kaspersky

卡巴斯基安全管理中心 16.3 Linux

© 2026 AO Kaspersky Lab

目錄

卡巴斯基安全管理中心 Linux 說明
版本更新摘要
已修復問題
關於卡巴斯基安全管理中心 Linux
- 分發套件
- 硬體和軟體需求
  - 管理伺服器要求
  - 網頁主控台要求
  - 網路代理要求
- 相容的卡巴斯基應用程式和解決方案
- 關於卡巴斯基安全管理中心 Linux 元件的相容性
- 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

架構和基本概念
- 架構
- 卡巴斯基安全管理中心 Linux 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 Linux 使用的連接埠
- 卡巴斯基安全管理中心 網頁主控台使用的連接埠
- 基本概念
  - 管理伺服器
  - 管理伺服器階層
  - 虛擬管理伺服器
  - 網頁伺服器
  - 卡巴斯基安全管理中心 Linux 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 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
  - 虛擬管理伺服器

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 Linux 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
正在啟動
硬化指南
強化檢查清單
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
事件傳輸到第三方系統
第三方資訊系統安全建議
使用卡巴斯基安全應用程式的建議
情境：驗證 MySQL 伺服器
情境：驗證 PostgreSQL 伺服器
佈署準備
選擇卡巴斯基安全管理中心 Linux 的設定
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
選取企業防護結構
佈署防毒軟體的標準流程
選取 DBMS
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
安裝
設定 MariaDB x64 伺服器以與 卡巴斯基安全管理中心 Linux 一起使用
設定 PostgreSQL 或 Postgres Pro 伺服器與卡巴斯基安全管理中心 Linux 搭配使用
設定 MySQL x64 伺服器以與 卡巴斯基安全管理中心 Linux 一起使用
準備一個高可用性 DBMS 叢集，以與卡巴斯基安全管理中心 Linux 搭配使用
安裝 卡巴斯基安全管理中心 Linux
以靜默模式安裝卡巴斯基安全管理中心 Linux
在封閉軟體環境模式下在 Astra Linux 上安裝卡巴斯基安全管理中心 Linux

安裝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
在封閉軟體環境模式下在 Astra Linux 上安裝卡巴斯基安全管理中心網頁主控台
使用指令碼安裝Kaspersky Security Center for Linux
部署卡巴斯基安全管理中心 Linux 容錯移轉叢集
卡巴斯基安全管理中心 Linux 容錯移轉叢集部署方案
卡巴斯基安全管理中心 Linux 容錯移轉叢集
情境：部署 卡巴斯基安全管理中心 Linux 容錯移轉叢集
卡巴斯基安全管理中心 Linux 容錯移轉叢集硬體和軟體需求
為卡巴斯基安全管理中心 Linux 容錯移轉叢集準備檔案伺服器
為卡巴斯基安全管理中心 Linux 容錯移轉叢集準備節點
在 卡巴斯基安全管理中心 Linux 容錯移轉叢集節點上安裝 卡巴斯基安全管理中心 Linux
手動啟動和停止叢集節點
重新安裝容錯移轉叢集節點
安裝連線到安裝在 卡巴斯基安全管理中心 Linux 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
異地分散式Kaspersky Security Center for Linux故障轉移叢集
使用PostgreSQL DBMS執行Ubuntu的異地分散式叢集
準備叢集節點的檔案系統
設定複製叢集檔案系統
在叢集節點上使用安裝程式安裝和設定Corosync和Pacemaker
安裝和設定PostgreSQL DBMS
在異地分散式故障轉移叢集節點上安裝卡巴斯基安全管理中心 Linux
使用Platform V Pangolin DBMS執行SberLinux的異地分散式叢集
準備叢集節點的檔案系統
設定複製叢集檔案系統
在叢集節點上使用安裝程式安裝和設定Corosync和Pacemaker
安裝與設定Platform V Pangolin DBMS
在異地分散式故障轉移叢集節點上安裝Kaspersky Security Center for Linux
在異地分散式故障轉移叢集節點上安裝卡巴斯基安全管理中心網頁主控台
使用 DBMS 的帳戶
設定 DBMS 帳戶以搭配使用 MySQL 和 MariaDB
設定 DBMS 帳戶以搭配使用 PostgreSQL 和 Postgres Pro
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
用於卡巴斯基安全管理中心 Linux 的憑證
關於卡巴斯基安全管理中心憑證
卡巴斯基安全管理中心 Linux 中使用的自訂憑證要求
重新發佈卡巴斯基安全管理中心網頁主控台憑證
取代卡巴斯基安全管理中心網頁主控台憑證
將 PFX 憑證轉換為 PEM 格式
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
將預設 IAM 憑證變更為自訂憑證
將管理伺服器位址新增至IAM伺服器設定
定義共用資料夾

登入到卡巴斯基安全管理中心網頁主控台並登出
卡巴斯基安全管理中心網頁主控台介面
變更卡巴斯基安全管理中心網頁主控台介面的語言
變更卡巴斯基安全管理中心網頁主控台首頁
新增和移除書籤
移除卡巴斯基安全管理中心網頁主控台
快速啟動精靈
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。關閉快速啟動精靈
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
升級卡巴斯基安全管理中心 Linux
升級Kaspersky Security Center for Linux 16或更高版本
使用安裝檔案將卡巴斯基安全管理中心 Linux 從版本 16 或更高版本進行升級
透過備份將卡巴斯基安全管理中心 Linux 從版本 16 或更高版本進行升級
在Kaspersky Security Center for Linux故障轉移叢集節點上升級Kaspersky Security Center for Linux 16或更高版本
升級Kaspersky Security Center for Linux 15.4或更早版本
使用安裝檔案將卡巴斯基安全管理中心 Linux 從 15.4 或更早版本升級
透過備份將卡巴斯基安全管理中心 Linux從版本 15.4 或更早版本進行升級
在Kaspersky Security Center for Linux故障轉移叢集節點上升級Kaspersky Security Center for Linux 15.4或更早版本
升級卡巴斯基安全管理中心網頁主控台
在封閉軟體環境模式下在 Astra Linux 上升級卡巴斯基安全管理中心網頁主控台
移轉到卡巴斯基安全管理中心 Linux
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
教程視頻：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

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
設定管理伺服器
配置管理伺服器連線位址
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
設定連線到卡巴斯基安全管理中心 Linux 的 IP 位址允許清單
設定管理伺服器網際網路存取設定
管理伺服器階層
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
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
配置管理伺服器連線事件記錄
設定事件儲存區中的最大事件數量
將管理伺服器移動至其他裝置
變更管理伺服器名稱
透過新增 DNS 記錄來維持連線
透過切換為以 IP 位址為基礎的連線方式來維持連線
變更伺服器名稱後恢復中斷的連線
變更 DBMS 憑證
備份複製和管理伺服器資料還原
建立管理伺服器資料備份工作
使用 klbackup 公用程式備份和還原資料
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
管理伺服器維護
刪除管理伺服器階層
存取公用 DNS 伺服器
設定介面
到管理伺服器的加密連線
使用 TLS 的加密通信
用於與外部服務交互的網路設定
子網路全域清單
使用 klscmodchk 和 integrity_checker 實用程式檢查模組的完整性
發現網路裝置
情境：發現網路裝置
Windows 網路輪詢
IP 範圍輪詢
新增和修改 IP 範圍
Zeroconf 輪詢
網域控制器輪詢

身分驗證與網域控制器連線
配置 Samba 網域控制器
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
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
將啟用 VDI 的裝置移至管理群組
管理用戶端裝置
受管理裝置設定
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
裝置移動規則
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
將裝置手動新增至管理群組
將裝置或者叢集手動移動至管理群組
關於叢集和伺服器陣列
叢集或伺服器陣列的屬性
發佈點和連線閘道的調整
關於發佈點
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
計算發佈點的數量和配置
自動分配發佈點
手動分配發佈點
在 DMZ 中新增連線閘道作為發佈點
修改管理群組的發佈點清單
啟用推送伺服器
增加 klnagent 服務的檔案描述符限制
關於裝置狀態
設定裝置狀態轉換
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
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
- 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
  - 在管理伺服器之間傳輸加密金鑰
- 變更用戶端裝置的管理伺服器
- 避免多個管理伺服器之間的衝突
- 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
- 當裝置顯示不活動時檢視和配置操作
- 傳送訊息到裝置使用者
- 遠端開啟、關閉和重新啟動用戶端裝置
- 遠端存取受管理裝置
  - 使用卡巴斯基安全管理中心網頁主控台從基於 Linux 的裝置遠端存取基於 Linux 的受管理裝置
  - 使用卡巴斯基安全管理中心網頁主控台從基於 Linux 的裝置遠端存取基於 Windows 的受管理裝置
  - 使用卡巴斯基安全管理中心網頁主控台從基於 Windows 的裝置遠端存取基於 Linux 的受管理裝置
  - 使用卡巴斯基安全管理中心網頁主控台從基於 Windows 的裝置遠端存取基於 Windows 的受管理裝置
- 管理行動裝置
  - 使用 Firebase Cloud Messaging
  - 與公共金鑰基礎架構整合
- 對管理群組進行管理
  - 建立管理群組
  - 將應用程式自動安裝到管理群組中的裝置
  - 移動管理群組
  - 刪除管理群組
- 佈署 Kaspersky 應用程式
  - 情境：卡巴斯基應用程式部署
  - 新增卡巴斯基應用程式的管理外掛程式
  - 安裝套件
    - 下載和建立 Kaspersky 應用程式的安裝套件
    - 從檔案建立安裝套件
    - 建立獨立安裝套件
    - 網路代理安裝套件設定
    - 執行 卡巴斯基安全管理中心 Linux 建立的獨立套件
    - 使用獨立安裝套件安裝應用程式
    - 安全應用程式安裝套件上的資料庫更新
    - 變更自訂安裝套件資料大小限制
    - 分發安裝套件至從屬管理伺服器
    - 檢視獨立安裝套件清單
  - 安裝 Network Agent for Linux
    - 準備 Linux 裝置以安裝網路代理
    - 準備一部執行 SUSE Linux Enterprise Server 15 的裝置以安裝網路代理

準備在封閉軟體環境模式下執行 Astra Linux 的裝置以安裝網路代理
準備在安裝了glibc 2.5（舊版作業系統）的Linux作業系統上安裝網路代理程式。
準備在安裝了OpenSSH 6.4（舊版作業系統）的Linux作業系統上安裝網路代理程式。
在 Linux 裝置上遠端安裝網路代理
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
對網路代理裝置檔案系統回溯的支援
安裝 Network Agent for Windows
以互動模式安裝 Windows 網路代理
以靜默模式安裝 Windows 網路代理
透過擷取和複製裝置映像來佈署
網路代理磁碟克隆模式
網路代理安裝參數
使用遠端軟體安裝工作安裝應用程式
關於 卡巴斯基安全管理中心 Linux 的遠端安裝工作
遠端安裝應用程式
在 macOS 裝置上遠端安裝應用程式
在從屬管理伺服器上安裝應用程式
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
透過卡巴斯基安全管理中心 Linux 的遠端安裝工作強制佈署
以靜默模式安裝應用程式
準備 macOS 裝置以遠端安裝網路代理
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
指定在 Unix 裝置上進行遠端安裝的設定
監控佈署
啟動和停止卡巴斯基應用程式
取代協力廠商安全應用程式
遠端移除應用程式或軟體更新
準備好用於遠端安裝的 Windows 裝置
建立「遠端執行指令碼」工作
根據清單檔案建立安裝套件
為遠端執行指令碼工作準備存檔
使用遠端執行腳本工作在設備上遠端安裝應用程式
為遠端執行指令碼工作配置通知和監控
產品授權
卡巴斯基安全管理中心 Linux 的產品授權
關於最終使用者產品授權協議
關於產品授權
關於產品授權憑證
關於產品授權金鑰
檢視隱私政策
卡巴斯基安全管理中心產品授權選項
關於金鑰檔案

- 關於資料提供
- 關於訂購
- 啟動 卡巴斯基安全管理中心 Linux
- 受管理卡巴斯基應用程式的產品授權
  - 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
  - 產品授權超限事件
  - 從儲存區刪除產品授權金鑰
  - 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
- 配置卡巴斯基應用程式
  - 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
  - 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
      - 一般政策設定
      - 修改政策
      - 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
      - 強制同步
      - 檢視政策發佈狀態圖表
      - 在出現病毒爆發事件時自動啟用政策
      - 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
      - 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
- 匯出和匯入政策設定檔
- 網路代理政策設定
- Windows、Linux 和 macOS 網路代理的使用：比較
- 按作業系統比較網路代理設定
- 啟用和停用網路代理的低資源消耗模式
- 配置受管理應用程式的防護設定
- 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
- 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 的使用
  - 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
  - 檢視 KSN 代理伺服器統計
- 管理工作
  - 關於工作
  - 關於工作範圍
  - 建立工作
  - 手動啟動工作
  - 為選取的裝置啟動工作
  - 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
  - 檢視儲存在管理伺服器中的工作執行結果
- 應用程式標籤
  - 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
- 使用 klscflag 實用程式開啟連接埠 13291
- 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

管理使用者和使用者角色

- 關於使用者帳戶
- 關於用於角色
- 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
為使用者或安全群組分配角色
新增使用者帳戶到內部安全群組
指派使用者作為裝置所有者
在安裝網路代理期間將使用者指定為裝置所有者
安裝網路代理後將使用者指派為 Linux 裝置所有者
將使用者作為裝置所有者移除
啟用帳戶防護以防止未經授權的修改
設定雙步驟驗證
關於帳戶的雙因素驗證
在卡巴斯基安全管理中心網頁主控台登入時設定雙因素驗證秘密金鑰
允許使用者配置雙因素驗證
重置和刪除雙因素驗證秘密金鑰
從雙因素驗證中排除帳戶
編輯安全碼簽發者的名稱
變更允許的密碼輸入嘗試次數
刪除使用者或安全群組
變更使用者帳戶的密碼
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
變更帳戶密碼
撤銷本機管理員權限
設定 Kerberos 網域身分驗證
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
為將更新下載到管理伺服器儲存區工作新增更新來源
批准和拒絕軟體更新
自動安裝 Kaspersky Endpoint Security for Windows 的更新
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
透過發佈點下載更新
在離線裝置上更新 Kaspersky 資料庫和軟體模組

監控、報告和稽核
方案：監控和報告
關於監控和報告的類型
智慧培訓模式中的規則觸發
檢視並確認使用自適應異常控制規則執行的偵測
從適應性異常控制規則新增排除
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
管理和防護報告
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
防護等級指示器
安全應用程式已安裝
已套用政策
已設定病毒資料庫更新
已設定備份
已設定管理伺服器維護
已啟用TLS加密
事件和事件分類
卡巴斯基安全管理中心 Linux 中的事件
卡巴斯基安全管理中心 Linux 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
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

匯出事件分類
匯入事件分類
檢視事件詳情
匯出事件到檔案
從事件檢視物件歷程
刪除事件
刪除事件分類
設定事件儲存期限
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
在管理伺服器上的事件處理和儲存
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
測試通知
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
用於回應警示的整合
配置與 Active Directory 的整合以執行回應操作
配置與 Kaspersky Automated Security Awareness Platform 的整合
配置與 Kaspersky Threat Intelligence Portal Sandbox 的整合
按屬性分組警示
Cloud Discovery
使用小工具啟用 Cloud Discovery
在儀表板中新增 Cloud Discovery 小工具
檢視雲端服務使用情況資訊
雲端服務的風險等級
封鎖對不需要的雲端服務進行的存取活動
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
使用 CEF 和 LEEF 格式匯出事件
將事件轉換為 CEF 或 LEEF 格式
標記事件，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
配置 卡巴斯基安全管理中心 Linux 以將事件匯出到 SIEM 系統
監控政策與政策設定檔變更
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 Linux 資料庫名稱
檢視匯出結果
管理物件修訂
檢視並儲存政策修訂
比較政策版本
回溯物件到先前修訂
活動威脅
解毒未處理檔案
下載未處理檔案
從"活動威脅"部分中刪除檔案
物件刪除
從隔離區和檔案備份下載和刪除檔案
從隔離區和檔案備份區下載檔案
關於從隔離區、檔案備份區或主動威脅儲存路中刪除物件
透過SNMP管理應用程式
在作業系統中設定snmpd服務
啟用和停用SNMP通知
在Kaspersky Security Center for Linux中啟用和停用SNMP
SNMP 的物件識別碼值
在 Kaspersky Next XDR Optimum 產品授權下使用卡巴斯基安全管理中心 Linux
用於回應警示的整合
配置與 Active Directory 的整合以執行回應操作
配置與 Kaspersky Automated Security Awareness Platform 的整合
配置與 Kaspersky Threat Intelligence Portal Sandbox 的整合
按屬性分組警示
卡巴斯基安全管理中心網頁主控台和其他卡巴斯基解決方案之間的互動
建立背景連線
配置代理伺服器連線
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
從用戶端裝置下載系統資訊
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 Linux 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
在基於 Linux 的用戶端裝置上執行遠端診斷

管理用戶端裝置上的協力廠商應用程式和可執行檔
使用「應用程式控制」來管理可執行檔
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
新增事件相關的可執行檔到應用程式類別
在 Kaspersky Endpoint Security for Windows 政策配置應用程式控制
取得並檢視安裝在用戶端裝置的應用程式清單
關於協力廠商應用程式
安裝協力廠商軟體更新
情境：更新協力廠商軟體
協力廠商軟體更新安裝選項
「弱點掃描和所需更新」工作設定
建立「弱點掃描和所需更新」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「安裝必要更新並修復弱點」工作
新增安裝更新的規則
建立工作後指定的「安裝所需更新並修復弱點」工作之設定
自動更新協力廠商應用程式
修復協力廠商軟體弱點
關於尋找與修復軟體弱點
情境：尋找與修復協力廠商軟體弱點
修復協力廠商軟體弱點
建立修復弱點工作
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
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
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
禁止在隔離網路中傳輸修補程式和安裝更新
API 參考手冊

服務供應商最佳實踐
計劃卡巴斯基安全管理中心 Linux 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 Linux 標準設定
關於發佈點
管理伺服器階層
虛擬管理伺服器
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
維護閒置連線
佈署網路代理和安全應用程式
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
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
關於漫遊使用者的連線設定檔
關於將網路代理切換到其他管理伺服器
為漫遊使用者建立連線設定檔
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

度量手冊
關於本手冊
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
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
管理大量裝置的管理伺服器的最佳實踐
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資料庫維護工作
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
已知問題
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
Cloud Discovery
HTTPS
iOS MDM 伺服器
iOS MDM 裝置
JavaScript
Kaspersky 更新伺服器
Provisioning 設定檔
SSL
不相容應用程式
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 Linux 管理員
卡巴斯基安全管理中心 Linux 網頁伺服器

卡巴斯基安全管理中心操作員
卡巴斯基安全管理中心系統健康驗證程式 (SHV)
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
應用程式商店
手動安裝
指定裝置的工作
授權檔案
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
裝置所有者
角色群組
設定檔
設定檔

身分識別與存取管理器 (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
第三方程式碼相關資訊
商標聲明

卡巴斯基安全管理中心 Linux 說明

新功能

- 新增內容

硬體和軟體要求

- 管理伺服器要求
- 網頁主控台要求
- 網路代理要求

正在啟動

- 安裝
- 快速啟動精靈
- 防護佈署精靈

產品授權和啟動

- 啟動 卡巴斯基安全管理中心 Linux
- 受管理應用程式的產品授權

部署與組態

- 發現網路裝置
- 發佈點和/或連線閘道的調整
- 取代協力廠商安全應用程式
- Kaspersky 應用程式。集中佈署

- 配置網路防護
- Kaspersky 應用程式。更新資料庫和軟體模組
- 配置管理伺服器連線位址
- 移轉到 卡巴斯基安全管理中心 Linux
- 關於升級卡巴斯基安全管理中心 Linux

監控

- 監控和報告
- Cloud Discovery

管理用戶端裝置

- 遠端存取受管理裝置

弱點和修補程式管理

- 尋找和修復協力廠商軟體中的弱點

附加功能

- 匯出事件到 SIEM 系統
- 檢視KSN代理伺服器統計資料
- 規模指南（僅限線上說明）

新增內容

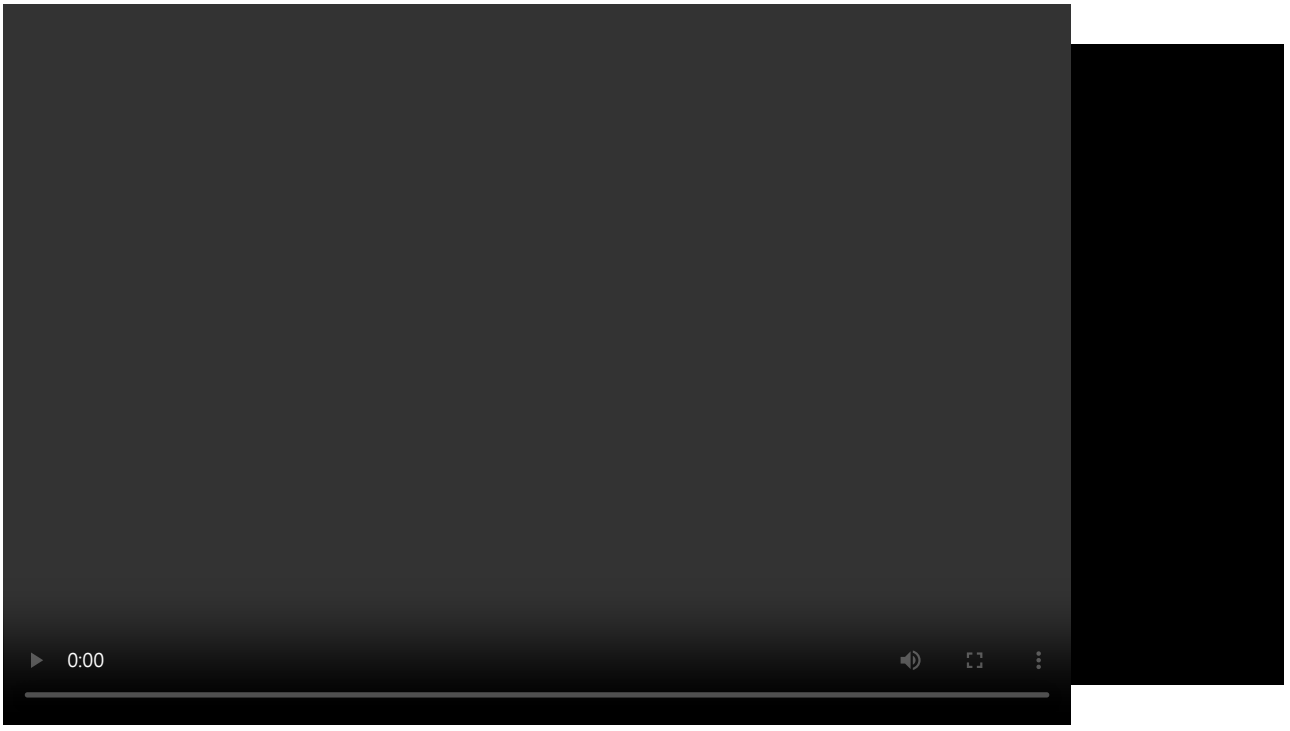
卡巴斯基安全管理中心 16.3 Linux

卡巴斯基安全管理中心 16.3 Linux 有幾項新功能和改善事項：

- 如果您修改政策，系統會為每個已變更的參數建立單獨的稽核事件。事件會匯出至 SIEM。
- 現已將對 **卡巴斯基 SIEM** (KUMA) 的支援新增至將事件匯出至 SIEM 系統功能。
- Kaspersky Security Center for Linux現在支援搭配Kaspersky Vulnerability Management解決方案使用。
- 為符合強化指南，我們制定了最佳化的Kaspersky Endpoint Security for Linux 組態，以安裝在具有管理伺服器、網頁主控台和資料庫管理系統的裝置上，以及部署卡巴斯基安全管理中心 Linux 容錯移轉叢集。
- 現在您可以在安裝Kaspersky Security Center for Linux時指定自訂資料庫結構描述。
- 在**監控** → **控制板**中，防護等級指示器可協助您評估管理伺服器和發佈點的安全性。如果指示器為黃色或紅色，您必須執行操作來解決問題，並將指示器狀態變更為綠色。
- 卡巴斯基安全管理中心 Linux 提供簡化的部署方法：您現在可以使用安裝指令碼。
- 提供適用於 Kaspersky Network Agent for Linux Legacy（glibc 2.5 版）的特殊分發套件，以支援以下過時的作業系統：
  - CentOS 5.2
  - CentOS 5.4
  - CentOS 6.4
  - CentOS 6.6
  - Astra Linux Special Edition RUSB.10015-01（操作更新 1.4）64 位元
- 網路代理程式現在支援與以下新作業系統版本搭配使用：
  - Microsoft Windows 11 IoT企業版25H2版64位元
  - SberOS 3.6.1
  - Ubuntu Server 26.04 LTS
- 以下DBMS不再受支援：
  - Aurora MySQL 5.7
  - MariaDB 10.1.30

- 使用者體驗改善：
  - 已增強**工作**和**政策**表格的篩選功能。您現在可以使用`OR`邏輯新增多個條件，也可以使用新的運算子，讓您能為單一屬性選取多個值，並顯示符合至少一個指定準則的記錄。
  - 在主功能表中：
    - 提供了新的**軟體管理**區段。下列區段現在已移至**軟體管理**：**安裝套件**、**卡巴斯基應用程式**、**第三方應用程式**、**最新應用程式版本**，以及 **修補程式管理**。
    - **未指派的裝置**和**硬體**部分現已移至**資產管理**。
    - **工作** 和 **儲存區** 區段已移至功能表的第一層級。
    - **Web 外掛程式備份**區段已不再使用，並已從網頁主控台中移除。

卡巴斯基安全管理中心 16.2 Linux



16.2 版本新增功能概述。視訊

卡巴斯基安全管理中心 16.2 Linux 有幾項新功能和改善事項：

- 在卡巴斯基安全管理中心網頁主控台中，您現在可以在非軍事區（DMZ）中設定連線閘道。

  使用「**依位址使用 DMZ 連線閘道**」選項設定連線閘道。
- 改進了在Linux裝置上儲存網路代理程式裝置ID（`Device ID`參數）的演算法。如果裝置的BIOS序列號、主機板序列號、儲存磁碟ID或MAC位址與之前已知的值匹配，則管理伺服器會在作業系統更新或MAC位址更改後正確識別裝置。
- 新增了對異地分散式Kaspersky Security Center for Linux故障轉移叢集的支援，該叢集的節點位於不同的資料中心。在異地分散式叢集組態中，所有元件都具有故障轉移功能。

- 現在，您可以將事件以CEF或LEEF格式匯出到SIEM系統。
- 新增了對高可用性PostgreSQL叢集的支援，其中Patroni用於自動故障轉移和HAProxy用於負載平衡。
- 您可以比較政策修訂版本。此選項適用於管理伺服器、網路代理程式、Kaspersky Endpoint Security for Windows（從14.0網頁外掛程式版本開始）和 Kaspersky Endpoint Security for Mac（從12.2.1 Patch A網頁外掛程式版本開始）。在未來版本中，支援此功能的卡巴斯基應用程式清單將會擴展。
- 現支援SNMP。您可以使用SNMP向協力廠商用戶端應用程式提供管理伺服器資訊、統計資料和事件。
- 現在支援對Windows發佈點進行Windows網路輪詢。
- 現在提供適用於Linux的網路代理程式的單一安裝程式套件。此安裝程式包含適用於不同軟體套件管理器和CPU架構的版本。在安裝程式過程中，系統會自動偵測環境並安裝對應的網路代理程式軟體套件。
- 事件現在包含有關在行動裝置上執行的命令發起者的資訊。
- NSQ元件已從卡巴斯基安全管理中心網頁主控台分發套件中移除。KSCWebConsoleMessageQueue.service服務已不再使用，並將在卡巴斯基安全管理中心網頁主控台更新後移除。
- 在隔離網路中，為Windows裝置建立安裝套件現在需要從卡巴斯基網站（ri_utils_win32.zip和ri_utils_arm64.zip存檔）下載其他模組。
- 網路代理現支援 Windows ARM 64 位元架構。您可以在對應的說明文件中驗證與受管應用程式管理的相容性。
- Kaspersky Security Center for Linux支援與Kaspersky Sandbox配合使用。
- 使用者體驗改善：
  - 現在您可以一次刪除事件分類和裝置事件清單中的所有事件。
    事件分類和裝置事件清單中均有**全選**和**全部選取目前頁面**選項。
  - 現在您可以手動指定移動規則的優先順序。
    選擇移動規則後，**變更優先順序**按鈕將變為可用狀態，讓您指定新的優先順序。
- Kaspersky Security Center for Linux支援與Platform V SberLinux OS Server (SLO) 9.6配合使用。
- 卡巴斯基安全管理中心 Linux 現在支援搭配使用以下DBMS：
  - MySQL標準版8.4
  - MySQL企業版8.4
  - PostgreSQL 18
  - Postgres Pro 18（所有版本）
  - Postgres Pro 18 Enterprise（叢集內建高可用）
- 網路代理現在支援搭配使用以下新作業系統版本：
  - Microsoft Windows 11家用版/專業版/工作站專業版/企業版/教育版ARM
  - Platform V SberLinux OS Server (SLO) 9.6

卡巴斯基安全管理中心 16.1 Linux

卡巴斯基安全管理中心 16.1 Linux 有幾項新功能和改善事項：

- 雙因素驗證現已預設啟用。停用雙因素驗證的全域選項不再可用。為確保使用者能夠登入卡巴斯基安全管理中心網頁主控台並繼續使用 OpenAPI 自動化指令碼，請在升級前為所有使用者啟用雙因素驗證。
- 您現在無需匯出政策，即可將政策設定檔儲存到 KLPROF 檔案，然後使用此 KLPROF 檔案將已儲存的設定檔匯入到政策。
- 網路代理現在可在執行 ALT OS 的裝置上以封閉軟體環境模式運作。
- 為無密碼網域使用者新增了對基於 Kerberos 的網域身分驗證的支援，該驗證使用SCRIL 協定，啟用基於憑證的單一登入 (SSO)。
- 使用者體驗改善：
  - 按作業系統版本和套件管理器篩選用戶端裝置的功能現在包含 Linux 作業系統版本。
  - 改進了卡巴斯基安全管理中心網頁主控台中表格的分頁機制：預設顯示的項目數增加到了 50，自訂的顯示項目數現在會在工作階段之間保留。
  - 應用程式類別註解可讓您新增包含和排除類別中應用程式的規則描述。
  - 預設情況下，可用安裝套件清單現在僅以卡巴斯基安全管理中心網頁主控台介面語言顯示卡巴斯基應用程式安裝套件，語言為英語。
- 卡巴斯基安全管理中心 Linux 支援與Kaspersky Endpoint Security for Linux 12.4搭配使用。
- 卡巴斯基安全管理中心 Linux 支援搭配使用以下新作業系統版本：
  - Debian GNU/Linux 13 (Trixie)
  - CentOS Stream 10
  - Red Hat Enterprise Linux Server 10.x
- 網路代理現在支援搭配使用以下新作業系統版本：
  - ALT Workstation 11
  - ALT Server 11
  - ALT Education 11
  - AlterOS 2025
  - SberOS 3.4.0
  - SberOS 3.5.0
  - OSnova 3.*

卡巴斯基安全管理中心 16 Linux

卡巴斯基安全管理中心 16 Linux 有幾項新功能和改善事項：

- FreeIPA 和 ALD Pro 網域控制器受到支援。
- 已實作網域身分驗證（單一登入）。單一登入功能可讓您在卡巴斯基安全管理中心 16 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。若要使用網域身分驗證，您必須在卡巴斯基安全管理中心網頁主控台安裝期間，在回應檔案中指定附加參數。
- 卡巴斯基安全管理中心 16 Linux 管理伺服器僅與卡巴斯基安全管理中心 16 網頁主控台相容。無法使用卡巴斯基安全管理中心網頁主控台的早期版本。
- 現在，您可以在試用產品授權下使用 Kaspersky Next XDR Optimum 功能，前提是您新增了從屬管理伺服器，在試用產品授權下啟動了此伺服器，並將產品授權金鑰部署到了從屬管理伺服器管理的裝置。
- 使用者體驗改善：
  - 透過管理群組和管理伺服器導覽已更新：您可以從單一導覽窗格輕鬆地在群組和伺服器之間切換。
  - 您的設定檔設定已移至上方窗格。
  - 主選單的一些部分已重新命名：
    - **資產（裝置）**部分現在稱為**資產管理**。
    - **受管理裝置**現在稱為**資產（裝置）**。
    - **快速連結**已被重新命名為**主控台導覽**。
  - 如有必要，您可以將主選單最小化為圖示。
  - **卡巴斯基新聞**版塊已被從**監控** → **通知**中刪除。
- 您套用於**操作** → **修補程式管理** → **軟體弱點** and **操作** → **修補程式管理** → **軟體更新**部分中表格的篩選器現已成功儲存，且不會重設。
- 卡巴斯基安全管理中心 Linux 支援：
  - 使用 Kaspersky NGFW
  - 使用下列作業系統版本（針對受管理裝置）：
    - MosOS 15.5 Arbat
    - Microsoft Windows 11 25H2
    - CentOS 6.4
    - CentOS 6.6

Kaspersky Next XDR Optimum 產品授權下的 卡巴斯基安全管理中心 15.4 Linux

如果您在Kaspersky Next XDR Optimum 產品授權下啟動了管理伺服器，並將 Kaspersky Next XDR Optimum 產品授權金鑰部署到您的受管理應用程式，您可以執行以下操作：

- 按屬性對警示進行分組。
- 配置回應威脅的整合。

卡巴斯基安全管理中心 15.4 Linux

卡巴斯基安全管理中心 15.4 Linux 有幾項新功能和改善事項：

- 現在可以使用 Linux 裝置漫遊使用者的連線設定檔。透過使用連線設定檔，您可以為 Linux 裝置上的網絡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。
- 現在可以在管理伺服器之間傳輸加密金鑰。
- Kaspersky Thin Client現在受支援。
- Platform V Pangolin 內建高可用性叢集現在受支援。
- Postgres Pro 內建高可用性叢集現在受支援。安裝卡巴斯基安全管理中心 Linux時，此 DBMS 叢集的節點會在連接字串中指定。
- 卡巴斯基安全管理中心 Linux 現在支援搭配使用以下 DBMS：
  - Platform V Pangolin 6.5.1
  - Tantor SE 1C for Astra Linux 特別版 RUSB.10015-01（操作更新 1.8）
  - Jatoba 5
- 支援Platform V SberLinux OS Server (SLO) 版本 8.10.1、9.0.1、9.5.1。
- KlAkOAPI.tar.gz 存檔被從說明中刪除。KlAkOAPI.tar.gz 存檔位於卡巴斯基安全管理中心 Linux 安裝資料夾中。
- **掃描**按鈕被從**隔離**部分刪除。
- 網路代理獨立套件或在虛擬管理伺服器上建立的任何套件的安裝套件清單中不再有關於大小、檔案雜湊和路徑的資訊，因為這些獨立套件在下載時產生。

卡巴斯基安全管理中心 15.3 Linux

卡巴斯基安全管理中心 15.3 Linux 有幾項新功能和改善事項：

- klcsngtgui 實用程式已被從卡巴斯基安全管理中心 Linux 分發套件中刪除。我們建議使用 klnagchk 實用程式而不是 klcsngtgui 實用程式。
- 網路代理現在支援搭配使用以下新作業系統版本：
  - Windows Server 2025
  - Fedora Linux Server 41
  - Fedora Linux Workstation 41
- 卡巴斯基安全管理中心 Linux 現在支援搭配使用以下 DBMS：
  - PostgreSQL 17
  - Postgres Pro 17
- 現在，您可以使用 Kaspersky Update Utility 僅下載卡巴斯基安全應用程式所需的資料庫和軟體模組更新。在**將更新下載至管理伺服器儲存區**工作屬性視窗中，啟用**自動下載更新請求檔案**選項，然後指定卡巴斯基安全管理中心 Linux 將建立更新請求檔案以及要下載的更新相關資訊的路徑。
- 現在可以檢視 KSN 代理伺服器的使用統計資料。
- 使用 klbackup 公用程式將卡巴斯基安全管理中心 Windows 管理伺服器資料移轉到卡巴斯基安全管理中心 Linux 的功能已更新。現在，您可以將儲存在 Microsoft SQL Server 資料庫中的管理伺服器資料移轉到 PostgreSQL 或 Postgres Pro。
- 現在可以設定管理伺服器連線位址。管理伺服器連線位址在建立網路代理安裝套件時用作預設位址，並在將受管理裝置連線到 KSN 時用作 KSN 代理伺服器位址。
- 您現在可以集中重新啟動受管理裝置。
- 有關目前登入 Linux 受管理裝置的使用者的資訊，現在顯示在裝置內容視窗的**一般 → 連線**區段中。
- 現在您可以透過安裝在這些裝置上的網路代理，遠端存取 Linux 和 Windows 受管理裝置。使用 RDP、VNC 或 WDS 建立連線。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。
- 上傳並執行應用程式（或指令碼），以便在受管理裝置上進行診斷。現在您可以上傳包含可執行檔的目錄或存檔，或可執行檔本身。應用程式成功執行後，您可以下載執行結果。
- 使用者體驗改進，包括新的**快速連接**部分。該部分顯示主功能表地圖，並為您提供對卡巴斯基安全管理中心網頁主控台所有區段的快速存取。依預設，**快速連接**被設定為首頁。

卡巴斯基安全管理中心 15.2 Linux

卡巴斯基安全管理中心 15.2 Linux 有幾項新功能和改善事項：

- 管理內部使用者帳戶密碼的新功能：
  - 您現在可以強制內部使用者在首次（或下次）嘗試登入卡巴斯基安全管理中心網頁主控台時變更密碼的新選項。
  - 用於配置內部使用者帳戶密碼有效期限的新選項。
- 您現在可以使用 klbackup 實用程式備份卡巴斯基安全管理中心 Windows管理伺服器資料並在 卡巴斯基安全管理中心 Linux 中還原它。可以在相同類型的 DBMS 或 Microsoft SQL Server → MySQL 或 MariaDB 之間執行遷移，而不會遺失資料。
- 卡巴斯基安全管理中心 Linux 現在支援搭配使用以下 DBMS：
  - PostgreSQL 16.x
  - Postgres Pro 16.x
- 卡巴斯基安全管理中心 Linux 現在支援某些類型的 PostgreSQL 和 Postgres Pro 叢集。
- 支援新作業系統和新作業系統版本，包括新版本的 OS MES (Moscow Electronic School)、MosTech 和 MosTech Server。
- 使用者體驗改善包含：
  - 政策設定視窗中新增**儲存**按鈕。如果您想儲存變更而不關閉政策設定視窗，請使用此按鈕。
- 現在您可以管理向 Android 裝置傳送檔案、刪除先前發送的檔案，並在卡巴斯基行動裝置防護和管理外掛程式的新"應用程式和檔案"部分中配置其設定。
- 現在，您可以將應用程式安裝套件和裝置管理設定檔傳輸到行動裝置，而無需使用連接閘道上的新 Web 伺服器服務直接將它們連線到管理伺服器。

卡巴斯基安全管理中心 15.1 Linux

卡巴斯基安全管理中心 15.1 Linux 有幾項新功能和改善事項：

- 卡巴斯基安全管理中心網頁主控台現在支援透過卡巴斯基行動裝置防護和管理外掛程式進行行動裝置管理。
- 現在您可以透過 iOS MDM Server 設定外掛程式安裝和設定 iOS MDM 伺服器來管理 iOS MDM 裝置。
- 現在您可以管理行動裝置的憑證。
- Kaspersky Endpoint Security for Android 現在受支援。
- Kaspersky Security for iOS 現在受支援。

- Kaspersky Endpoint Security for Aurora 現在受支援。
- Windows 型受管理裝置的弱點和修補程式管理。您可以管理 Windows 型受管理裝置上安裝的第三方軟體更新，並透過安裝必要更新來修復此類軟體中的弱點。
- 卡巴斯基安全管理中心 Linux 現在逐頁輪詢網域控制器，而不是一次輪詢整個網域控制器。這允許您輪詢包含大量項目的網域控制器。
- 自適應異常控制。這是 Kaspersky Endpoint Security for Windows 的功能，它使用一組規則來追蹤用戶端裝置上的非典型行為，並允許您阻止異常操作。
- 無縫更新 Windows 裝置上安裝的受管理卡巴斯基應用程式和 Linux 網路代理。您可以透過核准必須安裝的更新和拒絕不得安裝的更新來管理更新安裝流程。
- 延伸政策稽核。現在您可以查看政策修訂內容並將政策修訂儲存到文件中。目前，這些功能僅適用於管理伺服器政策和網路代理政策。
- Cloud Discovery。這是一項全新功能，可讓您監控執行 Windows 之受管理裝置上的雲端服務使用狀況，並封鎖您認為不需要的雲端服務存取權限。
- 主功能表**監控**區域中的新**警示**子區域。在**警示**子區域中，您可以檢視有關在端點裝置上偵測到的威脅的資訊。這些威脅由卡巴斯基安全應用程式偵測到。
- 卡巴斯基安全管理中心 Linux 現在可以作為 Kaspersky Managed Detection and Response 解決方案的元件。
- 支援 Kaspersky Security for Virtualization Light Agent。
- macOS 裝置的延伸硬體清單。macOS 裝置上的網路代理將 MAC 位址和裝置序號傳送到管理伺服器。
- 現在，當您透過自訂指令碼在受管理裝置上安裝軟體時，您可以收到有關遠端安裝的報告。
- 當您在受管理裝置上執行多個自訂指令碼時，您可以設定每個指令碼的優先順序以定義執行順序。執行指令碼時，將執行優先順序最高的指令碼再執行優先順序最低的指令碼。
- 若要減少 Kaspersky Endpoint Security for Linux 和 Linux 版網路代理消耗的 RAM 量，您可以對 Linux 版網路代理啟用特殊工作模式。在此模式下，Linux 版網路代理需要較少的 RAM，但其功能會受到限制。
- 您可以透過*遠端解除安裝應用程式*工作從受管理裝置解除安裝不相容的軟體。
- 網路攻擊報告現在包含攻擊裝置的 MAC 位址和連接埠。
- 內部使用者的最大密碼長度增加至 256 個字元。
- 使用者體驗改善包含：
  - 透過新增卡巴斯基安全管理中心網頁主控台部分到書籤實現主選單個性化，以便從**書籤**區域快速存取。
  - 優化表格工作。現在每張表格的預設視圖都包含最常用的列。此外，您現在可以選擇目前頁面或整張表格中的所有項目，並對整張表格中的項目進行排序。
  - 改進的報告傳送配置。現在您可以指定最多 20 個電子郵件位址用於接收報告，以及報告傳送時間表。
- 支援多種作業系統和新作業系統版本。
- 制定了新的 Sizing Guide 並在線上說明中發佈。

- 經過使用者介面審查，導致**遠端診斷**區域出現在管理伺服器屬性視窗中的問題已解決。
- 您可以建立*遠端執行指令碼*工作以在用戶端裝置上執行安裝套件並遠端安裝應用程式。
- 在 Linux 上的用戶端裝置上安裝網路代理程式期間或之後，可以將使用者指定為裝置所有者。
- 您可以根據裝置所有者、裝置所有者在安全性群組中的成員資格，以及裝置所有者的角色來配置裝置分類或建立裝置移動規則。
- 您可以撤銷帳戶中的本機管理員權限。這為您提供了額外的使用者帳戶控制。例如，您可以在單次分配完成後撤銷本機管理員權限。
- 您可以變更本機帳戶密碼，例如，當使用者忘記本機帳戶密碼或執行排程的密碼變更時。
- 在**使用者憑證管理**子區域中，您可以指定要安裝的根憑證。例如，這些憑證可用於驗證網站或網頁伺服器的真確性。

卡巴斯基安全管理中心 15 Linux

卡巴斯基安全管理中心 15 Linux 有幾項新功能和改善事項：

- 網域控制器輪詢允許您輪詢 Microsoft Active Directory 網域控制器和 Samba 網域控制器。您可以使用管理伺服器或發佈點來輪詢 Microsoft Active Directory。您只能透過基於 Linux 的發佈點輪詢 Samba 網域控制器。當您輪詢網域控制器時，管理伺服器或發佈點會檢索有關網域中包含的裝置的網域結構、使用者帳戶、安全群組和 DNS 名稱的資訊。
- 卡巴斯基安全管理中心 Linux 現在支援搭配使用以下 DBMS：
  - PostgreSQL 15.x
  - Postgres Pro 15.x
- 如果您使用 PostgreSQL 或 Postgres Pro 作為 DBMS，卡巴斯基安全管理中心 Linux 支援多達 50,000 個受管理裝置。
- 從 Kaspersky Security Center Windows 遷移到 Kaspersky Security Center Linux。您可以執行精靈來遷移卡巴斯基安全管理中心物件，包括工作、政策和管理群組結構。之後，您可以將匯入的受管理裝置移至 卡巴斯基安全管理中心 Linux 的管理之下。
- 卡巴斯基安全管理中心 Linux 現在支援搭配使用以下卡巴斯基應用程式：
  - Kaspersky Security for Virtualization Light Agent
  - Kaspersky Embedded Systems Security for Windows
  - Kaspersky Embedded Systems Security for Linux
  - Kaspersky Industrial CyberSecurity for Nodes
  - Kaspersky Industrial CyberSecurity for Networks
  - Kaspersky Endpoint Security for Mac

- Kaspersky Endpoint Agent
- Kaspersky Security for Virtualization Light Agent

- 遠端診斷基於 Windows 和 Linux 的受管理裝置。
- 改進的應用程式控制元件。您現在可以根據選定資料夾中的可執行檔清單或卡巴斯基應用程式類別建立應用程式類別。然後，您可以指定在組織中允許還是封鎖建立的類別中的應用程式。
- 匯出和匯入事件選擇。您可以將使用者定義的事件選擇及其設定導出到 KLO 檔案，然後將儲存的事件選擇匯入到 Kaspersky Security Center Windows 或 卡巴斯基安全管理中心 Linux。
- 在威脅報告中，您現在可以透過點擊**檢視警示**連接來開啟威脅發展鏈。
- Kaspersky Security Center Linux 現在支援叢集技術。如果管理群組包含叢集或伺服器陣列，則"**資產（裝置）**"頁面將顯示兩個頁簽：一個用於單個裝置，另一個用於叢集和伺服器陣列。受管理裝置被偵測為叢集節點後，叢集將作為單獨物件被新增到**叢集和伺服器陣列**頁簽中。叢集節點與其他受管理裝置一起列在**裝置**頁簽上。
- 卡巴斯基安全管理中心 Linux 對某些平台的支援已終止，因為這些平台不再受到其供應商的支援。

卡巴斯基安全管理中心 14.2 Linux

卡巴斯基安全管理中心 14.2 Linux 有幾項新功能和改善事項：

- 在一個管理伺服器階層中，基於 Linux 的管理伺服器現在可以充當主伺服器，可以管理充當從屬伺服器的基於 Linux 或基於 Windows 的伺服器。
- 卡巴斯基安全管理中心 Linux 現在支援卡巴斯基安全網路 (KSN)、KSN 代理服務和卡巴斯基私有安全網路 (KPSN)。
- 卡巴斯基安全管理中心 Linux 現在支援 Kaspersky Security for Windows 為受管理應用程式。

  只有透過基於 Windows 的發佈點使用作業系統工具，才能在用戶端裝置上遠端安裝 Windows 網路代理。
- 基於 Windows 的受管理裝置上的資料現在可以被加密以降低膝上型電腦或硬碟磁碟機被盜或丟失時敏感資料和公司資料意外洩露的風險。此功能可通過 Kaspersky Endpoint Security for Windows 實現。
- 卡巴斯基安全管理中心 Linux 允許您直接在 卡巴斯基安全管理中心 Linux 的使用者介面中下載和更新卡巴斯基應用程式的分發套件和管理 Web 外掛程式。
- 預設情況下，安裝在 Linux 和 Windows 受管理裝置上的應用程式的相關資訊會被傳送到管理伺服器。
- 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。
- 在主管理伺服器、從屬管理伺服器和網路代理之間傳輸的敏感資料現在起將受到 AES 加密算法的防護。
- 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 Linux 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）
- 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*

卡巴斯基安全管理中心 14 Linux

卡巴斯基安全管理中心 Linux 有幾項新功能和改善事項：

- 除了*將更新下載至管理伺服器儲存區*工作，卡巴斯基安全應用程式的病毒資料庫現在可以透過*將更新下載至發佈點儲存區*進行下載。
- 受管理裝置上的病毒資料庫和應用程式模組可以透過管理伺服器或發佈點進行傳播和更新。您可以選取最適合您的組織的更新方案，以減少管理伺服器上的負載並最佳化公司網路上的資料流量。
- 卡巴斯基安全管理中心 Linux 僅從卡巴斯基更新伺服器下載卡巴斯基安全應用程式請求的更新。這減少了下載資料的大小。
- 您現在可以使用diff 檔案功能下載病毒資料庫和軟體模組。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。
- *更新驗證*工作已新增。透過使用此工作，您可以在受管理裝置上安裝更新之前自動檢查下載的更新的可操作性和錯誤。
- 卡巴斯基安全管理中心 Linux 現在支援 Kaspersky Industrial Cybersecurity for Linux Nodes 1.3 作為受管理應用程式。

已修復問題

下表列出了卡巴斯基安全管理中心 Linux 先前版本中發現的所有問題，它們已在目前版本中修復。

卡巴斯基安全管理中心 Linux 16.3 已修復問題清單

Kaspersky Security Center for Linux版本中首次出現此問題	問題ID	問題描述
16.2	9959974	已修復裝置內容視窗的 **事件** 索引標籤包含 **全選** 選項，該選項可能會從管理伺服器資料庫中刪除所有事件的問題。
16.2	9392997	已修復成功輪詢 ALD Pro 或 FreeIPA 網域控制器後，事件記錄中新增錯誤訊息的問題。
16.2	9504495	已修復透過網路代理安裝套件參數指派裝置所有者時，可能導致使用者指派錯誤的問題。
16.1	9316206	已修復在開啟 **雙步驟驗證** 索引標籤後重新整理瀏覽器時，控制按鈕可能會從該索引標籤消失的問題。
16.1	7555541	已修復建立 *變更帳戶密碼 (僅限 Linux)* 工作時，如果啟用 **設為一次性密碼（使用者必須在首次登入後變更密碼）** 選項，可能會導致無法登入網頁主控台的問題。
15.4	7555788	已修復如果使用者裝置上已啟用 SELinux，*變更帳戶密碼* 工作可能無法正常運作的問題。
16.2	9603496	已修復必須在管理伺服器裝置上安裝網路代理，才能取得此裝置診斷資訊的問題。
16.2	9704308	已修復在包含大量管理群組的環境中，於頁面載入期間開啟 **群組的階層** 區段可能會導致 `429 Too Many Requests` 錯誤、中斷與管理伺服器的連線，並將使用者重新導向至登入頁面的問題。
16.2	9989231	已修復依連線 IP 位址篩選裝置時可能傳回錯誤結果的問題。
16.2	9990025	已修復在頁面之間瀏覽時，**政策** 和 **工作** 區段中的表格檢視設定未保留的問題。
15.3	9632613	已修復當 LDAP 網域控制站無法使用或不包含使用者帳戶時，網域使用者登入網頁主控台可能會嚴重延遲的問題。
15.1	9829027	已修復在 **病毒資料庫使用報告** 中設定 **更新狀態** 篩選器時可能導致錯誤的問題。
15.1	9844707	即使已設定代理伺服器，卡巴斯基安全管理中心和 FCM (Firebase Cloud Messaging) 仍會直接互動。

卡巴斯基安全管理中心 Linux 16.2 已修復問題清單

Kaspersky Security Center for Linux版本中首次出現此問題	問題ID	問題描述
15.1	10071566	修正了如果工作排程使用"按星期幾"設定則對工作排程所做的變更未傳播至受管理裝置的問題。
15.4	9067754	修復了以下問題：更新卡巴斯基行動裝置保護和管理外掛程式後導致新事件在之前建立的政策中顯示錯誤。
16	9329729	顯示Kaspersky Security Center for Linux從16版升級到16.1版後，如果在升級前為某些使用者設定了雙因素身份驗證，卡巴斯基事件日誌中會出現錯誤。
16.1	9256000	修復了以下問題：如果網路代理安裝在Microsoft Windows XP上，則無法獲得有關託管應用程式元件的資訊。
16.1	9251629	修復了以下問題：登入卡巴斯基安全管理中心網頁主控台時，某些必要的HTTP回應標頭未新增。

關於 卡巴斯基安全管理中心 Linux

本節說明卡巴斯基安全管理中心 Linux 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。

卡巴斯基安全管理中心 Linux（也稱為“卡巴斯基安全管理中心”）旨在透過使用 Linux 管理伺服器來部署和管理對用戶端裝置的防護。

卡巴斯基安全管理中心 Linux 使您能夠在公司網路的裝置上安裝卡巴斯基安全應用程式、遠端執行掃描和更新工作以及管理受管理受管理應用程式的安全政策。作為管理員，您可以使用資料詳細的主控台介面，該主控台提供公司裝置狀態的快照、詳細報告以及防護政策中的細項設定。

與擁有 Windows® 管理伺服器的卡巴斯基安全管理中心相比，卡巴斯基安全管理中心 Linux 有一個不同的功能集。

卡巴斯基安全管理中心 Linux 是一款主要供公司網路管理員和各種組織中負責裝置防護的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。
- 執行卡巴斯基和其他軟體供應商的應用程式遠端安裝。
- 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。
- 管理儲存在基於 Windows 的裝置的硬碟磁碟機和卸除式磁碟機上的資訊加密。
- 管理使用者對基於 Windows 的裝置上的加密資料的存取。
- 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 Linux。

如果透過 Kaspersky 購買卡巴斯基安全管理中心 Linux，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。

分發套件

在卡巴斯基網站上，您可以下載應用程式的所有必要分發套件。
卡巴斯基安全管理中心 Linux 分發套件包含以下檔案：

Kaspersky Security Center for Linux管理伺服器：

- 將安裝在運行Debian作業系統的裝置上的管理伺服器：
  ksc64_16.2.0-<build>_amd64.deb
- 將安裝在運行Red Hat Enterprise Linux作業系統的裝置上的管理伺服器：
  ksc64-16.2.0-<build>.x86_64.rpm

卡巴斯基安全管理中心網頁主控台：

- 將安裝在運行Debian作業系統的裝置上的網頁主控台：
  ksc-web-console-16.2.<build>.x86_64.deb
- 將被安裝在運行Red Hat Enterprise Linux作業系統的裝置上的網頁主控台：
  ksc-web-console-16.2.<build>.x86_64.rpm

Windows網路代理程式：

- 將安裝在包含x86-32或x64架構的裝置上的網路代理程式：
  ksc_16_16.2.0.<build>_NetAgent_<localization>.zip
- 將安裝在Arm架構的裝置上的網路代理程式：
  klnagent_winarm64-16.2.0.<build>-win_<localization>.zip
- 在運行Arm 64位元作業系統的裝置上遠端安裝網路代理程式的公用程式：
  ri_utils_arm64.zip
- 在運行32位元或64位元作業系統的裝置上遠端安裝網路代理程式的公用程式：
  ri_utils_win32.zip

Linux網路代理程式：

- 將被安裝在運行Debian作業系統的裝置上的網路代理程式：
  klnagent64_16.2.0-<組建>_<架構>.deb
- 將安裝在運行Red Hat Enterprise Linux作業系統的裝置上的網路代理程式：
  klnagent64-16.2.0-<組建>_<架構>.rpm
- 在運行Debian作業系統的裝置上遠端安裝網路代理程式的檔案：
  klnagent-<架構>-16.1.0.6517-deb_<在地化>.tar.gz
- 在運行Red Hat Enterprise Linux作業系統的裝置上遠端安裝網路代理程式的檔案：
  klnagent-<架構>-16.1.0.6517-rpm_<在地化>.tar.gz

- Linux網路代理程式的單一分發套件：

  klnagent-ALL-16.2.0.<組建>-ALL_<在地化>.tar.gz

  如果您有許多具有不同CPU架構和不同Linux的作業系統的用戶端裝置，單一分發套件會很有用。系統將自動選擇所需的網路代理程式版本，以便在裝置上進行後續安裝。

Kaspersky Endpoint Detection and Response Optimum網頁外掛程式：

- signed_irp.zip

> 您只能從應用程式的分發套件儲存庫中下載網頁外掛以進行遠端安裝。

如果您在選擇適用於 Linux 的網路代理安裝套件時遇到困難，請參閱文章：如何選擇適用於 Linux 的網路代理安裝套件。

硬體和軟體需求

- 管理伺服器要求
- 網頁主控台要求
- 網路代理要求

有關部署防護和管理行動裝置的 Android 和 iOS 版本要求，請參閱Kaspersky Security for Mobile for Mobile 說明和Kaspersky Secure Mobility Management 說明。

管理伺服器要求

最小硬體條件：

- 執行頻率為 2.5 GHz 或更高、2 核心的 CPU。
- RAM：6 GB。

  您需要在安裝了管理伺服器的裝置上啟用交換檔案。交換檔案的最小大小必須大於 RAM 容量的 1.5 倍。
- 可用磁碟空間：儲存管理伺服器資料的資料夾 (/var/opt/kaspersky/klnagent_srv) 需要 10 GB。

> 建議在裝置上安裝管理伺服器後，在該裝置上安裝 Kaspersky Endpoint Security for Linux。
> 若要進行併發安裝，您必須至少具備 300 IOPS，並在管理伺服器要求之外增加 1.5 GB RAM 和 15% CPU。
> 如需 Kaspersky Endpoint Security 的硬體需求，請參閱 Kaspersky Endpoint Security for Linux 說明。

支援以下作業系統：

> 對於作業系統中的進程間通訊，必須提供環回介面。

- Debian GNU/Linux 12 (Bookworm) 64 位元
- Debian GNU/Linux 13 (Trixie) 64位元
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 位元
- Ubuntu Server 24.04 LTS (Noble Numbat) 64 位元
- Ubuntu Server 26.04 LTS (Resolute Raccoon) 64 位元
- CentOS Stream 9 64 位元
- CentOS Stream 10 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
- Red Hat Enterprise Linux Server 10.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
- 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.10015-01（操作更新 1.8）64 位元
- Astra Linux 特別版 RUSB.10015-16（版本 1）（操作更新 1.6）64 位元
- Astra Linux 特別版 RUSB.10015-17（操作更新 1.7.3）64 位元
- Astra Linux 特別版 RUSB.10015-03（操作更新 7.6）64 位元
- Astra Linux 特別版 RUSB.10015-37（操作更新 7.7）64 位元
- Astra Linux 通用版（操作更新 2.12）64 位元
- ALT SP Server 10 64 位元
- ALT SP Workstation 10 64 位元
- Oracle Linux 7 64 位元
- Oracle Linux 8 64 位元

- Oracle Linux 9 64 位元
- Platform V SberLinux OS Server (SLO) 8.10.1 64 位元
- Platform V SberLinux OS Server (SLO) 9.5.1 64 位元
- Platform V SberLinux OS Server (SLO) 9.6 64 位元
- Platform V SberLinux OS Server (SLO) 9.7 64 位元
- RED OS 7.3 Server 64 位元
- RED OS 7.3 Certified Edition 64 位元
- RED OS 8 64 位元
- ROSA COBALT 7.9 64 位元
- M OS (Moscow Electronic School) 12 Server 64 位元
- Mostech Server 64 位元
- MosOS 15.5 Arbat 64 位元

建議您使用 EXT4 檔案系統及其預設設定。

支援以下資料庫伺服器（可以安裝在不同的裝置上）：

- 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
- MySQL Standard Edition 8.4 32 位元 / 64 位元
- MySQL Enterprise Edition 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 10.4.20 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 10.6（組建編號 10.6.20 及以上）32 位元/64 位元
- MariaDB 10.11（組建編號 10.11.10 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
- PostgreSQL 15.x 64 位元

- PostgreSQL 15.x 64 位元（叢集 Corosync/Pacemaker）
- PostgreSQL 16.x 64 位元
- PostgreSQL 17 64 位元
- PostgreSQL 18 64 位元
- Postgres Pro 13.x 64 位元（所有版本）
- Postgres Pro 14.x 64 位元（所有版本）
- Postgres Pro 15.x 64 位元（所有版本）
- Postgres Pro 15.x 64 位元（叢集 Corosync/Pacemaker）
- Postgres Pro 16.x 64 位元（所有版本）
- Postgres Pro 16.x Enterprise 64 位元（叢集內建高可用）
- Postgres Pro 17.x 64 位元（所有版本）
- Postgres Pro 17.x Enterprise 64 位元（叢集內建高可用）
- Postgres Pro 18 64 位元（所有版本）
- Postgres Pro 18 Enterprise 64 位元（叢集內建高可用）
- Platform V Pangolin 6.5.1 64 位元
- Platform V Pangolin 6.5.1 64 位元（叢集內建高可用性）
- Jatoba 4 64 位元
- Jatoba 5 64 位元
- Tantor SE 1C 64 位元

支援高可用 PostgreSQL 叢集。詳情請參閱以下文章：為Kaspersky Security Center for Linux準備高可用性DBMS叢集。

如需支援的虛擬化平台相關資訊，請參閱Kaspersky Security for Virtualization Light Agent線上說明。

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：2個核心，運作頻率：2.5GHz。
- RAM：4 GB。
- 可用磁碟空間：40GB，用於儲存管理伺服器資料的資料夾/var/opt/kaspersky。

建議在裝置上安裝卡巴斯基安全管理中心網頁主控台後，也在該裝置上安裝 Kaspersky Endpoint Security for Linux。對於Kaspersky Endpoint Security的硬體需求，請參閱 Kaspersky Endpoint Security for Linux 說明。

須為以下作業系統之一（**僅限 64 位元版本**）：

> 對於作業系統中的進程間通訊，必須提供環回介面。

- Debian GNU/Linux 12 (Bookworm)
- Debian GNU/Linux 13 (Trixie)
- Ubuntu Server 22.04 LTS (Jammy Jellyfish)
- Ubuntu Server 24.04 LTS (Noble Numbat)
- Ubuntu Server 26.04 LTS (Resolute Raccoon) 64 位元
- CentOS Stream 9
- CentOS Stream 10
- Red Hat Enterprise Linux Server 7.x
- Red Hat Enterprise Linux Server 8.x
- Red Hat Enterprise Linux Server 9.x
- Red Hat Enterprise Linux Server 10.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.10015-16（版本 1）（操作更新 1.6）

- Astra Linux 特別版 RUSB.10015-01（操作更新 1.7）
- Astra Linux 特別版 RUSB.10015-17（操作更新 1.7.3）
- Astra Linux 特別版 RUSB.10015-01（操作更新 1.8）
- Astra Linux 特別版 RUSB.10015-03（操作更新 7.6）
- Astra Linux 特別版 RUSB.10015-37（操作更新 7.7）
- Astra Linux 通用版 2.12
- ALT SP Server 10
- ALT SP Workstation 10
- Oracle Linux 7
- Oracle Linux 8
- Oracle Linux 9
- Platform V SberLinux OS Server (SLO) 8.10.1
- Platform V SberLinux OS Server (SLO) 9.5.1
- Platform V SberLinux OS Server (SLO) 9.6 64 位元
- Platform V SberLinux OS Server (SLO) 9.7 64 位元
- RED OS 7.3 Server
- RED OS 7.3 認證版
- RED OS 8
- ROSA COBALT 7.9
- M OS (Moscow Electronic School) 12 伺服器
- Mostech Server
- MosOS 15.5 Arbat

如需支援的虛擬化平台相關資訊，請參閱Kaspersky Security for Virtualization Light Agent線上說明。

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：

- Google Chrome 149.0.7827.115 或更新版本
- Microsoft Edge 149.0.4022.62 或更新版本
- macOS Safari 18.6（20621.3.11.11.3版本）
- Yandex Browser 26.4.4.799 或更高版本
- Mozilla Firefox 延伸支援版本 140.11.0 或更新版本

網路代理要求

最小硬體條件：

- 執行頻率為 1 GHz 或更高的 CPU。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。

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。

網路代理。支援的平台

作業系統。Microsoft Windows 工作站	Microsoft Windows Embedded POSReady 2009 with latest Service Pack 32 位元 Microsoft Windows Embedded 7 Standard (Service Pack 1) 32 位元/64 位元 Microsoft Windows Embedded 8.1 Industry Pro 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、1709、1803、1809 32 位元/64 位元 Microsoft Windows 10 20H2、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 TH1（2015 年 7 月）家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 10 TH2（2015 年 11 月）家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 10 RS1（2016 年 8 月）家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 10 RS2（2017 年 4 月）家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 10 RS3（秋季創作者更新，v1709）家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 10 RS4（2018 年 4 月更新，17134）家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 10 RS5（2018 年 10 月）家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 10 RS6（2019 年 5 月）家用版/專業版/工作站專業版/企業版/教育版 64 位元 Microsoft Windows 10 19H1、19H2 家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 10 20H1（2020 年 5 月更新）家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 10 20H2（2020 年 10 月更新）家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 10 21H1（2021 年 5 月更新）家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 10 21H2（2021 年 10 月更新）家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 10 22H2（2023 年 10 月更新）家用版/專業版/工作站專業版/企業版/教育版 32 位元/64 位元 Microsoft Windows 11 家用版/專業版/工作站專業版/企業版/教育版 64 位元 Microsoft Windows 11 家用版/專業版/工作站專業版/企業版/教育版 64 位元 Microsoft Windows 11 IoT企業版25H2 64位元 Microsoft Windows 11 22H2 家用版/專業版/工作站專業版/企業版/教育版 64 位元 Microsoft Windows 11 23H2 家用版/專業版/工作站專業版/企業版/教育版 64 位元 Microsoft Windows 11 24H2 家用版/專業版/工作站專業版/企業版/教育版 64 位元 Microsoft Windows 11 25H2 家用版/專業版/工作站專業版/企業版/教育版 64 位元 Microsoft Windows 8.1 專業版/企業版 32 位元/64 位元 Microsoft Windows 8 專業版/企業版 32 位元/64 位元 Microsoft Windows 7 專業版/企業版/旗艦版/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 2）32 位元/64 位元（僅受網路代理版本 10.5.1781 支援） Microsoft Windows XP Professional Service Pack 3及更高的32位元版本 （受網路代理版本14.0.0.20023支援，需要Windows XP的安全更新KB2868626） 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）

作業系統。Microsoft Windows 伺服器	Microsoft Windows MultiPoint Server 2011 Standard/Premium 64 位元 Microsoft Windows Server 2003 SP1 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 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） Microsoft 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） Microsoft Windows Server 2008 Foundation (Service Pack 2) 32 位元/64 位元 Microsoft Windows Server 2008 Standard/Enterprise/Datacenter (Service Pack 2) 32 位元/64 位元 Microsoft Windows Server 2008 R2 Datacenter/Enterprise/Foundation/Core Mode/Standard（Service Pack 1 和更高版本）64 位元 Microsoft Windows Server 2012 Server Core/Datacenter/Essentials/Foundation/Standard 64 位元 Microsoft Windows Server 2012 R2 Server Core/Datacenter/Essentials/Foundation/Standard 64 位元 Microsoft Windows Server 2016 Datacenter/Standard/Server Core（安裝選項）(LTSB) 64 位元 Microsoft Windows Server 2019 Standard/Datacenter/Core 64 位元 Microsoft Windows Server 2019 RS5 Essentials/Standard 64 位元 Microsoft Windows Server 2022 Standard/Datacenter/Core 64 位元 Microsoft Windows Server 2025 Standard/Datacenter/Core 64 位元 Microsoft Windows Server 2022 21H2 Standard/Datacenter 64 位元 Microsoft Windows Storage Server 2019 64 位元 Microsoft Windows Small Business Server 2011 Standard 64 位元 Microsoft Windows Small Business Server 2011 Essentials 64 位元 Microsoft Windows Small Business Server 2011 Premium Add-on 64 位元

作業系統。Linux	Debian GNU/Linux 10.x (Buster) 32 位元 / 64 位元 Debian GNU/Linux 11.x (Bullseye) 32 位元/64 位元 Debian GNU/Linux 12 (Bookworm) 32 位元 / 64 位元 Debian GNU/Linux 13 (Trixie) 64位元 Ubuntu Server 10.04 LTS (Lucid Lynx) 32 位元/64 位元 Ubuntu Server 16.04 LTS (Xenial Xerus) 32 位元 / 64 位元 Ubuntu Server 18.04 LTS (Bionic Beaver) 64 位元 Ubuntu Server 20.04 LTS (Focal Fossa) 64 位元 Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 位元 Ubuntu Server 22.04 LTS ARM 64 位元 Ubuntu Server 24.04 LTS (Noble Numbat) 64 位元 Ubuntu Server 26.04 LTS (Resolute Raccoon) 64 位元 Ubuntu Server 26.04 LTS ARM 64 位元 Ubuntu Desktop 10.04 LTS (Lucid Lynx) 32 位元/64 位元 Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32 位元 / 64 位元 CentOS 5.2 32 位元/64 位元（僅受 Linux Legacy 版網路代理支援，您可以透過網頁主控台介面或從卡巴斯基網站下載該網路代理） CentOS 5.4 32 位元/64 位元（僅受 Linux Legacy 版網路代理支援，您可以透過網頁主控台介面或從卡巴斯基網站下載該網路代理） CentOS 6.4 32 位元/64 位元（僅受 Linux Legacy 版網路代理支援，您可以透過網頁主控台介面或從卡巴斯基網站下載該網路代理） CentOS 6.6 32 位元/64 位元（僅受 Linux Legacy 版網路代理支援，您可以透過網頁主控台介面或從卡巴斯基網站下載該網路代理） CentOS 7.2 及更高版本 64 位元 CentOS Stream 8 64 位元 CentOS Stream 9 64 位元 CentOS Stream 9 ARM 64 位元 CentOS Stream 10 64位元 Red Hat Enterprise Linux Server 6.x 32 位元/64 位元 Red Hat Enterprise Linux Server 7.2 和更高版本 64 位元 Red Hat Enterprise Linux Server 8.x 64 位元 Red Hat Enterprise Linux Server 9.x 64 位元 Red Hat Enterprise Linux Server 10.x 64位元 SUSE Linux Enterprise Server 12.5 和更高版本（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 Server 15（所有服務套件）ARM 64 位元 openSUSE Leap 15 64 位元 EulerOS 2.0 SP10 64 位元 EulerOS 2.0 SP10 ARM 64 位元 Astra Linux Special Edition RUSB.10015-01（操作更新 1.4）32 位元 Astra Linux Special Edition RUSB.10015-01（操作更新 1.4）64 位元（僅受 Linux Legacy 版網路代理支援，您可以使用網頁主控台介面或從卡巴斯基網站下載此網路代理） Astra Linux 特別版 RUSB.10015-01（操作更新 1.5）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.10015-16（版本 1）（操作更新 1.6）64 位元 Astra Linux 特別版 RUSB.10015-17（操作更新 1.7.3）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.10015-01（操作更新 1.8）64 位元 Astra Linux 特別版 RUSB.10015-03（操作更新 7.6）64 位元 Astra Linux 特別版 RUSB.10015-37（操作更新 7.7）64 位元 Astra Linux 特別版 RUSB.10152-02（操作更新 4.7）ARM 64 位元 Astra Linux 通用版（操作更新 2.12）64 位元 ALT Workstation 11 64位元 ALT Server 11 64位元 ALT Education 11 64位元 ALT Workstation 10.1 64 位元 ALT Server 10.1 64 位元

ALT Education 10.1 64 位元
ALT SP Server 10 32 位元/64 位元
ALT SP Server 10 ARM 64 位元
ALT SP Workstation 10 32 位元/64 位元
ALT SP Workstation 10 ARM 64 位元
ALT 8 SP Server (LKNV.11100-01) 32 位元/64 位元
ALT 8 SP Server (LKNV.11100-02) 32 位元/64 位元
ALT 8 SP Server (LKNV.11100-03) 32 位元/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
Oracle Linux 7 64 位元
Oracle Linux 8 64 位元
Oracle Linux 9 64 位元
Linux Mint 21.1 及更高版本 64 位元
Linux Mint 22.x 64 位元
AlterOS 7.5 及更高版本 64 位元
AlterOS 2025 64位元
GosLinux IC6/7.17 64 位元
GosLinux IC6/7.2 64 位元
SberOS 3.4.0 64位元
SberOS 3.5.0 64位元
SberOS 3.6.1 64 位元
Platform V SberLinux OS Server (SLO) 8.10.1 64 位元
Platform V SberLinux OS Server (SLO) 9.1 64 位元
Platform V SberLinux OS Server (SLO) 9.5.1 64 位元
Platform V SberLinux OS Server (SLO) 9.6 64 位元
Platform V SberLinux OS Server (SLO) 9.7 64 位元
RED OS 7.3 Server 64 位元
RED OS 7.3 Certified Edition 64 位元
RED OS 8 64 位元
RED OS 8 ARM 64 位元
ROSA Enterprise Linux Server 7.9 64 位元
ROSA Enterprise Linux Desktop 7.9 64 位元
ROSA COBALT 7.9 64 位元
ROSA CHROME 12 64 位元
AlmaLinux 8 及更高版本 64 位元
AlmaLinux 9 及更高版本 64 位元
Rocky Linux 8 及更高版本 64 位元
Rocky Linux 9 及更高版本 64 位元
Atlant · Alcyone build · 版本 2022.02 64 位元
MSVSPHERE 9.2 伺服器 64 位元
MSVSPHERE 9.2 ARM 64 位元
MSVSPHERE 9.4 伺服器 64 位元
MSVSPHERE 9.4 ARM 64 位元
SynthesisM 伺服器 8.6 64 位元
SynthesisM 用戶端 8.6 64 位元
OSnova 2.* 64 位元
OSnova 3.* 64位元
Kylin 10 64 位元
EMIAS 1.0 64 位元
Amazon Linux 2 64 位元
MosOS 15.5 Arbat 64 位元
OS MES (Moscow Electronic School) 12（適用於電腦和膝上型電腦）64 位
OS MES (Moscow Electronic School) 12 Server （適用於互動平板電腦） 64 位元
M OS (Moscow Electronic School) 12 Server 64 位元

	Mostech 64 位元 Mostech Server 64 位元 Fedora Linux Server 41 64 位元 Fedora Linux Workstation 41 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。
虛擬化平台	如需支援的虛擬化平台相關資訊，請參閱Kaspersky Security for Virtualization Light Agent線上說明。

在早於Microsoft Windows Server 2008 R2（伺服器版本）和Microsoft Windows 7（桌面版）的Windows版本上，網路代理程式不支援下列功能：

- 更新重譯（發佈點使用）
- KSN代理程式（發佈點使用）
- 弱點掃描工作

在執行 Microsoft 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 MultiPoint Server 2011 的裝置上安裝網路代理之前，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 的安全性更新 (KB3063858)，適用於 x64 型系統的 Windows 7 安全性更新 (KB3063858)，適用於 Windows Server 2008 的安全性更新 (KB3063858)，適用於 Windows Server 2008 x64 版的安全性更新 (KB3063858)，適用於 Windows Server 2008 R2 x64 版的安全性更新 (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 的網路代理所需版本。

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

卡巴斯基安全管理中心 Linux 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 Linux 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。要了解應用程式和解決方案的版本，請參閱應用程式支援生命週期網頁。

受支援的卡巴斯基應用程式：

- Kaspersky Endpoint Security for Windows（支援檔案伺服器）
- Kaspersky Endpoint Security for Linux（支援檔案伺服器）
- Kaspersky Endpoint Security for Linux Elbrus Edition
- Kaspersky Endpoint Security for Mac
- Kaspersky Endpoint Security for Android
- Kaspersky Endpoint Security for Aurora
- Kaspersky Security for iOS
- Kaspersky Industrial CyberSecurity for Linux Nodes
- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Endpoint Agent
- Kaspersky Embedded Systems Security for Windows
- Kaspersky Embedded Systems Security for Linux
- Kaspersky Security for Virtualization Light Agent
- KATA Sandbox（Kaspersky Anti Targeted Attack Platform 的元件之一）
- Kaspersky Thin Client
- Kaspersky NGFW
- Kaspersky Sandbox
- Kaspersky Vulnerability Management

卡巴斯基安全管理中心 Linux 包含在以下解決方案中：

- Kaspersky Endpoint Detection and Response Optimum
- Kaspersky Managed Detection and Response
- Kaspersky Next XDR Optimum

請參閱適用於應用程式版本的產品支援生命週期網頁。

已知問題

Kaspersky Industrial CyberSecurity for Networks 不支援單一登入 (SSO)。

關於卡巴斯基安全管理中心 Linux 元件的相容性

在下表中，您可以找到有關卡巴斯基安全管理中心 Linux 元件相容性的資訊。

卡巴斯基安全管理中心 Linux 元件的相容性

元件	相容於
卡巴斯基安全管理中心 16.3 Linux 管理伺服器	• 以下版本的卡巴斯基安全管理中心網頁主控台：16.3、16.2、16.1 • 以下版本的卡巴斯基安全管理中心網路代理：16.3、16.2、16.1、16、15.4、15.3、15.2、15.1、15、14*、10.5**
卡巴斯基安全管理中心 16.3 網頁主控台	以下版本的卡巴斯基安全管理中心 Linux 管理伺服器：16.3、16.2、16.1、16
卡巴斯基安全管理中心 16.3 Linux 主管理伺服器	從屬管理伺服器： • 以下版本的卡巴斯基安全管理中心 Linux：16.3、16.2、16.1、16、15.4、15.3、15.2、15.1、15 • 下列版本的卡巴斯基安全管理中心 Windows：15.1
卡巴斯基安全管理中心 16.3 Linux 從屬管理伺服器	主管理伺服器： • 以下版本的卡巴斯基安全管理中心 Linux：16.3、16.2、16.1、16、15.4、15.3、15.2、15.1、15 • 下列版本的卡巴斯基安全管理中心 Windows：15.1
卡巴斯基安全管理中心 16.3 網路代理	管理伺服器： • 以下版本的卡巴斯基安全管理中心 Linux：16.3、16.2、16.1、16、15.4、15.3、15.2、15.1、15 • 下列版本的卡巴斯基安全管理中心 Windows：15.1
備份和還原卡巴斯基安全管理中心管理伺服器資料	以下卡巴斯基安全管理中心 Linux 管理伺服器版本支援資料備份與還原： 16.2、16.1、16、15.4、15.3、15.2、15.1、15

*此版本支援安裝了 Service Pack 3 的 Microsoft Windows XP Professional。您可以從此頁面下載此版本的網路代理程式。

**此版本支援安裝了 Service Pack 2 的 Microsoft Windows XP Professional。您可以透過技術支援申請取得此版本的網路代理程式。

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可能會受到限制。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，您必須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。

如果您擁有最新版本的卡巴斯基安全管理中心網頁主控台和先前版本的卡巴斯基安全管理中心，並且在網域身分驗證期間發生錯誤，錯誤文字將包含預設訊息。

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的資訊。有關基於 Windows 的解決方案的詳細資訊，請參閱卡巴斯基安全管理中心 Windows 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 15.1 Windows	卡巴斯基安全管理中心 16.3 Linux
管理伺服器		
資料庫管理系統 (DBMS) 地點	內部部署	內部部署 （不支援 Microsoft SQL）
在其上安裝管理伺服器的作業系統	Windows	Linux
管理伺服器階層	✓	✓
支援虛擬管理伺服器	✓	✓
部署卡巴斯基安全管理中心容錯移轉叢集	✓ 僅限單站點叢集	✓ 從Kaspersky Security Center for Linux 16.2版本開始，支援異地分散式故障轉移叢集
使用SNMP將管理伺服器統計資訊傳送到協力廠商應用程式	✓	✓
用於發布安裝套件和其他檔案的網頁伺服器	✓	✓
管理主控台		
管理主控台類型	基於 MMC 和基於網頁	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
使用網域身分驗證登入主控台	✓	✓
管理用戶端裝置和管理群組		
每個管理伺服器的最大受管理裝置數量	100,000（使用 Microsoft SQL Server）	50,000（使用 PostgreSQL 和 Postgres Pro）
網路輪詢	✓	✓
對受 Windows、macOS 和 Linux 管理的裝置的防護	✓	✓
對行動裝置的防護	✓ 行動裝置的基本管理	✓ MDM 和使用 Kaspersky Secure Mobility Management 功能（需取得產品授權）
虛擬機的防護管理	✓	✓
對公有雲端基礎結構的防護	✓	—
用戶端裝置的桌面遠端連線	✓	✓
資料加密與防護	✓ 在安裝有 Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Mac 的 Windows 受管理裝置上	✓ 在安裝有 Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Mac 的 Windows 受管理裝置上

功能或內容	卡巴斯基安全管理中心 15.1 Windows	卡巴斯基安全管理中心 16.3 Linux
支援管理群組中的叢集和伺服器陣列	✓	✓
管理群組階層	✓	✓
在 DMZ 中新增連線閘道作為發佈點	✓ （不支援網頁主控台）	✓
與使用者一起使用		
建立和管理使用者帳戶	✓	✓
管理卡巴斯基應用程式		
應用程式政策	✓	✓
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	✓	✓
用戶端裝置的遠端診斷	✓	✓
自動更新卡巴斯基應用程式	✓	✓
自適應異常控制支援	✓	✓
以裝置為中心的安全管理	✓	✓
以使用者為中心的安全管理	✓	✓
系統管理		
佈署作業系統至用戶端裝置	✓	—
管理協力廠商產品授權	✓	計劃於 2026 年實現
將管理伺服器用作 WSUS 伺服器	✓	✓ （僅限 Windows Update 被動搜尋模式）
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和修復協力廠商軟體弱點	✓	✓
匯出和匯出應用程式類別	✓ （不支援網頁主控台）	計劃於 2026 年實現
監控、報告和稽核		
管理物件修訂	✓	✓
比較政策修訂	✓	✓
檢視和使用 Kaspersky Endpoint Detection and Response Optimum 偵測到的警報	✓	✓
有關發生在受管理裝置上的事件的通知	✓	✓
監控政策狀態和工作狀態	✓	✓
整合		
與 Kaspersky Managed Detection and Response 整合	✓	✓
與 SIEM 系統整合	✓	✓
透過 Active Directory、KASAP 和 Kaspersky TIP Sandbox 聚合警示和執行回應操作	—	✓ 必須使用 Kaspersky Next XDR Optimum 產品授權來啟用管理伺服器，然後將 Kaspersky Next XDR Optimum 產品授權金鑰部署到受管理應用程式

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

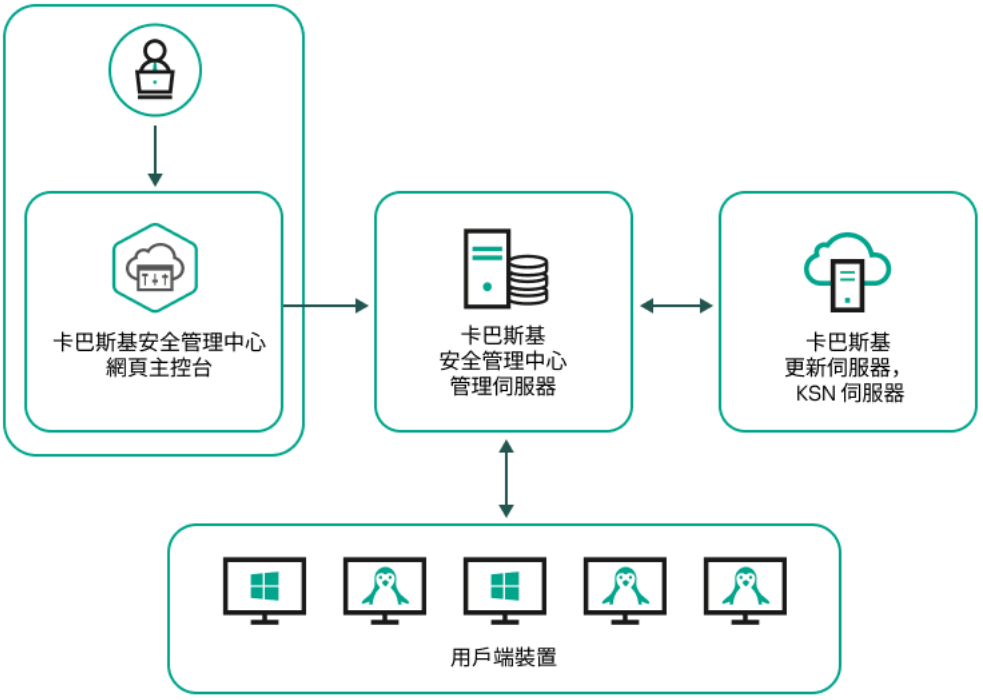
關於卡巴斯基安全管理中心雲端主控台 及其功能 的更多資訊請見卡巴斯基安全管理中心雲端主控台文檔 和 Kaspersky Endpoint Security for Business 文檔 。

架構和基本概念

本章節解釋關於卡巴斯基安全管理中心 Linux 的應用程式架構和基本概念。

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。



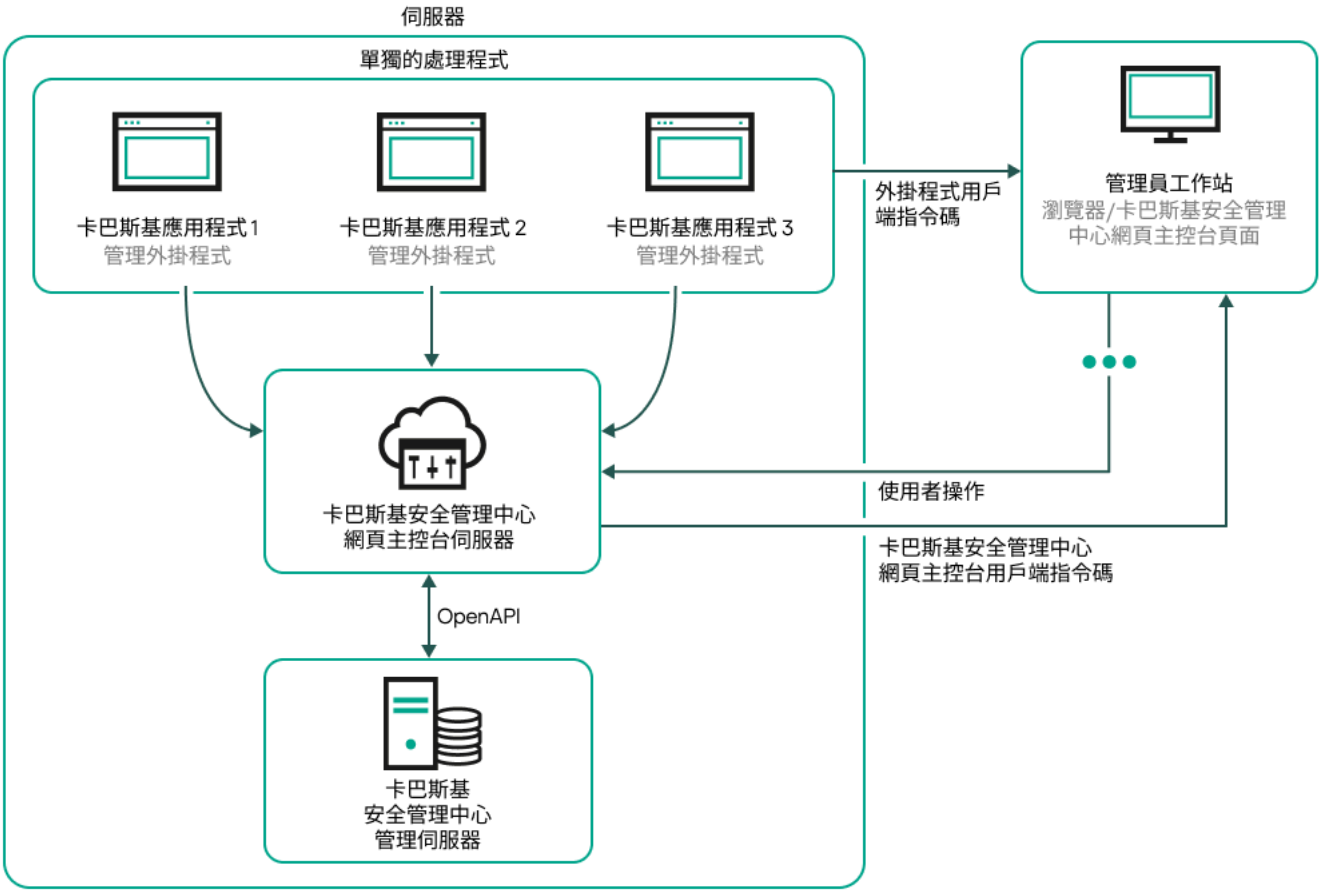
卡巴斯基安全管理中心 Linux 架構

卡巴斯基安全管理中心 Linux 含有以下主要元件：

- **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 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 Linux 防護。每個需要防護的裝置都必須安裝一個 Kaspersky 安全應用程式。

卡巴斯基安全管理中心 Linux 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 Linux 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 Linux 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 Linux 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 Linux 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 Linux 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。如果願意，您可以變更每個預設連接埠號。

埠號	開啟連接埠的處理程序名稱	協定	連接埠目的	範圍
8060	klcsweb	TCP	傳輸發佈的安裝套件到用戶端裝置	發佈安裝套件。 您可以在管理伺服器內容視窗的**網頁伺服器**區段中變更預設連接埠號。 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。 您可以在管理伺服器內容視窗的**網頁伺服器**區段中變更預設連接埠號。
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。 您可以在安裝 卡巴斯基安全管理中心 Linux 的過程中設定連線的連接埠時，變更用於從網路代理接收連線的預設埠號；您可以在建立管理伺服器的階層時，變更用於從次要管理伺服器接收連線的預設埠號。
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。 您可以在網路代理政策設定中變更預設埠號。
13291	klserver	TCP (TLS)	使用 klakaut 實用程式自動化卡巴斯基安全管理中心 Linux 操作	使用 klakaut 實用程式。klakaut 實用程式及其說明系統位於卡巴斯基安全管理中心 Linux 的安裝資料夾中。 預設情況下此連接埠已關閉。如果您想使用 klakaut 實用程式自動執行卡巴斯基安全管理中心 Linux 操作，請使用 klscflag 實用程式開啟 13291 連接埠。
13299	klserver	TCP (TLS)	接收從卡身分和存取管理器 (IAM) 到管理伺服器的連線；接收透過 OpenAPI 到管理伺服器的連線	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；使用OpenAPI。 您可以在管理伺服器屬性視窗中變更預設埠號（在"**一般**"區域的"**連線連接埠**"子區域）或建立管理伺服器階層結構時。
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 Linux 期間配置連線連接埠時，或將用戶端裝置手動連線至管理伺服器時，您可以變更預設埠號。 此連接埠可選，預設關閉。出於安全原因，我們建議使用 13000 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。
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。
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	受管理裝置的啟動代理伺服器。 您可以在管理伺服器屬性視窗中變更預設埠號（在"**一般**"區域的"**附加連接埠**"子區域中）。
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。
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。 您可以在管理伺服器內容視窗（**一般** → **連線連接埠** → **RDP 連線通道**）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
4444	kliam	HTTPS	使用 OpenID Connect 協定進行身分驗證	在瀏覽器和身分和存取管理器 (IAM)之間交換身分驗證權杖。
9050	kliam	HTTPS	使用 IAM 連線到管理伺服器	在卡巴斯基安全管理中心網頁主控台和 IAM 之間交換身分驗證權杖。

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 MariaDB）。請參閱 DBMS 文件以取得相關資訊。

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。 您可以在安裝卡巴斯基安全管理中心 網頁主控台時變更預設連接埠號。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。 您可以在網路代理政策設定中變更預設埠號。
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。 您可以在發佈點屬性視窗中變更預設埠號。
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。

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 Linux 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)	從網路代理和連線閘道接收連線	管理用戶端裝置、傳送更新和安裝套件。 您可以在發佈點屬性中變更預設埠號。
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。 您可以在發佈點屬性中變更預設埠號。
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。 您可以在發佈點屬性中變更預設埠號。
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。 您可以在發佈點屬性中變更預設埠號。
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。 您可以在發佈點屬性中變更預設埠號。
8060	klcsweb	TCP	傳輸發佈的安裝套件到用戶端裝置	發佈安裝套件。 您可以在管理伺服器內容視窗的**網頁伺服器**區段中變更預設連接埠號。
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。 您可以在管理伺服器內容視窗的**網頁伺服器**區段中變更預設連接埠號。

下表顯示了網域控制器裝置上使用的連接埠。

網域控制器裝置上使用的連接埠

埠號	協定	連接埠目的	範圍
389	透過 TCP 或 UDP 的 LDAP	連線到 LDAP 伺服器	網域控制器輪詢
636	透過 TLS 的 LDAP	連線到 LDAP 伺服器	網域控制器輪詢

下表包含在未安裝網路代理的用戶端裝置上必須開啟的連接埠。

未指派客戶端裝置上使用的連接埠

埠號	協定	連接埠目的	範圍
22	SSH	透過 SSH 連線至用戶端裝置	遠端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 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

埠號	服務名稱	協定	連接埠目的	範圍
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 處理程序
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
4222	卡巴斯基安全管理中心網頁主控台 NATS	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基於 NATS 的訊息代理 API 連接埠。 8222 連接埠用於監控 NATS。	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
4444	身分識別與存取管理器 (IAM)	HTTPS	OpenID Connect 驗證協定使用的連接埠。	卡巴斯基安全管理中心網頁主控台與身分和存取管理器 (IAM)之間的身分驗證權杖交換
9050	IAM	HTTPS	IAM 使用的連接埠。	卡巴斯基安全管理中心網頁主控台和 IAM 之間的互動

基本概念

本章節解釋關於卡巴斯基安全管理中心 Linux 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 `kladminserver_srv`
- 設定隨作業系統啟動而自動啟動
- 具有 `ksc` 帳戶或在安裝管理伺服器過程中所選取的使用者帳戶

有關安裝設定的完整列表，請參閱以下文章：安裝卡巴斯基安全管理中心 Linux。

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。

您可以使用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。

在階層結構中，基於 Linux 的管理伺服器既可以作為主伺服器也可以作為從屬伺服器。基於 Linux 的主伺服器可以管理基於 Linux 和基於 Windows 的從屬伺服器。基於 Windows 的主伺服器可以管理基於 Linux 的次要伺服器。

*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 Linux 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 Linux 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。

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。

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://<Web Server name>:<HTTPS port>/public/<object>
```

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。

卡巴斯基安全管理中心 Linux 網頁伺服器

卡巴斯基安全管理中心 Linux 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 Linux 的一個元件。網頁伺服器用於發佈獨立安裝套件以及共用資料夾的檔案。

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。

網頁伺服器設定

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。

連接閘道上的 Web 伺服器設定

單獨的 Web 伺服器服務以連線閘道模式在發佈點上實施，允許使用連線到卡巴斯基安全管理中心 Linux 的行動裝置。該服務負責將應用程式安裝套件和裝置管理設定檔傳輸到裝置而無需將其直接連線到管理伺服器。檔案在服務處理在連線閘道上的 HTTP/HTTPS 檔案請求時進行傳輸。

連線閘道上的 Web 伺服器服務與網路代理 Linux 一起安裝。若要使用此功能，您必須指派在連線閘道模式下充當發佈點的裝置用作 Web 伺服器，然後指定相應的設定。有關在連線閘道上配置 Web 伺服器設定的詳細資訊，請參閱Kaspersky Secure Mobility Management 說明。

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 Linux 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 Linux 來管理 Kaspersky 應用程式的裝置上。

安裝了網路代理的裝置被稱為*受管理裝置*或*裝置*。您可以從以下來源下載網路代理安裝套件：

- 管理伺服器儲存（您必須安裝了管理伺服器）
- Kaspersky 網路

Linux 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“卡巴斯基網路代理”
- 設定隨作業系統啟動而自動啟動
- 使用根帳戶

Windows 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“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

macOS 的網路代理作為服務安裝在裝置上，且具有以下屬性：

- 名稱“com.kaspersky.klnagent.core”
- 設定隨作業系統啟動而自動啟動
- 使用根帳戶

服務處理程序的名稱：

- 對於 Linux：
  - klnagent64.service（對於 64 位元作業系統）
  - klnagent.service（對於 32 位元作業系統）
- 對於 Windows：
  - klnagent
- 對於 macOS：
  - com.kaspersky.klnagent

預設情況下，網路代理安裝在以下位置：

- 對於 Linux：
  - 32位元系統：/opt/kaspersky/klnagent/
  - 64 位元系統：/opt/kaspersky/klnagent64/
- 對於 Windows：
  - 32 位元系統：C:\Program Files\Kaspersky Lab\NetworkAgent
  - 64 位元系統：C:\Program Files (x86)\Kaspersky Lab\NetworkAgent
- 對於 macOS：
  - 64位元系統：/Library/Application Support/Kaspersky Lab/klnagent/Binaries/klnagent

對於 Windows 裝置，您可以在安裝套件的設定中為網路代理的安裝指定不同的資料夾。但是對於 Linux 裝置，網路代理只能安裝在預設目錄中。

網路代理安裝資料夾還包含用於管理和診斷網路代理操作的公用程式，例如 klmover 和 klnagchk 公用程式。

安裝管理伺服器時，網路代理的伺服器版本會與管理伺服器一起自動安裝。儘管如此，若要像管理任何其他受管理裝置一樣管理管理伺服器裝置，請安裝 Network Agent for Linux在管理伺服器裝置上。在這種情況下，Linux 網路代理已安裝，並獨立於您與管理伺服器一起安裝的網路代理伺服器版本。

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 Linux 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*是執行 Linux、Windows 或 macOS 並安裝了網路代理的裝置。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。

您可以讓受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。一台管理伺服器能夠管理的裝置數量取決於託管管理伺服器的裝置的配置和 DBMS 限制。

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"**未指派的裝置**"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

安裝了卡巴斯基安全管理中心 網頁主控台伺服器的裝置稱作*管理員工作站*。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。

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 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。

您可以從卡巴斯基網站下載管理 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*是一組應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：

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。
- 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 Linux 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 Linux 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

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使用卡巴斯基安全管理中心 網頁主控台修改，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 Syslog 事件記錄和卡巴斯基安全管理中心 Linux 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）或 DNS 名稱作為該裝置的位址。您還可以選擇由管理伺服器偵測到的聯網裝置。

- 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（先前叫做更新代理）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。

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：

- 透過將從管理伺服器接收到的更新和安裝套件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）。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。

  發佈點加速更新發佈並釋放管理伺服器資源。

- 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。

- 執行卡巴斯基和其他軟體供應商的應用程式遠端安裝，包括在沒有網路代理的用戶端裝置上安裝。

  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 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。

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 Linux 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。應用程式先前版本分配的 IP 多點傳送位址將不被變更。

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 Linux 建立嚴重等級為*警告*的安全問題。安全問題將被發佈在裝置內容中，在**安全問題**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。

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：

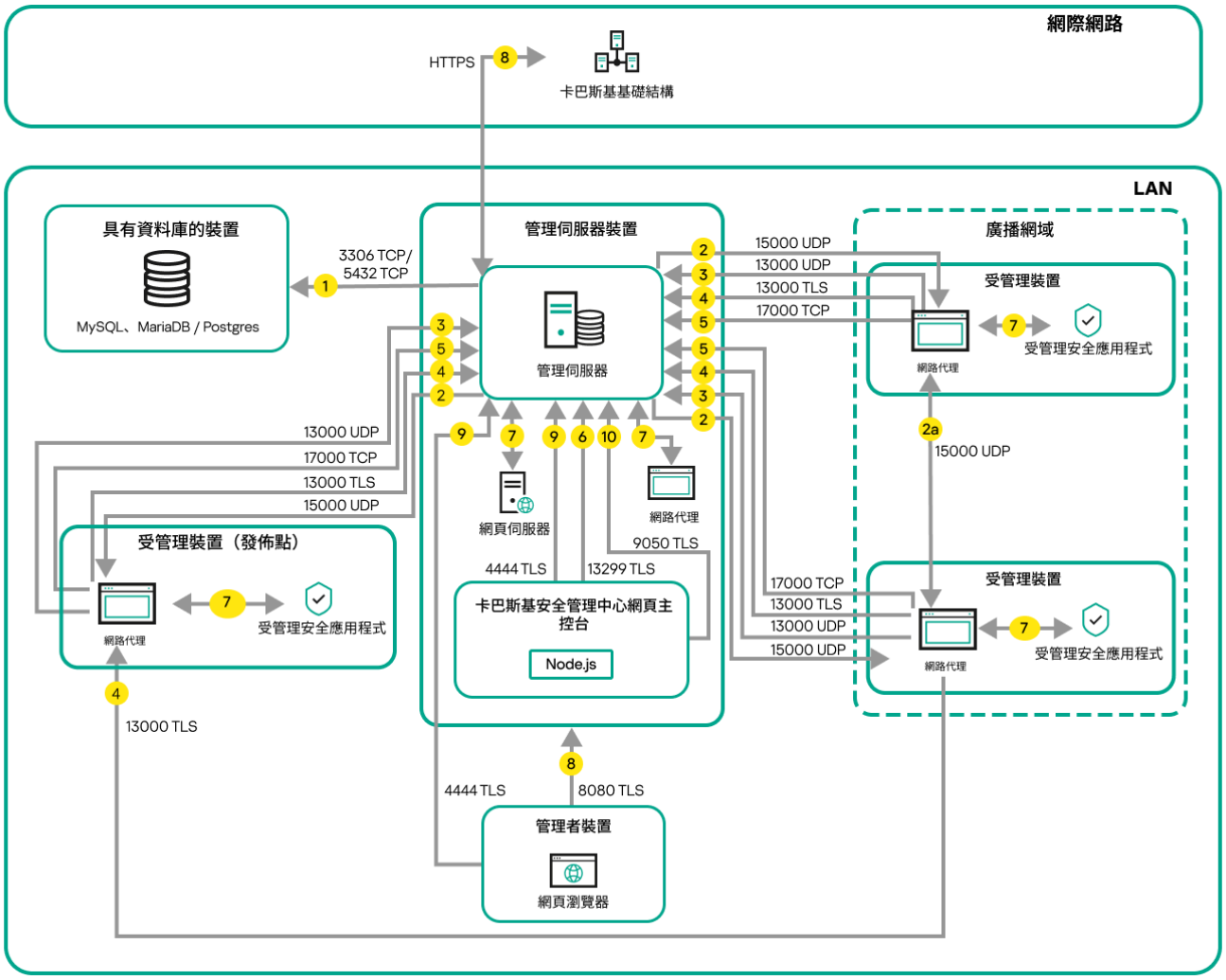
- 虛擬管理伺服器缺少多數全域設定和自己的 TCP 連接埠。
- 虛擬管理伺服器沒有從屬管理伺服器。
- 虛擬管理伺服器沒有其他虛擬管理伺服器。
- 實體管理伺服器可以檢視它所有虛擬管理伺服器的裝置、群組、事件和受管理裝置上的物件（隔離區項目、應用程式登錄資料等等）。
- 虛擬管理伺服器僅可以掃描連線了發佈點的網路。

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 Linux 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 和 MariaDB 伺服器，或連接埠 5432 用於 PostgreSQL Server 或 Postgres Pro 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。

   2a.非移動受管理裝置上的網路代理交換有關同一廣播網域內其他網路代理的資料（資料然後被傳送到管理伺服器）。

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。

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. 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。

   身分和存取管理器 (IAM) 元件經由 TLS 連接埠 13299 連線到管理伺服器。

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。

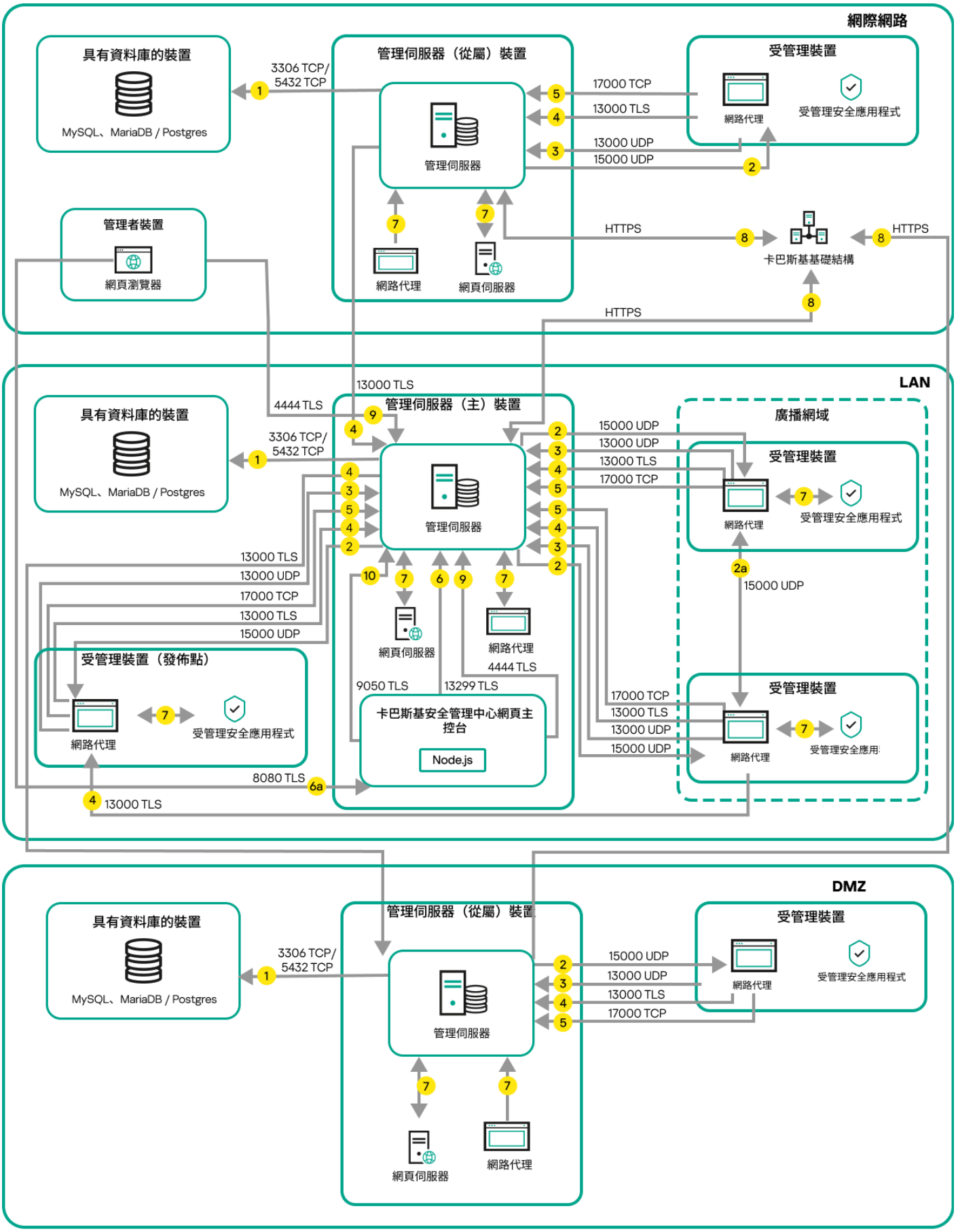
   如果您不想讓您的管理伺服器擁有網際網路連線，您必須手動管理該資料。

9. 卡巴斯基安全管理中心網頁主控台伺服器和瀏覽器（與卡巴斯基安全管理中心網頁主控台搭配使用）透過 OpenID Connect 身分驗證通訊協定，經由 TLS 連接埠 4444 連線到管理伺服器。

10. 卡巴斯基安全管理中心網頁主控台伺服器經由 TLS 連接埠 9050 連線到管理伺服器。

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 和 MariaDB 伺服器，或連接埠 5432 用於 PostgreSQL Server 或 Postgres Pro 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 Linux 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。

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. 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。

   身分和存取管理器 (IAM) 元件經由 TLS 連接埠 13299 連線到管理伺服器。

   6a.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。

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。

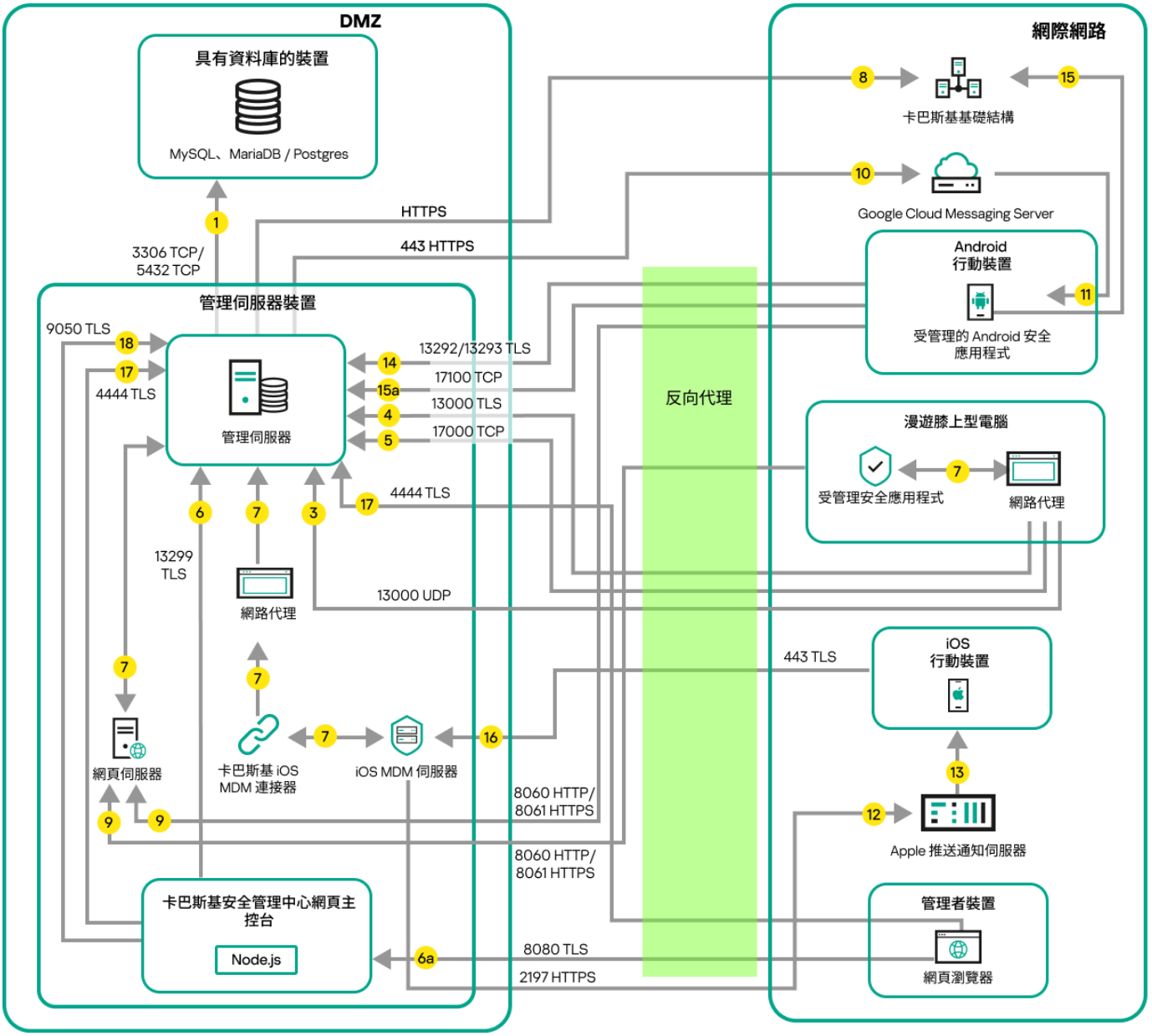
   如果您不想讓您的管理伺服器擁有網際網路連線，您必須手動管理該資料。

9. 卡巴斯基安全管理中心網頁主控台伺服器和瀏覽器（與卡巴斯基安全管理中心網頁主控台搭配使用）透過 OpenID Connect 身分驗證通訊協定，經由 TLS 連接埠 4444 連線到管理伺服器。

10. 卡巴斯基安全管理中心網頁主控台伺服器經由 TLS 連接埠 9050 連線到管理伺服器。

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

下圖顯示管理伺服器處於區域網路 (LAN) 中且受管理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 和 MariaDB 伺服器，或連接埠 5432 用於 PostgreSQL Server 或 Postgres Pro 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 Linux 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。

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. 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。

   身分和存取管理器 (IAM) 元件經由 TLS 連接埠 13299 連線到管理伺服器。

   6a.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。

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. 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。

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 iOS MDM Server。

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. 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。

17. 卡巴斯基安全管理中心網頁主控台伺服器和瀏覽器（與卡巴斯基安全管理中心網頁主控台搭配使用）透過 OpenID Connect 身分驗證通訊協定，經由 TLS 連接埠 4444 連線到管理伺服器。

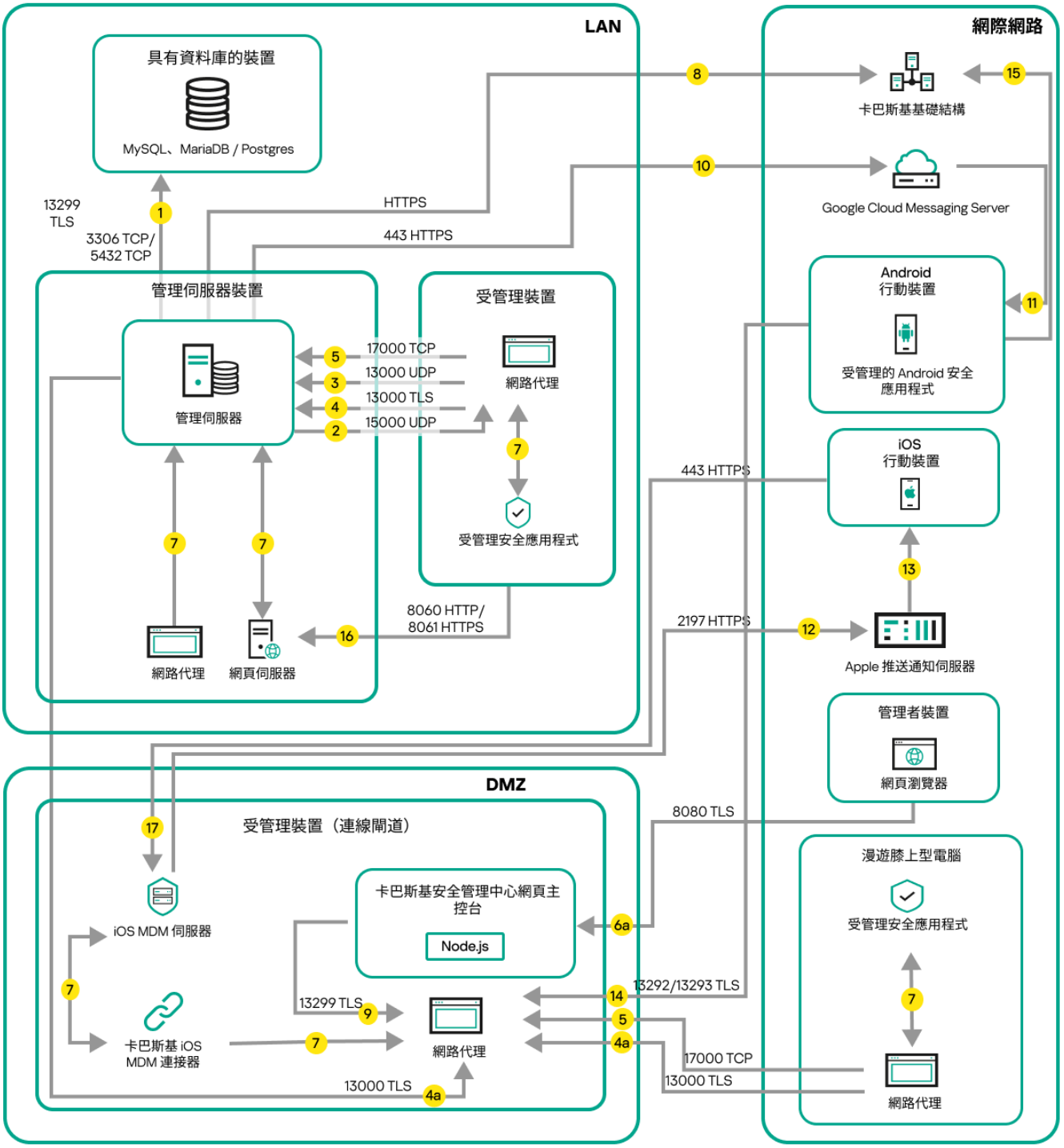
18. 卡巴斯基安全管理中心網頁主控台伺服器經由 TLS 連接埠 9050 連線到管理伺服器。

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 (LAN) 中且受管理裝置都在網際網路中時的資料流量。連線閘道使用中。

如果您不想讓受管理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。

> 對於此部署方案，身分和存取管理器 (IAM)提供的網域身分驗證（單一登入）不受支援。



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 和 MariaDB 伺服器，或連接埠 5432 用於 PostgreSQL Server 或 Postgres Pro 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 Linux 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。

   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. 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。

   6a.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。

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. 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。

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 iOS MDM Server。

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。

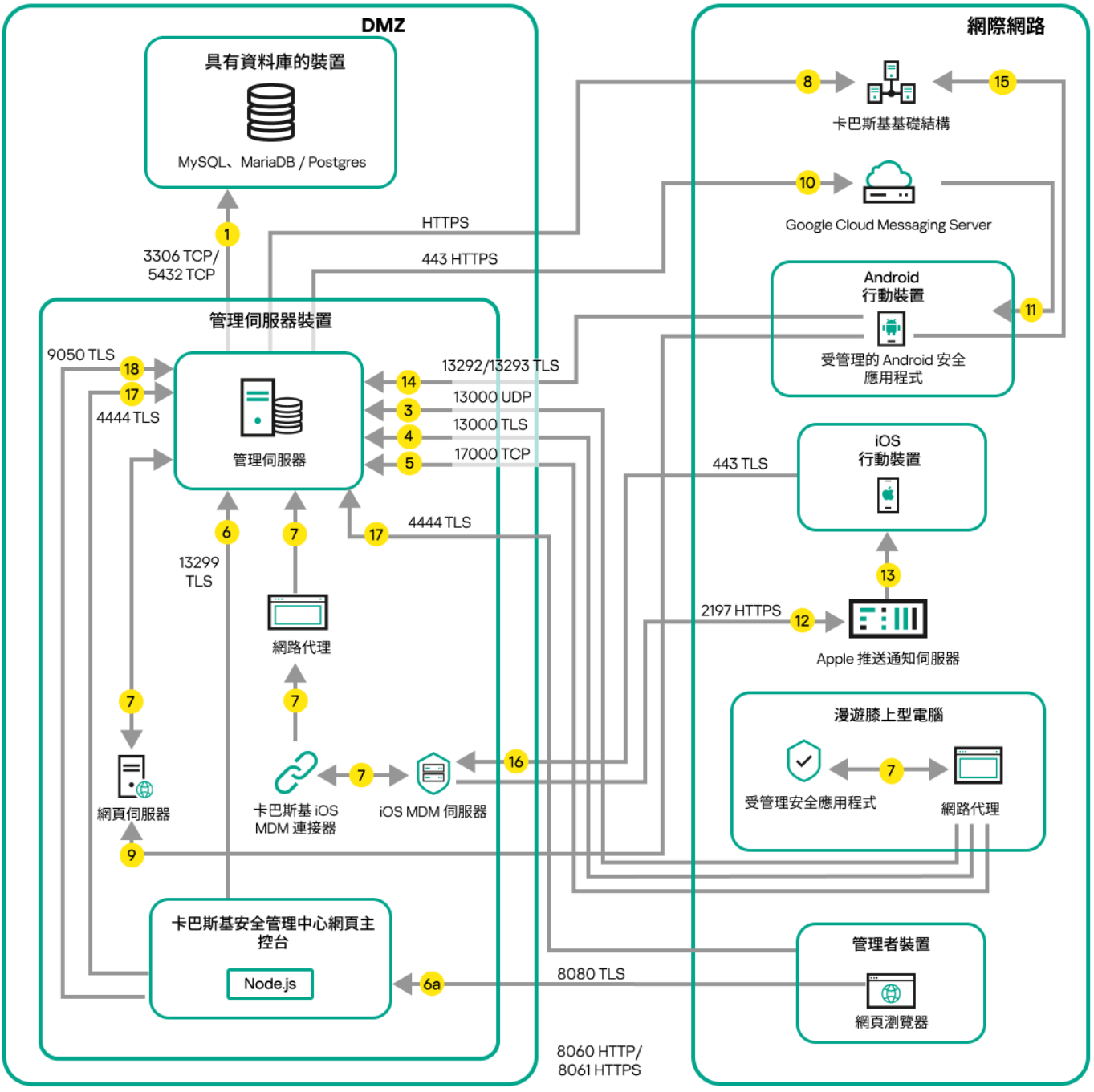
15. 僅對行動裝置：來自行動裝置的資料被傳輸到 Kaspersky 基礎架構。

> 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. 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隔離區 (DMZ) 中且受管理裝置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 和 MariaDB 伺服器，或連接埠 5432 用於 PostgreSQL Server 或 Postgres Pro 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 Linux 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。

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. 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。

   身分和存取管理器 (IAM) 元件經由 TLS 連接埠 13299 連線到管理伺服器。

   6a.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。

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. 來自受管理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。

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。FCM 服務也在 443 HTTPS 連接埠上執行。

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 iOS MDM Server。

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. 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。

17. 卡巴斯基安全管理中心網頁主控台伺服器和瀏覽器（與卡巴斯基安全管理中心網頁主控台搭配使用）透過 OpenID Connect 身分驗證通訊協定，經由 TLS 連接埠 4444 連線到管理伺服器。

18. 卡巴斯基安全管理中心網頁主控台伺服器經由 TLS 連接埠 9050 連線到管理伺服器。

與卡巴斯基安全管理中心 Linux 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 Linux 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。

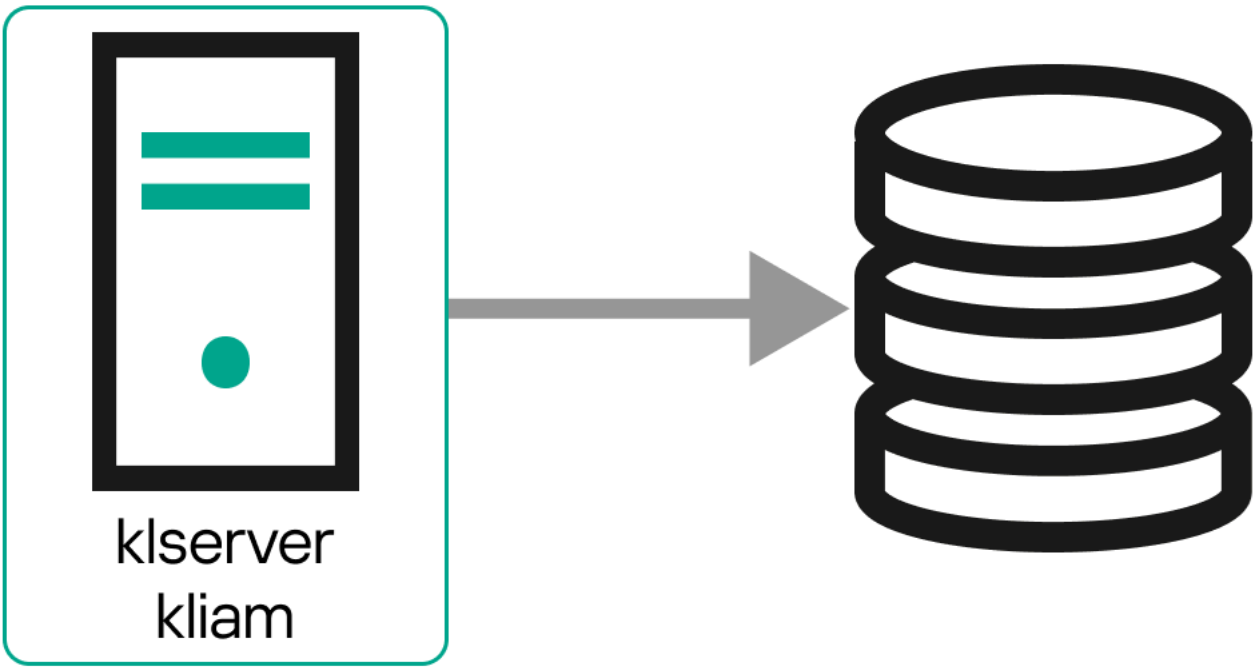
文件說明

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 Linux 可以管理的其他應用程式）
	連線閘道
	發佈點

	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）
	DBMS 傳輸
	DMZ 邊界

管理伺服器和 DBMS

管理伺服器和身分和存取管理器（IAM）的資料分別儲存在同一個DBMS中的不同資料庫中。



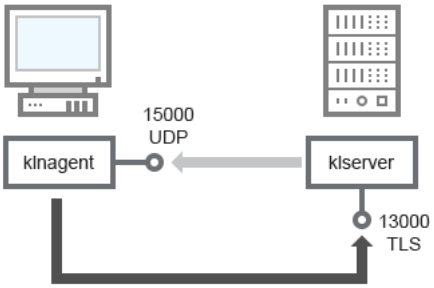
管理伺服器、身分和存取管理器以及 DBMS

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 MariaDB）。請參閱 DBMS 文件以取得相關資訊。
連接 IAM 至 DBMS 的連接埠由使用者在卡巴斯基安全管理中心 Linux 安裝期間指定。

當解除安裝伺服器或者將伺服器移動到另一部裝置時，管理伺服器不會自動刪除管理伺服器資料庫和 IAM 資料庫。如有必要，您必須手動移除這些資料庫。

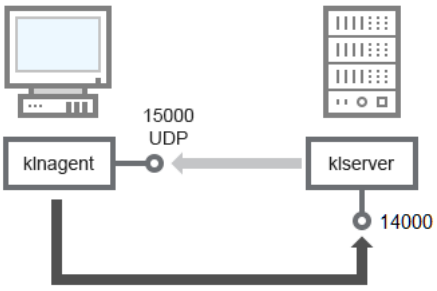
管理伺服器和用戶端裝置：管理安全應用程式

管理伺服器透過 TLS 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 Linux 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 Linux 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）

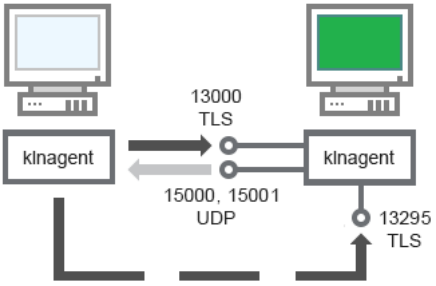
為了澄清方案，參見下圖。

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	連接埠目的
網路代理	15000	klnagent	UDP	網路代理多點傳送
管理伺服器	13000	klserver	TCP (TLS)	接收從網路代理的連線
管理伺服器	14000	klserver	TCP	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。

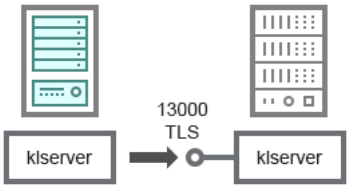
透過發佈點升級軟體（流量）

裝置	埠號	開啟連接埠的處理程序名稱	協定	連接埠目的
網路代理	15000	klnagent	UDP	網路代理多點傳送
網路代理	15001	klnagent	UDP	從發佈點接收更新和安裝套件
發佈點	13000	klnagent	TCP (TLS)	接收從網路代理的連線
發佈點	13295	klnagent	TCP (TLS)	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。

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卡巴斯基安全管理中心網頁主控台管理兩個管理伺服器。因此，主管理伺服器連接埠 13299 的可存取性是僅有的前提。



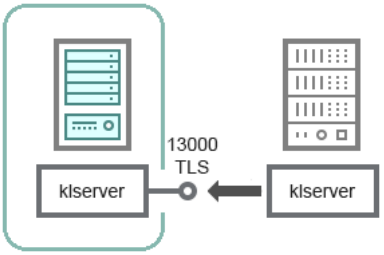
管理伺服器階層：主管理伺服器和從屬管理伺服器

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	連接埠目的
主管理伺服器	13000	klserver	TCP (TLS)	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

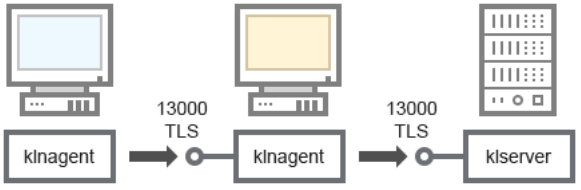
方案顯示了管理伺服器階層，其中 DMZ 中的從屬管理伺服器從主管理伺服器接收連線（請參閱下表）。當組合兩個管理伺服器到一個層級，確保連接埠 13299 在兩個管理伺服器上都可以存取。卡巴斯基安全管理中心網頁主控台透過連接埠 13299 連線到管理伺服器。

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卡巴斯基安全管理中心網頁主控台管理兩個管理伺服器。因此，主管理伺服器連接埠 13299 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	連接埠目的
從屬管理伺服器	13000	klserver	TCP (TLS)	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



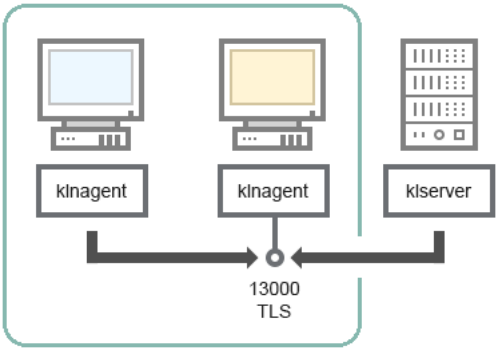
管理伺服器、網段連線閘道和用戶端裝置

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	連接埠目的
管理伺服器	13000	klserver	TCP (TLS)	接收從網路代理的連線
網路代理	13000	klnagent	TCP (TLS)	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



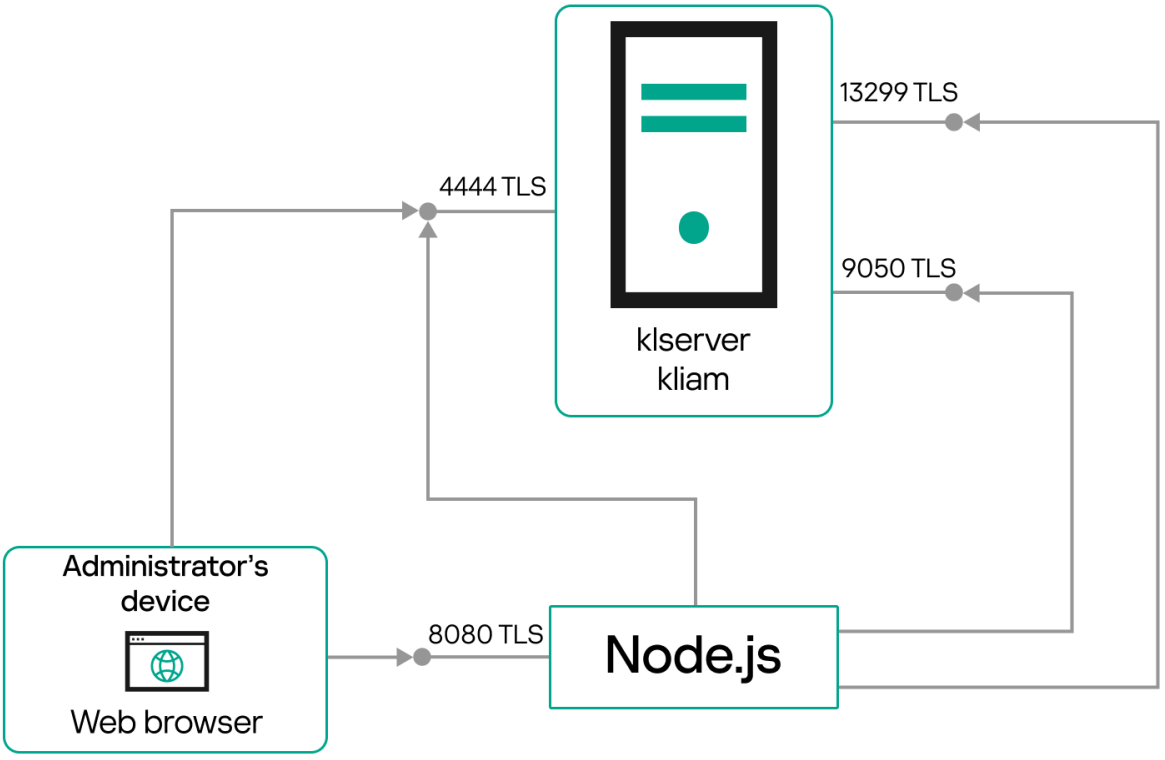
帶有連線閘道的管理伺服器和 DMZ 中的用戶端裝置

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	連接埠目的
網路代理	13000	klnagent	TCP (TLS)	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。

裝置	埠號	開啟連接埠的處理程序名稱	協定	連接埠目的
管理伺服器	13299	klserver	TCP (TLS)	透過 OpenAPI 接收從卡巴斯基安全管理中心網頁主控台和身分和存取管理器 (IAM)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 (TLS)	從卡巴斯基安全管理中心網頁主控台接收連線
管理伺服器	4444	kliam	TCP (TLS)	透過 OpenID Connect 驗證協定接收從卡巴斯基安全管理中心網頁主控台伺服器和瀏覽器（與卡巴斯基安全管理中心網頁主控台一起使用）到帶有 IAM 的管理伺服器的連線
管理伺服器	9050	kliam	TCP (TLS)	接收從卡巴斯基安全管理中心網頁主控台到 IAM 的連線

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。

正在啟動

透過遵循此情境，您可以安裝 卡巴斯基安全管理中心 Linux 管理伺服器和卡巴斯基安全管理中心網頁主控台，您可透過執行快速啟動精靈執行管理伺服器初始設定，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。

先決條件

您必須擁有 Kaspersky Endpoint Security for Business 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）。

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

階段

主要安裝情境分階段進行：

1. **選取組織防護結構**

   找到更多 卡巴斯基安全管理中心 Linux 元件。基於網路配置和通信管道的輸送量，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）。

   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。

2. **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。

3. **安裝資料庫管理系統 (DBMS)**

   安裝 卡巴斯基安全管理中心 Linux 將使用的 DBMS，或者使用現有資料庫。

   您可以選擇其中一個受支援的 DBMS。對於如何安裝所選 DBMS 的資訊，請參考其文件。

   如果 Linux 作業系統的發行版不包含支援的 DBMS，您可以從協力廠商套件儲存庫安裝 DBMS。如果禁止從協力廠商儲存庫安裝發行版，您可以將 DBMS 安裝在單獨的裝置上。

   > 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。

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

   > 如果您想在安裝後變更DBMS 類型，則必須重新安裝 卡巴斯基安全管理中心 Linux。您可以匯出工作和政策，以便在重新安裝後匯入。請參閱以下文章：匯出工作、匯出政策。

4 **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。

5 **安裝卡巴斯基安全管理中心 Linux**

選擇您打算用作管理伺服器的 Linux 裝置，確保該裝置符合軟體和硬體要求，然後安裝 卡巴斯基安全管理中心 Linux在裝置上。網路代理的伺服器版本會連同管理伺服器自動一起安裝。

6 **安裝卡巴斯基安全管理中心 網頁主控台和管理外掛程式**

選擇您打算用作管理員工作站的 Linux 裝置，確保該裝置符合軟體和硬體要求，然後在裝置上安裝卡巴斯基安全管理中心 網頁主控台。您可以在安裝管理伺服器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。

下載 Kaspersky Endpoint Security for Linux 管理 Web 外掛程式，然後將其安裝在安裝卡巴斯基安全管理中心 網頁主控台的同一台裝置上。

7 **在管理伺服器裝置上安裝 Kaspersky Endpoint Security for Linux 和網路代理**

預設情況下，應用程式不會將管理伺服器裝置視為受管理裝置。為防護管理伺服器免受病毒和其他威脅，並將裝置作為任何其他受管理裝置進行管理，我們建議您在管理伺服器裝置上安裝 Kaspersky Endpoint Security for Linux 和 Linux 網路代理。在這種情況下，Linux 網路代理已安裝，並獨立於您與管理伺服器一起安裝的網路代理伺服器版本。

8 **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。

9 **網路裝置探索**

手動發現裝置。卡巴斯基安全管理中心 Linux 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 Linux 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 Linux 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。

10 **整理裝置到管理群組**

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。

11 **分配發佈點**

發佈點被自動分配到管理群組，但您也可以在必要時手動分配它們。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到裝置（或裝置群組）。

12 **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。

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）。

13. **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。

14. **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。

15. **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。

硬化指南

卡巴斯基安全管理中心 Linux 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 Linux 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 Linux 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 Linux 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 Linux 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

強化檢查清單

管理伺服器佈署

- 將管理伺服器安裝在專用的實體伺服器或虛擬伺服器上。
- 請勿將專用伺服器用於執行其他服務。
- 請勿將管理伺服器（以下簡稱「伺服器」）安裝在以下位置：
  - 網域控制器
  - 終端伺服器
  - 使用者裝置

連線安全

- 設定防火牆，以限制存取伺服器裝置的所有連接埠和通訊協定（伺服器所需的連接埠除外）。僅允許受信任裝置存取伺服器裝置。
- 為用於將卡巴斯基安全管理中心網頁主控台（也稱為「網頁主控台」）連線到伺服器的伺服器連接埠設定 IP 位址允許清單。
- 設定防火牆，以僅允許受信任裝置透過網頁主控台存取伺服器。
- 在伺服器上設定 TLS 通訊協定版本 1.2 或更高版本。
- 設定防火牆，以限制存取安裝有伺服器 DBMS 的裝置。
- 在伺服器與 DBMS（MySQL 或 PostgreSQL）之間設定 SSL 身分驗證。

帳戶與授權

- 為伺服器存取配置雙因素驗證（TOTP、RFC 6238）。
- 請勿將身份驗證器應用程式安裝在用以透過網頁主控台連線到伺服器的同一裝置上。
- 建議使用權杖、智慧卡或其他方法，透過多因素身分驗證 (MFA) 存取伺服器裝置。
- 為伺服器裝置建立專用的管理群組，並為其建立特殊的安全政策。
- 限制擁有主管理員角色的使用者數量。

- 基於使用者和群組角色設定伺服器功能存取權限。
- 僅允許單獨的使用者帳戶遠端安裝應用程式。
- 建議定期稽核管理伺服器裝置上的所有使用者。

對管理伺服器防護的管理

- 在伺服器裝置上安裝安全應用程式：
  - 對於實體伺服器，安裝 Kaspersky Endpoint Security
  - 對於虛擬伺服器，安裝 Kaspersky Security for Virtualization
- 建立並套用單獨的伺服器防護政策（有別於其他受管理裝置的安全政策）。
- 在安全應用程式中啟用所有可用的防護模組。

為受管理應用程式設定政策和工作

- 為下列應用程式建立政策並將其套用至所有受管理裝置或包含新受管理裝置的群組：
  - 網路代理
  - Kaspersky Endpoint Security for Windows/Linux/macOS
  - Kaspersky Endpoint Agent（或其他卡巴斯基應用程式）。
- 啟用密碼防護，防止防護停用或解除安裝卡巴斯基應用程式。
- 鎖定政策設定（關閉「鎖定」），以防止在受管理裝置上重新指派這些設定。
- 建立排程工作，對所有裝置執行完整掃描。
- 啟用卡巴斯基安全網路 (KSN) 並接受最新的 KSN 聲明。
- 設定裝置發現並為新發現的裝置指定預設管理群組。
- 限制使用自動規則在管理群組之間移動裝置。
- 為發佈點提供防護，以免遭未經授權的存取。
- 避免在小型網路或高重要性網路中自動指派發佈點。

管理伺服器維護

- 請勿刪除或停用以下工作：
  - 備份
  - 管理伺服器維護
- 定期安裝作業系統和協力廠商軟體更新。

事件傳輸到協力廠商系統

- 設定安全事件的監控和報告。
- 設定將事件匯出到 SIEM 系統。
- 設定伺服器通知，以處理：
  - 稽核事件
  - 緊急事件
  - 失效事件和警告

第三方資訊系統安全建議

- 將 CIS 基準安全建議套用至所使用的作業系統、DBMS 和 hypervisor。
- 對於 Astra Linux，請遵循對應版本紅皮書中所述的安全建議。
- 對於 RED OS，請遵循 RED OS 官方文件中所述的建議。

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 Linux 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 Linux 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。

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。

用於安裝和執行管理伺服器的帳戶

在部署管理伺服器期間，需要建立兩個非特權帳戶。管理伺服器中包含的服務將在這些非特權帳戶下運作。為帳戶授予權利和權限時，請遵循最小權限原則。避免在「kladmins」群組中包含不必要的帳戶。

您還需要建立一個內部 DBMS 帳戶。管理伺服器使用此內部 DBMS 帳戶來存取選定的 DBMS。

所需帳戶及其權限集合取決於所選的 DBMS 類型和管理伺服器資料庫建立方法。

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，在發佈管理伺服器版本時，依預設，系統將設定加密協定以確保安全的資料傳輸。

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。

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，Kaspersky Security Center Linux 使用者可以從安裝卡巴斯基安全管理中心網頁主控台或者 OpenAPI 應用程式的任何裝置登入卡巴斯基安全管理中心 Linux。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 Linux，他或她將無法登入卡巴斯基安全管理中心 Linux。

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 Linux 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。在具有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

為了輪詢網域控制器，管理伺服器或 Linux 發佈點嘗試透過 LDAPS 連線到該網域。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` 標誌設定為 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 Linux 管理伺服器備份副本並將其儲存在安全位置。

為管理伺服器使用雙因素驗證

當登入卡巴斯基安全管理中心網頁主控台時，**卡巴斯基安全管理中心 Linux 使用基於 RFC 6238 標準（TOTP：基於時間的一次性密碼演算法）的雙因素驗證**。

每次登入卡巴斯基卡巴斯基安全管理中心網頁主控台時，您都需要輸入使用者名稱、密碼和一次性安全代碼。若要接收一次性安全碼，您必須在電腦或行動裝置上安裝身分驗證器應用程式。

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

為了確保使用雙因素驗證進行全面防護，不僅需要防護管理伺服器，還需要防護在其上安裝管理伺服器的裝置。

當連線到安裝了管理伺服器的裝置時（透過 SSH、RDP 或其他協定），我們建議使用多因素身分驗證 (MFA)，例如使用權杖、智慧卡或其他身分驗證方法。

限制儲存管理員密碼

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 Linux 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。

配置變更內部使用者帳戶密碼的選項

我們建議配置以下選項來變更內部使用者帳戶的密碼：

- 密碼輪替期
- 需要變更密碼的初步警告的時間
- **使用者必須在首次登入後更改密碼**選項的值

帳戶防護以防止未經授權的修改

我們建議啟用附加選項來防護管理伺服器的內部使用者帳戶免遭未經授權的修改。必須為每個內部使用者單獨配置此防護。

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。

限制主管理員角色的分配

由 kladduser 實用程式建立的使用者在管理伺服器或者虛擬管理伺服器的存取控制清單 (ACL) 中被指派為主管理員角色。我們建議避免將主管理員角色分配給大量使用者。

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 Linux 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。

角色型存取控制模型的主要優點：

- 易於管理
- 角色層次結構
- 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。

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。
- 推薦的安全產品。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產品相容性的建議（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13299 接收來自卡巴斯基安全管理中心網頁主控台的連線。我們建議限制可以使用該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至安裝套件，則所有對此資料夾具有讀取權限的使用者都可以存取該產品授權金鑰（直接或透過管理伺服器中嵌入的Web 伺服器）。

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。

卡巴斯基安全管理中心 Linux 使用者裝置的安全要求

卡巴斯基安全管理中心 Linux 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 Linux 使用者裝置包括以下內容：

- 卡巴斯基安全管理中心 Linux 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。
- 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 Linux 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 Linux，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 Linux 元件（網路代理、Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Security for Linux、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

我們強烈建議啟用密碼防護，以防止入侵者停用或解除安裝卡巴斯基安全應用程式。在支援密碼防護的平台上，您可以為 Kaspersky Endpoint Security、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"來鎖定相應的設定。

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。klmover 公用程式位於網路代理安裝資料夾中。

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。

> 如果您遺失或忘記了安裝在不再受 卡巴斯基安全管理中心 Linux 管理的裝置上的受密碼防護的網路代理密碼，則無法使用 klmover 實用程式或命令列移除網路代理。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。

在 Windows 裝置上啟用**使用解除安裝密碼**選項也會啟用 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：設定與網域控制器的整合，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。

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：

- 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。

事件傳輸到第三方系統

監控和報告

為了及時回應安全問題，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安全問題，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 Linux 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。

第三方資訊系統安全建議

CIS 基準的安全建議

當使用管理伺服器與網路代理支援的作業系統、虛擬化平台或資料庫伺服器版本時，我們建議應用網際網路安全中心 (CIS) 的最佳資訊安全實務（如果有）來微調這些資訊系統。

網際網路安全中心 (CIS) 是一個致力於提高資訊科技領域安全性的非營利組織。特別是，網際網路安全中心 (CIS) 開發和發佈如 CIS 控制和 CIS 基準等安全標準。這些標準是一組確保資訊系統安全的建議和實務。

網際網路安全中心 (CIS) 入口網站包含針對建議：

- 以下系列的作業系統：
  - 桌面版 Windows
  - 伺服器版 Windows
  - Debian
  - Ubuntu
  - CentOS
  - Oracle Linux
  - Red Hat Enterprise Linux
  - SUSE Linux Enterprise Server
  - macOS
- VMware 虛擬化平台
- 資料庫伺服器：
  - Microsoft SQL Server
  - MySQL
  - MariaDB
  - PostgreSQL

Astra Linux 作業系統的安全建議

使用 Astra Linux 作業系統時，您應該遵循 Astra Linux 對應版本紅皮書中所述的安全建議。

RED OS 作業系統的安全建議

使用 RED OS 作業系統時，您應該使用官方 RED OS 文件中所述的管理員指南中的安全建議。

使用卡巴斯基安全應用程式的建議

在 Kaspersky Endpoint Security for Windows 中使用 KLAdmin 密碼

KLAdmin 帳戶是管理員帳戶，可以不受限制地存取 Kaspersky Endpoint Security for Windows。KLAdmin 帳戶有權在 Kaspersky Endpoint Security for Windows 中執行任何受密碼防護的操作，包括刪除應用程式。KLAdmin 帳戶的權限無法撤銷。您可以在Kaspersky Endpoint Security for Windows 政策的屬性中設定 KLAdmin 帳戶的密碼。Kaspersky Endpoint Security for Windows 管理員對 KLAdmin 帳戶密碼的安全使用負全部責任。如果您的組織有自己的密碼政策，請遵循該政策的指示。密碼越長、越複雜，就越可靠。

我們對於防護組織免於 KLAdmin 密碼被盜的建議如下：

- **一般要求**

  請勿使用帳戶名稱或部分名稱作為密碼。

- **最小密碼長度要求**

  建立長度至少為 10 個字元的密碼。

- **使用多種字元類型的要求**

  設定包含不同類別字元的複雜密碼：小寫和大寫字母、數字和特殊字元。

- **密碼到期要求**

  將密碼的最短有效期限設定為 90 天。新密碼不得與最近 24 個密碼中的任何一個比對。

情境：驗證 MySQL 伺服器

我們建議您使用 TLS 憑證對 MySQL 伺服器進行身分驗證。您可使用來自信任的憑證授權單位 (CA) 或自簽發憑證。

管理伺服器支援 MySQL 的單向和雙向 SSL 身分驗證。

啟用單向 SSL 身分驗證

請按照以下步驟為 MySQL 配置單向 SSL 身分驗證：

1. **為 MySQL 伺服器產生自簽章 TLS 憑證**

   執行以下指令：

   ```
   openssl genrsa 1024 > ca-key.pem
   ```

   ```
   openssl req -new -x509 -nodes -days 365 -key ca-key.pem -config myssl.cnf > ca-cert.pem
   ```

   ```
   openssl req -newkey rsa:1024 -days 365 -nodes -keyout server-key.pem -config myssl.cnf
   > server-req.pem
   ```

```
openssl x09 -req -in server-req.pem -days 365 -CA ca-cert.pem -CAkey ca-key.pem -
set_serial 01 > server-cert.pem
```

2. **建立伺服器旗標檔案**

   使用 klscflag 公用程式建立 KLSRV_MYSQL_OPT_SSL_CA 伺服器標誌，並將憑證路徑指定為其值。klscflag 公用程式位於安裝管理伺服器的目錄中。預設安裝路徑為/opt/kaspersky/ksc64/sbin。

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <ca-cert.pem 的路徑> -t d
   ```

3. **設定資料庫**

   在 my.cnf 檔案中指定憑證。在文字編輯器中開啟 my.cnf 檔案並將以下行新增至 [mysqld] 部分中：

   ```
   [mysqld]
   ssl-ca=".../mysqlcerts/ca-cert.pem"
   ssl-cert=".../mysqlcerts/server-cert.pem"
   ssl-key=".../mysqlcerts/server-key.pem"
   ```

啟用雙向 SSL 身分驗證

請按照以下步驟為 MySQL 配置雙向 SSL 身分驗證：

1. **建立伺服器旗標檔案**

   使用 klscflag 公用程式建立伺服器標誌並將憑證檔案路徑指定為其值：

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <ca-cert.pem> -t s 的路徑
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CERT -v <server-cert.pem> -t s 的路徑
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_KEY -v <server-key.pem> -t s 的路徑
   ```

   klscflag 公用程式位於安裝管理伺服器的目錄中。預設安裝路徑為/opt/kaspersky/ksc64/sbin。

2. **指定密碼短語（可選）**

   如果 server-key.pem 需要複雜密碼，請建立 KLSRV_MARIADB_OPT_TLS_PASPHRASE 標誌並將複雜密碼指定為其值：

   ```
   klscflag -fset -pv klserver -n KLSRV_MARIADB_OPT_TLS_PASPHRASE -v <複雜密碼> -t s
   ```

3. **設定資料庫**

   在 my.cnf 檔案中指定憑證。在文字編輯器中開啟 my.cnf 檔案並將以下行新增至 [mysqld] 部分中：

   ```
   [mysqld]
   ssl-ca=".../mysqlcerts/ca-cert.pem"
   ssl-cert=".../mysqlcerts/server-cert.pem"
   ssl-key=".../mysqlcerts/server-key.pem"
   ```

情境：驗證 PostgreSQL 伺服器

我們建議您使用 TLS 憑證對 PostgreSQL 伺服器進行身分驗證。您可使用來自信任的憑證授權單位 (CA) 或自簽發憑證。

管理伺服器支援 PostgreSQL 的單向和雙向 SSL 身分驗證。

PostgreSQL 伺服器的身分驗證分為幾個階段進行：

1. **為 PostgreSQL 伺服器產生憑證**

   執行以下指令：

   ```
   openssl req -new -x509 -days 365 -nodes -text -out psql.crt -keyout psql.key -subj "/CN=psql"
   ```

   ```
   chmod og-rwx psql.key
   ```

2. **為管理伺服器產生憑證**

   執行以下指令。CN 值應與代表管理伺服器連線到 PostgreSQL 的使用者名稱相符。預設情況下，使用者名稱被設定為 postgres。

   ```
   openssl req -new -x509 -days 365 -nodes -text -out postgres.crt -keyout postgres.key -subj "/CN=postgres"
   ```

   ```
   chmod og-rwx postgres.key
   ```

3. **設定用戶端憑證身分驗證**

   修改 pg_hba.conf 如下：

   ```
   hostssl mydb myuser 192.168.1.0/16 scram-sha-256
   ```

   確保 pg_hba.conf 不包含以`host`開頭的記錄。

4. **指定 PostgreSQL 憑證**

   單向 SSL 身分驗證

   修改 postgresql.conf 如下（指定 .crt 和 .key 檔案的正確路徑）：

   ```
   listen_addresses ='localhost, server-ip'
   ssl = on
   ssl_cert_file = '<psql.crt>'
   ssl_key_file = '<psql.key>'
   ```

   雙向 SSL 身分驗證

   修改 postgresql.conf 如下（指定 .crt 和 .key 檔案的正確路徑）：

   ```
   listen_addresses ='localhost, server-ip'
   ssl = on
   ssl_ca_file = '<postgres.crt>'
   ssl_cert_file = '<psql.crt>'
   ssl_key_file = '<psql.key>'
   ```

5. **重新啟動 PostgreSQL 精靈進程**

   執行以下指令：

   ```
   systemctl restart postgresql-14.service
   ```

6. **指定管理伺服器的伺服器旗標**

   單向 SSL 身分驗證

   使用 klscflag 公用程式建立 KLSRV_POSTGRES_OPT_SSL_CA 伺服器標誌，並將憑證路徑指定為其值。

   執行命令行，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目錄中。預設安裝路徑為/opt/kaspersky/ksc64/sbin。

   執行以下指令：

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <psql.crt 的路徑> -t s
   ```

   雙向 SSL 身分驗證

   使用 klscflag 公用程式建立伺服器標誌並將憑證檔案路徑指定為其值。

   執行命令行，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目錄中。預設安裝路徑為/opt/kaspersky/ksc64/sbin。

   執行以下指令：

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <psql.crt 的路徑> -t s
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CERT -v <postgres.crt 的路徑> -t s
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_KEY -v <postgres.key 的路徑> -t s
   ```

   如果 `postgres.key` 需要複雜密碼，請建立 KLSRV_POSTGRES_OPT_TLS_PASSPHRASE 標誌並將複雜密碼指定為其值：

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_TLS_PASPHRASE -v <複雜密碼> -t s
   ```

7. **重新啟動管理伺服器服務**

佈署準備

本節介紹如何根據組織的需求選擇卡巴斯基安全管理中心 Linux 部署、卡巴斯基安全管理中心 Linux 設定和 DBMS 的選項。

在組織的網路上部署卡巴斯基安全管理中心 Linux 元件有多種選擇，具體取決於以下標準：

- 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

一台管理伺服器最多可支援 50,000 個裝置（使用 PostgreSQL 或 Postgres Pro 作為 DBMS）。如果組織網路中的裝置總數超過 50,000，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”一文。

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”一文。

“卡巴斯基安全管理中心 Linux 標準配置”部分提供了卡巴斯基安全管理中心 Linux 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

選擇卡巴斯基安全管理中心 Linux 的設定

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 Linux 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。

一台管理伺服器最多可支援 50,000 個裝置（使用 PostgreSQL 或 Postgres Pro 作為 DBMS）。請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。

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，請參閱以下文章：啟用推送伺服器。

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。

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：

- 透過卡巴斯基安全管理中心網頁主控台部署防護系統。

  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。

- 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不支援使用 Microsoft Active Directory® 群組政策進行部署。

選取 DBMS

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
MySQL（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。
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。
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，請使用此 DBMS。
Tantor（檢視受支援的版本）	如果您打算為少於 50,000 台裝置執行單個管理伺服器，請使用此 DBMS。 Tantor DBMS 僅支援在 Astra Linux Special Edition RUSB.10015-01（操作更新 1.8）上執行。

對於如何安裝所選 DBMS 的資訊，請參考其文件。

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式的通知。

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。

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

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週期。

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。

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，可以透過連接埠轉發方式從外部存取。

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，則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。

請注意，卡巴斯基安全管理中心 Linux 不支援使用 Microsoft Windows 群組政策進行部署。

您可以使用位於組織網路上的發佈點。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）。

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 Linux 網頁主控台的安裝。

設定 MariaDB x64 伺服器以與 卡巴斯基安全管理中心 Linux 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。

My.cnf 檔案的建議設定

如需更多 DBMS 設定詳情，另請參閱帳戶設定程序。如需 DBMS 安裝資訊，請參閱 DBMS 安裝程序。

要設定 my.cnf 檔案：

1. 在文字編輯器中開啟 my.cnf 檔案。

2. 將以下行輸入到 my.cnf 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 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` 參數已設定為 `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
```

預設會啟用最佳化程式附加元件 `join_cache_incremental`、`join_cache_hashed`、`join_cache_bka`。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. 確保其輸出包含以下幾行：

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

   如果這幾行存在且其值為 on，則會啟用最佳化程式附加元件。

   如果這幾行不存在或其值為 `off`，您需要執行以下操作：

   a. 在文字編輯器中開啟 my.cnf 檔案。

   b. 在 my.cnf 中新增以下幾行：

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

附加元件 `join_cache_incremental`、`join_cache_hash` 和 `join_cache_bka` 已啟用。

增加 MariaDB systemd 服務可以開啟的檔案（檔案描述符）的預設限制，以確保在負載下穩定運作。

若要增加檔案描述符的限制：

1. 執行以下命令：

   ```
   sudo systemctl edit mariadb.service
   ```

2. 在 `[Service]` 區段的 `LimitNOFILE` 參數中指定檔案描述符的限制：

   ```
   LimitNOFILE=1048576
   ```

3. 執行以下命令以確保參數指定正確：

   ```
   sudo systemd-analyze verify mariadb.service
   ```

4. 執行以下命令重新載入系統處理程序：

   ```
   sudo systemctl daemon-reload
   ```

5. 執行以下命令重新啟動 MariaDB 服務：

   ```
   sudo systemctl restart mariadb.service
   ```

   檔案描述符的限制已增加。

設定 PostgreSQL 或 Postgres Pro 伺服器與 卡巴斯基安全管理中心 Linux 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 Linux 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 Linux 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 Linux 一起運作。

設定檔的預設路徑為：`/etc/postgresql/< VERSION >/main/postgresql.conf`

在 Linux ALT 作業系統上，預設路徑為 `/var/lib/pgsql/data/postgresql.conf`

PostgreSQL 和 Postgres Pro 的建議參數：

- `max_connections = 151`

  如果您使用叢集 Postgres DBMS，請在所有 DBMS 伺服器以及叢集組態中指定 `max_connections` 參數。

- `shared_buffers` = N

  N = 資料庫管理伺服器 (DBMS) 預計 RAM 大小的 25%。如果 DBMS 與管理伺服器安裝在同一裝置上，則計算應基於分配給 DBMS 的 RAM，而不是裝置的總 RAM。

  如果 RAM 小於 1 GB，則保留預設值。

- `temp_buffers = 24MB`

- `work_mem = 16MB`

- `maintenance_work_mem = 128MB`

- `max_stack_depth` = 最大堆疊大小（執行 '`ulimit -s`' 命令以取得此值，單位為 KB）減去 1 MB 安全餘量

- `max_parallel_workers_per_gather = 0`

- `standard_conforming_strings` = on

如果您使用 Postgres Pro 15.7 或 Postgres Pro 15.7.1，請停用 `enable_compound_index_stats` 參數：

`enable_compound_index_stats = off`

更新組態檔後，重新載入配置或重新啟動DBMS伺服器。

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

有關如何為 PostgreSQL 和 Postgres Pro 建立和設定帳戶的詳細資訊，請參閱以下文章：設定帳戶以與 PostgreSQL 和 Postgres Pro 搭配使用。

有關如何配置高可用性 DBMS 叢集的詳細資訊，請參閱以下文章：為卡巴斯基安全管理中心 Linux 準備高可用性 DBMS 叢集。

設定 MySQL x64 伺服器以與 卡巴斯基安全管理中心 Linux 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 Server 用於卡巴斯基安全管理中心，請啟用儲存 InnoDB 和 MEMORY 以及 UTF-8 和 UCS-2 編碼的支援。

My.cnf 檔案的建議設定

如需更多 DBMS 設定詳情，另請參閱帳戶設定程序。如需 DBMS 安裝資訊，請參閱 DBMS 安裝程序。

要設定 my.cnf 檔案：

1. 在文字編輯器中開啟 my.cnf 檔案。

2. 將以下行新增到 my.cnf 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=< 實際值必須不少於預期 KAV 資料庫大小的 80% >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0 (在大多數情況下，伺服器使用小型交易)
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` 值中指定的記憶體會在伺服器啟動時分配。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` 參數已設定為 `1`。

準備一個高可用性 DBMS 叢集，以與卡巴斯基安全管理中心 Linux 搭配使用

Kaspersky Security Center for Linux支援以下高可用性叢集：

- Platform V Pangolin
- Postgres Pro內建高可用性
- Patroni（可選配HAProxy負載平衡器）。

複製類型必須設定為同步。

如果您使用的是 PostgreSQL 的 Patroni 範本 3.3.1 或更早版本，請確保`synchronous_standby_names`參數已正確套用。若要檢查是否使用了同步複製，請在主要節點上執行下列查詢：

```
SELECT application_name, client_addr, client_hostname, client_port, sync_state
FROM pg_stat_replication;
```

如果任何節點的`sync_state`列顯示的值不是`sync`或者`potential`，則叢集使用了異步複製，而異步複製不受支援。若要解決此問題，請執行下列任一操作：

- 將 Patroni 更新至 3.3.2 或更新版本。
- 在 Patroni 設定檔中，找到`bootstrap`部分的`dcs`子部分並將`synchronous_mode`參數設定為`true`：

  `bootstrap:`

  `dcs:`

  `<...>`

  `synchronous_mode: true`

建議的最低高可用性DBMS叢集組態必須包含至少三個節點。

要準備高可用性 DBMS 叢集以與卡巴斯基安全管理中心 Linux 配合使用，請執行以下操作：

1. 設定 PostgreSQL 或 Postgres Pro 伺服器與 卡巴斯基安全管理中心 Linux 搭配使用。
2. 如要管理伺服器自動發現叢集節點的位址，以便您只需在安裝期間指定主節點或副本節點的DNS名稱或IP位址，請執行下列步驟：

   a. 透過在`postgresql`部分中新增以下行，修改所有高可用性DBMS叢集節點上的組態檔/etc/pangolin-manager/postgres.yml（若使用Platform V Pangolin）或/etc/postgresql/<VERSION>/main/postgresql.conf（若使用Postgres Pro內建高可用性叢集）：

   `log_hostname=1`

   對於其他設定檔參數，您可以使用PostgreSQL 和 Postgres Pro 的建議參數值。

   b. 編輯組態檔後，在所有高可用性DBMS叢集節點上重新啟動DBMS叢集服務。

   c. 確保資料庫使用者擁有`pg_read_all_stats`權限。您可以透過執行以下命令授予此權限：

   `GRANT pg_read_all_stats TO "%1";`

其中`%1`是資料庫使用者的名稱。

使用者名稱在管理伺服器安裝程式期間在`KLSRV_UNATT_DBMS_LOGIN`參數中指定。

d. 為IAM資料庫設定負載平衡器。請參閱您所選負載平衡器的說明文件。

至此，高可用性 DBMS 叢集已準備就緒，可與卡巴斯基安全管理中心 Linux 搭配使用。

安裝卡巴斯基安全管理中心 Linux

該過程描述了如何安裝 卡巴斯基安全管理中心 Linux。

安裝之前，您必須執行以下操作：

- 為卡巴斯基安全管理中心 Linux 安裝 DBMS。您可以選擇一個受支援的 DBMS。對於如何安裝所選 DBMS 的資訊，請參考其文件。

  如果 Linux 作業系統的發行版不包含支援的 DBMS，您可以從協力廠商套件儲存庫安裝 DBMS。

  安裝 DBMS 後，請依照對應的說明進行操作：

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

    設定 DBMS 帳戶以搭配使用 PostgreSQL 和 Postgres Pro

    如果您希望管理伺服器自動發現叢集節點的位址，因此您只需要在安裝過程中指定主節點或副本節點的DNS名稱或IP地址，請確保您已執行以下文章中說明的第2步：準備高可用性DBMS叢集以使用Kaspersky Security Center for Linux。

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

    設定 DBMS 帳戶以搭配使用 MySQL 和 MariaDB

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

    設定 DBMS 帳戶以搭配使用 MySQL 和 MariaDB

- 確保您要安裝卡巴斯基安全管理中心 Linux 網頁主控台的裝置執行支援的 Linux 版本。

  如果您使用作業系統 RED OS 7.3.4 或更高版本或者 MSVSPHERE 9.2 或更高版本，請安裝 libxcrypt-compat 套件以便管理伺服器正確運作。

- 確保 DNS 伺服器在網路上可用。

- 從卡巴斯基網站下載安裝檔案。選擇與您裝置上安裝的 Linux 發行版相對應的安裝檔案 — ksc64_<version_number>_amd64.deb or ksc64-<version_number>.x86_64.rpm。

若要安裝卡巴斯基安全管理中心 Linux，您必須在具有 root 權限的帳戶下執行下列說明中提供的命令。

要安裝 卡巴斯基安全管理中心 Linux ：

1. 建立一個群組「kladmins」以及兩個非授權帳戶「ksc」和「ksciam」。該帳戶必須是「kladmins」群組成員。為此，請依次執行以下命令：

   ```
   adduser ksc
   ```

`groupadd kladmins`

`gpasswd -a ksc kladmins`

`usermod -g kladmins ksc`

`adduser ksciam`

`gpasswd -a ksciam kladmins`

`usermod -g kladmins ksciam`

2. 在 DBMS 伺服器上，為 IAM 建立一個資料庫。資料庫名稱必須不同於為卡巴斯基安全管理中心 Linux 安裝的資料庫。當解除安裝或將伺服器移至其他裝置時，管理伺服器不會自動刪除 IAM 資料庫，您必須手動刪除資料庫。

   - 對於 PostgreSQL，執行以下命令：

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - 對於 MariaDB，執行以下命令：

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

3. 如果您使用高可用性 DBMS 叢集，請執行以下步驟：

   a. 授予「ksc」使用者 `pg_read_all_stats` 權限：

   ```
   GRANT pg_read_all_stats TO "ksc";
   ```

   b. 在所有高可用性 DBMS 叢集節點上，修改設定檔 /etc/pangolin-manager/postgres.yml（如果使用 Platform V Pangolin）或 /etc/postgresql/main/postgresql.conf（如果使用 Postgres Pro 內建高可用性叢集）。如果在將叢集連線到Kaspersky Security Center for Linux 時僅指定主節點或副本節點的DNS名稱或IP位址，請將下列行新增至 `postgresql` 部分：

   ```
   log_hostname: '1'
   ```

   c. 編輯設定檔 /etc/pangolin-manager/postgres.yml 後，請在所有高可用性 DBMS 叢集節點（除仲裁節點外）上重新啟動 DBMS 叢集服務，操作如下：

   ```
   systemctl restart pangolin-manager.service
   ```

   或

   ```
   systemctl restart postgresql-<version>
   ```

4. 如有必要，增加用於管理伺服器服務功能的帳戶可以開啟的檔案（檔案描述符）的預設限制。為此，請開啟 /etc/security/limits.conf 檔案，然後指定檔案描述符的軟限制和硬限制，如下所示：

