的最大大小。當檔案達到最大大小時，最舊的偵錯資訊被新資訊覆蓋。

e. 點擊**"確定"**。

某些情況下，要啟用偵錯，必須重新啟動安全應用程式及其工作。

遠端診斷工具對所選應用程式啟用偵錯。

要下載應用程式的偵錯檔案：

1. 執行遠端診斷工具並連線到必要的裝置，敘述在**"**連線遠端診斷工具到用戶端裝置**"**。
2. 在應用程式節點，在**偵錯檔案**資料夾選取所需檔案。
3. 在遠端診斷實用程式視窗左側，點擊**下載整個檔案**。

   如果檔案較大，可只下載偵錯檔案的部分。

   您可以刪除已存在的偵錯檔案。停用偵錯後，您可以刪除此檔案。

所選檔案被下載到視窗下方指定的位置。

要在遠端裝置上停用偵錯：

1. 執行遠端診斷工具並連線到必要的裝置，敘述在**"**連線遠端診斷工具到用戶端裝置**"**。
2. 在裝置的物件樹狀目錄中，選取您要停用偵錯的應用程式。

   只有當裝置與管理伺服器連線時，才能為具有自我防護功能的應用程式啟用和停用偵錯。

3. 在遠端診斷實用程式視窗左側，點擊**停用偵錯**。

遠端診斷工具對所選應用程式停用偵錯。

下載應用程式設定

要從遠端裝置下載應用程式設定：

1. 執行遠端診斷工具並連線到必要的裝置，敘述在"連線遠端診斷工具到用戶端裝置"。
2. 從遠端診斷實用程式視窗的物件樹狀目錄中，選取裝置名稱最上層節點。
3. 在遠端診斷實用程式視窗的左側，從以下選項中選取您需要的操作：
   - **下載系統資訊**
   - **下載應用程式設定**
   - **產生處理程序記憶體傾印檔案**
     點擊此連結後，於開啟的視窗中，指定要為其產生記憶體傾印檔案的應用程式的可執行檔。
   - **啟動實用程式**
     點擊此連結後，在開啟的視窗中，指定實用程式的可執行檔及其執行設定。

選取的共用程式將被下載，並啟動於裝置上。

下載事件記錄

要從遠端裝置下載事件記錄：

1. 執行遠端診斷工具並連線到必要的裝置，敘述在"連線遠端診斷工具到用戶端裝置"。
2. 在裝置物件樹狀目錄的**系統事件記錄**資料夾，選取相關記錄。
3. 透過點擊遠端診斷實用程式視窗左側的**下載事件記錄 <事件記錄名稱>** 連結下載所選記錄。

所選事件記錄被下載到視窗下方指定的位置。

下載多個診斷資訊項目

卡巴斯基安全管理中心遠端診斷實用程式允許您下載診斷資訊的多個項目，包括事件記錄、系統資訊、偵錯檔案和記憶體傾印檔案。

要從遠端裝置下載診斷資訊：

1. 執行遠端診斷工具並連線到必要的裝置，敘述在"連線遠端診斷工具到用戶端裝置"。
2. 在遠端診斷實用程式視窗左側，點擊**下載**。
3. 選取您要下載的項目旁邊的核取方塊。
4. 點擊**開始**。

每個所選項目被下載到視窗下方指定的位置。

進行診斷並下載診斷結果

要為某遠端裝置應用程式啟動診斷並下載其執行結果，請執行以下操作：

1. 執行遠端診斷工具並連線到必要的裝置，敘述在"連線遠端診斷工具到用戶端裝置"。
2. 在裝置的物件樹狀目錄中，選取必要的應用程式。
3. 然後透過點擊遠端診斷實用程式視窗左側的**執行診斷**連結來啟動診斷。
   而診斷報告將顯示在物件樹狀目錄中所選應用程式的節點中。
4. 在物件樹狀目錄中選取新產生的診斷報告，然後點擊**下載資料夾**連結以下載該報告。

所選報告被下載到視窗下方指定的位置。

啟動、停止和重新啟動應用程式

只有與管理伺服器連線的裝置後，您才能啟動、停止和重新啟動應用程式。

若要啟動、停止和重新啟動應用程式，請執行以下操作：

1. 執行遠端診斷工具並連線到必要的裝置，敘述在"連線遠端診斷工具到用戶端裝置"。
2. 在裝置的物件樹狀目錄中，選取必要的應用程式。
3. 在遠端診斷實用程式視窗的左側選取操作：
   - **停止應用程式**
   - **重新啟動應用程式**
   - **啟動應用程式**

依據您選取的操作，應用程式被啟動、停止或重新啟動。

UEFI 防護裝置

*UEFI 防護裝置*是包含在 BIOS 層級整合的適用於 UEFI 的卡巴斯基解決方案或應用程式的裝置。整合的防護從系統啟動時開始確保裝置安全，未整合軟體的裝置僅在安全應用程式啟動後開始防護工作。支援這些裝置的管理的卡巴斯基安全管理中心。

要修改 UEFI 防護裝置的連線設定：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。
2. 在管理伺服器的上下文功能表中，選取**內容**。
3. 在管理伺服器內容視窗，選取**伺服器連線設定 → 附加連接埠**。

4. 在**附加連接埠**區域，修改相關設定：

   - **開啟 UEFI 防護裝置和 KasperskyOS 裝置的連接埠**

     UEFI 防護裝置可以連線到管理伺服器。

   - **UEFI 防護裝置和 KasperskyOS 裝置的連接埠**

     若啟用**開啟 UEFI 防護裝置和 KasperskyOS 裝置的連接埠**選項則可變更埠號。預設埠號為 13294。

5. 點擊**確定**。

受管理裝置設定

要檢視受管理裝置設定：

1. 在主控台樹狀目錄中，選擇**受管理裝置**資料夾。
2. 在資料夾的工作區，選擇一個裝置。
3. 在裝置的上下文功能表中，選取**內容**。

   所選裝置的內容視窗隨即開啟並已選取**一般**區域。

一般

一般區域顯示有關用戶端裝置的一般資訊。資訊基於上一次用戶端裝置與管理伺服器之間的同步接收的資料來提供：

- **名稱**

  在該欄位中，您可以檢視和修改管理群組中的用戶端裝置名稱。

- **敘述**

  在該欄位中，您可以輸入用戶端裝置的附加敘述。

- **Windows 網域**

  包含裝置的 Windows 網域或工作群組。

- **NetBIOS 名稱**

  用戶端裝置的 Windows 網路名稱。

- **DNS 名稱**

  用戶端裝置的 DNS 網域名稱。

- **IP 位址**

  裝置 IP 位址。

- **群組**

  包括了用戶端裝置的管理群組。

- **上次更新**

  裝置上病毒資料庫或應用程式最後更新日期。

- **上一次可見**

  裝置上次在網路中可見的日期和時間。

- **連線至管理伺服器**

  裝置上的網路代理上一次連線到管理伺服器的日期和時間。

- **不斷開與管理伺服器的連線**

  如果啟用此選項，受管裝置和管理伺服器之間將保持持續連線。如果您使用的不是推送伺服器，您可能想要使用此選項，它提供了這樣的連線。

  如果停用此選項且不在使用推送伺服器，則受管理裝置將僅在同步資料或傳輸資訊時連線至管理伺服器。

  不斷開與管理伺服器的連線選項所能選取的最大裝置總數是 300。

  預設情況下，受管理裝置上停用此選項。預設情況下，此選項在安裝了管理伺服器的裝置上處於啟用狀態，即使您嘗試停用它也會保持啟用狀態。

防護

防護區域將通知您用戶端裝置上病毒防護的目前狀態：

- **裝置狀態**

  根據管理員針對裝置病毒防護狀態定義之條件，以及網路上裝置的活動所指派的用戶端裝置狀態。

- **所有問題**

  該表格包含了用戶端裝置上安裝的受管理應用程式偵測到的問題的完整清單。每個問題都伴有一個狀態，應用程式建議您分配該狀態到該問題的裝置。

- **即時防護**

  該欄位顯示目前的用戶端裝置即時防護狀態。

  當裝置狀態變更時，新狀態僅在用戶端裝置與管理伺服器同步之後顯示在裝置屬性視窗。

- **上一次自訂掃描**

  用戶端裝置上執行的最後一次惡意軟體掃描的日期和時間。

- **偵測到的威脅總數**

  自安裝安全應用程式（第一次掃描）或自上次重設威脅計數器以來，在用戶端裝置上偵測到的威脅總數。

- **活動威脅**

  用戶端裝置上的未處理檔案數量。

  該欄位行動裝置上的未處理檔案數量。

- **磁碟加密狀態**

  裝置本機磁碟機上的目前檔案加密狀態。有關狀態的說明，請參閱 Kaspersky Endpoint Security for Windows 說明。

應用程式

應用程式區域列出用戶端裝置上安裝的所有 Kaspersky 應用程式。此部分包含開始按鈕（  ）和停止按鈕（  ），允許您啟動和停止選定的卡巴斯基應用程式（不包括網路代理）。如果受管理裝置上的連接埠 15000 UDP可用於接收來自管理伺服器的推播通知，則啟用這些按鈕。如果受管理裝置無法用於推播通知，但啟用了與管理伺服器的連續連線模式（啟用了**一般**部分中的**不斷開與管理伺服器的連線**選項），則開始和停止按鈕也可用。**應用程式**部分還包含以下按鈕：

- **事件**

按一下該按鈕可檢視當應用程式執行時在用戶端裝置上發生的事件的清單，以及檢視該應用程式的工作結果。

- **統計**

  按一下該按鈕可檢視有關應用程式的目前統計資訊。

- **內容**

  按一下該按鈕可接收有關應用程式的資訊並設定應用程式。

工作

在**工作**標籤中，您可以管理用戶端工作：檢視現有工作清單、建立新工作、移除、啟動和停止工作、修改工作設定以及檢視執行結果。該工作清單會根據用戶端最近一次與管理伺服器同步的連線期間所收到的資料提供。管理伺服器向用戶端裝置請求工作狀態詳情。

如果受管理裝置上的連接埠 15000 UDP可用於接收來自管理伺服器的推播通知，則啟用開始()、停止 () 和移除 () 按鈕。如果受管理裝置無法用於推播通知，但啟用了與管理伺服器的連續連線模式（啟用了**不斷開與管理伺服器的連線**部分中的**一般**選項），則開始和停止按鈕也可用。

如果未建立連線，則不顯示工作狀態，按鈕被停用。

事件

事件標籤將顯示選定用戶端裝置在管理伺服器上所記錄事件的資訊。

標籤

在**標籤**分頁，您可以編輯用來尋找用戶端裝置的關鍵字清單，並可以檢視現有標籤清單、從清單中配置標籤、設定自動標記規則、新增標籤和重新命名舊標籤以及移除標籤。

系統資訊

一般系統資訊區域將顯示用戶端裝置上安裝的應用程式的相關資訊。

應用程式登錄資料

在**應用程式登錄資料**區域，您可以檢視用戶端裝置上安裝的應用程式及其更新的登錄檔，您還可以設定應用程式登錄資料的顯示方式。

如果用戶端裝置上安裝的網路代理將所需資訊傳送到管理伺服器，則將提供有關已安裝應用程式的資訊。您可以在網路代理或其政策的內容視窗中的**儲存區**區域，設定將資訊傳送到管理伺服器。

- **只顯示不相容的資訊安全應用程式**

  如果啟用此選項，則應用程式清單僅包含不與 Kaspersky 應用程式相容的安全應用程式。

  預設情況下已停用該選項。

- **顯示更新**

  如果啟用此選項，則應用程式清單不僅包含應用程式而且包含為其所安裝的更新套件。

  顯示更新清單需要 100 KB 的流量。如果您關閉清單然後重新開啟它，您將不得不再次花費 100 KB 的流量。

  預設情況下已停用該選項。

- **匯出至檔案**

  按一下該按鈕匯出安裝在裝置上的應用程式清單到 CSV 檔案或 TXT 檔案。

- **歷程記錄**

  按一下該按鈕檢視裝置上的應用程式安裝事件。以下資訊被顯示：

  - 應用程式被安裝到裝置的日期和時間
  - 應用程式名稱
  - 應用程式版本

- **內容**

  按一下該按鈕檢視在裝置上安裝的應用程式清單中選中的應用程式的內容。以下資訊被顯示：

  - 應用程式名稱
  - 應用程式版本
  - 應用程式供應商

可執行檔

可執行檔區域會顯示在用戶端裝置上發現的可執行檔。

硬體登錄資料

在**硬體登錄資料**區域，您可以檢視安裝在用戶端裝置上的硬體資訊。您可以針對 Windows 裝置和 Linux 裝置檢視此資訊。

確保在要從中獲取硬體詳細資訊的 Linux 裝置上安裝了 lshw 公用程式。根據所使用的 hypervisor，從虛擬機獲取的硬體詳細資訊可能不完整。

如果網路代理安裝在執行 Windows 的裝置上，它會向管理伺服器傳送有關裝置硬體的下列資訊：

- RAM
- 大容量儲存裝置
- 主機板
- 處理器
- 網路卡
- 監視器
- 顯示卡
- 音效卡

如果網路代理安裝在執行 Linux 或 macOS 的裝置上，它會向管理伺服器傳送有關裝置硬體的下列資訊（如果該資訊由作業系統提供）：

- RAM 總容量
- 大容量儲存裝置總容量
- 主機板
- 處理器
- 網路卡

連線

連線區域僅對 Windows 裝置顯示，包含有關用戶端裝置所有者以及在所選用戶端裝置上工作的使用者帳戶的資訊。

基於 Active Directory 資料產生網域使用者相關資訊。本機使用者詳情由安裝在用戶端裝置上的 Windows Security Account Manager 提供。

- **裝置所有者**

  裝置所有者欄位顯示當管理員需要在用戶端裝置上執行操作時，他可以聯絡的使用者名稱。

  分配和**內容**按鈕可以用來選取裝置所有者和檢視所有者使用者資訊。

  帶有紅叉的按鈕可以用來刪除目前裝置所有者。

清單顯示使用用戶端裝置的帳戶。

- **名稱**

  在 Windows 網路中的裝置名稱。

- **參與者的名稱**

  登入至該裝置的系統的使用者名稱（網域或本機名稱）。

- **帳戶**

  登入至該裝置的使用者帳戶。

- **電子郵件**

  使用者電子郵件信箱。

- **電話**

  使用者電話號碼。

事件

在**事件**頁簽中，您可為用戶端裝置檢視、編輯和建立事件。事件可以透過安裝在用戶端裝置上的受管理卡巴斯基應用程式自動建立，也可以由管理員手動建立。例如，如果使用者定期將惡意軟體從其卸除式磁碟機移至裝置，則管理員可以建立事件。管理員可以在事故文字中提供情況的簡要說明和建議的操作（例如對於一個使用者的紀律性操作），還可以新增連結到使用者。

對其採用了所有必要操作的事件稱為*已處理*事件。存在的未處理事件可被選為將裝置的狀態變更為*緊急*或*警告*的條件。

此部分包含已為裝置建立的事故的清單。事故按照幾個等級和類型分類。事故類型由建立事故的 Kaspersky 應用程式定義。選中**已處理**列中的方塊即可突出顯示清單上的已處理事件。

軟體弱點

軟體弱點區域會顯示安裝在用戶端裝置上的協力廠商應用程式的弱點資訊。您可以使用清單上方的搜尋欄位透過名稱尋找弱點。

- **匯出至檔案**

  按一下**匯出至檔案**按鈕儲存弱點清單到檔案。預設，應用程式匯出弱點清單到 CSV 檔案。

- **僅顯示可以被修復的弱點**

  如果啟用此選項，該區域會顯示可透過使用修補程式修復的弱點。

  如果停用此選項，該區域會同時顯示可透過使用修補程式修復的弱點，以及未發佈修補程式的弱點。

  預設情況下已啟用該選項。

- **內容**

  選取清單中的軟體弱點並點擊**內容**按鈕，以在個別視窗中檢視所選軟體弱點的內容。在視窗中，您可以進行以下操作：

  - 在這部受管理的裝置忽略軟體弱點（在管理主控台或在卡巴斯基安全管理中心網頁主控台）。
  - 檢視對弱點的建議修復清單。
  - 手動指定軟體更新以修復弱點（在管理主控台或在卡巴斯基安全管理中心網頁主控台）。
  - 檢視弱點實例。
  - 檢視要修復弱點的現有工作清單，並建立新工作來修復弱點。

可用更新

該區域顯示在該裝置上發現的未安裝的軟體更新清單。有關可選 Microsoft Windows 更新的資訊未被傳送至管理伺服器。

- **顯示已安裝的更新**

  如果啟用此選項，清單會顯示在用戶端裝置上已安裝和未安裝的更新。

  預設情況下已停用該選項。

作用中的政策

此區域顯示目前目前分派給此裝置的 Kaspersky 應用程式政策清單。

- **匯出至檔案**

  您可以按一下**匯出至檔案**按鈕可將活動政策設定檔清單儲存到檔案。預設下，應用程式匯出政策清單到 CSV 檔案。

啟用政策設定檔

- **啟用政策設定檔**

  該清單允許您檢視用戶端裝置上啟用的現有政策設定檔資訊。您可以使用清單上的搜尋欄透過輸入政策名稱或政策設定檔名稱來搜尋活動政策設定檔。

- **匯出至檔案**

  您可以按一下「**匯出至檔案**」按鈕可將活動政策設定檔清單儲存到檔案。預設情況下，應用程式匯出政策設定檔清單到 CSV 檔案。

發佈點

該區域提供裝置與之互動的發佈點清單。

- **匯出至檔案**

  按一下**匯出至檔案**按鈕儲存裝置與之互動的發佈點清單檔案。預設下，應用程式匯出裝置清單到 CSV 檔案。

- **內容**

  按一下**屬性**按鈕檢視和配置裝置與之互動的發佈點。

一般政策設定

一般

在**一般**區域，您可以修改政策狀態並指定政策設定的繼承：

- 在**政策狀態**區塊中，您可以選取一種政策模式：
  - **啟用政策**

    如果選取該選項，政策將變為啟用狀態。
    預設情況下已選定此選項。

  - **漫遊政策**

    如果選取該選項，政策將在裝置離開企業網路時變為啟用狀態。

  - **停用政策**

    如果選取該選項，政策將變為不啟用狀態，但它仍然儲存在**政策**資料夾中。如果需要，您可以啟動該政策。

- 在**設定繼承**設定群組中，您可以配置政策繼承：
  - **從父政策繼承設定**

    如果啟用此選項，則政策設定值將繼承上一級群組政策，因而會受到鎖定。
    預設情況下已啟用該選項。

  - **在子政策中強制繼承設定**

    如果啟用此選項，則在套用政策變更之後，程式將執行以下操作：
    - 政策設定的值將被傳送到管理子群組的政策，也就是子政策。
    - 在每個子政策內容視窗的**一般**區域的**設定繼承**區塊，系統將自動選取**從父政策繼承設定**核取方塊。

    如果啟用此方塊，則會鎖定子政策設定。
    預設情況下已停用該選項。

事件配置

事件配置區域可讓您配置事件記錄和事件通知。事件根據嚴重等級用下面的標籤分佈：

- **緊急**

  緊急頁籤不會顯示在網路代理政策內容中。

- **功能失效**
- **警告**
- **資訊**

在每個標籤，清單顯示在管理伺服器上事件類型和預設事件儲存的期限（天）。點擊**內容** 按鈕，您可以指定清單中已選中的事件記錄和通知設定。預設下，為整個管理伺服器指定的通用通知設定被用於所有事件類型。然後，您可以變更所需事件類型的特別設定。

例如，在**警告**頁簽上，您可以配置**發生了事件**事件類型。例如，當發佈點的可用磁碟空間小於 2 GB（遠端安裝應用程式和下載更新至少需要 4 GB）時，此類事件可能發生。要配置**發生了事件**事件，請選擇它並點擊**內容**按鈕。之後，您可以指定將發生的事件儲存在何處以及如何通知它們。

如果網路代理偵測到事件，您可以使用受管理裝置設定。

要選取多個事件種類，使用 **Shift** 或 **Ctrl** 鍵；要選取所有類型，使用**選擇所有**按鈕。

網路代理政策設定

若設定網路代理政策：

1. 在主控台樹狀目錄中，選取**政策**資料夾。
2. 在資料夾的工作區中，選取網路代理政策。
3. 在政策的上下文功能表中，選取**內容**。

   網路代理政策的內容視窗開啟。

請參閱以下比較表，它詳情描述了如何根據使用的作業係統類型套用設定。

一般

在**一般**區域，您可以修改政策狀態並指定政策設定的繼承：

- 在**政策狀態**區塊中，您可以選取一種政策模式：
  - **啟用政策**

    如果選取該選項，政策將變為啟用狀態。
    預設情況下已選定此選項。

  - **漫遊政策**

    如果選取該選項，政策將在裝置離開企業網路時變為啟用狀態。

  - **停用政策**

    如果選取該選項，政策將變為不啟用狀態，但它仍然儲存在**政策**資料夾中。如果需要，您可以啟動該政策。

- 在**設定繼承**設定群組中，您可以配置政策繼承：
  - **從父政策繼承設定**

    如果啟用此選項，則政策設定值將繼承上一級群組政策，因而會受到鎖定。
    預設情況下已啟用該選項。

  - **在子政策中強制繼承設定**

    如果啟用此選項，則在套用政策變更之後，程式將執行以下操作：
    - 政策設定的值將被傳送到管理子群組的政策，也就是子政策。
    - 在每個子政策內容視窗的**一般**區域的**設定繼承**區塊，系統將自動選取**從父政策繼承設定**核取方塊。

    如果啟用此方塊，則會鎖定子政策設定。
    預設情況下已停用該選項。

事件配置

事件配置區域可讓您配置事件記錄和事件通知。事件根據嚴重等級用下面的標籤分佈：

- **緊急**
  緊急頁籤不會顯示在網路代理政策內容中。
- **功能失效**

- **警告**
- **資訊**

在每個標籤，清單顯示在管理伺服器上事件類型和預設事件儲存的期限（天）。點擊**內容** 按鈕，您可以指定清單中已選中的事件記錄和通知設定。預設下，為整個管理伺服器指定的通用通知設定被用於所有事件類型。然後，您可以變更所需事件類型的特別設定。

例如，在**警告**頁簽上，您可以配置**發生了事件**事件類型。例如，當發佈點的可用磁碟空間小於 2 GB（遠端安裝應用程式和下載更新至少需要 4 GB）時，此類事件可能發生。要配置**發生了事件**事件，請選擇它並點擊**內容**按鈕。之後，您可以指定將發生的事件儲存在何處以及如何通知它們。

如果網路代理偵測到事件，您可以使用受管理裝置設定。

要選取多個事件種類，使用 **Shift** 或 **Ctrl** 鍵；要選取所有類型，使用**選擇所有**按鈕。

設定

在**設定**區域，您可以配置網路代理政策：

- **僅透過發佈點分發檔案**

  如果啟用此選項，受管理裝置上的網路代理僅從發佈點擷取更新。

  如果停用此選項，受管理裝置上的網路代理從發佈點或從管理伺服器擷取更新。

  請注意，受管理裝置上的安全應用程式從每個安全應用程式的更新工作中的來源集中擷取更新。如果您啟用**僅透過發佈點分發檔案**選項，請確保在更新工作中將卡巴斯基安全管理中心設定為更新來源。

  預設情況下已停用該選項。

- **事件佇列最大值(MB)**

  在該欄位中，您可以指定事件佇列可在磁碟機上佔據的最大空間。

  預設值為 2 MB。

- **應用程式被允許在裝置上獲取政策延伸資料**

  安裝在受管理裝置的網路代理會傳輸已套用安全應用程式政策的相關資訊至安全應用程式（例如 Kaspersky Endpoint Security for Windows）。您可在安全應用程式介面檢視已傳輸的資訊。

  網路代理會傳輸以下資訊：

  - 政策傳送至受管理裝置的時間。
  - 政策傳送至受管理裝置時啟用中政策的名稱。
  - 政策傳送至受管理裝置時漫遊政策的名稱（對於 Linux 版網路代理不可用）。
  - 政策傳送至受管理裝置時，受管理裝置包含的管理群組名稱與連結路徑。
  - 政策傳送至受管理裝置時包含名稱和優先順序的活動政策設定檔的清單。

  您也可使用資訊確保套用正確政策至裝置和用於疑難排解。預設情況下已停用該選項。

- **防護網路代理服務免遭非授權的移除或終止，並防止設定變更**

  如果啟用該選項，則網路代理被安裝到受管理裝置之後，沒有所需權限元件無法被移除或重新設定。網路代理服務無法被停止。此選項對網域控制器沒有影響。

  啟用此選項可防護以本機管理員權限操作的工作站上的網路代理。

  預設情況下已停用該選項。

- **使用解除安裝密碼**

  如果選取該方塊，則按一下**修改**按鈕可以指定 klmover 公用程式和網路代理遠端移除的密碼。

  預設情況下已停用該選項。

儲存區

在**儲存區**區域，您可以選取將其資訊從網路代理傳送到管理伺服器的物件類型：

- **Windows Update 更新詳情**

  如果啟用此選項，會將用戶端裝置上應該安裝的 Microsoft Windows Update 更新資訊傳送至管理伺服器。

  有時候，即使停用該選項，更新也會顯示在**可用更新**區域的裝置屬性中。例如，若組織的裝置具有可由這些更新修復的弱點，就可能會發生這個情況。

  預設情況下已啟用該選項。它僅適用於 Windows。

  有關可選 Microsoft Windows 更新的資訊未被傳送至管理伺服器。

- **軟體弱點和對應更新的詳情**

  若啟用此選項，協力廠商的弱點（包含 Microsoft 軟體）、受管理裝置上偵測到的資訊以及修復協力廠商弱點的軟體更新資訊（不含 Microsoft 軟體）都會傳送至管理伺服器。

  選取此選項（**軟體弱點和對應更新的詳情**）會增加網路負載、管理伺服器磁碟負載和網路代理的資源消耗。

  預設情況下已啟用該選項。它僅適用於 Windows。

  若要管理 Microsoft 軟體更新，請使用**Windows Update 更新詳情**選項。

- **硬體登錄資料詳細資訊**

  安裝在裝置上的網路代理會向管理伺服器傳送關於裝置硬體的資訊。您可以在裝置內容中檢視硬體詳細資訊。

  確保在要從中獲取硬體詳細資訊的 Linux 裝置上安裝了 lshw 公用程式。根據所使用的 hypervisor，從虛擬機獲取的硬體詳細資訊可能不完整。

- **已安裝應用程式詳情**

  如果啟用此選項，會將安裝在用戶端裝置上的應用程式資訊傳送至管理伺服器。

  預設情況下已啟用該選項。

- **包括修補程式資訊**

  安裝在用戶端裝置的應用程式修補程式的資訊會傳送至管理伺服器。啟用此選項可能增加管理伺服器和 DBMS 的負載，並造成資料庫的流量增加。

  預設情況下已啟用該選項。它僅適用於 Windows。

如果網路代理政策禁止本區域中某些設定，則您無法修改這些設定。

軟體更新和弱點

在**軟體更新和弱點**區域，您可以設定搜尋和發佈 Windows 更新，以及啟用掃描可執行檔以發現弱點：

- **使用管理伺服器作為 WSUS 伺服器**

  如果啟用此選項，Windows 更新下載到管理伺服器。管理伺服器提供以集線模式透過網路代理下載更新到用戶端裝置的 Windows 更新服務。

  如果停用此選項，則不使用管理伺服器下載 Windows 更新。此種情況下，用戶端裝置自己接收 Windows 更新。

  預設情況下已停用該選項。

- 在**允許使用者管理 Windows Update 更新的安裝**下，您可以限制使用者可以使用 Windows Update 在他們的裝置上手動安裝的 Windows 更新。

  在執行 Windows 10 的裝置上，如果 Windows Update 已為裝置找到更新，您在**允許使用者管理 Windows Update 更新安裝**下選取的新選項將僅在發現的更新被安裝後才被套用。

  在下拉清單中選取項目：

  - **允許使用者安裝所有可套用 Windows Update 更新**

    使用者可以安裝所有可套用到他們裝置的 Microsoft Windows Update 更新。

    如果您不希望干預更新安裝，請選取該選項。

    當使用者手動安裝 Microsoft Windows Update 更新時，更新可能從 Microsoft 伺服器下載，而不是從管理伺服器。如果管理伺服器還未下載這些更新，這是可能的。從 Microsoft 伺服器下載更新導致額外流量。

  - **僅允許使用者安裝批准的 Windows Update 更新**

    使用者可以安裝所有可應用到他們裝置的和您批准的 Microsoft Windows Update 更新。

    例如，您可能想先在測試環境中檢查更新安裝以確保它們不干預裝置操作，僅在這之後允許安裝這些批准的更新到用戶端裝置。

    當使用者手動安裝 Microsoft Windows Update 更新時，更新可能從 Microsoft 伺服器下載，而不是從管理伺服器。如果管理伺服器還未下載這些更新，這是可能的。從 Microsoft 伺服器下載更新導致額外流量。

  - **不允許使用者安裝 Windows Update 更新**

使用者無法在他們的裝置上手動安裝 Microsoft Windows Update 更新。所有可套用更新根據您的設定而安裝。

如果您想要集中管理更新的安裝則選則此選項。

例如，您可以想最佳化更新排程以便網路不超載。您可以計畫稍後更新，以便它們不干預使用者工作。

- 在**Windows Update 搜尋模式**設定群組中，您可以選取更新搜尋模式：
  - **主動**

    如果選中該選項，管理伺服器支援使用網路代理在用戶端裝置上從 Windows 更新代理傳送請求至更新來源：Windows 更新伺服器（或簡稱為 WSUS）。然後，網路代理會將從 Windows 更新代理接收到的資訊傳送給管理伺服器。

    只有選取*弱點掃描和所需更新*工作的**連線更新伺服器更新資料**選項時，此選項才會發揮效力。

    預設情況下已選定此選項。

  - **被動**

    如果您選定該選項，網路代理將從上次同步更新來源之後定期從 Windows 更新代理將所擷取更新的資訊傳遞給管理伺服器。如果 Windows 更新代理沒有執行與更新來源同步，在管理伺服器上的更新資訊就不再是最新的。

    若要從更新來源的記憶體快取獲得更新，請選取此選項。

  - **已停用**

    如果選中該選項，管理伺服器不會請求任何有關更新的資訊。

    若您要在本機裝置先測試更新，請選取此選項。

- **當執行可執行檔時掃描其弱點**

  如果啟用此選項，系統將在執行可執行檔時掃描弱點。

  預設情況下已啟用該選項。

重新啟動管理

如果您的作業系統必須在您使用、安裝或移除安裝應用程式時重新啟動受管理裝置，請在**重新啟動管理**區域指定執行的操作：

- **不要重新啟動作業系統**

  作業系統將不重新啟動。

- **如果必要，自動重新啟動作業系統**

  如果必要，作業系統自動重新啟動。

- **提示使用者操作**

  程式提示使用者重新啟動作業系統。

  預設情況下已選定此選項。

  - **重複提示間隔（分鐘）**

    如果啟用此選項，程式會以方塊旁邊的欄位指定的頻率提示使用者重新啟動作業系統。預設情況下，提示頻率為 5 分鐘。

    如果停用此選項，應用程式不會反復提示使用者重新啟動。

    預設情況下已啟用該選項。

  - **在指定時間後強制重新啟動（分鐘）**

    如果啟用此選項，提示使用者之後，程式強制作業系統在方塊旁邊欄位指定的時間間隔結束後進行重新啟動。

    如果停用此選項，程式不會強制重新啟動。

    預設情況下已啟用該選項。

  - **在此時間後強制關閉封鎖連線中的應用程式 (分鐘)**

    使用者裝置鎖定時，程式以強制模式關閉（指定不活動間隔之後自動鎖定，或手動鎖定）。

    如果啟用此選項，一旦輸入區域指定的時間間隔結束，鎖定裝置上的程式以強制模式關閉。

    如果停用此選項，鎖定裝置上的程式將不會關閉。

    預設情況下已停用該選項。

Windows 桌面共用

您可以透過**Windows 共用桌面**區域啟用並設定在使用共用桌面存取時使用者的遠端裝置上執行的管理員操作的稽核：

- **啟用稽核**

  如果啟用此選項，則會啟用遠端裝置上管理員的操作稽核。遠端裝置上的管理員操作是被一一記錄下來的：

  - 在遠端裝置的事件記錄中
  - 在位於遠端裝置上網路代理安裝資料夾中的副檔名為 syslog 的檔案中
  - 卡巴斯基安全管理中心的事件資料庫

  當符合以下條件時，管理員可使用操作稽核：

  - 弱點和修補程式管理授權使用中
  - 管理員有權啟動共用存取遠端裝置的桌面

  如果清除該選項，則會停用遠端裝置上的管理員操作稽核。

  預設情況下已停用該選項。

- **讀取時要監控的檔案遮罩**

  清單包含檔案遮罩。啟用稽核時，應用程式會監控管理員的讀取檔案是否與已讀取檔案的遮罩和從屬資訊相符。若已選取**啟用稽核**核取方塊，則可使用該清單。您可編輯檔案遮罩並新增一個至清單。各個新檔案遮罩應在新行的清單中指定。

  預設，指定了以下檔案遮罩:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **修改時要監控的檔案遮罩**

  該清單包含遠端裝置上的檔案遮罩。啟用稽核時，應用程式會監控管理員在符合遮罩的檔案中所作的變更，並儲存這些修改的資訊。若已選取**啟用稽核**核取方塊，則可使用該清單。您可編輯檔案遮罩並新增一個至清單。各個新檔案遮罩應在新行的清單中指定。

  預設，指定了以下檔案遮罩:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

管理修補程式和更新

在**管理修補程式和更新**區域，您可以設定更新的下載和發佈以及修補程式在受管理裝置上的安裝：

- **對未定義狀態的元件自動安裝可套用更新和修補程式**

  如果啟用此選項，帶有*未定義*批准狀態的 Kaspersky 應用程式在從更新伺服器下載後將被自動安裝在受管理裝置。

  如果停用此選項，被下載和標注為*未定義*狀態的 Kaspersky 修補程式將僅在您改變其狀態為*已批准*是被安裝。

  預設情況下已啟用該選項。

- **提前從管理伺服器下載更新和病毒資料庫（建議）**

  如果啟用此選項，離線模式更新下載被使用。當管理伺服器接收更新時，它通知網路代理（安裝網路代理的裝置）將用於受管理應用程式的更新。當網路代理接收更新的資訊後，它提前從管理伺服器下載相關檔案。在第一次連線網路代理時，管理伺服器發起更新下載。網路代理下載所有更新到用戶端裝置後，更新對該裝置上的應用程式可用。

  當用戶端裝置上的受管理應用程式嘗試存取網路代理以更新時，該網路代理檢查其是否具有所有所需的更新。如果在受管理應用程式請求更新之前 25 小時內，更新已從管理伺服器收到，則網路代理不連線到管理伺服器，而是從本機快取提供更新給受管理應用程式。當網路代理提供更新到用戶端裝置上的應用程式時，可能不會建立到管理伺服器的連線，但是更新不需要連線。

  如果停用此選項，離線模式更新下載不被使用。更新依據更新下載工作的排程被發佈。

  預設情況下已啟用該選項。

連線

連線區域包含三個嵌套子區域：

- **網路**
- **連線設定檔**（僅限 Windows 和macOS）
- **連線排程**

在**網路**子區域，您可以設定到管理伺服器的連線、啟用 UDP 連接埠，和指定埠號。提供以下功能：

- 在**到管理伺服器的連線**設定群組中，您可以設定到管理伺服器的連線，並指定同步用戶端裝置和管理伺服器的時間間隔：
  - **壓縮網路流量**

    如果啟用此選項，則透過減少所傳輸的流量進而減少管理伺服器的負載來提高網路代理的資料傳輸速度。

    用戶端裝置上的 CPU 負載可能會增加。

    預設情況下會啟用此核取方塊。

  - **在 Microsoft Windows 防火牆中開啟網路代理連接埠**

    如果啟用此選項，網路代理工作所需的連接埠將新增到 Microsoft Windows 防火牆排除清單中。
    預設情況下已啟用該選項。

  - **使用 SSL**

    如果啟用此選項，則使用 SSL 通訊協定透過安全連接埠連線管理伺服器。
    預設情況下已啟用該選項。

  - **以預設連線設定在發佈點（如果可用）上使用連線閘道**

    如果啟用此選項，發佈點上的連線閘道在管理群組屬性指定的設定下使用。
    預設情況下已啟用該選項。

- **使用 UDP 連接埠**

  如果需要網路代理透過 UDP 連接埠連線到管理伺服器，啟用**使用 UDP 連接埠**選項，並指定 **UDP 連接埠號**。預設情況下已啟用該選項。連線到管理伺服器的預設 UDP 連接埠是 15000。

- **UDP 連接埠號**

  在該欄位中，您可以輸入 UDP 連接埠號。預設埠號為 15000。
  使用十進位系統記錄。
  如果用戶端裝置執行在 Windows XP Service Pack 2 系統下，則整合的防火牆會封鎖 UDP 連接埠 15000。請手動開啟此連接埠。

- **使用發佈點強制連線到管理伺服器**

  如果您選取了**將此發佈點用作推送伺服器**發佈點設定視窗中的選項。否則，發佈點將不會作為推送伺服器。

在**連線設定檔**區域中，您可以指定網路位置設定，為管理伺服器配置連線設定檔，和在管理伺服器不可用時啟用漫遊模式。

- **網路位置設定**

  網路位置設定定義用戶端裝置所連線的網路內容，並指定當網路內容改變時，網路代理從一個管理伺服器連線設定檔轉換到另一個的規則。

- **管理伺服器連線設定檔**

  在該區域中，您可以檢視和設定網路代理至管理伺服器的連線。在該區域，您也可以建立當以下事件發生時，轉換網路代理到不同管理伺服器的規則：

  - 當用戶端裝置連線到另一個本機網路時
  - 當裝置與組織的本機網路遺失連線時
  - 當連線閘道的位址變更或 DNS 伺服器位址修改時

  連線設定檔僅支援執行 Windows 和 macOS 的裝置。

- **當管理伺服器不可用時啟用漫遊模式**

  如果啟用此選項，則在透過該設定檔連線的情況下，用戶端裝置上安裝的應用程式將使用漫遊模式裝置的政策設定檔，以及漫遊政策。如果沒有為應用程式定義漫遊政策，則使用啟動政策。

  如果停用此選項，則應用程式將使用已啟動的政策。

  預設情況下已停用該選項。

在**連線排程**子區域中，可以指定網路代理傳送資料到管理伺服器的時間間隔：

- **必要時連線**

  如果選中此選項，當網路代理需要傳送資料到管理伺服器時連線才被建立。

  預設情況下已選定此選項。

- **在指定時間間隔連線**

  如果選中此選項，網路代理在指定時間連線到管理伺服器。您可以新增若干個連線時間段。

發佈點

發佈點區域包含四個嵌套子區域：

- **網路輪詢**
- **網際網路連線設定**

- **KSN 代理**
- **更新**

在**網路輪詢**子區域，您可以設定網路自動輪詢。您可以啟用三種類型的輪詢，即網路輪詢、IP 範圍輪詢和 Active Directory 輪詢：

- **啟用網路輪詢**

  如果啟用此選項，則管理伺服器將按照您按一下**設定快速輪詢排程**和**設定完整輪詢排程**連結所配置的排程自動輪詢網路。

  如果停用此選項，管理伺服器將以**網路輪詢頻率（分鐘）**欄位中指定的時間間隔輪詢網路。

  對於 10.2 之前的版本，網路代理的裝置發現間隔可在**Windows 網域的輪詢頻率（分鐘）**（對於快速 Windows 網路輪詢）和**網路輪詢頻率（分鐘）**（對於完整 Windows 網路輪詢）欄位中設定。

  預設情況下已停用該選項。

- **啟用 IP 範圍輪詢**

  如果啟用此選項，則發佈點將按照您按一下**設定輪詢排程**按鈕所配置的排程自動輪詢 IP 範圍。

  如果停用此選項，則發佈點將不輪詢 IP 範圍。

  在 10.2 版之前的網路代理中，可在**輪詢間隔（分鐘）**欄位中配置 IP 範圍的輪詢頻率。若啟用該選項，可使用區域。

  預設情況下已停用該選項。

- **使用 Zeroconf 輪詢（僅限 Linux 平台；將略過手動指定的 IP 範圍）**

  如果啟用此選項，發佈點將使用零配置網路（也稱為 *Zeroconf*）用 IPv6 裝置自動輪詢網路。在這種情況下，啟用的 IP 範圍輪詢將被忽略，因為發佈點會輪詢整個網路。

  要開始使用 Zeroconf，必須滿足以下條件：

  - 發佈點必須執行 Linux。
  - 您必須在發佈點上安裝 avahi-browse 公用程式。

  如果停用此選項，則發佈點不會使用 IPv6 裝置輪詢網路。

  預設情況下已停用該選項。

- **啟用 Active Directory 輪詢**

  如果啟用此選項，則發佈點將按照您按一下**設定輪詢排程**連結所配置的排程自動輪詢 Active Directory。

  如果停用此選項，則管理伺服器將不輪詢 Active Directory。

  在 10.2 版之前的網路代理中，可在 **輪詢間隔（分鐘）** 欄位中設定 Active Directory 的輪詢頻率。如果啟用此選項，則該欄位可用。

  預設情況下已停用該選項。

如果您的發佈點在連線到網際網路時使用代理伺服器，則可以在**網際網路連線設定**子部分中指定以下設定：

- **使用代理伺服器**

  如果選取該方塊，您可以在輸入欄位中配置代理伺服器連線。
  預設情況下已清空此方塊。

- **代理伺服器位址**

  代理伺服器位址。

- **連接埠號**

  用於連線的埠號。

- **略過本機位址的代理伺服器**

  如果啟用此選項，則不使用代理伺服器連線本機網路的裝置。
  預設情況下已停用該選項。

- **代理伺服器身分驗證**

  如果選取該方塊，您可以在輸入欄位中為代理伺服器身分驗證指定憑證。
  預設情況下已清空此方塊。

- **使用者名稱**

  建立連線代理伺服器的使用者帳戶。

- **密碼**

  工作執行時使用的帳戶的密碼。

在 **KSN 代理**子區域，您可以設定應用程式使用發佈點，以從受管理裝置轉發 KSN 請求：

- **在發佈點端啟用 KSN 代理**

  KSN 代理服務執行在用作發佈點的裝置上。使用該功能重新分發和最佳化網路流量。

  發佈點傳送列在卡巴斯基安全網路聲明中的統計資訊到 Kaspersky。依預設，KSN 聲明位於 %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula。

  預設情況下已停用該選項。啟用該選項僅在**使用管理伺服器作為代理伺服器**和**我同意使用卡巴斯基安全網路**選項在管理伺服器內容視窗中被啟用時起作用。

  您可以指派活動被動叢集節點到發佈點並在該節點上啟用 KSN 代理伺服器。

- **轉發 KSN 請求到管理伺服器**

  發佈點從受管理裝置轉發 KSN 請求到管理伺服器。

  預設情況下已啟用該選項。

- **透過網際網路直接存取 KSN 雲端 / 私有 KSN**

  發佈點從受管理裝置轉發 KSN 請求到 KSN 雲端或私有 KSN。在發佈點上自行產生的 KSN 要求頁會直接傳送至 KSN 雲端或私有 KSN。

  已安裝網路代理版本 11（或更早版本）的發佈點無法直接存取私有 KSN。若要重新設定發佈點傳送 KSN 要求至私有 KSN，請為各發佈點啟用 **轉發 KSN 請求到管理伺服器**選項。

  已安裝網路代理版本 12（或更新版本）的發佈點可直接存取私有 KSN。

- **TCP 連接埠**

  受管理裝置將用於連線到 KSN 代理伺服器的 TCP 埠號。預設埠號為 13111。

- **使用 UDP 連接埠**

  如果需要網路代理透過 UDP 連接埠連線到管理伺服器，啟用**使用 UDP 連接埠**選項，並指定 **UDP 連接埠號**。預設情況下已啟用該選項。連線到管理伺服器的預設 UDP 連接埠是 15000。

在**更新**子區段，您可以透過啟用或停用**下載差異檔案**選項指定網路代理是否應該下載差異檔案。（預設啟用該選項。）

變更歷程

在**變更歷程**頁籤，您可以檢視網路代理政策修訂歷程。您可以比較修訂、檢視修訂以及執行進階操作，例如儲存修訂到檔案、回溯到修訂和新增/編輯修訂敘述。

管理使用者帳戶

該區域包含程式支援的使用者帳戶及角色資訊。本章節包含有關如何建立卡巴斯基安全管理中心使用者帳戶和角色的說明。

卡巴斯基安全管理中心允許您管理使用者帳戶以及帳戶群組。該程式支援三種帳戶類型：

- 組織員工的帳戶。在輪詢組織的網域控制器時管理伺服器擷取資料的網域使用者帳戶。
- 本機使用者帳戶。受管理裝置上的本機帳戶，以及安裝了管理伺服器的裝置上的本機帳戶。
- 卡巴斯基安全管理中心內部使用者的帳戶。您可以建立內部使用者的帳戶。這些帳戶僅在卡巴斯基安全管理中心內使用。

使用使用者帳戶

卡巴斯基安全管理中心允許您管理使用者帳戶以及帳戶群組。該程式支援兩種帳戶類型：

- 組織員工的帳戶。在輪詢組織網路時管理伺服器擷取資料的使用者帳戶。
- 內部使用者帳戶。當使用虛擬管理伺服器時，這些帳戶被套用。只能在卡巴斯基安全管理中心內建立和使用內部使用者帳戶。

您可以透過以下方式之一檢視使用者帳戶清單：

- 在主控台樹狀圖中，前往**進階→使用者帳戶**。
- 在主控台樹狀圖中，前往**受管理裝置→裝置** 頁簽 → <裝置名稱>連結 →**連線** 部分。

  連線部分應顯示在執行 Windows 的裝置上具有活動工作階段的使用者帳戶。

如果滿足以下要求，則使用者帳戶清單可以正確顯示：

- 使用與管理伺服器版本相同或更高版本的網路代理。
- 已啟用Active Directory 輪詢以顯示網域使用者的帳戶。
- 在執行 Windows 的受管理裝置上，**伺服器(LanmanServer)** 服務正在執行。

您可以對使用者帳戶及帳戶群組執行以下操作：

- 透過使用角色配置存取應用程式特性的使用者權限。
- 透過使用郵件和 SMS 傳送資訊給使用者。
- 檢視使用者行動裝置清單。
- 交付並安裝使用者行動裝置上的憑證。
- 檢視發佈給使用者的憑證清單。
- 停用使用者帳戶的兩步驟驗證。

新增內部使用者帳戶

要新增新內部使用者帳戶到卡巴斯基安全管理中心：

1. 在主控台樹狀目錄中，選取**使用者帳戶**資料夾。
   使用者帳戶資料夾預設是**進階**資料夾的子資料夾。
2. 在工作區，點擊**新增使用者**按鈕。

3. 在開啟的**新使用者**視窗，指定新使用者帳戶設定：

- 使用者名稱()

  > 編輯使用者名稱時要小心。儲存變更後，您將不能變更它。

- **敘述**
- **完整名稱**
- **主電子郵件**
- **主電話**
- 連線到卡巴斯基安全管理中心的使用者**密碼**
  密碼必須符合以下規則：
  - 密碼必須是 8 到 16 位字元長度。
  - 密碼必須包含以下組中三組的字元：
    - 大寫字母 (A-Z)
    - 小寫字母 (a-z)
    - 數字 (0-9)
    - 特殊字元 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
  - 密碼不可以包含任何空白、Unicode 字元或 "." 和「@」的組合，並且「@」前不可有「.」。

  要檢視輸入的密碼，點擊並按住**顯示**按鈕。

  > 輸入密碼的嘗試次數有限。預設下，允許的最大密碼輸入嘗試次數是 10。您可以管理允許的密碼輸入嘗試次數，敘述在"變更允許的密碼輸入嘗試次數"。

  > 如果使用者輸入無效的密碼指定次數，使用者被鎖定一小時。在使用者帳戶清單，被封鎖帳戶的使用者圖示（  ）被灰掉（不可用）。您僅可以透過變更密碼解鎖封鎖使用者。

- 如果必要，選取**停用帳戶**核取方塊以禁止使用者連線到應用程式。您可以停用帳戶，例如，如果您要事先建立帳戶但是稍後啟動它。
- 如果要啟用其他選項以保護使用者帳戶免受未授權修改，請選取**修改帳戶設定時要求輸入密碼**核取方塊。如果啟用此選項，則修改使用者帳戶設定需要使用**一般功能：使用者權限**功能區域中的修改物件 ACL 權限來授權使用者。

4. 點擊**確定**。

新建立的使用者帳戶在**使用者帳戶**資料夾的工作區中顯示。

編輯內部使用者帳戶

要在卡巴斯基安全管理中心中編輯內部使用者帳戶：

1. 在主控台樹狀目錄中，選取**使用者帳戶**資料夾。

   使用者帳戶資料夾預設是**進階**資料夾的子資料夾。

2. 在工作區，點擊您要編輯的內部使用者帳戶。

3. 在開啟的**內容：<使用者名稱>**視窗，變更使用者帳戶設定：

- **敘述**
- **完整名稱**
- **主電子郵件**
- **主電話**
- 連線到卡巴斯基安全管理中心的使用者**密碼**
  密碼必須符合以下規則：
  - 密碼必須是 8 到 16 位字元長度。
  - 密碼必須包含以下組中三組的字元：
    - 大寫字母 (A-Z)
    - 小寫字母 (a-z)
    - 數字 (0-9)
    - 特殊字元 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
  - 密碼不可以包含任何空白、Unicode 字元或 "." 和「@」的組合，並且「@」前不可有「.」。

  要檢視輸入的密碼，點擊並按住**顯示**按鈕。

  > 輸入密碼的嘗試次數有限。預設下，允許的最大密碼輸入嘗試次數是 10。您可以管理允許的密碼輸入嘗試次數，敘述在"變更允許的密碼輸入嘗試次數"。

  > 如果使用者輸入無效的密碼指定次數，使用者被鎖定一小時。在使用者帳戶清單，被封鎖帳戶的使用者圖示（  ）被灰掉（不可用）。您僅可以透過變更密碼解鎖封鎖使用者。

- 如果必要，選取**停用帳戶**核取方塊以禁止使用者連線到應用程式。您可以停用帳戶，例如，在員工離職後。
- 如果要啟用其他選項以保護用戶帳戶免遭未經授權的修改，請選取「**修改帳戶設定時要求輸入密碼**」選項。如果啟用此選項，則修改使用者帳戶設定需要使用**一般功能：使用者權限**功能區域中的修改物件 ACL 權限來授權使用者。

4. 點擊**確定**。

編輯的使用者帳戶在**使用者帳戶**資料夾的工作區中顯示。

變更允許的密碼輸入嘗試次數

卡巴斯基安全管理中心使用者可以輸入無效的密碼有限次數。達到限制後，使用者帳戶被鎖定一小時。

依預設，可輸入密碼的嘗試次數上限為 10 次。您可以變更允許的密碼輸入嘗試次數，敘述在該部分。

要變更允許的密碼輸入嘗試次數：

1. 開啟安裝了管理伺服器的裝置的登錄檔（例如，在**開始 → 執行**功能表使用 regedit 指令）。
2. 轉至以下鍵：
   - 對於 32 位元系統：
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
   - 對於 64 位元系統：
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF
3. 如果 SrvSplPpcLogonAttempts 值不存在，建立它。數值型別是 DWORD。
   預設下，卡巴斯基安全管理中心被安裝後，該值未被建立。
4. 在 SrvSplPpcLogonAttempts 值中指定所需的嘗試次數。
5. 按一下**確定**儲存變更。
6. 重新啟動管理伺服器服務。

允許的最大密碼輸入嘗試次數被變更。

設定內部使用者名稱的唯一性檢查

您可以配置對卡巴斯基安全管理中心內部使用者的唯一性檢查。內部使用者名稱唯一性檢查僅可以在要建立該使用者的虛擬管理伺服器或主管理伺服器上執行，或者在所有虛擬管理伺服器和主管理伺服器上執行。預設下，內部使用者名稱唯一性在所有虛擬管理伺服器和主管理伺服器上檢查。

若要在虛擬管理伺服器或主管理伺服器上啟用內部使用者名稱唯一性檢查：

1. 開啟安裝了管理伺服器的裝置的登錄檔（例如，在**開始 → 執行**功能表使用 regedit 指令）。
2. 轉至以下分支：
   - 對於 32 位元系統：
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - 對於 64 位元系統：
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. 對於 LP_InterUserUniqVsScope（DWORD）鍵，設定 00000001 值。
   該鍵指定的預設值是 0。
4. 重新啟動管理伺服器服務。

名稱唯一性檢查在建立內部使用者的虛擬管理伺服器上執行，或者在建立內部使用者的主管理伺服器上執行。

要在所有虛擬管理伺服器和主管理伺服器上啟用內部使用者名稱唯一性檢查：

1. 開啟安裝了管理伺服器的裝置的登錄檔（例如，在**開始 → 執行**功能表使用 regedit 指令）。
2. 轉至以下分支：
   - 對於 64 位元系統：
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
   - 對於 32 位元系統：
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
3. 對於 LP_InterUserUniqVsScope（DWORD）鍵，設定 00000000 值。
   該鍵指定的預設值是 0。
4. 重新啟動管理伺服器服務。

內部使用者名稱唯一性檢查將在所有虛擬管理伺服器和主管理伺服器上執行。

新增安全群組

您可以新增安全群組（使用者群組），執行群組和安全群組對程式不同功能存取權限的複雜設定。可為安全群組分配與其各自的目的對應的名稱。例如，名字可以對應於使用者所在辦公室地點或者使用者所屬公司的組織機構單元名稱。

一個使用者可以屬於多個安全群組。一個虛擬管理伺服器管理的使用者帳戶可以僅屬於該虛擬伺服器的安全群組並僅具有該虛擬伺服器的存取權限。

要新增安全群組：

1. 在主控台樹狀目錄中，選取**使用者帳戶**資料夾。
   使用者帳戶資料夾預設是**進階**資料夾的子資料夾。
2. 點擊**新增安全群組**按鈕。
   新增安全群組視窗開啟。
3. 在**新增安全群組**視窗的**一般**區域，指定群組名稱。
   規則名稱不能包含多於 255 個字元並且不能包括任何特殊字元，例如 *, <, >, ?, \, :, |。群組名稱必須唯一。
   您可以在**敘述**輸入欄位中輸入群組敘述。您可選擇填寫**敘述**欄位。
4. 點擊**確定**。

您新增的安全群組會顯示在主控台樹狀目錄的**使用者帳戶**資料夾。您可以新增使用者到新建立的群組。

新增使用者到群組

要新增使用者到群組：

1. 在主控台樹狀目錄中，選取**使用者帳戶**資料夾。
   使用者帳戶資料夾預設是**進階**資料夾的子資料夾。
2. 在使用者帳戶和群組清單，選取您要新增使用者的群組。
3. 在管理伺服器內容視窗中，選取**群組使用者**區域並點擊**新增**按鈕。
   帶有使用者清單的視窗開啟。
4. 在清單中，選取您要包含在群組中的使用者。
5. 點擊**"確定"**。

使用者被新增到群組並顯示在使用者群組清單中。

設定應用程式功能的存取權限。角色型存取控制

卡巴斯基安全管理中心提供了適用於角色型存取的功能，可存取卡巴斯基安全管理中心和受管理 Kaspersky 應用程式的功能。

您可以透過以下其中一種方式為卡巴斯基安全管理中心使用者配置對應用程式功能的存取權限：

- 透過為每個使用者或使用者群組單獨設定權限。
- 透過使用一群組預先定義的權限建立標準使用者角色並根據使用者的職責範圍將這些角色分配給使用者。

使用者角色（也稱為角色）是對卡巴斯基安全管理中心或受管理 Kaspersky 應用程式功能的預定義存取權限集。您可將角色指派給一個使用者或使用者群組。

使用者角色的應用旨在簡化和縮短配置使用者對應應用程式功能存取權限的常規過程。角色內的存取權限根據標準工作和使用者的職責範圍設定。

可為使用者角色分配與其各自的目的對應的名稱。您可在程式中建立無限數量的角色。

您可以將預定義的使用者角色與已配置的一組權限一起使用，或者建立新角色並自己配置所需的權限。

存取管理伺服器及其物件的權限

在安裝卡巴斯基安全管理中心期間，程式將自動建立 **KLAdmins** 和 **KLOperators** 群組。這些群組被授予連線至管理伺服器和處理管理伺服器物件的權限。

依據安裝卡巴斯基安全管理中心時使用的帳戶類型，系統會建立如下所示的 **KLAdmins** 和 **KLOperators** 群組：

- 如果應用程式是在網域內包含的使用者帳戶下安裝的，則系統會在包含管理伺服器的網域內和管理伺服器上同時建立這些群組。
- 如果應用程式是在系統帳戶下安裝的，則系統僅會在管理伺服器上建立這些群組。

您可以使用作業系統的標準管理工具檢視 **KLAdmins** 和 **KLOperators** 群組，並且可以修改屬於 **KLAdmins** 和 **KLOperators** 群組使用者的存取權限。

KLAdmins 群組被授予擁有所有存取權限，**KLOperators** 群組僅被授予"讀取"和"執行"的權限。授予 **KLAdmins** 群組的權限被鎖定。

屬於 **KLAdmins** 群組的使用者稱為 *卡巴斯基安全管理中心管理員*；**KLOperators** 群組的使用者稱為 *卡巴斯基安全管理中心操作員*。

除 **KLAdmins** 群組包含的使用者外，系統還會將卡巴斯基安全管理中心管理員權限授予安裝裝置的本機管理員。

> 您可以將本機管理員從擁有卡巴斯基安全管理中心管理員權限的使用者清單中排除。

所有由卡巴斯基安全管理中心管理員執行的操作都將使用管理伺服器帳戶的權限執行。

可透過網路為每個管理伺服器建立單獨的 **KLAdmins** 群組；該群組將僅具有該掛歷伺服器所必須的權利。

如果歸屬相同網域的裝置被分派在不同管理伺服器的管理群組中，則網域管理員是所有群組的卡巴斯基安全管理中心管理員。對於這些管理群組而言，**KLAdmins** 群組是相同的；該群組是在安裝第一台管理伺服器期間建立的。啟動卡巴斯基安全管理中心管理員的帳戶權限管理伺服器時管理群組設定將會一同啟用。

安裝應用程式之後，卡巴斯基安全管理中心的管理員可以：

- 修改授予 **KLOperators** 群組的權限。
- 將存取卡巴斯基安全管理中心功能的權限授予其他安全群組及管理主控台中所建立的使用者。
- 為每個管理群組中分配使用者存取權限。

卡巴斯基安全管理中心管理員可以在選定物件的內容視窗中的"**安全性**"區域中將存取權限分配給每個管理群組或管理伺服器的其他物件。

您可以使用管理伺服器中的事件記錄追蹤使用者活動。事件記錄會顯示在**事件**頁籤的**管理伺服器**節點。這些事件具有重要等級**資訊事件**；事件類型以**稽核**開頭。

應用程式功能的存取權

下表顯示卡巴斯基安全管理中心功能，這些功能具有管理相關工作、報告、設定和執行相關使用者操作的存取權限。

要執行表中列出的使用者操作，使用者必須具有操作旁邊指定的權限。

讀取、**寫入**和**執行**權限適用於任何工作、報告或設定。除了這些權限外，使用者還必須具有**為裝置分類執行操作**的權限，才能管理裝置分類上的工作、報告或設定。

表中缺少的所有工作、報告、設定和安裝套件均屬於**一般功能：基本功能**的功能區域。

應用程式功能的存取權

功能區域	權限	使用者操作：執行操作所需的權限	工作	報告	其他
一般功能：管理群組的管理	**寫入**	• 將裝置新增到管理群組：**寫入** • 從管理群組中刪除裝置：**寫入** • 將管理群組新增到另一個管理群組：**寫入** • 從另一個管理群組中刪除管理群組：**寫入**	沒有	沒有	沒有
一般功能：存取物件而不考慮它們的 ACLs	**讀取**	獲得對所有物件的讀取存取權限：**讀取**	沒有	沒有	沒有

功能區域	權限	使用者操作：執行操作所需的權限	工作	報告	其他
一般功能：基本功能	• **讀取** • **寫入** • **執行** • **為裝置分類執行操作**	• 虛擬伺服器的裝置移動規則（建立、修改或刪除）：**寫入**、**為裝置分類執行操作** • 取得行動 (LWNGT) 通訊協定自訂憑證：**讀取** • 設定行動 (LWNGT) 通訊協定自訂憑證：**寫入** • 獲取 NLA 定義的網路清單：**讀取** • 新增、修改或刪除 NLA 定義的網路清單：**寫入** • 檢視群組的存取控制清單：**讀取** • 檢視卡巴斯基事件日誌：**讀取** • 檢視用來還原對 BitLocker 加密的硬碟磁碟機的存取權限的還原金鑰：**執行**	• 「將更新下載至管理伺服器儲存區」 • 「提交報告」 • 「分發安裝套件」 • 「在從屬管理伺服器上遠端安裝應用程式」	• 「防護狀態報告」 • 「威脅報告」 • 「受感染最嚴重的裝置報告」 • 「病毒資料庫狀態報告」 • 「錯誤報告」 • 「網路攻擊報告」 • 「已安裝郵件系統保護應用程式的摘要報告」 • 「已安裝的外圍防禦應用程式的摘要報告」 • 「已安裝的應用程式類型概要報告」 • 「受感染的裝置使用者報告」 • 「事件報告」 • 「事件報告」 • 「發佈點活動報告」 • 「從屬管理伺服器的報告」 • 「裝置控制事件報告」 • 「弱點報告」 • 「禁止的應用程式報告」 • 「Web 控制報告」 • 「受管理裝置加密狀態報告」 • 「大容量儲存裝置加密狀態報告」 • 「檔案加密錯誤報告」 • 「封鎖存取加密檔案的報告」 • 「加密磁碟機存取權限報告」 • 「有效使用者權限報告」 • 「權限報告」	沒有
一般功能：已刪除物件	• **讀取** • **寫入**	• 檢視資源回收桶中已刪除的物件：**讀取** • 從資源回收桶中刪除物件：**寫入**	沒有	沒有	沒有
一般功能：事件處理	• **刪除事件** • **編輯事件通知設定** • **編輯事件記錄設定** • **寫入**	• 變更事件註冊設定：**編輯事件記錄設定** • 變更事件通知設定：**編輯事件通知設定** • 刪除事件：**刪除事件**	沒有	沒有	設定： • 病毒爆發設定：建立病毒爆發事件所需的病毒偵測次數 • 病毒爆發設定：評估病毒偵測的時段 • 儲存在資料庫中的最大事件數量 • 儲存已刪除裝置中的事件時段

功能區域	權限	使用者操作：執行操作所需的權限	工作	報告	其他
一般功能：在管理伺服器上操作	• **讀取** • **寫入** • **執行** • **修改物件 ACL** • **為裝置分類執行操作**	• 指定適用於網路代理連線之管理伺服器的管理連接埠：**寫入** • 指定在管理伺服器上啟動的啟動代理連接埠：**寫入** • 指定在管理伺服器上啟動的行動啟動代理連接埠：**寫入** • 指定用於發佈獨立套件之網頁伺服器的連接埠：**寫入** • 指定用於發佈 MDM 設定檔的網頁伺服器的連接埠：**寫入** • 指定管理伺服器的 SSL 連接埠以透過卡巴斯基網頁主控台進行連線：**寫入** • 指定用於行動連線之管理伺服器的管理連接埠：**寫入** • 指定儲存在管理伺服器資料庫的事件最大數量：**寫入** • 指定管理伺服器可以傳送的最大事件數：**寫入** • 指定管理伺服器可以傳送事件的時段：**寫入**	• 「備份管理伺服器資料」 • 「資料庫維護」	沒有	沒有
一般功能：Kaspersky 軟體佈署	• **管理 Kaspersky 修補程式** • **讀取** • **寫入** • **執行** • **為裝置分類執行操作**	核准或拒絕安裝修補程式：**管理 Kaspersky 修補程式**	沒有	• 「虛擬管理伺服器產品授權金鑰使用報告」 • 「Kaspersky 軟體版本報告」 • 「不相容的應用程式報告」 • 「Kaspersky 軟體模組更新版本報告」 • 「防護部署報告」	安裝套件：「Kaspersky」
一般功能：產品授權金鑰管理	• **匯出金鑰檔案** • **寫入**	• 匯出金鑰檔案：**匯出金鑰檔案** • 修改管理伺服器產品授權金鑰設定：**寫入**	沒有	沒有	沒有
一般功能：強制報告管理	• **讀取** • **寫入**	• 建立報告，而不考慮其 ACL：**寫入** • 不論報告的 ACL 為何都加以執行：**讀取**	沒有	沒有	沒有
一般功能：管理伺服器階層	**設定管理伺服器階層**	註冊、更新或刪除從屬管理伺服器：**設定管理伺服器階層**	沒有	沒有	沒有

功能區域	權限	使用者操作：執行操作所需的權限	工作	報告	其他
一般功能：使用者權限	**修改物件 ACL**	• 變更任何物件的「安全性」屬性：**修改物件 ACL** • 管理使用者角色：**修改物件 ACL** • 管理內部使用者：**修改物件 ACL** • 管理安全群組：**修改物件 ACL** • 管理別名：**修改物件 ACL**	沒有	沒有	沒有
一般功能：虛擬管理伺服器	• **管理虛擬管理伺服器** • **讀取** • **寫入** • **執行** • **為裝置分類執行操作**	• 取得理虛擬管理伺服器的清單：**讀取** • 取得虛擬管理伺服器的資訊：**讀取** • 建立、更新或刪除虛擬管理伺服器：**管理虛擬管理伺服器** • 將虛擬管理伺服器移動到另一個群組：**管理虛擬管理伺服器** • 設定管理虛擬伺服器權限：**管理虛擬管理伺服器**	沒有	「協力廠商軟體更新安裝結果報告」	沒有
一般功能：加密金鑰管理	• **讀取** • **寫入**	• 匯出加密金鑰：**讀取** • 匯入加密金鑰：**寫入**	沒有	沒有	沒有
行動裝置管理：一般	• **連線新裝置** • **僅傳送指令資訊至行動裝置** • **傳送指令至行動裝置** • **管理憑證** • **讀取** • **寫入**	• 取得金鑰管理服務還原資料：**讀取** • 刪除使用者憑證：**管理憑證** • 取得使用者憑證公開部分：**讀取** • 檢查是否啟用公共金鑰基礎架構：**讀取** • 檢查公共金鑰基礎架構帳戶：**讀取** • 取得公共金鑰基礎架構範本：**讀取** • 透過延伸金鑰使用憑證取得公共金鑰基礎架構範本：**讀取** • 檢查公共金鑰基礎架構憑證是否遭撤銷：**讀取** • 更新使用者憑證發行設定：**管理憑證** • 取得使用者憑證發行設定：**讀取** • 按應用程式名稱和版本取得套件：**讀取** • 設定或取消使用者憑證：**管理憑證** • 續訂使用者憑證：**管理憑證** • 設定使用者憑證標籤：**管理憑證** • 執行 MDM 安裝套件的產生；取消產生 MDM 安裝套件：**連線新裝置**	沒有	沒有	沒有

功能區域	權限	使用者操作：執行操作所需的權限	工作	報告	其他
系統管理：連線	• **啟動 RDP 連線** • **連線到現有 RDP 連線** • **建立通道** • **在管理員工作站上儲存裝置檔案** • **讀取** • **寫入** • **執行** • **為裝置分類執行操作**	• 建立桌面共用工作階段：**啟動 RDP 連線** • 建立 RDP 工作階段：**連線到現有 RDP 連線** • 建立通道：**建立通道** • 儲存內容網路清單：**在管理員工作站上儲存裝置檔案**	沒有	「裝置使用者報告」	沒有
系統管理：硬體清單	• **讀取** • **寫入** • **執行** • **為裝置分類執行操作**	• 取得或匯出硬體詳細目錄物件：**讀取** • 新增、設定或刪除硬體詳細目錄物件：**寫入**	沒有	• 「硬體登錄資料的報告」 • 「組態更改的報告」 • 「硬體報告」	沒有
系統管理：網路存取控制	• **讀取** • **寫入**	• 檢視 CISCO 設定：**讀取** • 更改 CISCO 設定：**寫入**	沒有	沒有	沒有
系統管理：作業系統佈署	• **佈署 PXE 伺服器** • **讀取** • **寫入** • **執行** • **為裝置分類執行操作**	• 部署 PXE 伺服器：**佈署 PXE 伺服器** • 檢視 PXE 伺服器清單：**讀取** • 在 PXE 用戶端上啟動或停止安裝程序：**執行** • 管理 WinPE 和作業系統映像的驅動程式：**寫入**	「在參考裝置作業系統映像上建立安裝套件」	沒有	安裝套件：「作業系統映像檔」
系統管理：弱點和修補程式管理	• **讀取** • **寫入** • **執行** • **為裝置分類執行操作**	• 檢視協力廠商修補程式屬性：**讀取** • 更改協力廠商修補程式屬性：**寫入**	• 「執行 Windows Update 同步」 • 「安裝 Windows Update 更新」 • 「修復弱點」 • 「安裝必要更新並修復弱點」	「軟體更新報告」	沒有

功能區域	權限	使用者操作：執行操作所需的權限	工作	報告	其他
系統管理：遠端安裝	• **讀取** • **寫入** • **執行** • **為裝置分類執行操作**	• 檢視協力廠商弱點和修補程式管理的安裝套件屬性：**讀取** • 更改協力廠商弱點和修補程式管理的安裝套件屬性：**寫入**	沒有	沒有	安裝套件： • 「自訂應用程式」 • 「VAPM 套件」
系統管理：軟體清單	• **讀取** • **寫入** • **執行** • **為裝置分類執行操作**	沒有	沒有	• 「已安裝應用程式的報告」 • 「應用程式登錄資料歷程報告」 • 「已授權應用程式群組狀態報告」 • 「協力廠商軟體產品授權金鑰報告」	沒有

預先定義的使用者角色

分配給卡巴斯基安全管理中心使用者的使用者角色為他們提供了對應用程式功能的存取權限集。

在虛擬伺服器上建立的使用者，在管理伺服器上無法被分配到角色。

您可以將預定義的使用者角色與已配置的一組權限一起使用，或者建立新角色。當建立新角色時，您必須自行設定角色範圍並指派對卡巴斯基安全管理中心功能的存取權限。卡巴斯基安全管理中心中可用的一些預定義使用者角色可以與特定的職位相關聯，例如，**稽核員**、**安全官**、**監督者**（從卡巴斯基安全管理中心版本 11 開始存在這些角色）。這些角色的存取權限會根據標準工作和相關職位的職責範圍預先配置。下表顯示角色可以如何與特定職位建立關聯。

特定職位的角色範例

角色	注釋
稽核員	允許使用本機管理員權限（Linux 為 root）對透過網路代理連線到管理伺服器的裝置分類執行所有檢視操作和任何建立的工作。 我們建議謹慎地將該角色指派給需要它們來履行正式職責的有限使用者。
管理者	允許所有檢視操作，不允許其他操作。您可以分配該角色到負責您組織的 IT 安全的安全官和其他管理員。
安全官	允許所有檢視操作，允許報告管理；在**系統管理**：**連線**區域授予有限的權限。您可以分配該角色到負責您組織的 IT 安全的安全官。

下表顯示指派給每個預先定義使用者角色的存取權限。

角色	敘述

管理伺服器管理員	允許在以下功能區域中進行所有操作：
	• **一般功能**：
	  • **基本功能**
	  • **事件處理**
	  • **管理伺服器階層**
	  • **虛擬管理伺服器**
	• **系統管理**：
	  • **連線**
	  • **硬體清單**
	  • **軟體清查**
	在**一般功能：加密金鑰管理**功能區域中授予**讀取**和**寫入**權限。

管理伺服器憑證運算子	授予以下所有功能區域的**讀取**和**執行**權限：
	• **一般功能**：
	  • **基本功能**
	  • **虛擬管理伺服器**
	• **系統管理**：
	  • **連線**
	  • **硬體清單**
	  • **軟體清查**

稽核員	允許功能區域中的所有操作，位於**一般功能**： • **存取物件而不考慮它們的 ACLs** • **刪除物件** • **強制報告管理** 您可以分配該角色到執行您組織的稽核的人。

安裝管理員	允許在以下功能區域中進行所有操作：
	• **一般功能**：
	  • **基本功能**
	  • **Kaspersky 軟體部署**
	  • **產品授權金鑰管理**
	• **系統管理**：
	  • **作業系統部署**
	  • **弱點和修補程式管理**
	  • **遠端安裝**
	  • **軟體清查**
	在**一般功能：虛擬管理伺服器**功能區域中，授予**讀取**和**執行**權限。

角色	敘述

安裝運算子	授予以下所有功能區域的**讀取**和**執行**權限：
	• **一般功能**：
	  • **基本功能**
	  • **Kaspersky 軟體佈署**（也會在此區域授予**管理 Kaspersky 修補程式**權限）
	  • **虛擬管理伺服器**
	• **系統管理**：
	  • **作業系統部署**
	  • **弱點和修補程式管理**
	  • **遠端安裝**
	  • **軟體清查**

Kaspersky Endpoint Security 管理員	允許在以下功能區域中進行所有操作： • **一般功能：基本功能** • Kaspersky Endpoint Security 區域，包括所有功能 在**一般功能：加密金鑰管理**功能區域中授予**讀取**和**寫入**權限。
Kaspersky Endpoint Security 運算子	授予以下所有功能區域的**讀取**和**執行**權限： • **一般功能：基本功能** • Kaspersky Endpoint Security 區域，包括所有功能
主要管理員	允許功能區域內的所有操作，以下區域*除外*，在**一般功能**： • **存取物件而不考慮它們的 ACLs** • **強制報告管理** 在**一般功能：加密金鑰管理**功能區域中授予**讀取**和**寫入**權限。

主要運算子	授予以下所有功能區域的**讀取**和**執行**（如適用）權限：
	• **一般功能**：
	  • **基本功能**
	  • **刪除物件**
	  • **管理伺服器上的操作**
	  • **Kaspersky 軟體佈署**
	  • **虛擬管理伺服器**
	• **行動裝置管理：一般**
	• **系統管理**，包括所有功能
	• Kaspersky Endpoint Security 區域，包括所有功能

行動裝置管理管理員	允許在以下功能區域中進行所有操作： • **一般功能：基本功能** • **行動裝置管理：一般**
行動裝置管理運算子	在**一般功能**：**基本功能**的功能區域中授予**讀取**和**執行**權限。 在**行動裝置管理**：**一般**功能區域中授予**讀取**和**僅向行動裝置傳送資訊命令**。

角色	敘述
安全官	允許在以下功能區域中進行所有操作，在**一般功能**： • **存取物件而不考慮它們的 ACLs** • **強制報告管理** 在**系統管理：連線**功能區域中，授予**讀取**、**寫入**、**執行**、**將來自裝置的檔案儲存到管理員的工作站**以及**對裝置分類執行操作**的權限。 您可以分配該角色到負責您組織的 IT 安全的安全官。
自助服務入口使用者	允許**行動裝置管理：自助服務入口**功能區域中的所有操作。此功能僅適用於卡巴斯基安全管理中心 11 或更新版本。
管理者	在**一般功能**：**存取物件而不考慮它們的 ACL** 與**一般功能**：**強制報告管理**功能區域中授予**讀取**權限。 您可以分配該角色到負責您組織的 IT 安全的安全官和其他管理員。
弱點和修補程式管理管理員	允許在**一般功能**：**基本功能**與**系統管理**（包括所有功能）功能區域中的所有操作。
弱點和修補程式管理操作者	授予在**一般功能**：**基本功能**和**系統管理**（包括所有功能）功能區域中的**讀取**和**執行**權限（如適用）。
作為服務管理員的網頁主控台	在**一般功能**：應用程式整合功能區**中授予閱讀 和**寫入權限。

新增使用者角色

新增使用者角色：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。
2. 在管理伺服器的上下文功能表中，選取**內容**。
3. 在管理伺服器內容視窗的**區域**視窗選取**使用者角色**並點擊**新增**按鈕。

   若啟用**顯示安全設定區域**選項，可使用**使用者角色**區域。

4. 在**新角色**內容視窗中，設定角色：
   - 在**區域**中，選取**一般**並指定角色名稱。
     角色名稱不能包括 100 個以上字元。
   - 選取**權限**區域，透過選取程式功能旁邊的**允許**和**拒絕**核取方塊來設定權限集。

   如果您在主管理伺服器上操作，則可以啟用「將**角色中繼到輔助管理伺服器**」選項。
5. 點擊**確定**。

角色已新增。

已為管理伺服器建立的使用者角色會顯示在伺服器內容視窗的**使用者角色**區域。您可以修改或刪除使用者角色，也可以指定角色給安全群組或選定的使用者。

為使用者或安全群組分配角色

將角色分配給使用者或使用者群組：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。
2. 在管理伺服器的上下文功能表中，選取**內容**。
3. 在"管理伺服器內容"視窗中，選取"**安全性**"區域。

   若在介面設定視窗中選取**顯示安全設定區域**核取方塊，則可使用**安全性**區域。

4. 在**群組或使用者的名稱**欄位，選取您要指派角色的一個使用者或一組使用者。

   如果使用者或使用者群組未包含在該欄位中，您可以點擊**新增**按鈕進行新增。

   當點擊**新增**按鈕新增使用者時，您可以選取使用者認證類型（Microsoft Windows 或卡巴斯基安全管理中心）。卡巴斯基安全管理中心認證用於選取處理虛擬管理伺服器的內部使用者帳戶。

5. 開啟**角色**標籤並點擊**新增**按鈕。

   "**使用者角色**"視窗將開啟。該視窗顯示已經建立的使用者角色。

6. 在**使用者角色**視窗，為安全群組選取一個角色。
7. 點擊"**確定**"。

擁有一群組處理管理伺服器權限的角色將被指派給使用者或安全群組。分配的角色會顯示在管理伺服器內容視窗中**安全**區域的**角色**頁籤。

分配權限到使用者和群組

您可以給予使用者和使用者群組權限以使用管理伺服器和您擁有外掛程式的 Kaspersky 程式（例如，Kaspersky Endpoint Security for Windows）的不同功能。

將權限分配給使用者或使用者群組：

1. 在主控台樹狀目錄中，做以下之一：
   - 延伸**管理伺服器**節點並選取所需管理伺服器的子資料夾。
   - 選取管理群組。
2. 在管理伺服器或管理群組的上下文功能表中，選取**內容**。
3. 在開啟的管理伺服器內容視窗（或管理群組內容視窗），在左側**區域**視窗選取**安全性**。

   若在介面設定視窗中選取**顯示安全設定區域**核取方塊，則可使用**安全性**區域。

4. 在**安全性**區域的**群組或使用者的名稱**清單選取使用者或群組。

5. 在工作區的下方的權限清單中的**權限**頁籤為使用者或群組設定權限集：

   a. 按一下加號 (+) 以延伸清單中的節點並獲取到權限的存取。

   b. 選取您想要的權限旁邊的**允許**和**拒絕**核取方塊。
      例子 1： 延伸**存取物件而不考慮它們的 ACLs** 節點或**已刪除物件**節點，並選取**讀取**。
      例子 2： 延伸**基本功能**節點，並選取**寫入**。

6. 當您已設定了權限集時，點擊**套用**。

使用者或使用者群組的權限集將被設定。

管理伺服器（或管理群組）的權限被分成以下部分：

- 一般功能：
  - 管理群組的管理
  - 存取物件而不考慮它們的 ACLs
  - 基本功能
  - 刪除物件
  - 事件處理
  - 管理伺服器操作（僅在管理伺服器的內容視窗）
  - 佈署 Kaspersky 應用程式
  - 產品授權金鑰管理
  - 強制報告管理
  - 伺服器層級
  - 使用者權限
  - 虛擬管理伺服器
- 行動裝置管理：
  - 一般
- 系統管理：
  - 連線
  - 硬體清單
  - 網路存取控制
  - 佈署作業系統
  - 管理弱點和修補程式
  - 遠端安裝
  - 軟體清查

如果對權限未選取**允許**或**拒絕**，權限被認為是*未定義*：它在對使用者明確拒絕或允許之前被拒絕。

使用者權限是以下的集合：

- 使用者自己的權限
- 指派給該使用者的所有角色的權限

- 使用者所屬的所有安全群組的權限
- 指派給使用者所屬安全群組的所有角色的權限

如果至少一個權限集對權限**拒絕**，那麼使用者被拒絕該權限，即便其他集允許它或保持未定義。

傳輸使用者角色到從屬管理伺服器

預設下，主要和從屬管理伺服器的使用者角色清單都是獨立的。您可以設定應用程式自動傳輸在主管理伺服器上建立的使用者角色到所有從屬管理伺服器。使用者角色也可以從從屬管理伺服器傳輸到其自己的從屬管理伺服器。

若要從主管理伺服器傳輸使用者角色到從屬管理伺服器，請執行以下操作：

1. 開啟主應用程式視窗。
2. 執行以下操作之一：
   - 在主控台樹狀目錄，右擊管理伺服器的名稱，並在上下文功能表中選取**內容**。
   - 如果您有活動管理伺服器政策，在**政策**資料夾的工作區，右擊該政策並在上下文功能表中選取**內容**。
3. 在管理伺服器內容視窗，或在政策設定視窗，在**區域**視窗選取**使用者角色**。

   若啟用**顯示安全設定區域**選項，可使用**使用者角色**區域。

4. 啟用**轉發角色清單到從屬管理伺服器**選項。
5. 點擊**"確定"**。

   應用程式從主管理伺服器複製使用者角色到從屬管理伺服器。

當**轉發角色清單到從屬管理伺服器**選項被啟用且使用者角色被傳輸時，它們不能在從屬管理伺服器上被編輯或刪除。當您建立新角色或在主管理伺服器上編輯現有角色時，變更被自動複製到從屬管理伺服器。當您在主管理伺服器上刪除使用者角色時，該角色在從屬管理伺服器上被保留，但無法被編輯或刪除。

從主管理伺服器傳播到從屬管理伺服器的角色用鎖頭圖示（🔒）顯示。您無法在從屬管理伺服器上編輯這些角色。

如果您在主管理伺服器上建立角色，且在從屬管理伺服器上有相同名稱的角色，新角色被複製到從屬管理伺服器，其名稱後被新增索引，例如，~~1、~~2（索引可以隨機）。

如果您停用**轉發角色清單到從屬管理伺服器**選項，所有使用者角色在從屬管理伺服器上被保留，但是獨立於主管理伺服器上的角色。變成獨立角色後，從屬管理伺服器上的使用者角色就可以被編輯或刪除。

指派使用者作為裝置所有者

您可以指定使用者作為裝置所有者來分配裝置到使用者。如果您必須在裝置上執行一些操作（例如，升級硬體），管理員可以通知裝置所有者來授權這些操作。

要指定使用者作為裝置所有者：

1. 在主控台樹狀目錄中，選擇**受管理裝置**資料夾。
2. 在資料夾的工作區，在**裝置**頁籤，選取您要指定擁有者的裝置。
3. 在裝置的上下文功能表中，選取**內容**。
4. 在裝置內容視窗中，選取**系統資訊 → 連線**。
5. 點擊**裝置所有者**欄位旁的**分配**按鈕。
6. 在**使用者分類**視窗，選取您要指定為裝置所有者的使用者並點擊**確定**。
7. 點擊**確定**。

裝置所有者被指定。依預設，**裝置所有者**欄位用來自 Active Directory 的值填充並在每次 Active Directory 輪詢時更新。您可以在**裝置所有者報告**中檢視裝置所有者。您可以使用新報告範本精靈建立報告。

將資訊傳送給使用者

透過電子郵件將訊息傳送給使用者：

1. 在主控台樹狀目錄的**使用者帳戶**資料夾中，選取使用者。

   使用者帳戶資料夾預設是**進階**資料夾的子資料夾。
2. 在使用者的上下文功能表中，選取**透過郵件通知**。
3. 在**將訊息傳送至使用者**視窗中填寫相關欄位並點擊**確定**按鈕。

   訊息將傳送至已在使用者內容中指定的電子郵件信箱。

將 SMS 訊息傳送給使用者：

1. 在主控台樹狀目錄的**使用者帳戶**資料夾中，選取使用者。
2. 在使用者的上下文功能表中，選擇**傳送簡訊**。
3. 在 **SMS 文字**視窗中填寫相關欄位並點擊**確定**按鈕。

   訊息將傳送至在使用者內容中指定號碼的行動裝置。

檢視使用者的行動裝置清單

檢視使用者行動裝置清單：

1. 在主控台樹狀目錄的**使用者帳戶**資料夾中，選取使用者。
   使用者帳戶資料夾預設是**進階**資料夾的子資料夾。
2. 在使用者帳戶的上下文功能表中，選取**內容**。
3. 在使用者帳戶的內容視窗中，選取**行動裝置**區域。

在**行動裝置**區域，您可以檢視使用者行動裝置清單及每個裝置的相關資訊。您可以點擊**"匯出至檔案"**按鈕可將行動裝置清單儲存到檔案。

為使用者安裝憑證

您可以為使用者安裝三種類型憑證：

- 共用憑證，用於識別使用者的行動裝置。
- 郵件憑證，用於設定使用者行動裝置上的企業信箱。
- VPN 憑證，用於設定使用者行動裝置上的虛擬私有網路。

將憑證發佈給使用者並安裝它：

1. 在主控台樹狀目錄中，開啟**使用者帳戶**資料夾，選取使用者帳戶。
   使用者帳戶資料夾預設是**進階**資料夾的子資料夾。
2. 在使用者帳戶的上下文功能表中，選取**安裝憑證**。

   啟動憑證安裝精靈。遵照精靈的說明。

在憑證安裝精靈結束後，憑證將被建立並為使用者安裝。您可以檢視已安裝使用者憑證清單並將其匯出到檔案。

檢視發佈給使用者的憑證清單

檢視所有發佈給使用者的憑證清單：

1. 在主控台樹狀目錄的**使用者帳戶**資料夾中，選取使用者。
   使用者帳戶資料夾預設是**進階**資料夾的子資料夾。
2. 在使用者帳戶的上下文功能表中，選取**內容**。
3. 在使用者帳戶的內容視窗中，選取**憑證**區段。

在**憑證**區域，您可以檢視使用者憑證清單及每個憑證的相關資訊。您可以點擊**匯出至檔案**按鈕可將憑證清單儲存到檔案。

關於虛擬管理伺服器的管理員

透過虛擬管理伺服器管理的企業網路的管理員以該視窗中指定的使用者帳戶啟動卡巴斯基安全管理中心 網頁主控台以檢視病毒防護詳情。

如果需要，可以在虛擬伺服器上建立多個管理員帳戶。

在虛擬伺服器上建立的使用者，在管理伺服器上無法被分配角色。

虛擬管理伺服器的管理員是卡巴斯基安全管理中心的一個內部使用者。內部使用者的資料不會傳送到作業系統上。卡巴斯基安全管理中心將驗證內部使用者。

遠端佈署作業系統和應用程式

卡巴斯基安全管理中心允許您建立作業系統映像，以及將其佈署在網路用戶端裝置上，也可以執行遠端安裝 Kaspersky 或其他供應商的應用程式。

要建立作業系統映像，請在管理伺服器上安裝 Windows ADK 的部署工具 和 Windows ADK 的 Windows PE 加載項 工具。您可以建立符合卡巴斯基安全管理中心的要求的任何版本的 Windows 作業系統的映像。

卡巴斯基安全管理中心不支援 64 位元版本的 Windows ADK 和 Windows PE。

擷取作業系統映像

卡巴斯基安全管理中心可以從裝置轉換可擷取的作業系統映像到管理伺服器。作業系統映像儲存在管理伺服器的一個專屬資料夾中。參考裝置的作業系統映像被捕獲並透過安裝套件建立工作建立。

作業系統映像擷取功能具有以下特點：

- 無法擷取管理伺服器所在裝置的作業系統映像。
- 擷取作業系統映像時，名為 sysprep.exe 的公用程式將重設參考裝置的設定。如果您要還原參考裝置的設定，在作業系統映像建立精靈中選取**建立裝置狀態備份副本**核取方塊。
- 擷取映像過程中會重新啟動裝置。

在新裝置上佈署作業系統映像

您可透過網路佈署映像，在沒有作業系統的裝置上安裝作業系統。在這種情況下將使用名為 Preboot eXecution Environment (PXE) 的技術。您可以選取一個網路上的裝置作為 PXE 伺服器。該裝置必須符合以下要求：

- 裝置必須安裝網路代理。
- 該裝置上無法啟動 DHCP 伺服器，因為 PXE 伺服器使用 DHCP 伺服器的連接埠。
- 包含裝置網段內沒有任何其他的 PXE 伺服器。

部署作業系統必須符合以下條件：

- 裝置必須安裝網卡。
- 裝置必須連線網路。
- 裝置開機時，必須在 BIOS 中選取網路開機選項。

系統將執行以下作業系統佈署操作：

1. 用戶端裝置在啟動過程中與 PXE 伺服器建立連線。
2. 用戶端裝置將在 Windows Preinstallation Environment (WinPE) 中啟動。

   將裝置新增到 WinPE 中可能需要為 WinPE 設定驅動程式。

3. 用戶端裝置將在管理伺服器上註冊。
4. 管理員將派發作業系統映像安裝套件，到用戶端裝置上。

   管理員可以新增所需磁碟機到帶有作業系統映像的安裝套件。管理員也可以指定帶有作業系統設定的設定檔以在安裝過程中套用。

5. 作業系統將佈署到用戶端裝置上。

管理員可以手動指定尚未連線的用戶端裝置 MAC 地址，並派送作業系統映像安裝套件。選定用戶端裝置連線至 PXE 伺服器時，會自動安裝作業系統到那些裝置上。

將作業系統映像佈署在已經安裝其他作業系統的裝置上

將作業系統映像佈署在已經安裝其他作業系統的裝置上的操作將由指定裝置的遠端安裝工作執行。

請注意，執行的是作業系統的全新安裝。所有資料將被刪除。

安裝 Kaspersky 和其他供應商的應用程式

管理員可以建立任何應用程式的安裝套件，包括指定使用者，並遠端安裝應用程式到用戶端裝置上。

建立作業系統映像

作業系統映像使用刪除參考裝置的作業系統映像工作來建立。

若要建立作業系統映像製作工作，請執行以下操作：

1. 在主控台樹狀目錄**遠端安裝**資料夾中，選取**安裝套件**子資料夾。
2. 點擊**建立安裝套件**按鈕以執行新套件精靈。
3. 在精靈的**選取安裝套件類型**視窗中點擊**使用作業系統映像建立安裝套件**按鈕。
4. 遵照精靈的說明。

   當精靈結束時，以**基於參考裝置作業系統映像建立安裝套件**為名稱的管理伺服器工作被建立。您可以在**工作**資料夾中檢視該工作。

當"**基於參考裝置作業系統映像建立安裝套件**"工作完成後，安裝套件建立完成，您可以使用該安裝套件透過 PXE 伺服器或遠端安裝工作在用戶端裝置上佈署作業系統。您可以在**安裝套件**資料夾中檢視安裝套件。

安裝作業系統映像

卡巴斯基安全管理中心允許您佈署桌面和基於伺服器的 Windows® 作業系統 WIM 映像到組織網路上的裝置。

以下方法可以被用於獲取可以用卡巴斯基安全管理中心工具佈署的作業系統映像：

- 從包含在 Windows 分發套件中的 install.wim 檔案匯入
- 從參考裝置擷取映像

支援作業系統映像佈署的兩個方案：

- 在"乾淨"（沒有安裝任何作業系統）裝置上佈署
- 在執行 Windows 的裝置上佈署

使用 Windows 預安裝環境 (Windows PE) 捕獲和部署作業系統映像。所有目的裝置正常執行所需的驅動程式都必須被新增 WinPE。一般情況下，必須新增網路介面卡和儲存控制器驅動程式。

以下需求必須被滿足以便實現映像佈署和擷取方案：

- Windows 自動安裝工具套件 (WAIK) 版本 2.0 或更高版本，或 Windows ADK 與 Windows ADK 的 Windows PE 附加元件必須安裝在管理伺服器上。如果方案允許在 Windows XP 上安裝或擷取映像，WAIK 必須被安裝。
- 目標裝置所在的網路中必須可使用 DHCP 伺服器。
- 管理伺服器的共用資料夾必須為目的裝置所在的網路以讀取方式開啟。如果共用資料夾位於管理伺服器，KlPxeUser 帳戶需要存取權限（該帳戶在執行管理伺服器安裝程式時被自動建立）。如果共用資料夾位於管理伺服器以外，必須授予每個人存取權限。

當選取要安裝的作業系統映像時，管理員必須明確指定目的裝置的 CPU 架構：x86 或 x86-64。

設定 KSN 代理伺服器位址

預設情況下，管理伺服器的連線名稱或 IP 位址與 KSN 代理伺服器位址相符。如果您改變了管理伺服器的連線名稱或 IP 位址，您必須指定正確的 KSN 代理伺服器位址，以防止主機裝置和 KSN 之間失去連線。

若要設定 KSN 代理伺服器位址：

1. 在主控台樹狀目錄中，前往**進階 → 遠端安裝 → 安裝套件**。
2. 在**安裝套件**的上下文功能表中，選擇**內容**。
3. 在開啟的視窗中，在**一般** 頁簽中指定新的 KSN 代理伺服器位址。
4. 點擊**套用**按鈕。

從現在起，指定的位址將作為 KSN 代理伺服器位址。我們建議您啟用**使用 KSN 代理**選項來最佳化網路流量。

新增 Windows Preinstallation Environment (WinPE) 的驅動程式

要新增 Windows Preinstallation Environment (WinPE) 的驅動程式：

1. 在主控台樹狀目錄**遠端安裝**資料夾中，選取 **佈署裝置映像**子資料夾。
2. 在**佈署裝置映像**資料夾的工作區中，點擊**附加操作**按鈕，然後在下拉式清單中選擇**設定 Windows 預安裝環境 (WinPE)的驅動程式集**。

   Windows 預安裝環境驅動程式視窗開啟。
3. 在**Windows 預安裝環境驅動程式**視窗，點擊**新增**按鈕。

   選取驅動程式 視窗將開啟。
4. 在**選取驅動程式**視窗，從清單選取驅動程式。

   如果必要驅動程式從清單遺失，點擊**新增**按鈕並在開啟的**新增驅動程式**視窗中指定驅動程式名稱和驅動分發套件資料夾。

   您可以點擊**瀏覽**按鈕來選取資料夾。

   在**新增驅動程式**視窗中，點擊**確定**。
5. 在**選取驅動程式**視窗中，點擊**確定**。

   驅動程式將被新增到管理伺服器的儲存區。新增到儲存區時，驅動程式會顯示在**選取驅動程式**視窗中。
6. 在**Windows 預安裝環境驅動程式**視窗中，點擊 **確定**。

驅動程式將被新增到 Windows Preinstallation Environment (WinPE)。

將驅動程式新增至作業系統安裝套件

若要將驅動程式新增至帶有作業系統映像安裝套件，請執行以下操作：

1. 在主控台樹狀目錄**遠端安裝**資料夾中，選取**安裝套件**子資料夾。
2. 從帶有作業系統映像的安裝套件的上下文功能表中選取**內容**。
   "安裝套件內容"視窗將開啟。
3. 在安裝套件內容視窗中選取**附加驅動程式**區域。
4. 點擊**附加驅動程式**區域中的**新增**按鈕。
   選取驅動程式 視窗將開啟。
5. 在**選取驅動程式**視窗中選取安裝驅動，建立作業系統安裝套件。
   您可透過在**選取驅動程式**視窗中點擊**新增**按鈕以新增驅動程式至管理伺服器儲存區。
6. 點擊**確定**。

已新增的驅動程式將顯示在作業系統映像安裝套件內容視窗的**附加驅動程式**區域中。

設定 sysprep.exe 公用程式

sysrep.exe 公用程式用於為裝置建立作業系統映像。

若要設定 sysprep.exe 公用程式，請執行以下操作：

1. 在主控台樹狀目錄**遠端安裝**資料夾中，選取**安裝套件**子資料夾。
2. 從帶有作業系統映像的安裝套件的上下文功能表中選取**內容**。
   "安裝套件內容"視窗將開啟。
3. 在安裝套件內容視窗中，選取**sysprep.exe 設定**區段。
4. 在**sysprep.exe 設定**區域，指定要在用戶端裝置佈署作業系統時使用的設定檔：
   - **使用預設的設定檔**。擷取操作系統映像時，選取此選項可以使用預設的設定檔。
   - **指定主要設定的自訂值**。在使用介面的設定項目可以指定自訂的設定值。
   - **指定設定檔**。選取此選項可以使用一個自訂的設定檔。
5. 若要套用變更，請點擊"**套用**"按鈕。

佈署作業系統至新聯網的裝置

若要在尚未安裝任何作業系統的新裝置上佈署作業系統，請執行以下操作：

1. 在主控台樹狀目錄**遠端安裝**資料夾中，選取 **佈署裝置映像**子資料夾。

   請確保**顯示弱點和修補程式管理**選項在**設定介面**視窗中啟用。否則，**遠端安裝**資料夾不會顯示。

2. 點擊**附加操作**按鈕，然後在下拉式清單中選擇**管理網路中 PXE 伺服器的清單**。

   內容：**佈署裝置映像**視窗隨即開啟並顯示在 **PXE 伺服器**區域中。

3. 在 **PXE 伺服器**區域，點擊**新增**按鈕，並在開啟的 **PXE 伺服器**視窗中選取作為 PXE 伺服器的裝置。

   您新增的裝置會顯示在 PXE 伺服器區域。建立的 WinPE 檔案將被從管理伺服器傳輸到裝置。檔案傳輸過程通常需要 10 分鐘。傳輸完成後，顯示的**狀態**值會從**正在啟動**變更為**就緒**。

4. 在**PXE 伺服器**區域中選取 PXE 伺服器，然後點擊**內容**按鈕。

5. 在選定的 PXE 伺服器內容中的**PXE 伺服器連線設定**頁籤，設定管理伺服器和 PXE 伺服器之間的連線。

6. 重新啟動您要佈署作業系統的用戶端裝置。

7. 在用戶端裝置的 BIOS 中選取網路啟動安裝選項。

   用戶端裝置將連線至 PXE 伺服器，然後顯示在**佈署裝置映像**資料夾的工作區中。

8. 在"**操作**"區域中，點擊**分配安裝套件**連結，選取一個安裝套件，作為要在指定裝置上安裝的作業系統。

   在所選裝置上使用 DiskPart 工具檢查可用瓷碟。在 Windows PE 命令提示符下，鍵入`diskpart`以開啟 DiskPart 工具。鍵入`list disk`以列出瓷碟。

   新增裝置並指定派送一個安裝套件，作業系統佈署便會自動在這台裝置上啟動。

9. 若要取消在用戶端裝置的作業系統佈署，請點擊**操作**區域的**取消安裝作業系統映像**連結。

若要在 MAC 位址新增裝置：

- 在**佈署裝置映像**資料夾，點擊**新增裝置 MAC 位址**開啟**新裝置**視窗，並指定您要新增的裝置的 MAC 位址。
- 在**佈署裝置映像**資料夾，點擊**從檔案匯入裝置 MAC 位址**以選取包含您要佈署作業系統映像的裝置的 MAC 位址清單的檔案。

佈署作業系統至用戶端裝置

若要在已經安裝了其他作業系統的用戶端裝置上佈署作業系統，請執行以下操作：

1. 在主控台樹狀目錄中開啟**遠端安裝**資料夾並點擊**在受管理裝置上佈署安裝套件（工作站）**連結以執行防護佈署精靈。

2. 在精靈的**選取安裝套件**視窗中指定帶有作業系統映像的安裝套件。

3. 遵照精靈的說明。

當精靈結束操作時，將建立遠端安裝工作以安裝作業系統到用戶端裝置。您可以在**工作**資料夾中啟動或停止工作。

建立應用程式安裝套件

要建立應用程式安裝套件：

1. 在主控台樹狀目錄**遠端安裝**資料夾中，選取**安裝套件**子資料夾。

2. 點擊**建立安裝套件**按鈕以執行新套件精靈。

3. 在精靈的**選取安裝套件類型**頁面上，選取以下其中一個按鈕：

- **為 Kaspersky 應用程式建立安裝套件**。如果您要建立 Kaspersky 的程式安裝套件，請選取此項目。
- **為指定的可執行檔建立安裝套件**。如果您要透過使用可執行檔為協力廠商應用程式建立安裝套件，請選擇該選項。通常，可執行檔是應用程式的安裝檔案。

  - **複製整個資料夾至安裝套件**

    如果可執行檔伴隨應用程式安裝所需的附加檔案，則選擇該選項。在您啟用該選項之前，確保所有所需檔案都儲存在相同資料夾。如果啟用該選項，應用程式新增資料夾的全部內容，包括指定的可執行檔，到安裝套件。

  - **指定安裝參數**

    對於成功的遠端安裝，多數應用程式要求安裝在靜默模式執行。如果是這種情況，您必須靜默安裝參數。

    配置安裝設定：

    - **可執行檔命令列**

      如果應用程式需要更多參數以進行靜默安裝，在該欄位指定它們。參考供應商文件以獲取詳情。

      您也可以輸入其他參數。

    - **對被卡巴斯基安全管理中心辨識的應用程式轉換設定到建議值**

      如果指定應用程式的資訊被包含在 Kaspersky 資料庫，應用程式將以建議設定安裝。

      如果您在**可執行檔命令列**欄位中資料了參數，它們被使用建議設定重寫。

      預設情況下已啟用該選項。

      Kaspersky 資料庫由 Kaspersky 分析家建立和維護。對於每個新增到資料庫的應用程式，Kaspersky 分析家定義最優的安裝設定。設定被定義以確保成功將應用程式遠端安裝到用戶端裝置。當您執行將更新下載至管理伺服器儲存區工作時，資料庫在管理伺服器上被自動更新。

- **從 Kaspersky 資料庫中選取一個應用程式來建立安裝套件**。如果您要從 Kaspersky 資料庫選取所需協力廠商應用程式以建立安裝套件，則選取此選項。當您將更新下載至管理伺服器儲存區工作時，資料庫被自動建立；應用程式被顯示在清單。
- **建立帶有作業系統映像的安裝套件**。如果必須建立帶有指定裝置作業系統映像的安裝套件，選取此項目。

  當精靈結束時，會建立以**基於參考裝置作業系統映像建立安裝套件**為名稱的管理伺服器工作。當從指定電腦複製作業系統映像工作完成後，您可以透過 PXE 伺服器或遠端安裝佈署作業系統至用戶端電腦上。

4. 遵照精靈的說明。

當精靈完成時，安裝套件被建立，您可以用其安裝應用程式到裝置。您可以透過選擇主控台樹狀目錄中的**安裝套件**來檢視安裝套件。

為應用程式安裝套件發佈憑證

要為應用程式安裝套件發佈憑證：

1. 在主控台樹狀目錄**遠端安裝**資料夾中，選取**安裝套件**子資料夾。
   遠端安裝資料夾預設是**進階**資料夾的子資料夾。
2. 從**安裝套件**資料夾的上下文功能表中，選取**所有工作** → 進階。
   這將開啟 **安裝套件**資料夾的內容視窗。
3. 在**安裝套件**資料夾的內容視窗中，選取**簽署獨立安裝套件**區域。
4. 在**簽署獨立安裝套件**區域，點擊**指定**按鈕。
   憑證視窗。
5. 在**憑證類型**欄位，指定公有或私有憑證類型：
   - 如果選取了 **PKCS#12 容器**值，指定憑證檔案和密碼。
   - 若選取**X.509 憑證**值：
     a. 指定私有金鑰檔案（帶有 *.prk 或 *.pem 副檔名的檔案）。
     b. 指定私有金鑰密碼。
     c. 指定公共金鑰檔案（帶有 *.cer 副檔名）。
6. 點擊**確定**。

應用程式安裝套件的憑證被發佈。

安裝應用程式到用戶端裝置

若要在用戶端裝置上安裝應用程式，請執行以下操作：

1. 在主控台樹狀目錄中開啟**遠端安裝**資料夾並點擊**在受管理裝置上佈署安裝套件（工作站）**以執行防護佈署精靈。
2. 在精靈的**選取安裝套件**視窗中指定要安裝的應用程式安裝套件。
3. 遵照精靈的說明。

當精靈結束時，將建立遠端安裝工作以安裝作業系統到用戶端裝置。您可以在**工作**資料夾中啟動或停止工作。

使用防護佈署精靈，您可以安裝網路代理到執行 Windows、Linux 和 macOS 的用戶端裝置上。

要在執行 Linux 作業系統的裝置上使用卡巴斯基安全管理中心管理 64 位元安全應用程式，您必須使用 64 位元 Linux 網路代理。您可以從技術支援網站下載必要的網路代理版本。

在遠端安裝網路代理到執行 Linux 的裝置之前，您必須準備裝置。

管理物件修訂

該區域包含了物件修訂管理的資訊。卡巴斯基安全管理中心允許您跟蹤物件修改。您每次儲存變更到物件時，*修訂*被建立。每個修訂都有一個數字。

支援修訂管理的應用程式物件包括：

- 管理伺服器內容
- 政策
- 工作
- 管理群組
- 使用者帳戶
- 安裝套件

您可以對物件修訂採取以下操作：

- 將所選修訂與目前進行比較
- 比較所選的修訂
- 將物件與相同類型的其他物件的所選修訂進行比較
- 檢視所選修訂
- 回溯對物件所做的變更到所選的修訂
- 儲存修訂到 .txt 檔案

在支援修訂管理的任何物件的內容視窗中，**變更歷程**區域會顯示含有以下詳情的物件修訂清單：

- 物件修訂版本
- 物件修改的日期和時間

- 修改物件的使用者的名稱
- 執行在物件上的操作
- 與物件設定變更相關的修訂敘述

檢視修訂歷程區域

您可以將物件修訂與目前進行比較，比較清單中選取的不同修訂，或者將物件修訂與相同類型的其他物件的修訂進行比較。

*若要檢視物件的**變更歷程**區域：*

1. 在主控台樹狀目錄中，選取以下物件之一：
   - **管理伺服器**節點
   - **政策**資料夾
   - **工作**資料夾
   - 管理群組資料夾
   - **使用者帳戶**資料夾
   - **已刪除物件**資料夾
   - **安裝套件**子資料夾，嵌套於**遠端安裝**資料夾中
2. 根據相關物件的位置，做以下之一：
   - 如果物件位於**管理伺服器**節點或管理群組節點，請以滑鼠右鍵按一下節點，在上下文功能表中選取**內容**。
   - 若物件位於**政策**、**工作**、**使用者帳戶**、**已刪除物件**或**安裝套件**資料夾，選取該資料夾，並在對應工作區中選取該物件。

   物件內容視窗開啟。
3. 在左方**區域**窗格中，選取**變更歷程**。

   修訂歷程顯示在工作區。

比較物件修訂

你可以將物件過去修訂與目前進行比較，比較清單中選取的不同修訂，或將物件修訂與相同類型的其他物件的修訂進行比較。

要比較物件的修訂：

1. 選取一個物件並轉到物件的內容視窗。
2. 在內容視窗，轉到**變更歷程**區域。

3. 在工作區，在物件修訂清單中，選取修訂以比較。
   要選取物件的多個修訂，使用 **Shift** 和 **Ctrl** 鍵。

4. 執行以下操作之一：

   - 點擊**比較**按鈕並在下拉清單中選取其中一值。

     - **與目前版本比較**

       選取該選項以將所選修訂與目前進行比較。

     - **比較選定版本**

       選取該選項以比較兩個所選修訂。

     - **與其他工作比較**

       當使用工作修訂時，選取**與其他工作比較**選項以將所選修訂與其他工作的修訂進行比較。
       當使用政策修訂時，選取**與其他政策比較**以將所選修訂與其他政策修訂比較。

   - 點擊修訂名稱，在開啟的修訂內容視窗中點擊以下按鈕：

     - **與目前比較**

       點擊該按鈕以將所選修訂與目前進行比較。

     - **與先前比較**

       點擊該按鈕以將所選修訂與先前進行比較。

   一個關於修訂比較的 HTML 格式的檔案顯示在您的預設瀏覽器。

   在該報告中，您可以減少修訂設定的一些區域。要減少物件修訂設定的區域，點擊區域名稱旁邊的箭頭圖示 (▲)。

管理伺服器修訂包含所有變更的詳情，除了以下部分的詳情：

- **流量**區域
- **標記規則**區段
- **通知**區段
- **發佈點**區段
- **病毒爆發**區段
  觸發病毒爆發事件時，在**病毒爆發**區域未記錄政策啟動設定資訊。

您可以將已刪除物件的修訂和現有物件的修訂進行比較，而不是相反：您不能將現有物件的修訂和已刪除物件的修訂進行比較。

為物件修訂和已刪除物件資訊設定儲存期限

物件修訂的儲存期和已刪除物件的儲存期相同。預設儲存期是 90 天。這對程式的一般稽核是足夠的。

僅帶有**修改**權限的使用者在**已刪除物件**區域可以變更儲存期。

要變更物件修訂的儲存期和已刪除物件的儲存期：

1. 在主控台樹狀目錄中，選取您要變更其儲存期的管理伺服器。
2. 右擊並在上下文功能表中選取**內容**。
3. 在開啟的管理伺服器內容視窗，在**變更歷程儲存區**區域，輸入所需的儲存期限（天數）。
4. 點擊**"確定"**。

物件修訂和已刪除物件資訊將被儲存您輸入的天數。

檢視物件修訂

如果您需要瞭解物件在指定時間段內做了哪些修改，您可以檢視物件修訂。

要檢視物件的修訂：

1. 前往物件的**變更歷程**區域。
2. 在物件修訂清單中，選取您想要檢視設定的修訂。
3. 執行以下操作之一：
   - 點擊**檢視修訂**按鈕。
   - 點兩下修訂名稱視窗或點擊**檢視修訂**按鈕，以開啟修訂內容視窗。

一個 HTML 格式的包含所選物件修訂設定的報告被顯示。在該報告中，您可以減少物件修訂設定的一些區域。要減少物件修訂設定的區域，點擊區域名稱旁邊的箭頭圖示 ( )。

儲存物件修訂到檔案

你可以儲存物件修訂到文字檔案，例如，以便透過郵件傳送。

要儲存物件修訂到檔案：

1. 前往物件的**變更歷程**區域。
2. 在物件修訂清單中，選取您想要儲存設定的修訂。
3. 點擊**進階**按鈕並在下拉式清單中選取**儲存到檔案**值。

修訂被儲存到 .txt 檔案。

回溯變更

如果必要，您可以回溯對物件所做的變更。例如，您可能必須轉換政策設定到特定日期的狀態。

要回溯對物件所做的變更：

1. 前往物件的**變更歷程**區域。
2. 在物件修訂清單中，選取您要回溯的修訂號。
3. 點擊**進階**按鈕並在下拉清單中選取**回溯**。

該物件被回溯到所選修訂。物件修訂清單顯示所做的操作記錄。修訂敘述顯示了您轉換物件所到的修訂號的資訊。

新增修訂敘述

您可以為修訂新增敘述以簡化在清單中的修訂搜尋。

要新增修訂敘述：

1. 前往物件的**變更歷程**區域。
2. 在物件修訂清單中，選取您想要新增敘述的修訂。
3. 點擊**敘述**按鈕。
4. 在**物件修訂敘述**視窗，輸入修訂敘述的部分文字。

   預設下，物件修訂敘述為空。
5. 點擊**確定**。

物件刪除

本節提供有關刪除物件的資訊。

您可以刪除物件，包括以下：

- 政策
- 工作
- 安裝套件
- 虛擬管理伺服器
- 使用者

- 安全群組
- 管理群組

要刪除物件：

1. 開啟卡巴斯基安全管理中心網頁主控台的所需部分，然後選取物件。
2. 在工具列上，點擊**刪除**按鈕。
3. 在開啟的視窗中，點擊**確定**按鈕以確認您的選取。

   所選物件被刪除。

當您刪除物件時，其資訊保留在資料庫。已刪除物件的資訊的儲存期與物件修訂的儲存期一致（建議期限是 90 天）。只有當您在權限的**已刪除物件**區域有**修改**權限時才可變更儲存期。

關於刪除用戶端裝置

當您從管理群組中刪除受管理裝置時，應用程式會將裝置移至未分配的裝置群組。然後選取您需要執行測試更新安裝的裝置刪除裝置後，已安裝的卡巴斯基應用程式——網路代理和任何安全應用程式，例如 Kaspersky Endpoint Security ——將保留在裝置上。

卡巴斯基安全管理中心根據以下規則處理未分配裝置群組中的裝置：

- 如果您配置了裝置移動規則，並且裝置符合移動規則的條件，則該裝置會被根據規則自動移動到管理群組。
- 裝置會被儲存在未分配的裝置群組中，並被根據裝置保留規則自動從群組中刪除。

  裝置保留規則不會影響具有一個或多個使用完整磁碟加密進行加密的磁碟機的裝置。此類裝置不會被自動刪除——您只能手動刪除它們。如果您需要刪除帶有加密磁碟機的裝置，請先解密磁碟機，然後再刪除該裝置。

  > 當您刪除帶有加密磁碟機的裝置時，解密磁碟機所需的資料也會被刪除。如果您在刪除此類裝置（不論是從**未配置的裝置**或**受管理裝置**群組）時開啟的確認視窗中選取**我了解風險並希望刪除所選裝置**核取方塊，則表示您已知悉後續會有資料被刪除。

  想解密磁碟機，必須滿足以下條件：

  - 裝置被重新連線到管理伺服器以還原解密磁碟機所需的資料。
  - 裝置使用者記得解密密碼。
  - 用於加密磁碟機的安全應用程式（例如 Kaspersky Endpoint Security for Windows）仍安裝在裝置上。

  如果磁碟機由 Kaspersky Disk Encryption 技術加密，您還可以嘗試使用 FDERT Restore Utility 還原資料.

> 在 VDI 中，如果您的裝置有加密磁碟機，則刪除該裝置後，加密磁碟機上的資訊也會被刪除。

當您從未分配的裝置群組中手動刪除裝置時，應用程式會從清單中刪除該裝置。刪除裝置後，已安裝的卡巴斯基應用程式（如果有）將保留在裝置上。然後，如果該裝置對管理伺服器仍然可見並且您配置了常規網路輪詢，卡巴斯基安全管理中心會在網路輪詢期間發現該裝置並將其新增回未分配的裝置群組。因此，最好僅當裝置對管理伺服器不可見時再手動刪除該裝置。

刪除物件

您可以刪除例如政策、工作、安裝套件、內部使用者和內部安全群組的物件，如果您具有修改權限（權限的基本功能類別）（參見分配權限到使用者和群組一文以獲得更多資訊）。

> 您無法刪除遠端安裝工作中使用的安裝套件。您必須先停止相應的工作。有關管理群組中的自動安裝工作的更多資訊，請參閱在管理群組中的裝置上自動安裝應用程式一文。

要刪除物件：

1. 在主控台樹狀目錄，在所需資料夾的工作區選擇一個物件。
2. 執行以下操作之一：
   - 點擊該物件並選擇**刪除**。
   - 按 **DELETE** 鍵。

物件將被刪除，其資訊將被儲存在資料庫。

檢視關於已刪除物件的資訊

已刪除物件的資訊儲存在**已刪除物件**資料夾，儲存期與物件修訂一致（建議期限是 90 天）。

僅在權限**已刪除物件**區域有**讀取**權限的使用者可檢視已刪除物件的清單（請參閱配置權限給使用者和群組以取得詳細資訊）。

要檢視已刪除物件清單，

在主控台樹狀目錄中，選取**已刪除物件**（依預設，**已刪除物件**是**進階**資料夾的子資料夾）。

若您在權限**已刪除物件**區域沒有讀取權限，**已刪除物件**資料夾中會顯示空白清單。

已刪除物件資料夾的工作區包含以下已刪除物件的相關資訊：

- **名稱**。物件名稱。
- **類型**。物件類型，例如政策、工作或安裝套件。
- **時間**。刪除物件的時間。
- **使用者**。刪除物件的帳戶名稱。

要檢視關於物件的更多資訊：

1. 在主控台樹狀目錄中，選取**已刪除物件**（依預設，**已刪除物件**是**進階**資料夾的子資料夾）。
2. 在**已刪除物件**工作區，選取您需要的物件。
   使用所選物件的區塊出現在工作區的右側。
3. 執行以下操作之一：
   - 點擊方塊中的**內容**連結。
   - 右擊您在工作區中選中的物件，並在上下文功能表中選取**內容**。

   物件的內容視窗開啟，顯示以下標籤：
   - **一般**
   - **變更歷程**

從已刪除物件清單永久刪除物件

僅在權限**已刪除物件**區域有**修改**權限的使用者可從已刪除物件清單永久刪除物件（請參閱配置權限給使用者和群組以取得詳細資訊）。

要從已刪除物件清單刪除物件

1. 在主控台樹狀目錄，選取所需管理伺服器的節點並選取**已刪除物件**資料夾。
2. 在工作區，選取您要刪除的物件。
3. 執行以下操作之一：
   - 按 **DELETE** 鍵。
   - 在您所選物件的上下文功能表中，選取**刪除**。
4. 在確認對話方塊，點擊**是**。

   該物件已從已刪除物件清單永久刪除。此物件的所有資訊（含其修訂）已永久從資料庫刪除。您無法還原該資訊。

行動裝置管理

透過卡巴斯基安全管理中心的行動裝置防護的管理透過使用行動裝置管理功能執行，這需要專用產品授權。如果您要管理組織員工擁有的行動裝置，您必須啟用行動裝置管理。

該部分提供了啟用、配置和停用行動裝置管理的說明。該部分也敘述如何管理已連線至管理伺服器的行動裝置。

有關 Kaspersky Security for Mobile 的詳細資訊，請參閱 *Kaspersky Security for Mobile 說明*。

情境：行動裝置管理佈署

該部分提供在卡巴斯基安全管理中心中配置行動裝置管理功能的方案。

先決條件

確保您具有允許存取行動裝置管理功能的產品授權。

階段

行動裝置管理功能的佈署分步驟進行：

1. **準備連接埠**

   確保連接埠 13292 在管理伺服器上可用。該連接埠用於連線行動裝置。而且，您可能想要使連接埠 17100 可用。該連接埠僅用於受管理行動裝置的啟動代理伺服器；如果受管理行動裝置擁有網際網路連線，您不必使該連接埠可用。

2. **啟用行動裝置管理**

   當您正在執行或稍後將執行管理伺服器快速設定精靈時，您可以啟用行動裝置管理。

3. **指定管理伺服器外部位址**

   當您執行管理伺服器快速設定精靈時可以指定外部位址，或稍後。如果您安裝時未選取"行動裝置管理"且未在安裝精靈中指定位址，在安裝套件內容中指定外部位址。

4. **新增行動裝置到受管理裝置群組**

   新增行動裝置到受管理裝置群組，因此您可以透過政策管理這些裝置。您可以在管理伺服器快速設定精靈的某個步驟中建立移動規則。您也可以稍後建立移動規則。如果您不建立此類規則，您可以手動新增行動裝置到受管理裝置群組。

   您可以直接新增行動裝置到受管理裝置群組，或者您可以為其建立子群組（或多個子群組）。

   此後任何時候，您可以使用新行動裝置連線精靈連線任意新行動裝置到管理伺服器。

5. **為行動裝置建立政策**

   要管理行動裝置，在裝置所屬群組為其建立政策（或多個政策）。您可以在此後的任何時候變更該政策的設定。

結果

您完成這些方案後，您可以使用卡巴斯基安全管理中心管理 Android 和 iOS 裝置。您可以使用行動裝置憑證和傳送指令到行動裝置。

關於管理 EAS 和 iOS MDM 裝置的群組政策

要管理 iOS MDM 和 EAS 裝置，您可以使用包含在卡巴斯基安全管理中心發佈工具套件裡的 Kaspersky Device Management for iOS 的管理外掛程式。Kaspersky Device Management for iOS 允許您為指定 iOS MDM 和 EAS 裝置的配置設定建立群組政策，而不使用 iPhone® 配置實用程式和 Exchange ActiveSync 管理設定檔。

管理 EAS 和 iOS MDM 裝置的群組政策提供管理員以下選項：

- 用於管理 EAS 裝置：
  - 配置裝置-解鎖密碼。
  - 設定資料以加密形式儲存在裝置上。
  - 設定企業郵件的同步。
  - 設定行動裝置的硬體特性，比如卸除式磁碟機的使用、照相機的使用、或 Bluetooth® 的使用。
  - 設定在裝置上使用行動應用程式的限制。
- 用於管理 iOS MDM 裝置：
  - 設定裝置密碼安全設定。
  - 設定對裝置硬體功能的使用，以及行動應用程式的安裝與移除限制。
  - 配置限制預先安裝行動 APP 的使用，如 YouTube™、iTunes® Store 或 Safari。
  - 配置檢視，按裝置所在區域限制媒體內容（範例，電影和電視節目）。
  - 設定裝置透過代理伺服器連線網際網路的設定（Global HTTP 代理）。
  - 設定使用者用以存取企業應用程式和服務的帳戶（單點登入技術）。
  - 監控行動裝置上網際網路的使用（存取網站）。
  - 配置使用不同身分驗證機制和網路協定的無線網路 (Wi-Fi)，存取點 (APN)，以及虛擬私有網路 (VPN) 的設定。
  - 設定與 AirPlay® 裝置的連線設定，以傳送照片、音樂以及影片。
  - 配置從裝置到 AirPrint™ 印表機無線列印檔案的連線設定。
  - 設定與 Microsoft Exchange 伺服器的同步設定，以及在裝置上使用企業信箱的使用者帳戶。
  - 設定使用者憑證同步 LDAP 目錄服務。
  - 設定使用者憑證以連線 CalDAV 和 CardDAV 服務，允許使用者存取企業行事曆和聯絡人清單。
  - 在使用者裝置上配置 iOS 介面的設定，例如字型或者常用網站圖示。
  - 在裝置上新增新的安全憑證。
  - 設定 Simple Certificate Enrollment Protocol (SCEP) 伺服器的設定以自動檢索裝置認證中心的憑證。
  - 為使用行動 APP 新增自訂設定。

管理 EAS 和 iOS MDM 政策是特殊的，因為它指派到的管理群組中既包含 iOS MDM 伺服器又包含 Exchange ActiveSync 行動裝置伺服器（也稱"行動裝置伺服器"）。該政策中指定的所有設定首先套用到行動裝置伺服器，然後套用此類伺服器所管理的行動裝置上。在管理群組的階層架構中，從屬行動裝置伺服器從主要行動裝置伺服器接收該政策設定並發佈到行動裝置。

對於如何使用群組政策以在卡巴斯基安全管理中心管理主控台中管理 EAS 和 iOS MDM 裝置的詳情，請參考 *Kaspersky Security for Mobile* 文件。

啟用行動裝置管理

要管理行動裝置，您必須啟用行動裝置管理。如果您未在快速設定精靈中啟用該功能，您可以稍後啟用它。行動裝置管理需要產品授權。

啟用行動裝置管理僅在主管理伺服器上可用。

要啟用行動裝置管理：

1. 在主控台樹狀目錄中，選取**行動裝置管理**資料夾。
2. 在資料夾工作區中，選擇**啟用行動裝置管理**按鈕。此按鈕在您未啟用**行動裝置管理**之前可用。

   管理伺服器快速啟動精靈的**附加元件**頁面隨即顯示。
3. 選取**啟用行動裝置管理**以管理行動裝置。
4. 在**選取應用程式啟動方法**頁面，使用金鑰檔案或啟動碼啟動應用程式。

   如果您不啟動行動裝置管理功能，則行動裝置管理將不可用。
5. 如果您要在連線到網際網路時使用代理伺服器，請在**用於存取網際網路的代理伺服器設定**頁面選取**使用代理伺服器**核取方塊。如果選中了此方塊，欄位可用於輸入設定。為代理伺服器連線指定設定。
6. 在**檢查外掛程式和安裝套件的更新**頁面，選取以下選項之一：

   - **檢查外掛程式和安裝套件是否是最新**

     啟動更新狀態檢查。如果檢查偵測到一些外掛程式或安裝套件的到期版本，精靈提示您下載最新版本以代替到期版本。

   - **略過檢查**

     繼續工作而不檢查外掛程式和安裝套件是否是最新。您可以在，例如，沒有網際網路連線，或者您要繼續使用應用程式到期版本時選取該選項。

     條件對檢查更新的檢查可能導致應用程式功能不正常。
7. 在**最新外掛程式版本可用**頁面，下載並安裝應用程式版本所需之外掛程式語言的最新版本。更新外掛程式不需要產品授權。

   安裝外掛程式和安裝套件後，應用程式檢查是否所有外掛程式已安裝。如果偵測到一些外掛程式的過期版本，精靈提示您下載最新版本以代替過期版本。
8. 在**行動裝置連線設定**頁面，設定管理伺服器連接埠。

當精靈完成時，將發生以下變更：

- Kaspersky Endpoint Security for Android 政策將被建立。
- Kaspersky Device Management for iOS 政策將被建立。
- 連接埠將在用於行動裝置的管理伺服器上被開啟。

修改行動裝置管理設定

要啟用行動裝置支援：

1. 在主控台樹狀目錄中，選取**行動裝置管理**資料夾。
2. 在資料夾的工作區中，點擊**行動裝置連線連接埠**連結。
   管理伺服器內容視窗的**附加連接埠**區域隨即顯示。
3. 在**附加連接埠**區域，修改相關設定：
   - **啟動代理伺服器的 SSL 連接埠**
   - **為行動裝置開啟連接埠**

     行動裝置連線到產品授權伺服器的連接埠被開啟。您可以在以下欄位定義埠號和其他設定。
     預設情況下已啟用該選項。

   - **行動裝置同步連接埠**

     行動裝置連線到管理伺服器並與其交換資料的埠號。預設埠號為 13292。
     如果連接埠 13292 被用於其他目的，您可以分配其他連接埠。

   - **行動裝置啟動連接埠**

     用於將 Kaspersky Endpoint Security for Android 連線到 Kaspersky 啟動伺服器的連接埠。
     預設埠號為 17100。
4. 點擊**確定**。

停用行動裝置管理

停用行動裝置管理僅在主管理伺服器上可用。

若要停用行動裝置管理：

1. 在主控台樹狀目錄中，選取**行動裝置管理**資料夾。
2. 在此資料夾的工作區，點擊**設定附加元件**連結。
   管理伺服器快速啟動精靈的**附加元件**頁面隨即顯示。
3. 如果不要再管理行動裝置，請選取**不啟用行動裝置管理**。
4. 點擊**確定**。

先前連線的行動裝置將不能連線到管理伺服器。行動裝置連線連接埠和行動裝置啟動連接埠將被自動關閉。

為 Kaspersky Endpoint Security for Android 和 Kaspersky Device Management for iOS 建立的政策將不被刪除。憑證發佈規則不會被修改。安裝的外掛程式將不被刪除。行動裝置移動規則將不被刪除。

您在受管理行動裝置上重新啟用了行動裝置管理後，您可能需要重新安裝行動裝置管理所需的行動應用。

使用行動裝置指令

該區域包含卡巴斯基安全管理中心支援的行動裝置管理的指令資訊。該區域說明了如何傳送指令到行動裝置，以及如何在指令記錄中檢視指令的執行狀態。

行動裝置管理的指令

卡巴斯基安全管理中心支援行動裝置管理指令。

此指令用於遠端行動裝置佈署。範例，一旦您的行動裝置遺失，您可以使用一條指令刪除裝置上的企業資料。

您可以對如下受管理的行動裝置類型使用指令：

- iOS MDM 裝置
- Kaspersky Endpoint Security (KES) 裝置
- EAS 裝置

每個裝置類型支援一群組專用的指令。

指定指令的特殊考慮

- 對於所有裝置類型，如果成功執行**重設為出廠設定**命令，將從裝置刪除所有資料，裝置設定將回溯到它們的出廠值。
- 在 iOS MDM 裝置上成功執行**抹除企業資料**的命令後，所有已安裝的設定檔、provisioning 設定檔、iOS MDM 設定檔以及應用程式因選取了**與 iOS MDM 設定檔一同刪除**核取方塊，所以都會從裝置中刪除。

- 如果在 KES 裝置上執行了**抹除企業資料**命令，所有企業資料、通訊錄項目、SMS 記錄、電話記錄、行事曆、網際網路連線設定，以及使用者帳戶（除了 Google™ 帳戶）都將從裝置上刪除。對於 KES 裝置，記憶體卡中的所有資料也將刪除。

- 在傳送**定位**命令到 KES 裝置之前，您必須確認已授權使用該命令搜尋遺失且屬於您組織或員工的裝置。接收**定位**命令的行動裝置未被鎖定。

行動裝置指令清單

下表顯示 iOS MDM 裝置的指令集。

行動裝置管理支援的命令：iOS MDM 裝置

指令	指令執行結果
鎖定	行動裝置已鎖定。
解鎖	PIN 碼鎖定行動裝置被停用。之前指定的 PIN 碼已被重設。
重設為出廠設定	所有資料均從行動裝置中刪除，設定回溯至預設值。
抹除企業資料	所有已安裝的設定檔、provisioning 設定檔、iOS MDM 設定檔以及應用程式，因選取了**與 iOS MDM 設定檔一同刪除**核取方塊，所以都會從裝置中刪除。
同步裝置	行動裝置資料與管理伺服器同步。
安裝設定檔	在行動裝置上安裝設定檔。
移除設定檔	從行動裝置中刪除設定檔。
安裝 provisioning 設定檔	在行動裝置上安裝 provisioning 設定檔。
移除 provisioning 設定檔	從行動裝置上刪除 provisioning 設定檔。
安裝應用	應用程式被安裝在行動裝置。
移除應用	應用程式從行動裝置上移除。
輸入兌換碼	為已付費應用程式輸入授權碼。
設定漫遊	啟用和停用資料漫遊和語音漫遊。

下表顯示 KES 裝置的指令集。

行動裝置管理的支援指令：KES 裝置

命令	指令執行結果
鎖定	行動裝置已鎖定。
解鎖	PIN 碼鎖定行動裝置被停用。之前指定的 PIN 碼已被重設。
重設為出廠設定	所有資料均從行動裝置中刪除，設定回溯至預設值。
抹除企業資料	企業資料、通訊錄項目、SMS 記錄、電話記錄、行事曆、網際網路連線設定，以及使用者帳戶（除了 Google 帳戶），都已從裝置上刪除。記憶體卡資料已被抹除。
同步裝置	行動裝置資料與管理伺服器同步。
定位裝置	行動裝置已定位並顯示在 Google Maps™ 上。行動營運商收取傳送 SMS 訊息以及提供網際網路連線的費用。
臉部快照	行動裝置已鎖定。照片已經由裝置的前置鏡頭採集並儲存在管理伺服器上。可以在指令記錄中檢視照片。行動營運商收取傳送 SMS 訊息以及提供網際網路連線的費用。
警報	行動裝置發出警報。

下表顯示了 EAS 裝置的命令。

指令	指令執行結果
重設為出廠設定	所有資料均從行動裝置中刪除，設定回溯至預設值。

使用 Firebase Cloud Messaging

為了確保及時將指令交付到 Android 作業系統管理的 KES 裝置上，卡巴斯基安全管理中心使用推送通知機制。推播通知透過 Firebase Cloud Messaging（以下簡稱 FCM）在 KES 裝置和管理伺服器之間交換。在卡巴斯基安全管理中心管理主控台中，可以指定 Firebase Cloud Messaging 的設定從而將 KES 裝置連線到服務。

若要擷取 Firebase Cloud Messaging 的設定，您必須有 Google 帳戶。

要啟用對 FCM 的使用：

1. 在管理主控台中，選取**行動裝置管理** 節點以及**行動裝置**資料夾。
2. 在**行動裝置**的上下文功能表中，選取**內容**。
3. 在資料夾內容中，選取**Google Firebase Cloud Messaging 設定**區域。
4. 在**傳送者 ID**欄位中，指定 FCM 寄件者 ID。
5. 在**私密金鑰檔案（JSON 格式）**欄位中，選擇私鑰檔案。

   在下次同步管理伺服器時，由 Android 作業系統管理的 KES 裝置將被連線到 Firebase Cloud Messaging。

透過點擊**重設設定**按鈕，您可以編輯 Firebase Cloud Messaging 的設定。

傳送指令

傳送指令至使用者的行動裝置：

1. 在主控台樹狀目錄**行動裝置管理**資料夾中，選取**行動裝置**子資料夾。

   該資料夾工作區中將顯示一個受管理行動裝置的清單。
2. 選取您需要傳送指令的使用者行動裝置。
3. 在行動裝置的上下文功能表中，選取**顯示指令記錄**。
4. 在**行動裝置管理命令**視窗，前往您需要傳送到行動裝置的命令名稱的區域，然後點擊**傳送指令**按鈕。

   根據您選取的命令，點擊**傳送指令**按鈕可以開啟應用程式的進階設定視窗。範例，當您傳送從行動裝置刪除 provisioning 設定檔的指令時，程式提示您選取必須從行動裝置刪除的 provisioning 設定檔。在那個視窗定義指令的進階設定並且確認您的選取。在那之後，指令將被傳送到行動裝置。

   您可以點擊**重新傳送**按鈕再次傳送命令到使用者的行動裝置。

   如果還未執行後者，您可以點擊**從佇列刪除**按鈕取消已傳送的命令（如果還未執行命令）。

   指令記錄區域顯示已經被傳送到行動裝置的命令與各自的執行狀態。點擊**重新整理**以更新命令清單。
5. 點擊**確定**以關閉**行動裝置管理命令**視窗。

檢視指令記錄中的指令狀態

程式在指令記錄中儲存被傳送到行動裝置的所有指令的相關資訊。指令記錄包含每條指令傳送到行動裝置的事件和日期資訊，以及他們的相關狀態和指令執行結果的詳細敘述。範例，加入指令執行失敗，記錄顯示錯誤的原因。指令記錄中的記錄最多儲存 30 天。

傳送到行動裝置的指令由以下狀態：

- *執行中* – 命令已傳送到行動裝置。
- *已完成* – 指令執行已成功完成。
- *已完成，但存在錯誤* – 指令執行失敗。
- *正在刪除* – 正在從已傳送到行動裝置的指令佇列中刪除該指令。
- *已刪除* – 已經從傳送到行動裝置的指令佇列中成功刪除該指令。
- *刪除時出錯* – 無法從已傳送到行動裝置的指令佇列中刪除該指令。

程式為每個行動裝置保留一個指令記錄。

檢視已經被傳送到行動裝置的指令記錄：

1. 在主控台樹狀目錄**行動裝置管理**資料夾中，選取**行動裝置**子資料夾。
   該資料夾工作區中將顯示一個受管理行動裝置的清單。
2. 在行動裝置清單中，選取您要檢視其指令記錄的行動裝置。
3. 在行動裝置的上下文功能表中，選取**顯示指令記錄**。
   行動裝置管理指令視窗開啟。**"行動裝置管理指令"**視窗區域顯示能被傳送到行動裝置的指令。
4. 選取包含必要指令的區域，並且透過開啟**指令記錄**區域檢視關於如何傳送和執行指令的資訊。

在**指令記錄**區域，您可以檢視已傳送到行動裝置的指令清單和這些指令的詳細資訊。**顯示指令**篩選可讓您僅在清單中顯示有所選狀態的裝置。

使用行動裝置的憑證

該章節包含關於如何處理行動裝置憑證的資訊。

行動裝置的根憑證在產生後有 700 天的固定有效期限。備用憑證在到期日前 60 天產生。您可以使用以下命令修改產生備用憑證的時間段：

`klscflag.exe -fset -pv klserver -n KLSRV_AKLWNGT_MDM_CERT_CHANGE_TIMEOUT -t d -v <`逾時（以秒鐘為單位）`>`

用於產生備用憑證的時間段需要足夠長，以便所有受管理的行動裝置能夠與管理伺服器同步並檢索憑證。

klscflag 公用程式位於安裝管理伺服器的資料夾中。預設安裝路徑：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

不支援手動續約行動裝置的根憑證。

啟動憑證安裝精靈

您可以安裝以下類型的憑證用於使用者的行動裝置：

- 為識別行動裝置的共用憑證
- 在行動裝置上設定企業郵件的郵件憑證
- 在行動裝置上設定存取虛擬私有網路的 VPN 憑證

若要將憑證安裝在使用者的行動裝置上，請執行以下操作：

1. 在主控台樹狀目錄中，延伸**行動裝置管理**資料夾並選擇**憑證**子資料夾。
2. 在**憑證**資料夾的工作區中，點擊**新增憑證**連結以執行憑證安裝精靈。

   遵照精靈的說明。

在精靈完成後，將建立一個憑證並將其新增到使用者的憑證清單；此外，將向使用者傳送通知，為使用者提供下載憑證並在行動裝置上安裝的連結。您可以檢視所有憑證清單並將其匯出到檔案。您可以刪除和重新交付憑證，以及檢視他們的內容。

步驟 1：選取憑證類型

指定必須安裝到使用者行動裝置上的憑證類型：

- **行動憑證**—用來識別行動裝置
- **郵件憑證**—在行動裝置上設定企業郵件
- **VPN 憑證**—在行動裝置上設定存取虛擬私有網路

步驟 2：選取裝置類型

僅在您選取**郵件憑證** or **VPN 憑證**作為憑證類型時才會顯示此視窗。

指定裝置上的作業系統類型：

- **iOS MDM 裝置**。如果您必須安裝憑證到使用 iOS MDM 協定連線到 iOS MDM 伺服器的行動裝置，則選取該選項。
- **由 Kaspersky Security for Mobile 管理的 KES 裝置**。如果您必須安裝憑證到 KES 裝置，則選取該選項。此種情況下，憑證將用於每次連線管理伺服器時的使用者辨識。
- **未經使用者憑證身分驗證而連線到管理伺服器的 KES 裝置**。如果您必須安裝憑證到不使用憑證身分驗證的 KES 裝置，則選取該選項。在此情況下，在精靈中最後步驟的**使用者通知方式**視窗內，管理員必須選取每次連線管理伺服器使用的使用者身分驗證類型。

步驟 3：選取使用者

在清單中，選取使用者、安全群組或您要安裝憑證的 Active Directory 安全群組。

在**使用者分類**視窗中，您可以搜尋卡巴斯基安全管理中心內部使用者。您可以點擊**新增**以新增內部使用者。

步驟 4：選取憑證來源

在該視窗，您可以選取管理伺服器用於識別行動裝置的憑證來源。您可以使用以下其中一種方式來選取憑證：

- 自動建立憑證，透過管理伺服器工具，然後傳送憑證到裝置。
- 指定一個先前建立的憑證檔案。如果在上一步選取了多個使用者則該方法不可用。

如果您必須發送給使用者為其行動裝置建立憑證的通知，選取**發佈憑證**核取方塊。

如果使用者的行動裝置已經被使用憑證驗證，因此沒有必要指定帳戶名稱和密碼以接收新憑證，則清空**發佈憑證**核取方塊。在此情況下，**使用者通知方式**視窗將不被顯示。

步驟 5：為憑證指派標籤

若已在**裝置類型**選取**iOS MDM 裝置**則會顯示**憑證標籤**視窗。

在下拉清單中，您可以分配標籤到使用者的 iOS MDM 裝置憑證。帶有所分配標籤的憑證可能具有設定在 Kaspersky Device Management for iOS 政策內容中的特別參數。

下拉清單提示您選取*憑證範本 1*、*憑證範本 2* 或 *憑證範本 3* 標籤。您可以在以下區域設定標籤：

- 如果已在**憑證類型**視窗中選取**郵件憑證**，您可以在行動裝置 Exchange ActiveSync 帳戶內容中設定其標籤（**受管理裝置** → **政策** → Kaspersky Device Management for iOS 政策內容 → **Exchange ActiveSync** 區域 → **新增** → **進階**）。
- 如果已在**憑證類型**視窗中選取 **VPN 憑證**，您可以在行動裝置 VPN 內容中設定其標籤（**受管理裝置** → **政策** → Kaspersky Device Management for iOS 政策內容 → **VPN** 區域 → **新增** → **進階**）。如果 L2TP、PPTP 或 IPSec (Cisco™) 連線類型被選取您的 VPN，您無法設定用於 VPN 憑證的標籤。

步驟 6：指定憑證發佈設定

在該視窗中，您可以指定以下憑證發佈設定：

- **不通知使用者新憑證**

  如果您不想傳送使用者行動裝置憑證建立通知到使用者，請啟用該選項。此種情況下，**使用者通知方式**視窗將不被顯示。

  該選項僅適用於安裝了 Kaspersky Endpoint Security for Android 的裝置。

  您可能想要啟用該選項，例如，使用者行動裝置已經被使用憑證進行了身分驗證，因此不必指定帳戶名稱和密碼以接收新憑證。

- **允許裝置擁有單個憑證的多個憑證（僅對於安裝了 Kaspersky Endpoint Security for Android 的裝置）**

  如果您想讓卡巴斯基安全管理中心在憑證即將過期或遺失于目的裝置時自動重新傳送憑證，請啟用該選項。

  憑證在過期之前幾天被自動傳送。您可以在憑證發佈規則視窗設定天數。

  在一些情況下，憑證無法在裝置上找到。例如，當使用者重新安裝 Kaspersky 安全應用程式到裝置或重設裝置設定和資料到出廠設定時可能發生該情況。此種情況下，卡巴斯基安全管理中心在下一次裝置試圖連線到管理伺服器時檢查裝置 ID。如果裝置具有憑證發佈時的相同 ID，應用程式重新發佈憑證到裝置。

步驟 7：選取使用者通知方法

若您選取 **iOS MDM 裝置**作為裝置類型或您選取**不通知使用者新憑證**選項，則不會顯示此視窗。

在**使用者通知方式**視窗，您可以設定將憑證安裝到行動裝置的使用者通知。

在**身分驗證方法**欄位，指定使用者身分驗證類型：

- **憑證（網域或別名）**

  此種情況下，使用者使用網域密碼或卡巴斯基安全管理中心內部使用者密碼接收新憑證。

- **一次性密碼**

  此種情況下，使用者接收透過電子郵件或 SMS 傳送的一次性密碼。該密碼必須被輸入以接收新憑證。

  如果您在**憑證發佈設定**視窗啟用（選取）**允許多裝置使用單一憑證（僅對於安裝了 Kaspersky 行動裝置安全應用程式的裝置）**選項，則該選項變更為**密碼**。

- **密碼**

  此種情況下，密碼在每次憑證被傳送到使用者時使用。

  如果您在**憑證發佈設定**視窗停用（清空）**允許多裝置使用單一憑證（僅對於安裝了 Kaspersky 行動裝置安全應用程式的裝置）**選項，則該選項變更為**一次性密碼**。

若您在**憑證類型**視窗選取**行動憑證**或選取**未經使用者憑證身分驗證而連線到管理伺服器的 KES 裝置**作為裝置類型，則會顯示此欄位。

選取使用者通知選項：

- **當精靈完成時顯示身分驗證密碼**

  如果您選取該選項，使用者名稱、Security Account Manager (SAM) 中的使用者名稱和每個所選使用者接收憑證的密碼將顯示在憑證安裝精靈的最後一步。設定關於已安裝的憑證將不可用的使用者通知。

  當您為多個使用者新增憑證時，您可以透過點擊憑證安裝精靈最後一步的**匯出**按鈕儲存提供的憑證到檔案。

  若您在憑證安裝精靈的**使用者通知方法**步驟中選取**憑證（網域或別名）**，則無法使用此選項。

- **通知使用者新憑證**

  如果您選取該選項，您可以設定關於新憑證的使用者通知。

  - **透過電子郵件**

    在設定的該群組，您可以使用電子郵件訊息配置安裝新憑證到他的/她的行動裝置的使用者通知。該通知方法僅在啟用 SMTP 伺服器時可用。

    點擊**編輯訊息**連結檢視和編輯通知訊息，如果必要。

  - **透過簡訊**

    在該設定群組，您可以配置關於使用 SMS 安裝憑證到行動裝置的使用者通知。該通知方法僅在啟用 SMS 通知時可用。

    點擊**編輯訊息**連結檢視和編輯通知訊息，如果必要。

步驟 8：產生憑證

在此步驟會建立憑證。

您可以點擊**完成**結束精靈。

憑證被建立並顯示在**憑證**資料夾工作區的工作清單。

設定憑證發佈規則

憑證用於在管理伺服器上的裝置身分驗證。所有受管理行動裝置必須擁有憑證。您可以配置憑證如何被發佈。

要設定憑證發佈規則：

1. 在主控台樹狀目錄中，延伸**行動裝置管理**資料夾並選擇**憑證**子資料夾。
2. 在**憑證**資料夾中點擊**配置憑證發佈規則**按鈕，開啟**憑證發佈規則**視窗。

3. 轉到憑證類型名稱的區域：

   行動憑證發佈—設定行動裝置憑證的發佈。

   郵件憑證發佈—設定郵件憑證的發佈。

   VPN 憑證發佈—設定 VPN 憑證的發佈。

4. 在**發佈設定**區域，設定憑證的發佈：

   - 指定憑證期限（天）。

     行動裝置的憑證受根憑證到期日的限制。如果您指定的憑證期限長於根憑證的到期日期，則憑證期限將在產生時自動調整。

   - 選取憑證來源（**管理伺服器**或**手動指定憑證**）。

     管理伺服器被選定作為憑證的預設來源。

   - 指定憑證範本（**預設範本**, **其他範本**）。

     如果**與 PKI 整合**區域啟用了integration with Public Key Infrastructure，則可使用範本的設定。

5. 在**自動更新設定**區域，設定憑證自動更新：

   - 在**當憑證剩餘此天數時續約**欄位，指定憑證到期前還有多少天可續約。

   - 若要啟用憑證的自動更新，請選取**如果可能，自動重新發佈憑證**核取方塊。

6. 在**密碼防護**區域，在憑證加密過程中啟用和設定密碼的使用。

   密碼防護僅對行動憑證可用。

   a. 選擇**在憑證安裝過程中提示密碼**核取方塊。

   b. 使用滑軌定義加密密碼中符號的最大數量。

7. 點擊**確定**。

與公共金鑰基礎架構整合

需要將應用程式與公用金鑰基礎架構 (PKI) 整合才能簡化為使用者發佈網域憑證。整合後，憑證自動發佈。

支援的最小 PKI 伺服器版本是 Windows Server 2008。

您必須設定用於與 PKI 整合的帳戶。該帳戶必須符合以下要求：

- 在安裝了管理伺服器的裝置上是網域使用者或管理員。
- 在安裝了管理伺服器的裝置上被授予 SeServiceLogonRight 權限。

要建立一個永久的使用者設定檔，需要在安裝了管理伺服器的裝置上使用已設定的帳戶登入至少一次。在管理伺服器裝置上的使用者憑證儲存區中，安裝網域管理員提供的登錄代理憑證。

設定與公用金鑰基礎架構的整合：

1. 在主控台樹狀目錄中，延伸**行動裝置管理**資料夾並選擇**憑證**子資料夾。
2. 在工作區中，點擊**與公共金鑰基礎架構整合**按鈕以開啟**憑證發佈規則**視窗的**與 PKI 整合**區域。

   憑證發佈規則視窗的**與 PKI 整合**區域隨即開啟。
3. 選擇將**整合 PKI 憑證的發佈**核取方塊。
4. 在**帳戶**欄位中，指定用來與公鑰基礎設施整合的使用者帳戶名稱。
5. 在**密碼**欄位中，輸入該帳戶的網域密碼。
6. 在**在 PKI 系統中的憑證範本名稱**清單中，選取為網域使用者發佈憑證的憑證範本。

   在卡巴斯基安全管理中心指定帳戶下啟動一個專用服務。服務用於發佈使用者網域憑證。該服務在點擊**重新整理清單**按鈕載入憑證範本清單時，或者當憑證建立時啟動。
7. 點擊**確定**儲存設定。

整合後，憑證自動發佈。

啟用支援 Kerberos Constrained Delegation

應用程式支援 Kerberos Constrained Delegation 的使用。

要啟用支援 Kerberos Constrained Delegation：

1. 在主控台樹狀目錄中，開啟**行動裝置管理**資料夾。
2. 在主控台樹狀目錄**行動裝置管理**資料夾中，選取**行動裝置伺服器**子資料夾。
3. 在**行動裝置伺服器**資料夾的工作區中，選取 iOS MDM 伺服器。
4. 在 iOS MDM 伺服器的上下文功能表中，選取**內容**。
5. 在 iOS MDM 伺服器的"內容"視窗中，選取**"設定"**區域。
6. 在**設定**區域中，選取**確認與 Kerberos Constrained Delegation 相容**核取方塊。
7. 點擊**確定**。

新增 iOS 行動裝置到受管理裝置清單

要新增 iOS 行動裝置到受管理裝置清單，必須傳送並在裝置上提交與安裝共用憑證。共用憑證由管理伺服器使用以識別行動裝置。適用於 iOS 行動裝置的共用憑證會在 iOS MDM 設定檔中提交。在憑證傳送並安裝在行動裝置之後，裝置會出現在受管理裝置清單。

Kaspersky 不再支援 Kaspersky Safe Browser。

您可透過新行動裝置連線精靈新增使用者的行動裝置至受管理裝置清單。

要使用共用憑證將 iOS 裝置連線至管理伺服器：

1. 以下列其中一種方式啟動新行動裝置連線精靈：

   - 使用**使用者帳戶**資料夾中的上下文功能表：

     1. 在主控台樹狀目錄中，展開**進階**資料夾與**使用者帳戶**子資料夾。
     2. 在**使用者帳戶**資料夾的工作區中，選取使用者、安全群組或 Active Directory 安全群組，以新增行動裝置到受管理裝置清單。
     3. 在使用者帳戶的上下文功能表右擊，選取**新增行動裝置**。

        新行動裝置連線精靈啟動。

   - 在**行動裝置**資料夾工作區中，選擇**新增行動裝置**按鈕：

     1. 在主控台樹狀目錄中，延伸**行動裝置管理**資料夾並選擇**行動裝置**子資料夾。
     2. 在**行動裝置**子資料夾的工作區，點擊**新增行動裝置**按鈕。

        新行動裝置連線精靈啟動。

2. 在精靈的**作業系統**頁面，選取 **iOS**作為行動裝置作業系統類型。
3. 在 **選取 iOS MDM 伺服器** 頁面，選取 iOS MDM 伺服器。
4. 在**選取您要管理其行動裝置的使用者**頁面，選取使用者、安全群組或 Active Directory 安全群組，以新增行動裝置到受管理裝置清單。

   若透過在**使用者帳戶**資料夾的上下文功能表選取**新增行動裝置**來啟動精靈，則會略過此步驟。

   若要江心使用者帳戶新增至清單，請點擊**新增**按鈕並在開啟的視窗中輸入使用者內容。若要修改或檢閱使用者帳戶內容，請在清單中選取使用者帳戶並點擊**內容**按鈕。

5. 在精靈的**憑證來源**頁面，請指定建立管理伺服器用以識別裝置的共用憑證的方法。您可以使用下列可用方法之一指定一個共用憑證：

   - **透過管理伺服器發佈憑證**

     若您先前未建立憑證，選取此選項以透過管理伺服器工具建立新憑證。

     如果選取該選項，iOS MDM 設定檔將由管理伺服器自動產生的憑證簽署。

     預設情況下已選取此選項。

   - **指定憑證檔案**

     選取此選項來指定先前建立的憑證檔案。

     如果在上一步選取了多個使用者則該方法不可用。

6. 在精靈的**使用者通知方式**頁面，定義透過 SMS 或電子郵件通知行動裝置使用者關於憑證建立資訊的設定：

- **在精靈中顯示連結**

  如果您選取該選項，安裝套件的連結將顯示在行動裝置連線精靈的最後一步。

  如果為裝置連線選取了多個使用者則該選項不可用。

- **傳送連結到使用者**

  選取此選項允許您配置連線新行動裝置的使用者通知。

  您可以選取郵件信箱類型，指定附加郵件信箱以及編輯訊息文字。您還可以選取使用者電話類型以傳送 SMS 訊息，指定額外電話號碼以及編輯 SMS 訊息文字。

  如果未配置 SMTP 伺服器，郵件訊息無法傳送到使用者。如果未配置 SMS 通知，SMS 訊息無法傳送到使用者。

7. 在**結果**頁面，按一下**完成**以關閉精靈。

iOS MDM 設定檔被自動發佈在卡巴斯基安全管理中心網頁伺服器。行動裝置使用者收到一條帶有用於從網頁伺服器下載 iOS MDM 設定檔的連結的通知。使用者點選連結。此後，行動裝置作業系統會提示使用者接受 iOS MDM 設定檔安裝。用戶必須在 iOS MDM 設定檔可以被下載到行動裝置之前同意安裝 iOS MDM 設定檔。下載 iOS MDM 設定檔並且在 iOS MDM 行動裝置已與管理伺服器同步後，裝置會顯示在**行動裝置**資料夾中，它是在主控台樹狀目錄中**行動裝置管理**資料夾的子資料夾。

為讓使用者使用連結轉到卡巴斯基安全管理中心網頁伺服器，與管理伺服器的連線連接埠 8061 必須在行動裝置上可用。

新增 Android 行動裝置到受管理裝置清單

若要新增 Android 行動裝置至受管理裝置清單，您必須在行動裝置提交與安裝 Kaspersky Endpoint Security for Android 和共用憑證。共用憑證由管理伺服器使用以識別行動裝置。在憑證傳送並安裝在行動裝置之後，裝置會出現在受管理裝置清單。

您可透過新行動裝置連線精靈新增使用者的行動裝置至受管理裝置清單。該精靈會提供兩個選項以供您提交與安裝共用的憑證以及 Kaspersky Endpoint Security for Android：

- 透過使用 Google Play 連結
- 透過來自卡巴斯基安全管理中心網頁伺服器的連結

  在管理伺服器儲存用來分發的 Kaspersky Endpoint Security for Android 安裝套件會用來安裝

啟動新行動裝置連線精靈

若要啟動新行動裝置連線精靈，請執行以下其中一個操作：

- 使用**使用者帳戶**資料夾中的上下文功能表：

  1. 在主控台樹狀目錄中，展開**進階**資料夾與**使用者帳戶**子資料夾。
  2. 在**使用者帳戶**資料夾的工作區中，選取使用者、安全群組或 Active Directory 安全群組，以新增行動裝置到受管理裝置清單。
  3. 在使用者帳戶的上下文功能表右擊，選取**新增行動裝置**。

     新行動裝置連線精靈啟動。

- 在**行動裝置**資料夾工作區中，選擇**新增行動裝置**按鈕：

  1. 在主控台樹狀目錄中，延伸**行動裝置管理**資料夾並選擇**行動裝置**子資料夾。
  2. 在**行動裝置**子資料夾的工作區，點擊**新增行動裝置**按鈕。

     新行動裝置連線精靈啟動。

透過 Google Play 連結新增 Android 行動裝置

若要在行動裝置上使用 Google Play 連結安裝 Kaspersky Endpoint Security for Android 與共用憑證：

1. 啟動新行動裝置連線精靈。
2. 在精靈的**作業系統**視窗，選取 **Android** 作為行動裝置作業系統類型。
3. 在精靈的**Kaspersky Endpoint Security for Android 安裝方法**頁面中，選取**透過使用 Google Play 連結**。
4. 在精靈的**選取您要管理其行動裝置的使用者**頁面上，選取使用者、安全群組或 Active Directory 安全群組以新增行動裝置到受管理裝置清單。

   若透過在**新增行動裝置**資料夾的上下文功能表選取**使用者帳戶**來啟動精靈，則會略過此步驟。

   若要江心使用者帳戶新增至清單，請點擊**新增**按鈕並在開啟的視窗中輸入使用者內容。若要修改或檢閱使用者帳戶內容，請在清單中選取使用者帳戶並點擊**內容**按鈕。

5. 在精靈的**憑證來源**頁面，請指定建立管理伺服器用以識別裝置的共用憑證的方法。您可以使用下列可用方法之一指定一個共用憑證：

   - **透過管理伺服器發佈憑證**

     若您先前未建立憑證，選取此選項以透過管理伺服器工具建立新憑證。

     若已選取此選項，憑證會透過管理伺服器工具自動發佈。

     預設情況下已選取此選項。

   - **指定憑證檔案**

     選取此選項來指定先前建立的憑證檔案。

     如果在上一步選取了多個使用者則該方法不可用。

6. 在精靈的**使用者通知方式**頁面，定義透過 SMS 或電子郵件通知行動裝置使用者關於憑證建立資訊的設定：

   - **在精靈中顯示連結**

     如果您選取該選項，安裝套件的連結將顯示在行動裝置連線精靈的最後一步。

     如果為裝置連線選取了多個使用者則該選項不可用。

   - **傳送連結到使用者**

     選取此選項允許您配置連線新行動裝置的使用者通知。

     您可以選取郵件信箱類型，指定附加郵件信箱以及編輯訊息文字。您還可以選取使用者電話類型以傳送 SMS 訊息，指定額外電話號碼以及編輯 SMS 訊息文字。

     如果未配置 SMTP 伺服器，郵件訊息無法傳送到使用者。如果未配置 SMS 通知，SMS 訊息無法傳送到使用者。

7. 在**結果**頁面，按一下**完成**以關閉精靈。

精靈結束操作後，一個連結和 QR 代碼將被傳送到使用者行動裝置從而允許下載 Kaspersky Endpoint Security for Android。使用者點選連結或掃描 QR 代碼。此後，行動裝置作業系統會提示使用者接受 Kaspersky Endpoint Security for Android 的安裝。Kaspersky Endpoint Security for Android 下載並安裝後，行動裝置連線到管理伺服器並下載共用憑證。在行動裝置安裝憑證後，裝置會顯示在**行動裝置**資料夾中，它在主控台樹狀目錄是**行動裝置管理**資料夾的子資料夾。

使用來自卡巴斯基安全管理中心網頁伺服器的連結新增 Android 行動裝置

發佈在管理伺服器的 Kaspersky Endpoint Security for Android 安裝套件。

若要使用網頁伺服器連結在行動裝置安裝 Kaspersky Endpoint Security for Android 與共用憑證：

1. 啟動新行動裝置連線精靈。

2. 在精靈的**作業系統**視窗，選取 **Android** 作為行動裝置作業系統類型。

3. 在精靈的**Kaspersky Endpoint Security for Android 安裝方法**頁面中，選取**透過使用網頁伺服器連結**。

   在出現的欄位中，選取安裝套件或透過點擊**新增**建立新安裝套件。

4. 在精靈的**選取您要管理其行動裝置的使用者**頁面上，選取使用者、安全群組或 Active Directory 安全群組以新增行動裝置到受管理裝置清單。

   > 若透過在**新增行動裝置**資料夾的上下文功能表選取**使用者帳戶**來啟動精靈，則會略過此步驟。

   若要江心使用者帳戶新增至清單，請點擊**新增**按鈕並在開啟的視窗中輸入使用者內容。若要修改或檢閱使用者帳戶內容，請在清單中選取使用者帳戶並點擊**內容**按鈕。

5. 在精靈的**憑證來源**頁面，請指定建立管理伺服器用以識別裝置的共用憑證的方法。您可以使用下列可用方法之一指定一個共用憑證：

   - **透過管理伺服器發佈憑證**

     若您先前未建立憑證，選取此選項以透過管理伺服器工具建立新憑證。

     若已選取此選項，憑證會透過管理伺服器工具自動發佈。

     預設情況下已選取此選項。

   - **指定憑證檔案**

     選取此選項來指定先前建立的憑證檔案。

     如果在上一步選取了多個使用者則該方法不可用。

6. 在精靈的**使用者通知方式**頁面，定義透過 SMS 或電子郵件通知行動裝置使用者關於憑證建立資訊的設定：

   - **在精靈中顯示連結**

     如果您選取該選項，安裝套件的連結將顯示在行動裝置連線精靈的最後一步。

     > 如果為裝置連線選取了多個使用者則該選項不可用。

   - **傳送連結到使用者**

     選取此選項允許您配置連線新行動裝置的使用者通知。

     您可以選取郵件信箱類型，指定附加郵件信箱以及編輯訊息文字。您還可以選取使用者電話類型以傳送 SMS 訊息，指定額外電話號碼以及編輯 SMS 訊息文字。

     如果未配置 SMTP 伺服器，郵件訊息無法傳送到使用者。如果未配置 SMS 通知，SMS 訊息無法傳送到使用者。

7. 在**結果**頁面，按一下**完成**以關閉精靈。

Kaspersky Endpoint Security for Android 行動應用程式套件被自動發佈在卡巴斯基安全管理中心網頁伺服器。行動應用程式套件包含應用程式、行動裝置連線到管理伺服器的設定和憑證。行動裝置使用者將接收包含從網頁伺服器下載套件的連結的通知。使用者點選連結。裝置作業系統會提示使用者接受行動應用程式套件的安裝。如果使用者同意，套件將被下載到行動裝置。下載套件並在行動裝置已與管理伺服器同步後，裝置會顯示在**行動裝置**資料夾中，它是在主控台樹狀目錄中**行動裝置管理**資料夾的子資料夾。

管理 Exchange ActiveSync 行動裝置

此部分敘述透過卡巴斯基安全管理中心管理 EAS 裝置的進階功能。

除了透過指令方式管理 EAS 裝置，管理員可以使用如下選項：

- 建立 EAS 裝置管理設定檔，分配到使用者的郵箱。*EAS 管理設定檔*是 Exchange ActiveSync 的一個政策，該政策用在 Microsoft Exchange 伺服器管理 EAS 裝置。在 EAS 裝置管理設定檔中，您可以設定如下群組設定：
  - 使用者密碼管理設定
  - 郵件同步
  - 使用行動裝置功能的限制
  - 使用行動裝置行動應用程式的限制

  根據行動裝置型號，管理設定檔的設定可以部分套用。已經套用 Exchange ActiveSync 政策的狀態，可以在行動裝置內容檢視。
- 檢視關於設定 EAS 裝置管理的資訊。例如，在行動裝置內容中，管理員可以瞭解上一次與 Microsoft Exchange 伺服器同步的時間，EAS 裝置的 ID，Exchange ActiveSync 政策名稱，及其在行動裝置的目前狀態。
- 如果沒有使用，從管理斷開 EAS 裝置。
- 由 Exchange 行動裝置伺服器定義 Active Directory 的輪詢設定，它允許更新使用者的信箱和行動裝置的資訊。

新增管理設定檔

要管理 EAS 裝置，您可以建立 EAS 裝置管理設定檔，並指派它們到選定的 Microsoft Exchange 信箱。

只能將一個 EAS 裝置管理設定檔分配給 Microsoft Exchange 信箱。

要為 Microsoft Exchange 信箱新增 EAS 裝置管理設定檔：

1. 在主控台樹狀目錄中，開啟**行動裝置管理**資料夾。
2. 在主控台樹狀目錄**行動裝置管理**資料夾中，選取**行動裝置伺服器**子資料夾。
3. 在**行動裝置伺服器**資料夾的工作區中，選取 Exchange 行動裝置伺服器。
4. 從 Exchange 行動裝置伺服器的上下文功能表中選取**內容**。
   行動裝置伺服器內容視窗將開啟。
5. 在**Exchange 行動裝置伺服器**的內容視窗中，選取**郵件信箱**區域。

6. 選取信箱，點擊**配置設定檔**按鈕。
   政策設定檔視窗將開啟。
7. 在**政策設定檔**視窗中，點擊**新增**按鈕。
   新設定檔視窗隨即開啟。
8. 在**新設定檔**視窗的頁籤中對設定檔進行設定。
   - 如果您想要指定設定檔名稱並更新間隔，選取**一般**頁籤。
   - 如果您想設定行動裝置使用者的密碼，選取**密碼**頁籤。
   - 如果您想設定與 Microsoft Exchange 伺服器的同步，選取**同步**頁籤。
   - 如果您想設定裝置功能的限制，選取**功能限制**頁籤。
   - 如果您想設定行動裝置上移動應用程式的使用限制，選取**應用程式限制**頁籤。
9. 點擊**確定**。
   新設定檔將顯示在**政策設定檔**視窗中的設定檔清單中。
   如果您想要該設定檔自動指派給新信箱，以及設定檔被刪除的信箱，請在清單中選取設定檔並點擊**設定為預設的設定檔**按鈕。

   > 預設設定檔不能刪除。要刪除目前預設設定檔，您必須到不同的設定檔分配“預設設定檔”內容。

10. 在**政策設定檔**視窗，點擊**確定**。
    將在下次將 EAS 裝置與 Exchange 行動裝置伺服器同步時在裝置上套用管理設定檔設定。

刪除管理設定檔

要為 Microsoft Exchange 信箱刪除 EAS 裝置管理設定檔：

1. 在主控台樹狀目錄中，開啟**行動裝置管理**資料夾。
2. 在主控台樹狀目錄**行動裝置管理**資料夾中，選取**行動裝置伺服器**子資料夾。
3. 在**行動裝置伺服器**資料夾的工作區中，選取 Exchange 行動裝置伺服器。
4. 從 Exchange 行動裝置伺服器的上下文功能表中選取**內容**。
   行動裝置伺服器內容視窗將開啟。
5. 在 Exchange 行動裝置伺服器的內容視窗中，選取**郵件信箱**區域。

6. 選取信箱，點擊**變更設定檔**按鈕。

   "政策設定檔"視窗將開啟。

7. 在**政策設定檔**視窗，選取您想要刪除的設定檔並點擊點擊紅叉按鈕。

   選定的設定檔將從管理設定檔清單中刪除。目前預設設定檔將套用到被已刪除的設定檔管理的 EAS 裝置上。

   如果您想要刪除目前預設設定檔，需要重新給其他的設定檔指派"預設設定檔"內容，然後刪除第一個。

處理 Exchange ActiveSync 政策

在您安裝 Exchange 行動裝置伺服器後，在伺服器內容視窗的**郵件信箱**區域，您可以檢視透過輪詢目前網域或者網域樹系來獲取的 Microsoft Exchange 伺服器帳戶資訊。

而且，在 Exchange 行動裝置伺服器內容視窗，您可以使用以下按鈕：

- **變更設定檔**允許您開啟**政策設定檔**視窗，該視窗包含從 Microsoft Exchange 伺服器獲取的政策清單。在該視窗中，您可以建立、編輯或刪除 Exchange ActiveSync 政策。**政策設定檔**視窗幾乎與 Exchange Management Console 的政策編輯視窗相同。
- **指派設定檔給行動裝置**允許您分配所選的 Exchange ActiveSync 政策到一個或幾個帳戶。
- **啟動/停用 ActiveSync** 允許您為一個或多個帳戶啟用或停用 Exchange ActiveSync HTTP。

配置掃描範圍

在新安裝的 Exchange 行動裝置伺服器內容中，在**設定**區域，您可以配置掃描範圍。預設下，掃描範圍是安裝 Exchange 行動裝置伺服器的目前網域。選取**整個網域樹系**值可以延伸掃描範圍到整個網域樹系。

使用 EAS 裝置

在**行動裝置管理**節點的**行動裝置**資料夾，透過掃描 Microsoft Exchange 伺服器獲取的裝置將被新增到裝置通用清單。

如果您要**行動裝置**資料夾僅顯示 Exchange ActiveSync 裝置（EAS 裝置），透過點擊清單上方的**Exchange ActiveSync (EAS)**連結篩選裝置清單。

以指令管理 EAS 裝置。例如，**重設為出廠設定**命令可讓您從裝置移除所有資料，並重設裝置設定到出廠設定。該指令在裝置遺失或被盜時有用，當您需要防止企業或個人資料落入協力廠商之手時。

如果所有資料都從裝置上刪除，它將在裝置下次連線到 Microsoft Exchange 伺服器時再次被刪除。該指令將在裝置從裝置清單中被刪除之前再次被觸發。該行為由 Microsoft Exchange 伺服器操作原則導致。

若要從清單中刪除 EAS 裝置，請在裝置上下文功能表中，選取**刪除**.。如果 Exchange ActiveSync 帳戶被從 EAS 裝置上刪除，後者將在裝置與 Microsoft Exchange 伺服器同步後再次出現在裝置清單。

檢視有關 EAS 裝置的資訊

要檢視有關 EAS 裝置的資訊，請執行以下操作：

1. 在主控台樹狀目錄**行動裝置管理**資料夾中，選取**行動裝置**子資料夾。
   該資料夾工作區中將顯示一個受管理行動裝置的清單。
2. 在工作區中，點擊**Exchange ActiveSync (EAS)**連結篩選 EAS 裝置。
3. 從行動裝置的上下文功能表中，選取**內容**。
   開啟 EAS 裝置的內容視窗。

該行動裝置的內容視窗中將顯示已連線的 EAS 裝置的相關資訊。

將 EAS 裝置斷開管理

要從 Exchange 行動裝置伺服器斷開 EAS 裝置的管理：

1. 在主控台樹狀目錄**行動裝置管理**資料夾中，選取**行動裝置**子資料夾。
   該資料夾工作區中將顯示一個受管理行動裝置的清單。
2. 在工作區中，點擊**Exchange ActiveSync (EAS)**連結篩選 EAS 裝置。
3. 選取您要從 Exchange 行動裝置伺服器斷開管理的行動裝置。
4. 在行動裝置的上下文功能表中，選取**刪除**。

EAS 裝置使用紅色十字圖標標記刪除。裝置從 Exchange ActiveSync 伺服器的資料庫中刪除之後，也將從受管理裝置清單中刪除。為此，管理員必須刪除 Microsoft Exchange 伺服器上的使用者帳戶。

使用者管理 Exchange ActiveSync 行動裝置的權限

要管理在 Microsoft Exchange Server 2010 或 Microsoft Exchange Server 2013 中透過 Exchange ActiveSync 協定執行的行動裝置，請確保使用者包含在允許為其執行以下 commandlet 的角色群組中：

- Get-CASMailbox
- Set-CASMailbox
- Remove-ActiveSyncDevice
- Clear-ActiveSyncDevice
- Get-ActiveSyncDeviceStatistics
- Get-AcceptedDomain
- Set-AdServerSettings

- Get-ActiveSyncMailboxPolicy
- New-ActiveSyncMailboxPolicy
- Set-ActiveSyncMailboxPolicy
- Remove-ActiveSyncMailboxPolicy

要管理在 Microsoft Exchange Server 2007 中透過 Exchange ActiveSync 協定執行的行動裝置，請確保已為使用者授予管理員權限。如果尚未授予權限，則執行 commandlet 以為使用者分配管理員權限（請參閱下表）。

在 Microsoft Exchange Server 2007 上管理 Exchange ActiveSync 行動裝置所需的管理員權限

權限	物件	Cmdlet
完全	"CN=Mobile Mailbox Policies，CN=您的企業，CN=Microsoft Exchange，CN=Services,CN=Configuration,DC=您的網域"	`Add-ADPermission -User < 使用者或群組名稱 > -Identity "CN=Mobile Mailbox Policies,CN=< 組織名稱 >,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=< 網域名稱 >" -InheritanceType All -AccessRight GenericAll`
讀取	"CN=您的企業，CN=Microsoft Exchange，CN=Services，CN=Configuration，DC=您的網域"	`Add-ADPermission -User < 使用者或群組名稱 > -Identity "CN=< 組織名稱 >,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=< 網域名稱 >" -InheritanceType All -AccessRight GenericRead`
讀/寫	Active Directory 物件的 msExchMobileMailboxPolicyLink 和 msExchOmaAdminWirelessEnable 內容	`Add-ADPermission -User < 使用者或群組名稱 > -Identity "DC=< 網域名稱 >" -InheritanceType All -AccessRight ReadProperty,WriteProperty -Properties msExchMobileMailboxPolicyLink, msExchOmaAdminWirelessEnable`
完全	ms-Exch-Store-Admin 的信箱儲存區	`Get-MailboxDatabase | Add-ADPermission -User < 使用者或群組名稱 > -ExtendedRights ms-Exch-Store-Admin`

有關在 Exchange Management Shell 主控台使用 commandlet 的詳細資訊，請參閱 Microsoft Exchange Server 技術支援網站。

管理 iOS MDM 裝置

本章節介紹透過卡巴斯基安全管理中心管理 iOS MDM 裝置的進階功能。本程式支援使用以下功能管理 iOS MDM 裝置：

- 以集中模式定義受管 iOS MDM 裝置的設定，並透過設定檔限制裝置的功能。您可新增或修改設定檔並將其安裝到行動裝置上。
- 使用 provisioning 設定檔安裝應用到行動裝置，略過 App Store。範例，您可以使用 provisioning 設定檔在使用者行動裝置上安裝內部企業應用程式。Provisioning 設定檔包含有關應用程式和行動裝置的資訊。
- 透過 App Store 在 iOS MDM 裝置上安裝應用程式。將某個應用安裝至 iOS MDM 裝置之前，您必須將該應用新增至 iOS MDM 伺服器。

每 24 個小時向相連的所有 iOS MDM 裝置傳送一次推送通知，以便將資料與 iOS MDM 伺服器同步。

有關設定檔和 provisioning 設定檔，以及安裝在 iOS MDM 裝置上的應用程式的資訊，請參閱裝置內容視窗。

透過憑證籤署 iOS MDM 設定檔

您可以透過憑證籤署 iOS MDM 設定檔。您可以使用自己簽發的憑證，也可以從受信任的憑證簽發機構接收憑證。

iOS 裝置會針對未簽署的設定檔顯示免責聲明，並提示使用者在安裝設定檔時信任簽署者。

要透過憑證籤署 iOS MDM 設定檔：

1. 在主控台樹狀目錄**行動裝置管理**資料夾中，選取**行動裝置**子資料夾。
2. 在**行動裝置**的上下文功能表中，選取**內容**。
3. 在資料夾的內容視窗中，選取**iOS 裝置的連線設定**區域。
4. 點擊**選取憑證檔案**欄位下的**瀏覽**按鈕。
   憑證視窗。
5. 在**憑證類型**欄位，指定公有或私有憑證類型：
   - 如果選取了 **PKCS#12 容器**值，指定憑證檔案和密碼。
   - 若選取**X.509 憑證**值：
     a. 指定私有金鑰檔案（帶有 *.prk 或 *.pem 副檔名的檔案）。
     b. 指定私有金鑰密碼。
     c. 指定公共金鑰檔案（帶有 *.cer 副檔名）。
6. 點擊**確定**。

iOS MDM 設定檔由憑證簽署。

新增設定檔

若要建立組態文件，可以使用 Apple Configurator 2，您可從 Apple Inc. 網站上獲得。Apple Configurator 2 僅可在執行 macOS 的裝置上執行；如果您沒有這些裝置可用，則可以在有管理主控台的裝置上使用 iPhone Configuration Utility。但是，Apple Inc.不再支援 iPhone Configuration Utility。

若要使用 iPhone Configuration Utility 建立組態設定檔並將其新增至 iOS MDM 伺服器，請執行以下操作：

1. 在主控台樹狀目錄中，選取**行動裝置管理**資料夾。
2. 在**行動裝置管理**資料夾的工作區，選擇**行動裝置伺服器**子資料夾。
3. 在**行動裝置伺服器**資料夾的工作區中，選取 iOS MDM 伺服器。
4. 在 iOS MDM 伺服器的上下文功能表中，選取**內容**。
   行動裝置伺服器內容視窗將開啟。
5. 在 iOS MDM 行動裝置伺服器的內容視窗中，選取**設定檔**區域。
6. 在**設定檔**區域中，點擊**建立**按鈕。
   新設定檔視窗隨即開啟。
7. 在**新設定檔**視窗中，為設定檔指定名稱和 ID。
   設定檔的 ID 應為獨一無二的：需要用"反向 DNS"的格式指定值，如，*com.companyname.identifier*。

8. 點擊**確定**。

   如果安裝了 iPhone Configuration Utility，則系統會將其啟動。

9. 在 iPhone 配置公用程式中重設定設定檔。

   關於設定檔的設定的敘述和如何設定設定檔的介紹，請參閱 iPhone 配置公用程式隨附的檔案。

在您使用 iPhone 配置公用程式完成設定之後，新的設定檔將顯示在 iOS MDM 伺服器內容視窗的**設定檔**區域中。

您可以點擊**修改**按鈕修改設定檔。

您可以點擊**匯入**按鈕為程式載入設定檔。

您可以點擊**匯出**按鈕可以將設定檔儲存到檔案。

您建立的設定檔必須安裝到 iOS MDM 裝置。

將設定檔安裝至裝置

要將設定檔安裝至行動裝置：

1. 在主控台樹狀目錄**行動裝置管理**資料夾中，選取**行動裝置**子資料夾。

   該資料夾工作區中將顯示一個受管理行動裝置的清單。

2. 在工作台中，透過協議類型 (*iOS MDM*) 篩選 iOS MDM 裝置。

3. 選取您必須安裝設定檔的使用者行動裝置。

   您可以選取多個行動裝置同時安裝設定檔。

4. 在行動裝置的上下文功能表中，選取**顯示指令記錄**。

5. 在**行動裝置管理命令**視窗，前往**安裝設定檔**區域，點擊**傳送指令**按鈕。

   您也可以在行動裝置的上下文功能表中，選取**所有指令**向行動裝置傳送命令，然後選取**安裝設定檔**。

   選取設定檔視窗開啟，顯示設定檔清單。從清單中選取您必須在裝置上安裝的設定檔。您可以選取在行動裝置上同時安裝多個設定檔。選取設定檔範圍，使用 **Shift** 鍵。要合併設定檔到一個群組，使用 **CTRL** 鍵。

6. 點擊**確定**按鈕傳送命令到行動裝置。

   執行該指令後，將在使用者的行動裝置上安裝所選取的設定檔。如果指令成功執行，在指令記錄中指令的目前狀態顯示為*已完成*。

   您可以點擊**重新傳送**按鈕再次傳送命令到使用者的行動裝置。

   如果還未執行後者，您可以點擊**從佇列刪除**按鈕取消已傳送的命令（如果還未執行命令）。

   指令記錄區域顯示已經被傳送到行動裝置的命令與各自的執行狀態。點擊**重新整理**以更新命令清單。

7. 點擊**確定**以關閉**行動裝置管理命令**視窗。

您可以查看已安裝的設定檔，如有必要，也可將其刪除。

從裝置中刪除設定檔

若要將設定檔從行動裝置中刪除，請執行以下操作：

1. 在主控台樹狀目錄**行動裝置管理**資料夾中，選取**行動裝置**子資料夾。

   該資料夾工作區中將顯示一個受管理行動裝置的清單。

2. 在工作區中，按一下 **iOS MDM** 連結篩選 iOS MDM 裝置。

3. 選取您必須刪除設定檔的使用者行動裝置。

   您可以選取多個行動裝置同時刪除設定檔。

4. 在行動裝置的上下文功能表中，選取**顯示指令記錄**。

5. 在**行動裝置管理命令**視窗，前往**移除設定檔**區域，點擊**傳送指令**按鈕。

   您也可以從裝置的上下文功能表中，選取**所有指令**傳送命令到行動裝置，然後再選取**移除設定檔**。

   移除設定檔視窗會開啟，顯示設定檔的清單。

6. 從清單中選取您必須從行動裝置刪除的設定檔。您可以選取多個設定檔從行動裝置中同時刪除它們。選取設定檔範圍，使用 **Shift** 鍵。要合併設定檔到一個群組，使用 **CTRL** 鍵。

7. 點擊**確定**按鈕傳送命令到行動裝置。

   成功執行該指令後，將從使用者的行動裝置中刪除所選取的設定檔。如果指令被成功執行，指令的目前狀態將被顯示為*已完成*。

   您可以點擊**重新傳送**按鈕再次傳送命令到使用者的行動裝置。

   如果還未執行後者，您可以點擊**從佇列刪除**按鈕取消已傳送的命令（如果還未執行命令）。

   指令記錄區域顯示已經被傳送到行動裝置的命令與各自的執行狀態。點擊**重新整理**以更新命令清單。

8. 點擊**確定**以關閉**行動裝置管理命令**視窗。

透過發佈設定檔連結來新增新裝置

在管理主控台，管理員使用憑證安裝精靈來建立新的 iOS MDM 設定檔。該精靈執行以下操作：

- iOS MDM 設定檔自動發佈在網頁伺服器。
- 使用者透過 SMS 或電子郵件傳送到 iOS MDM 設定檔的連結。在接收連結時，使用者安裝 iOS MDM 設定檔到行動裝置。
- 行動裝置連線到 iOS MDM 伺服器。

由於 Apple 引入的更嚴厲的安全政策，在連線執行 iOS 11 的行動裝置到啟用了與公共金鑰基礎架構 (PKI) 的整合的管理伺服器時，您必須設定 TLS 1.1 和 TLS 1.2 協議版本。

透過由管理員安裝設定檔來新增新裝置

要透過安裝 iOS MDM 設定檔到行動裝置來連線行動裝置到 iOS MDM 伺服器，管理員必須執行以下操作：

1. 在管理主控台中，開啟憑證安裝精靈。
2. 透過在精靈視窗中選取**精靈完成後顯示憑證**核取方塊來建立新的 iOS MDM 設定檔。
3. 儲存 iOS MDM 設定檔。
4. 透過 Apple Configurator 公用程式安裝 iOS MDM 設定檔到使用者行動裝置。

   行動裝置連線到 iOS MDM 伺服器。

由於 Apple 引入的更嚴厲的安全政策，在連線執行 iOS 11 的行動裝置到啟用了與公共金鑰基礎架構 (PKI) 的整合的管理伺服器時，您必須設定 TLS 1.1 和 TLS 1.2 協議版本。

新增 provisioning 設定檔

要新增 provisioning 設定檔到 iOS MDM 伺服器：

1. 在主控台樹狀目錄中，開啟**行動裝置管理**資料夾。
2. 在主控台樹狀目錄**行動裝置管理**資料夾中，選取**行動裝置伺服器**子資料夾。
3. 在**行動裝置伺服器**資料夾的工作區中，選取 iOS MDM 伺服器。
4. 在 iOS MDM 伺服器的上下文功能表中，選取**內容**。

   行動裝置伺服器內容視窗將開啟。
5. 在 **iOS MDM 伺服器**的內容視窗中，轉到 **Provisioning 設定檔**區域。
6. 在 **provisioning 設定檔**區域，點擊**匯入**按鈕，然後指定 provisioning 設定檔的路徑。

   該設定檔將被新增至 iOS MDM 伺服器設定中。

   您可以點擊**匯出**按鈕可將 provisioning 設定檔儲存到檔案。

您可以安裝在 iOS MDM 裝置上匯入的 provisioning 設定檔。

將 provisioning 設定檔安裝至裝置

要將 provisioning 設定檔安裝至行動裝置：

1. 在主控台樹狀目錄**行動裝置管理**資料夾中，選取**行動裝置**子資料夾。

   該資料夾工作區中將顯示一個受管理行動裝置的清單。

2. 在工作台中，透過協議類型 (*iOS MDM*) 篩選 iOS MDM 裝置。

3. 選取您必須安裝 provisioning 設定檔的使用者行動裝置。

   您可以選取多個行動裝置同時安裝 provisioning 設定檔。

4. 在行動裝置的上下文功能表中，選取**顯示指令記錄**。

5. 在**行動裝置管理命令**視窗，轉到**安裝 provisioning 設定檔**區域，點擊**傳送指令**按鈕。

   您也可以從行動裝置的上下文功能表中透過選取**所有指令**傳送命令到行動裝置，然後選取**安裝 provisioning 設定檔**。

   選取 provisioning 設定檔視窗開啟顯示 provisioning 設定檔的清單。從清單中選取您需要安裝在行動裝置上的 provisioning 設定檔。您可以選取多個 provisioning 設定檔在行動裝置上同時安全它們。要選取 provisioning 設定檔的範圍，使用 **Shift** 鍵。要合併 provisioning 設定檔到一個群組，使用 **Ctrl** 鍵。

6. 點擊**確定**按鈕傳送命令到行動裝置。

   執行該指令後，將在使用者的行動裝置上安裝所選取的 provisioning 設定檔。如果命令成功執行，在命令記錄中命令的目前狀態顯示為*已完成*。

   您可以點擊**重新傳送**按鈕再次傳送命令到使用者的行動裝置。

   如果還未執行後者，您可以點擊**從佇列刪除**按鈕取消已傳送的命令（如果還未執行命令）。

   指令記錄區域顯示已經被傳送到行動裝置的命令與各自的執行狀態。點擊**重新整理**以更新命令清單。

7. 點擊**確定**以關閉**行動裝置管理命令**視窗。

您可以查看已安裝的設定檔，如有必要，也可將其刪除。

從裝置中刪除 provisioning 設定檔

若要將 provisioning 設定檔從行動裝置中刪除，請執行以下操作：

1. 在主控台樹狀目錄**行動裝置管理**資料夾中，選取**行動裝置**子資料夾。

   該資料夾工作區中將顯示一個受管理行動裝置的清單。

2. 在工作台中，透過協議類型 (*iOS MDM*) 篩選 iOS MDM 裝置。

3. 選取您需要刪除 provisioning 設定檔的使用者行動裝置。

   您可以選取多個行動裝置同時刪除 provisioning 設定檔。

4. 在行動裝置的上下文功能表中，選取**顯示指令記錄**。

5. 在**行動裝置管理命令**視窗，前往**刪除 provisioning 設定檔**區域，點擊**傳送指令**按鈕。

   您也可以從上下文功能表中透過選取**所有指令**傳送指令到行動裝置，然後選取**刪除 provisioning 設定檔**。

   移除 provisioning 設定檔視窗會開啟，顯示設定檔的清單。

6. 從清單中選取您需要從行動裝置刪除 provisioning 設定檔。您可以從行動裝置中選取多個 provisioning 設定檔同時刪除它們。要選取 provisioning 設定檔的範圍，使用 **Shift** 鍵。要合併 provisioning 設定檔到一個群組，使用 **Ctrl** 鍵。

7. 點擊**確定**按鈕傳送命令到行動裝置。

   成功執行該指令後，將從使用者的行動裝置中刪除所選取的 provisioning 設定檔。與已刪除 provisioning 設定檔相關的應用程式將不可操作。如果指令被成功執行，指令的目前狀態將被顯示為*已完成*。

   您可以點擊**重新傳送**按鈕再次傳送命令到使用者的行動裝置。

   如果還未執行後者，您可以點擊**從佇列刪除**按鈕取消已傳送的命令（如果還未執行命令）。

   指令記錄區域顯示已經被傳送到行動裝置的命令與各自的執行狀態。點擊**重新整理**以更新命令清單。

8. 點擊**確定**以關閉**行動裝置管理命令**視窗。

新增受管應用程式

將某個應用安裝至 iOS MDM 裝置之前，您必須將該應用新增至 iOS MDM 伺服器。如果已透過卡巴斯基安全管理中心將應用程式安裝到裝置上，則其被視為受管。可透過卡巴斯基安全管理中心遠端管理受管應用程式。

要將受管應用程式安裝至 iOS MDM 伺服器管理，請執行以下操作：

1. 在主控台樹狀目錄中，開啟**行動裝置管理**資料夾。

2. 在主控台樹狀目錄**行動裝置管理**資料夾中，選取**行動裝置伺服器**子資料夾。

3. 在**行動裝置伺服器**資料夾的工作區中，選取 iOS MDM 伺服器。

4. 在 iOS MDM 伺服器的上下文功能表中，選取**內容**。

   這將開啟 iOS MDM 伺服器的"內容"視窗。

5. 在 iOS MDM 伺服器的內容視窗中，選取**受管理應用程式**區域。

6. 點擊在**受管理應用程式**區域的**新增**按鈕。

   新增應用程式視窗開啟。

7. 在**新增應用程式**視窗中的**應用名稱**欄位中，指定要新增的應用程式名稱。

8. 在**Apple ID 或資訊清單檔案連結**欄位中，指定要新增的應用程式的 Apple ID，或指定可用於下載應用程式的清單檔案連結。

9. 如果想要在刪除 iOS MDM 設定檔時隨其從使用者行動裝置中刪除受管應用程式，請選取**與 iOS MDM 設定檔一同刪除**方塊。

10. 如果想要封鎖透過 iTunes 備份應用程式資料，請選取**封鎖資料備份**方塊。

11. 點擊**確定**。

已新增的應用程式將顯示在 iOS MDM 伺服器的內容視窗的**受管理應用程式**區域中。

在行動裝置上安裝應用程式

若要在 iOS MDM 行動裝置上安裝應用程式，請執行以下操作：

1. 在主控台樹狀目錄**行動裝置管理**資料夾中，選取**行動裝置**子資料夾。

   該資料夾工作區中將顯示一個受管理行動裝置的清單。

2. 選取您想要安裝應用程式的 iOS MDM 裝置。

   您可以選取多個行動裝置同時安裝應用程式。

3. 在行動裝置的上下文功能表中，選取**顯示指令記錄**。

4. 在**行動裝置管理命令**視窗，前往**安裝應用**區域，點擊**傳送指令**按鈕。

   您也可以在行動裝置的上下文功能表中選取**所有指令**以向行動裝置傳送命令，然後選取**安裝應用**。

   選取應用視窗開啟，顯示設定檔清單。從清單中選取您需要在行動裝置上安裝的應用程式。您可以選取在行動裝置上同時安裝多個應用程式。選取應用程式範圍，使用 **Shift** 鍵。要合併應用程式到一個群組，使用 **Ctrl** 鍵。

5. 點擊**確定**按鈕傳送指令到行動裝置。

   執行該指令後，將在使用者的行動裝置上安裝所選取的應用程式。如果命令成功執行，在命令記錄中命令的目前狀態顯示為*已完成*。

   您可以點擊**重新傳送**按鈕再次傳送命令到使用者的行動裝置。如果還未執行後者，您可以點擊**從佇列刪除**按鈕取消已傳送的命令（如果還未執行命令）。

   指令記錄區域顯示已經被傳送到行動裝置的命令與各自的執行狀態。點擊**重新整理**以更新命令清單。

6. 點擊**確定**以關閉**行動裝置管理命令**視窗。

已安裝應用程式的資訊顯示在 iOS MDM 行動裝置的內容裡。您可以從行動裝置移除應用程式，使用命令列記錄或行動裝置的上下文功能表。

將應用程式從裝置上移除

若要從行動裝置中移除應用程式，請執行以下操作：

1. 在主控台樹狀目錄**行動裝置管理**資料夾中，選取**行動裝置**子資料夾。

   該資料夾工作區中將顯示一個受管理行動裝置的清單。

2. 在工作台中，透過協議類型 (*iOS MDM*) 篩選 iOS MDM 裝置。

3. 選取您必須移除應用的使用者行動裝置。

   您可以選取多個行動裝置同時移除應用程式。

4. 在行動裝置的上下文功能表中，選取**顯示指令記錄**。

5. 在**行動裝置管理命令**視窗，轉到**移除應用**區域並點擊**傳送指令**按鈕。

   您也可以在行動裝置的上下文功能表中選取**所有指令**以向行動裝置傳送命令，然後選取**移除應用**。

   移除應用視窗隨即開啟並顯示應用程式的清單。

6. 從清單中選取您需要從行動裝置移除的應用程式。您可以選取多個應用程式從裝置中同時移除它們。選取應用程式範圍，使用 **Shift** 鍵。要合併應用程式到一個群組，使用 **Ctrl** 鍵。

7. 點擊**確定**按鈕傳送命令到行動裝置。

   成功執行該指令後，將從使用者的行動裝置中移除所選取的應用程式。如果指令被成功執行，指令的目前狀態將被顯示為*已完成*。

   您可以點擊**重新傳送**按鈕再次傳送命令到使用者的行動裝置。

   如果還未執行後者，您可以點擊**從佇列刪除**按鈕取消已傳送的命令（如果還未執行命令）。

   指令記錄區域顯示已經被傳送到行動裝置的命令與各自的執行狀態。點擊**重新整理**以更新命令清單。

8. 點擊**確定**以關閉**行動裝置管理命令**視窗。

在 iOS MDM 行動裝置上設定漫遊

要設定漫遊：

1. 在主控台樹狀目錄中，開啟**行動裝置管理**資料夾。

2. 在**行動裝置管理**資料夾中選取**行動裝置**資料夾。

   該資料夾工作區中將顯示一個受管理行動裝置的清單。

3. 選取您要設定漫遊的使用者所擁有的 iOS MDM 裝置。

   您可以選取多個行動裝置同時設定其漫遊。

4. 在行動裝置的上下文功能表中，選取**顯示指令記錄**。

5. 在**行動裝置管理命令**視窗，前往**設定漫遊**區域並點擊**傳送指令**按鈕。

   您也可以透過在裝置的上下文功能表中選取**所有指令 → 設定漫遊**傳送命令到行動裝置。

6. 在**漫遊設定**視窗中，指定相關設定：

   - **啟用資料漫遊**

     如果啟用該選項，iOS MDM 行動裝置上將啟用音訊漫遊。iOS MDM 行動裝置的使用者在漫遊時可以上網衝浪。

     預設情況下已停用該選項。

將為所選裝置設定漫遊。

檢視有關 iOS MDM 裝置的資訊

要檢視有關 iOS MDM 裝置的資訊，請執行以下操作：

1. 在主控台樹狀目錄**行動裝置管理**資料夾中，選取**行動裝置**子資料夾。

   該資料夾工作區中將顯示一個受管理行動裝置的清單。

2. 在工作區中，按一下 **iOS MDM** 連結篩選 iOS MDM 裝置。

3. 選取您要檢視其資訊的行動裝置。

4. 從行動裝置的上下文功能表中，選取**內容**。

   iOS MDM 裝置的內容視窗隨即開啟。

該行動裝置的內容視窗中將顯示已連線的 iOS MDM 裝置的相關資訊。

將 iOS MDM 裝置斷開管理

要從 iOS MDM 伺服器斷開 iOS MDM 裝置：

1. 在主控台樹狀目錄**行動裝置管理**資料夾中，選取**行動裝置**子資料夾。

   該資料夾工作區中將顯示一個受管理行動裝置的清單。

2. 在工作區中，按一下 **iOS MDM** 連結篩選 iOS MDM 裝置。

3. 選取您必須斷開的行動裝置。

4. 在行動裝置的上下文功能表中，選取**刪除**。

   iOS MDM 裝置將標記在已移除清單中。行動裝置從 iOS MDM 伺服器的資料庫中刪除後，會自動從受管理裝置清單中刪除。行動裝置將在一分鐘內從 iOS MDM 伺服器資料庫刪除。

iOS MDM 裝置斷開管理後，所有已安裝的設定檔、iOS MDM 設定檔以及應用程式因啟用了**與 iOS MDM 設定檔一同刪除**選項，所以都將從行動裝置中刪除。

傳送指令到裝置

要將指令傳送到 iOS MDM 裝置，請執行以下操作：

1. 在管理主控台中開啟**行動裝置管理**節點。

2. 選擇**行動裝置**資料夾。

3. 在**行動裝置**資料夾，選取要傳送命令的行動裝置。

4. 在行動裝置的上下文功能表中，選取**顯示指令記錄**。

5. 在出現的清單中，選取要傳送到行動裝置的指令。

檢查所傳送指令的執行狀態

要檢查已傳送到行動裝置之指令的執行狀態，請執行以下操作：

1. 在管理主控台中開啟**行動裝置管理**節點。

2. 選擇**行動裝置**資料夾。

3. 在**行動裝置**資料夾，選取要檢查所選命令執行狀態的行動裝置。

4. 在行動裝置的上下文功能表中，選取**顯示指令記錄**。

管理 KES 裝置

在卡巴斯基安全管理中心中，您可以透過以下方式管理 KES 行動裝置：

- 透過使用指令集中管理 KES 裝置。
- 檢視 KES 裝置參數設定的相關資訊。
- 透過使用行動應用程式套件安裝應用程式。
- 將 KES 裝置斷開管理。

建立 KES 裝置行動應用程式套件

Kaspersky Endpoint Security for Android 授權是為 KES 裝置建立行動 APP 安裝套件所必需的。

要建立行動裝置安裝套件：

1. 在主控台樹狀目錄**遠端安裝**資料夾中，選取**安裝套件**子資料夾。
   遠端安裝資料夾預設是**進階**資料夾的子資料夾。

2. 點擊**附加操作**按鈕並在下拉式清單選取**管理行動應用程式套件**。

3. 在**行動應用程式套件管理**視窗中，點擊**新增**按鈕。

4. 新套件精靈啟動。遵照精靈的說明。

新建立的行動應用程式安裝套件顯示在**行動應用程式套件管理**視窗中。

啟用 KES 裝置的憑證式驗證

若要啟用 KES 裝置的憑證式驗證：

1. 開啟安裝了管理伺服器的用戶端裝置的登錄檔（例如，在**開始 → 執行**功能表使用 regedit 指令）。

2. 轉至以下分支：

   - 對於 32 位元系統：
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - 對於 64 位元系統：
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\

3. 建立名為 LP_MobileMustUseTwoWayAuthOnPort13292 的鍵。

4. 指定 REG_DWORD 做為鍵類型。
5. 設定鍵值為 1。
6. 重新啟動管理伺服器服務。

在您執行管理伺服器服務後，系統將會啟用使用共用憑證對 KES 裝置強制執行憑證式驗證。

> KES 裝置到管理伺服器的第一次連線不需要憑證。

預設會停用 KES 裝置的憑證式驗證。

檢視有關 KES 裝置的資訊

檢視有關 KES 裝置的資訊：

1. 在主控台樹狀目錄**行動裝置管理**資料夾中，選取**行動裝置**子資料夾。

   該資料夾工作區中將顯示一個受管理行動裝置的清單。
2. 在工作區，依協定類型 (*KES*) 篩選 KES 裝置。
3. 選取您要檢視其資訊的行動裝置。
4. 從行動裝置的上下文功能表中，選取**內容**。

   開啟 KES 裝置的內容視窗。

該行動裝置的內容視窗中將顯示已連線的 KES 裝置的相關資訊。

將 KES 裝置斷開管理

要將 KES 裝置斷開管理，使用者必須從行動裝置上移除網路代理。使用者刪除了網路代理，行動裝置詳情就從管理伺服器資料庫刪除，因此管理員可以從受管理的裝置清單刪除行動裝置。

要從受管裝置清單中刪除 KES 裝置：

1. 在主控台樹狀目錄**行動裝置管理**資料夾中，選取**行動裝置**子資料夾。

   該資料夾工作區中將顯示一個受管理行動裝置的清單。
2. 在工作區，依協定類型 (*KES*) 篩選 KES 裝置。
3. 選取您必須斷開管理的行動裝置。
4. 在行動裝置的上下文功能表中，選取**刪除**。

   裝置就從受管理行動裝置清單中刪除了。

   如果 Kaspersky Endpoint Security for Android 未從行動裝置上移除，行動裝置在與管理伺服器同步後會再次出現在受管裝置清單中。

資料加密與防護

在筆記本、卸除式磁碟機或硬碟磁碟機被竊取或遺失，或未經授權的使用者和應用程式存取資料時，資料加密能夠降低資料意外洩漏的風險。

Kaspersky Endpoint Security for Windows 提供資料加密功能。Kaspersky Endpoint Security for Windows 可以加密儲存在裝置本機磁碟機和卸除式裝置上的檔案，也可以加密整個卸除式磁碟機和硬碟磁碟機。

資料加密規則透過卡巴斯基安全管理中心中定義的政策進行設定。按照現有規則進行的加密和解密將在套用政策時執行。

加密管理功能的可用性由使用者介面設定決定。

管理員可以操作以下功能：

- 在裝置的本機磁碟機配置和執行檔案加密或解密。
- 設定和執行卸除式磁碟機上的檔案加密。
- 建立加密檔案的存取規則。
- 如果檔案加密功能在使用者裝置上受限，則可以建立並傳遞給使用者存取加密檔案的權限金鑰，透過金鑰可對用戶端進行加密權限控管。
- 配置和執行硬碟磁碟機加密。
- 管理使用者存取加密硬碟和可卸除裝置（管理授權代理帳戶，建立關於帳戶名稱和密碼的資訊、加密裝置存取金鑰並傳遞給使用者）。
- 檢視加密狀態和檔案加密報告。

管理員可使用 Kaspersky Endpoint Security for Windows 提供的專屬工具執行這些操作。關於如何執行操作的詳細說明和加密功能的詳細資訊，請參閱 Kaspersky Endpoint Security for Windows Online Help。

卡巴斯基安全管理中心支援執行 macOS 作業系統的裝置使用加密管理功能。對於支援加密功能的應用程式版本，加密使用 Kaspersky Endpoint Security for Mac 工具配置。關於如何執行操作的詳細說明和加密功能的詳細資訊，請參閱 *Kaspersky Endpoint Security for Mac 管理手冊*。

檢視加密裝置的清單

若要檢視儲存加密資訊的裝置清單，請執行以下操作：

1. 在主控台樹狀目錄中，選取**資料加密與防護**節點。
2. 使用以下方法之一，開啟加密裝置清單：
   - 在**管理加密磁碟機**區域中點擊**移至加密磁碟機清單**連結。
   - 在主控台樹狀目錄中選取**加密磁碟機**資料夾。

此後，在工作台會顯示網路上的加密裝置儲存資訊，與加密等級。磁碟機上的資訊加密後，該裝置會自動從加密清單中移除。

您可以在裝置清單的任何欄中以遞減或遞增進行排序。

使用者介面設定會決定**資料加密與防護**資料夾是否出現在主控台樹狀目錄中。

檢視加密事件清單

在裝置上執行資料加密或解密工作時，Kaspersky Endpoint Security for Windows 會將以下類型的事件傳送給卡巴斯基安全管理中心：

- 無法加密或解密檔案，或由於磁碟空間不足無法建立加密的壓縮檔案。
- 無法加密或解密檔案，或由於授權問題無法建立加密的壓縮檔案。
- 無法加密或解密檔案，或由於缺少存取權限無法建立加密的壓縮檔案。
- 該應用程式已被封鎖存取加密檔案。
- 未知錯誤。

若要檢視在裝置上的加密資料時發生的錯誤清單，請執行以下操作：

1. 在主控台樹狀目錄中，選取**資料加密與防護**節點。
2. 使用以下方法之一開啟在加密期間所發生事件的清單：
   - 透過點擊**資料加密錯誤**區段中的**移到錯誤清單**連接。
   - 透過在主控台樹狀目錄中選取**加密磁碟機**資料夾。

此後，工作台將顯示裝置上在資料加密期間出現問題的相關資訊。

您可以對加密事件清單採取以下操作：

- 以遞減或遞增對任何欄中的資料進行排序。
- 執行事件的快速搜尋（由清單中的文字符號進行比對）。
- 將事件清單匯出到文字檔案中。

使用者介面設定會決定**資料加密與防護**資料夾是否出現在主控台樹狀目錄中。

將加密事件清單匯出到文字檔案中

要將加密事件清單匯出到文字檔案中，請執行以下操作：

1. 建立加密事件清單。
2. 從事件清單的上下文功能表中，選取**匯出清單**。

   "匯出清單"視窗將開啟。
3. 在**"匯出清單"**視窗中，指定包含指定事件清單的檔案名稱，並選取一個資料夾來儲存，然後點擊**"儲存"**按鈕。

   加密事件清單將存至您所指定的檔案中。

建立和檢視加密報告

您可以建立以下報告：

- 受管理裝置加密狀態報告。此報告提供有關各種受管理裝置的資料加密詳細資訊。例如，該報告顯示套用已設定加密規則之政策的裝置數量。此外，您還可以找出需要重新啟動的裝置數量。該報告還包含每台裝置的加密技術和演算法相關資訊。
- 大容量儲存裝置加密狀態報告。此報告包含的資訊與受管理裝置加密狀態報告類似，但它僅提供大容量儲存裝置和卸除式磁碟機的資料。
- 加密磁碟機存取權限報告。此報告會顯示哪些使用者帳戶可以存取加密磁碟機。
- 檔案加密錯誤報告。此報告包含在裝置上執行資料加密或解密工作時所發生錯誤的相關資訊。
- 封鎖存取加密檔案的報告。該報告包含了封鎖應用程式存取加密檔案的資訊。如果未經授權的使用者或應用程式試圖存取加密檔案或磁碟機，則此報告很有用。

若要產生裝置加密報告，請執行以下操作：

1. 在主控台樹狀目錄中，選取**資料加密與防護**資料夾。
2. 執行以下操作之一：
   - 若要產生受管理裝置的加密狀態報告，請點擊**檢視大容量儲存裝置加密狀態報告**連結。
     如果您未設定該報告，新報告範本精靈將啟動。遵照精靈的說明。
   - 若要產生大量儲存裝置加密狀態報告，請在主控台樹狀目錄選取**加密磁碟機**子資料夾，接著點擊**檢視大容量儲存裝置加密狀態報告**按鈕。

報告產生將開始。報告會顯示在**管理伺服器**節點的**報告**頁籤中。

若要產生有關已加密裝置存取權限的報告，請執行以下操作：

1. 在主控台樹狀目錄中，選取**資料加密與防護**資料夾。
2. 執行以下操作之一：
   - 在**管理加密磁碟機**區域中點擊**加密磁碟機存取權限報告**連結以啟動新報告範本精靈。
   - 選取**加密磁碟機**子資料夾，接著點擊**加密磁碟機存取權限報告**按鈕以啟動新報告範本精靈。
3. 按照「新報告範本精靈」的步驟進行操作。

報告產生將開始。報告會顯示在**管理伺服器**節點的**報告**頁籤中。

若要產生檔案加密錯誤報告，請執行以下操作：

1. 在主控台樹狀目錄中，選取**資料加密與防護**資料夾。
2. 執行以下操作之一：
   - 點擊**資料加密錯誤**區域中的**檢視檔案加密錯誤報告**連結以啟動新報告範本精靈。
   - 選取**加密事件**子資料夾，然後按一下**檔案加密錯誤報告**連結來啟動新報告精靈。
3. 按照「新報告範本精靈」的步驟進行操作。

報告產生將開始。報告會顯示在**管理伺服器**節點的**報告**頁籤中。

若要產生受管理裝置加密狀態報告，請執行以下操作：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。
2. 在節點的工作區中，選取**報告**標籤。
3. 按一下**新報告範本**按鈕啟動新報告範本精靈。

4. 按照「新報告範本精靈」的步驟進行操作。在**選取報告範本類型**視窗的**其他**區域選取**受管理裝置加密狀態報告**。

   在您完成新報告範本精靈後，一份新的報告範本出現在管理伺服器節點的**報告**頁籤。

5. 在管理伺服器節點的**報告**頁籤，選取在先前步驟中建立的報告範本。

報告產生將開始。報告會顯示在**管理伺服器**節點的**報告**頁籤中。

您也可以透過檢視管理伺服器節點的**統計**頁籤上的資訊窗格獲取有關裝置和卸除式磁碟機的加密狀態是否符合加密政策的資訊。

若要產生加密檔案存取封鎖報告，請執行以下操作：

1. 在主控台樹狀目錄中，選取擁有的管理伺服器名稱節點。

2. 在節點的工作區中，選取**報告**標籤。

3. 按一下**新增報告範本**按鈕啟動新報告範本精靈。

4. 按照「新報告範本精靈」的步驟進行操作。在**選取報告範本類型**視窗中的**其他**區域選取**封鎖存取加密檔案的報告**。

   在新報告範本精靈完成後，**管理伺服器**節點的**報告**頁籤會出現一份新報告範本。

5. 在**管理伺服器**節點的**報告**頁籤，選取在先前步驟中建立的報告範本。

報告產生將開始。報告會顯示在**管理伺服器**節點的**報告**頁籤中。

在管理伺服器之間傳輸加密金鑰

在受管理裝置上啟用資料加密功能後，加密金鑰會儲存在管理伺服器上。加密金鑰會用來存取加密資料以及管理加密政策。

在以下情況下必須將加密金鑰傳輸至其他管理伺服器：

- 您可在受管理裝置上重新設定網路代理，以指派裝置至其他管理伺服器。若此裝置內含加密資料，則加密金鑰必須傳輸至目標管理伺服器。否則，無法加密資料。

- 您加密已連接至裝置 D1 並由管理伺服器 S1 管理的卸除式磁碟機，之後您將此卸除式磁碟機連接至管理伺服器 S2 管理的裝置 D2。若要存取卸除式磁碟機上的資料，必須將加密金鑰從管理伺服器 S1 傳輸至管理伺服器 S2。

- 您加密由管理伺服器 S1 管理之裝置 D1 上的檔案，之後您嘗試存取由管理伺服器 S2 管理之裝置 D2 的檔案。若要存取檔案，加密金鑰必須從管理伺服器 S1 傳輸至管理伺服器 S2。

您可以透過下列方式傳輸加密金鑰：

- 系統會自動啟用必須傳輸加密金鑰的兩個管理伺服器內容中的**使用管理伺服器層級獲取加密金鑰**選項。若此選項在其中一個管理伺服器停用，則無法自動傳輸加密金鑰。

  在管理伺服器內容啟用**使用管理伺服器層級獲取加密金鑰**選項後，管理伺服器會將儲存於儲存區的所有加密金鑰傳送至在階層中高一級的主管理伺服器（若有）。

  當您嘗試存取加密資料，管理伺服器會先在自己的儲存區搜尋加密金鑰。若啟用**使用管理伺服器層級獲取加密金鑰**選項，且在儲存區中找不到所需的加密金鑰，則管理伺服器會另外將要求傳送至主管理伺服器（若有），以提供所需的加密金鑰。要求將會傳送至所有主管理伺服器，最終傳送至位於階層中最高層級的伺服器。

目前在網頁主控台介面中，無法使用**使用管理伺服器層級獲取加密金鑰**選項。如果您無法存取基於 MMC 的管理主控台，請使用主管理伺服器管理加密的主機。

- 匯出和匯入包含加密金鑰的檔案，以手動從某個管理伺服器傳送至另一個管理伺服器。

  加密金鑰的匯出和匯入是加密金鑰管理功能所包含的操作。要執行這些操作，請如下配置功能的存取權限給卡巴斯基安全管理中心使用者：

  - 將加密金鑰管理功能的**讀取**存取權限授予從屬管理伺服器匯出加密金鑰的使用者。
  - 將加密金鑰管理功能的**寫入**存取權限授予將加密金鑰匯入目的管理伺服器的使用者。

若要在階層內的管理伺服器之間自動傳輸加密金鑰：

1. 在主控台樹狀目錄中，選取您要啟動自動傳輸加密金鑰的管理伺服器。
2. 在管理伺服器的上下文功能表中，選取**內容**。
3. 在內容視窗中，選取**加密演算法**區域。
4. 啟用**使用管理伺服器層級獲取加密金鑰**選項。
5. 按一下**確定**以套用變更。

加密金鑰將會在下次同步時（活動訊號）傳輸至主管理伺服器。此管理伺服器也會在收到要求時，從其儲存區提供加密金鑰給從屬管理伺服器。

若要在管理伺服器之間手動傳輸加密金鑰：

1. 在管理伺服器的主控台樹狀目錄中，選取您要由此傳輸加密金鑰的從屬管理伺服器。
2. 在管理伺服器的上下文功能表中，選取**內容**。
3. 在內容視窗中，選取**加密演算法**區域。
4. 按一下**從管理伺服器匯出加密金鑰**。

   確保將加密金鑰管理功能的**讀取**存取權限授予從伺服器匯出加密金鑰的使用者。

5. 在**匯出加密金鑰**視窗：
   - 按一下**瀏覽**按鈕，然後指定要在哪裡儲存檔案。
   - 指定密碼以防護檔案，避免未獲授權的存取。

     記住密碼。無法擷取遺失的密碼。若遺失密碼，您必須重複匯出程序。因此，請記下密碼並放置於方便拿取的地方。

6. 將檔案傳輸至另一個管理伺服器，例如透過共用資料夾或卸除式磁碟機進行。
7. 在目標管理伺服器上，確保卡巴斯基安全管理中心管理主控台正在執行。
8. 在管理伺服器的主控台樹狀目錄中，選擇您要傳輸加密金鑰的目標管理伺服器。
9. 在管理伺服器的上下文功能表中，選取**內容**。
10. 在內容視窗中，選取**加密演算法**區域。
11. 點擊**匯入加密金鑰到管理伺服器**。
    確保將加密金鑰管理功能的**寫入**存取權限授予匯入加密金鑰到伺服器的使用者。
12. 在**匯入加密金鑰**視窗：
    - 按一下**瀏覽**按鈕，然後選取包含加密金鑰的檔案。
    - 指定密碼。
13. 點擊**"確定"**。

    加密金鑰會傳輸至目標管理伺服器。

資料儲存區

本章節介紹管理伺服器中儲存的、用來追蹤用戶端裝置的使用情況及進行服務的資料。

主控台樹狀目錄的**儲存區**資料夾會顯示用來追蹤用戶端裝置狀態的資料。

儲存區 資料夾包含下列物件：

- 分發到用戶端裝置的管理伺服器下載的更新
- 網路上偵測的裝置清單
- 用戶端裝置上偵測到的授權金鑰
- 被安全應用程式置於裝置隔離區的檔案
- 在用戶端裝置上置於備份區中的檔案
- 被安全應用程式推遲掃描的檔案

將儲存區物件清單匯出到文字檔案中

您可以將儲存區物件清單匯出為檔案。

要將儲存區物件清單匯出到文字檔案中，請執行以下操作：

1. 在主控台樹狀目錄中，在**儲存區**資料夾，選取相關儲存區的子資料夾。
2. 在儲存區子資料夾中，選取上下文功能表中的**匯出清單**。
   系統將開啟**匯出清單**視窗，您可在視窗中指定文字檔案名稱和儲存路徑。

安裝套件

卡巴斯基安全管理中心會將 Kaspersky 和協力廠商的安裝套件放置到資料儲存中。

*安裝套件*是安裝應用程式所需的一個檔案集合。安裝套件中含有安裝的應用程式及初始設定。

如果您希望將程式安裝到用戶端裝置上，您應該為此程式建立安裝套件或者使用現有安裝套件。所建立安裝套件的清單位於主控台樹狀目錄**遠端安裝**資料夾的**安裝套件**子資料夾內。

儲存區中檔案的主狀態

安全應用程式掃描裝置上的檔案以尋找已知病毒和其他可能導致威脅的程式，分配狀態到檔案並放置一些到儲存區。

例如，安全應用程式可以做如下：

- 刪除檔案之前儲存其副本到儲存區
- 隔離儲存區中的疑似感染檔案

檔案的主狀態顯示在下表。您可以在安全應用程式的 Help 系統中獲得更多關於對檔案所採取的操作的詳情。

儲存區中檔案的狀態

狀態名稱	狀態敘述
被感染	檔案具有已知病毒代碼或 Kaspersky 病毒資料庫發現的其他惡意軟體資訊部分。
未感染	檔案中未偵測到已知病毒或其他惡意軟體。
警告	檔案包含比對已知危險代碼的代碼片段。
疑似感染	檔案包含已知病毒的修改代碼或 Kaspersky 的未知病毒代碼。
由使用者放置到資料夾	使用者手動放置檔案到儲存區，因為檔案行為提高了威脅可疑度。使用者可以使用最新資料庫掃描該檔案以尋找威脅。
誤報	Kaspersky 應用程式分配已感染狀態到未感染的檔案，因為其代碼類似病毒代碼。使用最新資料庫掃描後，檔案被識別為未感染。
已解毒	檔案已成功解毒。
已刪除	檔案在處理過程中被刪除。
密碼防護	檔案無法被處理，因為它由密碼防護。

智慧培訓模式中的規則觸發

該部分提供了用戶端裝置上的 Kaspersky Endpoint Security for Windows 中的適應性異常控制規則執行的偵測資訊。

規則偵測用戶端裝置上的異常行為並可能封鎖它。如果規則工作在智慧培訓模式，它們偵測異常行為並傳送每個偵測的報告到卡巴斯基安全管理中心管理伺服器。此資訊會以清單儲存在**儲存區**資料夾的**智慧培訓狀態中的規則觸發**子資料夾中。您可以確認偵測為正確或新增它們為排除，因此該行為類型不再被認為是異常。

偵測資訊儲存在管理伺服器的事件記錄中（與其他事件一起）和適應性異常控制報告中。

關於適應性異常控制、規則以及它們的模式和狀態的更多資訊，請參閱 Kaspersky Endpoint Security for Windows 說明。

檢視使用適應性異常控制規則執行的偵測清單

要檢視使用適應性異常控制規則執行的偵測清單：

1. 在主控台樹狀目錄中，選取您需要的管理伺服器節點。
2. 選取**智慧培訓狀態中的規則觸發**子資料夾（依預設，這是**進階 → 儲存區**的子資料夾）。

   清單顯示使用適應性異常控制規則執行的偵測的以下資訊：

   - **管理群組**

     裝置所屬管理群組的名稱。

   - **裝置名稱**

     套用規則的用戶端裝置名稱。

   - **名稱**

     套用的規則名稱。

   - **狀態**

     正在排除 — 如果管理員處理該項目並新增其到排除規則清單。該狀態保持到下一次用戶端電腦與管理伺服器同步時，同步之後，該項目從清單消失。

     正在確認 — 如果管理員處理該項目並確認。該狀態保持到下一次用戶端電腦與管理伺服器同步時，同步之後，該項目從清單消失。

     空 — 如果管理員不處理該項目。

   - **規則被觸發的總數**

     一個啟發式規則中的偵測數量，一個處理程序和一個用戶端裝置。該數量由 Kaspersky Endpoint Security 計算。

   - **使用者名稱**

     執行產生偵測之處理程序的用戶端裝置使用者名稱。

   - **來源處理程序路徑**

     處理程序來源路徑，例如，執行操作的處理程序路徑（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

   - **來源處理程序雜湊**

處理程序原始檔案的 SHA256 雜湊（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

- **來源物件路徑**

  啟動處理程序的物件路徑（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

- **來源物件雜湊**

  原始檔案的 SHA256 雜湊（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

- **目的處理程序路徑**

  目的處理程序的路徑（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

- **目的處理程序雜湊**

  目的檔案的 SHA256 雜湊（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

- **目的物件路徑**

  目的物件的路徑（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

- **目的物件雜湊**

  目的檔案的 SHA256 雜湊（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

- **已處理**

  異常被偵測的日期。

要檢視每個資訊元素的內容：

1. 在主控台樹狀目錄中，選取您需要的管理伺服器節點。
2. 選取**智慧培訓狀態中的規則觸發**子資料夾（依預設，這是**進階 → 儲存區**的子資料夾）。
3. 在**智慧培訓狀態中的規則觸發**工作區中，選擇所需的物件。
4. 執行以下操作之一：
   - 在螢幕右側的資訊框點擊**內容**連結。
   - 右擊並在上下文功能表中選取**內容**。

物件內容視窗開啟，顯示關於已選取元素的資訊：

您可以確認或新增到排除適應性異常控制規則偵測清單的任何元素。

要確認元素，

在偵測清單中選取元素並點擊**確認**按鈕。

元素的狀態被變更為正在**正在確認**。

您的確認將被統計到規則使用的統計資訊（對於更多資訊請參閱 Kaspersky Endpoint Security 11 for Windows 說明）。

要新增元素作為排除，

在偵測清單右擊一個元素（或幾個元素）並在上下文功能表中選取**新增到排除**。

新增排除精靈啟動。請按照精靈的步驟進行操作。

如果您拒絕或確認偵測，它將在下一次用戶端裝置與管理伺服器同步時被從偵測清單中排除，且它將不再出現在清單。

從適應性異常控制規則新增排除

新增排除精靈允許您從 Kaspersky Endpoint Security 適應性異常控制規則新增排除。

您可以透過以下三個過程之一啟動精靈。

要透過適應性異常控制節點啟動新增排除精靈：

1. 在主控台樹狀目錄中，選取所需管理伺服器節點。
2. 選取**智慧培訓狀態中的規則觸發**（依預設，這是**進階 → 儲存區**的子資料夾）。
3. 在工作區，在偵測清單中右擊一個元素（或幾個元素）並選取**新增到排除**。
   您可以一次新增 1000 個排除項目。如果您選取更多元素且嘗試新增它們到排除，將顯示錯誤訊息。

   新增排除精靈啟動。

您可以從主控台樹狀目錄的其他節點啟動新增排除精靈：

- 使用管理伺服器主視窗的**事件**頁籤（接著選取**使用者請求**選項和**最近事件**選項）。
- **適應性異常控制規則狀態報告**，**偵測數量**列。

步驟 1：選取應用程式

如果您僅擁有一個 Kaspersky Endpoint Security for Windows 且沒有其他支援適應性異常控制規則的應用程式，該步驟可能被略過。

新增排除精靈顯示其管理外掛程式允許您新增排除到這些應用程式的政策的 Kaspersky 應用程式清單。從該清單選取應用程式並點擊**下一步**以選取要新增排除的政策。

步驟 2：選取政策

精靈顯示 Kaspersky Endpoint Security 政策清單（帶有政策設定檔）。

選取所有政策和您要新增排除的設定檔並點擊**下一步**。

步驟 3：執行政策

政策處理過程中精靈顯示進度條。您可以透過點擊**取消**中斷政策的執行。

繼承的政策無法被更新。如果您沒有權限修改政策，該政策將不被更新。

當所有政策執行後（或者如果您中斷了執行），報告出現。它顯示哪些政策被成功更新（綠色圖示）和哪些政策未被更新（紅色圖示）。

這是精靈的最後一步。點擊**完成**關閉精靈。

隔離區和備份區

安裝在用戶端裝置上的 Kaspersky 防毒應用程式可能在裝置掃描過程中放置檔案到隔離區或備份區。

*隔離區*是一個存放檔案的特殊區域，儲存疑似感染的檔案或偵測時無法解毒的檔案。

*備份區*設定用於儲存在解毒過程中被刪除或被修改的檔案的備份副本。

卡巴斯基安全管理中心會建立一個由裝置上的 Kaspersky 應用程式放入隔離區或備份區的檔案清單。用戶端裝置上的網路代理將隔離區和備份區檔案的資訊傳輸到管理伺服器。您可以使用管理主控台來檢視裝置儲存區中的檔案內容，對這些儲存的檔案執行惡意軟體掃描，並刪除儲存的檔案。檔案狀態圖示敘述在尾碼。

Kaspersky Endpoint Security 支援隔離和備份作業。

卡巴斯基安全管理中心並不會將檔案從儲存區複製到管理伺服器。所有檔案均儲存在裝置儲存區中。您可以僅在帶有防毒應用程式的裝置上復原檔案。

啟用儲存區檔案遠端管理

預設情況下，您無法管理用戶端裝置儲存區中物件。

要啟用用戶端裝置儲存區物件的遠端管理，請執行以下操作：

1. 在主控台樹狀目錄中，選取您要為其啟用儲存區物件進行遠端管理的管理群組。
2. 在群組工作區中，開啟**政策**頁籤。
3. 在**政策**標籤中，為把檔案放在裝置儲存區的安全應用程式選取政策。
4. 在政策設定視窗的**"到管理伺服器的資料傳輸"**設定群組中，選取與您希望為其啟動遠端系統管理的儲存區相應的方塊。

"到管理伺服器的資料傳輸"設定群組在政策內容視窗的位置以及方塊的名稱根據目前使用的安全應用程式而定。

檢視儲存區的檔案內容

要瀏覽隔離區或備份區檔案內容，請執行以下操作：

1. 在主控台樹狀目錄中，依序選取**儲存區**資料夾，**隔離**或**備份**子資料夾。
2. 在**隔離**（**備份**）資料夾的工作區中，選取您希望瀏覽其內容的檔案。
3. 從檔案的上下文功能表中選取**"內容"**。

從儲存區刪除檔案

要將檔案從隔離區或備份區刪除，請執行以下操作：

1. 在主控台樹狀目錄中的**儲存區**資料夾，選取**隔離**或**備份**子資料夾。
2. 在**隔離**（**備份**）資料夾的工作區中，使用 **Shift** 和 **Ctrl** 鍵選取您希望刪除的檔案。
3. 使用下列方式之一刪除檔案：
   - 透過從檔案的上下文功能表中，選取**"刪除"**。
   - 透過在所選檔案的資訊框中，點擊**刪除**（如果要刪除一個檔案，請點擊**刪除**）連結。

   將該檔案放入儲存區的那個安全應用程式將從儲存區中刪除該檔案。

從儲存區還原檔案

若要從隔離區或備份區中還原檔案，請執行以下操作：

1. 在主控台樹狀目錄中，依序選取**儲存區**資料夾，**隔離**或**備份**子資料夾。
2. 在**隔離**（**備份**）資料夾的工作區中，使用 **Shift** 和 **Ctrl** 鍵選取您希望還原的檔案。
3. 以下列方式之一開始還原檔案：
   - 透過從檔案的上下文功能表中，選取**"還原"**。
   - 透過在所選檔案的資訊框中，點擊**"還原"**連結。

   將該檔案放入儲存區的那個安全應用程式將把檔案還原至其原始資料夾中。

將儲存區中的檔案儲存到磁碟

卡巴斯基安全管理中心允許您將那些由安全應用程式放入用戶端裝置隔離區或備份區的檔案備份儲存至磁碟。這些檔案將複製到安裝卡巴斯基安全管理中心的裝置上的指定位置中。

要將隔離區或備份區中的檔案備份儲存到硬碟磁碟機，請執行以下操作：

1. 在主控台樹狀目錄中，依序選取**儲存區**資料夾，**隔離**或**備份**子資料夾。
2. 在**隔離**（**備份**）資料夾的工作區中，選取希望複製到硬碟的檔案。
3. 使用下列方式之一來複製檔案：
   - 透過從檔案的上下文功能表中，選取**"儲存到磁碟"**。
   - 透過在所選檔案的資訊框中，點擊**儲存到磁碟**連結。

將該檔案放入用戶端裝置隔離區的那個安全應用程式將把檔案副本儲存至指定資料夾。

掃描隔離區中的檔案

要掃描隔離區檔案，請執行以下操作：

1. 在主控台樹狀目錄中，依序選取**儲存區**資料夾，**隔離**子資料夾。
2. 在**隔離**資料夾的工作區中，使用 **Shift** 和 **Ctrl** 鍵選取您要掃描的檔案。
3. 以下列方式之一開始檔案掃描：
   - 透過從檔案的上下文功能表中，選取**"掃描"**。
   - 透過在所選檔案的資訊框中，點擊**掃描**連結。

應用程式會為那些將所選檔案移動至用戶端裝置隔離區的安全應用程式啟動自訂掃描工作。

主動威脅

用戶端裝置找到未處理的檔案資訊儲存在**儲存區**資料夾的**活動威脅**子資料夾中。

延遲處理和清除在請求時和指定事件發生時被安全應用程式執行。您可以為這些檔案進行後續處理。

解毒未處理檔案

要開始解毒未處理檔案：

1. 在主控台樹狀目錄中的**儲存區**資料夾，選取**活動威脅**子資料夾。
2. 在**活動威脅**資料夾的工作區中，選取要解毒的檔案。
3. 使用下列方式之一開始為檔案解毒：
   - 透過從檔案的上下文功能表中，選取**"解毒"**。
   - 在所選檔案的資訊框中，點擊**解毒**連結。

然後程式將執行檔案解毒的操作。

如果檔案被解毒，安裝在用戶端裝置上的安全應用程式將其還原到原始資料夾。該檔案的相關記錄將從**活動威脅**資料夾的清單中刪除。如果檔案無法被解毒，安全應用程式將其從裝置刪除。該檔案的相關記錄將從**活動威脅**資料夾的清單中刪除。

檔案解讀與刪除功能可能會因安裝的安全應用程式和其版本與設定而異。

將未處理的檔案儲存到磁碟

卡巴斯基安全管理中心允許您將用戶端裝置上發現的未處理的檔案的備份儲存至磁碟。這些檔案將複製到安裝卡巴斯基安全管理中心的裝置上的指定位置中。

您可以在以下情況下儲存檔案副本：

- 檔案在解毒期間被刪除或修改，其副本儲存在受管理裝置的 Kaspersky Endpoint Security for Windows 儲存 中。
- 在 Kaspersky Endpoint Security 政策中為**偵測到威脅時的操作** 參數選擇**僅記錄**選項（**關鍵威脅防護 → 檔案威脅防護**）。

要將未處理的檔案備份儲存至磁碟，請執行以下操作：

1. 在主控台樹狀目錄中的**儲存區**資料夾，選取**活動威脅**子資料夾。
2. 在**活動威脅**資料夾中，選取要複製到硬碟的檔案。
3. 使用下列方式之一來複製檔案：
   - 透過從檔案的上下文功能表中，選取**"儲存到磁碟"**。
   - 透過在所選檔案的資訊框中，點擊**儲存到磁碟**連結。

安裝在發現未處理檔案的用戶端裝置上的安全應用程式將一份檔案副本儲存至指定資料夾。

從「主動威脅」資料夾中刪除檔案

*要從**活動威脅**資料夾中刪除檔案，請執行以下操作：*

1. 在主控台樹狀目錄中的**儲存區**資料夾，選取**活動威脅**子資料夾。
2. 在**活動威脅**資料夾的工作區中，使用 **Shift** 和 **Ctrl** 鍵選取您要刪除的檔案。
3. 使用下列方式之一刪除檔案：
   - 透過從檔案的上下文功能表中，選取**"刪除"**。
   - 透過在所選檔案的資訊框中，點擊**刪除**（如果要刪除一個檔案，請點擊**刪除**）連結。

管理伺服器將進行從儲存區的用戶端電腦刪除檔案的動作。檔案的相關記錄將會從**活動威脅**資料夾的清單中刪除。

卡巴斯基安全網路 (KSN)

該區域敘述如何使用卡巴斯基安全網路 (KSN) 的線上服務基礎架構。該區域提供了關於 KSN 的詳細敘述，介紹了如何啟用 KSN，設定對 KSN 的存取，並檢視 KSN 代理伺服器的使用統計。

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

關於 KSN

卡巴斯基安全網路 (KSN) 是一種線上服務組織結構，可提供對 Kaspersky 網路知識庫的存取，其中包含與檔案信譽、網路資源和軟體相關的資訊。使用卡巴斯基安全網路中的資料可確保在遇到未知威脅時 Kaspersky 程式能夠做出更快速的回應，提高某些防護元件的效能可降低誤報的風險。KSN 允許您使用 Kaspersky 的信譽資料庫檢索有關安裝在受管理裝置上的應用程式資訊。

卡巴斯基安全管理中心支援以下 KSN 基礎架構解決方案：

- *全球 KSN* 是一種允許您與卡巴斯基安全網路交換資訊的解決方案。只要加入 KSN，即表示您同意以自動模式將透過卡巴斯基安全管理中心管理的用戶端裝置上安裝的 Kaspersky 應用程式的相關操作資訊傳送到 Kaspersky。依照目前 KSN 存取設定傳送資訊。卡巴斯基分析師會另外分析收到的資訊，並將其包含在卡巴斯基安全網路的信譽和統計資料庫中。卡巴斯基安全管理中心預設使用此解決方案。

- *私有 KSN* 是一種解決方案，可讓已安裝卡巴斯基應用程式的裝置使用者存取卡巴斯基安全網路的信譽資料庫和其他統計資料，而不必從自己的電腦傳送資料給 KSN。卡巴斯基私人安全網路（私有 KSN）專門用於由於以下原因無法參與卡巴斯基安全網路的企業客戶：

  - 使用者裝置未連線到網際網路。

  - 法律禁止或企業安全政策限制傳輸任何資料到國家/地區以外或企業區域網路以外。

  您可以在管理伺服器內容視窗的**KSN 代理設定**區段中，設定卡巴斯基私人安全網路的存取設定。

在執行快速啟動精靈時，應用程式會提示您加入 KSN。您可以在使用應用程式的任何時間啟用或者停止 KSN。

啟用 KSN 時，應根據閱讀與接受的 KSN 聲明啟用 KSN。如果 KSN 聲明已更新，則在更新或升級管理伺服器時會顯示給您。您可以接受更新的 KSN 聲明，也可以拒絕。如果您拒絕了它，那麼您將按照之前接受的 KSN 聲明的先前版本繼續使用 KSN。

啟用 KSN 後，卡巴斯基安全管理中心會檢查 KSN 伺服器是否可存取。如果無法使用系統 DNS 存取伺服器，則應用程式使用公用 DNS 伺服器。這是為了確保維護受管理裝置的安全級別。

管理伺服器管理的用戶端裝置透過 KSN 代理伺服器與 KSN 互動。KSN 代理伺服器提供以下功能：

- 即使無法直接連線網際網路，用戶端裝置也可向 KSN 傳送請求以及向 KSN 傳送資訊。

- KSN 代理可暫存已處理的資料，進而減少對外頻寬消耗以及用戶端裝置等待 KSN 回覆而花費的時間。

您可以在管理伺服器內容視窗的**KSN 代理設定**區域中設定 KSN 代理伺服器。

設定到卡巴斯基安全網路的存取

您可以在管理伺服器和發佈點上設定到卡巴斯基安全網路 (KSN) 的存取。

要設定管理伺服器到卡巴斯基安全網路 (KSN) 的存取：

1. 在主控台樹狀目錄中，選取要為其設定對 KSN 存取的管理伺服器。
2. 在管理伺服器的上下文功能表中，選取**內容**。
3. 在管理伺服器內容視窗中的**區域**區域，選取**KSN 代理 → KSN 代理設定**選項。
4. 在工作區，啟用**使用管理伺服器作為代理伺服器**選項以使用 KSN 代理服務。

   資料被從用戶端裝置傳送到 KSN，與在這些用戶端裝置上活動的 Kaspersky Endpoint Security 政策一致。如果清除此方塊，資料不會透過卡巴斯基安全管理中心從管理伺服器以及用戶端裝置傳送到 KSN。但是，用戶端裝置能夠根據其設定直接將資料傳送到 KSN（繞過卡巴斯基安全管理中心）。Kaspersky Endpoint Security for Windows 政策會在用戶端裝置上啟用，判定哪些資料要從哪些裝置傳送至 KSN（透過旁路卡巴斯基安全管理中心）。

5. 停用**我同意使用卡巴斯基安全網路**選項。

如果啟用了此選項，用戶端裝置將傳送修補程式安裝結果到 Kaspersky。啟用此選項時，請確保閱讀並接受 KSN 聲明的條款。

如果您正使用私有 KSN，啟用**設定私有 KSN**選項並點擊**選取 KSN 代理設定檔**按鈕以下載私有 KSN 設定（帶有 pkcs7 和 pem 副檔名的檔案）。下載完設定之後，介面會顯示提供商的名稱和聯絡人，以及私有 KSN 設定檔的建立日期。

當您啟用私有 KSN，請注意設定用來直接傳送 KSN 要求至雲端 KSN 的分佈點。已安裝網路代理版本 11（或更早版本）的分佈點會繼續傳送 KSN 要求至雲端 KSN。若要重新設定分佈點來傳送 KSN 要求至私有 KSN，請為每個分佈點啟用**轉發 KSN 請求到管理伺服器**選項。您可在發佈點內容或網路代理政策中啟用此選項。

當您選取**設定私有 KSN** 核取方塊時，將出現關於私有 KSN 詳情的訊息。

以下 Kaspersky 應用程式支援私有 KSN：

- 卡巴斯基安全管理中心
- Kaspersky Endpoint Security for Windows
- Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2
- Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent

如果您在卡巴斯基安全管理中心啟用**設定私有 KSN** 選項，這些應用程式接收支援私有 KSN 的相關資訊。在應用程式設定視窗，在**進階威脅防護**區域的**卡巴斯基安全網路**子區域中，**KSN 提供者：私有 KSN** 被顯示。否則，**KSN 提供者：全域 KSN** 被顯示。

如果您使用的應用程式版本早於 Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 或早於 Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent，在您執行私人 KSN 時，我們建議您使用未啟用私人 KSN 使用的從屬管理伺服器。

卡巴斯基安全管理中心不傳送任何統計資料到卡巴斯基安全網路，如果在管理伺服器內容視窗的 **KSN 代理 → KSN 代理設定**區域設定了私有 KSN。

若您已在管理伺服器內容中設定代理伺服器設定，但您的網路架構要求您直接使用私有 KSN，請啟用**當連線到私有 KSN 時略過代理伺服器設定**選項。否則，從受管理應用程式的請求無法到達私有 KSN。

6. 設定管理伺服器到 KSN 代理服務的連線：

- 在**連線設定**下的**TCP 連接埠**中，指定用於連線到 KSN 代理的 TCP 埠號。連線到 KSN 代理伺服器的預設連接埠是 13111。
- 如果您要讓管理伺服器透過 UDP 連接埠連線到 KSN 代理，啟用**使用 UDP 連接埠**選項，並在**UDP 連接埠**欄位中指定埠號。預設下，會停用此選項，並使用 TCP 連接埠。若啟用此選項，則 UDP 埠號 15111 預設會用來連線到 KSN 代理伺服器。
- 如果希望管理伺服器透過 HTTPS 連接埠連線到 KSN 代理伺服器，請啟用**透過連接埠使用 HTTPS**選項，並指定連接埠號。預設下，會停用此選項，並使用 TCP 連接埠。若啟用此選項，則 HTTPS 埠號 17111 預設會用來連線到 KSN 代理伺服器。

7. 啟用**透過主管理伺服器將從屬管理伺服器連線到 KSN**選項。

   如果啟用此選項，任何層級的從屬管理伺服器將使用主管理伺服器作為 KSN 代理伺服器。如果停用此選項，從屬管理伺服器會自己連線到 KSN。該情況下，受管理裝置使用從屬管理伺服器作為 KSN 代理伺服器。

   如果從屬管理伺服器內容中的 **KSN 代理設定**區域的右側面板中有**使用管理伺服器作為代理伺服器**核取方塊被選中，則從屬管理伺服器使用主管理伺服器作為代理伺服器。

8. 點擊**確定**。

KSN 存取設定將被儲存。

您也可以設定發佈點存取 KSN，例如，如果您想降低管理伺服器負載。作為 KSN 代理伺服器的發佈點從受管理裝置直接傳送 KSN 請求到 Kaspersky，不使用管理伺服器。

要設定發佈點到卡巴斯基安全網路 (KSN) 的存取：

1. 確保發佈點是手動分配。
2. 在主控台樹狀目錄中，選取**管理伺服器**節點。
3. 在管理伺服器的上下文功能表中，選取**內容**。
4. 在管理伺服器內容視窗，選取**發佈點**區域。
5. 在清單中選取發佈點並按一下**內容**按鈕來開啟內容視窗。
6. 在發佈點內容視窗，在 **KSN 代理**區域，選取**透過網際網路直接存取 KSN 雲端 / 私有 KSN**。
7. 點擊**"確定"**。

該發佈點將作為 KSN 代理伺服器。

啟用和停用 KSN

要啟用 KSN：

1. 在主控台樹狀目錄中，選取您希望為其啟用 KSN 的管理伺服器。
2. 在管理伺服器的上下文功能表中，選取**內容**。
3. 在管理伺服器內容視窗中的**KSN 代理**區域，選取**KSN 代理設定**子區域。
4. 選取**使用管理伺服器作為代理伺服器**。

   KSN 代理伺服器將被啟用。

5. 選擇**我同意使用卡巴斯基安全網路**核取方塊。

   KSN 將被啟用。

   如果選取了此方塊，用戶端裝置將傳送修補程式安裝結果到 Kaspersky。選定此方塊時，您應閱讀並接受 KSN 聲明的條款。

6. 點擊**確定**。

要停用 KSN：

1. 在主控台樹狀目錄中，選取您希望為其啟用 KSN 的管理伺服器。
2. 在管理伺服器的上下文功能表中，選取**內容**。
3. 在管理伺服器內容視窗中的**KSN 代理**區域，選取**KSN 代理設定**子區域。
4. 不選取**使用管理伺服器作為代理伺服器**核取方塊，停用 KSN 代理服務，或不選取**我同意使用卡巴斯基安全網路**核取方塊。

   如果清除選取此方塊，用戶端裝置將不傳送修補程式安裝結果到 Kaspersky。

   如果您使用私有 KSN，請不選取**設定私有 KSN**方塊。

   KSN 將被停用。
5. 點擊**確定**。

檢視接受的 KSN 聲明

啟用卡巴斯基安全網路 (KSN) 時，必須閱讀並接受 KSN 聲明。您可以隨時檢視已接受的 KSN 聲明。

若要檢視已接受的 KSN 聲明：

1. 在主控台樹狀目錄中，選取您希望為其啟用 KSN 的管理伺服器。
2. 在管理伺服器的上下文功能表中，選取**內容**。
3. 在管理伺服器內容視窗中的**KSN 代理**區域，選取**KSN 代理設定**子區域。
4. 透過點擊**檢視接受的 KSN 聲明**連結。

   在開啟的視窗中，您可以查看接受的 KSN 聲明的文字。

檢視 KSN 代理伺服器統計資訊

*KSN 代理伺服器*可確保卡巴斯基安全網路基礎架構和管理伺服器所管理的用戶端裝置之間的互動。

使用 KSN 代理伺服器提供您以下功能：

- 即使無法直接連線網際網路，用戶端裝置也可向 KSN 傳送請求以及向 KSN 傳送資訊。
- KSN 代理可暫存已處理的資料，進而減少對外頻寬消耗以及用戶端裝置等待 KSN 回覆而花費的時間。

在管理伺服器內容視窗，你可以配置 KSN 代理伺服器並檢視 KSN 代理伺服器使用統計資訊。

要檢視 KSN 代理伺服器統計:

1. 在主控台樹狀目錄中，選取您需要檢視 KSN 統計的管理伺服器。
2. 在管理伺服器的上下文功能表中，選取**內容**。

3. 在管理伺服器內容視窗中的**KSN 代理**區域，選取**KSN 代理統計資訊**子區域。

   此部分顯示 KSN 代理伺服器運作的實際統計資料（快取記錄、快取中處理的套件和收到的套件數量）。此外，如果管理伺服器連線到 KSN，則會顯示相應的資訊性訊息。

   如果必要，執行這些附加操作：

   - 點擊**重新整理**以更新 KSN 代理伺服器使用統計資訊。
   - 點擊**匯出至檔案**按鈕儲存統計資訊到 CSV 檔案。
   - 點擊**檢查 KSN 連線**按鈕以檢查是否管理伺服器目前已連線到 KSN。

4. 點擊**確定**按鈕以關閉管理伺服器內容視窗。

接受更新的 KSN 聲明

啟用 KSN 時，應根據閱讀與接受的 KSN 聲明啟用 KSN。如果 KSN 聲明已更新，則在更新或升級管理伺服器時會顯示給您。您可以接受更新的 KSN 聲明，也可以拒絕。如果您拒絕了它，那麼您將按照之前接受的 KSN 聲明的版本繼續使用 KSN。

更新或升級管理伺服器後，將自動顯示更新的 KSN 聲明。如果您拒絕更新的 KSN 聲明，則以後仍然可以查看並接受它。

要檢視然後接受或拒絕更新的 KSN 聲明，請執行以下操作：

1. 在主控台樹狀目錄中，選取**管理伺服器**節點。
2. 在**監控**頁籤的**監控**區段中，點擊**接受的卡巴斯基安全網路聲明已過時**連結。

   KSN 聲明視窗隨即開啟。
3. 仔細閱讀 KSN 聲明，然後做出決定。如果您接受更新的 KSN 聲明，請點擊**我接受產品授權協議的條款**按鈕。如果您拒絕更新的 KSN 聲明，請點擊**取消**按鈕。

根據您的選擇，KSN 會按照目前或更新的 KSN 聲明條款繼續有效。您可以隨時在管理伺服器屬性中檢視已接受的 KSN 聲明文字。

使用卡巴斯基安全網路獲得增強防護

Kaspersky 透過卡巴斯基安全網路為使用者提供更進一步的防護。此延伸層級的安全防護，主要是讓您免於 APT 及零時差威脅的攻擊。結合雲端技術和 Kaspersky 專業的病毒分析，使得 Kaspersky Endpoint Security 防護能即時應對各式複雜的網路威脅。

您可以在 Kaspersky 網站上獲得有關 Kaspersky Endpoint Security 防護強化的詳細資訊。

檢查發佈點是否作為 KSN 代理伺服器運作

在分配作為發佈點運作的受管理裝置上，可以啟用 KSN 代理伺服器。當 ksnproxy 服務在裝置上執行時，受管理裝置會作為 KSN 代理伺服器運作。您可以在本機裝置上檢查、開啟或關閉此服務。

您可以將基於 Windows 或基於 Linux 的裝置分配為發佈點。檢查發佈點的方法取決於該發佈點的作業系統。

若要檢查基於 Windows 的發佈點是否作為 KSN 代理伺服器運作，請執行以下操作：

1. 在發佈點裝置上的 Windows 系統中，開啟**服務**（**所有程序 → 管理工具 → 服務**）。
2. 在服務清單，檢查 ksnproxy 服務是否正在執行。

   如果 ksnproxy 服務正在執行，則裝置上的網路代理會加入卡巴斯基安全網路，並作為發佈點範圍內所管理裝置的 KSN 代理伺服器運作。

如果您想，您可以關閉 ksnproxy 服務。在這種情況下，發佈點上的網路代理停止參與卡巴斯基安全網路。該需要本機管理員權限。

若要檢查基於 Linux 的發佈點是否作為 KSN 代理伺服器運作，請執行以下操作：

1. 在發佈點裝置上，顯示正在執行的處理程序清單。
2. 在正在執行的處理程序清單中，檢查 `/opt/kaspersky/ksc64/sbin/ksnproxy` 處理程序是否正在執行。

如果 `/opt/kaspersky/ksc64/sbin/ksnproxy` 處理程序正在執行，則裝置上的網路代理會加入卡巴斯基安全網路，並作為發佈點範圍內所管理裝置的 KSN 代理伺服器運作。

在線上說明和離線說明之間切換

如果您沒有網際網路存取權限，則可以使用"離線說明"。

若要在線上說明和離線說明之間切換：

1. 在卡巴斯基安全管理中心主視窗，在主控台樹狀目錄選取**卡巴斯基安全管理中心 14.2**。
2. 點擊**全域介面設定**連結。

   設定視窗隨即開啟。
3. 在設定視窗中，點擊**使用離線說明**。
4. 點擊"**確定**"。

   裝置被套用並儲存。如果需要，您可以隨時更改設定，並隨時開始使用線上說明。

匯出到 SIEM 系統的事件

該部分解釋了如何匯出卡巴斯基安全管理中心註冊的事件到外部安全資訊和事件管理 (SIEM) 系統。

設定事件匯出到 SIEM 系統

卡巴斯基安全管理中心允許透過以下方法之一進行配置：匯出到使用 Syslog 格式的任何 SIEM 系統，匯出到使用 LEEF 和 CEF 格式的 QRadar、Splunk、ArcSight SIEM 系統或直接從卡巴斯基安全管理中心將事件匯出到 SIEM 系統資料庫。完成此場景後，管理伺服器會自動將事件傳送到 SIEM 系統。

先決條件

在卡巴斯基安全管理中心中開始配置匯出事件之前：

- 深入了解事件匯出的方法。
- 確保您有系統設定值。

> 您可以按任何順序執行此場景的步驟。

將事件匯出到 SIEM 系統的過程包括以下步驟：

- **配置 SIEM 系統以接收來自卡巴斯基安全管理中心的事件**

  說明：配置在 SIEM 系統中的事件匯出

- **選取要匯出到 SIEM 系統的事件：**

  說明：

  - 管理主控台：將 Kaspersky 應用程式的事件標記為以 Syslog 格式匯出、將一般事件標記為以 Syslog 格式匯出
  - 卡巴斯基安全管理中心網頁主控台：將 Kaspersky 應用程式的事件標記為以 Syslog 格式匯出、將一般事件標記為以 Syslog 格式匯出

- **使用以下方法之一配置事件到 SIEM 系統的匯出：**

  - 使用 TCP/IP、UDP 或 TLS over TCP 通訊協定。

    說明：

    - 管理主控台：配置匯出事件到 SIEM 系統
    - 卡巴斯基安全管理中心網頁主控台：配置匯出事件到 SIEM 系統

  - 直接從卡巴斯基安全管理中心資料庫匯出事件（卡巴斯基安全管理中心 資料庫中會提供一組公用視圖；您可以在 klakdb.chm 文件找到這些公用視圖的說明）。

結果

如果您選取了要匯出的事件，配置事件匯出到 SIEM 系統後，您可以查看匯出結果。

在您開始之前

當設定在卡巴斯基安全管理中心管理主控台中自動匯出事件時，您必須指定一些 SIEM 系統設定。建議您提前檢查這些設定，以便準備設定卡巴斯基安全管理中心。

要成功配置自動傳送事件到 SIEM 系統，您必須知道以下設定：

- **SIEM 系統伺服器位址**

  安裝了目前使用的 SIEM 系統的伺服器的 IP 位址。在您的 SIEM 系統設定中檢查此值。

- **SIEM 系統伺服器連接埠**

  用於建立卡巴斯基安全管理中心和您的 SIEM 系統伺服器之間連線的埠號。您在卡巴斯基安全管理中心設定中和您 SIEM 系統的接收設定中指定該值。

- **協定**

  用於從卡巴斯基安全管理中心傳輸訊息到您的 SIEM 系統的協定。您在卡巴斯基安全管理中心設定中和您 SIEM 系統的接收設定中指定該值。

卡巴斯基安全管理中心中的事件

卡巴斯基安全管理中心允許您接收受管理裝置上安裝的管理伺服器和其他 Kaspersky 應用程式的操作事件資訊。事件資訊儲存在管理伺服器資料庫。您可以匯出這些資訊到外部 SIEM 系統。匯出事件資訊到外部 SIEM 系統，可使 SIEM 系統管理員快速回應發生在受管理裝置或管理群組上的安全系統事件。

事件類型

在卡巴斯基安全管理中心中有以下事件類型：

- 一般事件。這些事件會發生在所有受管理的 Kaspersky 應用程式中。一般事件指的像是病毒爆發。一般事件已嚴格定義語法與語意。例如，一般事件會用於報告和儀表板。
- 受管理的 Kaspersky 應用程式特定的事件。每個 Kaspersky 應用程式都擁有自己的事件集。

事件來源

事件可以由以下應用程式產生：

- 卡巴斯基安全管理中心元件：
  - 管理伺服器
  - 網路代理
  - iOS MDM 伺服器
  - Exchange 行動裝置伺服器
- 受管卡巴斯基應用程式

  有關卡巴斯基受管理應用程式產生的事件的詳細資訊，請參閱相應應用程式的文件。

您可以在應用程式政策的**事件配置**頁簽中檢視可以由應用程式生產的事件的完整清單。對於管理伺服器，您還可以在管理伺服器屬性中檢視事件清單。

事件的重要等級

每個事件都有自己的重要等級。取決於發生的條件，一個事件可以被分配不同的重要等級。四個事件重要等級如下：

- *緊急事件*指示發生了可能導致資料遺失、作業系統異常或嚴重錯誤的嚴重問題。
- *功能失效*指示在應用程式操作中或執行過程中發生了嚴重問題、錯誤或功能異常。
- *警告*是不緊急的事件，但是也指示了今後可能發生的潛在問題。如果在事件發生後應用程式可以被還原而不遺失資料或功能，則這些事件是警告等級。
- *資訊*事件用於提示成功完成操作、應用程式的正常功能或完成了某過程。

每個事件都有一個儲存期限，在這時間內您可以在卡巴斯基安全管理中心中檢視或修改。一些事件預設下不儲存在管理伺服器資料庫，因為它們的儲存期限是零。僅可以在管理伺服器資料庫中儲存至少一天的事件可以被匯出到外部系統。

關於事件匯出

您可以將事件匯出用在處理組織和技術級別的安全問題的中心系統中，提供安全監控服務，以及從不同解決方案合併資訊。即是提供對網路硬體和應用程式生成的安全警告的即時分析的 SIEM 系統，或者安全操作中心 (SOCs)。

這些系統可以從許多來源接收資料，包括網路、安全、伺服器、資料庫和應用程式。SIEM 系統也提供功能以集成監控的資料，以便說明您避免遺失關鍵事件。而且，系統執行相關事件和警告的自動分析以通知管理員安全問題。警告可以透過儀表板實現，或可以透過協力廠商管道傳送，例如郵件。

從卡巴斯基安全管理中心匯出事件到外部 SIEM 系統的處理程序設計兩部分：事件傳送者 — 卡巴斯基安全管理中心和事件接收者 — SIEM 系統。要成功匯出事件，您必須在您的 SIEM 系統和卡巴斯基安全管理中心中對此進行配置。您可以先設定任意一端。您可以設定在卡巴斯基安全管理中心中的事件傳輸，然後設定 SIEM 系統對事件的接收，或者相反。

從卡巴斯基安全管理中心傳送事件的方法

有三種方法從卡巴斯基安全管理中心傳送事件到外部系統：

- 透過 Syslog 協定傳送事件到任意 SIEM 系統

  使用 Syslog 協定，您可以轉發發生在卡巴斯基安全管理中心管理伺服器上和受管理裝置上安裝的 Kaspersky 應用程式中的任意事件。Syslog 協定是標準訊息記錄協定。您可以用它匯出事件到任何 SIEM 系統。

  為此，您需要標記要轉送到 SIEM 系統的事件。您可在管理主控台或卡巴斯基安全管理中心 網頁主控台中標記事件。只有標記的事件才會被轉送到 SIEM 系統。如果您沒有標記任何內容，則不會轉送任何事件。

- 透過 CEF 和 LEEF 通訊協定傳送事件到 QRadar、Splunk 和 ArcSight 系統

  您可使用 CEF 和 LEEF 協定匯出一般事件。當透過 CEF 和 LEEF 協定匯出事件時，您不必能夠選取指定事件以匯出。相反，所有一般事件都被匯出。若要將卡巴斯基安全管理中心事件轉換為 CEF 和 LEEF 格式的事件，您需要使用siem_conversion_rules.xml 檔案。此檔案包含卡巴斯基安全管理中心事件屬性清單以及 CEF 和 LEEF 格式的事件的相應屬性。此外，siem_conversion_rules.xml 檔案包含用於產生與事件對應的訊息的規則。該檔案包含在卡巴斯基安全管理中心分發套件中。

  不同於 Syslog 協定，CEF 和 LEEF 協定不通用。CEF 和 LEEF 為 SIEM 系統所設計（QRadar、Splunk 和 ArcSight）。因此，當您選取透過這些協定匯出事件時，您使用 SIEM 系統所需解析器。

- 直接從卡巴斯基安全管理中心資料庫到 SIEM 系統

  以該方法匯出事件可以用於透過使用 SQL 查詢直接從資料庫公共視圖接收事件。查詢結果被儲存到 XML 檔案，可以用於外部系統的輸入資料。僅僅公共視圖中的事件可以被直接從資料庫中匯出。

透過 SIEM 系統接收事件

SIEM 系統必須接收和正確解析來自卡巴斯基安全管理中心的事件。因為這些目的，您必須正確設定 SIEM 系統。設定取決於特定的 SIEM 系統。然而，有一些設定所有 SIEM 系統的通用步驟，例如設定接收器和解析器。

配置在 SIEM 系統中的事件匯出

從卡巴斯基安全管理中心匯出事件到外部 SIEM 系統的處理程序設計兩部分：事件傳送者 — 卡巴斯基安全管理中心和事件接收者 — SIEM 系統。您必須在您的 SIEM 系統和卡巴斯基安全管理中心管理主控台中設定事件匯出。

您在 SIEM 系統中指定的設定取決於您使用的系統。通常，對於所有 SIEM 系統，您必須設定接收器和訊息解析器（可選）以解析接收的事件。

設定接收器

為了接收卡巴斯基安全管理中心傳送的事件，您必須在您的 SIEM 系統中設定接收器。通常，必須在 SIEM 系統指定以下設定：

- **匯出協定或輸入類型**

  它是訊息傳輸協定，TCP/IP 或 UDP。該協定必須與您在卡巴斯基安全管理中心中指定的協定相同。

- **連接埠**

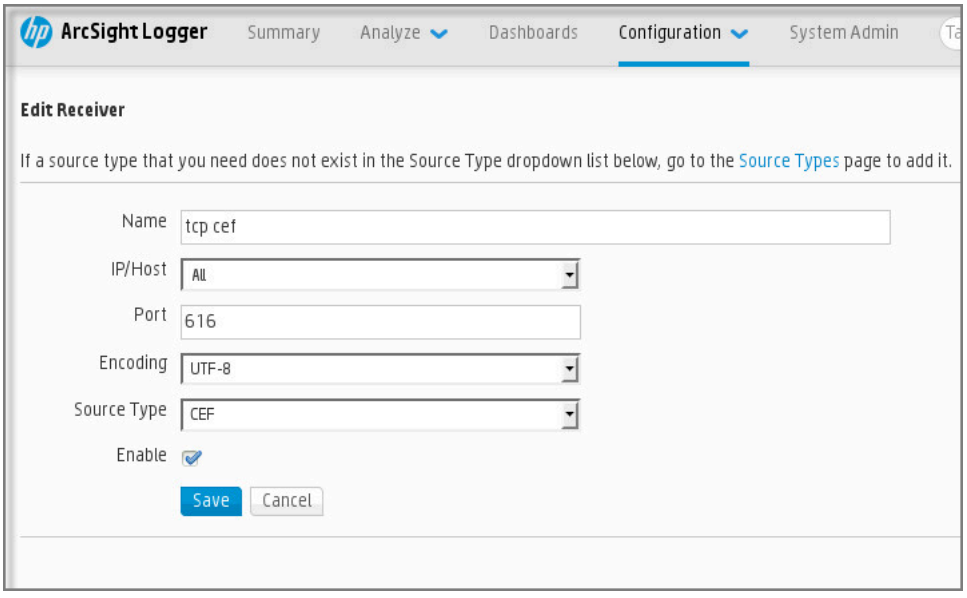
  連線到卡巴斯基安全管理中心的埠號。該連接埠必須與您在卡巴斯基安全管理中心中指定的連接埠相同。

- **訊息協定或來源類型**

  用於匯出事件到 SIEM 系統的協定。它可以是標準協定之一：Syslog、CEF 或 LEEF。SIEM 系統依據您指定的協定選取訊息解析器。

依據所使用的 SIEM 系統，您可能需要指定一些附加接收器設定。

下圖顯示 ArcSight 的接收器設定截圖。



ArcSight 的接收器設定

訊息解析器

匯出的事件作為訊息被傳遞到 SIEM 系統。這些訊息必須正確解析，以便事件資訊可以被 SIEM 系統使用。訊息解析器是 SIEM 系統的一部分，它們用於拆分訊息屬性到相關欄位，例如事件 ID、嚴重等級、敘述、參數。這將啟用 SIEM 系統以處理從卡巴斯基安全管理中心接收的事件，以便它們可以被儲存在 SIEM 系統資料庫。

標記事件，將其以 Syslog 格式匯出到 SIEM 系統

在啟用自動匯出事件後，您必須選取將被匯出到外部 SIEM 系統的事件。

您可以根據以下條件之一，設定以 Syslog 格式將事件匯出到外部系統：

- 標記一般事件。如果您在政策、事件設定或在管理伺服器設定中，標記要匯出的事件，SIEM 系統將接收由特定政策管理的所有應用程式上發生的所選事件。如果匯出的事件在政策中被選中，您將不能為由該政策管理的個別應用程式重新定義所選事件。

- 標記受管理應用程式的事件。如果您在受管理裝置上為安裝的受管理應用程式標記要匯出的事件，SIEM 系統將僅接收發生在該應用程式中的事件。

關於標記事件並將其以 Syslog 格式匯出到 SIEM 系統

在啟用自動匯出事件後，您必須選取將被匯出到外部 SIEM 系統的事件。

您可以根據以下條件之一，設定以 Syslog 格式將事件匯出到外部系統：

- 標記一般事件。如果您在政策、事件設定或在管理伺服器設定中，標記要匯出的事件，SIEM 系統將接收由特定政策管理的所有應用程式上發生的所選事件。如果匯出的事件在政策中被選中，您將不能為由該政策管理的個別應用程式重新定義所選事件。

- 標記受管理應用程式的事件。如果您在受管理裝置上為安裝的受管理應用程式標記要匯出的事件，SIEM 系統將僅接收發生在該應用程式中的事件。

將 Kaspersky 應用程式的事件標記為以 Syslog 格式匯出

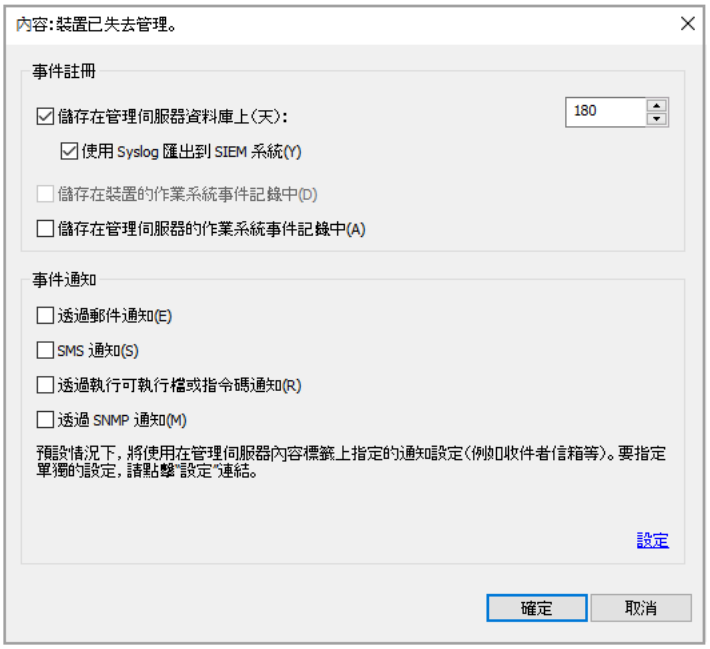
如果您要匯出發生在受管理裝置上安裝的個別受管理應用程式中的事件，選取事件以為應用程式匯出。如果先前匯出的事件在政策中標記，您將不能為由該政策管理的個別應用程式重新定義標記的事件。

若要為個別受管理應用程式標記要匯出的事件：

1. 在卡巴斯基安全管理中心主控台樹狀目錄，選取**受管理裝置**節點並轉到**裝置**頁籤。
2. 右鍵開啟相關裝置的上下文功能表並選取**內容**。
3. 在開啟的裝置內容視窗中，選取**應用程式**區域。
4. 在顯示的應用程式清單中，選取要匯出事件的應用程式，並點擊**內容**按鈕。
5. 在應用程式內容視窗中，選取**事件配置**區域。
6. 在顯示的事件清單中，選取一個或幾個需要匯出到 SIEM 系統的事件，並點擊**內容**按鈕。

7. 在出現的事件屬性視窗中，選取**使用 Syslog 匯出到 SIEM 系統**核取方塊，將標記選定的事件以 Syslog 格式匯出。清除**使用 Syslog 匯出到 SIEM 系統**核取方塊，以取消標記要以 Syslog 格式匯出的選定事件。

如果事件內容在政策中定義，該視窗的欄位無法被編輯。



"事件內容"視窗

8. 點擊**確定**儲存變更。

9. 在應用程式內容視窗和裝置內容視窗中點擊**確定**。

標記的事件將透過 Syslog 格式被傳送到 SIEM 系統。您取消選取的事件 **使用 Syslog 匯出到 SIEM 系統** 核取方塊，不會匯出到 SIEM 系統。匯出將在您啟用自動匯出和選取事件以匯出後立即開始。設定 SIEM 系統以確保它接收來自卡巴斯基安全管理中心的事件。

標記一般事件，將其以 Syslog 格式匯出

如果您要匯出發生在被特定政策管理的所有應用程式中的事件，標記事件以在政策中匯出。此種情況下，您無法為個別受管理應用程式標記事件。

標記一般事件以匯出到 SIEM 系統：

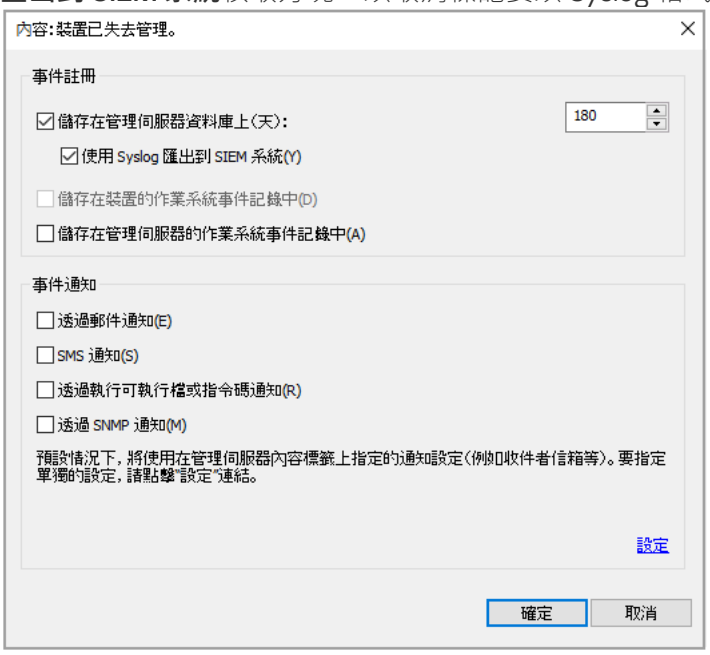
1. 在卡巴斯基安全管理中心主控台樹狀目錄中，選取**政策**節點。

2. 右鍵開啟相關政策的上下文功能表並選取**內容**。

3. 在開啟的工作內容視窗中，選取**事件配置**區域。

4. 在顯示的事件清單中，選取一個或幾個需要匯出到 SIEM 系統的事件，並點擊**內容**按鈕。
   如果您需要選取所有事件，點擊**全選**按鈕。

5. 在出現的事件屬性視窗中，選取**使用 Syslog 匯出到 SIEM 系統**核取方塊，將標記選定的事件以 Syslog 格式匯出。取消選取**使用 Syslog 匯出到 SIEM 系統**核取方塊，以取消標記要以 Syslog 格式匯出的選定事件。



管理伺服器事件內容視窗

6. 點擊**確定**儲存變更。

7. 在政策內容視窗，點擊**確定**。

標記的事件將透過 Syslog 格式被傳送到 SIEM 系統。您取消選取的事件 **使用 Syslog 匯出到 SIEM 系統** 核取方塊，不會匯出到 SIEM 系統。匯出將在您啟用自動匯出和選取事件以匯出後立即開始。設定 SIEM 系統以確保它接收來自卡巴斯基安全管理中心的事件。

關於使用 Syslog 格式匯出事件

您可以使用 Syslog 格式匯出管理伺服器和受管理裝置上安裝的其他 Kaspersky 應用程式中發生的事件到 SIEM 系統。

Syslog 是訊息記錄協定的標準。它允許分離生成訊息的軟體、儲存訊息的系統和報告和分析訊息的軟體。每個訊息都帶有裝置代碼標籤，指示生成訊息的軟體類型，並被分配嚴重等級。

Syslog 格式由 Request for Comments (RFC) 文件定義，該文件由 Internet Engineering Task Force（網際網路標準）發佈。RFC 5424 標準用於從卡巴斯基安全管理中心匯出事件到外部系統。

在卡巴斯基安全管理中心中，您可以設定使用 Syslog 格式匯出事件到外部系統。

匯出過程包含兩個步驟：

1. 啟用自動事件匯出。在該步驟，卡巴斯基安全管理中心被設定，以便能傳送事件到 SIEM 系統。卡巴斯基安全管理中心在您啟用自動匯出後立即開始傳送事件。

2. 選取事件以匯出到外部系統。在該步驟，您可以選取匯出哪些事件到 SIEM 系統。

使用 CEF 和 LEEF 格式匯出事件

您可使用 CEF 和 LEEF 格式來將一般事件以及由 Kaspersky 應用程式傳輸至管理伺服器的事件匯出至 SIEM 系統。匯出事件集是預定義的，您無法選取要匯出的事件。在將事件傳送到 SIEM 系統（QRadar、ArcSight 或 Splunk）之前，需要使用siem_conversion_rules.xml 檔案中指定的規則將卡巴斯基安全管理中心事件解釋為 CEF 和 LEEF 格式的事件。

基於使用的 SIEM 系統選取匯出格式。下表顯示了 SIEM 系統和對應的匯出格式。

匯出事件到 SIEM 系統的格式

SIEM 系統	匯出格式
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF（記錄事件延伸格式）是 IBM Security QRadar SIEM 的自訂事件格式。QRadar 可以整合、識別和處理 LEEF 事件。LEEF 事件必須使用 UTF-8 字元編碼。您可以在 IBM Knowledge Center 檢視 LEEF 協定的詳情。

- CEF（通用事件格式）—開放式日誌管理標準，涉及來自不同的網路裝置和應用程式的安全資訊的協同工作。CEF 允許您使用通用日誌格式，因此資料可以被簡易整合以用企業管理系統分析。CEF 事件必須使用 UTF-8 字元編碼。

自動匯出意味著卡巴斯基安全管理中心傳送一般事件到 SIEM 系統。事件自動匯出在您啟用後立即開始。該部分詳細解釋了如何啟用自動事件匯出。

將事件轉換為 CEF 或 LEEF 格式

在將事件傳送到 SIEM 系統（QRadar、ArcSight 或 Splunk）之前，需要使用 siem_conversion_rules.xml 檔案中指定的規則將卡巴斯基安全管理中心事件解釋為 CEF 和 LEEF 格式的事件。該檔案包含在卡巴斯基安全管理中心分發套件中。

siem_conversion_rules.xml 檔案包含將事件轉換為 CEF 和 LEEF 格式的預先定義容器解釋規則。如果想使用額外的事件解釋規則，您可以手動將它們新增至檔案。

siem_conversion_rules.xml 檔案包含 `<product name="SP_QRADAR" vendor="IBM">` 和 `<product name="SP_QRADAR" vendor="IBM">` 部分。`<product name="SP_QRADAR" vendor="IBM">` 部分包含用於產生 LEEF 格式事件的規則，可以匯出到 QRadar SIEM 系統。`<product name="SP_ARCSIGHT" vendor="HP">` 部分包含用於產生 CEF 格式事件的規則，可以匯出到 ArcSight 或 Splunk SIEM 系統。

每個部分都有 `<common>` 子部分，卡巴斯基安全管理中心事件屬性以及 LEEF 格式事件的相應屬性位於其中。這些通用屬性用於所有可以匯出的事件類型。

此外，每個部分都有 `<event>` 子部分。每個 `<event>` 子部分包含被新增到 `<common>` 部分中列出的屬性中的其他屬性。

您可以手動將新的事件產生規則新增至 siem_conversion_rules.xml 檔案。

若要新增新的事件產生規則：

1. 將新的<event>子部分新增到<product name="SP_QRADAR" vendor="IBM">或<product name="SP_QRADAR" vendor="IBM">部分，然後指定其他事件屬性（如果需要）。

2. 如果事件僅由通用屬性組成，<event>子部分將為空。

siem_conversion_rules.xml

```
<conversion_rules>
    <product name="SP_QRADAR" vendor="IBM">
        <common> <!-- Common Kaspersky Security Center event attributes and corresponding LEEF event attributes --
>
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="EVC_EV_DISP_HOST_NAME" type="AT_STRING" limit="255"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND"> <!-- 帶有額外屬性的 GNRL_EV_VIRUS_FOUND 事件的產生規則 -->
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="EVC_EV_SHA256" type="AT_STRING" limit="255"/>
            </param>
            ...
        </event>
...
</product>
    <product name="SP_ARCSIGHT" vendor="HP">
        <common> <!-- Common Kaspersky Security Center event attributes and corresponding LEEF event attributes --
>
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
</conversion_rules>
```

配置卡巴斯基安全管理中心以將事件匯出到 SIEM 系統

您可以在卡巴斯基安全管理中心中啟用自動事件匯出。

僅一般事件可以透過 CEF 和 LEEF 格式從受管理應用程式匯出。用於將事件轉換為 CEF 和 LEEF 格式的解釋規則在卡巴斯基安全管理中心分發套件中包含的siem_conversion_rules.xml檔案中指定。應用程式特定事件無法透過 CEF 和 LEEF 格式從受管理應用程式匯出。如果您需要匯出受管理的應用程式的事件或使用受管理的應用程式的政策配置的自訂事件集，您必須以 Syslog 格式匯出這些事件。

若要啟用事件自動匯出：

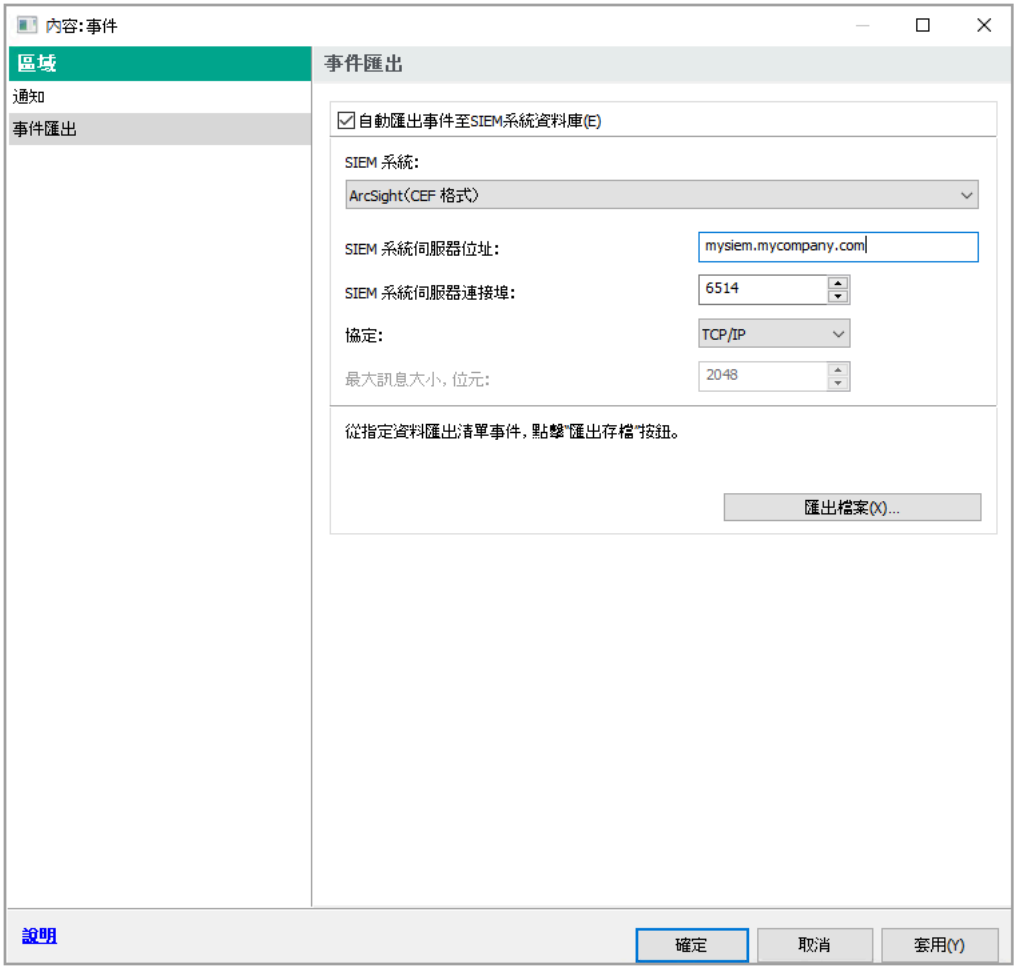
1. 在卡巴斯基安全管理中心主控台樹狀目錄，選取您要匯出事件的管理伺服器。

2. 在所選管理伺服器的工作區中，選擇**事件**頁簽。

3. 點擊**配置通知和事件匯出**連結旁的下拉箭頭並選取下拉清單的**設定匯出到 SIEM 系統**。

   事件內容視窗中將開啟**事件匯出**區域。

4. 在**事件匯出**區域中，指定以下匯出設定：



事件內容視窗的事件匯出區域

- **自動匯出事件至SIEM系統資料庫**

  選取此核取方塊以啟用自動匯出事件至 SIEM 系統。選取該核取方塊啟用**匯出事件**區域的所有欄位。

- **SIEM 系統**

  選擇要匯出事件的 SIEM 系統：QRadar® (LEEF 格式) 、 ArcSight (CEF 格式) 、Splunk® (CEF 格式) 和 Syslog 格式 (RFC 5424)。

  如果選取 Syslog 格式，則必須指定：

  最大訊息大小，位元

  指定 SIEM 系統訊息的最大大小。每個事件被一條訊息轉發。如果訊息的精確長度超過指定值，訊息被截斷且資料可能遺失。預設大小是 2048 位元組。如果您在 **SIEM 系統**欄位選取 Syslog 格式，則可使用該欄位。

- **SIEM 系統伺服器位址**

  指定 SIEM 系統伺服器位址。位址可以被指定為 DNS 或 NetBIOS 名稱或 IP 位址。

- **SIEM 系統伺服器連接埠**

指定用於連線至 SIEM 系統伺服器的埠號。該埠號必須和 SIEM 系統用於接收事件的連接埠相同（參見「設定 SIEM 系統」）。

- **協定**

  選取該協定用於傳輸訊息到 SIEM 系統。您可以選取 TCP/IP、UDP 或 TLS over TCP 通訊協定。

  如果您透過 TCP 通訊協定選取 TLS，則可以指定以下 TLS 設定：

  - **SIEM 和伺服器身分驗證**

    選擇以下其中一個方式，來對 SIEM 系統伺服器進行身分驗證：

    - **透過使用 CA 憑證**。您可以從受信任的憑證頒發機構 (CA) 接收帶有憑證清單的檔案，然後將該檔案上傳到卡巴斯基安全管理中心。卡巴斯基安全管理中心會檢查 SIEM 系統伺服器的憑證是否也由受信任的 CA 簽署。

      要新增受信任的憑證，請點擊**瀏覽**按鈕，然後上傳憑證。

      如果選擇**透過使用 CA 憑證**選項，您可以在**伺服器憑證的主旨(選用)**欄位中指定主體名稱。*主體名稱*是接收憑證的網域名稱。如果 SIEM 系統伺服器的網域與 SIEM 系統伺服器憑證的主體名稱不符，卡巴斯基安全管理中心將無法連線到 SIEM 系統伺服器。但是，如果憑證中的主體名稱已變更，則 SIEM 系統伺服器可以變更其網域名稱。如果要這麼做，請在**伺服器憑證的主旨(選用)**欄位中指定主體名稱。如果任何指定的主體名稱與 SIEM 系統憑證的主體名稱匹配，卡巴斯基安全管理中心將驗證 SIEM 系統伺服器憑證。

    - **透過使用伺服器憑證的 SHA-1 指紋**。您可以在卡巴斯基安全管理中心中指定 SIEM 系統憑證的 SHA-1 指紋。如要新增 SHA-1 指紋，請在選項下的欄位中輸入。

  - **用戶端身分驗證**

    對於用戶端身分驗證，您可以插入您的憑證或在卡巴斯基安全管理中心中產生它。

    - **插入憑證**。您可以使用從任何來源（例如，從任何受信任的憑證頒發機構）收到的憑證。要插入現有憑證，請點擊**瀏覽憑證**按鈕。在開啟的**憑證**視窗中，選擇下列其中一個憑證類型，然後指定憑證及其私密金鑰：

      - **X.509 憑證**.在**私密金鑰(*.prk, *.pem)**欄位中輸入一個包含私密金鑰的檔案，在**憑證(*.cer)**欄位中上傳包含憑證的檔案。為此，請按一下相應欄位右側的**瀏覽**按鈕，然後新增所需的檔案。這兩個檔案互不相依，檔案的載入順序並不重要。這兩個檔案上傳後，在**密碼**欄位中指定用於解碼私密金鑰的密碼。如果未編碼私密金鑰未編碼，則密碼可以為空值。

      - **PKCS#12 容器**。在**憑證檔案**欄位中，上傳包含憑證及其私密金鑰的單個檔案。為此，請按一下欄位右側的**瀏覽**按鈕，然後新增所需的檔案。檔案上傳後，在**密碼**欄位中指定用於解碼私密金鑰的密碼。如果未編碼私密金鑰未編碼，則密碼可以為空值。

    - **產生金鑰**。您可以在卡巴斯基安全管理中心中產生自簽章憑證。點擊**產生憑證**按鈕，然後在**主旨**欄位中輸入主體名稱。系統將為此主體名稱產生用戶端憑證，此憑證的 SHA-1 指紋會顯示在**用戶端憑證的 SHA-1 指紋** 欄位。因此，卡巴斯基安全管理中心會儲存產生的自我簽署憑證，您可以將憑證的公共部分或 SHA-1 指紋傳遞給 SIEM 系統。

5. 如果您要將發生在指定日期後的事件匯出到 SIEM 系統資料庫，請點擊**匯出檔案**按鈕並指定事件匯出的開始日期。預設下，事件匯出在您啟用後立即開始。

6. 點擊**確定**。

自動匯出事件被啟用。

在啟用自動匯出事件後，您必須選取將被匯出到 SIEM 系統的事件。

直接從資料庫匯出事件

您可以直接從卡巴斯基安全管理中心資料庫接收事件，而不必使用卡巴斯基安全管理中心介面。您可以直接查詢公共視圖並接收事件資料，或基於現有公共視圖建立您自己的視圖並定位它們以獲取您需要的資料。

公共視圖

為了您的方便，在卡巴斯基安全管理中心資料庫中提供了公共視圖集。您可以在 klakdb.chm 文件中找到這些公共視圖的敘述。

v_akpub_ev_event 公共視圖包含一組展示資料庫中事件參數的欄位集。在 klakdb.chm 文件中您也可以尋找對應於其他卡巴斯基安全管理中心實體的公共視圖資訊，例如，裝置、應用程式或使用者。您可以在您的查詢中使用該資訊。

該部分包含了使用 klsql2 實用程式執行 SQL 查詢的說明以及查詢例子。

要建立 SQL 查詢或資料庫視圖，您也可以使用其他程式以操作資料庫。關於如何檢視連線到卡巴斯基安全管理中心資料庫的參數的資訊，例如實例名稱和資料庫名稱，在對應區域給出。

使用 klsql2 實用程式執行 SQL 查詢

本文敘述了如何下載和使用 klsql2 實用程式，以及如何使用該實用程式執行 SQL 查詢。

要使用 klsql2 公用程式：

1. 在卡巴斯基安全管理中心的安裝資料夾中查找 klsql2 實用程式。預設安裝路徑：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.不要使用適用於舊版卡巴斯基安全管理中心的 klsql2 實用程式版本。

2. 在任何文字編輯器中建立副檔名為 .sql 的檔案，然後將該檔案與公用程式放在同一資料夾中。

3. 在建立的 .sql 檔案中，輸入所需的 SQL 查詢，然後儲存該檔案。

4. 在安裝了卡巴斯基安全管理中心管理伺服器的裝置上，在命令列，輸入以下命令以從 .sql 檔案執行 SQL 查詢並儲存結果到 result.xml 檔案：
   ```
   klsql2 -i src.sql -u < 使用者名稱 > -p < 密碼 > -o result.xml
   ```
   其中 < 使用者名稱 > 和 < 密碼 > 是有權存取資料庫的使用者帳戶的憑據。

5. 如果需要，輸入有權存取資料庫的使用者帳戶的登入名稱和密碼。

6. 開啟新建立的 result.xml 檔案以檢視 SQL 查詢結果。

您可以編輯 .sql 檔案並建立到公共視圖的任意 SQL 查詢。然後，從命令列，執行您的 SQL 查詢並儲存結果到檔案。

klsql2 實用程式中的 SQL 查詢例子

該部分顯示 SQL 查詢的例子，透過 klsql2 實用程式執行。

以下例子闡述了對過去七天發生在裝置上的事件的獲取，並依據事件發生時間顯示事件。首先顯示最近的事件。

示例：

```
SELECT

/* 事件標識 */
e.nId,

/* 事件發生的時間 */
e.tmRiseTime,

/* 事件類型的內部名稱 */
e.strEventType,

/* 事件的顯示名稱 */
e.wstrEventTypeDisplayName,

/* 事件的顯示敘述 */
e.wstrDescription,

/* 事件所在的群組名稱 */
e.wstrGroupName,

/* 發生事件的裝置的顯示名稱 */
h.wstrDisplayName,
CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +

/* 發生事件的裝置的 IP 位址 */
CAST(((h.nIp) & 255) AS varchar(4)) as strIp
FROM v_akpub_ev_event e
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

檢視卡巴斯基安全管理中心資料庫名稱

了解資料庫名稱會很有幫助，例如，傳送 SQL 查詢並從 SQL 指令碼編輯器連線至資料庫時會需要這個資料庫名稱。

要檢視卡巴斯基安全管理中心資料庫名稱：

1. 在卡巴斯基安全管理中心主控台樹狀目錄中，開啟"管理伺服器"**管理伺服器**"**內容**"。
2. 在管理伺服器內容視窗的區域視窗，選取**進階**之後選取**目前資料庫詳情**。

3. 在**目前資料庫詳情**區域注意以下資料庫內容（請參閱下圖）：

- **實例名稱**

  目前卡巴斯基安全管理中心資料庫實例名稱。預設值是 *.\KAV_CS_ADMIN_KIT*。

- **資料庫名稱**

  卡巴斯基安全管理中心 SQL 資料庫名稱。預設值是 *KAV*。

- **為卡巴斯基安全管理中心資料庫分配的空間**

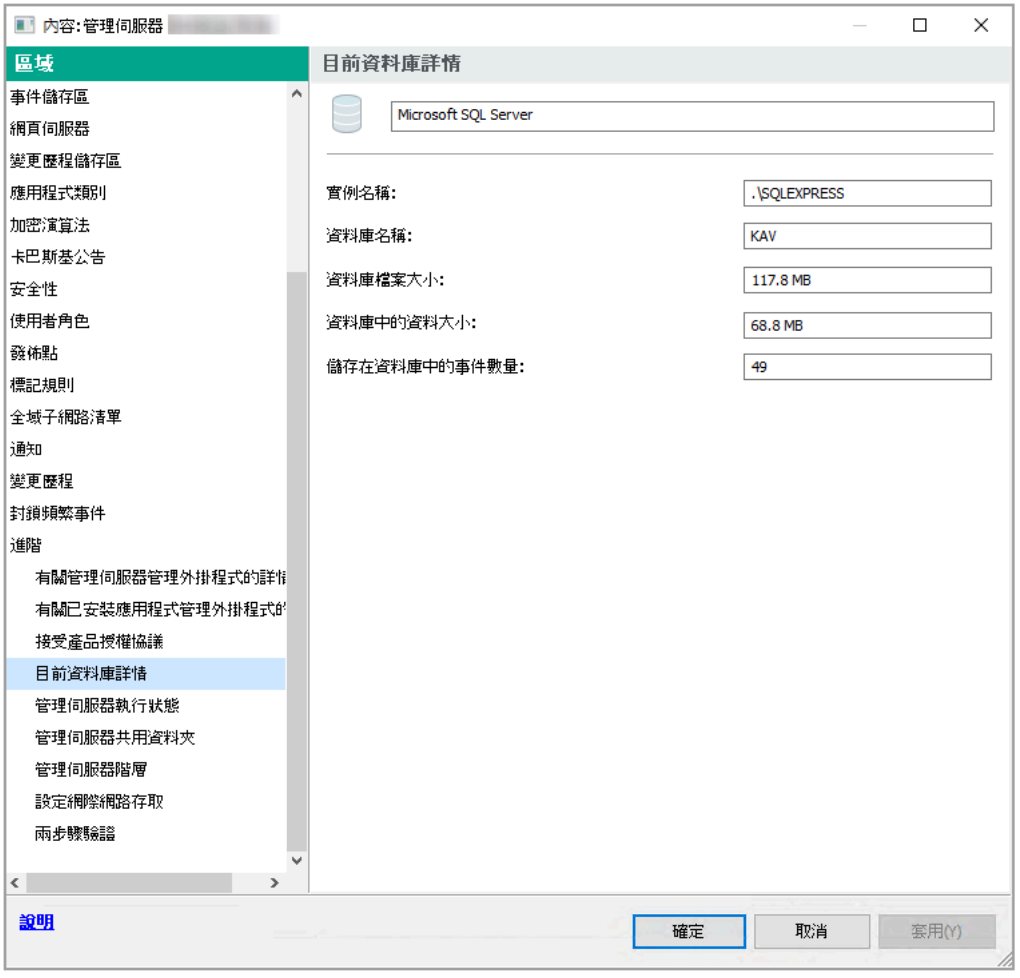
  資料庫檔案的大小。如果要清理不必要的資料，請使用*管理伺服器維護*工作來設定資料庫壓縮。

- **整個資料庫中的資料大小**

  DBMS 中目前使用的資料的實際大小。以下文章將介紹如何診斷 DBMS：資料庫大小超過限制。

- **儲存在資料庫中的事件數量**

  DBMS 中目前儲存的事件數量。有關詳細資訊，請參閱以下文章：事件處理和儲存。



帶有目前管理伺服器資料庫資訊的區域

4. 點擊**確定**按鈕以關閉管理伺服器內容視窗。

使用資料庫名稱在您的 SQL 查詢中定位資料庫。

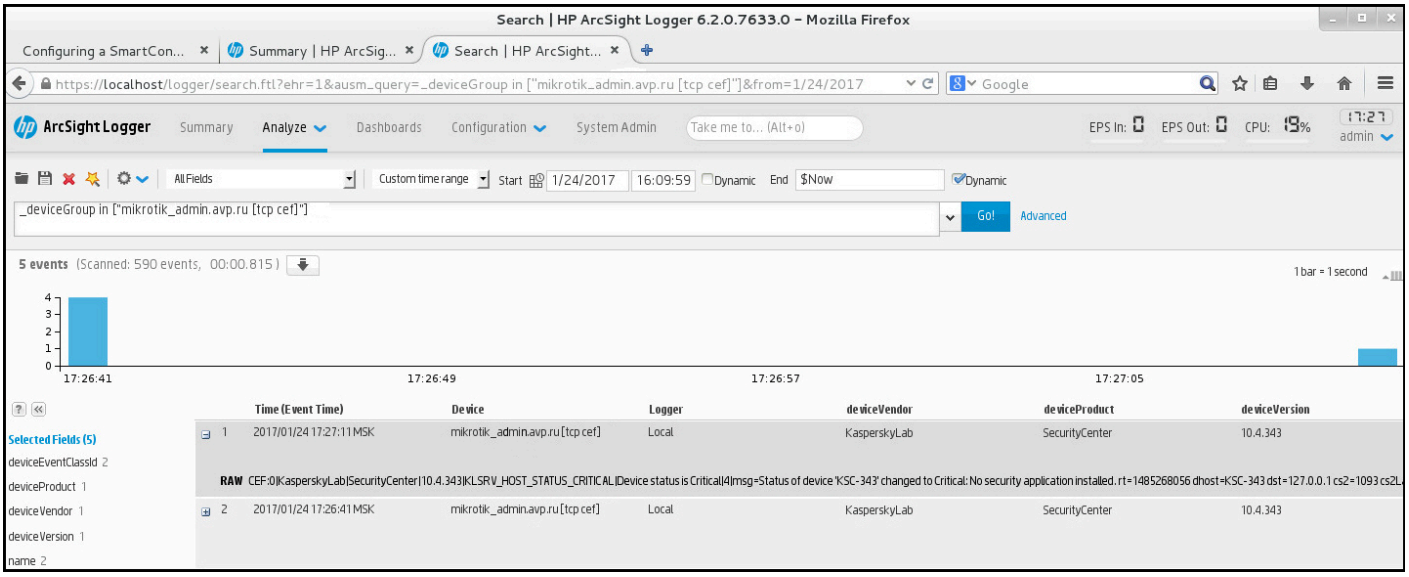
檢視匯出結果

您可以控制事件匯出過程的成功完成。為此，檢查帶有匯出事件的郵件是否被您的 SIEM 系統接收。

如果從卡巴斯基安全管理中心傳送的事件被接收並被您的 SIEM 系統正確解析，兩端的設定被正確完成。否則，檢查您在卡巴斯基安全管理中心中指定的設定是否與您的 SIEM 系統中的設定一致。

下圖顯示匯出到 ArcSight 的事件。例如，第一個事件是緊急的管理伺服器事件：「*Device status is Critical*」。

匯出事件在您 SIEM 系統中的顯示隨您使用的 SIEM 系統而不同。



例子事件

使用 SNMP 將統計資訊發送到協力廠商應用程式

本節介紹如何在 Windows 中使用簡單網路管理協議 (SNMP) 從管理伺服器取得資訊。卡巴斯基安全管理中心包含 SNMP 代理，該代理使用 OID 將管理伺服器效能的統計資訊傳輸到輔助應用程式。

本部分還包含解決在將 SNMP 用於卡巴斯基安全管理中心時可能遇到的問題資訊。

設定 SNMP 服務以與卡巴斯基安全管理中心結合使用

本節介紹如何在 Windows 上設定 SNMP 服務以使用簡單網路管理協定 (SNMP) 從管理伺服器取得資訊。

預設情況下在 Windows 上停用 SNMP 支援。

若要在 Windows 中啟用 SNMP 支援：

1. 導航到**控制面板**。
2. 開啟**新增或刪除程式**功能表。
3. 按一下**開啟或關閉 Windows功能**。
4. 在 Windows 功能清單中，瀏覽到 SNMP 功能，然後按一下**確定**。
5. 瀏覽至**控制面板 → 管理工具 → 服務**。
6. 選擇 **SNMP 服務**並執行它。
7. 透過使用 `netstat` 對標準的 UDP 連接埠進行測試來檢查偵聽是否正常。

Windows 上啟用了 SNMP 支援。

若要在 Windows 中設定 SNMP 服務：

1. 確保在**常規SNMP 代理靜默**安裝期間安裝了卡巴斯基安全管理中心的SNMP 代理元件。
2. 確保**SNMP 服務**和**SNMP 陷阱**Windows 服務正在執行。
3. 確保您的系統上安裝了 ManageEngine MIB 瀏覽器。
4. 在**SNMP Service**服務屬性的**安全性**標籤上，新增兩個具有下列權限的社區：

社區	權限
`kaspersky`	`NOTIFY`
`public`	`READ WRITE`

5. 在**接受這些主機的 SNMP 封包**欄位中，新增安裝了 ManageEngine MIB 瀏覽器的裝置的 IP 位址，例如 10.10.10.105。
6. 在**陷阱**頁簽上的**社區名稱**欄位中鍵入`kaspersky`。
7. 點擊**OK**儲存變更並且關閉服務內容視窗。
8. 在 ManageEngine MIB 瀏覽器中，從卡巴斯基安全管理中心安裝資料夾載入 adminkit.mib 檔案。預設情況下，adminkit.mib 檔案位於 <Disk>:\Program Files\Kaspersky Lab\Kaspersky Security Center\snmp 資料夾中。
9. 在 ManageEngine MIB 瀏覽器視窗的**主機**欄位中，新增安裝卡巴斯基安全管理中心管理伺服器的裝置的 IP 位址。

SNMP 服務配置用來使用簡單網路管理協定 (SNMP) 從管理伺服器取得資訊。

SNMP 代理和物件識別碼

對於卡巴斯基安全管理中心，SNMP 代理會實作為動態資料庫 `klsnmpag.dll`，該資料庫由安裝程序在管理伺服器安裝期間註冊。SNMP 代理會在 `snmp.exe` 程序（這是 Windows 服務）內部運作。協力廠商應用程式使用 SNMP 接收管理伺服器效能的統計資訊（以計數器的形式出現）。

每個計數器都有唯一的*物件識別碼*（也稱為 OID）。物件識別碼是以一個以點號分隔的數字序列。管理伺服器的物件識別碼以 1.3.6.1.4.1.23668.1093 前綴開頭。計數器的 OID 是該前綴與描述計數器的尾碼的串連。例如，OID 值為 1.3.6.1.4.1.23668.1093.1.1.4 的計數器具有值為 1.1.4 的後置詞。

您可以使用 SNMP 用戶端（例如 Zabbix）來監控系統狀態。為了獲取資訊，您可以搜尋與該資訊相對應的 OID 值，然後將該值輸入到 SNMP 用戶端中。然後，您的 SNMP 用戶端將傳回另一個表示系統狀態的值。

計數器和計數器類型清單位於管理伺服器上的 `adminkit.mib` 檔案中。*MIB* 是管理資訊資料庫的縮寫。您可以透過設計用於請求和顯示計數器值的 MIB Viewer 應用程式導入和解析 `.mib` 檔案。

從物件識別碼取得字串計數器名稱

為了使用物件識別碼 (OID) 將資訊傳輸到協力廠商應用程式，您可能需要從該 OID 獲取字串計數器名稱。

若要從 OID 獲取字串計數器名稱，請執行以下操作：

1. 在文字編輯器中，開啟位於管理伺服器上的 `adminkit.mib` 檔案。
2. 找到描述第一個值的名稱空間（從左到右）。

   例如，對於 1.1.4 的 OID 後置詞為 `"counters" (::= { kladminkit 1 })`。
3. 找到描述第二個值的名稱空間。

   例如，對於 1.1.4 的 OID 後置詞將是 `counters 1`，代表 `deployment`。
4. 找到描述第三個值的名稱空間。

   例如，對於 1.1.4 的 OID 後置詞將是 `deployment 4`，它代表 `hostsWithAntivirus`。

字串計數器名稱是這些值的串連，例如 `<MIB base namespace>.counters.deployment.hostsWithAntivirus`，並且對應於 OID，值為 1.3.6.1.4.1.23668.1093.1.1.4。

SNMP 的物件識別碼值

下表顯示物件識別碼（或為 OID）的值和說明，這些識別碼可在管理伺服器傳輸效能資訊給第三方應用程式時使用。

物件識別碼的值	數字資料類型	OID	敘述
deploymentStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.1.1	佈署狀態。此狀態可以是以下之一： • **資訊**。產品授權不再對 N 個裝置有效。 • **警告**。以下之一： 管理伺服器群組中的 N 台裝置上總共安裝了 M 台有 Kaspersky 應用程式的裝置 (N > M)。 N 台裝置上的產品授權 L 將在 M 天內到期。 已在 N 台裝置上成功完成了安裝應用程式的工作 T，M 台裝置需要重新啟動。 • **緊急**。N 台裝置的產品授權已到期。 • **確認**。以上都不是。
noAntivirusSoftware	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.1	deploymentStatus 原因顯示，管理伺服器群組包含太多沒有受管理應用程式的裝置。 如果找到沒有受管理應用程式的裝置，則該值等於 1，否則等於 0。
remoteInstallTaskFailed	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.2	deploymentStatus 原因顯示，有些裝置上的遠端安裝工作失敗。您可以透過 hostsRemoteInstallFailed 取得這些裝置的數量。
licenceExpiring	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.3	deploymentStatus 原因顯示，有些裝置的產品授權在未來 7 天內到期。您可以透過 hostsLicenseExpiring 取得這些裝置的數量。
licenceExpired	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.4	deploymentStatus 原因顯示，有些裝置的產品授權已到期。您可透過 hostsLicenseExpired 取得這些裝置的數量。
hostsInGroups	Counter32	.1.3.6.1.4.1.23668.1093.1.1.3	管理伺服器群組中的裝置數量。
hostsWithAntivirus	Counter32	.1.3.6.1.4.1.23668.1093.1.1.4	安裝了受管理應用程式的管理伺服器群組中的裝置數量。
hostsRemoteInstallFailed	Counter32	.1.3.6.1.4.1.23668.1093.1.1.5	遠端安裝工作失敗的裝置數量。
licenceExpiringSerial	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.1.6	即將過期（不到 7 天）的產品授權金鑰 ID。
licenceExpiredSerial	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.1.7	到期的產品授權金鑰 ID。
licenceExpiringDays	Unsigned32	.1.3.6.1.4.1.23668.1093.1.1.8	產品授權到期前的天數。對於此參數，如果距離到期日還剩不到 7 天，則認為產品授權期限已到期。 如果距離到期日還剩 7 天以上，則該值為 0。
hostsLicenceExpiring	Counter32	.1.3.6.1.4.1.23668.1093.1.1.9	產品授權即將到期（少於 7 天）的裝置數量。
hostsLicenceExpired	Counter32	.1.3.6.1.4.1.23668.1093.1.1.10	產品授權已到期的裝置數量。
updatesStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.2.1	防毒庫更新的目前狀態。此狀態可以是以下之一： • **資訊**。管理伺服器或裝置上的防毒庫已超過 1 天未更新，且應用程式安裝後不到 1 天。 • **警告**。管理伺服器或裝置上的防毒庫已超過 3 天沒有更新。該值可以在群組設定中變更。 • **緊急**。管理伺服器或裝置上的防毒庫已超過 7 天沒有更新。該值可以在群組設定中變更。 • **確認**。以上都不是。
serverNotUpdated	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.1	此原因顯示，在日誌記錄時間內未更新管理伺服器。在 updatesStatus 指定系統的長時間判定依據。
notUpdatedHosts	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.2	此原因顯示某些裝置很長時間沒有更新（預設情況下，**緊急**是指 7 天或以上未更新，**警告**是指 3 天未更新）。您可透過 hostsNotUpdated 取得這些裝置的數量。
lastServerUpdateTime	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.2.3	上次在管理伺服器上更新防毒庫的時間。
hostsNotUpdated	Counter32	.1.3.6.1.4.1.23668.1093.1.2.4	包含病毒資料庫且長時間未更新的裝置數量（預設情況下，**緊急**為 7 天或更長，**警告**為 3 天）。如果有處於**緊急**更新狀態的裝置，則僅統計這些裝置。您可以透過 updatesStatus 取得更新狀態。

物件識別碼的值	數字資料類型	OID	敘述
protectionStatus	INTEGER { ok(0), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.3.1	即時防護狀態。以下之一： • **警告**。以下之一： 在屬於管理伺服器群組的裝置上偵測到安全漏洞。 加密錯誤使某些裝置變更了防護狀態。 長時間未執行完整掃描。 • **緊急**。病毒防護在管理伺服器群組中的某些裝置上無法運作。 • **確認**。以上都不是。
antivirusNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.1	此原因顯示某些裝置上未執行安全應用程式。您可透過 hostsAntivirusNotRunning 取得這些裝置的數量。
realtimeNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.2	此原因顯示某些裝置上未執行即時防護。您可透過 hostsRealtimeNotRunning 取得這些裝置的數量。
notCuredFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.4	此原因顯示裝置含有未解毒的物件。您可透過 hostsNotCuredObject 取得這些裝置的數量。
tooManyThreats	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.5	此原因顯示某些裝置上發現威脅。您可透過 hostsTooManyThreats 取得這些裝置的數量。
virusOutbreak	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.6	此原因顯示系統的病毒爆發狀態。 如果在一定時間內發現一定數量的病毒，則該值等於 1，否則等於 0。透過使用病毒攻擊設定，您可以在管理伺服器上指定病毒數量和時間。
hostsAntivirusNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.3	未執行安全應用程式的裝置數量。
hostsRealtimeNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.4	未執行即時防護的裝置數量。
hostsRealtimeLevelChanged	Counter32	.1.3.6.1.4.1.23668.1093.1.3.5	即時防護層級不可接受的裝置數量。
hostsNotCuredObject	Counter32	.1.3.6.1.4.1.23668.1093.1.3.6	包含未解毒物件的裝置數量。
hostsTooManyThreats	Counter32	.1.3.6.1.4.1.23668.1093.1.3.7	包含威脅的裝置數量。
fullscanStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.4.1	防毒完整掃描的狀態。以下之一： • **資訊**。自安裝應用程式以來，已經過了不到 7 天的時間。 • **警告**。自安裝應用程式以來，已經超過 7 天未執行防毒完整掃描。 • **緊急**。自安裝應用程式以來，已經超過 14 天未執行防毒完整掃描。 • **確認**。以上都不是。
notScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.4.2.1	此原因顯示您在一定時間內未掃描某些裝置。您可透過 hostsNotScannedLately 取得這些裝置的數量。時間量可在 fullScanStatus 指定。
hostsNotScannedLately	Counter32	.1.3.6.1.4.1.23668.1093.1.4.3	一段時間內未掃描的裝置數量。時間量可在 fullScanStatus 指定。
logicalNetworkStatus	INTEGER { ok(0), warning(1), critical(2) }	.1.3.6.1.4.1.23668.1093.1.5.1	管理伺服器邏輯網路的狀態。以下之一： • **警告**。如果有處於警告狀態且無法存取的裝置，或者不屬於任何管理伺服器群組的裝置存在。 • **緊急**。如果有管理伺服器失去對某些裝置的控制權，或者如果有處於緊急狀態且無法存取的裝置存在。 • **確認**。以上都不是。
notConnectedLongTime	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.1	此原因顯示某些裝置已很長一段時間未連線到管理伺服器（**警告**狀態指裝置已 7 天或更長時間未連線，而**緊急**狀態則是指裝置已 4 天未連線）。您可透過 hostsNotConnectedLongTime 得這些裝置的數量。
controlLost	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.2	此原因顯示管理伺服器已失去某些裝置的控制權。您可透過 hostsControlLost 取得這些裝置的數量。
hostsFound	Counter32	.1.3.6.1.4.1.23668.1093.1.5.3	管理伺服器所發現不屬於任何管理伺服器群組的裝置數量。

物件識別碼的值	數字資料類型	OID	敘述
groupsCount	Counter32	.1.3.6.1.4.1.23668.1093.1.5.4	管理伺服器上的群組數量。
hostsNotConnectedLongTime	Counter32	.1.3.6.1.4.1.23668.1093.1.5.5	長時間未連線管理伺服器的裝置數量。在 notConnectedLongTime 中指定系統的長時間判定依據。
hostsControlLost	Counter32	.1.3.6.1.4.1.23668.1093.1.5.6	不受管理伺服器控制的裝置數量。
eventsStatus	INTEGER { ok(0), warning(1), critical(2) }	.1.3.6.1.4.1.23668.1093.1.6.1	事件子系統的狀態。以下之一： • **警告**。以下之一： 長時間未搜尋 Windows 更新項目的管理伺服器群組裝置。 有些裝置的狀態有問題。 • **緊急**。以下之一： 至少有一台裝置上發生"緊急"事件。 至少有一台裝置上發生"錯誤"事件。 至少有一台裝置上發生工作未能成功完成的事件。 長時間未搜尋 Windows 更新項目的管理伺服器群組裝置。 有些裝置的狀態有問題。 • **確認**。以上都不是。
criticalEventOccured	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.6.2.1	eventsStatus 原因顯示，管理伺服器上發生一些緊急事件。您可透過 criticalEventsCount 取得這些事件的數量。 如果任何裝置上至少有一個緊急事件，則該值等於 1，否則等於 0。
criticalEventsCount	Counter32	.1.3.6.1.4.1.23668.1093.1.6.3	管理伺服器上的緊急事件數。

故障解決

本節列出了使用 SNMP 服務時可能遇到的一些典型問題的解決方案。

協力廠商應用程式無法連線到 SNMP 服務

確保 SNMP 服務已依照設定 SNMP 服務以與卡巴斯基安全管理中心一起使用部分中所述進行了安裝和設定。

SNMP 服務正在執行，但是協力廠商應用程式無法取得任何值

允許 SNMP 代理追蹤，並確保建立非空白檔案。這代表 SNMP 代理已正確註冊並執行。此後，在端服務設定中允許來自 SNMP 服務的連線。如果輔助服務與 SNMP 代理在同一主機上執行，則 IP 位址清單應包含該主機的 IP 位址或 loopback 127.0.0.1。

與代理通訊的 SNMP 服務應在 Windows 中執行。您可以透過 regedit 在 Windows 註冊表中指定 SNMP 代理的路徑。

- 適用於 Windows 10：
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents
- 適用於 Windows Vista 和 Windows Server 2008：
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SNMP\Parameters\ExtensionAgents

您也可以透過 regedit 允許 SNMP 代理追蹤。

- 對於 32 位元系統：

  HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Debug

- 對於 64 位元系統：

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Deb

  "TraceLevel"=dword:00000004

  "TraceDir"="C:\\"

值與管理主控台的狀態不符

為了減少管理伺服器上的負載，系統會對 SNMP 代理實施值的快取。正在實現的快取與在管理伺服器上更改的值之間的等待時間，可能會導致 SNMP 代理傳回的值與實際值不符。使用協力廠商應用程式時，請考慮可能出現的延遲。

使用雲端環境

該部分提供了卡巴斯基安全管理中心在雲端環境中的佈署和維護資訊，例如 Amazon Web Services、Microsoft Azure 或 Google 雲端。

本文件中引用的網頁地址在 卡巴斯基安全管理中心 發布之日是正確的。

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

關於使用雲端環境

卡巴斯基安全管理中心 14.2 不僅工作在預置裝置上，也提供特殊功能以使用雲端環境。卡巴斯基安全管理中心可透過下列虛擬機運作：

- Amazon EC2 實例（以下亦稱為*實例*）。Amazon EC2 實例是基於 Amazon Web Services (AWS) 平台建立的虛擬機。卡巴斯基安全管理中心使用 AWS *API*（應用程式開發介面）。
- Microsoft Azure 虛擬機。卡巴斯基安全管理中心使用 Azure API。
- Google 雲端虛擬機實例。卡巴斯基安全管理中心使用 Google API。

您可以佈署卡巴斯基安全管理中心到實例或虛擬機以管理雲端環境中裝置的防護，並使用卡巴斯基安全管理中心的特殊功能以使用雲端環境。這些功能包括：

- 使用 API 工具輪詢雲端環境中的裝置
- 使用 API 工具安裝網路代理和安全應用程式到雲端環境中的裝置
- 基於其是否屬於指定雲端區段來搜尋裝置

您也可以使用佈署了卡巴斯基安全管理中心管理伺服器的實例或虛擬機以防護預置裝置（例如，如果對您而言雲端伺服器比實體機更容易服務和維護）。如果是這種情況，您像管理伺服器安裝在了預置裝置上一樣使用管理伺服器。

在從付費 Amazon Machine Image (AMI)（AWS 中）或基於使用的按月付費 SKU（Azure 中）佈署的卡巴斯基安全管理中心中，“弱點和修補程式管理”（包括與 SIEM 系統的整合）被自動啟動；行動裝置管理無法被啟動。

管理伺服器與管理主控台一起安裝。Kaspersky Security for Windows Server 也自動安裝到管理伺服器裝置。

您可以使用設定雲端環境精靈設定卡巴斯基安全管理中心，考慮到在雲端環境中工作的具體情況。

情境：在雲端環境中佈署

該部分敘述了佈署卡巴斯基安全管理中心以使用 Amazon Web Services、Microsoft Azure、Google 雲端等雲端環境。

在佈署方案完成後，會啟動並以預設參數設定卡巴斯基安全管理中心管理伺服器和管理主控台。由卡巴斯基安全管理中心管理的反病毒防護會佈署到所選 Amazon EC2 實例或 Microsoft Azure 虛擬機。然後您可以調整卡巴斯基安全管理中心的設定，建立管理群組複雜結構和為群組建立不同的政策和工作。

若要佈署卡巴斯基安全管理中心以在雲端環境中工作，需進行以下部分：

1. 準備工作
2. 佈署管理伺服器
3. 安裝 Kaspersky 防毒應用程式到需要被防護的虛擬裝置
4. 配置更新下載設定
5. 配置設定以管理裝置防護狀態報告

設定雲端環境精靈旨在執行初始化設定。首次從現成的映像佈署卡巴斯基安全管理中心時，它將自動啟動。您可以在任何時候手動啟動精靈。此外，您可以手動執行它執行的所有操作。

我們建議您至少分配一小時用於在雲端環境中佈署卡巴斯基安全管理中心管理伺服器，以及至少一個工作天來防護在雲端環境中的佈署。

在雲端環境中佈署卡巴斯基安全管理中心分步驟進行：

1 計畫雲端區段設定

學習卡巴斯基安全管理中心如何在雲端環境中工作。將佈署管理伺服器的計畫（在雲端環境內部或外部）；同時決定您計畫防護多少雲端區段。如果您計畫佈署雲端環境以外的管理伺服器，或者如果您計畫防護超過 5000 台裝置，您將需要手動安裝管理伺服器。

若要使用 Google 雲端，您只能手動安裝管理伺服器。

2 排程資源

確保您具有佈署所需的一切。

3 訂購到卡巴斯基安全管理中心作為現成映像

在 AWS Marketplace 選取現成 AMI 之一，或在 Azure Marketplace 選取依使用情況按月計費的 SKU，如果必要根據 Marketplace 規則支付（或使用 BYOL 模型），並使用該映像佈署安裝了卡巴斯基安全管理中心的 Amazon EC2 執行個體 / Microsoft Azure 虛擬機器。

只有當您計畫佈署管理伺服器到雲端環境中的實例 / 虛擬機上，且計畫佈署防護的裝置數不超過 5000 部時，才需要此階段。否則該步驟不是必要的，而您必須手動安裝管理伺服器、管理主控台和 DBMS。

此步驟不可用於 Google 雲端。

4 決定 DBMS 的位置

決定您的 DBMS 的位置。

如果您計畫在雲端環境之外使用資料庫，確保您擁有工作資料庫。

如果您打算使用Amazon Relational Database Service (RDS)，請在 AWS 雲端環境中使用 RDS 建立資料庫。

如果計劃使用 Microsoft Azure SQL DBMS，請在 Microsoft Azure 雲端環境中使用 Azure 資料庫服務建立資料庫。

如果您打算使用 Google MySQL，請在 Google Cloud 中建立一個資料庫（請參閱 https://cloud.google.com/sql/docs/mysql 以取得詳細資訊）。

5 在所選裝置手動安裝管理伺服器和管理主控台（以 Microsoft 管理主控台和/或 Web 主控台為基礎）

安裝管理伺服器、管理主控台和 DBMS 到所選裝置，如卡巴斯基安全管理中心主要安裝情境所述。

只有在您計畫將管理伺服器放到雲端環境外，或您計畫佈署防護的裝置數超過 5000 台裝置時，才需要此階段。然後，確保您的管理伺服器符合硬體要求。否則不需要此階段，訂閱卡巴斯基安全管理中心作為 AWS Marketplace、Azure Marketplace 或 Google Cloud 中的可用映像便已足夠。

6 確保管理伺服器具有使用雲端 API 的權限

在 AWS 管理主控台建立一個 IAM 角色或者一個 IAM 使用者帳戶。建立的 IAM 角色（或 IAM 使用者帳戶）將允許卡巴斯基安全管理中心使用 AWS API：輪詢雲端區段並佈署防護。

在 Azure，建立一個訂購和一個帶有密碼的應用程式 ID。卡巴斯基安全管理中心使用這些憑證以使用 Azure API：輪詢雲端區段和佈署防護。

在 Google 雲端中，註冊專案、取得專案 ID 和私密金鑰。卡巴斯基安全管理中心使用這些憑證輪詢使用 Google API 的雲端區段。

7 為受防護實例（僅 AWS）建立 IAM 角色

在 AWS 管理主控台，建立 IAM 角色，定義執行到 AWS 的請求的權限集。新建立的角色將被後續分配到新實例。IAM 角色用於使用卡巴斯基安全管理中心安裝應用程式到實例。

8 使用 Amazon Relational Database Service 或 Microsoft Azure SQL 準備資料庫

如果您計畫使用 Amazon Relational Database Service (RDS)，建立一個 Amazon RDS 資料庫實例和一個要備份資料庫的 S3 bucket。如果您想讓資料庫位於管理伺服器所在 EC2 實例，或者如果您想讓資料庫位於其他地方，您可以略過此步驟。

如果您排程使用 Microsoft Azure SQL，在 Microsoft Azure 中建立一個儲存帳戶和一個資料庫。

如果您打算使用 Google MySQL，請在 Google Cloud 中配置資料庫（請參閱 https://cloud.google.com/sql/docs/mysql 以取得詳細資訊）。

9 授權卡巴斯基安全管理中心以在雲端環境中使用

要確保您已授權卡巴斯基安全管理中心使用雲端環境並提供啟動碼或金鑰檔案以便應用程式可以新增其到產品授權儲存。這個階段可以在設定雲端環境過程中完成。

如果您正使用從基於 BYOL 模型的免費現成 AMI 安裝的卡巴斯基安全管理中心，或者如果您正手動安裝卡巴斯基安全管理中心而不使用 AMI，則需要此階段。這些情況下，您將需要 Kaspersky Security for Virtualization 產品授權或者 Kaspersky Hybrid Cloud Security 產品授權以啟動卡巴斯基安全管理中心。

如果您正在使用的卡巴斯基安全管理中心是從可用的映像安裝，則不需要該階段，且不會顯示對應的設定雲端環境精靈視窗。

10. **在雲端環境中授權**

    提供給卡巴斯基安全管理中心您的 AWS、Azure 或 Google Cloud 憑證，以便卡巴斯基安全管理中心可以使用必要權限操作。這個階段可以在在雲端環境中授權過程中完成。

11. **輪詢雲端區段以便管理伺服器可以接收雲端區段中裝置的資訊**

    啟動雲端區段輪詢。在 AWS 環境中，卡巴斯基安全管理中心將接收可以基於 IAM 角色或 IAM 使用者權限存取的所有實例的位址和名稱。在 Microsoft Azure 環境中，卡巴斯基安全管理中心將接收可以基於閱讀者權限存取的所有虛擬機的位址和名稱。

    然後您可以在偵測到的實例 / 虛擬機上，使用卡巴斯基安全管理中心安裝 Kaspersky 應用程式和其他供應商的軟體。

    卡巴斯基安全管理中心定期啟動輪詢，這代表會自動偵測新實例 / 虛擬機。

12. **組合所有網路裝置到雲端管理群組**

    移動所有發現的實例 / 虛擬機到**受管理裝置\雲端**管理群組，以便將其用於集中管理。如果您要將裝置分配到子群組，例如，根據在它們之上安裝的操作，您可以在**受管理裝置\雲端**群組中建立幾個管理群組。您可以啟用將一般輪詢中偵測到的所有裝置自動移動到**受管理裝置\雲端**群組。

13. **使用網路代理連線網路裝置到管理伺服器**

    安裝網路代理到雲端環境中的裝置。網路代理是提供裝置與管理伺服器間通訊的卡巴斯基安全管理中心元件。網路代理設定預設被自動配置。

    您可以在每個裝置本機安裝網路代理。您也可以使用卡巴斯基安全管理中心遠端安裝網路代理到裝置。或者，您可以略過此階段並與最新版本的安全應用程式一併安裝網路代理。

14. **安裝安全應用程式的最新版本到網路裝置**

    選取您要安裝安全應用程式的裝置，接著安裝最新版本的安全應用程式到這些裝置。您可以在管理伺服器上使用卡巴斯基安全管理中心執行遠端安裝或執行本機安裝。

    您可能需要手動為這些程式建立安裝套件。

    Kaspersky Endpoint Security for Linux 用於執行 Linux 的實例和虛擬機。

    Kaspersky Security for Windows Server 用於執行 Windows 的實例和虛擬機。

15. **配置更新設定**

當您啟動設定雲端環境時，**尋找弱點和所需更新**工作被自動建立。您也可以手動建立工作。該工作自動尋找和下載所需應用程式更新以便後續使用卡巴斯基安全管理中心工具安裝到網路裝置。

建議在雲端環境設定完成後完成以下步驟：

1. **設定報告管理**

    您可在 **管理伺服器**節點工作區的**監控**頁籤檢視報告。您也可以根據電子郵件接收報告。依預設可使用**監控**頁籤中的報告。要設定透過郵件接收報告，指定接收報告的郵件位址，接著設定報告格式。

結果

該方案完成後，您可以確保初始化配置是成功的：

- 透過管理主控台或卡巴斯基安全管理中心 網頁主控台連線到管理伺服器。
- Kaspersky 安全應用程式的最新版本被安裝並執行在受管理裝置。
- 卡巴斯基安全管理中心已為所有受管理裝置建立了預設政策和工作。

在雲端環境中佈署卡巴斯基安全管理中心的先決條件

在 Amazon Web Services 或 Microsoft Azure 雲端環境中佈署卡巴斯基安全管理中心之前，確保您具有以下：

- 網際網路存取
- 其中一個以下帳戶：
  - Amazon Web Services 帳戶（若搭配使用 AWS）
  - Microsoft 帳戶（若搭配使用 Azure）
  - Google 帳戶（若搭配使用 Google Cloud）
- 以下之一：
  - Kaspersky Security for Virtualization 的產品授權
  - Kaspersky Hybrid Cloud Security 的產品授權
  - 購買此類產品授權的資金（Kaspersky Security for Virtualization 或 Kaspersky Hybrid Cloud Security）
  - 在 Azure Marketplace 支付現成映像的基金
- 最新版本 Kaspersky Endpoint Security for Linux 和 Kaspersky Security for Windows Server 的手冊

雲端環境中管理伺服器的硬體要求

對於在雲端環境中的佈署，對管理伺服器和資料庫伺服器的要求會與對物理管理伺服器的要求相同（視要管理的裝置數量而定）。請參考雲端環境的說明文件以取得詳細資訊。

雲端環境中的產品授權選項

使用雲端環境是卡巴斯基安全管理中心基本功能之外的功能，因此需要專用產品授權。

兩個卡巴斯基安全管理中心產品授權選項可用於雲端環境：

- 付費 AMI（在 Amazon Web Services 中）或基於使用的按月付費 SKU（在 Microsoft Azure 中）。

  這授予卡巴斯基安全管理中心的產品授權以及 Kaspersky Endpoint Security for Linux 和 Kaspersky Security for Windows Server 的產品授權。您必須根據所使用的雲端環境規則進行支付。

  這個模型允許您對一個管理伺服器擁有不超過 200 台用戶端裝置。

- 一個使用專有產品授權的免費、現成映像，根據 Bring Your Own License (BYOL) 模型。

  對於在 AWS 或 Azure 中的卡巴斯基安全管理中心授權，您必須擁有以下應用程式之一的產品授權：

  - Kaspersky Security for Virtualization
  - Kaspersky Hybrid Cloud Security

  BYOL 模型允許您對一個管理伺服器擁有不超過 100,000 台用戶端裝置。該模型也允許您管理 AWS、Azure 或 Google 環境之外的裝置。

  您可以在以下任意情況選取 BYOL 模型：

  - 您已經擁有 Kaspersky Security for Virtualization 的有效產品授權。
  - 您已經擁有 Kaspersky Hybrid Cloud Security 的有效產品授權。
  - 您要在佈署卡巴斯基安全管理中心之前購買產品授權。

  在初始化設定階段，卡巴斯基安全管理中心提示您提供啟動碼或金鑰檔案。

  如果您選取 BYOL，您將不需要支付透過 Azure Marketplace 或 AWS Marketplace 使用卡巴斯基安全管理中心的費用。

兩種情況下，弱點和修補程式管理被自動啟動，且行動裝置管理無法被啟動。

如果在嘗試使用 Kaspersky Hybrid Cloud Security 的產品授權啟動雲端環境的功能支援時發生錯誤，請使用金鑰檔案。

訂購到卡巴斯基安全管理中心時，您獲取 Amazon Elastic Compute Cloud (Amazon EC2) 實例或卡巴斯基安全管理中心管理伺服器 Microsoft Azure 虛擬機。Kaspersky Security for Windows Server 和 Kaspersky Endpoint Security for Linux 的安裝套件在管理伺服器上可用。您可以安裝這些應用程式到雲端環境中的裝置。您不必授權這些應用程式。

如果受管理裝置超過一星期對管理伺服器不可見，該裝置上的應用程式（Kaspersky Security for Windows Server 或 Kaspersky Endpoint Security for Linux）將切換到受限制功能模式。要再次啟動應用程式，您將必須使安裝應用程式的裝置對管理伺服器再次可見。

在雲端環境中工作的資料庫選項

您必須擁有資料庫以使用卡巴斯基安全管理中心。當在 AWS、Microsoft Azure 或 Google Cloud 佈署卡巴斯基安全管理中心時，您有三個選項：

- 在管理伺服器裝置建立本機資料庫。卡巴斯基安全管理中心使用支援 5000 台受管理裝置的 SQL Server Express 資料庫。如果 SQL Server Express 版本足夠用則選取該選項。
- 在 AWS 雲端環境中使用 Relational Database Service (RDS) 建立資料庫，或者在 Microsoft Azure 雲端環境中使用 Azure 資料庫服務區建立資料庫。如果您想使用 DBMS 資料庫而不是 SQL Express 則選取該選項。您的資料將被傳輸到雲端環境中儲存，您將沒有任何多餘花費。如果您已經預先使用了卡巴斯基安全管理中心並在您的資料庫中擁有一些資料，您可以傳輸您的資料到新資料庫。

  對於在 Google 雲端平台上運作，您只能使用 Cloud SQL for MySQL。
- 使用現有資料庫伺服器。如果您已經擁有資料庫伺服器且想將其用於卡巴斯基安全管理中心，請選取該選項。如果該伺服器位於雲端環境之外，您的資料將透過網際網路傳輸，這將導致多餘花費。

卡巴斯基安全管理中心在雲端環境中的佈署過程具有建立（選取）資料庫的特殊步驟。

使用 Amazon Web Services 雲端環境

該部分提供了使用卡巴斯基安全管理中心在 Amazon Web Services 中工作的步驟。

本文件中引用的網頁地址在 卡巴斯基安全管理中心 發布之日是正確的。

關於使用 Amazon Web Services 雲端環境

您可以在 AWS Marketplace 以 Amazon 系統映像 (AMI) 的格式購買卡巴斯基安全管理中心，它是一個現成虛擬機映像。您可以訂購付費 AMI 或 BYOL AMI，並基於該映像建立員伺服器安裝了卡巴斯基安全管理中心管理伺服器的 Amazon EC2 實例。

要使用 AWS 平台，特別是在 AWS Marketplace 購買應用並建立實例，您需要一個 Amazon Web Services 帳戶。您可以在 https://aws.amazon.com/tw/ 建立免費帳戶。您也可以使用現有 Amazon 帳戶。

如果您在 AWS Marketplace 訂購了可用的 AMI，您接收帶有現成卡巴斯基安全管理中心的實例。您不必自己安裝應用程式。這種情況下，卡巴斯基安全管理中心管理伺服器會被自動安裝在實例上，而不需您的參與。安裝後，您可以啟動管理主控台並連線到管理伺服器以開始使用卡巴斯基安全管理中心。

關於更多 AMI 和 AWS Marketplace 如何工作的詳情，請存取 AWS Marketplace 說明頁面。對於更多使用 AWS 平台、使用實例和相關概念的資訊，請參考 Amazon Web Services 檔案。

本文件中引用的網頁地址在 卡巴斯基安全管理中心 發布之日是正確的。

為 Amazon EC2 實例建立 IAM 角色和 IAM 使用者帳戶

該部分敘述了為了確保管理伺服器的正確執行而必須執行的操作。這些操作包括使用 AWS 身分和 Access Management (IAM) 角色和使用者帳戶。還敘述了為了在用戶端裝置上安裝網路代理和 Kaspersky Security for Windows Server 以及 Kaspersky Endpoint Security for Linux 而必須執行的操作。

確保卡巴斯基安全管理中心管理伺服器具有使用 AWS 的權限

Amazon Web Services 雲端環境中的標準操作規定了一個分配到管理伺服器以使用 AWS 服務的特別 IAM 角色。IAM 角色是一個 IAM 實體，定義執行到 AWS 服務的請求的權限集的 IAM 實體。IAM 角色提供雲端區段輪詢和安裝應用程式到實例的權限。

在您建立 IAM 角色並分配其到管理伺服器後，您將可以使用該角色佈署實例的防護，而不提供任何附加資訊到卡巴斯基安全管理中心。

然而，可能建議您不要在以下情況下為管理伺服器建立 IAM 角色：

- 您計畫管理防護的裝置是 Amazon Web Services 雲端環境中的 EC2 實例，但是管理伺服器位於環境之外。
- 您計畫管理不僅您雲端區段中的實例，而且還有使用不同 AWS 帳戶建立的其他雲端區段中的實例的防護。此種情況下，您將僅需要用於您雲端區段的防護的 IAM 角色。IAM 角色將不被需要以防護其他雲端區段。

此些情況下，不是建立 IAM 角色，您將需要建立卡巴斯基安全管理中心用以使用 AWS 服務的 *IAM 使用者帳戶*。在開始使用管理伺服器之前，建立帶有 *AWS IAM 存取金鑰*（也叫 *IAM 存取金鑰*）的 IAM 使用者帳戶。

IAM 角色或 IAM 使用者帳戶的建立需要 AWS 管理主控台。要使用 AWS 管理主控台，您將需要 AWS 帳戶的使用者名稱和密碼。

為管理伺服器建立 IAM 角色

在您佈署管理伺服器之前，在 AWS 管理主控台建立帶有安裝應用程式到實例所需權限的 IAM 角色。如需更多詳細資訊，請參閱 AWS 說明區域瞭解 IAM 角色。

要為管理伺服器建立 IAM 角色：

1. 開啟 AWS 管理主控台並使用您的 AWS 帳戶登入。
2. 在**角色**區段中，建立具有以下權限的角色：
   - 在 **AmazonEC2ReadOnlyAccess**，如果您計畫僅執行雲端區段查詢而不計畫在 EC2 實例使用 AWS API 安裝應用程式。
   - 在 **AmazonEC2ReadOnlyAccess** 和 **AmazonSSMFullAccess**，如果您計畫執行雲端區段查詢並使用 AWS API 安裝應用程式到 EC2 實例。此種情況下，您將需要分配帶有 AmazonEC2RoleforSSM 權限的 IAM 角色到受防護的 EC2 實例。

您將需要分配該角色到用作管理伺服器的 EC2 實例。

新建立的角色可用於管理伺服器上的所有應用程式。因此，任何執行在管理伺服器上的應用程式都能輪詢雲端區段或安裝應用程式到雲端區段中的 EC2 實例。

本文件中引用的網頁地址在 卡巴斯基安全管理中心 發布之日是正確的。

建立 IAM 使用者帳戶以使用卡巴斯基安全管理中心

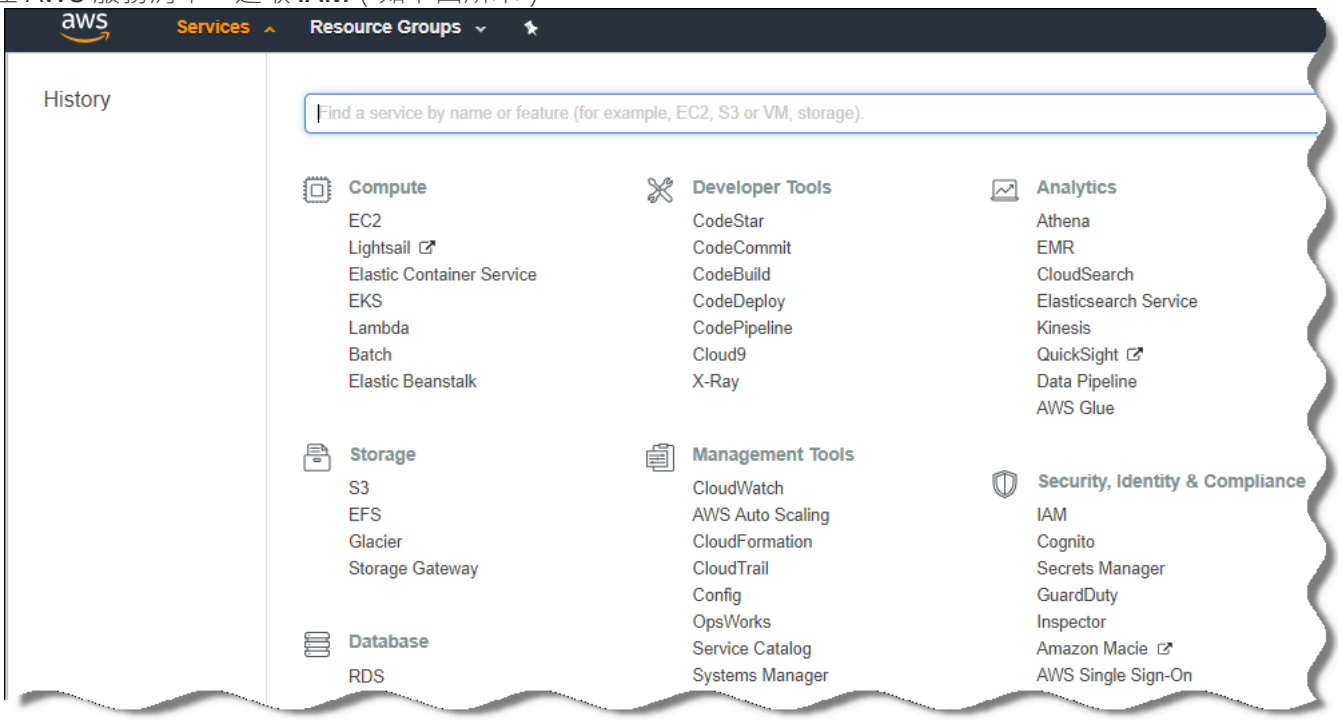
如果管理伺服器未被分配帶有裝置發現和安裝應用程式到實例的權限的 IAM 角色，則需要 IAM 使用者帳戶以使用卡巴斯基安全管理中心。相同帳戶，或者不同帳戶，如果您使用 S3 bucket，也被管理伺服器資料備份工作所需。您可以建立帶有所有必要權限的 IAM 使用者帳戶，或者您可以建立兩個不同的使用者帳戶。

初始化配置過程中您需要提供給卡巴斯基安全管理中心的 *IAM 存取金鑰* 為 IAM 使用者自動建立。IAM 存取金鑰由存取金鑰 ID 和金鑰組成。關於更多 IAM 服務的詳情，請參考以下 AWS 參考頁面：

- https://docs.aws.amazon.com/zh_tw/IAM/latest/UserGuide/introduction.html
  https://docs.aws.amazon.com/zh_tw/IAM/latest/UserGuide/introduction.html 。
- http://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2.

要建立帶有必要權限的 IAM 使用者帳戶：

1. 開啟 AWS 管理主控台 並使用您的帳戶登入。
2. 在 AWS 服務清單，選取 **IAM**（如下圖所示）。



AWS 管理主控台中的服務清單

包含使用者名稱清單和工具使用功能表的視窗開啟。

3. 在使用者帳戶相關區域導航，並新增新使用者名稱或名字。

4. 對於新增的使用者，指定以下 AWS 內容：

   - 存取類型：**程式設計存取**。
   - 未設定權限邊界。
   - 權限：
     - **ReadOnlyAccess**—如果您計畫僅執行雲端區段查詢而不計畫使用 AWS API 安裝應用程式到 EC2 實例。
     - **ReadOnlyAccess** 和 **AmazonSSMFullAccess**—如果您計畫執行雲端區段查詢並使用 AWS API 安裝應用程式到 EC2 實例。此種情況下，您將必須分配帶有 AmazonEC2RoleforSSM 權限的 IAM 角色到受防護的 EC2 實例。

   您新增權限後，精確檢視它們。一旦選取錯誤，返回上一個介面並再次做出選取。

5. 您建立使用者帳戶後，包含新 IAM 使用者的 IAM 存取金鑰的表格將出現。存取金鑰 ID 顯示在**存取金鑰 ID** 列。金鑰以星號顯示在**秘密存取金鑰**列。要檢視金鑰，點擊**顯示**。

新建立的帳戶顯示在對應於您的 AWS 帳戶的 IAM 使用者帳戶清單。

當在雲端區段中佈署卡巴斯基安全管理中心時，您必須指定您正在使用 IAM 使用者帳戶並提供存取金鑰 ID 和金鑰給卡巴斯基安全管理中心。

> 本文件中引用的網頁地址在 卡巴斯基安全管理中心 發布之日是正確的。

為安裝應用程式到 Amazon EC2 實例建立 IAM 角色

在您使用卡巴斯基安全管理中心在 EC2 實例上開始防護佈署之前，在 AWS 管理主控台 建立一個 IAM 具有安裝應用程式到實例所需權限的角色。如需更多詳細資訊，請參閱 AWS 說明 區域 AWS 說明瞭解 IAM 角色。

IAM 角色是必需的，因此您可以分配它到所有您要使用卡巴斯基安全管理中心安裝安全應用程式的 EC2 實例。如果您不分配給實例具有必要權限的 IAM 角色，使用 AWS API 工具安裝應用程式到該實例將導致錯誤。

要使用 AWS 管理主控台，您將需要 AWS 帳戶的使用者名稱和密碼。

為安裝應用程式到實例建立 IAM 角色

1. 開啟 AWS 管理主控台 並使用您的 AWS 帳戶登入。
2. 在左側功能表中，選取 **Roles**。
3. 點擊“**Create Role**”按鈕。
4. 在出現的服務清單中，選取 **EC2**，然後在 **Select Your Use Case** 清單中再次選取 **EC2**。
5. 點擊**下一步：權限**按鈕。
6. 在開啟的功能表中，選取 **AmazonEC2RoleforSSM** 旁邊的核取方塊。

7. 按一下**下一步：檢閱**按鈕。

8. 為 IAM 角色輸入名稱和敘述並點擊 **Create Role** 按鈕。

   您建立的角色出現在角色清單，顯示您輸入的名稱和敘述。

然後，您可以使用新建立的 IAM 角色建立新的您要透過卡巴斯基安全管理中心防護的 EC2 實例，以及使用現有實例進行關聯。

本文件中引用的網頁地址在 卡巴斯基安全管理中心 發布之日是正確的。

使用 Amazon RDS

該部分敘述了必須採取哪些操作以為卡巴斯基安全管理中心準備 Amazon Relational Database Service (RDS) 資料庫，放置其到選項群組，建立 IAM 角色以使用 RDS 資料庫，準備 S3 bucket 以儲存，和遷移現有資料庫到 RDS。

Amazon RDS 是幫助 AWS 使用者在 AWS 雲端環境中設定、操作和測量關聯式資料庫的 Web 服務。如果您想，您可以使用 Amazon RDS 資料庫以配合使用卡巴斯基安全管理中心。

您可搭配使用以下資料庫：

- Microsoft SQL Server
- SQL Express Edition
- Aurora MySQL 5.7
- Standard MySQL 5.7

建立 Amazon RDS 實例

如果您要使用 Amazon RDS 作為 DBMS，您必須建立 Amazon RDS 資料庫實例。此區段說明如何選取 SQL Express Edition；若您要使用 Aurora MySQL 或 Standard MySQL（版本 5.7，8.0），您必須選取這些引擎的其中一個。

要建立 Amazon RDS 資料庫實例：

1. 在 https://console.aws.amazon.com 開啟 AWS 管理主控台並使用您的帳戶登入。
2. 使用 AWS 介面，用以下設定建立資料庫：
   - 引擎：Microsoft SQL Server、SQL Express 版本
   - DB 引擎版本：SQL Server 2014 12.00.5546.0v1
   - DB 實例類：db.t2.medium
   - 儲存類型：一般目的
   - 分配的儲存：最小 50 GiB
   - 安全群組：卡巴斯基安全管理中心管理伺服器 EC2 實例所在群組

   為您的 RDS 實例建立識別碼、主使用者名稱和主密碼。

   您可以在其他所有欄位保留預設設定。或者，如果您要自訂您的 Amazon RDS 實例，則變更預設設定。要獲得說明，請參考 AWS 資訊頁面。
3. 在最後一步，AWS 顯示處理程序結果。如果您要檢視您的 Amazon RDS 實例的詳情，點擊**檢視 DB 實例詳情**。如果您要繼續操作，開始為您的 Amazon RDS 實例建立選項群組。

新 Amazon RDS 實例的建立可能花費幾分鐘。實例被建立後，您可以利用其使用卡巴斯基安全管理中心資料。

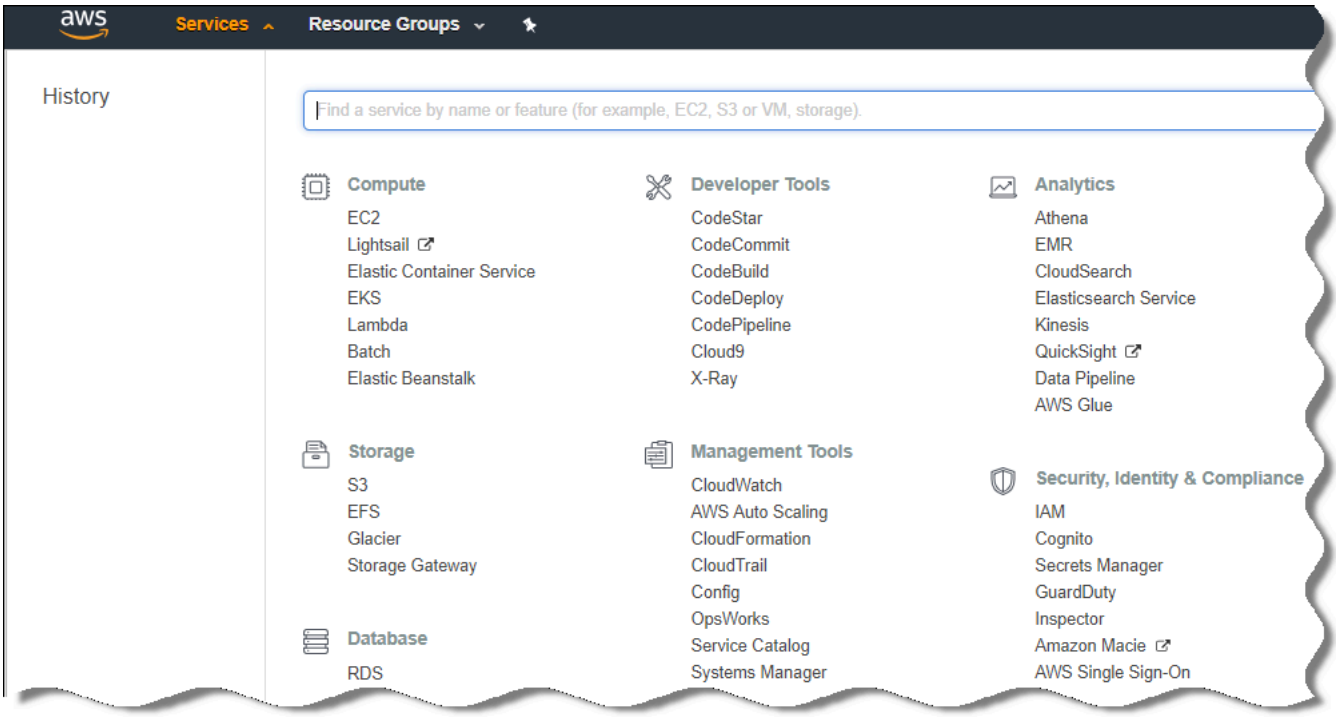
本文件中引用的網頁地址在 卡巴斯基安全管理中心 發布之日是正確的。

為 Amazon RDS 實例建立選項群組

您需要放置您的 Amazon RDS 實例到選項群組。

要為您的 Amazon RDS 實例建立選項群組：

1. 確保您在 AWS 管理主控台 (https://console.aws.amazon.com) 且以您的帳戶登入。
2. 在功能表中，點擊**服務**。
   可用服務清單出現（參見下圖）。



AWS 管理主控台中的服務清單

3. 在清單中，點擊 **RDS**。
4. 在左側視窗，點擊**選項群組**。
5. 點擊"**建立群組**"按鈕。
6. 如果您在建立 Amazon RDS 實例階段選取 SQL Server，使用以下設定建立選項群組：
   - 引擎：SQLserver-ex
   - 主引擎版本：12.00

   如果您在建立 Amazon RDS 實例階段選取不同 SQL 資料庫，那麼選取對應的引擎。

群組被建立並顯示在您的群組清單中。

在建立選項群組後，放置您的 Amazon RDS 實例到選項群組。

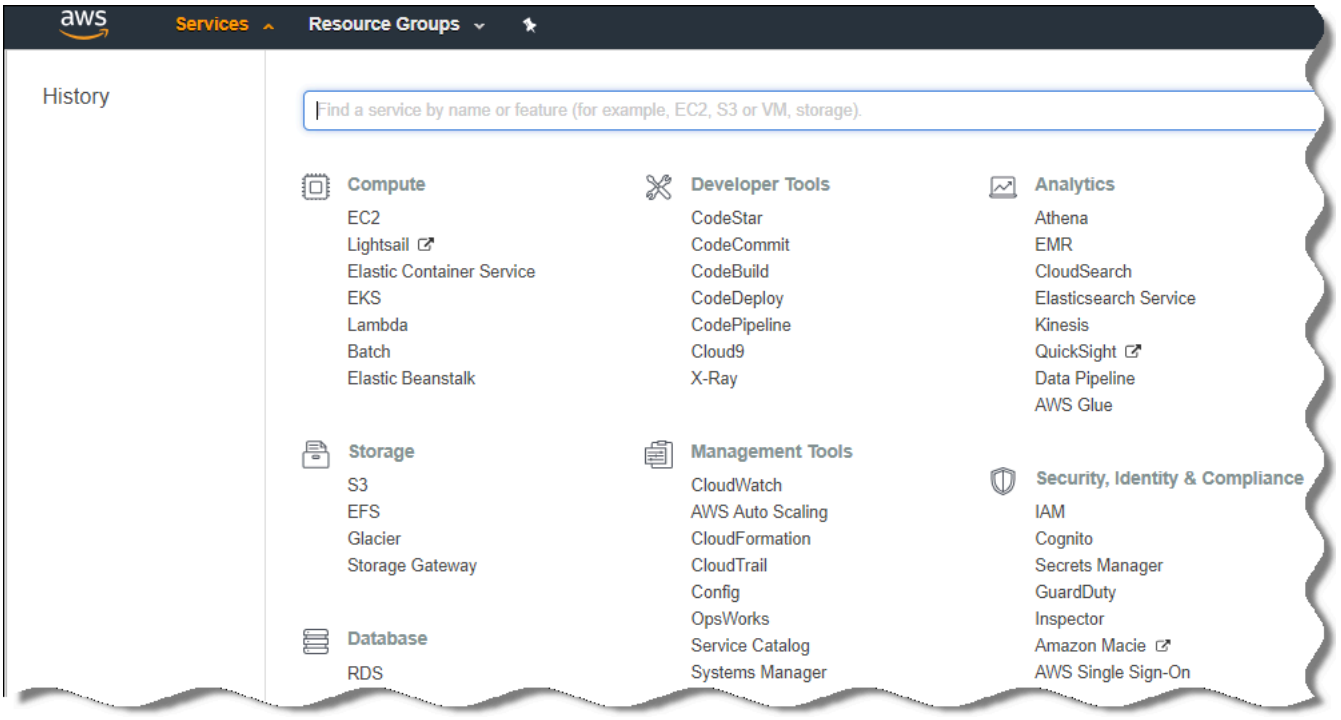
本文件中引用的網頁地址在 卡巴斯基安全管理中心 發布之日是正確的。

修改選項群組

您放置 Amazon RDS 實例的選項群組的預設設定不足以使用卡巴斯基安全管理中心資料庫。您必須新增選項到選項群組並建立新 IAM 角色以使用資料庫。

要修改選項群組並建立新 IAM 角色：

1. 確保您在 AWS 管理主控台 (https://console.aws.amazon.com) 且以您的帳戶登入。
2. 在功能表中，點擊**服務**。
   可用服務清單出現（參見下圖）。



AWS 管理主控台中的服務清單

3. 在清單中，選取 RDS。
4. 在左側視窗，點擊**選項群組**。
   選項群組清單被顯示。
5. 選取您放置您的 Amazon RDS 實例的選項群組並點擊**新增選項**按鈕。
   "**新增選項**"視窗將開啟。
6. 在 IAM 角色區域，選取**建立新角色 / 是**選項並輸入新 IAM 角色的名稱。
   角色使用預設權限集建立。稍後，您將必須變更它的權限。
7. 在 S3 bucket 區域，做以下之一：
   - 如果您沒有為資料備份建立 Amazon S3 bucket 實例，選取"**建立新 S3 bucket**"連線並使用 AWS 介面建立新 S3 bucket。
   - 如果您已經為管理伺服器資料備份工作建立了 Amazon S3 bucket 實例，從下拉式清單選取您的 S3 bucket。
8. 透過點擊頁面下方的**新增選項**按鈕結束新增選項。

您已修改了選項群組並建立了新 IAM 角色以使用 RDS 資料庫。

本文件中引用的網頁地址在 卡巴斯基安全管理中心 發布之日是正確的。

為 IAM 角色修改權限以使用 Amazon RDS 資料庫實例

在您新增選項到選項群組之後，您必須分配所需權限到您建立的 IAM 角色以使用 Amazon RDS 資料庫實例。

要分配所需權限到您建立的 IAM 角色以使用 Amazon RDS 資料庫實例：

1. 確保您在 AWS 管理主控台 (https://console.aws.amazon.com) 且以您的帳戶登入。
2. 在服務清單中，選取 **IAM**。
   包含使用者名稱清單和工具使用功能表的視窗開啟。
3. 在功能表中選取**角色**。
4. 在工作區中顯示的 IAM 角色清單，選取您在新增選項到選項群組時建立的角色。
5. 使用 AWS 介面，刪除 **sqlNativeBackup-<日期>** 政策。
6. 使用 AWS 介面，附加 **AmazonS3FullAccess** 政策到角色。

IAM 角色被分配所需權限以使用 Amazon RDS。

本文件中引用的網頁地址在 卡巴斯基安全管理中心 發布之日是正確的。

為資料庫準備 Amazon S3 bucket

如果您計畫使用 Amazon Relational Database System (ARDS) 資料庫，您必須建立儲存資料庫一般備份的 Amazon Simple Storage Service (Amazon S3) bucket 實例。對於 Amazon S3 和 S3 buckets 的資訊，請參考 Amazon 說明頁面。對於建立 Amazon S3 實例的更多資訊，請參考 Amazon S3 說明頁面。

要建立 Amazon S3 bucket：

1. 確保 AWS 管理主控台 被開啟且您已以您的帳戶登入。
2. 在 AWS 服務清單中，選取 S3。
3. 在控制台中導航以建立 bucket，遵循精靈的以下說明。
4. 選取您的管理伺服器所在（或將在）的相同區域。
5. 當精靈結束時，確保新 bucket 出現在 bucket 清單。

新 S3 bucket 被建立並出現在您的 bucket 清單。當新增選項到選項群組時，您必須指定該 bucket。當卡巴斯基安全管理中心正在建立 *管理伺服器資料備份* 工作時，您將必須指定您的 S3 bucket 位址給卡巴斯基安全管理中心。

本文件中引用的網頁地址在 卡巴斯基安全管理中心 發布之日是正確的。

遷移資料庫到 Amazon RDS

您可以從預置裝置遷移您的卡巴斯基安全管理中心資料到支援 Amazon RDS 的 Amazon S3 實例。為此，您需要 RDS 資料庫的 S3 bucket 和此 S3 bucket 的 帶有 AmazonS3FullAccess 權限的 IAM 使用者帳戶。

要執行資料庫遷移：

1. 確保您已建立了 RDS 實例（參考 Amazon RDS 參考頁面以獲得更多資訊）。
2. 在您的預置實體管理伺服器上，執行 Kaspersky 備份實用程式以備份管理伺服器資料。
   您必須確保該檔案名稱為 backup.zip。
3. 將 backup.zip 檔案複製到安裝管理伺服器的 EC2 執行個體。

   確保您在管理伺服器 EC2 實例上有足夠磁碟空間。在 AWS 環境中，您可以新增更多的磁碟空間到您的實例以容納資料庫遷移。
4. 在 AWS 管理伺服器，以互動模式啟動 Kaspersky 備份實用程式。
   這樣將啟動備份和還原精靈。
5. 在**選取操作**步驟選取**還原管理伺服器資料**並點擊**下一步**。
6. 在**還原設定**步驟，點擊**儲存備份副本的資料夾**旁的**瀏覽**按鈕。
7. 在開啟的**登入到線上儲存**視窗填寫以下欄位，之後點擊**確定**：

   - **S3 bucket 名稱**

     您的 S3 bucket 名稱。

   - **備份資料夾**

     指定用於備份的儲存資料夾位置。

   - **存取金鑰 ID**

     屬於具有使用 S3 bucket 的權限（AmazonS3FullAccess 權限）的 IAM 使用者的 AWS IAM 存取金鑰 ID。

   - **金鑰**

     屬於具有使用 S3 bucket 的權限（AmazonS3FullAccess 權限）的 IAM 使用者的 AWS IAM 金鑰。
8. 選取**從本機備份移轉**選項。**瀏覽**按鈕變得可用。

9. 點擊**瀏覽**按鈕在 AWS 管理伺服器選取您複製 backup.zip 檔案的資料夾。

10. 點擊**下一步**並完成過程。

您的資料將使用您的 S3 bucket 還原到 RDS 資料庫。您可以使用該資料庫以便進一步在 AWS 環境中使用卡巴斯基安全管理中心。

本文件中引用的網頁地址在 卡巴斯基安全管理中心 發布之日是正確的。

工作在 Microsoft Azure 雲端環境

該部分提供了卡巴斯基安全管理中心在 Microsoft Amazon 提供的雲端環境的佈署和維護資訊，以及在雲端環境中的虛擬機上的防護佈署詳情。

在依使用情況計費且按月付費 SKU 佈署的卡巴斯基安全管理中心中，「弱點和修補程式管理」會自動啟動，且「行動裝置管理」無法被啟動。

關於使用 Microsoft Azure

要使用 Microsoft Azure 平台，特別是要在 Azure Marketplace 購買應用並建立虛擬機，您將需要一個 Azure 訂購。在您佈署管理伺服器之前，建立帶有安裝應用程式到虛擬機所需權限的 Azure 應用程式 ID。

如果您在 Azure Marketplace 購買卡巴斯基安全管理中心映像，您可以使用您的現成卡巴斯基安全管理中心管理伺服器佈署虛擬機。要必須選取虛擬機設定，但是您不必自己安裝應用程式。安裝後，您可以啟動管理主控台並連線到管理伺服器以開始使用卡巴斯基安全管理中心。

您也可以使用佈署了卡巴斯基安全管理中心管理伺服器的 Azure 虛擬機以防護預置裝置（例如，如果雲伺服器比實體機更容易服務和維護）。如果是這種情況，您像管理伺服器安裝在了預置裝置上一樣使用管理伺服器。如果您不計畫使用 Azure API 工具，您不需要 Azure 應用程式 ID。此種情況下，Azure 訂購已足夠。

建立訂購、應用程式 ID 和密碼

要在 Microsoft Azure 環境中使用卡巴斯基安全管理中心，您需要一個 Azure 訂購、Azure 應用程式 ID 和 Azure 應用程式密碼。您可以使用現有訂購，如果您已經擁有。

Azure 訂購授予其所有者到 Microsoft Azure Platform Management Portal 和 Microsoft Azure 服務的存取權限。所有者可以使用 Microsoft Azure Platform 以管理服務，例如 Azure SQL 和 Azure Storage。

要建立 Microsoft Azure 訂購，

轉到https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/create-subscription並按照那裡的說明進行操作。

關於建立訂購的更多資訊在 Microsoft 網站 可用。您將獲得訂購 ID，您將稍後將其與應用程式 ID 和密碼一起提供給卡巴斯基安全管理中心。

要建立和儲存 Azure 應用程式 ID 和密碼，

1. 轉到 https://portal.azure.com 並確保您已登入。
2. 遵照 reference page 的說明，建立您的應用程式 ID。
3. 轉到應用程式設定的**金鑰**區域。
4. 在**金鑰**區域，填充**敘述**和**過期**欄位並置**參數值**欄位為空。
5. 點擊**儲存**。

   當您點擊**儲存**，系統自動使用一個長字元序列填充**參數值**欄位。該序列是您的 Azure 應用程式密碼（例如，yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QlfFvdU=）。敘述在您輸入時被顯示。
6. 複製密碼並儲存，以便您可以稍後提供應用程式 ID 和密碼到卡巴斯基安全管理中心。

   您僅可以在密碼被建立時複製它。稍後，密碼不再被顯示且您無法還原它。

本文件中引用的網頁地址在 卡巴斯基安全管理中心 發布之日是正確的。

分配角色到 Azure 應用程式 ID

如果您僅想使用裝置發現偵測虛擬機，您的 Azure 應用程式 ID 必須具有閱讀者角色。如果您不僅要偵測虛擬機，還想佈署防護到虛擬機，您的 Azure 應用程式 ID 必須具有虛擬機建立者角色。

按照 Microsoft 網站上的說明分配角色到您的 Azure 應用程式 ID。

在 Microsoft Azure 中佈署管理伺服器並選取資料庫

要在 Microsoft Azure 環境中佈署管理伺服器：

1. 使用您的帳戶登入到 Microsoft Azure。
2. 轉到 Azure 入口網站。
3. 在左側視窗，點擊綠色加號。
4. 在功能表中的搜尋欄位輸入“Kaspersky Hybrid Cloud Security”。

   Kaspersky Hybrid Cloud Security 是卡巴斯基安全管理中心和兩個即時防護安全應用程式的組合：Kaspersky Endpoint Security for Linux 和 Kaspersky Security for Windows Server。
5. 在結果清單中，選取 Kaspersky Hybrid Cloud Security 或 Kaspersky Hybrid Cloud Security (BYOL)。

   在螢幕的右側，資訊視窗出現。
6. 閱讀資訊並點擊資訊視窗後面的“建立”按鈕。
7. 填充所有必要欄位。使用工具提示獲得資訊和說明。

8. 當選取大小時，選取三個共用選項之一。

   在多數情況，8 gigabytes (GB) 記憶體已足夠。然而，在 Azure，您可以在任何時候增加記憶體和虛擬機其他資源的大小。

9. 當選取資料庫時，根據您的排程選取以下之一：

   - 本機 — 如果您想讓資料庫位於佈署管理伺服器的虛擬機。卡巴斯基安全管理中心帶有 SQL Server Express 資料庫。如果 SQL Server Express 足夠用則選取該選項。
   - 新 — 如果您想在 Azure 環境中使用新 RDS 資料庫。如果您想使用 DBMS 資料庫而不是 SQL Server Express 則選取該選項。您的資料將被傳輸到雲端環境以儲存，您將沒有任何多餘花費。
   - 現有 — 如果您想使用現有資料庫伺服器。此種情況下，您將必須指定其位置。如果該伺服器位於 Azure 環境之外，您的資料將透過網際網路傳輸，這將導致多餘花費。

10. 當輸入訂購 ID 時，使用您之前建立的訂購。

    佈署之後，您可以透過 RDP 連線到管理伺服器。您可以使用管理主控台來操作管理伺服器。

使用 Azure SQL

該部門敘述了需要採取什麼操作以為卡巴斯基安全管理中心準備 Microsoft Azure 資料庫、準備 Azure 儲存帳戶和遷移現有資料庫到 Azure SQL。

SQL 資料庫是一個 Microsoft Azure 中的關聯式資料庫管理服務。

本文件中引用的網頁地址在 卡巴斯基安全管理中心 發布之日是正確的。

建立 Azure 儲存帳戶

您必須在 Microsoft Azure 中建立儲存帳戶以使用 Azure SQL 資料庫以佈署指令碼。

要建立儲存帳戶：

1. 登入到 Azure 入口網站。
2. 在左側面板，選取**儲存帳戶**以轉到**儲存帳戶**視窗。
3. 在**儲存帳戶**視窗，點擊**新增**按鈕轉到**建立儲存帳戶**視窗。
4. 填充必要欄位以建立儲存帳戶：
   - 位置：必須和管理伺服器位置相同。
   - 其他欄位：您可能選取預設值。

   使用工具提示獲得每個欄位的資訊。

   建立儲存帳戶後，您的儲存帳戶清單被顯示。

5. 在您的儲存帳戶清單中，點擊新建立的帳戶名稱以檢視該帳戶的信息。

6. 確保您知道資源名稱、資源群組和該儲存帳戶的存取金鑰。您將需要該資訊以使用卡巴斯基安全管理中心。

您可以參考 Azure 網站以獲得幫助。

如果您已經擁有儲存帳戶，您可以將其用於卡巴斯基安全管理中心。

建立 Azure SQL 資料庫和 SQL Server

您需要 Azure 環境中的 SQL 資料庫和 SQL Server。

要建立 Azure SQL 資料庫和 SQL Server：

1. 遵照 Azure 網站的說明。

   當 Microsoft Azure 提示您時您可以建立新伺服器；如果您已經擁有 Azure SQL Server，您可以將其用於卡巴斯基安全管理中心，而不用建立新的。

2. 建立 SQL 資料庫和 SQL Server 後，確保您知道其資源名稱和資源群組：

   a. 轉到 https://portal.azure.com 並確保您已登入。

   b. 在左邊視窗中，選取 **SQL 資料庫**。

   c. 從您的資料庫清單裡點擊資料庫名稱。

      內容視窗隨即開啟。

   d. 資料庫的名稱是資源名稱。資源群組的名稱顯示在內容視窗的**概述**部分。

您需要資料庫的資源名稱和資源群組以遷移資料庫到 Azure SQL。

遷移資料庫到 Azure SQL

在管理伺服器被佈署到 Azure 環境之後，您可以從預置裝置遷移您的卡巴斯基安全管理中心資料庫到 Azure SQL。您需要一個 Azure 儲存帳戶用於 Azure SQL 資料庫。您還必須在您的管理伺服器上擁有 Microsoft SQL Server Data-Tier Application Framework (DacFx) 和 SQLSysCLRTypes。

要執行資料庫遷移：

1. 確保您建立了 Azure 儲存帳戶。

2. 確保您在您的管理伺服器上擁有 SQLSysCLRTypes 和 DacFx。

   您可以從官方 Microsoft 網站下載 Microsoft SQL Server 資料層應用程式架構 (17.0.1 DacFx) 和 SQLSysCLRTypes（選擇與 SQL Server 版本相對應的版本）。

3. 在您預置的實體管理伺服器上，執行 Kaspersky 備份實用程式以備份管理伺服器資料（啟用**移轉到 Azure 格式**選項）。

4. 複本備份檔案到管理伺服器。

確保您在管理伺服器 Azure 虛擬機上有足夠磁碟空間。在 Azure 環境中，您可以新增更多的磁碟空間到您的虛擬機以容納資料庫遷移。

5. 在位於 Microsoft Azure 環境的管理伺服器上，再次以互動模式啟動 Kaspersky 備份實用工具。
這樣將啟動備份和還原精靈。

6. 在**選取操作**步驟選取**還原管理伺服器資料**並點擊**下一步**。

7. 在**還原設定**步驟，點擊**儲存備份副本的資料夾**旁的**瀏覽**按鈕。

8. 在開啟的**登入到線上儲存**視窗填寫以下欄位，之後點擊**確定**：

- **Azure 儲存帳戶名稱**

  您建立了 Azure 儲存帳戶名稱以使用卡巴斯基安全管理中心。

- **備份資料夾**

  指定用於備份的儲存資料夾位置。

- **Azure 訂購 ID**

  您在 Azure 網站建立了該訂購。

- **Azure 應用程式密碼**

  當您建立應用程式 ID 時您收到應用程式 ID 的密碼。

  密碼的字元顯示為星號。在您開始輸入密碼後，**顯示**按鈕可用。按一下並按住該按鈕以檢視您輸入的字元。

- **Azure 儲存存取金鑰**

  在您的儲存帳戶內容中可用，在存取金鑰區域。您可以使用任何金鑰（key1 或 key2）。

- **Azure SQL Server 名稱**

  在您的 Azure SQL Server 內容中可用。

- **Azure SQL Server 資源群組**

  在您的 Azure SQL Server 內容中可用。

- **Azure 應用程式 ID**

  您在 Azure 網站建立了該應用程式 ID。

  您僅可以提供一個 Azure 應用程式 ID 用於輪詢和其他目的。如果您要輪詢其他 Azure 段，您必須先刪除現有 Azure 連線。

9. 選取**從本機備份移轉**選項。

   瀏覽按鈕變得可用。

10. 點擊**瀏覽**按鈕在 Azure 管理伺服器選取您複本備份檔案的資料夾。

11. 點擊**下一步**並完成過程。

您的資料將使用您的 Azure 儲存還原到 Azure SQL 資料庫。您可以使用該資料庫以便進一步在 Azure 環境中使用卡巴斯基安全管理中心。

本文件中引用的網頁地址在 卡巴斯基安全管理中心 發布之日是正確的。

在 Google 雲端中使用

本節提供在 Google 提供的雲環境中使用卡巴斯基安全管理中心工作的資訊。

建立客戶電子郵件，專案 ID 和私密金鑰

您可以使用 Google API 在 Google 雲端平台中使用卡巴斯基安全管理中心。您需要有 Google 帳戶。如需詳細資訊，請參閱 https://cloud.google.com 上的 Google 文件。

您將需要向卡巴斯基安全管理中心建立並提供以下憑證：

- **用戶端電子郵件**

  輸入您用來在 Google Cloud 註冊專案的電子郵件。

- **專案 ID**

  專案 ID 是您在 Google Cloud 註冊專案時收到的 ID。

- **私密金鑰**

  私密金鑰是您在 Google Cloud 註冊專案時作為私密金鑰收到的字元序列。您可能會想要複製並貼上此序列，以免出錯。

使用 Google Cloud SQL for MySQL 實例

您可以在 Google Cloud 中建立資料庫，並將該資料庫用於卡巴斯基安全管理中心。

卡巴斯基安全管理中心可與 MySQL 5.7 和 5.6 搭配使用。其他版本的 MySQL 尚未經過測試。

若要建立和配置 MySQL 資料庫：

在瀏覽器中，請前往 https://cloud.google.com/sql/docs/mysql/create-instance#create-2nd-gen，然後遵循提供的指示說明操作。

配置 MySQL 資料庫時，請使用以下旗標：

- **sort_buffer_size** 10000000
- **join_buffer_size** 20000000
- **innodb_lock_wait_timeout** 300
- **max_allowed_packet** 32000000
- **innodb_thread_concurrency** 20
- **max_connections** 151
- **tmp_table_size** 67108864
- **max_heap_table_size** 67108864
- **lower_case_table_names** 1

在雲端環境中準備必要的用戶端裝置以使用卡巴斯基安全管理中心

每個您要安裝管理伺服器、網路代理和 Kaspersky 安全應用程式的裝置，都必須符合以下條件：

- 安全群組配置使得以下連接埠在管理伺服器上可用（佈署所需的最小連接埠集）：
  - 8060 HTTP—用於從管理伺服器傳輸網路代理安裝套件和安全應用程式安裝套件到受防護實例
  - 8061 HTTP—用於從管理伺服器傳輸網路代理安裝套件和安全應用程式安裝套件到受防護實例
  - 13000 TCP—用於使用 SSL 從受防護執行個體和從屬管理伺服器傳輸資料到主管理伺服器
  - 13000 UDP—用於傳輸實例關閉的資訊到管理伺服器
  - 14000 TCP—適用於在不使用 SSL 的情況下，從防護的執行個體和從屬管理伺服器傳輸資料到主管理伺服器的情況
  - 13291—用於將管理主控台連線至管理伺服器
  - 40080—用於佈署指令碼操作

  您可以在 AWS 管理主控台或 Azure 網站配置安全群組。如果您要以非預設設定使用卡巴斯基安全管理中心，請參考知識庫文章。非預設配置的例子包括不安裝管理主控台到管理伺服器裝置而是安裝到您的工作站，或使用 KSN 代理伺服器。
- UDP 連接埠 15000 在用戶端裝置上可用（用於在與管理伺服器的互動中接收請求）。

- 在 AWS 雲端環境：
  - 如果您計畫使用 AWS API，安裝應用程式到實例的 IAM 角色被設定。
  - 在每個 Amazon EC2 實例上，Systems Manager Agent（SSM 代理）被安裝且正在執行。
  - SSM 代理啟用卡巴斯基安全管理中心以自動安裝應用程式到裝置和裝置群組，而不是每次都請求管理員確認。
  - 在執行 Windows 作業系統和從晚於 2016 年 11 月的 AMIs 佈署的實例上，SSM 代理被安裝並正在執行。您將必須在所有其他裝置上手動安裝 SSM 代理。關於更多安裝 SSM 代理到執行 Windows 和 Linux 作業系統的裝置的詳情，請參考 AWS 說明頁面。
- 在 Microsoft Azure 雲端環境：
  - 在每個 Azure 虛擬機，Azure VM Agent 被安裝且正在執行。

    預設下，新虛擬機被建立時帶有 Azure VM Agent，且您不必安裝或手動啟用它。請參考 Microsoft 說明頁面以獲得關於在 Windows 裝置和在 Linux 裝置上的 Azure VM Agent 詳情。
  - 您的 Azure 應用程式 ID 具有以下角色：
    - 閱讀者（使用網路輪詢發現虛擬機）
    - 虛擬機建立者（佈署防護到虛擬機）
    - SQL Server 建立者（在 Microsoft Azure 環境中使用 SQL 資料庫）

    如果您要執行所有操作，分配所有三個角色到您的 Azure 應用程式 ID。

建立設定雲端環境所需的安裝套件

如果您具有以下程式的安裝軟體套件和管理外掛程式，則可以使用卡巴斯基安全管理中心中的設定雲端環境精靈：

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Windows

  在雲端環境中部署 Kaspersky Endpoint Security for Windows 將在最近發佈 Kaspersky Endpoint Security 12.0 for Windows 後可用。
- Kaspersky Security for Windows Server

在您想要防護的實例上或虛擬機上安裝應用程式需要這些安裝套件。如果沒有這些安裝套件，則必須建立安裝套件。否則，設定雲端環境精靈無法工作。

要建立安裝套件：

1. 在卡巴斯基網站上下載應用程式和外掛程式的最新版本：
   - Kaspersky Security for Windows Server 的安裝程式和管理外掛程式。
   - 安裝程式是透過卡巴斯基安全管理中心進行遠端安裝的檔案，也是適用於 Kaspersky Endpoint Security for Linux 的管理外掛程式。
2. 將所有檔案儲存在安裝了管理伺服器的實例（或虛擬機器）上。
3. 從所有套件中擷取檔案。
4. 啟動卡巴斯基安全管理中心。
5. 從主控台樹狀目錄前往**進階** → **遠端安裝** → **安裝套件**，然後點擊**建立安裝套件**。
6. 選取**建立卡巴斯基安裝套件**。
7. 指定套件的名稱和應用程式安裝程式的路徑：<folder>\<file name>.kud，然後點擊**下一步**。
8. 閱讀最終使用者產品授權協議，並選取確認接受其條款的核取方塊，然後點擊**下一步**。

安裝套件將被上傳到管理伺服器，並將在安裝套件清單中提供。

一旦您建立了安裝套件並在管理伺服器上安裝了管理外掛程式，設定雲端環境即可使用。

設定雲端環境

要使用設定環境精靈配置卡巴斯基安全管理中心，您必須擁有以下事項：

- 以下為適用於雲端環境的特定憑證：
  - 已授予輪詢雲端區段的 IAM 角色或已授予輪詢雲端區段權利的 IAM 使用者帳戶（搭配 Amazon Web Services 使用）
  - Azure 應用程式 ID、密碼和訂閱（搭配 Microsoft Azure 使用）
  - Google 用戶端電子郵件、Project ID 與私密金鑰（搭配 Google Cloud 使用）
- 安裝套件：
  - Windows 網路輪詢
  - Linux 網路輪詢
  - Kaspersky Endpoint Security for Linux

- Kaspersky Endpoint Security for Linux 的 Web 外掛程式
- 至少以下一項：
  - Kaspersky Endpoint Security for Windows 的安裝套件和 Web 外掛程式（建議）
  - Kaspersky Security for Windows Server 的安裝套件和 Web 外掛程式

如果您不想使用雲端環境功能（如果，例如，您僅要管理實體用戶端裝置的防護），您可以關閉設定雲端環境並手動執行標準管理伺服器快速啟動精靈。

設定雲端環境操作在透過管理主控台第一次連線到管理伺服器時自動啟動，如果您正在從現成映像佈署卡巴斯基安全管理中心。您還可以在任意時刻手動啟動設定雲端環境精靈。

要手動啟動設定雲端環境精靈：

1. 在主控台樹狀目錄中，選取**管理伺服器**節點。
2. 在節點的上下文功能表中，選取**All Tasks → 設定雲端環境**。

平均連線時間約 15 分鐘。

關於設定雲端環境精靈

設定雲端環境精靈允許您配置卡巴斯基安全管理中心以在雲端環境中工作。

該精靈建立以下物件：

- 帶有預設設定的網路代理政策
- Kaspersky Endpoint Security for Linux 政策
- Kaspersky Security for Windows Server 政策
- 實例管理群組和自動移動實例到該管理群組的規則
- 管理伺服器資料備份工作
- 在執行 Linux 和 Windows 的裝置上安裝防護的工作
- 每個受管理裝置的工作：
  - 快速惡意軟體掃描
  - 更新下載

如果您選取了 BYOL 產品授權選項，設定雲端環境也會使用金鑰檔案或啟動碼啟動卡巴斯基安全管理中心，並將金鑰檔案或啟動碼放置到產品授權儲存中。

步驟 1：選取應用程式啟動方式

如果您註冊了現成的 AMI 之一（在 AWS Marketplace），或註冊了基於使用情況的按月計費的 SKU（在 Azure 市集），則不會顯示此步驟。在這種情況下，精靈會立即進行下一步。然而，您無法為 Google Cloud 購買現成的 AMI。

如果您為卡巴斯基安全管理中心選取了BYOL 產品授權選項，精靈提示您選取應用程式啟動方法。

使用啟動碼 / Kaspersky Security for Virtualization 或 Kaspersky Hybrid Cloud Security 的金鑰檔案啟動應用程式。

您可以透過以下的方式啟動應用程式：

- 透過輸入啟動碼。

  線上啟動將開始。該過程涉及對指定的啟動碼的驗證，以及對金鑰檔案的發佈和啟動。

- 透過指定金鑰檔案。

  應用程式將檢查金鑰檔案，如果它包含正確資訊則啟動，或提示您指定其他金鑰檔案。

卡巴斯基安全管理中心放置授權金鑰到產品授權儲存區並標記它為自動分發的金鑰。

如果您使用標準 Microsoft Windows Remote Desktop Connection 或相似應用程式連線到實例，在遠端連線內容中您必須指定用以連線的實體裝置磁碟機。這確保了您實體裝置上的實例到檔案的存取，並且允許您選取和指定金鑰檔案。

當使用從付費 AMI 佈署的卡巴斯基安全管理中心時，或者對於依使用情況計費且按月付費的 SKU，您無法新增金鑰檔案或啟動碼到產品授權儲存區。

步驟 2：選取雲端環境

選取您佈署卡巴斯基安全管理中心的雲端環境：AWS、Azure 或 Google 雲端。

步驟 3：在雲端環境中授權

AWS

如果您選取了 AWS，指定您具有帶有所需權限的 IAM 角色，或者提供給卡巴斯基安全管理中心一個 AWS IAM 存取金鑰。沒有 IAM 角色或 AWS IAM 存取金鑰，雲端區段輪詢不可用。

為將來輪詢雲端區段所使用的連線指定以下設定：

- **連線名稱**

  輸入連線名稱。名稱不能包括 256 個以上字元。僅允許 Unicode 字元。

  該名稱也將用作雲端裝置的管理群組名稱。

  若您計畫處理多個雲端環境，您可能想要在連線名稱中納入環境名稱，例如「Azure 區段」、「AWS 區段」或「Google 區段」。

- **使用 AWS IAM 角色**

  如果您已經為管理伺服器建立了 IAM 角色以使用 AWS 服務，則選取該方塊。

- **使用 AWS IAM 使用者帳戶**

  如果您擁有帶有必要權限的 IAM 使用者帳戶且您可以輸入金鑰 ID 和金鑰，則選取該方塊。

  - **存取金鑰 ID**

    IAM 存取金鑰 ID 是個字母數字序列。當您在建立 IAM 使用者帳戶時接收金鑰 ID。

    如果您選取了 AWS IAM 存取金鑰來授權而不是 IAM 角色，該欄位可用。

  - **金鑰**

    您建立 IAM 使用者帳戶時接收到的帶有存取金鑰 ID 的金鑰。

    金鑰的字元顯示為星號。在您開始輸入金鑰後，**顯示**按鈕被顯示。按一下並按住該按鈕一定時間以檢視輸入的字元。

    如果您選取了 AWS IAM 存取金鑰來授權而不是 IAM 角色，該欄位可用。

該連線儲存在應用程式設定。您只能使用配置雲端環境建立一個 AWS IAM 存取金鑰。後續，您可以指定更多的連線以管理其他雲端區段。

如果您要透過卡巴斯基安全管理中心安裝應用程式到實例，您必須確保您的 IAM 角色（或與您輸入的金鑰關聯的帳戶的 IAM 使用者）具有所有必要權限。

Azure

如果您選取了 Azure，為將來輪詢雲端區段所使用的連線指定以下設定：

- **連線名稱**

  輸入連線名稱。名稱不能包括 256 個以上字元。僅允許 Unicode 字元。

  該名稱也將用作雲端裝置的管理群組名稱。

  若您計畫處理多個雲端環境，您可能想要在連線名稱中納入環境名稱，例如「Azure 區段」、「AWS 區段」或「Google 區段」。

- **Azure 應用程式 ID**

  您在 Azure 網站建立了該應用程式 ID。

  您僅可以提供一個 Azure 應用程式 ID 用於輪詢和其他目的。如果您要輪詢其他 Azure 段，您必須先刪除現有 Azure 連線。

- **Azure 訂購 ID**

  您在 Azure 網站建立了該訂購。

- **Azure 應用程式密碼**

  當您建立應用程式 ID 時您收到應用程式 ID 的密碼。

  密碼的字元顯示為星號。在您開始輸入密碼後，**顯示**按鈕可用。按一下並按住該按鈕以檢視您輸入的字元。

- **Azure 儲存帳戶名稱**

  您建立了 Azure 儲存帳戶名稱以使用卡巴斯基安全管理中心。

- **Azure 儲存存取金鑰**

  您建立 Azure 儲存帳戶以使用卡巴斯基安全管理中心時接收密碼（金鑰）。

  金鑰在“Azure 儲存帳戶概述”區域的“金鑰”子區域可用。

該連線儲存在應用程式設定。

Google 雲端

如果您選取了 Google 雲端，為將來輪詢雲端區段所使用的連線指定以下設定：

- **連線名稱**

  輸入連線名稱。名稱不能包括 256 個以上字元。僅允許 Unicode 字元。

  該名稱也將用作雲端裝置的管理群組名稱。

  若您計畫處理多個雲端環境，您可能想要在連線名稱中納入環境名稱，例如「Azure 區段」、「AWS 區段」或「Google 區段」。

- **用戶端電子郵件**

  輸入您用來在 Google Cloud 註冊專案的電子郵件。

- **專案 ID**

  專案 ID 是您在 Google Cloud 註冊專案時收到的 ID。

- **私密金鑰**

  私密金鑰是您在 Google Cloud 註冊專案時作為私密金鑰收到的字元序列。您可能會想要複製並貼上此序列，以免出錯。

該連線儲存在應用程式設定。

步驟 4：配置與雲端的同步並選取後續操作

在該步驟，雲端區段輪詢開始，實例的特別管理群組被建立。輪詢中發現的實例被放置在該群組。雲端區段輪詢排程被設定（預設每 5 分鐘）。

與雲端同步自動移動規則也被建立。對於每個雲端網路的後續掃描，系統都會將偵測到的虛擬裝置移動到**受管理裝置\雲端**群組的對應子群組。

在**與雲端區段同步**頁面上，您可定義以下設定：

- **與雲端區段同步管理群組結構**

  如果啟用該選項，**雲端**群組被自動建立在**受管理裝置**群組，雲端裝置發現被啟動。在每個雲端網路掃描中偵測到的實例和虛擬機被放置到雲端群組。該群組的管理子群組結構比對您的雲端區段結構（在 AWS 中，可用網域和放置群組不出現在結構中；在 Azure 中，子網路不出現在結構中）。未被識別為雲端環境中實例的裝置在**未配置的裝置**群組。該群組結構允許您使用群組安裝工作安裝病毒防護應用程式到實例，以及為不同群組設定不同的政策。

  如果停用該選項，**雲端**群組也被建立，且雲端裝置發現也被啟動；然而，比對雲端區段結構的子群組不在群組中被建立。所有偵測到的實例都在**雲端**管理群組，因此顯示在單一清單。如果您使用的卡巴斯基安全管理中心需要同步，您可以修改**與雲端同步**規則的內容並強制它。強加該規則改變雲端群組的子群組結構，以便比對您雲端區段的結構。

  預設情況下已停用該選項。

- **佈署防護**

  如果選取該選項，精靈建立工作以安裝安全應用程式到實例。精靈完成後，防護佈署精靈自動在您的雲端區段的裝置上啟動，並且您將可以在這些裝置上安裝網路代理和安全應用程式。

  卡巴斯基安全管理中心可以使用其本機工具執行佈署。如果您沒有權限安裝應用程式到 EC2 實例或 Azure 虛擬機，您可以手動設定**遠端安裝**工作並指定帶有所需權限的帳戶。此種情況下，遠端安裝工作將不用於使用 AWS API 或 Azure 發現的裝置。該工作將僅用於使用 Active Directory 輪詢、Windows 網域輪詢或 IP 範圍輪詢發現的裝置。

  如果未選取該選項，防護佈署精靈不被啟動，安裝安全應用程式的工作未在實例上被建立。您可以稍後手動執行這些操作。

若為 Google Cloud，您僅可執行搭配卡巴斯基安全管理中心原生工具的佈署。若您選擇 Google Cloud，則無法使用**佈署防護**選項。

步驟 5：在雲端環境中配置卡巴斯基安全網路

指定設定以轉發卡巴斯基安全管理中心操作資訊到卡巴斯基安全網路知識庫。您可以選取以下其中一個方法：

- **我同意使用卡巴斯基安全網路**

  安裝在用戶端裝置上的卡巴斯基安全管理中心與受管理應用程式會自動傳輸其作業詳情至卡巴斯基安全網路。參與卡巴斯基安全網路確保了包含病毒和其他威脅的資料庫的快速更新，該資料庫確保了對緊急安全威脅的快速回應。

- **我不同意使用卡巴斯基安全網路**

  卡巴斯基安全管理中心和受管理應用程式將不會提供資訊至卡巴斯基安全網路。

  若您選取此選項，則會停用卡巴斯基安全網路。

Kaspersky 建議您參與卡巴斯基安全網路。

步驟 6：在雲端環境中配置電子郵件通知

在該視窗中，您可以設定如何傳遞 Kaspersky 應用程式在虛擬用戶端裝置上操作時記錄的事件通知。這些設定將被用作應用程式政策的預設設定。

要配置發生在 Kaspersky 應用程式上的事件的通知傳送，使用以下設定：

- **收件者 (電子郵件信箱)**

  應用程式將給其傳送通知的使用者的郵件位址。您可以輸入一個或更多位址；如果您輸入多個位址，使用分號分隔。

- **SMTP 伺服器**

  您組織郵件伺服器的位址。

  如果您輸入多個位址，使用分號分隔。您可以使用以下參數：

  - IPv4 或 IPv6 位址
  - 裝置的 Windows 網路名稱（NetBIOS 名稱）
  - SMTP 伺服器的 DNS 名稱

- **SMTP 伺服器連接埠**

  SMTP 伺服器的通訊埠號。如果您使用多部 SMTP 伺服器，則會透過指定的通訊連接埠與它們建立連線。預設埠號為 25。

- **使用 ESMTP 身分驗證**

  啟用 ESMTP 身分驗證支援。當選取了該核取方塊時，您可以在**使用者名稱**和**密碼**欄位指定 ESMTP 身分驗證設定。預設情況下已清空此方塊。

您可以透過按一下**傳送測試訊息**按鈕測試新郵件通知設定。如果測試訊息被**收件者（電子郵件信箱）**欄位中指定的位址成功接收，裝置被正確設定。

步驟 7：建立雲端環境保護的初始配置

在該步驟，卡巴斯基安全管理中心自動建立政策和工作。**設定初始化防護**視窗顯示應用程式建立的政策和工作清單。

如果您在 AWS 雲端環境中使用 RDS 資料庫，當管理伺服器備份工作被建立時，您必須提供 IAM 存取金鑰對給卡巴斯基安全管理中心。此種情況下，填充以下欄位：

- **S3 bucket 名稱**

  您為備份建立的 S3 bucket 名稱。

- **存取金鑰 ID**

  當您建立了 IAM 使用者帳戶以使用 S3 bucket 儲存實例時，您接收到金鑰 ID（數字字母序列）。

  如果您在 S3 bucket 上選取了 RDS 資料庫則該欄位可用。

- **金鑰**

  您建立 IAM 使用者帳戶時接收到的帶有存取金鑰 ID 的金鑰。

  金鑰的字元顯示為星號。在您開始輸入金鑰後，**顯示**按鈕被顯示。按一下並按住該按鈕一定時間以檢視輸入的字元。

  如果您選取了 AWS IAM 存取金鑰來授權而不是 IAM 角色，該欄位可用。

如果您在 Azure 雲端環境中使用 Azure SQL 資料庫，當管理伺服器備份工作被建立時，您必須提供您的 Azure SQL Server 資訊給卡巴斯基安全管理中心。此種情況下，填充以下欄位：

- **Azure 儲存帳戶名稱**

  您建立了 Azure 儲存帳戶名稱以使用卡巴斯基安全管理中心。

- **Azure 訂購 ID**

  您在 Azure 網站建立了該訂購。

- **Azure 應用程式密碼**

  當您建立應用程式 ID 時您收到應用程式 ID 的密碼。

  密碼的字元顯示為星號。在您開始輸入密碼後，**顯示**按鈕可用。按一下並按住該按鈕以檢視您輸入的字元。

- **Azure 應用程式 ID**

  您在 Azure 網站建立了該應用程式 ID。

  您僅可以提供一個 Azure 應用程式 ID 用於輪詢和其他目的。如果您要輪詢其他 Azure 段，您必須先刪除現有 Azure 連線。

- **Azure SQL Server 名稱**

  名稱和資源群組在您的 Azure SQL Server 內容中可用。

- **Azure SQL Server 資源群組**

  名稱和資源群組在您的 Azure SQL Server 內容中可用。

- **Azure 儲存存取金鑰**

  在您的儲存帳戶內容中可用，在存取金鑰區域。您可以使用任何金鑰（key1 或 key2）。

若您正在 Google 雲端中佈署管理伺服器，則必須選取將會儲存備份副本的資料夾。選取本機裝置上的資料夾或虛擬機實例上的資料夾。

下一步按鈕在建立完最小防護設定所需的所有政策和工作後可用。

如果要執行工作的裝置對管理伺服器不可見，則工作僅當裝置可見時啟動。如果您建立新 EC2 實例或新 Azure 虛擬機，可能需要一些時間使其對管理伺服器可見。如果您想把網路代理和安全應用程式立即安裝在所有新建立的裝置，確保**執行略過的工作**選項對**遠端安裝應用程式**工作啟用。否則，新建立的實例/虛擬機將不會獲得網路代理和安全應用程式，直到工作根據排程啟動。

步驟 8：選取安裝過程中必須重啟操作系統時的動作（針對雲端環境）

如果您先前已選取**佈署防護**，您必須在目標裝置作業系統重新啟動時選取要進行的操作。如果您未選取**佈署防護**選項，則會略過此步驟。

選取在安裝應用程式過程中裝置作業系統必須重新啟動時是否重新啟動實例：

- **不重新啟動裝置**

  如果選取該選項，安全應用程式安裝後裝置不被重新啟動。

- **重新啟動裝置**

  如果選取該選項，安全應用程式安裝後裝置將被重新啟動。

如果您要在重新啟動前強制關閉所有鎖定連線中的應用程式，選取**強行關閉鎖定連線中的應用程式**核取方塊。如果該核取方塊被清空，您將必須手動關閉所有鎖定連線中的應用程式。

步驟 9：透過管理伺服器接收更新

在此步驟，您可以檢視下載管理伺服器正確操作所需的必要更新的進度。您可以點擊**下一步**按鈕以轉到精靈的最後頁面，而不等待下載完成。

精靈結束。

檢查設定

要檢查是否卡巴斯基安全管理中心 14.2 被正確設定以工作在雲端環境：

1. 啟動卡巴斯基安全管理中心且確保您可以透過管理主控台連線到管理伺服器。
2. 在主控台樹狀目錄中，選取**受管理裝置\雲端**。
3. 當在**受管理裝置\雲端**群組檢視任意子群組時，確保**裝置**頁籤顯示子群組的所有裝置。
   如果裝置未顯示，您可以手動輪詢對應的雲端區段以尋找它們。
4. 確保**政策**頁籤對以下應用程式具有啟用政策：
   - 卡巴斯基安全管理中心網路代理
   - Kaspersky Security for Windows Server
   - Kaspersky Endpoint Security for Linux

   如果它們未列出，您可以手動建立它們。
5. 確保**工作**頁籤列出以下工作：
   - **備份管理伺服器資料**
   - **Windows Server 更新工作**
   - **管理伺服器維護**
   - **將更新下載至管理伺服器儲存區**
   - **弱點掃描和所需更新**
   - **為 Windows 安裝防護**
   - **為 Linux 安裝防護**
   - **Windows Server 快速掃描工作**
   - **快速掃描**
   - **為 Linux 安裝更新**

   如果它們未列出，您可以手動建立它們。

卡巴斯基安全管理中心 14.2 被正確配置以工作在雲端環境：

雲端裝置群組

您可以將雲端裝置合併為群組，以管理雲端裝置。在卡巴斯基安全管理中心初始化配置階段會預設建立**受管理裝置\雲端**管理群組，且會放置輪詢中偵測到的雲端裝置到該群組。

如果您在配置同步時選擇了將**與雲端區段同步管理群組結構**選項，則該管理群組中的子組結構與您的雲端區段結構相同。（不過，在 AWS 中，可用區和歸置組未在結構中表示；在 Microsoft Azure 中，子網路未在結構中表示。）輪詢期間偵測到的群組內的空子組將被自動刪除。

您還可以透過組合所有或指定裝置手動建立管理群組。

依預設，**受管理裝置\雲端**群組會從**受管理裝置**群組繼承政策和工作。如果在對應政策和工作的內容設定中選取了**編輯已允許**核取方塊，您可以變更設定。

網路段輪詢

管理伺服器透過使用 AWS API、zure API 或 Google API 工具對雲端區段進行一般輪詢來接收有關該網路中網路和裝置的結構的資訊。卡巴斯基安全管理中心使用該資訊更新**未配置的裝置**和**受管理裝置**資料夾的內容。如果您配置了裝置自動移動到管理群組，偵測到的裝置將被包含在管理群組中。

若要允許管理伺服器輪詢雲端區段，您必須對 IAM 角色或 IAM 使用者帳戶（在 AWS 中）或對應用程式 ID 和密碼（在 Azure 中）或對 Google 用戶端電子郵件、Google 專案 ID 和私密金鑰提供權限。

您可以新增或刪除連線，以及為每個雲端區段設定輪詢排程。

為雲端區段輪詢新增連線

要新增雲端區段輪詢連線到可用連線清單：

1. 在主控台樹狀目錄中，選取**裝置發現 → 雲端**節點。
2. 在該視窗的工作區，點擊**設定輪詢**。

   包含雲端區段輪詢的可用連線清單的內容視窗開啟。
3. 點擊**"新增"**按鈕。

   連線視窗將開啟。

4. 為將來輪詢雲端區段所使用的連線指定雲端環境名稱：

雲端環境

EC2 實例 (或虛擬機器) 所在環境可以是 Amazon Web Services (AWS)、Microsoft Azure 或 Google Cloud。

若您選取了 AWS，請指定下列設定：

- **連線名稱**

  輸入連線名稱。名稱不能包括 256 個以上字元。僅允許 Unicode 字元。

  該名稱也將用作雲端裝置的管理群組名稱。

  若您計畫處理多個雲端環境，您可能想要在連線名稱中納入環境名稱，例如「Azure 區段」、「AWS 區段」或「Google 區段」。

- **使用 AWS IAM 角色**

  如果您已經為管理伺服器建立了 IAM 角色以使用 AWS 服務，則選取該方塊。

- **使用 AWS IAM 使用者帳戶**

  如果您擁有帶有必要權限的 IAM 使用者帳戶且您可以輸入金鑰 ID 和金鑰，則選取該方塊。

  - **存取金鑰 ID**

    IAM 存取金鑰 ID 是個字母數字序列。當您在建立 IAM 使用者帳戶時接收金鑰 ID。

    如果您選取了 AWS IAM 存取金鑰來授權而不是 IAM 角色，該欄位可用。

  - **金鑰**

    您建立 IAM 使用者帳戶時接收到的帶有存取金鑰 ID 的金鑰。

    金鑰的字元顯示為星號。在您開始輸入金鑰後，**顯示**按鈕被顯示。按一下並按住該按鈕一定時間以檢視輸入的字元。

    如果您選取了 AWS IAM 存取金鑰來授權而不是 IAM 角色，該欄位可用。

設定雲端環境精靈僅允許您指定單個 AWS IAM 存取金鑰。後續，您可以指定更多的連線以管理其他雲端區段。

若您選取了 Azure，請指定下列設定：

- **連線名稱**

  輸入連線名稱。名稱不能包括 256 個以上字元。僅允許 Unicode 字元。

  該名稱也將用作雲端裝置的管理群組名稱。

  若您計畫處理多個雲端環境，您可能想要在連線名稱中納入環境名稱，例如「Azure 區段」、「AWS 區段」或「Google 區段」。

- **Azure 應用程式 ID**

  您在 Azure 網站建立了該應用程式 ID。

  您僅可以提供一個 Azure 應用程式 ID 用於輪詢和其他目的。如果您要輪詢其他 Azure 段，您必須先刪除現有 Azure 連線。

- **Azure 訂購 ID**

  您在 Azure 網站建立了該訂購。

- **Azure 應用程式密碼**

  當您建立應用程式 ID 時您收到應用程式 ID 的密碼。

  密碼的字元顯示為星號。在您開始輸入密碼後，**顯示**按鈕可用。按一下並按住該按鈕以檢視您輸入的字元。

- **Azure 儲存帳戶名稱**

  您建立了 Azure 儲存帳戶名稱以使用卡巴斯基安全管理中心。

- **Azure 儲存存取金鑰**

  您建立 Azure 儲存帳戶以使用卡巴斯基安全管理中心時接收密碼（金鑰）。

  金鑰在“Azure 儲存帳戶概述”區域的“金鑰”子區域可用。

若您選取了 Google 雲端，請指定下列設定：

- **連線名稱**

  輸入連線名稱。名稱不能包括 256 個以上字元。僅允許 Unicode 字元。

  該名稱也將用作雲端裝置的管理群組名稱。

  若您計畫處理多個雲端環境，您可能想要在連線名稱中納入環境名稱，例如「Azure 區段」、「AWS 區段」或「Google 區段」。

- **用戶端電子郵件**

  輸入您用來在 Google Cloud 註冊專案的電子郵件。

- **專案 ID**

  專案 ID 是您在 Google Cloud 註冊專案時收到的 ID。

- **私密金鑰**

私密金鑰是您在 Google Cloud 註冊專案時作為私密金鑰收到的字元序列。您可能會想要複製並貼上此序列，以免出錯。

5. 如果您想，選取**設定輪詢排程**和變更預設設定。

該連線儲存在應用程式設定。

第一次輪詢新雲端區段後，與該段對應的子群組會出現在**受管理裝置\雲端**管理群組。

如果您指定不正確的憑證，在雲端區段輪詢過程中將不會發現實例，且新子群組將不會出現在**受管理裝置\雲端**管理群組。

為雲端區段輪詢刪除連線

如果您不再必須輪詢特定雲端區段，您可以從可用連線清單刪除對應於段的連線。您還可以刪除連線，如果，例如輪詢雲端區段的權限被轉移給另一個帶有不同金鑰的 AWS IAM 使用者。

要刪除連線：

1. 在主控台樹狀目錄中，選取**裝置發現 → 雲端**節點。
2. 在該視窗的工作區，選取**設定輪詢**。
   包含雲端區段輪詢的可用連線清單的視窗開啟。
3. 選取您要刪除的連線並點擊視窗右側的**刪除**按鈕。
4. 在開啟的視窗中，點擊**確定**按鈕以確認您的選取。

如果您正從可用連線清單中刪除連線，相應段中的裝置被自動從對應的管理群組刪除。

配置輪詢排程

雲端區段輪詢依據排程執行。您可以設定輪詢頻率。

輪詢頻率被在設定雲端環境設定中自動設定為 5 分鐘。您可以在任意時刻變更該值並設定不同的排程。但不建議您設定比每 5 分鐘一次還要多的輪詢頻率，因為這可能導致 API 操作錯誤。

要設定雲端區段輪詢排程：

1. 在主控台樹狀目錄中，選取**裝置發現 → 雲端**節點。
2. 在工作區點擊**設定輪詢**。
   雲端內容視窗開啟。
3. 在清單中，選取您要的連線並按一下**內容**按鈕。
   連線內容視窗開啟。

4. 在內容視窗，按一下**設定輪詢排程**連結。

   排程視窗將開啟。

5. 定義下列設定：

   - **排程開始**

     輪詢排程選項：

     - **每 N 天**

       輪詢定期執行，按照指定天數間隔，從指定的日期和時間開始。

       預設下，輪詢每天執行一次，從目前系統日期和時間開始。

     - **每 N 分鐘**

       輪詢定期執行，按照指定分鐘間隔，從指定的時間開始。

       預設下，輪詢每五分鐘執行一次，從目前系統時間開始。

     - **周中天數**

       輪詢定期執行，在指定星期的指定時間。

       預設下，輪詢會每週五下午 6:00:00 執行。

     - **每個月所選週的指定日**

       輪詢定期執行，在指定月日的指定時間。

       預設下，未選取月日；預設啟動時間是 6:00:00 P.M.。

   - **執行略過的工作**

     如果在排程輪詢期間管理伺服器被切換掉或不可用，管理伺服器可以在切換回來後立即啟動輪詢，或者等待下次排程輪詢。

     如果啟用該選項，管理伺服器在它切換回來後立即啟動輪詢。

     如果停用該選項，管理伺服器等待下一次排程輪詢。

     預設情況下已啟用該選項。

6. 按一下**確定**儲存變更。

   輪詢排程被設定並儲存。

安裝應用程式到雲端環境中的裝置

您可以安裝以下 Kaspersky 應用程式到雲端環境中的裝置：Kaspersky Security for Windows Server（對於 Windows 裝置）和 Kaspersky Endpoint Security for Linux（對於 Linux 裝置）。

您要安裝防護的用戶端裝置必須滿足在雲端環境中操作卡巴斯基安全管理中心的需求。您必須擁有有效產品授權以安裝應用程式到 AWS 實例和 Microsoft Azure 虛擬機或 Google 虛擬機實例。

卡巴斯基安全管理中心 14.2 支援以下情境：

- 用戶端裝置會透過 API 探索；安裝也會透過 API 執行。若為 AWS 和 Azure 雲端環境，則支援此情境。
- 用戶端裝置透過活動目錄輪詢、Windows 網域輪詢或 IP 範圍輪詢被發現；安裝透過卡巴斯基安全管理中心執行。
- 用戶端裝置會透過 Google API 探索；安裝則會透過卡巴斯基安全管理中心執行。若為 Google Cloud，則僅支援此情境。

應用程式的其他安裝方法不被支援。

要在虛擬裝置上安裝應用程式，使用安裝套件。

要建立工作以遠端安裝應用程式到實例或透過使用 AWS API 或 Azure API：

1. 在主控台樹狀目錄中，選取**工作**資料夾。
2. 點擊**新工作**按鈕。

   新工作精靈啟動。遵照精靈的說明。
3. 在**選取工作類型**頁面中，將**遠端安裝應用程式**選取為工作類型。

4. 在**選取裝置**頁面中，從**受管理裝置\雲端**群組選取相關裝置。

5. 如果尚未安裝網路代理在您要安裝應用程式的裝置，請在**選取要執行此工作的帳戶**頁面選取**需要帳戶（不使用網路代理）**並在視窗右側點擊**新增**按鈕。在出現的功能表中，選取以下項：

- **雲端帳戶**

  如果您要安裝應用程式到 AWS 環境中的實例，且您擁有帶有所需權限的 AWS IAM 存取金鑰，但不擁有 IAM 角色，請選取該選項。如果您要安裝應用程式到 Azure 環境中的裝置，也選取該選項。

  在開啟的視窗中提供卡巴斯基安全管理中心憑證以獲取安裝應用程式到相關實例的權限。

  選取雲端環境：AWS 或 Azure。

  在**帳戶名稱**欄位，輸入這些憑證的名稱。此名稱將會顯示在要執行該工作的帳戶清單中。

  如果您選取了 AWS，在**存取金鑰 ID** 和**金鑰**欄位，輸入有權安裝應用程式到指定裝置的 IAM 使用者帳戶憑證。

  如果您選取了 Azure，在 **Azure 訂購 ID**和 **Azure 應用程式密碼**欄位，輸入有權安裝應用程式到指定裝置的 Azure 帳戶憑證。

  如果您指定錯誤的憑證，遠端安裝工作將在所排程的裝置上返回錯誤。

- **帳戶**

  對於執行 Windows 的實例，在您不想使用 AWS 或 Azure API 工具安裝應用程式時選取該選項。此種情況下，確保您雲端區段中的裝置滿足必要條件。卡巴斯基安全管理中心自行安裝應用程式，而不使用 AWS API 或 Azure API。

  如果您指定錯誤的資料，遠端安裝工作將在所排程的裝置上返回錯誤。

- **IAM 角色**

  如果您想安裝應用程式到 AWS 環境且擁有帶有所需權限的 IAM 角色，選取該選項。

  如果您選取該選項，但不擁有帶有所需權限的 IAM 角色，遠端安裝工作將在所排程的裝置上返回錯誤。

- **SSH 憑證**

  對於執行 Linux 的實例，在您不想使用 AWS API 或 Azure API 工具安裝應用程式時，請選取該選項。此種情況下，確保您雲端區段中的裝置滿足必要條件。卡巴斯基安全管理中心自行安裝應用程式，而不使用 AWS API 或 Azure API。

  要指定 SSH 憑證的私密金鑰，您可以使用 ssh-keygen 公用程式來產生這個金鑰。請注意，卡巴斯基安全管理中心支援 PEM 格式的私密金鑰，但 ssh-keygen 公用程式預設為產生 OPENSSH 格式的 SSH 金鑰。卡巴斯基安全管理中心不支援 OPENSSH 格式。要以支援的 PEM 格式建立私密金鑰，請在 ssh-keygen 命令中加入 `-m PEM` 選項。例如：

  ```
  ssh-keygen -m PEM -t rsa -b 4096 -C "< 使用者電子郵件 >"
  ```

您可以為每個實例透過按一下**新增**按鈕提供多個憑證。如果不同的雲端區段需要不同的憑證，則為所有段提供憑證。

在精靈結束後，應用程式的遠端安裝工作會顯示在**工作**資料夾工作區的工作清單中。

在 Microsoft Azure 中，遠端安裝安全應用程式到虛擬機可能導致刪除安裝在該虛擬機上的自訂指令碼延伸程式。

檢視雲端裝置內容

若要檢視雲端裝置內容：

1. 在主控台樹狀目錄的**裝置發現 → 雲端**節點中，選取相關實例所在群組對應的子節點。
   如果您不知道相關虛擬裝置所在的群組，使用搜尋功能：
   a. 右鍵點擊**受管理裝置 → 雲端**節點，然後在內容功能表中選取**搜尋** 。
   b. 在開啟的視窗中，執行搜尋。
      如果存在滿足您所設定的標準的裝置，它們名稱和詳情將顯示在視窗的下部。
2. 右擊相關節點的名稱。在右鍵選單中，選取**內容**。
   在開啟的視窗，物件內容被顯示。
   系統資訊 → 一般系統資訊區域包含雲端環境中裝置特定的內容：
   - **使用 API 發現的裝置**（**Amazon AWS**、**Azure** 或 **Google Cloud**；如果無法使用 API 工具檢測到該裝置，則會顯示 **No** 值）。
   - **雲端區域**。
   - **Cloud VPC**（僅適用於 AWS 和 Google Cloud 裝置）。
   - **雲端可用區域**（僅適用於 AWS 和 Google Cloud 裝置）。
   - **雲端子網路**。
   - **雲端位置群組** (此單元只會在實例屬於位置群組時顯示；否則，它將不會顯示)。

您可以點擊**匯出至檔案**按鈕匯出該資訊到 .csv 或 .txt 檔案。

與雲端同步

在設定雲端環境操作中，與雲端同步規則被自動建立。規則允許您從 **未配置的裝置**群組自動移動在輪詢中偵測到的實例到**受管理裝置\雲端**群組，使實例就可用於集中管理。預設下，規則在建立後被啟動。您可以在任意時刻停用、修改或強制規則。

要編輯與雲端同步規則的內容和/或強制規則：

1. 在主控台樹狀目錄中右擊**裝置發現**節點的名稱。
2. 在右鍵選單中，選取**內容**。

3. 在開啟的**內容**視窗中，在**區域**視窗選取**移動裝置**。

4. 在工作區的裝置移動規則清單中，選取**與雲端同步**，然後按一下視窗下部的**內容**按鈕。
   規則內容視窗隨即開啟。

5. 如果必要，在**雲端區段**設定群組指定以下設定：

- **裝置在雲端區段中**

  該規則僅套用到位於所選雲端區段的裝置。否則，該規則套用到發現的所有裝置。
  預設情況下已選定此選項。

  - **包含子物件**

    該規則套用到所選段和其所有嵌套雲端子區域中的所有裝置。否則，該規則僅套用到位於根段的裝置。
    預設情況下已選定此選項。

  - **將裝置從嵌套物件移動到對應子群組**

    如果啟用該選項，嵌套物件的裝置將被自動移動到對應其結構的子群組。
    如果停用該選項，嵌套物件的裝置將被自動移動到雲端子群組的根，而不再分支。
    預設情況下已啟用該選項。

    - **建立對應於新偵測到裝置的容器的子群組**

      如果啟用該選項，當**受管理裝置雲端**結構沒有比對包含裝置的區域的子群組，卡巴斯基安全管理中心將建立這類子群組。例如，如果一個子網在裝置發現中被發現，帶有相同名稱的新組將在**受管理裝置\雲端**群組下被建立。
      如果停用該選項，卡巴斯基安全管理中心不建立任何新子群組。例如，如果一個子網在網路輪詢中被發現，帶有相同名稱的新群組將不在**受管理裝置雲端**群組下被建立，且該子群組中的裝置將被移動到**受管理裝置雲端**群組。
      預設情況下已啟用該選項。

    - **刪除在雲端區段中找不到比對的子群組**

      如果啟用該選項，應用程式從雲端群組刪除所有不比對任何現有雲端物件的子群組。
      如果停用該選項，未比對任何現有雲端物件的子群組被保留。
      預設情況下已啟用該選項。

  如果您在執行設定雲端環境時啟用了**與雲端同步**選項，與雲端同步規則啟用**建立對應於新偵測到裝置的容器的子群組**和**刪除在雲端區段中找不到比對的子群組**核取方塊建立。
  如果您不啟用**與雲端同步**選項，與雲端同步規則停用（清空）這些核取方塊而建立。如果您的卡巴斯基安全管理中心需要**受管理裝置\雲端**子群組的結構與雲端區段結構比對，在規則內容中啟用**建立對應於新偵測到裝置的容器的子群組**和**刪除在雲端區段中找不到比對的子群組**選項，然後強制規則。

6. 在**使用 API 發現的裝置**下拉清單，選取以下值之一：
   - **AWS**。裝置使用 AWS API 發現，就是，裝置在 AWS 雲端環境中。
   - **Azure**。裝置使用 Azure API 發現，就是，裝置在 Azure 雲端環境中。
   - **Google Cloud**。裝置被使用 Google API 發現，即裝置一定在 Google 雲端環境中。
   - **否**。系統無法用 AWS、Azure 或 Google API 偵測裝置，意即裝置在雲端環境外或在雲端環境中，但無法使用 API 加以偵測。
7. **沒有值**。這項條件不適用。如果必要，在其他區域設定其他規則內容。
8. 如有必要，請點擊視窗下方的**強制**按鈕強制規則。

   規則執行精靈開始。遵照精靈的說明。當精靈結束後，規則將執行**受管理裝置\雲端**子群組的結構將與您的雲端區段結構比對。
9. 點擊**確定**按鈕。

   內容被設定並儲存。

要停用與雲端規則同步：

1. 在主控台樹狀目錄中右擊**裝置發現**節點的名稱。
2. 在右鍵選單中，選取**內容**。
3. 在開啟的**內容**視窗中，在**區域**視窗選取**移動裝置**。
4. 在工作區的裝置移動規則清單中，停用（清空）**與雲端同步**選項並按一下**確定**。

   規則被停用且不會再被套用。

卡巴斯基安全管理中心在 Yandex.Cloud 中的佈署

您可以在 Yandex.Cloud 中佈署卡巴斯基安全管理中心。僅適用於按使用付費模式；不支援雲端資料庫。

在 Yandex.Cloud 中，以下佈署方法適用於安全應用程式：

- 透過卡巴斯基安全管理中心的本機方式，即透過*遠端安裝*工作（僅當管理伺服器和要保護的虛擬機器位於同一網段時，才可以佈署安全程序）
- 透過佈署指令碼

若要在 Yandex.Cloud 中佈署卡巴斯基安全管理中心，您必須在 Yandex.Cloud 中擁有一個服務帳戶。您必須授予該帳戶 marketplace.meteringAgent 權限，並將該帳戶與虛擬機器建立關聯（如需詳細資訊，請參閱 https://cloud.yandex.com/en ）。

附錄

該部分提供了使用卡巴斯基安全管理中心的參考資訊和附加說明。

進階功能

該部分將說明卡巴斯基安全管理中心設計用於延伸集中式管理用戶端裝置上應用程式功能的一系列附加選項。

卡巴斯基安全管理中心自動化作業。klakaut 實用程式

您可以使用 klbackup 自動化卡巴斯基安全管理中心的操作。klakaut 實用程式及其說明系統位於卡巴斯基安全管理中心的安裝資料夾中。

自訂工具

卡巴斯基安全管理中心允許您建立*自訂工具*（以下亦簡稱為*工具*）清單 – 透過上下文功能表的**自訂工具**群組從管理主控台為用戶端裝置啟動的應用程式。清單中每個工具將與單獨的功能表指令（管理主控台使用該指令啟動與該工具相關的應用程式）相關聯。

應用程式將在管理員工作台中啟動。應用程式可接受將遠端用戶端裝置的內容作為命令列參數（NetBIOS 名稱、DNS 名稱、IP 位址）。到遠端裝置的連線可使用通道建立。

預設情況下，自訂工具清單包含每個用戶端裝置的下列服務程式：

- **遠端診斷**是卡巴斯基安全管理中心的遠端診斷公用程式。
- 透過使用名為**遠端桌面**的標準 Microsoft Windows 元件。
- **電腦管理**是標準的 Microsoft Windows 元件。

要新增或刪除自訂工具，或編輯其設定，

在用戶端裝置的上下文功能表中，選取**自訂工具 → 配置自訂工具**。

自訂工具視窗開啟。在此視窗中，您可以添加自訂工具或使用**新增**和**修改**按鈕編輯它們的設定。若要移除自訂工具，請點擊帶有紅色叉圖示（❌）.的按鈕。

網路代理磁碟克隆模式

克隆參考裝置的磁碟機是在新裝置上安裝軟體的流行方法。如果網路代理以標準模式執行在參考裝置的磁碟機上，會發生以下問題：

帶有網路代理的參考磁碟映像被佈署到新裝置後，它們以單一圖示顯示在管理主控台。該問題發生是因為在新裝置的克隆結果保持相同的內部資料，這將允許管理伺服器關聯裝置到管理主控台上的圖示。

一個特別的*網路代理磁碟克隆模式*允許您避免克隆後在管理主控台錯誤顯示新裝置的問題。在您透過克隆磁碟佈署軟體（帶有網路代理）到新裝置時使用該模式。

在磁碟克隆模式下，網路代理保持執行，但是不連線到管理伺服器。當結束克隆模式時，網路代理刪除內部資料，這將導致管理伺服器關聯多個裝置到管理主控台上的單一圖示。在完成參考裝置映射的克隆時，新裝置顯示在管理主控台內容中。

網路代理磁碟克隆模式使用方案

1. 管理員安裝網路代理到參考裝置。
2. 管理員使用 klnagchk 實用工具檢查網路代理到管理伺服器的連線。
3. 管理員啟用網路代理磁碟克隆模式。
4. 管理員安裝軟體和修補程式到裝置，並重新啟動所需的次數。
5. 管理員克隆參考裝置的硬碟磁碟機到任意數量的裝置。
6. 每個克隆的副本必須滿足以下條件：
   a. 裝置名稱必須變更。
   b. 裝置必須重新啟動。
   c. 磁碟克隆模式必須被停用。

使用 klmover 工具啟用和停用磁碟克隆模式

要啟用或停用網路代理磁碟克隆模式：

1. 在您必須克隆的安裝了網路代理的裝置上執行 klmover 工具。
   klmover 工具位於網路代理的安裝資料夾。
2. 要啟用磁碟克隆模式，請在 Windows 命令提示時輸入以下指令：
   `klmover -cloningmode 1`
   網路代理轉換到磁碟克隆模式。
3. 若需要求磁碟克隆模式的目前狀態，請在命令列提示處輸入以下指令：
   `klmover -cloningmode`
   工具顯示是否磁碟克隆模式已啟用或停用。
4. 要停用磁碟克隆模式，在實用程式命令列輸入以下指令：
   `klmover -cloningmode 0`

準備已安裝網路代理的參照裝置以建立作業系統映像

您可能希望建立已安裝網路代理之參照裝置的作業系統映像，之後在聯網裝置上佈署映像。在此情況下，您會建立參照裝置的作業系統映像，其中的網路代理尚未啟動。若您在建立作業系統映像前啟動參照裝置的網路代理，從參照裝置作業系統映像佈署的管理伺服器裝置身分識別將會發生問題。

若要準備參照裝置建立作業系統映像：

1. 確認 Windows 作業系統已安裝在參照裝置並且在該裝置上安裝您需要的其他軟體。
2. 在參照裝置上的 Windows 網路連線設定中，將參照裝置從已安裝卡巴斯基安全管理中心的網路斷開連線。
3. 在參照裝置上使用 setup.exe 檔案啟動本機安裝網路代理。
   卡巴斯基安全管理中心網路代理安裝精靈啟動。遵照精靈的說明。
4. 在精靈的**管理伺服器**頁面，指定管理伺服器 IP 位址。
   若您不知道管理伺服器確切位址，請輸入 localhost。您可稍後變更 IP 位址，方法是使用 klmover 實用程式搭配 `-address` 鍵值。
5. 在精靈的**啟動應用程式**頁面，停用**安裝期間啟動應用程式**選項。
6. 當網路代理安裝完成後，請勿先重新啟動裝置再建立作業系統映像。
   若您重新啟動裝置，您將需要重複準備參照裝置建立作業系統映像的整個過程。
7. 在參照裝置的命令行中，啟動 sysprep 公用程式並執行以下命令：
   `sysprep.exe /generalize /oobe /shutdown`。

參照裝置已做好建立作業系統映像的準備。

配置從檔案完整性監控接收訊息

類如 Kaspersky Security for Windows Server 或 Kaspersky Security for Virtualization Light Agent 的受管理應用程式從檔案完整性監控傳送訊息到卡巴斯基安全管理中心。卡巴斯基安全管理中心也允許您監控到系統重要元件（例如網頁伺服器和 ATM）的任何變更，並對系統的完整性的破壞做出回應。對於這些目的，您可以從檔案完整性監控元件接收訊息。檔案完整性監控元件允許您不僅監控裝置的檔案系統，也監控防火牆狀態和所連線硬體的狀態。

您必須配置卡巴斯基安全管理中心以從檔案完整性監控元件接收訊息，而不使用 Kaspersky Security for Windows Server 或 Kaspersky Security for Virtualization Light Agent。

要配置從檔案完整性監控接收訊息：

1. 開啟安裝了管理伺服器的裝置的登錄檔（例如，在**開始 → 執行**功能表使用 regedit 指令）。
2. 轉至以下分支：
   - 對於 32 位元系統：
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
   - 對於 64 位元系統：
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF

3. 建立鍵：

- 建立鍵 KLSRV_EVP_FIM_PERIOD_SEC 以指定計算所處理事件數量的時間段。指定下列設定：

  a. 指定 KLSRV_EVP_FIM_PERIOD_SEC 作為鍵名稱。

  b. 指定 DWORD 作為鍵類型。

  c. 指定介於 43 200 和 172 800 秒之間的時間區段值範圍。預設情況下，資訊重新整理間隔是 86 400 秒。

- 建立鍵 KLSRV_EVP_FIM_LIMIT 以限制指定時間段收到事件的數量。指定下列設定：

  a. 指定 KLSRV_EVP_FIM_LIMIT 作為鍵名稱。

  b. 指定 DWORD 作為鍵類型。

  c. 指定介於 2 000 和 50 000 的事件接收數量範圍。預設事件數量是 20 000。

- 建立鍵 KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC 以精確計算特定時間間隔的事件數量。指定下列設定：

  a. 指定 KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC 做為鍵名稱。

  b. 指定 DWORD 作為鍵類型。

  c. 指定介於 120 到 600 秒的值範圍。預設時間間隔為 300 秒。

- 建立鍵 KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC，以便在指定的時間段後，應用程式可以檢查在相應時間間隔內處理的事件數量是否少於指定限制。該檢查在達到接收事件的限制時執行。如果該條件被滿足，應用程式還原儲存事件到資料庫。指定下列設定：

  a. 指定 KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC 作為鍵名稱。

  b. 指定 DWORD 作為鍵類型。

  c. 指定介於 600 到 3 600 秒的值範圍。預設時間間隔為 1 800 秒。

如果鍵未建立，預設值被使用。

4. 重新啟動管理伺服器服務。

接收來自檔案完整性監控元件的事件的限制將被設定。您可在名為**在裝置上觸發頻率最高的檔案完整性監控器 / 系統完整性監控的十大規則**和**檔案完整性監控 / 系統完整性監控規則最常觸發的十大裝置**的報告中檢視檔案完整性監控元件的結果。

管理伺服器維護

管理伺服器維護可讓您釋放管理伺服器資料夾中的空間，並刪除不再需要的物件以減少資料庫容積。這有助於提高應用程式的效能和操作可靠性。我們建議您至少每週對管理伺服器進行一次維護。

管理伺服器維護透過專用工作執行。應用程式會在維護管理伺服器時執行以下操作：

- 從儲存資料夾中刪除不需要的資料夾與檔案。
- 從表格中刪除不必要的記錄（也稱為「懸空指標」）。
- 清除快取。
- 維護資料庫（如果您使用 SQL Server 或 PostgreSQL 作為 DBMS）：
  - 檢查資料庫是否存在錯誤（僅適用於 SQL Server）。
  - 重組資料庫索引。
  - 更新資料庫統計資訊。
  - 收縮資料庫（如果必要）。

*管理伺服器維護*工作支援MariaDB 版本 10.3 及更高版本。如果您使用 MariaDB 10.2 或更早的版本，管理員將必須自己維護此 DBMS。

要建立管理伺服器維護工作：

1. 在主控台樹狀目錄中，選取您要為其建立*管理伺服器維護*工作的管理伺服器節點。
2. 選取**工作**資料夾。
3. 在**工作**資料夾工作區中，點擊**新工作**按鈕。
   新工作精靈啟動。
4. 在精靈的**選取工作類型**視窗，選取**管理伺服器維護**作為工作類型，然後點擊**下一步**。
5. 如果您必須在維護過程中收縮管理伺服器資料庫，在精靈的**設定**視窗，選取**收縮資料庫**核取方塊。
6. 遵照剩餘的精靈說明。

新建立的工作顯示在**工作**資料夾工作區的工作清單。一個單一管理伺服器僅可以執行一個*管理伺服器維護*工作。如果已為管理伺服器建立了*管理伺服器維護*工作，則無法再建立新的*管理伺服器維護*工作。

存取公用 DNS 伺服器

如果無法使用系統 DNS 存取卡巴斯基伺服器，Kaspersky Security Center 可以按以下順序使用這些公用 DNS 伺服器：

1. Google Public DNS (8.8.8.8)
2. Cloudflare DNS (1.1.1.1)
3. Alibaba Cloud DNS (223.6.6.6)

4. Quad9 DNS (9.9.9.9)

5. CleanBrowsing (185.228.168.168)

對這些 DNS 伺服器的請求可能包含網域位址和管理伺服器的公用 IP 位址，因為應用程式建立了到 DNS 伺服器的 TCP/UDP 連線。如果卡巴斯基安全管理中心使用公用 DNS 伺服器，則資料處理受相關服務的隱私權政策約束。

要透過使用 klscflag 公用程式配置公共 DNS 的使用：

1. 使用管理員權限執行 Windows 命令提示符，然後將目前目錄變更為包含 klscflag 公用程式的目錄。klscflag 公用程式位於安裝管理伺服器的資料夾中。預設安裝路徑：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. 要停用公共 DNS 的使用，請執行以下指令：

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
   ```