```
ksc  soft  nofile  <max_number_of_opened_files>
ksc  hard  nofile  <max_number_of_opened_files>
```

預設情況下，檔案描述符的限制在安裝期間指定。軟檔案限制為 32,768 個檔案，硬檔案限制為 131,072 個檔案。

5. 執行卡巴斯基安全管理中心 Linux 安裝。根據您的 Linux 版本，執行以下命令之一：

```
sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb
sudo yum install /<path>/ksc64-<version_number>.x86_64.rpm
```

6. 執行 卡巴斯基安全管理中心 Linux 配置：

```
/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

7. 閱讀 最終使用者產品授權協議 (EULA) 和隱私政策。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，當出現提示時，輸入以下值：

   a. 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）。若要使用卡巴斯基安全管理中心 Linux ，您必須接受 EULA 的條款。

   b. 輸入 y，如果您理解並接受隱私政策的條款，並且您同意您的資料將按照隱私政策中的說明進行處理和傳輸（包括傳輸到第三國）。輸入 n（如果您不接受隱私政策的條款）。要使用卡巴斯基安全管理中心 Linux ，您必須接受隱私政策的條款。

8. 出現提示時，輸入以下設定：

   a. 選擇 **標準**作為管理伺服器安裝模式。

   b. 輸入管理伺服器 DNS 名稱或靜態 IP 位址。其他裝置將使用該位址連線到管理伺服器。

   c. 輸入管理伺服器 SSL 連接埠號。預設情況下使用連接埠 13000。

   d. 評估您打算管理的裝置的大致數量：

      - 如果您有 1 到 100 個受管理裝置，請輸入 1。
      - 如果您有 101 到 1000 個受管理裝置，請輸入 2。
      - 如果您有超過 1000 台受管理裝置，請輸入 3。

      此設定用於自動隨機延遲工作啟動以最佳化網路負載。下面的清單顯示了計算延遲的間隔：

      - 1 至 100 個受管理裝置，值 1。不使用延遲。
      - 101 至 1000 個受管理裝置，值 2。延遲 5 分鐘。
      - 超過 1000 個受管理裝置，價值 3。延遲 10 分鐘。

   e. 輸入服務的安全群組名稱。預設情況下，使用 `kladmins` 群組。

f. 輸入帳戶名稱以啟動管理伺服器服務。該帳戶必須是輸入的安全群組的成員。預設情況下，使用“`ksc`”帳戶。

g. 輸入帳號名稱以啟動其他服務。該帳戶必須是輸入的安全群組的成員。預設情況下，使用“`ksc`”帳戶。

h. 選擇您安裝的與 卡巴斯基安全管理中心 Linux 一起使用的 DBMS：

- 如果您安裝了 MySQL 或 MariaDB，請輸入 1。
- 如果您安裝了 PostgreSQL 或 Postgres Pro，請輸入 2。

i. 輸入安裝管理伺服器DBMS的裝置的DNS名稱或IP地址。本機DBMS安裝的預設為127.0.0.1。

若要使用高可用性故障轉移叢集，請執行下列其中一項操作：

- 以以下格式輸入所有節點的DNS名稱或IP位址和連接埠：

```
<fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>;
```

- 僅指定主節點或副本節點的DNS名稱或IP位址。

j. 輸入資料庫連接埠號。此連接埠用於與管理伺服器通信。如果您在步驟8.h中輸入了所有高可用性群集節點的DNS名稱或IP位址和連接埠，則跳過此步驟。

預設情況下，使用以下連接埠：

- 連接埠 `3306` 用於 MySQL 或 MariaDB
- 連接埠 `[[5432` 用於 PostgreSQL 或 Postgres Pro

k. 輸入資料庫名稱。

l. 輸入用於存取資料庫的資料庫管理員帳戶的登入名稱。

m. 輸入用於存取資料庫的資料庫管理員帳戶的密碼。

n. 如果您安裝了 PostgreSQL 或 Postgres Pro，可以指定管理伺服器要使用的資料庫結構描述。若要這麼做，請指定結構描述名稱。

> 結構描述名稱區分大小寫：您只能使用小寫字母。

如果您不想使用自訂結構描述，請按 ENTER 鍵，系統將使用預設結構描述。

o. 輸入 IAM 伺服器 FQDN。如果您未指定此變數，則使用安裝了管理伺服器的電腦的DNS名稱。

您必須指定您在步驟8a中輸入的管理伺服器DNS名稱。

p. 輸入帳戶名稱以啟動 IAM 服務。該帳戶必須是輸入的安全群組的成員。預設情況下，使用“ksciam”帳戶。

q. 選取為與 IAM 服務搭配使用而安裝的 DBMS：

- 如果您安裝了 MySQL 或 MariaDB，請輸入 1。
- 如果您安裝了 PostgreSQL 或 Postgres Pro，請輸入 2。

r. 輸入IAM 服務要使用的 IAM DBMS 位址。

若要使用高可用性群集，請執行以下其中一項操作：

- 以以下格式輸入所有節點的DNS名稱或IP位址和連接埠：

```
<fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>;
```

- 僅指定負載平衡器的DNS名稱或IP位址。

s. 輸入 IAM DBMS 連接埠號。此連接埠用於與 IAM 服務通訊。如果您在步驟8.p中輸入了所有高可用性群集節點的DNS名稱或IP位址和連接埠，則會跳過此步驟。

預設情況下，使用以下連接埠：

- 連接埠 3306 用於 MySQL 或 MariaDB
- 連接埠 5432 用於 PostgreSQL 或 Postgres Pro

t. 輸入IAM 服務要使用的 IAM 資料庫名稱。IAM 服務所使用的資料庫名稱應與管理伺服器所使用的資料庫名稱不同。

u. 輸入您用於存取 IAM 資料庫的資料庫帳戶的登入名稱。

v. 輸入您用於存取 IAM 資料庫的資料庫帳戶的密碼。

等待服務自動新增並啟動：

- `klnagent_srv`
- `kladminserver_srv`
- `klactprx_srv`
- `klwebsrv_srv`
- `kliam_srv`

w. 如果您安裝了 PostgreSQL 或 Postgres Pro，可以指定 IAM 要使用的資料庫結構描述。若要這麼做，請指定結構描述名稱。

如果您不想使用自訂結構描述，請按 ENTER 鍵，系統將使用 public 結構描述。

> 結構描述名稱區分大小寫：您只能使用小寫字母。
> 請勿指定保留的 iam 結構描述名稱：client、iam、ksc、locker、pat、scope、voltron。

x. 建立一個充當管理伺服器管理員的帳戶。輸入使用者名稱和密碼。

密碼必須符合以下規則：

- 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 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

如果跳過此步驟，您可以稍後使用下列命令建立新使用者：

```
/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <password>
```

使用者已新增，卡巴斯基安全管理中心 Linux 已安裝。

網路代理安裝

若要像管理任何其他受管理裝置一樣管理管理伺服器裝置，請安裝 Network Agent for Linux 在管理伺服器裝置上。在這種情況下，Linux 網路代理已安裝，並獨立於您與管理伺服器一起安裝的網路代理伺服器版本。

服務驗證

使用以下命令檢查服務是否正在執行：

- `systemctl status klnagent_srv.service`
- `systemctl status kladminserver_srv.service`
- `systemctl status klactprx_srv.service`
- `systemctl status klwebsrv_srv.service`
- `systemctl status kliam_srv.service`

以靜默模式安裝 卡巴斯基安全管理中心 Linux

您可以在 Linux 裝置上安裝卡巴斯基安全管理中心 Linux，方法是使用回應檔案以靜默模式執行安裝，即無需使用者參與。回應檔案包含一組自訂安裝參數：變數及其各自的值。

安裝前：

- 為卡巴斯基安全管理中心 Linux 安裝 DBMS。您可以選擇一個受支援的 DBMS。對於如何安裝所選 DBMS 的資訊，請參考其文件。

  如果 Linux 作業系統的發行版不包含支援的 DBMS，您可以從協力廠商套件儲存庫安裝 DBMS。

  安裝 DBMS 後，請依照對應的說明進行操作：

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

    設定 DBMS 帳戶以搭配使用 PostgreSQL 和 Postgres Pro

    如果您希望管理伺服器自動發現叢集節點的位址，因此您只需要在安裝過程中指定主節點或副本節點的DNS名稱或IP地址，請確保您已執行以下文章中說明的第2步：準備高可用性DBMS叢集以使用Kaspersky Security Center for Linux。

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

    設定 DBMS 帳戶以搭配使用 MySQL 和 MariaDB

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

    設定 DBMS 帳戶以搭配使用 MySQL 和 MariaDB

- 確保安裝有 DBMS 的裝置上不存在具有以下名稱的 DBMS 使用者帳戶：

  - client
  - iam
  - ksc
  - locker
  - pat
  - scope
  - voltron

- 確保您要安裝卡巴斯基安全管理中心 Linux 網頁主控台的裝置執行支援的 Linux 版本。

  > 如果您使用作業系統 RED OS 7.3.4 或更高版本或者 MSVSPHERE 9.2 或更高版本，請安裝 libxcrypt-compat 套件以便管理伺服器正確運作。

- 從卡巴斯基網站下載安裝檔案。選擇與您裝置上安裝的 Linux 發行版相對應的安裝檔案 — sc64_[version_number]_amd64.deb 或 ksc64-[version_number].x86_64.rpm。

若要以靜默模式安裝 卡巴斯基安全管理中心 Linux：

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，才遵循以下步驟操作。

2. 建立一個群組「kladmins」和兩個非授權帳戶「ksc」與「ksciam」，這兩個帳戶必須是「kladmins」群組成員。為此，請在具有 root 權限的帳戶下依次執行以下命令：

   ```
   adduser ksc
   ```

`groupadd kladmins`

`gpasswd -a ksc kladmins`

`usermod -g kladmins ksc`

`adduser ksciam`

`gpasswd -a ksciam kladmins`

`usermod -g kladmins ksciam`

3. 在 DBMS 伺服器上，為 IAM 建立一個資料庫。資料庫名稱必須不同於為卡巴斯基安全管理中心 Linux 安裝的資料庫。當解除安裝或將伺服器移至其他裝置時，管理伺服器不會自動刪除 IAM 資料庫，您必須手動刪除資料庫。

   - 對於 PostgreSQL，執行以下命令：

     `sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"`

   - 對於 MariaDB，執行以下命令：

     `sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"`

4. 建立回應檔案（TXT 格式），並以 `VARIABLE_NAME=variable_value` 格式將變數清單新增到回應檔案，每行一個變數。回應檔案應包括下表中列出的變數。

5. 在 root 或使用者環境中設定 `KLAUTOANSWERS` 環境變數的值，使其包含回應檔案的完整名稱（包含路徑），例如使用下列命令：

   `export KLAUTOANSWERS=/tmp/ksc_install/answers.txt`

6. 以靜默模式執行卡巴斯基安全管理中心 Linux 安裝—根據您的 Linux 發行版，執行以下命令之一：

   在根環境中：

   - `apt-get install /<path>/ksc64_[version_number]_amd64.deb -y`

   - `yum install /<path>/ksc64-[version_number].x86_64.rpm -y`

   在使用者環境中：

   - `sudo -E apt-get install /<path>/ksc64_[version_number]_amd64.deb -y`

   - `sudo -E yum install /<path>/ksc64-[version_number].x86_64.rpm -y`

7. 建立使用者以使用卡巴斯基安全管理中心網頁主控台。為此，請在具有 root 權限的帳戶下執行以下命令：

   `/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <密碼>`，其中密碼必須包含至少 8 個字元。

8. 安裝卡巴斯基安全管理中心網頁主控台。

回應檔案的變數會作為以靜默模式安裝卡巴斯基安全管理中心 Linux 的參數使用。

變數名稱	必要	敘述	可能的值
EULA_ACCEPTED	是	確認您瞭解和接受最終使用者產品授權協議的條款。	1
PP_ACCEPTED	是	確認您瞭解並接受隱私權政策的條款。	1
KLSRV_UNATT_SERVERADDRESS	是	管理伺服器 DNS 名稱或靜態 IP 位址。	DNS 名稱或 IP 位址
KLSRV_UNATT_PORT_SRV	否	管理伺服器連接埠號。預設值是 14000。	埠號
KLSRV_UNATT_PORT_SRV_SSL	否	管理伺服器 SSL 連接埠號。預設值是 13000。	埠號

KLSRV_UNATT_PORT_KLOAPI	否	用於使用OpenAPI 的連接埠號。此連接埠也用於接收來自卡巴斯基安全管理中心網頁控制台的連線。可選，預設值為 13299。	埠號
KLSRV_UNATT_PORT_GUI	否	用於使用 klakaut 實用程式的連接埠號。預設值是 13291。klakaut 實用程式及其說明系統位於卡巴斯基安全管理中心 Linux 的安裝資料夾中。 預設情況下此連接埠已關閉。如果您想使用 klakaut 實用程式自動執行卡巴斯基安全管理中心 Linux 操作，請使用 klscflag 實用程式開啟 13291 連接埠。	埠號
KLSRV_UNATT_NETRANGETYPE	否	您打算管理的裝置的大致數量：此設定用於最佳化網路負載。預設值是 1。	1（適用於 1 至 100 台受管理裝置）； 2（適用於 101 至 1000 台受管理裝置）； 3（適用於超過 1000 台受管理裝置）。
KLSRV_UNATT_DBMS_TYPE	是	資料庫管理系統類型：MySQL（MariaDB）或 Postgres。	mysql 或 postgres
KLSRV_UNATT_DBMS_INSTANCE	是	資料庫伺服器 IP 位址。 若要使用 PostgreSQL、Postgres Pro 內建高可用性叢集或者 Platform V Pangolin DBMS 叢集，請依照下列格式輸入所有節點的 DNS 名稱或 IP 位址和連接埠： `<fqdn1>:<port>,<fqdn2>:<port>,<...> <fqdnX>:<port>;` 或者，如果您想使用Platform V Pangolin DBMS叢集，則在指定DBMS位址時可以僅指定主節點或副本節點的DNS名稱或IP位址。	IP位址
KLSRV_UNATT_DBMS_PORT	是	資料庫伺服器連接埠。MySQL (MariaDB) 的預設值為 3306； Postgres 的預設值為 5432。	3306 或 5432
KLSRV_UNATT_DB_NAME	是	資料庫名稱。資料庫名稱必須與 KLSRV_UNATT_DB_IAM_NAME 變數中指定的 IAM 資料庫名稱不同。	kav
KLSRV_UNATT_DBMS_LOGIN	是	有權存取資料庫的使用者名稱。	
KLSRV_UNATT_DBMS_PASSWORD	是	有權存取資料庫的使用者的密碼。	
KLSRV_UNATT_DBMS_SCHEMA	否	自訂 DBMS 結構描述。 如果您未指定自訂結構描述，管理伺服器將使用預設結構描述。 結構描述名稱區分大小寫：您只能使用小寫字母。 只有在使用 PostgreSQL 或 Postgres Pro 作為 DBMS 時，才能指定自訂結構描述。否則，該變數會被忽略。	database_schema
KLSRV_UNATT_IAM_ADDRESS	是	使用者瀏覽器將被OpenIDConnect重定向到此位址。 輸入 IAM 伺服器 FQDN。您必須使用 KLSRV_UNATT_SERVERADDRESS 參數中指定的管理伺服器 DNS 名稱。	FQDN
KLSRV_UNATT_KLIAMUSER	是	啟動 IAM 服務的帳戶名稱。該帳戶必須是 KLSRV_UNATT_KLADMINSGROUP 變數中指定之安全群組的成員。	ksciam
KLSRV_UNATT_DBMS_IAM_TYPE	是	IAM 資料庫管理系統類型：MySQL（MariaDB）或 Postgres。	mysql 或 postgres

KLSRV_UNATT_DBMS_IAM_INSTANCE	是	IAM 資料庫伺服器位址。 若要使用 PostgreSQL、Postgres Pro 內建高可用性叢集或者 Platform V Pangolin DBMS 叢集，請依照下列格式輸入所有節點的 DNS 名稱或 IP 位址和連接埠： `<fqdn1>:<port>,<fqdn2>:<port>,<...> <fqdnX>:<port>;` 或者，如果您想使用Platform V Pangolin DBMS叢集，在指定DBMS位址時，您只能指定主節點或副本節點的DNS名稱或IP位址。	IP位址
KLSRV_UNATT_DBMS_IAM_PORT	是	IAM 資料庫伺服器連接埠。MySQL (MariaDB) 的預設值為 3306； Postgres 的預設值為 5432。	3306 或 5432
KLSRV_UNATT_DBMS_IAM_LOGIN	是	有權存取 IAM 資料庫的使用者的使用者名稱。 如果 IAM 資料庫類型為 MySQL (MariaDB) 並具有以下兩個設定： • `gtid_mode=ON` • `gtid_purged=ON|AUTO` 確保指定的使用者俱有以下 DBMS 權限之一： • `RELOAD` • `FLUSH_TABLES`	
KLSRV_UNATT_DBMS_IAM_PASSWORD	是	有權存取 IAM 資料庫的使用者的密碼。	
KLSRV_UNATT_DBMS_IAM_SCHEMA	否	自訂 DBMS 結構描述。 如果您未指定自訂結構描述，IAM 將使用 public 結構描述。 只有在使用 PostgreSQL 或 Postgres Pro 作為 DBMS 時，才能指定自訂結構描述。否則，該變數會被忽略。 結構描述名稱區分大小寫：您只能使用小寫字母。 請勿指定保留的 iam 結構描述名稱：`client, iam, ksc, locker, pat, scope, voltron`。	`database_schema`
KLSRV_UNATT_DB_IAM_NAME	是	IAM 資料庫名稱。IAM 資料庫的名稱必須與 `KLSRV_UNATT_DB_NAME` 變數中指定的資料庫名稱不同。 指定一個手動建立的空資料庫。	`iamdb`
KLSRV_UNATT_KLADMINSGROUP	是	服務的安全群組名稱。	`kladmins`
KLSRV_UNATT_KLSRVUSER	是	帳戶名稱以啟動管理伺服器服務。該帳戶必須是 `KLSRV_UNATT_KLADMINSGROUP` 變數中指定之安全群組的成員。	`ksc`
KLSRV_UNATT_KLSVCUSER	是	帳號名稱以啟動其他服務。該帳戶必須是 `KLSRV_UNATT_KLADMINSGROUP` 變數中指定之安全群組的成員。	`ksc`
如果要將管理伺服器部署為卡巴斯基安全管理中心 Linux 容錯移轉叢集，回應檔案必須包含以下額外變數：			

KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT	否	故障轉移叢集組態。如果應答檔案中省略了該參數，則使用預設值。
		可能的值：
		`0` — 節點位於單一資料中心的故障轉移叢集（預設值）。
		`2` — 節點位於不同資料中心的異地分散式故障轉移叢集。
			`0`
			或
			`2`

KLFOC_UNATT_NODE	是	節點號碼（1 或 2）。	`1`
			或
			`2`

KLFOC_UNATT_STATE_SHARE_MOUNT_PATH	是	狀態共用掛接點。	

KLFOC_UNATT_DATA_SHARE_MOUNT_PATH	是	資料共用掛接點。	
KLFOC_UNATT_CONN_MODE	是	容錯移轉叢集連線模式。	VirtualAdapter 或 ExternalLoadBalancer
如果 KLFOC_UNATT_CONN_MODE 變數具有 VirtualAdapter 值，則回應檔必須包含以下其他變數：			
KLFOC_UNATT_CONN_MODE_VA_NAME	是	虛擬網路介面卡名稱。	
KLFOC_UNATT_CONN_MODE_VA_IPV4	這些變數之一是必需的	虛擬網路介面卡 IP 位址。	IP 位址
KLFOC_UNATT_CONN_MODE_VA_IPV6		虛擬網路介面卡 IPv6 地址。	IPv6 位址

在封閉軟體環境模式下在 Astra Linux 上安裝 卡巴斯基安全管理中心 Linux

本節介紹如何在 Astra Linux 特別版作業係統上安裝卡巴斯基安全管理中心 Linux。

安裝前：

- 安裝資料庫管理系統。
- 下載kaspersky_astra_pub_key.gpg 應用程式金鑰。
- 從卡巴斯基網站下載 ksc64_[version_number]_amd64.deb 安裝檔案。

在具有 root 權限的帳戶下，以高完整性和零機密性執行本說明中提供的命令。

在 Astra Linux 特別版（操作更新 1.7.2）和 Astra Linux 特別版（操作更新 1.6）作業係統上安裝卡巴斯基安全管理中心 Linux：

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. 將應用程式金鑰放在上一步建立的目錄中：

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

5. 更新系統所有內核的初始 RAM 檔案系統映像：

   ```
   update-initramfs -u -k all
   ```

   重新啟動系統。

6. 建立一個群組「kladmins」以及兩個非授權帳戶「ksc」和「ksciam」。該帳戶必須是「kladmins」群組成員。為此，請依次執行以下命令：

   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   ```

```
# usermod -g kladmins ksc
# adduser ksciam
# gpasswd -a ksciam kladmins
# usermod -g kladmins ksciam
```

7. 執行卡巴斯基安全管理中心 Linux 安裝：

```
# apt install /<path>/ksc64_[ version_number ]_amd64.deb
```

8. 執行 卡巴斯基安全管理中心 Linux 配置：

```
# /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

9. 閱讀 最終使用者產品授權協議 (EULA) 和隱私政策。文字顯示在命令行視窗中。按空格鍵檢視下一個文字段。出現提示時，輸入以下值：

   a. 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）。若要使用卡巴斯基安全管理中心 Linux ，您必須接受 EULA 的條款。

   b. 若您瞭解並接受隱私權政策的條款，並同意您的資料將依照隱私權政策所述進行處理和傳輸（包括傳輸到第三國），請輸入 y。若您不接受隱私權政策的條款，請輸入 n。要使用卡巴斯基安全管理中心 Linux ，您必須接受隱私政策的條款。

10. 出現提示時，輸入以下設定：

   a. 輸入管理伺服器 DNS 名稱或靜態 IP 位址。

   b. 輸入管理伺服器連接埠號。預設情況下使用連接埠 14000。

   c. 輸入管理伺服器 SSL 連接埠號。預設情況下使用連接埠 13000。

   d. 評估您打算管理的裝置的大致數量：

      - 如果您有 1 到 100 個受管理裝置，請輸入 1。
      - 如果您有 101 到 1000 個受管理裝置，請輸入 2。
      - 如果您有超過 1000 台受管理裝置，請輸入 3。

      此設定用於自動隨機延遲工作啟動以最佳化網路負載。下面的清單顯示了計算延遲的間隔：

      - 1 至 100 個受管理裝置，值 1。不使用延遲。
      - 101 至 1000 個受管理裝置，值 2。延遲 5 分鐘。
      - 超過 1000 個受管理裝置，價值 3。延遲 10 分鐘。

   e. 輸入服務的安全群組名稱。預設情況下，使用“kladmins”群組。

   f. 輸入帳戶名稱以啟動管理伺服器服務。該帳戶必須是輸入的安全群組的成員。預設情況下，使用“ksc”帳戶。

   g. 輸入帳號名稱以啟動其他服務。該帳戶必須是輸入的安全群組的成員。預設情況下，使用“ksc”帳戶。

h. 選擇您安裝的與卡巴斯基安全管理中心 Linux 一起使用的 DBMS：

- 如果您安裝了 MySQL 或 MariaDB，請輸入 1。
- 如果您安裝了 PostgreSQL 或 Postgres Pro，請輸入 2。

i. 輸入在其上安裝資料庫的裝置的 IP 位址。

j. 輸入資料庫連接埠號。此連接埠用於與管理伺服器通信。預設情況下，使用以下連接埠：

- 連接埠 3306 用於 MySQL 或 MariaDB。
- 連接埠 5432 用於 PostgreSQL 或 Postgres Pro。

k. 輸入資料庫名稱。

l. 輸入用於存取資料庫的資料庫管理員帳戶的登入名稱。

m. 輸入用於存取資料庫的資料庫管理員帳戶的密碼。

n. 輸入 IAM 伺服器 FQDN 名稱。
   您必須指定您在步驟10a中輸入的管理伺服器DNS名稱。

o. 輸入帳戶名稱以啟動 kliam 服務。該帳戶必須是輸入的安全群組的成員。

p. 選取為與 IAM 服務搭配使用而安裝的 DBMS：

- 如果您安裝了 MySQL 或 MariaDB，請輸入 1。
- 如果您安裝了 PostgreSQL 或 Postgres Pro，請輸入 2。

q. 輸入IAM 服務要使用的 DBMS 位址。

r. 輸入資料庫連接埠號。此連接埠用於與 IAM 服務通訊。預設情況下，使用以下連接埠：

- 連接埠 3306 用於 MySQL 或 MariaDB。
- 連接埠 5432 用於 PostgreSQL 或 Postgres Pro。

s. 輸入IAM 服務要使用的資料庫名稱。IAM 服務所使用的資料庫名稱應與管理伺服器所使用的資料庫名稱不同。

t. 輸入用於存取 IAM 資料庫的資料庫根帳戶的登入名稱。

u. 輸入用於存取 IAM 資料庫的資料庫根帳戶的密碼。
   等待服務自動新增並啟動：

- `klnagent_srv`
- `kladminserver_srv`
- `klactprx_srv`

- klwebsrv_srv
- kliam_srv

v. 建立一個充當管理伺服器管理員的帳戶。輸入使用者名稱和密碼。
密碼必須符合以下規則：

- 使用者密碼必須最少包含 8 個字元，最多包含 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 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

卡巴斯基安全管理中心 Linux 已安裝，使用者已新增。

服務驗證

使用以下命令檢查服務是否正在執行：

- # systemctl status klnagent_srv.service
- # systemctl status kladminserver_srv.service
- # systemctl status klactprx_srv.service
- # systemctl status klwebsrv_srv.service
- # systemctl status kliam_srv.service

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）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 Linux管理伺服器。

> 如果您在封閉軟體環境模式下的 Astra Linux 上安裝卡巴斯基安全管理中心網頁主控台，請按照特定於 Astra Linux 的說明進行操作。

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

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 Linux 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：`/etc/ksc-web-console-setup.json`。

   包含最小參數集合的回應檔案範例

   回應檔案的參數集取決於卡巴斯基安全管理中心網頁主控台所連線的管理伺服器版本：

   - 16 或更高版本的管理伺服器

     以下是登入管理伺服器版本 16 或更高版本所需的採用最小參數集的回應檔案範例：

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

   - 15.4 或更早版本的管理伺服器

     以下是登入管理伺服器版本 15.4 或更早版本所需的採用最小參數集的回應檔案範例：

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

   您可以將卡巴斯基安全管理中心網頁主控台安裝到管理伺服器所在的同一裝置，也可以安裝到不同裝置。如果將卡巴斯基安全管理中心網頁主控台安裝到不同裝置，則其位址（由 `address` 指定）將會與管理伺服器位址（由 `iamHost` 或者 `kscHost` 指定）不同。如果將卡巴斯基安全管理中心網頁主控台安裝到管理伺服器所在的同一裝置，則這些參數的值將相同。

   `iamHost` 值必須與安裝管理伺服器時指定的IAM位址相符。若要取得指定的IAM位址，請在管理伺服器主機上執行下列命令：

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

有關詳細資訊，請參閱文章：卡巴斯基安全管理中心網頁主控台安裝程式參數。

您可以將多個不同版本的管理伺服器新增到受信任伺服器清單。在這種情況下，這些伺服器可以使用不同的身分驗證方法。

我們建議您指定 1024 以上的連接埠號。如果您希望卡巴斯基安全管理中心網頁主控台在 1024 以下的連接埠上工作，安裝後您必須確保您有 setcup 實用程式，然後執行以下命令：

```
sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
```

如果沒有 setcap 實用程式，您可以安裝它。**點擊此連結檢視命令**。

對於 Debian 和 Ubuntu 作業系統，請執行以下命令之一：

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

對於 SUSE Linux Enterprise Server 和 Red Hat Enterprise Linux，請執行以下命令：

- `sudo zypper install libcap-progs`

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 以外的連接埠埠號，因為作業系統使用的連接埠是 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 apt-get install ksc-web-console-<組建編號>.x86_64.deb`
   - 要從 .rpm 檔案安裝卡巴斯基安全管理中心網頁主控台，執行以下指令之一：
     `sudo yum install ksc-web-console-<組建編號>.x86_64.rpm`

     或

     `sudo alien -i 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 yum install ksc-web-console-<組建編號>.x86_64.rpm`
     - 對於執行基於 Debian 的作業系統的裝置：
       `sudo apt-get install ksc-web-console-<組建編號>.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。

5. 透過執行以下命令重新啟動所有卡巴斯基安全管理中心 網頁主控台服務：
   `sudo systemctl restart KSC*`

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。

如果管理伺服器通用憑證被備份中的另一個憑證替換，或被使用klsetsrvcert公用程式替換，則必須刪除，然後重新安裝卡巴斯基安全管理中心網頁主控台。否則，登入網頁主控台將受到限制。
如果重新安裝後無法登入網頁主控台，請檢查 IAM 伺服器設定。

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，您必須建立回應檔案 — 一個包含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的 .json 檔案。必須將該檔案命名為 ksc-web-console-setup.json，並將其放置到以下目錄：/etc/ksc-web-console-setup.json。

回應檔案的參數集取決於卡巴斯基安全管理中心網頁主控台所連線的管理伺服器版本。

- 16 或更高版本的管理伺服器

  管理伺服器版本16或更高版本包含身分和存取管理器（IAM），該元件支援在卡巴斯基安全管理中心網頁主控台中透過單一登入 (SSO) 進行網域身分驗證。為了讓卡巴斯基安全管理中心網頁主控台連線到管理伺服器，即使您不使用單一登入 (SSO)，回應檔案也必須包含與 IAM 元件互動所需的參數。

  以下是安裝網頁主控台所需的回應檔案範例，該主控台將連線到版本 16 或更高版本的管理伺服器。在本範例中，網頁主控台和管理伺服器安裝在不同的裝置上：

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "defaultLangId": 1049,
    "enableLog": true,
    "trusted":  {
        "Administration Server v16": {
    "iamHost": "ksc16.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
    "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
    "kscPort": 13299,
    "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "acceptEula": true,
    "certPath": "/root/server.crt",
    "keyPath": "/root/key-without-passphrase.pem",
    "webConsoleAccount": "Group1:User1",
    "managementServiceAccount": "Group1:User2",
    "serviceWebConsoleAccount": "Group1:User3",
    "pluginAccount": "Group1:User4",
    "natsMessageQueueAccount": "Group1:User6"
}
```

- 15.4 或更早版本的管理伺服器

  管理伺服器 15.4 或更早版本僅支援透過指定內部使用者或網域使用者的使用者名稱和密碼進行身分驗證。

  以下是安裝網頁主控台所需的回應檔案範例，該主控台將連線到版本 15.4 或更早版本的管理伺服器：

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "defaultLangId": 1049,
    "enableLog": true,
    "trusted":  {
        "Administration Server v15.4": {
    "kscHost": "ksc.example.com",
    "kscPort": 13299,
    "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "acceptEula": true,
```

```
    "certPath": "/root/server.crt",
    "keyPath": "/root/key-without-passphrase.pem",
    "webConsoleAccount": "Group1:User1",
    "managementServiceAccount": "Group1:User2",
    "serviceWebConsoleAccount": "Group1:User3",
    "pluginAccount": "Group1:User4",
    "natsMessageQueueAccount": "Group1:User6"
}
```

參數 `webConsoleAccount`、`managementServiceAccount`、`serviceWebConsoleAccount`、`pluginAccount, natsMessageQueueAccount`、`certPath` 與 `keyPath` 為選用。您可以在回應檔案中忽略這些參數。

如果要使用自訂憑證，請同時指定`certPath`和`keyPath`參數。如果您不指定參數或僅指定一個參數，Web 瀏覽器會不斷通知您您的連線不是私密的。

> 基於安全理由，不建議指定 `webConsoleAccount`、`managementServiceAccount`、`serviceWebConsoleAccount`、`pluginAccount` 與 `natsMessageQueueAccount` 參數。
> 如果您決定指定這些參數，請確保自訂使用者帳戶屬於同一安全群組。當未指定這些參數時，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。
> `webConsoleAccount`、`managementServiceAccount`、`serviceWebConsoleAccount`、`pluginAccount` 與 `natsMessageQueueAccount` 參數不得彼此分開使用：請為所有這些參數指定值，或都不要指定值。

您可以將卡巴斯基安全管理中心網頁主控台安裝到管理伺服器所在的同一裝置，也可以安裝到不同裝置。如果將卡巴斯基安全管理中心網頁主控台安裝到不同裝置，則其位址（由 `address` 指定）將會與管理伺服器位址（由 `iamHost` 或者 `kscHost` 指定）不同。如果將卡巴斯基安全管理中心網頁主控台安裝到管理伺服器所在的同一裝置，則這些參數的值將相同。

`iamHost`值必須與安裝管理伺服器時指定的 IAM 位址相符。若要取得指定的 IAM 位址，請在管理伺服器主機上執行下列命令：

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

我們建議您指定 1024 以上的連接埠號。如果您希望卡巴斯基安全管理中心網頁主控台在 1024 以下的連接埠上工作，則安裝程式後您必須執行以下命令：

```
sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
```

如果沒有 setcap 實用程式，您可以安裝它。**點擊此連結檢視命令**。

對於 Debian 和 Ubuntu 作業系統，請執行以下命令之一：

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

對於 SUSE Linux Enterprise Server 和 Red Hat Enterprise Linux，請執行以下命令：

- `sudo zypper install libcap-progs`

> 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	安裝有卡巴斯基安全管理中心網頁主控台的裝置位址（FQDN 或主機名稱）（必需）。 如果您在卡巴斯基安全管理中心伺服器上安裝卡巴斯基安全管理中心網頁主控台，請使用安裝卡巴斯基安全管理中心 Linux 時指定的位址。 如果將卡巴斯基安全管理中心網頁主控台安裝到不同裝置，請指定網頁瀏覽器用於連線至卡巴斯基安全管理中心網頁主控台伺服器的裝置位址（FQDN 或主機名稱）。	字串值。 示例：`"ksc.example.com"`
port	卡巴斯基安全管理中心網頁主控台用於接收來自 Web 瀏覽器的連線的連接埠（必要）。	數值。 建議值為 8080（Linux ALT 作業系統例
defaultLangId	使用者介面語言（預設，`1033`）。 如有必要，您可以變更卡巴斯基安全管理中心網頁主控台介面的語言。	語言數位： • 德文：`1031` • 英文：`1033` • 西班牙文：`1034` • 西班牙文（墨西哥）：`2058` • 法文：`1036` • 義大利語：`1040` • 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：`2052` • 繁體中文：`1028` 如果沒有指定值，則使用 English（en-l
enableLog	是否要啟用卡巴斯基安全管理中心 網頁主控台偵錯記錄。 我們建議您僅在卡巴斯基技術支援專家要求時才變更該參數的預設值。	布爾值： • `true` — 記錄已啟用。 • `false` — 記錄已停用（預設選中）

參數	敘述	可用值
`trusted`	卡巴斯基安全管理中心網頁主控台可以連線到的受信任管理伺服器位址清單。您可以將多個不同版本的管理伺服器新增到受信任伺服器清單。 版本 16 或更高版本的管理伺服器： • 將顯示在登入視窗中的管理伺服器名稱。 • `iamHost` 是管理伺服器的位址（FQDN 或主機名稱），其中包含 IAM 元件（自卡巴斯基安全管理中心 Linux 版本 16 起），且卡巴斯基安全管理中心網頁主控台將連線到該管理伺服器。`iamHost` 值必須與安裝管理伺服器時指定的 IAM 位址相符。若要取得指定的 IAM 位址，請在管理伺服器主機上執行下列命令：`grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml` • `iamOAuthPort` 是用於透過 OpenID Connect 身分驗證協定交換身分驗證權杖的連接埠（預設值為 4444）。此連接埠同時用於卡巴斯基安全管理中心網頁主控台伺服器與管理伺服器之間的通訊，以及瀏覽器（與卡巴斯基安全管理中心網頁主控台搭配使用）與管理伺服器之間的通訊。 • `iamProxyPort` 是用於將卡巴斯基安全管理中心網頁主控台連線到管理伺服器的連接埠（預設值為 9050）。 • `iamCertPath` 是 IAM 憑證的路徑。IAM 憑證會在首次執行管理伺服器時自動建立。憑證位於安裝管理伺服器的裝置上。憑證的預設路徑：/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem。自簽發 IAM 憑證會自動輪換。 • `iamPATPath` 是用於將卡巴斯基安全管理中心網頁主控台註冊為 IAM 中的 OAuth 用戶端時所用的權杖路徑。此檔案會在首次執行管理伺服器時自動產生。權杖位於安裝管理伺服器的裝置上。權杖的預設路徑：/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt。權杖永久有效，無需輪換。 • `kscPort` 是用於透過 OpenAPI 將卡巴斯基安全管理中心網頁主控台和 IAM 連線到管理伺服器的連接埠（預設值為 13299）。 • `kscCertPath` 是管理伺服器憑證的路徑。憑證位於安裝管理伺服器的裝置上。憑證的預設路徑：/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer。 版本 15.4 或更早版本的管理伺服器： • 將顯示在登入視窗中的管理伺服器名稱。 • `kscHost` 是卡巴斯基安全管理中心網頁主控台連線到的管理伺服器的位址（FQDN、主機名稱或 IP 位址）。 • `kscPort` 是用於將卡巴斯基安全管理中心網頁主控台連線到管理伺服器的 OpenAPI 連接埠（預設是 13299）。 • `kscCertPath` 是管理伺服器憑證的路徑。憑證位於安裝管理伺服器的裝置上。憑證的預設路徑：/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer。 將卡巴斯基安全管理中心網頁主控台安裝到非管理伺服器所在的裝置時，請將管理伺服器憑證檔案（由 `kscCertPath` 指定）、IAM 憑證檔案（由 `iamCertPath` 指定）以及權杖檔案（由 `iamPATPath` 指定）從已安裝管理伺服器的裝置複製到目標裝置。在網頁主控台安裝程式的回應檔案中指定檔案的本機路徑。	JSON 檔案的一部分採用以下格式： `"trusted": { "Administration Server v16": { "iamHost": "ksc-iam.example.com", "iamOAuthPort": 4444, "iamProxyPort": 9050, "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_ "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/init "kscPort": 13299, "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cer }, "Administration Server v15.4": { "kscHost": "ksc.example.com", "kscPort": 13299, "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cer } }` 您可以指定任何管理伺服器名稱，而不 `Administration Server v16` 和 `Adm Server v15.4`。
`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。	布爾值： • `true` — 我確認我已完整閱讀、理解 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 取）。 如果未指定任何值，卡巴斯基安全管理 安裝程式會向您顯示 EULA 並詢問您是 EULA 的條款。
`certDomain`	如果您想要產生新的自簽章憑證，請使用此參數指定用於將 Web 瀏覽器連線至卡巴斯基安全管理中心網頁主控台 的 FQDN。	字串值。
`certPath`	使用此參數指定在您的基礎架構中受信任且符合自訂憑證要求的卡巴斯基安全管理中心網頁主控台自訂憑證的路徑。 您只能為一個憑證或一個憑證鏈指定一個私鑰（`keyPath`）。	字串值。 卡巴斯基安全管理中心網頁主控台不支 在要安裝卡巴斯基安全管理中心網頁主 指定 PEM 格式的憑證檔案的路徑。 示例：`/root/server.crt`

參數	敘述	可用值
keyPath	使用該參數指定與 `certPath` 參數中指定的卡巴斯基安全管理中心網頁主控台自訂憑證關聯的私鑰路徑。	字串值。 帶有私鑰的檔案不得被加密。 在要安裝卡巴斯基安全管理中心網頁主指定 PEM 格式的金鑰檔案的路徑。 示例： `/root/key-without-passph`
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 >:< >""`。 例如： `""Group1:User1""`. 如果未指定任何值，卡巴斯基安全管理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帳戶名稱。	以下格式的字串值：`""< 群組名稱 >:< >""`。 例如：`""Group1:User2""`。 如果未指定任何值，卡巴斯基安全管理安裝程式會建立一個預設名稱為 `user_` 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 >:< >""`。 例如： `"Group1:User3"` 。 如果未指定任何值，卡巴斯基安全管理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服務的帳戶名稱。	以下格式的字串值：`""< 群組名稱 >:< >""`。 例如：`""Group1:User4""`。 如果未指定任何值，卡巴斯基安全管理安裝程式會建立一個預設名稱為 `user_web_plugin_%uid%` 的新帳戶。
natsMessageQueueAccount	執行卡巴斯基安全管理中心網頁主控台 NATS服務的帳戶名稱。	以下格式的字串值：`""< 群組名稱 >:< >""`。 例如：`""Group1:User6""`。 如果未指定任何值，卡巴斯基安全管理安裝程式會建立一個預設名稱為 `user_message_queue_%uid%` 的新帳

在封閉軟體環境模式下在 Astra Linux 上安裝卡巴斯基安全管理中心網頁主控台

該部分描述了如何在 Astra Linux 特別版作業系統上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 Linux管理伺服器。

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 Linux 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. 建立回應檔案，其中包含用於將卡巴斯基安全管理中心網頁主控台連線至管理伺服器的參數： `/etc/ksc-web-console-setup.json` 。

   包含最小參數集合的回應檔案範例

回應檔案的參數集取決於卡巴斯基安全管理中心網頁主控台所連線的管理伺服器版本：

- 16 或更高版本的管理伺服器

  以下是登入管理伺服器版本 16 或更高版本所需的採用最小參數集的回應檔案範例：

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- 15.4 或更早版本的管理伺服器

  以下是登入管理伺服器版本 15.4 或更早版本所需的採用最小參數集的回應檔案範例：

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

您可以將卡巴斯基安全管理中心網頁主控台安裝到管理伺服器所在的同一裝置，也可以安裝到不同裝置。如果將卡巴斯基安全管理中心網頁主控台安裝到不同裝置，則卡巴斯基安全管理中心網頁主控台位址（由 `address` 指定）將會與管理伺服器位址（由 `iamHost` 或 `kscHost` 指定）不同。如果將卡巴斯基安全管理中心網頁主控台安裝到管理伺服器所在的同一裝置，則這些參數的值將相同。

`iamHost` 值必須與您在安裝管理伺服器時指定的 IAM 位址相符。若要取得指定的IAM位址，請在管理伺服器主機上執行下列命令：

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

有關詳細資訊，請參閱文章：卡巴斯基安全管理中心網頁主控台安裝程式參數。

您可以將多個不同版本的管理伺服器新增到受信任伺服器清單。在這種情況下，這些伺服器可以使用不同的身分驗證方法。

4. 開啟 `/etc/digsig/digsig_initramfs.conf` 檔案，然後指定以下設定：

```
DIGSIG_ELF_MODE=1
```

5. 在指令行中，執行以下指令來安裝相容套件：

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

6. 為應用程式金鑰建立一個目錄：

```
mkdir -p /etc/digsig/keys/legacy/kaspersky/
```

7. 將應用程式金鑰 `/opt/kaspersky/ksc64/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 Linux 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。

8. 更新 RAM 瓷碟：

```
update-initramfs -u -k all
```

重新啟動系統。

9. 在具有 root 權限的帳戶下，使用指令行執行安裝檔案。您透過從 Kaspersky 網站下載來接收安裝檔案。

- 要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 apt-get install ksc-web-console-<build_number>.x86_64.deb
```

- 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：

```
sudo apt-get install 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`。

10. 透過執行以下命令重新啟動所有卡巴斯基安全管理中心 網頁主控台服務：

```
sudo systemctl restart KSC*
```

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。

使用指令碼安裝Kaspersky Security Center for Linux

`ksc_fast_install.py` 指令碼可讓您部署卡巴斯基安全管理中心 Linux，並執行其元件的初始設定：管理伺服器和網頁主控台，包括資料庫管理系統 (DBMS) 和所需的支援套件。

指令碼會從參數檔案讀取參數。使用參數的預設值。根據需要，您可以變更規則。

指令碼的運作方式

執行期間，指令碼會：

- 檢查是否符合以下條件：
  - 您具備執行指令碼所需的權限。
  - 指令碼與作業系統和資料庫管理系統相容。
  - 已接受 EULA 和隱私權政策。
    如果您未在參數檔案中接受這些條款，系統會在執行指令碼後提示您接受。
  - 管理伺服器和網頁主控台的硬體需求。
    這些需求已在 Sizing Guide 中定義。
- 安裝資料庫管理系統（若尚未安裝）並設定其參數
- 建立卡巴斯基安全管理中心資料庫，設定作業系統憑據
- 安裝管理伺服器、網頁主控台
- 提供用於登入網頁主控台的登入名稱和密碼。
  關閉命令列終端機之前，請以任何便利的方式儲存憑據。如果遺失憑據，您必須執行以下命令新增使用者帳戶：`/opt/kaspersky/ksc64/sbin/kladduser -n <使用者>`

如果未符合一或多個條件或發生錯誤，指令碼將會終止，並顯示對應通知。

> 此指令碼不包含系統強化操作。若要降低卡巴斯基安全管理中心遭入侵的風險，請考慮採用強化指南中的建議。
> 指令碼式安裝方法適用於在未安裝卡巴斯基安全管理中心 Linux 的裝置上部署卡巴斯基安全管理中心 Linux 16.3 及更新版本。
> 執行此指令碼需要 Python 3.6 及更新版本。

只有在目前裝置上未安裝卡巴斯基安全管理中心 Linux 時，才能進行部署。

您不能使用此指令碼升級至卡巴斯基安全管理中心 Linux 的新版本；如果已部署卡巴斯基安全管理中心 Linux 容錯移轉叢集，也不能使用此指令碼。

`ksc_fast_install.py` 指令碼支援在搭配表中所述 DBMS 的作業系統版本上安裝卡巴斯基安全管理中心 Linux。

作業系統版本	DBMS
Ubuntu Server 26.04 LTS	PostgreSQL 18
RED OS 8	PostgreSQL 16
Astra Linux特別版RUSB.10015-01（版本1.8.5）	PostgreSQL 15
CentOS Stream 10	PostgreSQL 18

指令碼不支援自訂資料庫結構描述。

如何透過指令碼執行部署

先決條件

在執行指令碼之前，請確保您已完成以下事項：

- 執行下列其中一個指令來更新您的作業系統：`dnf update` 或 `apt update`
- 透過執行以下指令取得超級使用者權限：`sudo -i`
- 透過執行以下指令，允許執行指令碼：`chmod +x ./ksc_fast_install.py`
- 透過執行以下指令，確保您作業系統的儲存庫包含受支援的 DBMS：`sudo apt policy postgresql`

若要透過執行指令碼部署Kaspersky Security Center for Linux：

1. 從 Kaspersky 網站 下載以下內容：
   - 適用於管理伺服器和網頁主控台的 .deb 或 .rpm 分發套件。
   - 「KSC 安裝指令碼」壓縮檔案。

     使用此指令碼時，請選擇與您作業系統的套件管理員相容的管理伺服器和網頁主控台分發套件。

     此壓縮檔案包含以下檔案：

     - `ksc_fast_install.py` 指令碼檔案。
     - 參數檔案。

       預設檔名為`params.txt`。如果您想重新命名該檔案，請確保在命令列終端機中執行指令碼時，已透過`--params`參數指定新名稱。
     - 包含管理伺服器 EULA 和隱私權政策的檔案。
     - 包含卡巴斯基安全管理中心網頁主控台 EULA 的檔案。
     - 包含 EULA 雜湊值的檔案。
2. 將所有下載的檔案放置在同一個本機目錄中。
3. 如有必要，請設定參數檔案。

   按一下此處，檢視包含參數說明的參數檔案範例

   ```
   # Required parameters:

   #klfi_server_eula_accepted=N

   #klfi_nwc_eula_accepted=N
   ```

```
#klfi_pp_accepted=N

# Optional parameters:

#klfi_klserver_db=KAV

#klfi_klserver_dbuser=klserver

#klfi_klserver_address=

#klfi_kliam_db=KAV_IAM

#klfi_kliam_dbuser=kliam

#klfi_kliam_address=

#klfi_sys_group_kladmin=kladmins

#klfi_sys_user_klserver=klsrvuser

#klfi_sys_user_kliam=kliamuser

#klfi_sys_user_svc=klsvcuser

#klfi_nwc_port=8080

#klfi_display_name=

#klfi_netsize=M
```

`klfi_server_eula_accepted=N`、`klfi_nwc_eula_accepted=N` 和 `klfi_pp_accepted=N` 參數為必填，且一律存在於參數檔案中。其他參數為選填。

針對必填參數：

- 如果您未取消該行的註解就變更預設值，系統會提示您接受 EULA 和隱私權政策。
- 如果您指定的值不是 `Y` 或 `N`，則無論您是否已取消該行的註解，系統都會提示您接受 EULA 和隱私權政策。
- 如果您取消該行的註解，但未變更預設值 `N`，指令碼將無法運作。
- 如果您取消該行的註解並設定 `Y` 值，指令碼將不會提示您。

參數及其預設值	參數說明和其他可能的值（如果有）
`klfi_server_eula_accepted=N`	管理伺服器的最終使用者產品授權協議。 可能的值： • `Y` – 已接受 EULA。 • `N` – 未接受 EULA。
`klfi_nwc_eula_accepted=N`	卡巴斯基安全管理中心網頁主控台的最終使用者產品授權協議。 可能的值： • `Y` – 已接受 EULA。 • `N` – 未接受 EULA。

klfi_pp_accepted=N	隱私權政策。 可能的值： • Y – 已接受隱私權政策。 • N – 未接受隱私權政策。
klfi_klserver_db=KAV	管理伺服器資料庫名稱。 該名稱必須與 klfi_kliam_db 參數中指定的 IAM 資料庫名稱不同。
klfi_kliam_db=KAV_IAM	IAM 資料庫名稱。 該名稱必須與 klfi_klserver_db 參數中指定的管理伺服器資料庫名稱不同。
klfi_klserver_dbuser=klserver	管理伺服器資料庫使用者名稱。
klfi_kliam_dbuser=kliam	IAM 資料庫使用者名稱。
klfi_klserver_address=FQDN	管理伺服器 FQDN 或目前的裝置名稱。 如果未指定參數值，指令碼會自動判定 FQDN 或您執行指令碼所在裝置的名稱。 如果指令碼無法判定這些值，安裝將完成但發生錯誤。
klfi_kliam_address=FQDN	IAM 伺服器 FQDN 或目前的裝置名稱。 如果未指定參數值，指令碼會自動判定 FQDN 或您執行指令碼所在裝置的名稱。 如果指令碼無法判定這些值，安裝將完成但發生錯誤。
klfi_sys_group_kladmin=kladmins	服務的安全群組名稱。
klfi_sys_user_klserver=klsrvuser	帳戶名稱以啟動管理伺服器服務。
klfi_sys_user_kliam=kliamuser	啟動 IAM 服務的帳戶名稱。
klfi_sys_user_svc=klsvcuser	帳號名稱以啟動其他服務。
klfi_nwc_port=8080	連線至卡巴斯基安全管理中心網頁主控台的連接埠。
klfi_display_name=FQDN	將顯示在登入視窗中的管理伺服器名稱。

`klfi_netsize=M`	您打算管理的裝置的大致數量：
	每項估算均已考量執行卡巴斯基應用程式所需的資源。此計算涵蓋在單一裝置上同時執行管理伺服器、網路代理、卡巴斯基安全管理中心網頁主控台和 Kaspersky Endpoint Security for Linux。
	這些計算不包含管理伺服器備份的儲存空間。使用外部檔案資源作為掛載點，以將備份儲存在個別裝置上，或增加可用磁碟空間以納入備份儲存需求。
	建議為安裝作業系統額外增加 4–6 GB RAM 和 20 GB 可用磁碟空間。
	依網路規模估算硬體資源：
	• `S` –1 至 1000 部受管理裝置。
	  • CPU–8 核心
	  • RAM–16 GB
	  • `/var` 目錄的可用磁碟空間–70 GB，300 IOPS 或更高
	• `M` –1001 至 10000 部受管理裝置。
	  • CPU–12 核心
	  • RAM–24 GB
	  • `/var` 目錄的可用磁碟空間–340 GB，300 IOPS 或更高
	• `L` –10001 至 30000 部受管理裝置。
	  • CPU–20 核心
	  • RAM–40 GB
	  • `/var` 目錄的可用磁碟空間–490 GB，300 IOPS 或更高
	• `XL` –30001 至 50000 部受管理裝置。
	  • CPU–28 核心
	  • RAM–54 GB
	  • `/var` 目錄的可用磁碟空間–640 GB，300 IOPS 或更高

參數檔案中的各行均已加上註解。如果您要設定這些值，請移除要取消註解之行開頭的 # 符號。

`klfi_server_eula_accepted`、`klfi_nwc_eula_accepted` 和 `klfi_pp_accepted` 參數為必填項目，其預設值為 `N`。如果您在未變更參數檔案中這些值的情況下執行指令碼，系統會提示您接受 EULA 和隱私權政策。

4. 執行指令碼。

指令碼執行後，會顯示Kaspersky Security Center for Linux元件部署成功的通知，以及用於登入網頁主控台的登入名稱和密碼。

如果不符合指令碼式安裝的條件、參數檔案中指定了未知參數，或某個參數重複多次，指令碼會傳回錯誤，並顯示相應通知。

如果指令碼在資源探索步驟中錯誤偵測到 RAM 不足，請在安裝期間停用動態 RAM 使用。

如果在安裝Kaspersky Security Center for Linux元件或DBMS時發生錯誤，指令碼會復原變更，然後終止。

安裝失敗時的復原

如果在安裝Kaspersky Security Center for Linux元件或DBMS時發生錯誤，指令碼會自動執行復原。錯誤發生前安裝的元件或DBMS會遭到刪除。

作業系統套件的升級和支援套件的安裝不會復原。

如果您手動終止指令碼，已成功完成的步驟不會復原。如有必要，您可以重新執行指令碼，安裝將從中斷的步驟繼續。

若要繼續安裝，您必須在命令列終端機中使用`rollback`參數執行指令碼：`python3 ksc_fast_install.py rollback`

部署 卡巴斯基安全管理中心 Linux 容錯移轉叢集

卡巴斯基安全管理中心 Linux 容錯移轉叢集提供 卡巴斯基安全管理中心 Linux 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 Linux 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。

卡巴斯基安全管理中心 Linux 故障轉移叢集支援兩種配置：

- 節點位於單一資料中心的故障轉移叢集；
- 節點位於不同資料中心的異地分散式故障轉移叢集。

在卡巴斯基安全管理中心 Linux 容錯移轉叢集中，所有卡巴斯基安全管理中心 Linux 服務都是自動管理的。不要嘗試手動重新啟動服務。

使用 syslog 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 Linux 服務（或處理程序）失敗或被意外終止。卡巴斯基安全管理中心 Linux 服務包括：klnagent_klfoc、kladminserver_klfoc、klactprx_klfoc、klwebsrv_klfoc。
- 活動節點與檔案伺服器上的儲存體之間的網路連線已中斷或終止（僅適用於位於單一資料中心的叢集）。

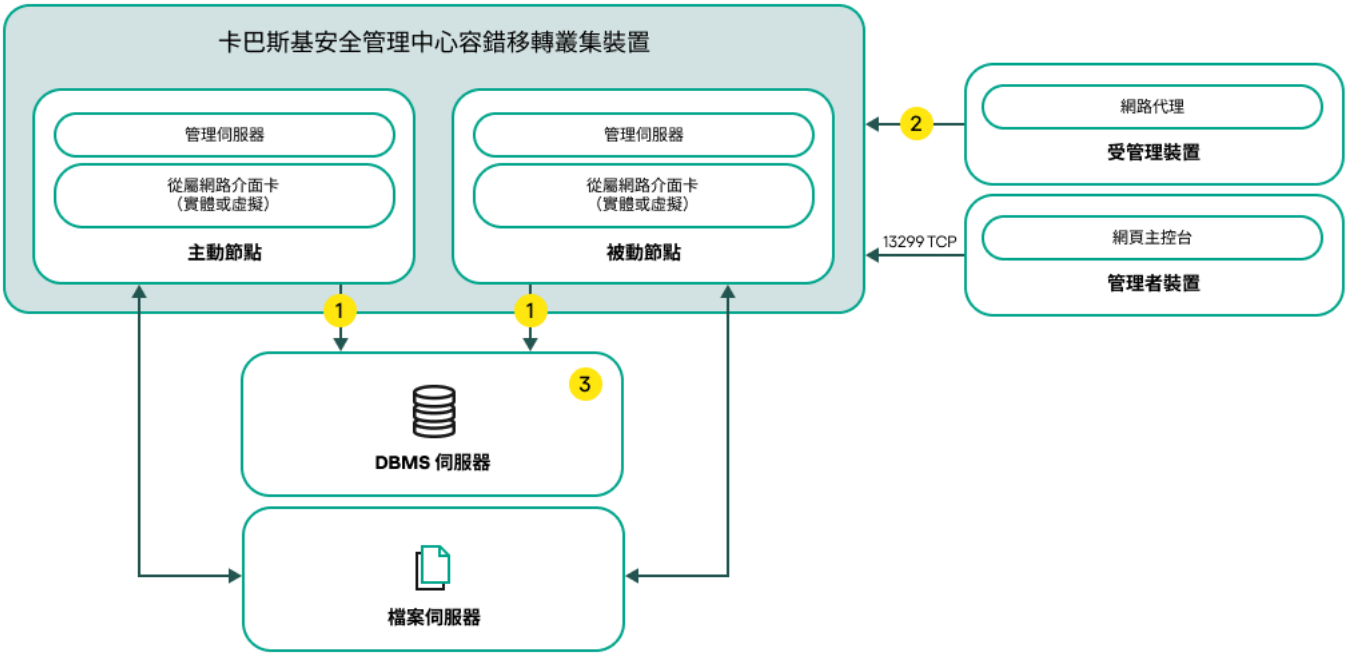
卡巴斯基安全管理中心 Linux 容錯移轉叢集部署方案

您可以選擇以下方案之一來部署卡巴斯基安全管理中心 Linux 容錯移轉叢集：

- Kaspersky Security Center for Linux故障轉移叢集部署在單一資料中心內：
  - 使用從屬網路介面卡和安裝在專用裝置上的 DBMS 的方案。
  - 使用第三方負載平衡器和安裝在專用裝置上的 DBMS 的方案。
- 異地分散式Kaspersky Security Center for Linux故障轉移叢集部署在多個資料中心內。

卡巴斯基安全管理中心 Linux 容錯移轉叢集

使用從屬網路介面卡和安裝在專用裝置上的 DBMS 的方案。



使用從屬網路介面卡和安裝在專用裝置上的 DBMS 的方案。

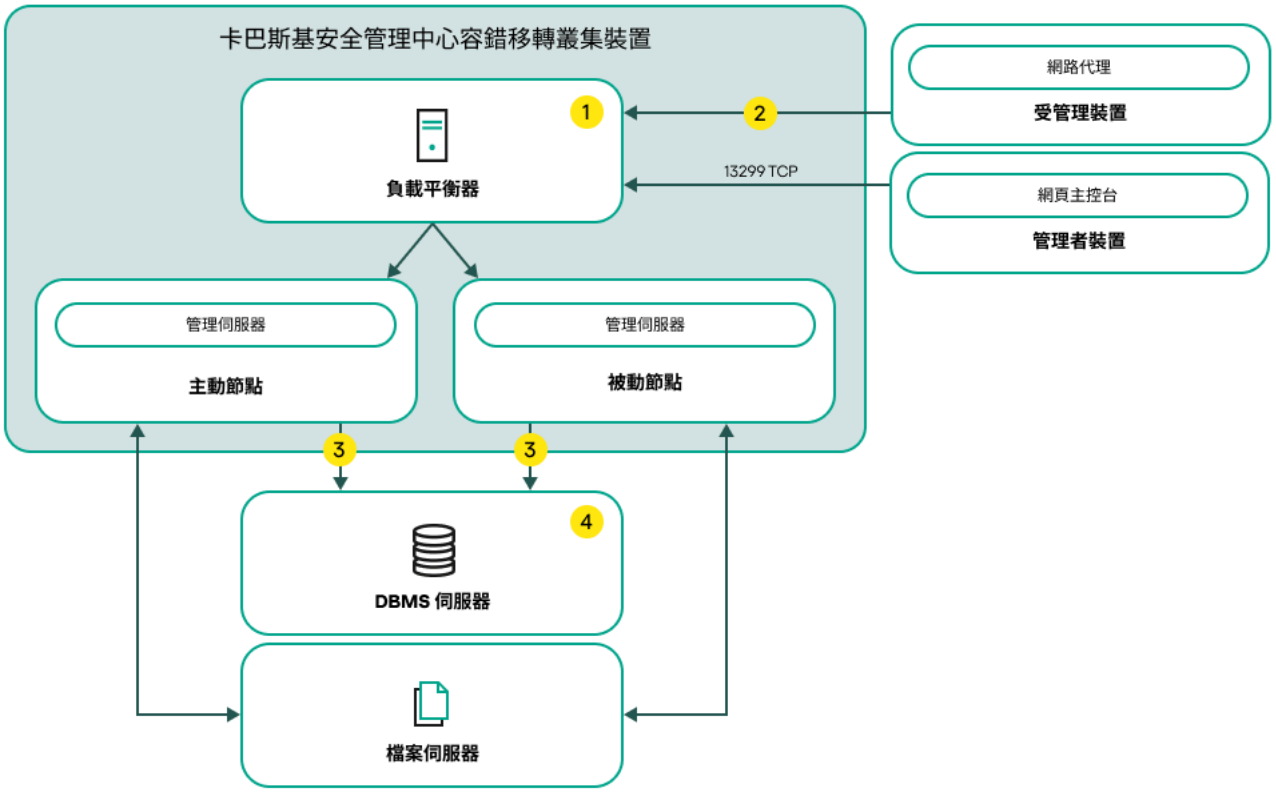
方案圖例：

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，PostgreSQL Server 或者 Postgres Pro 為 5432 連接埠。請參閱 DBMS 文件以取得相關資訊。

2 開啟具有管理伺服器的裝置上的下列連接埠以連線到受管理裝置：TCP 13000、UDP 13000 和 TCP 17000。

3 具有資料庫管理系統 (DBMS) 的裝置。如果您使用 MariaDB Galera Cluster 作為 DBMS，則不需要用於此目的的專用裝置。在每個節點上安裝 MariaDB Galera Cluster。

使用第三方負載平衡器和安裝在專用裝置上的 DBMS 的方案



使用第三方負載平衡器和安裝在專用裝置上的 DBMS 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。

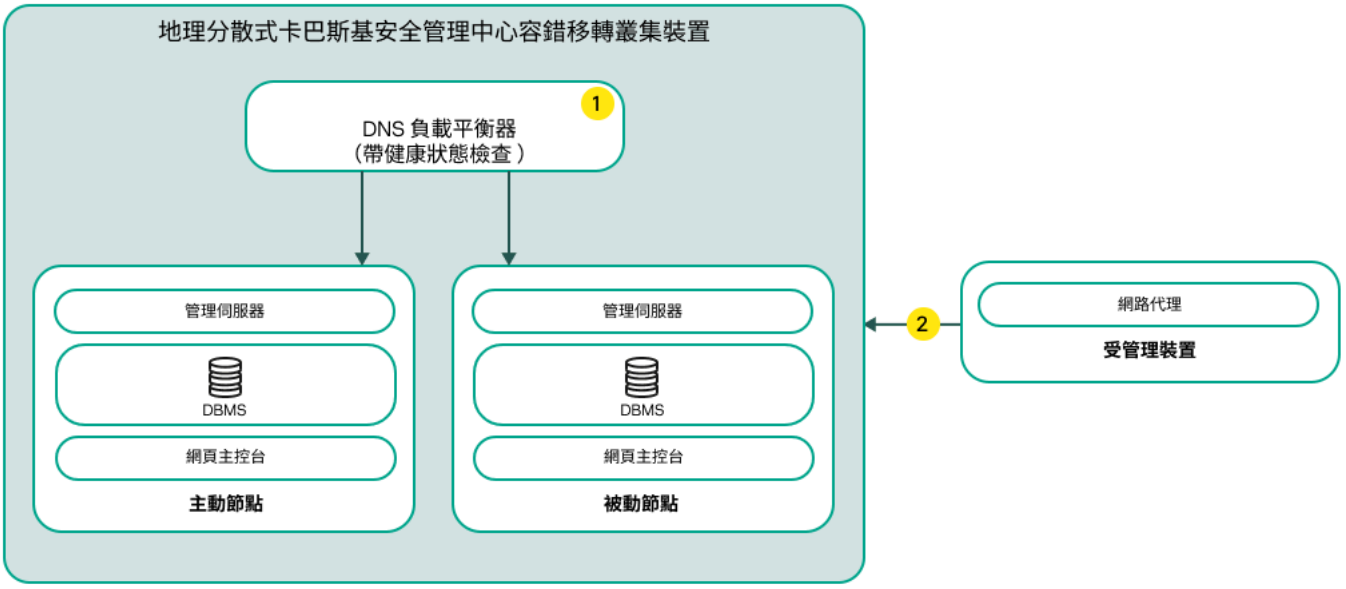
2 開啟具有管理伺服器的裝置上的下列連接埠以連線到受管理裝置：TCP 13000、UDP 13000 和 TCP 17000。

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，PostgreSQL Server 或者 Postgres Pro 為 5432 連接埠。請參閱 DBMS 文件以取得相關資訊。

4 具有資料庫管理系統 (DBMS) 的裝置。如果您使用 MariaDB Galera Cluster 作為 DBMS，則不需要用於此目的的專用裝置。在每個節點上安裝 MariaDB Galera Cluster。

異地分散式Kaspersky Security Center for Linux故障轉移叢集

此部署方案可確保所有元件的高可用性。在此方案中，管理伺服器、DBMS和卡巴斯基安全管理中心網頁主控台安裝在兩個叢集節點上。



異地分散式Kaspersky Security Center for Linux故障轉移叢集的部署方案

1 在安裝異地分散式Kaspersky Security Center for Linux故障轉移叢集之前，必須在您的伺服器上部署具有運行狀況檢查功能的DNS負載平衡器。

DNS負載平衡器會定期檢查叢集節點的運行狀態。當透過網域存取叢集時，DNS負載平衡器總是會傳回活動節點的IP位址。

2 開啟具有管理伺服器的裝置上的下列連接埠以連線到受管理裝置：TCP 13000、UDP 13000 和 TCP 17000。

卡巴斯基安全管理中心 Linux 容錯移轉叢集

本章節包含有關部署在單一資料中心內的Kaspersky Security Center for Linux故障轉移叢集的一般資訊，以及在網路中準備和部署Kaspersky Security Center for Linux故障轉移叢集的說明。

情境：部署 卡巴斯基安全管理中心 Linux 容錯移轉叢集

卡巴斯基安全管理中心 Linux 容錯移轉叢集提供 卡巴斯基安全管理中心 Linux 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 Linux 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。

Kaspersky 應用程式佈署分步驟進行：

建議遵循在此情境中描述的階段順序。

1. **檢查硬體要求**

   確保您擁有滿足容錯移轉叢集要求的硬體。

2. **選擇部署方案**

   選擇部署方案。這會影響部署的後續階段。

3. **為卡巴斯基安全管理中心 Linux 服務準備使用者帳戶**

   在主動節點、被動節點和檔案伺服器上執行以下步驟：

   1. 建立 `kladmins` 群組。執行以下指令：

      `sudo groupadd kladmins`

      `sudo groupmod -g <new_GID> kladmins`

      確保該群組在所有三個裝置上具有相同的 GID。執行以下指令：

      `getent group kladmins`

      如果 GID 不匹配，您可以使用以下命令指定 GID：

      `sudo groupmod -g <new_GID> kladmins`

   2. 建立 `ksc` 使用者帳戶。將使用者帳戶指派給 `kladmins` 群組。執行以下指令：

      `sudo adduser ksc`

      `sudo usermod -u <new_UID> ksc`

      `sudo gpasswd -a ksc kladmins`

      `sudo usermod -g kladmins ksc`

      確保使用者帳戶在所有三個裝置上具有相同的 UID。執行以下指令：

      `getent passwd ksc`

      如果 UID 不匹配，您可以使用以下命令指定 UID：

      `sudo usermod -u <new_UID> ksc`

   3. 建立`rightless`使用者帳戶。將使用者帳戶指派給 `kladmins` 群組。執行以下指令：

      `sudo adduser rightless`

      `sudo usermod -u <new_UID> rightless`

      `sudo gpasswd -a rightless kladmins`

      `sudo usermod -g kladmins rightless`

      確保使用者帳戶在所有三個裝置上具有相同的 UID。執行以下指令：

      `getent passwd rightless`

      如果 UID 不匹配，您可以使用以下命令指定 UID：

      `sudo usermod -u <new_UID> rightless`

   4. 建立`ksciam`使用者帳戶。將使用者帳戶指派給 `kladmins` 群組。執行以下指令：

`sudo adduser ksciam`

`sudo usermod -u <new_UID> ksciam`

`sudo gpasswd -a ksciam kladmins`

`sudo usermod -g kladmins ksciam`

確保使用者帳戶在所有三個裝置上具有相同的 UID。執行以下指令：

`getent passwd ksciam`

如果 UID 不匹配，您可以使用以下命令指定 UID：

`sudo usermod -u <new_UID> ksciam`

5. 如有必要，增加用於卡巴斯基安全管理中心 Linux 服務功能的帳戶可以開啟的檔案（檔案描述符）的預設限制。為此，請開啟 /etc/security/limits.conf 檔案，然後指定檔案描述符的軟限制和硬限制，如下所示：

   `ksc soft nofile <max_number_of_opened_files>`

   `ksc hard nofile <max_number_of_opened_files>`

   預設情況下，檔案描述符的限制在安裝期間指定。軟檔案限制為 32,768 個檔案，硬檔案限制為 131,072 個檔案。

4 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 Linux 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 Linux 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 Linux 容錯移轉叢集準備檔案伺服器

5 DBMS 安裝

為卡巴斯基安全管理中心 Linux 安裝 DBMS。您可以選擇一個受支援的 DBMS。對於如何安裝所選 DBMS 的資訊，請參考其文件。

如果 Linux 作業系統的發行版不包含支援的 DBMS，您可以從協力廠商套件儲存庫安裝 DBMS。

安裝 DBMS 後，請依照對應的說明進行操作：

- 設定 PostgreSQL 或 Postgres Pro 伺服器與 卡巴斯基安全管理中心 Linux 搭配使用
- 設定 MariaDB x64 伺服器以與 卡巴斯基安全管理中心 Linux 一起使用

為 IAM 建立一個資料庫。解除安裝或將伺服器移至其他裝置時，管理伺服器不會自動移除 IAM 資料庫，您必須手動移除資料庫。

- 對於 PostgreSQL，執行以下命令：

  `sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"`

- 對於 MariaDB，執行以下命令：

  `sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"`

在安裝了 DBMS 的設備上，配置將作為主動節點和被動節點運行的裝置的連線。

6 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 Linux 容錯移轉叢集準備節點

7 卡巴斯基安全管理中心 Linux 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 Linux。

您必須先在想要其成為主動節點的裝置上安裝卡巴斯基安全管理中心 Linux，然後再將其安裝在被動節點上。

說明：在卡巴斯基安全管理中心 Linux 容錯移轉叢集節點上安裝卡巴斯基安全管理中心 Linux。

8 **卡巴斯基安全管理中心網頁主控台安裝**

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。

在應答檔案中將容錯移轉叢集指定為管理伺服器位址。

管理伺服器憑證位於下列路徑：/mnt/KlFocDataShare_klfoc/1093/cert/klserver.cer

將憑證檔案複製到正在其上安裝卡巴斯基安全管理中心網頁主控台的裝置。在應答檔案中指定憑證的本機路徑。

9 **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，您可以執行下列命令啟動切換到被動節點：

```
/opt/kaspersky/ksc64/sbin/klfoc -failover --stp klfoc
```

使用下列命令驗證容錯移轉叢集管理服務是否在兩個節點上都處於`Active: active (running)`狀態：

```
systemctl status klfocsvc_klfoc
```

使用下列命令驗證其他容錯移轉叢集服務是否在主動節點上處於`Active: active (running)`狀態。在被動節點上，這些容錯移轉叢集服務必須處於`Active: inactive (dead)`或`Active: failed (Result: signal)`狀態。

- `systemctl status klnagent_klfoc`
- `systemctl status kladminserver_klfoc`
- `systemctl status klactprx_klfoc`
- `systemctl status klwebsrv_klfoc`

卡巴斯基安全管理中心 Linux 容錯移轉叢集已部署。

卡巴斯基安全管理中心 Linux 容錯移轉叢集硬體和軟體需求

建議您在主動和被動節點、具有DBMS的裝置以及檔案伺服器上安裝Kaspersky Endpoint Security for Linux。若要併發安裝卡巴斯基安全管理中心 Linux 容錯移轉叢集和 Kaspersky Endpoint Security for Linux，除了節點和檔案伺服器的需求外，還必須增加 1.5 GB 記憶體、15% CPU，並且至少具備 300 IOPS。

若要部署卡巴斯基安全管理中心 Linux 容錯移轉叢集，您必須擁有以下硬體：

- 兩台具有相同硬體和軟體的裝置。這些裝置將充當主動節點和被動節點。

主動和被動節點的最低配置

硬體	參數值
CPU	2 核，2500 MHz
RAM	6 GB
磁碟空間	10 GB、150 IOPS 或更高
網路介面控制器	1 Gbps

- 支援 CIFS/SMB 通訊協定的檔案伺服器，版本 2.0 或更高。您必須提供一台用作檔案伺服器的專用裝置。

檔案伺服器的配置

硬體	參數值
CPU	16 核心，2 500 MHz
RAM	32 GB
磁碟空間	500 GB，500 IOPS 或更高
網路介面控制器	10 Gbps

確保在檔案伺服器與主動和被動節點之間提供了高網路頻寬。

- 具有資料庫管理系統 (DBMS) 的裝置。如果您使用 MariaDB Galera Cluster 作為 DBMS，則不需要用於此目的的專用裝置。

為卡巴斯基安全管理中心 Linux 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 Linux 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. 安裝和配置 NFS 伺服器：
   - 必須在 NFS 伺服器設定中為兩個節點都啟用對檔案伺服器的存取。
   - NFS 通訊協定的版本必須為 4.0 或 4.1。
   - Linux 內核的最低要求：
     - 3.19.0-25（如果您使用 NFS 4.0）
     - 4.4.0-176，如果您使用 NFS 4.1

   根據您的 Linux 發行版，透過執行相應的命令來安裝 nfs-utils 軟體包或 nfs-kernel-server 軟體包：

   ```
   sudo yum install nfs-utils
   sudo apt install nfs-kernel-server
   ```

3. 在檔案伺服器上，建立兩個資料夾並使用 NFS 共用它們。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 Linux 的資料和設定。您將在配置 卡巴斯基安全管理中心 Linux 的安裝時指定共用資料夾的路徑。

   確保以下資料夾不存在：

   - `/mnt/KlFocStateShare`
   - `/mnt/KlFocDataShare_klfoc`

   如果存在任何這些資料夾，請遞歸刪除它。

   執行以下指令：

   `sudo mkdir -p /mnt/KlFocStateShare`

   `sudo mkdir -p /mnt/KlFocDataShare_klfoc`

`sudo chown ksc:kladmins /mnt/KlFocStateShare`

`sudo chown ksc:kladmins /mnt/KlFocDataShare_klfoc`

`sudo chmod -R 770 /mnt/KlFocStateShare /mnt/KlFocDataShare_klfoc`

`sudo sh -c "echo /mnt/KlFocStateShare *\(rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports"`

`sudo sh -c "echo /mnt/KlFocDataShare_klfoc *\(rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports"`

`sudo exportfs -a`

`sudo systemctl start rpcbind`

`sudo systemctl start nfs-server`

透過執行以下命令啟用自動啟動：

`sudo systemctl enable rpcbind`

您可以指定自訂資料夾，但我們建議您使用建議的資料夾名稱，以便於使用線上說明。

4. 重新啟動檔案伺服器。

檔案伺服器已準備就緒。若要部署卡巴斯基安全管理中心 Linux 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 Linux 容錯移轉叢集準備節點

在繼續之前，請確保您已完成情境：部署卡巴斯基容錯移轉叢集中的先前步驟。

準備兩台裝置作為卡巴斯基安全管理中心 Linux 容錯移轉叢集的主動和被動節點。

通用資料夾設定

要設定通用資料夾，請執行以下操作：

1. 根據您的 Linux 發行版，透過執行對應的命令在每個節點上安裝 nfs-utils 軟體包或 nfs-kernel-server 軟體包：

   `yum install nfs-utils`

   `apt install nfs-kernel-server`

2. 透過執行以下命令建立掛接點：

   `mkdir -p /mnt/KlFocStateShare`

   `mkdir -p /mnt/KlFocDataShare_klfoc`

3. 匹配掛接點和共用資料夾：

   `sudo sh -c "echo <`檔案伺服器`>:/mnt/KlFocStateShare /mnt/KlFocStateShare nfs vers=4,soft,timeo=50,retrans=2,auto,user,rw 0 0 >> /etc/fstab"`

   `sudo sh -c "echo <`檔案伺服器`>:/mnt/KlFocDataShare_klfoc /mnt/KlFocDataShare_klfoc nfs vers=4,noauto,user,rw,exec 0 0 >> /etc/fstab"`

   其中，`{`檔案伺服器`}`是帶有共用資料夾的檔案伺服器的 FQDN。

4. 透過執行以下命令掛載共用資料夾：

   `mount /mnt/KlFocStateShare`

   `mount /mnt/KlFocDataShare_klfoc`

5. 確保存取共用資料夾的權限屬於 ksc:kladmins。

   執行以下指令：

   `ls -la /mnt/`

網路卡設定

從屬網路介面卡可以是實體的，也可以是虛擬的。如果您選擇了具有次要網路介面卡的部署方案，請在兩個節點上執行對應的程序：

- 使用基於實體網路介面卡（MACVLAN 技術）的虛擬次要網路介面卡：

  1. 安裝 iputils-arping 套件。根據您的 Linux 版本，執行以下命令之一：

     - `yum install iputils`

     或

     - `apt install iputils-arping`

  2. 要確保使用 NetworkManager 來管理實體網路介面卡，請執行以下命令：

     `nmcli device status`

     如果命令輸出顯示實體網路介面卡未受管理，請設定 NetworkManager 來管理實體網路介面卡。確切的配置步驟取決於您的 Linux 發行版。

  3. 要識別介面，請使用以下命令：

     `ip a`

  4. 要建立設定檔，請執行以下命令：

     `nmcli connection add type macvlan dev <`實體介面`> mode bridge ifname <`虛擬介面`> ipv4.addresses <`位址遮罩`> ipv4.method manual autoconnect no`

- 使用實體次要網路介面卡或使用 Hypervisor 建立虛擬 TAP 裝置。在這種情況下，請停用 NetworkManager 軟體。

  1. 將次要網路介面卡連線到節點。

  2. 安裝 iputils-arping 套件。根據您的 Linux 版本，執行以下命令之一：

     - `yum install iputils`

     或

     - `apt install iputils-arping`

  3. 要刪除目標介面的 NetworkManager 連線，請執行以下命令：

     `nmcli con del <`連線名稱`>`

     要檢查與目標介面的連線，請執行以下命令：

     `nmcli con show`

  4. 修改 NetworkManager.conf 檔案。找到金鑰檔案區段，並將目標介面指派給 `unmanaged-devices` 參數：

     `[keyfile]`

`unmanaged-devices=interface-name:<介面名稱>`

5. 重新啟動 NetworkManager：

   `systemctl reload NetworkManager`

   要確保目標介面不再處於受管狀態，請執行以下命令：

   `nmcli dev status`

負載平衡器設定

如果您選擇了具有負載均衡器的部署方案，請遵照以下說明進行設定。

要設定負載均衡器，請執行以下操作：

1. 準備一個安裝了 nginx 或其他負載平衡器的專用 Linux 裝置。

2. 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。

3. 在 nginx 伺服器上，根據以下文章開啟所有管理伺服器連接埠：卡巴斯基安全管理中心 Linux 使用的連接埠。

若要部署卡巴斯基安全管理中心 Linux 容錯移轉叢集，請按照情境中的進一步說明進行操作。

> 容錯移轉叢集節點的可用性應由管理伺服器主連線連接埠的可用性決定。在切換發生之前，被動節點不接受任何外部連線。

在 卡巴斯基安全管理中心 Linux 容錯移轉叢集節點上安裝 卡巴斯基安全管理中心 Linux

在繼續之前，請確保您已完成情境：部署卡巴斯基容錯移轉叢集中的先前步驟。

該過程描述了如何在 卡巴斯基安全管理中心 Linux 容錯移轉叢集的節點上安裝 卡巴斯基安全管理中心 Linux。卡巴斯基安全管理中心 Linux 分別安裝在卡巴斯基安全管理中心 Linux 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。

根據裝置上安裝的 Linux 分發套件，您需要使用以下安裝檔案之一：

- ksc64_[version_number]_amd64.deb

- ksc64-[version_number].x86_64.rpm

您透過從 Kaspersky 網站下載來接收安裝檔案。

如果您使用 RED OS 7.3.4 或更新版本，或 MSVSPHERE 9.2 或更新版本，則需要在兩個節點上安裝 libxcrypt-compat 套件。

在主動節點上安裝

要在主動節點上安裝卡巴斯基安全管理中心 Linux，請執行以下操作：

1. 確保您要安裝卡巴斯基安全管理中心 Linux 網頁主控台的裝置執行支援的 Linux 版本。

2. 如果您使用次要網路介面卡，請在提示時輸入其名稱。您可以輸入下列指令顯示所有網路介面：

   ```
   ip addr
   ```

3. 執行卡巴斯基安全管理中心 Linux 安裝。根據您的 Linux 版本，執行以下命令之一：

   - `sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb`

   - `sudo yum install /<path>/ksc64-<version_number>.x86_64.rpm`

4. 執行 卡巴斯基安全管理中心 Linux 配置：

   ```
   /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. 閱讀 最終使用者產品授權協議 (EULA) 和隱私政策。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，當出現提示時，輸入以下值：

   a. 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）。若要使用卡巴斯基安全管理中心 Linux ，您必須接受 EULA 的條款。

   b. 若您瞭解並接受隱私權政策的條款，並同意您的資料將依照隱私權政策所述進行處理和傳輸（包括傳輸到第三國），請輸入 y。若您不接受隱私權政策的條款，請輸入 n。要使用卡巴斯基安全管理中心 Linux ，您必須接受隱私政策的條款。

6. 選擇**主叢集節點**作為管理伺服器安裝模式。

7. 出現提示時，指定以下設定：

   a. 輸入狀態共用掛接點的本機路徑：`/mnt/KlFocStateShare`

   b. 輸入資料共用掛接點的本機路徑：`/mnt/KlFocDataShare_klfoc`

   c. 選擇容錯移轉叢集連線模式：透過從屬網路介面卡或外部負載平衡器。

   d. 如果您使用從屬網路介面卡，請輸入其名稱。

   e. 輸入次要網路介面卡的 FQDN/IP 位址，或外部負載均衡器的 FQDN/IP 位址。

   f. 輸入管理伺服器 SSL 連接埠號。預設情況下使用連接埠 13000。

   g. 評估您打算管理的裝置的大致數量：

      - 如果您有 1 到 100 個受管理裝置，請輸入 1。

      - 如果您有 101 到 1000 個受管理裝置，請輸入 2。

      - 如果您有超過 1000 台受管理裝置，請輸入 3。

此設定用於自動隨機延遲工作啟動以最佳化網路負載。下面的清單顯示了計算延遲的間隔：

- 1 至 100 個受管理裝置，值 1。不使用延遲。
- 101 至 1000 個受管理裝置，值 2。延遲 5 分鐘。
- 超過 1000 個受管理裝置，價值 3。延遲 10 分鐘。

h. 輸入服務的安全群組名稱。預設情況下，使用 kladmins 群組。

i. 輸入帳戶名稱以啟動管理伺服器服務。該帳戶必須是輸入的安全群組的成員。預設情況下，使用“ksc”帳戶。

j. 輸入帳號名稱以啟動其他服務。該帳戶必須是輸入的安全群組的成員。預設情況下，使用“ksc”帳戶。

k. 選擇您安裝的與 卡巴斯基安全管理中心 Linux 一起使用的 DBMS：

- 如果您安裝了 MySQL 或 MariaDB，請輸入 1。
- 如果您安裝了 PostgreSQL 或 Postgres Pro，請輸入 2。

l. 輸入在其上安裝資料庫的裝置的 DNS 名稱或 IP 位址。

m. 輸入資料庫連接埠號。此連接埠用於與管理伺服器通信。預設情況下，使用以下連接埠：

- 連接埠 3306 用於 MySQL 或 MariaDB
- 連接埠 5432 用於 PostgreSQL 或 Postgres Pro

n. 輸入資料庫名稱。

o. 輸入用於存取資料庫的資料庫管理員帳戶的登入名稱。

p. 輸入用於存取資料庫的資料庫管理員帳戶的密碼。

q. 輸入 IAM 伺服器 FQDN。
您必須指定您在步驟7e中輸入的管理伺服器DNS名稱。

r. 輸入帳戶名稱以啟動 IAM 服務。該帳戶必須是輸入的安全群組的成員。預設情況下，使用“ksciam”帳戶。

s. 選取為與 IAM 服務搭配使用而安裝的 DBMS：

- 如果您安裝了 MySQL 或 MariaDB，請輸入 1。
- 如果您安裝了 PostgreSQL 或 Postgres Pro，請輸入 2。

t. 輸入IAM 服務要使用的 IAM DBMS 位址。

u. 輸入 IAM DBMS 連接埠號。此連接埠用於與 IAM 服務通訊。預設情況下，使用以下連接埠：

- 連接埠 3306 用於 MySQL 或 MariaDB
- 連接埠 5432 用於 PostgreSQL 或 Postgres Pro

v. 輸入IAM 服務要使用的 IAM 資料庫名稱。IAM 服務所使用的資料庫名稱應與管理伺服器所使用的資料庫名稱不同。

w. 輸入您用於存取 IAM 資料庫的資料庫帳戶的登入名稱。

x. 輸入您用於存取 IAM 資料庫的資料庫帳戶的密碼。

8. 等待服務自動新增並啟動：

- klfocsvc_klfoc
- kladminserver_klfoc
- klwebsrv_klfoc
- klactprx_klfoc
- klnagent_klfoc
- kliam_klfoc

9. 建立一個充當管理伺服器管理員的帳戶。輸入使用者名稱和密碼。使用者密碼不能少於 8 個或多於 256 個字元。

   如果您跳過此步驟，可以稍後透過執行下列命令來建立帳戶：

   `/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <密碼>`

使用者已新增，卡巴斯基安全管理中心 Linux 已安裝在主節點上。

在次要（被動）節點上安裝

要在次要節點上安裝卡巴斯基安全管理中心 Linux：

1. 確保您要安裝卡巴斯基安全管理中心 Linux 網頁主控台的裝置執行支援的 Linux 版本。

2. 執行卡巴斯基安全管理中心 Linux 安裝。根據您的 Linux 版本，執行以下命令之一：

   - `sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb`
   - `sudo yum install /<path>/ksc64-<version_number>.x86_64.rpm`

3. 執行 卡巴斯基安全管理中心 Linux 配置：

   `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`

4. 閱讀 最終使用者產品授權協議 (EULA) 和隱私政策。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，當出現提示時，輸入以下值：

   a. 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）。若要使用卡巴斯基安全管理中心 Linux ，您必須接受 EULA 的條款。

   b. 若您瞭解並接受隱私權政策的條款，並同意您的資料將依照隱私權政策所述進行處理和傳輸（包括傳輸到第三國），請輸入 y。若您不接受隱私權政策的條款，請輸入 n。要使用卡巴斯基安全管理中心 Linux ，您必須接受隱私政策的條款。

5. 選擇 **次要叢集節點**作為管理伺服器安裝模式。

6. 出現提示時，輸入狀態共用掛接點的本機路徑：`/mnt/KlFocStateShare`

   卡巴斯基安全管理中心 Linux 安裝在次要節點上。

服務驗證

使用下列命令驗證容錯移轉叢集管理服務是否處於`Active: active (running)`狀態：

```
systemctl status klfocsvc_klfoc
```

使用下列命令驗證其他容錯移轉叢集服務是否處於`Active: inactive (dead)`狀態：

- `systemctl status klnagent_klfoc`
- `systemctl status kladminserver_klfoc`
- `systemctl status klactprx_klfoc`
- `systemctl status klwebsrv_klfoc`
- `systemctl status kliam_klfoc`

現在，您可以測試卡巴斯基安全管理中心 Linux 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 Linux 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：

在主動節點上，執行下列指令之一：

- 若要停止叢集，請執行：`/opt/kaspersky/ksc64/sbin/klfoc -stopcluster --stp klfoc`
- 若要啟動叢集，請執行：`/opt/kaspersky/ksc64/sbin/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. 在主動節點上，使用`klfoc -stopcluster --stp klfoc`命令停止容錯移轉叢集。
2. 在您要維護的節點上，轉到 /opt/kaspersky/ksc64/sbin。

3. 開啟命令列，然後透過執行`detach_node.sh`命令將節點從叢集中分離。

4. 在主動節點上，使用`klfoc -startcluster --stp klfoc`命令啟動容錯移轉叢集。

5. 執行維護活動。

6. 在主動節點上，使用`klfoc -stopcluster --stp klfoc`命令停止容錯移轉叢集。

7. 在維護的節點上，轉到 /opt/kaspersky/ksc64/sbin。

8. 開啟命令列，然後透過執行`attach_node.sh`命令將節點附加到叢集。

9. 在主動節點上，使用`klfoc -startcluster --stp klfoc`命令啟動容錯移轉叢集。

10. 為了確保目前節點處於活動狀態，請執行下列命令檢查服務是否正在執行：

    `systemctl status klnagent_klfoc.service`

    `systemctl status kladminserver_klfoc.service`

    `systemctl status klactprx_klfoc.service`

    `systemctl status klwebsrv_klfoc.service`

    `systemctl status kliam_klfoc.service`

    這些服務在主動節點上執行，而不是在被動節點上執行。

該節點得到維護並被附著到容錯移轉叢集。

重新安裝容錯移轉叢集節點

若要重新安裝容錯移轉叢集節點：

1. 建立管理伺服器的備份。

2. 將主動節點切換到維護模式。

3. 如果需要保留目前作業系統，請執行以下步驟。
   如果要取代裝置或作業系統，請跳過此步驟。

   a. 要停止容錯移轉叢集，請執行以下命令：
   `klfoc -stopcluster --stp klfoc`

   b. 要強制停止容錯移轉叢集服務，請執行以下命令：
   `sudo systemctl stop klfocsvc_klfoc`
   `systemctl status kl*klfoc*`

   c. 要取消掛載容錯移轉叢集目錄，請執行以下命令：
   `sudo umount /mnt/KlFocDataShare_klfoc`
   `sudo umount /mnt/KlFocStateShare`

   d. 要解除安裝卡巴斯基安全管理中心 Linux，請根據 Linux 分發套件執行以下任一命令：

   - `sudo dpkg --remove ksc64`

或

- `sudo yum remove ksc64`

e. 針對被動節點執行下列說明中的所有步驟：

1. 為卡巴斯基安全管理中心 Linux 容錯移轉叢集準備節點。

2. 在卡巴斯基安全管理中心 Linux 容錯移轉叢集節點上安裝卡巴斯基安全管理中心 Linux。

4. 結束維護模式。請從手動啟動和停止叢集節點說明的步驟 6（停止容錯移轉叢集）繼續操作。

安裝連線到安裝在 卡巴斯基安全管理中心 Linux 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 Linux 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，在卡巴斯基安全管理中心 Linux 容錯移轉叢集節點上安裝資料庫管理系統和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網頁主控台不支援在叢集節點上進行安裝。我們建議在單獨的伺服器上安裝卡巴斯基安全管理中心網頁主控台。

要安裝連線到安裝在卡巴斯基安全管理中心 Linux 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的步驟 1 和步驟 2。

2. 在第 3 步，在回應檔案中指定 `trusted` 安裝參數，以允許卡巴斯基安全管理中心網頁主控台連線到卡巴斯基安全管理中心 Linux 容錯移轉叢集。

   `trusted` **安裝參數**的元件

   如果您透過單一登入進行網域身分驗證，從而連線到卡巴斯基安全管理中心 Linux 容錯移轉叢集，請按如下方式指定 trusted 安裝參數：如果您將卡巴斯基安全管理中心網頁主控台連線到管理伺服器版本 16 或更新版本，則將使用身分和存取管理器 (IAM) 透過單一登入 (SSO) 進行網域身分驗證。在這種情況下，請按如下方式指定 `trusted` 安裝參數：

```
"trusted":  {
  "<管理伺服器名稱>": {
    "iamHost": "ksc-iam.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "<共用資料資料夾>/iam/main_certificate.pem",
    "iamPATPath": "<共用資料資料夾>/iam/initial_token.txt",
    "kscPort": 13299,
    "kscCertPath": "<共用資料夾>/1093/cert/klserver.cer"
  }
}
```

其中：

- < 管理伺服器名稱 > 是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卡巴斯基安全管理中心 Linux 容錯移轉叢集名稱。

- `iamHost` 是安裝管理伺服器和 IAM 的裝置的位址。如果您在準備叢集節點時建立了次要網路介面卡，請使用該介面卡的 FQDN 或主機名稱作為卡巴斯基安全管理中心 Linux 容錯移轉叢集位址。否則，請指定所使用協力廠商負載均衡器的 FQDN 或主機名稱。

  `iamHost` 值必須與安裝管理伺服器時指定的 IAM 位址相符。若要取得指定的 IAM 位址，請在管理伺服器主機上執行下列命令：

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

- `iamOAuthPort` 是用於透過 OpenID Connect 身分驗證協定交換身分驗證權杖的連接埠（預設值為 4444）。此連接埠同時用於卡巴斯基安全管理中心網頁主控台伺服器與管理伺服器之間的通訊，以及瀏覽器（與卡巴斯基安全管理中心網頁主控台搭配使用）與管理伺服器之間的通訊。

- `iamProxyPort` 是用於將卡巴斯基安全管理中心網頁主控台伺服器連線到管理伺服器的連接埠（預設值為 9050）。

- `iamCertPath` 是 IAM 憑證的路徑。IAM 憑證會在首次執行管理伺服器時自動建立。憑證位於安裝管理伺服器的裝置上。憑證的預設路徑為：< 共用資料夾 >`/iam/main_certificate.pem`。憑證位於卡巴斯基安全管理中心 Linux 容錯移轉叢集中。自簽章 IAM 憑證會自動輪換。

- `iamPATPath` 是用於將卡巴斯基安全管理中心網頁主控台註冊為 IAM 中的 OAuth 用戶端的權杖路徑。此檔案會在首次執行管理伺服器時產生。權杖位於安裝管理伺服器的裝置上。權杖的預設路徑：<共用資料夾 >/iam/initial_token.txt。權杖位於卡巴斯基安全管理中心 Linux 容錯移轉叢集的共用資料儲存中。權杖永久有效，無需輪換。

- `kscPort` 是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）。

- `kscCertPath` 是位於卡巴斯基安全管理中心 Linux 容錯移轉叢集的共用資料儲存中的管理伺服器憑證。憑證檔案的預設路徑為：< 共用資料夾 >`\1093\cert\klserver.cer`。

  > 將管理伺服器憑證檔案（由 `kscCertPath` 指定）、IAM 憑證檔案（由 `iamCertPath` 指定）和權杖檔案（由 `iamPATPath` 指定）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。

如果將卡巴斯基安全管理中心網頁主控台連線到管理伺服器版本 15.4 或更早版本，則將透過指定網域使用者或內部使用者的名稱和密碼進行身分驗證。在這種情況下，請按如下方式指定 trusted 安裝參數：

```
"trusted":  {
  "<管理伺服器名稱>": {
    "kscHost": "ksc.example.com",
    "kscPort": 13299,
    "kscCertPath": "<共用資料夾>/1093/cert/klserver.cer"
  }
}
```

其中：

- < 管理伺服器名稱 > 是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卡巴斯基安全管理中心 Linux 容錯移轉叢集名稱。
- `kscHost` 是管理伺服器位址（FQDN 或主機名稱）。如果您在準備叢集節點時建立了次要網路介面卡，請使用介面卡的位址作為卡巴斯基安全管理中心 Linux 容錯移轉叢集位址。否則，請指定所使用協力廠商負載均衡器的位址。
- `kscPort` 是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）。
- `kscCertPath` 是位於卡巴斯基安全管理中心 Linux 容錯移轉叢集的共用資料儲存中的管理伺服器憑證。憑證檔案的預設路徑為：< 共用資料夾 >`\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. 繼續卡巴斯基安全管理中心網頁主控台的標準安裝。

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。

異地分散式Kaspersky Security Center for Linux故障轉移叢集

本章節包含有關異地分散式Kaspersky Security Center for Linux故障轉移叢集的一般資訊，以及針對以下組態在網路中準備和部署異地分散式故障轉移叢集的說明：

- 使用PostgreSQL DBMS執行Ubuntu的叢集節點
- 使用Platform V Pangolin DBMS執行SberLinux的叢集節點

使用PostgreSQL DBMS執行Ubuntu的異地分散式叢集

依照此方案，您可以準備基礎設施並部署異地分散式Kaspersky Security Center for Linux故障轉移叢集。

先決條件

- 部署具有運行狀況檢查功能的高可用性DNS負載平衡器。
- 確保主動和被動群集節點是兩個具有相同硬體和軟體組態的裝置。
  - 硬體需求：
    - CPU—16核心，2500 MHz
    - RAM：32GB。
    - 磁碟空間 - 500GB，300 IOPS或更高
    - 網路介面控制器 - 1 Gbps

- 軟體需求：
  - 作業系統：Ubuntu Server 24.04 LTS（Noble Numbat）64 位元
  - DBMS：PostgreSQL 17 64 位元

階段

部署在單個資料中心內的Kaspersky Security Center for Linux故障轉移叢集無法升級到異地分散式故障轉移叢集。

異地分散式Kaspersky Security Center for Linux故障轉移叢集的部署分階段進行：

1. **準備故障轉移叢集節點的檔案系統**

   在兩個叢集節點上準備檔案系統。準備工作包括建立LVM邏輯磁碟區並將目錄設定為掛載點。

2. **設定複製叢集檔案系統**

   安裝DRBD公用程式並設定DRBD資源，以便在故障轉移叢集節點之間進行資料複製。之後，在活動叢集節點上建立複製檔案系統。

3. **在故障轉移叢集節點上安裝和設定Corosync和Pacemaker**

   安裝Corosync和Pacemaker以提供叢集通訊和資源管理，從而實現高可用性。

4. **安裝和設定PostgreSQL DBMS**

   在叢集節點上安裝並設定PostgreSQL。

5. **在故障轉移叢集節點上安裝Kaspersky Security Center for Linux**

   在叢集節點上安裝Kaspersky Security Center for Linux ，然後在叢集節點之間設定加密。

6. **在故障轉移叢集節點上安裝卡巴斯基安全管理中心網頁主控台**

   在兩個故障轉移叢集節點上安裝卡巴斯基安全管理中心網頁主控台，從而實現高可用性。

準備叢集節點的檔案系統

作為部署異地分散式Kaspersky Security Center Linux故障轉移叢集的第一步，您必須在兩個叢集節點上設定檔案系統。準備工作包括建立LVM邏輯磁碟區並將目錄設定為掛載點。在兩個叢集節點上執行下列步驟。

若要準備叢集節點的檔案系統：

1. 為管理伺服器資料和資料庫建立LVM邏輯磁碟區：

   ```
   lvcreate -L <volume size> -n klfocdata <volume group name>
   ```

   建立一個單獨的LVM邏輯磁碟區來儲存應答檔案：

   ```
   lvcreate -L <volume size> -n klfocstate <volume group name>
   ```

其中：

- `volume group name`是LVM使用的磁碟區群組名稱。
- `klfocdata`和`klfocstate`是邏輯磁碟區名稱。這些邏輯磁碟區是在磁碟區群組內建立的。

  為了保持一致性，我們建議使用這些磁碟區名稱，不過如果需要，您可以指定自訂名稱。
- `volume size`為磁碟區大小。我們建議為管理伺服器資料和資料庫分配至少500GB的空間。儲存應答檔案的磁碟區只需要少量空間。

2. 建立用作邏輯磁碟區掛載點的目錄。
   - 對於管理伺服器資料和資料庫：

     ```
     mkdir -p /mnt/KlFocDataShare_klfoc
     ```
   - 對於應答檔案：

     ```
     mkdir -p /mnt/KlFocStateShare_klfoc
     ```

我們建議使用`/mnt/KlFocDataShare_klfoc`和`/mnt/KlFocStateShare_klfoc`目錄來保持一致性，不過如果需要，您可以指定自訂名稱。

叢集節點的檔案系統隨即準備就緒。之後，您需要設定複製的叢集檔案系統。

設定複製叢集檔案系統

安裝和設定DRBD

*DRBD*是一款用於複製資料的第三方軟體（專門用於上一步中準備的資料磁碟區和掛載點）。

在準備好叢集節點的檔案系統後，您必須安裝DRBD公用程式並設定DRBD資源，以便在叢集節點之間複製資料。在兩個叢集節點上執行下列步驟。

若要在叢集節點上安裝和設定DRBD：

1. 安裝DRBD公用程式：

   ```
   apt update
   apt install -y drbd-utils
   ```

   我們建議使用DRBD 9.2.6或更高版本，因為它提供了內建的流量加密功能。

   DRBD 流量也可以使用您自己的 VPN 解決方案進行加密。

2. 為檔案系統準備期間建立的每個邏輯磁碟區建立DRBD資源組態檔（`klfocdata`和`klfocstate`）。

   所有組態檔必須放置在`/etc/drbd.d/`中。

   - 資源`klfocdata`（管理伺服器資料和資料庫）

     對klfocdata資源使用非同步複製（協定A）。根據您的環境設定所有其他參數。

組態檔範例

```
resource klfocdata {
    protocol A;
    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }
    syncer {
        rate 110M;
    }
    # Hostname of the active node
    on db1 {
        device    /dev/drbd0;
        disk      /dev/<volume group name>/klfocdata;
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd0;
        disk      /dev/<volume group name>/klfocdata;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

- 資源`klfocstate`（應答檔案）

  使用同步複製（協定C）建立klfocstate資源。根據您的環境設定所有其他參數。

  組態檔範例

```
resource klfocstate {
    protocol C;
    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }
    syncer {
        rate 110M;
    }
    # Hostname of the active node
    on db1 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

3. Initialize DRBD metadata for both resources:

```
drbdadm create-md klfocdata
drbdadm create-md klfocstate
```

4. 在所有已設定的資源上啟動 DRBD：

```
drbdadm up all
```

DRBD隨即在兩個叢集節點上安裝和設定。

在活動叢集節點上建立複製檔案系統

在兩個叢集節點上安裝並設定DRBD後，在活動叢集節點上建立複製檔案系統。在活動叢集節點上執行下列步驟。

在活動叢集節點上建立複製檔案系統：

1. 將兩個DRBD資源都提升為主要角色：

```
drbdadm primary --force klfocdata
drbdadm primary --force klfocstate
```

2. 格式化DRBD裝置，以準備複製的磁碟區，以便用於叢集節點：

```
mkfs.ext4 /dev/drbd0
mkfs.ext4 /dev/drbd2
```

3. 設定檔案系統參數：

```
tune2fs -m 0 /dev/drbd0
tune2fs -m 0 /dev/drbd2
```

4. 將DRBD裝置掛載到先前建立的目錄：

```
mount -o noatime /dev/drbd0 /mnt/KlFocDataShare_klfoc
mount -o noatime /dev/drbd2 /mnt/KlFocStateShare_klfoc
```

如果安裝了multipathd服務，則必須在兩個叢集節點上將其設定為忽略裝置`/dev/drbd*`。

5. 驗證複製狀態：

```
drbdadm status
```

正確的檔案系統組態輸出：

```
klfocdata role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate
klfocstate role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate
```

複製檔案系統隨即在活動叢集節點上設定。之後，您必須在叢集節點上安裝和設定 Corosync 和 Pacemaker。

在叢集節點上使用安裝程式安裝和設定Corosync和Pacemaker

Corosync和Pacemaker提供叢集通訊和資源管理，以實現高可用性。它們確保在發生故障時服務自動遷移到正常運行的節點，從而最大限度地減少停機時間。

若要在叢集節點上安裝和設定Corosync和Pacemaker：

1. 在兩個叢集節點上，安裝所需的軟體套件：

```
sudo apt install pacemaker -y
sudo apt install crmsh -y
sudo apt install resource-agent-extra -y
```

2. 根據官方說明文件，在兩個叢集節點上設定Corosync和Pacemaker。這包括啟用自動啟動、產生和分發身份驗證金鑰，以及設定身份驗證金鑰檔案的存取權限。

   為確保設定正確，請在叢集節點之一上執行下列命令：

```
crm status
```

   預期輸出應顯示叢集狀態並列出所有活動節點，以確認Corosync運作正常且節點之間通訊正常。

3. 在兩個叢集節點上，配置Pacemaker叢集的基本設定：

```
crm configure property stonith-enabled="false"
crm configure property symmetric-cluster="false"
crm configure rsc_defaults resource-stickiness="110"
crm configure rsc_defaults migration-threshold=3
crm configure property no-quorum-policy=ignore
```

4. 在兩個叢集節點上，停用由Corosync管理的指令碼的啟動：

```
systemctl disable drbd.service
```

5. 在其中一個叢集節點上，在 Pacemaker 中建立 DRBD 資源。

   - DRBD resource for klfocdata

     a. 為DRBD磁碟區`klfocdata`建立叢集資源，使叢集能夠管理其狀態並自動監控其運行狀況：

```
crm configure primitive drbd_klfocdata ocf:linbit:drbd params drbd_resource="klfocdata" \
op monitor interval="60s" op start interval="0" timeout="240s" op stop interval="0" \
timeout="240s" op monitor role=Master interval="10s" op monitor role=Slave interval="30s"
```

     b. 根據建立的資源`drbd_klfocdata`建立叢集管理資源`ms_drbd_klfocdata`：

```
crm configure ms ms_drbd_klfocdata drbd_klfocdata meta master-max="1" master-node-max="1" \
clone-max="2" clone-node-max="1" notify="true"
```

     c. 為DRBD磁碟區`fs_klfocdata`建立掛載點，指定裝置、目標目錄、檔案系統類型和掛載選項：

```
crm configure primitive fs_klfocdata ocf:heartbeat:Filesystem params device="/dev/drbd0" \
directory="/mnt/KlFocDataShare_klfoc" fstype="ext4" options="data=journal"
```

- DRBD resource for klfocstate

  a. 為DRBD磁碟區`klfocstate`建立叢集資源，使群集能夠管理其狀態並自動監控其執行狀況：

  ```
  crm configure primitive drbd_klfocstate ocf:linbit:drbd params drbd_resource="klfocstate" \
  op monitor interval="60s" op start interval="0" timeout="240s" op stop interval="0" \
  timeout="240s" op monitor role=Master interval="10s" op monitor role=Slave interval="30s"
  ```

  b. 根據建立的資源`drbd_klfocstate`建立一個由叢集管理的資源ms_drbd_klfocstate：

  ```
  crm configure ms ms_drbd_klfocstate drbd_klfocstate meta master-max="1" master-node-max="1" \
  clone-max="2" clone-node-max="1" notify="true"
  ```

  c. 為DRBD磁碟區`fs_klfocstate`建立掛載點，指定裝置、目標目錄、檔案系統類型和掛載選項：

  ```
  crm configure primitive fs_klfocstate ocf:heartbeat:Filesystem params device="/dev/drbd2" \
  directory="/mnt/KlFocStateShare_klfoc" fstype="ext4" options="noatime"
  ```

6. 在兩個叢集節點上，停用DRBD服務的自動啟動：

   ```
   systemctl disable drbd.service
   ```

   Corosync和Pacemaker隨即在叢集節點上安裝並設定完成。之後，您必須安裝DBMS並建立管理伺服器資料庫和IAM資料庫。

安裝和設定PostgreSQL DBMS

在叢集節點上安裝並設定Corosync和Pacemaker後，您必須在兩個叢集節點上安裝DBMS。

若要安裝和設定DBMS：

1. 在兩個叢集節點上，安裝PostgreSQL 17 x64或更高版本。

   有關如何安裝PostgreSQL的資訊，請參閱其說明文件。

2. 確保安裝了 DBMS 的叢集節點沒有具有以下名稱的 DBMS 使用者帳戶：

   - client
   - iam
   - ksc
   - locker
   - pat
   - scope
   - voltron

3. 在兩個叢集節點上，停止DBMS，然後停用DBMS服務的自動啟動：

```
sudo systemctl stop postgresql
sudo systemctl disable postgresql
```

4. 在活動叢集節點上，將DBMS目錄複製到`/mnt/KlFocDataShare_klfoc/dbms`目錄：

```
rsync -av /var/lib/postgresql/17/main/ /mnt/KlFocDataShare_klfoc/dbms
mv /var/lib/postgresql/17/main /var/lib/postgresql/17/main.bk
```

5. 在活動叢集節點上，將PostgreSQL設定檔複製到`/mnt/KlFocDataShare_klfoc/dbms`目錄：

```
sudo cp /etc/postgresql/17/main/pg_hba.conf /mnt/KlFocDataShare_klfoc/dbms
sudo cp /etc/postgresql/17/main/pg_ident.conf /mnt/KlFocDataShare_klfoc/dbms
```

6. 在兩個叢集節點上，開啟組態檔`/etc/postgresql/17/main/postgresql.conf`，然後將目錄`/mnt/KlFocDataShare_klfoc/dbms`設定為資料庫資料目錄。

   同時指定設定檔路徑（`/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf`和`/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf`），並移除`include_dir`參數：

```
data_directory = '/mnt/KlFocDataShare_klfoc/dbms'
hba_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf'
ident_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf'
listen_addresses = '*'
```

7. 在組態檔`/etc/postgresql/17/main/postgresql.conf`，調整DBMS組態以滿足Kaspersky Security Center for Linux的需求。

8. 建立 PostgreSQL 服務資源：

```
crm configure primitive klfocsvc_dbms ocf:heartbeat:pgsql \
params pgctl="/usr/lib/postgresql/17/bin/pg_ctl" \
psql="/usr/bin/psql" \
pgdata="/mnt/KlFocDataShare_klfoc/dbms" \
config="/etc/postgresql/17/main/postgresql.conf" \
sudo cp /etc/postgresql/17/main/pg_hba.conf /mnt/KlFocDataShare_klfoc/dbms
op start timeout=60s \
op stop timeout=60s \
op monitor interval=30s timeout=60s
```

9. 將PostgreSQL資源新增到`group_klfoc`叢集群組：

```
crm configure edit klfoc_group
```

10. 在清單末尾新增PostgreSQL資源名稱`klfocsvc_dbms`，例如：

```
group klfoc_group {
...
klfocsvc_dbms
}
```

11. 在活動叢集節點上，在DBMS伺服器上，為IAM建立一個資料庫。 資料庫名稱必須與您安裝的資料庫不同，以便與Kaspersky Security Center for Linux配合使用。解除安裝或將伺服器移動到其他裝置時，管理伺服器不會自動刪除IAM資料庫，您必須手動刪除資料庫：

```
sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
```

DBMS隨即安裝和設定完成。管理伺服器資料庫和IAM資料庫隨即建立。之後，您需要在叢集節點上安裝Kaspersky Security Center for Linux。

在異地分散式故障轉移叢集節點上安裝卡巴斯基安全管理中心 Linux

卡巴斯基安全管理中心 Linux 是透過使用應答檔案以靜默模式安裝在異地分散式故障轉移叢集節點上的，即無需使用者操作。回應檔案包含一組自訂安裝參數：變數及其各自的值。

先決條件：

- 完成所有準備步驟：
  - 準備叢集節點的檔案系統
  - 設定複製叢集檔案系統
  - 在叢集節點上使用安裝程式安裝和設定Corosync和Pacemaker
  - 安裝和設定PostgreSQL DBMS
- 確保叢集節點執行 Ubuntu Server 24.04 LTS (Noble Numbat) x64。
- 從卡巴斯基網站下載安裝檔案 `ksc64_[version_number]_amd64.deb`。

在主動節點上安裝

若要在活動節點上以靜默模式安裝Kaspersky Security Center for Linux：

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，才遵循以下步驟操作。
2. 建立群組 `kladmins` 和非授權帳戶 `ksc` 與 `ksciam`，這兩個帳戶必須是 `kladmins` 群組成員。為此，請在具有 root 權限的帳戶下依次執行以下命令：

```
adduser ksc
groupadd kladmins
gpasswd -a ksc kladmins
usermod -g kladmins ksc
adduser ksciam
gpasswd -a ksciam kladmins
usermod -g kladmins ksciam
```

3. 在目錄 `/mnt/KlFocDataShare_klfoc/` 中，建立一個目錄，用於存放Kaspersky Security Center for Linux檔案：

```
mkdir /mnt/KlFocDataShare_klfoc/ksc/
```

4. 建立回應檔案（TXT 格式），並以 VARIABLE_NAME=variable_value 格式將變數清單新增到回應檔案，每行一個變數。

在靜默模式下安裝Kaspersky Security Center for Linux的參數清單中，指定異地分散式叢集部署所需的以下參數：

- `KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT=2`

  設定值`2`，以部署異地分散式叢集。

- `KLSRV_UNATT_SERVERADDRESS=<DNS balancer address>`和`KLSRV_UNATT_IAM_ADDRESS=<DNS balancer address>`

  必須已經部署了包含運行狀況檢查功能的DNS負載平衡器。這些參數的值必須相同，並且設定為DNS負載平衡器的FQDN。

5. 使用下列命令，在包含回應檔案全名的 root 或使用者環境中設定`KLAUTOANSWERS`環境變數之值（包含路徑）：

```
export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
```

6. 執行以下命令，以靜默模式啟動Kaspersky Security Center for Linux安裝程式：

   - 在根環境中：

```
apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

   - 在使用者環境中：

```
sudo -E apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

7. 停用klfocsvc_klfoc.service服務的自動啟動：

```
systemctl disable klfocsvc_klfoc.service
```

8. 安裝完Kaspersky Security Center for Linux後，停止活動的叢集節點。

9. 將所有叢集資源移至被動節點。

   您可以使用該命令`crm node standby`（並透過`crm node online`將其還原）。

在被動節點上安裝

若要在被動節點上安裝Kaspersky Security Center for Linux：

1. 執行卡巴斯基安全管理中心 Linux 安裝：

```
sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb
```

2. 執行 卡巴斯基安全管理中心 Linux 配置：

```
/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

3. 閱讀 最終使用者產品授權協議 (EULA) 和隱私政策。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，當出現提示時，輸入以下值：

   - 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）。若要使用卡巴斯基安全管理中心 Linux ，您必須接受 EULA 的條款。

   - 輸入`y`，如果您理解並接受隱私政策的條款，並且您同意您的資料將按照隱私政策中的說明進行處理和傳輸（包括傳輸到第三國）。輸入 n（如果您不接受隱私政策的條款）。要使用卡巴斯基安全管理中心 Linux ，您必須接受隱私政策的條款。

4. 將被動叢集節點選為管理伺服器安裝模式。

5. 出現提示時，輸入狀態共用掛接點的本機路徑：`/mnt/KlFocStateShare_klfoc`。

6. 停用klfocsvc_klfoc.service服務的自動啟動：

```
systemctl disable klfocsvc_klfoc.service
```

7. 建立`klfocsvc_klfoc`服務資源：

```
crm configure primitive klfocsvc_klfoc systemd:klfocsvc_klfoc \
op start timeout="900s" interval="0" \
op stop timeout="900s" interval="0" \
op monitor interval="30s" timeout="90s"
```

8. 將`klfocsvc_klfoc`資源新增至`group_klfoc`群組：

```
crm configure edit klfoc_group
```

9. 在群組末尾新增行`klfocsvc_klfoc`，例如：

```
group klfoc_group {
...
klfocsvc_klfoc
}
```

10. 驗證活動節點上的所有資源是否都處於啟動狀態。

```
crm status
```

在叢集節點之間設定加密

若要在叢集節點之間設定加密，

若在設定複製叢集檔案系統期間安裝了DRBD 9.2.6或更高版本，請根據DRBD官方說明文件在叢集節點之間設定加密。

或者，您可以使用自己的VPN解決方案加密叢集節點之間的流量。

異地分散式Kaspersky Security Center for Linux容錯移轉叢集隨即安裝。之後，您必須在兩個叢集節點上都安裝卡巴斯基安全管理中心網頁主控台 。

使用Platform V Pangolin DBMS執行SberLinux的異地分散式叢集

依照此方案，您可以準備基礎設施並部署異地分散式Kaspersky Security Center for Linux故障轉移叢集。

先決條件

- 部署具有運行狀況檢查功能的高可用性DNS負載平衡器。
- 確保主動和被動群集節點是兩個具有相同硬體和軟體組態的裝置。
  - 硬體需求：
    - CPU—16核心，2500 MHz
    - RAM：32GB。
    - 磁碟空間 - 500GB，300 IOPS或更高
    - 網路介面控制器 - 1 Gbps
  - 軟體需求：
    - 作業系統：Platform V SberLinux OS Server (SLO) 9.5.1 64 位元
    - DBMS: Platform V Pangolin 6.5.1 64 位元

階段

> 部署在單個資料中心內的Kaspersky Security Center for Linux故障轉移叢集無法升級到異地分散式故障轉移叢集。

異地分散式Kaspersky Security Center for Linux故障轉移叢集的部署分階段進行：

1. **準備故障轉移叢集節點的檔案系統**

   在兩個叢集節點上準備檔案系統。準備工作包括建立LVM邏輯磁碟區並將目錄設定為掛載點。

2. **設定複製叢集檔案系統**

   安裝DRBD公用程式並設定DRBD資源，以便在故障轉移叢集節點之間進行資料複製。之後，在活動叢集節點上建立複製檔案系統。

3. **在故障轉移叢集節點上安裝和設定Corosync和Pacemaker**

   安裝Corosync和Pacemaker以提供叢集通訊和資源管理，從而實現高可用性。

4. **安裝與設定Platform V Pangolin DBMS**

   在叢集節點上安裝和設定Platform V Pangolin。

5. **在故障轉移叢集節點上安裝Kaspersky Security Center for Linux**

   在叢集節點上安裝Kaspersky Security Center for Linux ，然後在叢集節點之間設定加密。

6 **在故障轉移叢集節點上安裝卡巴斯基安全管理中心網頁主控台**

在兩個故障轉移叢集節點上安裝卡巴斯基安全管理中心網頁主控台，從而實現高可用性。

準備叢集節點的檔案系統

作為部署異地分散式Kaspersky Security Center Linux故障轉移叢集的第一步，您必須在兩個叢集節點上設定檔案系統。準備工作包括建立LVM邏輯磁碟區並將目錄設定為掛載點。在兩個叢集節點上執行下列步驟。

若要準備叢集節點的檔案系統：

1. 為管理伺服器資料和資料庫建立LVM邏輯磁碟區：

   ```
   lvcreate -L <volume size> -n klfocdata <volume group name>
   ```

   建立一個單獨的LVM邏輯磁碟區來儲存應答檔案：

   ```
   lvcreate -L <volume size> -n klfocstate <volume group name>
   ```

   其中：

   - `volume group name`是LVM使用的磁碟區群組名稱。
   - `klfocdata`和`klfocstate`是邏輯磁碟區名稱。這些邏輯磁碟區是在磁碟區群組內建立的。

     為了保持一致性，我們建議使用這些磁碟區名稱，不過如果需要，您可以指定自訂名稱。
   - `volume size`為磁碟區大小。我們建議為管理伺服器資料和資料庫分配至少500GB的空間。儲存應答檔案的磁碟區只需要少量空間。

2. 建立用作邏輯磁碟區掛載點的目錄。

   - 對於管理伺服器資料和資料庫：

     ```
     mkdir -p /mnt/KlFocDataShare_klfoc
     ```

   - 對於應答檔案：

     ```
     mkdir -p /mnt/KlFocStateShare_klfoc
     ```

   我們建議使用`/mnt/KlFocDataShare_klfoc`和`/mnt/KlFocStateShare_klfoc`目錄來保持一致性，不過如果需要，您可以指定自訂名稱。

叢集節點的檔案系統隨即準備就緒。之後，您需要設定複製的叢集檔案系統。

設定複製叢集檔案系統

安裝和設定DRBD

*DRBD*是一款用於複製資料的第三方軟體（專門用於上一步中準備的資料磁碟區和掛載點）。

在準備好叢集節點的檔案系統後，您必須安裝DRBD公用程式並設定DRBD資源，以便在叢集節點之間複製資料。在兩個叢集節點上執行下列步驟。

若要在叢集節點上安裝和設定DRBD：

1. 如下安裝DRBD公用程式：

   a. 在兩個節點上啟用EPEL和ELRepo儲存庫：

   ```
   dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
   dnf install https://www.elrepo.org/elrepo-release-9.el9.elrepo.noarch.rpm
   ```

   b. 輸出kmod-drbd9x軟體套件的所有可用版本，並篩選為el9_6平台構建的軟體套件清單（例如，使用Platform V SberLinux OS Server (SLO) 9.6）：

   ```
   dnf search --showduplicates kmod-drbd9x | grep el9_6
   ```

   c. 從兩個節點的清單中安裝最新的可用版本。Platform V SberLinux OS Server (SLO) 9.6範例：

   ```
   dnf install kmod-drbd9x-9.2.14-1.el9_6.elrepo.x86_64
   dnf install drbd drbd-utils drbd-udev drbd-pacemaker drbd-selinux
   modprobe drbd
   ```

   如果將來出現更新版本，請相應地替換版本字串。

   我們建議使用DRBD 9.2.6或更高版本，因為它提供了內建的流量加密功能。
   DRBD 流量也可以使用您自己的 VPN 解決方案進行加密。

2. 為檔案系統準備期間建立的每個邏輯磁碟區建立DRBD資源組態檔（`klfocdata`和`klfocstate`）。
   所有組態檔必須放置在`/etc/drbd.d/`中。

   - 資源`klfocdata`（管理伺服器資料和資料庫）
     對klfocdata資源使用非同步複製（協定A）。根據您的環境設定所有其他參數。
     組態檔範例

     ```
     resource klfocdata {
         protocol A;
         net {
             after-sb-0pri    discard-least-changes;
             after-sb-1pri    call-pri-lost-after-sb;
             after-sb-2pri    call-pri-lost-after-sb;
         }
         syncer {
             rate 110M;
         }
         # Hostname of the active node
         on db1 {
             device    /dev/drbd0;
             disk      /dev/<volume group name>/klfocdata;
             address   <disk IP address>;
             meta-disk internal;
         }
         # Hostname of the passive node
         on db2 {
             device    /dev/drbd0;
             disk      /dev/<volume group name>/klfocdata;
             address   <disk IP address>;
             meta-disk internal;
         }
     }
     ```

   - 資源`klfocstate`（應答檔案）

使用同步複製（協定C）建立klfocstate資源。根據您的環境設定所有其他參數。

組態檔範例

```
resource klfocstate {
    protocol C;
    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }
    syncer {
        rate 110M;
    }
    # Hostname of the active node
    on db1 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

3. Initialize DRBD metadata for both resources:

```
drbdadm create-md klfocdata
drbdadm create-md klfocstate
```

4. 在所有已設定的資源上啟動 DRBD：

```
drbdadm up all
```

DRBD隨即在兩個叢集節點上安裝和設定。

在活動叢集節點上建立複製檔案系統

在兩個叢集節點上安裝並設定DRBD後，在活動叢集節點上建立複製檔案系統。在活動叢集節點上執行下列步驟。

在活動叢集節點上建立複製檔案系統：

1. 將兩個DRBD資源都提升為主要角色：

```
drbdadm primary --force klfocdata
drbdadm primary --force klfocstate
```

2. 格式化DRBD裝置，以準備複製的磁碟區，以便用於叢集節點：

```
mkfs.ext4 /dev/drbd0
mkfs.ext4 /dev/drbd2
```

3. 設定檔案系統參數：

```
tune2fs -m 0 /dev/drbd0
tune2fs -m 0 /dev/drbd2
```

4. 將DRBD裝置掛載到先前建立的目錄：

```
mount -o noatime /dev/drbd0 /mnt/KlFocDataShare_klfoc
mount -o noatime /dev/drbd2 /mnt/KlFocStateShare_klfoc
```

如果安裝了multipathd服務，則必須在兩個叢集節點上將其設定為忽略裝置`/dev/drbd*`。

5. 驗證複製狀態：

```
drbdadm status
```

正確的檔案系統組態輸出：

```
klfocdata role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate
klfocstate role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate
```

複製檔案系統隨即在活動叢集節點上設定。之後，您必須在叢集節點上安裝和設定 Corosync 和 Pacemaker。

在叢集節點上使用安裝程式安裝和設定Corosync和Pacemaker

Corosync和Pacemaker提供叢集通訊和資源管理，以實現高可用性。它們確保在發生故障時服務自動遷移到正常運行的節點，從而最大限度地減少停機時間。

若要在叢集節點上安裝和設定Corosync和Pacemaker：

1. 在兩個叢集節點上，安裝所需的軟體套件：

```
dnf install pcs
dnf install drbd-pacemaker
```

2. 根據官方說明文件，在兩個叢集節點上設定Corosync和Pacemaker。這包括啟用自動啟動、產生和分發身份驗證金鑰，以及設定身份驗證金鑰檔案的存取權限。

   為確保設定正確，請在叢集節點之一上執行下列命令：

```
crm status
```

預期輸出應顯示叢集狀態並列出所有活動節點，以確認Corosync運作正常且節點之間通訊正常。

3. 在兩個叢集節點上，配置Pacemaker叢集的基本設定：

```
pcs property set stonith-enabled=false
pcs property set symmetric-cluster=false
pcs resource defaults resource-stickiness=110
pcs resource defaults migration-threshold=3
pcs property set no-quorum-policy=ignore
```

4. 在兩個叢集節點上，停用由Corosync管理的指令碼的啟動：

```
systemctl disable drbd.service
```

5. 在其中一個叢集節點上，在 Pacemaker 中建立 DRBD 資源。

- DRBD resource for klfocdata

  a. 為DRBD磁碟區`klfocdata`建立叢集資源，使叢集能夠管理其狀態並自動監控其運行狀況：

  ```
  pcs resource create drbd_klfocdata ocf:linbit:drbd \
  drbd_resource="klfocdata" \
  op monitor interval=60s \
  op start interval=0 timeout=240s \
  op monitor interval=60s \
  op monitor role=Master interval=10s \
  op monitor role=Slave interval=30s \
  ```

  b. 根據建立的資源`drbd_klfocdata`建立叢集管理資源`ms_drbd_klfocdata`：

  ```
  pcs resource clone drbd_klfocdata promotable=true
  master-max=1
  clone-max=2
  clone-node-max=1 notify=true
  ```

  c. 為DRBD磁碟區`fs_klfocdata`建立掛載點，指定裝置、目標目錄、檔案系統類型和掛載選項：

  ```
  pcs resource create fs_klfocdata ocf:heartbeat:Filesystem \
  device="/dev/drbd0" \
  directory="/mnt/KlFocDataShare_klfoc" \
  fstype="ext4" \
  options="data=journal"
  ```

- DRBD resource for klfocstate

  a. 為DRBD磁碟區`klfocstate`建立叢集資源，使群集能夠管理其狀態並自動監控其執行狀況：

  ```
  pcs resource create drbd_klfocstate ocf:linbit:drbd \
  drbd_resource=klfocstate \
  op monitor interval=60s \
  op start interval=0 timeout=240s \
  op monitor interval=60s \
  op monitor role=Promoted interval=10s \
  op monitor role=Unpromoted interval=30s \
  ```

b. 根據建立的資源`drbd_klfocstate`建立一個由叢集管理的資源ms_drbd_klfocstate：

```
pcs resource clone drbd_klfocstate promotable=true \
master-max=1 \
clone-max=2 \
clone-node-max=1 \
notify=true
```

c. 為DRBD磁碟區`fs_klfocstate`建立掛載點，指定裝置、目標目錄、檔案系統類型和掛載選項：

```
pcs resource create fs_klfocstate ocf:heartbeat:Filesystem \
device="/dev/drbd2" \
directory="/mnt/KlFocStateShare_klfoc" \
fstype="ext4" \
options="noatime"
```

6. 在兩個叢集節點上，停用DRBD服務的自動啟動：

```
systemctl disable drbd.service
```

Corosync和Pacemaker隨即在叢集節點上安裝並設定完成。之後，您必須安裝DBMS並建立管理伺服器資料庫和IAM資料庫。

安裝與設定Platform V Pangolin DBMS

在叢集節點上安裝並設定Corosync和Pacemaker後，您必須在兩個叢集節點上安裝DBMS。

若要安裝和設定DBMS：

1. 在兩個叢集節點上，安裝Platform V Pangolin 6.5.1 x64或更高版本。

   有關如何安裝Platform V Pangolin的資訊，請參閱其說明文件。

2. 確保安裝了 DBMS 的叢集節點沒有具有以下名稱的 DBMS 使用者帳戶：

   - client
   - iam
   - ksc
   - locker
   - pat
   - scope
   - voltron

3. 在活動叢集節點上，將DBMS目錄複製到`/mnt/KlFocDataShare_klfoc/dbms`目錄：

```
sudo rsync -av  /pgdata/06/data/ /mnt/KlFocDataShare_klfoc/dbms
sudo mv /pgdata/06/data/ /pgdata/06/data.bk/
```

4. 在兩個叢集節點上，開啟組態檔`/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf`，然後將目錄`/mnt/KlFocDataShare_klfoc/dbms`設定為資料庫資料目錄。

   同時指定設定檔路徑（`/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf`和`/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf`），並移除`include_dir`參數：

```
data_directory = '/mnt/KlFocDataShare_klfoc/dbms'
hba_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf'
ident_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf'
listen_addresses = '*'
```

5. 建立DBMS服務資源：

```
pcs resource create klfocsvc_dbms pgsql \
pgctl="/usr/pangolin-6.5/bin/pg_ctl"  psql="/usr/bin/psql" pgdata="/mnt/KlFocDataShare_klfoc/dbms"
config="/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf" socketdir="/tmp" \
op start timeout=60s interval=0s \
op stop timeout=60s interval=0s \
op monitor interval=30s timeout=60s \
op promote timeout=120s interval=0s \
op demote timeout=120s interval=0s \
meta target-role=Started
```

6. 在叢集的兩個節點上，停用DBMS服務的自動啟動：

```
sudo systemctl disable pangolin.service
```

7. 將DBMS資源`klfocsvc_dbms`新增到`group_klfoc`叢集群組：

```
pcs resource group add group_klfoc klfocsvc_dbms
```

8. 在清單末尾新增DBMS資源名稱`klfocsvc_dbms`，例如：

```
group klfoc_group {
...
klfocsvc_dbms
}
```

9. 在活動叢集節點上，在DBMS伺服器上，為IAM建立一個資料庫。 資料庫名稱必須與您安裝的資料庫不同，以便與Kaspersky Security Center for Linux配合使用。解除安裝或將伺服器移動到其他裝置時，管理伺服器不會自動刪除IAM資料庫，您必須手動刪除資料庫：

```
sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
```

DBMS隨即安裝和設定完成。管理伺服器資料庫和IAM資料庫隨即建立。之後，您需要在叢集節點上安裝Kaspersky Security Center for Linux。

在異地分散式故障轉移叢集節點上安裝Kaspersky Security Center for Linux

卡巴斯基安全管理中心 Linux 是透過使用應答檔案以靜默模式安裝在異地分散式故障轉移叢集節點上的，即無需使用者操作。回應檔案包含一組自訂安裝參數：變數及其各自的值。

先決條件：

- 完成所有準備步驟：
  - 準備叢集節點的檔案系統
  - 設定複製叢集檔案系統
  - 在叢集節點上使用安裝程式安裝和設定Corosync和Pacemaker
  - 安裝與設定Platform V Pangolin DBMS
- 確保叢集節點執行 Platform V SberLinux OS Server (SLO) 9.5.1 x64。
- 從卡巴斯基網站下載安裝檔案 `ksc64_[version_number]_amd64.deb`。

在主動節點上安裝

若要在活動節點上以靜默模式安裝Kaspersky Security Center for Linux：

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，才遵循以下步驟操作。
2. 建立群組 `kladmins` 和非授權帳戶 `ksc` 與 `ksciam`，這兩個帳戶必須是 `kladmins` 群組成員。為此，請在具有 root 權限的帳戶下依次執行以下命令：

   ```
   adduser ksc
   groupadd kladmins
   gpasswd -a ksc kladmins
   usermod -g kladmins ksc
   adduser ksciam
   gpasswd -a ksciam kladmins
   usermod -g kladmins ksciam
   ```

3. 在目錄`/mnt/KlFocDataShare_klfoc/`中，建立一個目錄，用於存放Kaspersky Security Center for Linux檔案：

   ```
   mkdir /mnt/KlFocDataShare_klfoc/ksc/
   ```

4. 建立回應檔案（TXT 格式），並以 VARIABLE_NAME=variable_value 格式將變數清單新增到回應檔案，每行一個變數。

   在靜默模式下安裝Kaspersky Security Center for Linux的參數清單中，指定異地分散式叢集部署所需的以下參數：

   - `KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT=2`

     設定值`2`，以部署異地分散式叢集。

   - `KLSRV_UNATT_SERVERADDRESS=<DNS balancer address>`和`KLSRV_UNATT_IAM_ADDRESS=<DNS balancer address>`

     必須已經部署了包含運行狀況檢查功能的DNS負載平衡器。這些參數的值必須相同，並且設定為DNS負載平衡器的FQDN。

5. 使用下列命令，在包含回應檔案全名的 root 或使用者環境中設定 `KLAUTOANSWERS` 環境變數之值（包含路徑）：

```
export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
```

6. 執行以下命令，以靜默模式啟動Kaspersky Security Center for Linux安裝程式：

   - 在根環境中：

     ```
     apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
     ```

   - 在使用者環境中：

     ```
     sudo -E apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
     ```

7. 停用klfocsvc_klfoc.service服務的自動啟動：

   ```
   systemctl disable klfocsvc_klfoc.service
   ```

8. 安裝完Kaspersky Security Center for Linux後，停止活動的叢集節點。

9. 將所有叢集資源移至被動節點。

   您可以使用命令`pcs node standby`（並透過`pcs node online`將其還原）。

在被動節點上安裝

若要在被動節點上安裝Kaspersky Security Center for Linux：

1. 執行卡巴斯基安全管理中心 Linux 安裝：

   ```
   sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb
   ```

2. 執行 卡巴斯基安全管理中心 Linux 配置：

   ```
   /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

3. 閱讀 最終使用者產品授權協議 (EULA) 和隱私政策。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，當出現提示時，輸入以下值：

   - 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）。若要使用卡巴斯基安全管理中心 Linux ，您必須接受 EULA 的條款。

   - 輸入`y`，如果您理解並接受隱私政策的條款，並且您同意您的資料將按照隱私政策中的說明進行處理和傳輸（包括傳輸到第三國）。輸入 n（如果您不接受隱私政策的條款）。要使用卡巴斯基安全管理中心 Linux ，您必須接受隱私政策的條款。

4. 將被動叢集節點選為管理伺服器安裝模式。

5. 出現提示時，輸入狀態共用掛接點的本機路徑：`/mnt/KlFocStateShare_klfoc`。

6. 停用klfocsvc_klfoc.service服務的自動啟動：

```
systemctl disable klfocsvc_klfoc.service
```

7. 建立`klfocsvc_klfoc`服務資源：

```
crm configure primitive klfocsvc_klfoc systemd:klfocsvc_klfoc \
op start timeout="900s" interval="0" \
op stop timeout="900s" interval="0" \
op monitor interval="30s" timeout="90s"
```

8. 將`klfocsvc_klfoc`資源新增至`group_klfoc`群組：

```
pcs resource group add group_klfoc klfocsvc_klfoc
```

9. 在群組末尾新增行`klfocsvc_klfoc`，例如：

```
group klfoc_group {
...
klfocsvc_klfoc
}
```

10. 驗證活動節點上的所有資源是否都處於啟動狀態。

```
pcs status
```

在叢集節點之間設定加密

若要在叢集節點之間設定加密，

若在設定複製叢集檔案系統期間安裝了DRBD 9.2.6或更高版本，請根據DRBD官方說明文件在叢集節點之間設定加密。

或者，您可以使用自己的VPN解決方案加密叢集節點之間的流量。

異地分散式Kaspersky Security Center for Linux容錯移轉叢集隨即安裝。之後，您必須在兩個叢集節點上都安裝卡巴斯基安全管理中心網頁主控台 。

在異地分散式故障轉移叢集節點上安裝卡巴斯基安全管理中心網頁主控台

對於異地分散式的Kaspersky Security Center for Linux故障轉移叢集部署，必須支援卡巴斯基安全中心網頁主控台的高可用性。要實現這一點，必須在兩個叢集節點上都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. 在兩個節點上，建立使用者以使用卡巴斯基安全管理中心網頁主控台。為此，請在具有 root 權限的帳戶下執行以下命令：

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <password>
   ```

   其中密碼必須包含至少8個字元。

2. 在兩個節點上，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 Linux 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. 在兩個節點上，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：`/etc/ksc-web-console-setup.json`。

   包含最小參數集合的回應檔案範例

   回應檔案的參數集取決於卡巴斯基安全管理中心網頁主控台所連線的管理伺服器版本：

   - 16 或更高版本的管理伺服器

     以下是登入管理伺服器版本 16 或更高版本所需的採用最小參數集的回應檔案範例：

     ```
     {
         "address": "ksc-web-console.example.com",
         "port": 8080,
         "trusted":  {
             "Administration Server v16": {
                 "iamHost": "ksc16.example.com",
                 "iamOAuthPort": 4444,
                 "iamProxyPort": 9050,
                 "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
                 "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
                 "kscPort": 13299,
                 "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
             }
         },
         "certDomain":"ksc-web-console.example.com",
         "acceptEula": true
     }
     ```

   - 15.4 或更早版本的管理伺服器

     以下是登入管理伺服器版本 15.4 或更早版本所需的採用最小參數集的回應檔案範例：

     ```
     {
         "address": "ksc-web-console.example.com",
         "port": 8080,
         "trusted":  {
              "Administration Server v15.4": {
                  "kscHost": "ksc.example.com",
                  "kscPort": 13299,
                  "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
              }
         },
         "certDomain":"ksc-web-console.example.com",
         "acceptEula": true
     }
     ```

   您可以將卡巴斯基安全管理中心網頁主控台安裝到管理伺服器所在的同一裝置，也可以安裝到不同裝置。如果將卡巴斯基安全管理中心網頁主控台安裝到不同裝置，則其位址（由 `address` 指定）將會與管理伺服器位址（由 `iamHost` 或者 `kscHost` 指定）不同。如果將卡巴斯基安全管理中心網頁主控台安裝到管理伺服器所在的同一裝置，則這些參數的值將相同。

`iamHost`值必須與安裝管理伺服器時指定的IAM位址相符。若要取得指定的IAM位址，請在管理伺服器主機上執行下列命令：

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

有關詳細資訊，請參閱文章：卡巴斯基安全管理中心網頁主控台安裝程式參數。

您可以將多個不同版本的管理伺服器新增到受信任伺服器清單。在這種情況下，這些伺服器可以使用不同的身分驗證方法。

我們建議您指定 1024 以上的連接埠號。如果您希望卡巴斯基安全管理中心網頁主控台在 1024 以下的連接埠上工作，安裝後您必須確保您有 setcup 實用程式，然後執行以下命令：

```
sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
```

如果沒有 setcap 實用程式，您可以安裝它。**點擊此連結檢視命令**。

對於 Debian 和 Ubuntu 作業系統，請執行以下命令之一：

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

對於 SUSE Linux Enterprise Server 和 Red Hat Enterprise Linux，請執行以下命令：

- `sudo zypper install libcap-progs`

4. 在兩個節點上，在具有根權限的帳戶下執行設定檔。

```
sudo apt-get install 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`。

5. 在其中一個叢集節點上，為KSCWebConsole服務建立一個Pacemaker資源，使KSCWebConsole成為Pacemaker管理的服務：

```
crm configure primitive ksc_webconsole systemd:KSCWebConsole \
op monitor interval=30s timeout=60s \
op start timeout=120s \
op stop timeout=120s \
meta target-role=Stopped
```

6. 在兩個節點上，停止KSCWebConsole服務並停用其自動啟動：

```
sudo systemctl stop KSCWebConsole
sudo systemctl disable KSCWebConsole
```

7. 在其中一個叢集節點上，將`ksc_webconsole`資源新增至`group_klfoc`群組：

```
crm configure edit klfoc_group
```

8. 在群組末尾新增行`ksc_webconsole`，之後`klfocsvc_dbms`，例如：

```
group klfoc_group {
...
klfocsvc_dbms
ksc_webconsole
}
```

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。

使用 DBMS 的帳戶

要安裝管理伺服器並使用它，您需要一個內部 DBMS 帳戶。此帳戶允許您存取 DBMS 並需要特定權限。所需的權限集合取決於以下標準：

- DBMS 類型：
  - MySQL 或 MariaDB
  - PostgreSQL 或 Postgres Pro
- 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，您可以使用管理伺服器安裝程式（以下簡稱「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或指令碼來建立空資料庫。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。

請勿手動變更管理伺服器資料庫和IAM資料庫，包括修改值、刪除或新增結構、表格和索引。任何非管理伺服器本身執行的資料庫變更都會立即或稍後（例如，升級到新版本後或從備份副本還原時）中斷管理伺服器的正常運作。只有在收到卡巴斯基技術支援的明確指示後，才允許編輯資料庫。

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 DBMS 權限資訊。

MySQL 和 MariaDB

如果您選擇 MySQL 或 MariaDB 作為 DBMS，請建立一個 DBMS 內部帳戶來存取 DBMS，然後授予該帳戶所需的權限。請注意，資料庫建立方法不影響權限集合。所需的權利如下所列：

- 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。

有關如何設定帳戶權限的更多資訊，請參閱設定 DBMS 帳戶以與 MySQL 和 MariaDB 搭配使用。

有關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格一個檔案的表空間。

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。

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 DBMS 帳戶以與 PostgreSQL 或 Postgres Pro 搭配使用。

Postgres 角色的權限

自動建立資料庫		手動建立資料庫
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。

當使用 Postgres 高可用性叢集（版本 14 或更高版本）作為資料庫時，資料庫使用者必須具有 `pg_read_all_stats` 權限。您可以透過執行以下命令授予此權限：

```
GRANT pg_read_all_stats TO "%1";
```

其中 `%1` 是資料庫使用者的名稱。

使用者名稱在管理伺服器安裝程式期間在 `KLSRV_UNATT_DBMS_LOGIN` 參數中指定。

設定用於復原管理伺服器資料的權限

若要從備份還原管理伺服器資料，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 DBMS 帳戶以搭配使用 MySQL 和 MariaDB

先決條件

在為 DBMS 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。

請勿手動變更管理伺服器資料庫和IAM資料庫，包括修改值、刪除或新增結構、表格和索引。任何非管理伺服器本身執行的資料庫變更都會立即或稍後（例如，升級到新版本後或從備份副本還原時）中斷管理伺服器的正常運作。只有在收到卡巴斯基技術支援的明確指示後，才允許編輯資料庫。

設定 DBMS 帳戶來安裝管理伺服器

要為管理伺服器安裝設定 DBMS 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。

   要建立帶密碼的 DBMS 帳戶，請執行以下命令：

   ```
   /* Create a user named kscdbadmin and specify the password for kscdbadmin */
   CREATE USER 'kscdbadmin' IDENTIFIED BY '< 密碼 >';
   ```

3. 為建立的 DBMS 帳戶授予以下權限：
   - 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

   要向建立的 DBMS 帳戶授予所需的權限，請執行以下指令碼：

```
/* Grant privileges to kscdbadmin */
GRANT USAGE ON *.* TO 'kscdbadmin';
GRANT ALL ON kav.* TO 'kscdbadmin';
GRANT SELECT, SHOW VIEW ON mysql.* TO 'kscdbadmin';
GRANT SELECT, SHOW VIEW ON sys.* TO 'kscdbadmin';
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'kscdbadmin';
GRANT PROCESS ON *.* TO 'kscdbadmin';
GRANT SUPER ON *.* TO 'kscdbadmin';
```

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 'kscdbadmin'`。

4. 要檢視授予 DBMS 帳戶的權限清單，請執行以下指令碼：

```
SHOW grants for 'kscdbadmin';
```

5. 為 IAM 建立一個 DBMS 帳戶。執行以下命令：

```
/* Create a user named iamdbadmin and specify the password for iamdbadmin */
CREATE USER 'iamdbadmin' IDENTIFIED BY '<password>';
```

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 'iamdbadmin'@'%' 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 'iamdbadmin'@'%' IDENTIFIED WITH mysql_native_password BY '< 密碼 >';
  ```

6. 為建立的 DBMS 帳戶授予以下權限：

- 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

要向建立的 DBMS 帳戶授予所需的權限，請執行以下指令碼：

```
/* Grant privileges to iamdbadmin */
GRANT USAGE ON *.* TO 'iamdbadmin';
GRANT ALL ON iamdb.* TO 'iamdbadmin';
GRANT SELECT, SHOW VIEW ON mysql.* TO 'iamdbadmin';
GRANT SELECT, SHOW VIEW ON sys.* TO 'iamdbadmin';
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin';
GRANT PROCESS ON *.* TO 'iamdbadmin';
GRANT SUPER ON *.* TO 'iamdbadmin';
```

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，請從指令碼中排除以下命令：`GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin'`。

7. 要檢視授予 DBMS 帳戶的權限清單，請執行以下指令碼：

   ```
   SHOW grants for 'iamdbadmin';
   ```

8. 若要手動建立管理伺服器資料庫，請執行以下命令（在此命令中，管理伺服器資料庫名稱為*kav*）：

   ```
   CREATE DATABASE kav
   ```

   使用您在建立 DBMS 帳戶的指令碼中指定的相同資料庫名稱。

9. 要手動建立 IAM 資料庫，請執行以下指令碼（在此命令中，IAM 資料庫名稱為*iam*）：

   ```
   CREATE DATABASE iam
   ```

   當解除安裝或將伺服器移至其他裝置時，管理伺服器不會自動刪除 IAM 資料庫，您必須手動刪除資料庫。

10. 安裝管理伺服器。

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。

設定 DBMS 帳戶以搭配使用 PostgreSQL 和 Postgres Pro

先決條件

在為 DBMS 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 Linux 搭配使用。

請勿手動變更管理伺服器資料庫和IAM資料庫，包括修改值、刪除或新增結構、表格和索引。任何非管理伺服器本身執行的資料庫變更都會立即或稍後（例如，升級到新版本後或從備份副本還原時）中斷管理伺服器的正常運作。只有在收到卡巴斯基技術支援的明確指示後，才允許編輯資料庫。

設定 DBMS 帳戶來安裝管理伺服器

要為管理伺服器安裝設定 DBMS 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 *kscdbadmin*）：

   ```
   CREATE USER "kscdbadmin" WITH PASSWORD '<password>';
   ```

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 "kscdbadmin";
```

建議您將本指示步驟 3 中建立的 Postgres 角色指定為資料庫所有者（在此範例中，該角色為 *kscdbadmin*）。

指定其他使用者為資料庫所有者

如需指定其他 Postgres 角色，請以該所有者（或超級使用者）角色連線至資料庫，並執行以下命令：

```
GRANT ALL PRIVILEGES ON DATABASE "kav" TO "kscdbadmin";
GRANT USAGE ON SCHEMA public TO "kscdbadmin";
GRANT CREATE ON SCHEMA public TO "kscdbadmin";
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "kscdbadmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "kscdbadmin";
```

確保資料庫所有者角色具有 CONNECT 與 TEMPORARY 權限。

```
如果發生「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 "kscdbadmin" TEMPLATE template0;
而非：
CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin";
```

5. 為 IAM 建立新的 Postgres 角色（在此範例中，Postgres 角色為 `iamdbadmin`）：

```
CREATE USER "iamdbadmin" WITH PASSWORD '<password>';
```

6. 建立 IAM 資料庫（在此範例中，IAM 資料庫名稱為 `iam`）：

```
CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin";
```

建議您將本指示步驟 5 中建立的 Postgres 角色指定為資料庫所有者（在此範例中，該角色為 *iamdbadmin*）。

指定其他使用者為 IAM 資料庫所有者

如需指定其他 Postgres 角色，請以該所有者（或超級使用者）角色連線至資料庫，並執行以下命令：

```
GRANT ALL PRIVILEGES ON DATABASE "iam" TO "iamdbadmin";
GRANT USAGE ON SCHEMA public TO "iamdbadmin";
GRANT CREATE ON SCHEMA public TO "iamdbadmin";
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "iamdbadmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "iamdbadmin";
```

確保資料庫所有者角色具有 CONNECT 與 TEMPORARY 權限。

```
如果發生「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 "iam" ENCODING 'UTF8' OWNER "iamdbadmin" TEMPLATE template0;
而不是：
CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin";
```

當解除安裝或將伺服器移至其他裝置時，管理伺服器不會自動刪除 IAM 資料庫，您必須手動刪除資料庫。

7. 安裝管理伺服器。

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。

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。

> 僅當您將 MySQL 或 MariaDB DBMS 用於管理伺服器時，才建議執行此程序。
> 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。

用於卡巴斯基安全管理中心 Linux 的憑證

本節包含與卡巴斯基安全管理中心 Linux 憑證相關的資訊，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。

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
- 網頁伺服器憑證
- 卡巴斯基安全管理中心網頁主控台憑證
- 身分和存取管理器憑證

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。使用自訂憑證時，憑證檔案必須包含完整的公共金鑰鏈，包括所有中間憑證，直到根憑證授權機構 (CA)。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 公用程式或透過卡巴斯基安全管理中心 網頁主控台中的「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。

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

管理伺服器憑證需要用於以下目的：

- 當卡巴斯基安全管理中心網頁主控台連線到管理伺服器時對其進行身分驗證。
- 受管理裝置上管理伺服器和網路代理之間的安全互動。
- 主管理伺服器連線到從屬管理伺服器時的身分驗證。

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 /var/opt/kaspersky/klnagent_srv/1093/cert/ 資料夾中。您在建立回應檔案以安裝卡巴斯基安全管理中心 網頁主控台時指定管理伺服器憑證。該憑證稱為通用憑證 ("C")。

管理伺服器憑證 397 天有效。卡巴斯基安全管理中心會在通用憑證到期前 90 天自動產生一個一般儲備 ("CR") 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。

任何管理伺服器憑證的最長有效期不得超過 397 天。

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。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。

在管理伺服器憑證被備用憑證或自訂憑證取代後，在回應檔案中指定新憑證，然後使用此檔案重新安裝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網頁主控台將無法連線到管理伺服器。

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。

您也可以與其他管理伺服器設定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。

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。

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」）。您可以在管理伺服器內容中指定行動憑證。

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。卡巴斯基安全管理中心會在通用憑證到期前 60 天自動產生此憑證。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。

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），則您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，在管理伺服器內容中，您可以指定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。

此外，為了在執行 iOS 作業系統的行動裝置上對管理伺服器進行身分驗證，需要 iOS MDM 伺服器憑證。有關詳細資訊，請參閱配置 iOS MDM 伺服器憑證。

網頁伺服器憑證

Web 伺服器是卡巴斯基安全管理中心管理伺服器的一個元件，使用特殊類型的憑證。發佈網路代理安裝套件（隨後將其下載到受管理裝置）以及發佈 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。

身分和存取管理器憑證

身分和存取管理器憑證（IAM 憑證）需要用於以下目的：

- 當使用者的瀏覽器透過 OAuth 協定連線到管理伺服器時，對管理伺服器進行身分驗證。
- 當卡巴斯基安全管理中心網頁主控台連線到管理伺服器時對其進行身分驗證。

IAM 憑證會在首次執行管理伺服器時自動建立。憑證儲存在管理伺服器裝置的以下目錄中：/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem（對於卡巴斯基安全管理中心容錯移轉叢集，路徑為：<共用資料夾>/iam/main_certificate.pem）。在建立用於安裝卡巴斯基安全管理中心網頁主控台的回應檔案時，必須使用 `iamCertPath` 參數指定 IAM 憑證的路徑。

IAM 憑證的有效期為 365 天。卡巴斯基安全管理中心會在目前憑證到期前 48 小時自動產生一個一般備用 IAM 憑證。備用憑證隨後會被用來無縫替換過期的 IAM 憑證。

任何 IAM 憑證的最長有效期不得超過 397 天。

如有必要，您可以指派自訂 IAM 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。

> 在 IAM 憑證被備用憑證或自訂憑證取代後，在回應檔案中指定新憑證，然後使用此檔案重新安裝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網頁主控台將無法連線到管理伺服器。

當您登入卡巴斯基安全管理中心網頁主控台時，瀏覽器會重新導向至管理伺服器登入頁面（https://<管理伺服器位址>:4444）進行身分驗證。瀏覽器和管理伺服器之間的流量使用 TLS 協定和 IAM 憑證加密。

瀏覽器可能會告知您與管理伺服器的連線非私密，且 IAM 憑證無效。出現此警告是因為 IAM 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 IAM 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 IAM 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。

卡巴斯基安全管理中心 Linux 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 Linux 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 Linux 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。 憑證必須包含有效的使用者備用名稱（SAN），其中包含管理伺服器環回位址： • IPv4位址：127.0.0.1 • IPv6位址：0:0:0:0:0:0:0:1	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」。

憑證類型	要求	註解
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 容器會包括完整的公共金鑰鏈。 出現憑證的主題替代名稱 (SAN)；也就是說，`subjectAltName` 欄位值有效。 該憑證符合網頁瀏覽器對伺服器憑證施加的有效要求，以及 CA/瀏覽器論壇 的當前基準要求。	—
卡巴斯基安全管理中心網頁主控台憑證	金鑰擴充功能：伺服器身份驗證、用戶端身份驗證。 從中指定憑證的 PEM 容器會包括完整的公共金鑰鏈。 出現憑證的主題替代名稱 (SAN)；也就是說，`subjectAltName` 欄位值有效。該值必須與安裝管理伺服器時指定的 IAM 位址相符。若要取得指定的 IAM 位址，請在管理伺服器主機上執行下列命令： `grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml` 該憑證符合網頁瀏覽器對伺服器憑證的有效要求，以及 CA/瀏覽器論壇 的當前基準要求。	卡巴斯基安全管理中心網頁主控台不支援加密憑證。
身分和存取管理器憑證（IAM 憑證）	延伸金鑰使用：伺服器身分驗證。 從中指定憑證的 PEM 容器會包括完整的公共金鑰鏈。 憑證必須有效並支援用戶端身分驗證。 該憑證符合網頁瀏覽器對伺服器憑證的有效要求，以及 CA/瀏覽器論壇 的當前基準要求。	卡巴斯基安全管理中心網頁主控台不支援加密憑證。

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。

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有，並且卡巴斯基安全管理中心網頁主控台憑證無效。出現此警告是因為網頁主控台憑證為自簽名並由卡巴斯基安全管理中心 Linux 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，將卡巴斯基安全管理中心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。

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：

透過執行以下操作之一重新安裝卡巴斯基安全管理中心 網頁主控台：

- 如果想要使用卡巴斯基安全管理中心 網頁主控台的相同安裝檔案，請刪除卡巴斯基安全管理中心 網頁主控台，然後安裝相同的卡巴斯基安全管理中心 網頁主控台版本。
- 如果想要使用升級版的安裝檔案，請執行升級命令。

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。

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（也叫卡巴斯基安全管理中心 網頁主控台）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 網頁主控台的憑證：

1. 開啟在安裝程式卡巴斯基安全管理中心網頁主控台時所建立的回應檔案。

   如果您想，您可以建立新的回應檔案。

2. 在檔案中，指定以下路徑：

   - 使用`certPath`參數存取卡巴斯基安全管理中心網頁主控台自訂憑證檔案
   - 使用`keyPath`參數存取與卡巴斯基安全管理中心網頁主控台自訂憑證關聯的私鑰。

   > 您必須指定這兩條路徑。否則，Web 瀏覽器會不斷通知您您的連線不是私密的。

3. 透過指定新的回應檔案重新安裝卡巴斯基安全管理中心 網頁主控台。執行以下操作之一：

   - 如果想要使用卡巴斯基安全管理中心 網頁主控台的相同安裝檔案，請刪除卡巴斯基安全管理中心 網頁主控台，然後安裝相同的卡巴斯基安全管理中心 網頁主控台版本。
   - 如果想要使用升級版的安裝檔案，請執行升級命令。

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。

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。

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。 憑證必須包含有效的使用者備用名稱（SAN），其中包含管理伺服器環回位址： • IPv4位址：127.0.0.1 • IPv6位址：0:0:0:0:0:0:0:1
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 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。

憑證類型	要求
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**

   替換憑證後，在回應檔案中指定它，然後使用該檔案更新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

為了避免失去對裝置的控制，請參考應用情境：指定自定義管理伺服器憑證，然後再繼續。

要取代管理伺服器憑證：

在命令列下，執行以下公用程式：

```
/opt/kaspersky/ksc64/sbin/klsetsrvcert [-t <certificate type> {-i <path to new certificate> [-p <password>] [-o <validation parameters>] | -g <dns name>}][-f <replacement time>][-r <root certificates>][-l <log file path>]
```

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 的通用憑證。 • `CR` – 取代連接埠 13000 和 13291 的通用儲備憑證。
`-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。
`-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）。 要在沒有簽署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 公用程式中指定 `-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 >	系統將為指定的DNS名稱（通用名稱和主題備用名稱）建立一個新憑證。
`-r` < 根憑證 >	信任的根憑證授權機構清單，格式 PEM。
`-l` < 記錄檔路徑 >	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 <新憑證的路徑> -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 -t CR -i <新憑證的路徑> -p <密碼> -o NoCA
```

2. 指定套用新憑證的日期：

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

其中，「`DD-MM-YYYY hh:mm`」是比目前日期晚 3 至 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。

更換管理伺服器通用憑證後，還需要哪些其他步驟？

1. 確保**滿足自訂憑證的需求**。

   如果您使用的是自訂憑證而不是自簽名憑證，則在將 Kaspersky Security Center for Linux 升級到更高版本之前，必須確保憑證包含主體替代名稱（SAN）。否則，請務必在升級 Kaspersky Security Center for Linux 之前替換憑證。否則，升級後您將無法登入網頁主控台。

   若要確保憑證包含SAN，請執行下列操作：

   1. 在安裝了管理伺服器的裝置上，執行以下命令：

      - 對於Linux裝置：

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

      - 對於Windows裝置：

        ```
        certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
        ```

   2. 確保命令輸出中存在主題備用名稱，并包含管理伺服器裝置的地址。

   3. 如果缺少主題備用名稱，請使用klsetsrvcert公用程式將自訂憑證替換為滿足需求的憑證。

2. 確保 IAM 伺服器組態檔包含目前管理伺服器的位址。如果沒有，請將該位址新增至組態檔。

3. 重新安裝網頁主控台以避免以下錯誤：

   管理伺服器使用不受信任的憑證。請透過指定有效憑證重新設定應用程式，或聯絡主管理員。

使用 klmover 公用程式將網路代理連線到管理伺服器

您可以使用 klmover 公用程式還原不受控裝置與管理伺服器之間的連線，例如，在管理伺服器發生故障後，如果無法從備份中還原。

若要還原連線，請從命令列執行 klmover 公用程式：

- 對於 Linux：

  - 對於 32 位元系統：`/opt/kaspersky/klnagent/bin/klmover [-address <伺服器位址>] [-pn <連接埠號碼>] [-ps <SSL 連接埠號碼>] [-nossl] [-cert <憑證檔案路徑>]`

  - 對於 64 位元系統：`/opt/kaspersky/klnagent64/bin/klmover [-address <伺服器位址>] [-pn <連接埠號碼>] [-ps <SSL 連接埠號碼>] [-nossl] [-cert <憑證檔案路徑>]`

- 對於 Windows：
  - 對於 32 位元系統：`<路徑>\klmover.exe [-address <伺服器位址>] [-pn <連接埠號碼>] [-ps <SSL 連接埠號碼>] [-nossl] [-cert <憑證檔案路徑>]`
  - 對於 64 位元系統：`<路徑>\klmover.exe [-address <伺服器位址>] [-pn <連接埠號碼>] [-ps <SSL 連接埠號碼>] [-nossl] [-cert <憑證檔案路徑>]`
- 對於 macOS：

  `/Library/Application Support/Kaspersky Lab/klnagent/Binaries/klmover [-address <伺服器位址>] [-pn <連接埠號碼>] [-ps <SSL 連接埠號碼>] [-nossl] [-cert <憑證檔案路徑>]`

其中<路徑>是網路代理的預設安裝路徑，或您在網路代理安裝套件設定中指定的安裝路徑。

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。

如果您遺失或忘記了安裝在不再受 Kaspersky Security Center Linux 管理的裝置上的受密碼防護的網路代理密碼，則無法使用 klmover 實用程式或命令列移除網路代理。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。

klmover 公用程式需要本機管理員權限。

在 Windows 裝置上啟用**使用解除安裝密碼**選項也會啟用 Cleaner 工具 (cleaner.exe) 的密碼防護。

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 位址或 DNS 名稱。
`-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。
`-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。

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 Linux 中使用的網頁伺服器憑證。根據目前的應用程式設定，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 Linux 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。卡巴斯基安全中心 Linux 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。

> 如果您從未在管理伺服器屬性視窗的**網頁伺服器**區域中將自己的自訂憑證指定為網頁伺服器憑證，則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 Linux 中的使用做好準備。請檢查您的自訂憑證是否滿足 Kaspersky Security Center for Linux的需求。如有必要，請修改憑證。
2. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。
3. 在**一般**索引標籤，選取**網頁伺服器**區域。
4. 在**透過 HTTP**子區域中，選取**從檔案上傳憑證**選項，然後點擊**變更憑證**按鈕。
5. 在開啟的視窗中，於**憑證格式**欄位內選取憑證的類型：
   - 如果您已選取**PKCS#12 容器**，請點擊**憑證**欄位旁邊的**瀏覽**按鈕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**欄位。
   - 如果您已選取**X.509 憑證**，請點擊**私密金鑰**欄位旁邊的**瀏覽**按鈕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**欄位中輸入密碼。
6. 點擊**儲存**按鈕，然後點擊**確定**。

   視窗即會關閉。
7. 如有必要，請在**網頁伺服器 HTTPS 連接埠**欄位中變更 Web 伺服器的 HTTPS 連接埠號碼，然後點擊**儲存**按鈕。

重新發佈網頁伺服器憑證。

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. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。
2. 在**一般**索引標籤，選取**憑證**區域。

3. 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. 選擇**透過管理伺服器發佈的憑證**選項，然後點擊**瀏覽**按鈕。

   b. 在開啟的視窗中，於設定的**連線位址**和**啟動條款**群組，選取相關選項並點擊**確定**。

或者，如果您打算使用自己的自訂憑證，請執行以下操作：

a. 請檢查您的自訂憑證是否滿足Kaspersky Security Center for Linux的需求。如有必要，請修改憑證。

b. 選擇**其他憑證**選項，點擊**管理憑證**按鈕，然後在開啟的視窗中點擊**瀏覽**按鈕。

c. 在開啟的視窗中，於**憑證格式**欄位內選取憑證的類型：

   - 如果您已選取**PKCS#12 容器**，請點擊**憑證**欄位旁邊的**瀏覽**按鈕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**欄位。

   - 如果您已選取**X.509 憑證**，請點擊**私密金鑰**欄位旁邊的**瀏覽**按鈕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**欄位中輸入密碼。

d. 點擊**儲存**按鈕，然後點擊**確定**。

重新發佈行動憑證以用作網頁伺服器憑證。

將預設 IAM 憑證變更為自訂憑證

若要變更預設 IAM 憑證：

1. 產生自訂憑證，並為卡巴斯基安全管理中心 Linux 中的使用做好準備。請檢查您的自訂憑證是否滿足Kaspersky Security Center for Linux的需求。

2. 確保kladmins 群組有權存取 IAM 憑證檔案。

3. 查找 IAM 設定檔：`/var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`

   在此檔案中，將 IAM 憑證檔案的路徑新增至`server_iam`部分：

   - `certificates.main.cert`：主憑證檔案路徑。

   - `certificates.main.key`：主憑證的私密金鑰路徑。私有金鑰不得受密碼保護。

4. 查找網頁主控台設定檔：`/etc/ksc-web-console-setup.json`

   在此檔案中，將 `iamCertPath` 欄位值設定為主憑證的公共金鑰路徑。

5. 透過執行以下命令重新啟動 kliam 服務：

   ```
   sudo service kliam_srv restart
   ```

6. 重新安裝網頁主控台。

   重新安裝後，網頁主控台將使用自訂 IAM 憑證。

要變更 IAM 備用憑證，請執行以下操作：

1. 查找 IAM 設定檔：`/var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`

在此檔案中，指定 IAM 憑證檔案的路徑：

- `server_iam.certificates.reserve.cert`：主憑證檔案路徑。
- `server_iam.certificates.reserve.key`：主憑證的私密金鑰路徑。私有金鑰不得受密碼保護。

2. 透過執行以下命令重新啟動 kliam 服務：

   ```
   sudo systemctl restart kliam_srv.service
   ```

   主憑證檔案過期後，將改為使用 IAM 備用憑證。

將管理伺服器位址新增至IAM伺服器設定

在升級、移動或遷移期間更改通用管理伺服器憑證（「C」）後，您需要在IAM伺服器組態檔中指定管理伺服器地址，以確保IAM伺服器和管理伺服器之間的驗證憑證正確。

若要將管理伺服器位址新增至IAM伺服器組態：

1. 透過執行下列命令，從通用管理伺服器憑證（「C」）取得主題備用名稱 (SAN) 值：

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

2. 根據命令輸出，執行下列其中一項操作：

   - 如果輸出結果顯示缺少該值，請檢查**自訂憑證的需求**。

     如果您使用的是自訂憑證而不是自簽名憑證，則在將 Kaspersky Security Center for Linux 升級到更高版本之前，必須確保憑證包含主體替代名稱（SAN）。否則，請務必在升級 Kaspersky Security Center for Linux 之前替換憑證。否則，升級後您將無法登入網頁主控台。

     若要確保憑證包含SAN，請執行下列操作：

     1. 在安裝了管理伺服器的裝置上，執行以下命令：

        - 對於Linux裝置：

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

        - 對於Windows裝置：

          ```
          certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
          ```

     2. 確保命令輸出中存在主題備用名稱，并包含管理伺服器裝置的地址。

     3. 如果缺少主題備用名稱，請使用klsetsrvcert公用程式將自訂憑證替換為滿足需求的憑證。

     若不滿足需求，請使用klsetsrvcert公用程式替換上一個管理伺服器上的管理伺服器通用憑證。之後，重複升級、移動或遷移步驟。

   - 如果值與Kaspersky Security Center for Linux安裝期間指定的值匹配（在安裝精靈的**輸入IAM伺服器DNS名稱**步驟中，或者對於靜默模式安裝，在`KLSRV_UNATT_IAM_ADDRESS`參數中），則無需進一步操作。IAM伺服器和管理伺服器將正常互動。

   - 如果該值包含環回位址（127.0.0.1和/或 0:0:0:0:0:0:0:1），請在組態檔中使用其中一個。建議使用127.0.0.1。

3. 將管理伺服器通用憑證中的一個SAN地址值新增至IAM伺服器組態檔的`server_iam`區塊中，格式如下：`ksc_address: "<SAN_address>"`。

   您可以使用文字編輯器來修改IAM伺服器的組態檔，例如，vi。以下命令在vi文字編輯器中開啟檔案：

   ```
   vi /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
   ```

   IAM伺服器組態檔中server_iam區塊的範例：

   ```
   server_iam:
       iam_address: "ksc.example.com"
       server_display_name: "ksc.example.com"
       ksc_address: "oldksc.example.internal"
       ksc_ca: "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
   ```

   確保使用與範例相同的間距。

4. 檢查`ksc_address`參數中的網路名稱是否解析為管理伺服器的IP位址。為此，您可以使用管理伺服器上的Ping公用程式。

   如果解析的位址不同，請確保舊管理伺服器與網路斷開連線，並且沒有保留舊IP位址的DNS記錄。如果無法解析位址，請使用企業DNS中的DNS記錄對其進行對映，或向管理伺服器上的主機檔案新增條目。

5. 透過執行以下命令重新啟動IAM伺服器服務以套用組態更改：

   ```
   sudo systemctl restart kliam_srv.service
   ```

管理伺服器位址隨即從管理伺服器通用憑證新增至IAM伺服器組態檔。

故障排除

IAM伺服器上的組態問題可能會導致登入網頁主控台時發生錯誤。下表描述了可能的錯誤及其解決方法。

錯誤	描述	解決方法
您的請求目前無法處理。請稍後重試。	除了升級或恢復Kaspersky Security Center for Linux後的資料初始化過程之外，如果使用指定的網路位址連線到管理伺服器失敗，也可能發生此錯誤。	使用ping公用程式檢查網路名稱解析到哪個IP位址。
管理伺服器使用不受信任的憑證。請透過指定有效憑證重新設定應用程式，或聯絡主管理員。	如果IAM伺服器組態檔中的位址值與管理伺服器通用憑證的「使用者備用名稱 (SAN)」屬性中的值不匹配，則可能會發生此錯誤。	請依照上述說明操作。
使用者名稱或者密碼不正確。	除了憑據錯誤之外，如果網路上存在另一個同名的管理伺服器，也可能發生此錯誤。	檢查指定的位址是否解析為目前管理伺服器的IP位址。

定義共用資料夾

安裝管理伺服器後，您可以在管理伺服器屬性中指定共用資料夾的位置。預設情況下，共用資料夾是在帶有管理伺服器的裝置上建立的。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。

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（單一登入）

  此方法用於在連線到管理伺服器 16 及更高版本的卡巴斯基安全管理中心網頁主控台中進行安全性驗證。若要使用網域身分驗證，您必須在卡巴斯基安全管理中心網頁主控台安裝期間，指定與身分和存取管理器 (IAM) 互動的附加參數。

- 透過指定網域使用者的名稱和密碼

  在使用網域使用者帳戶登入之前，請先輪詢網域控制器以取得網域使用者清單。然後，您必須指定網域使用者名稱和密碼才能登入管理伺服器。此方法僅支援透過 Microsoft Active Directory 進行身分驗證。

- 透過指定內部使用者的名稱和密碼

您想要使用其登入卡巴斯基安全管理中心網頁主控台的使用者帳戶必須具有已指派的角色。登入前，請確保網域帳戶或內部使用者帳戶已被指派角色。否則，將會出現登入錯誤。

透過使用網域身分驗證（單一登入）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>。

   管理伺服器選擇頁面將顯示。

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，則不會顯示管理伺服器清單。

   瀏覽器將重定向到 https://<管理伺服器位址>:4444。

3. 設定 Kerberos 網域身分驗證。

4. 執行以下操作之一：

   - 點擊**使用網域身分驗證**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**顯示虛擬伺服器選項**。

     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**使用網域身分驗證**按鈕。

5. 指定身分驗證器應用程式在行動裝置上產生的一次性安全碼。

   首次登入時，請為您的帳戶配置雙步驟身分驗證。如果您無法設定雙因素驗證，請聯絡在「**一般功能: 使用者權限**」功能區域中擁有修改物件 ACL 權限且已設定雙因素驗證的使用者，以將您的帳戶新增至雙因素驗證允許清單中。

登入後，卡巴斯基安全管理中心網頁主控台首頁將顯示，其中包含您上次使用的語言和主題。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 Linux。

透過指定網域或內部使用者的名稱和密碼登入

要透過指定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：

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>。

   管理伺服器選擇頁面將顯示。

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，則不會顯示管理伺服器清單。

   瀏覽器將重定向到 https://<管理伺服器位址>:4444。

3. 執行以下操作之一：

   - 若要使用網域使用者帳戶登入管理伺服器，請輸入網域使用者的使用者名稱和密碼。

     您可以採用以下格式之一輸入網域使用者的使用者名稱：

     - 使用者名稱@ `dns.domain`
     - `NTDOMAIN\`使用者名稱

     使用網域使用者帳戶登入之前，請輪詢網域控制器以獲取網域使用者清單。

   - 若要透過指定管理員的使用者名稱和密碼登入管理伺服器，請輸入內部使用者的使用者名稱和密碼。

- 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**顯示虛擬伺服器選項**。

  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。

4. 點擊**登入**按鈕。

5. 指定身分驗證器應用程式在行動裝置上產生的一次性安全碼。

   首次登入時，請為您的帳戶配置雙步驟身分驗證。如果您無法設定雙因素驗證，請聯絡在「**一般功能: 使用者權限**」功能區域中擁有修改物件 ACL 權限且已設定雙因素驗證的使用者，將您的帳戶新增至雙因素驗證允許清單中。

6. 如果您的帳戶啟用了強制修改密碼或您的密碼已過期，則會彈出密碼修改視窗。設定新密碼以登入卡巴斯基安全管理中心網頁主控台。

登入後，卡巴斯基安全管理中心網頁主控台首頁將顯示，其中包含您上次使用的語言和主題。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 Linux。

登出

要登出卡巴斯基安全管理中心網頁主控台，

在上方窗格中，按一下您的帳戶名稱以前往您的帳戶功能表，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。

卡巴斯基安全管理中心網頁主控台介面

卡巴斯基安全管理中心 Linux 透過卡巴斯基安全管理中心網頁主控台介面進行管理。

卡巴斯基安全管理中心網頁主控台視窗包含以下項目：

- 視窗左側的主功能表
- 視窗上部的上部窗格
- 視窗右側的工作區

主功能表

主功能表會包含以下區段：

- **管理伺服器**。顯示您目前所連管理伺服器的名稱。您可以透過按一下管理伺服器名稱來開啟管理伺服器屬性。
- **主控台導覽**。顯示主功能表地圖。大部分顯示的部分都可以加入書籤或設定為首頁。預設**主控台導覽**被設定為首頁。您可以變更這些設定。
- **監控**。提供基礎架構、防護狀態和統計資料概覽。
- **資產管理**。包含裝置和硬體管理工具，以及卡巴斯基應用程式政策。
- **工作**。包含用於建立和執行工作的工具。
- **使用者和角色**。可讓您管理使用者和角色、透過向使用者分配角色來設定使用者權限，以及為角色設定關聯的政策設定檔。
- **儲存區**。可讓您存取應用程式儲存庫。
- **軟體管理**。可讓您管理卡巴斯基和協力廠商應用程式，以及安裝套件和修補程式。
- **操作**。包含多種操作，包括應用程式產品授權、檢視和管理加密磁碟機和加密事件。
- **發現和佈署**。可讓您輪詢網路來發現用戶端裝置，以及手動或自動將裝置分發到管理群組。其中也包含快速啟動精靈和防護佈署精靈。
- **市集**。包含完整卡巴斯基業務解決方案系列的資訊，可讓您選取所需的解決方案，然後繼續在卡巴斯基網站購買這些解決方案。
- **設定**。允許您備份 網頁外掛程式 的目前狀態，以便以後能夠還原儲存的狀態。其中包含您個人的介面外觀相關設定，例如介面語言或主題。

如有必要，您可以透過點擊位於螢幕底部的 V 形符號 (⌄) 來最小化主選單。

上方窗格

上方窗格始終顯示在所有主控台部分中，且無法隱藏。

窗格左側包含應用程式名稱和徽標。如果點擊應用程式名稱或徽標，卡巴斯基安全管理中心網頁主控台主頁將開啟。

窗格右側會顯示以下內容：

- 通知圖示 (🔔) 。如果點擊該圖示，一個包含通知的窗格將開啟。
- 您的帳戶選單。包含卡巴斯基安全管理中心 Linux 幫助的連結。它還允許您登出卡巴斯基安全管理中心 Linux、變更您的帳戶的密碼、檢視卡巴斯基安全管理中心網頁主控台版本和已安裝的管理 Web 外掛程式清單。

工作區

工作區會顯示您在卡巴斯基安全管理中心網頁主控台介面視窗的區域中選擇檢視的資訊。其中還會包含供您設定資訊顯示方式的控制元素。

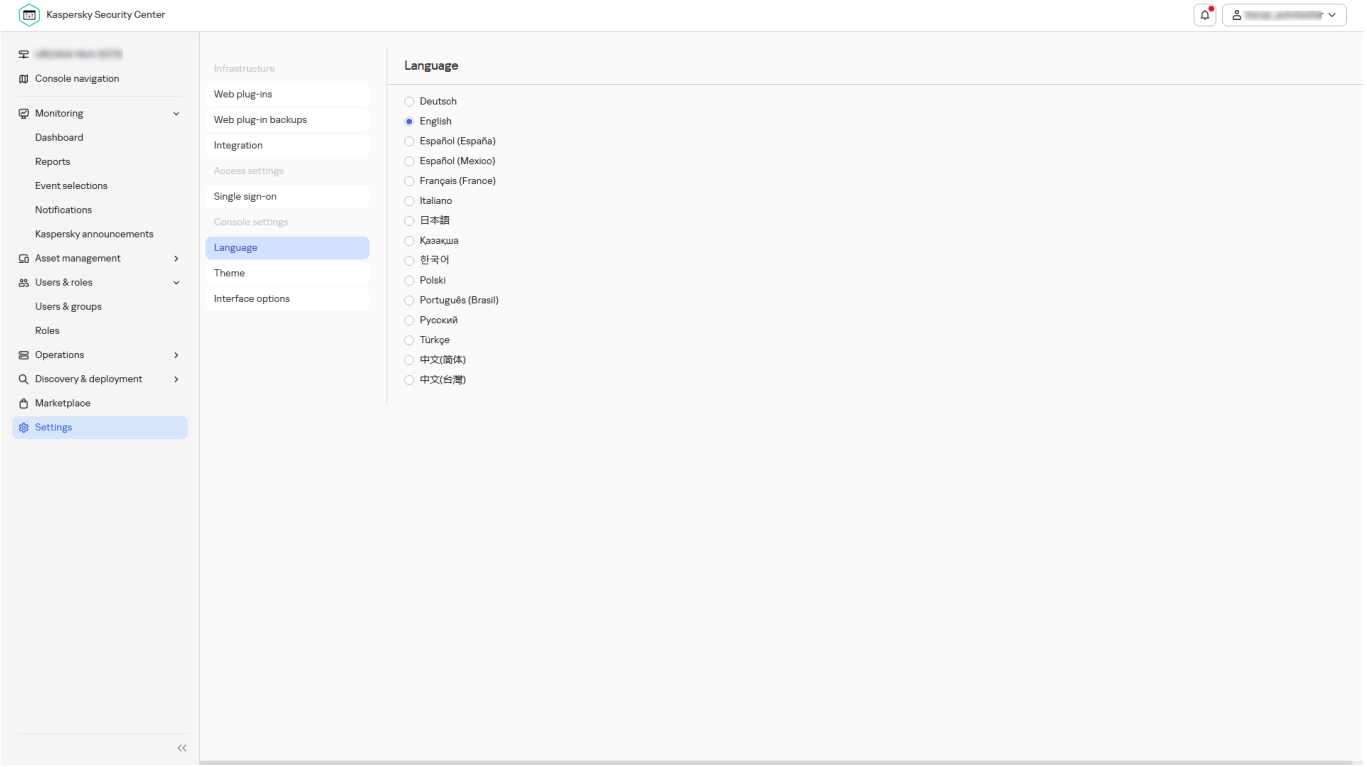
> 我們建議使用單一瀏覽器索引標籤來操作卡巴斯基安全管理中心網頁主控台。

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，轉至**設定 → 語言**。
2. 選擇一種受支援的當地語係化語言。



變更卡巴斯基安全管理中心網頁主控台介面的語言

變更卡巴斯基安全管理中心網頁主控台首頁

登入卡巴斯基安全管理中心網頁主控台後，首頁將顯示。

預設**主控台導覽**區域被設定為首頁。如果需要的話，您可以變更首頁。

變更首頁：

1. 在**主控台導覽**部分，將滑鼠遊標懸停在您想要設定為首頁的項目上。
2. 在首頁 (⌂) 圖示顯示後，點擊圖示。

   首頁被變更，螢幕上顯示相應的訊息，被選為首頁的項目標有首頁 (⌂) 圖示.