3. 要啟用公共 DNS 的使用，請執行以下指令：

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
   ```

使用者通知方法視窗

在**使用者通知方式**視窗，您可以設定將憑證安裝到行動裝置的使用者通知：

- **在精靈中顯示連結**.如果您選取該選項，安裝套件的連結將顯示在行動裝置連線精靈的最後一步。
- **傳送連結到使用者**。如果您選取該選項，您可以指定通知使用者有關裝置連線的設定。

在設定的**透過電子郵件**群組，您可以使用電子郵件訊息設定安裝新憑證到他的/她的行動裝置的使用者通知。該通知方法僅在啟用 SMTP 伺服器時可用。

在設定的**透過簡訊**群組，您可以使用 SMS 設定安裝新憑證到他的/她的行動裝置的使用者通知。該通知方法僅在啟用 SMS 通知時可用。

在**透過電子郵件**和**透過簡訊**的設定群組中，點擊**編輯訊息**連結來檢視和編輯通知訊息（如有必要）。

“一般”區域

您可以在該區域中調整 Exchange ActiveSync 行動裝置的一般設定檔：

- **名稱**

  設定檔名稱。

- **允許不規則的裝置**

  如果啟用此選項，則無法存取所有 Exchange ActiveSync 政策設定的裝置也被允許連線到行動裝置伺服器。您可以使用連線管理 Exchange ActiveSync 行動裝置。例如，您可以設定密碼、配置傳送電子郵件或檢視裝置資訊，例如裝置 ID 或政策狀態。

  如果停用此選項，您將無法連線到行動裝置伺服器和管理 Exchange ActiveSync 行動裝置。

  預設情況下已啟用該選項。如果您不打算管理 Exchange ActiveSync 行動裝置並接收有關它們的資訊，可以停用此選項。

- **更新頻率（小時）**

  如果啟用該選項，該程式將按照輸入欄位中所指定時間間隔重新整理 Exchange ActiveSync 政策的相關資訊。

  如果停用該選項，有關 Exchange ActiveSync 政策的資訊不重新整理。

  預設開啟該選項，重新整理間隔為 1 小時。

裝置分類視窗

從**裝置分類**清單選擇分類。清單包含預定義分類和使用者建立的分類。

您可在 **裝置分類** 區段工作區檢視裝置分類的詳細資訊。

定義新物件名稱視窗

在該視窗，指定新建立物件的名稱。名稱不能包含多於 100 個字元並且不能包括任何特殊字元（"*<>-_?:\|）。

“應用程式類別”區域

在該區域，您可以配置用戶端裝置上應用程式類別的資訊發佈。

完整資料傳輸（對於網路代理 Service Pack 2 和更早版本）

如果選中此方塊，如果政策被變更，應用程式類別的所有資料被傳輸到用戶端裝置。該資料傳輸選項使用在 Network Agent Service Pack 2 和更早版本。

僅傳輸修改的資料（對於網路代理版本 Service Pack 2 和更新）

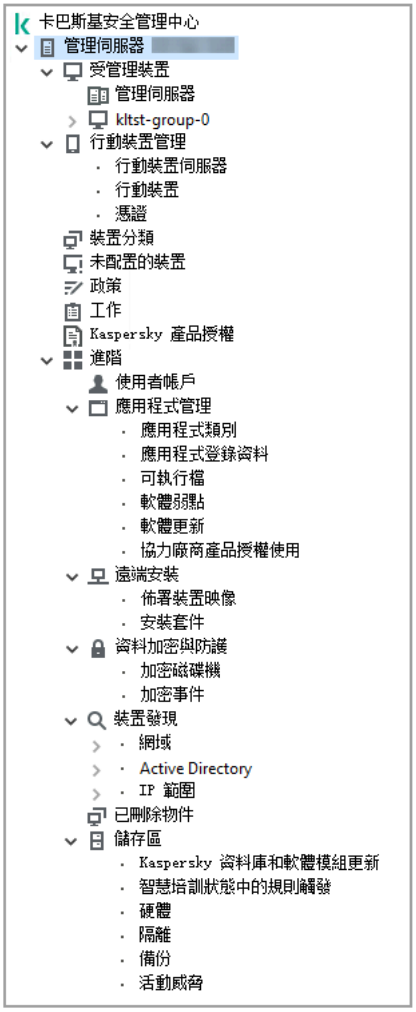
如果選中此選項，當應用程式類別變更時，僅修改的資料被傳輸到用戶端裝置，並不是類別中所有資料。該傳輸選項使用在 Network Agent Service Pack 2 和更新版本。

使用管理介面的功能

該部分將說明您在卡巴斯基安全管理中心主視窗中可以執行的操作。

主控台樹狀目錄

主控台樹狀目錄（參閱下圖）的設計是用來顯示公司網路中管理伺服器的階層、管理群組的結構及其他應用程式物件，如**儲存區**或**應用程式管理**資料夾。卡巴斯基安全管理中心的名稱空間可包含數個節點，包括階層中安裝之管理伺服器所對應的伺服器名稱。



主控台樹狀目錄

管理伺服器節點

管理伺服器 – <裝置名稱> 節點是一個顯示選取之管理伺服器的結構化組織容器。

管理伺服器的工作空間節點包含受管理伺服器管理之應用程式和裝置的目前狀態摘要資訊。工作空間中的資訊將會分佈在以下各個頁面之間：

- **監控**。以即時模式顯示應用程式作業及用戶端裝置目前狀態資訊。管理員的重要訊息（如弱點、錯誤或偵測到的病毒訊息）會以特定顏色標示。您可以使用**監控**頁面上的連結來執行標準管理員工作（例如，在用戶端裝置安裝和設定安全應用程式），以及透過主控台樹狀目錄前往其他資料夾。

- **統計**。包含一組按主題（防護狀態、防毒統計、更新等）分類的圖表。這些圖表可視覺化應用程式作業與用戶端裝置目前的狀態資訊。

- **報告**。包含應用程式所產生的報告範本。在此頁面上，您可以使用預設範本建立報告，也可以建立自訂報告範本。

- **事件**視窗。包含應用程式作業期間登錄的事件記錄。這些記錄會分佈在各個主題之間，以方便讀取和篩選。在此頁面上，您可以檢視自動產生的事件選項，也可以建立自訂選項。

管理伺服器節點中的資料夾

管理伺服器 – <裝置名稱> 節點包含下列資料夾：

- **受管理裝置**。此資料夾是用來儲存、顯示、設定和修改管理群組、群組政策及群組工作的結構。

- **行動裝置管理**。此資料夾是用來管理行動裝置。**行動裝置管理**資料夾包含下列子資料夾：

  - **行動裝置伺服器**。用來管理 iOS MDM 伺服器和 Microsoft Exchange 伺服器行動裝置伺服器。

  - **行動裝置**。用來管理行動裝置、KES、Exchange ActiveSync 網域和 iOS MDM。

  - **憑證**。用來管理行動裝置憑證。

- **裝置分類**。此資料夾用來在所有受管理裝置中快速分類符合特定標準（裝置分類）的裝置。例如，您可以快速選擇未安裝任何安全應用程式的裝置並繼續執行這些裝置（檢視清單）。您可以針對這些選取的裝置執行特定操作，例如，分配它們一些工作。您可以使用預設選項或建立自己的自訂選項。

- **未配置的裝置**。此資料夾包含了未納入任何管理群組中的裝置清單。您可以在未配置的裝置上執行一些操作，例如，移動它們到管理群組或在其上安裝應用程式。

- **政策**。此資料夾用來檢視和建立政策。

- **工作**。此資料夾用來檢視和建立工作。

- **Kaspersky 產品授權**。包含 Kaspersky 應用程式可用的產品授權金鑰清單。在此資料夾工作空間，您可以將新的產品授權金鑰新增到產品授權金鑰儲存區，在受管理裝置上佈署金鑰，以及檢視產品授權金鑰使用報告。

- **進階**。此資料夾包含一組對應各種應用程式功能組的子資料夾。

進階資料夾。移動主控台樹狀目錄中的資料夾

進階資料夾包含下列子資料夾：

- **使用者帳戶**。包含網路使用者帳戶清單。
- **應用程式管理**。用來管理網路上裝置安裝的應用程式。**應用程式管理**資料夾包含下列子資料夾：
  - **應用程式類別**。用來管理自訂應用程式類別。
  - **應用程式登錄資料**。包含安裝了網路代理之裝置上的應用程式清單。
  - **可執行檔**。包含安裝了網路代理之用戶端裝置上儲存的可執行檔清單。
  - **軟體弱點**。包含安裝了網路代理之裝置上的應用程式弱點清單。
  - **軟體更新**。包含可在裝置上分發的管理伺服器接收到的應用程式更新清單。
  - **協力廠商產品授權使用**。包含已授權應用程式群組清單。您可以使用已授權應用程式群組來監視協力廠商軟體（非 Kaspersky 應用程式）的使用授權及可能的產品授權限制違規。
- **遠端安裝**。此資料夾用來管理作業系統和應用程式的遠端安裝。**遠端安裝**資料夾包含下列子資料夾：
  - **佈署裝置映像**。用來佈署裝置上作業系統的映像。
  - **安裝套件**。包含裝置上遠端安裝應用程式可用的安裝套件清單。
- **資料加密與防護**。此資料夾用來管理硬碟和卸除式磁碟機上資料加密的程序。
- **網路輪詢**。此資料夾會顯示安裝了管理伺服器的網路。管理伺服器會透過定期輪詢公司網路的 Windows 網路、IP 子網路遮罩和 Active Directory® 來接收網路及其裝置結構的相關資訊。輪詢結果會顯示在對應的資料夾工作空間中：**網域**、**IP 範圍** 和 **Active Directory**。
- **儲存區**。此資料夾用來對監視裝置狀態和執行維護的物件進行操作。**儲存區**資料夾包含下列物件：
  - **自適應異常偵測**。包含在用戶端裝置上智慧培訓模式下工作的 Kaspersky Endpoint Security 規則所執行的偵測清單。
  - **Kaspersky 軟體更新和修補程式**。包含可分發到裝置之管理伺服器接收到的更新清單。
  - **硬體**。包含連線至組織網路的硬體清單。
  - **隔離**。包含裝置上防毒應用程式移除到隔離區的物件清單。
  - **備份**。包含裝置上未受感染期間所刪除或修改的檔案備份副本清單。
  - **未處理的檔案**。包含指定為稍後再透過防毒應用程式掃描的檔案清單。

您可以變更**進階**資料夾中所包含的子資料夾集。常用的子資料夾可以從**進階**資料夾往上移動一層。不常用的子資料夾可以移動到**進階**資料夾中。

*若要將子資料夾移出**進階**資料夾：*

1. 在主控台樹狀目錄中，選取您想移出**進階**資料夾的子資料夾。
2. 在子資料夾的內容功能表中，選取**檢視 → 從進階資料夾移出**。

> 您也可以在**進階**資料夾的工作空間中將子資料夾從**進階**資料夾中移出，方法是點擊該資料夾名稱區段中的**從進階資料夾移出**連結。

*若要將子資料夾移至**進階**資料夾：*

1. 在主控台樹狀目錄中，選取您想移至**進階**資料夾的子資料夾。
2. 在子資料夾的內容功能表中，選取**檢視 → 移至進階資料夾**。

如何在工作台中更新資料

> 在卡巴斯基安全管理中心中，工作台資料（例如裝置狀態、統計資訊和報告）從不被自動更新。

要更新工作台中的資料，請執行以下操作：

- 按 **F5** 鍵。
- 在主控台樹狀目錄中的物件上下文功能表中，選取**重新整理**。
- 點擊工作區中的重新整理圖示 ()。

如何瀏覽主控台樹狀目錄

要瀏覽主控台樹狀目錄，您可以使用下列工具列按鈕：

- – 後退一步。
- – 向前一步。
- – 向上一級。

您還可以使用工作台右上角的導航連結。導航連結包含您當在所在主控台樹狀目錄中的資料夾的絕對路徑。連結的所有元素（最後一個除外）均連結至主控台樹狀目錄中的物件。

如何在工作台開啟物件內容視窗

您可以在物件內容視窗中變更絕大部分管理主控台物件的內容。

要開啟工作台中某個物件的內容視窗，請執行以下操作：

- 從物件的上下文功能表中，選取**內容**。
- 選取一個物件，然後點擊 **ALT+ENTER** 組合鍵。

如何在工作台中選取一群組物件

您可以在工作台選取一群組物件。您可以選取一組物件，例如您要建立工作的裝置集合。

要選取物件範圍，請執行以下操作：

1. 選取範圍中的第一個物件，按 **Shift**鍵。
2. 按住 **Shift** 鍵，然後選取範圍中的最後一個物件。

   該範圍將被選定。

要將單獨物件進行分組，請執行以下操作：

1. 選取組中的第一個物件，按 **Ctrl** 鍵。
2. 按住 **Ctrl** 鍵，然後選取群組中的其他物件。

   物件將被分組。

如何在工作台中變更表列集

管理主控台允許您變更工作台中顯示的列集。

要在工作台中變更列集，請執行以下操作：

1. 在主控台樹狀目錄中，點擊要為其變更列集的物件。
2. 在資料夾的工作區，透過點擊**新增/刪除欄位**連結開啟欄集設定的配置視窗。
3. 在**新增/刪除欄位**視窗中，指定要顯示的欄集。

參考資訊

該部分的表格將為您提供有關管理主控台物件的上下文功能表的概覽資訊，以及有關主控台樹狀目錄物件和工作台物件的概覽資訊。

上下文功能表指令

本區域列出管理主控台物件和相應的上下文功能表項（請見下表）。

物件	功能表項	功能表項用途
上下文功能表的一般項	**搜尋**	開啟裝置搜尋視窗。
	重新整理	重新整理所選物件的顯示。
	匯出清單	匯出目前清單到檔案。
	內容	開啟所選物件的內容視窗。
	檢視 → 新增/刪除欄位	在工作台的物件表格中新增或刪除欄位。
	檢視 → 大圖示	在工作台中以大圖示顯示物件。
	檢視 → 小圖示	在工作台中以小圖示顯示物件。
	檢視 → 清單	在工作台中以清單形式顯示物件。
	檢視 → 表格	在工作台中以表格形式顯示物件。
	檢視 → 配置	設定管理主控台元素的顯示。
卡巴斯基安全管理中心	**新增 → 管理伺服器**	將管理伺服器新增至主控台樹狀目錄。
<管理伺服器名稱>	**連線至管理伺服器**	連線至管理伺服器。
	中斷與管理伺服器的連線	中斷與管理伺服器的連線。
受管理裝置	**安裝應用程式**	啟動遠端安裝精靈。
	檢視 → 設定介面	設定介面元素的顯示。
	刪除	從主控台樹狀目錄中刪除管理伺服器。
	安裝應用程式	為管理群組啟動遠端安裝精靈。
	重設病毒計數器	重設管理群組中包含的裝置的病毒計數器。
	檢視威脅報告	建立管理群組中包含的裝置上的威脅和病毒活動報告。
	新 → 群組	建立管理群組。
	所有工作 → 新群組結構	依據網域結構或 Active Directory，建立管理群組結構。
	All Tasks → 顯示訊息	為管理群組中包含的用戶端裝置啟動「使用者新訊息精靈」。
受管理裝置 → 管理伺服器	**新 → 從屬管理伺服器**	啟動新增從屬管理伺服器精靈。
	新 → 虛擬管理伺服器	啟動新增虛擬管理伺服器精靈。
行動裝置管理 → 行動裝置	**新增 → 行動裝置**	連線使用者的新行動裝置。
行動裝置管理 → 憑證	**New → 憑證**	建立憑證。
	建立 → 行動裝置	連線使用者的新行動裝置。
裝置分類	**New → 新分類**	建立裝置分類。
	所有工作 → 匯入	從檔案中匯入分類。
Kaspersky 產品授權	**新增啟動碼或金鑰檔案**	新增授權金鑰到管理伺服器儲存區。
	啟動應用程式	啟動程式啟動工作建立精靈。
	產品授權金鑰使用報告	建立並檢視用戶端裝置授權金鑰報告。
應用程式管理 → 應用程式類別	**新 → 類別**	建立應用程式類別。
應用程式管理 → 應用程式登錄資料	**篩選器**	設定應用程式清單篩選器。
	監控的應用程式	設定應用程式安裝事件發佈。
	刪除未安裝的應用程式	清除不在網路裝置上安裝的應用程式的詳情清單。
應用程式管理 → 軟體更新	**同意產品授權協議的更新**	接受軟體更新的產品授權協議。
應用程式管理 → 協力廠商產品授權使用	**新 → 已授權應用程式群組**	建立授權的應用程式群組。

物件	功能表項	功能表項用途
遠端安裝 → 安裝套件	**顯示最新應用程式版本**	檢視網路伺服器上可用的最新版 Kaspersky 應用程式的清單。
	New → 安裝套件	建立安裝套件。
	All Tasks → 更新資料庫	更新安裝套件中的應用程式資料庫。
	所有工作 → 顯示獨立安裝套件一般清單	顯示為安裝套件建立的獨立安裝套件清單。
裝置發現 → 網域	**All Tasks → 裝置活動**	設定管理伺服器對網路裝置閒置的回應。
裝置發現 → IP 範圍	**新 → IP 範圍**	建立一個 IP 範圍。
儲存區 → Kaspersky 資料庫和軟體模組更新	**下載更新**	啟動管理伺服器的「將更新下載至儲存區」工作內容視窗。
	更新下載設定	設定管理伺服器的「將更新下載至儲存區」工作。
	病毒資料庫使用報告	建立並顯示資料庫版本報告。
	All Tasks → 清除更新儲存區	清除管理伺服器上的更新儲存區。
儲存區 → 硬體	**New → 裝置**	建立新裝置。

受管理裝置清單。列敘述

下表顯示受管理裝置清單的列名稱及各自的敘述。

受管理裝置清單的列敘述

列名稱	參數值
名稱	用戶端裝置的 NetBIOS 名稱。裝置名稱的圖示說明在附錄中提供。
作業系統類型	用戶端裝置上安裝的作業系統的類型。
Windows 網域	用戶端裝置所在的 Windows 網域的名稱。
網路代理已安裝	用戶端裝置上的網路代理安裝結果：*是*, *否*, *未知*。
網路代理正在執行	網路代理的操作結果：*是*, *否*, *未知*。
即時防護	安全應用程式已安裝：*是*, *否*, *未知*。
上一次連線到管理伺服器	用戶端裝置已連線到管理伺服器的時間。
上次更新的防護	自上次更新受管理裝置以來經過的時間段。
狀態	用戶端裝置的目前狀態：「*正常*」、「*緊急*」、「*警告*」。

列名稱	參數值

狀態敘述	將用戶端裝置的狀態變更為*緊急*或*警告*的條件。
	在以下條件下，裝置的狀態將變更為*警告*或*緊急*：
	• 安全應用程式未安裝。
	• 偵測到太多病毒。
	• 即時防護不符合管理員的設定等級。
	• 惡意軟體掃描已長時間未執行。
	• 資料庫已過期。
	• 長時間未連線。
	• 偵測到活動威脅。
	• 需要重新啟動。
	重新啟動裝置的原因可以是以下之一：
	  • 由於未知原因重新啟動。
	  • 應用程式在重新啟動前不會執行。
	  • 需要重新啟動以完成更新；應用程式正在執行。
	  • 需要重新啟動以啟動更新。
	  • 需要重新啟動以完成掃描或解毒。
	  • 需要重新啟動以完成遠端安裝 / 移除。
	  • 即將完成磁碟的資料加密。
	  您可以在設定裝置狀態轉換時設定原因。
	• 安裝了不相容的應用程式。
	• 偵測到軟體弱點。
	• Windows Update 更新檢查已長時間未執行。
	• 無效的加密狀態。
	• 行動裝置設定與政策不同。
	• 偵測到未處理的事件。
	• 應用程式定義的裝置狀態。
	• 裝置磁碟空間不足。
	• 產品授權即將到期。
	裝置狀態僅會因以下原因變更為*緊急*：
	• 產品授權已到期。
	• 裝置已失去管理。
	• 防護已停用。
	• 安全應用程式沒有執行。
	用戶端裝置上受管的 Kaspersky 應用程式可以新增狀態敘述到清單。卡巴斯基安全管理中心可以從裝置上安裝的受管的 Kaspersky 應用程式接收用戶端裝置狀態敘述。如果被受管的應用程式分配到裝置的狀態不同於被卡巴斯基安全管理中心分配的狀態，管理主控台顯示該狀態，這也是對裝置安全最關鍵的事件。例如，如果受管應用程式分配了*緊急*狀態到裝置，而卡巴斯基安全管理中心分配了*警告*狀態，管理主控台為該裝置顯示*緊急*狀態以及受管應用程式提供的相關敘述。

上次更新的資訊	距離用戶端裝置上次與管理伺服器成功同步的時間（意即距離上次網路掃描的時間）。
DNS 名稱	用戶端裝置的 DNS 網域名稱。
DNS 網域	主 DNS 前置詞。
IP 位址	用戶端裝置的 IP 位址。建議使用 IPv4 位址。
上一次可見	用戶端裝置在網路上保持可見的持續時間。
上一次完整掃描	在使用者請求後安全應用程式對用戶端裝置執行上一次掃描的日期和時間。
偵測到的威脅總數	發現的威脅數量。
即時防護狀態	即時防護狀態：*正在啟動*, *執行中*, *正在執行（最高防護）*, *正在執行（最快速度）*, *正在執行（建議設定）*, *正在執行（自訂設定）*, *已停止*, *已暫停*, *失敗*。
連線 IP 位址	用於連線卡巴斯基安全管理中心管理伺服器的 IP 位址。
網路代理版本	網路代理版本。

列名稱	參數值
應用程式版本	安裝在用戶端裝置上的安全應用程式版本。
病毒資料庫上次更新	病毒資料庫的版本。
系統上次啟動	用戶端裝置上次開啟的日期和時間。
需要重新啟動	需要重新啟動用戶端裝置。
發佈點	用作此用戶端裝置的發佈點的裝置的名稱。
敘述	在網路掃描後接收的用戶端裝置敘述。
加密狀態	用戶端裝置的資料加密狀態。
WUA 狀態	用戶端裝置上的 Windows 更新代理的狀態。 「*是*」值與透過 Windows 更新從管理伺服器接收更新的用戶端裝置對應。 「*否*」值與透過 Windows 更新從其他來源接收更新的用戶端裝置對應。
作業系統 bit 大小	用戶端裝置上安裝的作業系統的大小。
垃圾郵件防護狀態	垃圾郵件防護元件：*執行中*、*正在啟動*、*已停止*、*已暫停*、*失敗*、*裝置上無資料*
資料洩漏防護狀態	資料外洩防護元件狀態：*執行中*、*正在啟動*、*已停止*、*已暫停*、*失敗*、*裝置上無資料*
協作伺服器防護狀態	內容篩選元件狀態：*執行中*、*正在啟動*、*已停止已暫停*、*失敗*、*裝置上無資料*
郵件伺服器的病毒防護狀態	郵件伺服器病毒防護元件狀態：*執行中*、*正在啟動*、*已停止*、*已暫停*、*失敗*、*裝置上無資料*
端點感應器狀態	Endpoint Detection and Response 元件 (KATA) 狀態：*執行中*、*正在啟動*、*已停止*、*已暫停*、*失敗*、*裝置上無資料*
建立日期	建立 <裝置名稱> 圖示的時間。此屬性用於相互比較各種事件。
虛擬或從屬管理伺服器名稱	虛擬或從屬管理伺服器名稱。該欄僅在包含來自不同管理伺服器的裝置清單中可用。
父群組	<裝置名稱>圖示所在的管理群組名稱。該欄僅在包含來自不同管理伺服器的裝置清單中可用。
由不同管理伺服器管理	該參數可以採用以下值之一： • 的確如此，如果在裝置上遠端安裝安全應用程式時，事實證明該裝置由其他管理伺服器管理。 • 錯誤，否則。
作業系統版本	作業系統版本號。您可以指定所選作業系統是否必須具有相等、更早或更晚的版本號。您也可以設定對所有版本號的搜尋，除了指定的值。
作業系統發佈 ID	作業系統發佈 ID。您可以指定所選作業系統是否必須具有相等、更早或更晚的發佈 ID。您也可以設定對所有發佈 ID 的搜尋，除了指定的值。

裝置、工作和政策的狀態

下表包含顯示在管理主控台工作台內和主控台樹狀目錄中顯示的圖示的清單，這些圖示位於裝置、工作和政策的一旁。這些圖示定義了物件的狀態。

裝置、工作和政策的狀態

圖示	狀態
	在系統中偵測到並且未包含在任何管理群組中的執行工作站作業系統的裝置。
	包含在管理群組中且工作站作業系統狀態為*確定*的裝置。
	包含在管理群組中且工作站作業系統狀態為*警告*的裝置。
	包含在管理群組中且工作站作業系統狀態為*緊急*的裝置。
	包含在管理群組中且執行工作站作業系統的已遺失管理伺服器連線的裝置。
	在系統中偵測到並且未包含在任何管理群組中的執行伺服器作業系統的裝置。
	包含在管理群組中且伺服器作業系統狀態為*確定*的裝置。
	包含在管理群組中且伺服器作業系統狀態為*警告*的裝置。
	包含在管理群組中且伺服器作業系統狀態為*緊急*的裝置。
	包含在管理群組中且執行伺服器作業系統的已遺失管理伺服器連線的裝置。
	網路中偵測到的、不包含在任何管理群組中的行動裝置。
	包含在管理群組中且狀態為*確定*的行動裝置。
	包含在管理群組中且狀態為 *警告*的行動裝置。
	包含在管理群組中且狀態為*緊急*的行動裝置。
	包含在管理群組中的行動裝置，與管理伺服器遺失了連線。
	網路中偵測到的但不包含在任何管理群組的 UEFI 防護裝置。UEFI 防護裝置在網路中。
	網路中偵測到的但不包含在任何管理群組的 UEFI 防護裝置。UEFI 防護裝置不在網路中。
	包含在管理群組中且狀態為*確定*的 UEFI 防護裝置。UEFI 防護裝置在網路中。
	包含在管理群組中且狀態為*確定*的 UEFI 防護裝置。UEFI 防護裝置不在網路中。
	包含在管理群組中且狀態為*警告*的 UEFI 防護裝置。UEFI 防護裝置在網路中。
	包含在管理群組中且狀態為*警告*的 UEFI 防護裝置。UEFI 防護裝置不在網路中。
	包含在管理群組中且狀態為*緊急*的 UEFI 防護裝置。UEFI 防護裝置在網路中。
	包含在管理群組中且狀態為*緊急*的 UEFI 防護裝置。UEFI 防護裝置不在網路中。
	活動政策。
	停用政策。
	從主管理伺服器上建立的群組中繼承的活動政策。

	從頂級群組繼承的活動政策。
	擁有*已排程*或*成功完成*狀態的工作（群組工作、管理伺服器工作或指定裝置的工作）。
	擁有*執行中*狀態的工作（群組工作、管理伺服器工作或指定裝置的工作）。
	擁有*失敗*狀態的工作（群組工作、管理伺服器工作或指定裝置的工作）。
	從主管理伺服器上建立的群組中繼承的工作。
	從頂級群組繼承的工作。

管理主控台上的檔案狀態圖示

為便於卡巴斯基安全管理中心管理主控台中的檔案管理，圖示顯示在檔案名稱旁邊（見下表）。圖示顯示了用戶端裝置上 Kaspersky 應用程式分配給檔案的狀態。圖示顯示在**隔離**、**備份**和**活動威脅**資料夾的工作區。

狀態由安裝到用戶端裝置上的 Kaspersky Endpoint Security 分配到物件。

圖示和檔案狀態的一致性

圖示	狀態
	帶有*被感染*狀態的檔案。
	*有警告*或*疑似被感染*狀態的檔案。
	狀態為*由使用者新增*的檔案。
	帶有*誤報*狀態的檔案。
	帶有*已解毒*狀態的檔案。
	帶有*已刪除*狀態的檔案。
	在**隔離**資料夾且有*未感染*、*密碼防護*或*必須被傳送到 Kaspersky*狀態的檔案。如果圖示旁邊沒有狀態敘述，這意味著用戶端裝置上受管理的 Kaspersky 應用程式已經報告了未知狀態到卡巴斯基安全管理中心。
	在**備份**資料夾且有*未感染*, *密碼防護*或*必須被傳送到 Kaspersky*狀態的檔案。如果圖示旁邊沒有狀態敘述，這意味著用戶端裝置上受管理的 Kaspersky 應用程式已經報告了未知狀態到卡巴斯基安全管理中心。
	在**活動威脅**資料夾且有*未感染*、*密碼防護*或*必須被傳送到 Kaspersky*狀態的檔案。如果圖示旁邊沒有狀態敘述，這意味著用戶端裝置上受管理的 Kaspersky 應用程式已經報告了未知狀態到卡巴斯基安全管理中心。

搜尋和匯出資料

該部分包含資料搜尋方法和匯出資料的資訊。

尋找裝置

卡巴斯基安全管理中心允許您按照指定規則尋找裝置。搜尋結果可儲存至文字檔案。

搜尋功能允許您尋找以下裝置：

- 管理伺服器及其從屬伺服器的管理群組中的用戶端裝置。
- 管理伺服器及其從屬伺服器下執行的未配置的裝置。

若要尋找管理群組中的用戶端裝置，請執行以下操作：

1. 在主控台樹狀目錄中，選取一個管理群組項目。
2. 從管理群組資料夾的上下文功能表中選取**搜尋**。
3. 在**搜尋**視窗的頁籤上，指定搜尋用戶端裝置的條件，並點擊**立即尋找**按鈕。

   滿足指定搜尋條件的裝置顯示在**搜尋**視窗底部的表格裡。

要尋找未配置的裝置：

1. 在主控台樹狀目錄中，選取**未配置的裝置**資料夾。
2. 在**未配置的裝置**的上下文功能表中選取**搜尋**。
3. 在**搜尋**視窗的頁籤上，指定搜尋用戶端裝置的條件，並點擊**立即尋找**按鈕。

   滿足指定搜尋條件的裝置顯示在**搜尋**視窗底部的表格裡。

若要不考慮裝置是否包括在管理群組中而進行搜尋，請執行以下操作：

1. 在主控台樹狀目錄中，選取**管理伺服器**節點。
2. 在節點的上下文功能表中，選取**搜尋**。
3. 在**搜尋**視窗的頁籤上，指定搜尋用戶端裝置的條件，並點擊**立即尋找**按鈕。

   滿足指定搜尋條件的裝置顯示在**搜尋**視窗底部的表格裡。

> 在**搜尋**視窗，您也可以使用視窗右上角的下拉清單搜尋管理群組和從屬管理伺服器。在您從**未配置的裝置**資料夾開啟**搜尋**視窗時無法使用管理群組與從屬管理伺服器的搜尋功能。

若要尋找裝置，您可在**搜尋**視窗的欄位中使用規則運算式。

在**搜尋**視窗的完整文字搜尋可用：

- 在**網路**頁籤的**敘述**欄位
- 在**硬體**頁籤的**裝置**、**供應商**與**敘述**欄位

裝置搜尋設定

以下為搜尋受管理裝置設定的說明。搜尋結果顯示在視窗的下部。

網路

您可以在**網路**標籤上指定依據網路資料搜尋裝置所使用的標準：

- **裝置名稱或 IP 位址**

  裝置的 Windows 網路名稱（NetBIOS 名稱），或者 IPv4 或 IPv6 位址。

- **Windows 網域**

  顯示指定的 Windows 網域中包括的所有裝置。

- **管理群組**

  顯示指定的管理群組中包括的裝置。

- **敘述**

  裝置內容視窗中的文字：在**一般**區域的**敘述**欄位。
  您可以使用以下特徵說明**敘述**欄位中的文字：

  - 在單詞中：
    - *****。用任意數量的字元更換任何字串。

      例如：
      要敘述單詞 **Server** 或 **Server's**，您可以輸入 **Server***。
    - **?**。更換任意單個字元。

      例如：
      要敘述單詞 **Window** 或 **Windows**，您可以輸入 **Windo?**。
      星號 (*****) 或問號 (**?**) 不能用於查詢中的第一個字元。
  - 要尋找多個單詞：
    - 空格。顯示所有在其敘述中包含列出的任何單詞的裝置。

      例如：
      要尋找在其敘述中包含**從屬**或**虛擬**單詞的短語，您可以在查詢中包含**從屬虛擬**等字。
    - **+**。當單詞帶有加號前綴時，所有搜尋結果都將包含該單詞。

      例如：
      要搜尋同時包含**從屬**和**虛擬**的短語，請輸入**+從屬+虛擬**查詢。
    - **-**。當單詞帶有減號前綴時，所有搜尋結果都不包含該單詞。

      例如：
      要尋找包含**從屬**但不包含**虛擬**的短語，請輸入**+從屬-虛擬**查詢。
    - **「<某些文字>」**。引號中圍繞的文字必須存在文字中。

      例如：
      要尋找包含**從屬伺服器**單詞群組合的短語，您可以在查詢中輸入**「從屬伺服器」**。

- **IP 範圍**

  如果啟用此選項，您可以輸入應該包括相關裝置的 IP 範圍的初始和最終 IP 位址。

  預設情況下已停用該選項。

- **由不同管理伺服器管理**

  您可以選取以下值之一：

  - **是**。僅被其他管理伺服器管理的用戶端裝置被考慮。
  - **否**。僅考慮由相同管理伺服器管理的用戶端裝置。
  - **未選取值**。將不套用標準。

標籤

在**標籤**頁籤，您可以基於先前新增到受管理裝置的敘述的關鍵字（標籤）設定裝置搜尋：

- **如果有至少一個指定的標籤符合則套用**

  如果啟用此選項，搜尋結果將顯示包含帶有所選標籤的敘述的裝置。

  如果停用此選項，搜尋結果將僅顯示包含帶有所有標籤的敘述的裝置。

  預設情況下已停用該選項。

- **必須包含標籤**

  如果選取了該選項，搜尋結果將顯示帶有包含了所選標籤的敘述的裝置。要尋找裝置，您可以使用星號，它表示任何字元長度的字串。

  預設情況下已選定此選項。

- **必須排除標籤**

  如果選取了該選項，搜尋結果將顯示不帶有包含了所選標籤的敘述的裝置。要尋找裝置，您可以使用星號，它表示任何字元長度的字串。

Active Directory

在**Active Directory**頁簽上，您可以指定應在 Active Directory 組織單元 (OU) 或群組中搜尋裝置。您還可以在選擇中包括來自指定 Active Directory OU 的所有子 OU 的裝置。要選擇裝置，請定義以下設定：

- **裝置在 Active Directory 組織單元中**

  如果啟用此選項，選取範圍將包括輸入欄位中指定的 Active Directory 單元中的裝置。
  預設情況下已停用該選項。

- **包括子組織單元**

  如果啟用此選項，選取範圍將包括指定 Active Directory 組織單元的所有子組織單元中的裝置。
  預設情況下已停用該選項。

- **該裝置是 Active Directory 群組成員**

  如果啟用此選項，選取範圍將包括輸入欄位中指定的 Active Directory 群組中的裝置。
  預設情況下已停用該選項。

網路活動

您可以在**網路活動**頁籤上，指定依據網路活動搜尋裝置所使用的標準：

- **該裝置是發佈點**

  在下拉清單中，可設定執行搜尋時在分類中包括裝置的標準：
  - **是**。選取範圍將包括充當發佈點的裝置。
  - **否**。分類不包含作為發佈點的裝置。
  - **未選取值**。將不套用標準。

- **不斷開與管理伺服器的連線**

  在下拉清單中，可設定執行搜尋時在分類中包括裝置的標準：
  - **已啟用**。分類將包含已選取**不斷開與管理伺服器的連線**核取方塊的裝置。
  - **已停用**。分類將包含未選取**不斷開與管理伺服器的連線**核取方塊的裝置。
  - **未選取值**。將不套用標準。

- **連線設定檔已轉換**

  在下拉清單中，可設定執行搜尋時在分類中包括裝置的標準：

  - **是**。該分類將包含連線設定檔轉換後連線到管理伺服器的裝置。
  - **否**。該分類將不包含連線設定檔轉換後連線到管理伺服器的裝置。
  - **未選取值**。將不套用標準。

- **上一次連線到管理伺服器**

  您可使用此方塊設定按上一次連線到管理伺服器的時間搜尋裝置的標準。

  如果選取該方塊，則在輸入欄位中，您可以指定在用戶端裝置上安裝的網路代理和管理伺服器之間建立上一次連線的時間間隔（日期和時間）。選取將包括位於指定間隔的裝置。

  如果清除此方塊，則將不會套用標準。

  預設情況下已清空此方塊。

- **網路輪詢時偵測到新裝置**

  搜尋最近幾天透過網路輪詢偵測到的新裝置。

  如果選取此核取方塊，分類將只包括在**偵測週期（天）**欄位中指定的天數內透過裝置發現偵測到的新裝置。

  如果停用此選項，分類將包括透過裝置發現偵測到的所有裝置。

  預設情況下已停用該選項。

- **裝置可見**

  在下拉清單中，可設定執行搜尋時在分類中包括裝置的標準：

  - **是**。程式在分類中包括網路中目前可見的裝置。
  - **否**。應用程式在分類中包括網路中目前不顯示的裝置。
  - **未選取值**。將不套用標準。

應用程式

您可以在**應用程式**頁籤上，指定依據所選受管理應用程式搜尋裝置所使用的標準：

- **應用程式名稱**

  在下拉清單中，可設定按 Kaspersky 應用程式名稱執行搜尋時在分類中包括裝置的標準。
  清單僅提供管理員工作站上已安裝管理外掛程式的應用程式的名稱。
  如果未選取任何應用程式，則將不會套用該標準。

- **應用程式版本**

  在輸入欄位，可設定按 Kaspersky 應用程式版本號執行搜尋時在分類中包括裝置的標準。
  如果未指定版本號，則將不會套用該標準。

- **重大更新名稱**

  在輸入欄位中，可設定按應用程式名稱或更新套件編號執行搜尋時在分類中包括裝置的標準。
  如果欄位留空，則將不會套用該標準。

- **上一次模組更新**

  您可以使用此選項來設定按這些裝置上安裝的程式模組上次更新的時間搜尋裝置的標準。
  如果選中此方塊，則您可以在輸入欄位中指定執行這些裝置上安裝的程式模組的上一次更新的時間間隔（日期和時間）。
  如果清除此方塊，則將不會套用標準。
  預設情況下已清空此方塊。

- **裝置透過卡巴斯基安全管理中心管理**

  在該下拉清單，您可以包含透過卡巴斯基安全管理中心管理的裝置到分類：
  - **是**。應用程式包含透過卡巴斯基安全管理中心管理的裝置。
  - **否**。若裝置不透過卡巴斯基安全管理中心管理，則應用程式會將其包含在分類中。
  - **未選取值**。將不套用標準。

- **安全應用程式已安裝**

  在該下拉清單，您可以包含已安裝安全應用程式的裝置到分類：
  - **是**。應用程式包含安裝了安全應用程式的裝置到分類。
  - **否**。應用程式會在分類中包含未安裝安全應用程式的裝置。
  - **未選取值**。將不套用標準。

作業系統

在**作業系統**頁籤上，您可以設定如何依據作業系統類型搜尋裝置。

- **作業系統版本**

  如果選中該方塊，您可以從清單中選取一個作業系統。安裝了指定作業系統的裝置會包含在搜尋結果中。

- **作業系統 bit 大小**

  在該下拉清單中可選取作業系統的架構，這將決定將移動規則套用到裝置（**未知**、**x86**、**AMD64** 或 **IA64**）的方式。預設情況下，不選取清單中的任何選項，這樣就不會對作業系統的架構進行定義。

- **作業系統服務套件版本**

  在該欄位中，可以指定作業系統的更新套件版本（採用 *X.Y* 格式），這將決定將移動規則套用到裝置的方式。預設情況下，不指定版本值。

- **作業系統版本**

  該設定僅套用到 Windows 作業系統。

  作業系統版本號。您可以指定所選作業系統是否必須具有相等、更早或更晚的版本號。您也可以設定對所有版本號的搜尋，除了指定的值。

- **作業系統發佈 ID**

  該設定僅套用到 Windows 作業系統。

  作業系統發佈 ID。您可以指定所選作業系統是否必須具有相等、更早或更晚的發佈 ID。您也可以設定對所有發佈 ID 的搜尋，除了指定的值。

裝置狀態

在**裝置狀態**頁籤，您可以指定基於受管理應用程式的裝置狀態搜尋裝置的標準：

- **裝置狀態**

  在該下拉清單中，您可以選取下列裝置狀態之一：*確定*、*緊急*或*警告*。

- **即時防護狀態**

  您可以在該下拉清單中選取即時防護狀態。具有指定即時防護狀態的裝置將被包括在選取範圍中。

- **裝置狀態敘述**

  在此欄位中，您可以選取條件旁邊的核取方塊，若滿足這些條件，程式會為裝置分配下列狀態之一：*確定*、*緊急*或*警告*。

- **應用程式定義的裝置狀態**

  您可以在該下拉清單中選取即時防護狀態。具有指定即時防護狀態的裝置將被包括在選取範圍中。

防護元件

在**防護元件**頁籤上，您可以設定按防護狀態搜尋用戶端裝置的標準。

- **資料庫發佈日期**

  如果啟用此選項，您可以按病毒資料庫發佈日期搜尋用戶端裝置。在該輸入欄位中，您可以設定執行搜尋的時間間隔。

  預設情況下已停用該選項。

- **上一次掃描**

  如果啟用此選項，您可以按上次惡意軟體掃描時間來搜尋用戶端裝置。在該輸入欄位中，您可以指定執行上一次惡意軟體掃描的時段。

  預設情況下已停用該選項。

- **偵測到的威脅總數**

  如果啟用此選項，您可以依據發現的病毒數量來搜尋用戶端裝置。在輸入欄位中，您可以設定發現病毒總數的上限值和下限值。

  預設情況下已停用該選項。

應用程式登錄資料

在**應用程式登錄資料**標籤上，您可以依據裝置已安裝的應用程式設定裝置搜尋：

- **應用程式名稱**

  在該下拉清單中，您可以選取應用程式。安裝有指定應用程式的裝置將包括在選取範圍中。

- **應用程式版本**

  在該輸入欄位中，您可以指定選定應用程式的版本。

- **供應商**

  在該下拉清單中，您可以選取已安裝應用程式的生產商。

- **應用程式狀態**

  在該下拉清單中，您可以選取應用程式的狀態（*已安裝*、*未安裝*）。已安裝或未安裝指定應用程式的裝置，取決於所選狀態，將被包含在分類。

- **根據更新尋找**

  如果啟用此選項，則搜尋操作將使用相關裝置內應用程式更新的有關資訊來執行。選取核取方塊後，**應用程式名稱**、**應用程式版本**與**應用程式狀態**欄位會各自變成**更新名稱**、**更新版本**和**狀態**。

  預設情況下已停用該選項。

- **不相容的安全應用程式名稱**

  在該下拉清單中，您可以選取協力廠商安全應用程式。在搜尋過程中，安裝有指定程式的裝置將包括在選取範圍中。

- **應用程式標籤**

  在該下拉清單中，您可以選取應用程式標籤。所有安裝了敘述中帶有所選標籤的應用程式的裝置都被包含在裝置分類。

管理伺服器階層

若要系統在搜尋裝置時考量到儲存在從屬管理伺服器與輸入欄位中的資料，您可在搜尋裝置時指定要考量資訊的從屬管理伺服器的嵌套等級，請在**管理伺服器階層**頁籤，勾選**包含來自從屬管理伺服器（下至等級）的資料**方塊。預設情況下已清空此方塊。

虛擬機

在**虛擬機**頁籤，您可以根據它們是否是虛擬機或虛擬桌面基礎架構 (VDI) 的一部分來設定裝置搜尋：

- **這是一台虛擬機**

  在此下拉清單中，您可以選取以下選項：
  - **不重要**。
  - **否**。尋找不是虛擬機的裝置。
  - **是**。搜尋虛擬機裝置。

- **虛擬機類型**

  在該下拉清單中，您可以選取虛擬機製造商。
  若在**這是一台虛擬機**下清單中選取**是**或**不重要**值，則可使用此下拉清單。

- **虛擬桌面基礎架構的一部分**

  在此下拉清單中，您可以選取以下選項：
  - **不重要**。
  - **否**。尋找不是虛擬桌面基礎架構一部分的裝置。
  - **是**。搜尋屬於虛擬桌面基礎架構 (VDI) 一部分的裝置。

硬體

在**硬體**頁籤上，您可以設定如何依據硬體搜尋用戶端裝置：

- **裝置**

  在該下拉清單中，您可以選取單元類型。所有帶有該單元的裝置被包含在搜尋結果。
  該欄位支援完整文字搜尋。

- **供應商**

  在該下拉清單中，您可以選取單元生產商的名稱。所有帶有該單元的裝置被包含在搜尋結果。
  該欄位支援完整文字搜尋。

- **敘述**

  裝置或硬體單元的敘述。帶有該欄位中指定的敘述的裝置將包括在分類範圍內。
  可在裝置的內容視窗輸入任何格式的裝置敘述。該欄位支援完整文字搜尋。

- **清單號**

  帶有該欄位中指定的清單編號的裝置將包括在選取範圍內。

- **CPU 頻率 (MHz)**

  CPU 的頻率範圍。CPU 與這些輸入欄位（含）中頻率範圍比對的裝置將包括在分類範圍內。

- **虛擬 CPU 核心**

  CPU 中虛擬內核的數量範圍。CPU 與這些輸入欄位（含）中範圍比對的裝置將包括在分類範圍內。

- **硬碟磁區 (GB)**

  裝置硬碟容量值的範圍。硬碟與這些輸入欄位（含）中範圍比對的裝置將包括在分類範圍內。

- **記憶體大小 (MB)**

  裝置 RAM 大小的值的範圍。RAM 與這些輸入欄位（含）中範圍比對的裝置將包括在分類範圍內。

弱點與更新

在**弱點與更新**頁籤，您可以設定根據 Windows 更新來源搜尋裝置的標準：

- **WUA 已轉換到管理伺服器**

  您可以在下拉清單中選取以下搜尋選項之一：
  - **是**。如果選中該選項，搜尋結果會包含從管理伺服器收到 Windows Update 更新的裝置。
  - **否**。如果選中該選項，結果會包含從其他來源收到 Windows Update 更新的裝置。

使用者

在**使用者**頁籤，您可以設定依據登入到作業系統的使用者帳戶搜尋裝置的標準。

- **最後一次登入系統的使用者**

  如果啟用此選項，按一下**瀏覽**按鈕可以指定使用者帳戶。搜尋結果包含其上一次登入使用者為指定使用者的裝置。

- **登入系統至少一次的使用者**

  如果啟用此選項，按一下**瀏覽**按鈕可以指定使用者帳戶。搜尋結果包含指定使用者至少登入一次的裝置。

影響受管理應用程式狀態的問題

在**影響受管理應用程式狀態的問題**頁籤，您可以設定根據受管理應用程式提供的狀態敘述搜尋裝置：

- **裝置狀態敘述**

  您可以選取受管理應用程式狀態敘述的核取方塊；接收這些狀態時，裝置將被包含在分類。當您選取幾個應用程式的狀態時，您可以選取在所有清單中自動選取該狀態。

受管理應用程式元件的狀態

在**受管理應用程式元件的狀態**頁籤中，您可以設定根據受管理應用程式元件狀態搜尋裝置的標準：

- **資料洩漏防護狀態**

  根據資料外洩防護的狀態搜尋裝置（*裝置上無資料*, *已停止*, *正在啟動*, *已暫停*, *執行中*, *失敗*）。

- **協作伺服器防護狀態**

  根據伺服器協作防護狀態搜尋裝置（*裝置上無資料*, *已停止*、*正在啟動*、*已暫停*, *執行中*、*失敗*）。

- **郵件伺服器的病毒防護狀態**

  根據郵件伺服器防護狀態搜尋裝置（*裝置上無資料*、*已停止*、*正在啟動*、*已暫停*、*執行中*、*失敗*）。

- **端點感應器狀態**

  根據端點感應器元件狀態搜尋裝置（*裝置上無資料*、*已停止*、*正在啟動*、*已暫停*、*執行中失敗*）。

加密

- **加密**

  進階加密標準 (AES) 對稱區塊編碼器演算法。在下拉清單中，您可以選取加密金鑰大小（56-bit、128-bit、192-bit 或 256-bit）。

  可用值：*AES56*、*AES128*、*AES192* 和 *AES256*。

雲端區段

在**雲端區段**頁籤，您可以基於裝置是否屬於特定雲端區段來配置搜尋：

- **裝置在雲端區段中**

  如果啟用此選項，您可以按一下**瀏覽**按鈕可以指定要搜尋的區段。
  如果啟用**包含子物件**選項，則搜尋會在指定區段的所有子物件上執行。
  搜尋結果僅包含所選段的裝置。

- **使用 API 發現的裝置**

  在下拉清單，您可以選取裝置是否由 API 工具偵測：
  - **AWS**。裝置使用 AWS API 發現，就是，裝置在 AWS 雲端環境中。
  - **Azure**。裝置使用 Azure API 發現，就是，裝置在 Azure 雲端環境中。
  - **Google Cloud**。裝置被使用 Google API 發現，即裝置一定在 Google 雲端環境中。
  - **否**。系統無法用 AWS、Azure 或 Google API 偵測裝置，意即裝置在雲端環境外或在雲端環境中，但無法使用 API 加以偵測。
  - **沒有值**。這項條件不適用。

應用程式元件

該區域包含了在管理主控台中安裝了管理外掛程式的這些應用程式的元件清單。

在**應用程式元件**區域中，您可以根據所選應用程式元件的狀態和版本編號指定將裝置納入分類的標準：

- **狀態**

  根據應用程式傳送到管理伺服器的元件狀態搜尋裝置。您可以選取以下狀態之一：*裝置上無資料*、*已停止*、*正在啟動*、*已暫停*、*執行中*、*故障*或*未安裝*。如果安裝在受管理裝置上的應用程式的所選元件具有指定狀態，裝置被包含到裝置分類。

  由應用程式傳送的狀態：

  - *正在啟動* - 元件處於初始化處理程序中。
  - *執行中* - 元件被啟用且在正常工作。
  - *已暫停* - 元件被暫停，例如，在使用者在受管理應用程式上停止了防護後。
  - *故障* - 元件操作中發生錯誤。
  - *已停止* - 元件被停用且不在工作。
  - *未安裝* - 當設定應用程式自訂安裝時，使用者未選取該元件以安裝。

  不同於其他狀態，*裝置上無資料*狀態不由應用程式傳送。該選項顯示應用程式沒有所選元件狀態的資訊。例如，這可能發生在所選元件不屬於任何在裝置上安裝的應用程式時，或裝置關閉時。

- **版本**

  根據您在清單中選取的版本號搜尋裝置。您可以輸入版本號，例如 `3.4.1.0`，然後指定所選元件是否必須具有相同、更早或更新版本。您也可以設定對所有版本的搜尋，除了指定的值。

在字串變數中使用遮罩

允許在字串變數中使用遮罩。建立遮罩時，您可以使用以下一般運算式：

- 萬用字元 (*) — 任意零個或更多字串。
- 問號 (?) — 任意單個字元。
- [<range>] — 指定範圍或集合中的任意單個字元。
  例如： [0–9] - 任何數字。 [abcdef] - 任何字元 a、b、c、d、e 或 f。

在搜尋欄位使用規則運算式

你可以在搜尋欄位使用以下規則運算式來搜尋特別字和字元：

- *.取代字元的任何順序。若要搜尋 Server，Servers，或 Server room，在搜尋區域輸入 `Server*` 運算式。
- ?。更換任意單個字元。若要搜尋 Word 或 Ward，在搜尋區域輸入 `W?rd` 來表示。

  > 搜尋區域的文字不能以問號（?）開頭。

- [<range>]。從指定的範圍或集合中更換任何單個字元。若要搜尋任何數字，在搜尋區域輸入 `[0-9]` 來表示。若要搜尋字母中的一個—a, b, c, d, e, or f—在搜尋區域輸入 `[abcdef]` 來表示。

關於事件敘述的範例中，您可以在篩選內容欄位中使用下列字元：

- 空格。結果是所有在其敘述中包含列出的任何單詞的裝置。例如，若要搜尋字詞包含 Secondary 或 Virtual（或兩個都包含），在搜尋欄位輸入 `Secondary Virtual` 運算式。
- 加號（+），AND 或 &&。當單詞帶有加號前綴時，所有搜尋結果都將包含該單詞。例如，若要搜尋包含「Secondary」和「Virtual」的字詞，您可以在搜尋欄位輸入以下任意運算式：`+Secondary+Virtual`、`Secondary AND Virtual`、`Secondary && Virtual`。
- OR 或 ||。當放在兩個字詞中間時，它表示可以在文字中找到一個字詞或另一個字詞。若要搜尋包含「Secondary」或「Virtual」的字詞，您可以在搜尋欄位輸入以下任一運算式：`Secondary OR Virtual`、`Secondary || Virtual`。
- 減號（-）。當單詞帶有減號前綴時，所有搜尋結果都不包含該單詞。若要搜尋必續包含 Secondary 但不得包含 Virtual 的字詞，您必須在搜尋欄位中輸入則運算式 `+Secondary-Virtual`。
- `"<` 某些文字 `>"`。引號中圍繞的文字必須存在文字中。若要搜尋字詞包含 Secondary Server，您必須在搜尋欄位輸入 `" Secondary Server "` 來表示。

全文字搜尋在下面的篩選可使用：

- 在事件清單篩選區域中，根據**事件**和**敘述**欄進行篩選。
- 在使用者帳戶篩選區域，根據**名稱**欄進行篩選。
- 如果**顯示在清單**區域選取了**不分組**作為篩選標準，則在應用程式註冊篩選塊會根據**名稱**欄位篩選。

從對話方塊匯出清單

在應用程式對話方塊，您可以匯出物件清單到文字檔案。

物件清單的匯出可以使用對話方塊區域的**匯出至檔案**按鈕。

工作設定

該區域列出了卡巴斯基安全管理中心中工作的所有設定。

一般工作設定

此區段包含您可檢視與為大多數工作配置的清單。可用設定清單取決於您正在配置的工作。

工作建立過程中指定的設定

您可以在建立工作時指定以下設定。一些設定也可以在所建立工作的內容中修改。

- 作業系統重新啟動設定：
  - **不重新啟動裝置**

    用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

  - **重新啟動裝置**

    如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

  - **提示使用者操作**

    用戶端裝置螢幕上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。該選項適用於使用者必須可以選取最方便的時間進行重新啟動的工作站。

    預設情況下已選定此選項。

  - **重複提示間隔（分鐘）**

    如果啟用該選項，應用程式以指定頻率提示使用者重新啟動作業系統。

    預設情況下已啟用該選項。預設間隔是 5 分鐘。可用值介於 1 和 1440 分鐘之間。

    如果停用該選項，提示僅顯示一次。

  - **在該時間後重新啟動（分鐘）**

    提示使用者之後，應用程式在指定時間間隔後強制作業系統重新啟動。

    預設情況下已啟用該選項。預設延時是 30 分鐘。可用值介於 1 和 1440 分鐘之間。

  - **強制關閉已鎖定連線的應用程式**

    執行應用程式可能會阻止用戶端裝置重新啟動。例如，如果文件在文書處理應用程式中編輯且未儲存，應用程式不會允許裝置重新啟動。

    如果啟用該選項，鎖定裝置上的此類應用程式在裝置重新啟動前被強制關閉。結果，使用者可能遺失他們未儲存的變更。

    如果停用該選項，鎖定裝置不被重新啟動。此裝置上的工作狀態表示裝置需要重新啟動。使用者必須手動關閉所有執行在鎖定裝置上的應用程式並重新啟動這些裝置。

    預設情況下已停用該選項。

- 工作排程設定：

- **排程開始設定：**
  - **每 N 小時**

    工作定期執行，按照指定小時數間隔，從指定的日期和時間開始。

    預設下，工作每 6 小時執行一次，從目前系統日期和時間開始。

  - **每 N 天**

    工作定期執行，按照指定天數間隔。此外，您可指定第一個工作執行的日期與時間。這些額外選項會在您建立的工作受到應用程式支援時可用。

    預設下，工作每天執行一次，從目前系統日期和時間開始。

  - **每 N 星期**

    工作定期執行，按照指定星期數間隔，從指定的星期和時間開始。

    預設下，工作每星期一於目前系統時間執行一次。

  - **每 N 分鐘**

    工作定期執行，按照指定分鐘數間隔，從工作建立日期的指定時間開始。

    預設下，工作每 30 分鐘執行一次，從目前系統時間開始。

  - **每天（不支援日光節約時間）**

    工作定期執行，按照指定天數間隔。排程不支援日光節約時間 (DST)。這意味著在夏令時開始和結束時當時鐘向前或向後撥動一小時時，實際工作啟動時間不變更。

    我們不建議您使用該排程。它用於向後相容卡巴斯基安全管理中心。

    預設下，工作每天於目前系統時間執行一次。

  - **每週**

    工作每週在指定星期和指定時間執行。

  - **按每星期中的指定日**

    工作定期執行，在每周指定日期的指定時間。

    預設下，工作每週五 6:00:00 P.M. 執行。

  - **每月**

    工作定期執行，在指定月日的指定時間。

    在缺少指定日的月份，工作在最後一天執行。

    預設下，工作在每月的第一天執行，在目前系統時間。

- **手動**

  工作不自動執行。您僅可以手動啟動。

  預設情況下已選定此選項。

- **每個月在所選週的指定天**

  工作定期在指定月日的指定時間執行。

  預設情況下，不選取一個月中的任何一天。預設開始時間為 18:00。

- **當新更新下載至儲存區時**

  工作會在更新下載至儲存區時執行。例如，您可能希望使用此排程進行「尋找弱點和必要更新」工作。

- **在偵測到病毒爆發時**

  工作在發生*病毒爆發*事件後執行。選取將監控病毒爆發的應用程式類型。有下列應用程式類型可用：

  - 病毒防護工作站和檔案伺服器
  - 用於週邊防護的防毒軟體
  - 用於郵件伺服器的防毒軟體

  預設情況下選定所有應用程式類型。

  您可能想根據報告病毒爆發的安全應用程式類型執行不同的工作。此種情況下，刪除您不需要的應用程式類型選項。

- **在完成其它工作時**

  目前工作在其他工作完成後啟動。您可以選取先前工作如何結束（成功或帶有錯誤）以觸發目前工作的啟動。例如，您可能想使用***Turn on the device***選項執行開啟裝置工作，完成後，請執行*惡意軟體掃描*工作。只有當這兩項工作都被分配給相同的裝置時，此參數才會有作用。

- **執行錯過的工作**

  該選項決定在工作要啟動時用戶端裝置在網路中不可見時工作的行為。

  如果啟用該選項，系統將在下一次在用戶端裝置上執行 Kaspersky 應用程式時嘗試啟動工作。如果工作排程是**手動**、**一次**或**立即**，裝置在網路中可見或包含在工作範圍後，工作會立即啟動。

  如果停用此選項，則僅限排程的工作會在用戶端裝置上執行。若為**手動**、**一次**與**立即**排程，工作僅會在網路上顯示的用戶端裝置上執行。例如，您可能想為消耗資源的工作停用該選項，您僅想在業餘時間執行該工作。

  預設情況下已停用該選項。

- **使用工作啟動自動隨機延遲**

如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動，即是，*分佈式工作啟動*。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

當工作被建立時，根據工作中包含用戶端裝置的數量，分發啟動時間被自動計算。然後，工作總是在計算的開始時間啟動。然後當工作設定被編輯或者工作被手動啟動時，計算的工作啟動時間值被變更。

如果該選項被停用，工作依據排程在用戶端裝置上啟動。

- **使用工作啟動隨機延遲間隔（分鐘）**

如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

如果該選項被停用，工作依據排程在用戶端裝置上啟動。

預設情況下已停用該選項。預設時間間隔為一分鐘。

- 要分配工作的裝置：
  - **選取管理伺服器偵測到的網路裝置**

    工作被分配到指定裝置。特定裝置可以包含管理群組的裝置和未配置的裝置。

    例如，您可能要在安裝網路代理到未配置的裝置的工作中使用該選項。

  - **手動指定裝置位址或從清單匯入位址**

    您可以指定您要為其分配工作的裝置的 NetBIOS 名稱、DNS 名稱、IP 位址和 IP 子網路。

    您可能要使用該選項以對特定子網路執行工作。例如，您可能要安裝特定應用程式到會計裝置，或者掃描疑似被感染子網路中的裝置。

  - **分配工作到裝置分類**

    該工作被分配到裝置選項中的裝置。您可以指定其中一個現有選項。

    例如，您可能要使用該選項在特定作業系統版本的裝置上執行工作。

  - **分配工作到管理群組**

    工作被分配到包含在管理群組中的裝置。您可以指定其中一個現有群組或者建立新群組。

    例如，您可能要使用該選項執行傳送訊息到使用者工作，如果訊息針對包含在特定管理群組中的裝置。

    如果工作被指派給管理群組，則工作屬性視窗中不會顯示**安全**標籤，因為群組工作受其所套用的群組的安全設定的約束。

- 帳戶設定：
  - **預設帳戶**

    在與執行該工作的應用程式相同的帳戶下執行該工作。

    預設情況下已選定此選項。

  - **指定帳戶**

    填寫**帳戶**與**密碼**欄位以指定工作要在其下執行的帳戶詳情。帳戶必須對此工作有足夠的權限。

  - **帳戶**

    執行該工作的帳戶。

  - **密碼**

    工作執行時使用的帳戶的密碼。

如果您的目標裝置上未安裝網路代理，則必須指定在目標裝置上用於存取 admin$ share 的帳戶。您指定的帳戶僅用於將資料複製到您的裝置。如果您的目標裝置上安裝了網路代理，則資料將透過網路代理進行複製，並且您在建立工作時無需指定任何帳戶。

工作建立後指定的設定

您可以在建立工作後指定以下設定。

- 群組工作設定：
  - **分發到子群組**

    此選項僅在群組工作的設定中可用。

    啟用此選項時，工作範圍包括：

    - 您在建立工作時選擇的管理群組。
    - 依據群組階層，所選管理群組底下任何層級的管理群組。

    停用此選項時，工作範圍僅包括您在建立工作時選擇的管理群組。

    預設情況下已啟用該選項。

  - **分發到從屬和虛擬管理伺服器**

    啟用此選項時，在主管理伺服器上有效的工作也將套用於從屬管理伺服器（包括虛擬伺服器）。如果從屬管理伺服器上已經存在相同類型的工作，則這兩個工作都將套用到從屬管理伺服器上 — 現有的工作和從主管理伺服器繼承的工作。

    此選項僅在**分發到子群組**選項已啟用的情況下可用。

    預設情況下已停用該選項。

- 進階排程設定：
  - **透過使用 Wake-On-LAN 功能在啟動工作之前開啟裝置（分鐘）**

    裝置上的作業系統在工作開始之前的指定時間啟動。預設時間段為五分鐘。

    如果您想要工作在工作範圍內的所有用戶端裝置上執行，包括工作要啟動時關閉的裝置，則啟用該選項。

    若要裝置在工作完成後自動關閉，請啟用**完成工作後關閉裝置**選項。此選項可在相同視窗中找到。

    預設情況下已停用該選項。

  - **完成工作後關閉裝置**

    例如，您可能想為每週五工作時間後安裝更新到用戶端裝置的更新安裝工作啟用該選項，然後在週末關閉這些裝置。

    預設情況下已停用該選項。

  - **停止工作，若時間超過（分鐘）**

在指定時間段過後，工作被自動停止，無論它是否完成。
如果您想要中斷或停止執行時間太長的工作，則啟用該選項。
預設情況下已停用該選項。預設工作執行時間是 120 分鐘。

- 通知設定：
  - **儲存工作歷程記錄**塊：
    - **在管理伺服器上(天)**

      有關工作範圍內所有用戶端裝置上的工作執行的應用程式事件在指定的天數內被儲存在管理伺服器。當該時間段過後，資訊被從管理伺服器刪除。

      預設情況下已啟用該選項。

    - **儲存在裝置的作業系統事件記錄中**

      有關工作執行的應用程式事件被儲存在每個用戶端裝置的本機 Windows 事件記錄中。

      預設情況下已停用該選項。

    - **儲存在管理伺服器的作業系統事件記錄中**

      有關工作範圍內所有用戶端裝置上的工作執行的應用程式事件被集中儲存在管理伺服器作業系統 (OS) 的 Windows 事件記錄中。

      預設情況下已停用該選項。

    - **儲存所有事件**

      如果選取該選項，所有工作相關事件被儲存到事件記錄。

    - **儲存工作進度相關事件**

      如果選取該選項，僅工作執行相關事件被儲存到事件記錄。

    - **僅儲存工作執行結果**

      如果選取該選項，僅工作結果相關事件被儲存到事件記錄。

  - **通知管理員工作執行的結果**

    您可以選取管理員接收工作執行通知的方法：透過電子郵件、透過 SMS 和透過執行可執行檔。若要配置通知，請點擊**設定**連結。

    預設下，所有通知方法被停用。

  - **僅通知錯誤**

    如果該選項被啟用，管理員僅在工作執行完成但帶有錯誤時被通知。

    如果該選項被停用，管理員在每次工作執行完成後被通知。

    預設情況下已啟用該選項。

- 安全設定
- 工作範圍設定：
  取決於工作範圍決定的方式，以下設定被展現：
  - **裝置**

    如果工作範圍由管理群組決定，您可以檢視該群組。這裡不可以變更。但您可設定**工作範圍排除項目**。

    如果工作範圍由裝置清單決定，您可以透過新增和刪除裝置修改該清單。

  - **裝置分類**

    您可以變更應用程式工作的裝置分類。

  - **工作範圍排除項目**

    您可以指定套用工作的裝置群組。要排除的群組僅可以是套用工作的管理群組的子群組。

- **變更歷程**

“將更新下載至管理伺服器儲存區”工作設定

工作建立過程中指定的設定

您可以在建立工作時指定以下設定。一些設定也可以在所建立工作的內容中修改。

- **更新來源**

  可使用以下資源作為管理伺服器的更新來源：

  - 卡巴斯基更新伺服器

    Kaspersky 應用程式可以從 Kaspersky 的 HTTP(S) 伺服器下載資料庫和程式模組更新。預設下，管理伺服器與 Kaspersky 更新伺服器通訊並使用 HTTPS 協定下載更新。您可以配置管理伺服器使用 HTTP 協定，而不是 HTTPS。

    預設選取。

  - 主管理伺服器

    該資源套用到為從屬或虛擬管理伺服器建立的工作。

  - 本機或網路資料夾

    包含最新更新的本機或網路資料夾。網路資料夾可以是 FTP 或 HTTP 伺服器，或者 SMB 共用。如果網路資料夾需要身分驗證，則僅支援 SMB 通訊協定。在選取本機資料夾時，您必須在安裝了管理伺服器的裝置上指定一個資料夾。

    > 更新來源所使用的 FTP 或 HTTP 伺服器或網路資料夾必須包含比對 Kaspersky 更新伺服器所建立的結構的資料夾結構（帶有更新）。

- **其他設定**

  強制執行從屬管理伺服器的更新

  如果啟用該選項，當新更新下載後管理伺服器立刻在從屬管理伺服器上啟動更新工作。更新工作透過使用在從屬管理伺服器上的工作屬性中配置的更新來源來啟動。

  如果停用此選項，從屬管理伺服器上的更新工作將根據排程啟動。

  預設情況下已停用該選項。

  複製下載的更新至其他資料夾

  管理伺服器接收更新後，它複製它們到指定資料夾。如果您想要在您的網路上手動管理更新的分發，則使用該選項。

  例如，您可能要在以下情況下使用該選項：您組織的網路包含幾個獨立子網路，且每個子網路的裝置不能存取其他子網路。然而，所有子網路中的裝置都可以存取通用網路共用。此種情況下，您在子網路之一設定管理伺服器從 Kaspersky 更新伺服器下載更新，啟用該選項，然後指定該網路共用。對於其他管理伺服器的「將更新下載至儲存區」工作中，指定與更新來源相同的網路共用。

  預設情況下已停用該選項。

除非複製完成，否則不強制更新裝置和從屬管理伺服器

下載更新到用戶端裝置和從屬管理伺服器工作僅在這些更新從主更新資料夾被複製到附加更新資料夾後才啟動。

如果用戶端裝置和從屬管理伺服器從附加網路資料夾下載更新，則必須啟用該選項。

預設情況下已停用該選項。

工作建立後指定的設定

您可以在建立工作後指定以下設定。

- **設定**區域，**更新內容**區塊

  下載差異檔案

  該選項啟用下載 diff 檔案功能。

  預設情況下已停用該選項。

- **更新驗證**區段

  發佈前驗證更新

  管理伺服器會從源下載更新並將其儲存到暫時儲存區，之後執行**更新驗證工作**欄位中定義的工作。如果工作成功完成，系統會從暫時儲存區將更新複製到管理伺服器共用資料夾，然後分發到所有以管理伺服器作為更新來源的裝置（系統會啟動有**當新更新下載至儲存區時**排程類型的工作）。「將更新下載至儲存區」工作僅在*更新驗證*工作完成後結束。

  預設情況下已停用該選項。

  更新驗證工作

  該工作在更新被分發到所有以管理伺服器作為更新來源的裝置之前驗證更新。

  在此欄位中，您可以指定之前建立的"*更新驗證*"工作。或者，您可以建立新的"*更新驗證*"工作。

「將更新下載至發佈點儲存區」工作設定

工作建立過程中指定的設定

您可以在建立工作時指定以下設定。一些設定也可以在所建立工作的內容中修改。

- **更新來源**

  以下資源可作為發佈點的更新來源：

  - Kaspersky 更新伺服器

    Kaspersky 應用程式可以從 Kaspersky 的 HTTP(S) 伺服器下載資料庫和程式模組更新。

    預設情況下已選取此選項。

  - 主管理伺服器

    該資源套用到為從屬或虛擬管理伺服器建立的工作。

  - 本機或網路資料夾

    包含最新更新的本機或網路資料夾。網路資料夾可以是 FTP 或 HTTP 伺服器，或者 SMB 共用。如果網路資料夾需要身分驗證，則僅支援 SMB 通訊協定。在選取本機資料夾時，您必須在安裝了管理伺服器的裝置上指定一個資料夾。

    更新來源所使用的 FTP 或 HTTP 伺服器或網路資料夾必須包含比對 Kaspersky 更新伺服器所建立的結構的資料夾結構（帶有更新）。

- **其他設定** → **更新儲存資料夾**

  用於儲存已儲存更新的指定資料夾的路徑。您可以將指定的資料夾路徑複製到剪貼簿。您不能變更群組工作的指定資料夾的路徑。

工作建立後指定的設定

您可以在**設定**區域中指定以下設定，僅在建立工作後在**更新內容**塊中指定。

下載差異檔案

該選項啟用下載 diff 檔案功能。

預設情況下已停用該選項。

「弱點掃描和所需更新」工作設定

工作建立過程中指定的設定

您可以在建立工作時指定以下設定。一些設定也可以在所建立工作的內容中修改。

- **搜尋 Microsoft 列出的弱點和更新**

  搜尋弱點與更新時，卡巴斯基安全管理中心會使用適用 Microsoft 更新的資訊（來自 Microsoft 更新來源），這些更新都是當下可取得的資訊。

  例如，如果您對 Microsoft 更新和協力廠商應用程式更新有不同設定與不同工作，您可能會需要停用此選項。

  預設情況下已啟用該選項。

  有關可選 Microsoft Windows 更新的資訊未被傳送至管理伺服器。

  - **連線更新伺服器更新資料**

受管理裝置上的 Windows Update 代理程式會連線至 Microsoft 更新來源。以下伺服器會以 Microsoft 更新來源運作：

- 卡巴斯基安全管理中心管理伺服器（請參閱網路代理政策的設定）
- 具備 Microsoft Windows Server Update Services (WSUS) 的 Windows 伺服器會佈署在貴組織的網路中
- Microsoft Updates 伺服器

如果啟用該選項，受管理裝置上的 Windows Update 代理程式會連線至 Microsoft 更新來源，以重新整理可應用的 Microsoft Windows Update 資訊。

若停用此選項，受管理裝置上的 Windows Update 代理程式會使用適用 Microsoft Windows 更新的資訊，此資訊先前從 Microsoft 更新來源取得。

到 Microsoft 更新來源的連線可能消耗資源。若您的其他工作或網路代理政策內容中的**軟體更新和弱點**區域設定一般連線至此更新來源，您可能需要停用此選項。若您不要停用此選項，為了降低伺服器過載，您可設定工作排程來隨機使工作在 360 分鐘內延遲啟動。

預設情況下已啟用該選項。

網路代理政策設定的以下選項組合會定義取得更新的模式：

- 僅當在**尋找弱點和所需更新連線更新伺服器更新資料工作的屬性中**啟用了*連線到更新伺服器以更新資料弱點掃描和所需更新選項*並且**Windows Update 搜尋模式**選項在網路代理政策的設定中被設定為**主動**時，受管理裝置上的 Windows 更新代理才會連線到更新伺服器以獲取更新。
- 如果在執行*弱點掃描*工作時不需要網路代理來啟動與 Microsoft Windows 更新來源的連線並下載更新，則可以將**Windows Update 搜尋模式**選項設為**被動**，同時**連線更新伺服器更新資料**選項必須保持啟用狀態。這可讓您節省資源並使用先前收到的 Windows 更新來掃描弱點。如果您設定以不同方式接收 Microsoft Windows 更新，則可以使用被動模式。如果未以其他方式設定接收 Microsoft Windows 更新，請勿將**Windows Update 搜尋模式**選項設為**被動**，因為在這種情況下，將永遠不會收到有關更新的資訊。
- 無論**連線更新伺服器更新資料**選項是何狀態（啟用還是停用），只要 **Windows Update 搜尋模式**選項被設定為**已停用**，卡巴斯基安全管理中心便不會請求任何更新資訊。

- **搜尋 Kaspersky 列出的第三方弱點和更新**

  如果啟用該選項，卡巴斯基安全管理中心在 Windows 登錄檔和**指定檔案系統中應用程式進階搜尋的路徑**下指定的資料夾中搜尋弱點和協力廠商應用程式所需更新（由非 Kaspersky 和 Microsoft 軟體供應商製作的應用程式）。支援的協力廠商應用程式的完整清單由 Kaspersky 管理。

  如果停用該選項，卡巴斯基安全管理中心不為協力廠商應用程式尋找弱點和所需更新。例如，如果您有帶有不同 Microsoft Windows 更新和協力廠商應用程式更新設定的不同工作，您可能想要停用該選項。

  預設情況下已啟用該選項。

- **指定檔案系統中應用程式進階搜尋的路徑**

  卡巴斯基安全管理中心搜尋需要修復弱點和安裝更新的協力廠商應用程式。您可以使用系統變數。

  指定應用程式安裝資料夾。預設下，清單包含大多數應用程式所安裝的系統資料夾。

- **啟用進階診斷**

  如果啟用該功能，即便寫入偵錯檔案在卡巴斯基安全管理中心遠端診斷公用程式中對網路代理停用，網路代理也寫入偵錯檔案。偵錯輪流寫入兩個檔案中；兩個檔案的最大大小由**進階診斷檔案的最大大小 (MB)**值決定。當兩個檔案都滿時，網路代理再次開始寫入它們。帶有偵錯的檔案儲存在 %WINDIR%\Temp 資料夾。這些檔案在遠端診斷公用程式中可以被存取，您可以在那裡下載或刪除它們。

  如果停用該功能，網路代理根據卡巴斯基安全管理中心遠端診斷公用程式中的設定寫入偵錯。沒有附加偵錯被寫入。

  當建立工作時，您不必啟用進階診斷。您可能想要使用該功能，如果，例如，工作在一些裝置上失敗且您想要在另一個工作執行期間獲取額外資訊。

  預設情況下已停用該選項。

  - **進階診斷檔案的最大大小 (MB)**

    預設值是 100 MB，可用值介於 1 MB 和 2,048 MB 之間。當您所傳送的進階診斷檔案資訊不足以定位問題時，您可能被 Kaspersky 技術支援專家需求變更預設值。

「安裝所需更新並修復弱點」工作設定

工作建立過程中指定的設定

您可以在建立工作時指定以下設定。一些設定也可以在所建立工作的內容中修改。

- **指定安裝更新規則**

  這些規則被套用到用戶端裝置上的更新安裝。如果規則未被指定，工作無可執行。對於使用規則操作的資訊，請參考更新安裝規則。

- **在裝置重新啟動或關閉時開始安裝**

  如果啟用該選項，更新在裝置被重新啟動或關閉時安裝。否則，更新根據排程安裝。

  如果安裝更新可能影響裝置效能則使用該選項。

  預設情況下已停用該選項。

- **安裝所需的一般系統元件**

  如果啟用該選項，在安裝更新之前，應用程式自動安裝所需的所有一般系統元件（先決條件）。例如，這些先決條件可以是作業系統更新。

  如果停用該選項，您可能必須手動安裝先決條件。

  預設情況下已停用該選項。

- **更新過程中允許安裝新的應用程式版本**

  如果啟用該**選項**，如果更新導致軟體應用程式新版本的安裝，更新將被允許。

  如果停用該選項，軟體不被升級。您可以稍後手動或透過其他工作安裝軟體的新版本。例如，如果公司基礎架構不被新軟體版本支援，或者如果您想要在測試基礎架構中檢查升級，您可能使用該選項。

  預設情況下已啟用該選項。

  升級應用程式可能導致安裝在用戶端裝置上的獨立應用程式功能異常。

- **下載更新到裝置而不安裝**

  如果啟用該選項，應用程式下載更新到裝置但是不自動安裝它們。您可以稍後手動安裝下載的更新。

  Microsoft 更新被下載到系統 Windows 儲存。協力廠商應用程式更新（由非 Kaspersky 和 Microsoft 軟體供應商製作的應用程式）會下載到在**下載更新資料夾**欄位指定的資料夾。

  如果停用該選項，更新被自動安裝到裝置。

  預設情況下已停用該選項。

  - **下載更新資料夾**

    該資料夾用於下載協力廠商應用程式（由非 Kaspersky 和 Microsoft 軟體供應商製作的應用程式）更新。

- **啟用進階診斷**

  如果啟用該功能，即便寫入偵錯檔案在卡巴斯基安全管理中心遠端診斷公用程式中對網路代理停用，網路代理也寫入偵錯檔案。偵錯輪流寫入兩個檔案中；兩個檔案的最大大小由**進階診斷檔案的最大大小 (MB)**值決定。當兩個檔案都滿時，網路代理再次開始寫入它們。帶有偵錯的檔案儲存在 %WINDIR%\Temp 資料夾。這些檔案在遠端診斷公用程式中可以被存取，您可以在那裡下載或刪除它們。

  如果停用該功能，網路代理根據卡巴斯基安全管理中心遠端診斷公用程式中的設定寫入偵錯。沒有附加偵錯被寫入。

  當建立工作時，您不必啟用進階診斷。您可能想要使用該功能，如果，例如，工作在一些裝置上失敗且您想要在另一個工作執行期間獲取額外資訊。

  預設情況下已停用該選項。

  - **進階診斷檔案的最大大小 (MB)**

    預設值是 100 MB，可用值介於 1 MB 和 2,048 MB 之間。當您所傳送的進階診斷檔案資訊不足以定位問題時，您可能被 Kaspersky 技術支援專家需求變更預設值。

工作建立後指定的設定

您可以在建立工作後指定下列部分中的設定。有關工作設定的完整說明，請參閱一般工作設定。

- **一般**。此區域會顯示有關工作的一般資訊。此外，您還可以指定哪些裝置應套用*安裝所需更新並修復弱點*工作：

  - **分發到子群組**

    此選項僅在群組工作的設定中可用。

    啟用此選項時，工作範圍包括：

    - 您在建立工作時選擇的管理群組。
    - 依據群組階層，所選管理群組底下任何層級的管理群組。

    停用此選項時，工作範圍僅包括您在建立工作時選擇的管理群組。

    預設情況下已啟用該選項。

  - **分發到從屬和虛擬管理伺服器**

    啟用此選項時，在主管理伺服器上有效的工作也將套用於從屬管理伺服器（包括虛擬伺服器）。如果從屬管理伺服器上已經存在相同類型的工作，則這兩個工作都將套用到從屬管理伺服器上 — 現有的工作和從主管理伺服器繼承的工作。

    此選項僅在**分發到子群組**選項已啟用的情況下可用。

    預設情況下已停用該選項。

- 要安裝的更新

  在**要安裝的更新**區域中，您可以檢視工作安裝的更新清單。僅比對套用的工作設定的更新被顯示。

- 更新的安裝測試：

  - **不掃描**。如果您不希望執行更新的測試安裝，請選取該選項。
  - **在選定裝置上執行掃描**。如果要在指定裝置上測試更新安裝，請選取此選項。點擊**新增**按鈕，然後選取您需要執行測試更新安裝的裝置。
  - **在指定群組中的裝置上執行掃描**。如果要在一組電腦上測試更新安裝，請選取此選項。在**指定測試群組**欄位中，指定您要在其上執行測試更新安裝的一組裝置。
  - **在指定百分比的裝置上執行掃描**。如果要在一部分裝置上測試更新安裝，請選取此選項。在**所有目標裝置中測試裝置的百分比**欄位中，指定您要在其上執行更新測試安裝的裝置比例。

子網路全域清單

該區域提供您在規則中可以使用的子網路全域清單。

要儲存您的網路中的子網路資訊，您可以為您使用的每個管理伺服器設定子網路全域清單。該清單幫助您比對對（IP 位址、遮罩）和實體單元，例如分支辦公室。您可以在網路規則和設定中使用該清單中的子網路。

新增子網路到子網路全域清單

您可以新增子網路和其敘述到子網路全域清單。

要新增子網路到子網路全域清單：

1. 在主控台樹狀目錄中，選取您需要的管理伺服器節點。
2. 在管理伺服器的上下文功能表中，選取**內容**。
3. 在開啟的**內容**視窗中，在**區域**視窗選取**全域子網路清單**。
4. 點擊**新增** 按鈕。
   新子網路 視窗隨即開啟。
5. 填充以下欄位：

   - **一般設定**

     您正新增的子網路的子網路 IP 位址。

   - **子網路遮罩**

     您正新增的子網路的子網路遮罩。

   - **名稱**

     子網路名稱。它必須在子網路全域清單中唯一。如果您輸入清單中已有的名稱，索引將被新增，例如：~~1、~~2。

   - **敘述**

     敘述可能包含一些具有此子網路的分支辦公室的附加資訊。該文字將出現在子網路所在的所有清單，例如，在流量限制規則清單。

     該欄位不是必須的且可以為空。

6. 點擊**確定**。

子網路出現在子網路清單。

在子網路全域清單中檢視和修改子網路內容

您可以在子網路全域清單中檢視和修改子網路內容。

要在子網路全域清單中檢視和修改子網路內容：

1. 在主控台樹狀目錄中，選取您需要的管理伺服器節點。
2. 在管理伺服器的上下文功能表中，選取**內容**。
3. 在開啟的**內容**視窗中，在左側**區域**視窗選取**全域子網路清單**。
4. 在清單，選取您要的子網路。
5. 點擊**內容**按鈕。
   新子網路 視窗隨即開啟。
6. 如果必要，變更子網路設定。
7. 點擊**確定**。

如果您已做了變更，它們將被儲存。

Windows、macOS 和 Linux 網路代理的使用：比較

網路代理的用法因裝置的作業係統而異。網路代理政策和安裝套件設定也根據作業系統不同而不同。下表比較適用於 Windows、macOS 和 Linux 作業系統的網路代理功能和使用情境。

網路代理功能比較

網路代理功能	Windows	macOS	Linux
安裝			
安裝卡巴斯基安全管理中心後，網路代理安裝套件的自動產生功能	✓	–	–
以強制模式安裝，使用卡巴斯基安全管理中心遠端安裝工作的特殊選項	✓	✓	✓
透過程式裝置使用者連結到卡巴斯基安全管理中心產生的獨立安裝套件進行安裝	✓	✓	✓
使用卡巴斯基安全管理中心提供的磁碟映像處理工具，透過複製帶有作業系統和網路代理的管理員硬碟磁碟機映像安裝	✓	–	–
使用協力廠商工具，透過複製帶有作業系統和網路代理的管理員硬碟磁碟機映像安裝	✓	✓	✓
使用應用程式遠端安裝的協力廠商工具佈署	✓	✓	✓
在裝置上手動執行應用程式安裝程式安裝	✓	✓	✓
使用靜默模式安裝網路代理	✓	✓	✓
將用戶端裝置手動連線至管理伺服器。klmover 公用程式	✓	✓	✓
卡巴斯基安全管理中心元件的更新和修補程式的自動安裝	✓	–	–
自動發佈金鑰	✓	✓	✓
強制同步	✓	✓	✓

網路代理功能	Windows	macOS	Linux
發佈點			
用作發佈點	✓	✓	✓
自動分配發佈點	✓	✓ 不使用網路位置感知 (NLA)。	✓ 不使用網路位置感知 (NLA)。
行動模式更新下載	✓	✓	✓
網路輪詢	✓ • IP 範圍輪詢 • Windows 網路輪詢 • Active Directory 輪詢	—	✓ IP 範圍輪詢
在發佈點端執行 KSN 代理服務	✓	—	✓
通過 Kaspersky 更新伺服器將更新下載到將更新發佈到受管理裝置的發佈點儲存區	✓	— (若一或多個執行 Linux 或 macOS 的裝置位於下載更新至發佈點儲存區工作範圍內，該工作會以失敗狀態完成，即使工作已在所有 Windows 裝置上成功完成。)	✓
應用程式的推送安裝	✓	受限制：無法使用 macOS 發佈點在 Windows 裝置上執行推送安裝。	受限制：無法使用 Linux 發佈點在 Windows 裝置上執行推送安裝。
作為推送伺服器使用	✓	—	✓
處理協力廠商應用程式			
在裝置上遠端安裝應用程式	✓	—	—
軟體更新	✓	—	—
在網路代理政策中配置作業系統更新	✓	—	—
檢視軟體弱點資訊	✓	—	—
掃描應用程式以尋找弱點	✓	—	—
清查裝置上所安裝的軟體	✓	—	—
虛擬機			
在虛擬機上安裝網路代理	✓	✓	✓
虛擬桌面基礎結構 (VDI) 的最佳化設定	✓	✓	✓
對動態虛擬機的支援	✓	✓	✓
其他			
在遠端用戶端裝置使用 Windows 共用桌面稽核操作	✓	—	—
監控防毒防護狀態	✓	✓	✓
管理裝置重新啟動	✓	—	—
支援檔案系統復原	✓	✓	✓
使用該網路代理作為連線閘道	✓	✓	✓
連線管理員	✓	✓	✓
從一部管理伺服器切換至另一部的網路代理（依網路位置自動進行）	✓	✓	—
檢查用戶端裝置與管理伺服器之間的連線。klnagchk 公用程式	✓	✓	✓

網路代理功能	Windows	macOS	Linux
用戶端裝置的遠端桌面連線	✓	✓ 透過使用虛擬網路計算 (VNC) 系統。	—
透過移轉精靈下載獨立安裝套件	✓	✓	✓
Zeroconf 輪詢	—	—	✓

按作業系統比較網路代理設定

下表顯示了可用的網路代理設定，具體取決於安裝網路代理的受管理裝置的作業系統。

網路代理設定：按作業系統比較

設定部分	Windows	macOS	Linux
一般	✓	✓	✓
事件配置	✓	✓	✓
設定	✓	✓	✓ 提供以下功能： • **僅透過發佈點分發檔案** • **事件佇列最大值(MB)** • **應用程式被允許在裝置上獲取政策延伸資料**
儲存區	✓	—	✓ 提供以下功能： • **已安裝應用程式詳情** • **硬體登錄資料詳細資訊**
軟體更新和弱點	✓	—	—
重新啟動管理	✓	—	—
Windows 共用桌面	✓	—	—
管理修補程式和更新	✓	—	—
連線→網路	✓	✓	✓ 除了**在 Microsoft Windows 防火牆上開啟網路代理連接埠**選項。
連線→連線設定檔	✓	✓	—
連線→連線排程	✓	✓	✓
透過發佈點的網路輪詢	✓ 只有**Windows 網路**、**IP 範圍**和**Active Directory**選項可用。	—	✓ 提供以下功能： • **Zeroconf** • **IP 範圍**
發佈點網路設定	✓	✓	✓
KSN 代理（發佈點）	✓	—	✓
更新（發佈點）	✓	—	✓
變更歷程	✓	✓	✓

卡巴斯基安全管理中心網頁主控台

本章節說明您可以使用卡巴斯基安全管理中心網頁主控台執行的操作。

關於卡巴斯基安全管理中心網頁主控台

卡巴斯基安全管理中心網頁主控台（以下簡稱「卡巴斯基安全管理中心網頁主控台」）是一個網路應用程式，設計用於管理由卡巴斯基應用程式防護的網路的安全系統狀態。

使用該應用程式，您可以執行以下操作：

- 管理組織的安全系統狀態。
- 將 Kaspersky 應用程式安裝到您網路上的裝置並管理已安裝的應用程式。
- 管理為您網路中的裝置所建立的政策。
- 管理使用者帳戶。
- 管理安裝在您的網路裝置上的應用程式工作。
- 檢視關於安全系統狀態的報告。
- 管理向系統管理員和其他 IT 專家傳送報告的行為。

卡巴斯基安全管理中心網頁主控台是一個網路頁面，可確保您的裝置和管理伺服器能夠透過瀏覽器進行通訊。管理伺服器是一個旨在對您網路中的裝置上安裝的 Kaspersky 應用程式管理的應用程式。管理伺服器透過安全通訊協定 (SSL) 防護的通道連線到您的網路裝置。當您使用瀏覽器連線至卡巴斯基安全管理中心網頁主控台時，瀏覽器會建立與卡巴斯基安全管理中心網頁主控台伺服器的連線。

你按以下方式操作卡巴斯基安全管理中心網頁主控台：

1. 使用瀏覽器連線至卡巴斯基安全管理中心網頁主控台，其中顯示了 Web 入口的介面。
2. 使用網頁入口控件選取您想要執行的指令。卡巴斯基安全管理中心網頁主控台執行以下操作：
    - 如果您已選取用於接收資訊的指令（例如，檢視裝置清單），卡巴斯基安全管理中心網頁主控台會向管理伺服器傳送一個資訊請求，接收必要資料，然後將其以適合檢視的格式傳送到瀏覽器。
    - 如果您已選取用於管理的指令（例如，遠端安裝應用程式），卡巴斯基安全管理中心網頁主控台會從瀏覽器接收該指令並將其傳送至管理伺服器。然後，應用程式從管理伺服器接收結果並以易於檢視的格式將其傳送到瀏覽器。

卡巴斯基安全管理中心網頁主控台是一個多語言的應用程式。您可以在任意時刻變更介面語言，而不重新開啟應用程式。當您將卡巴斯基安全管理中心網頁主控台與卡巴斯基安全管理中心一起安裝時，卡巴斯基安全管理中心網頁主控台具有和安裝檔案一樣的介面語言。當您僅安裝卡巴斯基安全管理中心網頁主控台時，應用程式具有和您的作業系統一樣的介面語言。若卡巴斯基安全管理中心網頁主控台不支援安裝檔案或作業系統的語言，預設會設定為英文。

行動裝置管理在卡巴斯基安全管理中心網頁主控台中不被支援。然而，如果您使用 Microsoft 管理主控台新增行動裝置到管理群組，這些裝置也顯示在卡巴斯基安全管理中心網頁主控台。

卡巴斯基安全管理中心網頁主控台的硬體和軟體需求

卡巴斯基安全管理中心網頁主控台伺服器

最小硬體條件：

- CPU：4 核心，作業頻率 2.5 GHz
- RAM：8 GB
- 可用磁碟空間：40 GB

卡巴斯基安全管理中心網頁主控台伺服器支援的作業係統

作業系統。Microsoft Windows（僅 64 位元版本）：	Windows Server 2012 Server Core Windows Server 2012 Datacenter Windows Server 2012 Essentials Windows Server 2012 Foundation Windows Server 2012 Standard Windows Server 2012 R2 Server Core Windows Server 2012 R2 Datacenter Windows Server 2012 R2 Essentials Windows Server 2012 R2 Foundation Windows Server 2012 R2 Standard Windows Server 2016 Datacenter (LTSB) Windows Server 2016 Standard (LTSB) Windows Server 2016 Server Core（安裝選項）(LTSB) Windows Server 2019 Standard Windows Server 2019 Datacenter Windows Server 2019 Core Windows Server 2022 Standard Windows Server 2022 Datacenter Windows Server 2022 Core Windows Storage Server 2012 Windows Storage Server 2012 R2 Windows Storage Server 2016 Windows Storage Server 2019
作業系統。Linux（僅 64 位元版本）	Debian GNU/Linux 9.x (Stretch) Debian GNU/Linux 10.x (Buster) Debian GNU/Linux 11.x (Bullseye) Ubuntu Server 18.04 LTS (Bionic Beaver) Ubuntu Server 20.04 LTS (Focal Fossa) Ubuntu Server 22.04 LTS (Jammy Jellyfish) CentOS 7.x Red Hat Enterprise Linux Server 7.x Red Hat Enterprise Linux Server 8.x Red Hat Enterprise Linux Server 9.x SUSE Linux Enterprise Server 12（所有服務套件） SUSE Linux Enterprise Server 15（所有服務套件） Astra Linux 特別版 RUSB.10015-01（操作更新 1.6） Astra Linux 特別版 RUSB.10015-01（操作更新 1.7）

	Astra Linux 通用版 2.12 ALT Server 9.2 ALT Server 10 ALT 8 SP Server (LKNV.11100-01) ALT 8 SP Server (LKNV.11100-02) ALT 8 SP Server (LKNV.11100-03) Oracle Linux 7 Oracle Linux 8 Oracle Linux 9 RED OS 7.3 Server RED OS 7.3 認證版 基於內核的虛擬機（卡巴斯基安全管理中心網頁主控台伺服器支援的所有 Linux 作業系統）

用戶端裝置

對於用戶端裝置，卡巴斯基安全管理中心網頁主控台的使用僅需要一個瀏覽器。

最小螢幕解析度為 1366x768 像素。

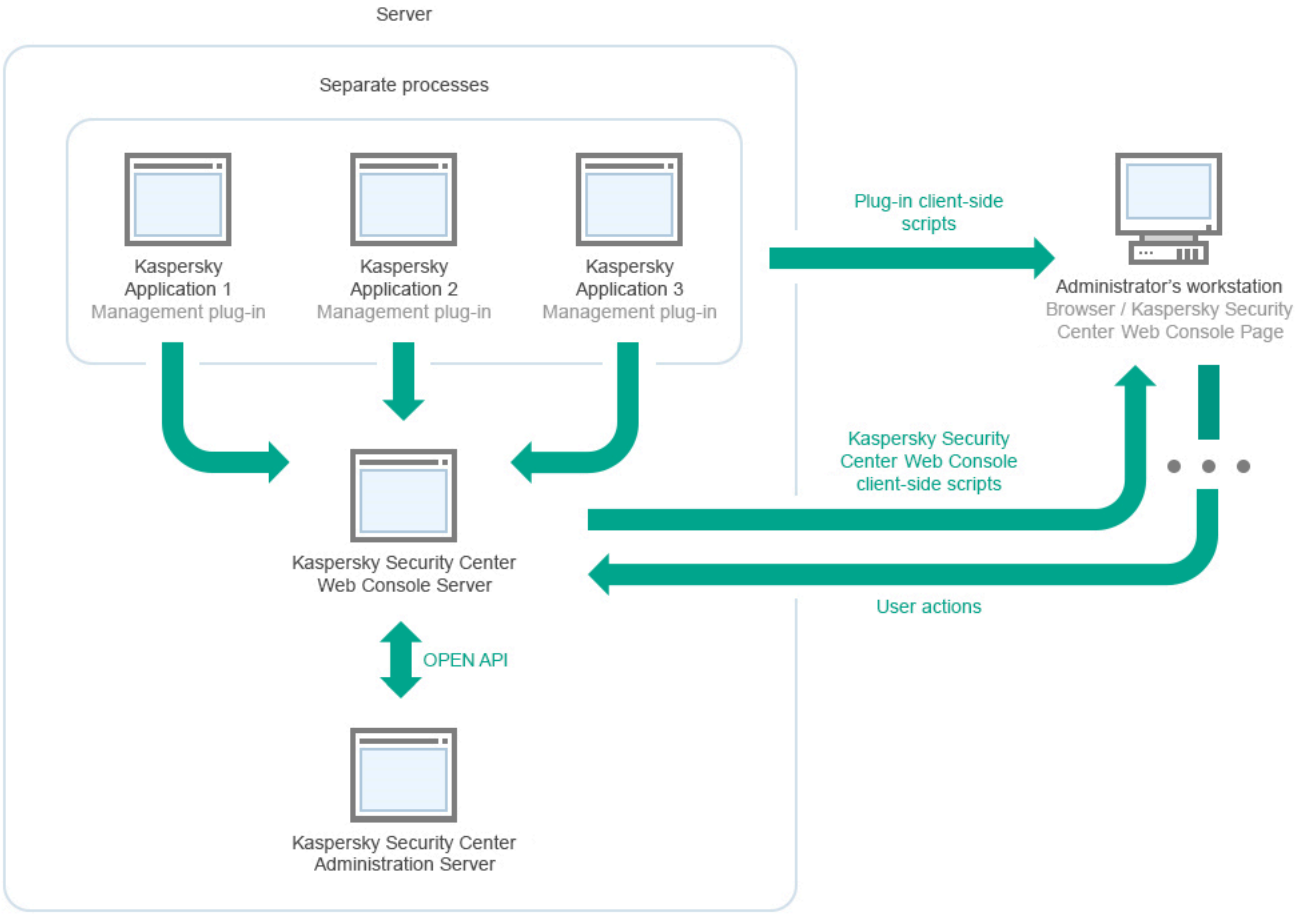
裝置的硬體和軟體需求和卡巴斯基安全管理中心網頁主控台所使用的瀏覽器的需求是相同的。

瀏覽器：

- Mozilla Firefox 延伸程式支援版本 91.8.0 或更高版本（91.8.0 於 2022 年 4 月 5 日發布）
- Google Chrome 100.0.4896.88 或更高版本（官方版本）
- Microsoft Edge 100 或更高版本
- macOS 的 Safari 15

卡巴斯基安全管理中心管理伺服器佈署圖表和卡巴斯基安全管理中心網頁主控台

下圖顯示卡巴斯基安全管理中心管理伺服器佈署圖表和卡巴斯基安全管理中心 網頁主控台



卡巴斯基安全管理中心管理伺服器佈署圖表和卡巴斯基安全管理中心網頁主控台

安裝到受防護裝置上的 Kaspersky 應用程式管理外掛程式（每個應用程式一個外掛程式）與卡巴斯基安全管理中心 網頁主控台伺服器一起佈署。

作為管理員，您透過使用工作站瀏覽器來存取卡巴斯基安全管理中心 網頁主控台。

當您在卡巴斯基安全管理中心 網頁主控台中執行特定操作時，卡巴斯基安全管理中心 網頁主控台伺服器會與卡巴斯基安全管理中心管理伺服器透過 OpenAPI 通訊。卡巴斯基安全管理中心 網頁主控台伺服器會從卡巴斯基安全管理中心管理伺服器要求必要資訊，並在卡巴斯基安全管理中心 網頁主控台中顯示操作結果。

卡巴斯基安全管理中心 網頁主控台使用的連接埠

下表列出必須在已安裝卡巴斯基安全管理中心 網頁主控台伺服器（又稱為卡巴斯基安全管理中心 網頁主控台）的裝置上開啟的連接埠。

卡巴斯基安全管理中心 網頁主控台使用的連接埠

埠號	服務名稱	協定	連接埠目的	範圍
2001	卡巴斯基安全管理中心產品外掛程式伺服器	HTTPS	被管理外掛程式處理程序用來接收來自"卡巴斯基安全管理中心網頁主控台管理服務"的請求的 API 連接埠	執行管理外掛程式的 node.exe 處理程序
1329，2003	卡巴斯基安全管理中心網頁主控台管理服務	HTTPS	被用來接收在相同裝置上執行之"卡巴斯基安全管理中心網頁主控台服務"的要求的 API 連接埠	更新卡巴斯基安全管理中心 網頁主控台元件
2005	卡巴斯基安全管理中心網頁主控台	HTTPS	被用來接收在相同裝置上執行之"卡巴斯基安全管理中心網頁主控台服務"的要求的 API 連接埠	執行卡巴斯基安全管理中心 網頁主控台的 node.exe 處理程序
3333	Kaspersky OSMP KAS 服務	HTTPS	OAuth2.0 授權端點連接埠	身分和存取管理器
4004	Kaspersky OSMP Facade 服務	HTTPS	OAuth2.0 身分提供者連接埠	身分和存取管理器
4444	Kaspersky OSMP KAS 服務	HTTPS	OAuth2.0 Token introspection 端點連接埠	身分和存取管理器
8200	—	HTTP	透過 HashiCorp Vault 產生憑證的 API 連接埠（如需詳細資訊，請參閱 HashiCorp Vault 網站）	安裝卡巴斯基安全管理中心 網頁主控台並更新卡巴斯基安全管理中心 網頁主控台元件
4150, 4151, 4152	卡巴斯基安全管理中心網頁主控台訊息佇列	HTTPS	處理卡巴斯基安全管理中心 網頁主控台和管理外掛程式之間通訊所用的訊息代理 API 連接埠	卡巴斯基安全管理中心 網頁主控台和管理外掛程式之間的互動

下表列出了在安裝了卡巴斯基安全管理中心 網頁主控台伺服器的裝置上不必開啟的連接埠。但是，卡巴斯基安全管理中心 網頁主控台會將這些連接埠用於身分和存取管理器。

卡巴斯基安全管理中心 網頁主控台為身分和存取管理器使用的連接埠

埠號	服務名稱	協定	連接埠目的	範圍
4445	Kaspersky OSMP KAS 服務	HTTPS	為 OAuth2.0 授權端點連接埠從卡巴斯基安全管理中心 網頁主控台接收配置的的身分和存取管理器主連接埠（有關 OAuth 2.0 的更多資訊，請參閱 OAuth 網站）	身分和存取管理器
2444	Kaspersky OSMP Facade 服務	HTTPS	用於配置身分和存取管理器的連接埠	身分和存取管理器
2445	Kaspersky OSMP Facade 服務	HTTPS	用於將 "Kaspersky OSMP KAS 服務"連線到 "Kaspersky OSMP Facade 服務"的連接埠	身分和存取管理器

情境：卡巴斯基安全管理中心網頁主控台的安裝和初始化設定

此情境說明如何安裝卡巴斯基安全管理中心管理伺服器和卡巴斯基安全管理中心網頁主控台，您可使用快速啟動精靈來執行管理伺服器的初始設定，並使用防護佈署精靈在受管理裝置上安裝卡巴斯基應用程式。

卡巴斯基安全管理中心網頁主控台安裝和初始化設定分步驟進行：

1. **安裝資料庫管理系統 (DBMS)**

   安裝卡巴斯基安全管理中心將使用的 DBMS，或者使用現有資料庫。

   對於如何安裝所選 DBMS 的資訊，請參考其文件。

2. **安裝管理伺服器、管理主控台、網路代理**

   管理主控台和網路代理的伺服器版本與管理伺服器一起安裝。

在安裝卡巴斯基安全管理中心管理伺服器時，指定您是否要安裝卡巴斯基安全管理中心網頁主控台到相同裝置。如果您選取安裝元件到相同裝置，您不必另外安裝卡巴斯基安全管理中心網頁主控台，因為它是自動安裝的。如果您要安裝卡巴斯基安全管理中心網頁主控台到不同裝置，那麼在安裝卡巴斯基安全管理中心管理伺服器後，繼續安裝卡巴斯基安全管理中心網頁主控台。

3 安裝卡巴斯基安全管理中心網頁主控台

如果您在上一步未選取將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伺服器一起安裝，安裝卡巴斯基安全管理中心網頁主控台到不同裝置。您可以將已安裝卡巴斯基安全管理中心網頁主控台安裝在不同裝置上或安裝了管理伺服器的同一裝置上。

4 執行初始化設定

當管理伺服器安裝完成後，在第一次連線至管理伺服器時，快速啟動精靈自動開始。依據現有需求指定管理伺服器初始化設定。在初始化配置步驟，精靈使用預設設定建立防護佈署所需的政策和工作。然而，預設設定可能少於您組織需要的最優設定。您可以編輯政策和工作設定。

5 卡巴斯基安全管理中心授權（可選）

有管理主控台基本功能支援的卡巴斯基安全管理中心不需要產品授權。如果您要使用一個或幾個附加功能，包括「弱點和修補程式管理」、「行動裝置管理」和「與 SIEM 系統整合」，則您需要商業產品授權。您可在快速啟動精靈對應步驟或手動針對這些功能新增金鑰檔案或啟動碼。

6 網路裝置探索

該步驟使用快速啟動精靈執行。您也可以手動發現裝置。卡巴斯基安全管理中心接收網路中偵測到的所有裝置的位址和名稱。然後您可以使用卡巴斯基安全管理中心在偵測到的裝置上安裝 Kaspersky 應用程式和其他供應商的軟體。卡巴斯基安全管理中心定期啟動裝置發現，這意味著如果任何新實例出現在網路，它們將被自動偵測。

7 整理裝置到管理群組

該步驟使用快速啟動精靈執行，但您也可以手動移動偵測到的裝置到群組。

8 安裝網路代理和安全應用程式到網路裝置

企業網路的防護佈署涉及到在裝置發現中管理伺服器偵測到的裝置上安裝網路代理和安全應用程式（例如，Kaspersky Endpoint Security for Windows）。

要遠端安裝應用程式，執行防護佈署精靈。

安全應用程式防護裝置以防病毒和其他威脅程式。網路代理確保裝置和管理伺服器之間的通訊。網路代理設定預設被自動配置。

在您開始安裝網路代理和安全應用程式到網路裝置之前，確保這些裝置是可存取的（已開啟電源）。

9 佈署產品授權金鑰到用戶端裝置

佈署產品授權金鑰到用戶端裝置以在這些裝置上啟動受管理安全應用程式。

10 安裝 Kaspersky Security for Mobile（可選）

如果您計劃管理公司行動裝置，請按照 Kaspersky Security for Mobile 說明 中提供的指示瞭解有關 Kaspersky Endpoint Security for Android 部署的資訊。

11 配置 Kaspersky 應用程式政策

要應用不同應用程式設定到不同裝置，您可以使用以裝置為中心的安全管理和/或以使用者為中心的安全管理。以裝置與中心的安全管理可以使用政策和工作實現。您僅可以套用工作到滿足特定條件的裝置。要設定篩選裝置的條件，使用裝置分類和標籤。

12 監控網路防護狀態

您可以使用儀表板的工具來監控您的網路，從卡巴斯基應用程式產生報告，配置和檢視從受管理裝置上的應用程式接收的事件分類，以及檢視通知清單。

安裝

該部分敘述了卡巴斯基安全管理中心和卡巴斯基安全管理中心 網頁主控台的安裝。

安裝卡巴斯基安全管理中心網頁主控台

該部分描述了如何單獨安裝卡巴斯基安全管理中心網頁主控台伺服器（也叫卡巴斯基安全管理中心網頁主控台）。安裝之前，您必須安裝資料庫管理系統和卡巴斯基安全管理中心管理伺服器。您可以在安裝卡巴斯基安全管理中心的同一台裝置或另一台裝置上安裝卡巴斯基安全管理中心網頁主控台。

要安裝卡巴斯基安全管理中心網頁主控台：

1. 在具有管理員權限的帳戶下，執行 ksc-web-console-<版本號>.<組建編號>.exe 安裝檔案。

   這會啟動安裝精靈。

2. 選取安裝精靈的語言。

3. 在歡迎視窗，點擊**下一步**。

4. 在**產品授權協議**視窗閱讀並接受最終使用者產品授權協議。安裝在您接受最終使用者產品授權協議後繼續，否則**下一步**按鈕不可用。

5. 在**目的資料夾**視窗中，選取要安裝卡巴斯基安全管理中心 網頁主控台的資料夾（預設為 %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console）。如果這個資料夾不存在，安裝精靈將會自動的產生此資料夾。

   您可以使用**瀏覽**按鈕變更目的資料夾。

6. 在 **卡巴斯基安全管理中心網頁主控台連線設定**視窗，指定以下資訊：

   - 卡巴斯基安全管理中心網頁主控台位址（預設 127.0.0.1）。
   - 卡巴斯基安全管理中心網頁主控台將用於傳入連線的連接埠，即用於從瀏覽器存取卡巴斯基安全管理中心網頁主控台的連接埠（預設為 8080）。

   我們建議您為位址和埠號選取預設值。

   如果願意，您可以點擊**測試**以確保所選連接埠可用。

   如果您要啟用卡巴斯基安全管理中心網頁主控台活動記錄，選取適當選項。如果您不選取該選項，將不會建立卡巴斯基安全管理中心網頁主控台記錄檔案。

7. 在**帳戶設定**視窗，指定帳戶名稱和密碼。

   我們建議您使用預設帳戶。

8. 在**用戶端憑證**視窗，選取以下之一：

- **產生新憑證**。如果您沒有瀏覽器憑證，則建議該選項。
- **選取現有憑證**。如果您已經擁有瀏覽器憑證，則選取該選項；此種情況下，指定其路徑。
- 如果您選擇產生新的憑證，當您開啟卡巴斯基安全管理中心網頁主控台時，瀏覽器可能會通知您與卡巴斯基安全管理中心網頁主控台的連線不是私密連線，並且卡巴斯基安全管理中心網頁主控台憑證無效。出現此警告是因為卡巴斯基安全管理中心網頁主控台憑證為自我簽署憑證，並且由卡巴斯基安全管理中心自動產生。若要移除此警告，請建立一個在您的基礎架構中受信任且滿足自訂憑證的要求的憑證。接下來，在**用戶端憑證**視窗中選擇**選取現有憑證**選項，然後指定您的自訂憑證的路徑。

卡巴斯基安全管理中心網頁主控台不支援 PFX 格式的憑證。要使用這樣的憑證，您必須使用基於 OpenSSL 的跨平台公用程式（例如 Windows OpenSSL）將其轉換為受支援的 PEM 格式。

9. 在**受信任的管理伺服器**視窗，確保您的管理伺服器在清單中，然後按**下一步**以繼續安裝程式的最後一個視窗。

如果您需要將新的管理伺服器新增到清單中，請點擊**新增**按鈕。在開啟的視窗中，指定新的受信任管理伺服器的內容：

- **管理伺服器名稱**

  將顯示在卡巴斯基安全管理中心網頁主控台登入視窗中的管理伺服器名稱。

- **管理伺服器位址**

  安裝管理伺服器的裝置的 IP 位址。

- **管理伺服器連接埠**

  卡巴斯基安全管理中心網頁主控台用於連線管理伺服器的 OpenAPI 連接埠（預設值為 13299）。

- **管理伺服器憑證**

  憑證檔案儲存在安裝管理伺服器的裝置上。管理伺服器憑證的預設路徑：

  - 對於 Windows—%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert
  - 對於 Linux—/var/opt/kaspersky/klnagent_srv/1093/cert/

  如果您在安裝管理伺服器的同一裝置上安裝卡巴斯基安全管理中心網頁主控台，請使用上面給出的路徑之一。否則，將憑證檔案從安裝管理伺服器的裝置複製到安裝卡巴斯基安全管理中心網頁主控台的裝置，然後指定憑證的本機路徑。

10. 在 **身分識別與存取管理器 (IAM)** 視窗，指定是否要安裝 Identity and Access Manager （也稱為 IAM）。如果選擇安裝身分和存取管理器，請指定以下連接埠號：

    - **KAS 管理員連接埠**。預設情況下使用連接埠 4445 從卡巴斯基安全管理中心網頁主控台接收適用於 OAuth2.0 授權端點連接埠的配置。
    - **Facade 管理員連接埠**。預設情況下使用連接埠 2444 配置身分和存取管理器。
    - **Facade 互動連接埠**。預設情況下使用連接埠 2445 將 Kaspersky OSMP KAS 服務連線到 Kaspersky OSMP Facade 服務。

    如果願意，您可以變更預設連接埠號。將來您將無法透過卡巴斯基安全管理中心網頁主控台變更它們。

11. 在安裝程式的最後一個視窗，點擊**安裝**以開始安裝。

在安裝成功完成後，桌面上會出現一個捷徑，您可以登入到卡巴斯基安全管理中心網頁主控台。

管理伺服器快速啟動精靈開始，如果您未在基於 Microsoft Management Console 的管理主控台執行。

故障解決

如果瀏覽器未在您鍵入的 URL 上顯示卡巴斯基安全管理中心網頁主控台，請嘗試以下操作：

1. 檢查您是否指定了安裝了卡巴斯基安全管理中心網頁主控台的裝置的正確主機名稱或 IP 位址。
2. 檢查您要操作的裝置是否具有安裝了卡巴斯基安全管理中心網頁主控台的裝置的存取權限。
3. 檢查安裝了卡巴斯基安全管理中心網頁主控台的裝置的防火牆設定是否允許應用程式 node.exe 透過連接埠 8080 的入站連線。
4. 在 Windows，開啟**服務**。檢查卡巴斯基安全管理中心網頁主控台服務是否正在執行。
5. 檢查您是否可以使用管理主控台存取卡巴斯基安全管理中心。
6. 在 Windows，開啟**事件檢視器**，然後選取**應用程式和服務日誌 → 卡巴斯基事件記錄**。確保日誌不包含錯誤。

安裝卡巴斯基安全管理中心 網頁主控台到 Linux 平台

該部分描述了如何安裝卡巴斯基安全管理中心 網頁主控台伺服器（也叫卡巴斯基安全管理中心 網頁主控台）到執行 Linux 作業系統的裝置（參見支援的 Linux 分類清單）。

安裝卡巴斯基安全管理中心網頁主控台到 Linux 平台

該部分描述了如何單獨安裝卡巴斯基安全管理中心網頁主控台伺服器（也叫卡巴斯基安全管理中心網頁主控台）到執行 Linux 作業系統的裝置。安裝之前，您必須安裝資料庫管理系統和卡巴斯基安全管理中心管理伺服器。

使用與您裝置上安裝的 Linux 發佈相對應的以下安裝檔案之一：

- 對於 Debian: ksc-web-console-<build number>.x86_64.deb
- 對於基於 RPM 的作業系統: ksc-web-console-<build number>.x86_64.rpm
- 對於 Alt 8 SP: ksc-web-console-<build number>-alt8p.x86_64.rpm

您透過從 Kaspersky 網站下載來接收安裝檔案。

要安裝卡巴斯基安全管理中心網頁主控台：

1. 確保您要安裝卡巴斯基安全管理中心網頁主控台的裝置執行支援的 Linux 分類。
2. 閱讀最終使用者產品授權協議 (EULA)。如果卡巴斯基安全管理中心分發套件不包含帶有 EULA 文字的 TXT 檔案，您可以從卡巴斯基網站 下載此檔案。如果您不接受產品授權協議中的條款，不要安裝應用程式。

3. 建立包含參數的回應檔案以連線卡巴斯基安全管理中心網頁主控台到管理伺服器。命名該檔案為 ksc-web-console-setup.json，然後將其放置到以下目錄：/etc/ksc-web-console-setup.json。

   回應檔案的一個例子，它包含最小參數集以及預設位址和連接埠：

   ```
   {
     "address": "ksc.example.com",
     "port": 8080,
     "trusted":
   "192.168.2.130|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC 伺服器",
     "acceptEula": true
   }
   ```

   在 Linux ALT 作業系統上安裝卡巴斯基安全管理中心網頁主控台時，必須指定 8080 以外的連接埠號，因為作業系統使用的是連接埠 8080。

   卡巴斯基安全管理中心網頁主控台無法使用相同的 .rpm 安裝檔案更新。如果您要在回應檔案中變更設定並使用該檔案重新安裝應用程式，您必須先移除該應用程式，然後使用新的回應檔案再次安裝。

4. 在具有根特權的帳戶下，根據您的 Linux 分類使用命令列執行 .deb 或 .rpm 安裝檔案。

   - 要從 .deb 檔案安裝或升級卡巴斯基安全管理中心網頁主控台，執行以下指令：
     ```
     $ sudo dpkg -i ksc-web-console-<build number>.deb
     ```
   - 要從 .rpm 檔案安裝卡巴斯基安全管理中心網頁主控台，請執行以下指令之一：
     ```
     $ sudo rpm -ivh --nodeps ksc-web-console-<build number>.x86_64.rpm
     ```
   - 若要升級卡巴斯基安全管理中心網頁主控台的先前版本，請執行以下命令之一：
     - 對於執行基於 RPM 的作業系統的裝置：
       ```
       $ sudo rpm -Uvh --nodeps --force ksc-web-console-<build number>.x86_64.rpm
       ```
     - 對於執行基於 Debian 的作業系統的裝置：
       ```
       $ sudo dpkg -i ksc-web-console-<build number>.x86_64.deb
       ```

   這會開始解壓縮安裝檔案。請等待安裝完成。卡巴斯基安全管理中心網頁主控台會安裝到以下目錄：/var/opt/kaspersky/ksc-web-console。

當安裝完成時，您可以使用您的瀏覽器開啟和登入卡巴斯基安全管理中心網頁主控台。

卡巴斯基安全管理中心網頁主控台安裝參數

對於在執行 Linux 的裝置上安裝卡巴斯基安全管理中心網頁主控台伺服器，您必須建立一個 JSON 格式的回應檔案，它包含用於連線卡巴斯基安全管理中心網頁主控台到管理伺服器的參數。

回應檔案的一個例子，它包含最小參數集以及預設位址和連接埠：

```
{
  "address": "ksc.example.com",
  "port": 8080,
  "defaultLangId": 1049,
  "enableLog": false,
```

```
  "trusted":
"192.168.2.130|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC Server",
  "acceptEula": true,
  "certPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer",
  "webConsoleAccount": "Group1:User1",
  "managementServiceAccount": "Group1:User2",
  "serviceWebConsoleAccount": "Group1:User3",
  "pluginAccount": "Group1:User4",
  "messageQueueAccount": "Group1:User5"
}
```

在 Linux ALT 作業系統上安裝卡巴斯基安全管理中心網頁主控台時，必須指定 8080 以外的連接埠號，因為作業系統使用的是連接埠 8080。

下表描述了可以在回應檔案中指定的參數。

安裝卡巴斯基安全管理中心網頁主控台到執行 Linux 的裝置的參數

參數	敘述	可用值
`address`	卡巴斯基安全管理中心網頁主控台伺服器（必需）。	字串值。
`port`	卡巴斯基安全管理中心網頁主控台將用於連線到管理伺服器的連接埠號（必需）。	數值。
`defaultLangId`	使用者介面語言（預設，`1033`）。	語言數位： • 德文：`1031` • 英文：`1033` • 西班牙文：`3082` • 西班牙文（墨西哥）：`2058` • 法文：`1036` • 日文：`1041` • 哈薩克文：`1087` • 波蘭文：`1045` • 葡萄牙文（巴西）：`1046` • 俄文：`1049` • 土耳其文：`1055` • 簡體中文：`4` • 繁體中文：`31748` 如果沒有指定值，則使用 English 語言。
`enableLog`	是否要啟用卡巴斯基安全管理中心網頁主控台活動記錄。	布爾值： • `true`—啟用記錄（預設選中）。 • `false`—停用記錄。

參數	敘述	可用值
`trusted`	允許連線卡巴斯基安全管理中心網頁主控台的信任的管理伺服器清單（必須）。各管理伺服器必須以下列參數定義： • 管理伺服器位址 • 卡巴斯基安全管理中心網頁主控台用以連線到管理伺服器的 OpenAPI 連接埠（預設是 13299） • 管理伺服器憑證路徑 • 將顯示在登入視窗的管理伺服器名稱 參數使用豎線分隔。如果指定了幾個管理伺服器，使用兩個豎線將它們分隔。	以下格式的字串值： "< 伺服器位址 >|< 連接埠 >|< 憑證路徑 >|< 伺服器名稱 >"。 示例： `"X.X.X.X|13299|/cert/server-1.cer|Server 1||Y.Y.Y.Y|13299|/cert/server-2.cer|Server 2"`。
`acceptEula`	您是否要接受最終使用者產品授權協議（EULA）的條款。包含 EULA 條款的檔案和安裝檔案一起下載（必須）。	布爾值： • `true` — 我確認我已完整閱讀、理解並接受此最終使用者產品授權協議的條款和條件。 • `false`—我不接受產品授權協議的條款（預設選取）。
`certDomain`	如果您要產生新憑證，使用該參數指定產生新憑證的網域名稱。	字串值。
`certPath`	如果您要使用現有憑證，使用該參數指定憑證檔案位置。	字串值。 指定路徑" `/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer` "以使用現有憑證。對於自訂憑證，請指定儲存此自訂憑證的路徑。
`keyPath`	如果您要使用現有憑證，使用該參數指定金鑰檔案位置。	字串值。
`webConsoleAccount`	執行卡巴斯基安全管理中心網頁主控台服務的帳戶名稱。	以下格式的字串值："< 群組名稱 >:< 使用者名稱 >"。 例如：`""Group1:User1""`. 如果未指定任何值，卡巴斯基安全管理中心網頁主控台安裝程式會建立一個預設名稱為 `user_management_%uid%` 的新帳戶。
`managementServiceAccount`	執行卡巴斯基安全管理中心網頁主控台管理服務的特權帳戶名稱。	以下格式的字串值："< 群組名稱 >:< 使用者名稱 >"。 例如：`""Group1:User1""`. 如果未指定任何值，卡巴斯基安全管理中心網頁主控台安裝程式會建立一個預設名稱為 `user_nodejs_%uid%` 的新帳戶。
`serviceWebConsoleAccount`	執行卡巴斯基安全管理中心網頁主控台服務的帳戶名稱。	以下格式的字串值："< 群組名稱 >:< 使用者名稱 >"。 例如：`""Group1:User1""`. 如果未指定任何值，卡巴斯基安全管理中心網頁主控台安裝程式會建立一個預設名稱為 `user_svc_nodejs_%uid%` 的新帳戶。
`pluginAccount`	執行卡巴斯基安全管理中心產品外掛程式伺服器服務的帳戶名稱。	以下格式的字串值："< 群組名稱 >:< 使用者名稱 >"。 例如：`""Group1:User1""`. 如果未指定任何值，卡巴斯基安全管理中心網頁主控台安裝程式會建立一個預設名稱為 `user_web_plugin_%uid%` 的新帳戶。
`messageQueueAccount`	執行卡巴斯基安全管理中心網頁主控台訊息佇列服務的帳戶名稱。	以下格式的字串值："< 群組名稱 >:< 使用者名稱 >"。 例如：`""Group1:User1""`. 如果未指定任何值，卡巴斯基安全管理中心網頁主控台安裝程式會建立一個預設名稱為 `user_message_queue_%uid%` 的新帳戶。

基於安全性原因，我們不建議使用`webConsoleAccount`、`managementServiceAccount`、`serviceWebConsoleAccount`、`pluginAccount`和`messageQueueAccount`參數。

如果您指定 `webConsoleAccount`、`managementServiceAccount`、`serviceWebConsoleAccount`、`pluginAccount` 或 `messageQueueAccount` 參數，請確保自訂使用者帳戶屬於同一安全群組。如果未指定這些參數，卡巴斯基安全管理中心網頁主控台安裝程式會建立一個預設安全群組，然後在該組中建立具有預設名稱的使用者帳戶。

安裝連線到安裝在容錯移轉叢集節點上的管理伺服器的卡巴斯基安全管理中心網頁主控台

本節介紹如何安裝卡巴斯基安全管理中心網頁主控台伺服器（以下也稱為卡巴斯基安全管理中心網頁主控台），它連線到安裝在卡巴斯基安全管理中心或 Windows Server 容錯移轉叢集節點上的管理伺服器。在安裝卡巴斯基安全管理中心網頁主控台之前，請在卡巴斯基安全管理中心容錯移轉叢集節點或在Windows Server 容錯移轉叢集節點上安裝一個資料庫管理系統和卡巴斯基安全管理中心管理伺服器。

如果您使用 Windows Server 容錯移轉叢集，我們不建議在容錯移轉叢集節點上安裝卡巴斯基安全管理中心網頁主控台。如果節點出現故障，您將無法存取管理伺服器。

要安裝連線到安裝在容錯移轉叢集節點上的管理伺服器的卡巴斯基安全管理中心網頁主控台：

1. 執行卡巴斯基安全管理中心網頁主控台安裝步驟, 從第 1 步開始到第 8 步。
2. 在第 9 步，在**受信任的管理伺服器**視窗中，點擊**新增**按鈕將故障移轉叢集新增為受信任的管理伺服器。

   在開啟的視窗中，指定以下內容：

   - **管理伺服器名稱**

     將顯示在卡巴斯基安全管理中心網頁主控台登入視窗中的叢集名稱。

   - **管理伺服器位址**

     根據容錯移轉叢集類型，指定叢集位址：

     - **卡巴斯基安全管理中心容錯移轉叢集**。如果您在準備叢集節點時建立了介面卡，請指定從屬網路介面卡的 IP 位址作為叢集位址。否則，請指定您使用的協力廠商負載均衡器的 IP 位址。
     - **Windows Server 容錯移轉叢集**。指定您在建立 Windows Server 容錯移轉叢集時獲得的叢集位址。

   - **管理伺服器連接埠**

     卡巴斯基安全管理中心網頁主控台用於連線管理伺服器的 OpenAPI 連接埠（預設值為 13299）。

   - **管理伺服器憑證**

     管理伺服器憑證位於卡巴斯基安全管理中心容錯移轉叢集或者 Windows Server 容錯移轉叢集的共用資料儲存中。憑證檔案的預設路徑：<shared data folder> \1093\cert\klserver.cer。將憑證檔案從共用資料儲存複製到安裝卡巴斯基安全管理中心網頁主控台的裝置。指定管理伺服器憑證的本機路徑。

3. 繼續執行卡巴斯基安全管理中心網頁主控台的標準安裝。

在安裝完成後，桌面上會出現一個捷徑，您可以登入到卡巴斯基安全管理中心網頁主控台。

升級卡巴斯基安全管理中心網頁主控台

如果要使用更高版本的卡巴斯基安全管理中心網頁主控台而不刪除當前安裝的實例，則可以使用卡巴斯基安全管理中心網頁主控台安裝程式中提供的標準升級過程。

若要升級卡巴斯基安全管理中心網頁主控台：

1. 在具有管理員權限的帳戶下，執行 ksc-web-console-<版本號>.<組建編號>.exe 安裝檔案，其中 <組建編號> 代表卡巴斯基安全管理中心網頁主控台內部版本，其編號高於目前安裝實例。

2. 在開啟的"安裝精靈"視窗中，選取一種語言，然後點擊**確定**。

3. 在歡迎視窗中，選取**升級**選項，然後點擊**下一步**。

4. 在**產品授權協議**視窗閱讀並接受最終使用者產品授權協議。安裝在您接受最終使用者產品授權協議後繼續，否則**下一步**按鈕不可用。

5. 逐步完成安裝精靈的步驟，直到您完成安裝。進行時，您還可以修改在先前安裝期間指定的卡巴斯基安全管理中心 網頁主控台設定。當您進行**卡巴斯基安全管理中心網頁主控台修改已就緒**步驟時，請點擊**升級**按鈕。等待套用新設定的作業完成，然後在安裝精靈的下一步中，點擊**完成**。您也可以點擊**在您的瀏覽器中啟動卡巴斯基安全管理中心網頁主控台**連結，以立即啟動卡巴斯基安全管理中心 網頁主控台的升級實例。

   僅卡巴斯基安全管理中心網頁主控台版本 12.2 或更高版本中，才可要在升級期間修改卡巴斯基安全管理中心網頁主控台設定。

   已安裝卡巴斯基安全管理中心網頁主控台伺服器。

用於卡巴斯基安全管理中心網頁主控台的憑證

本節介紹如何發佈和替代卡巴斯基安全管理中心網頁主控台憑證，以及如何在伺服器與卡巴斯基安全管理中心網頁主控台交互動為管理伺服器續訂憑證。

取代卡巴斯基安全管理中心網頁主控台憑證

預設下，當您安裝卡巴斯基安全管理中心 網頁主控台伺服器時，應用程式的瀏覽器憑證被自動產生。您可以使用自訂憑證取代自動產生的憑證。

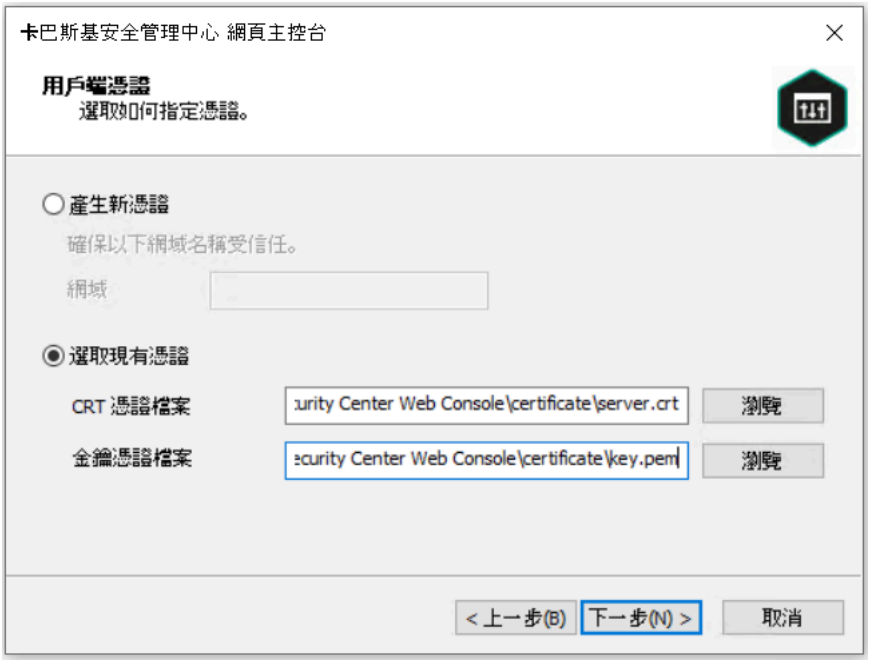
要用自訂憑證卡巴斯基安全管理中心 網頁主控台伺服器的憑證：

1. 在安裝了卡巴斯基安全管理中心 網頁主控台伺服器的裝置上，在具有管理員權限的帳戶下執行 ksc-web-console-<版本號>.exe 安裝檔案。

   這會啟動安裝精靈。

2. 在精靈的第一頁，選擇**升級**選項。

3. 在**用戶端憑證**頁面，選擇**選擇現有憑證**選項並指定自訂憑證的路徑。



指定用戶端憑證

4. 在精靈的最後一頁，點擊**修改**以套用設定。

5. 在應用程式重新設定成功完成後，按一下**完成**按鈕。

卡巴斯基安全管理中心網頁主控台使用指定的憑證工作。

在卡巴斯基安全管理中心網頁主控台中，為受信任的管理伺服器指定憑證

現有管理伺服器憑證在過期日期之前被新憑證自動取代。您也可以使用自訂憑證取代現有管理伺服器憑證。每次變更憑證時，新憑證必須在卡巴斯基安全管理中心網頁主控台設定中被指定。否則，卡巴斯基安全管理中心網頁主控台將無法連線到管理伺服器。

要指定管理伺服器新憑證：

1. 在管理伺服器所在裝置上，複製憑證檔案到（例如大容量）儲存裝置。

   預設情況下，憑證檔案儲存在以下資料夾中：

   - 對於 Windows—%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert
   - 對於 Linux—/var/opt/kaspersky/klnagent_srv/1093/cert/

2. 在安裝了卡巴斯基安全管理中心網頁主控台的裝置上，將憑證檔案放到本機資料夾。

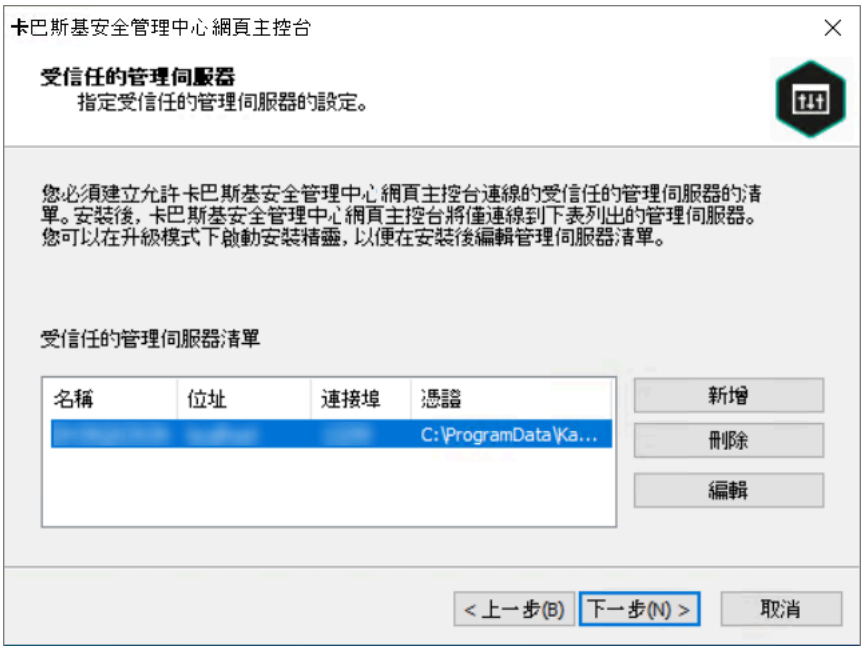
3. 在具有管理員權限的帳戶下執行 ksc-web-console-<版本號>.<組建編號>.exe 安裝檔案。

   這會啟動安裝精靈。

4. 在第一個精靈頁面上，選擇**升級**選項。

   遵照精靈的說明。

5. 在精靈的**受信任的管理伺服器**頁面，選擇所需管理伺服器並點擊**編輯**按鈕。



指定受信任管理伺服器

6. 在開啟的**編輯管理伺服器**視窗中，點擊"**瀏覽**按鈕，指定新憑證檔案的路徑，然後點擊**更新**按鈕套用變更。

7. 在精靈的**卡巴斯基安全管理中心網頁主控台修改已就緒**頁面，點擊**升級**按鈕開始升級。

8. 在應用程式重新設定成功完成後，按一下**完成**按鈕。

9. 登入到卡巴斯基安全管理中心網頁主控台。

卡巴斯基安全管理中心網頁主控台使用指定的憑證工作。

將 PFX 憑證轉換為 PEM 格式

要在卡巴斯基安全管理中心網頁主控台中使用 PFX 憑證，您必須先使用任何方便使用的 OpenSSL 跨平台公用程式將其轉換為 PEM 格式。

在 Windows 作業系統中將 PFX 憑證轉換為 PEM 格式：

1. 在 OpenSSL 跨平台公用程式中，執行以下命令：

   ```
   openssl pkcs12 -in <檔案名稱.pfx> -clcerts -nokeys -out server.crt
   openssl pkcs12 -in <檔案名稱.pfx> -nocerts -nodes -out key.pem
   ```

   結果，您將獲得一個 .crt 檔案形式的公鑰和一個受密碼防護的 .pem 檔案形式的私鑰。

2. 確保 .crt 和 .pem 檔案會在儲存 .pfx 檔案的同一資料夾中產生。

3. 如果 .crt 和 .pem 檔案包含「封包屬性」，請使用任何方便使用的文字編輯器刪除這些屬性，然後儲存檔案。

4. 重新啟動 Windows 服務。

5. 卡巴斯基安全管理中心網頁主控台不支援受密碼防護的憑證。因此，在基於 OpenSSL 的跨平台公用程式中執行以下命令以從 .pem 檔案中刪除複雜密碼：

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > 不要對輸入和輸出 .pem 檔案使用相同的名稱。

   結果，新的 .pem 檔案未加密。您無需輸入複雜密碼即可使用它。

格式為 .crt 和 .pem 的檔案已準備就緒，您可以在卡巴斯基安全管理中心網頁主控台安裝程式中指定它們。

要在 Linux 作業系統中將 PFX 憑證轉換為 PEM 格式：

1. 在 OpenSSL 跨平台公用程式中，執行以下命令：

   ```
   openssl pkcs12 -in <檔案名稱.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <檔案名稱.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. 確保在儲存 .pfx 檔案的目錄中產生憑證檔案和私密金鑰。

3. 卡巴斯基安全管理中心網頁主控台不支援受密碼防護的憑證。因此，在基於 OpenSSL 的跨平台公用程式中執行以下命令以從 .pem 檔案中刪除複雜密碼：

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > 不要對輸入和輸出 .pem 檔案使用相同的名稱。

   結果，新的 .pem 檔案未加密。您無需輸入複雜密碼即可使用它。

格式為 .crt 和 .pem 的檔案已準備就緒，您可以在卡巴斯基安全管理中心網頁主控台安裝程式中指定它們。

從 Kaspersky Security Center Windows 進行移轉

本節說明如何將受管理裝置和相關物件（政策、工作、群組、標記和其他物件）從 Kaspersky Security Center Windows 移轉到：

- 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 Linux
- Kaspersky Next XDR Expert

移轉至卡巴斯基安全管理中心雲端主控台

您可以執行從卡巴斯基安全管理中心網頁主控台轉移到卡巴斯基安全管理中心雲端主控台。之後，您可以存取託管在卡巴斯基基礎結構中的管理伺服器和資料庫管理系統 (DBMS)。您不需要實體伺服器或 DBMS — 兩者都由卡巴斯基專家為您維護。

您可以轉移在卡巴斯基安全管理中心雲端主控台控制下執行 Windows、Linux 或 macOS 作業系統的受管理裝置。如果您的網路包含管理伺服器的階層，您可以將其儲存在卡巴斯基安全管理中心雲端主控台中。此外，您可以傳輸：

- 受管理應用程式的工作和政策
- 全域工作
- 自訂裝置分類
- 管理群組結構和包含的裝置
- 指派給轉移裝置的頁簽

完成轉移後，您可以使用卡巴斯基安全管理中心雲端主控台來管理裝置。同時，傳輸的物件被保留，網路代理會重新安裝在所有受管理裝置上。

有關如何執行轉移的資訊和先決條件清單，請參閱*卡巴斯基安全管理中心雲端主控台說明*。

遷移到 Kaspersky Next XDR Expert

依照此情境執行，您可以將管理群組結構、所包含的受管理裝置和其他群組物件（政策、工作、全域工作、標記和裝置分類）從 Kaspersky Security Center Windows 轉移到 Kaspersky Next XDR Expert 的管理之下。

限制：

- 您只能從 Kaspersky Security Center 14.2 Windows 移轉到 Kaspersky Next XDR Expert（自版本 1.0 起）。
- 您只能使用 Kaspersky Security Center Web 控制台來執行此情境。

階段

移轉情境分階段進行：

1. **選擇移轉方法**

   您是透過移轉精靈移轉到 Kaspersky Next XDR Expert。移轉精靈步驟取決於 Kaspersky Security Center Windows 與 Kaspersky Next XDR Expert 的管理伺服器是否已按階層排列：

   - 使用管理伺服器階層移轉

     如果 Kaspersky Security Center Windows 的管理伺服器是 Kaspersky Next XDR Expert 管理伺服器的從屬伺服器，請選擇此選項。您是在 OSMP 主控台內管理移轉程序以及伺服器之間的切換。如果您更喜歡此選項，可以將管理伺服器排列成階層以簡化遷移過程。為此，請在開始遷移之前建立層次結構。

- 使用匯出檔案（ZIP 存檔）進行移轉

  如果 Kaspersky Security Center Windows 與 Kaspersky Next XDR Expert 的管理伺服器未按階層排列，請選擇此選項。您是使用兩個主控台來管理移轉程序：一個是 Kaspersky Security Center Windows 適用的執行個體，另一個是 OSMP 主控台。在這個案例中，您將使用在從 Kaspersky Security Center Windows 匯出期間建立和下載的匯出檔案，將此檔案匯入到 Kaspersky Next XDR Expert。

2. **從卡巴斯基安全管理中心 Windows 匯出資料**

   開啟卡巴斯基安全管理中心 Windows，然後執行移轉精靈。

3. **將資料匯入到 Kaspersky Next XDR Expert**

   繼續執行移轉精靈將匯出的資料匯入到 Kaspersky Next XDR Expert。

   如果伺服器按階層排列，則在相同精靈中成功匯出後，匯入會自動開始。如果伺服器未按階層排列，您會在切換到 Kaspersky Next XDR Expert 後繼續執行移轉精靈。

4. **執行額外操作以手動將物件和設定從 Kaspersky Security Center Windows 傳輸到 Kaspersky Next XDR Expert（可選步驟）**

   您可能還想傳輸無法透過移轉精靈進行傳輸的物件和設定。例如，您也可以執行下列操作：

   - 設定管理伺服器的全域工作
   - 設定網路代理政策設定
   - 建立應用程式安裝套件
   - 建立虛擬伺服器
   - 分配和配置發佈點
   - 設定裝置移動規則
   - 設定自動標記裝置規則
   - 建立應用程式類別

5. **將匯入的受管理裝置移到 Kaspersky Next XDR Expert 的管理之下**

   若要完成移轉，請將匯入的受管理裝置移到 Kaspersky Next XDR Expert 的管理之下。這可以透過下列其中一種方法進行：

   - 透過 Kaspersky Security Center 群組工作進行

     利用變更管理伺服器工作，將特定用戶端裝置的管理伺服器變更為另一台管理伺服器。

   - 透過 klmover 公用程式

     使用 klmover 公用程式並指定新管理伺服器的連線設定。

   - 透過在受管理裝置上安裝或重新安裝網路代理

     建立新的網路代理安裝套件，在安裝套件內容中指定新管理伺服器的連線設定。使用安裝套件透過遠端安裝工作在匯入的受管理裝置上安裝網路代理。

     您也可以建立並使用獨立安裝套件在本機安裝網路代理。

6. **將網路代理更新到最新版本**

   建議您將網路代理升級到與 Kaspersky OSMP 主控台相同的版本。

7. **確保受管理裝置在新管理伺服器上可見**

   在 Kaspersky Next XDR Expert 管理伺服器上，開啟受管理裝置清單（**裝置 → 受管理裝置**），然後檢查**可見**、**網路代理已安裝**與**上一次連線到管理伺服器**欄位中的值。

其他資料移轉方法

除了移轉精靈之外，您還可以傳輸特定工作和政策：

- 從 Kaspersky Security Center Windows 匯出工作，然後將這些工作匯入到 Kaspersky Next XDR Expert。
- 從 Kaspersky Security Center Windows 匯出政策，然後將這些政策匯入到 Kaspersky Next XDR Expert。相關政策設定檔被與所選政策一起匯出和匯入。

移轉到卡巴斯基安全管理中心 Linux

透過使用管理伺服器資料備份（使用klbackup 實用程式）和移轉精靈，可以從卡巴斯基安全管理中心 Windows 遷移到卡巴斯基安全管理中心 Linux。

下表可讓您比較使用管理伺服器資料備份和移轉精靈進行遷移的主要功能和限制，以決定哪種方法更適合您的組織。

遷移方法比較

參數	管理伺服器資料備份	移轉精靈
遷移過程	建立卡巴斯基安全管理中心 Windows 管理伺服器資料的完整備份並將其還原到卡巴斯基安全管理中心 Linux 管理伺服器上	選擇並匯出管理伺服器資料進行遷移，將這些資料匯入卡巴斯基安全管理中心 Linux 管理伺服器，並將受管理裝置切換至卡巴斯基安全管理中心 Linux 的管理之下
遷移方法的特點	• 遷移所有管理伺服器資料 • 遷移任意數量的受管理裝置 • 用於取得卡巴斯基安全管理中心 Windows 管理伺服器資料的完整副本並將其傳輸到卡巴斯基安全管理中心 Linux 管理伺服器	• 部分遷移管理伺服器資料 • 可以選擇要遷移的物件 • 要移轉的管理群組或子群組最多可包含 10,000 個裝置 • 用於部分傳輸管理伺服器資料，僅包括遷移範圍內的群組物件；遷移範圍之外的群組物件必須手動還原
遷移範圍	管理伺服器資料的完整傳輸，受管理裝置數量不受限制	• 管理群組結構 • 管理群組中包含的受管理裝置（**不超過 10,000 台裝置**） • 分配給遷移裝置的標籤 • 網路代理和應用程式管理的全域工作（不適用於管理伺服器） • 網路代理和應用程式管理的群組工作 • 受管理應用程式的政策 • 報告範本 • 使用者角色 • 內部使用者和安全群組 • 含有手動新增內容的自訂應用程式類別 • 自訂裝置分類

未遷移範圍	—	• 管理伺服器的全域工作 • 儲存在管理伺服器上的事件 • 用於遠端安裝的應用程式分發套件的儲存 • 管理伺服器憑證 • 管理伺服器和受管理應用程式使用的產品授權金鑰 • 虛擬管理伺服器 • 網路代理政策設定 • 裝置移動規則 • 裝置自動標記規則 • 發佈點 • 管理伺服器上保存的卡巴斯基應用程式設定
支援遷移的卡巴斯基安全管理中心版本	• 任何受支援的卡巴斯基安全管理中心 Windows 版本 • 安裝卡巴斯基安全管理中心 Linux 版本 15.2 或更高版本	• 安裝卡巴斯基安全管理中心 Windows 版本 14.2 或更高版本 • 安裝卡巴斯基安全管理中心 Linux 版本 15 或更高版本
可以在之間進行遷移的 DBMS	• Microsoft SQL Server → MySQL、MariaDB • Microsoft SQL Server → PostgreSQL、Postgres Pro（僅適用於從已安裝修補程式的卡巴斯基安全管理中心 Windows 版本 14.2 或更高版本遷移至卡巴斯基安全管理中心 Linux 版本 15.3 或更高版本） • MySQL → MySQL、MariaDB • MariaDB → MySQL、MariaDB	在受支援的 DBMS之間無限制遷移

透過使用移轉精靈移轉到卡巴斯基安全管理中心 Linux

通過使用此方案，您可以將管理群組結構、所包含的受管理裝置和其他群組物件（政策、工作、全局工作、標籤和裝置分類）從卡巴斯基安全管理中心 Windows 轉移到卡巴斯基安全管理中心 Linux 的管理下。在遷移之前，請確保卡巴斯基安全管理中心 Linux 中支援卡巴斯基安全管理中心 Windows 的必要功能。

限制：

- 只能從卡巴斯基安全管理中心 Windows 14.2 或更高版本遷移到卡巴斯基安全管理中心 Linux 版本 15 或更高版本。
- 您只能使用 Kaspersky Security Center Web 控制台來執行此情境。

階段

移轉情境分階段進行：

1 選擇移轉方法

您可以透過移轉精靈移轉到卡巴斯基安全管理中心 Linux。移轉精靈步驟取決於卡巴斯基安全管理中心 Windows 和卡巴斯基安全管理中心 Linux 的管理伺服器是否排列為階層：

- 使用管理伺服器階層移轉

  如果卡巴斯基安全管理中心 Windows 管理伺服器充當卡巴斯基安全管理中心 Linux 管理伺服器的從屬伺服器，請選擇此選項。您可以在卡巴斯基安全管理中心網頁主控台的單個實例中管理遷移流程並在伺服器之間切換。如果您更喜歡此選項，可以將管理伺服器排列成階層以簡化遷移過程。為此，請在開始遷移之前建立層次結構。

- 使用匯出檔案（ZIP 存檔）進行移轉

  如果卡巴斯基安全管理中心 Windows 和卡巴斯基安全管理中心 Linux 的管理伺服器未按階層排列，請選擇此選項。您使用卡巴斯基安全管理中心網頁主控台的兩個實例管理遷移流程 — 一個實例用於卡巴斯基安全管理中心 Windows，另一個實例用於卡巴斯基安全管理中心 Linux。在這種情況下，您將使用在從卡巴斯基安全管理中心 Windows 匯出期間建立和下載的匯出檔案並將此檔案匯入到卡巴斯基安全管理中心 Linux。

2. **備份卡巴斯基安全管理中心 Windows 管理伺服器的憑證和私鑰（可選步驟）**

   您可能希望透過從備份副本還原管理伺服器的憑證和私鑰，將受管理裝置置於卡巴斯基安全管理中心 Linux 管理伺服器的管理之下。在此情況下，備份卡巴斯基安全管理中心 Windows 管理伺服器的憑證和私鑰。然後在第 6 階段，還原憑證和私鑰。

3. **從卡巴斯基安全管理中心 Windows 匯出資料**

   開啟卡巴斯基安全管理中心 Windows，然後執行移轉精靈。

4. **將資料匯入卡巴斯基安全管理中心 Linux**

   繼續執行移轉精靈將匯出的資料匯入到卡巴斯基安全管理中心 Linux。如果伺服器按階層排列，則在相同精靈中成功匯出後，匯入會自動開始。如果伺服器未按階層排列，您可以在切換到卡巴斯基安全管理中心 Linux 後繼續執行移轉精靈。

5. **執行其他操作以手動將物件和設定從卡巴斯基安全管理中心 Windows 傳輸到卡巴斯基安全管理中心 Linux（可選步驟）**

   您可能還想傳輸無法透過移轉精靈進行傳輸的物件和設定。例如，您也可以執行下列操作：

   - 傳輸管理伺服器和受管理應用程式使用的產品授權金鑰
   - 設定管理伺服器的全域工作
   - 設定網路代理政策設定
   - 建立應用程式安裝套件
   - 建立虛擬伺服器
   - 分配和配置發佈點
   - 設定裝置移動規則
   - 設定自動標記裝置規則
   - 建立應用程式類別

6. **移動在卡巴斯基安全管理中心 Linux 管理下的匯入受管理裝置**

   若要完成移轉，請將匯入的受管理裝置移至卡巴斯基安全管理中心 Linux 的管理下。這可以透過下列其中一種方法進行：

   - 透過 klmover 公用程式

     使用 klmover 公用程式並指定新管理伺服器的連線設定。

   - 透過*變更管理伺服器*工作

     建立*變更管理伺服器*工作，指定匯入的受管理裝置、新管理伺服器和其他工作設定。然後執行工作將受管理裝置置於卡巴斯基安全管理中心 Linux 管理伺服器的管理之下。

   - 透過在受管理裝置上刪除（如果已安裝）並進一步安裝網路代理

建立新的網路代理安裝套件，在安裝套件內容中指定新管理伺服器的連線設定。刪除匯入的受管理裝置上的網路代理，然後使用安裝套件透過遠端安裝工作在匯入的受管理裝置上安裝網路代理。您也可以建立並使用獨立安裝套件在本機安裝網路代理。有關更多資訊，請參閱切換卡巴斯基安全管理中心 Linux 管理的受管理裝置。

- 透過從備份副本還原管理伺服器的憑證和私鑰（僅適用於遷移到卡巴斯基安全管理中心 Linux 15.1 或更高版本）

  對安裝有卡巴斯基安全管理中心 Linux 的管理伺服器指派與卡巴斯基安全管理中心 Windows 的管理伺服器上相同的網路位址。執行帶有 `-cert_only` 參數的klbackup 公用程式，從您在第 2 階段保存的備份副本中還原管理伺服器憑證和私鑰。在命令列中，執行以下命令：`/opt/kaspersky/ksc64/sbin/klbackup -path <管理伺服器憑證備份副本的路徑> -restore -cert_only`。有關詳細資訊，請參閱使用 klbackup 公用程式切換在另一個管理伺服器的管理下的受管理裝置。

7. **將網路代理更新到最新版本**

   我們建議您將 Linux 網路代理升級到與卡巴斯基安全管理中心相同的版本。

8. **確保受管理裝置在新管理伺服器上可見**

   在卡巴斯基安全管理中心 Linux 管理伺服器上，開啟受管理裝置清單（**裝置→受管理裝置**），然後檢查**可見**、**網路代理已安裝**和**上一次連線到管理伺服器**列中的值。

其他資料移轉方法

除了移轉精靈之外，您還可以傳輸特定工作和政策：

- 從 Kaspersky Security Center Windows 匯出工作，然後匯入工作到 卡巴斯基安全管理中心 Linux。
- 從卡巴斯基安全管理中心 Windows 匯出特定政策，然後匯入工作到卡巴斯基安全管理中心 Linux。相關政策設定檔被與所選政策一起匯出和匯入。

從卡巴斯基安全管理中心 Windows 匯出群組物件

從卡巴斯基安全管理中心 Windows 到卡巴斯基安全管理中心 Linux 的遷移管理群組結構、包含的受管理裝置和其他群組物件需要您首先選擇要匯出的資料並建立匯出檔案。匯出檔案包含有關要遷移的所有群組物件的資訊。匯出檔案將會用來後續匯入卡巴斯基安全管理中心 Linux。

您可以匯出以下物件：

- 受管理應用程式的工作和政策
- 全域工作
- 自訂裝置分類
- 管理群組結構和包含的裝置
- 指派給轉移裝置的頁簽

開始匯出前，請閱讀有關遷移到 卡巴斯基安全管理中心 Linux 的一般資訊。選擇遷移方法 — 透過使用或不使用卡巴斯基安全管理中心 Windows 和卡巴斯基安全管理中心 Linux 管理伺服器的階層。

透過遷移精靈匯出受管理裝置和相關群組物件：

1. 根據卡巴斯基安全管理中心 Windows 和卡巴斯基安全管理中心 Linux 的管理伺服器是否排列成階層，執行以下操作之一：

   - 如果伺服器排列成階層，開啟卡巴斯基安全管理中心網頁主控台，然後切換到卡巴斯基安全管理中心 Windows 的伺服器。

   - 如果伺服器未排列成階層，開啟連線到卡巴斯基安全管理中心 Windows 伺服器的卡巴斯基安全管理中心網頁主控台。

2. 在主功能表中，轉至**操作 → 移轉**。

3. 若要啟動精靈並依照其步驟操作，請選取要將資料和設定傳輸到的位置。

   - 如果要將資料和設定傳輸到 卡巴斯基安全管理中心雲端主控台，請選取**移轉至 Kaspersky Security Center Cloud Console**。

   - 如果要將資料和設定傳輸到 卡巴斯基安全管理中心 Linux 或 Kaspersky Next XDR Expert，請選取**遷移到 Kaspersky Security Center Linux**。

4. 選取您要匯出的管理群組或子群組。請注意，所選的管理群組或子群組包含不超過 10,000 台裝置。

5. 選取您希望匯出其工作和政策的受管理應用程式。僅選取卡巴斯基安全管理中心 Linux 支援的應用程式。不受支援的應用程式的物件仍將被匯出，但它們將無法使用。

6. 使用左側的連結選取全域工作、裝置分類和要匯出的報告。**群組物件**連結允許您從匯出中排除自訂角色、內部使用者和安全群組以及自訂應用程式類別。

匯出檔案（ZIP 封存）已建立。根據您是否使用管理伺服器層次結構支援執行遷移，匯出檔案會被儲存如下：

- 如果伺服器排列成層次結構，匯出檔案將儲存到卡巴斯基安全管理中心網頁主控台伺服器上的臨時資料夾中。

- 如果伺服器未排列成層次結構，則匯出檔案將被下載到您的裝置。

對於具有管理伺服器層次結構支援的遷移，匯入會在成功匯出後自動開始。對於沒有管理伺服器層次結構支援的遷移，您可以手動將儲存的匯出檔案匯入到卡巴斯基安全管理中心 Linux。

將匯出的檔案匯入到卡巴斯基安全管理中心 Linux

若要傳輸您從卡巴斯基安全管理中心 Windows 匯出之受管理裝置、物件與其設定的相關資訊，您必須將其匯入卡巴斯基安全管理中心 Linux 或 Kaspersky Next XDR Expert。

透過遷移精靈匯入受管理裝置和相關群組物件：

1. 根據卡巴斯基安全管理中心 Windows 和卡巴斯基安全管理中心 Linux 的管理伺服器是否排列成階層，執行以下操作之一：

   - 如果伺服器排列成階層，則在匯出完成後繼續執行移轉精靈的下一步。在此精靈中成功匯出後，匯入會自動開始（請參閱本說明的步驟 2）。

   - 如果伺服器未排列成階層：

     a. 開啟連線到卡巴斯基安全管理中心 Linux 或 Kaspersky Next XDR Expert 的卡巴斯基安全管理中心 網頁主控台。

     b. 在主功能表中，轉至**操作 → 移轉**。

     c. 選擇您在從卡巴斯基安全管理中心 Windows 匯出過程中建立並下載的匯出檔案（ZIP 存檔）。開始上傳匯出檔案。

2. 匯出檔案上傳成功後，即可繼續匯入。如果要指定其他匯出檔案，請點擊**變更**連接，然後選擇所需的檔案。

3. 卡巴斯基安全管理中心 Linux 管理群組的整個階層將得以顯示。

   選中目標管理群組旁邊的核取方塊，匯出的管理群組的物件（受管理裝置、政策、工作和其他群組物件）必須還原到該目標管理群組。

4. 開始匯入群組物件。您無法最小化移轉精靈並在匯入期間執行任何並行作業。請等待片刻，直到物件清單中所有物件旁的重新整理圖示 (🔄) 更換為綠色勾號標記 (✓)，匯入隨即完成。

5. 完成匯入時，管理群組的匯出結構，包含裝置的詳細資料，會顯示在所選目標管理群組下。若您還原的物件名稱與現有物件名稱相同，前者會使用增量尾碼新增。

> 如果在遷移的工作中指定了執行該工作的帳戶的詳細資訊，則匯入完成後您必須開啟該工作並再次輸入密碼。

如果匯入已完成但出現錯誤，您可以執行以下操作之一：

- 對於具有管理伺服器層次結構支援的遷移，您可以再次開始匯入匯出檔案。
- 對於沒有管理伺服器層次結構支援的遷移，您可以啟動移轉精靈選擇另一個匯出檔案，然後再次匯入。

您可以檢查匯出範圍中包含的群組物件是否已成功匯入到卡巴斯基安全管理中心 Linux。為此，請轉到**裝置**部分並確保匯入的物件出現在相應的子部分中。

請注意，匯入的受管理裝置顯示在**受管理裝置**子部分中，但它們在網路中不可見，並且網路代理未安裝並在其上執行（**"可見"**、 **網路代理已安裝"**和**網路代理正在執行"**列中的*否*值）。

要完成遷移，您需要將受管理裝置切換到卡巴斯基安全管理中心 Linux 的管理之下。

將受管理裝置切換到 卡巴斯基安全管理中心 Linux 的管理之下

將受管理裝置、物件及其設定的資訊成功匯入卡巴斯基安全管理中心 Linux 後，您需要將受管理裝置切換到卡巴斯基安全管理中心 Linux 的管理下才能完成遷移。

您可以透過以下方法之一將受管理裝置移至卡巴斯基安全管理中心 Linux 下：

- 使用 klmover 公用程式。
- 使用*變更管理伺服器*工作。
- 透過遠端安裝工作在受管理裝置上安裝網路代理。

要通過安裝網路代理將受管理裝置切換為由卡巴斯基安全管理中心 Linux 管理：

1. 刪除將在卡巴斯基安全管理中心 Linux 管理下切換的匯入受管理裝置上的網路代理程式。
2. 轉到卡巴斯基安全管理中心 Windows 的管理伺服器。
3. 進入**發現和佈署→佈署和分配→安裝套件**，然後開啟網路代理現有安裝套件的屬性。
   如果套件清單中沒有網路代理安裝套件，請下載新的安裝套件。
   您也可以建立並使用獨立安裝套件在本機安裝網路代理。
4. 在**設定**頁簽上， 選擇**連線**部分。指定卡巴斯基安全管理中心 Linux 管理伺服器的連線設定。
5. 為匯入的受管理裝置建立遠端安裝工作，然後指定重新配置的網路代理安裝套件。
   您可以透過卡巴斯基安全管理中心 Windows 的管理伺服器或透過充當發佈點的 Windows 裝置安裝網路代理。如果您使用管理伺服器，請啟用**透過管理伺服器使用作業系統資源**選項。如果您使用發佈點，請啟用**透過發佈點使用作業系統資源**選項。
6. 執行遠端安裝工作。

遠端安裝工作成功完成後，轉至卡巴斯基安全管理中心 Linux 的管理伺服器並確保受管理裝置在網路中可見，並且網路代理已安裝並在其上執行（**可見**、**網路代理已安裝**和**網路代理正在執行**列中的*是*值）。

使用管理伺服器資料備份遷移到卡巴斯基安全管理中心 Linux

您可以使用資料備份將卡巴斯基安全管理中心 Windows 管理伺服器資料移至卡巴斯基安全管理中心 Linux。在遷移之前，請確保卡巴斯基安全管理中心 Linux 中支援卡巴斯基安全管理中心 Windows 的必要功能。

限制：

- 遷移可以在下列 DBMS 之間執行：
  - Microsoft SQL Server → MySQL、MariaDB
  - Microsoft SQL Server → PostgreSQL、Postgres Pro
  - MySQL → MySQL、MariaDB
  - MariaDB → MySQL、MariaDB
- 支援將儲存在 Microsoft SQL Server、MySQL 或 MariaDB 資料庫中的管理伺服器資料從任何支援的卡巴斯基安全管理中心 Windows 版本移轉到 MySQL 或 MariaDB 至卡巴斯基安全管理中心 Linux 版本 15.2 或更高版本。

- 支援將儲存在 Microsoft SQL Server 資料庫中的管理伺服器資料遷移到 PostgreSQL 或 Postgres Pro，以便從卡巴斯基安全管理中心 Windows 版本 14.2 或更高版本遷移到卡巴斯基安全管理中心 Linux 版本 15.3 或更高版本。

  為了支援遷移到 PostgreSQL 或 Postgres Pro，您必須安裝卡巴斯基安全管理中心 Windows 管理伺服器的修補程式。使用以下一個修補程式：

  - 對於基於卡巴斯基安全管理中心 Windows 14.2 的 Kaspersky Secure Mobility Management：14.2.0.48079-pf5
  - 對於卡巴斯基安全管理中心 Windows 14.2：14.2.0.26967-pf5

  聯絡卡巴斯基技術支援以取得所需的修補程式。

- 如果您使用 MySQL 或 MariaDB 作為卡巴斯基安全管理中心 Windows 和卡巴斯基安全管理中心 Linux 的 DBMS，則目前 DBMS 和新 DBMS 的`lower_case_table_names`參數必須相符。

  在建立資料備份之前，請檢查`lower_case_table_names`參數。然後，在為卡巴斯基安全管理中心 Linux 安裝 MySQL 或 MariaDB 時，必須將此參數設定為與為 Windows 指定的此參數相同的值。

階段

使用管理伺服器資料備份進行遷移分階段進行：

1. **檢查您是否擁有管理員的內部使用者帳戶，以便您可以登入管理伺服器**

   管理員帳戶將用於登入卡巴斯基安全管理中心 Linux 管理伺服器。如果您沒有此帳戶，並且僅在本機 Windows 帳戶或網域帳戶下登入，則還原備份後將無法登入卡巴斯基安全管理中心 Linux 管理伺服器。卡巴斯基安全管理中心 Linux 管理伺服器不支援使用本機 Windows 帳號登入。可以使用網域帳戶登入，但可能需要對管理伺服器進行額外設定。

   如果您沒有管理員帳戶，則必須在使用 kladduser 實用程式還原備份副本後建立此帳戶。

2. **建立卡巴斯基安全管理中心 Windows 管理伺服器資料的最新備份副本**

   根據卡巴斯基安全管理中心 Windows 和卡巴斯基安全管理中心 Linux 使用的 DBMS 類型，執行下列一項操作：

   - 對於將 MySQL 或 MariaDB 遷移到 MySQL 或 MariaDB：在安裝了管理伺服器的裝置上使用klbackup 實用程式或資料備份工作建立備份部分。
   - 對於將 Microsoft SQL Server 移轉到 MySQL 或 MariaDB：使用klbackup 實用程式建立備份副本，啟用**遷移到 MySQL/MariaDB 格式**選項。
   - 對於將 Microsoft SQL Server 移轉到 PostgreSQL 或 Postgres Pro：

     1. 安裝管理伺服器修補程式以支援遷移到 PostgreSQL 和 Postgres Pro。聯絡卡巴斯基技術支援以取得此修補程式。

     1. 使用 klbackup 實用程式建立備份副本。

        如果從命令列執行 klbackup，請使用`-migrate_postgres`旗標。

        如果您使用 klbackup 介面，請啟用**遷移到 Postgres 格式**選項。

   建立備份副本後，中斷卡巴斯基安全管理中心 Windows 管理伺服器與網路的連線。

3. **準備新裝置以安裝卡巴斯基安全管理中心 Linux**

   在方案的此步驟中，進行以下操作：

1. 選擇要在上面安裝管理伺服器的新裝置。該裝置必須滿足硬體和軟體要求。另外，檢查一下管理伺服器上使用的連接埠是否可用。

2. 為新裝置分配相同的位址。

   可以為新管理伺服器指派 NetBIOS 名稱、FQDN 和靜態 IP 位址。這取決於部署網路代理時在網路代理安裝套件中設定的管理伺服器位址。或者，您可以使用確定網路代理連線到管理伺服器的連線位址（您可以使用klnagchk 公用程式在受管理裝置上取得此位址）。

4 安裝和設定 DBMS

在方案的此步驟中，進行以下操作：

1. 選擇可提供最佳效能的 DBMS 類型。考慮連網裝置的數量、網路拓撲和網路上的工作負載。您可以選擇其中一個受支援的 DBMS。

2. 根據建立備份時所選擇的 DBMS 類型安裝DBMS。對於如何安裝所選 DBMS 的資訊，請參考其文件。

   > 新的資料庫版本不得低於目前資料庫版本。

3. 配置 DBMS 以與卡巴斯基安全管理中心 Linux 一起使用。

5 安裝卡巴斯基安全管理中心 Linux

在新裝置上安裝卡巴斯基安全管理中心 Linux。

安裝期間建立的管理員內部使用者帳戶以及從備份還原管理伺服器資料之前建立的其他物件（群組、政策、群組工作、使用者）將在還原後遺失。這些物件將被備份中包含的物件取代。

6 從備份副本還原管理伺服器資料

在方案的此步驟中，進行以下操作：

1. 使用klbackup 實用程式在新裝置上還原管理伺服器資料。

2. 如果您沒有用於登入卡巴斯基安全管理中心 Windows 管理伺服器的管理員內部使用者帳戶，並且使用了本機 Windows 帳戶或網域帳戶，請使用 kladduser 實用程式建立管理員帳戶，如下所示：