> **市場** 和**設定** 部分不能被設定為首頁。

新增和移除書籤

您可以將卡巴斯基安全管理中心網頁主控台的常用部分新增至書籤以從主功能表中的**書籤**區域快速存取它們。

> 如果您未將任何部分新增至書籤，則**書籤**區域不會顯示在主功能表中。

您只能將顯示頁面的區域新增至書籤。例如，如果您前往**資產管理 → 資產（裝置）**，則會開啟包含裝置表的頁面，這表示您可以將該部分新增到書籤。若在主功能表中選擇該部分後出現視窗或未出現任何元素，則您無法將此類區域新增至書籤。

若要將一個區域新增至書籤：

1. 在主功能表中，將滑鼠遊標停留在要釘選的區段上。
2. 在書籤 (🔖) 圖示顯示後，點擊圖示。

   該區域顯示在**書籤**區域中。

要將區域從書籤中移除：

1. 在主功能表中，轉至**書籤**區域。
2. 將滑鼠遊標停留在要移除的區域上，然後點擊取書籤 (🔖) 圖示。

   該區段已從書籤中刪除。

您可以透過將滑鼠游標懸浮在區域上面然後點擊 (🔖) 圖示將區域新增至或者從 **主控台導覽** 區域的書籤中移除。所選項目將用書籤 (🔖) 圖示標記並顯示在主功能表的 **書籤** 區域中。如果您想要從書籤移除項目，請點擊書籤 (🔖) 圖示。

> **書籤** 區域僅顯示在主功能表中。它從來不顯示在 **主控台導覽** 頁面上。

移除卡巴斯基安全管理中心網頁主控台

在以下情況下，您可能需要移除卡巴斯基安全管理中心網頁主控台伺服器（也稱為卡巴斯基安全管理中心網頁主控台）：

- 使用另一個通用憑證從備份中還原資料。
- 重新簽署管理伺服器通用憑證。
- 將網頁主控台憑證替換為自訂憑證。
- 裝置上已不再使用卡巴斯基安全管理中心網頁主控台。

若要移除卡巴斯基安全管理中心網頁主控台：

1. 根據您的Linux版本，執行以下其中一項命令：
   - `sudo dnf remove ksc-web-console`
   - `sudo apt remove ksc-web-console`
2. 透過執行以下命令來檢查結果：

   `sudo systemctl status KSC*`

   命令輸出中不能包含「卡巴斯基安全管理中心網頁主控台」。

若要恢復卡巴斯基安全管理中心網頁主控台，請按照文章安裝卡巴斯基安全管理中心網頁主控台中所述在裝置上安裝它。

快速啟動精靈

卡巴斯基安全管理中心 Linux 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。
- 設定以電子郵件通知您管理伺服器和受管理應用程式操作期間發生的事件。
- 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**資產（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。

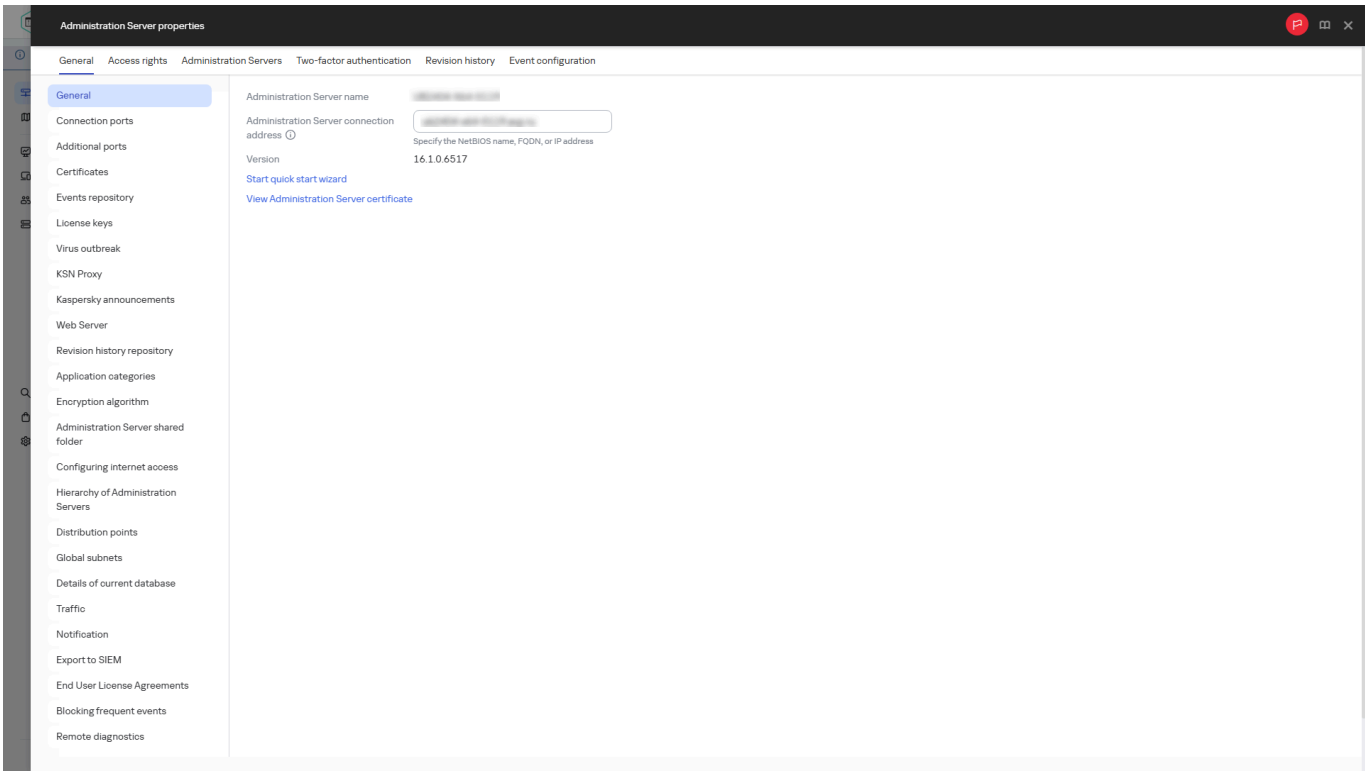
在安裝管理伺服器後，在第一次連線時，應用程式自動提示您執行快速啟動精靈。您還可以在任意時刻手動啟動快速啟動精靈。

要手動啟動快速啟動精靈：

1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在**一般**頁籤，選取**一般**區段。



管理伺服器事件內容視窗

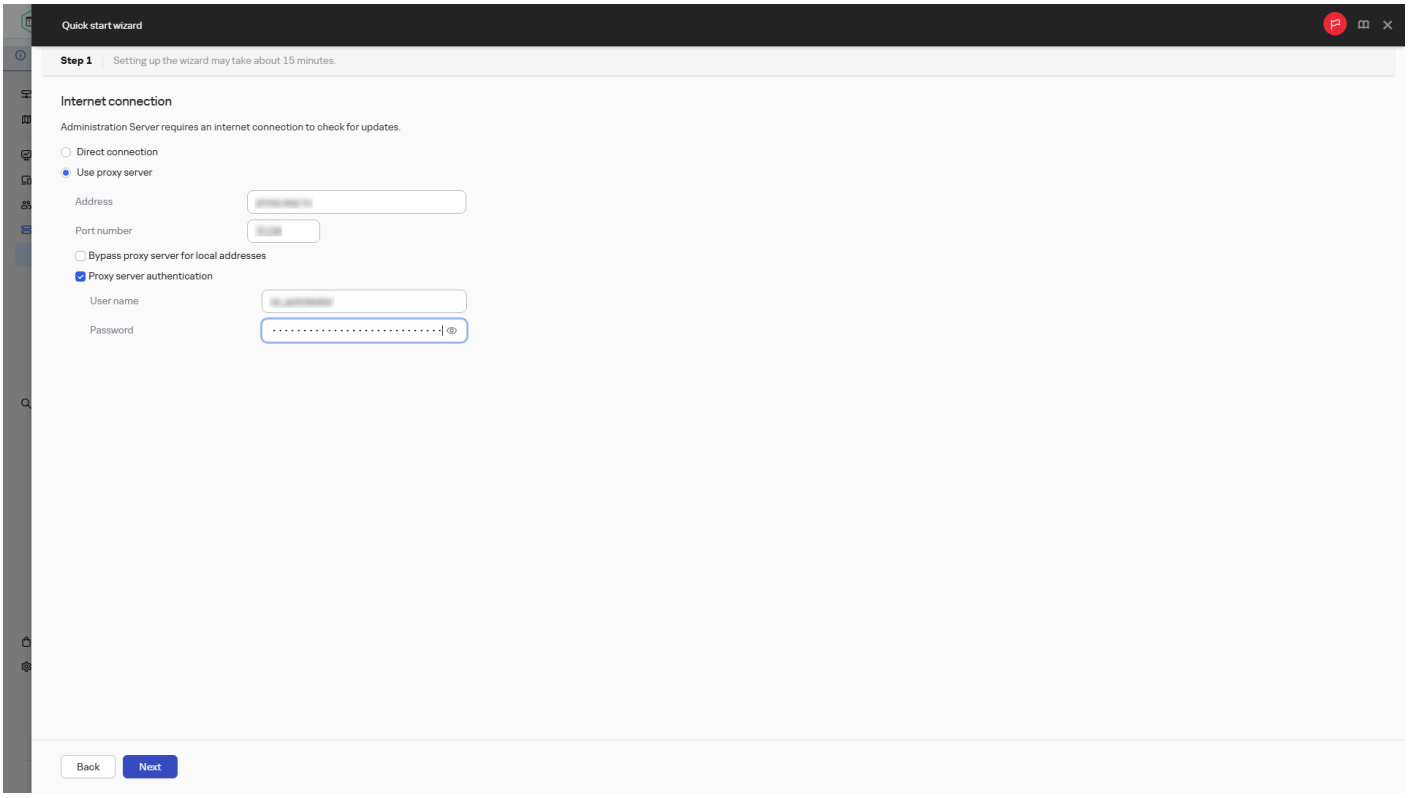
3. 點擊 **開始快速啟動精靈**。

   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 Linux 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：



網際網路連線設定

- **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 Linux 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**

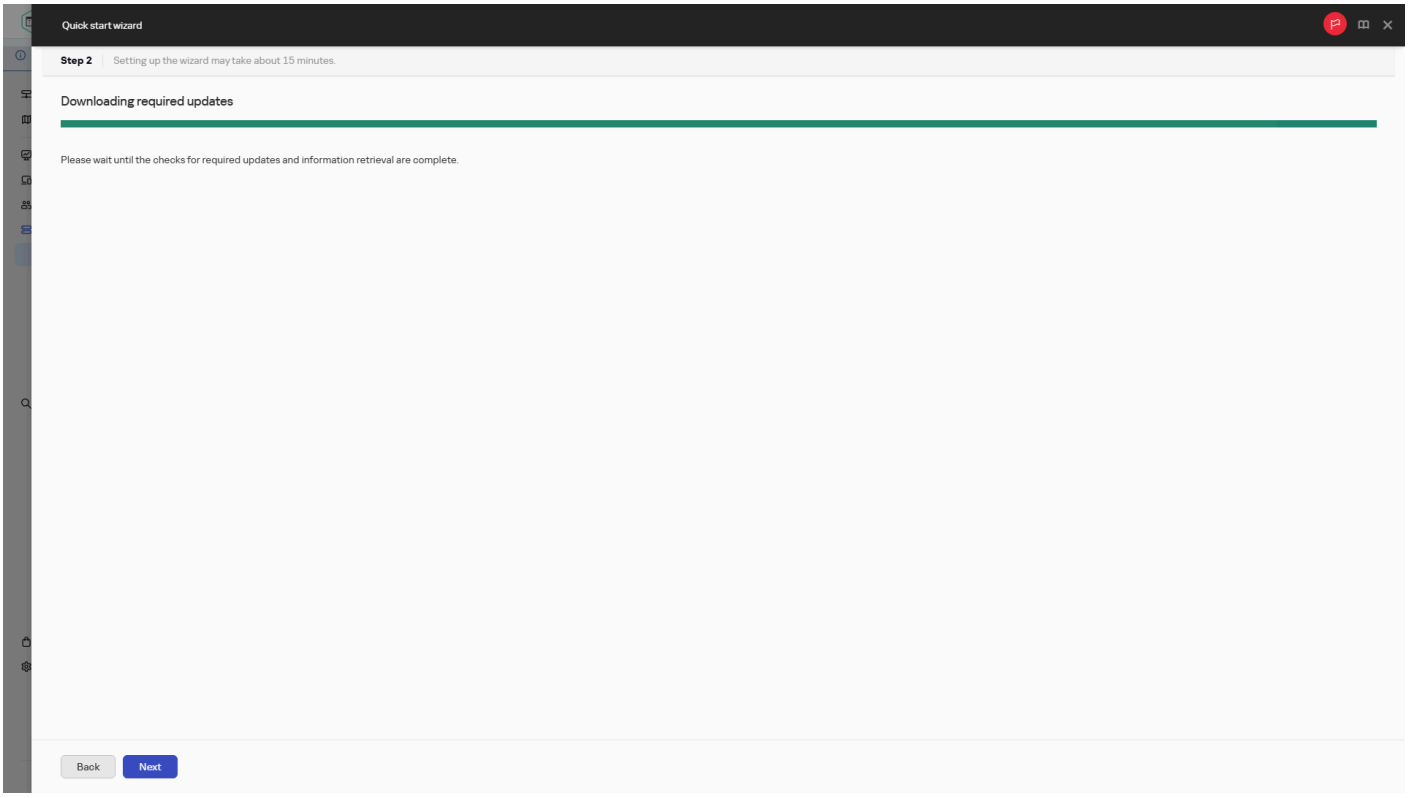
  其帳戶用來建立 Proxy 伺服器連線的使用者所設定的密碼（若選取了**代理伺服器身分驗證**核取方塊，則此欄位可用）。

  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

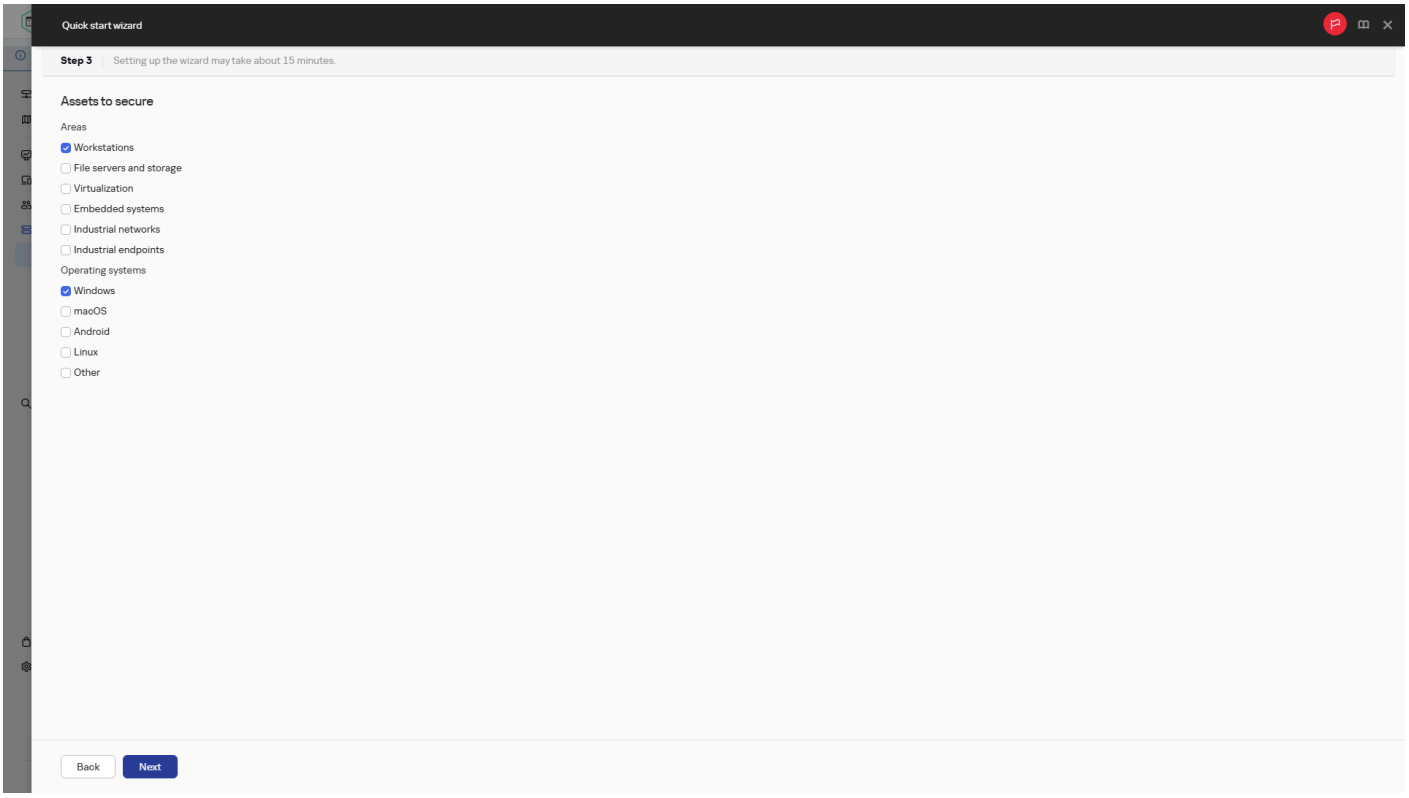
所需更新被從 Kaspersky 伺服器自動下載。



正在下載所需更新

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。



選擇要防護的資產

選取選項：

- **地區**

  您可選取以下防護範圍：

  - **工作站**
  - **檔案伺服器和儲存**
  - **虛擬化**
  - **嵌入式系統**
  - **產業網路**
  - **產業端點**

- **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。

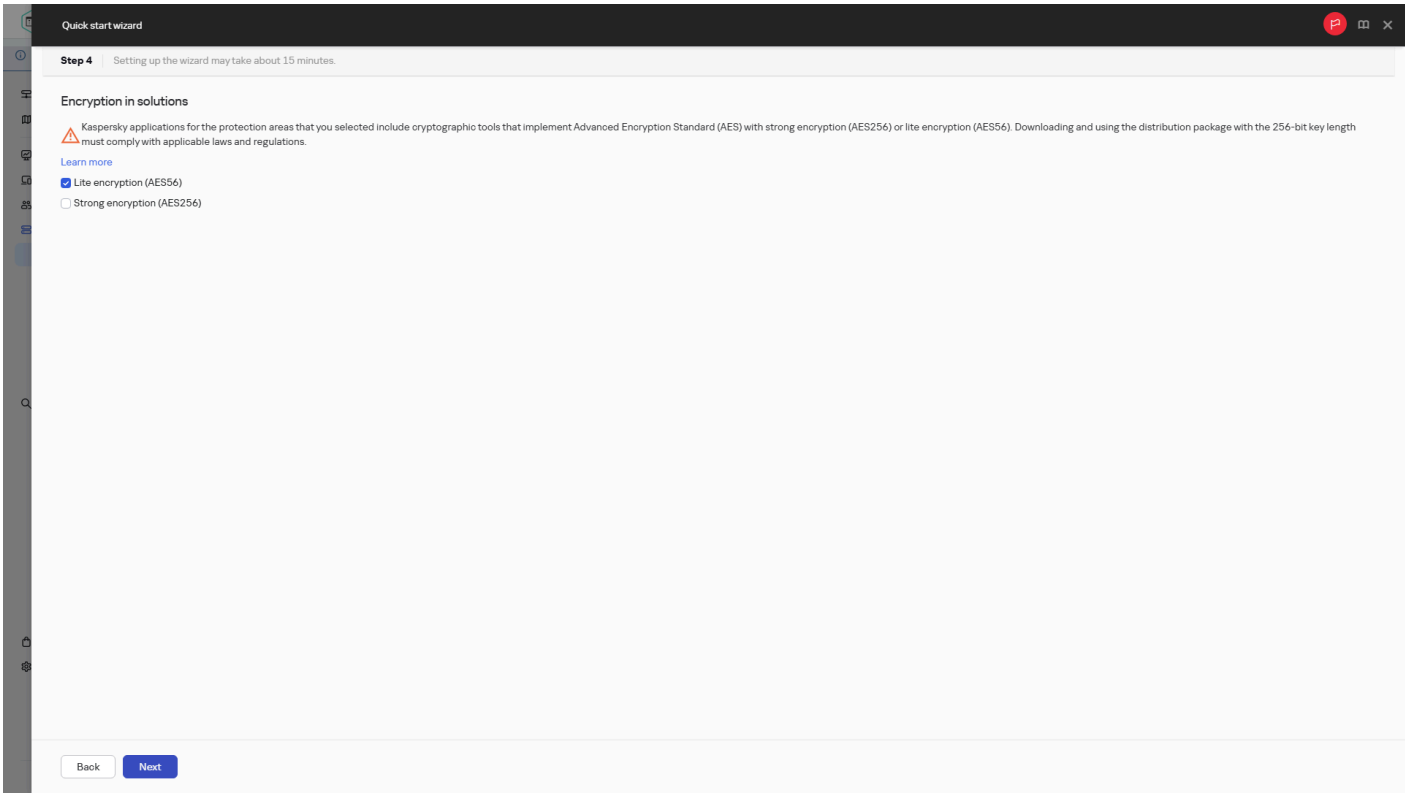
您可以稍後從可用套件清單中選擇卡巴斯基應用程式套件，單獨從快速啟動精靈執行。為了簡化搜尋所需套件的作業，您可以使用各種條件篩選可用套件清單。

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。



在解決方案中選取加密方式

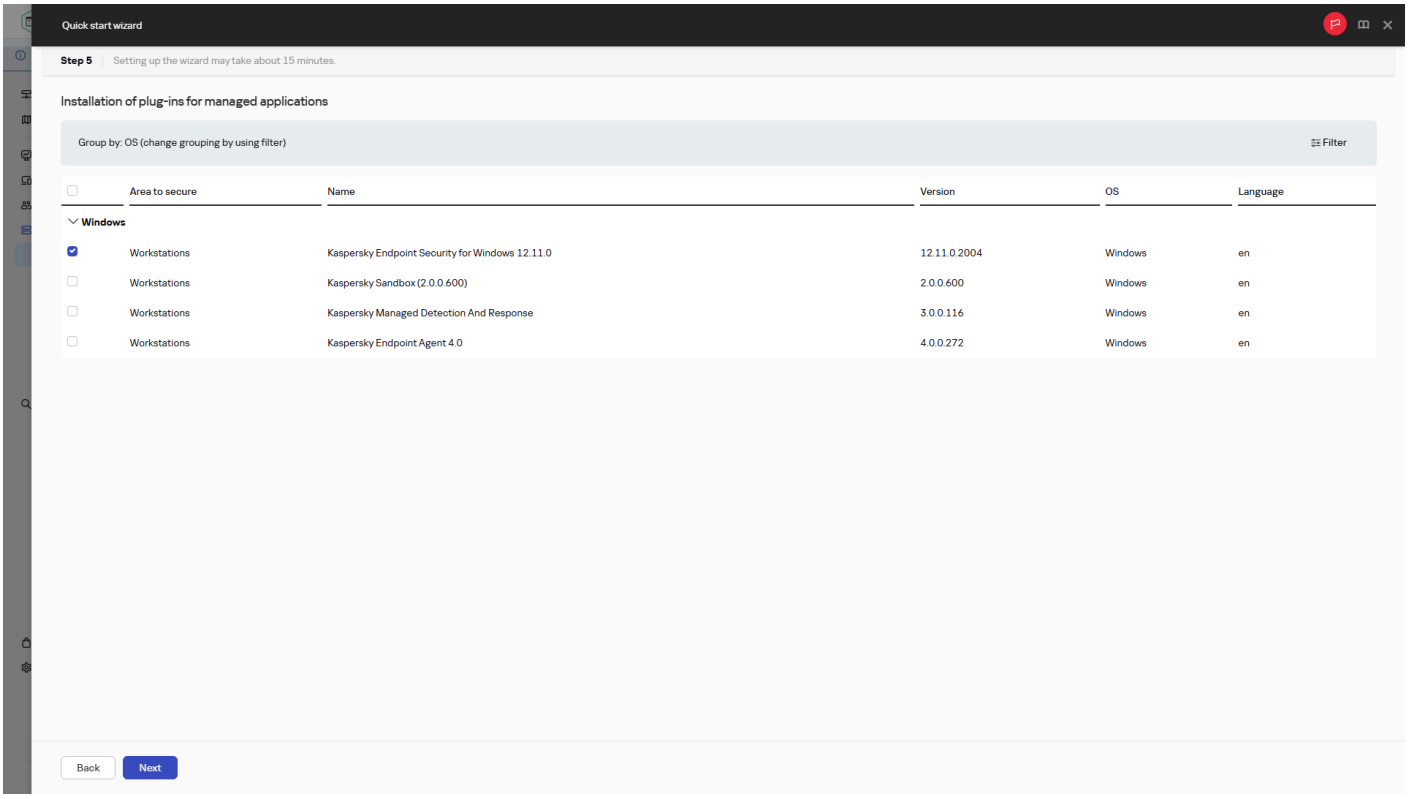
在**加密進行中**視窗中，選取以下加密類型之一：

- 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。



受管理應用程式的外掛程式安裝

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 Linux 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。

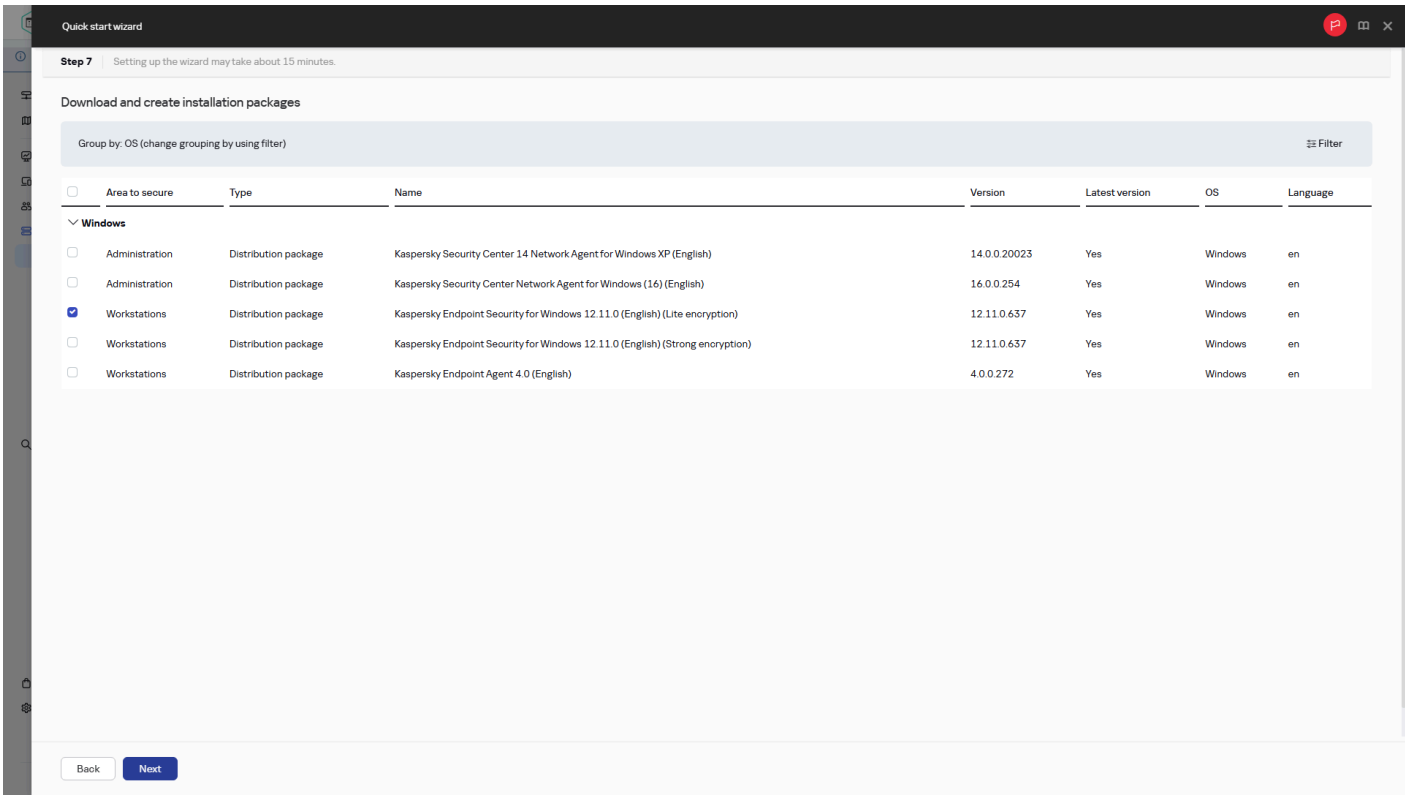
安裝所有選定的外掛程式後，“快速啟動精靈”會自動將您帶到下一步。

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 Linux 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 Linux 語言。如果不存在 卡巴斯基安全管理中心 Linux 語言的應用程式分發套件，則選擇英文分發套件。



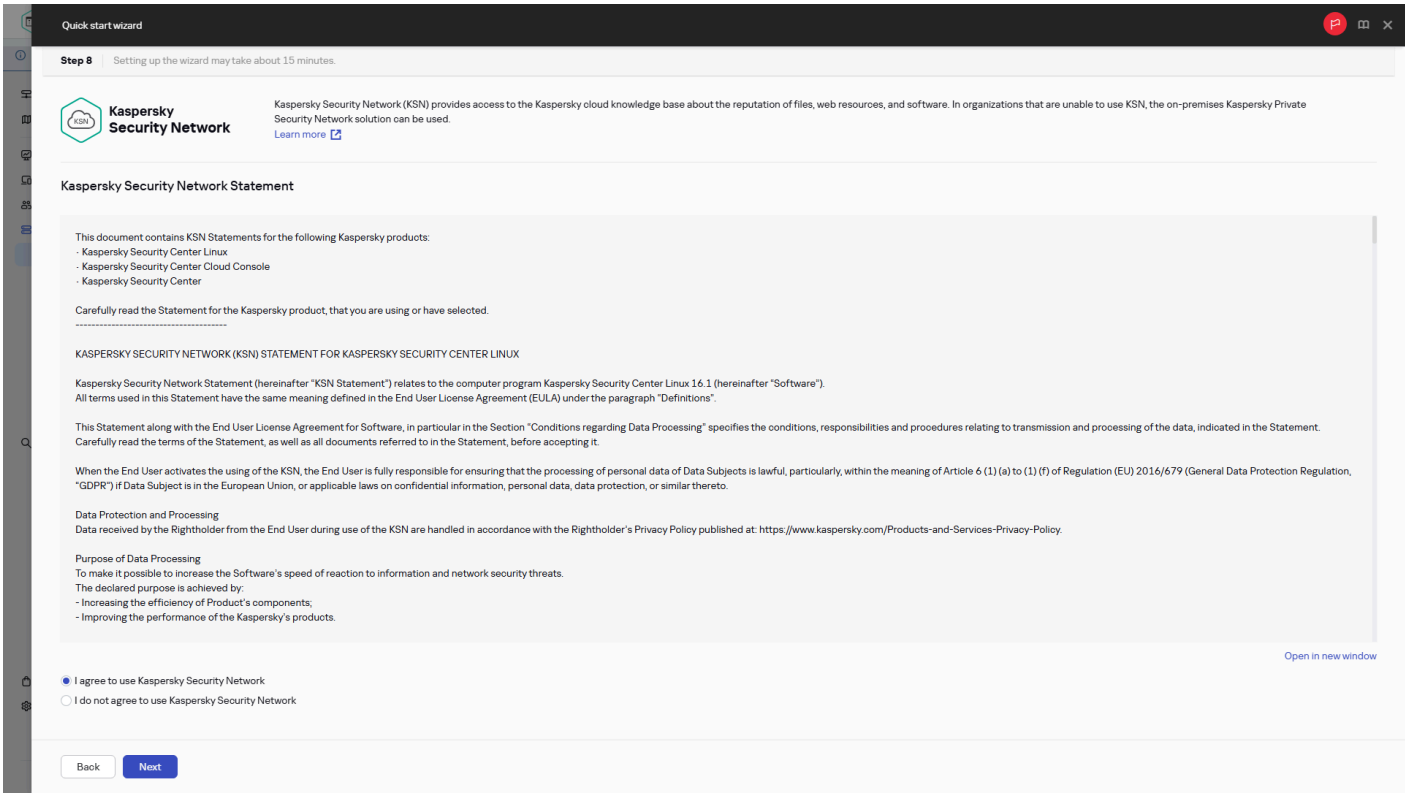
下載分發套件並建立安裝套件

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。

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 Linux 操作資訊到卡巴斯基安全網路知識庫。



設定卡巴斯基安全網路

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 Linux 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 Linux 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

選取以下卡巴斯基安全管理中心 Linux 啟動選項之一：

- **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 Linux。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**自動將授權金鑰佈署至受管理裝置**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，您可以稍後在主功能表的**操作** → **產品授權** → **產品授權**區域中，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。

  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金鑰檔案。

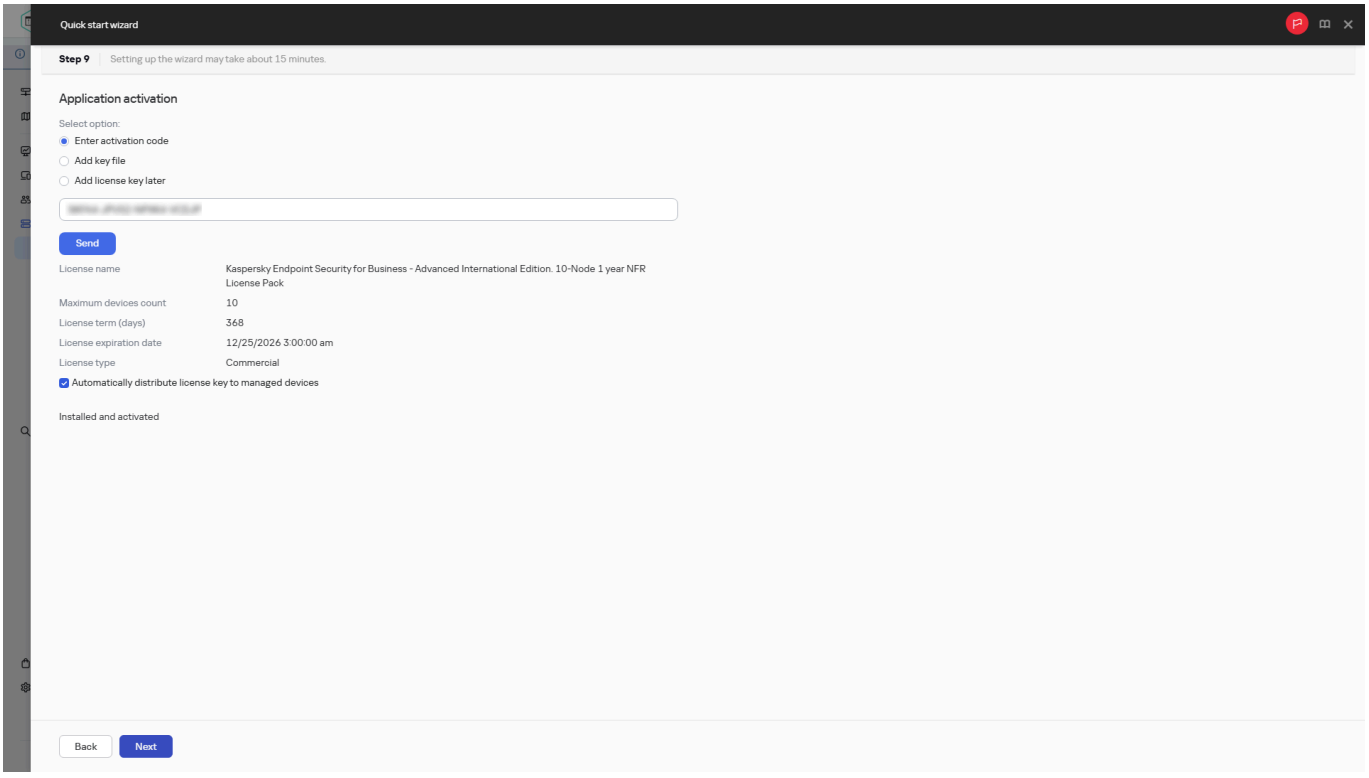
  若使用金鑰檔案啟動程式，您無需連線至 Kaspersky 啟動伺服器。

  若您已選取此啟動選項，就能啟用**自動將授權金鑰佈署至受管理裝置**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，您可以稍後在主功能表的**操作** → **產品授權** → **產品授權**區域中，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



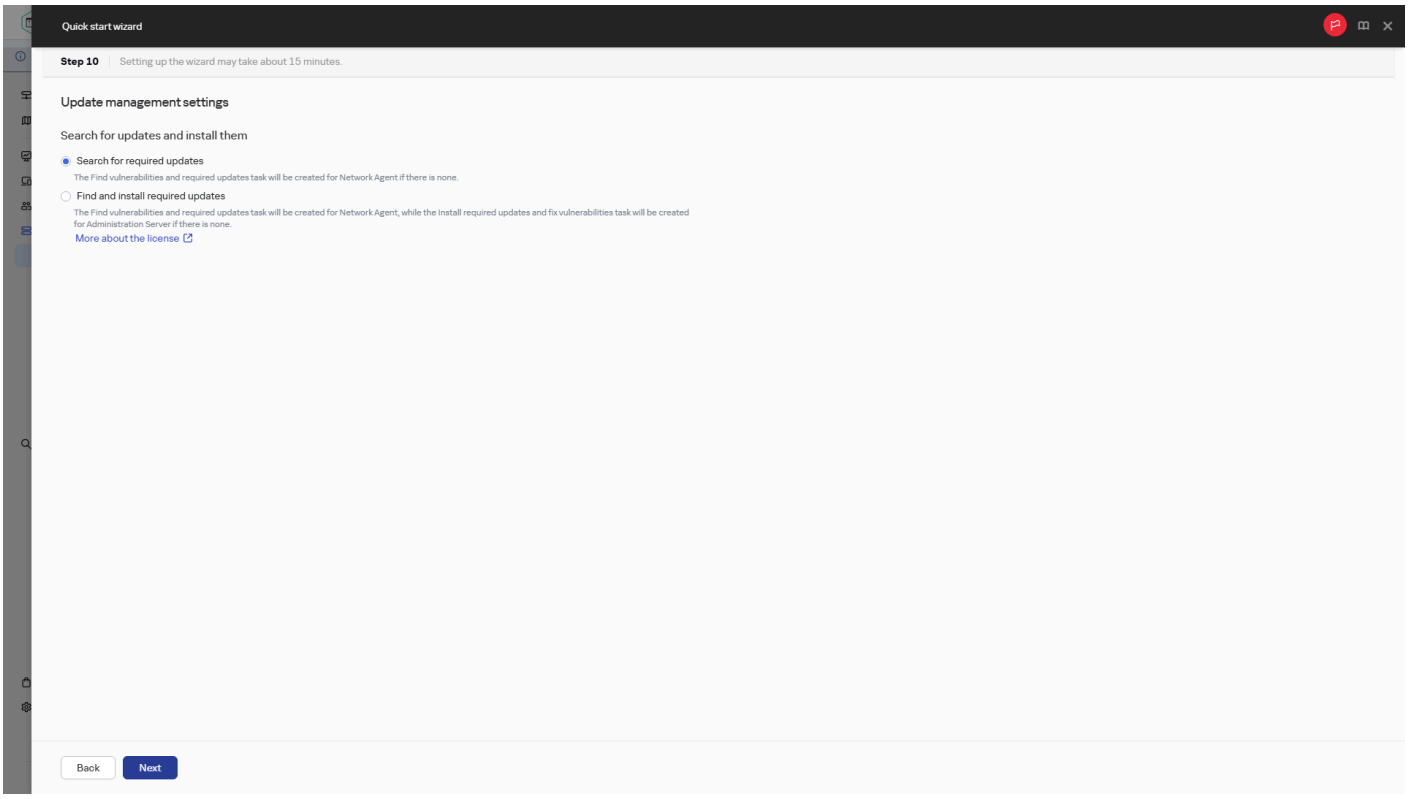
選取應用程式啟動方式

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，則快速啟動精靈的**更新管理設定**步驟不會顯示。



協力廠商更新管理設定

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。

- **尋找並安裝所需更新**

  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，請選取**使用更新網域政策中定義的來源。**

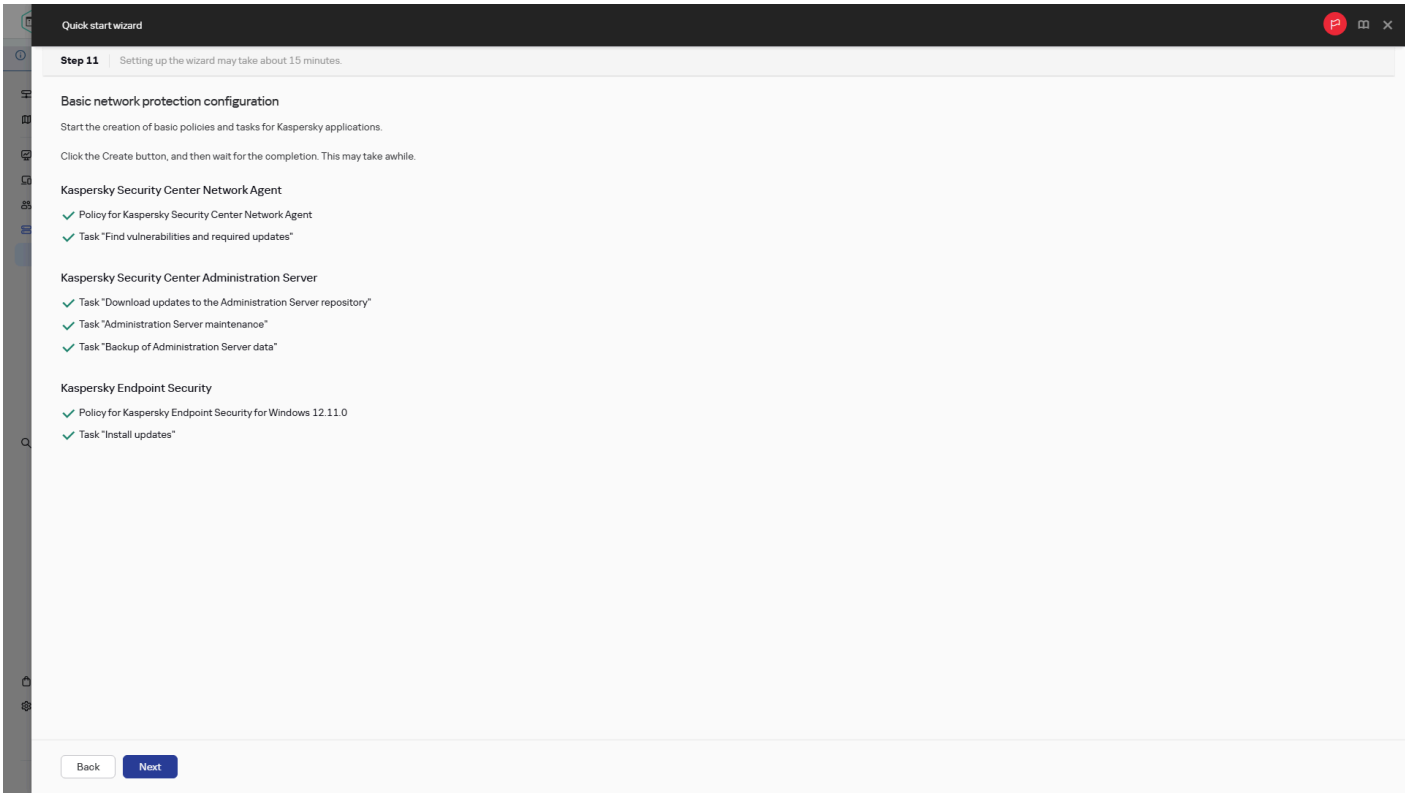
用戶端裝置將會根據網域政策設定下載 Windows Update 更新。若您沒有，會自動建立網路代理政策。

您可以從快速啟動精靈分別建立*弱點掃描和所需更新*和*安裝所需更新並修復弱點*工作。

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。

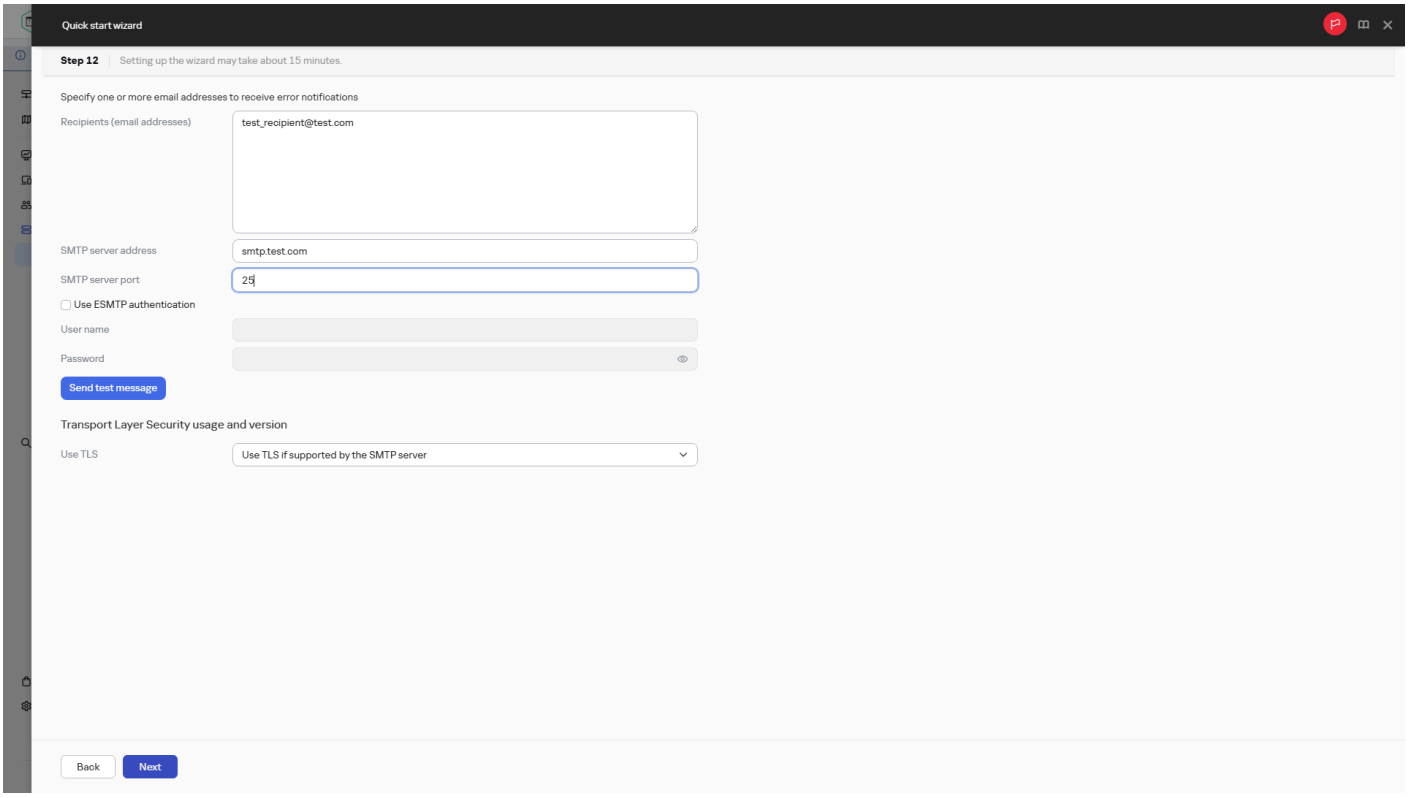
等待政策和工作完成建立，然後轉到精靈的下一步。



建立基本的網路防護設定

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。



設定電子郵件通知

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
  - 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。

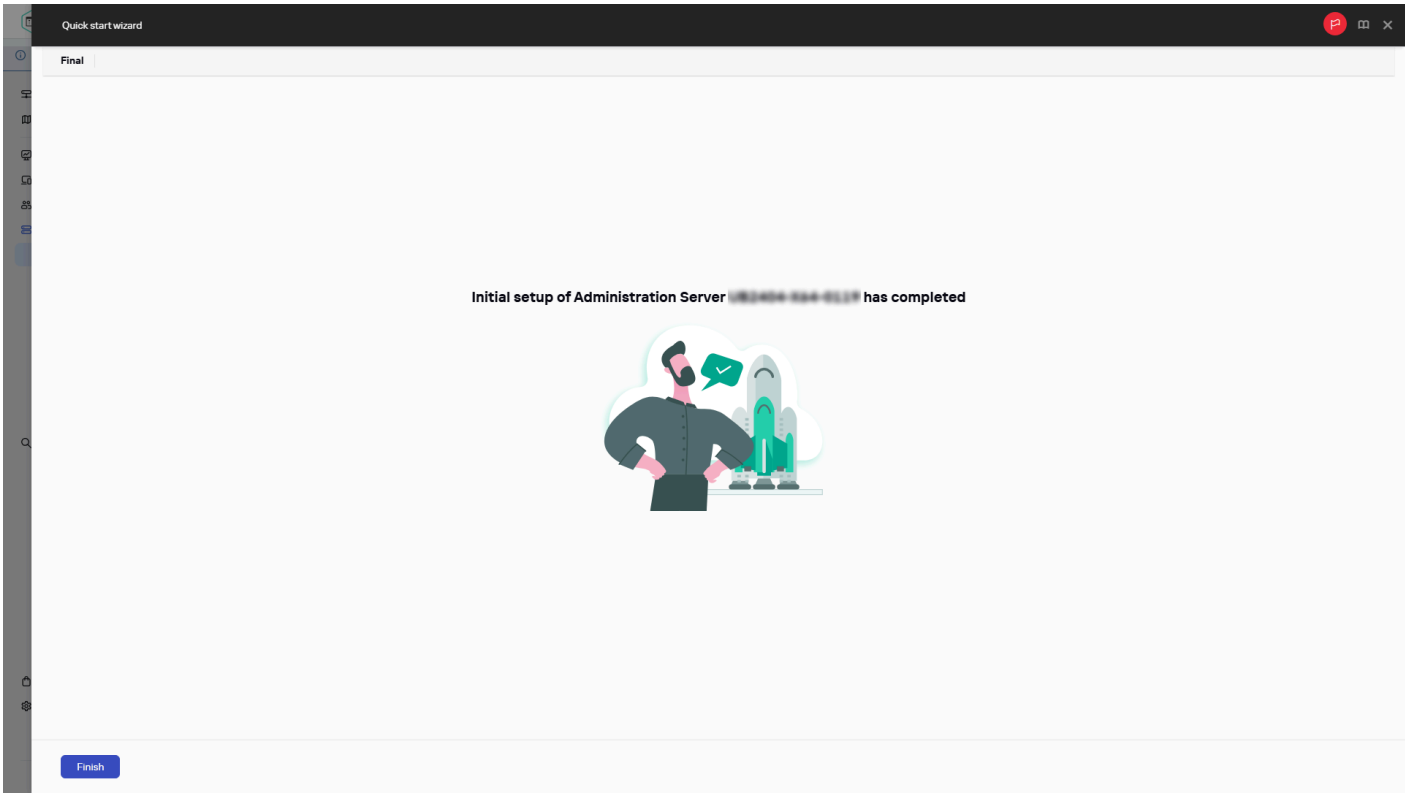
- **使用 ESMTP 身分驗證**

  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。

您可以透過點擊**傳送測試訊息**按鈕測試新郵件通知設定。

步驟 12：關閉快速啟動精靈

要關閉精靈，請點擊**完成**按鈕。



快速啟動精靈的最後一個步驟

完成快速啟動精靈後，您可以執行防護部署精靈以在網路上的裝置上自動安裝防病毒應用程式或網路代理。

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）。安裝套件位於**軟體管理 → 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

您可以隨時手動啟動防護佈署精靈。

要手動啟動防護佈署精靈，

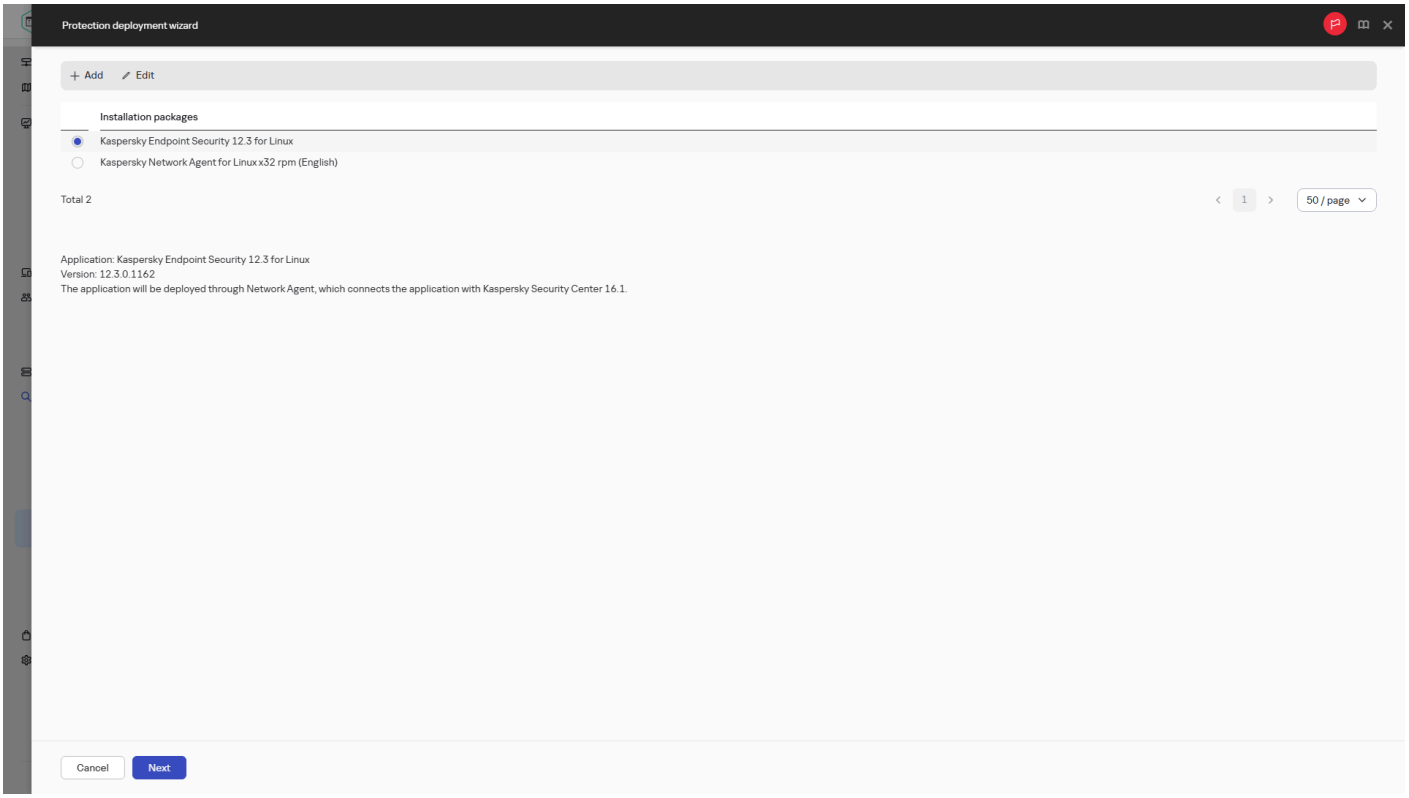
在主功能表中，轉至**發現和佈署 → 佈署和指派 → 防護佈署精靈**。

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。



選取安裝套件

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：

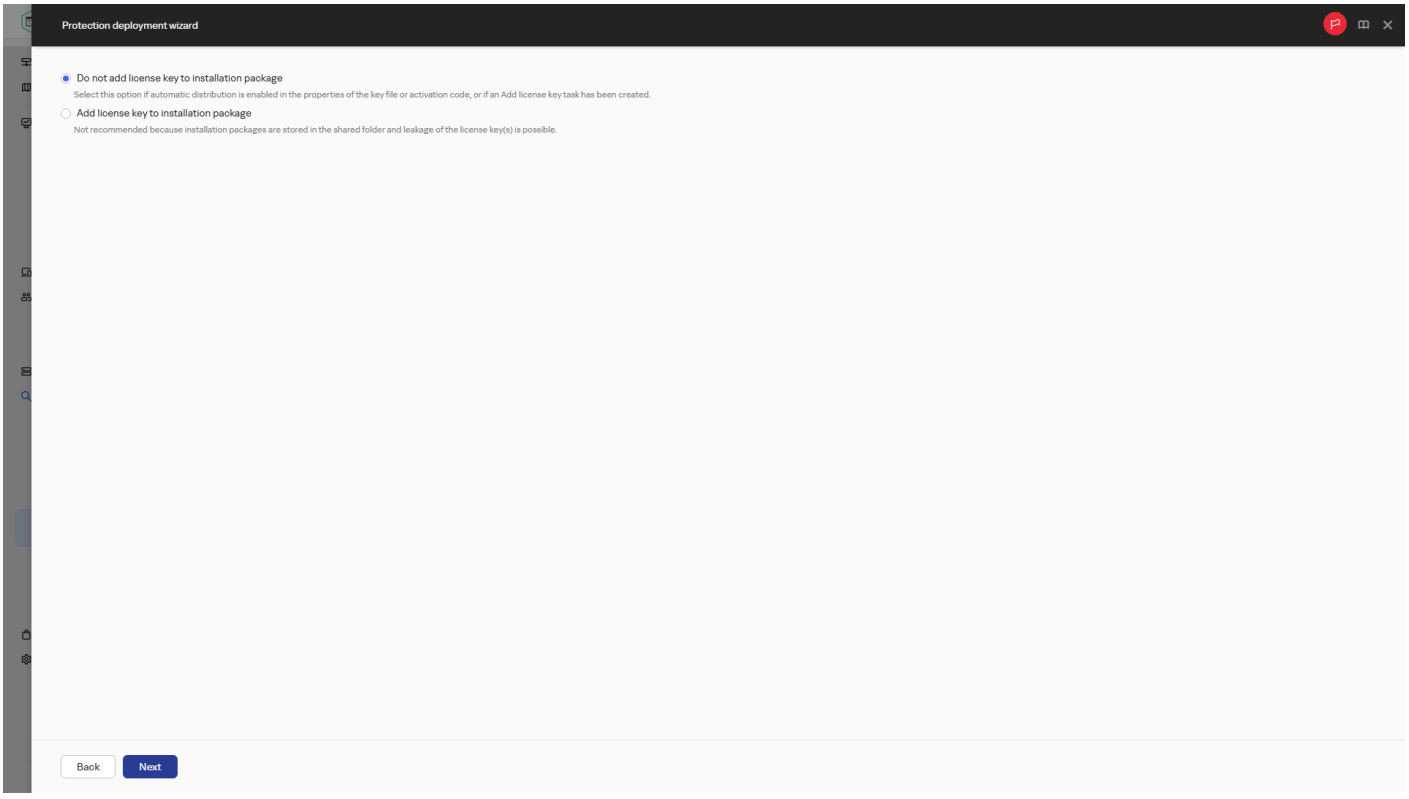
  - 如果自動分發已在金鑰內容中啟用。
  - 如果已建立**新增金鑰**。

- **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。

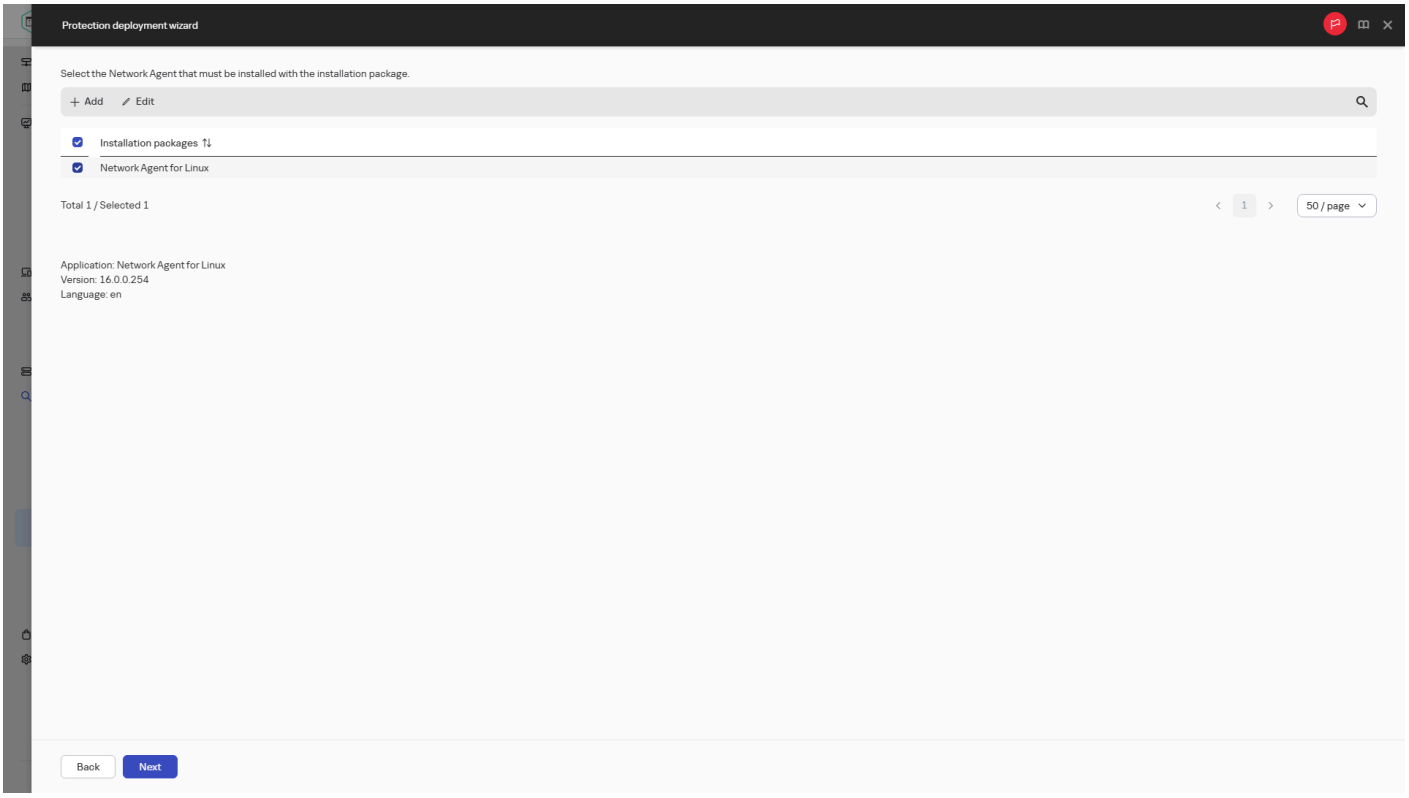


選擇金鑰檔案或啟動碼的分發方式

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。



選取網路代理版本

步驟 5：選取裝置

指定要安裝應用程式的裝置清單：

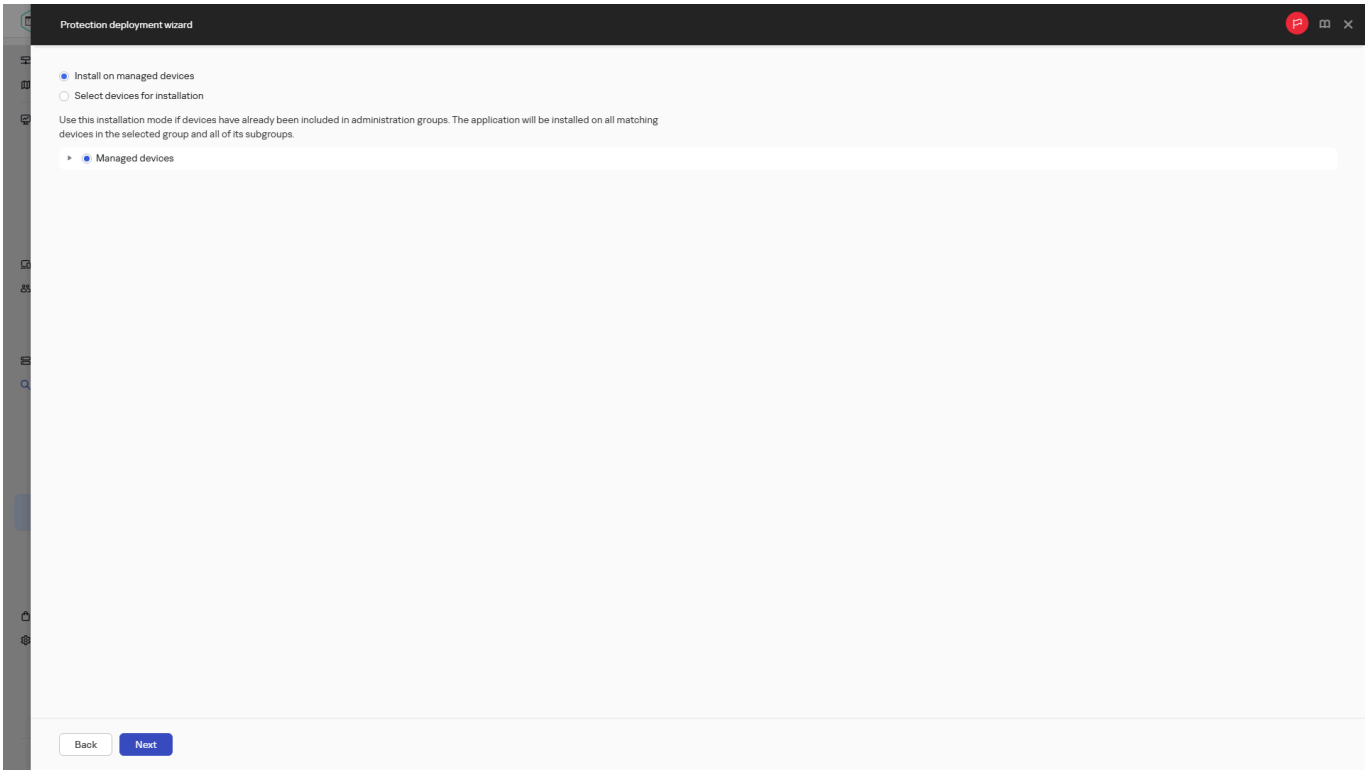
- **安裝到受管理裝置**

  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。



指定要在上面安裝應用程式的裝置清單

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。

  在未安裝網路代理的裝置上安裝 Windows 應用程式（包括 Windows 網路代理）的唯一方法是使用基於 Windows 的發佈點。因此，當您安裝 Windows 應用程式時：

  - 選擇此選項。
  - 確保為目標用戶端裝置分配了發佈點。
  - 確保發佈點基於 Windows。

- **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。

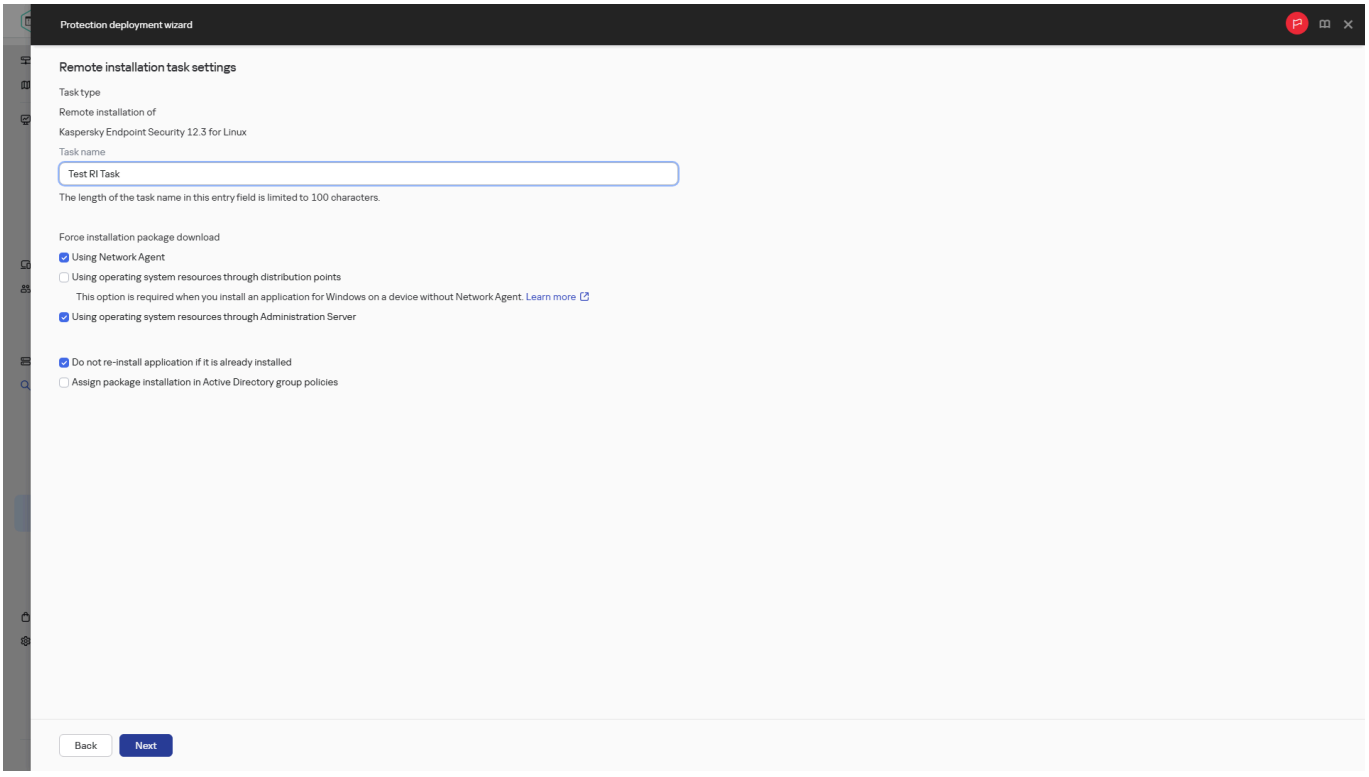
  預設情況下已啟用該選項。

- **在 Active Directory 群組政策中指派安裝套件的安裝**

  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。



指定遠端安裝工作設定

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。

- **提示使用者動作**

  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。

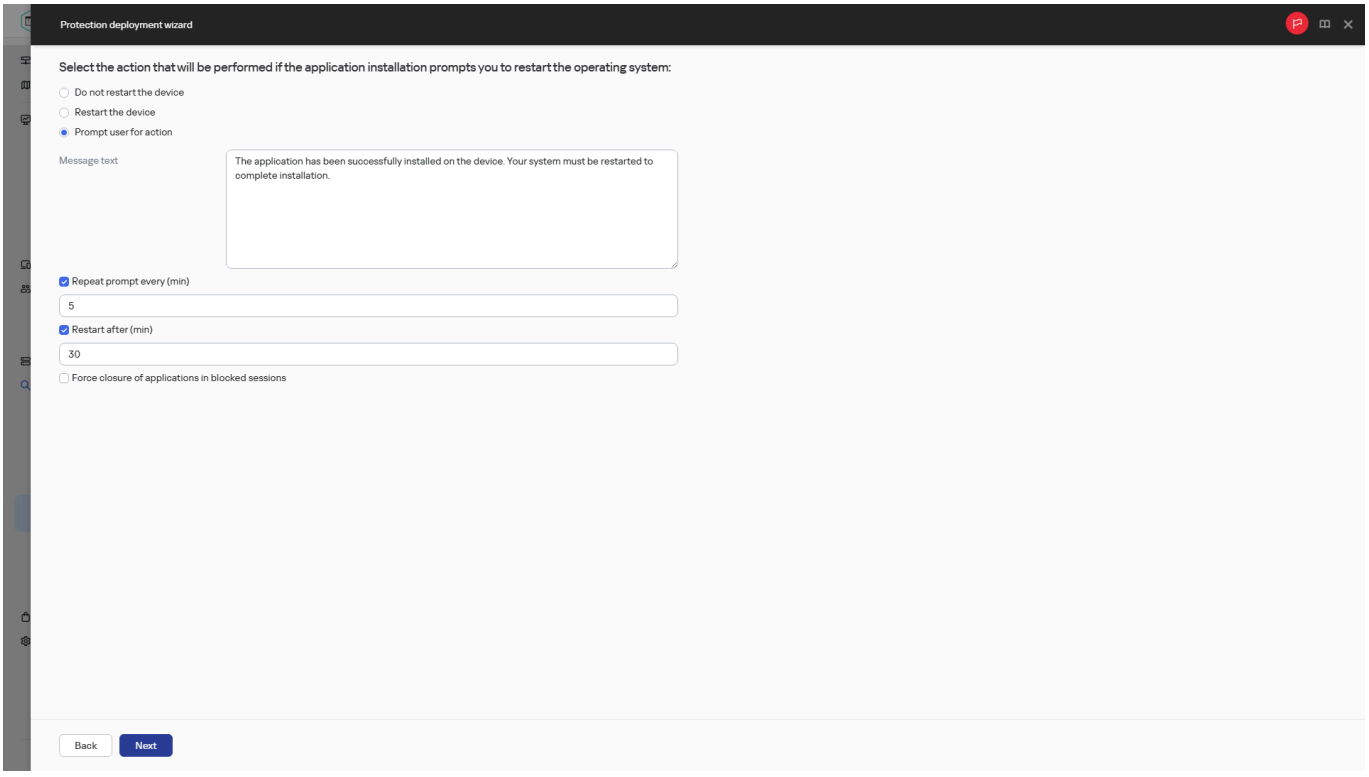
- **強制關閉被封鎖工作階段中的應用程式**

  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。



選取作業系統重新啟動選項

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 Linux 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。

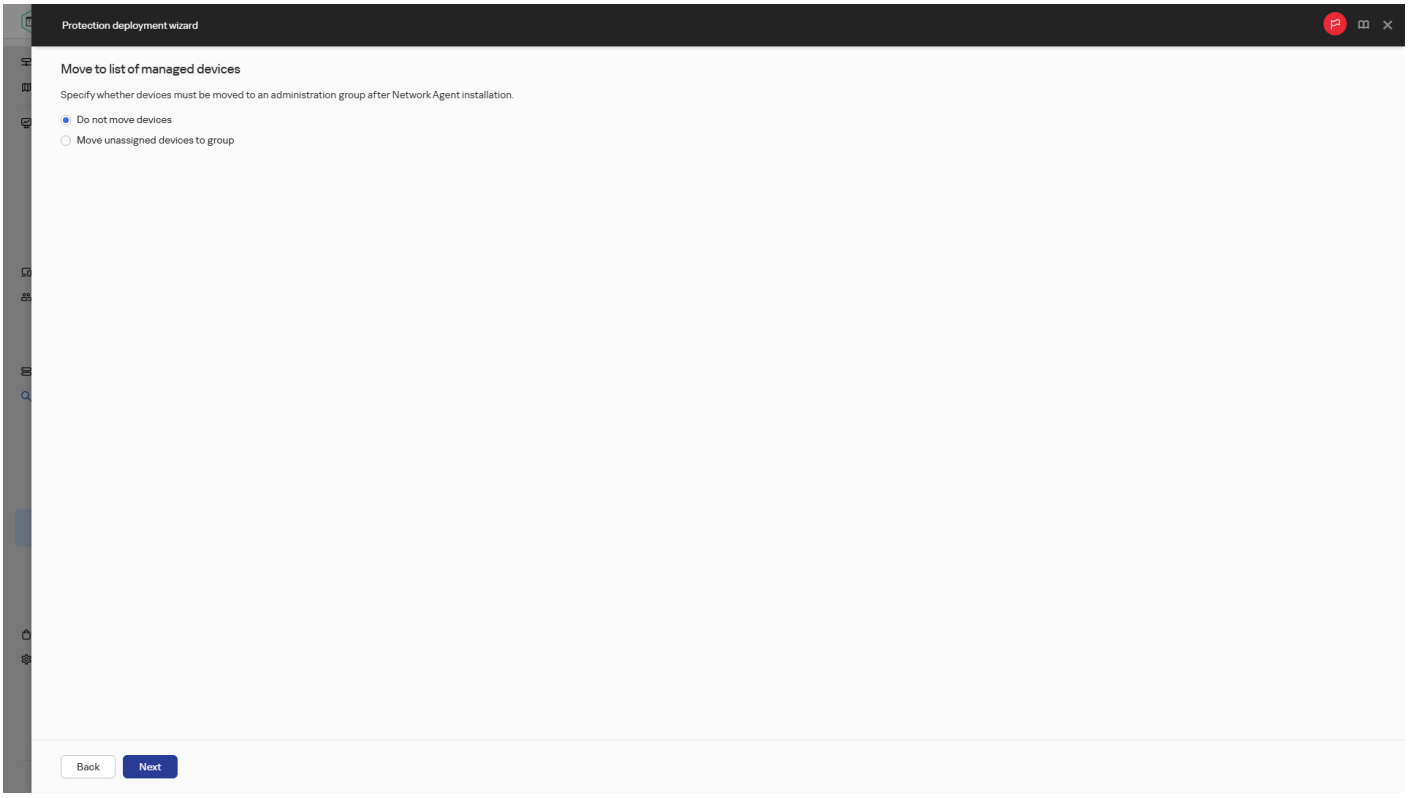
- **不移動裝置**

  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。

- **將未指派的裝置移動到群組**

  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。



選擇將裝置移至管理群組的選項

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，該選項不可用。

- **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。

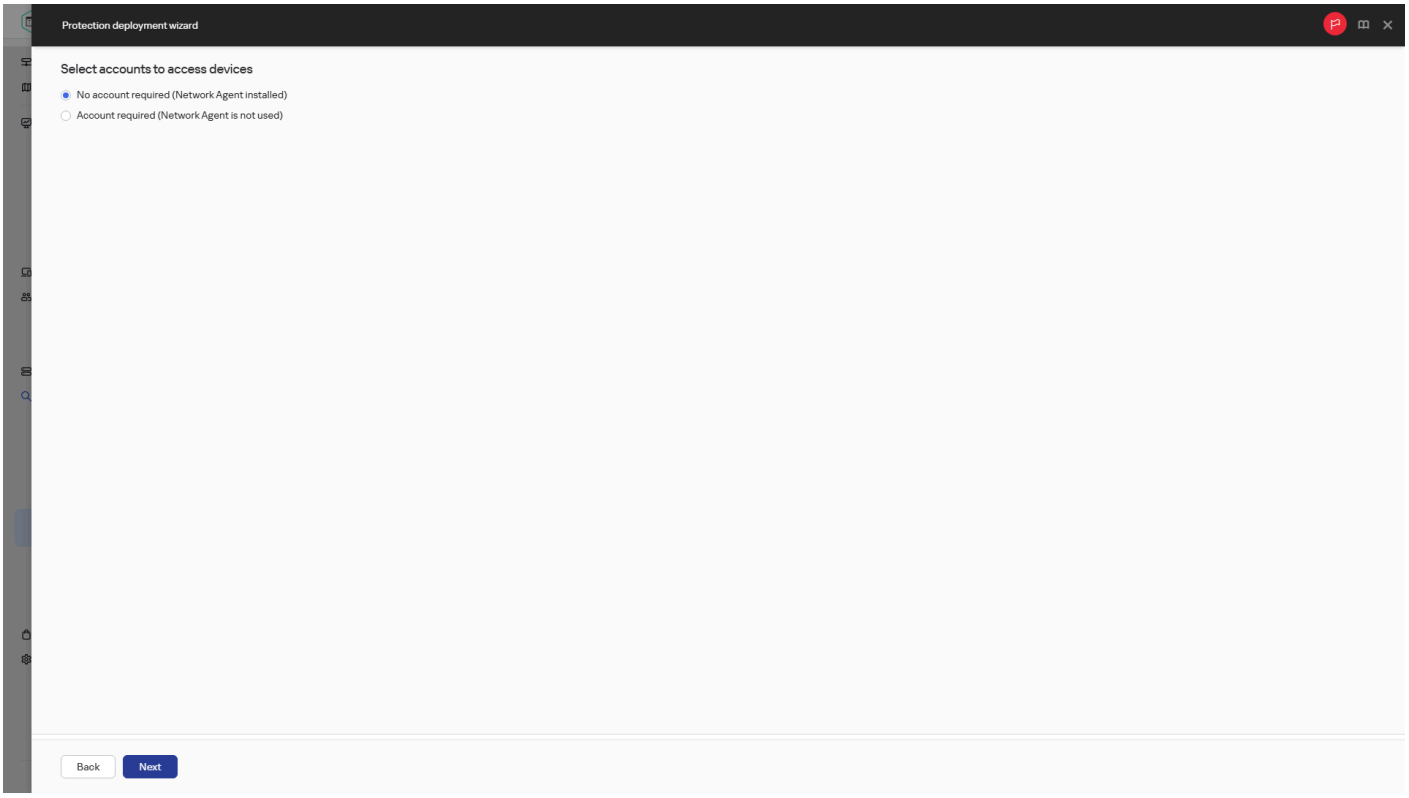
  - **本機或網域帳戶**。如果選取此選項，請指定用於執行應用程式安裝程式的使用者帳戶。點擊**新增**按鈕，選擇**本機或網域帳戶**，然後指定使用者帳戶憑據。

    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 Linux 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 Linux 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 >"
    ```



選取存取裝置的帳戶

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。

升級卡巴斯基安全管理中心 Linux

您可以安裝版本 16.3 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 13 開始）。當升級至版本 16.3 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。

先決條件

- 在開始升級之前建立管理伺服器資料的備份副本。
- 將管理伺服器從 16 或更早版本升級到 16.1 或更高版本時，將啟用雙因素驗證。如需更多資訊，請參閱關於帳戶的雙步驟驗證。

  為確保使用者可以使用已設定的雙因素驗證金鑰透過現有帳戶登入網頁主控台，並確保OpenAPI 自動化指令碼在升級後繼續運行，您必須執行下列步驟：

  - 為所有使用者啟用雙因素驗證
  - 管理員必須為其自己的帳戶設定雙因素驗證
  - 從雙因素驗證中排除所需帳戶

    如有需要，請將用於透過 OpenAPI 執行指令碼的整合帳戶新增至排除清單。
- 請確保您使用管理伺服器版本 16.3 支援的作業系統和 DBMS 版本。如有必要，您可以將管理伺服器移至具有更高版本作業系統和 DBMS 的另一台裝置。
- 將管理伺服器從 15.4 或更早版本升級到 16 或更高版本時，請在 DBMS 伺服器上為 IAM 建立一個資料庫。資料庫名稱必須與您為卡巴斯基安全管理中心 Linux 安裝的資料庫名稱不同。

  - 對於 PostgreSQL，執行以下命令：

    ```
    sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
    ```

  - 對於 MariaDB，執行以下命令：

    ```
    sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
    ```
- 將管理伺服器從 15.4 或更早版本升級到 16 或更高版本時，請準備包含 IAM 新參數的應答檔案。有關所需參數的清單，請參閱文章以靜默模式安裝卡巴斯基安全管理中心 Linux。新增 `KLAUTOANSWERS` 環境變數，並將其值設為應答檔案的路徑。
- 確保用於 OpenID Connect 通訊協定身分驗證的 kliam 處理程序的連接埠處於可用狀態。預設為 4444。請參閱以下文章中的 `trusted` 參數說明：卡巴斯基安全管理中心網頁主控台安裝參數。

階段

1. **管理伺服器的升級**

您可以使用以下方法之一升級管理伺服器版本：

- 透過使用卡巴斯基安全管理中心 Linux 安裝檔案
- 透過建立管理伺服器資料備份，安裝新的管理伺服器版本，從備份中還原管理伺服器資料

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。

如果您的網路包含多個管理伺服器，則必須手動升級每個伺服器。卡巴斯基安全管理中心 Linux 不支援集中升級。

2. **執行 postinstall.pl 指令碼（可選步驟）**

如果應答檔案不包含 IAM 參數或未找到應答檔案，則升級期間終端中會顯示一則訊息，要求您執行 postinstall.pl 指令碼。

在方案的此步驟中，進行以下操作：

1. 在管理伺服器作業系統中，建立一個未獲授權的使用者帳戶「ksciam」，該帳戶必須是「kladmins」群組成員：

```
adduser ksciam

gpasswd -a ksciam kladmins

usermod -g kladmins ksciam
```

2. 在具有 root 權限的帳戶下，執行 /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl 指令碼來設定升級後的管理伺服器。出現提示時，輸入以下設定：

   1. 輸入 IAM 伺服器 FQDN。必須使用安裝卡巴斯基安全管理中心 Linux 時指定的管理伺服器 DNS 名稱。
   2. 輸入帳戶名稱以啟動 IAM 服務。該帳戶必須是輸入的安全群組的成員。預設情況下，使用“ksciam”帳戶。
   3. 選取為與 IAM 服務搭配使用而安裝的 DBMS：
      - 如果您安裝了 MySQL 或 MariaDB，請輸入 1。
      - 如果您安裝了 PostgreSQL 或 Postgres Pro，請輸入 2。
   4. 輸入IAM 服務要使用的 IAM DBMS 位址。
   5. 輸入 IAM DBMS 連接埠號。此連接埠用於與 IAM 服務通訊。預設情況下，使用以下連接埠：
      - 連接埠 3306 用於 MySQL 或 MariaDB
      - 連接埠 5432 用於 PostgreSQL 或 Postgres Pro
   6. 輸入IAM 服務要使用的 IAM 資料庫名稱。IAM 服務所使用的資料庫名稱應與管理伺服器所使用的資料庫名稱不同。

3. **將卡巴斯基安全管理中心網頁主控台升級到新版本。**

4. **（可選）將裝置上的網路代理程式升級到新版本。**

5. **確保雙因素驗證允許清單僅包含必須有權存取管理伺服器的使用者帳戶。**

審核雙因素驗證允許清單，從中刪除任何其他帳戶。

請注意，如果您將管理伺服器升級到版本 16.3，則將無法建立網路代理版本 15 或更早版本的新安裝套件。但是，將可使用先前建立的安裝套件。

從先前版本升級卡巴斯基安全管理中心 Linux 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。

升級Kaspersky Security Center for Linux 16或更高版本

本節介紹將卡巴斯基安全管理中心 Linux 從版本 16 或更高版本升級到最新版本的以下選項：

- 使用安裝檔案進行升級
- 透過備份進行升級
- 在Kaspersky Security Center for Linux故障轉移叢集節點上升級

使用安裝檔案將卡巴斯基安全管理中心 Linux 從版本 16 或更高版本進行升級

要將管理伺服器從版本16或更高版本升級到最新版本，您可以使用Kaspersky Security Center for Linux安裝檔案在早期版本上安裝新版本。

若要使用安裝檔案將卡巴斯基安全管理中心 Linux 從 16 或更高版本升級至最新版本：

1. 從卡巴斯基網站下載包含版本 16.3 的完整套件的 卡巴斯基安全管理中心 Linux 安裝檔案：
   - 對於執行基於 RPM 的作業系統的裝置—`ksc64-<version number>.x86_64.rpm`
   - 對於執行基於 Debian 的作業系統的裝置—`ksc64_<version number>_amd64.deb`
2. 開始升級Kaspersky Security Center for Linux。在命令列終端中執行以下一項命令：
   - 對於執行基於 RPM 的作業系統的裝置：

     ```
     sudo yum install ./ksc64-<version number>.x86_64.rpm
     ```

   - 對於執行基於 Debian 的作業系統的裝置：

     ```
     sudo apt-get install ./ksc64_<version number>_amd64.deb
     ```

   成功執行命令後，會建立 `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` 指令碼。相關訊息將顯示在終端中。
3. 執行 `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` 指令碼，以設定升級後的管理伺服器：

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

4. 閱讀命令行終端中顯示的產品授權協議和隱私權政策。如果您同意產品授權協議和隱私權政策的所有條款：

   a. 輸入 `Y` 以確認您已完整閱讀、理解並接受 EULA 的條款和條件。

   b. 再次輸入 `Y` 以確認您已完整閱讀、理解並接受描述資料處理的隱私權政策。

   在您兩次輸入 `Y` 後，您裝置上的應用程式安裝將繼續。

5. 輸入 `1` 以選擇標準管理伺服器安裝模式。

   下圖顯示了最後兩個步驟。

```
Enter 'Y' to confirm that you understand and accept the terms of the End
User License Agreement (EULA). You must accept the terms and conditions of
the EULA to install the application. Enter 'N' providing you do not accept
the terms of the EULA or 'R' to view it again [N]:
y

Enter 'Y' to confirm that you accept the terms of the Privacy Policy. You
must accept the terms and conditions of the Privacy Policy to install the
application. Entering 'Y' means that you are aware that your data will be
handled and transmitted (including to third countries) as described in the
Privacy Policy. Enter 'N' providing you do not accept the Privacy Policy
[N]:
y

Choose the Administration Server installation mode:
1) Standard
2) Primary cluster node
3) Secondary cluster node
Enter the range number (1, 2, or 3) [1]:
```

接受 EULA 和隱私權政策的條款，並在命令行終端中選擇標準的管理伺服器安裝模式

   下一步，指令碼將配置和完成升級管理伺服器。升級期間，您不可以變更升級之前調整過的管理伺服器設定。

6. 將卡巴斯基安全管理中心網頁主控台升級到新版本。

7. 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 Linux 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：

     ```
     sudo apt-get -y autoremove
     sudo apt -y autoremove
     ```

   - 對於基於 RPM 的資產，執行以下命令之一：

     ```
     sudo dnf autoremove
     sudo yum autoremove
     ```

透過備份將卡巴斯基安全管理中心 Linux 從版本 16 或更高版本進行升級

要將管理伺服器從版本16或更高版本升級到最新版本，您可以建立管理伺服器資料的備份，並在安裝新版本的Kaspersky Security Center for Linux後恢復此資料。如果在安裝過程中發生問題，您可以利用升級前所建立的管理伺服器資料備份還原先前版本的管理伺服器。

若要透過備份將卡巴斯基安全管理中心 Linux 從 16 或更高版本升級到最新版本：

1. 升級前，請使用舊版本的應用程式備份管理伺服器資料。

2. 解除安裝舊版本的 卡巴斯基安全管理中心 Linux。

3. 在先前安裝了管理伺服器的裝置上安裝卡巴斯基安全管理中心 Linux 版本 16.3 。

   如果備份副本中的資料庫結構描述與管理伺服器或 IAM 目前使用的結構描述不同，資料將會還原至目前的結構描述。

   如果備份副本中使用 public 結構描述，則必須符合以下條件：

   - 資料庫中存在 public 資料庫結構描述。

   - 您可以使用管理伺服器或 IAM 用於存取資料庫的 DBMS 帳戶，修改 public 資料庫結構描述。

   否則，資料還原會因錯誤而結束。

4. 從升級前建立的備份還原管理伺服器資料。

5. 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。

6. 對於安裝了更早版本網路代理的裝置，建立並執行新版本網路代理的遠端安裝工作。

   > 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 Linux 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：

     ```
     sudo apt-get -y autoremove
     sudo apt -y autoremove
     ```

- 對於基於 RPM 的資產，執行以下命令之一：

```
sudo dnf autoremove
sudo yum autoremove
```

在Kaspersky Security Center for Linux故障轉移叢集節點上升級Kaspersky Security Center for Linux 16或更高版本

您可以在每個已安裝管理伺服器版本 16 或更高版本的卡巴斯基安全管理中心 Linux 容錯移轉叢集節點上安裝最新版本的管理伺服器。升級到最新版本時，上一版本的管理伺服器的所有資料和設定將會保留。

如果您之前在裝置上本機安裝了 卡巴斯基安全管理中心 Linux，您還可以透過使用安裝檔案或透過備份在這些裝置上升級 卡巴斯基安全管理中心 Linux。

若要在Kaspersky Security Center for Linux故障轉移叢集節點上升級Kaspersky Security Center for Linux 16或更高版本：

1. 從卡巴斯基網站下載包含版本 16.3 的完整套件的 卡巴斯基安全管理中心 Linux 安裝檔案：
   - 對於執行基於 RPM 的作業系統的裝置—`ksc64-<version number>-<build number>.x86_64.rpm`
   - 對於執行基於 Debian 的作業系統的裝置—`ksc64_<version number>-<build number>_amd64.deb`
2. 停止叢集。
3. 在叢集的活動節點上，在命令列終端中執行以下命令來執行升級：
   - 對於執行基於 RPM 的作業系統的裝置：

     ```
     sudo yum install ./ksc64-<version number>-<build number>.x86_64.rpm
     ```

   - 對於執行基於 Debian 的作業系統的裝置：

     ```
     sudo apt-get install ./ksc64_<version number>-<build number>_amd64.deb
     ```

   成功執行命令後，會建立 `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` 指令碼。相關訊息將顯示在終端中。
4. 執行 `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` 指令碼，以設定升級後的管理伺服器：

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. 閱讀命令行終端中顯示的產品授權協議和隱私權政策。如果您同意產品授權協議和隱私權政策的所有條款：
   a. 輸入 `Y` 以確認您已完整閱讀、理解並接受 EULA 的條款和條件。
   b. 再次輸入 `Y` 以確認您已完整閱讀、理解並接受描述資料處理的隱私權政策。

在您兩次輸入 `Y` 後，您裝置上的應用程式安裝將繼續。

6. 透過輸入 `2` 選擇要升級的節點。

   下圖顯示了最後兩個步驟。

```
Enter 'Y' to confirm that you understand and accept the terms of the End
User License Agreement (EULA). You must accept the terms and conditions of
the EULA to install the application. Enter 'N' providing you do not accept
the terms of the EULA or 'R' to view it again [N]:
y

Enter 'Y' to confirm that you accept the terms of the Privacy Policy. You
must accept the terms and conditions of the Privacy Policy to install the
application. Entering 'Y' means that you are aware that your data will be
handled and transmitted (including to third countries) as described in the
Privacy Policy. Enter 'N' providing you do not accept the Privacy Policy
[N]:
y

Choose the Administration Server installation mode:
1) Standard
2) Primary cluster node
3) Secondary cluster node
Enter the range number (1, 2, or 3) [1]:
```

接受 EULA 和隱私權政策的條款，並在命令行終端中選擇安裝模式

   下一步，指令碼將配置和完成升級管理伺服器。升級期間，您不可以變更升級之前調整過的管理伺服器設定。

7. 在被動節點上執行步驟 3–5。

   在第 6 步中，輸入 `3` 以選擇節點。

8. 啟動叢集。

   > 您可以在任何節點上啟動叢集。如果在被動節點上啟動叢集，它將成為主動節點。

9. 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網路代理程式升級到與Kaspersky Security Center for Linux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：

     ```
     sudo apt-get -y autoremove
     sudo apt -y autoremove
     ```

   - 對於基於 RPM 的資產，執行以下命令之一：

     ```
     sudo dnf autoremove
     sudo yum autoremove
     ```

   結果，您在卡巴斯基安全管理中心 Linux 容錯移轉叢集節點上安裝了最新版本的管理伺服器。

升級Kaspersky Security Center for Linux 15.4或更早版本

本節介紹將卡巴斯基安全管理中心 Linux 從 15.4 或更早版本升級到 16 或更高版本的以下選項：

- 使用安裝檔案進行升級
- 透過備份進行升級
- 在Kaspersky Security Center for Linux故障轉移叢集節點上升級

卡巴斯基安全管理中心 Linux 從 15.4 或更早版本升級到 16 或更高版本的每個選項都包括在 DBMS 伺服器上建立和設定IAM 資料庫、建立非特權“ksciam”帳戶來執行 IAM 服務以及將此帳戶新增至“kladmins”安全群組的步驟。

使用安裝檔案將卡巴斯基安全管理中心 Linux 從 15.4 或更早版本升級

要將管理伺服器從版本13—15.4升級到版本16或更高版本，您可以使用Kaspersky Security Center for Linux安裝檔案在早期版本上安裝新版本。

開始之前，**檢查自訂憑證的需求**。

如果您使用的是自訂憑證而不是自簽名憑證，則在將Kaspersky Security Center for Linux升級到更高版本之前，必須確保憑證包含主體替代名稱（SAN）。否則，請務必在升級 Kaspersky Security Center for Linux 之前替換憑證。否則，升級後您將無法登入網頁主控台。

若要確保憑證包含SAN，請執行下列操作：

1. 在安裝了管理伺服器的裝置上，執行以下命令：
   - 對於Linux裝置：

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

   - 對於Windows裝置：

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. 確保命令輸出中存在主題備用名稱，并包含管理伺服器裝置的地址。
3. 如果缺少主題備用名稱，請使用klsetsrvcert公用程式將自訂憑證替換為滿足需求的憑證。

若要使用安裝檔案將卡巴斯基安全管理中心 Linux 從 15.4 或更早版本升級至最新版本：

1. 從卡巴斯基網站下載包含版本 16.3 的完整套件的 卡巴斯基安全管理中心 Linux 安裝檔案：
   - 對於執行基於 RPM 的作業系統的裝置—`ksc64-<version number>.x86_64.rpm`
   - 對於執行基於 Debian 的作業系統的裝置—`ksc64_<version number>_amd64.deb`

2. 在資料庫管理伺服器 (DBMS) 伺服器上，為IAM建立一個資料庫。IAMIAM 名稱必須與管理伺服器所使用的 IAM 名稱不同。

   - 對於 PostgreSQL，執行以下命令：

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - 對於 MariaDB，執行以下命令：

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name[[>;"
     ```

3. 建立一個名為“ksciam”的非特權帳戶，將其新增至“kladmins”安全群組，然後將“kladmins”群組設定為“ksciam”帳戶的主群組。為此，請依次執行以下命令：

   ```
   sudo adduser ksciam
   sudo gpasswd -a ksciam kladmins
   sudo usermod -g kladmins ksciam
   ```

4. 開始升級Kaspersky Security Center for Linux。在命令列終端中執行以下一項命令：

   - 對於執行基於 RPM 的作業系統的裝置：

     ```
     sudo yum install ./ksc64-<版本號>.x86_64.rpm
     ```

   - 對於執行基於 Debian 的作業系統的裝置：

     ```
     sudo apt-get install ./ksc64_<版本號>_amd64.deb
     ```

   成功執行命令後，將建立`/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`指令碼。相關訊息將顯示在終端中。

5. 執行`/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`指令碼來配置升級的管理伺服器：

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

6. 閱讀命令行終端中顯示的產品授權協議和隱私權政策。如果您同意產品授權協議和隱私權政策的所有條款：

   a. 輸入`Y`以確認您已完整閱讀、理解並接受 EULA 的條款和條件。

   b. 再次輸入`Y`以確認您已完整閱讀、理解並接受描述資料處理的隱私權政策。

   在您兩次輸入`Y`後，您裝置上的應用程式安裝將繼續。

7. 輸入`1`以選擇標準管理伺服器安裝模式。

下圖顯示了最後兩個步驟。

```
Enter 'Y' to confirm that you understand and accept the terms of the End
User License Agreement (EULA). You must accept the terms and conditions of
the EULA to install the application. Enter 'N' providing you do not accept
the terms of the EULA or 'R' to view it again [N]:
y

Enter 'Y' to confirm that you accept the terms of the Privacy Policy. You
must accept the terms and conditions of the Privacy Policy to install the
application. Entering 'Y' means that you are aware that your data will be
handled and transmitted (including to third countries) as described in the
Privacy Policy. Enter 'N' providing you do not accept the Privacy Policy
[N]:
y

Choose the Administration Server installation mode:
1) Standard
2) Primary cluster node
3) Secondary cluster node
Enter the range number (1, 2, or 3) [1]:
```

接受 EULA 和隱私權政策的條款，並在命令行終端中選擇標準的管理伺服器安裝模式

8. 下一步，指令碼將配置和完成升級管理伺服器。升級期間，您不可以變更升級之前調整過的管理伺服器設定。出現提示時，輸入以下設定：

   a. 輸入 IAM 伺服器 FQDN。

      在安裝Kaspersky Security Center for Linux時，必須使用指定的管理伺服器DNS名稱。

   b. 輸入帳戶名稱以啟動 IAM 服務。該帳戶必須是輸入的安全群組的成員。預設情況下，使用“ksciam”帳戶。

   c. 選取為與 IAM 服務搭配使用而安裝的 DBMS：

      - 如果您安裝了 MySQL 或 MariaDB，請輸入`1`。
      - 如果您安裝了 PostgreSQL 或 Postgres Pro，請輸入`2`。

   d. 輸入IAM 服務要使用的 IAM DBMS 位址。

   e. 輸入 IAM DBMS 連接埠號。此連接埠用於與 IAM 服務通訊。預設情況下，使用以下連接埠：

      - 連接埠 3306 用於 MySQL 或 MariaDB
      - 連接埠 5432 用於 PostgreSQL 或 Postgres Pro

   f. 輸入IAM 服務要使用的 IAM 資料庫名稱。IAM 服務所使用的資料庫名稱應與管理伺服器所使用的資料庫名稱不同。

   g. 輸入IAM服務要使用的DBMS登入名和密碼。

   h. 如果您安裝了 PostgreSQL 或 Postgres Pro，可以指定 IAM 要使用的資料庫結構描述。若要這麼做，請指定結構描述名稱。

      如果您不想使用自訂結構描述，請按 `ENTER`，系統將使用 public 結構描述。

      > 結構描述名稱區分大小寫：您只能使用小寫字母。
      > 請勿指定保留的 iam 結構描述名稱：`client, iam, ksc, locker, pat, scope, voltron`。

9. 將卡巴斯基安全管理中心網頁主控台升級到新版本。

10. 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 Linux 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：

```
sudo apt-get -y autoremove
sudo apt -y autoremove
```

- 對於基於 RPM 的資產，執行以下命令之一：

```
sudo dnf autoremove
sudo yum autoremove
```

透過備份將卡巴斯基安全管理中心 Linux從版本 15.4 或更早版本進行升級

若要將管理伺服器從版本 14.2—15.4 升級到 16 或更高版本，您可以建立管理伺服器資料的備份，並在安裝新版本的卡巴斯基安全管理中心 Linux 後將其還原。如果在安裝過程中發生問題，您可以利用升級前所建立的管理伺服器資料備份還原先前版本的管理伺服器。

先決條件

1. **檢查自訂憑證的需求**

   如果您使用的是自訂憑證而不是自簽名憑證，則在將 Kaspersky Security Center for Linux 升級到更高版本之前，必須確保憑證包含主體替代名稱（SAN）。否則，請務必在升級 Kaspersky Security Center for Linux 之前替換憑證。否則，升級後您將無法登入網頁主控台。

   若要確保憑證包含SAN，請執行下列操作：

   1. 在安裝了管理伺服器的裝置上，執行以下命令：

      - 對於Linux裝置：

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

      - 對於Windows裝置：

        ```
        certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
        ```

   2. 確保命令輸出中存在主題備用名稱，并包含管理伺服器裝置的地址。

   3. 如果缺少主題備用名稱，請使用klsetsrvcert公用程式將自訂憑證替換為滿足需求的憑證。

2. 使用舊版本的應用程式備份管理伺服器資料。

升級步驟

若要透過備份將卡巴斯基安全管理中心 Linux 從 15.4 或更早版本升級到最新版本：

1. 解除安裝舊版本的 卡巴斯基安全管理中心 Linux。

2. 在資料庫管理伺服器 (DBMS) 伺服器上，為IAM建立一個資料庫。IAMIAM 名稱必須與管理伺服器所使用的 IAM 名稱不同。

   - 對於 PostgreSQL，執行以下命令：

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - 對於 MariaDB，執行以下命令：

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name[[>;"
     ```

3. 建立一個名為“ksciam”的非特權帳戶，將其新增至“kladmins”安全群組，然後將“kladmins”群組設定為“ksciam”帳戶的主群組。為此，請依次執行以下命令：

   ```
   sudo adduser ksciam
   sudo gpasswd -a ksciam kladmins
   sudo usermod -g kladmins ksciam
   ```

4. 在先前安裝了管理伺服器的裝置上安裝卡巴斯基安全管理中心 Linux 版本 16.3。

   如果備份副本中的資料庫結構描述與管理伺服器或 IAM 目前使用的結構描述不同，資料將會還原至目前的結構描述。

   如果備份副本中使用 public 結構描述，則必須符合以下條件：

   - 資料庫中存在 public 資料庫結構描述。
   - 您可以使用管理伺服器或 IAM 用於存取資料庫的 DBMS 帳戶，修改 public 資料庫結構描述。

   否則，資料還原會因錯誤而結束。

5. 從升級前建立的備份還原管理伺服器資料。

6. 設定管理伺服器和IAM伺服器的憑證驗證。

7. 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。

8. 對於安裝了更早版本網路代理的裝置，建立並執行新版本網路代理的遠端安裝工作。

   > 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 Linux 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：

```
sudo apt-get -y autoremove
sudo apt -y autoremove
```

- 對於基於 RPM 的資產，執行以下命令之一：

```
sudo dnf autoremove
sudo yum autoremove
```

在Kaspersky Security Center for Linux故障轉移叢集節點上升級Kaspersky Security Center for Linux 15.4或更早版本

您可以在每個已安裝管理伺服器版本 14—15.4 的卡巴斯基安全管理中心 Linux 容錯移轉叢集節點上安裝管理伺服器版本 16 或更高版本。升級時，上一版本的管理伺服器的所有資料和設定將會保留。

開始之前，**檢查自訂憑證的需求**。

如果您使用的是自訂憑證而不是自簽名憑證，則在將Kaspersky Security Center for Linux升級到更高版本之前，必須確保憑證包含主體替代名稱（SAN）。否則，請務必在升級 Kaspersky Security Center for Linux 之前替換憑證。否則，升級後您將無法登入網頁主控台。

若要確保憑證包含SAN，請執行下列操作：

1. 在安裝了管理伺服器的裝置上，執行以下命令：

   - 對於Linux裝置：

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

   - 對於Windows裝置：

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. 確保命令輸出中存在主題備用名稱，并包含管理伺服器裝置的地址。

3. 如果缺少主題備用名稱，請使用klsetsrvcert公用程式將自訂憑證替換為滿足需求的憑證。

如果您之前在裝置上本機安裝了 卡巴斯基安全管理中心 Linux，您還可以透過使用安裝檔案或透過備份在這些裝置上升級 卡巴斯基安全管理中心 Linux。

若要在Kaspersky Security Center for Linux故障轉移叢集節點上升級Kaspersky Security Center for Linux 15.4或更早版本：

1. 從卡巴斯基網站下載包含版本 16.3 的完整套件的 卡巴斯基安全管理中心 Linux 安裝檔案：
   - 對於執行基於 RPM 的作業系統的裝置—`ksc64-<version number>-<build number>.x86_64.rpm`
   - 對於執行基於 Debian 的作業系統的裝置—`ksc64_<version number>-<build number>_amd64.deb`
2. 停止叢集。
3. 在 DBMS 伺服器上，為 IAM 建立資料庫。IAM 資料庫名稱必須不同於管理伺服器所使用的資料庫名稱。
   - 對於 PostgreSQL，執行以下命令：

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - 對於 MariaDB，執行以下命令：

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name[[>;"
     ```

4. 建立一個名為“ksciam”的非特權帳戶，將其新增至“kladmins”安全群組，然後將“kladmins”群組設定為“ksciam”帳戶的主群組。為此，請依次執行以下命令：

   ```
   sudo adduser ksciam
   sudo gpasswd -a ksciam kladmins
   sudo usermod -g kladmins ksciam
   ```

5. 在叢集的活動節點上，在命令列終端中執行以下命令之一以開始升級：
   - 對於執行基於 RPM 的作業系統的裝置：

     ```
     sudo yum install ./ksc64-<版本號>-<內建版本號>.x86_64.rpm
     ```

   - 對於執行基於 Debian 的作業系統的裝置：

     ```
     sudo apt-get install ./ksc64_<版本號>-<內建版本號>_amd64.deb
     ```

   成功執行命令後，將建立`/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`指令碼。相關訊息將顯示在終端中。

6. 執行`/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`指令碼來配置升級的管理伺服器：

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

7. 閱讀命令行終端中顯示的產品授權協議和隱私權政策。如果您同意產品授權協議和隱私權政策的所有條款：
   a. 輸入`Y`以確認您已完整閱讀、理解並接受 EULA 的條款和條件。
   b. 再次輸入`Y`以確認您已完整閱讀、理解並接受描述資料處理的隱私權政策。

在您兩次輸入`Y`後，您裝置上的應用程式安裝將繼續。

8. 透過輸入`2`選擇要升級的節點。

   下圖顯示了最後兩個步驟。

```
Enter 'Y' to confirm that you understand and accept the terms of the End
User License Agreement (EULA). You must accept the terms and conditions of
the EULA to install the application. Enter 'N' providing you do not accept
the terms of the EULA or 'R' to view it again [N]:
y

Enter 'Y' to confirm that you accept the terms of the Privacy Policy. You
must accept the terms and conditions of the Privacy Policy to install the
application. Entering 'Y' means that you are aware that your data will be
handled and transmitted (including to third countries) as described in the
Privacy Policy. Enter 'N' providing you do not accept the Privacy Policy
[N]:
y

Choose the Administration Server installation mode:
1) Standard
2) Primary cluster node
3) Secondary cluster node
Enter the range number (1, 2, or 3) [1]:
```

接受 EULA 和隱私權政策的條款，並在命令行終端中選擇安裝模式

9. 下一步，指令碼將配置和完成升級管理伺服器。升級期間，您不可以變更升級之前調整過的管理伺服器設定。出現提示時，輸入以下設定：

   a. 輸入 IAM 伺服器 FQDN。

      在安裝Kaspersky Security Center for Linux時，必須使用指定的管理伺服器DNS名稱。

   b. 輸入帳戶名稱以啟動 IAM 服務。該帳戶必須是輸入的安全群組的成員。預設情況下，使用“ksciam”帳戶。

   c. 選取為與 IAM 服務搭配使用而安裝的 DBMS：

      - 如果您安裝了 MySQL 或 MariaDB，請輸入`1`。
      - 如果您安裝了 PostgreSQL 或 Postgres Pro，請輸入`2`。

   d. 輸入IAM 服務要使用的 IAM DBMS 位址。

   e. 輸入 IAM DBMS 連接埠號。此連接埠用於與 IAM 服務通訊。預設情況下，使用以下連接埠：

      - 連接埠 3306 用於 MySQL 或 MariaDB
      - 連接埠 5432 用於 PostgreSQL 或 Postgres Pro

   f. 輸入IAM 服務要使用的 IAM 資料庫名稱。IAM 服務所使用的資料庫名稱應與管理伺服器所使用的資料庫名稱不同。

   g. 輸入IAM服務要使用的DBMS登入名和密碼。

10. 在被動節點上執行步驟 5。

    在第 6 步中，輸入`3`以選擇節點。

11. 啟動叢集。

    > 您可以在任何節點上啟動叢集。如果在被動節點上啟動叢集，它將成為主動節點。

12. 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 Linux 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：

```
sudo apt-get -y autoremove
sudo apt -y autoremove
```

- 對於基於 RPM 的資產，執行以下命令之一：

```
sudo dnf autoremove
sudo yum autoremove
```

結果，您在卡巴斯基安全管理中心 Linux 容錯移轉叢集節點上安裝了最新版本的管理伺服器。

升級卡巴斯基安全管理中心網頁主控台

該文描述了如何升級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。

如果您需要在封閉軟體環境模式下的 Astra Linux 上升級卡巴斯基安全管理中心網頁主控台，請按照特定於 Astra Linux 的說明進行操作。

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：

- 對於基於 Debian 的作業系統: 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

您透過從 Kaspersky 網站下載來接收安裝檔案。

若要升級卡巴斯基安全管理中心網頁主控台：

1. 確保您要在其上升級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. 閱讀並接受最終使用者產品授權協議 (EULA)。如果卡巴斯基安全管理中心 Linux 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的條款，請勿使用安裝檔案升級卡巴斯基安全管理中心網頁主控台。
3. 使用您在安裝卡巴斯基安全管理中心網頁主控台之前準備的相同回應檔案。回應檔案名稱為 ksc-web-console-setup.json ，檔案位置為 /etc/ksc-web-console-setup.json。

如果您在安裝卡巴斯基安全管理中心網頁主控台時指定了 `webConsoleAccount`、`managementServiceAccount`、`serviceWebConsoleAccount`、`pluginAccount` 和 `natsMessageQueueAccount` 參數的值，請確保在回應檔案中指定所有這些參數。

如果回應檔案不存在，請建立一個新的回應檔案，其中包含用於將卡巴斯基安全管理中心網頁主控台連線到管理伺服器的參數。命名該檔案為 ksc-web-console-setup.json，然後將其放置到 /etc目錄中。

包含最小參數集合的回應檔案範例

回應檔案的參數集取決於卡巴斯基安全管理中心網頁主控台所連線的管理伺服器版本：

- 16 或更高版本的管理伺服器

  以下是登入管理伺服器版本 16 或更高版本所需的採用最小參數集的回應檔案範例：

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- 15.4 或更早版本的管理伺服器

  以下是登入管理伺服器版本 15.4 或更早版本所需的採用最小參數集的回應檔案範例：

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

您可以將卡巴斯基安全管理中心網頁主控台安裝到管理伺服器所在的同一裝置，也可以安裝到不同裝置。如果將卡巴斯基安全管理中心網頁主控台安裝到不同裝置，則卡巴斯基安全管理中心網頁主控台位址（由 `address` 指定）將會與管理伺服器位址（由 `iamHost` 或 `kscHost` 指定）不同。如果將卡巴斯基安全管理中心網頁主控台安裝到管理伺服器所在的同一裝置，則這些參數的值將相同。

`iamHost` 值必須與您在安裝管理伺服器時指定的 IAM 位址相符。若要取得指定的IAM位址，請在管理伺服器主機上執行下列命令：

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

有關詳細資訊，請參閱文章：卡巴斯基安全管理中心網頁主控台安裝程式參數。

您可以將多個不同版本的管理伺服器新增到受信任伺服器清單。在這種情況下，這些伺服器可以使用不同的身分驗證方法。

如果要升級連線到卡巴斯基安全管理中心 Linux 容錯移轉叢集節點上安裝之管理伺服器的卡巴斯基安全管理中心網頁主控台，請在回應檔案中指定 trusted 安裝參數，以允許卡巴斯基安全管理中心 Linux 容錯移轉叢集連線到卡巴斯基安全管理中心網頁主控台。

`trusted` **安裝參數**的元件

如果您透過單一登入進行網域身分驗證，從而連線到卡巴斯基安全管理中心 Linux 容錯移轉叢集，請按如下方式指定 trusted 安裝參數：如果您將卡巴斯基安全管理中心網頁主控台連線到管理伺服器版本 16 或更新版本，則將使用身分和存取管理器 (IAM) 透過單一登入 (SSO) 進行網域身分驗證。在這種情況下，請按如下方式指定 `trusted` 安裝參數：

```
"trusted":  {
  "<管理伺服器名稱>": {
    "iamHost": "ksc-iam.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "<共用資料資料夾>/iam/main_certificate.pem",
    "iamPATPath": "<共用資料資料夾>/iam/initial_token.txt",
    "kscPort": 13299,
    "kscCertPath": "<共用資料夾>/1093/cert/klserver.cer"
  }
}
```

其中：

- < 管理伺服器名稱 > 是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卡巴斯基安全管理中心 Linux 容錯移轉叢集名稱。

- `iamHost` 是安裝管理伺服器和 IAM 的裝置的位址。如果您在準備叢集節點時建立了次要網路介面卡，請使用該介面卡的 FQDN 或主機名稱作為卡巴斯基安全管理中心 Linux 容錯移轉叢集位址。否則，請指定所使用協力廠商負載均衡器的 FQDN 或主機名稱。

  `iamHost` 值必須與安裝管理伺服器時指定的 IAM 位址相符。若要取得指定的 IAM 位址，請在管理伺服器主機上執行下列命令：

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

- `iamOAuthPort` 是用於透過 OpenID Connect 身分驗證協定交換身分驗證權杖的連接埠（預設值為 4444）。此連接埠同時用於卡巴斯基安全管理中心網頁主控台伺服器與管理伺服器之間的通訊，以及瀏覽器（與卡巴斯基安全管理中心網頁主控台搭配使用）與管理伺服器之間的通訊。

- `iamProxyPort` 是用於將卡巴斯基安全管理中心網頁主控台伺服器連線到管理伺服器的連接埠（預設值為 9050）。

- `iamCertPath` 是 IAM 憑證的路徑。IAM 憑證會在首次執行管理伺服器時自動建立。憑證位於安裝管理伺服器的裝置上。憑證的預設路徑為：< 共用資料夾 >`/iam/main_certificate.pem`。憑證位於卡巴斯基安全管理中心 Linux 容錯移轉叢集中。自簽章 IAM 憑證會自動輪換。

- `iamPATPath` 是用於將卡巴斯基安全管理中心網頁主控台註冊為 IAM 中的 OAuth 用戶端的權杖路徑。此檔案會在首次執行管理伺服器時產生。權杖位於安裝管理伺服器的裝置上。權杖的預設路徑：<共用資料夾 >/iam/initial_token.txt。權杖位於卡巴斯基安全管理中心 Linux 容錯移轉叢集的共用資料儲存中。權杖永久有效，無需輪換。

- `kscPort` 是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）。

- `kscCertPath` 是位於卡巴斯基安全管理中心 Linux 容錯移轉叢集的共用資料儲存中的管理伺服器憑證。憑證檔案的預設路徑為：< 共用資料夾 >`\1093\cert\klserver.cer`。

  將管理伺服器憑證檔案（由 `kscCertPath` 指定）、IAM 憑證檔案（由 `iamCertPath` 指定）和權杖檔案（由 `iamPATPath` 指定）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。

如果將卡巴斯基安全管理中心網頁主控台連線到管理伺服器版本 15.4 或更早版本，則將透過指定網域使用者或內部使用者的名稱和密碼進行身分驗證。在這種情況下，請按如下方式指定 trusted 安裝參數：

```
"trusted":  {
  "<管理伺服器名稱>": {
    "kscHost": "ksc.example.com",
    "kscPort": 13299,
    "kscCertPath": "<共用資料夾>/1093/cert/klserver.cer"
  }
}
```

其中：

- < 管理伺服器名稱 > 是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卡巴斯基安全管理中心 Linux 容錯移轉叢集名稱。
- `kscHost` 是管理伺服器位址（FQDN 或主機名稱）。如果您在準備叢集節點時建立了次要網路介面卡，請使用介面卡的位址作為卡巴斯基安全管理中心 Linux 容錯移轉叢集位址。否則，請指定所使用協力廠商負載均衡器的位址。
- `kscPort` 是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）。
- `kscCertPath` 是位於卡巴斯基安全管理中心 Linux 容錯移轉叢集的共用資料儲存中的管理伺服器憑證。憑證檔案的預設路徑為：< 共用資料夾 >`\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。

卡巴斯基安全管理中心網頁主控台無法使用相同的安裝檔案升級。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。

   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 yum install ksc-web-console-<build_number>.x86_64.rpm
     ```
   - 對於執行基於 Debian 的作業系統的裝置：
     ```
     sudo apt-get install 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。

5. 透過執行以下命令重新啟動所有卡巴斯基安全管理中心 網頁主控台服務：
   ```
   sudo systemctl restart KSC*
   ```

當升級完成時，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。

在封閉軟體環境模式下在 Astra Linux 上升級卡巴斯基安全管理中心網頁主控台

該文描述了如何在 Astra Linux 特別版作業系統上升級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）。

若要升級卡巴斯基安全管理中心網頁主控台：

1. 確保您要在其上升級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. 閱讀並接受最終使用者產品授權協議 (EULA)。如果卡巴斯基安全管理中心 Linux 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的條款，請勿使用安裝檔案升級卡巴斯基安全管理中心網頁主控台。

3. 使用您在安裝卡巴斯基安全管理中心網頁主控台之前準備的相同回應檔案。回應檔案名稱為 ksc-web-console-setup.json ，檔案位置為 /etc/ksc-web-console-setup.json。

   如果回應檔案不存在，請建立一個新的回應檔案，其中包含用於將卡巴斯基安全管理中心網頁主控台連線到管理伺服器的參數。命名該檔案為 ksc-web-console-setup.json，然後將其放置到 /etc目錄中。

   包含最小參數集合的回應檔案範例

   回應檔案的參數集取決於卡巴斯基安全管理中心網頁主控台所連線的管理伺服器版本：

   - 16 或更高版本的管理伺服器

     以下是登入管理伺服器版本 16 或更高版本所需的採用最小參數集的回應檔案範例：

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

   - 15.4 或更早版本的管理伺服器

     以下是登入管理伺服器版本 15.4 或更早版本所需的採用最小參數集的回應檔案範例：

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

   您可以將卡巴斯基安全管理中心網頁主控台安裝到管理伺服器所在的同一裝置，也可以安裝到不同裝置。如果將卡巴斯基安全管理中心網頁主控台安裝到不同裝置，則卡巴斯基安全管理中心網頁主控台位址（由 `address` 指定）將會與管理伺服器位址（由 `iamHost` 或 `kscHost` 指定）不同。如果將卡巴斯基安全管理中心網頁主控台安裝到管理伺服器所在的同一裝置，則這些參數的值將相同。

   `iamHost` 值必須與您在安裝管理伺服器時指定的 IAM 位址相符。若要取得指定的IAM位址，請在管理伺服器主機上執行下列命令：

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

有關詳細資訊，請參閱文章：卡巴斯基安全管理中心網頁主控台安裝程式參數。

您可以將多個不同版本的管理伺服器新增到受信任伺服器清單。在這種情況下，這些伺服器可以使用不同的身分驗證方法。

4. 確保在 `/etc/digsig/digsig_initramfs.conf` 檔案中，`DIGSIG_ELF_MODE` 參數指定如下：

   ```
   DIGSIG_ELF_MODE=1
   ```

5. 確保已安裝 `astra-digsig-oldkeys` 相容性套件。

   如果未安裝此套件，請執行以下命令：

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

6. 為應用程式金鑰建立一個目錄（如果不存在）：

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

7. 將應用程式金鑰 /opt/kaspersky/ksc64/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 Linux 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。

8. 更新 RAM 瓷碟：

   ```
   update-initramfs -u -k all
   ```

   重新啟動系統。

9. 在具有 root 權限的帳戶下，使用指令行執行安裝檔案。您透過從 Kaspersky 網站下載來接收安裝檔案。

   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：

   ```
   sudo apt-get install ksc-web-console-<版本編號>.x86_64.deb
   ```

   這會開始解壓縮安裝檔案。請等待安裝完成。

10. 透過執行以下命令重新啟動所有卡巴斯基安全管理中心 網頁主控台服務：

    ```
    sudo systemctl restart KSC*
    ```

當升級完成時，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。

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 • PostgreSQL → PostgreSQL Postgres Pro → Postgres Pro（僅適用於從卡巴斯基安全管理中心 Windows 版本 15.1 或更高版本移轉到卡巴斯基安全管理中心 Linux 版本 16 或更高版本）	在受支援的 DBMS 之間無限制遷移

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。

為了清楚起見，我們提供了一個教程視頻，介紹如何使用備份將管理伺服器資料遷移到卡巴斯基安全管理中心 Linux 。

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
  - PostgreSQL → PostgreSQL
  - Postgres Pro → Postgres Pro
- 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 PostgreSQL 資料庫中的管理伺服器資料移轉到 PostgreSQL 或將 Postgres Pro 資料庫移轉到 Postgres Pro，以便從卡巴斯基安全管理中心 Windows 版本 15.1 或更高版本移轉到卡巴斯基安全管理中心 Linux 版本 16 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。

  若要支援遷移至 PostgreSQL 或 Postgres Pro，您必須向卡巴斯基技術支援提出請求並安裝下列修補程式之一：
  - 對於卡巴斯基安全管理中心 Windows 14.2：14.2.0.26967-pf5
  - 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 15.1Windows：15.1.0.20748-pf2

  將卡巴斯基安全管理中心 Windows 更新至版本 15.1.0.22239 後，也可以移轉到PostgreSQL 或 Postgres Pro。

- 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。

先決條件

開始之前，**檢查自訂憑證的需求**。

如果您使用的是自訂憑證而不是自簽名憑證，則在將Kaspersky Security Center for Linux升級到更高版本之前，必須確保憑證包含主體替代名稱（SAN）。否則，請務必在升級 Kaspersky Security Center for Linux 之前替換憑證。否則，升級後您將無法登入網頁主控台。

若要確保憑證包含SAN，請執行下列操作：

1. 在安裝了管理伺服器的裝置上，執行以下命令：

   - 對於Linux裝置：

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

   - 對於Windows裝置：

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. 確保命令輸出中存在主題備用名稱，并包含管理伺服器裝置的地址。

3. 如果缺少主題備用名稱，請使用klsetsrvcert公用程式將自訂憑證替換為滿足需求的憑證。

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。
- 如需將 PostgreSQL 移轉到 PostgreSQL 以及將 Postgres Pro 移轉到 Postgres Pro：請在安裝有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副本。
- 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**移轉到 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。

     對於卡巴斯基安全管理中心 15.1 Windows，您可以更新至版本 15.1.0.22239 而不是安裝修補程式。

  2. 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的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。您可以選擇任何受支援的 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，請參考其文檔。

   為 IAM 手動建立資料庫。

   > 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。

- 設定 MariaDB x64 伺服器以與 卡巴斯基安全管理中心 Linux 一起使用
- 設定 PostgreSQL 或 Postgres Pro 伺服器與 卡巴斯基安全管理中心 Linux 搭配使用
- 設定 MySQL x64 伺服器以與 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。

      由於PostgreSQL 的限制，您需要暫時授予管理伺服器用於連線到 DBMS 的帳戶的 PostgreSQL 超級使用者權限。

   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 kscadmin -p <密碼>`

      其中 <密碼 [[> 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. **設定管理伺服器和IAM伺服器的憑證驗證。**

8. **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. 查看已遷移的工作。如果其任何參數包含 Windows 檔案路徑，則將其替換為相應的 Linux 檔案路徑。

   5. 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。

      同一網路上不能有多個管理伺服器共用相同的連線位址和管理伺服器憑證。

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。

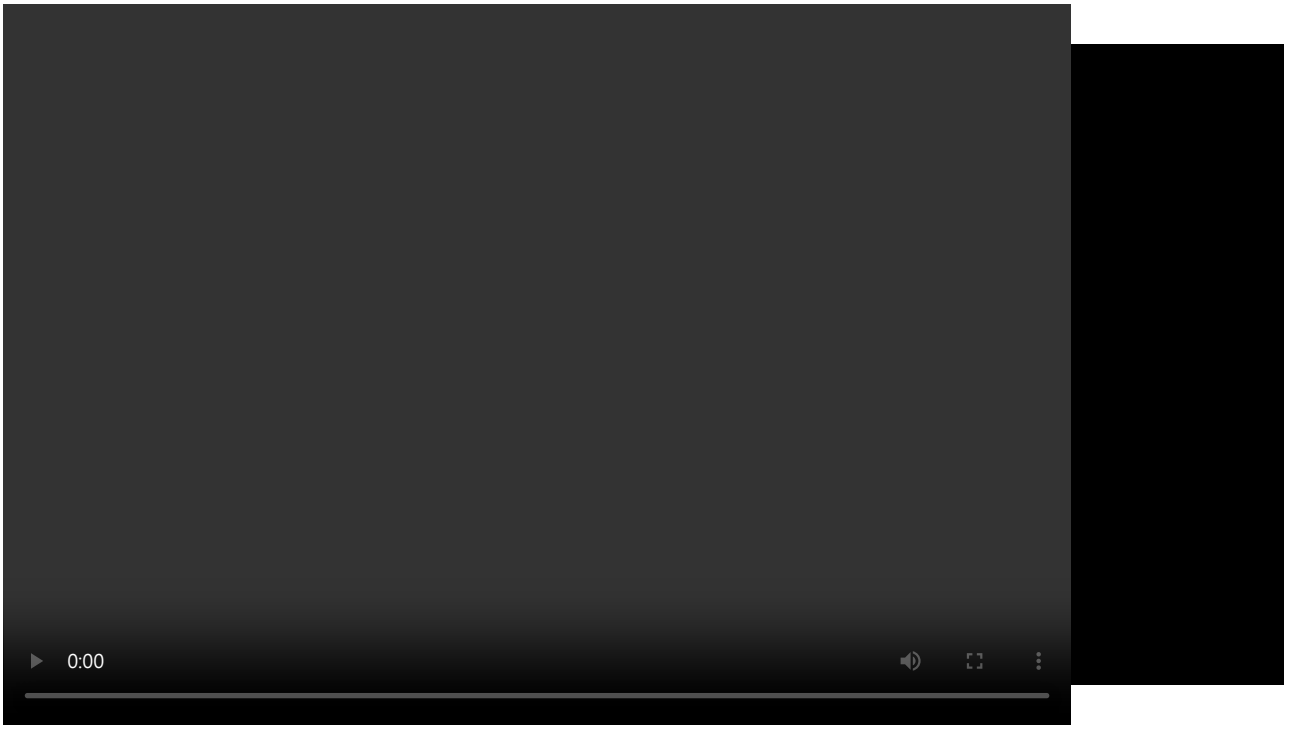
教程視頻：使用管理伺服器資料備份遷移到卡巴斯基安全管理中心 Linux

觀看視頻，了解如何使用管理伺服器資料備份（使用klbackup 實用程式）將卡巴斯基安全管理中心 Windows 管理伺服器資料遷移到卡巴斯基安全管理中心 Linux。

要支援遷移到 PostgreSQL 或 Postgres Pro，您必須向卡巴斯基技術支援請求並安裝以下修補程式之一：

- 對於卡巴斯基安全管理中心14.2 Windows：14.2.0.26967-pf5
- 對於基於卡巴斯基安全管理中心14.2 Windows 的Kaspersky Secure Mobility Management：14.2.0.48079-pf5
對於卡巴斯基安全管理中心15.1 Windows：15.1.0.20748-pf2

將卡巴斯基安全管理中心 Windows 更新至版本 15.1.0.22239後，也可以移轉到 PostgreSQL 或 Postgres Pro。



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。視訊

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。

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。
- 您只能使用卡巴斯基安全管理中心網頁主控台來執行此情境。

在開始之前，請先詳細瞭解卡巴斯基安全管理中心 Linux 的功能和限制：

- 卡巴斯基安全管理中心 Windows 和卡巴斯基安全管理中心 Linux 之間的功能差異
- 由卡巴斯基安全管理中心 Linux 支援的 Kaspersky 應用程式清單

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 Kaspersky Security Center 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，您必須還原憑證和私鑰。

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
- 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
- 分配和配置發佈點

  如果您將充當發佈點的裝置移動到另一台管理伺服器，包括在發佈點範圍中的裝置不會被自動移動。您必須單個移動每個裝置如果發佈點作為閘道運作，您必須執行 `# /opt/kaspersky/klnagent64/bin/setup/postinstall.pl` 指令碼，讓該發佈點不再作為閘道。

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 版本 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 klbackup 公用程式並使用 `-cert_only` 參數，以從您在第 2 階段儲存的備份副本中還原管理伺服器憑證和私密金鑰。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（**資產管理→資產（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，還有其他方法可以傳輸您當前的物件，但這些方法只允許您傳輸政策和工作：

- 從卡巴斯基安全管理中心 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. 選擇**移轉到卡巴斯基安全管理中心 Linux 或者 Open Single Management Platform**以啟動精靈並按照其步驟操作。

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層次結構：

     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**資產管理**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。
- 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）。
  詳情請參考主要遷移場景的第 6 階段。
- 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**軟體管理** → **安裝套件**，然後開啟網路代理程式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）。

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。

配置管理伺服器連線位址

管理伺服器連連線址是用於以下用途的網路位址：

- 作為建立網路代理安裝套件時的預設位址
  安裝網路代理後，受管理裝置透過此位址連線到管理伺服器。
- 作為 KSN 代理伺服器位址
  受管理裝置透過此位址連線到 KSN 代理伺服器。

設定管理伺服器連線位址：

1. 在主選單中，按一下管理伺服器名稱。
   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. 在開啟的視窗中，在**管理伺服器連線位址** 欄位中，指定新的管理伺服器連線位址。
   連線位址的最大長度為 255 個字元。
   您可以將管理伺服器連線位址指定為 NetBIOS 名稱、FQDN 或管理伺服器的 IP 位址。
4. 點擊**儲存**按鈕。

指定的位址用作管理伺服器位址和 KSN 代理伺服器位址。

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

您可以透過管理伺服器屬性或使用管理伺服器政策設定來設定卡巴斯基安全管理中心網頁主控台與管理伺服器的連線。

要透過管理伺服器內容設定連線連接埠：

1. 在主選單中，按一下管理伺服器名稱。
   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. 如有必要，請指定**網頁主控台的 SSL 連接埠**設定或指定其他管理伺服器連線連接埠。

所選伺服器的主要連線設定已指定。

若要透過管理伺服器政策設定設定連線連接埠：

1. 在主功能表中，轉至 **資產管理** → **政策**。

2. 點擊管理伺服器政策的名稱，然後前往**應用程式設定**標籤。

3. 如有必要，請指定**網頁主控台的 SSL 連接埠**設定或指定其他管理伺服器連線連接埠。

> 如果停用**開啟網頁主控台的連接埠**選項且此政策設定將被套用至裝置，您將無法使用 卡巴斯基安全管理中心網頁主控台連線至管理伺服器。在這種情況下，連線將被終止。如果有管理伺服器上未套用此政策，您可以透過 卡巴斯基安全管理中心網頁主控台重新連線至此管理伺服器。

所選伺服器的主要連線設定已指定。

設定連線到卡巴斯基安全管理中心 Linux 的 IP 位址允許清單

預設情況下，允許從任何裝置連線到卡巴斯基安全管理中心 Linux。例如，您可以在任何符合要求的裝置上安裝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將與卡巴斯基安全管理中心 Linux 進行通訊。不過，您可以設定管理伺服器，以便僅允許具有您指定 IP 位址的裝置進行連線。在這種情況下，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 Linux，他或她將無法登入卡巴斯基安全管理中心 Linux。

當使用者登入卡巴斯基安全管理中心 Linux 或執行透過卡巴斯基安全中心 Linux 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，裝置上的應用程式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：

- 卡巴斯基安全管理中心網頁主控台伺服器

  如果您透過卡巴斯基安全管理中心網頁主控台登入卡巴斯基安全管理中心 Linux ，可以使用作業系統的標準方式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配置防火牆。然後，如果有人嘗試在一台裝置上登入卡巴斯基安全管理中心 Linux 但卡巴斯基安全管理中心網頁主控台伺服器安裝在另一台裝置上，防火牆將有助於防止入侵者乾擾。

- 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 Linux ：

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 Linux 安裝資料夾（通常為 /opt/kaspersky/ksc64/sbin ）。
3. 在根帳號下輸入以下命令：
   ```
   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 Syslog 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. 在根帳戶下的命令提示下輸入以下命令：
   `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。

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 Linux 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. 在主選單中，按一下管理伺服器名稱。

   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 Linux 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。

管理伺服器階層

一些用戶端公司，例如MSP，可能執行多台管理伺服器。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。在階層結構中，基於 Linux 的管理伺服器既可以作為主伺服器也可以作為從屬伺服器。基於 Linux 的主伺服器可以管理基於 Linux 和基於 Windows 的從屬伺服器。基於 Windows 的主伺服器可以管理基於 Linux 的次要伺服器。

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、工作、使用者角色和安裝套件，從而防止重複設定。
- 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）。
- 主管理伺服器可作為從屬管理伺服器的更新來源。

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。

管理伺服器的層次結構為多組織用戶模式提供支援。此模式允許主管理員獨立地集中管理多個用戶端。每個用戶端組織或辦公室都與其他用戶端組織或辦公室隔離，被稱為租用戶。您可以將多個受管理裝置及其相關資料、設定、政策和工作指派給一個租用戶，並按租用戶配置使用者權限。

安裝在主要組織基礎結構中的主管理伺服器可充當主要租用戶。主管理伺服器使從屬或虛擬管理伺服器（其獨立的租用戶）能夠獨立接收和處理自己的事件並使用自己的資源、服務和配置。

擁有多個用戶端組織的服務提供商可以向每個用戶端組織獨立提供卡巴斯基安全管理中心 Linux 功能，包括警示聚合和回應操作。為了實現這一點，服務提供商將從屬或虛擬管理伺服器作為每個用戶端組織的租用戶進行連線。服務提供商利用自己的人員和資源提供服務。

建立管理伺服器階層：新增次要管理伺服器

在階層結構中，基於 Linux 的管理伺服器既可以作為主伺服器也可以作為從屬伺服器。基於 Linux 的主伺服器可以管理基於 Linux 和基於 Windows 的從屬伺服器。基於 Windows 的主伺服器可以管理基於 Linux 的次要伺服器。

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. 請確保未來主管理伺服器的連接埠 13000 可用。

   建立階層後，此連接埠將用於主管理伺服器與從屬管理伺服器之間的互動。

2. 前往未來主管理伺服器的屬性：

   a. 在主選單中，選擇一個部分（**市場**、**主控台導覽**和**設定**除外），然後在頁面頂部點擊**顯示階層**按鈕。

   b. 在開啟的導覽窗格中，將滑鼠遊標停留在所需管理伺服器的名稱上，然後點擊設定圖示 (⚙)。

      或者，您可以按一下管理伺服器名稱，然後在主選單中顯示該名稱後，在主選單中按一下它以開啟伺服器屬性視窗。

3. 在開啟的屬性視窗中，點擊**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：

   - **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到 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**

     指定建立階層後用於主管理伺服器與從屬管理伺服器之間互動的 SSL 連接埠號碼。預設埠號為 13000。

   - **管理伺服器 API 連接埠**

     網頁主控台用於透過 OpenAPI 接收來自從屬管理伺服器之連線的連接埠號碼。預設埠號為13299。

     在構建層級結構時，網頁主控台會連線至未來的從屬伺服器、請求憑據、擷取公開憑證，並執行初始設定。

     管理伺服器的層級結構構建完成後，將不再使用連接埠 13299。管理伺服器將透過連接埠 13000 進行互動。

   - **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。

   - **使用代理伺服器**

     如果您使用代理伺服器連線到次要管理伺服器，選取該選項。

此種情況下，您也必須指定代理伺服器的以下設定：

- **代理伺服器位址**
- **使用者名稱**
- **密碼**

7. 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。
8. 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。

精靈已完成，與未來的從屬伺服器的連線已建立，並已建立「主要/從屬」階層。

主管理伺服器和次要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。

連線在以下情況下會失敗：

- 連線設定不正確。

  您必須檢查設定，或手動指定未來的從屬伺服器憑證。

- 未來的從屬伺服器使用卡巴斯基安全管理中心 Linux 自動產生的自我簽署憑證進行身分驗證。因此，瀏覽器可能會封鎖下載自我簽署憑證。

  您可以執行下列其中一項操作：

  - 針對未來的從屬伺服器，建立一個在您的基礎架構中受信任且滿足自訂憑證要求的憑證。
  - 將未來的從屬伺服器的自我簽署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。有關將憑證新增到受信任憑證清單的資訊，請參閱瀏覽器的文件。

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，因為它臨時被斷開或無法連線，或從屬管理伺服器的憑證檔案為自簽章），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，位於 /var/opt/kaspersky/klnagent_srv/1093/cert/。

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. 按一下管理伺服器名稱。
   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. 若未來主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：

1. 在主功能表中，選擇一個部分（**市場**、**主控台導覽**和**設定**除外）。

2. 在頁面頂部，點擊**顯示階層**按鈕。

   在開啟的導覽窗格中，從屬（包括虛擬）管理伺服器的清單將顯示。您可透過點及其名稱前往這些管理伺服器的任何一個。

> 如果您從**IP 範圍**和**已刪除物件**部分開啟了導覽窗格，則無法前往虛擬管理伺服器。
> 管理群組也會顯示。如果您從下列部分開啟導覽窗格，則可以管理這些群組：**資產（裝置）**、**政策**、**工作**和**發佈點**。否則，這些群組將成為灰色。

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，使用具有管理權限的帳戶執行與您裝置上安裝的 Linux 發行版相對應的卡巴斯基安全管理中心網頁主控台安裝檔案。

     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。

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
- 啟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. 在主選單中，按一下管理伺服器名稱。

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。

如有必要，您可以使用 kladduser 公用程式建立一個將充當虛擬管理伺服器的新帳戶。為此，請使用以下指令：

```
kladduser -n <用戶名稱> -p <密碼> -vs <虛擬伺服器名稱>
```

其中 虛擬伺服器名稱 是虛擬管理伺服器的名稱。

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，使用具有管理權限的帳戶執行與您裝置上安裝的 Linux 發行版相對應的卡巴斯基安全管理中心網頁主控台安裝檔案。

     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。

啓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. 在主選單中，按一下管理伺服器名稱。

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. 切換到所需的虛擬管理伺服器：
   a. 在主選單中，選擇一個部分（**市場**、**主控台導覽**和**設定**除外），然後在頁面頂部點擊**顯示階層**按鈕。
   b. 在開啟的導覽窗格中，點擊所需虛擬管理伺服器的名稱。

   > 您無法從**IP 範圍**和**已刪除物件**部分切換到虛擬管理伺服器。

   在主選單中，管理伺服器將變更為您選擇的伺服器。

2. 在主選單中點選管理伺服器的名稱，移至其屬性。
   或者，在導覽窗格中，將滑鼠遊標停留在所需虛擬管理伺服器的名稱上，然後按一下設定圖示 (⚙)。
   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。

若要為多個虛擬管理伺服器指派管理員：

1. 在主選單中，按一下主管理伺服器名稱。

2. 在開啟的頁面上，轉至**存取權限**頁籤，然後按一下**指派**。
   在開啟的**新增使用者或群組**視窗中，選取要指派為管理員的使用者旁的核取方塊。

3. 您可以切換到**群組**頁籤來選擇使用者群組。

4. 按一下**下一步**。

5. 選取要為其指派管理員的伺服器，然後按一下**下一步**。

6. 如有必要，請選取要為使用者設定的管理員角色。
   如果要為使用者設定目前管理伺服器的自訂角色，請前往所需管理伺服器的內容，按一下**設定角色**，然後選取自訂角色。

7. 按一下**完成**以套用變更。

具有所選角色的管理員現在已指派給多個虛擬管理伺服器。

若要撤銷管理員存取權限：

1. 切換到所需的管理伺服器。

2. 在主選單中，按一下管理伺服器名稱。

3. 在開啟的頁面上，轉至**存取權限**頁籤。

4. 選取要撤銷其存取權限的使用者旁的核取方塊。

5. 按一下**撤銷**並確認您的操作。

所選使用者的存取權限被撤銷。

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. 切換到所需的虛擬管理伺服器：

   a. 在主選單中，選擇一個部分（**市場**、**主控台導覽**和**設定**除外），然後在頁面頂部點擊**顯示階層**按鈕。

   b. 在開啟的導覽窗格中，點擊所需虛擬管理伺服器的名稱。

   > 您無法從**IP 範圍**和**已刪除物件**部分切換到虛擬管理伺服器。

   在主選單中，管理伺服器將變更為您選擇的伺服器。

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 **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**新工作設定**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：

      - **指派工作給管理群組**

        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，則工作內容視窗中不會顯示**安全**頁籤，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是從清單匯入位址**

        您可以指定您要為其分配工作的裝置的 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。

      - **指派工作給裝置分類**

        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 Linux 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. 切換到要刪除的虛擬管理伺服器所屬的主實體管理伺服器：

   a. 在主選單中，選擇任意部分（**市場**、**主控台導覽**和**設定**除外），然後在頁面頂部點擊**顯示階層**按鈕。

   b. 在開啟的導覽窗格中，點擊主實體管理伺服器的名稱。
   在主選單中，管理伺服器將變更為您選擇的伺服器。

2. 透過以下方式之一移動到主實體管理伺服器的屬性：

   - 在導覽窗格中，將滑鼠遊標停留在所需虛擬管理伺服器的名稱上，然後按一下設定圖示 (⚙)。
   - 在主選單中，按一下管理伺服器名稱。

3. 在開啟的屬性頁面中，前往**管理伺服器**頁籤。

4. 選擇要刪除的虛擬管理伺服器。

5. 在功能表行中，點擊 **刪除**按鈕。

虛擬管理伺服器將被刪除。

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. 在主選單中，按一下管理伺服器名稱。
   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 錯誤將被儲存到檔案 /var/opt/kaspersky/klnagent_srv/logs/SC.syslog。

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作業系統記錄。新事件被列隊，然後在刪除操作後被儲存到資料庫。預設情況下，事件佇列的上限為 20,000 個事件。您可以透過編輯 KLEVP_MAX_POSTPONED_CNT 標誌的值來自訂佇列上限。

要限制儲存在管理伺服器事件儲存區中的事件的數量：

1. 在主選單中，按一下管理伺服器名稱。

   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。

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。

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. 將管理伺服器安裝在新裝置上。

   請注意，如果將資料庫伺服器移動到其他裝置上，請將本機位址指定為安裝資料庫的裝置的 IP 位址（安裝卡巴斯基安全管理中心 Linux 操作說明中的“h”項目）。如果需要將資料庫伺服器保留在前一個裝置上，在安裝卡巴斯基安全管理中心 Linux操作說明的“h”項目中輸入前一個裝置的 IP 位址。

7. 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。

8. 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。

9. 驗證所有受管理裝置都已連線到管理伺服器。

10. 從之前的裝置中解除安裝管理伺服器和資料庫伺服器。

變更管理伺服器名稱

變更伺服器名稱的步驟可能會因您的環境而異。您可以選擇下列其中一種情境來變更伺服器名稱：

- 透過新增 DNS 記錄來維持連線。
- 透過切換為以 IP 位址為基礎的連線方式來維持連線。
- 變更伺服器名稱後恢復中斷的連線。

如果您在變更伺服器名稱時遇到困難，請聯絡技術支援。

透過新增 DNS 記錄來維持連線

在此情況下，重新命名管理伺服器後，受管理裝置和卡巴斯基安全管理中心網頁主控台會繼續連線至舊的管理伺服器位址。若要進行此設定，請新增下列其中一種 DNS 記錄類型：

- 舊管理伺服器位址的 A 記錄，指向新的管理伺服器 IP 位址。
- 將舊管理伺服器名稱對應到新管理伺服器名稱的 CNAME 記錄。

  如需有關設定必要記錄的詳細資訊，請參閱您的 DNS 伺服器文件。

若要透過新增新的 DNS 記錄保留連線：

1. **變更伺服器名稱**。

   由於安裝期間元件的設定方式，若不重新安裝管理伺服器，您無法變更管理伺服器名稱。

   若要變更伺服器名稱：

   1. 使用 klbackup 公用程式建立新的管理伺服器備份。
   2. 在所有管理員工作站上解除安裝卡巴斯基安全管理中心 Linux 和 卡巴斯基安全管理中心網頁主控台。
   3. 手動刪除管理伺服器資料庫和 IAM 資料庫。管理伺服器在解除安裝期間不會自動刪除這些資料庫。
   4. 根據您的作業系統說明文件，在管理伺服器的作業系統中重新命名裝置。
   5. 使用管理伺服器的新 FQDN 安裝卡巴斯基安全管理中心 Linux 管理伺服器。
   6. 安裝後，還原先前準備的 管理伺服器備份。
   7. 檢查 IAM 伺服器組態，如有必要，將管理伺服器位址新增至 IAM 伺服器組態檔。
   8. 在回應檔中指定管理伺服器的新 FQDN，在所有管理員工作站上安裝網頁主控台。

2. 為舊管理伺服器位址新增 DNS 記錄。
3. 在卡巴斯基安全管理中心網頁主控台的管理伺服器設定中指定新位址。
4. 在可直接存取管理伺服器的裝置上執行 **變更管理伺服器** 工作。之後，受管理裝置將能夠使用新名稱連線至管理伺服器。

   > 請勿在無法直接存取伺服器的裝置上執行此工作，否則這些裝置將失去與管理伺服器和連線閘道的連線。

   透過連線閘道連線的受管理裝置不會檢查管理伺服器名稱。因此，無需對這些裝置採取任何其他動作。管理伺服器位址的資訊不會在 klnagchk 診斷命令 的輸出中更新。

伺服器名稱變更後，與管理伺服器的連線會保留。

變更伺服器名稱後，憑證資訊將會過時。由於這不會影響元件運作，因此我們不建議在排程外取代自我簽署憑證。這些憑證會在安裝卡巴斯基安全管理中心期間產生，並由伺服器自動更新。在下一次自動憑證更換期間，這些憑證將以新的管理伺服器名稱重新簽發。

重新安裝期間，系統將為 IAM 伺服器和網頁主控台伺服器簽發新的憑證。如有必要，請將這些憑證取代為由您的憑證授權單位針對新的管理伺服器名稱所簽發的自訂憑證。如需詳細資訊，請參閱以下文章：關於卡巴斯基安全管理中心 Linux 憑證。

透過切換為以 IP 位址為基礎的連線方式來維持連線

在此案例中，受管理裝置連線至管理伺服器的方式會變更。裝置會使用管理伺服器 IP 位址，而不是管理伺服器名稱進行連線。切換所有受管理裝置可能需要一些時間，具體取決於裝置數量，以及它們在具有管理伺服器的網路上出現的頻率。

若要透過切換至以 IP 位址為基礎的連線方式來保留連線：

1. **在變更管理伺服器名稱之前，準備卡巴斯基安全管理中心基礎架構**。

   1. 使用 IP 位址將受管理裝置連線至管理伺服器。變更管理伺服器名稱後，使用其名稱進行連線的裝置將會與伺服器中斷連線。若要透過 IP 位址連線，請在可直接看見管理伺服器的裝置上執行「變更管理伺服器」工作，包括作為連線閘道的裝置。

      請勿在無法直接看見伺服器的裝置上執行該工作，否則這些裝置將失去與管理伺服器和連線閘道的連線。

      透過連線閘道連線的受管理裝置不會檢查管理伺服器名稱。因此，無需對這些裝置採取任何其他動作。管理伺服器位址的資訊不會在 klnagchk 診斷命令 的輸出中更新。

   2. 請確保所有受管理裝置都透過 IP 位址連線至管理伺服器。為此，請檢查以下項目：

      - 可直接看見管理伺服器的受管理裝置上，管理伺服器位址列中的 klnagchk 診斷命令結果。
      - 在裝置上安裝時，網路代理安裝套件的屬性資訊。

        網路代理必須一開始即設定為使用 IP 位址連線至管理伺服器。

        如果您未先解除安裝網路代理，就在現有安裝上安裝網路代理，則網路代理設定中指定的管理伺服器連線位址和憑證將不會更新。

   3. 在現有管理伺服器連線設定檔中指定新名稱。

   4. 如果您使用行動裝置管理角色（管理 Android 和 iOS 裝置），請按照如何變更使用 Kaspersky Endpoint Security for Android 並搭配 MDM 或 KSMM 角色的行動裝置上的管理伺服器位址 中的指示。

2. **變更伺服器名稱**。

   由於安裝期間元件的設定方式，若不重新安裝管理伺服器，您無法變更管理伺服器名稱。

   若要變更伺服器名稱：

   1. 使用 klbackup 公用程式建立新的管理伺服器備份。
   2. 在所有管理員工作站上解除安裝卡巴斯基安全管理中心 Linux 和 卡巴斯基安全管理中心網頁主控台。
   3. 手動刪除管理伺服器資料庫和 IAM 資料庫。管理伺服器在解除安裝期間不會自動刪除這些資料庫。
   4. 根據您的作業系統說明文件，在管理伺服器的作業系統中重新命名裝置。
   5. 使用管理伺服器的新 FQDN 安裝卡巴斯基安全管理中心 Linux 管理伺服器。
   6. 安裝後，還原先前準備的 管理伺服器備份。
   7. 檢查 IAM 伺服器組態，如有必要，將管理伺服器位址新增至 IAM 伺服器組態檔。
   8. 在回應檔中指定管理伺服器的新 FQDN，以在所有管理員工作站上安裝網頁主控台。

3. **在管理伺服器設定中更新管理伺服器位址**。

   變更管理伺服器名稱後，請在卡巴斯基安全管理中心網頁主控台的管理伺服器設定中指定新的 FQDN 位址。為此，請檢查並更新下列各設定中的 FQDN 位址：

   - 卡巴斯基安全網路代理伺服器位址
   - 網頁伺服器
   - 網路代理安裝套件屬性
   - 安全碼簽發者名稱 (2FA)

   此外，請執行下列操作：

   - 請在其他卡巴斯基應用程式的政策與設定中指定新的伺服器名稱。
   - 重新發布每個已發布的獨立套件和行動裝置套件。
   - 如果您使用管理伺服器階層，且伺服器是依名稱而非依 IP 位址連線，請重新連線從屬管理伺服器。

4. 在可直接存取管理伺服器的裝置上執行 **變更管理伺服器** 工作，以將受管理裝置上的連線位址變更為新的管理伺服器名稱。

伺服器名稱變更後，與管理伺服器的連線仍會保留。

變更伺服器名稱後，憑證資訊將會過時。由於這不會影響元件運作，因此我們不建議在排程外取代自我簽署憑證。這些憑證會在安裝卡巴斯基安全管理中心期間產生，並由伺服器自動更新。在下一次自動憑證更換期間，這些憑證將以新的管理伺服器名稱重新簽發。

重新安裝期間，系統將為 IAM 伺服器和網頁主控台伺服器簽發新的憑證。如有必要，請將這些憑證取代為由您的憑證授權單位針對新的管理伺服器名稱所簽發的自訂憑證。如需詳細資訊，請參閱以下文章：關於卡巴斯基安全管理中心 Linux 憑證。

變更伺服器名稱後恢復中斷的連線

此情境適用於下列情況：

- 如果您已失去管理伺服器所在裝置之網域名稱的所有權，但仍可存取管理伺服器。
- 如果管理伺服器不再管理受管理裝置。
- 如果因其他原因無法為舊的卡巴斯基安全管理中心 Linux 位址新增 DNS 記錄。

若要在變更伺服器名稱後還原中斷的連線：

1. **變更伺服器名稱**。

   由於安裝期間元件的設定方式，若不重新安裝管理伺服器，您無法變更管理伺服器名稱。

若要變更伺服器名稱：

1. 使用 klbackup 公用程式建立新的管理伺服器備份。
2. 在所有管理員工作站上解除安裝卡巴斯基安全管理中心 Linux 和 卡巴斯基安全管理中心網頁主控台。
3. 手動刪除管理伺服器資料庫和 IAM 資料庫。管理伺服器在解除安裝期間不會自動刪除這些資料庫。
4. 根據您的作業系統說明文件，在管理伺服器的作業系統中重新命名裝置。
5. 使用管理伺服器的新 FQDN 安裝卡巴斯基安全管理中心 Linux 管理伺服器。
6. 安裝後，還原先前準備的 管理伺服器備份。
7. 檢查 IAM 伺服器組態，如有必要，將管理伺服器位址新增至 IAM 伺服器組態檔。
8. 在回應檔中指定管理伺服器的新 FQDN，以在所有管理員工作站上安裝網頁主控台。

2. **在管理伺服器設定中更新管理伺服器位址**。

   變更管理伺服器名稱後，請在卡巴斯基安全管理中心網頁主控台的管理伺服器設定中指定新的 FQDN 位址。為此，請檢查並更新下列各設定中的 FQDN 位址：

   - 卡巴斯基安全網路代理伺服器位址
   - 網頁伺服器
   - 網路代理安裝套件屬性
   - 安全碼簽發者名稱 (2FA)

   此外，請執行下列操作：

   - 請在其他卡巴斯基應用程式的政策與設定中指定新的伺服器名稱。
   - 重新發布每個已發布的獨立套件和行動裝置套件。
   - 如果您使用管理伺服器階層，且伺服器是以名稱而非 IP 位址連線，請重新連線從屬管理伺服器。

3. 在先前受管理的裝置上還原與管理伺服器的連線：

   - 在可直接連線至管理伺服器的裝置上，使用 klmover 公用程式指定包含新管理伺服器名稱的連線位址。如需詳細資訊，請參閱以下文章：使用 klmover 公用程式將網路代理連線至管理伺服器。
   - 在作為連線閘道的裝置上，重新安裝網路代理並重新設定連線閘道角色。如需詳細資訊，請參閱下列文章：在 DMZ 中新增連線閘道作為發佈點。
   - 透過連線閘道連線的裝置會在連線閘道還原後自動重新連線。網路代理連線至連線閘道時，不會使用管理伺服器名稱。

     請勿在透過連線閘道連線的裝置上使用 klmover 公用程式。如需詳細資訊，請參閱以下文章：將透過連線閘道連線至管理伺服器的裝置移至另一個管理伺服器。

伺服器名稱變更後，與管理伺服器的連線會還原。

變更伺服器名稱後，憑證資訊將會過時。由於這不會影響元件運作，因此我們不建議在排程外取代自我簽署憑證。這些憑證會在安裝卡巴斯基安全管理中心期間產生，並由伺服器自動更新。在下一次自動憑證更換期間，這些憑證將以新的管理伺服器名稱重新簽發。

重新安裝期間，系統將為 IAM 伺服器和網頁主控台伺服器簽發新的憑證。如有必要，請將這些憑證取代為由您的憑證授權單位針對新的管理伺服器名稱所簽發的自訂憑證。如需詳細資訊，請參閱以下文章：關於卡巴斯基安全管理中心 Linux 憑證。

變更 DBMS 憑證

有時，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。

更改管理伺服器資料庫憑據

要使用klsrvconfig公用程式在Linux環境中更改管理伺服器資料庫憑據：

1. 執行klsrvconfig公用程式：
   `sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred`
2. 指定一個新的帳戶名稱。您應該指定 DBMS 中存在之帳戶的憑證。
3. 輸入新密碼。
4. 指定新密碼進行確認。

管理伺服器資料庫憑據已變更。

更改IAM資料庫憑據

若要在Linux環境中透過修改組態檔來變更IAM資料庫憑據：

1. 查找 IAM 設定檔：/var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
2. 在 `dbms_iam` 區段中，在使用者和密碼欄位中指定新帳戶憑證。您應該指定 DBMS 中存在之帳戶的憑證。
3. 執行以下指令：
   `systemctl restart kliam_srv.service`

IAM資料庫憑據即已變更。

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）。

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。

在備份管理伺服器資料之前，請執行以下操作：

- **遵循在管理伺服器 16 或更早版本上建立備份並將其還原到 16.1 或更高版本的要求。**
  - 如果在管理伺服器 16 或更早版本上建立資料備份，並在管理伺服器 16.1 或更高版本上還原，則會啟用雙因素驗證。有關更多資訊，請參閱關於帳戶的雙因素驗證。

    為確保使用者可以使用已設定的雙因素驗證金鑰透過現有帳戶登入網頁主控台，並確保OpenAPI 自動化指令碼在還原後繼續運行，您必須執行下列步驟：

    - 為所有使用者啟用雙因素驗證
    - 管理員必須為其自己的帳戶設定雙因素驗證
    - 從雙因素驗證中排除所需帳戶

      如有需要，請將用於透過 OpenAPI 執行指令碼的整合帳戶新增至排除清單。

    如果在建立備份之前無法設定雙因素驗證，則使用者帳戶將被新增至雙因素驗證允許清單中，並在登入網頁主控台時能夠設定雙因素驗證。有關將帳戶新增至允許清單的更詳細條件，請參閱允許使用者配置雙因素驗證主題。

- 檢查虛擬管理伺服器是否已被新增至管理群組。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。

- 如果您想要備份或還原卡巴斯基安全管理中心容錯移轉叢集，您必須在備份或還原完成後停止整個叢集進行維護，然後重新啟動它。

您可以使用以下方式之一建立管理伺服器資料備份：

- 透過使用卡巴斯基安全管理中心網頁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 實用程式。該實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，該實用程式位於程式安裝時指定資料夾的根目錄中（通常是 /opt/kaspersky/ksc64/sbin/klbackup）。

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。
- 已為使用者帳戶配置雙因素驗證秘密金鑰。
- 被從雙因素驗證中排除的使用者帳戶清單。

您可以透過建立並執行資料備份任務或使用 klbackup 公用程式來建立管理伺服器資料的備份副本。只用使用 klbackup 公用程式才能進行管理伺服器資料還原。您必須在剛被安裝、與建立的備份副本具有相同或更新版本的管理伺服器的可運作實例上執行還原。請勿使用任何協力廠商工具進行備份或還原，並且如果可能，請在配置和資料傳輸完全完成之前不要刪除先前的卡巴斯基安全管理中心 Linux。

建立管理伺服器資料備份工作

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。

*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，它不會顯示在工作類型選取視窗中。

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 **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**清單中，選取**卡巴斯基安全管理中心 16.3**並在**工作類型**清單中選取**備份管理伺服器資料**。
4. 在相應的步驟中指定以下資訊：
   - 用於儲存備份副本的資料夾
   - 備份密碼（可選）
   - 要儲存的最大備份副本數
5. 若在**完成工作建立**步驟啟用**建立完成時開啟工作詳情**選項，您可修正預設工作設定。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。
6. 點擊**完成**按鈕。

工作被建立並顯示在工作清單。

使用 klbackup 公用程式備份和還原資料

您可以使用卡巴斯基安全管理中心發佈套件中隨附的 klbackup 實用程式複製管理伺服器資料以作備份和將來還原之用。

在執行還原的管理伺服器上的實例，必須使用相同類型的 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。

如果您在使用早期版本的 MariaDB DBMS 時備份了卡巴斯基安全管理中心 Linux 15 或更早版本中包含的管理伺服器的資料，然後在具有更高版本的 MariaDB 的裝置上還原資料，可能會發生錯誤。有關詳細資訊，請參閱如何從在早期 DBMS 版本上建立的備份還原管理伺服器資料。

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。

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。

公用程式的命令列語法：