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <password>
   ```

   其中 `<password>` 參數符合以下要求：

   - 使用者密碼不能少於 8 個或多於 256 個字元。
   - 密碼必須包含以下組中三組的字元：
     - 大寫字母 (A-Z)
     - 小寫字母 (a-z)
     - 數字 (0-9)
     - 特殊字元 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

7 安裝卡巴斯基安全管理中心網頁主控台和配置管理伺服器

在方案的此步驟中，進行以下操作：

1. 安裝卡巴斯基安全管理中心網頁主控台。

如果卡巴斯基安全管理中心網頁主控台先前已安裝，請使用相同的回應檔案重新安裝。

使用管理員的內部使用者帳戶登入卡巴斯基安全管理中心網頁主控台。

還原管理伺服器資料後，資料初始化過程通常需要最多 15 分鐘，但該時間取決於硬體效能和管理伺服器資料的大小。在此期間，卡巴斯基安全管理中心網頁主控台可能無法連線並顯示錯誤。

2. 資料庫中的資料初始化完成後，檢查主要管理伺服器功能的功能。驗證管理伺服器是否與受管設備同步且管理伺服器資料已還原。

3. 輪詢網域控制器可還原關於網域結構、使用者帳戶、安全群組以及網域所含裝置的 DNS 名稱的資訊。

4. 如有必要，從之前的裝置中解除安裝管理伺服器和資料庫伺服器。

   同一網路上不得有多個具有相同連線位址和管理伺服器憑證的管理伺服器。

考慮到卡巴斯基安全管理中心 Linux 中支援的功能，管理員有權存取在卡巴斯基安全管理中心 Windows 中的管理伺服器資料和受管理裝置。

登入到卡巴斯基安全管理中心網頁主控台並登出

您可以在安裝管理伺服器和網頁主控台伺服器後登入到卡巴斯基安全管理中心網頁主控台。您必須知道安裝過程中指定的管理伺服器的 Web 位址和埠號（預設下，埠號是 8080）。在您的瀏覽器中，JavaScript 必須被啟用。

您可以使用以下方法登入卡巴斯基安全管理中心網頁主控台：

- 透過使用網域身分驗證

  如果選擇此方法，請確保 Active Directory 輪詢已啟動並且網域使用者已新增到管理伺服器。

- 透過指定管理員的使用者名稱和密碼

透過使用網域身分驗證登入

要透過使用網域身分驗證登入卡巴斯基安全管理中心網頁主控台，請執行以下操作：

1. 在瀏覽器中，前往 https://<卡巴斯基安全管理中心網頁主控台位址>:<連接埠號>
   登入頁面顯示。
2. 如果您新增若干個受信任的伺服器，在管理伺服器清單選取您要連線的管理伺服器。
   如果您只新增了一台管理伺服器，則管理伺服器清單被鎖定。
3. 執行以下操作之一：
   - 點擊**網域驗證**按鈕。
   - 如果在伺服器上建立了一個或多個虛擬管理伺服器，並且您希望使用網域驗證登入到虛擬伺服器：
     a. 點擊**進階設定**。
     b. 建立虛擬伺服器時輸入您指定的虛擬管理伺服器名稱。
     c. 點擊**網域驗證**按鈕。

登入後，儀表板使用您最後使用的語言和主題顯示。您可以透過卡巴斯基安全管理中心 網頁主控台導航並使用其操作卡巴斯基安全管理中心。

透過指定管理員的使用者名稱和密碼登入

要透過指定管理員的使用者名稱和密碼登入卡巴斯基安全管理中心網頁主控台，請執行以下操作：

1. 在瀏覽器中，前往 https://<卡巴斯基安全管理中心網頁主控台位址>:<連接埠號>
   登入頁面顯示。
2. 如果您新增若干個受信任的伺服器，在管理伺服器清單選取您要連線的管理伺服器。
   如果您只新增了一台管理伺服器，則管理伺服器清單被鎖定。
3. 執行以下操作之一：
   - 若要登入管理伺服器：
     a. 輸入本機管理員的使用者名稱和密碼。
     b. 點擊**登入**按鈕。
   - 如果在伺服器上建立了一個或多個虛擬管理伺服器，並且您希望登入到虛擬伺服器：
     a. 點擊**進階設定**。
     b. 建立虛擬伺服器時輸入您指定的虛擬管理伺服器名稱。
     c. 輸入對虛擬管理伺服器具有權限的管理員的使用者名稱和密碼。
     d. 點擊**登入**按鈕。

登入後，儀表板使用您最後使用的語言和主題顯示。您可以透過卡巴斯基安全管理中心 網頁主控台導航並使用其操作卡巴斯基安全管理中心。

登出

要登出卡巴斯基安全管理中心網頁主控台，

在主功能表中，轉到您的帳戶設定，然後選擇**登出**。

卡巴斯基安全管理中心 網頁主控台被關閉，且登入頁面被顯示。

在卡巴斯基安全管理中心網頁主控台中的身分和存取管理器

本節提供有關身分和存取管理器（也稱為 IAM）的資訊。

關於身分和存取管理器

身分和存取管理器（也稱為 IAM）是一個卡巴斯基安全管理中心 網頁主控台元件，使您能夠在卡巴斯基安全管理中心 網頁主控台和 Kaspersky Industrial CyberSecurity for Networks Web 介面之間使用單一登入 (SSO)。IAM 使用 OAuth 2.0 通訊協定來確保在卡巴斯基安全管理中心 網頁主控台中的 Kaspersky Industrial CyberSecurity for Networks 的授權。

在這種情況下，您可以透過卡巴斯基安全管理中心 網頁主控台存取的 Kaspersky Industrial CyberSecurity for Networks 被稱為*資源伺服器*，卡巴斯基安全管理中心 網頁主控台和 Kaspersky Industrial CyberSecurity for Networks Web 介面被稱為 *OAuth 2.0 用戶端*。資源伺服器是一個與多個使用者一起工作並需要授權的程式。用戶端使用*權杖*進行資源伺服器上的授權。權杖是一個唯一的位元組序列。當權杖過期時，它會自動重新發行。IAM 為多個 OAuth 2.0 用戶端充當單一授權伺服器。

您可以在安裝卡巴斯基安全管理中心 網頁主控台時安裝 IAM。您可以稍後在卡巴斯基安全管理中心 網頁主控台設定中隨時啟用它。如果一台 Kaspersky Industrial CyberSecurity 伺服器或者一台 Kaspersky Industrial CyberSecurity Web 介面安裝在同一台管理伺服器管理的裝置上，IAM 將檢測到該程式，卡巴斯基安全管理中心 網頁主控台中會顯示一條通知，告知您有關情況。您可以註冊 Kaspersky Industrial CyberSecurity for Networks，然後將 SSO 用於卡巴斯基安全管理中心 網頁主控台和 Kaspersky Industrial CyberSecurity for Networks Web 介面。

如果您登出卡巴斯基安全管理中心 網頁主控台，您在 Kaspersky Industrial CyberSecurity for Networks Web 介面中的工作階段將結束，您必須再次登入到卡巴斯基安全管理中心 網頁主控台。

啟用身分和存取管理器：情境

先決條件

在開始之前，請確保您可以存取 Kaspersky Industrial CyberSecurity for Networks 3.1 或更高版本。

階段

啟用身分和存取管理器（也稱為 IAM）分階段進行：

1. **檢查必要的連接埠**

   確保在已安裝卡巴斯基安全管理中心 網頁主控台伺服器的裝置上開啟了連接埠 3333、4004 和 4444。使用 OAuth 2.0 需要這些連接埠。如果需要，您可以在卡巴斯基安全管理中心 網頁主控台設定視窗中變更預設連接埠號。

   除了連接埠 3333、4004 和 4444，卡巴斯基安全管理中心 網頁主控台還為了各種目的使用連接埠 4445、2444 和 2445。

2. **安裝身分和存取管理器**

   在卡巴斯基安全管理中心 網頁主控台安裝期間，指定您要安裝身分和存取管理器。如果您沒有這樣做，請再次執行卡巴斯基安全管理中心 網頁主控台設定精靈。

3. **配置身分和存取管理器**

   在卡巴斯基安全管理中心網頁主控台設定視窗中，確保**身分識別與存取管理器 (IAM)** 切換按鈕已啟用。此外，指定安裝了卡巴斯基安全管理中心 網頁主控台的裝置的 DNS 名稱：用戶端應用程式將連線到此裝置。

4. **指定權杖設定**

   在卡巴斯基安全管理中心 網頁主控台設定視窗中，指定身分和存取管理器將使用的權杖的存留期和授權逾時。您可以使用預設值，也可以根據需要指定自己的值。

5. **授予憑證**

   如果您更喜歡使用管理伺服器產生的憑證，則在卡巴斯基安全管理中心 網頁主控台中下載 IAM 使用的連接埠的根憑證並將它們發佈到卡巴斯基安全管理中心 網頁主控台使用者的工作站。否則，嘗試連線到卡巴斯基安全管理中心 網頁主控台時，使用者的瀏覽器將顯示錯誤訊息。

6. **註冊 Kaspersky Industrial CyberSecurity for Networks 伺服器 和 Kaspersky Industrial CyberSecurity for Networks Web 介面**

   安裝 IAM 後，卡巴斯基安全管理中心 網頁主控台會顯示一條訊息，指出一個 Industrial CyberSecurity for Networks 伺服器（或多個伺服器）和一個或多個 Kaspersky Industrial CyberSecurity for Networks Web 介面正在等待註冊。點擊此訊息可註冊您的 Kaspersky Industrial CyberSecurity for Networks 伺服器（或多個伺服器）和 Web 介面（或多個 Web 介面）。

結果

完成此情節後，您將能夠將 SSO 和 IAM 用於 Kaspersky Industrial CyberSecurity for Networks 和卡巴斯基安全管理中心網頁主控台。

在卡巴斯基安全管理中心 網頁主控台中配置身分和存取管理器

若要根據您的需要配置身分和存取管理器：

1. 在主功能表中，轉至 **主控台設定 → 整合**。
2. 在**身分識別與存取管理器**區段，確保啟用了身分和存取管理器。
3. 點擊**設定**連接，在 **身分識別與存取管理器裝置的網路名稱** 行中。

4. 指定要在其上安裝身分和存取管理器的裝置的 DNS 名稱。用戶端應用程式將連線到此裝置。

5. 如果您願意，請透過點擊相關設定群組下的 **設定** 連接變更“預設權杖設定”、“憑證設定”和“連接埠號”。

身分和存取管理器已啟用並在根據您的需要工作。

在卡巴斯基安全管理中心網頁主控台中註冊 Kaspersky Industrial CyberSecurity for Networks 應用程式

要開始透過卡巴斯基安全管理中心網頁主控台使用 Kaspersky Industrial CyberSecurity for Networks 應用程式，您必須首先在卡巴斯基安全管理中心網頁主控台中註冊它。

要註冊 Kaspersky Industrial CyberSecurity for Networks 應用程式：

1. 確保完成以下操作：

   - 已下載並安裝 Kaspersky Industrial CyberSecurity for Networks Web 外掛程式。

     不過，您可以稍後在等待 Kaspersky Industrial CyberSecurity for Networks Server 與管理伺服器同步時執行此操作。

   - 您已完成單點登入 (SSO) 技術使用準備情境。

   - Kaspersky Industrial CyberSecurity for Networks Web 介面中的必要設定已在卡巴斯基安全管理中心頁面上指定。詳情請參閱 Kaspersky Industrial CyberSecurity for Networks 線上說明。

   - 您已以管理員帳戶登入卡巴斯基安全管理中心網頁主控台。

   - IAM 已配置。

2. 將安裝 Kaspersky Industrial CyberSecurity for Networks Server 的裝置從未分配裝置群組移動到受管理裝置群組：

   a. 在主功能表中，轉至 **發現和佈署 → 未配置的裝置**。

   b. 選中安裝了 Kaspersky Industrial CyberSecurity for Networks Server 的裝置旁邊的核取方塊。

   c. 點擊**移至群組**按鈕。

   d. 在管理群組層次中，選中受管理裝置群組旁邊的核取方塊。

   e. 點擊**移動**按鈕。

3. 前往安裝了 Kaspersky Industrial CyberSecurity for Networks Server 的裝置的內容。

4. 在裝置內容頁面的**一般**區域，選擇**不要中斷與管理伺服器的連線**選項，然後按一下**儲存**按鈕。

5. 在裝置內容頁面上，選擇**應用程式**區域。

6. 在**應用程式**區域中，選擇卡巴斯基網路代理。

7. 如果應用程式的目前狀態是*已停止*，等到它變為*正在執行*。

   這大約需要 15 分鐘。如果您尚未安裝 Kaspersky Industrial CyberSecurity for Networks Web 外掛程式，可以在等待期間立即安裝。

8. 在主功能表中，轉至 **主控台設定 → 整合**。

   在**註冊請求**欄位中，顯示一個待處理的請求。

9. 按一下**註冊請求**欄位中的**設定**連結。

10. 在開啟的註冊用戶端清單中，選中 Kaspersky Industrial CyberSecurity for Networks Server 名稱旁邊的核取方塊，其狀態為*待處理*，然後按一下**批准**按鈕。

    如果您不想註冊 Kaspersky Industrial CyberSecurity for Networks Server，可以按一下拒絕按鈕，稍後返回此清單。

    按一下**批准**按鈕後，狀態會變為*已批准*，然後變為*就緒*。如果狀態沒有變更，您可以按一下重新整理按鈕。

11. 關閉註冊用戶端清單並確保**已註冊用戶端**欄位的值已增加。

12. 要在儀表板上新增 Kaspersky Industrial CyberSecurity for Networks 小部件：

    a. 在主功能表中，轉至 **監控和報告 → 控制板**。

    b. 在儀表板上，點擊**新增或還原 Web 小部件**按鈕。

    c. 在開啟的小部件功能表中，選取**其它**。

    d. 選擇 Kaspersky Industrial CyberSecurity for Networks 小部件。

    您現在可以使用小部件中的連結前往 Kaspersky Industrial CyberSecurity for Networks Web 介面。

完成註冊程序後，一個新的按鈕，**卡巴斯基安全中心**，出現在 Kaspersky Industrial CyberSecurity for Networks Web 介面的登入頁面上。您可以按一下此按鈕用卡巴斯基安全管理中心憑據登入 Kaspersky Industrial CyberSecurity for Networks Web 介面。

身分和存取管理器的權杖存留期和授權逾時

在配置身分和存取管理器（也稱為 IAM）時，您必須指定權杖存留期和授權逾時的設定。預設設定旨在反映安全標準和伺服器負載。但是，您可以根據組織的政策變更這些設定。

當權杖即將到期時，IAM 會自動重新發行權杖。

下表列出了預設權杖存留期設定。

權杖存留期設定

權杖	預設存留期（以秒為單位）	敘述
身分識別權仗 (id_token)	86400	OAuth 2.0 用戶端（即卡巴斯基安全管理中心 網頁主控台或 Kaspersky Industrial CyberSecurity Console）使用的身分權杖。IAM 向用戶端傳送包含使用者資訊（即使用者設定檔）的 ID 權杖。
存取權仗 (access_token)	86400	OAuth 2.0 用戶端用於代表 IAM 識別的資源所有者存取資源伺服器的存取權杖。
重新整理權仗 (refresh_token)	172800	OAuth 2.0 用戶端使用此權杖重新發放身分權杖和存取權杖。

下表列出了 auth_code 和 login_consent_request 的逾時。

設定	預設逾時（以秒為單位）	敘述
授權碼 (auth_code)	3600	為權杖交換代碼的逾時。OAuth 2.0 用戶端將此代碼發送到資源伺服器並獲取存取權杖作為交換。
登入同意請求逾時 (login_consent_request)	3600	將用戶權限委派給 OAuth 2.0 用戶端的逾時時間。

有關權杖的更多資訊，請參閱 OAuth 網站。

下載和分發 IAM 憑證

預設情況下，身分和存取管理器使用管理伺服器產生的憑證授予瀏覽器存取卡巴斯基安全管理中心 網頁主控台的權限。但是，如果願意，您可以使用自訂憑證。無論您使用什麼憑證，您都必須確保卡巴斯基安全管理中心 網頁主控台使用者從中存取卡巴斯基安全管理中心 網頁主控台的所有工作站都信任此憑證。

若要下載和分發憑證：

1. 在主功能表中，轉至 **主控台設定 → 整合**。
2. 對於每個憑證，點擊相關設定群組下的“**設定**”連接，然後執行以下操作之一：
   - 如果您想使用管理伺服器在安裝卡巴斯基安全管理中心 網頁主控台期間產生的憑證：
     1. 在開啟的憑證內容視窗中選擇“**由管理伺服器產生的憑證** ”。
     2. 按一下“**下載**”按鈕下載憑證。
     3. 將下載的憑證分發到卡巴斯基安全管理中心 網頁主控台使用者從中存取卡巴斯基安全管理中心 網頁主控台的所有工作站。
   - 如果您有想要使用的憑證：
     1. 在開啟的憑證內容視窗中選擇“**自訂 TLS 憑證**”。
     2. 選擇憑證檔案和私鑰。
     3. 點擊**確定**按鈕。
     4. 將憑證分發到使用者從其存取卡巴斯基安全管理中心 網頁主控台或 Kaspersky Industrial CyberSecurity Console 的所有工作站。

這些憑證授予使用者存取卡巴斯基安全管理中心 網頁主控台和 Kaspersky Industrial CyberSecurity Console 的權限。

您必須及時重新發放所有憑證。管理伺服器產生的憑證必須手動重新產生。卡巴斯基安全管理中心 網頁主控台產生的憑證安裝程式必須使用安裝程式重新產生。

停用身分和存取管理器

如果願意，您可以停用身分和存取管理器（也稱為 IAM）。

若要停用 IAM，

在卡巴斯基安全管理中心 網頁主控台設定視窗中，將 IAM 切換按鈕切換為已停用。

您可以稍後隨時啟用 IAM。

如果您透過安裝程式更新卡巴斯基安全管理中心 網頁主控台並指定您不想安裝 IAM，則卡巴斯基安全管理中心 網頁主控台將升級並且不會安裝 IAM。所有關於與 Kaspersky Industrial CyberSecurity for Networks 整合的資訊以及 IAM 設定檔和日誌檔案將從您的電腦中刪除。

使用 NTLM 和 Kerberos 通訊協定設定網域身分驗證

卡巴斯基安全管理中心 14.2 使您可以透過使用 NTLM 和 Kerberos 通訊協定在 OpenAPI 中使用網域身分驗證。使用網域身分驗證，Windows 使用者可以在卡巴斯基安全管理中心 網頁主控台中啟用安全身分驗證，而不必在公司網路上重新輸入密碼（單一登入）。

透過 Kerberos 通訊協定在 OpenAPI 中進行網域身分驗證具有以下限制：

- 必須使用 Kerberos 通訊協定在 Active Directory 中對卡巴斯基安全管理中心 網頁主控台的使用者進行身分驗證。使用者必須具有有效的 Kerberos 票證授予票（也稱為 TGT）。當您對網域進行身分驗證時，將自動簽發 TGT。
- 您必須在瀏覽器中設定 Kerberos 身分驗證。相關詳細資料，請參閱所用瀏覽器的文件。

如果要透過使用 Kerberos 通訊協定使用網域身分驗證，則您的網路必須符合以下條件：

- 管理伺服器必須以網域帳戶名稱執行。
- 卡巴斯基安全管理中心網頁主控台伺服器必須安裝在安裝管理伺服器的同一裝置上。
- 您必須為管理伺服器帳戶指定以下服務主體名稱 (SPN)：
  - "http/<server.fqnd.name>"
  - "http/<server>"

  這裡，<server> 是管理伺服器裝置的網路名稱，並且 <server.fqnd.name> 是管理伺服器裝置的 FQDN 名稱。
- 連線管理主控台或卡巴斯基安全管理中心網頁主控台時，必須將管理伺服器位址指定為與註冊服務主體名稱 (SPN) 的位址完全相同的位址。您可以指定 <server.fqnd.name> 或者 <server>。
- 對於無密碼登入，必須以網域帳戶執行瀏覽器處理程序，在該處理程序中，以瀏覽器的身分開啟卡巴斯基安全管理中心網頁主控台。

僅卡巴斯基安全管理中心 14.2 的 OpenAPI 支援 Kerberos 和 NTLM 通訊協定。卡巴斯基安全管理中心 Linux 版的 OpenAPI 不支援該通訊協定。

設定管理伺服器

此區段說明設定過程與卡巴斯基安全管理中心管理伺服器的內容。

配置卡巴斯基安全管理中心 網頁主控台到管理伺服器的連線

要設定管理伺服器連線連接埠：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。

   管理伺服器內容視窗將開啟。

2. 在**一般**標籤，選取**連線連接埠**區段。

   應用程式顯示所選伺服器的主要連線設定。

卡巴斯基安全管理中心網頁主控台透過 SSL 連接埠 TCP 13291 連線至管理伺服器。klakaut 自動化物件可使用相同的連接埠。

連接埠 TCP 14000 可以用於連線卡巴斯基安全管理中心網頁主控台、發佈點、從屬管理伺服器和 klakaut 自動化物件，以及用於從用戶端裝置接收資料。

通常，SSL 連接埠 TCP 13000 僅可以由網路代理、從屬管理伺服器和 DMZ 中的主管理伺服器使用。在一些情況下，卡巴斯基安全管理中心網頁主控台可能需要透過 SSL 連接埠 13000 連線：

- 如果將單一的 SSL 連接埠用於卡巴斯基安全管理中心網頁主控台和其他活動（從用戶端裝置接收資料、連線發佈點、連線從屬管理伺服器）。
- 如果 klakaut 自動化物件未直接連線到管理伺服器，而是透過 DMZ 中的發佈點。

配置管理伺服器連線事件記錄

操作期間的連線歷程和到管理伺服器的連線嘗試可以被儲存到檔案。檔案中的資訊允許您跟蹤不僅您的網路基礎架構中的連線，還有對伺服器的非授權存取嘗試。

要記錄連線管理伺服器事件：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。

   管理伺服器內容視窗將開啟。

2. 在**一般**標籤，選取**連線連接埠**區段。

3. 啟用**記錄管理伺服器連線事件**選項。

   所有連入管理伺服器的後續事件、身分驗證結果和 SSL 錯誤將被儲存到 %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog。

設定管理伺服器網際網路存取設定

您必須設定網際網路存取權限，才能使用卡巴斯基安全網路並下載卡巴斯基安全管理中心病毒資料庫和受管理卡巴斯基應用程式的更新。

指定管理伺服器的網際網路存取設定：

1. 在主功能表中，按一下管理伺服器名稱旁邊的設定圖示（ ）。

   管理伺服器內容視窗將開啟。

2. 在**一般**頁簽上，選取**設定網際網路存取**區段。

3. 如果您要在連線到網際網路時使用代理伺服器，請啟用**使用代理伺服器**選項。如果啟用此選項，可將欄位用於輸入設定。為代理伺服器連線指定以下設定：

   - **位址**

     卡巴斯基安全管理中心用於連線到網際網路的代理伺服器位址。

   - **連接埠號**

     將建立卡巴斯基安全管理中心代理伺服器連線的埠號。

   - **略過本機位址的代理伺服器**

     將不會使用代理伺服器連線本機網路的裝置。

   - **代理伺服器身分驗證**

     如果選取該方塊，您可以在輸入欄位中為代理伺服器身分驗證指定憑證。

     如果選取**使用代理伺服器**核取方塊，則可使用該輸入欄位。

   - **使用者名稱**

     用來建立前往 Proxy 伺服器之連線的使用者帳戶（若選取了**代理伺服器身分驗證**核取方塊，則此欄位可用）。

   - **密碼**

     其帳戶用來建立 Proxy 伺服器連線的使用者所設定的密碼（若選取了**代理伺服器身分驗證**核取方塊，則此欄位可用）。

     若要檢視輸入的密碼，依您所需的時間長度點擊並按住**顯示**按鈕。

您還可以使用快速啟動精靈設定網際網路存取。

設定事件儲存區中的最大事件數量

在管理伺服器內容視窗的**事件儲存區**區域中，您可以透過限制事件記錄數和儲存期限來編輯管理伺服器資料庫的事件儲存設定。當您指定事件最大數時，應用程式計算用於指定數目的儲存空間的大概大小。您可以使用該大概計算來評估您在磁碟上是否具有足夠空間以避免資料庫溢出。管理伺服器資料庫的預設容量是 400,000 個事件。最大建議的資料庫容量是 45,000,000 個事件。

應用程式每 10 分鐘檢查一次資料庫。如果事件數達到指定的最大值加 10,000，應用程式將刪除最舊的事件，以便僅保留指定的最大事件數。

若管理伺服器刪除舊事件，則無法儲存新事件到資料庫。在此時間段內，拒絕事件的資訊被寫入卡巴斯基事件記錄。新事件被列隊，然後在刪除操作後被儲存到資料庫。

要限制儲存在管理伺服器事件儲存區中的事件的數量：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**標籤，選取**事件儲存區**區段。指定儲存在資料庫中的最大事件數量。
3. 點擊**儲存**按鈕。

此外，您可以執行以下操作：

- 變更任何工作的設定，以儲存與工作進度相關的事件，或者只儲存工作執行結果。
- 減少或停用安裝在受管理裝置上的管理伺服器、網路代理和卡巴斯基應用程式的事件的儲存期限。

為此，您將降低資料庫中的事件數量，提高與資料庫中事件表分析相關之情境的執行速度，並降低緊急事件被大數量事件覆寫的風險。

UEFI 防護裝置連線設定

*UEFI 防護裝置*是包含在 BIOS 層級整合的適用於 UEFI 的卡巴斯基解決方案或應用程式的裝置。整合的防護從系統啟動時開始確保裝置安全，未整合軟體的裝置僅在安全應用程式啟動後開始防護工作。支援這些裝置的管理的卡巴斯基安全管理中心。

要修改 UEFI 防護裝置的連線設定：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**標籤，選取**附加連接埠**區段。

3. 修改相關設定：

- **開啟 UEFI 防護裝置和 KasperskyOS 裝置的連接埠**

  UEFI 防護裝置可以連線到管理伺服器。

- **UEFI 防護裝置和 KasperskyOS 裝置的連接埠**

  若啟用**開啟 UEFI 防護裝置和 KasperskyOS 裝置的連接埠**選項則可變更埠號。預設埠號為 13294。

4. 點擊**儲存**按鈕。

UEFI 防護裝置現在可以連線到管理伺服器。

建立管理伺服器階層：新增次要管理伺服器

新增從屬管理伺服器（在未來的主管理伺服器上執行）

您可以新增管理伺服器作為從屬管理伺服器，進而建立「主要/從屬」層級。

要新增可以透過卡巴斯基安全管理中心網頁主控台連線的從屬管理伺服器：

1. 確保未來主管理伺服器的連接埠 13000 可用於從從屬管理伺服器接收連線。
2. 在未來主管理伺服器上，按一下設定圖示 ( )。
3. 在開啟的內容頁面中，選擇**管理伺服器**頁籤。
4. 選取您要向其新增管理伺服器的管理群組名稱旁邊的核取方塊。
5. 在功能表行中，點擊**連線從屬管理伺服器**。
   新增從屬管理伺服器精靈啟動。使用**下一步**按鈕進行精靈。

6. 填充以下欄位：

- **將主管理伺服器連線到 DMZ 中的從屬管理伺服器**

  如果從屬管理伺服器位於非武裝區 (DMZ)，選取該選項。

  如果選取此選項，則需要指定**從屬伺服器位址**參數。

  如果選擇此選項，主管理伺服器將啟動與從屬管理伺服器的連線。否則，從屬管理伺服器將啟動與主管理伺服器的連線。

- **從屬管理伺服器顯示名稱**

  從屬管理伺服器將顯示在層級的名稱。如果需要，您可以輸入 IP 位址作為名稱，也可以使用例如「群組 1 的從屬伺服器」之類的名稱。

- **從屬管理伺服器位址（可選）**

  指定從屬管理伺服器的 IP 位址或網域名稱。

  如果啟用了**將主管理伺服器連線至 DMZ 中的從屬管理伺服器**選項，則需要此參數。

- **管理伺服器 SSL 連接埠號**

  指定主管理伺服器上的 SSL 埠號。預設埠號為 13000。

- **管理伺服器 API 連接埠**

  指定主管理伺服器上的埠號以透過 OpenAPI 接收連線。預設埠號為 13299。

7. 指定從屬管理伺服器的憑證。如果指定了**從屬伺服器位址**參數，則可以點擊**從從屬管理伺服器獲取**按鈕來取得憑證。否則，請點擊**瀏覽憑證檔案**按鈕，然後找到憑證檔案。

8. 指定連線設定：

   - 輸入未來的主管理伺服器位址。
   - 如果未來的從屬管理伺服器使用代理伺服器，請輸入代理伺服器位址和使用者憑證以連線到代理伺服器。

9. 輸入對未來的從屬管理伺服器具有存取權限的使用者憑證。

10. 如果啟用並設定了雙步驟驗證，請指定身份驗證器應用程式產生的安全碼。

    如果啟用了雙步驟驗證，但並未針對您指定的帳戶進行設定，請從未來的從屬伺服器中建立階層（請參閱下面的說明）。

如果連線設定正確，則與未來的從屬伺服器建立連線，並建立「主要/從屬」階層。如果連線失敗，請檢查連線設定或手動指定未來的從屬伺服器的憑證。

主管理伺服器和從屬管理伺服器之間的連線是透過連接埠 13000 建立的。主管理伺服器的工作和政策被接收和套用。從屬管理伺服器顯示在主管理伺服器上，在新增其的管理群組中。

新增從屬管理伺服器（執行在未來從屬管理伺服器）

如果您無法連線到未來從屬管理伺服器（例如，它臨時被斷開或無法連線），您仍可以新增從屬管理伺服器。

要新增不可以透過卡巴斯基安全管理中心網頁主控台連線的從屬管理伺服器：

1. 傳送未來主要管理伺服器的憑證檔案到未來次要管理伺服器所在辦公室的系統管理員。（您可以，例如，寫入檔案到外部裝置，例如快閃記憶體磁碟機，或者透過郵件傳送它）

   憑證檔案位於未來的主管理伺服器上，位置是 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer。

2. 提示未來從屬管理伺服器的責任系統管理員做以下事情：

   a. 按一下設定圖示（）。

   b. 在開啟的內容頁面中，前往**一般**頁籤的**管理伺服器階層**區段。

   c. 選擇**此管理伺服器是階層中的從屬伺服器**選項。

   d. 在**主管理伺服器位址**欄位，輸入未來主要管理伺服器的網路名稱。

   e. 透過按一下**瀏覽**選取先前儲存的帶有未來主管理伺服器憑證的檔案。

   f. 如有需要，請選取**將主管理伺服器連線到 DMZ 中的從屬管理伺服器**核取方塊。

   g. 若未來次要管理伺服器的連線會透過代理伺服器執行，請選取**使用代理伺服器**選項並指定連線設定。

   h. 點擊**儲存**。

「主要/從屬」層級被建立。主管理伺服器開始使用連接埠 13000 從從屬管理伺服器接收連線。主管理伺服器的工作和政策被接收和套用。從屬管理伺服器顯示在主管理伺服器上，在新增其的管理群組中。

檢視次要管理伺服器清單

要檢視從屬（包括虛擬）管理伺服器清單：

在主功能表中，按一下管理伺服器名稱，其位於設定圖示（）旁邊。

從屬（包括虛擬）管理伺服器下拉清單被顯示。

您可透過點及其名稱前往這些管理伺服器的任何一個。

管理群組也會予以顯示，但是灰色的，無法在此功能表中進行管理。

如果您在卡巴斯基安全管理中心網頁主控台中連線到主管理伺服器，但無法連線到由從屬管理伺服器管理的虛擬管理伺服器，您可以使用以下方法之一：

- **修改現有的卡巴斯基安全管理中心網頁主控台安裝以將從屬伺服器新增到受信任的管理伺服器清單中**。然後，您將能夠連線到卡巴斯基安全管理中心網頁主控台中的虛擬管理伺服器。

  1. 在安裝了卡巴斯基安全管理中心網頁主控台的裝置上，在具有管理員權限的帳戶下執行 ksc-web-console-<版本號>.<組建編號>.exe 安裝檔案。

     安裝精靈將啟動。使用**下一步**按鈕進行精靈。

  2. 選取**升級**選項。

  3. 在**修改類型**步驟，選擇**編輯連線設定**選項。

  4. 在**受信任的管理伺服器**步驟，新增所需的從屬管理伺服器。

  5. 在最後的步驟，按一下**修改**以套用新設定。

  6. 在應用程式重新設定成功完成後，按一下**完成**按鈕。

- 使用卡巴斯基安全管理中心網頁主控台直接連線到在其上建立虛擬伺服器的從屬管理伺服器。然後，您將能夠切換到卡巴斯基安全管理中心網頁主控台中的虛擬管理伺服器。

- 使用基於 MMC 的管理主控台直接連線到虛擬伺服器。

刪除管理伺服器階層

如果不再想擁有管理伺服器階層，您可以從該階層將其斷開連線。

要刪除管理伺服器階層：

1. 在主功能表中，按一下主管理伺服器名稱旁邊的設定圖示（ ）。

2. 在開啟的頁面中，前往**管理伺服器**標籤。

3. 在您要刪除次要管理伺服器的管理群組，選取次要管理伺服器。

4. 在功能表中，點擊**刪除**。

5. 在開啟的視窗中，點擊**確定**以確認您要刪除該次要管理伺服器。

   先前的主要和次要管理伺服器現在彼此獨立。層級不再存在。

管理伺服器維護

管理伺服器維護可讓您釋放管理伺服器資料夾中的空間，並刪除不再需要的物件以減少資料庫容積。這有助於提高應用程式的效能和操作可靠性。我們建議您至少每週維護一次管理伺服器。

管理伺服器維護透過專用工作執行。應用程式會在維護管理伺服器時執行以下操作：

- 從儲存資料夾中刪除不需要的資料夾與檔案。
- 從表格中刪除不必要的記錄（也稱為「懸空指標」）。
- 清除快取。
- 維護資料庫（如果您使用 SQL Server 或 PostgreSQL 作為 DBMS）：
  - 檢查資料庫是否存在錯誤（僅適用於 SQL Server）。
  - 重組資料庫索引。
  - 更新資料庫統計資訊。
  - 收縮資料庫（如果必要）。

管理伺服器維護工作支援 MariaDB 版本 10.3 及更高版本。如果您使用 MariaDB 10.2 或更早的版本，管理員將必須自己維護此 DBMS。

管理伺服器維護工作在您安裝卡巴斯基安全管理中心時自動建立。如果管理伺服器維護工作被刪除，您可以手動建立它。

要建立管理伺服器維護工作：

1. 在主功能表中，轉至 **裝置 → 工作**。
2. 按一下**新增**按鈕。
   新工作精靈啟動。
3. 在精靈的**新工作**視窗中，選擇**管理伺服器維護**作為工作類型，然後點擊**下一步**按鈕。
4. 遵照剩餘的精靈說明。

新建立的工作會顯示在工作清單。一個單一管理伺服器僅可以執行一個管理伺服器維護工作。如果已為管理伺服器建立了管理伺服器維護工作，則無法再建立新的管理伺服器維護工作。

設定介面

您可設定卡巴斯基安全管理中心網頁主控台介面根據使用的功能顯示和隱藏區段與介面元素。

若要根據目前使用的功能集設定卡巴斯基安全管理中心網頁主控台介面：

1. 在主功能表中，轉到您的帳戶設定，然後選擇**介面選項**。
2. 在開啟的**介面選項**視窗中，啟用或停用所需選項。
3. 按一下**儲存**。

之後，主控台會根據啟用的選項在主功能表中顯示相關區域。例如，如果您啟用**顯示 EDR 警示**，則**監控和報告 → 警示**區域會出現在主功能表中。

管理虛擬管理伺服器

本章節說明用來管理虛擬管理伺服器的以下操作：

- 建立虛擬管理伺服器
- 啓用和停用虛擬管理伺服器
- 為虛擬管理伺服器指派管理員
- 變更用戶端裝置的管理伺服器
- 刪除虛擬管理伺服器

建立虛擬管理伺服器

您可以建立虛擬管理伺服器並新增它們到管理群組。

當您建立虛擬管理伺服器時，它會繼承主管理伺服器的使用者清單和所有使用者權限。如果使用者有權存取主伺服器，則該使用者也有權存取虛擬伺服器。建立後，您可以分別設定對伺服器的存取權限。

要建立和新增虛擬管理伺服器：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
2. 在開啟的頁面中，前往**管理伺服器**頁籤。
3. 選取您要新增虛擬管理伺服器到的管理群組。
   虛擬管理伺服器將管理所選群組（包括子群組）中的裝置。
4. 在功能表行中，點擊**新虛擬管理伺服器**。
5. 在開啟的頁面上，定義新虛擬管理伺服器的內容：
   - **虛擬管理伺服器名稱**。
   - **管理伺服器連線位址**
     您可指定管理伺服器的名稱或 IP 位址。
6. 從使用者清單中，選擇虛擬管理伺服器管理員。如果您想，您可以編輯現有帳戶之一，然後分配其管理員角色，或建立一個新使用者帳戶。
7. 點擊**儲存**。

新虛擬管理伺服器會建立並新增至管理群組，同時顯示在**管理伺服器**頁籤上。

如果您在卡巴斯基安全管理中心網頁主控台中連線到主管理伺服器，但無法連線到由從屬管理伺服器管理的虛擬管理伺服器，您可以使用以下方法之一：

- **修改現有的卡巴斯基安全管理中心網頁主控台安裝以將從屬伺服器新增到受信任的管理伺服器清單中**。然後，您將能夠連線到卡巴斯基安全管理中心網頁主控台中的虛擬管理伺服器。

  1. 在安裝了卡巴斯基安全管理中心網頁主控台的裝置上，在具有管理員權限的帳戶下執行 ksc-web-console-<版本號>.<組建編號>.exe 安裝檔案。

     安裝精靈將啟動。使用**下一步**按鈕進行精靈。

  2. 選取**升級**選項。

  3. 在**修改類型**步驟，選擇**編輯連線設定**選項。

  4. 在**受信任的管理伺服器**步驟，新增所需的從屬管理伺服器。

  5. 在最後的步驟，按一下**修改**以套用新設定。

  6. 在應用程式重新設定成功完成後，按一下**完成**按鈕。

- 使用卡巴斯基安全管理中心網頁主控台直接連線到在其上建立虛擬伺服器的從屬管理伺服器。然後，您將能夠切換到卡巴斯基安全管理中心網頁主控台中的虛擬管理伺服器。

- 使用基於 MMC 的管理主控台直接連線到虛擬伺服器。

啟用和停用虛擬管理伺服器

當您建立新的虛擬管理伺服器時，預設情況下會啟用它。您可以隨時停用或再次啟用它。停用或啟用虛擬管理伺服器等同於關閉或開啓實體管理伺服器。

要啓用或停用虛擬管理伺服器：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。

2. 在開啟的頁面中，前往**管理伺服器**頁籤。

3. 選擇要啟用或停用的虛擬管理伺服器。

4. 在功能表行上，點擊**啟用 / 停用虛擬管理伺服器**按鈕。

   虛擬管理伺服器狀態被變更為啟用或停用，具體取決於其先前的狀態。更新後的狀態顯示在管理伺服器名稱旁邊。

為虛擬管理伺服器指派管理員

當您的組織使用虛擬管理伺服器時，您可能希望為每個虛擬管理伺服器指派一個專用管理員。例如，當您建立虛擬管理伺服器來管理組織的獨立辦公室或部門時，或者如果您是 MSP 供應商並透過虛擬管理伺服器管理您的租用戶，這可能很有用。

當您建立虛擬管理伺服器時，它會繼承主管理伺服器的使用者清單和所有使用者權限。如果使用者有權存取主伺服器，則該使用者也有權存取虛擬伺服器。建立後，您可以分別設定對伺服器的存取權限。如果您只想為虛擬管理伺服器指派管理員，請確保該管理員沒有主管理伺服器的存取權限。

您可以授予管理員對虛擬管理伺服器的存取權限，來為虛擬管理伺服器指派管理員。您可以透過以下方式之一授予所需的存取權限：

- 手動設定管理員的存取權限
- 為管理員指派一個或多個使用者角色

要登入卡巴斯基安全管理中心網頁主控台，虛擬管理伺服器的管理員需指定虛擬管理伺服器名稱、使用者名稱和密碼。卡巴斯基安全管理中心網頁主控台對管理員進行身分驗證，並開啟管理員有權存取的虛擬管理伺服器。管理員不能在管理伺服器之間切換。

先決條件

在開始之前，請確保滿足以下條件：

- 已建立虛擬管理伺服器。
- 在主管理伺服器上，您已為虛擬管理伺服器指派的管理員建立一個帳戶。
- 您在**一般功能**：**使用者權限**功能區域中有**修改物件 ACL** 權限。

手動設定存取權限

為虛擬管理伺服器指派管理員：

1. 在主功能表中，切換到所需的虛擬管理伺服器：
   a. 按一下目前管理伺服器名稱右側的 > 形箭號圖示（ ）。
   b. 選取所需的管理伺服器。
2. 在主功能表中，按一下管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
3. 在**存取權限**頁簽上，點擊**新增**按鈕。
   主管理伺服器和當前虛擬管理伺服器的統一使用者清單開啟。
4. 從使用者清單中，選擇要指派給虛擬管理伺服器的管理員帳戶，然後按一下**確定**按鈕。
   應用程式將選取的使用者新增到**存取權限**頁籤上的使用者清單。
5. 選取新增帳戶旁邊的核取方塊，然後點擊**存取權限**按鈕。
6. 設定管理員對虛擬管理伺服器的權限。
   要成功進行身分驗證，管理員至少必須具有以下權限：
   - **一般功能** → **基本功能**功能區域中的**讀取**權限。
   - **一般功能** → **虛擬管理伺服器**功能區域中的**讀取**權限。

應用程式將修改後的使用者權限儲存到管理員帳戶中。

指派使用者角色來設定存取權限

或者，您可以透過使用者角色，將存取權限授予虛擬管理伺服器管理員。例如，如果您想在同一個虛擬管理伺服器上指派多個管理員，這可能很有用。如果是這種情況，您可以為管理員帳戶指派相同的一個或多個使用者角色，而不是為多個管理員設定相同的使用者權限。

要指派使用者角色來為虛擬管理伺服器指派管理員：

1. 在主管理伺服器上，建立一個新的使用者角色，然後指定管理員必須在虛擬管理伺服器上擁有的所有必需存取權限。您可以建立多個角色，例如，如果您想要單獨存取不同的功能區域。
2. 在主功能表中，切換到所需的虛擬管理伺服器：
   a. 按一下目前管理伺服器名稱右側的 > 形箭號圖示（ ）。
   b. 選取所需的管理伺服器。
3. 將新角色或多個角色指派給管理員帳戶。

應用程式將角色指派給管理員帳戶。

在物件層級設定存取權限

除了指派功能區域層級的存取權限，您還可以在虛擬管理伺服器上設定對特定物件的存取，例如，特定的管理群組或工作。為此，請切換到虛擬管理伺服器，然後在物件的屬性中設定存取權限。

變更用戶端裝置的管理伺服器

您可以使用"*變更管理伺服器*"工作來變更用戶端裝置連線的管理伺服器。工作完成後，所選用戶端裝置將被置於您指定的管理伺服器的管理之下。

您無法對透過連線閘道連線到管理伺服器的用戶端裝置使用*變更管理伺服器*工作。對於這樣的裝置，您必須重新設定網路代理或重新安裝網路代理並指定連線閘道。

要變更用戶端裝置連線的管理伺服器：

1. 在主功能表中，轉至 **裝置** → **工作**。
2. 點擊**新增**。

   新工作精靈啟動。使用**下一步**按鈕進行精靈。

3. 在精靈的**新工作**步驟中，指定以下設定：

   a. 在**應用程式**下拉清單中，選擇**卡巴斯基安全管理中心**。

   b. 在**工作類型**欄位中，選擇**變更管理伺服器**。

   c. 在**工作名稱**視窗中，指定您正在建立的工作的名稱。
   工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。

   d. 選取要對其分配工作的裝置：

   - **分配工作到管理群組**

     工作被分配到包含在管理群組中的裝置。您可以指定其中一個現有群組或者建立新群組。

     例如，您可能要使用該選項執行傳送訊息到使用者工作，如果訊息針對包含在特定管理群組中的裝置。

     如果工作被指派給管理群組，則工作屬性視窗中不會顯示**安全**標籤，因為群組工作受其所套用的群組的安全設定的約束。

   - **手動指定裝置位址或從清單匯入位址**

     您可以指定您要為其分配工作的裝置的 NetBIOS 名稱、DNS 名稱、IP 位址和 IP 子網路。

     您可能要使用該選項以對特定子網路執行工作。例如，您可能要安裝特定應用程式到會計裝置，或者掃描疑似被感染子網路中的裝置。

   - **分配工作到裝置分類**

     該工作被分配到裝置選項中的裝置。您可以指定其中一個現有選項。

     例如，您可能要使用該選項在特定作業系統版本的裝置上執行工作。

4. 在精靈的**工作範圍**步驟，指定管理群組、具有特定位址的裝置或裝置選擇。

5. 在精靈的該步驟，確認您同意變更用戶端裝置的管理伺服器的條款。

6. 在精靈的該步驟，選擇您想要用來管理所選裝置的管理伺服器：

- **變更到另一個主管理伺服器**

  若要將用戶端裝置移至另一台主管理伺服器，請指定下列管理伺服器連線設定：

  1. 在**管理伺服器位址**欄位中，指定新的主管理伺服器的位址。
  2. 在**連接埠號**欄位中，指定連線到管理伺服器的連接埠號碼。
     預設埠號為 14000。
  3. 在**SSL 連接埠**欄位中，指定主管理伺服器上的 SSL 連接埠號。
     預設埠號為 13000。
  4. 如有必要，請啟用**使用代理伺服器**選項。
     如果停用此選項，則使用直接連線將裝置連線到管理伺服器。
     如果啟用此選項，請指定代理伺服器參數：
     - **代理伺服器位址**
     - **代理伺服器連接埠**

     如果您的代理伺服器需要身分驗證，請在**使用者名稱** 和 **密碼**欄位中指定與代理伺服器建立連線的帳戶的憑據。我們建議您指定僅具有代理伺服器身分驗證所需的最低權限的帳戶的憑據。
  5. 如果有必要，請上傳新的管理伺服器憑證。

- **變更到該主伺服器上的另一個虛擬伺服器**

  選擇此選項可以將用戶端裝置移至目前主管理伺服器上的虛擬管理伺服器。為此，在**虛擬管理伺服器名稱**下拉清單中，選擇必要的虛擬管理伺服器。

7. 在精靈的**選取要執行此工作的帳戶**步驟中，指定帳戶設定：

- **預設帳戶**

  在與執行該工作的應用程式相同的帳戶下執行該工作。
  預設情況下已選定此選項。

- **指定帳戶**

  填寫**帳戶**與**密碼**欄位以指定工作要在其下執行的帳戶詳情。帳戶必須對此工作有足夠的權限。

  - **帳戶**

    執行該工作的帳戶。

  - **密碼**

    工作執行時使用的帳戶的密碼。

8. 如果要變更預設工作設定，請在精靈的**完成工作建立**步驟中啟用**建立完成時開啟工作詳情**選項。
   如果您不啟用該選項，工作使用預設設定建立。您可以稍後隨時變更預設設定。

9. 點擊**完成**按鈕。
   工作被建立並顯示在工作清單。

10. 按一下建立的工作的名稱以開啟工作內容視窗。

11. 如果要變更預設工作設定，請在工作屬性視窗中根據需要指定一般工作設定。

12. 點擊**儲存**按鈕。
    工作被建立和配置。

13. 執行建立的工作。

在工作完成後，為其建立工作的用戶端裝置將被工作設定中指定的管理伺服器管理。

刪除虛擬管理伺服器

當您刪除虛擬管理伺服器時，在管理伺服器上建立的所有物件（包括政策和工作）也將被刪除。由虛擬管理伺服器管理的管理群組中的受管理裝置將被從管理群組中移除。要返回卡巴斯基安全管理中心管理的裝置，請執行網路輪詢，然後將找到的裝置從未分配的裝置群組移動到管理群組。

要刪除虛擬管理伺服器：

1. 在主功能表中，按一下管理伺服器名稱旁邊的設定圖示（ ）。

2. 在開啟的頁面中，前往**管理伺服器**頁籤。

3. 選擇要刪除的虛擬管理伺服器。

4. 在功能表行中，點擊 **刪除**按鈕。

虛擬管理伺服器將被刪除。

啟用帳戶防護以防止未經授權的修改

您可以啟用其他選項以防護使用者帳戶免遭未經授權的修改。如果啟用此選項，則修改使用者帳戶設定需要具有修改權限的使用者授權。

要啟用或停用未經授權的帳戶防護，請執行以下操作：

1. 在主功能表中，轉至 **使用者和角色 → 使用者**。

2. 點擊您要為其指定帳戶防護免受未經授權修改的內部使用者帳戶名稱。

3. 在開啟的使用者設定視窗中，選取**帳戶防護**頁籤。

4. 在**帳戶防護**頁籤中，如果您希望每次變更或修改帳戶設定時都要請求憑證，請選取**請求身分驗證以檢查權限來修改使用者帳戶**選項。否則，請選取**允許使用者無需其他身分驗證即可修改此帳戶**選項。

5. 按一下**儲存**按鈕。

為使用者帳戶啟用了防止未經授權的修改的帳戶防護。

兩步驟驗證

本節介紹如何使用兩步驟驗證來減少未授權存取卡巴斯基安全管理中心 網頁主控台的風險。

關於雙步驟驗證

為帳戶啟用雙步驟驗證後，除了使用者名稱和密碼外，還需要一次性安全代碼才能登入網頁主控台或卡巴斯基安全管理中心網頁主控台。啟用網域身分驗證後，使用者只需輸入一次性安全碼即可。

要使用雙步驟驗證，請在行動裝置或電腦上安裝可產生一次性安全碼的身份驗證器應用程式。您可以使用任何支援基於時間的一次性密碼演算法 (TOTP) 的應用程式，例如：

- Google Authenticator
- Microsoft Authenticator
- Bitrix24 OTP
- Yandex Key
- Avanpost 驗證器
- Aladdin 2FA

要檢查卡巴斯基安全管理中心是否支援您要使用的身分驗證器應用程式，請為所有使用者或特定使用者啟用雙步驟驗證。

其中步驟之一建議您指定由身分驗證器應用程式產生的安全代碼。如果成功，則卡巴斯基安全管理中心支援所選的身分驗證器。

強烈建議將秘密金鑰或 QR 碼儲存在安全的地方。如果您遺失了行動裝置，這有助於您復原對卡巴斯基安全管理中心網頁主控台的存取。

為了確保使用卡巴斯基安全管理中心，您可以為自己的帳戶啟用雙步驟驗證，並為所有使用者啟用雙步驟驗證。

您可以從雙步驟驗證中排除帳戶。對於無法接收身分驗證安全碼的服務帳戶，這可能是必需的。

規則和限制

為了能夠為所有使用者啟動雙步驟驗證並為特定使用者停用雙步驟驗證：

- 確保您的帳戶在**一般功能：使用者權限**功能區域中有修改物件 ACL 權限。
- 對帳戶啟用雙步驟驗證。

為了能夠為所有使用者停用雙步驟驗證：

- 確保您的帳戶在**一般功能：使用者權限**功能區域中有修改物件 ACL 權限。
- 使用雙步驟驗證登入卡巴斯基安全管理中心網頁主控台。

如果在卡巴斯基安全管理中心管理伺服器 13 或者更高版本上為使用者帳戶啟用了雙步驟驗證，則該使用者將無法登入卡巴斯基安全管理中心網頁主控台版本 12、12.1 或 12.2。

重新發布金鑰

任何使用者都可以重新發布用於雙步驟驗證的金鑰。當使用者使用重新發布的秘密金鑰登入到管理伺服器時，新的秘密金鑰將為使用者帳戶進行儲存。如果使用者輸入錯誤的新秘密金鑰，新秘密金鑰將不會得到儲存，當前秘密金鑰仍然有效。

安全碼具有名為*簽發者名稱*的識別碼。安全碼簽發者名稱用作驗證應用程式中管理伺服器的識別碼。安全碼簽發者名稱的預設值與管理伺服器的名稱相同。您可以變更安全碼簽發者名稱的名稱。如果變更了安全碼簽發者名稱，則必須簽發新的金鑰並將其傳遞給驗證應用程式。

為所有使用者配置兩步驟驗證

此情境說明如何為所有使用者啟用雙步驟驗證，以及如何從雙步驟驗證中排除使用者帳戶。如果在為其他使用者啟用帳戶前未啟用帳戶的雙步驟驗證，則應用程式會先開啟用於為帳戶啟用雙步驟驗證的視窗。此情境還說明如何為您自己的帳戶啟用雙步驟驗證。

如果您為帳戶啟用了雙步驟驗證，則可以進入為所有使用者啟用雙步驟驗證的階段。

先決條件

開始之前：

- 確保您的使用者帳戶具有**一般功能：使用者權限**功能區域的修改物件 ACL 權限，用於修改其他使用者帳戶的安全設定。
- 確保管理伺服器的其他使用者在其裝置上安裝驗證應用程式。

階段

為所有使用者啟用雙步驟驗證將分階段進行：

1. **在裝置上安裝驗證應用程式**

   您可以安裝任何支援基於時間的一次性密碼演算法 (TOTP) 的應用程式，例如：

   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP
   - Yandex Key
   - Avanpost 驗證器
   - Aladdin 2FA

   要檢查卡巴斯基安全管理中心是否支援您要使用的身分驗證器應用程式，請為所有使用者或特定使用者啟用雙步驟驗證。

   其中步驟之一建議您指定由身分驗證器應用程式產生的安全代碼。如果成功，則卡巴斯基安全管理中心支援所選的身分驗證器。

   我們強烈建議不要在與管理伺服器建立連線的同一台裝置上安裝驗證器應用程式。

2. **將驗證應用程式時間與安裝了管理伺服器的裝置時間同步**

   透過使用外部時間來源，確保具有身分驗證器應用程式的裝置上的時間和具有管理伺服器的裝置上的時間與 UTC 同步。否則，雙步驟驗證的認證和啟動過程中可能會出現失敗。

3. **對您的帳戶啟用雙步驟驗證，並為您的帳戶接收金鑰**

   說明：

   - 對於 MMC 型管理主控台：對您自己的帳戶啟用雙步驟驗證
   - 對於卡巴斯基安全管理中心網頁主控台：對您自己的帳戶啟用雙步驟驗證

   為帳戶啟用雙步驟驗證後，您可以為所有使用者啟用雙步驟驗證。

4. **對所有使用者啟用雙步驟驗證**

   啟用了雙步驟驗證的使用者必須使用它登入管理伺服器。

   說明：

   - 對於 MMC 型管理主控台：對所有使用者啟用雙步驟驗證
   - 對於卡巴斯基安全管理中心網頁主控台：對所有使用者啟用雙步驟驗證

5. **編輯安全碼簽發者的名稱**

   如果您有多個具有相似名稱的管理伺服器，則可能必須更改安全碼簽發者的名稱，以便更進一步識別不同的管理伺服器。

   說明：

   - 對於 MMC 型管理主控台：編輯安全碼簽發者的名稱
   - 對於卡巴斯基安全管理中心網頁主控台：編輯安全碼簽發者的名稱

6. **排除不需要啟用兩步驟驗證的使用者帳戶**

   如有需要，您可以從雙步驟驗證中排除使用者。具有被排除帳戶的使用者不必使用雙步驟驗證即可登入管理伺服器。

   說明：

   - 對於 MMC 型管理主控台：從雙步驟驗證中排除帳戶
   - 對於卡巴斯基安全管理中心網頁主控台：從雙步驟驗證中排除帳戶

7. **為您自己的帳戶配置兩步驟驗證**

   如果使用者未被排除在雙步驟驗證之外，並且尚未為其帳戶配置雙步驟驗證，則他們需要在登入卡巴斯基安全管理中心時開啟的視窗中進行配置。否則，他們將無法按照其權限存取管理伺服器。

   說明：

   - 對於 MMC 型管理主控台：為您自己的帳戶配置雙步驟驗證
   - 對於卡巴斯基安全管理中心網頁主控台：為您自己的帳戶配置雙步驟驗證

結果

完成此情境後：

- 對帳戶啟用雙步驟驗證。
- 為管理伺服器的所有使用者帳戶啟用了雙步驟驗證，但已排除的使用者帳戶除外。

對您自己的帳戶啟用雙步驟驗證（網頁主控台）

您只能為自己的帳戶啟用兩步驟驗證。

在為帳戶啟用雙步驟驗證之前，請確保在行動裝置上安裝了身份驗證器應用程式。確保驗證應用程式中設定的時間必須與管理伺服器上設定的裝置時間同步。

要啟用使用者帳戶的兩步驟驗證：

1. 在主功能表中，轉至 **使用者和角色 → 使用者**。
2. 請點擊帳戶的名稱。
3. 在開啟的使用者設定視窗中，選取**驗證安全性**頁籤。
4. 在**驗證安全性**標籤上：
   a. 選擇**請求使用者名稱、密碼和安全碼（兩步驟驗證）**選項。點擊**儲存**按鈕。
   b. 在開啟的雙步驟驗證視窗中，點擊**檢視設定兩步驟驗證的方式**。
      在身份驗證器應用程式中輸入秘密金鑰，或點擊**檢視 QR 代碼**並透過行動裝置上的身份驗證器應用程式掃描 QR 碼以接收一次性安全碼。
   c. 在開啟的兩步驟驗證視窗中，指定由身分驗證器應用程式產生的安全碼，然後點擊**確認並套用**按鈕。
5. 點擊**儲存**按鈕。

對帳戶啟用雙步驟驗證。

對所有使用者啟用要求的雙步驟驗證（網頁主控台）

如果您的帳戶具有**一般功能：使用者權限**功能區域中的修改物件 ACL 權限，並且您透過雙步驟驗證進行了身分驗證，則可以為管理伺服器的所有使用者啟用雙步驟驗證。

若要為多個使用者啟用或停用雙步驟驗證，請執行以下操作：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。

   管理伺服器內容視窗將開啟。

2. 在屬性視窗的**驗證安全性**頁籤上，切換**所有使用者的兩步驟驗證**選項設定按鈕為啟用位置。

3. 如果未啟用帳戶的雙步驟驗證，則該應用程式將開啟一個視窗，以為您自己的帳戶啟用雙步驟驗證。

   a. 在雙步驗證視窗中，點擊**檢視設定兩步驟驗證的方式**。

   b. 在身份驗證器應用程式中手動輸入秘密金鑰，或點擊**檢視 QR 代碼**並透過行動裝置上的身份驗證器應用程式掃描 QR 碼以接收一次性安全碼。

   c. 在開啟的兩步驟驗證視窗中，指定由身分驗證器應用程式產生的安全碼，然後點擊**確認並套用**按鈕。

為所有使用者啟用了雙步驟驗證。從現在開始，除了其帳戶不包括在雙步驟驗證中的使用者之外，管理伺服器的使用者（包括在啟用此選項後新增的使用者）都必須為其帳戶設定雙步驟驗證。

對使用者帳戶停用雙步驟驗證（網頁主控台）

您可以為自己的帳戶以及任何其他使用者的帳戶停用兩步驟驗證。

如果您的帳戶具有**一般功能：使用者權限**功能區域中的修改物件 ACL 權限，並且您透過雙步驟驗證進行了身分驗證，則可以為另一個使用者帳戶停用雙步驟驗證。

要停用使用者帳戶的兩步驟驗證：

1. 在主功能表中，轉至 **使用者和角色 → 使用者**。

2. 點擊您想要為其停用兩步驟驗證之內部使用者帳戶的名稱。這可以是您自己的帳戶，也可以是任何其他使用者的帳戶。

3. 在開啟的使用者設定視窗中，選取**帳戶防護**頁籤。

4. 如果您要為使用者帳戶停用兩步驟驗證，請在**帳戶防護**頁籤上選取**僅請求使用者名稱和密碼**選項。

5. 點擊**儲存**按鈕。

該使用者帳戶已停用兩步驟驗證。

如果想為無法使用雙步驟驗證登入卡巴斯基安全管理中心網頁主控台的使用者恢復存取權限，請為此使用者帳戶停用雙步驟驗證，然後如上文所述，選擇**僅請求使用者名稱和密碼**選項。之後，以停用了雙步驟驗證的使用者帳戶登入卡巴斯基安全管理中心網頁主控台，然後再次啟用驗證。

對所有使用者停用要求的雙步驟驗證（網頁主控台）

如果您的帳戶啟用了雙步驟驗證，並且具有**一般功能：使用者權限**功能區域中的修改物件 ACL 權限，您就可為所有使用者停用要求的雙步驟驗證。如果您的帳戶未啟用雙步驟驗證，則必須先為帳戶啟用雙步驟驗證，然後再為所有使用者停用該功能。

若要為所有使用者啟用和停用雙步驟驗證：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在屬性視窗的**驗證安全性** 頁籤上，將**所有使用者的兩步驟驗證**選項切換至停用的位置。

所有使用者均停用雙步驟驗證。為所有使用者停用雙步驟驗證並不適用於先前單獨啟用雙步驟驗證的特定帳戶。

從雙步驟驗證中排除帳戶

如果您的帳戶具有**一般功能：使用者權限**功能區域中的修改物件 ACL 權限，則可以從雙步驟驗證中排除使用者帳戶。

如果某個使用者帳戶被排除在所有使用者的雙步驟驗證清單之外，則該使用者不必使用雙步驟驗證。

> 對於在身分驗證期間無法通過安全碼驗證的服務帳戶，可能有必要從雙步驟驗證中排除帳戶。

如果排除某些使用者帳戶的雙步驟驗證：

1. 如果要排除 Active Directory 帳戶，您必須執行 Active Directory 輪詢，以重新整理管理伺服器使用者清單。
2. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
3. 在屬性視窗的**驗證安全性**頁籤上的兩步驟驗證排除表中，點擊**新增**按鈕。
4. 在開啟的視窗中：
   a. 選取您要排除的使用者帳戶。
   b. 點擊**確定**按鈕。

所選取的使用者帳戶將排除在雙步驟驗證之外。

產生新的金鑰

僅當您透過兩步驟驗證獲得授權時，才能為帳戶的兩步驟驗證產生新的金鑰。

要為使用者帳戶產生新的金鑰：

1. 在主功能表中，轉至 **使用者和角色 → 使用者**。
2. 點擊您想要為其產生新的兩步驟驗證金鑰的使用者帳戶名稱。
3. 在開啟的使用者設定視窗中，選取**帳戶防護**頁籤。
4. 在**帳戶防護**頁籤中，點擊**產生新的金鑰**連結。
5. 在開啟的兩步驟驗證視窗中，指定由身分驗證應用程式產生的新安全金鑰。
6. 點擊**確認並套用**按鈕。

為使用者產生一個新的金鑰。

如果無法使用行動裝置，您可以在另一台行動裝置上安裝身分驗證器應用程式並產生新秘密金鑰，以還原對卡巴斯基安全管理中心網頁主控台的存取。

編輯安全碼簽發者的名稱（網頁主控台）

您可以為不同的管理伺服器使用多個識別碼（這稱為簽發者）。以防萬一，您可以變更安全碼簽發者的名稱，例如，管理伺服器已經為另一台管理伺服器使用了類似的安全碼簽發者名稱。預設情況下，安全碼簽發者的名稱與管理伺服器的名稱相同。

變更安全碼簽發者名稱後，您必須重新簽發新的金鑰並將其傳遞給驗證應用程式。

若要指定安全碼簽發者的新名稱：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在開啟的使用者設定視窗中，選取**帳戶防護**頁籤。
3. 在**帳戶防護**頁籤上，點擊**編輯**連結。
   編輯安全碼簽發者區段隨即開啟。
4. 指定新的安全碼簽發者名稱。
5. 點擊**確定**按鈕。

為管理伺服器指定了新的安全碼簽發者名稱。

對您自己的帳戶停用雙步驟驗證（網頁主控台）

啟用雙步驟驗證後首次登入卡巴斯基安全管理中心時，為您自己的帳戶配置雙步驟驗證的視窗將開啟。

在為帳戶配置雙步驟驗證之前，請確保在行動裝置上安裝了身份驗證器應用程式。

透過使用外部時間來源，確保具有身分驗證器應用程式的裝置上的時間和具有管理伺服器的裝置上的時間與 UTC 同步。

若要對帳戶配置雙步驟驗證，請執行以下操作：

1. 使用行動裝置上的身份驗證器應用程式產生一次性安全碼。要這麼做，請執行以下操作之一：

   - 在身分驗證器應用程式中手動輸入安全碼。
   - 點擊**檢視 QR 代碼**並使用身分驗證器應用程式掃描 QR 代碼。

   一個安全碼將顯示在行動裝置上。

2. 在配置雙步驟驗證視窗中，指定由身分驗證器應用程式產生的安全碼，然後點擊**確認並套用**按鈕。

   對帳戶配置雙步驟驗證。您可以根據您的權限存取管理伺服器。

備份複製和管理伺服器資料還原

資料備份允許您將管理伺服器從一台裝置上轉移至其他裝置且無資料遺失。將管理伺服器從一台裝置上轉移至其他裝置或者將其轉換為新版本卡巴斯基安全管理中心時，您可以使用備份還原資料。此外，您也可以使用資料備份將管理伺服器資料從卡巴斯基安全管理中心 Windows 移動到卡巴斯基安全管理中心 Linux 管理下（不支援將資料從卡巴斯基安全管理中心 Linux 移至卡巴斯基安全管理中心 Windows）。

請注意，已安裝的管理外掛程式沒有備份。從備份副本還原管理伺服器資料後，您需要下載並重新安裝受管應用程式的外掛程式。

備份管理伺服器資料之前，請檢查管理群組中是否新增了虛擬管理伺服器。如果新增了虛擬管理伺服器，請確保在備份之前為該虛擬管理伺服器分配了管理員。備份後，您將無法授予管理員對虛擬管理伺服器的存取權限。請注意，如果管理員帳戶憑據丟失，您將無法向虛擬管理員伺服器分配新管理員。

您可以使用以下方式之一建立管理伺服器資料備份：

- 透過使用管理主控台建立並執行資料備份工作。
- 透過在已安裝管理伺服器的裝置上執行 klbackup 公用程式。該公用程式包含在卡巴斯基安全管理中心分發套件。管理伺服器安裝完畢後，該公用程式位於程式安裝時指定資料夾的根目錄中。

以下資料儲存在管理伺服器的備份副本中：

- 管理伺服器資料庫（政策、工作、應用程式設定、管理伺服器上儲存的事件）。
- 有關管理群組和用戶端裝置的架構的設定資訊。
- 用於遠端安裝的應用程式分發套件的儲存。
- 管理伺服器憑證。

只用使用 klbackup 公用程式才能進行管理伺服器還原。

重新發佈卡巴斯基安全管理中心網頁主控台憑證

大多數瀏覽器都對憑證的有效期施加了限制。為了符合此限制，卡巴斯基安全管理中心 網頁主控台憑證的有效期會限制為 397 天。您可以透過手動發佈新的自主簽署憑證來取代從憑證機構 (CA) 收到的現有憑證。或者，您可以重新發佈過期的卡巴斯基安全管理中心 網頁主控台憑證。

自動重新發佈卡巴斯基安全管理中心網頁主控台的憑證不受支援。您必須手動重新發佈過期的憑證。

如果您已經使用了自主簽署憑證，則還可以透過按照安裝程式中的標準步驟升級卡巴斯基安全管理中心 網頁主控台來重新發佈憑證（ **升級**選項）。

當您開啟網頁主控台時，瀏覽器會通知您與網頁主控台的連線不是私有，並且網頁主控台憑證無效。出現此警告是因為網頁主控台憑證為自簽名並由卡巴斯基安全管理中心自動產生。要刪除或防止此警告，您可以執行以下操作之一：

- 重新發行憑證時指定自訂憑證（建議選項）。建立一個在您的基礎架構中受信任且滿足自訂憑證的要求的憑證。
- 重新發行憑證後，將網頁主控台憑證新增到受信任的瀏覽器憑證清單中。我們建議您僅在無法建立自訂憑證時使用此選項。

首次安裝卡巴斯基安全管理中心 網頁主控台時要發行新憑證：

1. 執行卡巴斯基安全管理中心 網頁主控台的常規安裝。
2. 當您到達**用戶端憑證**安裝精靈的步驟，選取**產生新憑證**選項，然後點擊**下一步**按鈕。
3. 完成安裝精靈的其餘步驟，直到完成安裝。

   卡巴斯基安全管理中心 網頁主控台新憑證的有效期為 397 天。

若要重新發佈已過期卡巴斯基安全管理中心 網頁主控台的憑證：

1. 在具有管理員權限的帳戶下，執行 ksc-web-console-<版本號>.<組建號碼>.exe 安裝檔案。
2. 在開啟的"安裝精靈"視窗中，選取一種語言，然後點擊**確定**。

3. 在歡迎視窗中，選取**重新發佈憑證**選項，然後點擊**下一步**。

4. 在下一步中，等待卡巴斯基安全管理中心 網頁主控台的重新配置完成，然後點擊**完成** 。

   重新頒發卡巴斯基安全管理中心 網頁主控台憑證的有效期為 397 天。

如果使用身分和存取管理器，您還必須為身分和存取管理器使用的連接埠重新發行所有 TLS 憑證。.卡巴斯基安全管理中心網頁主控台會在憑證過期時顯示通知。您必須遵循通知指示。

建立資料備份工作

備份工作是管理伺服器工作，透過快速啟動精靈進行建立。如果由快速啟動精靈建立的備份工作被刪除，您可以手動建立備份工作。

若要建立管理伺服器資料備份工作，請執行以下操作：

1. 在主功能表中，轉至 **裝置 → 工作**。

2. 按一下**新增**按鈕。

   新工作精靈啟動。

3. 在精靈的**新工作**視窗中，選取名為**備份管理伺服器資料**的工作類型。

4. 遵照剩餘的精靈說明。

備份管理伺服器資料工作只能建立單份副本。如果已經為管理伺服器建立了管理伺服器資料備份工作，它不會顯示在管理伺服器備份工作建立精靈的工作類型選取視窗中。

若要設定管理伺服器資料備份工作：

1. 在主功能表中，前往**裝置→工作**，然後選擇**備份管理伺服器資料**。

2. 點擊**備份管理伺服器資料**工作。

   工作內容視窗隨即開啟。

3. 如有必要，請根據您的需求指定一般工作設定。

4. 在**應用程式設定**部分中，指定用於儲存管理伺服器資料備份副本的資料夾路徑，設定備份防護密碼以及備份副本數量（如果需要）。

5. 點擊**儲存**以套用變更。

*管理伺服器資料備份*工作已配置。

將管理伺服器移動至其他裝置

如果您需要在新裝置上使用管理伺服器，您可以通過以下方式之一移動它：

- 將管理伺服器和資料庫伺服器移至新裝置（資料庫伺服器可以與管理伺服器一起安裝在新裝置上，也可以安裝在其他裝置上）。
- 將資料庫伺服器保留在以前的裝置上，僅將管理伺服器移動到新裝置上。

要將管理伺服器和資料庫伺服器移動到新裝置：

1. 在之前的裝置上，建立管理伺服器資料的備份。

   為此，您可以通過卡巴斯基安全管理中心網頁主控台執行資料備份工作或執行 klbackup 公用程式。

   > 如果您目前使用 SQL Server 作為管理伺服器的 DBMS，則可以將資料從 SQL Server 遷移到 MySQL 或 MariaDB DBMS。若要這麼做，請執行互動模式下的 klbackup 公用程式來建立資料備份。在備份和還原精靈的**備份設定**視窗中啟用**遷移到 MySQL/MariaDB 格式**選項。卡巴斯基安全管理中心將建立一個與 MySQL 和 MariaDB 相容的備份。之後，您可以將資料從備份還原到 MySQL 或 MariaDB。

   > 如果您想要將資料從 SQL Server 遷移到 Azure SQL DBMS，也可以啟用**移轉到 Azure 格式**選項。

2. 在之前的裝置上，中斷管理伺服器與網路的連線。

3. 選擇要在上面安裝管理伺服器的新裝置。確保所選裝置上的硬體和軟體符合管理伺服器、卡巴斯基安全管理中心網頁主控台和網路代理的要求。另外，檢查一下管理伺服器上使用的連接埠是否可用。

4. 為新裝置分配相同的位址。

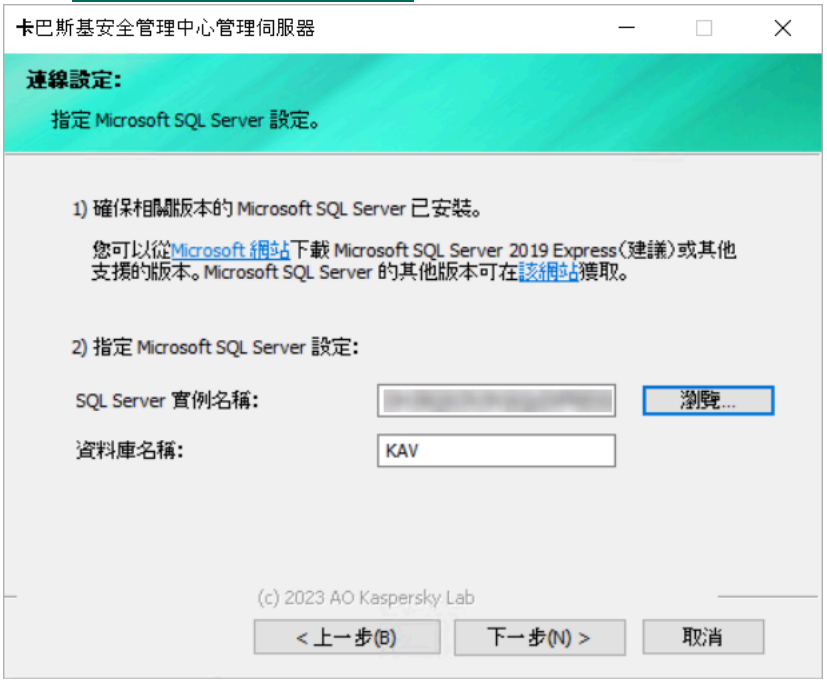
   可以為新管理伺服器指派 NetBIOS 名稱、FQDN 和靜態 IP 位址。這取決於部署網路代理時在網路代理安裝套件中設定的管理伺服器位址。或者，您可以使用確定網路代理連線到管理伺服器的連線位址（您可以使用 klnagchk 公用程式在受管理裝置上取得此位址）。

5. 如有需要，在其他裝置上，安裝管理伺服器將使用的資料庫管理系統 (DBMS)。

   資料庫可以與管理伺服器一起安裝在新裝置上，也可以安裝在其他裝置上。確保該裝置符合硬體和軟體要求。選擇 DBMS 時，請考慮管理伺服器涵蓋的裝置數量。

6. 在新裝置上執行管理伺服器安裝。

7. 在管理伺服器安裝過程中，配置資料庫伺服器連線設定。



Microsoft SQL Server 的連線設定視窗範例

根據所需放置資料庫伺服器的位置，執行以下操作之一：

- **將資料庫伺服器保留在先前裝置上**

  1. 點擊**SQL Server 實例名稱**欄位旁邊的**瀏覽**按鈕，然後在出現的清單中選擇之前的裝置名稱。
     請注意，先前裝置必須可用於連線新的管理伺服器。
  2. 在**資料庫名稱**欄位中輸入以前的資料庫名稱。

- **將資料庫伺服器移至另一個裝置**

  1. 點擊**瀏覽**欄位旁邊的**SQL Server 實例名稱**按鈕，然後在出現的清單中選擇裝置名稱。
  2. 在**資料庫名稱**欄位中輸入新資料庫名稱。
     請注意，新資料庫名稱必須與先前裝置中的資料庫名稱相符。資料庫的名稱必須相同，才能使用管理伺服器備份。預設資料庫名稱是 *KAV*。

8. 安裝完成後，使用 klbackup 公用程式在新裝置上還原管理伺服器資料。

   如果您在舊裝置和新裝置上使用 SQL Server 作為 DBMS，請注意新裝置上安裝的 SQL Server 版本必須與舊裝置上安裝的 SQL Server 版本相同或更高。否則，您將無法在新裝置上還原管理伺服器資料。

9. 開啟卡巴斯基安全管理中心網頁主控台然後連線到管理伺服器。

10. 驗證所有受管理裝置都已連線到管理伺服器。

11. 從之前的裝置中解除安裝管理伺服器和資料庫伺服器。

您也可以使用管理主控台將管理伺服器和資料庫伺服器移動到另一台裝置。

使用 klscmodchk 和 integrity_checker 實用程式檢查模組的完整性

卡巴斯基安全管理中心包含多個二進位模組，形式包括動態連結庫、可執行檔、設定檔和介面檔案。入侵者可以用包含惡意程式碼的其他檔案取代一個或多個可執行模組或應用程式檔案。為了防止模組和檔案替換，卡巴斯基安全管理中心使用 klscmodchk 和integrity_checker 實用程式提供元件完整性檢查。這些實用程式可檢查模組和檔案是否有未經授權的變更或損壞。如果模組或應用程式檔案的總和檢查碼不正確，則被視為已損壞。

klscmodchk 實用程式對以下卡巴斯基安全管理中心元件執行完整性檢查：

- 管理伺服器
- 網路代理
- 帶有清單檔案的管理主控台的管理外掛程式

integrity_checker 實用程式對以下卡巴斯基安全管理中心元件執行完整性檢查：

- 管理伺服器
- 網路代理
- 卡巴斯基安全管理中心網頁主控台

這兩個實用程式都根據 kl_file_integrity_manifest.xml 清單檔案檢查模組完整性，該檔案是卡巴斯基安全管理中心內建版本的一部分，位於安裝資料夾中。元件清單檔案包含的檔案的完整性對於卡巴斯基安全管理中心元件的正確運作非常重要。清單檔案本身的完整性也會得到檢查。

強烈建議不要修改 kl_file_integrity_manifest.xml 清單檔案，因為這將使數位簽章無效並導致完整性檢查失敗。

若要檢查卡巴斯基安全管理中心元件的完整性檢查，請執行下列命令之一：

- `$ klscmodchk [ 參數 ]`

  klscmodchk 實用程式使用 `--verbose` 參數啟動 integrity_checker 實用程式並檢查模組的完整性。

  klscmodchk 實用程式的參數：

  - `-logfile <log_file_path>`—指定磁碟上用於記錄的檔案的路徑。預設情況下，資訊被輸出到主控台。
  - `-chkplugins`—檢查已安裝的管理主控台管理外掛程式（包括清單檔案）的完整性。預設情況下，不檢查管理外掛程式。
  - `-verbose`—在完整性檢查期間輸出延伸資訊。

- `$ integrity_checker [ 參數 ] <manifest_file_path>`

  integrity_checker 實用程式的參數：

  - `--help`—顯示 integrity_checker 實用程式說明。
  - `--version`—顯示 integrity_checker 實用程式版本。
  - `--verbose`—顯示有關實用程式操作的資訊。執行完整性檢查時，在指令中使用此參數就足夠了。

每個清單檔案的檢查結果以以下格式顯示在清單檔案名稱旁邊：

- SUCCEEDED — 檔案完整性得到確認（回傳代碼 0）。
- FAILED — 檔案完整性未確認（非零回傳代碼）。

卡巴斯基安全管理中心網頁主控台初始設定

該部分敘述了安裝卡巴斯基安全管理中心 網頁主控台後，要執行初始設定必須採取的操作。

快速啟動精靈（卡巴斯基安全管理中心網頁主控台）

本節提供了管理伺服器快速啟動精靈的資訊。

> 該精靈需要網際網路存取。如果您的管理伺服器無法存取網際網路，我們建議您透過卡巴斯基安全管理中心網頁控制台界面手動執行精靈的所有步驟。

卡巴斯基安全管理中心允許您對構建集中式管理系統以實施網路安全威脅防護所需的最小設定集合進行調整。此功能就是使用快速啟動精靈來達成。當精靈執行時，您可以對應用程式做以下變更：

- 新增可自動佈署至管理群組內的裝置的金鑰檔案或啟動碼。
- 設定與卡巴斯基安全網路 (KSN) 的互動。如果您允許使用 KSN，則精靈會啟用外部 KSN 與裝置連線的 KSN 代理伺服器服務。

- 為管理伺服器和受管理應用程式的操作事件通知設定郵件傳送設定（成功的通知傳送需要訊息服務在管理伺服器和所有接收端裝置上執行）。
- 為工作站和伺服器建立防護政策，以及為受管理裝置階層的最上層群組建立惡意軟體掃描工作、更新下載工作和資料備份工作。

> 快速設定精靈僅為其**受管理裝置**資料夾不包含任何政策的應用程式建立政策。如果已經為受管理裝置階層的最上層群組建立相同名稱的工作，則快速啟動精靈不會建立同名工作。

在安裝管理伺服器後，在第一次連線時，應用程式自動提示您執行快速啟動精靈。您還可以在任意時刻手動啟動快速啟動精靈。

要手動啟動快速啟動精靈：

1. 在主功能表中，按一下管理伺服器名稱旁邊的設定圖示（  ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**一般**區段。
3. 點擊 **開始快速啟動精靈**。

精靈提示您執行管理伺服器初始化設定。遵照精靈的說明。使用**下一步**按鈕進行精靈。

步驟 1：指定網際網路連線設定

指定管理伺服器的網際網路存取設定。您必須設定網際網路存取權限，才能使用卡巴斯基安全網路並下載卡巴斯基安全管理中心病毒資料庫和受管理卡巴斯基應用程式的更新。

如果您要在連線到網際網路時使用代理伺服器，請啟用**使用代理伺服器**選項。如果啟用此選項，可將欄位用於輸入設定。為代理伺服器連線指定以下設定：

- **位址**

  卡巴斯基安全管理中心用於連線到網際網路的代理伺服器位址。

- **連接埠號**

  將建立卡巴斯基安全管理中心代理伺服器連線的埠號。

- **略過本機位址的代理伺服器**

  將不會使用代理伺服器連線本機網路的裝置。

- **代理伺服器身分驗證**

  如果選取該方塊，您可以在輸入欄位中為代理伺服器身分驗證指定憑證。
  如果選取**使用代理伺服器**核取方塊，則可使用該輸入欄位。

- **使用者名稱**

  用來建立前往 Proxy 伺服器之連線的使用者帳戶（若選取了**代理伺服器身分驗證**核取方塊，則此欄位可用）。

- **密碼**

  其帳戶用來建立 Proxy 伺服器連線的使用者所設定的密碼（若選取了**代理伺服器身分驗證**核取方塊，則此欄位可用）。

  若要檢視輸入的密碼，依您所需的時間長度點擊並按住**顯示**按鈕。

您可以稍後設定網際網路存取，單獨從速啟動精靈執行。

步驟 2：下載所需的更新

所需更新被從 Kaspersky 伺服器自動下載。

步驟 3：選擇要防護的資產

選取您網路中使用的防護區域和作業系統。當您選取這些選項，您就在 Kaspersky 伺服器上指定了應用程式管理外掛程式的篩選和分發套件，您可下載此程式以在網路中的用戶端裝置上安裝。

選取選項：

- **地區**

  您可選取以下防護範圍：

  - **工作站**。若您要在網路中防護工作站，請選取此選項。依預設會選定此選項。
  - **檔案伺服器和儲存**。若要防護網路中的檔案伺服器，請選取此選項。
  - **行動裝置**。若要防護公司或公司員工擁有的行動裝置，請選取此選項。若您選取此選項，但您未透過行動裝置管理功能提供授權，則會出現一則訊息，告知您透過行動裝置管理功能提供授權的必要性。若您沒有提供授權，則您無法使用行動裝置功能。
  - **虛擬化**。若您要防護網路中的虛擬機，請選取此選項。
  - **Kaspersky 垃圾郵件防護**。若要防護組織中的郵件伺服器不要受到垃圾郵件、詐騙和惡意郵件攻擊，請選取此選項。
  - **嵌入式系統**。如果您想要防護基於 Windows 的嵌入式系統，例如自動櫃員機 (ATM)，則選擇此選項。
  - **產業網路**。如果您想要監控整個產業網路的資料並從受卡巴斯基應用程式防護的網路端點進行監控，則選擇此選項。
  - **產業端點**。若您要防護產業網路中的單個節點，請選取此選項。

- **作業系統**

  您可以選取以下平台：

  - Microsoft Windows
  - macOS
  - Android
  - Linux
  - 其他

  如需有關受支援的作業系統的資訊，請參閱卡巴斯基安全管理中心網頁主控台的硬體和軟體需求。

您可以稍後從可用套件清單中選擇卡巴斯基應用程式套件，單獨從快速啟動精靈執行。為了簡化搜尋所需套件的作業，您可以使用各種條件篩選可用套件清單。

步驟 4：在解決方案中選取加密方式

只有在您選取了**工作站**作為防護範圍時，才會顯示**加密進行中**視窗。

Kaspersky Endpoint Security for Windows 包含適用於儲存在 Windows 型用戶端裝置上資訊的加密工具。這些加密工具包含具有以 256 位元或 56 位元金鑰長度實作的進階加密標準 (AES) 的加密工具。

下載和使用具有 256 位元金鑰長度的分發套件必須在符合適用之法律和規定下執行。若要下載符合您組織需要的 Kaspersky Endpoint Security for Windows 分發套件，請諮詢組織用戶端裝置所在的國家或地區的法務部門。

在**加密進行中**視窗中，選取以下加密類型之一：

- 輕度加密。此加密類型會使用 56 位元的金鑰長度。
- 強加密。此加密類型會使用 256 位元的金鑰長度。

您可以稍後為 Kaspersky Endpoint Security for Windows 選擇具有所需加密類型的分發套件，單獨從快速啟動精靈執行。

步驟 5：為受管理應用程式配置外掛程式安裝

選取要安裝且適用於受管理應用程式的外掛程式。系統會顯示 Kaspersky 伺服器上的外掛程式清單。會根據在精靈的上一步選取的選項篩選清單。依預設，完整清單包含所有語言的外掛程式。若僅顯示特定語言的外掛程式，請使用篩選程式。

外掛程式清單包含以下欄：

- **要保護安全的區域**

  選定的要保護的區域顯示在此欄中。

- **類型**

  外掛程式類型顯示在此欄中。

- **名稱**

  您在先前步驟中已選取的外掛程式會依存在防護範圍和平台中，系統會選取這些程式。

- **版本**

  清單包含放在 Kaspersky 伺服器中所有版本的外掛程式。依預設會選取最新版本的外掛程式。

- **最新版本**

  該欄表示外掛程式版本是否為最新。如果顯示為**true** 值，則對應的外掛程式是最新版本。如果顯示**false** 值，則對應的外掛程式版本更高。

- **作業系統**

  此欄顯示外掛程式作業係統。

- **語言**

  依預設，外掛程式的本地化語言會由您在安裝時選取的卡巴斯基安全管理中心語言來決定。您可在**顯示管理主控台中文化語言或**下拉清單指定其他語言。

選取外掛程式後，點擊**下一步**開始安裝。

你可以手動為卡巴斯基應用程式安裝管理外掛程式，單獨從快速啟動精靈執行。

快速啟動精靈會自動安裝選定的外掛程式。若要安裝一些外掛程式，您必須接受 EULA 條款。請閱讀 EULA 條款，選取**我同意使用卡巴斯基安全網路**核取方塊並點擊**安裝**按鈕。若您不接受 EULA 條款，則不會安裝外掛程式。

安裝所有選定的外掛程式後，"快速啟動精靈"會自動將您帶到下一步。

步驟 6：下載分發套件並建立安裝套件

選取要下載的分發套件。

受管理應用程式的發佈，可能需要安裝卡巴斯基安全管理中心特定的最低版本。

選取 Kaspersky Endpoint Security for Windows 的加密類型後，會顯示兩種加密類型的分發套件清單。清單中會選取有所選加密類型的分發套件。您可以選取任何一種加密類型的分發套件。分發套件語言會對應卡巴斯基安全管理中心語言。若適用於卡巴斯基安全管理中心的 Kaspersky Endpoint Security for Windows 分發套件不存在該語言，則會選取英文版分發套件。

若要完成下載某些分發套件，您必須接受 EULA。當您點擊**同意**按鈕時，顯示 EULA 條款。若要繼續至精靈的下個步驟，您必須接受 EULA 的條款與條件，以及 Kaspersky 隱私政策的條款與條件。若您不接受條款與條件，系統會取消套件的下載程序。

接受 EULA 與 Kaspersky Privacy 隱私政策的條款與條件後，會繼續分發套件下載程序。之後您可以使用安裝套件在用戶端裝置上佈署 Kaspersky 應用程式。

您可以稍後下載分發套件並建立安裝套件，單獨從快速啟動精靈執行。

步驟 7。設定卡巴斯基安全網路

指定設定以轉發卡巴斯基安全管理中心操作資訊到卡巴斯基安全網路知識庫。

您可以選取以下其中一個方法：

- **我同意使用卡巴斯基安全網路**

  安裝在用戶端裝置上的卡巴斯基安全管理中心與受管理應用程式會自動傳輸其作業詳情至卡巴斯基安全網路。參與卡巴斯基安全網路確保了包含病毒和其他威脅的資料庫的快速更新，該資料庫確保了對緊急安全威脅的快速回應。

- **我不同意使用卡巴斯基安全網路**

  卡巴斯基安全管理中心和受管理應用程式將不會提供資訊至卡巴斯基安全網路。

  若您選取此選項，則會停用卡巴斯基安全網路。

你可以稍後設定到卡巴斯基安全網路 (KSN) 的存取，單獨從快速啟動精靈執行。

步驟 8：選取應用程式啟動方式

選取以下其中一個卡巴斯基安全管理中心啟動選項：

- **透過輸入您的啟動碼**

  *啟動碼*是一串由 20 個字元數字組成的唯一序列。您可以輸入啟動碼來新增一個金鑰來啟動卡巴斯基安全管理中心。您會透過您在購買卡巴斯基安全管理中心後指定的電子郵件地址收到啟動碼。

  若要使用啟動碼啟動應用程式，您需要網際網路來建立與 Kaspersky 啟動伺服器的連線。

  若您已選取此啟動選項，就能啟用**自動分發產品授權金鑰到受管理裝置**選項。

  若啟用此選項，授權金鑰將會自動佈署至受管理裝置。

  若停用此選項，您可以稍後在管理主控台樹狀目錄的 **Kaspersky** 產品授權節點中，將產品授權金鑰佈署至受管理裝置。

- **透過指定金鑰檔案**

  *金鑰檔案*是 Kaspersky 提供的 .key 副檔名的檔案。金鑰檔案被用來啟動應用程式。

  金鑰檔案的取得方法請參閱關於金鑰檔案章節。

  若使用金鑰檔案啟動程式，您無需連線至 Kaspersky 啟動伺服器。

  若您已選取此啟動選項，就能啟用**自動分發產品授權金鑰到受管理裝置**選項。

  若啟用此選項，授權金鑰將會自動佈署至受管理裝置。

  若停用此選項，您可以稍後在管理主控台樹狀目錄的 **Kaspersky** 產品授權節點中，將產品授權金鑰佈署至受管理裝置。

- **透過高推遲應用程式啟動**

  應用程式將使用基本功能操作，沒有行動裝置管理也沒有弱點和修補程式管理。

如果您選擇延遲啟動應用程式，您可以透過選取**操作 → 產品授權**來隨時新增產品授權金鑰。

當使用從付費 AMI 佈署的卡巴斯基安全管理中心時，或者對於基於使用量的按月付費 SKU，您無法指定金鑰檔案或輸入碼。

步驟 9：指定協力廠商更新管理設定

如果您沒有弱點和修補程式管理產品授權，並且*弱點掃描和所需更新*工作已存在，則此步驟不會顯示。

對於協力廠商軟體更新，請選取以下選項之一：

- **搜尋必要更新**

  如果您沒有*弱點掃描和所需更新*工作，系統會自動建立該工作。

  預設情況下已選取此選項。

- **尋找與安裝需要的更新**

  若您沒有，系統會自動建立*弱點掃描和所需更新*和*安裝所需更新並修復弱點*的工作。

  此選項僅在有弱點和修補程式管理產品授權下才可使用。

對於 Windows Update 更新，請選擇以下選項之一：

- **使用與更新網域政策中定義的來源**

  用戶端裝置將會根據網域政策設定下載 Windows Update 更新。若您沒有，會自動建立網路代理政策。

- **使用管理伺服器作為 WSUS 伺服器**

  用戶端裝置將會從管理伺服器下載 Windows Update 更新。若您沒有，會自動建立*執行 Windows Update 同步*工作和網路代理政策。

  此選項僅在有弱點和修補程式管理產品授權下才可使用。

您可以從快速啟動精靈單獨建立*尋找弱點和所需更新*和*安裝所需更新並修復弱點*工作。若要使用管理伺服器作為 WSUS 伺服器，請建立*執行 Windows Update 同步*工作，然後選取網路代理政策中的**使用管理伺服器作為 WSUS 伺服器**選項。

步驟 10。建立基本的網路保護設定

您可以檢查建立的政策和工作清單。

等待政策和工作完成建立，然後轉到精靈的下一步。

您可以稍後建立所需的工作和政策，單獨從快速啟動精靈執行。

步驟 11：設定電子郵件通知

設定如何傳遞 Kaspersky 應用程式在用戶端裝置上操作期間記錄的事件通知。這些設定將被用作應用程式政策的預設設定。

要配置發生在 Kaspersky 應用程式上的事件的通知傳送，使用以下設定：

- **收件者（電子郵件信箱）**

  應用程式將給其傳送通知的使用者的郵件位址。您可以輸入一個或更多位址；如果您輸入多個位址，使用分號分隔。

- **SMTP 伺服器位址**

  您組織郵件伺服器的位址。

  如果您輸入多個位址，使用分號分隔。您可以使用以下參數：

  - IPv4 或 IPv6 位址
  - 裝置的 Windows 網路名稱（NetBIOS 名稱）
  - SMTP 伺服器的 DNS 名稱

- **SMTP 伺服器連接埠**

  SMTP 伺服器的通訊埠號。如果您使用多部 SMTP 伺服器，則會透過指定的通訊連接埠與它們建立連線。預設埠號為 25。

- **使用 ESMTP 身分驗證**

  啟用 ESMTP 身分驗證支援。當選取了該核取方塊時，您可以在**使用者名稱**和**密碼**欄位指定 ESMTP 身分驗證設定。預設情況下已清空此方塊。

- **使用 TLS**

  您可以用 SMTP 伺服器指定連線的 TLS 設定：

  - **不使用 TLS**

    如果您想停用電子郵件訊息加密，您可以選取此選項。

  - **如果受 SMTP 伺服器支援則使用 TLS**

    如果要使用 TLS 連線到 SMTP 伺服器，則可以選取此選項。如果 SMTP 伺服器不支援 TLS，管理伺服器將不使用 TLS 連線 SMTP 伺服器。

  - **始終使用 TLS，檢查伺服器憑證是否有效**

    如果要使用 TLS 身分驗證設定，則可以選取此選項。如果 SMTP 伺服器不支援 TLS，管理伺服器將無法連線 SMTP 伺服器。

    我們建議您使用此選項以更好地防護與 SMTP 伺服器的連線。如果選取此選項，則可以為 TLS 連線設定身分驗證設定。

    如果您選取**始終使用 TLS，檢查伺服器憑證是否有效**值，您可以指定用於驗證 SMTP 伺服器的憑證，並選取是要透過任何版本的 TLS，還是僅透過 TLS 1.2 或更高版本啟用通訊。此外，您可以指定在 SMTP 伺服器上進行用戶端身分驗證的憑證。

  您可以透過點擊**指定憑證**連結指定 TLS 連線的憑證：

  - 瀏覽 SMTP 伺服器憑證檔案：

    您可以從受信任的憑證頒發機構接收帶有憑證清單的檔案，然後將該檔案上傳到管理伺服器。卡巴斯基安全管理中心會檢查 SMTP 伺服器的憑證是否也由受信任的憑證頒發機構簽署。如果未從受信任的憑證頒發機構收到 SMTP 伺服器的憑證，卡巴斯基安全管理中心將無法連線到 SMTP 伺服器。

  - 瀏覽用戶端憑證檔案：

    您可以使用從任何來源（例如，從任何受信任的憑證頒發機構）收到的憑證。您必須使用以下憑證類型之一指定憑證及其私密金鑰：

    - X-509 憑證：

      您必須指定一個帶有憑證的檔案和一個帶有私密金鑰的檔案。這兩個檔案互不相依，檔案的載入順序並不重要。當同時載入兩個檔案時，您必須指定用於解碼私密金鑰的密碼。如果未編碼私密金鑰未編碼，則密碼可以為空值。

    - pkcs12 容器：

      您必須上傳包含憑證及其私密金鑰的單一檔案。載入檔案後，您必須指定用於解碼私密金鑰的密碼。如果未編碼私密金鑰未編碼，則密碼可以為空值。

您可以透過點擊**傳送測試訊息**按鈕測試新郵件通知設定。

您可以稍後設定事件通知，單獨從快速啟動精靈執行。

步驟 12。執行網路輪詢

管理伺服器執行初始化輪詢。輪詢中，進度條被顯示。當輪詢完成時，**檢視偵測到的裝置**連結變得可用。您可以點擊該連結檢視被管理伺服器偵測到的網路裝置。要返回快速設定精靈，點擊 **Escape** 鍵。

您可以稍後輪詢您的網路，單獨從快速啟動精靈這行。使用卡巴斯基安全管理中心網頁主控台配置 Windows 網域、Active Directory、IP 範圍和IPv6 網絡 的輪詢。

步驟 13：關閉快速啟動精靈

在快速設定精靈完成頁面，如果您想啟動自動安裝病毒防護應用程式或網路代理到您的網路，請選取**執行防護佈署精靈**核取方塊。

要關閉精靈，請點擊**完成**按鈕。

連線漫遊裝置

本節說明如何將漫遊裝置（即位於主網路外的受管理裝置）連線到管理伺服器。

情境：透過連線閘道連線辦公室外的裝置

此方案說明如何將位於主網路外的受管理裝置連線到管理伺服器。

先決條件

該情境需有以下先決條件：

- 非警戒區域 (DMZ) 會在組織的網路中組織。
- 卡巴斯基安全管理中心管理伺服器已佈署在公司網路上。

階段

此情境分階段進行：

1. **在 DMZ 中選取用戶端裝置**

   此裝置將作為連線閘道使用。您選取的裝置必須滿足連線閘道的要求。

2. **以連線閘道角色安裝網路代理**

   我們建議您使用本機安裝在所選裝置上安裝網路代理。

   預設情況下，安裝檔案位於：\\<伺服器名稱>\KLSHARE\PkgInst\NetAgent_<版本編號>

在網路代理安裝精靈的**連線閘道**視窗中，選取**使用網路代理作為 DMZ 連線閘道**。此模式同時啟動連線閘道角色，並通知網路代理等待來自管理伺服器的連線，而不是建立與管理伺服器的連線。

或者，您可以在 Linux 裝置上安裝網路代理並將網路代理設定為連線閘道使用，但是要注意在 Linux 裝置上執行的網路代理限制清單。

3 允許連線閘道上防火牆中的連線

為確保管理伺服器實際上可以連線到 DMZ 中的連線閘道，請允許連線到管理伺服器和連線閘道間所有防火牆中的 TCP 連接埠 13000。

如果連線閘道在網際網路上沒有真實 IP 地址，而是位於網路位址轉換 (NAT) 後面，請配置規則以透過 NAT 轉發連線。

4 建立外部裝置的管理群組

在**受管理裝置**群組下建立新群組。此新群組將包含外部受管理裝置。

5 將連線閘道連到管理伺服器

您配置的連線閘道正在等待來自管理伺服器的連線。但是，管理伺服器未在受管理裝置中列出具有連線閘道的裝置。這是因為連線閘道尚未嘗試建立與管理伺服器的連線。因此，您需要一個特殊程序來確保管理伺服器啟動到連線閘道的連線。

請執行下列操作：

1. 將連線閘道新增為發佈點。
2. 將連線閘道從**未配置的裝置**群組移動到您為外部裝置建立的群組。

連線閘道已連線並配置。

6 將外部桌上型裝置連線到管理伺服器

通常，外部桌上型裝置不會在週邊環境中移動。因此，在安裝網路代理時，需要配置它們以透過閘道連線到管理伺服器。

7 設定外部桌上型裝置的更新

如果將安全應用程式的更新設定為從管理伺服器下載，則外部裝置將透過連線閘道下載更新。這有兩個缺點：

- 這是不必要的流量，會佔用公司的網際網路通訊頻道的頻寬。
- 這不一定是獲取更新的最快方法。對於外部裝置來說，從卡巴斯基更新伺服器接收更新可能會更便宜、更快捷。

請執行下列操作：

1. 將所有外部裝置移至您先前建立的單獨管理群組。
2. 從更新工作中排除具有外部裝置的群組。
3. 使用外部裝置為該群組建立單獨的更新工作。

8 將行動的筆記型電腦連線到管理伺服器

行動的筆記型電腦有時位於網路內部，而其他時間位於網路外部。為了有效管理，您需要根據其位置以不同的方式連線到管理伺服器。為了有效利用流量，他們還需要根據所在位置從不同來源接收更新。

您需要為漫遊使用者配置規則：連線設定檔和網路位置描述。每個規則都根據其位置定義了行動筆記型電腦必須連線到的管理伺服器實例，以及必須從中接收更新的管理伺服器實例。

情境：通過 DMZ 中的從屬管理伺服器連線漫遊裝置

如果要將位於主網路外的受管理裝置連線到管理伺服器，可以使用位於隔離區 (DMZ) 中的從屬管理伺服器來實現。

先決條件

在您開始之前，確保您已做了如下：

- DMZ 會在組織的網路中組織。
- 卡巴斯基安全管理中心管理伺服器已佈署在組織的內部網路上。

階段

此情境分階段進行：

1. **在 DMZ 中選取用戶端裝置**

   在 DMZ 中，選擇將用作從屬管理伺服器的用戶端裝置。

2. **安裝卡巴斯基安全管理中心管理伺服器**

   在此用戶端裝置上安裝卡巴斯基安全管理中心管理伺服器。

3. **建立管理伺服器階層**

   如果將從屬管理伺服器放置在 DMZ 中，則從屬管理伺服器必須接收來自主管理伺服器的連線。為此，可以新增新管理伺服器作為從屬管理伺服器，以便主管理伺服器透過連接埠 13000 連線到從屬管理伺服器。當組合兩個管理伺服器到一個層級，確保連接埠 13299 在兩個管理伺服器上都可以存取。卡巴斯基安全管理中心網頁主控台透過連接埠 13299 連線到管理伺服器。

4. **將不在辦公室的受管理裝置連線到從屬管理伺服器。**

   您可以將不在辦公室的裝置連線到 DMZ 中的管理伺服器，其連線方式與在管理伺服器和位於主網路中的受管理裝置之間建立連線的方式相同。不在辦公室的受管理裝置通過連線埠 13000 發起連線。

關於連線辦公室外的裝置

部分受管理裝置永遠位在主網路之外（例如，地區分公司中的裝置；資訊站、ATM 和安裝在各個銷售點的終端機；員工居家辦公的裝置）。有些裝置不時在外圍移動（例如，存取地區分公司或客戶辦公室的使用者筆記型電腦）。

您仍然需要監控和管理漫遊裝置受保護的情況，接收其保護狀態的實際資訊，並使裝置上的安全應用程式保持最新狀態。這是必要措施，因為如果這樣的裝置在遠離主網路時受到威脅，一旦它們連到主網路，就可能成為傳播威脅的平台。要將辦公室外的裝置連線到管理伺服器，可以使用兩種方法：

- 非警戒區 (DMZ) 中的連線閘道

  請參閱資料流量方案：LAN 上的管理伺服器、網際網路上的受管理裝置、正在使用的連線閘道

- DMZ 中的管理伺服器

  請參閱資料流量方案：DMZ 中的管理伺服器、網際網路上的受管理裝置。

DMZ 中的連線閘道

將辦公室外的裝置連線到管理伺服器的推薦方法是在組織的網路中組織 DMZ，並在 DMZ 中安裝連線閘道。外部裝置將連線到連線閘道，網路內部的管理伺服器將透過連線閘道啟動與裝置的連線。

與其他方法相比，此方法更安全：

- 您不需要從網路外部開啟對管理伺服器的存取。
- 受損的連線閘道不會對網路裝置的安全構成高風險。連線閘道本身實際上並不管理任何東西，也不會建立任何連線。

而且，連線閘道不需要很多硬體資源。

但是，此方法的設定過程較為複雜：

- 若要使裝置作為 DMZ 中的連線閘道，您需要安裝網路代理並以特定方式將其連線到管理伺服器。
- 在所有情況下，您將無法使用相同的位址連線到管理伺服器。從週邊以外，您不僅需要使用其他位址（連線閘道位址），還需要使用其他連線模式：透過連線閘道。
- 您還需要為不同位置的筆記型電腦定義不同的連線設定。

要將連線閘道新增到先前配置的網路：

1. 以連線閘道模式安裝網路代理。
2. 在要連線到新增的連線閘道的裝置上重新安裝網路代理。

DMZ 中的管理伺服器

另一種方法是在 DMZ 中安裝一個管理伺服器。

此配置不如其他方法安全。在這種情況下，要管理外部筆記型電腦，管理伺服器必須接受來自網際網路上任何位址的連線。它仍然將管理內部網路中的所有裝置，但會透過 DMZ 進行管理。因此，儘管發生此類事件的可能性很小，但有風險的伺服器可能會造成巨大的損失。

如果 DMZ 中的管理伺服器不管理內部網路中的裝置，則風險將大大降低。例如，服務提供商可以使用這種設定來管理客戶的裝置。

在以下情況下，您可能要使用此方法：

- 如果您熟悉安裝和配置管理伺服器，並且不想執行其他過程來安裝和設定連線閘道。
- 如果您需要管理更多裝置。管理伺服器的最大容量為 100,000 台裝置，而連線閘道最多可支援 10,000 台裝置。

此解決方案也可能有困難：

- 管理伺服器需要更多的硬體資源和一個資料庫。
- 有關裝置的資訊將儲存在兩個不相關的資料庫中（用於網路內的管理伺服器，另一個用於 DMZ 中的資料庫），這使監控變得複雜。
- 若要管理所有裝置，則需要將管理伺服器連線到一個階層中，使得監控和管理變得複雜。從屬管理伺服器執行個體對管理群組的可能架構施加了限制。您必須決定如何以及將哪些工作和政策分配給從屬管理伺服器執行個體。
- 配置外部裝置以從外部使用 DMZ 中的管理伺服器並從內部使用主管理伺服器，並不比僅設定它們透過閘道使用條件式連線簡單。
- 高安全風險。受到破壞的管理伺服器實例可以更輕鬆地破壞其受管理的筆記型電腦。如果發生這種情況，駭客只需要等待其中一台筆記本電腦返回公司網路，即可繼續對區域網路展開攻擊。

將外部桌上型裝置連線到管理伺服器

永遠位在主網路之外的桌上型裝置（例如，地區分公司中的裝置；資訊站、ATM 和安裝在各個銷售點的終端機；員工居家辦公的裝置）不能直接連線到管理伺服器。它們必須透過安裝在非軍事區 (DMZ) 中的連線閘道連線到管理伺服器。在這些裝置上安裝網路代理時，將進行此設定。

要將外部桌上型裝置連線到管理伺服器，請執行以下操作：

1. 為網路代理建立一個新的安裝套件。
2. 開啟已建立的安裝套件屬性，轉到**設定 → 進階**，然後選取**透過使用連線閘道連線到管理伺服器**選項。

   透過使用連線閘道連線到管理伺服器設定與**使用網路代理作為 DMZ 連線閘道**設定不相容。您不能同時啟用這兩個設定。

3. 在**連線閘道位址**欄位中，指定連線閘道的公共位址。

   如果連線閘道位於網路位址轉換 (NAT) 後面並且沒有自己的公用位址，請配置 NAT 閘道規則以將連線從公用位址轉發到連線閘道的內部位址。

4. 建立以已建立安裝套件為基礎的獨立安裝套件。
5. 透過電子方式或在卸除式磁碟機上將獨立安裝套件傳輸至目標裝置。
6. 從獨立安裝套件安裝網路代理。

外部桌上型裝置已連線到管理伺服器。

關於漫遊使用者的連線設定檔

可攜式電腦（也叫"裝置"）的漫遊使用者需要變更連線到管理伺服器的方法或者根據目前裝置在企業網路中的位置在管理伺服器之間進行轉換。

連線設定檔僅支援執行 Windows 和 macOS 的裝置。

使用單一管理伺服器的不同位址

網路代理裝置從組織網路或內部網可以連線到管理伺服器。該情況可能需要網路代理使用不同的位址以連線到管理伺服器：對於網際網路連線的外部管理伺服器位址和對於內部網路連線的內部管理伺服器位址。

為此，請在網路代理政策內容中新增一個用於從網際網路連線到管理伺服器的設定檔（在**應用程式設定→連線→連線設定檔→管理伺服器連線設定檔**部分）。在設定檔建立視窗中，停用**僅用來接收更新**選項並確保選取**在此設定檔中指定的管理伺服器設定同步連線設定**選項。如果您使用連線閘道存取管理伺服器（例如，在"網際網路存取：DMZ 中作為連線閘道的網路代理"部分敘述的卡巴斯基安全管理中心設定中），您必須在連線設定檔的對應欄位指定連線閘道位址。

根據目前網路在管理伺服器之間進行轉換

如果組織有帶有多個管理伺服器的多個辦公室，並且一些網路代理裝置在期間進行移動，您需要網路代理連線到裝置所在的本機網路中的管理伺服器。

此種情況下，為每個辦公室在網路代理政策內容中建立連線管理伺服器的設定檔，除了歸屬管理伺服器所在的主辦公室。在連線設定檔中指定管理伺服器位址，並啟用或停用**僅用來接收更新**選項：

- 在使用本機伺服器下載更新時，如果您需要網路代理與歸屬管理伺服器同步，則選中此選項。
- 如果網路代理必須被本機管理伺服器完全管理，則停用此選項。

此後，您必須設定轉換到新建立的設定檔的條件：每個辦公室至少一個條件，除了歸屬辦公室。每個條件的目的包括辦公室網路環境項目的偵測。如果條件是真，對應設定檔被啟動。如果沒有條件是真，網路代理轉換到歸屬管理伺服器。

為漫遊使用者建立連線設定檔

管理伺服器連線設定檔僅在執行 Windows 和 macOS 的裝置上可用。

若要為漫遊使用者建立網路代理連線至管理伺服器的連線設定檔，請執行以下操作：

1. 如果要為一組受管理裝置建立連線設定檔，請開啟該群組的網路代理政策。為此，請執行以下操作：

   a. 在主功能表中，轉至 **裝置 → 政策和設定檔**。

   b. 點擊目前路徑連接。

   c. 在開啟的視窗中，選擇所需的管理群組。
   之後，目前路徑被變更。

   d. 為受管理裝置群組新增網路代理政策。如果您已經建立它，請點擊網路代理政策名稱以開啟政策內容。

2. 如果要為特定受管理裝置建立連線設定檔，請執行以下操作：

   a. 在主功能表中，轉至 **裝置 → 受管理裝置**。

   b. 點擊受管理裝置的名稱。

   c. 在開啟的受管理裝置內容視窗中，轉至**應用程式**頁簽。

   d. 點擊僅適用於選定受管理裝置的網路代理政策的名稱。

3. 在開啟的內容視窗中，轉到**應用程式設定→連線→連線設定檔。**

4. 在**管理伺服器連線設定檔**區域中，點擊**新增**按鈕。

   預設下，連線設定檔清單包含<離線模式>和<歸屬管理伺服器>設定檔。您不能編輯或刪除設定檔。

   <離線模式>設定檔不指定任何伺服器以連線。因此，網路代理，當切換到該設定檔時，當用戶端裝置上的應用程式工作在漫遊政策下時不試圖連線到任何管理伺服器。如果裝置與網路斷開連線，可以使用<離線模式>設定檔。

   <歸屬管理伺服器>設定檔指定在網路代理安裝過程中管理伺服器的連線。當裝置在外部網路中執行了一段時間後重新連線到管理伺服器時，<歸屬管理伺服器>設定檔被套用。

5. 在開啟的**配置設定檔**視窗中，配置連線設定檔：

   - **設定檔名稱**

     在該輸入欄位中，您可以檢視或變更連線設定檔名稱。

   - **管理伺服器位址**

     用戶端裝置在設定檔啟動期間必須連線的管理伺服器位址。

   - **連接埠號**

     用於連線的埠號。

   - **SSL 連接埠**

     使用 SSL 協定時的埠號。

   - **使用 SSL 連線**

     如果啟用此選項，則使用 SSL 協定透過安全埠建立連線。

     預設情況下已啟用該選項。我們建議您不要停用此選項，以便您的連線保持安全。

   - 如果您要在連線到網際網路時使用代理伺服器，選取**使用代理伺服器**選項。如果選取此選項，可將欄位用於輸入設定。為代理伺服器連線指定以下設定：

     - **位址**

       卡巴斯基安全管理中心用於連線到網際網路的代理伺服器位址。

     - **連接埠號**

       將建立卡巴斯基安全管理中心代理伺服器連線的埠號。

     - **代理伺服器身分驗證**

       如果選取該方塊，您可以在輸入欄位中為代理伺服器身分驗證指定憑證。

- **使用者名稱**

  用來建立前往 Proxy 伺服器之連線的使用者帳戶（若選取了**代理伺服器身分驗證**核取方塊，則此欄位可用）。

- **密碼**

  其帳戶用來建立 Proxy 伺服器連線的使用者所設定的密碼（若選取了**代理伺服器身分驗證**核取方塊，則此欄位可用）。

  若要檢視輸入的密碼，依您所需的時間長度點擊並按住**顯示**按鈕。

- **連線閘道位址**

  透過用戶端裝置連線至管理伺服器的閘道位址。

- **當管理伺服器不可用時啟用漫遊模式**

  選取該核取方塊允許用戶端裝置上安裝的應用程式在在不可使用管理伺服器進行的任何離線嘗試時，以漫遊模式使用政策設定檔和漫遊政策。如果沒有為應用程式定義漫遊政策，則使用啟動政策。

  如果停用此選項，則應用程式將使用已啟動的政策。

  預設情況下已清空此方塊。

- **僅用來接收更新**

  如果啟用此選項，則該設定檔將僅被用戶端裝置上安裝的應用程式用來下載更新。對於其他操作，程式將使用在網路代理安裝過程中定義的初始連線設定連線管理伺服器。

  預設情況下已啟用該選項。

- **在此設定檔中同步連線設定和管理伺服器設定**

  如果停用此選項，網路代理將使用設定檔屬性中指定的設定連線至管理伺服器。

  如果停用此選項，網路代理將使用安裝期間已指定的原始設定連線至管理伺服器。

  如果停用**僅用來接收更新**選項，則此選項可用。

  預設情況下已停用該選項。

程式將為漫遊使用者建立一個用於將網路代理連線至管理伺服器的設定檔。當使用此設定檔將網路代理連線至管理伺服器後，用戶端裝置上安裝的應用程式將使用漫遊模式裝置的政策，或漫遊政策。

關於將網路代理切換到其他管理服務器

如果變更了下列網路設定，卡巴斯基安全管理中心允許您將用戶端裝置網路代理轉換至其他管理伺服器：

- **DHCP 伺服器位址條件** — 網路 Dynamic Host Configuration Protocol (DHCP) 伺服器的 IP 位址已變更。
- **預設連線閘道位址條件** — 主要網路閘道的位址已變更。

- **DNS 網域條件** – 子網路的 DNS 後置詞已變更。
- **DNS 伺服器位址條件** – 網路 DNS 伺服器的 IP 位址已變更。
- **WINS 伺服器位址條件** – 網路 WINS 伺服器的 IP 位址已變更。此設定僅適用於執行 Windows 的裝置。
- **名稱可解析性條件** – 用戶端裝置的 DNS 或 NetBIOS 名稱已更改。
- **子網路條件** – 可變更子網路位址和遮罩。
- **Windows 網域可存取性條件** – 可變更用戶端裝置連線到的 Windows 網域的狀態。此設定僅適用於執行 Windows 的裝置。
- **SSL 連線位址可存取性條件** – 用戶端裝置可以或無法（取決於您選取的選項）與指定伺服器（名稱：連接埠）建立 SSL 連線。對於每個伺服器，您還可以指定 SSL 憑證。在這種情況下，除了檢查 SSL 連線的功能之外，網路代理還會驗證伺服器憑證。如果憑證不相符，則連線會失敗。

僅執行 Windows 或 macOS 的裝置上安裝的網路代理支援此功能。

網路代理連線至管理伺服器的初始設定在安裝網路代理時定義。此後，如果建立了將網路代理轉換至其他管理伺服器的規則，網路代理將以下列方式回應網路設定的變更：

- 如果網路設定符合已建立的規則之一，網路代理將連線至該規則中指定的管理伺服器。如果該規則中已經啟用漫遊轉換政策，用戶端裝置上的應用程式將轉換至漫遊政策。
- 如果未套用任何規則，網路代理將回溯至安裝過程中指定的管理伺服器連線預設設定。用戶端裝置上安裝的應用程式將回溯至活動政策。
- 如果無法存取管理伺服器，網路代理將使用使用者漫遊政策。

網路代理只會在網路代理政策設定中的**當管理伺服器不可用時啟用漫遊模式**選項啟用時才會切換至漫遊政策。

網路代理連線至管理伺服器的設定儲存在連線設定檔中。在連線設定檔中，您可以建立將用戶端裝置轉換至漫遊政策的規則，並可對設定檔進行設定，使其僅可用於下載更新。

依據網路位置建立網路代理轉換規則

根據網路位置切換網路代理僅在執行 Windows 和 macOS 的裝置上可用。

若要建立一個當網路設定改變時將網路代理從一個管理伺服器轉換至另一個的規則，請執行以下操作：

1. 如果要為一組受管理裝置建立規則，請開啟該群組的網路代理政策。為此，請執行以下操作：

   a. 在主功能表中，轉至 **裝置 → 政策和設定檔**。

   b. 點擊目前路徑連接。

   c. 在開啟的視窗中，選擇所需的管理群組。
   之後，目前路徑被變更。

   d. 為受管理裝置群組新增網路代理政策。如果您已經建立它，請點擊網路代理政策名稱以開啟政策內容。

2. 如果要為特定受管理裝置建立規則，請執行以下操作：

   a. 在主功能表中，轉至 **裝置 → 受管理裝置**。

   b. 點擊受管理裝置的名稱。

   c. 在開啟的受管理裝置內容視窗中，轉至**應用程式**頁簽。

   d. 點擊僅適用於選定受管理裝置的網路代理政策的名稱。

3. 在開啟的內容視窗中，轉到**應用程式設定→連線→連線設定檔。**

4. 在**網路位置設定**區域，點擊**新增**按鈕。

5. 在開啟的內容視窗中，設定網路位置敘述和轉換規則。指定以下網路位置敘述設定：

   - **敘述**

     網路位置敘述名稱不能超過 255 字元或包含特殊字元，例如 ("*<>?\/:|)。

   - **使用連線設定檔**

     在該下拉清單中，您可以指定網路代理用於連線至管理伺服器的連線設定檔。該設定檔將在網路位置敘述條件被滿足時使用。連線設定檔包含網路代理連線到管理伺服器的設定；它還定義了用戶端裝置轉換到漫遊政策的時間。設定檔僅用於下載更新。

   - **敘述已啟用**

     選中此核取方塊以啟用新的網路位置描述。

6. 選擇網路代理切換規則條件：

- **DHCP 伺服器位址條件** — 網路 Dynamic Host Configuration Protocol (DHCP) 伺服器的 IP 位址已變更。
- **預設連線閘道位址條件** — 主要網路閘道的位址已變更。
- **DNS 網域條件** — 子網路的 DNS 後置詞已變更。
- **DNS 伺服器位址條件** — 網路 DNS 伺服器的 IP 位址已變更。
- **WINS 伺服器位址條件** — 網路 WINS 伺服器的 IP 位址已變更。此設定僅適用於執行 Windows 的裝置。
- **名稱可解析性條件** — 用戶端裝置的 DNS 或 NetBIOS 名稱已更改。
- **子網路條件** — 可變更子網路位址和遮罩。
- **Windows 網域可存取性條件** — 可變更用戶端裝置連線到的 Windows 網域的狀態。此設定僅適用於執行 Windows 的裝置。
- **SSL 連線位址可存取性條件** — 用戶端裝置可以或無法（取決於您選取的選項）與指定伺服器（名稱：連接埠）建立 SSL 連線。對於每個伺服器，您還可以指定 SSL 憑證。在這種情況下，除了檢查 SSL 連線的功能之外，網路代理還會驗證伺服器憑證。如果憑證不相符，則連線會失敗。

使用邏輯運算子 AND 可組合規則中的條件。要基於網路位置敘述觸發切換規則，必須滿足所有規則切換條件。

7. 在條件部分，指定何時應將網路代理切換到另一台管理伺服器。為此，點擊**新增**按鈕，然後設定條件值。

   此外，預設情況下會啟用**至少符合清單中的一個參數值**選項。如果您希望所有指定值都滿足條件，則可以停用此選項。

8. 儲存您的變更。

會建立網路位置敘述的新切換規則；當滿足其條件時，網路代理將使用此規則指定的設定檔連線至管理伺服器。

防護佈署精靈

要安裝 Kaspersky 應用程式，您可以使用防護佈署精靈。防護佈署精靈允許使用特別建立的安裝套件或直接從分發套件來遠端安裝應用程式。

防護佈署精靈會執行以下操作：

- 為應用程式安裝下載安裝套件（如果之前未建立）。該安裝套件位於**發現和佈署 → 佈署和分配 → 安裝套件**。您可以使用這些套件進行遠端安裝。
- 您可以為您指定的裝置或是管理群組，建立並啟動遠端安裝工作。新建立的遠端安裝工作會儲存在**工作**區段。您可以稍後自行執行此工作。工作類型為**遠端安裝應用程式**。

如果您想在裝有 SUSE Linux Enterprise Server 15 作業系統的裝置上安裝網路代理，請首先安裝 insserv-compat 套件配置網路代理。

步驟 1：開始防護佈署精靈

要手動啟動防護佈署精靈，

在主功能表中，轉至**發現和佈署 → 佈署和分配 → 防護佈署精靈**。

防護佈署精靈啟動。使用**下一步**按鈕進行精靈。

步驟 2：選取安裝套件

選取您要安裝的應用程式安裝套件。

若未列出必要應用程式的安裝套件，請點擊**新增**按鈕，接著從清單中選取應用程式。

步驟 3：選取金鑰檔案或啟動碼的發佈方式

選取金鑰檔案或啟動碼的發佈方式：

- **不新增產品授權金鑰到安裝套件**

  金鑰被自動分發到所相容的所有裝置：
  - 如果自動分發在金鑰內容中啟用。
  - 如果已建立**新增金鑰**。

- **新增產品授權金鑰到安裝套件**

  金鑰與安裝套件一起被分發到裝置。

  我們不建議您使用該方法分發金鑰，因為共用讀取存取權限已被啟用到安裝套件儲存區。

若安裝套件已包含金鑰檔案或啟動碼，此視窗隨即顯示、但僅會包含產品授權金鑰的資訊。

步驟 4：選取網路代理版本

如果您選取了非網路代理安裝套件，您也必須安裝網路代理，它連線應用程式到卡巴斯基安全管理中心管理伺服器。

選取網路代理的最新版本。

步驟 5：選取裝置

指定要安裝應用程式的裝置清單：

- **安裝到受管理裝置**

  如果選取該選項，程式將為該裝置群組建立遠端安裝工作。

- **選取需要安裝的裝置**

  該工作被分配到裝置選項中的裝置。您可以指定其中一個現有選項。

  例如，您可能要使用該選項在特定作業系統版本的裝置上執行工作。

步驟 6：指定遠端安裝工作設定

在**遠端安裝工作設定**頁面，指定應用程式遠端安裝設定。

在**強制下載安裝套件**設定群組中，指定如何將安裝應用程式所需的檔案分發到用戶端裝置中：

- **使用網路代理**

  如果啟用此選項，安裝套件透過安裝在裝置上的網路代理傳送到用戶端裝置。

  如果停用此選項，則會使用用戶端裝置的作業系統工具傳送安裝套件。

  如果已指派工作給安裝了網路代理的裝置，建議您選取該核取方塊。

  預設情況下已啟用該選項。

- **透過發佈點使用作業系統資源**

  如果啟用此選項，安裝套件使用作業系統工具透過發佈點傳送到用戶端裝置。如果網路中存在不止一個發佈點，那麼您可以選取本選項。

  如果選取**使用網路代理**方塊，僅在網路代理工具不可用時才透過作業系統工具傳送檔案。

  預設情況下，已經為虛擬管理伺服器上建立的遠端安裝工作選取該選項。

- **透過管理伺服器使用作業系統資源**

  如果啟用此選項，檔案將使用用戶端裝置的作業系統工具透過管理伺服器傳輸到用戶端裝置。如果使用者端裝置上未安裝網路代理，但是使用者端裝置與管理伺服器在同一網路，則您可以啟用此選項。

  預設情況下已啟用該選項。

定義附加設定：

- **如果已經安裝應用程式則不再重新安裝**

  如果啟用此選項，則如果選定的應用程式已安裝到該用戶端裝置上，將不再重新安裝它。
  如果停用此選項，系統仍將安裝應用程式。
  預設情況下已啟用該選項。

- **在 Active Directory 群組政策中指定安裝套件的安裝**

  如果選取此方塊，安裝套件會使用 Active Directory 的群組政策安裝。
  如果選取網路代理安裝套件，則該方塊可用。
  預設情況下已停用該選項。

步驟 7：重新啟動管理

如果安裝應用程式時作業系統必須重新啟動，指定要執行的操作：

- **不重新啟動裝置**

  用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

- **重新啟動裝置**

  如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

- **提示使用者操作**

  用戶端裝置螢幕上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。該選項適用於使用者必須可以選取最方便的時間進行重新啟動的工作站。

  預設情況下已選定此選項。

  - **重複提示間隔（分鐘）**

    如果啟用該選項，應用程式以指定頻率提示使用者重新啟動作業系統。

    預設情況下已啟用該選項。預設間隔是 5 分鐘。可用值介於 1 和 1440 分鐘之間。

    如果停用該選項，提示僅顯示一次。

  - **在該時間後重新啟動（分鐘）**

    提示使用者之後，應用程式在指定時間間隔後強制作業系統重新啟動。

    預設情況下已啟用該選項。預設延時是 30 分鐘。可用值介於 1 和 1440 分鐘之間。

- **強制關閉已鎖定連線的應用程式**

  執行應用程式可能會阻止用戶端裝置重新啟動。例如，如果文件在文書處理應用程式中編輯且未儲存，應用程式不會允許裝置重新啟動。

  如果啟用該選項，鎖定裝置上的此類應用程式在裝置重新啟動前被強制關閉。結果，使用者可能遺失他們未儲存的變更。

  如果停用該選項，鎖定裝置不被重新啟動。此裝置上的工作狀態表示裝置需要重新啟動。使用者必須手動關閉所有執行在鎖定裝置上的應用程式並重新啟動這些裝置。

  預設情況下已停用該選項。

步驟 8：安裝前移除不相容的應用程式

該步驟僅在您佈署的應用程式已知與其他應用程式不相容時才顯示。

如果您想讓卡巴斯基安全管理中心自動移除不相容的應用程式，則選取該選項。

不相容應用程式清單也被顯示。

如果您不選取該選項，應用程式將僅被安裝到沒有不相容應用程式的裝置。

步驟 9：移動裝置到受管理裝置

指定裝置是否在安裝網路代理後必須被移動到管理群組。

- **不移動裝置**

裝置保留在目前所在群組中。未被放置在任何群組的裝置保持未分配。

- **將未配置的裝置移動到群組**

  裝置被移動到您選取的管理群組。

預設情況下已選取**不移動裝置** 選項。為了安全，您可能會希望手動移動裝置。

步驟 10：選取存取裝置的帳戶

如果必要，新增要用於啟動遠端安裝工作的帳戶。

- **不需要帳戶（網路代理已安裝）**

  如果該選項被選中，您不是必須指定一個帳戶，並在該帳戶下執行程式的安裝。將使用執行管理伺服器服務的帳戶執行該工作。

  如果網路代理未安裝在用戶端裝置，則此選項無法使用。

- **需要帳戶（不使用網路代理）**

  如果您為其分配遠端安裝工作的裝置上未安裝網路代理，請選取此選項。在這種情況下，您可以指定使用者帳戶或 SSH 憑證來安裝應用程式。

  - **本機帳戶**。如果選取此選項，請指定用於執行應用程式安裝程式的使用者帳戶。點擊**新增**按鈕，選擇**本機帳戶**，然後指定使用者帳戶憑據。

    您可以根據情況指定多個帳戶，例如，沒有一個帳戶在分配工作的所有裝置上擁有全部所需權限時。在此情況下，已新增的所有帳戶會用於從上到下按順序執行該工作。

  - **SSH 憑證**。如果要在 Linux 用戶端裝置上安裝應用程式，您可以指定 SSH 憑證而不是指定使用者帳戶。按一下**新增**按鈕，選擇**SSH 憑證**，然後指定憑證的私鑰和公鑰。

    如要產生私密金鑰，您可以使用 ssh-keygen 公用程式。請注意，卡巴斯基安全管理中心支援 PEM 格式的私密金鑰，但 ssh-keygen 公用程式預設為產生 OPENSSH 格式的 SSH 金鑰。卡巴斯基安全管理中心不支援 OPENSSH 格式。要以支援的 PEM 格式建立私密金鑰，請在 ssh-keygen 命令中加入 -m PEM 選項。例如：

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "< 使用者電子郵件 >"
    ```

步驟 11：啟動安裝

該頁面是精靈的最後一步。在該步驟，**遠端安裝工作**已被成功建立並配置。

預設不會選取**精靈完成時執行工作**選項。如果您選取該選項，**遠端安裝工作**將在您完成精靈後立即啟動。如果您不選取該選項，**遠端安裝工作**不會啟動。您可以稍後自行執行此工作。

點擊**確定**以完成防護佈署精靈的最終步驟。

透過卡巴斯基安全管理中心網頁主控台佈署 Kaspersky 應用程式

本節說明如何透過卡巴斯基安全管理中心 網頁主控台在貴組織內的用戶端裝置上佈署 Kaspersky 應用程式。

情境：透過卡巴斯基安全管理中心網頁主控台佈署 Kaspersky 應用程式

此情境說明如何透過卡巴斯基安全管理中心 網頁主控台佈署 Kaspersky 應用程式。您可以使用快速啟動精靈和防護佈署精靈，或者您可以手動完成所有必要步驟。

以下應用程式可以透過使用卡巴斯基安全管理中心 網頁主控台佈署：

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux

階段

Kaspersky 應用程式佈署分步驟進行：

1. **為應用程式下載外掛程式**

   該步驟使用快速設定精靈執行。如果您選取不執行精靈，手動下載 Kaspersky Endpoint Security for Windows 外掛程式。

   如果您計劃管理公司行動裝置，請按照 Kaspersky Security for Mobile 說明中提供的指示下載並安裝 Kaspersky Endpoint Security for Android 的管理外掛程式。

2. **下載並建立安裝套件**

   該步驟使用快速設定精靈執行。

   快速設定精靈可讓您透過管理外掛程式下載安裝套件。若您執行精靈時不選取此選項，或若您完全不要執行精靈，您必須手動下載該套件。

   您不可在相同裝置上透過卡巴斯基安全管理中心安裝 Kaspersky 應用程式，例如在遠端員工的裝置，您可建立適用於應用程式的獨立安裝套件。如果您使用獨立軟體套件安裝 Kaspersky 應用程式，則不必建立和執行遠端安裝工作，也不必為 Kaspersky Endpoint Security for Windows 建立和配置工作。

3. **建立、配置和執行遠端安裝工作**

   對於 Kaspersky Endpoint Security for Windows，該階段是防護佈署精靈的一部分，它在快速設定精靈完成後自動啟動。如果您選取不執行防護佈署精靈，您必須手動建立該工作並手動配置它。

   您也可以為不同管理群組或不同裝置分類手動建立幾個遠端安裝工作。您可以在這些工作中佈署應用程式的不同版本。

   請確保搜尋到網路上所有裝置，之後執行遠端安裝工作。

如果您想在裝有 SUSE Linux Enterprise Server 15 作業系統的裝置上安裝網路代理，請首先安裝 insserv-compat 套件配置網路代理。

4. **為受管理應用程式建立和配置工作**

   必須配置 Kaspersky Endpoint Security for Windows 的*安裝更新*工作。

   該階段是快速設定精靈的一部分：工作被使用預設設定自動建立和配置。如果您未執行精靈，您必須手動建立該工作並手動配置它。如果您使用快速啟動精靈，請確保工作排程滿足您的要求。（預設情況下，排程的工作開始時間設定為**手動**，但您可能想要選擇其他選項。）

   其他 Kaspersky 應用程式可能具有其他預設工作。請參考對應應用程式的文件。

   請確保您建立的各工作排程符合您的需求。

5. **安裝 Kaspersky Security for Mobile（可選）**

   如果您計劃管理公司行動裝置，請按照 Kaspersky Security for Mobile 說明 中提供的指示瞭解有關 Kaspersky Endpoint Security for Android 部署的資訊。

6. **建立政策**

   手動為每個應用程式建立政策或（如果是 Kaspersky Endpoint Security for Windows）透過快速設定精靈。您可以使用政策預設設定；您也可以根據需要隨時修改政策預設設定。

7. **驗證結果**

   確保佈署成功完成：您的每個應用程式都擁有政策和工作，這些應用程式被安裝到受管理裝置。

結果

完成情境可以導致如下：

- 所選應用程式的所有所需政策和工作被建立。
- 工作排程根據您的需要被配置。
- 所選應用程式被佈署，或者排程在所選用戶端裝置上佈署。

獲取 Kaspersky 應用程式外掛程式

要佈署 Kaspersky 應用程式，例如 Kaspersky Endpoint Security for Windows，您必須為此應用程式下載管理外掛程式。

要為 Kaspersky 應用程式下載外掛程式：

1. 在主功能表中，轉至 **主控台設定 → Web 外掛程式**。
2. 在開啟的視窗中，點擊**新增**按鈕。
   可用外掛程式清單被顯示。
3. 在可用外掛程式清單中，透過點擊其名稱選取您要下載的外掛程式（例如，Kaspersky Endpoint Security 11 for Windows）。
   外掛程式敘述頁面被顯示。

4. 在外掛程式說明頁面，點擊**安裝外掛程式**。

5. 安裝完成時，點擊**確定**。

管理外掛程式使用預設配置被下載並顯示在管理外掛程式清單。

您可以從檔案中新增外掛程式和更新下載的外掛程式。您可以從卡巴斯基技術支持網頁下載管理外掛程式和 Web 管理外掛程式。

若要從檔案中下載或更新外掛程式：

1. 在主功能表中，轉至 **主控台設定 → Web 外掛程式**。

2. 執行以下操作之一：

   - 點擊**從檔案新增**，以從檔案中下載外掛程式。
   - 點擊**從檔案更新**，以從檔案中下載外掛程式的更新。

3. 指定檔案和檔案的簽名。

4. 下載指定的檔案。

管理外掛程式會從檔案中下載，並顯示在管理外掛程式的清單中。

下載和建立 Kaspersky 應用程式的安裝套件

若您的管理伺服器有網際網路的存取權，您可從 Kaspersky 網路伺服器建立 Kaspersky 應用程式的安裝套件。

下載和建立 Kaspersky 應用程式的安裝套件：

1. 執行以下操作之一：

   - 在主功能表中，轉至 **發現和佈署 → 佈署和分配 → 安裝套件**。
   - 在主功能表中，轉至 **操作 → 儲存區 → 安裝套件**。

   您也可在螢幕通知清單中檢視通知關於 Kaspersky 應用程式新套件的通知。如果有關於新安裝套件的通知，您可以按一下通知旁邊的連結並轉到可用安裝套件清單。

   系統會顯示可在管理伺服器使用的安裝套件清單。

2. 點擊**新增**。

   新套件精靈啟動。使用**下一步**按鈕進行精靈。

3. 選擇**為 Kaspersky 應用程式建立安裝套件**。

   Kaspersky 網路伺服器可用安裝套件清單隨即顯示。該清單僅包含與當前版本的卡巴斯基安全管理中心相容的那些應用程式的安裝套件。

4. 按一下安裝套件的名稱，例如 Kaspersky Endpoint Security for Windows (11.1.0)。

   帶有安裝套件資訊的視窗開啟。

   如果符合適用的法律和規定，您可以下載並使用包含加密工具以實施強加密的安裝套件。若要下載符合您組織需要的 Kaspersky Endpoint Security for Windows 安裝套件，請諮詢組織用戶端裝置所在的國家或地區的法務部門。

5. 請閱讀資訊並點擊**下載並建立安裝套件**按鈕。

   若分發套件無法轉換為安裝套件，**下載分發套件**按鈕則會取代 **下載並建立安裝套件**顯示。

   下載安裝套件到管理伺服器開始。您可以關閉精靈視窗或繼續執行指示的下一步。如果關閉精靈視窗，下載程序將在後台模式下繼續。

   如果要追蹤安裝套件的下載程序，請執行以下操作：

   a. 在主功能表中，轉至 **操作 → 儲存區 → 安裝套件 → 進行中 ()**。

   b. 追蹤操作進度**下載進度**欄和**下載狀態**表的欄。

   該程序完成後，請安裝套件將新增到**已下載**頁籤的清單。如果下載程序停止並且下載狀態切換為**接受 EULA**，然後點擊安裝套件名稱，然後繼續進行指示的下一步。

   若包含在所選分發套件的資料大小超過目前限制，便會顯示錯誤訊息。您可變更限制值，接著繼續建立安裝套件。

6. 對於一些 Kaspersky 應用程式，下載過程中，**顯示 EULA**按鈕被顯示。如果它不顯示，做以下操作：

   a. 點擊**顯示 EULA**按鈕以閱讀最終使用者產品授權協議 (EULA)。

   b. 閱讀螢幕顯示的 EULA，並再次點擊**同意**。

      您接受 EULA 後下載便會繼續。若您點擊**拒絕**，下載便會暫停。

7. 下載完成後，按一下**關閉**按鈕。

   所選的安裝套件或套件被下載到管理伺服器分享資料夾，到 Packages 子資料夾。下載後，安裝套件出現在安裝套件清單。

變更自訂安裝套件資料大小限制

在建立自訂安裝套件期間解壓縮資料的總大小有所限制。預設限制為 1 GB。

若您嘗試上傳的封存檔案內有超過目前限制的資料，則會顯示錯誤訊息。從大型分發套件建立安裝套件時，您可能需要增加此限制值。

若要變更自訂安裝套件大小的限制值：

1. 在管理伺服器裝置上，使用安裝管理伺服器所用的帳戶執行命令提示字元。
2. 將當前目錄變更為卡巴斯基安全管理中心安裝資料夾（通常為 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center）。
3. 根據管理伺服器安裝的類型，使用管理員權限輸入以下命令之一：

   - 標準本機安裝：

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <number of bytes>
     ```

   - 在卡巴斯基安全管理中心容錯移轉叢集上安裝：

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <number of bytes> --stp klfoc
     ```

   - 在 Windows 伺服器容錯移轉叢集上安裝：

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <字元組數> --stp cluster
     ```

   其中 <number of bytes> 是十六進位或十進位格式的字元組數。

   例如，如果要求的限制為 2 GB，您可以指定十進制值 2147483648 或十六進制值 0x80000000。在這種情況下，要進行管理伺服器的本機安裝時，您可以使用以下命令：

   ```
   klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
   ```

自訂安裝套件資料的大小限制隨即變更。

為 Kaspersky 應用程式下載分發套件

在卡巴斯基安全管理中心 網頁主控台，您可以為 Kaspersky 應用程式下載和儲存分發套件。您可以使用分發套件手動安裝應用程式，而不使用卡巴斯基安全管理中心。

要為 Kaspersky 應用程式下載和儲存分發套件：

1. 在主功能表中，轉到**操作 → 卡巴斯基應用程式 → 目前應用程式版本**。

   可用分發套件、外掛程式與修補程式清單隨即開啟。卡巴斯基安全管理中心僅顯示與其當前版本相容的項目。

2. 在清單中，點擊您要下載的套件名稱。

   套件敘述開啟。

3. 請閱讀說明並點擊**下載並建立安裝套件** 按鈕。

   若分發套件無法轉換為安裝套件，**下載分發套件**按鈕會取代**下載並建立安裝套件**顯示。

   下載安裝套件到管理伺服器隨即開始。

所選的安裝套件或分發套件被下載到管理伺服器分享資料夾，到 **Packages** 子資料夾。下載後，安裝套件會顯示在安裝套件清單中。

檢查 Kaspersky Endpoint Security 已成功部署

要確保您已正確佈署了 Kaspersky 應用程式，例如 Kaspersky Endpoint Security：

1. 使用卡巴斯基安全管理中心 網頁主控台，確保您具有如下：
   - Kaspersky Endpoint Security 和/或您使用的其他安全應用程式的政策。
   - Kaspersky Endpoint Security for Windows 工作：*快速掃描*工作和*安裝更新*工作（如果您使用 Kaspersky Endpoint Security for Windows）。
   - 您使用的其他安全應用程式工作。
2. 在選取用於安裝的受管理裝置之一上，確保以下：
   - Kaspersky Endpoint Security 或其他 Kaspersky 安全應用程式被安裝。
   - 在 Kaspersky Endpoint Security 上，檔案威脅防護、Web 威脅防護和郵件威脅防護設定與您為該裝置建立的政策比對。
   - Kaspersky Endpoint Security 服務可以被手動停止和啟動。
   - 可以被手動停止和啟動的群組工作。

建立獨立安裝套件

貴組織中您與裝置使用者可使用獨立安裝套件在裝置上手動安裝應用程式。

獨立安裝套件是可執行檔 (installer.exe)，您可將其儲存在網頁伺服器或共用資料夾、由電子郵件傳送，或以其他方式傳輸至用戶端裝置。在用戶端裝置上，使用者會本機執行已接收檔案而不透過卡巴斯基安全管理中心以安裝應用程式。您可以為 Kaspersky 應用程式和 Windows、macOS 和 Linux 平台的協力廠商應用程式建立獨立安裝套件。若要建立協力廠商的應用程式獨立安裝套件，您必須建立自訂安裝套件。

請確保未獲授權的人員無法取得獨立安裝套件。

若要建立獨立安裝套件：

1. 執行以下操作之一：
   - 在主功能表中，轉至 **發現和佈署 → 佈署和分配 → 安裝套件**。
   - 在主功能表中，轉至 **操作 → 儲存區 → 安裝套件**。

   系統會顯示可在管理伺服器使用的安裝套件清單。
2. 在安裝套件的清單中，選取安裝套件並在上列清單中，點擊**佈署**按鈕。
3. 選擇**使用獨立安裝套件**選項。

   獨立安裝套件建立精靈啟動。使用**下一步**按鈕進行精靈。

4. 若您要隨所選的應用程式安裝網路代理，請確認**網路代理與該應用程式一同安裝**選項已啟用。

   顯示的選項取決於您為其建立獨立安裝套件的應用程式。

   預設情況下已啟用該選項。若您不確認裝置是否安裝網路代理，建議啟用此選項。若網路代理已在裝置上安裝，在安裝含網路代理的獨立安裝套件後，網路代理將會更新至新版本。

   若您停用此選項，網路代理將不會安裝在裝置上，且裝置不會受到管理。

   若管理伺服器已存在所選應用程式的獨立安裝套件，精靈會告知您此資訊。在此情況下，您必須選取以下其中一個動作：

   - **建立獨立安裝套件**。若您要針對新應用程式版本建立獨立安裝套件，並同時希望保留針對先前應用程式版本建立的獨立安裝套件，請選取此選項。新獨立安裝套件會放在另一個資料夾中。
   - **使用存在的獨立安裝套件**。若要使用現有獨立安裝套件，請選取此選項。建立套件的程序將不會啟動。
   - **重新建立存在的獨立安裝套件**。如果您要再次針對相同應用程式建立獨立安裝套件，請選取此選項。獨立安裝套件會放在相同資料夾。

5. 在**移動到受管理裝置清單**步驟，預設會啟用**不移動裝置**選項。若您在網路代理安裝後不想要移動用戶端裝置至任何管理群組，請啟用此選項。

   如果要在網路代理安裝後移動客戶端裝置，請選取**將未配置的裝置移動到此群組**選項並指定要將將客戶端裝置移動到的管理群組。依預設，裝置會移至**受管理裝置**群組。

6. 獨立安裝套件建立完成後，按一下**完成**按鈕。

   獨立安裝套件建立精靈即會關閉。

系統會在管理伺服器共用資料夾的 PkgInst 子資料夾建立和放置獨立安裝套件。您可透過點擊在安裝套件清單上的**檢視獨立安裝套件清單**按鈕檢視獨立安裝套件的清單。

檢視獨立安裝套件清單

您可檢視獨立安裝套件的清單以及各獨立安裝套件的內容。

若要所有安裝套件的獨立安裝套件清單：

在上述清單中，點擊**檢視獨立安裝套件清單**按鈕。

在獨立安裝套件清單中，其屬性顯示如下：

- **檔案名稱**。自動形成為包含在套件與應用程式版本中之應用程式名稱的獨立安裝套件名稱。
- **應用程式名稱**。包含在獨立安裝套件中的應用程式名稱。
- **應用程式版本**。
- **網路代理的安裝檔案名稱**。僅在網路代理包含在獨立安裝套件中時才會顯示內容。
- **網路代理版本**。僅在網路代理包含在獨立安裝套件中時才會顯示內容。
- **大小**。檔案大小為 MB。

- **群組**。網路代理安裝後要將用戶端裝置移動過去的群組名稱。
- **建立日期**。建立獨立安裝套件的日期和時間。
- **已修改**。修改獨立安裝套件的日期和時間。
- **路徑**。獨立安裝套件所在資料夾的完整路徑。
- **網址**。獨立安裝套件位置的網址。
- **檔案雜湊值**。該內容會用來驗證獨立安裝套件不是由協力廠商變更，且使用者有您建立與傳輸給使用者的相同檔案。

若要檢視特定安裝套件的獨立安裝套件清單：

選取清單中的安裝套件，並在清單上點擊**檢視獨立安裝套件清單**按鈕。

在獨立安裝套件清單中，您可執行以下操作：

- 點擊**發佈**按鈕，在網路伺服器上發佈獨立安裝套件。收到您傳送之獨立安裝套件連結的使用者，可下載已發佈的獨立安裝套件。
- 點擊**取消發佈**按鈕，取消網路伺服器上獨立安裝套件的發佈。只有您與其他管理員可下載取消發佈的獨立安裝套件。
- 點擊**下載**按鈕，下載獨立安裝套件至您的裝置。
- 點擊**透過電子郵件傳送**按鈕，傳送含有連至獨立安裝套件的連結。
- 點擊**刪除**按鈕，移除獨立安裝套件。

建立自訂安裝套件

您可使用自訂安裝套件進行以下操作：

- 在用戶端裝置安裝應用程式（如文字編輯器），例如根據工作方式。
- 建立獨立安裝套件。

自訂安裝套件是有一組檔案的資料夾。建立自訂安裝套件的來源是*封存檔案*。封存檔案內含檔案或必須包含在自訂安裝套件的檔案。建立自訂安裝套件期間，您可指定命令行參數，例如在靜默模式中安裝應用程式。

如果您具有弱點和修補程式管理 (VAPM) 功能的啟動產品授權金鑰，則可以轉換相關自訂安裝套件的預設安裝設定，並使用 Kaspersky 專家建議的值。只有當協力廠商應用程式的 Kaspersky 資料庫中含有對應的可執行檔時，系統才會在建立自訂安裝套件的程序中自動轉換設定。

若要建立應用程式安裝套件：

1. 執行以下操作之一：

   - 在主功能表中，轉至 **發現和佈署 → 佈署和分配 → 安裝套件**。
   - 在主功能表中，轉至 **操作 → 儲存區 → 安裝套件**。

   系統會顯示可在管理伺服器使用的安裝套件清單。

2. 點擊**新增**。

   新套件精靈啟動。使用**下一步**按鈕進行精靈。

3. 選擇 **從檔案建立安裝套件**。

4. 指定套件名稱並按一下**瀏覽**按鈕。

   標準 Windows **開啟**視窗隨即在您的瀏覽器開啟，您可在其中選擇檔案建立安裝套件。

5. 選擇位於可用磁碟的封存檔案。

   您可以上傳 ZIP、CAB、TAR 或 TAR.GZ 封存。您無法從 SFX（自行解壓封存）檔案來建立安裝套件。

   > 如果要在套件安裝程序中轉換設定，請確保選取**在精靈完成後，針對卡巴斯基安全管理中心 辨識出的應用程式將設定轉換為建議值**核取方塊，然後點擊**下一步**。

   將檔案上傳到卡巴斯基安全管理中心管理伺服器的程序隨即啟動。

   > 如果啟用了建議的安裝設定，則卡巴斯基安全管理中心 14.2 會檢查第三方應用程式的 Kaspersky 資料庫中是否包含可執行檔。如果檢查成功，您會收到一條通知，通知您系統已識別檔案。已轉換設定；已建立自訂安裝套件。不需要進一步操作。點擊**完成**按鈕以關閉精靈。

6. 選取檔案（從已選封存檔案擷取的檔案清單），接著指定可執行檔命令列參數。

   您可指定命令行參數以靜默模式從安裝應用程式來安裝套件。您可選擇指定命令行參數。

   系統會啟動建立安裝套件的程序。

   精靈會通知您程序已完成。

   若未建立安裝套件，系統會顯示適合的訊息。

7. 點擊**完成**按鈕以關閉精靈。

您建立的安裝套件會下載至管理伺服器共用資料夾的套件子資料夾。下載後，安裝套件出現在安裝套件清單。

在管理伺服器可用之安裝套件的清單中，透過點擊自訂安裝套件名稱的連結，您可：

- 檢視安裝套件的以下內容：
  - **名稱**。自訂安裝檔案名稱。
  - **來源**。應用程式供應商名稱。
  - **應用程式**。封裝在自訂安裝套件的應用程式名稱。
  - **版本**。應用程式版本。
  - **語言**。封裝在自訂安裝套件的應用程式語言。
  - **大小 (MB)**。安裝套件大小。
  - **作業系統**。適用安裝套件的作業系統類型。
  - **建立日期**。安裝套件建立日期。
  - **已修改**。安裝套件修改日期。
  - **類型**。安裝套件的類型。
- 變更檔案名稱與命令行參數。此功能僅可在套件使用，而非在 Kaspersky 應用程式建立時可用。

如果在建立自訂套件期間將套件安裝設定轉換為建議值，則在自訂安裝套件屬性的**設定**頁籤可能會顯示兩個區段：**設定**和**安裝處理程序**。

設定區段包含下表顯示的以下屬性：

- **名稱**。此欄會顯示分配給安裝參數的名稱。
- **類型**。此欄會顯示安裝參數的類型。
- **參數值**。此欄會顯示由安裝參數（Bool、Filepath、Numeric、Path 或 String）定義的資料類型。

安裝處理程序區段包含一張表格，其中說明自訂安裝套件中內含更新的以下屬性：

- **名稱**。更新的名稱。
- **敘述**。更新的說明。
- **來源**。更新的來源，由 Microsoft 或其他第三方開發人員發布。
- **類型**。更新的類型，適用於驅動程式還是應用程式。
- **類別**。顯示 Microsoft 更新（關鍵更新、定義更新、驅動程式、功能套件、安全更新、Service Pack、工具、更新匯總、更新或升級）的 Windows Server Update Services (WSUS) 類別。
- **以 MSRC 為依據的嚴重等級**。Microsoft 安全回應中心 (MSRC) 定義的更新嚴重等級。
- **嚴重等級**。Kaspersky 定義的更新嚴重等級。

- **修補程式嚴重等級（適用於 Kaspersky 應用程式的修補程式）**。修補程式的嚴重等級（如果適用於 Kaspersky 應用程式）。
- **文章**。知識庫中描述更新的文章識別碼 (ID)。
- **公告**。說明更新的安全公告 ID。
- **未指派安裝**。顯示更新是否具有未指派安裝狀態。
- **待安裝**。顯示更新是否具有「待安裝」狀態。
- **安裝中**。顯示更新是否具有「安裝中」狀態。
- **已安裝**。顯示更新是否具有「已安裝」狀態。
- **已失敗**。顯示更新是否具有「已失敗」狀態。
- **需要重新啟動**。顯示更新是否具有「需要重新啟動」狀態。
- **已註冊**。顯示註冊更新的日期和時間。
- **以互動模式安裝**。顯示更新是否需要在安裝期間與使用者進行互動。
- **已撤銷**。顯示撤銷更新的日期和時間。
- **更新批准狀態**。顯示更新是否獲准安裝。
- **修訂版**。顯示更新的當前修訂版號。
- **更新 ID**。顯示更新的 ID。
- **應用程式版本**。顯示應用程式將更新到的版號。
- **已取代**。顯示可以取代更新的其他更新。
- **取代中**。顯示可以由更新取代的其他更新。
- **您必須接受產品授權協議的條款**。顯示更新是否需要接受最終使用者產品授權協議 (EULA) 的條款。
- **供應商**。顯示更新供應商的名稱。
- **應用程式系列**。顯示更新所屬的應用程式系列名稱。
- **應用程式**。顯示更新所屬的應用程式名稱。
- **語言**。顯示更新本地化的語言。
- **未指派安裝（新版本）**。顯示更新是否具有「未指派安裝（新版本）」的狀態。
- **需要先決條件安裝**。顯示更新是否具有「需要先決條件」的安裝狀態。
- **下載模式**。顯示更新下載的模式。

- **是修補程式**。顯示更新是否為修補程式。
- **未安裝**。顯示更新是否具有「未安裝」狀態。

分發安裝套件至從屬管理伺服器

卡巴斯基安全管理中心允許您建立安裝套件以用於卡巴斯基應用程式和協力廠商應用程式，以及將安裝套件分發到用戶端裝置並從套件中安裝應用程式。要最佳化主管理伺服器上的負載，您可以將安裝套件分發到從屬管理伺服器。之後，從屬伺服器將套件傳輸到用戶端裝置，然後您可以在用戶端裝置上執行應用程式的遠端安裝。

若要分發安裝套件至從屬管理伺服器：

1. 請確定，從屬管理伺服器已連線到主管理伺服器。
2. 在主功能表中，轉至 **裝置 → 工作**。

   工作清單隨即顯示。
3. 點擊**新增**按鈕。

   新工作精靈啟動。遵照精靈的說明。
4. 在**新工作**頁面的**應用程式**下拉清單中，選取**卡巴斯基安全管理中心**。然後，從**工作類型**下拉清單中選擇**發佈安裝套件**，然後指定工作名稱。
5. 在 **工作範圍**頁面，透過以下方式之一選擇要將工作分配到哪些裝置：
   - 如果您要為管理群組中的所有從屬管理伺服器建立工作，您可以選取該群組，然後為其建立群組工作。
   - 如果要為特定的從屬管理伺服器建立工作，請選取這些伺服器，然後為其建立工作。
6. 在**發佈的安裝套件**頁面，選擇要複製到從屬管理伺服器的安裝套件。
7. 指定一個帳戶，以便在這個帳戶下執行*分發安裝套件*工作。您可以使用您的帳戶並保持**預設帳戶**選項處於啟用狀態。或者，您可以指定工作應在具有必要存取權限的另一個帳戶下執行。為此，請選擇**指定帳戶**選項，然後輸入該帳戶的憑據。
8. 在**完成工作建立**頁面上，您可以啟用**建立完成時開啟工作詳情**選項以開啟工作屬性視窗，然後修改預設工作設定。否則，您可以稍後隨時配置工作設定。
9. 點擊**完成**按鈕。

   為了將安裝套件分發到從屬管理伺服器而建立的工作，會顯示在工作清單中。
10. 您可以手動執行此工作，或等候工作設定中指定的排程將其啟動。

工作完成後，所選的安裝套件將複製到指定的從屬管理伺服器。

使用遠端軟體安裝工作安裝應用程式

卡巴斯基安全管理中心允許您遠端安裝應用程式到裝置，使用遠端安裝工作。那些工作透過專門精靈被建立被分配到裝置。要更快和更便捷地分配工作，您可以在精靈視窗中指定裝置（最多 1000 台裝置），使用以下方式之一：

- **選取管理伺服器偵測到的網路裝置**。此種情況下，工作被分配到指定裝置。特定裝置可以包含管理群組的裝置和未配置的裝置。
- **手動指定裝置位址或從清單匯入位址**。您可以指定您要為其分配工作的裝置的 NetBIOS 名稱、DNS 名稱、IP 位址和 IP 子網路。
- **分配工作到裝置分類**。此種情況下，工作被分配到先前建立的分類中的裝置。您可以指定預先定義的分類或您所建立的自訂分類。
- **分配工作到管理群組**。此種情況下，工作被分配到先前建立的管理群組中的裝置。

為避免在未安裝網路代理的用戶端裝置上安裝應用程式時可能出現的問題，您必須按照透過卡巴斯基安全管理中心的遠端安裝工作強制部署中所述進行操作。

遠端安裝應用程式

本節包含有關如何在管理群組、具有特定 IP 位址的裝置或選擇的受管裝置上遠端安裝應用程式的資訊。

若要安裝應用程式到特定裝置：

1. 在主功能表中，轉至 **裝置 → 工作**。
2. 點擊**新增**。

   新工作精靈啟動。
3. 在**工作類型**欄位中，選擇**遠端安裝應用程式**。

4. 您可以選取以下其中一個方法：

- **分配工作到管理群組**

  工作被分配到包含在管理群組中的裝置。您可以指定其中一個現有群組或者建立新群組。

  例如，您可能要使用該選項執行傳送訊息到使用者工作，如果訊息針對包含在特定管理群組中的裝置。

  如果工作被指派給管理群組，則工作屬性視窗中不會顯示**安全**標籤，因為群組工作受其所套用的群組的安全設定的約束。

- **手動指定裝置位址或從清單匯入位址**

  您可以指定您要為其分配工作的裝置的 NetBIOS 名稱、DNS 名稱、IP 位址和 IP 子網路。

  您可能要使用該選項以對特定子網路執行工作。例如，您可能要安裝特定應用程式到會計裝置，或者掃描疑似被感染子網路中的裝置。

- **分配工作到裝置分類**

  該工作被分配到裝置選項中的裝置。您可以指定其中一個現有選項。

  例如，您可能要使用該選項在特定作業系統版本的裝置上執行工作。

5. 遵照精靈的說明。

   新工作精靈會在特定裝置上建立精靈中所選應用程式的遠端安裝工作。如果您選擇了**分配工作到管理群組**選項，工作將是一個組工作。

6. 您可以手動執行此工作，或等候工作設定中指定的排程將其啟動。

遠端安裝工作完成後，所選應用程式將安裝在指定裝置上。

透過 Active Directory 群組政策安裝應用程式

卡巴斯基安全管理中心可以讓您在受管理裝置上使用 Active Directory 群組政策安裝 Kaspersky 應用程式。

> 您必須連同安裝套件中的網路代理一起安裝，才使用 Active Directory 的群組政策進行安裝應用程式。

使用 Active Directory 的群組政策安裝應用程式，請執行以下操作：

1. 執行防護佈署精靈。遵照精靈的說明。
2. 在防護部署精靈的**遠端安裝工作設定**頁面上，啟用**在 Active Directory 群組政策中指定安裝套件的安裝**。
3. 在**選取帳戶以存取裝置**頁面上，選擇**需要帳戶（不使用網路代理）**選項。
4. 在安裝了卡巴斯基安全管理中心的裝置上新增帶有管理員權限的帳戶或包含在「群組政策建立器所有者」網域群組的帳戶。

5. 將權限授予所選帳戶：

   a. 轉到**控制面板→管理工具**，然後開啟**群組政策管理**。

   b. 按一下具有所需網域的節點。

   c. 按一下**委派**區段。

   d. 在**權限**下拉功能表中，選取**連結 GPOs**。

   e. 按一下**新增**。

   f. 在開啟的**選取使用者、電腦或群組**視窗中，選取所需的帳戶。

   g. 按一下**確定**關閉**選取使用者、電腦或群組**視窗。

   h. 在**群組和使用者**清單中，選取剛剛新增的帳戶，然後按一下**進階 → 進階**。

   i. 在**權限項目**清單中，按兩下剛剛新增的帳戶。

   j. 授予以下權限：

      - **建立群組物件**
      - **刪除群組物件**
      - **建立群組政策容器物件**
      - **刪除群組政策容器物件**

   k. 按一下**確定**儲存變更。

6. 按照精靈的說明定義其他設定。

7. 手動執行建立的遠端安裝工作，或等待排程啟動。

啟動該工作之後，將會進行遠端安裝的流程：

1. 工作執行時，以下的物件將會建立在指定裝置上的網域中：

   - 名稱 **Kaspersky_AK{GUID}** 下的群組政策物件 (GPO)。
   - 對應於 GPO 的安全群組。該安全群組包含工作覆蓋的用戶端裝置。安全群組的內容定義了 GPO 的範圍。

2. 在這種情況下，卡巴斯基安全管理中心會直接從程式名為 KLSHARE 的共用網路資料夾在用戶端裝置上安裝程式。在卡巴斯基安全管理中心的安裝資料夾中，系統將建立一個輔助子資料夾，其中包含安裝應用程式所需的 .msi 檔案。

3. 當新裝置新增到此工作範圍內時，這些新電腦將會在下個工作啟動時，自動加入到安全性群組。如果在工作排程中選定**執行略過的工作**選項，則裝置將立即加入安全群組。

4. 當從工作範圍中刪除了裝置，在下個工作啟動時，將會將其安全性群組中刪除。

5. 當您從 Active Directory 中刪除了此工作，GPO、連至 GPO 的連結，還有安全性群組都會刪除。

如果您要透過 Active Directory 安裝其他的程式，您可以手動的進行調整這些設定。例如，這可能會發生在以下狀況：

- 當病毒防護管理員沒有權限進行更動網域中的 Active Directory 時
- 原始安裝套件必須儲存在單獨的網路資源上時
- 當需要將 GPO 連結到特定的 Active Directory 單元時

在 Active Directory 中有以下情況，可使用下列另一種安裝方式：

- 如果直接從卡巴斯基安全管理中心共用資料夾進行安裝，您必須在 GPO 屬性中為所需應用程式指定 .msi 檔案（位於安裝套件的 exec 子資料夾中）。
- 如果必須將安裝套件放置在其他網路資源上，您必須將整個 exec 資料夾的內容複製過去，因為除了副檔名為 .msi 的檔案外，該資料夾還包含建立安裝套件時建立的設定檔。要安裝與該程式相關聯的產品授權金鑰，請將金鑰檔案一起複製到該資料夾中。

在從屬管理伺服器上安裝應用程式

在從屬管理伺服器上安裝應用程式：

1. 與控制相關從屬管理伺服器的管理伺服器建立連線。
2. 請您確定每台從屬管理伺服器都必須有要安裝的應用程式套件。如果在任何從屬伺服器上都找不到安裝套件，請發佈它。為此，建立一個工作類型為**發佈安裝套件**的工作。
3. 在從屬管理伺服器上建立一個遠端應用程式安裝工作。選擇**將應用程式遠端安裝到從屬管理伺服器**工作類型。

   新工作精靈會在特定的從屬管理伺服器上建立精靈中所選應用程式的遠端安裝工作。
4. 您可以手動執行此工作，或等候工作設定中指定的排程將其啟動。

遠端安裝工作完成後，所選應用程式將安裝在從屬管理伺服器上。

指定在 Unix 裝置上進行遠端安裝的設定

使用遠端安裝工作在 Unix 裝置上安裝應用程式時，可以為工作指定 Unix 特定的設定。建立工作後，這些設定可在工作屬性中使用。

要為遠端安裝工作指定特定於 Unix 的設定，請執行以下操作：

1. 在主功能表中，轉至 **裝置 → 工作**。
2. 按一下您要為其指定 Unix 特定設定的遠端安裝工作名稱。

   工作內容視窗隨即開啟。
3. 前往**應用程式設定 → Unix 特定設定**。

4. 指定下列設定：

- **設定根帳戶密碼（僅適用於透過 SSH 佈署）**

  如果不指定密碼則無法在目標裝置上使用 sudo 指令，選擇此選項，然後指定 root 帳戶的密碼。卡巴斯基安全管理中心會以加密形式將密碼傳送到目標裝置，解密該密碼，然後代表具有指定密碼的 root 帳戶啟動安裝程序。

  卡巴斯基安全管理中心不會使用該帳戶或指定的密碼來建立 SSH 連線。

- **指定前往暫存資料夾的路徑，具有目標裝置上的執行權限（僅適用於透過 SSH 佈署）**

  如果目標裝置上的 /tmp 目錄沒有執行權限，請選擇此選項，然後指定具有執行權限的目錄路徑。卡巴斯基安全管理中心使用指定的目錄作為透過 SSH 存取的暫存目錄。應用程式會將安裝套件放在目錄中並執行安裝程序。

5. 點擊**儲存**按鈕。

隨即儲存指定的工作設定。

啟動和停止卡巴斯基應用程式

您可以使用*啟動或停止應用程式*工作來啟動和停止受管理裝置上的卡巴斯基應用程式。

若要建立啟動或停止應用程式工作：

1. 在主功能表中，轉至 **裝置** → **工作**。
2. 點擊**新增**。
   新工作精靈啟動。使用**下一步**按鈕進行精靈。
3. 在**應用程式**下拉清單，選取要為其建立工作的應用程式。
   如果您之前已為這些應用程式新增了管理 Web 外掛程式，則卡巴斯基應用程式將顯示在清單中。
4. 在**工作類型**清單中，選取**應用程式啟動**工作。
5. 在**工作名稱**欄位，指定新工作的名稱。
   工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。
6. 選取要將工作分配到的裝置。
7. 在**應用程式**視窗，執行以下操作：
   - 選取要為其建立工作的應用程式名稱旁的核取方塊。
   - 選擇**啟動應用程式**或**停止應用程式**選項。
8. 若要修改預設工作設定，請啟用**建立完成時開啟工作詳情**步驟的**完成工作建立**選項。如果您不啟用該選項，工作使用預設設定建立。您可以稍後隨時修改預設設定。

9. 點擊**完成**按鈕。

   工作被建立並顯示在工作清單。

10. 按一下建立的工作的名稱以開啟工作內容視窗。

11. 在工作內容視窗中，依需求指定一般工作設定，然後儲存設定。

    工作被建立和配置。

若要執行工作，請在工作清單選取該工作，然後點擊**開始**按鈕。

行動裝置管理

透過卡巴斯基安全管理中心的行動裝置防護的管理透過使用行動裝置管理功能執行，這需要專用產品授權。如果您要管理組織員工擁有的行動裝置，請啟用和配置行動裝置管理。

行動裝置管理可讓您管理員工的 Android 裝置。該防護由安裝在裝置上的 Kaspersky Endpoint Security for Android 行動應用程式提供。此行動應用程式可確保行動裝置免受 Web 威脅、病毒和其他構成威脅的程式的侵害。若要透過卡巴斯基安全管理中心網頁主控台進行集中管理，您必須在安裝了卡巴斯基安全管理中心網頁主控台的裝置上安裝以下 Web 管理外掛程式：

- Kaspersky Security for Mobile 外掛程式
- Kaspersky Endpoint Security for Android 外掛程式

有關行動裝置的防護部署和管理的資訊，請參閱Kaspersky Security for Mobile 說明。

在卡巴斯基安全管理中心網頁主控台中修改行動裝置管理設定

要修改行動裝置管理設定：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。

   管理伺服器內容視窗將開啟。

2. 在**一般**標籤，選取**附加連接埠**區段。

3. 修改相關設定：

- **為行動裝置開啟連接埠**

  如果啟用該切換開關，則將在管理伺服器上開啟行動裝置連接埠。
  僅在已安裝行動裝置管理元件時才可以使用行動裝置連接埠。
  如果未啟用該切換開關，則管理伺服器上的行動裝置連接埠將不被使用。
  預設情況下已停用該切換開關。

- **行動裝置同步連接埠**

  用於連線行動裝置到管理伺服器的埠號。預設埠號為 13292。
  使用十進位系統記錄。

- **行動裝置啟動連接埠**

  用於將 Kaspersky Endpoint Security for Android 連線到 Kaspersky 啟動伺服器的連接埠。
  預設埠號為 17100。

4. 點擊**儲存**按鈕。

行動裝置現在可以連線到管理伺服器。

取代協力廠商安全應用程式

透過卡巴斯基安全管理中心進行 Kaspersky 安全應用程式的安裝可能需要移除與正在安裝的應用程式不相容的協力廠商軟體。卡巴斯基安全管理中心提供幾種移除協力廠商應用程式的方法。

透過使用安裝程式移除不相容應用程式

該選項僅在基於 Microsoft 管理主控台的管理主控台可用。

移除不相容應用程式的安裝程式方法被各種應用程式支援。如果在該安全應用程式安裝套件的內容視窗中選取（**不相容的應用程式**區域）**自動解除安裝不相容的應用程式**選項，在安裝安全應用程式之前，會自動移除所有不相容的應用程式。

當配置應用程式遠端安裝時移除不相容應用程式

您可以在配置安全應用程式遠端安裝時，啟用**自動解除安裝不相容的應用程式**選項。在基於 Microsoft Management Console (MMC) 的管理主控台，該選項在遠端安裝精靈可用。在卡巴斯基安全管理中心網頁主控台，您可以在防護佈署精靈中找到該選項。當該選項被啟用時，卡巴斯基安全管理中心在安裝安全應用程式到受管理裝置之前移除不相容的應用程式。

說明：

- 管理主控台：使用0遠端安裝精靈移除不相容的應用程式
- 卡巴斯基安全管理中心網頁主控台：安裝前移除不相容的應用程式

透過專用工作移除不相容的應用程式

要移除不相容的應用程式，使用**遠端移除應用程式**工作。該工作應該在安全應用程式安裝工作執行之前執行在裝置。例如，在安裝工作中，您可以選取**在完成其它工作時**作為排程類型，其中其他工作為**遠端解除安裝應用程式**。

該移除方法在安全應用程式無法正確移除不相容應用程式時是很有用的。

管理主控台的操作說明：建立工作。

發現網路裝置

該部分描述網路裝置的搜尋和發現。

卡巴斯基安全管理中心允許您按照指定規則尋找裝置。您可以儲存搜尋結果到文字檔案。

搜尋和發現功能允許您尋找以下裝置：

- 卡巴斯基安全管理中心管理伺服器及其從屬管理伺服器的管理群組中的受管理裝置。
- 由卡巴斯基安全管理中心管理伺服器及其從屬管理伺服器管理的未配置裝置。

情境：發現網路裝置

您必須在安裝安全應用程式之前執行裝置發現。管理伺服器接收有關已發現裝置的資訊，並允許您通過政策管理這些裝置。需要定期進行網路輪詢以更新網路中可用裝置的清單。

在開始網路輪詢之前，請確保已啟用 SMB 協定。否則，卡巴斯基安全管理中心將無法發現輪詢網路中的裝置。要啟用 SMB 協定，請按照您的作業系統的說明進行操作。

網路裝置探索按以下階段進行：

1. **探索裝置**

   快速啟動精靈透過初始裝置發現指引您，並幫助您尋找網路裝置，例如電腦、平板電腦和行動電話。您也可以手動執行裝置發現。

2. **設定排程輪詢**

   決定您要定期使用哪些輪詢類型。啟用所需的類型並設定輪詢排程。您可以參考網路輪詢頻率建議。

3. **設定規則以新增發現的裝置到管理群組（可選）**

如果新裝置出現在您的網路，它們會在常規輪詢中被發現並被自動包含在**未配置的裝置**群組。您可以設定裝置移動規則以自動分配裝置到**受管理裝置**群組。您也可以設定保留規則。

如果跳過步驟 3，新發現的裝置將被分配給**未配置的裝置**群組。如果您想，您可以手動移動這些裝置到**受管理裝置**群組。如果您手動移動這些裝置到**受管理裝置**群組，您可以分析每部裝置的資訊，並決定您是否要移動它到管理群組以及移動到具體哪個群組。

結果

完成情境可以導致如下：

- 卡巴斯基安全管理中心管理伺服器發現網路中的裝置並提供您它們的資訊。
- 未來輪詢被設定並根據指定的排程工作。
- 新發現的裝置按照配置的規則進行排列。（或者，如果未配置規則，裝置將保留在**未配置的裝置**群組中）。

裝置發現

該部分敘述了卡巴斯基安全管理中心中可用的裝置發現類型並給出使用每種類型的資訊。

管理伺服器透過一般輪詢接收網路結構資訊和網路裝置資訊。資訊被記錄到管理伺服器資料庫。管理伺服器可使用下列類型的輪詢：

- **Windows 網路輪詢**。管理伺服器可以執行兩種 Windows 網路輪詢：快速和完整。在快速輪詢過程中，管理伺服器只會從所有網域和工作群組中裝置的 NetBIOS 名稱清單獲取資訊。在完整輪詢中，需要每台用戶端裝置的更多資訊，例如作業系統名稱、IP 位址、DNS 名稱和 NetBIOS 名稱。預設下，快速和完整輪詢都被啟用。Windows 網路輪詢可能發現裝置失敗，例如，如果連接埠 UDP 137、UDP 138、TCP 139 在路由器上或被防火牆關閉。
- **Active Directory 輪詢**。管理伺服器接收 Active Directory 單元結構以及 Active Directory 群組中裝置的 DNS 名稱的資訊。預設情況下已啟用該輪詢類型。如果您使用 Active Directory，我們建議您使用 Active Directory 輪詢；否則，管理伺服器不發現任何裝置。如果您使用 Active Directory 但是一些網路裝置不列為成員，這些裝置無法透過 Active Directory 輪詢發現。
- **IP 範圍輪詢**。管理伺服器將使用 ICMP 封包或 NBNS 通訊協定輪詢指定的 IP 範圍，並收集 IP 範圍內裝置上的一組完整資料。預設情況下已停用該輪詢類型。如果您使用 Windows 網路輪詢和/或 Active Directory 輪詢，不建議您使用該輪詢類型。
- **Zeroconf 輪詢**。透過使用零配置網路（也稱為*零配置*）輪詢 IPv6 網路的發佈點。預設情況下已停用該輪詢類型。如果發佈點執行 Linux，您可以使用 Zeroconf 輪詢。

如果您設定和啟用了裝置移動規則，新發現的裝置會自動包含在**受管理裝置**群組中。如果未啟用移動規則，新發現的裝置被自動包含在**未配置的裝置**群組。

您可以為每種類型修改裝置發現設定。例如，您可能想要修改輪詢排程或者設定是否輪詢整個 Active Directory 樹系還是僅指定網域。

在開始網路輪詢之前，請確保已啟用 SMB 協定。否則，卡巴斯基安全管理中心將無法發現輪詢網路中的裝置。要啟用 SMB 協定，請按照您的作業系統的說明進行操作。

Windows 網路輪詢

關於 Windows 網路輪詢

在快速輪詢過程中，管理伺服器只會從所有網域和工作群組中裝置的 NetBIOS 名稱清單獲取資訊。在完整輪詢中，以下資訊被從每個用戶端裝置請求：

- 作業系統名稱
- IP 位址
- DNS 名稱
- NetBIOS 名稱

快速輪詢和完整輪詢都需要以下：

- 連接埠 UDP 137/138、TCP 139、UDP 445、TCP 445 必須在網路中可用。
- SMB 協定已啟用。
- 必須使用 Microsoft Computer Browser 服務，且主瀏覽器電腦必須在管理伺服器上啟用。
- 必須使用 Microsoft Computer Browser 服務，且主瀏覽器電腦必須在用戶端裝置上啟用。
  - 至少一台裝置上，如果網路裝置數量不超過 32。
  - 對每 32 台網路裝置至少一台裝置上。

完整輪詢僅在快速輪詢至少執行了一次時可以執行。

檢視和修改 Windows 網路輪詢設定

要修改 Windows 網路輪詢內容：

1. 在主功能表中，轉至 **發現和佈署 → 發現 → Windows 網域**。
2. 點擊**內容**按鈕。
   Windows 網域內容視窗將開啟。
3. 透過**啟用 Windows 網路輪詢**開關按鈕啟用或停用 Windows 網路輪詢。

4. 設定輪詢排程。預設下，快速輪詢每 15 分鐘執行一次，完整輪詢每 60 分鐘執行一次。

   輪詢排程選項：

   - **每 N 天**

     輪詢定期執行，按照指定天數間隔，從指定的日期和時間開始。

     預設下，輪詢每天執行一次，從目前系統日期和時間開始。

   - **每 N 分鐘**

     輪詢定期執行，按照指定分鐘間隔，從指定的時間開始。

   - **按每星期中的指定日**

     輪詢定期執行，在指定星期的指定時間。

   - **每個月在所選週的指定天**

     輪詢定期執行，在指定月日的指定時間。

   - **執行錯過的工作**

     如果在排程輪詢期間管理伺服器被切換掉或不可用，管理伺服器可以在切換回來後立即啟動輪詢，或者等待下次排程輪詢。

     如果啟用該選項，管理伺服器在它切換回來後立即啟動輪詢。

     如果停用該選項，管理伺服器等待下一次排程輪詢。

     預設情況下已停用該選項。

5. 點擊**儲存**按鈕。

   內容被儲存並套用到所有發現的 Windows 網域和工作群組。

手動執行輪詢

要立即執行輪詢，

點擊**開始快速輪詢** 或**開始完整輪詢**。

輪詢完成時，您可透過選取網域名稱旁的核取方塊，在 **Windows 網域**頁面檢視已發現裝置的清單並點擊**裝置**按鈕。

Active Directory 輪詢

如果您使用 Active Directory 則使用 Active Directory 輪詢；否則，建議使用其他類型的輪詢。如果您使用 Active Directory 但是一些網路裝置不列為成員，這些裝置無法透過使用 Active Directory 輪詢發現。

卡巴斯基安全管理中心傳送請求到網域控制站並接收 Active Directory 裝置結構。Active Directory 輪詢按小時執行。

在開始網路輪詢之前，請確保已啟用 SMB 協定。否則，卡巴斯基安全管理中心將無法發現輪詢網路中的裝置。要啟用 SMB 協定，請按照您的作業系統的說明進行操作。

瀏覽和修改 Active Directory 輪詢設定

要瀏覽和修改 Active Directory 輪詢設定：

1. 在主功能表中，轉至 **發現和佈署 → 發現 → Active Directory**。
2. 點擊**內容**按鈕。

   Active Directory 內容視窗開啟。
3. 在 Active Directory 內容視窗，您可以定義以下設定：

   a. 使用開關按鈕開啟或關閉 Active Directory 輪詢。

   b. 變更輪詢排程。

   預設間隔是一小時。下次輪詢接收的資料取代舊資料。

   c. 配置進階設定以選取輪詢範圍：

   - 卡巴斯基安全管理中心所屬的 Active Directory 網域
   - 卡巴斯基安全管理中心所屬的網域樹系
   - Active Directory 網域的指定清單

   要新增網域到輪詢範圍，選取域選項，點擊**新增**按鈕，然後指定網域控制站位址和存取它的帳戶名稱密碼。
4. 要套用新設定，請按一下**儲存**按鈕。

新設定被套用到 Active Directory 輪詢。

手動執行輪詢

要立即執行輪詢，

點擊**開始輪詢**。

檢視 Active Directory 輪詢結果：

要檢視 Active Directory 輪詢結果：

1. 在主功能表中，轉至 **發現和佈署 → 發現 → Active Directory**。

   發現的組織單元清單被顯示。

2. 如有需要，請選取組織單元，之後點擊**裝置**按鈕。

   組織單元中的裝置清單被顯示。

您可以搜尋清單和篩選結果。

IP 範圍輪詢

開始，卡巴斯基安全管理中心從其所在裝置的網路設定獲取 IP 輪詢範圍。如果裝置位址是 192.168.0.1 且子網路遮罩是 255.255.255.0，卡巴斯基安全管理中心自動包含網路 192.168.0.0/24 到輪詢位址。卡巴斯基安全管理中心從 192.168.0.1 到 192.168.0.254 之間輪詢所有位址。

如果您使用 Windows 網路輪詢和/或 Active Directory 輪詢，則不建議您使用 IP 範圍輪詢。

卡巴斯基安全管理中心可以透過反向 DNS 查找或使用 NBNS 協定輪詢 IP 範圍：

- **反向 DNS 查找**

  卡巴斯基安全管理中心嘗試使用標準 DNS 請求為指定範圍的每個 IP 位址執行反向名稱解析到 DNS 名稱。如果該操作成功，伺服器傳送 `ICMP ECHO REQUEST`（和 ping 指令相同）到所接收名稱。如果裝置回應，其資訊被新增到卡巴斯基安全管理中心資料庫。反向名稱解析對於排除具有 IP 位址但不是電腦的網路裝置是必要的，例如網路印表機或路由器。

  該輪詢方法依賴正確配置的本機 DNS 服務。它必須具有反向查詢網域。在使用 Active Directory 的網路中，此類網域被自動維護。但是在這些網路中，IP 子網路輪詢不比 Active Directory 輪詢提供更多資訊。而且，小網路的管理員經常不配置反向查詢區，因為它對許多網路服務來說是不必要的。由於所有這些原因，IP 子網路輪詢預設被停用。

- **NBNS 協定**

  如果由於某種原因無法在您的網路中進行反向名稱解析，卡巴斯基安全管理中心將使用 NBNS 協定來輪詢 IP 範圍。如果對 IP 位址的請求返回 NetBIOS 名稱，則有關此裝置的資訊將被新增到卡巴斯基安全管理中心資料庫。

在開始網路輪詢之前，請確保已啟用 SMB 協定。否則，卡巴斯基安全管理中心將無法發現輪詢網路中的裝置。要啟用 SMB 協定，請按照您的作業系統的說明進行操作。

瀏覽和修改 IP 範圍輪詢設定

要瀏覽和修改 IP 範圍輪詢設定：

1. 在主功能表中，轉至 **發現和佈署 → 發現 → IP 範圍**。

2. 點擊**內容**按鈕。

   IP 輪詢內容視窗將開啟。

3. 透過使用**允許輪詢**切換按鈕來啟用或停用 IP 輪詢。

4. 設定輪詢排程。預設下，IP 輪詢每 420 分鐘（七小時）執行一次。

   當指定輪詢間隔時，確保該設定不超過 IP 位址生命週期參數值。如果 IP 位址在 IP 位址生命週期中不被輪詢所驗證，該 IP 位址被從輪詢結果中自動刪除。預設下，輪詢結果的生命期是 24 小時，因為動態 IP 位址（使用 Dynamic Host Configuration Protocol (DHCP)）分配每 24 小時變更一次。

   輪詢排程選項：

   - **每 N 天**

     輪詢定期執行，按照指定天數間隔，從指定的日期和時間開始。

     預設下，輪詢每天執行一次，從目前系統日期和時間開始。

   - **每 N 分鐘**

     輪詢定期執行，按照指定分鐘間隔，從指定的時間開始。

   - **按每星期中的指定日**

     輪詢定期執行，在指定星期的指定時間。

   - **每個月在所選週的指定天**

     輪詢定期執行，在指定月日的指定時間。

   - **執行錯過的工作**

     如果在排程輪詢期間管理伺服器被切換掉或不可用，管理伺服器可以在切換回來後立即啟動輪詢，或者等待下次排程輪詢。

     如果啟用該選項，管理伺服器在它切換回來後立即啟動輪詢。

     如果停用該選項，管理伺服器等待下一次排程輪詢。

     預設情況下已停用該選項。

5. 點擊**儲存**按鈕。

內容封包儲存並套用到所有 IP 範圍。

手動執行輪詢

要立即執行輪詢，

點擊**開始輪詢**。

新增和修改 IP 範圍

開始，卡巴斯基安全管理中心從其所在裝置的網路設定獲取 IP 輪詢範圍。如果裝置位址是 192.168.0.1 且子網路遮罩是 255.255.255.0，卡巴斯基安全管理中心自動包含網路 192.168.0.0/24 到輪詢位址。卡巴斯基安全管理中心從 192.168.0.1 到 192.168.0.254 之間輪詢所有位址。您可以修改自動定義的 IP 範圍或新增自訂 IP 範圍。

您只能為 IPv4 位址建立範圍。如果您啟用 Zeroconf 輪詢，卡巴斯基安全管理中心將輪詢整個網路。

要新增新 IP 範圍：

1. 在主功能表中，轉至 **發現和佈署 → 發現 → IP 範圍**。
2. 若要建立新的 IP 範圍，請點擊**新增**按鈕。
3. 在開啟的視窗，指定以下設定：
   - **IP 範圍名稱**

     IP 範圍名稱。您可能想指定 IP 範圍本身作為名稱，例如，"192.168.0.0/24"。

   - **IP 間隔或子網路位址和遮罩**

     透過指定開始和結束位址或子網路位址和子網路遮罩設定 IP 範圍。您也可透過點擊**瀏覽**按鈕選取其中一個已存在的 IP 範圍。

   - **IP 位址使用期限（小時）**

     當指定該參數時，確保它超過輪詢排程中設定的輪詢間隔。如果 IP 位址在 IP 位址生命週期中不被輪詢所驗證，該 IP 位址被從輪詢結果中自動刪除。預設下，輪詢結果的生命期是 24 小時，因為動態 IP 位址（使用 Dynamic Host Configuration Protocol (DHCP)）分配每 24 小時變更一次。
4. 若您要輪詢子網路或您已新增間隔，請選取**啟用 IP 範圍輪詢**。否則，您新增的子網路或間隔將不被輪詢。
5. 點擊**儲存**按鈕。

新 IP 範圍被新增到 IP 範圍清單。

您可使用**開始輪詢**按鈕分別執行各 IP 範圍的輪詢。輪詢完成時，您可使用**裝置**按鈕檢視已發現裝置的清單。預設下，輪詢結果的壽命是 24 小時，且等於 IP 位址生命週期設定。

要新增子網路到現有 IP 範圍：

1. 在主功能表中，轉至 **發現和佈署 → 發現 → IP 範圍**。
2. 點擊您要新增到子網路的 IP 範圍名稱。
3. 在開啟的視窗中，點擊**新增**按鈕。

4. 透過使用位址或者遮罩指定子網路，或者透過使用 IP 範圍中的第一個和最後一個 IP 位址。或者，透過點擊**瀏覽**按鈕新增現有子網路。

5. 點擊**儲存**按鈕。

   新子網路被新增到 IP 範圍。

6. 點擊**儲存**按鈕。

IP 範圍的新設定被儲存。

您可以新增無限多的子網路。命名 IP 範圍不被允許重疊，IP 範圍中的非命名子網路沒有此限制。您可以對每個 IP 範圍獨立啟用和停用輪詢。

Zeroconf 輪詢

僅基於 Linux 的分發點支援此輪詢類型。

分發點可以輪詢具有 IPv6 位址的裝置的網路。在這種情況下，不會指定 IP 範圍，分發點將使用以下零配置網路（稱為“*零配置*”）輪詢整個網路 。要開始使用 Zeroconf，您必須在分發點上安裝 avahi-browse 公用程式。

若要啟用 Ipv6 網路輪詢：

1. 在主功能表中，轉至 **發現和佈署 → 發現 → IP 範圍**。

2. 點擊**內容**按鈕。

3. 在開啟的視窗中，開啟**使用 Zeroconf 來輪詢 IPv6 網路**切換按鈕。

之後，分發點開始輪詢您的網路。在這種情況下，指定的 IP 範圍將被忽略。

為未配置的裝置配置保留規則

Windows 網路輪詢完成後，發現的裝置被放置到“未配置的裝置”管理群組的子群組。該管理群組可以在**發現和佈署 → 發現 → Windows 網域**中取得。**Windows 網域**資料夾是父群組。它包含以對應網域為名稱的子群組和在輪詢過程中發現的工作群組。父群組可能也包含行動裝置管理群組。您可以為父群組和每個子群組配置未配置的裝置的保留規則。保留規則不取決於裝置發現設定並在裝置發現被停用時也工作。

裝置保留規則不會影響具有一個或多個使用完整磁碟加密進行加密的磁碟機的裝置。此類裝置不會被自動刪除——您只能手動刪除它們。如果您需要刪除帶有加密磁碟機的裝置，請先解密磁碟機，然後再刪除該裝置。

要為未配置的裝置設定保留規則：

1. 在主功能表中，轉至 **發現和佈署 → 發現 → Windows 網域**。
2. 執行以下操作之一：
   - 要配置父群組的設定，請點擊**內容**按鈕。
     Windows 網域內容視窗將開啟。
   - 要配置子群組設定，點擊其名稱。
     子群組內容視窗將開啟。
3. 定義下列設定：
   - **若裝置未活動超過下列天數，則從群組刪除裝置**
     如果啟用該選項，您可以指定從組中自動移除裝置的時間間隔。預設下，該選項也被分發到子群組。預設時間間隔為 7 天。
     預設情況下已啟用該選項。
   - **從父群組繼承**
     如果啟用該選項，裝置在目前群組的保留期從父群組繼承且無法被變更。
     該選項僅對子群組可用。
     預設情況下已啟用該選項。
   - **強制子群組繼承**
     該設定值將被分發到子群組，但在子群組的內容中這些設定被鎖定。
     預設情況下已停用該選項。
4. 點擊**同意**按鈕。

您的變更已儲存並套用。

Kaspersky 應用程式：產品授權和啟動

本章節說明使用受管理的 Kaspersky 應用程式產品授權金鑰的卡巴斯基安全管理中心功能。

卡巴斯基安全管理中心使您可以集中為用戶端裝置上的 Kaspersky 應用程式分發產品授權金鑰、監控其使用情況，以及續約產品授權。

使用卡巴斯基安全管理中心新增產品授權金鑰時，該金鑰的設定會儲存在管理伺服器上。應用程式會根據該資訊產生一份產品授權金鑰使用情況的報告，並通知管理員產品授權金鑰內容中指定的產品授權期滿日期，以及是否違反此限制。您可以在管理伺服器設定內配置產品授權金鑰使用情況的通知。

受管理應用程式的產品授權

安裝到受管理裝置上的 Kaspersky 應用程式必須透過套用產品金鑰檔案或啟動碼到每個應用程式而被授權。金鑰檔案或啟動碼可以按以下方法佈署：

- 自動佈署
- 受管理應用程式安裝套件
- 受管理應用程式的「*新增產品授權金鑰*」工作
- 受管理應用程式的手動啟動

您可以透過上面列出的任何方法新增啟動或備用產品授權金鑰。卡巴斯基應用程式當前使用一個啟動金鑰並儲存一個備用金鑰以在啟動金鑰到期後套用。您為其新增產品授權金鑰的應用程式定義該金鑰是啟動還是備用金鑰。金鑰定義不依賴於您用於新增產品授權金鑰的方法。

自動佈署

如果您使用不同的受管理應用程式且您必須佈署特定金鑰檔案或啟動碼到裝置，請選取其他方法佈署啟動碼或金鑰檔案。

卡巴斯基安全管理中心允許您自動佈署可用產品授權金鑰到裝置。例如，三個產品授權金鑰被儲存在管理伺服器儲存區。您已為所有三個產品授權金鑰選取**自動分發產品授權金鑰到受管理裝置**核取方塊。Kaspersky 安全應用程式—例如，Kaspersky Endpoint Security for Windows—被安裝到組織裝置。發現必須佈署產品授權金鑰的新裝置。應用程式決定，例如，儲存區中的兩個產品授權金鑰可以被佈署到裝置：產品授權金鑰 *Key_1*和產品授權金鑰 *Key_2*。這些產品授權金鑰之一被佈署到裝置。此種情況下，無法預見兩個產品授權金鑰中的哪個將被佈署到裝置，因為自動佈署產品授權金鑰不提供給任何管理員活動。

當佈署產品授權金鑰時，裝置為該產品授權金鑰重新計算。您必須確保佈署產品授權金鑰的裝置數量不超過產品授權限制。如果裝置數量超過產品授權限制，所有不被產品授權覆蓋的裝置將被分配緊急狀態。

佈署之前，您必須新增產品授權金鑰或啟動碼到管理伺服器儲存區。

說明：

- 管理主控台：
  - 新增產品授權金鑰到管理伺服器儲存區
  - 自動分發產品授權金鑰

  或
- 卡巴斯基安全管理中心網頁主控台：
  - 新增產品授權金鑰到管理伺服器儲存區
  - 自動分發產品授權金鑰

請注意，在以下情況下，自動分發的產品授權金鑰可能不會顯示在虛擬管理伺服器儲存庫中：

- 產品授權金鑰對於應用程式無效。
- 虛擬管理伺服器沒有受管理裝置。
- 產品授權金鑰已用於由另一個虛擬管理伺服器管理的裝置，並且已達到裝置數量限制。

新增金鑰檔案或啟動碼至受管理應用程式安裝套件

對於安全應用程式，該選項不被建議。新增至安裝套件的產品授權金鑰或啟動碼可能會有安全風險。

如果您使用安裝套件安裝受管理應用程式，您可以在該安裝套件中或在應用程式政策中指定啟動碼或金鑰檔案。產品授權金鑰將在下一次裝置與管理伺服器同步時被佈署到受管理裝置。

說明：

- 管理主控台：
  - 建立安裝套件
  - 安裝應用程式到用戶端裝置

  或
- 卡巴斯基安全管理中心網頁主控台：新增產品授權金鑰到安裝套件

透過為受管理應用程式新增產品授權金鑰工作佈署。

如果您選擇為受管理應用程式*新增產品授權金鑰*工作，您可以選取要佈署到裝置的產品授權金鑰，並以任何便捷方法選取裝置–例如，選取管理群組或裝置分類。

佈署之前，您必須新增產品授權金鑰或啟動碼到管理伺服器儲存區。

說明：

- 管理主控台：
  - 新增產品授權金鑰到管理伺服器儲存區
  - 佈署產品授權金鑰到用戶端裝置

  或
- 卡巴斯基安全管理中心網頁主控台：
  - 新增產品授權金鑰到管理伺服器儲存區
  - 佈署產品授權金鑰到用戶端裝置

手動新增啟動碼或金鑰檔案至裝置

您可以啟動本機安裝的 Kaspersky 應用程式，透過使用應用程式介面提供的工具。請參考已安裝應用程式的文件。

新增產品授權金鑰到管理伺服器儲存區

要新增產品授權金鑰到管理伺服器儲存區：

1. 在主功能表中，轉至 **操作 → 產品授權 → Kaspersky 產品授權**。
2. 點擊**新增**按鈕。
3. 選取您要新增的內容：
   - **新增金鑰檔案**
     點擊**選取金鑰檔案**按鈕並瀏覽至要新增的金鑰檔案。
   - **輸入啟動碼**
     指定文字欄位中的啟動碼並點擊**傳送**按鈕。
4. 點擊**關閉**按鈕。

產品授權金鑰或幾個產品授權金鑰被新增到管理伺服器儲存區。

佈署產品授權金鑰到用戶端裝置

卡巴斯基安全管理中心網頁主控台允許您自動或是透過**應用程式啟動**工作，將產品授權金鑰分發至用戶端裝置。您可以使用該工作將金鑰分發到特定裝置群組。在透過工作分發產品授權金鑰期間，系統不會將產品授權的裝置數量限制納入考慮。使用自動金鑰分發可在達到許可限制時自動停止分發產品授權金鑰。

如果您啟用自動分發產品授權金鑰，請勿建立**應用程式啟動**工作來將該金鑰分發到用戶端裝置。否則，管理伺服器的負載會因頻繁同步而增加。

部署前，請新增產品授權金鑰到管理伺服器儲存區。

*若要透過**應用程式啟動**工作將產品授權金鑰分發至用戶端裝置：*

1. 在主功能表中，轉至 **裝置 → 工作**。
2. 點擊**新增**。
   新工作精靈啟動。使用**下一步**按鈕進行精靈。
3. 在**應用程式**下拉清單，選取要為其新增產品授權金鑰的應用程式。
4. 在**工作類型**清單中，選取**應用程式啟動**工作。

5. 在**工作名稱**欄位，指定新工作的名稱。

6. 選取要將工作分配到的裝置。

7. 在精靈的**選取產品授權金鑰**步驟，點擊**新增金鑰**連結以新增產品授權金鑰。

8. 在金鑰新增窗格，使用以下選項之一新增產品授權金鑰：

   如果您在建立**應用程式啟動**工作之前，就已將產品授權金鑰新增至管理伺服器儲存區，則不需要新增產品授權金鑰。

   - 選取**輸入啟動碼**選項以輸入啟動碼，然後執行下列操作：

     a. 指定啟動碼，然後點擊**傳送**按鈕。
     金鑰新增窗格中即會顯示產品授權金鑰的資訊。

     b. 點擊**儲存**按鈕。

     如果要自動將產品授權金鑰分發至受管理裝置，請啟用**自動分發產品授權金鑰到受管理裝置**選項。

     金鑰新增窗格即會關閉。

   - 選取**新增金鑰檔案**選項以新增金鑰檔案，然後執行以下操作：

     a. 點擊**選取金鑰檔案**按鈕。

     b. 在開啟的視窗中，選取金鑰檔案，然後點擊**開啟**按鈕。
     產品授權金鑰新增窗格中即會顯示產品授權金鑰的資訊。

     c. 點擊**儲存**按鈕。

     如果要自動將產品授權金鑰分發至受管理裝置，請啟用**自動分發產品授權金鑰到受管理裝置**選項。

     金鑰新增窗格即會關閉。

9. 在金鑰表格中選取產品授權金鑰。

10. 如果要取代作用中產品授權金鑰，請在精靈的**產品授權資訊**步驟中清除預設的**用作備用金鑰**核取方塊。
    例如，當組織發生變化並且裝置上需要另一個組織的金鑰時，或者重新頒發了金鑰、新產品授權早於目前的產品授權到期時，就需要這樣做。為了避免錯誤，您必須清除**用作備用金鑰**核取方塊。
    如果您想了解有關將產品授權金鑰新增到卡巴斯基安全管理中心時可能出現的問題及其解決方法的更多資訊，請參閱卡巴斯基安全管理中心知識庫。

11. 在精靈的**完成工作建立**步驟中啟用**建立完成時開啟工作詳情**選項，即可修改預設工作設定。
    如果您不啟用該選項，工作將以預設設定來建立。您可以稍後再修改預設設定。

12. 點擊**完成**按鈕。

    精靈即會建立物件。如果您啟用了**建立完成時開啟工作詳情**選項，工作內容視窗即會自動開啟。在此視窗中，您可以指定一般工作設定，並視需要變更在工作建立期間指定的設定。

    > 您也可以透過在工作清單中點擊所建立工作的名稱，開啟工作內容視窗。

    工作隨即受到建立、設定，並顯示在工作清單。

13. 若要執行工作，請在工作清單選取該工作，然後點擊**開始**按鈕。

    您也可以在工作內容視窗的**排程**頁籤上，設定工作啟動排程。

    如需排程啟動設定的詳細說明，請參閱一般工作設定。

工作完成後，產品授權金鑰即會佈署到所選裝置。

自動分發產品授權金鑰

如果金鑰位於管理伺服器上的產品授權金鑰儲存區中，則卡巴斯基安全管理中心允許將這些產品授權金鑰自動發佈至受管理裝置。

要將產品授權金鑰自動分發至受管理裝置，請執行以下操作：

1. 在主功能表中，轉至 **操作 → 產品授權 → Kaspersky 產品授權**。
2. 選取您要自動發佈到裝置的產品授權金鑰名稱。
3. 在開啟的產品授權金鑰內容視窗中，選取**自動分發產品授權金鑰到受管理裝置**核取方塊。
4. 點擊**儲存**按鈕。

產品授權金鑰將被自動分發到所有相容的裝置。

產品授權金鑰發佈是使用網路代理執行的。沒有為應用程式建立產品授權金鑰發佈工作。

在自動分發產品授權金鑰過程中，系統會考慮產品授權對裝置數量的限制。授權限制會在產品授權金鑰的內容中設定。若達授權限制，則會自動停止分發此裝置上的產品授權金鑰。

請注意，在以下情況下，自動分發的產品授權金鑰可能不會顯示在虛擬管理伺服器儲存庫中：

- 產品授權金鑰對於應用程式無效。
- 虛擬管理伺服器沒有受管理裝置。
- 產品授權金鑰已用於由另一個虛擬管理伺服器管理的裝置，並且已達到裝置數量限制。

虛擬管理伺服器會自動從其儲存區和管理伺服器的儲存區中分發產品授權金鑰。我們建議您：

- 使用*新增產品授權金鑰*工作以選擇必須部署到裝置的產品授權金鑰。
- 避免在虛擬管理伺服器設定中停用**允許從該虛擬管理伺服器自動佈署產品授權金鑰到它的裝置**選項。否則，虛擬管理伺服器將不會向裝置分發產品授權金鑰，包括管理伺服器儲存區中的產品授權金鑰。

如果您在產品授權金鑰內容視窗中選擇**自動分發產品授權金鑰到受管理裝置**核取方塊，產品授權金鑰會立即在您的網路上分發。如果不選擇此選項，您可以之後使用工作分發產品授權金鑰。

自動分發在主管理伺服器上配置的產品授權金鑰不會延伸到由非虛擬從屬管理伺服器管理的裝置。

檢視使用中產品授權金鑰的相關資訊

要檢視新增到管理伺服器儲存區的產品授權金鑰清單：

在主功能表中，轉至 **操作 → 產品授權 → Kaspersky 產品授權**。

顯示清單包含新增至管理伺服器儲存區的金鑰檔案與啟動碼。

要檢視關於產品授權金鑰的詳細資訊：

1. 在主功能表中，轉至 **操作 → 產品授權 → Kaspersky 產品授權**。
2. 點擊所需產品授權金鑰的名稱。

在開啟的產品授權金鑰內容視窗，您可以檢視：

- 在**一般**頁籤—產品授權金鑰的主資訊
- 在**裝置**頁籤—用戶端裝置清單，裝置中的產品授權金鑰用來啟動已安裝的 Kaspersky 應用程式

要檢視哪些產品授權金鑰被佈署到特定用戶端裝置：

1. 在主功能表中，轉至 **裝置 → 受管理裝置**。
2. 點擊所需裝置的名稱。
3. 在開啟的裝置內容視窗中，點擊**應用程式**標籤。
4. 點擊您要檢視其產品授權金鑰資訊的應用程式名稱。
5. 在開啟的應用程式內容視窗中，選擇**一般**頁籤，接著開啟**產品授權**區域。

關於啟用與備用產品授權金鑰主資訊隨即顯示。

要定義虛擬管理伺服器產品授權金鑰的即時設定，管理伺服器每天至少傳送一次請求到 Kaspersky 啟動伺服器。如果無法使用系統 DNS 存取伺服器，則應用程式使用公用 DNS 伺服器。

從儲存區移除產品授權金鑰

當您為管理伺服器附加功能（例如弱點和修補程式管理或行動裝置管理）移除啟動產品授權金鑰時，對應功能變得不可用。若已新增備用產品授權金鑰，備用產品授權金鑰會在移除先前啟用的產品授權金鑰後，自動成為啟動產品授權金鑰。

當您移除佈署到受管理裝置上的啟動產品授權金鑰時，應用程式將繼續工作在受管理裝置。

若要從管理伺服器儲存區移除金鑰檔案或啟動碼：

1. 檢查管理伺服器並未使用您要移除的金鑰檔案或啟動碼。如果管理伺服器使用了您將刪除的金鑰，您將無法移除該金鑰。若要執行檢查：

   a. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。

   管理伺服器內容視窗將開啟。

   b. 在**一般**頁簽上，選取**產品授權金鑰**區段。

   c. 如果所需的金鑰檔案或啟動碼顯示在開啟的區段中，請按一下**刪除啟動產品授權金鑰**按鈕，然後確認操作。在此之後，管理伺服器將不會使用移除的產品授權金鑰，但該金鑰仍保留在管理伺服器儲存區中。如果未顯示所需的金鑰檔案或啟動碼，表示管理伺服器不使用金鑰檔案或啟動碼。

2. 在主功能表中，轉至 **操作 → 產品授權 → Kaspersky 產品授權**。

3. 選擇所需的金鑰檔案或激活碼，然後點擊**刪除**按鈕。

選取的金鑰檔案或啟動碼已從儲存區移除。

您可以再次新增一個已移除的產品授權金鑰或新增一個新產品授權金鑰。

撤銷最終使用者產品授權協議的許可

若您決定停止防護您的一些用戶端裝置，您可針對任何受管理的 Kaspersky 應用程式撤銷最終使用者產品授權協議 (EULA)。您必須先解除安裝所選的應用程式在撤銷其 EULA。

在虛擬管理伺服器上接受的 EULA 可以在虛擬管理伺服器或主管理伺服器上撤銷。在主管理伺服器上接受的 EULA 只能在主管理伺服器上撤銷。

若要撤銷 Kaspersky 受管理應用程式的 EULA：

1. 在開啟的管理伺服器內容視窗中的**一般**頁籤，選取**最終使用者產品授權協議**區段。

   會顯示在建立安裝套件時、在無縫安裝更新時或在佈署 Kaspersky Security for Mobile 時接受的 EULA 清單。

2. 在清單中，選取您要撤銷協議的 EULA。

   您可以檢視 EULA 的下列內容：

   - 接受 EULA 的日期
   - 接受 EULA 的使用者名稱

3. 點擊任何 EULA 的接受日期以開啟其顯示以下資料的內容視窗：

   - 接受 EULA 的使用者名稱
   - 接受 EULA 的日期
   - EULA 的唯一識別碼 (UID)
   - EULA 的完整內容
   - EULA 連結的物件清單（安裝套件、無縫更新、行動應用程式），以及其各自的名稱與類型

4. 在 EULA 內容視窗的下部，點擊**撤銷產品授權協議**按鈕。

   若存在任何物件（安裝套件與其各自工作）防止撤銷 EULA，則會顯示對應的通知。刪除這些物件前，您無法處理撤銷。

   在開啟的視窗中，系統會告知您必須先解除安裝對應至 EULA 的 Kaspersky 應用程式。

5. 按一下按鈕以確認撤銷。

EULA 已撤銷。這不會在顯示於 **最終使用者產品授權協議** 區段的產品授權協議清單中。EULA 內容視窗關閉；應用程式將不再繼續安裝。

續約 Kaspersky 應用程式的產品授權

您可以續約已過期或即將過期（少於 30 天）的 Kaspersky 應用程式產品授權。

要續約過期的產品授權或即將過期的產品授權：

1. 做以下之一：

   - 在主功能表中，轉至 **操作 → 產品授權 → Kaspersky 產品授權**。
   - 在主功能表中，轉到**監控和報告 → 控制板**，然後點擊通知旁邊的"**檢視即將到期的產品授權**"連接。

   Kaspersky 產品授權 視窗將開啟，您可以在其中檢視和續約產品授權。

2. 點擊所需產品授權旁邊的**續約產品授權**連接。

   點擊產品授權續約連接，即表示您同意向 Kaspersky 傳輸關於卡巴斯基安全管理中心的以下資訊：其版本、您使用的當地語係化版本、軟體產品授權 ID（即您要續約的產品授權 ID）以及您是否透過合作夥伴公司購買了產品授權。

3. 在開啟的產品授權續約服務視窗中，按照說明續約產品授權。

   產品授權已續約。

在卡巴斯基安全管理中心 網頁主控台中，當產品授權即將到期時，會根據以下排程顯示通知：

- 到期前 30 天
- 到期前 7 天
- 到期前 3 天
- 到期前 24 小時
- 產品授權過期時

使用卡巴斯基市場選擇卡巴斯基商業解決方案

市場是主功能表中的一個區段，可讓您檢視整個 Kaspersky 業務解決方案範圍，選擇您需要的解決方案，然後在 Kaspersky 網站上進行購買。您可以使用篩選器僅檢視適合您的組織和資訊安全系統要求的那些解決方案。當您選擇一個解決方案時，卡巴斯基安全管理中心會將您重新導向到 Kaspersky 網站上的相關網頁，以了解有關該解決方案的更多資訊。每個網頁都可讓您繼續購買或包含有關購買流程的指示。

在 **市場** 區段，您可以使用以下條件篩選 Kaspersky 解決方案：

- 您想要防護的裝置（端點、伺服器和其他類型的資產）數量：
  - 50–250
  - 250–1000
  - 大於 1000
- 貴組織資訊安全團隊的成熟度：
  - **基金會**

    此級別對於只有一個 IT 團隊的企業來說很典型。自動封鎖最大可能數量的威脅。
  - **最佳**

    此級別對於在 IT 團隊內具有特定 IT 安全功能的企業很典型。在此級別，公司需要能夠讓他們應對商品威脅和繞過現有預防機制的威脅的解決方案。
  - **專家**

    此級別對於具有復雜和分佈式 IT 環境的企業來說很典型。IT 安全團隊成熟或公司有 SOC（安全運營中心）團隊。所需解決方案使公司能夠應對複雜的威脅和有針對性的攻擊。
- 您想要防護的資產類型：
  - **端點**：員工工作站、實體和虛擬機、內嵌系統
  - **伺服器**: 實體和虛擬伺服器
  - **雲端**：公有、私有或混合雲端環境；雲端服務
  - **網路**：區域網路，IT 基礎結構
  - **服務**：Kaspersky 提供的安全相關服務

若要查找和購買 Kaspersky 業務解決方案：

1. 在主功能表中，轉至 **市場**。
   預設情況下，該區段顯示所有可用的 Kaspersky 業務解決方案。
2. 要僅檢視適合您組織的解決方案，請在篩選器中選擇所需的值。
3. 點擊您想要購買或了解更多資訊的解決方案。

   您將被重新導向到解決方案網頁。您可以按照熒幕上的指示進行購買。

配置網路防護

本節包含有關政策和工作的手動配置、使用者角色、建構管理群組結構和工作階層的資訊。

情境：配置網路防護

快速啟動精靈會建立含預設設定的政策與工作。這些設定可能對組織來說並不是最佳設定，甚至不被允許。因此，建議您微調這些政策與工作，並在您網路有需求時，建立其他政策與工作。

先決條件

在您開始之前，確保您已做了如下：

- 已安裝卡巴斯基安全管理中心管理伺服器
- 已安裝卡巴斯基安全管理中心網頁主控台（選用）
- 完成卡巴斯基安全管理中心主安裝情境
- 完成快速設定精靈，或在**受管理裝置**管理群組手動建立以下政策和工作：
  - Kaspersky Endpoint Security 政策
  - 更新 Kaspersky Endpoint Security 的群組工作
  - 網路代理政策
  - *尋找弱點和必要更新*工作

設定要以階段進行的網路防護：

1. **設定和傳播 Kaspersky 應用程式政策和政策設定檔**

   要為安裝在受管理裝置上的 Kaspersky 應用程式配置和傳播設定，您可以使用兩種不同的安全管理方法—以裝置為中心或以使用者為中心。這兩種方法也可以被合併。要實現以裝置為中心的安全管理，您可以使用提供在基於 Microsoft Management Console 的管理主控台或卡巴斯基安全管理中心網頁主控台的工具。以使用者為中心的安全管理僅可以透過卡巴斯基安全管理中心網頁主控台實現。

2. **配置工作以遠端管理 Kaspersky 應用程式**

   檢查使用快速啟動精靈建立的工作並調整它們，如有必要。

   說明：

   - 管理主控台：
     - 為 Kaspersky Endpoint Security 設定群組工作
     - 排程「尋找弱點和所需更新」工作
   - 卡巴斯基安全管理中心網頁主控台：
     - 為 Kaspersky Endpoint Security 設定群組工作
     - 「尋找弱點和所需更新」工作設定

   如果必要，建立附加工作以管理安裝在用戶端裝置上的 Kaspersky 應用程式。

3. **評估和限制資料庫上的事件負載**

   受管應用程式操作相關的事件資訊將被從用戶端電腦上傳輸並記錄至管理伺服器資料庫。要降低管理伺服器負載，評估和限制可以儲存在資料庫的最大事件數量。

   說明：

   - 管理主控台：設定事件最大數量
   - 卡巴斯基安全管理中心網頁主控台：設定事件最大數量

結果

當您完成該情境時，您將透過配置 Kaspersky 應用程式、工作和管理伺服器接收的事件來防護您的網路：

- Kaspersky 應用程式會根據政策與政策設定檔設定。
- 應用程式會透過一組工作管理。
- 儲存在資料庫的事件數量上限已設定。

當網路防護配置完成時，您可以繼續配置 Kaspersky 資料庫和應用程式的一般更新。

有關如何配置針對 Kaspersky Sandbox 偵測到的威脅的自動回應的詳細資訊，請參閱 Kaspersky Sandbox 2.0 線上說明。

關於以裝置為中心和以使用者為中心的安全管理方法

您可以從裝置功能的立場和從使用者角色的立場管理安全設定。第一種方法叫做*以裝置為中心的安全管理*，第二種叫做*以使用者為中心的安全管理*。要應用不同的應用程式設定到不同的裝置，您可以使用兩種方法的任意或組合。要實現以裝置為中心的安全管理，您可以使用提供在基於 Microsoft Management Console 的管理主控台或卡巴斯基安全管理中心網頁主控台的工具。以使用者為中心的安全管理僅可以透過卡巴斯基安全管理中心網頁主控台實現。

裝置特定安全性管理可讓您根據裝置特定的功能，套用不同的安全應用程式設定至受管理裝置。例如，您可套用不同設定至分配在不同管理群組中的裝置。您也可在 Active Directory 根據裝置使用量或其硬體規格來區分裝置。

以使用者為中心的安全性管理可讓您套用不同安全應用程式設定至不同的使用者角色。您可建立一些使用者角色，將適當的使用者角色指派給每位使用者，並將不同的應用程式設定定義至不同角色使用者擁有的裝置。例如，您可能要應用不同的應用程式設定到會計和人力資源 (HR) 人員的裝置。結果，當實現了以使用者為中心的安全管理時，每個部門—財務部門和人事部門—具有自己的 Kaspersky 應用程式設定配置。設定配置定義了哪些應用程式設定可以被使用者變更以及哪些被強制設定並被管理員鎖定。

透過使用以使用者為中心的安全管理，您可以應用特別應用程式設定到單個使用者。這可能用在員工在公司有獨一角色或您要監控與個別人的裝置相關的安全事故時。取決於該員工在公司的角色，您可以延伸或限制該員工變更應用程式設定的權限。例如，您可能要延伸在本機辦公室管理用戶端裝置的系統管理員的權限。

您也可以組合以裝置為中心的安全管理和以使用者為中心的安全管理方法。例如，您可以為每個管理群組設定特別的應用程式政策，然後為一個或幾個使用者角色建立政策設定檔。在此情況下，政策和政策設定檔會按照以下優先順序加以套用：

1. 為以裝置為中心的安全管理建立的政策被應用。
2. 政策設定檔會根據政策設定檔優先順序內容加以修改。
3. 政策被與使用者角色關聯的政策設定檔修改。

政策設定和傳播：以裝置為中心的方法

當您完成該方案後，應用程式將在所有受管理裝置上被設定，與您定義的應用程式政策和政策設定檔一致。

先決條件

開始前，請確保您已安裝了卡巴斯基安全管理中心管理伺服器和卡巴斯基安全管理中心網頁主控台（選用）。如果您安裝了卡巴斯基安全管理中心網頁主控台，您可能也想考慮以使用者為中心的安全管理作為以裝置為中心的安全管理的備選或附加選項。

階段

以裝置為中心的 Kaspersky 應用程式管理情境包含以下步驟：

1. **管理應用程式政策**

   透過為每個應用程式建立政策來配置安裝在受管理裝置上的 Kaspersky 應用程式設定。政策集將被傳播到用戶端裝置。

   當您在快速啟動精靈配置您網路的防護時，卡巴斯基安全管理中心會為以下應用程式建立預設政策。

   - Kaspersky Endpoint Security for Windows—適用於 Windows 用戶端裝置
   - Kaspersky Endpoint Security for Linux—適用於 Linux 用戶端裝置

   如果您透過使用該精靈完成了設定過程，您不必為該應用程式建立新政策。轉到 Kaspersky Endpoint Security 政策的手動設定。

如果您有幾個管理伺服器和/或管理群組的層級結構，次要管理伺服器和子管理伺服器預設從主要管理伺服器繼承政策。您可以強制子群組和從屬管理伺服器的繼承以防止上流政策設定的修改。如果您僅要一部分設定被強制繼承，您可以在上游政策中鎖定它們。剩餘未鎖定的設定將可以在下流政策中修改。建立的政策層級將允許您有效管理管理群組中的裝置。

說明：

- 管理主控台：建立政策
- 卡巴斯基安全管理中心網頁主控台：建立政策

2 建立政策設定檔（可選）

如果您想讓單一管理群組中的裝置在不同政策設定下執行，為這些裝置建立政策設定檔。政策設定檔是政策設定的命名子集。子集會連同政策一起分發至目標裝置，並根據名為*設定檔啟動條件*的特別條件來作為輔助政策。設定檔僅包含與「基本」政策不同的設定，並在受管理裝置上活動。

透過使用設定檔啟動條件您可以應用不同的政策設定檔，例如，到特定單元中的裝置或到 Active Directory 安全群組，具有特別硬體設定或被特別標籤標記。使用標籤篩選滿足特別標準的裝置。例如，您可以建立叫做 *Windows* 的標籤，使用該標籤標記所有執行 Windows 作業系統的裝置，然後指定該標籤作為政策設定檔啟動條件。結果，安裝在所有 Windows 裝置上的 Kaspersky 應用程式將被使用它們自己的政策設定檔管理。

說明：

- 管理主控台：
  - 建立政策設定檔
  - 建立政策設定檔啟動規則
- 卡巴斯基安全管理中心網頁主控台：
  - 建立政策設定檔
  - 建立政策設定檔啟動規則

3 傳播政策和政策設定檔到受管理裝置

預設情況下，管理伺服器每 15 分鐘自動與受管理裝置同步一次。您可以避免自動同步並透過使用強制同步指令手動執行同步。在您建立或更改政策或政策設定檔之後，系統也會強制同步。同步過程中，新的或變更的政策和政策設定檔被傳播到受管理裝置。

如果您使用卡巴斯基安全管理中心網頁主控台，您可以檢查政策和政策設定檔是否被傳送到裝置。卡巴斯基安全管理中心在裝置內容中指定傳送日期和時間。

說明：

- 管理主控台：強制同步
- 卡巴斯基安全管理中心網頁主控台：強制同步

結果

當以裝置為中心的情境完成時，Kaspersky 應用程式根據指定的設定被設定並透過政策層級傳播。

設定的應用程式政策和政策設定檔將被自動應用到新增到管理群組的新裝置。

政策設定和傳播：以使用者為中心的方法

該部分敘述了以使用者為中心的集中配置安裝到受管理裝置上的 Kaspersky 應用程式的方案。當您完成該方案後，應用程式將在所有受管理裝置上被設定，與您定義的應用程式政策和政策設定檔一致。

此情境可透過卡巴斯基安全管理中心網頁主控台版本 13 或更高版本實現。

先決條件

開始前，請確保您已成功安裝了卡巴斯基安全管理中心管理伺服器和卡巴斯基安全管理中心 網頁主控台，並完成主要安裝情境。您也可能要考慮以裝置為中心的安全管理作為以用於為中心的方案的附加選項。瞭解更多兩個管理方法的詳情。

過程

以使用者為中心的 Kaspersky 應用程式管理方案包含以下步驟：

1. **管理應用程式政策**

   透過為每個應用程式建立政策來配置安裝在受管理裝置上的 Kaspersky 應用程式設定。政策集將被傳播到用戶端裝置。

   當您在快速啟動精靈配置您網路的防護時，卡巴斯基安全管理中心為 Kaspersky Endpoint Security 建立預設政策。如果您透過使用該精靈完成了設定過程，您不必為該應用程式建立新政策。轉到 Kaspersky Endpoint Security 政策的手動設定。

   如果您有幾個管理伺服器和/或管理群組的層級結構，次要管理伺服器和子管理伺服器預設從主要管理伺服器繼承政策。您可以強制子群組和從屬管理伺服器的繼承以防止上流政策設定的修改。如果您僅要一部分設定被強制繼承，您可以在上游政策中鎖定它們。剩餘未鎖定的設定將可以在下流政策中修改。建立的政策層級將允許您有效管理管理群組中的裝置。

   說明：建立一個政策

2. **指定裝置所有者**

   分配受管理裝置到對應使用者。

   說明：指派使用者作為裝置所有者

3. **為您的企業定義使用者角色**

   聯想您企業的員工所做的不同工作。您必須根據他們的角色劃分所有員工。例如，您可以按照部門、專業或職位劃分他們。然後您將需要為每個群組建立使用者角色。記住，每個使用者角色將擁有其自己的政策設定檔，包含該角色特有的應用程式設定。

4. **建立使用者角色**

   為每個員工群組建立和配置使用者角色或使用預定義使用者角色。使用者角色將包含到應用程式功能的存取權限群組。

   說明：建立一個使用者角色

5. **定義每個使用者角色範圍**

對於每個建立的使用者角色，定義使用者和/或安全群組以及管理群組。與使用者角色關聯的設定僅套用到屬於該角色使用者的裝置，以及僅在這些裝置屬於與該角色關聯的群組（包括子群組）時。

說明：編輯使用者角色範圍

6 **建立政策設定檔**

為您企業中的每個使用者角色建立政策設定檔。政策設定檔決定了哪些設定將被根據使用者角色套用到使用者裝置上的應用程式。

說明：建立一個政策設定檔

7 **關聯政策設定檔與使用者角色**

關聯建立的政策設定檔與使用者角色。此後：政策設定檔對具有特定角色的使用者活動。政策設定檔中配置的設定將被套用到安裝於使用者裝置上的 Kaspersky 應用程式。

說明：關聯政策設定檔到角色

8 **傳播政策和政策設定檔到受管理裝置**

預設情況下，管理伺服器每 15 分鐘自動與受管理裝置同步一次。同步過程中，新的或變更的政策和政策設定檔被傳播到受管理裝置。您可以避免自動同步並透過使用強制同步指令手動執行同步。一旦同步完成，政策和政策設定檔被傳送和應用到安裝的 Kaspersky 應用程式。

您可以檢查政策和政策設定檔是否被傳送到了裝置。卡巴斯基安全管理中心在裝置內容中指定傳送日期和時間。

說明：強制同步

結果

當以使用者為中心的方案完成時，Kaspersky 應用程式根據指定的設定被配置並透過政策和政策設定檔層級傳播。

對於新使用者，您將必須建立新帳戶，分配一個建立的使用者角色，並分配裝置到使用者。配置的應用程式政策和政策設定檔將被自動套用到該使用者的新裝置。

網路代理政策設定

若設定網路代理政策：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。
2. 按一下網路代理政策的名稱。

   網路代理政策的內容視窗開啟。

請參閱以下比較表，它詳情描述了如何根據使用的作業係統類型套用設定。

一般

在此頁簽上，您可以修改政策狀態並指定政策設定的繼承：

- 在**政策狀態**下，您可以選取以下政策模式之一：
  - **作用中**

    如果選取該選項，政策將變為啟用狀態。

    預設情況下已選定此選項。

  - **非作用中**

    如果選取該選項，政策將變為不啟用狀態，但它仍然儲存在**政策**資料夾中。如果需要，您可以啟動該政策。

- 在**設定繼承**設定群組中，您可以配置政策繼承：
  - **從父政策繼承設定**

    如果啟用此選項，則政策設定值將繼承上一級群組政策，因而會受到鎖定。

    預設情況下已啟用該選項。

  - **在子政策中強制繼承設定**

    如果啟用此選項，則在套用政策變更之後，程式將執行以下操作：
    - 政策設定的值將被傳送到管理子群組的政策，也就是子政策。
    - 在每個子政策內容視窗的**一般**區域的**設定繼承**區塊，系統將自動選取**從父政策繼承設定**核取方塊。

    如果啟用此方塊，則會鎖定子政策設定。

    預設情況下已停用該選項。

事件配置

在此頁簽上，您可以配置事件記錄和事件通知。事件根據重要性級別分佈在以下部分中的 **事件配置** 頁簽上：

- **功能失效**
- **警告**
- **資訊**

在每個區域，事件類型清單顯示事件類型和在管理伺服器上的預設事件儲存期限（天）。點擊事件類型後，您可以指定清單中已選中的事件記錄和通知設定。預設下，為整個管理伺服器指定的通用通知設定被用於所有事件類型。然後，您可以變更所需事件類型的特別設定。

例如，在**警告**區域，您可以配置**發生了事件**事件類型。例如，當發佈點的可用磁碟空間小於 2 GB（遠端安裝應用程式和下載更新至少需要 4 GB）時，此類事件可能發生。若要配置**發生了事件**事件，按一下它並指定儲存發生的事件的位置以及如何通知它們。

如果網路代理偵測到事件，您可以使用受管理裝置設定。

應用程式設定

設定

在**設定**區域，您可以配置網路代理政策：

- **僅透過發佈點分發檔案**

  如果啟用此選項，受管理裝置上的網路代理僅從發佈點擷取更新。

  如果停用此選項，受管理裝置上的網路代理從發佈點或從管理伺服器擷取更新。

  請注意，受管理裝置上的安全應用程式從每個安全應用程式的更新工作中的來源集中擷取更新。如果您啟用**僅透過發佈點分發檔案**選項，請確保在更新工作中將卡巴斯基安全管理中心設定為更新來源。

  預設情況下已停用該選項。

- **事件佇列最大值 (MB)**

  在該欄位中，您可以指定事件佇列可在磁碟機上佔據的最大空間。

  預設值為 2 MB。

- **應用程式被允許在裝置上獲取政策延伸資料**

  安裝在受管理裝置的網路代理會傳輸已套用安全應用程式政策的相關資訊至安全應用程式（例如 Kaspersky Endpoint Security for Windows）。您可在安全應用程式介面檢視已傳輸的資訊。

  網路代理會傳輸以下資訊：

  - 政策傳送至受管理裝置的時間。
  - 政策傳送至受管理裝置時啟用中政策的名稱。
  - 政策傳送至受管理裝置時漫遊政策的名稱（對於 Linux 版網路代理不可用）。
  - 政策傳送至受管理裝置時，受管理裝置包含的管理群組名稱與連結路徑。
  - 政策傳送至受管理裝置時包含名稱和優先順序的活動政策設定檔的清單。

  您也可使用資訊確保套用正確政策至裝置和用於疑難排解。預設情況下已停用該選項。

- **防護網路代理服務免遭非授權的移除或終止，並防止設定變更**

  如果啟用該選項，則網路代理被安裝到受管理裝置之後，沒有所需權限元件無法被移除或重新設定。網路代理服務無法被停止。此選項對網域控制器沒有影響。

  啟用此選項可防護以本機管理員權限操作的工作站上的網路代理。

  預設情況下已停用該選項。

- **使用解除安裝密碼**

  如果選取該方塊，則按一下**修改**按鈕可以指定 klmover 公用程式和網路代理遠端移除的密碼。

  預設情況下已停用該選項。

儲存區

在**儲存區**區域，您可以選取將其資訊從網路代理傳送到管理伺服器的物件類型。如果網路代理政策禁止本區域中某些設定，則您無法修改這些設定。

- **已安裝應用程式詳情**

  如果啟用此選項，會將安裝在用戶端裝置上的應用程式資訊傳送至管理伺服器。

  預設情況下已啟用該選項。

- **包括修補程式資訊**

  安裝在用戶端裝置的應用程式修補程式的資訊會傳送至管理伺服器。啟用此選項可能增加管理伺服器和 DBMS 的負載，並造成資料庫的流量增加。

  預設情況下已啟用該選項。它僅適用於 Windows。

- **Windows Update 更新詳情**

  如果啟用此選項，會將用戶端裝置上應該安裝的 Microsoft Windows Update 更新資訊傳送至管理伺服器。

  有時候，即使停用該選項，更新也會顯示在**可用更新**區域的裝置屬性中。例如，若組織的裝置具有可由這些更新修復的弱點，就可能會發生這個情況。

  預設情況下已啟用該選項。它僅適用於 Windows。

  有關可選 Microsoft Windows 更新的資訊未被傳送至管理伺服器。

- **軟體弱點和對應更新的詳情**

  若啟用此選項，協力廠商的弱點（包含 Microsoft 軟體）、受管理裝置上偵測到的資訊以及修復協力廠商弱點的軟體更新資訊（不含 Microsoft 軟體）都會傳送至管理伺服器。

  選取此選項（**軟體弱點和對應更新的詳情**）會增加網路負載、管理伺服器磁碟負載和網路代理的資源消耗。

  預設情況下已啟用該選項。它僅適用於 Windows。

  若要管理 Microsoft 軟體更新，請使用**Windows Update 更新詳情**選項。

- **硬體登錄資料詳細資訊**

  安裝在裝置上的網路代理會向管理伺服器傳送關於裝置硬體的資訊。您可以在裝置內容中檢視硬體詳細資訊。

  確保在要從中獲取硬體詳細資訊的 Linux 裝置上安裝了 lshw 公用程式。根據所使用的 hypervisor，從虛擬機獲取的硬體詳細資訊可能不完整。

軟體更新和弱點

在**軟體更新和弱點**區域，您可以設定搜尋和發佈 Windows 更新，以及啟用掃描可執行檔以發現弱點：

- **使用管理伺服器作為 WSUS 伺服器**

  如果啟用此選項，Windows 更新下載到管理伺服器。管理伺服器提供以集線模式透過網路代理下載更新到用戶端裝置的 Windows 更新服務。

  如果停用此選項，則不使用管理伺服器下載 Windows 更新。此種情況下，用戶端裝置自己接收 Windows 更新。

  預設情況下已停用該選項。

- 您可以限制使用者可以透過使用 Windows Update 手動安裝到裝置的 Windows 更新。

  在執行 Windows 10 的裝置上，如果 Windows Update 已為裝置找到更新，您在**允許使用者管理 Windows Update 更新安裝**下選取的新選項將僅在發現的更新被安裝後才被套用。

  在下拉清單中選取項目：

  - **允許使用者安裝所有可套用 Windows Update 更新**

    使用者可以安裝所有可套用到他們裝置的 Microsoft Windows Update 更新。

    如果您不希望干預更新安裝，請選取該選項。

    當使用者手動安裝 Microsoft Windows Update 更新時，更新可能從 Microsoft 伺服器下載，而不是從管理伺服器。如果管理伺服器還未下載這些更新，這是可能的。從 Microsoft 伺服器下載更新導致額外流量。

  - **僅允許使用者安裝批准的 Windows Update 更新**

    使用者可以安裝所有可應用到他們裝置的和您批准的 Microsoft Windows Update 更新。

    例如，您可能想先在測試環境中檢查更新安裝以確保它們不干預裝置操作，僅在這之後允許安裝這些批准的更新到用戶端裝置。

    當使用者手動安裝 Microsoft Windows Update 更新時，更新可能從 Microsoft 伺服器下載，而不是從管理伺服器。如果管理伺服器還未下載這些更新，這是可能的。從 Microsoft 伺服器下載更新導致額外流量。

  - **不允許使用者安裝 Windows Update 更新**

    使用者無法在他們的裝置上手動安裝 Microsoft Windows Update 更新。所有可套用更新根據您的設定而安裝。

    如果您想要集中管理更新的安裝則選則此選項。

    例如，您可以想最佳化更新排程以便網路不超載。您可以計畫稍後更新，以便它們不干預使用者工作。

- 在**Windows Update 搜尋模式**設定群組中，您可以選取更新搜尋模式：
  - **作用中**

    如果選中該選項，管理伺服器支援使用網路代理在用戶端裝置上從 Windows 更新代理傳送請求至更新來源：Windows 更新伺服器（或簡稱為 WSUS）。然後，網路代理會將從 Windows 更新代理接收到的資訊傳送給管理伺服器。

    只有選取*弱點掃描和所需更新*工作的**連線更新伺服器更新資料**選項時，此選項才會發揮效力。

    預設情況下已選定此選項。

  - **被動**

    如果您選定該選項，網路代理將從上次同步更新來源之後定期從 Windows 更新代理將所擷取更新的資訊傳遞給管理伺服器。如果 Windows 更新代理沒有執行與更新來源同步，在管理伺服器上的更新資訊就不再是最新的。

    若要從更新來源的記憶體快取獲得更新，請選取此選項。

  - **已停用**

    如果選中該選項，管理伺服器不會請求任何有關更新的資訊。

    若您要在本機裝置先測試更新，請選取此選項。

- **當執行可執行檔時掃描其弱點**

  如果啟用此選項，系統將在執行可執行檔時掃描弱點。

  預設情況下已啟用該選項。

重新啟動管理

如果您的作業系統必須在您使用、安裝或移除安裝應用程式時重新啟動受管理裝置，請在**重新啟動管理**區域指定執行的操作：

- **不要重新啟動作業系統**

  用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

- **如果必要，自動重新啟動作業系統**

  如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

- **提示使用者操作**

  用戶端裝置螢幕上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。該選項適用於使用者必須可以選取最方便的時間進行重新啟動的工作站。

  預設情況下已選定此選項。

  - **重複提示間隔（分鐘）**

    如果啟用該選項，應用程式以指定頻率提示使用者重新啟動作業系統。

    預設情況下已啟用該選項。預設間隔是 5 分鐘。可用值介於 1 和 1440 分鐘之間。

    如果停用該選項，提示僅顯示一次。

  - **在指定時間後強制重新啟動（分鐘）**

    提示使用者之後，應用程式在指定時間間隔後強制作業系統重新啟動。

    預設情況下已啟用該選項。預設延時是 30 分鐘。可用值介於 1 和 1440 分鐘之間。

  - **強制關閉已鎖定連線的應用程式**

    執行應用程式可能會阻止用戶端裝置重新啟動。例如，如果文件在文書處理應用程式中編輯且未儲存，應用程式不會允許裝置重新啟動。

    如果啟用該選項，鎖定裝置上的此類應用程式在裝置重新啟動前被強制關閉。結果，使用者可能遺失他們未儲存的變更。

    如果停用該選項，鎖定裝置不被重新啟動。此裝置上的工作狀態表示裝置需要重新啟動。使用者必須手動關閉所有執行在鎖定裝置上的應用程式並重新啟動這些裝置。

    預設情況下已停用該選項。

Windows 共用桌面

您可以透過**Windows 共用桌面**區域啟用並設定在使用共用桌面存取時使用者的遠端裝置上執行的管理員操作的稽核：

- **啟用稽核**

  如果啟用此選項，則會啟用遠端裝置上管理員的操作稽核。遠端裝置上的管理員操作是被一一記錄下來的：

  - 在遠端裝置的事件記錄中
  - 在位於遠端裝置上網路代理安裝資料夾中的副檔名為 syslog 的檔案中
  - 卡巴斯基安全管理中心的事件資料庫

  當符合以下條件時，管理員可使用操作稽核：

  - 弱點和修補程式管理授權使用中
  - 管理員有權啟動共用存取遠端裝置的桌面

  如果清除該選項，則會停用遠端裝置上的管理員操作稽核。

  預設情況下已停用該選項。

- **讀取時要監控的檔案遮罩**

  清單包含檔案遮罩。啟用稽核時，應用程式會監控管理員的讀取檔案是否與已讀取檔案的遮罩和從屬資訊相符。若已選取**啟用稽核**核取方塊，則可使用該清單。您可編輯檔案遮罩並新增一個至清單。各個新檔案遮罩應在新行的清單中指定。

  預設，指定了以下檔案遮罩:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **修改時要監控的檔案遮罩**

  該清單包含遠端裝置上的檔案遮罩。啟用稽核時，應用程式會監控管理員在符合遮罩的檔案中所作的變更，並儲存這些修改的資訊。若已選取**啟用稽核**核取方塊，則可使用該清單。您可編輯檔案遮罩並新增一個至清單。各個新檔案遮罩應在新行的清單中指定。

  預設，指定了以下檔案遮罩:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

管理修補程式和更新

在**管理修補程式和更新**區域，您可以設定更新的下載和發佈以及修補程式在受管理裝置上的安裝：

- **對未定義狀態的元件自動安裝可套用更新和修補程式**

  如果啟用此選項，帶有*未定義*批准狀態的 Kaspersky 應用程式在從更新伺服器下載後將被自動安裝在受管理裝置。

  如果停用此選項，被下載和標注為*未定義*狀態的 Kaspersky 修補程式將僅在您改變其狀態為*已批准*是被安裝。

  預設情況下已啟用該選項。

- **提前從管理伺服器下載更新和病毒資料庫（建議）**

  如果啟用此選項，離線模式更新下載被使用。當管理伺服器接收更新時，它通知網路代理（安裝網路代理的裝置）將用於受管理應用程式的更新。當網路代理接收更新的資訊後，它提前從管理伺服器下載相關檔案。在第一次連線網路代理時，管理伺服器發起更新下載。網路代理下載所有更新到用戶端裝置後，更新對該裝置上的應用程式可用。

  當用戶端裝置上的受管理應用程式嘗試存取網路代理以更新時，該網路代理檢查其是否具有所有所需的更新。如果在受管理應用程式請求更新之前 25 小時內，更新已從管理伺服器收到，則網路代理不連線到管理伺服器，而是從本機快取提供更新給受管理應用程式。當網路代理提供更新到用戶端裝置上的應用程式時，可能不會建立到管理伺服器的連線，但是更新不需要連線。

  如果停用此選項，離線模式更新下載不被使用。更新依據更新下載工作的排程被發佈。

  預設情況下已啟用該選項。

連線

連線區域包含三個子區域：

- **網路**
- **連線設定檔**
- **連線排程**

在**網路**子區域，您可以設定到管理伺服器的連線、啟用 UDP 連接埠，和指定 UDP 連接埠號。

- 在**連線至管理伺服器**設定群組中，您可以設定到管理伺服器的連線，並指定同步用戶端裝置和管理伺服器的時間間隔：

  - **同步間隔（分鐘）**

    網路代理同步管理伺服器的受管理裝置。我們建議您將同步間隔（也叫心跳）設為每 10,000 台受管理裝置 15 分鐘。

    若同步間隔社為少於 15 分鐘，同步會每 15 分鐘執行一次。若同步間隔設為 15 分鐘或更多，同步會以特定同步間隔執行。

  - **壓縮網路流量**

    如果啟用此選項，則透過減少所傳輸的流量進而減少管理伺服器的負載來提高網路代理的資料傳輸速度。

    用戶端裝置上的 CPU 負載可能會增加。

    預設情況下會啟用此核取方塊。

  - **在 Microsoft Windows 防火牆上開啟網路代理連接埠**

    如果啟用此選項，網路代理和管理伺服器工作所需的 UDP 連接埠將新增到 Microsoft Windows 防火牆排除清單中。

    預設情況下已啟用該選項。

  - **使用 SSL 連線**

    如果啟用此選項，則使用 SSL 通訊協定透過安全連接埠連線管理伺服器。

    預設情況下已啟用該選項。

  - **以預設連線設定在發佈點（如果可用）上使用連線閘道**

    如果啟用此選項，發佈點上的連線閘道在管理群組屬性指定的設定下使用。

    預設情況下已啟用該選項。

- **使用 UDP 連接埠**

  如果需要網路代理透過 UDP 連接埠連線到管理伺服器，啟用**使用 UDP 連接埠**選項，並指定 **UDP 連接埠號**。預設情況下已啟用該選項。連線到管理伺服器的預設 UDP 連接埠是 15000。

- **UDP 連接埠號**

  在該欄位中，您可以輸入 UDP 連接埠號。預設埠號為 15000。

  使用十進位系統記錄。

  如果用戶端裝置執行在 Windows XP Service Pack 2 系統下，則整合的防火牆會封鎖 UDP 連接埠 15000。請手動開啟此連接埠。

- **使用發佈點強制連線到管理伺服器**

  如果您選取了**將此發佈點用作推送伺服器**發佈點設定視窗中的選項。否則，發佈點將不會作為推送伺服器。

在**連線設定檔**子區域中，您可以指定網路位置設定，並在管理伺服器不可用時啟用不在辦公室模式：

- **網路位置設定**

  網路位置設定定義用戶端裝置所連線的網路內容，並指定當網路內容改變時，網路代理從一個管理伺服器連線設定檔轉換到另一個的規則。

- **管理伺服器連線設定檔**

  在該區域中，您可以檢視和設定網路代理至管理伺服器的連線。在該區域，您也可以建立當以下事件發生時，轉換網路代理到不同管理伺服器的規則：

  - 當用戶端裝置連線到另一個本機網路時
  - 當裝置與組織的本機網路遺失連線時
  - 當連線閘道的位址變更或 DNS 伺服器位址修改時

  連線設定檔僅支援執行 Windows 和 macOS 的裝置。

- **當管理伺服器不可用時啟用漫遊模式**

  如果啟用此選項，則在透過該設定檔連線的情況下，用戶端裝置上安裝的應用程式將使用漫遊模式裝置的政策設定檔，以及漫遊政策。如果沒有為應用程式定義漫遊政策，則使用啟動政策。

  如果停用此選項，則應用程式將使用已啟動的政策。

  預設情況下已停用該選項。

在**連線排程**子區域中，可以指定網路代理傳送資料到管理伺服器的時間間隔：

- **必要時連線**

  如果選中此選項，當網路代理需要傳送資料到管理伺服器時連線才被建立。

  預設情況下已選定此選項。

- **在指定時間間隔連線**

  如果選中此選項，網路代理在指定時間連線到管理伺服器。您可以新增若干個連線時間段。

透過發佈點的網路輪詢

在**透過發佈點的網路輪詢**區域，您可以設定網路自動輪詢。您可以使用以下選項啟用輪詢並設定其頻率：

- **Windows 網路**

  如果啟用此選項，則管理伺服器將按照您按一下**設定快速輪詢排程**和**設定完整輪詢排程**連結所配置的排程自動輪詢網路。

  如果停用此選項，管理伺服器將以**網路輪詢頻率（分鐘）**欄位中指定的時間間隔輪詢網路。

  對於 10.2 之前的版本，網路代理的裝置發現間隔可在**Windows 網域的輪詢頻率（分鐘）**（對於快速 Windows 網路輪詢）和**網路輪詢頻率（分鐘）**（對於完整 Windows 網路輪詢）欄位中設定。

  預設情況下已停用該選項。

- **Zeroconf**

  如果啟用此選項，發佈點將使用零配置網路（也稱為 *Zeroconf*）用 IPv6 裝置自動輪詢網路。在這種情況下，啟用的 IP 範圍輪詢將被忽略，因為發佈點會輪詢整個網路。

  要開始使用 Zeroconf，必須滿足以下條件：

  - 發佈點必須執行 Linux。
  - 您必須在發佈點上安裝 avahi-browse 公用程式。

  如果停用此選項，則發佈點不會使用 IPv6 裝置輪詢網路。

  預設情況下已停用該選項。

- **IP 範圍**

  如果啟用此選項，則發佈點將按照您按一下**設定輪詢排程**按鈕所配置的排程自動輪詢 IP 範圍。

  如果停用此選項，則發佈點將不輪詢 IP 範圍。

  在 10.2 版之前的網路代理中，可在**輪詢間隔（分鐘）**欄位中配置 IP 範圍的輪詢頻率。若啟用該選項，可使用區域。

  預設情況下已停用該選項。

- **Active Directory**

  如果啟用此選項，則發佈點將按照您按一下**設定輪詢排程**連結所配置的排程自動輪詢 Active Directory。

  如果停用此選項，則管理伺服器將不輪詢 Active Directory。

  在 10.2 版之前的網路代理中，可在 **輪詢間隔（分鐘）** 欄位中設定 Active Directory 的輪詢頻率。如果啟用此選項，則該欄位可用。

  預設情況下已停用該選項。

發佈點網路設定

在**發佈點網路設定**區域中，您可以指定網際網路存取設定：

- **使用代理伺服器**
- **位址**
- **連接埠號**
- **略過本機位址的代理伺服器**

  如果啟用此選項，則不使用代理伺服器連線本機網路的裝置。

  預設情況下已停用該選項。

- **代理伺服器身分驗證**

  如果選取該方塊，您可以在輸入欄位中為代理伺服器身分驗證指定憑證。

  預設情況下已清空此方塊。

- **使用者名稱**
- **密碼**

KSN 代理（發佈點）

在 **KSN 代理（發佈點）**區域，您可以設定應用程式使用發佈點，以從受管理裝置轉發卡巴斯基安全網路 (KSN) 請求。

- **在發佈點端啟用 KSN 代理**

  KSN 代理服務執行在用作發佈點的裝置上。使用該功能重新分發和最佳化網路流量。

  發佈點傳送列在卡巴斯基安全網路聲明中的統計資訊到 Kaspersky。依預設，KSN 聲明位於 %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula。

  預設情況下已停用該選項。啟用該選項僅在**使用管理伺服器作為代理伺服器**和**我同意使用卡巴斯基安全網路**選項在管理伺服器內容視窗中被啟用時起作用。

  您可以指派活動被動叢集節點到發佈點並在該節點上啟用 KSN 代理伺服器。

- **轉發 KSN 請求到管理伺服器**

  發佈點從受管理裝置轉發 KSN 請求到管理伺服器。

  預設情況下已啟用該選項。

- **透過網際網路直接存取 KSN 雲端 / 私有 KSN**

  發佈點從受管理裝置轉發 KSN 請求到 KSN 雲端或私有 KSN。在發佈點上自行產生的 KSN 要求頁會直接傳送至 KSN 雲端或私有 KSN。

  已安裝網路代理版本 11（或更早版本）的發佈點無法直接存取私有 KSN。若要重新設定發佈點傳送 KSN 要求至私有 KSN，請為各發佈點啟用 **轉發 KSN 請求到管理伺服器**選項。

  已安裝網路代理版本 12（或更新版本）的發佈點可直接存取私有 KSN。

- **連接埠**

  受管理裝置將用於連線到 KSN 代理伺服器的 TCP 埠號。預設埠號為 13111。

- **UDP 連接埠**

  如果需要網路代理透過 UDP 連接埠連線到管理伺服器，啟用**使用 UDP 連接埠**選項，並指定 **UDP 連接埠號**。預設情況下已啟用該選項。連線到管理伺服器的預設 UDP 連接埠是 15000。

更新（發佈點）

在**更新（發佈點）**部分，您可以啟用下載差異檔案功能，以便發佈點以差異檔案的形式從卡巴斯基更新伺服器獲取更新。

變更歷程

在此頁籤上，您可以檢視政策修訂的清單並復原對政策進行的變更（如有必要）。

Kaspersky Endpoint Security 政策的手動設定

本節提供有關如何設定 Kaspersky Endpoint Security 政策的建議。您可以在政策內容視窗中執行設定。編輯設定時，請按一下相關設定群組右側的鎖定圖示，將指定的值套用到工作站。

設定卡巴斯基安全網路

卡巴斯基安全網路 (KSN) 是雲端服務的基礎架構，包含有關檔案、網路資源和軟體信譽的資訊。卡巴斯基安全網路讓 Kaspersky Endpoint Security for Windows 能更快回應不同類型的威脅，增強防護元件的效能，並降低誤報的可能性。如需有關卡巴斯基安全網路的更多資訊，請參閱 Kaspersky Endpoint Security for Windows 說明。

要指定建議的 KSN 設定：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。
2. 按一下 Kaspersky Endpoint Security for Windows 的政策。

   所選政策的內容視窗開啟。
3. 在政策內容中，前往**應用程式設定 → 進階威脅防護 → 卡巴斯基安全網路**。
4. 確保**卡巴斯基安全網路**選項被啟用。使用該功能有助於重新分發和最佳化網路流量。
5. 如果無法使用 KSN 代理服務，啟用對 KSN 伺服器的使用。KSN 伺服器可能位於 Kaspersky 端（當全域 KSN 被使用）或協力廠商端（當私有 KSN 被使用）。
6. 點擊**確定**。

建議的 KSN 設定被指定。

檢查受防火牆保護的網路清單

確保 Kaspersky Endpoint Security for Windows 防火牆防護您的所有網路。預設情況下，防火牆防護具有以下連線類型的網路：

- **公用網路**。安全應用程式、防火牆或過濾器不防護此類網路中的裝置。
- **本機網路**。限制此網路中的裝置存取檔案和印表機。
- **受信任網路**。此類網路中的裝置受到防護，可防止攻擊以及未經授權的檔案和資料存取。

如果您配置了自訂網路，請確保防火牆會防護這個網路。為此，請檢查 Kaspersky Endpoint Security for Windows 政策內容中的網路清單。該清單可能不包含所有網路。

如需有關防火牆的詳細資訊，請參閱 Kaspersky Endpoint Security for Windows 說明。

要檢視網路清單：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。
2. 按一下 Kaspersky Endpoint Security for Windows 的政策。
   所選政策的內容視窗開啟。
3. 在政策內容中，前往**應用程式設定 → 關鍵威脅防護 → 防火牆**。
4. 在**可用網路**下面，點擊**網路設定**連接。
   網路連線視窗將開啟。該視窗顯示網路清單。
5. 如果清單有缺少的網路，請新增它。

停用網路磁碟機掃描

當 Kaspersky Endpoint Security for Windows 掃描網路磁碟機時，會對它們帶來很大的負載。在檔案伺服器上執行間接掃描更方便。

您可以在 Kaspersky Endpoint Security for Windows 政策內容中停用網路磁碟機掃描。如需這些政策內容的說明，請參閱 Kaspersky Endpoint Security for Windows 說明。

要停用網路磁碟機掃描：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。
2. 按一下 Kaspersky Endpoint Security for Windows 的政策。
   所選政策的內容視窗開啟。
3. 在政策內容中，前往**應用程式設定 → 關鍵威脅防護 → 檔案威脅防護**。
4. 在**防護範圍**下，停用**所有網路磁碟機**選項。
5. 點擊**確定**。

網路磁碟機掃描被停用。

從管理伺服器記憶體中排除軟體詳細資訊

我們建議管理伺服器不要儲存有關在網路裝置上啟動的軟體模組資訊。如此，管理伺服器記憶體才不會過度執行。

您可以在 Kaspersky Endpoint Security for Windows 政策內容中停用對此資訊的儲存。

要停用對已安裝軟體模組資訊的儲存：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。
2. 按一下 Kaspersky Endpoint Security for Windows 的政策。
   所選政策的內容視窗開啟。
3. 在政策內容中，前往**應用程式設定 → 一般設定 → 報告和儲存**。
4. 在**到管理伺服器的資料傳輸**下，停用**關於已啟動的應用程式**核取方塊（如果它仍然在頂級政策中被啟用）。
   當選中該核取方塊時：如果選中此核取方塊，管理伺服器資料庫儲存網路裝置上所有軟體模組的所有版本資訊。該資訊可能需要卡巴斯基安全管理中心資料庫上的大量磁碟空間（幾十 G）。

已安裝軟體模組的資訊不被儲存到管理伺服器資料庫。

在工作站上設定對 Kaspersky Endpoint Security for Windows 介面的存取

如果組織網路的威脅防護必須以集中模式透過卡巴斯基安全管理中心管理，請在 Kaspersky Endpoint Security for Windows 政策內容中指定介面設定，如下所述。如此，您才能防止他人未經授權存取工作站上的 Kaspersky Endpoint Security for Windows 以及變更 Kaspersky Endpoint Security for Windows 設定。

如需這些政策內容的說明，請參閱 Kaspersky Endpoint Security for Windows 說明。

要指定建議的介面設定：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。
2. 按一下 Kaspersky Endpoint Security for Windows 的政策。
   所選政策的內容視窗開啟。
3. 在政策內容中，前往**應用程式設定 → 一般設定 → 介面**。
4. 在**使用者互動**下，選中**不顯示使用者介面**選項。這將停用在工作站上顯示 Kaspersky Endpoint Security for Windows 使用者介面，因此它們的使用者無法變更 Kaspersky Endpoint Security for Windows 的設定。
5. 在**密碼防護**下，啟用切換開關。這降低了對工作站上 Kaspersky Endpoint Security for Windows 設定的非授權或意外的變更。

Kaspersky Endpoint Security for Windows 介面的建議設定被指定。

在管理伺服器資料庫中儲存重要的政策事件

為了避免管理伺服器資料溢出，我們建議您僅儲存重要事件到資料庫。

要配置註冊重要事件到管理伺服器資料庫：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。
2. 按一下 Kaspersky Endpoint Security for Windows 的政策。
   所選政策的內容視窗開啟。

3. 在政策內容中，開啟**事件配置**頁籤。

4. 在**緊急**區段，點擊**新增事件**並僅選取以下事件旁的核取方塊：

- *違反了最終使用者產品授權協議*
- *應用程式自動執行已停用*
- *啟動錯誤*
- *偵測到活動威脅。應該啟動進階解毒技術*
- *無法解毒*
- *偵測到之前開啟的危險連結*
- *處理程序已終止*
- *網路活動已封鎖*
- *偵測到網路攻擊*
- *已禁止應用程式啟動*
- *存取被拒絕 (本機資料庫)*
- *存取被拒絕 (KSN)*
- *本機更新錯誤*
- *不能同時執行兩項工作*
- *與卡巴斯基安全管理中心互動時發生錯誤*
- *未更新所有元件*
- *套用檔案加密/解密規則時出錯*
- *啟用攜帶模式時出錯*
- *停用攜帶模式時出錯*
- *無法載入加密模組*
- *無法套用政策*
- *變更應用程式元件時出錯*

5. 點擊**確定**。

6. 在**功能失效**區段，點擊**新增事件**並僅選取事件*有效工作設定旁的核取方塊。設定未套用*。

7. 點擊**確定**。

8. 在**警告**區段，點擊**新增事件**並僅選取以下事件旁的核取方塊：

   - *自我防護被停用*
   - *防護元件被停用*
   - *備用金鑰不正確*
   - *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）*
   - *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)*
   - *物件已刪除*
   - *物件已解毒*
   - *使用者選擇了結束加密政策*
   - *檔案已被管理員從 Kaspersky Anti Targeted Attack Platform 伺服器上的隔離區還原*
   - *檔案已被管理員在 Kaspersky Anti Targeted Attack Platform 伺服器上隔離*
   - *傳送給管理員的應用程式啟動封鎖訊息*
   - *傳送給管理員的裝置存取封鎖訊息*
   - *傳送給管理員的網頁存取封鎖訊息*

9. 點擊**確定**。

10. 在**資訊**區段，點擊**新增事件**並僅選取以下事件旁的核取方塊：

    - *物件的備份副本已建立*
    - *禁止應用程式在測試模式下啟動*

11. 點擊**確定**。

註冊重要事件到管理伺服器資料庫被配置。

Kaspersky Endpoint Security 更新群組工作的手動設定

Kaspersky Endpoint Security 的最佳化和建議排程選項是**當新更新下載至儲存區時**時，當**使用工作啟動自動隨機延遲**核取方塊被選中時。

授予離線存取權限給受裝置控制封鎖的外部裝置

在 Kaspersky Endpoint Security for Windows 政策的裝置控制元件中，您可管理使用者對安裝在或連線至用戶端裝置之外部裝置的存取權限（例如硬碟、相機或 Wi-Fi 模組）。這可讓您連線至此類外部裝置時保護用戶端裝置不受感染，並且避免資料遺失或洩漏。

若需授予臨時存取權限給受裝置控制封鎖的外部裝置，但無法將裝置新增至信任的裝置清單，您可臨時授予離線存取權限給外部裝置。離線存取代表用戶端裝置沒有存取網路的權限。

僅當在**應用程式設定 → 安全控制 → 裝置控制**區段中，已啟用 Kaspersky Endpoint Security 政策設定中的**允許暫時存取請求**選項時，您才可以授予離線存取權限給受裝置控制封鎖的外部裝置。

授予離線存取權限給受裝置控制封鎖的外部裝置包含以下階段：

1. 在 Kaspersky Endpoint Security for Windows 對話視窗中，要存取已封鎖外部裝置的使用者，會產生請求存取檔案並將其傳送給卡巴斯基安全管理中心的管理員。
2. 卡巴斯基安全管理中心管理員收到此要求後會建立存取金鑰檔案並將其傳送給裝置使用者。
3. 在 Kaspersky Endpoint Security for Windows 對話視窗中，裝置使用者會啟動存取金鑰檔案並取得外部裝置的臨時存取權限。

要授予離線存取權限給受裝置控制封鎖的外部裝置：

1. 在主功能表中，轉至 **裝置 → 受管理裝置**。

   受管理裝置清單隨即顯示。
2. 在此清單中，選取要求存取受裝置控制封鎖的外部裝置的使用者裝置。

   您僅可以選取一部裝置。
3. 在受管理裝置清單上方，按一下省略符號按鈕 (**...**)，然後按一下**同意存取離線模式下的裝置**按鈕。
4. 在開啟的**應用程式設定**視窗的**裝置控制**部分中，點擊**瀏覽**按鈕。
5. 選擇您從使用者那裡收到的檔案存取要求，然後按一下**開啟**按鈕。該檔案應使用 AKEY 格式。

   要求存取權限的使用者鎖定裝置的詳細資料隨即顯示。
6. 指定**存取持續時間**設定的值。

   此設定會定義您授予使用者存取鎖定裝置的時間長度。預設值為使用者建立請求存取檔案指定的值。
7. 指定存取金鑰可以在裝置上啟動的時間段。

   透過提供的存取金鑰，此設定會定義使用者可啟動對鎖定裝置存取的期間。
8. 點擊**儲存**按鈕。

   這會開啟 Microsoft Windows 標準的**儲存存取金鑰**視窗。
9. 選取目的地資料夾，以儲存內含封鎖裝置的存取金鑰的檔案。
10. 點擊**儲存**按鈕。

之後，當您傳送使用者存取金鑰檔案以及使用者在 Kaspersky Endpoint Security for Windows 對話視窗中啟動時，使用者會擁有對已封鎖裝置特定期間的存取權限。

遠端移除應用程式或軟體更新

要從所選裝置遠端刪除應用程式或軟體更新，請執行以下操作：

1. 在主功能表中，轉至 **裝置 → 工作**。
2. 點擊**新增**。
   新工作精靈啟動。使用**下一步**按鈕進行精靈。
3. 對於卡巴斯基安全管理中心應用程式，選擇**遠端解除安裝應用程式**工作類型。
4. 指定您正建立的工作的名稱。
   工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。
5. 選取要分配工作的裝置。

6. 選擇要刪除的軟體類型，然後選擇要刪除的特定應用程式，更新或修補程式：

- **解除安裝受管理應用程式**

  顯示 Kaspersky 應用程式清單。選取您要移除的弱點。

- **解除安裝不相容的應用程式**

  顯示與 Kaspersky 安全應用程式或卡巴斯基安全管理中心不相容的應用程式清單。選取您要刪除之項目旁的核取方塊。

- **從應用程式登錄資料中解除安裝應用程式**

預設情況下，網路代理會傳送管理伺服器有關受管理裝置上安裝的應用程式資訊。已安裝的應用程式清單會儲存在應用程式登錄資料中。

要從應用程式登錄資料中選取一個應用程式：

a. 點擊**要解除安裝的應用程式**欄位，然後選擇要刪除的應用程式。

如果您選擇卡巴斯基安全管理中心網路代理，則當您執行工作時，狀態*已成功完成*會顯示刪除過程已開始。如果卡巴斯基安全管理中心網路代理被移除，則狀態不會變更。如果工作失敗，狀態將變更為*失敗*。

b. 指定移除選項：

- **解除安裝模式**

選取您要如何移除該應用程式：

- **自動定義解除安裝指令**

  如果應用程式具有應用程式供應商定義的解除安裝命令，則卡巴斯基安全管理中心將使用此命令。我們建議您選取此選項。

- **指定解除安裝指令**

  如果要為解除安裝應用程式指定自己的命令，請選取此選項。

  建議您先嘗試使用**自動定義解除安裝指令**選項。如果透過自動定義的解除安裝命令失敗，請使用自己的命令。

  在該欄位中鍵入安裝命令，然後指定以下選項：

  除非未自動偵測預設指令，否則將使用此指令進行解除安裝

  卡巴斯基安全管理中心會檢查所選應用程式是否具有應用程式供應商定義的解除安裝命令。如果找到該命令，則卡巴斯基安全管理中心將使用該命令，而不是**應用程式解除安裝指令**欄位中指定的命令。

  我們建議您啟用該選項。

- **應用程式成功解除安裝後執行重新啟動**

如果應用程式要求成功移除後在受管理裝置上重新啟動作業系統，則作業系統將會自動重新啟動。

- **解除安裝指定的應用程式更新、修補程式或其他應用程式**

顯示更新、修補程式和協力廠商應用程式的清單。選取您要移除的項目。

顯示的清單是應用程式和更新的常規清單，並不對應於受管理裝置上安裝的應用程式和更新。選取項目之前，建議您確保在工作範圍中定義的裝置上安裝了應用程式或更新。您可以透過內容視窗檢視安裝了應用程式或更新的裝置清單。

若要檢視裝置清單：

a. 按一下應用程式名稱或更新。

內容視窗隨即開啟。

b. 開啟**裝置**區段。

您還可以在裝置內容視窗中檢視已安裝的應用程式和更新的清單。

7. 指定用戶端裝置將如何下載解除安裝公用程式：

- **使用網路代理**

  檔案會透過安裝在這些用戶端裝置上的網路代理傳遞到用戶端裝置。

  如果停用此選項，則會使用 Microsoft Windows 工具傳送檔案。

  如果已指派工作給安裝了網路代理的裝置，建議您選取該核取方塊。

- **透過管理伺服器使用作業系統資源**

  使用管理伺服器作業系統工具將檔案傳輸到用戶端裝置。如果使用者端裝置上未安裝網路代理，但是使用者端裝置與管理伺服器在同一網路，則您可以啟用此選項。

- **透過發佈點使用作業系統資源**

  使用作業系統工具透過發佈點將檔案傳輸到用戶端裝置。如果網路中存在不止一個發佈點，那麼您可以選取此選項。

  如果啟用**使用網路代理**方塊，僅在網路代理工具不可使用時才會透過作業系統工具傳送檔案。

- **同時下載的最大數量**

  管理伺服器可以同時向其傳輸檔案的最大用戶端裝置數量。此數字越大，應用程式解除安裝的速度越快，但是管理伺服器上的負載會更高。

- **解除安裝嘗試次數上限**

  若是在執行*遠端解除安裝應用程式*工作時，卡巴斯基安全管理中心解除安裝受管理裝置的應用程式失敗超過指定次數，卡巴斯基安全管理中心會停止傳送解除安裝公用程式到該受管理裝置，且不再在該裝置上啟動安裝程式。

  解除安裝嘗試次數上限參數允許您節省受管理裝置資源，以及減少流量（移除、MSI 檔案執行和錯誤訊息）。

  重複的工作啟動嘗試可能提示裝置具有妨礙解除安裝的問題。管理員應在指定的移除嘗試次數內解決問題，然後重新啟動工作（手動或按排程）。

  如果解除安裝始終未完成，問題被視為無法解決且後續工作啟動被認為是不必要的資源和流量浪費。

  建立該工作時，嘗試技術會設定為 `0`。返回錯誤的安裝程式的每次執行都增加計數。

  如果超過指定的嘗試次數且裝置已準備好解除安裝應用程式，您可以增加**解除安裝嘗試次數上限**參數的值並啟動工作以解除安裝應用程式。或者，您可以建立新的*遠端解除安裝應用程式*工作。

- **下載之前驗證作業系統類型**

  在將檔案傳輸到用戶端裝置之前，卡巴斯基安全管理中心將檢查「安裝公用程式」設定是否適用於用戶端裝置的作業系統。如果設定不適用，則卡巴斯基安全管理中心不會傳輸檔案，也不會嘗試安裝應用程式。例如，要將某些應用程式安裝到包括執行各種作業系統之裝置的管理群組裝置，您可以將安裝工作指派給管理群組，然後啟用此選項以跳過執行不是要求的作業系統的裝置。

- **使用解除安裝密碼**

如果您在上一步中選擇了**解除安裝受管理應用程式**，然後在**要解除安裝的應用程式**欄位中指定了卡巴斯基安全管理中心網路代理，則會顯示此參數。

如果您之前在網路代理政策設定中設定了網路代理遠端解除安裝的密碼，請選中**使用解除安裝密碼**核取方塊，然後在**密碼**欄位中輸入解除安裝密碼。如果您沒有設定網路代理遠端解除安裝的密碼，請勿選中該核取方塊。

8. 指定作業系統重新啟動設定：

- **不重新啟動裝置**

  用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

- **重新啟動裝置**

  如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

- **提示使用者操作**

  用戶端裝置螢幕上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。該選項適用於使用者必須可以選取最方便的時間進行重新啟動的工作站。

  預設情況下已選定此選項。

- **重複提示間隔（分鐘）**

  如果啟用該選項，應用程式以指定頻率提示使用者重新啟動作業系統。

  預設情況下已啟用該選項。預設間隔是 5 分鐘。可用值介於 1 和 1440 分鐘之間。

  如果停用該選項，提示僅顯示一次。

- **在該時間後重新啟動（分鐘）**

  提示使用者之後，應用程式在指定時間間隔後強制作業系統重新啟動。

  預設情況下已啟用該選項。預設延時是 30 分鐘。可用值介於 1 和 1440 分鐘之間。

- **強制關閉已鎖定連線的應用程式**

  執行應用程式可能會阻止用戶端裝置重新啟動。例如，如果文件在文書處理應用程式中編輯且未儲存，應用程式不會允許裝置重新啟動。

  如果啟用該選項，鎖定裝置上的此類應用程式在裝置重新啟動前被強制關閉。結果，使用者可能遺失他們未儲存的變更。

  如果停用該選項，鎖定裝置不被重新啟動。此裝置上的工作狀態表示裝置需要重新啟動。使用者必須手動關閉所有執行在鎖定裝置上的應用程式並重新啟動這些裝置。

  預設情況下已停用該選項。

9. 如果必要，請新增要用於啟動遠端解除安裝工作的帳戶：

- **不需要帳戶（網路代理已安裝）**

  如果該選項被選中，您不是必須指定一個帳戶，並在該帳戶下執行程式的安裝。將使用執行管理伺服器服務的帳戶執行該工作。

  如果網路代理未安裝在用戶端裝置，則此選項無法使用。

- **需要帳戶（不使用網路代理）**

  如果您為其分配*遠端解除安裝應用程式*工作的裝置上未安裝網路代理，請選取此選項。在這種情況下，您可以指定使用者帳戶或 SSH 憑證來取消安裝應用程式。

  - **本機帳戶**。如果選取此選項，請指定用於執行應用程式安裝程式的使用者帳戶。點擊**新增**按鈕，選擇**本機帳戶**，然後指定使用者帳戶憑據。

    您可以根據情況指定多個帳戶，例如，沒有一個帳戶在分配工作的所有裝置上擁有全部所需權限時。在此情況下，已新增的所有帳戶會用於從上到下按順序執行該工作。

  - **SSH 憑證**。如果要在 Linux 型用戶端裝置上安裝應用程式，您可以指定 SSH 憑證而不是指定使用者帳戶。按一下**新增**按鈕，選擇**SSH 憑證**，然後指定憑證的私鑰和公鑰。

    如要產生私密金鑰，您可以使用 ssh-keygen 公用程式。請注意，卡巴斯基安全管理中心支援 PEM 格式的私密金鑰，但 ssh-keygen 公用程式預設為產生 OPENSSH 格式的 SSH 金鑰。卡巴斯基安全管理中心不支援 OPENSSH 格式。要以支援的 PEM 格式建立私密金鑰，請在 ssh-keygen 命令中加入 -m PEM 選項。

    例如：

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "< 使用者電子郵件 >"
    ```

10. 若要修改預設工作設定，請啟用**完成工作建立**頁面的**建立完成時開啟工作詳情**選項。如果您不啟用該選項，工作使用預設設定建立。您可以稍後隨時修改預設設定。

11. 點擊**完成**按鈕。

    工作被建立並顯示在工作清單。

12. 按一下建立的工作的名稱以開啟工作內容視窗。

13. 在工作內容視窗中，指定一般工作設定。

14. 點擊**儲存**按鈕。

15. 您可以手動執行此工作，或等候工作設定中指定的排程將其啟動。

遠端解除安裝工作完成時，所選應用程式從特定的裝置中移除。

遠端解除安裝問題

有時遠端解除安裝協力廠商應用程式可能會在結束時出現以下警告：“遠端解除安裝已在該裝置上完成，但有警告：要移除的應用程式未安裝。”當要解除安裝的應用程式已被解除安裝或者僅為單個使用者安裝時，會發生該問題。如果使用者未登入，則為單個使用者安裝的應用程式（也稱為按照使用者發放的應用程式）不可見或者無法進行遠端解除安裝。

該行為與同一裝置上供多名使用者使用的應用程式（也稱為按照裝置發放的應用程式）不同。按照裝置發放的應用程式可供裝置的所有使用者看見和存取。

因此，僅當使用者登入時才可解除安裝按照使用者發放的應用程式。

有關已安裝應用程式的資訊來源

網路代理從以下登錄機碼提取關於安裝在 Windows 裝置上的軟體的資訊：

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall
  包含關於為所有使用者安裝的應用程式的資訊。
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall
  包含關於為所有使用者安裝的應用程式的資訊。
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall
  包含關於為目前使用者安裝的應用程式的資訊。
- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall
  包含關於為特定使用者安裝的應用程式的資訊。

回溯物件到先前修訂

如果必要，您可以回溯對物件所做的變更。例如，您可能必須轉換政策設定到特定日期的狀態。

要回溯對物件所做的變更：

1. 在物件的內容視窗中，開啟**變更歷程**頁籤。
2. 在物件修訂清單中，選取您必須復原的修訂。
3. 點擊**回溯**按鈕。
4. 點擊**確定**以確認操作。

   該物件被回溯到所選修訂。物件修訂清單顯示所做的操作記錄。修訂敘述顯示了您轉換物件所到的修訂號的資訊。

復原操作僅適用於政策和工作物件。

工作

該部分描述了卡巴斯基安全管理中心使用的工作。

關於工作

卡巴斯基安全管理中心透過建立和執行*工作*來管理裝置上安裝的 Kaspersky 應用程式。安裝、啟用和停用應用程式、掃描檔案、更新病毒資料庫和軟體模組以及應用程式的其他行為均需要使用工作來完成。

特定應用程式的工作可以使用卡巴斯基安全管理中心網頁主控台建立，僅在該應用程式的管理外掛程式安裝在卡巴斯基安全管理中心網頁主控台伺服器上時。

工作可以在管理伺服器和裝置上執行。

管理伺服器上執行的工作包含以下：

- 自動發佈報告
- 將更新下載至儲存區
- 備份管理伺服器資料
- 資料庫維護

以下類型的工作在裝置上執行：

- *本機工作* — 在特定裝置上執行的工作。

  本機工作可以被管理員透過管理主控台工具修改，或者被遠端裝置使用者修改（例如，透過安全應用程式介面）。如果本機工作同時被管理員和受管理裝置使用者修改，管理員的修改將生效，因為其具有更高優先順序。

- *群組工作* — 在特定裝置上執行的工作。

  除非在工作內容中指定了其他項目，群組工作也影響所選群組的所有子群組。群組工作也影響（可選）佈署在其群組或子群組的連線到從屬和虛擬管理伺服器的裝置。

- *全域工作* — 選取指定裝置來執行的工作，與裝置屬於哪個管理群組無關。

您可以為每個應用程式建立任意數量群組工作、全域工作或本機工作。

您可以修改工作設定、檢視工作進度、複製、匯出、匯入和刪除工作。

只有當裝置上應用程式被執行，建立之工作才會執行。

工作執行結果儲存在每台裝置的作業系統事件記錄、管理伺服器作業系統事件記錄和管理伺服器資料庫中。

請勿在工作設定中包含私密資料。例如，避免指定網域管理員密碼。

關於工作範圍

*工作範圍*是執行工作的裝置集合。範圍的類型包括以下：

- 對於*本機工作*，範圍是裝置本身。
- 對於*管理伺服器工作*，範圍是管理伺服器。
- 對於*群組工作*，範圍是包含在群組中的裝置清單。

當建立*全域工作*時，您可以使用以下方法指定範圍：

- 手動指定特定裝置。

  您可以使用 IP 位址（或 IP 範圍）、NetBIOS 名稱或 DNS 名稱作為該裝置的位址。

- 從包含有要新增的裝置位址的 TXT 檔案來匯入裝置清單（每一個電腦位址必須單獨一行）。

  如果透過檔案匯入裝置清單或手動建立裝置清單，且如果裝置是以名稱定義，則清單可以只包含其資訊已被輸入到管理伺服器資料庫中的裝置。而且，資訊必須在裝置被連線或裝置發現中輸入。

- 指定裝置分類。

  後續，工作範圍隨著包含在分類中的裝置集的變更而變更。裝置分類可以基於裝置內容（包含安裝在裝置上的軟體）建立，也可以基於分配到裝置的標籤來建立。裝置分類是指定工作範圍的最靈活的方法。

  裝置分類的工作總是按管理伺服器排程執行。這些工作無法執行在缺少管理伺服器連線的裝置上。使用其他方法指定範圍的工作直接執行在裝置上，且因此不取決於到管理伺服器的裝置連線。

裝置分類的工作不會按裝置本機時間執行；相反，它們將按照管理伺服器本機時間執行。使用其他方法指定範圍的工作以裝置本機時間執行。

建立工作

要建立工作：

1. 在主功能表中，轉至 **裝置 → 工作**。
2. 點擊**新增**。

   新工作精靈啟動。遵循其說明。

3. 若要修改預設工作設定，請啟用**完成工作建立**頁面的**建立完成時開啟工作詳情**選項。如果您不啟用該選項，工作使用預設設定建立。您可以稍後隨時修改預設設定。
4. 點擊**完成**按鈕。

工作被建立並顯示在工作清單。

若要建立分配給所選裝置的新工作：

1. 在主功能表中，轉至 **裝置 → 受管理裝置**。

   受管理裝置清單隨即顯示。

2. 在受管理裝置清單中，選取裝置旁的核取方塊以為其執行工作。您可以使用搜尋和過濾功能來查找您正在尋找的裝置。

3. 點擊**執行工作**按鈕，然後選擇**新增一個新工作**。

   新工作精靈啟動。

   在精靈的第一步中，您可以刪除被選擇包含在工作範圍中的裝置。請按照精靈的步驟進行操作。

4. 點擊**完成**按鈕。

該工作是為選定的裝置建立的。

手動啟動工作

該應用程式會根據在各工作內容中指定的排程設定啟動工作。您可以隨時從工作清單中手動啟動工作。或者，您也可以在**受管理裝置**清單中選取裝置，然後對這些裝置啟動現有工作。

若要手動啟動工作：

1. 在主功能表中，轉至 **裝置 → 工作**。

2. 在工作清單中，請選取您要啟動之工作旁的核取方塊。

3. 點擊**"開始"**按鈕。

工作啟動。您可在**狀態**欄中檢視工作狀態或點擊**結果**按鈕。

檢視工作清單

您可檢視在卡巴斯基安全管理中心建立的工作清單。

若要檢視工作清單，

在主功能表中，轉至 **裝置 → 工作**。

工作清單隨即顯示。工作會依與應用程式名稱的關聯來分組。例如，*遠端解除安裝應用程式*工作會與管理伺服器相關，*弱點掃描和所需更新*工作指網路代理。

若要檢視工作內容，

請按一下工作的名稱。

工作內容視窗會一起顯示數個命名的頁籤。例如，**工作類型**會顯示在**一般**頁籤，以及工作排程—位於**排程**頁籤。

一般工作設定

此區段包含您可檢視與為大多數工作配置的清單。可用設定清單取決於您正在配置的工作。

工作建立過程中指定的設定

您可以在建立工作時指定以下設定。一些設定也可以在所建立工作的內容中修改。

- 作業系統重新啟動設定：
  - **不重新啟動裝置**

    用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

  - **重新啟動裝置**

    如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

  - **提示使用者操作**

    用戶端裝置螢幕上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。該選項適用於使用者必須可以選取最方便的時間進行重新啟動的工作站。

    預設情況下已選定此選項。

  - **重複提示間隔（分鐘）**

    如果啟用該選項，應用程式以指定頻率提示使用者重新啟動作業系統。

    預設情況下已啟用該選項。預設間隔是 5 分鐘。可用值介於 1 和 1440 分鐘之間。

    如果停用該選項，提示僅顯示一次。

  - **在該時間後重新啟動（分鐘）**

    提示使用者之後，應用程式在指定時間間隔後強制作業系統重新啟動。

    預設情況下已啟用該選項。預設延時是 30 分鐘。可用值介於 1 和 1440 分鐘之間。

  - **強制關閉已鎖定連線的應用程式**

    執行應用程式可能會阻止用戶端裝置重新啟動。例如，如果文件在文書處理應用程式中編輯且未儲存，應用程式不會允許裝置重新啟動。

    如果啟用該選項，鎖定裝置上的此類應用程式在裝置重新啟動前被強制關閉。結果，使用者可能遺失他們未儲存的變更。

    如果停用該選項，鎖定裝置不被重新啟動。此裝置上的工作狀態表示裝置需要重新啟動。使用者必須手動關閉所有執行在鎖定裝置上的應用程式並重新啟動這些裝置。

    預設情況下已停用該選項。

- 工作排程設定：

- **排程開始設定：**
  - **每 N 小時**

    工作定期執行，按照指定小時數間隔，從指定的日期和時間開始。

    預設下，工作每 6 小時執行一次，從目前系統日期和時間開始。

  - **每 N 天**

    工作定期執行，按照指定天數間隔。此外，您可指定第一個工作執行的日期與時間。這些額外選項會在您建立的工作受到應用程式支援時可用。

    預設下，工作每天執行一次，從目前系統日期和時間開始。

  - **每 N 星期**

    工作定期執行，按照指定星期數間隔，從指定的星期和時間開始。

    預設下，工作每星期一於目前系統時間執行一次。

  - **每 N 分鐘**

    工作定期執行，按照指定分鐘數間隔，從工作建立日期的指定時間開始。

    預設下，工作每 30 分鐘執行一次，從目前系統時間開始。

  - **每天（不支援日光節約時間）**

    工作定期執行，按照指定天數間隔。排程不支援日光節約時間 (DST)。這意味著在夏令時開始和結束時當時鐘向前或向後撥動一小時時，實際工作啟動時間不變更。

    我們不建議您使用該排程。它用於向後相容卡巴斯基安全管理中心。

    預設下，工作每天於目前系統時間執行一次。

  - **每週**

    工作每週在指定星期和指定時間執行。

  - **按每星期中的指定日**

    工作定期執行，在每周指定日期的指定時間。

    預設下，工作每週五 6:00:00 P.M. 執行。

  - **每月**

    工作定期執行，在指定月日的指定時間。

    在缺少指定日的月份，工作在最後一天執行。

    預設下，工作在每月的第一天執行，在目前系統時間。

- **手動**

  工作不自動執行。您僅可以手動啟動。

  預設情況下已選定此選項。

- **每個月在所選週的指定天**

  工作定期在指定月日的指定時間執行。

  預設情況下，不選取一個月中的任何一天。預設開始時間為 18:00。

- **當新更新下載至儲存區時**

  工作會在更新下載至儲存區時執行。例如，您可能希望使用此排程進行「尋找弱點和必要更新」工作。

- **在偵測到病毒爆發時**

  工作在發生*病毒爆發*事件後執行。選取將監控病毒爆發的應用程式類型。有下列應用程式類型可用：

  - 病毒防護工作站和檔案伺服器
  - 用於週邊防護的防毒軟體
  - 用於郵件伺服器的防毒軟體

  預設情況下選定所有應用程式類型。

  您可能想根據報告病毒爆發的安全應用程式類型執行不同的工作。此種情況下，刪除您不需要的應用程式類型選項。

- **在完成其它工作時**

  目前工作在其他工作完成後啟動。您可以選取先前工作如何結束（成功或帶有錯誤）以觸發目前工作的啟動。例如，您可能想使用***Turn on the device***選項執行開啟裝置工作，完成後，請執行*惡意軟體掃描*工作。只有當這兩項工作都被分配給相同的裝置時，此參數才會有作用。

- **執行略過的工作**

  該選項決定在工作要啟動時用戶端裝置在網路中不可見時工作的行為。

  如果啟用該選項，系統將在下一次在用戶端裝置上執行 Kaspersky 應用程式時嘗試啟動工作。如果工作排程是**手動**、**一次**或**立即**，裝置在網路中可見或包含在工作範圍後，工作會立即啟動。

  如果停用此選項，則僅限排程的工作會在用戶端裝置上執行。若為**手動**、**一次**與**立即**排程，工作僅會在網路上顯示的用戶端裝置上執行。例如，您可能想為消耗資源的工作停用該選項，您僅想在業餘時間執行該工作。

  預設情況下已停用該選項。

- **使用工作啟動自動隨機延遲**

如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動，即是，*分佈式工作啟動*。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

當工作被建立時，根據工作中包含用戶端裝置的數量，分發啟動時間被自動計算。然後，工作總是在計算的開始時間啟動。然後當工作設定被編輯或者工作被手動啟動時，計算的工作啟動時間值被變更。

如果該選項被停用，工作依據排程在用戶端裝置上啟動。

- **使用工作啟動隨機延遲間隔（分鐘）**

如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

如果該選項被停用，工作依據排程在用戶端裝置上啟動。

預設情況下已停用該選項。預設時間間隔為一分鐘。

- 要分配工作的裝置：
  - **選取管理伺服器偵測到的網路裝置**

    工作被分配到指定裝置。特定裝置可以包含管理群組的裝置和未配置的裝置。

    例如，您可能要在安裝網路代理到未配置的裝置的工作中使用該選項。

  - **手動指定裝置位址或從清單匯入位址**

    您可以指定您要為其分配工作的裝置的 NetBIOS 名稱、DNS 名稱、IP 位址和 IP 子網路。

    您可能要使用該選項以對特定子網路執行工作。例如，您可能要安裝特定應用程式到會計裝置，或者掃描疑似被感染子網路中的裝置。

  - **分配工作到裝置分類**

    該工作被分配到裝置選項中的裝置。您可以指定其中一個現有選項。

    例如，您可能要使用該選項在特定作業系統版本的裝置上執行工作。

  - **分配工作到管理群組**

    工作被分配到包含在管理群組中的裝置。您可以指定其中一個現有群組或者建立新群組。

    例如，您可能要使用該選項執行傳送訊息到使用者工作，如果訊息針對包含在特定管理群組中的裝置。

    如果工作被指派給管理群組，則工作屬性視窗中不會顯示**安全**標籤，因為群組工作受其所套用的群組的安全設定的約束。

- 帳戶設定：
  - **預設帳戶**

    在與執行該工作的應用程式相同的帳戶下執行該工作。

    預設情況下已選定此選項。

  - **指定帳戶**

    填寫**帳戶**與**密碼**欄位以指定工作要在其下執行的帳戶詳情。帳戶必須對此工作有足夠的權限。

  - **帳戶**

    執行該工作的帳戶。

  - **密碼**

    工作執行時使用的帳戶的密碼。

工作建立後指定的設定

您可以在建立工作後指定以下設定。

- 群組工作設定：
  - **分發到子群組**

    此選項僅在群組工作的設定中可用。

    啟用此選項時，工作範圍包括：
    - 您在建立工作時選擇的管理群組。
    - 依據群組層次結構從屬於所選管理群組的任何級別下的管理群組。

    停用此選項時，工作範圍僅包括您在建立工作時選擇的管理群組。

    預設情況下已啟用該選項。

  - **分發到從屬和虛擬管理伺服器**

    啟用此選項時，在主管理伺服器上有效的工作也將套用於從屬管理伺服器（包括虛擬伺服器）。如果從屬管理伺服器上已經存在相同類型的工作，則這兩個工作都將套用到從屬管理伺服器上 — 現有的工作和從主管理伺服器繼承的工作。

    此選項僅在**分發到子群組**選項已啟用的情況下可用。

    預設情況下已停用該選項。

- 進階排程設定：
  - **透過使用 Wake-On-LAN 功能在啟動工作之前開啟裝置（分鐘）**

    裝置上的作業系統在工作開始之前的指定時間啟動。預設時間段為五分鐘。

    如果您想要工作在工作範圍內的所有用戶端裝置上執行，包括工作要啟動時關閉的裝置，則啟用該選項。

    若要裝置在工作完成後自動關閉，請啟用**完成工作後關閉裝置**選項。此選項可在相同視窗中找到。

    預設情況下已停用該選項。

  - **完成工作後關閉裝置**

    例如，您可能想為每週五工作時間後安裝更新到用戶端裝置的更新安裝工作啟用該選項，然後在週末關閉這些裝置。

    預設情況下已停用該選項。

  - **停止工作，若時間超過（分鐘）**

在指定時間段過後，工作被自動停止，無論它是否完成。
如果您想要中斷或停止執行時間太長的工作，則啟用該選項。
預設情況下已停用該選項。預設工作執行時間是 120 分鐘。

- 通知設定：
  - **儲存工作歷程記錄**塊:
    - **儲存在管理伺服器資料庫上（天）**

      有關工作範圍內所有用戶端裝置上的工作執行的應用程式事件在指定的天數內被儲存在管理伺服器。當該時間段過後，資訊被從管理伺服器刪除。

      預設情況下已啟用該選項。

    - **儲存在裝置的作業系統事件記錄中**

      有關工作執行的應用程式事件被儲存在每個用戶端裝置的本機 Windows 事件記錄中。

      預設情況下已停用該選項。

    - **儲存在管理伺服器的作業系統事件記錄中**

      有關工作範圍內所有用戶端裝置上的工作執行的應用程式事件被集中儲存在管理伺服器作業系統 (OS) 的 Windows 事件記錄中。

      預設情況下已停用該選項。

    - **儲存所有事件**

      如果選取該選項，所有工作相關事件被儲存到事件記錄。

    - **儲存工作進度相關事件**

      如果選取該選項，僅工作執行相關事件被儲存到事件記錄。

    - **僅儲存工作執行結果**

      如果選取該選項，僅工作結果相關事件被儲存到事件記錄。

  - **通知管理員工作執行的結果**

    您可以選取管理員接收工作執行通知的方法：透過電子郵件、透過 SMS 和透過執行可執行檔。若要配置通知，請點擊**設定**連結。

    預設下，所有通知方法被停用。

  - **僅通知錯誤**

    如果該選項被啟用，管理員僅在工作執行完成但帶有錯誤時被通知。

    如果該選項被停用，管理員在每次工作執行完成後被通知。

    預設情況下已啟用該選項。

- 安全設定。
- 工作範圍設定。

  取決於工作範圍決定的方式，以下設定被展現：

  - **裝置**

    如果工作範圍由管理群組決定，您可以檢視該群組。這裡不可以變更。但您可設定**工作範圍排除項目**。

    如果工作範圍由裝置清單決定，您可以透過新增和刪除裝置修改該清單。

  - **裝置分類**

    您可以變更應用程式工作的裝置分類。

  - **工作範圍排除項目**

    您可以指定套用工作的裝置群組。要排除的群組僅可以是套用工作的管理群組的子群組。

- **變更歷程**。

匯出工作

卡巴斯基安全管理中心允許您將工作及其設定儲存到 KLT 檔案。您可以使用此 KLT 檔案匯入儲存的工作到卡巴斯基安全管理中心 Windows 和卡巴斯基安全管理中心 Linux。

要匯出工作，請執行以下操作：

1. 在主功能表中，轉至 **裝置 → 工作**。
2. 選取您要匯出之工作旁邊的核取方塊。

   您不能同時匯出多個工作。如果您選擇了多個工作，**匯出**按鈕將被停用。此外，管理伺服器工作也不供匯出。
3. 點擊**匯出**按鈕。
4. 在開啟的**另存新檔**視窗中，指定工作檔案的名稱和路徑。按一下**儲存**按鈕。

   另存新檔視窗僅當您使用 Google Chrome、Microsoft Edge 或 Opera 時才會顯示。如果您使用其他瀏覽器，工作檔案會自動儲存在**下載**資料夾。

匯入工作

卡巴斯基安全管理中心允許您從 KLT 檔案匯入工作。KLT 檔案包含匯出工作及其設定。

要匯入工作，請執行以下操作：

1. 在主功能表中，轉至 **裝置 → 工作**。
2. 點擊**匯入**按鈕。
3. 點擊**瀏覽**按鈕選擇要匯入的工作檔案。
4. 在開啟的視窗中，指定 KLT 工作檔案的路徑，然後按一下**開啟**按鈕。請注意，您只能選擇一個工作檔案。
   工作處理開始。
5. 工作處理成功後，選擇要將工作分配到哪些裝置。如要這麼做，請選擇以下選項之一：

   - **分配工作到管理群組**

     工作被分配到包含在管理群組中的裝置。您可以指定其中一個現有群組或者建立新群組。

     例如，您可能要使用該選項執行傳送訊息到使用者工作，如果訊息針對包含在特定管理群組中的裝置。

     如果工作被指派給管理群組，則工作屬性視窗中不會顯示**安全**標籤，因為群組工作受其所套用的群組的安全設定的約束。

   - **手動指定裝置位址或從清單匯入位址**

     您可以指定您要為其分配工作的裝置的 NetBIOS 名稱、DNS 名稱、IP 位址和 IP 子網路。

     您可能要使用該選項以對特定子網路執行工作。例如，您可能要安裝特定應用程式到會計裝置，或者掃描疑似被感染子網路中的裝置。

   - **分配工作到裝置分類**

     該工作被分配到裝置選項中的裝置。您可以指定其中一個現有選項。

     例如，您可能要使用該選項在特定作業系統版本的裝置上執行工作。

6. 指定工作範圍。
7. 點擊**完成**按鈕以完成工作匯入。

此時會顯示匯入結果通知。如果工作匯入成功，您可以按一下**詳細資訊**連結以檢視工作內容。

匯入成功後，工作會顯示在工作清單中。工作設定和排程也會一起匯入。工作將根據其排程來啟動。

如果新匯入的工作與現有工作的名稱相同，則匯入工作的名稱將加上 **(<next sequence number>)** 索引，例如：**(1)**、**(2)**。

啟動變更工作密碼精靈

對於非本機工作，您可在指定必須在其下執行工作的帳戶。您可在建立工作期間或在現有工作的內容中指定帳戶。若根據組織安全指示使用指定帳戶，這些指示可能不實需要變更帳戶密碼。當帳戶密碼過期且您設定了新密碼，工作將無法啟動直到您在工作內容中指定新的有效密碼。

變更工作密碼精靈可讓您自動在指定帳戶的所有工作中以新密碼取代密碼。或者，您可在各工作的內容中手動變更此密碼。

若要啟動變更工作密碼精靈：

1. 在主功能表中，轉至 **裝置** → **工作**。
2. 點擊**管理啟動工作的帳戶憑證**。

遵照精靈的說明。

步驟 1：指定憑證

指定您系統中目前有效的新憑證（例如在 Active Directory）。當您切換至精靈的下一步時，卡巴斯基安全管理中心會檢查指定帳戶名稱是否符合各個非本機內容中的帳戶名稱。若帳戶名稱相符，則工作內容中的密碼將自動取代為新的。

若要指定新帳戶，請選取選項：

- **使用目前帳戶**

  精靈會使用您目前登入卡巴斯基安全管理中心 網頁主控台的帳戶名稱。接著在**在工作中使用的目前密碼**欄位手動指定帳戶密碼。

- **指定不同帳戶**

  指定必須啟動工作的帳戶名稱。接著在**在工作中使用的目前密碼**欄位指定帳戶密碼。

若您填寫**先前密碼(可選，如果您要使用目前密碼更換它)**欄位，卡巴斯基安全管理中心僅會對已找到帳戶名稱與密碼的工作取代密碼。取代會自動執行。在所有其他情況下，您必須選擇進行精靈的下個步驟。

步驟 2：選取要採取的動作

若您未在精靈的第一步指定舊密碼或指定的舊密碼與工作內容中的密碼不符，您必須對已找到的工作選擇要採取的動作。

若要為工作選擇操作：

1. 選取您要為其選擇操作之工作旁邊的核取方塊。
2. 執行以下操作之一：

   - 若要移除工作內容中的密碼，請點擊**刪除憑證**。
     工作會切換為在預設帳戶下執行。
   - 若要用新的密碼取代，請點擊**即便舊密碼錯誤或未指定也強制密碼變更**。
   - 若要取消密碼變更，請點擊**未選擇操作**。

所選操作會在您移至精靈的下一步時套用。

步驟 3：檢視結果

在精靈的最後步驟中，檢視各個已找到工作的結果。要完成精靈，請點擊**完成**按鈕。

管理用戶端裝置

卡巴斯基安全管理中心允許您管理用戶端裝置：

- 檢視受管理裝置的設定和狀態，包括叢集和伺服器陣列。
- 配置發佈點。
- 管理工作。

您可以使用管理群組將用戶端裝置合併到一個集合中，並將其作為一個單元進行管理。一台客戶端裝置只能包含在一個管理群組中。裝置可以根據**規則條件**被自動分配到群組：

- 建立裝置移動規則。
- 複製裝置移動規則。
- 裝置移動規則的條件。

您可以使用裝置分類來根據條件過濾裝置。您也可以標記裝置以建立分類、尋找裝置以及在管理群組之間發佈裝置。

受管理裝置設定

要檢視受管理裝置設定：

1. 選擇**裝置→受管理裝置**。

   受管理裝置清單隨即顯示。

2. 在受管理裝置清單中，按一下有所需裝置名稱的連結。

所選裝置的屬性視窗隨即顯示。

以下分頁顯示在屬性視窗的上部，代表主設定群組：

- **一般**

此分頁包含以下區段：

- **一般**區域顯示有關用戶端裝置的一般資訊。資訊基於上一次用戶端裝置與管理伺服器之間的同步接收的資料來提供：
  - **名稱**

    在該欄位中，您可以檢視和修改管理群組中的用戶端裝置名稱。
  - **敘述**

    在該欄位中，您可以輸入用戶端裝置的附加敘述。
  - **裝置狀態**

    根據管理員針對裝置病毒防護狀態定義之條件，以及網路上裝置的活動所指派的用戶端裝置狀態。
  - **完整的群組名稱**

    包括了用戶端裝置的管理群組。
  - **上次更新的防護**

    裝置上病毒資料庫或應用程式最後更新日期。
  - **連線至管理伺服器**

    裝置上的網路代理上一次連線到管理伺服器的日期和時間。
  - **上一次可見**

    裝置在網路中最後可見的日期和時間。
  - **網路代理版本**

    安裝的網路代理的版本。
  - **建立日期**

    在 Kaspersky Security Center 中建立裝置的日期。
  - **裝置所有者**

    裝置擁有者的名稱。作為裝置擁有者，您可以點擊**管理裝置所有者**連接來分配或刪除使用者。

- **不斷開與管理伺服器的連線**

  如果啟用此選項，受管裝置和管理伺服器之間將保持持續連線。如果您使用的不是推送伺服器，您可能想要使用此選項，它提供了這樣的連線。

  如果停用此選項且不在使用推送伺服器，則受管理裝置將僅在同步資料或傳輸資訊時連線至管理伺服器。

  不斷開與管理伺服器的連線選項所能選取的最大裝置總數是 300。

  預設情況下，受管理裝置上停用此選項。預設情況下，此選項在安裝了管理伺服器的裝置上處於啟用狀態，即使您嘗試停用它也會保持啟用狀態。

- **網路**區段會顯示有關用戶端裝置網路屬性的以下資訊：

  - **IP 位址**

    裝置 IP 位址。

  - **Windows 網域**

    包含裝置的 Windows 網域或工作群組。

  - **DNS 名稱**

    用戶端裝置的 DNS 網域名稱。

  - **NetBIOS 名稱**

    用戶端裝置的 Windows 網路名稱。

  - **IPv6 位址**

- **系統**區段會顯示安裝在用戶端裝置上應用程式的相關資訊。

  - **作業系統**
  - **CPU 架構**
  - **裝置名稱**
  - **虛擬機類型**

    虛擬機製造商。

  - **作為 VDI 一部分的動態虛擬機**

    此行顯示用戶端裝置是否是作為 VDI 一部分的動態虛擬機。

- **防護**區域將提供有關用戶端裝置上病毒防護的目前狀態的一下資訊：

- **可見**

  用戶端裝置的可見性狀態。

- **裝置狀態**

  根據管理員針對裝置病毒防護狀態定義之條件，以及網路上裝置的活動所指派的用戶端裝置狀態。

- **狀態敘述**

  用戶端裝置防護狀態和與管理伺服器的連線。

- **防護狀態**

  該欄位顯示目前的用戶端裝置即時防護狀態。

  當裝置狀態變更時，新狀態僅在用戶端裝置與管理伺服器同步之後顯示在裝置屬性視窗。

- **上一次完整掃描**

  用戶端裝置上執行的最後一次惡意軟體掃描的日期和時間。

- **偵測到的病毒**

  自安裝安全應用程式（第一次掃描）或自上次重設威脅計數器以來，在用戶端裝置上偵測到的威脅總數。

- **解毒失敗的物件**

  用戶端裝置上的未處理檔案數量。

  該欄位行動裝置上的未處理檔案數量。

- **磁碟加密狀態**

  裝置本機磁碟機上的目前檔案加密狀態。有關狀態的說明，請參閱 Kaspersky Endpoint Security for Windows 說明。

- **應用程式定義的裝置狀態**區段會提供相關資訊，說明由裝置上安裝的受管理應用程式所定義的裝置狀態。該裝置狀態可能與卡巴斯基安全管理中心定義的狀態不同。

- **應用程式**

此標籤列出了用戶端裝置上安裝的所有卡巴斯基應用程式。此標籤包含的**開始**和**停止**按鈕可讓您啟動和停止選定的卡巴斯基應用程式（不包括網路代理）。如果受管理裝置上的連接埠 15000 UDP可用於接收來自管理伺服器的推播通知，則可以使用這些按鈕。如果受管理裝置無法用於推播通知，但啟用了與管理伺服器的連續連線模式（啟用了**不斷開與管理伺服器的連線**部分中的**一般**選項），則**開始**和**停止**按鈕也可用。否則，當您嘗試啟動或停止應用程式時，會顯示錯誤訊息。您也可以按一下應用程式名稱以檢視有關該應用程式的一般資訊、裝置上發生的事件清單以及應用程式設定。

- **啟用政策和政策設定檔**

  此標籤會列出分派給受管理裝置的政策和政策設定檔。

- **工作**

  在**工作**標籤上，您可以管理用戶端工作：檢視現有工作清單、建立新工作、移除、啟動和停止工作、修改工作設定以及檢視執行結果。該工作清單會根據用戶端最近一次與管理伺服器同步的連線期間所收到的資料提供。管理伺服器向用戶端裝置請求工作狀態詳情。如果受管理裝置上的連接埠 15000 UDP可用於接收來自管理伺服器的推播通知，則會顯示工作狀態並啟用用於管理工作的按鈕。如果受管理裝置無法用於推播通知，但啟用了與管理伺服器的連續連線模式（啟用了**一般**部分中的**不斷開與管理伺服器的連線**選項），則也可對工作進行操作。

  如果未建立連線，則不顯示狀態，按鈕被停用。

- **事件**

  事件標籤將顯示選定用戶端裝置在管理伺服器上所記錄事件的資訊。

- **事件**

  在**事件**頁簽中，您可為用戶端裝置檢視、編輯和建立事件。事件可以透過安裝在用戶端裝置上的受管理卡巴斯基應用程式自動建立，也可以由管理員手動建立。例如，如果使用者定期將惡意軟體從其卸除式磁碟機移至裝置，則管理員可以建立事件。管理員可以在事故文字中提供情況的簡要說明和建議的操作（例如對於一個使用者的紀律性操作），還可以新增連結到使用者。

  對其採用了所有必要操作的事件稱為*已處理*事件。存在的未處理事件可被選為將裝置的狀態變更為*緊急*或*警告*的條件。

  此部分包含已為裝置建立的事故的清單。事故按照幾個等級和類型分類。事故類型由建立事故的 Kaspersky 應用程式定義。選中**已處理**列中的方塊即可突出顯示清單上的已處理事件。

- **標籤**

  在**標籤**分頁，您可以編輯用來尋找用戶端裝置的關鍵字清單，並可以檢視現有標籤清單、從清單中配置標籤、設定自動標記規則、新增標籤和重新命名舊標籤以及移除標籤。

- **進階**

此分頁包含以下區段：

- **應用程式登錄資料**。在此區域，您可以檢視用戶端裝置上安裝的應用程式及其更新的登錄檔，您還可以設定應用程式登錄資料的顯示方式。

  如果用戶端裝置上安裝的網路代理將所需資訊傳送到管理伺服器，則將提供有關已安裝應用程式的資訊。您可以在網路代理或其政策的內容視窗中的**儲存區**區域，設定將資訊傳送到管理伺服器。

  按一下應用程式名稱會開啟一個視窗，其中包含應用程式詳細資訊以及為該應用程式安裝的更新軟體套件的清單。

- **可執行檔**。此區域會顯示在用戶端裝置上發現的可執行檔案。

- **發佈點**。該區域提供裝置與之互動的發佈點清單。

  - **匯出至檔案**

    按一下**匯出至檔案**按鈕儲存裝置與之互動的發佈點清單檔案。預設下，應用程式匯出裝置清單到 CSV 檔案。

  - **內容**

    按一下**屬性**按鈕檢視和配置裝置與之互動的發佈點。

- **硬體登錄資料**。在此區域，您可以檢視安裝在用戶端裝置上的硬體資訊。

- **可用更新**。該區域顯示在該裝置上發現的未安裝的軟體更新清單。

- **軟體弱點**。此區域會顯示安裝在用戶端裝置上的協力廠商應用程式的弱點資訊。

  若要將弱點儲存到檔案中，請選擇要儲存之弱點旁邊的核取方塊，然後點擊「確定」，接著點擊**將行匯出到 csv 檔案**按鈕或**將行匯出到 txt 檔案**按鈕。

  區段會包含以下設定：

  - **僅顯示可以被修復的弱點**

    如果啟用此選項，該區域會顯示可透過使用修補程式修復的弱點。

    如果停用此選項，該區域會同時顯示可透過使用修補程式修復的弱點，以及未發佈修補程式的弱點。

    預設情況下已啟用該選項。

  - **弱點內容**

選取清單中的軟體弱點並按一下名稱，以在個別視窗中檢視所選軟體弱點的屬性。在視窗中，您可以進行以下操作：

- 在這部受管理的裝置忽略軟體弱點（在管理主控台或在卡巴斯基安全管理中心網頁主控台）。
- 檢視對弱點的建議修復清單。
- 手動指定軟體更新以修復弱點（在管理主控台或在卡巴斯基安全管理中心網頁主控台）。
- 檢視弱點實例。
- 檢視要修復弱點的現有工作清單，並建立新工作來修復弱點。

- **遠端診斷**。在本節中，您可以執行用戶端裝置的遠端診斷。

建立管理群組

立即安裝卡巴斯基安全管理中心後，管理群組的階層結構僅會包含一個稱為**受管理裝置**的管理群組。當建立管理群組階層架構時，您可以將裝置（包括虛擬機器）新增到**受管理裝置**群組中，也可以新增嵌套群組（參閱下圖）。



檢視管理群組階層架構

要建立管理群組，請執行以下操作：

1. 在主功能表中，轉至 **裝置 → 群組的階層**。
2. 在管理群組結構中，選取要加入新管理群組的管理群組。
3. 點擊**新增**按鈕。
4. 在開啟的**新管理群組名稱**視窗中，輸入群組名稱，然後點擊**新增**按鈕。

管理群組階層中將顯示帶有指定名稱的新管理群組。

程式允許基於 Active Directory 的架構或域網架構建立管理群組結構。您也可以從文字檔案建立群組架構。

要建立管理群組的架構：

1. 在主功能表中，轉至 **裝置 → 群組的階層**。
2. 點擊**匯入**按鈕。

新管理群組架構精靈啟動。遵照精靈的說明。

將裝置手動新增至管理群組

您可用下列方式將裝置自動移至管理群組：建立裝置移動規則、手動將裝置從某一管理群組移至另一個，或將裝置新增至選取的管理群組。下節說明如何手動將裝置新增至管理群組。

新增一或多個裝置至選取的管理群組：

1. 在主功能表中，轉至 **裝置 → 受管理裝置**。
2. 按一下清單上方的**目前路徑：** `<current path>` 連結。
3. 在開啟的視窗中，選取您要向其新增裝置的管理群組。
4. 點擊**新增裝置**按鈕。
   行動裝置精靈啟動。
5. 列出您希望新增裝置的管理群組。

   > 您只可新增建立裝置時或裝置發現後已將資訊新增至管理伺服器資料庫的裝置。

   選取您希望將裝置新增至清單的方式：

   - 點擊**新增裝置**按鈕，接著以下列其中一種方式指定裝置：
     - 從管理伺服器偵測到的裝置清單中選取該裝置。
     - 指定裝置 IP 位址或 IP 範圍。
     - 指定裝置 NetBIOS 名稱或 DNS 名稱。

       > 裝置名稱欄位不得包含空格以及以下禁用字元：\ / * ; : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %

   - 點擊**從檔案匯入裝置**按鈕以從 .txt 檔案匯入裝置清單。各裝置位址或名稱均需在獨立的資料行中指定。

     > 檔案不得包含空格或者以下禁用字元：\ / * ; : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %

6. 檢視要新增至管理群組的裝置清單。您可新增或移除裝置來編輯清單。
7. 確認清單正確後，請點擊**下一步**按鈕。

精靈會處理裝置清單並顯示結果。系統會將已成功處理的裝置新增至管理群組，並顯示在管理伺服器產生的名稱下的裝置清單中。

將裝置手動移動至管理群組

您可將裝置從一個管理群組移至另一個，或從未配置的裝置群組移至另一個管理群組。

要把一台或多台裝置新增至一個選定的管理群組中，請執行以下操作：

1. 從您要移動裝置的位置開啟管理群組。要這麼做，請執行以下操作之一：
   - 要開啟管理群組，請在主功能表中轉到**裝置→受管理裝置**，點擊**目前路徑**字段中的路徑連接，然後在開啟的左側窗格中選擇一個管理群組。
   - 若要開啟**未配置的裝置**群組，請在主功能表中前往**發現和佈署 → 未配置的裝置**。
2. 選取您要移至不同群組之裝置旁的核取方塊。
3. 點擊**移至群組**按鈕。
4. 在管理群組階層中，選取您要將選取的裝置移至管理群組旁的核取方塊。
5. 點擊**移動**按鈕。

選取的裝置會移至選取的管理群組。

建立裝置移動規則

您可以設定裝置移動規則，即自動分配裝置到管理群組的規則。

要建立移動規則：

1. 在主功能表中，轉至 **裝置 → 移動規則**。
2. 點擊**新增**。

3. 在開啟的視窗中，在**一般**頁籤指定以下資訊：

- **規則名稱**

  輸入新規則名稱。
  如果您正複製規則，新規則與來源規則名稱相同，但是索引格式（ ）被新增到名稱，例如：（1）。

- **管理群組**

  選取要自動移動裝置的管理群組。

- **套用規則**

  您可以選取以下選項之一：

  - **對每台裝置執行一次**
    規則對比對標準的每台裝置套用一次。
  - **對每台裝置執行一次，然後在每次網路代理重新安裝時執行**
    規則對比對標準的每台裝置套用一次，然後僅在網路代理被重新安裝到這些裝置時。
  - **持續套用規則**
    規則根據管理伺服器自動設定的排程被套用（通常每幾個小時）。

- **僅移動不屬於任何管理群組的裝置**

  如果啟用該選項，僅未配置的裝置將被移動到所選群組。
  如果停用該選項，已經屬於其他管理群組的裝置以及未配置的裝置將被移動到所選群組。

- **啟用規則**

  如果啟用該選項，規則被啟用並在被儲存後開始工作。
  如果停用該選項，規則被建立，但不被啟用。直到您啟用該選項它才工作。

4. 在**規則條件**頁簽上，指定至少一個標準，裝置將根據該標準被移至管理群組。

5. 點擊**儲存**。

移動規則被建立。它顯示在移動規則清單。

位置在清單中越高，規則的優先順序越高。要提高或降低移動規則的優先順序，請使用滑鼠分別在清單中向上或向下移動規則。

如果選擇**持續套用規則**選項，無論優先順序設定為何都會套用移動規則。此類規則係根據管理伺服器自動設定的時間表來套用。

如果裝置內容滿足多個規則的條件，裝置被移動到具有高優先順序的規則的目的群組。

複製裝置移動規則

您可以複製移動規則，例如，如果您要對不同目標管理群組擁有幾個相同規則。

要複製現有移動規則：

1. 執行以下操作之一：

   - 在主功能表中，轉至 **裝置 → 移動規則**。
   - 在主功能表中，轉至 **發現和佈署 → 佈署和分配 → 移動規則**。

   移動規則清單被顯示。

2. 選取您要複製的規則旁邊的核取方塊。
3. 點擊**複製**。

4. 在開啟的視窗中，變更在**一般**頁籤的以下資訊，若您緊要複製規則而不改變其設定，請不要進行任何變更：

- **規則名稱**

  輸入新規則名稱。
  如果您正複製規則，新規則與來源規則名稱相同，但是索引格式（ ）被新增到名稱，例如：（1）。

- **管理群組**

  選取要自動移動裝置的管理群組。

- **套用規則**

  您可以選取以下選項之一：
  - **對每台裝置執行一次**
    規則對比對標準的每台裝置套用一次。
  - **對每台裝置執行一次，然後在每次網路代理重新安裝時執行**
    規則對比對標準的每台裝置套用一次，然後僅在網路代理被重新安裝到這些裝置時。
  - **持續套用規則**
    規則根據管理伺服器自動設定的排程被套用（通常每幾個小時）。

- **僅移動不屬於任何管理群組的裝置**

  如果啟用該選項，僅未配置的裝置將被移動到所選群組。
  如果停用該選項，已經屬於其他管理群組的裝置以及未配置的裝置將被移動到所選群組。

- **啟用規則**

  如果啟用該選項，規則被啟用並在被儲存後開始工作。
  如果停用該選項，規則被建立，但不被啟用。直到您啟用該選項它才工作。

5. 在**規則條件**標籤上，為要自動移動的裝置指定至少一個條件。

6. 點擊**儲存**。

新移動規則被建立。它顯示在移動規則清單。

裝置移動規則的條件

當您建立或者複製將用戶端裝置移動到管理群組的規則時，在**規則條件**頁籤上，設定移動裝置的條件。如要確定要移動哪些裝置，您可以使用以下標準：

- 分配給用戶端裝置的標籤。
- 網路參數。例如，您可以移動具有指定範圍內 IP 位址的裝置。

- 安裝在用戶端裝置上的受管應用程式，例如網路代理或管理伺服器。
- 虛擬機，即用戶端裝置。
- 具有用戶端裝置的 Active Directory 組織單位 (OU) 相關資訊。
- 具有用戶端裝置的雲端區段相關資訊。

下面，您可以找到有關如何在裝置移動規則中指定此資訊的描述。

如果您在規則中指定了多個條件，則 AND 邏輯運算子起作用並且所有條件同時套用。如果您不選擇任何選項或將某些欄位留空，則此類條件不套用。

標籤標籤

在此標籤上，您可以基於先前新增到受管理裝置的裝置標籤設定裝置移動規則。為此，請選擇所需的標籤。此外，您可以啟用以下選項：

- **套用到沒有指定標籤的裝置**

  如果啟用此選項，則具有指定標籤的所有裝置都將被從裝置移動規則中排除。如果停用此選項，則裝置移動規則套用到具有所有選定標籤的裝置。

  預設情況下已停用該選項。

- **如果有至少一個指定的標籤符合則套用**

  如果啟用此選項，則裝置移動規則將套用到具有至少一個選定標籤的用戶端裝置。如果停用此選項，則裝置移動規則套用到具有所有選定標籤的裝置。

  預設情況下已停用該選項。

網路標籤

在此頁簽上，您可以指定裝置移動規則要考慮的裝置的網路資料：

- **Windows 網路中的裝置名稱**

  裝置的 Windows 網路名稱（NetBIOS 名稱），或者 IPv4 或 IPv6 位址。

- **Windows 網域**

  裝置移動規則會套用於指定 Windows 網域中包含的所有裝置。

- **裝置的 DNS 名稱**

  您要移動的用戶端裝置的 DNS 網域名稱。如果您的網路包含 DNS 伺服器，請填寫此欄位。

  如果為您用於卡巴斯基安全管理中心的資料庫設定了區分大小寫的排序規則，請在指定裝置 DNS 名稱時保持大小寫。否則，裝置移動規則將不起作用。

- **DNS 網域**

  裝置移動規則套用於指定主 DNS 後綴中包括的所有裝置。如果您的網路包含 DNS 伺服器，請填寫此欄位。

- **IP 範圍**

  如果啟用此選項，您可以輸入應該包括相關裝置的 IP 範圍的初始和最終 IP 位址。

  預設情況下已停用該選項。

- **用於連線管理伺服器的 IP 位址**

  如果啟用此選項，您可以設定用戶端裝置連線到管理伺服器的 IP 地址。為此，請指定包括所有必要 IP 位址的 IP 範圍。

  預設情況下已停用該選項。

- **裝置在 IP 範圍中**

  如果啟用此選項，您可以選擇先前在**IP 範圍**部分新增的 IP 範圍。相關裝置必須包含在所選的 IP 範圍內。

  預設情況下已停用該選項。

- **連線設定檔已變更**

  您可以選取以下值之一：

  - **是**。裝置移動規則僅套用於連線設定檔已變更的用戶端裝置。
  - **否**。裝置移動規則僅套用於連線設定檔未變更的用戶端裝置。
  - **未選取值**。該條件不適用。

- **由不同管理伺服器管理**

  您可以選取以下值之一：

  - **是**。裝置移動規則僅套用於由其他管理伺服器管理的用戶端裝置。這些伺服器與您配置裝置移動規則的伺服器不同。
  - **否**。裝置移動規則僅套用於由目前管理伺服器管理的用戶端裝置。
  - **未選取值**。該條件不適用。

應用程式標籤

在此頁籤上，您可以根據用戶端裝置上安裝的受管應用程式和作業系統設定裝置移動規則：

- **網路代理已安裝**

  您可以選取以下值之一：

  - **是**。裝置移動規則僅適用於安裝了網路代理的用戶端裝置。
  - **否**。裝置移動規則僅適用於未安裝網路代理的用戶端裝置。
  - **未選取值**。該條件不適用。

- **應用程式**

  指定應在用戶端裝置上安裝哪些受管應用程式，以便裝置移動規則套用於這些裝置。例如，您可以選擇**卡巴斯基安全管理中心 14.2 網路代理**或**卡巴斯基安全管理中心 14.2 管理伺服器**。

  如果您不選擇任何受管應用程式，則該條件不適用。

- **作業系統版本**

  您可以根據作業系統版本剔除用戶端裝置。為此，請指定應安裝在用戶端裝置上的作業系統。因此，裝置移動規則將套用到具有所選作業系統的用戶端裝置。

  如果您不啟用此選項，則條件不適用。依預設已停用該選項。

- **作業系統 bit 大小**

  您可以透過作業系統位元大小來剔除用戶端裝置。在**作業系統 bit 大小**欄位，您可以選擇以下一個值：

  - **未知**
  - **x86**
  - **AMD64**
  - **IA64**

  要檢查用戶端裝置的作業系統位元大小：

  1. 在主功能表中，轉至 **裝置 → 受管理裝置**。
  2. 在右側點擊**欄設定**按鈕 (⚙)。
  3. 選擇**作業系統 bit 大小**選項，然後點擊**儲存**按鈕。

     之後，將顯示每個受管理裝置的作業系統位元大小。

- **作業系統服務套件版本**

  在該欄位中，可以指定作業系統的更新套件版本（採用 *X.Y* 格式），這將決定將移動規則套用到裝置的方式。預設情況下，不指定版本值。

- **使用者憑證**

  您可以選取以下值之一：

  - **已安裝**。裝置移動規則僅套用到具有行動憑證的行動裝置。
  - **未安裝**.裝置移動規則僅套用到沒有行動憑證的行動裝置。
  - **未選取值**。該條件不適用。

- **作業系統版本**

  該設定僅套用到 Windows 作業系統。

  您可以指定所選作業系統是否必須具有相等、更早或更晚的版本號。您也可以設定對所有版本號的裝置移動規則，除了指定的版本號。

- **作業系統發佈號**

  該設定僅套用到 Windows 作業系統。

  您可以指定所選作業系統是否必須具有相等、更早或更晚的發行版本號。您也可以設定對所有發行版本號的裝置移動規則，除了指定的版本號。

虛擬機頁簽

在此頁籤上，您可以根據用戶端是否是虛擬機或虛擬桌面基礎架構 (VDI) 的一部分來設定裝置移動規則：

- **這是一台虛擬機**

  在該下拉清單中，您可以選取以下一個值：
  - **N/A**。該條件不適用。
  - **否**。移動不是虛擬機的裝置。
  - **是**。移動是虛擬機的裝置。

- **虛擬機類型**
- **虛擬桌面基礎架構的一部分**

  在該下拉清單中，您可以選取以下一個值：
  - **N/A**。該條件不適用。
  - **否**。移動不屬於 VDI 的裝置。
  - **是**。移動屬於 VDI 的裝置。

Active Directory 頁簽

在此頁籤上，您可以指定必須移動 Active Directory OU 中包含的裝置。您還可以移動指定 Active Directory OU 所有子 OU 中的裝置。

- **裝置在 Active Directory 組織單元中**

  如果啟用此選項，則裝置移動規則將套用於該選項下清單中指定 Active Directory 組織單元中的裝置。
  預設情況下已停用該選項。

- **包括子組織單元**

  如果啟用此選項，選取範圍將包括指定 Active Directory 組織單元的所有子組織單元中的裝置。
  預設情況下已停用該選項。

- **將裝置從子單元移動到對應子群組**
- **建立對應於新偵測到裝置的容器的子群組**

- **刪除 Active Directory 中不存在的子群組**
- **該裝置是 Active Directory 群組成員**

  如果啟用此選項，裝置移動規則將套用於該選項下清單中指定 Active Directory 群組中的裝置。

  預設情況下已停用該選項。

雲端區段頁簽

在此頁籤上，您可以指定必須移動屬於特定雲端區段的裝置：

- **裝置在雲端區段中**

  如果選擇此選項，則裝置移動規則將套用於屬於雲端區段的用戶端裝置。您可以在選項下的清單中選擇所需的雲端區段，甚至選擇子網路。

  依預設已停用該選項。

- **包含子物件**

  如果選擇此選項，則裝置移動規則不僅會套用於所選雲端區段，也會套用於該區段的子物件。

  依預設已停用該選項。

- **從嵌套物件移動裝置到對應子群組**
- **建立對應於新偵測到裝置的容器的子群組**
- **刪除在雲端區段中找不到比對的子群組**
- **使用 API 發現的裝置**

  在下拉清單，您可以選取裝置是否由 API 工具偵測：

  - **AWS**。裝置使用 AWS API 發現，就是，裝置在 AWS 雲端環境中。
  - **Azure**。裝置使用 Azure API 發現，就是，裝置在 Azure 雲端環境中。
  - **Google Cloud**。裝置被使用 Google API 發現，即裝置一定在 Google 雲端環境中。
  - **否**。系統無法用 AWS、Azure 或 Google API 偵測裝置，意即裝置在雲端環境外或在雲端環境中，但無法使用 API 加以偵測。
  - **沒有值**。這項條件不適用。

當裝置顯示不活動時檢視和配置操作

如果組中的用戶端裝置不活動，您可以獲取關於它的通知。您也可以自動刪除此類裝置。

要在組中裝置顯示不活動時檢視或設定操作：

1. 在主功能表中，轉至 **裝置 → 群組的階層**。
2. 點擊所需管理群組的名稱。
   管理群組內容視窗將開啟。
3. 在內容視窗中，前往**設定**頁籤。
4. 在**繼承**區段，啟用或停用以下選項：

   - **從父群組繼承**

     該區域的設定將從包含用戶端裝置的父群組繼承。如果啟用此選項，**網路中的裝置活動**下的設定會禁止任何變更。

     該選項僅在管理群組擁有父群組時可用。

     預設情況下已啟用該選項。

   - **在子群組中強制繼承設定**

     該設定值將被分發到子群組，但在子群組的內容中這些設定被鎖定。

     預設情況下已停用該選項。

5. 在**裝置活動**區段，啟用或停用以下選項：

   - **若裝置未活動超過下列天數，則通知管理員**

     如果啟用該選項，管理員接收不活動裝置的通知。您可以指定**裝置在網路上已長時間沒有活動**事件被建立的時間間隔。預設時間間隔為 7 天。

     預設情況下已啟用該選項。

   - **若裝置未活動超過下列天數，則從群組刪除裝置**

     如果啟用該選項，您可以指定從組中自動移除裝置的時間間隔。預設時間間隔為 60 天。

     預設情況下已啟用該選項。

6. 點擊**儲存**。

   您的變更已儲存並套用。

關於裝置狀態

卡巴斯基安全管理中心會為每部受管理裝置指派狀態。特定狀態會根據是否符合使用者定義的條件而指派。在有些情況下，指派狀態給裝置時，卡巴斯基安全管理中心會考量裝置在網路中的能見度標記（請參閱下表）。若卡巴斯基安全管理中心在兩小時內未在網路中找到裝置，裝置的能見度標記會設為*不可見*。

這些狀態如下：

- *緊急*或*緊急/可見*
- *警告*或*警告/可見*
- *正常*或*正常/可見*

下表列出在指派給裝置的*緊急*或*警告*狀態時必須符合的預設條件，其中包含所有可能的值。

分配狀態到裝置的條件

條件	條件敘述	可用值
安全應用程式未安裝	網路代理已安裝到裝置，但是安全應用程式未安裝。	• 開關按鈕被開啟。 • 開關按鈕被關閉。
偵測到太多病毒	一些病毒被病毒偵測工作在裝置上發現，例如，*惡意軟體掃描*工作，且發現的病毒數量超過指定值。	大於 0。
即時防護不符合管理員的設定等級	裝置在網路中可見，但即時防護等級與管理員在裝置狀態條件中設定的等級不同。	• 已停止。 • 已暫停。 • 執行中。
惡意軟體掃描已長時間未執行	裝置在網路中可見且安全應用程式已安裝到裝置，但*惡意軟體掃描*工作在指定時間內未執行。條件僅套用到於 7 天之前或更早新增到管理伺服器資料庫的裝置。	多於 1 天。
資料庫已過期	裝置在網路中可見且安全應用程式已安裝到裝置，但病毒資料庫在指定時間內未在該裝置上更新。條件僅套用到於 1 天之前或更早新增到管理伺服器資料庫的裝置。	多於 1 天。
長時間未連線	網路代理已安裝到裝置，但由於裝置關閉，裝置在指定時間段內未連線到管理伺服器。	多於 1 天。
偵測到活動威脅	**活動威脅**資料夾中的未處理的物件的數量超過指定的值。	多於 0 個項目。
需要重新啟動	裝置在網路中可見，但應用程式基於所選原因之一在指定時間之前請求裝置重新啟動。	多於 0 分鐘。
安裝了不相容的應用程式	裝置在網路中可見，但透過網路代理執行的軟體清查在裝置上偵測到了不相容的應用程式。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
偵測到軟體弱點	裝置在網路中可見且網路代理已安裝到裝置，但*弱點掃描和所需更新*工作在裝置應用程式中偵測到指定嚴重等級的弱點。	• 緊急。 • 高。 • 中等。 • 如果弱點無法被修補則略過。 • 如果為安裝分配了更新則略過。
產品授權已到期	裝置在網路中可見，但產品授權已過期。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
產品授權即將到期	裝置在網路中可見，但裝置上的產品授權即將在指定天數內過期。	少於 0 天。
Windows Update 更新檢查已長時間未執行	裝置在網路中可見，但「*執行 Windows 更新同步*」工作在指定時間段內未執行。	多於 1 天。

條件	條件敘述	可用值
無效的加密狀態	網路代理已安裝到裝置，但裝置加密結果等於指定值。	• 由於使用者拒絕未遵從政策（僅對外部裝置）。 • 由於錯誤未遵從政策。 • 套用政策時需要重新啟動。 • 未指定加密政策。 • 不支援。 • 當套用政策時。
行動裝置設定與政策不同	行動裝置設定不同於 Kaspersky Endpoint Security for Android 政策中指定的設定。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
偵測到未處理的事件	裝置上發現了一些未處理的事故。事件可以透過安裝在用戶端裝置上的受管理卡巴斯基應用程式自動建立，也可以由管理員手動建立。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
應用程式定義的裝置狀態	裝置狀態由受管理應用程式定義。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
裝置磁碟空間不足	裝置剩餘磁碟空間少於指定值或裝置無法與管理伺服器同步。當裝置已與管理伺服器成功同步且裝置上的剩餘空間大於或等於指定值時，*緊急*或*警告*狀態被變更為*正常*狀態。	大於 0 MB。
裝置已失去管理	在裝置發現過程中，裝置在網路中可見，但是超過三次嘗試與管理伺服器同步都失敗了。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
防護已停用	裝置在網路中可見，但裝置上的安全應用程式已被停用大於指定的時間段。 在這種情況下，安全應用程式的狀態為*stopped*或*failure*，不同於下列狀態：*starting*、*running*或*suspended*。	多於 0 分鐘。
安全應用程式沒有執行	裝置在網路中可見且安全應用程式已安裝到裝置，但其未在執行。	• 開關按鈕被關閉。 • 開關按鈕被開啟。

卡巴斯基安全管理中心允許您設定管理群組中裝置狀態在指定條件滿足時的自動轉換。當指定條件滿足時，用戶端裝置被分配以下狀態之一：*緊急*或*警告*。未滿足特定條件時，系統會為用戶端裝置指派*正常*狀態。

一個條件的不同值可對應於不同的狀態。例如，依預設，若**資料庫已過期**條件有**多於 3 天**的值，則用戶端裝置會被指派*警告*狀態，逖值為**多於 7 天**，則會指派*緊急*狀態。

如果您從以前的版本升級卡巴斯基安全管理中心，指定*緊急*或*警告*狀態的 **資料庫已過期** 條件的值不會改變。

當卡巴斯基安全管理中心指派狀態給裝置時，對於有些條件（請參閱條件說明欄），系統會將能見度標記列入考量。例如，若受管理裝置因符合資料庫已過期條件而被指派*緊急*狀態，之後能見度標記也已針對該裝置設定，則裝置會被指派*正常*狀態。

設定裝置狀態轉換

您可變更條件以為裝置配置*緊急*或*警告*狀態。

要啟用變更裝置狀態到緊急：

1. 在主功能表中，轉至 **裝置 → 群組的階層**。
2. 在開啟的群組清單中，針對您要變更切換裝置狀態的群組，點擊有該群組名稱的連結。
3. 在開啟的工作內容視窗中，選取**裝置狀態**頁籤。
4. 在左方窗格中，選取**緊急**。
5. 在右方窗格中的**若指定以下條件，則設為"緊急"**區段，啟用將裝置切換為*緊急*狀態的條件。

   然而，您可以變更在父政策中未鎖定的設定。

6. 在清單中選取條件旁的選項按鈕。
7. 在清單左上角，點擊**編輯**按鈕。
8. 為所選條件設定所需的值。
   可以不為每個條件設定值。
9. 點擊**確定**。

未滿足特定條件時，系統會為受管理裝置配置*緊急*狀態。

要啟用變更裝置狀態到警告：

1. 在主功能表中，轉至 **裝置 → 群組的階層**。
2. 在開啟的群組清單中，針對您要變更切換裝置狀態的群組，點擊有該群組名稱的連結。
3. 在開啟的工作內容視窗中，選取**裝置狀態**頁籤。
4. 在左方窗格中，選取**警告**。
5. 在右方窗格中的**若指定以下條件，則設為"警告"**區段，啟用將裝置切換為*警告*狀態的條件。

   然而，您可以變更在父政策中未鎖定的設定。

6. 在清單中選取條件旁的選項按鈕。
7. 在清單左上角，點擊**編輯**按鈕。
8. 為所選條件設定所需的值。
   可以不為每個條件設定值。
9. 點擊**確定**。

未滿足特定條件時，系統會為受管理裝置配置*警告*狀態。

用戶端裝置的遠端桌面連線

管理員可以在安裝網路代理的用戶端裝置上使用遠端桌面連線。如果裝置的 TCP 和 UDP 連接埠關閉，也可透過網路代理遠端連線至用戶端裝置。

在與裝置建立連線後，管理員會獲取對此裝置上儲存資訊的完全存取權限，以便他或她可以管理其上安裝的應用程式。

您必須在目標受管理裝置的作業系統設定中允許目標遠端連線。例如，在 Windows 10 中，此選項名為**允許遠端協助連線至此電腦**（您可在**主控台 → 系統和安全性 → 系統 → 遠端設定**找到此選項）。若您有「弱點和修補程式管理」的授權，您可建立與受管理裝置的連線時強制啟用此選項。若您沒有授權，請在目標受管理裝置上啟用此選項。如果停用此選項，則無法使用遠端連線。

若要建立遠端裝置連線，您需有兩個公用程式：

- Kaspersky 公用程式，名稱為 klsctunnel。此公用程式必須儲存在管理員工作站。您可使用此公用程式進行用戶端裝置與管理伺服器之間的通道連線。

  卡巴斯基安全管理中心允許透過管理伺服器的從管理主控台的 TCP 連線通道，然後透過網路代理到受管理裝置上的指定連接埠。通道設計用於連線安裝管理主控台的裝置上的用戶端應用程式到受管理裝置上的 TCP 連接埠—如果管理主控台和目的裝置之間沒有直接連線可用。

  如果用於連線到管理伺服器的連接埠在裝置上不可用，則需要遠端用戶端裝置和管理伺服器之間的連線隧道。在以下情況下裝置連接埠可能無法使用：

  - 遠端裝置使用 NAT 機制連線到本機網路。
  - 遠端裝置是本機網路管理伺服器的一部分，但是它的連接埠已被防火牆關閉。

- 名為「遠端桌面連線」的標準 Microsoft Windows 元件。根據標準 Windows 公用程式 mstsc.exe 的設定建立遠端桌面的連線。

  在使用者不知道的情況下遠端連線到使用者目前的桌面。一旦管理員連線上，裝置使用者將在沒有提前通知的情況下中斷連線。

若要連線至用戶端裝置的桌面：

1. 在 MMC 型管理主控台的管理伺服器的上下文功能表中，選取**內容**。
2. 在開啟的"管理伺服器內容"視窗中，前往**管理伺服器連線設定 → 連線連接埠**。
3. 確認已啟用**為卡巴斯基安全管理中心網頁主控台開啟遠端桌面協定連接埠**選項。
4. 在卡巴斯基安全管理中心網頁主控台中，轉到**裝置 → 受管理裝置**。
5. 在受管理裝置清單上方的**目前路徑**欄位中，點擊路徑連接。
6. 在開啟的左側窗格中，選擇包含您要存取的裝置的管理群組。
7. 選取您要取得存取權限之裝置名稱旁邊的核取方塊。
8. 點擊**連線到遠端桌面**按鈕。

   遠端桌面（僅限 Windows）視窗隨即開啟。

9. 啟用**允許受管理裝置的遠端桌面連線**選項。在此情況下將會建立連線，即使受管理裝置作業系統設定中目前禁止遠端連線。

   只有在您有「弱點和修補程式管理」的授權時才可使用此選項。

10. 點擊**下載**按鈕以下載 klsctunnel 實用程式。

11. 點擊**複製到剪貼簿**按鈕以複製文字欄位的文字。此文字為二進位大型物件 (BLOB)，其中包含建立管理伺服器與受管理裝置間連線的設定。

    BLOB 有效時間為 3 分鐘。若 BLOB 已到期，請重新開啟遠端桌面（僅限 Windows）視窗以產生新的 BLOB。

12. 執行 klsctunnel 公用程式。

    公用程式視窗隨即開啟。

13. 貼上複製的文字至文字欄位。

14. 若您使用代理伺服器，請選取**使用代理伺服器**核取方塊，接著指定代理伺服器連線設定。

15. 點擊**開啟連接埠**按鈕。

    「遠端桌面連線」登入視窗隨即開啟。

16. 指定您目前用來登入卡巴斯基安全管理中心 網頁主控台的帳戶憑證。

17. 點擊**連線**按鈕。

    與裝置建立連線後，您將能在 Microsoft Windows 的遠端連線視窗中使用桌面。

透過 Windows 桌面共用連線到用戶端裝置

管理員可以在安裝網路代理的用戶端裝置上使用遠端桌面連線。如果裝置的 TCP 和 UDP 連接埠關閉，也可透過網路代理遠端連線至用戶端裝置。

管理員可以連線至用戶端裝置上的現有連線而不會斷開此連線中的使用者。在此情況下，裝置上的管理員和使用者連線將桌面共用存取。

若要建立遠端裝置連線，您需有兩個公用程式：

- Kaspersky 公用程式，名稱為 klsctunnel。此公用程式必須儲存在管理員工作站。您可使用此公用程式進行用戶端裝置與管理伺服器之間的通道連線。

  卡巴斯基安全管理中心允許透過管理伺服器的從管理主控台的 TCP 連線通道，然後透過網路代理到受管理裝置上的指定連接埠。通道設計用於連線安裝管理主控台的裝置上的用戶端應用程式到受管理裝置上的 TCP 連接埠—如果管理主控台和目的裝置之間沒有直接連線可用。

  如果用於連線到管理伺服器的連接埠在裝置上不可用，則需要遠端用戶端裝置和管理伺服器之間的連線隧道。在以下情況下裝置連接埠可能無法使用：

  - 遠端裝置使用 NAT 機制連線到本機網路。
  - 遠端裝置是本機網路管理伺服器的一部分，但是它的連接埠已被防火牆關閉。

- Windows 桌面共用。當連線到遠端桌面的現有連線時，裝置上的連線使用者會收到來自管理員的連線請求。卡巴斯基安全管理中心建立的報告中不會儲存有關裝置上的遠端操作及其結果的任何資訊。

  管理員可以在遠端用戶端裝置上設定使用者活動稽核。稽核期間，應用程式會儲存用戶端裝置上管理員開啟和/或修改過的檔案資訊。

使用 Windows 桌面共用連線到用戶端裝置必須符合以下需求：

- 管理員工作站電腦系統環境必須是 Microsoft Windows Vista 或以上版本。管理伺服器裝置作業系統的類型對透過 Windows 桌面共用進行連線沒有限制。

  若要檢查 Windows 桌面共用功能是否隨附於您的 Windows 版本中，請確保 Windows 登錄檔中包含 CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} 機碼。

- 用戶端裝置安裝了 Microsoft Windows Vista 或更新版本。
- 卡巴斯基安全管理中心已安裝弱點和修補程式管理產品授權。

若要透過 Windows 桌面共用連線到用戶端裝置的桌面：

1. 在 MMC 型管理主控台的管理伺服器的上下文功能表中，選取**內容**。
2. 在開啟的"管理伺服器內容"視窗中，前往**管理伺服器連線設定 → 連線連接埠**。
3. 確認已啟用**為卡巴斯基安全管理中心網頁主控台開啟遠端桌面協定連接埠**選項。
4. 在卡巴斯基安全管理中心網頁主控台中，轉到**裝置 → 受管理裝置**。
5. 在受管理裝置清單上方的**目前路徑**欄位中，點擊路徑連接。
6. 在開啟的左側窗格中，選擇包含您要存取的裝置的管理群組。
7. 選取您要取得存取權限之裝置名稱旁邊的核取方塊。
8. 點擊**Windows 共用桌面**按鈕。

   Windows 共用桌面精靈隨即開啟。
9. 點擊**下載**按鈕下載 klsctunnel 實用程式，接著等待下載程序完成。

   若您已有 klsctunnel 公用程式，請略過此步驟。
10. 點擊**下一步**按鈕。

11. 選取裝置上您要連線的工作階段，接著點擊**下一步**按鈕。

12. 在目標裝置上開啟的對話方塊中，使用者必須允許共用工作階段。否該工作階段將無法完成。

    裝置使用者確認桌面共用的工作階段後，精靈的下一頁面隨即開啟。

13. 點擊**複製到剪貼簿**按鈕以複製文字欄位的文字。此文字為二進位大型物件 (BLOB)，其中包含建立管理伺服器與受管理裝置間連線的設定。

    BLOB 有效時間為 3 分鐘。若已過期，請產生全新 BLOB。

14. 執行 klsctunnel 公用程式。

    公用程式視窗隨即開啟。

15. 貼上複製的文字至文字欄位。

16. 若您使用代理伺服器，請選取**使用代理伺服器**核取方塊，接著指定代理伺服器連線設定。

17. 點擊**開啟連接埠**按鈕。

桌面共用會在新視窗啟動。若您要與裝置互動，請點擊視窗左上角的功能表圖示 ( )，接著選取**互動模式**。

裝置分類

*裝置分類*是根據特定條件篩選裝置的工具。您可以使用裝置分類管理幾個裝置：例如，檢視僅檢視這些裝置的報告或移動所有這些裝置到其他群組。

卡巴斯基安全管理中心提供大範圍的*預先定義分類*（例如，**處於"緊急"狀態的裝置**、**防護已停用**, **偵測到活動威脅**）。預先定義分類無法被刪除。您也可以建立和配置附加*使用者定義分類*。

在使用者定義分類中，您可以設定搜尋範圍並選取所有裝置、受管理裝置、或者未配置的裝置。搜尋參數在條件中指定。在裝置分類中，您可以建立帶有不同搜尋參數的多個條件。例如，您可以建立兩個條件並指定不同的 IP 範圍。如果多個條件被指定，分類顯示滿足任意條件的裝置。相比之下，條件中的搜尋參數是附加的。如果 IP 範圍和已安裝應用程式名稱都被指定在一個條件，僅安裝了應用程式且 IP 位址處於指定範圍的裝置被顯示。

從裝置分類中檢視裝置清單

卡巴斯基安全管理中心允許您從裝置分類中檢視裝置清單。

從裝置分類中檢視裝置清單：

1. 在主功能表中，轉到**裝置 → 裝置分類** or **發現和佈署 → 裝置分類**區域。
2. 在選項清單中，按一下裝置分類的名稱。
   該頁面會顯示一個表格，其中包含有關裝置分類中包含的裝置的資訊。
3. 您可以按如下方式對裝置表格資料進行分組和篩選：
   - 點擊設定圖示 (⚙)，然後選擇要在表中顯示的列。
   - 點擊篩選圖示 (▽), 然後在喚起的功能表中指定並套用篩選條件。
     顯示篩選後的裝置表格。

您可以在裝置分類中選擇一個或多個裝置，然後點擊**新工作**按鈕以建立將套用於這些裝置的工作。

要將裝置分類中的選定裝置移動到另一個管理群組，請點擊**移至群組**按鈕，然後選擇目標管理群組。

建立裝置分類

要建立裝置分類，請執行以下操作：

1. 在主功能表中，轉至 **裝置 → 裝置分類**。
   裝置選項清單頁面隨即顯示。
2. 點擊**新增**按鈕。
   裝置分類設定視窗開啟。
3. 輸入新選項的名稱。
4. 指定包含要包括在裝置分類中的裝置的群組：
   - **尋找任何裝置**— 搜尋符合選擇標準並被包含在**受管理裝置**或未**未配置的裝置**群組中的裝置。
   - **尋找受管理裝置** — 搜尋符合選擇標準並被包含在**受管理裝置**群組中的裝置。
   - **尋找未配置的裝置**— 搜尋符合選擇標準並被包含在**未配置的裝置**群組中的裝置。

   您可以啟用**包含次要管理伺服器的資料**核取方塊以啟用搜尋滿足選擇條件並由從屬管理伺服器管理的裝置。
5. 點擊**新增**按鈕。
6. 在開啟的視窗中，指定將裝置包括在此選項中時必須符合的條件，然後點擊**確定**按鈕。
7. 點擊**儲存**按鈕。

裝置選項已建立並新增到裝置選項清單中。

配置裝置分類

要配置裝置分類：

1. 在主功能表中，轉至 **裝置 → 裝置分類**。
   裝置選項清單頁面隨即顯示。
2. 選擇相關的使用者自定義裝置分類，然後點擊**內容**按鈕。
   裝置分類設定視窗開啟。
3. 在**一般**標籤上，點擊**新條件**連接。
4. 指定包含裝置到該分類所必須滿足的條件。
5. 點擊**儲存**按鈕。

   裝置被套用並儲存。

以下是分配裝置到分類的條件敘述。多個條件使用 OR 邏輯運算子組合在一起：分類範圍將包含至少符合列出的一個條件的裝置。

一般

在**一般**區域，您可以變更分類條件的名稱，指定是否必須倒轉條件：

反轉分類條件

預設情況下已停用該選項。

如果啟用此選項，指定的分類條件將倒轉。此分類將包含所有不符合該條件的裝置。

以下範例展示了反轉工作的邏輯：

- **條件**：您的裝置上安裝了 Linux 類型且內部版本號為 00.0.000 的作業系統。
- **反轉條件**：您的裝置上安裝了非 Linux 類型且內部版本號為 00.0.000 的作業系統，這等價於：
  安裝了非 Linux 類型或內部版本號非 00.0.000 的作業系統。

因此，分類將包括安裝了 Windows 類型且內部版本號為 00.0.000 的裝置，或安裝了 Linux 類型但內部版本號不為 00.0.000 的裝置。

網路基礎架構

在**網路**子區域，您可以指定依據網路資料裝置納入分類的標準：

- **裝置名稱**

  裝置的 Windows 網路名稱（NetBIOS 名稱），或者 IPv4 或 IPv6 位址。

- **Windows 網域**

  顯示指定的 Windows 網域中包括的所有裝置。

- **管理群組**

  顯示指定的管理群組中包括的裝置。

- **敘述**

  裝置內容視窗中的文字：在**一般**區域的**敘述**欄位。
  您可以使用以下特徵說明**敘述**欄位中的文字：

  - 在單詞中：
    - *****。用任意數量的字元更換任何字串。

      例如：
      要敘述單詞 **Server** 或 **Server's**，您可以輸入 **Server***。
    - **?**。更換任意單個字元。

      例如：
      要敘述單詞 **Window** 或 **Windows**，您可以輸入 **Windo?**。
      星號 (*****) 或問號 (**?**) 不能用於查詢中的第一個字元。
  - 要尋找多個單詞：
    - 空格。顯示所有在其敘述中包含列出的任何單詞的裝置。

      例如：
      要尋找在其敘述中包含**從屬**或**虛擬**單詞的短語，您可以在查詢中包含**從屬虛擬**等字。
    - **+**。當單詞帶有加號前綴時，所有搜尋結果都將包含該單詞。

      例如：
      要搜尋同時包含**從屬**和**虛擬**的短語，請輸入**+從屬+虛擬**查詢。
    - **-**。當單詞帶有減號前綴時，所有搜尋結果都不包含該單詞。

      例如：
      要尋找包含**從屬**但不包含**虛擬**的短語，請輸入**+從屬-虛擬**查詢。
    - **「<某些文字>」**。引號中圍繞的文字必須存在文字中。

      例如：
      要尋找包含**從屬伺服器**單詞群組合的短語，您可以在查詢中輸入**「從屬伺服器」**。

- **IP 範圍**

  如果啟用此選項，您可以輸入應該包括相關裝置的 IP 範圍的初始和最終 IP 位址。

  預設情況下已停用該選項。

- **由不同管理伺服器管理**

  您可以選取以下值之一：

  - **是**。裝置移動規則僅套用於由其他管理伺服器管理的用戶端裝置。這些伺服器與您配置裝置移動規則的伺服器不同。
  - **否**。裝置移動規則僅套用於由目前管理伺服器管理的用戶端裝置。
  - **未選取值**。該條件不適用。

在**Active Directory**子區域，您可以根據 Active Directory 資料設定將裝置納入分類的標準：

- **裝置在 Active Directory 組織單元中**

  如果啟用此選項，選取範圍將包括輸入欄位中指定的 Active Directory 單元中的裝置。

  預設情況下已停用該選項。

- **包括子組織單元**

  如果啟用此選項，選取範圍將包括指定 Active Directory 組織單元的所有子組織單元中的裝置。

  預設情況下已停用該選項。

- **該裝置是 Active Directory 群組成員**

  如果啟用此選項，選取範圍將包括輸入欄位中指定的 Active Directory 群組中的裝置。

  預設情況下已停用該選項。

在**網路活動**子區域，您可以根據網路活動指定將裝置納入分類的標準：

- **作為發佈點**

  在下拉清單中，可設定執行搜尋時在分類中包括裝置的標準：

  - **是**。選取範圍將包括充當發佈點的裝置。
  - **否**。分類不包含作為發佈點的裝置。
  - **未選取值**。將不套用標準。

- **不斷開與管理伺服器的連線**

  在下拉清單中，可設定執行搜尋時在分類中包括裝置的標準：

  - **已啟用**。分類將包含已選取**不斷開與管理伺服器的連線**核取方塊的裝置。
  - **已停用**。分類將包含未選取**不斷開與管理伺服器的連線**核取方塊的裝置。
  - **未選取值**。將不套用標準。

- **連線設定檔已轉換**

  在下拉清單中，可設定執行搜尋時在分類中包括裝置的標準：

  - **是**。該分類將包含連線設定檔轉換後連線到管理伺服器的裝置。
  - **否**。該分類將不包含連線設定檔轉換後連線到管理伺服器的裝置。
  - **未選取值**。將不套用標準。

- **上一次連線到管理伺服器**

  您可使用此方塊設定按上一次連線到管理伺服器的時間搜尋裝置的標準。

  如果選取該方塊，則在輸入欄位中，您可以指定在用戶端裝置上安裝的網路代理和管理伺服器之間建立上一次連線的時間間隔（日期和時間）。選取將包括位於指定間隔的裝置。

  如果清除此方塊，則將不會套用標準。

  預設情況下已清空此方塊。

- **網路輪詢時偵測到新裝置**

  搜尋最近幾天透過網路輪詢偵測到的新裝置。

  如果選取此核取方塊，分類將只包括在**偵測週期（天）**欄位中指定的天數內透過裝置發現偵測到的新裝置。

  如果停用此選項，分類將包括透過裝置發現偵測到的所有裝置。

  預設情況下已停用該選項。

- **裝置可見**

  在下拉清單中，可設定執行搜尋時在分類中包括裝置的標準：

  - **是**。程式在分類中包括網路中目前可見的裝置。
  - **否**。應用程式在分類中包括網路中目前不顯示的裝置。
  - **未選取值**。將不套用標準。

在**雲端區段**子區域中，您可以根據相關雲端區段設定將裝置納入分類的標準：

- **裝置在雲端區段中**

  如果啟用此選項，您可以從 AWS、Azure 和 Google 雲端區段中選擇裝置。

  如果也啟用了**包含子物件**選項，則搜尋會在選取區段的所有子物件上執行。

  搜尋結果僅包含所選段的裝置。

- **使用 API 發現的裝置**

  在下拉清單，您可以選取裝置是否由 API 工具偵測：

  - **是**。裝置使用 AWS、Azure 或 Google API 進行偵測。
  - **否**。裝置無法使用 AWS、Azure 或 Google API 進行偵測。即裝置要么在雲端環境之外，要么在雲端環境中，但無法通過 API 偵測到。
  - 沒有值。這項條件不適用。

裝置狀態

在**受管理裝置狀態**子區域，您可以根據受管理應用程式的裝置狀態的敘述設定將裝置納入分類的標準：

- **裝置狀態**

  在該下拉清單中，您可以選取下列裝置狀態之一：*確定*、*緊急*或*警告*。

- **即時防護狀態**

  您可以在該下拉清單中選取即時防護狀態。具有指定即時防護狀態的裝置將被包括在選取範圍中。

- **裝置狀態敘述**

  在此欄位中，您可以選取條件旁邊的核取方塊，若滿足這些條件，程式會為裝置分配下列狀態之一：*確定*、*緊急*或*警告*。

在**受管理應用程式元件的狀態**子區域中，您可以根據受管理應用程式元件狀態設定將裝置納入分類的標準：

- **資料洩漏防護狀態**

  根據資料外洩防護的狀態搜尋裝置（*裝置上無資料*, *已停止*, *正在啟動*, *已暫停*, *執行中*, *失敗*）。

- **協作伺服器防護狀態**

  根據伺服器協作防護狀態搜尋裝置（*裝置上無資料*, *已停止*、*正在啟動*、*已暫停*, *執行中*、*失敗*）。

- **郵件伺服器的病毒防護狀態**

  根據郵件伺服器防護狀態搜尋裝置（*裝置上無資料*、*已停止*、*正在啟動*、*已暫停*、*執行中*、*失敗*）。

- **端點感應器狀態**

  根據端點感應器元件狀態搜尋裝置（*裝置上無資料*、*已停止*、*正在啟動*、*已暫停*、*執行中失敗*）。

在**影響受管理應用程式狀態的問題**子區域，您可以根據由受管理應用程式偵測到的可能問題清單指定將裝置納入分類的標準。如果至少一個您選取的問題存在於裝置，裝置將被包含到分類。當您選取幾個應用程式的問題時，您可以選取在所有清單中自動選取該問題。

您可以選取受管理應用程式狀態敘述的核取方塊；接收這些狀態時，裝置將被包含在分類。當您選取幾個應用程式的狀態時，您可以選取在所有清單中自動選取該狀態。

系統詳情

在**作業系統**區域，您可以根據作業系統指定將裝置納入分類的標準。

- **平台類型**

  如果選中該方塊，您可以從清單中選取一個作業系統。安裝了指定作業系統的裝置會包含在搜尋結果中。

- **作業系統服務套件版本**

  在該欄位中，可以指定作業系統的更新套件版本（採用 *X.Y* 格式），這將決定將移動規則套用到裝置的方式。預設情況下，不指定版本值。

- **作業系統 bit 大小**

  在該下拉清單中可選取作業系統的架構，這將決定將移動規則套用到裝置（**未知**、**x86**、**AMD64** 或 **IA64**）的方式。預設情況下，不選取清單中的任何選項，這樣就不會對作業系統的架構進行定義。

- **作業系統版本**

  該設定僅套用到 Windows 作業系統。

  作業系統版本號。您可以指定所選作業系統是否必須具有相等、更早或更晚的版本號。您也可以設定對所有版本號的搜尋，除了指定的值。

- **作業系統發佈號**

  該設定僅套用到 Windows 作業系統。

  作業系統發佈 ID。您可以指定所選作業系統是否必須具有相等、更早或更晚的發佈 ID。您也可以設定對所有發佈 ID 的搜尋，除了指定的值。

在**虛擬機**區域中，您可以根據它們是否是虛擬機或虛擬桌面基礎架構 (VDI) 的一部分來指定將裝置納入分類的標準：

- **這是一台虛擬機**

  在此下拉清單中，您可以選取以下選項：
  - **未定義**。
  - **否**。尋找不是虛擬機的裝置。
  - **是**。搜尋虛擬機裝置。

- **虛擬機類型**

  在該下拉清單中，您可以選取虛擬機製造商。
  若在**這是一台虛擬機**下清單中選取**是**或**不重要**值，則可使用此下拉清單。

- **虛擬桌面基礎架構的一部分**

  在此下拉清單中，您可以選取以下選項：
  - **未定義**。
  - **否**。尋找不是虛擬桌面基礎架構一部分的裝置。
  - **是**。搜尋屬於虛擬桌面基礎架構 (VDI) 一部分的裝置。

在**硬體登錄資料**子區域，您可以根據所安裝的硬體設定將裝置納入分類的標準：

確保在要從中獲取硬體詳細資訊的 Linux 裝置上安裝了 lshw 公用程式。根據所使用的 hypervisor，從虛擬機獲取的硬體詳細資訊可能不完整。

- **裝置**

  在該下拉清單中，您可以選取單元類型。所有帶有該單元的裝置被包含在搜尋結果。
  該欄位支援完整文字搜尋。

- **供應商**

  在該下拉清單中，您可以選取單元生產商的名稱。所有帶有該單元的裝置被包含在搜尋結果。
  該欄位支援完整文字搜尋。

- **裝置名稱**

  在 Windows 網路中的裝置名稱。具有指定名稱的裝置將包括在該分類中。

- **敘述**

  裝置或硬體單元的敘述。帶有該欄位中指定的敘述的裝置將包括在分類範圍內。

  可在裝置的內容視窗輸入任何格式的裝置敘述。該欄位支援完整文字搜尋。

- **裝置製造商**

  裝置製造商的名稱。被指定生產商製造的裝置將包括在分類範圍內。

  您可以在裝置的內容視窗中輸入製造商的名稱。

- **序號**

  帶該欄位中指定序號的所有硬體裝置將包括在該分類中。

- **清單號**

  帶有該欄位中指定的清單編號的裝置將包括在選取範圍內。

- **使用者**

  該欄位中指定使用者的所有硬體裝置都將包括在該分類中。

- **位置**

  裝置或硬體單元的位置（例如，在總部或分公司）。在該欄位中指定的位置佈署的電腦或其他裝置將包括在該分類中。

  您可以在該裝置的內容視窗中以任何格式敘述裝置的位置。

- **CPU 時鐘頻率 (MHz)，從**

  CPU 的最小時鐘速率。CPU 與輸入欄位中指定的時鐘速率範圍（含）比對的裝置將被包含在分類中。

- **CPU 時鐘頻率 (MHz)，到**

  CPU 的最大時鐘速率。CPU 與輸入欄位中指定的時鐘速率範圍（含）比對的裝置將被包含在分類中。

- **虛擬 CPU 內核數量，從**

  虛擬 CPU 核心的最小數量。CPU 與輸入欄位中指定的虛擬核心數範圍（含）比對的裝置將被包含在分類中。

- **虛擬 CPU 內核數量，到**

  虛擬 CPU 核心的最大數量。CPU 與輸入欄位中指定的虛擬核心數範圍（含）比對的裝置將被包含在分類中。

- **硬碟磁區，以 GB 為單位，從**

  裝置上硬碟磁碟機的最小容量。硬碟磁碟機與這些輸入欄位中指定的容量範圍（含）比對的裝置將包括在分類範圍內。

- **硬碟磁區，以 GB 為單位，到**

  裝置上硬碟磁碟機的最大容量。硬碟磁碟機與這些輸入欄位中指定的容量範圍（含）比對的裝置將包括在分類範圍內。

- **RAM 大小 (MB)，從**

  裝置 RAM 的最小大小。RAM 與輸入欄位中指定的大小範圍（含）比對的裝置將被包含在分類中。

- **記憶體大小 (MB)**

  裝置 RAM 的最大大小。RAM 與輸入欄位中指定的大小範圍（含）比對的裝置將被包含在分類中。

協力廠商軟體詳情

在**應用程式登錄資料**子區域，您可以根據已安裝的應用程式設定搜尋裝置的標準：

- **應用程式名稱**

  在該下拉清單中，您可以選取應用程式。安裝有指定應用程式的裝置將包括在選取範圍中。

- **應用程式版本**

  在該輸入欄位中，您可以指定選定應用程式的版本。

- **供應商**

  在該下拉清單中，您可以選取已安裝應用程式的生產商。

- **應用程式狀態**

  在該下拉清單中，您可以選取應用程式的狀態（*已安裝*、*未安裝*）。已安裝或未安裝指定應用程式的裝置，取決於所選狀態，將被包含在分類。

- **根據更新尋找**

  如果啟用此選項，則搜尋操作將使用相關裝置內應用程式更新的有關資訊來執行。選取核取方塊後，**應用程式名稱**、**應用程式版本**與**應用程式狀態**欄位會各自變成**更新名稱**、**更新版本**和**狀態**。

  預設情況下已停用該選項。

- **不相容安全應用程式名稱**

  在該下拉清單中，您可以選取協力廠商安全應用程式。在搜尋過程中，安裝有指定程式的裝置將包括在選取範圍中。

- **應用程式標籤**

  在該下拉清單中，您可以選取應用程式標籤。所有安裝了敘述中帶有所選標籤的應用程式的裝置都被包含在裝置分類。

- **套用到沒有指定標籤的裝置**

  如果啟用此選項，分類將包含未帶有所選標籤的敘述的裝置。

  如果停用該選項，則不套用標準。

  預設情況下已停用該選項。

在**弱點與更新**子區域中，您可以根據 Windows 更新來源指定將裝置納入分類的標準：

WUA 已轉換到管理伺服器

您可以在下拉清單中選取以下搜尋選項之一：

- **是**。如果選中該選項，搜尋結果會包含從管理伺服器收到 Windows Update 更新的裝置。
- **否**。如果選中該選項，結果會包含從其他來源收到 Windows Update 更新的裝置。

Kaspersky 應用程式詳情

在 **Kaspersky 應用程式**子區域中，您可以根據所選的受管理應用程式設定將裝置納入分類的標準：

- **應用程式名稱**

  在下拉清單中，可設定按 Kaspersky 應用程式名稱執行搜尋時在分類中包括裝置的標準。

  清單僅提供管理員工作站上已安裝管理外掛程式的應用程式的名稱。

  如果未選取任何應用程式，則將不會套用該標準。

- **應用程式版本**

  在輸入欄位，可設定按 Kaspersky 應用程式版本號執行搜尋時在分類中包括裝置的標準。

  如果未指定版本號，則將不會套用該標準。

- **重大更新名稱**

  在輸入欄位中，可設定按應用程式名稱或更新套件編號執行搜尋時在分類中包括裝置的標準。

  如果欄位留空，則將不會套用該標準。

- **應用程式狀態**

  在該下拉清單中，您可以選取應用程式的狀態（*已安裝*、*未安裝*）。已安裝或未安裝指定應用程式的裝置，取決於所選狀態，將被包含在分類。

- **上一次模組更新**

  您可以使用此選項來設定按這些裝置上安裝的程式模組上次更新的時間搜尋裝置的標準。

  如果選中此方塊，則您可以在輸入欄位中指定執行這些裝置上安裝的程式模組的上一次更新的時間間隔（日期和時間）。

  如果清除此方塊，則將不會套用標準。

  預設情況下已清空此方塊。

- **裝置透過卡巴斯基安全管理中心 14.2 管理**

  在該下拉清單，您可以包含透過卡巴斯基安全管理中心管理的裝置到分類：

  - **是**。應用程式包含透過卡巴斯基安全管理中心管理的裝置。
  - **否**。若裝置不透過卡巴斯基安全管理中心管理，則應用程式會將其包含在分類中。
  - **未選取值**。將不套用標準。

- **安全應用程式已安裝**

  在該下拉清單，您可以包含已安裝安全應用程式的裝置到分類：

  - **是**。應用程式包含安裝了安全應用程式的裝置到分類。
  - **否**。應用程式會在分類中包含未安裝安全應用程式的裝置。
  - **未選取值**。將不套用標準。

在**病毒防護**子區域，您可以根據防護狀態設定將裝置納入分類的標準：

- **資料庫發佈日期**

  如果啟用此選項，您可以按病毒資料庫發佈日期搜尋用戶端裝置。在該輸入欄位中，您可以設定執行搜尋的時間間隔。

  預設情況下已停用該選項。

- **資料庫記錄數**

  如果啟用此選項，您可以依據資料庫記錄數量來搜尋用戶端裝置。在輸入欄位中，您可以設定病毒資料庫記錄數的上限值和下限值。

  預設情況下已停用該選項。

- **上一次掃描**

  如果啟用此選項，您可以按上次惡意軟體掃描時間來搜尋用戶端裝置。在該輸入欄位中，您可以指定執行上一次惡意軟體掃描的時段。

  預設情況下已停用該選項。

- **偵測到的威脅**

  如果啟用此選項，您可以依據發現的病毒數量來搜尋用戶端裝置。在輸入欄位中，您可以設定發現病毒總數的上限值和下限值。

  預設情況下已停用該選項。

在**加密**子區域中，您可以根據所選的加密演算法設定將裝置納入分類的標準：

加密演算法

進階加密標準 (AES) 對稱區塊編碼器演算法。在下拉清單中，您可以選取加密金鑰大小（56-bit、128-bit、192-bit 或 256-bit）。

可用值：*AES56*、*AES128*、*AES192* 和 *AES256*。

應用程式元件子區域包含在卡巴斯基安全管理中心網頁主控台中安裝了相應管理外掛程式的那些應用程式的元件清單。

在**應用程式元件**子區域中，您可以根據所選應用程式元件的狀態和版本編號指定將裝置納入分類的標準：

- **狀態**

  根據應用程式傳送到管理伺服器的元件狀態搜尋裝置。您可以選擇以下狀態之一：*N/A*、*Stopped*、*Paused*、*Starting*、*Running*、*Failed*、*Not installed*、*Not supported by license*。如果安裝在受管理裝置上的應用程式的所選元件具有指定狀態，裝置被包含到裝置分類。

  由應用程式傳送的狀態：

  - *已停止* - 元件被停用且不在工作。
  - *已暫停* - 元件被暫停，例如，在使用者在受管理應用程式上停止了防護後。
  - *正在啟動* - 元件處於初始化處理程序中。
  - *執行中* - 元件被啟用且在正常工作。
  - *失敗* – 元件操作中發生錯誤。
  - *未安裝* - 當設定應用程式自訂安裝時，使用者未選取該元件以安裝。
  - *不受產品授權支援* – 產品授權不涵蓋所選元件。

  不同於其他狀態，裝置上*N/A* 狀態不由應用程式傳送。該選項顯示應用程式沒有所選元件狀態的資訊。例如，這可能發生在所選元件不屬於任何在裝置上安裝的應用程式時，或裝置關閉時。

- **版本**

  根據您在清單中選取的版本號搜尋裝置。您可以輸入版本號，例如 `3.4.1.0`，然後指定所選元件是否必須具有相同、更早或更新版本。您也可以設定對所有版本的搜尋，除了指定的值。

標籤

在**標籤**區域中，您可以根據先前新增到受管理裝置的敘述的關鍵字（標籤）設定將裝置納入分類的標準：

如果有至少一個指定的標籤符合則套用

如果啟用此選項，搜尋結果將顯示包含帶有所選標籤的敘述的裝置。
如果停用此選項，搜尋結果將僅顯示包含帶有所有標籤的敘述的裝置。
預設情況下已停用該選項。

要將標籤新增到條件，請點擊**新增**按鈕，然後點擊**標籤**輸入欄位來選擇標籤。指定是否在裝置分類中包括或排除具有所選標籤的裝置。

- **必須被包含**

  如果選取了該選項，搜尋結果將顯示帶有包含了所選標籤的敘述的裝置。要尋找裝置，您可以使用星號，它表示任何字元長度的字串。

  預設情況下已選定此選項。

- **必須被排除**

  如果選取了該選項，搜尋結果將顯示不帶有包含了所選標籤的敘述的裝置。要尋找裝置，您可以使用星號，它表示任何字元長度的字串。

使用者

在**使用者**區域中，您可以根據登入到作業系統的使用者帳戶設定將裝置納入分類的標準。

- **最後一次登入系統的使用者**

  如果啟用此選項，您可以選擇用於配置標準的使用者帳戶。搜尋結果包含所選使用者上一次登入係統的裝置。

- **登入系統至少一次的使用者**

  如果啟用此選項，按一下**瀏覽**按鈕可以指定使用者帳戶。搜尋結果包含指定使用者至少登入一次的裝置。

從裝置分類中匯出裝置清單

卡巴斯基安全管理中心允許您將裝置分類中的裝置資訊儲存在 CSV 或 TXT 檔案中。

要將裝置清單從裝置分類匯出到檔案：

1. 從裝置分類中開啟包含裝置的表格。
2. 您可以通過以下方式之一從表中匯出有關裝置的資訊：

   - 匯出選定裝置。

     選中所需裝置旁邊的核取方塊，然後點擊**將行匯出到 csv 檔案**或**將行匯出到 txt 檔案**按鈕，具體取決於您喜歡的匯出格式。表中包含的有關所選裝置的所有資訊都將被匯出到 TXT 或 CSV 檔案。

   - 匯出目前頁面上顯示的所有裝置。

     點擊**將行匯出到 csv 檔案** 或 **將行匯出到 txt 檔案**按鈕，視您偏好的匯出格式而定。您不需要從表中選擇裝置。目前頁面上顯示的所有裝置資訊都將被匯出到 TXT 檔案。

請注意，如果您將篩選條件套用於裝置表，則只有來自顯示列的篩選資料將被匯出到 CSV 或 TXT 檔案。

在分類中從管理群組中刪除裝置

在使用裝置分類時，你可以直接從管理群組中刪除裝置，而不是轉換到包含這些裝置的管理群組。

要從管理群組刪除裝置，請執行以下操作：

1. 在主功能表中，轉到**裝置 → 裝置分類** or **發現和佈署 → 裝置分類**。
2. 在選項清單中，按一下裝置分類的名稱。
   該頁面會顯示一個表格，其中包含有關裝置分類中包含的裝置的資訊。
3. 選取您要移除的裝置，之後點擊**刪除**。
   所選裝置即從對應管理群組中刪除。

裝置標籤

該部分描述了裝置標籤，提供了建立和修改它們以及手動或自動標記裝置的說明。

裝置標籤

卡巴斯基安全管理中心允許您*標記*裝置。標記是裝置的標籤，可以用於分組、描述或尋找裝置。分配到裝置的標籤可以用於建立分類、尋找裝置以及分發裝置到管理群組。

您可以手動或自動標記裝置。如果您想標記單一裝置，可以使用手動標記。卡巴斯基安全管理中心透過以下方式之一執行自動標記：

- 按照指定的標記規則。
- 透過應用程式。

不建議使用不同的標記方式來指派相同的標籤。例如，若某種標籤是按規則指派，則不建議手動將此標籤指派給裝置。

如果某種標籤是按規則指派，則在滿足指定規則時就會自動為裝置做標記。單個規則對應於每個標記。規則應用到裝置網路內容、作業系統、裝置上安裝的應用程式以及其他裝置內容。例如，如果您擁有物理機、Amazon EC2 實例和 Microsoft Azure 虛擬機 hybrid 基礎架構，您可以設定分配 [Azure] 標籤到所有 Microsoft Azure 虛擬機的規則。然後，您可以在建立裝置分類時使用該標籤；這將協助您整理所有 Microsoft Azure 虛擬機並分配工作給它們。

每個標籤只能新增一條自動標記規則。如果為相同標籤建立新規則，則會取代先前的規則。

在以下情況下標籤從裝置上被自動刪除：

- 當裝置停止滿足分配標籤的規則的條件時。
- 當分配標籤的規則被停用或刪除時。

每個管理伺服器的標籤清單和規則清單是獨立的，包括主管理伺服器和從屬虛擬管理伺服器。規則僅被套用到來自建立規則的相同管理伺服器的裝置。

建立裝置標籤

要建立裝置標籤：

1. 在主功能表中，轉至 **裝置** → **標籤** → **裝置標籤**。
2. 點擊**新增**。
   新標籤視窗開啟。
3. 在**標籤**欄位中，輸入頁籤名稱。
4. 點擊**儲存**以儲存變更。

新標籤出現在裝置標籤清單。

重命名裝置標籤

要重命名裝置標籤：

1. 在主功能表中，轉至 **裝置** → **標籤** → **裝置標籤**。
2. 點擊您要重命名的標籤名稱。
   標籤內容視窗開啟。
3. 在**標籤**欄位，輸入頁籤名稱。
4. 點擊**儲存**以儲存變更。

更新的標籤出現在裝置標籤清單。

刪除裝置標籤

要刪除裝置標籤：

1. 在主功能表中，轉至 **裝置** → **標籤** → **裝置標籤**。
2. 在清單中，選取您想要刪除的裝置標籤。
3. 點擊**刪除**按鈕。
4. 在開啟的視窗中，點擊**是**按鈕。

裝置標籤被刪除。刪除的標籤被從其分配的所有裝置上自動刪除。

您刪除的標籤不會自動從自動標記規則中刪除。標籤被刪除後，它僅在裝置第一次滿足標籤分配條件時被分配到新裝置。

如果此標記由應用程式或網路代理分配給裝置，則已刪除的標記不會被自動從裝置中刪除。要從您的裝置中刪除標籤，請使用 klscflag 公用程式。

檢視分配了標籤的裝置

要檢視分配了標籤的裝置：

1. 在主功能表中，轉至 **裝置 → 標籤 → 裝置標籤**。
2. 點擊您要檢視已指派裝置之標籤的**檢視裝置**連結。

   裝置清單僅顯示分配了標籤的裝置。

要返回裝置標籤清單，點擊您瀏覽器的**後退**按鈕。

檢視分配到裝置的標籤

要檢視分配到裝置的標籤：

1. 在主功能表中，轉至 **裝置 → 受管理裝置**。
2. 點擊您要檢視其標籤的裝置名稱。
3. 在開啟的裝置內容視窗中，選取**標籤**頁籤。

   分配給所選裝置的標籤清單被顯示。在**分配的標籤**列中，您可以檢視標籤的分配方式。

在工具列中，您可以進行以下操作：

- 為裝置指派另一個標籤。
- 刪除已經指派的標籤。
- 檢視管理伺服器上存在的所有裝置標籤。

您無法在裝置上本機檢視已指派的標籤。

手動標記裝置

要手動分配標籤到裝置：

1. 檢視分配到您要分配其他標籤的裝置的標籤。
2. 點擊**新增**。
3. 在開啟的視窗中，執行以下操作之一：
   - 若要建立並指派新標籤，請選取**建立新標籤**，之後指定新標籤的名稱。
   - 若要選取現有標籤，請選取**分配現有標籤**，之後在下拉清單選取必要標籤。
4. 點擊**確定**以套用變更。
5. 點擊**儲存**以儲存變更。

所選的標籤被分配到裝置。

從裝置上刪除分配的標籤

要從裝置上刪除標籤：

1. 在主功能表中，轉至 **裝置 → 受管理裝置**。
2. 點擊您要檢視其標籤的裝置名稱。
3. 在開啟的裝置內容視窗中，選取**標籤**頁籤。
4. 選取您要刪除的項目旁邊的核取方塊。
5. 在清單頂部，點擊**取消分配標籤**按鈕。
6. 在開啟的視窗中，點擊**是**按鈕。

標籤從裝置上刪除。

未配置的裝置標籤不被刪除。如果您想，您可以手動刪除它。

您不能手動刪除應用程式或網路代理分配給裝置的標籤。要刪除這些標籤，請使用 klscflag 公用程式。

檢視自動標記裝置規則

要檢視自動標記裝置規則，

做以下任意：

- 在主功能表中，轉至 **裝置** → **標籤** → **自動標記規則**。
- 在主功能表中，前往**裝置** → **標籤** → **裝置標籤**，然後點擊**設定自動標記規則**連結。
- 檢視指派給裝置的標籤，接著點擊**設定**按鈕。

自動標記裝置規則清單出現。

編輯自動標記裝置規則

要編輯自動標記裝置規則：

1. 檢視自動標記裝置規則。
2. 點擊您要編輯的規則名稱。
   規則設定視窗開啟。
3. 編輯規則的一般內容：
   a. 在**規則名稱**欄位，輸入規則名稱。
      名稱不能包括 256 個以上字元。
   b. 做以下任意：
      - 透過切換開關按鈕至**規則已啟用**啟用規則。
      - 透過切換開關按鈕至**規則已停用**停用規則。
4. 做以下任意：
   - 如果要新增新條件，請點擊**新增**按鈕，然後在開啟的視窗中指定新條件的設定。
   - 若要編輯現有條件，請點擊您要編輯之條件的名稱，接著編輯條件設定。
   - 若您要刪除條件，請選取您要刪除之條件名稱旁的核取方塊，接著點擊**刪除**。
5. 在條件設定視窗點擊**確定**。
6. 點擊**儲存**以儲存變更。

編輯的規則顯示在清單。

建立自動標記裝置規則

要建立自動標記裝置規則：

1. 檢視自動標記裝置規則。
2. 點擊**新增**。
   新規則設定視窗開啟。

3. 配置規則的一般內容：

   a. 在**規則名稱**欄位中，輸入規則名稱。
   名稱不能包括 256 個以上字元。

   b. 執行以下操作之一：

   - 透過切換開關按鈕至**規則已啟用**啟用規則。
   - 透過切換開關按鈕至**規則已停用**停用規則。

   c. 在**標籤**欄位中，輸入新裝置標籤名稱或從清單中選取其中一個現有裝置標籤。
   名稱不能包括 256 個以上字元。

4. 在條件區段中，點擊**新增**按鈕以新增新條件。
   新條件設定視窗開啟。

5. 輸入條件名稱。
   名稱不能包括 256 個以上字元。名稱必須在規則內唯一。

6. 設定根據以下條件的規則觸發。您可以選取多個條件。

   - **網路**—裝置網路內容，例如 Windows 網路中的裝置名稱，或裝置是否屬於網域或 IP 範圍。

     如果為您用於卡巴斯基安全管理中心的資料庫設定了區分大小寫的排序規則，請在指定裝置 DNS 名稱時保持大小寫。否則，自動標記規則將不起作用。

   - **應用程式**—網路代理在裝置上的出現，和作業系統類型、版本和架構。
   - **虛擬機**—裝置屬於虛擬機的特定類型。
   - **Active Directory**—裝置在 Active Directory 組織單元中的出現和裝置在 Active Directory 群組中的成員關係。
   - **應用程式登錄資料**—裝置上不同供應商應用程式的出現。

7. 點擊**確定**儲存變更。
   如果必要，您可以為一個規則設定多個條件。此種情況下，在滿足至少一個條件時，標籤將被分配到裝置。

8. 點擊**儲存**以儲存變更。

新建立的規則會在所選管理伺服器管理的裝置上強制執行。如果裝置的設定滿足規則條件，標籤被分配到裝置。

然後，規則被套用到以下情況：

- 自動和間歇性，取決於伺服器負載
- 在您編輯規則之後

- 當您手動執行規則時
- 在管理伺服器偵測到滿足規則條件的裝置設定的變更或包含此裝置的群組設定的變更後

您可以建立多個標記規則。如果您建立了多個標記規則且規則對應的條件同時被滿足，單個裝置可以被分配多個標籤。您可以在裝置內容中檢視所有分配的標籤清單。

為自動標記裝置執行規則

當規則執行時，規則內容中指定的標籤被分配到滿足相同規則中指定條件的裝置。您僅可以執行活動規則。

要為自動標記裝置執行規則：

1. 檢視自動標記裝置規則。
2. 選取您要執行的活動規則旁邊的核取方塊。
3. 點擊**執行規則**按鈕。

   所選規則被執行。

刪除自動標記裝置規則

要刪除自動標記裝置規則：

1. 檢視自動標記裝置規則。
2. 選取您要刪除的規則旁邊的核取方塊。
3. 點擊**刪除**。
4. 在開啟的視窗中，再次點擊**刪除**按鈕。

   所選規則被刪除。規則內容中指定的標籤從所有所分配的裝置上取消分配。

> 未配置的裝置標籤不被刪除。如果您想，您可以手動刪除它。

使用 klscflag 公用程式管理裝置標籤

若要向裝置指派一組標籤，您需要在要指派標籤的用戶端裝置上執行 klscflag 公用程式。

klscflag 實用程式會覆寫指派給裝置的現有標籤。這意味著，您可以透過在命令中指定所需的標籤集合來新增或刪除標籤。該公用程式沒有用於新增或刪除單一標籤的單獨命令。相反，您會修改整個標籤集合。

> 在 klscflag 等命令中指定標籤名稱時，建議使用一致的大小寫方法，例如全部大寫。使用全部大寫可以幫助避免僅大小寫不同的頁籤的潛在問題，具體取決於 DBMS 組態。

要使用 klscflag 公用程式對您的裝置分配標籤：

1. 使用管理員權限執行 Windows 命令提示符，然後將目前目錄變更為包含 klscflag 公用程式的目錄。klscflag 公用程式位於安裝網路代理的資料夾中。預設安裝路徑：<Disk>:\Program Files (x86)\Kaspersky Lab\NetworkAgent。

2. 輸入以下一個指令：

   - 要指派一組標籤：

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"標籤名稱 1\",\"標籤名稱 2\",\"標籤名稱 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     其中 [\"標籤名稱 1\",\"標籤名稱 2\",\"標籤名稱 3\"] 是您要指派給裝置的標籤清單。

     如果將方括號留空，這將從裝置中刪除所有標籤：

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

   - 若要將新標籤指派給現有標籤集合：

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"新標籤名稱\",\"標籤名稱 1\",\"標籤名稱 2\",\"標籤名稱 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     其中NEW TAG NAME是您想要指派給裝置的標籤的名稱，而TAG NAME 1、TAG NAME 2、TAG NAME 3是已指派給裝置的標籤的名稱。

   - 若要刪除特定標籤而不刪除已指派給裝置的其他標籤，請使用更新的標籤集合執行該指令。

     例如，如果您目前的標籤是標籤名稱 1、標籤名稱 2、標籤名稱 3，並且您想要刪除標籤名稱 2，請執行下列命令：

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"標籤名稱 1\",\"標籤名稱 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

3. 重新啟動網路代理服務。

   klscflag 公用程式將把指定標籤指派給您的裝置。

4. 如果您想要確保 klscflag 公用程式已成功指派了指定標籤，請檢視指派給裝置的標籤。

或者，您可以手動分配裝置標籤。

政策和政策設定檔

在卡巴斯基安全管理中心網頁主控台中，您可以為 Kaspersky 應用程式建立政策。該部分描述了政策和政策設定檔，並提供建立和修改它們的說明。

關於政策和政策設定檔

*政策*是一組套用於管理群組及其子群組的卡巴斯基應用程式設定。您可以在管理群組的裝置上安裝多個 Kaspersky 應用程式。卡巴斯基安全管理中心為管理群組中的每個卡巴斯基應用程式提供單一政策。政策會有下列其中一種狀態（請見下表）：

政策狀態

狀態	敘述
活動	套用至裝置的目前政策。每個管理群組中的 Kaspersky 應用程式只能啟用一個政策。裝置將為卡巴斯基應用程式套用活動政策的設定值。
不啟用	目前未將政策套用至裝置。
漫遊	如果選取該選項，政策將在裝置離開企業網路時變為啟用狀態。

政策會根據以下規則執行：

- 您可以為單個應用程式配置擁有不同值的多個政策。
- 對於目前應用程式只有一個政策可以處於啟用狀態。
- 您可在特定事件發生時啟動非作用中的政策。例如，這代表您可以在病毒爆發時定義更加嚴謹的病毒防護設定。
- 政策可以有子政策。

通常，您可以將政策作為緊急情況 (例如病毒攻擊) 的準備。例如，如果有透過快閃記憶體磁碟機的攻擊，則可以啟動阻止存取快閃記憶體磁碟機的政策。在這種情況下，目前的啟用政策將自動變為非啟用狀態。

為了防止維護多個政策，例如，當不同場合僅假設變更多個設定時，您可以使用政策設定檔。

*政策設定檔*是政策設定值的已命名子集，用於替換政策的設定值。政策設定檔會影響受管理裝置上有效的設定形式。*有效設定*是目前應用於裝置的一組政策設定，政策設定檔設定和本機應用程式設定。

政策設定檔會根據以下規則執行：

- 當特定的啟動條件發生時，政策設定檔會生效。
- 政策設定檔包含與政策設定不同的設定值。
- 政策設定檔的啟動會變更受管理裝置的有效設定。
- 政策可以包含最多 100 個設定檔。

關於鎖定和已鎖定的設定

每個政策設定都有一個鎖定按鈕圖示 ( )。下表顯示鎖定按鈕的狀態：

鎖定按鈕狀態

狀態	敘述
未定義	如果設定旁邊顯示開啟鎖，並且停用了切換按鈕，則該設定未在政策中指定。使用者可以在受管理應用程式介面中變更這些設定。這些類型的設定稱為*解鎖*。
強制	如果設定旁邊顯示關閉的鎖頭，並且啟用了切換按鈕，則該設定將套用於強制執行政策的裝置。使用者無法在受管理應用程式介面中修改這些設定的值。這些類型的設定稱為*鎖定*。

我們強烈建議您關閉要在受管理裝置上套用的政策設定的鎖定。解鎖的政策設定可以由卡巴斯基應用程式設定在受管理裝置上重新分配。

您可以使用鎖定按鈕執行以下操作：

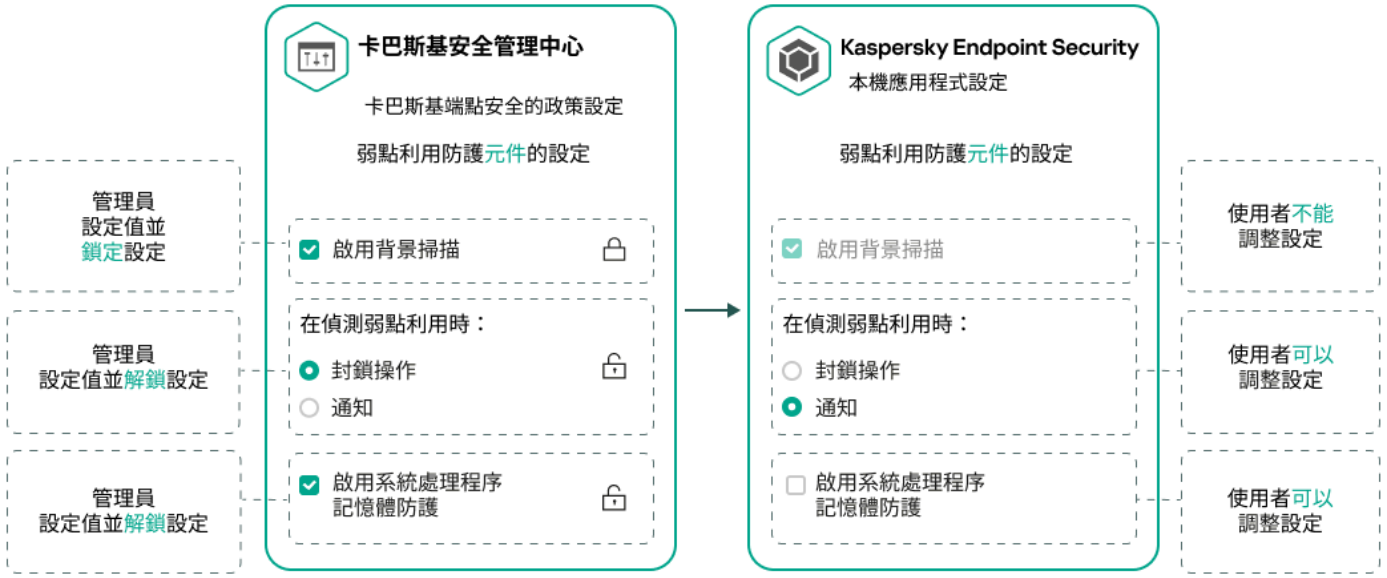
- 鎖定管理子群組政策的設定
- 在受管理裝置上鎖定卡巴斯基應用程式的設定

因此，鎖定設定可用於在受管理裝置上實作有效的設定。

有效設定的實作程序包括以下操作：

- 受管理裝置會套用卡巴斯基應用程式的設定值。
- 受管理裝置會套用政策的鎖定設定值。

政策和受管理卡巴斯基應用程式包含相同的設定集。配置政策設定時，卡巴斯基應用程式設定會變更受管理裝置上的值。您無法調整受管理裝置上的鎖定設定（請參閱下圖）：



鎖定和卡巴斯基應用程式設定

政策繼承和政策設定檔

本節提供政策和政策設定檔的階層和繼承資訊。

政策層級

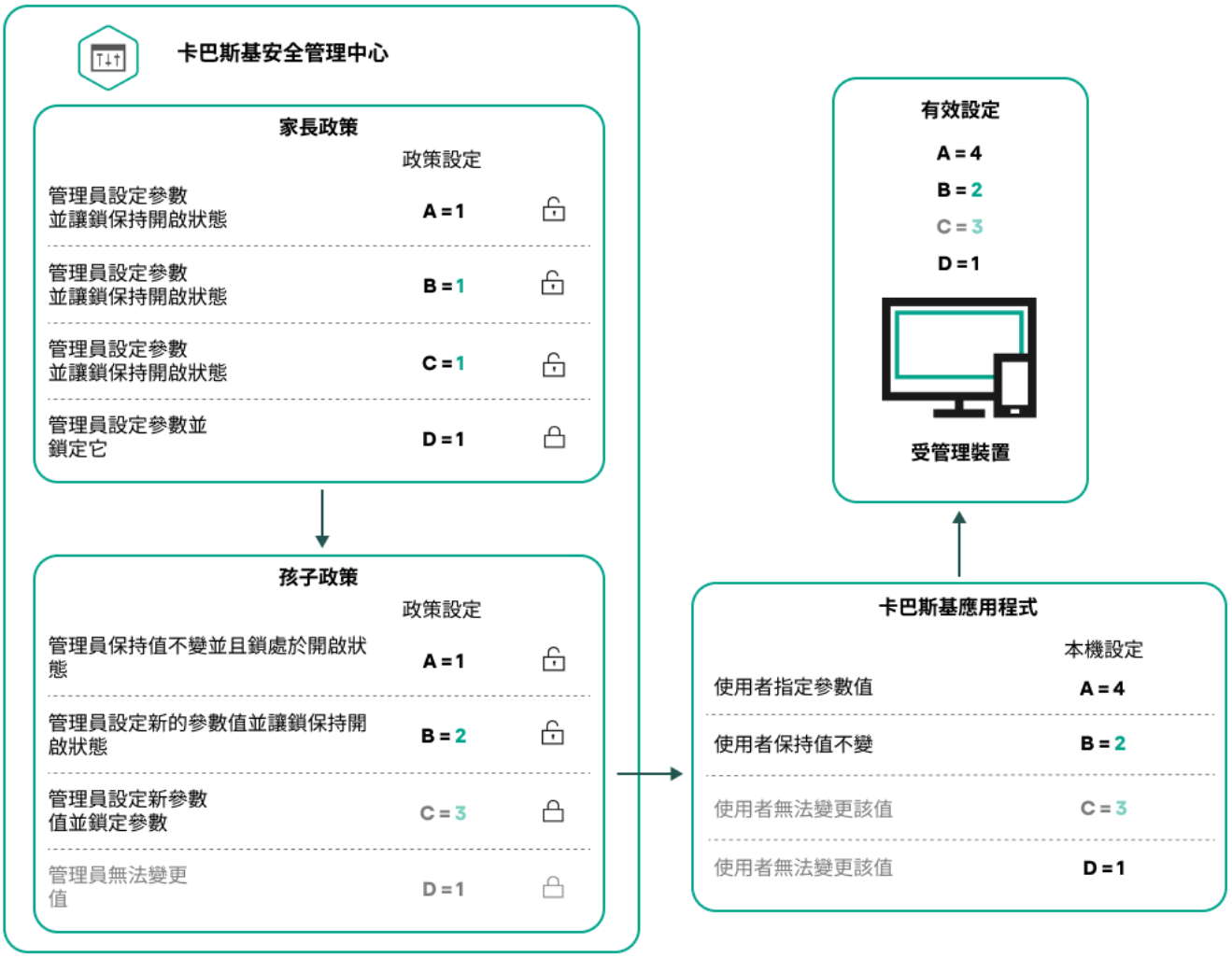
如果不同的裝置需要不同的設定，則可以將裝置組織到管理群組中。

您可以為單一管理群組指定政策。政策設定可以*繼承*。繼承代表從上級（父）管理群組的政策接收子群組（子群組）中的政策設定值。

因此，父群組政策也叫*父政策*。子群組的政策也叫*子政策*。

預設情況下，管理伺服器上至少存在受管理裝置群組。如果要建立自訂組，它們將作為受管理裝置群組內的子群組（子群組）建立。

根據管理群組的層次結構，相同應用程式的政策會互相作用。上級（父）管理群組政策的鎖定設定將重新分配子群組的政策設定值（請參閱下圖）。

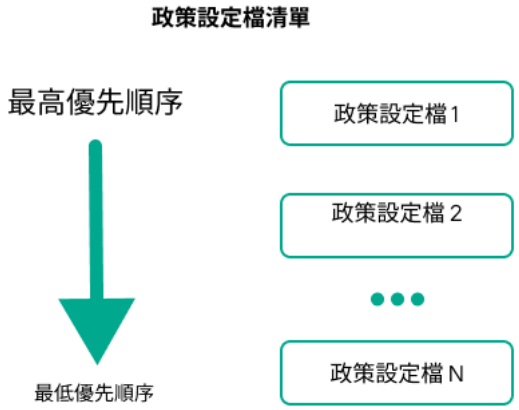


政策層級

政策層次結構中的政策設定檔

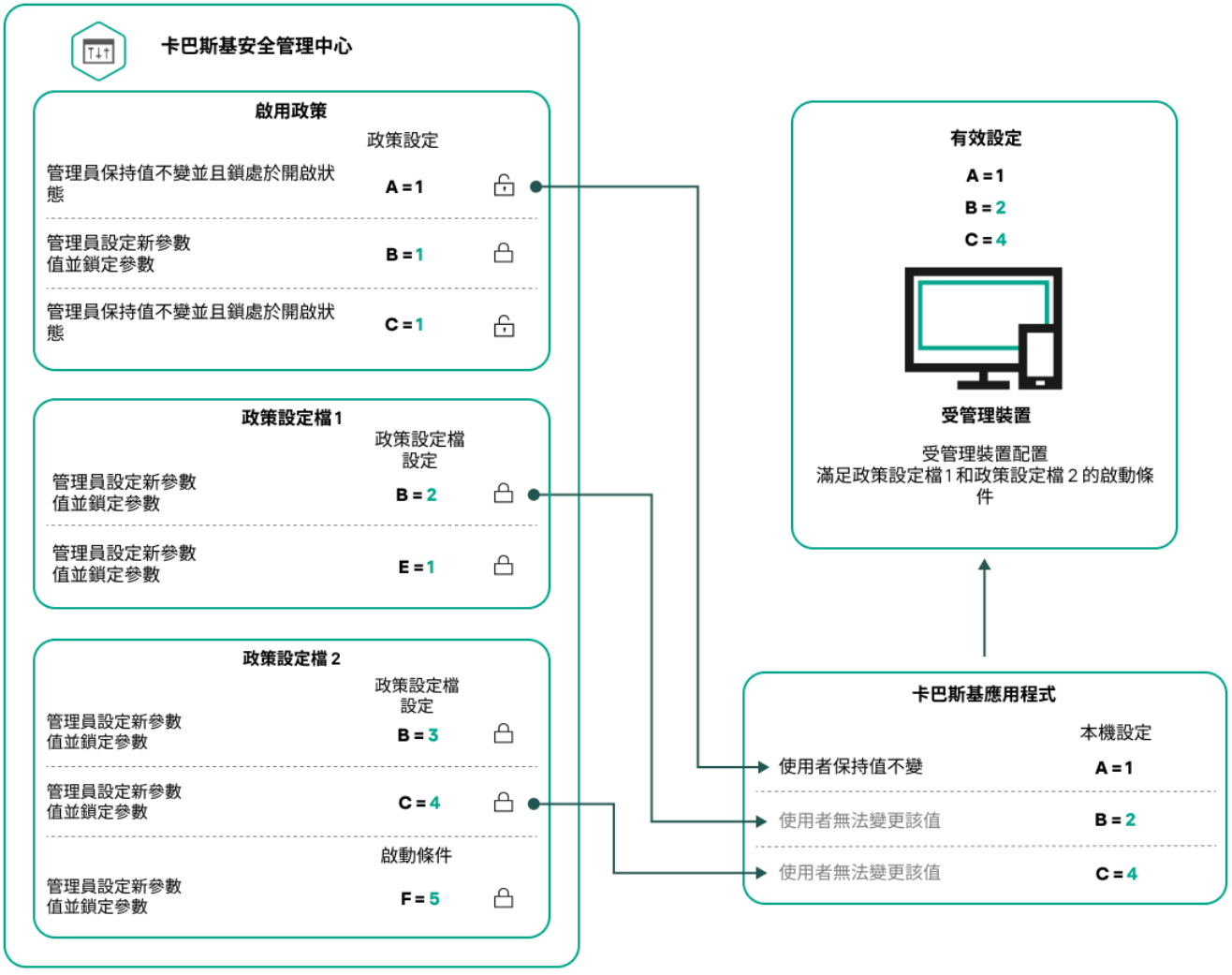
政策設定檔具有以下優先等級分配條件：

- 設定檔在政策設定檔清單中的位置指示其優先等級。您可變更政策設定檔的優先順序。清單中的最高位置表示最高優先等級（請參閱下圖）。



政策設定檔的優先等級定義

- 政策設定檔的啟動條件互不依賴。您可以同時啟動多個政策設定檔。如果多個政策設定檔影響相同設定，則裝置將從政策設定檔中取得具有最高優先等級的設定值（請參閱下圖）。

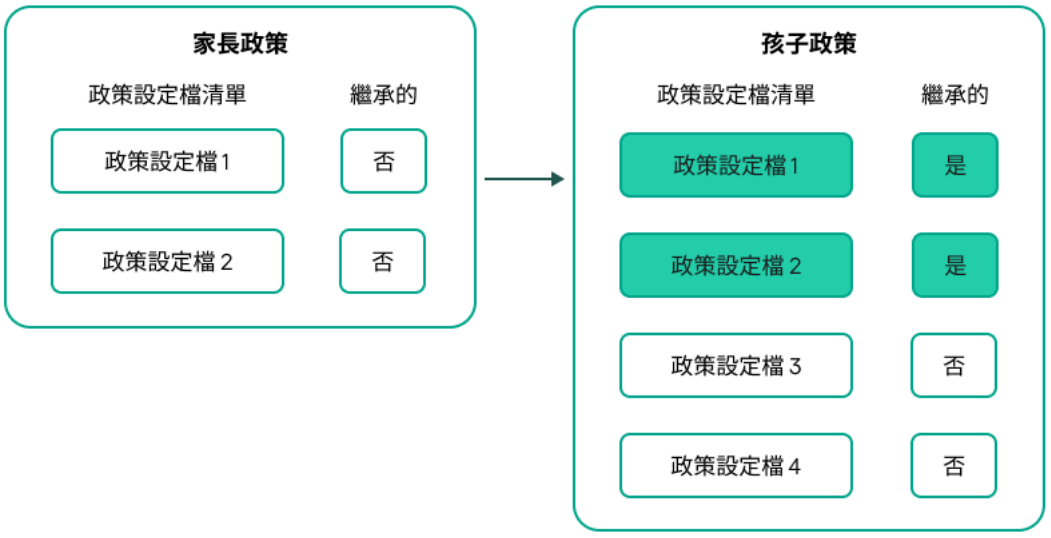


受管理裝置配置滿足幾個政策設定檔的啟動條件

繼承層次結構中的政策設定檔

來自不同層次結構層級政策的政策設定檔符合以下條件：

- 較低層級的政策從較高層級的政策繼承政策設定檔。從較高級政策繼承的政策設定檔比原始政策設定檔的層級具有更高的優先等級（請參閱下圖）。
- 您不能變更繼承之政策設定檔的優先等級（請參見下圖）。

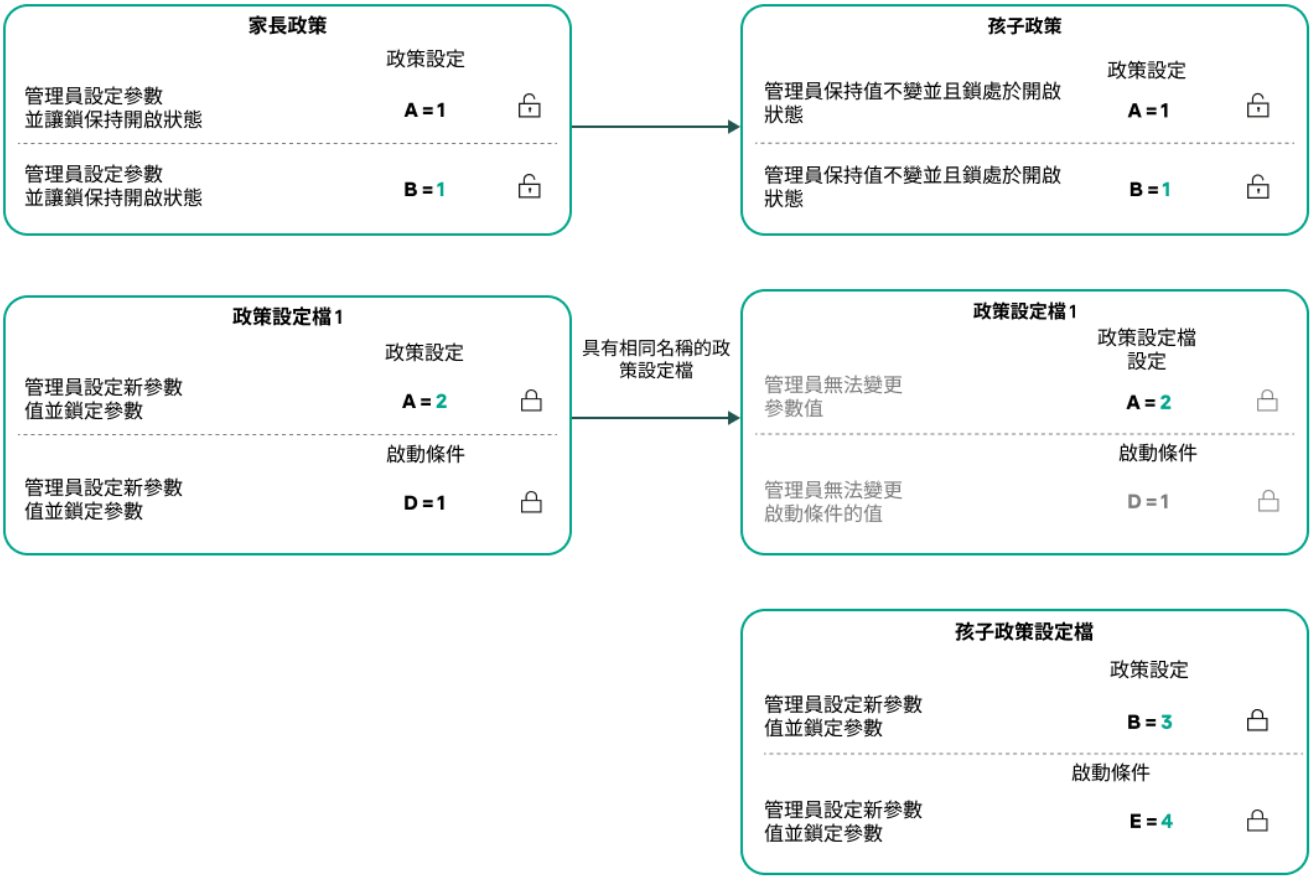


政策設定檔繼承

具有相同名稱的政策設定檔

如果在不同的層次結構層級中有兩個名稱相同的政策，則這些政策將根據以下規則執行：

- 上級政策設定檔的鎖定設定和設定檔啟動條件會變更下級政策設定檔的設定和設定檔啟動條件（請參閱下圖）。



子設定檔從父政策設定檔繼承設定值

- 上級政策設定檔的解鎖設定和設定檔啟動條件不會變更下級政策設定檔的設定和設定檔啟動條件。

如何在受管理裝置上實作設定

以下提供在受管理裝置上實作有效設定的說明：

- 所有未被鎖定的設定值都取自於政策。
- 然後，這將被受管理應用程式設定的值覆寫。
- 接著，將套用有效政策中被鎖定的設定值。鎖定的設定值會變更未鎖定的有效設定值。

管理政策

本節說明管理政策，並提供檢視政策清單、建立政策、修改政策、複製政策、移動政策、強制同步、檢視政策分發狀態圖，以及刪除政策的資訊。

檢視政策清單

您可以檢視為管理伺服器或任何管理群組建立的政策清單。

要檢視政策清單，請執行以下操作：

1. 在主功能表中，轉至 **裝置 → 群組的階層**。
2. 在管理群組結構中，選擇您要檢視其政策清單的管理群組。

政策清單以表格格式出現。如果沒有政策，表格為空。您可以顯示或隱藏表格的列，變更它們的順序，僅檢視包含指定值的行，或者使用尋找。

建立政策

您可以建立政策；您也可以修改和刪除現有政策。

要建立政策：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。
2. 選擇要為其建立政策的管理群組：
   - 對於根群組。
     在這種情況下，您可以繼續執行下一步。
   - 對於子群組：
     a. 點擊視窗頂部的目前路徑連結。
     b. 在開啟的面板中，按一下包含所需子群組名稱的連結。

   目前路徑會發生變更以反映所選的子群組。
3. 點擊**新增**。
   選取應用程式視窗將開啟。
4. 選取您要建立政策的應用程式。
5. 點擊**"下一步"**。
   新政策設定視窗會開啟，並含有所選的**一般**頁籤。
6. 如果您需要，變更政策的預設名稱、預設狀態和預設繼承設定。
7. 選取 **應用程式設定**頁籤。
   或者，您可點擊**儲存**並結束。政策將出現在政策清單，且您可以稍後編輯其設定。

8. 在**應用程式設定**頁籤的左窗格中選取您需要的類別，在優方的結果窗格中編輯政策的設定。您可以在每個類別中（區域）編輯政策設定。

   設定集會以您建立政策的應用程式為依據。如需詳細資訊，請參閱以下內容：

   - 管理伺服器配置
   - 網路代理政策設定
   - Kaspersky Endpoint Security for Windows 文件

   如需設定其他安全應用程式設定的詳細資訊，請參閱對應應用程至的文件。

   編輯設定時，您可點擊**取消**來取消最後的操作。

9. 點擊**儲存**儲存政策。

該政策將顯示在政策清單中。

修改政策

要修改政策：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。
2. 點擊您要修改的政策。

   政策設定視窗隨即開啟。
3. 指定通用設定和為其建立政策的應用程式的設定。如需詳細資訊，請參閱以下內容：

   - 管理伺服器配置
   - 網路代理政策設定
   - Kaspersky Endpoint Security for Windows 文件

   如需設定其他安全應用程式設定的詳細資訊，請參閱對應應用程式的文件。
4. 點擊**儲存**。

對政策所做的變更將儲存在政策內容中，並且會顯示在**變更歷程**區段。

一般政策設定

一般

在**一般**區域，您可以修改政策狀態並指定政策設定的繼承：

- 在**政策狀態**區塊中，您可以選取一種政策模式：
  - **作用中**

    如果選取該選項，政策將變為啟用狀態。
    預設情況下已選定此選項。

  - **漫遊**

    如果選取該選項，政策將在裝置離開企業網路時變為啟用狀態。

  - **非作用中**

    如果選取該選項，政策將變為不啟用狀態，但它仍然儲存在**政策**資料夾中。如果需要，您可以啟動該政策。

- 在**設定繼承**設定群組中，您可以配置政策繼承：
  - **從父政策繼承設定**

    如果啟用此選項，則政策設定值將繼承上一級群組政策，因而會受到鎖定。
    預設情況下已啟用該選項。

  - **在子政策中強制繼承設定**

    如果啟用此選項，則在套用政策變更之後，程式將執行以下操作：
    - 政策設定的值將被傳送到管理子群組的政策，也就是子政策。
    - 在每個子政策內容視窗的**一般**區域的**設定繼承**區塊，系統將自動選取**從父政策繼承設定**核取方塊。

    如果啟用此方塊，則會鎖定子政策設定。
    預設情況下已停用該選項。

事件配置

事件配置區域可讓您配置事件記錄和事件通知。事件根據嚴重等級用下面的標籤分佈：

- **緊急**

  緊急頁籤不會顯示在網路代理政策內容中。

- **功能失效**
- **警告**
- **資訊**

在每個區域，清單顯示在管理伺服器上事件類型和預設事件儲存的期限（天）。點擊事件類型允許您指定以下設定：

- **事件註冊**

  您可以指定儲存事件的天數和選取儲存事件的位置：

  - **使用 Syslog 匯出到 SIEM 系統**
  - **儲存在裝置的作業系統事件記錄中**
  - **儲存在管理伺服器的作業系統事件記錄中**

- **事件通知**

  您可以選取您是否想由以下方法之一被通知事件：

  - **透過郵件通知**
  - **透過簡訊通知**
  - **透過執行可執行檔或指令碼通知**
  - **透過 SNMP 通知**

  預設下，使用在管理伺服器內容標籤中指定的通知設定（例如收件者位址）。如有需要，您可在**電子郵件**、**SMS**與**要執行的可執行檔**頁籤變更這些設定。

變更歷程

變更歷程頁籤可讓您檢視政策修訂的清單，並復原對政策進行的變更（如有必要）。

啟用和停用政策繼承選項

若要啟用或停用政策中的繼承選項：

1. 開啟所需的政策。
2. 開啟**一般**標籤。

3. 啟用或停用政策繼承：

   - 如果您對子群組啟用**從父政策繼承設定**，並在父政策中鎖定一些設定，那麼您無法在子政策中變更這些設定。
   - 如果您對子政策停用**從父政策繼承設定**，那麼您可以變更子政策中的所有設定，即便一些設定在父政策中是鎖定的。
   - 如果您在父群組啟用**在子政策中強制繼承設定**，這將為每個子政策啟用**從父政策繼承設定**。此種情況下，您無法為任何子政策停用該選項。所有在父政策中被鎖定的設定被強制繼承到子群組，且您無法在子群組中變更這些設定。

4. 點擊**儲存**按鈕儲存變更，或點擊**取消**按鈕拒絕變更。

依預設，政策會啟用**從父政策繼承設定**選項。

如果政策有設定檔，所有子政策都會繼承這些設定檔。

複製政策

您可以從一個管理群組複製政策到另一個。

要複製政策到其他管理群組：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。
2. 選取您要複製的政策旁邊的核取方塊。
3. 點擊**複製**按鈕。

   在螢幕的右側，管理群組樹狀目錄被顯示。
4. 在樹狀目錄中，選取目的群組，意即您要複製政策到該群組。
5. 點擊畫面底部的**複製**按鈕。
6. 點擊**確定**以確認操作。

政策將連帶其所有設定檔被複製到目的群組。目標群組中各個複製的政策將會**非作用中**。您可隨時變更狀態至**作用中**。

如果目的群組中已包含名稱與新移動政策的名稱一致的政策，那麼會在新移動政策的名稱後附加一個（<下一個序號>）的索引，例如：（1）。

移動政策

您可以從一個管理群組移動政策到另一個。例如，您要刪除一個群組，但您要為其他群組使用其政策。在此情況下，您可能要先將政策從舊群組移動至新群組，再刪除舊群組。

要移動政策到其他管理群組：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。
2. 選取您要移動的政策旁邊的核取方塊。

3. 點擊**移動**按鈕。

   在螢幕的右側，管理群組樹狀目錄被顯示。

4. 在樹狀目錄中，選取目的群組，例如，您要將政策移動到該群組。

5. 點擊畫面底部的**移動**按鈕。

6. 點擊**確定**以確認操作。

   如果政策不是從資源群組繼承的，它連帶所有設定檔被移動到目的群組。目標群組中的政策狀態是**非作用中**。您可隨時變更狀態至**作用中**。

   如果政策繼承自資源群組，它將保持在資源群組中。它連帶所有其設定檔被複製到目的群組。目標群組中的政策狀態是**非作用中**。您可隨時變更狀態至**作用中**。

如果目的群組中已包含名稱與新移動政策的名稱一致的政策，那麼會在新移動政策的名稱後附加一個（<下一個序號>）的索引，例如：（1）。

匯出政策

卡巴斯基安全管理中心允許您將政策及其設定和政策設定檔儲存到 KLP 檔案。您可以使用此 KLP 檔案匯入儲存的政策到卡巴斯基安全管理中心 Windows 和卡巴斯基安全管理中心 Linux。

要匯出政策，請執行以下操作：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。

2. 選取您要匯出之政策旁邊的核取方塊。

   您不能同時匯出多個政策。如果您選擇了多個政策，**匯出**按鈕將被停用。

3. 點擊**匯出**按鈕。

4. 在開啟的**另存新檔**視窗中，指定政策檔案的名稱和路徑。按一下**儲存**按鈕。

   另存新檔視窗僅當您使用 Google Chrome、Microsoft Edge 或 Opera 時才會顯示。如果您使用其他瀏覽器，政策檔案會自動儲存在**下載**資料夾。

匯入政策

卡巴斯基安全管理中心允許您從 KLP 檔案匯入政策。KLP 檔案包含匯出的政策及其設定和政策設定檔。

要匯入政策，請執行以下操作：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。

2. 點擊**匯入**按鈕。

3. 點擊**瀏覽**按鈕選擇要匯入的政策檔案。

4. 在開啟的視窗中，指定 KLP 政策檔案的路徑，然後按一下**開啟**按鈕。請注意，您只能選擇一個政策檔案。

   政策處理開始。

5. 政策處理完畢後，選擇要將政策套用到哪些管理群組。

6. 點擊**完成**按鈕以完成政策匯入。

此時會顯示匯入結果通知。如果政策匯入成功，您可以按一下**詳細資訊**連結以檢視政策內容。

匯入成功後，政策會顯示在政策清單中。政策的設定和設定檔也會一併匯入。無論匯出期間選取的政策狀態如何，匯入的政策都處於非使用中狀態。您可以在政策內容中變更政策狀態。

如果新匯入政策的名稱與現有政策的名稱相同，則匯入政策的名稱將加上 **(<next sequence number>)** 索引，例如：**(1)**、**(2)**。

檢視政策發佈狀態圖表

在卡巴斯基安全管理中心中，您可以在政策分發狀態圖中查看每個裝置上政策應用程式的狀態。

要檢視每個裝置上的政策發佈狀態：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。

2. 選取要在裝置上檢視分配狀態之政策名稱旁的核取方塊。

3. 在出現的選單中，選取**分發**連結。
   <政策名稱>分發結果視窗隨即開啟。

4. 在開啟的**<政策名稱>分發結果**視窗中，顯示政策的**狀態描述**。

您可以使用政策分發變更清單中顯示的結果數量。裝置最高數量是 100,000。

若要使用政策發佈結果變更清單中顯示的裝置數量：

1. 在主功能表中，轉到您的帳戶設定，然後選擇**介面選項**。

2. 在**政策分發結果中顯示的裝置限制**中，輸入裝置數量（最多 100,000）。
   預設情況下，數量為 5000。

3. 點擊**儲存**。
   設定已儲存並套用。

刪除政策

如果您不再需要一個政策，您可以刪除它。您僅可以刪除一個在指定管理群組中繼承的政策。如果一個政策是繼承的，您僅可以在其被建立的上級群組刪除它。

要刪除政策，請執行以下操作：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。
2. 選取您要刪除之政策旁的核取方塊並點擊**刪除**。
   若您選取繼承的政策，則**刪除**按鈕會變成無法使用（暗顯）。
3. 點擊**確定**以確認操作。

政策連帶其所有設定檔被刪除。

管理政策設定檔

本節說明管理政策設定檔，並提供查看政策設定檔、更改政策設定檔優先等級、建立政策設定檔、修改政策設定檔、複製政策設定檔、建立政策設定檔啟動規則，以及刪除政策設定檔的資訊。

檢視政策設定檔

要檢視政策設定檔：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。
2. 點擊您要檢視其設定檔的政策名稱。
   政策內容視窗會開啟，並含有所選的**一般**頁籤。
3. 開啟**政策設定檔**頁籤。

政策設定檔清單以表格格式出現。如果政策沒有設定檔，將顯示空表。

變更政策設定檔優先順序

要變更政策設定檔優先順序：

1. 轉到您要的政策的設定檔清單。
   將出現政策設定檔清單。
2. 在**政策設定檔**頁籤，選取您要變更優先權之政策設定檔旁的核取方塊。
3. 透過點擊**提高優先順序**或**降低優先順序**，在清單中設定政策設定檔的新位置。
   政策設定檔在清單中的位置越高，其優先順序越高。
4. 點擊**儲存**按鈕。

所選政策設定檔的優先順序被變更並套用。

建立政策設定檔

要建立政策設定檔：

1. 轉到您要的政策的設定檔清單。
   將出現政策設定檔清單。如果政策沒有設定檔，將顯示空表。
2. 點擊**新增**。
3. 如果您需要，變更設定檔的預設名稱和預設繼承設定。
4. 選取 **應用程式設定**頁籤。
   或者，您可點擊 **儲存**並結束。您建立的設定檔將出現在政策設定檔清單，且您可以稍後編輯其設定。
5. 在**應用程式設定**頁籤的左窗格與右邊的結果窗格中選取您要的類別，接著編輯設定檔的設定。您可以在每個類別中（區域）編輯政策設定檔設定。
   編輯設定時，您可點擊**取消**來取消最後的操作。
6. 點擊**儲存**以儲存設定檔。

該設定檔顯示在政策設定檔清單中。

修改政策設定檔

只有 Kaspersky Endpoint Security for Windows 的政策才支援編輯政策設定檔。

修改政策設定檔：

1. 轉到您要的政策的設定檔清單。
   將出現政策設定檔清單。
2. 在**政策設定檔**頁籤，選取您要修改的政策設定檔。
   "政策設定檔"視窗開啟。
3. 在內容視窗中設定設定檔：
   - 如有需要，請在**一般**區域中變更設定檔名稱，並啟用或停用設定檔。
   - 編輯設定檔啟動規則。
   - 編輯應用程式設定。

   對於其他安全應用程式設定詳情，請參閱對應應用程式文件。
4. 點擊**儲存**。

您已變更的設定將在裝置與管理伺服器同步之後生效（如果政策設定檔處於活動狀態），或在啟動規則觸發後生效（如果政策設定檔處於非活動狀態）。

複製政策設定檔

您可以複製政策設定檔到目前政策或其他政策，例如，如果您要對不同政策擁有相同設定檔。您也可以使用複製，如果您想擁有兩個或更多僅在少數設定不同的設定檔。

要複製政策設定檔：

1. 轉到您要的政策的設定檔清單。

   將出現政策設定檔清單。如果政策沒有設定檔，將顯示空表。

2. 在**政策設定檔**頁籤，選取您要複製的政策設定檔。

3. 點擊**複製**。

4. 在開啟的視窗中，選取您要複製設定檔的政策。

   您可以複製政策設定檔到相同政策或您指定的政策。

5. 點擊**複製**。

   政策設定檔被複製到您選取的政策。新複製的設定檔具有最低優先順序。如果您複製設定檔到相同政策，新複製的設定檔名稱將附加（ ）索引，例如：（1）、（2）。

稍後，您可以變更設定檔設定，包括它的名稱和內容；原始政策設定檔此種情況下將不被變更。

建立政策設定檔啟動規則

要建立政策設定檔啟動規則：

1. 轉到您要的政策的設定檔清單。

   將出現政策設定檔清單。

2. 在**政策設定檔**頁籤，點擊您需在其中建立啟動規則的政策設定檔。

   如果政策設定檔清單為空，您可以建立政策設定檔。

3. 在**啟動規則**標籤上，點擊**新增**按鈕。

   政策設定檔啟動規則視窗開啟。

4. 指定規則的名稱。

5. 選取影響您目前建立的政策設定檔的啟動的條件的核取方塊：

- **政策設定檔啟動一般規則**

  選取該核取方塊依據裝置行動模式狀態設定裝置上的政策設定檔啟動規則、連線管理伺服器規則和分配給裝置的標記。

  對於該選項，指定在下一步：

  - **裝置狀態**

    定義裝置出現在網路的條件：

    - **線上**—裝置位在網路中，因此可使用管理伺服器。
    - **離線**—裝置位在網路外，因此無法使用管理伺服器。
    - **N/A**—將不套用標準。

  - **本裝置上已啟動管理伺服器連線規則**

    選取政策設定檔啟動條件（規則是否被執行）並選取規則名稱。

    規則定義裝置網路位置以便連線到管理伺服器，它的條件必須被滿足（或不滿足）以便啟動政策設定檔。

    用於連線到管理伺服器的裝置網路位置敘述可以在網路代理轉換規則中被建立或設定。

- **特別裝置所有者規則**

  對於該選項，指定在下一步：

  - **裝置所有者**

    啟用此選項依據裝置所有者在其上設定和啟用設定檔啟動規則。在此方塊下的下拉清單，你可以選取設定檔啟動標準：

    - 裝置屬於指定的擁有者（“=”符號）。
    - 裝置不屬於指定的擁有者（“#”符號）。

      如果啟用該選項，設定檔根據配置的標準在裝置上啟動。啟用此選項時，您可以指定裝置所有者。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

  - **裝置所有者在內部安全群組中**

    啟用此選項以卡巴斯基安全管理中心內部安全群組的資格在裝置上設定和啟用設定檔啟動規則。在此方塊下的下拉清單，你可以選取設定檔啟動標準：

    - 裝置所有者是指定安全群組的成員（“=”符號）。
    - 裝置所有者不是指定安全群組的成員（“#”符號）。

      如果啟用該選項，設定檔根據配置的標準在裝置上啟動。您可以指定卡巴斯基安全管理中心的安全性群組。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

- **硬體說明書規則**

  選取該核取方塊依據記憶體和邏輯處理器數量設定裝置上的政策設定檔啟動規則。

  對於該選項，指定在下一步：

  - **記憶體大小 (MB)**

    啟用此選項透過裝置上可用 RAM 容量在裝置上設定和啟用設定檔啟動規則。在此方塊下的下拉清單，你可以選取設定檔啟動標準：

    - 該裝置記憶體大小小於指定值（"<" 符號）。
    - 該裝置記憶體大小大於指定值（">" 符號）。

    如果啟用該選項，設定檔根據配置的標準在裝置上啟動。您可以指定裝置上的 RAM 容量。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

  - **邏輯處理器數量**

    啟用此選項透過裝置上邏輯處理器數量在裝置上設定和啟用設定檔啟動規則。在此方塊下的下拉清單，你可以選取設定檔啟動標準：

    - 裝置上邏輯處理器數量少於或等於指定值（“<”符號）。
    - 裝置上邏輯處理器數量大於或等於指定值（“>”符號）。

    如果啟用該選項，設定檔根據配置的標準在裝置上啟動。您可以指定裝置上的邏輯處理器數量。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

- **角色分配規則**

  對於該選項，指定在下一步：

  由裝置所有者特定角色啟動政策設定檔

  選取該選項以在裝置上根據所有者角色配置和啟用設定檔啟動規則。從現有角色清單手動新增角色。

  如果啟用該選項，設定檔根據配置的標準在裝置上啟動。

- **標籤使用規則**

  選取該核取方塊根據分配到裝置的標籤設定裝置上的政策設定檔啟動規則。您可以在有選取標籤或沒有選取標籤的裝置啟動政策設定檔。

  對於該選項，指定在下一步：

  - **標籤**

    在標籤清單中，透過選中與相應標籤對應的方塊，可以指定政策設定檔中的裝置包含規則。

    您可以透過清單上方的欄位新增新標籤到清單，並點擊**新增**按鈕。

    政策設定檔包含具有選定標籤的裝置。如果清除方塊，則將不套用該標準。預設情況下已清除這些方塊。

- **套用到沒有指定標籤的裝置**

  如果您必須轉換您的標籤選項則啟用此選項。

  如果啟用此選項，政策設定檔將包含未帶有所選標籤的敘述的裝置。如果停用該選項，則不套用標準。

  預設情況下已停用該選項。

- **Active Directory 使用規則**

  選取該核取方塊依據裝置在 Active Directory 組織單元中的出現或者裝置在 Active Directory 安全性群組中的成員關係設定裝置上的政策設定檔啟動規則。

  對於該選項，指定在下一步：

  - **裝置所有者列入 Active Directory 安全群組**

    如果啟用此選項，當裝置屬於指定的安全群組或指定安全群組的子群組時，裝置上的政策設定檔被啟動。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

  - **裝置列入 Active Directory 安全群組**

    如果選取此核取方塊，則會在裝置上啟動政策設定檔。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

  - **在 Active Directory 組織單元中的裝置分配**

    如果啟用此選項，包含在指定 Active Directory 組織單元 (OU) 中的裝置上的政策設定檔將會啟動。如果停用此選項，則不套用設定檔啟動標準。

    預設情況下已停用該選項。

  精靈的附加頁面數量取決於您在第一步選取的設定。您可以稍後修改政策設定檔啟動規則。

6. 檢查所配置參數的清單。若清單正確，請點擊**建立**。

設定檔將被儲存。當觸發啟動規則時，將在裝置上啟動該設定檔。

針對顯示在**啟動規則**頁籤中政策設定檔內容的設定檔，所建立的政策設定檔啟動規則。您可以修改或刪除任何政策設定檔啟動規則。

多個啟動規則可以被一起觸發。

刪除政策設定檔

要刪除政策設定檔：

1. 轉到您要的政策的設定檔清單。

   將出現政策設定檔清單。

2. 在**政策設定檔**頁籤上，選取要刪除之政策設定檔旁的核取方塊，接著點擊**刪除**。

3. 在開啟的視窗中，再次點擊**刪除**按鈕。

   政策設定檔被刪除。如果政策從低級別群組繼承，設定檔保持在該群組，但變成該群組的政策設定檔。這可以消除低級別群組裝置上安裝的受管理應用程式的設定的顯著修改。

資料加密與防護

在筆記型電腦或硬碟磁碟機被竊取或遺失，或未經授權的使用者和應用程式存取資料時，資料加密能夠降低資料意外洩漏的風險。

以下 Kaspersky 應用程式支援加密：

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Mac

您可以使用使用者介面設定來顯示或隱藏與加密管理功能相關的某些介面元素。

我們不建議在 VDI 中啟用加密。

Kaspersky Endpoint Security for Windows 中的資料加密

您可以管理以下類型的加密：

- 在執行 Windows 作業系統的裝置上，適用於伺服器的 BitLocker 磁碟機加密
- 在執行 Windows 作業系統的裝置上，適用於工作站的卡巴斯基磁碟機加密

例如，透過使用這些 Kaspersky Endpoint Security for Windows 元件，您可以啟用或停用加密、檢視加密磁碟機清單、或產生和檢視有關加密的報告。

您可以透過在卡巴斯基安全管理中心中定義 Kaspersky Endpoint Security for Windows 的政策來設定加密。Kaspersky Endpoint Security for Windows 會根據使用的政策執行加密和解密。關於如何設定規則和加密功能說明的詳細說明，請參閱 Kaspersky Endpoint Security for Windows 說明。

Kaspersky Endpoint Security for Mac 中的資料加密

您可以在執行 macOS 的裝置上使用 FileVault 加密。在使用 Kaspersky Endpoint Security for Mac 時，您可以啟用或停用此加密。

您可以透過在卡巴斯基安全管理中心中定義 Kaspersky Endpoint Security for Mac 的政策來設定加密。Kaspersky Endpoint Security for Mac 將根據使用中的政策執行加密和解密。有關加密功能的詳細說明，請參閱 Kaspersky Endpoint Security for Mac 說明。

檢視加密磁碟機的清單

在卡巴斯基安全管理中心中，您可以檢視有關加密磁碟機和磁碟機層級加密裝置的詳細資訊。磁碟機上的資訊解密後，該裝置會自動從該清單中移除。

檢視加密磁碟機的清單，

在主功能表中，轉至 **操作 → 資料加密與防護 → 加密磁碟機**。

如果功能表上沒有這個區段，表示它隱藏起來了。在使用者介面設定中，啟用**顯示資料加密與防護**選項即可顯示該區段。

匯出加密磁碟機清單為 CSV 或 TXT 檔案。為此，請點擊**將行匯出到 csv 檔案**或**將行匯出到 txt 檔案**按鈕。

檢視加密事件清單

在裝置上執行資料加密或解密工作時，Kaspersky Endpoint Security for Windows 會將以下類型的事件傳送給卡巴斯基安全管理中心：

- 無法加密或解密檔案，或由於磁碟空間不足無法建立加密的壓縮檔案。
- 無法加密或解密檔案，或由於授權問題無法建立加密的壓縮檔案。
- 無法加密或解密檔案，或由於缺少存取權限無法建立加密的壓縮檔案。
- 該應用程式已被封鎖存取加密檔案。
- 未知錯誤。

若要檢視在裝置上的加密資料時發生的錯誤清單，請執行以下操作：

在主功能表中，轉至 **操作 → 資料加密與防護 → 加密事件**。

如果功能表上沒有這個區段，表示它隱藏起來了。在使用者介面設定中，啟用**顯示資料加密與防護**選項即可顯示該區段。

匯出加密磁碟機清單為 CSV 或 TXT 檔案。為此，請點擊**將行匯出到 csv 檔案**或**將行匯出到 txt 檔案**按鈕。

或者，您可以檢查每個受管理裝置的加密事件清單。

若要檢視受管理裝置的加密事件：

1. 在主功能表中，轉至 **裝置 → 受管理裝置**。
2. 按一下受管理裝置的名稱。
3. 在**一般**頁簽上，轉到**防護**部分。
4. 點擊**檢視資料加密錯誤**連接。

建立和檢視加密報告

您可以建立以下報告：

- 受管理裝置加密狀態報告。此報告提供有關各種受管理裝置的資料加密詳細資訊。例如，該報告顯示套用已設定加密規則之政策的裝置數量。此外，您還可以找出需要重新啟動的裝置數量。該報告還包含每台裝置的加密技術和演算法相關資訊。
- 大容量儲存裝置加密狀態報告。此報告包含的資訊與受管理裝置加密狀態報告類似，但它僅提供大容量儲存裝置和卸除式磁碟機的資料。
- 加密磁碟機存取權限報告。此報告會顯示哪些使用者帳戶可以存取加密磁碟機。
- 檔案加密錯誤報告。此報告包含在裝置上執行資料加密或解密工作時所發生錯誤的相關資訊。
- 封鎖存取加密檔案的報告。該報告包含了封鎖應用程式存取加密檔案的資訊。如果未經授權的使用者或應用程式試圖存取加密檔案或磁碟機，則此報告很有用。

您可在**監控和報告 → 報告**區域中產生任何報告。或者，在**操作→資料加密與防護**區域中，您可以產生以下加密報告：

- 大容量儲存裝置加密狀態報告
- 加密磁碟機存取權限報告
- 檔案加密錯誤報告

*要在**資料加密與防護**部分產生加密報告：*

1. 請確保您在介面選項啟用了**顯示資料加密與防護**選項。
2. 在政策內容中，開啟**事件配置**頁籤。
3. 在**緊急**區域，點擊**新增事件**並選取*套用檔案加密/解密規則時出錯*事件旁的核取方塊。
4. 點擊**確定**。
5. 在主功能表中，轉至 **操作 → 資料加密與防護**。

6. 您可以開啟以下其中一個區段：

   - **加密磁碟機**會產生大容量儲存裝置加密狀態報告或加密磁碟機存取權限報告。
   - **加密事件**會產生檔案加密錯誤報告。

7. 按一下您要產生的報告名稱。

報告產生將開始。

以離線模式授予加密磁碟機的存取權限

使用者可要求對加密裝置的存取權限，例如，當 Kaspersky Endpoint Security for Windows 未安裝在受管理裝置時。收到要求後，您可建立存取金鑰檔案並將其傳送給使用者。所有使用案例和詳細指示都會在 Kaspersky Endpoint Security for Windows 說明中提供。

若要以離線模式授予加密磁碟機的存取權限：

1. 從使用者那裡取得要求存取檔案（副檔名為 FDERTC 的檔案）。按照 Kaspersky Endpoint Security for Windows 說明 中的指示，在 Kaspersky Endpoint Security for Windows 中產生該檔案。
2. 在主功能表中，轉至 **操作 → 資料加密與防護 → 加密磁碟機**。

   加密磁碟機清單隨即顯示。
3. 選取使用者要求存取權限的磁碟機。
4. 點擊**同意存取離線模式下的裝置**按鈕。
5. 在開啟的視窗中，選取對應 Kaspersky 應用程式用來加密已選取磁碟機的外掛程式。

   若磁碟機使用卡巴斯基安全管理中心網頁主控台不支援的 Kaspersky 應用程式加密，使用基於 Microsoft Management Console 的管理主控台授予離線存取權限。
6. 按照 Kaspersky Endpoint Security for Windows 說明 提供的說明操作（請參閱本節最後的展開區塊）。

之後，使用者套用收到的檔案來存取加密磁碟機，並讀取儲存在磁碟機上的資料。

使用者和使用者角色

該部分描述了使用者和使用者角色，並提供建立和修改它們、分配角色和群組到使用者以及關聯政策設定檔到角色的說明。

關於用於角色

使用者角色（也叫*角色*）是包含一組權限集的物件。角色可以與安裝在使用者裝置上的 Kaspersky 應用程式設定關聯。您可以在管理伺服器階層中任何層級或在指定物件層級，指派角色給使用者集或安全群組集。

如果您透過包含虛擬管理伺服器的管理伺服器階層管理裝置，請注意您只能從實體管理伺服器建立、修改或刪除使用者角色。然後，您可以將使用者角色傳播到從屬管理伺服器，包括虛擬伺服器。

您可以關聯使用者角色到政策設定檔。若使用者獲派一個角色，此使用者會取得執行工作職能必要的安全設定。

一個使用者角色可以與特定管理群組中的裝置使用者關聯。

使用者角色範圍

*使用者角色範圍*是使用者和管理群組的組合。與使用者角色關聯的設定僅套用到屬於該角色使用者的裝置，以及僅在這些裝置屬於與該角色關聯的群組（包括子群組）時。

使用角色的好處

使用角色的好處之一是您不必為每個受管理裝置或使用者指定安全設定。公司內使用者與裝置的數量可能很多，但不同的工作職能所需的不同安全設定則很小。

與使用政策設定檔的不同點

政策設定檔是為每個 Kaspersky 應用程式建立的政策的內容。角色與許多為不同應用程式建立的政策設定檔相關聯。因此，角色是聯合特定使用者類型的設定到一處的方法。

檢視使用者帳戶和工作階段

卡巴斯基安全管理中心允許您管理使用者帳戶以及帳戶群組。該程式支援兩種帳戶類型：

- 組織員工的帳戶。在輪詢組織網路時管理伺服器擷取資料的使用者帳戶。
- 內部使用者帳戶。當使用虛擬管理伺服器時，這些帳戶被套用。只能在卡巴斯基安全管理中心內建立和使用內部使用者帳戶。

您可以透過以下方式之一檢視使用者帳戶和工作階段清單：

- 在主功能表中，轉至**使用者和角色 → 使用者**。
- 在主功能表中，前往**裝置 →受管理裝置→**<裝置名稱>連結 **→一般**頁簽 **→一般**部分 **→連線**塊。
  連線部分應顯示在執行 Windows 的裝置上具有活動工作階段的使用者帳戶。

如果滿足以下要求，則使用者帳戶和工作階段清單將正確顯示：

- 使用與管理伺服器版本相同或更高版本的網路代理。
- 已啟用Active Directory 輪詢以顯示網域使用者的帳戶。
- 在執行 Windows 的受管理裝置上，**伺服器(LanmanServer)** 服務正在執行。

設定應用程式功能的存取權限。角色型存取控制

卡巴斯基安全管理中心提供了適用於角色型存取的功能，可存取卡巴斯基安全管理中心和受管理 Kaspersky 應用程式的功能。

您可以透過以下其中一種方式為卡巴斯基安全管理中心使用者配置對應用程式功能的存取權限：

- 透過為每個使用者或使用者群組單獨設定權限。
- 透過使用一群組預先定義的權限建立標準使用者角色並根據使用者的職責範圍將這些角色分配給使用者。

使用者角色的應用旨在簡化和縮短配置使用者對應應用程式功能存取權限的常規過程。角色內的存取權限根據標準工作和使用者的職責範圍設定。

可為使用者角色分配與其各自的目的對應的名稱。您可在程式中建立無限數量的角色。

您可以將預定義的使用者角色與已配置的一組權限一起使用，或者建立新角色並自己配置所需的權限。

應用程式功能的存取權

下表顯示卡巴斯基安全管理中心功能，這些功能具有管理相關工作、報告、設定和執行相關使用者操作的存取權限。

要執行表中列出的使用者操作，使用者必須具有操作旁邊指定的權限。

讀取、**寫入**和**執行**權限適用於任何工作、報告或設定。除了這些權限外，使用者還必須具有**為裝置分類執行操作**的權限，才能管理裝置分類上的工作、報告或設定。

表中缺少的所有工作、報告、設定和安裝套件均屬於**一般功能：基本功能**的功能區域。

功能區域	權限	使用者操作：執行操作所需的權限	工作	報告	其他
一般功能：**管理群組的管理**	**寫入**	• 將裝置新增到管理群組：**寫入** • 從管理群組中刪除裝置：**寫入** • 將管理群組新增到另一個管理群組：**寫入** • 從另一個管理群組中刪除管理群組：**寫入**	沒有	沒有	沒有
一般功能：**存取物件而不考慮它們的 ACLs**	**讀取**	獲得對所有物件的讀取存取權限：**讀取**	沒有	沒有	**一般功能：存取物件而不考慮它們的 ACLs** 功能區域均旨在用於稽核目的。當使用者被授予此功能區域的**讀取**權限時，他們將獲得對所有物件的完全**讀取**權限，並且能夠在透過具有本機管理員權限 (對於 Linux 為 root) 的網路代理連線到管理伺服器的選定裝置上執行任何已建立的工作。我們建議謹慎地將這些權利授予需要這些權利來履行正式職責的有限使用者。 無論其他權限如何，系統都會授予存取權限，即使已禁止對特定物件的讀取存取。

功能區域	權限	使用者操作：執行操作所需的權限	工作	報告	其他
一般功能：**基本功能**	• **讀取** • **寫入** • **執行** • **為裝置分類執行操作**	• 虛擬伺服器的裝置移動規則（建立、修改或刪除）：**寫入**、**為裝置分類執行操作** • 取得行動 (LWNGT) 通訊協定自訂憑證：**讀取** • 設定行動 (LWNGT) 通訊協定自訂憑證：**寫入** • 獲取 NLA 定義的網路清單：**讀取** • 新增、修改或刪除 NLA 定義的網路清單：**寫入** • 檢視群組的存取控制清單：**讀取** • 檢視卡巴斯基事件日誌：**讀取** • 檢視用來還原對 BitLocker 加密的硬碟磁碟機的存取權限的還原金鑰：**執行**	• 「將更新下載至管理伺服器儲存區」 • 「提交報告」 • 「分發安裝套件」 • 「在從屬管理伺服器上遠端安裝應用程式」	• 「防護狀態報告」 • 「威脅報告」 • 「受感染最嚴重的裝置報告」 • 「病毒資料庫狀態報告」 • 「錯誤報告」 • 「網路攻擊報告」 • 「已安裝郵件系統保護應用程式的摘要報告」 • 「已安裝的外圍防禦應用程式的摘要報告」 • 「已安裝的應用程式類型概要報告」 • 「受感染的裝置使用者報告」 • 「事件報告」 • 「事件報告」 • 「發佈點活動報告」 • 「從屬管理伺服器的報告」 • 「裝置控制事件報告」 • 「弱點報告」 • 「禁止的應用程式報告」 • 「Web 控制報告」 • 「受管理裝置加密狀態報告」 • 「大容量儲存裝置加密狀態報告」 • 「檔案加密錯誤報告」 • 「封鎖存取加密檔案的報告」 • 「加密磁碟機存取權限報告」 • 「有效使用者權限報告」 • 「權限報告」	沒有
一般功能：**已刪除物件**	• **讀取** • **寫入**	• 檢視資源回收桶中已刪除的物件：**讀取** • 從資源回收桶中刪除物件：**寫入**	沒有	沒有	沒有

功能區域	權限	使用者操作：執行操作所需的權限	工作	報告	其他
一般功能：事件處理	• **刪除事件** • **編輯事件通知設定** • **編輯事件記錄設定** • **寫入**	• 變更事件註冊設定：**編輯事件記錄設定** • 變更事件通知設定：**編輯事件通知設定** • 刪除事件：**刪除事件**	沒有	沒有	設定： • 病毒爆發設定：建立病毒爆發事件所需的病毒偵測次數 • 病毒爆發設定：評估病毒偵測的時段 • 儲存在資料庫中的最大事件數量 • 儲存已刪除裝置中的事件時段
一般功能：在管理伺服器上操作	• **讀取** • **寫入** • **執行** • **修改物件 ACL** • **為裝置分類執行操作**	• 指定適用於網路代理連線之管理伺服器的管理連接埠：**寫入** • 指定在管理伺服器上啟動的啟動代理連接埠：**寫入** • 指定在管理伺服器上啟動的行動啟動代理連接埠：**寫入** • 指定用於發佈獨立套件之網頁伺服器的連接埠：**寫入** • 指定用於發佈 MDM 設定檔的網頁伺服器的連接埠：**寫入** • 指定管理伺服器的 SSL 連接埠以透過卡巴斯基網頁主控台進行連線：**寫入** • 指定用於行動連線之管理伺服器的管理連接埠：**寫入** • 指定儲存在管理伺服器資料庫的事件最大數量：**寫入** • 指定管理伺服器可以傳送的最大事件數：**寫入** • 指定管理伺服器可以傳送事件的時段：**寫入**	• 「備份管理伺服器資料」 • 「資料庫維護」	沒有	沒有

功能區域	權限	使用者操作：執行操作所需的權限	工作	報告	其他
一般功能：**Kaspersky 軟體佈署**	• **管理 Kaspersky 修補程式** • **讀取** • **寫入** • **執行** • **為裝置分類執行操作**	核准或拒絕安裝修補程式：**管理 Kaspersky 修補程式**	沒有	• 「虛擬管理伺服器產品授權金鑰使用報告」 • 「Kaspersky 軟體版本報告」 • 「不相容的應用程式報告」 • 「Kaspersky 軟體模組更新版本報告」 • 「防護部署報告」	安裝套件：「Kaspersky」
一般功能：**產品授權金鑰管理**	• **匯出金鑰檔案** • **寫入**	• 匯出金鑰檔案：**匯出金鑰檔案** • 修改管理伺服器產品授權金鑰設定：**寫入**	沒有	沒有	沒有
一般功能：**強制報告管理**	• **讀取** • **寫入**	• 建立報告，而不考慮其 ACL：**寫入** • 不論報告的 ACL 為何都加以執行：**讀取**	沒有	沒有	沒有
一般功能：**管理伺服器階層**	**設定管理伺服器階層**	註冊、更新或刪除從屬管理伺服器：**設定管理伺服器階層**	沒有	沒有	沒有
一般功能：**使用者權限**	**修改物件 ACL**	• 變更任何物件的「安全性」屬性：**修改物件 ACL** • 管理使用者角色：**修改物件 ACL** • 管理內部使用者：**修改物件 ACL** • 管理安全群組：**修改物件 ACL** • 管理別名：**修改物件 ACL**	沒有	沒有	沒有

功能區域	權限	使用者操作：執行操作所需的權限	工作	報告	其他
一般功能：**虛擬管理伺服器**	• **管理虛擬管理伺服器** • **讀取** • **寫入** • **執行** • **為裝置分類執行操作**	• 取得理虛擬管理伺服器的清單：**讀取** • 取得虛擬管理伺服器的資訊：**讀取** • 建立、更新或刪除虛擬管理伺服器：**管理虛擬管理伺服器** • 將虛擬管理伺服器移動到另一個群組：**管理虛擬管理伺服器** • 設定管理虛擬伺服器權限：**管理虛擬管理伺服器**	沒有	「協力廠商軟體更新安裝結果報告」	沒有
一般功能：**加密金鑰管理**	**寫入**	匯入加密金鑰：**寫入**	沒有	沒有	沒有

功能區域	權限	使用者操作：執行操作所需的權限	工作	報告	其他
行動裝置管理：一般	• **連線新裝置** • **僅傳送指令資訊至行動裝置** • **傳送指令至行動裝置** • **管理憑證** • **讀取** • **寫入**	• 取得金鑰管理服務還原資料：**讀取** • 刪除使用者憑證：**管理憑證** • 取得使用者憑證公開部分：**讀取** • 檢查是否啟用公共金鑰基礎架構：**讀取** • 檢查公共金鑰基礎架構帳戶：**讀取** • 取得公共金鑰基礎架構範本：**讀取** • 透過延伸金鑰使用憑證取得公共金鑰基礎架構範本：**讀取** • 檢查公共金鑰基礎架構憑證是否遭撤銷：**讀取** • 更新使用者憑證發行設定：**管理憑證** • 取得使用者憑證發行設定：**讀取** • 按應用程式名稱和版本取得套件：**讀取** • 設定或取消使用者憑證：**管理憑證** • 續訂使用者憑證：**管理憑證** • 設定使用者憑證標籤：**管理憑證** • 執行 MDM 安裝套件的產生；取消產生 MDM 安裝套件：**連線新裝置**	沒有	沒有	沒有
系統管理：連線	• **啟動 RDP 連線** • **連線到現有 RDP 連線** • **建立通道** • **在管理員工作站上儲存裝置檔案** • **讀取** • **寫入** • **執行** • **為裝置分類執行操作**	• 建立桌面共用工作階段：**啟動 RDP 連線** • 建立 RDP 工作階段：**連線到現有 RDP 連線** • 建立通道：**建立通道** • 儲存內容網路清單：**在管理員工作站上儲存裝置檔案**	沒有	「裝置使用者報告」	沒有

功能區域	權限	使用者操作：執行操作所需的權限	工作	報告	其他
系統管理：硬體清單	• **讀取** • **寫入** • **執行** • **為裝置分類執行操作**	• 取得或匯出硬體詳細目錄物件：**讀取** • 新增、設定或刪除硬體詳細目錄物件：**寫入**	沒有	• 「硬體登錄資料的報告」 • 「組態更改的報告」 • 「硬體報告」	沒有
系統管理：網路存取控制	• **讀取** • **寫入**	• 檢視 CISCO 設定：**讀取** • 更改 CISCO 設定：**寫入**	沒有	沒有	沒有
系統管理：作業系統佈署	• **佈署 PXE 伺服器** • **讀取** • **寫入** • **執行** • **為裝置分類執行操作**	• 部署 PXE 伺服器：**佈署 PXE 伺服器** • 檢視 PXE 伺服器清單：**讀取** • 在 PXE 用戶端上啟動或停止安裝程序：**執行** • 管理 WinPE 和作業系統映像的驅動程式：**寫入**	「在參考裝置作業系統映像上建立安裝套件」	沒有	安裝套件：「作業系統映像檔」
系統管理：弱點和修補程式管理	• **讀取** • **寫入** • **執行** • **為裝置分類執行操作**	• 檢視協力廠商修補程式屬性：**讀取** • 更改協力廠商修補程式屬性：**寫入**	• 「執行 Windows Update 同步」 • 「安裝 Windows Update 更新」 • 「修復弱點」 • 「安裝必要更新並修復弱點」	「軟體更新報告」	沒有
系統管理：遠端安裝	• **讀取** • **寫入** • **執行** • **為裝置分類執行操作**	• 檢視協力廠商弱點和修補程式管理的安裝套件屬性：**讀取** • 更改協力廠商弱點和修補程式管理的安裝套件屬性：**寫入**	沒有	沒有	安裝套件： • 「自訂應用程式」 • 「VAPM 套件」
系統管理：軟體清單	• **讀取** • **寫入** • **執行** • **為裝置分類執行操作**	沒有	沒有	• 「已安裝應用程式的報告」 • 「應用程式登錄資料歷程報告」 • 「已授權應用程式群組狀態報告」 • 「協力廠商軟體產品授權金鑰報告」	沒有

預先定義的使用者角色

分配給卡巴斯基安全管理中心使用者的使用者角色為他們提供了對應用程式功能的存取權限集。

在虛擬伺服器上建立的使用者，在管理伺服器上無法被分配到角色。

您可以將預定義的使用者角色與已配置的一組權限一起使用，或者建立新角色。當建立新角色時，您必須自行設定角色範圍並指派對卡巴斯基安全管理中心功能的存取權限。卡巴斯基安全管理中心中可用的一些預定義使用者角色可以與特定的職位相關聯，例如，**稽核員**、**安全官**、**監督者**（從卡巴斯基安全管理中心版本 11 開始存在這些角色）。這些角色的存取權限會根據標準工作和相關職位的職責範圍預先配置。下表顯示角色可以如何與特定職位建立關聯。

特定職位的角色範例

角色	注釋
稽核員	允許使用本機管理員權限（Linux 為 root）對透過網路代理連線到管理伺服器的裝置分類執行所有檢視操作和任何建立的工作。 我們建議謹慎地將該角色指派給需要它們來履行正式職責的有限使用者。
管理者	允許所有檢視操作，不允許其他操作。您可以分配該角色到負責您組織的 IT 安全的安全官和其他管理員。
安全官	允許所有檢視操作，允許報告管理；在**系統管理**：**連線**區域授予有限的權限。您可以分配該角色到負責您組織的 IT 安全的安全官。

下表顯示指派給每個預先定義使用者角色的存取權限。

角色	敘述

管理伺服器管理員	允許在以下功能區域中進行所有操作：
	• **一般功能**：
	  • **基本功能**
	  • **事件處理**
	  • **管理伺服器階層**
	  • **虛擬管理伺服器**
	• **系統管理**：
	  • **連線**
	  • **硬體清單**
	  • **軟體清查**
	在**一般功能：加密金鑰管理**功能區域中授予**讀取**和**寫入**權限。

管理伺服器憑證運算子	授予以下所有功能區域的**讀取**和**執行**權限：
	• **一般功能**：
	  • **基本功能**
	  • **虛擬管理伺服器**
	• **系統管理**：
	  • **連線**
	  • **硬體清單**
	  • **軟體清查**

稽核員	允許功能區域中的所有操作，位於**一般功能**： • **存取物件而不考慮它們的 ACLs** • **刪除物件** • **強制報告管理** 您可以分配該角色到執行您組織的稽核的人。

安裝管理員	允許在以下功能區域中進行所有操作：
	• **一般功能**：
	  • **基本功能**
	  • **Kaspersky 軟體部署**
	  • **產品授權金鑰管理**
	• **系統管理**：
	  • **作業系統部署**
	  • **弱點和修補程式管理**
	  • **遠端安裝**
	  • **軟體清查**
	在**一般功能：虛擬管理伺服器**功能區域中，授予**讀取**和**執行**權限。

角色	敘述

安裝運算子	授予以下所有功能區域的**讀取**和**執行**權限：
	• **一般功能**：
	  • **基本功能**
	  • **Kaspersky 軟體佈署**（也會在此區域授予**管理 Kaspersky 修補程式**權限）
	  • **虛擬管理伺服器**
	• **系統管理**：
	  • **作業系統部署**
	  • **弱點和修補程式管理**
	  • **遠端安裝**
	  • **軟體清查**

Kaspersky Endpoint Security 管理員	允許在以下功能區域中進行所有操作： • **一般功能：基本功能** • Kaspersky Endpoint Security 區域，包括所有功能 在**一般功能：加密金鑰管理**功能區域中授予**讀取**和**寫入**權限。
Kaspersky Endpoint Security 運算子	授予以下所有功能區域的**讀取**和**執行**權限： • **一般功能：基本功能** • Kaspersky Endpoint Security 區域，包括所有功能
主要管理員	允許功能區域內的所有操作，以下區域*除外*，在**一般功能**： • **存取物件而不考慮它們的 ACLs** • **強制報告管理** 在**一般功能：加密金鑰管理**功能區域中授予**讀取**和**寫入**權限。

主要運算子	授予以下所有功能區域的**讀取**和**執行**（如適用）權限：
	• **一般功能**：
	  • **基本功能**
	  • **刪除物件**
	  • **管理伺服器上的操作**
	  • **Kaspersky 軟體佈署**
	  • **虛擬管理伺服器**
	• **行動裝置管理：一般**
	• **系統管理**，包括所有功能
	• Kaspersky Endpoint Security 區域，包括所有功能

行動裝置管理管理員	允許在以下功能區域中進行所有操作： • **一般功能：基本功能** • **行動裝置管理：一般**
行動裝置管理運算子	在**一般功能**：**基本功能**的功能區域中授予**讀取**和**執行**權限。 在**行動裝置管理**：**一般**功能區域中授予**讀取**和**僅向行動裝置傳送資訊命令**。

角色	敘述
安全官	允許在以下功能區域中進行所有操作，在**一般功能**： • **存取物件而不考慮它們的 ACLs** • **強制報告管理** 在**系統管理：連線**功能區域中，授予**讀取**、**寫入**、**執行**、**將來自裝置的檔案儲存到管理員的工作站**以及**對裝置分類執行操作**的權限。 您可以分配該角色到負責您組織的 IT 安全的安全官。
自助服務入口使用者	允許**行動裝置管理：自助服務入口**功能區域中的所有操作。此功能僅適用於卡巴斯基安全管理中心 11 或更新版本。
管理者	在**一般功能**：**存取物件而不考慮它們的 ACL** 與**一般功能**：**強制報告管理**功能區域中授予**讀取**權限。 您可以分配該角色到負責您組織的 IT 安全的安全官和其他管理員。
弱點和修補程式管理管理員	允許在**一般功能**：**基本功能**與**系統管理**（包括所有功能）功能區域中的所有操作。
弱點和修補程式管理操作者	授予在**一般功能**：**基本功能**和**系統管理**（包括所有功能）功能區域中的**讀取**和**執行**權限（如適用）。
作為服務管理員的網頁主控台	在**一般功能**：應用程式整合功能區**中授予閱讀 和**寫入權限。

為特定物件分配存取權限

除了分配伺服器層級的存取權限，您可以設定對特定物件的存取，例如，對特定工作的存取。該應用程式允許您指定對以下物件類型的存取權限：

- 管理群組
- 工作
- 報告
- 裝置分類
- 事件分類

若要為特定物件分配存取權限：

1. 根據物件類型，在主功能表中，轉至相對應的部分：
   - **裝置 → 群組的階層**
   - **裝置→工作**
   - **監控和報告→報告**
   - **裝置→裝置分類**
   - **監控和報告 → 事件分類**
2. 開啟物件的內容，以將存取權限指派給物件。

   要開啟管理群組或工作的內容視窗，請按一下物件名稱。您可以使用工具列上的按鈕開啟其他物件的內容。
3. 在內容視窗中，開啟**存取權限**部分。

   使用者清單開啟。列出的使用者和安全群組具有物件的存取權限。預設情況下，如果您使用管理群組或伺服器的階層，則清單和存取權限是從父管理群組或主伺服器繼承的。

4. 為了能夠修改清單，啟用**使用自訂權限**選項。

5. 設定存取權限：

   - 使用**新增**和**刪除**按鈕修改清單。
   - 指定使用者或安全群組的存取權限。執行以下操作之一：
     - 如果要手動指定存取權限，請選擇使用者或安全群組，按一下**存取權限**按鈕，然後指定存取權限。
     - 如果你想分配使用者角色到使用者或安全群組，請選擇使用者或安全群組，按一下**角色**按鈕，然後選擇要分配的角色。

6. 點擊**儲存**按鈕。

物件的存取權限已設定好。

分配存取權限給使用者和安全群組

您可以授予使用者和安全群組存取權限以使用管理伺服器的不同功能，例如 Kaspersky Endpoint Security for Linux。

對使用者或安全群組分配存取權限：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。

   管理伺服器內容視窗將開啟。

2. 在"**存取權限**"頁簽上，選中要對其分配權限的使用者或安全群組名稱旁邊的核取方塊，然後點擊"**存取權限**"按鈕。

   您不能同時選擇多個使用者或安全群組。如果您選擇了多個項目，**存取權限**按鈕將被停用。

3. 配置使用者或群組的權限集：

   a. 使用管理伺服器或其他卡巴斯基應用程式的功能擴展節點。

   b. 選擇所需功能或存取權限旁邊的**允許**或**拒絕**核取方塊。

   *示例 1：*選中**應用程式集成**節點旁邊的**允許**核取方塊，向使用者或群組授予對應用程式集成功能（**讀取**、**寫入**和**執行**）的所有可用存取權限。

   *示例 2：*展開**加密金鑰管理**節點，然後選中寫入權限旁邊**的允許**核取方塊，以授予使用者或群組對加密金鑰管理功能的**寫入**存取權限。

4. 配置存取權限集合後，點擊**確定**。

使用者或使用者群組的權限集將被設定。

管理伺服器（或管理群組）的權限被分成以下部分：

- 一般功能：
  - 管理群組的管理
  - 存取物件而不考慮它們的 ACLs
  - 基本功能
  - 已刪除物件
  - 加密金鑰管理
  - 事件處理
  - 在管理伺服器上操作（僅在管理伺服器的內容視窗中）
  - Kaspersky 軟體佈署
  - 產品授權金鑰管理
  - 應用程式整合（用於與 Kaspersky Managed Detection and Response 整合以及身分和存取管理器的功能）
  - 強制報告管理
  - 管理伺服器階層
  - 使用者權限
  - 虛擬管理伺服器
- 行動裝置管理：
  - 一般
  - 自動服務入口
- 系統管理：
  - 連線
  - 硬體清單
  - 網路存取控制
  - 作業系統佈署
  - 弱點和修補程式管理
  - 遠端安裝
  - 軟體清單

如果對權限未選取**允許** 或 **拒絕**，則存取權限被認為是*未定義*：它在對使用者明確拒絕或允許之前被拒絕。

使用者權限是以下的集合：

- 使用者自己的權限
- 指派給該使用者的所有角色的權限
- 使用者所屬的所有安全群組的權限
- 指派給使用者所屬安全群組的所有角色的權限

如果至少一個權限集對權限**拒絕**，那麼使用者被拒絕該權限，即便其他集允許它或保持未定義。

您也可以將使用者和安全群組新增至使用者角色的範圍以使用管理伺服器的不同功能。與使用者角色關聯的設定將僅套用到屬於該角色使用者的裝置，以及僅在這些裝置屬於與該角色關聯的群組（包括子群組）時。

新增內部使用者帳戶

要新增新內部使用者帳戶到卡巴斯基安全管理中心：

1. 在主功能表中，轉至 **使用者和角色 → 使用者**。
2. 點擊**新增**。

3. 在開啟的**新實體**視窗，指定新使用者帳戶設定：

   - 保留預設選項 **使用者**。
   - **名稱**。
   - 連線到卡巴斯基安全管理中心的使用者**密碼**。
     密碼必須符合以下規則：
     - 密碼必須是 8 到 16 位字元長度。
     - 密碼必須包含以下組中三組的字元：
       - 大寫字母 (A-Z)
       - 小寫字母 (a-z)
       - 數字 (0-9)
       - 特殊字元 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - 密碼不可以包含任何空白、Unicode 字元或 "." 和「@」的組合，並且「@」前不可有「.」。

     若要檢視您輸入的字元，請按住**顯示**按鈕。

     > 輸入密碼的嘗試次數有限。預設下，允許的最大密碼輸入嘗試次數是 10。您可以管理允許的密碼輸入嘗試次數，敘述在"變更允許的密碼輸入嘗試次數"。

     > 如果使用者輸入無效的密碼指定次數，使用者被鎖定一小時。您僅可以透過變更密碼解鎖封鎖使用者。

   - **完整名稱**
   - **敘述**
   - **郵件信箱**
   - **電話**

4. 點擊**確定**儲存變更。

新使用者帳戶出現在使用者和安全群組清單。

建立安全群組

要建立安全群組：

1. 在主功能表中，轉至 **使用者和角色 → 使用者**。
2. 點擊**新增**。

3. 在開啟的**新實體**視窗中，選取**群組**。

4. 為新安全群組指定以下設定：

   - **群組名稱**
   - **敘述**

5. 點擊**確定**儲存變更。

新安全群組出現在使用者和安全群組清單。

編輯內部使用者帳戶

要在卡巴斯基安全管理中心中編輯內部使用者帳戶：

1. 在主功能表中，轉至 **使用者和角色 → 使用者**。

2. 點擊您要編輯的使用者帳戶名稱。

3. 在開啟的使用者設定視窗中的**一般**頁籤，變更使用者帳戶設定：

   - **敘述**
   - **完整名稱**
   - **郵件信箱**
   - **主電話**
   - 為連線到卡巴斯基安全管理中心的使用者**設定新密碼**。
     密碼必須符合以下規則：
     - 密碼必須是 8 到 256 位字元長度。
     - 密碼必須包含以下組中三組的字元：
       - 大寫字母 (A-Z)
       - 小寫字母 (a-z)
       - 數字 (0-9)
       - 特殊字元 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - 密碼不可以包含任何空白、Unicode 字元或 ":" 和「@」的組合，並且「@」前不可有「.」。

     要檢視輸入的密碼，點擊並按住**顯示**按鈕。

     > 輸入密碼的嘗試次數有限。預設下，允許的最大密碼輸入嘗試次數是 10。您可以變更允許的嘗試次數；但是，出於安全原因，我們不建議您減少此數字。如果使用者輸入無效的密碼指定次數，使用者被鎖定一小時。您僅可以透過變更密碼解鎖封鎖使用者。

   - 如有必要，請切換開關按鈕至**已停用**，以禁止使用者連線到應用程式。您可以停用帳戶，例如，在員工離職後。

4. 在**驗證安全性**頁籤中，您可以指定此帳戶的安全設定。

5. 在**群組**頁籤，您可新增使用者至安全群組。

6. 在**裝置**頁籤，您可指派裝置給使用者。

7. 在**角色**頁籤，您可指派角色給使用者。

8. 點擊**儲存**以儲存變更。

更新的使用者帳戶出現在使用者和安全群組清單。

編輯安全群組

> 您僅可以編輯內部群組。

要編輯安全群組：

1. 在主功能表中，轉至 **使用者和角色 → 使用者**。
2. 點擊您要編輯的安全群組名稱。
3. 在開啟的群組設定視窗中，變更安全群組設定：
   - **名稱**
   - **敘述**
4. 點擊**儲存**以儲存變更。

更新的安全群組出現在使用者和安全群組清單。

新增使用者帳戶到內部群組

您僅可以新增內部使用者帳戶到內部群組。

要新增使用者帳戶到內部群組：

1. 在主功能表中，轉至 **使用者和角色 → 使用者**。
2. 選取您要新增到群組的使用者帳戶旁邊的核取方塊。
3. 點擊**分配群組**按鈕。
4. 在開啟的**分配群組**視窗中，選取您要新增使用者帳戶的群組。
5. 點擊**分配**按鈕。

使用者帳戶被新增到群組。

指派使用者作為裝置所有者

有關指派使用者為行動裝置擁有者的資訊，請參閱Kaspersky Security for Mobile 說明。

要指派使用者作為裝置所有者：

1. 如果要指派連線到虛擬管理伺服器的裝置所有者，請先切換到虛擬管理伺服器：
   a. 在主功能表中，按一下目前管理伺服器名稱右側的 v 形箭號圖示（ ）。
   b. 選取所需的管理伺服器。
2. 在主功能表中，轉至 **使用者和角色 → 使用者**。
   使用者清單開啟。如果您目前已連線到虛擬管理伺服器，該清單會包括來自目前虛擬管理伺服器和主管理伺服器的使用者。
3. 按一下您要指派為裝置所有者的使用者帳戶名稱。
4. 在開啟的使用者設定視窗中，選擇**裝置**頁籤。
5. 點擊**新增**。
6. 從裝置清單中，選取您要分配給使用者的裝置。
7. 點擊**確定**。

所選的裝置被新增到分配給使用者的裝置清單。

您可在**裝置 → 受管理裝置**執行相同操作，方法是點擊您要指派之裝置的名稱，之後點擊**管理裝置所有者**連結。

刪除使用者或安全群組

您僅可以刪除內部使用者或內部安全群組。

要刪除使用者或安全群組：

1. 在主功能表中，轉至 **使用者和角色 → 使用者**。
2. 選取您要刪除的使用者或安全群組旁邊的核取方塊。
3. 點擊**刪除**。
4. 在開啟的視窗中，點擊**確定**。

使用者或安全群組被刪除。

建立使用者角色

要建立使用者角色：

1. 在主功能表中，轉至 **使用者和角色 → 角色**。
2. 點擊**新增**。
3. 在開啟的**新角色名稱**視窗中，輸入新角色的名稱。
4. 點擊**確定**以套用變更。
5. 在開啟的角色內容視窗中，變更角色設定：
   - 在**一般**頁籤，編輯角色名稱。
     您無法編輯預定義角色名稱。
   - 在**設定**頁籤，編輯角色範圍和政策以及與角色相關的設定檔。
   - 在**存取權限**頁籤，編輯存取 Kaspersky 應用程式的權限。
6. 點擊**儲存**以儲存變更。

新角色出現在使用者角色清單。

編輯使用者角色

要編輯使用者角色：

1. 在主功能表中，轉至 **使用者和角色 → 角色**。
2. 點擊您要編輯的角色名稱。
3. 在開啟的角色內容視窗中，變更角色設定：
   - 在**一般**頁籤，編輯角色名稱。
     您無法編輯預定義角色名稱。
   - 在**設定**頁籤，編輯角色範圍和政策以及與角色相關的設定檔。
   - 在**存取權限**頁籤，編輯存取 Kaspersky 應用程式的權限。
4. 點擊**儲存**以儲存變更。

更新的角色出現在使用者角色清單。

編輯使用者角色範圍

*使用者角色範圍*是使用者和管理群組的組合。與使用者角色關聯的設定僅套用到屬於該角色使用者的裝置，以及僅在這些裝置屬於與該角色關聯的群組（包括子群組）時。

要新增使用者、安全群組和管理群組到使用者角色範圍，您可以使用以下其中一種方法：

方法 1：

1. 在主功能表中，轉至 **使用者和角色** → **使用者**。
2. 選取您要新增到使用者角色範圍的使用者和安全群組旁邊的核取方塊。
3. 點擊**分配角色**按鈕。
   角色分配精靈啟動。使用**下一步**按鈕進行精靈。
4. 在**選擇角色**步驟，選取您要指派的使用者角色。
5. 在**定義範圍**步驟，選取您要新增至使用者角色範圍的管理群組。
6. 點擊**分配角色**按鈕以關閉視窗。

所選使用者或安全群組和所選管理群組被新增到使用者角色範圍。

方法 2：

1. 在主功能表中，轉至 **使用者和角色** → **角色**。
2. 按一下您要定義範圍的角色名稱。
3. 在開啟的角色內容頁面中，選擇**設定**頁籤。
4. 在**角色範圍**區段中，點擊**新增**。
   角色分配精靈啟動。使用**下一步**按鈕進行精靈。
5. 在**定義範圍**步驟，選取您要新增至使用者角色範圍的管理群組。
6. 在**選取使用者**步驟，選取您要新增到使用者角色範圍的使用者和安全群組。
7. 點擊**分配角色**按鈕以關閉視窗。
8. 按一下**關閉**按鈕 (⨯) 以關閉角色內容視窗。

所選使用者或安全群組和所選管理群組被新增到使用者角色範圍。

方法 3：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。

   管理伺服器內容視窗將開啟。

2. 在"**存取權限**"頁簽上，選中要新增到使用者角色範圍的使用者或安全群組名稱旁邊的核取方塊，然後點擊"**角色**"按鈕。

   您不能同時選擇多個使用者或安全群組。如果您選擇了多個項目，**角色**按鈕將被停用。

3. 在**角色**視窗中，選擇要指派的使用者角色，然後點擊**確定**並儲存變更。

   所選使用者或安全群組被新增到使用者角色範圍。

刪除使用者角色

要刪除使用者角色：

1. 在主功能表中，轉至 **使用者和角色 → 角色**。
2. 選取您要刪除的角色旁邊的核取方塊。
3. 點擊**刪除**。
4. 在開啟的視窗中，點擊**確定**。

使用者角色被刪除。

關聯政策設定檔到角色

您可以關聯使用者角色到政策設定檔。此種情況下，該政策設定檔的啟動規則基於角色：政策設定檔對具有指定角色的使用者可用。

例如，政策禁止在管理群組的所有裝置上執行 GPS 導航軟體。GPS 導航軟體僅在"使用者"管理群組中的單個裝置上是必須的——該裝置屬於導遊。此種情況下，您可以分配"導遊"角色給其所有者，然後建立一個政策設定檔，允許 GPS 導航軟體僅在分配了"導遊"角色的使用者的裝置上執行。所有其他政策設定被保留。僅帶有"導遊"角色的使用者將被允許執行 GPS 導航軟體。然後，如果其他員工被分配了"導遊"角色，該新員工也在組織的裝置上執行導航軟體。執行 GPS 導航軟體在相同管理群組的其他裝置上仍將被禁止。

要關聯角色到政策設定檔：

1. 在主功能表中，轉至 **使用者和角色 → 角色**。
2. 選取您要關聯政策設定檔的角色名稱。

   角色內容視窗會開啟，並含有所選的**一般**頁籤。

3. 選取**設定**頁籤，之後向下捲動至**政策和設定檔**區段。
4. 點擊**編輯**。

5. 要關聯角色到：

- **現有政策設定檔**—點擊所學政策名稱旁邊的臂章圖示（ ）），然後選取您要關聯角色的設定檔旁邊的核取方塊。
- **新政策設定檔**：
  a. 選取您要建立設定檔的政策旁邊的核取方塊。
  b. 點擊**新政策設定檔**。
  c. 為新設定檔指定名稱並配置設定檔設定。
  d. 點擊**儲存**按鈕。
  e. 選取新設定檔旁邊的核取方塊。

6. 點擊**分配到角色**。

設定檔被關聯到角色並顯示在角色內容中。設定檔自動應用到分配了該角色的使用者的任意裝置。

傳輸使用者角色到從屬管理伺服器

預設下，主要和從屬管理伺服器的使用者角色清單都是獨立的。您可以設定應用程式自動傳輸在主管理伺服器上建立的使用者角色到所有從屬管理伺服器。使用者角色也可以從從屬管理伺服器傳輸到其自己的從屬管理伺服器。

若要從主管理伺服器傳輸使用者角色到從屬管理伺服器，請執行以下操作：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗會開啟，並含有所選的**一般**頁籤。
2. 前往**管理伺服器階層**區域。
3. 啟用**將角色清單轉發到從屬管理伺服器**選項，然後點擊**儲存**按鈕。

應用程式從主管理伺服器複製使用者角色到從屬管理伺服器。

當**將角色清單轉發到從屬管理伺服器**選項被啟用且使用者角色被傳輸時，它們不能在從屬管理伺服器上被編輯或刪除。當您建立新角色或在主管理伺服器上編輯現有角色時，變更被自動複製到從屬管理伺服器。當您在主管理伺服器上刪除使用者角色時，該角色在從屬管理伺服器上被保留，但無法被編輯或刪除。

從主管理伺服器傳播到從屬管理伺服器的角色用綠色勾號標記（ ）顯示。您無法在從屬管理伺服器上編輯這些角色。

如果您在主管理伺服器上建立角色，且在從屬管理伺服器上有相同名稱的角色，新角色被複製到從屬管理伺服器，其名稱後被新增索引，例如，~~1、~~2（索引可以隨機）。

如果您停用**將角色清單轉發到從屬管理伺服器**選項，所有使用者角色在從屬管理伺服器上被保留，但是獨立於主管理伺服器上的角色。變成獨立角色後，從屬管理伺服器上的使用者角色就可以被編輯或刪除。

在卡巴斯基安全管理中心網頁主控台中管理物件

該區域包含了物件修訂管理的資訊。卡巴斯基安全管理中心允許您跟蹤物件修改。您每次儲存變更到物件時，*修訂*被建立。每個修訂都有一個數字。

支援修訂管理的應用程式物件包括：

- 管理伺服器內容
- 政策
- 工作
- 管理群組
- 使用者帳戶
- 安裝套件

您可以檢視修訂清單並將對物件所做的變更回溯到選取的修訂。

在支援修訂管理的任何物件的內容視窗中，**變更歷程**區域會顯示含有以下詳情的物件修訂清單：

- **修訂** — 物件修訂版本。
- **時間** — 物件修改的日期和時間。
- **使用者** — 修改物件的使用者的名稱。
- **操作** — 對物件執行的操作。
- **敘述** — 與物件設定變更相關的修訂敘述。

  預設下，物件修訂敘述為空。若要為某次修訂新增說明，請選取該修訂，然後點擊**編輯描述**按鈕。在開啟的視窗中，輸入修訂敘述的部分文字。

新增修訂敘述

卡巴斯基安全管理中心允許您跟蹤物件修改。您每次儲存變更到物件時，修訂被建立。每個修訂都有一個數字。

您可以為修訂新增敘述以簡化在清單中的修訂搜尋。

要新增修訂敘述：

1. 在物件的內容視窗中，開啟**變更歷程**頁籤。
2. 在物件修訂清單中，選取您想要新增敘述的修訂。
3. 點擊**編輯描述**按鈕。

   敘述視窗開啟。

4. 在**敘述**視窗，輸入修訂敘述的部分文字。

   預設下，物件修訂敘述為空。

5. 儲存修訂描述。

為物件的修訂新增了描述。

物件刪除

本節提供有關刪除物件的資訊。

您可以刪除物件，包括以下：

- 政策
- 工作
- 安裝套件
- 虛擬管理伺服器
- 使用者
- 安全群組
- 管理群組

要刪除物件：

1. 開啟卡巴斯基安全管理中心網頁主控台的所需部分，然後選取物件。
2. 在工具列上，點擊**刪除**按鈕。
3. 在開啟的視窗中，點擊**確定**按鈕以確認您的選取。

   所選物件被刪除。

當您刪除物件時，其資訊保留在資料庫。已刪除物件的資訊的儲存期與物件修訂的儲存期一致（建議期限是 90 天）。只有當您在權限的**已刪除物件**區域有**修改**權限時才可變更儲存期。

關於刪除用戶端裝置

當您從管理群組中刪除受管理裝置時，應用程式會將裝置移至未分配的裝置群組。然後選取您需要執行測試更新安裝的裝置刪除裝置後，已安裝的卡巴斯基應用程式——網路代理和任何安全應用程式，例如 Kaspersky Endpoint Security ——將保留在裝置上。

卡巴斯基安全管理中心根據以下規則處理未分配裝置群組中的裝置：

- 如果您配置了裝置移動規則，並且裝置符合移動規則的條件，則該裝置會被根據規則自動移動到管理群組。
- 裝置會被儲存在未分配的裝置群組中，並被根據裝置保留規則自動從群組中刪除。

  裝置保留規則不會影響具有一個或多個使用完整磁碟加密進行加密的磁碟機的裝置。此類裝置不會被自動刪除——您只能手動刪除它們。如果您需要刪除帶有加密磁碟機的裝置，請先解密磁碟機，然後再刪除該裝置。

  > 當您刪除帶有加密磁碟機的裝置時，解密磁碟機所需的資料也會被刪除。如果您在刪除此類裝置（不論是從**未配置的裝置**或**受管理裝置**群組）時開啟的確認視窗中選取**我了解風險並希望刪除所選裝置**核取方塊，則表示您已知悉後續會有資料被刪除。

  想解密磁碟機，必須滿足以下條件：

  - 裝置被重新連線到管理伺服器以還原解密磁碟機所需的資料。
  - 裝置使用者記得解密密碼。
  - 用於加密磁碟機的安全應用程式（例如 Kaspersky Endpoint Security for Windows）仍安裝在裝置上。

  如果磁碟機由 Kaspersky Disk Encryption 技術加密，您還可以嘗試使用 FDERT Restore Utility 還原資料.

> 在 VDI 中，如果您的裝置有加密磁碟機，則刪除該裝置後，加密磁碟機上的資訊也會被刪除。

當您從未分配的裝置群組中手動刪除裝置時，應用程式會從清單中刪除該裝置。刪除裝置後，已安裝的卡巴斯基應用程式（如果有）將保留在裝置上。然後，如果該裝置對管理伺服器仍然可見並且您配置了常規網路輪詢，卡巴斯基安全管理中心會在網路輪詢期間發現該裝置並將其新增回未分配的裝置群組。因此，最好僅當裝置對管理伺服器不可見時再手動刪除該裝置。

卡巴斯基安全網路 (KSN)

該區域敘述如何使用卡巴斯基安全網路 (KSN) 的線上服務基礎架構。該區域提供了關於 KSN 的詳細敘述，介紹了如何啟用 KSN，設定對 KSN 的存取，並檢視 KSN 代理伺服器的使用統計。

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

關於 KSN

卡巴斯基安全網路 (KSN) 是一種線上服務組織結構，可提供對 Kaspersky 網路知識庫的存取，其中包含與檔案信譽、網路資源和軟體相關的資訊。使用卡巴斯基安全網路中的資料可確保在遇到未知威脅時 Kaspersky 程式能夠做出更快速的回應，提高某些防護元件的效能可降低誤報的風險。KSN 允許您使用 Kaspersky 的信譽資料庫檢索有關安裝在受管理裝置上的應用程式資訊。

卡巴斯基安全管理中心支援以下 KSN 基礎架構解決方案：

- *全球 KSN* 是一種允許您與卡巴斯基安全網路交換資訊的解決方案。只要加入 KSN，即表示您同意以自動模式將透過卡巴斯基安全管理中心管理的用戶端裝置上安裝的 Kaspersky 應用程式的相關操作資訊傳送到 Kaspersky。依照目前 KSN 存取設定傳送資訊。卡巴斯基分析師會另外分析收到的資訊，並將其包含在卡巴斯基安全網路的信譽和統計資料庫中。卡巴斯基安全管理中心預設使用此解決方案。

- *私有 KSN* 是一種解決方案，可讓已安裝卡巴斯基應用程式的裝置使用者存取卡巴斯基安全網路的信譽資料庫和其他統計資料，而不必從自己的電腦傳送資料給 KSN。卡巴斯基私人安全網路（私有 KSN）專門用於由於以下原因無法參與卡巴斯基安全網路的企業客戶：

  - 使用者裝置未連線到網際網路。

  - 法律禁止或企業安全政策限制傳輸任何資料到國家/地區以外或企業區域網路以外。

  您可以在管理伺服器內容視窗的**KSN 代理設定**區段中，設定卡巴斯基私人安全網路的存取設定。

在執行快速啟動精靈時，應用程式會提示您加入 KSN。您可以在使用應用程式的任何時間啟用或者停止 KSN。

啟用 KSN 時，應根據閱讀與接受的 KSN 聲明啟用 KSN。如果 KSN 聲明已更新，則在更新或升級管理伺服器時會顯示給您。您可以接受更新的 KSN 聲明，也可以拒絕。如果您拒絕了它，那麼您將按照之前接受的 KSN 聲明的先前版本繼續使用 KSN。

啟用 KSN 後，卡巴斯基安全管理中心會檢查 KSN 伺服器是否可存取。如果無法使用系統 DNS 存取伺服器，則應用程式使用公用 DNS 伺服器。這是為了確保維護受管理裝置的安全級別。

管理伺服器管理的用戶端裝置透過 KSN 代理伺服器與 KSN 互動。KSN 代理伺服器提供以下功能：

- 即使無法直接連線網際網路，用戶端裝置也可向 KSN 傳送請求以及向 KSN 傳送資訊。

- KSN 代理可暫存已處理的資料，進而減少對外頻寬消耗以及用戶端裝置等待 KSN 回覆而花費的時間。

您可以在管理伺服器內容視窗的**KSN 代理設定**區域中設定 KSN 代理伺服器。

設定對 KSN 的存取

您可以在管理伺服器和發佈點上設定到卡巴斯基安全網路 (KSN) 的存取。

要設定管理伺服器到 KSN 的存取：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。

   管理伺服器內容視窗將開啟。

2. 在**一般**標籤上，選取**KSN 代理設定**區段。

3. 將切換按鈕切換到**在管理伺服器上啟用 KSN 代理 已啟用**位置。

   資料被從用戶端裝置傳送到 KSN，與在這些用戶端裝置上活動的 Kaspersky Endpoint Security 政策一致。如果清除此方塊，資料不會透過卡巴斯基安全管理中心從管理伺服器以及用戶端裝置傳送到 KSN。但是，用戶端裝置能夠根據其設定直接將資料傳送到 KSN（繞過卡巴斯基安全管理中心）。Kaspersky Endpoint Security 政策會在用戶端裝置上啟用，判定哪些資料要從哪些裝置傳送至 KSN（繞過卡巴斯基安全管理中心）。

4. 將切換按鈕切換到**使用卡巴斯基安全網路 已啟用**位置。

   如果啟用了此選項，用戶端裝置將傳送修補程式安裝結果到 Kaspersky。啟用此選項時，請確保閱讀並接受 KSN 聲明的條款。

   如果您正使用私有 KSN，將切換按鈕切換到**使用卡巴斯基私人安全網路 已啟用**位置並點擊**選取 KSN 代理設定檔**按鈕以下載私有 KSN 設定（帶有 pkcs7 和 pem 副檔名的檔案）。下載完設定之後，介面會顯示提供商的名稱和聯絡人，以及私有 KSN 設定檔的建立日期。

   當您啟用私有 KSN，請注意設定用來直接傳送 KSN 要求至雲端 KSN 的分佈點。已安裝網路代理版本 11（或更早版本）的分佈點會繼續傳送 KSN 要求至雲端 KSN。若要重新設定分佈點來傳送 KSN 要求至私有 KSN，請為每個分佈點啟用**轉發 KSN 請求到管理伺服器**選項。您可在發佈點內容或網路代理政策中啟用此選項。

   當您將切換按鈕切換到**使用卡巴斯基私人安全網路 已啟用**位置，將顯示一則含有有關私有 KSN 詳細資料的訊息。

   以下 Kaspersky 應用程式支援私有 KSN：

   - 卡巴斯基安全管理中心
   - Kaspersky Endpoint Security for Windows
   - Kaspersky Endpoint Security for Linux
   - Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2
   - Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent

   如果您在卡巴斯基安全管理中心啟用私有 KSN，這些應用程式會接收支援私有 KSN 的相關資訊。在應用程式設定視窗，在**進階威脅防護**區域的**卡巴斯基安全網路**子區域中，**KSN 提供者：私有 KSN** 被顯示。否則，**KSN 提供者：全域 KSN** 被顯示。

   如果您使用的應用程式版本早於 Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 或早於 Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent，在您執行私人 KSN 時，我們建議您使用未啟用私人 KSN 使用的從屬管理伺服器。

   卡巴斯基安全管理中心不傳送任何統計資料到卡巴斯基安全網路，如果在管理伺服器內容視窗的 **KSN 代理設定**區域設定了私有 KSN。

5. 若您已在管理伺服器內容中設定代理伺服器設定，但您的網路架構要求您直接使用私有 KSN，請啟用**當連線到私有 KSN 時略過代理伺服器設定**選項。否則，從受管理應用程式的請求無法到達私有 KSN。

6. 設定管理伺服器到 KSN 代理服務的連線：

   - 在**連線設定**下的**TCP 連接埠**中，指定用於連線到 KSN 代理的 TCP 埠號。連線到 KSN 代理伺服器的預設連接埠是 13111。
   - 如果您要讓管理伺服器透過 UDP 連接埠連線到 KSN 代理，啟用**使用 UDP 連接埠**選項，並在**UDP 連接埠**欄位中指定埠號。預設下，會停用此選項，並使用 TCP 連接埠。若啟用此選項，則 UDP 埠號 15111 預設會用來連線到 KSN 代理伺服器。
   - 如果您要讓管理伺服器透過 HTTPS 連接埠連線到 KSN 代理伺服器，請啟用**使用 HTTPS** 選項，並在 **透過連接埠使用 HTTPS**中指定埠號。預設下，會停用此選項，並使用 TCP 連接埠。若啟用此選項，則 HTTPS 埠號 17111 預設會用來連線到 KSN 代理伺服器。

7. 將切換按鈕切換到**透過主管理伺服器將從屬管理伺服器連線到 KSN 已啟用**位置 。

   如果啟用此選項，從屬管理伺服器使用主管理伺服器作為 KSN 代理伺服器。如果停用此選項，從屬管理伺服器會自己連線到 KSN。該情況下，受管理裝置使用從屬管理伺服器作為 KSN 代理伺服器。

   如果在**KSN 代理設定**區段的右側面板中，從屬管理伺服器內容的切換按鈕是切換到**在管理伺服器上啟用 KSN 代理 已啟用**位置，則從屬管理伺服器會使用主管理伺服器作為代理伺服器。

8. 點擊**儲存**按鈕。

KSN 存取設定將被儲存。

您也可以設定發佈點存取 KSN，例如，如果您想降低管理伺服器負載。作為 KSN 代理伺服器的發佈點從受管理裝置直接傳送 KSN 請求到 Kaspersky，不使用管理伺服器。

要設定發佈點到卡巴斯基安全網路 (KSN) 的存取：

1. 確保發佈點是手動分配。
2. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。

   管理伺服器內容視窗將開啟。
3. 在**一般**頁籤，選取**發佈點**區段。
4. 按一下發佈點的名稱以開啟工作內容視窗。
5. 在發佈點內容視窗中的**KSN 代理**區段，啟用**在發佈點端啟用 KSN 代理**選項，然後啟用**透過網際網路直接存取 KSN 雲端 / 私有 KSN**選項。
6. 點擊**確定**。

該發佈點將作為 KSN 代理伺服器。

啟用和停用 KSN

要啟用 KSN：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**標籤上，選取**KSN 代理設定**區段。
3. 將切換按鈕切換到**在管理伺服器上啟用 KSN 代理 已啟用**位置。
   KSN 代理伺服器將被啟用。
4. 將切換按鈕切換到**使用卡巴斯基安全網路 已啟用**位置。
   KSN 將被啟用。
   如果啟用了此切換按鈕，用戶端裝置將傳送修補程式安裝結果到卡巴斯基。啟用此切換按鈕時，您應閱讀並接受 KSN 聲明的條款。
5. 點擊**儲存**按鈕。

要停用 KSN：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**標籤上，選取**KSN 代理設定**區段。
3. 將切換按鈕切換到**在管理伺服器上啟用 KSN 代理 已停用**位置以停用 KSN 代理服務，或將切換按鈕切換到**使用卡巴斯基安全網路 已停用**位置。
   如果停用其中一個切換按鈕，用戶端裝置將不會傳送修補程式安裝結果到卡巴斯基。
   如果您使用的是私有 KSN，請將切換按鈕切換到**使用卡巴斯基私人安全網路 已停用**位置。
   KSN 將被停用。
4. 點擊**儲存**按鈕。

檢視接受的 KSN 聲明

啟用卡巴斯基安全網路 (KSN) 時，必須閱讀並接受 KSN 聲明。您可以隨時檢視已接受的 KSN 聲明。

若要檢視已接受的 KSN 聲明：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**標籤上，選取**KSN 代理設定**區段。
3. 點擊**檢視卡巴斯基安全網路聲明**連接。

在開啟的視窗中，您可以檢視接受的 KSN 聲明的文字。

接受更新的 KSN 聲明

啟用 KSN 時，應根據閱讀與接受的 KSN 聲明啟用 KSN。如果 KSN 聲明已更新，則在升級管理伺服器時會顯示給您。您可以接受更新的 KSN 聲明，也可以拒絕。如果您拒絕了它，那麼您將按照之前接受的 KSN 聲明的版本繼續使用 KSN。

升級管理伺服器版本後，會自動顯示更新的 KSN 聲明。如果您拒絕更新的 KSN 聲明，則以後仍然可以檢視並接受它。

要檢視然後接受或拒絕更新的 KSN 聲明，請執行以下操作：

1. 點擊**檢視通知**主應用程式視窗右上角的連結。

   通知 視窗隨即開啟。

2. 點擊**檢視更新的 KSN 聲明**連結。

   卡巴斯基安全網路聲明更新視窗開啟。

3. 閱讀 KSN 聲明，然後透過按一下以下其中一個按鈕做出決定：

   - **我接受更新的 KSN 聲明**
   - **在舊聲明下使用 KSN**

   根據您的選擇，KSN 會按照目前或更新的 KSN 聲明條款繼續有效。您可以隨時在管理伺服器屬性中檢視已接受的 KSN 聲明文字。

檢查發佈點是否作為 KSN 代理伺服器運作

在分配作為發佈點運作的受管理裝置上，可以啟用 KSN 代理伺服器。當 ksnproxy 服務在裝置上執行時，受管理裝置會作為 KSN 代理伺服器運作。您可以在本機裝置上檢查、開啟或關閉此服務。

您可以將基於 Windows 或基於 Linux 的裝置分配為發佈點。檢查發佈點的方法取決於該發佈點的作業系統。

若要檢查基於 Windows 的發佈點是否作為 KSN 代理伺服器運作，請執行以下操作：

1. 在發佈點裝置上的 Windows 系統中，開啟**服務**（**所有程序 → 管理工具 → 服務**）。

2. 在服務清單，檢查 ksnproxy 服務是否正在執行。

   如果 ksnproxy 服務正在執行，則裝置上的網路代理會加入卡巴斯基安全網路，並作為發佈點範圍內所管理裝置的 KSN 代理伺服器運作。

   如果您想，您可以關閉 ksnproxy 服務。在這種情況下，發佈點上的網路代理停止參與卡巴斯基安全網路。該需要本機管理員權限。

若要檢查基於 Linux 的發佈點是否作為 KSN 代理伺服器運作，請執行以下操作：

1. 在發佈點裝置上，顯示正在執行的處理程序清單。

2. 在正在執行的處理程序清單中，檢查 `/opt/kaspersky/ksc64/sbin/ksnproxy` 處理程序是否正在執行。

如果 `/opt/kaspersky/ksc64/sbin/ksnproxy` 處理程序正在執行，則裝置上的網路代理會加入卡巴斯基安全網路，並作為發佈點範圍內所管理裝置的 KSN 代理伺服器運作。

更新 Kaspersky 資料庫和應用程式

該部分敘述了定期更新以下內容必須採取的步驟：

- 卡巴斯基資料庫和軟體模組
- 已安裝的 Kaspersky 應用程式，包括卡巴斯基安全管理中心元件和安全應用程式

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

情境：定期更新 Kaspersky 資料庫與應用程式

該部分提供了定期更新 Kaspersky 資料庫、軟體模組和應用程式的情境。完成設定網路防護情境後，您必須維持防護系統的可靠性，確保管理伺服器和受管理裝置受到多種威脅的防護，包含病毒、網路攻擊與釣魚攻擊。

網路防護透過更新以下內容保持最新：

- 卡巴斯基資料庫和軟體模組
- 已安裝的 Kaspersky 應用程式，包括卡巴斯基安全管理中心元件和安全應用程式

當您完成此情境，您可確保以下事項：

- 您的網路被最近的 Kaspersky 軟體防護，包括卡巴斯基安全管理中心元件和安全應用程式。
- 對網路安全關鍵的病毒資料庫和其他 Kaspersky 資料庫保持最新。

先決條件

受管理裝置必須有與管理伺服器的連線。若沒有連線，請考慮手動更新 Kaspersky 資料庫、軟體模組與應用程式，或直接從 Kaspersky 更新伺服器更新。

管理伺服器必須具有到網際網路的連線。

在您開始之前，確保您已做了如下：

1. 根據透過卡巴斯基安全管理中心網頁主控台佈署 Kaspersky 應用程式的情境佈署 Kaspersky 安全應用程式到受管理裝置。
2. 建立了配置了所有所需政策、政策設定檔和工作，根據網路防護配置情境。
3. 分配了適當數量的發佈點，與受管理裝置和網路拓撲一致。

更新 Kaspersky 資料庫和應用程式分步驟進行：

1. **選取更新方案**

   您可使用多種方案為卡巴斯基安全管理中心元件和安全應用程式安裝更新。選取一個或多個滿足您網路需求的方案。

2. **建立管理伺服器的「將更新下載至儲存區」工作**

   該工作由卡巴斯基安全管理中心快速啟動精靈自動建立。如果您未執行精靈，立即建立工作。

   需要該工作以從 Kaspersky 更新伺服器下載更新到管理伺服器儲存區，以及為卡巴斯基安全管理中心更新 Kaspersky 資料庫和軟體模組。更新被下載後，它們可以被傳播到受管理裝置。

   如果您的網路被分配了發佈點，更新被從管理伺服器儲存區自動下載到發佈點儲存區。此種情況下，發佈點所在範圍的受管理裝置從發佈點儲存區下載更新，而不是從管理伺服器儲存區。

   說明：

   - 管理主控台：建立管理伺服器的「將更新下載至儲存區」工作
   - 卡巴斯基安全管理中心網頁主控台：建立管理伺服器的「將更新下載至儲存區」工作

3. **建立「將更新下載至發佈點儲存區」工作（可選）**

   預設下，更新被從管理伺服器下載到發佈點。您可以配置卡巴斯基安全管理中心直接從 Kaspersky 更新伺服器下載更新到發佈點。您可以下載到發佈點儲存區，例如，如果管理伺服器和發佈點之間的流量比發佈點和 Kaspersky 更新伺服器之間的流量貴，或者如果您的管理伺服器沒有網際網路存取。

   當您的網路獲得指派的發佈點並且建立了*將更新下載至發佈點儲存區*工作後，發佈點會從 Kaspersky 更新伺服器下載更新，而非管理伺服器儲存區。

   說明：

   - 管理主控台：建立「將更新下載至發佈點儲存區」工作
   - 卡巴斯基安全管理中心網頁主控台：建立「將更新下載至發佈點儲存區」工作

4. **配置發佈點**

   當您的網路有指派的發佈點時，請確保**佈署更新**選項已在所有必要發佈點中啟用。當該選項對發佈點停用時，包含在發佈點範圍中的裝置從管理伺服器儲存區下載更新。

   若您要受管理裝置僅從發佈點接收更新，請啟用網路代理政策的**僅透過發佈點分發檔案**選項。

5. **使用行動模式更新下載或 diff 檔案最佳化更新程序（選用）**

   您可以透過使用行動模式更新下載（預設啟用）或使用 diff 檔案最佳化更新過程。對於每個網路段，您必須選取應用哪個功能，因為它們無法同時工作。

   當行動模式更新下載被啟用時，一旦更新被下載到管理伺服器儲存區，在安全應用程式請求更新之前，網路代理就下載所需更新到受管理裝置。這確保了更新過程的可靠性。若要使用此功能，請啟用網路代理政策中的**提前從管理伺服器下載更新和病毒資料庫（建議）**選項。

   如果您不使用行動模式更新下載，您透過使用 diff 檔案最佳化管理伺服器和受管理裝置之間的流量。當該功能被啟用時，管理伺服器或發佈點下載 diff 檔案，而不是整個 Kaspersky 資料庫或軟體模組檔案。diff 檔案敘述了資料庫或軟體模組的檔案的兩個版本之間的差異。因此，diff 檔案比整個檔案佔用更少的空間。這導致降低管理伺服器之間或發佈點和受管理裝置之間的流量。若要使用此功能，請啟用*將更新下載至管理伺服器儲存區*工作和/或*將更新下載至發佈點儲存區*工作內容中的**下載差異檔案**選項。

   說明：

   - 使用 diff 檔案更新 Kaspersky 資料庫和軟體模組
   - 管理主控台：啟用和停用行動模式更新下載
   - 卡巴斯基安全管理中心網頁主控台：啟用和停用行動模式更新下載

6 驗證已下載的更新（可選）

安裝下載的更新之前，您可以透過*更新驗證*工作驗證更新。該工作按順序執行透過測試裝置集的設定來配置的裝置更新工作和惡意軟體掃描工作。獲取工作結果時，管理伺服器開始或封鎖更新傳播到剩餘裝置。

*更新驗證*工作可作為「*將更新下載至管理伺服器儲存區*」工作的一部分執行。在「*將更新下載至管理伺服器儲存區*」工作的內容中，啟用管理主控台中的**發佈前驗證更新**選項，或卡巴斯基安全管理中心網頁主控台的**執行更新驗證**選項。

說明：

- 管理主控台：驗證下載的更新
- 卡巴斯基安全管理中心網頁主控台：驗證下載的更新

7 批准和拒絕軟體更新

預設下，下載的軟體更新具有*未定義*狀態。您可以變更狀態到*已批准*或*已拒絕*。批准的更新總是被安裝。如果更新需要檢視和接受最終使用者產品授權協議的條款，您需要先接受它們。此後，更新可以被傳播到受管理裝置。未定義的更新僅可以被安裝到網路代理和其他卡巴斯基安全管理中心元件，與網路代理政策設定一致。您設定了*已拒絕*狀態的更新將不被安裝到裝置。若先前安裝了安全應用程式的拒絕更新，卡巴斯基安全管理中心會嘗試從所有裝置解除安裝該更新。卡巴斯基安全管理中心元件更新無法被移除。

說明：

- 管理主控台：批准和拒絕軟體更新
- 卡巴斯基安全管理中心網頁主控台：批准和拒絕軟體更新

8 配置卡巴斯基安全管理中心元件的更新和修補程式的自動安裝

下載的網路代理更新和修補程式以及其他卡巴斯基安全管理中心元件被自動安裝。若您在網路代理內容中保持啟用**對未定義狀態的元件自動安裝可套用更新和修補程式**選項，則所有更新都會在下載至儲存區後自動安裝（或數個儲存區）。如果停用此選項，被下載和標注為*未定義*狀態的 Kaspersky 修補程式將僅在您改變其狀態為*已批准*是被安裝。

說明：

- 管理主控台：啟用和停用卡巴斯基安全管理中心元件的自動更新和修補程式
- 卡巴斯基安全管理中心網頁主控台：啟用和停用卡巴斯基安全管理中心元件的自動更新和修補程式

9 為管理伺服器安裝更新

管理伺服器軟體更新不取決於更新狀態。這些更新不會自動安裝，必須由管理員在管理主控台的**監控**頁籤（**管理伺服器** <伺服器名稱> → **監控**）或卡巴斯基安全管理中心網頁主控台中的**通知**區段（**監控和報告** → **通知**）進行初步核准。此後，管理員必須明確執行更新安裝。

10 為安全應用程式配置更新的自動安裝

為受管理應用程式建立*更新*工作，以提供對應用程式、軟體模組和 Kaspersky 資料庫（包括病毒資料庫）的及時更新。為了確保定期更新，建議您在配置工作排程時選取**當新更新下載至儲存區時**選項。

如果您的網路包括僅支援 IPv6 的裝置，並且您想要定期更新安裝在這些裝置上的安全應用程式，請確保管理伺服器（不早於 13.2 版）和網路代理（不早於 13.2 版）安裝在受管理裝置上。

預設下，Kaspersky Endpoint Security for Windows 和 Kaspersky Endpoint Security for Linux 的更新在您變更更新狀態到*已批准*後被安裝。您可以在*更新*工作中變更更新設定。

如果更新需要檢視和接受最終使用者產品授權協議的條款，您需要先接受它們。此後，更新可以被傳播到受管理裝置。

說明：

- 管理主控台：在裝置上自動安裝 Kaspersky Endpoint Security 更新
- 卡巴斯基安全管理中心網頁主控台：在裝置上自動安裝 Kaspersky Endpoint Security 更新

結果

當情境完成時，卡巴斯基安全管理中心被配置在更新被下載至管理伺服器儲存區或發佈點儲存區時更新 Kaspersky 資料庫和已安裝的 Kaspersky 應用程式。您然後可以繼續監控網路狀態。

關於更新 Kaspersky 資料庫、軟體模組和應用程式

為了確保管理伺服器和受管理裝置的防護是最新的，您必須提供以下內容的定期更新：

- 卡巴斯基資料庫和軟體模組

  在下載卡巴斯基資料庫和軟體模組之前，卡巴斯基安全管理中心會檢查卡巴斯基伺服器是否可以存取。如果無法使用系統 DNS 存取伺服器，則應用程式使用公用 DNS 伺服器。這是為了確保更新病毒資料庫並維護受管裝置的安全級別。

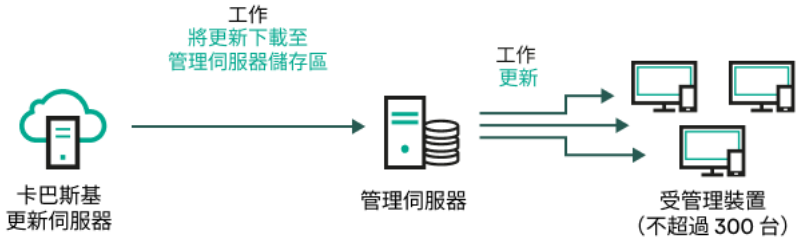
- 已安裝的 Kaspersky 應用程式，包括卡巴斯基安全管理中心元件和安全應用程式

取決於您網路的配置，您可以使用以下方案來下載和分發所需更新到受管理裝置：

- 通過使用單個工作：*將更新下載至管理伺服器儲存區*
- 透過使用兩個工作：
  - *將更新下載至管理伺服器儲存區*工作
  - *將更新下載至發佈點儲存區*工作
- 透過本機資料夾、共用資料夾或 FTP 伺服器手動。
- 直接從卡巴斯基更新伺服器到受管理裝置上的 Kaspersky Endpoint Security
- 如果管理伺服器沒有網際網路連線，則透過本機或網路資料夾

使用將更新下載至管理伺服器儲存區工作

在此方案中，卡巴斯基安全管理中心會透過*將更新下載至管理伺服器儲存區*工作下載更新。在單一網段包含少於 300 台受管理裝置或每個網段包含少於 10 台受管理裝置的小網路中，更新直接從管理伺服器儲存區被分發到受管理裝置（參見下圖）。

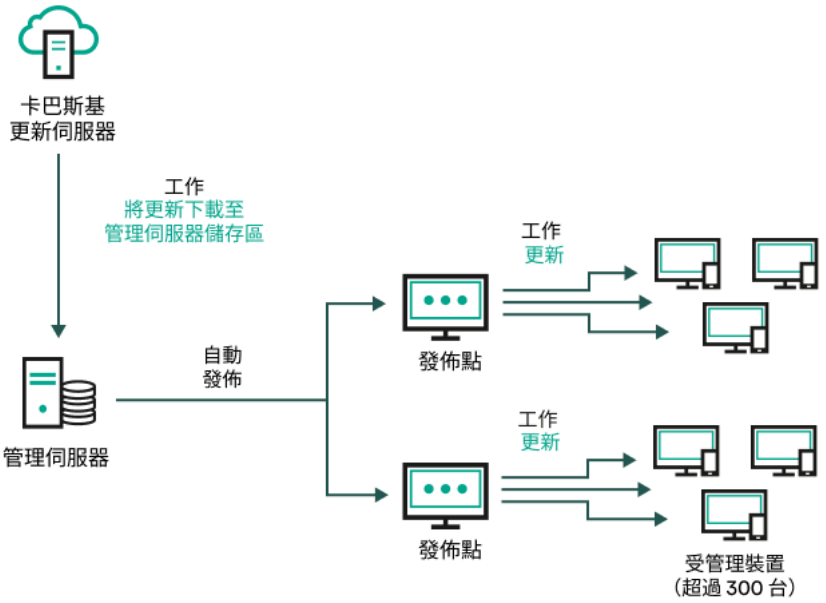


使用將更新下載至管理伺服器儲存區工作在沒有發佈點狀態下更新

預設下，管理伺服器與 Kaspersky 更新伺服器通訊並使用 HTTPS 協定下載更新。您可以配置管理伺服器使用 HTTP 協定，而不是 HTTPS。

如果您的網路中單一網段包含多於 300 台受管理裝置或每個網段包含多於 9 台受管理裝置，我們建議您使用發佈點傳播更新到受管理裝置（參見下圖）。發佈點降低管理伺服器負載並最佳化管理伺服器和受管理裝置之間的流量。您可以計算數字並配置您網路所需的發佈點。

此種方案中，更新被從管理伺服器儲存區自動下載到發佈點儲存區。發佈點所在範圍的受管理裝置從發佈點儲存區下載更新，而不是從管理伺服器儲存區。



使用將更新下載至管理伺服器儲存區工作在有發佈點狀態下更新

當*將更新下載至管理伺服器儲存區*工作完成時，系統會將以下更新下載至管理伺服器儲存區：

- Kaspersky 資料庫和卡巴斯基安全管理中心軟體模組

  這些更新被自動安裝。

- Kaspersky 資料庫和受管理裝置上安全應用程式的軟體模組

  這些更新透過 Kaspersky Endpoint Security for Windows 更新工作安裝。

- 管理伺服器更新

  這些更新不被自動安裝。管理員必須明確批准和執行更新安裝。

  > 需要本機管理員權限以安裝修補程式到管理伺服器。

- 卡巴斯基安全管理中心模組更新

  預設下，這些更新被自動安裝。您可以在網路代理政策中變更設定。

- 安全應用程式更新

  預設情況下，Kaspersky Endpoint Security for Windows 僅安裝您批准的更新。（您可以透過管理主控台或者透過卡巴斯基安全管理中心網頁主控台批准更新）。更新透過*更新*工作安裝且可以在工作內容中被配置。

> *將更新下載至管理伺服器儲存區*工作在虛擬管理伺服器上不可用。虛擬管理伺服器的儲存區節點下的更新，將顯示已下載至主管理伺服器的更新。

您可以配置在測試裝置集上進行更新的操作和錯誤驗證。如果驗證成功，更新被分發到其他受管理裝置。

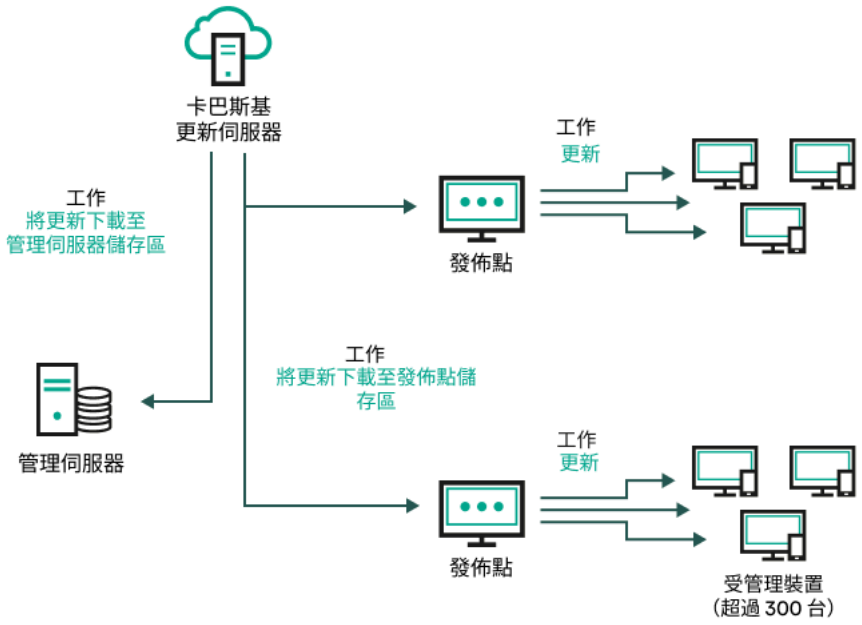
每個 Kaspersky 應用程式都從管理伺服器請求所需更新。管理伺服器集合這些更新並僅下載應用程式請求的更新。這確保了相同更新不被下載多次，且不必要更新不被下載。當執行*將更新下載至管理伺服器儲存區*工作時，管理伺服器自動傳送以下資訊到 Kaspersky 更新伺服器以便確保相關版本的 Kaspersky 資料庫和軟體模組的下載：

- 應用程式 ID 和版本
- 應用程式安裝 ID
- 啟動金鑰 ID
- 「*將更新下載至管理伺服器儲存區*」工作執行 ID

傳輸的資訊均不含個人詳情或其他機密資訊。AO Kaspersky Lab 依照法律需求防護資訊。

使用兩個工作：將更新下載至管理伺服器儲存區工作與將更新下載至發佈點儲存區工作

您可以直接從 Kaspersky 更新伺服器下載更新到發佈點儲存區，而不是從管理伺服器儲存區，然後分發更新到受管理裝置（參見下圖）。您可以下載到發佈點儲存區，例如，如果管理伺服器和發佈點之間的流量比發佈點和 Kaspersky 更新伺服器之間的流量貴，或者如果您的管理伺服器沒有網際網路存取。



使用將更新下載至管理伺服器儲存區工作與將更新下載至發佈點儲存區工作更新

預設下，管理伺服器和發佈點與 Kaspersky 更新伺服器通訊並使用 HTTPS 協定下載更新。您可以配置管理伺服器和/或發佈點使用 HTTP 協定，而不是 HTTPS。

若要實現該方案，請在*將更新下載至管理伺服器儲存區*工作外再建立*將更新下載至發佈點儲存區*工作。此後，發佈點將從 Kaspersky 更新伺服器下載更新，而不是從管理伺服器儲存區。

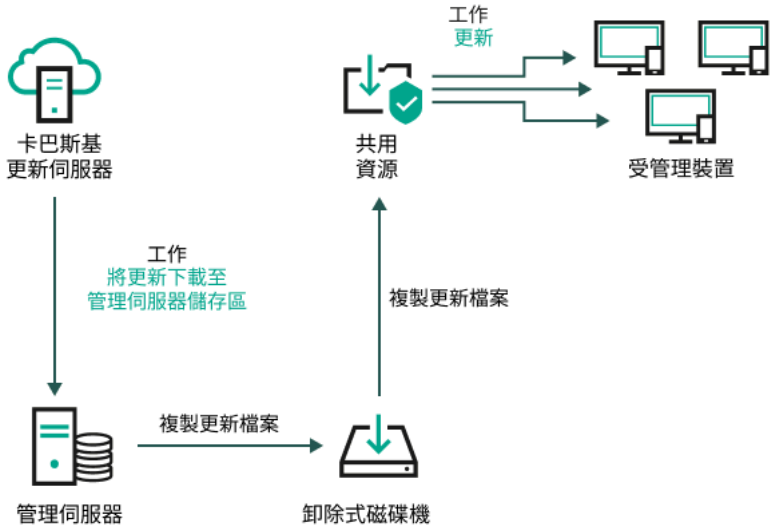
執行 macOS 的發佈點裝置無法從 Kaspersky 更新伺服器下載更新。

若一或多個執行 macOS 的裝置位於*下載更新至發佈點儲存區*工作範圍內，該工作會以*失敗*狀態完成，即使工作已在所有 Windows 裝置上成功完成。

此方案也需要*將更新下載至管理伺服器儲存區*工作，因為該工作被用於下載 Kaspersky 資料庫和卡巴斯基安全管理中心軟體模組。

透過本機資料夾、共用資料夾或 FTP 伺服器手動。

如果裝置未連線到管理伺服器，您可以使用本機資料夾或共用資料夾作為更新 Kaspersky 資料庫、軟體模組和應用程式的更新來源。在此方案中，您需要從管理伺服器儲存區複製所需更新到卸除式磁碟機，然後複製更新到在 Kaspersky Endpoint Security 設定中指定的本機資料夾或共用資料夾（參見下圖）。



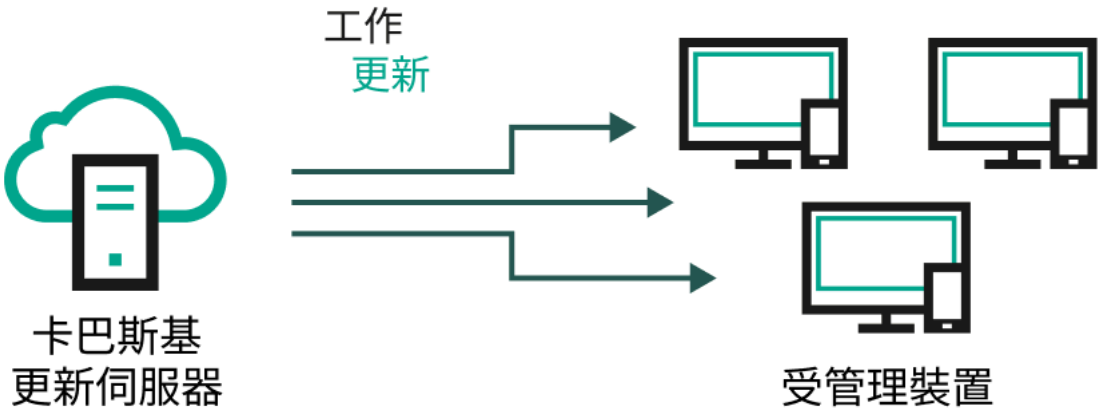
透過本機資料夾、共用資料夾或 FTP 伺服器更新

有關 Kaspersky Endpoint Security 更新來源的更多資訊，請參閱以下說明：

- Kaspersky Endpoint Security for Windows 說明
- Kaspersky Endpoint Security for Linux 說明

直接從卡巴斯基更新伺服器到受管理裝置上的 Kaspersky Endpoint Security

在受管理裝置上，您可以配置 Kaspersky Endpoint Security 直接從卡巴斯基更新伺服器接收更新（參見下圖）。



直接從卡巴斯基更新伺服器更新安全應用程式

在此方案中，安全應用程式不使用卡巴斯基安全管理中心提供的儲存區。要直接從 Kaspersky 更新伺服器接收更新，在安全應用程式介面中指定 Kaspersky 更新伺服器作為更新來源。有關這些設定的詳細資訊，請參閱以下說明：

- Kaspersky Endpoint Security for Windows 說明
- Kaspersky Endpoint Security for Linux 說明

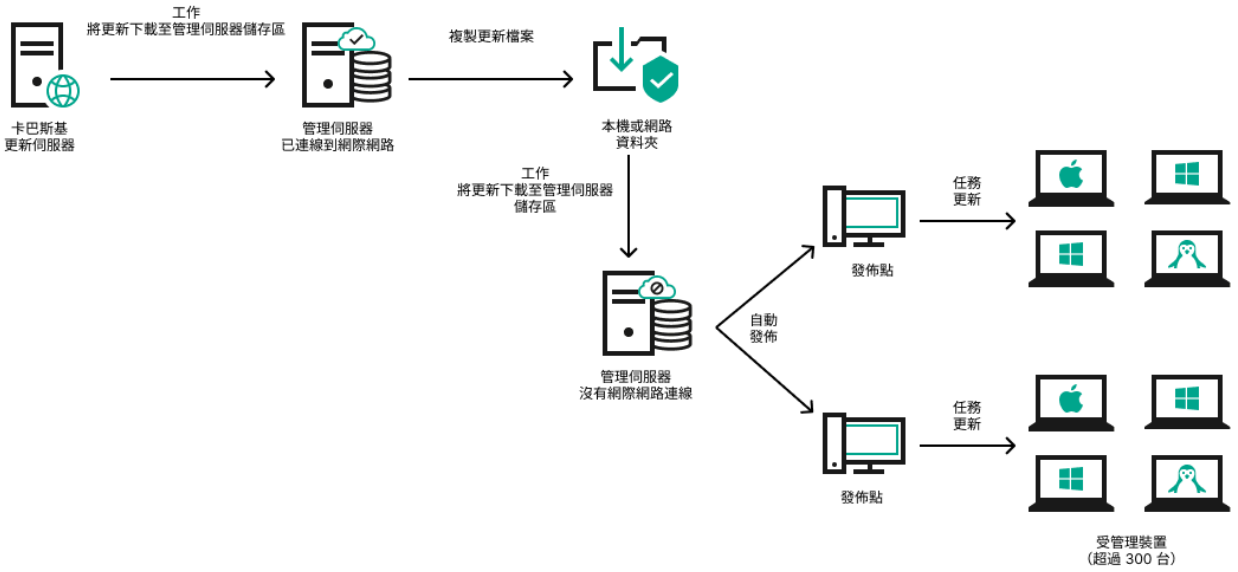
如果管理伺服器沒有網際網路連線，則透過本機或網路資料夾

如果管理伺服器沒有網際網路連線，您可以配置*將更新下載至管理伺服器儲存區*本機或網路資料夾下載更新。在這種情況下，您必須不時將所需的更新檔案複製到指定的資料夾中。例如，您可以從以下來源之一複制所需的更新檔案：

- 具有網際網路連線的管理伺服器（參見下圖）

  因為管理伺服器只下載安全應用程式請求的更新，所以管理伺服器管理的安全應用程式集合（一個有網際網路連線，一個沒有網際網路連線）必須比對。

  如果您用於下載更新的管理伺服器版本為 13.2 或更早，請開啟*將更新下載至管理伺服器儲存區*工作，然後啟用**使用舊配置下載更新**選項。



如果管理伺服器沒有網際網路連線，則透過本機或網路資料夾更新

- Kaspersky Update Utility

  由於此公用程式使用舊方案下載更新，請開啟*將更新下載至管理伺服器儲存區*工作的內容，然後啟用**使用舊配置下載更新**選項。

建立「將更新下載至管理伺服器儲存區」工作

管理伺服器的*將更新下載至管理伺服器儲存區*工作會由卡巴斯基安全管理中心快速設定精靈自動建立。您僅可建立一個*將更新下載至管理伺服器儲存區*工作。因此，只有在*將更新下載至管理伺服器儲存區*工作從管理伺服器工作清單中移除時，您才可建立此工作。

該工作用在從 Kaspersky 更新伺服器下載更新到管理伺服器儲存區時。更新清單包含：

- 管理伺服器資料庫和軟體模組更新
- Kaspersky 安全應用程式資料庫和軟體模組更新
- 卡巴斯基安全管理中心元件更新
- Kaspersky 安全應用程式更新

更新被下載後，它們可以被傳播到受管理裝置。

在向受管理裝置分發更新之前，您可以執行*更新驗證*工作。這可讓您確保管理伺服器將正確安裝下載的更新，並且安全級別不會因為更新而降低。若要在分發之前驗證它們，請在*將更新下載至管理伺服器儲存區*工作設定中配置**執行更新驗證**選項。

*要建立**將更新下載至管理伺服器儲存區**工作：*

1. 在主功能表中，轉至 **裝置 → 工作**。
2. 點擊**新增**。

   新工作精靈啟動。遵照精靈的說明。
3. 對於卡巴斯基安全管理中心應用程式，請選取**將更新下載至管理伺服器儲存區**工作類型。
4. 指定您正建立的工作的名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。
5. 若要修改預設工作設定，請啟用**完成工作建立**頁面的**建立完成時開啟工作詳情**選項。如果您不啟用該選項，工作使用預設設定建立。您可以稍後隨時修改預設設定。
6. 點擊**建立**按鈕。

   工作被建立並顯示在工作清單。
7. 按一下建立的工作的名稱以開啟工作內容視窗。

8. 在開啟的工作內容視窗的**應用程式設定**頁籤，指定以下設定：

- **更新來源**

  可使用以下資源作為管理伺服器的更新來源：

  - 卡巴斯基更新伺服器

    Kaspersky 應用程式可以從 Kaspersky 的 HTTP(S) 伺服器下載資料庫和程式模組更新。預設下，管理伺服器與 Kaspersky 更新伺服器通訊並使用 HTTPS 協定下載更新。您可以配置管理伺服器使用 HTTP 協定，而不是 HTTPS。

    預設選取。

  - 主管理伺服器

    該資源套用到為從屬或虛擬管理伺服器建立的工作。

  - 本機或網路資料夾

    包含最新更新的本機或網路資料夾。網路資料夾可以是 FTP 或 HTTP 伺服器，或者 SMB 共用。如果網路資料夾需要身分驗證，則僅支援 SMB 通訊協定。在選取本機資料夾時，您必須在安裝了管理伺服器的裝置上指定一個資料夾。

    > 更新來源所使用的 FTP 或 HTTP 伺服器或網路資料夾必須包含比對 Kaspersky 更新伺服器所建立的結構的資料夾結構（帶有更新）。

  如果包含更新的共用資料夾受密碼防護，請啟用**指定帳戶以存取更新來源的共用資料夾（如果有）**選項並輸入存取所需的帳戶憑據。

- **更新儲存資料夾**

  用於儲存已儲存更新的指定資料夾的路徑。您可以將指定的資料夾路徑複製到剪貼簿。您不能變更群組工作的指定資料夾的路徑。

- 其他設定:

  - **強制執行從屬管理伺服器的更新**

    如果啟用該選項，當新更新下載後管理伺服器立刻在從屬管理伺服器上啟動更新工作。更新工作透過使用在從屬管理伺服器上的工作屬性中配置的更新來源來啟動。

    如果停用此選項，從屬管理伺服器上的更新工作將根據排程啟動。

    預設情況下已停用該選項。

  - **複製下載的更新至其他資料夾**

管理伺服器接收更新後，它複製它們到指定資料夾。如果您想要在您的網路上手動管理更新的分發，則使用該選項。

例如，您可能要在以下情況下使用該選項：您組織的網路包含幾個獨立子網路，且每個子網路的裝置不能存取其他子網路。然而，所有子網路中的裝置都可以存取通用網路共用。此種情況下，您在子網路之一設定管理伺服器從 Kaspersky 更新伺服器下載更新，啟用該選項，然後指定該網路共用。對於其他管理伺服器的「將更新下載至儲存區」工作中，指定與更新來源相同的網路共用。

預設情況下已停用該選項。

- **除非複製完成，否則不強制更新裝置和從屬管理伺服器**

  下載更新到用戶端裝置和從屬管理伺服器工作僅在這些更新從主更新資料夾被複製到附加更新資料夾後才啟動。

  如果用戶端裝置和從屬管理伺服器從附加網路資料夾下載更新，則必須啟用該選項。

  預設情況下已停用該選項。

- **更新內容**：

  - **下載差異檔案**

    該選項啟用下載 diff 檔案功能。

    預設情況下已停用該選項。

- **使用舊配置下載更新**

  從版本 14 開始，卡巴斯基安全管理中心使用新方案下載資料庫和軟體模組的更新。對於使用新方案下載更新的應用程式，更新來源必須包含具有與新方案相容的中繼資料的更新檔案。如果更新來源包含的更新檔案的中繼資料僅與舊方案相容，請啟用 **使用舊配置下載更新**選項。否則，更新下載工作將失敗。

  例如，當本機或網路資料夾被指定為更新來源並且此資料夾中的更新檔案由以下應用程式之一下載時，您必須啟用此選項：

  - Kaspersky Update Utility

    此公用程式使用舊方案下載更新。

  - 卡巴斯基安全管理中心 13.2 或更早版本

    例如，您的管理伺服器 1 沒有網際網路連線。在這種情況下，您可以使用具有網際網路連線的管理伺服器 2 下載更新，然後將更新放置到本機或網路資料夾以將其用作管理伺服器 1 的更新來源。如果管理伺服器 2 的版本為 13.2 或更早，請啟用管理伺服器 1 的工作中的**使用舊配置下載更新**選項。

  預設情況下已停用該選項。

- **執行更新驗證**

管理伺服器會從源下載更新並將其儲存到暫時儲存區，之後執行**更新驗證工作**欄位中定義的工作。如果工作成功完成，系統會從暫時儲存區將更新複製到管理伺服器共用資料夾，然後分發到所有以管理伺服器作為更新來源的裝置（系統會啟動有**當新更新下載至儲存區時**排程類型的工作）。「將更新下載至儲存區」工作僅在*更新驗證*工作完成後結束。

預設情況下已停用該選項。

9. 在工作內容視窗的**排程**頁籤，建立工作開始的排程。如果必要，指定以下設定：

- **排程開始：**

  選取工作執行排程並設定所選排程。

  - **手動**

    工作不自動執行。您僅可以手動啟動。

    預設情況下已選定此選項。

  - **每 N 分鐘**

    工作定期執行，按照指定分鐘數間隔，從工作建立日期的指定時間開始。

    預設下，工作每 30 分鐘執行一次，從目前系統時間開始。

  - **每 N 小時**

    工作定期執行，按照指定小時數間隔，從指定的日期和時間開始。

    預設下，工作每 6 小時執行一次，從目前系統日期和時間開始。

  - **每 N 天**

    工作定期執行，按照指定天數間隔。此外，您可指定第一個工作執行的日期與時間。這些額外選項會在您建立的工作受到應用程式支援時可用。

    預設下，工作每天執行一次，從目前系統日期和時間開始。

  - **每 N 星期**

    工作定期執行，按照指定星期數間隔，從指定的星期和時間開始。

    預設下，工作每星期一於目前系統時間執行一次。

  - **每天（不支援日光節約時間）**

    工作定期執行，按照指定天數間隔。排程不支援日光節約時間 (DST)。這意味著在夏令時開始和結束時當時鐘向前或向後撥動一小時時，實際工作啟動時間不變更。

    我們不建議您使用該排程。它用於向後相容卡巴斯基安全管理中心。

    預設下，工作每天於目前系統時間執行一次。

  - **每週**

    工作每週在指定星期和指定時間執行。

  - **周中天數**

工作定期執行，在每周指定日期的指定時間。

預設下，工作每週五 6:00:00 P.M. 執行。

- **每月**

  工作定期執行，在指定月日的指定時間。

  在缺少指定日的月份，工作在最後一天執行。

  預設下，工作在每月的第一天執行，在目前系統時間。

- **每個月所選週的指定日**

  工作定期在指定月日的指定時間執行。

  預設情況下，不選取一個月中的任何一天。預設開始時間為 18:00。

- **在偵測到病毒爆發時**

  工作在發生*病毒爆發*事件後執行。選取將監控病毒爆發的應用程式類型。有下列應用程式類型可用：

  - 病毒防護工作站和檔案伺服器
  - 用於週邊防護的防毒軟體
  - 用於郵件伺服器的防毒軟體

  預設情況下選定所有應用程式類型。

  您可能想根據報告病毒爆發的安全應用程式類型執行不同的工作。此種情況下，刪除您不需要的應用程式類型選項。

- **在完成其它工作時**

  目前工作在其他工作完成後啟動。您可以選取先前工作如何結束（成功或帶有錯誤）以觸發目前工作的啟動。例如，您可能想使用***Turn on the device***選項執行開啟裝置工作，完成後，請執行*惡意軟體掃描*工作。只有當這兩項工作都被分配給相同的裝置時，此參數才會有作用。

- **執行略過的工作**

  該選項決定在工作要啟動時用戶端裝置在網路中不可見時工作的行為。

  如果啟用該選項，系統將在下一次在用戶端裝置上執行 Kaspersky 應用程式時嘗試啟動工作。如果工作排程是**手動**、**一次**或**立即**，裝置在網路中可見或包含在工作範圍後，工作會立即啟動。

  如果停用此選項，則僅限排程的工作會在用戶端裝置上執行。若為**手動**、**一次**與**立即**排程，工作僅會在網路上顯示的用戶端裝置上執行。例如，您可能想為消耗資源的工作停用該選項，您僅想在業餘時間執行該工作。

  預設情況下已停用該選項。

- **使用工作啟動自動隨機延遲**

如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動，即是，*分佈式工作啟動*。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

當工作被建立時，根據工作中包含用戶端裝置的數量，分發啟動時間被自動計算。然後，工作總是在計算的開始時間啟動。然後當工作設定被編輯或者工作被手動啟動時，計算的工作啟動時間值被變更。

如果該選項被停用，工作依據排程在用戶端裝置上啟動。

- **使用工作啟動隨機延遲間隔（分鐘）**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

  預設情況下已停用該選項。預設時間間隔為一分鐘。

- **停止工作，若時間超過（分鐘）**

  在指定時間段過後，工作被自動停止，無論它是否完成。

  如果您想要中斷或停止執行時間太長的工作，則啟用該選項。

  預設情況下已停用該選項。預設工作執行時間是 120 分鐘。

10. 點擊**儲存**按鈕。

    工作被建立和配置。

當管理伺服器執行*將更新下載至管理伺服器儲存區*工作時，資料庫和軟體模組更新將從更新來源下載並儲存在管理伺服器共用資料夾中。如果您為管理群組建立此工作，它將僅被套用到包含在指定管理群組中的網路代理。

這些更新將從管理伺服器共用資料夾分發至用戶端裝置和從屬管理伺服器。

驗證已下載的更新

安裝更新到受管理裝置之前，您可以先透過*更新驗證*工作檢查更新。*更新驗證*工作會自動作為*將更新下載至管理伺服器儲存區*工作的一部分執行。管理伺服器從更新來源下載更新、將其儲存在臨時儲存區並執行*更新驗證*工作。如果工作成功完成，更新將從臨時儲存區複製到管理伺服器共用資料夾。它們被分發到所有以該管理伺服器為更新來源的用戶端裝置。

如果*更新驗證*工作的結果顯示位於臨時儲存區中的更新是錯誤的，或*更新驗證*工作發生錯誤，這些更新不會被複製到共用資料夾。管理伺服器保留之前的更新集。此外，有**當新更新下載至儲存區時**排程類型的工作也不會啟動。若新更新的掃描成功完成，這些操作會在*將更新下載至管理伺服器儲存區*工作下次啟動時執行。

如果在一台或多台測試裝置上出現以下情況，那麼更新就被認為是無效的：

- 發生了更新工作錯誤。
- 安全應用程式的即時防護狀態在套用更新後變更。

- 執行自訂掃描工作過程中發現一個被感染的物件。
- Kaspersky 程式出現執行階段錯誤。

如果在任何測試裝置上未出現以上情況，則此更新集就被認為是有效的，*更新驗證*工作被認為已成功完成。

在開始建立*更新驗證*工作之前，執行先決條件：

1. 用幾個測試裝置建立管理群組。您將需要該組來驗證更新。

   我們建議使用網路中防護最可靠、應用程式設定最常用的裝置作為測試裝置。這種方法提高了掃描期間病毒偵測的品質和概率，將誤報的風險降至最低。如果在測試裝置上偵測到病毒，*更新驗證*工作將被判定為不成功。

2. 為卡巴斯基安全管理中心支援的應用程式（例如 Kaspersky Endpoint Security for Windows 或 Kaspersky Security for Windows Server）建立更新和惡意軟體掃描工作。當建立更新和惡意軟體掃描工作時，指定測試裝置的管理群組。

   *更新驗證*工作將在測試裝置上順序執行更新和惡意軟體掃描工作以檢查所有更新是否有效。此外，在建立*更新驗證*工作時，您需要指定更新和惡意軟體掃描工作。

3. 建立*將更新下載至管理伺服器儲存區*工作。

要讓卡巴斯基安全管理中心將更新發佈至用戶端裝置前對下載的更新進行驗證，請執行以下操作：

1. 在主功能表中，轉至 **裝置 → 工作**。
2. 點擊**將更新下載至管理伺服器儲存區**工作。
3. 在開啟的工作內容視窗中，轉到**應用程式設定**頁簽，然後啟用**執行更新驗證**選項。
4. 如果存在*更新驗證*工作，請點擊**選取工作**按鈕。在開啟的視窗中，在測試裝置的管理群組中選取*更新驗證*工作。

5. 如果您之前沒有建立*更新驗證*工作，請執行以下操作：

   a. 點擊**新工作**按鈕。

   b. 在開啟的新工作精靈中，如果要變更預設名稱，請指定工作名稱。

   c. 選擇您之前建立的具有測試裝置的管理群組。

   d. 首先，選擇卡巴斯基安全管理中心支援的所需應用程式的更新工作，然後選擇惡意軟體掃描工作。

   之後，將出現以下選項。我們建議啟用它們：

   - **在資料庫更新後重新啟動裝置**

     在裝置上更新病毒資料庫後，我們建議重新啟動裝置。

     依預設已啟用該選項。

   - **在資料庫更新和裝置重新啟動後檢查即時防護狀態**

     如果啟用此選項，則*更新驗證*工作將檢查下載到管理伺服器儲存區的更新是否有效，以及在病毒資料庫更新和裝置重啟後防護等級是否降低了。

     預設情況下已啟用該選項。

   e. 指定一個帳戶，*更新驗證*工作將從該帳戶執行。您可以使用您的帳戶並啟用**預設帳戶**選項。或者，您可以指定工作應在具有必要存取權限的另一個帳戶下執行。為此，請選擇**指定帳戶**選項，然後輸入該帳戶的憑據。

6. 點擊**儲存**關閉*將更新下載至管理伺服器儲存區*工作的內容視窗。

自動更新驗證被啟用。現在，您可以執行*將更新下載至管理伺服器儲存區*工作，它將從更新驗證開始。

建立「將更新下載至發佈點儲存區」工作

*下載更新至發佈點的儲存區*工作僅在發佈點裝置執行 Windows 時作用。執行 Linux 或 macOS 的發佈點裝置無法從 Kaspersky 更新伺服器下載更新。若工作範圍內有至少一部裝置執行 Linux 或 macOS，該工作將處於*已失敗*狀態。即使該工作在所有 Windows 裝置上成功完成，其餘裝置仍會返回錯誤。

您可以為管理群組建立*將更新下載至發佈點儲存區*工作。該工作將為包含在指定管理群組中的發佈點執行。

您可以使用該工作，例如，如果管理伺服器和發佈點之間的流量比發佈點和 Kaspersky 更新伺服器之間的流量貴，或者如果您的管理伺服器沒有網際網路存取。

該工作用在從 Kaspersky 更新伺服器下載更新到發佈點儲存區時。更新清單包含：

- Kaspersky 安全應用程式資料庫和軟體模組更新
- 卡巴斯基安全管理中心元件更新
- Kaspersky 安全應用程式更新

更新被下載後，它們可以被傳播到受管理裝置。

*若要針對選取的管理群組建立**將更新下載至發佈點儲存區**工作：*

1. 在主功能表中，轉至 **裝置** → **工作**。
2. 點擊**新增**按鈕。

   新工作精靈啟動。遵照精靈的說明。
3. 若為卡巴斯基安全管理中心應用程式，請在**工作類型**欄位選取**將更新下載至發佈點儲存區**。
4. 指定您正建立的工作的名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。
5. 選取一個選項按鈕以指定管理群組、裝置分類或應用程式工作的裝置。
6. 在**完成工作建立**步驟中，如果要修改預設工作設定，請啟用**建立完成時開啟工作詳情**選項。如果您不啟用該選項，工作使用預設設定建立。您可以稍後隨時修改預設設定。
7. 點擊**建立**按鈕。

   工作被建立並顯示在工作清單。
8. 按一下建立的工作的名稱以開啟工作內容視窗。

9. 在工作內容視窗的**應用程式設定**頁籤，指定以下設定：

- **更新來源**

  以下資源可作為發佈點的更新來源：

  - Kaspersky 更新伺服器

    Kaspersky 應用程式可以從 Kaspersky 的 HTTP(S) 伺服器下載資料庫和程式模組更新。

    預設情況下已選取此選項。

  - 本機或網路資料夾

    包含最新更新的本機或網路資料夾。網路資料夾可以是 FTP 或 HTTP 伺服器，或者 SMB 共用。如果網路資料夾需要身分驗證，則僅支援 SMB 通訊協定。在選取本機資料夾時，您必須在安裝了管理伺服器的裝置上指定一個資料夾。

    更新來源所使用的 FTP 或 HTTP 伺服器或網路資料夾必須包含比對 Kaspersky 更新伺服器所建立的結構的資料夾結構（帶有更新）。

- **更新儲存資料夾**