```
klbackup -path <備份路徑> [-linux_path <資料庫管理系統備份路徑>-node_cert <憑證路徑>] [-logfile <日誌檔案> [-use_ts]|[-restore] [-password <密碼>] [-cert_only]
```

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）。
- `-linux_path <DBMS backup path>` — 包含 DBMS 備份資料的資料夾的本機路徑。

  資料庫伺服器帳戶和 klbackup 公用程式需要獲得變更 DBMS 備份資料夾中資料的權限。
- `-node_cert <certificate path>` — 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。
- `-logfile <log file>` — 儲存關於管理伺服器資料備份和還原的報告。

  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。
- `-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 `/tmp/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。要從備份還原管理伺服器的資料，建議在新安裝的管理伺服器上執行該公用程式。

- `-cert_only`：僅儲存或還原管理伺服器的憑證和金鑰。

  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，此標誌可能會有用。此外，您還可以在卡巴斯基安全管理中心 Linux 管理伺服器之間以及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。

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 的管理下。
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，您必須將 `lower_case_table_names` 參數設定為與為 Windows 指定的該參數的值相同的值。

如果在還原中，管理伺服器通用憑證會被備份中的另一個憑證替換，請執行下列步驟以確保正常運作：
1.重新安裝網頁主控台以避免下列錯誤：
管理伺服器使用不受信任的憑證。請透過指定有效憑證重新設定應用程式，或聯絡主管理員。
2.檢查IAM伺服器組態，如有必要，將管理伺服器位址新增至IAM伺服器組態檔。

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，您還可以在卡巴斯基安全管理中心 Linux 管理伺服器之間以及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。

開始之前，**請檢查自訂憑證的需求**。

如果您使用的是自訂憑證而不是自簽名憑證，則在將Kaspersky Security Center for Linux升級到更高版本之前，必須確保憑證包含主體替代名稱（SAN）。否則，請務必在升級 Kaspersky Security Center for Linux 之前替換憑證。否則，升級後您將無法登入網頁主控台。

若要確保憑證包含SAN，請執行下列操作：

1. 在安裝了管理伺服器的裝置上，執行以下命令：

   - 對於Linux裝置：

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

   - 對於Windows裝置：

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. 確保命令輸出中存在主題備用名稱，并包含管理伺服器裝置的地址。

3. 如果缺少主題備用名稱，請使用klsetsrvcert公用程式將自訂憑證替換為滿足需求的憑證。

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. 在之前的裝置上，建立管理伺服器憑證和私鑰的備份副本。

   您可以使用下列方法之一建立備份副本：

   - 透過使用 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。

   - 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 實用程式，以建立管理伺服器憑證和私密金鑰的備份副本：

     `klbackup -path <管理伺服器憑證備份副本的路徑> -cert_only`

2. 在之前的裝置上，中斷管理伺服器與網路的連線。

3. 將相同的域名指派給具有其他管理伺服器的裝置。

   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的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）。

   如果無法為具有其他管理伺服器的裝置分配相同的地址，則必須產生新的管理伺服器憑證並在 IAM 設定檔中指定此憑證。安裝管理伺服器後，您需要手動將網路代理切換到新的管理伺服器。

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：

   - 透過使用 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。

   - 使用命令提示字元（對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
```

5. 設定管理伺服器和IAM伺服器的憑證驗證。

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。

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 PostgreSQL 作為 DBMS）：
  - 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 Linux 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 **工作**。
2. 按一下**新增**按鈕。

   新工作精靈啟動。
3. 在精靈的**新工作設定**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。

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. 在主選單中，按一下管理伺服器名稱。
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。

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，卡巴斯基安全管理中心 Linux 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 Linux 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. 執行命令行，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目錄中。預設安裝路徑為/opt/kaspersky/ksc64/sbin。
2. 要停用公共 DNS 的使用，請在根帳戶下執行以下指令：

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
   ```

3. 要啟用公共 DNS 的使用，請在根帳戶下執行以下指令：

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
   ```

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，轉至**設定** → **介面選項**。
2. 啟用或停用所需的選項：
   - **顯示資料加密與防護**
   - **顯示 EDR 警示**
3. 按一下**儲存**。

啟用所需選項後，主控台會在主功能表中顯示對應區域。例如，如果您啟用 **顯示 EDR 警示**，**監控** → **警示**區域會出現在主功能表中。

到管理伺服器的加密連線

用戶端裝置和管理伺服器之間的資料交換可以使用 TLS（傳輸層安全）協定進行。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。

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。

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上啟用 TLS 加密協定和受支援的密碼套裝。卡巴斯基安全管理中心 Linux 支援 TLS 協定版本 1.0、1.1、1.2 和 1.3。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 Linux 使用自簽發憑證。您也可以使用您自己的憑證。卡巴斯基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裝：

1. 執行命令行，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目錄中。預設安裝路徑為/opt/kaspersky/ksc64/sbin。

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。在根帳戶下的命令行中執行以下命令：

   ```
   ./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 和 TLS 1.3 協定。此外，還啟用了具有 TLS_RSA_WITH_AES_256_GCM_SHA384 的密碼套裝（必須具有這些密碼套裝，才能向後相容卡巴斯基安全管理中心 Linux 的先前版本）。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

TLS 1.3 協定支援的密碼套裝：

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

- 5 — 僅啟用 TLS 1.2 和 TLS 1.3 協定。對於 TLS 1.2 和 TLS 1.3 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

  TLS 1.3 協定支援的密碼套裝：

  - TLS_AES_256_GCM_SHA384
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_128_CCM_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）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 Linux 服務：

   - 管理伺服器
   - 網頁伺服器
   - 啟動代理

這樣就啟用了使用 TLS 協定的流量加密。

您可以使用 KLTR_TLS12_ENABLED 和 KLTR_TLS13_ENABLED 標誌分別啟用對 TLS 1.2 和 TLS 1.3 協定的支援。這些標誌預設啟用。

要啟用或停用對 TLS 1.2 和 TLS 1.3 協定的支援：

1. 執行 klscflag 公用程式。

   執行命令行，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目錄中。預設安裝路徑為/opt/kaspersky/ksc64/sbin。

2. 在根帳戶下的命令行中執行以下命令之一：

   - 使用此指令啟用或停用對 TLS 1.2 協定的支援：

     ```
     ./klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS12_ENABLED -v <值> -t d
     ```

   - 使用此指令啟用或停用對 TLS 1.3 協定的支援：

     ```
     ./klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v <值> -t d
     ```

   指定旗標的 < 值 > 參數：

   - `1` — 啟用對 TLS 協定的支援。
   - `0` — 停用對 TLS 協定的支援。

用於與外部服務交互的網路設定

卡巴斯基安全管理中心 Linux 使用以下網路設定與外部服務交互。

網路設定	位址	敘述
連接埠： 443 協定： HTTPS	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。
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 Linux 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。

網路設定	位址	敘述
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	https://ds.kaspersky.com https://dc1.ksn.kaspersky-labs.com https://dc1-file.ksn.kaspersky-labs.com https://dc1-pp.ksn.kaspersky-labs.com https://dc1-st.ksn.kaspersky-labs.com/ https://dc1-cert.ksn.kaspersky-labs.com https://dc1-cf.ksn.kaspersky-labs.com https://dc1-file.ksn.kaspersky-labs.com https://dc1-kas.ksn.kaspersky-labs.com https://dc1-ml.ksn.kaspersky-labs.com https://dc1-pp.ksn.kaspersky-labs.com https://dc1-st.ksn.kaspersky-labs.com https://dc1.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	https://ksn-file-geo.kaspersky-labs.com https://ksn-verdict-geo.kaspersky-labs.com https://ksn-url-geo.kaspersky-labs.com https://ksn-a-p2p-geo.kaspersky-labs.com https://ksn-info-geo.kaspersky-labs.com https://ksn-cinfo-geo.kaspersky-labs.com	使用卡巴斯基安全網路。
連接埠：443、1443 協定：KSN	ksn://ksn-a-p2p-geo.kaspersky-labs.com ksn://ksn-a-stat-geo.kaspersky-labs.com ksn://ksn-ca-geo.kaspersky-labs.com ksn://ksn-cinfo-geo.kaspersky-labs.com ksn://ksn-crypto-catm-geo.kaspersky-labs.com ksn://ksn-crypto-dnscheck-geo.kaspersky-labs.com ksn://ksn-crypto-hash-geo.kaspersky-labs.com ksn://ksn-crypto-ipm-geo.kaspersky-labs.com ksn://ksn-crypto-whocalls-geo.kaspersky-labs.com ksn://ksn-crypto-wifiplus-geo.kaspersky-labs.com ksn://ksn-eu-stat-kmp.kaspersky-labs.com ksn://ksn-file-geo.kaspersky-labs.com ksn://ksn-his-geo.kaspersky-labs.com ksn://ksn-info-geo.kaspersky-labs.com ksn://ksn-kas-geo.kaspersky-labs.com ksn://ksn-kddi.kaspersky-labs.com ksn://ksn-ml-geo.kaspersky-labs.com ksn://ksn-oui-geo.kaspersky-labs.com ksn://ksn-pp.kaspersky-labs.com ksn://ksn-src.kaspersky-labs.com ksn://ksn-stat-geo.kaspersky-labs.com ksn://ksn-tcert-geo.kaspersky-labs.com ksn://ksn-url-geo.kaspersky-labs.com ksn://ksn-verdict-geo.kaspersky-labs.com ksn://mdr.ksn.kaspersky-labs.com ksn://stat-eu.ksn.kaspersky-labs.com ksn://stat-hq.ksn.kaspersky-labs.com ksn://stat-ru.ksn.kaspersky-labs.com ksn://stat-sa.ksn.kaspersky-labs.com ksn://stat-sbr.ksn.kaspersky-labs.com	使用卡巴斯基安全網路。
連接埠：443 協定：HTTPS	https://click.kaspersky.com https://redirect.kaspersky.com	開啟介面中的連接。

網路設定	位址	敘述
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。
連接埠：443 協定：HTTPS	https://tip.kaspersky.com	透過 Kaspersky Threat Intelligence Portal 應對威脅（使用 Kaspersky Next XDR Optimum 功能時）。
連接埠：443 協定：HTTPS	有關完整位址清單，請參閱位址和網域結構文章	透過 Kaspersky Automated Security Awareness Platform 應對威脅（使用 Kaspersky Next XDR Optimum 功能時）。

為了讓卡巴斯基安全管理中心 Linux 與外部服務正確互動，請考量以下建議：
- 必須允許未加密的網路流量通過貴組織的網路設備和代理伺服器上的連接埠 443 和 1443。
- 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互動時，必須避免透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. 執行命令行，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目錄中。預設安裝路徑為/opt/kaspersky/ksc64/sbin。

2. 如果您想透過 HTTP 協定下載更新，請在根帳戶下執行以下命令之一：

   - 在安裝了管理伺服器的裝置上：

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

   - 在發佈點上：

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

   如果您想透過 HTTPS 協定下載更新，請在根帳戶下執行以下命令之一：

   - 在安裝了管理伺服器的裝置上：

     ```
     klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
     ```

   - 在發佈點上：

     ```
     klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
     ```

子網路全域清單

對於您使用的每台管理伺服器，您可以設定一個全域子網路清單來儲存有關網路子網路的資訊。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。

要新增子網路到子網路全域清單：

1. 在主選單中，按一下管理伺服器名稱。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**全域子網路**區段。
3. 點擊**新增**按鈕。
   新子網路 視窗開啟。
4. 填充以下欄位：
   - **名稱**
   - **子網路位址**
   - **子網路遮罩**
   - **描述**
5. 按一下**儲存**按鈕。

視窗關閉，子網路出現在子網路清單中。

如有必要，您可以在全域子網路清單中執行下列操作：

- 透過選擇所需子網路並點擊**移除**按鈕，從清單中刪除子網路。
- 按一下所需子網路名稱的連接，然後執行步驟 4-5 中所述的操作，修改子網路的屬性。

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 Linux 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 Linux 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 Linux 元件執行完整性檢查：

- 管理伺服器
- 網路代理

integrity_checker 實用程式對以下卡巴斯基安全管理中心 Linux 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 Linux 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 Linux 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 Linux 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。
  - `-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）。

您也可以設定完整性檢查，使其在啟動應用程式時自動啟動。預設情況下，自動進行完整性檢查處於停用狀態。

若要啟用自動進行完整性檢查：

1. 在安裝了管理伺服器的裝置上，在命令提示符處輸入以下命令：

   ```
   ./klscflag -fset -pv klserver -n KLMODCHK_ENABLE_CHECKING -t d -v 1
   ```

2. 重新啟動裝置。

   自動進行完整性檢查已啟用。

下次執行卡巴斯基安全管理中心時，klscmodchk 實用程式將與管理伺服器一起執行，並啟動模組完整性檢查。完整性檢查的結果將被寫入卡巴斯基事件記錄。

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 Linux 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。當所有網路裝置被發現時，您可以接收它們的資訊並透過政策管理。一般網路輪詢用於發現是否有新裝置以及先前發現的裝置是否仍在網路中。

網路裝置發現分步驟進行：

1. **初始裝置發現**

   完成快速啟動精靈後，手動執行裝置發現。

2. **配置未來輪詢**

   確保 IP 範圍輪詢被啟用且輪詢排程滿足您組織的需要。當設定輪詢排程時，使用建議的網路輪詢頻率。

   如果您的網路包含 IPv6 裝置，也可以啟用 Zeroconf 輪詢。

   如果網域中包含聯網裝置，建議使用網域控制器輪詢。

   使用Windows發佈點來輪詢Windows網路。

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**未指派的裝置**群組。如有需要，您可以設定自動移動這些裝置到**受管理裝置**群組。您也可以建立保留規則。

   如果您略過該規則設定步驟，所有先發現的裝置都移到**未指派的裝置**群組並留在該處。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 Linux 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**未指派的裝置**群組中）。

Windows 網路輪詢

關於 Windows 網路輪詢

卡巴斯基安全管理中心 Linux 管理伺服器不支援 Windows 網路輪詢。使用基於 Windows 的發佈點來輪詢 Windows 網路。

在快速輪詢過程中，發佈點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。

IP 範圍輪詢

卡巴斯基安全管理中心 Linux 嘗試使用標準 DNS 請求為指定範圍的每個 IPv4 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 Linux 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。如果該網域未被配置，IP 子網路輪詢將沒有結果。

開始，卡巴斯基安全管理中心 Linux 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 Linux 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 Linux 從 192.168.0.1 到 192.168.0.254 之間輪詢所有位址。

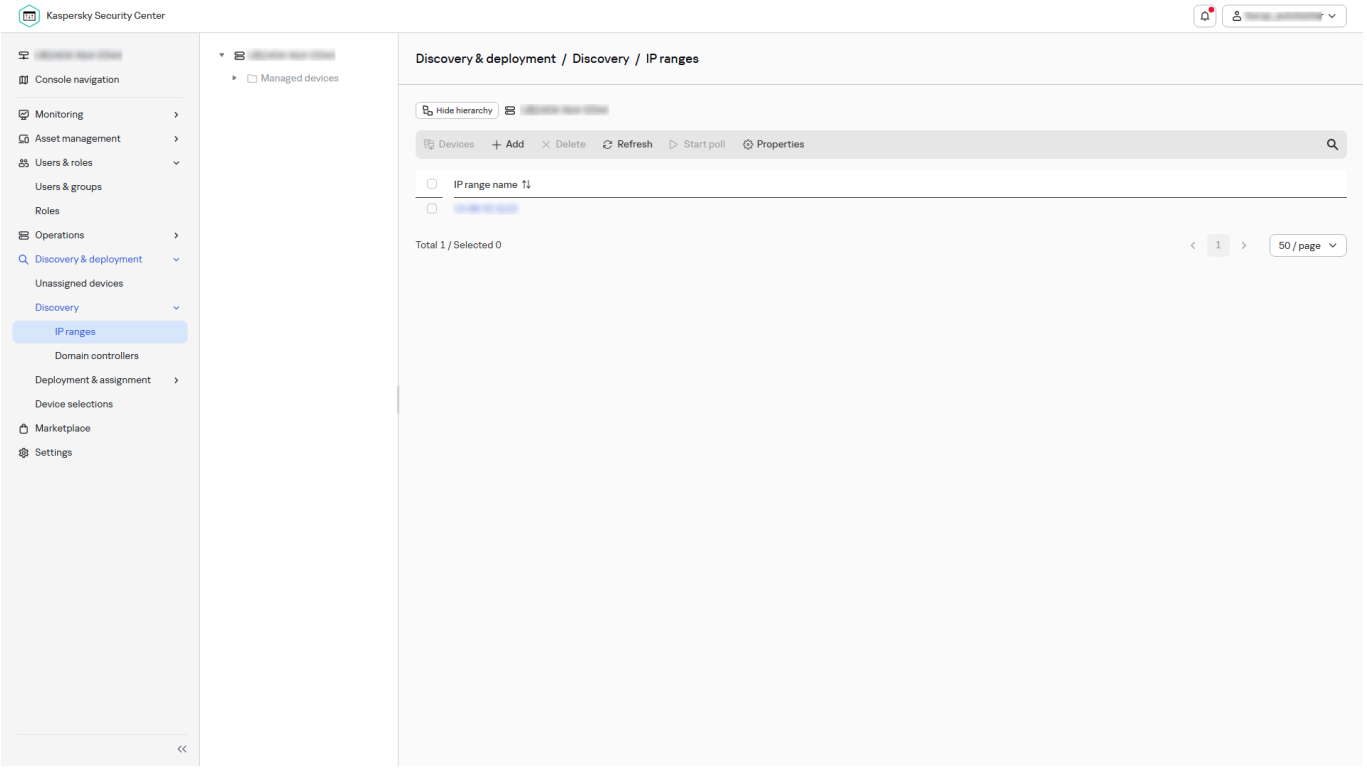
如果僅啟用 IP 範圍輪詢，卡巴斯基安全管理中心 Linux 將僅發現具有 IPv4 位址的裝置。如果您的網路包含 IPv6 裝置，請開啟裝置的 Zeroconf 輪詢。

對於 Microsoft Active Directory、Samba、FreeIPA 或 ALD Pro 網域控制器內的所有基於 Linux 的主機，請在 `/etc/samba/smb.conf` 檔案中指定 `netbios name` 和 `workgroup` 參數。否則，輪詢結果可能包含重複的主機。

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：

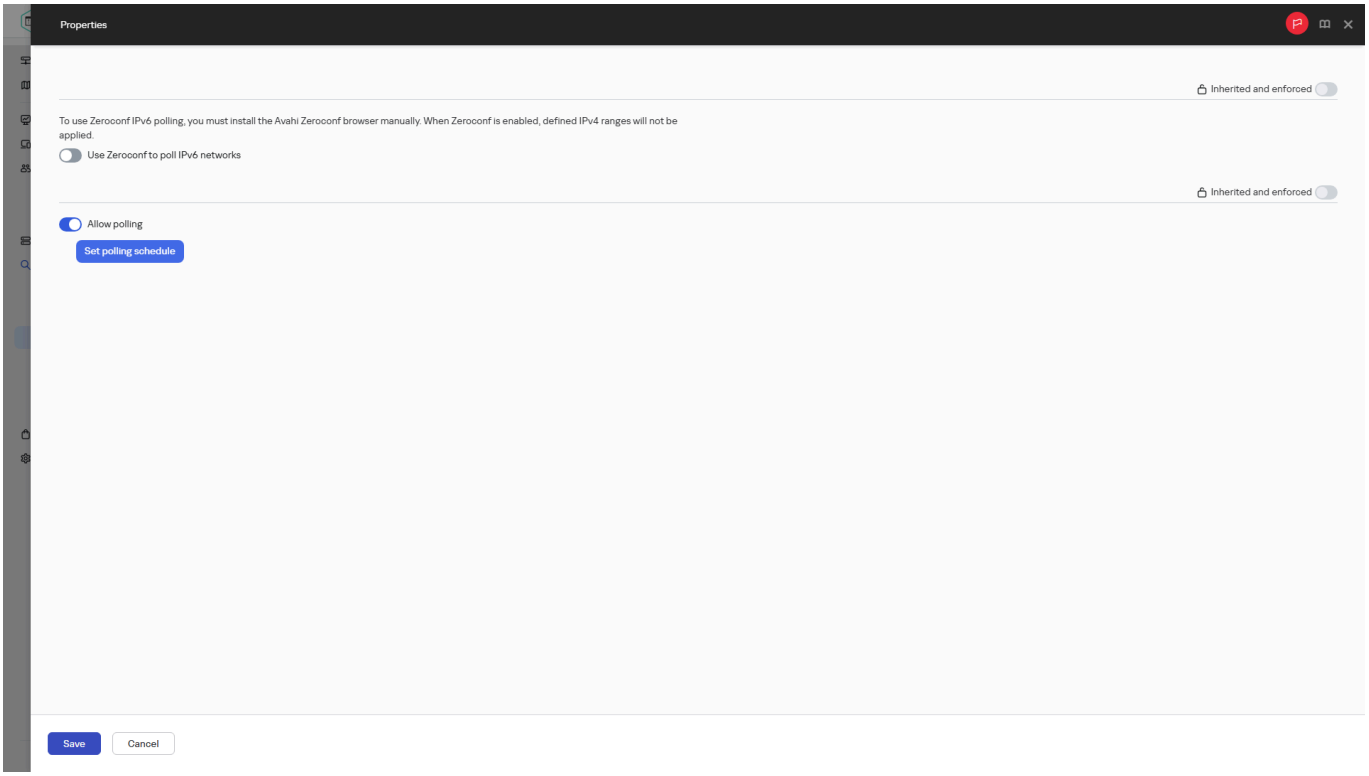
1. 在主功能表中，轉至 **發現和佈署** → **發現** → **IP 範圍**。



IP 範圍清單

2. 點擊**內容**按鈕。

IP 輪詢內容視窗將開啟。



IP 輪詢內容

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。

   - **按每週中的指定日**

     輪詢定期執行，在指定星期的指定時間。

   - **每月於選定的週間日**

     輪詢定期執行，在指定月日的指定時間。

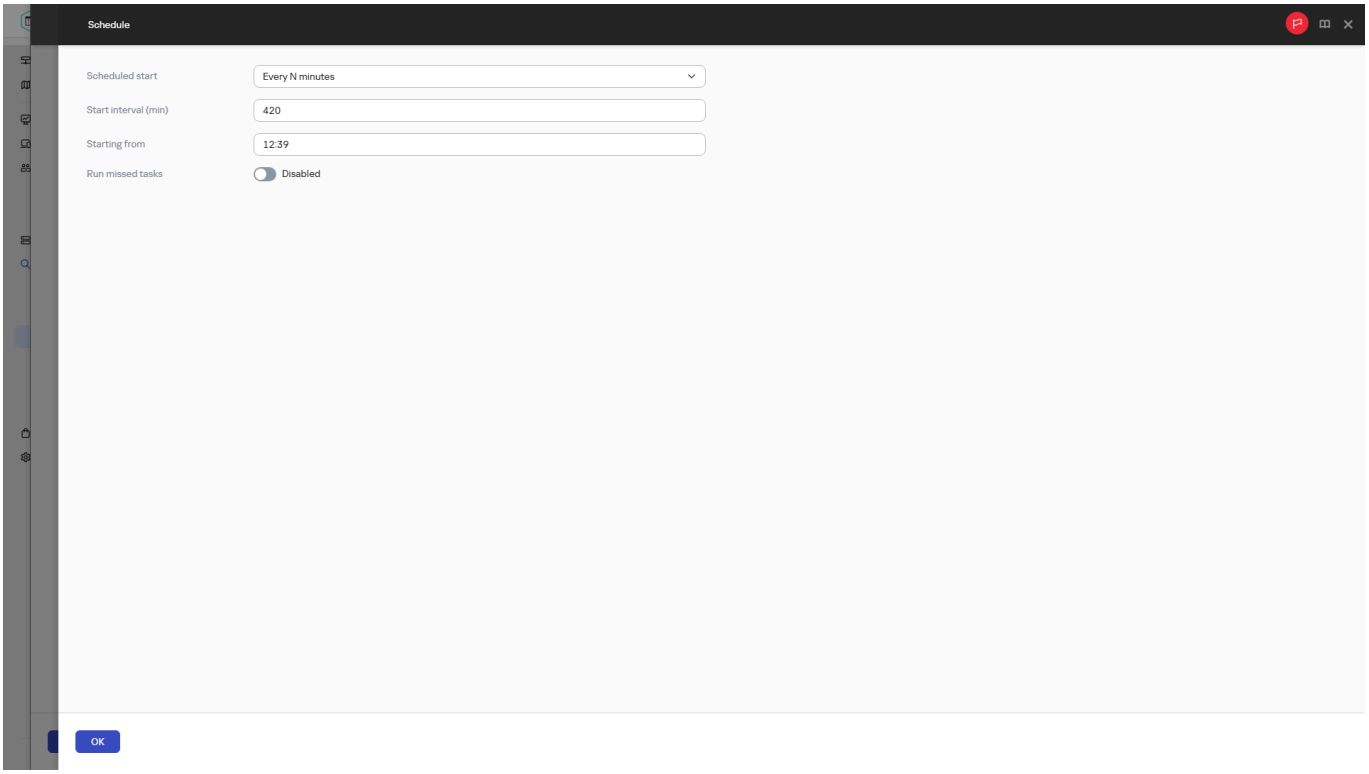
   - **執行錯過的工作**

     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。



配置輪詢排程

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**。

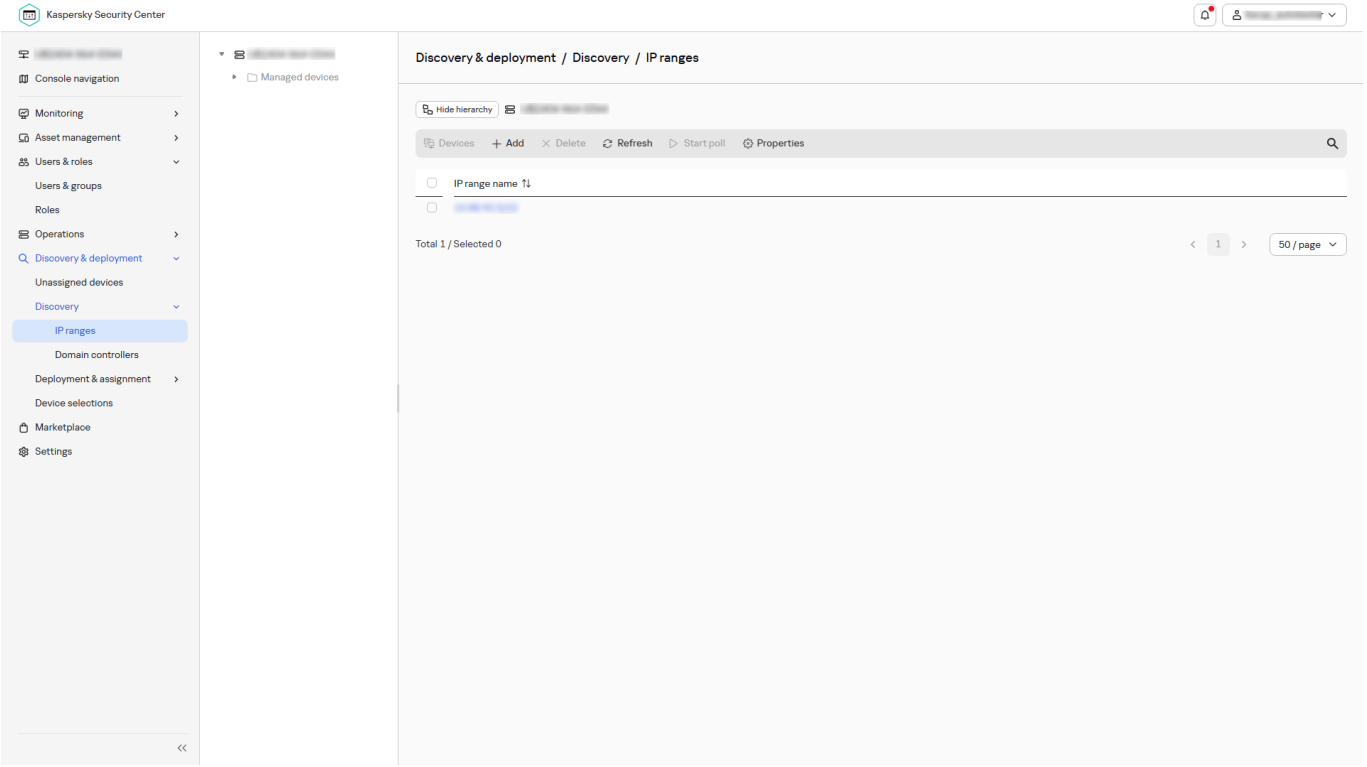
新增和修改 IP 範圍

開始，卡巴斯基安全管理中心 Linux 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 Linux 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 Linux 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 Linux 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**。



IP 範圍清單

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"。

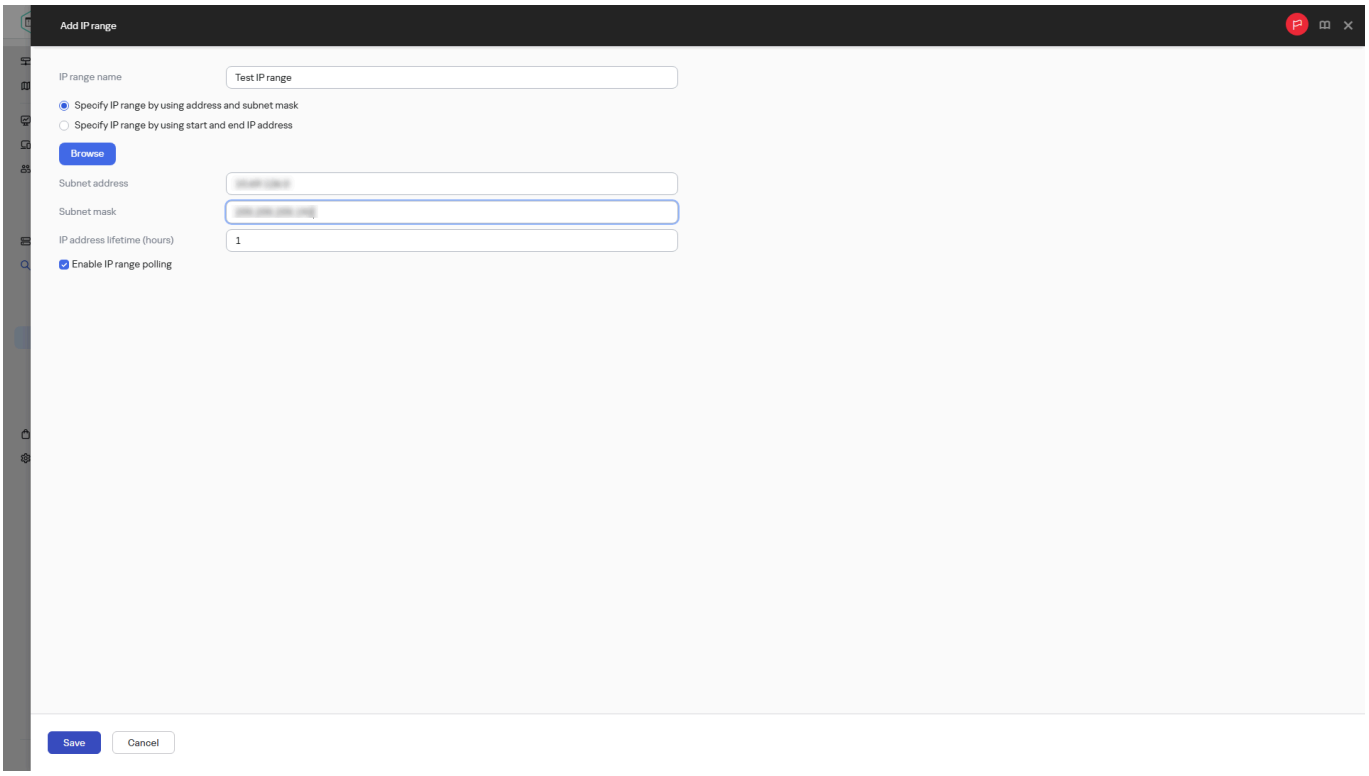
- **IP 間隔或子網路位址和遮罩**

  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。



指定 IP 範圍設定

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。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 的發佈點支援此輪詢類型。

卡巴斯基安全管理中心 Linux 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，卡巴斯基安全管理中心 Linux 將使用以下零配置網路（稱為"*Zeroconf*"）輪詢整個網路。要開始使用 Zeroconf，您必須在輪詢網路的 Linux 裝置（管理伺服器或發佈點）上安裝 avahi-browse 實用程式。

要啟用 Zeroconf 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，卡巴斯基安全管理中心 Linux 開始輪詢您的網路。在這種情況下，指定的 IP 範圍將被忽略。

網域控制器輪詢

卡巴斯基安全管理中心 Linux 支援輪詢下列網域控制器類型：

- Microsoft Active Directory
- Samba
- FreeIPA
- ALD Pro

對於 Samba 網域控制器， Samba 4 用作 Active Directory 網域控制器。

當您輪詢網域控制器時，管理伺服器或發佈點會檢索有關網域中包含的裝置的網域結構、使用者帳戶、安全群組和 DNS 名稱的資訊。

如果所有聯網裝置都是網域的成員，我們建議使用網域控制器輪詢。如果某些聯網裝置未包含在網域中，則網域控制器輪詢無法發現這些裝置。

先決條件

在輪詢網域控制器之前，請確保您有允許透過防火牆或代理伺服器連線到網域控制器。另請確保網域控制器上有啟用以下協定：

- 輕量級目錄訪問協定 (LDAP)
- 簡單身分驗證和安全層 (SASL)

  如果是使用 SASL 驗證建立與網域控制器的連線，則使用此協定。管理伺服器和發佈點僅支援 DIGEST-MD5 機制。
- 基於安全通訊端層的輕量級目錄存取協定 (LDAPS)

  如果需要透過加密連線連接到網域控制器，則使用此協定。

確保網域控制器裝置上的以下連接埠可用：

- 389 用於 LDAP 協定和簡單驗證 (包括 SASL)
- 636 用於 LDAPS 協定

> 對於 FreeIPA 和 ALD Pro，LDAP 和 LDAPS 協定僅用於網域輪詢。卡巴斯基安全管理中心 Linux 不支援透過 LDAP (S) 對 FreeIPA 帳戶進行身分驗證。若要允許 FreeIPA 和 ALD Pro 使用者登入網頁主控台，您必須透過 IAM 服務設定 Kerberos身分驗證。

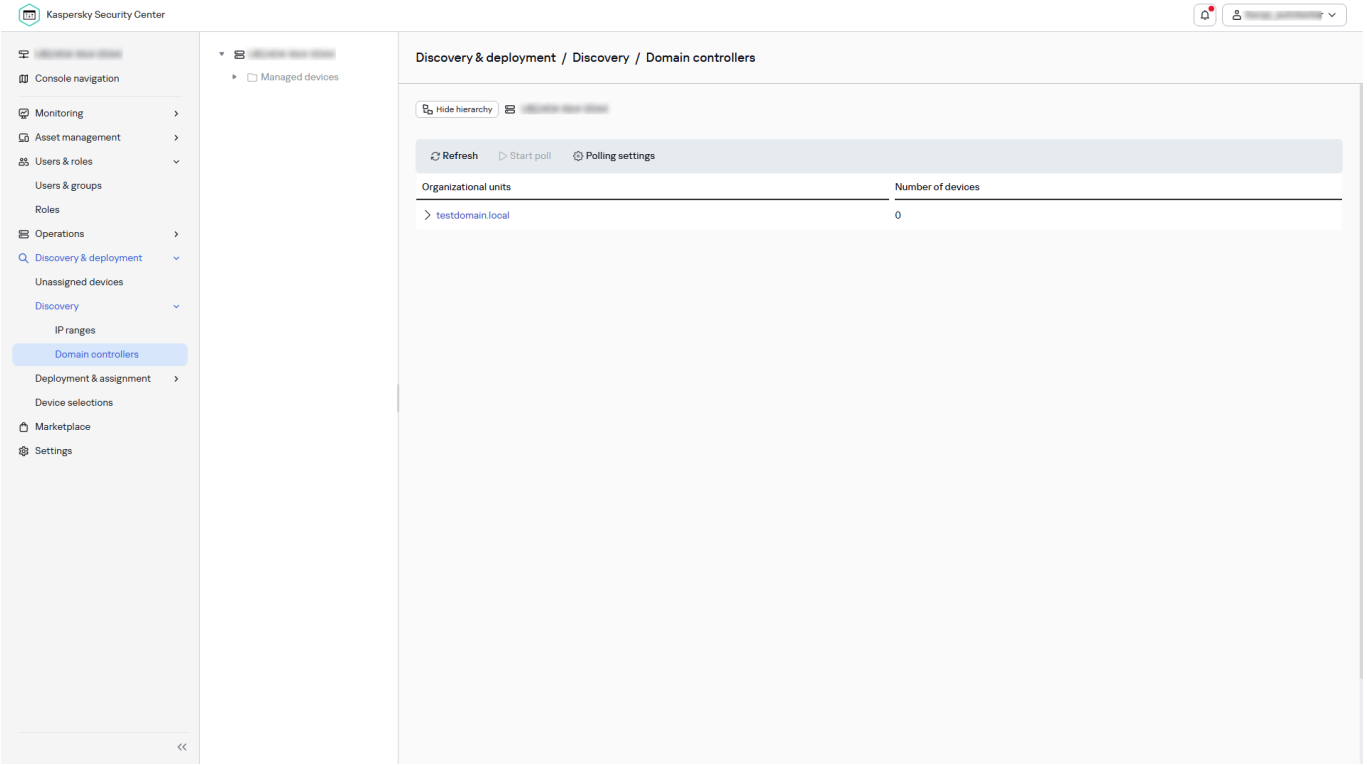
對於 Microsoft Active Directory、Samba、FreeIPA 或 ALD Pro 網域控制器內的所有 Linux 型主機，需要在 `/etc/samba/smb.conf` 檔案中指定 `netbios name` 和 `workgroup` 參數。否則，輪詢結果可能包含重複的主機。

> 如果 Microsoft Active Directory 網域包含多個網域控制器，則不支援在網域輪詢期間選取特定控制器。將與偵測到的第一個網域控制器建立連線。為確保與 Microsoft Active Directory 網域進行正確的身分驗證，憑證的「主體別名 (SAN)」欄位必須包含此網域中包含的所有網域控制器位址，以及 Microsoft Active Directory 網域的 NetBIOS 名稱。

使用管理伺服器進行網域控制器輪詢

要使用管理伺服器輪詢網域控制器：

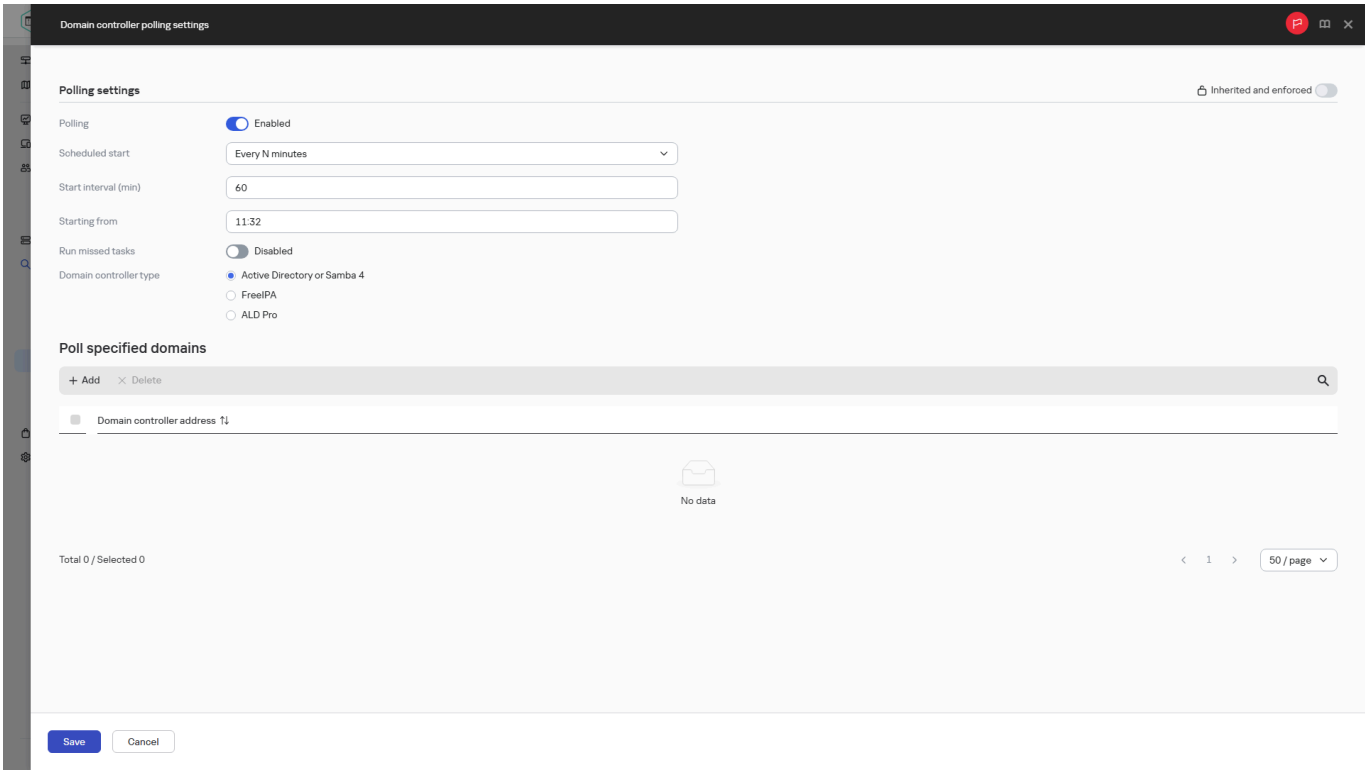
1. 在主功能表中，轉至**發現和佈署 → 發現 → 網域控制器**。



網域控制器輪詢視窗

2. 點擊**配置輪詢設定**。

   網域控制器輪詢設定視窗將開啟。



網域控制器輪詢設定

3. 在**輪詢**欄位中，將切換按鈕切換到**已啟用**位置。

4. 在**輪詢指定網域**中，點擊**新增** ，然後指定網域控制器的位址和使用者憑據。

5. 在**網域控制器輪詢設定**視窗中，執行下列操作：

- 選擇要輪詢的網域控制器的類型：**Active Directory 或 Samba 4**、**FreeIPA**、**ALD Pro**。
- 如果必要，指定輪詢排程。預設間隔是一小時。下次輪詢接收的資料完全取代舊資料。

  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。

  - **按每週中的指定日**

    輪詢定期執行，在指定星期的指定時間。

  - **每月於選定的週間日**

    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。

> 如果您變更網域安全群組中的使用者帳戶，這些變更將在您輪詢網域控制器一小時後顯示在卡巴斯基安全管理中心 Linux 中。

6. 點擊**儲存**以套用變更。

7. 如果您要立即執行輪詢，請點擊**開始輪詢**按鈕。

使用發佈點進行網域控制器輪詢

您還可以使用發佈點輪詢網域控制器。基於 Windows 或 Linux 的受管理裝置可以充當發佈點。

> 對於 Linux 發佈點，支援輪詢所有類型的網域控制器。
> 對於 Windows 發佈點，僅支援輪詢 Microsoft Active Directory 網域控制器。
> 不支援使用 Mac 發佈點進行輪詢。

要使用發佈點配置網域控制器輪詢：

1. 開啟發佈點內容。
2. 選擇**網域控制器輪詢**部分。
3. 在**輪詢**欄位中，將切換按鈕切換到**已啟用**位置。
4. 如果使用 Linux 發佈點，請選擇要輪詢的網域控制器的類型：**Active Directory 或 Samba 4**、**FreeIPA**、**ALD Pro**。

   當使用發佈點和管理伺服器設定輪詢時，無需指定相同的網域控制器類型。
5. 選擇要輪詢的網域控制器。

   如果您使用 Linux 發佈點，請在**輪詢指定網域**部分中點擊**新增**，然後指定網域控制器的位址和使用者憑據。

   如果您使用 Windows 發佈點，則可以選擇以下選項之一：

   - **輪詢目前網域**
   - **輪詢整個網域樹系**
   - **輪詢指定網域**
6. 如果需要，點擊**設定輪詢排程**按鈕以指定輪詢排程選項。

   輪詢僅根據指定的排程開始。無法手動啟動輪詢。

輪詢完成後，網域結構將顯示在**網域控制器**部分中。

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**未指派的裝置**群組。

被發現的使用者帳戶可用於在卡巴斯基安全管理中心網頁主控台中進行網域身分驗證。

身分驗證與網域控制器連線

輪詢網域時進行驗證並與網域控制器連線

輪詢網域控制器時，管理伺服器或發佈點會識別連線協定，以建立與網域控制器的初始連線。未來所有與該網域控制器的連線，都會使用此通訊協定。建立與網域控制器的初始連線時，您可使用網路代理標誌（`KLNAG_LDAP_TLS_REQCERT` 和 `KLNAG_LDAP_SSL_CACERT`）變更連線選項。您可以使用 klscflag 設定網路代理標誌，如本文所述。

初次與網域控制器連線的程序如下：

1. 管理伺服器或發佈點嘗試透過 LDAPS 連線到網域控制器。

   預設並不會要求執行憑證驗證。將 `KLNAG_LDAP_TLS_REQCERT` 標誌設為 1，即可強制執行憑證驗證。

   `KLNAG_LDAP_TLS_REQCERT` 標誌的可能值：

   - `0`：請求憑證，但如果未提供或憑證驗證失敗，仍認為 TLS 連線已成功建立（預設值）。
   - `1`：需要嚴格驗證 LDAP 伺服器憑證。

   預設情況下，如果未指定 `KLNAG_LDAP_SSL_CACERT` 標誌，會使用依作業系統而定的憑證授權單位 (CA) 路徑來存取憑證鏈。使用 `KLNAG_LDAP_SSL_CACERT` 旗標，即可指定自訂路徑。

2. 如果 LDAPS 連線失敗，管理伺服器或發佈點會嘗試使用 SASL (DIGEST-MD5)，透過非加密 TCP 連線連接到網域控制器。

向管理伺服器驗證網域使用者時進行驗證並與網域控制器連線

當網域使用者在管理伺服器上進行驗證時，管理伺服器會識別與網域控制器建立連線的協定。

> 對於 FreeIPA 和 ALD Pro，LDAP 和 LDAPS 協定僅用於網域輪詢。卡巴斯基安全管理中心 Linux 不支援透過 LDAP (S) 對 FreeIPA 帳戶進行身分驗證。若要允許 FreeIPA 和 ALD Pro 使用者登入網頁主控台，您必須透過 IAM 服務設定 Kerberos身分驗證。

與網域控制器連線的步驟如下：

1. 管理伺服器嘗試透過 LDAPS 連線到網域控制器。

   需要嚴格驗證 LDAP 伺服器憑證。

   預設情況下，如果未指定 `KLNAG_LDAP_SSL_CACERT` 標誌，會使用依作業系統而定的憑證授權單位 (CA) 路徑來存取憑證鏈。使用 `KLNAG_LDAP_SSL_CACERT` 旗標，即可指定自訂路徑。

2. 如果 LDAPS 連線失敗，則連線到網域控制器時會發生錯誤，且不會使用其他連線協定。

設定標誌

您可以使用 klscflag 公用程式設定旗標。

執行命令行，然後將目前目錄變更為包含 klscflag 公用程式的目錄。在管理伺服器裝置上，klscflag 公用程式位於安裝目錄中。預設安裝路徑為/opt/kaspersky/ksc64/sbin。

例如，以下命令會強制執行憑證驗證：

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

配置 Samba 網域控制器

卡巴斯基安全管理中心 Linux 支援僅在 Samba 4 上執行的 Linux 網域控制器。

Samba 網域控制器支援與 Microsoft Active Directory 網域控制器相同的架構延伸。您可以使用 Samba 4 架構延伸啟用 Samba 網域控制器與 Microsoft Active Directory 網域控制器的完全相容。這是一個可選操作。

> 我們建議啟用 Samba 網域控制器與 Microsoft Active Directory 網域控制器的完全相容。這將確保卡巴斯基安全管理中心 Linux 和 Samba 網域控制器之間的正確交互。

要啟用 Samba 網域控制器與 Microsoft Active Directory 網域控制器的完全相容：

1. 執行以下指令以使用 RFC2307 架構延伸：

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. 在 Samba 網域控制器中啟用架構更新。若要執行此操作，請將以下行新增至 `/etc/samba/smb.conf` 檔案：

   ```
   dsdb:schema update allowed = true
   ```

   > 如果架構更新完成時出現錯誤，則需要對充當架構主機的網域控制器執行完整還原。

對於 Samba 網域控制器中的所有 Linux 型主機，請在 `/etc/samba/smb.conf` 檔案中指定 `netbios name` 和 `workgroup` 參數。否則，輪詢結果可能包含重複的主機。

設備清查

您用於清查裝置的硬體清單（**資產管理→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 Linux 允許註銷設備。為此，請選取裝置內容中的**已勾銷**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. 在主功能表中，轉至**資產管理→硬體**。
2. 點選新增**新增**按鈕開啟**新裝置**視窗。
3. 在**新裝置**視窗中，從**裝置類型**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。
   - **已勾銷**。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**頁面的工作區中。

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. 在主功能表中，轉至**資產管理→硬體**。

2. 在**硬體**頁面頂部，點擊**設定企業裝置規則**連結。

   A **設定企業裝置規則** 面板被調用。

3. 在**設定企業裝置規則**面板中，啟用**為裝置自動設定「企業」裝置屬性**。指定對其自動分配*企業*屬性的裝置類型。

   > 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。

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 Linux 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。此外，卡巴斯基安全管理中心網頁主控台中可能會顯示不存在的虛擬機。

為了防止不存在的虛擬機被儲存，卡巴斯基安全管理中心 Linux 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 動態模式支援。

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. 在主功能表中，轉至**軟體管理→安裝套件**。

2. 在網路代理安裝套件的右鍵，選取“**內容**”。

   內容視窗隨即開啟。

3. 在**內容**視窗中，選取**進階**區域。

4. 在**進階**區段上選取**為 VDI 啟用動態模式**選項。

   要安裝網路代理的裝置將成為 VDI 的一部分。

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. 轉至**資產管理 → 移動規則**。
2. 點擊**新增**。
3. 在**規則條件**頁簽上，選擇**虛擬機**頁簽。
4. 將**這是一台虛擬機**規則設定為**是** ，將**虛擬桌面基礎架構的一部分**設定為**是。**
5. 點擊**儲存**。

管理用戶端裝置

卡巴斯基安全管理中心 Linux 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。**規則條件**裝置可以根據規則條件自動分配到群組：

- 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. 在主功能表中，轉至 **資產管理 → 資產（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。

所選裝置的內容視窗隨即顯示。

以下分頁顯示在屬性視窗的上部，代表主設定群組：

- **一般**

  此頁籤包含以下部分：

  - **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。

    - **描述**

      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。

- **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。

- **完整的群組名稱**

  包括了用戶端裝置的管理群組。

- **上次病毒資料庫更新**

  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 卡巴斯基安全管理中心 Linux 中建立裝置的日期。

- **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。

- **連線**

  本節包含一個表格，其中含有有關目前登入裝置的使用者的資訊。該表格在對應的欄中顯示以下資料：

  - 使用者名稱
  - SAM 帳戶名稱
  - 使用者主體名稱
  - 電子郵件地址

  若要正確顯示有關網域使用者工作階段的資訊，必須使用網域控制器輪詢。

- **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**

    包含裝置的工作組。
  - **DNS 名稱**

    用戶端裝置的 DNS 網域名稱。
  - **NetBIOS 名稱**

    用戶端裝置的名稱。
  - **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。
  - **狀態描述**

    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。

  檔案只能在安裝了 Kaspersky Endpoint Security for Windows 的受管理裝置上進行加密。

- **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 Linux 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。如果推送伺服器無法與受管理裝置建立連線，但啟用了與管理伺服器的持續連線模式（啟用了**一般**部分中的**不斷開與管理伺服器的連線**選項），則也可以使用工作操作。

  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。

  您可以匯出、複製和刪除裝置事件。

- **安全問題**

  在**安全問題**頁籤中，您可為用戶端裝置檢視、編輯和建立安全問題。安全問題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，則管理員可以建立安全問題。管理員可以在安全問題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安全問題稱為*已處理安全問題*。存在的未處理安全問題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安全問題的清單。安全問題按照幾個等級和類型分類。安全問題的類型是由建立安全問題的 Kaspersky 應用程式定義。選中**已處理**列中的核取方塊即可突出顯示清單上的已處理安全問題。

- **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查檔案。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。

    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
    - CPU
    - 網卡
    - 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
    - CPU
    - 網卡

- **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**匯出到 CSV**按鈕或**匯出到 TXT**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：

        - 在這部受管理裝置上忽略軟體弱點（在卡巴斯基安全管理中心網頁主控台中）。
        - 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（在卡巴斯基安全管理中心網頁主控台中）。
        - 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。

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週期。

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。

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 實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 實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 Linux 常見問題解答。

裝置移動規則

建議您，將裝置設定為透過*裝置移動規則*自動指派到管理群組。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 Linux 管理員明確建立，在**資產管理** → **移動規則**區域中。

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。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）。

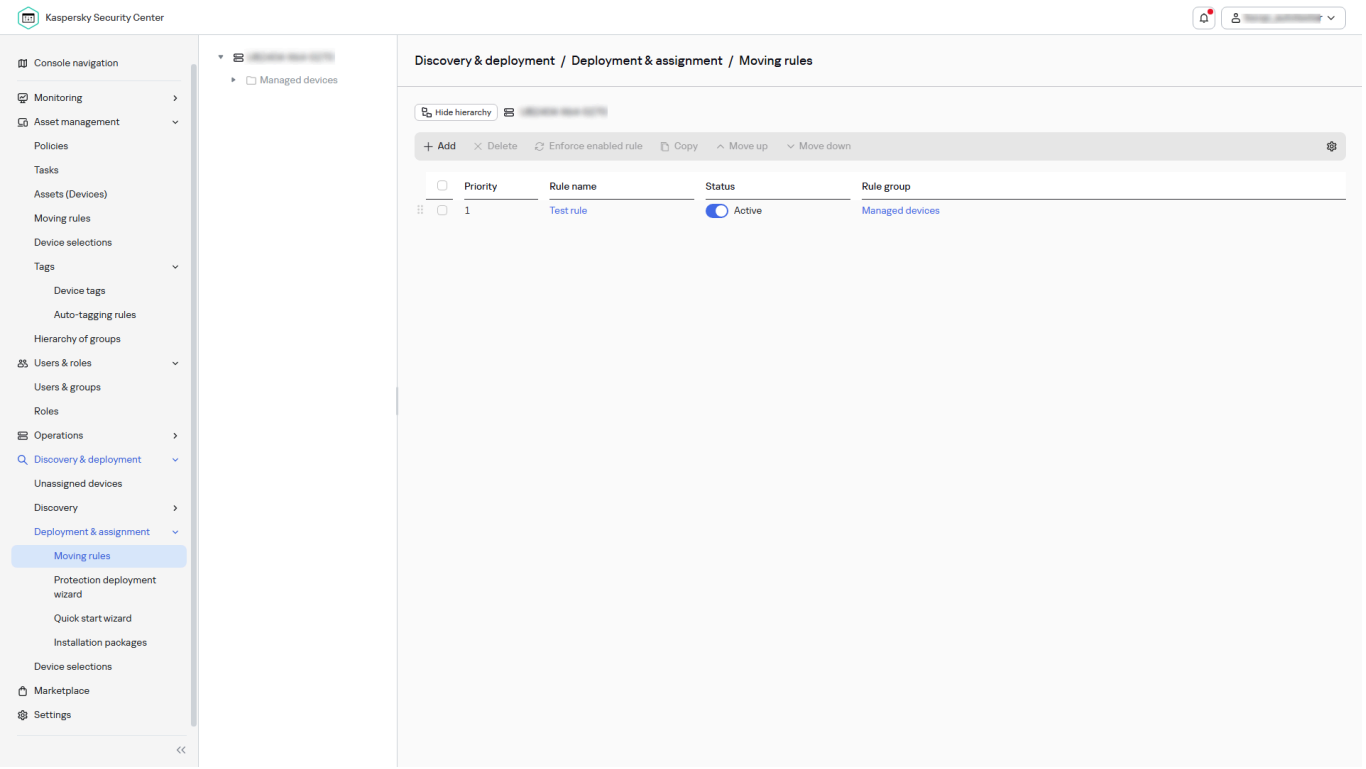
此類方案不被支援，因為它們顯著增加了管理伺服器負載和網路流量。這些方案也與卡巴斯基安全管理中心 Linux 的操作原則衝突（尤其在存取權限、事件和報告方面）。必須找到其他解決方案，例如，透過使用政策設定檔、裝置分類的工作、根據標準方案分配網路代理。

建立裝置移動規則

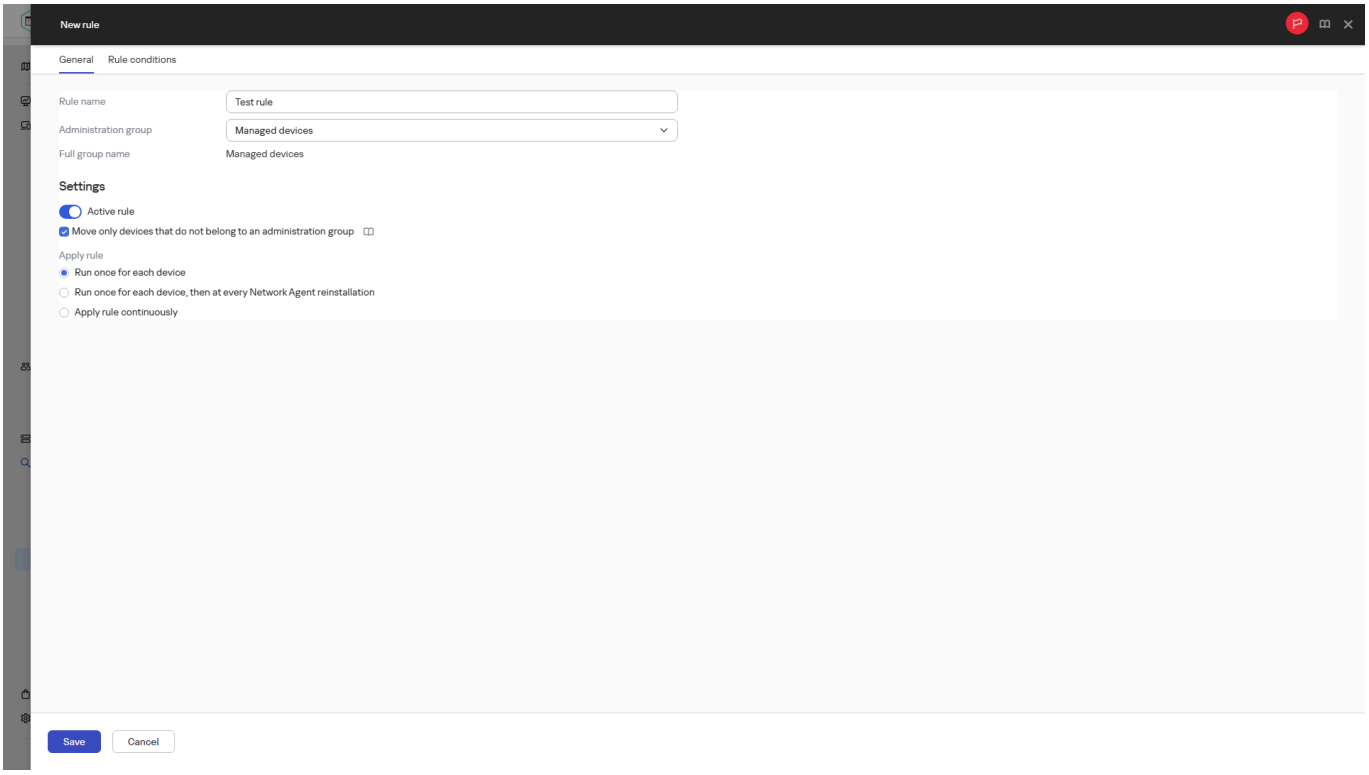
您可以設定裝置移動規則，即自動分配裝置到管理群組的規則。

要建立移動規則：

1. 在主功能表中，轉至 **資產管理** → **移動規則**。



2. 點擊**新增**。**新規則** 視窗隨即開啟。



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。

- **啟動的規則**

  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。

- **優先順序**

  您可以指定移動規則的優先順序。最高優先等級為1。**優先順序**值越大，規則的優先順序及其在清單中的位置就越低。

  如果未指派優先等級，則規則將被指派最低優先等級。

  複製規則時，規則副本將被指派原始規則的優先等級。然後，原始規則的優先等級將提升1。

- **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。

- **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）。

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。

若要變更優先順序：

1. 選取移動規則的核取方塊。

2. 執行以下操作之一：

   - 點擊**變更優先順序**按鈕，然後指定新的優先順序。

   - 按一下**向上移動**或**向下移動**按鈕，即可分別在清單中向上或向下移動規則。

3. 點擊**儲存**按鈕。

> 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

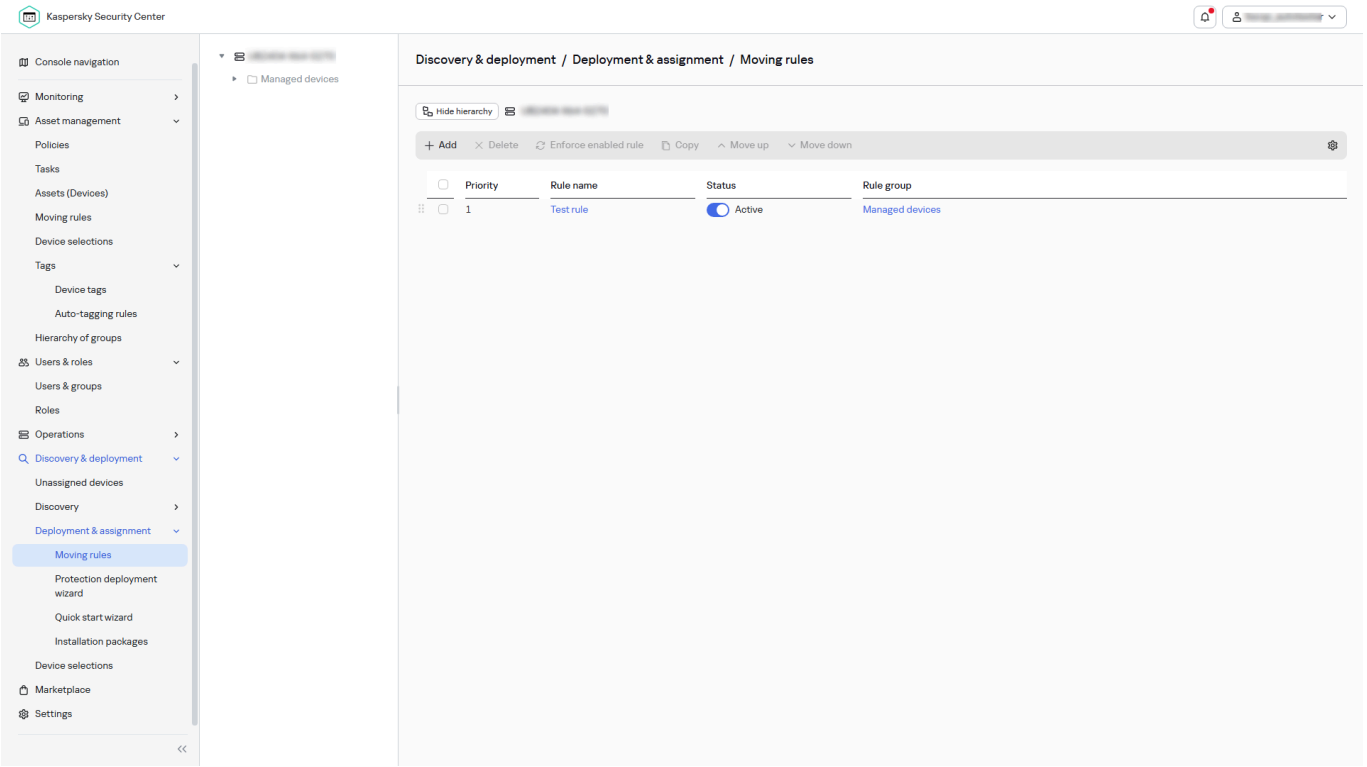
您可以複製移動規則，例如，如果您要對不同目標管理群組擁有幾個相同規則。

要複製現有移動規則：

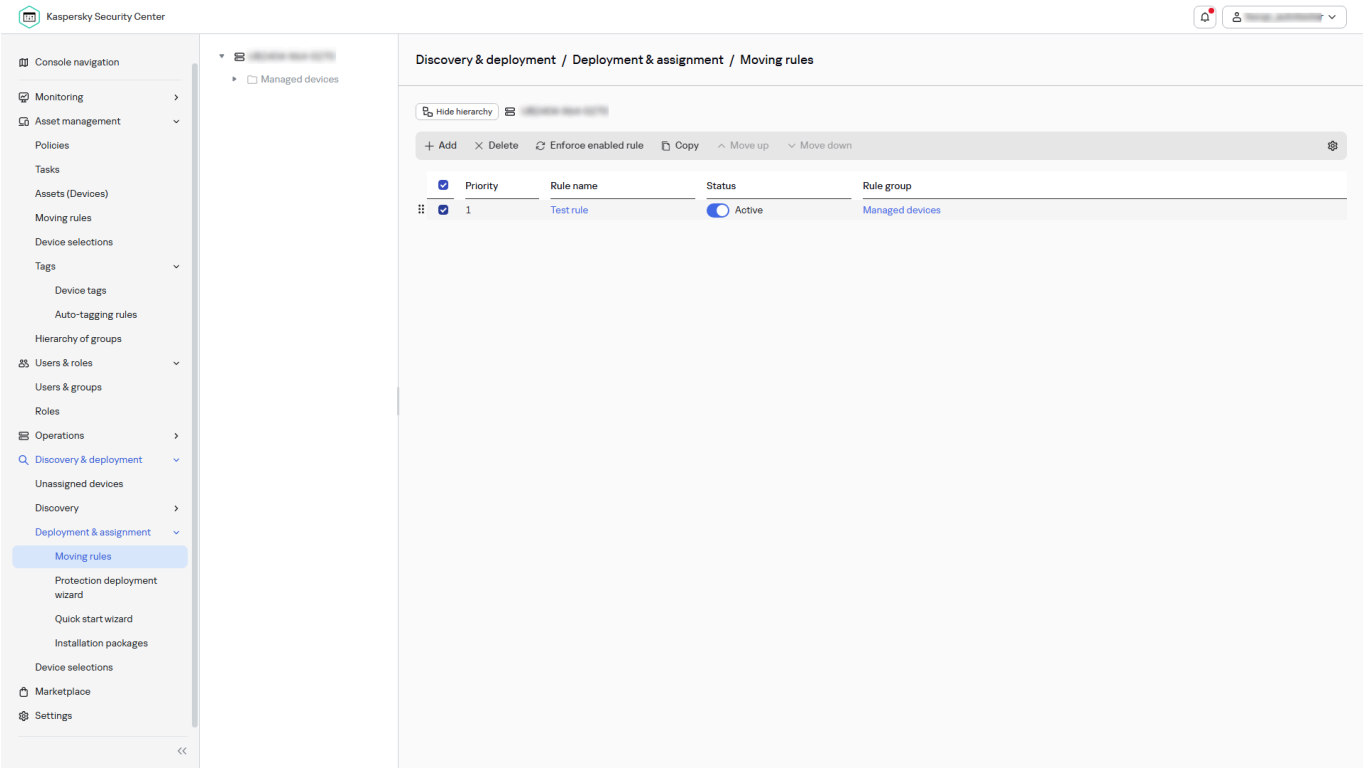
1. 執行以下操作之一：

   - 在主功能表中，轉至 **資產管理 → 移動規則**。
   - 在主功能表中，轉至 **發現和佈署 → 佈署和指派 → 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。

- **啟動的規則**

  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。

- **優先順序**

  您可以指定移動規則的優先順序。最高優先等級為1。**優先順序**值越大，規則的優先順序及其在清單中的位置就越低。

  如果未指派優先等級，則規則將被指派最低優先等級。

  複製規則時，規則副本將被指派原始規則的優先等級。然後，原始規則的優先等級將提升1。

- **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。

- **套用規則**

  您可以選取以下選項之一：

  - **對每台裝置執行一次**

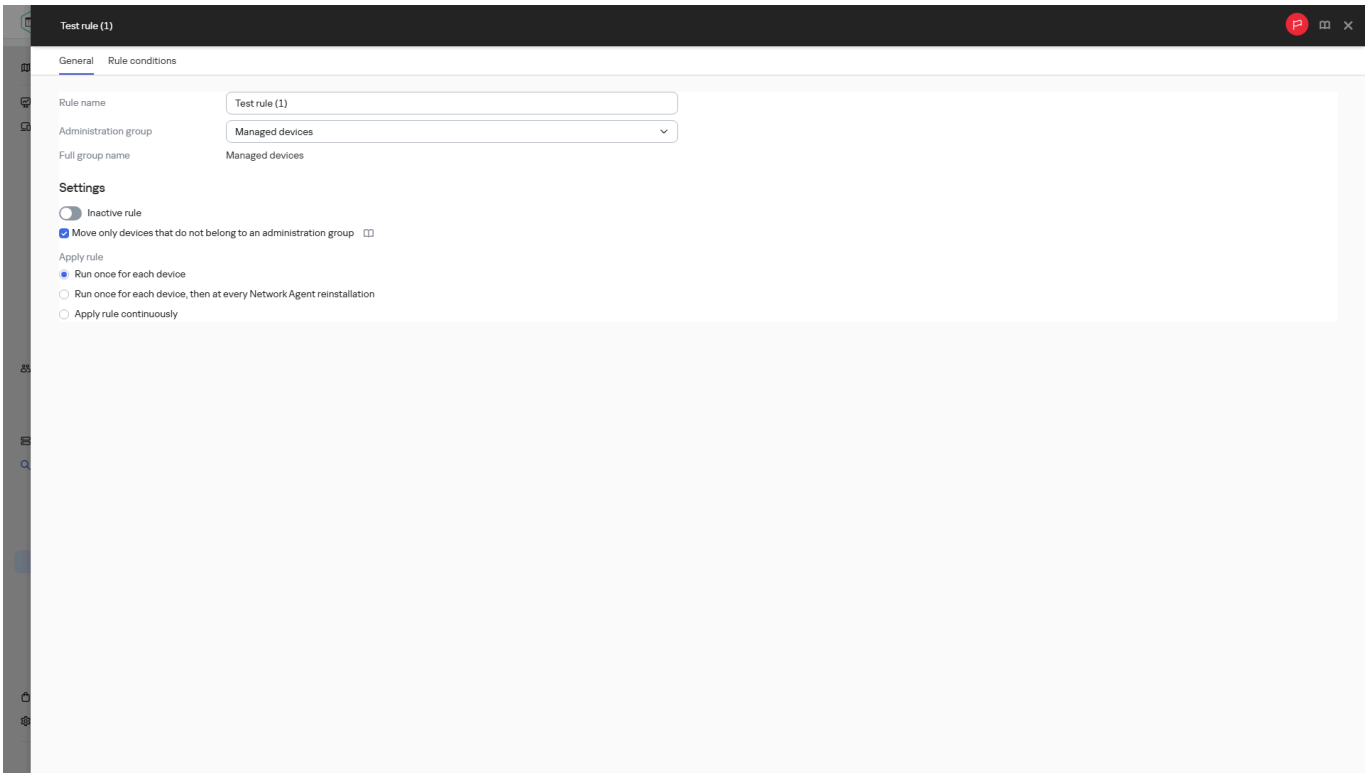
    規則對比對標準的每台裝置套用一次。

  - **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）。



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。

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。

- **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 Linux 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。

裝置所有者頁籤

在此頁籤上，您可以根據裝置所有者、安全群組成員資格和角色設定裝置移動規則：

- **裝置所有者**

  從內部安全群組中選擇裝置所有者的使用者名稱。在本節中了解有關使用者和使用者角色的更多資訊。

  > 最多只能有一名使用者註冊為裝置所有者。

- **裝置所有者列入 Active Directory 安全群組**

  選擇裝置所有者所屬的外部 Active Directory 安全群組。

  > 使用者可以是 Active Directory 安全群組的一部分，也可以是此 Active Directory 安全群組中包含的群組的一部分。

- **裝置所有者角色**

  選擇裝置所有者的指派角色。在本文中了解有關使用者角色的更多資訊。

- **裝置所有者在內部安全群組中之成員資格**

  選擇裝置所有者所屬的內部安全群組。

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 16.3 網路代理**或**卡巴斯基安全管理中心 16.3 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。

- **作業系統架構**

  您可以透過作業系統位元大小來剔除用戶端裝置。在**作業系統架構**欄位，您可以選擇以下一個值：

  - **未知**
  - **x86**
  - **AMD64**
  - **IA64**

  若要檢查用戶端裝置的作業系統架構：

  1. 在主功能表中，轉至 **資產管理 → 資產（裝置）**。
  2. 點擊右側的**列設定**按鈕（⚙）。
  3. 選擇**作業系統架構**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架構。

- **作業系統套件管理程序**

  您可以透過作業系統套件管理器來剔除用戶端裝置。在**作業系統套件管理程序**欄位，您可以選擇以下一個值：

  - rpm - 適用於運行Red Hat Enterprise Linux、CentOS、Fedora、SUSE、Oracle Linux作業系統的裝置
  - apt (dpkg) - 適用於運行Debian、 Ubuntu、Kali作業系統的裝置
  - pkg - 適用於運行FreeBSD、OpenBSD作業系統的裝置

  若要檢查用戶端裝置的作業系統套件管理器：

  1. 在主功能表中，轉至 **資產管理 → 資產（裝置）**。
  2. 點擊右側的**列設定**按鈕（⚙）。
  3. 選擇**作業系統套件管理程序**選項，然後按一下**儲存**按鈕。

     每個受管理裝置都會顯示作業系統套件管理器。

- **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（格式為*X.Y*），這將決定將移動規則套用至裝置的方式。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。

- **作業系統組建版本**

  > 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設施 (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。

網域控制器頁簽

在此頁籤上，您可以指定必須移動網域組織單元中包含的裝置。您還可以從指定網域組織單元的所有下級組織單元移動裝置：

- **裝置包括在以下組織單元中**

  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網域控制器組織單元中的裝置。
  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網域控制器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**

- **刪除網域中不存在的子群組**

- **裝置包括在以下網域安全群組中**

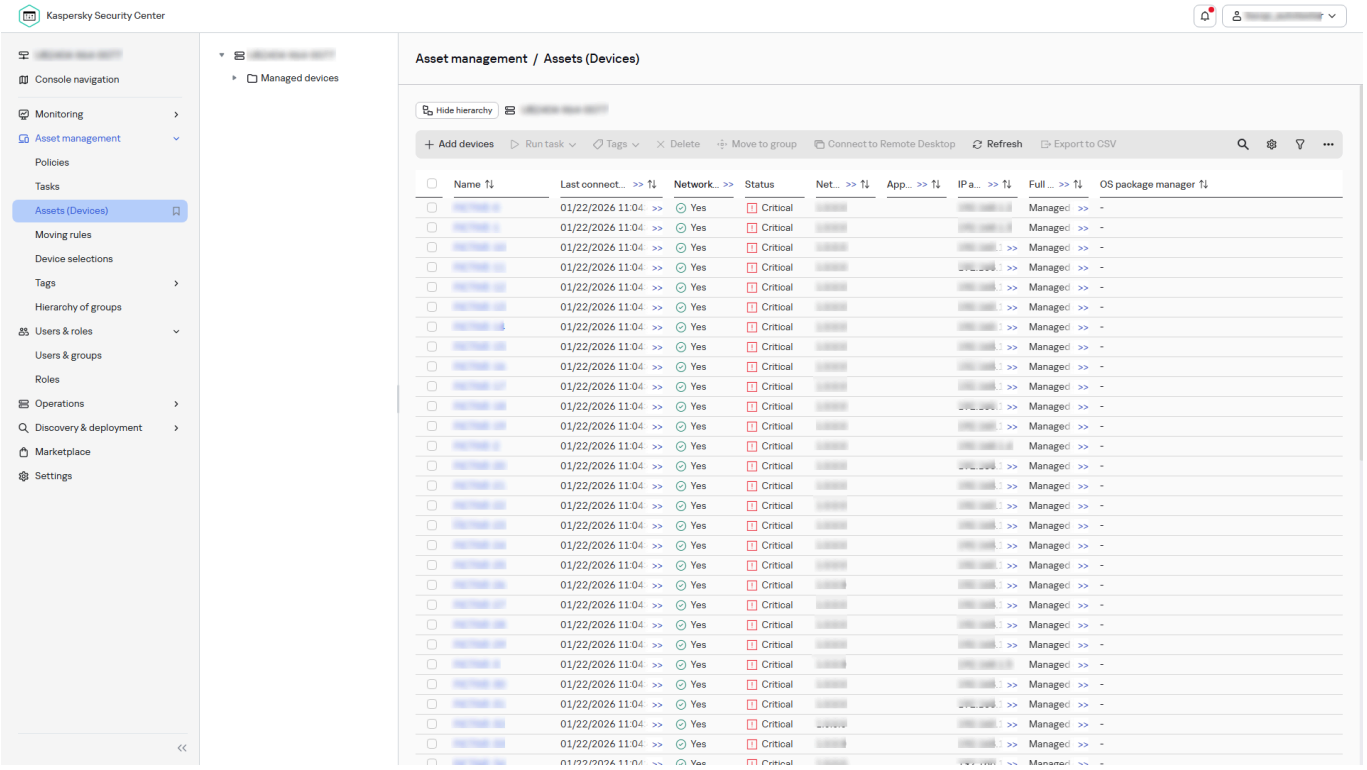
  如果啟用此選項，裝置移動規則將套用於該選項下清單中指定安全群組中的裝置。
  預設情況下已停用該選項。

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 **資產管理 → 資產（裝置）**。



受管理裝置清單

2. 選擇您要向其新增裝置的管理群組：

   - 對於根群組：

     在這種情況下，您可以繼續執行下一步。

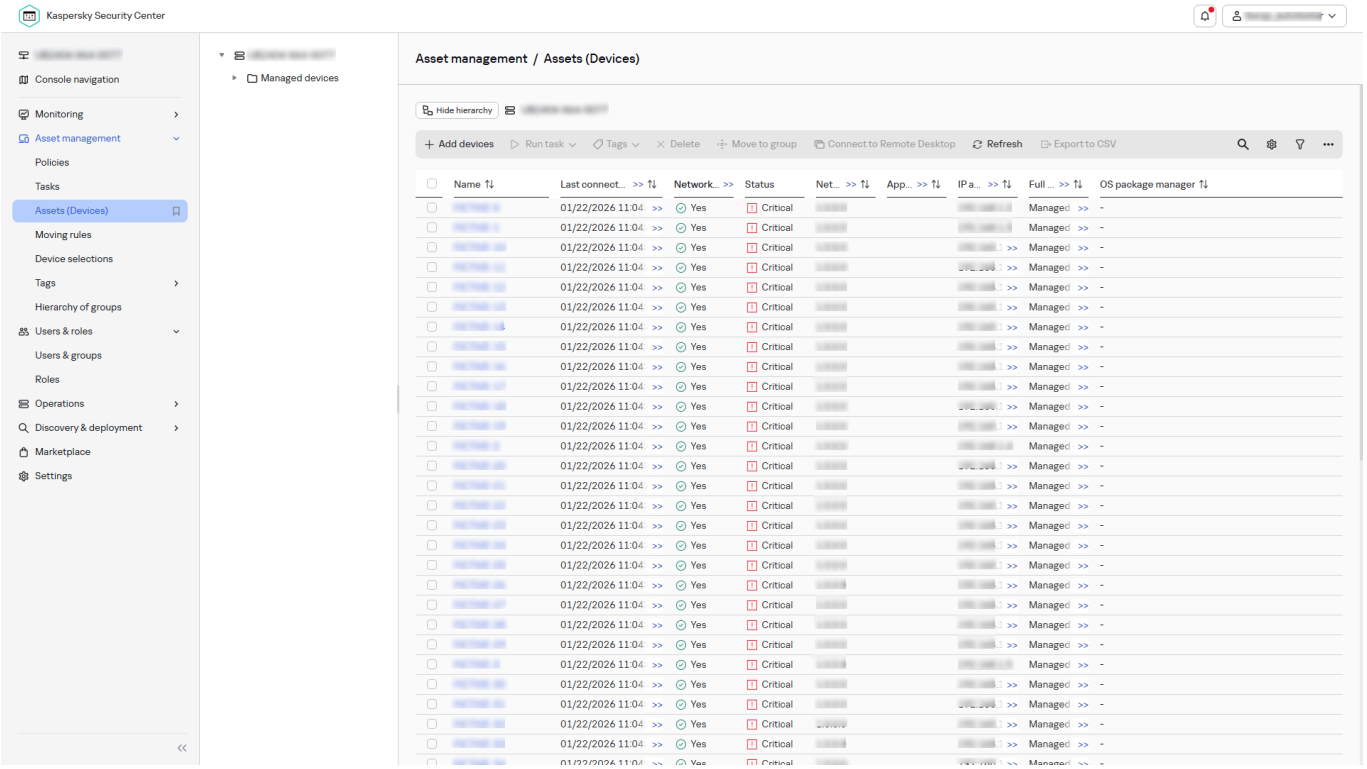
   - 對於子群組：

     a. 點擊頁面頂部的**顯示階層**按鈕。

     按鈕名稱將變更為**隱藏階層**。

     b. 在開啟的視窗中，按一下子群組的名稱。

所選群組的路徑將顯示在頁面頂部。如果需要，您可以點擊帶有管理群組名稱的連結進入該群組。預設情況下，路徑中的最後一個連結不活動。您也可以點擊**隱藏階層**按鈕關閉層次結構視窗。



選取管理群組

3. 點擊**新增裝置**按鈕。

   行動裝置精靈啟動。

4. 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。

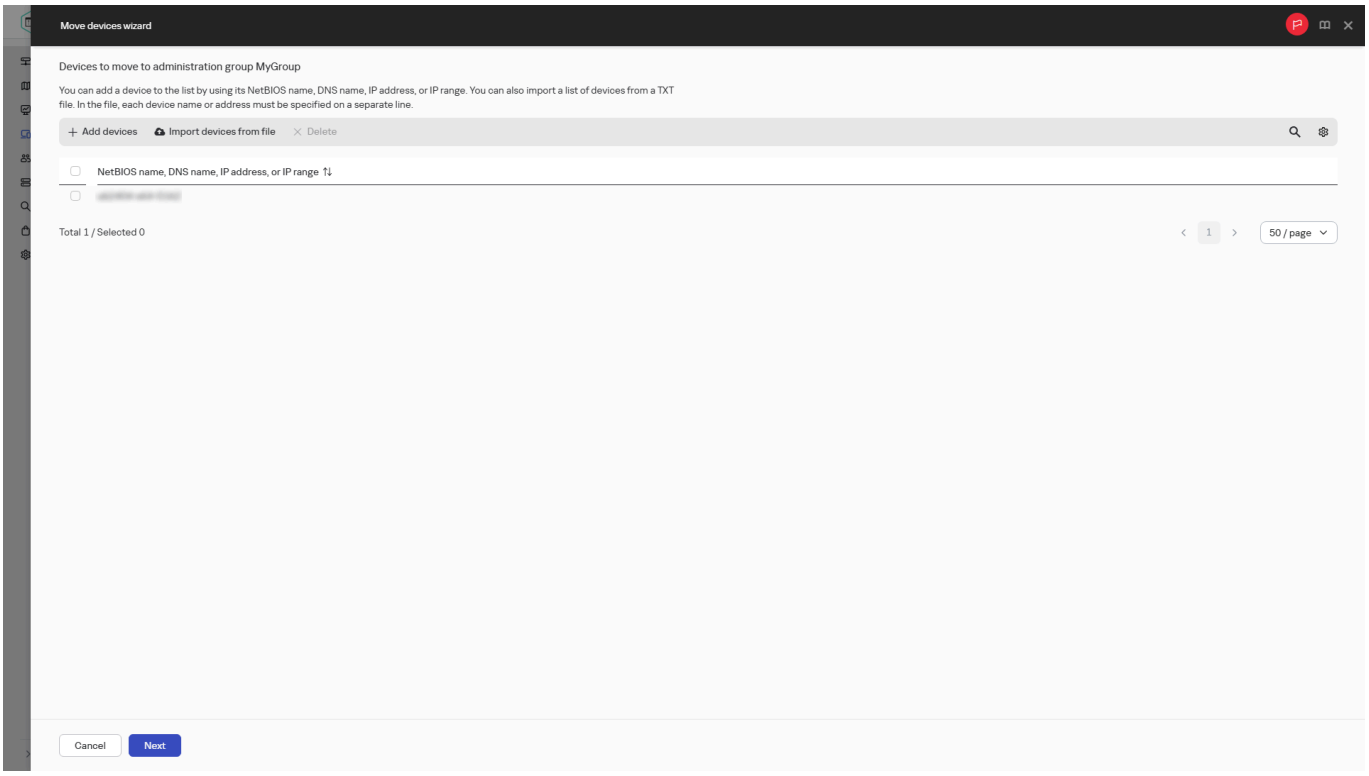
    > IP位址範圍不得超過1,048,576個位址。

  - 指定裝置 DNS 名稱。

    > 裝置名稱欄位不得包含空格、退格鍵，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、退格鍵，以及以下停用字元：:,\/*‘“;:&`~!@#$^()=+[]{}|<>%



選取要移動到管理群組的裝置

5. 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。

6. 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。

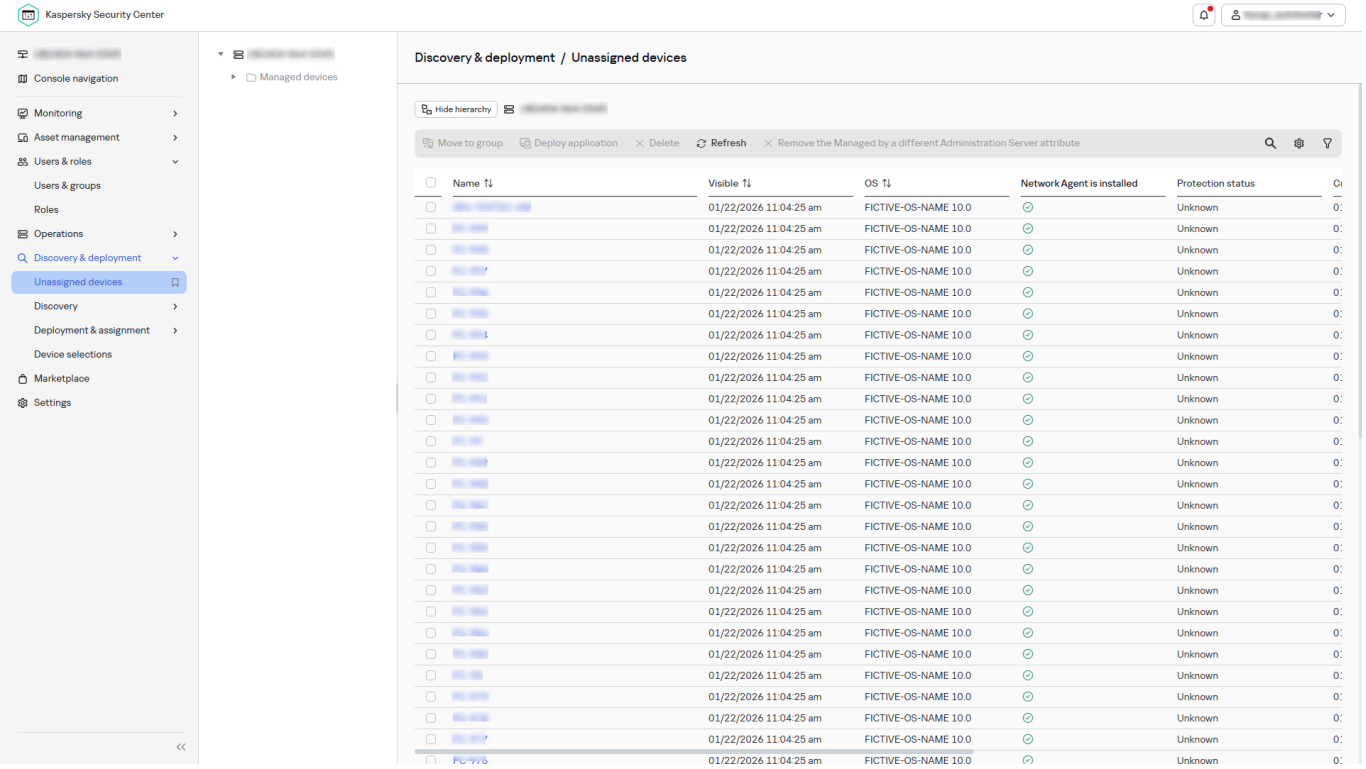
將裝置或者叢集手動移動至管理群組

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。

您還可以將叢集或伺服器陣列從一個管理群組移動到另一個管理群組。當您將叢集或伺服器陣列移動到另一個群組時，其所有節點都會隨之移動，因為叢集及其任何節點始終屬於同一管理群組。當您在**裝置**頁簽上選擇單個叢集節點時，**移至群組**按鈕將變得不可用。

要把一台或多台裝置或者叢集移動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：
   - 若要開啟管理群組，請在主功能表中前往**資產管理→資產（裝置）**，然後選擇所需的管理群組。
     - 對於根群組，您可以繼續下一步。
     - 對於子群組，請按一下頁面頂部的**顯示階層**按鈕，然後在開啟的視窗中選擇所需的管理群組。
   - 若要開啟**未指派的裝置**群組，請在主功能表中，轉至**資產管理→未指派的裝置**。



未指派的裝置清單

2. 如果管理群組包含叢集或伺服器陣列，則**資產（裝置）**部分將分為兩個頁簽：**裝置**頁簽以及**叢集和伺服器陣列**頁簽。開啟要移動的物件的頁簽。
3. 選取您要移至不同群組之裝置或者叢集旁的核取方塊。
4. 點擊**移至群組**按鈕。
5. 在管理群組階層中，選取您要將選取的裝置或者叢集移至管理群組旁的核取方塊。
6. 點擊**移動**按鈕。

   選取的裝置或者叢集會移至選取的管理群組。

關於叢集和伺服器陣列

卡巴斯基安全管理中心 Linux 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。

如果管理群組包含叢集或伺服器陣列，則**資產（裝置）**頁面將顯示兩個頁簽：一個用於單個裝置，另一個用於叢集和伺服器陣列。受管理裝置被偵測為叢集節點後，叢集將作為單獨物件被新增到**叢集和伺服器陣列**頁簽中。

叢集或伺服器陣列節點與其他受管理裝置一起列在**裝置**頁簽上。您可以將節點作為單個裝置檢視屬性並執行其他操作，但不能刪除叢集節點或將其從叢集中單獨移動到另一個管理群組。您只能刪除或移動整個叢集。

您可以對叢集或伺服器陣列執行以下操作：

- 檢視屬性
- 將叢集或伺服器陣列移至另一個管理群組

  當您將叢集或伺服器陣列移動到另一個群組時，其所有節點都會隨之移動，因為叢集及其任何節點始終屬於同一管理群組。

- 刪除

  僅當組織網路中不再存在叢集或伺服器陣列時，刪除該叢集或伺服器陣列才合理。如果叢集在您的網路上仍然可見，並且網路代理和卡巴斯基安全應用程式仍然安裝在叢集節點上，卡巴斯基安全管理中心 Linux 會自動將已刪除的叢集及其節點返回到受管理裝置清單。

叢集或伺服器陣列的屬性

檢視叢集或伺服器陣列的設定：

1. 在主功能表中，轉至**資產管理 → 資產（裝置） → 叢集和伺服器陣列**。

   叢集和伺服器陣列的清單將得以顯示。

2. 點擊所需叢集或伺服器陣列的名稱。

所選叢集或伺服器陣列的屬性視窗將得以顯示。

一般

一般區域顯示有關叢集或伺服器陣列的一般資訊。資訊基於上一次叢集節點與管理伺服器之間的同步接收的資料來提供：

- **名稱**
- **描述**
- **Windows 網域**

  Windows 網域或工作群組，包含叢集或伺服器陣列。

- **NetBIOS 名稱**

  叢集或伺服器陣列的 Windows 網路名稱。

- **DNS 名稱**

  叢集或伺服器陣列的 DNS 網域名稱。

工作

在**工作**標籤中，您可以管理被分配給叢集或者伺服器陣列的工作：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。列出的工作與安裝在叢集節點上的卡巴斯基安全應用程式相關。卡巴斯基安全管理中心 Linux 從叢集節點接收工作清單和工作狀態詳細資訊。如果未建立連線，則不顯示狀態。

節點

此頁簽顯示叢集或伺服器陣列中包含的節點清單。您可以點擊節點名稱來檢視裝置屬性視窗。

Kaspersky 應用程式

屬性視窗還可包含其他頁簽，其中包含與叢集節點上安裝的卡巴斯基安全應用程式相關的資訊和設定。

發佈點和連線閘道器的調整

卡巴斯基安全管理中心 Linux 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*。
- 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。

關於發佈點

已安裝網路代理裝置可以作為發佈點使用。在此模式下，網路代理可以發佈更新，這些更新可以從管理伺服器或卡巴斯基伺服器擷取。在後一種情況下，為發佈點配置更新下載。

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。

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。

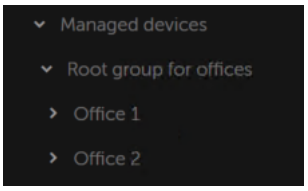
有以下構建管理群組結構的方法：

- 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。

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。

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 Linux 將自行選取哪個裝置要被分配為發佈點。

運行Microsoft Windows on Arm的裝置不能充當發佈點。

要自動分配發佈點：

1. 在主選單中，按一下管理伺服器名稱。

   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**自動指派發佈點**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 Linux 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 Linux 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指派發佈點（例如，如果您要使用單獨指派的伺服器），您可以在計算發佈點的數量和組態後手動指派。

> 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。

> 運行Microsoft Windows on Arm的裝置不能充當發佈點。

要手動指派裝置作為發佈點：

1. 在主選單中，按一下管理伺服器名稱。
   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**手動指派發佈點**選項。
4. 點擊**指派**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進行互動的設定。
     - **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。

- **已啟用**

  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 Linux 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。

- **已啟用**

  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。

- **已啟用**

  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。

- **已啟用**

  在 卡巴斯基安全管理中心 Linux 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，指定發佈點將向其分發更新的管理群組。
- 在**更新來源**區域，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**

    如果選取此核取方塊，將使用網際網路代理伺服器將發佈點連線至卡巴斯基更新伺服器。您可以在輸入欄位中設定代理伺服器連線。

    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。

    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/KPSN**

    發佈點從受管理裝置轉發 KSN 請求到 KSN 雲端或 KPSN。在發佈點上自行產生的 KSN 要求頁會直接傳送至 KSN 雲端或 KPSN。

  - **當連線到 KPSN 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 KPSN，請啟用此選項。否則，從受管理應用程式的請求無法到達 KPSN。

    如果您選擇**透過網際網路直接存取 KSN 雲端/KPSN**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。

  - **使用 HTTPS**

    如果需要受管理裝置透過 HTTPS 連接埠連線到 KSN 代理伺服器，啟用**使用 HTTPS** 選項，並指定 **HTTPS 連接埠**號。連線到 KSN 代理伺服器的預設 HTTPS 連接埠是 17111。

  - **HTTPS 連接埠**

    受管理裝置將用於連線到 KSN 代理伺服器的 HTTPS 埠號。連線到 KSN 代理伺服器的預設 HTTPS 連接埠是 17111。

- 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發佈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，憑證僅在發佈點上建立 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，發佈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Windows的發佈點設定Windows網路輪詢。

  - **Windows 網域**

    您可以啟用 Windows 網域裝置發現並為發現設定排程。

- 配置發佈點的網域控制器輪詢。

  - **網域控制器輪詢**

    您可以對網域控制器啟用裝置發現

    在**輪詢**欄位中，將切換按鈕切換到**已啟用**位置後，您可以選擇要輪詢的網域控制器，也可以為它們指定輪詢排程。

    如果您使用 Linux 發佈點，請在**輪詢指定網域**部分中點擊**新增** ，然後指定網域控制器的位址和使用者憑據。另外，您可以指定要輪詢的網域的類型：Active Directory 或 Samba、FreeIPA、ALD Pro。

如果您使用 Windows 發佈點，則可以選擇以下選項之一：

- **輪詢目前網域**
- **輪詢整個網域樹系**
- **輪詢指定網域**

- 配置發佈點對 IP 範圍的輪詢。
  - **IP 範圍輪詢**

    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。

在 DMZ 中新增連線閘道作為發佈點

如果管理伺服器不在非軍事區 (DMZ)，則安裝在外部裝置上的網路代理程式無法連線到管理伺服器。在這種情況下，您可以將發佈點用作非軍事區的連線閘道。發佈點將打開一個連接埠，供管理伺服器建立連線。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。

如果您需要在管理伺服器和網路代理程式和管理伺服器之間的同步期之外的管理伺服器和託管裝置之間建立連線，您必須在發佈點端啟用推送伺服器和開啟連接埠13295。

我們建議您將指派的特定裝置用作連線閘道。有關用戶端裝置（包括行動裝置）最大數量的資訊，請參閱容量大小指南。

> 連線閘道會等待來自管理伺服器的連線，而不是與管理伺服器建立連線。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. 在主選單中，按一下管理伺服器名稱。

   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**手動指派發佈點**選項。

4. 在工具列上，點擊**指派**按鈕。

5. 在開啟的右側窗格中，執行以下操作：

   a. 選擇**依位址使用 DMZ 連線閘道**選項。

   b. 在**連線閘道位址**欄位中，指定裝置IP位址或DNS名稱。

   c. 點擊**“指派”**按鈕。

   d. 窗格關閉，顯示名為**暫時的連線閘道**的發佈點。

6. 點擊**儲存**按鈕。

   管理伺服器嘗試連線到您指定位址的連線閘道。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。

如果點擊**暫時的連線閘道**名稱開啟發佈點屬性，則所有選項都會灰顯。您只能檢視顯示發佈點名稱的“一般”頁簽。預設情況下使用連接埠13000。只有在管理伺服器連線到發佈點後，您才能設定發佈點。當連線閘道的臨時條目被轉換為命名條目時，連線閘道也會出現在「未指派裝置」群組中。

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。

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 **資產管理 → 資產（裝置）**。

2. 透過點擊頁面頂部的**顯示階層**按鈕選擇要檢視其指派的發佈點的管理群組，然後在開啟的視窗中按一下所需群組的名稱。

   這將啟用**發佈點**功能表項。

   所選群組的路徑將顯示在頁面頂部。如果需要，您可以在此路徑中按一下帶有管理群組名稱的連結前往該群組。預設情況下，路徑中的最後一個連結不活動。

3. 在主功能表中，轉至 **資產管理 → 發佈點**。

4. 要為管理群組新增新的發佈點，請點擊**指派**按鈕。

5. 要刪除分配的發佈點，請從清單中選擇裝置並點擊**取消指派**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。

啟用推送伺服器

在卡巴斯基安全管理中心 Linux 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. 在主選單中，按一下管理伺服器名稱。

   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**已啟用**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。

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. 在用作發佈點的 Linux 裝置上，執行以下命令：