  用於儲存已儲存更新的指定資料夾的路徑。您可以將指定的資料夾路徑複製到剪貼簿。您不能變更群組工作的指定資料夾的路徑。

- **下載差異檔案**

  該選項啟用下載 diff 檔案功能。

  預設情況下已停用該選項。

- **使用舊配置下載更新**

  從版本 14 開始，卡巴斯基安全管理中心使用新方案下載資料庫和軟體模組的更新。對於使用新方案下載更新的應用程式，更新來源必須包含具有與新方案相容的中繼資料的更新檔案。如果更新來源包含的更新檔案的中繼資料僅與舊方案相容，請啟用 **使用舊配置下載更新**選項。否則，更新下載工作將失敗。

  例如，當本機或網路資料夾被指定為更新來源並且此資料夾中的更新檔案由以下應用程式之一下載時，您必須啟用此選項：

  - Kaspersky Update Utility

    此公用程式使用舊方案下載更新。

  - 卡巴斯基安全管理中心 13.2 或更早版本

    例如，發佈點被配置為從本機或網路資料夾獲取更新。在這種情況下，您可以使用具有網際網路連線的管理伺服器下載更新，然後將更新放在發佈點上的本機資料夾中。如果管理伺服器的版本為 13.2 或更早，請啟用*將更新下載到發佈點的儲存區*工作中的**使用舊配置下載更新**選項。

  預設情況下已停用該選項。

10. 為工作啟動建立排程。如果必要，指定以下設定：

- **排程開始**

  選取工作執行排程並設定所選排程。

  - **手動**

    工作不自動執行。您僅可以手動啟動。

    預設情況下已選定此選項。

  - **每 N 分鐘**

    工作定期執行，按照指定分鐘數間隔，從工作建立日期的指定時間開始。

    預設下，工作每 30 分鐘執行一次，從目前系統時間開始。

  - **每 N 小時**

    工作定期執行，按照指定小時數間隔，從指定的日期和時間開始。

    預設下，工作每 6 小時執行一次，從目前系統日期和時間開始。

  - **每 N 天**

    工作定期執行，按照指定天數間隔。此外，您可指定第一個工作執行的日期與時間。這些額外選項會在您建立的工作受到應用程式支援時可用。

    預設下，工作每天執行一次，從目前系統日期和時間開始。

  - **每 N 星期**

    工作定期執行，按照指定星期數間隔，從指定的星期和時間開始。

    預設下，工作每星期一於目前系統時間執行一次。

  - **每天（不支援日光節約時間）**

    工作定期執行，按照指定天數間隔。排程不支援日光節約時間 (DST)。這意味著在夏令時開始和結束時當時鐘向前或向後撥動一小時時，實際工作啟動時間不變更。

    我們不建議您使用該排程。它用於向後相容卡巴斯基安全管理中心。

    預設下，工作每天於目前系統時間執行一次。

  - **每週**

    工作每週在指定星期和指定時間執行。

  - **按每星期中的指定日**

工作定期執行，在每周指定日期的指定時間。

預設下，工作每週五 6:00:00 P.M. 執行。

- **每月**

  工作定期執行，在指定月日的指定時間。

  在缺少指定日的月份，工作在最後一天執行。

  預設下，工作在每月的第一天執行，在目前系統時間。

- **每個月在所選週的指定天**

  工作定期在指定月日的指定時間執行。

  預設情況下，不選取一個月中的任何一天。預設開始時間為 18:00。

- **在偵測到病毒爆發時**

  工作在發生*病毒爆發*事件後執行。選取將監控病毒爆發的應用程式類型。有下列應用程式類型可用：

  - 病毒防護工作站和檔案伺服器
  - 用於週邊防護的防毒軟體
  - 用於郵件伺服器的防毒軟體

  預設情況下選定所有應用程式類型。

  您可能想根據報告病毒爆發的安全應用程式類型執行不同的工作。此種情況下，刪除您不需要的應用程式類型選項。

- **在完成其它工作時**

  目前工作在其他工作完成後啟動。您可以選取先前工作如何結束（成功或帶有錯誤）以觸發目前工作的啟動。例如，您可能想使用***Turn on the device***選項執行開啟裝置工作，完成後，請執行*惡意軟體掃描*工作。只有當這兩項工作都被分配給相同的裝置時，此參數才會有作用。

- **執行略過的工作**

  該選項決定在工作要啟動時用戶端裝置在網路中不可見時工作的行為。

  如果啟用該選項，系統將在下一次在用戶端裝置上執行 Kaspersky 應用程式時嘗試啟動工作。如果工作排程是**手動**、**一次**或**立即**，裝置在網路中可見或包含在工作範圍後，工作會立即啟動。

  如果停用此選項，則僅限排程的工作會在用戶端裝置上執行。若為**手動**、**一次**與**立即**排程，工作僅會在網路上顯示的用戶端裝置上執行。例如，您可能想為消耗資源的工作停用該選項，您僅想在業餘時間執行該工作。

  預設情況下已停用該選項。

- **使用工作啟動自動隨機延遲**

如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動，即是，*分佈式工作啟動*。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

當工作被建立時，根據工作中包含用戶端裝置的數量，分發啟動時間被自動計算。然後，工作總是在計算的開始時間啟動。然後當工作設定被編輯或者工作被手動啟動時，計算的工作啟動時間值被變更。

如果該選項被停用，工作依據排程在用戶端裝置上啟動。

- **使用工作啟動隨機延遲間隔（分鐘）**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

  預設情況下已停用該選項。預設時間間隔為一分鐘。

11. 點擊**儲存**按鈕。

    工作被建立和配置。

除了您在工作建立過程中指定的設定，您還可以變更所建立工作的其他屬性。

執行*將更新下載至發佈點儲存區*工作時，資料庫和軟體模組更新從更新來源下載並儲存在共用資料夾。下載的更新將僅被包含在指定管理群組的發佈點和沒有更新下載工作的更新代理使用。

啟用和停用卡巴斯基安全管理中心元件的自動更新和修補程式

管理伺服器更新和修補程式僅可以手動安裝，在獲得管理員的明確批准後。

在裝置上安裝網路代理時，自動安裝卡巴斯基安全管理中心元件更新和修補程式被預設啟用。您可以在網路代理安裝過程中停用它，或稍後使用政策停用。

要在裝置上本機安裝網路代理時停用卡巴斯基安全管理中心元件自動更新和修補程式：

1. 在裝置上啟動網路代理本機安裝。
2. 在**進階設定**步驟，清空**自動安裝元件的未定義狀態的可應用更新和修補程式**核取方塊。
3. 遵照精靈的說明。

   停用了卡巴斯基安全管理中心元件自動更新和修補程式的網路代理將被安裝在裝置。您可以稍後使用政策啟用自動更新和修補程式。

要在透過安裝套件安裝網路代理到裝置時停用卡巴斯基安全管理中心元件自動更新和修補程式：

1. 在主功能表中，轉至 **操作 → 儲存區 → 安裝套件**。
2. 點擊**卡巴斯基安全管理中心網路代理 <版本號>** 套件。

3. 在內容視窗中，開啟**設定**頁籤。

4. 關閉**對未定義狀態的元件自動安裝可套用更新和修補程式**開關按鈕。

   停用了卡巴斯基安全管理中心元件自動更新和修補程式的網路代理將被從該封包安裝。您可以稍後使用政策啟用自動更新和修補程式。

如果在網路代理安裝到裝置時選取（清空）了該核取方塊，您可以後續啟用（或停用）使用網路代理政策自動更新。

要使用網路代理政策啟用或停用卡巴斯基安全管理中心元件的自動更新和修補程式：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。

2. 點擊網路代理政策。

3. 在政策內容視窗中，開啟**應用程式設定**頁籤。

4. 在**管理修補程式和更新**區段中，開啟或關閉**對未定義狀態的元件自動安裝可套用更新和修補程式**開關按鈕以個別啟用或停用自動更新和修補。

5. 為該開關按鈕設定鎖（🔒）。

   該政策將被應用到所選裝置，且卡巴斯基安全管理中心元件自動更新和修補程式將在這些裝置上被啟用（停用）。

自動安裝 Kaspersky Endpoint Security for Windows 的更新

您可以在用戶端裝置上配置 Kaspersky Endpoint Security for Windows 自動更新資料庫和軟體模組。

要在裝置上配置下載和自動安裝 Kaspersky Endpoint Security for Windows 更新：

1. 在主功能表中，轉至 **裝置 → 工作**。

2. 點擊**新增**按鈕。

   新工作精靈啟動。遵照精靈的說明。

3. 對於 Kaspersky Endpoint Security for Windows 應用程式，選取**更新**作為工作子類型。

4. 指定您正建立的工作的名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。

5. 選取工作範圍。

6. 指定管理群組、裝置分類或應用程式工作的裝置。

7. 在**完成工作建立**步驟中，如果要修改預設工作設定，請啟用**建立完成時開啟工作詳情**選項。如果您不啟用該選項，工作使用預設設定建立。您可以稍後隨時修改預設設定。

8. 點擊**建立**按鈕。

   工作被建立並顯示在工作清單。

9. 按一下建立的工作的名稱以開啟工作內容視窗。

10. 在工作內容視窗的**應用程式設定**頁籤，定義本機或行動模式的更新工作設定：

    - **本機模式**：連線會在裝置和管理伺服器之間建立。
    - **行動模式**：卡巴斯基安全管理中心與裝置間不會建立連線（例如裝置未與網際網路連線時）。

11. 啟用您要用來更新 Kaspersky Endpoint Security for Windows 資料庫與應用程式模組的更新來源。如有必要，請使用**向上移動**與**向下移動**按鈕變更清單中的來源位置。若啟用數個更新來源，Kaspersky Endpoint Security for Windows 會嘗試逐一連線，從清單頂端開始，並透過第一個可用來源的更新套件執行更新工作。

12. 啟用**安裝批准的應用程式模組更新**選項，在更新應用程式資料庫同時下載和安裝軟體模組。

    如果啟用該選項，Kaspersky Endpoint Security for Windows 在執行更新工作時，會通知使用者有可用的軟體模組更新並且更新套件包含軟體模組更新。Kaspersky Endpoint Security for Windows 僅會安裝您設定*已核准*狀態的更新，這些更新將透過卡巴斯基安全管理中心進行本機安裝。

    您也可以啟用**自動安裝關鍵應用程式模組更新**選項。如果軟體模組有任何更新，Kaspersky Endpoint Security for Windows 自動安裝*關鍵*狀態的更新；其餘的更新會在您批准後安裝。

    如果軟體模組更新需要審查並接受產品授權協議的隱私政策，程式將在使用者接受最終使用者產品授權協議的條款和隱私政策後安裝更新。

13. 選取**複製更新到資料夾**核取方塊，程式將已下載的更新儲存到指定的資料夾。

14. 排程工作。若要確保定期更新，建議您選取**當新更新下載至儲存區時**選項。

15. 點擊**儲存**。

更新工作在執行時，程式傳送請求到 Kaspersky 更新伺服器。

一些更新需要安裝最新版本的管理外掛程式。

批准和拒絕軟體更新

更新安裝工作的設定可能需要對要安裝的更新進行批准。您可以批准必須安裝的更新並拒絕不能安裝的更新。

例如，您可能想先在測試環境中檢查更新安裝以確保它們不干預裝置操作，僅在這之後允許安裝這些更新到用戶端裝置。

要批准或拒絕一個或幾個更新：

1. 在主功能表中，轉到**操作 → Kaspersky 應用程式 → 無縫更新**。

   可用更新清單被顯示。

   受管理應用程式的更新可能需要安裝卡巴斯基安全管理中心特定的最低版本。如果此版本晚於目前版本，則顯示這些更新，但無法核准。同樣，在升級卡巴斯基安全管理中心之前，無法從此類更新中建立安裝軟體套件。提示您將卡巴斯基安全管理中心執行個體升級到所需的最低版本。

2. 選取您要批准或拒絕的更新。

3. 點擊**批准**以核准選取的更新或**拒絕**以拒絕選取的更新。

   預設值是*未定義*。

您分配了*已批准*狀態的更新被放置在安裝佇列。

您分配了*已拒絕*狀態的更新被從先前將其安裝的裝置上移除（如果可能）。而且，它們將來也不會被安裝到其他裝置。

Kaspersky 應用程式的一些更是無法被移除。如果您為其設定了*已拒絕*狀態，卡巴斯基安全管理中心將不會從先前將其安裝的裝置上移除這些更新。然而，這些更新將來也不會被安裝到其他裝置。

如果您為協力廠商軟體更新設定了*已拒絕*狀態，則已計畫但未安裝這些更新的裝置將不會安裝這些更新。更新將保持在已將其安裝的裝置上。如果您必須刪除更新，您可以在本機手動刪除它們。

更新管理伺服器

您可以使用以下方法安裝管理伺服器更新：更新管理伺服器精靈。

要安裝管理伺服器更新：

1. 在主功能表中，轉到**操作 → Kaspersky 應用程式 → 無縫更新**。

2. 以下列方式之一執行更新管理伺服器精靈：

   - 在更新清單中，點擊管理伺服器更新的名稱，然後在開啟的視窗中，點擊**執行更新管理伺服器精靈**連結。
   - 點擊**執行更新管理伺服器精靈**視窗頂端通知欄位中的連結。

3. 在更新管理伺服器精靈視窗中，選擇以下選項之一以指定何時安裝更新：

   - **現在安裝**。如果您想要立即安裝更新則選則此選項。
   - **延遲安裝**。如果您想要稍後安裝更新則選則此選項。在這種情況下，將顯示有關此更新的通知。
   - **略過更新**。如果您不想安裝更新並且不想接收有關此更新的通知，請選擇此選項。

4. 如果要在安裝更新之前建立管理伺服器的備份，選擇**更新安裝前建立管理伺服器備份副本**選項。

5. 點擊**確定**按鈕以完成精靈。

在備份過程被中斷的情況下，更新安裝過程也會被中斷。

啟用和停用行動模式更新下載

我們建議您避免停用行動模式更新下載。停用它可能導致更新傳送到裝置失敗。特殊情況下，Kaspersky 技術支援專家可能建議您停用**提前從管理伺服器下載更新和病毒資料庫**選項。然後，您將必須確保接收 Kaspersky 應用程式更新的工作被設定。

要為管理群組啟用或停用行動模式更新下載：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。

2. 點擊**群組**。

3. 在管理群組結構中，選取您要啟用行動模式更新下載的管理群組。

4. 點擊網路代理政策。

   網路代理政策的內容視窗開啟。

   預設下，子政策的設定從父政策繼承且無法被修改。如果您要修改的政策是繼承的，您首先需要在所需管理群組為網路代理建立新政策。在新建立的政策中，您可以修改未在父政策中鎖定的設定。

5. 在**應用程式設定**頁籤，選取**管理修補程式和更新**區段。

6. 啟用或停用**提前從管理伺服器下載更新和病毒資料庫（建議）**選項以啟用或停用行動模式更新下載。

   預設下，行動模式更新下載已啟用。

這樣便啟用或停用了行動模式更新下載。

在離線裝置上更新 Kaspersky 資料庫和軟體模組

在受管理裝置上更新 Kaspersky 資料庫和軟體模組是個重要的工作，它維持裝置的防護以防範病毒和其他威脅。管理員通常透過使用管理伺服器儲存區或發佈點儲存區來配置定期更新。

當您需要在未連線到管理伺服器（主要或次要）、發佈點或網際網路的裝置（或裝置群組）上更新資料庫和軟體模組時，您必須使用其他更新來源，例如 FTP 伺服器或本機資料夾。此種情況下，您必須使用大容量裝置傳送所需更新的檔案，例如快閃記憶體磁碟機或外部硬碟磁碟機。

您可以從這裡複製所需更新：

- 管理伺服器。

  為確保管理伺服器儲存區包含所需的安裝在離線裝置上的安全應用程式的更新，至少一台受管理的線上裝置必須安裝了相同的安全應用程式。您必須設定此應用程式，才可透過將更新下載至管理伺服器儲存區工作，從管理伺服器儲存區接收更新。

- 任何安裝了相同安全應用程式的裝置，並配置了從管理伺服器儲存區接收更新，或直接從 Kaspersky 更新伺服器接收更新。

以下是透過從管理伺服器儲存區複製而更新資料庫和軟體模組的例子。

要在離線裝置上更新 Kaspersky 資料庫和軟體模組：

1. 連線卸除式磁碟機到管理伺服器所在裝置。
2. 複製更新檔案到卸除式磁碟機。

   預設下，更新位於：\\<server name>\KLSHARE\Updates。

   或者，您可以配置卡巴斯基安全管理中心定期複製更新到您選取的資料夾。為此，請使用將更新下載至管理伺服器儲存區工作內容中的**複製下載的更新至其他資料夾**選項。如果您指定快閃記憶體磁碟機或外部硬碟磁碟機上的資料夾作為該選項的目的資料夾，該大容量裝置將總是包含更新的最新版本。
3. 在離線裝置上，配置安全應用程式（例如，Kaspersky Endpoint Security for Windows）以從本機資料夾或共用資料夾接收更新，例如 FTP 伺服器或共用資料夾。
4. 從卸除式磁碟機複製更新到您想用作更新來源的本機資料夾或共用資源。
5. 在需要安裝更新的離線裝置上，開始 Kaspersky Endpoint Security for Windows 的更新工作。

在更新工作完成後，Kaspersky 資料庫和軟體模組在裝置上變為最新。

備份和還原 Web 外掛程式

卡巴斯基安全管理中心 網頁主控台允許您備份 Web 外掛程式的目前狀態，以便以後能夠還原儲存的狀態。例如，您可以在將 Web 外掛程式更新到較新版本之前對其進行備份。更新後，如果較新的版本不符合您的要求或期望，您可以從備份中還原以前版本的 Web 外掛程式。

要備份 Web 外掛程式：

1. 在主功能表中，轉至 **主控台設定 → Web 外掛程式**。

   主控台設定視窗隨即開啟。
2. 在**Web 外掛程式**頁簽上，選擇要備份的 Web 外掛程式，然後點擊**建立備份副本**按鈕。

選定的 Web 外掛程式被備份。您可以在**備份**頁簽上檢視建立的備份。

要從備份中還原 Web 外掛程式：

1. 在主功能表中，轉至 **主控台設定 → 備份**。

   主控台設定視窗隨即開啟。
2. 在**備份**頁簽上，選擇要還原的 Web 外掛程式的備份，然後點擊**從備份還原**按鈕。

Web 外掛程式將被從選定的備份中還原。

發佈點和連線閘道器的調整

卡巴斯基安全管理中心中的管理群組結構執行以下功能：

- 設定政策範圍

  套用相關設定到裝置有另一種方式，透過使用*政策設定檔*。在此情況下，您可以設定有標籤的政策範圍、在 Active Directory 組織單元中的裝置位置、或Active Directory 安全群組的成員關係。

- 設定群組工作範圍

  還有一個不基於管理群組層級定義群組工作範圍的方法：使用裝置分類的工作和特定裝置的工作。

- 設定裝置、虛擬管理伺服器和次要管理伺服器的存取權限

- 分配發佈點

當建立管理群組結構時，您必須考慮到組織網路的拓撲以便最優分配發佈點。發佈點的最優分發允許您在企業網路中儲存流量。

根據組織圖表和網路拓撲，以下標準配置可以被套用到管理群組結構：

- 單一辦公室

- 多個小遠端分辦公室

作為發佈點的裝置必須被防護，包括實體防護，以防範非授權的存取。

發佈點的標準配置：單一辦公室

在標準「單一辦公室」配置中，所有裝置都在組織網路上，因此它們能看見彼此。組織網路可能包含幾部分（網路或網段），由窄通道連線。

有以下構建管理群組結構的方法：

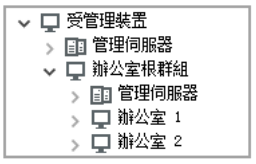
- 構建管理群組結構涉及到網路拓撲。管理群組結構可能不精確反映網路拓撲。網路各部分之間以及特定管理群組相互比對。您可以使用發佈點自動分配或手動分配它們。

- 不考慮網路拓撲而構建管理群組結構。在此情況下，您必須停用發佈點自動分配，然後為網路中每個部分的根管理群組（例如**受管理裝置**群組）分配一或多個裝置作為發佈點。所有發佈點將處於相同等級，並將掌控組織網路中所有裝置的相同範圍。此種情況下，每個網路代理將連線到具有最小路由的發佈點。發佈點的路由可以使用 tracert 公用程式偵錯。

發佈點的標準配置：多個小遠端辦公室

該標準配置用於一定數量的小型遠端辦公室，您可透過網際網路與總部通訊。每個遠端辦公室都位於 NAT 之外，就是說，從一個遠端辦公室到另一個遠端辦公室的連線是不可能的，因為辦公室是彼此隔離的。

配置必須在管理群組中體現：必須為每個遠端辦公室建立各自的管理群組（下圖中的群組**辦公室 1**和**辦公室 2**）。



遠端辦公室包含在管理群組結構

您必須指定一或多個發佈點給一間辦公室的每個對應管理群組。發佈點必須是遠端辦公室中具有足夠剩餘磁碟空間的裝置。佈署在**辦公室 1**群組的裝置，例如，將存取分配到**辦公室 1**管理群組的發佈點。

如果一些使用者在辦公室之間移動他們的攜帶式電腦，您必須在遠端辦公室選取兩個或更多裝置（除了現有的發佈點）並分配它們作為等級管理群組的發佈點（上圖中**辦公室根群組**）。

例如：攜帶式電腦佈署在**辦公室 1**管理群組，然後被移動到對應於**辦公室 2** 管理群組的辦公室。在移動攜帶式電腦後，網路代理試圖存取分配到**辦公室 1**群組的發佈點，但是那些發佈點不可用。然後，網路代理開始嘗試存取分配到**辦公室根群組**的發佈點。因為遠端辦公室是彼此隔離的，嘗試存取分配到**辦公室根群組**管理群組的發佈點僅在網路代理嘗試存取**辦公室 2** 群組中的發佈點時才會成功。就是說，攜帶式電腦將保持在原始辦公室對應的管理群組，但是將使用它當時所在辦公室的發佈點。

關於分配發佈點

您可以手動或自動將受管理裝置分配為發佈點。

如果手動將受管理裝置分配為發佈點，則可以選擇網路中的任何裝置。

如果自動分配發佈點，則卡巴斯基安全管理中心只能選擇滿足以下條件的受管理裝置：

- 裝置有至少 50 GB 的可用磁碟空間。
- 受管理裝置直接與卡巴斯基安全管理中心連線（不透過閘道）。
- 受管理裝置不是膝上型電腦。

> 如果您的網路沒有滿足指定條件的裝置，卡巴斯基安全管理中心將不會自動將任何裝置分配為發佈點。

自動分配發佈點

我們建議您自動分配發佈點。此種情況下，卡巴斯基安全管理中心將自行選取哪個裝置要被分配為發佈點。

要自動分配發佈點：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**發佈點**區段。

3. 選取**自動分配發佈點**選項。

> 如果自動指派裝置作為發佈點被啟用，您無法手動配置發佈點，也不能編輯發佈點清單。

4. 點擊**儲存**按鈕。

管理伺服器便自動指派和配置發佈點。

手動分配發佈點

卡巴斯基安全管理中心允許您手動指定裝置作為發佈點。

我們建議您自動分配發佈點。此種情況下，卡巴斯基安全管理中心將自行選取哪個裝置要被分配為發佈點。然後，如果您由於一些原因必須不自動分配發佈點（例如，如果您要使用單獨分配的伺服器），您可以在計算數量和配置後手動分配發佈點。

作為發佈點的裝置必須被防護，包括實體防護，以防範非授權的存取。

要手動指派裝置作為發佈點：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**發佈點**區段。
3. 選取**手動分配發佈點**選項。
4. 點擊**分配**按鈕。
5. 選擇您要製作發佈點的裝置。
   選取裝置時，請牢記發佈點的操作功能以及裝置作為發佈點的需求。
6. 選擇您要包含在所選發佈點範圍的管理群組。
7. 點擊**確定**按鈕。
   您新增的發佈點將顯示在**發佈點**區域的發佈點清單。
8. 在清單中點擊新增的發佈點以開啟其內容視窗。

9. 在內容視窗中配置發佈點：

- **一般**區域中包含用於設定發佈點與用戶端裝置的互動設定：

  - **SSL 連接埠**

    用戶端裝置與發佈點之間，使用 SSL 進行安全連線的 SSL 埠號。

    預設情況下使用連接埠 13000。

  - **使用多點傳送**

    如果啟用此選項，程式會使用 IP 多點傳送，在群組中的各用戶端裝置上自動發佈安裝套件。

    IP 多點傳送會減少從安裝套件安裝應用程式至一組用戶端裝置的時間，但當您安裝應用程式至單一用戶端裝置時安裝時間會增加。

  - **IP 多點傳送位址**

    用於多點傳送的 IP 位址。您可以定義範圍是 224.0.0.0 – 239.255.255.255 的 IP 位址

    依預設，卡巴斯基安全管理中心會在指定範圍內自動指派唯一 IP 多點傳送位址。

  - **IP 多點傳輸連接埠號**

    IP 多點傳輸的埠號。

    預設情況下，埠號指定為 15001。如果執行管理伺服器的裝置指定為發佈點，連接埠 13001 預設用於 SSL 連線。

  - **遠端裝置發佈點位址**

    遠端裝置連線到發佈點所用的 IPv4 位址。

  - **佈署更新**

    更新被從以下來源分發到受管理裝置：

    - 此發佈點（如果啟用此選項）。
    - 其他發佈點、管理伺服器或卡巴斯基更新伺服器（如果停用此選項）。

    使用發佈點來佈署更新可以節省流量，因為您減少了下載次數。此外，您可以減輕管理伺服器上的負載並在發佈點之間重新定位負載。您可以計算網路的發佈點數量以最佳化流量和負載。

    如果停用此選項，管理伺服器上的更新下載和負載數量可能會增加。預設情況下已啟用該選項。

  - **佈署安裝套件**

安裝套件被從以下來源分發到受管理裝置：

- 此發佈點（如果啟用此選項）。
- 其他發佈點、管理伺服器或卡巴斯基更新伺服器（如果停用此選項）。

使用發佈點來佈署安裝套件可以節省流量，因為您減少了下載次數。此外，您可以減輕管理伺服器上的負載並在發佈點之間重新定位負載。您可以計算網路的發佈點數量以最佳化流量和負載。

如果停用此選項，管理伺服器上的安裝套件下載和負載數量可能會增加。預設情況下已啟用該選項。

- **執行推入伺服器**

在卡巴斯基安全管理中心中，發佈點可以作為透過移動通訊協定管理之裝置和受網路代理管理之裝置的推送伺服器。例如，如果您希望能夠對 KasperskyOS 裝置與管理伺服器進行強制同步，則必須啟用推送伺服器。推送伺服器與啟用推送伺服器的發佈點具有相同的受管理裝置範圍。如果為相同管理群組指派了多個發佈點，則可以在每個發佈點上啟用推送伺服器。在這種情況下，管理伺服器會平衡發佈點之間的負載。

- **推入伺服器連接埠**

推送伺服器的連接埠號。您可以指定任何未佔用連接埠的編號。

- 在**範圍**區域中，指定發佈點將發佈更新的範圍（管理群組和/或網路定位）。

僅執行 Windows 作業系統的裝置可以定義網路位置。網路位置無法定義在執行其他作業系統的裝置上。

- 如果發佈點在管理伺服器以外的機器上運行，則在**更新來源**區域中，您可以選擇發佈點的更新來源：

- **更新來源**

選擇發佈點的更新來源：

- 要允許發佈點從管理伺服器自動接收更新，選取**從管理伺服器接收**。
- 若要透過工作允許發佈點接收更新，請選取 **使用更新下載工作**，然後指定一個*將更新下載到發佈點的儲存區*工作：
  - 如果裝置上已存在此類工作，請在清單中選擇該工作。
  - 如果裝置上尚不存在此類工作，請按一下**建立工作**連結以建立工作。新工作精靈啟動。遵照精靈的說明。

- **下載差異檔案**

該選項啟用下載 diff 檔案功能。

預設情況下已啟用該選項。

- 如果您的發佈點在連線到網際網路時使用代理伺服器，則可以在**網際網路連線設定**子部分中指定以下設定：
  - **使用代理伺服器**

    如果選取該方塊，您可以在輸入欄位中配置代理伺服器連線。
    預設情況下已清空此方塊。

  - **代理伺服器位址**

    代理伺服器位址。

  - **埠號**

    用於連線的埠號。

  - **略過本機位址的代理伺服器**

    如果啟用此選項，則不使用代理伺服器連線本機網路的裝置。
    預設情況下已停用該選項。

  - **代理伺服器身分驗證**

    如果選取該方塊，您可以在輸入欄位中為代理伺服器身分驗證指定憑證。
    預設情況下已清空此方塊。

  - **使用者名稱**

    建立連線代理伺服器的使用者帳戶。

  - **密碼**

    工作執行時使用的帳戶的密碼。

- 在 **KSN 代理**區域，您可以設定應用程式使用發佈點，以從受管理裝置轉發 KSN 請求：
  - **在發佈點端啟用 KSN 代理**

    KSN 代理服務執行在用作發佈點的裝置上。使用該功能重新分發和最佳化網路流量。
    發佈點傳送列在卡巴斯基安全網路聲明中的統計資訊到 Kaspersky。依預設，KSN 聲明位於 %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula。
    預設情況下已停用該選項。啟用該選項僅在**使用管理伺服器作為代理伺服器**和**我同意使用卡巴斯基安全網路**選項在管理伺服器內容視窗中被啟用時起作用。
    您可以指派活動被動叢集節點到發佈點並在該節點上啟用 KSN 代理伺服器。

  - **轉發 KSN 請求到管理伺服器**

發佈點從受管理裝置轉發 KSN 請求到管理伺服器。

預設情況下已啟用該選項。

- **透過網際網路直接存取 KSN 雲端 / 私有 KSN**

  發佈點從受管理裝置轉發 KSN 請求到 KSN 雲端或私有 KSN。在發佈點上自行產生的 KSN 要求頁會直接傳送至 KSN 雲端或私有 KSN。

  已安裝網路代理版本 11（或更早版本）的發佈點無法直接存取私有 KSN。若要重新設定發佈點傳送 KSN 要求至私有 KSN，請為各發佈點啟用 **轉發 KSN 請求到管理伺服器**選項。

  已安裝網路代理版本 12（或更新版本）的發佈點可直接存取私有 KSN。

- **當連線到私有 KSN 時略過代理伺服器設定**

  若您已在發佈點內容或網路代理政策中設定代理伺服器設定，但您的網路架構要求您直接使用私有 KSN，請啟用此選項。否則，從受管理應用程式的請求無法到達私有 KSN。

  如果您選擇**透過網際網路直接存取 KSN 雲端 / 私有 KSN**選項，則此選項可用。

- **連接埠**

  受管理裝置將用於連線到 KSN 代理伺服器的 TCP 埠號。預設埠號為 13111。

- **使用 UDP 連接埠**

  如果需要受管理裝置透過 UDP 連接埠連線到 KSN 代理伺服器，啟用**使用 UDP 連接埠**選項，並指定 UDP 連接埠號。預設情況下已啟用該選項。

- **UDP 連接埠**

  受管理裝置將用於連線到 KSN 代理伺服器的 UDP 埠號。連線到 KSN 代理伺服器的預設 UDP 連接埠是 15111。

- 如果發佈點在管理伺服器以外的機器上運行，則在“**連線閘道**”部分，您可以將發佈點配置為充當網路代理實例和管理伺服器之間連線的閘道：

  - **連線閘道**

    如果由於您的網路組織而無法在管理伺服器和網路代理之間建立直接連線，您可以使用發佈點充當管理伺服器和網路代理之間的連線閘道。

    如果您需要發佈點充當網路代理和管理伺服器之間的連線閘道，請啟用此選項。預設情況下已停用該選項。

  - **從管理伺服器建立連線到閘道（如果閘道位於 DMZ 中）**

如果管理伺服器位於隔離區域 (DMZ) 之外，在區域網路中，則安裝在遠端裝置上的網路代理無法連線到管理伺服器。您可以使用發佈點作為具有反向連線能力的連線閘道（管理伺服器建立到發佈點的連線）。

如果您需要將管理伺服器連線到 DMZ 中的連線閘道，請啟用此選項。

- **為卡巴斯基安全管理中心網頁主控台開啟本機連接埠**

  如果您需要 DMZ 內的連線閘道為位於 DMZ 中或網際網路上的 Web 主控台開啟一個連接埠，請啟用此選項。指定將用於從 Web 主控台連線到發佈點的連接埠號。預設埠號為 13299。

  如果您啟用**從管理伺服器建立連線到閘道（如果閘道位於 DMZ 中）**選項，則此選項可用。

透過充當連接閘道的分發點將行動裝置連線到管理伺服器時，您可以啟用以下選項：

- **為行動裝置開啟連接埠（僅管理伺服器 SSL 身分驗證）**

  如果您需要連線閘道為移動裝置開啟一個連接埠並指定行動裝置將用於連線到發佈點的連接埠號，請啟用此選項。預設埠號為 13292。行動裝置將檢查管理伺服器憑證。建立連線時，只有管理伺服器需經過身分驗證。

- **為行動裝置開啟連接埠（雙向 SSL 身分驗證）**

  如果您需要連線閘道開啟一個將用於管理伺服器和行動裝置的雙向身分驗證的連接埠，請啟用此選項。行動裝置將檢查管理伺服器憑證，管理伺服器將檢查行動裝置憑證。指定以下參數：

  - 行動裝置將用於連線到發佈點的連接埠號。預設埠號為 13293。
  - 行動裝置將使用的連線閘道的 DNS 網域名稱。用逗號分隔網域名稱。指定的網域名稱將包含在發佈點憑證中。如果行動裝置使用的網域名稱與發佈點憑證中的一般名稱不比對，則行動裝置不會連線到發佈點。

    預設 DNS 網域名稱是連線閘道的 FQDN 名稱。

在這兩種情況下，憑證僅在分發點上建立 TLS 工作階段期間接受檢查。憑證不會被轉送給管理伺服器進行檢查。與行動裝置建立 TLS 工作階段後，分發點會使用管理伺服器憑證建立行動裝置和管理伺服器之間同步的隧道。如果您開啟雙向 SSL 身分驗證連接埠，則分發行動裝置憑證的唯一方法是透過安裝套件。

- 透過發佈點配置 Windows 網域、Active Directory 和 IP 範圍的輪詢：

  - **Windows 網域**

    您可以啟用 Windows 網域裝置發現並為發現設定排程。

  - **Active Directory**

您可以啟用 Active Directory 網域網路輪詢並為輪詢設定排程。

如果您使用 Windows 發佈點，則可以選擇以下選項之一：

- **輪詢目前 Active Directory 網域**。
- **輪詢 Active Directory 網域樹系**。
- **僅輪詢所選 Active Directory 網域**。如果您選取該選項，新增一個或更多 Active Directory 網域到清單。

如果您使用安裝了網路代理版本 15 的 Linux 發佈點，則只能輪詢為其指定位址和使用者憑據的 Active Directory 網域。目前 Active Directory 網域和 Active Directory 網域樹系的輪詢不可用。

- **IP 範圍**

  您可以為 IPv4 範圍和 IPv6 網路啟用裝置發現。

  如果啟用**啟用範圍輪詢**核取方塊，您可以新增掃已描範圍並為其設定排程。您可以新增 IP 範圍到已掃描範圍清單。

  如果啟用**使用 Zeroconf 來輪詢 IPv6 網路**選項，發佈點將使用零配置網路（也稱為"*Zeroconf*"）自動輪詢 IPv6 網路。在這種情況下，指定的 IP 範圍將被忽略，因為發佈點會輪詢整個網路。如果發佈點執行 Linux，則**使用 Zeroconf 來輪詢 IPv6 網路**選項可用。要使用 Zeroconf Ipv6 輪詢，您必須在發佈點上安裝 avahi-browse 公用程式。

- 在**進階**區域，指定發佈點必須使用以儲存發佈資料的資料夾：
  - **使用預設的資料夾**

    如果您選取此選項，應用程式使用發佈點上的網路代理安裝資料夾。

  - **使用指定的資料夾**

    如果您選取該選項，則可以在下面的欄位中指定該資料夾的路徑。它可以是發佈點上的本機資料夾，也可以是企業網路上任何裝置的資料夾。

    發佈點上用於執行網路代理的帳戶必須具有對指定資料夾的存取權限以進行讀寫操作。

10. 點擊**確定**按鈕。

所選裝置作為發佈點執行。

修改管理群組的發佈點清單

您可以檢視為特定管理群組分配的發佈點清單並透過新增或刪除發佈點來修改清單。

要檢視和修改分配給管理群組的發佈點清單：

1. 在主功能表中，轉至 **裝置 → 受管理裝置**。
2. 在受管理裝置清單上方的**目前路徑**欄位中，點擊路徑連接。

3. 在開啟的左側窗格中，選擇您要檢視其分配的發佈點的管理群組。

   這將啟用**發佈點**功能表項。

4. 在主功能表中，轉至 **裝置 → 發佈點**。

5. 要為管理群組新增分發點，請點擊受管理裝置清單上方的**分配**按鈕，然後從開啟的窗格中選擇裝置。

6. 要刪除分配的發佈點，請從清單中選擇裝置並點擊**取消分配**按鈕。

根據於您的修改，新發佈點被新增到清單或現有發佈點被從清單刪除。

強制同步

儘管卡巴斯基安全管理中心會自動同步受管裝置的狀態、設定、工作和政策，但在某些情況下，您可能希望強制為指定裝置執行同步。您可以為以下裝置執行強制同步：

- 安裝了網路代理的裝置
- 執行 KasperskyOS 的裝置

  在為 KasperskyOS 裝置執行強制同步之前，請確保該裝置包含在分發點範圍內，並且 推入伺服器已啟用 在分發點上。

- iOS 裝置
- Android 裝置

  在為 Android 裝置執行強制同步之前，您必須 配置 Firebase Cloud Messaging。

同步單一裝置

要強制同步管理伺服器和受管理裝置：

1. 在主功能表中，轉至 **裝置 → 受管理裝置**。
2. 點擊要與管理伺服器同步的裝置名稱。

   政策內容視窗會開啟，並含有所選的**一般**區段。

3. 點擊**強制同步**按鈕。

應用程式將所選裝置與管理伺服器同步。

同步多部裝置

強制同步管理伺服器和受管理裝置：

1. 開啟管理群組的裝置清單或裝置分類：
   - 在主功能表中，轉到**裝置 → 受管理裝置**，點擊受管理裝置清單上方的**目前路徑**欄位中的路徑連接，然後選擇包含要同步的裝置的管理群組。
   - 執行裝置分類以檢視裝置清單。
2. 選取您要與管理伺服器同步之裝置旁的核取方塊。
3. 在受管理裝置清單上方，點擊省略號按鈕 (...)，然後點擊**強制同步**按鈕。
   應用程式將所選裝置與管理伺服器同步。
4. 在裝置清單中，檢視上次連線管理伺服器的時間已針對選取的裝置變更為目前時間。若時間未變更，請點擊**重新整理**按鈕更新頁面內容。

所選裝置會與管理伺服器同步。

檢視政策交付的時間

在管理伺服器上變更 Kaspersky 應用程式政策後，管理員可以檢查是否被變更的政策被傳輸到了特定受管理裝置。政策可以在定期同步或者強制同步中傳輸。

若要檢視應用程式政策交付至受管理裝置的日期與時間：

1. 在主功能表中，轉至 **裝置 → 受管理裝置**。
2. 點擊要與管理伺服器同步的裝置名稱。
   政策內容視窗會開啟，並含有所選的**一般**區段。
3. 選擇**應用程式**頁簽。
4. 選取您要檢視政策同步日期的應用程式。
   應用程式政策視窗會開啟，並含有所選的**一般**區段，並且顯示政策交付日期與時間。

啟用推送伺服器

在卡巴斯基安全管理中心中，發佈點可以作為透過移動通訊協定管理之裝置和受網路代理管理之裝置的推送伺服器。例如，如果您希望能夠對 KasperskyOS 裝置與管理伺服器進行強制同步，則必須啟用推送伺服器。推送伺服器與啟用推送伺服器的發佈點具有相同的受管理裝置範圍。如果為相同管理群組指派了多個發佈點，則可以在每個發佈點上啟用推送伺服器。在這種情況下，管理伺服器會平衡發佈點之間的負載。

您可能希望將發佈點用作推送伺服器，以確保受管理裝置和管理伺服器之間存在持續連線。某些操作需要持續連線，例如執行和停止本機工作、接收受管理應用程式的統計資訊或建立隧道。如果使用發佈點作為推送伺服器，則不必在受管理裝置上使用**不要中斷與管理伺服器的連線**選項或將封包傳送到網路代理的 UDP 連接埠。

推送伺服器支援負載最多 50,000 個同時連線。

要在發佈點上啟用推入伺服器：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**發佈點**區段。
3. 點擊要在其上啟用推入伺服器的發佈點的名稱。
   發佈點內容視窗將開啟。
4. 在**一般**區段上啟用**執行推入伺服器**選項。
5. 在 **推入伺服器連接埠** 欄位中，鍵入連接埠編號。您可以指定任何未佔用連接埠的編號。
6. 在 **遠端主機位址** 欄位中，指定發佈點裝置的 IP 位址或名稱。
7. 點擊**確定**按鈕。

推入伺服器將在所選發佈點上啟用。

管理用戶端裝置上的協力廠商應用程式

本節說明卡巴斯基安全管理中心功能如何管理安裝在用戶端裝置上的協力廠商應用程式。

關於協力廠商應用程式

卡巴斯基安全管理中心可以幫助您更新安裝在用戶端裝置上的第三方軟體，並修復第三方軟體的弱點。卡巴斯基安全管理中心只能將協力廠商軟體從目前版本更新到最新版本。

協力廠商軟體清單可以變更，並動態更新。您可以透過檢視 基於 MMC 的管理主控台和卡巴斯基安全管理中心網頁主控台中的可用更新清單，用卡巴斯基安全管理中心檢查是否可以更新協力廠商軟體（安裝在使用者的裝置上）。

以下概述的過程僅用於檢視可使用卡巴斯基安全管理中心更新的協力廠商軟體清單。請按照以下步驟存取相關資訊，無需啟動任何工作。

若要檢視可以在卡巴斯基安全管理中心雲端主控台中使用卡巴斯基安全管理中心更新的協力廠商軟體清單：

1. 在主功能表中，轉至 **裝置 → 工作**。
2. 點擊**新增**。
   新工作精靈啟動。使用**下一步**按鈕進行精靈。

3. 在精靈的**新工作**步驟中，指定以下設定：

   a. 在**應用程式**下拉清單中，選擇**卡巴斯基安全管理中心**。

   b. 在**工作類型**清單中，選取**安裝所需更新並修復弱點**工作類型。

4. 在精靈的**工作範圍**步驟中，選擇**受管理裝置**選項。

5. 在精靈的**指定安裝更新規則**步驟中，點擊**新增**按鈕。
   規則建立精靈開始。使用**下一步**按鈕進行精靈。

6. 在精靈的**選擇規則類型**步驟中，選取**協力廠商更新的規則**選項。

7. 在精靈的**General criteria**步驟中，選取**安裝所有更新（除了拒絕的）**選項，然後點擊**下一步**。

顯示第三方軟體清單。

要檢視可以使用基於 MMC 的控制台中的卡巴斯基安全管理中心更新的協力廠商軟體清單，您需要弱點和修補程式管理產品授權。否則，**安裝所需更新並修復弱點**工作不可用。

1. 在主控台樹狀目錄中，選擇**受管理裝置**資料夾。

2. 在工作區中，選取**工作**標籤。

3. 點擊**建立工作**按鈕以執行新工作精靈。遵照精靈的說明。

4. 在精靈的**選取工作類型**頁面中，選取**安裝所需更新並修復弱點**。

5. 在精靈的**指定安裝更新規則**步驟中，點擊**新增**按鈕。
   規則建立精靈開始。使用**下一步**按鈕進行精靈。

6. 在精靈的**選擇規則類型**步驟中，選取**協力廠商更新的規則**選項。

7. 在精靈的**General criteria**步驟中，選取**安裝所有更新（除了拒絕的）**選項，然後點擊**下一步**。

   顯示第三方軟體清單。

安裝協力廠商軟體更新

卡巴斯基安全管理中心允許您管理安裝在受管理裝置上的協力廠商軟體更新，並安裝所需更新修復 Microsoft 應用程式和其他軟體廠商的產品弱點。

卡巴斯基安全管理中心會搜尋透過*弱點掃描和所需更新*工作搜尋更新。完成此工作時，管理伺服器會收到偵測到的弱點清單，以及安裝於您在工作內容指定裝置上已安裝軟體需要的更新。在檢視可用更新資訊後，您可以將它們安裝到裝置。

卡巴斯基安全管理中心透過移除先前的應用程式並安裝新應用程式來更新應用程式。

在受管理裝置上更新協力廠商應用程式或修復協力廠商應用程式中的弱點時，可能需要使用者互動。例如，若協力廠商應用程式目前開啟，可能會提示使用者關閉協力廠商應用程式。

出於安全原因，卡巴斯基技術會自動掃描您使用弱點和修補程式管理功能安裝的任何協力廠商軟體更新以查找惡意軟體。這些技術用於自動檢查檔案，包括病毒掃描、靜態分析、動態分析、沙箱環境中的行為分析和機器學習。

卡巴斯基專家不會對可以使用弱點和修補程式管理功能安裝的協力廠商軟體更新進行手動分析。此外，卡巴斯基專家不會在此類更新中搜尋弱點（已知或未知）或未記錄的功能，也不會對上述段落中指定的更新以外的其他類型的更新進行分析。

安裝協力廠商軟體更新工作

當系統將協力廠商軟體更新的中繼資料下載至儲存區後，您可使用以下工作將更新安裝在用戶端裝置：

- *安裝所需更新並修復弱點*工作

  *安裝所需更新並修復弱點*工作用來安裝 Microsoft 應用程式的更新，包括由 Windows Update 服務提供的更新，以及其他廠商軟體的更新。請注意，只有當您有弱點和修補程式管理功能的授權時，才可建立此工作。

  此工作完成時，更新會自動安裝在受管理裝置上。系統會將新更新的中繼資料下載至管理伺服器儲存區，卡巴斯基安全管理中心會檢查更新是否符合更新規則中指定的條件。系統會下載符合條件的所有新更新，並在下次工作執行時安裝。

- *安裝 Windows Update 更新*工作

  *安裝 Windows Update 更新*工作不需要產品授權，但僅可用來安裝 Windows Update 更新。

  完成此工作時，僅會安裝這些工作內容中指定的更新。未來若要安裝下載至管理伺服器儲存區的新更新，您必須新增必要更新至現有工作的更新清單，或建立新安裝 Windows Update 更新工作。

將管理伺服器用作 WSUS 伺服器

Microsoft Windows 的可用更新透過 Windows Update 服務提供。管理伺服器可以被用作 Windows Server Update Services（WSUS）伺服器。若要使用管理伺服器作為 WSUS 伺服器，您可建立執行 Windows Update 同步工作，並選取網路代理政策中的**使用管理伺服器作為 WSUS 伺服器**選項。在您設定了和 Windows Update 的資料同步後，管理伺服器以集中模式和設定的頻率在裝置上更新到 Windows Update 服務。

安裝協力廠商軟體更新

您可建立並執行以下其中一項工作在受管理裝置上安裝協力廠商軟體更新：

- *安裝所需更新並修復弱點*

  請注意，只有當您有弱點和修補程式管理功能的授權時，才可建立*安裝所需更新並修復弱點*工作。您可以使用此工作來安裝 Microsoft 提供的 Windows Update 更新和其他供應商的軟體更新。

- *安裝 Windows Update 更新*

  您僅可以使用*安裝 Windows Update 更新*安裝 Windows Update 更新的工作。

在受管理裝置上更新協力廠商應用程式或修復協力廠商應用程式中的弱點時，可能需要使用者互動。例如，若協力廠商應用程式目前開啟，可能會提示使用者關閉協力廠商應用程式。

您可以建立工作，透過以下方式作為安裝所需更新的選擇：

- 透過開啟更新清單並指定要安裝的更新。

  這會建立安裝所選更新的新工作。您也可以選擇將選定的更新新增到現有工作。

- 透過執行更新安裝精靈。

  > 僅弱點和修補程式管理的產品授權可使用更新安裝精靈功能。

  此精靈簡化了更新安裝工作的建立和組態，並讓您避免建立的多餘且會重複安裝相同更新的工作。

使用更新清單安裝協力廠商軟體更新

若要使用更新清單安裝協力廠商軟體更新：

1. 開啟更新清單之一：

   - 要開啟一般更新清單，請在主功能表中，前往**操作** → **修補程式管理** → **軟體更新**。
   - 要開啟受管理裝置的更新清單，請在主功能表中，前往**裝置** → **受管理裝置** → <device name> → **進階** → **可用更新**。
   - 要開啟特定應用程式的更新清單，請在主功能表中，前往**操作** → **協力廠商應用程式** → **應用程式登錄資料** → <application name> → **可用更新**。

   可用更新清單被顯示。

2. 選取您要安裝之更新旁邊的核取方塊。

3. 點擊**安裝更新**按鈕。

   若要安裝一些軟體更新，您必須接受最終使用者產品授權協議 (EULA)。若您拒絕 EULA，則無法安裝該軟體更新。

4. 您可以選取以下其中一個方法：

   - **新工作**

     新工作精靈啟動。如果您擁有弱點和修補程式程序管理產品授權，則*安裝所需更新並修復弱點*預設會需先選取工作類型。如果您沒有產品授權，將預先選取*安裝 Windows Update 更新*工作。請按照精靈的步驟完成工作建立。

   - **安裝更新（新增規則到指定工作）**

     選取要向其新增所選更新的工作。如果您具有弱點和修補程式管理產品授權，請選取*安裝所需更新並修復弱點*工作。安裝所選更新的新規則將自動新增到所選工作中。如果您沒有產品授權，請選取*安裝 Windows Update 更新*工作。所選的更新將新增到工作屬性。

     工作內容視窗隨即開啟。按一下**儲存**按鈕以儲存變更。

如果您選擇建立工作，則會建立該工作並將其顯示在以下位置的工作清單中：**裝置** → **工作**。如果您選擇將更新新增到現有工作，則這些更新將儲存在工作屬性中。

若要安裝協力廠商軟體更新，請啟動*安裝所需更新並修復弱點*工作或*安裝 Windows Update 更新*工作。您可手動啟動任何這類工作，或在您啟動的工作內容中指定排程設定。指定工作排誠實，請確保更新安裝工作會在*弱點掃描和所需更新*工作完成後啟動。

使用更新安裝精靈安裝協力廠商軟體更新

僅弱點和修補程式管理的產品授權可使用更新安裝精靈功能。

若要建立工作以使用「更新安裝精靈」安裝協力廠商軟體更新：

1. 在主功能表中，轉至 **操作 → 修補程式管理 → 軟體更新**。
   可用更新清單被顯示。
2. 選取您要安裝之更新旁邊的核取方塊。
3. 點擊**執行更新安裝精靈**按鈕。
   更新安裝精靈開始。**選取更新安裝工作**頁面顯示以下類型的所有現有工作清單：
   - *安裝所需更新並修復弱點*
   - *安裝 Windows Update 更新*
   - *修復弱點*

   您不能修改後兩種類型的工作來安裝新更新。要安裝新更新，您只能使用*安裝所需更新並修復弱點*工作。

4. 如果希望精靈僅顯示安裝所選更新的那些工作，請啟用**僅顯示安裝此更新的工作**選項。

5. 選取您要新增的內容：

- 若要啟動工作，請選取工作名稱旁邊的核取方塊，然後點擊**開始**按鈕。
- 若要將新規則新增到現有工作：

  a. 選取工作名稱旁邊的核取方塊，然後點擊**新增規則**按鈕。

  b. 在開啟的頁面上，配置新規則：

  - **此嚴重等級之更新的安裝規則**

    有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

    如果啟用該選項，更新僅修復 Kaspersky 設定的嚴重等級等於或高於所選更新之嚴重性（**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

    如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

    預設情況下已停用該選項。

  - **根據 MSRC 此嚴重等級之更新的安裝規則**

    有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

    如果啟用該選項（僅適用於 Windows Update 更新），更新僅修復 Microsoft Security Response Center (MSRC) 設定的安全等級等於或高於清單中選定的值（**低**、**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

    如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

    預設情況下已停用該選項。

  - **該供應商的更新的安裝規則**

    此選項僅適用於協力廠商應用程式的更新。卡巴斯基安全管理中心僅安裝與由同一供應商提供的應用程式相關的更新，這些更新與所選更新相同。未安裝拒絕更新和其他供應商提供的應用程式更新。

    預設情況下已停用該選項。

  - **類型更新的安裝規則**
  - **所選更新的安裝規則**
  - **核准所選更新**

    所選更新將被批准安裝。如果一些應用的更新安裝規則僅允許安裝批准的更新，啟用該選項。

    預設情況下已停用該選項。

  - **自動安裝所選更新安裝時需要的所有先前應用程式更新**

如果在安裝所選更新需要時，您同意安裝暫時應用程式版本，保持該選項被啟用。

如果停用該選項，僅選定的應用程式版本被安裝。如果您想直截了當地更新應用程式，而不嘗試安裝增量版本，請停用該選項。如果安裝所選更新不能不安裝先前版本的應用程式，應用程式更新失敗。

例如，您在裝置上安裝了應用程式的版本 3，您想更新它到版本 5，但是該應用程式的版本 5 僅可以在版本 4 之上安裝。如果啟用該選項，軟體先安裝版本 4，然後安裝版本 5。如果停用該選項，軟體更新應用程式失敗。

預設情況下已啟用該選項。

c. 點擊**新增**按鈕。

- 要建立工作：

a. 點擊**新工作**按鈕。

b. 在開啟的頁面上，配置新規則：

- **此嚴重等級之更新的安裝規則**

有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

如果啟用該選項，更新僅修復 Kaspersky 設定的嚴重等級等於或高於所選更新之嚴重性（**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

預設情況下已停用該選項。

- **根據 MSRC 此嚴重等級之更新的安裝規則**

有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

如果啟用該選項（僅適用於 Windows Update 更新），更新僅修復 Microsoft Security Response Center (MSRC) 設定的安全等級等於或高於清單中選定的值（**低**、**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

預設情況下已停用該選項。

- **該供應商的更新的安裝規則**

此選項僅適用於協力廠商應用程式的更新。卡巴斯基安全管理中心僅安裝與由同一供應商提供的應用程式相關的更新，這些更新與所選更新相同。未安裝拒絕更新和其他供應商提供的應用程式更新。

預設情況下已停用該選項。

- **類型更新的安裝規則**
- **所選更新的安裝規則**
- **核准所選更新**

所選更新將被批准安裝。如果一些應用的更新安裝規則僅允許安裝批准的更新，啟用該選項。

預設情況下已停用該選項。

- **自動安裝所選更新安裝時需要的所有先前應用程式更新**

  如果在安裝所選更新需要時，您同意安裝暫時應用程式版本，保持該選項被啟用。

  如果停用該選項，僅選定的應用程式版本被安裝。如果您想直截了當地更新應用程式，而不嘗試安裝增量版本，請停用該選項。如果安裝所選更新不能不安裝先前版本的應用程式，應用程式更新失敗。

  例如，您在裝置上安裝了應用程式的版本 3，您想更新它到版本 5，但是該應用程式的版本 5 僅可以在版本 4 之上安裝。如果啟用該選項，軟體先安裝版本 4，然後安裝版本 5。如果停用該選項，軟體更新應用程式失敗。

  預設情況下已啟用該選項。

c. 點擊**新增**按鈕。

如果選擇啟動工作，則可以關閉精靈。該工作將在後台模式下完成。不需要進一步操作。

如果您選擇將規則新增到現有工作，則會開啟工作內容視窗。新規則已新增到工作屬性中。您可以檢視或修改規則或其他工作設定。按一下**儲存**按鈕以儲存變更。

如果選擇建立工作，請在「新工作精靈」中繼續建立工作。您在更新安裝精靈中新增的規則將顯示在「新建工作精靈」中。完成「精靈」後，*安裝所需更新並修復弱點*工作將新增到工作清單中。

建立「弱點掃描和所需更新」工作

透過弱點掃描和所需更新工作，卡巴斯基安全管理中心會收到已偵測弱點清單，與安裝在受管理裝置上協力廠商軟體必要更新的清單。

弱點掃描和所需更新工作會在快速設定精靈執行時自動建立。如果您未執行精靈，您可手動建立該工作。

若要建立弱點掃描和所需更新工作：

1. 在主功能表中，轉至 **裝置 → 工作**。
2. 點擊**新增**。

   新工作精靈啟動。遵照精靈的說明。
3. 對於卡巴斯基安全管理中心應用程式，選擇**弱點掃描和所需更新**工作類型。
4. 指定您正建立的工作的名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。
5. 選取要分配工作的裝置。
6. 若要修改預設工作設定，請啟用**完成工作建立**頁面的**建立完成時開啟工作詳情**選項。如果您不啟用該選項，工作使用預設設定建立。您可以稍後隨時修改預設設定。
7. 點擊**建立**按鈕。

   工作被建立並顯示在工作清單。

8. 按一下建立的工作的名稱以開啟工作內容視窗。

9. 在工作內容視窗中，指定一般工作設定。

10. 在**應用程式設定**頁籤中，指定以下設定：

- **搜尋 Microsoft 列出的弱點和更新**

  搜尋弱點與更新時，卡巴斯基安全管理中心會使用適用 Microsoft 更新的資訊（來自 Microsoft 更新來源），這些更新都是當下可取得的資訊。

  例如，如果您對 Microsoft 更新和協力廠商應用程式更新有不同設定與不同工作，您可能會需要停用此選項。

  預設情況下已啟用該選項。

  有關可選 Microsoft Windows 更新的資訊未被傳送至管理伺服器。

- **連線更新伺服器更新資料**

  受管理裝置上的 Windows Update 代理程式會連線至 Microsoft 更新來源。以下伺服器會以 Microsoft 更新來源運作：

  - 卡巴斯基安全管理中心管理伺服器（請參閱網路代理政策的設定）
  - 具備 Microsoft Windows Server Update Services (WSUS) 的 Windows 伺服器會佈署在貴組織的網路中
  - Microsoft Updates 伺服器

  如果啟用該選項，受管理裝置上的 Windows Update 代理程式會連線至 Microsoft 更新來源，以重新整理可應用的 Microsoft Windows Update 資訊。

  若停用此選項，受管理裝置上的 Windows Update 代理程式會使用適用 Microsoft Windows 更新的資訊，此資訊先前從 Microsoft 更新來源取得。

  到 Microsoft 更新來源的連線可能消耗資源。若您的其他工作或網路代理政策內容中的**軟體更新和弱點**區域設定一般連線至此更新來源，您可能需要停用此選項。若您不要停用此選項，為了降低伺服器過載，您可設定工作排程來隨機使工作在 360 分鐘內延遲啟動。

  預設情況下已啟用該選項。

  網路代理政策設定的以下選項組合會定義取得更新的模式：

  - 僅當在**尋找弱點和所需更新連線更新伺服器更新資料工作的屬性中**啟用了*連線到更新伺服器以更新資料弱點掃描和所需更新選項*並且**Windows Update 搜尋模式**選項在網路代理政策的設定中被設定為**主動**時，受管理裝置上的 Windows 更新代理才會連線到更新伺服器以獲取更新。
  - 如果在執行*弱點掃描*工作時不需要網路代理來啟動與 Microsoft Windows 更新來源的連線並下載更新，則可以將**Windows Update 搜尋模式**選項設為**被動**，同時**連線更新伺服器更新資料**選項必須保持啟用狀態。這可讓您節省資源並使用先前收到的 Windows 更新來掃描弱點。如果您設定以不同方式接收 Microsoft Windows 更新，則可以使用被動模式。如果未以其他方式設定接收 Microsoft Windows 更新，請勿將**Windows Update 搜尋模式**選項設為**被動**，因為在這種情況下，將永遠不會收到有關更新的資訊。
  - 無論**連線更新伺服器更新資料**選項是何狀態（啟用還是停用），只要 **Windows Update 搜尋模式**選項被設定為**已停用**，卡巴斯基安全管理中心便不會請求任何更新資訊。

- **搜尋 Kaspersky 列出的第三方弱點和更新**

如果啟用該選項，卡巴斯基安全管理中心在 Windows 登錄檔和**指定檔案系統中應用程式進階搜尋的路徑**下指定的資料夾中搜尋弱點和協力廠商應用程式所需更新（由非 Kaspersky 和 Microsoft 軟體供應商製作的應用程式）。支援的協力廠商應用程式的完整清單由 Kaspersky 管理。

如果停用該選項，卡巴斯基安全管理中心不為協力廠商應用程式尋找弱點和所需更新。例如，如果您有帶有不同 Microsoft Windows 更新和協力廠商應用程式更新設定的不同工作，您可能想要停用該選項。

預設情況下已啟用該選項。

- **指定檔案系統中應用程式進階搜尋的路徑**

  卡巴斯基安全管理中心搜尋需要修復弱點和安裝更新的協力廠商應用程式。您可以使用系統變數。

  指定應用程式安裝資料夾。預設下，清單包含大多數應用程式所安裝的系統資料夾。

- **啟用進階診斷**

  如果啟用該功能，即便寫入偵錯檔案在卡巴斯基安全管理中心遠端診斷公用程式中對網路代理停用，網路代理也寫入偵錯檔案。偵錯輪流寫入兩個檔案中；兩個檔案的最大大小由**進階診斷檔案的最大大小 (MB)**值決定。當兩個檔案都滿時，網路代理再次開始寫入它們。帶有偵錯的檔案儲存在 %WINDIR%\Temp 資料夾。這些檔案在遠端診斷公用程式中可以被存取，您可以在那裡下載或刪除它們。

  如果停用該功能，網路代理根據卡巴斯基安全管理中心遠端診斷公用程式中的設定寫入偵錯。沒有附加偵錯被寫入。

  當建立工作時，您不必啟用進階診斷。您可能想要使用該功能，如果，例如，工作在一些裝置上失敗且您想要在另一個工作執行期間獲取額外資訊。

  預設情況下已停用該選項。

- **進階診斷檔案的最大大小 (MB)**

  預設值是 100 MB，可用值介於 1 MB 和 2,048 MB 之間。當您所傳送的進階診斷檔案資訊不足以定位問題時，您可能被 Kaspersky 技術支援專家需求變更預設值。

11. 點擊**儲存**按鈕。

工作被建立和配置。

若工作結果包含 0x80240033「Windows 更新代理錯誤 80240033（「無法下載產品授權期限」）」警告，您可以透過 Windows 登錄資料解決此問題。

「弱點掃描和所需更新」工作設定

*弱點掃描和所需更新*工作會在快速設定精靈執行時自動建立。如果您未執行精靈，您可手動建立該工作。

除了一般工作設定外，您可在建立*弱點掃描和所需更新*工作，或在之後設定已建立工作的內容時，指定以下設定：

- **搜尋 Microsoft 列出的弱點和更新**

  搜尋弱點與更新時，卡巴斯基安全管理中心會使用適用 Microsoft 更新的資訊（來自 Microsoft 更新來源），這些更新都是當下可取得的資訊。

  例如，如果您對 Microsoft 更新和協力廠商應用程式更新有不同設定與不同工作，您可能會需要停用此選項。

  預設情況下已啟用該選項。

  有關可選 Microsoft Windows 更新的資訊未被傳送至管理伺服器。

- **連線更新伺服器更新資料**

  受管理裝置上的 Windows Update 代理程式會連線至 Microsoft 更新來源。以下伺服器會以 Microsoft 更新來源運作：

  - 卡巴斯基安全管理中心管理伺服器（請參閱網路代理政策的設定）
  - 具備 Microsoft Windows Server Update Services (WSUS) 的 Windows 伺服器會佈署在貴組織的網路中
  - Microsoft Updates 伺服器

  如果啟用該選項，受管理裝置上的 Windows Update 代理程式會連線至 Microsoft 更新來源，以重新整理可應用的 Microsoft Windows Update 資訊。

  若停用此選項，受管理裝置上的 Windows Update 代理程式會使用適用 Microsoft Windows 更新的資訊，此資訊先前從 Microsoft 更新來源取得。

  到 Microsoft 更新來源的連線可能消耗資源。若您的其他工作或網路代理政策內容中的**軟體更新和弱點**區域設定一般連線至此更新來源，您可能需要停用此選項。若您不要停用此選項，為了降低伺服器過載，您可設定工作排程來隨機使工作在 360 分鐘內延遲啟動。

  預設情況下已啟用該選項。

  網路代理政策設定的以下選項組合會定義取得更新的模式：

  - 僅當在**尋找弱點和所需更新連線更新伺服器更新資料工作的屬性中**啟用了*連線到更新伺服器以更新資料弱點掃描和所需更新選項*並且**Windows Update 搜尋模式**選項在網路代理政策的設定中被設定為**主動**時，受管理裝置上的 Windows 更新代理才會連線到更新伺服器以獲取更新。
  - 如果在執行*弱點掃描*工作時不需要網路代理來啟動與 Microsoft Windows 更新來源的連線並下載更新，則可以將**Windows Update 搜尋模式**選項設為**被動**，同時**連線更新伺服器更新資料**選項必須保持啟用狀態。這可讓您節省資源並使用先前收到的 Windows 更新來掃描弱點。如果您設定以不同方式接收 Microsoft Windows 更新，則可以使用被動模式。如果未以其他方式設定接收 Microsoft Windows 更新，請勿將**Windows Update 搜尋模式**選項設為**被動**，因為在這種情況下，將永遠不會收到有關更新的資訊。
  - 無論**連線更新伺服器更新資料**選項是何狀態（啟用還是停用），只要 **Windows Update 搜尋模式**選項被設定為**已停用**，卡巴斯基安全管理中心便不會請求任何更新資訊。

- **搜尋 Kaspersky 列出的第三方弱點和更新**

  如果啟用該選項，卡巴斯基安全管理中心在 Windows 登錄檔和**指定檔案系統中應用程式進階搜尋的路徑**下指定的資料夾中搜尋弱點和協力廠商應用程式所需更新（由非 Kaspersky 和 Microsoft 軟體供應商製作的應用程式）。支援的協力廠商應用程式的完整清單由 Kaspersky 管理。

  如果停用該選項，卡巴斯基安全管理中心不為協力廠商應用程式尋找弱點和所需更新。例如，如果您有帶有不同 Microsoft Windows 更新和協力廠商應用程式更新設定的不同工作，您可能想要停用該選項。

  預設情況下已啟用該選項。

- **指定檔案系統中應用程式進階搜尋的路徑**

  卡巴斯基安全管理中心搜尋需要修復弱點和安裝更新的協力廠商應用程式。您可以使用系統變數。

  指定應用程式安裝資料夾。預設下，清單包含大多數應用程式所安裝的系統資料夾。

- **啟用進階診斷**

  如果啟用該功能，即便寫入偵錯檔案在卡巴斯基安全管理中心遠端診斷公用程式中對網路代理停用，網路代理也寫入偵錯檔案。偵錯輪流寫入兩個檔案中；兩個檔案的最大大小由**進階診斷檔案的最大大小 (MB)**值決定。當兩個檔案都滿時，網路代理再次開始寫入它們。帶有偵錯的檔案儲存在 %WINDIR%\Temp 資料夾。這些檔案在遠端診斷公用程式中可以被存取，您可以在那裡下載或刪除它們。

  如果停用該功能，網路代理根據卡巴斯基安全管理中心遠端診斷公用程式中的設定寫入偵錯。沒有附加偵錯被寫入。

  當建立工作時，您不必啟用進階診斷。您可能想要使用該功能，如果，例如，工作在一些裝置上失敗且您想要在另一個工作執行期間獲取額外資訊。

  預設情況下已停用該選項。

- **進階診斷檔案的最大大小 (MB)**

  預設值是 100 MB，可用值介於 1 MB 和 2,048 MB 之間。當您所傳送的進階診斷檔案資訊不足以定位問題時，您可能被 Kaspersky 技術支援專家需求變更預設值。

工作排程的建議

排程*弱點掃描和所需更新*工作時，請確保啟用**執行略過的工作**與**使用工作啟動自動隨機延遲**兩個選項。

依預設，*弱點掃描和所需更新*工作設定為手動啟動。如果組織的工作規則要在此時關閉所有裝置，*弱點掃描和所需更新*工作將在裝置再次開啟電源時執行，意即，在星期三早上。此活動可能不是必須的，因為弱點掃描可能增加 CPU 和磁碟子系統負載。您必須根據組織的工作規則為該工作設定最方便的排程。

建立安裝必要更新並修復弱點工作

*安裝所需更新並修復弱點*工作僅在有弱點和修補程式程序管理產品授權下才可使用。

*安裝所需更新並修復弱點*工作會用來更新與修復協力廠商軟體中的弱點，包含安裝在受管理裝置上的 Microsoft 軟體。此工作可讓您根據特定規則安裝多項更新並修復多個弱點。

若要使用*安裝所需更新並修復弱點*工作安裝更新或修復弱點，您可進行以下一項操作：

- 執行更新安裝精靈或弱點修復精靈。
- 建立*安裝所需更新並修復弱點*工作。
- 對現有*安裝所需更新並修復弱點*工作新增安裝更新規則。

要建立安裝所需更新並修復弱點工作：

1. 在主功能表中，轉至 **裝置 → 工作**。
2. 點擊**新增**。

   新工作精靈啟動。遵照精靈的說明。
3. 對於卡巴斯基安全管理中心應用程式，選擇**安裝所需更新並修復弱點**工作類型。

   如果沒有顯示該工作，請檢查您的帳戶是否具有**系統管理**：**弱點和修補程式管理**功能區域的**讀取**、**修改**和**執行**權限。如果沒有這些存取權限，您就不能建立及設定*安裝所需更新並修復弱點*的工作。
4. 指定您正建立的工作的名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。
5. 選取要分配工作的裝置。

6. 指定更新安裝的規則，然後指定以下設定：

- **在裝置重新啟動或關閉時開始安裝**

  如果啟用該選項，更新在裝置被重新啟動或關閉時安裝。否則，更新根據排程安裝。

  如果安裝更新可能影響裝置效能則使用該選項。

  預設情況下已停用該選項。

- **安裝所需的一般系統元件**

  如果啟用該選項，在安裝更新之前，應用程式自動安裝所需的所有一般系統元件（先決條件）。例如，這些先決條件可以是作業系統更新。

  如果停用該選項，您可能必須手動安裝先決條件。

  預設情況下已停用該選項。

- **更新過程中允許安裝新的應用程式版本**

  如果啟用該**選項**，如果更新導致軟體應用程式新版本的安裝，更新將被允許。

  如果停用該選項，軟體不被升級。您可以稍後手動或透過其他工作安裝軟體的新版本。例如，如果公司基礎架構不被新軟體版本支援，或者如果您想要在測試基礎架構中檢查升級，您可能使用該選項。

  預設情況下已啟用該選項。

  升級應用程式可能導致安裝在用戶端裝置上的獨立應用程式功能異常。

- **下載更新到裝置而不安裝**

  如果啟用該選項，應用程式下載更新到裝置但是不自動安裝它們。您可以稍後手動安裝下載的更新。

  Microsoft 更新被下載到系統 Windows 儲存。協力廠商應用程式更新（由非 Kaspersky 和 Microsoft 軟體供應商製作的應用程式）會下載到在**下載更新資料夾**欄位指定的資料夾。

  如果停用該選項，更新被自動安裝到裝置。

  預設情況下已停用該選項。

- **下載更新資料夾**

  該資料夾用於下載協力廠商應用程式（由非 Kaspersky 和 Microsoft 軟體供應商製作的應用程式）更新。

- **啟用進階診斷**

如果啟用該功能，即便寫入偵錯檔案在卡巴斯基安全管理中心遠端診斷公用程式中對網路代理停用，網路代理也寫入偵錯檔案。偵錯輪流寫入兩個檔案中；兩個檔案的最大大小由**進階診斷檔案的最大大小 (MB)**值決定。當兩個檔案都滿時，網路代理再次開始寫入它們。帶有偵錯的檔案儲存在 %WINDIR%\Temp 資料夾。這些檔案在遠端診斷公用程式中可以被存取，您可以在那裡下載或刪除它們。

如果停用該功能，網路代理根據卡巴斯基安全管理中心遠端診斷公用程式中的設定寫入偵錯。沒有附加偵錯被寫入。

當建立工作時，您不必啟用進階診斷。您可能想要使用該功能，如果，例如，工作在一些裝置上失敗且您想要在另一個工作執行期間獲取額外資訊。

預設情況下已停用該選項。

- **進階診斷檔案的最大大小 (MB)**

  預設值是 100 MB，可用值介於 1 MB 和 2,048 MB 之間。當您所傳送的進階診斷檔案資訊不足以定位問題時，您可能被 Kaspersky 技術支援專家需求變更預設值。

7. 指定作業系統重新啟動設定：

- **不重新啟動裝置**

  用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

- **重新啟動裝置**

  如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

- **提示使用者操作**

  用戶端裝置螢幕上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。該選項適用於使用者必須可以選取最方便的時間進行重新啟動的工作站。

  預設情況下已選定此選項。

- **重複提示間隔（分鐘）**

  如果啟用該選項，應用程式以指定頻率提示使用者重新啟動作業系統。

  預設情況下已啟用該選項。預設間隔是 5 分鐘。可用值介於 1 和 1440 分鐘之間。

  如果停用該選項，提示僅顯示一次。

- **在該時間後重新啟動（分鐘）**

  提示使用者之後，應用程式在指定時間間隔後強制作業系統重新啟動。

  預設情況下已啟用該選項。預設延時是 30 分鐘。可用值介於 1 和 1440 分鐘之間。

- **在此時間後強制關閉封鎖連線中的應用程式 (分鐘)**

  使用者裝置鎖定時，程式以強制模式關閉（指定不活動間隔之後自動鎖定，或手動鎖定）。

  如果啟用此選項，一旦輸入區域指定的時間間隔結束，鎖定裝置上的程式以強制模式關閉。

  如果停用此選項，鎖定裝置上的程式將不會關閉。

  預設情況下已停用該選項。

8. 若要修改預設工作設定，請啟用**完成工作建立**頁面的**建立完成時開啟工作詳情**選項。如果您不啟用該選項，工作使用預設設定建立。您可以稍後隨時修改預設設定。

9. 點擊**完成**按鈕。

   工作被建立並顯示在工作清單。

10. 按一下建立的工作的名稱以開啟工作內容視窗。

11. 在工作內容視窗中，依需求指定一般工作設定。

12. 點擊**儲存**按鈕。

    工作被建立和配置。

若工作結果包含 0x80240033「Windows 更新代理錯誤 80240033（「無法下載產品授權期限」）」警告，您可以透過 Windows 登錄資料解決此問題。

新增安裝更新的規則

此功能僅在有弱點和修補程式管理產品授權下才可使用。

使用*安裝所需更新並修復弱點*工作安裝軟體更新或修復軟體弱點時，您必須指定安裝更新的規則。這些規則決定要安裝的更新和要修復的弱點。

精確設定會視您是否建立 Microsoft 應用程式、協力廠商應用程式（由非 Kaspersky 和 Microsoft 軟體供應商製作的應用程式）、或所有應用程式更新的規則而定。當新增 Windows Update 更新或協力廠商應用程式的更新規則時，您可以選取特定的應用程式和您要安裝更新的應用程式版本。當新增所有更新的規則時，您可以選取要安裝的特定更新，以及要透過安裝更新而修復的弱點。

您可以透過以下方式建立更新的安裝規則：

- 透過在建立新安裝所需更新並修復弱點工作時新增規則。
- 透過在現有*安裝所需更新並修復弱點*工作屬性視窗的**應用程式設定**索引標籤上新增規則。
- 透過更新安裝精靈或弱點修復精靈。

若要為所有更新建立新規則：

1. 點擊**新增**按鈕。

   規則建立精靈開始。使用**下一步**按鈕進行精靈。

2. 在**規則類型**頁面上，選擇**所有更新的規則**。

3. 在**一般標準**頁面，使用下拉清單指定以下設定：

- **要安裝的更新集**

  選取必須在用戶端裝置上安裝的更新：

  - **僅安裝批准的更新**。這僅安裝批准的更新。
  - **安裝所有更新（除了拒絕的）**。這安裝帶有*已批准*或*未定義*批准狀態的更新。
  - **安裝所有更新（包含拒絕的）**。這安裝所有更新，無論什麼批准狀態。警惕選取該選項。例如，如果您想要在測試基礎架構中檢查一些被拒絕的更新的安裝，使用該選項。

- **修復弱點的時機為嚴重等級大於或等於**

  有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

  如果啟用該選項，更新僅修復 Kaspersky 設定的安全等級等於或高於清單中選定的值（**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

  如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

  預設情況下已停用該選項。

4. 在**更新**頁面，選取要安裝的更新：

- **安裝所有合適的更新**

  安裝滿足在精靈中**一般標準**頁面指定標準的所有軟體更新。預設選取。

- **僅安裝清單中的更新**

  僅安裝您從清單中手動選取的軟體更新。該清單包含所有可用軟體更新。

  例如，您可能想要在以下情況下選取特定更新：要在測試環境中檢查它們的安裝、要僅更新嚴重應用程式、或者要僅更新特定應用程式。

  - **自動安裝所選更新安裝時需要的所有先前應用程式更新**

    如果在安裝所選更新需要時，您同意安裝暫時應用程式版本，保持該選項被啟用。

    如果停用該選項，僅選定的應用程式版本被安裝。如果您想直截了當地更新應用程式，而不嘗試安裝增量版本，請停用該選項。如果安裝所選更新不能不安裝先前版本的應用程式，應用程式更新失敗。

    例如，您在裝置上安裝了應用程式的版本 3，您想更新它到版本 5，但是該應用程式的版本 5 僅可以在版本 4 之上安裝。如果啟用該選項，軟體先安裝版本 4，然後安裝版本 5。如果停用該選項，軟體更新應用程式失敗。

    預設情況下已啟用該選項。

5. 在**弱點**頁面，選取將由安裝所選更新修復的弱點。

- **修復所有符合其他標準的弱點**

  修復滿足在精靈中**一般標準**頁面指定標準的所有弱點。預設選取。

- **僅修復清單中的弱點**

  僅修復您手動從清單中選取的弱點。清單包含所有偵測到的弱點。

  例如，您可能想要在以下情況下選取特定弱點：要在測試環境中檢查它們的修復、要僅修復嚴重應用程式中的弱點、或者要僅修復特定應用程式中的弱點。

6. 在**名稱**頁面，指定您正在建立的規則名稱。您可以稍後在所建立工作的內容視窗的**設定**區域變更該名稱。

「規則建立精靈」完成操作後，系統會建立新規則並顯示在「新工作精靈」或工作屬性的欄位中。

若要為 Windows Update 更新建立新規則：

1. 點擊**新增**按鈕。

   規則建立精靈開始。使用**下一步**按鈕進行精靈。

2. 在**規則類型**頁面上，選擇 **Windows Update 的規則**。

3. 在**一般標準**頁面中，指定以下設定：

- **要安裝的更新集**

  選取必須在用戶端裝置上安裝的更新：

  - **僅安裝批准的更新**。這僅安裝批准的更新。
  - **安裝所有更新（除了拒絕的）**。這安裝帶有*已批准*或*未定義*批准狀態的更新。
  - **安裝所有更新（包含拒絕的）**。這安裝所有更新，無論什麼批准狀態。警惕選取該選項。例如，如果您想要在測試基礎架構中檢查一些被拒絕的更新的安裝，使用該選項。

- **修復弱點的時機為嚴重等級大於或等於**

  有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

  如果啟用該選項，更新僅修復 Kaspersky 設定的安全等級等於或高於清單中選定的值（**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

  如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

  預設情況下已停用該選項。

- **修復弱點的時機為 MSRC 嚴重等級大於**

  有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

  如果啟用該選項，更新僅修復 Microsoft Security Response Center (MSRC) 設定的安全等級等於或高於清單中選定的值（**低**、**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

  如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

  預設情況下已停用該選項。

4. 在**應用程式**頁面，選取您要安裝更新的應用程式和應用程式版本。預設情況下選定所有應用程式。

5. 在**更新類別**頁面，選取要安裝的更新類別。這些類別與 Microsoft Update Catalog 中的類別相同。預設情況下選定所有類別。

6. 在**名稱**頁面，指定您正在建立的規則名稱。您可以稍後在所建立工作的內容視窗的**設定**區域變更該名稱。

「規則建立精靈」完成操作後，系統會建立新規則並顯示在「新工作精靈」或工作屬性的欄位中。

若要為協力廠商應用程式更新建立規則：

1. 點擊**新增**按鈕。

   規則建立精靈開始。使用**下一步**按鈕進行精靈。

2. 在**規則類型**頁面上，選擇**協力廠商更新的規則**。

3. 在**一般標準**頁面中，指定以下設定：

- **要安裝的更新集**

  選取必須在用戶端裝置上安裝的更新：

  - **僅安裝批准的更新**。這僅安裝批准的更新。
  - **安裝所有更新（除了拒絕的）**。這安裝帶有*已批准*或*未定義*批准狀態的更新。
  - **安裝所有更新（包含拒絕的）**。這安裝所有更新，無論什麼批准狀態。警惕選取該選項。例如，如果您想要在測試基礎架構中檢查一些被拒絕的更新的安裝，使用該選項。

- **修復弱點的時機為嚴重等級大於或等於**

  有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

  如果啟用該選項，更新僅修復 Kaspersky 設定的安全等級等於或高於清單中選定的值（**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

  如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

  預設情況下已停用該選項。

4. 在**應用程式**頁面，選取您要安裝更新的應用程式和應用程式版本。預設情況下選定所有應用程式。

5. 在**名稱**頁面，指定您正在建立的規則名稱。您可以稍後在所建立工作的內容視窗的設定區域變更該名稱。

「規則建立精靈」完成操作後，系統會建立新規則並顯示在「新工作精靈」或工作屬性的欄位中。

建立安裝 Windows Update 更新工作

*安裝 Windows Update 更新*工作可讓您在受管理裝置上，安裝由 Windows Update 服務提供的軟體更新。

如果您沒有弱點和修補程式程序管理產品授權，則無法建立 *安裝 Windows Update 更新* 類型的新工作。若要安裝新更新，您可以將其新增到現有的*安裝 Windows Update 更新*工作。建議您使用*安裝所需更新並修復弱點*工作而不是*安裝 Windows Update 更新*工作。*安裝所需更新並修復弱點*工作可讓您根據定義的規則自動安裝多個更新並修復多個弱點。此外，此工作可讓您安裝 Microsoft 以外的軟體供應商更新。

在受管理裝置上更新協力廠商應用程式或修復協力廠商應用程式中的弱點時，可能需要使用者互動。例如，若協力廠商應用程式目前開啟，可能會提示使用者關閉協力廠商應用程式。

若要建立安裝 Windows Update 更新的工作：

1. 在主功能表中，轉至 **裝置 → 工作**。

2. 點擊**新增**。

   新工作精靈啟動。使用**下一步**按鈕進行精靈。

3. 對於卡巴斯基安全管理中心應用程式，選擇**安裝 Windows Update 更新**工作類型。

4. 指定您正建立的工作的名稱。

   工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。

5. 選取要分配工作的裝置。

6. 點擊**新增**按鈕。

   更新清單隨即開啟。

7. 選取您要安裝的 Windows Update，之後點擊**確定**。

8. 指定作業系統重新啟動設定：

- **不重新啟動裝置**

  用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

- **重新啟動裝置**

  如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

- **提示使用者操作**

  用戶端裝置螢幕上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。該選項適用於使用者必須可以選取最方便的時間進行重新啟動的工作站。

  預設情況下已選定此選項。

- **重複提示間隔（分鐘）**

  如果啟用該選項，應用程式以指定頻率提示使用者重新啟動作業系統。

  預設情況下已啟用該選項。預設間隔是 5 分鐘。可用值介於 1 和 1440 分鐘之間。

  如果停用該選項，提示僅顯示一次。

- **在該時間後重新啟動（分鐘）**

  提示使用者之後，應用程式在指定時間間隔後強制作業系統重新啟動。

  預設情況下已啟用該選項。預設延時是 30 分鐘。可用值介於 1 和 1440 分鐘之間。

- **強制關閉已鎖定連線的應用程式**

  執行應用程式可能會阻止用戶端裝置重新啟動。例如，如果文件在文書處理應用程式中編輯且未儲存，應用程式不會允許裝置重新啟動。

  如果啟用該選項，鎖定裝置上的此類應用程式在裝置重新啟動前被強制關閉。結果，使用者可能遺失他們未儲存的變更。

  如果停用該選項，鎖定裝置不被重新啟動。此裝置上的工作狀態表示裝置需要重新啟動。使用者必須手動關閉所有執行在鎖定裝置上的應用程式並重新啟動這些裝置。

  預設情況下已停用該選項。

9. 指定帳戶設定：

- **預設帳戶**

  在與執行該工作的應用程式相同的帳戶下執行該工作。

  預設情況下已選定此選項。

- **指定帳戶**

  填寫**帳戶**與**密碼**欄位以指定工作要在其下執行的帳戶詳情。帳戶必須對此工作有足夠的權限。

- **帳戶**

  執行該工作的帳戶。

- **密碼**

  工作執行時使用的帳戶的密碼。

10. 若要修改預設工作設定，請啟用**完成工作建立**頁面的**建立完成時開啟工作詳情**選項。如果您不啟用該選項，工作使用預設設定建立。您可以稍後隨時修改預設設定。

11. 點擊**完成**按鈕。

    工作被建立並顯示在工作清單。

12. 按一下建立的工作的名稱以開啟工作內容視窗。

13. 在工作內容視窗中，依需求指定一般工作設定。

14. 點擊**儲存**按鈕。

工作被建立和配置。

檢視可用協力廠商軟體更新的資訊

您可檢視安裝在用戶端裝置之協力廠商軟體可用更新的清單，包含 Microsoft 軟體。

若要檢視安裝在用戶端裝置之協力廠商應用程式的可用更新清單，

在主功能表中，轉至 **操作 → 修補程式管理 → 軟體更新**。

可用更新清單被顯示。

您可指定篩選條件以檢視軟體更新的清單。點擊軟體更新清單右上角的**篩選器**圖示（ ）來管理篩選條件。您也可從軟體弱點清單上方的**預設篩選器** 下拉清單選取其中一個預設篩選條件。

要檢視更新的內容：

1. 點擊所需軟體更新的名稱。
2. 更新的屬性視窗隨即開啟，並顯示透過以下索引標籤分組的資訊：

- **一般**

  此索引標籤顯示所選更新的一般詳細資料：

  - 更新批准狀態（您可以透過在下拉清單中選取新狀態來手動更改）
  - 此更新所屬的 Windows Server Update Services (WSUS) 類別
  - 登錄更新的日期和時間
  - 建立更新的日期和時間
  - 更新的重要層級
  - 更新要求的安裝要求
  - 更新所屬的應用程式系列
  - 更新適用的應用程式
  - 更新修訂編號

- **內容**

  此索引標籤會顯示一組屬性，您可將其用來取得所選更新的詳細資訊。此集合將視更新是由 Microsoft 還是協力廠商供應商發布的而有所不同。

  該索引標籤會顯示 Microsoft 更新的以下資訊：

  - Microsoft 安全回應中心 (MSRC) 定義的更新嚴重等級
  - 連結到 Microsoft 知識庫中說明更新的文章
  - 連結到 Microsoft 安全公告中說明此更新的文章
  - 更新識別碼 (ID)

  該索引標籤顯示以下協力廠商更新的相關資訊：

  - 此更新是修補程式還是完整分發套件
  - 更新的本地化語言
  - 是自動安裝還是手動安裝更新
  - 套用後是否撤銷該更新
  - 下載更新的連結

- **裝置**

  此索引標籤顯示已安裝所選更新裝置的清單。

- **已修復弱點**

  此索引標籤顯示所選更新可以修復的弱點清單。

- **更新融合**

  此索引標籤顯示相同應用程式發佈之各種更新間的可能交集，即所選更新是否可以取代其他更新，反之是否可以由其他更新取代（僅適用於 Microsoft 更新）。

- **安裝該更新的工作**

  此索引標籤顯示工作清單，其範圍包括所選更新的安裝。該索引標籤還使您可以為更新建立新的遠端安裝工作。

若要檢視更新安裝的統計：

1. 選取所需軟體更新旁邊的核取方塊。
2. 點擊**更新安裝狀態統計資訊**按鈕。

   更新安裝狀態圖表隨即顯示。點擊狀態會開啟裝置清單，其更新為所選狀態。

在所選取且執行 Windows 的受管理裝置上，您可檢視已安裝之協力廠商軟體可用軟體更新的資訊，包含 Microsoft 軟體。

若要在選取的受管理裝置上，檢視已安裝的協力廠商軟體可用更新清單：

1. 在主功能表中，轉至 **裝置 → 受管理裝置**。

   受管理裝置清單隨即顯示。
2. 在受管理裝置清單中，點擊有您要檢視之協力廠商軟體更新的裝置名稱連結。

   所選裝置的屬性視窗隨即顯示。
3. 在所選裝置的內容視窗中，選取**進階**頁籤。
4. 在左窗格中，選取**可用更新**區段。若要只檢視已安裝的更新，請啟用**顯示已安裝的更新**選項。

   選取的裝置上可用協力廠商軟體更新的清單隨即顯示。

將可用軟體更新清單匯出至檔案

您可匯出協力廠商軟體更新清單，包含 Microsoft 軟體，目前可以 CSV 或 TXT 檔案顯示。您可使用這些檔案，例如將它們傳送至您的資訊安全經理，或儲存起來以供統計使用。

若要將所有受管理裝置安裝之協力廠商軟體的可用更新清單匯出為文字檔案：

1. 在主功能表中，轉至 **操作 → 修補程式管理 → 軟體更新**。
   此頁面會顯示在所有受管理裝置上已安裝之協力廠商軟體的可用更新清單。
2. 點擊**將行匯出到 txt 檔案**或**將行匯出到 csv 檔案**按鈕，視您偏好的匯出格式而定。

內含協力廠商軟體可用更新清單的檔案，包含 Microsoft 軟體，會現在至您目前使用的裝置。

若要將所選受管理裝置安裝之協力廠商軟體的可用更新清單匯出為文字檔案：

1. 開啟所選受管理裝置之協力廠商軟體更新的清單。
2. 選取您要匯出的軟體更新。
   若要匯出完整的軟體更新清單請略過此步驟。
   若要匯出軟體更新的完整清單，僅會匯出顯示在目前頁面的更新。
   若要僅匯出安裝的更新，請選取 **顯示已安裝的更新** 核取方塊。
3. 點擊**將行匯出到 txt 檔案**或**將行匯出到 csv 檔案**按鈕，視您偏好的匯出格式而定。

含在所選受管理裝置安裝之協力廠商軟體更新清單的檔案，包含 Microsoft 軟體，會下載至您目前使用的裝置。

核准與拒絕協力廠商軟體更新

在設定*安裝所需更新並修復弱點*工作時，您可以建立一個規則，該規則要求待安裝更新具有特定狀態。例如，更新規則可允許以下安裝：

- 僅核准的更新
- 僅核准且未定義的更新
- 無論更新狀態為何的所有更新

您可以批准必須安裝的更新並拒絕不能安裝的更新。

對於少量更新而言，使用*已批准*狀態來管理更新安裝非常有效。若要安裝多個更新，請使用可在*安裝所需更新並修復弱點*工作中設定的規則。建議您僅為那些不符合規則中指定條件的特定更新設定*已批准*狀態。當您手動批准大量更新時，管理伺服器的效能下降，這可能導致伺服器過載。

要批准或拒絕一個或幾個更新：

1. 在主功能表中，轉至 **操作 → 修補程式管理 → 軟體更新**。
   可用更新清單被顯示。
2. 選取您要批准或拒絕的更新。
3. 點擊**批准**以核准選取的更新或**拒絕**以拒絕選取的更新。
   預設值是*未定義*。

選取的更新有您定義的狀態。

您也可以選擇在特定更新的屬性中更改批准狀態。

批准或拒絕其屬性中的更新：

1. 在主功能表中，轉至 **操作 → 修補程式管理 → 軟體更新**。
   可用更新清單被顯示。
2. 點擊您要批准或拒絕的更新名稱。
   更新屬性視窗隨即開啟。
3. 在**一般**區段，透過更改**更新批准狀態**選項來選取更新狀態。您可以選取*已批准*、*已拒絕*或*未定義*狀態。
4. 按一下**儲存**按鈕以儲存變更。

選取的更新有您定義的狀態。

如果您為協力廠商軟體更新設定了**已拒絕**狀態，則已計畫但未安裝這些更新的裝置將不會安裝這些更新。更新將保持在已將其安裝的裝置上。如果您必須刪除它們，您可以在本機手動刪除它們。

建立執行 Windows Update 同步的工作

*執行 Windows Update 同步*工作僅在有弱點和修補程式程序管理產品授權下才可使用。

*執行 Windows Update 同步*如果要將管理伺服器作為 WSUS 伺服器，則需要執行此工作。在這種情況下，管理伺服器會將 Windows 更新下載到資料庫，並透過網路代理以集中模式向用戶端裝置的 Windows Update 提供更新。如果網路不使用 WSUS 伺服器，例如每個用戶端裝置都從外部伺服器獨立下載 Microsoft 更新。

*執行 Windows Update 同步*作業僅會從 Microsoft 伺服器下載中繼資料。當您執行更新安裝工作時，卡巴斯基安全管理中心會下載更新，並且僅下載您選擇安裝的那些更新。

執行**執行 Windows Update 同步**工作時，應用程式會從 Microsoft 更新伺服器收到目前更新清單。下一步，卡巴斯基安全管理中心編輯過期更新清單。在下次啟動**弱點掃描和所需更新**工作時，卡巴斯基安全管理中心會篩選所有過期更新並為其設定刪除時間。在下次啟動**執行 Windows Update 同步**工作時，所有 30 天前篩選出的過期更新都會被刪除。卡巴斯基安全管理中心也檢查刪除了 180 天以上的過期更新，並刪除更早的更新。

當**執行 Windows Update 同步**工作完成且過期更新被刪除時，資料庫可能仍會在 %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles 檔案中保留刪除的更新的雜湊碼和對應檔案（如果已早期下載這些項目）。您可以執行**管理伺服器維護**工作以從資料庫和對應檔案中刪除這些過期的記錄。

要建立執行 Windows Update 同步工作：

1. 在主功能表中，轉至 **裝置 → 工作**。
2. 點擊**新增**。
   新工作精靈啟動。遵照精靈的說明。
3. 對於卡巴斯基安全管理中心應用程式，選擇**執行 Windows Update 同步**工作類型。
4. 指定您正建立的工作的名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。

5. 如果要在執行工作時下載快速更新文件，請啟用**下載明示安裝檔案**選項。

   在卡巴斯基安全管理中心與 Microsoft Windows Update Servers 同步更新時，所有檔案的資訊被儲存在管理伺服器資料庫。所有更新所需的檔案也在與 Windows 更新代理的互動過程中被下載到磁碟機。特別地，卡巴斯基安全管理中心儲存快速更新檔案的資訊到資料庫並在必要時下載它們。下載快速更新檔案導致磁碟機空間的減少。

   為了避免磁碟空間減少以及流量降低，請取消選取所有**下載明示安裝檔案**的核取方塊。

6. 選取您要下載更新的應用程式。

   如果清空**所有應用程式**核取方塊，更新將為所有現有應用程式以及可能在將來發佈的應用程式下載。

7. 選擇要下載到管理伺服器的更新類別。

   如果選取**所有類別**核取方塊，更新將為所有現有更新類別以及可能在將來出現的類別下載。

8. 選取要下載到管理伺服器的更新的本地化語言。您可以選取以下其中一個方法：

   - **下載包含新語言在內的所有語言**

     如果選定了該方塊，所有可用的更新中文化語言都將被下載至管理伺服器。預設情況下已選定此選項。

   - **下載選取語言**

     如果選定了該方塊，您可以從更新的中文化語言清單中進行選取以便下載到管理伺服器中。

9. 指定執行工作時要使用的帳戶。您可以選取以下其中一個方法：

   - **預設帳戶**

     在與執行該工作的應用程式相同的帳戶下執行該工作。

     預設情況下已選定此選項。

   - **指定帳戶**

     填寫**帳戶**與**密碼**欄位以指定工作要在其下執行的帳戶詳情。帳戶必須對此工作有足夠的權限。

10. 若要修改預設工作設定，請啟用**完成工作建立**頁面的**建立完成時開啟工作詳情**選項。如果您不啟用該選項，工作使用預設設定建立。您可以稍後隨時修改預設設定。

11. 點擊**完成**按鈕。

    工作被建立並顯示在工作清單。

12. 按一下建立的工作的名稱以開啟工作內容視窗。

13. 在工作內容視窗中，依需求指定一般工作設定。

14. 點擊**儲存**按鈕。

工作被建立和配置。

自動更新協力廠商應用程式

某些協力廠商應用程式可以自動更新。應用程式供應商會定義應用程式是否支持自動更新功能。如果受管理裝置上安裝的協力廠商應用程式支援自動更新，則可以在應用程式屬性中指定自動更新設定。更改自動更新設定後，網路代理會在安裝了應用程式的每個受管理裝置上套用新設定。

自動更新設定獨立於其他物件和弱點和修補程式管理功能的設定。例如，此設定會以更新批准狀態或更新安裝工作為依據，例如*安裝所需更新並修復弱點*、*安裝 Windows Update 更新*和*修復弱點*。

若要為協力廠商應用程式配置自動更新設定：

1. 在主功能表中，轉至 **操作 → 協力廠商應用程式 → 應用程式登錄資料**。
2. 點擊要為其更改自動更新設定的應用程式名稱。

   若要簡化搜尋，您可以依照**自動更新狀態**欄篩選清單。

   應用程式屬性視窗隨即開啟。
3. 在**一般**區段中，為以下設定選取一個值：

   自動更新狀態

   您可以選取以下其中一個方法：

   - **未定義**

     自動更新功能已停用。卡巴斯基安全管理中心透過以下工作來安裝協力廠商應用程式更新：*安裝所需更新並修復弱點*、*安裝 Windows Update 更新*和*修復弱點*。
   - **允許**

     供應商發布該應用程式的更新後，此更新將自動安裝在受管理裝置上。不需要進一步操作。
   - **已封鎖**

     這些更新不會自動安裝。卡巴斯基安全管理中心透過以下工作來安裝協力廠商應用程式更新：*安裝所需更新並修復弱點*、*安裝 Windows Update 更新*和*修復弱點*。
4. 按一下**儲存**按鈕以儲存變更。

自動更新設定將套用在所選應用程式。

情境：更新協力廠商軟體

本節提供在用戶端裝置安裝更新協力廠商軟體的情境。協力廠商軟體包含來自 Microsoft 和其他軟體廠商的應用程式。Microsoft 應用程式的更新會由 Windows Update 服務提供。

先決條件

管理伺服器必須連線到網際網路才能安裝除了 Microsoft 軟體之外的協力廠商軟體更新。

預設情況下，管理伺服器不需要網際網路連線即可在受管理裝置上安裝 Microsoft 軟體更新。例如，受管理裝置可以直接從 Microsoft Update 伺服器下載 Microsoft 軟體更新，也可以從具有組織網路中佈署的 Microsoft Windows Server Update Services (WSUS) 的 Windows Server 下載 Microsoft 軟體更新。將管理伺服器用作 WSUS 伺服器時，必須將管理伺服器連線到網際網路。

階段

更新協力廠商軟體採分階段進行：

1. **搜尋所需更新**

   若要尋找受管理裝置必要的協力廠商軟體更新，請執行*弱點掃描和所需更新*工作。完成此工作時，卡巴斯基安全管理中心會收到偵測到的弱點清單，以及安裝於您在工作內容指定裝置上已安裝軟體需要的更新。

   *弱點掃描和所需更新*工作會由管理伺服器快速設定精靈自動建立。若您未執行該精靈，請建立工作或立即執行快速啟動精靈。

   說明：

   - 管理主控台：掃描應用程式是否有弱點，排程尋找弱點和所需更新的工作
   - 卡巴斯基安全管理中心網頁主控台：建立弱點掃描和所需更新工作、尋找弱點和所需更新的工作設定

2. **分析已知更新清單**

   檢視**軟體更新**清單並決定要安裝的更新。若要檢視各更新的詳細資訊，請按一下清單中的更新名稱。對於清單中的各個更新，您也可檢視用戶端裝置上更新的統計資料。

   說明：

   - 管理主控台：檢視可用更新資訊
   - 卡巴斯基安全管理中心網頁主控台：檢視可用協力廠商軟體更新的資訊

3. **配置更新的安裝**

   當卡巴斯基安全管理中心收到協力廠商軟體更新清單時，您可使用*安裝必要更新並修復弱點*工作或*安裝 Windows Update 更新*，以在用戶端裝置安裝這些更新。建立其中一種這類工作。您可在**工作**頁籤或使用**軟體更新**清單建立這類工作。

   *安裝所需更新並修復弱點*工作用來安裝 Microsoft 應用程式的更新，包括由 Windows Update 服務提供的更新，以及其他廠商軟體的更新。請注意，只有當您有弱點和修補程式管理功能的授權時，才可建立此工作。

   *安裝 Windows Update 更新*工作不需要產品授權，但僅可用來安裝 Windows Update 更新。

   若要安裝一些軟體更新，您必須接受安裝軟體的最終使用者產品授權協議 (EULA)。若您拒絕 EULA，則無法安裝該軟體更新。

   您可依排程啟動更新安裝工作。指定工作排誠實，請確保更新安裝工作會在*弱點掃描和所需更新*工作完成後啟動。

   說明：

   - 管理主控台：修復應用程式中的弱點、檢視可用更新的資訊
   - 卡巴斯基安全管理中心網頁主控台：建立安裝必要更新並修復弱點工作、建立並安裝 Windows Update 更新工作、檢視可用協力廠商軟體更新的資訊

4. **排程工作**

   為確定更新清單永遠處於最新狀態，請排程*弱點掃描和所需更新*工作以不時自動執行。依預設，*弱點掃描和所需更新*工作設定為手動啟動。

若您已建立*安裝必要更新並修正弱點*工作，您可排程此工作與*弱點掃描和所需更新*工作的執行頻率相同或更少。排程*安裝 Windows Update 更新*工作時，請注意對於此工作，您必須在每次啟動此工作時定義更新清單。

排程工作時，請確定更新安裝工作會在*弱點掃描和所需更新*工作完成後啟動。

5. **核准和拒絕軟體更新（選用）**

若您已建立安裝必要更新並修復弱點工作，您可在工作內容中，指定更新安裝的規則。若您已建立安裝 Windows Update 更新工作，請略過此步驟。

對於各規則，您可定義更新來根據更新狀態進行安裝：*未定義*、*已核准*或*已拒絕*。例如，您可能要針對伺服器建立特定工作，並針對此工作設定規則，以允許僅安裝 Windows Update 更新，以及僅安裝有*已核准*狀態的更新。針對您要安裝的這些更新手動設定*已核准*狀態後。在此情況下，處於*未定義*或*已拒絕*狀態的 Windows Update 更新將不會安裝到您在工作中指定的伺服器。

對於少量更新而言，使用*已批准*狀態來管理更新安裝非常有效。若要安裝多個更新，請使用可在*安裝所需的更新和修復漏洞*工作中配置的規則。建議您僅為那些不符合規則中指定條件的特定更新設定*已批准*狀態。當您手動批准大量更新時，管理伺服器的效能下降，這可能導致伺服器過載。

預設下，下載的軟體更新具有*未定義*狀態。您可在**軟體更新**清單（**操作 → 修補程式管理 → 軟體更新**）變更狀態至*已核准*或*已拒絕*。

說明：

- 管理主控台：批准和拒絕軟體更新
- 卡巴斯基安全管理中心網頁主控台：批准和拒絕協力廠商軟體更新

6. **配置管理伺服器作為 Windows Server 更新服務 (WSUS) 伺服器（選用）運作**

依預設，Windows Update 更新會從 Microsoft 伺服器下載至受管理裝置。您可變更此設定以使用管理伺服器作為 WSUS 伺服器。在此情況下，管理伺服器會以特定頻率將更新資料與 Windows Update 同步，並以集中模式提供更新給在網路裝置的 Windows Update。

若要使用管理伺服器作為 WSUS 伺服器，您可建立執行 Windows Update 同步工作，並選取網路代理政策中的**使用管理伺服器作為 WSUS 伺服器**核取方塊。

說明：

- 管理主控台：從 Windows Update 透過管理伺服器同步更新、在網路代理政策中配置 Windows 更新
- 卡巴斯基安全管理中心網頁主控台：建立執行 Windows Update 同步工作

7. **執行更新安裝工作**

啟動*安裝所需更新並修復弱點*工作或*安裝 Windows Update 更新*工作。啟動這類工作時，更新會自動下載並安裝至受管理裝置。工作完成後，請確保工作清單出現*已成功完成*狀態。

8. **建立協力廠商軟體更新安裝結果的報告（選用）**

若要檢視更新安裝的詳細統計，請建立**協力廠商軟體更新安裝結果報告**。

說明：

- 管理主控台：建立與檢視報告
- 卡巴斯基安全管理中心網頁主控台：產生與檢視報告

結果

若已建立並設定*安裝所需更新並修復弱點*工作，更新會自動安裝在受管理裝置。系統會將新更新下載至管理伺服器儲存區，卡巴斯基安全管理中心會檢查更新是否符合更新規則中指定的條件。系統會將符合條件的所有新更新在下次工作執行時安裝。

若已建立*安裝 Windows Update 更新*工作，則系統僅會*安裝 Windows Update 更新*工作屬性中指定的這類更新。未來若要安裝下載至管理伺服器儲存區的新更新，您必須新增必要更新至現有工作的更新清單，或建立新*安裝 Windows Update 更新*工作。

修復協力廠商軟體弱點

本節說明卡巴斯基安全管理中心如何修復受管理裝置上已安裝軟體的弱點。

情境：尋找與修復協力廠商軟體弱點

本節說明在執行 Windows 的受管理裝置上尋找與修復弱點的情境。您可在作業系統與協力廠商軟體（包含 Microsoft 軟體）中尋找並修復軟體弱點。

先決條件

- 系統會將卡巴斯基安全管理中心佈署在您的組織中。
- 您組織中有執行 Windows 的受管理裝置。
- 管理伺服器需要網際網路連線才能執行以下工作：
  - 列出針對 Microsoft 軟體弱點的建議修補程式。該清單由卡巴斯基專家建立並定期更新。
  - 修復 Microsoft 軟體以外的協力廠商軟體中的漏洞。

階段

分階段尋找並修復軟體弱點：

1. **受管理裝置中已安裝軟體的掃描弱點**

   若要在受管理裝置已安裝軟體中尋找弱點，請執行*弱點掃描和所需更新*工作。完成此工作時，卡巴斯基安全管理中心會收到偵測到的弱點清單，以及安裝於您在工作內容指定裝置上已安裝軟體需要的更新。

   *弱點掃描和所需更新*工作會由卡巴斯基安全管理中心快速啟動精靈自動建立。如果您未執行精靈，請立即將其啟動或手動建立工作。

   說明：

   - 管理主控台：掃描應用程式是否有弱點，排程尋找弱點和所需更新的工作
   - 卡巴斯基安全管理中心網頁主控台：建立弱點掃描和所需更新工作、尋找弱點和所需更新的工作設定

2. **分析偵測到的軟體弱點清單**

檢視**軟體弱點**清單並決定要修復的弱點。若要檢視各弱點的詳細資訊，請按一下清單中的弱點名稱。對於清單中的各個，您也可檢視受管理裝置上弱點的統計資料。

說明：

- 管理主控台：檢視關於軟體弱點的資訊、檢視受管理裝置上弱點的統計資料
- 卡巴斯基安全管理中心網頁主控台：檢視關於軟體弱點的資訊、檢視受管理裝置上弱點的統計資料

3 設定弱點修復

偵測到軟體弱點時，您可使用*安裝所需更新並修復弱點*工作或*修復弱點*工作修復受管理裝置上的軟體弱點。

*安裝所需更新並修復弱點*工作會用來更新與修復協力廠商軟體中的弱點，包含安裝在受管理裝置上的 Microsoft 軟體。此工作可讓您根據特定規則安裝多項更新並修復多個弱點。請注意，只有當您有弱點和修補程式管理功能的授權時，才可建立此工作。為了修復軟體弱點，*安裝所需更新並修復弱點*工作會使用建議的軟體更新。

*修復弱點*工作不需要弱點與修補程式管理功能的授權選項。若要使用此工作，您必須為列於工作設定中協力廠商軟體清單的弱點指定軟體使用者修復項目。*修復弱點*工作會使用適用於 Microsoft 軟體的建議修復項目，以及適用於協力廠商軟體的使用者修復項目。

您可啟動弱點修復精靈，精靈會自動建立以下其中一種這類工作或您可手動建立其中一種這類工作。

說明：

- 管理主控台：選取適用於協力廠商軟體中弱點的使用者修復項目、修復應用程式中的弱點
- 卡巴斯基安全管理中心網頁主控台：選取適用於協力廠商軟體中弱點的使用者修復項目、修復協力廠商軟體中的弱點、建立安裝必要的更新並修復弱點工作

4 排程工作

為確定弱點清單永遠處於最新狀態，請排程*弱點掃描和所需更新*工作以不時自動執行。建議平均頻率為每週一次。

若您已建立*安裝所需更新並修復弱點*工作，您可排程與*弱點掃描和所需更新*工作的執行頻率相同會更少。排程*修復弱點*工作時，請注意，您必須在每次開始工作時，選擇 Microsoft 軟體的修復項目或指定協力廠商軟體的使用者修復項目。

排程工作時，請確定修復弱點的工作會在*弱點掃描和所需更新*工作完成後啟動。

5 忽略軟體弱點（選用）

如有需要，您可忽略所有受管理裝置，或僅忽略已選受管理裝置上要修復的軟體弱點。

說明：

- 管理主控台：忽略軟體弱點
- 卡巴斯基安全管理中心網頁主控台：忽略軟體弱點

6 執行修復弱點工作

啟動*安裝必要更新並修復弱點*工作或修復*弱點*工作。工作完成時，請確保工作清單出現*已成功完成*狀態。

7 建立修復軟體弱點的結果報告（選用）

若要檢視弱點修復的詳細統計資料，請產生弱點報告。報告會顯示未修復之軟體弱點的資訊。您已知道如何在組織中尋找與修復協力廠商軟體中的弱點（包含 Microsoft 軟體）。

說明：

- 管理主控台：建立與檢視報告

- 卡巴斯基安全管理中心網頁主控台：產生與檢視報告

8. **檢查尋找與修復協力廠商軟體中的弱點的配置**

   請確保您已完成以下項目：

   - 取得並檢閱受管理裝置上軟體弱點的清單
   - 忽略軟體弱點（如有需要）
   - 設定修復弱點的工作
   - 排程在之後啟動的工作以尋找並修復軟體弱點
   - 檢查修復軟體弱點工作是否執行

結果

若您已建立並設定*安裝所需更新並修復弱點*工作，弱點會自動在受管理裝置上修復。當工作執行時，會將可用軟體更新的清單與工作設定中指定的規則建立關聯。符合規則中條件的所有軟體更新都將會下載至管理伺服器儲存區，且安裝以修復軟體弱點。

若您已建立*修復弱點*工作，僅 Microsoft 軟體中的軟體弱點會被修復。

關於尋找與修復軟體弱點

卡巴斯基安全管理中心會在執行 Microsoft Windows 系列作業系統的受管理裝置上偵測並修復軟體弱點。作業系統和協力廠商軟體（包含 Microsoft 軟體）會偵測弱點。

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

尋找軟體弱點

為了尋找軟體弱點，卡巴斯基安全管理中心會使用來自已知弱點資料庫的特徵。此資料庫會由 Kaspersky 專家建立。資料庫會包含弱點的資訊，例如弱點敘述、弱點偵測日期、弱點嚴重等級。您可以在 Kaspersky 網站上搜尋軟體弱點詳情。

卡巴斯基安全管理中心會使用*弱點掃描和所需更新*工作尋找軟體弱點。

在某些情況下，可以使用下列任一方法修復 Microsoft Windows 作業系統中偵測到的弱點：

- 安裝作業系統更新。
- 將作業系統升級到較新版本（例如，從 Windows 10 升級到 Windows 11）。

在這種情況下，卡巴斯基安全管理中心顯示相同弱點的兩個項目。

修復軟體弱點

為了修復軟體弱點，卡巴斯基安全管理中心會使用由軟體供應上提供的軟體更新。執行以下工作後，系統會下載軟體更新中繼資料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*。此工作是為了 Kaspersky 與協力廠商軟體下載更新中繼資料。該工作由卡巴斯基安全管理中心快速啟動精靈自動建立。您只能手動建立將更新下載至管理伺服器儲存區工作。
- *執行 Windows Update 同步*。此工作是為了下載 Microsoft 軟體的更新中繼資料。

修復弱點的軟體更新可使用完整分發套件或修補程式代表。修復軟體弱點的軟體更新又稱為*修復項目*。*建議的修復項目*是指由 Kaspersky 專家建議安裝的項目。*使用者修復項目*是指由使用者手動指定安裝的項目。若要安裝使用者修復項目，您需建立包含此修復項目的安裝套件。

若您有具備弱點和修補程式管理功能的卡巴斯基安全管理中心授權，若要修復軟體弱點，您可使用*安裝所需更新並修復弱點*工作。此工作會安裝建議的修復項目來自動修復多個弱點。針對此工作，您可手動設定特定規則來修復多個弱點。

若您沒有具備弱點和修補程式管理功能的卡巴斯基安全管理中心授權，若要修復軟體弱點，您可使用*修復弱點*工作。透過使用此工作，您可透過安裝適用於 Microsoft 軟體的建議修復項目，以及適用於其他協力廠商軟體的使用者修復項目來修復弱點。

出於安全原因，卡巴斯基技術會自動掃描您使用弱點和修補程式管理功能安裝的任何協力廠商軟體更新以查找惡意軟體。這些技術用於自動檢查檔案，包括病毒掃描、靜態分析、動態分析、沙箱環境中的行為分析和機器學習。

卡巴斯基專家不會對可以使用弱點和修補程式管理功能安裝的協力廠商軟體更新進行手動分析。此外，卡巴斯基專家不會在此類更新中搜尋弱點（已知或未知）或未記錄的功能，也不會對上述段落中指定的更新以外的其他類型的更新進行分析。

在受管理裝置上更新協力廠商應用程式或修復協力廠商應用程式中的弱點時，可能需要使用者互動。例如，若協力廠商應用程式目前開啟，可能會提示使用者關閉協力廠商應用程式。

若要修復一些軟體弱點，您必須接受安裝軟體的最終使用者產品授權協議 (EULA)（若系統要求您接受 EULA）。若您拒絕 EULA，則無法修復軟體弱點。

修復協力廠商軟體弱點

取得軟體弱點清單後，您可在執行 Windows 的受管理裝置上修復軟體弱點。您可以透過建立並執行*修復弱點*工作或*安裝所需更新並修復弱點*工作來修復操作系統和協力廠商軟體（包括 Microsoft 軟體）中的軟體弱點。

在受管理裝置上更新協力廠商應用程式或修復協力廠商應用程式中的弱點時，可能需要使用者互動。例如，若協力廠商應用程式目前開啟，可能會提示使用者關閉協力廠商應用程式。

您可以建立工作，透過以下方式作為修復軟體弱點的選擇：

- 透過開啟弱點清單並指定要修復的弱點。

  結果，建立了修復軟體弱點的新工作。作為選擇，您可以將所選弱點新增到現有工作。

- 透過執行「弱點修復精靈」。

  > 「弱點修復精靈」僅在有弱點和修補程式管理產品授權下才可使用。

  此精靈簡化了修復弱點工作的建立和組態，並讓您避免建立的多餘且會重複安裝相同更新的工作。

使用弱點清單修復軟體弱點

若要修復軟體弱點：

1. 開啟弱點清單之一：

   - 要開啟一般弱點清單，請在主功能表中，前往**操作 → 修補程式管理 → 軟體弱點**。
   - 要開啟受管理裝置的弱點清單，請在主功能表中，前往**裝置 → 受管理裝置** → <device name> → **進階 → 軟體弱點**。
   - 要開啟特定應用程式的弱點清單，請在主功能表中，前往**操作 → 協力廠商應用程式 → 應用程式登錄資料** → <application name> → **弱點**。

   在協力廠商軟體的弱點清單頁面隨即顯示。

2. 選取清單中的一或多個弱點並點擊**修復弱點**按鈕。

   若沒有要修復其中一個所選弱點的建議軟體更新，則會顯示通知訊息。

   若要修復一些軟體弱點，您必須接受安裝軟體的最終使用者產品授權協議 (EULA)（若系統要求您接受 EULA）。若您拒絕 EULA，則無法修復軟體弱點。

3. 您可以選取以下其中一個方法：

   - **新工作**

     新工作精靈啟動。如果您擁有弱點和修補程式程序管理產品授權，則*安裝所需更新並修復弱點*預設會需先選取工作類型。如果您沒有產品授權，則*修復弱點*預設會需先選取工作類型。請按照精靈的步驟完成工作建立。

   - **修復弱點（新增規則到指定工作）**

     選取要向其中新增所選弱點的工作。如果您具有弱點和修補程式管理產品授權，請選取*安裝所需更新並修復弱點*工作。修復所選弱點的新規則將自動新增到所選工作中。如果您沒有產品授權，請選取*修復弱點*工作。所選弱點將新增到工作屬性中。

     工作內容視窗隨即開啟。按一下**儲存**按鈕以儲存變更。

   如果您選擇建立工作，則會建立該工作並將其顯示在以下位置的工作清單中：**裝置 → 工作**。如果您選擇將弱點新增到現有工作中，則這些弱點將儲存在工作屬性中。

要修復協力廠商軟體弱點，請啟動*安裝所需更新並修復弱點*工作或*修復弱點*工作。若您已建立*修復弱點*工作，您需手動指定軟體更新來修復工作設定中的軟體弱點清單。

使用「弱點修復精靈」修復軟體弱點

「弱點修復精靈」僅在有弱點和修補程式管理產品授權下才可使用。

要使用「弱點修復精靈」來修復軟體弱點：

1. 在主功能表中，轉至 **操作 → 修補程式管理 → 軟體弱點**。
   安裝在受管理裝置之協力廠商軟體的弱點清單頁面隨即顯示。
2. 選取您要移除之規則旁邊的核取方塊。
3. 點擊**執行修復弱點精靈**按鈕。
   弱點修復精靈啟動。**選取修復弱點工作**頁面顯示以下類型的所有現有工作清單：
   - *安裝所需更新並修復弱點*
   - *安裝 Windows Update 更新*
   - *修復弱點*

   您不能修改最後兩種工作來安裝新更新。要安裝新更新，您只能使用*安裝所需更新並修復弱點*工作。

4. 如果您希望精靈僅顯示修復所選弱點的工作，請啟用**僅顯示修復此弱點的工作**選項。

5. 選取您要新增的內容：

- 若要啟動工作，請選取工作名稱旁邊的核取方塊，然後點擊**開始**按鈕。
- 若要將新規則新增到現有工作：

  a. 選取工作名稱旁邊的核取方塊，然後點擊**新增規則**按鈕。

  b. 在開啟的頁面上，配置新規則：

  - **修復該嚴重等級的弱點規則**

    有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

    如果啟用該選項，更新僅修復 Kaspersky 設定的嚴重等級等於或高於所選更新之嚴重性（**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

    如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

    預設情況下已停用該選項。

  - **透過與所選弱點建議定義的更新類型相同的更新來修復弱點的規則**（僅適用於 Microsoft 軟體弱點）
  - **修復所選供應商應用程式中的弱點規則**（僅適用於協力廠商軟體弱點）
  - **修復所選應用程式的所有版本中的弱點的規則**（僅適用於協力廠商軟體弱點）
  - **修復所選弱點的規則**
  - **批准修復該弱點的更新**

    所選更新將被批准安裝。如果一些應用的更新安裝規則僅允許安裝批准的更新，啟用該選項。

    預設情況下已停用該選項。

  c. 點擊**新增**按鈕。

- 要建立工作：

  a. 點擊**新工作**按鈕。

  b. 在開啟的頁面上，配置新規則：

  - **修復該嚴重等級的弱點規則**

有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

如果啟用該選項，更新僅修復 Kaspersky 設定的嚴重等級等於或高於所選更新之嚴重性（**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

預設情況下已停用該選項。

- **透過與所選弱點建議定義的更新類型相同的更新來修復弱點的規則**（僅適用於 Microsoft 軟體弱點）
- **修復所選供應商應用程式中的弱點規則**（僅適用於協力廠商軟體弱點）
- **修復所選應用程式的所有版本中的弱點的規則**（僅適用於協力廠商軟體弱點）
- **修復所選弱點的規則**
- **批准修復該弱點的更新**

所選更新將被批准安裝。如果一些應用的更新安裝規則僅允許安裝批准的更新，啟用該選項。

預設情況下已停用該選項。

c. 點擊**新增**按鈕。

如果選擇啟動工作，則可以關閉精靈。該工作將在後台模式下完成。不需要進一步操作。

如果您選擇將規則新增到現有工作，則會開啟工作內容視窗。新規則已新增到工作屬性中。您可以檢視或修改規則或其他工作設定。按一下**儲存**按鈕以儲存變更。

如果選擇建立工作，請在「新工作精靈」中繼續建立工作。您在「弱點修復精靈」中新增的規則將顯示在「新工作精靈」中。完成「精靈」後，*安裝所需更新並修復弱點*工作將新增到工作清單中。

建立修復弱點工作

*修復弱點*工作可讓您修復執行 Windows 受管理裝置的軟體弱點。您可在協力廠商軟體中（包含 Microsoft 軟體）修復軟體弱點。

如果您沒有弱點和修補程式程序管理產品授權，則無法建立*修復弱點*類型的新工作。要修復新弱點，您可以將其新增到現有*修復弱點*工作。建議您使用*安裝所需更新並修復弱點*工作而不是*修復弱點*工作。*安裝所需更新並修復弱點*工作可讓您根據定義的規則自動安裝多個更新並修復多個弱點。

在受管理裝置上更新協力廠商應用程式或修復協力廠商應用程式中的弱點時，可能需要使用者互動。例如，若協力廠商應用程式目前開啟，可能會提示使用者關閉協力廠商應用程式。

建立修復弱點工作：

1. 在主功能表中，轉至 **裝置** → **工作**。
2. 點擊**新增**。

   新工作精靈啟動。使用**下一步**按鈕進行精靈。
3. 對於卡巴斯基安全管理中心應用程式，選擇**修復弱點**工作類型。
4. 指定您正建立的工作的名稱。

   工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。
5. 選取要分配工作的裝置。
6. 點擊**新增**按鈕。

   更新清單隨即開啟。
7. 選取您要修復的弱點，之後點擊**確定**。

   Microsoft 軟體弱點通常有建議的修復程序。無需對這些程序進行其他操作。對於其他供應商的軟體弱點，您首先需要為要修復的每個弱點指定一個使用者修復程序。之後，您將能夠將這些弱點新增到*修復弱點*工作。

8. 指定作業系統重新啟動設定：

- **不重新啟動裝置**

  用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

- **重新啟動裝置**

  如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

- **提示使用者操作**

  用戶端裝置螢幕上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。該選項適用於使用者必須可以選取最方便的時間進行重新啟動的工作站。

  預設情況下已選定此選項。

- **重複提示間隔（分鐘）**

  如果啟用該選項，應用程式以指定頻率提示使用者重新啟動作業系統。

  預設情況下已啟用該選項。預設間隔是 5 分鐘。可用值介於 1 和 1440 分鐘之間。

  如果停用該選項，提示僅顯示一次。

- **在該時間後重新啟動（分鐘）**

  提示使用者之後，應用程式在指定時間間隔後強制作業系統重新啟動。

  預設情況下已啟用該選項。預設延時是 30 分鐘。可用值介於 1 和 1440 分鐘之間。

- **強制關閉已鎖定連線的應用程式**

  執行應用程式可能會阻止用戶端裝置重新啟動。例如，如果文件在文書處理應用程式中編輯且未儲存，應用程式不會允許裝置重新啟動。

  如果啟用該選項，鎖定裝置上的此類應用程式在裝置重新啟動前被強制關閉。結果，使用者可能遺失他們未儲存的變更。

  如果停用該選項，鎖定裝置不被重新啟動。此裝置上的工作狀態表示裝置需要重新啟動。使用者必須手動關閉所有執行在鎖定裝置上的應用程式並重新啟動這些裝置。

  預設情況下已停用該選項。

9. 指定帳戶設定：

- **預設帳戶**

  在與執行該工作的應用程式相同的帳戶下執行該工作。
  預設情況下已選定此選項。

- **指定帳戶**

  填寫**帳戶**與**密碼**欄位以指定工作要在其下執行的帳戶詳情。帳戶必須對此工作有足夠的權限。

- **帳戶**

  執行該工作的帳戶。

- **密碼**

  工作執行時使用的帳戶的密碼。

10. 若要修改預設工作設定，請啟用**完成工作建立**頁面的**建立完成時開啟工作詳情**選項。如果您不啟用該選項，工作使用預設設定建立。您可以稍後隨時修改預設設定。

11. 點擊**完成**按鈕。
    工作被建立並顯示在工作清單。

12. 按一下建立的工作的名稱以開啟工作內容視窗。

13. 在工作內容視窗中，依需求指定一般工作設定。

14. 點擊**儲存**按鈕。

    工作被建立和配置。

建立安裝必要更新並修復弱點工作

*安裝所需更新並修復弱點*工作僅在有弱點和修補程式程序管理產品授權下才可使用。

*安裝所需更新並修復弱點*工作會用來更新與修復協力廠商軟體中的弱點，包含安裝在受管理裝置上的 Microsoft 軟體。此工作可讓您根據特定規則安裝多項更新並修復多個弱點。

若要使用*安裝所需更新並修復弱點*工作安裝更新或修復弱點，您可進行以下一項操作：

- 執行更新安裝精靈或弱點修復精靈。
- 建立*安裝所需更新並修復弱點*工作。
- 對現有*安裝所需更新並修復弱點*工作新增安裝更新規則。

要建立安裝所需更新並修復弱點工作：

1. 在主功能表中，轉至 **裝置 → 工作**。

2. 點擊**新增**。

   新工作精靈啟動。遵照精靈的說明。

3. 對於卡巴斯基安全管理中心應用程式，選擇**安裝所需更新並修復弱點**工作類型。

   如果沒有顯示該工作，請檢查您的帳戶是否具有**系統管理**：**弱點和修補程式管理**功能區域的**讀取**、**修改**和**執行**權限。如果沒有這些存取權限，您就不能建立及設定*安裝所需更新並修復弱點*的工作。

4. 指定您正建立的工作的名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。

5. 選取要分配工作的裝置。

6. 指定更新安裝的規則，然後指定以下設定：

- **在裝置重新啟動或關閉時開始安裝**

  如果啟用該選項，更新在裝置被重新啟動或關閉時安裝。否則，更新根據排程安裝。

  如果安裝更新可能影響裝置效能則使用該選項。

  預設情況下已停用該選項。

- **安裝所需的一般系統元件**

  如果啟用該選項，在安裝更新之前，應用程式自動安裝所需的所有一般系統元件（先決條件）。例如，這些先決條件可以是作業系統更新。

  如果停用該選項，您可能必須手動安裝先決條件。

  預設情況下已停用該選項。

- **更新過程中允許安裝新的應用程式版本**

  如果啟用該**選項**，如果更新導致軟體應用程式新版本的安裝，更新將被允許。

  如果停用該選項，軟體不被升級。您可以稍後手動或透過其他工作安裝軟體的新版本。例如，如果公司基礎架構不被新軟體版本支援，或者如果您想要在測試基礎架構中檢查升級，您可能使用該選項。

  預設情況下已啟用該選項。

  升級應用程式可能導致安裝在用戶端裝置上的獨立應用程式功能異常。

- **下載更新到裝置而不安裝**

  如果啟用該選項，應用程式下載更新到裝置但是不自動安裝它們。您可以稍後手動安裝下載的更新。

  Microsoft 更新被下載到系統 Windows 儲存。協力廠商應用程式更新（由非 Kaspersky 和 Microsoft 軟體供應商製作的應用程式）會下載到在**下載更新資料夾**欄位指定的資料夾。

  如果停用該選項，更新被自動安裝到裝置。

  預設情況下已停用該選項。

- **下載更新資料夾**

  該資料夾用於下載協力廠商應用程式（由非 Kaspersky 和 Microsoft 軟體供應商製作的應用程式）更新。

- **啟用進階診斷**

如果啟用該功能，即便寫入偵錯檔案在卡巴斯基安全管理中心遠端診斷公用程式中對網路代理停用，網路代理也寫入偵錯檔案。偵錯輪流寫入兩個檔案中；兩個檔案的最大大小由**進階診斷檔案的最大大小 (MB)**值決定。當兩個檔案都滿時，網路代理再次開始寫入它們。帶有偵錯的檔案儲存在 %WINDIR%\Temp 資料夾。這些檔案在遠端診斷公用程式中可以被存取，您可以在那裡下載或刪除它們。

如果停用該功能，網路代理根據卡巴斯基安全管理中心遠端診斷公用程式中的設定寫入偵錯。沒有附加偵錯被寫入。

當建立工作時，您不必啟用進階診斷。您可能想要使用該功能，如果，例如，工作在一些裝置上失敗且您想要在另一個工作執行期間獲取額外資訊。

預設情況下已停用該選項。

- **進階診斷檔案的最大大小 (MB)**

  預設值是 100 MB，可用值介於 1 MB 和 2,048 MB 之間。當您所傳送的進階診斷檔案資訊不足以定位問題時，您可能被 Kaspersky 技術支援專家需求變更預設值。

7. 指定作業系統重新啟動設定：

- **不重新啟動裝置**

  用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

- **重新啟動裝置**

  如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

- **提示使用者操作**

  用戶端裝置螢幕上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。該選項適用於使用者必須可以選取最方便的時間進行重新啟動的工作站。

  預設情況下已選定此選項。

- **重複提示間隔（分鐘）**

  如果啟用該選項，應用程式以指定頻率提示使用者重新啟動作業系統。

  預設情況下已啟用該選項。預設間隔是 5 分鐘。可用值介於 1 和 1440 分鐘之間。

  如果停用該選項，提示僅顯示一次。

- **在該時間後重新啟動（分鐘）**

  提示使用者之後，應用程式在指定時間間隔後強制作業系統重新啟動。

  預設情況下已啟用該選項。預設延時是 30 分鐘。可用值介於 1 和 1440 分鐘之間。

- **在此時間後強制關閉封鎖連線中的應用程式 (分鐘)**

  使用者裝置鎖定時，程式以強制模式關閉（指定不活動間隔之後自動鎖定，或手動鎖定）。

  如果啟用此選項，一旦輸入區域指定的時間間隔結束，鎖定裝置上的程式以強制模式關閉。

  如果停用此選項，鎖定裝置上的程式將不會關閉。

  預設情況下已停用該選項。

8. 若要修改預設工作設定，請啟用**完成工作建立**頁面的**建立完成時開啟工作詳情**選項。如果您不啟用該選項，工作使用預設設定建立。您可以稍後隨時修改預設設定。

9. 點擊**完成**按鈕。

   工作被建立並顯示在工作清單。

10. 按一下建立的工作的名稱以開啟工作內容視窗。

11. 在工作內容視窗中，依需求指定一般工作設定。

12. 點擊**儲存**按鈕。

    工作被建立和配置。

若工作結果包含 0x80240033「Windows 更新代理錯誤 80240033（「無法下載產品授權期限」）」警告，您可以透過 Windows 登錄資料解決此問題。

新增安裝更新的規則

此功能僅在有弱點和修補程式管理產品授權下才可使用。

使用*安裝所需更新並修復弱點*工作安裝軟體更新或修復軟體弱點時，您必須指定安裝更新的規則。這些規則決定要安裝的更新和要修復的弱點。

精確設定會視您是否建立 Microsoft 應用程式、協力廠商應用程式（由非 Kaspersky 和 Microsoft 軟體供應商製作的應用程式）、或所有應用程式更新的規則而定。當新增 Windows Update 更新或協力廠商應用程式的更新規則時，您可以選取特定的應用程式和您要安裝更新的應用程式版本。當新增所有更新的規則時，您可以選取要安裝的特定更新，以及要透過安裝更新而修復的弱點。

您可以透過以下方式建立更新的安裝規則：

- 透過在建立新安裝所需更新並修復弱點工作時新增規則。
- 透過在現有*安裝所需更新並修復弱點*工作屬性視窗的**應用程式設定**索引標籤上新增規則。
- 透過更新安裝精靈或弱點修復精靈。

若要為所有更新建立新規則：

1. 點擊**新增**按鈕。

   規則建立精靈開始。使用**下一步**按鈕進行精靈。

2. 在**規則類型**頁面上，選擇**所有更新的規則**。

3. 在**一般標準**頁面，使用下拉清單指定以下設定：

- **要安裝的更新集**

  選取必須在用戶端裝置上安裝的更新：

  - **僅安裝批准的更新**。這僅安裝批准的更新。
  - **安裝所有更新（除了拒絕的）**。這安裝帶有*已批准*或*未定義*批准狀態的更新。
  - **安裝所有更新（包含拒絕的）**。這安裝所有更新，無論什麼批准狀態。警惕選取該選項。例如，如果您想要在測試基礎架構中檢查一些被拒絕的更新的安裝，使用該選項。

- **修復弱點的時機為嚴重等級大於或等於**

  有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

  如果啟用該選項，更新僅修復 Kaspersky 設定的安全等級等於或高於清單中選定的值（**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

  如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

  預設情況下已停用該選項。

4. 在**更新**頁面，選取要安裝的更新：

- **安裝所有合適的更新**

  安裝滿足在精靈中**一般標準**頁面指定標準的所有軟體更新。預設選取。

- **僅安裝清單中的更新**

  僅安裝您從清單中手動選取的軟體更新。該清單包含所有可用軟體更新。

  例如，您可能想要在以下情況下選取特定更新：要在測試環境中檢查它們的安裝、要僅更新嚴重應用程式、或者要僅更新特定應用程式。

  - **自動安裝所選更新安裝時需要的所有先前應用程式更新**

    如果在安裝所選更新需要時，您同意安裝暫時應用程式版本，保持該選項被啟用。

    如果停用該選項，僅選定的應用程式版本被安裝。如果您想直截了當地更新應用程式，而不嘗試安裝增量版本，請停用該選項。如果安裝所選更新不能不安裝先前版本的應用程式，應用程式更新失敗。

    例如，您在裝置上安裝了應用程式的版本 3，您想更新它到版本 5，但是該應用程式的版本 5 僅可以在版本 4 之上安裝。如果啟用該選項，軟體先安裝版本 4，然後安裝版本 5。如果停用該選項，軟體更新應用程式失敗。

    預設情況下已啟用該選項。

5. 在**弱點**頁面，選取將由安裝所選更新修復的弱點。

- **修復所有符合其他標準的弱點**

  修復滿足在精靈中**一般標準**頁面指定標準的所有弱點。預設選取。

- **僅修復清單中的弱點**

  僅修復您手動從清單中選取的弱點。清單包含所有偵測到的弱點。

  例如，您可能想要在以下情況下選取特定弱點：要在測試環境中檢查它們的修復、要僅修復嚴重應用程式中的弱點、或者要僅修復特定應用程式中的弱點。

6. 在**名稱**頁面，指定您正在建立的規則名稱。您可以稍後在所建立工作的內容視窗的**設定**區域變更該名稱。

「規則建立精靈」完成操作後，系統會建立新規則並顯示在「新工作精靈」或工作屬性的欄位中。

若要為 Windows Update 更新建立新規則：

1. 點擊**新增**按鈕。

   規則建立精靈開始。使用**下一步**按鈕進行精靈。

2. 在**規則類型**頁面上，選擇 **Windows Update 的規則**。

3. 在**一般標準**頁面中，指定以下設定：

- **要安裝的更新集**

  選取必須在用戶端裝置上安裝的更新：

  - **僅安裝批准的更新**。這僅安裝批准的更新。
  - **安裝所有更新（除了拒絕的）**。這安裝帶有*已批准*或*未定義*批准狀態的更新。
  - **安裝所有更新（包含拒絕的）**。這安裝所有更新，無論什麼批准狀態。警惕選取該選項。例如，如果您想要在測試基礎架構中檢查一些被拒絕的更新的安裝，使用該選項。

- **修復弱點的時機為嚴重等級大於或等於**

  有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

  如果啟用該選項，更新僅修復 Kaspersky 設定的安全等級等於或高於清單中選定的值（**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

  如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

  預設情況下已停用該選項。

- **修復弱點的時機為 MSRC 嚴重等級大於**

  有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

  如果啟用該選項，更新僅修復 Microsoft Security Response Center (MSRC) 設定的安全等級等於或高於清單中選定的值（**低**、**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

  如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

  預設情況下已停用該選項。

4. 在**應用程式**頁面，選取您要安裝更新的應用程式和應用程式版本。預設情況下選定所有應用程式。

5. 在**更新類別**頁面，選取要安裝的更新類別。這些類別與 Microsoft Update Catalog 中的類別相同。預設情況下選定所有類別。

6. 在**名稱**頁面，指定您正在建立的規則名稱。您可以稍後在所建立工作的內容視窗的**設定**區域變更該名稱。

「規則建立精靈」完成操作後，系統會建立新規則並顯示在「新工作精靈」或工作屬性的欄位中。

若要為協力廠商應用程式更新建立規則：

1. 點擊**新增**按鈕。

   規則建立精靈開始。使用**下一步**按鈕進行精靈。

2. 在**規則類型**頁面上，選擇**協力廠商更新的規則**。

3. 在**一般標準**頁面中，指定以下設定：

- **要安裝的更新集**

  選取必須在用戶端裝置上安裝的更新：

  - **僅安裝批准的更新**。這僅安裝批准的更新。
  - **安裝所有更新（除了拒絕的）**。這安裝帶有*已批准*或*未定義*批准狀態的更新。
  - **安裝所有更新（包含拒絕的）**。這安裝所有更新，無論什麼批准狀態。警惕選取該選項。例如，如果您想要在測試基礎架構中檢查一些被拒絕的更新的安裝，使用該選項。

- **修復弱點的時機為嚴重等級大於或等於**

  有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

  如果啟用該選項，更新僅修復 Kaspersky 設定的安全等級等於或高於清單中選定的值（**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

  如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

  預設情況下已停用該選項。

4. 在**應用程式**頁面，選取您要安裝更新的應用程式和應用程式版本。預設情況下選定所有應用程式。

5. 在**名稱**頁面，指定您正在建立的規則名稱。您可以稍後在所建立工作的內容視窗的設定區域變更該名稱。

「規則建立精靈」完成操作後，系統會建立新規則並顯示在「新工作精靈」或工作屬性的欄位中。

選取適用於協力廠商軟體中弱點的使用者修復項目

若要使用*修復弱點*工作，您必須手動指定軟體更新來修復列於工作設定中協力廠商軟體清單中的弱點。*修復弱點*工作會使用適用於 Microsoft 軟體的建議修復項目，以及適用於其他協力廠商軟體的使用者修復項目。*使用者修復項目*是管理員手動指定安裝用來修復適用於弱點的軟體更新。

若要在協力廠商軟體中選取適用於弱點的使用者修復項目：

1. 在主功能表中，轉至 **操作 → 修補程式管理 → 軟體弱點**。

   此頁會顯示在用戶端裝置中偵測到的軟體弱點清單。

2. 在軟體弱點清單中，按一下您要指定使用者修復之軟體弱點名稱的連結。

   弱點的內容視窗隨即開啟。

3. 在左窗格中，選取**使用者修復和其他修復**區段。

   針對選取的軟體弱點的使用者修復清單已顯示。

4. 按一下**新增**。

   系統會顯示可用安裝套件清單。顯示的安裝套件清單會對應**操作 → 儲存區 → 安裝套件**清單。若您未建立內含適用於所選弱點之使用者修復項目的安裝套件，您可啟動新安裝套件精靈以立即建立套件。

5. 在協力廠商軟體中，選取內含適用於弱點之使用者修復項目的安裝套件（或套件）。

6. 按一下**儲存**。

系統會指定包含適用於軟體弱點之使用者修復項目的安裝套件。當啟動*修復弱點*工作時，系統會安裝安裝套件並修復軟體弱點。

檢視在所有受管理裝置上偵測到的軟體弱點

掃描受管理裝置上軟體的弱點後，您可檢視在所有受管理裝置上軟體弱點的清單。如果針對管理伺服器層次結構執行該工作，則可以檢視僅針對所選管理伺服器偵測到弱點的受管理裝置清單。

要檢視在所有受管理裝置上偵測的軟體弱點清單，

在主功能表中，轉至 **操作 → 修補程式管理 → 軟體弱點**。

此頁會顯示在用戶端裝置中偵測到的軟體弱點清單。

您也可以產生並檢視弱點報告。

您可指定檢視軟體弱點清單的篩選器。點擊軟體弱點清單右上角的**篩選器**圖示（ ）來管理篩選條件。您也可從軟體弱點清單上方的**預設篩選器** 下拉清單選取其中一個預設篩選條件。

您可從清單取得關於任何弱點的詳細資訊。

若要取得軟體弱點資訊：

在軟體弱點清單中，按一下有弱點名稱的連結。

軟體弱點內容視窗隨即開啟。

檢視在受管理裝置上偵測到的軟體弱點的資訊

您可檢視在所選且執行 Windows 的受管理裝置上偵測到的軟體弱點資訊。

若要檢視在選取的受管理裝置上偵測的軟體弱點：

1. 在主功能表中，轉至 **裝置 → 受管理裝置**。
   受管理裝置清單隨即顯示。

2. 在受管理裝置清單中，按一下您要檢視之已偵測軟體弱點的裝置名稱連結。
   所選裝置的屬性視窗隨即顯示。

3. 在所選裝置的內容視窗中，選取**進階**頁籤。

4. 在左窗格中，選取**軟體弱點**區段。

在所選受管理裝置上偵測到的軟體弱點清單隨即顯示。

若要檢視所選軟體弱點的內容，

按一下軟體弱點清單中軟體弱點名稱的連結。

所選軟體弱點的內容視窗隨即顯示。

檢視受管理裝置的弱點統計資料

您可檢視受管理裝置上各軟體弱點的統計資料。統計資料會以圖表顯示。圖表會顯示裝置數量搭配以下狀態：

- *已忽略：<裝置數量>*。若您在弱點內容中手動設定選項以忽略弱點，則會配置此狀態。
- *已修復：<裝置數量>*。若修復弱點的工作完成，則會指派此狀態。
- *修復已排程：<裝置數量>*。若您已建立工作修復弱點，但該工作尚未執行，則會指派此狀態。
- *修補程式已套用：<裝置數量>*。若您已手動選取軟體更新來修復弱點，但此更新的軟體尚未修復弱點，則會指派此狀態。
- *需要修復：<裝置數量>*。如果弱點僅在某些受管理裝置上得到修復，並且需要在更多受管理裝置上修復弱點，則會指派此狀態。

若要檢視受管理裝置的弱點統計資料：

1. 在主功能表中，轉至 **操作 → 修補程式管理 → 軟體弱點**。
   此頁會顯示受管理裝置中偵測到的應用程式弱點清單。
2. 選取所需弱點旁邊的核取方塊。
3. 點擊**裝置弱點統計資訊**按鈕。

弱點狀態圖表隨即顯示。按一下狀態會開啟裝置清單，其中會顯示有所選狀態弱點的裝置。

將軟體弱點匯出至檔案中

您可將顯示的弱點清單匯出為 CSV 或 TXT 檔案。您可使用這些檔案，例如將它們傳送至您的資訊安全經理，或儲存起來以供統計使用。

若要匯出所有受管理裝置上偵測到的軟體弱點清單為文字檔案：

1. 在主功能表中，轉至 **操作 → 修補程式管理 → 軟體弱點**。
   此頁會顯示受管理裝置中偵測到的應用程式弱點清單。
2. 點擊**將行匯出到 txt 檔案**或**將行匯出到 csv 檔案**按鈕，視您偏好的匯出格式而定。

內含軟體弱點清單的檔案會下載至您目前使用的裝置。

若要匯出所選受管理裝置上偵測到的軟體弱點清單為文字檔案：

1. 開啟所選受管理裝置偵測到的軟體弱點清單。
2. 選取您要匯出的軟體弱點。
   若您要匯出在受管理裝置偵測到的軟體弱點完整清單，請略過此步驟。
   若您要匯出在受管理裝置偵測到的軟體弱點完整清單，僅會匯出顯示在目前頁面的弱點。
3. 點擊**將行匯出到 txt 檔案**或**將行匯出到 csv 檔案**按鈕，視您偏好的匯出格式而定。

含檔案所選受管理裝置偵測到的軟體弱點清單的檔案會下載至您目前使用的裝置。

忽略軟體弱點

您可忽略要修復的軟體弱點。忽略軟體弱點的原因可能如下：

- 您認為軟體弱點對您組織不緊急。
- 您瞭解軟體弱點修復會損壞需弱點修復之軟體的相關資料。
- 您確定軟體弱點對您組織網路並不危險，因為您使用其他措施防護您的受管理裝置。

您可在所有受管理裝置或僅在選取的受管理裝置忽略軟體弱點。

若要在所有受管理裝置上忽略軟體弱點：

1. 在主功能表中，轉至 **操作 → 修補程式管理 → 軟體弱點**。
   此頁會顯示在受管理裝置中偵測到的軟體弱點清單。
2. 在軟體弱點清單中，按一下有要忽略的軟體弱點名稱連結。
   軟體弱點內容視窗開啟。
3. 在**一般**頁籤，點擊**略過弱點**選項。
4. 點擊**儲存**按鈕。
   軟體弱點內容視窗關閉。

軟體弱點會在所有受管理裝置遭到忽略。

若要在選取的受管理裝置忽略軟體弱點：

1. 在主功能表中，轉至 **裝置 → 受管理裝置**。
   受管理裝置清單隨即顯示。
2. 在受管理裝置清單中，按一下有您要忽略之軟體弱點的裝置名稱連結。
   弱點內容視窗隨即開啟。
3. 在裝置內容視窗中，選取**進階**頁籤。
4. 在左窗格中，選取**軟體弱點**區段。
   在裝置上偵測到的軟體弱點清單隨即顯示。

5. 在軟體弱點清單中，選取您要在選取裝置上忽略的弱點。

   軟體弱點內容視窗開啟。

6. 在軟體弱點內容視窗中的**一般**頁籤，啟用**略過弱點**選項。

7. 點擊**儲存**按鈕。

   軟體弱點內容視窗關閉。

8. 關閉裝置內容視窗。

軟體弱點會在選取的裝置上遭到忽略。

忽略的軟體弱點在完成*修復弱點*工作或*安裝所需更新並修復弱點*工作將不會修復。您可從弱點清單使用篩選器排除忽略的軟體弱點。

管理用戶端裝置上的應用程式執行

本節說明卡巴斯基安全管理中心功能如何管理用戶端裝置上的應用程式執行。

使用「應用程式控制」來管理可執行檔

您可以使用「應用程式控制」元件來允許或阻止使用者裝置上可執行檔的啟動。「應用程式控制」元件支援基於 Windows 和 Linux 的作業系統。

對於基於 Linux 的作業系統，從 Kaspersky Endpoint Security 11.2 for Linux 開始可以使用應用程式控制元件。此元件也可供 Kaspersky Embedded Systems Security for Windows 3.0 或更高版本使用。

先決條件

- 系統會將卡巴斯基安全管理中心佈署在您的組織中。
- Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Linux 的政策已建立並處於使用中狀態。

階段

應用程式控制使用情境分階段進行：

1. **形成和檢視用戶端裝置上可執行檔的清單**

   此階段可提供您受管理裝置上有哪些可執行檔的資訊。檢視可執行檔清單，並將其與允許和禁止的可執行檔清單比較。對可執行檔使用的限制可能與您組織中的資訊安全政策相關。

   說明：

   - 管理主控台：可執行檔清單

- 卡巴斯基安全管理中心網頁主控台：取得並檢視儲存在用戶端裝置的可執行檔清單

2 為組織中使用的可執行檔建立類別

分析受管理裝置上儲存的可執行檔清單。基於分析為可執行檔建立類別。建議您建立涵蓋組織中使用的可執行檔標準集的「工作應用程式」類別。若不同的安全群組在其工作中使用各自的可執行檔集，則可針對各安全群組建立獨立的應用程式類別。

說明：

- 建立含手動新增屬性的應用程式類別、建立含所選裝置可執行檔的應用程式類別、建立含特定資料夾之可執行檔的應用程式類別。
- 卡巴斯基安全管理中心網頁主控台：建立含手動新增內容的應用程式類別、建立含所選裝置可執行檔的應用程式類別、建立含特定資料夾之可執行檔的應用程式類別。

3 在 Kaspersky Endpoint Security 政策設定應用程式控制

使用您在先前階段已建立的類別在 Kaspersky Endpoint Security 政策中設定應用程式控制元件。

說明：

- 管理主控台：設定應用程式在用戶端裝置上的啟動管理
- 卡巴斯基安全管理中心網頁主控台：在 Kaspersky Endpoint Security for Windows 政策配置應用程式控制項目

4 在測試模式中開啟應用程式控制元件

若要確定應用程式控制規則沒有封鎖使用者工作所需的可執行檔，建議啟用應用程式控制規則測試，並在建立新規則後分析其運作。啟用測試後，Kaspersky Endpoint Security for Windows 不會封鎖應用程式控制規則封鎖啟動的可執行檔，但會改為傳送有關其啟動的資訊至管理伺服器。

測試應用程式控制規則時，建議執行以下動作：

- 決定測試期間。測試期間可從數日到兩個月。
- 檢查因應用程式控制作業產生的測試事件。

卡巴斯基安全管理中心網頁主控台操作說明：在 Kaspersky Endpoint Security for Windows 政策中設定應用程式控制元件。遵循此指示並在組態程序中啟用**測試模式**選項。

5 變更應用程式控制元件的類別設定

如有必要，請變更應用程式控制設定。根據測試結果，您可於包含手動新增內容的類別中，新增與「應用程式控制」元件事件相關的可執行檔。

說明：

- 管理主控台：新增事件相關的可執行檔到應用程式類別
- 卡巴斯基安全管理中心網頁主控台：新增事件相關可執行檔至應用程式類別

6 在操作模式套用應用程式控制規則

測試應用程式控制規則且完成類別組態後，您可在操作模式中套用應用程式控制規則。

卡巴斯基安全管理中心網頁主控台操作說明：在 Kaspersky Endpoint Security for Windows 政策中設定應用程式控制元件。請遵循此指示，並在組態程式中停用**測試模式**選項。

7 確認應用程式控制組態

請確保您已完成以下項目：

- 為可執行檔建立類別。
- 使用類別設定「應用程式控制」。
- 在操作模式中套用應用程式控制規則。

結果

當情境完成時，受管理裝置上的可執行檔啟動會受到控制。使用者僅可啟動組織中允許的這些可執行檔，不可啟動被禁止的可執行檔。

如需有關應用程式控制的詳細資訊，請參閱以下說明主題：

- Kaspersky Endpoint Security for Windows 線上說明
- Kaspersky Endpoint Security for Linux 線上說明
- Kaspersky Security for Virtualization Light Agent
- Kaspersky Embedded Systems Security for Windows 說明
- Kaspersky Embedded Systems Security for Linux 說明

應用程式控制模式和類別

「應用程式控制」元件監控使用者啟動可執行檔的嘗試。您可以使用應用程式控制規則來控制可執行檔的啟動。

應用程式控制元件適用於 Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Security 11.2 for Linux 及更高版本以及 Kaspersky Security for Virtualization Light Agent。本節所有指示會說明 Kaspersky Endpoint Security for Windows 應用程式控制的組態。

與任何應用程式控制規則不符的可執行檔啟動的設定，會由該元件選取的操作模式規管：

- *拒絕清單*。若您要允許啟動所有可執行檔（除了封鎖規則所指定者），則會使用此模式。預設情況下會選取此模式。
- *允許清單*。若您要封鎖啟動所有可執行檔（除了允許規則所指定者），則會使用此模式。

應用程式控制規則是透過可執行檔的類別進行實作。在卡巴斯基安全管理中心中有三種類型的類別：

- 含有手動新增內容的類別。您會定義條件，例如檔案中繼資料、檔案雜湊碼、檔案憑證、KL 類別、檔案路徑，以在類別中包含可執行檔。
- 包含來自所選服務的可執行檔的類別。您指定之裝置的可執行檔會自動包含在類別中。
- 包含來自所選資料夾的可執行檔的類別。您指定之資料夾中的可執行檔會自動包含在類別中。

如需有關應用程式控制的詳細資訊，請參閱以下說明主題：

- Kaspersky Endpoint Security for Windows 線上說明
- Kaspersky Endpoint Security for Linux 線上說明
- Kaspersky Security for Virtualization Light Agent
- Kaspersky Embedded Systems Security for Windows 說明
- Kaspersky Embedded Systems Security for Linux 說明

取得並檢視安裝在用戶端裝置的應用程式清單

卡巴斯基安全管理中心會清查所有安裝在執行 Linux 和 Windows 的受管理用戶端裝置上的軟體。

網路代理編輯安裝在裝置上的應用程式清單，並把該清單傳給管理伺服器。網路代理更新應用程式清單大約需要 10-15 分鐘。

對於 Windows 用戶端裝置，網路代理從 Windows 登錄接收有關已安裝應用程式的大部分資訊。對於 Linux 用戶端裝置，套件管理工具會向網路代理提供有關已安裝應用程式的資訊。

如果在 Linux 裝置上偵測到來自**應用程式登錄資料**部分的應用程式，則應用程式內容不包含有關相關可執行檔的資訊。

若要檢視安裝在受管理裝置上的應用程式清單：

1. 在主功能表中，轉至 **操作 → 協力廠商應用程式 → 應用程式登錄資料**。

   該頁面顯示一個表格，其中包含安裝在受管理裝置上的應用程式。選取應用程式以檢視其內容，例如，供應商名稱、版本號、可執行檔清單、安裝了該應用程式的裝置清單、可用軟體更新清單和偵測到的軟體弱點清單。

2. 您可以按如下方式對包含已安裝應用程式的表格資料進行分組和篩選：

   - 按一下表格右上角的設定圖示（ ）。

     在叫用的**欄設定**功能表中，選擇要在表格中顯示的欄。要檢視安裝應用程式的用戶端裝置的作業系統類型，請選擇**作業系統類型**欄。

   - 按一下表格右上角的篩選圖示（ ），然後在叫用的功能表中指定並套用篩選條件。

     顯示篩選後的已安裝應用程式表格。

若要檢視安裝在特定受管理裝置上的應用程式清單：

在主功能表中，轉至 **裝置 → 受管理裝置 → <裝置名稱> → 進階 → 應用程式登錄資料**。在此功能表中，您可將應用程式清單匯出為 CSV 檔案或 TXT 檔案。

如需有關應用程式控制的詳細資訊，請參閱以下說明主題：

- Kaspersky Endpoint Security for Windows 線上說明
- Kaspersky Endpoint Security for Linux 線上說明

- Kaspersky Security for Virtualization Light Agent
- Kaspersky Embedded Systems Security for Windows 說明
- Kaspersky Embedded Systems Security for Linux 說明

取得並檢視儲存在用戶端裝置上的可執行檔清單

您可以透過以下方式之一獲取儲存在用戶端裝置上的可執行檔清單：

- 在 Kaspersky Endpoint Security 政策中啟用應用程式啟動通知。
- 建立清查工作。

在 Kaspersky Endpoint Security 政策中啟用應用程式啟動通知

要啟用有關應用程式啟動的通知：

1. 開啟 Kaspersky Endpoint Security 政策設定，然後轉至**一般設定 → 報告和儲存**。
2. 在**到管理伺服器的資料傳輸**設定群組中，選擇**關於啟動的應用程式**核取方塊，然後保存變更。

當使用者嘗試啟動可執行檔時，關於這些檔案的資訊將被新增到用戶端裝置上的可執行檔清單中。Kaspersky Endpoint Security 會將該資訊傳送到網路代理，然後網路代理會將其傳送到管理伺服器。

建立清查工作

清查可執行檔的功能可用於以下應用程式：

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux 版本 11.2 和以上版本
- Kaspersky Security for Virtualization 4.0 Light Agent 和更高版本

您可以在獲取已安裝應用程式的資訊時降低資料庫的負載。為了節省資料庫空間，請在安裝了標準軟體集合的參考裝置上執行清查工作。建議的裝置數量是 1-3。

當使用以下資料庫時，我們強烈不建議執行清查工作：MySQL、PostgreSQL、SQL Server Express Edition、MariaDB（所有版本）。

要在用戶端裝置上為可執行檔建立清查工作：

1. 在主功能表中，轉至**裝置 → 工作**。
   工作清單隨即顯示。
2. 點擊**新增**按鈕。
   新工作精靈啟動。遵照精靈的說明。

3. 在**新工作**頁面的**應用程式**下拉清單中，根據用戶端裝置的作業系統類型選擇 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Windows。

4. 在**工作類型**下拉式清單中，選取**清單**。

5. 在**完成工作建立**頁面上，點擊**完成**按鈕。

在新工作精靈完成後，**清單**工作隨即建立且設定。如有需要，您可變更已建立工作的設定。新建立的工作會顯示在工作清單。

關於清查工作的詳細說明，請參考以下說明：

- Kaspersky Endpoint Security for Windows 說明
- Kaspersky Endpoint Security for Linux 說明
- Kaspersky Security for Virtualization Light Agent

執行**清單**工作後，會形成儲存在受管理裝置的可執行檔清單，您可檢視該清單。

清查期間可偵測以下格式的可執行檔（取決於您在清查工作內容中選擇的選項）：MZ、COM、PE、NE、SYS、CMD、BAT、PS1、JS、VBS、REG、MSI、CPL、DLL、JAR 和 HTML。

檢視受管理裝置上儲存的可執行檔清單

要檢視儲存在用戶端裝置的可執行檔清單：

在主功能表中，轉至 **操作 → 協力廠商應用程式 → 可執行檔**。

此頁面會顯示儲存在用戶端裝置上的可執行檔清單。

如有必要，您可以將受管理裝置的可執行檔傳送到卡巴斯基安全管理中心網頁主控台在其中開啟的裝置。

若要傳送可執行檔：

1. 在主功能表中，轉至 **操作 → 協力廠商應用程式 → 可執行檔**。

2. 按一下要傳送的可執行檔的連結。

3. 在開啟的視窗中，轉至**裝置**區域，然後選擇要從其傳送可執行檔的受管理裝置的核取方塊。

在傳送可執行檔之前，請確保受管理裝置與管理伺服器有直接連線，方法是選擇**不斷開與管理伺服器的連線** 核取方塊。

4. 點擊**傳送**按鈕。

選定的可執行檔將下載，以便進一步傳送到卡巴斯基安全管理中心網頁主控台在其中開啟的裝置。

建立含有手動新增內容的應用程式類別

您可指定一組準則作為可執行檔的範本，這些範本是您希望在組織中允許或封鎖的啟動範本。根據對應該準則的可執行檔，您可建立應用程式類別並在應用程式控制元件組態中加以使用。

要建立含有手動新增內容的應用程式類別：

1. 在主功能表中，轉至 **操作 → 協力廠商應用程式 → 應用程式類別**。

   應用程式類別清單頁面隨即顯示。

2. 點擊**新增**按鈕。

   新類別精靈啟動。使用**下一步**按鈕進行精靈。

3. 在**選擇類別建立方法**步驟，選擇**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**選項。

4. 在**條件**步驟，點擊**新增**按鈕新增條件準則，以在建立的類別中包含檔案。

5. 在**條件標準**步驟，從清單選取建立類別時所遵從的規則類型：

- **從 KL 類別**

  如果選中此選項，作為新增應用程式到使用者類別的條件，您可以為應用程式指定 Kaspersky 類別。來自指定 Kaspersky 類別的應用程式將被新增到自訂應用程式類別。

- **從儲存區選擇憑證**

  如果選中此選項，則可以指定來自儲存空間的憑證。類別條件僅符合指定憑證簽署的可執行檔。

- **指定應用程式路徑（支援遮罩）**

  如果選中此選項，您可以指定包含要新增到使用者應用程式類別的可執行檔的用戶端裝置上的檔案或資料夾路徑。您可以使用正規表示式，例如*C:\path_to_exe**，例如：*C:\Program Files\Internet Explorer**。

- **卸除式磁碟機**

  如果選中此選項，您可以指定應用程式在其上執行的媒體類型（任意裝置或行動裝置）。在所選驅動類型上執行的應用程式被新增到使用者應用程式類別。

- **雜湊、檔案內容或憑證**：

  - **從可執行檔清單選擇**

    如果選中此選項，可以使用用戶端裝置上的可執行檔清單來選取應用程式並將其新增到類別。

  - **從應用程式登錄資料選擇**

    若已選取此選項，會顯示應用程式登錄資料。從登錄檔中選擇一個應用程式後，視窗將開啟，其中的參數將使用您選擇的應用程式的中繼資料進行填充：

    - 檔案名稱。
    - 檔案版本。您可指定版本的準確值或說明條件，例如「大於 5.0」。
    - 應用程式名稱。
    - 應用程式版本。您可指定版本的準確值或說明條件，例如「大於 5.0」。
    - 供應商。

    請注意，僅阻止滿足指定參數的可執行檔的啟動，而不是阻止您選擇的應用程式的啟動。如果選定的應用程式中繼資料與啟動應用程式時啟動的可執行檔的中繼資料相匹配，則可以繼續下一步。否則，您必須手動變更值以匹配可執行檔的中繼資料。

  - **手動指定**

如果選取此選項，您必須指定檔案雜湊或中繼資料或憑證，以作為新稱應用程式至使用者類別的條件。

檔案雜湊值

取決於您網路裝置上安裝的安全應用程式版本，您必須為此類別中的檔案選取卡巴斯基安全管理中心使用的雜湊值演算法。有關由雜湊函數計算的雜湊值的資訊儲存在管理伺服器資料庫中。

SHA256 是密碼雜湊函數：未在其演算法中找到弱點，因此是現今公認最可靠的加密功能。Kaspersky Endpoint Security 10 Service Pack 2 for Windows 和更新版本支援 SHA256 計算。計算 MD5 雜湊被所有 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 的早期版本支援。

為該類別中的檔案選取任意卡巴斯基安全管理中心使用的雜湊值演算法選項：

- 如果您網路上安裝的所有安全應用程式實例都是 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更高版本，請選取 **SHA-256** 核取方塊。對於 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 早期版本，我們不建議您新增根據可執行檔 SHA256 雜湊為標準建立的類別。這將導致安全應用程式操作失敗。此種情況下，您可以為類別中的檔案使用 MD5 加密演算法。
- 如果您的網路上安裝了 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 之前的任何版本，請選取**MD5 雜湊值**。對於 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本，您無法新增基於可執行檔的 MD5 總和檢查碼的條件所建立的類別。此種情況下，您可以為類別中的檔案使用 SHA256 加密演算法。
- 如果您網路上的不同裝置同時使用早期和更新版本的 Kaspersky Endpoint Security 10，請選取 **SHA-256** 核取方塊和 **MD5 雜湊值** 核取方塊。

檔案內容

若已選取此選項，您可指定檔案中繼資料作為檔案名稱、檔案版本、供應商。類別條件僅匹配具有相同中繼資料的可執行檔。

憑證

如果選中此選項，則可以指定來自儲存空間的憑證。類別條件僅符合指定憑證簽署的可執行檔。

- **從檔案或從 MSI 套件 / 存檔資料夾**

如果選中此選項，作為新增應用程式到使用者類別的一個條件，您可以指定 MSI 安裝程式的檔。應用程式安裝程式的檔案內容將被傳送到管理伺服器。與指定的 MSI 安裝程式具有相同檔案內容的應用程式被新增到自訂應用程式類別。

選取的準則會新增至條件清單。

您可視需要新增所需數量的應用程式類別。

6. 在**排除**步驟，點擊**新增**按鈕新增排除條件準則，以從建立的類別排除檔案。
7. 在**條件標準**步驟，從清單選取規則類型，與您為建立類別選取規則類型的方式一樣。

當精靈結束時就會建立自訂應用程式類別。它顯示在應用程式類別清單中。當您設定應用程式控制時，您可使用建立的應用程式類別。

如需有關應用程式控制的詳細資訊，請參閱以下說明主題：

- Kaspersky Endpoint Security for Windows 線上說明
- Kaspersky Endpoint Security for Linux 線上說明
- Kaspersky Security for Virtualization Light Agent

- Kaspersky Embedded Systems Security for Windows 說明
- Kaspersky Embedded Systems Security for Linux 說明

建立應用程式類別以包含來自所選裝置的可執行檔

您可從選取的裝置使用可執行檔作為您希望允許或封鎖的可執行檔範本。根據選取裝置的可執行檔，您可建立類別並在應用程式控制元件組態中加以使用。

若要從裝置檢索可執行檔清單：

1. 確保 Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Linux 的政策已建立並處於使用中狀態。在政策中啟用應用程式控制元件。
2. 取得儲存在用戶端裝置上的可執行檔清單。

若要建立類別以包含來自所選裝置的可執行檔：

1. 在主功能表中，轉至 **操作 → 協力廠商應用程式 → 應用程式類別**。

   類別清單頁面隨即顯示。
2. 點擊**新增**按鈕。

   新類別精靈啟動。使用**下一步**按鈕進行精靈。
3. 在**選擇類別建立方法**步驟，指定類別名稱並選取**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**選項。
4. 點擊**新增**。

5. 在開啟的視窗中，選取一部裝置，或其中的可執行檔將用來建立類別的裝置。

6. 指定下列設定：

- **雜湊值計算方法**

  取決於您網路裝置上安裝的安全應用程式版本，您必須為此類別中的檔案選取卡巴斯基安全管理中心使用的雜湊值演算法。有關由雜湊函數計算的雜湊值的資訊儲存在管理伺服器資料庫中。

  SHA256 是密碼雜湊函數：未在其演算法中找到弱點，因此是現今公認最可靠的加密功能。Kaspersky Endpoint Security 10 Service Pack 2 for Windows 和更新版本支援 SHA256 計算。計算 MD5 雜湊被所有 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 的早期版本支援。

  為該類別中的檔案選取任意卡巴斯基安全管理中心使用的雜湊值演算法選項：

  - 如果您網路上安裝的所有安全應用程式實例都是 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更高版本，請選取 **SHA-256** 核取方塊。對於 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 早期版本，我們不建議您新增根據可執行檔 SHA256 雜湊為標準建立的類別。這將導致安全應用程式操作失敗。此種情況下，您可以為類別中的檔案使用 MD5 加密演算法。

  - 如果您的網路上安裝了 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 之前的任何版本，請選取**MD5 雜湊值**。對於 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本，您無法新增基於可執行檔的 MD5 總和檢查碼的條件所建立的類別。此種情況下，您可以為類別中的檔案使用 SHA256 加密演算法。

  如果您網路上的不同裝置同時使用早期和更新版本的 Kaspersky Endpoint Security 10，請選取 **SHA-256** 核取方塊和 **MD5 雜湊值** 核取方塊。

  依預設，系統將選取**為該類別中的檔案計算 SHA256（由 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本支援）**核取方塊。

  為該類別中的檔案計算 MD5（在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 更早版本中支援）核取方塊被預設清空。

- **與管理伺服器儲存區同步資料**

  選取此選項，若您希望管理伺服器定期在指定資料夾（或資料夾）檢查變更。

  預設情況下已停用該選項。

  若您啟用此選項，請指定時段（小時）以檢查指定資料夾（或資料夾）中的變更。依預設，掃描間隔為 24 小時。

- **檔案類型**

  在此區段內，您可指定用來建立應用程式類別的檔案類型。

  所有檔案。所有檔案都會在建立類別時納入考量。預設情況下已選定此選項。

  僅應用程式類別之外的檔案。僅應用程式類別外的檔案會在建立類別時納入考量。

- **資料夾**

在此區段中，您可要指定已選取裝置中要用來建立應用程式類別的資料夾。

所有資料夾。所有資料夾都會納入建立類別的考量。預設情況下已選定此選項。

指定資料夾。僅指定的資料夾會納入建立類別的考量。若您選取此選項，您必須指定連至資料夾的路徑。

精靈完成後就會建立可執行檔類別。它顯示在類別清單中。當您設定「應用程式控制」時，可使用已建立的類別。

建立應用程式類別以包含來自所選資料夾的可執行檔

您可從選取的資料夾使用可執行檔，將其作為組織中允許或封鎖的標準。以所選資料夾的可執行檔為依據，您可建立應用程式類別並在應用程式控制元件組態中加以使用。

若要建立類別以包含來自所選資料夾的可執行檔：

1. 在主功能表中，轉至 **操作 → 協力廠商應用程式 → 應用程式類別**。

   類別清單頁面隨即顯示。

2. 點擊**新增**按鈕。

   新類別精靈啟動。使用**下一步**按鈕進行精靈。

3. 在**選擇類別建立方法**步驟，指定類別名稱並選取**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**選項。

4. 指定其可執行檔將用於建立類別的資料夾。

5. 定義下列設定：

- **包含動態連結程式庫 (DLL) 到該類別**

  應用程式類別包含動態連結程式庫（DLL 格式的檔案），應用程式控制元件記錄系統中執行的此類庫的操作。包含 DLL 檔案到類別可能降低卡巴斯基安全管理中心的效能。

  預設情況下已清空此方塊。

- **包含指令碼到該類別**

  應用程式類別包含指令碼資料，指令碼不被 Web 威脅防護封鎖。包含指令碼資料到類別可能降低卡巴斯基安全管理中心的效能。

  預設情況下已清空此方塊。

- **雜湊值計算演算法**：**為該類別中的檔案計算 SHA-256（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）**

  取決於您網路裝置上安裝的安全應用程式版本，您必須為此類別中的檔案選取卡巴斯基安全管理中心使用的雜湊值演算法。有關由雜湊函數計算的雜湊值的資訊儲存在管理伺服器資料庫中。

  SHA256 是密碼雜湊函數：未在其演算法中找到弱點，因此是現今公認最可靠的加密功能。Kaspersky Endpoint Security 10 Service Pack 2 for Windows 和更新版本支援 SHA256 計算。計算 MD5 雜湊被所有 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 的早期版本支援。

  為該類別中的檔案選取任意卡巴斯基安全管理中心使用的雜湊值演算法選項：

  - 如果您網路上安裝的所有安全應用程式實例都是 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更高版本，請選取 **SHA-256** 核取方塊。對於 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 早期版本，我們不建議您新增根據可執行檔 SHA256 雜湊為標準建立的類別。這將導致安全應用程式操作失敗。此種情況下，您可以為類別中的檔案使用 MD5 加密演算法。

  - 如果您的網路上安裝了 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 之前的任何版本，請選取**MD5 雜湊值**。對於 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本，您無法新增基於可執行檔的 MD5 總和檢查碼的條件所建立的類別。此種情況下，您可以為類別中的檔案使用 SHA256 加密演算法。

  如果您網路上的不同裝置同時使用早期和更新版本的 Kaspersky Endpoint Security 10，請選取 **SHA-256** 核取方塊和 **MD5 雜湊值** 核取方塊。

  依預設，系統將選取**為該類別中的檔案計算 SHA256（由 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本支援）**核取方塊。

  為該類別中的檔案計算 MD5（在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 更早版本中支援）核取方塊被預設清空。

- **強制掃描資料夾以尋找變更**

如果啟用此選項，應用程式會定期檢查「類別屬性新增」資料夾的任何變化。您可以在該方塊旁的輸入欄位中指定檢查頻率（小時）。預設情況下，強制檢查的時間間隔為 24 小時。

如果停用此選項，應用程式不會強制檢查資料夾。如果檔案被修改、新增或刪除，伺服器會嘗試存取這些檔案。

預設情況下已停用該選項。

精靈完成後就會建立可執行檔類別。該類別顯示在類別清單中。您可在「應用程式控制」組態使用該類別。

如需有關應用程式控制的詳細資訊，請參閱以下說明主題：

- Kaspersky Endpoint Security for Windows 線上說明
- Kaspersky Endpoint Security for Linux 線上說明
- Kaspersky Security for Virtualization Light Agent
- Kaspersky Embedded Systems Security for Windows 說明
- Kaspersky Embedded Systems Security for Linux 說明

檢視應用程式類別清單

您可檢視已設定可執行檔類別清單以及各類別的設定。

要檢視應用程式類別清單，

在主功能表中，轉至 **操作 → 協力廠商應用程式 → 應用程式類別**。

類別清單頁面隨即顯示。

若要檢視應用程式類別內容，

點擊類別的名稱。

類別的內容視窗隨即開啟。內容會在數個頁籤上分組。

在 Kaspersky Endpoint Security for Windows 政策配置應用程式控制

建立應用程式控制類別後，您可將其用來在 Kaspersky Endpoint Security for Windows 政策配置應用程式控制。

若要在 Kaspersky Endpoint Security for Windows 政策設定應用程式控制：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。

   政策清單頁面隨即顯示。

2. 按一下 **Kaspersky Endpoint Security for Windows** 政策。

   政策設定視窗隨即開啟。

3. 轉到**應用程式設定→安全控制→應用程式控制**。

   含應用程式控制設定的**應用程式控制**視窗隨即顯示。

4. **應用程式控制**選項預設為啟用。確保**應用程式控制已停用**切換按鈕已切換到停用位置。

5. 在**應用程式控制設定**封鎖設定中，啟用操作模式以套用應用程式控制規則，並允許 Kaspersky Endpoint Security for Windows 封鎖應用程式啟動。

   如果要測試應用程式控制規則，請在**應用程式控制設定**區域啟用測試模式。在測試模式下，Kaspersky Endpoint Security for Windows 不會封鎖應用程式啟動，但會在報告中記錄有關觸發規則的資訊。點擊**檢視報告**連接可檢視此資訊。

6. 若您希望在使用者啟動應用程式時，要 Kaspersky Endpoint Security for Windows 監控 DLL 模組載入情況，請啟用**控制 DLL 模組載入**選項。

   模組與載入模組之應用程式的相關資訊將儲存至報告中。

   選取**控制 DLL 模組載入**選項後，Kaspersky Endpoint Security for Windows 僅會監控 DLL 模組和載入的驅動程式。選取**控制 DLL 模組載入**選項後，若您要 Kaspersky Endpoint Security for Windows 監控所有 DLL 模組和驅動程式，包含那些在 Kaspersky Endpoint Security for Windows 啟動前就已載入的項目，請重新啟動裝置。

7. （選用）在**訊息範本**區塊中，變更應用程式被封鎖啟動時顯示的訊息範本，以及會傳送給您的電子郵件訊息範本。

8. 在**應用程式控制模式**封鎖設定中，選取**拒絕清單**或**允許清單**模式。

   依預設會選取**拒絕清單**模式。

9. 按一下**規則清單設定**連結。

   拒絕清單與允許清單視窗隨即開啟以供您新增應用程式類別。選取**拒絕清單**模式時，依預設會選取**拒絕清單**頁籤，選取**允許清單**模式時會選取**允許清單**頁籤。

10. 在**拒絕清單與允許清單**視窗中，點擊**新增**按鈕。

    應用程式控制規則視窗將啟動。

11. 按一下**請選擇一個類別**連結。

    應用程式類別視窗隨即開啟。

12. 新增您先前建立的應用程式類別。

    您可按一下**編輯**按鈕來編輯已建立類別的設定。

    您可按一下**新增**按鈕建立新類別。

    您可按一下**刪除**按鈕從清單中刪除類別。

13. 完成應用程式類別清單後，請點擊**確定**按鈕。

    應用程式類別視窗隨即關閉。

14. 在**應用程式控制規則**視窗的**物件與其權限**區段中，建立要套用應用程式控制規則的使用者與使用者群組清單。

15. 點擊**確定**按鈕以儲存設定並關閉**應用程式控制規則**視窗。

16. 點擊 **確定** 按鈕以儲存設定並關閉**拒絕清單與允許清單**視窗。

17. 點擊**確定**按鈕以儲存設定並關閉**應用程式控制**視窗。

18. 關閉包含 Kaspersky Endpoint Security for Windows 政策設定的視窗。

    應用程式控制已設定。政策填入用戶端裝置後，可執行檔啟動就會受管理。

如需有關應用程式控制的詳細資訊，請參閱以下說明主題：

- Kaspersky Endpoint Security for Windows 線上說明
- Kaspersky Endpoint Security for Linux 線上說明
- Kaspersky Security for Virtualization Light Agent
- Kaspersky Embedded Systems Security for Windows 說明
- Kaspersky Embedded Systems Security for Linux 說明

新增事件相關的可執行檔到應用程式類別

當您在 Kaspersky Endpoint Security for Windows 政策中配置應用程式控制，以下事件會顯示在事件清單中：

- **應用程式遭禁止啟動**（*緊急*事件）。若您已設定應用程式控制來套用規則，則會顯示此事件。
- **應用程式在測試模式中遭禁止啟動**（*資訊*事件）。若您已設定用程式控制來測試規則，則會顯示此事件。
- **向管理員傳送的有關應用程式啟動禁止的訊息**（*警告*事件）。若您已設定應用程式控制來套用規則，則會顯示此事件，並且使用者已要求存取在啟動時遭封鎖的應用程式。

建議您建立事件分類來檢視與應用程式控制操作相關的事件。

您可新增與應用程式控制事件相關的可執行檔至現有應用程式類別或新的應用程式類別。您僅可將可執行檔，新增至透過手動新增內容的應用程式類別。

若要新增與應用程式控制事件相關的可執行檔到應用程式類別：

1. 在主功能表中，轉至 **監控和報告 → 事件分類**。

   事件分類清單已顯示。

2. 選取事件分類來檢視與應用程式控制相關的事件並啟動此事件分類。

   若您尚未建立與應用程式控制相關的事件分類，您可選取並啟動預先定義的分類，例如**最近的事件**。

   事件清單隨即顯示。

3. 選取其中有您要新增至應用程式類別之可執行檔的事件，接著點擊**分配到類別**按鈕。

   新類別精靈啟動。使用**下一步**按鈕進行精靈。

4. 在精靈頁面上，指定相關設定：

- 在**對事件相關可執行檔所採取的操作**區段，選取以下其中一個選項：
  - **新增到新的應用程式類別**

    如果您需要根據事件相關的可執行檔建立新的應用程式類別，請選取此選項。

    預設情況下已選定此選項。

    若您已選取此選項，請指定新類別名稱。

  - **新增到現有應用程式類別**

    如果您需要新增事件相關可執行檔至現有應用程式類別，請選取此選項。

    預設情況下未選定此選項。

    若您已選取此選項，請選取您要新增可執行檔且有手動新增內容的應用程式類別。

- 在**規則類型**區域，選取以下選項之一：
  - **新增到包含的規則**
  - **新增到排除的規則**
- 在**用作條件的參數**區段中，選擇以下選項之一：
  - **憑證詳情（或沒有憑證的檔案的 SHA-256 雜湊）**

    檔案可能使用憑證簽署。多個檔案可能使用相同的憑證簽署。例如，相同應用程式的不同版本可能使用相同的憑證簽署，或者相同供應商的多個不同應用程式可能使用相同憑證簽署。當您選取憑證時，應用程式的多個版本或相同供應商的多個應用程式可能組成一個類別。

    每個檔案都有其獨特的 SHA256 雜湊函數。當您選取 SHA256 雜湊函數時，僅一個對應的檔案（例如定義的應用程式版本）組成類別。

    如果您要在類別規則中新增可執行檔的憑證詳情（或無憑證檔案的 SHA256 雜湊），請選取此選項。

    預設情況下已選定此選項。

  - **憑證詳情（沒有憑證的檔案將被略過）**

    檔案可能使用憑證簽署。多個檔案可能使用相同的憑證簽署。例如，相同應用程式的不同版本可能使用相同的憑證簽署，或者相同供應商的多個不同應用程式可能使用相同憑證簽署。當您選取憑證時，應用程式的多個版本或相同供應商的多個應用程式可能組成一個類別。

    如果您要新增可執行檔的憑證詳情到類別規則，請選取此選項。如果可執行檔沒有憑證，該檔案將被略過。該檔案的資訊將不被新增到類別。

  - **僅 SHA-256（沒有雜湊的檔案將被略過）**

    每個檔案都有其獨特的 SHA256 雜湊函數。當您選取 SHA256 雜湊函數時，僅一個對應的檔案（例如定義的應用程式版本）組成類別。

    如果您要僅新增可執行檔的 SHA256 雜湊函數詳情，請選取此選項。

- **僅 MD5（停產模式，僅對 Kaspersky Endpoint Security 10 Service Pack 1 版本）**

  每個檔案都有單獨的 MD5 雜湊。當您選取 MD5 雜湊時，僅一個對應的檔案，例如，定義的應用程式版本，組成類別。

  如果您要僅新增可執行檔的 MD5 雜湊詳情，請選取此選項。MD5 雜湊碼計算功能被 Kaspersky Endpoint Security 10 Service Pack 1 for Windows 和所有早期版本支援。

5. 點擊**確定**。

當精靈完成時，系統會新增與應用程式控制事件相關的可執行檔至現有應用程式類別或新的應用程式類別。您可檢視已修改或建立的應用程式類別的設定。

如需有關應用程式控制的詳細資訊，請參閱以下說明主題：

- Kaspersky Endpoint Security for Windows 線上說明
- Kaspersky Endpoint Security for Linux 線上說明
- Kaspersky Security for Virtualization Light Agent
- Kaspersky Embedded Systems Security for Windows 說明
- Kaspersky Embedded Systems Security for Linux 說明

從卡巴斯基資料庫建立協力廠商應用程式的安裝套件

卡巴斯基安全管理中心 網頁主控台允許您使用安裝套件執行協力廠商應用程式的遠端安裝。此類協力廠商應用程式會隨附於專用的 Kaspersky 資料庫中。當您初次執行*Download updates to the repository of the Administration Server*工作時，系統會自動建立資料庫。

若要從 Kaspersky 資料庫建立協力廠商應用程式的安裝套件，請執行以下操作：

1. 在主功能表中，轉至 **發現和佈署 → 佈署和分配 → 安裝套件**。
2. 點擊**新增**按鈕。
3. 在開啟的「新安裝套件精靈」頁面上，選取**從 Kaspersky 資料庫中選取一個應用程式來建立安裝套件**選項並點擊**下一步**。
4. 在開啟的應用程式清單中，選取相關應用程式，然後點擊**下一步**。
5. 在下拉清單中選擇相關的本地化語言，然後點擊**下一步**。

   僅當應用程式提供多種語言選項的選擇時，才顯示此步驟。

6. 如果系統提示您接受產品授權協議，請在**最終使用者產品授權協議**開啟頁面，點擊連結以讀取供應商網站上的產品授權協議，然後選取**本人确认已完全阅读、理解并接受本《最终用户授权许可协议》的条款和条件**核取方塊。
7. 在開啟的**新安裝套件的名稱**頁面中的**檔案名稱**欄位，輸入安裝套件的名稱，然後點擊**下一步**。

等待直到新建立的安裝套件上傳到管理伺服器。當「新套件精靈」顯示訊息通知您套件建立過程成功時，請點擊**完成**。

新建立的安裝套件會出現在安裝套件清單。您可以在建立或重新配置*遠端安裝應用程式*工作時選取此套件。

從卡巴斯基資料庫檢視和修改協力廠商應用程式的安裝套件設定

如果您先前已經建立 Kaspersky 資料庫中列出之協力廠商應用程式的任何安裝套件，則可以隨後檢視和修改這些軟體套件的設定。

從 Kaspersky 資料庫修改協力廠商應用程式安裝套件的設定僅在「弱點和修補程式管理」產品授權下可用。

要從 Kaspersky 資料庫檢視和修改協力廠商應用程式的安裝套件的設定，請執行以下操作：

1. 在主功能表中，轉至 **發現和佈署 → 佈署和分配 → 安裝套件**。
2. 在開啟的安裝套件清單中，點擊相關套件的名稱。
3. 如有必要，在開啟的屬性頁面上修改設定。
4. 點擊**儲存**按鈕。

您修改的設定隨即保存。

Kaspersky 資料庫協力廠商應用程式的安裝套件設定

協力廠商應用程式的安裝套件設定會用以下頁籤分組：

預設情況下，僅顯示下面列出的一部分設定，因此您可以透過點擊**篩選器**按鈕，然後從清單中選取相關的欄名稱。

- **一般**頁籤：
  - 包含可以手動編輯的安裝套件名稱的輸入欄位
  - **應用程式**

    為其建立安裝套件的協力廠商應用程式名稱。
  - **版本**

    為其建立安裝套件的協力廠商應用程式的版本編號。
  - **大小**

    協力廠商安裝套件的大小（以 KB 為單位）。
  - **建立日期**

    協力廠商安裝套件的建立日期和時間。
  - **路徑**

    儲存獨立安裝套件網路資料夾的路徑。
- **安裝處理程序**頁籤：
  - **安裝所需的一般系統元件**

    如果啟用該選項，在安裝更新之前，應用程式自動安裝所需的所有一般系統元件（先決條件）。例如，這些先決條件可以是作業系統更新。

    如果停用該選項，您可能必須手動安裝先決條件。

    預設情況下已停用該選項。
  - 顯示更新屬性並包含以下各列的表格：
    - **名稱**

      更新的名稱。

- **敘述**

  更新的說明。

- **來源**

  更新的來源，由 Microsoft 或其他第三方開發人員發布。

- **類型**

  更新的類型，適用於驅動程式還是應用程式。

- **類別**

  顯示 Microsoft 更新（關鍵更新、定義更新、驅動程式、功能套件、安全更新、Service Pack、工具、更新匯總、更新或升級）的 Windows Server Update Services (WSUS) 類別。

- **根據 MSRC 的嚴重等級**

  Microsoft 安全回應中心 (MSRC) 定義的更新嚴重等級。

- **嚴重等級**

  Kaspersky 定義的更新嚴重等級。

- **修補程式嚴重等級（對於 Kaspersky 應用程式的修補程式）**

  修補程式的嚴重等級（如果適用於 Kaspersky應用程式）。

- **文章**

  知識庫中描述更新的文章識別碼 (ID)。

- **公告**

  說明更新的安全公告 ID。

- **未指定安裝（新版本）**

  顯示更新是否具有未指派安裝狀態。

- **即將安裝**

  顯示更新是否具有「待安裝」狀態。

- **正在安裝**

  顯示更新是否具有「安裝中」狀態。

- **已安裝**

  顯示更新是否具有「已安裝」狀態。

- **失敗**

  顯示更新是否具有「已失敗」狀態。

- **需要重新啟動**

  顯示更新是否具有「需要重新啟動」狀態。

- **已註冊**

  顯示註冊更新的日期和時間。

- **以互動模式安裝**

  顯示更新是否需要在安裝期間與使用者進行互動。

- **已撤銷**

  顯示撤銷更新的日期和時間。

- **更新批准狀態**

  顯示更新是否獲准安裝。

- **修訂**

  顯示更新的當前修訂版號。

- **更新 ID**

  顯示更新的 ID。

- **應用程式版本**

  顯示應用程式要更新的版號。

- **被替代的**

  顯示可以取代更新的其他更新。

- **替代**

  顯示可以由更新取代的其他更新。

- **您必須接受產品授權協議的條款**

  顯示更新是否需要接受最終使用者產品授權協議 (EULA) 的條款。

- **URL 敘述**

  顯示更新供應商的名稱。

- **應用程式系列**

  顯示更新所屬的應用程式系列名稱。

- **應用程式**

  顯示更新所屬的應用程式名稱。

- **中文化語言**

  顯示更新本地化的語言。

- **未指定安裝（新版本）**

  顯示更新是否具有「未指派安裝（新版本）」的狀態。

- **需要安裝的先決條件**

  顯示更新是否具有「需要先決條件」的安裝狀態。

- **下載模式**

  顯示更新下載的模式。

- **是一個修補程式**

  顯示更新是否為修補程式。

- **未安裝**

  顯示更新是否具有「未安裝」狀態。

- 顯示安裝套件設定（包含名稱、描述和值）的**設定**頁簽，在安裝過程中用來作為命令行參數。如果套件未提供此類設定，則會顯示相應的訊息。您可以修改這些設定的值。
- **變更歷程**頁籤，顯示安裝套件修訂版號並包含以下各欄：
  - **修訂**– 安裝套件的修訂號。
  - **時間**– 修改安裝套件設定的日期和時間。
  - **使用者** – 修改安裝套件設定的使用者的名稱。
  - **操作** – 對修訂中的安裝套件執行的操作。
  - **敘述** – 與安裝套件設定變更相關的修訂敘述。

    預設下，修訂敘述為空。若要為某次修訂新增說明，請選取該修訂，然後點擊**編輯描述**按鈕。在開啟的視窗中，輸入修訂敘述的部分文字。

應用程式標籤

卡巴斯基安全管理中心能夠讓您從應用程式登錄資料中標記應用程式。標籤是應用程式標誌，可以用於分組或尋找應用程式。分配給應用程式的標籤可以作為裝置分類中的條件。

例如，您可以建立 [瀏覽器] 標籤並分配其到所有瀏覽器（諸如 Microsoft Internet Explorer、Google Chrome、Mozilla Firefox。）

建立應用程式標籤

要建立應用程式標籤：

1. 在主功能表中，轉至 **操作 → 協力廠商應用程式 → 應用程式標籤**。
2. 點擊**新增**。

   新標籤視窗開啟。
3. 輸入標籤名稱。
4. 點擊**確定**儲存變更。

新標籤出現在應用程式標籤清單。

重命名應用程式標籤

要重命名應用程式標籤：

1. 在主功能表中，轉至 **操作 → 協力廠商應用程式 → 應用程式標籤**。
2. 選取您要重新命名之標籤旁的核取方塊，接著點擊**編輯**。

   標籤內容視窗開啟。
3. 變更標籤名稱。
4. 點擊**確定**儲存變更。

更新的標籤出現在應用程式標籤清單。

分配標籤到應用程式

要分配一個或多個標籤到一個應用程式：

1. 在主功能表中，轉至 **操作 → 協力廠商應用程式 → 應用程式登錄資料**。
2. 點擊您要分配標籤的應用程式名稱。
3. 選取**標籤**頁簽。

   標籤顯示所有存在於管理伺服器的應用程式標籤。對於指派給選取的應用程式的標記，系統會選取**分配的標籤**欄中的核取方塊。
4. 對於要指派的標籤，請在**分配的標籤**欄中選取核取方塊。
5. 點擊**儲存**以儲存變更。

標籤被分配到應用程式。

從應用程式上刪除分配的標籤

要從應用程式刪除一個或多個標籤：

1. 在主功能表中，轉至 **操作 → 協力廠商應用程式 → 應用程式登錄資料**。
2. 點擊您要刪除標籤的應用程式名稱。
3. 選取**標籤**頁簽。

   標籤顯示所有存在於管理伺服器的應用程式標籤。對於指派給選取的應用程式的標記，系統會選取**分配的標籤**欄中的核取方塊。

4. 對於您要移除的標記，請不要選取**分配的標籤**欄中的核取方塊。

5. 點擊**儲存**以儲存變更。

標籤被從應用程式刪除。

已移除應用程式的標籤不被刪除。如果您想，您可以手動刪除它們。

刪除應用程式標籤

要刪除應用程式標籤：

1. 在主功能表中，轉至 **操作 → 協力廠商應用程式 → 應用程式標籤**。

2. 在清單中，選取您想要刪除的應用程式標籤。

3. 點擊**刪除**按鈕。

4. 在開啟的視窗中，點擊**確定**。

應用程式標籤被刪除。刪除的標籤被從其分配的所有應用程式上自動刪除。

監控和報告

該部分敘述了卡巴斯基安全管理中心的監控和報告功能。這些功能給您一個基礎架構、防護狀態和統計資訊的總覽。

在卡巴斯基安全管理中心佈署之後或操作過程中，您可以配置監控和報告以適應您的需要。

方案：監控和報告

該部分提供在卡巴斯基安全管理中心中配置監控和報告功能的方案。

先決條件

在組織網路中佈署卡巴斯基安全管理中心後，您可開始監控此程式並對其功能運作產生報告。

組織網路中的監控和報告分步驟進行：

1. **設定裝置狀態轉換**

   熟悉取決於特定條件的裝置狀態設定。透過變更這些設定，您可以變更帶有*緊急*或*警告*嚴重等級的事件數量。當配置裝置狀態切換時，確保以下：

   - 新設定不與您組織的安全政策資訊衝突。

- 您可以及時對您組織網路中的重要安全事件做出反應。

2. **配置用戶端裝置上的事件通知**

   說明：

   配置用戶端裝置上的事件通知（透過郵件、SMS 或執行可執行檔）

3. **變更安全網路對病毒爆發事件的回應**

   您可以在管理伺服器內容中變更特定閾值。您也可以建立要啟動的更嚴格政策，或者建立要在事件發生時執行的工作。

4. **對嚴重、警告、資訊通知執行建議的操作**

   說明：

   對您的組織網路執行建議的操作

5. **檢視您組織網路的安全狀態**

   說明：

   - 檢閱防護狀態小工具
   - 產生並檢閱防護狀態報告
   - 產生並檢閱錯誤報告

6. **定位不被防護的用戶端裝置**

   說明：

   - 檢閱新裝置部件
   - 產生並檢閱防護佈署報告

7. **檢查用戶端裝置防護**

   說明：

   - 從防護狀態和威脅統計資料類別產生並檢閱報告
   - 啟動並檢閱緊急事件分類

8. **評估和限制資料庫上的事件負載**

   受管應用程式操作相關的事件資訊將被從用戶端電腦上傳輸並記錄至管理伺服器資料庫。要降低管理伺服器負載，評估和限制可以儲存在資料庫的最大事件數量。

   說明：

   - 資料庫空間計算
   - 限制最大事件數量

9. **檢視產品授權資訊**

   說明：

   - 新增產品授權金鑰使用小工具至控製板並加以檢閱
   - 產生並檢閱產品授權金鑰使用報告

結果

完成方案後，您被通知您組織網路的防護，因此可以為進一步防護排程操作。

關於監控和報告的類型

組織網路的安全事件資訊儲存在管理伺服器資料庫。基於事件，卡巴斯基安全管理中心 網頁主控台提供對於您組織網路的以下類型的監控和報告：

- 控製板
- 報告
- 事件分類
- 通知

控製板

儀表板透過對資訊進行圖形顯示來允許您監控您組織網路的安全趨勢。

報告

報告功能允許您獲取您組織網路的詳細安全數字資訊、儲存該資訊到檔案、透過郵件傳送它和列印它。

事件分類

事件選項提供從管理伺服器資料庫中選取的事件的命名集合的螢幕視圖。這些事件集會根據以下類別分組：

- 依嚴重等級—**緊急事件**、**功能失效**、**警告**和**資訊事件**
- 依時間—**最近事件**
- 依類型—**使用者請求**和**稽核事件**

您可以基於卡巴斯基安全管理中心網頁主控台介面上可以配置的設定，建立和檢視使用者定義的事件選項。

通知

通知會警示您關於事件的資訊，並協助您透過執行建議動作或您認為適當的動作加速回應這些事件。

儀表板和小部件

本部分包含有關儀表板和儀表板提供的小部件的資訊。該部分包括有關如何管理小部件和配置小部件設定的說明。

使用儀表板

控製板透過對資訊進行圖形顯示來允許您監控您組織網路的安全趨勢。

控製板可在卡巴斯基安全管理中心網頁主控台使用，請在**監控和報告**區段點擊**控制板**。

儀表板提供可以自訂的部件。您可以選取大量不同的部件，顯示為圓形圖、表格、圖表和清單。小部件中顯示的資訊會自動更新，更新周期為一到兩分鐘。更新間隔根據不同部件而不同。您可以在任意時刻透過設定功能表在部件上手動重新整理資料。

預設下，部件包含儲存在管理伺服器資料庫中的所有事件的資訊。

卡巴斯基安全管理中心網頁主控台具有以下類別的預設部件集：

- **防護狀態**
- **佈署**
- **更新**
- **威脅統計資料**
- **其他**

一些部件具有帶連結的文字資訊。您可以透過點擊連結檢視詳細資訊。

當配置儀表板時，您可以新增您需要的部件或隱藏您不需要的部件，變更部件的大小或外觀，移動部件以及變更它們的設定。

新增小部件到儀表板

要新增工具到儀表板：

1. 在主功能表中，轉至 **監控和報告 → 控制板**。
2. 點擊**新增或還原 Web 小部件**按鈕。
3. 在可用工具清單，選取您要新增到儀表板的工具。
   工具按類別分組。要檢視包含在類別中的工具清單，點擊類別名稱旁邊的臂章圖示（ > ）。
4. 點擊**新增**按鈕。

所選的工具被新增到儀表板結尾。

您現在可以編輯所新增工具的展示和參數。

從儀表板隱藏小部件

要從儀表板隱藏工具：

1. 在主功能表中，轉至 **監控和報告 → 控制板**。
2. 點擊您要隱藏的工具旁邊的設定圖示（⚙）。
3. 選擇**隱藏 Web 小部件**。
4. 在開啟的**警告**視窗中，點擊**確定**。

   所選工具被隱藏。稍後，您可以再次新增該工具到儀表板。

移動儀表板上的小部件

要移動工具到儀表板：

1. 在主功能表中，轉至 **監控和報告 → 控制板**。
2. 點擊您要移動的工具旁邊的設定圖示（⚙）。
3. 選擇**移動**。
4. 點擊您要移動工具的地方。您僅可以選取其他工具。

   所選工具的地方被清掃。

變更部件尺寸或樣子

對於顯示圖表的工具，您可以變更其展示–線條圖或線形圖。對於一些工具，您可以變更其大小：最小、中度或最大。

要變更工具展示：

1. 在主功能表中，轉至 **監控和報告 → 控制板**。
2. 點擊您要編輯的工具旁邊的設定圖示（⚙）。
3. 執行以下操作之一：
   - 若要顯示小工具作為條狀圖，請選取 **圖表類型：線條**。
   - 若要顯示小工具作為直線圖，請選取 **圖表類型：線形**。
   - 若要變更由小工具佔據的區域，請選取其中一個值：
     - **最小**
     - **最小（僅線條）**
     - **中度（餅圖）**
     - **中度（線條圖）**
     - **最大**

所選工具的展示被變更。

變更部件設定

要變更工具設定：

1. 在主功能表中，轉至 **監控和報告 → 控制板**。
2. 點擊您要變更的小工具旁邊的設定圖示（⚙）。
3. 選擇**顯示設定**。
4. 在開啟的工具設定視窗，變更所需的工具設定。
5. 點擊**儲存**以儲存變更。

所選工具的設定被變更。

設定集合取決於特定工具。以下是一些通用設定：

- **Web 小部件範圍**（小工具顯示資訊的物件集）—例如，管理群組或裝置分類。
- **選取工作**（小工具顯示資訊的工作）。
- **時間間隔**（小工具中顯示資訊的時間間隔）—介於兩個指定日期；從指定日期至當前日期；或從當前日期扣除目前日期的指定天數。
- **若指定以下條件，則設為"緊急"**與**若指定以下條件，則設為"警告"**（規判交通號誌燈號的規則）。

更改小部件設定後，您可以手動重新整理小部件上的資料。

要重新整理小部件上的資料：

1. 在主功能表中，轉至 **監控和報告 → 控制板**。
2. 點擊您要移動的工具旁邊的設定圖示（ ）。
3. 選擇**重新整理**。

   小部件上的資料已重新整理。

關於“僅儀表板”模式

你可以為不管理網路但希望在卡巴斯基安全管理中心中檢視網路防護統計資訊的員工（例如，高級經理）配置僅儀表板模式。當使用者啟用此模式時，只會向使用者顯示帶有一組預定義小工具的儀表板。因此，他或她可以監控小工具中指定的統計資訊，例如，所有受管理裝置的防護狀態、最近偵測到的威脅數量或網路中最常見的威脅清單。

當使用者在僅儀表板模式下工作時，將套用以下限制：

- 主功能表不向使用者顯示，因此他或她無法變更網路防護設定。
- 使用者不能用小工具執行任何操作，例如，新增或隱藏它們。因此，您需要將使用者所需的所有小工具都放在儀表板上並進行配置，例如，設定計數物件的規則或指定時間間隔。

您不能將僅儀表板模式分配給自己。如果要在此模式下工作，請聯絡系統管理員、受管理服務提供商 (MSP) 或在**一般功能：使用者權限**功能區域中具有**修改物件 ACL** 權限的使用者。

配置“僅儀表板”模式

在開始配置僅儀表板模式之前，請確保滿足以下先決條件：

- 您在**一般功能：使用者權限**功能區域中有**修改物件 ACL** 權限。如果您沒有此權限，則用於配置模式的標籤將缺失。
- 使用者在「**一般功能：基本功能**」功能區域中有**讀取**權限。

如果在您的網路中安排了管理伺服器的層次結構，為了配置僅儀表板模式，請轉到伺服器，其中使用者帳戶可在**使用者和角色 → 使用者**部分中使用。它可以是主伺服器或實體從屬伺服器。無法在虛擬伺服器上調整模式。

若要配置僅儀表板模式：

1. 在主功能表中，轉至 **使用者和角色 → 使用者**。
2. 按一下要使用小工具調整儀表板的使用者帳戶名稱。
3. 在開啟的帳戶設定視窗中，選取**儀表板**標籤。

   在開啟的標籤上，為您和使用者顯示相同的儀表板。

4. 如果**以僅儀表板模式顯示主控台**選項已啟用，用切換按鈕停用它。

   啟用此選項後，您也無法變更儀表板。停用該選項後，您可以管理小工具。

5. 配置儀表板外觀。在**儀表盤**標籤上準備的小工具集合可供具有可自訂帳戶的使用者使用。他或她不能變更小工具的任何設定或大小，也不能從儀表板新增或刪除任何小工具。因此，為使用者調整它們，以便他或她可以檢視網路防護統計資訊。為此，在**儀表板**標籤上，您可以對小部件執行於在**監控和報告→控制板**部分中相同的操作：

   - 新增小工具到儀表板。
   - 隱藏使用者不需要的小工具。
   - 移動小工具到特定的順序。
   - 變更小工具的大小或外觀。
   - 變更小工具設定。

6. 轉換切換按鈕以啟用**以僅儀表板模式顯示主控台**選項。

   之後，只有儀表板可供使用者使用。他或她可以監控統計資料，但不能變更網路防護設定和儀表板外觀。由於為您顯示的儀表板與為使用者顯示的儀表板相同，您也無法變更儀表板。

   如果您保持停用該選項，則會為使用者顯示主功能表，因此他或她可以在卡巴斯基安全管理中心中執行各種操作，包括變更安全設定和小工具。

7. 完成配置僅儀表板模式後按一下**儲存**按鈕。只有在那之後，準備好的儀表板才會顯示給使用者。

8. 如果使用者想要檢視受支援的卡巴斯基應用程式的統計資訊並且需要存取權限來執行此操作，請為使用者配置權限。之後，卡巴斯基應用程式資料將在這些應用程式的小工具中顯示給使用者。

現在使用者可以在自訂帳戶下登入卡巴斯基安全管理中心並在「僅儀表板」模式下監控網路防護統計資訊。

報告

本節介紹如何使用報告、管理自定義報告範本、使用報告範本產生新報告以及建立報告交付工作。

使用報告

報告功能允許您獲取您組織網路的詳細安全數字資訊、儲存該資訊到檔案、透過郵件傳送它和列印它。

報告可在卡巴斯基安全管理中心網頁主控台的**監控和報告**區段，透過點擊**報告**取得。

預設下，報告包含 30 天內的資訊。

卡巴斯基安全管理中心具有以下類別的預設報告集：

- **防護狀態**
- **佈署**
- **更新**

- **威脅統計資料**
- **其他**

您可以建立自訂報告範本、編輯報告範本和刪除它們。

您可以基於現有範本建立報告、匯出報告到檔案和建立報告傳送工作。

建立報告範本

要建立報告範本，請執行以下操作：

1. 在主功能表中，轉至 **監控和報告 → 報告**。
2. 點擊**新增**。

   程式將啟動"新報告範本精靈"。使用**下一步**按鈕進行精靈。
3. 輸入報告名稱並選擇報告類型。
4. 在精靈的**範圍**步驟，選取根據此報告範本，其資料會顯示在報告中的用戶端裝置集（管理群組、裝置分類、選取的裝置，或所有網路裝置）。
5. 在精靈的**報告週期**步驟，指定報告期間。有以下可用值：
   - 在兩個指定日期之間
   - 從指定日期到報告建立日期
   - 從報告建立日期減去指定天數

   該頁對一些報告可能不顯示。
6. 點擊**確定**以關閉精靈。
7. 執行以下操作之一：
   - 點擊**儲存和執行**按鈕以儲存新報告範本並據此執行報告。

     報告範本被儲存。報告被生成。
   - 點擊**儲存**按鈕以儲存新報告範本精靈。

     報告範本被儲存。

您可以使用新範本來生成和檢視報告。

檢視和編輯報告範本內容

您可以檢視和編輯報告範本的基本內容，例如，報告範本名稱或顯示在報告中的欄位。

要檢視和編輯報告範本內容：

1. 在主功能表中，轉至 **監控和報告** → **報告**。
2. 選取您要檢視並編輯其內容的報告範本旁邊的核取方塊。
   或者，您可以先產生報告，然後點擊**編輯**按鈕。
3. 點擊**開啟報告範本內容**按鈕。
   編輯報告 <報告名稱>視窗會開啟，並含有所選的**一般**頁籤。

4. 編輯報告範本內容：

- **一般**頁籤：
  - 報告範本名稱
  - **顯示項目的最大數量**

    如果啟用該選項，顯示在表格中的帶有詳細報告資料的項目數量不會超過指定值。

    報告項目首先根據指定在報告範本內容的**欄位 → 詳細資料欄位**區域的規則被儲存，然後僅第一個結果項目被儲存。帶有詳細報告資料的表頭展示顯示的項目數量和比對其他報告範本設定的可用項目總數。

    如果停用該選項，帶有詳細報告資料的表顯示所有可用項目。我們不建議您停用該選項。限制顯示的報告項目數量會降低資料庫管理系統 (DBMS) 負載，也會降低產生和匯出報告所需的時間。一些報告包含太多項目。如果是這樣，您可能難於閱讀和分析所有。而且，您的裝置可能在產生此報告時記憶體不夠，進而您將無法檢視報告。

    預設情況下已啟用該選項。預設值是 1000。

  - **群組**

    點擊**設定**按鈕以變更建立報告的用戶端裝置集。對於一些報告類型，按鈕可能不可用。實際設定取決於建立報告範本時指定的設定。

  - **時間間隔**

    點擊**設定**按鈕以修改報告時段。對於一些報告類型，按鈕可能不可用。有以下可用值：

    - 在兩個指定日期之間
    - 從指定日期到報告建立日期
    - 從報告建立日期減去指定天數

  - **包含來自從屬和虛擬管理伺服器的資料**

    如果啟用該選項，報告包含屬於建立範本的管理伺服器的從屬和虛擬管理伺服器的資訊。

    如果您要僅從目前管理伺服器檢視資料，停用該選項。

    預設情況下已啟用該選項。

  - **嵌套等級**

    報告包含位於目前管理伺服器下小於或等於指定巢狀等級的從屬和虛擬管理伺服器的資料。

    預設值是 1。如果您必須從樹中位於低等級的從屬管理伺服器接收資訊，您可能要變更該值。

  - **資料等待間隔（分鐘）**

    在產生報告之前，建立報告範本的管理伺服器等待從屬管理伺服器的資料指定分鐘數。如果在該時間段後未從從屬管理伺服器接收到資料，報告依然執行。除了實際資料，報告也會顯示從快取接收的資料（如果**從屬管理伺服器的快取資料**選項已啟用），否則為 **N/A**（不可用）。

    預設值是 5 分鐘。

- **從屬管理伺服器的快取資料**

  從屬管理伺服器定期傳輸資料到建立報告範本的管理伺服器。傳輸的資料儲存在快取。

  如果在產生報告時目前管理伺服器無法從從屬管理伺服器接收資料，報告顯示從快取接收的資料。資料傳輸到快取的日期也被顯示。

  啟用該選項允許您檢視從屬管理伺服器資訊，即便即時資料無法被獲取。然而，所顯示資料可能過期。

  預設情況下已停用該選項。

- **記憶體緩衝區更新頻率（小時）**

  從屬管理伺服器會在一定間隔時間傳輸資料到建立報告範本的管理伺服器。您可以以小時為單位指定此期間。如果指定值是 0 小時，資料僅會在產生報告時被傳輸。

  預設值是 0。

- **從從屬管理伺服器傳輸詳細資訊**

  在產生的報告中，帶有詳細報告資料的表格包含建立報告範本的管理伺服器的從屬管理伺服器的資料。

  啟用該選項會減慢報告產生並增加管理伺服器之間的流量。然而，您可以在一個報告中檢視所有資料。

  除了啟用該選項，您可能想分析詳細報告資料以偵測故障從屬管理伺服器，然後僅為該故障管理伺服器產生相同報告。

  預設情況下已停用該選項。

- **欄位**頁籤

  選取要在報告上顯示的欄位，並使用**向上移動**按鈕與**向下移動**按鈕變更這些欄位的順序。使用**新增**按鈕或**編輯** 按鈕指定報告中的資訊是否必須根據每個欄位排序或篩選。

  在**詳細欄位篩選器**區段，您也可以點擊**轉換篩選器**按鈕以開始使用延伸的篩選格式。此格式使您可以使用邏輯 OR 運算子來組合在各個欄位中指定的篩選條件。點擊該按鈕後，會開啟 **轉換篩選器** 面板。點擊 **轉換篩選器** 按鈕以確認轉換。現在，您可以使用邏輯 OR 運算子從套用的 **詳細資料欄位** 區段定義轉換篩選條件。

  將報告轉換為支援複雜篩選條件的格式將使該報告與卡巴斯基安全管理中心的早期版本（11 和更早版本）不相容。另外，轉換後的報告將不包含來自執行此類不相容版本的從屬管理伺服器的任何資料。

5. 點擊**儲存**以儲存變更。

6. 關閉**編輯報告<報告名稱>**視窗。

更新的報告範本顯示在報告範本清單。

匯出報告到檔案

您可以匯出報告到 XML、HTML 或 PDF 檔案。

要匯出報告到檔案：

1. 在主功能表中，轉至 **監控和報告 → 報告**。
2. 選取您要匯出到檔案的報告旁邊的核取方塊。
3. 點擊**匯出報告**按鈕。
4. 在開啟的視窗中，變更**名稱**欄位的報告檔案名稱。預設下，檔案名稱與所選的報告範本名稱一致。
5. 選取報告檔案類型：XML、HTML 或 PDF。
6. 點擊**匯出報告**按鈕。

   所選格式的報告將被下載到您的裝置—到您裝置的預設資料夾—或您瀏覽器中開啟的標準**另存為**視窗將允許您儲存檔案到您想要的位置。

報告被儲存到檔案。

生成和瀏覽報告

要建立和瀏覽報告，請執行以下操作：

1. 在主功能表中，轉至 **監控和報告 → 報告**。
2. 點擊要用來建立報告的報告範本名稱。

會產生並顯示使用所選範本的報告。

報告資料根據為管理伺服器設定的當地語係化顯示。

此報告將顯示下列資料：

- 在**概要**頁籤：
  - 報告名稱和類型、簡要說明和報告時間區段，以及該報告為哪個裝置群組產生的相關資訊。
  - 圖表顯示最有代表性的報告資料。
  - 帶有計算好的報告指示器的加固表格。
- 在**詳細資訊**頁籤會顯示包含詳細報告資料的表格。

建立報告傳送工作

您可以建立傳送所選報告的工作。

要建立報告傳送工作：

1. 在主功能表中，轉至 **監控和報告 → 報告**。
2. 【可選】選取您要建立報告傳送工作的報告範本旁邊的核取方塊。
3. 點擊**新報告傳送工作**按鈕。
4. 新工作精靈啟動。使用**下一步**按鈕進行精靈。
5. 在精靈的第一頁，輸入工作名稱。預設名稱為 **傳送報告(<N>)**，其中 <N> 是工作的序號。
6. 在精靈的工作設定頁面，指定以下設定：
   a. 要使用工作傳送的報告範本。如果您在步驟 2 選取了它們，請略過此步驟。
   b. 報告格式：HTML、XLS 或 PDF。
   c. 報告是否使用電子郵件連同郵件通知設定一起傳送。
   d. 報告是否被儲存到資料夾，先前在該資料夾中儲存的報告是否被覆蓋，以及是否使用特定帳戶存取資料夾（對於共用資料夾）。
7. 若要在建立工作後修改其他工作設定，請精靈的**完成工作建立**頁面啟用**建立完成時開啟工作詳情**選項。
8. 點擊**建立**按鈕以建立工作並關閉精靈。

   報告傳送工作被建立。若您啟用**建立完成時開啟工作詳情**選項，工作設定視窗隨即開啟。

刪除報告範本

要刪除一個或幾個報告範本：

1. 在主功能表中，轉至 **監控和報告 → 報告**。
2. 選取您要刪除的報告範本旁邊的核取方塊。
3. 點擊**刪除**按鈕。
4. 在開啟的視窗中，點擊**確定**按鈕以確認您的選取。

所選報告範本被刪除。如果這些報告範本被包含在報告傳送工作中，它們也被從工作刪除。

事件和事件選擇

本節提供有關事件和事件選擇、卡巴斯基安全管理中心元件中發生的事件類型以及管理頻繁事件封鎖的資訊。

關於卡巴斯基安全管理中心事件

卡巴斯基安全管理中心允許您接收受管理裝置上安裝的管理伺服器和其他 Kaspersky 應用程式的操作事件資訊。事件資訊儲存在管理伺服器資料庫。

事件類型

在卡巴斯基安全管理中心中有以下事件類型：

- 一般事件。這些事件會發生在所有受管理的 Kaspersky 應用程式中。一般事件指的像是病毒爆發。一般事件已嚴格定義語法與語意。例如，一般事件會用於報告和儀表板。
- 受管理的 Kaspersky 應用程式特定的事件。每個 Kaspersky 應用程式都擁有自己的事件集。

事件來源

事件可以由以下應用程式產生：

- 卡巴斯基安全管理中心元件：
  - 管理伺服器
  - 網路代理
  - iOS MDM 伺服器
  - Exchange 行動裝置伺服器
- 受管卡巴斯基應用程式

  有關卡巴斯基受管理應用程式產生的事件的詳細資訊，請參閱相應應用程式的文件。

您可以在應用程式政策的**事件配置**頁簽中檢視可以由應用程式生產的事件的完整清單。對於管理伺服器，您還可以在管理伺服器屬性中檢視事件清單。

事件的重要等級

每個事件都有自己的重要等級。取決於發生的條件，一個事件可以被分配不同的重要等級。四個事件重要等級如下：

- *緊急事件*指示發生了可能導致資料遺失、作業系統異常或嚴重錯誤的嚴重問題。
- *功能失效*指示在應用程式操作中或執行過程中發生了嚴重問題、錯誤或功能異常。
- *警告*是不緊急的事件，但是也指示了今後可能發生的潛在問題。如果在事件發生後應用程式可以被還原而不遺失資料或功能，則這些事件是警告等級。
- *資訊*事件用於提示成功完成操作、應用程式的正常功能或完成了某過程。

每個事件都有一個儲存期限，在這時間內您可以在卡巴斯基安全管理中心中檢視或修改。一些事件預設下不儲存在管理伺服器資料庫，因為它們的儲存期限是零。僅可以在管理伺服器資料庫中儲存至少一天的事件可以被匯出到外部系統。

使用事件分類

事件選項提供從管理伺服器資料庫中選取的事件的命名集合的螢幕視圖。這些事件集會根據以下類別分組：

- 依嚴重等級—**緊急事件**、**功能失效**、**警告**和**資訊事件**
- 依時間—**最近事件**
- 依類型—**使用者請求**和**稽核事件**

您可以基於卡巴斯基安全管理中心網頁主控台介面上可以配置的設定，建立和檢視使用者定義的事件選項。

事件分類可在卡巴斯基安全管理中心網頁主控台使用，請在**監控和報告**區段點擊**事件分類**。

預設下，事件分類包含 7 天內的資訊。

卡巴斯基安全管理中心擁有預設的事件分類集：

- 不同重要等級的事件：
  - **緊急事件**
  - **功能失效**
  - **警告**
  - **資訊事件**
- **使用者請求**（受管理應用程式事件）
- **最近事件**（上周）
- **稽核事件**。

您也可以建立和配置附加使用者定義分類。在使用者定義分類中，您可以根據裝置內容（裝置名稱、IP 範圍和管理群組）、根據事件類型和嚴重等級、根據應用程式和元件名稱、以及根據時間間隔來篩選事件。也可以包含工作結果到搜尋範圍。您也可以單一搜尋欄位，可以輸入一個詞或幾個詞。所有內容（例如事件名稱、描述、元件名稱）中包含任意所輸入詞的事件被顯示。

對於預先定義和使用者定義的分類，您可以限制顯示事件的數量或者要搜尋的記錄的數量。兩個選項都影響卡巴斯基安全管理中心顯示事件所花費的時間。資料庫越大，過程越耗時。

您可以執行以下操作：

- 編輯事件分類的內容
- 產生事件分類
- 檢視事件分類的詳細資訊

- 刪除事件分類
- 從管理伺服器資料庫中刪除事件

建立事件分類

要建立事件分類，請執行以下操作：

1. 在主功能表中，轉至 **監控和報告** → **事件分類**。
2. 點擊**新增**。
3. 在開啟的**新事件分類**視窗，指定新事件分類的設定。在視窗中重複此操作。
4. 點擊**儲存**以儲存變更。
   確認視窗開啟。
5. 若要檢視事件分類結果，請持續選取**轉到分類結果**核取方塊。
6. 點擊**儲存**以確認建立事件分類。

若您持續選取**轉到分類結果**核取方塊，會顯示事件分類結果。否則，新事件分類出現在事件分類清單。

編輯事件分類

要編輯事件分類：

1. 在主功能表中，轉至 **監控和報告** → **事件分類**。
2. 選取您要編輯的事件分類旁邊的核取方塊。
3. 點擊**內容**按鈕。
   事件分類設定視窗開啟。
4. 編輯事件分類內容。

   對於預先定義的事件分類，您盡可編輯以下頁籤的內容：**一般**（分類名稱除外）、**時間**以及**存取權限**。

   對於使用者定義分類，您可以編輯所有內容。
5. 點擊**儲存**以儲存變更。

編輯的事件分類顯示在清單。

查看事件分類清單

要檢視事件分類，請執行以下操作：

1. 在主功能表中，轉至 **監控和報告 → 事件分類**。
2. 選取您要啟動的事件分類旁邊的核取方塊。
3. 執行以下操作之一：
   - 如果您要在事件分類結果中配置排序，做以下：
     a. 點擊**重新配置排序並啟動**按鈕。
     b. 在顯示的 **重新配置事件分類排序** 視窗中指定排序設定。
     c. 請點擊選項的名稱。
   - 或者，若您要在管理伺服器上排序好事件後檢視事件清單，請點擊選項名稱。

事件分類結果被顯示。

刪除事件分類

您僅可以刪除使用者定義的事件分類。預定義事件分類無法被刪除。

要刪除一個或幾個事件分類：

1. 在主功能表中，轉至 **監控和報告 → 事件分類**。
2. 選取您要刪除的事件分類旁邊的核取方塊。
3. 點擊**刪除**。
4. 在開啟的視窗中，點擊**確定**。

事件分類被刪除。

檢視事件詳情

要檢視事件詳情：

1. 啟動事件分類。
2. 點擊所需事件的時間。
   事件內容視窗開啟。
3. 在顯示的視窗中，您可以做以下：
   - 檢視關於所選事件的資訊
   - 在事件分類結果中轉到上一個事件和下一個事件
   - 轉到發生事件的裝置
   - 轉到包含發生事件的裝置的管理群組
   - 對於工作相關事件，轉到工作內容

匯出事件到檔案

卡巴斯基安全管理中心可讓您將事件分類中的事件儲存到 TXT 檔案。

要匯出事件到檔案：

1. 啟動事件分類。
2. 選取所需事件旁邊的核取方塊。
   您也可以選擇多個事件或整個事件分類。
3. 點擊**匯出至檔案**按鈕。

所選事件被匯出到 TXT 檔案。

匯出事件到 SIEM 系統

本節將介紹如何配置匯出事件到 SIEM 系統。

設定事件匯出到 SIEM 系統

卡巴斯基安全管理中心允許透過以下方法之一進行配置：匯出到使用 Syslog 格式的任何 SIEM 系統，匯出到使用 LEEF 和 CEF 格式的 QRadar、Splunk、ArcSight SIEM 系統或直接從卡巴斯基安全管理中心將事件匯出到 SIEM 系統資料庫。完成此場景後，管理伺服器會自動將事件傳送到 SIEM 系統。

先決條件

在卡巴斯基安全管理中心中開始配置匯出事件之前：

- 深入了解事件匯出的方法。
- 確保您有系統設定值。

> 您可以按任何順序執行此場景的步驟。

將事件匯出到 SIEM 系統的過程包括以下步驟：

- **配置 SIEM 系統以接收來自卡巴斯基安全管理中心的事件**

  說明：配置在 SIEM 系統中的事件匯出

- **選取要匯出到 SIEM 系統的事件：**

  說明：

  - 管理主控台：將 Kaspersky 應用程式的事件標記為以 Syslog 格式匯出、將一般事件標記為以 Syslog 格式匯出
  - 卡巴斯基安全管理中心網頁主控台：將 Kaspersky 應用程式的事件標記為以 Syslog 格式匯出、將一般事件標記為以 Syslog 格式匯出

- **使用以下方法之一配置事件到 SIEM 系統的匯出：**

  - 使用 TCP/IP、UDP 或 TLS over TCP 通訊協定。

    說明：

    - 管理主控台：配置匯出事件到 SIEM 系統
    - 卡巴斯基安全管理中心網頁主控台：配置匯出事件到 SIEM 系統

  - 直接從卡巴斯基安全管理中心資料庫匯出事件（卡巴斯基安全管理中心 資料庫中會提供一組公用視圖；您可以在 klakdb.chm 文件找到這些公用視圖的說明）。

結果

如果您選取了要匯出的事件，配置事件匯出到 SIEM 系統後，您可以查看匯出結果。

在您開始之前

當設定在卡巴斯基安全管理中心管理主控台中自動匯出事件時，您必須指定一些 SIEM 系統設定。建議您提前檢查這些設定，以便準備設定卡巴斯基安全管理中心。

要成功配置自動傳送事件到 SIEM 系統，您必須知道以下設定：

- **SIEM 系統伺服器位址**

  安裝了目前使用的 SIEM 系統的伺服器的 IP 位址。在您的 SIEM 系統設定中檢查此值。

- **SIEM 系統伺服器連接埠**

  用於建立卡巴斯基安全管理中心和您的 SIEM 系統伺服器之間連線的埠號。您在卡巴斯基安全管理中心設定中和您 SIEM 系統的接收設定中指定該值。

- **協定**

  用於從卡巴斯基安全管理中心傳輸訊息到您的 SIEM 系統的協定。您在卡巴斯基安全管理中心設定中和您 SIEM 系統的接收設定中指定該值。

關於事件匯出

您可以將事件匯出用在處理組織和技術級別的安全問題的中心系統中，提供安全監控服務，以及從不同解決方案合併資訊。即是提供對網路硬體和應用程式生成的安全警告的即時分析的 SIEM 系統，或者安全操作中心 (SOCs)。

這些系統可以從許多來源接收資料，包括網路、安全、伺服器、資料庫和應用程式。SIEM 系統也提供功能以集成監控的資料，以便說明您避免遺失關鍵事件。而且，系統執行相關事件和警告的自動分析以通知管理員安全問題。警告可以透過儀表板實現，或可以透過協力廠商管道傳送，例如郵件。

從卡巴斯基安全管理中心匯出事件到外部 SIEM 系統的處理程序設計兩部分：事件傳送者 — 卡巴斯基安全管理中心和事件接收者 — SIEM 系統。要成功匯出事件，您必須在您的 SIEM 系統和卡巴斯基安全管理中心中對此進行配置。您可以先設定任意一端。您可以設定在卡巴斯基安全管理中心中的事件傳輸，然後設定 SIEM 系統對事件的接收，或者相反。

從卡巴斯基安全管理中心傳送事件的方法

有三種方法從卡巴斯基安全管理中心傳送事件到外部系統：

- 透過 Syslog 協定傳送事件到任意 SIEM 系統

  使用 Syslog 協定，您可以轉發發生在卡巴斯基安全管理中心管理伺服器上和受管理裝置上安裝的 Kaspersky 應用程式中的任意事件。Syslog 協定是標準訊息記錄協定。您可以用它匯出事件到任何 SIEM 系統。

  為此，您需要標記要轉送到 SIEM 系統的事件。您可在管理主控台或卡巴斯基安全管理中心 網頁主控台中標記事件。只有標記的事件才會被轉送到 SIEM 系統。如果您沒有標記任何內容，則不會轉送任何事件。

- 透過 CEF 和 LEEF 通訊協定傳送事件到 QRadar、Splunk 和 ArcSight 系統

  您可使用 CEF 和 LEEF 協定匯出一般事件。當透過 CEF 和 LEEF 協定匯出事件時，您不必能夠選取指定事件以匯出。相反，所有一般事件都被匯出。若要將卡巴斯基安全管理中心事件轉換為 CEF 和 LEEF 格式的事件，您需要使用siem_conversion_rules.xml 檔案。此檔案包含卡巴斯基安全管理中心事件屬性清單以及 CEF 和 LEEF 格式的事件的相應屬性。此外，siem_conversion_rules.xml 檔案包含用於產生與事件對應的訊息的規則。該檔案包含在卡巴斯基安全管理中心分發套件中。

  不同於 Syslog 協定，CEF 和 LEEF 協定不通用。CEF 和 LEEF 為 SIEM 系統所設計（QRadar、Splunk 和 ArcSight）。因此，當您選取透過這些協定匯出事件時，您使用 SIEM 系統所需解析器。

- 直接從卡巴斯基安全管理中心資料庫到 SIEM 系統

  以該方法匯出事件可以用於透過使用 SQL 查詢直接從資料庫公共視圖接收事件。查詢結果被儲存到 XML 檔案，可以用於外部系統的輸入資料。僅僅公共視圖中的事件可以被直接從資料庫中匯出。

透過 SIEM 系統接收事件

SIEM 系統必須接收和正確解析來自卡巴斯基安全管理中心的事件。因為這些目的，您必須正確設定 SIEM 系統。設定取決於特定的 SIEM 系統。然而，有一些設定所有 SIEM 系統的通用步驟，例如設定接收器和解析器。

配置在 SIEM 系統中的事件匯出

從卡巴斯基安全管理中心匯出事件到外部 SIEM 系統的處理程序設計兩部分：事件傳送者 — 卡巴斯基安全管理中心和事件接收者 — SIEM 系統。您必須在您的 SIEM 系統和卡巴斯基安全管理中心管理主控台中設定事件匯出。

您在 SIEM 系統中指定的設定取決於您使用的系統。通常，對於所有 SIEM 系統，您必須設定接收器和訊息解析器（可選）以解析接收的事件。

設定接收器

為了接收卡巴斯基安全管理中心傳送的事件，您必須在您的 SIEM 系統中設定接收器。通常，必須在 SIEM 系統指定以下設定：

- **匯出協定或輸入類型**

  它是訊息傳輸協定，TCP/IP 或 UDP。該協定必須與您在卡巴斯基安全管理中心中指定的協定相同。

- **連接埠**

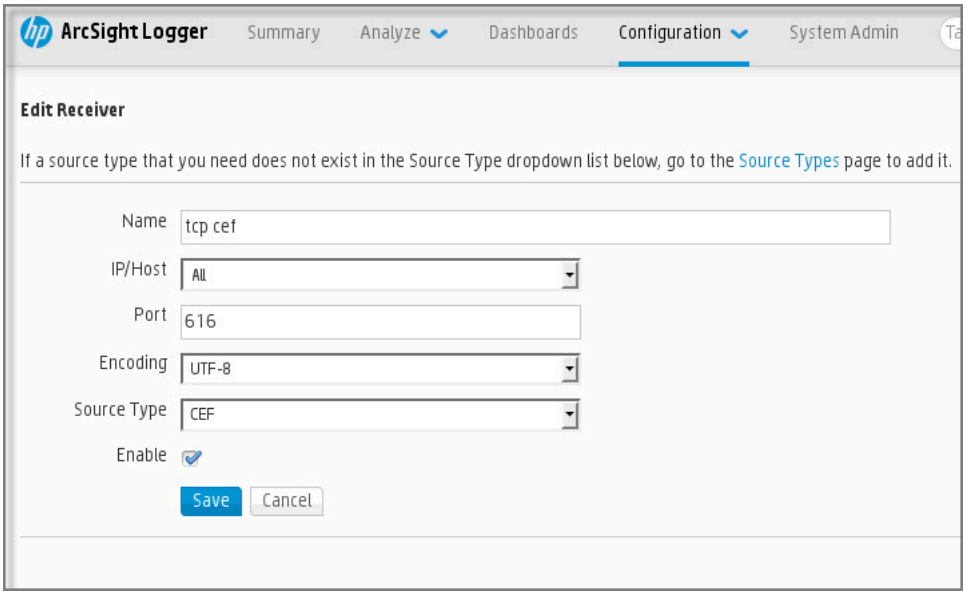
  連線到卡巴斯基安全管理中心的埠號。該連接埠必須與您在卡巴斯基安全管理中心中指定的連接埠相同。

- **訊息協定或來源類型**

  用於匯出事件到 SIEM 系統的協定。它可以是標準協定之一：Syslog、CEF 或 LEEF。SIEM 系統依據您指定的協定選取訊息解析器。

依據所使用的 SIEM 系統，您可能需要指定一些附加接收器設定。

下圖顯示 ArcSight 的接收器設定截圖。



ArcSight 的接收器設定

訊息解析器

匯出的事件作為訊息被傳遞到 SIEM 系統。這些訊息必須正確解析，以便事件資訊可以被 SIEM 系統使用。訊息解析器是 SIEM 系統的一部分，它們用於拆分訊息屬性到相關欄位，例如事件 ID、嚴重等級、敘述、參數。這將啟用 SIEM 系統以處理從卡巴斯基安全管理中心接收的事件，以便它們可以被儲存在 SIEM 系統資料庫。

標記事件，將其以 Syslog 格式匯出到 SIEM 系統

在啟用自動匯出事件後，您必須選取將被匯出到外部 SIEM 系統的事件。

您可以根據以下條件之一，設定以 Syslog 格式將事件匯出到外部系統：

- 標記一般事件。如果您在政策、事件設定或在管理伺服器設定中，標記要匯出的事件，SIEM 系統將接收由特定政策管理的所有應用程式上發生的所選事件。如果匯出的事件在政策中被選中，您將不能為由該政策管理的個別應用程式重新定義所選事件。

- 標記受管理應用程式的事件。如果您在受管理裝置上為安裝的受管理應用程式標記要匯出的事件，SIEM 系統將僅接收發生在該應用程式中的事件。

關於標記事件並將其以 Syslog 格式匯出到 SIEM 系統

在啟用自動匯出事件後，您必須選取將被匯出到外部 SIEM 系統的事件。

您可以根據以下條件之一，設定以 Syslog 格式將事件匯出到外部系統：

- 標記一般事件。如果您在政策、事件設定或在管理伺服器設定中，標記要匯出的事件，SIEM 系統將接收由特定政策管理的所有應用程式上發生的所選事件。如果匯出的事件在政策中被選中，您將不能為由該政策管理的個別應用程式重新定義所選事件。

- 標記受管理應用程式的事件。如果您在受管理裝置上為安裝的受管理應用程式標記要匯出的事件，SIEM 系統將僅接收發生在該應用程式中的事件。

將 Kaspersky 應用程式的事件標記為以 Syslog 格式匯出

如果您要匯出發生在特定受管理裝置上安裝的個別受管理應用程式中的事件，標記要在應用程式政策中匯出的時間。在這種情況下，標記的事件將從注冊範圍內的所有裝置中匯出。

若要為特定受管理應用程式標記要匯出的事件：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。
2. 點擊您要爲其標記事件的應用程式的政策。

   政策設定視窗隨即開啟。
3. 轉到**事件配置**部分。
4. 選取您要匯出到 SIEM 系統的事件旁邊的核取方塊。
5. 點擊**透過使用 Syslog 標記為匯出到 SIEM 系統**按鈕。

   您還可以在 **事件註冊** 部分中標記匯出到 SIEM 系統的事件，它可透過點擊事件連結開啟。
6. 一個複選標記 (✓) 出現在您標記為匯出到 SIEM 系統的一個或多個事件的欄的 **Syslog** 中。
7. 點擊**儲存**按鈕。

受管理應用程式中的標記事件已準備好匯出到 SIEM 系統。

您可以為特定受管理裝置標記要匯出到 SIEM 系統的事件。如果先前匯出的事件在應用程式的政策中標記過，您將不能為受管理的裝置重新定義標記的事件。

若要為受管理裝置標記要匯出的事件：

1. 在主功能表中，轉至 **裝置 → 受管理裝置**。
   受管理裝置清單隨即顯示。
2. 點擊所需裝置名稱在受管理裝置清單中的連結。
   所選裝置的屬性視窗隨即顯示。
3. 轉到**應用程式**區域。
4. 點擊所需應用程式名稱在應用程式清單中的連結。
5. 轉到**事件配置**部分。
6. 選取您要匯出到 SIEM 的事件旁邊的核取方塊。
7. 點擊**透過使用 Syslog 標記為匯出到 SIEM 系統**按鈕。

   此外，您可以在 **事件註冊** 部分中標記匯出到 SIEM 系統的事件，它可透過點擊事件連結開啟。

8. 一個複選標記 (✓) 出現在您標記為匯出到 SIEM 系統的一個或多個事件的欄的 **Syslog** 中。

從現在開始，如果配置了匯出到 SIEM 系統，管理伺服器會將標記的事件發送到 SIEM 系統。

標記一般事件，將其以 Syslog 格式匯出

您可以使用 Syslog 格式標記管理伺服器將匯出到 SIEM 系統的一般事件。

標記一般事件以匯出到 SIEM 系統：

1. 執行以下操作之一：
   - 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示 ( ) 。
   - 轉到**裝置 → 政策和設定檔**，然後點擊某個政策的連接。
2. 在開啟的視窗中，請前往**事件配置**頁籤。
3. 點擊**透過使用 Syslog 標記為匯出到 SIEM 系統**。

   此外，您可以在 **事件註冊** 部分中標記匯出到 SIEM 系統的事件，它可透過點擊事件連結開啟。

4. 一個複選標記 (✓) 出現在您標記為匯出到 SIEM 系統的一個或多個事件的欄的 **Syslog** 中。

從現在開始，如果配置了匯出到 SIEM 系統，管理伺服器會將標記的事件發送到 SIEM 系統。

使用 CEF 和 LEEF 格式匯出事件

您可使用 CEF 和 LEEF 格式來將一般事件以及由 Kaspersky 應用程式傳輸至管理伺服器的事件匯出至 SIEM 系統。匯出事件集是預定義的，您無法選取要匯出的事件。在將事件傳送到 SIEM 系統（QRadar、ArcSight 或 Splunk）之前，需要使用siem_conversion_rules.xml 檔案中指定的規則將卡巴斯基安全管理中心事件解釋為 CEF 和 LEEF 格式的事件。

基於使用的 SIEM 系統選取匯出格式。下表顯示了 SIEM 系統和對應的匯出格式。

匯出事件到 SIEM 系統的格式

SIEM 系統	匯出格式
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF（記錄事件延伸格式）是 IBM Security QRadar SIEM 的自訂事件格式。QRadar 可以整合、識別和處理 LEEF 事件。LEEF 事件必須使用 UTF-8 字元編碼。您可以在 IBM Knowledge Center 檢視 LEEF 協定的詳情。

- CEF（通用事件格式）—開放式日誌管理標準，涉及來自不同的網路裝置和應用程式的安全資訊的協同工作。CEF 允許您使用通用日誌格式，因此資料可以被簡易整合以用企業管理系統分析。CEF 事件必須使用 UTF-8 字元編碼。

自動匯出意味著卡巴斯基安全管理中心傳送一般事件到 SIEM 系統。事件自動匯出在您啟用後立即開始。該部分詳細解釋了如何啟用自動事件匯出。

關於使用 Syslog 格式匯出事件

您可以使用 Syslog 格式匯出管理伺服器和受管理裝置上安裝的其他 Kaspersky 應用程式中發生的事件到 SIEM 系統。

Syslog 是訊息記錄協定的標準。它允許分離生成訊息的軟體、儲存訊息的系統和報告和分析訊息的軟體。每個訊息都帶有裝置代碼標籤，指示生成訊息的軟體類型，並被分配嚴重等級。

Syslog 格式由 Request for Comments (RFC) 文件定義，該文件由 Internet Engineering Task Force（網際網路標準）發佈。RFC 5424 標準用於從卡巴斯基安全管理中心匯出事件到外部系統。

在卡巴斯基安全管理中心中，您可以設定使用 Syslog 格式匯出事件到外部系統。

匯出過程包含兩個步驟：

1. 啟用自動事件匯出。在該步驟，卡巴斯基安全管理中心被設定，以便能傳送事件到 SIEM 系統。卡巴斯基安全管理中心在您啟用自動匯出後立即開始傳送事件。

2. 選取事件以匯出到外部系統。在該步驟，您可以選取匯出哪些事件到 SIEM 系統。

配置卡巴斯基安全管理中心以將事件匯出到 SIEM 系統

本文將介紹如何配置匯出事件到 SIEM 系統。

在將事件傳送到 SIEM 系統（QRadar、ArcSight 或 Splunk）之前，需要使用siem_conversion_rules.xml檔案中指定的規則將卡巴斯基安全管理中心事件解釋為 CEF 和 LEEF 格式的事件。

若要在卡巴斯基安全管理中心 網頁主控台中配置匯出到 SIEM 系統：

1. 在主功能表中，轉至 **主控台設定 → 整合**。
2. 在**整合**頁籤，選取**SIEM**區域。
3. 點擊**設定**連結。

   匯出設定區域將開啟。

4. 在**匯出設定**區域中指定設定：

- **SIEM 系統伺服器位址**

  安裝了目前使用的 SIEM 系統的伺服器的 IP 位址。在您的 SIEM 系統設定中檢查此值。

- **SIEM 系統連接埠**

  用於建立卡巴斯基安全管理中心和您的 SIEM 系統伺服器之間連線的埠號。您在卡巴斯基安全管理中心設定中和您 SIEM 系統的接收設定中指定該值。

- **協定**

選取該協定用於傳輸訊息到 SIEM 系統。您可以選取 TCP、UDP 或 TLS over TCP 通訊協定。

如果您透過 TCP 通訊協定選取 TLS，則可以指定以下 TLS 設定：

- **伺服器身分驗證**

  在**伺服器身分驗證**欄位，您可以選擇**受信任的憑證**或者 **SHA 指紋**值：

  - **受信任的憑證**。您可以從受信任的憑證頒發機構 (CA) 接收完整的憑證鏈（包含根憑證），並將該檔案上傳到卡巴斯基安全管理中心。卡巴斯基安全管理中心會檢查 SIEM 系統伺服器的憑證鏈是否也由受信任的 CA 簽署。

    要新增受信任的憑證，請點擊**瀏覽 CA 憑證檔案**按鈕，然後上傳憑證。

  - **SHA 指紋**。您可以在卡巴斯基安全管理中心中指定 SIEM 系統完整憑證鏈（包含根憑證）的 SHA1 指紋。要新增 SHA1 指紋，請在**指紋**欄位中輸入該指紋，然後點擊**新增**按鈕。

  透過使用**新增用戶端身分驗證**設定，您可以產生憑證來驗證卡巴斯基安全管理中心。因此，您將使用卡巴斯基安全管理中心發佈的自簽章憑證。在此情況下，您可以同時使用受信任的憑證和 SHA 指紋來驗證 SIEM 系統伺服器。

- **新增主體名稱/主體別名**

  主體名稱是接收憑證的網域。如果 SIEM 系統伺服器的網域與 SIEM 系統伺服器憑證的主體名稱不符，卡巴斯基安全管理中心將無法連線到 SIEM 系統伺服器。但是，如果憑證中的名稱已變更，則 SIEM 系統伺服器可以變更其網域名稱。在此情況下，您可以在 **新增主體名稱/主體別名**欄位中指定主體名稱。如果任何指定的主體名稱與 SIEM 系統憑證的主體名稱匹配，卡巴斯基安全管理中心將驗證 SIEM 系統伺服器憑證。

- **新增用戶端身分驗證**

  對於用戶端身分驗證，您可以插入您的憑證或在卡巴斯基安全管理中心中產生它。

  - **插入憑證**。您可以使用從任何來源（例如，從任何受信任的憑證頒發機構）收到的憑證。您必須使用以下憑證類型之一指定憑證及其私密金鑰：

    - **X.509 憑證 PEM**。在**包含憑證的檔案**欄位中上傳帶有憑證的檔案，在**包含金鑰的檔案**欄位中上傳帶有私密金鑰的檔案。這兩個檔案互不相依，檔案的載入順序並不重要。當兩個檔案都上傳後，在**密碼或者憑證驗證**欄位中指定解碼私密金鑰的密碼。如果未編碼私密金鑰未編碼，則密碼可以為空值。

    - **X.509 憑證 PKCS12**。上傳包含憑證及其私密金鑰的單個檔案到**包含憑證的檔案**欄位。當兩個檔案都上傳後，在**密碼或者憑證驗證**欄位中指定解碼私密金鑰的密碼。如果未編碼私密金鑰未編碼，則密碼可以為空值。

  - **生產金鑰**。您可以在卡巴斯基安全管理中心中產生自簽章憑證。結果，卡巴斯基安全管理中心儲存自簽章憑證，您可以將憑證的公共部分或 SHA1 指紋傳遞給 SIEM 系統。

- 日期格式

  您可以根據 SIEM 系統的要求選擇系統日誌、CEF 或 LEEF 格式。

如果選取 Syslog 格式，則必須指定：

- 事件訊息的最大大小（位元組）

指定 SIEM 系統訊息的最大大小。每個事件被一條訊息轉發。如果訊息的精確長度超過指定值，訊息被截斷且資料可能遺失。預設大小是 2048 位元組。如果您在“**Protocol**”欄位中選取了系統日誌格式，則可使用該欄位。

5. 將選項切換到**自動匯出事件至 SIEM 系統資料庫 已啟用**位置。
6. 點擊**儲存**按鈕。

匯出到 SIEM 系統已配置。

直接從資料庫匯出事件

您可以直接從卡巴斯基安全管理中心資料庫接收事件，而不必使用卡巴斯基安全管理中心介面。您可以直接查詢公共視圖並接收事件資料，或基於現有公共視圖建立您自己的視圖並定位它們以獲取您需要的資料。

公共視圖

為了您的方便，在卡巴斯基安全管理中心資料庫中提供了公共視圖集。您可以在 klakdb.chm 文件中找到這些公共視圖的敘述。

v_akpub_ev_event 公共視圖包含一組展示資料庫中事件參數的欄位集。在 klakdb.chm 文件中您也可以尋找對應於其他卡巴斯基安全管理中心實體的公共視圖資訊，例如，裝置、應用程式或使用者。您可以在您的查詢中使用該資訊。

該部分包含了使用 klsql2 實用程式執行 SQL 查詢的說明以及查詢例子。

要建立 SQL 查詢或資料庫視圖，您也可以使用其他程式以操作資料庫。關於如何檢視連線到卡巴斯基安全管理中心資料庫的參數的資訊，例如實例名稱和資料庫名稱，在對應區域給出。

使用 klsql2 實用程式執行 SQL 查詢

本文敘述了如何下載和使用 klsql2 實用程式，以及如何使用該實用程式執行 SQL 查詢。

要使用 klsql2 公用程式：

1. 在卡巴斯基安全管理中心的安裝資料夾中查找 klsql2 實用程式。預設安裝路徑：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.不要使用適用於舊版卡巴斯基安全管理中心的 klsql2 實用程式版本。
2. 在任何文字編輯器中建立副檔名為 .sql 的檔案，然後將該檔案與公用程式放在同一資料夾中。
3. 在建立的 .sql 檔案中，輸入所需的 SQL 查詢，然後儲存該檔案。
4. 在安裝了卡巴斯基安全管理中心管理伺服器的裝置上，在命令列，輸入以下命令以從 .sql 檔案執行 SQL 查詢並儲存結果到 result.xml 檔案：
   ```
   klsql2 -i src.sql -u <使用者名稱> -p <密碼> -o result.xml
   ```
   其中 <使用者名稱> 和 <密碼> 是有權存取資料庫的使用者帳戶的憑據。
5. 如果需要，輸入有權存取資料庫的使用者帳戶的登入名稱和密碼。
6. 開啟新建立的 result.xml 檔案以檢視 SQL 查詢結果。

您可以編輯 .sql 檔案並建立到公共視圖的任意 SQL 查詢。然後，從命令列，執行您的 SQL 查詢並儲存結果到檔案。

klsql2 實用程式中的 SQL 查詢例子

該部分顯示 SQL 查詢的例子，透過 klsql2 實用程式執行。

以下例子闡述了對過去七天發生在裝置上的事件的獲取，並依據事件發生時間顯示事件。首先顯示最近的事件。

示例：