```
systemctl edit klnagent64.service
```

2. 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。

3. 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。

4. 執行以下命令重新載入系統處理程序：

   ```
   systemctl daemon-reload
   ```

5. 執行以下命令重新啟動網路代理服務：

   ```
   systemctl restart klnagent
   ```

6. 執行以下命令以確保指定的參數得到正確套用：

   `less /proc/<` `nagent 處理程序 ID` `>/limits`

   其中 `<` `nagent 處理程序 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。

關於裝置狀態

卡巴斯基安全管理中心 Linux 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。在某些情況下，當為裝置指派狀態時，卡巴斯基安全管理中心 Linux 會考量裝置在網路中的能見度標記（請參閱下表）。例如，若受管理裝置因符合「*資料庫已過期*」條件而被指派為*緊急*狀態，之後又為該裝置設定了能見度標記，則裝置會被指派為*正常*狀態。若卡巴斯基安全管理中心 Linux 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。

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。
即時保護等級不符合管理員設定的等級	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。
自重新啟動以來需要的時間	裝置在網路上可見，但應用程式要求重新啟動的時間已超過指定時間間隔。	多於 0 分鐘。
重新啟動的原因	裝置在網路上可見，但應用程式因所選原因之一需要重新啟動裝置。	• 未知原因 • 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
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。	多於 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*尋找弱點和所需更新*工作未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。
偵測到未處理的安全問題	裝置上發現了一些未處理的安全問題。安全問題可以透過安裝在使用者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。 無論卡巴斯基安全管理中心 Linux 的設定為何，受管理裝置的狀態都可由受管理應用程式定義。當此狀態恢復為由卡巴斯基安全管理中心 Linux 定義的其中一種狀態後，管理伺服器會為受管理裝置指派受管理應用程式傳回且由管理伺服器指派的狀態中最緊急的狀態。由受管理應用程式定義的狀態，其描述同樣由受管理應用程式提供。您可以在受管理裝置清單的「**狀態描述**」欄位中檢視這些描述。	• 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。
裝置已不受管理	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 Linux 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。當滿足指定條件時，用戶端裝置會被分配以下狀態之一：*緊急*或*警告*。當不滿足指定條件時，用戶端裝置會被分配*正常*狀態。

一個條件的不同值可對應於不同的狀態。例如，預設情況下，若**資料庫已過期**條件的值為**多於 3 天**，則用戶端裝置會被指派*警告*狀態；若值為**多於 7 天**，則會被指派*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 Linux，用於指派為*緊急*或*警告*狀態的**資料庫已過期**條件的值不會改變。

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 **資產管理 → 群組的階層**。

2. 透過以下方式之一，前往要變更切換裝置狀態的管理群組內容：

   - 點擊管理群組的名稱。

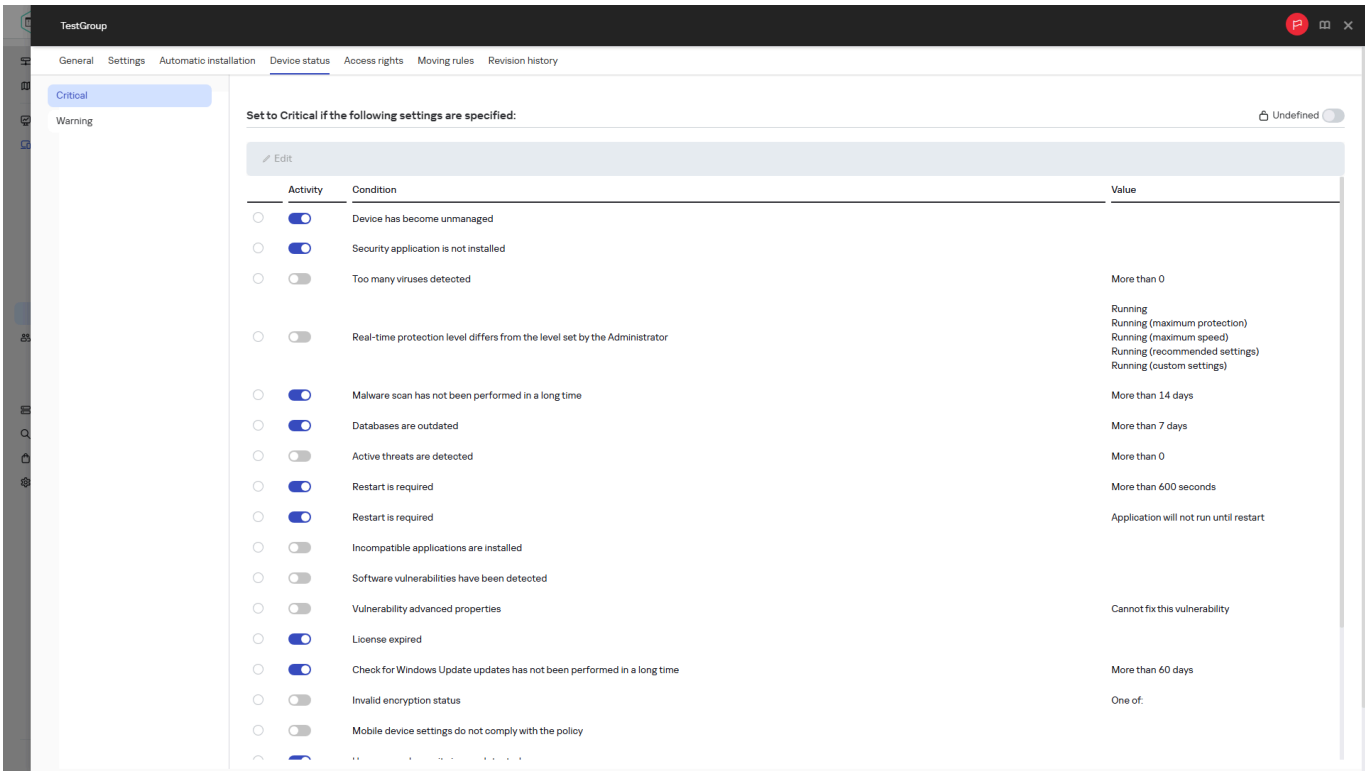
   - 點擊頁面頂部的**顯示階層**按鈕。在開啟的導覽窗格中，將滑鼠游標懸浮在所需群組的名稱之上，然後按一下設定圖示（ ⚙ ）。

   管理群組內容視窗將開啟。

3. 在屬性視窗中，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**如果指定了以下設定，則設定為「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 **資產管理 → 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**如果指定了以下設定則設定為「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。

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 Linux 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 Linux 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**資產管理 → 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 **資產管理** → **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**未指派的裝置**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。
   - **尋找未指派的裝置**– 搜尋符合選擇標準並被包含在**未指派的裝置**群組中的裝置。

   您可以啟用**包含來自從屬管理伺服器的資料**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 **資產管理** → **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。

- **網域**

  顯示指定的工作組中包括的所有裝置。

- **管理群組**

  顯示指定的管理群組中包括的裝置。

- **描述**

  裝置內容視窗中的文字：在**一般**區域的**描述**欄位。

  您可以使用以下特徵說明**描述**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：

    若要描述短語，例如 **SUSE Linux 企業伺服器 12** 或者 **SUSE Linux 企業伺服器 15**, 你可以輸入 **SUSE Linux 企業伺服器 1 ?** 。

    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**網域控制器**子區域，您可以根據網域成員身分設定將裝置納入分類的標準：

- **裝置在網域組織單元中**

  如果啟用此選項，選取範圍將包括輸入欄位中指定的網域組織單元中的裝置。

  預設情況下已停用該選項。

- **該裝置是網域安全群組成員**

  如果啟用此選項，選取範圍將包括輸入欄位中指定的網域安全群組中的裝置。

  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。

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（*未知, 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（*未知, 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（*未知*、*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（*未知*、*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（格式為*X.Y*），這將決定將移動規則套用至裝置的方式。預設情況下，不指定版本值。

- **作業系統架構**

  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。

- **作業系統組建版本**

  > 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**

  具有指定名稱的裝置將包括在該分類中。

- **描述**

  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。

- **庫存編號**

  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。

- **RAM 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。

第三方軟體詳情

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。

卡巴斯基應用程式詳情

在 **卡巴斯基應用程式**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。

- **選取上次更新模組的期間**

  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。

- **裝置透過管理伺服器進行管理**

  在該下拉清單，您可以包含透過 卡巴斯基安全管理中心 Linux 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 Linux 管理的裝置。
  - **否**。若裝置不透過 卡巴斯基安全管理中心 Linux 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。

- **帶此標籤的所有裝置**

  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。

- **不帶此標籤的所有裝置**

  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。

裝置所有者

在**裝置所有者**區域中，您可以根據裝置的註冊所有者、其角色及其在安全性群組中的成員資格，設定標準以將裝置包含在選擇中：

- **裝置所有者**

  從內部安全群組中選擇裝置所有者的使用者名稱。在本節中了解有關使用者和使用者角色的更多資訊。

  > 最多只能有一名使用者註冊為裝置所有者。

- **裝置所有者列入 Active Directory 安全群組**

  選擇裝置所有者所屬的外部 Active Directory 安全群組。

  > 使用者可以是 Active Directory 安全群組的一部分，也可以是此 Active Directory 安全群組中包含的群組的一部分。

- **裝置所有者角色**

  選擇裝置所有者的指派角色。在本文中了解有關使用者角色的更多資訊。

- **裝置所有者在內部安全群組中之成員資格**

  選擇裝置所有者所屬的內部安全群組。

從裝置分類中匯出裝置清單

卡巴斯基安全管理中心 Linux 允許您將裝置分類中的裝置資訊匯出為 CSV 或 TXT 檔案。

從裝置分類中匯出裝置清單：

1. 從裝置分類中開啟包含裝置的表格。
2. 使用以下方法之一選擇要匯出的裝置：
   - 要選擇特定裝置，請選取它們旁邊的核取方塊。
   - 要從當前表頁面選擇所有裝置，請選取裝置表標頭中的核取方塊，然後選取**全選當前頁面**核取方塊。
   - 要從表中選擇所有裝置，請選取裝置表標頭中的核取方塊，然後選擇**全選**核取方塊。
3. 點擊**匯出到 CSV**或**匯出到 TXT**按鈕。表中包含的有關所選裝置的所有資訊都將被匯出。

> 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。

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**資產管理 → 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

卡巴斯基安全管理中心 Linux 允許您*標記*裝置。標籤是用來分組、敘述或查找裝置的字串值。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 Linux 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，您可以設定規則以指派 `[CentOS]` 標籤到執行 CentOS 作業系統的所有裝置。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 CentOS 裝置並給它們指派工作。

> 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 **資產管理** → **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 **資產管理** → **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

您只能刪除手動指派的標籤。

要刪除手動指派的裝置標籤：

1. 在主功能表中，轉至 **資產管理** → **標籤** → **裝置標籤**。
   標籤清單隨即顯示。
2. 選取要刪除的裝置標籤。

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。

當您刪除以自動標記規則指派給裝置的標籤時，該規則不會被刪除，並且當裝置首次符合規則條件時，該標籤還將被指派給新裝置。如果您刪除自動標記規則，則規則條件中指定的標籤將從有指派該標籤的所有裝置中刪除，但不會從標籤清單中刪除。如有必要，您可以手動從清單中刪除該標籤。

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。若要管理這些標籤，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 **資產管理** → **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。

   您將被重定向到主功能表的**資產（裝置）**部分，其中裝置按您點擊**檢視裝置**連結的標籤進行篩選。

3. 如果您想要返回裝置標籤清單，點擊您瀏覽器的**後退**按鈕。

檢視分配了標籤的裝置後，您可以建立並指派新標籤，也可以將現有標籤指派給其他裝置。在這種情況下，您必須按標籤刪除過濾器，選擇裝置，然後指派標籤。

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 **資產管理** → **資產（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**指派的標籤**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**指派現有標籤**，之後在下拉清單選取必要標籤。
4. 點擊**正常**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 **資產管理 → 資產（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**取消指派標籤**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。若要管理這些標籤，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 **資產管理** → **標籤** → **自動標記規則**。
- 在主功能表中，前往**資產管理** → **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，例如裝置的 DNS 名稱，或裝置是否屬於 IP 子網路。

     > 如果為您用於卡巴斯基安全管理中心 Linux 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**—出現在裝置上的網路代理程式、作業系統類型、版本、架構以及套件管理工具。
- **虛擬機**—裝置屬於虛擬機的特定類型。
- **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指派一個或者多個標籤：

1. 在有根權限的帳戶下執行命令提示符，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目錄中。預設安裝目錄為/opt/kaspersky/klnagent64/sbin。

2. 輸入以下一個指令：

   - 要指派一組標籤：

     ```
     /opt/kaspersky/klnagent64/sbin/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：

     ```
     /opt/kaspersky/klnagent64/sbin/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：

     ```
     /opt/kaspersky/klnagent64/sbin/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：

     ```
     /opt/kaspersky/klnagent64/sbin/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。

資料加密與防護

如果您的膝上型電腦或硬碟磁碟機被盜或丟失，資料加密可降低敏感資料和公司資料意外洩露的風險。此外，資料加密還允許您防止未經授權的使用者和應用程式進行存取。

如果您的網路包括安裝了 Kaspersky Endpoint Security for Windows 的 Windows 受管理裝置，您可以使用資料加密功能。在這種情況下，在執行 Windows 作業系統的裝置上，您可以管理以下類型的加密：

- BitLocker 磁碟機加密
- 卡巴斯基磁碟機加密

我們不建議在 VDI 中啟用加密。

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。

若要設定加密，請在卡巴斯基安全管理中心 Linux 中定義 Kaspersky Endpoint Security for Windows 政策。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。

目前在網頁主控台中，無法為管理伺服器的層次結構進行加密管理。請使用主管理伺服器管理加密的裝置。

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。

檢視加密磁碟機的清單

在卡巴斯基安全管理中心 Linux 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**匯出到 CSV**或**匯出到 TXT**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 Linux ：

- 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**匯出到 CSV**或**匯出到 TXT**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 **資產管理 → 資產（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 → 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**事件組態**頁籤。
3. 在**緊急**區域，點擊**新增事件**並選取*Error applying file encryption / decryption rules*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 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所需平台的 Kaspersky Endpoint Security 說明中提供。

若要在Kaspersky Endpoint Security for Windows中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，選擇 Kaspersky Endpoint Security for Windows 外掛程式。

6. 按照 Kaspersky Endpoint Security for Windows 說明提供的說明操作（請參閱本節最後的卡巴斯基安全管理中心網頁主控台操作說明）。

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。

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：

- 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。

- 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。

- 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。

- 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 Linux 使用者：

  - 將加密金鑰管理功能的**讀取**存取權限授予從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. 前往所需管理伺服器的屬性：

   a. 在主選單中，選擇一個部分（**市場**、**主控台導覽**和**設定**除外），然後在頁面頂部點擊**顯示階層**按鈕。

   b. 在開啟的導覽窗格中，將滑鼠遊標停留在所需管理伺服器的名稱上，然後點擊設定圖示 (⚙)。

   或者，您可以按一下管理伺服器名稱，然後在主選單中顯示該名稱後，在主選單中按一下它以開啟伺服器屬性視窗。

2. 在開啟的屬性視窗中，選取**加密演算法**部分。

3. 啟用**使用管理伺服器層級獲取加密金鑰**選項。

4. 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. 前往要從中匯出加密金鑰的管理伺服器的屬性：

   a. 在主選單中，選擇一個部分（**市場**、**主控台導覽**和**設定**除外），然後在頁面頂部點擊**顯示階層**按鈕。

   b. 在開啟的導覽窗格中，將滑鼠遊標停留在所需管理伺服器的名稱上，然後點擊設定圖示 (⚙)。

   或者，您可以按一下管理伺服器名稱，然後在主選單中顯示該名稱後，在主選單中按一下它以開啟伺服器屬性視窗。

2. 在開啟的屬性視窗中，選取**加密演算法**部分。

3. 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。

4. 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。

5. 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。

6. 前往要為其匯入加密金鑰的管理伺服器的屬性。

7. 在內容視窗中，選取**加密演算法**區域。

8. 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。

9. 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。

10. 點擊“**確定**”。

加密金鑰會傳輸至目標管理伺服器。

變更用戶端裝置的管理伺服器

對於特定用戶端裝置，您可以將管理伺服器變更為不同的管理伺服器。為此，請使用*變更管理伺服器*工作。

要變更用戶端裝置連線的管理伺服器：

1. 連線至管理裝置的管理伺服器。

2. 建立管理伺服器變更工作。

   新工作精靈啟動。遵照精靈的說明。在新工作精靈的**新工作**視窗中，選擇**卡巴斯基安全管理中心 16.3**應用程式和**變更管理伺服器**工作類型。之後，指定要變更管理伺服器的裝置：

   - **指派工作給管理群組**

     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，則工作內容視窗中不會顯示**安全**頁籤，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是從清單匯入位址**

     您可以指定您要為其分配工作的裝置的 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。

   - **指派工作給裝置分類**

     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。

3. 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。

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。

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：

- 顯示受管理裝置
- 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**資產管理** → **未指派的裝置**。
2. 選擇所需的裝置，然後按一下**刪除「由不同管理伺服器管理」屬性**按鈕。

   由不同管理伺服器管理屬性被重設。

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 "<閘道IP或名稱>" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`

     在此，`<閘道 IP 或者名稱>`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。

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。

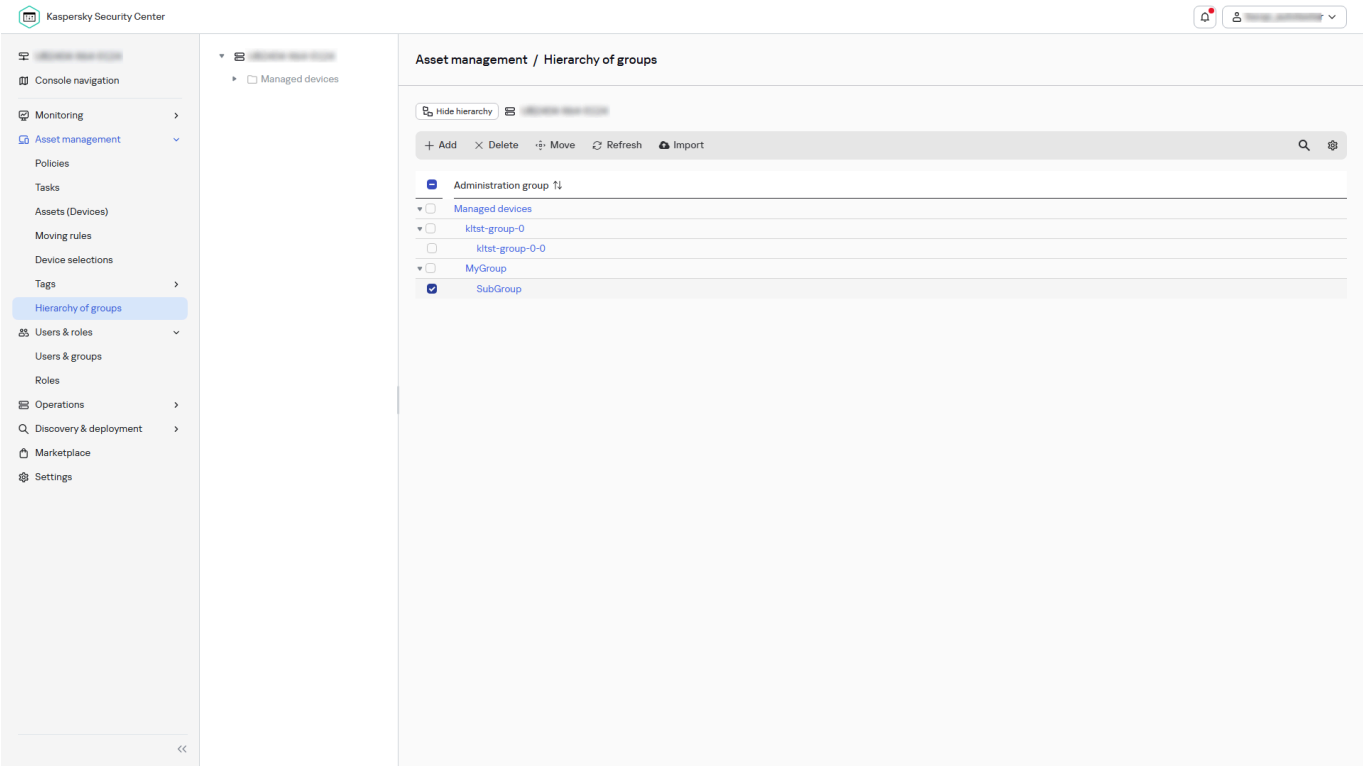
要在組中裝置顯示不活動時檢視或設定操作：

1. 在主功能表中，轉至 **資產管理 → 群組的階層**。

2. 透過下列方式之一轉到所需管理群組的屬性：

   - 點擊管理群組的名稱。

   - 點擊頁面頂部的**顯示階層**按鈕。在開啟的導覽窗格中，將滑鼠游標懸浮在所需群組的名稱之上，然後按一下設定圖示（ ⚙ ）。



管理群組的層級結構

   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。

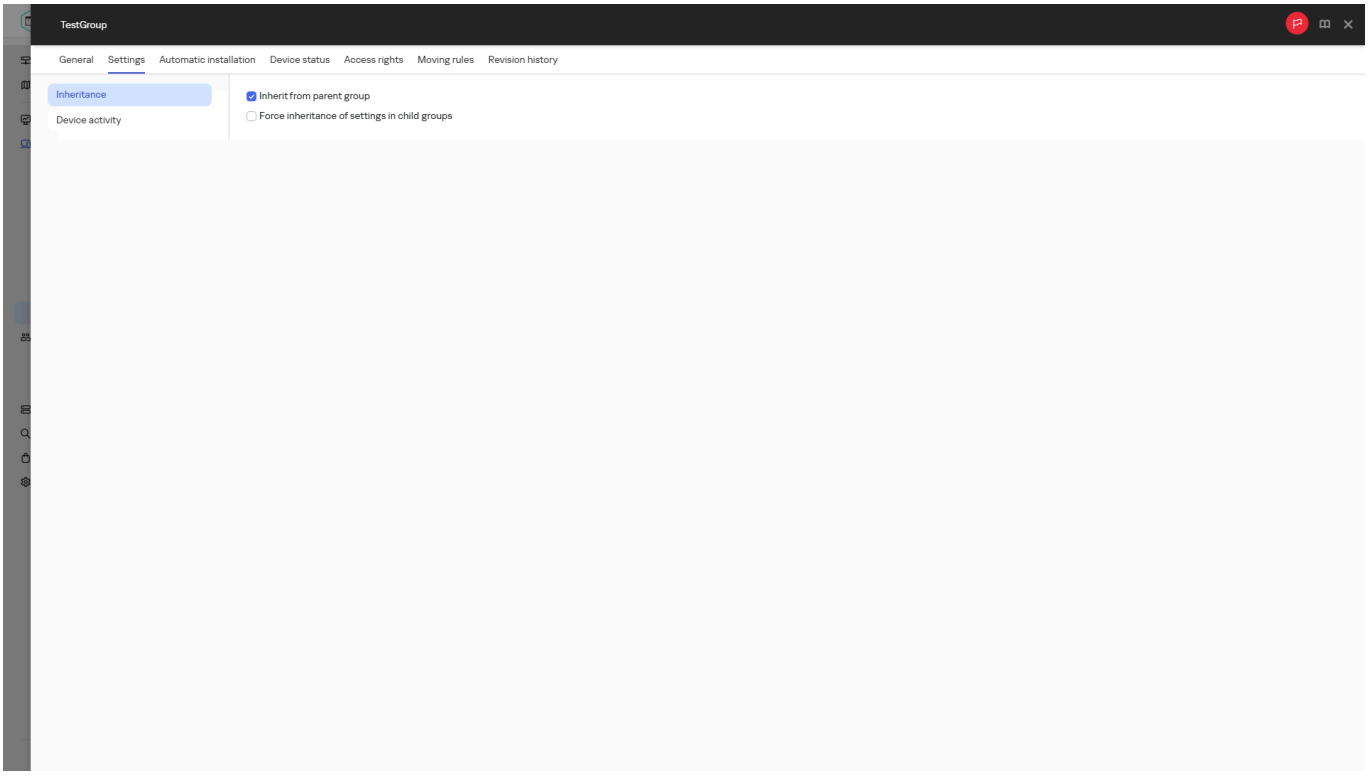
  該選項僅在管理群組擁有父群組時可用。

  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。



管理群組內容

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**

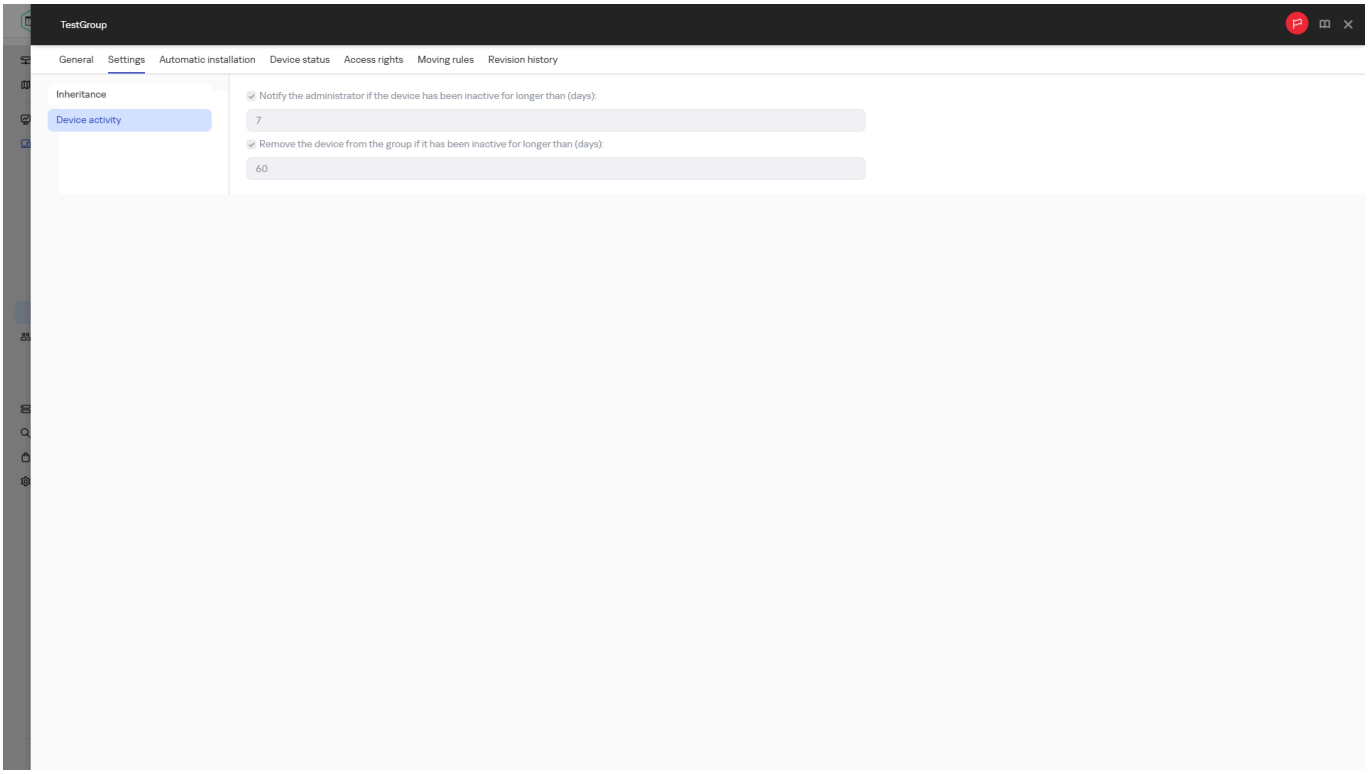
  如果啟用該選項，管理員接收不活動裝置的通知。您可以指定**裝置在網路上已長時間沒有活動**事件被建立的時間間隔。預設時間間隔為 7 天。

  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。



管理群組內容

6. 點擊**儲存**。

   您的變更已儲存並套用。

傳送訊息到裝置使用者

要傳送訊息到裝置使用者：

1. 在主功能表中，轉至 **工作**。
2. 點擊**新增**。
   新工作精靈啟動。
3. 在**工作類型**下拉清單中，選擇**將訊息傳送至使用者**。
4. 選取一個選項以指定管理群組、裝置分類或應用程式工作的裝置。
5. 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。**將訊息傳送至使用者**工作僅對 Windows 裝置可用。

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 Linux 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. 在主功能表中，轉至 **工作**。
2. 點擊**新增**。
   新工作精靈啟動。
3. 在**工作類型**下拉式清單中，選取**管理裝置**。
4. 選取一個選項以指定管理群組、裝置分類或應用程式工作的裝置。
5. 選擇命令（開啟、關閉或重新啟動）。
6. 如有必要，請為關閉和重新啟動命令配置以下設定：
   - 開啟**提示使用者確認**切換按鈕以指定使用者提示訊息以及您想要重複提示以及重新啟動或關閉裝置的時間間隔。
   - 選取**強制關閉封鎖工作階段中應用程式前的等待時間（分鐘）**核取方塊並指定時間。

   這些設定僅適用於 Windows 用戶端裝置。Linux 裝置將在工作完成後立即重新啟動或關閉。

7. 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）。

遠端存取受管理裝置

卡巴斯基安全管理中心 Linux 允許您建立與受管理裝置的遠端連線。管理員可以透過裝置上安裝的網路代理，遠端存取受管理裝置。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，以便管理員可以管理其上安裝的應用程式。

建立遠端連線的方法取決於安裝有卡巴斯基安全管理中心網頁主控台的裝置上使用的平台。卡巴斯基安全管理中心網頁主控台可以安裝在管理伺服器裝置以外的裝置上，也就是基於 Windows 或 Linux 的裝置上。

您可以從安裝在 Linux 裝置上的卡巴斯基安全管理中心網頁主控台建立以下連線：

- 使用以下方式連線到基於 Linux 的受管理裝置：
  - 遠端桌面連線 (RDP)
  - 虛擬網路運算 (VNC)
- 使用以下方式連線到基於 Windows 的受管理裝置：
  - 遠端桌面連線 (RDP)
  - 虛擬網路運算 (VNC)

您可以從安裝在 Windows 裝置上的卡巴斯基安全管理中心網頁主控台建立以下連線：

- 使用以下方式連線到基於 Linux 的受管理裝置：
  - 遠端桌面連線 (RDP)
  - 虛擬網路運算 (VNC)
- 使用以下方式連線到基於 Windows 的受管理裝置：
  - 遠端桌面連線 (RDP)
  - Windows 桌面共用 (WDS)

> 從執行Microsoft Windows on Arm的裝置存取卡巴斯基安全管理中心網頁主控台時，不支援遠端連線到受管理裝置。

若要與裝置建立遠端連線，您必須擁有以下工具：

- klsctunnel 公用程式

  卡巴斯基公用程式用於建立受管理裝置和管理伺服器之間的通道連線。

  卡巴斯基安全管理中心 Linux 允許以先途經管理伺服器、再途經網路代理的方式，建立從卡巴斯基安全管理中心網頁主控台到受管理裝置上所指定連接埠的 TCP 連線通道。通道設計用於將安裝卡巴斯基安全管理中心網頁主控台的裝置上的用戶端應用程式連線到受管理裝置上的 TCP 連接埠（如果卡巴斯基安全管理中心網頁主控台和目標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。

  當透過卡巴斯基安全中心網頁主控台或從卡巴斯基網站手動建立遠端連線時，可以下載該公用程式。

  klsctunnel公用程式安裝在管理伺服器裝置上，用於所有類型的遠端連線（RDP、VNC、WDS）。

- RDP 或 VNC 用戶端

  RDP 或 VNC 用戶端安裝在管理伺服器裝置上。此用戶端允許您使用 klsctunnel 公用程式提供的本機連線的位址和連接埠，取得對受管理裝置的遠端存取權。

  在使用者不知道的情況下，以 RDP 連線方式連線到使用者目前的遠端桌面。一旦管理員連線到工作階段，裝置使用者將在未通知的情況下中斷與工作階段的連線。

- Windows 桌面共用（僅適用於基於 Windows 的受管理裝置）

  此功能允許您連線到用戶端裝置上的現有工作階段，而不使該工作階段中的使用者中斷連線。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。

  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 Linux 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。在稽核期間，應用程式會儲存用戶端裝置上經管理員開啟並/或修改過之檔案的資訊。

使用卡巴斯基安全管理中心網頁主控台從基於 Linux 的裝置遠端存取基於 Linux 的受管理裝置

先決條件

在您開始之前，確保您已做了如下：

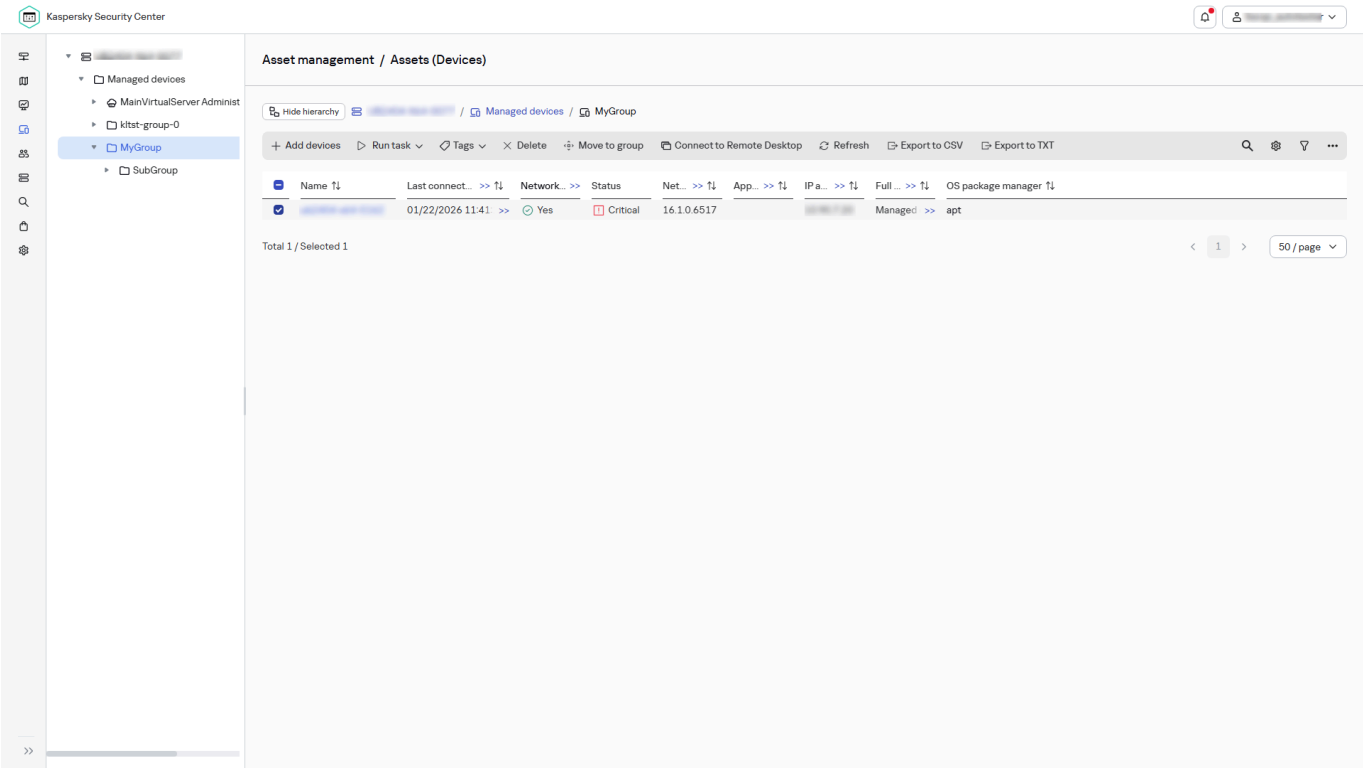
- 在執行 Linux 的受管理裝置上，安裝了網路代理版本 15.3 或更高版本。
- 在執行 Linux 的受管理裝置上，安裝了 RDP 伺服器（如果您使用遠端桌面連線功能連線到受管理裝置）。
- 在執行 Linux 的受管理裝置上，安裝了 VNC 伺服器（如果您使用虛擬網路運算功能連線到受管理裝置）。
- 用於建立 RDP 通道連線的連接埠已開啟（在管理伺服器內容視窗的**連線連接埠**區段中啟用了**開啟用於建立 RDP 連線通道的連接埠**選項）。
- 管理員具有**啟動 RDP 連線**權限，可以建立 RDP 連線（如果您使用遠端桌面連線功能連線到受管理裝置）。
- 管理員具有**建立通道** 權限，可以建立 VNC 通道連線（如果您使用虛擬網路運算功能連線到受管理裝置）。

若要透過在基於 Linux 的裝置上開啟的卡巴斯基安全管理中心網頁主控台使用 RDP 或 VNC 連線到基於 Linux 的受管理裝置：

1. 在主功能表中，前往**資產管理 → 資產（裝置）**區段或開啟裝置分類。
2. 選取要遠端連線的受管理裝置旁的核取方塊，然後點擊**連線到遠端桌面**按鈕。

   將開啟**連線到遠端桌面**視窗。

如果您選取多台裝置、一台行動裝置或一台執行 macOS 的裝置，則**連線到遠端桌面**按鈕將會停用。



受管理裝置清單

3. 點擊**下載**按鈕下載 klsctunnel 公用程式，然後執行。

   下載該公用程式時，請考慮以下事項：

   - 若要取得 klsctunnel 公用程式的最新版本，請確保管理伺服器可以存取卡巴斯基更新伺服器。

     您可以執行*下載更新至管理伺服器儲存區*工作，並選取卡巴斯基更新伺服器作為更新來源。如果工作成功完成，管理伺服器就可以存取卡巴斯基更新伺服器。

   - 如果公用程式檔案無法下載，則會顯示錯誤訊息。在這種情況下，手動下載公用程式，然後將其放在管理伺服器裝置的/var/opt/kaspersky/klnagent目錄中。

4. 在**連線到遠端桌面**視窗中，指定連線連接埠。預設情況下使用連接埠 3389。

5. 點擊**產生 Blob**按鈕以產生具有編碼連線參數的文字 blob，然後將文字複製並貼到 klsctunnel 公用程式中的對應欄位中。

   blob 包含在管理伺服器和受管理裝置之間建立連線所需的設定。blob 有效時間為 3 分鐘。若已過期，請產生全新 blob。

6. 在 klsctunnel 公用程式中，如果使用代理伺服器，請指定代理伺服器連線設定。

   klsctunnel 公用程式顯示遠端存取用戶端的本機連線的位址和連接埠。

   該公用程式允許管理員關閉通道連線。如果通道連線關閉，則目前與遠端桌面的連線將終止。

7. 執行遠端存取用戶端（RDP 或 VNC），並使用 klsctunnel 公用程式提供的位址和連接埠將其連线到受管理裝置。

與受管理裝置的連線已建立，並且桌面在遠端存取用戶端視窗中可用。

使用卡巴斯基安全管理中心網頁主控台從基於 Linux 的裝置遠端存取基於 Windows 的受管理裝置

遠端桌面連線 (RDP)

先決條件

在您開始之前，確保您已做了如下：

- 受管理裝置的作業系統設定中允許遠端連線。
- 在執行 Windows 的受管理裝置上，安裝了網路代理版本 13.0 或更高版本。
- 管理員具有**啟動 RDP 連線**權限，可以建立 RDP 連線。
- 用於建立 RDP 通道連線的連接埠已開啟（在管理伺服器內容視窗的**連線連接埠**區段中啟用了**開啟用於建立 RDP 連線通道的連接埠**選項）。

若要透過在基於 Linux 的裝置上開啟的卡巴斯基安全管理中心網頁主控台使用 RDP 連線到基於 Windows 的受管理裝置：

1. 在主功能表中，前往**資產管理 → 資產（裝置）**區段或開啟裝置分類。
2. 選取要遠端連線的受管理裝置旁的核取方塊，然後點擊**連線到遠端桌面**按鈕。

   將開啟**連線到遠端桌面**視窗。

   如果您選取多台裝置、一台行動裝置或一台執行 macOS 的裝置，則**連線到遠端桌面**按鈕將會停用。
3. 在**連線到遠端桌面**視窗中，選取 **RDP** 連線類型。
4. 如果受管理裝置的作業系統設定中不允許遠端連線，請點擊**變更設定**按鈕以集中允許遠端連線。

   如果設定正確套用，則會顯示通知。另外，在受管理裝置上，在**設定 → 系統 → 遠端桌面**區段中，**啟用遠端桌面**選項已啟用。

   如果受管理裝置的作業系統設定中允許遠端連線，則不會顯示**變更設定**按鈕。
5. 點擊**下載**按鈕下載 klsctunnel 公用程式，然後執行。

   下載該公用程式時，請考慮以下事項：

   - 若要取得 klsctunnel 公用程式的最新版本，請確保管理伺服器可以存取卡巴斯基更新伺服器。

     您可以執行*下載更新至管理伺服器儲存區*工作，並選取卡巴斯基更新伺服器作為更新來源。如果工作成功完成，管理伺服器就可以存取卡巴斯基更新伺服器。
   - 如果公用程式檔案無法下載，則會顯示錯誤訊息。在這種情況下，手動下載公用程式，然後將其放在管理伺服器裝置的/var/opt/kaspersky/klnagent目錄中。

6. 點擊**產生 Blob**按鈕以產生具有編碼連線參數的文字 blob，然後將文字複製並貼到 klsctunnel 公用程式中的對應欄位中。

   blob 包含在管理伺服器和受管理裝置之間建立連線所需的設定。blob 有效時間為 3 分鐘。若已過期，請產生全新 blob。

7. 在 klsctunnel 公用程式中，如果使用代理伺服器，請指定代理伺服器連線設定。

   klsctunnel 公用程式顯示與遠端裝置的連線的位址和連接埠。

   该公用程式允許管理員關閉通道連線。如果通道連線關閉，則目前與遠端桌面的連線將終止。

8. 執行 RDP 用戶端並使用 klsctunnel 公用程式提供的位址和連接埠將其連線到受管理裝置。

   與受管理裝置的連線已建立，並且可以在 RDP 用戶端視窗中使用桌面。

在使用者不知道的情況下遠端連線到使用者目前的桌面。一旦管理員連線到工作階段，裝置使用者將在無通知的情況下中斷與工作階段的連線。

虛擬網路運算系統 (VNC)

先決條件

在您開始之前，確保您已做了如下：

- 在執行 Windows 的受管理裝置上，安裝了網路代理版本 13.0 或更高版本。
- 在執行 Windows 的受管理裝置上，安裝了 VNC 伺服器。
- 管理員具有**建立通道**權限，可以為 VNC 建立通道連線。
- 用於建立 RDP 通道連線的連接埠已開啟（在管理伺服器內容視窗的**連線連接埠**區段中啟用了**開啟用於建立 RDP 連線通道的連接埠**選項）。

若要透過在基於 Linux 的裝置上開啟的卡巴斯基安全管理中心網頁主控台使用 VNC 連接到基於 Windows 的受管理裝置：

1. 在主功能表中，前往**資產管理 → 資產（裝置）**區段或開啟裝置分類。
2. 選取要遠端連線的受管理裝置旁的核取方塊，然後點擊**連線到遠端桌面**按鈕。

   將開啟**連線到遠端桌面**視窗。

   如果您選取多台裝置、一台行動裝置或一台執行 macOS 的裝置，則**連線到遠端桌面**按鈕將會停用。

3. 在**連線到遠端桌面**視窗中，選取連線類型 **VNC**。
4. 點擊**下載**按鈕下載 klsctunnel 公用程式，然後執行。

   如果公用程式檔案無法下載，則會顯示錯誤訊息。在這種情況下，手動下載公用程式。

5. 在**連線到遠端桌面**視窗中，指定 VNC 連線連接埠。預設情況下使用連接埠 5900。

6. 點擊**產生 Blob**按鈕以產生具有編碼連線參數的文字 blob，然後將文字複製並貼到 klsctunnel 公用程式中的對應欄位中。

   blob 包含在管理伺服器和受管理裝置之間建立連線所需的設定。blob 有效時間為 3 分鐘。若已過期，請產生全新 blob。

7. 在 klsctunnel 公用程式中，如果使用代理伺服器，請指定代理伺服器連線設定。

   klsctunnel 公用程式顯示 VNC 用戶端本機連線的位址和連接埠。

   該公用程式允許遠端用戶關閉通道連線。如果通道連線關閉，則目前與遠端桌面的連線將終止。

8. 執行 VNC 用戶端並使用 klsctunnel 公用程式提供的位址和連接埠將其連線到受管理裝置。

與受管理裝置的連線已建立，並且可以在 VNC 用戶端視窗中使用桌面。

使用卡巴斯基安全管理中心網頁主控台從基於 Windows 的裝置遠端存取基於 Linux 的受管理裝置

遠端桌面連線 (RDP)

先決條件

在您開始之前，確保您已做了如下：

- 在運行 Linux 的受管理裝置上，安裝了 RDP 伺服器。
- 在執行 Linux 的受管理裝置上，安裝了網路代理版本 15.3 或更高版本。
- 管理員具有**啟動 RDP 連線**權限，可以建立 RDP 連線。
- 用於建立 RDP 通道連線的連接埠已開啟（在管理伺服器內容視窗的**連線連接埠**區段中啟用了**開啟用於建立 RDP 連線通道的連接埠**選項）。

若要透過在基於 Windows 的裝置上開啟的卡巴斯基安全管理中心網頁主控台使用 RDP 連線到基於 Linux 的受管理裝置：

1. 在主功能表中，前往**資產管理 → 資產（裝置）**區段或開啟裝置分類。
2. 選取要遠端連線的受管理裝置旁的核取方塊，然後點擊**連線到遠端桌面**按鈕。

   將開啟**連線到遠端桌面**視窗。

   如果您選取多台裝置、一台行動裝置或一台執行 macOS 的裝置，則**連線到遠端桌面**按鈕將會停用。

3. 在**連線到遠端桌面**視窗中，選取 **RDP** 連線類型。
4. 點擊**下載**按鈕下載 klsctunnel 公用程式，然後執行。

下載該公用程式時，請考慮以下事項：

- 若要取得 klsctunnel 公用程式的最新版本，請確保管理伺服器可以存取卡巴斯基更新伺服器。

  您可以執行*下載更新至管理伺服器儲存區*工作，並選取卡巴斯基更新伺服器作為更新來源。如果工作成功完成，管理伺服器就可以存取卡巴斯基更新伺服器。

- 如果公用程式檔案無法下載，則會顯示錯誤訊息。在這種情況下，手動下載公用程式，然後將其放在管理伺服器裝置的/var/opt/kaspersky/klnagent目錄中。

5. 點擊**產生 Blob**按鈕以產生具有編碼連線參數的文字 blob，然後將文字複製並貼到 klsctunnel 公用程式中的對應欄位中。

   blob 包含在管理伺服器和受管理裝置之間建立連線所需的設定。blob 有效時間為 3 分鐘。若已過期，請產生全新 blob。

6. 在 klsctunnel 公用程式中，如果使用代理伺服器，請指定代理伺服器連線設定。

   為此，請選取**使用代理伺服器**核取方塊，然後指定連線設定。

7. 點擊**開啟連接埠**按鈕。

   「遠端桌面連線」登入視窗隨即開啟。

8. 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，然後連線到受管理裝置。

   klsctunnel 公用程式顯示與遠端裝置的連線的位址和連接埠。

   该公用程式允許管理員關閉通道連線。如果通道連線關閉，則目前與遠端桌面的連線將終止。

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。

在使用者不知道的情況下遠端連線到使用者目前的桌面。一旦管理員連線到工作階段，裝置使用者將在無通知的情況下中斷與工作階段的連線。

虛擬網路運算系統 (VNC)

先決條件

在您開始之前，確保您已做了如下：

- 在執行 Linux 的受管理裝置上，安裝了網路代理版本 15.3 或更高版本。
- 在執行 Linux 的受管理裝置上，安裝了 VNC 伺服器。
- 管理員具有**建立通道**權限，可以為 VNC 建立通道連線。
- 用於建立 RDP 通道連線的連接埠已開啟（在管理伺服器內容視窗的**連線連接埠**區段中啟用了**開啟用於建立 RDP 連線通道的連接埠**選項）。

若要透過在基於 Windows 的裝置上開啟的卡巴斯基安全管理中心網頁主控台使用 VNC 連接到基於 Linux 的受管理裝置：

1. 在主功能表中，前往**資產管理 → 資產（裝置）**區段或開啟裝置分類。
2. 選取要遠端連線的受管理裝置旁的核取方塊，然後點擊**連線到遠端桌面**按鈕。

將開啟**連線到遠端桌面**視窗。

如果您選取多台裝置、一台行動裝置或一台執行 macOS 的裝置，則**連線到遠端桌面**按鈕將會停用。

3. 在**連線到遠端桌面**視窗中，選取連線類型 **VNC**。

4. 點擊**下載**按鈕下載 klsctunnel 公用程式，然後執行。

   如果公用程式檔案無法下載，則會顯示錯誤訊息。在這種情況下，手動下載公用程式。

5. 在**連線到遠端桌面**視窗中，指定 VNC 連線連接埠。預設情況下使用連接埠 5900。

6. 點擊**產生 Blob**按鈕以產生具有編碼連線參數的文字 blob，然後將文字複製並貼到 klsctunnel 公用程式中的對應欄位中。

   blob 包含在管理伺服器和受管理裝置之間建立連線所需的設定。blob 有效時間為 3 分鐘。若已過期，請產生全新 blob。

7. 在 klsctunnel 公用程式中，如果使用代理伺服器，請指定代理伺服器連線設定。

   為此，請選取**使用代理伺服器**核取方塊，然後指定連線設定。

8. 點擊**開啟連接埠**按鈕。

   klsctunnel 公用程式顯示 VNC 用戶端本機連線的位址和連接埠。

   該公用程式允許遠端用戶關閉通道連線。如果通道連線關閉，則目前與遠端桌面的連線將終止。

9. 執行 VNC 用戶端並使用 klsctunnel 公用程式提供的位址和連接埠將其連線到受管理裝置。

與受管理裝置的連線已建立，並且可以在 VNC 用戶端視窗中使用桌面。

使用卡巴斯基安全管理中心網頁主控台從基於 Windows 的裝置遠端存取基於 Windows 的受管理裝置

遠端桌面連線 (RDP)

先決條件

在您開始之前，確保您已做了如下：

- 在執行 Windows 的受管理裝置上，安裝了網路代理版本 13.0 或更高版本。
- 管理員具有**啟動 RDP 連線**權限，可以建立 RDP 連線。
- 用於建立 RDP 通道連線的連接埠已開啟（在管理伺服器內容視窗的**連線連接埠**區段中啟用了**開啟用於建立 RDP 連線通道的連接埠**選項）。
- 受管理裝置的作業系統設定中允許遠端連線。

若要透過在基於 Windows 的裝置上開啟的卡巴斯基安全管理中心網頁主控台使用 RDP 連線到基於 Windows 的受管理裝置：

1. 在主功能表中，前往**資產管理 → 資產（裝置）**區段或開啟裝置分類。

2. 選取要遠端連線的受管理裝置旁的核取方塊，然後點擊**連線到遠端桌面**按鈕。

   將開啟**連線到遠端桌面**視窗。

   如果您選取多台裝置、一台行動裝置或一台執行 macOS 的裝置，則**連線到遠端桌面**按鈕將會停用。

3. 在**連線到遠端桌面**視窗中，選取**遠端桌面連線**連線類型。

4. 如果受管理裝置的作業系統設定中不允許遠端連線，請點擊**變更設定**按鈕以集中允許遠端連線。

   如果設定正確套用，則會顯示通知。另外，在受管理裝置上，在**設定 → 系統 → 遠端桌面**區段中，**啟用遠端桌面**選項已啟用。

   如果受管理裝置的作業系統設定中允許遠端連線，則不會顯示**變更設定**按鈕。

5. 點擊**下載**按鈕下載 klsctunnel 公用程式，然後執行。

   下載該公用程式時，請考慮以下事項：

   - 若要取得 klsctunnel 公用程式的最新版本，請確保管理伺服器可以存取卡巴斯基更新伺服器。

     您可以執行*下載更新至管理伺服器儲存區*工作，並選取卡巴斯基更新伺服器作為更新來源。如果工作成功完成，管理伺服器就可以存取卡巴斯基更新伺服器。

   - 如果公用程式檔案無法下載，則會顯示錯誤訊息。在這種情況下，手動下載公用程式，然後將其放在管理伺服器裝置的/var/opt/kaspersky/klnagent目錄中。

6. 點擊**產生 Blob**按鈕以產生具有編碼連線參數的文字 blob，然後將文字複製並貼到 klsctunnel 公用程式中的對應欄位中。

   blob 包含在管理伺服器和受管理裝置之間建立連線所需的設定。blob 有效時間為 3 分鐘。若已過期，請產生全新 blob。

7. 在 klsctunnel 公用程式中，如果使用代理伺服器，請指定代理伺服器連線設定。

   為此，請選取**使用代理伺服器**核取方塊，然後指定連線設定。

8. 點擊**開啟連接埠**按鈕。

   「遠端桌面連線」登入視窗隨即開啟。

9. 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，然後連線到受管理裝置。

   klsctunnel 公用程式顯示與遠端裝置的連線的位址和連接埠。

   該公用程式允許管理員關閉通道連線。如果通道連線關閉，則目前與遠端桌面的連線將終止。

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。

在使用者不知道的情況下遠端連線到使用者目前的桌面。一旦管理員連線到工作階段，裝置使用者將在無通知的情況下中斷與工作階段的連線。

Windows 桌面共用 (WDS)

先決條件

在您開始之前，確保您已做了如下：

- 在執行 Windows 的受管理裝置上，安裝了網路代理版本 13.0 或更高版本。
- 管理員具有**連線到現有 RDP 連線**權限，可以建立 WDS 連線。
- 弱點和修補程式管理授權可用。
- 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。

  檢查 Windows 桌面共用功能是否隨附於您的 Windows 版本中，並確保 Windows 登錄檔中包含 CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} 金鑰。
- 用戶端裝置安裝了 Microsoft Windows Vista 或更新版本。

若要透過在 Windows 的裝置上開啟的卡巴斯基安全管理中心網頁主控台使用 VNC 連線到基於 Windows 的受管理裝置：

1. 在主功能表中，前往**資產管理 → 資產（裝置）**區段或開啟裝置分類。
2. 選取要遠端連線的受管理裝置旁的核取方塊，然後點擊**連線到遠端桌面**按鈕。

   將開啟**連線到遠端桌面**視窗。

   如果您選取多台裝置、一台行動裝置或一台執行 macOS 的裝置，則**連線到遠端桌面**按鈕將會停用。
3. 在**連線到遠端桌面**視窗中，選取連線類型 **Windows 桌面共用**。

   如果弱點和修補程式管理授權不可用，則會顯示錯誤訊息。
4. 點擊**下載**按鈕下載 klsctunnel 公用程式，然後執行。

   如果公用程式檔案無法下載，則會顯示錯誤訊息。在這種情況下，手動下載公用程式。
5. 在選定裝置上的可用活動使用者工作階段清單中，選取要連線的工作階段。

   遠端使用者必須允許連線。如果遠端使用者拒絕連線或遠端使用者在逾時期限內不允許連線，則會顯示錯誤訊息。
6. 點擊**產生 Blob**按鈕以產生具有編碼連線參數的文字 blob，然後將文字複製並貼到 klsctunnel 公用程式中的對應欄位中。

   blob 包含在管理伺服器和受管理裝置之間建立連線所需的設定。blob 有效時間為 3 分鐘。若已過期，請產生全新 blob。
7. 在 klsctunnel 公用程式中，如果使用代理伺服器，請指定代理伺服器連線設定。

   為此，請選取**使用代理伺服器**核取方塊，然後指定連線設定。
8. 點擊**開啟連接埠**按鈕。

   klsctunnel 公用程式顯示 VNC 用戶端本機連線的位址和連接埠。

   該公用程式允許遠端用戶關閉通道連線。如果通道連線關閉，則目前與遠端桌面的連線將終止。

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**。

管理行動裝置

若要透過卡巴斯基安全管理中心管理行動裝置防護，必須使用「行動裝置管理」功能。您必須在每個行動裝置上新增產品授權金鑰才能啟動防護應用程式。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 和 iOS 裝置。防護由安裝在行動裝置上的 Kaspersky Endpoint Security for Android 應用程式和 iOS 裝置管理系統提供。這些行動應用程式會確保防護行動裝置免受 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：

- 卡巴斯基行動裝置防護與管理

  卡巴斯基行動裝置防護和管理外掛程式可讓您在卡巴斯基安全管理中心網頁主控台中管理執行 Android 和 iOS 的裝置。

- iOS MDM 伺服器設定

  iOS MDM 伺服器設定外掛程式可讓您設定用於將 iOS 裝置連線到管理伺服器並管理 iOS 裝置的 iOS MDM 伺服器的設定。

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 和 Kaspersky Secure Mobility Management 說明。

使用 Firebase Cloud Messaging

為了確保及時向 Android 裝置發送命令，卡巴斯基安全管理中心 Linux 使用推播通知機制。推播通知透過 Firebase Cloud Messaging（以下簡稱 FCM）在 Android 裝置和管理伺服器之間交換。在卡巴斯基安全管理中心網頁主控台中，您可以指定Firebase Cloud Messaging設定，將Android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. 在卡巴斯基安全管理中心網頁主控台的主視窗中，選擇**資產管理** →**Mobile**→**Devices**。
2. 開啟三點功能表（ ⋮ ）並選擇**Forced Android device synchronization**。
3. 在**Firebase project number**欄位中，指定 FCM 寄件者 ID。
4. 在**Private key**欄位中，選擇私鑰檔案。

   在下次同步管理伺服器時，Android 裝置將被連線到 Firebase Cloud Messaging。

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 Android 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
  - oauth2.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

如果在卡巴斯基安全管理中心網頁主控台的管理伺服器屬性中指定了代理伺服器設定，則這些設定將用於與 FCM 進行互動。

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

您可以透過公共金鑰基礎架構（PKI）將憑證發放與 Microsoft Certification Authority (CA) 整合。與 PKI 整合旨在簡化管理伺服器對網域使用者憑證的發放。整合後，憑證自動發放。

有關配置與 PKI 整合以發放憑證的詳細資訊，請參閱Kaspersky Secure Mobility Management 說明。

您可以使用指定的設定執行 PKI 整合，並指定 PKI 充當特定類型憑證的憑證來源。PKI 整合設定可讓您為所有類型的憑證設定單獨的預設範本。

使用 PKI 整合發放憑證的具體情況：

- 預設情況下停用 PKI 整合。有關啟用 PKI 和配置其設定的詳細資訊，請參閱Kaspersky Secure Mobility Management 說明。
- 憑證發放使用 Network Agent Windows 進行，它支援管理伺服器和 Microsoft CA 之間的整合。由於可以有多個安裝了網路代理的裝置，因此您可以在**Issuance rules**中指定將連線到 Microsoft CA 的裝置。此裝置必須在執行與 PKI 整合的帳戶的憑證儲存庫中安裝了註冊代理程式 (EA) 憑證。此憑證由網域的 CA 管理員頒發。
- 用於與 PKI 整合的帳戶必須是網域用戶，並且具有*作為服務登入*的權限。
- 卡巴斯基安全管理中心 Linux 一次只能與一個 PKI (Microsoft CA) 整合搭配使用。

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

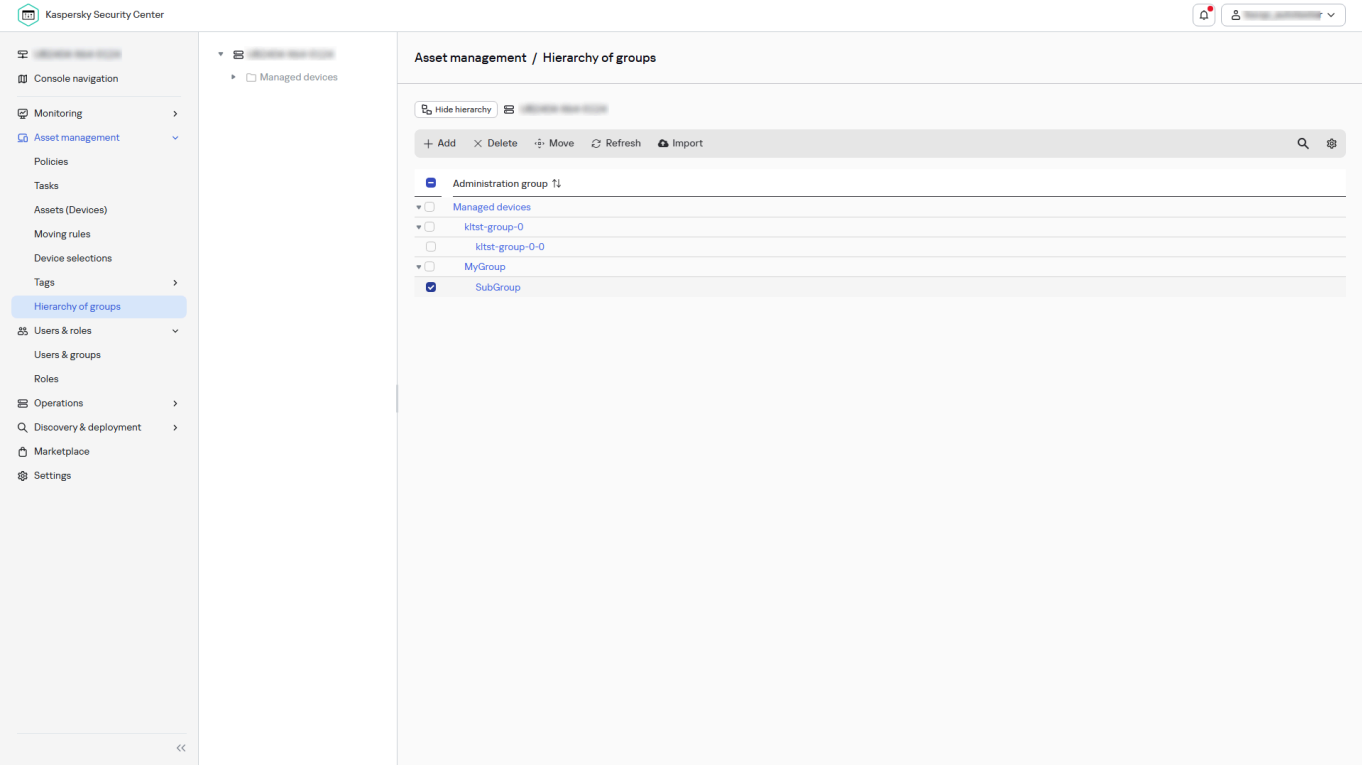
立即安裝卡巴斯基安全管理中心後，管理群組的階層結構僅會包含一個稱為**受管理裝置**的管理群組。當建立管理群組階層架構時，您可以將裝置和虛擬機器新增到**受管理裝置**群組中，也可以新增嵌套群組（參閱下圖）。

檢視管理群組階層架構

要建立管理群組，請執行以下操作：

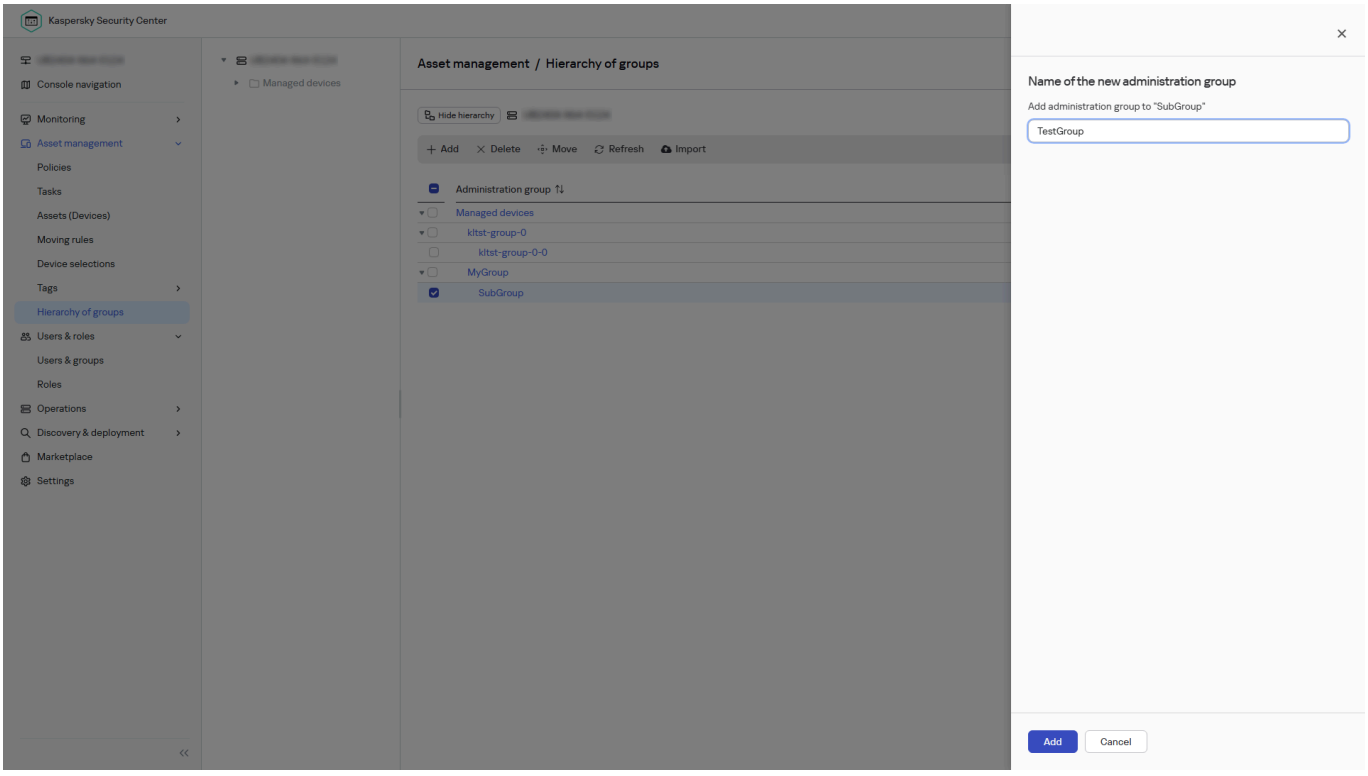
1. 在主功能表中，轉至 **資產管理** → **群組的階層**。

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。

要建立管理群組的架構：

1. 在主功能表中，轉至 **資產管理** → **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. 在主功能表中，轉至 **資產管理** → **群組的階層**。
2. 透過下列方式之一轉到所需管理群組的屬性：
   - 點擊管理群組的名稱。
   - 點擊頁面頂部的**顯示階層**按鈕。在開啟的導覽窗格中，將滑鼠游標懸浮在所需群組的名稱之上，然後按一下設定圖示（ ⚙ ）。

   管理群組內容視窗將開啟。
3. 在內容視窗中，前往**自動安裝**頁籤。
4. 選擇要在裝置上安裝的應用程式的安裝套件，然後點擊**儲存**按鈕。

   若您選擇了同一應用程式的多個僅版本不同的安裝套件，則會儲存最新版本的安裝套件。

   選擇安裝套件後，將為每個應用程式建立一組在管理群組中的裝置上安裝應用程式的群組工作。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。

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)**。

> 您不能重新命名和移動**受管理裝置**群組。

若要將管理群組移至管理群組層次結構的另一個層級：

1. 在主功能表中，前往 **資產管理 →群組的階層**，然後選取要移動的管理群組旁的核取方塊。
2. 點擊工具列上的**移動**按鈕。
3. 在開啟的視窗中，選擇要移動管理群組的位置，然後點擊**移動** 按鈕。

   視窗被關閉，管理群組被移至群組層次結構的另一個層級。

刪除管理群組

如果刪除包含從屬管理伺服器、巢狀群組、用戶端裝置、群組工作或為此群組建立的政策的管理群組，則所有這些也將被刪除。

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。

要刪除管理群組，請執行以下操作：

1. 在主功能表中，前往 **資產管理 →群組的階層**，然後選取要刪除的管理群組旁的核取方塊。
2. 點擊工具列上的**刪除**按鈕。

   該管理群組即會刪除。

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。

案例：卡巴斯基應用程式部署

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 Linux
- Kaspersky Endpoint Security for Windows

階段

Kaspersky 應用程式佈署分步驟進行：

1. **為應用程式下載管理 Web 外掛程式**

   該步驟使用快速設定精靈執行。如果您選擇不執行精靈，請手動下載外掛程式。

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 Web 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 Linux 安裝卡巴斯基應用程式，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。

   或者，您可以從卡巴斯基網站下載網路代理和安全應用程式的分發套件。如果由於某種原因無法遠端安裝應用程式，您可以使用下載的分發套件本機安裝應用程式。

3. **建立、配置和執行遠端安裝工作**

   該步驟是防護部署精靈的一部分。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。

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。

4 **建立和配置工作**

必須配置 Kaspersky Endpoint Security 的*更新*工作。

該步驟是快速啟動精靈的一部分：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。）

5 **建立政策**

手動或透過快速啟動精靈為 Kaspersky Endpoint Security 建立政策。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。

6 **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：

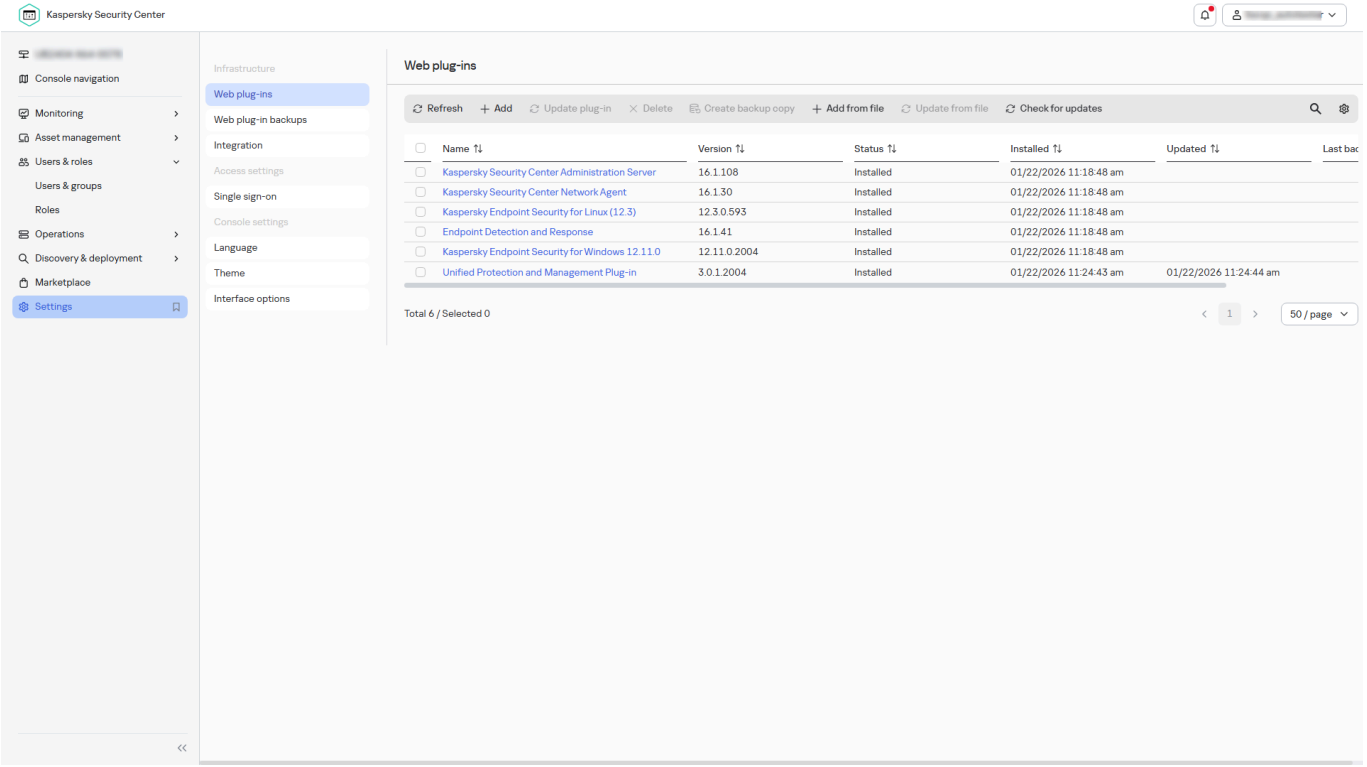
- 所選應用程式的所有所需政策和工作被建立。
- 工作排程根據您的需要被配置。
- 所選應用程式被佈署，或者排程在所選用戶端裝置上佈署。

新增卡巴斯基應用程式的管理外掛程式

要佈署卡巴斯基應用程式，例如 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Windows，您必須新增和安裝此應用程式的管理 Web 外掛程式。

要為卡巴斯基應用程式下載管理 Web 外掛程式：

1. 在主功能表中，轉至**設定 → Web 外掛程式**。



已安裝的 Web 外掛程式清單

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 for Linux）。
   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 Web 外掛程式使用預設配置被下載並顯示在管理 Web 外掛程式清單中。

您可以從檔案中新增外掛程式和更新下載的外掛程式。您可以從卡巴斯基網站下載管理 Web 外掛程式。

若要從檔案中下載或更新管理 Web 外掛程式：

1. 在主功能表中，轉至**設定 → Web 外掛程式**。

2. 請指定外掛程式的檔案和檔案簽名：

   - 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 Web 外掛程式會從檔案中下載，並顯示在管理 Web 外掛程式的清單中。

安裝套件

*安裝套件*是為遠端安裝卡巴斯基應用程式而建立的一組檔案。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。

安裝套件藉由使用以下方法產生：

- 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 ZIP、CAB、TAR 或 TAR.GZ 封存檔案，適用於標準或支援的應用程式。

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卡巴斯基安全管理中心網頁主控台的使用者介面定義。當透過卡巴斯基安全管理中心 Linux 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 Linux 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。

使用 Microsoft Windows 群組政策佈署不受支援。

在卡巴斯基安全管理中心 Linux 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。

下載和建立 Kaspersky 應用程式的安裝套件

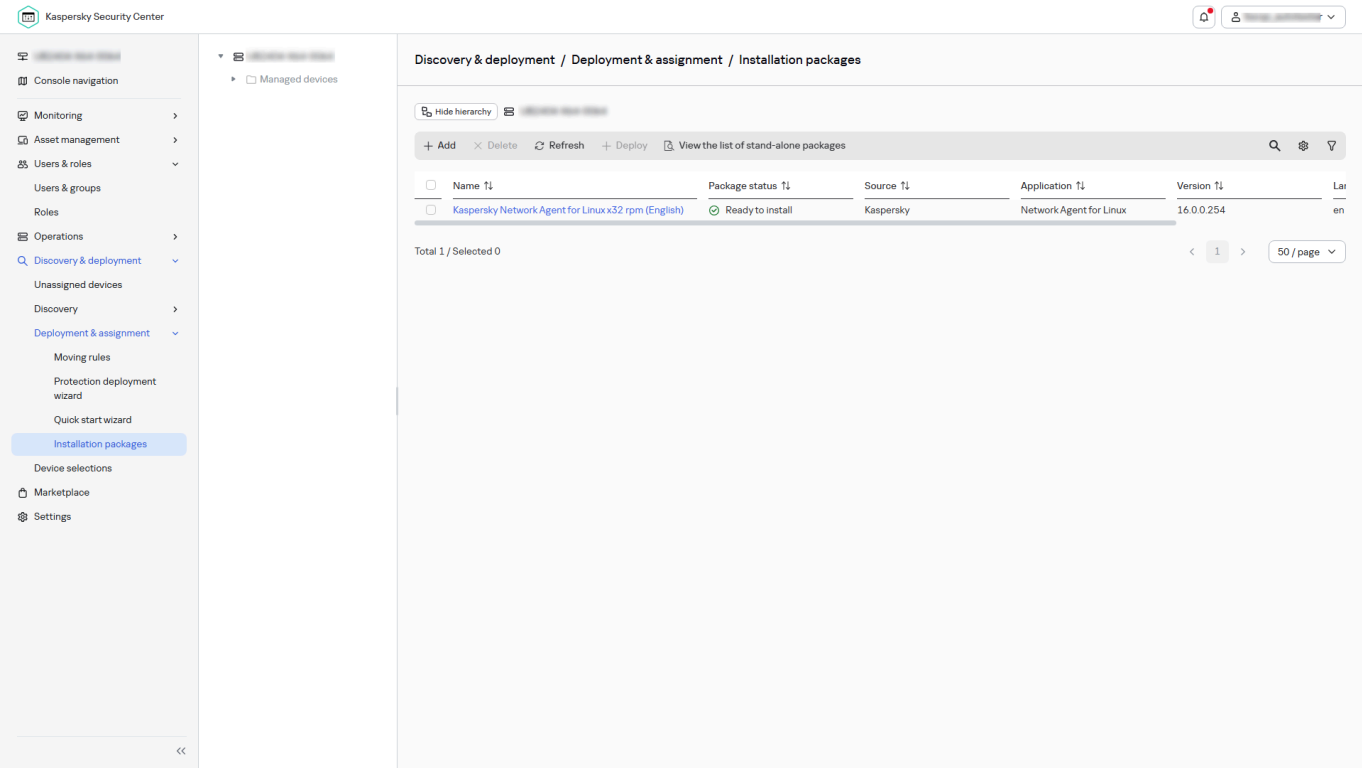
若您的管理伺服器有網際網路的存取權，您可從 Kaspersky 網路伺服器建立 Kaspersky 應用程式的安裝套件。

下載和建立 Kaspersky 應用程式的安裝套件：

1. 在主功能表中，轉至**軟體管理→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。

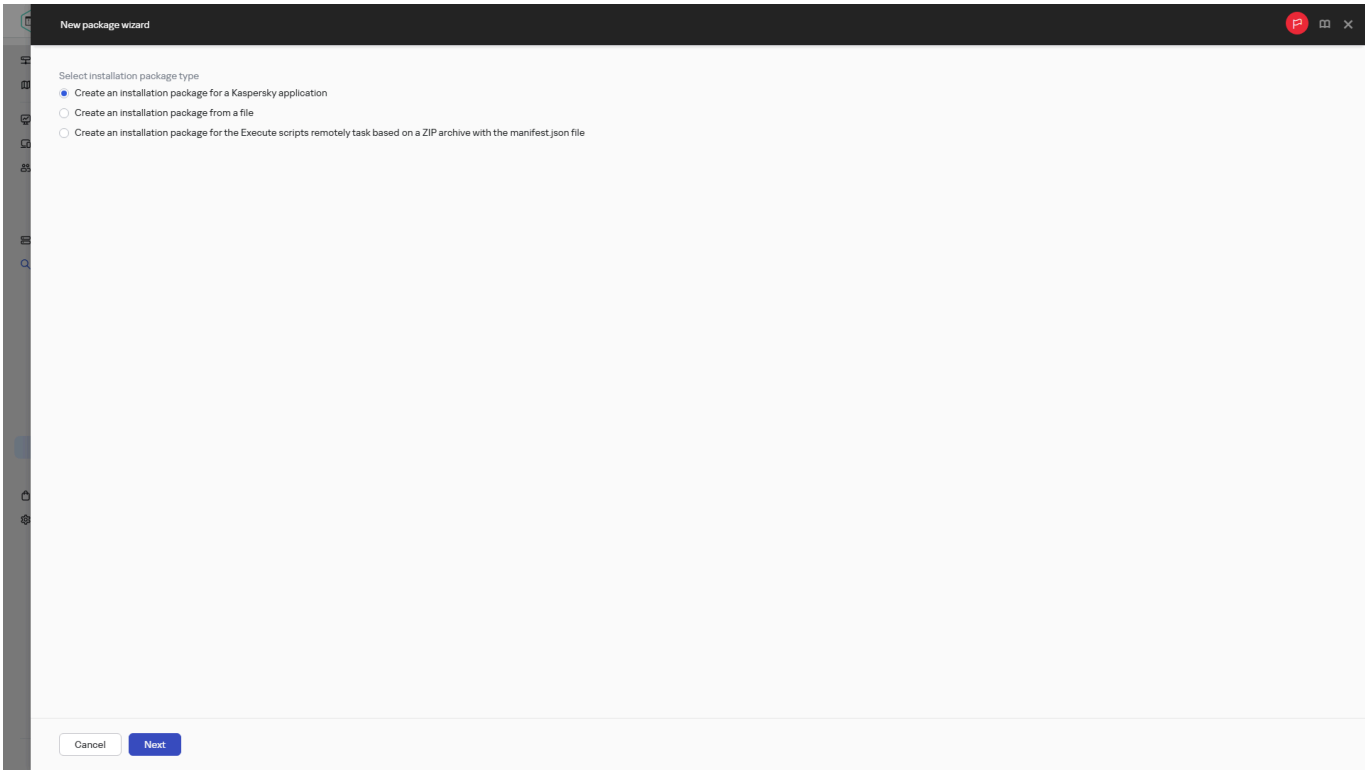


安裝套件清單

2. 點擊**新增**。

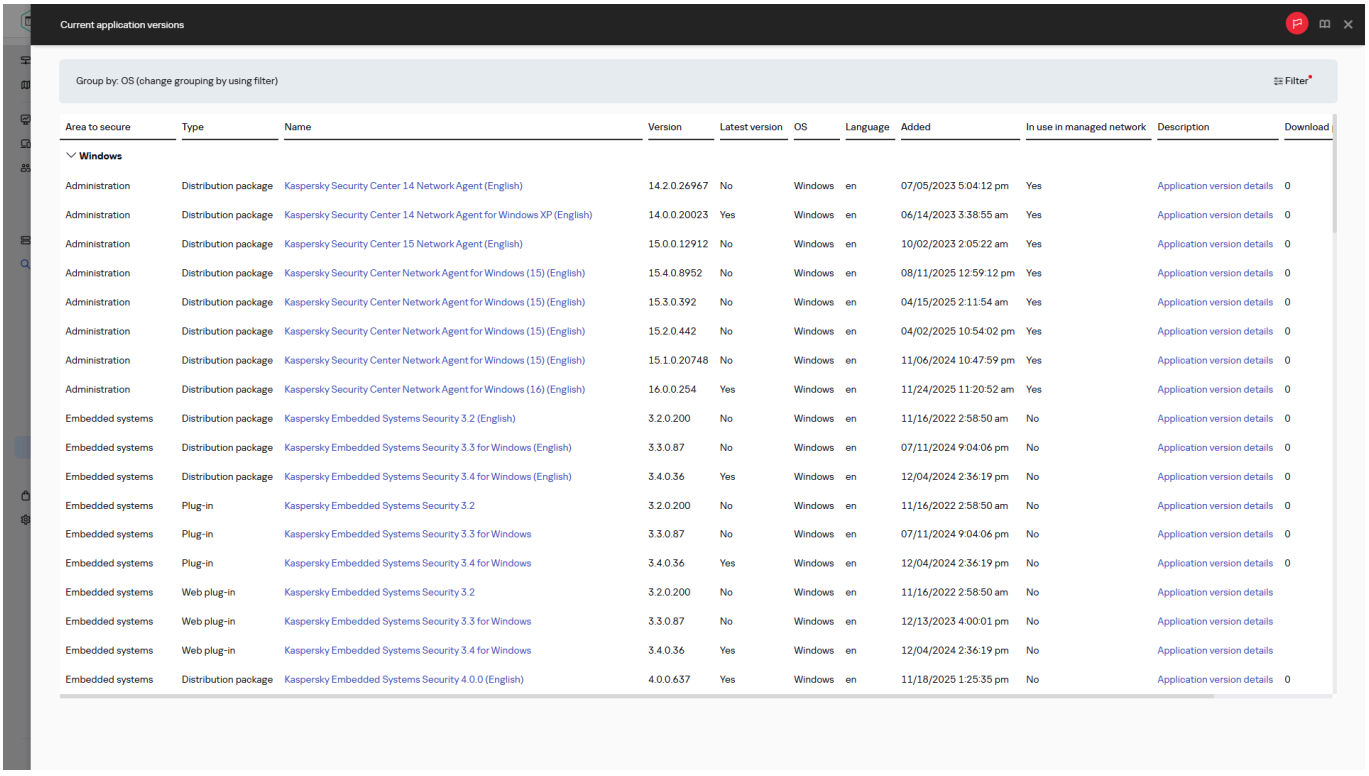
   新套件精靈啟動。使用**下一步**按鈕進行精靈。

3. 選擇**為卡巴斯基應用程式建立安裝套件**。



選取安裝套件類型

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 Linux 相容的那些應用程式的安裝套件。預設情況下，清單僅顯示英文應用程式以及語言與介面語言相符的應用程式。若要顯示其他語言，請按一下**篩選**並配置篩選設定。



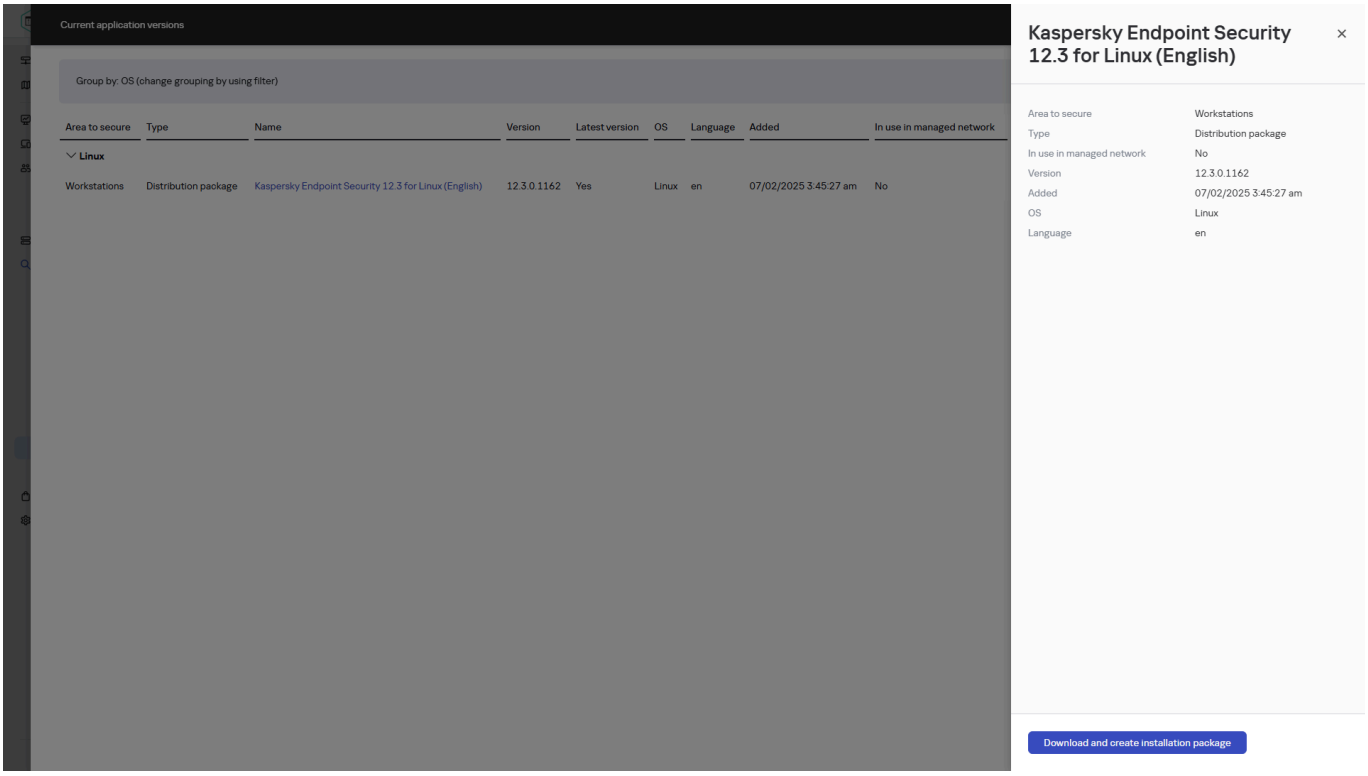
Area to secure	Type	Name	Version	Latest version	OS	Language	Added	In use in managed network	Description	Download
Windows										
Administration	Distribution package	Kaspersky Security Center 14 Network Agent (English)	14.2.0.26967	No	Windows	en	07/05/2023 5:04:12 pm	Yes	Application version details	0
Administration	Distribution package	Kaspersky Security Center 14 Network Agent for Windows XP (English)	14.0.0.20023	Yes	Windows	en	06/14/2023 3:38:55 am	Yes	Application version details	0
Administration	Distribution package	Kaspersky Security Center 15 Network Agent (English)	15.0.0.12912	No	Windows	en	10/02/2023 2:05:22 am	Yes	Application version details	0
Administration	Distribution package	Kaspersky Security Center Network Agent for Windows (15) (English)	15.4.0.8952	No	Windows	en	08/11/2025 12:59:12 pm	Yes	Application version details	0
Administration	Distribution package	Kaspersky Security Center Network Agent for Windows (15) (English)	15.3.0.392	No	Windows	en	04/15/2025 2:11:54 am	Yes	Application version details	0
Administration	Distribution package	Kaspersky Security Center Network Agent for Windows (15) (English)	15.2.0.442	No	Windows	en	04/02/2025 10:54:02 pm	Yes	Application version details	0
Administration	Distribution package	Kaspersky Security Center Network Agent for Windows (15) (English)	15.1.0.20748	No	Windows	en	11/06/2024 10:47:59 pm	Yes	Application version details	0
Administration	Distribution package	Kaspersky Security Center Network Agent for Windows (16) (English)	16.0.0.254	Yes	Windows	en	11/24/2025 11:20:52 am	Yes	Application version details	0
Embedded systems	Distribution package	Kaspersky Embedded Systems Security 3.2 (English)	3.2.0.200	No	Windows	en	11/16/2022 2:58:50 am	No	Application version details	0
Embedded systems	Distribution package	Kaspersky Embedded Systems Security 3.3 for Windows (English)	3.3.0.87	No	Windows	en	07/11/2024 9:04:06 pm	No	Application version details	0
Embedded systems	Distribution package	Kaspersky Embedded Systems Security 3.4 for Windows (English)	3.4.0.36	Yes	Windows	en	12/04/2024 2:36:19 pm	No	Application version details	0
Embedded systems	Plug-in	Kaspersky Embedded Systems Security 3.2	3.2.0.200	No	Windows	en	11/16/2022 2:58:50 am	No	Application version details	0
Embedded systems	Plug-in	Kaspersky Embedded Systems Security 3.3 for Windows	3.3.0.87	No	Windows	en	07/11/2024 9:04:06 pm	No	Application version details	0
Embedded systems	Plug-in	Kaspersky Embedded Systems Security 3.4 for Windows	3.4.0.36	Yes	Windows	en	12/04/2024 2:36:19 pm	No	Application version details	0
Embedded systems	Web plug-in	Kaspersky Embedded Systems Security 3.2	3.2.0.200	No	Windows	en	11/16/2022 2:58:50 am	No	Application version details	
Embedded systems	Web plug-in	Kaspersky Embedded Systems Security 3.3 for Windows	3.3.0.87	No	Windows	en	12/13/2023 4:00:01 pm	No	Application version details	
Embedded systems	Web plug-in	Kaspersky Embedded Systems Security 3.4 for Windows	3.4.0.36	Yes	Windows	en	12/04/2024 2:36:19 pm	No	Application version details	
Embedded systems	Distribution package	Kaspersky Embedded Systems Security 4.0.0 (English)	4.0.0.637	Yes	Windows	en	11/18/2025 1:25:35 pm	No	Application version details	0

可用安裝套件清單

4. 按一下安裝套件的名稱，例如 Kaspersky Endpoint Security for Linux。

   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。



下載安裝套件

5. 請閱讀資訊並點擊**下載並建立安裝套件**按鈕。

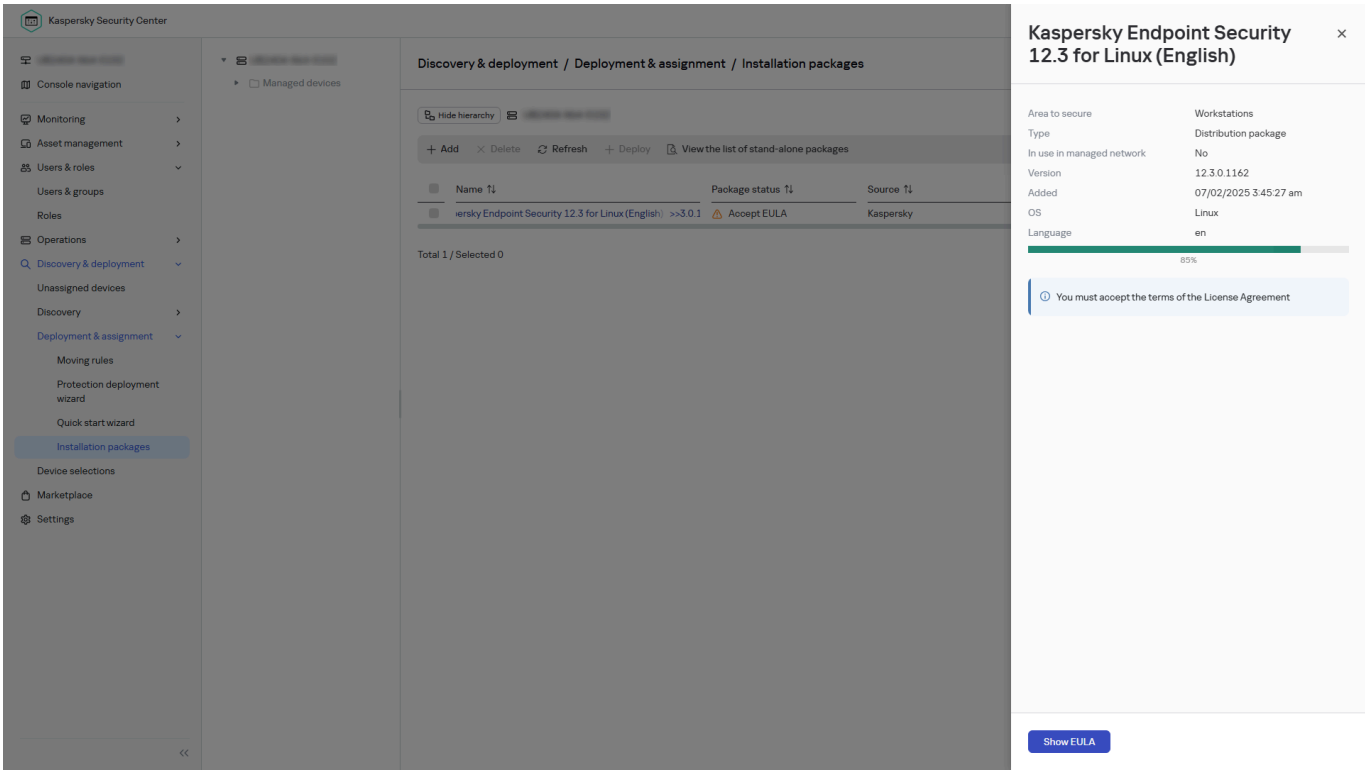
   若分發套件無法轉換為安裝套件，**下載分發套件**按鈕則會取代 **下載並建立安裝套件**顯示。

對於一些卡巴斯基應用程式，下載之前或下載過程中，會顯示「**顯示 EULA**」按鈕。如果不顯示按鈕，請執行以下操作：

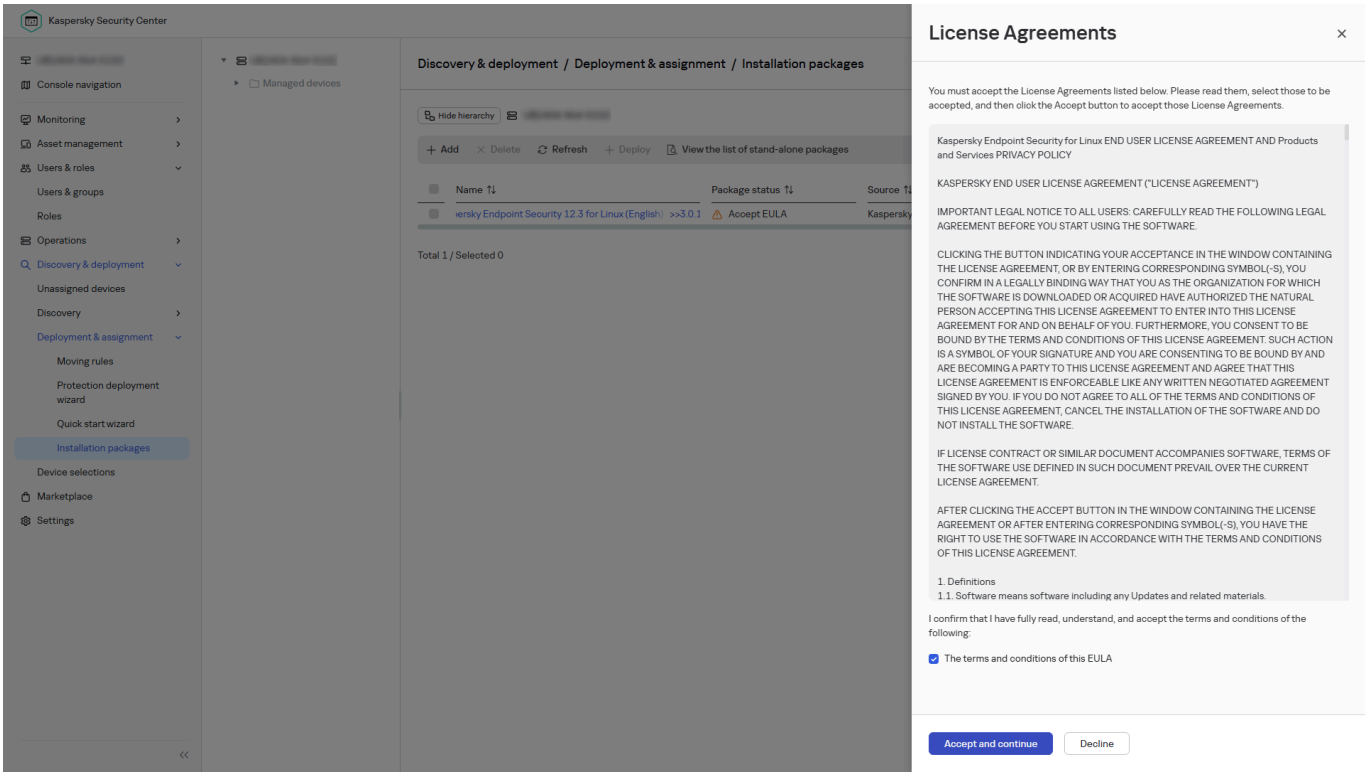
a. 點擊「**顯示 EULA**」按鈕，閱讀《最終使用者產品授權協議 (EULA)》。

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。



下載安裝套件



接受 EULA

您可以關閉精靈視窗。在這種情況下，下載程序將在背景模式下繼續。您可以在**套件狀態**欄中追蹤安裝套件的下載狀態並對狀態進行篩選和排序。

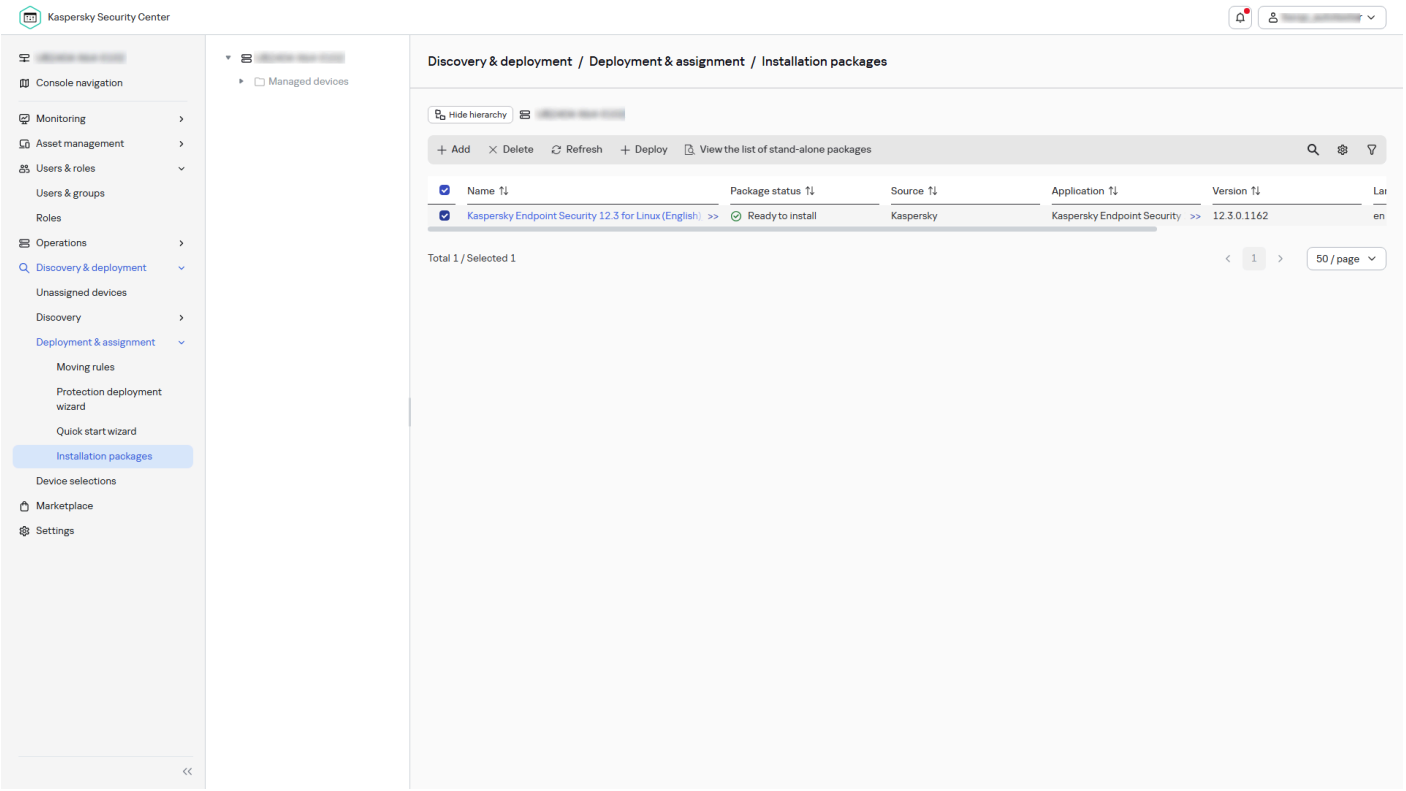
如果下載程序停止並且下載狀態切換為「**接受 EULA**」，則點擊安裝套件名稱，然後執行步驟 5.a 和 5.b。

依預設，狀態為**進行中**和**接受 EULA**的安裝套件會放在清單的開頭。

> 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. 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。



安裝套件清單

從檔案建立安裝套件

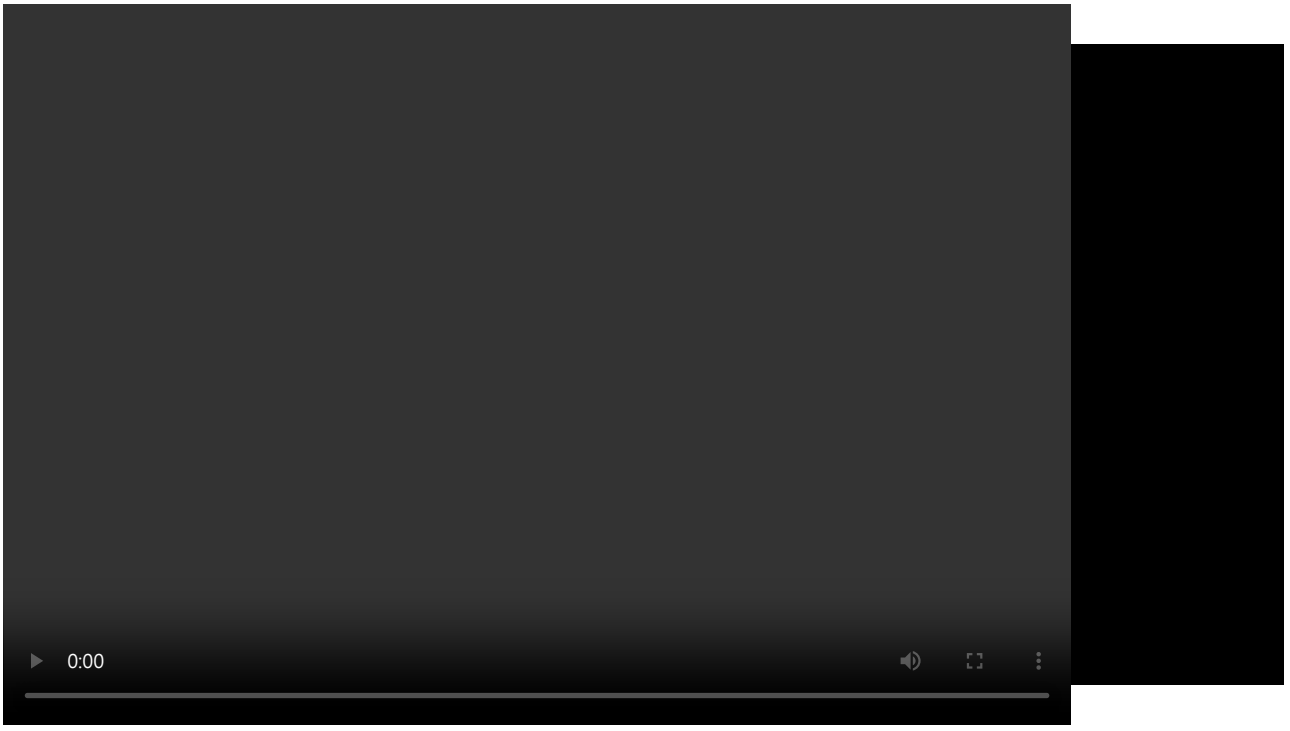
您可使用自訂安裝套件進行以下操作：

- 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。

觀看視訊，了解如何建立和部署適用於 Windows 的自訂安裝套件。本教程的文字版（適用於 Windows 和 Linux 裝置）如下所示。

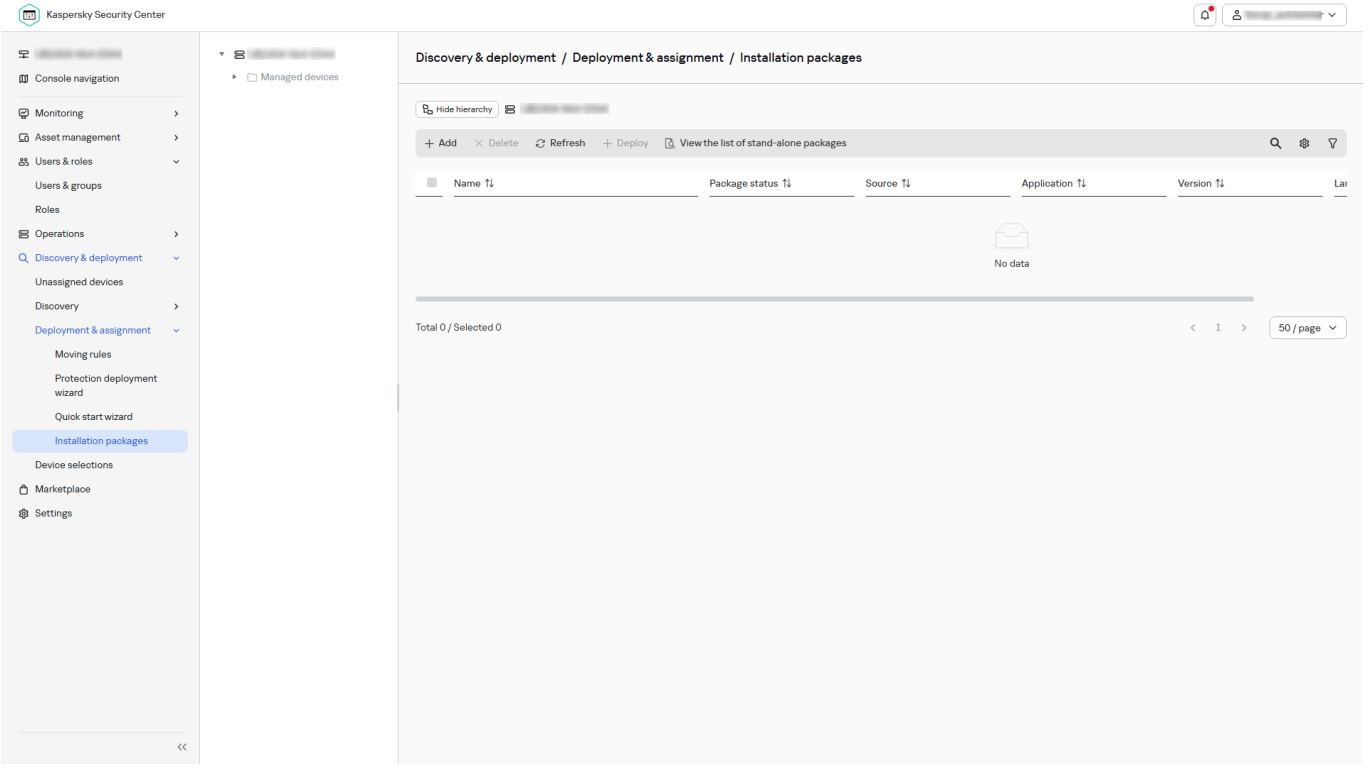


從檔案建立和部署適用於 Windows 的自訂安裝套件。視訊

若要建立應用程式安裝套件：

1. 在主功能表中，轉至**軟體管理→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。

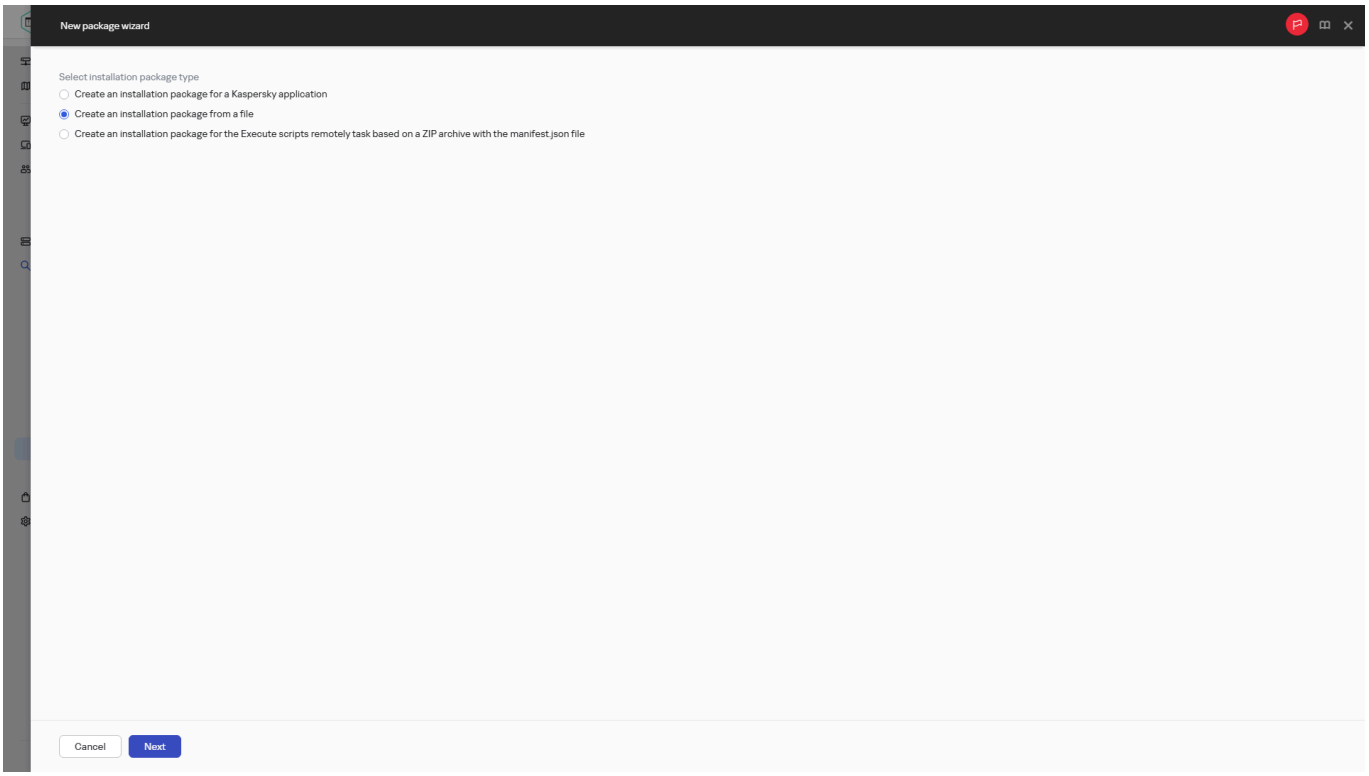


安裝套件清單

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**。



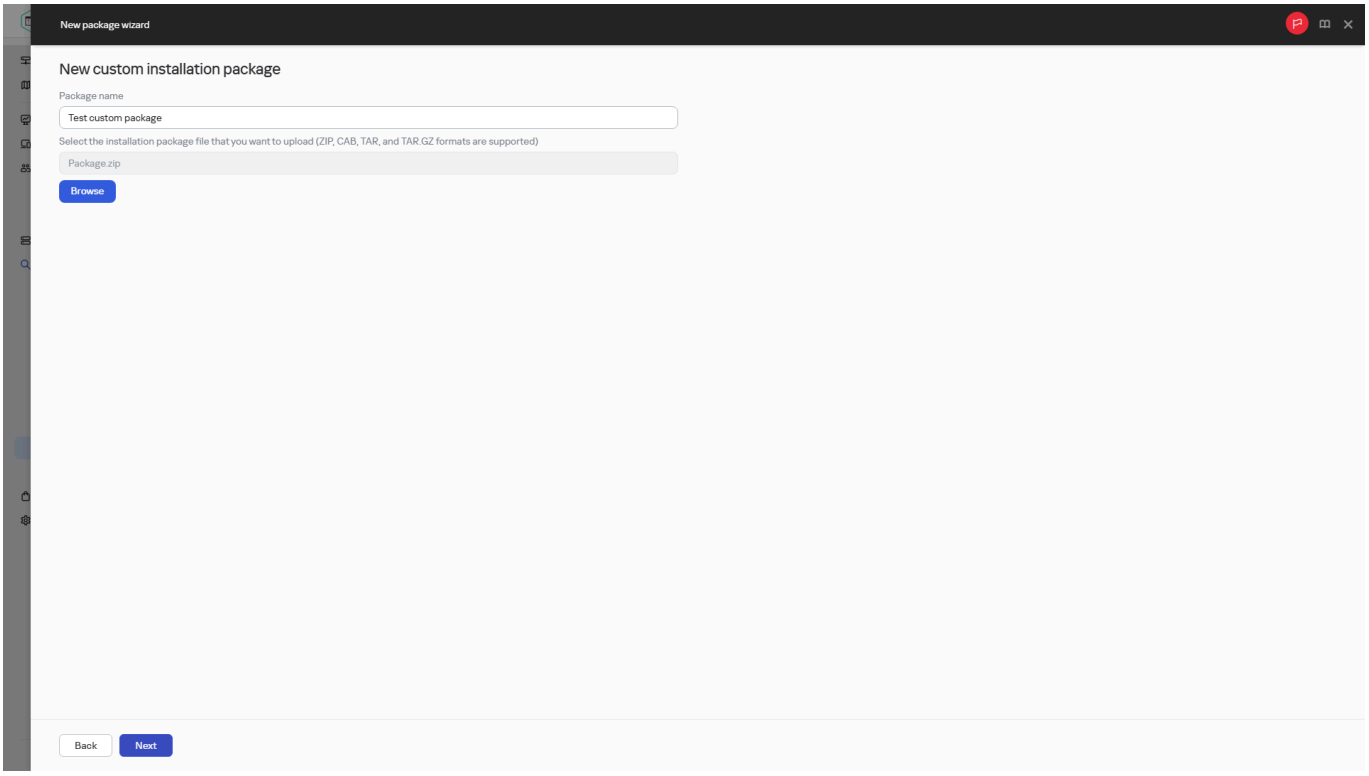
選取安裝套件類型

4. 指定套件名稱並按一下**瀏覽**按鈕。

5. 在開啟的視窗中，選擇位於可用磁盤上的封存檔案。

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。

檔案上傳到管理伺服器開始。



指定安裝套件檔案

6. 如果您指定了卡巴斯基應用程式的檔案，系統可能會提示您閱讀並接受應用程式的最終使用者產品授權協議 (EULA)。要繼續，您必須接受 EULA。僅當您已完全閱讀、理解並接受 EULA 的條款後再選擇**接受此最終使用者產品授權協議的條款和條件**選項。

   此外，系統可能會提示您閱讀並接受隱私政策。要繼續，您必須接受隱私政策。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，才選擇**我接受隱私政策**選項。

7. 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。

   如何建立 deb 或 rpm 格式的安裝套件

   1. 使用以下命令建立 `.sh` 指令碼：

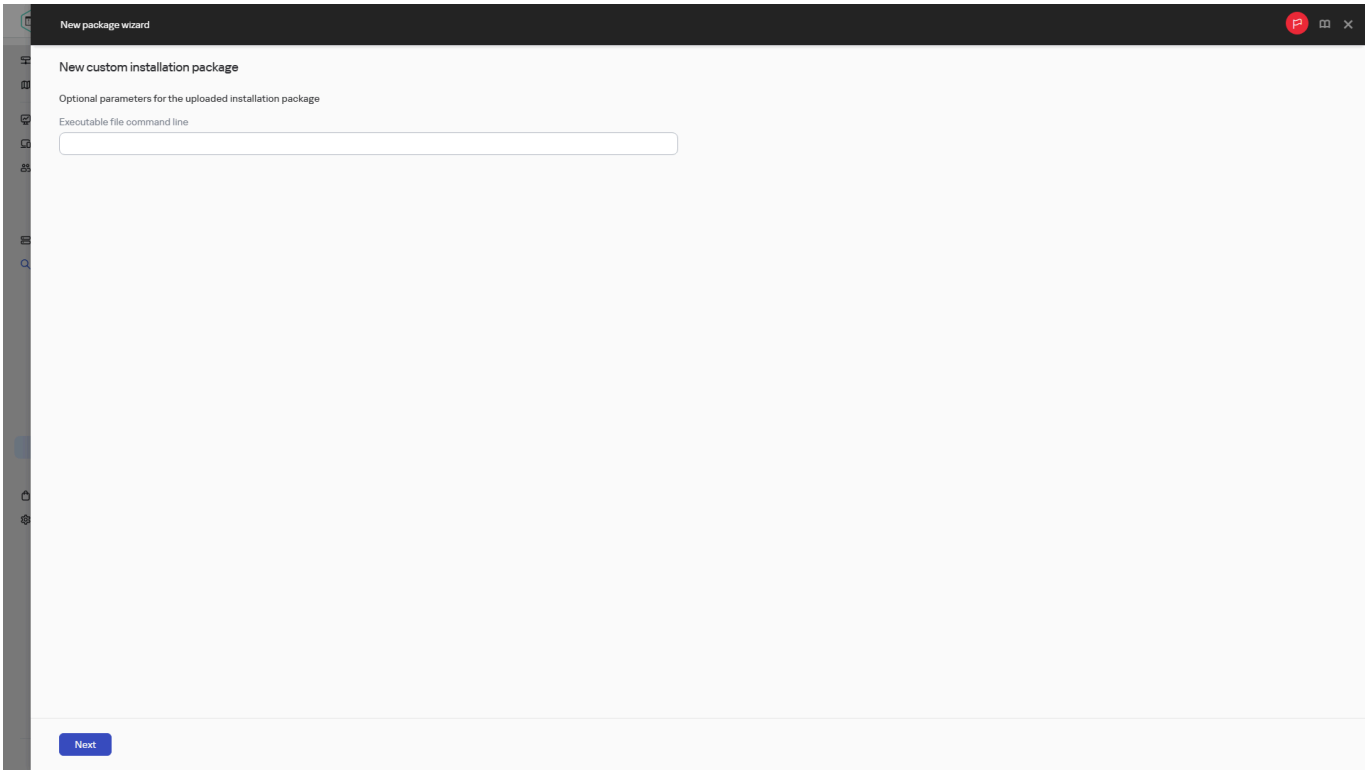
      ```
      #!/bin/sh
      script_dir="$(dirname "$0")"
      apt-get install --yes "$script_dir/<package_name>.deb" </dev/null
      ```

      指令碼內容和命令可能因套件格式和其他細節而異。您可以修改指令碼以適應您的特定配置。

   2. 將建立的指令碼連同以下檔案一起放入壓縮檔案中：`.deb`或者`.rpm`檔案。

   3. 建立安裝套件時，請選擇已建立的指令碼作為可執行檔。

   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。



指定可選的命令列參數

   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。

8. 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。
  - **套件狀態**。安裝套件下載狀態。
  - **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。
  - **修改日期**。安裝套件修改日期。
  - **類型**。安裝套件的類型。
- 變更命令行參數。

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，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 Linux 以安裝應用程式。您可以為 Kaspersky 應用程式或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。

如果管理伺服器可以存取網際網路，則使用**將更新下載至管理伺服器儲存區**工作下載建立網路代理程式獨立安裝套件所需的依賴項。如果管理伺服器無法存取網際網路，請執行下列步驟：

1. 執行下列命令建立RIUtilsArchiveDirUsed標誌：

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. 執行以下命令以重新啟動管理伺服器服務：

   ```
   systemctl restart kladminserver_srv.service
   ```

3. 從卡巴斯基網站下載下列歸檔檔案，並將歸檔檔案放置在/var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives資料夾中：
   - ri_utils_win32.zip
   - ri_utils_arm64.zip

請勿重新命名歸檔檔案。

管理伺服器現在已具備所需的依賴項。

> 請確保第三人無法取得獨立安裝套件。

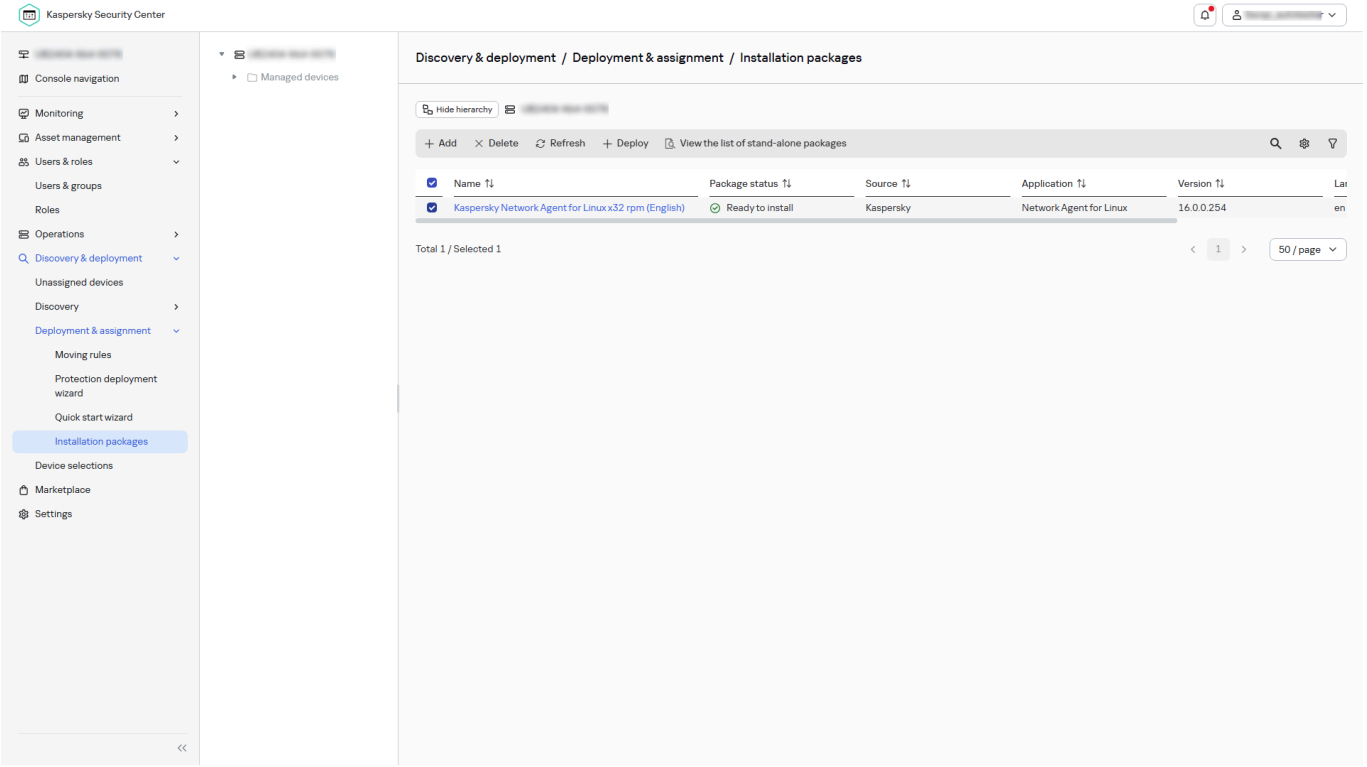
若要建立獨立安裝套件：

1. 在主功能表中，轉至**軟體管理→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。

   > 網路代理獨立套件或在虛擬管理伺服器上建立的任何套件的安裝套件清單中沒有關於大小、檔案雜湊和路徑的資訊。這些獨立套件在下載時產生。

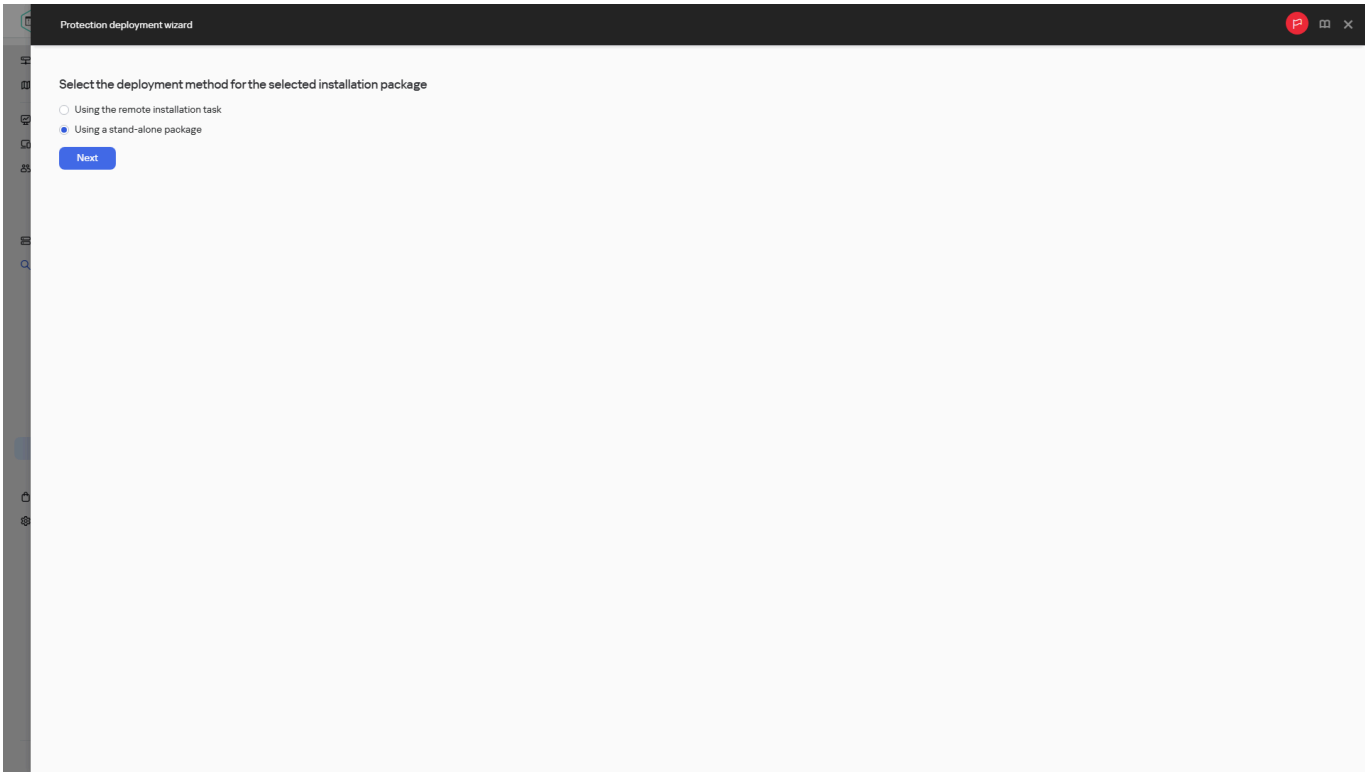
2. 在安裝套件的清單中，選取安裝套件並在上列清單中，點擊**佈署**按鈕。



安裝套件清單

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。



為安裝套件選擇佈署方法

4. 若您要隨所選的應用程式安裝網路代理，請確認**隨此應用程式一起安裝網路代理**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。
- **重新建立已經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，預設會選取**不移動裝置**選項。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，請勾選此選項。

如果要在網路代理安裝後移動用戶端裝置，請選取**將未指派的裝置移動到此群組**選項並指定要將用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。

選擇管理群組來移動用戶端裝置

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。

網路代理安裝套件設定

要設定網路代理安裝套件：

1. 在主功能表中，轉至**軟體管理→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. 按一下網路代理安裝套件的名稱。

“網路代理安裝套件”內容視窗將開啟。

網路代理安裝套件的設定分為以下頁籤：

- **一般**頁籤

  此頁籤顯示有關安裝套件的以下資訊：

  - 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**頁籤

  此頁籤顯示為確保網路代理在安裝後正確工作所需的設定。

  - **設定**區域

    - **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。

    - **使用解除安裝密碼**

      如果啟用此選項，您可以輸入移除密碼（僅適用於執行 Windows 作業系統的裝置上的網路代理）。

      預設情況下已停用該選項。

    - **保護網路代理服務免遭未經授權的移除或終止，並防止設定遭到變更**

      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。

    - **自動為處於「未定義」狀態的元件安裝適用的更新與修補程式**

      如果啟用此選項，將自動安裝管理伺服器、網路代理、卡巴斯基安全管理中心網頁主控台和 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**區域

    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：

    - **管理伺服器位址**

      安裝了管理伺服器的裝置位址。

    - **連接埠號**

      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**

  如果啟用此選項，網路代理存取管理伺服器的身分驗證將使用可由您透過點擊**選取憑證檔案**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**管理伺服器位址**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。

  預設情況下已停用該選項。

- **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**

  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。

- **不使用代理伺服器**

  如果啟用此選項，則使用直接連線將裝置連線到管理伺服器。

- **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。

- **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。

  > 此選項僅適用於設計用於執行 Windows 的裝置的網路代理安裝套件。

- **進階**區域

  在該區域中，您可以配置如何使用連線閘道。

在**連線閘道**設定群組中，您可以設定裝置與管理伺服器之間的連線方法：

- **使用網路代理作為 DMZ 連線閘道**

  如果啟用此選項，將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**

  如果啟用此選項，則將透過連線閘道與管理伺服器建立連線，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**欄位中輸入將充當連線閘道的裝置位址。

在**虛擬機器**設定群組中，如果網路包含虛擬機，則可設定虛擬桌面基礎架構 (VDI) 的連線：

- **為 VDI 啟用動態模式**

  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。

- **為 VM 最佳化設定**

  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。

如果您希望在 Linux 裝置上安裝網路代理後自動提示使用者註冊為裝置所有者，請啟用**允許在安裝網路代理後執行使用者註冊公用程式**選項。

如果啟用此選項，使用者註冊為裝置所有者公用程式將在網路代理安裝後執行。預設情況下已停用該選項。

- **標籤**區域

  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。

  > 自動標記規則不適用於執行 Linux 和 macOS 的裝置所用的網路代理安裝套件。

- **獨立套件**頁籤

在此頁籤上，您可以進行以下操作：

- 檢視可用的獨立安裝套件清單。
- 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**移除**按鈕，移除獨立安裝套件。

- **變更歷史**頁籤

  在此頁籤上，您可以檢視安裝套件變更歷史。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。

執行 卡巴斯基安全管理中心 Linux 建立的獨立套件

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 Linux 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包含在卡巴斯基安全管理中心 Linux 的內部網頁伺服器（如果這是合理的，已為目的裝置使用者設定該網頁伺服器的外部存取權限），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 Linux，向已選取的使用者傳送電子郵件，其中包含在目前使用之網頁伺服器上的獨立套件檔案連結，提示他們執行該檔案（在互動模式或以 "-s" 金鑰進行靜默安裝）。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。

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。

要使用獨立安裝套件安裝應用程式：

1. 在主功能表中，轉至**軟體管理→安裝套件**。
2. 選取所需應用程式的安裝套件旁的核取方塊，然後按一下**佈署**按鈕。
3. 在開啟的視窗中，選擇**使用獨立安裝套件**，然後按一下**下一步**按鈕。
   獨立安裝套件建立精靈啟動。使用**下一步**按鈕進行精靈。
4. 選擇**建立獨立安裝套件**選項。
5. 指定在網路代理安裝後裝置是否必須被移動到管理群組。
6. 在精靈的最後一步，選擇將獨立安裝套件傳輸到用戶端裝置的方法，然後按一下**完成** 按鈕結束嚮導。
7. 將獨立安裝套件傳送到用戶端裝置上。
8. 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。

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。

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 Linux 安裝資料夾（通常為 /opt/kaspersky/ksc64/sbin）。
3. 根據管理伺服器安裝的類型，在根帳戶下輸入以下命令之一：
   - 標準本機安裝：
     `klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <位元組數>`

- 在 卡巴斯基安全管理中心 Linux 容錯移轉叢集上安裝：

  ```
  klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v < number of bytes > --stp klfoc
  ```

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。

分發安裝套件至從屬管理伺服器

卡巴斯基安全管理中心 Linux 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 **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**新工作設定**頁面的**應用程式**下拉清單，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。

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：

- **套件名稱**。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**。
- **網路代理的安裝套件名稱**。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。
- **修改日期**。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。

網路代理獨立套件或在虛擬管理伺服器上建立的任何套件的安裝套件清單中沒有關於大小、檔案雜湊和路徑的資訊。這些獨立套件在下載時產生。

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**移除**按鈕，移除獨立安裝套件。

安裝 Network Agent for Linux

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。佈署分發的卡巴斯基安全管理中心 Linux 到組織裝置通常開始於在其上安裝網路代理。

在 Linux 受管理裝置上初始安裝網路代理的方法如下：

- 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。

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之間的通訊類型以及那些子網中的網路通道容量。
- 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。

準備 Linux 裝置以安裝網路代理

在 Linux 裝置上安裝網路代理之前，您必須執行任何 Linux 裝置所需的準備步驟。

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. 如果要在AltOS上以封閉軟體環境模式安裝網路代理程式，請停用封閉軟體環境模式，直到安裝完成。
3. 使用網頁主控台介面或從卡巴斯基網站下載網路代理安裝套件。

   如果您需要在執行含glibc 2.5的Linux作業系統的裝置上安裝網路代理程式，則必須使用網頁主控台介面或從卡巴斯基網站下載 *Kaspersky Network Agent for Linux Legacy*安裝套件。

4. 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
   - ps公用程式

5. 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. 確保TCP連接埠 22在未指派的Linux裝置上處於開放和可存取。

      若要成功安裝Linux的網路代理程式，必須啟用TCP連接埠22。

   c. 停用要連線裝置的使用者帳戶的 sudo 密碼。

   d. 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`

   e. 儲存並關閉 sudoers 檔案。

   f. 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。

6. 如果要在執行包含 systemd 初始化系統之作業系統的裝置上遠端安裝網路代理，請開啟 `/etc/systemd/logind.conf` 檔案，然後執行下列操作之一：

   - 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`。

   Astra Linux 目標裝置

   若目標裝置正在執行 Astra Linux，在 `/home/<` 使用者名稱 `>/.bashrc` 檔案新增 `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` 字串，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。

   OSnova 目標裝置

如果目標裝置執行 OSnova，請做以下操作：

a. 開啟 `/usr/lib/systemd/logind.conf/10-enable-kill-user-processes.conf` 檔案，然後註解掉 `#KillUserProcess=yes` 行。

b. 開啟 `/usr/lib/NESS/pam-user-session` 檔案，然後註解掉 `"#loginctl terminate-session "$XDG_SESSION_ID""` 行。

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
```

7. 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。

8. 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。

9. 如果要在執行 Ubuntu Server 或 Ubuntu Desktop 版本 10.04 的裝置上安裝網路代理，請執行其他步驟來準備這些裝置。

10. 如果要在執行Linux作業系統且安裝有glibc 2.5的裝置上安裝網路代理程式，請執行額外步驟來準備目標裝置。

11. 如果您在AltOS上以封閉軟體環境模式安裝網路代理程式，請重新啟用封閉軟體環境模式。

12. 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。

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。

準備一部執行 SUSE Linux Enterprise Server 15 的裝置以安裝網路代理

在執行 SUSE 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。

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，以檢查套件是否已安裝。

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，可以製作自己的指令碼 — 使用任何方便的方法。

若裝置沒有 SUSE Linux Enterprise 的 GPG 簽名金鑰，您可能會遇到以下警告：`Package header is not signed!`。選取 `i` 選項即可略過該警告。

準備好 Linux 裝置後，您可以以遠端、互動模式或靜默模式安裝網路代理。

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

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 裝置的常規準備步驟。

> 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 Linux 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。

準備在安裝了glibc 2.5（舊版作業系統）的Linux作業系統上安裝網路代理程式。

在執行含有glibc 2.5的Linux作業系統（舊版作業系統）的裝置上安裝網路代理程式之前，您必須執行兩項準備步驟：適用於任何Linux裝置的一般準備步驟以及本文所述的步驟。

我們建議您使用本機安裝方式在安裝了glibc 2.5（舊版作業系統）的Linux作業系統上安裝網路代理程式。如果此方案需要使用遠端安裝工作，則必須執行以下說明中所述的其他步驟。

> 在具有 root 權限的帳戶下執行本過程中提供的命令。

我們建議您使用本機安裝方式在安裝了glibc 2.5（舊版作業系統）的Linux作業系統上安裝網路代理程式。如果此方案需要使用遠端安裝工作，則必須執行以下說明中所述的其他步驟。

1. 在運行Linux作業系統且安裝了glibc 2.5的裝置上，執行適用於任何Linux裝置的通用準備步驟。

2. 在`/etc/sudoers`檔案中，刪除`Defaults requiretty`行。

3. 停用SSH連線的有效加密演算法允許清單，以便在運行glibc 2.5的Linux作業系統的裝置上安裝網路代理程式。

   為此，請在安裝了管理伺服器的裝置上，或在作為發佈點且其作用範圍包含目標裝置的裝置上，在命令列中執行下列命令：

   ```
   klscflag -fset -pv ".core/.independent" -s "Transport" -n
   SSH_CLIENT_DISABLE_ALGS_PROTECT -t d -v 1
   ```

Linux裝置已準備好遠端安裝網路代理程式。

停用有效加密演算法的允許清單可能會影響SSH連線的安全性。我們強烈建議您在安裝網路代理後立即重新啟用有效加密演算法的允許清單。若要重新啟用有效加密演算法的允許清單，請執行以下命令：

```
klscflag -fset -pv ".core/.independent" -s "Transport" -n SSH_CLIENT_DISABLE_ALGS_PROTECT
-t d -v 0
```

安裝網路代理程式並重新啟用有效加密演算法的允許清單後，運行帶有glibc 2.5（舊版作業系統）的Linux作業系統的裝置現在由管理伺服器管理。

準備在安裝了OpenSSH 6.4（舊版作業系統）的Linux作業系統上安裝網路代理程式

在執行OpenSSH 6.4或更早版本（舊版作業系統）的裝置上安裝網路代理程式之前，必須執行兩項準備步驟：適用於任何Linux裝置的通用準備步驟以及本文所述的步驟。

我們建議您使用本機安裝方式在安裝了glibc 2.5（舊版作業系統）的Linux作業系統上安裝網路代理程式。如果此方案需要使用遠端安裝工作，則必須執行以下說明中所述的其他步驟。

> 在具有root權限的帳戶下執行本指令中提供的命令。

若要準備使用 OpenSSH 6.4 或更早版本的裝置來安裝網路代理：

1. 在使用 OpenSSH 6.4 或更早版本的裝置上，執行對任何 Linux 裝置通用的準備步驟。

2. 停用SSH連線的有效加密演算法的允許清單，以便能夠在使用OpenSSH版本6.4或更早版本的裝置上安裝網路代理。

   為此，請在安裝了管理伺服器的裝置上，或在作為發佈點且其作用範圍包含目標裝置的裝置上，在命令列中執行下列命令：

   ```
   klscflag -fset -pv ".core/.independent" -s "Transport" -n
   SSH_CLIENT_DISABLE_ALGS_PROTECT -t d -v 1
   ```

Linux裝置已準備好遠端安裝網路代理程式。

停用有效加密演算法的允許清單可能會影響SSH連線的安全性。我們強烈建議您在安裝網路代理後立即重新啟用有效加密演算法的允許清單。若要重新啟用有效加密演算法的允許清單，請執行以下命令：

```
klscflag -fset -pv ".core/.independent" -s "Transport" -n SSH_CLIENT_DISABLE_ALGS_PROTECT
-t d -v 0
```

安裝網路代理程式並重新啟用有效加密演算法的允許清單後，運行帶有glibc 2.5（舊版作業系統）的Linux作業系統的裝置現在由管理伺服器管理。

在 Linux 裝置上遠端安裝網路代理

在基於 Linux 的裝置上安裝網路代理之前，您必須完成所有基於 Linux 的裝置所需的一般準備步驟。

完成一般步驟後，您可以按照特定於您的作業系統的附加說明進行操作：

- 準備執行 SUSE Linux Enterprise Server 15 的裝置
- 準備一部在封閉軟體環境模式下執行 Astra Linux 的裝置
- 準備一個執行 Ubuntu Server/Desktop 版本 10.04 和 16.04 的裝置
- 準備執行 Linux 作業系統且安裝有 glibc 2.5 的裝置

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`。

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。

在基於 Linux 的裝置上安裝網路代理之前，您必須完成所有基於 Linux 的裝置所需的一般準備步驟。

完成一般步驟後，您可以按照特定於您的作業系統的附加說明進行操作：

- 準備執行 SUSE Linux Enterprise Server 15 的裝置
- 準備一部在封閉軟體環境模式下執行 Astra Linux 的裝置
- 準備一部執行 Ubuntu Server/Desktop 版本 10.04 和 16.04 的裝置
- 準備一個執行 Linux 作業系統且安裝有 glibc 2.5 的裝置

若要以靜默模式安裝適用於 Linux 的網路代理：

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，才遵循以下步驟操作。
2. 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頁籤名稱。
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。需要 KLNAGENT_GW_ADDRESS。 4—網路代理實例會在隔離區域 (DMZ) 作為連線閘道使用。需要伺服器憑證。
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。
KLNAGENT_DEVICEOWNER_REGISTRATION_START	否	允許在網路代理安裝後作為裝置所有者公用程式執行使用者註冊。如果關閉，則使用者無法註冊為裝置所有者。	1— 使用者註冊為裝置所有者公用程式將在網路代理安裝後執行。 其他—已關閉。
PTCH_ALLOW_APPLY_NONAPROVED_PATCHES	否	定義是否為網路代理自動安裝已下載但處於*未定義*狀態的更新。	true（預設）：更新會被自動安裝。 false：更新不會被自動安裝。

3. 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>.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操作的提示。

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。

在基於 Linux 的裝置上安裝網路代理之前，您必須完成所有基於 Linux 的裝置所需的一般準備步驟。

完成一般步驟後，您可以按照特定於您的作業系統的附加說明進行操作：

- 準備執行 SUSE Linux Enterprise Server 15 的裝置
- 準備一部在封閉軟體環境模式下執行 Astra Linux 的裝置
- 準備一部執行 Ubuntu Server/Desktop 版本 10.04 和 16.04 的裝置
- 準備一個執行 Linux 作業系統且安裝有 glibc 2.5 的裝置

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/lib/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。

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 Linux 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 Linux 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 /var/opt/kaspersky/klnagent 目錄的情景僅是卡巴斯基安全管理中心 Linux 的關鍵情景。因此，如果可能，您必須總是從還原步驟中排除該資料夾。

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 Linux ，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 Linux 中被啟用。

盡量不要回溯網路代理裝置的 /var/opt/kaspersky/klnagent 目錄，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。

安裝 Network Agent for Windows

您也可以在組織的基於 Windows 的裝置上安裝網路代理，以便使用管理伺服器對其進行管理。

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）下載更新並作為 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）。

在執行Microsoft Windows on Arm的裝置上安裝網路代理程式之前，請確保尚未安裝適用於Microsoft Windows x86-64的網路代理程式。否則，安裝程式將會失敗。

在 Windows 受管理裝置上初始安裝網路代理的方法如下：

- 透過 Windows 發佈點執行遠端安裝工作。

  在對未指派的 Windows 裝置執行遠端安裝之前，基於 Windows 的發佈點會自動檢查 UDP 連接埠 137 以確定目標裝置的作業系統類型。如果 UDP 連接埠 137 不可用，發佈點會嘗試連線到目標裝置上的 TCP 連接埠 445，這是執行安裝所必需的。

- 透過使用網路代理的 Windows 安裝套件 (MSI)，借助第三方工具進行應用程式的遠端安裝。

- 透過在受管理裝置上執行應用程式安裝程式。

- 透過程式裝置使用者連結到卡巴斯基安全管理中心 Linux 產生的獨立套件。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。

以互動模式安裝 Windows 網路代理

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 ksc_<版本號>.<build number>_full_<當地語係化語音>.exe 檔案。

   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網路代理**連結以啟動網路代理安裝精靈。遵照精靈的說明。

   當安裝精靈執行時，您可以指定網路代理的進階設定（參閱下文）。

3. 若要使用您的裝置作為指定管理群組的連線閘道，請在設定精靈的**連線閘道**視窗選取**使用網路代理作為 DMZ 連線閘道**。

4. 要在虛擬機上安裝時設定網路代理：

   a. 如果您計畫從虛擬機映像建立動態虛擬機，為虛擬桌面基礎架構 (VDI) 啟用網路代理動態模式。要執行此操作，請在設定精靈的**進階設定**視窗中，選取**為 VDI 啟用動態模式**選項。

      如果您不想從虛擬機映像建立動態虛擬機，略過此步。

   b. 最佳化網路代理的 VDI 操作。要執行此操作，請在設定精靈的**進階設定**視窗中，選取**為 VM 最佳化設定**選項。

      電腦啟動時掃描可執行檔中是否有弱點將被停用。另外，會停用傳送關於以下物件資訊至管理伺服器：

      - 硬體登錄資料
      - 裝置上安裝的應用程式
      - 必須安裝在本機用戶端裝置上的 Microsoft Windows 更新
      - 在本機用戶端裝置上偵測到的軟體弱點

      而且，您將可以在網路代理內容或網路代理政策設定中啟用此資訊的傳送。

安裝精靈完成後，網路代理被安裝在裝置。

您可以檢視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。

以靜默模式安裝 Windows 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 Linux 分發套件，此項目位於 Packages\NetAgent\exec 資料夾中。

> 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 <安裝參數>
   ```

   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
```

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 Linux 專用工作分發該映像到新裝置。

   要捕獲和安裝瓷碟映像，請使用組織中可用的協力廠商工具。

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：

- 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。
- 請確保在目標裝置上首次執行網路代理服務之前，先使用 `-dupfix` 金鑰執行 klmover 公用程式。這是強制性要求，必須在映像部署後首次啟動作業系統時完成。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，您可以解決此問題。

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。

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，它們以單一裝置顯示在卡巴斯基安全管理中心主控台中。該問題發生是因為克隆過程導致新裝置保持相同的內部資料，這將允許管理伺服器在卡巴斯基安全管理中心網頁主控台中關聯裝置到其自己的記錄。

一個特別的*網路代理磁碟克隆模式*允許您避免克隆後在卡巴斯基安全管理中心網頁主控台中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卡巴斯基安全管理中心網頁主控台中的單一記錄。在完成參考裝置映射的克隆時，新裝置會適當顯示在卡巴斯基安全管理中心網頁主控台中（個別記錄下）。

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，在 Linux 命令列輸入以下指令 shell：

```
./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
```

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。
USEPROXY	是否使用代理伺服器。	• 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。

MSI 內容	敘述	可用值
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。
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。

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 Linux 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：

- **指派工作給管理群組**。此種情況下，工作被分配到先前建立的管理群組中的裝置。
- **手動指定裝置位址或是從清單匯入位址**。您可以指定您要為其分配工作的裝置的 DNS 名稱、IP 位址和 IP 子網路。
- **指派工作給裝置分類**。此種情況下，工作被分配到先前建立的分類中的裝置。您可以指定預設分類或您所建立的自訂分類。您最多只能選擇 1000 個裝置。

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 Linux 的遠端安裝工作強制部署中所述進行操作。

關於 卡巴斯基安全管理中心 Linux 的遠端安裝工作

卡巴斯基安全管理中心 Linux 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、透過複製磁碟機映像安裝）。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（此類工作顯示在卡巴斯基安全管理中心網頁主控台的**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。

遠端安裝應用程式

本節包含有關如何在管理群組、具有特定位址的裝置或選擇的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 **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：

   - **指派工作給管理群組**

     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，則工作內容視窗中不會顯示**安全**頁籤，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是從清單匯入位址**

     您可以指定您要為其分配工作的裝置的 DNS 名稱、IP 位址和 IP 子網路。

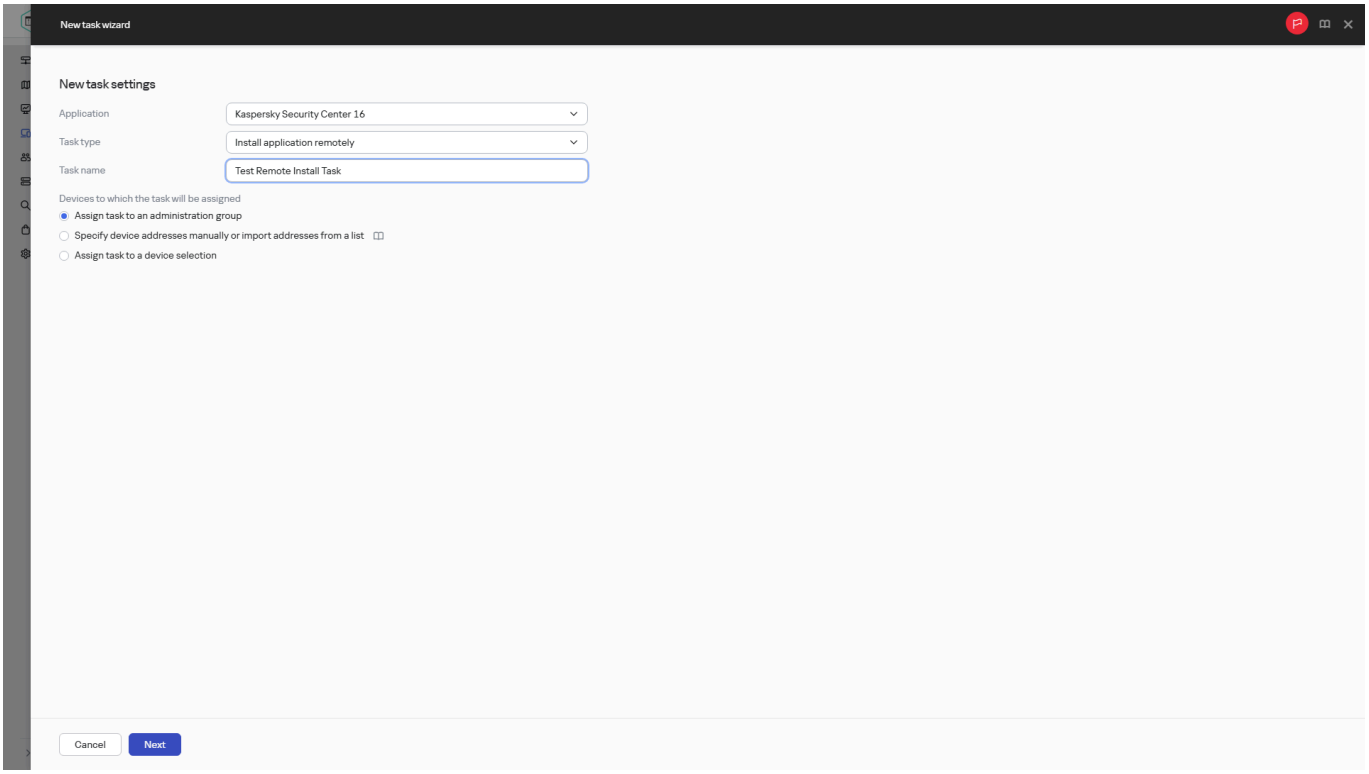
     您可能要使用該選項以對特定子網路執行工作。例如，您可能要安裝特定應用程式到會計裝置，或者掃描疑似被感染子網路中的裝置。

   - **指派工作給裝置分類**

     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。

*遠端安裝應用程式*工作得以為指定裝置建立。如果您選擇了**指派工作給管理群組**選項，工作將是一個組工作。



建立遠端安裝應用程式工作

5. 在**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。

   可用設定取決於在上一步中選擇的選項。

6. 在**安裝套件**步驟中，指定以下設定：

   - 在**選取安裝套件**欄位中，選擇要安裝的應用程式的安裝套件。
   - 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。

在未安裝網路代理的裝置上安裝 Windows 應用程式（包括 Windows 網路代理）的唯一方法是使用基於 Windows 的發佈點。因此，當您安裝 Windows 應用程式時：

- 選擇此選項。
- 確保為目標用戶端裝置分配了發佈點。
- 確保發佈點基於 Windows。

- **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。

- 在**同時下載的最大數量**欄位中，指定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。

- 在**安裝嘗試次數上限**欄位中，指定安裝程式執行的最大允許次數。

  如果超過參數中指定的嘗試次數，卡巴斯基安全管理中心 Linux 將不再在裝置上啟動安裝程式。若要重新啟動*遠端安裝應用程式*工作，請增加**安裝嘗試次數上限**參數的值並啟動工作。或者，您可以建立新的"*遠端安裝應用程式*"工作。

- 如果您從一個卡巴斯基應用程式移轉到另一個卡巴斯基應用程式，並且當前應用程式受密碼保護，請在**用來解除安裝目前卡巴斯基應用程式的密碼**中輸入密碼。請注意，在移轉過程中，將會解除安裝您目前的卡巴斯基應用程式。

  僅當您在**強制下載安裝套件**設定群組中選擇**使用網路代理**選項時，才可使用**用來解除安裝目前卡巴斯基應用程式的密碼**欄位。

  使用遠端安裝應用程式工作安裝 Kaspersky Endpoint Security for Windows 時，您只能在從 Kaspersky Security for Windows Server 到 Kaspersky Endpoint Security for Windows 遷移方案中使用移除密碼。安裝其他元件時使用移除密碼可能會導致安裝錯誤。

  若要成功完成移轉情境，請確保滿足以下先決條件：

  - 您使用的是適用於 Windows 的卡巴斯基安全管理中心網路代理 14.2 或更高版本。
  - 您正在執行 Windows 的裝置上安裝應用程式。

- 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。

  - **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。

無論**下載之前驗證作業系統類型**的設定為何，當您在未指派的裝置上遠端安裝網路代理程式時，卡巴斯基安全管理中心 Linux 或分發點會自動確定裝置的作業系統類型。

- **在 Active Directory 群組政策中指派安裝套件的安裝**

  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。

- **提示使用者關閉執行中的應用程式**

  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。

- 選擇要在哪些裝置上安裝應用程式：

  - **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。

- 指定裝置是否在安裝後必須被移動到管理群組：

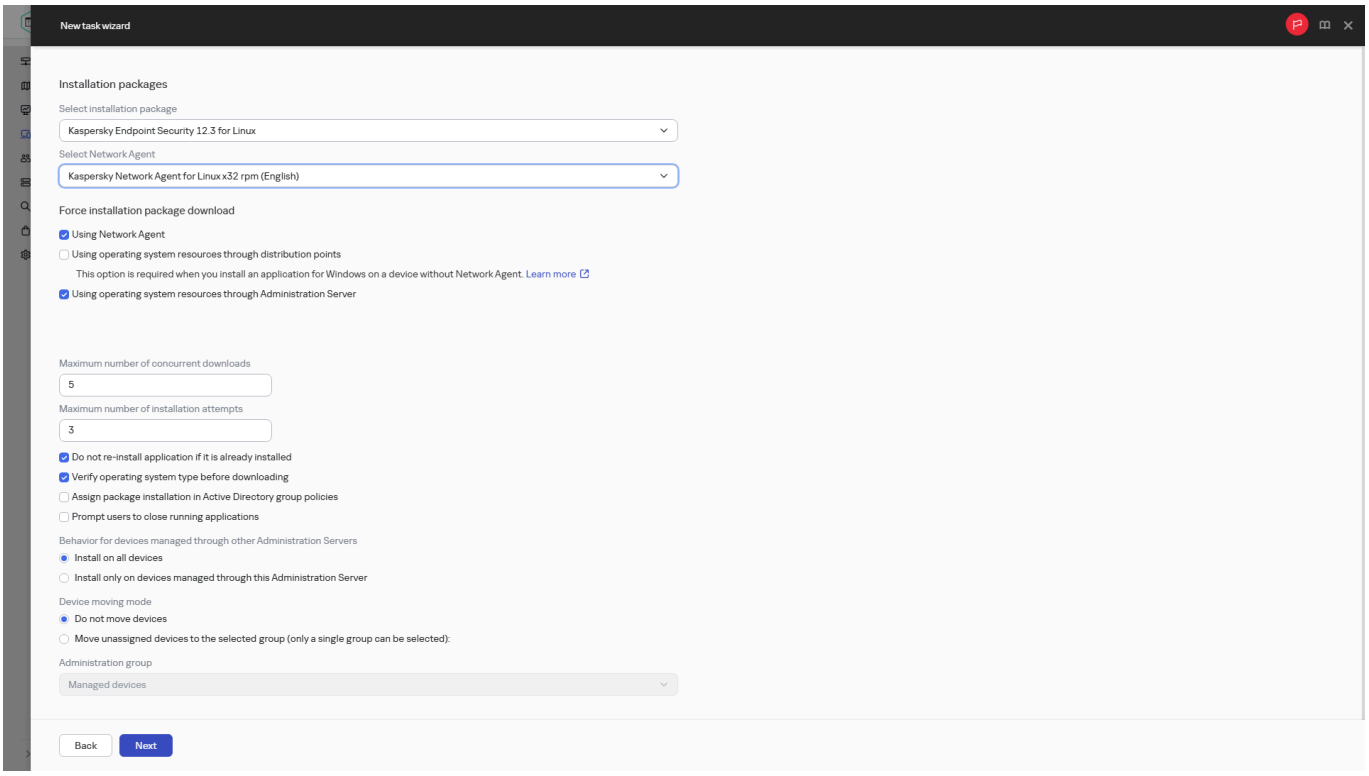
  - **不移動裝置**

    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。

  - **移動未指派的裝置到所選群組（僅可以選取單一群組）**

    裝置被移動到您選取的管理群組。

請注意，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。



指定工作設定

7. 在精靈的這一步，指定在安裝應用程式期間是否必須重新啟動裝置：

- **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。

8. 如有必要，在**選取帳戶以存取裝置**步驟，新增將用於啟*動遠端安裝應用程式*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，該選項不可用。

- **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。

  - **本機或網域帳戶**。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**本機或網域帳戶**，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 Linux 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 Linux 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 "< 使用者電子郵箱 >"
```

9. 在**完成工作建立**步驟中，點擊**完成**按鈕以建立工作並關閉精靈。

   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。在此視窗中，您可以檢查工作參數、修改它們或配置工作啟動排程（如有必要）。

10. 在工作清單中，選擇您建立的工作，然後點擊**開始**。

    或者，等候工作按照您在工作設定中指定的排程啟動。

遠端安裝工作完成後，所選應用程式將安裝在指定裝置上。

在 macOS 裝置上遠端安裝應用程式

若要使用遠端安裝工作在執行 macOS 的裝置上安裝應用程式：

1. 建立一個包含安裝套件和 .sh 安裝指令碼的檔案。

2. 在新工作精靈中停用**下載之前驗證作業系統類型**選項。

或者，您可以使用**遠端執行指令碼**工作。以下文章介紹如何為此工作設定檔案：使用遠端執行指令碼工作在裝置上遠端安裝應用程式。

在從屬管理伺服器上安裝應用程式

> 如果您的管理伺服器版本為 15.4 或更高版本，則只能在從屬管理伺服器上安裝應用程式，前提是從屬管理伺服器的版本為 15.4 或更高版本。

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。

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。

當透過網路代理與管理伺服器之間的通訊管道，將安裝套件傳輸到管理伺服器時，所有準備傳輸的安裝套件都將被快取在 /var/opt/kaspersky/klnagent_srv/1093/.working/ 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。

發佈點收到的資料會儲存在資料夾 /var/opt/kaspersky/klnagent_srv/1103/。

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），您必須在卡巴斯基安全管理中心網頁主控台中編輯安裝套件的任何設定。在卡巴斯基安全管理中心網頁主控台中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。

伺服器在遠端安裝期間向目標裝置發送 ICMP echo-requests（和 ping 命令相同）。

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 Linux 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。

透過卡巴斯基安全管理中心 Linux 的遠端安裝工作強制佈署

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 Linux 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 Linux 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**執行錯過的工作**，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 Linux 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 Linux 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 /var/opt/kaspersky/KSC_Backups* 所在磁碟分割的可用磁碟空間，必須超過所安裝應用程式的分發套件的總大小的好幾倍。

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. 在主功能表中，轉至**軟體管理→安裝套件**。

2. 選取所需應用程式的安裝套件旁的核取方塊，或為該應用程式建立一個新的安裝套件。

   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 Linux 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。

準備 macOS 裝置以遠端安裝網路代理

有以下方法可以在 macOS 受管理裝置上初始安裝網路代理：

- 透過在 macOS 發佈點上執行遠端安裝工作。

- 透過程式裝置使用者連結到卡巴斯基安全管理中心 Linux 產生的獨立套件。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。

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：

      - 透過使用應用程式介面
      - 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。

虛擬基礎架構

卡巴斯基安全管理中心 Linux 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 Linux 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 Linux 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卡巴斯基安全管理中心網頁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 Linux 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 Linux 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**為 VDI 啟用動態模式**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

當安裝網路代理到實體裝置時，不要選取**為 VDI 啟用動態模式**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**為 VDI 啟用動態模式**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。

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 **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）**

  若必須指定密碼才能在目標裝置上使用 sudo 命令，請選取此選項，然後指定 root 帳戶的密碼。卡巴斯基安全管理中心 Linux 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 Linux 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 Linux 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。

監控佈署

要監控卡巴斯基安全管理中心 Linux 部署並確保受管理裝置上安裝了安全應用程式和網路代理，請使用監控和報告功能：

- 使用儀表板的部署小部件即時監控部署。
- 使用報告獲取詳細資訊。

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 **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。

取代協力廠商安全應用程式

透過 卡巴斯基安全管理中心 Linux 進行卡巴斯基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 Linux 提供幾種移除協力廠商應用程式的方法。

當配置應用程式遠端安裝時移除不相容應用程式

您可以在防護部署精靈中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。當該選項被啟用時，卡巴斯基安全管理中心 Linux 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。

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。

遠端移除應用程式或軟體更新

您只能使用網路代理刪除遠端執行 Linux 的受管理裝置上的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：

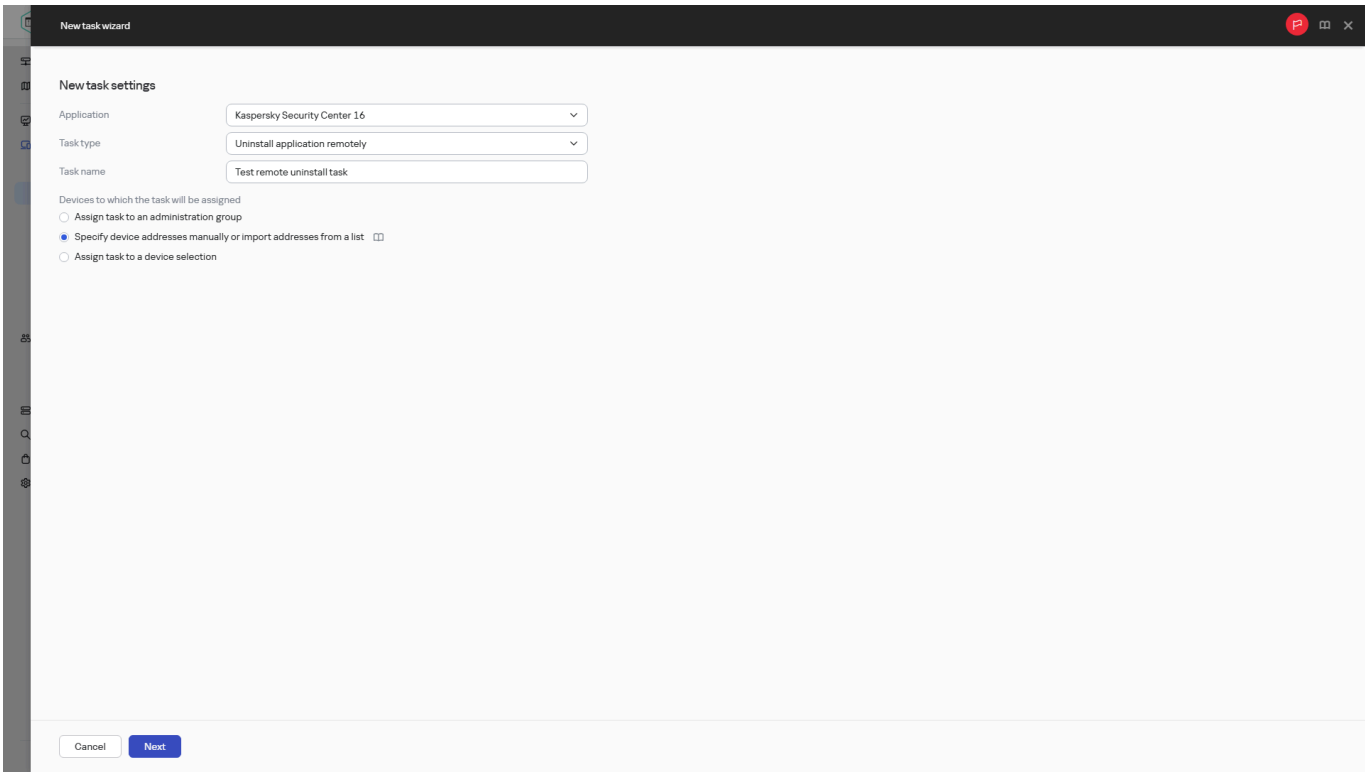
1. 在主功能表中，轉至 **工作**。

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**下拉清單中，選擇卡巴斯基安全管理中心。

4. 在**工作類型**清單中，選擇**遠端解除安裝應用程式**工作類型。

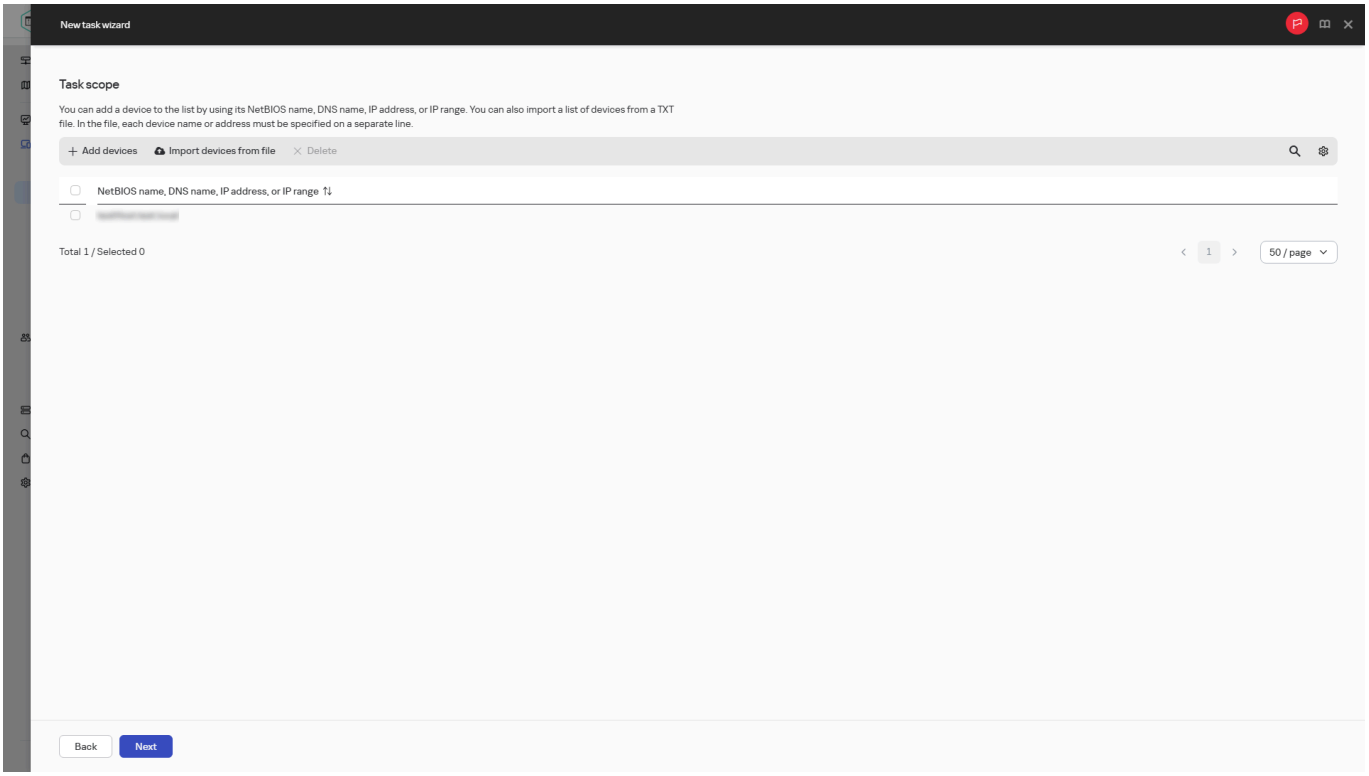
5. 在**工作名稱**欄位，指定新工作的名稱。
   工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。



建立遠端解除安裝應用程式工作

6. 選取要將工作分配到的裝置。

轉到精靈的下一個步驟。



指定工作範圍

7. 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 Linux 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 Linux 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 Linux 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 Linux 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。

8. 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 Linux 作業系統工具傳送檔案。

  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**

> 該選項已過時。請改用**使用網路代理**或**透過發佈點使用作業系統資源**選項。

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 Linux 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 Linux 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。

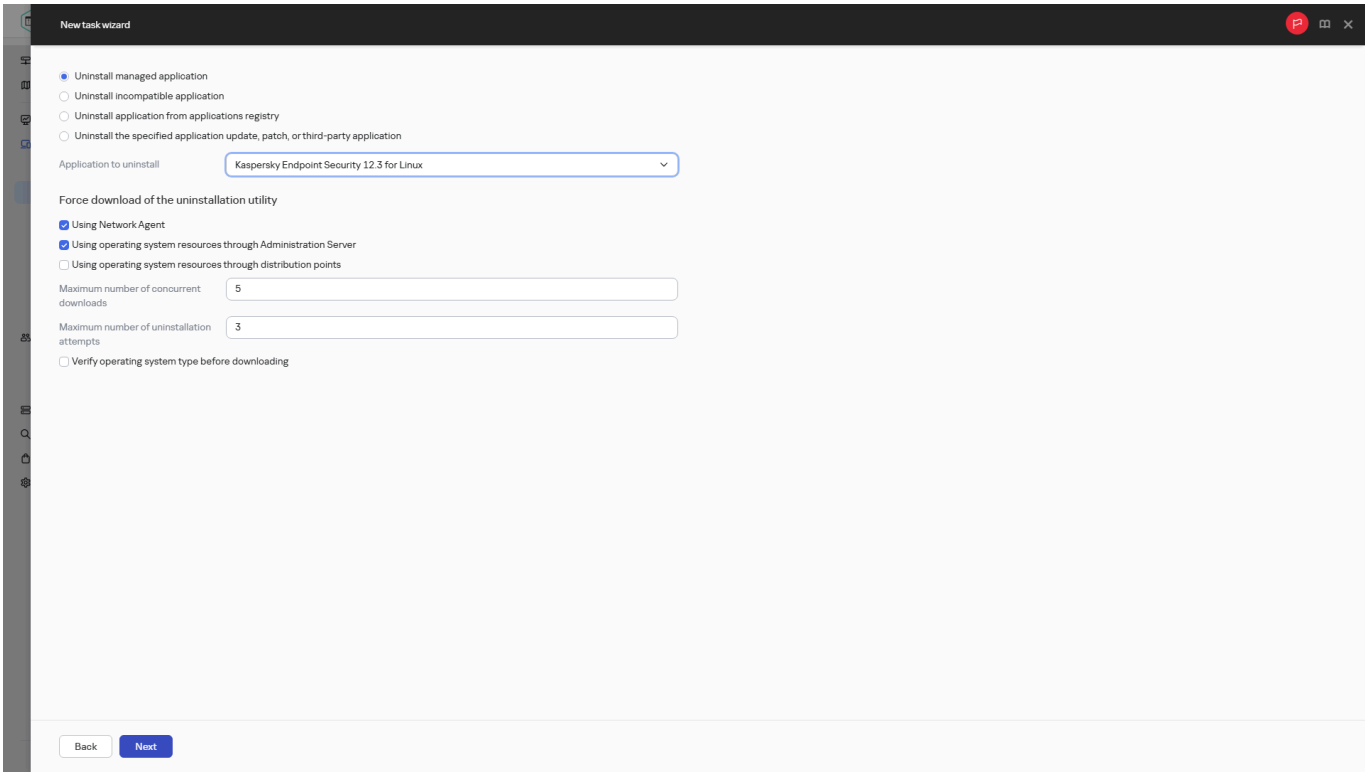
如果超過指定的嘗試次數且裝置已準備好解除安裝應用程式，您可以增加**解除安裝嘗試次數上限**參數的值並啟動工作以解除安裝應用程式。或者，您可以建立新的*遠端解除安裝應用程式*工作。

- **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。

無論**下載之前驗證作業系統類型**的設定為何，當您在未指派的裝置上遠端安裝網路代理程式時，卡巴斯基安全管理中心 Linux 或分發點會自動確定裝置的作業系統類型。

轉到精靈的下一個步驟。



指定工作設定

9. 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。

- **提示使用者動作**

  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）**

  - **在該時間後重新啟動（分鐘）**

- **強制關閉被封鎖工作階段中的應用程式**

  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。

轉到精靈的下一個步驟。

10. 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，該選項不可用。

- **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。

  - **本機或網域帳戶**。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**本機或網域帳戶**，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 Linux 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 Linux 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 >"
    ```

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。

    工作隨即建立、設定，並顯示在**工作**的工作清單中。

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，選中的應用程式會被從所選裝置中移除。

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。

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**選項。
  - 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 Linux 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。

建立「遠端執行指令碼」工作

您可以建立*遠端執行指令碼*工作以在用戶端裝置上執行安裝套件並遠端安裝應用程式。

安裝套件包含一個 ZIP 存檔，其中包含一組用於在用戶端裝置上執行的指令碼以及一個 manifest.json 檔案。透過本文了解有關創建此類安裝套件的更多資訊。

此工作必須僅在具有 Linux 網路代理的裝置上啟動。

啟動遠端執行指令碼工作：

1. 轉至**新工作精靈**並選擇**遠端執行指令碼**工作類型。
2. 輸入工作名稱並選擇工作將指派的裝置。點擊**下一步**按鈕。
3. 選擇一個用於遠端執行且基於 ZIP 存檔、包含 manifest.json 檔案的安裝套件。

   如果您不想在已完成工作的裝置上重新執行工作，請啟用**不要在已完成該工作的裝置上啟動該工作**選項。
4. 選取要執行此工作的帳戶。

   如果選擇預設帳戶，則該工作將由網路代理（root 帳戶）執行。

   當*遠端執行指令碼*工作啟動時，您無法變更為其指派的帳戶。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以正確的帳戶資訊重新啟動它。
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**完成**按鈕。

   *遠端執行指令碼*工作將建立並顯示在工作清單。

從*遠端執行指令碼*工作接收資料後，網路代理會限制所有使用者對接收的資料的訪問，管理員和工作設定中指定的使用者除外。

根據清單檔案建立安裝套件

依據清單檔案建立安裝套件：

1. 在主功能表中，轉至**軟體管理→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. 選取**根據包含 manifest.json 檔案的 ZIP 存檔建立一個用於「遠端執行指令碼」工作的安裝套件**。

4. 指定套件名稱並按一下**瀏覽**按鈕。
   在開啟的視窗中，選擇一個檔案來建立安裝套件。

5. 選擇位於可用磁碟的封存檔案。在本文中了解如何為此工作準備存檔。
   檔案將開始上傳到卡巴斯基安全管理中心 Linux 管理伺服器。
   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。

6. 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，您可以透過點擊自訂安裝套件名稱的連結：

- 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。
  - **版本**。應用程式版本。
  - **建立日期**。安裝套件建立日期。
  - **修改日期**。安裝套件修改日期。
  - **路徑**。前往管理伺服器自訂安裝套件的路徑。
- 變更檔案名稱與命令行參數。此功能僅供非在卡巴斯基應用程式建立之套件使用。

為「遠端執行指令碼」工作準備存檔

基於 manifest.json 檔案的*遠端執行指令碼*工作存檔必須符合以下要求：

- 存檔格式：ZIP。
- 總大小：不超過 1 GB。
- 存檔中的檔案和資料夾的數量是無限的。
- 存檔的清單檔案必須與下面的架構匹配，並且必須命名為 manifest.json。僅在裝置上執行工作期間驗證架構。

  清單檔案的 JSON 架構和陣列描述

  JSON 架構

```
{
 "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "Schema for execute scripts task",
   "type": "object",
    "properties": {
        "version": {
            "type": "integer",
            "enum": [1]
        },
        "actions":{
            "type": "array",
            "items": {
                "type": "object",
                "properties": {
                    "type": {
                        "type": "string",
                        "enum": ["execute"]
                    },
                    "path": {
                        "type": "string"
                    },
                    "args": {
                        "type": "string"
                    },
                    "results":{
                        "type": "array",
                        "items": {
                            "type": "object",
                            "properties": {
                                "code": {
                                    "type": "integer",
                                    "minimum": -255,
                                    "maximum": 255
```

```
                                    },
                                    "next":{
                                        "type": "string",
                                        "enum": ["break", "continue"]
                                    }
                                },
                                "required": [
                                    "code",
                                    "next"
                                ]
                            }
                        },
                        "default_next":{
                            "type": "string",
                            "enum": ["break", "continue"]
                        }
                    },
                    "required": [
                        "type",
                        "path",
                        "default_next"
                    ]
                }
            }
        },
        "required": [
            "version",
            "actions"
        ]
}
```

清單檔案範例

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "scripts/run1.cmd",
      "args": "testArg",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run2.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
```

```
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run3.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

- 檔案的結構必須如下：

  `manifest.json`

  `<file1>`

  `<file2>`

  `<folder1>/<file3>`

  `<folder2>/<folder3>/<file4>`

  `...`

  `<fileX>`

  manifest.json 是工作的清單檔案。

  `<file1>, ...., <fileX>` 是包含要執行之指令碼的一組檔案。

使用「遠端執行指令碼」工作在裝置上遠端安裝應用程式

*遠端執行指令碼*工作可用於透過建立自訂安裝套件在用戶端裝置上遠端安裝應用程式。

在本文中了解如何為此工作準備存檔。

若要建立用於在用戶端裝置上遠端安裝應用程式的安裝套件，您要為此工作上傳的檔案中必須包含下列檔案：

- <套件名稱>.deb

- **install.sh**

  `sudo apt-get install <套件名稱>.deb`

- **manifest.json**

  用於遠端安裝應用程式的 JSON 架構

```
{
  "version": 1,
  "actions": [
```

```
    {
      "type": "execute",
      "path": "install.sh",
      "args": "< 視需要輸入引數 >",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

陣列的描述

1. version：清單檔案和工作的版本。

   目前唯一可接受的值為 1。

2. actions 陣列的元素決定工作中執行的指令碼的組成和順序。

   指令碼的執行順序對應陣列中元素的索引（位置）。

3. 對於 actions 陣列的每個元素，定義了以下元素。

   a. type：指令碼中可執行指令的類型。目前該值始終為 `execute`。

   b. path：壓縮檔案中指令碼檔案的路徑。

   c. args：作為可執行指令的一部分傳遞給指令碼的參數。

   d. results：根據工作結果定義進一步操作的陣列。

      1. code：傳回指令碼的值。

      2. next：接下來要完成的操作。`continue` 操作會繼續執行下一個指令碼（actions 陣列中的元素）；`break` 操作則會停止工作。

   e. default_next：指令碼傳回的值未包含在 results 中時要執行的操作。

當*遠端執行指令碼*工作啟動時，網路代理會將具有應用程式的安裝套件上傳到用戶端裝置。當用戶端裝置收到安裝套件時，該裝置上的網路代理會解析 manifest.json 檔案，並根據結果定義指令碼和操作的執行順序，然後開始執行。

*遠端執行指令碼*工作完成後，應用程式將安裝在用戶端裝置上。

為「遠端執行指令碼」工作設定通知和監控

您可以為*遠端執行指令碼*工作設定監視、事件儲存行為和通知。

檢視遠端執行指令碼的狀態：

1. 在主功能表中，轉至 **工作**。
   工作清單隨即顯示。

2. 選擇工作並點擊**裝置歷史**記錄。
   顯示工作的進度。

設定事件保存行為：

1. 在工作清單中，點擊該工作並轉到**設定**頁籤。

2. 在**通知**區域中，點擊**設定**按鈕。

3. 選取以下選項之一以了解工作完成後應用程式的行為：

   - **儲存所有事件**。

   - **儲存工作進度相關事件**。

   - **僅儲存工作執行結果**。
     事件儲存在**裝置歷史**和**事件儲存區**中。
     預設情況下，只儲存工作執行結果。

     > 如果選擇**儲存所有事件**，則僅儲存工作執行結果。

4. 如果您要將事件保留在管理伺服器資料庫、管理伺服器上的事件日誌或裝置上，請開啟對應的選項。

在本文中了解更多有關設定通知的資訊。

產品授權

此部分提供下列資訊：

- 與 卡巴斯基安全管理中心 Linux 產品授權相關的一般概念
- 有關受管理卡巴斯基應用程式產品授權管理的說明

卡巴斯基安全管理中心 Linux 的產品授權

本節描述與卡巴斯基安全管理中心 Linux 產品授權相關的一般概念。

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 Linux 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 Linux 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 Linux 網路代理最終使用者產品授權協議的條款：

- 從卡巴斯基 Web 伺服器下載網路代理分發套件期間。
- 在安裝 Linux 網路代理期間。
- 透過閱讀 Linux 網路代理分發套件中包含的 license.txt 文件。
- 透過閱讀 Linux 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

*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 Linux 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。

  產品授權到期後，卡巴斯基安全管理中心 Linux 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。

檢視隱私政策。

隱私權政策可在線獲取：https://www.kaspersky.com/Products-and-Services-Privacy-Policy。

隱私權政策也離線提供：

- 您可以在安裝 卡巴斯基安全管理中心 Linux之前先閱讀隱私權政策。
- 隱私權政策文字包含在 卡巴斯基安全管理中心 Linux 安裝資料夾的 license.txt 檔案中。
- privacy_policy.txt 檔案可在受管理裝置的網路代理安裝資料夾中獲取。
- 您可以從網路代理分發套件中解除封裝 privacy_policy.txt 檔案。

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：

- **管理主控台的基本功能**

  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」內容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 Linux 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 Linux 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。 • 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 Linux 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。 • *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。	✓	✓
弱點和修補程式管理：進階功能 您可以定義自動遠端安裝軟體更新和自動修復弱點的規則。	—	✓
系統管理 提供以下功能選項： • 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。	—	✓
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。	✓	✓
透過 Active Directory、KASAP 和 Kaspersky TIP Sandbox 聚合警示和執行回應操作	—	✓

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。

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。如果使用者已配置 Google Firebase Cloud Messaging 服務的使用，則使用者同意以自動模式向 Google Firebase Cloud Messaging 服務提供以下資訊：

- 實例 ID
- Google Firebase Cloud Messaging 服務中的軟體 ID
- 安裝的軟體的版本
- 完整版本的軟體
- Google Play 版本
- 軟體分發套件名稱
- 所提供資料的方案版本
- 作業系統版本
- 軟體 ID

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。

傳輸至 AO Kaspersky Lab 的資料

如果使用者可以使用 Kaspersky Extended Detection and Response Optimum 功能，卡巴斯基安全管理中心 Linux 會在以下情況下傳輸資料：

- 為了向員工指派訓練課程，卡巴斯基安全管理中心 Linux 會將以下資料傳輸到 Automated Security Awareness Platform (KASAP)：使用者電子郵件、備用使用者電子郵件（如果有）、KASAP 中的使用者 ID、培訓群組 ID。
- 為了使用 Kaspersky Sandbox 服務自動執行和偵測惡意行為，受管理的卡巴斯基應用程式會將隔離的物件以及在執行傳輸物件期間建立的檔案從管理伺服器透過網路代理傳輸，然後透過卡巴斯基安全管理中心網頁主控台傳輸到 Kaspersky Sandbox 服務。

本機處理的資料

卡巴斯基安全管理中心 Linux 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 Linux 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 Linux 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 Linux 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
- 啟用與卡巴斯基服務的整合

若要執行其主要功能，卡巴斯基安全管理中心 Linux 可以接收、儲存和處理下列資訊：

- 通過掃描網域控制器（Active Directory、Samba、FreeIPA 和 ALD Pro）或通過掃描 IP 間隔收到的有關組織網路上的裝置的資訊。管理伺服器獨立取得資料或接收來自網路代理的資料。
- 來自網域控制器（Active Directory、Samba、FreeIPA 和 ALD Pro）的有關組織單位、網域、使用者和群組的資訊。管理伺服器自行獲取資料或從被分配充當發佈點的網路代理接收資料。

- 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（適用於屬於 Windows 網域的裝置）、Windows 環境中的裝置名稱（適用於屬於 Windows 網域的裝置）、DNS 網域和 DNS 名稱、IPv4 位址、IPv6 位址、網路位置、MAC 位址、序號、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：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；若裝置是虛擬機，也包括虛擬機類型、管理裝置的虛擬管理伺服器的名稱。
  - 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。
- 通過在受管理裝置上執行遠端診斷接收到的資料：跟踪檔案、系統資訊、裝置上安裝的卡巴斯基應用程式的詳細資訊、傾印檔案、事件日誌、執行從卡巴斯基技術支援接收到的診斷指令碼的結果。
- 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。使用者在卡巴斯基安全管理中心網頁主控台中輸入資料。
- 使用行動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：
  - 有關應用程式的資訊：應用程式名稱、應用程式的完整版本、應用程式的安裝日期和時間、裝置的即時防護狀態、工作階段 ID。
  - 有關應用程式使用的產品授權金鑰的資訊：產品授權金鑰序號和產品授權類型、產品授權狀態、產品授權金鑰有效期（以天為單位）、產品授權金鑰產生和到期日期、提供產品授權的公司名稱、使用訂購時的其他資訊（訂購標誌、到期日期和可用於續約訂購的天數、訂購提供者的網址、目前訂購狀態以及獲得此狀態的原因）、在裝置上啟動應用程式的日期和時間、裝置上的產品授權過期日期和時間。
  - 有關受管理裝置的資訊：裝置名稱、裝置 ID、裝置類型、裝置 IMEI（如果有）、裝置序號（如果有）、裝置製造商、裝置 CPU 系列名稱、裝置擁有者憑證指紋、作業系統類型、作業系統版本、作業系統名稱、裝置上的總磁碟空間、裝置所屬伺服器的名稱、裝置 IP 位址、裝置群組名稱、使用者的可分辨名稱、網域的可分辨名稱、一次性密碼或網域密碼。
  - 自訂命令執行結果資訊：命令 ID、命令執行狀態、命令執行結果；對於裝置定位指令：裝置的緯度、經度、高度和移動速度；對於特寫照片指令：嘗試解鎖時移動裝置前置鏡頭拍攝的照片。
  - 有關裝置掃描的資訊：上次裝置掃描的日期和時間；從其開始掃描的檔案系統中的完整路徑；掃描物件的數量；偵測到的惡意物件的數量；封鎖、刪除和解毒的物件數量；無法解毒的物件數量；驗證錯誤數量；終止的處理程序數量。
  - 有關每個應用程式元件的功能以及每個工作的效能的資訊（以事件的形式呈現）：
    - 事件 ID。
    - 嚴重等級。
    - 事件名稱和類型。

    - 事件原因的描述。
    - 事件發生的日期和時間。
    - 有關竊盜防護操作事件的資訊（裝置解鎖碼、裝置座標、指令傳遞方式、已刪除資料清單）。
    - 處理偵測到的物件或操作的結果（裝置上的檔案名稱；應用程式名稱；威脅名稱；威脅類型；對檔案執行的操作類型；操作結果；錯誤代碼（如果發生）。
    - 有關觸發的合規性規則的資訊（規則標準；套用的操作；套用操作時錯誤的描述（如果發生））。
    - 有關應用程式操作錯誤的資訊（應用程式版本、作業系統版本、裝置名稱、錯誤描述）。
    - 有關 Samsung KNOX 錯誤的資訊（錯誤代碼、無法從其下載檔案的 URL）。
    - 有關授予應用程式的權限的資訊。
    - 有關受管理裝置上安裝的每個應用程式的資訊（應用程式名稱、安裝狀態）。
    - 有關全球接受最終使用者產品授權協議 (EULA) 的資訊：EULA ID、EULA 時間戳記、EULA 文字。
    - Google Firebase Cloud Messaging 設定：寄件者 ID、裝置註冊 ID。
  - 有關裝置公共 IP 位址的資訊。
- 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、型號、作業系統名稱、版本和組建編號、裝置型號、IMEI 編號、電話號碼、UDID、MEID、序號、完整和可用記憶體數量、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。
  - 行動裝置的安全性設定：密碼使用及其對政策設定的遵守情況、已安裝憑證、應用程式和設定檔清單。
  - 與管理伺服器的上一次同步日期和時間以及裝置管理狀態。
- 使用 WebRTC 協定傳輸的行動裝置資料詳情：裝置螢幕映像。
- 被指定傳輸到行動裝置的檔案的詳細資訊。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。
- 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：
  - 受管理裝置上安裝的卡巴斯基應用程式的設定：卡巴斯基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、物件消毒失敗數量、應用程式元件的可用性和狀態、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。

- 來自卡巴斯基安全管理中心 Linux 元件和卡巴斯基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 Linux 與 SIEM 系統整合以進行事件匯出所需的資料。使用者在卡巴斯基安全管理中心網頁主控台中輸入資料。
- 將卡巴斯基安全管理中心 Linux 與網域控制器（Active Directory、Samba、FreeIPA 和 ALD Pro）整合所需的資料。使用者將資料輸入卡巴斯基安全管理中心網頁主控台中。
- 用連線接 Kerberos 單一登入 (SSO) 的 Keytab 檔案。使用者將資料輸入卡巴斯基安全管理中心網頁主控台中。
- 配置與代理伺服器連線網際網路所需的資料。使用者將資料輸入卡巴斯基安全管理中心網頁主控台中。
- 存在於政策和政策設定檔中的 卡巴斯基安全管理中心 Linux 元件和卡巴斯基受管理應用程式的設定。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 Linux 元件和 Kaspersky 受管理應用程式的工作設定。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。
- 系統管理功能處理的資料。網路代理將以下資訊從裝置傳輸到管理伺服器：
  - 受管理裝置上偵測到的硬體相關資訊（硬體登錄檔）。

    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
    - CPU
    - 網卡
    - 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（如果該資訊由作業係統提供）：

    - RAM 總容量
    - 大容量儲存裝置總容量
    - 主機板
    - CPU
    - 網路卡
  - 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。應用程式可以與應用程式控制功能在裝置上偵測到的可執行檔資訊進行比較。

- 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。

- 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。
- 應用程式使用者類別。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。
- 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。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 Windows 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。
- 有關裝置上資料加密錯誤的資訊。加密由卡巴斯基應用程式的加密資料功能執行。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。相應應用程式的線上說明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。
- 組織員工嘗試存取雲端服務的相關資訊。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。
- 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。
- 將卡巴斯基安全管理中心 Linux 與 Kaspersky Cloud Sandbox 和 Kaspersky Threat Intelligence Portal 整合所需的資料（需要安裝卡巴斯基安全管理中心網頁主控台的相應外掛程式）：整合權杖、授權權杖。使用者在卡巴斯基安全管理中心網頁主控台介面中輸入整合權杖。卡巴斯基安全管理中心網頁主控台會將請求中的授權權杖傳送到 Kaspersky Sandbox API。
- 將卡巴斯基安全管理中心 Linux 與 Kaspersky Automated Security Awareness Platform (KASAP) 服務整合所需的資料：用於存取 KASAP Open API 的 API 權杖、URL（透過 Open API 存取 KASAP 的連結）。
- 輸入的啟動碼和金鑰檔案的詳細資訊。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。

- 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、管理伺服器產生的秘密金鑰，以及用於雙因素驗證的一次性密碼。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。

- 管理物件的修訂歷史記錄。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。

- 使用者在其上建立修訂的裝置 IP 位址。IP 位址由管理伺服器自動定義。

- 已刪除之管理物件的登錄資料。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。

- 從檔案建立的安裝套件以及安裝設定。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。

- 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。

- 與受管理裝置和 卡巴斯基安全管理中心 Linux 元件的安全連線憑證。使用者使用管理伺服器 klsetsrvcert 實用程式輸入和傳輸資料。

- 用於對組織內部 Web 資源建立信任的憑證。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。

- 有關使用者已接受卡巴斯基法律協議條款的資訊。

- 使用者在卡巴斯基安全管理中心網頁主控台或程序介面卡巴斯基安全管理中心 OpenAPI 中輸入的管理伺服器資料。

- 使用者在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 Linux：

- 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。

- 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。

- 管理伺服器自行獲取有關聯網裝置的資訊或從被分配充當發佈點的網路代理接收資料。

- 使用 iOS MDM 協定或行動協定，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。密碼雜湊值以加密形式儲存。

本機處理的所有資料只能透過 卡巴斯基安全管理中心 Linux 元件的傾印檔案、偵錯檔案或記錄檔案傳輸至 Kaspersky，包含安裝程式和公用程式建立的記錄檔案。

卡巴斯基安全管理中心 Linux 元件的傾印檔案、偵錯檔案或記錄檔案包含管理伺服器、網路代理和卡巴斯基安全管理中心網頁主控台的任意資料。這些檔案可能包含個人或機密資料。傾印檔案、偵錯檔案或記錄檔案以非加密形式儲存在裝置上。傾印檔案、偵錯檔案或記錄檔案不會自動傳輸到卡巴斯基；但是管理員可以在技術支援要求下手動傳輸資料到卡巴斯基以便解決 卡巴斯基安全管理中心 Linux 效能相關問題。

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。

依照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 Linux 代碼
- 卡巴斯基安全管理中心 Linux 版本
- 卡巴斯基安全管理中心 Linux 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。

關於訂購

*卡巴斯基安全管理中心 Linux 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 Linux 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 Linux，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 Linux 套用不同的啟動碼。

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 Linux 在指定時間間隔自動嘗試存取啟動伺服器，直到訂購到期。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。

啟動 卡巴斯基安全管理中心 Linux

您可以啟動卡巴斯基安全管理中心 Linux 以使用其附加功能。有兩種方法可以完成此工作：使用管理伺服器快速啟動精靈或管理伺服器內容。

要啟動卡巴斯基安全管理中心 Linux：

1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在**一般**頁簽上，選取**產品授權金鑰**區段。

3. 在**目前產品授權**下，按一下**選擇**按鈕。

4. 在開啟的視窗中，選擇要用於啟動卡巴斯基安全管理中心 Linux 的產品授權金鑰。如果產品授權金鑰未列出，請按一下**新增新的產品授權金鑰**按鈕，然後指定新的產品授權金鑰。

5. 如有必要，您也可以新增備用產品授權金鑰。為此，請在**備用產品授權金鑰**下，按一下**選擇**按鈕，然後選擇現有產品授權金鑰或新增產品授權金鑰。請注意，如果沒有啟動的產品授權金鑰，則無法新增備用產品授權金鑰。

6. 點擊**儲存**按鈕。

受管理卡巴斯基應用程式的產品授權

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 Linux 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。您已對所有三個授權金鑰啟用了**自動分發的產品授權金鑰**。卡巴斯基安全應用程式—例如，Kaspersky Endpoint Security for Linux—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：

- 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。

操作說明：新增產品授權金鑰至安裝套件

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：

- 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

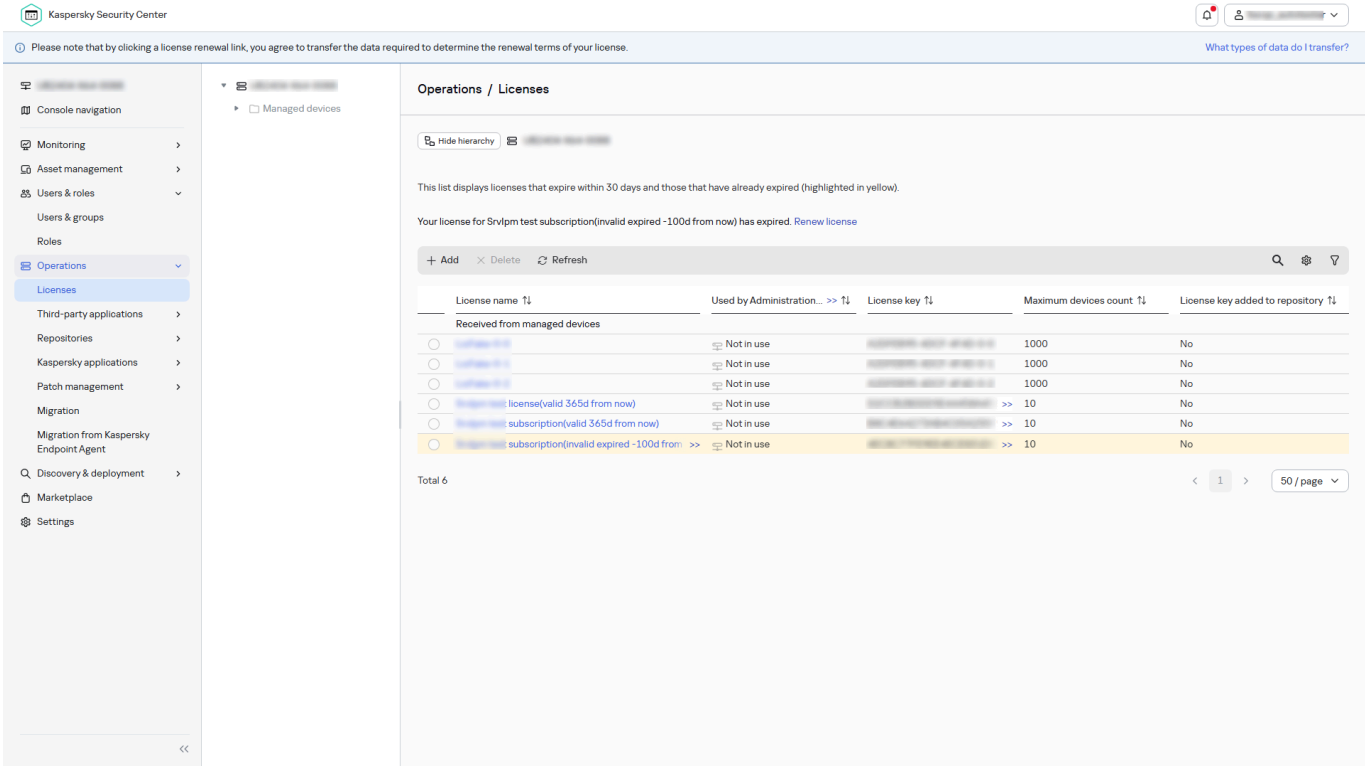
手動新增啟動碼或金鑰檔案至裝置

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**。



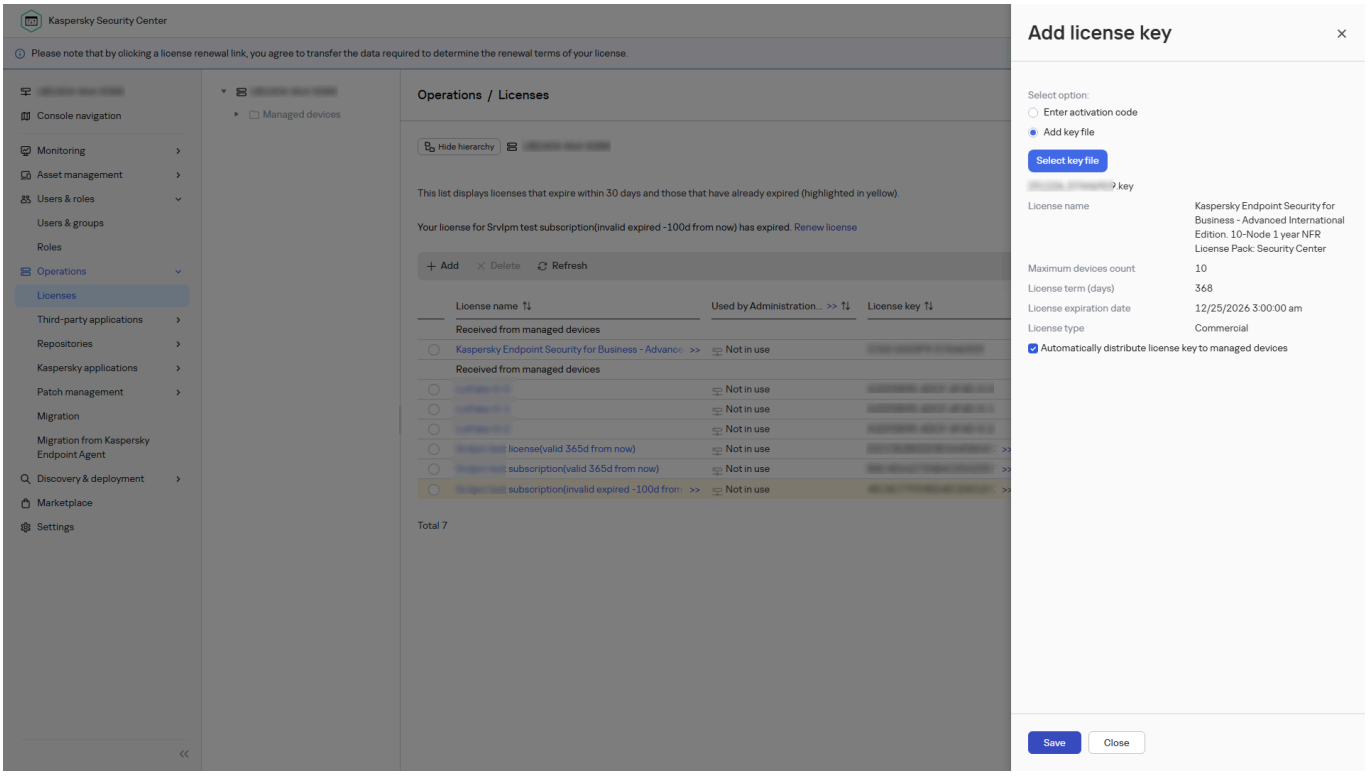
新增的卡巴斯基產品授權金鑰清單

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。



透過套用金鑰檔案新增產品授權金鑰

- **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

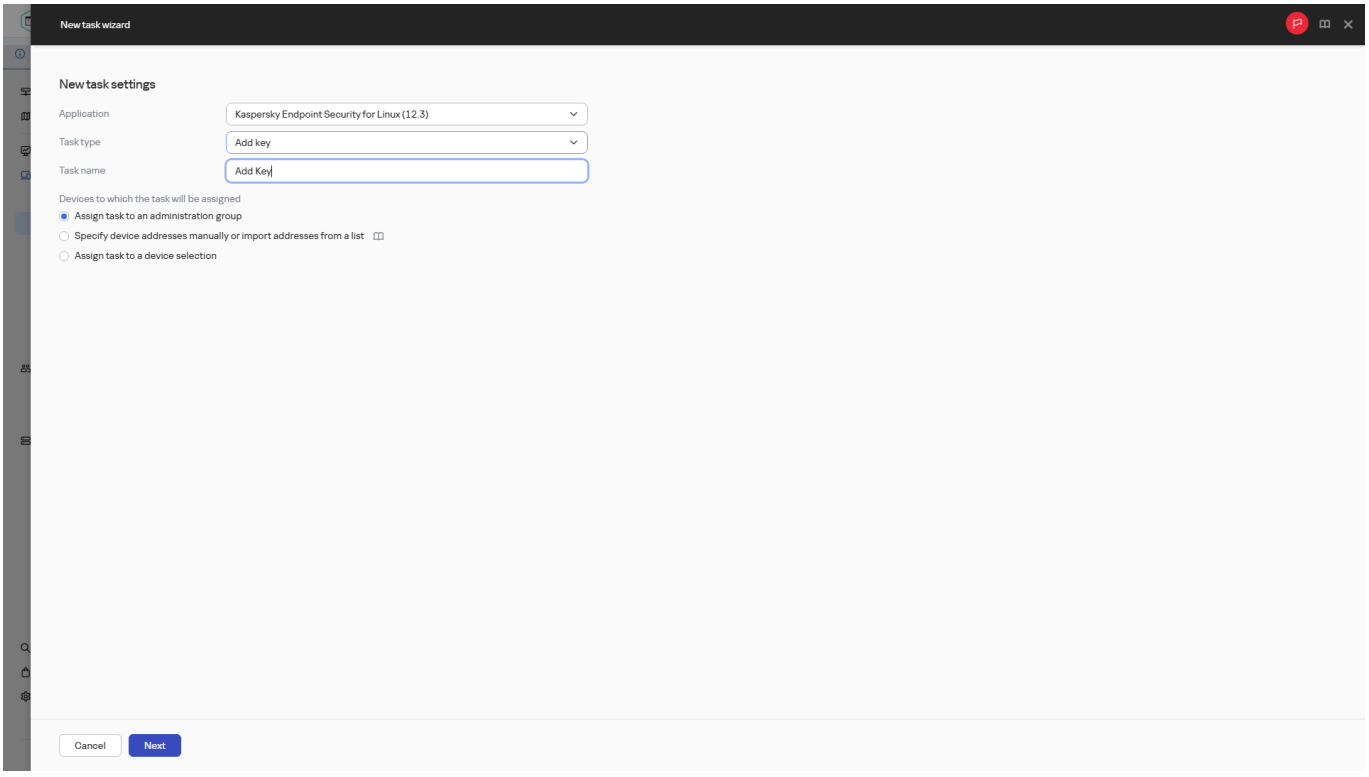
卡巴斯基安全管理中心網頁主控台允許您自動或是透過**應用程式啟動**工作，將產品授權金鑰分發至用戶端裝置。您可以使用該工作將金鑰分發到特定裝置群組。在透過工作分發產品授權金鑰期間，系統不會將產品授權的裝置數量限制納入考慮。使用自動金鑰分發可在達到許可限制時自動停止分發產品授權金鑰。

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。

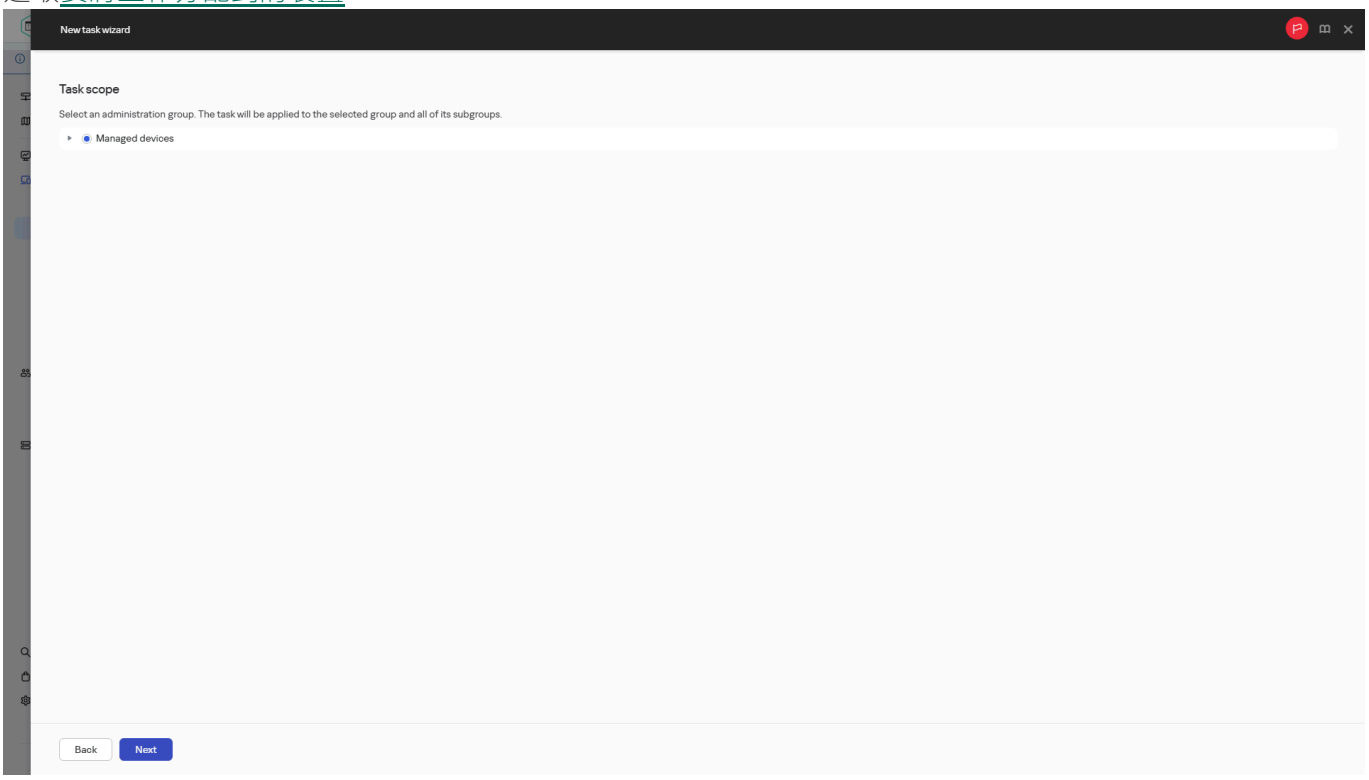
*若要透過**應用程式啟動**工作將產品授權金鑰分發至用戶端裝置：*

1. 在主功能表中，轉至 **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。



建立"新增金鑰"工作

6. 選取要將工作分配到的裝置。



指定工作範圍

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。

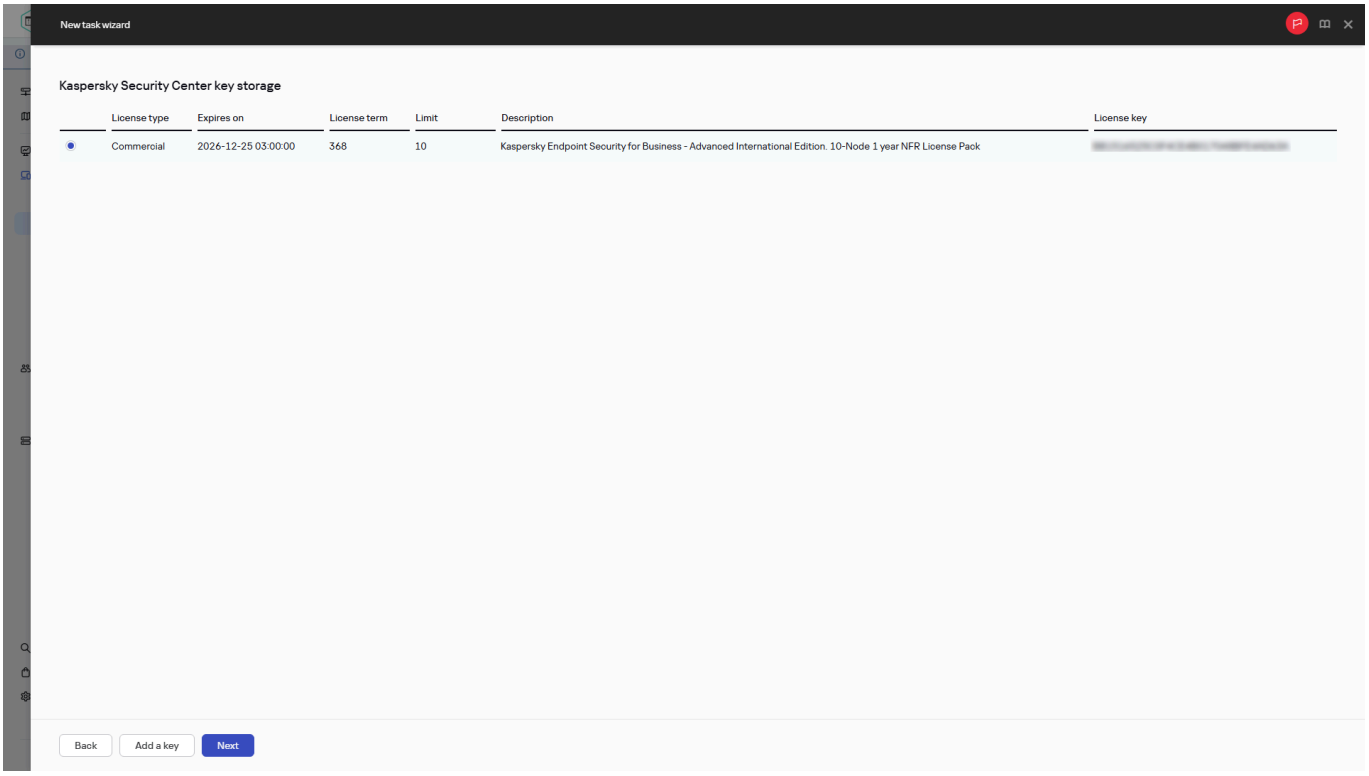
  b. 在開啟的視窗中，選取金鑰檔案，然後點擊**開啟**按鈕。
  產品授權金鑰新增窗格中即會顯示產品授權金鑰的資訊。

  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。

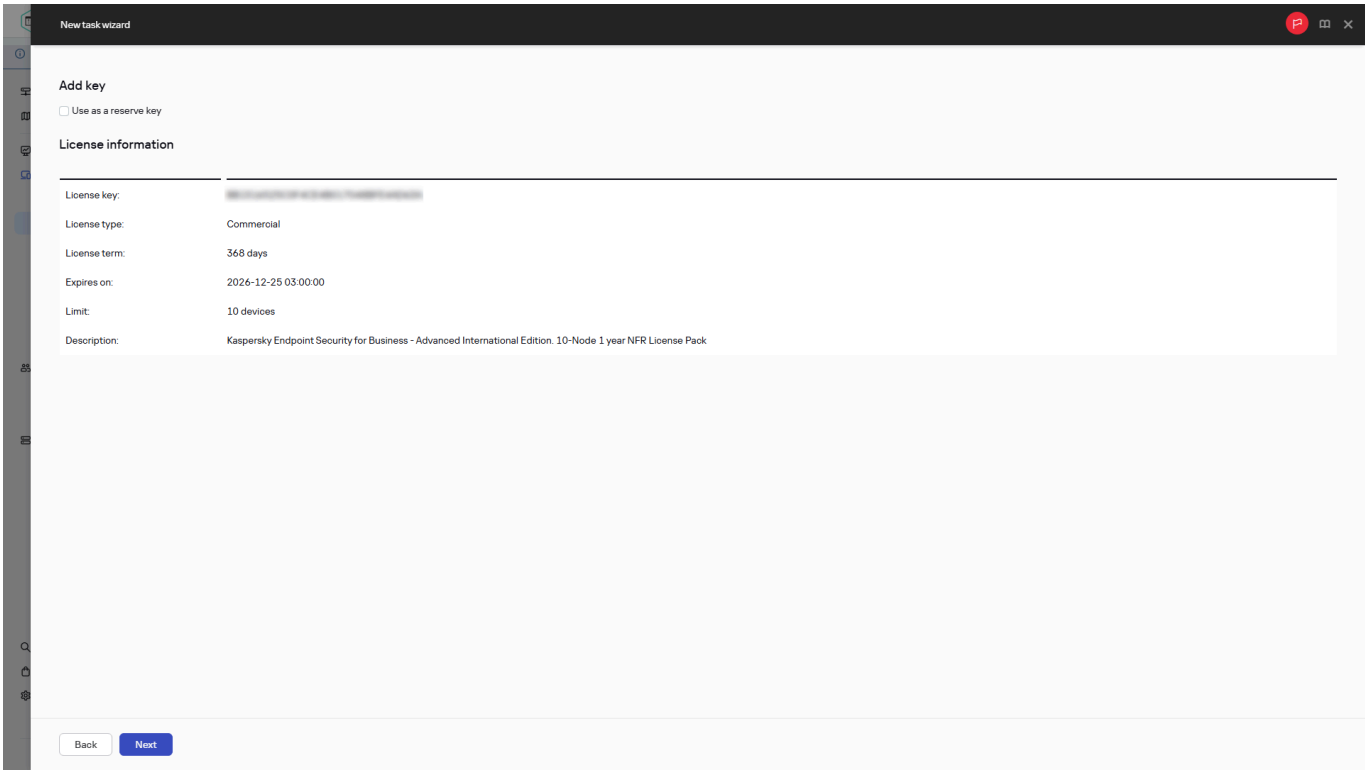


選取產品授權金鑰

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。



指定備用產品授權金鑰

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。

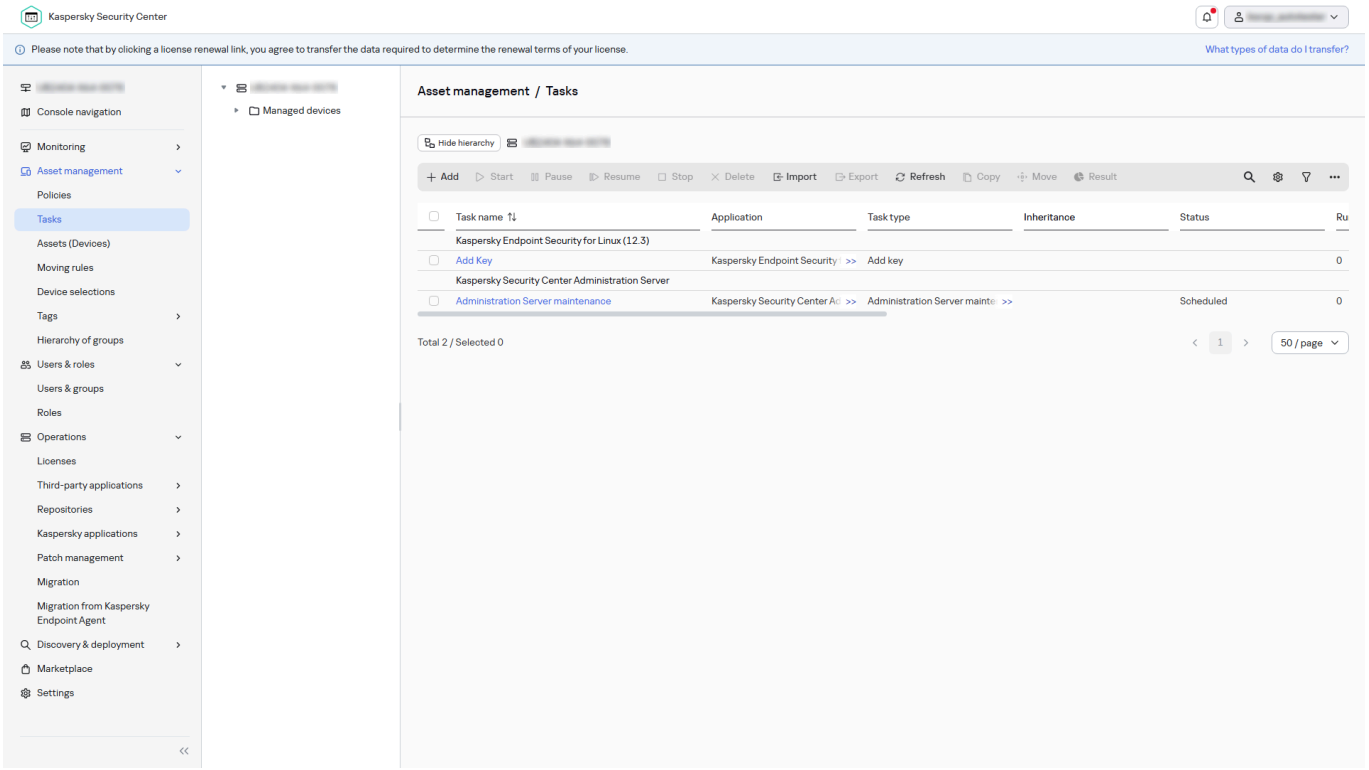
    如果您不啟用該選項，工作將以預設設定來建立。您可以稍後再修改預設設定。

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。



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。

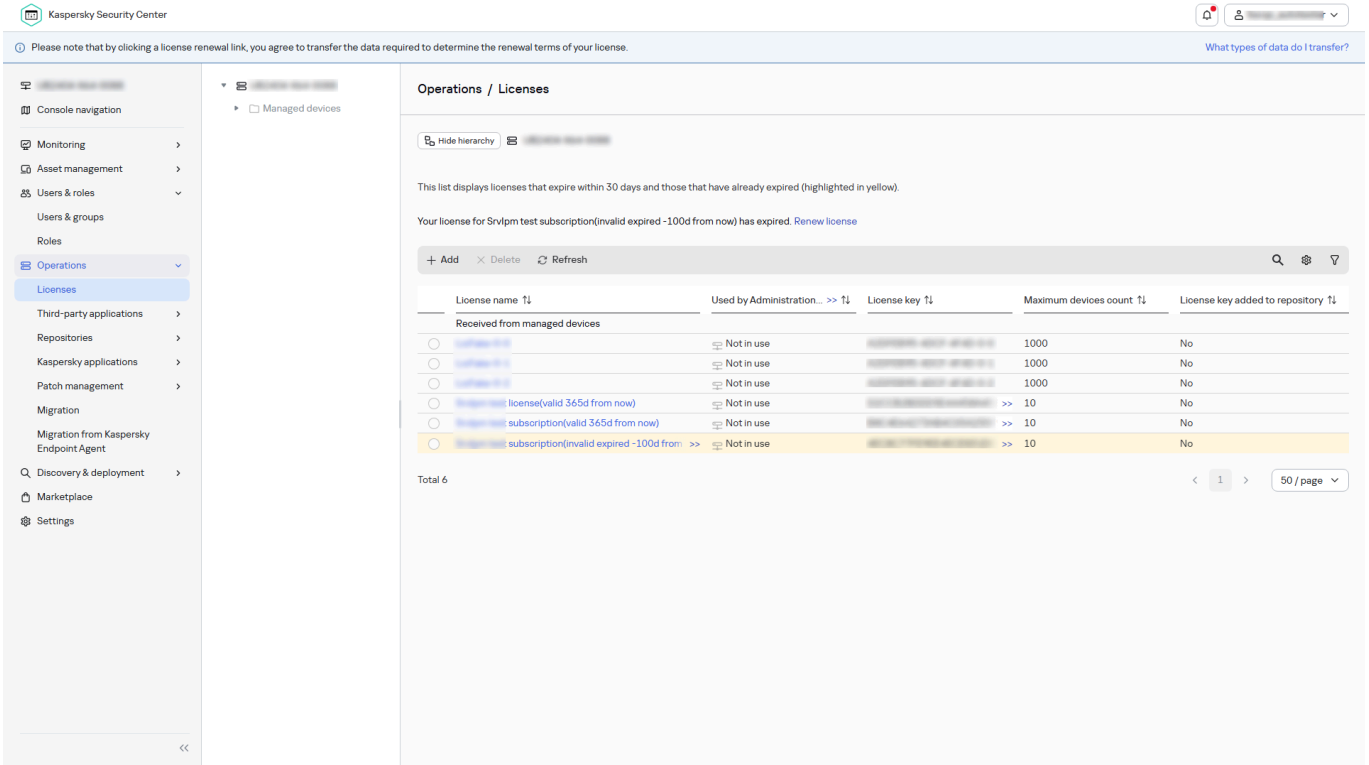
工作完成後，產品授權金鑰即會佈署到所選裝置。

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 Linux 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：

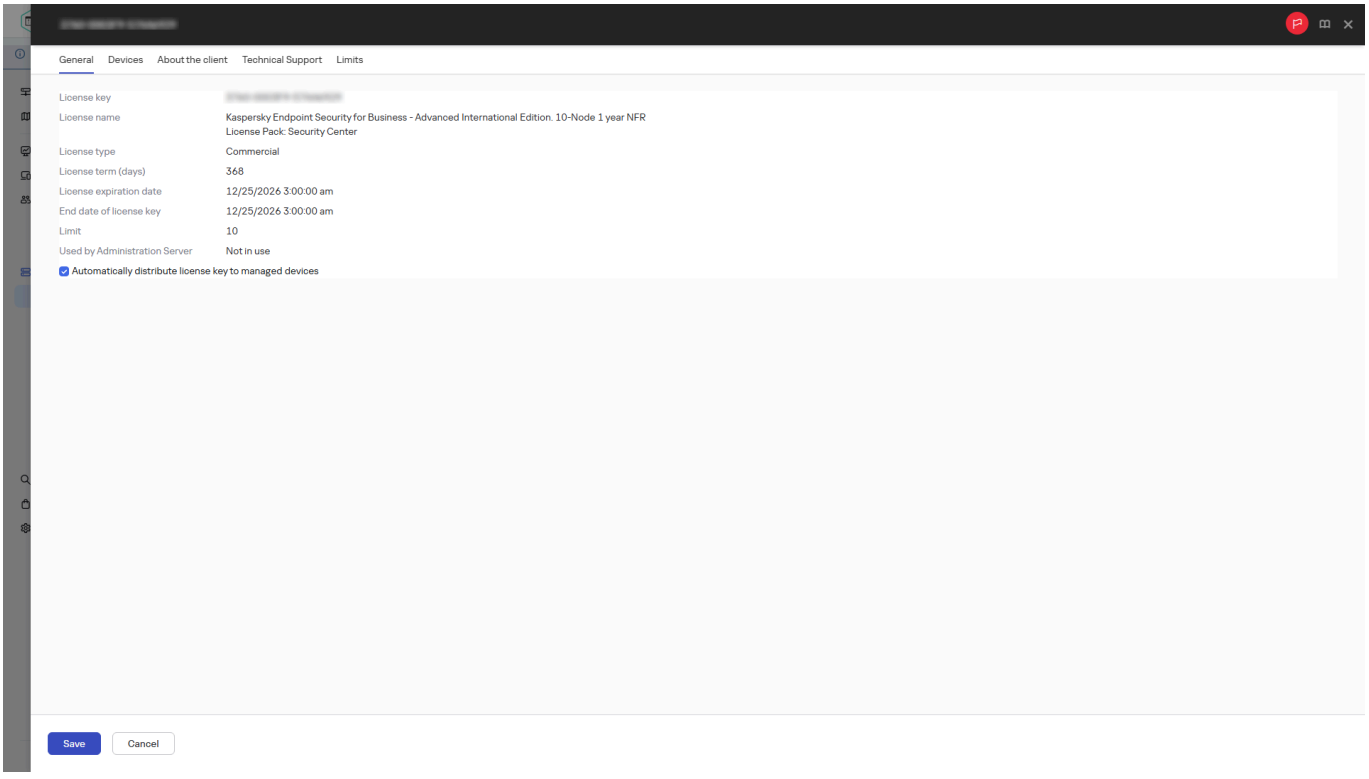
1. 在主功能表中，轉至 **操作 → 產品授權 → 產品授權**。



產品授權清單

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。



產品授權金鑰內容視窗

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** → **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** → **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
- 在**限制**頁簽上 — 產品授權限制清單

  如果您在 Kaspersky Next XDR Optimum 產品授權下啟動了管理伺服器，則**限制** 頁簽會顯示具有**已啟用**值的 **XDR-O**欄位。

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 **資產管理 → 資產（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。

產品授權超限事件

Kaspersky Security Center for Linux允許您獲取用戶端裝置上安裝的卡巴斯基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。

從儲存區刪除產品授權金鑰

當您刪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刪除金鑰檔案或啟動碼：

1. 檢查管理伺服器並未使用您要刪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，您將無法刪除該金鑰。若要執行檢查：

   a. 在主選單中，按一下管理伺服器名稱。

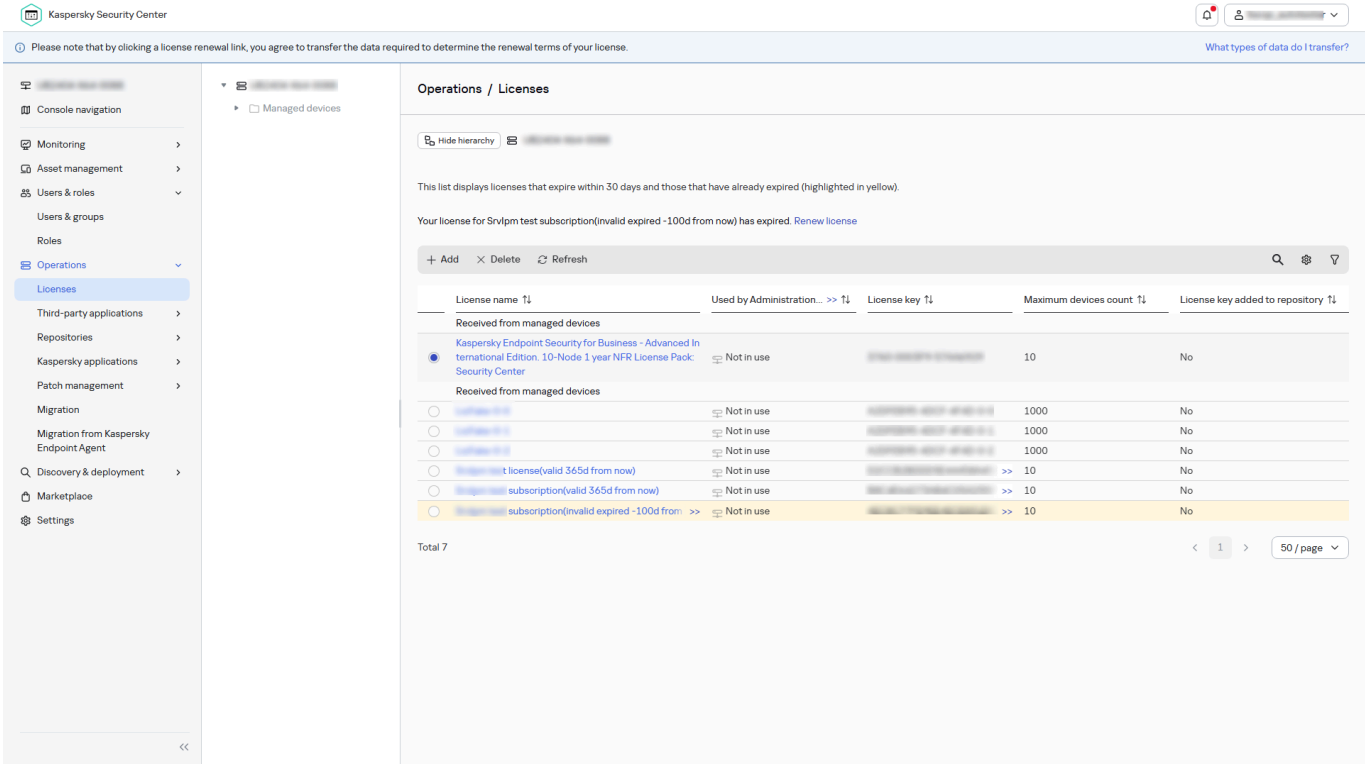
      管理伺服器內容視窗將開啟。

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**刪除生效的產品授權金鑰**按鈕，然後確認操作。在此之後，管理伺服器將不會使用刪除的產品授權金鑰，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** → **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。



產品授權清單

選取的金鑰檔案或啟動碼已從儲存區刪除。

您可以再次新增一個已刪除的產品授權金鑰或新增一個新產品授權金鑰。

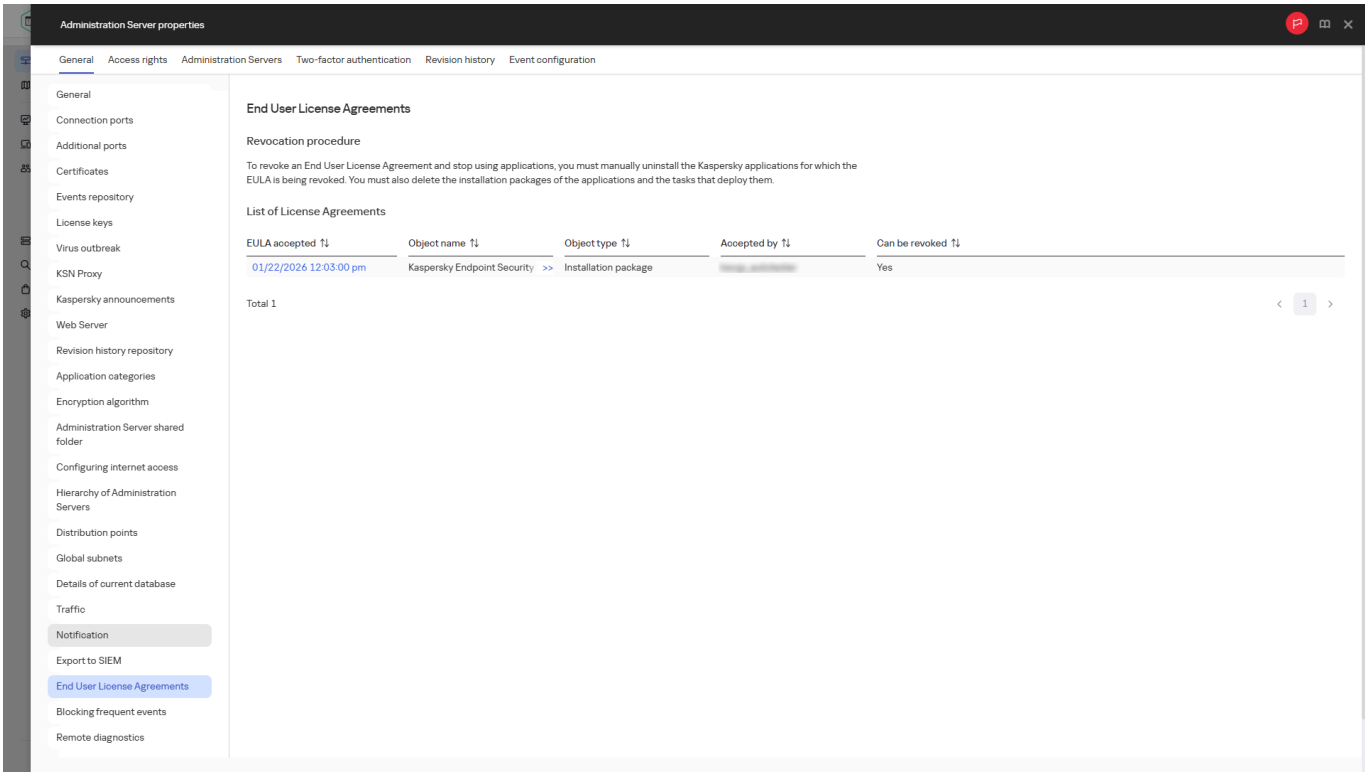
撤銷最終使用者產品授權協議的許可

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。

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。



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** → **產品授權**。
   - 在主功能表中，轉到**監控** → **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。

   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 Linux 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 Linux 會將您重新導向到卡巴斯基網站上的相關網頁，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。

配置卡巴斯基應用程式

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，甚至不受允許。因此，建議您微調這些政策與工作，然後視您網路的需要，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 Linux 管理伺服器
- 已安裝卡巴斯基安全管理中心 網頁主控台
- 已完成 卡巴斯基安全管理中心 Linux 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

階段

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。這兩種方法也可以並用。

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。

   操作說明：設定用於更新 Kaspersky Endpoint Security 的群組工作、建立「弱點掃描和所需更新」工作。

   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。

   操作說明：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。

當網路防護設定完成時，您可以繼續為 Kaspersky 資料庫和應用程式設定定期更新。

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一種或其組合。

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。

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，您可以應用特定的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問題時。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 Linux 管理伺服器和卡巴斯基安全管理中心網頁主控台。您也可能要考慮以使用者為中心的安全管理作為以用於以裝置為中心的方法的附加選項。瞭解更多兩個管理方法的詳情。

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 Linux 會為以下應用程式建立預設政策。

   - Kaspersky Endpoint Security for Linux—適用於 Linux 用戶端裝置
   - Kaspersky Endpoint Security for Windows—適用於 Windows 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。

   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. **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套用不同的政策設定檔（例如）具有特別硬體設定或被特別標籤標記的裝置。使用標籤篩選滿足特別標準的裝置。例如，您可以建立叫做 *CentOS* 的標籤，使用該標籤標記所有執行 CentOS 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，安裝在所有執行 CentOS 裝置上的卡巴斯基應用程式將被使用它們自己的政策設定檔管理。

   說明：

   - 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。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 Linux 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。

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 Linux 管理伺服器和卡巴斯基安全管理中心網頁主控台，並完成主要佈署情境。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 Linux 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。

   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**

   預設下，卡巴斯基安全管理中心 Linux 每 15 分鐘自動同步管理伺服器與受管理裝置。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 Linux 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。

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*是一組應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：

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。
- 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：

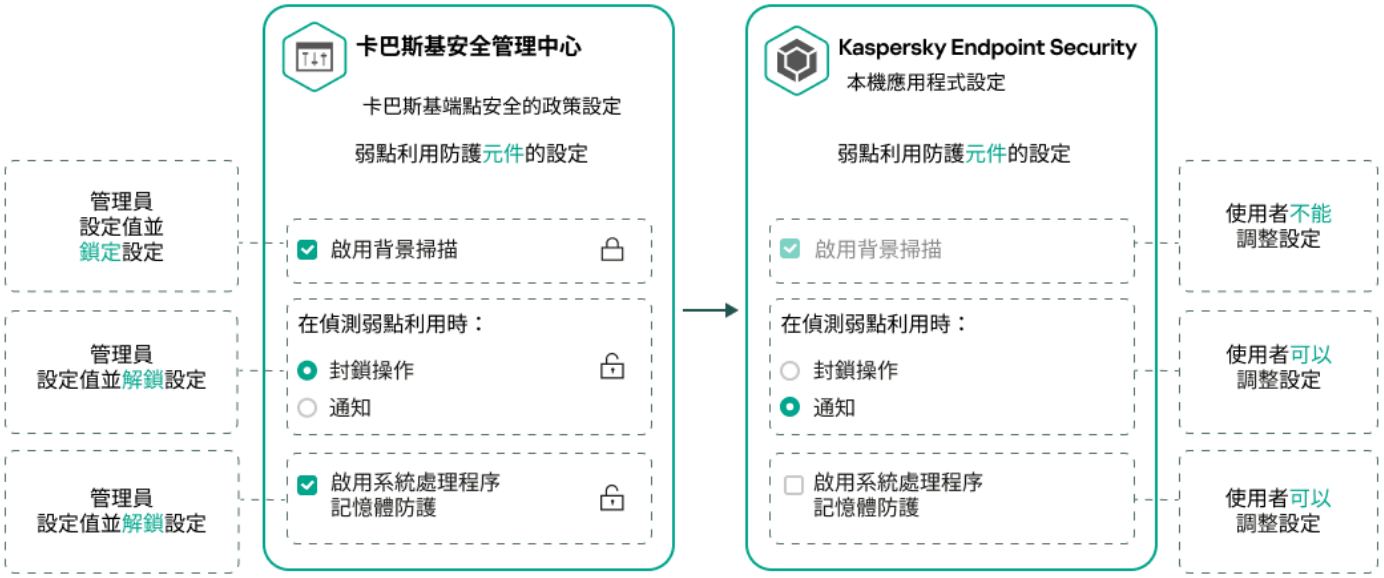
- 鎖定管理子群組政策的設定
- 在受管理裝置上鎖定卡巴斯基應用程式的設定

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

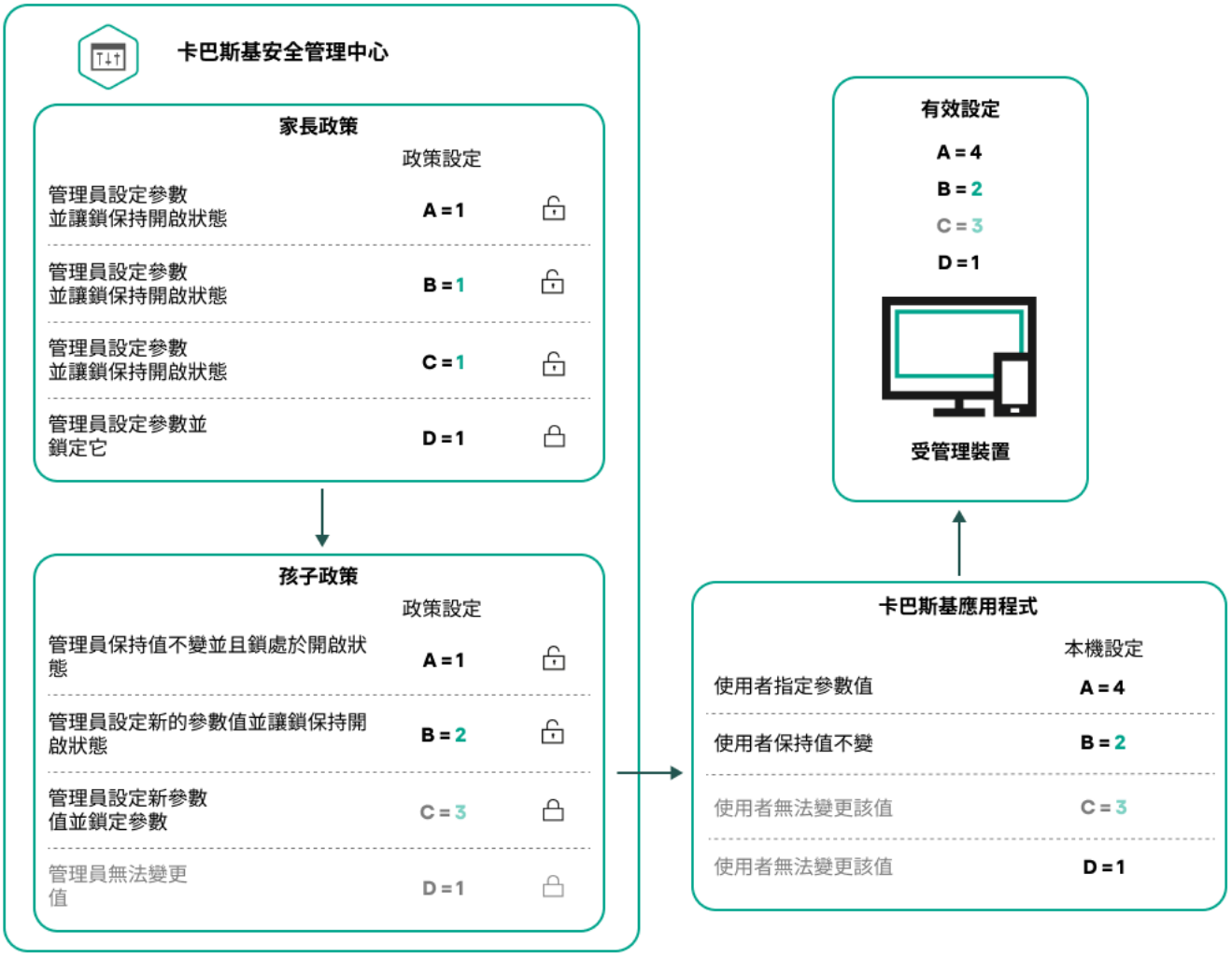
如果不同的裝置需要不同的設定，則可以將裝置組織到管理群組中。

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）。

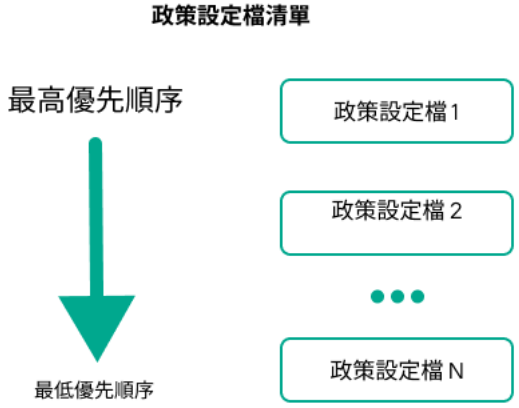


政策層級

政策層次結構中的政策設定檔

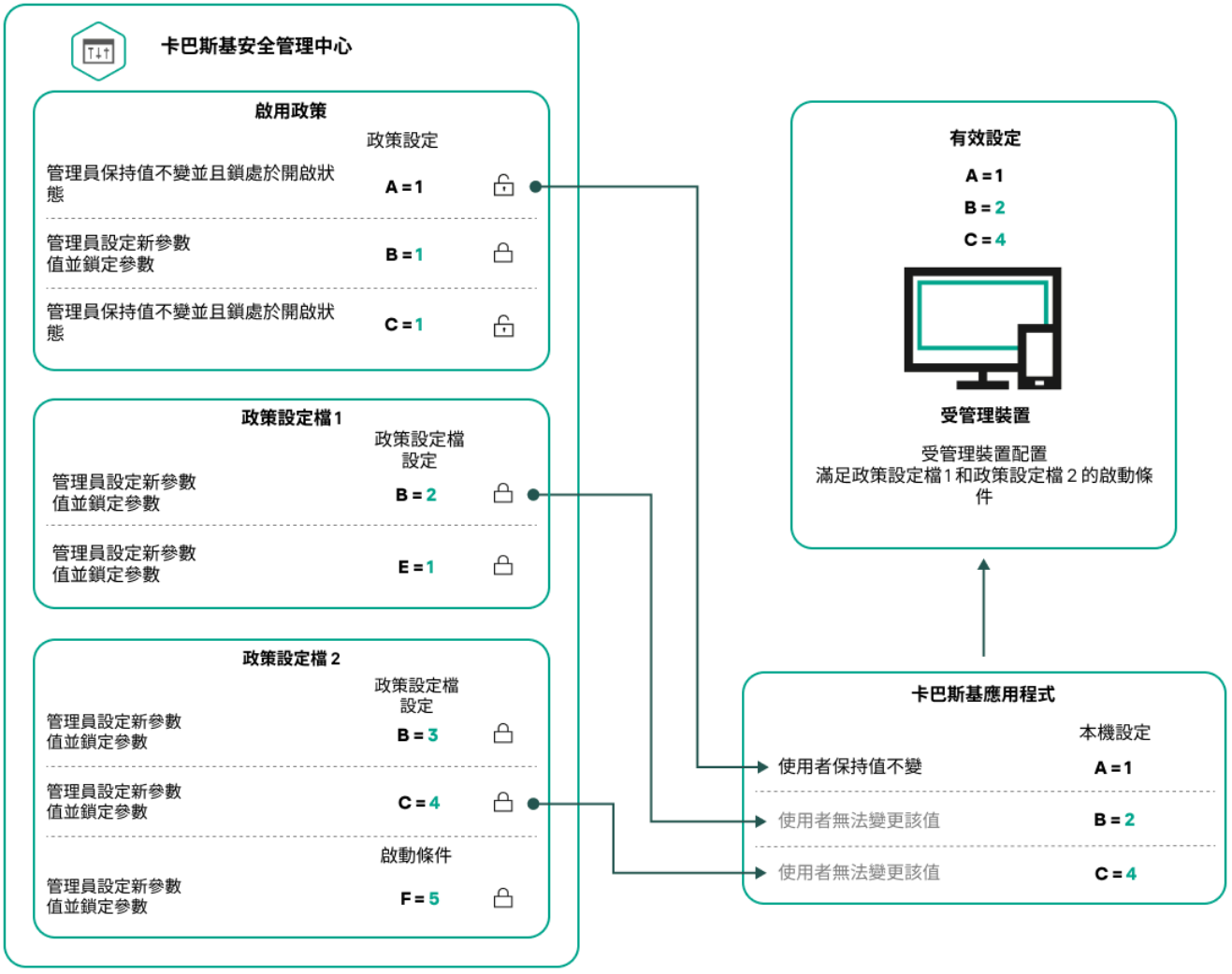
政策設定檔具有以下優先等級分配條件：

- 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）。

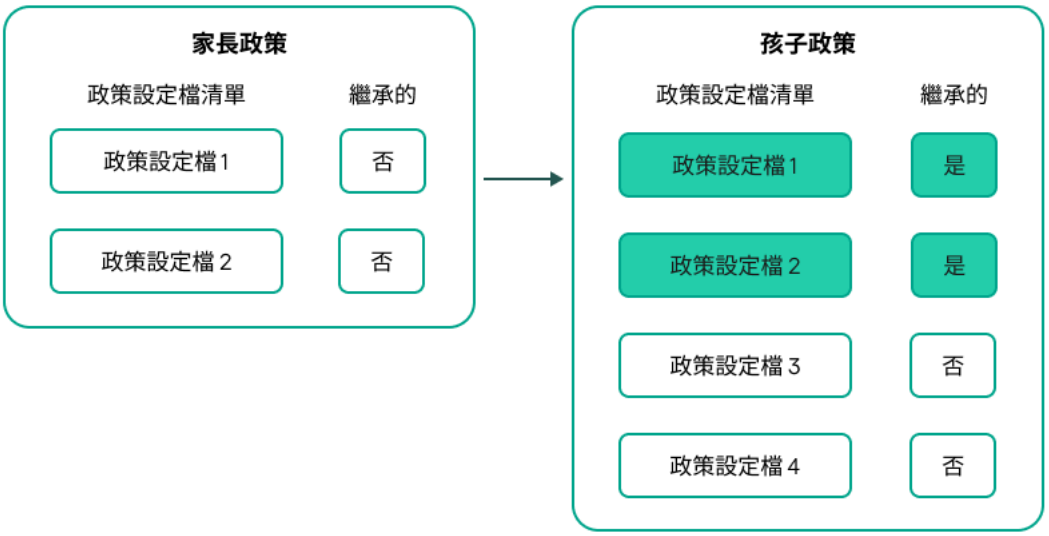


受管理裝置配置滿足幾個政策設定檔的啟動條件

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）。

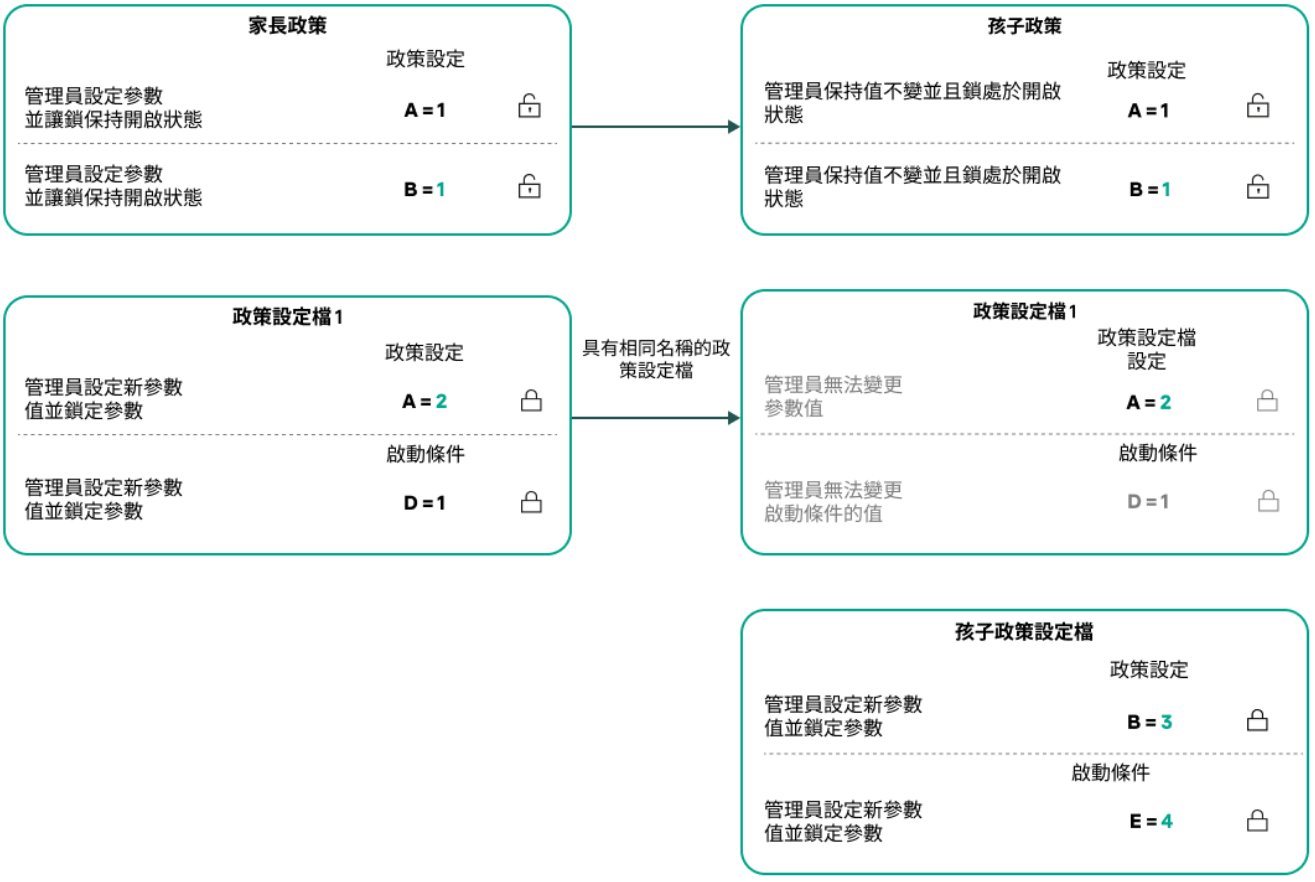


政策設定檔繼承

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 **資產管理 → 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：

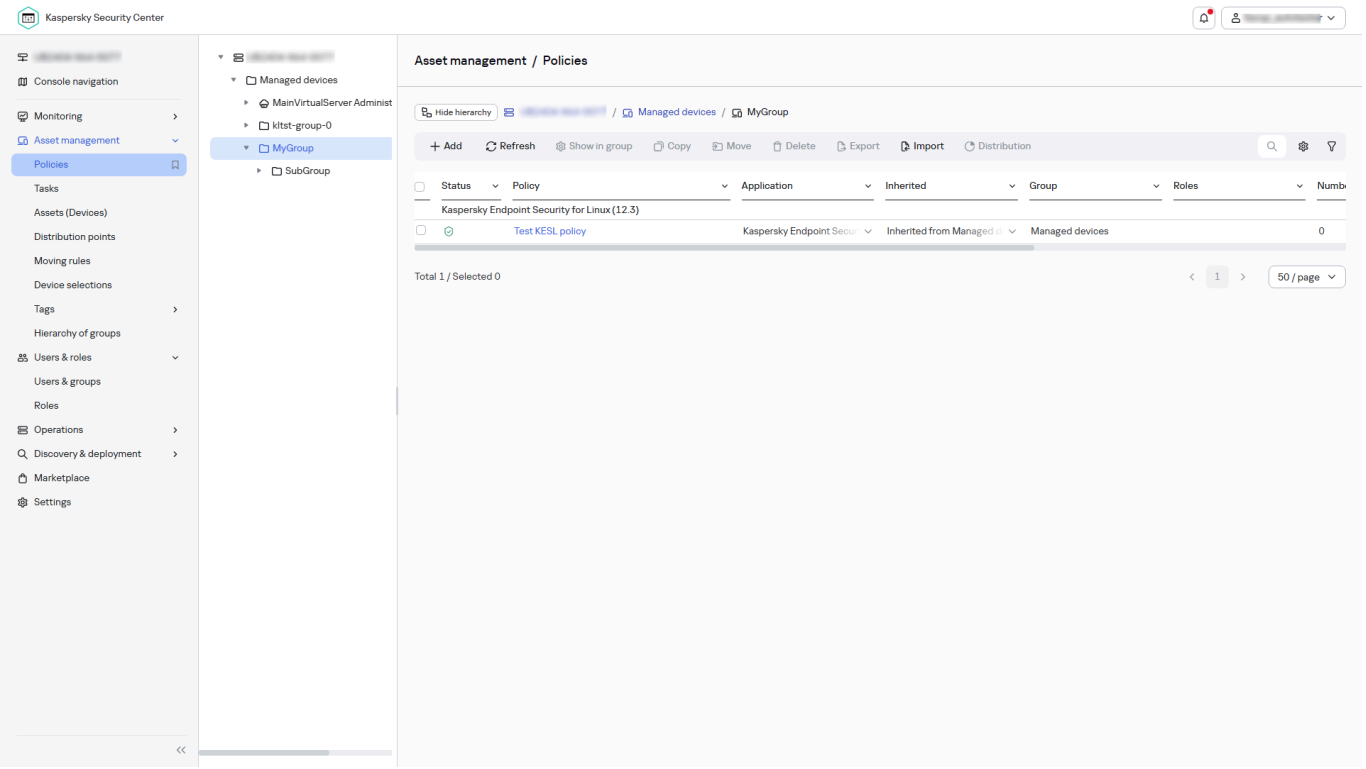
1. 在主功能表中，轉至 **資產管理 → 政策**。
2. 選擇要為其建立政策的管理群組：
   - 對於根群組。

     在這種情況下，您可以繼續執行下一步。
   - 對於子群組：
     a. 點擊頁面頂部的**顯示階層**按鈕。

        按鈕名稱將變更為**隱藏階層**。

     b. 在開啟的視窗中，按一下所需子群組的名稱。

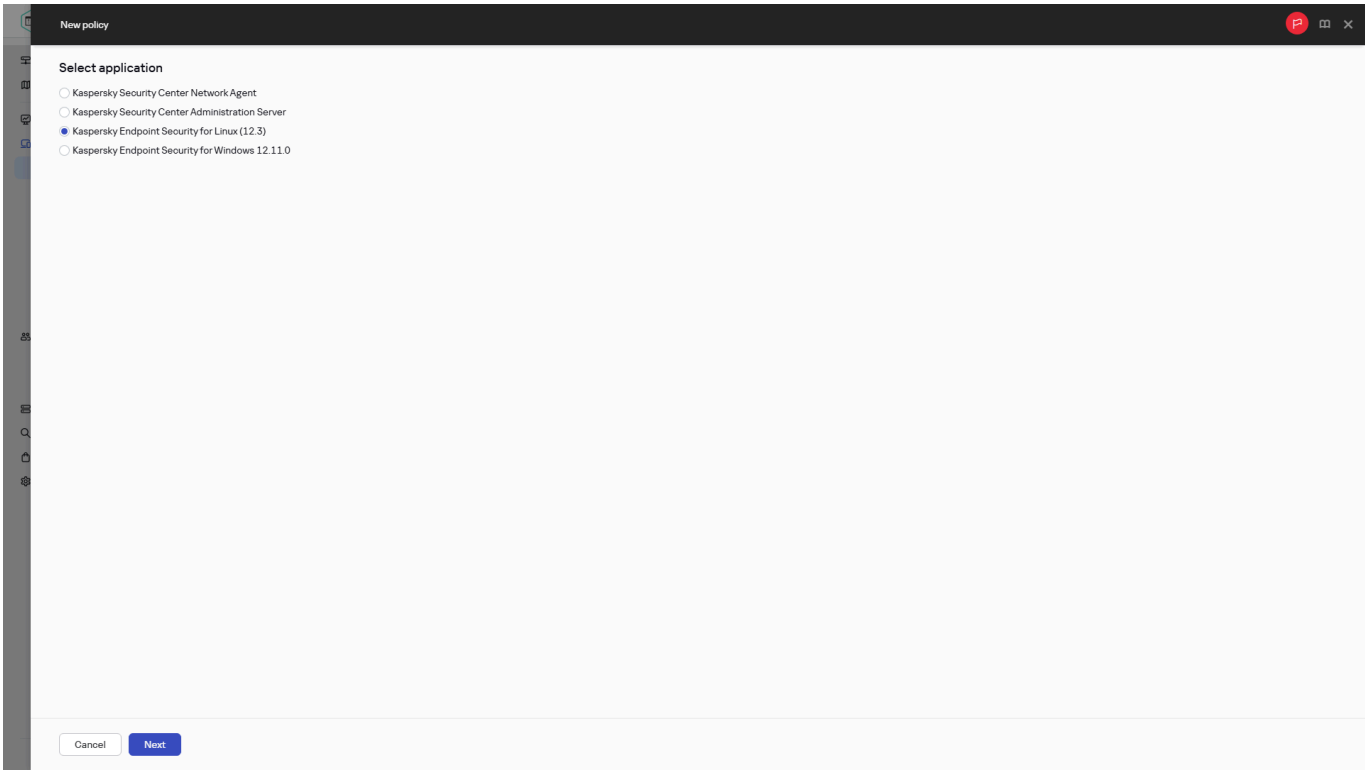
所選群組的路徑將顯示在頁面頂部。如果需要，您可以點擊帶有管理群組名稱的連結進入該群組。預設情況下，路徑中的最後一個連結不活動。您也可以點擊**隱藏階層**按鈕關閉層次結構視窗。



政策清單

3. 點擊**新增**。

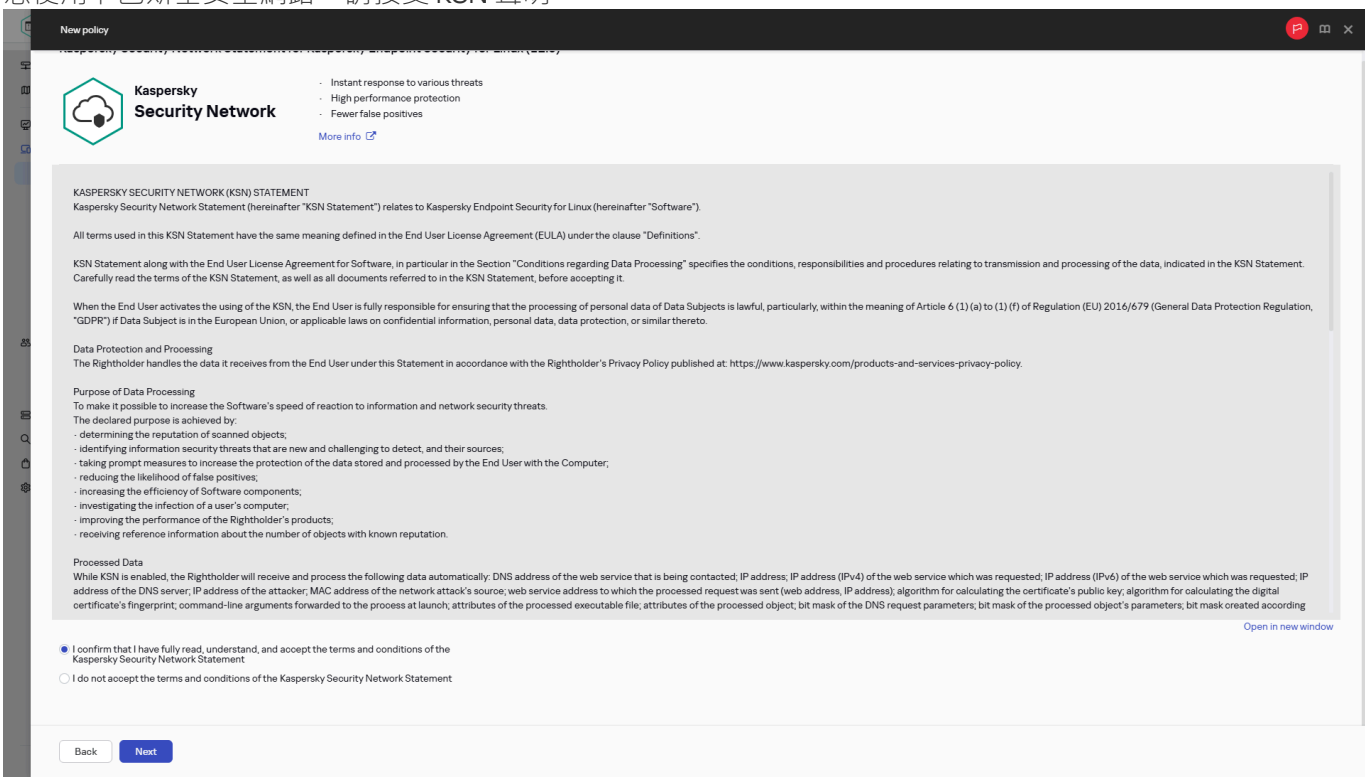
選取應用程式視窗將開啟。



建立新政策

4. 選取您要建立政策的應用程式。

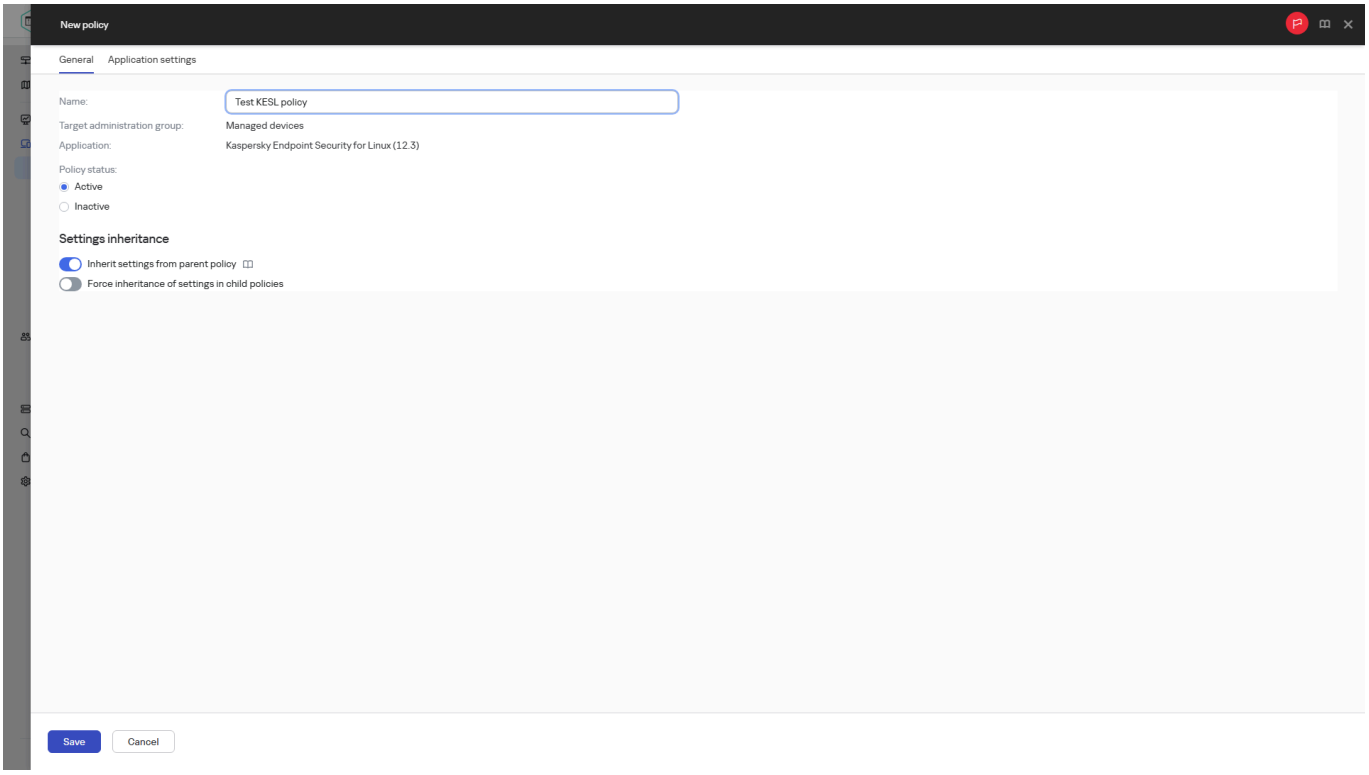
5. 如果您正在為其建立政策的卡巴斯基應用程式支援卡巴斯基安全網路，系統將提示您接受 KSN 聲明。如果您想使用卡巴斯基安全網路，請接受 KSN 聲明。



接受 KSN 聲明

6. 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。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。



新政策設定視窗

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 Linux 說明
   - Kaspersky Endpoint Security for Windows 說明

   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。

   系統會顯示包含以下訊息的通知：**正在儲存政策並透過管理伺服器階層分發**。

   如果政策通過驗證，則會顯示以下通知：**政策已儲存**。

   如果政策驗證失敗，則會顯示以下通知：**無法儲存政策 並透過管理伺服器階層分發。請聯絡技術支援**。您可以檢閱並修訂政策設定，然後再試一次。如果問題持續存在，請聯絡技術支援。

該政策將顯示在政策清單中。政策建立後，如果已啟用此選項，政策變更事件會匯出至 SIEM 系統。

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。

事件組態

事件組態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**
  - **儲存在裝置上的作業系統事件記錄中**
  - **儲存在管理伺服器上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：
  - **透過電子郵件通知**
  - **透過 SMS 通知**
  - **透過執行可執行檔或指令碼來進行通知**
  - **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。

此外，當新增新的事件類型（例如，在新版本的應用程式中）時，**事件組態**頁簽會顯示通知，並允許您透過點擊**儲存** 或**儲存並關閉**按鈕來套用新設定。

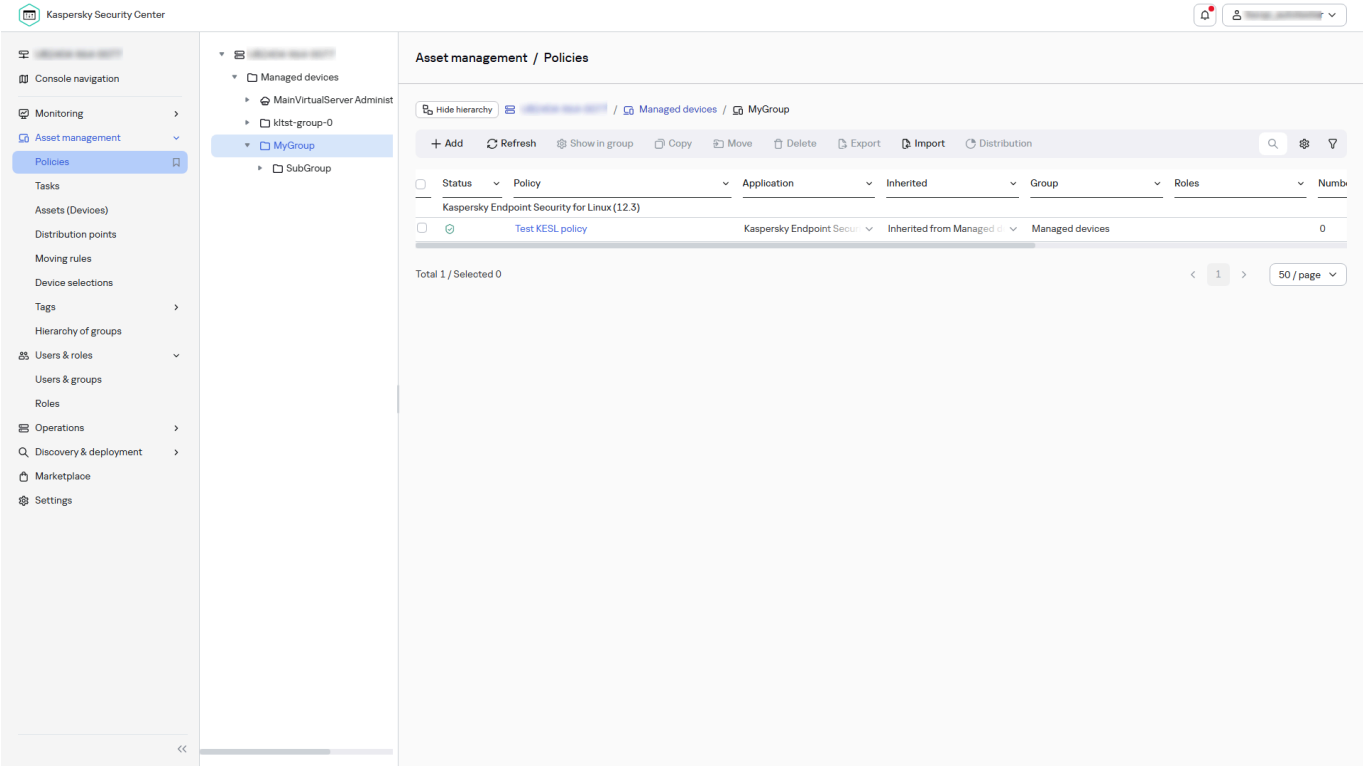
變更歷史

變更歷史頁籤允許您檢視政策修訂版本的清單，比較政策修訂版本，並在必要時恢復對政策所做的變更。

修改政策

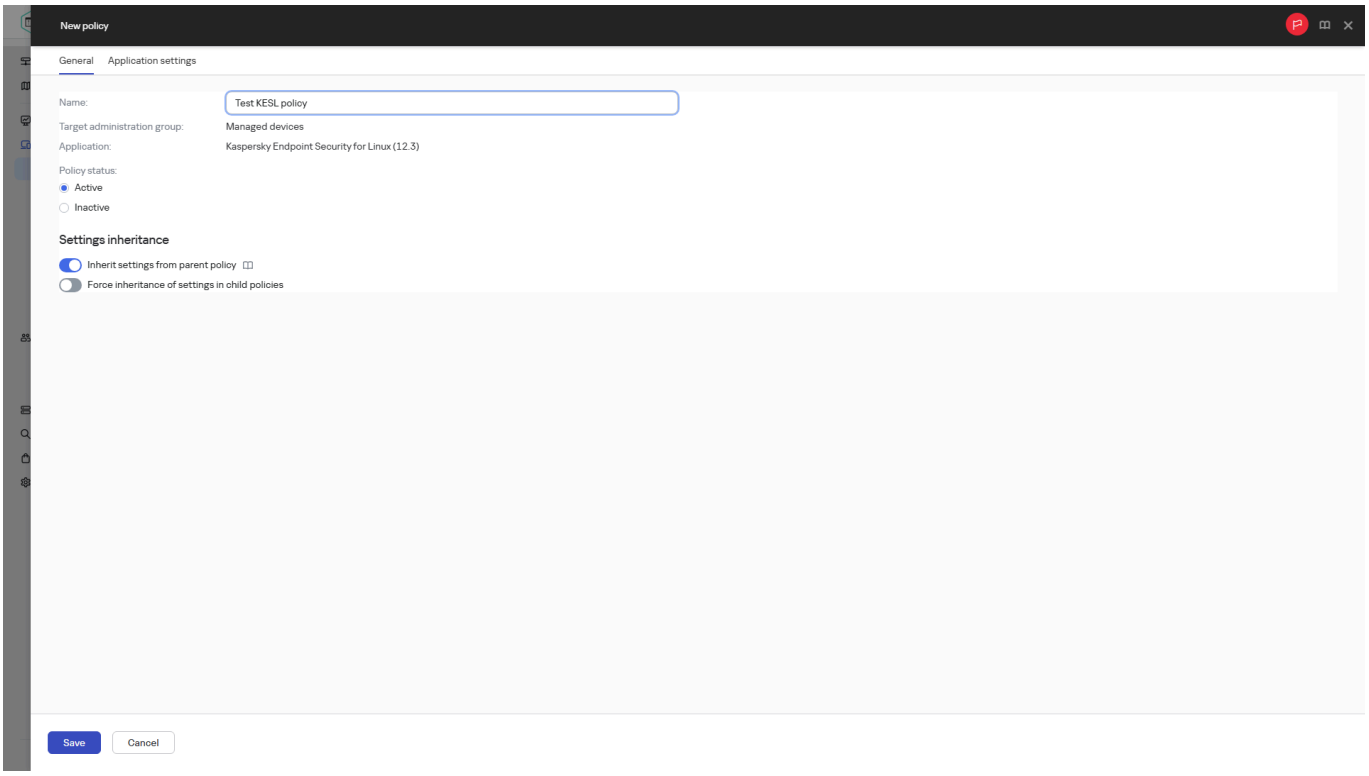
要修改政策：

1. 在主功能表中，轉至 **資產管理** → **政策**。



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 Linux 說明
   - Kaspersky Endpoint Security for Windows 說明

   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**。

   系統會顯示包含以下訊息的通知：**正在儲存政策並透過管理伺服器階層分發**。

   如果政策通過驗證，則會顯示以下通知：**政策已儲存**。

   如果政策驗證失敗，則會顯示以下通知：**無法儲存政策 並透過管理伺服器階層分發。請聯絡技術支援**。您可以檢閱並修訂政策設定，然後再試一次。如果問題持續存在，請聯絡技術支援。

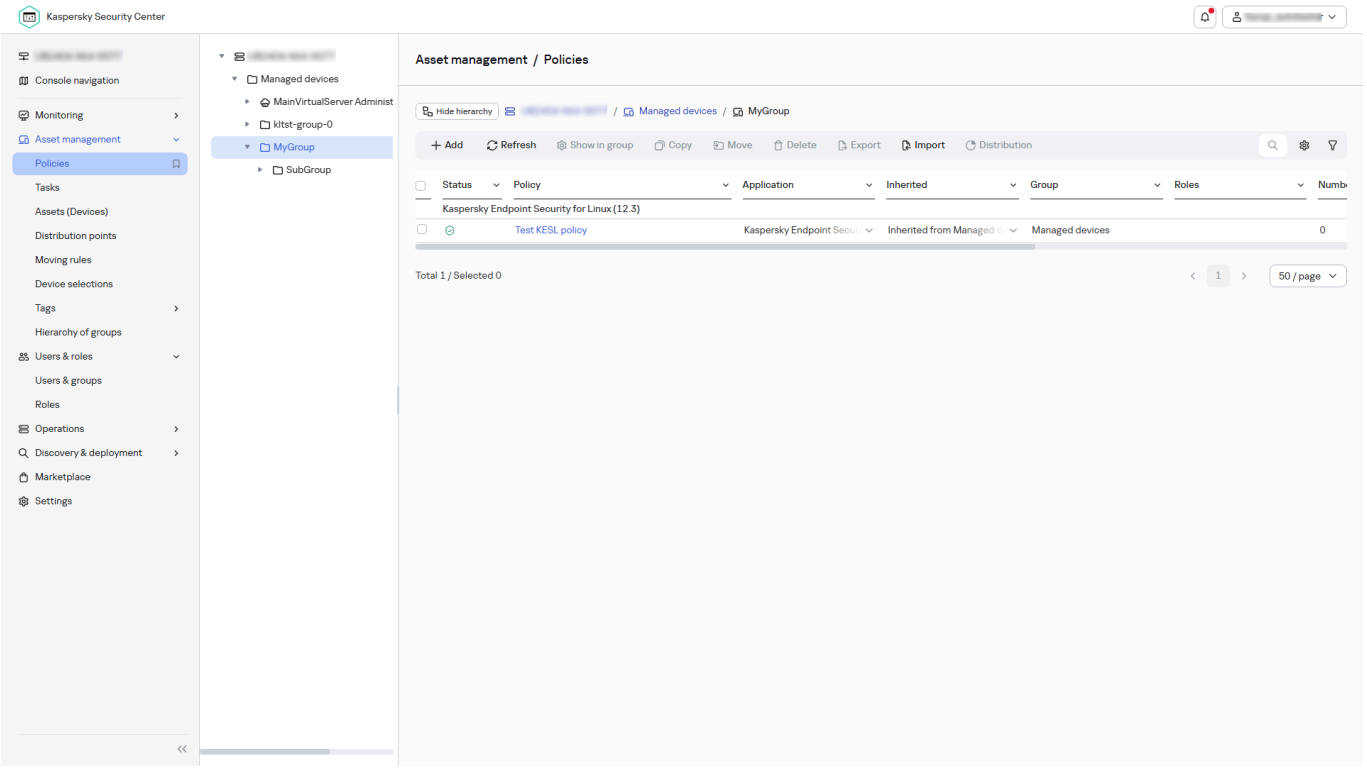
   對政策所做的變更將儲存在政策內容中，並且會顯示在**變更歷史**區段。修改政策後，如果已啟用此選項，政策變更事件會匯出至 SIEM 系統。

如有必要，您可以比較政策修訂版本。此選項適用於管理伺服器、網路代理程式、Kaspersky Endpoint Security for Windows（從14.0網頁外掛程式版本開始）和 Kaspersky Endpoint Security for Mac（從12.2.1 Patch A網頁外掛程式版本開始）。

啟用和停用政策繼承選項

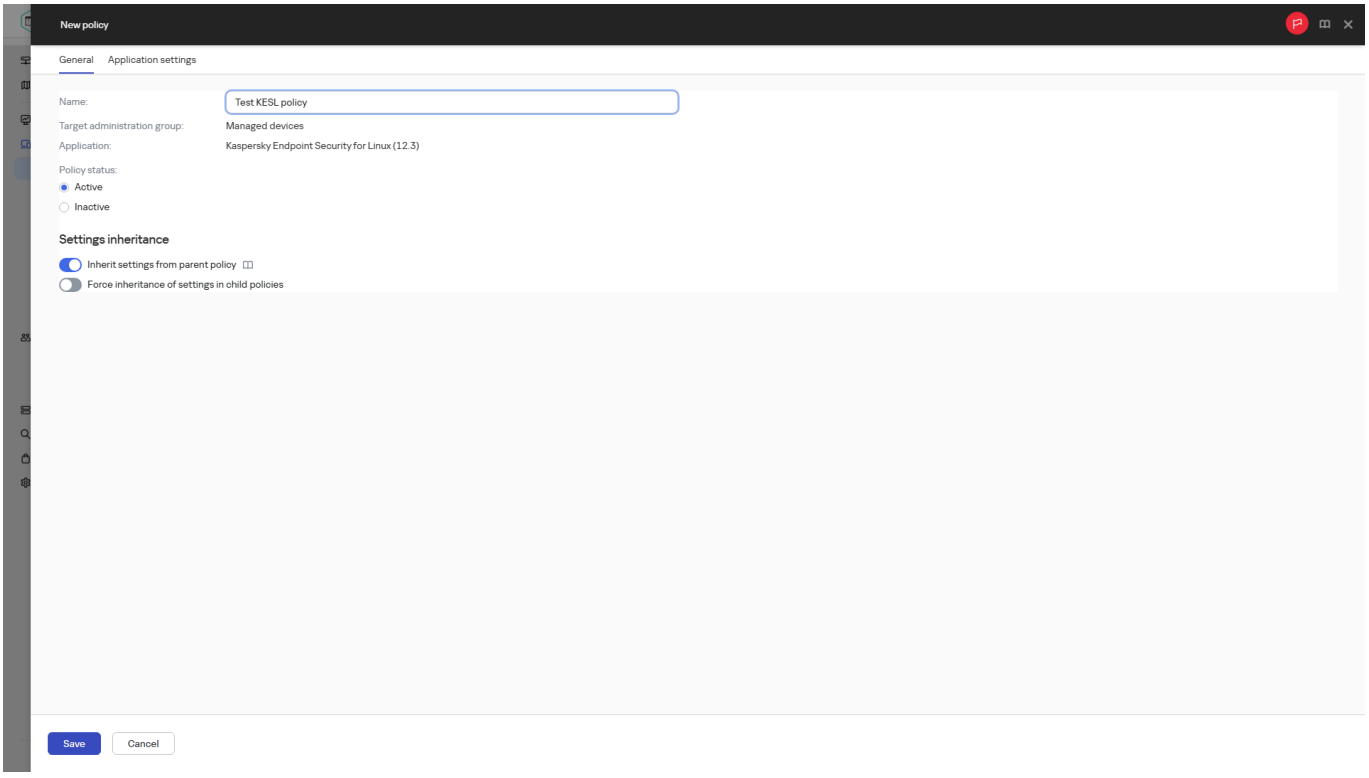
若要啟用或停用政策中的繼承選項：

1. 開啟所需的政策。



政策清單

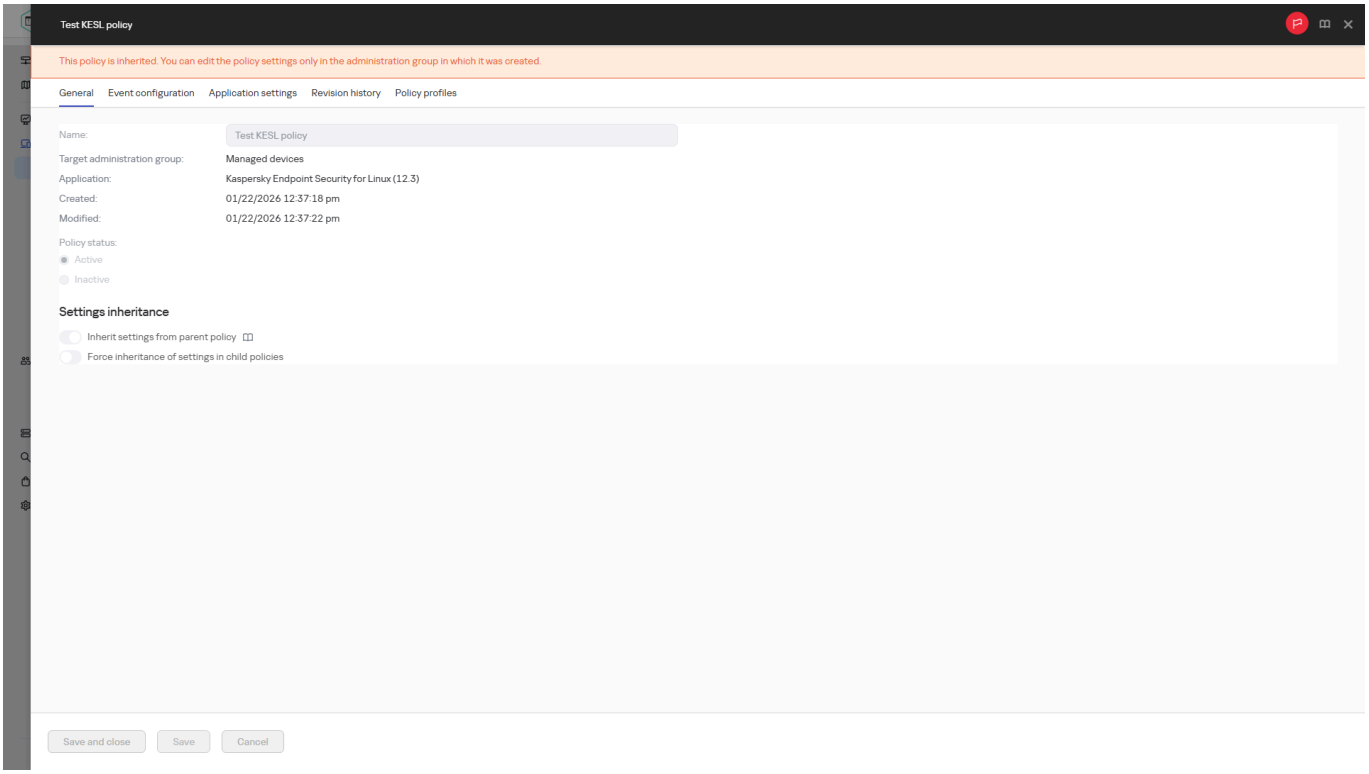
2. 開啟**一般**標籤。



建立新政策

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。



鎖定的政策設定

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。

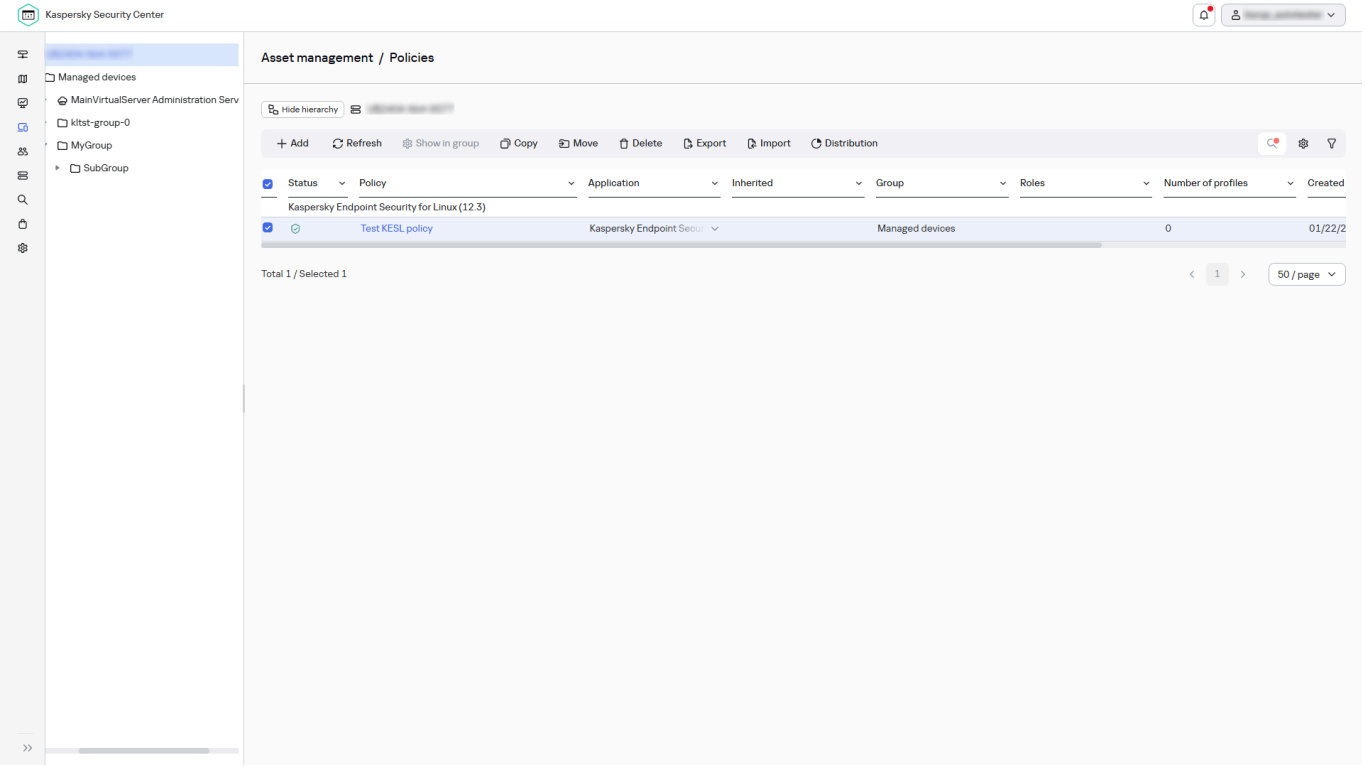
複製政策

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：

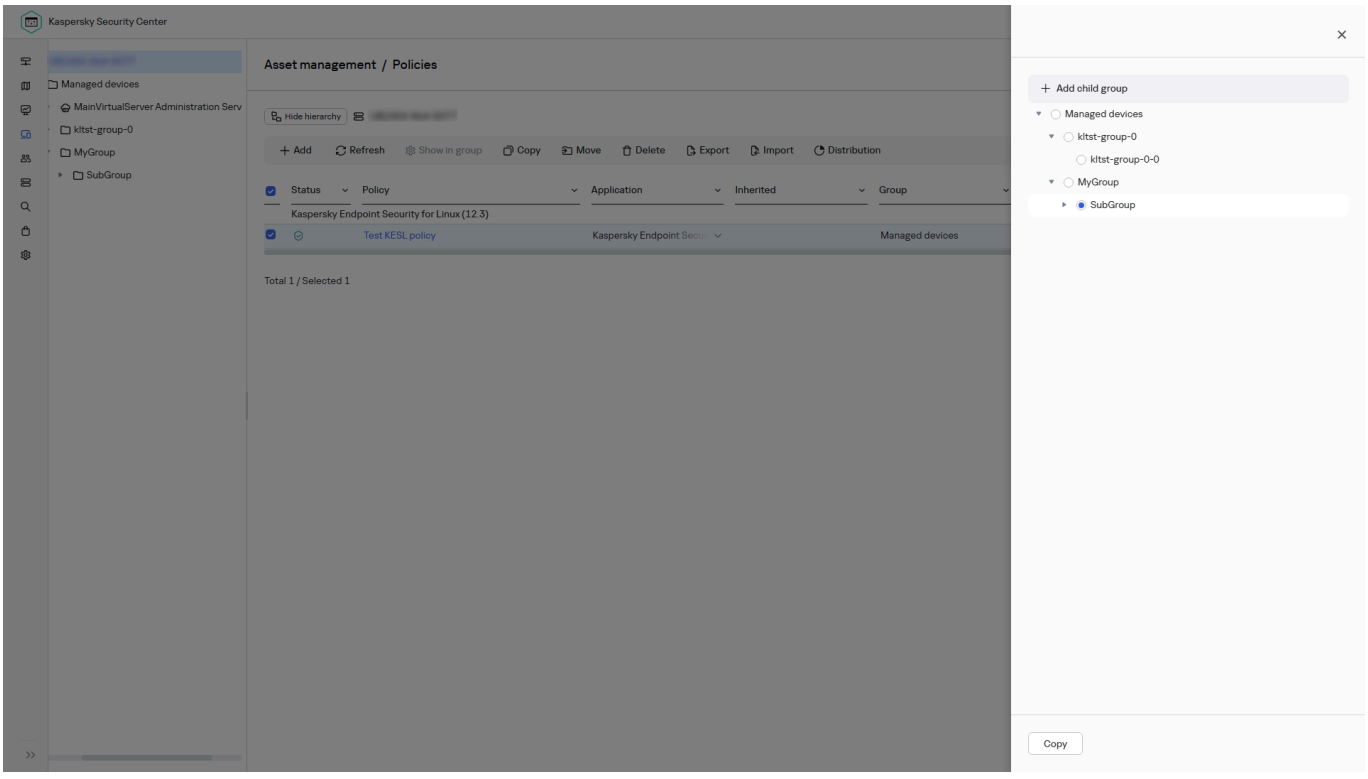
1. 在主功能表中，轉至 **資產管理** → **政策**。

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

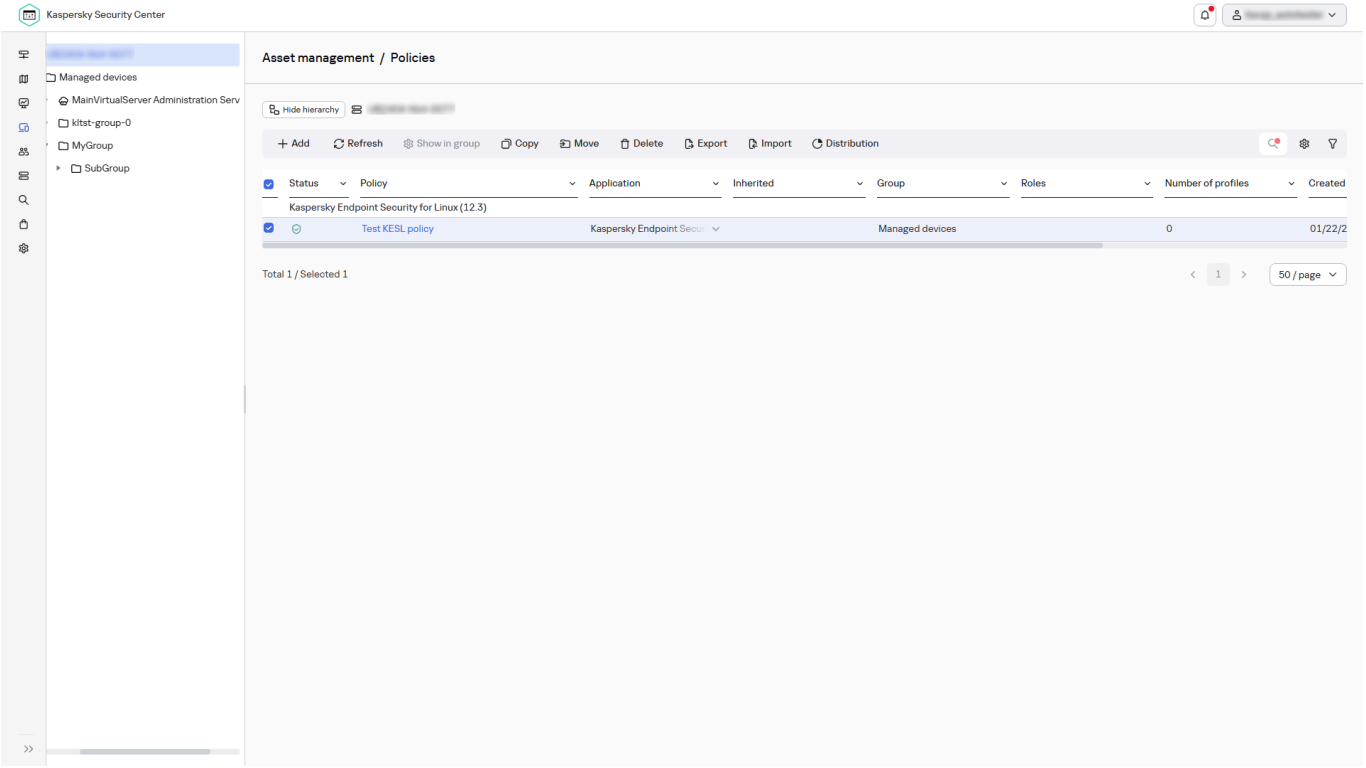
您可以從一個管理群組移動政策到另一個。例如，您要刪除一個群組，但您要為其他群組使用其政策。在此情況下，您可能要先將政策從舊群組移動至新群組，再刪除舊群組。

> 將政策移至另一個管理群組時，政策的修訂歷程記錄將被清除。「**變更歷史**」頁籤僅顯示有關最新變更的資訊。

要移動政策到其他管理群組：

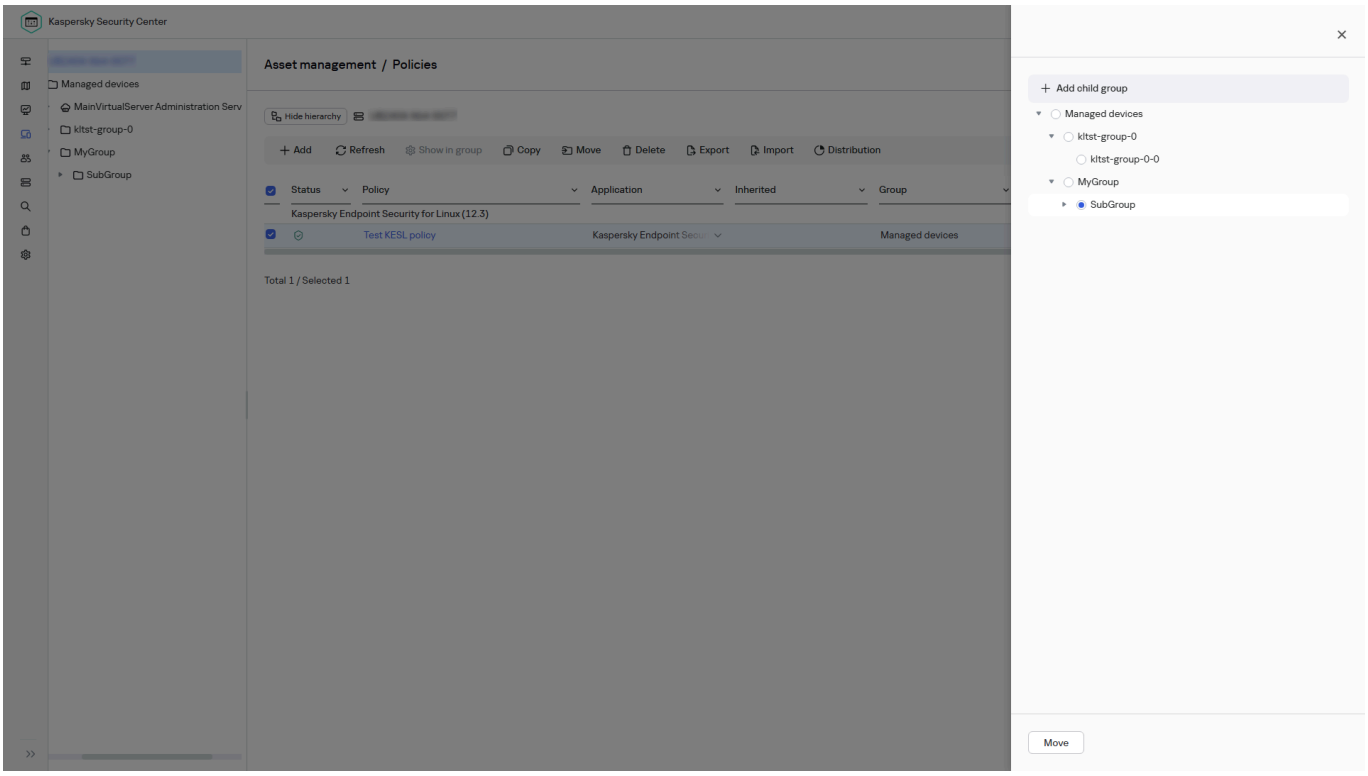
1. 在主功能表中，轉至 **資產管理** → **政策**。

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

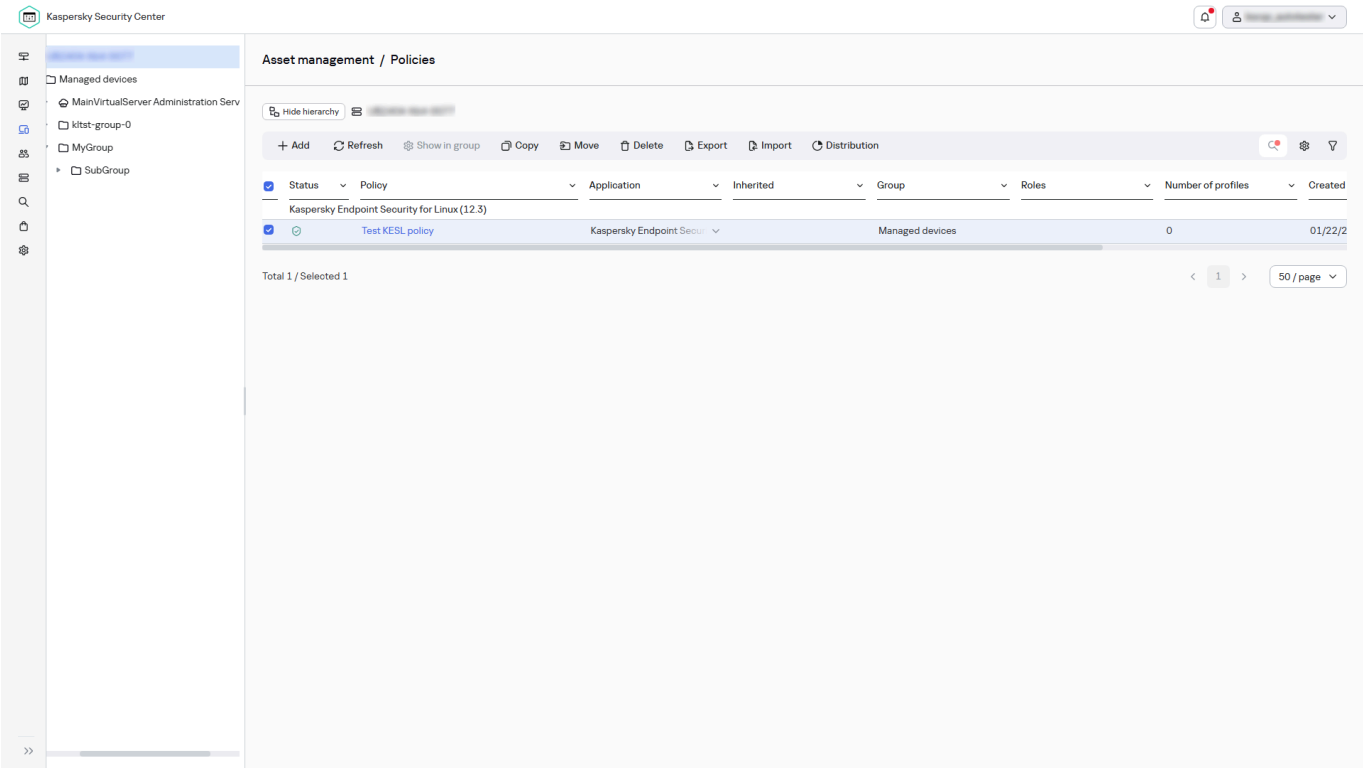
卡巴斯基安全管理中心 Linux 允許您將政策及其設定和政策設定檔儲存到 KLP 檔案。您可以使用此 KLP 檔案匯入儲存的政策到卡巴斯基安全管理中心 Windows 和卡巴斯基安全管理中心 Linux。

要匯出政策，請執行以下操作：

1. 在主功能表中，轉至 **資產管理** → **政策**。

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。



選擇要匯出的政策

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 Linux 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 **資產管理 → 政策**。

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)**。

強制同步

儘管 卡巴斯基安全管理中心 Linux 自動為受管理裝置同步狀態、設定、工作和政策，在某些情況下，管理員必須準確知道是否同步已經在指定裝置上執行。

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 **資產管理** → **資產（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：
   - 執行裝置分類以檢視裝置清單。
   - 在主功能表中，前往**資產管理** → **資產（裝置）**，然後選取要同步的裝置所在的管理群組：
     - 對於根群組，您可以繼續下一步。
     - 對於子群組，請按一下頁面頂部的**顯示階層**按鈕，然後在開啟的視窗中按一下子群組的名稱。

       所選群組的路徑將顯示在頁面頂部。如果需要，您可以點擊帶有管理群組名稱的連結進入該群組。預設情況下，路徑中的最後一個連結不活動。您也可以點擊**隱藏階層**按鈕關閉層次結構視窗。
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 **資產管理 → 資產（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**應用程式**標籤。

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。

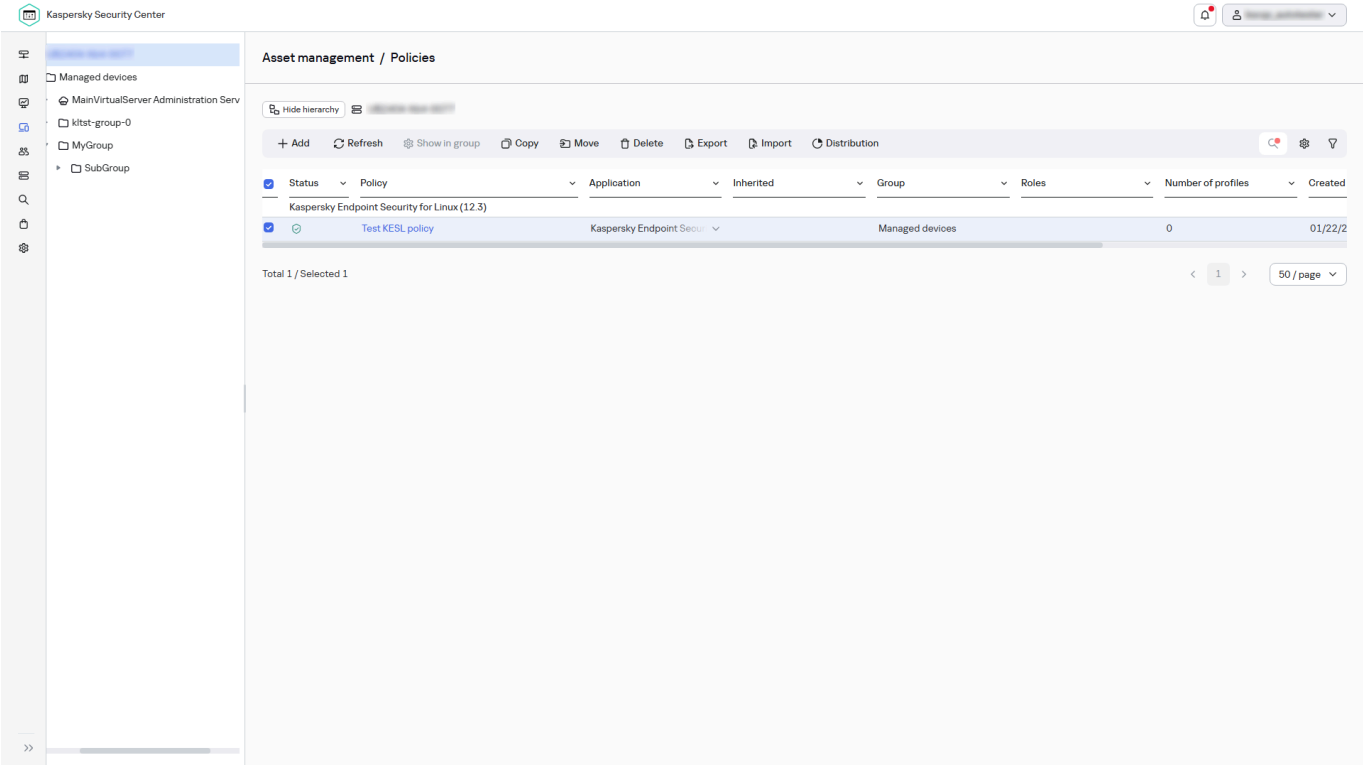
檢視政策發佈狀態圖表

在卡巴斯基安全管理中心 Linux 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 **資產管理 → 政策**。

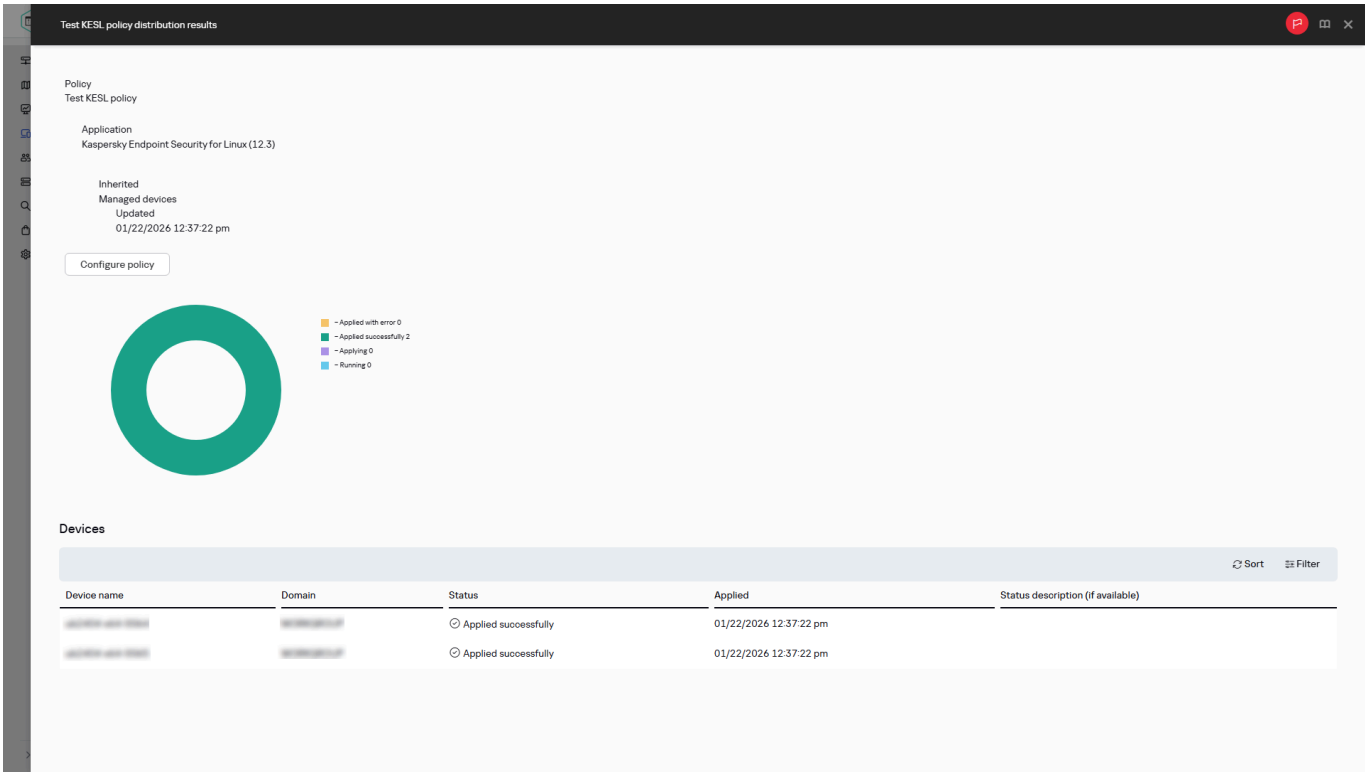
2. 選取要在裝置上檢視分配狀態之政策名稱旁的核取方塊。



政策清單

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。



政策的分發結果

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，轉至**設定 → 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。

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. 在主功能表中，按一下管理伺服器名稱。
   管理伺服器內容視窗會開啟，並含有所選的**一般**頁籤。
2. 選擇**病毒爆發**區段。
3. 在右側面板中，點擊**設定在病毒爆發事件發生時要啟動的政策**連結。
   啟動政策視窗將開啟。
4. 在與偵測到病毒爆發的該元件相關區段中—適用於工作站與檔案伺服器的防毒軟體、適用於郵件伺服器的防毒軟體，或適用於週邊防護的防毒軟體—選取您要輸入項旁的選項按鈕，之後點擊**新增**。
   內含**受管理裝置**管理群組的視窗隨即開啟。
5. 點擊**受管理裝置**旁的 V 型圖示（>）。
   管理群組層級和它們的政策被顯示。
6. 在管理群組層級和它們的政策中，點擊政策名稱或偵測到病毒爆發時啟動的政策的名稱。
   要在清單或群組中選擇所有政策，選擇所需名稱旁邊的核取方塊。
7. 點擊**儲存**按鈕。
   管理群組層級和它們的政策的視窗被關閉。

所選的政策被新增到偵測到病毒爆發時啟動的政策清單。所選政策在病毒爆發中被啟動，無論它們是活動的還是非活動的。

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。

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 **資產管理** → **政策**。
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。政策刪除後，如果此選項已啟用，政策變更事件會匯出至 SIEM 系統。

管理政策設定檔

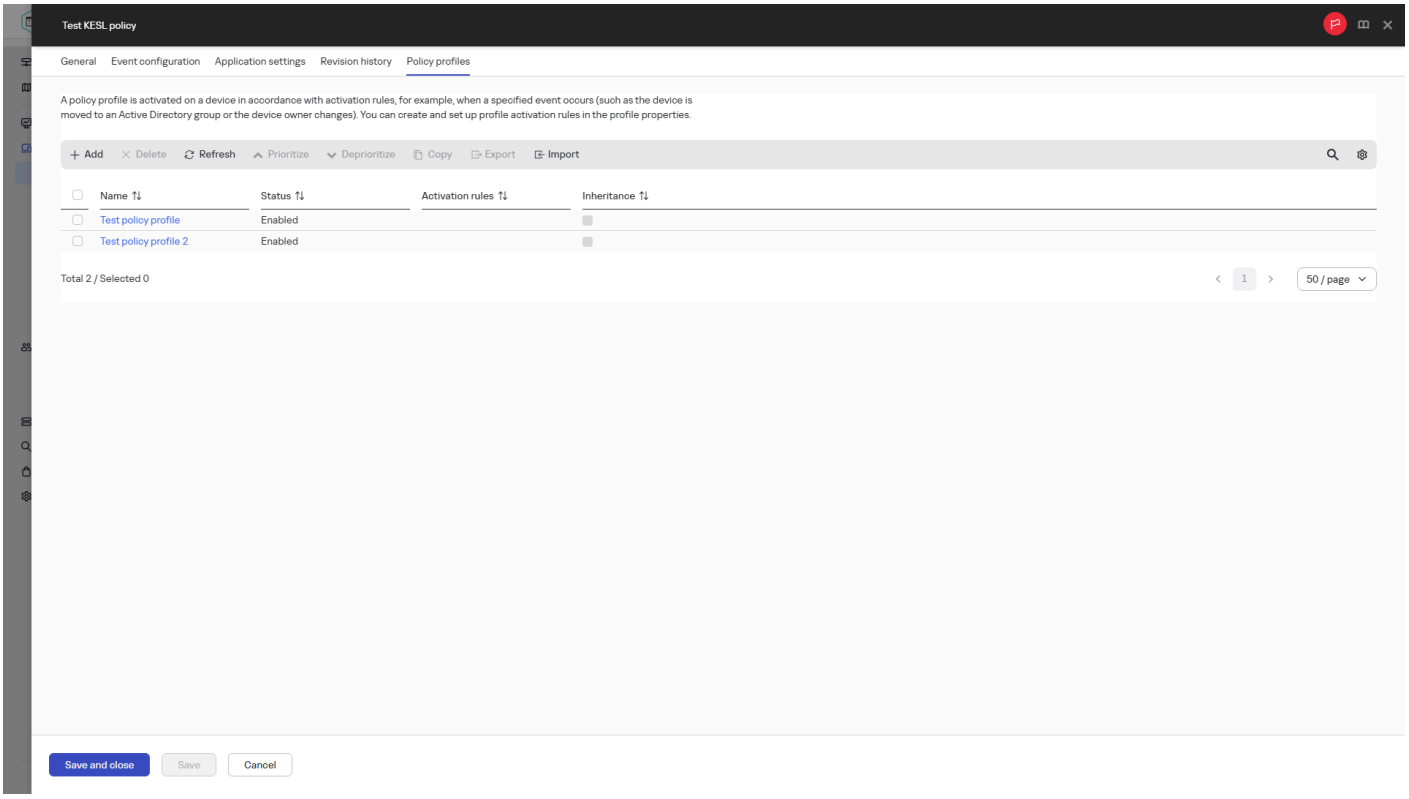
本節說明如何管理政策設定檔，並提供有關檢視政策設定檔、變更政策設定檔優先順序、建立政策設定檔、複製政策設定檔、建立政策設定檔啟用規則、刪除以及匯出和匯入政策設定檔的資訊。

檢視政策設定檔

要檢視政策設定檔：

1. 在主功能表中，轉至 **資產管理** → **政策**。
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。

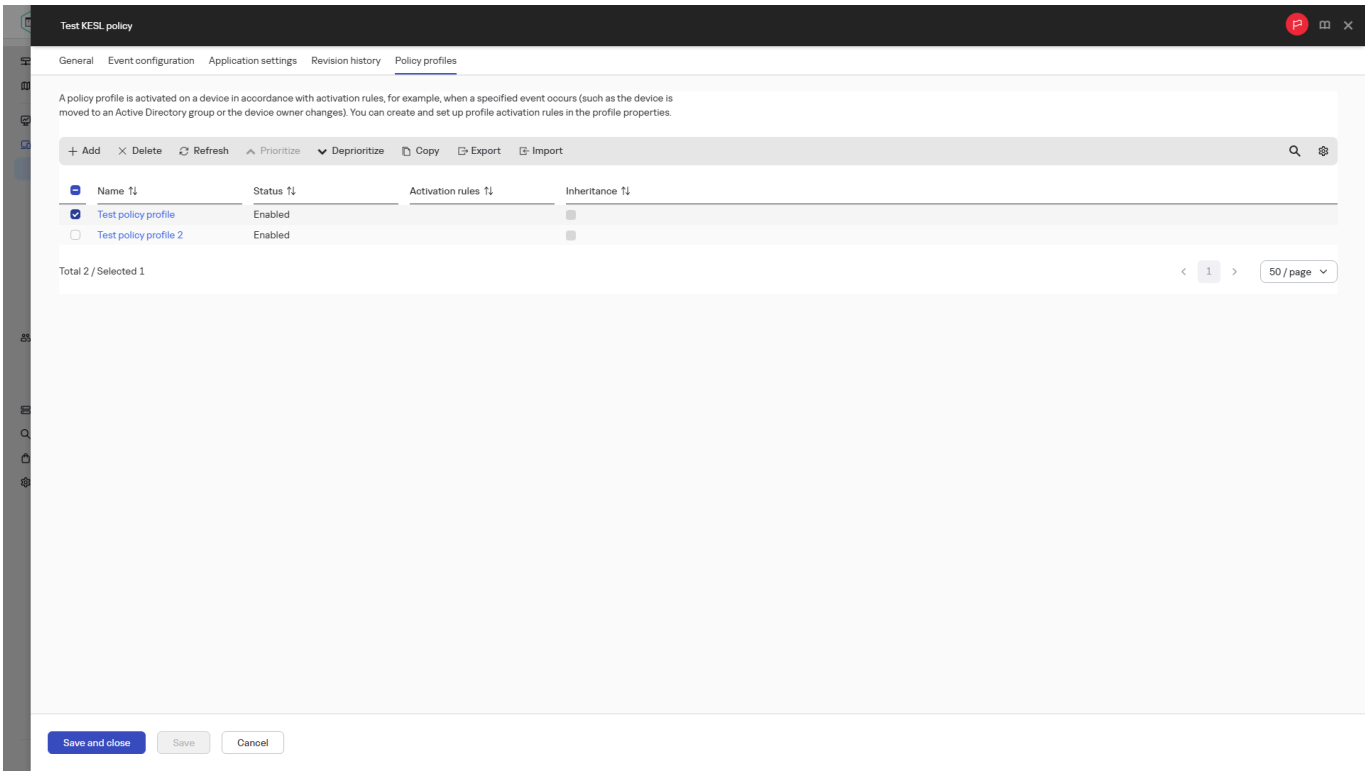


政策設定檔清單

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。

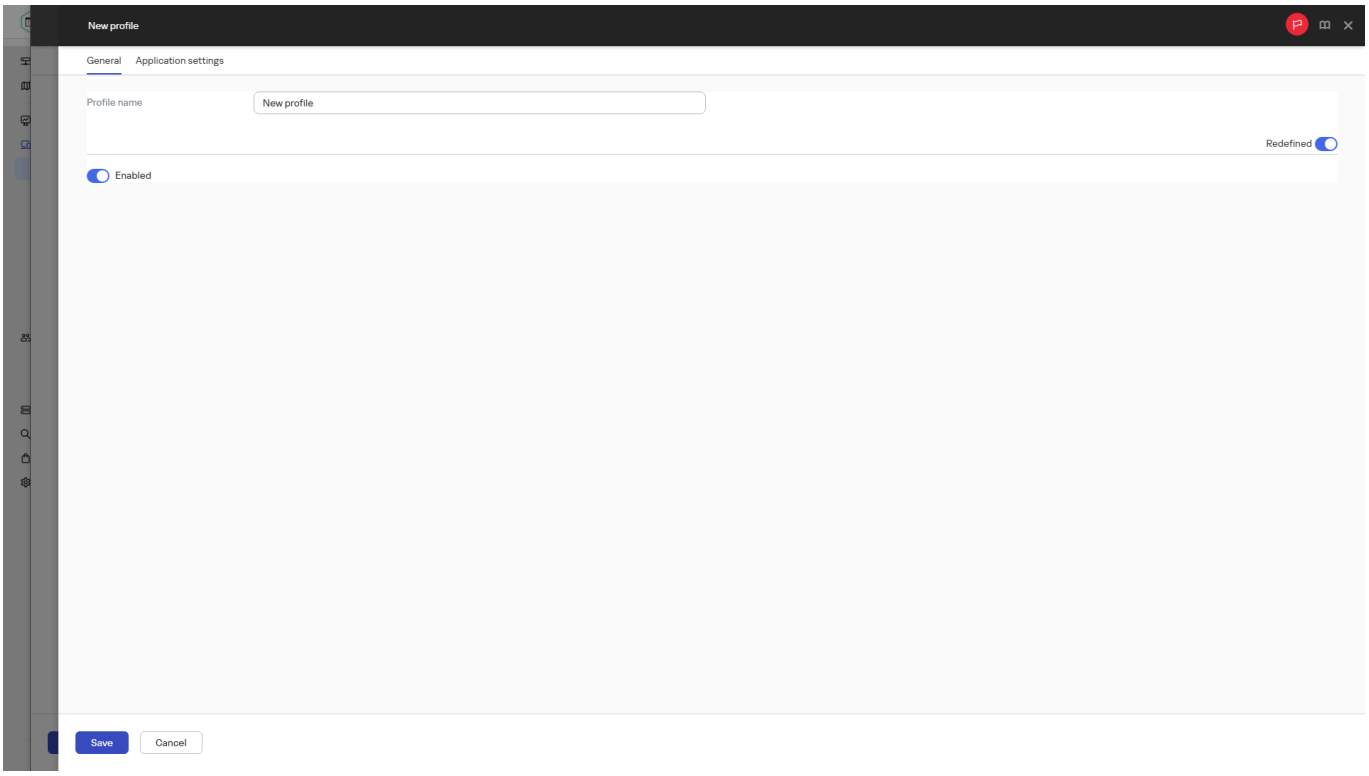
建立政策設定檔

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。



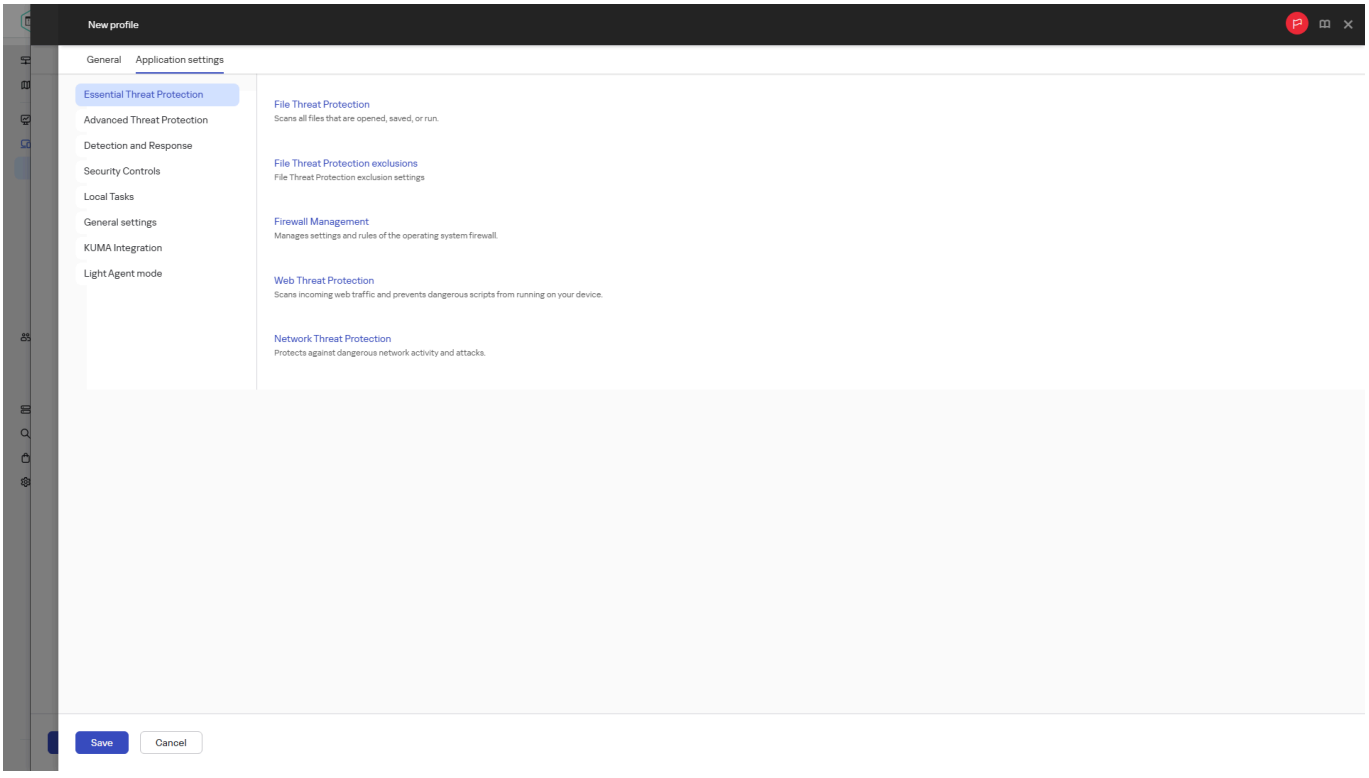
建立新政策設定檔

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。



指定政策設定檔設定

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。

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。

- **裝置網路位置**

  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。

- **特定裝置所有者規則**

  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 Linux 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 Linux 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。

- **硬體規格規則**

  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：

- **RAM 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。

- **角色指派規則**

  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。

- **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：

- **裝置所有者在 Active Directory 安全群組中的身分**

  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**

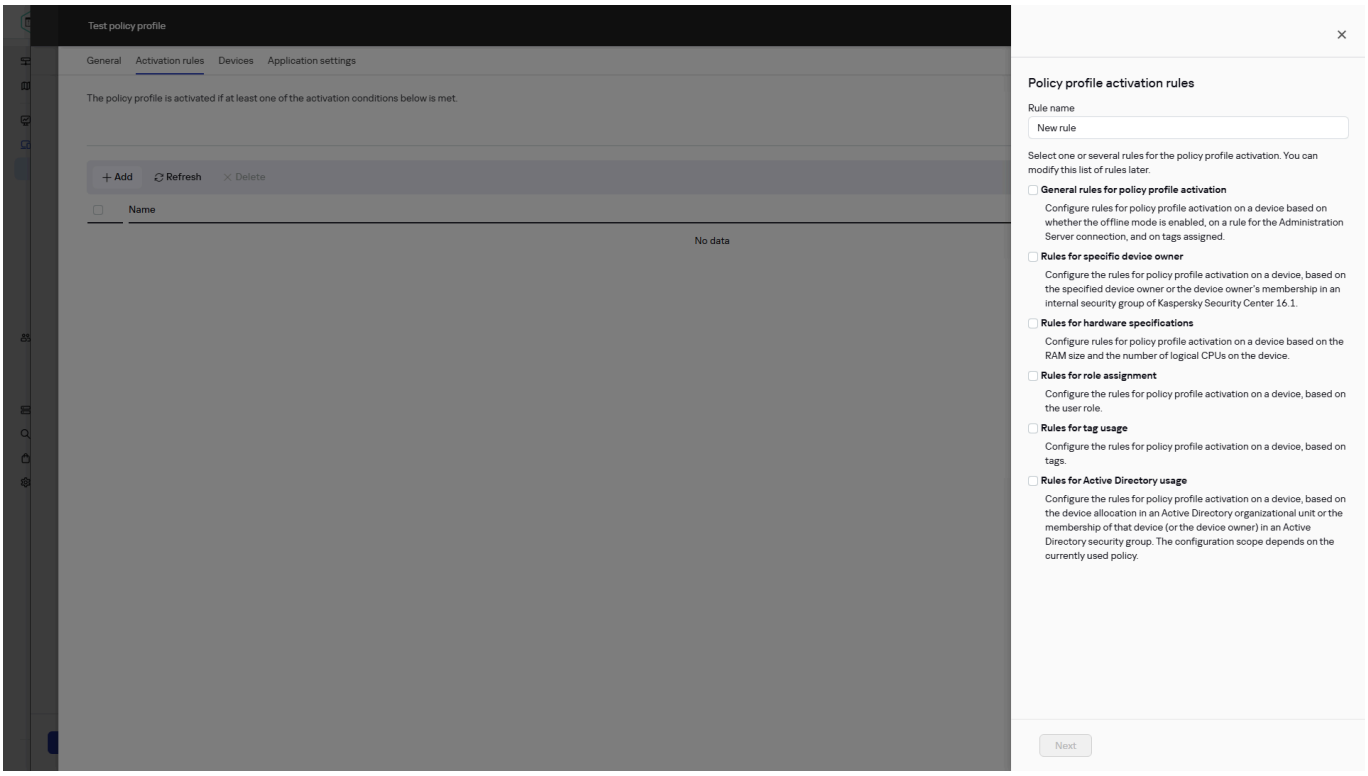
  如果選取此核取方塊，則會在裝置上啟動政策設定檔。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

- **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。



建立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。

匯出和匯入政策設定檔

無需匯出政策，即可將政策設定檔儲存到 KLPROF 檔案，然後使用此 KLPROF 檔案將已儲存的設定檔匯入到政策。

這可讓您快速恢復策略設定檔設定，而不是再設定它們。

政策設定檔會匯入到與匯出該設定檔的應用程式版本相同的政策中。對於支援政策向後相容的應用程式（例如，Kaspersky Endpoint Security for Windows），您可以將政策設定檔匯入到不同版本的政策中。

要匯出政策設定檔，請執行以下操作：

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**」索引標籤上，點擊要匯出的政策設定檔。

3. 在工具列上，點擊「**匯出**」按鈕。

4. 在開啟的視窗中，指定要儲存包含政策設定檔之檔案的目錄。

   如有必要，可變更檔案名稱。

5. 按一下**儲存**按鈕。

如果操作成功完成，螢幕上將顯示相應訊息。否則，將顯示錯誤訊息。

要匯入政策設定檔，請執行以下操作：

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. 在工具列上，點擊「**匯入**」按鈕。

3. 在開啟的視窗中，選取包含所需政策設定檔的 KLPROF 檔案，然後點擊「**開啟**」按鈕。
   匯入檔案的大小上限為 4 GB。

如果操作成功完成，螢幕上將顯示相應訊息。否則，將顯示錯誤訊息。

政策設定檔會以匯出時的名稱匯入，而不是以 KLPROF 檔案的名稱匯入。
檔案會以「**已停用**」狀態和最低優先順序匯入，無論政策設定檔在匯出前的優先順序為何。

在以下情況下無法執行匯入：

- 政策中已存在同名設定檔。
- 政策中的設定檔數量已達 100 個。

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 **資產管理** → **政策**。
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。內容視窗包含如下所述的頁簽和設定。

請參閱以下比較表，它詳情描述了如何根據使用的作業系統類型套用設定。

一般

在此頁籤上，您可以修改政策名稱、政策狀態並指定政策設定的繼承：

- 在**名稱**欄位中，您可以修改政策名稱。
- 在**政策狀態**區塊，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。

事件組態

在此頁簽上，您可以配置事件記錄和事件通知。事件根據重要性等級分佈在以下部分：

- **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週期（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**發生了安全問題**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**發生了安全問題**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安全問題，您可以使用受管理裝置設定管理該問題。

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 Linux 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 Linux）。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。

- **保護網路代理服務免遭未經授權的移除或終止，並防止設定遭到變更**

  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**

  如果啟用該選項，透過點擊**修改**按鈕，您可以在 Windows 裝置上指定 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：

- **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，會將用戶端裝置上必須安裝的 Microsoft Windows Update 更新資訊傳送至管理伺服器。

  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。

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，您可以啟用可執行檔的弱點掃描：

- **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。

- **提示使用者動作**

  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。

  - **強制關閉被封鎖工作階段中的應用程式**

    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。

管理修補程式和更新

在管理修補程式和更新區域，您可以設定受管理裝置上的更新下載和發佈，以及修補程式安裝：

- **自動為處於「未定義」狀態的元件安裝適用的更新與修補程式**

  如果啟用此選項，帶有*未定義*核准狀態的巴卡斯基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*狀態的卡巴斯基修補程式將僅在您改變其狀態為*已核准*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。我們建議您設定同步間隔（也叫心跳）為每 10,000 台受管理裝置 15 分鐘。

  - **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 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。

- **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**

  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

- **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**

  此選項僅適用於Windows的分發點。

  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。

  網路代理程式版本的裝置發現間隔可以在**Windows 網域的輪詢頻率（分鐘）**（用於快速的Windows網路輪詢）和**網路輪詢頻率（分鐘）**（用於完整的Windows網路輪詢）欄位中進行設定。

  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。

- **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。

- **網域控制器**

  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網域控制器。

  如果停用此選項，則發佈點將不輪詢網域控制器。

在 10.2 版之前的網路代理中，可在**輪詢間隔（分鐘）**欄位中配置網域控制器的輪詢頻率。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。

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。

  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/KPSN**

  發佈點從受管理裝置轉發 KSN 請求到 KSN 雲端或 KPSN。在發佈點上自行產生的 KSN 要求頁會直接傳送至 KSN 雲端或 KPSN。

- **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。

- **HTTPS 連接埠**

  如果您需要受管裝置透過 HTTPS 連接埠連線至 KSN 代理伺服器，請啟用**使用 HTTPS**選項，然後在**HTTPS 連接埠**欄位中指定連接埠號碼。預設情況下已停用該選項。連線到 KSN 代理伺服器的預設 HTTPS 連接埠是 17111。

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。

本機帳戶管理（僅限 Linux）

本機帳戶管理（僅限 Linux）區域包括三個子區域：

- **使用者憑證管理**
- **新增或編輯適用的本機管理員群組**
- **上傳參考檔案以防護使用者裝置上的 sudoers 檔案免受變更**

在**使用者憑證管理**子區域中，您可以指定要安裝的根憑證。例如，這些憑證可用於驗證網站或網頁伺服器的真確性。

- **安裝根憑證**

  如果啟用此選項，則新增至表格中的憑證將安裝在指定的裝置上。

  如果停用此選項，則不會在指定裝置上安裝任何憑證。

  預設情況下已停用該選項。

- **新增**

  點擊此按鈕將開啟一個視窗，您可以在其中新增憑證。

  憑證必須小於 10 MB。

  卡巴斯基安全管理中心支援具有 CER、CRT、CERT、PEM 和 KEY 副檔名的憑證。

在**新增或編輯適用的本機管理員群組**子區域中，您可以管理本機管理員群組。例如，在撤銷本機管理員權限時就會用到這些群組。您也可以使用**特權裝置使用者報告（僅限 Linux）**檢查特權使用者帳戶清單。

- **新增**

  點擊此按鈕將開啟一個視窗，您可以在其中新增本機管理員群組。

- **編輯**

  點擊此按鈕將開啟一個視窗，您可以在其中編輯本機管理員群組。

  如果選取本機管理員群組旁邊的核取方塊，則可使用此按鈕。

- **刪除**

  點擊此按鈕即從表格中刪除已選取的本機管理員群組。

  如果選取本機管理員群組旁邊的核取方塊，則可使用此按鈕。

在**上傳參考檔案以防護使用者裝置上的 sudoers 檔案免受變更**子區域中，您可以設定 sudoers 檔案的控制。特權群組和裝置使用者是由裝置上的 sudoers 檔案定義。sudoers 檔案位於 `/etc/sudoers`。您可以上傳參考 sudoers 檔案，以保護 sudoers 檔案免於變更。這將防止對 sudoers 檔案進行不必要的變更。

無效的參考 sudoers 檔案可能會導致使用者的裝置故障。

- **控制 sudoers 檔案**

  如果啟用此選項，sudoers 檔案將被目前的參考 sudoers 檔案取代。

  如果停用此選項，sudoers 檔案將保持不變。

  預設情況下已停用該選項。

- **參考 sudoers 檔案**

  此欄位顯示上傳的參考 sudoers 檔案名稱。

- **上傳**

  點擊此按鈕將開啟一個視窗，您可以在其中上傳參考 sudoers 檔案。

- **目前的參考 sudoers 檔案**

  點擊此按鈕將顯示目前 sudoers 檔案的內容。

變更歷史

在**變更歷史**頁籤上，您可以：

- 檢視並儲存政策修訂歷程記錄。
- 回溯到政策修訂。

- 新增和編輯政策修訂描述。
- 比較政策修訂版本。

Windows、Linux 和 macOS 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、Linux 和 macOS 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	Linux	macOS
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	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	✓	✓
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	✓	✓	✓ 除推播伺服器外
發佈點			
用作發佈點	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	✓	✓
計算發佈點的數量和配置	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	✓ 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	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	✓	✓
網路輪詢	✓ • IP 範圍輪詢 • 網域控制器輪詢（Active Directory） 限制：不支援Microsoft Windows on Arm的網路代理程式。	✓ IP 範圍輪詢 Zeroconf 輪詢 網域控制器輪詢（Microsoft Active Directory、Samba 4 Active Directory，FreelPA，ALD Pro）	—
在發佈點端執行 KSN 代理服務	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	✓	—

網路代理功能	Windows	Linux	macOS
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	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	✓	— (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	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	受限制：無法使用 Linux 發佈點在 Windows 裝置上執行推送安裝。	受限制：無法使用 macOS 發佈點在 Windows 裝置上執行推送安裝。
作為推送伺服器使用	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	✓	—
處理協力廠商應用程式			
在裝置上遠端安裝應用程式	✓	✓	✓ 有關詳細資訊，請參閱以下文章：在 macOS 裝置上遠端安裝應用程式。
在網路代理政策中配置作業系統更新	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	—	—
檢視軟體弱點資訊	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	—	—
掃描應用程式以尋找弱點	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	—	—
軟體更新	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	—	—
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	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	✓	✓
對動態虛擬機的支援	✓ 限制：不支援Microsoft Windows on Arm的網路代理程式。	✓	✓
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	✓	✓	✓
漫遊使用者的連線設定檔	✓	✓	✓

網路代理功能	Windows	Linux	macOS
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	✓	✓	✓
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	✓	✓	✓
檢視用戶端裝置硬體的資訊	✓	✓ 安裝在這些裝置上的網路代理傳送給管理伺服器的 Linux 裝置硬體資訊僅限於受管理裝置設定說明中指定的資訊。	✓ 安裝在這些裝置上的網路代理向管理伺服器傳送的有關 macOS 裝置硬體的資訊僅限於受管理裝置設定說明中指定的資訊。

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政策設定，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	Linux	macOS
一般	✓	✓	✓
事件組態	✓	✓	✓
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**	✓ **硬體登錄資料詳細資訊**選項可用。
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	✓ 提供以下功能： • **Windows 網路** • **IP 範圍** • **網域控制器**	✓ 提供以下功能： • **Zeroconf** • **IP 範圍** • **網域控制器**	—
發佈點網路設定	✓	✓	✓
KSN 代理（發佈點）	✓	✓	—
更新（發佈點）	✓	✓	—
變更歷史	✓	✓	✓

啟用和停用網路代理的低資源消耗模式

低資源消耗模式讓您能限制用戶端裝置上安裝的網路代理的 RAM 使用量。在預設情況下，低資源消耗模式處於停用狀態。

以下功能不會在低資源消耗模式下執行：

- 無法指定網路代理扮演發佈點（手動或自動）。
- 網路代理不會在單獨的文字檔案中記錄網路代理狀態的資訊。
- 網路代理不支援離線更新下載模式。
- 以下元件和進程已停用：
  - 取得有關第三方更新和弱點的資訊。
  - 在發佈點端執行 KSN 代理。
  - 將更新上傳到發佈點儲存區。
  - 繞過 DNS 伺服器封鎖。
  - 獲取有關可用磁碟空間的資訊。

停用低資源消耗模式後，元件和進程恢復運作。

若要啟用低資源消耗模式：

1. 在用戶端裝置的命令列中執行以下指令：

   ```
   sudo /opt/kaspersky/klnagent64/sbin/klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 1
   ```

2. 使用以下指令重新啟動網路代理：

   ```
   sudo service klnagent64 restart
   ```

3. 在作業系統日誌中，檢查**卡巴斯基安全管理中心網路代理正以低資源消耗模式工作**項目是否顯示。

   低資源消耗模式已啟用。

若要停用低資源消耗模式：

1. 在用戶端裝置的命令列中執行以下指令：

   ```
   sudo /opt/kaspersky/klnagent64/sbin/klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 0
   ```

2. 使用以下指令重新啟動網路代理：

   ```
   sudo service klnagent64 restart
   ```

   低資源消耗模式已停用。

您也可以透過使用*遠端執行指令碼工作*遠端啟用低資源消耗模式。

配置受管理應用程式的防護設定

若要配置受管理卡巴斯基應用程式的防護設定，您可以使用政策。

有關配置 Kaspersky Endpoint Security 政策的詳細資訊，請參閱對應說明：

- Kaspersky Endpoint Security for Windows 說明
- Kaspersky Endpoint Security for Linux 說明
- Kaspersky Endpoint Security for Mac 說明

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化延遲**核取方塊被選中時。

Kaspersky Endpoint Security 裝置掃描群組工作的手動設定

快速啟動精靈建立掃描裝置的群組工作。如果自動指定的群組掃描工作排程不適合您的組織，您必須根據組織採用的工作場所規則手動設定最方便的排程。

例如，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。在這種情況下，您需要手動設定群組掃描工作。

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。

一旦加入 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 Linux 管理的用戶端裝置上安裝的 Kaspersky 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。

卡巴斯基安全管理中心 Linux 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 Linux 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 Linux 預設使用此解決方案。

- *卡巴斯基私人安全網路 (KPSN)* 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，而不必從自己的裝置傳送資料給全球 KSN。KPSN 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**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 Linux 會檢查 KSN 伺服器是否可存取，以確保受管理裝置維持安全等級。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。

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：

- 即使無法直接存取網際網路，用戶端裝置也可向 KSN 傳送請求、從 KSN 獲取資訊、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**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. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在**一般**標籤上，選取**KSN 代理**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。

   如果啟用此選項，KSN 代理伺服器會將資料傳送至 KSN，以提高卡巴斯基安全管理中心元件的效率並改進卡巴斯基應用程式的效能。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。如果停用此切換按鈕，資料不會透過卡巴斯基安全管理中心 Linux 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 Linux）。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 Linux）。

4. 選擇 KSN 基礎設施解決方案。

   在**參與 KSN**子區域中，執行下列其中一項操作：

   - 如果您使用的是全球 KSN，請將切換按鈕切換到**使用卡巴斯基安全網路 已啟用**位置。

     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 KPSN，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**選取包含 KSN 代理設定的檔案**按鈕以下載 KPSN 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 KPSN 設定檔的建立日期。

   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 KPSN 詳細資料的訊息。

   以下卡巴斯基應用程式支援 KPSN：

   - 卡巴斯基安全管理中心 Linux
   - Kaspersky Endpoint Security for Linux
   - Kaspersky Endpoint Security for Windows

   如果您在 卡巴斯基安全管理中心 Linux 啟用 KPSN，這些應用程式會接收支援私有 KPSN 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，將顯示關於所選 KSN 提供者的資訊 — KSN 或 KPSN。

   > 如果在管理伺服器內容視窗的**KSN 代理**區域設定了 KPSN，卡巴斯基安全管理中心 Linux 將不傳送任何統計資料到卡巴斯基安全網路。

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 KPSN，請啟用**當連線到 KPSN 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 KPSN。

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**HTTPS 連接埠**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**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. 在主選單中，按一下管理伺服器名稱。

   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/KPSN**選項。
6. 點擊**確定**。

   該發佈點將作為 KSN 代理伺服器。

> 請注意，發佈點不支援使用 NTLM 協定進行受管理裝置身分驗證。

啟用和停用 KSN 的使用

若要啟用 KSN 的使用：

1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在**一般**標籤上，選取**KSN 代理**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 代理伺服器會啟用並將資料傳送至 KSN，以提高卡巴斯基安全管理中心元件的效率並改進卡巴斯基應用程式的效能。

1. 根據您使用的KSN 基礎架構解決方案，啟用對應的切換按鈕。

   - 如果您使用的是全球 KSN，請將切換按鈕切換到**使用卡巴斯基安全網路 已啟用**位置。

     現在可以向 KSN 傳送資料。啟用此選項時，您必須閱讀並接受 KSN 聲明的條款。

   - 如果您正使用 KPSN，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，然後點擊**選取包含 KSN 代理設定的檔案**按鈕以下載 KPSN 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 KPSN 設定檔的建立日期。

     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 KPSN 詳細資料的訊息。

2. 點擊**儲存**按鈕。

若要停用 KSN：

1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在**一般**頁籤上，選取**KSN 代理**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。

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. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在**一般**標籤上，選取**KSN 代理**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，可以啟用卡巴斯基安全網路 (KSN) 代理。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 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，執行`ps aux`命令以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/klnagent64/sbin/ksnproxy` 處理程序是否正在執行。

如果 `/opt/kaspersky/klnagent64/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。

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程式停止加入Kaspersky Security Network。該需要本機管理員權限。

檢視KSN代理伺服器統計資料

卡巴斯基安全管理中心網頁主控台可讓您檢視 KSN 代理伺服器的使用統計資料。

統計資料包括以下參數：

- 與 KSN 的連線狀態
- 快取記錄數
- 快取中處理的封包數量
- 收到的封包數量

如果您使用 KPSN 作為基礎架構解決方案，則會顯示 KPSN 的使用統計資料。

檢視統計資料：

1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。
2. 在**一般**頁簽上，選擇**KSN 代理**部分，然後開啟**統計**頁簽。

   該頁簽顯示 KSN 代理伺服器使用的實際統計。統計資料每 15 秒重新整理一次。

您可以透過點擊**複製到剪貼簿**按鈕來複製統計資料。

管理工作

該部分描述了 卡巴斯基安全管理中心 Linux 使用的工作。

關於工作

卡巴斯基安全管理中心 Linux 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使用卡巴斯基安全管理中心 網頁主控台修改，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）或 DNS 名稱作為該裝置的位址。您還可以選擇由管理伺服器偵測到的聯網裝置。

- 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：

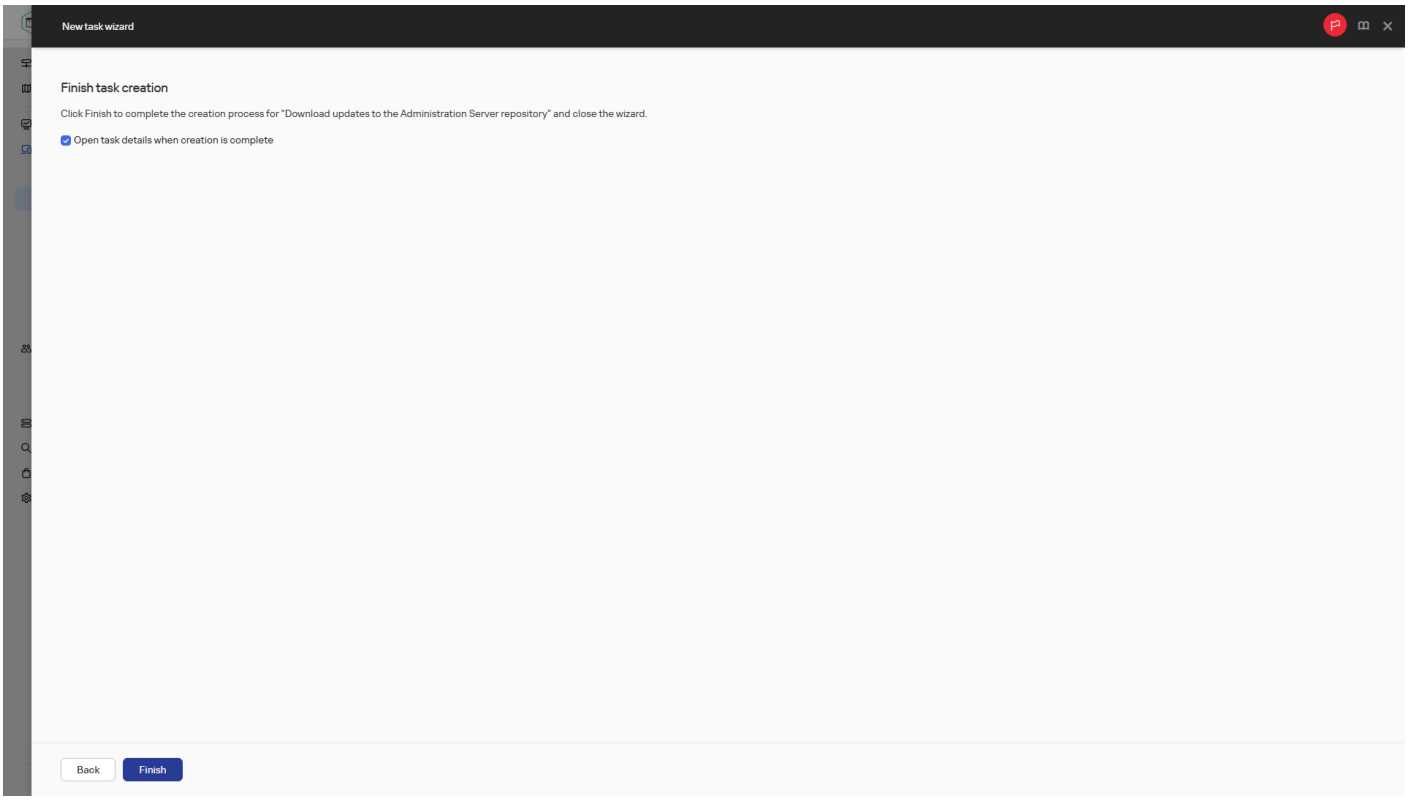
1. 在主功能表中，轉至 **工作**。
2. 點擊**新增**。

   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。



完成工作建立

若要建立分配給所選裝置的新工作：

1. 在主功能表中，轉至 **資產管理 → 資產（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

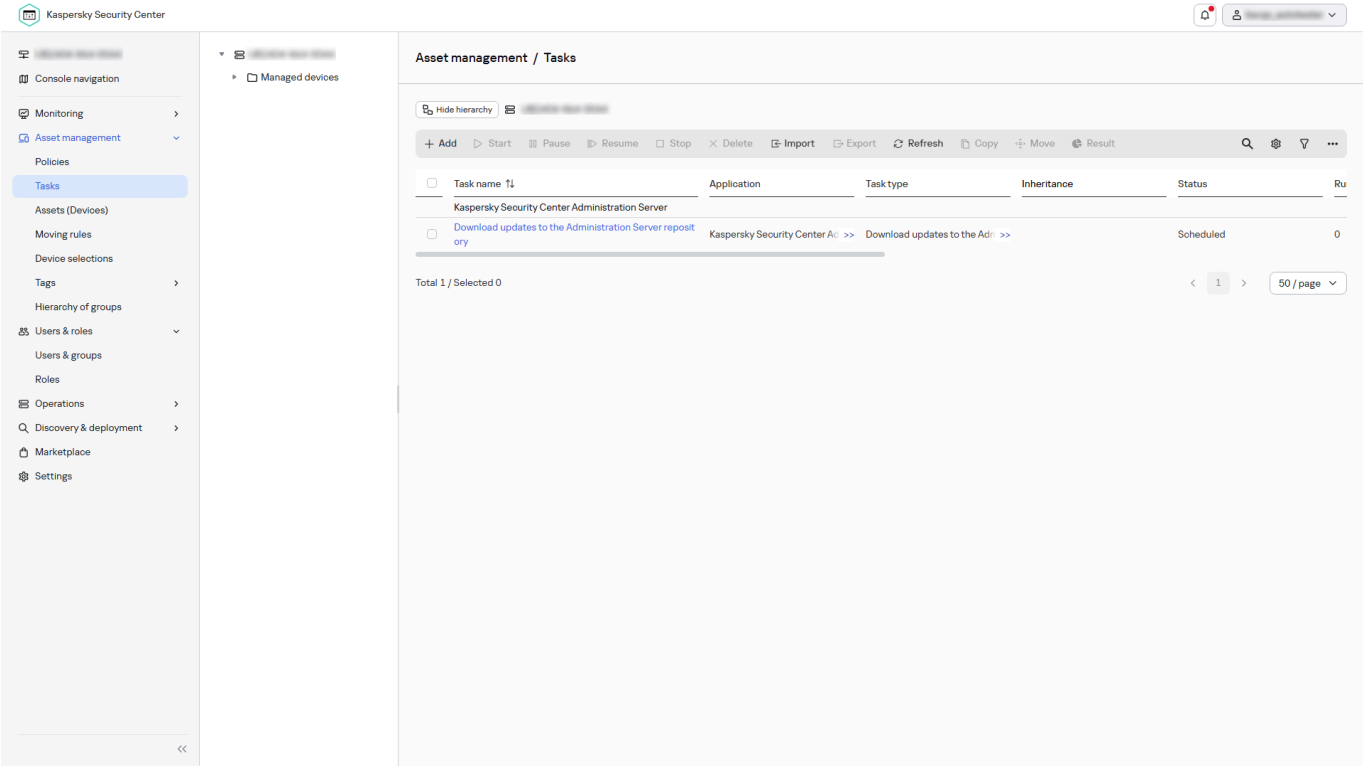
該應用程式會根據在各工作內容中指定的排程設定啟動工作。您可以隨時從工作清單中手動啟動工作。或者，您也可以在**資產（裝置）**清單中選取裝置，然後對這些裝置啟動現有工作。

若要手動啟動工作：

1. 在主功能表中，轉至 **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。



從工作清單啟動工作

工作啟動。您可在**狀態**欄中檢視工作狀態或點擊**結果**按鈕。

為選取的裝置啟動工作

您可以在裝置清單中選擇一台或多台用戶端裝置，然後啟動先前為它們建立的工作。這可讓您執行先前為一組特定裝置建立的工作。

> 這會將工作被指派到的裝置變更到您在執行工作時選擇的裝置清單。

為選取的裝置啟動工作：

1. 在主功能表中，轉至 **資產管理 → 資產（裝置）**。受管理裝置清單隨即顯示。

2. 在受管理裝置清單中，使用核取方塊選擇要為其執行工作的裝置。您可以使用搜尋和過濾功能來查找您正在尋找的裝置。

3. 按一下**執行工作**按鈕，然後選擇**套用現有工作**。

   現有工作清單隨即顯示。

4. 所選裝置顯示在工作清單上方。如有必要，您可以從此清單中刪除裝置。您可以刪除除一台裝置之外的所有裝置。

5. 在清單中選擇所需的工作。您可以使用清單上方的搜尋框按名稱搜尋所需的工作。只能選擇一項工作。

6. 按一下**儲存並啟動工作**。

所選工作將立即為所選裝置啟動。工作中的排程啟動設定不會變更。

檢視工作清單

您可檢視在卡巴斯基安全管理中心 Linux 建立的工作清單。

若要檢視工作清單，

在主功能表中，轉至 **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，*遠端安裝應用程式*工作會與管理伺服器相關，*更新*工作則指 Kaspersky Endpoint Security。

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。

  - **強制關閉被封鎖工作階段中的應用程式**

    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：

排程類型可能因工作而異。

某些類型的計劃可能不適用於其他卡巴斯基應用程式。

- **開始工作設定：**

  - **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 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。

  - **按每週中的指定日**

    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**

    此任務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。

- **立即**

  工作在其設定儲存後立即執行。

- **每月於選定的週間日**

  工作定期在指定月日的指定時間執行。

  預設情況下，開始時間為18:00，且未選擇當月的任何日期。

  > 請注意，您選擇的是當月的週幾，而不是特定的日期或週數（例如，當月的第一週或第二週）。例如，如果您將遊標放在**週二**行的**第一**單元格中，則表示該工作將在每個月的第一個星期二執行。

  您可以選擇一週中的多個日期。

- **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*更新*工作。

- **在完成其它工作時**

  目前工作在其他工作完成後啟動。只有在將這兩項工作指派給相同的裝置時，此選項才會發揮作用。例如，您可能想使用**開啟裝置**選項執行*受管理裝置*工作，完成後，請執行*病毒掃描*工作作為觸發工作。

  您必須從表格中選擇觸發工作以及此工作必須完成的狀態（**成功完成**或**失敗**）。

  如有需要，您可以對表格中的工作進行搜尋、排序和篩選，如下所示：

  - 在搜尋欄位中輸入工作名稱，可依其名稱搜尋工作。
  - 點擊排序圖示，可依名稱對工作進行排序。

    預設情況下，工作會依字母遞增排序。
  - 點擊篩選器圖示，在開啟的視窗中依群組篩選工作，然後點擊**套用**按鈕。

- **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化延遲**

  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。

- **對於在以下間隔內啟動的工作，使用工作啟動自動隨機化延遲**

  如果該選項被啟用，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 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，則工作內容視窗中不會顯示**安全**頁籤，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：
  - **在啟動工作之前，使用 Wake-On-LAN 功能開啟裝置**

    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**完成工作後將裝置關機**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。

  - **完成工作後將裝置關機**

    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，若執行時間超過**

    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中（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。

    - **儲存在裝置上的作業系統事件記錄中**

      有關工作執行的應用程式事件被本機儲存在每個用戶端裝置的 Syslog 事件記錄中。

      預設情況下已停用該選項。

    - **儲存在管理伺服器上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的 Syslog 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 Linux 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 **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 Linux 允許您從 KLT 檔案匯入工作。KLT 檔案包含匯出工作及其設定。

為了正確匯入卡巴斯基應用程式工作，您必須安裝相應的管理外掛程式。

要匯入工作，請執行以下操作：

1. 在主功能表中，轉至 **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：

   - **指派工作給管理群組**

     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，則工作內容視窗中不會顯示**安全**頁籤，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是從清單匯入位址**

     您可以指定您要為其分配工作的裝置的 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。

   - **指派工作給裝置分類**

     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 **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

指定目前在您的系統中有效的新憑據。當您切換至精靈的下一步時，卡巴斯基安全管理中心 Linux 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 Linux 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**未選取行動**。

   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。

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 Linux 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。

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。

查看從屬管理伺服器的工作結果：

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。
3. 點擊**來自從屬伺服器的統計資訊**。
4. 選取要顯示其**工作結果**視窗的次要伺服器。

應用程式標籤

該部分描述了應用程式標籤，提供了建立和修改它們以及標記協力廠商應用程式的說明。

應用程式標籤

卡巴斯基安全管理中心 Linux 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 **軟體管理 → 第三方應用程式 → 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**軟體管理 → 第三方應用程式 → 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 **軟體管理 → 第三方應用程式 → 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**指派的標籤**欄中的核取方塊。

4. 對於要指派的標籤，請在**指派的標籤**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**軟體管理 → 第三方應用程式 → 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**指派的標籤**欄中的核取方塊。

4. 對於您要移除的標記，請不要選取**指派的標籤**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**軟體管理 → 第三方應用程式 → 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。

使用 klscflag 實用程式開啟連接埠 13291

您可以使用 klbackup 自動化卡巴斯基安全管理中心 Linux 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 Linux 的安裝資料夾中。如果您要使用 klakaut 實用程式，請使用 klscflag 實用程式開啟 13291 連接埠。

實用程式 klscflag 可變更 KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN 參數的值。

要開啟連接埠 13291：

1. 在命令行中執行以下命令：
   ```
   /opt/kaspersky/ksc64/sbin/klscflag -ssvset -pv klserver -s 87 -n
   KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv true -svt BOOL_T -ss "|ss_type =
   \"SS_SETTINGS\";"
   ```

2. 透過執行以下命令重新啟動卡巴斯基安全管理中心管理伺服器服務：
   ```
   sudo systemctl restart kladminserver_srv
   ```

連接埠 13291 已開啟。

要檢查 13291 連接埠是否已成功開啟：

在命令行中執行以下命令：

```
/opt/kaspersky/ksc64/sbin/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)true
```

`true`值表示連接埠已開啟。否則，系統將顯示`false`值。

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。

     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。下載並安裝外掛程式後，卡巴斯基安全管理中心網頁主控台主功能表中將顯示**KICS for Networks**部分。

   - 在 Kaspersky Industrial CyberSecurity for Networks 網頁介面中，配置並啟用了與卡巴斯基安全管理中心的互動。詳情請參閱 Kaspersky Industrial CyberSecurity for Networks 線上說明。

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 **資產管理 → 未指派的裝置**。

   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. 在管理群組層次結構中，選中**受管理裝置**群組旁邊的核取方塊。

   e. 點擊**移動**按鈕。

3. 開啟安裝了 Kaspersky Industrial CyberSecurity for Networks Server 的裝置的內容視窗。

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，選擇卡巴斯基安全管理中心網路代理。

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，可以立即安裝。

8. 如果您想檢視 Kaspersky Industrial CyberSecurity for Networks 的統計資訊，您可以在儀表板上新增小部件。要新增小部件，請執行以下操作：

   a. 在主功能表中，「**監控**」→「**儀表板**」。

   b. 在儀表板上，點擊**新增或者還原網頁小部件**按鈕。

   c. 在開啟的小部件功能表中，選取**其它**。

   d. 選取您要新增的小部件：

      - KICS for Networks 部署圖
      - 有關 KICS for Networks 伺服器的資訊
      - KICS for Networks 的最新事件
      - KICS for Networks 中存在問題的裝置
      - KICS for Networks 中的緊急事件
      - KICS for Networks 中的狀態

9. 要繼續前往 Kaspersky Industrial CyberSecurity for Networks 網頁介面，請執行以下操作：

   a. 在主功能表中，轉至**KICS for Networks→ 搜尋**。

   b. 點擊**查找事件或裝置**按鈕。

   c. 在開啟的**查詢參數**視窗中，點擊**伺服器**欄位。

   d. 從與卡巴斯基安全管理中心整合的伺服器下拉清單中，選擇 Kaspersky Industrial CyberSecurity for Networks 伺服器，然後點擊**查找**按鈕。

   e. 點擊 Kaspersky Industrial CyberSecurity for Networks 伺服器名稱旁邊的**轉至伺服器**連接。

      Kaspersky Industrial CyberSecurity for Networks 登入頁面將顯示。

      要登入 Kaspersky Industrial CyberSecurity for Networks 網頁介面，您需要提供應用程式使用者帳戶憑據。

管理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。

關於使用者帳戶

卡巴斯基安全管理中心 Linux 允許您管理使用者帳戶以及安全群組。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 Linux 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 Linux 內使用。

kladmins 群組無法用於存取卡巴斯基安全管理中心 Linux 中的卡巴斯基安全管理中心網頁主控台。kladmins 群組只能包含用於啟動卡巴斯基安全管理中心 Linux 服務的帳戶。

要檢視使用者帳戶和安全群組表：

1. 在主功能表中，轉至**使用者和角色 → 使用者和群組**。
2. 選擇**使用者**或**群組**頁簽。

使用者或安全群組表將開啟。如果要檢視僅包含內部使用者或群組或僅包含本機使用者或群組的表，請將**帳戶類型**過濾條件分別設定為**內部**或**本機**。

如果使用者表包含超過 50,000 個使用者，則僅顯示前 50,000 個使用者，其餘使用者將不顯示。

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。

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 Linux 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 Linux 和受管理理卡巴斯基應用程式的功能。

您可以透過以下其中一種方式為 卡巴斯基安全管理中心 Linux 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 Linux 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**對裝置分類執行操作**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：**對管理群組的管理功能**	**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

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：存取物件而不考慮它們的 ACL	**讀取**	獲得對所有物件的存取權限：**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。
一般功能：基本功能	• **讀取** • **寫入** • **執行** • **對裝置分類執行操作**	• 虛擬伺服器的裝置移動規則（建立、修改或刪除）：**寫入**、**對裝置分類執行操作** • 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** • 檢視作業系統記錄：**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」 • 「已安裝的工作站防護和 Windows Server 防護應用程式概要報告」 • 「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」 • "安全問題報告" • 「事件報告」 • 「發佈點活動報告」 • 「從屬管理伺服器的報告」 • 「裝置控制項事件報告」 • 「弱點報告」 • 「禁止的應用程式報告」 • 「Web控制項報告」 • "受管理裝置加密狀態報告" • "大容量儲存裝置加密狀態報告" • "加密磁碟機存取權限報告" • "檔案加密錯誤報告" • "封鎖存取加密檔案的報告" • 「有效使用者權限報告」 • 「權限報告」	沒有
一般功能：刪除的物件	• **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**	• 變更事件註冊設定：**編輯事件記錄設定** • 變更事件通知設	沒有	沒有	設定： • 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
	• **編輯事件記錄設定** • **寫入**	定：**編輯事件通知設定** • 刪除事件：**刪除事件**			
一般功能：管理伺服器上的操作	• **讀取** • **寫入** • **執行** • **修改物件 ACL** • **對裝置分類執行操作**	• 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 軟體部署	• **管理 Kaspersky 修補程式** • **讀取** • **寫入** • **執行** • **對裝置分類執行操作**	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：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：管理伺服器的層次結構	**配置管理伺服器的層次結構**	• 註冊、更新或刪除從屬管理伺服器：**配置管理伺服器的層次結構**	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** • **對裝置分類執行操作**	• 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	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：**加密金鑰管理**	**寫入**	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** • **僅向行動裝置傳送資訊命令** • **傳送命令到行動裝置** • **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：**連線性**	• **開始 RDP 工作階段** • **連線到現有的 RDP 工作階段** • **啟動通道建立功能** • **將來自裝置的檔案儲存到管理員的工作站** • **讀取** • **寫入** • **執行** • **對裝置分類執行操作**	• 建立桌面共用工作階段：**建立桌面共用工作階段的權限** • 建立 RDP 工作階段：**連線到現有的 RDP 工作階段** • 建立通道：**啟動通道建立功能** • 儲存內容網路清單：**將來自裝置的檔案儲存到管理員的工作站**	沒有	「裝置使用者報告」	沒有
系統管理：**弱點和修補程式管理**	• **讀取** • **寫入** • **執行** • **對裝置分類執行操作**	• 檢視協力廠商修補程式屬性：**讀取** • 變更協力廠商修補程式屬性：**寫入**	• 「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：**遠端執行指**	• **讀取** • **寫入**	使用者可以查看工作內容：**讀取**	「遠端執行指令碼」	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
令碼	• **執行** • **對裝置分類執行操作**	使用者可以建立、刪除或修改安裝套件：**寫入** 使用者可以執行工作：**寫入**。在用戶端 Linux 裝置上，指令碼以 root 權限執行。 使用者可以執行工作或安排其執行：**執行** 使用者可以在選擇的裝置上運行工作：**對選擇的裝置執行操作**			

預先定義的使用者角色

分配給卡巴斯基安全管理中心 Linux 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 Linux 功能的存取權限。卡巴斯基安全管理中心 Linux 中可用的一些預定義使用者角色可以與特定的工作職位相關聯，例如，**稽核員**、**保安人員**、**主管**。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**
	  • **加密金鑰管理**
	  • **事件處理**
	  • **管理伺服器的層次結構**
	  • **虛擬管理伺服器**
	• **系統管理**：
	  • **連線**
	  • **硬體清單**
	  • **軟體清查**

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**（如適用）權限：
	• **一般功能**：
	  • **基本功能**
	  • **加密金鑰管理**
	  • **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** • **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**
	  • **卡巴斯基應用程式佈署**
	  • **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**（如適用）權限：
	• **一般功能：**
	  • **基本功能**
	  • **卡巴斯基應用程式佈署**（也會在此區域授予**管理卡巴斯基修補程式**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** • **一般功能：加密金鑰管理** • **Kaspersky Endpoint Security** 區域，包括所有功能
Kaspersky Endpoint Security 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** • **一般功能：加密金鑰管理** • **Kaspersky Endpoint Security** 區域，包括所有功能
主管理員	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**

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**
	  • **加密金鑰管理**
	  • **在管理伺服器上操作**
	  • **裝置標籤**
	  • **卡巴斯基應用程式佈署**
	  • **應用程式整合**
	  • **虛擬管理伺服器**
	• **行動裝置管理**區域，包括所有功能
	• **系統管理**区域，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**區域，包括所有功能 在**一般功能：金鑰管理**中授予**匯出金鑰檔案**權限。 授予**系統管理：弱點和修補程式管理**中的**讀取**權限。
行動裝置管理操作員	在**一般功能：基本功能**中授予**讀取**和**執行**權限。 在**行動裝置管理**中，授予**讀取**和**僅向行動裝置傳送資訊命令**權限： • **一般** • **自動服務入口**
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**功能區中授予下列權限：**讀取**、**寫入**、**執行**、**將檔案從裝置儲存到管理員工作站**以及**對裝置分類執行操作**。 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。

角色	敘述
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，*除了***遠端執行指令碼**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，*除了***遠端執行指令碼**功能）功能區域中的**讀取**和**執行**權限（如適用）。

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：
   - **資產管理 → 群組的階層**
   - **工作**
   - **監控→報告**
   - **資產管理→裝置分類**
   - **監控 → 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層次結構，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. 在主選單中，按一下管理伺服器名稱。

   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）
    - 裝置標籤
    - 卡巴斯基應用程式佈署
    - 產品授權金鑰管理
    - 應用程式整合
    - 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
    - 遠端執行指令碼
    - 硬體清單
    - 網路存取控制
    - 作業系統部署
    - 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

如果要新增使用者帳戶，請確保您的帳戶在一般功能：使用者權限功能區域中具有修改物件 ACL權限。

要新增新內部使用者帳戶到卡巴斯基安全管理中心 Linux：

1. 在主功能表中，轉至**使用者和角色** → **使用者和群組**，然後選擇**使用者**頁簽。
2. 點擊**新增**。
3. 在開啟的**新增使用者**視窗中，指定新使用者帳戶設定：
   - **名稱**。
   - 連線到 卡巴斯基安全管理中心 Linux 的使用者的**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"."。

     若要查看輸入的密碼，請按一下👁。
     您可以啟用**使用者必須在首次登入後更改密碼**選項，以強制在首次進行使用者身分驗證時變更密碼。
4. 儲存變更以完成新使用者帳戶的建立。

新的使用者帳戶被新增到使用者清單中。

若要在卡巴斯基安全管理中心網頁主控台上使用建立的內部使用者帳戶登入，必須為該使用者帳戶指派角色。登入前，請確保內部使用者帳戶已被指派角色。否則，將會出現登入錯誤。

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 → 使用者和群組**，然後選擇**群組**頁簽。
2. 點擊**新增**。
3. 在開啟的**建立安全群組**視窗中，為新安全群組指定以下設定：
   - **群組名稱**
   - **描述**
4. 點擊**儲存**以儲存變更。

新的安全群組被新增到群組清單中。

編輯內部使用者帳戶

如果要編輯使用者帳戶，請確保您的帳戶在一般功能：使用者權限功能區域中具有修改物件 ACL 權限。

要在卡巴斯基安全管理中心 Linux 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 → 使用者和群組**，然後選擇**使用者**頁簽。
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：
   - **使用者帳戶**

     如有必要，請切換開關按鈕至**非作用中**，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。
   - 描述
   - **完整名稱**
   - **電子郵件地址**
   - **主電話**

- **密碼**

  如有必要，您可以為卡巴斯基安全管理中心 Linux 的使用者連線設定新密碼，如下所示：

  a. 按一下**變更密碼**按鈕，然後為使用者帳戶設定新密碼。
     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"."。

     若要查看輸入的密碼，請按一下 。

  b. 如有必要，啟用**使用者必須在首次登入後更改密碼**選項以強制在下次進行使用者身分驗證時變更密碼。

  c. 如果使用者帳戶受到防護以防止未經授權的修改，您必須確認您擁有變更此帳戶的權限。在**帳戶防護**視窗中，在一般功能：使用者權限功能區域中指定具有修改物件 ACL 權限的帳戶的憑據。

4. 在**雙步驟驗證**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. 儲存變更以完成使用者帳戶的編輯。

更新的使用者帳戶出現在使用者清單。

編輯安全群組

要編輯安全群組：

1. 在主功能表中，轉至**使用者和角色** → **使用者和群組**，然後選擇**群組**頁簽。

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：
   - 在**一般**頁簽上，您可以變更**名稱**和**描述**設定。這些設定僅適用於內部安全群組。
   - 在**使用者**頁籤，您可新增使用者至安全群組。此設定僅適用於內部使用者和內部安全群組。
   - 在**角色**頁籤，您可指派角色給安全群組。
4. 點擊**儲存**以儲存變更。

變更被套用於安全群組。

為使用者或安全群組分配角色

對使用者或安全群組分配角色：

1. 在主功能表中，轉至**使用者和角色→使用者和群組**，然後選擇**使用者**或**群組**頁簽。
2. 選擇要對其分配角色的使用者或安全群組的名稱。

   您可以選取多個名稱。
3. 在功能表行中，點擊**指派角色**按鈕。

   角色分配精靈啟動。
4. 按照精靈的說明進行操作：選擇要分配給所選使用者或安全群組的角色，然後選擇角色的範圍。

   *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。

擁有處理管理伺服器權限集合的角色將被指派給使用者（或者多個使用者，或者安全群組）。在使用者或安全群組清單中，**已指派角色**列中會出現一個核取方塊。

新增使用者帳戶到內部安全群組

> 您僅可以新增內部使用者帳戶到內部安全群組。

要新增使用者帳戶到內部安全群組：

1. 在主功能表中，轉至**使用者和角色 → 使用者和群組**，然後選擇**使用者**頁簽。
2. 選取您要新增到安全群組的使用者帳戶旁邊的核取方塊。
3. 點擊**指派群組**按鈕。
4. 在開啟的**指派群組**視窗中，選取您要向其新增使用者帳戶的安全群組。
5. 點擊**儲存**按鈕。

使用者帳戶被新增到安全群組。您還可以使用群組設定將內部使用者新增到安全群組。

將使用者指派為裝置所有者

有關將使用者指派為行動裝置所有者的資訊，請參閱Kaspersky Security for Mobile說明。

若要將使用者指派為裝置所有者：

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 → 使用者和群組**，然後選擇**使用者**頁簽。

   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**資產管理 → 資產（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。

在安裝網路代理期間將使用者指定為裝置所有者

若要在透過安裝套件安裝網路代理時將使用者指派為裝置所有者，請將下表中指定的變數新增至網路代理安裝套件設定。

變數名稱	必要	敘述	可能的值
KLNAGENT_DEVICEOWNER_REGISTRATION_START	否	允許在安裝網路代理後，執行用於將使用者註冊為裝置所有者的實用程式。如果關閉，則使用者無法註冊為裝置所有者。	1 — 安裝網路代理後，將啟動用於將使用者註冊為裝置所有者的實用程式。 其他 — 該實用程式不可用。

KLNAGENT_DEVICEOWNER_LOGIN	否 是的，如果您輸入密碼	包含將註冊為裝置所有者的使用者登入資訊。	卡巴斯基安全管理中心 Linux 使用者清單中指定的使用者登入名稱。
KLNAGENT_DEVICEOWNER_PASSWORD	否 是的，如果您輸入登入名稱	包含將註冊為裝置所有者的使用者加密密碼。	使用者的密碼。

網路代理將在安裝卡巴斯基安全管理中心 Linux 期間解密指定的登入名稱和密碼，並且使用者將被註冊為裝置所有者。

當使用回應檔案以靜默模式安裝網路代理時，您也可以將使用者指定為裝置所有者。

在使用回應檔案以靜默模式安裝網路代理時將使用者指定為裝置所有者：

1. 將 KLNAGENT_DEVICEOWNER_REGISTRATION_START 參數新增至回應檔案並將其設為 1。
   安裝網路代理後，將啟動用於將使用者註冊為裝置所有者的實用程式。
2. 在用戶端裝置的命令列中輸入登入名稱和密碼。
   使用者將被指定為裝置所有者。

如果使用者包含在內部安全群組中，則登入名稱必須包含該使用者名稱。

如果使用者包含在 Active Directory 安全群組中，則登入名稱必須包含使用者名稱和網域名稱。

您必須輸入來自應用程式、基於時間的一次性密碼 (TOTP) 來進行雙因素驗證。

安裝網路代理後將使用者指派為 Linux 裝置所有者

允許使用者註冊為 Linux 裝置所有者：

1. 在卡巴斯基安全管理中心網頁主控台中，前往**軟體管理** → **安裝套件**。
   安裝套件清單開啟。
2. 點擊網路代理安裝套件。
   所選安裝套件的內容視窗開啟。
3. 在安裝套件內容視窗中，點擊**設定** → **進階**。
4. 在**將使用者註冊為裝置所有者（僅限 Linux）**區域中，開啟**允許在安裝網路代理後執行使用者註冊公用程式**選項，然後點擊**儲存**。

用於將使用者註冊為裝置所有者的實用程式可透過用戶端裝置上的命令列運行。

將使用者註冊為用戶端裝置上的 Linux 裝置所有者：

1. 在用戶端裝置的命令列中執行以下指令：
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner
   ```
2. 如果出現提示，請輸入登入名稱和密碼。
   如果登入名稱和密碼包含在網路代理的應答檔案或安裝套件中，請在用戶端裝置的命令列中執行以下指令：
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner -unattended
   ```