```
SELECT

/* 事件標識 */
e.nId,

/* 事件發生的時間 */
e.tmRiseTime,

/* 事件類型的內部名稱 */
e.strEventType,

/* 事件的顯示名稱 */
e.wstrEventTypeDisplayName,

/* 事件的顯示敘述 */
e.wstrDescription,

/* 事件所在的群組名稱 */
e.wstrGroupName,

/* 發生事件的裝置的顯示名稱 */
h.wstrDisplayName,
CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +

/* 發生事件的裝置的 IP 位址 */
CAST(((h.nIp) & 255) AS varchar(4)) as strIp
FROM v_akpub_ev_event e
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

檢視卡巴斯基安全管理中心資料庫名稱

如果您要透過 SQL Server、MySQL 或 MariaDB 資料庫管理工具存取卡巴斯基安全管理中心，您必須知道資料庫的名稱以便從您的 SQL 指令碼編輯器連線。

要檢視卡巴斯基安全管理中心資料庫名稱：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。

   管理伺服器內容視窗將開啟。

2. 在**一般**頁簽上，選擇**目前資料庫詳情**區域。

   資料庫名稱在**資料庫名稱**欄位中指定。使用資料庫名稱在您的 SQL 查詢中定位資料庫。

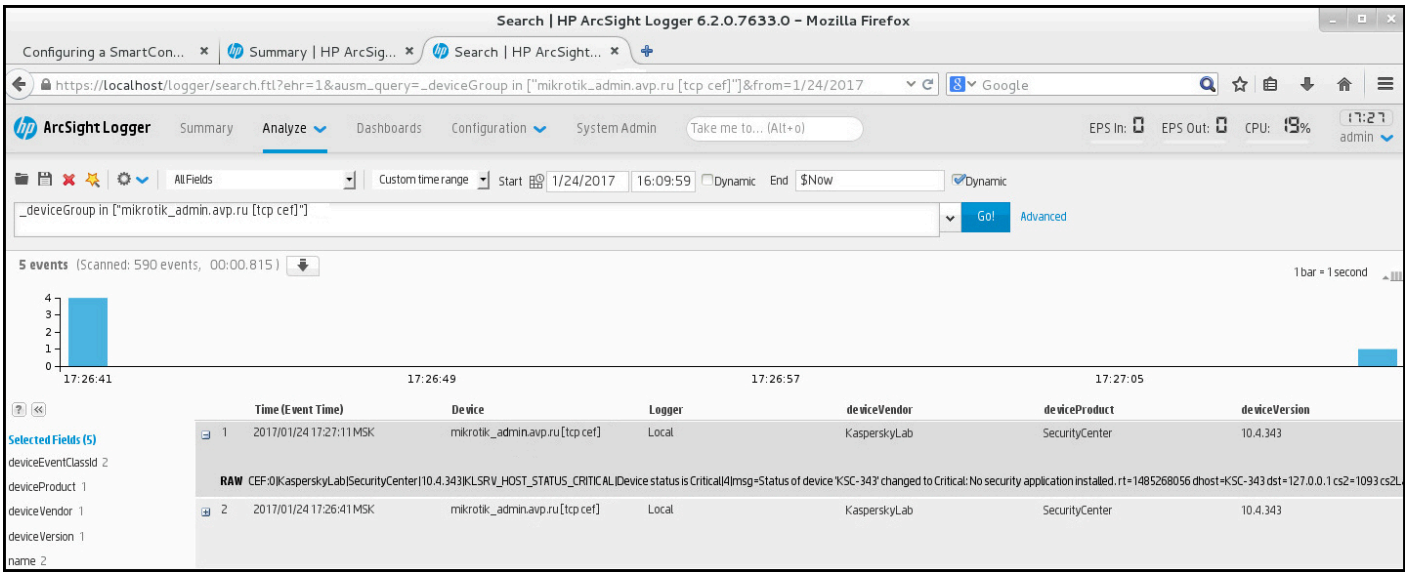
檢視匯出結果

您可以控制事件匯出過程的成功完成。為此，檢查帶有匯出事件的郵件是否被您的 SIEM 系統接收。

如果從卡巴斯基安全管理中心傳送的事件被接收並被您的 SIEM 系統正確解析，兩端的設定被正確完成。否則，檢查您在卡巴斯基安全管理中心中指定的設定是否與您的 SIEM 系統中的設定一致。

下圖顯示匯出到 ArcSight 的事件。例如，第一個事件是緊急的管理伺服器事件：「*Device status is Critical*」。

匯出事件在您 SIEM 系統中的顯示隨您使用的 SIEM 系統而不同。



例子事件

從事件檢視物件歷程

從建立或修改支援修訂管理的物件的事件，您可以切換到物件的修訂歷程。

要從事件檢視物件歷程：

1. 啟動事件分類。
2. 選取所需事件旁邊的核取方塊。
3. 點擊**變更歷程**按鈕。

   物件修訂歷程被開啟。

刪除事件

要刪除一個或幾個事件：

1. 啟動事件分類。
2. 選取所需事件旁邊的核取方塊。
3. 點擊**刪除**按鈕。

   所選事件被刪除且無法還原。

設定事件儲存期限

卡巴斯基安全管理中心允許您接收受管理裝置上安裝的管理伺服器和其他 Kaspersky 應用程式的操作事件資訊。事件資訊儲存在管理伺服器資料庫。您可能需要比預設值將一些事件儲存較長或較短的時間。您可以變更事件儲存期限的預設設定。

若您有意在管理伺服器資料庫中儲存部分事件，您可在管理伺服器政策和 Kaspersky 應用程式政策或管理伺服器內容中停用適當設定（僅限管理伺服器事件）。這將降低資料庫中的事件類型數量。

事件的儲存期限越長，資料庫達到最大值速度越快。然而，較長期的事件可讓您執行較長時間的監控與回報工作。

要為管理伺服器中的事件設定儲存期限：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。
2. 點擊所需政策的名稱。

   您可以選擇受管理卡巴斯基應用程式、網路代理或管理伺服器的政策。對於管理伺服器，您也可以透過點擊位於所需管理伺服器的名稱旁的設定圖示 () 來配置事件的儲存期限。
3. 選擇**事件配置**標籤。

   與**緊急**區段相關的事件類型清單隨即顯示。如果需要，您可以移動到**功能失效**、**警告**或**資訊**部分。
4. 在右側面板中的事件類型清單中，點擊您要變更其儲存期限的事件的連結。

   在開啟的視窗的**事件註冊**區段，會啟用**儲存在管理伺服器資料庫上（天）**切換開關。
5. 在該開關按鈕下面的編輯方塊中，輸入儲存事件的天數。
6. 若您要在管理伺服器資料庫儲存事件，請停用**儲存在管理伺服器資料庫上（天）**選項。

   若您在管理伺服器內容視窗中設定管理伺服器事件，以及若事件設定在卡巴斯基安全管理中心管理伺服器政策中鎖定，您無法重新定義事件的儲存期限值。
7. 按一下**確定** ，然後在右側窗格關閉後，按一下**儲存**按鈕。

   政策內容視窗隨即關閉。

從現在開始，當管理伺服器接收並儲存所選類型的事件時，它們將具有變更的儲存期限。管理伺服器不會變更以前接收到的事件的儲存期限。

卡巴斯基安全管理中心元件的事件

每個 Kaspersky 元件都擁有自己的事件類型集。該區域列出出現在卡巴斯基安全管理中心管理伺服器、網路代理、iOS MDM 伺服器和 Exchange 行動裝置伺服器的事件類型。Kaspersky 應用程式中發生的事件類型不在此區域列出。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。對於管理伺服器，您還可以在管理伺服器屬性中檢視和設定事件清單。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

事件類型描述的資料結構

對於每個事件類型，它的顯示名稱、ID、字母碼、描述和預設儲存期限被提供。

- **事件類型顯示名稱**。該文字當您配置事件時和它們發生時被顯示在卡巴斯基安全管理中心中。
- **事件類型 ID**。該數碼在您使用協力廠商工具分析事件時使用。
- **事件類型**（字母碼）。該代碼用於您使用卡巴斯基安全管理中心資料庫中提供的公共視圖瀏覽和處理事件時以及事件被匯出到 SIEM 系統時。
- **敘述**。該文字包含事件發生的情況以及此種情況下您可以做的事。
- **預設儲存期限**。這是事件儲存在管理伺服器資料庫的天數，顯示在管理伺服器事件清單中。該時間段之後，事件被刪除。如果事件儲存期限值是 0，此類事件被偵測但不顯示在管理伺服器事件清單。如果您設定了儲存此類事件到作業系統事件記錄，您可以在那裡找到它們。

  您可以變更事件儲存期限：

  - 管理主控台：設定事件儲存期限
  - 卡巴斯基安全管理中心網頁主控台：設定事件儲存期限

其他資料可能包含以下欄位：

- **event_id**：資料庫中獨特的事件編號，由系統自動產生與指派；請勿與**事件類型 ID** 混淆。
- **Task_id**：造成事件發生的工作 ID（如有）
- **severity**：其中一個以下嚴重等級（以嚴重等級的遞增順序排列）：

  0) 無效的嚴重等級

  1) 資訊

  2) 警告

  3) 錯誤

  4) 緊急

管理伺服器事件

該部分包含管理伺服器相關事件資訊。

管理伺服器緊急事件

下表顯示具有**緊急**重要等級的卡巴斯基安全管理中心管理伺服器事件類型。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。對於管理伺服器，您還可以在管理伺服器屬性中檢視和設定事件清單。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

如果您在管理主控台的管理伺服器內容視窗中指定了連接埠，**卡巴斯基安全管理中心會發布其指標**和關鍵事件，以供 Prometheus（一個用於監控和警報的系統）取得。Prometheus 取得指標和關鍵事件，然後為每個事件產生警報。

// KL.KSC.Common—Kaspersky Security Center common counters

"xdr_klserver_errors", "counter", "klserver errors"

"xdr_klserver_api_calls_time", "counter", "klserver api calls time"

// KL.KSC.Transport—Transport counters set

"ksc_Transport__Number_of_all_connections", "counter", "number of all connections"

"ksc_Transport__Number_of_all_nagent_connection", "counter", "number of all Network Agent connection"

"ksc_Transport__Number_of_controlled_nagent_connections", "counter", "number of controlled Network Agent connections"

"ksc_Transport__Total_active_hosts_count", "gauge", "total active devices count"

"ksc_Transport__Number_of_pings_processed", "counter", "number of pings processed"

"ksc_Transport__Number_of_pings_rejected", "counter", "number of pings rejected"

"ksc_Transport__Number_of_ping_processing_errors", "counter", "number of ping processing errors"

"ksc_Transport__Number_of_TCP_connections_accepted", "counter", "number of TCP connections accepted"

"ksc_Transport__Number_of_failed_TCP_connections", "counter", "number of failed TCP connections"

"ksc_Transport__Bytes_sent_by_TCP", "counter", "bytes sent by TCP"

"ksc_Transport__Bytes_received_by_TCP", "counter", "bytes received by TCP"

"ksc_Transport__Number_of_GetNextFileChunk_requests", "counter", "number of GetNextFileChunk requests"

"ksc_Transport__Number_of_GetNextFileChunk_rejected", "counter", "number of GetNextFileChunk rejected"

"ksc_Transport__Bytes_transmitted_through_GetNextFileChunk", "counter", "bytes transmitted through GetNextFileChunk"

// KL.KSC.Events—Events delivery counters set

"ksc_Events__Number_of_event_bulks_processed", "counter", "number of event bulks processed"

"ksc_Events__Number_of_event_bulks_rejected", "counter", "number of event bulks rejected"

"ksc_Events__Number_of_event_bulks_processing_errors", "counter", "number of event bulks processing errors"

"ksc_Events__Number_of_event_bulks_processing_just_now", "gauge", "number of event bulks processing just now"

"ksc_Events__Number_of_events_processed", "counter", "number of events processed"

"ksc_Events__Number_of_events_rejected", "counter", "number of events rejected"

"ksc_Events__Number_of_events_processing_errors", "counter", "number of events processing errors"

"ksc_Events__Number_of_events_processing_just_now", "gauge", "number of events processing just now"

// KL.KSC.Resources—Kaspersky Security Center resources usage

"ksc_Resources__CPU_time_in_user_mode", "counter", "CPU time in user mode"

"ksc_Resources__CPU_time_in_kernel_mode", "counter", "CPU time in kernel mode"

"ksc_Resources__PID_of_klserver_process", "gauge", "process ID of klserver"

"ksc_Resources__PID_of_klnagent_process", "gauge", "process ID of klnagent"

"ksc_Resources__Available_disk_user_quota_for_server_data", "gauge", "available disk user quota for server data"

"ksc_Resources__Available_disk_user_quota_for_packages", "gauge", "available disk user quota for packages"

"ksc_Resources__Current_OpenAPI_threads_count", "counter", "current OpenAPI threads count"

"ksc_Resources__Maximum_OpenAPI_threads_count", "counter", "maximum OpenAPI threads count"

// KL.KSC.NLST

// KL.KSC.NLST.Trans.Common—List of server transactions

"ksc_NLST__Common__Current_transactions_count", "gauge", "current transactions count"

"ksc_NLST__Common__Transactions_queue_ful", "gauge", "transactions queue full"

"ksc_NLST__Common__Transactions_queue_near_to_ful", "gauge", "transactions queue near to full"

// KL.KSC.NLST.InvAppCtrlLink—Application Control link

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvSoft—Software Inventory

"ksc_NLST__Software_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Software_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Software_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Software_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Software_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Software_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Software_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Software_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Software_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvHard—Hardware Inventory

"ksc_NLST__Hardware_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Hardware_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Hardware_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Hardware_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Hardware_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Hardware_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Hardware_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Hardware_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Hardware_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DevCtrl—Device Control

"ksc_NLST__Device_control__items_changed", "gauge", "items changed"

"ksc_NLST__Device_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_control__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDM—Mobile Device Management

"ksc_NLST__Mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__Mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDMmails—Device management emails

"ksc_NLST__Device_management_emails__items_changed", "gauge", "items changed"

"ksc_NLST__Device_management_emails__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_management_emails__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_management_emails__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_management_emails__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_management_emails__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_management_emails__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_management_emails__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_management_emails__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AppCtrl—Application Control

"ksc_NLST__Application_control__items_changed", "gauge", "items changed"

"ksc_NLST__Application_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_control__transactions_in_queue", "gauge", "transactions in queue"

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DPEErrors—Data protection errors

"ksc_NLST__Data_protection_errors__items_changed", "gauge", "items changed"

"ksc_NLST__Data_protection_errors__items_deleted", "gauge", "items deleted"

"ksc_NLST__Data_protection_errors__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Data_protection_errors__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Data_protection_errors__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Data_protection_errors__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Data_protection_errors__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Data_protection_errors__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Data_protection_errors__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.iOsMDM—iOS Mobile Device Management

"ksc_NLST__iOS_mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__iOS_mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__iOS_mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__iOS_mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__iOS_mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__iOS_mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__iOS_mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Vapm—Vulnerability assessment and patch management

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment_and_patch_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment_and_patch_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Va—Vulnerability assessment

"ksc_NLST__Vulnerability_assesment__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.VM—Virtual machines

"ksc_NLST__Virtual_machines__items_changed", "gauge", "items changed"

"ksc_NLST__Virtual_machines__items_deleted", "gauge", "items deleted"

"ksc_NLST__Virtual_machines__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Virtual_machines__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Virtual_machines__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Virtual_machines__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Virtual_machines__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Virtual_machines__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Virtual_machines__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.WUS—Windows Update

"ksc_NLST__Windows_update__items_changed", "gauge", "items changed"

"ksc_NLST__Windows_update__items_deleted", "gauge", "items deleted"

"ksc_NLST__Windows_update__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Windows_update__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Windows_update__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Windows_update__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Windows_update__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Windows_update__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Windows_update__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.CIP_PLC—CIP PLC

"ksc_NLST__CIP_PLC__items_changed", "gauge", "items changed"

"ksc_NLST__CIP_PLC__items_deleted", "gauge", "items deleted"

"ksc_NLST__CIP_PLC__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__CIP_PLC__change_item_operations", "gauge", "change item operations"

"ksc_NLST__CIP_PLC__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__CIP_PLC__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__CIP_PLC__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__CIP_PLC__list_is_pending", "gauge", "list is pending"

"ksc_NLST__CIP_PLC__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.NagentNetScan—Network Agent Network Scan

"ksc_NLST__Network_scan__items_changed", "gauge", "items changed"

"ksc_NLST__Network_scan__items_deleted", "gauge", "items deleted"

"ksc_NLST__Network_scan__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Network_scan__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Network_scan__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Network_scan__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Network_scan__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Network_scan__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Network_scan__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AS—Adaptive Security

"ksc_NLST__Adaptive_security__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.ASS—Adaptive Security State

"ksc_NLST__Adaptive_security_state__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security_state__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security_state__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security_state__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security_state__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security_state__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security_state__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security_state__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security_state__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.KillChain—Kill Chain

"ksc_NLST__Kill_chain__items_changed", "gauge", "items changed"

"ksc_NLST__Kill_chain__items_deleted", "gauge", "items deleted"

"ksc_NLST__Kill_chain__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Kill_chain__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Kill_chain__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Kill_chain__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Kill_chain__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Kill_chain__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Kill_chain__transactions_in_queue", "gauge", "transactions in queue"

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
已超過產品授權數量限制	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	每天一次，卡巴斯基安全管理中心 Linux 檢查是否超過產品授權限制。 當管理伺服器發現安裝在用戶端裝置上的 Kaspersky 應用程式超過了產品授權限制，以及由單一產品授權覆寫的目前使用的產品授權單元數量超過了該產品授權覆寫的單元總數的 110%，則該類型的事件發生。 即便當該事件發生時，用戶端裝置是被防護的。 您可以透過以下方式回應事件： • 檢視受管理裝置清單。刪除不在使用的裝置。 • 為更多裝置提供產品授權（新增有效的啟動碼或金鑰檔案至管理伺服器）。 卡巴斯基安全管理中心決定當產品授權限制被超過時產生事件的規則。	180 天
病毒爆發	26（對於檔案威脅防護）	GNRL_EV_VIRUS_OUTBREAK	當短時間內在若干受管理裝置上偵測到的惡意物件數量超過上限值時，該類型的事件發生。 您可以透過以下方式回應事件： • 您可以在管理伺服器內容中配置上限值。 • 您也可以建立嚴格政策以便被啟動，或者建立工作以便在事件發生時執行。	180 天
病毒爆發	27（對於郵件威脅防護）	GNRL_EV_VIRUS_OUTBREAK	當短時間內在若干受管理裝置上偵測到的惡意物件數量超過上限值時，該類型的事件發生。 您可以透過以下方式回應事件： • 您可以在管理伺服器內容中配置上限值。 • 您也可以建立嚴格政策以便被啟動，或者建立工作以便在事件發生時執行。	180 天
病毒爆發	28（對於防火牆）	GNRL_EV_VIRUS_OUTBREAK	當短時間內在若干受管理裝置上偵測到的惡意物件數量超過上限值時，該類型的事件發生。 您可以透過以下方式回應事件： • 您可以在管理伺服器內容中配置上限值。 • 您也可以建立嚴格政策以便被啟動，或者建立工作以便在事件發生時執行。	180 天
裝置已失去管理	4111	KLSRV_HOST_OUT_CONTROL	如果受管理裝置在網路中可見，但一定時間未連線到管理伺服器，則該類型的事件發生。 找到什麼封鎖了裝置上網路代理的正常功能。可能的原因包括網路問題和從裝置移除網路代理。	180 天
裝置狀態為"緊急"	4113	KLSRV_HOST_STATUS_CRITICAL	當受管理裝置被分配緊急狀態時，該類型的事件發生。您可設定裝置狀態要變更為緊急的條件。	180 天
金鑰檔案已新增到黑名單	4124	KLSRV_LICENSE_BLACKLISTED	當 Kaspersky 已新增您使用的啟動碼或金鑰檔案到拒絕清單時，會發生該類型的事件。 聯絡技術支援獲得更多詳情。	180 天
受限功能模式	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	當卡巴斯基安全管理中心開始用基本功能操作，沒有"弱點和修補程式管理"和"行動裝置管理"功能時，該類型的事件發生。 以下是事件發生的原因和正確回應： • 產品授權期限已到期。提供授權以使用卡巴斯基安全管理中心的完整功能模式（新增有效的啟動碼或金鑰檔案到管理伺服器）。 • 管理伺服器管理比產品授權限制更多的裝置。從管理伺服器的管理群組移動裝置到其他管理伺服器的管理群組（如果其他管理伺服器的產品授權限制允許）。	180 天

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
產品授權即將到期	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	當接近商業授權到期日時，就會發生此類事件。 卡巴斯基安全管理中心每天會檢查一次產品授權是否接近到期日。此類事件會在產品授權到期日期前 30 天、15 天、5 天和 1 天發布。您不能變更天數。如果管理伺服器在許可證到期日期前的指定日期關閉，則事件將在第二天發布。 當商業授權到期時，卡巴斯基安全管理中心僅提供基本功能。 您可以透過以下方式回應事件： • 請確保將備用產品授權金鑰新增到管理伺服器。 • 如果您使用訂購方案，請確保續訂該方案。無限制訂購如果已經預付給服務提供商了，則會在到期日自動續約。	180 天
憑證已到期	4132	KLSRV_CERTIFICATE_EXPIRED	當行動裝置上的用戶端憑證過期時，就會發生此類事件。	180 天
Kaspersky 軟體模組更新已撤銷	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	如果無縫更新被 Kaspersky 技術專家撤銷（這些更新顯示*已撤銷*狀態）；例如，它們必須被更新到新版本，則該類型的事件發生。該事件涉及卡巴斯基安全管理中心修補程式且不涉及 Kaspersky 受管理應用程式模組。事件提供無縫更新未被安裝的原因。	180 天

管理伺服器功能失效事件

下表顯示有**功能失效**重要等級的卡巴斯基安全管理中心管理伺服器事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。對於管理伺服器，您還可以在管理伺服器屬性中檢視和設定事件清單。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

管理伺服器功能失效事件

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
執行時錯誤	4125	KLSRV_RUNTIME_ERROR	由於未知問題，該類型的事件發生。 多數情況下，這些是 DBMS 問題、網路問題和其他軟體和硬體問題。 事件詳情可以在事件描述中找到。	180 天
其中一個已授權應用程式群組已超過最大安裝數量	4126	KLSRV_INVLICPROD_EXCEDED	管理伺服器定期產生該類型的事件（每小時）。如果在卡巴斯基安全管理中心中，您管理協力廠商應用程式的授權金鑰，以及如果安裝數量超過了協力廠商應用程式授權金鑰設定的限制，則會發生該類型的事件。 您可以透過以下方式回應事件： • 檢視受管理裝置清單。從未使用協力廠商應用程式的裝置上移除該應用程式。 • 為更多裝置使用協力廠商產品授權。 您可以使用已授權應用程式群組的功能管理協力廠商應用程式的產品授權金鑰。這是一組由滿足您所設標準的協力廠商應用程式組成的授權應用程式群組。	180 天
輪詢雲端區段失敗	4143	KLSRV_KLCLOUD_SCAN_ERROR	當管理伺服器無法在雲端環境中輪詢網路區段時，將發生此類事件。讀取事件敘述中的詳細資訊，並據此做出回應。	未儲存
將更新複製到指定資料夾失敗	4123	KLSRV_UPD_REPL_FAIL	當軟體更新被複製到附加分享資料夾時，該類型的事件發生。 您可以透過以下方式回應事件： • 檢查用於獲取資料夾存取的使用者帳戶是否具有寫權限。 • 檢查資料夾的使用者名稱和 / 或金鑰是否變更。 • 檢查網際網路連線，因為它可能是事件原因。遵照指示更新資料庫和軟體模組。	180 天

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
沒有剩餘硬碟空間	4107	KLSRV_DISK_FULL	當安裝管理伺服器的裝置磁碟空間不足時，就會發生此類事件。 釋出裝置上的磁碟空間。	180 天
共用資料夾無法使用	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	如果管理伺服器共用資料夾不可用，則該類型的事件發生。 您可以透過以下方式回應事件： • 檢查管理伺服器（共用資料夾所在位置）是否已開啟並可用。 • 檢查資料夾的使用者名稱和 / 或金鑰是否變更。 • 檢查網路連線。	180 天
管理伺服器資料庫無法使用	4109	KLSRV_DATABASE_UNAVAILABLE	如果管理伺服器資料庫不可用則該類型的事件發生。 您可以透過以下方式回應事件： • 檢查安裝了 SQL Server 的遠端伺服器是否可用。 • 檢視 DBMS 記錄以發現管理伺服器資料庫不可用的原因。例如，因為維護，安裝了 SQL Server 的遠端伺服器可能不可用。	180 天
管理伺服器資料庫空間不足	4110	KLSRV_DATABASE_FULL	當管理伺服器資料庫沒有剩餘空間時，該類型的事件發生。 當管理伺服器的資料庫達到其容量，以及當不可能再往資料庫記錄時，管理伺服器不工作。 以下是根據您使用的 DBMS，該事件的原因，以及到該事件的正確回應： • 您使用 SQL Server Express 版本 DBMS： 在 SQL Server Express 文件中，檢查您使用版本的資料庫大小限制。可能您的管理伺服器資料庫已超過了資料庫大小限制。 限制儲存在管理伺服器資料庫的事件數量。 在管理伺服器資料庫中有太多由應用程式控制元件傳送的事件。您可以變更關於管理伺服器資料庫中應用程式事件儲存的 Kaspersky Endpoint Security for Windows 政策設定。 • 您使用 DBMS 而不是 SQL Server Express Edition： 不限制儲存在管理伺服器資料庫的事件數量。 降低儲存在管理伺服器資料庫的事件數量。 在 DBMS 選項處檢視資訊。	180 天

管理伺服器警告事件

下表顯示具有**警告**重要等級的卡巴斯基安全管理中心管理伺服器事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。對於管理伺服器，您還可以在管理伺服器屬性中檢視和設定事件清單。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
已偵測到頻繁事件		KLSRV_EVENT_SPAM_EVENTS_DETECTED	當管理伺服器在受管理裝置上偵測到頻繁發生的事件時，就會發生這種類型的事件。有關詳細資訊，請參閱以下部分： 阻止頻繁事件。	90 天
已超過產品授權數量限制	4098	KLSRV_EV_LICENSE_CHECK_100_110	每天一次，卡巴斯基安全管理中心 Linux 檢查是否超過產品授權限制。 當管理伺服器發現安裝在用戶端裝置上的 Kaspersky 應用程式超過了產品授權限制，以及由單一產品授權覆寫的目前使用的產品授權單元數量達到了該產品授權覆寫的單元總數的 100% 到 110%，則該類型的事件發生。 即便當該事件發生時，用戶端裝置是被防護的。 您可以透過以下方式回應事件： • 檢視受管理裝置清單。刪除不在使用的裝置。 • 為更多裝置提供產品授權（新增有效的啟動碼或金鑰檔案至管理伺服器）。 卡巴斯基安全管理中心決定當產品授權限制被超過時產生事件的規則。	90 天
裝置在網路上已長時間沒有活動	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	當受管理裝置顯示閒置狀態時，有時會發生該類型的事件。 最常在停用受管理裝置時發生。 您可以透過以下方式回應事件： • 要從受管理裝置清單中手動刪除裝置。 • 指定系統使用管理主控台或使用卡巴斯基安全管理中心網頁主控台建立**裝置在網路上已長時間沒有活動**事件後的時間間隔。 • 指定使用管理主控台或卡巴斯基安全管理中心網頁主控台將裝置自動從群組中刪除的時間間隔。	90 天
裝置名稱衝突	4102	KLSRV_EVENT_HOSTS_CONFLICT	當管理伺服器將兩個或更多受管理裝置視為單一裝置時，會發生此類事件。 當複製的硬碟用在受管理裝置上進行軟體佈署，並且沒有將網路代理切換到參考裝置上的專用磁碟複製模式時，通常會發生這種情況。 為避免此問題，請在複製該裝置硬碟之前將網路代理切換到參考裝置上的磁碟複製模式。	90 天
裝置狀態為“警告”	4114	KLSRV_HOST_STATUS_WARNING	當受管理裝置被分配*警告*狀態時，該類型的事件發生。您可設定裝置狀態要變更為*警告*的條件。	90 天
其中一個已授權應用程式群組總數即將超過最大安裝數量	4127	KLSRV_INVLICPROD_FILLED	當已授權應用程式群組中包含的協力廠商應用程式的安裝數量達到產品授權金鑰屬性中指定之最大允許值的 90% 時，將發生此類事件。 您可以透過以下方式回應事件： • 如果某些受管理裝置上未使用協力廠商應用程式，請從這些裝置上刪除該應用程式。 • 如果您預計協力廠商應用程式的安裝數量將在不久的將來超過允許的最大值，請考慮預先獲取更多裝置的協力廠商授權。 您可以使用已授權應用程式群組的功能管理協力廠商應用程式的產品授權金鑰。	90 天
憑證已被請求	4133	KLSRV_CERTIFICATE_REQUESTED	當無法自動重新發佈行動裝置管理憑證時，將發生此類事件。 以下可能是事件的原因和適當的回應： • 對憑證啟動了自動重新簽發，但憑證的**如果可能，自動重新發佈憑證**選項已停用。這可能是由於建立憑證期間發生的錯誤。可能需要手動重新發佈憑證。 • 如果您使用與公開金鑰基礎架構的整合，則可能是由於缺少適用於與 PKI 整合和發佈憑證之帳戶的 SAM-Account-Name 屬性。檢視帳戶屬性。	90 天

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
憑證已刪除	4134	KLSRV_CERTIFICATE_REMOVED	當管理員為行動裝置管理移除任何類型的憑證（一般、郵件、VPN）時，會發生此類事件。 移除憑證後，透過此憑證連線的行動裝置將無法連線到管理伺服器。 在調查與行動裝置管理相關的故障時，此事件可能會有所幫助。	90 天
憑證將到期	6128	ServerCertificateExpiresSoon	當行動裝置和 UEFI 裝置的管理伺服器憑證過期時，會發生此類事件。 您需要更新過期的憑證 。	90 天
APNs 憑證已到期	4135	KLSRV_APN_CERTIFICATE_EXPIRED	當 APNs 憑證過期時，會發生此類事件。 您需要手動續訂 APNs 憑證並將其安裝在 iOS MDM 伺服器上。	未儲存
APNs 憑證即將到期	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	當 APNs 憑證剩餘時間不足 14 天時，就會發生此類事件。 當 APNs 憑證到期時，您需要手動續訂 APNs 憑證並將其安裝在 iOS MDM 伺服器上 。 建議您在到期日之前安排續訂 APNs 憑證。	未儲存
傳送 FCM 訊息到行動裝置失敗	4138	KLSRV_GCM_DEVICE_ERROR	當行動裝置管理被配置使用 Firebase Cloud Messaging (FCM) 連線到具有 Android 作業系統的受管理行動裝置並且 FCM 伺服器無法處理從管理伺服器收到的某些要求時，會發生此類事件。這意味著某些受管理行動裝置將不會收到推送通知。 讀取事件事件敘述詳細資訊中的 HTTP 程式碼，並據此做出回應。如需從 FCM 伺服器接收到的 HTTP 程式碼以及相關錯誤的詳細資訊，請參閱 Firebase 服務文件（請參閱「下游訊息錯誤回應程式碼」一章）。	90 天
傳送 FCM 訊息到 FCM 伺服器時發生 HTTP 錯誤	4139	KLSRV_GCM_HTTP_ERROR	當行動裝置管理被配置使用 Firebase Cloud Messaging (FCM) 連線到具有 Android 作業系統的受管理行動裝置並且 FCM 伺服器透過 200 (OK) 以外的 HTTP 程式碼還原管理伺服器的要求時，會發生此類事件。 以下可能是事件的原因和適當的回應： • FCM 伺服器端出現問題。讀取事件事件敘述詳細資訊中的 HTTP 程式碼，並據此做出回應。如需從 FCM 伺服器接收到的 HTTP 程式碼以及相關錯誤的詳細資訊，請參閱 Firebase 服務文件（請參閱「下游訊息錯誤回應程式碼」一章）。 • 代理伺服器端的問題（如果使用代理伺服器）。讀取事件事件敘述詳細資訊中的 HTTP 程式碼，並據此做出回應。	90 天
傳送 FCM 訊息到 FCM 伺服器失敗	4140	KLSRV_GCM_GENERAL_ERROR	使用 Firebase Cloud Messaging HTTP 通訊協定時，由於管理伺服器端發生意外錯誤，因此會發生此類事件。 讀取事件敘述中的詳細資訊，並據此做出回應。 如果您自己找不到問題的解決方案，建議您與卡巴斯基技術支援聯絡。	90 天
硬碟剩餘空間少	4105	KLSRV_NO_SPACE_ON_VOLUMES	當安裝管理伺服器的裝置硬碟空間不足時，就會發生此類事件。 釋出裝置上的磁碟空間。	90 天

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
管理伺服器資料庫的剩餘空間少	4106	KLSRV_NO_SPACE_IN_DATABASE	如果管理伺服器資料庫受限制則該類型的事件發生。如果您不糾正情況，管理伺服器資料庫就將達到其容量且管理伺服器將不工作。 以下是根據您使用的 DBMS，該事件的原因，以及到該事件的正確回應。 您使用 SQL Server Express 版本 DBMS： • 在 SQL Server Express 文件中，檢查您使用版本的資料庫大小限制。可能您的管理伺服器資料庫即將超過資料庫大小限制。 • 限制儲存在管理伺服器資料庫的事件數量。 • 在管理伺服器資料庫中有太多由應用程式控制元件傳送的事件。您可以變更關於管理伺服器資料庫中應用程式事件儲存的 Kaspersky Endpoint Security for Windows 政策設定。 您使用 DBMS 而不是 SQL Server Express Edition： • 不限制儲存在管理伺服器資料庫的事件數量 • 降低儲存在管理伺服器資料庫的事件數量 在 DBMS 選項處檢視資訊。	90 天
連到從屬管理伺服器的連線已中斷	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	當與次要管理伺服器的連線中斷時，會發生此類事件。 在安裝了次要管理伺服器的裝置上讀取卡巴斯基事件記錄，並據此做出回應。	90 天
連到主管理伺服器的連線已中斷	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	當與主要管理伺服器的連線中斷時，會發生此類事件。 在安裝了主要管理伺服器的裝置上讀取卡巴斯基事件記錄，並據此做出回應。	90 天
已註冊 Kaspersky 軟體模組的新更新	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	當管理伺服器為需要批准安裝的受管理裝置上安裝的 Kaspersky 軟體註冊新更新時，將發生此類事件。 使用管理主控台或卡巴斯基安全管理中心網頁主控台核准或拒絕更新。	90 天
超過資料庫中的事件數量限制，刪除事件開始	4145	KLSRV_EVP_DB_TRUNCATING	當從管理伺服器資料庫刪除舊事件在管理伺服器資料庫達到容量後開始時，該類型的事件發生。 您可以透過以下方式回應事件： • 變更儲存在管理伺服器資料庫的事件數量上限 • 降低儲存在管理伺服器資料庫的事件數量	未儲存
超過資料庫中的事件數量限制，事件已被刪除	4146	KLSRV_EVP_DB_TRUNCATED	當從管理伺服器資料庫刪除舊事件在管理伺服器資料庫達到容量後完成時，該類型的事件發生。 您可以透過以下方式回應事件： • 變更允許儲存在管理伺服器資料庫的事件數量上限 • 降低儲存在管理伺服器資料庫的事件數量	未儲存
自動簽發憑證失敗		KLSRV_CERTIFICATE_AUTO_ISSUE_ERROR	如果為行動裝置（在行動協定下執行的裝置）建立用戶端憑證時發生錯誤，則會發生此事件。	90 天

管理伺服器資訊事件

下表顯示具有 **資訊**重要等級的卡巴斯基安全管理中心管理伺服器事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。對於管理伺服器，您還可以在管理伺服器屬性中檢視和設定事件清單。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

事件類型顯示名稱	事件類型 ID	事件類型	預設儲存期限	評論
產品授權金鑰的 90% 已經使用	4097	KLSRV_EV_LICENSE_CHECK_90	30 天	
已偵測到新裝置	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 天	
裝置已被自動新增到群組	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 天	
裝置已從群組中刪除：長時間在網路中不活動	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 天	
已授權應用程式群組之一的安裝即將超過限制（已經使用 95% 以上）	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 天	
找到了要傳送至 Kaspersky 以分析的檔案	4131	KLSRV_APS_FILE_APPEARED	30 天	
此行動裝置上的 FCM 實例 ID 已被變更	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 天	
更新被成功複製至指定的資料夾	4122	KLSRV_UPD_REPL_OK	30 天	
連到從屬管理伺服器的連線已建立	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 天	
連到主管理伺服器的連線已建立	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 天	
資料庫已更新	4144	KLSRV_UPD_BASES_UPDATED	30 天	
稽核：到管理伺服器的連線已建立	4147	KLAUD_EV_SERVERCONNECT	30 天	當使用者使用管理主控台或卡巴斯基安全管理中心網頁主控台連線到管理伺服器時，會發生此類事件。這些事件包括安裝了 MMC 型管理主控台或卡巴斯基安全管理中心網頁主控台伺服器的裝置的 IP 位址的資訊。
稽核：物件已修改	4148	KLAUD_EV_OBJECTMODIFY	30 天	此事件追蹤以下物件的變更： • 管理群組 • 安全群組 • 使用者 • 套件 • 工作 • 政策 • 伺服器 • 虛擬伺服器
稽核：物件狀態已修改	4150	KLAUD_EV_TASK_STATE_CHANGED	30 天	例如，當工作因錯誤而失敗時會發生此事件。
稽核：群組設定已修改	4149	KLAUD_EV_ADMGROUP_CHANGED	30 天	
稽核: 連到管理伺服器的連線已終止	4151	KLAUD_EV_SERVERDISCONNECT	30 天	

事件類型顯示名稱	事件類型 ID	事件類型	預設儲存期限	評論
稽核：物件內容已修改	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 天	此事件追蹤以下屬性的變更： • 使用者 • 產品授權 • 伺服器 • 虛擬伺服器
稽核：使用者權限已修改	4153	KLAUD_EV_OBJECTACLMODIFIED	30 天	
稽核：加密金鑰已從管理伺服器匯入或者匯出	5100	KLAUD_EV_DPEKEYSEXPORT	30 天	

網路代理事件

該部分包含網路代理相關事件資訊。

網路代理功能失效事件

下表顯示具有**功能失效**嚴重等級的卡巴斯基安全管理中心網路代理事件類型。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

網路代理功能失效事件

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
更新安裝錯誤	7702	KLNAG_EV_PATCH_INSTALL_ERROR	如果卡巴斯基安全管理中心元件自動更新和修補程式未成功，則該類型的事件發生。事件不包含受管理的 Kaspersky 應用程式的更新。 閱讀事件描述。管理伺服器上的 Windows 問題可能是該事件的原因。如果描述提到 Windows 配置的任何問題，解決該問題。	30 天
安裝協力廠商軟體更新失敗	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	如果"弱點和修補程式管理"和"行動裝置管理"功能正在使用且協力廠商軟體更新未成功，則該類型的事件發生。 檢查到協力廠商軟體的連結是否合法。閱讀事件描述。	30 天
安裝 Windows Update 更新失敗	7717	KLNAG_EV_WUA_INSTALL_ERROR	如果 Windows 更新未成功，則該類型的事件發生。在網路代理政策中配置 Windows 更新。 閱讀事件描述。在 Microsoft 知識庫中尋找錯誤。如果您無法自己解決問題，請聯絡 Microsoft 技術支援。	30 天

網路代理警告事件

下表顯示具有**警告**嚴重等級的卡巴斯基安全管理中心網路代理事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

網路代理警告事件

事件類型顯示名稱	事件類型 ID	事件類型	預設儲存期限
在安裝軟體模組更新期間返回了警告	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 天
協力廠商軟體更新安裝已完成但存在警告	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 天

事件類型顯示名稱	事件類型 ID	事件類型	預設儲存期限
協力廠商軟體更新已延時	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 天
發生了事件	549	GNRL_EV_APP_INCIDENT_OCCURED	30 天
KSN 代理已啟動。檢查 KSN 可用性失敗	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 天

網路代理資訊事件

下表顯示具有**資訊**嚴重等級的卡巴斯基安全管理中心網路代理事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

網路代理資訊事件

事件類型顯示名稱	事件類型 ID	事件類型	預設儲存期限
軟體模組更新已成功安裝	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 天
軟體模組更新安裝已啟動	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 天
應用程式已安裝	7703	KLNAG_EV_INV_APP_INSTALLED	30 天
應用程式已解除安裝	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 天
已安裝監控的應用程式	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 天
已解除安裝監控的應用程式	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 天
已安裝協力廠商應用程式	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 天
已新增裝置	7708	KLNAG_EV_DEVICE_ARRIVAL	30 天
裝置已被刪除	7709	KLNAG_EV_DEVICE_REMOVE	30 天
已偵測到新裝置	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 天
裝置已被授權	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 天
Windows 共用桌面：檔案已讀取	7712	KLUSRLOG_EV_FILE_READ	30 天
Windows 共用桌面：檔案已修改	7713	KLUSRLOG_EV_FILE_MODIFIED	30 天
Windows 共用桌面：應用程式已啟動	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 天
Windows 共用桌面：已啟動	7715	KLUSRLOG_EV_WDS_BEGIN	30 天
Windows 共用桌面：已停止	7716	KLUSRLOG_EV_WDS_END	30 天
協力廠商軟體更新已成功安裝	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 天
協力廠商軟體更新安裝已開始	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 天
KSN 代理已啟動。KSN 可用性檢查已成功完成	7719	KSNPROXY_STARTED_CON_CHK_OK	30 天
KSN 代理已停止	7720	KSNPROXY_STOPPED	30 天

iOS MDM 伺服器事件

該部分包含 iOS MDM 伺服器相關事件資訊。

iOS MDM 伺服器功能失效事件

下表顯示有**功能失效**嚴重等級的卡巴斯基安全管理中心 iOS MDM 伺服器事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

iOS MDM 伺服器功能失效事件

事件類型顯示名稱	事件類型	預設儲存期限
請求設定檔清單失敗	設定檔清單_指令_失敗	30 天
安裝設定檔失敗	安裝設定檔_指令_失敗	30 天
刪除設定檔失敗	刪除設定檔_指令_失敗	30 天
請求 provisioning 設定檔清單失敗	PROVISIONING 設定檔清單_指令_失敗	30 天
安裝 provisioning 設定檔失敗	安裝 PROVISIONING 設定檔_指令_失敗	30 天
刪除 provisioning 設定檔失敗	刪除 PROVISIONING 設定檔_指令_失敗	30 天
請求數位憑證清單失敗	憑證清單_指令_失敗	30 天
請求已安裝應用程式清單失敗	已安裝應用程式清單_指令_失敗	30 天
請求行動裝置一般資訊失敗	裝置資訊_指令_失敗	30 天
請求安全資訊失敗	安全資訊_指令_失敗	30 天
鎖定行動裝置失敗	裝置鎖_指令_失敗	30 天
重設密碼失敗	清除密碼_指令_失敗	30 天
從行動裝置抹除資料失敗	抹除裝置_指令_失敗	30 天
安裝應用失敗	安裝應用程式_指令_失敗	30 天
為應用設定兌換碼失敗	應用兌換碼_指令_失敗	30 天
請求受管理應用清單失敗	受管理應用程式清單_指令_失敗	30 天
刪除受管理應用失敗	移除應用程式_指令_失敗	30 天
漫遊設定已被拒絕	設定漫遊設定_指令_失敗	30 天
應用操作中發生錯誤	產品_失敗	30 天
指令結果包含無效資料	畸形_指令	30 天
傳送推送通知失敗	傳送_推送_通知_失敗	30 天
傳送指令失敗	傳送_指令_失敗	30 天
未找到裝置	裝置_未_發現	30 天

iOS MDM 伺服器警告事件

下表顯示有**警告**嚴重等級的卡巴斯基安全管理中心 iOS MDM 伺服器事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

iOS MDM 伺服器警告事件

事件類型顯示名稱	事件類型	預設儲存期限
偵測到連線鎖定行動裝置的企圖	不活動_裝置_嘗試_已連線	30 天
設定檔已被刪除	MDM_設定檔_已_被刪除	30 天
偵測到重新使用用戶端憑證的企圖	用戶端_憑證_已_在_使用	30 天
偵測到不活動裝置	發現_不活動_裝置	30 天
兌換碼已請求	需要_兌換_碼	30 天
設定檔已被包含到從裝置刪除的政策	UMDM_設定檔_已_被刪除	30 天

iOS MDM 伺服器資訊事件

下表顯示有**資訊**嚴重等級的卡巴斯基安全管理中心 iOS MDM 伺服器事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

iOS MDM 伺服器資訊事件

事件類型顯示名稱	事件類型	預設儲存期限
新行動裝置已被連線	新_裝置_已連線	30 天
設定檔清單已被成功請求	設定檔清單_指令_成功	30 天
設定檔已被成功安裝	安裝設定檔_指令_成功	30 天
設定檔已被成功刪除	刪除設定檔_指令_成功	30 天
Provisioning 設定檔清單已被成功請求	PROVISIONING 設定檔清單_指令_成功	30 天
Provisioning 設定檔已被成功安裝	安裝 PROVISIONING 設定檔_指令_成功	30 天
Provisioning 設定檔已被成功刪除	刪除 PROVISIONING 設定檔_指令_成功	30 天
數位憑證清單已被成功請求	憑證清單_指令_成功	30 天
已安裝應用程式清單已被成功請求	已安裝應用程式清單_指令_成功	30 天
行動裝置一般資訊已被成功請求	裝置資訊_指令_成功	30 天
安全資訊已被成功請求	安全資訊_指令_成功	30 天
行動裝置已被成功鎖定	裝置鎖_指令_成功	30 天
密碼已被成功重設	清除密碼_指令_成功	30 天
資料已被從行動裝置成功抹除	抹除裝置_指令_成功	30 天
應用已被成功安裝	安裝應用程式_指令_成功	30 天
兌換碼已為應用成功設定	應用兌換碼_指令_成功	30 天
受管理應用清單已被成功請求	受管理應用程式清單_指令_成功	30 天
受管理應用已被成功刪除	刪除應用程式_指令_成功	30 天
漫遊設定已被成功應用	設定漫遊設定_指令_成功	30 天

Exchange 行動裝置伺服器事件

該部分包含 Exchange 行動裝置伺服器相關事件資訊。

Exchange 行動裝置伺服器功能失效事件

下表顯示具有**功能失效**嚴重等級的卡巴斯基安全管理中心 Exchange 行動裝置伺服器事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

Exchange 行動裝置伺服器功能失效事件

事件類型顯示名稱	事件類型	預設儲存期限
從行動裝置抹除資料失敗	抹除_失敗	30 天
無法刪除行動裝置連線到郵箱的資訊	裝置_刪除_失敗	30 天
應用 ActiveSync 政策到郵箱失敗	政策_套用_失敗	30 天
應用程式操作錯誤	產品_失敗	30 天
修改 ActiveSync 功能狀態失敗	變更_活動_同步_狀態_失敗	30 天

Exchange 行動裝置伺服器資訊事件

下表顯示具有**資訊**嚴重等級的卡巴斯基安全管理中心 Exchange 行動裝置伺服器事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

事件類型顯示名稱	事件類型	預設儲存期限
已連線新行動裝置	新_裝置_已連線	30 天
資料已被從行動裝置成功抹除	抹除_成功	30 天

封鎖頻發事件

本節提供有關管理頻繁事件封鎖和移除對頻繁事件封鎖的資訊。

關於封鎖頻發事件

安裝在單個或多個受管理裝置上的受管理應用程式（例如，Kaspersky Endpoint Security for Windows）可以將許多相同類型的事件傳送到管理伺服器。接收頻繁的事件可能會使管理伺服器資料庫超載並覆寫其他事件。當所有接收到的事件數超過資料庫的指定限制時，管理伺服器將開始封鎖最頻繁的事件。

管理伺服器會封鎖自動接收頻發事件。您不能自己封鎖頻發事件，也不能選擇要封鎖的事件。

如果您想了解某個事件是否被封鎖，您可檢視通知清單或檢視該事件是否存在於**封鎖頻繁事件**的管理伺服器屬性區段。在封鎖的事件中，您可以進行以下操作：

- 如果要封鎖覆寫資料庫，則可以繼續封鎖接收此類事件。
- 例如，如果要查找將頻發事件傳送到管理伺服器的原因，則可以取消封鎖頻發事件並繼續接收此類事件。
- 如果要繼續接收頻發事件直到再次被封鎖，可以從封鎖頻發事件中刪除。

管理頻發事件封鎖

管理伺服器封鎖自動接收頻繁事件，但是您可以取消封鎖並繼續接收頻繁事件。您還可以封鎖接收以前取消封鎖的頻繁事件。

若要管理頻發的事件封鎖：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**封鎖頻繁事件**區段。
3. 在**封鎖頻繁事件**區段中：
   - 如果要取消封鎖接收頻繁事件，請執行以下操作：
     a. 選取您要封鎖的頻繁事件並點擊**排除**按鈕。
     b. 點擊**儲存**按鈕。
   - 如果要封鎖接收頻繁事件：
     a. 選取您要封鎖的頻繁事件並點擊**封鎖**按鈕。
     b. 點擊**儲存**按鈕。

管理伺服器會接收取消封鎖的頻繁事件，並且不會接收已封鎖的頻繁事件。

移除對頻發事件的封鎖

您可以刪除對頻繁事件的封鎖並開始接收它們，直到管理伺服器再次封鎖這些頻繁事件為止。

要移除對頻繁事件的封鎖：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**封鎖頻繁事件**區段。
3. 在**封鎖頻繁事件**區段，選擇要為其移除封鎖的頻繁事件類型。
4. 點擊**移除封鎖** 按鈕。

頻繁事件將從頻繁事件清單中移除。管理伺服器將接收此類型的事件。

從 Kaspersky Security for Microsoft Exchange Server 接收事件

有關受管理應用程式（例如 Kaspersky Endpoint Security for Windows）執行期間事件的資訊被從受管理裝置傳輸並註冊在管理伺服器資料庫中。預設情況下，來自 Kaspersky Security for Microsoft Exchange Servers 版本 9.0 MR6 和更早版本的事件未在管理伺服器資料庫中註冊。如果 Kaspersky Security for Microsoft Exchange Servers 9.0 MR6 和更早版本安裝在您組織的受管理裝置上，並且您希望接收來自此應用程式的事件，請使用 klscflag 公用程式啟用此應用程式的事件註冊。

要為 Kaspersky Security for Microsoft Exchange Servers 啟用事件註冊：

1. 在管理伺服器裝置上，在具有管理員權限的帳戶下執行 Windows 命令提示符。
2. 將當前目錄變更為卡巴斯基安全管理中心安裝資料夾（通常為 C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center）。
3. 執行以下其中一個指令：

   - 管理伺服器安裝在 Windows Server 容錯移轉叢集上：

     ```
     klscflag.exe --stp cluster -fset -pv klserver -n
     KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
     ```

   - 管理伺服器安裝在 Kaspersky Security Center 容錯移轉叢集節點上：

     ```
     klscflag.exe --stp klfoc -fset -pv klserver -n
     KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
     ```

   - 管理伺服器未在叢集上執行：

     ```
     klscflag.exe -fset -pv klserver -n KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d
     -v 0
     ```

為 Kaspersky Security for Microsoft Exchange Servers 進行事件註冊已啟用。

對於 Kaspersky Security for Microsoft Exchange Server，您無法設定事件的儲存期限或選擇哪些事件必須儲存在管理伺服器儲存庫中。您可以設定可以儲存在儲存庫中的最大事件數量。此設定適用於從所有卡巴斯基應用程式接收到的事件。

通知和裝置狀態

本節包含有關如何檢視通知、配置通知傳遞、使用裝置狀態和啟用變更裝置狀態的資訊。

使用通知

通知會警示您關於事件的資訊，並協助您透過執行建議動作或您認為適當的動作加速回應這些事件。

根據選取的通知方法，有以下類型的通知可用：

- 螢幕通知
- 透過簡訊通知
- 透過電子郵件通知
- 透過可執行檔或指令碼通知

螢幕通知

螢幕通知提醒您按照重要等級分組的事件（*緊急*、*警告*和*資訊*）。

螢幕通知可以有兩種狀態之一：

- *已檢視*。您已對通知執行建議操作，或您已手動為通知分配該狀態。
- *未檢視*。您未對通知執行建議操作，或您未手動為通知分配該狀態。

預設下，通知清單包含*未檢視*狀態的通知。

您可以透過檢視螢幕通知和即時回應它們來監控您的組織網路。

透過電子郵件、SMS 和可執行檔或指令碼通知

卡巴斯基安全管理中心提供透過傳送您認為重要的事件的通知來監控您的組織網路。對任意事件，您可以配置透過電子郵件、SMS 或執行可執行檔或指令碼進行通知。

在透過電子郵件或 SMS 接收通知時，您可以決定您對事件的回應。該回應應該是最適合您組織網路的。透過執行可執行檔或指令碼，您預定義對事件的回應。您也可以認為執行可執行檔或指令碼是對事件的首選回應。可執行檔執行後，您可以採取其他步驟回應事件。

檢視螢幕通知

您可以透過三種方式在螢幕上檢視通知：

- 在**監控和報告** 中 → **通知**區段。這裡，您可以檢視預定義類別的通知。
- 您可以開啟單獨的視窗。此種情況下，您可以標記通知為已檢視。
- 在 **監控和報告** 上的**所選嚴重等級的通知**小工具中 → **控制板**區段。在部件中，您可以僅檢視處在*嚴重*和*警告*重要性等級的事件通知。

您可以執行操作，例如，您可以回應事件。

要檢視預定義類別的通知：

1. 在主功能表中，轉至 **監控和報告 → 通知**。

   在左窗格中選取**所有通知**類別，右窗格會顯示所有通知。

2. 在左側面板，選取類別之一：

   - **佈署**
   - **裝置**
   - **防護**
   - **更新**(這包含可以下載的 Kaspersky 應用程式通知和已下載的病毒資料庫更新通知)
   - **弱點利用防禦**
   - **管理伺服器**(這僅包含管理伺服器相關事件)
   - **有用連結** (這包含到 Kaspersky 資源的連結，例如 Kaspersky 技術支援、Kaspersky 論壇、產品授權續約頁面或 Kaspersky IT 百科全書)
   - **Kaspersky 新聞** (這包含 Kaspersky 應用程式發佈資訊)

   所選類別的通知清單被顯示。清單包含以下：

- 與通知主題相關的圖示：佈署（ ）、防護（ ）、更新（ ）、裝置管理（ ）、弱點利用防禦（ ）、管理伺服器（ ）。
- 通知重要性等級。以下重要等級通知會顯示：**緊急通知** ( )，**警告通知** ( )，**資訊通知**。清單中的通知按重要性等級分組。
- **通知**。這包含通知敘述。
- **操作**。這包含建議您執行的快速操作連結。例如，透過按一下該連結，您可以轉到儲存區並安裝安全應用程式到裝置，或檢視裝置清單或事件清單。您為通知執行建議操作之後，該通知被分配*已檢視*狀態。
- **註冊的狀態**。這包含從通知被註冊到管理伺服器到現在為止過去的天數或小時數。

要按照重要性等級在單獨的視窗中檢視螢幕通知：

1. 在卡巴斯基安全管理中心網頁主控台的右上角，按一下旗幟圖示（ ）。

   如果旗幟圖示具有紅點，表示有未檢視的通知。

   列出通知的視窗被開啟。依預設會選取**所有通知**頁籤，通知會根據重要等級分組：*Critical*、*Warning*和*Info*。

2. 選取 **系統**標籤。

   嚴重（ ）和*警告*（ ）重要性等級通知清單被顯示。通知清單包含以下：

   - 顏色標記。嚴重通知標記為紅色。警告通知標記為黃色。
   - 指出通知主題的圖示：佈署（ ）、防護（ ）、更新（ ）、裝置管理（ ）、弱點利用防禦（ ）、管理伺服器（ ）。
   - 通知敘述。
   - 旗幟圖示。旗幟圖示是灰色的，如果通知被分配了*未檢視*狀態。當您選取灰色旗幟圖示並分配*已檢視*狀態到通知時，圖示變更顏色到白色。
   - 建議操作的連結。您對通知執行建議操作之後，該通知會變成*已檢視*狀態。
   - 從通知被註冊到管理伺服器到現在為止過去的天數。

3. 選取 **更多**標籤。

   *資訊*重要性等級通知清單被顯示。

   清單的組織會與**系統**頁籤上的清單相同（請參閱以上說明）。僅有的不同是沒有顏色標記。

您可以透過註冊在管理伺服器上的日期間隔來過濾通知。使用**顯示篩選器**核取方塊來管理篩選條件。

要在部件上檢視螢幕通知：

1. 在**控制板**區段上，選取**新增或還原 Web 小部件**。

2. 在開啟的視窗中，點擊**其他**類別，選取**所選嚴重等級的通知**小工具，接著點擊新增。

   小工具現在會顯示在**控制板**頁籤上。預設下，*嚴重*重要性等級的通知顯示在部件。

   您可以按一下部件上的**設定**按鈕並變更部件設定以檢視*警告*重要性等級的通知。或者，您可以新增其他部件：**所選嚴重等級的通知**，帶有*警告*重要性等級。

   部件上的通知清單由尺寸限制並包含兩個通知。這兩個通知是關於最近事件的。

部件上的通知清單包含以下：

- 與通知主題相關的圖示：佈署（ ）、防護（ ）、更新（ ）、裝置管理（ ）、弱點利用防禦（ ）、管理伺服器（ ）。
- 通知敘述和建議操作的連結。您對通知執行建議操作之後，該通知會變成*已檢視*狀態。
- 從通知被註冊到管理伺服器到現在為止過去的天數或小時數。
- 到其他通知的連結。點擊此連結後，系統會將您轉移至**監控和報告**區段中**通知**區段的通知檢視畫面。

關於裝置狀態

卡巴斯基安全管理中心會為每部受管理裝置指派狀態。特定狀態會根據是否符合使用者定義的條件而指派。在有些情況下，指派狀態給裝置時，卡巴斯基安全管理中心會考量裝置在網路中的能見度標記（請參閱下表）。若卡巴斯基安全管理中心在兩小時內未在網路中找到裝置，裝置的能見度標記會設為*不可見*。

這些狀態如下：

- *緊急*或*緊急/可見*
- *警告*或*警告/可見*
- *正常*或*正常/可見*

下表列出在指派給裝置的*緊急*或*警告*狀態時必須符合的預設條件，其中包含所有可能的值。

分配狀態到裝置的條件

條件	條件敘述	可用值
安全應用程式未安裝	網路代理已安裝到裝置，但是安全應用程式未安裝。	• 開關按鈕被開啟。 • 開關按鈕被關閉。
偵測到太多病毒	一些病毒被病毒偵測工作在裝置上發現，例如，*惡意軟體掃描*工作，且發現的病毒數量超過指定值。	大於 0。
即時防護不符合管理員的設定等級	裝置在網路中可見，但即時防護等級與管理員在裝置狀態條件中設定的等級不同。	• 已停止。 • 已暫停。 • 執行中。
惡意軟體掃描已長時間未執行	裝置在網路中可見且安全應用程式已安裝到裝置，但*惡意軟體掃描*工作在指定時間內未執行。條件僅套用到於 7 天之前或更早新增到管理伺服器資料庫的裝置。	多於 1 天。
資料庫已過期	裝置在網路中可見且安全應用程式已安裝到裝置，但病毒資料庫在指定時間內未在該裝置上更新。條件僅套用到於 1 天之前或更早新增到管理伺服器資料庫的裝置。	多於 1 天。
長時間未連線	網路代理已安裝到裝置，但由於裝置關閉，裝置在指定時間段內未連線到管理伺服器。	多於 1 天。
偵測到活動威脅	**活動威脅**資料夾中的未處理的物件的數量超過指定的值。	多於 0 個項目。
需要重新啟動	裝置在網路中可見，但應用程式基於所選原因之一在指定時間之前請求裝置重新啟動。	多於 0 分鐘。
安裝了不相容的應用程式	裝置在網路中可見，但透過網路代理執行的軟體清查在裝置上偵測到了不相容的應用程式。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
偵測到軟體弱點	裝置在網路中可見且網路代理已安裝到裝置，但*弱點掃描和所需更新*工作在裝置應用程式中偵測到指定嚴重等級的弱點。	• 緊急。 • 高。 • 中等。 • 如果弱點無法被修補則略過。 • 如果為安裝分配了更新則略過。
產品授權已到期	裝置在網路中可見，但產品授權已過期。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
產品授權即將到期	裝置在網路中可見，但裝置上的產品授權即將在指定天數內過期。	少於 0 天。

條件	條件敘述	可用值
Windows Update 更新檢查已長時間未執行	裝置在網路中可見，但「*執行 Windows 更新同步*」工作在指定時間段內未執行。	多於 1 天。
無效的加密狀態	網路代理已安裝到裝置，但裝置加密結果等於指定值。	• 由於使用者拒絕未遵從政策（僅對外部裝置）。 • 由於錯誤未遵從政策。 • 套用政策時需要重新啟動。 • 未指定加密政策。 • 不支援。 • 當套用政策時。
行動裝置設定與政策不同	行動裝置設定不同於 Kaspersky Endpoint Security for Android 政策中指定的設定。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
偵測到未處理的事件	裝置上發現了一些未處理的事故。事件可以透過安裝在用戶端裝置上的受管理卡巴斯基應用程式自動建立，也可以由管理員手動建立。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
應用程式定義的裝置狀態	裝置狀態由受管理應用程式定義。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
裝置磁碟空間不足	裝置剩餘磁碟空間少於指定值或裝置無法與管理伺服器同步。當裝置已與管理伺服器成功同步且裝置上的剩餘空間大於或等於指定值時，*緊急*或*警告*狀態被變更為*正常*狀態。	大於 0 MB。
裝置已失去管理	在裝置發現過程中，裝置在網路中可見，但是超過三次嘗試與管理伺服器同步都失敗了。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
防護已停用	裝置在網路中可見，但裝置上的安全應用程式已被停用大於指定的時間段。 在這種情況下，安全應用程式的狀態為*stopped*或*failure*，不同於下列狀態：*starting*、*running*或*suspended*。	多於 0 分鐘。
安全應用程式沒有執行	裝置在網路中可見且安全應用程式已安裝到裝置，但其未在執行。	• 開關按鈕被關閉。 • 開關按鈕被開啟。

卡巴斯基安全管理中心允許您設定管理群組中裝置狀態在指定條件滿足時的自動轉換。當指定條件滿足時，用戶端裝置被分配以下狀態之一：*緊急*或*警告*。未滿足特定條件時，系統會為用戶端裝置指派*正常*狀態。

一個條件的不同值可對應於不同的狀態。例如，依預設，若**資料庫已過期**條件有**多於 3 天**的值，則用戶端裝置會被指派*警告*狀態，逖值為**多於 7 天**，則會指派*緊急*狀態。

如果您從以前的版本升級卡巴斯基安全管理中心，指定*緊急*或*警告*狀態的 **資料庫已過期** 條件的值不會改變。

當卡巴斯基安全管理中心指派狀態給裝置時，對於有些條件（請參閱條件說明欄），系統會將能見度標記列入考量。例如，若受管理裝置因符合資料庫已過期條件而被指派*緊急*狀態，之後能見度標記也已針對該裝置設定，則裝置會被指派*正常*狀態。

設定裝置狀態轉換

您可變更條件以為裝置配置*緊急*或*警告*狀態。

要啟用變更裝置狀態到緊急：

1. 在主功能表中，轉至 **裝置 → 群組的階層**。
2. 在開啟的群組清單中，針對您要變更切換裝置狀態的群組，點擊有該群組名稱的連結。
3. 在開啟的工作內容視窗中，選取**裝置狀態**頁籤。
4. 在左方窗格中，選取**緊急**。
5. 在右方窗格中的**若指定以下條件，則設為"緊急"**區段，啟用將裝置切換為*緊急*狀態的條件。

   然而，您可以變更在父政策中未鎖定的設定。

6. 在清單中選取條件旁的選項按鈕。
7. 在清單左上角，點擊**編輯**按鈕。
8. 為所選條件設定所需的值。
   可以不為每個條件設定值。
9. 點擊**確定**。

未滿足特定條件時，系統會為受管理裝置配置*緊急*狀態。

要啟用變更裝置狀態到警告：

1. 在主功能表中，轉至 **裝置 → 群組的階層**。
2. 在開啟的群組清單中，針對您要變更切換裝置狀態的群組，點擊有該群組名稱的連結。
3. 在開啟的工作內容視窗中，選取**裝置狀態**頁籤。
4. 在左方窗格中，選取**警告**。
5. 在右方窗格中的**若指定以下條件，則設為"警告"**區段，啟用將裝置切換為*警告*狀態的條件。

   然而，您可以變更在父政策中未鎖定的設定。

6. 在清單中選取條件旁的選項按鈕。
7. 在清單左上角，點擊**編輯**按鈕。
8. 為所選條件設定所需的值。
   可以不為每個條件設定值。
9. 點擊**確定**。

未滿足特定條件時，系統會為受管理裝置配置*警告*狀態。

配置通知傳送

您可以配置發生在卡巴斯基安全管理中心中的事件的通知。根據選取的通知方法，有以下類型的通知可用：

- 電子郵件—當發生事件時，卡巴斯基安全管理中心向指定的電子郵件信箱傳送通知。
- SMS—當發生事件時，卡巴斯基安全管理中心向指定的電話號碼傳送通知。
- 可執行檔—當事件發生時，可執行檔被執行在管理伺服器。

要配置發生在卡巴斯基安全管理中心中的事件的通知傳送：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗會開啟，並含有所選的**一般**頁籤。

2. 點擊**通知**區段，並在右窗格選取您需要之通知方法的頁籤：

   - **電子郵件**

電子郵件標籤允許您透過電子郵件配置事件通知。

在**收件者（電子郵件信箱）**欄位，指定應用程式傳送通知的電子郵件信箱。您可以在該欄位指定多個位址，以分號分隔。

在 **SMTP 伺服器**欄位，指定郵件伺服器位址，以分號分隔。您可以使用以下參數：

- IPv4 或 IPv6 位址
- 裝置的 Windows 網路名稱（NetBIOS 名稱）
- SMTP 伺服器的 DNS 名稱

在 **SMTP 伺服器連接埠**欄位，指定 SMTP 伺服器通訊埠號。預設埠號為 25。

如果您啟用**使用 DNS MX 尋找**選項，您可以將 IP 位址的多個 MX 記錄用於 SMTP 伺服器的相同 DNS 名稱。相同 DNS 名稱可能有幾個 MX 記錄，具有不同的接收電子郵件的優先次序。管理伺服器嘗試按 MX 記錄優先次序向 SMTP 伺服器傳送電子郵件通知。

如果您啟用**使用 DNS MX 尋找**選項並且不啟用 TLS 設定的使用，我們建議您使用伺服器裝置上的 DNSSEC 設定作為傳送電子郵件通知的額外防護措施。

如果啟用 **使用 ESMTP 身分驗證** 選項，則可以在 **使用者名稱** 和 **密碼** 欄位中指定 ESMTP 身分驗證設定。預設情況下，該選項被停用，ESMTP 身分驗證設定不可用。

您可以用 SMTP 伺服器指定連線的 TLS 設定：

- **不使用 TLS**

如果您想停用電子郵件訊息加密，您可以選取此選項。

- **如果受 SMTP 伺服器支援則使用 TLS**

如果要使用 TLS 連線到 SMTP 伺服器，則可以選取此選項。如果 SMTP 伺服器不支援 TLS，管理伺服器將不使用 TLS 連線 SMTP 伺服器。

- **始終使用 TLS，檢查伺服器憑證是否有效**

如果要使用 TLS 身分驗證設定，則可以選取此選項。如果 SMTP 伺服器不支援 TLS，管理伺服器將無法連線 SMTP 伺服器。

我們建議您使用此選項以更好地防護與 SMTP 伺服器的連線。如果選取此選項，則可以為 TLS 連線設定身分驗證設定。

如果您選取**始終使用 TLS，檢查伺服器憑證是否有效**值，您可以指定用於驗證 SMTP 伺服器的憑證，並選取是要透過任何版本的 TLS，還是僅透過 TLS 1.2 或更高版本啟用通訊。此外，您可以指定在 SMTP 伺服器上進行用戶端身分驗證的憑證。

您可以透過點擊**指定憑證**連結指定 TLS 連線的憑證：

- 瀏覽 SMTP 伺服器憑證檔案：

您可以從受信任的憑證頒發機構接收帶有憑證清單的檔案，然後將該檔案上傳到管理伺服器。卡巴斯基安全管理中心會檢查 SMTP 伺服器的憑證是否也由受信任的憑證頒發機構簽署。如果未從受信任的憑證頒發機構收到 SMTP 伺服器的憑證，卡巴斯基安全管理中心將無法連線到 SMTP 伺服器。

- 瀏覽用戶端憑證檔案：

您可以使用從任何來源（例如，從任何受信任的憑證頒發機構）收到的憑證。您必須使用以下憑證類型之一指定憑證及其私密金鑰：

- X-509 憑證：

您必須指定一個帶有憑證的檔案和一個帶有私密金鑰的檔案。這兩個檔案互不相依，檔案的載入順序並不重要。當同時載入兩個檔案時，您必須指定用於解碼私密金鑰的密碼。如果未編碼私密金鑰未編碼，則密碼可以為空值。

- pkcs12 容器：

您必須上傳包含憑證及其私密金鑰的單一檔案。載入檔案後，您必須指定用於解碼私密金鑰的密碼。如果未編碼私密金鑰未編碼，則密碼可以為空值。

在**主旨**欄位，指定電子郵件主旨。您可以置此欄位為空。

在**主旨範本**下拉清單中，選取您主旨的範本。選取的範本判定的變數會自動放在**主旨**欄位。您可以選取幾個郵件範本構建郵件主旨。

在**寄件者電子郵件地址**欄位中，指定寄件者的電子郵件位址。如果您將該欄位置空，收件者信箱被使用。不建議使用虛假郵件信箱。

通知訊息欄位包含事件發生時應用程式傳送的事件資訊標準文字。該文字包含替代參數，例如事件名稱、裝置名稱和網域名稱。您可以透過新增其他帶有更新事件詳情的替代參數編輯訊息文字。

> 如果通知文字包含百分號 (%) 字元，您必須指定兩次以允許訊息傳送。範例，“CPU 負載是 100%”。

點擊**設定通知限制數**連結允許您指定應用程式在指定時間段可以傳送的最大通知數量。

點擊**傳送測試訊息**按鈕允許您檢查是否正確配置了通知：應用程式傳送測試通知到您指定的郵件信箱。

- SMS

SMS 頁籤可讓您設定將各種事件的 SMS 通知傳到手機。SMS 訊息透過郵件閘道傳送。

在 **SMTP 伺服器**欄位，指定郵件伺服器位址，以分號分隔。您可以使用以下參數：

- IPv4 或 IPv6 位址
- 裝置的 Windows 網路名稱（NetBIOS 名稱）
- SMTP 伺服器的 DNS 名稱

在 **SMTP 伺服器連接埠**欄位，指定 SMTP 伺服器通訊埠號。預設埠號為 25。

如果啟用**使用 ESMTP 身分驗證**選項，則可以在**使用者名稱**和 **密碼**欄位中指定 ESMTP 身分驗證設定。預設情況下，該選項被停用，ESMTP 身分驗證設定不可用。

您可以用 SMTP 伺服器指定連線的 TLS 設定：

- **不使用 TLS**

如果您想停用電子郵件訊息加密，您可以選取此選項。

- **如果受 SMTP 伺服器支援則使用 TLS**

如果要使用 TLS 連線到 SMTP 伺服器，則可以選取此選項。如果 SMTP 伺服器不支援 TLS，管理伺服器將不使用 TLS 連線 SMTP 伺服器。

- **始終使用 TLS，檢查伺服器憑證是否有效**

如果要使用 TLS 身分驗證設定，則可以選取此選項。如果 SMTP 伺服器不支援 TLS，管理伺服器將無法連線 SMTP 伺服器。

我們建議您使用此選項以更好地防護與 SMTP 伺服器的連線。如果選取此選項，則可以為 TLS 連線設定身分驗證設定。

如果您選取**始終使用 TLS，檢查伺服器憑證是否有效**值，您可以指定用於驗證 SMTP 伺服器的憑證，並選取是要透過任何版本的 TLS，還是僅透過 TLS 1.2 或更高版本啟用通訊。此外，您可以指定在 SMTP 伺服器上進行用戶端身分驗證的憑證。

您可以透過點擊**指定憑證**連結指定 SMTP 伺服器憑證檔案：

您可以從受信任的憑證頒發機構接收帶有憑證清單的檔案，然後將該檔案上傳到管理伺服器。卡巴斯基安全管理中心會檢查 SMTP 伺服器的憑證是否也由受信任的憑證頒發機構簽署。如果未從受信任的憑證頒發機構收到 SMTP 伺服器的憑證，卡巴斯基安全管理中心將無法連線到 SMTP 伺服器。

在**收件者（電子郵件信箱）**欄位，指定應用程式傳送通知的電子郵件信箱。您可以在該欄位指定多個位址，以分號分隔。通知將被傳送到指定郵件信箱關聯的電話號碼。

在**主旨**欄位，指定電子郵件主旨。

在**主旨範本**下拉清單中，選取您主旨的範本。以已選取範本為依據的變數會放在**主旨**欄位。您可以選取幾個郵件範本構建郵件主旨。

在**寄件者郵件信箱：如果未指定該設定，則將使用收件者信箱。 警告：我們不建議您使用虛構郵件信箱**欄位中，指定寄件者的電子郵件位址。如果您將該欄位置空，收件者信箱被使用。不建議使用虛假郵件信箱。

在**SMS 訊息接收者電話號碼**欄位中，指定短信通知接收人的手機號碼。

通知訊息欄位中會包含事件發生時應用程式傳送的事件資訊標準文字。該文字可以包含替代參數，例如事件名稱、裝置名稱和網域名稱。

如果通知文字包含百分號 (%) 字元，您必須指定兩次以允許訊息傳送。範例，“CPU 負載是 100%”。

點擊**設定通知限制數**連結指定應用程式在指定時段內可以傳送的最大通知數量。

點擊**傳送測試訊息**檢查是否正確配置了通知：應用程式傳送測試通知到您指定的收件者。

- **要執行的可執行檔**

  如果選取該通知方法，您可以在輸入欄位指定事件發生時要啟動的應用程式。

  在**當事件發生時要在管理伺服器上執行的可執行檔**欄位中，指定要執行的資料夾與檔案名稱。在指定檔案之前，準備檔案並指定預留位置，後者將定義要在通知訊息中傳送的事件詳情。您指定的資料夾和檔案必須位於管理伺服器上。

  點擊**設定通知限制數**連結允許您指定應用程式在指定時間段可以傳送的最大通知數量。

3. 在標籤上，定義通知設定。

4. 點擊**確定**按鈕以關閉管理伺服器內容視窗。

儲存的通知傳送設定被應用到在卡巴斯基安全管理中心中發生的所有事件。

您可在管理伺服器設定、政策設定或應用程式設定的**事件配置**區域覆寫特定事件的通知交付設定。

透過執行可執行檔顯示的事件通知

卡巴斯基安全管理中心可透過執行可執行檔將用戶端裝置上發生的事件通知管理員。可執行檔必須包含另外一個可執行檔，而後者具有要轉發給管理員的事件的佔位符（請參見下表）。

敘述事件的佔位符

佔位符	佔位符敘述
%SEVERITY%	事件嚴重等級。可能的值： • **資訊** • **警告** • **錯誤** • **緊急**
%COMPUTER%	發生事件的裝置的名稱。 裝置名稱的最大長度為 256 個字元。
%DOMAIN%	發生事件的裝置的網域名稱。
%EVENT%	事件類型的名稱。 事件類型名稱的最大長度為 50 個字元。
%DESCR%	事件敘述。 敘述的最大長度為 1000 個字元。
%RISE_TIME%	事件建立時間。
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	工作名稱。 工作名稱的最大長度為 100 個字元。
%KL_PRODUCT%	應用程式名稱。
%KL_VERSION%	應用程式版本號。
%KLCSAK_EVENT_SEVERITY_NUM%	事件嚴重性編號。可能的值： • 1—**資訊** • 2—**警告** • 3—**錯誤** • 4—**緊急**

佔位符	佔位符敘述
%HOST_IP%	發生事件的裝置的 IP 位址。
%HOST_CONN_IP%	發生事件的裝置的連線 IP。

例如：
事件通知由某個可執行檔（例如，script1.bat）發出，在該可執行檔中，將啟動具有 %COMPUTER% 佔位符的另一個可執行檔（例如，script2.bat）。當發生事件時，將在管理員的裝置上執行 script1.bat 檔案，而該檔案隨後執行具有 %COMPUTER% 佔位符的 script2.bat 檔案。管理員將接收到發生事件的裝置的名稱。

卡巴斯基公告

本節說明如何使用、設定和停用卡巴斯基公告。

關於卡巴斯基公告

卡巴斯基公告部分（**監控和報告 → 卡巴斯基公告**）透過提供與您的卡巴斯基安全管理中心版本和受管理裝置上安裝的受管理應用程式相關資訊，讓您隨時了解最新資訊。卡巴斯基安全管理中心會透過刪除過時的公告並新增資訊來定期更新此部分中的資訊。

卡巴斯基安全管理中心僅顯示與目前連線的管理伺服器和安裝在該管理伺服器的受管理裝置上的 Kaspersky 應用程式相關的 Kaspersky 公告。對於任何類型的管理伺服器（主要、次要或虛擬），公告會單獨顯示。

管理伺服器必須具有網際網路連線才能接收卡巴斯基公告。

公告包括以下類型的資訊：

- 與安全相關的公告

  與安全相關的公告旨在使網路中安裝的卡巴斯基應用程式保持最新狀態並具有完整功能。公告可能包括有關卡巴斯基應用程式的重要更新、已發現弱點的修復以及解決卡巴斯基應用程式中其他問題的方法資訊。預設情況下，與安全相關的公告是啟用的。如果您不想接收卡巴斯基公告，則可以停用此功能。

  為了向您顯示與您的網路防護配置相對應的資訊，卡巴斯基安全管理中心將資料傳送到卡巴斯基雲端伺服器，並僅接收與網路中安裝的卡巴斯基應用程式有關的公告。可以傳送到伺服器的資料集在您安裝卡巴斯基安全管理中心管理伺服器時接受的最終使用者產品授權協議中有說明。

- 行銷公告

  行銷公告包括有關卡巴斯基應用程式的特別優惠、廣告和卡巴斯基新聞的資訊。預設情況下，會停用行銷公告。僅在啟用卡巴斯基安全網路 (KSN) 的情況下，您才會收到此類公告。您可以透過停用 KSN 停用行銷公告。

  為了僅向您顯示可能有助於防護網路裝置和日常工作的相關資訊，卡巴斯基安全管理中心會將資料傳送到卡巴斯基雲端伺服器並接收相應的公告。可傳送到伺服器的資料集在 KSN 聲明的“已處理資料”區段中有說明。

根據重要性，新資訊分為以下幾類：

1. 重要資訊
2. 重要新聞

3. 警告

4. 資訊

當"卡巴斯基公告"部分中出現新資訊時，卡巴斯基安全管理中心 網頁主控台將顯示一個通知標籤，該標籤與公告的嚴重等級相對應。您可以在"卡巴斯基公告"部分中點擊標籤以檢視此公告。

您可以指定卡巴斯基公告設定，包括您要檢視的公告類別以及顯示通知標籤的位置。

指定卡巴斯基公告設定

在卡巴斯基公告區段，您可以指定卡巴斯基公告設定，包括您要檢視的公告類別以及顯示通知標籤的位置。

設定卡巴斯基公告：

1. 在主功能表中，轉至 **監控和報告 → 卡巴斯基公告**。

2. 點擊**設定**連結。

   隨即開啟"卡巴斯基公告設定"視窗。

3. 指定下列設定：

   - 選取您要檢視的公告嚴重等級。其他類別的公告將不會顯示。
   - 選擇通知標籤要顯示的位置。該標籤可以顯示在所有主控台部分，也可以顯示在**監控和報告**部分及其子部分。

4. 點擊**確定**按鈕。

   卡巴斯基公告設定已配置完成。

停用卡巴斯基公告

卡巴斯基公告部分（**監控和報告 → 卡巴斯基公告**）透過提供與您的卡巴斯基安全管理中心版本和受管理裝置上安裝的受管理應用程式相關資訊，讓您隨時了解最新資訊。如果您不想接收卡巴斯基公告，則可以停用此功能。

卡巴斯基公告包括兩種類型的資訊：與安全相關的公告和行銷公告。您可以分別停用每種類型的公告。

停用與安全性有關的公告：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。

   管理伺服器內容視窗將開啟。

2. 在**一般**頁籤，選取**卡巴斯基公告**部分。

3. 將切換按鈕切換到**與安全相關的公告 已停用**位置。

4. 點擊**儲存**按鈕。

   卡巴斯基的公告已停用。

預設情況下，會停用行銷公告。僅在啟用卡巴斯基安全網路 (KSN) 的情況下，您才會收到行銷公告。您可以透過停用 KSN 來停用此類型的公告。

停用行銷公告：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**標籤上，選取**KSN 代理設定**區段。
3. 停用**使用卡巴斯基安全網路 已啟用**選項。
4. 點擊**儲存**按鈕。
   行銷公告隨即停用。

檢視有關威脅偵測的資訊

您可以啟用或停用顯示警示資訊。

*要在主功能表中啟用或停用顯示**警示**部分：*

1. 在主功能表中，轉到您的帳戶設定，然後選擇**介面選項**。
2. 在開啟的**介面選項**視窗中，啟用或停用**顯示 EDR 警示**選項。
3. 按一下**儲存**。

主控台在主功能表的 **監控和報告** 部分中顯示**警示**子部分。在**警示**子部分中，您可以檢視有關在端點裝置上偵測威脅的資訊。如果您新增 EDR Optimum 產品授權金鑰，則卡巴斯基安全管理中心網頁主控台會在主功能表的**監控和報告**部分自動顯示**警示** 子部分。另外，您可以新增小工具以顯示有關警示的資訊。

> 只有當您在啟用**警示**選項之前新增了 EDR Optimum 的產品授權金鑰時，**顯示 EDR 警示**子部分才會自動顯示。如果您在啟用**顯示 EDR 警示**選項後新增了產品授權金鑰，則只有在重新啟用此選項後才會顯示**警示**子部分。

要在警示卡中正確顯示有關偵測到的威脅的詳細資訊，您必須從可用外掛程式清單中選擇EDR Optimum 外掛程式，然後進行更新。此外，您還必須安裝Kaspersky Endpoint Agent 外掛程式 以及 Kaspersky Endpoint Security 外掛程式的相容版本（Kaspersky Endpoint Security for Linux 12.1 或更高版本、Kaspersky Endpoint Security for Mac 12.1 或更高版本、或 Kaspersky Endpoint Security for Windows 12.6 或更高版本）。

使用**篩選**功能表按日期和欄位值篩選警示。

物件類型欄位包含以下值：

- 未知
- 釣魚連結
- 病毒
- 木馬

- 惡意工具
- 後門程式
- 蠕蟲
- 其他應用程式
- 廣告軟體
- 色情軟體
- 危險封裝程式
- 危險行為

自動回應欄位包含以下值：

- 偵測到惡意物件
- 物件已刪除
- 物件已解毒
- 物件解毒失敗
- 物件已移動到隔離
- 偵測到密碼防護的存檔
- 偵測到的病毒

從隔離區和備份區下載和刪除檔案

本節提供有關如何從卡巴斯基安全管理中心 網頁主控台的隔離區和備份區中下載和刪除檔案的資訊。

從隔離區和備份區下載檔案

僅當滿足以下兩個條件之一時，您才能從隔離和備份區下載檔案：裝置設定中啟用了**不斷開與管理伺服器的連線**選項，或者正在使用連線閘道。否該下載將無法完成。

要將隔離區或備份區中的檔案備份儲存到硬碟磁碟機，請執行以下操作：

1. 執行以下操作之一：
   - 如果要從隔離區儲存檔案副本，請在主功能表中，轉到**操作 → 儲存區 → 隔離**。
   - 如果要從備份儲存檔案副本，請在主功能表中，轉到**操作 → 儲存區 → 備份**。
2. 在開啟的視窗中，選擇要下載的檔案，然後點擊**下載**。

下載開始。已放置在用戶端裝置上隔離區中的檔案的副本將被儲存到指定的資料夾中。

卡巴斯基安全管理中心網頁主控台活動記錄

卡巴斯基安全管理中心 網頁主控台活動記錄可以說明調查軟體故障原因。當您就卡巴斯基安全管理中心 網頁主控台的故障聯絡 Kaspersky 技術支援時，Kaspersky 技術支援專家可以向您請求卡巴斯基安全管理中心 網頁主控台記錄檔案。您使用應用程式的整個時間內，卡巴斯基安全管理中心 網頁主控台記錄檔案儲存在 <卡巴斯基安全管理中心 網頁主控台安裝資料夾>/logs 資料夾。記錄檔案不被自動傳送到 Kaspersky 技術支援專家。

要啟用卡巴斯基安全管理中心 網頁主控台活動記錄

在**卡巴斯基安全管理中心 14 網頁主控台安裝精靈**中的**啟用卡巴斯基安全管理中心網頁主控台活動記錄**視窗中，選取卡巴斯基安全管理中心網頁主控台連線設定核取方塊。

記錄檔案是文字格式。

記錄檔案名稱是<元件名稱>.<裝置名稱>-<檔案修訂號>.YYYY-MM-DD 格式，其中：

- <元件名稱>是卡巴斯基安全管理中心元件或卡巴斯基安全管理中心 網頁主控台管理外掛程式名稱。
- <裝置名稱>是正在執行<元件名稱>的裝置的名稱。
- <檔案修訂號>是為在<裝置名稱>中操作的<元件名稱>建立的記錄檔案號碼。一天中，相同<元件名稱>和<裝置名稱>的若干記錄檔案可以被建立。記錄檔案的最大大小是 50 MB。當達到最大大小時，新記錄檔案被建立。新記錄檔案<檔案修訂號>增加 1。
- YYYY、MM 和 DD 是記錄首次被建立的年、月、日。當新的一天開始時，新的記錄檔案被建立。

卡巴斯基安全管理中心和其他解決方案之間的整合

本節介紹如何設定從卡巴斯基安全管理中心網頁主控台到另一個卡巴斯基應用程式的存取，例如 Kaspersky Endpoint Detection and Response。此部分還介紹如何配置匯出到 SIEM 系統。

配置到 KATA / KEDR 網頁主控台的存取

Kaspersky Anti Targeted Attack（KATA）和 Kaspersky Endpoint Detection and Response（KEDR）是 Kaspersky Anti Targeted Attack Platform 的兩個功能塊。您可以透過 Kaspersky Anti Targeted Attack Platform 的網頁主控台（KATA / KEDR 網頁主控台）管理這些功能塊。如果您使用卡巴斯基安全管理中心 網頁主控台和 KATA / KEDR 網頁主控台，您可以從卡巴斯基安全管理中心 網頁主控台介面直接配置到 KATA / KEDR 網頁主控台的存取。

要配置到 KATA / KEDR 網頁主控台的存取：

1. 在主功能表中，轉至 **主控台設定 → 整合**。
2. 在**整合**頁籤，選取**KATA**區段。

3. 在 **KATA / KEDR 網頁主控台的網址** 欄位中輸入 KATA/KEDR 網頁主控台的 URL。

4. 點擊**儲存**按鈕。

進階管理 下拉清單被新增到主應用程式視窗中。您可以使用該功能表開啟 KATA / KEDR 網頁主控台。您點擊 **進階網路安全** 後，帶有您指定網址的新頁籤在您的瀏覽器開啟。

建立背景連線

要讓卡巴斯基安全管理中心網頁主控台執行背景工作，您必須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。如果您的帳戶具有**一般功能：使用者權限**功能區域中的**修改物件 ACL** 權限，則可以建立此連線。

如果您安裝 Kaspersky Endpoint Security for Windows 12.3 的外掛程式，或者如果您從 11.7 之前的版本更新 Kaspersky Endpoint Security for Windows 外掛程式並且尚未建立背景連線，則會顯示通知您必須建立背景連線。此外，您必須授予服務帳戶**一般功能：在管理伺服器上操作**功能區域的權限。

要建立背景連線：

1. 在主功能表中，轉至 **主控台設定 → 整合**。

2. 在**整合** 頁簽上，將建立背景連線的切換按鈕切換到以下位置：**為整合建立背景連線 已啟用**。

3. 在開啟的**建立背景連線的服務將在卡巴斯基安全管理中心網頁主控台伺服器上啟動**區段中，點擊**確定**按鈕。

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。管理伺服器會為背景連線建立一個帳戶，該帳戶會當作服務帳戶使用，以維護卡巴斯基安全管理中心與另一個卡巴斯基應用程式或解決方案之間的互動。該服務帳戶的名稱包含 NWCSvcUser 前置碼。

出於安全考量，管理伺服器每 30 天會自動變更一次服務帳戶的密碼。您無法手動刪除此服務帳戶。當您停用跨服務連線時，管理伺服器會自動刪除此帳戶。管理伺服器會為每個管理主控台建立一個服務帳戶，並將所有服務帳戶分配給名稱為 ServiceNwcGroup 的安全群組。在卡巴斯基安全管理中心安裝過程中，管理伺服器會自動建立此安全群組。您無法手動刪除此安全群組。

在雲端環境中搭配卡巴斯基安全管理中心網頁主控台使用

本節說明在雲端環境中與卡巴斯基安全管理中心部署與維護相關的卡巴斯基安全管理中心網頁主控台功能資訊，例如 Amazon Web Services、Microsoft Azure 或 Google Cloud。

若要在雲端環境中作業，您需要特殊產品授權。如果沒有這類產品授權，則不會顯示雲端裝置相關的介面元素。

卡巴斯基安全管理中心網頁主控台中的雲端環境設定

要使用設定環境精靈配置卡巴斯基安全管理中心，您必須擁有以下事項：

- 以下為適用於雲端環境的特定憑證：
  - 已授予輪詢雲端區段的 IAM 角色或已授予輪詢雲端區段權利的 IAM 使用者帳戶（搭配 Amazon Web Services 使用）
  - Azure 應用程式 ID、密碼和訂閱（搭配 Microsoft Azure 使用）
  - Google 用戶端電子郵件、Project ID 與私密金鑰（搭配 Google Cloud 使用）
- 安裝套件：
  - Windows 網路輪詢
  - Linux 網路輪詢
  - Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Linux 的 Web 外掛程式
- 至少以下一項：
  - Kaspersky Endpoint Security for Windows 的安裝套件和 Web 外掛程式（建議）
  - Kaspersky Security for Windows Server 的安裝套件和 Web 外掛程式

設定雲端環境精靈在透過管理主控台第一次連線到管理伺服器時自動啟動，如果您正在從現成映像佈署卡巴斯基安全管理中心。您還可以在任意時刻手動啟動精靈。

要手動啟動設定雲端環境精靈，

在主功能表中，轉至 **發現和佈署 → 佈署和分配 → 設定雲端環境**。

精靈隨即啟動。

雲端環境設定的平均連線時間約 15 分鐘。

步驟 1：檢查需要的外掛程式和安裝套件

如果您擁有下面列出的所有必要 Web 外掛程式和安裝套件，則不會顯示此步驟。

要設定雲端環境，您必須具有以下元件：

- 安裝套件：
  - Windows 網路輪詢
  - Linux 網路輪詢
  - Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Linux 的 Web 外掛程式
- 至少以下一項：
  - Kaspersky Endpoint Security for Windows 的安裝套件和 Web 外掛程式（建議）
  - Kaspersky Security for Windows Server 的安裝套件和 Web 外掛程式
    我們建議您使用 Kaspersky Endpoint Security for Windows 而不是 Kaspersky Security for Windows Server。

卡巴斯基安全管理中心會自動偵測您已有的元件，僅列出缺少的元件。按一下**選擇要下載的應用程式**按鈕，然後選擇需要的外掛程式和安裝套件，來下載列出的元件。下載元件後，您可以使用**重新整理**按鈕更新缺少的元件清單。

步驟 2：許可應用程式

此步驟僅會在您使用 BYOL AMI 且您尚未啟動應用程式進行 Kaspersky Security for Virtualization 授權或 Kaspersky Hybrid Cloud Security 授權時顯示。

指定產品授權金鑰並點擊**下一步**繼續。

該授權金鑰會新增至管理伺服器儲存區。

若要再次執行精靈，則不會顯示此步驟。

步驟 3：選取雲端環境與授權

該部分描述僅套用到卡巴斯基安全管理中心 12.1 或更新版本的功能。

指定下列設定：

- **雲端環境**

  選取您佈署卡巴斯基安全管理中心的雲端環境：AWS、Azure 或 Google 雲端。

  若您不只一個雲端環境中工作，請選取一個環境接著再次執行精靈。

- **連線名稱**

  輸入連線名稱。名稱不能包括 256 個以上字元。僅允許 Unicode 字元。

  該名稱也將用作雲端裝置的管理群組名稱。

  若您計畫處理多個雲端環境，您可能想要在連線名稱中納入環境名稱，例如「Azure 區段」、「AWS 區段」或「Google 區段」。

輸入憑證以接收您指定之雲端環境的驗證。

AWS

若您選取 AWS 作為雲端區段類型，您需要 IAM 角色或 AWS IAM 存取金鑰來勁一步輪詢雲端區段。

- **分配給 EC2 實例的 AWS IAM 角色**

  若您有管理伺服器必要權限的 IAM 角色，請選取此選項。

- **AWS IAM 使用者**

  若您有選取 AWS IAM 存取金鑰，請選取此選項。輸入您的金鑰資料：

  - **存取金鑰 ID**

    IAM 存取金鑰 ID 是個字母數字序列。當您在建立 IAM 使用者帳戶時接收金鑰 ID。

    如果您選取了 AWS IAM 存取金鑰來授權而不是 IAM 角色，該欄位可用。

  - **金鑰**

    您建立 IAM 使用者帳戶時接收到的帶有存取金鑰 ID 的金鑰。

    金鑰的字元顯示為星號。在您開始輸入金鑰後，**顯示**按鈕被顯示。按一下並按住該按鈕一定時間以檢視輸入的字元。

    如果您選取了 AWS IAM 存取金鑰來授權而不是 IAM 角色，該欄位可用。

    若要檢視您輸入的字元，請按住**顯示**按鈕。

Azure

如果您選取了 Azure 作為雲端區段類型，請為將來輪詢雲端區段所使用的連線指定以下設定：

- **Azure 應用程式 ID**

  您在 Azure 網站建立了該應用程式 ID。

  您僅可以提供一個 Azure 應用程式 ID 用於輪詢和其他目的。如果您要輪詢其他 Azure 段，您必須先刪除現有 Azure 連線。

- **Azure 訂購 ID**

  您在 Azure 網站建立了該訂購。

- **Azure 應用程式密碼**

  當您建立應用程式 ID 時您收到應用程式 ID 的密碼。

  密碼的字元顯示為星號。在您開始輸入密碼後，**顯示**按鈕可用。按一下並按住該按鈕以檢視您輸入的字元。

  若要檢視您輸入的字元，請按住**顯示**按鈕。

- **Azure 儲存帳戶名稱**

  您建立了 Azure 儲存帳戶名稱以使用卡巴斯基安全管理中心。

- **Azure 儲存存取金鑰**

  您建立 Azure 儲存帳戶以使用卡巴斯基安全管理中心時接收密碼（金鑰）。

  金鑰在“Azure 儲存帳戶概述”區域的“金鑰”子區域可用。

  若要檢視您輸入的字元，請按住**顯示**按鈕。

Google Cloud

如果您選取了 Google Cloud 作為雲端區段類型，請為將來輪詢雲端區段所使用的連線指定以下設定：

- **用戶端電子郵件地址**

  輸入您用來在 Google Cloud 註冊專案的電子郵件。

- **項目 ID**

  專案 ID 是您在 Google Cloud 註冊專案時收到的 ID。

- **私密金鑰**

  私密金鑰是您在 Google Cloud 註冊專案時作為私密金鑰收到的字元序列。您可能會想要複製並貼上此序列，以免出錯。

  若要檢視您輸入的字元，請按住**顯示**按鈕。

您指定的連線會儲存在應用程式設定。

設定雲端環境精靈允許您僅指定一個區段。之後，您可以指定更多的連線以管理其他雲端區段。

點擊**下一步**繼續。

步驟 4：區段輪詢，設定與雲端的同步並選取後續操作

在此步驟，雲端區段輪詢開始，雲端裝置的特別管理群組隨即自動建立。裝置中發現的實例會放置在此群組。雲端區段輪詢排程已配置（依預設為每 5 分鐘一次，您可稍後變更此設定）。

與雲端同步自動移動規則也被建立。對於每個雲端網路的後續掃描，系統都會將偵測到的虛擬裝置移動到**受管理裝置\雲端**群組的對應子群組。

定義下列設定：

- **與雲端結構同步管理群組**

  如果啟用該選項，**雲端**群組被自動建立在**受管理裝置**群組，雲端裝置發現被啟動。在每個雲端網路掃描中偵測到的實例和虛擬機被放置到雲端群組。該群組的管理子群組結構比對您的雲端區段結構（在 AWS 中，可用網域和放置群組不出現在結構中；在 Azure 中，子網路不出現在結構中）。未被識別為雲端環境中實例的裝置在**未配置的裝置**群組。該群組結構允許您使用群組安裝工作安裝病毒防護應用程式到實例，以及為不同群組設定不同的政策。

  如果停用該選項，**雲端**群組也被建立，且雲端裝置發現也被啟動；然而，比對雲端區段結構的子群組不在群組中被建立。所有偵測到的實例都在**雲端**管理群組，因此顯示在單一清單。如果您使用的卡巴斯基安全管理中心需要同步，您可以修改**與雲端同步**規則的內容並強制它。強加該規則改變雲端群組的子群組結構，以便比對您雲端區段的結構。

  預設情況下已停用該選項。

- **佈署防護**

  如果選取該選項，精靈建立工作以安裝安全應用程式到實例。精靈完成後，防護佈署精靈自動在您的雲端區段的裝置上啟動，並且您將可以在這些裝置上安裝網路代理和安全應用程式。

  卡巴斯基安全管理中心可以使用其本機工具執行佈署。如果您沒有權限安裝應用程式到 EC2 實例或 Azure 虛擬機，您可以手動設定**遠端安裝**工作並指定帶有所需權限的帳戶。此種情況下，遠端安裝工作將不用於使用 AWS API 或 Azure 發現的裝置。該工作將僅用於使用 Active Directory 輪詢、Windows 網域輪詢或 IP 範圍輪詢發現的裝置。

  如果未選取該選項，防護佈署精靈不被啟動，安裝安全應用程式的工作未在實例上被建立。您可以稍後手動執行這些操作。

若您選取佈署防護選項，**正在重啟裝置**區段會變為可用。在此區段，您必須在目標裝置作業系統重新啟動時才選取要進行的操作。選取在安裝應用程式過程中裝置作業系統必須重新啟動時是否重新啟動實例：

- **不重新啟動**

  如果選取該選項，安全應用程式安裝後裝置不被重新啟動。

- **重新啟動**

  如果選取該選項，安全應用程式安裝後裝置將被重新啟動。

點擊**下一步**繼續。

若為 Google Cloud，您僅可執行搭配卡巴斯基安全管理中心原生工具的佈署。若您選擇 Google Cloud，則無法使用**佈署防護**選項。

步驟 5：選擇一個應用程式來為其建立政策和工作

僅當您同時擁有 Kaspersky Endpoint Security for Windows 和 Kaspersky Security for Windows Server 的安裝套件和外掛程式時才會顯示此步驟。如果您只有其中一個應用程式的外掛程式和安裝套件，則會跳過此步驟，卡巴斯基安全管理中心會為現有應用程式建立政策和工作。

選取您要為其建立政策和工作的應用程式：

- Kaspersky Endpoint Security for Windows
- Kaspersky Security for Windows Server

步驟 6：設定適用於卡巴斯基安全管理中心的卡巴斯基安全網路

指定設定以轉發卡巴斯基安全管理中心操作資訊到卡巴斯基安全網路 (KSN) 知識庫。您可以選取以下其中一個方法：

- **我同意使用卡巴斯基安全網路**

  安裝在用戶端裝置上的卡巴斯基安全管理中心與受管理應用程式會自動傳輸其作業詳情至卡巴斯基安全網路。參與卡巴斯基安全網路確保了包含病毒和其他威脅的資料庫的快速更新，該資料庫確保了對緊急安全威脅的快速回應。

- **我不同意使用卡巴斯基安全網路**

  卡巴斯基安全管理中心和受管理應用程式將不會提供資訊至卡巴斯基安全網路。

  若您選取此選項，則會停用卡巴斯基安全網路。

Kaspersky 建議您參與卡巴斯基安全網路。

受管理應用程式的 KSN 協議也會隨即顯示。若您同意使用卡巴斯基安全網路，受管理應用程式會將資料傳送至 Kaspersky。若您不同意參與卡巴斯基安全網路，受管理應用程式不會將資料傳送至 Kaspersky。（您可之後在應用程式政策中變更此設定。）

點擊**下一步**繼續。

步驟 7：建立初始保護設定

您可以檢查建立的政策和工作清單。

等候建立政策與工作完成後，接著點擊**下一步**。在精靈的最後一頁上，點擊**完成**按鈕退出。

透過卡巴斯基安全管理中心網頁主控台進行網路區段輪詢

管理伺服器透過使用 AWS API、Azure API 或 Google API 工具對雲端區段進行一般輪詢來接收有關該網路中網路和裝置的結構的資訊。卡巴斯基安全管理中心使用此資訊更新未配置裝置的內容與受管理裝置資料夾。如果您配置了裝置自動移動到管理群組，偵測到的裝置將被包含在管理群組中。

要允許管理伺服器輪詢雲端區段，您必須對 IAM 角色或 IAM 使用者帳戶（在 AWS 中）或對應用程式 ID 和密碼（在 Azure 中）或對 Google 用戶端電子郵件、Google 專案 ID 和私密金鑰提供相應權限（在 Google Cloud）。

您可以新增或刪除連線，以及為每個雲端區段設定輪詢排程。

為雲端區段輪詢新增連線

要新增雲端區段輪詢連線到可用連線清單：

1. 在主功能表中，轉至 **發現和佈署** → **發現** → **雲端**。
2. 在開啟的視窗中，點擊**內容**。
3. 在開啟的**設定**視窗中，點擊**新增**按鈕。
   雲端區段設定視窗開啟。
4. 為將來輪詢雲端區段所使用的連線指定雲端環境名稱：