如果使用者包含在內部安全性群組中，則登入名稱必須包含該使用者名稱。

如果使用者包含在 Active Directory 安全群組中，則登入名稱必須包含使用者名稱和網域名稱。

您必須輸入來自應用程式、基於時間的一次性密碼 (TOTP) 來進行雙因素驗證。

使用者將被註冊為裝置所有者。

將使用者作為裝置所有者移除

在使用者端裝置上刪除作為裝置所有者的使用者：

1. 在用戶端裝置的命令列中執行以下指令：

   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -remove_owner
   ```

2. 輸入使用者名稱和密碼。

如果使用者包含在內部安全性群組中，則登入名稱必須包含該使用者名稱。

如果使用者包含在 Active Directory 安全群組中，則登入名稱必須包含使用者名稱和網域名稱。

您必須輸入來自應用程式、基於時間的一次性密碼 (TOTP) 來進行雙因素驗證。

使用者將自裝置所有者移除。

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 → 使用者和群組**，然後選擇**使用者**頁簽。

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**雙步驟驗證**頁籤。

4. 在**雙步驟驗證**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據和一次性安全碼，請選取**請求進行身分驗證來驗證是否有修改使用者帳戶的權限**選項。否則，請選取**允許使用者在不需要額外身分驗證的情況下修改此帳戶**選項。

5. 儲存變更。

設定雙步驟驗證

從管理伺服器版本 16.1 開始，雙因素驗證將自動啟用。不支援全域停用雙因素驗證的選項。此情景提供了在首次登入時配置雙因素驗證以及在管理伺服器上配置雙因素驗證設定的步驟。

階段

雙因素驗證的設定分階段進行：

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。

   在俄羅斯可用：

   - Bitrix24 OTP
   - Yandex ID
   - Avanpost 驗證器
   - Aladdin 2FA
   - Rutoken OTP

   全球皆可用（包括俄羅斯）：

   - Google Authenticator
   - Microsoft Authenticator

   要檢查卡巴斯基安全管理中心 Linux 是否支援要使用的身份驗證器應用程式，請為所有使用者或特定使用者啟用雙因素驗證。

   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 Linux 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身分驗證應用程式。

2. **將身分驗證器應用程式裝置上的時間與安裝了管理伺服器的裝置的時間同步**

   確保具有身分驗證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。為了提高準確性，我們建議在整個基礎設施中使用相同的NTP伺服器。否則，在設定雙因素驗證時可能會發生故障。

3. **為使用者帳號登入網頁主控台時設定雙因素驗證**

   登入網頁主控台並設定雙因素驗證。

   如果您無法設定雙因素驗證，請聯絡具有**一般功能：使用者權限**功能區中修改物件ACL權限且已設定雙因素驗證的使用者，將您的帳戶新增至雙因素驗證允許清單中。

4. **在管理伺服器上設定雙因素驗證設定**

如果您已設定雙步驟驗證並具有**一般功能**：**使用者權限**功能區域中修改物件ACL權限，則可以如下在管理伺服器上配置雙步驟驗證設定：

1. 檢視可在登入時設定雙步驟驗證的使用者清單：
   - 對於全新安裝管理伺服器 16.1的使用者：將所需使用者新增至雙因素驗證允許清單中，以便他們能夠在首次登入時設定雙因素驗證。
   - 要升級或恢復到管理伺服器16.1：查看雙因素驗證允許清單，並刪除不應有權存取管理伺服器的帳戶。
2. 排除不需要啟用雙因素驗證的使用者帳戶（可選）

   將使用者帳戶從雙因素驗證中排除，以便即使他們未設定雙因素驗證，也能登入管理伺服器。對於在身分驗證期間無法提供安全碼的整合帳戶，可能需要將帳戶從雙因素驗證中排除。整合帳戶用於透過OpenAPI執行指令碼。
3. 重設或刪除雙因素驗證密鑰（可選）

   當使用者無法存取其雙因素驗證裝置，或需要在新裝置上設定雙因素驗證時，您可以重設雙因素驗證密鑰。您也可以重設自己帳戶的密鑰。

   您可以刪除密鑰以完全阻止使用者登入網頁主控台並阻止其存取管理伺服器。
4. 編輯安全碼簽發者的名稱（可選）

   如果您有多個具有相似名稱的管理伺服器，則可能必須變更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。

結果

完成此情境後：

- 雙因素驗證設定適用於您自己的帳戶以及需要存取管理伺服器的其他使用者帳戶。
- 整合帳戶將排除在雙因素驗證之外。

關於帳戶的雙因素驗證

卡巴斯基安全管理中心 Linux 為卡巴斯基安全管理中心網頁主控台的使用者提供雙因素驗證。雙步驟身分驗證基於RFC 6238標準執行（TOTP：基於時間的一次性密碼演算法）。

每次登入卡巴斯基卡巴斯基安全管理中心網頁主控台時，您都需要輸入使用者名稱、密碼和一次性安全代碼。若要接收一次性安全碼，電腦或行動裝置上必須具有身分驗證器應用程式。

> 任何支援時效型一次性密碼演算法 (TOTP) 的身分驗證軟體都可以用作身分驗證應用程式，例如Google Authenticator。為了產生一次性安全碼，您必須將裝置上透過身分驗證應用程式設定的時間與管理伺服器裝置上設定的時間同步。為了提高準確性，我們建議在整個基礎設施中使用相同的NTP伺服器。

若要檢查卡巴斯基安全管理中心 Linux是否支援您要使用的身分驗證器應用程式，請嘗試使用此身分驗證器應用程式設定雙因素驗證。

其中步驟之一建議您指定由身分驗證應用程式產生的安全碼。如果成功，則 卡巴斯基安全管理中心 Linux 支援所選的身分驗證器。

使用身分驗證器應用程式產生密碼

驗證應用程式將產生安全碼，如下所示：

1. 管理伺服器會產生一個特殊的秘密金鑰和 QR 碼。

2. 您將產生的秘密金鑰或 QR 碼傳遞給驗證應用程式。

3. 驗證應用程式產生一次性使用的安全碼，您將其傳遞到管理伺服器的身分驗證視窗。

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。您可以變更安全碼簽發者名稱的名稱。安全碼簽發者名稱的預設值與管理伺服器的名稱相同。下次登入後，管理伺服器將被指派一個新的安全碼簽發者名稱。安全碼為一次性，有效期最長為 30 秒（具體時間可能會有所不同）。

> 強烈建議將秘密金鑰（或 QR 碼）儲存在安全的地方。如果您丟失了行動裝置，這將有助於您恢復對卡巴斯基安全管理中心網頁主控台的存取。

雙因素驗證具有以下功能：

- 從管理伺服器版本 16.1 開始，雙因素驗證將自動啟用，並且預設停用登入時配置雙因素驗證的選項。只有包含在雙因素驗證允許清單中的使用者才能設定登入時執行雙因素驗證。

- 使用者僅可以為其帳戶啟用雙步驟身分驗證。

- 使用者可以從雙因素驗證中排除帳戶。對於無法接收一次性身份驗證安全碼的整合帳戶來說，這可能是必要的。整合帳戶用於透過OpenAPI執行指令碼。

- 若要重新產生雙步驟身分驗證密鑰，使用者必須重設其自身帳戶的密鑰。

- 若要重設或刪除其他使用者帳戶的雙步驟身分驗證密鑰，該使用者必須擁有已設定雙步驟身分驗證的帳戶，並且在**一般功能**：**使用者權限**功能區域中擁有修改物件ACL權限。

- 若要將其他使用者的帳戶從雙因素驗證中排除，或修改雙因素驗證允許清單，使用者必須擁有已設定雙因素驗證的帳戶，並且在**一般功能**: **使用者權限**功能區域中擁有修改物件ACL的權限。

- 應該始終至少有一個使用者配置了雙因素驗證，以便該使用者可以管理雙因素驗證允許清單和排除清單。

- 雙步驟身分驗證僅在管理伺服器版本16.1中自動啟用。如果其他主管理伺服器或輔助管理伺服器執行的是16或更早版本，則它們的雙步驟身分驗證設定將保持不變。

- 虛擬管理伺服器會繼承實體管理伺服器的雙步驟身分驗證設定，因此，如果實體管理伺服器啟用了雙步驟身分驗證，虛擬管理伺服器也會啟用該功能。您無法在虛擬管理伺服器上配置雙步驟身分驗證設定。

- 要使雙步驟身分驗證正常運作，您需要將管理伺服器和網頁主控台升級到16.1或更高版本。

> 為了確保使用雙步驟身分驗證提供全面保護，不僅需要保護管理伺服器，還需要保護安裝該伺服器的裝置。為此，請參考強化指南建議。

在卡巴斯基安全管理中心網頁主控台登入時設定雙因素驗證秘密金鑰

首次登入卡巴斯基安全管理中心 Linux 16.1 或更高版本時，雙因素驗證配置視窗將開啟。

要為帳戶設定雙因素驗證，請執行以下操作：

1. 請在行動裝置或電腦上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 ID
   - Avanpost 驗證器
   - Aladdin 2FA
   - Rutoken OTP

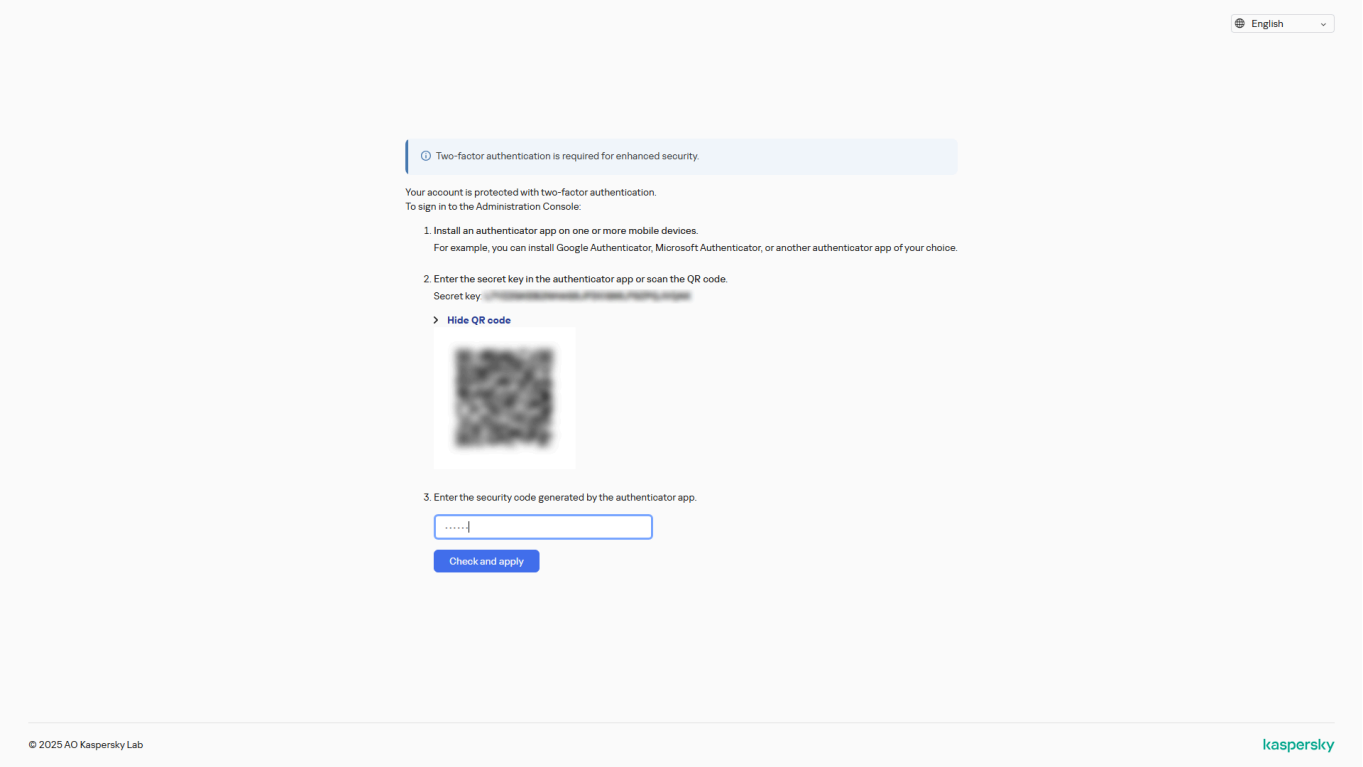
   > 我們強烈建議不要在與管理伺服器建立連線的同一台裝置上安裝身分驗證應用程式。

2. 確保具有身分驗證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。為了提高準確性，我們建議在整個基礎設施中使用相同的NTP伺服器。

3. 使用行動裝置或電腦上的身份驗證應用程式生成一次性安全碼。要這麼做，請執行以下操作之一：

   - 在身分驗證應用程式中手動輸入雙步驟身分驗證密鑰。
   - 點擊**檢視 QR 碼**並使用身分驗證器應用程式掃描 QR 代碼。

行動裝置上將顯示一個6位數的一次性安全碼。



在卡巴斯基安全管理中心網頁主控台登入時設定雙因素驗證秘密金鑰

4. 在開啟的**雙步驟驗證**視窗中，指定由身分驗證應用程式產生的安全碼，然後點擊**確認並套用**按鈕。

Rutoken OTP 設定

若您使用 Rutoken OTP，則需要一台已安裝 Rutoken OTP 應用程式的 Android 行動裝置。Android 行動裝置須滿足以下要求：

- 作業系統為 Android 7 或更新版本。
- NFC 模組可用且已啟用

在 Rutoken OTP 應用程式中，必須設定以下參數：

- 掃描雙步驟設定精靈中顯示的 QR 碼。
- 將時間間隔設定為 30 秒。
- 選取 SHA1 作為演算法。

若要設定 Rutoken OTP：

1. 將 Rutoken OTP 裝置放在有 NFC 模組的行動裝置旁。
2. 在 Rutoken OTP 應用程式中，按**連線權杖**。
3. 在 Rutoken OTP 應用程式中，按**配置設定**，然後按**儲存秘密金鑰**。

如果權杖成功連線到行動裝置，Rutoken OTP 應用程式將顯示下列狀態訊息：

- **權杖已連線。**
- **設定已配置。**
- **秘密金鑰已儲存。**

4. 在 Rutoken OTP 裝置上，按下按鈕。

   一個安全碼會安裝在裝置上。

5. 在卡巴斯基安全管理中心網頁主控台的雙步驟驗證視窗中，輸入安全碼。

至此，帳戶已完雙因素驗證設定。您可以根據您的權限存取管理伺服器。

> 如果您無法設定雙因素驗證，請聯絡在「**General features**: **一般功能**」功能區域中擁有使用者權限 權限且已設定雙因素驗證的使用者，將您的帳戶新增至雙因素驗證允許清單中。

允許使用者配置雙因素驗證

雙因素驗證允許清單是一份使用者清單，這些使用者可以在登入網頁主控台時對雙因素驗證進行初始設定。此清單包含未配置雙因素驗證的使用者帳戶。預設情況下，新使用者帳戶不包含在雙因素驗證允許清單中，這些帳戶必須由管理員新增至清單。如果新帳戶是用於執行OpenAPI指令碼的整合帳戶，則必須被從雙因素驗證中排除。

當使用者帳戶設定了雙因素驗證或被排除在雙因素驗證之外時，該帳戶將自動從雙因素驗證允許清單中刪除。

對於已設定雙因素驗證且在「**一般功能**: **使用者權限**」功能區域中擁有修改物件 ACL 權限的帳戶，可以手動修改雙因素驗證允許清單。

若要手動將使用者帳戶新增到雙因素驗證允許清單中：

1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在內容視窗的**雙步驟驗證**頁簽上，在**允許產生秘密金鑰的使用者**表中，按一下**新增**按鈕。

3. 在開啟的視窗中：

   a. 選取您要新增的使用者帳戶。

      只有未被排除在雙因素驗證之外且沒有雙因素驗證秘密金鑰的使用者才能被新增至允許清單。

   b. 如果帳戶受到防護以防止未經授權的修改，您必須確認您擁有變更此帳戶的權限。在**帳戶防護**視窗中，指定您自己的帳戶憑證和用於雙步驟驗證的一次性安全碼。

   c. 儲存變更。

   選定的使用者帳戶將新增到雙因素驗證允許清單中。下次登入時，用戶將能夠產生秘密金鑰。

在為使用者帳戶設定雙因素驗證之前，可以從雙因素驗證允許清單中刪除該帳戶。

手動從雙因素驗證允許清單中刪除使用者帳戶：

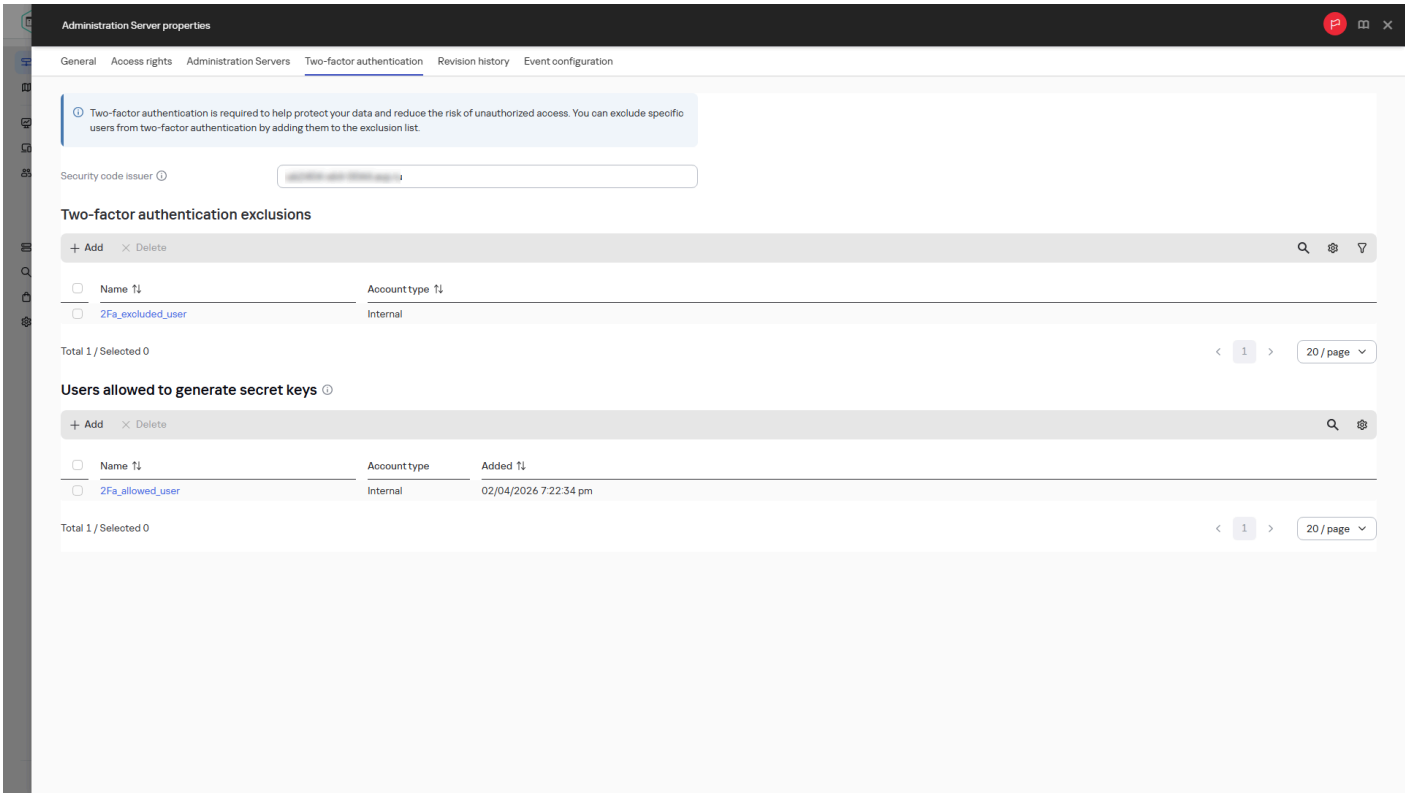
1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在內容視窗的**雙步驟驗證**頁籤上的**允許產生秘密金鑰的使用者**表中，選擇要刪除的使用者帳戶，然後按一下**刪除**。

3. 如果帳戶受到防護以防止未經授權的修改，您必須確認您擁有變更此帳戶的權限。在**帳戶防護**視窗中，指定您自己的帳戶憑證和用於雙步驟驗證的一次性安全碼。

選定的使用者帳戶將從雙因素驗證允許清單中刪除。



設定雙因素驗證允許清單

如果在管理伺服器上的活躍會話期間，您的雙因素身份驗證金鑰被其他使用者刪除，或者您自己重置金鑰但沒有建立新金鑰，則您將無法修改雙因素身份驗證允許清單。

使用者帳戶也可以自動新增到雙因素驗證允許清單或從中刪除。

為其他帳戶重設雙因素驗證秘密金鑰時，這些帳戶會自動新增到雙因素驗證允許清單中，以便產生新的秘密金鑰。

當您將管理伺服器從16或更早版本升級到16.1或更新版本，以及在管理伺服器16或更早版本上建立資料備份並將其還原到管理伺服器16.1或更新版本時，如果滿足以下所有條件，使用者帳戶將會自動新增至雙因素驗證允許清單：

- 使用者在功能區域*一般功能：基本功能*中擁有"讀取"權限，該權限被直接（而非透過安全性群組）指派給使用者。具有此權限的使用者角色範圍必須包含所有受管理和未指派的裝置，並且必須在管理伺服器層級設定。

- 使用者未被排除在雙因素驗證之外。

- 使用者沒有雙因素驗證秘密金鑰。
- 先前版本的管理伺服器上未對所有使用者啟用雙重身分驗證。

即使僅未滿足其中一項條件，使用者也無法新增到雙因素驗證允許清單中。

> 升級或還原後，我們建議確保允許清單僅包含必須有權存取管理伺服器的使用者帳戶。審核雙因素驗證允許清單，從中刪除任何其他帳戶。將用於透過 OpenAPI 執行指令碼的整合帳戶新增至排除清單中，以防止指令碼失敗。

如果滿足以下所有條件，則使用者帳戶在升級或恢復後將失去對管理伺服器的存取權限：

- 使用者在功能區*一般功能：基本功能*擁有透過安全性群組（不是直接指派給使用者）指派的“讀取”權限，或者根本沒有此權限。
- 使用者未被排除在雙因素驗證之外。
- 使用者沒有雙因素驗證秘密金鑰。
- 在先前版本的管理伺服器上已為所有使用者啟用雙因素驗證。

如有需要，可手動將這些帳戶新增至雙因素驗證允許清單中。

重置和刪除雙因素驗證秘密金鑰

當使用者無法存取其雙因素驗證裝置或需要在新裝置上設定雙因素驗證時，您可以重置秘密金鑰。重置秘密金鑰後，使用者可以再次登入網頁主控台並產生新的秘密金鑰。

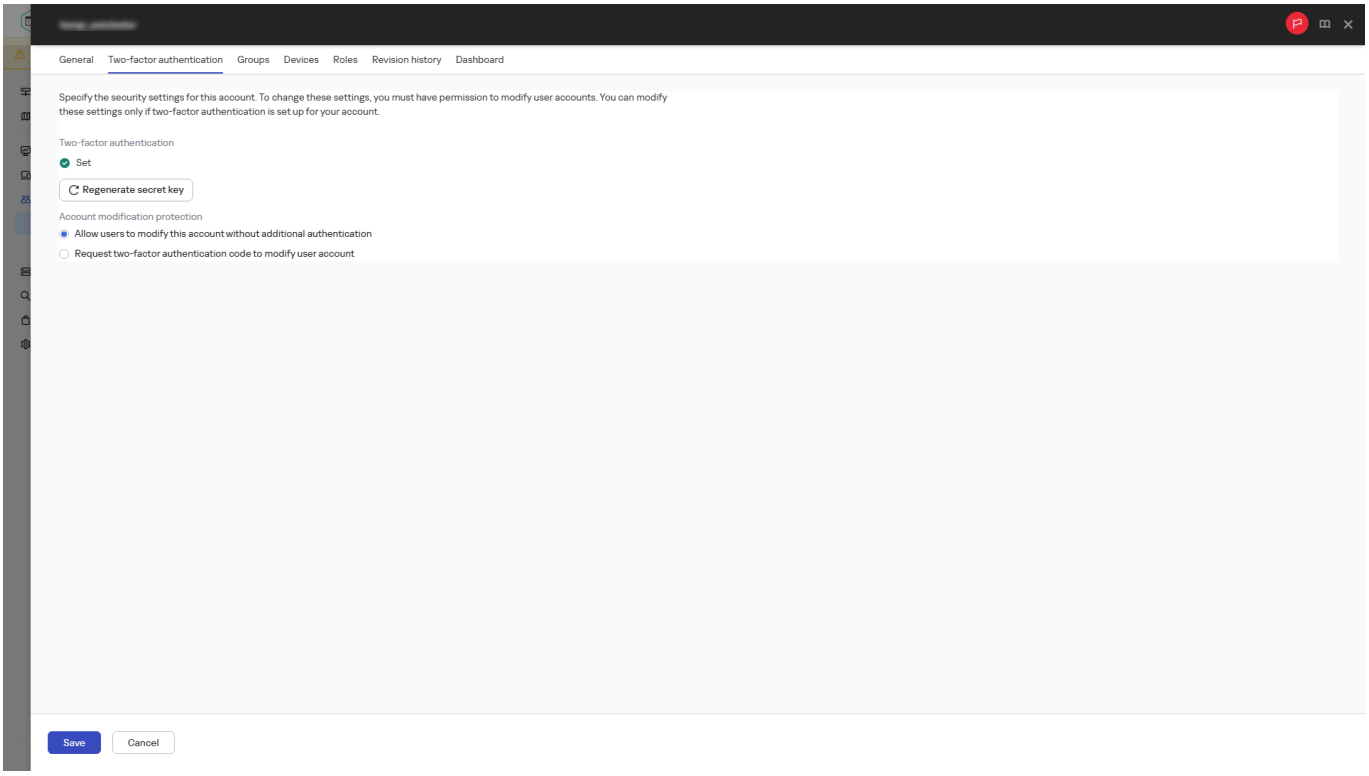
> 只有當您配置了雙因素驗證，並且在一般功能**一般功能**使用者權限**使用者權限修改物件 ACL**權限時，才能重置或刪除其他使用者帳戶的雙因素驗證秘密金鑰。您也可以重新產生自己的秘密金鑰。

重置帳戶的秘密金鑰：

1. 在主功能表中，轉至**使用者和角色 → 使用者和群組**，然後選擇**使用者**頁簽。
2. 按一下您要為其重置秘密金鑰的使用者帳戶名稱。

3. 如果您想重置帳戶的秘密金鑰：

a. 在**雙步驟驗證**頁簽上，按一下**重新產生秘密金鑰**按鈕。

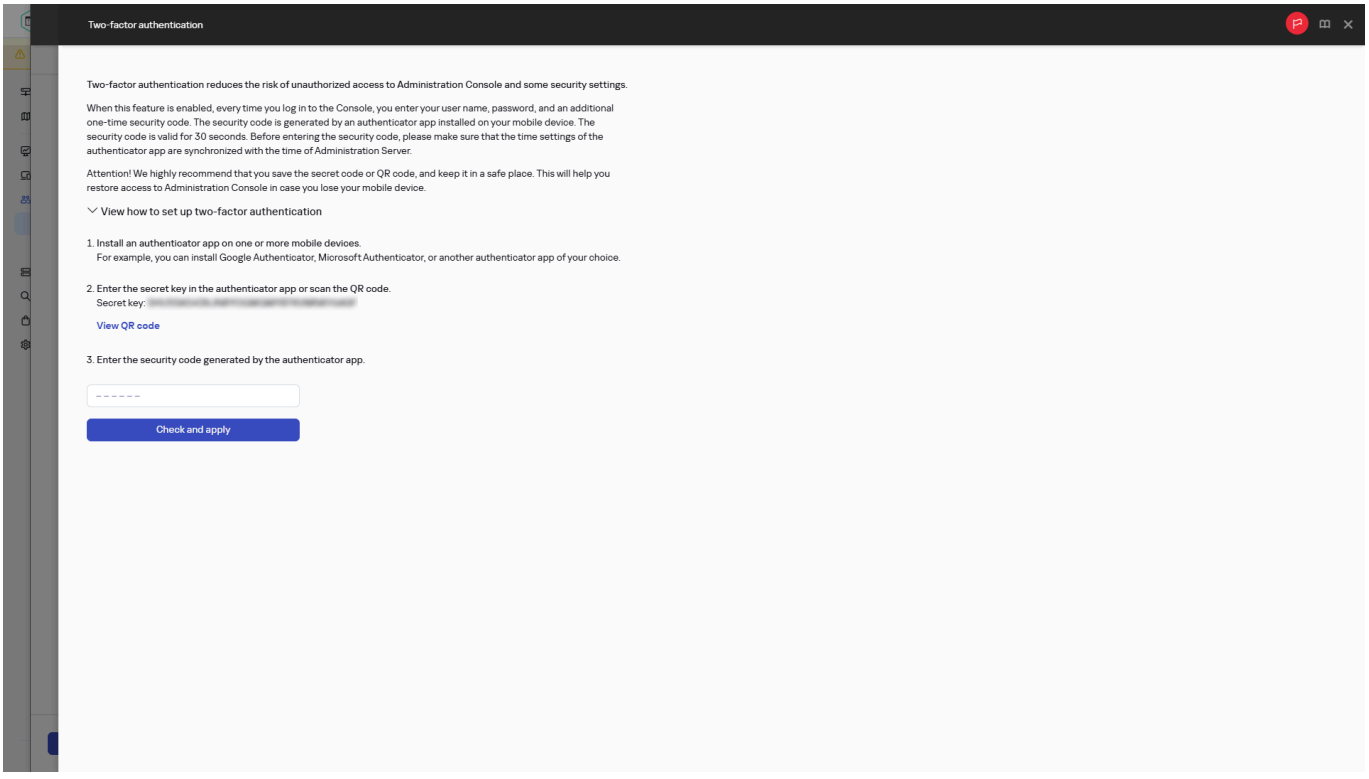


為目前使用者帳戶重新產生雙因素驗證秘密金鑰

a. 如果您的帳戶受到防護以防止未經授權的修改，您必須確認您擁有變更此帳戶的權限。在**帳戶防護**視窗中，指定您自己的帳戶憑據和雙因素驗證代碼。

b. 在**雙步驟驗證**視窗中，點擊**檢視設定雙步驟驗證的方式**，然後點擊**檢視 QR 碼**。

c. 使用行動裝置上的身分驗證器應用程式掃描 QR 代碼和接收一次性安全碼。



a. 在**雙步驟驗證**視窗中，指定由身分驗證器應用程式產生的一次性安全碼，點擊**確認並套用**按鈕，然後保存變更。

Rutoken OTP 設定

若您使用 Rutoken OTP，則需要一台已安裝 Rutoken OTP 應用程式的 Android 行動裝置。Android 行動裝置須滿足以下要求：

- 作業系統為 Android 7 或更新版本。
- NFC 模組可用且已啟用

在 Rutoken OTP 應用程式中，必須設定以下參數：

- 掃描雙步驟設定精靈中顯示的 QR 碼。
- 將時間間隔設定為 30 秒。
- 選取 SHA1 作為演算法。

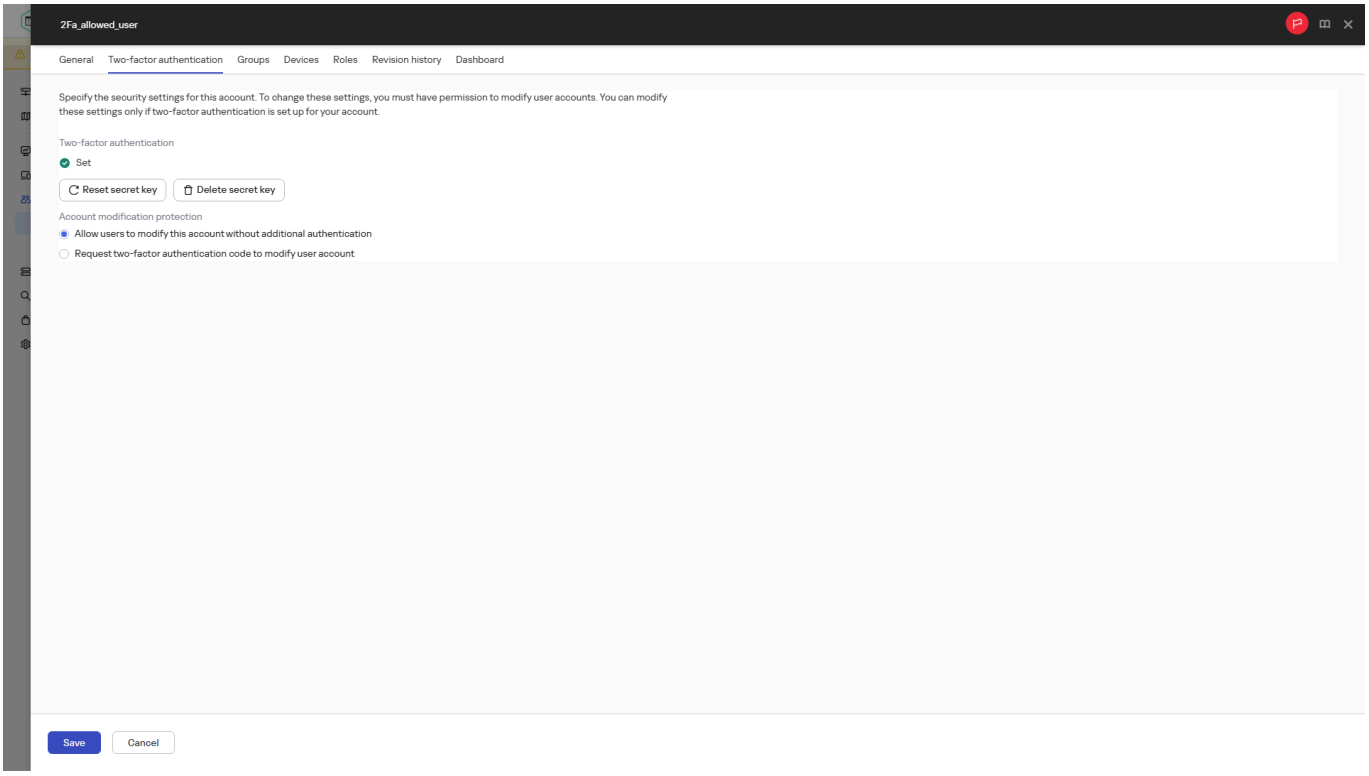
若要設定 Rutoken OTP：

1. 將 Rutoken OTP 裝置放在有 NFC 模組的行動裝置旁。
2. 在 Rutoken OTP 應用程式中，按**連線權杖**。
3. 在 Rutoken OTP 應用程式中，按**配置設定**，然後按**儲存秘密金鑰**。
   如果權杖成功連線到行動裝置，Rutoken OTP 應用程式將顯示下列狀態訊息：
   - **權杖已連線。**
   - **設定已配置。**
   - **秘密金鑰已儲存。**
4. 在 Rutoken OTP 裝置上，按下按鈕。
   一個安全碼會安裝在裝置上。
5. 在卡巴斯基安全管理中心網頁主控台的雙步驟驗證視窗中，輸入安全碼。

您的帳戶秘密金鑰已變更。

4. 如果您想重置其他帳戶的秘密金鑰：

   a. 在**雙步驟驗證**頁簽上，按一下**重設秘密金鑰**按鈕。



為其他使用者帳戶重設雙因素驗證秘密金鑰

   a. 如果帳戶受到防護以防止未經授權的修改，您必須確認您擁有變更此帳戶的權限。在**帳戶防護**視窗中，指定您自己的帳戶憑據和雙因素驗證的一次性安全代碼。

   b. 確認重置秘密金鑰，然後儲存變更。

   當為另一個帳戶重置秘密金鑰時，現有秘密金鑰將被刪除，並且使用者帳戶將被新增到「管理伺服器」內容中的雙因素身份驗證允許清單中。下次登入時，使用者將能夠產生新的秘密金鑰。

   使用者帳戶的秘密金鑰已重置。

您可以刪除密鑰以完全阻止使用者登入網頁主控台並阻止其存取管理伺服器。

若要刪除秘密金鑰：

1. 在主功能表中，轉至**使用者和角色 → 使用者和群組**，然後選擇**使用者**頁簽。

2. 按一下您要刪除其秘密金鑰的內部使用者帳戶名稱。

   > 您無法刪除自己帳戶的秘密金鑰。

3. 在**雙步驟驗證**頁簽上，按一下**刪除秘密金鑰**按鈕。

4. 如果帳戶受到防護以防止未經授權的修改，您必須確認您擁有變更此帳戶的權限。在**帳戶防護**視窗中，指定您自己的帳戶憑據和雙因素驗證的一次性安全代碼。

5. 確認刪除秘密金鑰，然後儲存變更。

使用者帳戶的秘密金鑰被刪除。

您可以透過在管理伺服器內容中將使用者新增至雙因素驗證允許清單中來還原存取權限。在此情況下，下次登入時，使用者將能夠產生新的秘密金鑰。

從雙因素驗證中排除帳戶

您可以將使用者帳戶排除在雙因素驗證之外，以允許他們登入管理伺服器，即使他們沒有設定雙因素驗證。對於在身份驗證期間無法提供一次性安全碼的整合帳戶，可能需要將帳戶排除在雙因素驗證之外。整合帳戶用於透過OpenAPI執行指令碼。

> 如果您的帳戶已設定雙步驟驗證，並且您在**一般功能**：**使用者權限**功能區中擁有修改物件ACL權限，則可以修改排除清單。

若要從雙因素驗證中排除使用者帳戶：

1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在內容視窗的**雙步驟驗證**選項卡上，在**雙步驟驗證排除項目**中，按一下**新增**按鈕。

3. 在開啟的視窗中：

   a. 選取您要排除的使用者帳戶。

   b. 如果帳戶受到防護以防止未經授權的修改，您必須確認您擁有變更此帳戶的權限。在**帳戶防護**視窗中，指定您自己的帳戶憑證和用於雙步驟驗證的一次性安全碼。

   c. 儲存變更。

   選定的使用者帳戶將被排除在雙因素驗證之外，並且如果存在，其密鑰將被刪除。在管理伺服器16.1上還原備份或將管理伺服器升級到16.1或更高版本時，排除的帳戶清單不會變更。如果排除清單中的帳戶在先前版本的管理伺服器中擁有密鑰，則這些密鑰將在16.1版本中刪除。

您可以從排除清單中刪除使用者帳戶，以完全阻止使用者登入網頁主控台並阻止使用者存取管理伺服器。

若要從排除清單中刪除使用者帳戶：

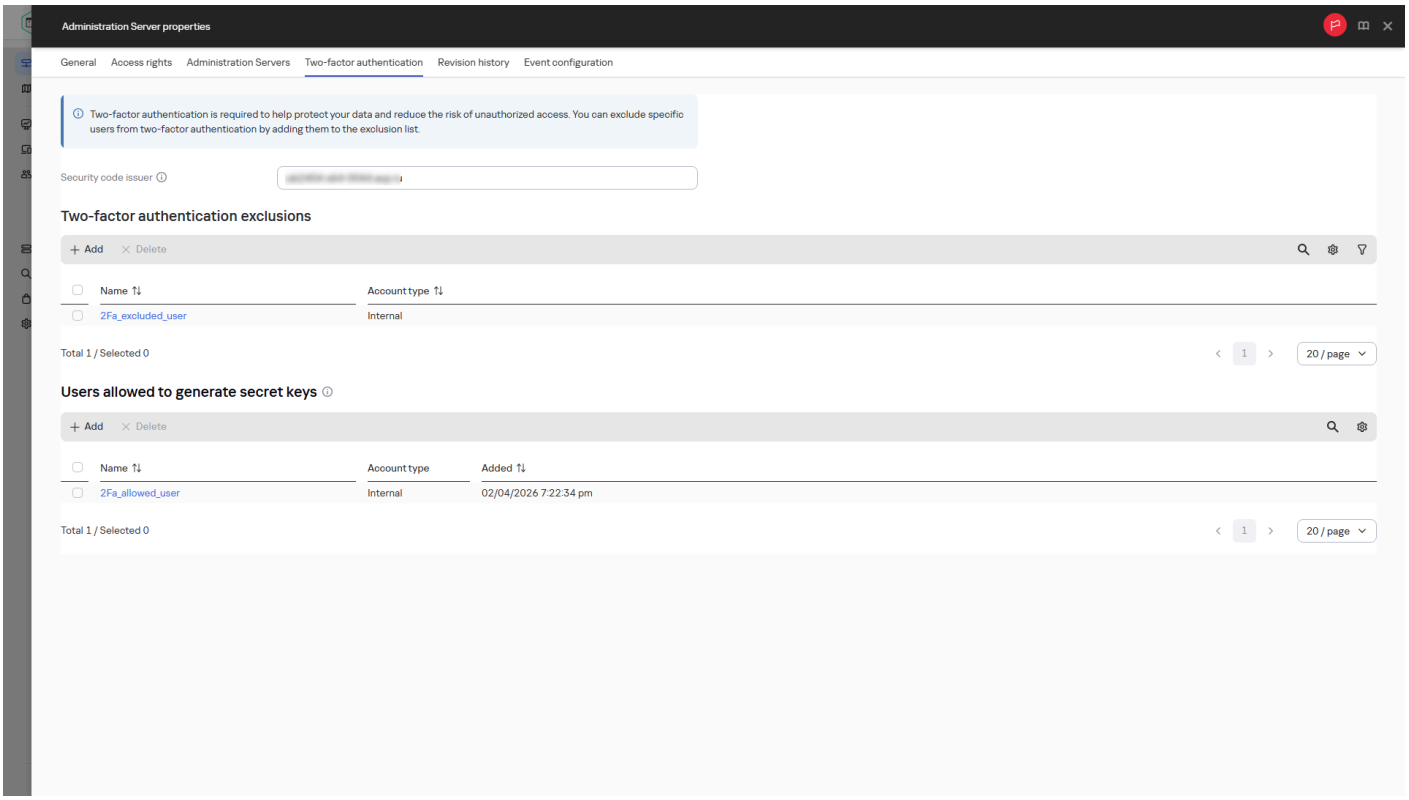
1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在內容視窗的**雙步驟驗證**頁籤上的**雙步驟驗證排除項目**表中，選擇要刪除的使用者帳戶，然後按一下**刪除**。

3. 如果帳戶受到防護以防止未經授權的修改，您必須確認您擁有變更此帳戶的權限。在**帳戶防護**視窗中，指定您自己的帳戶憑證和用於雙步驟驗證的一次性安全碼。

選定的使用者帳戶將從排除清單中移除。



設定雙因素驗證排除項目清單

編輯安全碼簽發者的名稱

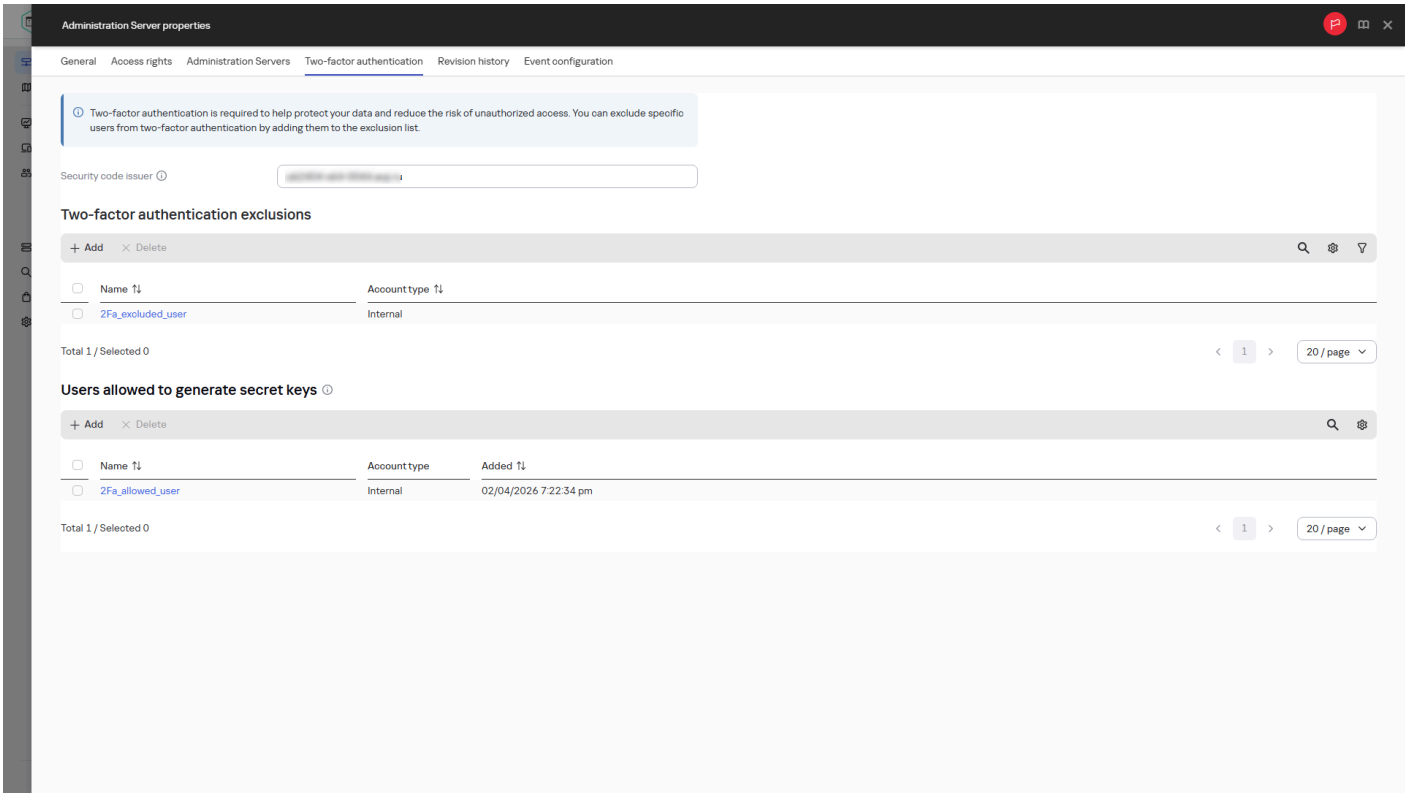
您可以為不同的管理伺服器使用多個識別碼（這稱為簽發者）。您可以更改安全碼簽發者的名稱以防萬一，例如，管理伺服器已經為另一台管理伺服器使用了類似的安全碼簽發者名稱。預設情況下，安全碼簽發者的名稱與管理伺服器的名稱相同。

若要指定安全碼簽發者的新名稱，請執行以下操作：

1. 在主選單中，按一下管理伺服器名稱。
   管理伺服器內容視窗將開啟。

2. 在內容視窗的**雙步驟驗證**頁籤中，在**安全碼簽發者**欄位中輸入新名稱，然後儲存變更。

下次登入後，新的安全碼簽發者名稱將指派給管理伺服器。



指定安全碼簽發者的名稱

變更允許的密碼輸入嘗試次數

卡巴斯基安全管理中心 Linux 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. 在管理伺服器裝置上，執行 Linux 命令行。

2. 對於 klscflag 實用程式，執行以下命令：

   ```
   sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n SrvSplPpcLogonAttempts -t d -v N
   ```

   其中 N 是嘗試輸入密碼的次數。

3. 要套用變更，請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。

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→使用者和群組**，然後選擇**使用者**或**群組**頁簽。
2. 選取您要刪除的使用者或安全群組旁邊的核取方塊。

   應該始終至少有一個使用者配置了雙因素驗證，以便該使用者可以管理雙因素驗證允許清單和排除清單。

3. 點擊**刪除**。
4. 在開啟的視窗中，點擊**正常**。

   使用者或安全群組被刪除。

變更使用者帳戶的密碼

如果目前密碼即將過期或您想將其變更為更安全的密碼，您可能需要變更您自己的帳戶或其他使用者帳戶的密碼。

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“.”。

變更您自己帳戶的密碼

若要編輯您的帳戶的密碼：

1. 在上方窗格中，按一下您的帳戶名稱以前往您的帳戶功能表。
2. 從下拉清單中，選擇**變更密碼**。
3. 在開啟的右側窗格中，輸入目前密碼，然後指定用於連線到卡巴斯基安全管理中心 Linux 的新密碼。

   若要查看輸入的密碼，請按一下 。
4. 如果您的帳戶受到防護以防止未經授權的修改，您必須確認您擁有變更此帳戶的權限。在**帳戶防護**視窗中，在**一般功能**：**使用者權限**功能區域中指定您自己的帳戶或具有修改物件 ACL 權限的帳戶的憑據。
5. 輸入身分驗證器應用程式在行動裝置上產生的一次性安全碼。

變更內部使用者帳戶的密碼

若要編輯內部使用者帳戶的密碼：

1. 在主功能表中，轉至**使用者和角色** → **使用者和群組**，然後選擇**使用者**頁簽。
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**頁簽上，按一下**變更密碼**按鈕。
4. 為連線到卡巴斯基安全管理中心 Linux 的使用者設定新密碼。

   若要查看輸入的密碼，請按一下 。
5. 如有必要，啟用**使用者必須在首次登入後更改密碼**選項以強制在下次進行使用者身分驗證時變更密碼。
6. 如果使用者帳戶受到防護以防止未經授權的修改，您必須確認您擁有變更此帳戶的權限。在**帳戶防護**視窗中，在**一般功能**：**使用者權限**功能區域中指定具有修改物件 ACL 權限的帳戶的憑據。
7. 輸入身分驗證器應用程式在行動裝置上產生的一次性安全碼。

配置使用伺服器標誌變更密碼的選項

您可以使用 klscflag 公用程式透過以下命令來設定變更密碼：

- 配置密碼輪換週期（`LP_SplPwdChangePeriodDays` 標誌）

  `klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangePeriodDays -t d -v <輪換週期>`

  其中 <輪換週期> 是使用者密碼過期之前的一段時間（以天為單位）。可能的值：0–730。如果該參數值為 0，則停用密碼輪換。

- 設定需要變更密碼的初步警告的時間（`LP_SplPwdChangeNotificationHours` 旗標）

  `klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangeNotificationHours -t d -v <警告時間>`

  其中 <警告時間> 是使用者密碼過期之前的一段時間（以小時為單位）。在此期間，將顯示有關需要變更密碼的通知。可能的值：0–17520。如果此參數值為 0，則警告時間為密碼輪換週期的25%。

- 指定「**使用者必須在首次登入後更改密碼**」選項的預設值（`LP_SplPwdForceChange`旗標）

  `klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdForceChange -t d -v <值>`

  其中 <值> 旗標的可能值：

  `1`：「**使用者必須在首次登入後更改密碼**」選項已啟用。

  `0`：「**使用者必須在首次登入後更改密碼**」選項已停用。

若要檢視目前標誌值，請執行下列命令：

`klscflag -fget -pv .core/.independent -s KLLIM -n <旗標> -t d`

其中 <旗標> 是 `LP_SplPwdChangePeriodDays`、`LP_SplPwdChangeNotificationHours` 或 `LP_SplPwdForceChange` 旗標。

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**正常**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→使用者和群組**，然後選擇**使用者**或**群組**頁簽。
2. 選取您要新增到使用者角色範圍的使用者或安全群組旁邊的核取方塊。
3. 點擊**指派角色**按鈕。
   角色分配精靈啟動。使用**下一步**按鈕進行精靈。
4. 在**選取角色**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**指派角色**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**指派角色**按鈕以關閉視窗。
8. 按一下**關閉**按鈕 (X) 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. 在主選單中，按一下管理伺服器名稱。
   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，然後套用並儲存變更。
   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**正常**。

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**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**指派到角色**。

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. 在主選單中，按一下管理伺服器名稱。

   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。

變更帳戶密碼

您可以變更本機帳戶密碼，例如，當使用者忘記本機帳戶密碼或執行排程的密碼變更時。

即使使用者尚未登入該帳戶，密碼變更也將套用。您也可以變更本機根帳戶的密碼。

> 此工作只能在 Linux 裝置上執行。

變更特定裝置上的本機帳戶密碼：

1. 在主功能表中，轉至 **工作**。

2. 點擊**新增**。

   新工作精靈啟動。

3. 在**工作類型**欄位中，選取**變更帳戶密碼（僅限 Linux）**。

4. 您可以選取以下其中一個方法：

   - **指派工作給管理群組**

     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，則工作內容視窗中不會顯示**安全**頁籤，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是從清單匯入位址**

  您可以指定您要為其分配工作的裝置的 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。

- **指派工作給裝置分類**

  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。

為指定裝置建立*變更帳戶密碼（僅限 Linux）*工作。如果您選擇了**指派工作給管理群組**選項，工作將是一個組工作。

5. 在**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。

   可用設定取決於在上一步中選擇的選項。

6. 在**輸入帳戶名稱和新密碼**步驟中，指定以下設定：

   - 在**帳戶名稱**欄位中，指定要變更密碼的帳戶名稱。

   - 在**新密碼**欄位中，指定將為上一個欄位中指定之帳戶設定的密碼。

     若要檢視您輸入的字元，請按住**顯示**按鈕。

   - 如有必要，請選取**設為一次性密碼（使用者必須在首次登入後變更密碼）**核取方塊。

     - **設為一次性密碼（使用者必須在首次登入後變更密碼）**

       如果選取此核取方塊，則系統會在使用者第一次登入後提示使用者設定新密碼。

       如果清除此核取方塊，則系統不會在使用者第一次登入後提示使用者設定新密碼。

       預設情況下已清空此方塊。

7. 在**完成工作建立**步驟中，點擊**完成**按鈕以建立工作並關閉精靈。

   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。在此視窗中，您可以檢查工作參數、修改它們或配置工作啟動排程（如有必要）。

8. 在工作清單中，選擇您建立的工作，然後點擊**開始**。

   或者，等候工作按照您在工作設定中指定的排程啟動。

變更帳戶密碼工作完成後，將變更指定裝置上指定本機帳戶的密碼。

> 為了確保能正確地操作更改帳戶密碼工作，您必須在使用者裝置上停用 SELinux。

撤銷本機管理員權限

您可以撤銷帳戶中的本機管理員權限。這為您提供了額外的使用者帳戶控制。例如，您可以在單次分配完成後撤銷本機管理員權限。

執行此工作時，將檢查指定的本機帳戶是否屬於本機管理員群組。這些群組是由網路代理政策設定定義。您可以在網路代理政策設定中自訂本機管理員群組清單。您也可以使用**特權裝置使用者報告（僅限 Linux）**檢查特權使用者帳戶清單。

> 此工作只能在 Linux 裝置上執行。

撤銷特定裝置上的本機管理員權限：

1. 在主功能表中，轉至 **工作**。
2. 點擊**新增**。

   新工作精靈啟動。
3. 在**工作類型**欄位中，選取**撤銷本機管理員權限（僅限 Linux）**。
4. 您可以選取以下其中一個方法：

   - **指派工作給管理群組**

     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，則工作內容視窗中不會顯示**安全**頁籤，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是從清單匯入位址**

     您可以指定您要為其分配工作的裝置的 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。

   - **指派工作給裝置分類**

     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。

   為指定裝置建立*撤銷本機管理員權限（僅限 Linux）*工作。如果您選擇了**指派工作給管理群組**選項，工作將是一個組工作。
5. 在**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。

   可用設定取決於在上一步中選擇的選項。
6. 在精靈的這個步驟中，您可以指定以下設定：

   - 在**作業模式**設定群組中，選擇操作模式：

     - **從所列帳戶中撤銷本機管理員權限**

       如果選取此選項，將撤銷指定本機帳戶中的本機管理員權限。

       預設情況下已選定此選項。

     - **從本機管理員權限撤銷中排除所列帳戶**

       如果選取此選項，除了指定帳戶以外，將撤銷所有本機帳戶中的本機管理員權限。

預設情況下未選定此選項。

- 指定本機帳戶：
  - 點擊**新增**。
  - 在開啟的視窗中，執行以下操作：
    - 在**帳戶名稱**欄位，指定本機帳戶的名稱。
    - 在**帳戶行動**設定群組中（僅在選取**從所列帳戶中撤銷本機管理員權限**選項時適用），選擇操作。
    - **保留帳戶**

      如果選取此選項，則在撤銷本機管理員權限後不會刪除本機帳戶。

      預設情況下已選定此選項。
    - **刪除帳戶**

      如果選取此選項，則無論本機帳戶是否具有本機管理員權限，都將刪除本機帳戶。

      預設情況下未選定此選項。

7. 在**完成工作建立**步驟中，點擊**完成**按鈕以建立工作並關閉精靈。

   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。在此視窗中，您可以檢查工作參數、修改它們或配置工作啟動排程（如有必要）。

8. 在工作清單中，選擇您建立的工作，然後點擊**開始**。

   或者，等候工作按照您在工作設定中指定的排程啟動。

撤銷本機管理員權限工作完成後，將撤銷指定裝置上指定本機帳戶的本機管理員權限。

設定 Kerberos 網域身分驗證

憑藉卡巴斯基安全管理中心 Linux，您可以透過 Kerberos 通訊協定使用網域身分驗證。透過網域身分驗證，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，而無需在公司網路上重新輸入密碼（單一登入）。

您必須先設定您的網域控制器以使用 Kerberos 並產生 keytab 檔案。有關更多資訊，請參閱網域控制器文件。

Microsoft Active Directory 支援 SCRIL（互動式登入需要智慧卡）。

為 FreeIPA 和 AldPro 產生 keytab 檔案

要產生 keytab 檔案，請執行以下操作：

1. 建立一個使用者帳戶，供 IAM 用於存取網域控制器。

2. 如果管理伺服器位於FreeIPA/AldPro網域之外，請新增DNS記錄項目和主機項目：

   `ipa dnsrecord-add <zoneName> <recordName> --a-rec <管理伺服器IP位址>`

```
ipa host-add --password=<password> <管理伺服器主機位址>
```

3. 為管理伺服器建立 HTTP 服務時，請指定 PAC 類型：

```
ipa service-add HTTP/<管理伺服器主機 FQDN>@<大寫的網域名稱> --ok-to-auth-as-delegate=true --pac-type PAD
```

4. 指定用於身分驗證的使用者帳戶：

```
ipa service-allow-retrieve-keytab HTTP/<管理伺服器主機位址>@<大寫的網域名稱> --user=<user>
```

5. 匯出 keytab 檔案：

```
ipa-getkeytab -s <網域控制器位址> -p HTTP/<管理伺服器主機位址>@<大寫的網域名稱> -k /tmp/h.keytab
```

為 Microsoft Active Directory 產生 keytab 檔案

要產生 keytab 檔案，請執行以下操作：

1. 建立一個使用者帳戶，供 IAM 用於與網域控制器通訊。

2. 為使用者帳戶啟用以下選項：

   - **使用者無法變更密碼**

   - **Kerberos AES 256 位元加密**

   您可以啟用「**密碼永不過期**」選項，避免每次密碼過期時重新簽發 keytab 檔案。

3. 為使用者帳戶新增服務主體名稱 (SPN)：

```
setspn -S HTTP/<管理伺服器主機 FQDN> <大寫的網域名稱>\<user>
```

4. 匯出 keytab 檔案：

```
ktpass -out C:\<folder>\<keytab檔名> -princ HTTP/<管理伺服器主機 FQDN>@<大寫的網域名稱> -mapuser <大寫的網域名稱>\<user> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass <password> -mapop set
```

為 Samba 產生 keytab 檔案

要產生 keytab 檔案，請執行以下操作：

1. 建立一個使用者帳戶，供 IAM 用於與網域控制器通訊：

```
samba-tool user add <user>
```

2. 將 SPN 新增到使用者帳戶：

```
samba-tool spn add HTTP/<管理伺服器主機 FQDN> <user>
```

3. 匯出 keytab 檔案：

```
samba-tool domain exportkeytab /tmp/file.keytab --principal=HTTP/<管理伺服器主機 FQDN>
```

設定 Kerberos 網域身分驗證

若要啟用 Kerberos 網域身分驗證：

1. 執行網域控制器輪詢。
2. 在主功能表中，轉至**設定** → **單一登入**。
3. 啟用**Kerberos 身分驗證**選項。
4. 上傳 keytab 檔案。
5. 為網域使用者指派可存取卡巴斯基安全管理中心網頁主控台的角色。
   至此，已為網域使用者啟用 Kerberos 網域身分驗證。

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 Linux 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 Linux 元件和安全應用程式

當您完成此情境，您可確保以下事項：

- 您的網路被最近的卡巴斯基軟體防護，包括卡巴斯基安全管理中心 Linux 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，請考慮手動更新卡巴斯基資料庫和軟體模組，或直接從卡巴斯基更新伺服器更新。

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**

   要為安全應用程式安裝更新，您有多種方案可用。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 Linux 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。

   操作說明：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 Linux 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。

   操作說明：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**已啟用**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。

5. **使用差異檔案最佳化更新過程（可選）**

   您可以使用以下差異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。

   如何使用 diff 檔案：使用 diff 檔案更新 Kaspersky 資料庫和軟體模組

6. **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，以提供對軟體模組和卡巴斯基資料庫（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。

7. **核准和拒絕受管理卡巴斯基應用程式的更新**

   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。如果受管理卡巴斯基應用程式更新需要檢視和接受最終使用者產品授權協議的條款，您需要先接受該條款。此後，更新可以被傳播到受管理裝置。您設定了*已拒絕*狀態的更新將不被安裝到裝置。若先前安裝了受管理應用程式的拒絕更新，卡巴斯基安全管理中心 Linux 將嘗試從所有裝置解除安裝該更新。

   核准和拒絕更新僅適用於安裝在 Windows 型和 Linux 型用戶端裝置上的網路代理和受管理卡巴斯基應用程式。不支援管理伺服器、卡巴斯基安全管理中心網頁主控台和管理 Web 外掛程式的無縫更新。

   操作說明：核准與拒絕軟體更新

   有時，網路代理更新後，您可能會被提示重新啟動受管理裝置。如果顯示所需重啟通知，按一下通知中的**檢視裝置**連接，選取要重新啟動的裝置旁的核取方塊，然後按一下**重新啟動**按鈕以完成網路代理更新。

結果

當方案完成時，卡巴斯基安全管理中心 Linux 被配置為在更新被下載至管理伺服器儲存區後更新卡巴斯基資料庫。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 Linux 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理裝置的安全級別。

- 已安裝的 Kaspersky 應用程式，包括卡巴斯基安全管理中心 Linux 元件和安全應用程式

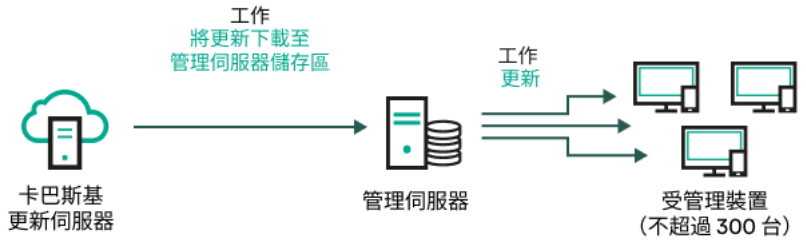
  卡巴斯基安全管理中心 Linux 可讓您自動更新安裝在 Windows 型和 Linux 型用戶端裝置上的網路代理和卡巴斯基應用程式。不支援管理伺服器、卡巴斯基安全管理中心網頁主控台和管理 Web 外掛程式的無縫更新。若要更新這些元件，您必須從卡巴斯基網站下載最新版本，然後手動安裝它們。

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 Linux 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）。



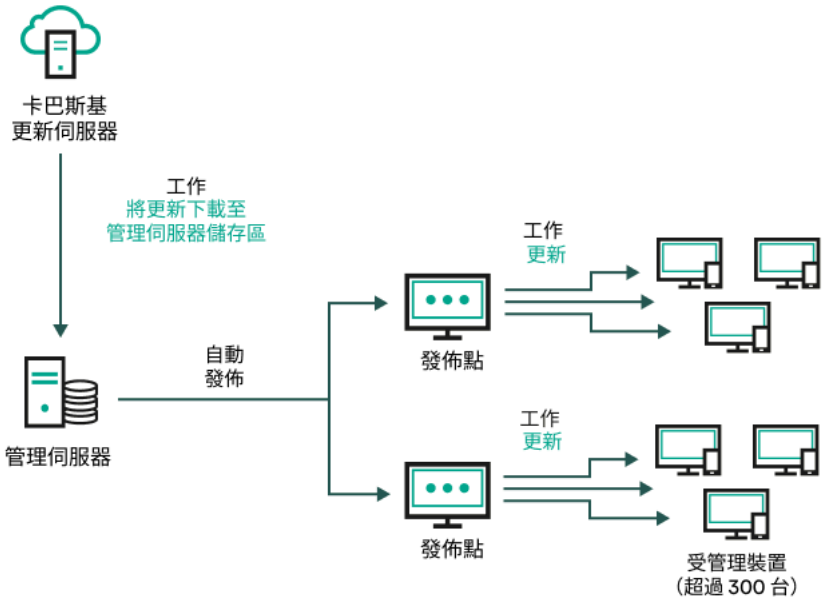
使用*將更新下載至管理伺服器儲存區*工作在沒有發佈點狀態下更新

作為更新來源，您不僅可以使用卡巴斯基更新伺服器，還可以使用本機或網路資料夾。

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 300 台或更多受管理裝置，或您的網路由多個網段組成，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*工作搭配發佈點更新

當*將更新下載至管理伺服器儲存區*工作完成後，Kaspersky Endpoint Security 的卡巴斯基資料庫和軟體模組的更新將下載到管理伺服器儲存區。這些更新透過 Kaspersky Endpoint Security 的*更新*工作安裝。

> *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。

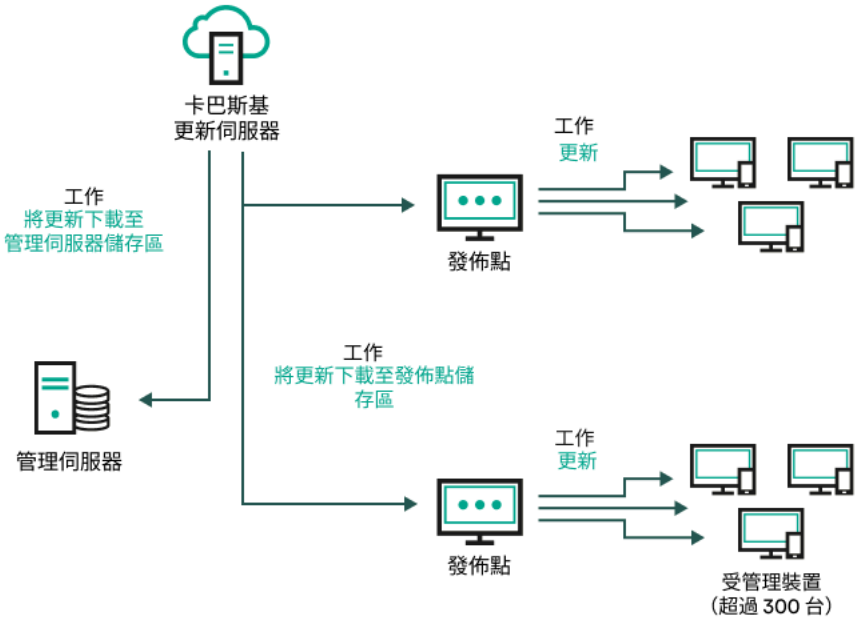
每個 Kaspersky 應用程式都從管理伺服器請求所需更新。管理伺服器集合這些更新並僅下載應用程式請求的更新。這確保了相同更新不被下載多次，且不必要更新不被下載。當執行*將更新下載至管理伺服器儲存區*工作時，管理伺服器自動傳送以下資訊到 Kaspersky 更新伺服器以便確保相關版本的 Kaspersky 資料庫和軟體模組的下載：

- 應用程式 ID 和版本
- 應用程式啟動 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

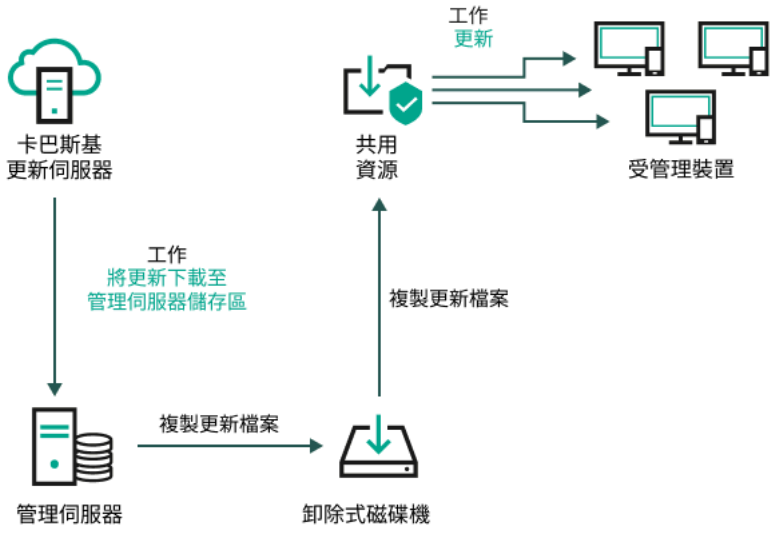
> 預設下，管理伺服器和發佈點與 Kaspersky 更新伺服器通訊並使用 HTTPS 協定下載更新。您可以配置管理伺服器和/或發佈點使用 HTTP 協定，而不是 HTTPS。

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。

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 Linux 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）。



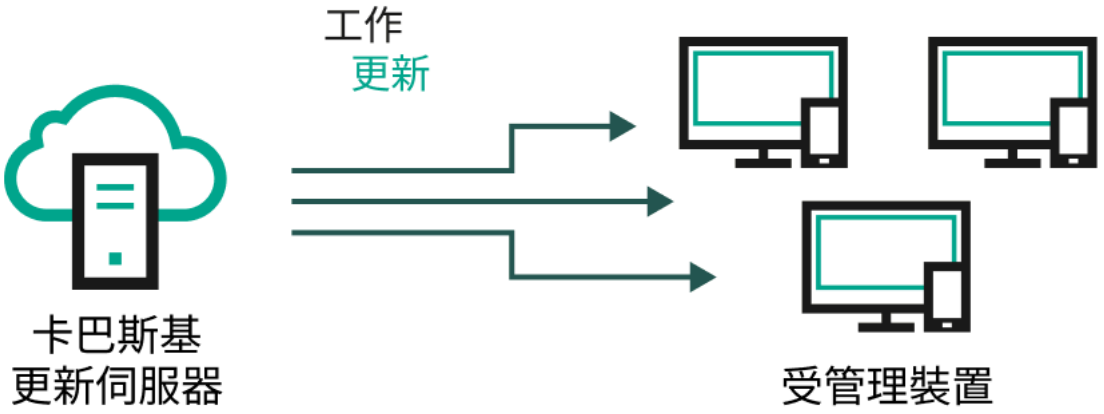
透過本機資料夾、共用資料夾或 FTP 伺服器更新

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 Linux 說明
- Kaspersky Endpoint Security for Windows 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 Linux 提供的儲存區。要直接從卡巴斯基更新伺服器接收更新，在安全應用程式中指定卡巴斯基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 Linux 說明
- Kaspersky Endpoint Security for Windows 說明

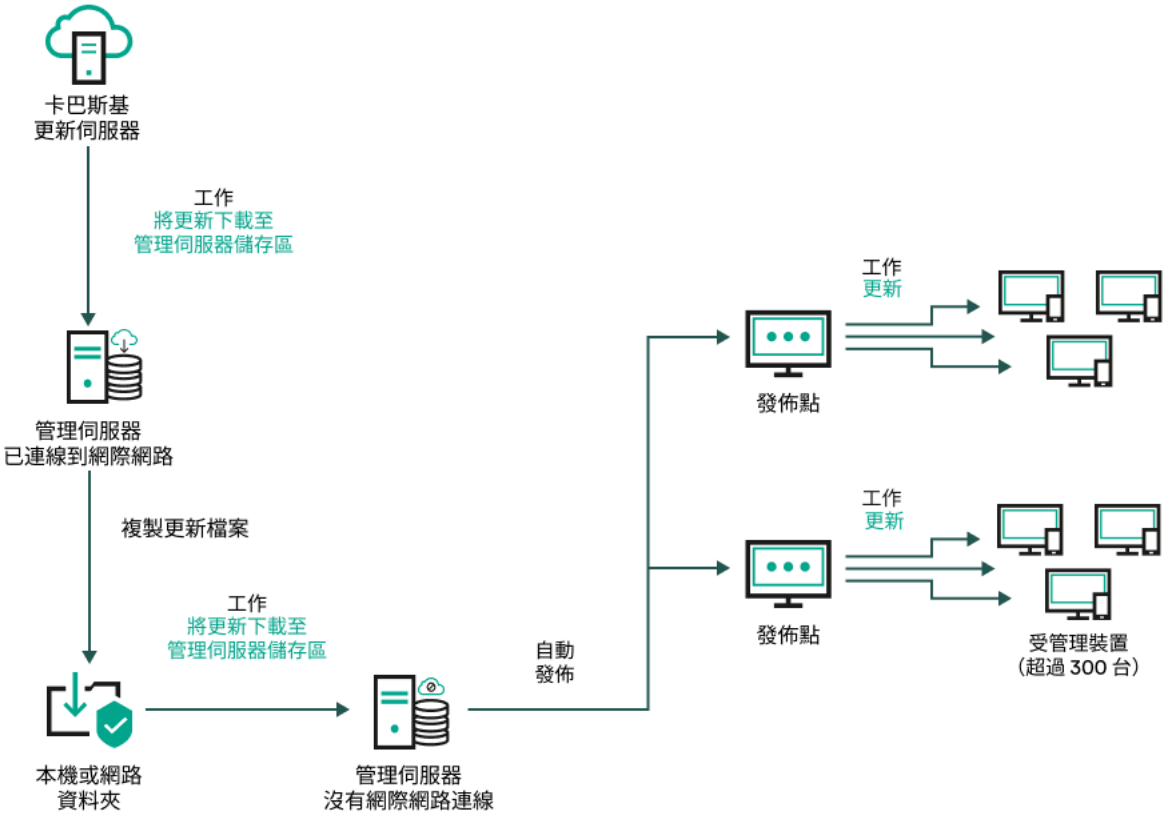
如果管理伺服器沒有網際網路連線，則透過本機或網路資料夾

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。如有必要，您還可以設定*自動下載更新請求檔案*選項，以便卡巴斯基更新實用程式僅下載所需的更新。

建立「將更新下載至管理伺服器儲存區」工作

*將更新下載至管理伺服器儲存區*工作可讓您將 Kaspersky Endpoint Security for Linux 的資料庫和軟體模組更新從卡巴斯基更新伺服器下載到管理伺服器儲存區。

卡巴斯基安全管理中心快速啟動精靈會自動建立管理伺服器的的*將更新下載至管理伺服器儲存區*工作。在工作清單中，只能有一個*將更新下載至管理伺服器儲存區*工作。如果該工作已被從管理伺服器的工作清單中刪除，您可以再次建立該工作。

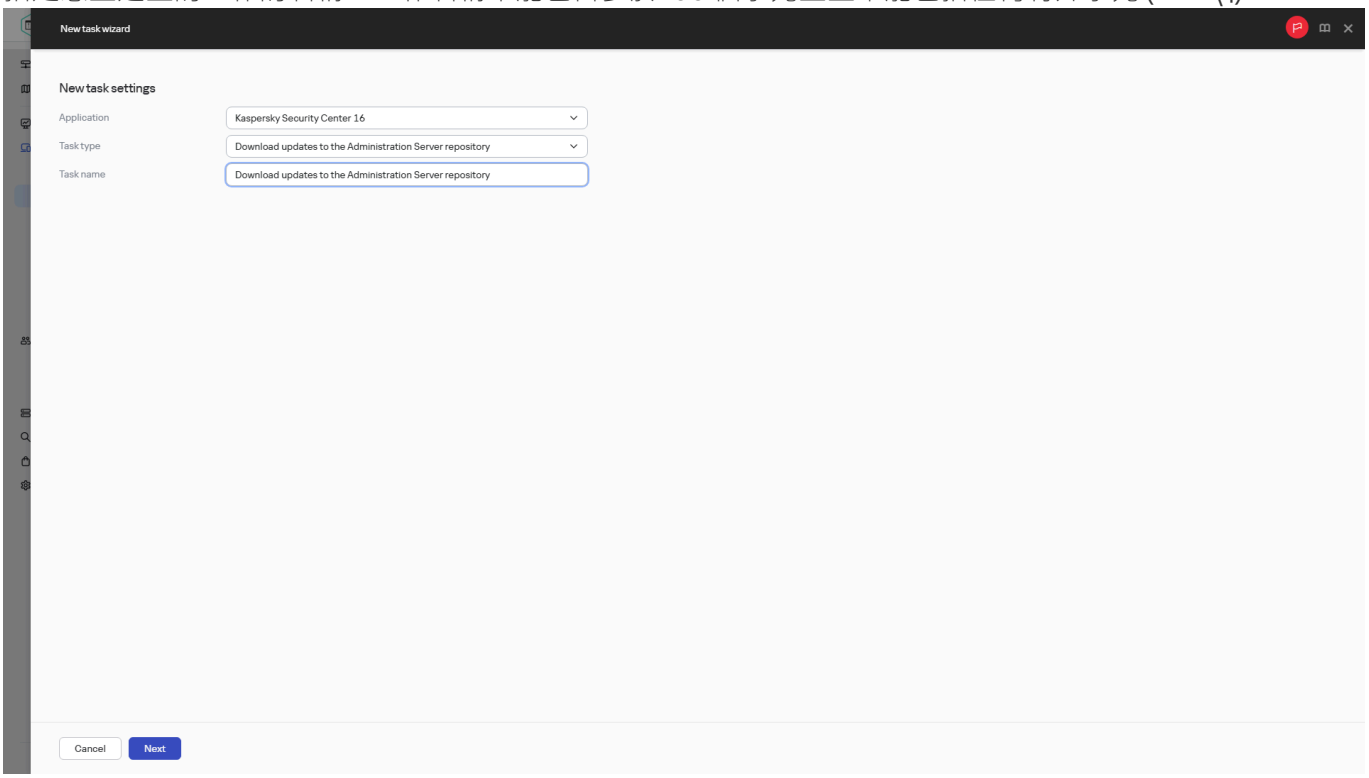
*將更新下載至管理伺服器儲存區*工作完成和更新被下載後，它們可以被傳播到受管理裝置。

> 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：

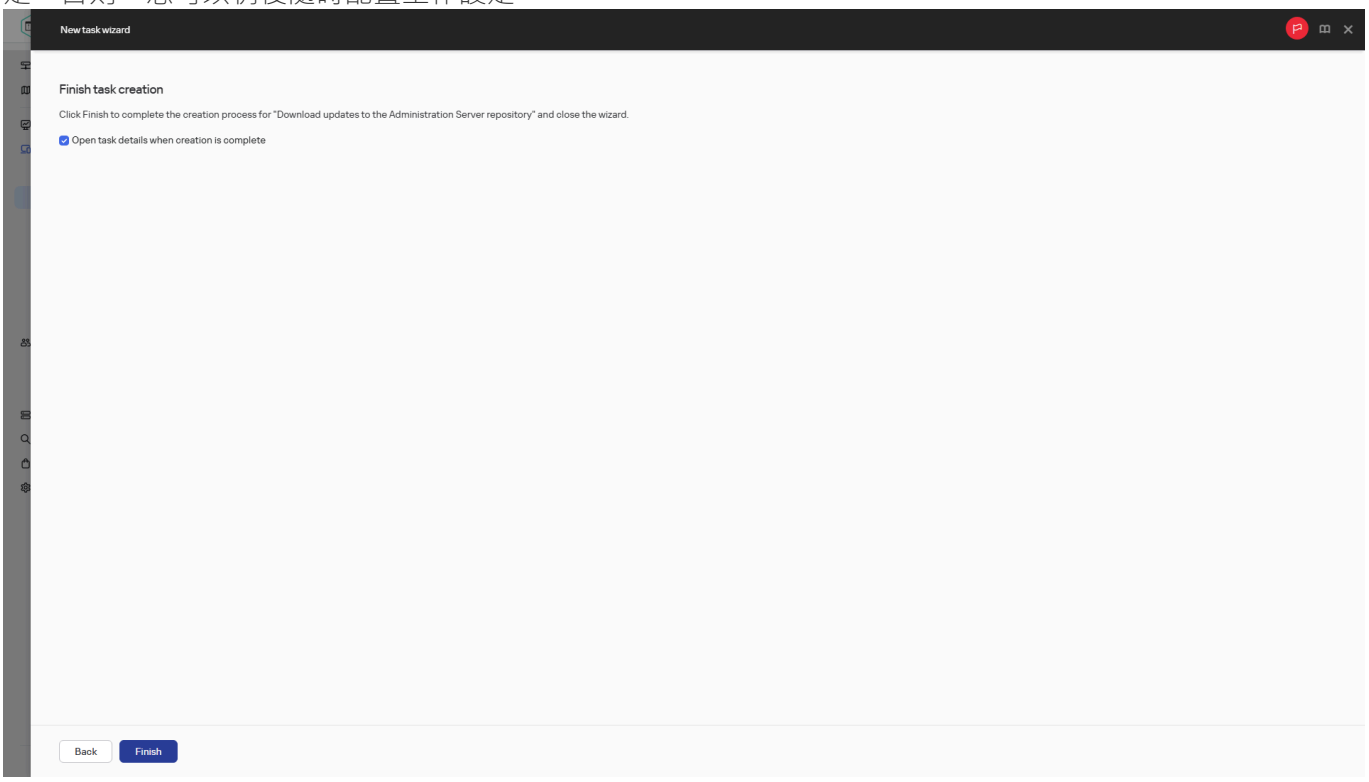
1. 在主功能表中，轉至 **工作**。
2. 點擊**新增**。

   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 ("*<>?\:|)。



建立「將更新下載至管理伺服器儲存區」工作

5. 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**選項以開啟工作內容視窗並修改預設工作設定。否則，您可以稍後隨時配置工作設定。



完成工作建立

6. 點擊**完成**按鈕。

   工作被建立並顯示在工作清單。

7. 點擊建立的工作名稱以開啟屬性視窗。

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**

     作為更新來源，您可以使用：

     - 卡巴斯基更新伺服器（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。

       在選取本機資料夾時，必須在安裝有管理伺服器的裝置上指定一個資料夾。資料夾路徑取決於裝置的作業系統。由於本機資料夾位於基於 Linux 的管理伺服器上，因此您必須指定 POSIX 路徑。例如 /path/to/dir。

       在選取 SMB 網路資料夾作為更新來源時，請先將該資料夾掛載到安裝管理伺服器的裝置上，然後再選取該資料夾。然後使用其本機檔案系統路徑，指定已掛載資料夾的路徑。透過 SMB 通訊協定提供對該資料夾的存取。

用作更新來源的本機或網路資料夾，或 FTP 或 HTTP 伺服器，必須包含與卡巴斯基更新伺服器上的資料夾結構相符的資料夾結構。您可以使用Kaspersky Update Utility取得此結構。

在*將更新下載至管理伺服器儲存區*工作和*將更新下載至發佈點的儲存區*工作中，如果您選擇受密碼防護的本機或網路資料夾作為更新來源，則使用者身分驗證不起作用。要解決此問題，首先掛接受密碼防護的資料夾，然後指定所需的憑據，例如，透過作業系統。之後，您可以選擇此資料夾作為更新下載工作中的更新來源。卡巴斯基安全管理中心 Linux 不會要求您輸入憑據。

- **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。

- **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。

  如果選擇將下載的更新複製到本機資料夾，則必須在已安裝管理伺服器的的裝置上指定資料夾。資料夾路徑取決於裝置的作業系統。由於本機資料夾位於基於 Linux 的管理伺服器上，因此您必須指定 POSIX 路徑。例如 /path/to/dir。

  選取位於基於 Linux 的管理伺服器上的網路資料夾時，必須事先透過掛載該資料夾，來確保安裝有管理伺服器的裝置可以存取該網路資料夾。存取資料夾將透過 SMB 通訊協定實現。

  預設情況下已停用該選項。

- **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 Linux 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 Linux

  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，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。

- **自動下載更新請求檔案**

  如果您想要卡巴斯基更新實用程式僅下載具有適當配置的所需更新，請啟用此選項並指定 卡巴斯基安全管理中心 Linux 將建立更新請求檔案的路徑，其中包含有關要下載的更新的資訊。更新請求檔案包含用於版本控制的時間戳記和 MD5 雜湊。

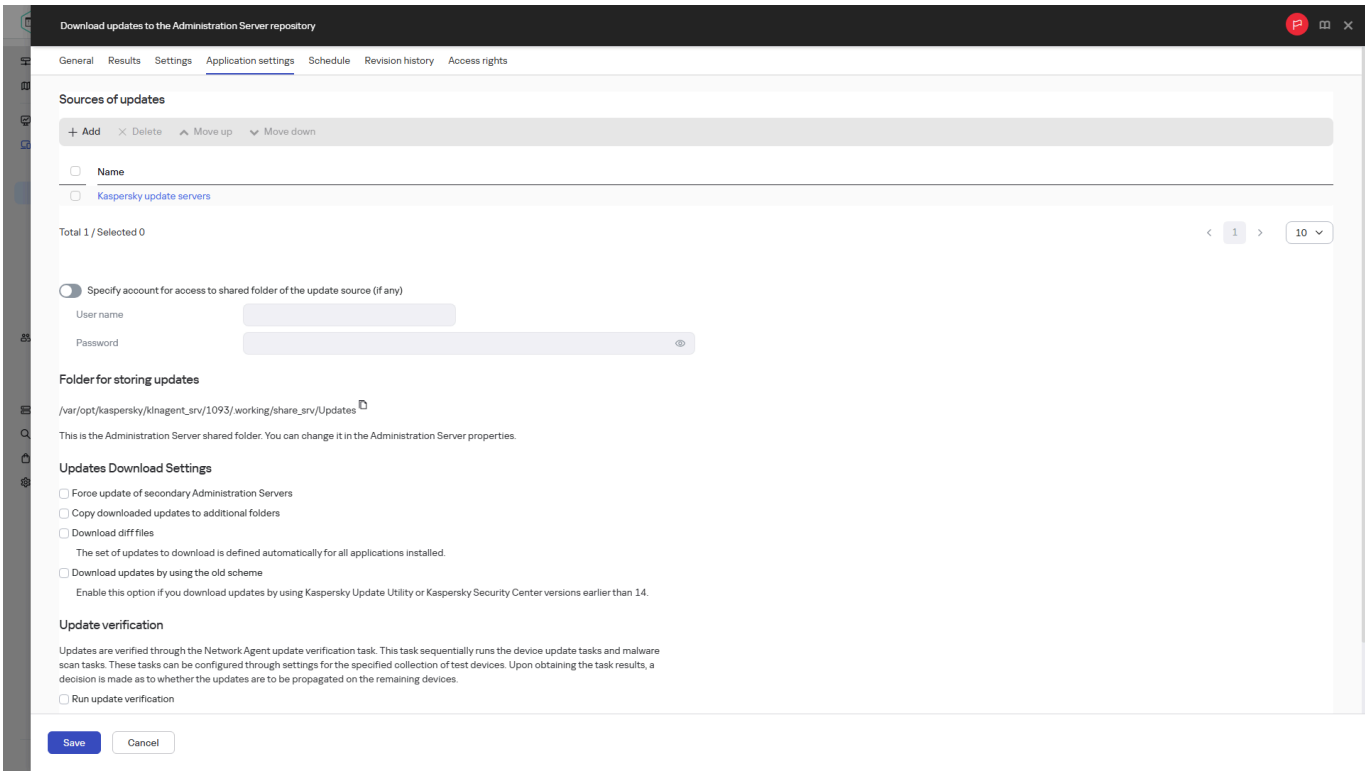
  請確保**使用舊配置下載更新**選項已停用。

  此外，還必須配置卡巴斯基更新實用程式中的更新下載。

  預設指定以下路徑：/var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/retranslation_request.xml。如有必要，您可以變更預設名稱（retranslation_request）和路徑。

  > 請求檔案可以放在本機或共用資料夾中。使用共用資料夾時，您必須確保可疑從安裝了管理伺服器的裝置存取該資料夾。確保存取的方法和使用的工具取決於您的基礎架構。

  執行*將更新下載到管理伺服器儲存區*工作時，卡巴斯基安全管理中心 Linux 會在您指定的路徑下建立 .xml 格式的更新請求檔案。卡巴斯基更新實用程式會自動從請求檔案中獲取資訊，然後僅下載所需的更新。如果卡巴斯基更新實用程式無法自動取得資訊（例如，卡巴斯基更新實用程式無法存取卡巴斯基安全管理中心 Linux 在其中建立請求檔案的資料夾），您必須使用第三方工具傳輸該檔案。



指定"將更新下載至發佈點儲存區"工作的內容

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：

- **開始工作**:

  - **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 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。

  - **按每週中的指定日**

    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。

- **每月於選定的週間日**

  工作定期在指定月日的指定時間執行。

  預設情況下，開始時間為18:00，且未選擇當月的任何日期。

  > 請注意，您選擇的是當月的週幾，而不是特定的日期或週數（例如，當月的第一週或第二週）。例如，如果您將遊標放在**週二**行的**第一**單元格中，則表示該工作將在每個月的第一個星期二執行。

  您可以選擇一週中的多個日期。

- **在完成其它工作時**

  目前工作在其他工作完成後啟動。只有在將這兩項工作指派給相同的裝置時，此選項才會發揮作用。例如，您可能想使用**開啟裝置**選項執行*受管理裝置*工作，完成後，請執行*病毒掃描*工作作為觸發工作。

  您必須從表格中選擇觸發工作以及此工作必須完成的狀態（**成功完成**或**失敗**）。

  如有需要，您可以對表格中的工作進行搜尋、排序和篩選，如下所示：

  - 在搜尋欄位中輸入工作名稱，可依其名稱搜尋工作。
  - 點擊排序圖示，可依名稱對工作進行排序。

    預設情況下，工作會依字母遞增排序。
  - 點擊篩選器圖示，在開啟的視窗中依群組篩選工作，然後點擊**套用**按鈕。

- 其它工作設定：

  - **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化延遲**

    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。

- **對於在以下間隔內啟動的工作，使用工作啟動自動隨機化延遲**

  如果該選項被啟用，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。

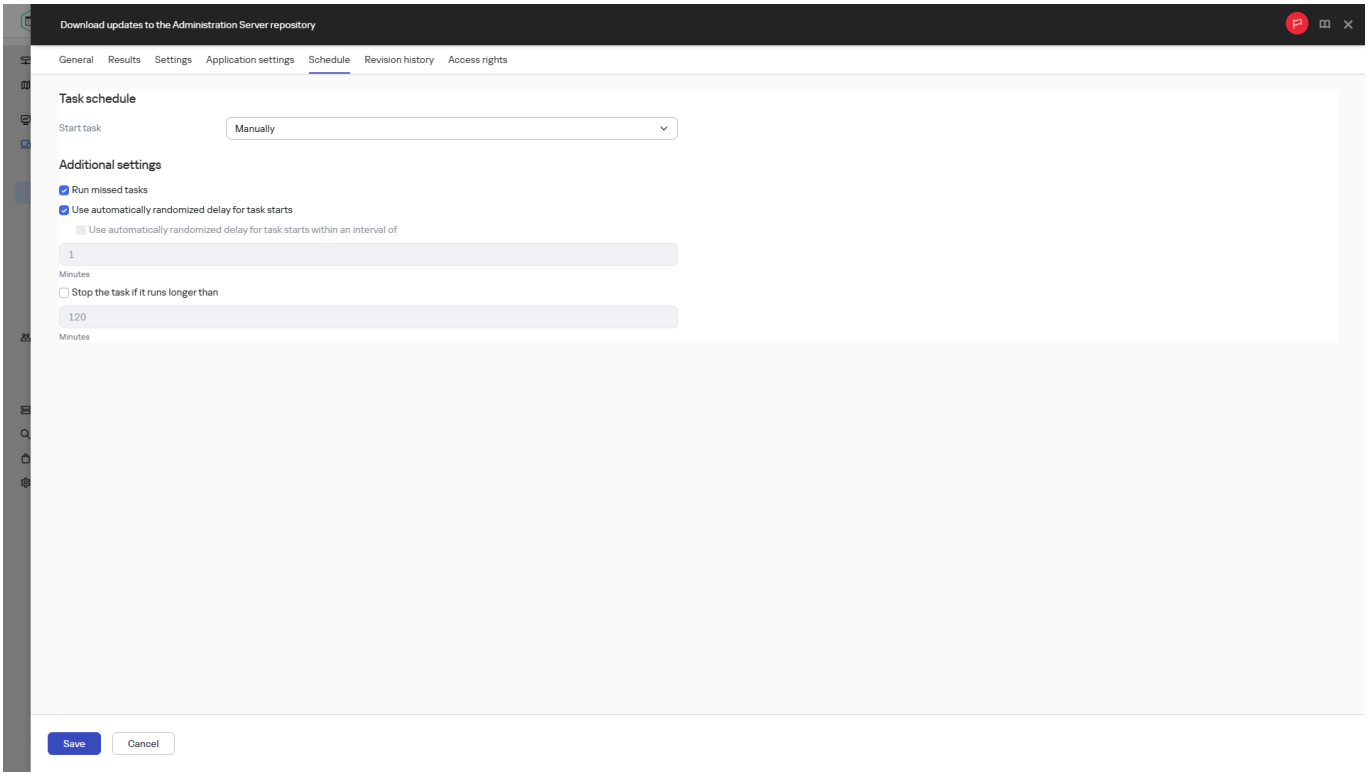
  預設情況下已停用該選項。預設時間間隔為一分鐘。

- **停止工作，若執行時間超過**

  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。

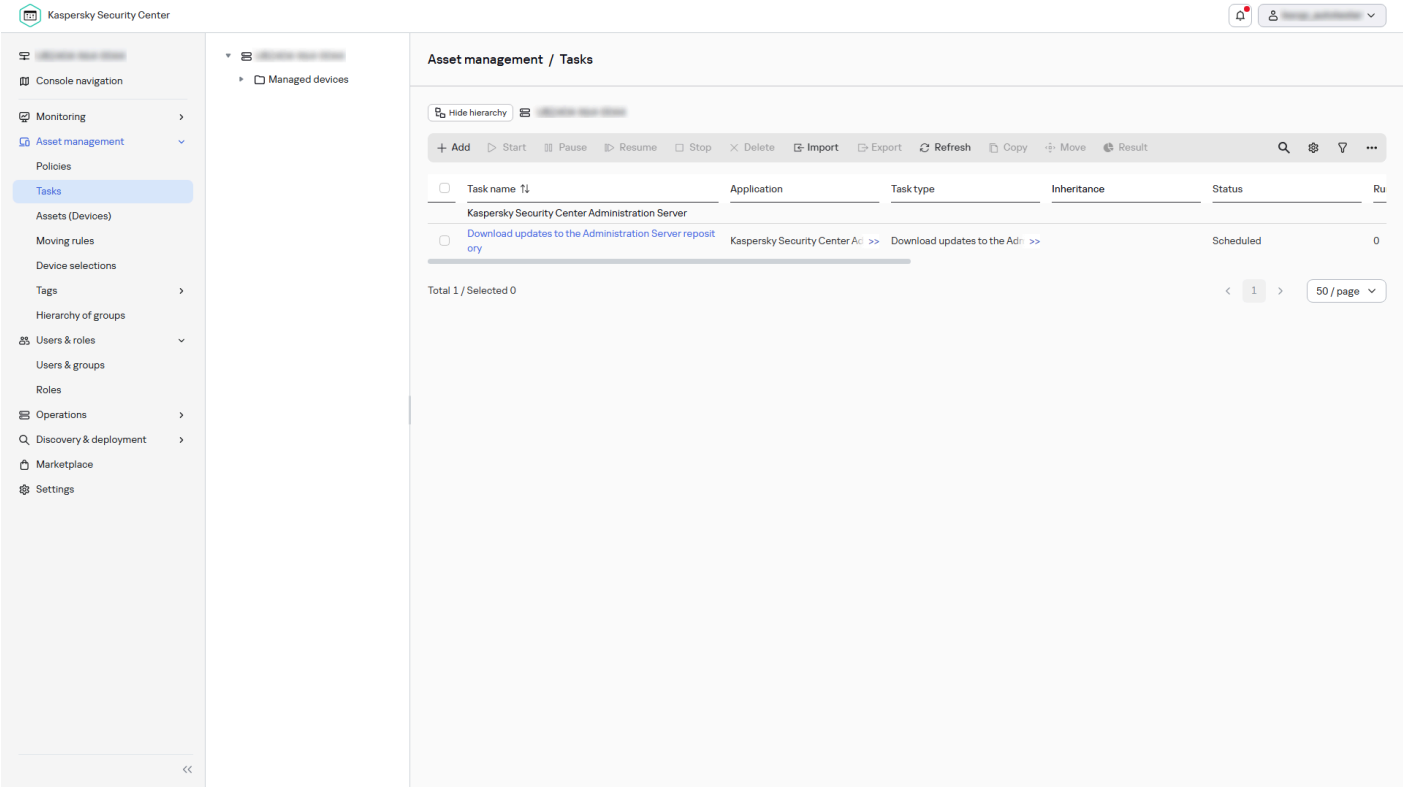
  預設情況下已停用該選項。預設工作執行時間是 120 分鐘。



指定“將更新下載至發佈點儲存區”工作的排程

10. 點擊**儲存**按鈕。

工作被建立和配置。



工作清單

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 Linux 支援的應用程式（例如 Kaspersky Endpoint Security for Linux）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。

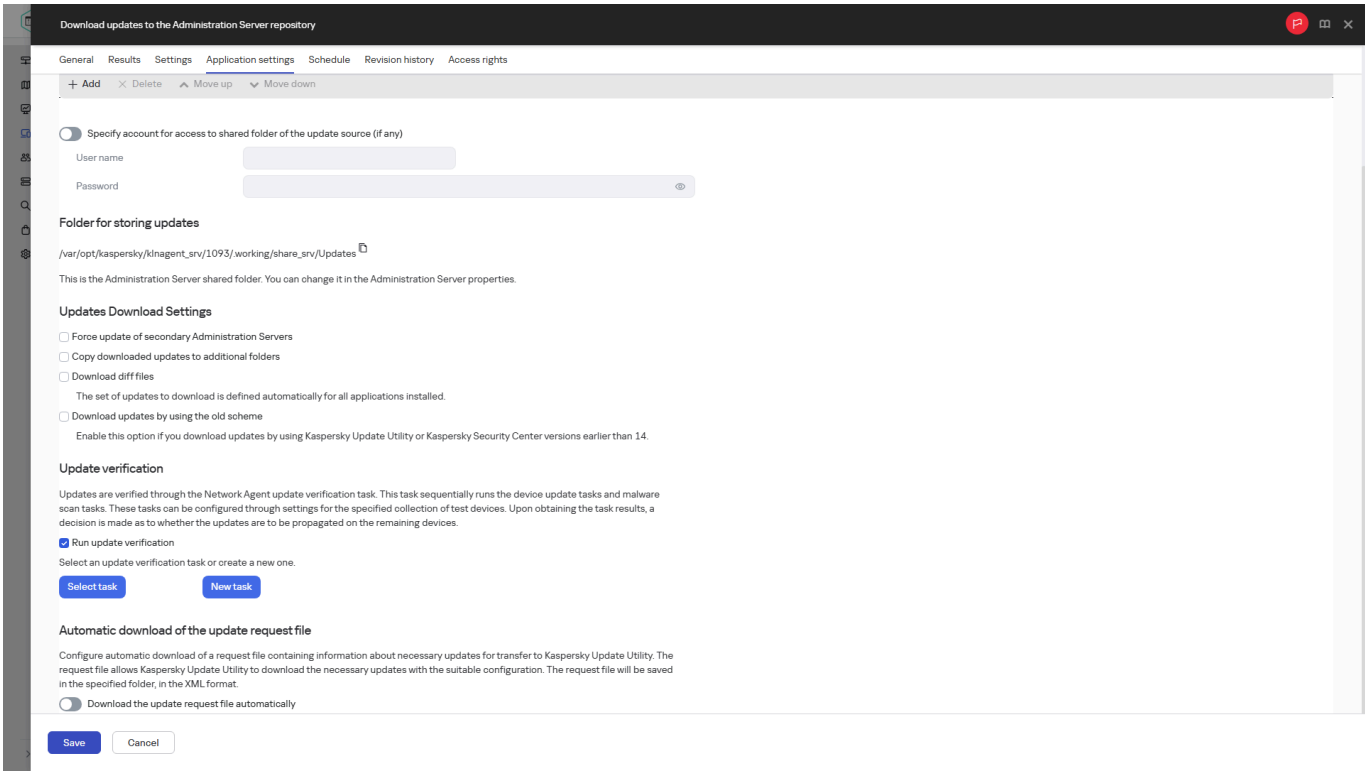
3. 建立*將更新下載至管理伺服器儲存區*工作。

要讓卡巴斯基安全管理中心 Linux 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 **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。



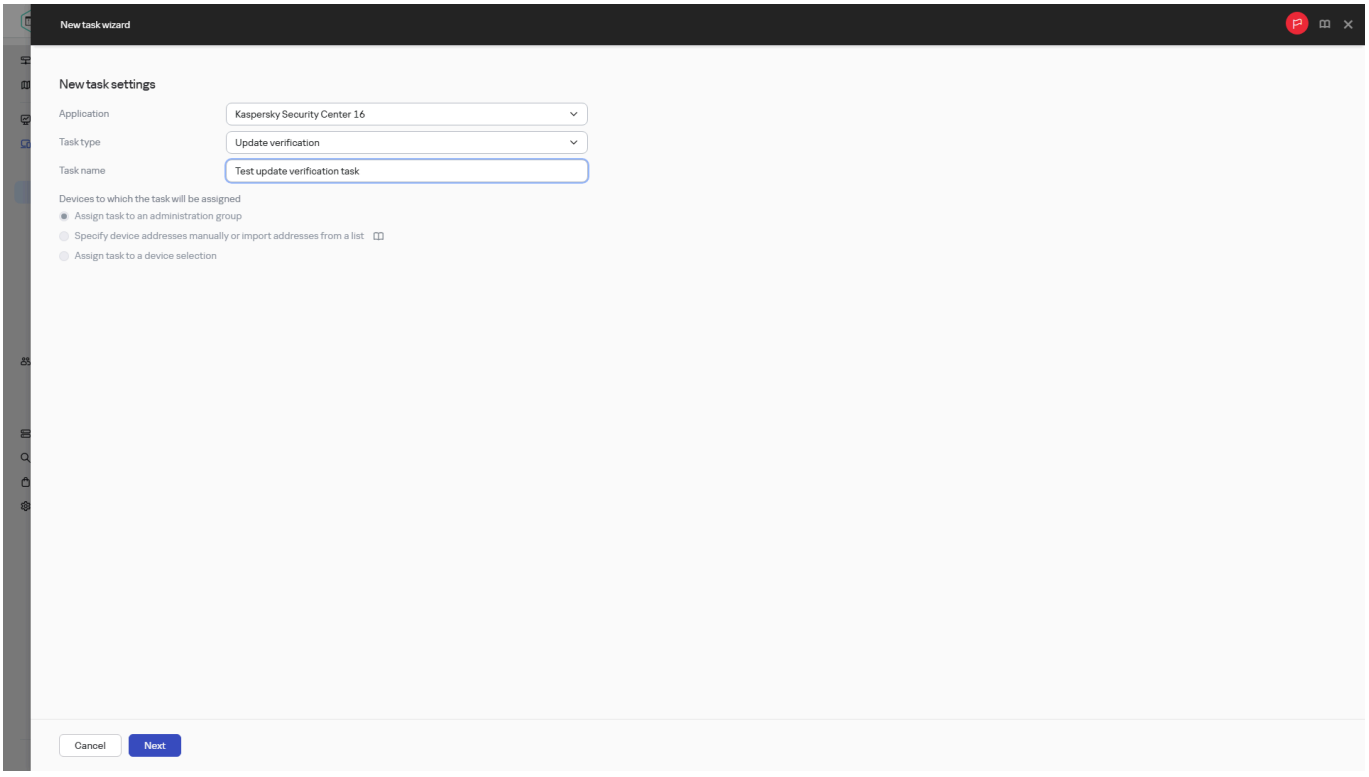
"將更新下載至管理伺服器儲存區"工作的內容

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。

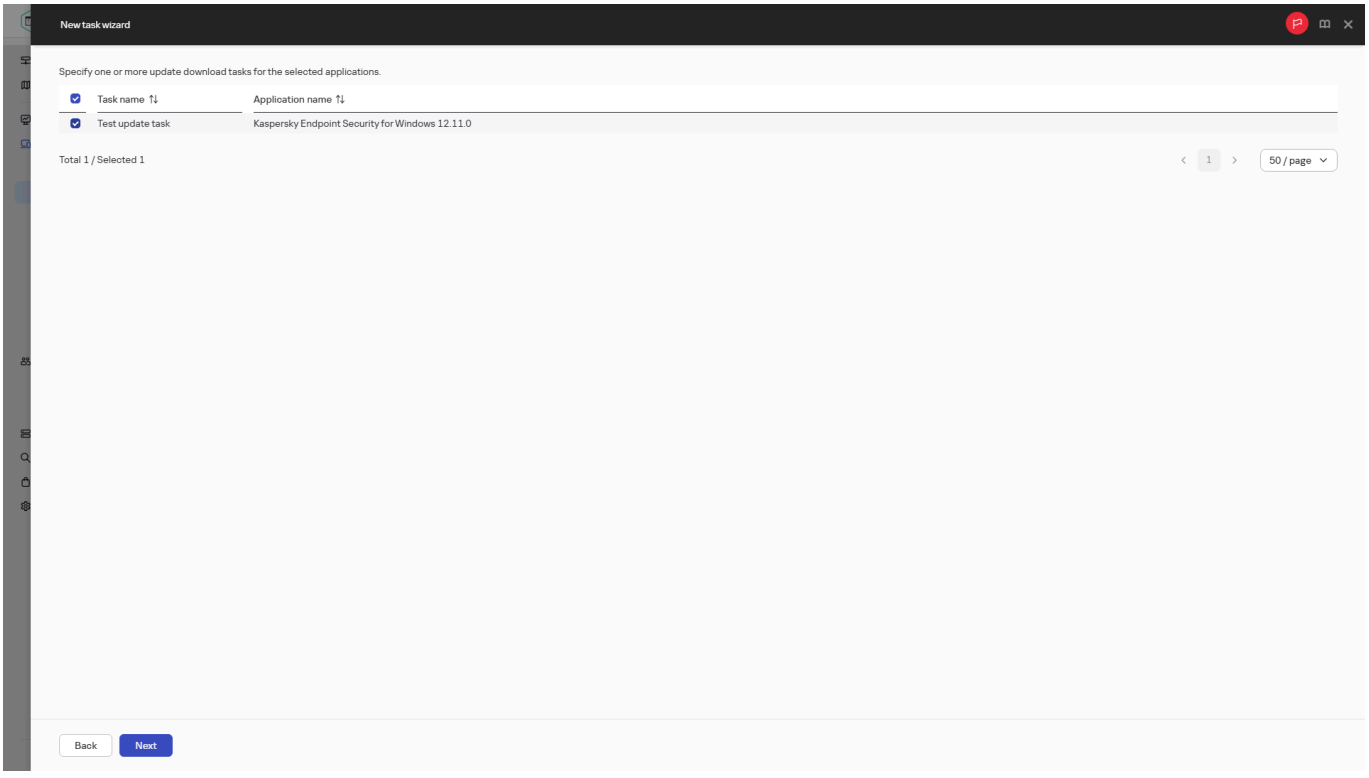
b. 在開啟的新工作精靈中，如果要變更預設名稱，請指定工作名稱。



建立"更新驗證"工作

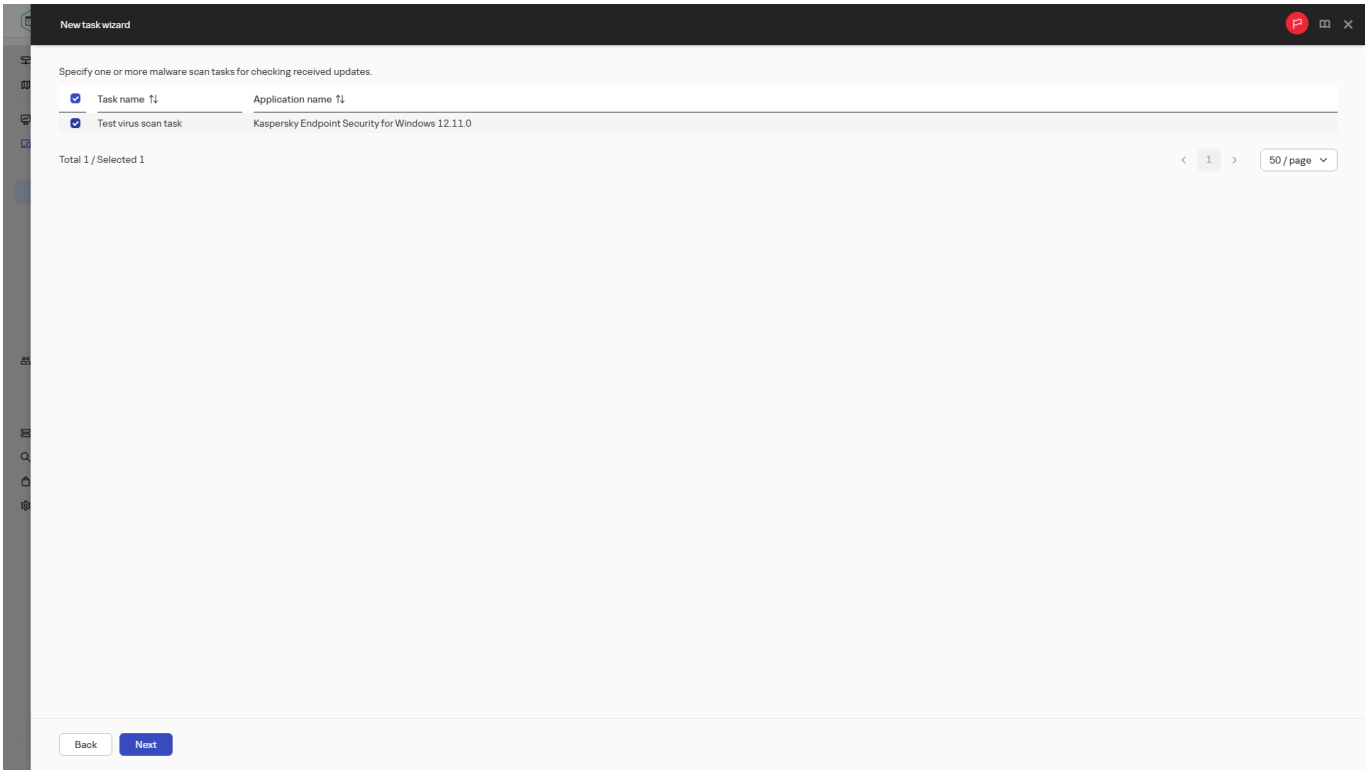
a. 選擇您之前建立的具有測試裝置的管理群組。

b. 選擇卡巴斯基安全管理中心 Linux 支援的所需應用程式的更新工作。



選擇應用程式更新工作

a. 選擇卡巴斯基安全管理中心 Linux 支援的所需應用程式的惡意軟體掃描工作。



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**

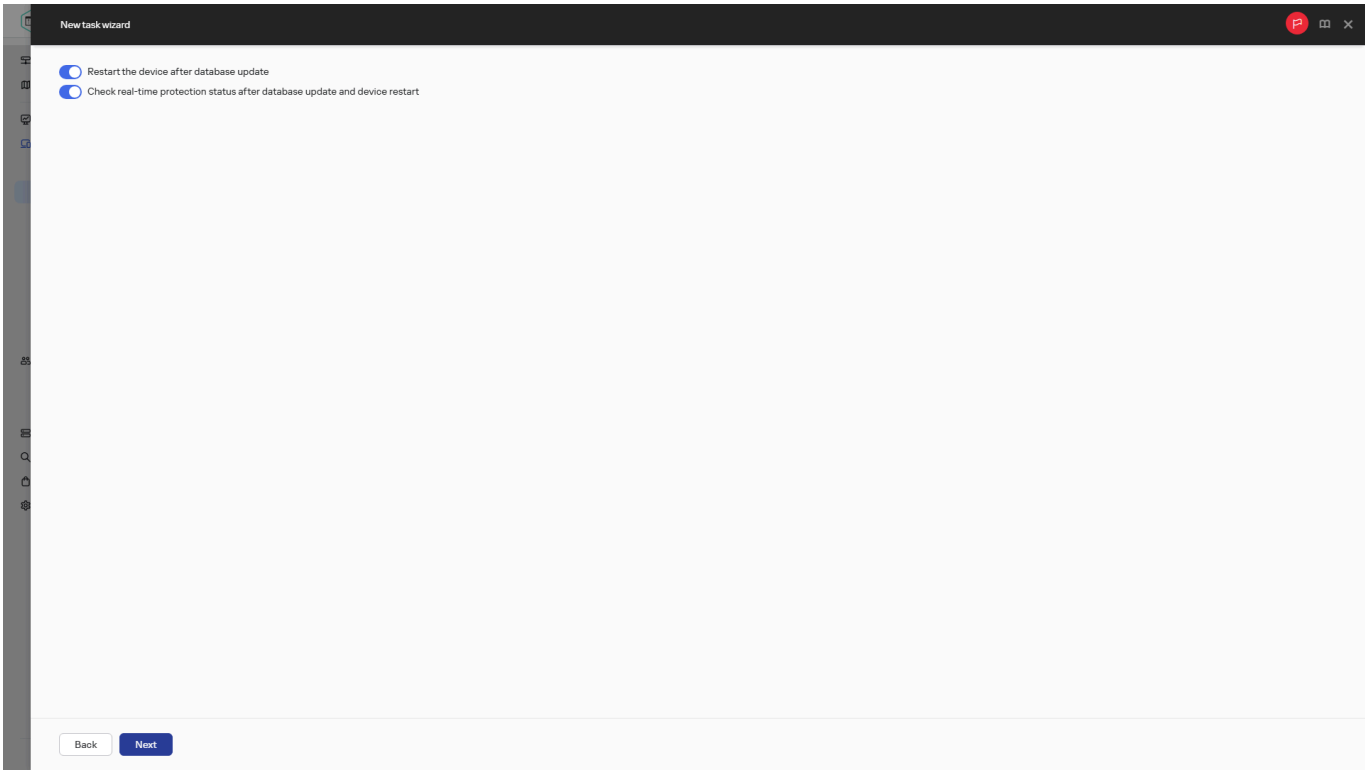
  在裝置上更新病毒資料庫後，我們建議重新啟動裝置。

  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。



指定工作設定

a. 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

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。

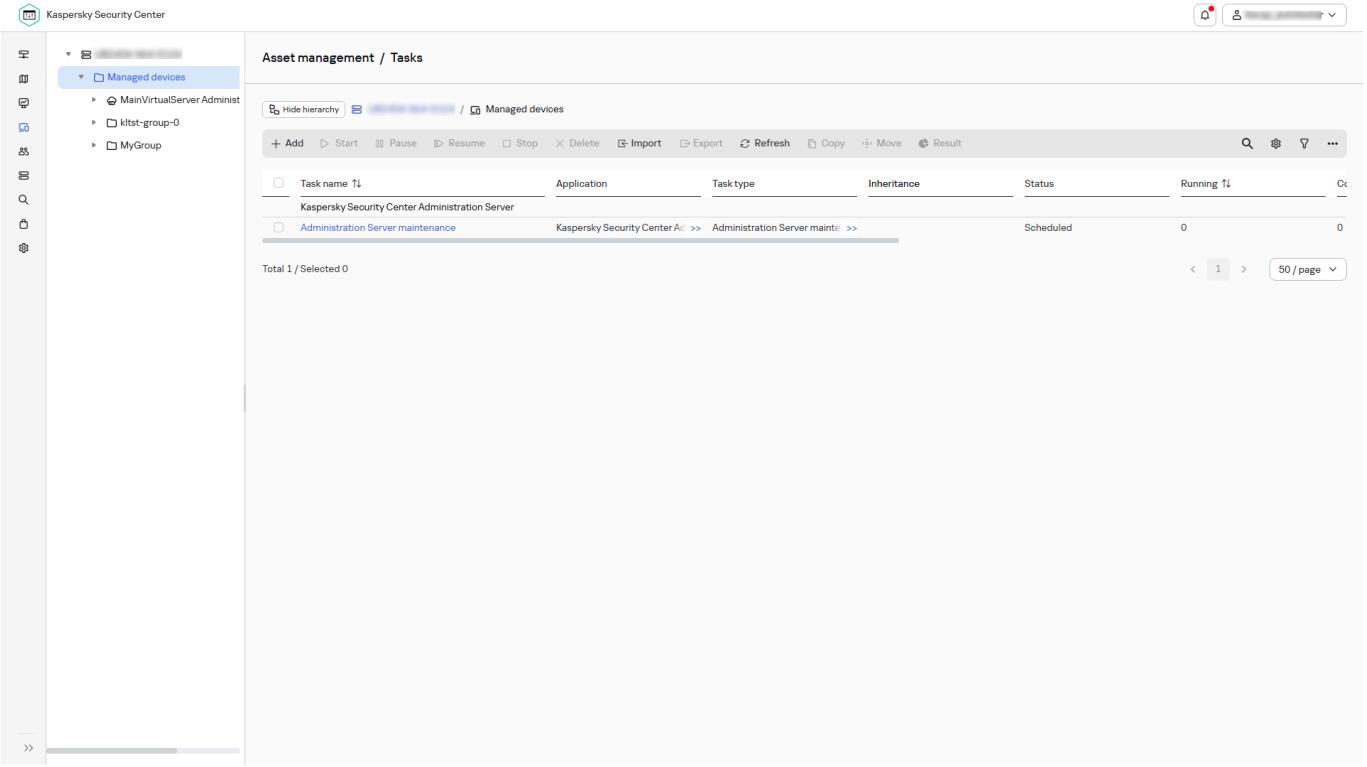
該工作用在從 Kaspersky 更新伺服器下載更新到發佈點儲存區時。更新清單包含：

- 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 **工作**。



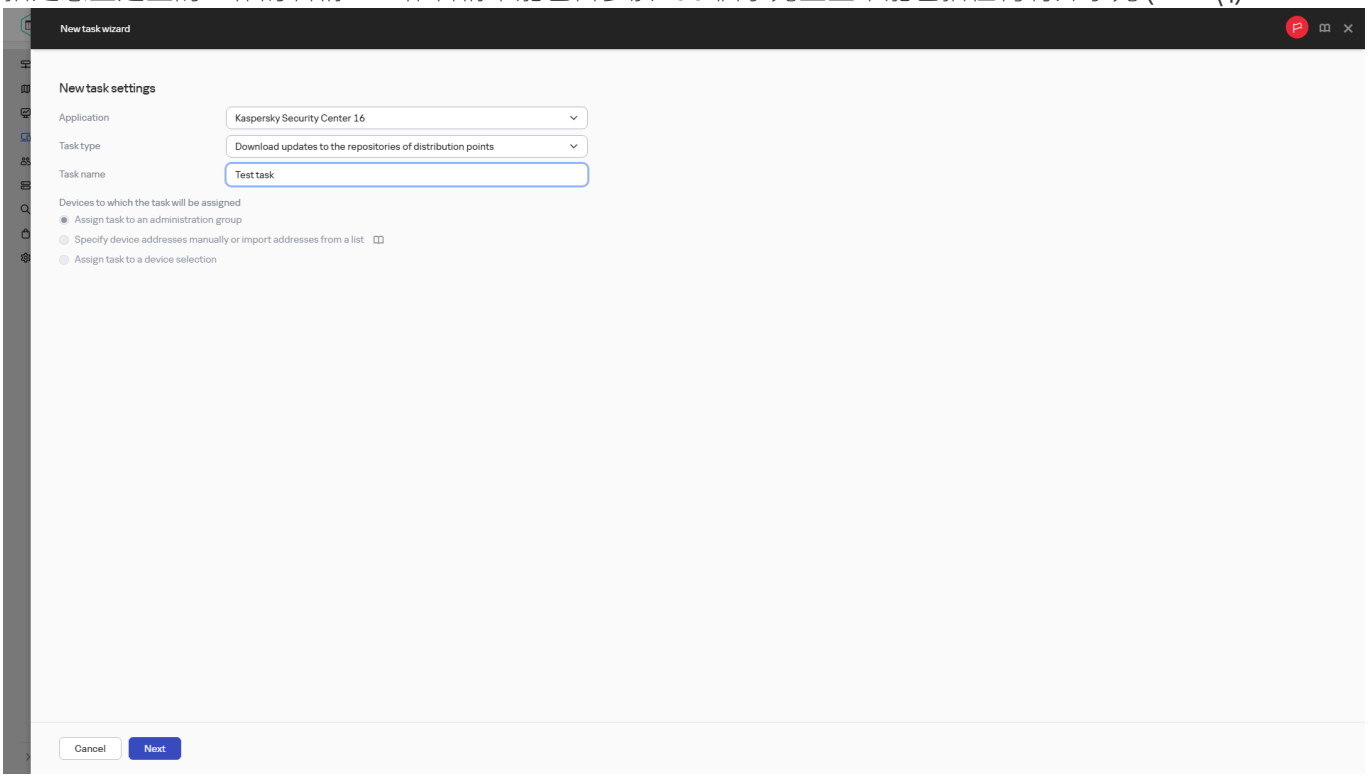
工作 部分

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 ("*<>?\:|)。



建立"將更新下載至發佈點儲存區"工作

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。只有已安裝的 SMB 共用才能用作網路資料夾。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。

       > 在*將更新下載至管理伺服器儲存區*工作和*將更新下載至發佈點的儲存區* 工作中，如果您選擇受密碼防護的本機或網路資料夾作為更新來源，則使用者身分驗證不起作用。要解決此問題，首先掛接受密碼防護的資料夾，然後指定所需的憑據，例如，透過作業系統。之後，您可以選擇此資料夾作為更新下載工作中的更新來源。卡巴斯基安全管理中心 Linux 不會要求您輸入憑據。

   - **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。

   - **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 Linux 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 Linux

       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，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：

- **開始工作**:

  - **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 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。

  - **按每週中的指定日**

    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。

  - **每月於選定的週間日**

    工作定期在指定月日的指定時間執行。

    預設情況下，開始時間為18:00，且未選擇當月的任何日期。

    > 請注意，您選擇的是當月的週幾，而不是特定的日期或週數（例如，當月的第一週或第二週）。例如，如果您將遊標放在**週二**行的**第一**單元格中，則表示該工作將在每個月的第一個星期二執行。

    您可以選擇一週中的多個日期。

- **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。只有在將這兩項工作指派給相同的裝置時，此選項才會發揮作用。例如，您可能想使用**開啟裝置**選項執行*受管理裝置*工作，完成後，請執行*病毒掃描*工作作為觸發工作。

  您必須從表格中選擇觸發工作以及此工作必須完成的狀態（**成功完成**或**失敗**）。

  如有需要，您可以對表格中的工作進行搜尋、排序和篩選，如下所示：

  - 在搜尋欄位中輸入工作名稱，可依其名稱搜尋工作。
  - 點擊排序圖示，可依名稱對工作進行排序。

    預設情況下，工作會依字母遞增排序。
  - 點擊篩選器圖示，在開啟的視窗中依群組篩選工作，然後點擊**套用**按鈕。

- **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化延遲**

  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。

- **對於在以下間隔內啟動的工作，使用工作啟動自動隨機化延遲**

  如果該選項被啟用，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。

為將更新下載到管理伺服器儲存區工作新增更新來源

當您建立或使用將更新下載到管理伺服器儲存區的工作時，您可以選擇以下更新來源：

- Kaspersky 更新伺服器
- 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

> 在*將更新下載至管理伺服器儲存區*工作和*將更新下載至發佈點的儲存區* 工作中，如果您選擇受密碼防護的本機或網路資料夾作為更新來源，則使用者身分驗證不起作用。要解決此問題，首先掛接受密碼防護的資料夾，然後指定所需的憑據，例如，透過作業系統。之後，您可以選擇此資料夾作為更新下載工作中的更新來源。卡巴斯基安全管理中心 Linux 不會要求您輸入憑據。

預設使用卡巴斯基更新伺服器，但您也可以從本機或網路資料夾下載更新。如果您的網路無法存取網際網路，您可能希望使用該資料夾。在這種情況下，您可以從卡巴斯基更新伺服器手動下載更新，並將下載的檔案放在必要的資料夾中。您只能指定一個本機或網路資料夾路徑。

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。資料夾路徑取決於裝置的作業系統。由於本機資料夾位於基於 Linux 的管理伺服器上，因此您必須指定 POSIX 路徑。例如 /path/to/dir。

只有已安裝的 SMB 共用才能用作網路資料夾。如果 SMB 共用需要身分驗證，必須事先在系統中使用所需的憑證將其掛載。我們建議不要使用 SMB1 協定，因為它不安全。

要新增更新來源：

1. 在主功能表中，轉至 **工作**。
2. 點擊**將更新下載至管理伺服器儲存區**。
3. 轉到**應用程式設定**標籤。
4. 在**更新來源**表中，點擊**新增**按鈕。
5. 在開啟的視窗中，新增必要的來源，然後點擊**儲存**按鈕。

   如果您選擇**本機或網路資料夾**核取方塊，請指定資料夾的路徑。
6. 點擊工作視窗中的**儲存**按鈕。

現在更新被從指定來源下載到管理伺服器儲存區。

如果同時新增卡巴斯基更新伺服器及本機或網路資料夾，您可以設定更新的優先順序。為此，在**更新來源**表中，選取要變更優先順序的更新旁的複選框，然後點擊**向上移動**或**向下移動**按鈕。

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。

核准和拒絕更新僅適用於安裝在 Windows 型用戶端裝置上的網路代理和受管理應用程式。不支援管理伺服器、卡巴斯基安全管理中心網頁主控台和管理 Web 外掛程式的無縫更新。若要更新這些元件，您必須從卡巴斯基網站下載最新版本，然後手動安裝它們。

要批准或拒絕一個或幾個更新：

1. 在主功能表中，轉至**軟體管理→卡巴斯基應用程式→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. 如有必要，請點擊**檢視和接受產品授權協議**按鈕以接受 EULA。

3. 選取您要批准或拒絕的更新。

4. 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 Linux 將不會從先前安裝這些更新的裝置上解除安裝這些更新。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。

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 **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 Linux 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，這些更新將透過應用程式介面或卡巴斯基安全管理中心 Linux 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。

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 Linux 從卡巴斯基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。

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

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的網路代理政策設定中啟用該功能。

   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啟用，並且當您手動分配發佈點，而且您要在管理伺服器內容中的**發佈點**區域覆寫政策設定。

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。

透過發佈點下載更新

卡巴斯基安全管理中心 Linux 允許發佈點從管理伺服器、卡巴斯基伺服器或本機網路資料夾接收更新。

要為發佈點設定更新下載：

1. 在主選單中，按一下管理伺服器名稱。

   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. 點擊將透過其將更新傳送到群組中的用戶端裝置的發佈點的名稱。

4. 在發佈點內容視窗中，選取**更新來源**區域。

5. 為發佈點選取更新來源：

   - **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。

   發佈點將從指定的更新來源接收更新。

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： /var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/Updates/.

   或者，您可以配置 卡巴斯基安全管理中心 Linux 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 Kaspersky Endpoint Security 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。

   說明：

   - Kaspersky Endpoint Security for Linux 說明
   - Kaspersky Endpoint Security for Windows 說明

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. 在需要更新安裝的離線裝置上，啟動 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Windows 的*更新*工作，具體取決於離線裝置的作業系統。

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。

監控、報告和稽核

該部分敘述了 卡巴斯基安全管理中心 Linux 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 Linux 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 Linux 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 Linux 後，您可開始監控此程式並產生其功能運作報告。

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. **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

4. **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

5. **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

6. **檢查用戶端裝置防護**

   說明：

   - 從防護狀態和威脅統計資訊類別產生並檢閱報告
   - 啟動並檢閱緊急事件分類

7. **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：

   - 限制最大事件數量

8. **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。

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。如果工作為智慧培訓模式，它們將偵測異常行為並傳送每個偵測的報告到管理伺服器。您可以在**儲存區→智慧培訓狀態中的規則觸發器**中檢視有關偵測到的異常行為的報告。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。

檢視並確認使用自適應異常控制規則執行的偵測

要檢視使用適應性異常控制規則執行的偵測清單：

1. 在主功能表中，轉至**儲存區→智慧培訓狀態中的規則觸發器**。

   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。

   - **虛擬管理伺服器**

     管理裝置的虛擬管理伺服器。

   - **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。

   - **偵測數量**

     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）。

- **目標處理程序路徑**

  目的處理程序的路徑（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

- **目標處理程序雜湊**

  目的檔案的 SHA256 雜湊（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

- **目標物件路徑**

  目的物件的路徑（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

- **目標物件雜湊**

  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。

檢視偵測內容：

1. 在主功能表中，轉至**儲存區→智慧培訓狀態中的規則觸發器**。
2. 執行以下操作之一：
   - 在**名稱**欄中，點擊包含要檢視的偵測名稱的連結。
   - 在偵測清單中，選取要檢視的偵測旁的核取方塊，然後點擊**內容**按鈕。

   將開啟所選偵測的內容視窗，顯示有關它的資訊。

您可以從自適應異常控制規則的偵測清單或所選偵測的內容視窗中確認任何偵測。

確認偵測：

- 在偵測清單中選取一個或多個偵測，然後點擊**確認**按鈕。
- 開啟選定偵測的內容視窗，然後點擊**確認**按鈕。

  偵測的狀態被變更為**正在確認**。用戶端裝置與管理伺服器下次同步後，偵測將從偵測清單中消失。

  您的確認將有助於規則使用的統計資料。有關詳細資訊，請參閱Kaspersky Endpoint Security for Windows 說明。

從適應性異常控制規則新增排除

“新增到自適應異常控制排除項目”精靈允許您從 Kaspersky Endpoint Security 的自適應異常控制規則中新增排除項目。

使用精靈新增自適應異常控制規則的排除項目：

1. 以下列方式之一啟動精靈：

   - 在主功能表中，轉至**儲存區→智慧培訓狀態中的規則觸發器**，選取一個或多個偵測，然後點擊**排除**按鈕。

     您可以一次新增 1000 個排除項目。

     在將偵測新增至排除項目之前，您可以透過點擊偵測名稱或**內容**按鈕來檢視偵測的屬性。在開啟的偵測內容視窗中，您也可以點擊**排除**按鈕。

   - 在主功能表中，前往**監控 → 事件分類**，點擊所需事件分類的連結，選中要排除的偵測旁邊的核取方塊，然後點擊**從自適應異常控制中排除**按鈕。

   "新增到自適應異常控制排除項目"精靈啟動。使用**下一步**按鈕進行精靈。

2. 選取您要新增排除的政策和設定檔。

   繼承的政策無法被更新。如果您沒有權限修改政策，政策將不被更新。

3. 點擊**完成**關閉精靈。

   偵測狀態被變更為**正在排除**。用戶端裝置與管理伺服器下次同步後，偵測將從偵測清單中消失。已配置並套用自適應異常控制規則的排除項。

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工具的資訊。該部分包括有關如何管理小工具和配置小工具設定的說明。

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**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**

- **威脅統計資訊**
- **其他**

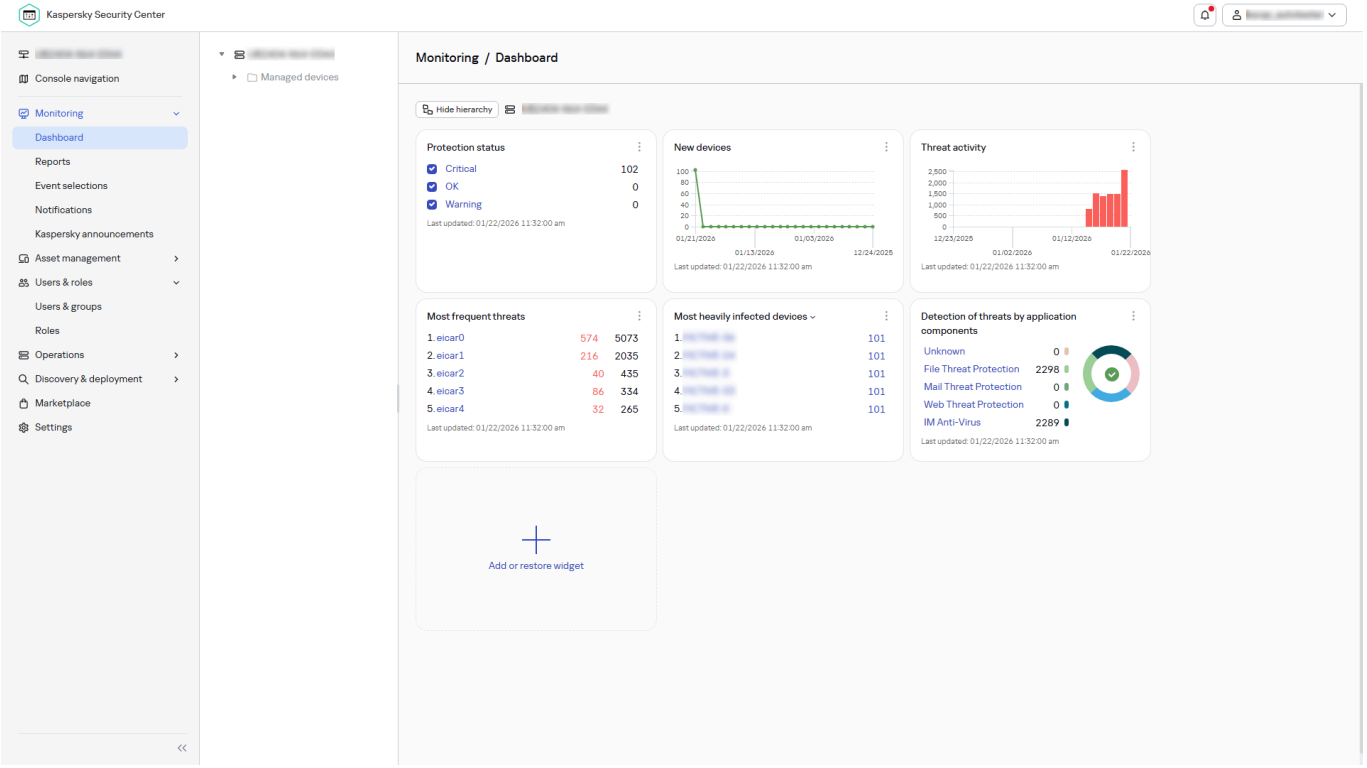
一些部件具有帶連結的文字資訊。您可以透過點擊連結檢視詳細資訊。

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

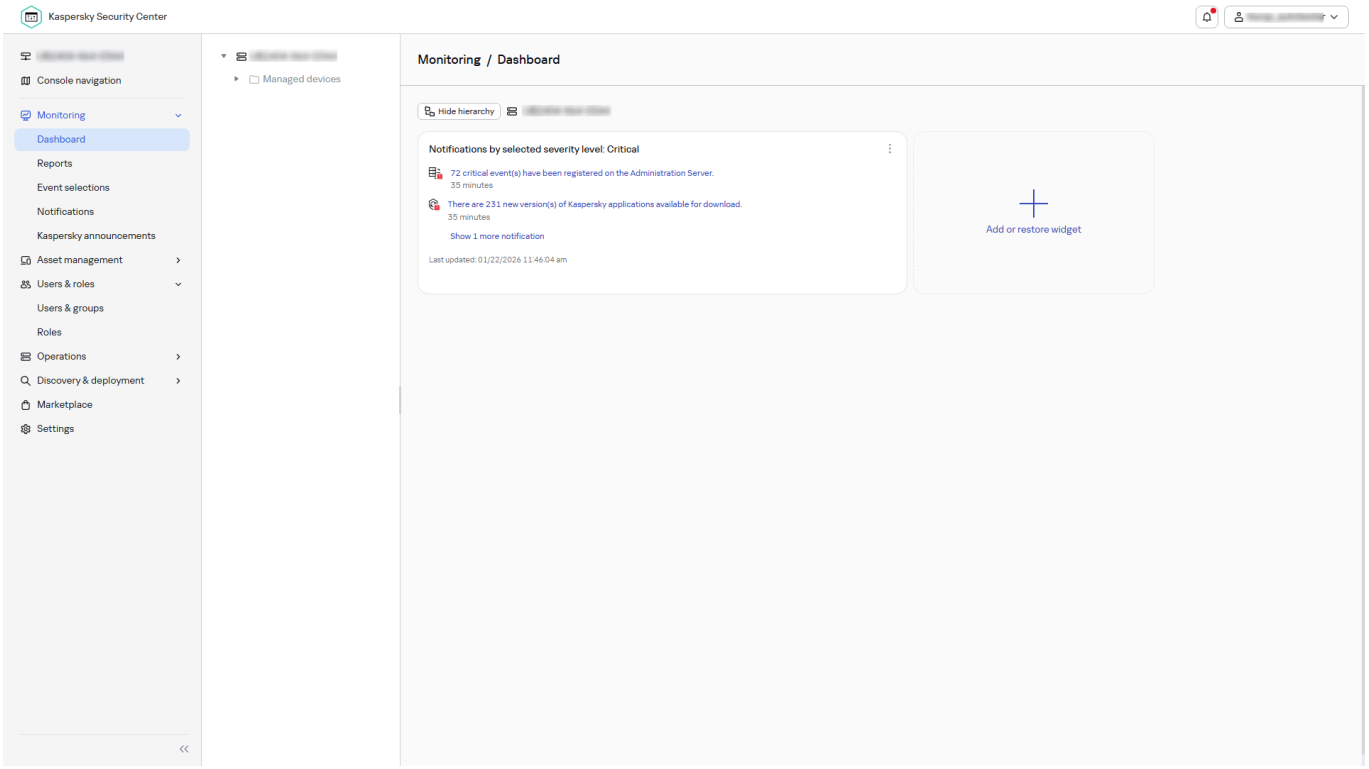
要新增工具到儀表板：

1. 在主功能表中，轉至 **監控** → **控制板**。



帶有小工具的儀表板

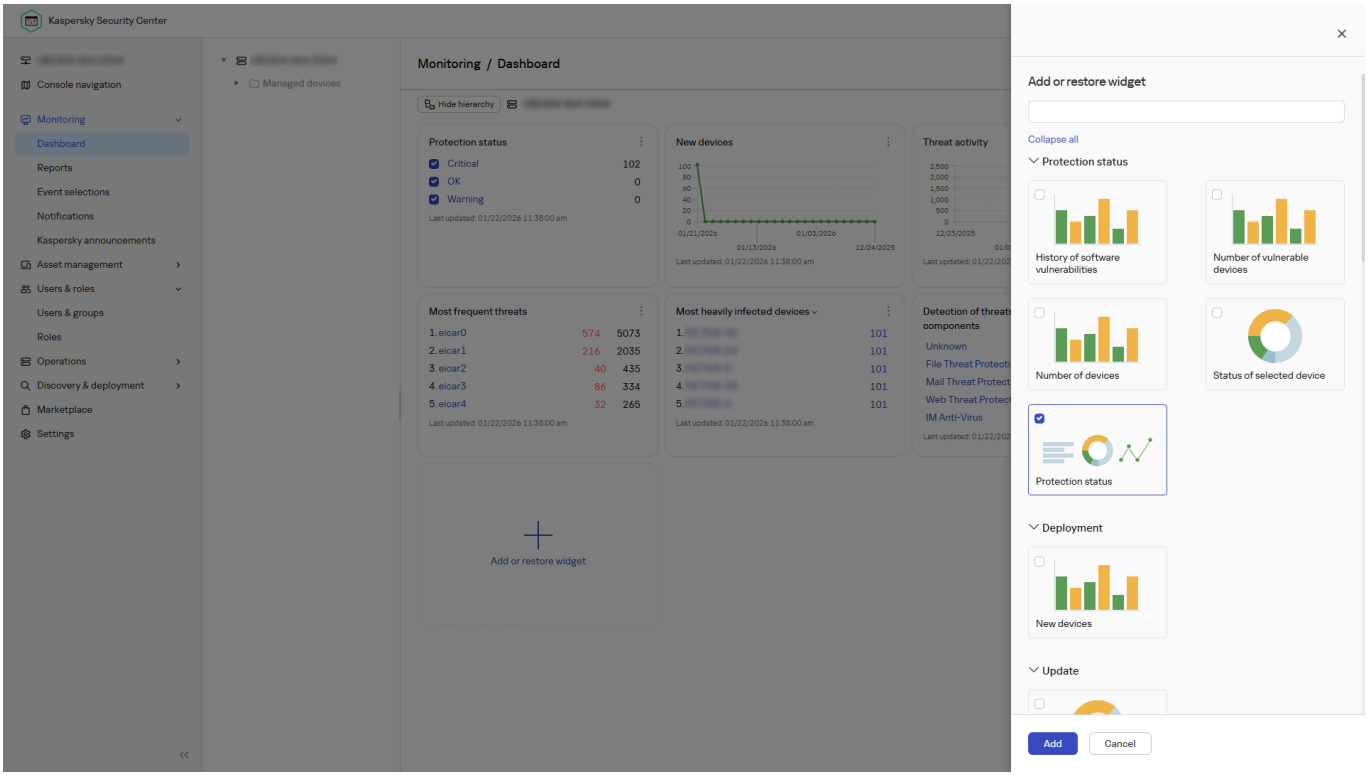
2. 點擊**新增或還原小部件**按鈕。



新增小工具

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（>）。



選取小工具類型

4. 點擊**新增**按鈕。

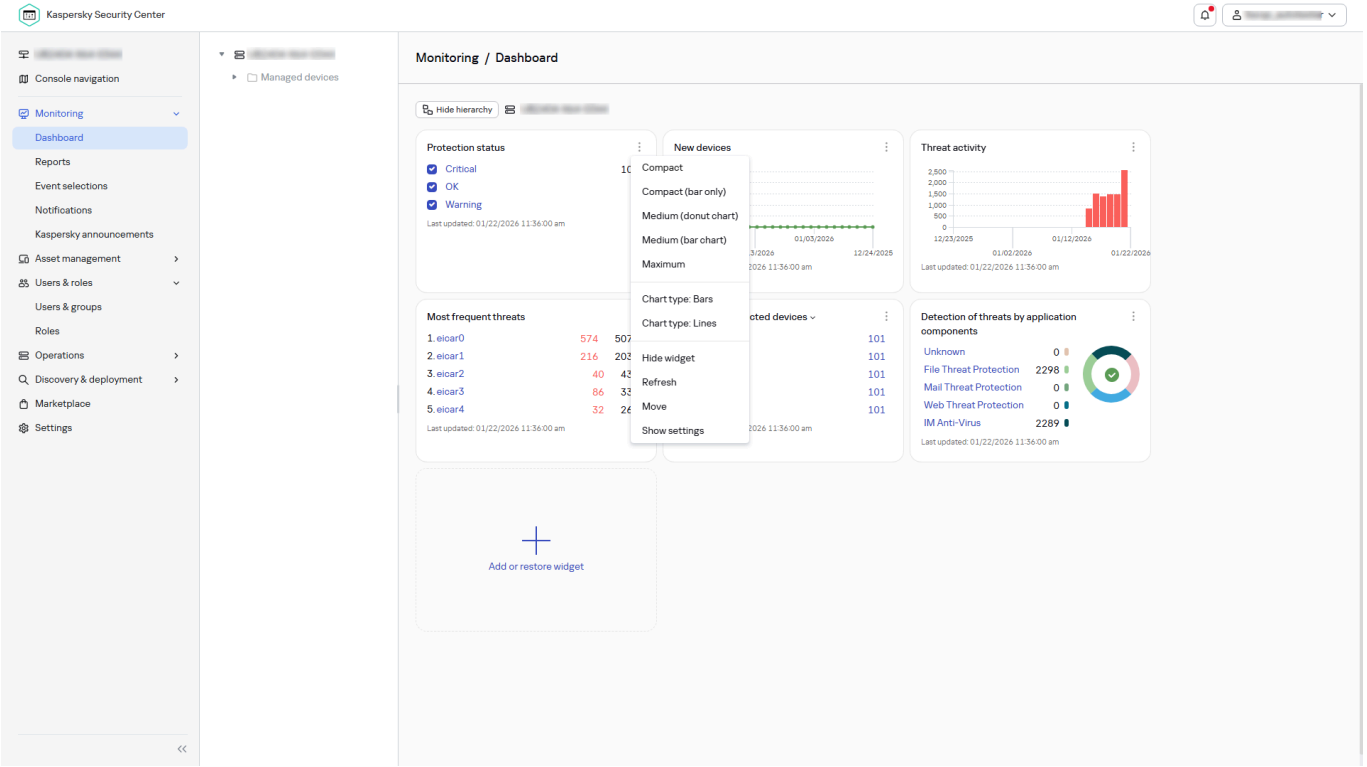
所選的工具被新增到儀表板結尾。

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** → **控制板**。
2. 點擊您要隱藏的工具旁邊的設定圖示（⚙）。



小工具選單

3. 選擇**隱藏小部件**。
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** → **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** → **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：長條**。
   - 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（僅長條）**
     - **中度（餅圖）**
     - **中度（長條圖）**
     - **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** → **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：

- **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。
- **如果指定了以下設定，則設定為「緊急」**與**如果指定了以下設定則設定為「警告」**（規判交通號誌燈號的規則）。

更改小工具設定後，您可以手動重新整理小工具上的資料。

要重新整理小工具上的資料：

1. 在主功能表中，轉至 **監控** → **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**。

   小工具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 Linux 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 → 使用者和群組** 部分的**使用者**頁簽中使用。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 → 使用者和群組**，然後選擇**使用者**頁簽。
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**頁籤上，您可以對小工具執行於在**監控→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 Linux 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 Linux 並在「僅儀表板」模式下監控網路防護統計資訊。

管理和防護報告

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**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 Linux 具有以下類別的預設報告集：

- **防護狀態**
- **佈署**
- **更新**
- **威脅統計資訊**
- **其他**

您可以建立自訂報告範本、編輯報告範本和刪除它們。

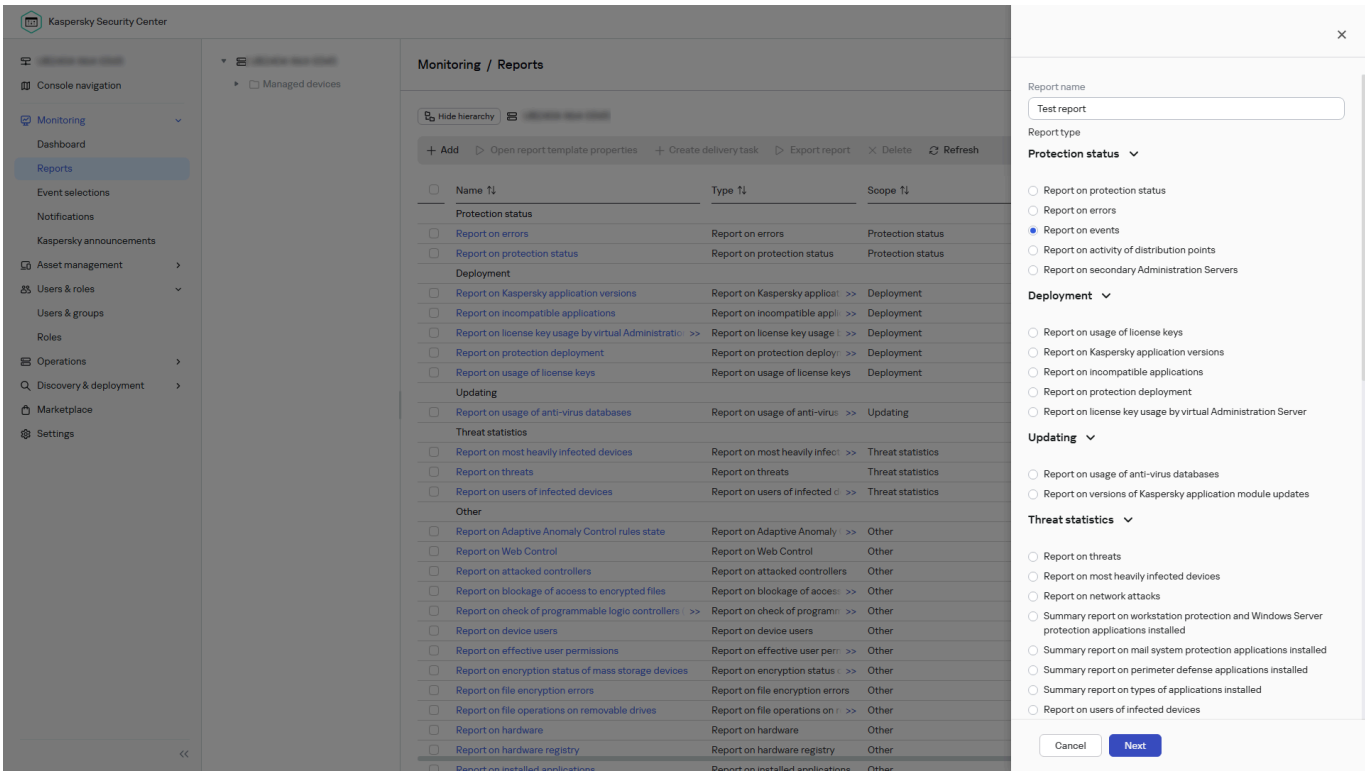
您可以基於現有範本建立報告、匯出報告到檔案和建立報告傳送工作。

建立報告範本

要建立報告範本，請執行以下操作：

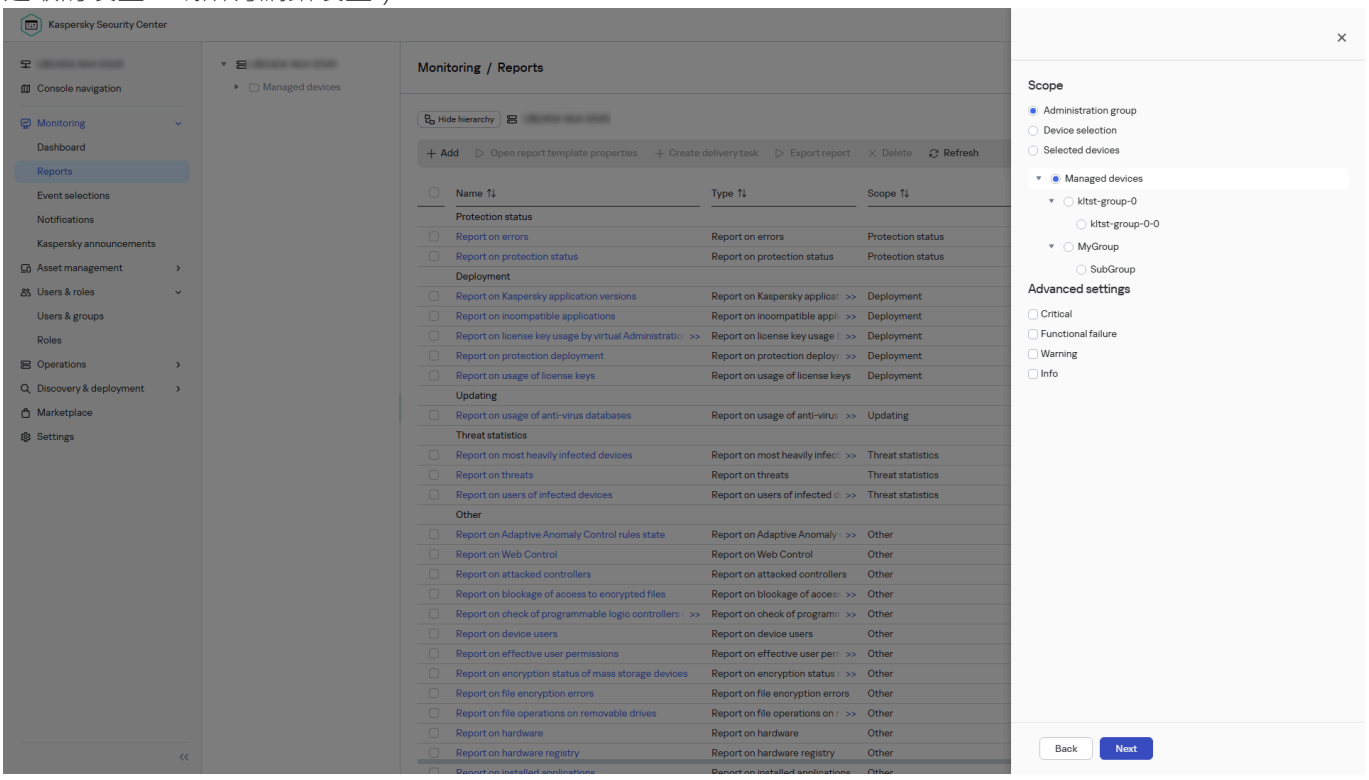
1. 在主功能表中，轉至 **監控** → **報告**。
2. 點擊**新增**。
   程式將啟動“新報告範本精靈”。使用**下一步**按鈕進行精靈。

3. 輸入報告名稱並選擇報告類型。



指定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）。

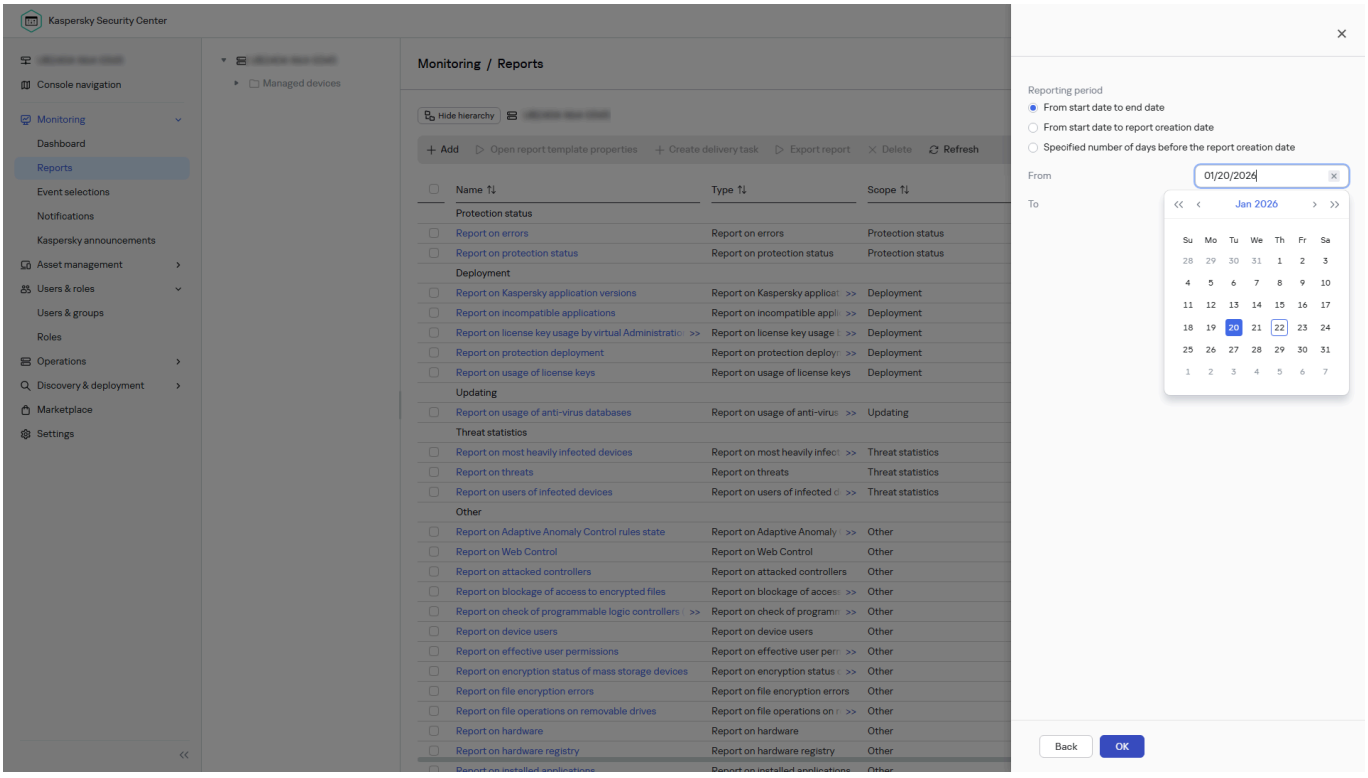


指定報告範圍

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。



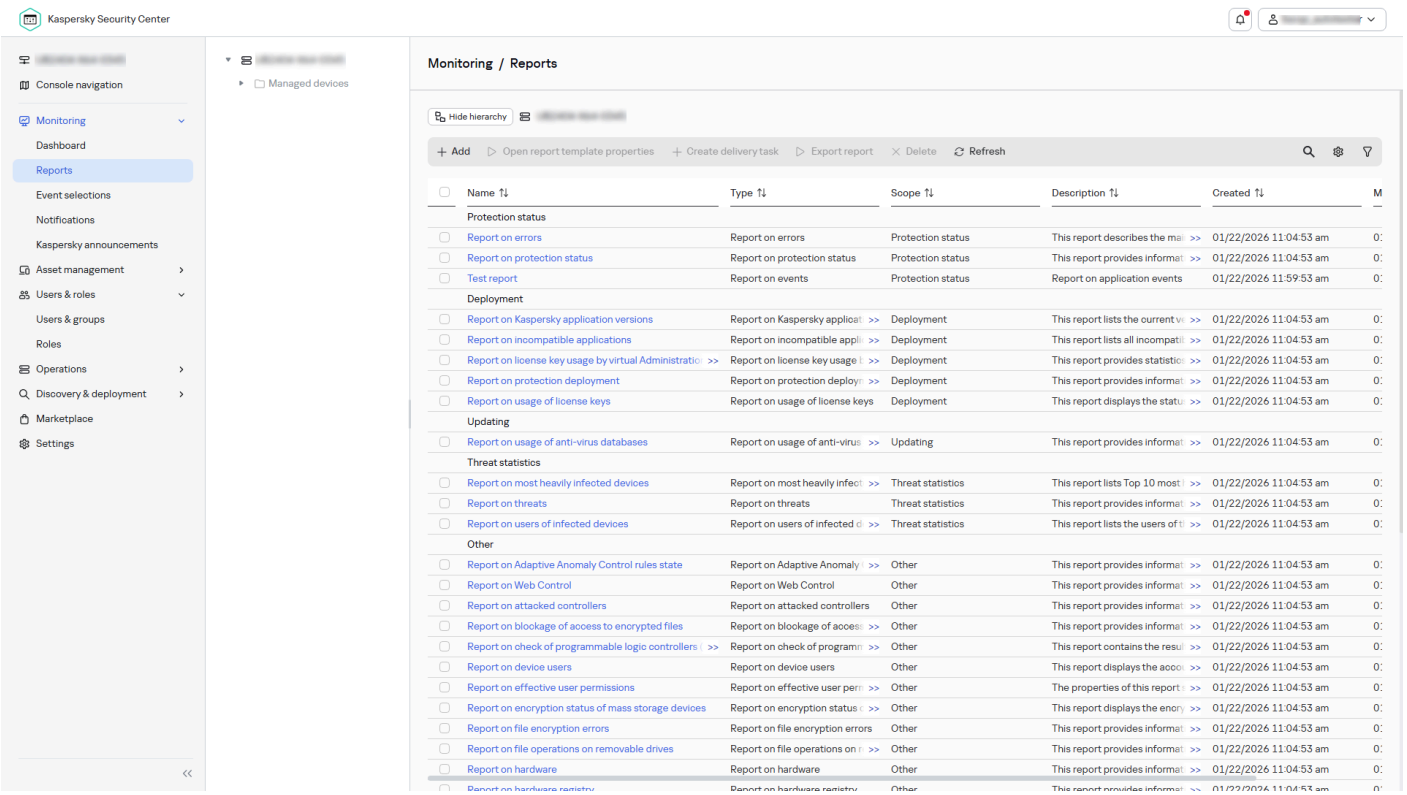
指定報告期間

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。



報告清單

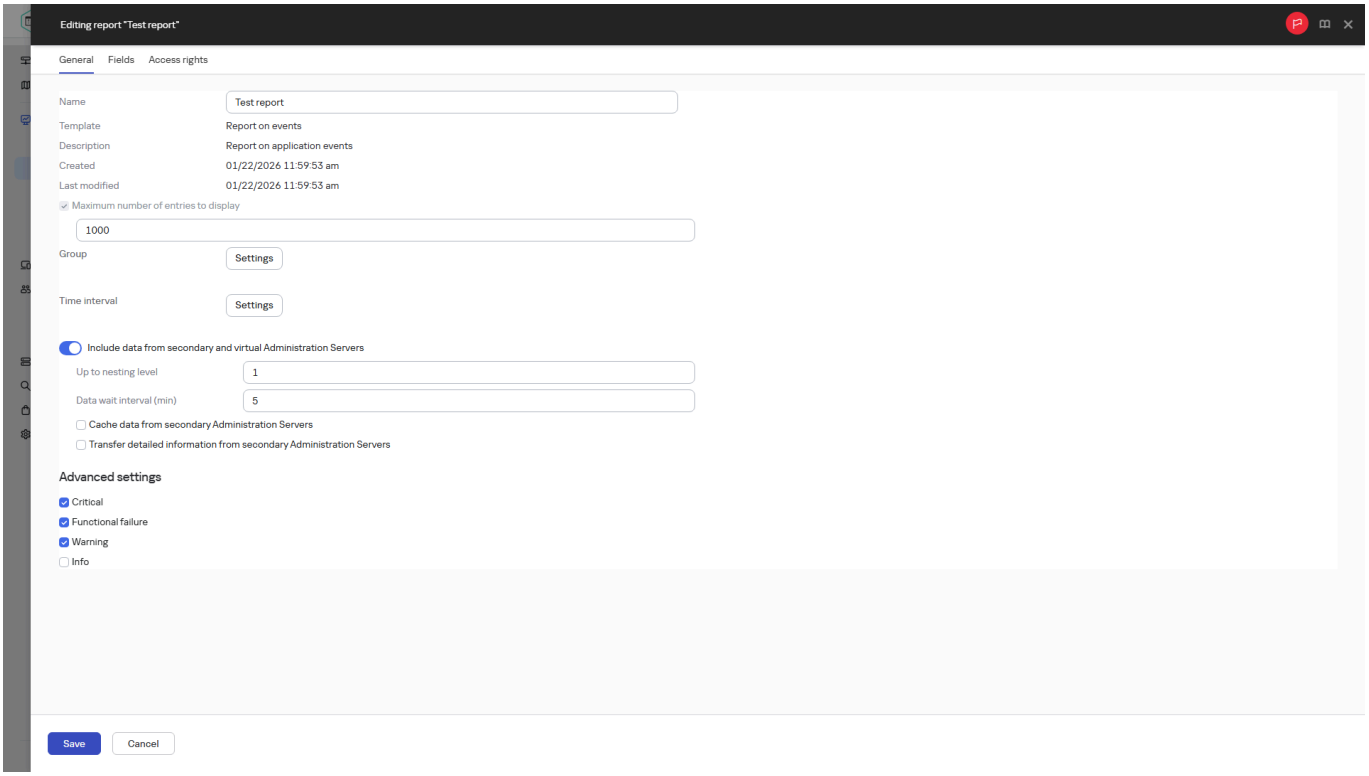
檢視和編輯報告範本內容

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** → **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。



報告範本內容

4. 編輯報告範本內容：

- **一般**頁籤：
  - 報告範本名稱
  - **顯示的項目數量上限**

    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。請注意，此選項不會影響將報告匯出到檔案時可包含在報告中的最大事件數。

    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

- **包含來自從屬管理伺服器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。

- **最大嵌套層級**

  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**快取來自從屬管理伺服器的資料**選項已啟用），否則為 **N/A**（不可用）。

  預設值是 5 分鐘。

- **快取來自從屬管理伺服器的資料**

  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。

- **快取更新頻率（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

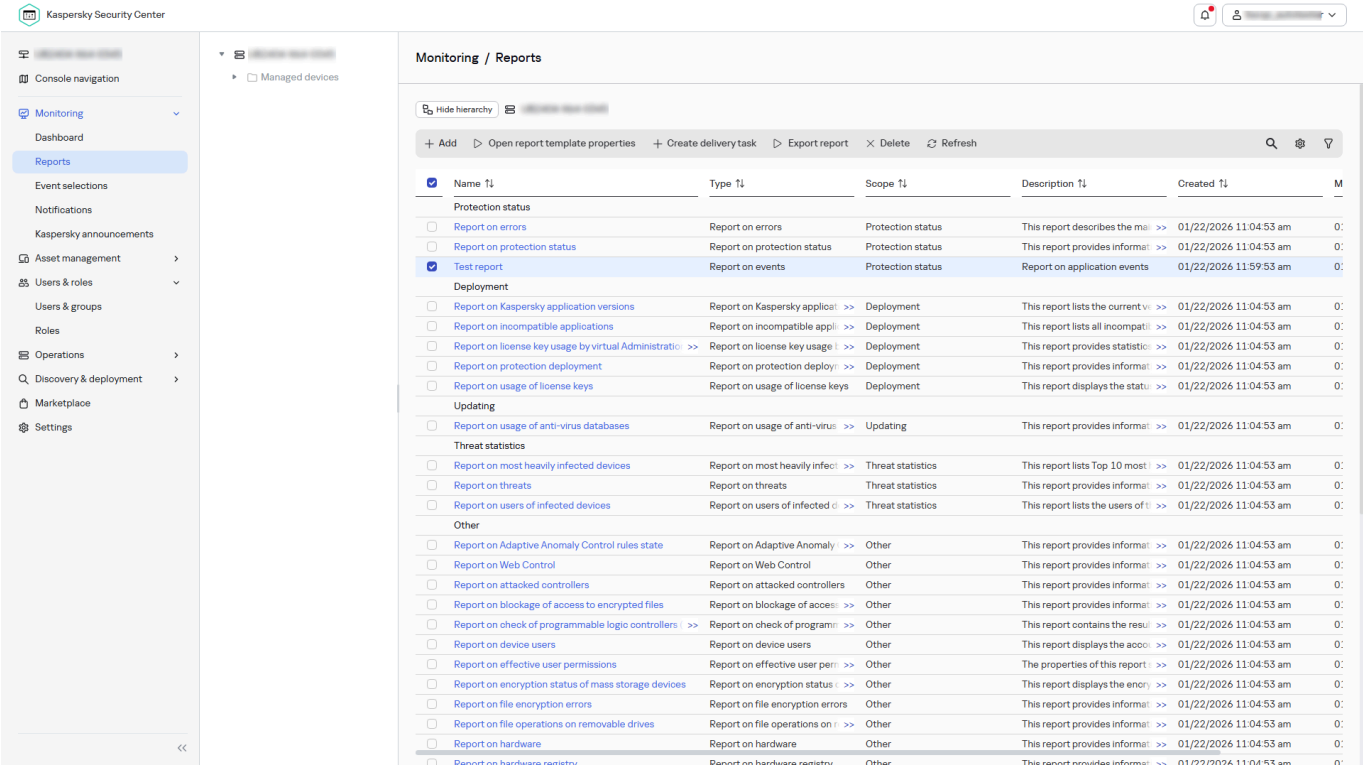
您可以將一份或多份報告儲存為 XML、HTML 或 PDF。卡巴斯基安全管理中心 Linux 允許您同時將最多 10 個報告匯出為指定格式的檔案。

要匯出報告到檔案：

1. 在主功能表中，轉至 **監控 → 報告**。

2. 選取您要匯出的報告。

   如果您選取超過 10 個報告，**匯出報告**按鈕將被停用。



報告清單

3. 點擊**匯出報告**按鈕。

4. 在開啟的視窗中，指定以下匯出參數：

   - **檔案名稱**。

     如果您選擇匯出一份報告，請指定報告檔案名稱。

     如果您選擇多個報告，報告檔案名稱將與所選報告模板的名稱一致。

   - **項目數量上限**。

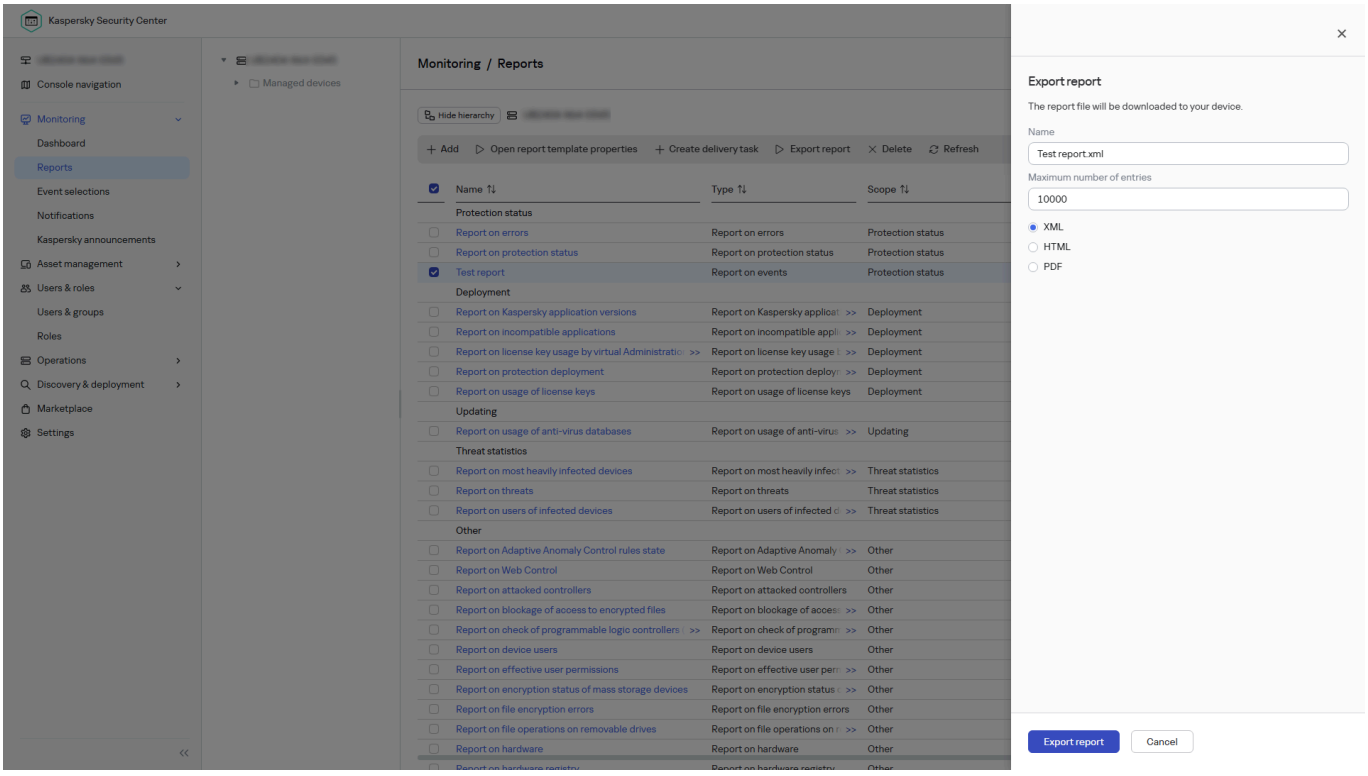
     指定報告檔案中包含的最大項目數。預設值是 10,000。

     您可以匯出包含無限數量項目的報告。請注意，如果您的報告包含大量項目，則產生和匯出報告所需的時間會增加。

- **檔案格式**。

  選取報告檔案格式：XML、HTML 或 PDF。如果匯出多個報告，所有選定的報告都會以指定的格式儲存為單獨檔案。

> 需要使用 wkhtmltopdf 工具將報告轉換為 PDF。當您選擇 PDF 選項時，管理伺服器會檢查裝置上是否安裝了 wkhtmltopdf 工具。如果未安裝該工具，應用程式會顯示一條訊息，說明必須在管理伺服器裝置上安裝該工具。手動安裝該工具，然後繼續下一步。



指定報告匯出設定

5. 點擊**匯出報告**按鈕。

報告以指定格式儲存到檔案中。

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** → **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。

> 在產生的報告中，某些字體可能無法正確顯示在圖表上。要解決此問題，請安裝 fontconfig 庫。另外，請檢查作業系統中是否安裝了與您的作業系統區域設定相對應的字體。

此報告將顯示下列資料：

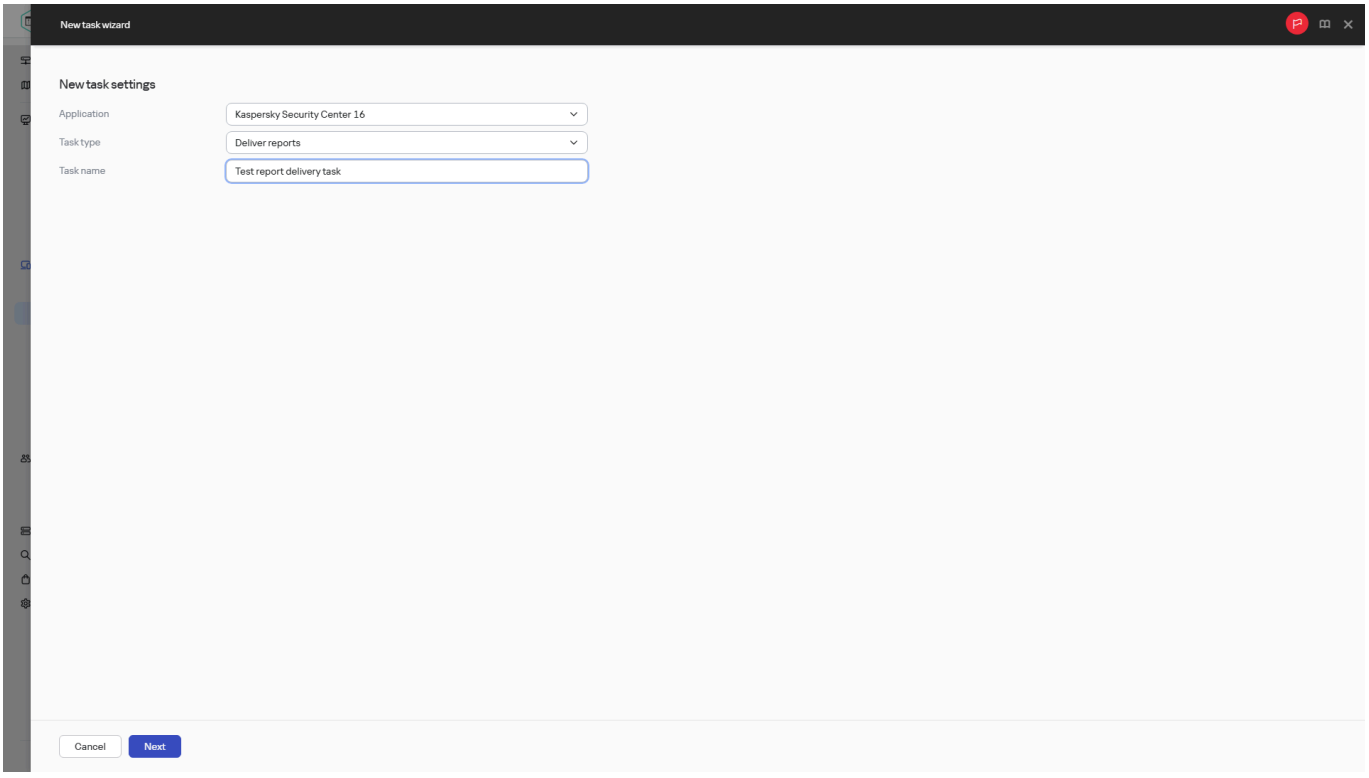
- 在**概要**頁籤：
  - 報告名稱和類型、簡要說明和報告時間區段，以及該報告為哪個裝置群組產生的相關資訊。
  - 圖表顯示最有代表性的報告資料。
  - 帶有計算好的報告指示器的加固表格。
- 在**詳細資訊**頁籤會顯示包含詳細報告資料的表格。

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** → **報告**。
2. 選取您要建立報告傳送工作之報告範本旁邊的核取方塊。
3. 點擊**建立交付工作**按鈕。
   新工作精靈啟動。使用**下一步**按鈕進行精靈。
4. 在精靈的**新工作設定**步驟中，輸入工作名稱。
   預設名稱是「**傳送報告**」。如果具有此名稱的工作已存在，則序號 (<N>) 會新增到工作名稱。



建立報告傳送工作

5. 在精靈的**報告組態**步驟中，指定以下設定：

   a. 要使用工作傳送的報告範本。

   b. 報告格式：HTML、XLS 或 PDF。

      需要使用 wkhtmltopdf 工具將報告轉換為 PDF。當您選擇 PDF 選項時，管理伺服器會檢查裝置上是否安裝了 wkhtmltopdf 工具。如果未安裝該工具，應用程式會顯示一條訊息，說明必須在管理伺服器裝置上安裝該工具。手動安裝該工具，然後繼續下一步。

   c. 報告是否使用電子郵件連同郵件通知設定一起傳送。

      您最多可以指定 20 個電子郵件地址。若要分開電子郵件地址，請按 **Enter**。您也可以貼上以逗號分隔的電子郵件地址清單，然後按 **Enter**。

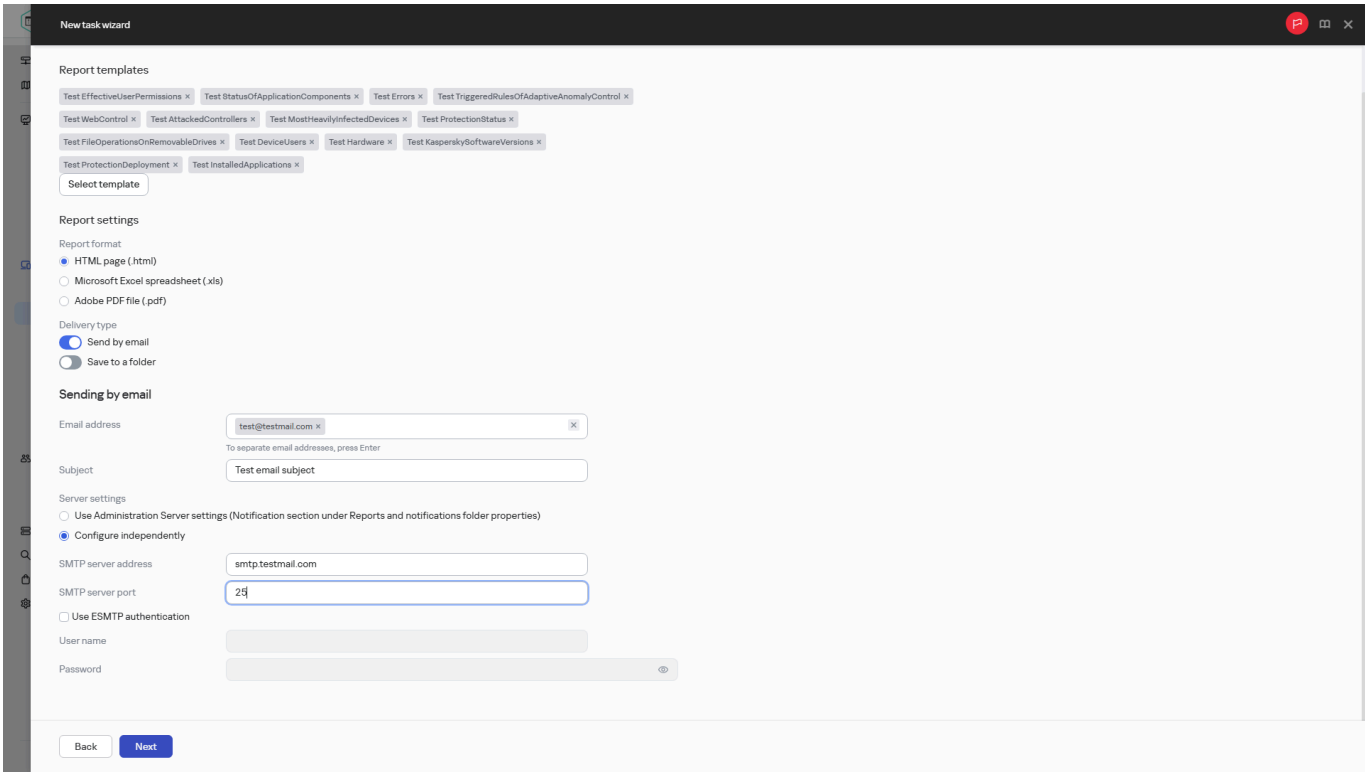
   d. 是否將報告以及相應的設定儲存到資料夾中。

      啟用 **儲存到資料夾**選項後，您必須指定該資料夾的 POSIX 路徑。如果要將報告儲存到共用資料夾，您還必須選取**指定帳戶以存取共用資料夾**核取方塊，然後指定用於存取此資料夾的使用者帳戶和密碼。

      > 如果選擇將報告儲存到共用資料夾，則必須確保可用從安裝了管理伺服器的裝置存取該資料夾。確保存取的方法和使用的工具取決於您的基礎架構。

      將報告儲存到本機資料夾時，通常不需要憑據，因為執行管理伺服器的帳戶可以存取此資料夾。如有必要，您可以在精靈的**選取要執行此工作的帳戶**步驟中指定使用者憑據。

      無論選擇哪個資料夾，如果您希望新的報告檔案覆蓋上次工作啟動時儲存在報告資料夾中的檔案，您也可以選取“**覆蓋相同類型的舊報告**核取方塊。



指定工作設定

6. 在精靈的**設定工作排程**步驟中，選取工作啟動排程。

可使用下方的工作排程選項：

- **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，工作每星期五於目前系統時間執行一次。

- **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。

- **在指定日期**

  工作定期在指定月日的指定時間執行。

  預設情況下，開始時間為18:00，且未選擇當月的任何日期。

  > 請注意，您選擇的是當月的週幾，而不是特定的日期或週數（例如，當月的第一週或第二週）。例如，如果您將遊標放在**週二**行的**第一**單元格中，則表示該工作將在每個月的第一個星期二執行。

  您可以選擇一週中的多個日期。

- **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**

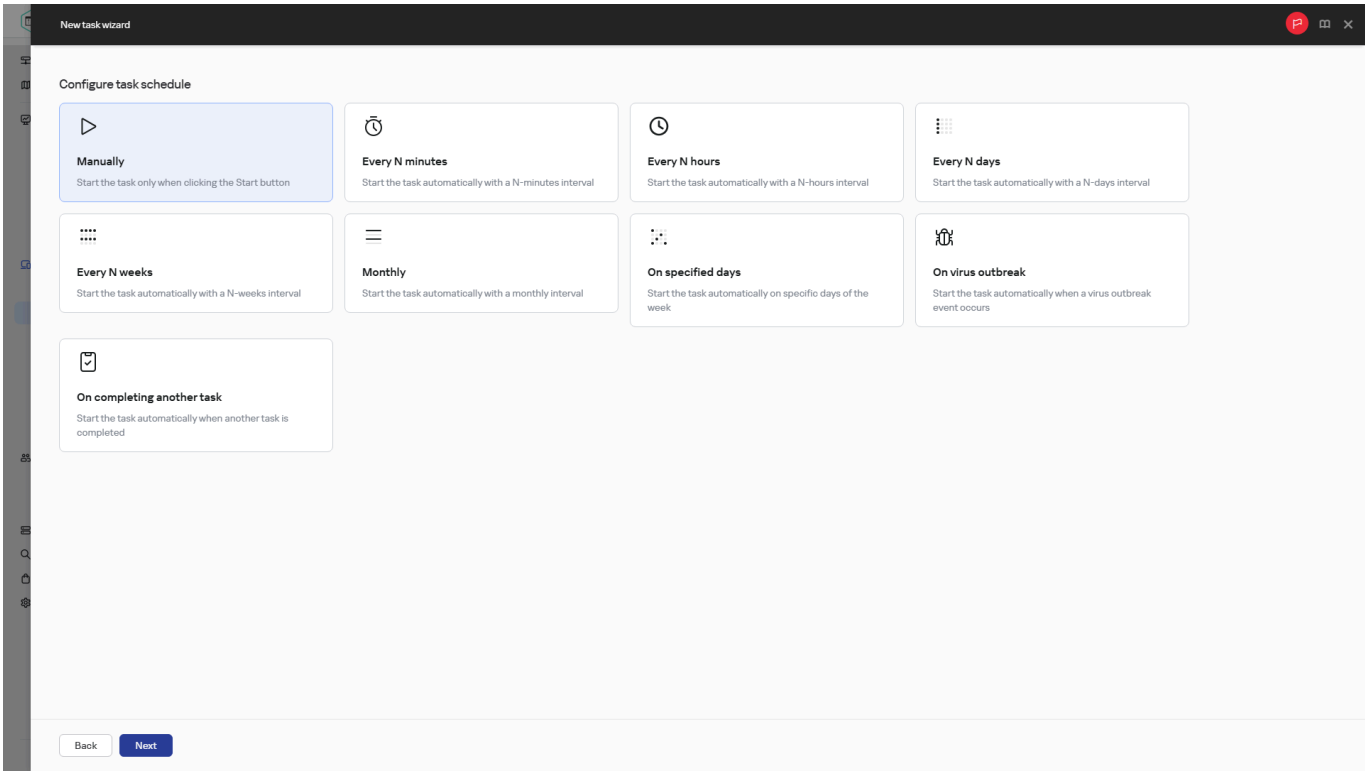
  目前工作在其他工作完成後啟動。只有在將這兩項工作指派給相同的裝置時，此選項才會發揮作用。例如，您可能想使用**開啟裝置**選項執行*受管理裝置*工作，完成後，請執行*病毒掃描*工作作為觸發工作。

  您必須從表格中選擇觸發工作以及此工作必須完成的狀態（**成功完成**或**失敗**）。

  如有需要，您可以對表格中的工作進行搜尋、排序和篩選，如下所示：

  - 在搜尋欄位中輸入工作名稱，可依其名稱搜尋工作。
  - 點擊排序圖示，可依名稱對工作進行排序。

    預設情況下，工作會依字母遞增排序。
  - 點擊篩選器圖示，在開啟的視窗中依群組篩選工作，然後點擊**套用**按鈕。



選擇工作啟動排程

7. 在精靈的這個步驟中，設定其他工作排程設定：

- 在**工作排程**區域中，檢查或重新設定先前選取的排程並設定時間間隔、每月或每週的天數、設定病毒爆發條件或完成另一個工作作為啟動工作的觸發條件。如果選擇了適用的排程，也可以在此區域中指定開始時間。

- 在**其他設定**區域中，指定下方設定：

  - **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化延遲**

    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。

  - **對於在以下間隔內啟動的工作，使用工作啟動自動隨機化延遲**

    如果該選項被啟用，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。

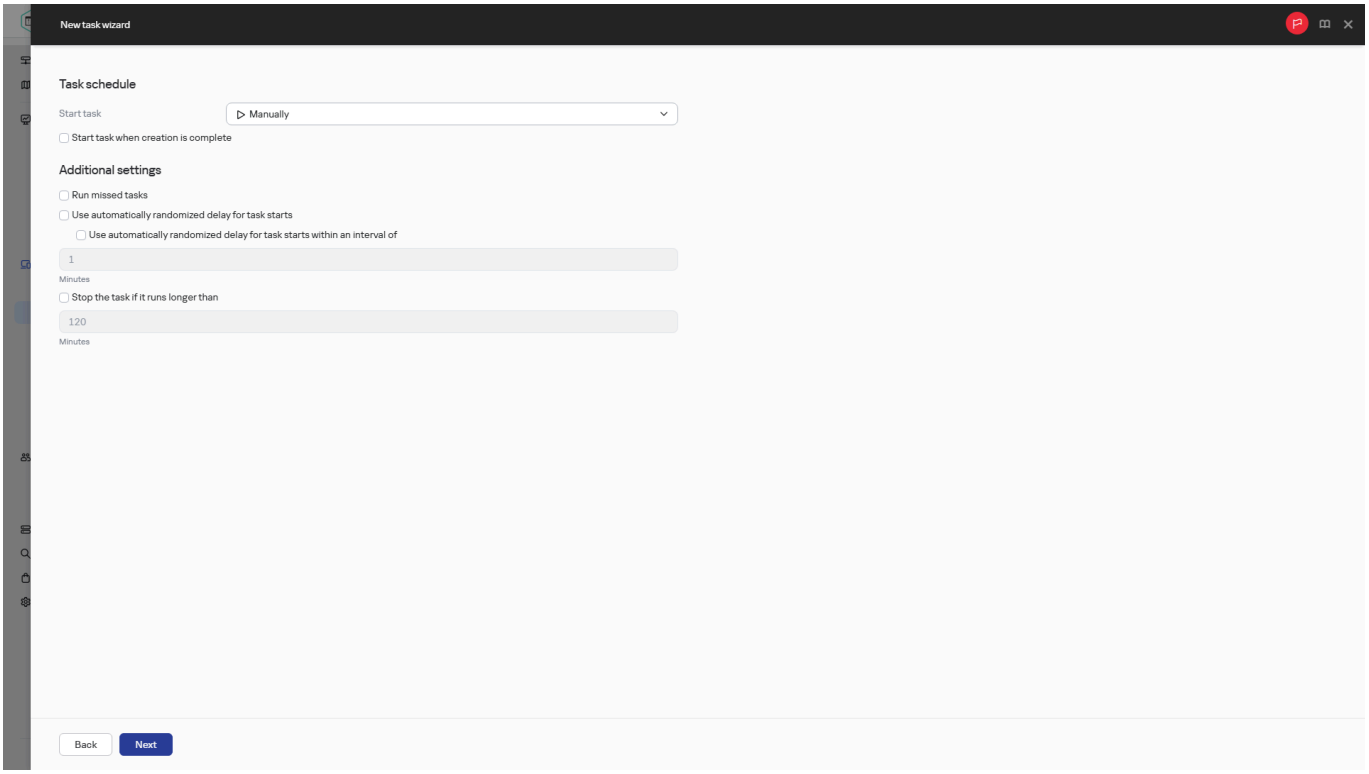
    預設情況下已停用該選項。預設時間間隔為一分鐘。

  - **停止工作，若執行時間超過**

    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。

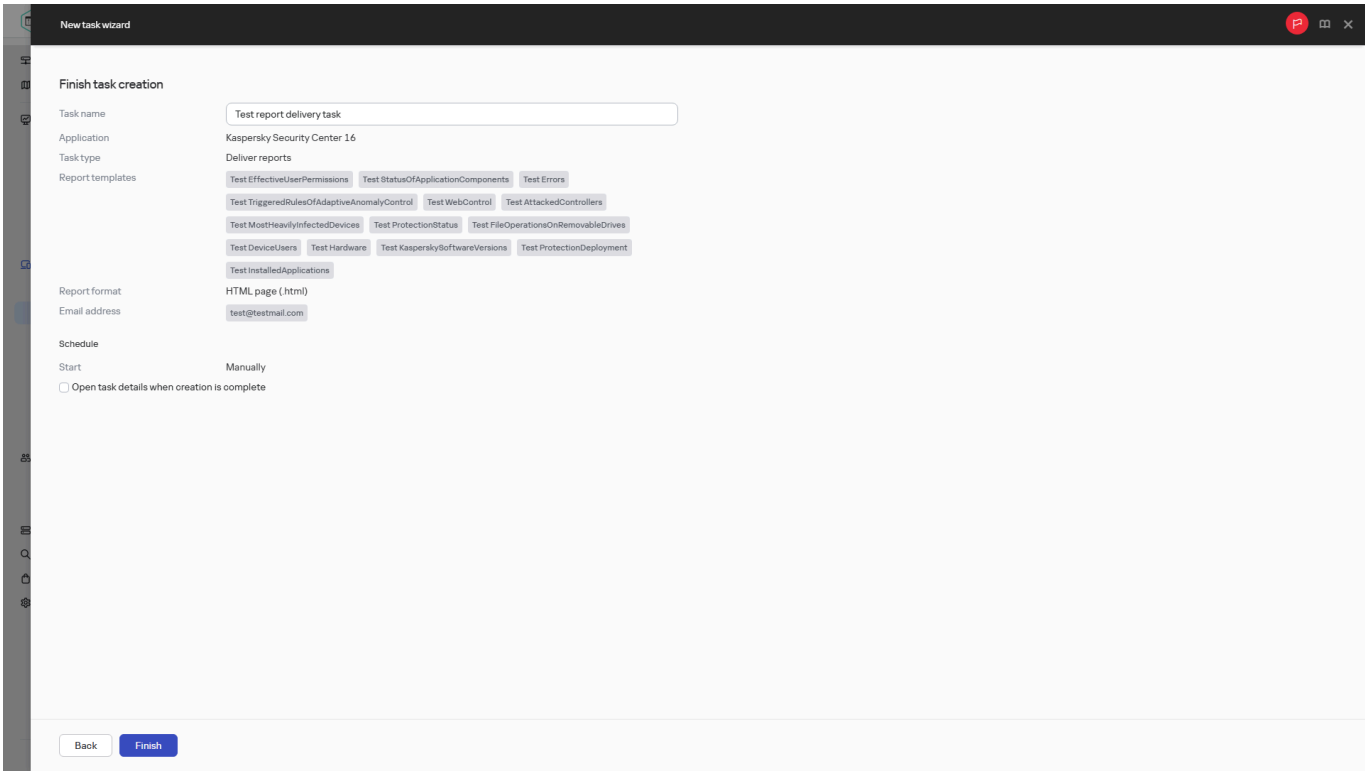


指定工作排程設定

8. 在精靈的**選取要執行此工作的帳戶**步驟中，指定用於執行工作的使用者帳戶憑證。

9. 若要在建立工作後修改其他工作設定，則在精靈的**完成工作建立**步驟中啟用**建立完成時開啟工作詳情**選項（預設啟用此選項）。

10. 點擊**完成**按鈕以建立工作並關閉精靈。



完成工作建立

報告傳送工作被建立。如果啟用**建立完成時開啟工作詳情**選項，則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** → **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。

防護等級指示器

防護等級指示器會顯示有關您的管理伺服器和發佈點防護的最新資訊。這可讓您追蹤強化指南的實作情況。此指示器會顯示在**監控→控制板** 中，且無法隱藏或放置到網頁主控台功能表的其他區段。按一下此指示器，即可轉至強化中心，檢視管理伺服器和發佈點的防護參數狀態。若要增強基礎設施的安全性，您必須解決任何指出的問題。

此指示器可能處於以下其中一種狀態：

- 已設定防護。
- 已部分設定防護。
- 未設定防護。

如何檢視防護等級的詳細資訊

整體指示器狀態由防護參數的狀態構成。

若要檢視參數，請按一下指示器。

在開啟的**強化中心** 視窗中，參數會依受保護物件分組：管理伺服器和發佈點。

每個防護參數會根據您的存取權限顯示為以下其中一種狀態：

- ：沒有需要解決的問題，或您沒有所需的存取權限。
- 或：有需要解決的問題。

以下參數僅針對管理伺服器顯示：

- 已設定備份
- 已設定管理伺服器維護
- 已啟用TLS加密

以下參數同時針對管理伺服器和發佈點顯示：

- 安全應用程式已安裝
- 已套用政策
- 已設定病毒資料庫更新

管理伺服器功能：

- 所有保護參數僅針對實體管理伺服器計算，並不套用至虛擬伺服器。

  如果您有多個管理伺服器的層級結構，保護等級指示器會分別針對每個實體伺服器計算。

- **已安裝的安全應用程式**、**已套用的政策**、**已設定**的**病毒資料庫更新**參數是針對已安裝管理伺服器的裝置計算的。

- 部署卡巴斯基安全管理中心 Linux 容錯移轉叢集時，會針對每個節點計算 **安全應用程式已安裝**、**已套用政策**、**病毒資料庫更新已設定**參數。只有在節點變成作用中後，才會將其納入指示器狀態計算。

指示器狀態的計算方式

指示器狀態的計算方法如表格所示。

指示器狀態	條件
已設定防護。	所有防護參數皆處於 ✅ 狀態。
已部分設定防護。	**已設定的病毒資料庫更新**參數處於 ⚠️ 狀態，而所有其他參數皆處於 ✅ 狀態。
未設定防護。	如果下列防護參數中至少有一個處於 ❌ 狀態。

安全應用程式已安裝

安全應用程式可讓您保護裝置免受各種類型的威脅，包括網路攻擊、網路釣魚攻擊和詐騙攻擊。

如果符合其中一個條件，參數會顯示為 ✅ 狀態：

- 您沒有這些裝置的存取權限。
- 您在**一般功能→基本功能**功能區域中擁有**讀取**權限，同時裝置上已安裝網路代理程式和安全應用程式。

> 根據您的存取權限，您可用的所有裝置都必須符合此條件，但以下裝置除外：已安裝不需要任何病毒防護之應用程式的裝置（例如，受保護的作業系統）、未安裝網路代理且其裝置資訊在不到 24 小時前才出現在管理伺服器上的裝置，以及上次連線至管理伺服器是在 7 天或更久之前的離線裝置。

如果符合下列至少一個條件，該參數會顯示為 ❌ 狀態。

您必須點擊**檢視裝置**按鈕，並針對顯示的裝置執行表格中說明的操作。

條件	解決方案
裝置上未安裝網路代理程式	安裝網路代理。 對於管理伺服器裝置，安裝網路代理程式最簡單的方法是使用獨立安裝套件。
裝置位於**未指派的裝置**群組中	將裝置移至「受管理裝置」群組或其子群組
找不到安全應用程式，或已安裝的安全應用程式未執行即時保護	安裝安全應用程式。應用程式會將防護狀態相關資料傳送至管理伺服器。 您可以在裝置設定：**一般**區段→**裝置狀態**中檢視裝置的防護狀態。 在管理伺服器裝置上，您必須安裝Kaspersky Endpoint Security for Linux。

已套用政策

政策是一組套用於管理群組及其子群組的安全應用程式設定。

如果符合其中一個條件，參數會顯示為 ✅ 狀態：

- 您沒有這些裝置的存取權限。
- 您在 **一般功能→基本功能**功能區域中具有**讀取**權限，而您的裝置上已安裝安全應用程式，且此安全應用程式的啟用政策已套用至這些裝置。

> 根據您的存取權限，您可用的所有裝置都必須符合此條件，但以下裝置除外：已安裝不需要任何病毒防護之應用程式的裝置（例如，受保護的作業系統）、未安裝網路代理且其裝置資訊在不到 24 小時前才出現在管理伺服器上的裝置，以及上次連線至管理伺服器是在 7 天或更久之前的離線裝置。

如果符合下列至少一個條件，該參數會顯示為 ❌ 狀態。

您必須點擊**檢視裝置**按鈕，並針對顯示的裝置執行表格中說明的操作。

條件	解決方案
裝置上未安裝安全應用程式。	請確認該裝置未包含在 **已安裝安全應用程式** 防護參數的選取範圍中。
政策未套用至裝置。	請確認已為裝置所屬的管理群組建立政策。 若未建立，請建立並啟用政策。 若已建立，請確保： • 已建立的政策處於啟用狀態。若未啟用，請啟用該政策。 • 政策分發狀態為**已成功套用**。 如果狀態為**套用時發生錯誤**，則必須在安全應用程式端修正此問題。

已設定病毒資料庫更新

由於病毒資料庫可保護您的裝置免受威脅，因此您必須定期且及時更新裝置上的病毒資料庫。

如果符合其中一個條件，參數會顯示為 ✅ 狀態：

- 您沒有這些裝置的存取權限。
- 您在 一般功能→基本功能 功能區域中擁有讀取權限，且裝置上的病毒資料庫已更新。

> 根據您的存取權限，您可用的所有裝置都必須符合此條件，但以下裝置除外：已安裝不需要任何病毒防護之應用程式的裝置（例如，受保護的作業系統）、未安裝網路代理且其裝置資訊在不到 24 小時前才出現在管理伺服器上的裝置，以及上次連線至管理伺服器是在 7 天或更久之前的離線裝置。

如果裝置上的病毒資料庫上次更新時間是在3天以前，該參數會顯示為 ⚠️ 狀態。

如果裝置上的病毒資料庫上次更新時間是在7天以前，該參數會顯示為 ❌ 狀態。

若要解決此問題：

1. 點擊該參數旁的「檢視裝置」按鈕。
2. 對於顯示的裝置，請執行下列操作：
   a. 請確認網路代理程式與管理伺服器之間已建立連線。
   如果尚未建立連線，請參閱以下文章：
   解決Kaspersky Endpoint Security for Linux病毒資料庫更新問題
   從卡巴斯基安全管理中心儲存庫更新病毒資料庫時出現的問題
   b. 請確保您檢查的病毒資料庫的卡巴斯基應用程式依舊在運行。
   如果應用程式不在運行，請啟動它。
   c. 在裝置上，檢視更新後發生的錯誤。

已設定備份

如需管理伺服器資料備份的建議，請參閱管理伺服器資料的備份與還原。

如果符合其中一個條件，參數會顯示為 ✅ 狀態：

- 您沒有執行管理伺服器資料備份工作的存取權限。
- 您在**一般功能** → **在管理伺服器上操作**功能區域中具有**讀取**、**寫入**和**執行**權限，且備份已設定並定期執行。

如果符合下列至少一個條件，該參數會顯示為 ❌ 狀態。

條件	解決方案
尚未建立管理伺服器資料備份工作。	建立工作。
尚未為管理伺服器資料備份工作設定必要的排程。	在「管理伺服器」維護工作中，指定**在偵測到病毒爆發時**和**手動**以外的**開始工作**設定。

已設定管理伺服器維護

管理伺服器維護可讓您釋放管理伺服器資料夾中的空間，並將資料庫大小降至最低。這有助於加快請求處理速度，並提高系統的整體穩定性。

如果符合其中一個條件，參數會顯示為 ✅ 狀態：

- 您沒有執行管理伺服器維護工作的存取權限。
- 您在**一般功能** → **在管理伺服器上操作**功能區域中具有**讀取**、**寫入**和**執行**權限，且已設定管理伺服器維護並定期執行。

> 必須在管理伺服器層級設定權限。

如果符合下列至少一個條件，該參數會顯示為 ❌ 狀態。

條件	解決方案
尚未建立管理伺服器維護工作。	建立工作。
未設定管理伺服器維護工作所需的排程。	在「管理伺服器」維護工作中，指定**在偵測到病毒爆發時**和**手動**以外的**開始工作**設定。

已啟用TLS加密

您必須確保僅允許使用TLS通訊協定1.2和1.3版本。允許使用舊版本會造成嚴重的資料安全風險，並使系統容易受到攻擊。

如果僅允許使用TLS通訊協定1.2和1.3版本，則此參數會顯示為 ✅ 狀態。

如果允許使用早於1.2的過時TLS版本，則此參數會顯示為 ❌ 狀態。

若要解決此問題，您必須將SrvUseStrictSslSettings旗標設定為4或5值。

事件和事件分類

本節提供有關事件和事件分類、卡巴斯基安全管理中心 Linux 元件中發生的事件類型以及管理頻繁事件封鎖的資訊。

卡巴斯基安全管理中心 Linux 中的事件

卡巴斯基安全管理中心 Linux 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 Linux 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

您可以在應用程式政策的**事件組態**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。

事件可以由以下應用程式產生：

- 卡巴斯基安全管理中心 Linux 元件：
  - 管理伺服器
  - 網路代理
- 受管卡巴斯基應用程式

  有關卡巴斯基受管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。

事件重要性等級

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過程執行中發生了嚴重問題、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 Linux 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。

卡巴斯基安全管理中心 Linux 元件的事件

每個 卡巴斯基安全管理中心 Linux 元件都擁有自己的事件類型集。本章列出了 卡巴斯基安全管理中心 管理伺服器和網路代理中發生的事件的類型。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**事件組態**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、識別碼（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 Linux 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 Linux 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。

  您可以變更事件的儲存期限：設定事件的儲存期限

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。

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**事件組態**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。

管理伺服器緊急事件

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
行動裝置的管理伺服器憑證已過期	6129	KLSRV_EV_SRV_CERT_EXPIRED_DN	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。	180 天
稽核：匯出到 SIEM 失敗	5130	KLAUD_EV_SIEM_EXPORT_ERROR	當匯出事件到 SIEM 系統因 SIEM 系統連線錯誤而失敗時，會發生此類型的事件。	180 天
裝置已不受管理	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。您可設定將裝置狀態變更為緊急的條件。	180 天
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 Linux 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。無法變更此天數。如果管理伺服器在產品授權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 Linux 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
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 Linux 決定當產品授權限制被超過時產生事件的規則。	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
受限功能模式	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	當卡巴斯基安全管理中心 Linux 開始用基本功能操作，而非「弱點和修補程式管理」及「行動裝置管理」功能時，該類型事件發生。 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 Linux 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
MDM 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
金鑰檔案已新增到拒絕清單	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
卡巴斯基應用程式模組更新已撤銷	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 Linux 修補程式且不涉及卡巴斯基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
病毒爆發	• 26（對於檔案威脅防護） • 27（對於郵件威脅防護） • 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。	

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**事件組態**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
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
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
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 Linux 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
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
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： • 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 政策設定。 在 DBMS 選項處檢視資訊。	180 天
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
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 DBMS 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。	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**事件組態**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
行動裝置的管理伺服器憑證即將過期	6128	KLSRV_EV_SRV_CERT_EXPIRES_SOON	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
APN 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
APN 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
稽核：SIEM 伺服器連線測試失敗	5120	KLAUD_EV_SIEM_TEST_FAILED	當 SIEM 伺服器自動連線測試失敗時，會發生此類型的事件。	90 天
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： • 已針對憑證的以下內容啟動自動重新發佈：已停用**如果可能，自動重新發佈憑證**選項。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
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
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作業係統記錄，並據此做出回應。	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作業係統記錄，並據此做出回應。	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

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
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。您可設定將裝置狀態變更為*警告*的條件。	90 天
下載檔案到裝置失敗	4165	KLSRV_FILE_DOWNLOAD_FAILED	此類事件會在以下情況發生： • 您嘗試將檔案下載到企業容器中，但尚未建立企業容器。 • 裝置空間不足。 • 無法從伺服器下載檔案資訊。 • 無法從伺服器下載檔案內容。 • 無法在裝置上建立資料夾。 • 個人裝置上缺少檔案存取權限。 • 企業容器中缺少檔案存取權限。	90 天
傳送 FCM 訊息到 FCM 伺服器失敗	4140	KLSRV_GCM_GENERAL_ERROR	使用 Google 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
傳送 FCM 訊息到行動裝置失敗	4138	KLSRV_GCM_DEVICE_ERROR	當配置行動裝置管理使用 Google 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 Google Firebase 服務文件（請參閱「下游訊息錯誤回應程式碼」一章）。	90 天
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
硬碟磁碟機幾乎已滿	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
傳送 FCM 訊息到 FCM 伺服器時發生 HTTP 錯誤	4139	KLSRV_GCM_HTTP_ERROR	當配置行動裝置管理使用 Google 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 Google 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）。讀取事件詳細資訊中的 HTTP 程式碼，並據此做出回應。	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
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 Linux 決定當產品授權限制被超過時產生事件的規則。	90 天
已授權應用程式群組之一的安裝即將達到限制	4128	KLSRV_INVLICPROD_EXPIRED_SOON	當已授權應用程式群組中包含的協力廠商應用程式的產品授權金鑰之一即將過期時，就會發生此類事件。結果，其中一個群組的安裝限制將被減少。 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
已註冊卡巴斯基應用程式模組的新更新	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。 使用卡巴斯基安全管理中心網頁主控台核准或拒絕更新。	90 天
管理伺服器資料庫空間不足	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。 • 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
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

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**事件組態**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
行動裝置的管理伺服器憑證正在更新中	6127	KLSRV_EV_SRV_CERT_RENEWED	當管理伺服器憑證已續約時會發生此事件。	30 天
稽核：指令已傳送到裝置	4170	KLAUD_EV_COMMAND_SENT	當使用者向行動裝置傳送指令時，會發生此類事件。	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：到管理伺服器的連線已建立	4147	KLAUD_EV_SERVERCONNECT	當使用者使用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。	30 天
稽核：加密金鑰已匯入/匯出	5100	KLAUD_EV_DPEKEYSEXPORT	例如，遷移期間會發生該事件。	30 天
稽核：群組設定已修改	4149	KLAUD_EV_ADMGROUP_CHANGED	當安全群組已被編輯時，該類型事件發生。	30 天
稽核：物件已修改	4148	KLAUD_EV_OBJECTMODIFY	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	30 天
稽核：物件內容已修改	4152	KLAUD_EV_OBJECTPROPMODIFIED	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	30 天
稽核：物件狀態已修改	4150	KLAUD_EV_TASK_STATE_CHANGED	例如，當工作因錯誤而失敗時會發生此事件。	30 天
稽核（SIEM 伺服器連線測試成功）	5110	KLAUD_EV_SIEM_TEST_SUCCESS	當 SIEM 伺服器連線測試成功時，該事件發生。	30 天
稽核：使用者權限已修改	4153	KLAUD_EV_OBJECTACLMODIFIED	當使用者權限被修改時會發生該事件。	30 天
連到主管理伺服器的連線已建立	4117	KLSRV_EV_MASTER_SRV_CONNECTED		30 天
連到從屬管理伺服器的連線已建立	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	有關詳細資訊，請參閱以下文章：建立管理伺服器階層架構：新增從屬管理伺服器。	30 天
資料庫已更新	4144	KLSRV_UPD_BASES_UPDATED	當**將更新下載至管理伺服器儲存區**工作完成資料庫更新時，該類型事件發生。	30 天
裝置已被自動新增到群組	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	當根據行動裝置規則將裝置分配到群組時，會發生此類事件。	30 天
根據規則自動移動裝置	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	當已使用裝置移動規則將裝置移動到管理群組時，會發生此類事件。	30 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
裝置已從群組中刪除：長時間在網路中不活動	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	當裝置因無活動而自動從群組中刪除時，該類型事件發生。	30 天
此行動裝置上的 FCM 實例 ID 已被變更	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	當裝置上的 Firebase Cloud Messaging 權杖變更時，該類型事件發生。 有關 FCM 權杖輪換的資訊，請參閱 Firebase 服務文件。	30 天
檔案被從管理伺服器中刪除	4163	KLSRV_FILE_REMOVED	當檔案被從管理伺服器中刪除時會發生該事件。	30 天
檔案已下載到裝置	4164	KLSRV_FILE_DOWNLOADED	在以下情況下發生該事件： • 在工作階段中檔案已被下載到裝置。 • 檔案已從管理伺服器下載。	30 天
找到了要傳送至 Kaspersky 以分析的檔案	4131	KLSRV_APS_FILE_APPEARED		30 天
檔案已上傳到管理伺服器	4162	KLSRV_FILE_UPLOADED	當檔案被上傳到管理伺服器時會發生該事件。	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 90% 以上）	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。	30 天
已偵測到新裝置	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	當發現新的連網裝置時，就會發生此類事件。	30 天
產品授權金鑰的 90% 已經使用	4097	KLSRV_EV_LICENSE_CHECK_90	當管理伺服器偵測到安裝在用戶端裝置上的 Kaspersky 應用程式即將超過某些產品授權限制，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構成超過該產品授權覆寫的單元總數的 90%，則該類型的事件發生。 即使超出許可限制，用戶端裝置也會受到防護。 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 Linux 決定當產品授權限制被超過時產生事件的規則。	30 天
已為行動裝置創建預留管理伺服器憑證	6126	KLSRV_EV_SRV_CERT_RESERVE_CREATED	當管理伺服器憑證已建立時會發生此事件。	30 天
更新被成功複製至指定的資料夾	4122	KLSRV_UPD_REPL_OK	當**將更新下載至管理伺服器儲存區**工作已將檔案複製到指定資料夾時，該類型事件發生。	30 天

僅當對行動裝置和UEFI裝置的管理伺服器憑證執行了對應操作時，管理伺服器才會自動發布並在管理主控台中顯示**備用憑證已建立**與**憑證續約**事件。

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 Linux 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**事件組態**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
安裝根憑證失敗	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	事件包含憑證安裝錯誤的描述。	30 天
安裝協力廠商軟體更新失敗	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	如果正在使用弱點和修補程式管理功能，且協力廠商軟體更新未成功，該類型事件發生。 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。 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
無法刪除根憑證	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	事件包含憑證移除錯誤的描述。	30 天
未能將 sudoers 檔案還原到參考值	7726	KLNAG_EV_SUDOER_RESTORED_ERR	事件包含 sudoers 文件替換錯誤的描述。	30 天
更新安裝錯誤	7702	KLNAG_EV_PATCH_INSTALL_ERROR	如果卡巴斯基安全管理中心 Linux 元件自動更新和修補程式未成功，該類型事件發生。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
使用者管理：錯誤	7723	KLNAG_EV_USR_MNG_ERR	一般警告事件。	30 天

網路代理警告事件

下表顯示具有**警告**嚴重等級的網路代理事件。

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**事件組態**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	敘述	預設儲存期限
KSN 代理已啟動。檢查 KSN 可用性失敗	7718	KSNPROXY_STARTED_CON_CHK_FAILED	當已設定的 KSN 代理連線的連線測試失敗時，該類型事件發生。	30 天
發生了安全問題	549	GNRL_EV_APP_INCIDENT_OCCURED	當在裝置上發現事件時，該類型事件發生。例如，當裝置磁碟空間不足時，就會發生該類型事件。	30 天
Sudoers 檔案與參考值不匹配	7724	KLNAG_EV_SUDOER_DIFFERENT	當 sudoers 檔案與參考檔案不符時，就會發生此類事件。	30 天
協力廠商軟體更新已延時	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	例如，當第協力廠商更新安裝的 EULA 被拒絕時，就會發生該類型事件。	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	下載偵錯檔案並檢查 KLRI_PATCH_RES_DESC 欄位的值以了解詳細資訊。	30 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
使用者管理：警告	7722	KLNAG_EV_USR_MNG_WRN	一般警告事件。	30 天
在安裝軟體模組更新期間返回了警告	7701	KLNAG_EV_PATCH_INSTALL_WARNING	下載偵錯檔案並檢查 KLRI_PATCH_RES_DESC 欄位的值以了解詳細資訊。	30 天

網路代理資訊事件

下表顯示具有**資訊**嚴重等級的網路代理事件。

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**事件組態**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
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
收到網頁伺服器 HTTPS 連接埠的憑證	—	WEB_SERVER_CERTIFICATE_RENEWED	30 天
裝置已被授權	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 天
已偵測到新裝置	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 天
裝置已被刪除	7709	KLNAG_EV_DEVICE_REMOVE	30 天
軟體模組更新安裝已啟動	7700	KLNAG_EV_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
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
已新增裝置	7708	KLNAG_EV_DEVICE_ARRIVAL	30 天
根憑證已安裝	7727	KLNAG_EV_ROOT_CERT_INSTALLED	30 天
根憑證已移除	7729	KLNAG_EV_ROOT_CERT_REMOVED	30 天
Sudoers 檔案已被成功還原到參考值	7725	KLNAG_EV_SUDOER_RESTORED	30 天
已安裝協力廠商應用程式	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	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
軟體模組更新已成功安裝	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 天
使用者管理：資訊	7721	KLNAG_EV_USR_MNG_INF	30 天
網頁伺服器在主機上啟動	—	WEB_SERVER_STARTED	30 天
網頁伺服器在主機上停止	—	WEB_SERVER_STOPPED	30 天
Windows 桌面共用：應用程式已啟動	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 天
Windows 桌面共用：檔案已修改	7713	KLUSRLOG_EV_FILE_MODIFIED	30 天
Windows 桌面共用：檔案已讀取	7712	KLUSRLOG_EV_FILE_READ	30 天
Windows 桌面共用：已啟動	7715	KLUSRLOG_EV_WDS_BEGIN	30 天
Windows 桌面共用：已停止	7716	KLUSRLOG_EV_WDS_END	30 天

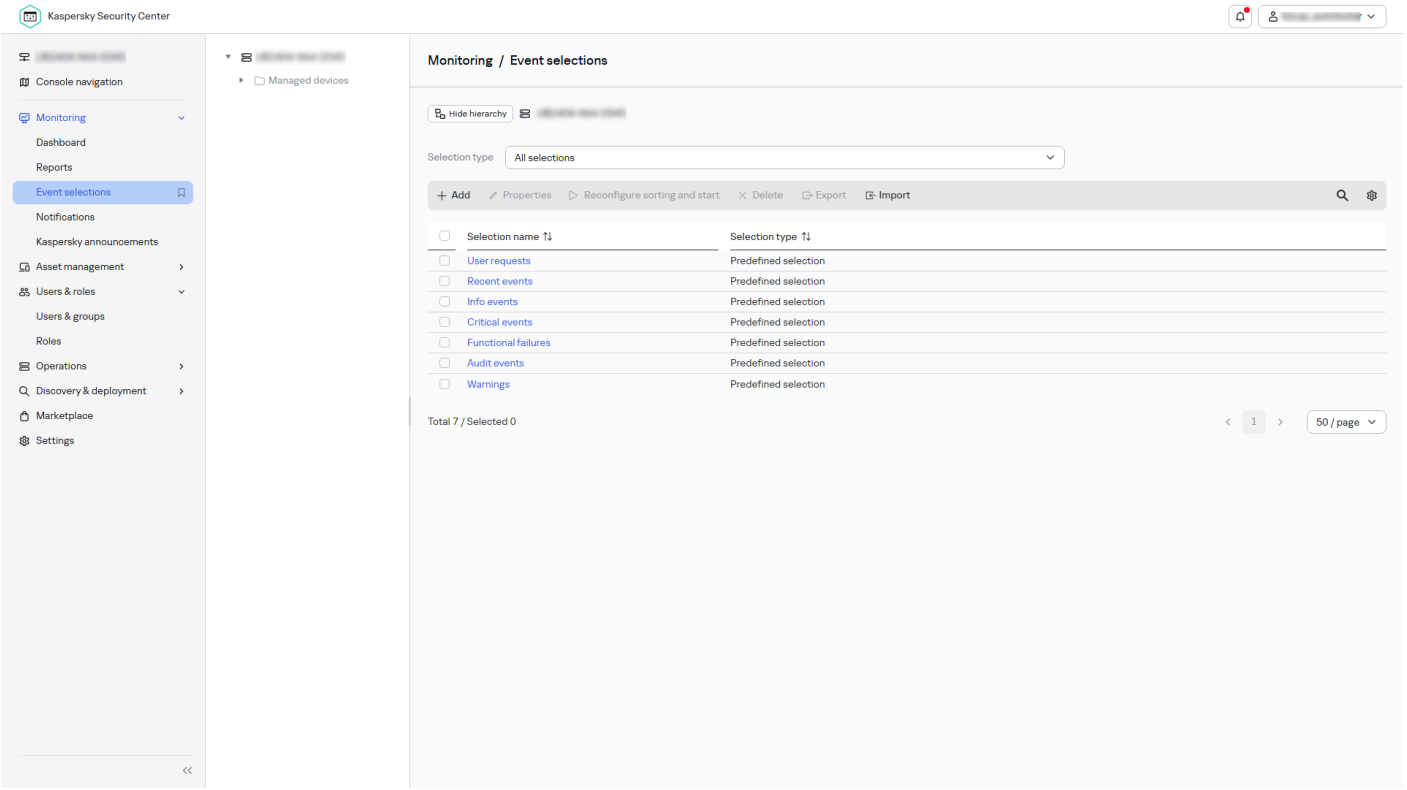
使用事件分類

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**區段點擊**事件分類**。



事件分類清單

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 Linux 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 Linux 顯示事件所花費的時間。資料庫越大，過程越耗時。

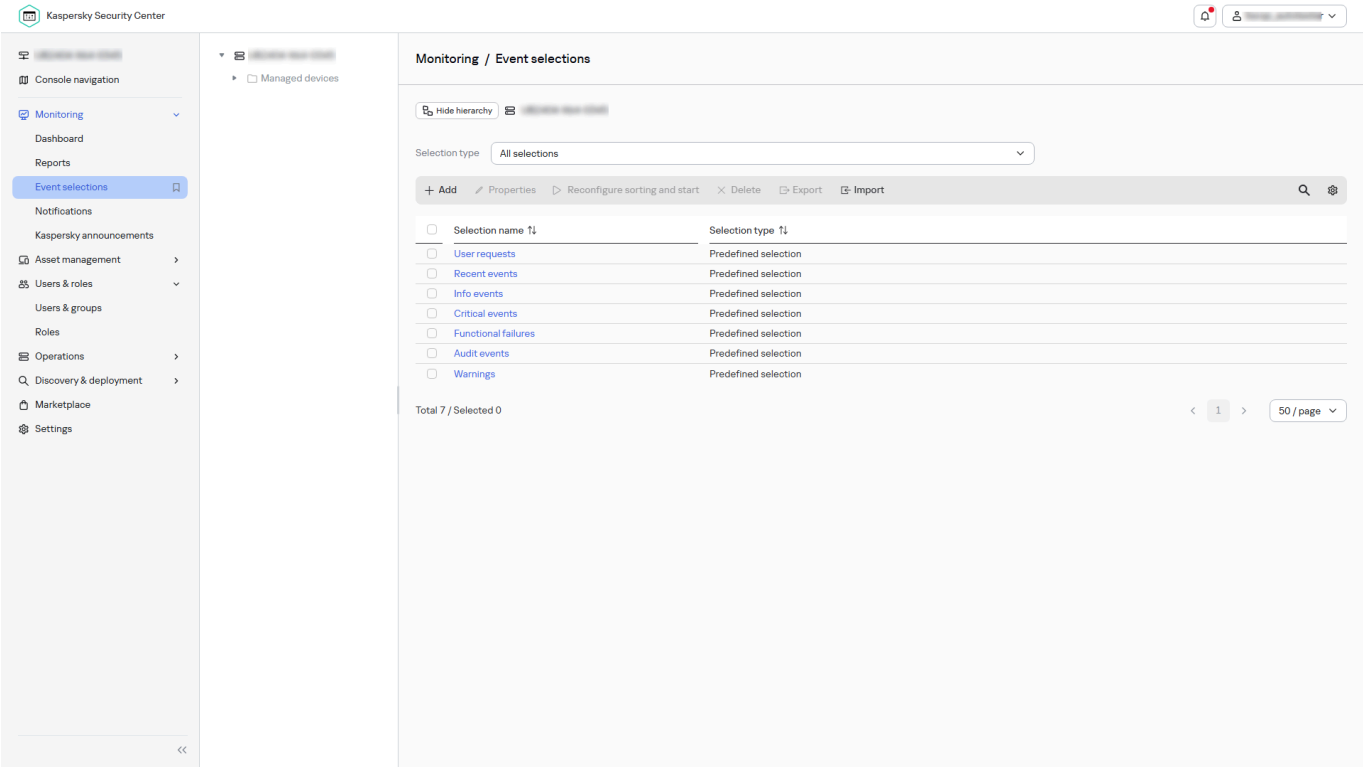
您可以執行以下操作：

- 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：

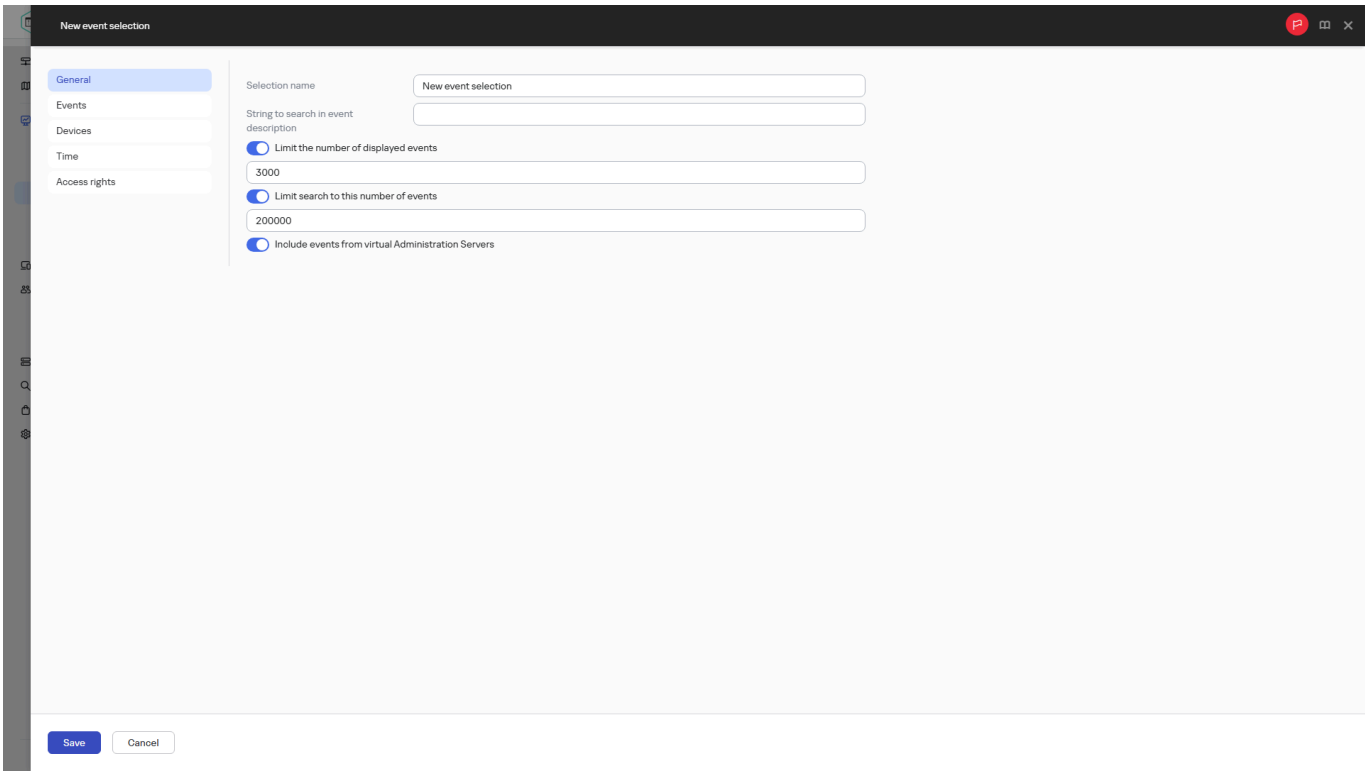
1. 在主功能表中，轉至 **監控** → **事件分類**。



事件分類清單

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。



建立新的事件分類

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。

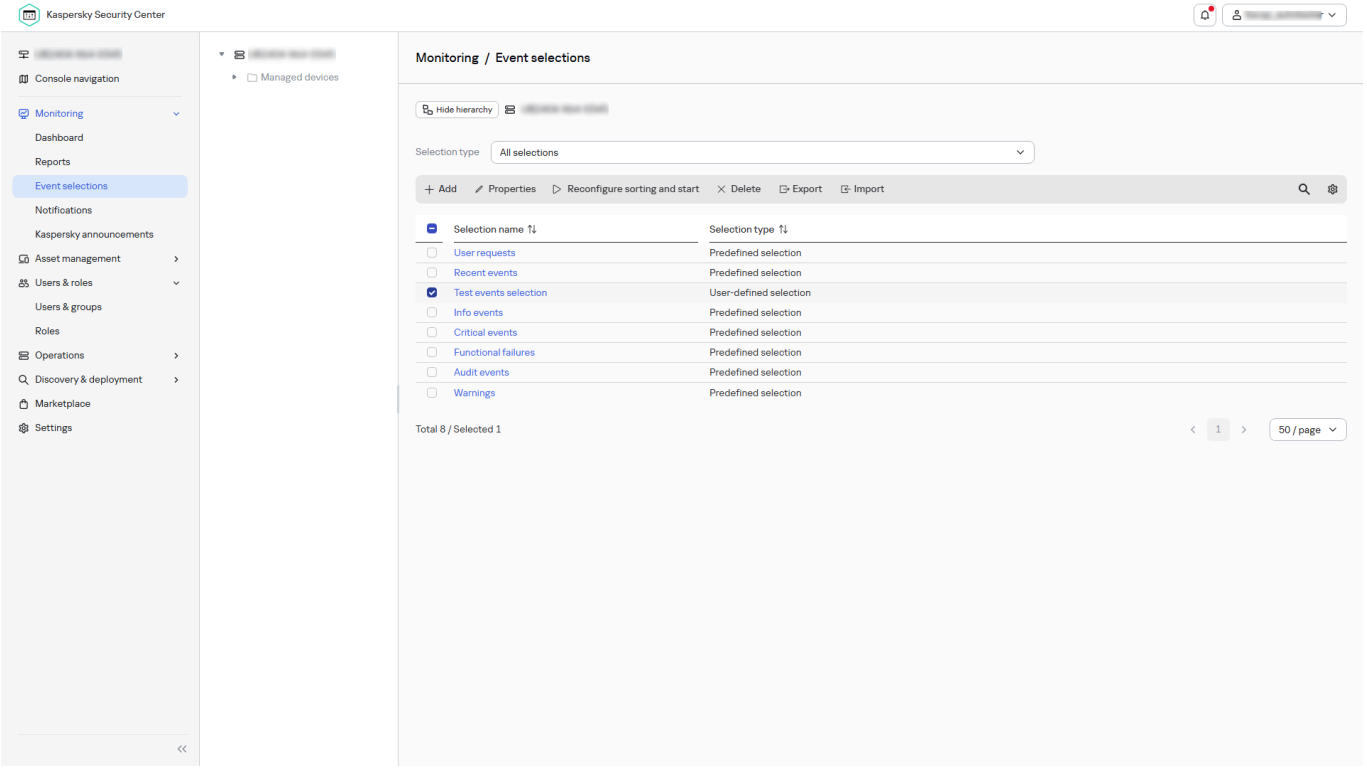
若您持續選取**轉到分類結果**核取方塊，會顯示事件分類結果。否則，新事件分類出現在事件分類清單。

編輯事件分類

要編輯事件分類：

1. 在主功能表中，轉至 **監控** → **事件分類**。

2. 選取您要編輯的事件分類旁邊的核取方塊。



事件分類清單

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。

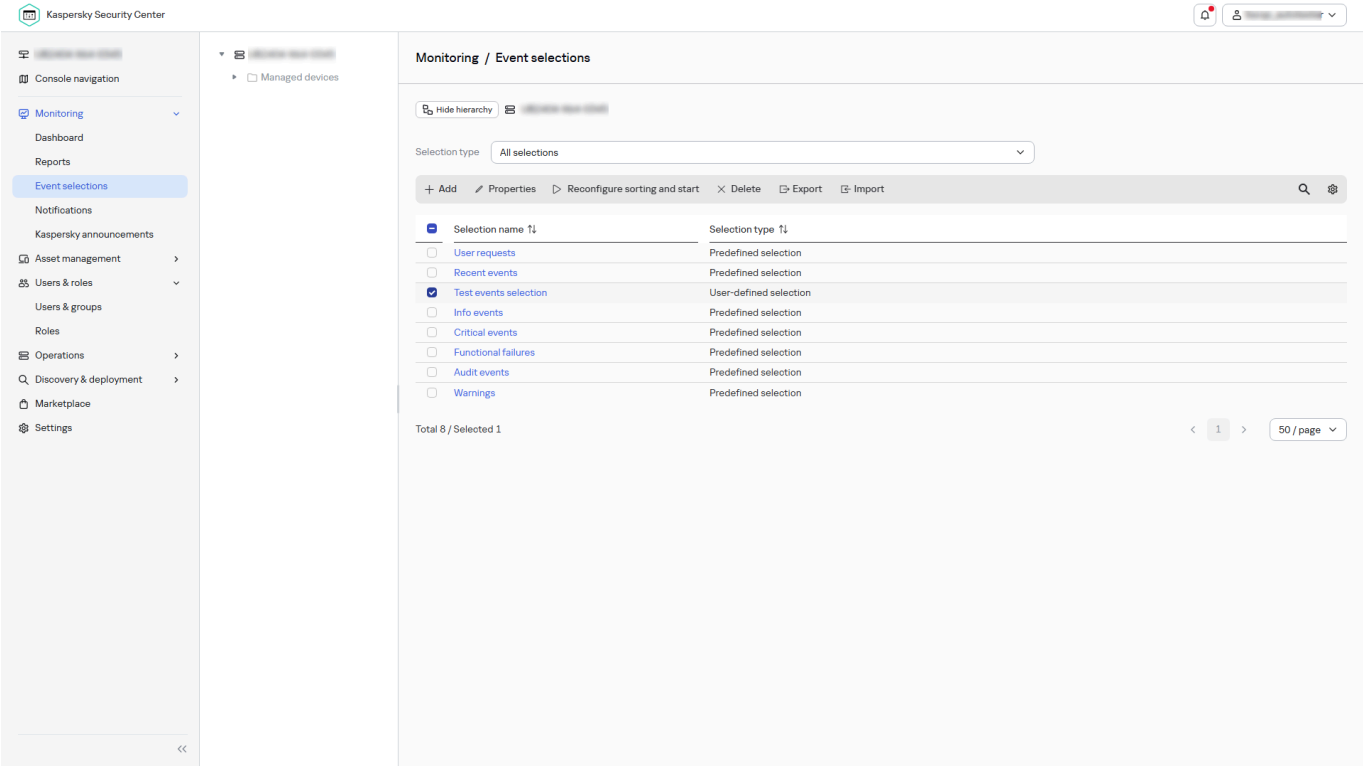
編輯的事件分類顯示在清單。

檢視事件分類清單

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** → **事件分類**。

2. 選取您要啟動的事件分類旁邊的核取方塊。



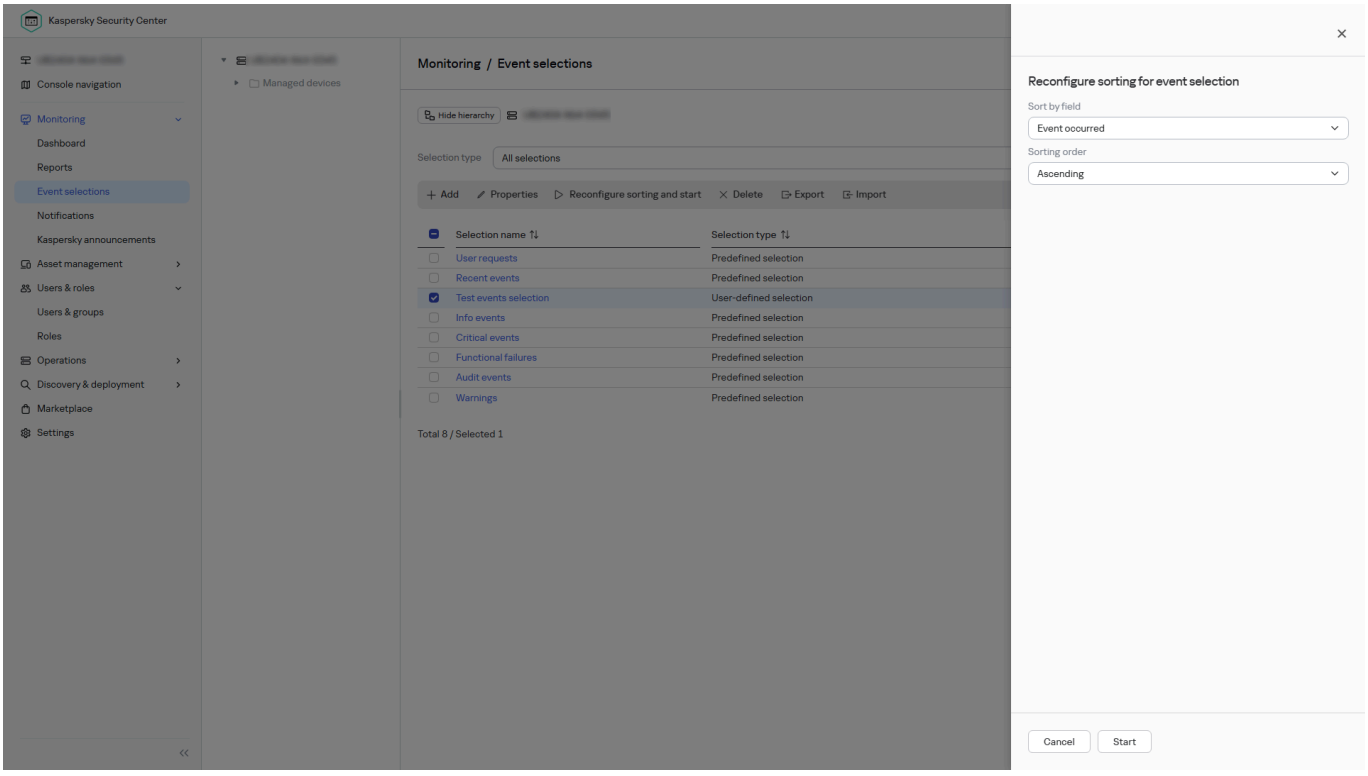
事件分類清單

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**重新設定排序並啟動**按鈕。

  b. 在顯示的 **重新設定事件分類排序** 視窗中指定排序設定。

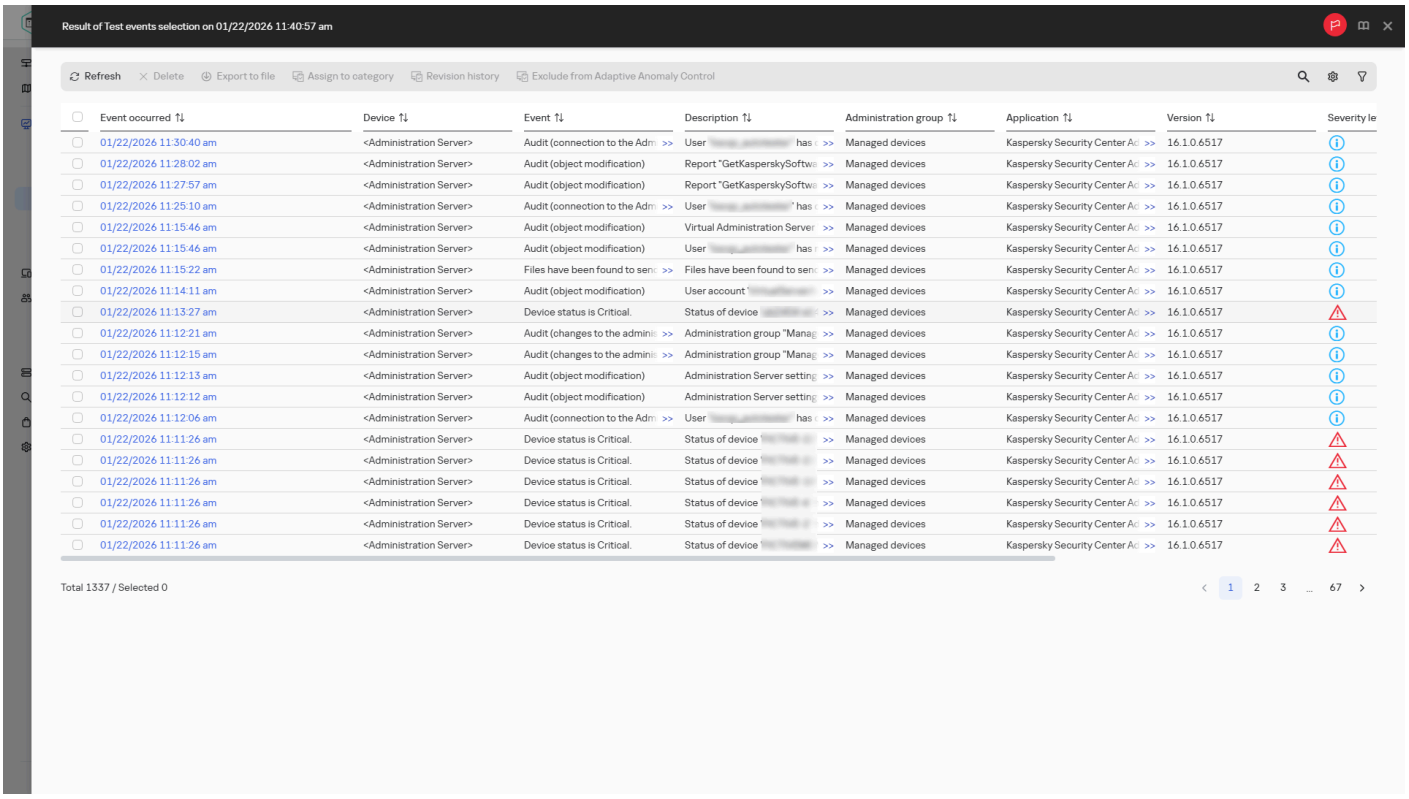


指定事件分類的排序設定

  a. 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。



事件分類結果

匯出事件分類

卡巴斯基安全管理中心 Linux 允許您將事件分類及其設定儲存到 KLO 檔案。您可以使用此 KLO 檔案匯入儲存的事件分類到卡巴斯基安全管理中心 Windows 和卡巴斯基安全管理中心 Linux。

請注意，您只能匯出使用者定義的事件分類。卡巴斯基安全管理中心 Linux 預設集合中的事件分類（預定義選擇）無法儲存到檔案中。

要匯出事件分類，請執行以下操作：

1. 在主功能表中，轉至**監控** → **事件分類**。
2. 選取您要匯出的事件分類旁邊的核取方塊。

   您不能同時匯出多個事件分類。如果您選擇了多個分類，**匯出**按鈕將被停用。
3. 點擊**匯出**按鈕。
4. 在開啟的**另存為**視窗中，指定事件分類檔案名稱和路徑，然後點擊**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，事件分類檔案會自動儲存在**下載**資料夾中。

匯入事件分類

卡巴斯基安全管理中心 Linux 允許您從 KLO 檔案匯入事件分類。KLO 檔案包含匯出事件分類及其設定。

要匯入事件分類，請執行以下操作：

1. 在主功能表中，轉至**監控 → 事件分類**。
2. 點擊**匯入**按鈕，然後選擇要匯入的事件分類檔案。
3. 在開啟的視窗中，指定 KLO 檔案的路徑，然後按一下**開啟**按鈕。請注意，您只能選擇一個事件分類檔案。
   事件分類處理開始。

此時會顯示匯入結果通知。如果事件分類匯入成功，您可以點擊**檢視匯入詳細資訊**連接來檢視事件分類屬性。

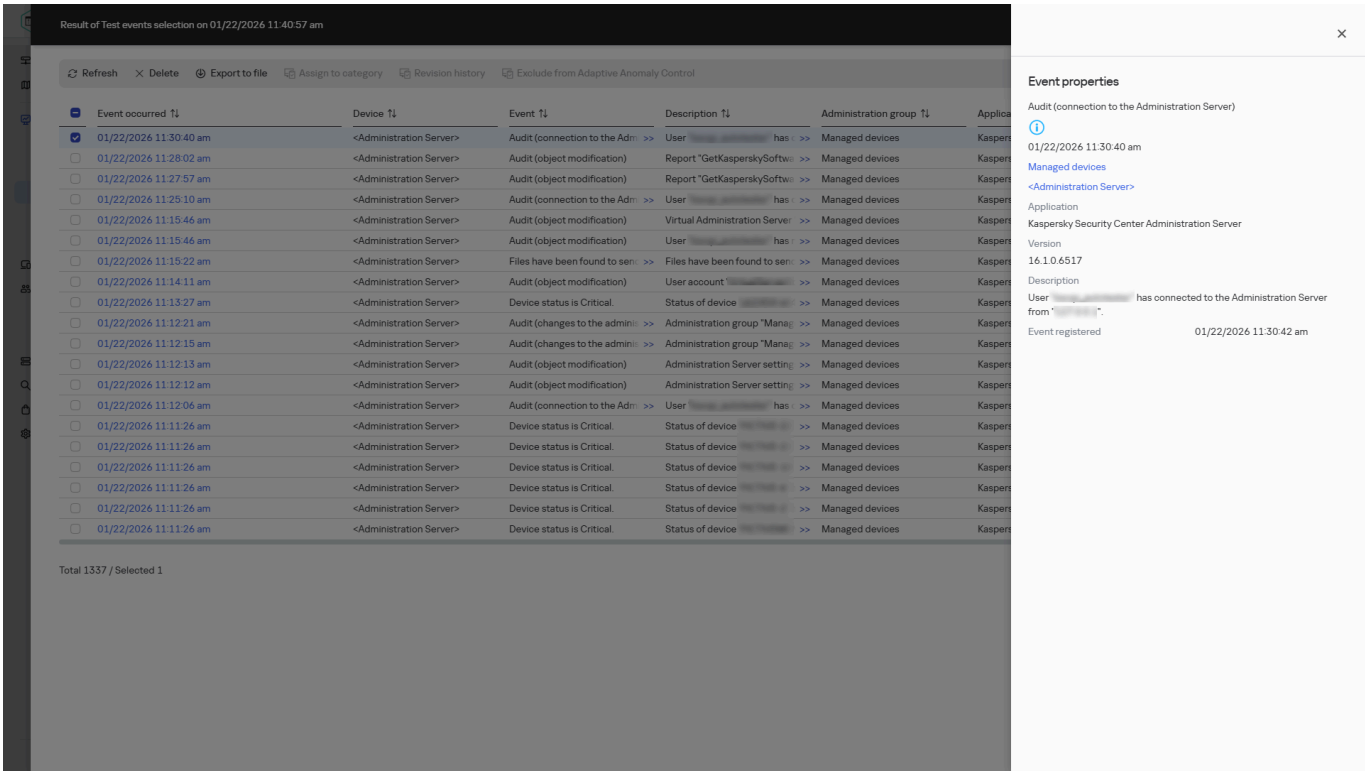
匯入成功後，事件分類會顯示在分類清單中。事件分類的設定也會被匯入。

> 如果新匯入事件分類的名稱與現有事件分類的名稱相同，則匯入分類的名稱將加上 **(<next sequence number>)** 索引，例如：**(1)**、**(2)**。

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。



"事件內容"視窗

3. 在顯示的視窗中，您可以做以下：

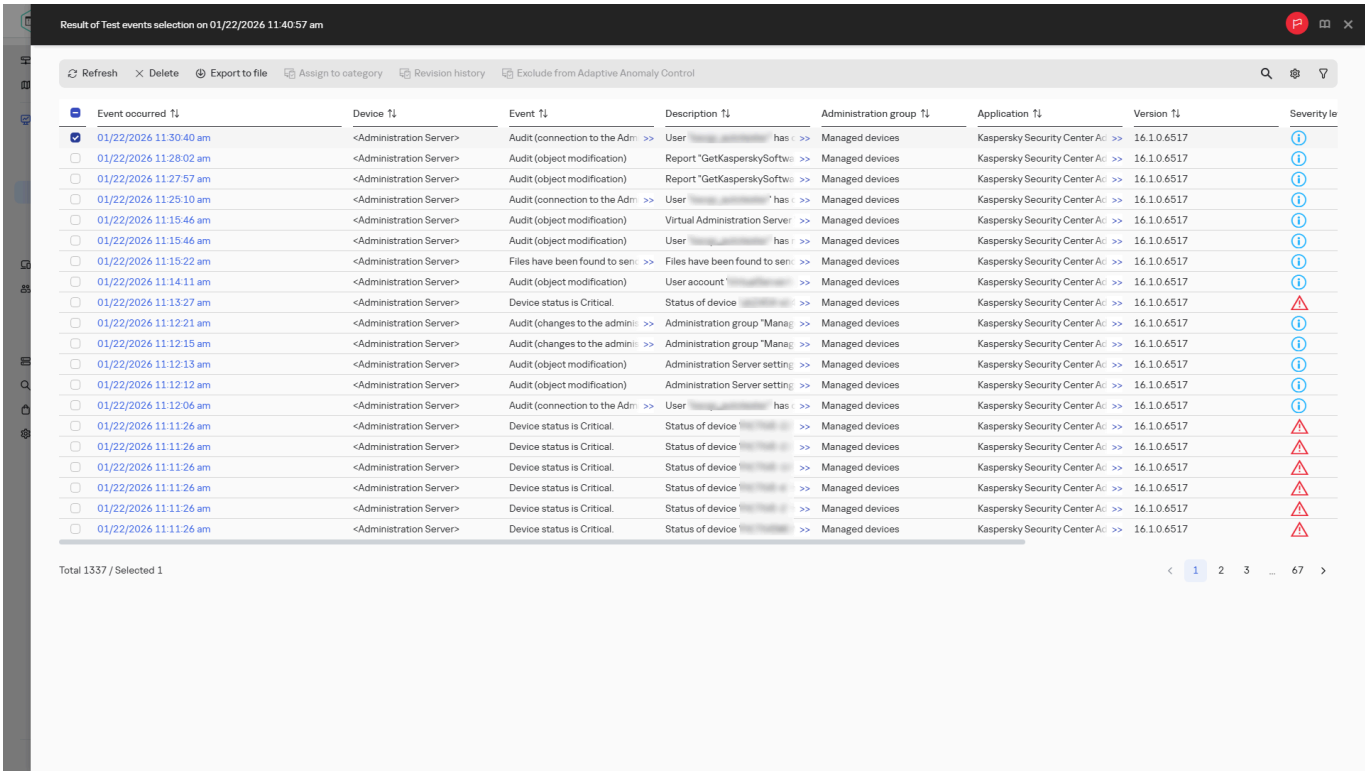
- 檢視關於所選事件的資訊
- 轉到發生事件的裝置
- 轉到包含發生事件的裝置的管理群組
- 對於工作相關事件，轉到工作內容

匯出事件到檔案

卡巴斯基安全管理中心 Linux 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。



事件分類結果

3. 點擊**匯出至檔案**按鈕。

所選事件被匯出到 TXT 檔案。

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**變更歷史**按鈕。

   物件修訂歷程被開啟。

刪除事件

要從事件分類中刪除事件：

1. 啟動事件分類。
2. 選擇事件：
   - 若要刪除一個或多個事件，請選取其旁邊的核取方塊。
   - 若要刪除目前頁面上的所有事件，請選取事件清單上方的核取方塊，然後按一下**全部選取目前頁面**選項。
   - 若要刪除選定區域中的所有事件，請選取事件清單上方的核取方塊，然後按一下**全選**選項。
3. 點擊**刪除**按鈕。
4. 在開啟的視窗中，點擊**刪除**按鈕。

若要從裝置事件清單中刪除事件：

1. 開啟裝置清單。
   - 對於受管理裝置：**資產管理→資產（裝置）**。
   - 對於未指派的裝置：**資產管理→未指派的裝置**。
2. 在裝置清單中，按一下所需裝置名稱的連結，然後轉至**事件**標籤。
3. 選擇事件：
   - 若要刪除一個或多個事件，請選取其旁邊的核取方塊。
   - 若要刪除目前頁面上的所有事件，請選取事件清單上方的核取方塊，然後按一下**全部選取目前頁面**選項。
   - 若要刪除選定區域中的所有事件，請選取事件清單上方的核取方塊，然後按一下**全選**選項。

4. 按一下**刪除**，然後確認操作。

5. 在開啟的視窗中，點擊**刪除**按鈕。

   所選事件被刪除且無法還原。

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 → 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。

設定事件儲存期限

卡巴斯基安全管理中心 Linux 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 **資產管理 → 政策**。

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，您也可以點擊管理伺服器名稱來設定事件的儲存期限。

3. 選擇**事件組態**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中（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中（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。

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 Linux）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. 在主選單中，按一下管理伺服器名稱。

   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：

- 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. 按一下**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. 按一下**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. 在主選單中，按一下管理伺服器名稱。
   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。

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，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。

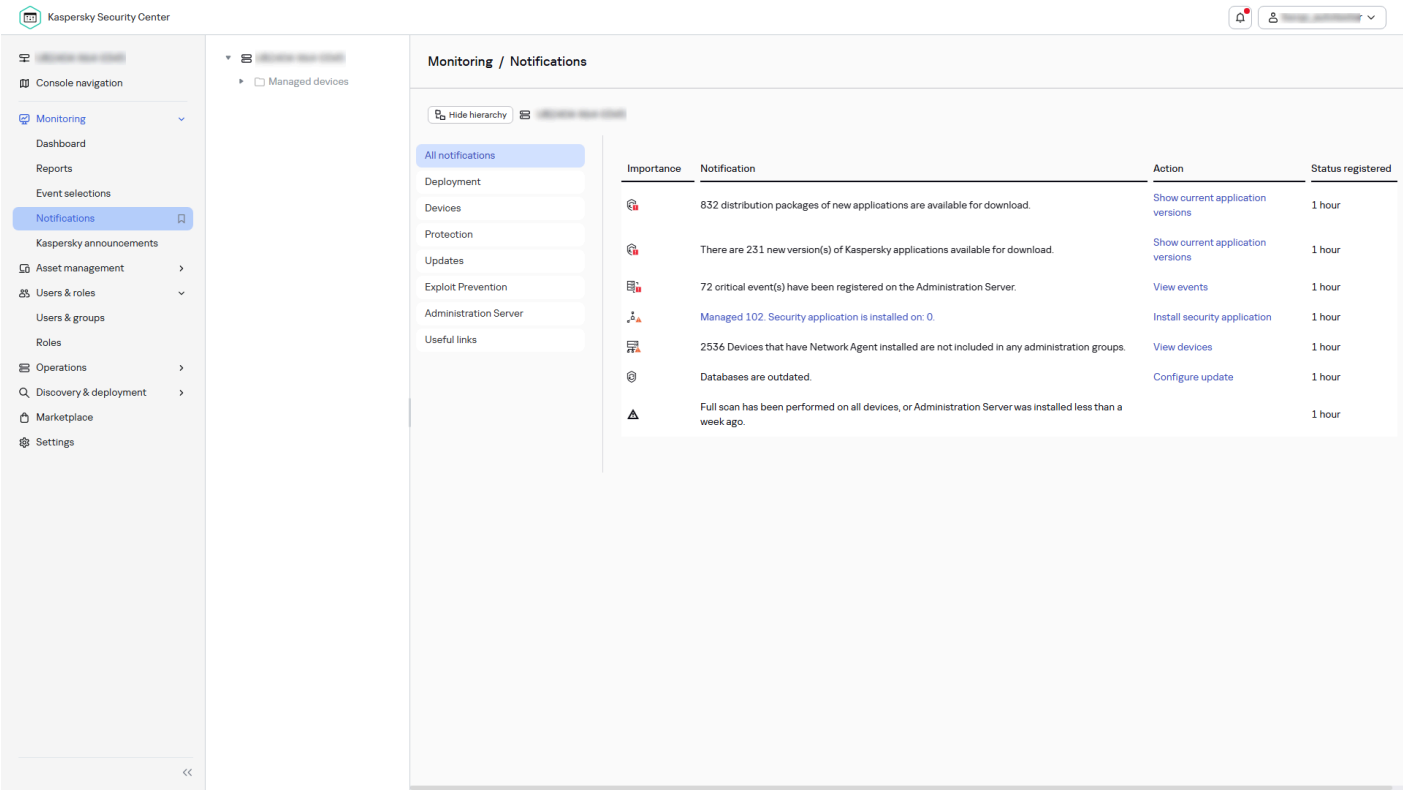
若管理伺服器刪除舊事件，則無法儲存新事件到資料庫。在此時間段內，拒絕事件的資訊被寫入作業係統記錄。新事件被列隊，然後在刪除操作後被儲存到資料庫。預設情況下，事件佇列的上限為 20,000 個事件。您可以透過編輯 KLEVP_MAX_POSTPONED_CNT 標誌的值來自訂佇列上限。

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。



通知清單

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 Linux 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：

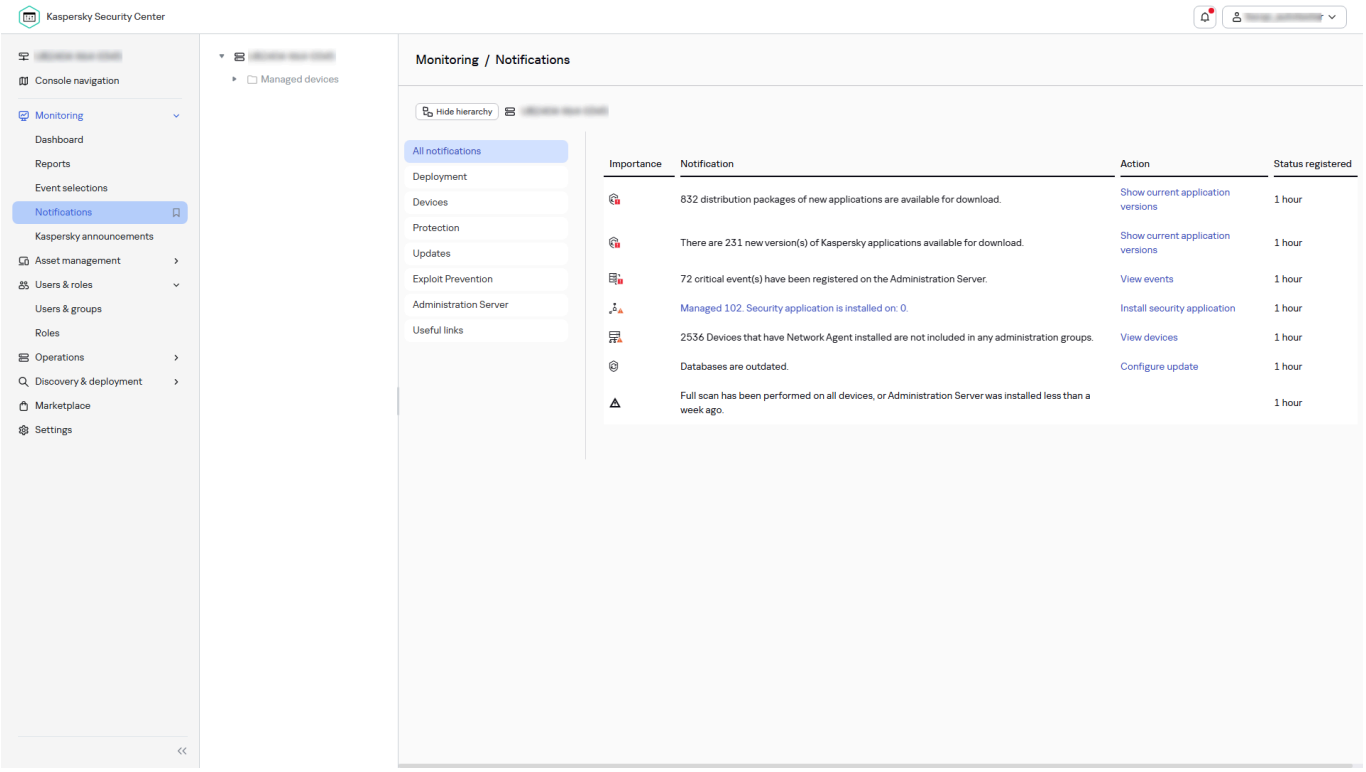
- 在**監控** 中 → **通知**區段。這裡，您可以檢視預定義類別的通知。
- 您可以開啟單獨的視窗。此種情況下，您可以標記通知為已檢視。
- 在 **監控** 上的**所選嚴重等級的通知**小工具中 → **控制板**區段。在部件中，您可以僅檢視處在*嚴重*和*警告*重要性等級的事件通知。

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** → **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。



通知清單

2. 在左側面板，選取類別之一：

- **佈署**
- **裝置**
- **防護**
- **更新**（這包括有關可下載的卡巴斯基應用程式的通知、有關已下載的病毒資料庫更新的通知，以及網路代理更新後需要重新啟動的裝置（如果有）的通知）
- **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)

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。

- **動作**。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。

- **狀態註冊時間**。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**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 Linux 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。在某些情況下，當為裝置指派狀態時，卡巴斯基安全管理中心 Linux 會考量裝置在網路中的能見度標記（請參閱下表）。例如，若受管理裝置因符合「*資料庫已過期*」條件而被指派為*緊急*狀態，之後又為該裝置設定了能見度標記，則裝置會被指派為*正常*狀態。若卡巴斯基安全管理中心 Linux 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。
即時保護等級不符合管理員設定的等級	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。

條件	條件敘述	可用值
自重新啟動以來需要的時間	裝置在網路上可見，但應用程式要求重新啟動的時間已超過指定時間間隔。	多於 0 分鐘。
重新啟動的原因	裝置在網路上可見，但應用程式因所選原因之一需要重新啟動裝置。	• 未知原因 • 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
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。	多於 0 天。
Windows Update 更新檢查已長時間未執行	裝置在網路中可見，但*尋找弱點和所需更新*工作未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。
偵測到未處理的安全問題	裝置上發現了一些未處理的安全問題。安全問題可以透過安裝在使用者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。 無論卡巴斯基安全管理中心 Linux 的設定為何，受管理裝置的狀態都可由受管理應用程式定義。當此狀態恢復為由卡巴斯基安全管理中心 Linux 定義的其中一種狀態後，管理伺服器會為受管理裝置指派受管理應用程式傳回且由管理伺服器指派的狀態中最緊急的狀態。由受管理應用程式定義的狀態，其描述同樣由受管理應用程式提供。您可以在受管理裝置清單的「**狀態描述**」欄位中檢視這些描述。	• 開關按鈕被關閉。 • 開關按鈕被開啟。

條件	條件敘述	可用值
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。
裝置已不受管理	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 Linux 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。當滿足指定條件時，用戶端裝置會被分配以下狀態之一：*緊急*或*警告*。當不滿足指定條件時，用戶端裝置會被分配*正常*狀態。

一個條件的不同值可對應於不同的狀態。例如，預設情況下，若**資料庫已過期**條件的值為**多於 3 天**，則用戶端裝置會被指派*警告*狀態；若值為**多於 7 天**，則會被指派*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 Linux，用於指派為*緊急*或*警告*狀態的**資料庫已過期**條件的值不會改變。

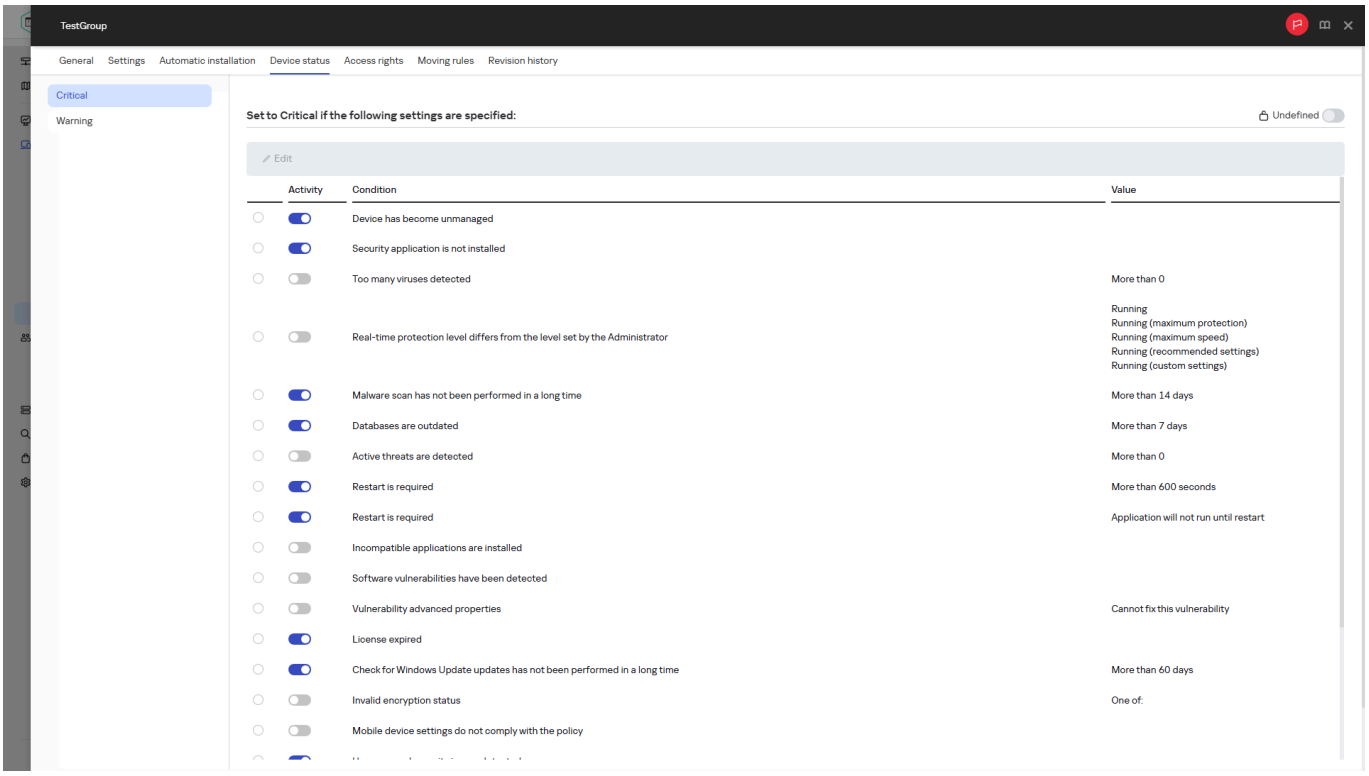
設定裝置狀態轉換

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 **資產管理** → **群組的階層**。
2. 透過以下方式之一，前往要變更切換裝置狀態的管理群組內容：
   - 點擊管理群組的名稱。
   - 點擊頁面頂部的**顯示階層**按鈕。在開啟的導覽窗格中，將滑鼠游標懸浮在所需群組的名稱之上，然後按一下設定圖示（ ⚙ ）。

   管理群組內容視窗將開啟。
3. 在屬性視窗中，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**如果指定了以下設定，則設定為「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 **資產管理** → **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**如果指定了以下設定則設定為「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 Linux 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 Linux 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 Linux 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 Linux 中的事件的通知傳送：

1. 在主選單中，按一下管理伺服器名稱。

   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 **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
     - 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 Linux 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 Linux 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。

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。

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**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**寄件者電子郵件信箱：如果未指定此設定，則將使用收件者信箱。 警告：我們不建議您使用虛構的電子郵件信箱**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。

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。

- **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
- 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 Linux 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 Linux 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**寄件者電子郵件信箱：如果未指定此設定，則將使用收件者信箱。 警告：我們不建議您使用虛構的電子郵件信箱**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 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**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。

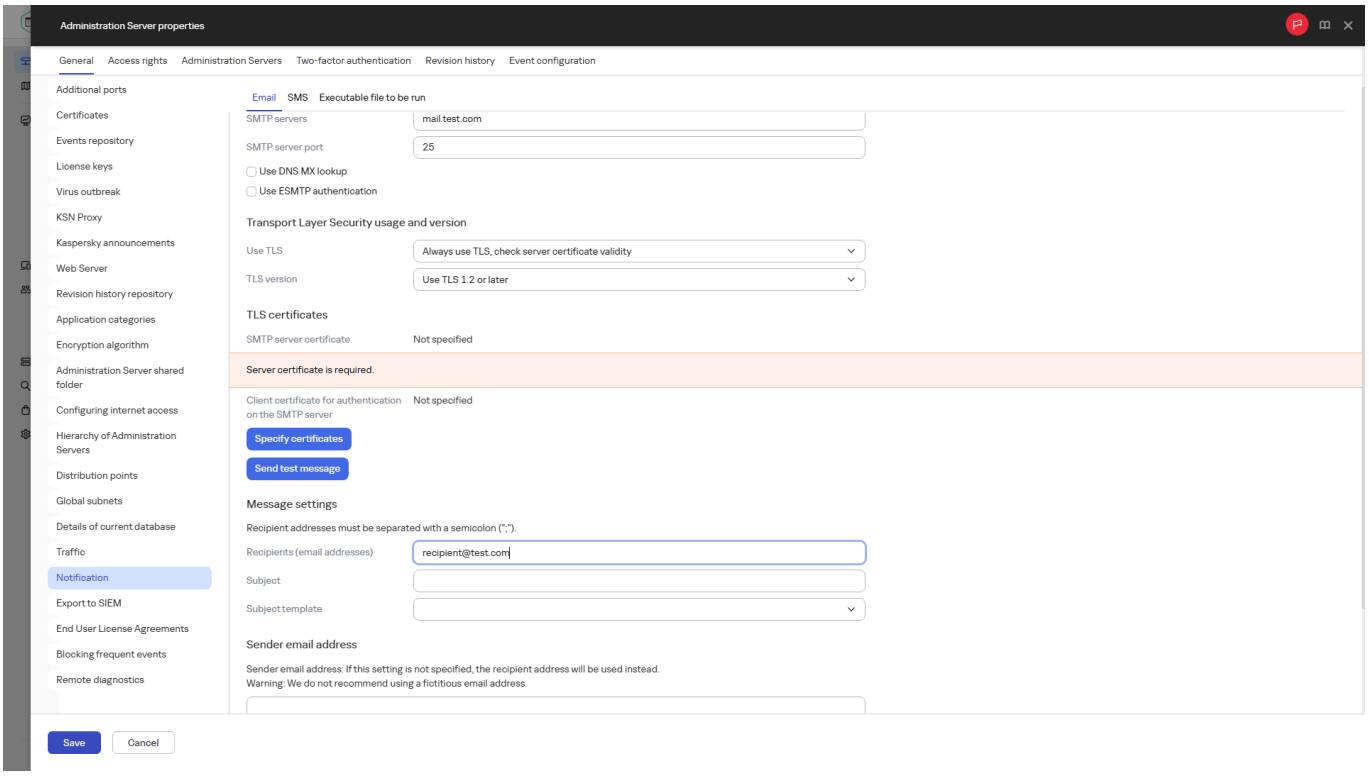
點擊**設定通知限制數**連結指定應用程式在指定時段內可以傳送的最大通知數量。

- **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。



選取通知方法

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 Linux 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**事件組態**區域覆寫特定事件的通知交付設定。

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 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 測試病毒的裝置。

   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。

要開啟測試病毒偵測記錄：

1. 在主功能表中，轉至 **監控 → 事件分類**。
2. 點擊**最近事件**分類名稱。

   在開啟的視窗中，將顯示有關測試病毒的通知。

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 Linux 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環境變數（請參見下表）。

用於敘述事件的環境變數

環境變數	環境變數說明
$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**
$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。

範例：
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 環境變數的另一個可執行檔（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 環境變數的 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 → 卡巴斯基公告**）透過提供與您的 卡巴斯基安全管理中心 Linux 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 Linux 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 Linux 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。預設情況下啟用與安全相關的公告。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 Linux 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 Linux 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。如果您不想接收卡巴斯基公告，則可以停用此功能。

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** → **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**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** → **卡巴斯基公告**）透過提供與您的 卡巴斯基安全管理中心 Linux 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. 在主選單中，按一下管理伺服器名稱。
   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**已停用相關安全公告**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. 在主選單中，按一下管理伺服器名稱。
   管理伺服器內容視窗將開啟。

2. 在**一般**頁籤上，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。

在 Kaspersky Extended Detection and Response Optimum 授權或 Kaspersky Next XDR Optimum 授權下啟動管理伺服器後，卡巴斯基安全管理中心網頁主控台會自動在主功能表的**監控**區域中顯示**警示**子區域。

*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，轉至**設定** → **介面選項**。

2. 啟用或停用**顯示 EDR 警示**選項。

3. 按一下**儲存**。

啟用**顯示 EDR 警示**選項後，主控台會在主功能表的**監控**區域中顯示**警示**子區域。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。

另外，您可以新增小工具以顯示有關警示的資訊。

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
- 物件已移動到隔離區
- 偵測到密碼防護的存檔
- 偵測到的病毒

用於回應警示的整合

如果您擁有 Kaspersky Next XDR Optimum 產品授權，則可以配置與以下解決方案的整合以回應威脅：

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal Sandbox
- Active Directory

如果您已在 Kaspersky Next XDR Optimum 產品授權下啟用管理伺服器，則可使用這些整合。
若要執行回應動作，您必須將 Kaspersky Next XDR Optimum 產品授權金鑰部署到受管理的應用程式。
透過試用產品授權使用 Kaspersky Next XDR Optimum 功能時，必須先新增從屬實體管理伺服器，並在試用產品授權下啟用此從屬管理伺服器，然後才能將產品授權金鑰部署到由此管理伺服器管理的裝置。

如果您使用的是 Kaspersky Next EDR Optimum 產品授權，則無需啟動在 Kaspersky Next XDR Optimum 產品授權下安裝在受管理裝置上的應用程式。您僅需為新裝置（如有）執行此操作。

因為 Kaspersky Next XDR Optimum 產品授權支援多租戶，您可以集中將產品授權金鑰發佈到受管理應用程式。不支援將產品授權自動分發到從屬和虛擬管理伺服器。

要配置整合，您必須具有**一般功能：應用程式整合**功能區域的**讀取**和**寫入**權限。

配置與 Active Directory 的整合以執行回應操作

與 Active Directory 整合可讓您對受到警示影響或涉及警示的 Active Directory 使用者執行回應操作。

若要設定與 Active Directory 的整合以回應警示，您必須使用卡巴斯基安全管理中心 Linux 管理伺服器 15.4 或更高版本。

與 Active Directory 整合以回應警示，以及在配置網域控制器輪詢時指定的 Active Directory 網域控制器掃描設定（網域控制器的位址和使用者憑據）是兩種不同的設定。由於您需要確保要對其執行回應操作的使用者擁有 Active Directory 帳戶，因此您必須配置這兩個整合：用於掃描和用於回應。順序不重要。

整合設定不會被繼承，僅被套用於您在其上配置這些設定的管理伺服器（實體或虛擬）。

若要配置與 Active Directory 的整合以回應警示：

1. 在主功能表中，按一下管理伺服器名稱。

   管理伺服器內容視窗會開啟，含有所選的**一般**頁籤。

2. 執行以下其中一項操作：

   - 選擇**發佈點**部分，按一下所需發佈點的名稱，然後在開啟的內容視窗中選擇**Active Directory**部分。
   - 選取「**Active Directory 回應**」區域。

3. 在右側窗格中，啟用**Active Directory 整合**切換開關。

   稍後，如果想關閉整合，您只能透過停用**Active Directory 整合**切換開關對所有連線執行此操作。您無法關閉單獨連線的整合。相反，您可以刪除該連線。

   > 當您啟用或停用「**Active Directory 整合**」切換開關時，此設定將同時套用於「**Active Directory 回應**」與「**發佈點**」區域。

4. 點擊「**新增**」按鈕，以建立與 Active Directory 網域控制器的連線。

5. 在開啟的視窗中，指定連線的以下參數：

   - **網域控制器位址**

     電腦名稱，例如：`server.mycompany.com`。

     您可以指定多個位址。您指定位址的所有網域控制器必須屬於同一個網域。

   - **Active Directory 網域名稱**

     DNS 完整網域名稱，例如：`mycompany.com`

     此外，您也可以指定 SAM 或 NetBIOS 名稱，例如： `mycompany`

     使用小寫字母。如果為管理伺服器或發佈點建立多個連線，請為每個連線指定不同的名稱。

     > 若要執行回應操作，您在此欄位中指定的 Active Directory 網域必須與警示中指定的 Active Directory 網域名稱相符。

   - **登入**

     具有管理員權限的 Active Directory 帳戶的登入名，回應操作在該帳戶下執行。

   - **密碼**

     具有管理員權限的 Active Directory 帳戶的密碼，回應操作在該帳戶下執行。

6. 若要檢查連線狀態，請點擊「**偵測連線**」按鈕。

若連線成功建立，則會顯示「**已連線**」狀態。否則，狀態將顯示為「**失敗**」，且會顯示無法連線至網域控制器的錯誤訊息。

> 您必須考慮連線到 Active Directory 的方式：**從 Linux 裝置還是從 Windows 裝置**。

從 Linux 裝置連線

預設情況下，從 Linux 裝置連線並驗證網域控制器時，邏輯如下：

1. 管理伺服器或發佈點嘗試透過 LDAPS 連線到網域控制器。
   需要執行 LDAP 伺服器憑證強驗證。
2. 將網域控制器憑證的公共部分放入系統憑證儲存區以驗證憑證。
   會使用依作業系統而定的系統憑證授權單位 (CA) 路徑來存取憑證鏈。
   例如：
   - /etc/ssl/certs/ca-certificates.crt — 基於 Debian 的作業系統 (Debian、Ubuntu、Astra) 的路徑。
   - /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem — CentOS 或 Red Hat 的路徑。
3. 如果 LDAPS 連線失敗，則會發生錯誤，不會使用其他連線協定。

   > 如果出現 LDAPS 問題，您可以聯絡卡巴斯基技術支援。

如果您不想將憑證安裝到系統憑證儲存區中，可以使用 KLNAG_LDAP_SSL_CACERT 標誌來設定網域控制器憑證的路徑。為此，請執行以下命令：

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "</path/to/domain-controller/cert>"
```