- **雲端環境**

  選取您佈署卡巴斯基安全管理中心的雲端環境：AWS、Azure 或 Google 雲端。
  若您不只一個雲端環境中工作，請選取一個環境接著再次執行精靈。

- **連線名稱**

  輸入連線名稱。名稱不能包括 256 個以上字元。僅允許 Unicode 字元。
  該名稱也將用作雲端裝置的管理群組名稱。
  若您計畫處理多個雲端環境，您可能想要在連線名稱中納入環境名稱，例如「Azure 區段」、「AWS 區段」或「Google 區段」。

5. 輸入憑證以接收您指定之雲端環境的驗證。

- 若您選取了 AWS，請指定下列設定：

  - **使用 AWS IAM 角色**

    如果您已經為管理伺服器建立了 IAM 角色以使用 AWS 服務，則選取該方塊。

  - **AWS IAM 使用者憑據**

    如果您擁有帶有必要權限的 IAM 使用者帳戶且您可以輸入金鑰 ID 和金鑰，則選取該方塊。

    若您指定已有AWS IAM 使用者憑據，請指定以下項目：

    - **存取金鑰 ID**

      IAM 存取金鑰 ID 是個字母數字序列。當您在建立 IAM 使用者帳戶時接收金鑰 ID。

      如果您選取了 AWS IAM 存取金鑰來授權而不是 IAM 角色，該欄位可用。

    - **金鑰**

      您建立 IAM 使用者帳戶時接收到的帶有存取金鑰 ID 的金鑰。

      金鑰的字元顯示為星號。在您開始輸入金鑰後，**顯示**按鈕被顯示。按一下並按住該按鈕一定時間以檢視輸入的字元。

      如果您選取了 AWS IAM 存取金鑰來授權而不是 IAM 角色，該欄位可用。

    若要檢視您輸入的字元，請按住**顯示**按鈕。

- 若您選取了 Azure，請指定下列設定：

  - **Azure 應用程式 ID**

    您在 Azure 網站建立了該應用程式 ID。

    您僅可以提供一個 Azure 應用程式 ID 用於輪詢和其他目的。如果您要輪詢其他 Azure 段，您必須先刪除現有 Azure 連線。

  - **Azure 訂購 ID**

    您在 Azure 網站建立了該訂購。

  - **Azure 應用程式密碼**

    當您建立應用程式 ID 時您收到應用程式 ID 的密碼。

    密碼的字元顯示為星號。在您開始輸入密碼後，**顯示**按鈕可用。按一下並按住該按鈕以檢視您輸入的字元。

    若要檢視您輸入的字元，請按住**顯示**按鈕。

- **Azure 儲存帳戶名稱**

  您建立了 Azure 儲存帳戶名稱以使用卡巴斯基安全管理中心。

- **Azure 儲存存取金鑰**

  您建立 Azure 儲存帳戶以使用卡巴斯基安全管理中心時接收密碼（金鑰）。

  金鑰在“Azure 儲存帳戶概述”區域的“金鑰”子區域可用。

  若要檢視您輸入的字元，請按住**顯示**按鈕。

若您選取了 Google Cloud，請指定下列設定：

- **用戶端電子郵件地址**

  輸入您用來在 Google Cloud 註冊專案的電子郵件。

- **項目 ID**

  專案 ID 是您在 Google Cloud 註冊專案時收到的 ID。

- **私密金鑰**

  私密金鑰是您在 Google Cloud 註冊專案時作為私密金鑰收到的字元序列。您可能會想要複製並貼上此序列，以免出錯。

  若要檢視您輸入的字元，請按住**顯示**按鈕。

6. 如有需要，請點擊**設定輪詢排程**接著變更預設設定。

該連線儲存在應用程式設定。

第一次輪詢新雲端區段後，與該段對應的子群組會出現在**受管理裝置\雲端**管理群組。

如果您指定不正確的憑證，在雲端區段輪詢過程中將不會發現實例，且新子群組將不會出現在**受管理裝置\雲端**管理群組。

為雲端區段輪詢刪除連線

如果您不再必須輪詢特定雲端區段，您可以從可用連線清單刪除對應的連線。您還可以刪除連線，如果，例如輪詢雲端區段的權限被轉移給另一個帶有不同憑證的使用者。

要刪除連線：

1. 在主功能表中，轉至 **發現和佈署 → 發現 → 雲端**。
2. 在開啟的視窗中，點擊**內容**。

3. 在開啟的**設定**視窗中，點擊要刪除之區段的名稱。

4. 點擊**刪除**。

5. 在開啟的視窗中，點擊**確定**按鈕以確認您的選取。

連線已刪除。對應此連線的雲端區段中的裝置會自動從管理群組中刪除。

透過卡巴斯基安全管理中心網頁主控台設定輪詢排程

雲端區段輪詢依據排程執行。您可以設定輪詢頻率。

輪詢頻率被在設定雲端環境設定中自動設定為 5 分鐘。您可以在任意時刻變更該值並設定不同的排程。但不建議您設定比每 5 分鐘一次還要多的輪詢頻率，因為這可能導致 API 操作錯誤。

要設定雲端區段輪詢排程：

1. 在主功能表中，轉至 **發現和佈署 → 發現 → 雲端**。

2. 在開啟的視窗中，點擊**內容**。

3. 在開啟的**設定**視窗中，點擊要配置輪詢排程的區段名稱。

   這將開啟**雲端區段設定**視窗。

4. 在**雲端區段設定**視窗中，點擊**設定輪詢排程**按鈕。

   這會開啟**排程**視窗。

5. 在**排程**視窗，指定以下設定：

- **排程開始**

  輪詢排程選項：

  - **每 N 天**

    輪詢定期執行，按照指定天數間隔，從指定的日期和時間開始。

    預設下，輪詢每天執行一次，從目前系統日期和時間開始。

  - **每 N 分鐘**

    輪詢定期執行，按照指定分鐘間隔，從指定的時間開始。

    預設下，輪詢每五分鐘執行一次，從目前系統時間開始。

  - **周中天數**

    輪詢定期執行，在指定星期的指定時間。

    預設下，輪詢會每週五下午 6:00:00 執行。

  - **每個月所選週的指定日**

    輪詢定期執行，在指定月日的指定時間。

    預設下，未選取月日；預設啟動時間是 6:00:00 P.M.。

- **開始間隔（分鐘）**

  指定 N 等於的值（分鐘或延遲）。

- **開始於**

  指定要完成初次輪群的時間。

- **執行略過的工作**

  如果在排程輪詢期間管理伺服器被切換掉或不可用，管理伺服器可以在切換回來後立即啟動輪詢，或者等待下次排程輪詢。

  如果啟用該選項，管理伺服器在它切換回來後立即啟動輪詢。

  如果停用該選項，管理伺服器等待下一次排程輪詢。

  預設情況下已啟用該選項。

6. 點擊**Save**以儲存變更。

區段的輪詢排程隨即配置並儲存。

透過卡巴斯基安全管理中心 網頁主控台檢視雲端區段輪詢結果

您可檢視雲端區段輪詢的結果，意即檢視受管理伺服器管理的雲端裝置清單。

要檢視雲端區段輪詢結果：

在主功能表中，轉至 **發現和佈署 → 發現 → 雲端**。

這會顯示可輪詢的雲端區段。

透過卡巴斯基安全管理中心 網頁主控台檢視雲端裝置內容

您可以檢視每一個雲端裝置的內容。

若要檢視雲端裝置內容：

1. 在主功能表中，轉至 **裝置 → 受管理裝置**。
2. 點擊您要檢視內容的裝置名稱。
   內容視窗開啟，**一般**區域被選中。
3. 若您想檢視特定的雲端裝置內容，請在內容視窗中選擇**系統**區域。
   隨即會視裝置的雲端平台來顯示內容。
   針對 AWS 中的裝置，會顯示下列內容：

   - **使用 API** (值：**AWS**) 發現的裝置
   - **雲端區域**
   - **雲端 VPC**
   - **雲端可用性區域**
   - **雲端子網路遮罩**
   - **雲端位置群組** (此單元只會在實例屬於位置群組時顯示；否則，它將不會顯示)

   針對 Azure 中的裝置，會顯示下列內容：

   - **使用 API** (值：**Microsoft Azure**) 發現的裝置
   - **雲端區域**
   - **雲端子網路遮罩**

   針對 Google Cloud 中的裝置，會顯示下列內容：

   - **使用 API** (值：**Google Cloud**) 發現的裝置
   - **雲端區域**
   - **雲端 VPC**
   - **雲端可用性區域**
   - **雲端子網路遮罩**

與雲端同步：設定移動規則

在設定雲端環境操作中，與雲端同步規則被自動建立。規則允許您從「未配置的裝置」群組自動移動在輪詢中偵測到的實例到受管理裝置\雲端群組，使實例就可用於集中管理。預設下，規則在建立後被啟動。您可以在任意時刻停用、修改或強制規則。

要編輯與雲端同步規則的內容和/或強制規則：

1. 在主功能表中，轉至**發現和佈署 → 佈署和分配 → 移動規則**。
   這會開啟移動規則的清單。

2. 在移動規則的清單中，選取**與雲端同步**。
   這會開啟規則內容視窗。

3. 如有需要，請在**規則條件**頁籤的**雲端區段**頁籤中指定以下設定：

- **裝置在雲端區段中**

  該規則僅套用到位於所選雲端區段的裝置。否則，該規則套用到發現的所有裝置。

  預設情況下已選定此選項。

- **包含子物件**

  該規則套用到所選段和其所有嵌套雲端子區域中的所有裝置。否則，該規則僅套用到位於根段的裝置。

  預設情況下已選定此選項。

- **從嵌套物件移動裝置到對應子群組**

  如果啟用該選項，嵌套物件的裝置將被自動移動到對應其結構的子群組。

  如果停用該選項，嵌套物件的裝置將被自動移動到雲端子群組的根，而不再分支。

  預設情況下已啟用該選項。

- **建立對應於新偵測到裝置的容器的子群組**

  如果啟用該選項，當**受管理裝置雲端**結構沒有比對包含裝置的區域的子群組，卡巴斯基安全管理中心將建立這類子群組。例如，如果一個子網在裝置發現中被發現，帶有相同名稱的新組將在**受管理裝置\雲端**群組下被建立。

  如果停用該選項，卡巴斯基安全管理中心不建立任何新子群組。例如，如果一個子網在網路輪詢中被發現，帶有相同名稱的新群組將不在**受管理裝置雲端**群組下被建立，且該子群組中的裝置將被移動到**受管理裝置雲端**群組。

  預設情況下已啟用該選項。

- **刪除在雲端區段中找不到比對的子群組**

  如果啟用該選項，應用程式從雲端群組刪除所有不比對任何現有雲端物件的子群組。

  如果停用該選項，未比對任何現有雲端物件的子群組被保留。

  預設情況下已啟用該選項。

若您在使用雲端環境設定精靈啟用**與雲端結構同步管理群組**選項，**與雲端同步**規則會在啟用**建立對應於新偵測到裝置的容器的子群組**與**刪除在雲端區段中找不到比對的子群組**選項時建立。

若您不啟用**與雲端結構同步管理群組** 選項，**與雲端同步**規則會在這些選項停用（未核取）時建立。若您使用卡巴斯基安全管理中心，則在**受管理裝置\雲端**子群組的子群組結構需符合雲端區段結構，在規則內容中啟用**建立對應於新偵測到裝置的容器的子群組** 與**刪除在雲端區段中找不到比對的子群組**選項，接著強制執行該規則。

4. 在**使用 API 發現的裝置**下拉清單，選取以下值之一：

   - **否**。系統無法用 AWS、Azure 或 Google API 偵測裝置，意即裝置在雲端環境外或在雲端環境中，但由於一些原因無法使用 API 加以偵測。
   - **AWS**。裝置使用 AWS API 發現，就是，裝置在 AWS 雲端環境中。
   - **Azure**。裝置使用 Azure API 發現，就是，裝置在 Azure 雲端環境中。
   - **Google Cloud**。裝置使用 Google API 發現，就是，裝置在 Google 雲端環境中。
   - 沒有值。該標準無法被套用。

5. 如果必要，在其他區域設定其他規則內容。

移動規則隨即配置完成。

將應用程式遠端安裝到 Azure 虛擬機

您必須擁有有效產品授權，才能安裝應用程式到 Microsoft Azure 虛擬機。

卡巴斯基安全管理中心支援以下情境：

- 用戶端裝置會透過 Azure API 探索；安裝也會透過 API 執行。使用 Azure API 意味著您只能安裝以下應用程式：
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Security for Windows Server
- 用戶端裝置會透過 Azure API 探索；安裝則透過發佈點執行，如果沒有發佈點，則使用獨立安裝套件手動進行。您可以透過這種方式安裝卡巴斯基安全管理中心支援的任何應用程式。

若要在 Azure 虛擬機上建立遠端安裝應用程式工作：

1. 在主功能表中，轉至 **裝置** → **工作**。
2. 點擊**新增**。
   新工作精靈啟動。
3. 遵照精靈的說明：
   a. 選擇**遠端安裝應用程式**作為工作類型。
   b. 在**安裝套件**頁面上，選擇**Microsoft Azure API 的遠端安裝**。
   c. 選擇存取裝置的帳戶時，請使用現有的 Azure 帳戶，或請按一下**新增**並輸入 Azure 帳戶的憑據：
      - **Azure 帳戶名稱**
        為您指定的憑證輸入任何名稱。此名稱將會顯示在要執行該工作的帳戶清單中。
      - **Azure 應用程式 ID**
        您在 Azure 網站建立了該應用程式 ID。
        您僅可以提供一個 Azure 應用程式 ID 用於輪詢和其他目的。如果您要輪詢其他 Azure 段，您必須先刪除現有 Azure 連線。
      - **Azure 應用程式密碼**
        當您建立應用程式 ID 時您收到應用程式 ID 的密碼。
        密碼的字元顯示為星號。在您開始輸入密碼後，**顯示**按鈕可用。按一下並按住該按鈕以檢視您輸入的字元。
   d. 從**受管理裝置\雲端**群組中選擇相關裝置。

在精靈結束後，應用程式遠端安裝工作會顯示在工作清單中。

使用雲端 DBMS建立管理伺服器資料的備份工作

備份工作是管理伺服器的工作。若要使用位於雲端環境的 DBMS，您可建立備份工作（AWS 或 Azure）。

若要建立管理伺服器資料備份工作，請執行以下操作：

1. 在主功能表中，轉至 **裝置** → **工作**。
2. 點擊**新增**。
   新工作精靈啟動。

3. 在精靈首頁上的**應用程式**清單中，選取**卡巴斯基安全管理中心 14.2**並在**工作類型**清單中選取**備份管理伺服器資料**。

4. 在精靈的對應頁面，指定以下資訊：

   - 若您要在 AWS 中使用資料庫：

     - **S3 bucket 名稱**

       您為備份建立的 S3 bucket 名稱。

     - **存取金鑰 ID**

       當您建立了 IAM 使用者帳戶以使用 S3 bucket 儲存實例時，您接收到金鑰 ID（數字字母序列）。

       如果您在 S3 bucket 上選取了 RDS 資料庫則該欄位可用。

     - **金鑰**

       您建立 IAM 使用者帳戶時接收到的帶有存取金鑰 ID 的金鑰。

       金鑰的字元顯示為星號。在您開始輸入金鑰後，**顯示**按鈕被顯示。按一下並按住該按鈕一定時間以檢視輸入的字元。

       如果您選取了 AWS IAM 存取金鑰來授權而不是 IAM 角色，該欄位可用。

   - 若您要在 Microsoft Azure 中使用資料庫：

     - **Azure 儲存帳戶名稱**

       您建立了 Azure 儲存帳戶名稱以使用卡巴斯基安全管理中心。

     - **Azure 訂購 ID**

       您在 Azure 網站建立了該訂購。

     - **Azure 密碼**

       當您建立應用程式 ID 時您收到應用程式 ID 的密碼。

       密碼的字元顯示為星號。在您開始輸入密碼後，**顯示**按鈕可用。按一下並按住該按鈕以檢視您輸入的字元。

     - **Azure 應用程式 ID**

       您在 Azure 網站建立了該應用程式 ID。

       您僅可以提供一個 Azure 應用程式 ID 用於輪詢和其他目的。如果您要輪詢其他 Azure 段，您必須先刪除現有 Azure 連線。

     - **Azure SQL Server 名稱**

名稱和資源群組在您的 Azure SQL Server 內容中可用。

- **Azure SQL Server 資源群組**

  名稱和資源群組在您的 Azure SQL Server 內容中可用。

- **Azure 儲存存取金鑰**

  在您的儲存帳戶內容中可用，在存取金鑰區域。您可以使用任何金鑰（key1 或 key2）。

工作被建立並顯示在工作清單。若您啟用**建立完成時開啟工作詳情**選項，您可在工作建立後立即修改預設工作設定。如果您不啟用該選項，工作使用預設設定建立。您可以稍後隨時修改預設設定。

用戶端裝置的遠端診斷

您可在用戶端裝置遠端執行遠端診斷：

- 啟用和關閉偵錯、變更偵錯等級並下載偵錯檔案
- 下載系統資訊和應用程式設定
- 下載事件記錄
- 為應用程式建立記憶體傾印檔案
- 開始進行診斷並下載診斷報告
- 啟動、停止和重新啟動應用程式

您可以使用從用戶端裝置下載的事件記錄和診斷報告以自行定位問題。同時，若您聯絡 Kaspersky 技術支援，他們可能會請您從用戶端裝置下載偵錯檔案、傾印檔案、事件記錄和診斷報告以讓 Kaspersky 進一步分析。

遠端診斷會使用管理伺服器進行。

開啟遠端診斷視窗

若要執行對用戶端裝置的遠端診斷，您必須開啟遠端診斷視窗。

開啟遠端診斷視窗：

1. 選取您要開啟遠端診斷視窗的裝置，並執行以下其中一個動作：
   - 若裝置屬於管理群組，請在主功能表中，前往**裝置 → 受管理裝置**。
   - 若裝置屬於「未配置的裝置」群組，請在主功能表中，前往**發現和佈署 → 未配置的裝置**。
2. 點擊所需裝置的名稱。

3. 在開啟的裝置內容視窗中，選取**進階**頁籤。

4. 在開啟的視窗中，點擊**遠端診斷**。
   這會開啟用戶端裝置的**遠端診斷** 視窗。

啟用與停用應用程式偵錯

您可啟用和停用對應用程式的偵錯，包含 Xperf 偵錯。

啟用和停用偵錯

在遠端裝置上啟用或停用偵錯：

1. 開啟用戶端裝置的遠端診斷視窗。

2. 在遠端診斷視窗，點擊**遠端診斷**。

3. 在開啟的**狀態和報告**視窗，選取**Kaspersky 應用程式**區段。
   這會開啟安裝在裝置上的 Kaspersky 應用程式清單。

4. 在應用程式清單上，選取您要啟用或停用偵錯的應用程式。
   遠端診斷選項清單隨即顯示。

5. 若您要啟用偵錯：

   a. 在清單的**偵錯**區段中，點擊**啟用偵錯**。

   b. 在開啟的**修改偵錯等級**視窗中，建議您保留設定的預設值。當需要時，技術支援專家將指導您設定過程。
   下列設定可用：

   - **偵錯等級**

     偵錯等級定義偵錯檔案包含的詳情資料量。

   - **基於循環的偵錯**

     應用程式覆蓋偵錯資訊以防止偵錯檔案過量增長。指定用於儲存偵錯資訊的檔案最大數量，以及每個檔案的最大大小。如果寫入了最大數量的最大大小的偵錯檔案，最舊的檔案被刪除以便新偵錯檔案可以被寫入。

     此設定僅適用於 Kaspersky Endpoint Security

   c. 點擊**儲存**。

   偵錯會針對選取的應用程式啟用。某些情況下，要啟用偵錯，必須重新啟動安全應用程式及其工作。

6. 若您要停用對選取的應用程式偵錯，請點擊**停用偵錯**。
   系統會針對選取的應用程式停用偵錯。

啟用 Xperf 偵錯

對於 Kaspersky Endpoint Security，技術支援專家可能需求您對系統效能資訊啟用 Xperf 偵錯。

啟用和設定 Xperf 偵錯：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗，點擊**遠端診斷**。
3. 在開啟的**狀態和報告**視窗，選取**Kaspersky 應用程式**區段。
   這會開啟安裝在裝置上的 Kaspersky 應用程式清單。
4. 在應用程式清單中，選取 Kaspersky Endpoint Security for Windows。
   適用於 Kaspersky Endpoint Security for Windows 遠端診斷選項的清單隨即顯示。

5. 在清單的**Xperf 偵錯**區段中，點擊**啟用 Xperf 偵錯**。
   若已啟用 Xperf 偵錯，則會改為顯示**停用 Xperf 偵錯**按鈕。

6. 在開啟的**變更 Xperf 偵錯等級**視窗，根據技術支援專員的要求執行以下動作：

   a. 選取以下其中一個偵錯等級：

   - **輕度等級**

     該類型的偵錯檔案包含系統最少量資訊。
     預設情況下已選定此選項。

   - **深度等級**

     相比於*輕度*類型的偵錯檔案，該類型的偵錯檔案包含更多詳細資訊，且可能在*輕度*類型偵錯檔案不足以評估效能時被技術支援專家需求。*深度*偵錯檔案包含關於系統的硬體、作業系統、應用程式的啟動和結束處理程序清單、用於效能評估的事件和來自 Windows System Assessment 工具的事件的技術資訊。

   b. 選取以下其中一個 Xperf 偵錯類型：

   - **基本類型**

     偵錯資訊在 Kaspersky Endpoint Security 應用程式執行期間被接收。
     預設情況下已選定此選項。

   - **重新啟動時類型**

     偵錯資訊在作業系統從受管理裝置上啟動時接收。該偵錯類型在影響系統效能的問題發生時，在裝置被開啟後和 Kaspersky Endpoint Security 啟動之前有效。

   系統可能要求您啟用**循環檔案大小 (MB)**選項，以防止偵錯檔案的過量增長。然後指定偵錯檔案的最大大小。當檔案達到最大大小時，最舊的偵錯資訊被新資訊覆蓋。

   c. 定義輪換檔案大小。

   d. 點擊**儲存**。

系統會啟用並設定 Xperf 偵錯。

停用 Xperf 偵錯：

1. 開啟用戶端裝置的遠端診斷視窗。

2. 在遠端診斷視窗，點擊**遠端診斷**。

3. 在開啟的**狀態和報告**視窗，選取**Kaspersky 應用程式**區段。
   這會開啟安裝在裝置上的 Kaspersky 應用程式清單。

4. 在應用程式清單中，選取 Kaspersky Endpoint Security for Windows。
   適用於 Kaspersky Endpoint Security for Windows 的偵錯選項隨即顯示。
5. 在清單的**Xperf 偵錯**區段中，點擊**停用 Xperf 偵錯**。
   若已停用 Xperf 偵錯，則會改為顯示**啟用 Xperf 偵錯**按鈕。

Xperf 偵錯已停用。

下載應用程式偵錯檔案

要下載應用程式的偵錯檔案：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗，點擊**遠端診斷**。
3. 在開啟的**狀態和報告**視窗，選取**Kaspersky 應用程式**區段。
   這會開啟安裝在裝置上的 Kaspersky 應用程式清單。
   在**偵錯**部分中，點擊**偵錯檔案**按鈕。
   這會開啟**裝置偵錯記錄**，其中會顯示偵錯檔案清單。
4. 在偵錯檔案清單中，選取您要的檔案。
5. 執行以下操作之一：
   - 點擊**下載整個檔案**來下載所選檔案。
   - 下載部分選取的檔案：
     a. 點擊**下載一部分**。
     b. 在開啟的視窗中，根據您的需求指定要下載的名稱與檔案部分。
     c. 點擊**下載**。

選取的檔案或其部分會下載至您指定的位置。

刪除偵錯檔案

您可刪除不再需要的偵錯檔案。

若要刪除偵錯檔案：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在開啟的遠端診斷視窗中，請點擊**遠端診斷**。
3. 在開啟的**狀態和報告**視窗中，確保已選取**作業系統記錄**區段。

4. 在**偵錯檔案**區段中，點擊**Windows Update 記錄**按鈕或**遠端安裝記錄**按鈕，視您要刪除的偵錯檔案而定。這會開啟偵錯檔案清單。
5. 在偵錯檔案清單中，選取您要刪除的檔案。
6. 點擊**刪除**按鈕。

選取的偵錯檔案已刪除。

下載應用程式設定

從用戶端裝置下載應用程式設定：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在開啟的遠端診斷視窗中，請點擊**遠端診斷**。
3. 在開啟的**狀態和報告**視窗中，確保已在右窗格中選取**作業系統記錄**。
   - 在**系統資訊**區段中，點擊**下載檔案**按鈕以下載有關用戶端裝置的系統資訊。
   - 在**應用程式設定**區段中點擊**下載檔案**按鈕，下載裝置上已安裝應用程式設定的資訊。

系統會將該資訊作為檔案下載至您指定的地點。

下載事件記錄

要從遠端裝置下載事件記錄：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗，點擊**裝置記錄**。
3. 在**所有裝置記錄**視窗中，選取相關記錄。
4. 執行以下操作之一：
   - 點擊**下載整個檔案**來下載所選日誌。
   - 下載部分選取的記錄：
     a. 點擊**下載一部分**。
     b. 在開啟的視窗中，根據您的需求指定要下載的名稱與檔案部分。
     c. 點擊**下載**。

選取的事件記錄或其部分，會下載至您指定的位置。

啟動、停止、重新啟動應用程式

您可在用戶端裝置啟動、停止、重新啟動應用程式。

若要啟動、停止和重新啟動應用程式，請執行以下操作：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗，點擊**遠端診斷**。
3. 在開啟的**狀態和報告**視窗，選取**Kaspersky 應用程式**區段。
   這會開啟安裝在裝置上的 Kaspersky 應用程式清單。
4. 在應用程式清單中，選取您要啟動、停止或重新啟動的應用程式。
5. 點擊以下其中一個按鈕以選取動作：

   - **停止應用程式**
     此按鈕僅在應用程式正在執行時可供使用。
   - **重新啟動應用程式**
     此按鈕僅在應用程式正在執行時可供使用。
   - **啟動應用程式**
     此按鈕僅在應用程式不是正在執行時可供使用。

   視您選取的動作而定，系統會啟動、停止或重新啟動應用程式。

若您重新啟動網路代理，系統會顯示訊息表示將失去裝置對管理伺服器的目前連線。

執行卡巴斯基安全管理中心網路代理的遠端診斷並下載結果

若要在遠端裝置上啟動卡巴斯基安全管理中心網路代理的診斷並下載結果：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗，點擊**遠端診斷**。
3. 在開啟的**狀態和報告**視窗，選取**Kaspersky 應用程式**區段。
   這會開啟安裝在裝置上的 Kaspersky 應用程式清單。
4. 在應用程式清單中，選擇**卡巴斯基安全管理中心網路代理**。
   遠端診斷選項清單隨即顯示。

5. 在該清單的**診斷報告**區段中，點擊**執行診斷**按鈕。

   這會啟動遠端診斷程序並產生診斷報告。診斷程序完成時，您就能使用**下載診斷報告**按鈕。

6. 點擊**下載診斷報告**按鈕來下載報告。

該報告會下載至您指定的位置。

在用戶端裝置執行應用程式

您可能需要在用戶端裝置上執行應用程式，若卡巴斯基支援專家要求這樣做。

您無需在該裝置上安裝該應用程式。

若要在用戶端裝置上執行應用程式：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在開啟的遠端診斷視窗中，請點擊**遠端診斷**。
3. 在開啟的**狀態和報告**視窗，選取**執行遠端應用程式**區段。
4. 在**執行遠端應用程式**視窗中的**應用程式檔案**區段，根據 Kaspersky 專員的要求，執行以下其中一個動作：
   - 點擊**瀏覽**按鈕以對您要在用戶端裝置上執行的應用程式選取 ZIP 封存。

     > ZIP 封存必須包含公用程式資料夾。此資料夾包含要在遠端裝置上執行的可執行檔。

   - 如有需要，請指定命令行應用程式與其引數。為此，請填寫**要在遠端裝置上執行的封存中的可執行檔**和**命令列參數**欄位。
5. 點擊**上傳和執行**按鈕以在用戶端裝置上執行指定的應用程式。
6. 請遵循專家的指示。

為應用程式建立記憶體傾印檔案

應用程式傾印檔案允許您檢視某個時間點在用戶端裝置上執行的應用程式的參數。該檔案還包含有關為應用程式加載的模組的資訊。

> 不支援來自 Linux 裝置的傾印收集。

若要透過遠端診斷收集傾印，請使用 kldumper 公用程式。該公用程式旨在應技術支援專家的要求收集卡巴斯基應用程式處理程序的傾印。卡巴斯基安全管理中心知識庫中提供了有關使用 kldumper 公用程式的要求的詳細資訊。

要為應用程式建立傾印檔案：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在開啟的遠端診斷視窗中，請點擊**開啟**按鈕。
3. 在開啟的**狀態和報告**視窗，選取**執行遠端應用程式**區段。
4. 在**正在產生處理程序記憶體傾印檔案**區域中，指定要為其產生傾印檔案的應用程式的可執行檔。
5. 點選**下載傾印檔案**按鈕。

   包含指定應用程式的傾印檔案的存檔被下載。

   如果指定的應用程式未在用戶端裝置上執行，則下載的存檔中包含的「結果」資料夾將為空。

   如果指定的應用程式正在執行，但下載失敗並出現錯誤，或下載的存檔中包含的「結果」資料夾為空，請參閱卡巴斯基安全管理中心知識庫。

變更卡巴斯基安全管理中心網頁主控台介面的語言

您可以選擇卡巴斯基安全管理中心網頁主控台介面的語言。

要變更介面語言：

1. 在主功能表中，轉到您的帳戶設定，然後選擇**語言**。
2. 選擇一種受支援的當地語係化語言。

API 參考手冊

本《卡巴斯基安全管理中心 OpenAPI 參考手冊》旨在協助完成以下工作：

- 自動化和客製化。您可以 自動化您可能不想使用管理主控台手動處理的工作。您還可以實作管理主控台中尚不支援的自訂方案。例如，作為管理員，您可以使用卡巴斯基安全管理中心 OpenAPI 建立和執行指令碼，這些指令碼將有助於開發管理群組的結構並使該結構保持在最新狀態。

- 自訂開發。例如，您可以為客戶開發一個替代的 MMC 管理主控台，該主控台允許執行一組有限的操作。

在《OpenAPI 參考手冊》中，您可以使用螢幕右側的搜尋欄位找出您所需的資訊。

OPENAPI 參考手冊

指令碼範例

OpenAPI 參考指南包含下表中列出的 Python 指令碼範例。這些範例展示如何調用 OpenAPI 方法並自動完成各種網路防護工作，例如，建立一個"主要/從屬"階層結構，在卡巴斯基安全管理中心中執行工作，或分配發佈點。您可以按原樣執行範例，也可以根據範例建立自己的指令碼。

要調用 OpenAPI 方法並執行指令碼：

1. 下載 KlAkOAPI.tar.gz 存檔。此存檔包括 KlAkOAPI 套件和範例（您可以從存檔或 OpenAPI 參考指南中復制它們）。KlAkOAPI.tar.gz 存檔也位於卡巴斯基安全管理中心安裝資料夾中。

2. 從安裝了管理伺服器的裝置上的 KlAkOAPI.tar.gz 存檔安裝 KlAkOAPI 套件。

   您只能在安裝了管理伺服器和 KlAkOAPI 套件的裝置上調用 OpenAPI 方法、執行範例和您自己的指令碼。

符合使用者方案和卡巴斯基安全管理中心 OpenAPI 方法的樣本

樣本	樣本目的	情景
記錄 KlAkParams	您可以使用 `KlAkParams` 資料結構來擷取與處理資料。該範例顯示如何使用此資料結構。 範例輸出可以以不同的方式呈現。您可以取得資料來傳送 HTTP 方法或在您的程式碼中使用它。	監控和報告
建立和刪除"主要/從屬"層級結構	您可以新增次要管理伺服器，進而建立「主要 / 次要」層級。或者，您可以中斷次要管理伺服器與層級結構的連線。	• 建立管理伺服器階層：新增次要管理伺服器 • 刪除管理伺服器階層
根據 Active Directory 單位結構建立群組階層結構	您可以輪詢 Active Directory 單位結構並形成已發現之裝置群組的層次結構。	建立管理群組
根據快取的 Active Directory 單位結構建立群組階層結構	您可以根據之前輪詢的 Active Directory 單位結構形成受管理裝置群組的階層結構。如果新裝置在上次輪詢後出現在 Active Directory 中，則不會將它們新增到群組中，因為它們不在儲存的輪詢結果中。	建立管理群組
透過連線閘道下載網路清單檔案到指定裝置	您可以透過使用連線閘道連線到所需裝置的網路代理，然後將包含網路清單的檔案下載到您的裝置。	發佈點和連線閘道器的調整
將儲存在主管理伺服器儲存區中的產品授權金鑰安裝到從屬管理伺服器上	您可以連線到主管理伺服器，從其下載所需的產品授權金鑰，然後將此金鑰傳輸到層次結構中包含的所有從屬管理伺服器。	受管理應用程式的產品授權
建立有效的使用者權限報告	您可以建立不同的報告。例如，您可以使用此範例產生有效的使用者權限報告。此報告描述了使用者擁有的權限，具體取決於他或她的群組和角色而定。 您可以下載 HTML、PDF 或 Excel 格式的報告。	生成和瀏覽報告
為裝置啟動工作	您可以透過使用連線閘道連線到所需裝置上的網路代理，然後執行必要的工作。	手動啟動工作
根據 Active Directory 站點和服務建立 IP 子網路	您可以根據您使用的 Active Directory 單位結構建立 IP 子遮罩。 該範例啟動對指定 IP 範圍的輪詢並刪除發現的子遮罩，以避免它們與新子遮罩發生衝突。因此，請勿在需要保留子遮罩的網路中執行此範例。 輪詢後，範例會參考 Active Directory，檢查其中的每個裝置，並建立 IP 子遮罩。為此，範例會使用所有裝置的遮罩和 IP 位址。	配置網路防護
為群組中的裝置註冊分發點	您可以將受管理裝置分配為發佈點（以前稱為更新代理）。	更新 Kaspersky 資料庫和應用程式
列舉所有群組	您可以對管理群組採取以下操作。該範例顯示如何執行以下操作： • 取得「受管理裝置」根群組的識別碼 • 在群組階層結構中移動 • 獲取完整的、擴展的群組階層結構及其名稱和嵌套	設定管理伺服器

樣本	樣本目的	情景
列舉工作、查詢工作統計並執行工作	您可以找到以下資訊： • 工作進度記錄 • 目前工作狀態 • 不同狀態的工作數量 您還可以執行工作。預設情況下，範例會在輸出統計資訊後執行工作。	監視工作執行
建立並執行工作	您可以建立工作。在範例中指定以下工作參數： • 類型 • 執行方法 • 名稱 • 將使用工作的裝置群組 預設情況下，範例會建立一個「顯示訊息」類型的工作。您可以為管理伺服器的所有受管理裝置執行此工作。如有需要，您可以指定自己的工作參數。	建立工作
列舉產品授權金鑰	您可以獲得安裝在管理伺服器受管理裝置上之卡巴斯基應用程式的所有啟動產品授權金鑰的清單。該清單包含關於每個產品授權金鑰的詳細資料，例如名稱、類型或到期日期。	檢視使用中產品授權金鑰的相關資訊
建立與尋找內部使用者	您可以建立一個帳戶以進行進一步的工作。	選取帳戶以啟動管理伺服器
建立一個自訂類別	您可以根據需要建立應用程式類別參數。	建立含有手動新增內容的應用程式類別
使用 SrvView 列舉使用者	您可以使用 SrvView 類別請求獲得管理伺服器的詳細資料。例如，您可以使用此範例取得使用者清單。	管理使用者帳戶

透過 OpenAPI 與卡巴斯基安全管理中心互動的應用程式

一些應用程式透過 OpenAPI 與卡巴斯基安全管理中心互動。例如，此類應用程式包括 Kaspersky Anti Targeted Attack Platform 或 Kaspersky Security for Virtualization。這也可以是您基於 OpenAPI 開發的自訂用戶端應用程式。

透過 OpenAPI 與卡巴斯基安全管理中心互動的應用程式連線至管理伺服器。如果您配置了一個連線至管理伺服器的 IP 位址允許清單，請新增安裝了使用卡巴斯基安全管理中心 OpenAPI 的應用程式的裝置的 IP 位址。要了解您使用的應用程式是否透過 OpenAPI 工作，請參閱此應用程式的說明。

服務供應商最佳實踐

該區域提供有關如何配置和使用卡巴斯基安全管理中心的資訊。

該區域包含如何佈署、配置和使用應用程式的建議，敘述了解決應用程式操作中的典型問題的方法。

排程卡巴斯基安全管理中心佈署

當在組織網路中排程卡巴斯基安全管理中心元件的佈署時，您必須考慮到項目的大小和範圍，尤其是以下因素：

- 裝置總數
- MSP 用戶端數量

一個管理伺服器可以支援最多 100,000 台裝置。如果組織網路中的裝置總數超過 100,000，必須在服務提供者端佈署多個管理伺服器，併合並到一個方便集中管理的層級。

500 台虛擬伺服器可以被建立在單一管理伺服器，因此每 500 台 MSP 用戶端需要一個單一管理伺服器。

在佈署排程階段，必須考慮到特別憑證 X.509 到管理伺服器的分配。X.509 憑證到管理伺服器的分配可能用在以下情況（部分清單）：

- 透過 SSL 終端代理檢查安全通訊端層 (SSL) 流量
- 在憑證欄位中指定所需值
- 提供所需的憑證加密長度

提供到管理伺服器的網際網路存取

要允許用戶端網路裝置透過網際網路存取管理伺服器，您必須啟用以下管理伺服器連接埠：

- 13000 TCP—管理伺服器 TLS 連接埠，用於連線佈署在用戶端網路的網路代理
- 8061 TCP—HTTPS 連接埠，用於使用管理主控台工具發佈獨立安裝套件
- 8060 TCP—HTTP 連接埠，用於使用管理主控台工具發佈獨立安裝套件
- 13292 TCP—TLS 連接埠，僅在有需要被管理的行動裝置時需要

如果您需要提供用戶端透過卡巴斯基安全管理中心 網頁主控台進行網路管理的基本選項，您也必須開啟卡巴斯基安全管理中心網頁主控台連接埠 8080 TCP（HTTPS 連接埠）。

卡巴斯基安全管理中心標準設定

一個或幾個管理伺服器被佈署到 MSP 伺服器。管理伺服器數量可以基於可用硬體、服務的 MSP 用戶端總數或受管理裝置總數來選取。

一個管理伺服器可以支援最多 100,000 台裝置。您必須考慮今後增加受管理裝置的數量的可能性：最好連線較少裝置到單一管理伺服器。

500 台虛擬伺服器可以被建立在單一管理伺服器，因此每 500 台 MSP 用戶端需要一個單一管理伺服器。

如果使用了多個伺服器，建議您合併它們到一個層級。使用管理伺服器階層允許您避免冗餘政策和工作、處理整個受管理裝置，使它們看起來是被單一管理伺服器管理：例如，搜尋裝置、建立裝置分類和建立報告。

在每個對應於 MSP 用戶端的虛擬伺服器上，您必須分配一個或幾個發佈點。如果 MSP 用戶端和管理伺服器透過網際網路連線，最好為發佈點建立*將更新下載至發佈點儲存區*工作，這樣它們將從 Kaspersky 伺服器直接下載更新，而不是從管理伺服器。

如果 MSP 用戶端網路的一些裝置不能直接存取網際網路，您必須切換發佈點到連線閘道模式。此種情況下，MSP 用戶端網路裝置上的網路代理將被透過閘道而不是直接連線到管理伺服器，為了後期同步。

作為管理伺服器，很可能無法輪詢 MSP 用戶端網路，最好把該功能轉給發佈點。

管理伺服器將無法傳送通知到 MSP 用戶端網路 NAT 以外的受管理裝置的連接埠 15000 UDP。要解決該問題，最好在作為發佈點並執行在連線閘道模式的裝置的內容中啟用持續連線到管理伺服器模式（**不斷開與管理伺服器的連線**核取方塊）。如果發佈點總數不超過 300 則持續連線模式可用。

關於發佈點

網路代理裝置可以用作發佈點。在該模式中，網路代理可以執行以下功能：

- 傳輸檔案到用戶端裝置，包括：
  - Kaspersky 資料庫和軟體模組更新

    更新可以從管理伺服器獲取，或者從 Kaspersky 更新伺服器獲取。在後一種情況下，"*將更新下載到發佈點儲存區*"工作必須為作為發佈點的裝置建立。
  - 協力廠商軟體更新
  - 安裝套件
  - 將管理伺服器作為 WSUS 伺服器使用時的 Windows 更新
- 安裝軟體（包括網路代理初始化佈署）到其他裝置。
- 輪詢網路以偵測新裝置並更新現有裝置的資訊。發佈點套用與管理伺服器相同的裝置發現方法。

在組織網路中佈署發佈點可以帶來以下好處：

- 使用管理伺服器作為更新來源，則降低其負載。
- 如果 MSP 用戶端網路的每個裝置都沒有必要存取 Kaspersky 伺服器或管理伺服器以更新，則最佳化網際網路流量。
- 提供管理伺服器到 MSP 用戶端網路 NAT 之外的存取（與管理伺服器相關），這允許管理伺服器執行以下操作：
  - 在 IPv4 或 IPv6 網路上透過 UDP 傳送通知到裝置
  - 輪詢 IPv4 或 Ipv6 網路
  - 執行初始化佈署
  - 作為推送伺服器使用

為每個管理群組分配發佈點。此種情況下，發佈點的範圍包括管理群組和其所有子群組中的所有裝置。然而，作為發佈點的裝置不必須包含在它被分配的管理群組。

您可以讓發佈點作為連線閘道工作。此種情況下，發佈點範圍內的裝置將被透過閘道，而不是直接連線到管理伺服器。該模式用在不允許在網路代理和管理伺服器裝置之間建立直接連線的情景。

作為發佈點的裝置必須被防護，包括實體防護，以防範非授權的存取。

管理伺服器階層

一個 MSP 可能執行多個管理伺服器。可能不方便管理幾個不同的管理伺服器，因此可以應用階層結構。兩個管理伺服器的"主要/從屬"組態提供了以下選項：

- 一個從屬管理伺服器從主管理伺服器繼承政策和工作，這防止了重複設定。
- 主管理伺服器上的裝置分類可以包含從屬管理伺服器的裝置。
- 主管理伺服器的報告可以包含從屬管理伺服器的資料（包括詳細資訊）。

主管理伺服器僅會從上列選項範圍內的非虛擬從屬管理伺服器收到資料。此限制之所以不適用於虛擬管理伺服器，是因為虛擬管理伺服器與其主管理伺服器共用一個資料庫。

虛擬管理伺服器

基於實體管理伺服器，可以建立多個虛擬管理伺服器，它們與從屬管理伺服器相似。相比於基於存取控制清單 (ACLs) 的任意存取模式，虛擬管理伺服器模式功能更強大並且提供更高度隔離。除了適用於含政策與工作的已配置裝置的管理群組專屬結構外，各虛擬伺服器會具備其自己未配置的裝置的群組、自己的報告集、選取的裝置和事件、安裝套件、移動規則等。為了最大限度地實現 MSP 用戶端的相互隔離，我們建議您選擇虛擬管理伺服器作為要使用的功能。而且，為每個 MSP 用戶端建立虛擬管理伺服器允許您提供用戶端透過卡巴斯基安全管理中心 網頁主控台的網路管理的基本選項。

虛擬管理伺服器與從屬管理伺服器非常相似，但是有以下不同點：

- 虛擬管理伺服器缺少多數全域設定和自己的 TCP 連接埠。
- 虛擬管理伺服器沒有從屬管理伺服器。
- 虛擬管理伺服器沒有其他虛擬管理伺服器。
- 實體管理伺服器可以檢視它所有虛擬管理伺服器的裝置、群組、事件和受管理裝置上的物件（隔離區項目、應用程式登錄資料等等）。
- 虛擬管理伺服器僅可以掃描連線了發佈點的網路。

使用 Kaspersky Endpoint Security for Android 管理行動裝置

安裝了 Kaspersky Endpoint Security for Android™ 的行動裝置（也叫 KES 裝置）透過管理伺服器管理。卡巴斯基安全管理中心支援以下管理 KES 裝置的功能：

- 將行動裝置處理為用戶端裝置：
  - 管理群組中的成員關係
  - 監控，例如檢視狀態、事件和報告
  - 修改本機設定和為 Kaspersky Endpoint Security for Android 分配政策
- 以集中模式傳送指令
- 遠端安裝行動應用程式套件

管理伺服器透過 TLS、TCP 連接埠 13292 管理 KES 裝置。

佈署和初始化設定

卡巴斯基安全管理中心是一個分發的應用程式。卡巴斯基安全管理中心包含以下應用程式：

- 管理伺服器 — 核心元件，設計用於管理組織裝置和在 DBMS 中整理資料。
- 管理主控台 — 管理員基本工具。管理主控台與管理伺服器一起出貨，但是它也可以被單獨安裝在一個或幾個由管理員執行的裝置上。
- 卡巴斯基安全管理中心 網頁主控台 — 設計用於基本操作的管理伺服器 Web 介面。您可以安裝該元件到滿足硬體和軟體需求的裝置。
- 網路代理 — 設計用於管理安裝在裝置上的安全應用程式，同時取得裝置資訊。網路代理安裝在組織裝置上。

卡巴斯基安全管理中心在組織網路上的佈署執行如下：

- 管理伺服器的安裝
- 卡巴斯基安全管理中心 網頁主控台的安裝
- 管理員裝置上管理主控台的安裝
- 網路代理和企業裝置上安全應用程式的安裝

管理伺服器安裝建議

該部分包含了如何安裝管理伺服器的建議。該部分還提供了使用管理伺服器上的共用資料夾以便佈署網路代理到用戶端裝置的情境。

在失敗轉移叢集上為管理伺服器服務建立帳戶

預設下，安裝程式自動為管理伺服器服務建立非特權帳戶。該行為對於在一般裝置上安裝管理伺服器來說是最方便的。

然而，在失敗轉移的叢集上安裝管理伺服器需要不同的方案：

1. 為管理伺服器服務建立非特權網域帳戶，並把它們作為以 KLAdmins 為名稱的全域網域安全群組的成員。
2. 在管理伺服器安裝程式中，指定為服務建立的網域帳戶。

選取 DBMS

當選取管理伺服器使用的資料庫管理系統 (DBMS) 時，您必須考慮到被管理伺服器覆寫的裝置數量。

下表列出了有效 DBMS 選項，以及對它們使用的建議和限制。

對 DBMS 的建議和限制

DBMS	建議和限制
SQL Server Express Edition 2012 或後續版本	如果您打算為少於 10,000 台裝置執行單個管理伺服器，請使用此 DBMS。 建議停用軟體清查工作並停用（在 Kaspersky Endpoint Security 政策設定中）管理伺服器對已啟動應用程序的通知。 您可以限制事件儲存庫中事件的最大數量，以防止資料庫外溢。 有關詳細資訊，請參閱以下主題：資料庫空間的計算。 SQL Server Express Edition DBMS 被管理伺服器和其他應用程式同時使用是被嚴格禁止的。 **執行 Windows Update 同步**工作不支援 Microsoft SQL Express 資料庫。
本機 SQL Server 版本，而不是 Express 2014 或後續版本	沒有限制。
遠端 SQL Server 版本，而不是 Express 2014 或後續版本	僅在兩台裝置都在相同 Windows® 網域中時可用；如果網域不同，必須在它們之間建立雙向信任關係。

DBMS	建議和限制
本機或遠端 MySQL 5.5、5.6 或 5.7（MySQL 版本 5.5.1、5.5.2、5.5.3、5.5.4 和 5.5.5 不再被支援）。	如果您打算為少於 10,000 台裝置執行單個管理伺服器，請使用此 DBMS。 建議停用軟體清查工作並停用（在 Kaspersky Endpoint Security 政策設定中）管理伺服器對已啟動應用程序的通知。有關詳細資訊，請參閱以下主題：資料庫空間的計算。
本機或遠端 MySQL 8.0.20 或更新版本	如果您打算為少於 50,000 台裝置執行單個管理伺服器，請使用此 DBMS。 建議停用軟體清查工作並停用（在 Kaspersky Endpoint Security 政策設定中）管理伺服器對已啟動應用程序的通知。有關詳細資訊，請參閱以下主題：資料庫空間的計算。
本機或遠端 MariaDB（參見受支援的版本）	如果您打算為少於 20,000 台裝置執行單個管理伺服器，請使用此 DBMS。 建議停用軟體清查工作並停用（在 Kaspersky Endpoint Security 政策設定中）管理伺服器對已啟動應用程序的通知。有關詳細資訊，請參閱以下主題：資料庫空間的計算。
PostgreSQL、Postgres Pro（查看支援的版本）	如果您打算為少於 50,000 台裝置執行單個管理伺服器，請使這些 DBMS 之一。 建議停用軟體清查工作並停用（在 Kaspersky Endpoint Security 政策設定中）管理伺服器對已啟動應用程序的通知。有關詳細資訊，請參閱以下主題：資料庫空間的計算。

如果您使用 PostgreSQL、MariaDB 或 MySQL DBMS，**事件**頁簽可能會顯示所選用戶端裝置的不完整事件清單。當 DBMS 儲存大量事件時，就會發生這種情況。您可以執行下列任一操作來增加顯示的事件數目：

- 刪除不必要的事件。
- 減少不必要事件的儲存期限。

若要查看裝置的管理伺服器上記錄的事件的完整清單，請使用報告。

若您使用 SQL Server 2019 作為 DBMS，且沒有累積修補 CU12 或更新版本，您必須在安裝卡巴斯基安全管理中心後執行以下項目：

1. 使用 SQL Management Studio 連線至 SQL Server。
2. 請執行以下指令 (若您為資料庫選擇不同名稱，請使用開名稱而非 KAV)：

```
USE KAV
GO
ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
GO
```

3. 請重新啟動 SQL Server 2019 服務。

否則，使用 SQL Server 2019 可能造成錯誤，例如「資源集區『內部』的系統記憶體不足，無法執行此查詢。」

指定管理伺服器位址

當安裝管理伺服器時，您必須指定管理伺服器外部位址。該位址將用作建立網路代理安裝套件時的預設位址。此後，您將可以透過使用管理主控台工具變更管理伺服器主機位址；位址將不會在所建立的網路代理安裝套件中自動變更。

在用戶端組織網路中設定防護

管理伺服器安裝完成後，管理主控台啟動並提示您透過相關精靈執行初始化設定。當快速設定精靈執行時，以下政策和工作在根管理群組中被建立：

- Kaspersky Endpoint Security 政策
- 更新 Kaspersky Endpoint Security 的群組工作
- 掃描 Kaspersky Endpoint Security 裝置的群組工作
- 網路代理政策
- 弱點掃描工作（網路代理工作）
- 更新安裝和弱點修復工作（網路代理工作）

政策和工作使用預設設定建立，這對組織來說可能是不佳的或不合理的。因此，您必須檢查所建立物件的內容並在必要時手動修改它們。

此部分包含有關手動配置政策、工作和其他管理伺服器設定的資訊，以及發佈點、構建管理群組結構和工作層次結構以及其他設定的資訊。

Kaspersky Endpoint Security 政策的手動設定

該部分提供了如何配置 Kaspersky Endpoint Security 政策的建議，該政策由快速設定精靈建立。您可以在政策屬性窗口中執行設置。

當編輯設定時，請記住您必須點擊相關設定之上的鎖圖示以便允許在工作站上使用該值。

在進階威脅防護區域配置政策

對於該區域設定的完整敘述，請參考 Kaspersky Endpoint Security for Windows 文件。

在**進階威脅防護**區域中，您可設定 Kaspersky Endpoint Security for Windows 如何使用卡巴斯基安全網路。您也可設定 Kaspersky Endpoint Security for Windows 模組，例如行為偵測、弱點利用防禦、主機入侵防禦和補救引擎。

在**卡巴斯基安全網路**子區域，建議您啟用使用**卡巴斯基安全網路**選項。使用該功能有助於重新分發和最佳化網路流量。如果**卡巴斯基安全網路**選項已停用，您可以啟用直接使用 KSN 伺服器。

在關鍵威脅防護部分配置政策

對於該區域設定的完整敘述，請參考 Kaspersky Endpoint Security for Windows 文件。

在政策內容視窗的**關鍵威脅防護**區段，我們建議您在**防火牆**和**檔案威脅防護**子區段中指定額外設定。

防火牆子區段包含的設定可讓您控制用戶端裝置上應用程式的網路活動。用戶端裝置使用指派了以下狀態之一的網路：公用、本機或受信任。根據網路狀態，Kaspersky Endpoint Security 可以允許或拒絕裝置上的網路活動。將新網路新增至您的組織時，您必須為其指派適當的網路狀態。例如，如果用戶端裝置是筆記型電腦，我們建議此裝置使用公用或受信任的網路，因為筆記型電腦不一定永遠都連線到本機網路。在**防火牆**子區段，您可以檢查是否正確將狀態指派給組織中使用的網路。

要檢視網路清單：

1. 在政策內容中，前往**關鍵威脅防護 → 防火牆**。
2. 在**可用網路**區域中，按一下**設定**按鈕。
3. 在開啟的**防火牆**視窗中，前往**網路**頁籤檢視網路清單。

在**檔案威脅防護**子區段中，您可以停用網路磁碟機掃描。掃描網路磁碟機會顯著提高網路磁碟機負載。在檔案伺服器上執行間接掃描更方便。

要停用網路磁碟機掃描：

1. 在政策內容中，前往**關鍵威脅防護 → 檔案威脅防護**。
2. 在**安全等級**區域中，按一下**設定**按鈕。
3. 在開啟的**檔案威脅防護**視窗中，在**一般**頁籤，清空**所有網路磁碟機**核取方塊。

在一般設定部分配置政策

對於該區域設定的完整敘述，請參考 Kaspersky Endpoint Security for Windows 文件。

在政策內容視窗的**一般設定**區段中，我們建議在**報告和儲存**和**介面**子區段中指定額外設定。

在**報告和儲存**子區段中，前往**到管理伺服器的資料傳輸**區段。**關於已啟動的應用程式**核取方塊指定管理伺服器資料庫是否儲存網路裝置上所有軟體模組的所有版本資訊。如果選取此核取方塊，所儲存的資訊可能需要使用卡巴斯基安全管理中心資料庫上的大量磁碟空間（數十 GB）。如果在最上層政策中選取了**關於已啟動的應用程式**核取方塊，請取消勾選。

如果管理主控台以集中模式管理組織網路上的威脅防護，請停用工作站上 Kaspersky Endpoint Security for Windows 使用者介面的顯示。為此，在**介面**子區段中，前往**使用者互動**區段，然後勾選**不顯示使用者介面**選項。

如要在工作站上啟用密碼防護，請在**介面**子區段中，前往**密碼防護**區段，點擊**設定**按鈕，然後選取**啟用密碼防護**核取方塊。

在事件配置區域配置政策

在**事件配置**區域，您應該停用儲存任何事件到管理伺服器，除了以下事件：

- 在**緊急**頁籤：
  - *應用程式自動執行已停用*
  - *存取被拒絕*
  - *已禁止應用程式啟動*
  - *無法解毒*
  - *違反了最終使用者產品授權協議*
  - *無法載入加密模組*
  - *不能同時執行兩項工作*
  - *偵測到活動威脅。應該啟動進階解毒技術*
  - *偵測到網路攻擊*
  - *未更新所有元件*
  - *啟動錯誤*
  - *啟用攜帶模式時出錯*
  - *與卡巴斯基安全管理中心互動時發生錯誤*
  - *停用攜帶模式時出錯*
  - *變更應用程式元件時出錯*
  - *套用檔案加密/解密規則時出錯*
  - *無法套用政策*
  - *處理程序已終止*
  - *網路活動已封鎖*
- 在**功能失效**頁籤上：*工作設定無效，未套用設定*

- 在**警告**頁籤：
  - *自我防護被停用*
  - *備用金鑰不正確*
  - *使用者選擇了結束加密政策*
- 在**資訊**頁籤：*禁止應用程式在測試模式下啟動*

Kaspersky Endpoint Security 更新群組工作的手動設定

如果管理伺服器作為更新來源，Kaspersky Endpoint Security 的最優和建議排程選項是**當新更新下載至儲存區時**，其中**使用工作啟動自動隨機延遲**核取方塊被選擇。

如果從 Kaspersky 伺服器下載更新到儲存區的本機工作已在每個發佈點上建立，時段性排程將是最優的並被建議給 Kaspersky Endpoint Security 群組更新工作。此種情況下，隨機時段值應該被設定為 1 小時。

Kaspersky Endpoint Security 裝置掃描群組工作的手動設定

快速設定精靈建立掃描裝置的群組工作。預設下，工作被分配**在星期五下午 7:00 執行**排程，並且不選取**執行錯過的工作**核取方塊。

這意味著如果組織中的裝置在星期五關閉，例如在下午 6:30，裝置掃描工作將永遠不會被執行。您必須基於組織的工作規則為該工作設定最方便的排程。

排程「尋找弱點和所需更新」工作

快速設定精靈為網路代理建立*尋找弱點和所需更新*工作。預設下，工作被分配**在星期二下午 7:00 執行**排程，並且**執行略過的工作**核取方塊被選中。

如果組織的工作規則要在此時關閉所有裝置，*尋找弱點和所需更新*工作將在裝置再次開啟時執行，也就是，在星期三早晨。此活動可能不是必須的，因為弱點掃描可能增加 CPU 和磁碟子系統負載。您必須根據組織的工作規則為該工作設定最方便的排程。

更新安裝和弱點修復群組工作的手動設定

該快速設定精靈為網路代理建立更新安裝和弱點修復群組工作。預設下，工作被設定在每天 01:00 AM 執行，並且不會啟用**執行略過的工作**選項。

如果組織工作規則整夜關閉所有裝置，則更新安裝將永遠不會執行。您必須基於組織的工作規則為弱點掃描工作設定最方便的排程。值得注意的是，更新的安裝可能需要重新啟動裝置。

建立管理群組結構和分配發佈點

卡巴斯基安全管理中心中的管理群組結構執行以下功能：

- 設定政策範圍。

  套用相關設定到裝置有另一種方式，透過使用政策設定檔。在此情況下，政策範圍會用（例如）Active Directory 組織單元中的標籤、裝置裝置和Active Directory 安全群組中的成員關係進行設定。

- 設定群組工作範圍。

  還有一個不基於管理群組層級定義群組工作範圍的方法：使用裝置分類的工作和特定裝置的工作。

- 設定裝置、虛擬管理伺服器和次要管理伺服器的存取權限。

- 分配發佈點。

當建立管理群組結構時，您必須考慮到組織網路的拓撲以便最優分配發佈點。發佈點的最優分發允許您在企業網路中儲存流量。

根據組織圖表和 MSP 用戶端採用的網路拓撲，以下標準設定可以被套用到管理群組結構：

- 單一辦公室
- 多個小拆分辦公室

標準 MSP 用戶端設定：單一辦公室

在標準「單一辦公室」配置中，所有裝置都在組織網路上，因此它們能看見彼此。組織網路可能包含幾部分（網路或網段），由窄通道連線。

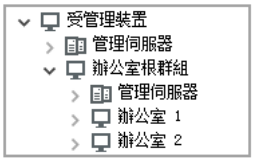
有以下構建管理群組結構的方法：

- 構建管理群組結構涉及到網路拓撲。管理群組結構可能不精確反映網路拓撲。網路各部分之間以及特定管理群組相互比對。您可以使用發佈點自動分配或手動分配它們。
- 不考慮網路拓撲而構建管理群組結構。此種情況下，您必須停用發佈點自動分配，然後為網路中每個部分的根管理群組分配一個或幾個裝置作為發佈點，例如為**受管理裝置**群組。所有發佈點將處於相同等級，並將掌控組織網路中所有裝置的相同範圍。此種情況下，每個網路代理將連線到具有最小路由的發佈點。發佈點的路由可以使用 tracert 實用程式偵錯。

標準 MSP 用戶端設定：多個小遠端辦公室

該標準配置用於一定數量的小遠端辦公室，它們可能透過網際網路與總部聯絡。每個遠端辦公室都位於 NAT 之外，就是說，從一個遠端辦公室到另一個遠端辦公室的連線是不可能的，因為辦公室是彼此隔離的。

配置必須在管理群組中體現：必須為每個遠端辦公室建立各自的管理群組（下圖中的群組**辦公室 1**和**辦公室 2**）。



遠端辦公室包含在管理群組結構

必須指定一個或多個發佈點給每個辦公室的對應管理群組。發佈點必須是遠端辦公室中具有足夠剩餘磁碟空間的裝置。佈署在**辦公室 1**群組的裝置，例如，將存取分配到**辦公室 1**管理群組的發佈點。

如果一些使用者在辦公室之間移動他們的攜帶式電腦，您必須在遠端辦公室選取兩個或更多裝置（除了現有的發佈點）並分配它們作為等級管理群組的發佈點（上圖中**辦公室根群組**）。

例如：攜帶式電腦佈署在**辦公室 1**管理群組，然後被移動到對應於**辦公室 2** 管理群組的辦公室。在移動攜帶式電腦後，網路代理試圖存取分配到**辦公室 1**群組的發佈點，但是那些發佈點不可用。然後，網路代理開始嘗試存取分配到**辦公室根群組**的發佈點。因為遠端辦公室是彼此隔離的，嘗試存取分配到**辦公室根群組**管理群組的發佈點僅在網路代理嘗試存取**辦公室 2** 群組中的發佈點時才會成功。就是說，攜帶式電腦將保持在原始辦公室對應的管理群組，但是將使用它當時所在辦公室的發佈點。

政策層級，使用政策設定檔

本章節提供關於如何套用政策到管理群組裝置的資訊。此外，還提供有關政策設定檔的資訊。

政策層級

在卡巴斯基安全管理中心，您使用政策來定義一個單一設定集到多個裝置。例如，應用程式 P 的政策範圍，為管理群組 G 定義，包含安裝了應用程式 P 的佈署在群組 G 和其子群組的受管理裝置，除了在內容中清空了**從父群組繼承**核取方塊的子群組。

政策透過設定旁邊的鎖頭圖示（🔒）不同於本機設定。如果一個設定（或設定群組）在政策內容中被鎖定，您必須首先在建立有效設定時使用該設定（或設定群組），其次，必須將設定或設定群組寫入 downstream 政策。

在裝置上建立有效設定可以如此敘述：所有未鎖定的設定值必須來自政策，然後被本機設定覆蓋，然後結果集被來自政策的鎖定設定的值覆蓋。

相同應用程式的政策透過管理群組層級互相影響：來自 upstream 政策的鎖定設定覆蓋來自 downstream 政策的相同設定。

漫遊使用者有特殊政策。該政策在裝置切換到漫遊模式時在裝置上生效。漫遊使用者的政策不透過管理群組層級影響其他政策。

政策設定檔

僅透過管理群組層級套用政策到裝置可能在許多環境下不方便。有必要建立單一政策的幾個實例，這些實例對於不同的管理群組在一兩個設定上有所不同，可以在將來同步這些政策的內容。

為了幫助您避免此類問題，卡巴斯基安全管理中心支援*政策設定檔*。政策設定檔是政策設定的命名子集。子集會連同政策一起分發至目標裝置，並根據名為*設定檔啟動條件*的特別條件來作為輔助政策。設定檔僅包含與「基本」政策不同的設定，並在用戶端裝置（電腦或行動裝置）上活動。啟動設定檔會變更設定檔啟動之前已在電腦上活動的政策設定。這些設定將使用已在設定檔中指定的值。

以下限制被施加在政策設定檔：

- 政策可以包含最多 100 個設定檔。
- 政策設定檔不能包含其他設定檔。
- 政策設定檔不能包含通知設定。

設定檔內容

政策設定檔包含以下組成部分：

- 名稱。帶有相同名稱的設定檔透過管理群組層級互相影響。
- 政策設定子集。不同於包含所有設定的政策，設定檔僅包含實際所需的設定（鎖定設定）。
- 啟動條件是裝置內容的邏輯表達。設定檔僅在設定檔啟動條件為真是活動（補充政策）。在其他所有情況，設定檔是非啟動和略過的。以下裝置內容可以被包含在邏輯表達：
  - 漫遊模式狀態。
  - 網路環境內容 – 用於網路代理連線的活動規則名稱。
  - 裝置上指定標籤的出現和消失。
  - 裝置在 Active Directory 組織單元 (OU) 上的分配：明確（裝置在指定 OU 中），或不明確（裝置是 OU，以嵌套級別包含在指定 OU）。
  - 裝置在 Active Directory 安全群組中的資格（明確或不明確）。
  - Active Directory 安全群組中裝置所有者的成員關係（明確或不明確）。
- 設定檔停用核取方塊。被停用的設定檔總是被略過，並且它們的啟動條件不被驗證。
- 設定檔優先順序。不同設定檔的啟動條件是獨立的，因此幾個設定檔可以一起啟動。如果活動設定檔包含設定的非重疊集合，將不會發生問題。然而，如果兩個活動設定檔包含不同的相同設定的值，將發生歧義。該歧義可以透過政策優先順序避免：歧義變數的值將來自高優先順序的設定檔（在設定檔清單中評級較高）。

政策透過層級互相影響時的設定檔行為

帶有相同名稱的設定檔根據政策合併規則合併到一起。upstream 政策的設定檔比 downstream 政策的設定檔擁有更高優先順序。如果編輯設定在 upstream 政策中被禁止（鎖定），downstream 政策使用 upstream 政策的設定檔啟動條件。如果編輯設定在 upstream 政策中被允許，downstream 政策的設定檔啟動條件被使用。

由於政策設定檔可能在啟動條件中包含**裝置已離線**內容，因此設定檔會完全取代漫遊使用者的政策功能，即此功能將不再受到支援。

漫遊使用者的政策可能包含設定檔，但是它們設定檔僅可以在裝置轉換到漫遊模式後啟動。

工作

卡巴斯基安全管理中心透過建立和執行*工作*來管理裝置上安裝的 Kaspersky 應用程式。安裝、啟用和停用應用程式、掃描檔案、更新病毒資料庫和軟體模組以及應用程式的其他行為均需要使用工作來完成。

特定應用程式的工作僅在安裝了該應用程式的管理外掛程式時可以被建立。

工作可以在管理伺服器和裝置上執行。

以下工作管理伺服器上執行：

- 自動發佈報告
- 將更新下載至管理伺服器儲存區
- 備份管理伺服器資料
- 資料庫維護
- Windows Update 同步
- 建立以一個作業系統 (OS) 映像為參照裝置的安裝套件

以下類型的工作在裝置上執行：

- *本機工作* — 在特定裝置上執行的工作。

  本機工作可以被管理員透過管理主控台工具修改，或者被遠端裝置使用者修改（例如，透過安全應用程式介面）。如果本機工作同時被管理員和受管理裝置使用者修改，管理員的修改將生效，因為其具有更高優先順序。

- *群組工作* — 在特定裝置上執行的工作。

  除非在工作內容中指定了其他項目，群組工作也影響所選群組的所有子群組。群組工作也影響（可選）佈署在其群組或子群組的連線到從屬和虛擬管理伺服器的裝置。

- *全域工作* — 選取指定裝置來執行的工作，與裝置屬於哪個管理群組無關。

您可以為每個應用程式建立任意數量群組工作、全域工作或本機工作。

您可以修改工作設定、檢視工作進度、複製、匯出、匯入和刪除工作。

只有當裝置上應用程式被執行，建立之工作才會執行。

工作結果會儲存在 Microsoft Windows 事件記錄和卡巴斯基安全管理中心的事件記錄中，這兩個記錄會集中儲存在管理伺服器上，以及本機儲存在每個裝置上。

請勿在工作設定中包含私密資料。例如，避免指定網域管理員密碼。

裝置移動規則

我們建議您自動分配裝置到虛擬伺服器上的對應於 MSP 用戶端的管理群組，使用*裝置移動規則*。裝置移動規則由三個主要部分組成：名稱、執行條件（裝置內容邏輯表達）和目的管理群組。如果裝置內容滿足規則執行條件，則規則移動裝置到目的管理群組。

所有裝置移動規則都有優先順序。管理伺服器檢查裝置內容以檢視它們是否滿足每條規則的執行條件（昇冪優先順序）。如果裝置內容滿足某條規則的執行條件，裝置被移動到目的群組，至此規則處理在該裝置上完成。如果裝置內容滿足多個規則的條件，裝置被移動到具有高優先順序的規則的目的群組。

裝置移動規則可以被間接建立。例如，在安裝套件或遠端安裝工作的內容中，您可以指定安裝網路代理後裝置必須被移動到的管理群組。而且，裝置移動規則可以被卡巴斯基安全管理中心管理員明確建立，在移動規則清單。清單位於管理主控台，在**未配置的裝置**群組內容中。

預設下，裝置移動規則用於裝置到管理群組的一次性初始分配。規則僅移動**未配置的裝置**群組的裝置一次。一旦裝置被該規則移動，該規則不會再次移動該裝置，即便您把裝置手動放回**未配置裝置**群組。這是應用移動規則的建議方法。

您可以移動已經被分配的裝置到一些管理群組。為此，在規則的內容中，清空**僅移動不屬於任何管理群組的裝置**核取方塊。

應用移動規則到已經分配到一些管理群組中的裝置會顯著增加管理伺服器負載。

您可以建立重複影響單一裝置的移動規則。

我們強烈建議您避免從一個群組重複移動單一裝置到另一個群組（例如，為了套用特別政策到該裝置，執行特別群組工作，或者透過特別發佈點更新裝置）。

此類方案不被支援，因為它們顯著增加了管理伺服器負載和網路流量。這些情境也與卡巴斯基安全管理中心的操作原則衝突（尤其在存取權限、事件和報告方面）。必須找到其他解決方案，例如，透過使用政策設定檔、裝置分類的工作、根據標準情境分配網路代理，等等。

軟體分類

監控應用程式執行的主要工具是 *Kaspersky 類別*（也叫 *KL 類別*）。KL 類別說明卡巴斯基安全管理中心管理員簡化軟體分類和減少到受管理裝置的流量。

使用者類別必須僅對無法被分類成現有 KL 類別的應用程式建立（例如，對於自訂軟體）。基於應用程式安裝套件 (MSI) 或帶有安裝套件的資料夾建立的使用者類別。

如果有未透過 KL 類別分類的大軟體集可用，最好建立一個自動更新的類別。每次對包含分發套件的資料夾進行修改時，可執行檔的核對總和將被自動新增到該類別。

不要為資料夾 My Documents、%windir%、%ProgramFiles% 和 %ProgramFiles(x86)% 建立自動更新的軟體類別。在這些資料夾的檔案輪詢受頻繁變更的影響，這將導致增加管理伺服器負載和網路流量。您必須為軟體集建立專用資料夾並定期新增新項目。

關於多租戶應用程式

卡巴斯基安全管理中心啟用服務提供商管理員和租戶管理員來使用支援多租戶的 Kaspersky 應用程式。在多租戶 Kaspersky 應用程式被安裝到服務提供商基礎架構後，租戶可以開始使用應用程式。

要區分不同租戶相關的工作和政策，您必須在卡巴斯基安全管理中心中為每個租戶建立專用的虛擬管理伺服器。所有為一個租戶執行的多租戶應用程式的工作和政策必須為對應於該租戶的虛擬管理伺服器的受管理裝置管理群組而建立。為與主管理伺服器相關的管理群組建立的工作不影響租戶裝置。

和服務提供商管理員不同，租戶管理員僅可以為租戶對應的裝置建立和檢視工作和應用程式政策。服務提供商管理員和租戶管理員可以使用的工作和政策設定集是不同的。一些工作和政策設定對租戶管理員不可用。

在租戶的分級結構中，為多租戶應用程式建立的政策被繼承到低級別管理群組以及高等級管理群組：政策被傳播到屬於該租戶的所有用戶端裝置。

管理伺服器設定的備份和還原

管理伺服器設定和其資料庫的備份透過備份工作和 klbackup 公用程式執行。備份副本包括與管理伺服器有關的所有主要設定和物件，例如憑證、用於加密受管理裝置上磁碟機的主金鑰、各種產品授權的金鑰、管理群組的結構及其所有內容、工作、政策等。使用備份副本，您可以盡快還原管理伺服器的運行，這需要花費十幾分鐘到幾個小時的時間。

如果沒有備份副本可用，失敗可能導致憑證和管理伺服器設定的不可挽回的損失。這將導致要重新開始配置卡巴斯基安全管理中心，並在組織網路上重新執行網路代理初始化佈署。所有受管理裝置驅動程式加密金鑰也將遺失，導致 Kaspersky Endpoint Security 裝置上不可挽回的加密資料遺失。因此，不要略過使用標準備份工作對管理伺服器做一般備份。

快速啟動精靈為管理伺服器設定建立備份工作，並設定成每日在 4:00 AM 執行。備份副本預設儲存在 %ALLUSERSPROFILE%\Application Data\KasperskySC 資料夾。

如果安裝在其他裝置上的 Microsoft SQL Server 實例被用作 DBMS，您必須透過指定 UNC 路徑修改備份工作，這可以透過管理伺服器服務和 SQL Server 服務寫入，作為儲存備份副本的資料夾。這個需求來自 Microsoft SQL Server DBMS 備份的特殊功能。

如果一個本機 Microsoft SQL Server 執行個體被作為 DBMS 使用，建議您儲存備份副本到專用媒介，以便保證它們的安全。

因為備份副本包含重要資料，備份工作和 klbackup 公用程式用於備份副本密碼防護。預設下，備份工作使用空密碼建立。您必須在備份工作內容中設定密碼。略過該需求將導致管理伺服器憑證所有金鑰、產品授權金鑰和受管理裝置驅動程式加密金鑰保持未加密。

除了一般備份，您必須在每個顯著變更之前建立備份副本，包括管理伺服器升級和修補程式的安裝。

如果您使用 Microsoft SQL Server 作為 DBMS，則可以最小化備份副本的大小。如要最小化備份副本的大小，請啟用 SQL Server 設定中的**壓縮備份**選項。

從備份副本的還原使用管理伺服器上剛剛安裝的與建立的備份副本具有相同或更新版本的公用程式 klbackup 來執行。

欲執行還原的管理伺服器實例，必須使用相同類型（例如，相同的 SQL Server 或 MariaDB）和相同或更新版本的 DBMS。管理伺服器版本可以相同（帶有相同或更新修補程式）或更新。

這部分敘述了還原管理伺服器設定和物件的標準情境。

管理伺服器裝置不可操作

如果管理伺服器裝置由於失敗而不可操作，建議您執行以下操作：

- 新管理伺服器必須分配相同的位址：NetBIOS 名稱、FQDN 或靜態 IP（取決於佈署網路代理時的設定）。
- 安裝管理伺服器，使用相同類型、相同版本（或更新）的 DBMS。您可以安裝帶有相同（或更新）修補程式的相同（或更新）版本的伺服器。安裝後，不要透過精靈執行初始化安裝。
- 在**開始**功能表，執行 klbackup 公用程式並執行還原。

管理伺服器設定或資料庫被損壞

如果管理伺服器由於設定或資料庫損壞（例如斷電）而不可操作，建議您使用以下還原方案：

1. 掃描被損壞裝置上的檔案系統。
2. 移除管理伺服器的不可操作版本。
3. 重新安裝管理伺服器，使用相同類型、相同版本（或更新）的 DBMS。您可以安裝帶有相同（或更新）修補程式的相同（或更新）版本的伺服器。安裝後，不要透過精靈執行初始化安裝。
4. 在**開始**功能表，執行 klbackup 公用程式並執行還原。

禁止用除了透過 klbackup 公用程式的其他方法還原管理伺服器。

任何試圖透過協力廠商軟體還原管理伺服器的操作都將不可避免地導致卡巴斯基安全管理中心分發節點上的資料的不一致和應用程式操作不正常。

佈署網路代理和安全應用程式

要管理組織裝置，您必須在其上安裝網路代理。佈署分發的卡巴斯基安全管理中心到組織裝置通常開始於在其上安裝網路代理。

在 Microsoft Windows XP 中，網路代理可能錯誤執行以下操作：直接從 Kaspersky 伺服器（作為發佈點）下載更新；作為 KSN 代理伺服器（作為發佈點）；偵測協力廠商弱點（如果弱點和修補程式管理被使用）。

初始化佈署

如果已經有網路代理安裝在裝置，在該裝置上遠端安裝應用程式透過該網路代理執行。要安裝的應用程式分發套件透過網路代理和管理伺服器之間的通訊管道，與管理員定義的安裝設定一併傳輸。若要轉移分發套件，您可使用轉發分發節點，也就是發佈點、多點傳送等。如須如何在已安裝網路代理的受管理裝置上安裝應用程式的詳細資訊，請參閱本節下方。

您可以在執行 Windows 的裝置上執行網路代理初始化安裝，使用以下方法之一：

- 使用應用程式遠端安裝的協力廠商工具。
- 使用 Windows 群組政策：使用標準 Windows 群組政策管理工具。
- 在強制模式，使用卡巴斯基安全管理中心遠端安裝工作的特殊選項。
- 透過程式裝置使用者連結到卡巴斯基安全管理中心生成的獨立安裝套件。獨立安裝套件是包含所選應用程式分發套件的定義了設定的可執行模組集合。
- 在裝置上手動執行應用程式安裝程式。

在非 Microsoft Windows 平台上，您必須在受管理裝置上執行網路代理初始化安裝，透過現有協力廠商工具，或者手動傳送給使用者帶有預先設定的分發套件的存檔。您可以升級網路代理到新版本或安裝其他 Kaspersky 應用程式到非 Windows 平台，使用網路代理（已經安裝在裝置）執行遠端安裝工作。此種情況下，安裝和在 Windows 裝置上的安裝相同。

當選取佈署應用程式到受管理網路的方法和政策時，您必須考慮很多因素（部分清單）：

- 企業網路設定
- 裝置總數
- 受管理網路的 Windows 網域，可以在這些網域修改 Active Directory 群組政策
- 對排程了 Kaspersky 應用程式的初始化佈署的裝置具有本機管理員權限的使用者帳戶（例如，帶有本機管理員權限的網域使用者帳戶，帶有這些裝置的管理員權限的統一本機使用者帳戶）
- 管理伺服器和 MSP 用戶端網路之間網路通道的連線類型和頻寬，以及這些網路內部通道的頻寬
- 佈署之初套用在遠端裝置上的安全設定（例如 UAC 和簡單檔案分享模式的使用）

配置安裝程式

在開始佈署 Kaspersky 應用程式到網路之前，您必須指定安裝設定，就是在應用程式安裝過程中定義的設定。當安裝網路代理時，您應該指定最小值、連線管理伺服器和代理設定的位址，也可能需要一些進階設定。取決於您選取的安裝方法，您可以用不同方法定義設定。在最簡單的情況（在所選裝置上的手動互動安裝），所有相關設定都可以透過安裝程式使用者介面來定義，因為，在一些情況下，初始化佈署甚至可以透過傳送給使用者網路代理分發套件連結以及使用者必須在安裝程式介面輸入的設定（管理伺服器位址等等）來執行。

該方法不建議使用，因為它對使用者來說不方便，在手動定義設定的時候容易引發風險；它也在裝置群組上靜默安裝應用程式時不可用。通常情況下，管理員必須集中指定設定值；這些值可以用於建立獨立安裝套件。獨立安裝套件是包含帶有由管理員定義的設定的分發套件的自解壓存檔。獨立安裝套件可以位於允許使用者下載的資源（例如，在卡巴斯基安全管理中心網頁伺服器），以及允許在所選網路裝置上靜默安裝。

安裝套件

定義應用程式安裝設定的第一個和主要的方法是通用的，因此適用於所有安裝方法，用卡巴斯基安全管理中心工具和多數協力廠商工具。該方法包括在卡巴斯基安全管理中心中建立應用程式安裝套件。

安裝套件使用以下方法產生：

- 基於包含的*敘述符*（帶有 .kud 副檔名的包含了安裝和結果分析規則以及其他資訊的檔案）從指定的分發套件自動產生。
- 從安裝程式可執行檔或 Microsoft Windows Installer (MSI) 格式的安裝程式產生標準或所支援應用程式安裝套件。

產生的安裝套件以子資料夾和檔案層級組織。除了原始分發套件，安裝套件包含可編輯設定（包含安裝程式設定和是否在安裝結束時重新啟動作業系統等處理規則）以及小的輔助模組。

當建立安裝套件時，所選應用程式的安裝設定值可以被指定在管理主控台使用者介面（更多設定可以在所建立的安裝套件內容中找到）。當透過卡巴斯基安全管理中心工具執行遠端應用程式安裝時，安裝套件被傳送到目的裝置，因此運行應用程式安裝程式使得所有管理員定義的設定對其可用。當使用協力廠商工具安裝 Kaspersky 應用程式時，您僅需要確保目的裝置上整個安裝套件的可用性，即是分發套件和其設定的可用性。安裝套件被卡巴斯基安全管理中心建立和儲存在共用資料夾下的專用資料夾。

不在安裝套件參數中顯示授權帳戶的任何細節。

關於在透過協力廠商工具佈署之前對 Kaspersky 應用程式使用該配置方法的說明，參見「使用 Microsoft Windows 群組政策佈署」。

在卡巴斯基安全管理中心安裝之後，一些安裝套件被自動產生；它們可用於安裝並包含網路代理和 Microsoft Windows 安全應用程式套件。

在一些情況下，使用安裝套件佈署應用程式到 MSP 用戶端網路需要在對應於 MSP 用戶端的虛擬伺服器上建立安裝套件。在虛擬伺服器上建立安裝套件允許您對不同的 MSP 用戶端使用不同的安裝設定。在第一個實例中，這在處理網路代理安裝套件時是有用的，因為佈署在不同 MSP 用戶端網路的網路代理使用不同的位址連線到管理伺服器。實際上，連線位址決定了網路代理要連線的伺服器。

除了在虛擬管理伺服器上立即建立新安裝套件的可能，虛擬管理伺服器上安裝套件的主要操作模式是從主管理伺服器「分發」安裝套件到虛擬管理伺服器。你可以分發所選（或所有）安裝套件到所選的虛擬管理伺服器（包含所有所選管理群組的伺服器），使用對應的管理伺服器工作。您也可以在建立新虛擬管理伺服器時選取主管理伺服器的安裝套件清單。您所選取的安裝套件將被立即分發到新建立的虛擬管理伺服器。

當分發安裝套件時，它的內容不被整個複製。虛擬管理伺服器上的檔案儲存區，對應於正在被分發的安裝套件，僅儲存該虛擬伺服器的設定檔案。安裝套件的主要部分（包括被安裝的應用程式分發套件）保持未變更；它僅儲存在主管理伺服器儲存區。這允許您顯著提高系統效能並減少所需磁碟磁區。當處理分發到虛擬管理伺服器的安裝套件時（例如，當執行遠端安裝或建立獨立安裝套件時），主管理伺服器原始安裝套件的資料被使用對應於虛擬管理伺服器上分發的安裝套件的設定檔案「合併」。

儘管應用程式授權金鑰可以在安裝套件內容中設定，還是建議避免使用此產品授權分發方法，因為它可以輕易取得資料夾檔案的讀取權限。您應該使用自動分發的產品授權金鑰或產品授權金鑰來安裝工作。

MSI 內容和轉換檔案

另一個在 Windows 平台上配置安裝的方法是定義 MSI 內容和轉換檔案。該方法可以用在透過為 Microsoft Installer 格式的安裝設計的協力廠商工具執行安裝的時候，以及透過 Windows 群組政策使用標準 Microsoft 工具或用於處理 Windows 群組政策的其他協力廠商工具執行安裝的時候。

使用應用程式遠端安裝的協力廠商工具佈署

當任何應用程式遠端安裝工具（例如 Microsoft System Center）都在組織中可用時，可以使用這些工具進行初始化佈署。

必須執行以下操作：

- 選取能最好配合佈署工具的配置應用程式的方法。
- 定義用於同步安裝套件設定修改（透過管理主控台介面）和所選的用於從安裝套件資料佈署應用程式的協力廠商工具的操作的裝置。

卡巴斯基安全管理中心中遠端安裝工作的一般資訊

卡巴斯基安全管理中心提供遠端安裝應用程式的眾多方法，都實現在遠端安裝工作中。您可以為指定管理群組和指定裝置或裝置分類建立遠端安裝工作（此類工作顯示在管理主控台，在**工作**資料夾）。當建立工作時，您可以選取安裝套件（網路代理和/或其他應用程式的安裝套件）以用此工作安裝，並指定定義遠端安裝方法的設定。

管理群組的工作影響指定群組的裝置和所有管理群組子群組的裝置。如果工作中啟用了相應設定，工作包含了群組和其任何子群組中的從屬管理伺服器裝置。

指定裝置的工作在每一次執行時根據分類內容重新整理用戶端裝置清單。如果分類包含連線到從屬管理伺服器的裝置，工作也將在那些裝置上執行。

要確保遠端安裝工作在連線到從屬管理伺服器的裝置上成功操作，您必須使用分發工作提前分發您工作使用的安裝套件到對應的從屬管理伺服器。

使用 Microsoft Windows 群組政策佈署

建議您透過 Microsoft Windows 群組政策執行網路代理初始化佈署，如果滿足以下條件：

- 該裝置是 Active Directory 網域中的成員。
- 到網域控制站的存取被授予管理員權限，這允許您建立和修改 Active Directory 群組政策。
- 設定的安裝套件可以被移動到目的受管理裝置的網路（到可以被所有目的裝置讀取的共用資料夾）。
- 佈署方案允許您在開始佈署網路代理到裝置之前，等待下一次目的裝置例行重新啟動（或者您可以強制 Windows 群組政策套用到這些裝置）。

該佈署方案包含以下：

- Microsoft Installer 格式的應用程式分發套件（MSI 套件）位於共用資料夾（目的裝置的 LocalSystem 帳戶對該資料夾具有讀權限）。
- 在 Active Directory 群組政策中，安裝物件被建立用於分發套件。
- 安裝範圍透過指定組織單元 (OU) 和/或安全群組設定，包含目的裝置。
- 目的裝置下一次登入到網域中時（裝置使用者登入到系統之前），所有已安裝的應用程式被檢查。如果未找到應用程式，分發套件從指定在政策中的資源中下載，然後被安裝。

該佈署方案的一個好處就是被分配的應用程式在目的裝置的作業系統正在載入時被安裝，甚至在使用者登入到系統之前。即便有帶有足夠權限的使用者移除了該應用程式，它也將在作業系統下一次重新啟動時被重新安裝。該佈署方案的劣勢是管理員對群組政策所做的變更在裝置重新啟動之前將不會生效（如果不涉及附加工具）。

您可以使用群組政策安裝網路代理和其他應用程式，如果它們的安裝程式是 Windows Installer 格式。

僅可以靜默模式從 MSI 套件安裝網路代理，不支援以互動模式從 MSI 套件進行安裝。

而且，當選取該佈署方案後，您必須評估在應用 Windows 群組政策後，從中複製檔案到目的裝置的檔案資源負載。您還必須選取傳送所配置的安裝套件到該資源的方法，以及同步其設定中的相關變更的方法。

透過卡巴斯基安全管理中心遠端安裝工作處理 Microsoft Windows 政策

該佈署方法僅在從管理伺服器裝置可以存取包含目的裝置的網域控制站時可用，同時管理伺服器的共用資料夾（儲存安裝套件）可以從目的裝置讀取。基於上述原因，該佈署方法不被視為對 MSP 可應用。

透過 Microsoft Windows 政策獨立安裝應用程式

管理員可以用自己名義在 Windows 群組政策中建立安裝所需的物件。此種情況下，您必須上傳封包到獨立檔案伺服器並提供其連結。

可能有以下安裝方案：

- 管理員建立安裝套件並在管理主控台設定其內容。然後管理員複製卡巴斯基安全管理中心共用資料夾中整個 EXEC 子資料夾到組織專用檔案資源的資料夾。群組政策物件提供組織專用檔案資源子資料夾中的套件的 MSI 檔案的連結。
- 管理員從網際網路下載應用程式分發套件（包括網路代理封包）並將其上傳到組織專用檔案資源。群組政策物件提供組織專用檔案資源子資料夾中的套件的 MSI 檔案的連結。安裝設定透過配置 MSI 內容或透過配置 MST 轉換檔案來定義。

透過卡巴斯基安全管理中心遠端安裝工作的強制佈署

若要執行網路代理或其他應用程式的初始部署，您可以使用卡巴斯基安全管理中心的遠端安裝工作強制安裝選定的安裝套件，前提是每個裝置都有一個具有本機管理員權限的使用者帳戶。

強制安裝也可以在裝置無法被管理伺服器直接存取時套用：例如，裝置在隔離網路中，或者裝置在本機網路但管理伺服器在 DMZ。

在初始部署的情況下，不會安裝網路代理。因此，在遠端安裝工作的設定中，您無法選擇使用網路代理進行應用程式安裝所需的檔案分發。您只能透過管理伺服器或發佈點選擇使用作業系統資源來分發檔案。

管理伺服器服務必須在對目標裝置具有管理權限的帳戶下執行。或者，您可以在遠端安裝工作的設定中指定有權存取 admin$ share 的帳戶。

預設情況下，遠端安裝工作使用執行管理伺服器的帳戶（例如用於存取 admin$ share 的帳戶）的憑證連線到裝置。只有當目標裝置上未安裝網路代理時，您才必須在遠端安裝工作設定中指定此帳戶。
當建立要在基於 Linux 的裝置上執行的遠端安裝工作時，您必須始終指定一個用於建立 SSH 連線的帳戶。

您可以明確指定目的裝置（使用清單），透過選取它們所屬的卡巴斯基安全管理中心管理群組，或透過基於指定標準建立裝置分類。安裝開始時間定義在工作排程中。如果工作內容中啟用了**執行略過的工作**，工作可以在裝置開啟時立即執行，或裝置被移動到目的管理群組時立即執行。

強制安裝套件包括傳送安裝套件到目的裝置、隨後複製檔案到每個目的裝置的 admin$ 資源，和在這些裝置上遠端註冊支援服務。傳送安裝套件到目的裝置透過卡巴斯基安全管理中心的網路互動功能執行。以下條件必須在此種情況下被滿足：

- 目的裝置可從管理伺服器端或分發點端存取。
- 目的裝置的名稱解析在網路中正常運作。
- 裝置上的管理分享 (admin$) 保持啟用。
- 目標裝置上正在執行以下系統服務：
  - 伺服器 (LanmanServer)
    預設情況下，該服務正在執行。
  - DCOM 伺服器處理程序啟動器 (DcomLaunch)
  - RPC Endpoint Mapper (RpcEptMapper)
  - 遠端過程呼叫 (RpcS)
- 目標裝置上開啟了連接埠 TCP 445，以便透過 Windows 工具啟用遠端存取。

  TCP 139、UDP 137 和 UDP 138 由舊協定使用，目前應用程式不再需要。

  防火牆上必須允許動態出站存取連接埠，以便實現從管理伺服器和發佈點到目標裝置的連線。
- 在部署網路代理期間，Active Directory 網域政策安全性設定被允許提供 NTLM 協定的操作。
- 在執行 Microsoft Windows XP 的目的裝置上，簡單檔案共用模式被停用。

- 在目標裝置上，存取共用和安全模型被設定為*經典 - 本機使用者以自己的身分進行身分驗證*。它絕不可能是*僅限訪客 - 本機使用者以訪客身分進行身分驗證*。

- 目的裝置是網域成員，或帶有管理員權限的統一帳戶提前在目的裝置上被建立。

若要將網路代理或其他應用程式成功部署到未加入 Windows Server 2003 或更高版本 Active Directory 網域的裝置，必須在該裝置上停用遠端 UAC。遠端 UAC 是阻止本機管理帳戶存取 admin$ 的原因之一，這對於強制部署網路代理或其他應用程式必不可少。停用遠端 UAC 不會影響本機 UAC。

在未配置到任何卡巴斯基安全管理中心管理群組的新裝置上進行安裝時，您可以開啟遠端安裝工作內容並指定網路代理安裝後裝置要移動到的管理群組。

當建立群組工作時，記住每個群組工作都影響所選群組的潛逃群組中的所有裝置。因此，您必須避免在子群組中的重複安裝工作。

建立強制安裝應用程式工作的一種簡化方法是自動安裝。為此，您必須開啟管理群組內容，開啟安裝套件清單，然後選取必須在該群組中的裝置上安裝的套件。結果，所選安裝套件將被自動安裝在該群組和其所有子群組中的所有裝置上。套件被安裝的時間間隔取決於網路吞吐量和網路裝置總數。

為了減少傳送安裝套件到目的裝置期間管理伺服器的負載，您可以在安裝工作中選擇透過發佈點安裝。注意，該安裝方法給作為發佈點的裝置增加了大量負載。因此，建議您選擇符合發佈點要求的裝置。如果您使用發佈點，必須確保它們存在於託管目的裝置的每個隔離子網路中。

使用發佈點作為本機安裝中心也可以用在與管理伺服器具有窄通道通訊的子網路裝置上的安裝，此時子網路中的通道頻寬很高。

資料夾 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit 所在分區的磁碟剩餘空間必須超過所安裝應用程式的分發套件的總大小的好幾倍。

執行卡巴斯基安全管理中心建立的獨立安裝套件

以上敘述的網路代理和其他應用程式的初始化佈署方法無法總被實現，因為不可能滿足所有可套用條件。此種情況下，您可以透過卡巴斯基安全管理中心建立通用可執行檔，叫做*獨立安裝套件*，使用管理員準備的帶有相關安裝設定的安裝套件。獨立安裝套件可以被發佈在內部網頁伺服器（包含在卡巴斯基安全管理中心），如果這是合理的（到該網頁伺服器的外部存取已為目的裝置使用者設定），或發佈在包含在卡巴斯基安全管理中心 網頁主控台中的單獨佈署的網頁伺服器。您也可以複製獨立封包到其他網頁伺服器。

您可以使用卡巴斯基安全管理中心來給所選使用者傳送包含目前使用的網頁伺服器中該獨立安裝套件檔案連結的電子郵件，提示他們執行該檔案（在互動模式或帶有"-s"參數的靜默模式）。您可以附加獨立安裝套件到電子郵件，然後傳送它到對網頁伺服器沒有存取權限的裝置使用者。管理員也可以複製獨立安裝套件到外部裝置，將其傳送到相關裝置然後稍後執行。

您可以從網路代理套件或其他應用程式套件建立獨立安裝套件（例如，安全應用程式）。如果獨立安裝套件從網路代理和其他應用程式建立，安裝和網路代理一起啟動。

當建立帶有網路代理的獨立安裝套件時，您可以指定當網路代理安裝完成時，新裝置（未配置到任何管理群組的裝置）將被自動移動到的管理群組。

獨立安裝套件可以在互動模式下執行（預設），顯示應用程式安裝結果，或者可以執行在靜默模式（以參數 "-s" 執行）。靜默模式可以用在從指令碼安裝，例如作業系統映像佈署後要執行的指令碼。靜默模式安裝的結果決定與處理程序返回程式碼。

手動安裝應用程式的選項

管理員或資深使用者可以在互動模式下手動安裝應用程式。他們可以使用原始分發套件或從其他建立並儲存在卡巴斯基安全管理中心共用資料夾的安裝套件。預設下，安裝程式在互動模式下執行並提示使用者所需的設定值。然而，當使用參數 "-s" 從安裝套件根目錄執行 setup.exe 處理程序時，安裝程式將執行在靜默模式，使用配置安裝套件時定義的設定。

當從安裝套件的根目錄執行 setup.exe 時，套件先被複製到暫時資料夾，然後應用程式安裝程式將從本機資料夾執行。

建立 MST 檔案

若要轉換 MSI 套件的內容並將自訂設定套用到現有 MSI 檔案，您必須建立 MST 格式的轉換檔案。為此，請使用 Windows SDK 中包含的 Orca.exe 編輯器。

若要建立 MST 檔案：

1. 執行 Orca.exe 編輯器。
2. 轉到**檔案**頁簽，然後在功能表中點擊**開啟**。
3. 選擇 Kaspersky Network Agent.msi 檔案。
4. 轉到**轉換**頁簽，然後在功能表中選擇**新建轉換**。
5. 在**「表格」**列中，選擇**「屬性」**並寫入以下值：
   - *EULA=1*
   - *SERVERADDRESS=<管理伺服器位址>*

   點擊**儲存**按鈕。
6. 轉到**轉換**頁簽，然後在功能表中選擇**產生轉換**。
7. 在開啟的視窗中，指定您建立的轉換檔案的名稱，然後點擊**儲存**按鈕。

MST 檔案已儲存。

在安裝有網路代理的裝置上遠端安裝應用程式

如果連線到主管理伺服器（或任何其從屬管理伺服器）的可操作網路代理被安裝到裝置，您可以升級該裝置上的網路代理，以及透過網路代理安裝、升級或移除支援的應用程式。

您可在遠端安裝工作的內容中，透過選取**使用網路代理**核取方塊來啟用此選項。

如果該核取方塊被選中，帶有管理員定義的安裝設定的安裝套件將被透過網路代理和管理伺服器之間的通訊渠道傳輸到目的裝置。

要最佳化管理伺服器負載和最小化管理伺服器和裝置之間的流量，最實用的方法是為每個遠端網路或每個多點群播網域分配發佈點（請參閱「管理發佈點」一節和「建立管理群組結構和分配發佈點」一節）。此種情況下，安裝套件和安裝設定透過發佈點從管理伺服器分發到目的裝置。

而且，您可以使用發佈點來多點群播傳送安裝套件，這將允許您在佈署應用程式時顯著降低網路流量。

當透過網路代理和管理伺服器之間的通訊渠道傳輸安裝套件到目的裝置時，所有準備傳輸的安裝套件都將被快取在 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer 資料夾。當使用多個不同類型的大安裝套件並涉及大量發佈點時，該資料夾的大小將顯著增長。

檔案不能從 FTServer 資料夾手動刪除。當原始安裝套件被刪除時，對應資料將被自動從 FTServer 資料夾刪除。

發佈點收到的所有資料被儲存到 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp 資料夾。

檔案不能從 $FTCITmp 資料夾手動刪除。使用該資料夾資料的工作完成後，該資料夾的內容將被永久刪除。

因為安裝套件從中轉儲存區以最佳化傳輸的格式透過管理伺服器與網路代理之間的通訊渠道進行分發，原始資料夾裡的安裝套件不允許變更。這些變更將不會被管理伺服器自動註冊。如果您需要手動修改安裝套件的檔案（儘管建議您避免此方案），您必須在管理主控台編輯安裝套件的任何設定。在管理主控台編輯安裝套件的設定導致管理伺服器在目的裝置傳輸快取中更新安裝套件映像。

在遠端安裝工作中管理裝置重新啟動

裝置經常需要在完成應用程式遠端安裝時重新啟動（尤其在 Windows）。

如果您使用卡巴斯基安全管理中心遠端安裝工作，在新工作精靈或所建立工作的內容視窗（**作業系統重新啟動**區域），您可以選取 Windows 裝置需要重新啟動時的操作：

- **不重新啟動裝置**。此種情況下，自動重新啟動不會執行。要完成安裝，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊將被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的安裝工作。

- **重新啟動裝置**。此種情況下，如果完成安裝需要重新啟動，裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的安裝工作。

- **提示使用者操作**。此種情況下，用戶端裝置上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。**提示使用者操作**最適用於使用者需要選取最合適重新啟動時間的工作站。

病毒防護應用程式安裝套件上的資料庫更新

開始防護佈署之前，您必須注意要隨安全應用程式的分發套件一起更新病毒資料庫（包括模組和自動修補程式）。最好在開始佈署之前更新應用程式安裝套件中的資料庫（例如，透過使用所選安裝套件上下文功能表中的相關指令）。這將減少目的裝置在完成防護佈署後所需的重新啟動次數。如果您的遠端安裝涉及到從主管理伺服器中繼到虛擬伺服器的安裝套件，您僅需要更新主要伺服器原始封包中的資料庫。此種情況下，您不必更新虛擬伺服器上中繼的封包中的資料庫。

刪除不相容的協力廠商安全應用程式

透過卡巴斯基安全管理中心進行 Kaspersky 安全應用程式的安裝可能需要移除與正在安裝的應用程式不相容的協力廠商軟體。有兩種移除協力廠商應用程式的方法。

透過使用安裝程式自動移除不相容的應用程式

當您執行安裝程式，它會顯示一個與卡巴斯基應用程式不相容的應用程式清單：



在遠端安裝精靈中顯示的不相容應用程式清單

卡巴斯基安全管理中心會偵測不相容軟體。因此，您可以選中**自動解除安裝不相容的應用程式**核取方塊以繼續安裝。如果清除此核取方塊並且不卸除安裝不相容的軟體，則會發生錯誤並且不會安裝卡巴斯基應用程式。

自動移除不相容應用程式受各種應用程式支援。

透過專用工作移除不相容的應用程式

要移除不相容的應用程式，使用*遠端解除安裝應用程式*工作。該工作應該在安全應用程式安裝工作執行之前執行在裝置。例如，在安裝工作中，您可以選取**在完成其它工作時**作為排程類型，其中的其他工作為*遠端解除安裝應用程式*。

該移除方法在安全應用程式無法正確移除不相容應用程式時是很有用的。

使用命令提示字元刪除受密碼防護的網路代理

若要遠端卸載已為其設定卸載密碼的網路代理，您可以使用命令提示字元。

如果您遺失或忘記了安裝在不再受 Kaspersky Security Center 管理的裝置上的受密碼防護的網路代理的密碼，則無法使用 klmover 公用程式、清理工具 (cleaner.exe)、或命令提示字元移除網路代理。在這種情況下，您必須在安裝了受密碼防護的網路代理的裝置上重新安裝作業系統。

若要透過命令提示字元卸載網路代理：

1. 將您的卸載密碼轉換為十六進位代碼。

   使用網際網路資源、程式設計環境、文字編輯器或其他合適的工具將您的密碼轉換為十六進位代碼。

   確保用於將產生的十六進位代碼分成幾部分的輸出分隔符號設定為`00`。例如，十六進位代碼`51 77 65 72 74 79`不正確，十六進位代碼`5100770065007200740079 00`正確。

2. 在命令提示字元中輸入以下命令，然後按**ENTER** ：

   ```
   msiexec.exe /x{<product code>} /qn KLUNINSTPASSWD=<hex code of your uninstallation password>
   ```

   您可以在下表中尋找您的網路代理的產品代碼。

   網路代理產品代碼

當地語係化	產品代碼
阿拉伯語	{FA7BF140-F356-404A-BDA3-3EF0878D7C63}
保加利亞語	{4DBF6741-FA51-4C14-AFD2-B7D9246995F6}
捷克文	{478A6A0B-D177-4402-B703-808C05C56B13}
英語	{BCF4CF24-88AB-45E1-A6E6-40C8278A70C5}
法語	{2924BEDA-E0D7-4DAF-A224-50D2E0B12F5B}
德語	{2F383CB3-6D7C-449D-9874-164E49E1E0F5}
匈牙利文	{8899A4D4-D678-49F8-AD96-0B784F58D355}
義大利文	{DC3A3164-36B3-4FB4-B7BF-16A41C35A728}
日文	{790C176F-7780-4C84-8B9C-455F5C0E61C5}
韓文	{70812A40-973B-4DA1-96B9-C2011280CD99}
波蘭文	{1A7B331A-ABBE-4230-995E-BCD99C5A18CF}
葡萄牙文	{0F05E4E5-5A89-482C-9A62-47CC58643788}
羅馬尼亞文	{FF802D76-E241-41D3-AAB4-DC7FBD659446}
俄語	{ED1C2D7E-5C7A-48D8-A697-57D1C080ABA7}
簡體中文	{FBD7C01E-49CB-4182-8714-9DB1EAE255CB}
西班牙語	{F03982CF-1C5C-4E12-9F9E-D36C35E62402}
西班牙語（墨西哥）	{29748B5F-D88A-4933-B614-1CCCD6EFB0B7}
繁體中文	{F6AD731A-36B4-4739-B1D4-70D6EDA35147}
土耳其文	{2475A66D-698B-4050-93FF-9B48EE82E2BA}

在卡巴斯基安全管理中心中使用工具遠端安裝應用程式以便在受管理裝置上執行相關可執行檔

使用新安裝套件精靈，您可以選取任何可執行檔並為其定義命令列設定。為此，您可以新增所選檔案或整個檔案所在資料夾到安裝套件。然後，您必須建立遠端安裝工作並選取所建立的安裝套件。

當工作正在執行時，帶有命令列所定義設定的指定可執行檔將在目的裝置上執行。

如果您使用 Microsoft Windows Installer (MSI) 格式的安裝程式，卡巴斯基安全管理中心使用標準工具分析安裝結果。

如果有弱點和修補程式管理產品授權可用，卡巴斯基安全管理中心（當為任何企業環境中支援的應用程式建立安裝套件時）也使用安裝和安裝結果分析規則。

否則，可執行檔的預設工作將等待執行中處理程序和所有子處理程序的完成。在所有執行中處理程序完成後，工作將被成功完成，不管初始處理程序的返回碼是什麼。若要變更此工作的這種行為，在建立工作之前，您必須手動修改卡巴斯基安全中心在新建的安裝套件及其子資料夾中產生的 .kpd 檔案。

.kpd 檔案使用 ASCII 編碼。 .kud 檔案使用 Unicode 編碼。

對於不需要等待執行中處理程序完成的工作，設定 [SetupProcessResult] 區域的等待設定的值為 0：

```
[SetupProcessResult]
Wait=0
```

對於僅需要等待 Windows 執行中處理程序，而不是所有子處理程序完成的工作，設定 [SetupProcessResult] 區域的 WaitJob 設定值為 0，例如：

```
[SetupProcessResult]
WaitJob=0
```

若要工作根據正在執行的處理程序的返回代碼成功完成或者返回錯誤，請建立一個儲存錯誤代碼到檔案的 .bat 檔案，例如：

```
echo [ResponseResult] > setup.log
echo ResultCode=2 >> setup.log
exit 0
```

然後修改卡巴斯基安全管理中心在新建立的安裝套件的資料夾中產生的 .kud 檔案：

```
[SetupMainResult]
File=setup.log
Section=ResponseResult
Value=ResultCode
[SetupMainResult_SuccessCodes]
0=安裝成功完成。
[SetupMainResult_ErrorCodes]
1=安裝指令碼錯誤
2=自訂錯誤
```

此種情況下，任何非清單中的返回碼都會導致返回錯誤。

要在工作成功完成或工作結果錯誤中顯示註釋，在 [SetupProcessResult_SuccessCodes] 和 [SetupProcessResult_ErrorCodes] 區域根據處理程序返回碼輸入錯誤的簡短敘述，例如：

```
[SetupProcessResult_SuccessCodes]
0=安裝成功完成
3010=需要重新啟動以完成安裝
[SetupProcessResult_ErrorCodes]
1602=安裝被使用者取消
1603=安裝過程中出現致命錯誤
```

要使用卡巴斯基安全管理中心工具管理裝置重新啟動（如果需要重新啟動以完成操作），列出暗示重新啟動的處理程序返回碼，在 [SetupProcessResult_NeedReboot] 區域：

```
[SetupProcessResult_NeedReboot]
3010=
```

監控佈署

要監控卡巴斯基安全管理中心佈署和確保安全應用程式和網路代理成功安裝在受管理裝置，您必須在**佈署**區域檢查信號燈。該信號燈位於管理主控台主視窗的管理伺服器節點工作區。信號燈反映了目前佈署狀態。安裝了網路代理和安全應用程式的裝置數量顯示在信號燈旁邊。當任何安裝工作正在執行時，您可以監控它們的處理程序。如果有任何安裝錯誤發生會顯示錯誤數量。您可以透過按連結檢視錯誤詳情。

在**受管理裝置**資料夾的工作區的**群組**頁籤，您也可以使用佈署圖表。圖表反映了佈署處理程序，顯示沒有網路代理、帶有網路代理或帶有網路代理和安全應用程式的裝置數量。

若需更多佈署處理程序（或者特定安裝工作的操作）的詳情，開啟相關遠端安裝工作的結果視窗：點擊工作並在上下文功能表中選取**結果**。視窗顯示了兩個清單：上面一個包含裝置上的工作狀態，下面一個包含從上面清單中選取的裝置上的工作事件。

佈署錯誤的資訊被新增到管理伺服器上的卡巴斯基事件記錄。錯誤資訊也在**報告和通知**資料夾，**事件**子資料夾的對應事件分類中可用。

配置安裝程式

該部分提供了卡巴斯基安全管理中心安裝程式檔案和安裝設定的資訊，以及如何在靜默模式安裝管理伺服器和網路代理的建議。

一般資訊

卡巴斯基安全管理中心 14.2 元件（管理伺服器、網路代理和管理主控台）的安裝程式根據 Windows Installer 技術建立。MSI 套件是安裝程式的核心。該格式的套件允許使用 Windows Installer 的所有好處：可量測性、修補程式系統可用性、轉換系統、透過協力廠商解決方案集中安裝以及在作業系統中透明註冊。

在靜默模式下安裝（帶有回應檔案）

管理伺服器和網路代理安裝程式可以使用回應檔案工作 (ss_install.xml)，其中整合了不需要使用者參與的靜默模式安裝參數。ss_install.xml 檔案位於與 MSI 套件相同的資料夾；在靜默模式安裝時被自動使用。您可以使用指令行鍵 "/s" 啟用靜默安裝模式。

一個大概例子執行如下：

```
setup.exe /s
```

在靜默模式中啟動安裝程式之前，請閱讀最終使用者產品授權協議 (EULA)。如果卡巴斯基安全管理中心分發套件不包含帶有 EULA 文字的 TXT 檔案，您可以從卡巴斯基網站下載此檔案。

ss_install.xml 檔案卡巴斯基安全管理中心安裝程式參數的內部格式的實例。分發套件包含帶有預設參數的 ss_install.xml 檔案。

請不要手動修改 ss_install.xml 檔案。該檔案可以透過卡巴斯基安全管理中心工具修改，當在管理主控台編輯安裝套件參數時。

如要修改管理伺服器安裝的回應檔案，請執行以下操作：

1. 開啟卡巴斯基安全管理中心分發套件。如果您是使用完整的套件 EXE 檔案，然後將其解壓縮。
2. 從伺服器資料夾中，開啟命令列，然後執行以下命令：

   ```
   setup.exe /r ss_install.xml
   ```

   卡巴斯基安全管理中心安裝程式啟動。
3. 按照精靈的步驟設定卡巴斯基安全管理中心安裝。

   當您完成精靈時，回應檔案會根據您指定的新設定自動修改。

在靜默模式下安裝（沒有回應檔案）

您可以使用單獨 .msi 套件安裝網路代理，以標準方法指定 MSI 內容的值。該方案允許網路代理使用群組政策安裝。

請勿重新命名安裝套件 Kaspersky Network Agent.msi。重新命名此套件可能會在網路代理的未來更新期間導致安裝錯誤。

要避免透過 MSI 套件內容定義的參數與回應檔案中定義的參數衝突，您可以透過設定內容 `DONT_USE_ANSWER_FILE=1` 來停用回應檔案。MSI 檔案位於卡巴斯基安全管理中心分發套件，此項目位於 Packages\NetAgent\exec 資料夾中。一個帶有 .msi 套件的網路代理安裝程式執行例子如下。

在靜默模式中安裝網路代理需要接受最終使用者產品授權協議的條款。只有在您已完整閱讀、瞭解和接受最終使用者產品授權協議的條款，才使用 `EULA=1` 參數。

```
示例：
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1
```

您也可以透過提前準備回應檔案（帶有 .mst 副檔名）來定義 msi 套件的安裝參數。該指令顯示如下：

```
例如：
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

您可以在單一命令列中指定幾個回應檔案。

如果要使用 Windows 安裝程式升級網路代理，請執行下列命令：

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

透過 setup.exe 的部分安裝配置

當透過 setup.exe 執行應用程式安裝時，您可以新增 MSI 任何內容的值到 MSI 套件。

該指令顯示如下：

例如：
```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

管理伺服器安裝參數

下表敘述了安裝管理伺服器時您可以配置的 MSI 內容。所有參數都是可選的，除了 EULA 和隱私政策。

靜默模式下安裝管理伺服器的參數

MSI 內容	敘述	可用值
EULA	是否接受授權協議的條款（必需）。	• 1—我已完整閱讀、瞭解和接受最終使用者產品授權協議的條款。 • 其它值或未指定 – 表示我不接受產品授權協議的條款（將不會執行安裝）。
隱私政策	是否接受隱私政策條款（必需）。	• 1—我瞭解並同意將我的資料進行處理和傳輸(包括向第三國)，如所述於隱私權政策。我確認已完整閱讀並理解隱私權政策。 • 其它值或未指定 – 表示我不接受隱私政策的條款（將不會執行安裝）。
INSTALLATIONMODETYPE	管理伺服器的安裝類型	• 標準 • 自訂
INSTALLDIR	應用程式的安裝資料夾	字串值。
ADDLOCAL	要安裝的元件清單（以逗號分隔）	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. 管理伺服器安裝正常執行的最小元件清單： `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	網路的大小	• NRT_1_100 — 1 to 100 台裝置。 • NRT_100_1000 — 101 到 1000 台裝置。 • NRT_GREATER_1000 —多於 1,000 部裝置。
SRV_ACCOUNT_TYPE	指定操作管理伺服器服務的使用者的方法	• SrvAccountDefault —將自動建立使用者帳戶。 • SrvAccountUser —手動定義使用者帳戶。
SERVERACCOUNTNAME	服務使用者名稱	字串值。
SERVERACCOUNTPWD	服務使用者密碼	字串值。
DBTYPE	資料庫類型	• MySQL – 將使用 MySQL 或 MariaDB 資料庫。 • MSSQL – 將使用 Microsoft SQL Server (SQL Express) 資料庫。
MYSQLSERVERNAME	MySQL Server 或 MariaDB 伺服器完整名稱	字串值。
MYSQLSERVERPORT	連線到 MySQL 或 MariaDB 伺服器連接埠號碼	數值。
MYSQLDBNAME	MySQL 或 MariaDB 伺服器資料庫的名稱	字串值。
MYSQLACCOUNTNAME	連線到 MySQL 或 MariaDB 伺服器資料庫的使用者名稱	字串值。
MYSQLACCOUNTPWD	連線到 MySQL 或 MariaDB 伺服器資料庫的使用者密碼	字串值。

MSI 內容	敘述	可用值
MSSQLCONNECTIONTYPE	MSSQL 資料庫使用類型	• InstallMSSEE – 從套件安裝 • ChooseExisting – 使用已安裝伺服器
MSSQLSERVERNAME	SQL Server 實例的完整名稱	字串值。
MSSQLDBNAME	SQL Server 資料庫名稱	字串值。
MSSQLAUTHTYPE	連線到 SQL Server 的身分驗證方法	• Windows • SQLServer
MSSQLACCOUNTNAME	以 SQLServer 模式連線到 SQL Server 的使用者名稱	字串值。
MSSQLACCOUNTPWD	以 SQLServer 模式連線到 SQL Server 的使用者密碼	字串值。

CREATE_SHARE_TYPE	指定共用資料夾的方法	• Create – 建立新共用資料夾。此種情況下，必須定義以下內容：
		  • SHARELOCALPATH – 本機資料夾路徑
		  • SHAREFOLDERNAME – 資料夾網路名稱
		• Null – EXISTSHAREFOLDERNAME 必須被正確指定

EXISTSHAREFOLDERNAME	現有共用資料夾的完整路徑	字串值。
SERVERPORT	連線至管理伺服器的埠號	數值。
SERVERSSLPORT	建立到管理伺服器的 SSL 連線的埠號	數值。
SERVERADDRESS	管理伺服器位址	字串值。
SERVERCERT2048BITS	管理伺服器憑證金鑰長度（位元）	• 1 – 管理伺服器憑證的金鑰長度為 2048 位元。 • 0 – 管理伺服器憑證的金鑰長度為 1024 位元。 • 如果未指定值，管理伺服器憑證的金鑰長度為 2048 位元。
MOBILESERVERADDRESS	連線行動裝置的管理伺服器位址；如果未選取 MobileSupport 元件則略過	字串值。

網路代理安裝參數

下表敘述了安裝網路代理時您可以配置的 MSI 內容。所有參數都是可選的，除了 EULA 和伺服器位址。

靜默模式下安裝網路代理的參數

MSI 內容	敘述	可用值
EULA	設定是否接受授權協議的條款	• 1—我確認我已完整閱讀、理解並接受此最終使用者產品授權協議的條款和條件。 • 0—表示我不接受產品授權協議的條款（將不會執行安裝）。 • 沒有值—表示我不接受產品授權協議的條款（將不會執行安裝）。
DONT_USE_ANSWER_FILE	從回應檔案讀取安裝設定	• 1—不使用。 • 其他值或沒有值 – 讀取。
INSTALLDIR	網路代理的安裝資料夾路徑	字串值。
SERVERADDRESS	管理伺服器位址（必需）	字串值。
SERVERPORT	連線管理伺服器的埠號	數值。

MSI 內容	敘述	可用值
SERVERSSLPORT	使用 SSL 協定加密連線到管理伺服器的埠號	數值。
USESSL	是否使用 SSL 連線	• 1 – 使用。 • 其它值或未指定 – 不使用。
OPENUDPPORT	是否開啟 UDP 連接埠	• 1 – 開啟。 • 其它值或未指定 – 不開啟。
UDPPORT	UDP 埠號	數值。
USEPROXY	是否使用代理伺服器。 出於相容性目的，不建議在網路代理安裝套件設定中指定代理連線設定。	• 1 – 使用。 • 其它值或未指定 – 不使用。
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	連線到 Proxy 伺服器的 Proxy 位址和埠號	字串值。
PROXYLOGIN	連線代理伺服器的帳戶	字串值。
PROXYPASSWORD	用於連線至代理伺服器的帳戶密碼（請勿在安裝套件的參數中指定權限帳戶的任何詳細資訊）。	字串值。
GATEWAYMODE	連線閘道使用模式	• 0 – 不使用連線閘道。 • 1 – 使用該網路代理作為連線閘道。 • 2 – 使用連線閘道連線到管理伺服器。
GATEWAYADDRESS	連線閘道位址	字串值。
CERTSELECTION	接收憑證的方法	• GetOnFirstConnection – 從管理伺服器接收憑證。 • GetExistent – 如果選中此選項則選取現有憑證，必須指定 CERTFILE 內容。
CERTFILE	憑證檔案路徑	字串值。
VMVDI	啟用虛擬桌面基礎架構 (VDI) 的動態模式	• 1 – 啟用。 • 0 – 不啟用。 • 沒有值 – 不啟用。
VMOPTIMIZE	網路代理設定是否最適用於 hypervisor	• 1 – 啟用。 • 0 – 不啟用。 • 沒有值 – 不啟用。
LAUNCHPROGRAM	安裝後是否啟動網路代理服務。如果 VMVDI=1，則忽略該參數	• 1 – 啟動。 • 其他值或沒有值 – 不啟動。
NAGENTTAGS	網路代理標籤（具有比回應檔案中標籤高的優先順序）	字串值。

虛擬基礎架構

卡巴斯基安全管理中心支援虛擬機的使用。您可以將網路代理和安全應用程式安裝在每台虛擬機器，以及在 hypervisor 級別的虛擬機器防護。在第一種情況下，您可以使用標準安全應用程式或 Kaspersky Security for Virtualization Light Agent 來防護您的虛擬機器。在第二種情況下，您可以使用 Kaspersky Security for Virtualization Agentless。

卡巴斯基安全管理中心支援將虛擬機器回溯到其以前的狀態。

降低虛擬機負載的竅門

當安裝網路代理到虛擬機時，建議您停用一些對虛擬機沒有用的卡巴斯基安全管理中心功能。

當在虛擬機或虛擬機範本上安裝網路代理時，我們建議執行以下操作：

- 如果您正執行遠端安裝，在網路代理安裝套件的內容視窗（在**進階**下），選取**最佳化 VDI 設定**選項。
- 如果您正透過精靈在互動式介面上執行，在精靈視窗，選中**為虛擬架構最佳化網路代理設定**選項。

選中這些選項將改變網路代理設定，因此以下功能保持預設被停用（在套用政策之前）：

- 獲取已安裝軟體的資訊
- 獲取硬體資訊
- 獲取偵測到的弱點資訊
- 獲取需要更新的資訊

通常，這些功能對於虛擬機不必要，因為它們使用統一軟體和虛擬硬體。

停用該功能是不可逆的。如果需要任何被停用的功能，您可以透過網路代理政策啟用它，或透過網路代理本機設定。網路代理本機設定透過管理主控台中相關裝置的上下文功能表可用。

對動態虛擬機的支援

卡巴斯基安全管理中心支援動態虛擬機。如果虛擬架構佈署在組織網路，動態（暫時）虛擬機可以被用在特定情況。動態虛擬機基於管理員提供的範本以獨立名稱建立。使用者工作在虛擬機一定時間，然後關閉虛擬機後，該虛擬機將被從虛擬架構刪除。如果卡巴斯基安全管理中心被佈署在組織網路，安裝了網路代理的虛擬機將被新增到管理伺服器資料庫。在您關閉虛擬機後，對應的項目必須從管理伺服器資料庫中刪除。

要自動刪除虛擬機項目，當安裝網路代理到範本或動態虛擬機時，選取**啟用 VDI 動態模式**選項：

- 對於遠端安裝—在網路代理安裝套件的內容視窗（**進階**區段）
- 對於互動式安裝 — 在網路代理安裝精靈中

> 當安裝網路代理到實體裝置時，不要選取**啟用 VDI 動態模式**選項。

如果您要在刪除虛擬機後將動態虛擬機的事件儲存在管理伺服器一段時間，那麼，在管理伺服器內容視窗，在**事件儲存區**區域，選取**裝置被刪除後儲存事件**選項並指定事件的最大儲存期限（天）。

> 我們不建議在動態虛擬機上啟用加密磁碟機。

對虛擬機複製的支援

複製安裝了網路代理的虛擬機或從安裝了網路代理的範本建立虛擬機，和擷取和複製硬碟磁碟機映像的網路代理佈署相同。因此，一般情況下，當複製虛擬機時，您需要執行與透過複製磁碟映像佈署網路代理時相同的操作。

然而，以下敘述的兩種情況展示了自動偵測複製的網路代理。由於以上原因，您不必執行"透過擷取和複製裝置磁碟映像佈署"中敘述的複雜操作：

- 安裝網路代理時勾選**啟用 VDI 動態模式**選項：在每次重新啟動作業系統後，系統會將此虛擬機視為新裝置，無論此虛擬機是否為複製的虛擬機。
- 以下 hypervisors 之一被使用：VMware™, HyperV®, 或 Xen®：網路代理透過變更的虛擬硬體 ID 偵測虛擬機的複製。

虛擬硬體變更分析並不絕對可靠。在廣泛套用該方法之前，您必須在小組虛擬機上測試您組織中使用的目前 hypervisor 版本。

對網路代理裝置檔案系統回溯的支援

卡巴斯基安全管理中心是一個分發的應用程式。在安裝了網路代理的裝置上回溯檔案系統到先前狀態將導致資料不同步和卡巴斯基安全管理中心功能不正常。

檔案系統（或一部分）可以在以下情況下回溯：

- 當複製硬體磁碟機映像時。
- 當透過虛擬架構還原虛擬機狀態時。
- 當從備份副本或還原點還原資料時。

安裝了網路代理的裝置上的協力廠商軟體影響 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ 資料夾的情景僅是卡巴斯基安全管理中心的關鍵情景。因此，如果可能，您必須總是從還原處理程序中排除該資料夾。

因此一些組織的工作規則提供了對裝置檔案系統的回溯，對安裝了網路代理的裝置的檔案系統回溯的支援被新增到了卡巴斯基安全管理中心，從版本 10 Maintenance Release 1 開始（管理伺服器和網路代理必須是版本 10 Maintenance Release 1 或更新）。當偵測到時，這些裝置被自動連線到管理伺服器，帶有完整資料清除和完整同步。

預設下，對檔案系統回溯偵測的支援在卡巴斯基安全管理中心 14.2 中被啟用。

盡量不要回溯網路代理裝置的 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ 資料夾，因為完整資料的重新同步需要大量資源。

系統狀態回溯在管理伺服器裝置上是不允許的。管理伺服器使用的資料庫的回溯也是不允許的。

您可以僅可以使用標準的 klbackup 公用程式從備份副本還原管理伺服器狀態。

關於漫遊使用者的連線設定檔

可攜式電腦（也叫"裝置"）的漫遊使用者需要變更連線到管理伺服器的方法或者根據目前裝置在企業網路中的位置在管理伺服器之間進行轉換。

連線設定檔僅支援執行 Windows 和 macOS 的裝置。

使用單一管理伺服器的不同位址

網路代理裝置從組織網路或內部網可以連線到管理伺服器。該情況可能需要網路代理使用不同的位址以連線到管理伺服器：對於網際網路連線的外部管理伺服器位址和對於內部網路連線的內部管理伺服器位址。

為此，您必須新增設定檔（為了從網際網路連線到管理伺服器）到網路代理政策。在政策內容中新增設定檔（**連線**區域，**連線設定檔**子區域）。在建立設定檔視窗中，您必須停用**僅用來接收更新**選項並選取**在此設定檔中同步連線設定和管理伺服器設定**選項。如果您使用連線閘道存取管理伺服器（例如，在"網際網路存取：DMZ 中作為連線閘道的網路代理"部分敘述的卡巴斯基安全管理中心設定中），您必須在連線設定檔的對應欄位指定連線閘道位址。

根據目前網路在管理伺服器之間進行轉換

如果組織有帶有多個管理伺服器的多個辦公室，並且一些網路代理裝置在期間進行移動，您需要網路代理連線到裝置所在的本機網路中的管理伺服器。

此種情況下，您必須為每個辦公室在網路代理政策內容中建立連線管理伺服器的設定檔，除了歸屬管理伺服器所在的主辦公室。您必須在連線設定檔中指定管理伺服器位址，並啟用或停用**僅用來接收更新**選項：

- 在使用本機伺服器下載更新時，如果您需要網路代理與歸屬管理伺服器同步，則選中此選項。
- 如果網路代理必須被本機管理伺服器完全管理，則停用此選項。

此後，您必須設定轉換到新建立的設定檔的條件：每個辦公室至少一個條件，除了歸屬辦公室。每個條件的目的包括辦公室網路環境項目的偵測。如果條件是真，對應設定檔被啟動。如果沒有條件是真，網路代理轉換到歸屬管理伺服器。

佈署行動裝置管理功能

此區域提供初始佈署行動裝置管理功能的資訊。

將 KES 裝置連線至管理伺服器

根據連線裝置到管理伺服器的方法，對 KES 裝置 Kaspersky Device Management for iOS 有兩個佈署方案：

- 直接連線裝置到管理伺服器來佈署的方案
- 涉及支援 Kerberos 約束委派的反向代理的部署方案

直接連線裝置到管理伺服器

KES 裝置可以直接連線到管理伺服器的連接埠 13292。

根據使用的身分驗證方法，連線 KES 裝置到管理伺服器有兩個選項：

- 使用使用者憑證連線裝置
- 不用使用者憑證連線裝置

運用使用者憑證連線裝置

當連線帶有使用者憑證的裝置時，裝置與透過管理伺服器工具被分配憑證的使用者帳戶相關聯。

此種情況下，雙向 SSL 身分驗證（雙向認證）將被使用。管理伺服器和裝置都將使用憑證認證。

不用使用者憑證連線裝置

當連線沒有使用者憑證的裝置時，裝置不與任何管理伺服器上的使用者帳戶關聯。然而，當裝置接收任何憑證時，裝置將與透過管理伺服器工具被分配憑證的使用者相關聯。

當連線裝置到管理伺服器時，將套用單向 SSL 身分驗證，這意味著僅管理伺服器使用憑證進行身分驗證。裝置獲取使用者憑證後，身分驗證類型將變更為雙向 SSL 身分驗證（雙向 SSL 身分驗證，共有身分驗證）。

連線 KES 裝置到 Kerberos constrained delegation (KCD) 伺服器的方案

連線 KES 裝置到 Kerberos constrained delegation (KCD) 管理伺服器的方案包括如下：

- 與支援 KCD 的反向代理整合。
- 將 Kerberos Constrained Delegation (KCD) 用於行動裝置身分驗證。
- 與公共金鑰基礎架構 (PKI) 整合以套用使用者憑證。

當使用該連線方案時，請注意以下幾點：

- 連線 KES 裝置到反向代理的類型必須是"雙向 SSL 身分驗證"，就是，裝置必須透過先前使用者憑證連線到反向代理。為此，您不要整合使用者憑證到 Kaspersky Endpoint Security for Android 安裝套件。該 KES 套件必須由裝置指定的管理伺服器建立。

- 您必須指定特定（自訂）憑證，而不是行動協定的預設伺服器憑證：

  1. 在管理伺服器的內容視窗，在**設定**區域，選取**為行動裝置開啟連接埠**核取方塊，然後在下拉清單中選取**新增憑證**。

  2. 在開啟的視窗中，指定當到行動協定的存取點被發佈在管理伺服器時設定在反向代理上的憑證。

- KES 裝置的使用者憑證必須由網域中的 Certificate Authority (CA) 發佈。記住，如果網域包含多個多個根 CA，使用者憑證必須被該 CA 發佈，這已設定在反向代理發佈中。

  您可以透過以下方法確保使用者憑證與上述需求相容：

  - 在新增安裝套件精靈和憑證安裝精靈中指定使用者憑證。

  - 將管理伺服器與網域的 PKI 整合並在憑證發佈規則中定義對應的設定：

    1. 在主控台樹狀目錄中，延伸**行動裝置管理**資料夾並選擇**憑證**子資料夾。

    2. 在**憑證**資料夾中點擊**配置憑證發佈規則**按鈕，開啟**憑證發佈規則**視窗。

    3. 在**與 PKI 整合**區域，配置與公共金鑰基礎架構的整合。

    4. 在**行動憑證發佈**區域，指定憑證來源。

以下是使用以下假定設定 Kerberos Constrained Delegation (KCD) 的例子：

- 管理伺服器到行動協定的存取點被設定成連接埠 13292。

- 具有反向代理的裝置的名稱是firewall.mydom.local。

- 管理伺服器裝置名稱是 ksc.mydom.local。

- 存取點到行動協定的外部發佈位址是 kes4mob.mydom.global。

管理伺服器網域帳戶

您必須建立執行管理伺服器服務的網域帳戶（例如，KSCMobileSrvcUsr）。您可以在安裝管理伺服器或使用 klsrvswch 公用程式時指定管理伺服器服務帳戶。klsrvswch 公用程式位於管理伺服器安裝資料夾。預設安裝路徑：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

網域帳戶必須由以下原因指定：

- KES 裝置管理功能是管理伺服器的一部分。

- 要確保 Kerberos Constrained Delegation (KCD) 的正常功能，接收端（例如，管理伺服器）必須執行在網域帳戶下。

http/kes4mob.mydom.local 的服務主體名稱

在網域中，在 KSCMobileSrvcUsr 帳戶下，新增 SPN 以在管理伺服器裝置的連接埠 13292 發佈行動協議服務。對於管理伺服器裝置 kes4mob.mydom.local，將是如下：

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

配置具有反向代理的裝置的網域內容 (firewall.mydom.local)

要授權流量，您必須信任反向代理裝置 (firewall.mydom.local) 到由 SPN 定義的服務 (http/kes4mob.mydom.local:13292)。

要信任反向代理裝置到由 SPN 定義的服務 (http/kes4mob.mydom.local:13292)，管理員必須執行以下操作：

1. 在名稱為「Active Directory 使用者和電腦」的 Microsoft Management Console 中，選取安裝了反向代理的裝置 (firewall.mydom.local)。
2. 在裝置內容視窗，在**授權**頁籤，設定**信任此電腦到指定服務的授權**轉換鍵到**使用任何身分驗證協議**。
3. 在**該帳戶可以展示已授權憑證的服務**清單，新增 SPN http/kes4mob.mydom.local:13292。

要發佈的特定（自訂）憑證 (kes4mob.mydom.global)

要發佈管理伺服器行動協議，您必須發佈一個 FQDN kes4mob.mydom.global 特定（自訂）憑證並在管理主控台中管理伺服器的行動協議設定中指定它以代替預設伺服器憑證。為此，在管理伺服器的內容視窗，在**設定**區域，選取**為行動裝置開啟連接埠**核取方塊，然後在下拉清單中選取**新增憑證**。

請注意伺服器憑證容器（帶有 .p12 或 .pfx 副檔名的檔案）必須也包含根憑證鏈（公共金鑰）。

配置在反向代理上發布

在反向代理上，對於從行動裝置到連接埠 kes4mob.mydom.global 連接埠 13292 的流量，您必須在 SPN (http/kes4mob.mydom.local:13292) 上配置 KCD，使用為 FQND kes4mob.mydom.global 發佈的憑證。請注意，正發佈和已發佈的存取點（管理伺服器連接埠 13292）必須共用相同的伺服器憑證。

使用 Firebase Cloud Messaging

為了確保及時將指令交付到 Android 作業系統管理的 KES 裝置上，卡巴斯基安全管理中心使用推送通知機制。推播通知透過 Firebase Cloud Messaging（以下簡稱 FCM）在 KES 裝置和管理伺服器之間交換。在卡巴斯基安全管理中心管理主控台中，可以指定 Firebase Cloud Messaging 的設定從而將 KES 裝置連線到服務。

若要擷取 Firebase Cloud Messaging 的設定，您必須有 Google 帳戶。

要啟用對 FCM 的使用：

1. 在管理主控台中，選取**行動裝置管理** 節點以及**行動裝置**資料夾。
2. 在**行動裝置**的上下文功能表中，選取**內容**。
3. 在資料夾內容中，選取**Google Firebase Cloud Messaging 設定**區域。

4. 在**傳送者 ID**欄位中，指定 FCM 寄件者 ID。

5. 在**私密金鑰檔案（JSON 格式）**欄位中，選擇私鑰檔案。

在下次同步管理伺服器時，由 Android 作業系統管理的 KES 裝置將被連線到 Firebase Cloud Messaging。

透過點擊**重設設定**按鈕，您可以編輯 Firebase Cloud Messaging 的設定。

當您切換到其他 Firebase 項目時，您需要等待 10 分鐘 FCM 才能還原。

FCM 服務在以下位址範圍內執行：

- 從 KES 裝置端，需要對以下位址的連接埠 443 (HTTPS)、5228 (HTTPS)、5229 (HTTPS) 和 5230 (HTTPS) 的存取：
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - Google's ASN 15169 中列出的所有 IP 位址
- 從管理伺服器端，需要對以下位址的連接埠 443 (HTTPS) 的存取：
  - fcm.googleapis.com
  - Google's ASN 15169 中列出的所有 IP 位址

如果將代理伺服器設定（**進階 / 設定網際網路存取**）指定在管理主控台的管理伺服器內容中，系統會將其將用來與 FCM 互動。

設定 FCM：獲取寄件者 ID 和私鑰檔案

要設定 FCM：

1. 在 Google 入口註冊。
2. 前往Firebase 主控台。
3. 執行以下操作之一：
   - 若要建立新項目，請按一下**建立項目**並按照螢幕上的指示進行操作。
   - 開啟現有項目。
4. 點擊齒輪圖示並選擇**項目設定**。
   項目設定視窗將開啟。
5. 選擇**Cloud Messaging**頁簽。
6. 從**Firebase Cloud Messaging API (V1)**部分的**寄件者 ID**欄位中檢索相關寄件者 ID。

7. 選擇**服務帳戶**頁簽，然後按一下**產生新私鑰**。

8. 在開啟的視窗中，按一下**產生金鑰**以產生並下載私鑰檔案。

Firebase Cloud Messaging 現已配置。

與公共金鑰基礎架構整合

與公共金鑰基礎架構 (PKI) 整合旨在管理伺服器對網域使用者憑證的發佈。

管理員可以在管理主控台中為使用者分配網域憑證。這可以使用以下方法完成：

- 在憑證建立精靈中，從檔案將特別（自訂）憑證指派給使用者。
- 執行與 PKI 的整合並分配 PKI 以作為制定類型憑證或所有類型憑證的憑證來源。

與 PKI 整合的設定可在 **行動裝置管理 / 憑證**資料夾中取得，方法是點擊**與公共金鑰基礎架構整合**連結。

用於網域使用者憑證發佈的與 PKI 整合的一般原則

在管理主控台的**行動裝置管理 / 憑證**資料夾工作區中點擊**與公共金鑰基礎架構整合**連結，以指定管理伺服器用來透過網域 CA（這指的是執行 PKI 整合的帳戶）發佈網域使用者憑證的網域帳戶。

請注意以下：

- 與 PKI 整合的設定允許您為所有類型的憑證指定預設範本。請注意，憑證發佈規則（可在**行動裝置管理 / 憑證**資料夾工作區點擊**配置憑證發佈規則**按鈕取得）可讓您為每種類型的憑證指定各自的範本。
- 特殊 Enrollment Agent (EA) 憑證必須安裝在管理伺服器裝置，在與 PKI 整合的帳戶的憑證儲存區中。Enrollment Agent (EA) 憑證由網域 CA (Certificate Authority) 管理員發佈。

與 PKI 整合的帳戶必須滿足以下標準：

- 它是網域使用者。
- 它是發起與 PKI 的整合的管理伺服器裝置本機管理員。
- 它具有*作為服務登入*的權限。
- 管理伺服器裝置必須在此帳戶下執行至少一次以建立永久使用者設定檔。

卡巴斯基安全管理中心網頁伺服器

卡巴斯基安全管理中心網頁伺服器（以下簡稱"網頁伺服器"）是卡巴斯基安全管理中心的一個元件。網頁伺服器用於發佈獨立安裝套件、行動裝置獨立安裝套件和共用資料夾的檔案。

所建立的安裝套件被自動發佈在網頁伺服器並在第一次下載後被刪除。管理員可以以任意方式例如電子郵件等方式將新連結傳送給使用者。

透過點擊連結，使用者可將所需資訊下載至行動裝置。

如果需要網頁伺服器的 fine-tuning，其內容允許您變更 HTTP (8060) 和 HTTPS (8061) 連接埠。除了變更連接埠，您可以為 HTTPS 取代伺服器憑證並為 HTTP 變更網頁伺服器的 FQDN。

其他日常工作

該部分提供佈署卡巴斯基安全管理中心的一般使用建議。

在管理控制台中監控交通信號燈和記錄的事件

管理主控台允許您透過檢查信號燈快速評估目前卡巴斯基安全管理中心狀態和受管理裝置。信號燈會顯示在**管理伺服器**節點的工作區，此工作區位於**監控**標籤上。頁籤提供了帶有信號燈的六個資訊面板。信號燈是面板左側的彩色欄。每個帶有信號燈的面板對應於卡巴斯基安全管理中心的特定功能範圍（參見下表）。

管理主控台中信號燈覆蓋的範圍

面板名稱	信號燈範圍
佈署	在組織網路裝置上安裝網路代理和安全應用程式
管理方案	管理群組結構。網路掃描。裝置移動規則
防護設定	安全應用程式功能：防護狀態、惡意軟體掃描
更新	更新和修補程式
監控	防護狀態
管理伺服器	管理伺服器功能和屬性

每個信號燈可以變換四種顏色（參見下表）。信號燈的顏色取決於卡巴斯基安全管理中心的目前狀態和記錄的事件。

信號燈的顏色碼

狀態	信號燈顏色	信號燈顏色意義
資訊	綠色	不需要管理員介入。
警告	黃色	需要管理員介入。
緊急	紅色	發生了嚴重問題。需要管理員介入以解決。
資訊	淡藍色	與受管理裝置的潛在或實際威脅無關的事件被記錄。

管理員的目標是，保持**監控**標籤上所有資訊視窗的信號燈都是綠燈。

資訊面板還顯示影響紅綠燈和 Kaspersky Security Center 狀態的記錄事件（見下表）。

信號燈顏色	事件類型顯示名稱	事件類型	敘述
紅色	**%1 台裝置上的產品授權已到期**	IDS_AK_STATUS_LIC_EXPAIRED	當商業授權到期時，會發生此類事件。 卡巴斯基安全管理中心每天會檢查一次產品授權是否接近到期日。 當商業授權到期時，卡巴斯基安全管理中心僅提供基本功能。 要繼續使用卡巴斯基安全管理中心，您必須續約您的正式產品授權。
紅色	**安全應用程式沒有執行：%1 台裝置**	IDS_AK_STATUS_AV_NOT_RUNNING	當安裝在裝置上的安全應用程式未運行時，會發生此類事件。 確保 Kaspersky Endpoint Security 正在裝置上運行。
紅色	**已停用防護：%1 台裝置**	IDS_AK_STATUS_RTP_NOT_RUNNING	當裝置上的安全應用程式被停用的時間比指定時間間隔，會發生此類事件。 檢查即時防護現狀在裝置上並確保啟用了您需要的所有保護組件。
紅色	**在裝置上偵測到軟體弱點**	IDS_AK_STATUS_VULNERABILITIES_FOUND	當*查找漏洞和所需的更新*工作在裝置上安裝的應用程式偵測到具有指定嚴重級別的漏洞，會發生此類事件。 管理員可在**Application management**資料夾包含的**Software updates**子資料夾中檢視可用更新的清單。該資料夾包含了管理伺服器擷取的可以被發佈到裝置的 Microsoft 應用程式和其他軟體廠商產品的更新清單。 查看有關可用更新的資訊後，在裝置上安裝更新。
紅色	**管理伺服器上註冊了緊急事件**	IDS_AK_STATUS_EVENTS_OCCURED	當偵測到管理伺服器緊急事件，會發生此類事件。 檢查儲存在管理伺服器上的事件列表，然後將緊急事件一一修復。
紅色	**管理伺服器上記錄了錯誤事件**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	當在管理伺服器端記錄意外錯誤時，會發生此類事件。 檢查儲存在管理伺服器上的事件列表，然後一一修復錯誤。
紅色	**失去與 %1 台裝置的連線**	IDS_AK_STATUS_ADM_LOST_CONTROL1	當管理伺服器和裝置之間的連接遺失時，會發生此類事件。 查看斷開連接的裝置列表並嘗試重新連接它們。
紅色	**%1 台裝置已長時間未連線到管理伺服器**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	當由於裝置關閉，裝置在指定時間間隔內未連線到管理伺服器，會發生此類事件。 確保裝置已打開並且網路代理正在運行。
紅色	**有 %1 台裝置的狀態異常**	IDS_AK_STATUS_HOST_NOT_OK	當連接到管理伺服器的裝置 *OK* 狀態變更為*緊急*或者*警告*，會發生此類事件。 您可以使用以下方法解決問題 Kaspersky Security Center 遠程診斷實用程序。
紅色	**資料庫過期： %1 台裝置**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	當裝置上的防毒資料庫未在指定時間間隔內更新時，會發生此類事件。 按照說明進行操作更新卡巴斯基資料庫。

信號燈顏色	事件類型顯示名稱	事件類型	敘述
紅色	**Windows Update 更新檢查長時間沒有執行的裝置：%1**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	當「*執行 Windows 更新同步*」工作在指定時間間隔內未執行，會發生此類事件。 按照說明進行操作 將來自 Windows Update 的更新與管理伺服器同步。
紅色	**卡巴斯基安全管理中心的 %1 個外掛程式必須安裝**	IDS_AK_STATUS_PLUGINS_REQUIRED2	當您需要為 Kaspersky應用程式安裝附加外掛程式時，會發生此類事件。 下載並安裝卡巴斯基應用程式所需的管理外掛程式 卡巴斯基技術支援網頁。
紅色	**在 %1 台裝置上偵測到活動威脅。**	IDS_AK_STATUS_NONCURED_FOUND	當在受管理裝置上偵測到活動威脅時，就會發生此類事件。 檢視有關偵測到的威脅的資訊，然後按照建議進行操作。
紅色	**工作 %1 已完成但存在錯誤**	IDS_AK_STATUS_TASK_FAILED	當工作執行完成但出現錯誤時，會發生此類事件。 檢查工作的屬性，然後重新配置工作。
紅色	**偵測到大量病毒：%1 台裝置**	IDS_AK_STATUS_TOO_MANY_THREATS	當在受管理裝置上偵測到病毒時，就會發生此類事件。 檢視有關偵測到的病毒的資訊，然後按照建議進行操作。
紅色	**病毒爆發**	IDS_AK_STATUS_VIRUS_OUTBREAK	當短時間內在若干受管理裝置上偵測到的惡意物件數量超過上限值時，該類型的事件發生。 檢視有關偵測到的威脅的資訊，然後按照建議進行操作。
紅色	**儲存區中的資料庫已長時間未更新**	IDS_AK_STATUS_UPD_SERVER_NOT_UPTODATE	當裝置上的防毒資料庫兩天未更新時，會發生此類事件。 檢查防毒資料庫的更新頻率，然後更新防毒資料庫。
黃色	**儲存區中的資料庫已長時間未更新**	IDS_AK_STATUS_UPD_SERVER_NOT_UPTODATE	當裝置上的防毒資料庫超過一天但少於兩天未更新時，就會發生此類事件。 檢查防毒資料庫的更新頻率，然後更新防毒資料庫。
黃色	**裝置上偵測到 NetBIOS 名稱衝突**	IDS_AK_STATUS_ADM_NAME_CONFLICT	當裝置具有相同的 NetBIOS 名稱時，就會發生此類事件。 重命名裝置。
黃色	**在 %s 台裝置上，資料加密已轉換到裝置狀態偵測標準中指定的狀態**	IDS_AK_STATUS_ENCRYPTION_FAULTS_FOUND	當在受管理裝置上資料加密失敗時，就會發生此類事件。
黃色	**產品授權 %1 還有 %2 天到期**	IDS_AK_STATUS_LIC_EXPAIRING	當裝置上的產品授權在指定天數內到期時，就會發生此類事件。 要繼續使用卡巴斯基安全管理中心，您必須續約您的正式產品授權。
黃色	**安裝了網路代理的未配置的裝置：%1**	IDS_AK_STATUS_NAGENTS_IN_UNASSIGNED	當網路上發現新裝置時，就會發生此類事件。 將具有網路代理程式的裝置移至受管理裝置群組。
黃色	**重新啟動之前，%1 裝置上的網路代理無法執行。上一次，此狀態為 %2**	IDS_AK_STATUS_NAGENTS_NOT_RUNNING_UNTIL_REBOOT	當網路代理未在裝置上執行時，會發生此類事件。 重新啟動裝置。

信號燈顏色	事件類型顯示名稱	事件類型	敘述
黃色	**偵測到的檔案必須傳送至 Kaspersky 以供進一步分析**	IDS_AK_STATUS_NEW_APS_FILE_APPEARED	當偵測到可能感染病毒的檔案並將其移至隔離區時，就會發生此類事件。 將檔案傳送給卡巴斯基進行進一步分析。
黃色	**受管理裝置：%1。安全應用程式安裝在：%2 台裝置**	IDS_AK_STATUS_NO_AV	當 Kaspersky Endpoint Security 未安裝在所有受管理裝置上時，會發生此類事件。 在所有受管理裝置上安裝 Kaspersky Endpoint Security。
黃色	**安裝工作 %1 已在 %2 台裝置上成功完成；%3 台裝置需要重新啟動**	IDS_AK_STATUS_RI_NEED_REBOOT	當 Kaspersky Endpoint Security 剛安裝在受管理裝置上時，會發生此類事件。 安裝 Kaspersky Endpoint Security 後重新啟動裝置。
黃色	**惡意軟體掃描已長時間未執行：%1 台裝置**	IDS_AK_STATUS_SCAN_LATE	當您需要在受管理裝置上執行惡意軟體掃描時，會發生此類事件。 執行病毒掃描。
黃色	**偵測到軟體弱點的裝置：%1**	IDS_AK_STATUS_VULNERABLE_HOSTS_FOUND	當在受管理裝置上偵測到弱點時，就會發生此類事件。 檢視有關偵測到的弱點的資訊並修復它們。
綠色	**受管理裝置：%3。偵測到未分配的裝置：%1**	IDS_AK_STATUS_ADM_OK1	當在管理群組中偵測到新裝置時，會發生此類事件。
綠色	**安全應用程式被安裝在所有受管理的裝置**	IDS_AK_STATUS_DEPLOYMENT_OK	當 Kaspersky Endpoint Security 安裝在所有受管理裝置上時，會發生此類事件。
綠色	**卡巴斯基安全管理中心正在正常執行**	IDS_AK_STATUS_GENERAL_OK	當卡巴斯基安全管理中心正常運作時，會發生此類事件。
綠色	**沒有安裝即時防護程式**	IDS_AK_STATUS_RTP_NA	當受管理裝置上未安裝病毒防護應用程式時，會發生此類事件。
綠色	**防護已啟用**	IDS_AK_STATUS_RTP_OK	當在受管理裝置上啟用即時防護時，會發生此類事件。
綠色	**安全應用程式未安裝**	IDS_AK_STATUS_SCAN_NA	當受管理裝置上未安裝病毒防護應用程式時，會發生此類事件。
綠色	**惡意軟體掃描正依照排程執行**	IDS_AK_STATUS_SCAN_OK	當*惡意軟體掃描*工作按排程執行時，會發生此類事件。
綠色	**上次更新更新儲存區的時間：%1**	IDS_AK_STATUS_UPD_OK	更新儲存庫進行更新時會發生此類事件。
淡藍色	**儲存區中的資料庫已長時間未更新**	IDS_AK_STATUS_UPD_SERVER_NOT_UPTODATE	當防毒資料庫在白天更新時，就會發生此類事件。
淡藍色	**接受的卡巴斯基安全網路聲明已過時**	IDS_AK_STATUS_ACCEPTED_KSN_AGREEMENT_OBSOLETE	當卡巴斯基安全網路聲明過期時，就會發生此類事件。
淡藍色	**卡巴斯基軟體更新尚未得到批准**	IDS_AK_STATUS_APPLICABLE_KL_PATCHES_NOT_APPROVED	當管理員尚未批准受管理卡巴斯基應用程式的適用修補程式時，就會發生此類事件。
淡藍色	**Kaspersky 應用程式更新已被取消**	IDS_AK_STATUS_APPLICABLE_KL_PATCHES_REVOKED	當管理員尚未拒絕已撤銷的修補程式時，就會發生此類事件。
淡藍色	**Kaspersky 行動軟體的最終使用者產品授權協議未被接受**	IDS_AK_STATUS_KL_MOBILE_EULAS_NOT_ACCEPTED	當管理員尚未接受卡巴斯基行動軟體的最終使用者產品授權協議時，就會發生此類事件。

信號燈顏色	事件類型顯示名稱	事件類型	敘述
淡藍色	**Kaspersky 軟體更新的最終使用者產品授權協議未被接受**	IDS_AK_STATUS_KL_PATCHES_EULAS_NOT_ACCEPTED	當管理員尚未接受卡巴斯基軟體更新的最終使用者產品授權協議時，就會發生此類事件。
淡藍色	**關於卡巴斯基軟體更新的卡巴斯基安全網路聲明尚未被接受**	IDS_AK_STATUS_KL_PATCHES_KSN_AGREEMENTS_NOT_ACCEPTED	當管理員尚未接受卡巴斯基軟體更新的卡巴斯基安全網路聲明時，就會發生此類事件。
淡藍色	**您必須接受產品授權協議以安裝更新**	IDS_AK_STATUS_NEED_ACCEPT_EULA	當有新的更新可供安裝但管理員尚未接受產品授權協議時，會發生此類事件。
淡藍色	**Kaspersky 應用程式的新版本已可用**	IDS_AK_STATUS_NEW_DISTRIBUTIVES_AVAILABLE	當新版本的卡巴斯基應用程式可在受管理裝置上安裝時，就會發生此類事件。
淡藍色	**有卡巴斯基安全管理中心元件更新可用**	IDS_AK_STATUS_NEW_KSC_VERSIONS_AVAILABLE	當卡巴斯基安全管理中心元件有可用更新時，會發生此類事件。
淡藍色	**有 Kaspersky 應用程式更新可用**	IDS_AK_STATUS_NEW_VERSIONS_AVAILABLE	當卡巴斯基應用程式有可用更新時，就會發生此類事件。
淡藍色	**應用程式安裝工作 %1 已在 %2 台裝置上成功完成，在 %3 台裝置上失敗**	IDS_AK_STATUS_RI_FAILED	當*應用程式安裝*工作僅在指定集區中的某些裝置上安裝軟體時，會發生此類事件。
淡藍色	**執行佈署工作 - %1 (%2%%)**	IDS_AK_STATUS_RI_RUNNING	當部署工作在受管理裝置上執行時，會發生此類事件。
淡藍色	**在 %1 台裝置上從未執行過完整掃描**	IDS_AK_STATUS_SCAN_NOT_SCANNED	當從未對指定數量的裝置執行完整掃描時，會發生此類事件。
淡藍色	**正在執行更新下載工作（進度：%1%%）**	IDS_AK_STATUS_UPD_SRV_UPDATE_IN_PROGRESS	當下載更新工作在受管理裝置上執行時，會發生此類事件。

遠端存取受管理裝置

該部分提供了遠端存取受管理裝置的資訊。

使用“不要中斷與管理伺服器的連線”選項在受管理裝置和管理伺服器之間提供持續連線

如果您不使用推送伺服器，則卡巴斯基安全管理中心不提供受管理裝置和管理伺服器之間的持續連線。受管理裝置上的網路代理定期建立連線並與管理伺服器同步。同步工作階段的間隔定義在網路代理政策中。如果需要提前同步，管理伺服器（或發佈點，如果正在使用）將透過 IPv4 或 IPv6 網路將簽名的網路資料包發送到網路代理的 UDP 連接埠。預設情況下，埠號指定為 15000。如果在管理伺服器和受管理裝置之間無法建立 UDP 連線，同步將在下次網路代理和管理伺服器一般連線時在同步間隔內執行。

如果沒有網路代理和管理伺服器之間的提前連線，某些操作將無法執行，例如執行和停止本機工作、接收受管理應用程式的統計資訊或建立隧道。要解決此問題，如果您不使用推送伺服器，您可以使用**不斷開與管理伺服器的連線**選項來確保受管理裝置和管理伺服器之間存在持續連線。

要提供受管理裝置與管理伺服器之間的持續連線：

1. 在主控台樹狀目錄中，選擇**受管理裝置**資料夾。
2. 在資料夾的工作區中，選擇要用其提供持續連線的受管理裝置。
3. 在裝置的上下文功能表中，選取**內容**。
   所選裝置的內容視窗開啟。
4. 在所顯示視窗的**一般**區段中，選擇**不斷開與管理伺服器的連線**選項。

持續連線會在受管理裝置和管理伺服器之間建立。

不斷開與管理伺服器的連線選項所能選取的最大裝置總數是 300。

關於檢查裝置和管理伺服器之間的連線時間

在關閉裝置時，網路代理通知管理伺服器該事件。在裝置顯示為已關閉的管理主控台。然而，網路代理無法通知管理伺服器所有此類事件。因此，管理伺服器會定期分析每台裝置的**連線至管理伺服器**內容（內容值會顯示在管理主控台，在裝置內容中的**一般**區域），並將它與網路代理目前設定中的同步間隔相比較。如果一台裝置在超過三次成功的同步間隔後未回應，該裝置被標記為已關閉。

關於強制同步

儘管卡巴斯基安全管理中心自動為受管理裝置同步狀態、設定、工作和政策，一些情況下，管理員需要準確知道是否同步已經在指定裝置上執行。

在管理主控台受管理裝置的上下文功能表中，**所有工作**功能表包含**強制同步**命令。當卡巴斯基安全管理中心 14.2 執行該指令時，管理伺服器試圖連線到裝置。如果該嘗試成功，強制同步將被執行。否則，同步將僅在網路代理與管理伺服器的下一次排程連線後被強制。

關於通道

卡巴斯基安全管理中心允許透過管理伺服器的從管理主控台的 TCP 連線通道，然後透過網路代理到受管理裝置上的指定連接埠。通道設計用於連線安裝管理主控台的裝置上的用戶端應用程式到受管理裝置上的 TCP 連接埠—如果管理主控台和目的裝置之間沒有直接連線可用。

例如，通道用於連線到遠端桌面，可以連線到已存在連線，也可以建立一個新的遠端連線。

通道也可以使用外部工具啟用。例如，管理員可以執行 putty 公用程式、VNC 用戶端和其他工具。

度量手冊

該部分提供了卡巴斯基安全管理中心尺寸資訊。

關於本手冊

卡巴斯基安全管理中心 14.2（也稱為卡巴斯基安全管理中心）Sizing Guide 專為安裝管理卡巴斯基安全管理中心的專業人員，以及為使用卡巴斯基安全管理中心的企業提供技術支援的人員而設計。

所有建議都給予由卡巴斯基安全管理中心管理安裝了 Kaspersky 軟體的裝置（包括行動裝置）的防護的網路。如果行動裝置、或者工作其他受管理裝置要被特殊考慮，這將特別闡述。

要在不同的操作條件下獲取和維持最佳化執行，您必須考慮網路裝置數量、網路拓撲和您需要的卡巴斯基安全管理中心功能集。

此手冊提供下列資訊：

- 卡巴斯基安全管理中心的限制
- 卡巴斯基安全管理中心關鍵節點的限制（管理伺服器和發佈點）：
  - 管理伺服器和發佈點的硬體需求
  - 管理伺服器數量和層級限制
  - 計算發佈點的數量和配置
- 資料庫中的事件記錄配置取決於網路裝置的數量
- 效能最佳化的常見最佳實踐
- 特定工作的配置旨在最佳化卡巴斯基安全管理中心的效能
- 卡巴斯基安全管理中心管理伺服器和每個受防護裝置間的流量率（網路負載）

以下情況下建議參考該文件：

- 當在安裝卡巴斯基安全管理中心前排程資源時
- 當向佈署了卡巴斯基安全管理中心的網路排程顯著變更時
- 在企業網路的受限網段（測試環境）中，從使用卡巴斯基安全管理中心切換至以完整規模佈署卡巴斯基安全管理中心
- 當對使用的卡巴斯基安全管理中心功能集做變更時

卡巴斯基安全管理中心的限制資訊

下表顯示卡巴斯基安全管理中心目前版本的限制。

卡巴斯基安全管理中心的限制

限制類型	參數值
每個管理伺服器的最大受管理裝置數量	100,000
選取**不斷開與管理伺服器的連線**選項時的裝置數量上限。	300
管理群組最大數量	10,000
要儲存的事件的最大數量	45,000,000
政策的最大數量	2000
工作的最大數量	2000
Active Directory 物件的最大總數（組織單元 (OU) 和使用者帳戶、裝置和安全群組）	1,000,000
政策中設定檔的最大數量	100
單一主管理伺服器的從屬管理伺服器的最大數量	500
虛擬管理伺服器的最大數量	500
單一發佈點可以覆蓋的最大裝置數量（發佈點僅可以覆蓋非行動裝置）	10,000
可以使用單一連線閘道的最大裝置數量	10,000，包括行動裝置
每個管理伺服器的最大行動裝置數量	100,000 減去固定的受管理裝置數量

管理伺服器計算

該部分提供了管理伺服器裝置的軟體和硬體需求。也提供了根據組織網路設定計算管理伺服器數量和層級的建議。

管理伺服器的硬體資源計算

該部分包含為計畫管理伺服器的硬體資源提供精靈的計算。當使用弱點和修補程式管理功能時還建議計算磁碟空間。

DBMS 和管理伺服器的硬體需求

下表給出了測試中獲取的 DBMS 和管理伺服器的建議最小硬體需求。對於支援的作業系統和 DBMS 的完整清單，請參考硬體和軟體需求清單。

管理伺服器和 DBMS 位於不同裝置，網路包含 50,000 部裝置

安裝了管理伺服器的裝置的配置。

硬體	參數值
CPU	4 核心，2 500 MHz
RAM	8 GB
硬碟磁碟機	300 GB，RAID（建議）
網卡	1 Gbit

安裝了 DBMS 的裝置的配置

硬體	參數值
CPU	4 核心，2 500 MHz
RAM	16 GB
硬碟磁碟機	200 GB，SATA RAID
網卡	1 Gbit

管理伺服器和 DBMS 位於相同裝置，網路包含 50,000 台裝置

安裝了管理伺服器和 DBMS 的裝置的配置

硬體	參數值
CPU	8 核心，2 500 MHz
RAM	16 GB
硬碟磁碟機	500 GB，SATA RAID
網卡	1 Gbit

管理伺服器和 DBMS 位於不同裝置，網路包含 100,000 部裝置

安裝了管理伺服器的裝置的配置。

硬體	參數值
CPU	8 核，2.13 GHz
RAM	8 GB
硬碟磁碟機	1 TB，RAID
網卡	1 Gbit

已安裝 DBMS 的裝置的配置

硬體	參數值
CPU	8 核，2.53 GHz
RAM	26 GB
硬碟磁碟機	500 GB，SATA RAID
網卡	1 Gbit

虛擬機上的 DBMS SQL Server，網路包括 50,000 個裝置

安裝了 SQL Server 的虛擬機的配置，最多 50,000 個裝置

Hypervisor 上保留的資源	參數值
CPU	10 GHz
RAM	16 GB
磁碟 IOPS	150 IOPS
磁碟可用空間	200 GB
SQL Server 實例共用	不共用

虛擬機上的 DBMS SQL Server，網路包括 100,000 個裝置

安裝了 SQL Server 的虛擬機的配置，最多 100,000 個裝置

Hypervisor 上保留的資源	參數值
CPU	20 GHz
RAM	26 GB
磁碟 IOPS	150 IOPS
磁碟可用空間	500 GB
SQL Server 實例共用	不共用

測試在以下系統上執行：

- 自動分配發佈點在管理伺服器上啟用，或者發佈點根據建議的表格被手動指定。
- 備份工作儲存備份副本到位於專用伺服器的檔案資源。
- 網路代理的同步間隔按下表設定。

  網路代理同步間隔

同步間隔（分鐘）	受管理裝置數量
15	10,000
30	20,000
45	30,000
60	40,000
75	50,000
150	100,000

資料庫空間計算

必須在資料庫中保留的大約空間可以使用以下公式計量：

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), KB

其中：

- C 是裝置數量。
- E 要儲存的事件的數量。
- A 是 Active Directory 物件的總數：
  - 裝置帳戶
  - 使用者帳戶
  - 安全群組帳戶
  - Active Directory 組織單元

  如果 Active Directory 掃描被停用，A 等效於 0。
- N 是端點裝置上已清查可執行檔的平均數目。
- F 是端點裝置的數目，其中可執行檔已清查。

如果您計畫在 Kaspersky Endpoint Security 政策設定中啟用通知管理伺服器您執行的應用程式，您將需要額外空間 (0.03 * C GB) 在資料庫中儲存您執行的應用程式資訊。

如果管理伺服器發佈 Windows 更新（做為 Windows Server Update Services 伺服器），資料庫將需要額外的 2.5 GB。

操作期間，一定的*未佔用時間*總是出現在資料庫。因此，資料庫檔案的實際尺寸（預設下，如果您使用 SQL Server 作為 DBMS 的話，是 KAV.MDF 檔案）經常是兩倍於資料庫中被佔用空間的尺寸。

不建議明確限制透明日誌（預設下，檔案 KAV_log.LDF，如果您使用 SQL Server 作為 DBMS）的大小。建議保留 MAXSIZE 參數的預設值。然而，如果您必須限制該檔案的大小，請考慮對於 KAV_log.LDF，參數 MAXSIZE 的典型必要最小值是 20480 MB。

磁碟空間計算（使用或不使用弱點和修補程式管理功能）

磁碟空間計算（不使用弱點和修補程式管理功能）

管理伺服器需要的磁碟空間 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit 資料夾可以使用以下公式估算：

(724 * C + 0.15 * E + 0.17 * A)，KB

其中：

- C 是裝置數量。
- E 要儲存的事件的數量。
- A 是 Active Directory 物件的總數：
  - 裝置帳戶
  - 使用者帳戶
  - 安全群組帳戶
  - Active Directory 組織單元

如果 Active Directory 掃描被停用，A 等效於 0。

附加磁碟空間計算（使用弱點和修補程式管理功能）

- 更新。共用資料夾額外需要至少 4 GB 來儲存更新。
- 安裝套件。如果一些安裝套件儲存在管理伺服器，共用資料夾將需要額外磁碟空間，等於所有要安裝的應用程式套裝的總大小。
- "遠端安裝"工作。如果管理伺服器上有任何遠端安裝工作，額外的磁碟空間（在 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit 資料夾），與要安裝的所有安裝套件大小相當。
- 修補程式。如果管理伺服器需要安裝修補程式，將需要額外的磁碟空間：
  - 修補程式資料夾應該具有與下載的所有修補程式的總大小相當的磁碟空間。預設情況下，修補程式儲存在 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles 資料夾中。

    您可以使用 klsrvswch 公用程式指定用於儲存修補程式的不同資料夾。klsrvswch 公用程式位於安裝管理伺服器的資料夾中。預設安裝路徑：<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

    如果管理伺服器被用作 WSUS 伺服器，建議您分配至少 100 GB 到該資料夾。
  - %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit 資料夾必須具有與更新安裝和弱點修復工作所引用的修補程式的總大小相當的磁碟空間。

計算管理伺服器的數量和配置

要減少主管理伺服器負載，您可以分配另外的管理伺服器到每個管理群組。每個主管理伺服器的從屬管理伺服器的數量不能超過 500。

我們建議您基於您組織網路的設定來建立管理伺服器設定。

將動態虛擬機連線到卡巴斯基安全管理中心時的建議事項

動態虛擬機（也稱為動態 VM）比靜態虛擬機消耗更多資源。

有關動態虛擬機的更多資訊，請參閱對動態虛擬機的支援。

連線新的動態 VM 時，卡巴斯基安全管理中心會在管理主控台中為該動態 VM 建立一個圖示並將動態 VM 移至管理群組。此後，動態 VM 會被新增到管理伺服器資料庫中。管理伺服器與安裝在該動態 VM 上的網路代理完全同步。

在組織的網路中，網路代理會為每個動態 VM 建立以下網路清單：

- 硬體
- 安裝的軟體
- 偵測到的弱點
- 應用程式控制元件的事件和可執行檔清單

網路代理會將這些網路清單傳輸到管理伺服器。網路清單的大小取決於安裝在動態 VM 上的元件，並且可能會影響卡巴斯基安全管理中心和資料庫管理系統 (DBMS) 的效能。請注意，負載可以非線性增長。

在使用者完成使用動態 VM 並將其關閉後，該機器將從虛擬基礎架構中移除，並且有關該機器的項目也將從管理伺服器資料庫中移除。

所有這些操作都會消耗大量卡巴斯基安全管理中心和管理伺服器資料庫資源，並會降低卡巴斯基安全管理中心和 DBMS 的效能。我們建議您最多將 20,000 個動態 VM 連線到卡巴斯基安全管理中心。

如果連線的動態 VM 執行標準操作（例如，資料庫更新）並且消耗不超過 80% 的記憶體和 75-80% 的可用核心，您可以將超過 20,000 個動態 VM 連線到卡巴斯基安全管理中心。

更改動態 VM 上的政策設定、軟體或作業系統可以減少或增加資源消耗。80-95% 的資源消耗被視為最佳。

發佈點和連線閘道的計算

該部分提供了用作發佈點的裝置的硬體需求，以及根據企業網路配置計算發佈點和連線閘道數量的建議。

發佈點需求

若要處理多達 10,000 部用戶端裝置，發佈點必須至少滿足以下需求（已提供測試機器配置）：

- CPU：Intel® Core™ i7-7700 CPU, 3.60 GHz 4 核心。
- RAM：8 GB。
- 可用儲存空間：120 GB。

不建議指派管理伺服器為發佈點，因為這將增加管理伺服器上的負荷。

如果管理伺服器上有任何遠端安裝工作等待，帶有發佈點的裝置也會請求一定的剩餘磁碟空間，這些空間與要安裝的安裝套件大小相當。

如果管理伺服器上有一個或多個更新（修補程式）安裝和弱點修復工作實例，帶有發佈點的裝置也會請求一定的剩餘磁碟空間，這些空間相當於兩倍的修補程式總大小。

如果在發佈點直接從卡巴斯基更新伺服器接收資料庫更新和應用程式軟體模組時使用該方案，則發佈點必須連線到網際網路。

計算發佈點的數量和配置

網路包含越多的用戶端裝置，就需要越多的發佈點。我們建議您停用發佈點的自動分配。當發佈點的自動分配被啟用時，如果用戶端裝置數量很大，管理伺服器就分配發佈點並定義其配置。

使用單獨分配的發佈點

如果您計畫使用特定裝置作為發佈點（就是，單獨分配的伺服器），您可以不使用發佈點的自動分配。此種情況下，確保您要分配為發佈點的裝置具有足夠的剩餘磁碟空間磁區，不定期關閉，且停用了睡眠模式。

網路中基於網路裝置數量被專門分配的包含單一網段的發佈點的數量

網段中的用戶端裝置的數量	發佈點數量
少於 300	0（不分配發佈點）
大於 300	可接受：(N/10,000 + 1)，建議：(N/5000 + 2)，N 是網路裝置數量

網路中基於網路裝置數量被專門分配的包含多個網段的發佈點的數量

每個網段中的用戶端裝置的數量	發佈點數量
少於 10	0（不分配發佈點）
10–100	1
大於 100	可接受：(N/10000 + 1)，建議：(N/5000 + 2)，N 是網路裝置數量

使用標準用戶端裝置（工作站）作為發佈點

如果您計畫使用標準用戶端裝置（就是，工作站）作為發佈點，我們建議您按照所示分配發佈點（參見下表），以便避免通信管道和管理伺服器超載。

網路中基於網路裝置數量作為發佈點工作的包含單一網段的工作站的數量

網段中的用戶端裝置的數量	發佈點數量
少於 300	0（不分配發佈點）
大於 300	(N/300 + 1)，N 是網路裝置數量；至少有三台發佈點

網路中基於網路裝置數量作為發佈點工作的包含多個網段的工作站的數量

每個網段中的用戶端裝置的數量	發佈點數量
少於 10	0（不分配發佈點）
10–30	1
31–300	2
大於 300	(N/300 + 1)，N 是網路裝置數量；至少有三台發佈點

如果裝置被關閉（或由於某些原因不可用），其範圍內的受管理裝置可以存取管理伺服器以更新。

連線閘道數量計算

如果您計畫使用連線閘道，我們建議您為該功能指定特別的裝置。

一個連線閘道可以覆蓋最多 10,000 台受管理裝置，包括行動裝置。

工作和政策事件資訊的記錄

本節提供了管理伺服器資料庫中的事件儲存計算，並提供如何最小化事件數量的建議，從而降低管理伺服器負載。

預設下，每個工作和政策的內容可以用於儲存所有工作執行和政策施加的相關事件。

然而，如果工作執行過於頻繁（例如，每週多於一次）且在大量裝置間（例如，多於 10,000 台），事件數量可能過大且事件可能溢出資料庫。此種情況下，建議選取工作設定的兩個選項中的一個：

- **儲存工作進度相關事件**。此種情況下，資料庫僅從執行工作的每個裝置接收工作啟動、進度和完成資訊（成功、帶有警告或錯誤）。
- **僅儲存工作執行結果**。此種情況下，資料庫僅從執行工作的每個裝置接收工作完成資訊（成功、帶有警告或錯誤）。

如果政策為大數量裝置定義（例如，多於 10,000 台），事件數量可能很大且事件可能溢出資料庫。此種情況下，建議在政策設定中僅選取最關鍵的事件並啟用它們的記錄。建議您停用所有其他事件的記錄。

為此，您將降低資料庫中的事件數量，提高與資料庫中事件表分析相關之情境的執行速度，並降低緊急事件被大數量事件覆寫的風險。

您也可以降低工作或政策相關事件的儲存期限。預設期限是工作相關事件 7 天和政策相關事件 30 天。當變更事件儲存期限時，請考慮您組織的工作過程和系統管理員可以分析每個事件的時間。

建議在以下情況修改事件儲存設定：

- 關於群組工作中間狀態變化的事件，以及關於套用政策的事件，在卡巴斯基安全管理中心的所有事件中佔據很大的比例。
- 當超過資料庫中儲存的事件總數限制時，卡巴斯基事件記錄就會開始顯示自動移除事件的相關項目。

以每天每部裝置的事件數量不超過 20 個為假設基準，來選擇事件記錄選項。如果必要，您可以稍微增加該限制，但僅是在您網路中的裝置數量相對小時（少於 10,000 台）。

特別考慮和特定工作的最佳化設定

特定工作受制於基於網路裝置數量的特別考慮。該部分提供了此類別工作設定的最佳化設定建議。

裝置發現、資料備份工作、管理伺服器維護工作和更新 Kaspersky Endpoint Security 的群組工作是卡巴斯基安全管理中心的基本功能部分。

裝置發現頻率

不建議增加裝置發現的預設頻率，因為這可以增加網域控制器負載。相反，建議使用您組織需要的最小頻率排程輪詢。計算最佳化排程的建議提供在下表。

裝置發現排程

網路裝置數量	建議的裝置發現頻率
少於 10,000	預設頻率或更低
10,000 或更多	每天一次或更低

管理伺服器資料備份工作和管理伺服器維護工作

當以下工作執行時管理伺服器停止工作：

- 備份管理伺服器資料
- 管理伺服器維護

當這些工作執行時，資料庫無法接收任何資料。

您可能必須重新排程這些工作以便它們和其他管理伺服器工作不同時執行。

更新 Kaspersky Endpoint Security 的群組工作

如果管理伺服器作為更新來源，Kaspersky Endpoint Security 10 和後續版本的群組更新工作的建議排程選項是**當新更新下載至儲存區時**，其中**使用工作啟動自動隨機延遲**核取方塊被選擇。

如果從 Kaspersky 伺服器下載更新到儲存區的本機工作已在每個發佈點上建立，時段性排程將被建議給 Kaspersky Endpoint Security 群組更新工作。隨機時段值必須是一小時。

清查工作

> 您可以在獲取可執行檔的資訊時降低資料庫的負載。為此，我們建議您在安裝了標準軟體集合的參考裝置上為 Kaspersky Endpoint Security 執行清查工作。

管理伺服器從單個裝置接收的可執行檔數量不能超過 150,000。當卡巴斯基安全管理中心達到了該限制，它無法接收任何新檔案。

通常，一般用戶端裝置上的檔案數量不超過 60,000。檔案伺服器上的可執行檔數量可能更大甚至超過 150,000 閾值。

測試度量顯示清查工作在安裝了 Kaspersky Endpoint Security 11 而未安裝協力廠商應用程式的執行 Windows 7 作業系統的裝置上具有以下結果。

- 清空 **DLL 模組清查**和**指令碼檔案清查**核取方塊：大約 3000 個檔案。
- 選中 **DLL 模組清查**和**指令碼檔案清查**核取方塊：10,000 到 20,000 個檔案，根據安裝的作業系統服務套件數量。
- 僅選中**指令碼檔案清查**核取方塊：大概 10,000 個檔案。

管理伺服器和受防護裝置間的網路負載詳情

該部分提供了一定條件下的網路流量測試度量結果。當您計畫網路基礎架構和您組織網路中（或管理伺服器和其他要防護其裝置的組織間）吞吐量時，可以參考該資訊。知道了網路吞吐量，您也可以估算不同資料傳輸操作將花費的時間。

不同方案下的流量消耗

下表顯示不同方案下管理伺服器和受管理裝置之間流量度量測試的結果。

預設下，裝置每 15 分鐘或更長間隔與管理伺服器同步一次。然而，如果您在管理伺服器上修改政策 / 工作設定，早期同步發生在可套用政策 / 工作的的裝置，從而新設定被傳輸到裝置。

管理伺服器和受管理裝置間的流量率

情景	從管理伺服器到每台受管理裝置的流量	從每台受管理裝置到管理伺服器的流量
安裝帶有更新資料庫的 Kaspersky Endpoint Security 11.7 for Windows	390 MB	3.3 MB
網路代理安裝	75 MB	397 KB
網路代理與 Kaspersky Endpoint Security 11.7 for Windows 一起安裝	459 MB	3.6 MB
病毒資料庫初始化更新（如果停用了卡巴斯基安全網路的參與）	113 MB	1,8 MB
病毒資料庫每日更新（如果啟用了卡巴斯基安全網路的參與）	22 MB	373 MB
裝置資料庫更新之前的初始化同步（政策和工作傳輸）。	382 KB	446 KB
在裝置上更新資料庫之後初次同步	20 KB	157 KB
與管理伺服器的同步（根據排程）	18 KB	23 KB
當群組政策中單個裝置被變更時同步（設定變更時立即）	19 KB	20 KB
當群組工作中單個裝置被變更時同步（設定變更時立即）	14 KB	11 KB
強制同步	110 KB	109 KB
偵測到的病毒事件（1 個病毒）	44 KB	50 KB
偵測到的病毒事件（10 個病毒）	58 KB	77 KB
啟用應用程式註冊表清單後的一次性流量	高達10 KB	高達12 KB
啟用應用程式註冊表清單時的日常流量	高達840 KB	高達 1 MB

24 小時平均流量使用

管理伺服器與受管理裝置間平均 24 小時的流量使用情況如下：

- 從管理伺服器到受管理裝置的流量為 840 KB。
- 從受管理裝置到管理伺服器的流量為 1 MB。

流量會根據以下條件測量：

- 受管理裝置已安裝網路代理和 Kaspersky Endpoint Security 11.6 for Windows。
- 未指派裝置的發佈點。
- 弱點和修補程式管理未啟用。
- 與管理伺服器的同步頻率是 15 分鐘。

聯絡技術支援

該部分描述如何獲取技術支援和其可用條款。

如何取得技術支援

如果您無法在卡巴斯基安全管理中心文件或其中一個有關卡巴斯基安全管理中心的資訊來源中找到問題的解決方案，請聯絡卡巴斯基技術支援中心。技術支援專家將回答您關於卡巴斯基安全管理中心安裝和使用的所有問題。

Kaspersky 在此卡巴斯基安全管理中心的生命週期內提供支援（請參見應用程式支援生命週期頁面）。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與技術支援聯絡：

- 透過造訪技術支援網站
- 透過使用 Kaspersky CompanyAccount 入口傳送請求到技術支援

透過 Kaspersky CompanyAccount 取得技術支援

Kaspersky CompanyAccount 是一項針對使用 Kaspersky 應用程式的公司入口網站。Kaspersky CompanyAccount 入口設計用於方便使用者與 Kaspersky 專家之間透過線上請求進行互動。您可以使用 Kaspersky CompanyAccount 偵錯您的線上請求狀態並儲存它們的歷史。

您可以在 Kaspersky CompanyAccount 上透過單個帳戶註冊貴組織的所有員工。單個帳戶允許集中管理已註冊員工向 Kaspersky 傳送的電子請求，還允許透過 Kaspersky CompanyAccount 管理這些員工的權限。

Kaspersky CompanyAccount 入口採用以下語言提供：

- 英語
- 西班牙語
- 意大利語
- 德語
- 波蘭語
- 葡萄牙語
- 俄語
- 法語
- 日語

要瞭解有關 Kaspersky CompanyAccount 的更多資訊，請造訪技術支援網站。

取得管理伺服器的傾印檔案

管理伺服器的傾印檔案包含有關某個時間點管理伺服器處理程序的所有資訊。管理伺服器的傾印檔案儲存在 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\~dumps 資料夾中。只要卡巴斯基安全管理中心正在使用，傾印檔案就會被存儲，並在刪除時永久刪除。傾印檔案不會被自動傳輸給卡巴斯基。

如果管理伺服器崩潰，您可以聯絡卡巴斯基技術支援。技術支援專家可能會要求您傳送管理伺服器的傾印檔案以供卡巴斯基進一步分析。

傾印檔案可能包含個人資料。我們建議在發送給卡巴斯基之前，保護資訊，以免遭未經授權的存取。

有關程式的資訊來源

Kaspersky 網站上的卡巴斯基安全管理中心頁面

在 Kaspersky 網站的卡巴斯基安全管理中心頁面上，您可以檢視有關程式、程式功能和特性的一般資訊。

知識庫中的卡巴斯基安全管理中心頁

*知識庫*是 Kaspersky 技術支援網站的一部分。

在知識庫的卡巴斯基安全管理中心頁面上，您可以閱讀文章，這些文章提供了有用的資訊、建議以及有關如何購買、安裝和使用程式的常見問題解答。

知識庫中的文章可能提供關於卡巴斯基安全管理中心和 Kaspersky 應用程式的問題的答案。知識庫中的文章也可能包含技術支援新聞。

在社區討論 Kaspersky 應用程式

如果您的問題不需要立即回答，您可以在我們的論壇中與 Kaspersky 專家和其他使用者一起進行討論。

在該論壇上，可以檢視討論主題，發表您的評論，建立新討論主題。

需要網際網路連線以存取網站資源。

如果您無法找到問題的解決方案，請聯絡技術支援。

詞彙表

Amazon EC2 實例

使用 Amazon Web Service 基於 AMI 映像建立的虛擬機。

Amazon 系統映像 (AMI)

範本包含執行虛擬機必要的軟體設定。多個實例可以基於單個 AMI 建立。

Android 裝置

一個連線到卡巴斯基安全管理中心管理伺服器和透過 Kaspersky Endpoint Security for Android 應用程式進行管理的行動裝置。

AWS Application Program Interface (AWS API)

AWS 平台的用於卡巴斯基安全管理中心的應用程式開發介面。特別地，AWS API 工具用於雲端區段輪詢和安裝網路代理到實例。

AWS IAM 存取金鑰

包含金鑰 ID（「AKIAIOSFODNN7EXAMPLE」樣式）和金鑰（「wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY」樣式）的組合。這對屬於 IAM 使用者並用於獲取對 AWS 服務的存取。

AWS 管理主控台

檢視和管理 AWS 資源的 Web 介面。AWS 管理主控台在 https://aws.amazon.com/tw/console/ 可用。

EAS 裝置

透過 Exchange ActiveSync 協定連線至管理伺服器的行動裝置。iOS、Android 和 Windows Phone® 作業系統的行動裝置可透過使用 Exchange ActiveSync 協定來連線和管理。

Exchange 行動裝置伺服器

卡巴斯基安全管理中心的一個元件，允許您連線 Exchange ActiveSync 行動裝置到管理伺服器。

HTTPS

在網路瀏覽器和網路伺服器之間使用加密傳送資料的安全通訊協定。HTTPS 用於存取受限制的資訊，如企業或財務資料。

IAM 使用者

AWS 服務使用者。IAM 使用者可能具有執行雲端區段輪詢的權限。

IAM 角色

請求 AWS 服務的權限設定。IAM 角色不關聯於特定使用者或群組；它們提供不帶 AWS IAM 存取金鑰的存取權限。您可以分配 IAM 角色到 IAM 使用者、EC2 實例和 AWS 應用程式或服務。

iOS MDM 伺服器

安裝在用戶端裝置上的卡巴斯基安全管理中心的一個元件，允許透過 Apple Push Notifications (APN) 將 iOS 行動裝置連線至管理伺服器並管理 iOS 行動裝置。

iOS MDM 裝置

透過 iOS MDM 協定連線到 iOS MDM 伺服器的行動裝置。可透過 iOS MDM 協定連線和管理執行 iOS 作業系統的裝置。

iOS MDM 設定檔

用於將 iOS 行動裝置伺服器連線至管理伺服器的設定集合。使用者將 iOS MDM 設定檔安裝至行動裝置，因此，該行動裝置將連線至管理伺服器。

JavaScript

一種對網頁功能進行擴充的程式語言。使用 JavaScript 建立的網頁無需使用來自網路伺服器的新資料更新網頁即可執行功能（例如，變更介面元素的圖示或開啟附加視窗）。要檢視使用 JavaScript 建立的頁面，請在您的瀏覽器的設定中啟用 JavaScript 支援。

Kaspersky 更新伺服器

Kaspersky 應用程式可以從 Kaspersky 的 HTTP(S) 伺服器下載資料庫和程式模組更新。

KES 裝置

一個連線到卡巴斯基安全管理中心管理伺服器和透過 Kaspersky Endpoint Security for Android 應用程式進行管理的行動裝置。

Provisioning 設定檔

應用程式在 iOS 行動裝置上執行的設定的集合。Provisioning 設定檔包含有關產品授權的資訊，它連線至特定的應用程式。

SSL

網際網路和本機網上的使用的資料加密協定。Secure Sockets Layer (SSL) 協定用在網路應用程式中，以便在用戶端和伺服器之間建立安全的連線。

UEFI 防護裝置

包含在 BIOS 層級整合了適用於 UEFI 的卡巴斯基解決方案或應用程式的裝置。整合的防護從系統啟動時開始確保裝置安全，未整合軟體的裝置僅在安全應用程式啟動後開始防護工作。

Windows Server 更新服務 (WSUS)

用於派發 Microsoft 應用程式更新至組織網路使用者的電腦上。

不相容應用程式

協力廠商開發的病毒防護應用程式，或不支援透過卡巴斯基安全管理中心管理的 Kaspersky 應用程式。

中間人攻擊

中間人。對組織的 IT 基礎設施的攻擊，其中駭客劫持兩個接入點之間的通信鏈路，進行中繼轉發，並在必要時修改這些接入點之間的連線。

事件儲存區

管理伺服器資料庫的一部分，用於儲存發生在卡巴斯基安全管理中心中的事件資訊。

事件嚴重等級

在 Kaspersky 程式操作過程中遇到的事件的內容。有以下嚴重等級：

- 緊急事件
- 功能失效
- 警告
- 資訊

根據事件發生時的情況，相同類型的事件可能具有不同的嚴重等級。

修補程式重要等級

修補程式內容。有五個 Microsoft 修補程式和協力廠商修補程式的嚴重等級：

- 緊急
- 高
- 中等
- 低等
- 未知

協力廠商修補程式或 Microsoft 修補程式的嚴重等級由修補程式需要修補的弱點的最不利的嚴重等級決定。

備份資料夾

用於儲存使用備份公用程式建立的管理伺服器資料副本的專用資料夾。

內部使用者

內部使用者的帳戶可用於管理虛擬管理伺服器。卡巴斯基安全管理中心授權應用程式的內部使用者擁有真實使用者的所有權限。

只能在卡巴斯基安全管理中心內建立和使用內部使用者帳戶。內部使用者的資料不會傳送到作業系統上。卡巴斯基安全管理中心將驗證內部使用者。

共用憑證

憑證用於識別使用者的行動裝置。

卡巴斯基安全管理中心操作員

對透過卡巴斯基安全管理中心管理的防護系統的狀態和操作進行監視的使用者。

卡巴斯基安全管理中心管理員

透過卡巴斯基安全管理中心遠端集中管理系統來管理應用程式操作的人。

卡巴斯基安全管理中心系統健康驗證程式 (SHV)

在卡巴斯基安全管理中心和 Microsoft NAP 並行執行時，用於檢查作業系統執行能力的卡巴斯基安全管理中心的一個元件。

卡巴斯基安全管理中心網頁伺服器

卡巴斯基安全管理中心元件，與管理伺服器一同安裝。網頁伺服器用於透過網路傳輸獨立安裝套件、iOS MDM 設定檔、以及共用資料夾的檔案。

卡巴斯基安全網路 (KSN)

一種雲端服務基礎架構，可提供對 Kaspersky 資料庫的存取，其中包含持續更新的檔案、網路資源和軟體信譽資訊。卡巴斯基安全網路確保在遇到未知威脅時 Kaspersky 應用程式能夠做出更快速的回應，提高某些防護元件的效能並降低誤報的可能性。

卡巴斯基私有安全網路 (KPSN)

私有卡巴斯基安全網路允許已安裝 Kaspersky 應用程式裝置的使用者，存取卡巴斯基安全網路信譽資料庫和其他統計資料，而不從他們的裝置傳送資料到卡巴斯基安全網路。私有卡巴斯基安全網路用於由於以下原因無法參與卡巴斯基安全網路的企業客戶：

- 裝置未連線到網際網路。
- 傳輸任何資料到國家/地區以外或企業區域網路以外被法律或企業安全政策禁止。

受管理裝置

包括在管理群組中的企業網路裝置。

可用更新

Kaspersky 應用程式模組的更新集，包含特定時間段積累的關鍵更新和應用程式架構變更。

安裝套件

使用卡巴斯基安全管理中心遠端管理系統建立的一組用於遠端安裝 Kaspersky 程式的檔案。安裝套件包含安裝應用程式所需的一系列設定，這些設定在安裝後立即執行。應用程式預設值。使用包含在應用程式安裝套件中的附檔名 .kpd 和 .kud 的檔案建立安裝套件。

工作

Kaspersky 應用程式執行的功能會以工作執行，範例：即時檔案防護、電腦完整掃描、資料庫更新。

工作設定

對於每個工作類型的特別應用程式設定。

廣播網域

網路的一個邏輯區域，在這裡所有節點可以使用廣播通道在 OSI 層 (Open Systems Interconnection Basic Reference Model) 交換資料。

弱點

作業系統或應用程式存在的弱點，惡意軟體研發者會利用這種弱點入侵系統或應用程式並破壞其完整性。系統中的大量弱點會使系統不安全，因為能夠入侵系統的病毒會導致系統或其所安裝的應用程式發生執行故障。

強制安裝

遠端安裝 Kaspersky 應用程式的方法，允許您安裝軟體到指定用戶端裝置。為了成功完成強制安裝，用於執行該工作的帳戶必須具有足夠的權限，以便在用戶端裝置上遠端啟動應用程式。該方法建議用於安裝應用程式到執行 Microsoft Windows 作業系統並支援該功能的裝置。

應用程式商店

卡巴斯基安全管理中心元件。應用程式商店用於安裝應用程式到使用者 Android 裝置。應用程式商店允許您發佈應用程式 APK 檔案和連結到 Google Play。

手動安裝

從分發套件安裝安全應用程式到企業網路中的裝置。手動安裝需要管理員或其他 IT 專家的參與。通常情況下，如果遠端安裝發生錯誤，則執行手動安裝。

指定裝置的工作

從任意管理群組分配給一批用戶端裝置並且在那些裝置上執行的工作。

授權檔案

帶有 .key 副檔名的檔案，可以用來以試用或正式產品授權使用 Kaspersky 應用程式。

授權的應用程式群組

由管理員根據的標準設定（範例，根據供應商）建立的應用程式群組，系統將維護已安裝至用戶端裝置的應用程式的統計資訊。

政策

政策決定應用程式設定並管理應用程式在管理群組中電腦上的配置。必須為每個應用程式都建立單獨的政策。您可以為安裝在每個管理群組中之電腦的應用程式建立多個政策，但是對於管理群組中的每個應用程式，一次只能套用一個政策。

啟動產品授權

應用程式目前使用的金鑰。

更新

替換或者新增從 Kaspersky 更新伺服器接收到的新檔案（資料庫或應用程式模組）的過程。

服務供應商管理員

病毒防護服務提供者的員工。該管理員為基於 Kaspersky 病毒防護產品的病毒防護系統執行安裝和維護工作，並且向客戶提供技術支援。

本機安裝

將安全應用程式安裝在企業網路的裝置上，手動安裝會從安全應用程式分發套件開始，或者從預先下載到裝置的已發佈安裝套件開始。

本機工作

在單台用戶端電腦上定義和執行的工作。

歸屬管理伺服器

主管理伺服器是網路代理安裝過程中指定的管理伺服器。主管理伺服器可在網路代理連線設定檔中被使用。

產品授權期限

您可以存取程式功能並且有權使用進階服務的時間段。您可以使用的服務取決於產品授權的類型。

用戶端管理員

客戶組織中負責監控病毒防護狀態的員工。

病毒活動臨界值

在特定時間內指定類型事件的最大允許數量，當超過該數量時，程式將把其解釋為病毒活動增加並看做是一種病毒爆發。該功能在病毒爆發期間很重要，因為它使管理員能夠即時對病毒攻擊威脅做出反應。

病毒爆發

使裝置感染病毒的一系列蓄意嘗試。

病毒資料庫

包含 Kaspersky 已知的電腦安全威脅資訊。病毒資料庫中的項目使得惡意程式碼在被掃描物件中被偵測。病毒資料庫由 Kaspersky 專家建立並且每小時都會更新。

病毒防護服務供應商

提供給用戶端組織基於 Kaspersky 解決方案的病毒防護服務的組織。

發佈點

安裝了網路代理並用於更新發佈、遠端安裝應用程式、取得管理群組和/或廣播網域中電腦資訊的電腦。發佈點用來降低發佈更新時管理伺服器的負載並最佳化網路流量。發佈點可以被自動指定、被管理伺服器指定或被管理員手動指定。發佈點先前叫做更新代理。

直接應用程式管理

透過本機介面進行的應用程式管理。

程式設定

對所有工作類型通用並且掌管應用程式總體操作的應用程式設定，例如：應用程式效能設定、報告設定和備份設定。

管理主控台

基於 Windows 的卡巴斯基安全管理中心的一個元件（也稱為基於 MMC 的管理主控台）。該元件為管理伺服器和網路代理的管理服務提供使用者介面。

管理伺服器

卡巴斯基安全管理中心的一個元件，可集中儲存公司網路安裝的所有 Kaspersky 應用程式相關資訊。它也可用於管理這些應用程式。

管理伺服器憑證

管理伺服器用於以下目的的憑證：

- 連線至基於 MMC 的管理主控台或卡巴斯基安全管理中心網頁主控台時，對管理伺服器進行身分驗證
- 受管裝置上管理伺服器和網路代理之間的安全交互
- 將主管理伺服器連線到從屬管理伺服器時對管理伺服器進行身分驗證

憑證會在安裝管理伺服器時自動建立，然後儲存在管理伺服器上。

管理伺服器用戶端（用戶端裝置）

安裝網路代理和執行受管理的 Kaspersky 應用程式的裝置、伺服器或工作站。

管理伺服器資料備份

使用備份工具複製管理伺服器資料，以便進行備份和後續的還原。該工具可以儲存：

- 管理伺服器資料庫（政策、工作、應用程式設定、管理伺服器上儲存的事件）
- 有關管理群組和用戶端裝置架構的配置詳情
- 用於遠端安裝應用程式的安裝檔案儲存區，包含了以下目錄：資料夾內容：應用程式、移除更新
- 管理伺服器憑證

管理員工作站

安裝管理主控台或用於開啟卡巴斯基安全管理中心網頁主控台的裝置。該元件提供了卡巴斯基安全管理中心管理介面。

管理員工作站用於設定和管理卡巴斯基安全管理中心的伺服器部分。使用管理員工作站，管理員基於 Kaspersky 應用程式為企業區域網路建立和管理一個集中的病毒防護系統。

管理員權限

在 Exchange 組織內管理 Exchange 物件所需的使用者權限。

管理外掛程式

一個提供應用程式管理介面的專用元件，以便透過管理主控台管理該應用程式。每個應用程式都有自己的外掛程式。外掛程式會包含在使用卡巴斯基安全管理中心管理的所有 Kaspersky 應用程式中。

管理群組

一組按照功能和已安裝的 Kaspersky 應用程式分組的裝置。裝置被分組成一個單一實體以便管理。群組可以包含其他群組。群組政策和群組工作可以為群組中每個安裝的應用程式建立。

網路代理

卡巴斯基安全管理中心的一個元件，它對管理伺服器和特定網路節點（工作站或伺服器）上安裝的 Kaspersky 程式之間的互動進行協調。該元件是公司內所有 Microsoft® Windows® 應用程式的通用元件。對於為類 Unix OS 和 macOS 開發的 Kaspersky 應用程式，分別有不同版本的網路代理。

網路位置辨識 (NLA)

幫助作業系統辨識目前網路的 Windows 服務。NLA 可偵測網路變化並調整裝置的安全配置。

網路病毒防護

一組技術和組織措施，能降低病毒和垃圾郵件可能感染組織網路的機會並防止網路攻擊、釣魚和其他威脅。當您使用安全應用程式和服務和應用企業資料安全政策時，網路安全被增加。

網路防護狀態

目前防護狀態，它定義了企業網路裝置的安全。網路防護狀態包括已安裝的安全應用程式、產品授權金鑰的使用及偵測到的威脅數量和類型等項目。

群組工作

為某個管理群組定義並且在該組織中所有用戶端裝置上執行的工作。

虛擬管理伺服器

卡巴斯基安全管理中心元件，其用途是管理用戶端組織網路的防護系統。

虛擬管理伺服器是特殊的從屬管理伺服器，與實體的管理伺服器相比，它具有以下限制：

- 只能在主管理伺服器上建立虛擬管理伺服器。
- 虛擬管理伺服器在其操作中使用主管理伺服器資料庫。虛擬管理伺服器不支援資料備份和還原工作，以及更新掃描和下載工作。
- 虛擬伺服器無法建立從屬管理伺服器（包括虛擬伺服器）。

行動裝置伺服器

卡巴斯基安全管理中心的一個元件，可以提供對行動裝置的存取，允許您透過管理主控台來管理這些行動裝置。

裝置所有者

裝置所有者就是管理員需要在裝置上執行操作時可以聯絡的使用者。

角色群組

授予相同的管理員權限的 Exchange ActiveSync 行動裝置的一組使用者。

設定檔

包含設定集合和 iOS MDM 行動裝置限制的政策。

設定檔

Exchange 行動裝置的設定集合，定義了行動裝置連線到 Microsoft Exchange 伺服器後的行為。

身分和存取管理 (IAM)

啟用了使用者到其他 AWS 服務和資源的存取管理的 AWS 服務。

身分驗證代理

允許您完成存取已加密硬碟磁碟機的身分驗證和在可啟動磁碟機加密後載入作業系統的介面。

輕量級 Nagent（LWNGT）

用於與行動裝置上的 Kaspersky Endpoint Security 進行互動的協定。LWNGT（又稱行動協定）起到網路代理的作用，而無需在行動裝置上實際安裝網路代理。

連線閘道

*連線閘道*是一種以特殊模式執行的網路代理。連線閘道接受來自其他網路代理的連線，並透過其自身與伺服器的連線將它們透過通道傳送到管理伺服器。與普通的網路代理不同，連線閘道會等待來自管理伺服器的連線，而不是建立與管理伺服器的連線。

遠端安裝

使用卡巴斯基安全管理中心提供的服務安裝 Kaspersky 程式。

還原

將物件從隔離區或備份區還原至其在隔離、解毒或刪除前所在的原始位置或移動至使用者定義的資料夾。

還原管理伺服器資料

使用備份工具從備份區中儲存的資訊還原管理伺服器資料。該工具可以還原：

- 管理伺服器資料庫（政策、工作、應用程式設定、管理伺服器上儲存的事件）
- 有關管理群組和用戶端裝置架構的配置詳情
- 用於遠端安裝應用程式的安裝檔案儲存區，包含了以下目錄：資料夾內容：應用程式、移除更新
- 管理伺服器憑證

防護狀態

目前防護狀態，反映了電腦安全等級。

附加（或備用）產品授權金鑰

程式已驗證可使用，但是目前還未使用的金鑰。

隔離區域 (DMZ)

隔離區是一段本機網路，其中包含相應來自全局網路的請求的伺服器。為確保組織的本機網路的安全性 LAN 的存取受防火牆的防護。

集中式應用程式管理

使用卡巴斯基安全管理中心中提供的管理服務進行遠端應用程式管理。

雲端環境

以雲端平台為基礎並合併至網路的虛擬機和虛擬資源。

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 legal_notices.txt 檔案內，在應用程式安裝資料夾內。

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、Shockwave、Flash 和 PostScript 是 Adobe 在美國和/或其他國家/地區的商標或註冊商標。

AMD 和 AMD64 是 Advanced Micro Devices, Inc. 的商標和註冊商標。

Amazon、Amazon Web Services、AWS、Amazon EC2、AWS Marketplace 是 Amazon.com, Inc. 或其附屬公司的商標。

Apache 是 Apache Software Foundation 的註冊商標或商標。

AirPlay、AirDrop、AirPrint、App Store、Apple Configurator、AppleScript、FaceTime、FileVault、iBook、iBooks、iCloud、iPad、iPhone、iTunes、Leopard、macOS、Mac、Mac OS、OS X、Safari、Snow Leopard、Tiger、QuickTime 和 Touch ID 是 Apple Inc. 的商標。

Arm 是 Arm Limited（或其子公司）在美國和/或其他地方的註冊商標。

Bluetooth 註冊商標和服務標誌皆為 Bluetooth SIG, Inc. 所有。

Ubuntu、LTS 是 Canonical Ltd 的註冊商標。

Cisco Systems、Cisco、Cisco Jabber、IOS是 Cisco Systems, Inc. 和/或其附屬公司在美國和其他特定國家/地區的註冊商標。

Citrix、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。

Corel 是 Corel Corporation 和/或其附屬公司在美國和其他特定國家/地區的註冊商標。

Cloudflare、Cloudflare 標誌和 Cloudflare Workers 是 Cloudflare, Inc. 在美國和其他司法管轄區的商標和/或註冊商標。

Dropbox 是 Dropbox, Inc. 的商標。

Radmin 是 Famatech 的註冊商標。

Firebird 是 Firebird Foundation 的註冊商標。

Foxit 是 Foxit Corporation 的註冊商標。

FreeBSD 是 FreeBSD foundation 的註冊商標。

Google、Android、Chrome、Chromium、Dalvik、Firebase、Google Chrome、Google Earth、Google Play、Google Maps、Hangouts、Google Public DNS 和 YouTube 是 Google LLC 的商標。

EulerOS、FusionCompute、FusionSphere 是華為技術有限公司的商標。

Intel、Core、Xeon 是 Intel Corporation 或其子公司的商標。

IBM 和 QRadar 是 International Business Machines Corporation 在全球眾多司法管轄區的註冊商標。

Node.js 是 Joyent, Inc. 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/地區的註冊商標或商標。

Active Directory、ActiveSync、BitLocker、Excel、Forefront、Internet Explorer、InfoPath、Hyper-V、Microsoft Edge、MultiPoint、MS-DOS、Office 365、PowerShell、PowerPoint、SharePoint、SQL Server、OneNote、Outlook、Skype、Tahoma、Visio、Win32、Windows、Windows PowerShell、Windows Media、Windows Mobile、Windows Server、Windows Phone、Windows Vista 和 Windows Azure 是 Microsoft 集團公司的商標。

CVE 是 MITRE Corporation 的註冊商標。

Mozilla、Firefox、Thunderbird 是 Mozilla Foundation 在美國和其他國家/地區的商標。

Novell 是 Novell Enterprises Inc. 在美國和其他國家/地區的註冊商標。

NetWare 是 Novell Inc. 在美國和其他國家/地區的註冊商標。

OpenSSL 是 OpenSSL 軟體基金會擁有的商標。

OpenVPN 是 OpenVPN, Inc. 的註冊商標。

Oracle、Java、JavaScript 和 TouchDown 是 Oracle 和/或其附屬公司的註冊商標。

Parallels、Parallels 標誌和 Coherence 是 Parallels International GmbH 的商標或註冊商標。

Chef 是 Progress Software Corporation 和/或其子公司或附屬公司之一在美國和/或其他國家/地區的商標或註冊商標。

Puppet 是 Puppet, Inc. 的商標或註冊商標。

Python 是 Python 軟體基金會的商標或註冊商標。

Red Hat、Fedora 和 Red Hat Enterprise Linux 是 Red Hat Inc. 或其子公司在美國和其他國家/地區的商標或註冊商標。

Ansible 是 Red Hat, Inc. 在美國和其他國家/地區的註冊商標。

CentOS 是 Red Hat 或其附屬公司在美國和其他國家/地區的商標或註冊商標。

BlackBerry 是 Research In Motion Limited 所有的商標，在美國和/或其他國家註冊。

SAMSUNG 是 SAMSUNG 在美國或其他國家/地區的商標。

Debian 是 Public Interest, Inc. 公司的軟體的註冊商標。

Splunk 和 SPL 是 Splunk Inc. 在美國和其他國家/地區的商標和註冊商標。

SUSE 是 SUSE LLC 在美國和其他國家/地區的註冊商標。

Symbian 是 Symbian Foundation Ltd. 所擁有的商標。

OpenAPI 是 The Linux Foundation 的商標。

UNIX 是在美國和其他國家/地區的註冊商標，透過 X/Open Company Limited 授權。

Zabbix 是 Zabbix SIA 的註冊商標。

已知問題

卡巴斯基安全管理中心網頁主控台具有許多限制，這些限制對於應用程式的執行並不重要：

- 如果變更裝置上的時間或時區，您必須重新啟動卡巴斯基安全管理中心網頁主控台服務。
- 如果裝置上使用了代理，並且設定了代理環境變量，卡巴斯基安全管理中心網頁主控台安裝程式可能會凍結。
- 如果您更新 Kaspersky Endpoint Inspection and Response Optimum 外掛程式，然後重新發佈卡巴斯基安全管理中心網頁主控台憑證，Kaspersky Endpoint Inspection and Response Optimum 的外掛程式將自動還原為分發套件中包含的版本。
- 當您匯入*「將更新下載到發佈點儲存庫」*或*「更新驗證」*工作時，將啟用**「選擇工作將被指派到的裝置」選項**。這些工作不能被指派給裝置分類或特定裝置。如果將*下載更新指派到發佈點儲存庫*或將*更新驗證*工作指派到特定裝置，則工作將無法正確匯入。
- 如果您使用安裝了網路代理版本 15 的 Linux 發佈點執行 Active Directory 輪詢，則只能輪詢為其指定位址和使用者憑據的 Active Directory 網域。目前 Active Directory 網域和 Active Directory 網域樹系的輪詢不可用。
- 如果應用程式控制規則基於包含在 Linux 裝置上偵測到的應用程式的應用程式類別，則該規則不起作用。當您從應用程式登錄檔中選擇應用程式以將它們新增到應用程式類別時，請確保選擇在 Windows 裝置上偵測到的應用程式。
- 如果在 Linux 裝置上偵測到來自**應用程式登錄資料**部分的應用程式，則應用程式內容不包含有關相關可執行檔的資訊。
- 如果您通過遠端安裝工作在執行 ALT Linux 作業係統的裝置上安裝網路代理，並且您在具有非 root 權限的帳戶下執行此工作，則該工作將失敗。在 root 賬戶下執行遠端安裝工作，或者建立並使用网路代理的獨立安裝套件在本機安裝應用程式。
- 如果清單包含 20 個以上的項目並且您點擊**全選**核取方塊，網頁主控台將僅選取那些顯示在當前頁面上的項目。請注意，這不適用於**受管理裝置** 、 **裝置分類**和**工作**部分中的清單，您可以在其中選擇清單中的所有項目。
- 本機工作*IOC 掃描*完成後，工作狀態顯示為*已排程*。
- 執行 Windows 網路輪詢後可能找不到用戶端裝置。
- 在 Kaspersky Endpoint Security for Windows 政策中，當您在配置應用程式控制功能時選擇並套用一個應用程式類別時，該類別會被套用，但在您儲存並重新開啟政策後它不會顯示為已選擇的類別。
- 停用 KSN 代理服務後，受管理裝置組中的裝置會將其狀態變更為*緊急*，但子群組中的裝置顯示狀態 *確定*。
- 如果為您用於卡巴斯基安全管理中心的資料庫設定了區分大小寫的排序規則，請在裝置移動規則和自動標記規則中指定裝置 DNS 名稱時保持大小寫。否則，規則將不起作用。
- 在**新增從屬管理伺服器精靈**中，如果您指定在未來的從屬伺服器上啟用雙步驗證進行身分驗證的帳戶，精靈將會結束並顯示錯誤。要解決此問題，請指定停用雙步驗證的帳戶或從未來的從屬伺服器建立階層。
- 登入卡巴斯基安全管理中心網頁主控台時，如果您使用網域身分驗證並指定要連線的虛擬管理伺服器，然後您登出，然後嘗試登入主管理伺服器，則卡巴斯基安全管理中心網頁主控台會連線到虛擬管理伺服器。要連線到主管理伺服器，請重新開啟瀏覽器。

- 裝置屬性的工作清單中可能會顯示本機工作的不正確狀態。
- 快速/完整 Windows 網路輪詢返回空結果。
- 如果您安裝帶有身分和存取管理器的卡巴斯基安全管理中心網頁主控台，然後變更卡巴斯基安全管理中心網頁主控台的管理伺服器，則身分和存取管理器不會獲得有關新管理伺服器的資訊。
- 如果您在不同的瀏覽器中開啟卡巴斯基安全管理中心網頁主控台並在管理伺服器屬性視窗中下載管理伺服器憑證檔案，則下載的檔案具有不同名稱。
- 當您嘗試從**備份**儲存庫（**操作→儲存區→備份**）還原物件或將物件傳送到卡巴斯基時，會發生錯誤。
- 具有多個網路介面卡的受管裝置可傳送有關網路介面卡 MAC 位址的管理伺服器資訊，該網路介面卡不是用於連線到管理伺服器的網路介面卡。
- 如果您安裝帶有身分和存取管理器的卡巴斯基安全管理中心網頁主控台，然後變更卡巴斯基安全管理中心網頁主控台的管理伺服器，則身分和存取管理器不會獲得有關新管理伺服器的資訊。
- 如果您為指定帳戶啟動遠端執行指令碼工作並變更工作設定中為其指派的帳戶，則不會儲存變更。若要變更工作指派到的帳戶，請在工作設定中停止該工作並重新啟動它。