其中`</path/to/domain-controller/cert>`是網域控制器憑證公共部分的路徑。

例如，如果路徑是`"/var/opt/kaspersky/ldap_cert.crt"`，則命令為`klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "/var/opt/kaspersky/ldap_cert.crt"`

從 Windows 裝置連線

從 Windows 裝置連線並驗證網域控制器時，連線設定由網域定義。

您只需確保：

- LDAPS 已啟用且連接埠 636 在裝置上可用。
- 您允許透過防火牆或代理伺服器連線到網域控制器。

7. 按一下**儲存**按鈕。

視窗關閉，連線顯示在連線表中。

在連線表中，您可以進行以下操作：

- 編輯連接參數。

  為此，請按一下所需連接的**網域控制器位址**參數的連結。在開啟的視窗中，變更所需設定，然後點擊**儲存**按鈕。

  您只能編輯**登入** 和**密碼** 參數。

- 刪除連接。

  為此，請選取要刪除的連線旁邊的核取方塊，按一下工具列中的**移除**按鈕，然後確認刪除連線。

配置與 Kaspersky Automated Security Awareness Platform 的整合

與Kaspersky Automated Security Awareness Platform整合（以下也稱為 KASAP）可讓您指派 KASAP 學習課程給與警示相關的使用者。

整合設定不會被繼承，僅被套用於您在其上配置這些設定的管理伺服器（實體或虛擬）。

> 在卡巴斯基安全管理中心網頁主控台中配置整合之前，您必須在 KASAP 中建立授權權杖並取得 API 請求的 URL。

要配置與 Kaspersky Automated Security Awareness Platform 的整合：

1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗會開啟，並含有所選的**一般**頁籤。

2. 選取「**KASAP**」區域。

3. 在右側窗格中，啟用**KASAP 整合**切換開關。

4. 指定用於連線 KASAP 的設定：

   - **API 權杖**— 您建立的用於存取 KASAP Open API 的權杖。
   - **URL** — 建立 API 令牌時所取得的 API 請求的 URL。
   - **使用代理伺服器** — 可讓您在連線到 KASAP 時啟用代理伺服器的切換開關。

     依預設已停用該切換開關。

5. 如有必要，請按一下**偵測連線**按鈕以驗證您指定的設定。

   連線狀態將顯示。

6. 按一下**儲存**按鈕。

已配置與 Kaspersky Automated Security Awareness Platform 的整合。

儲存 KASAP 整合設定後，您可以點擊**檢視群組**按鈕檢視 KASAP 學習群組清單。

如有必要，當顯示群組清單時，您可以透過點擊**重新整理群組**按鈕來更新它。

開啟清單後，您將無法隱藏它。如果停用**KASAP 整合**切換開關，則不會顯示 KASAP 群組清單。

配置與 Kaspersky Threat Intelligence Portal Sandbox 的整合

與Kaspersky Threat Intelligence Portal整合（以下也稱為 Kaspersky TIP）可讓您使用**Kaspersky Sandbox隔離**隔離區的檔案。

整合設定不會被繼承，僅被套用於您在其上配置這些設定的管理伺服器（實體或虛擬）。

在配置整合之前，您必須取得 Kaspersky TIP 上 API 請求的授權權杖。

要配置與 Kaspersky TIP Sandbox 的整合：

1. 在主選單中，按一下管理伺服器名稱。
   管理伺服器內容視窗會開啟，並含有所選的**一般**頁籤。
2. 選取「**Kaspersky TIP**」。
3. 在右側窗格中，啟用**整合**切換開關。
   與 Kaspersky TIP 的連線設定將顯示。

   如果在配置並儲存整合設定後停用**整合** 撥動開關，設定不會被刪除，但您將無法執行回應操作。

4. 按一下**新增權杖**按鈕，在開啟的視窗中，指定您先前在 Kaspersky TIP 上取得的權杖，然後按一下**新增** 按鈕。
   視窗關閉，API 權杖已新增。
5. 如果您想在連接到 Kaspersky TIP 時使用代理伺服器，請啟用**使用代理伺服器**切換開關。
   依預設已停用該切換開關。
6. 點擊**儲存**按鈕。

與 Kaspersky TIP Sandbox 的整合得到配置。

現在，您可以將檔案從 **隔離** 部分傳送到 Kaspersky TIP 和 Kaspersky Sandbox 進行威脅分析。檔案的最大大小是 100 MB

由於 Kaspersky Next XDR Optimum 產品授權支援多租戶，因此放置在**隔離區隔離** 由租戶劃分。如果管理員使用專用的 TIP 帳戶和與每個租用戶相關的 API 權杖，則此租用戶層級的分離也適用於將檔案傳送至 Kaspersky Sandbox 並檢視結果時。但是，由於隔離清單不會根據伺服器層次結構顯示物件，因此無法集中管理所有租用戶的**隔離**部分。

按屬性分組警示

警示聚合有助於識別可能與相同事件相關的警示，從而簡化調查過程。

若要啟用警示聚合功能，您必須執行下列操作：

- 在主選單中啟用**警示**子部分。
- 在 Kaspersky Next XDR Optimum 產品授權下啟動管理伺服器，然後將 Kaspersky Next XDR Optimum 產品授權金鑰部署到您的受管理應用程式。

  在測試模式下透過試用產品授權使用 Kaspersky Next XDR Optimum 時，必須先新增從屬實體管理伺服器，然後透過該產品授權啟用此伺服器。

如果您使用的是 Kaspersky Next EDR Optimum 產品授權，則無需啟動在 Kaspersky Next XDR Optimum 產品授權下安裝在受管理裝置上的應用程式。您僅需為新裝置（如有）執行此操作。
因為 Kaspersky Next XDR Optimum 產品授權支援多組織用戶，您可以集中將產品授權金鑰發佈到受管理應用程式。不支援將產品授權自動分發到從屬和虛擬管理伺服器。

您可以按裝置名稱、帳戶或雜湊名稱（SHA256）聚合警示。

> 僅當屬性不為空時，才會根據屬性聚合警示。

如果警示至少共用一個屬性，並且在群組中任何其他警示的 24 小時內發生，則這些警示會聚合在一起。

要按屬性聚合警示：

1. 在主功能表中，轉至**監控** → **警示**。
2. 執行以下其中一項操作：
   - 啟用 **警示聚合** 切換開關，然後選擇用來聚合警示的一個或多個屬性：
     - **裝置名稱**
     - **帳戶**
     - **檔案雜湊值**雜湊名稱（SHA256）

     預設選擇**裝置名稱** 和 **帳戶**屬性。
   - 按一下設定圖示 (⚙)。在開啟的**表格設定**窗格中，前往 **分組**頁簽。選擇 **聚合群組 ID** 並點擊 **套用**。

啟用聚合後，警示將按**事件時間**從最新到最舊進行排序。不支援其他排序選項。選擇不同的分組選項將停用聚合。

該表顯示按屬性匯總的警示。未匯總的警示顯示在表格的底部。

聚合後，每個警示僅被指派給一個群組。

Cloud Discovery

卡巴斯基安全管理中心 Linux 可讓您監控執行 Windows 的受管理裝置上使用雲端服務的情況，甚至封鎖您認為不需要的雲端服務存取權限。Cloud Discovery 會追蹤使用者嘗試透過瀏覽器和桌面應用程式對這些服務進行的存取活動。它還會追蹤使用者嘗試透過未加密連線（例如，使用 HTTP 通訊協定）對雲端服務進行的存取活動。此功能可協助您偵測並制止"影子 IT"使用雲端服務。

只有當您在Kaspersky Next EDR Optimum 或 Kaspersky Next XDR Expert 產品授權下啟動卡巴斯基安全管理中心 Linux 時，才可使用封鎖功能。

僅當您使用 Kaspersky Endpoint Security 11.2 for Windows 或以上版本時，封鎖功能才可使用。該安全應用程式的更早版本僅能讓您監控雲端服務的使用情況。

您可以啟用 Cloud Discovery 功能，然後選取要啟用該功能的安全政策或設定檔。您也可以分別在每個安全政策或設定檔中啟用或停用該功能。對於您不想讓使用者存取的雲端服務，您可以封鎖對這些雲端服務進行的存取活動。

為了能夠封鎖對不需要的雲端服務進行的存取活動，請確保滿足以下先決條件：

- 使用 Kaspersky Endpoint Security 11.2 for Windows 或更高版本。該安全應用程式的更早版本僅能讓您監控雲端服務的使用情況。
- 您已購買 Kaspersky NEXT 產品授權，其層級允許您封鎖對不需要的雲端服務進行的存取活動。詳情請參閱 Kaspersky Next 說明。

Cloud Discovery 小工具和 Cloud Discovery 報告會顯示與嘗試存取雲端服務時成功與遭封鎖的活動有關的資訊。該小工具還會顯示每項雲端服務的風險等級。卡巴斯基安全管理中心 Linux 會從所有受安全政策或設定檔（啟用了該功能）保護的受管理裝置，取得雲端服務使用情況相關資訊。

使用小工具啟用 Cloud Discovery

Cloud Discovery 功能可讓您向所有受安全政策（啟用了該功能）保護的受管理裝置，取得雲端服務使用情況資訊。僅能對 Kaspersky Endpoint Security for Windows 政策啟用或停用 Cloud Discovery。

有兩種方式啟用 Cloud Discovery 功能：

- 透過使用 Cloud Discovery 小工具。
- 在 Kaspersky Endpoint Security for Windows 政策內容中完成。

  有關如何在 Kaspersky Endpoint Security for Windows 政策內容中啟用 Cloud Discovery 功能的詳細信息，請參閱 Kaspersky Endpoint Security for Windows 幫助的 Cloud Discovery 部分。

請注意，只能在 Kaspersky Endpoint Security for Windows 政策參數中停用 Cloud Discovery 功能。

要能夠啟用 Cloud Discovery，您必須在**一般功能：基本功能**功能區域中具有**寫入**權限。

要使用 Cloud Discovery 小工具啟用 Cloud Discovery 功能：

1. 前往卡巴斯基安全管理中心 Linux。
2. 在主功能表中，轉至 **監控** → **控制板**。
3. 在 **Cloud Discovery** 小工具上，點擊**啟用**按鈕。

   如果您安裝了 Kaspersky Endpoint Security for Windows 版本 12.4，請在 Kaspersky Endpoint Security for Windows 政策屬性中啟用 Cloud Discovery 功能。如需取得詳細資訊，請參閱 Kaspersky Endpoint Security for Windows 說明的 Cloud Discovery 區域。

   如果您擁有早於 12.4 版本的 Kaspersky Endpoint Security for Windows，請將 Kaspersky Endpoint Security for Windows 外掛程式更新至版本 12.5。

4. 在開啟的**啟用 Cloud Discovery** 視窗中，選取要啟用該功能的安全政策，然後點擊**啟用**按鈕。

   以下政策設定將自動啟用：**將指令碼注入 Web 流量以與網頁互動**、 **Web 工作階段監控**和**加密連線掃描**。

Cloud Discovery 功能已啟用，且小工具已新增至儀表板中。

在儀表板中新增 Cloud Discovery 小工具

您可以在儀表板中新增 **Cloud Discovery** 小工具，以監控受管理裝置上使用雲端服務的情況。

若要在儀表板中新增 Cloud Discovery 小工具，您必須在**一般功能：基本功能**功能區域中具有**寫入**權限。

若要在儀表板中新增 Cloud Discovery 小工具：

1. 前往卡巴斯基安全管理中心 Linux。
2. 在主功能表中，轉至 **監控** → **控制板**。
3. 點擊**新增或還原小部件**按鈕。
4. 在可用小工具清單中，點擊**其他**類別旁邊的箭頭圖示 (>)。

5. 選取 **Cloud Discovery** 小工具，然後點擊**新增**按鈕。

   如果 Cloud Discovery 功能已停用，請依照使用小工具啟用 Cloud Discovery 部分中的說明進行操作。

所選的小工具即會新增到儀表板的尾端。

檢視雲端服務使用情況資訊

您可以檢視 **Cloud Discovery** 小工具，其中會顯示與嘗試對雲端服務進行的存取活動有關的資訊。該小工具還會顯示每項雲端服務的風險等級。卡巴斯基安全管理中心 Linux 會從所有受安全設定檔（啟用了該功能）保護的受管理裝置，取得雲端服務使用情況資訊。

在檢視之前，請確定：

- Cloud Discovery 小工具已新增至儀表板中。
- Cloud Discovery 功能已啟用。
- 您在**一般功能：基本功能**功能區域中具有**讀取**權限。

若要檢視 Cloud Discovery 小工具：

1. 前往卡巴斯基安全管理中心 Linux。
2. 在主功能表中，轉至 **監控** → **控制板**。

   Cloud Discovery 小工具會顯示在儀表板中。
3. 在 **Cloud Discovery** 小工具的左側，選取雲端服務類別。

   小工具右側的表格會顯示所選類別中，最多五項最常為使用者所嘗試存取的服務。所謂的嘗試，同時包括了成功和遭封鎖的嘗試。
4. 在小工具的右側，選取特定服務。

   下方的表格會顯示最多十台最常嘗試存取該服務的裝置。在此表中，您可以產生兩種類型的報告：成功存取嘗試的報告和被阻止存取嘗試的報告。

   此外，在此表中您可以阻止特定裝置對雲端服務的存取。

小工具即會顯示所請求的資訊。

在顯示的小工具中，您可以執行以下操作：

- 前往**監控** → **報告**區段以檢視 Cloud Discovery 報告。
- 封鎖或允許存取所選的雲端服務。

只有當您在Kaspersky Next EDR Optimum 或 Kaspersky Next XDR Expert 產品授權下啟動卡巴斯基安全管理中心 Linux 時，才可使用封鎖功能。

僅當您使用 Kaspersky Endpoint Security 11.2 for Windows 或以上版本時，封鎖功能才可使用。該安全應用程式的更早版本僅能讓您監控雲端服務的使用情況。

雲端服務的風險等級

對於每項雲端服務，Cloud Discovery 會向您顯示風險等級。風險等級可幫助您判斷哪些服務不符合組織安全要求。例如，您可以在決定是否封鎖對特定服務的存取活動時，將風險等級納入考慮。

風險等級是一項估計的指數，並未指出任何與雲端服務品質或服務製造商有關的資訊。風險等級純粹為來自 Kaspersky 專家的建議。

在 Cloud Discovery 小工具以及列出所有受監控雲端服務的清單中，會顯示雲端服務的風險等級。

封鎖對不需要的雲端服務進行的存取活動

對於您不想讓使用者存取的雲端服務，您可以封鎖對這些雲端服務進行的存取活動。您也可以允許對先前封鎖的雲端服務進行存取。

您在決定是否封鎖對特定服務進行的存取活動時，除了其他眾多考量，還可以將風險等級納入考慮。

您可以在安全政策或設定檔中封鎖或允許對雲端服務進行的存取活動。

有兩種方法封鎖對不需要的雲端服務進行的存取活動：

- 透過使用 Cloud Discovery 小工具啟用。

  在這種情況下，您可以逐一封鎖對服務的存取。

- 在 Kaspersky Endpoint Security for Windows 政策內容中完成。

  在這種情況下，您可以逐一封鎖對服務的存取，或一次性封鎖整個類別。

  有關如何在 Kaspersky Endpoint Security for Windows 政策內容中啟用 Cloud Discovery 功能的詳細資訊，請參閱 Kaspersky Endpoint Security for Windows 幫助的 Cloud Discovery 部分。

要封鎖或允許透過小工具對雲端服務的存取：

1. 開啟 Cloud Discovery 小工具，然後選取所需的雲端服務。
2. 在**使用服務的前 10 台裝置**中，找到要用於封鎖或允許該服務的安全政策或設定檔。
3. 在所需行的**政策或設定檔中的存取狀態**欄位中，執行以下任一操作：
   - 若要封鎖服務，請在下拉清單中選取**已封鎖**。
   - 若要允許服務，請在下拉清單中選取**允許**。
4. 點擊**儲存**按鈕。

   安全政策或設定檔即會封鎖或允許對所選服務進行的存取活動。

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 Linux 可讓您透過下列其中一種方法設定將事件匯出到 SIEM 系統：匯出到任何使用 Syslog 格式的 SIEM 系統、匯出到使用 LEEF 和 CEF 格式的 Kaspersky SIEM、QRadar、Splunk、ArcSight SIEM 系統，或直接從卡巴斯基安全管理中心資料庫將事件匯出到 SIEM 系統。完成此情境後，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 Linux 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情境的步驟。

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 Linux 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**

  標記要匯出到 SIEM 系統的事件。首先，標記發生在所有受管理的卡巴斯基應用程式中的一般事件。然後，您可以標記特定受管理的卡巴斯基應用程式的事件。

- **配置匯出事件到 SIEM 系統**

  您可以使用下列方法之一匯出事件：

  - 使用 TCP、UDP 或 TLS over TCP 通訊協定
  - 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，您可以檢視匯出結果。

在您開始之前

當設定在卡巴斯基安全管理中心 Linux 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 Linux。

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 Linux 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 Linux 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 Linux 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 Linux 設定中和您 SIEM 系統的接收設定中指定該值。

關於事件匯出

卡巴斯基安全管理中心 Linux 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 Linux 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 Linux 中的事件傳輸，然後設定 SIEM 系統對事件的接收，或者相反。

從Kaspersky Security Center Linux傳送事件的方法

有三種方法從Kaspersky Security Center for Linux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 協定將事件傳送到 Kaspersky SIEM、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 Kaspersky Security Center for Linux 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 Kaspersky Security Center for Linux 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 Kaspersky Security Center for Linux 分發套件中。

  不同於 Syslog 協定，CEF 和 LEEF 協定不通用。CEF 和 LEEF 是為相應的 SIEM 系統（Kaspersky SIEM、QRadar、Splunk 和 ArcSight）所設計。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 Kaspersky Security Center for Linux 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 Linux 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 Linux 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 Linux 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 Linux 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 Linux 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**

  透過 TCP 的訊息傳輸通訊協定，UDP 或 TCP。該協定必須與您在卡巴斯基安全管理中心 Linux 中指定的協定相同。

- **連接埠**

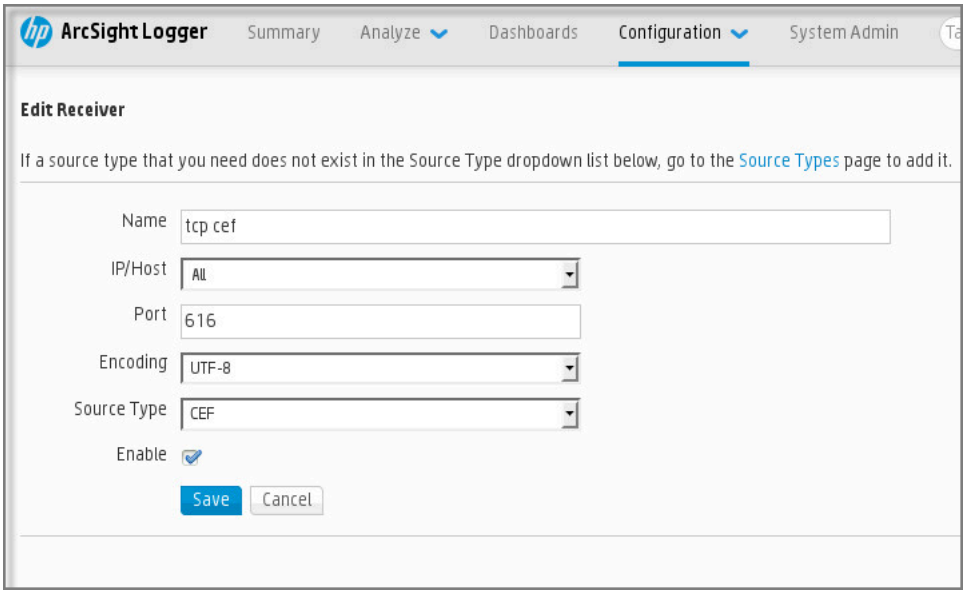
  指定連線到卡巴斯基安全管理中心 Linux 的連接埠號。此連接埠必須與您在配置 SIEM 系統期間在卡巴斯基安全管理中心 Linux 中指定的連接埠相同。

- **資料格式**

  指定Syslog、CEF或LEEF格式。

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 Linux 接收的事件，以便它們可以被儲存在 SIEM 系統資料庫。

使用 CEF 和 LEEF 格式匯出事件

您可使用 CEF 和 LEEF 格式，將一般事件、政策變更事件以及由 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（Kaspersky SIEM、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 Linux 事件解譯為 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
Kaspersky SIEM	CEF
ArcSight	CEF
Splunk	CEF
QRadar	LEEF

- 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Kaspersky Security Center for Linux將一般事件傳送到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（Kaspersky SIEM、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 Linux 事件解譯為 CEF 和 LEEF 格式的事件。該檔案包含在Kaspersky Security Center for Linux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檔案包含以下區段：

- `<product name="SP_QRADAR" vendor="IBM">`

  此區段包含用於產生LEEF格式事件的規則，這些事件可以匯出到QRadar SIEM系統。

- `<product name="SP_ARCSIGHT" vendor="HP">`。

  此區段包含用於產生CEF格式事件的規則，這些事件可以匯出到ArcSight或Splunk SIEM系統。

- `<product name="Kaspersky SIEM" vendor="Kaspersky">`。

  此區段包含用於產生CEF格式事件的規則，這些事件可以匯出到KUMA。

每個部分都有`<common>`子部分，Kaspersky Security Center for Linux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`<event>`子區段新增至`<product name="SP_QRADAR" vendor="IBM">`、`<product name="SP_QRADAR" vendor="IBM">`或`<product name="Kaspersky SIEM" vendor="Kaspersky">`區段，然後視需要指定其他事件屬性。

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 Linux 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"> <!-- Generation rule for the GNRL_EV_VIRUS_FOUND event with additional
attributes -->
            <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 Linux 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>
    <product name="Kaspersky SIEM" vendor="Kaspersky">
        <common> <!-- Common Kaspersky Security Center Linux 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>
```

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。

對於政策變更事件，您只能啟用或停用將所有此類事件匯出到 SIEM 系統。

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 **資產管理** → **政策**。

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**事件組態**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 **資產管理 → 資產（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**事件組態**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. 在主功能表中，執行以下操作之一：
   - 按一下管理伺服器名稱。
   - 轉到 **資產管理** → **政策**，然後單擊某個政策的連接。
2. 在開啟的視窗中，請前往**事件組態**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。

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 Linux 匯出事件到外部系統。

在卡巴斯基安全管理中心 Linux 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 Linux 被設定，以便能傳送事件到 SIEM 系統。卡巴斯基安全管理中心 Linux 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 Linux 以將事件匯出到 SIEM 系統

要將事件匯出到 SIEM 系統，您必須在 卡巴斯基安全管理中心 Linux 中配置匯出過程。

在將事件傳送到 SIEM 系統（Kaspersky SIEM、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譯為 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. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在**一般**頁簽，選擇**匯出至 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 Linux 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 Linux 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 Linux。卡巴斯基安全管理中心 Linux 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 Linux 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**欄位中輸入它，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 Linux。因此，您將使用 卡巴斯基安全管理中心 Linux 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。

     - **新增主旨名稱/主旨別名**

       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 Linux 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 **新增主旨名稱/主旨別名**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比對，卡巴斯基安全管理中心 Linux 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 Linux 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。

- **產生金鑰**。您可以在 卡巴斯基安全管理中心 Linux 中產生自簽章憑證。結果，卡巴斯基安全管理中心 Linux 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 Kaspersky SIEM、IBM QRadar SIEM、ArcSight、Splunk 或系統日誌格式。

  如果選擇系統日誌資料格式，則必須指定**最大訊息大小（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. 如果需要，您可以從管理伺服器資料庫中匯出封存事件，並設定開始匯出封存事件的開始日期：

   a. 點擊**設定匯出開始日期**連接。

   b. 在開啟的部分中，在**啟動匯出日期自**欄位中指定開始日期。

   c. 點擊**確定**按鈕。

6. 啟用**匯出事件至 SIEM**選項。

7. 若要將政策變更事件傳送至SIEM，請啟用**將政策變更的擴充事件匯出至 SIEM**選項。針對每項已變更的政策設定，都會向SIEM傳送一個單獨事件。

8. 若要檢查 SIEM 系統連線是否已配置，請點擊**偵測連線**按鈕。

   與 SIEM 系統伺服器的連線已建立，測試事件已傳送。連線狀態即會顯示。

9. 點擊**儲存**按鈕。

匯出到 SIEM 系統已配置。從現在開始，如果您已在 SIEM 系統中配置事件接收，管理伺服器會將標記的事件或政策變更事件匯出到 SIEM 系統。如果設定匯出的開始日期，管理伺服器也會匯出儲存在管理伺服器資料庫中從指定日期開始的標記事件。

監控政策與政策設定檔變更

政策設定變更時，會產生政策變更事件，您可以接著匯出至 SIEM 系統，以監控政策變更並產生警示。政策變更事件只能透過 SIEM 系統存取。

政策變更事件產生後不會儲存在管理伺服器資料庫中，且無法在卡巴斯基安全管理中心網頁主控台的 **監控 → 事件分類** 區段中檢視。您也無法在 **事件組態** 索引標籤上指定這些事件的通知設定和儲存設定。

建立政策時，會針對每個政策設定產生政策變更事件。變更政策時，會針對政策中每個已變更的設定產生政策變更事件。刪除政策時，會產生一個事件。例如，建立卡巴斯基安全管理中心政策會產生約 1000 個事件，而建立 Kaspersky Endpoint Security 政策會產生超過 7000 個事件。

產生政策變更事件的條件

在下列情況下會建立政策變更事件：

- 以下應用程式的政策遭到建立、修改或刪除：
  - 卡巴斯基安全管理中心網路代理
  - 卡巴斯基安全管理中心管理伺服器
  - Kaspersky Endpoint Security for Windows 14.1
  - Kaspersky Endpoint Security for Linux 12.5
  - Kaspersky Endpoint Security for Linux 12.4
  - Kaspersky Endpoint Security for Mac 12.2.1
- 管理伺服器內容中的 **將政策變更的擴充事件匯出至 SIEM** 選項已啟用。
- 透過卡巴斯基安全管理中心網頁主控台介面手動修改政策。

在下列情況下不會建立政策變更事件：

- 修改一般政策設定。
- 修改從父政策繼承的政策設定。
- 透過 卡巴斯基安全管理中心 OpenAPI 修改政策設定。
- 直接在應用程式中修改卡巴斯基應用程式設定。

政策變更事件欄位

下表顯示一組政策變更事件欄位。這些欄位的表示方式取決於輸出事件格式（例如 Syslog、CEF 或 LEEF）。如需確切的欄位名稱和事件範本，請參閱 siem_conversion_rules.xml 檔案。事件參數僅提供英文版。

事件欄位	資料類型	描述
`eventType`	字串	事件類型。可針對特定事件類型建立關聯規則。 可能值："Policy created", "Policy modified", "Policy deleted"。
`srvName`	字串	管理伺服器名稱。

eventTime	日期時間	事件的日期與時間 (UTC)。
eventGroupID	整數	修改事件群組的 ID。
objectID	整數	物件的內部 ID。
objectName	字串	政策顯示名稱。
objectGroup	字串	包含該政策的管理群組完整路徑和名稱。
user	字串	進行修改的使用者名稱。
operation	字串	參數修改類型。 可能值："Added"、"Removed"、"Changed"。
path	字串	參數路徑。包含末端參數父節點的路徑。路徑是根據政策區段和子區段的名稱建立。此路徑結構與網路代理政策設定、一般政策設定及比較政策修訂中所述的路徑結構相同。
parameter	字串	末端參數名稱。
oldValue	字串	末端參數的舊值。
newValue	字串	末端參數的新值。

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 Linux 資料庫接收事件，而不必使用 卡巴斯基安全管理中心 Linux 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 Linux 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 Linux 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 Linux 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

本文旨在說明如何使用 klsql2 公用程式，以及如何使用該公用程式執行 SQL 查詢。使用安裝的 卡巴斯基安全管理中心 Linux 版本中包含的 klsql2 公用程式版本。

要使用 klsql2 公用程式：

1. 轉至安裝管理伺服器的目錄。預設安裝路徑為/opt/kaspersky/ksc64/sbin。

2. 在此目錄中，建立一個副檔名為 .sql 的空白檔案。

3. 在任意文字編輯器中開啟建立的 .sql 檔案。

4. 在 .sql 檔案中，輸入所需的 SQL 查詢，然後儲存該檔案。

5. 在安裝有管理伺服器的裝置上，在命令列，輸入以下指令以從 .sql 檔案執行 SQL 查詢並儲存結果到 result.xml 檔案：
   `sudo ./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。

6. 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。

7. 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。

PostgreSQL 的例子：

```
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",

  /* 事件的顯示敘述 */
  "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" AS "e"
  INNER JOIN "v_akpub_host" AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc' + make_interval(days => CAST(-7 AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

MySQL 或 MariaDB 的例子：

```
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`,

  /* 裝置群組名稱 */
  `e`.`wstrGroupName`,

  /* 發生事件的裝置的顯示名稱 */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp` DIV 1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp` DIV 65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp` DIV 256) & 255) AS CHAR), 4), '.',

    /* 發生事件的裝置的 IP 位址 */
    LEFT(CAST((`h`.`nIp`) & 255) AS CHAR), 4)
  ) AS `strIp`
FROM `v_akpub_ev_event` AS `e`
  INNER JOIN `v_akpub_host` AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7 DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

檢視卡巴斯基安全管理中心 Linux 資料庫名稱

如果要透過 MySQL 或 MariaDB 資料庫管理工具存取卡巴斯基安全管理中心 Linux 的資料庫，您必須知道資料庫的名稱，以便從您的 SQL 指令碼編輯器連線該資料庫。

要檢視卡巴斯基安全管理中心 Linux 資料庫名稱：

1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在**一般**頁簽上，選擇**目前資料庫詳細資訊**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。

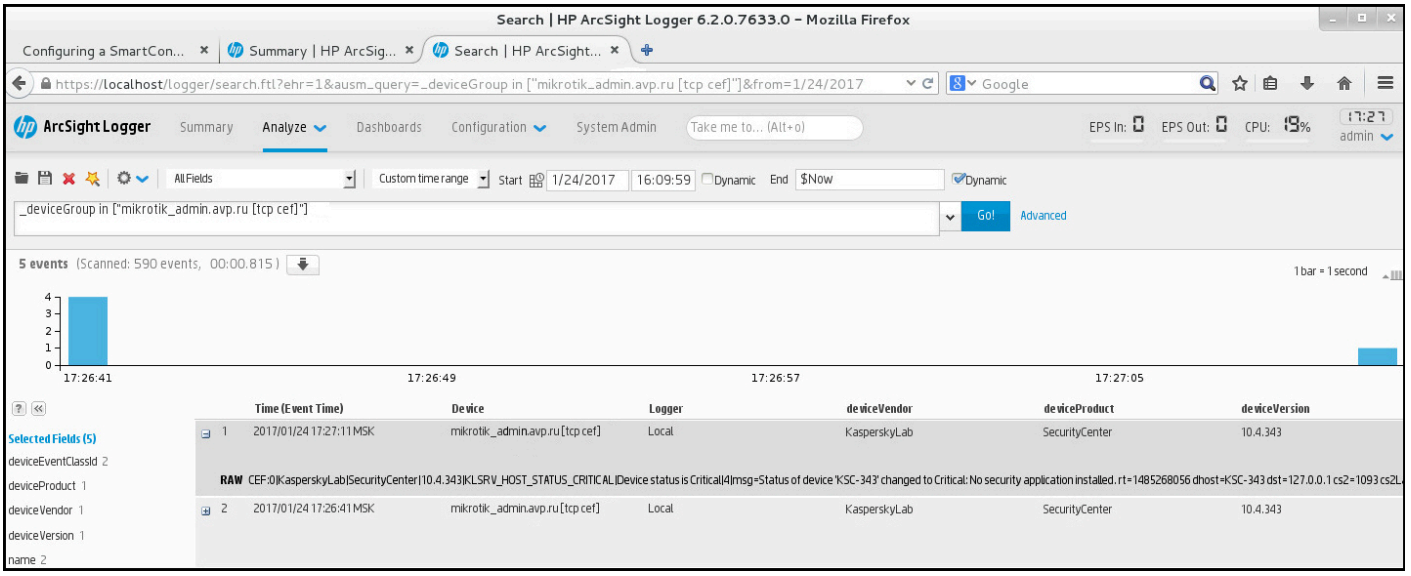
檢視匯出結果

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 Linux 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 Linux 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

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 Linux 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：

- 檢視已選取的修訂（僅適用於政策）
- 將對物件所做的變更回溯到選取的修訂
- 將修訂儲存為 JSON 檔案（僅適用於政策）

在支援修訂管理的任何物件的內容視窗中，**變更歷史**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。
- **使用者裝置 IP 位址** — 從中修改物件之裝置的 IP 位址。
- **網頁主控台 IP 位址** — 用於修改物件的卡巴斯基安全管理中心網頁主控台的 IP 位址。
- **動作** — 對物件執行的操作。
- **描述** — 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。

檢視並儲存政策修訂

卡巴斯基安全管理中心 Linux 可讓您檢視在特定時間段內對政策進行了哪些修改，並將這些修改的相關資訊儲存在檔案中。

如果對應的管理 Web 外掛程式支援此功能，則可以檢視和儲存政策修訂。

檢視政策修訂：

1. 在主功能表中，前往**資產管理** → **政策**。
2. 按一下要檢視修訂的政策，然後前往**變更歷史**區域。
3. 在政策修訂清單中，按一下要檢視的修訂編號。

   如果修訂大小超過 10 MB，您將無法使用卡巴斯基安全管理中心網頁主控台查看它。系統將提示您將已選取的修訂儲存到 JSON 檔案。

   如果修訂大小未超過 10 MB，則會顯示 HTML 格式的報告，其中包含已選取政策修訂的設定。由於報告會顯示在彈出視窗中，請確保您的瀏覽器允許彈出視窗。

對於 Kaspersky Endpoint Security for Windows 和 Kaspersky Endpoint Security for Mac 的政策，報告將不包含政策設定檔資訊。

若要將政策修訂儲存到 JSON 檔案，

在政策修訂清單中，選取要儲存的修訂，然後點擊**儲存到檔案**。

修訂將儲存到 JSON 檔案。

如有必要，您可以比較政策修訂版本。此選項適用於管理伺服器、網路代理程式、Kaspersky Endpoint Security for Windows（從14.0網頁外掛程式版本開始）和 Kaspersky Endpoint Security for Mac（從12.2.1 Patch A網頁外掛程式版本開始）。

比較政策版本

您可以將政策的歷史版本與其目前版本進行比較，比較清單中選定的不同版本，或將一個政策的版本與另一個政策的版本進行比較。此選項適用於管理伺服器、網路代理程式、Kaspersky Endpoint Security for Windows（14.0及更高版本的網頁外掛程式）和 Kaspersky Endpoint Security for Mac （12.2.1 Patch A及更高版本的網頁外掛程式）。

若要檢視政策版本：

1. 在主功能表中，轉至**資產管理→政策**。
2. 按一下要比較其版本的政策。
   政策設定視窗隨即開啟。
3. 前往**變更歷史**頁籤，然後選取要比較的版本旁的核取方塊。
4. 在工具列中，按一下**比較**按鈕，然後從下拉清單中選擇以下選項之一：
   - **與目前版本比較**，如果您想將在步驟3中選擇的版本與相同政策的上次儲存版本進行比較。
   - **與選定版本比較**，若要比較步驟3中選取的兩個版本。

     核取方塊的選擇順序不會影響比較結果。預設情況下，會將所選版本的較早版本與最新版本進行比較。例如，若選取版本5和版本1旁邊的核取方塊，則會將版本1與版本5進行比較。報告將包含版本1中相對於版本5新增、刪除或變更的設定資訊。

   - **與其他政策版本比較**，若要比較兩個不同政策的版本。
     在開啟的右側窗格中，執行以下操作：
     a. 在**應用程式名稱**欄位中，選擇要比較的政策：網路代理程式或管理伺服器。
     b. 在**政策名稱**欄位中，指定要與步驟3中所選的政策版本進行比較的政策名稱。
        政策版本清單隨即顯示。
     c. 選取所需的版本，然後點擊**比較**按鈕。

   版本比較報告將以HTML格式顯示在瀏覽器的新頁籤中。

如果比較結果超過10MB，則會顯示對應的對話方塊。您可以點擊**儲存到檔案**按鈕將報告儲存為檔案，或取消操作。

該報告以您的卡巴斯基安全管理中心網頁主控台的介面語言顯示。您可以透過點擊該部分旁邊的向下箭頭圖示（▼）來展開報告的某些部分，或者透過點擊向上箭頭（▲）圖示來摺疊該部分。

報告包含以下資訊：

- 卡巴斯基標誌。
- 報告名稱。
- 報告建立時間和日期。
- 政策名稱、管理伺服器和管理群組，其中包括比較版本的政策。
- **另存為HTML**按鈕。點擊此按鈕，報告將儲存到您的電腦。
- **摘要**部分顯示有關比較版本的常規資訊：政策名稱、版本號、版本儲存的時間和日期、儲存版本的使用者以及版本描述

  對於繼承的政策，不顯示使用者。

- 比較版本之間的差異。差異顯示在以下部分：
  - **新增的設定**
  - **刪除的設定**
  - **變更設定**
  - **僅適用於物件1的設定**（若比較了兩個不同政策的版本）
  - **僅適用於物件 2 的設定**（如果您比較了兩個不同政策的修訂版本）

  如果某個部分沒有資料，則不會顯示該部分。

對於 Kaspersky Endpoint Security for Windows 和 Kaspersky Endpoint Security for Mac 的政策，版本比較報告將不包含政策設定檔資訊。

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**變更歷史**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。

主動威脅

有關在用戶端裝置上偵測到的未處理檔案的資訊儲存在**儲存區**部分，**活動威脅**子部分中。

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. 在主功能表中，轉至**儲存區→活動威脅**。

2. 執行以下操作之一：

   - 選取要解毒的檔案旁邊的核取方塊。

   - 點擊要解毒的檔案名稱。

3. 點擊**解毒**按鈕開始對檔案進行解毒。

   然後將嘗試對所選檔案進行殺毒。

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。檔案的記錄將從**活動威脅**部分的清單中刪除。如果檔案無法被解毒，安全應用程式將其從裝置刪除。檔案的記錄將從**活動威脅**部分的清單中刪除。

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。

下載未處理檔案

Kaspersky Security Center for Linux允許您下載用戶端裝置上未處理檔案的副本。這指的是已由應用程式處理或刪除的檔案。這些檔案將複製到已安裝Kaspersky Security Center for Linux的裝置上，並存放於指定資料夾中。

如果檔案在殺毒期間被刪除或修改，並且檔案的副本儲存在受管理裝置上的Kaspersky Endpoint Security for Windows儲存體中，您可以儲存檔案的副本。

若要下載未處理檔案的副本：

1. 在主功能表中，轉至**儲存區→活動威脅**。
2. 執行以下操作之一：
   - 選中要下載檔案旁邊的核取方塊。
   - 點擊要下載的檔案名稱。
3. 點選**下載**按鈕開始下載。

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“活動威脅”部分中刪除檔案

*若要從**活動威脅**中刪除文件：*

1. 在主功能表中，轉至**儲存區→活動威脅**。
2. 執行以下操作之一：
   - 選取要刪除的檔案旁邊的核取方塊。
   - 點擊要刪除的檔案名稱。
3. 點選**刪除**按鈕來刪除檔案。
4. 在開啟的視窗中，點擊**刪除**按鈕。

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。檔案的記錄從**活動威脅**部分的清單中刪除。

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 Linux 根據以下規則處理未分配裝置組中的裝置：

- 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**未指派的裝置**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 Linux 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。

從隔離區和檔案備份下載和刪除檔案

本節提供有關如何從卡巴斯基安全管理中心網頁主控台中的隔離區和檔案備份下載和刪除檔案的資訊。

從隔離區和檔案備份區下載檔案

僅當滿足以下兩個條件之一時，您才能從隔離區和檔案備份下載檔案：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。

要將隔離區或檔案備份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** → **檔案備份**。
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。

關於從隔離區、檔案備份區或主動威脅儲存路中刪除物件

當安裝在用戶端裝置上的卡巴斯基安全應用程式將物件放入隔離、備份或活動威脅儲存區時，它們會將有關新增物件的資訊傳送到卡巴斯基安全管理中心 Linux 的**隔離**、**檔案備份**或**活動威脅**區域。開啟其中一個部分時，您可以刪除所需的物件。

對於**檔案備份**或**活動威脅**部分，從清單中選擇一個物件，然後按一下**刪除**按鈕。

對於**隔離**，您可以進行以下操作之一：

- 選取要刪除的物件名稱旁的核取方塊，然後在工具列中按一下**刪除**按鈕。
- 點擊要刪除的物件名稱，然後在開啟的詳細資料視窗的工具列中點擊**刪除**按鈕。

  在這種情況下，物件將被刪除，螢幕上會顯示相應的通知，詳細資料視窗會關閉。

卡巴斯基安全管理中心 Linux 會從清單中移除所選物件，或從儲存庫中刪除所選物件。要執行的操作由將選定物件放置到存放庫的卡巴斯基應用程式定義。卡巴斯基應用程式在“**項目新增者**”欄位中指定。

有關要執行的操作的詳細資訊，請參閱卡巴斯基應用程式的文件。

透過SNMP管理應用程式

本章節介紹如何在Linux中使用SNMP（簡單網路管理協議）從管理伺服器取得資訊。

SNMP是一種用於管理網路裝置的協定。

為了透過SNMP運作， Kaspersky Security Center for Linux使用作業系統中包含的snmpd服務和SNMP代理程式來監控管理伺服器的效能，並透過OID將資料傳送到其他應用程式。Kaspersky Security Center for Linux可以統計資料或SNMP陷阱的形式發送此訊息，SNMP陷阱是關於應用程式事件的通知。

SNMP可讓您存取有關應用程式的以下資訊：

- 一般資訊
- 自應用程式安裝以來Kaspersky Security Center for Linux的統計資料
- 關於Kaspersky Security Center for Linux事件的資訊

已授予唯讀權限。

有關SNMP陷阱和透過SNMP發送的統計資料的資訊儲存在adminkit.mib檔案中。預設情況下，adminkit.mib檔案位於/opt/kaspersky/ksc64/share/snmp/資料夾中。

每個叢集節點上的本機snmpd服務充當SNMP伺服器，接收統計資料。不支援與外部SNMP伺服器互動。可以透過在每個叢集節點上本機使用snmptrapd服務來接收SNMP陷阱，或者可以將它們重新導向到外部伺服器。

對於透過SNMP進行的操作，請在每個叢集節點的作業系統中預先設定snmpd服務。

在作業系統中設定snmpd服務

在設定之前，請確保您的作業系統中已安裝snmpd服務。

建立用於存取資料的使用者帳戶

在建立帳戶之前，請執行以下命令停止snmpd服務：

```
bash
sudo systemctl stop snmpd
```

為了確保透過SNMPv3進行資料存取的安全性（包括身分驗證和加密），您需要在snmpd服務端建立使用者帳戶，並填寫以下資訊：

- 使用者名稱（區分大小寫）
- 身分驗證演算法（MD5 或 SHA，建議使用 SHA）
- 身份驗證密碼
- 加密演算法（僅支援AES）
- 加密密碼

您可以透過以下方式建立使用者帳戶：

- 使用net-snmp-create-v3-user公用程式（若在作業系統中可用）。
- 手動將適當的指令新增到 snmpd 服務的設定檔中。

若要使用net-snmp-create-v3-user工具建立使用者帳戶，請執行以下命令：

```
net-snmp-create-v3-user -ro -a <身分驗證演算法> -x <加密演算法> <使用者名稱>
```

身份驗證和加密密碼將以互動方式提示。

例如：

```
net-snmp-create-v3-user -ro -a SHA -x AES MonitoringUser
```

若要手動建立使用者帳戶：

1. 若要建立/var/lib/snmp/snmpd.conf組態檔，請執行以下命令：

   ```
   touch /var/lib/snmp/snmpd.conf
   ```

2. 將以下行新增至組態檔：

   ```
   createUser <使用者名稱> <身分驗證演算法> "<身分驗證密碼>" <加密演算法> "<加密密碼>"
   ```

   例如：

   ```
   createUser MonitoringUser SHA "MonitoringAuthSecret" AES "MonitoringPrivSecret"
   ```

建立用於接收SNMP陷阱的使用者帳戶

若要透過SNMPv3接收經過身分驗證和加密的SNMP陷阱，需要在監控系統端的相應服務（通常是snmptrapd服務）的上下文中建立帳戶。

帳戶必須包含以下資訊：

- 使用者名稱
- 身份驗證演算法
- 身份驗證密碼
- 加密演算法
- 加密密碼

> 出於安全考慮，請使用不同的使用者帳戶分別存取資料並接收SNMP陷阱。

有關建立用於接收SNMP陷阱的使用者帳戶的說明，請參閱監控系統的說明文件。

設定snmpd服務

snmpd服務的組態儲存在/etc/snmp/snmpd.conf檔案中。您可以將必要的資訊新增至現有設定檔中，也可以新建一個設定檔，並依照給定順序新增對應的行。

> 如果選擇新建組態檔，請確保只有超級使用者才能存取它。如果未設定所需的存取權限，請依指定順序執行以下命令進行設定：
> `[[chown root:root /etc/snmp/snmpd.conf`
> `[[chmod 600 /etc/snmp/snmpd.conf`

若要設定snmpd服務：

1. 在組態檔中，指定snmpd服務監聽傳入請求的協定、網路介面位址和連接埠號碼。
   - 若要監聽所有網路介面上的請求，請將以下行新增至組態檔：

     ```
     agentAddress udp:161
     ```

   - 若只想監聽本機網路介面上的請求（例如，如果監控系統安裝程式在同一台機器上），請將下列行新增至組態檔：

     ```
     agentAddress udp:127.0.0.1:161
     ```

2. 設定卡巴斯基安全管理中心 Linux 與 snmpd 服務之間的互動。您可以使用UNIX套接字或TCP套接字。

- 如果您使用UNIX套接字：

  a. 指定UNIX套接字的路徑和權限。為此，請將以下行新增至組態檔：

  ```
  master agentx
  agentXSocket unix:/var/run/agentx-master.socket
  agentXPerms 770 770 kluser klusers
  ```

  b. 將klusers群組新增為{'KLSRV_UNATT_KLSVCUSER'}帳戶的補充群組。

- 如果您使用TCP套接字，請指定TCP套接字的連接埠和位址。為此，請將以下行新增至組態檔：

  ```
  master agentx
  agentXSocket tcp:127.0.0.1:705,tcp6:[::1]:705
  ```

3. 將最小回應超時時間設定為至少30秒。為此，請將以下行新增至組態檔：

```
agentxTimeout 30
```

4. 如有必要，您可以提供設定了 SNMP的伺服器的描述、系統位置以及管理員的聯絡位址。為此，請將以下行新增至組態檔：

```
sysDescr <伺服器描述>
sysLocation <伺服器位置>
sysContact <管理員的聯絡位址>
sysServices 72
```

5. 請指定要透過SNMP協定向監控系統開放的OID樹狀圖範圍。為此，請將以下行新增至組態檔：

```
view monitoring included .1.3.6.1.4.1.23668.1093.1
view systemonly included .1.3.6.1.4.1.23668.1093.1
```

6. 如有必要，您也可以指定包含snmpd服務儲存的作業系統資訊的OID樹狀圖範圍。此範圍將可用於您的監控系統。

有關作業系統的資訊包括有關 CPU 和 RAM 使用情況的資訊、磁碟分割區上的可用空間、網路介面的負載情況、已安裝軟體清單、開放網路的連線清單以及正在執行的程序清單。部分資訊可能屬於機密資訊。

- 如果您只想允許存取一般系統資訊以及有關RAM、CPU和磁碟裝置使用情況的資訊，請在組態檔中新增以下行：

```
# SNMPv2-MIB - Basic system information
view monitoring included .1.3.6.1.2.1.1
# HOST-RESOURCES-MIB - CPU, Memory, Filesystems
view monitoring included .1.3.6.1.2.1.25.1
view monitoring included .1.3.6.1.2.1.25.2
view monitoring included .1.3.6.1.2.1.25.3
view monitoring included .1.3.6.1.2.1.25.5
# UCD-SNMP-MIB - Memory and CPU usage
view monitoring included .1.3.6.1.4.1.2021.4
view monitoring included .1.3.6.1.4.1.2021.10
view monitoring included .1.3.6.1.4.1.2021.11
# UCD-SNMP-DISKIO-MIB - Block devices I/O statistics
view monitoring included .1.3.6.1.4.1.2021.13
# IF-MIB - Network interfaces I/O statistics
view monitoring included .1.3.6.1.2.1.2
view monitoring included .1.3.6.1.2.1.31
```

- 如果您想允許存取所有系統資訊，請在組態檔中新增以下行：

```
view monitoring included .1
```

7. 為建立的使用者帳戶指定存取模式和資訊範圍。為此，請將以下行新增至組態檔：

```
rouser <user name> priv -V monitoring
```

8. 若要傳送SNMP陷阱，請指定監控系統的IP位址和接收陷阱的使用者憑據。為此，請將以下行新增至組態檔：

```
trapsess -Ci -v3 -t0.1 -r1 -l authPriv -u <接收陷阱的使用者名稱> -a <身分驗證演算法> -A "<接收陷阱的使用者密碼>" -x
<加密演算法> -X "<加密密碼>" udp:<IP位址>:162
```

snmpd服務隨即設定完成。

若要與多個監控系統整合，請為每個系統建立一個單獨的使用者帳戶，指定每個使用者帳戶的可用資訊範圍（「view」和「rouser」指令），並設定SNMP陷阱的傳送（「trapsess」指令）。

使用新組態啟動snmpd服務

若要套用新組態：

1. 重新啟動snmpd服務：

```
systemctl restart snmpd
```

2. 檢查snmpd服務的狀態：

```
systemctl status snmpd
```

狀態必須為`running`。

3. 允許該服務在作業系統啟動時自動啟動：

```
systemctl enable snmpd
```

4. 如果您在作業系統或網路裝置中使用防火牆，請新增規則，讓SNMP資料包通過。

snmpd服務隨即運行。

如果klcssnmp服務在設定snmpd服務時正在執行，也請重新啟動klcssnmp服務。

檢查snmpd服務的運行狀況

若要測試 snmpd 服務，請在卡巴斯基安全管理中心 Linux 中設定 SNMP 的使用，並使用 snmpwalk 公用程式請求 SNMP 資料。

若要取得Kaspersky Security Center for Linux提供的SNMP資料範圍，

執行以下命令：

```
snmpwalk -v3 -l authPriv -u <使用者名稱> -a <驗證演算法> -A "<驗證密碼>" -x <加密演算法> -X "<加密密碼>" <IP 位址>
.1.3.6.1.4.1.23668.1093.1
```

例如：

```
snmpwalk -v3 -l authPriv -u MonitoringUser -a SHA -A "MonitoringAuthSecret" -x AES -X "MonitoringPrivSecret"
127.0.0.1 .1.3.6.1.4.1.23668.1093.1
```

啟用和停用SNMP通知

卡巴斯基安全管理中心 Linux 以 SNMP 陷阱的形式傳送有關管理伺服器事件的通知。

預設情況下，Kaspersky Security Center for Linux事件的SNMP通知是停用的。

啟用或停用Kaspersky Security Center for Linux事件的SNMP通知：

1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗將開啟。

2. 在內容視窗的**事件組態**頁籤上，點擊要接收SNMP通知的事件類型。

3. 在開啟的窗格中，啟用或停用**透過 SNMP 通知**切換開關。
   僅當啟用**透過 SNMP 傳送統計資料**選項時，此選項才可用。

Kaspersky Security Center for Linux事件的SNMP通知根據您的選擇啟用或停用。

在Kaspersky Security Center for Linux中啟用和停用SNMP

預設情況下，透過SNMP傳送統計資料是啟用的。若要傳送SNMP陷阱，請設定snmpd服務。

若要啟用或停用透過SNMP傳送統計資料：

1. 在主選單中，按一下管理伺服器名稱。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**SNMP**區段。
3. 啟用或停用**透過 SNMP 傳送統計資料**開關。
4. 點擊**儲存**。

根據您的選擇，透過SNMP傳送統計資料的功能將啟用或停用。

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。

SNMP 物件識別碼的值和說明

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` 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。 如果找到一些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` 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` 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。

物件識別碼的值	數字資料類型	OID	敘述
licenceExpired	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.4	deploymentStatus 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	在不到 7 天內過期的產品授權金鑰 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	產品授權在不到 7 天內過期的的裝置數量。
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	管理伺服器長時間未更新。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	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	Hex-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	包含長時間未更新的病毒資料庫的裝置數量（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）。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。
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	某些裝置上的安全應用程式未執行。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	某些裝置上的即時保護未執行。您可透過 hostsRealtimeNotRunning 取得這些裝置的數量。
psRealtimeLevelChanged	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.3	執行階段的防護等級與管理員在管理群組中 N 台電腦上設定的等級不同。
notCuredFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.4	有包含未解毒物件的裝置。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	在某些裝置上發現威脅。您可透過 hostsTooManyThreats 取得這些裝置的數量。

物件識別碼的值	數字資料類型	OID	敘述
virusOutbreak	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.6	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。
psVulnerabilitiesFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.7	偵測到弱點。
psEncryptionFaultsFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.8	偵測到導致裝置防護狀態變更的加密錯誤。
psVulnerableHostsFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.9	在某些裝置上偵測到弱點。
psNotScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.10	偵測到長時間未進行完整掃描的裝置。
psNagentsNotRunningUntilReboot	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.11	偵測到網路代理僅在重新啟動後才啟動的裝置。
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	病毒完整掃描的狀態為以下之一： • **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	某些裝置一段時間內未掃描。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	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	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。
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。

物件識別碼的值	數字資料類型	OID	敘述
`eventsStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.6.1	事件子系統的狀態為以下之一： • **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： 至少一台裝置上存在“緊急”事件。 至少一台裝置上存在“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。 • **資訊**。以下之一： 所有裝置上次進行完整病毒掃描至今不到一週。 遠端安裝任務已完成，無需重新啟動任何裝置。 上次管理伺服器更新至今不到一週。 管理伺服器已長時間未更新，但目前正在進行更新。 • **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` 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。

在 Kaspersky Next XDR Optimum 產品授權下使用卡巴斯基安全管理中心 Linux

如果您購買了 Kaspersky Next XDR Optimum 產品授權作為 EPP 應用程式產品授權和卡巴斯基安全管理中心 Linux 產品授權的一部分，則在執行初始設定後，您將能夠使用 Kaspersky Next XDR Optimum 功能。

如果您在裝置上安裝並啟動卡巴斯基應用程式後，單獨購買了 Kaspersky Next XDR Optimum 產品授權作為先前購買的產品授權的延伸程式，則必須使用新的啟動碼或金鑰檔案在裝置上重新啟動卡巴斯基安全管理中心 Linux，具體取決於您購買 Kaspersky Next XDR Optimum 產品授權的方式。之後，您可以執行初始設定。

此外，您也可以在測試模式下使用 Kaspersky Next XDR Optimum 的功能。為此，必須先新增從屬實體管理伺服器，然後透過 Kaspersky Next XDR Optimum 試用產品授權啟用此伺服器。在試用產品授權有效期內，Kaspersky Next XDR Optimum 功能將在從屬伺服器上可用。

在您使用 Kaspersky Next XDR Optimum 產品授權啟動管理伺服器並將產品授權金鑰部署到相關管理伺服器管理的裝置後，您可以執行下列操作：

- 透過與 Kaspersky Automated Security Awareness Platform、Kaspersky Threat Intelligence Portal Sandbox和 Active Directory整合來回應威脅。
- 按屬性對警示進行分組。

有關 Kaspersky Next XDR Optimum 產品授權啟用的功能的更多資訊，請參閱Kaspersky Endpoint Detection and Response Optimum 說明。

用於回應警示的整合

如果您擁有 Kaspersky Next XDR Optimum 產品授權，則可以配置與以下解決方案的整合以回應威脅：

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal Sandbox
- Active Directory

如果您已在 Kaspersky Next XDR Optimum 產品授權下啟用管理伺服器，則可使用這些整合。
若要執行回應動作，您必須將 Kaspersky Next XDR Optimum 產品授權金鑰部署到受管理的應用程式。
透過試用產品授權使用 Kaspersky Next XDR Optimum 功能時，必須先新增從屬實體管理伺服器，並在試用產品授權下啟用此從屬管理伺服器，然後才能將產品授權金鑰部署到由此管理伺服器管理的裝置。

如果您使用的是 Kaspersky Next EDR Optimum 產品授權，則無需啟動在 Kaspersky Next XDR Optimum 產品授權下安裝在受管理裝置上的應用程式。您僅需為新裝置（如有）執行此操作。

因為 Kaspersky Next XDR Optimum 產品授權支援多租戶，您可以集中將產品授權金鑰發佈到受管理應用程式。不支援將產品授權自動分發到從屬和虛擬管理伺服器。

要配置整合，您必須具有**一般功能：應用程式整合**功能區域的**讀取**和**寫入**權限。

配置與 Active Directory 的整合以執行回應操作

與 Active Directory 整合可讓您對受到警示影響或涉及警示的 Active Directory 使用者執行回應操作。

若要設定與 Active Directory 的整合以回應警示，您必須使用卡巴斯基安全管理中心 Linux 管理伺服器 15.4 或更高版本。

與 Active Directory 整合以回應警示，以及在配置網域控制器輪詢時指定的 Active Directory 網域控制器掃描設定（網域控制器的位址和使用者憑據）是兩種不同的設定。由於您需要確保要對其執行回應操作的使用者擁有 Active Directory 帳戶，因此您必須配置這兩個整合：用於掃描和用於回應。順序不重要。

整合設定不會被繼承，僅被套用於您在其上配置這些設定的管理伺服器（實體或虛擬）。

若要配置與 Active Directory 的整合以回應警示：

1. 在主功能表中，按一下管理伺服器名稱。

   管理伺服器內容視窗會開啟，含有所選的**一般**頁籤。

2. 執行以下其中一項操作：

   - 選擇**發佈點**部分，按一下所需發佈點的名稱，然後在開啟的內容視窗中選擇**Active Directory**部分。
   - 選取「**Active Directory 回應**」區域。

3. 在右側窗格中，啟用**Active Directory 整合**切換開關。

   稍後，如果想關閉整合，您只能透過停用**Active Directory 整合**切換開關對所有連線執行此操作。您無法關閉單獨連線的整合。相反，您可以刪除該連線。

   > 當您啟用或停用「**Active Directory 整合**」切換開關時，此設定將同時套用於「**Active Directory 回應**」與「**發佈點**」區域。

4. 點擊「**新增**」按鈕，以建立與 Active Directory 網域控制器的連線。

5. 在開啟的視窗中，指定連線的以下參數：

   - **網域控制器位址**

     電腦名稱，例如：`server.mycompany.com`。

     您可以指定多個位址。您指定位址的所有網域控制器必須屬於同一個網域。

   - **Active Directory 網域名稱**

     DNS 完整網域名稱，例如：`mycompany.com`

     此外，您也可以指定 SAM 或 NetBIOS 名稱，例如： `mycompany`

     使用小寫字母。如果為管理伺服器或發佈點建立多個連線，請為每個連線指定不同的名稱。

     > 若要執行回應操作，您在此欄位中指定的 Active Directory 網域必須與警示中指定的 Active Directory 網域名稱相符。

- **登入**

  具有管理員權限的 Active Directory 帳戶的登入名，回應操作在該帳戶下執行。

- **密碼**

  具有管理員權限的 Active Directory 帳戶的密碼，回應操作在該帳戶下執行。

6. 若要檢查連線狀態，請點擊「**偵測連線**」按鈕。

   若連線成功建立，則會顯示「**已連線**」狀態。否則，狀態將顯示為「**失敗**」，且會顯示無法連線至網域控制器的錯誤訊息。

> 您必須考慮連線到 Active Directory 的方式：**從 Linux 裝置還是從 Windows 裝置**。

從 Linux 裝置連線

預設情況下，從 Linux 裝置連線並驗證網域控制器時，邏輯如下：

1. 管理伺服器或發佈點嘗試透過 LDAPS 連線到網域控制器。

   需要執行 LDAP 伺服器憑證強驗證。

2. 將網域控制器憑證的公共部分放入系統憑證儲存區以驗證憑證。

   會使用依作業系統而定的系統憑證授權單位 (CA) 路徑來存取憑證鏈。

   例如：

   - /etc/ssl/certs/ca-certificates.crt — 基於 Debian 的作業系統 (Debian、Ubuntu、Astra) 的路徑。
   - /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem — CentOS 或 Red Hat 的路徑。

3. 如果 LDAPS 連線失敗，則會發生錯誤，不會使用其他連線協定。

> 如果出現 LDAPS 問題，您可以聯絡卡巴斯基技術支援。

如果您不想將憑證安裝到系統憑證儲存區中，可以使用 KLNAG_LDAP_SSL_CACERT 標誌來設定網域控制器憑證的路徑。為此，請執行以下命令：

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "</path/to/domain-controller/cert>"
```

其中`</path/to/domain-controller/cert>`是網域控制器憑證公共部分的路徑。

例如，如果路徑是`"/var/opt/kaspersky/ldap_cert.crt"`，則命令為`klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "/var/opt/kaspersky/ldap_cert.crt"`

從 Windows 裝置連線

從 Windows 裝置連線並驗證網域控制器時，連線設定由網域定義。

您只需確保：

- LDAPS 已啟用且連接埠 636 在裝置上可用。
- 您允許透過防火牆或代理伺服器連線到網域控制器。

7. 按一下**儲存**按鈕。

視窗關閉，連線顯示在連線表中。

在連線表中，您可以進行以下操作：

- 編輯連接參數。

  為此，請按一下所需連接的**網域控制器位址**參數的連結。在開啟的視窗中，變更所需設定，然後點擊**儲存**按鈕。

  您只能編輯**登入** 和**密碼** 參數。

- 刪除連接。

  為此，請選取要刪除的連線旁邊的核取方塊，按一下工具列中的**移除**按鈕，然後確認刪除連線。

配置與 Kaspersky Automated Security Awareness Platform 的整合

與Kaspersky Automated Security Awareness Platform整合（以下也稱為 KASAP）可讓您指派 KASAP 學習課程給與警示相關的使用者。

整合設定不會被繼承，僅被套用於您在其上配置這些設定的管理伺服器（實體或虛擬）。

> 在卡巴斯基安全管理中心網頁主控台中配置整合之前，您必須在 KASAP 中建立授權權杖並取得 API 請求的 URL。

要配置與 Kaspersky Automated Security Awareness Platform 的整合：

1. 在主選單中，按一下管理伺服器名稱。

   管理伺服器內容視窗會開啟，並含有所選的**一般**頁籤。

2. 選取「**KASAP**」區域。

3. 在右側窗格中，啟用**KASAP 整合**切換開關。

4. 指定用於連線 KASAP 的設定：

   - **API 權杖**— 您建立的用於存取 KASAP Open API 的權杖。
   - **URL** — 建立 API 令牌時所取得的 API 請求的 URL。
   - **使用代理伺服器** — 可讓您在連線到 KASAP 時啟用代理伺服器的切換開關。

     依預設已停用該切換開關。

5. 如有必要，請按一下**偵測連線**按鈕以驗證您指定的設定。
   連線狀態將顯示。

6. 按一下**儲存**按鈕。

已配置與 Kaspersky Automated Security Awareness Platform 的整合。

儲存 KASAP 整合設定後，您可以點擊**檢視群組**按鈕檢視 KASAP 學習群組清單。

如有必要，當顯示群組清單時，您可以透過點擊**重新整理群組**按鈕來更新它。

> 開啟清單後，您將無法隱藏它。如果停用**KASAP 整合**切換開關，則不會顯示 KASAP 群組清單。

配置與 Kaspersky Threat Intelligence Portal Sandbox 的整合

與Kaspersky Threat Intelligence Portal整合（以下也稱為 Kaspersky TIP）可讓您使用**Kaspersky Sandbox隔離**隔離區的檔案。

整合設定不會被繼承，僅被套用於您在其上配置這些設定的管理伺服器（實體或虛擬）。

> 在配置整合之前，您必須取得 Kaspersky TIP 上 API 請求的授權權杖。

要配置與 Kaspersky TIP Sandbox 的整合：

1. 在主選單中，按一下管理伺服器名稱。
   管理伺服器內容視窗會開啟，並含有所選的**一般**頁籤。

2. 選取「**Kaspersky TIP**」。

3. 在右側窗格中，啟用**整合**切換開關。
   與 Kaspersky TIP 的連線設定將顯示。

   > 如果在配置並儲存整合設定後停用**整合** 撥動開關，設定不會被刪除，但您將無法執行回應操作。

4. 按一下**新增權杖**按鈕，在開啟的視窗中，指定您先前在 Kaspersky TIP 上取得的權杖，然後按一下**新增** 按鈕。
   視窗關閉，API 權杖已新增。

5. 如果您想在連接到 Kaspersky TIP 時使用代理伺服器，請啟用**使用代理伺服器**切換開關。
   依預設已停用該切換開關。

6. 點擊**儲存**按鈕。

與 Kaspersky TIP Sandbox 的整合得到配置。

現在，您可以將檔案從 **隔離** 部分傳送到 Kaspersky TIP 和 Kaspersky Sandbox 進行威脅分析。檔案的最大大小是 100 MB

由於 Kaspersky Next XDR Optimum 產品授權支援多租戶，因此放置在**隔離區隔離** 由租戶劃分。如果管理員使用專用的 TIP 帳戶和與每個租用戶相關的 API 權杖，則此租用戶層級的分離也適用於將檔案傳送至 Kaspersky Sandbox 並檢視結果時。但是，由於隔離清單不會根據伺服器層次結構顯示物件，因此無法集中管理所有租用戶的**隔離**部分。

按屬性分組警示

警示聚合有助於識別可能與相同事件相關的警示，從而簡化調查過程。

若要啟用警示聚合功能，您必須執行下列操作：

- 在主選單中啟用**警示**子部分。
- 在 Kaspersky Next XDR Optimum 產品授權下啟動管理伺服器，然後將 Kaspersky Next XDR Optimum 產品授權金鑰部署到您的受管理應用程式。

  在測試模式下透過試用產品授權使用 Kaspersky Next XDR Optimum 時，必須先新增從屬實體管理伺服器，然後透過該產品授權啟用此伺服器。

如果您使用的是 Kaspersky Next EDR Optimum 產品授權，則無需啟動在 Kaspersky Next XDR Optimum 產品授權下安裝在受管理裝置上的應用程式。您僅需為新裝置（如有）執行此操作。
因為 Kaspersky Next XDR Optimum 產品授權支援多組織用戶，您可以集中將產品授權金鑰發佈到受管理應用程式。不支援將產品授權自動分發到從屬和虛擬管理伺服器。

您可以按裝置名稱、帳戶或雜湊名稱（SHA256）聚合警示。

> 僅當屬性不為空時，才會根據屬性聚合警示。

如果警示至少共用一個屬性，並且在群組中任何其他警示的 24 小時內發生，則這些警示會聚合在一起。

要按屬性聚合警示：

1. 在主功能表中，轉至**監控** → **警示**。
2. 執行以下其中一項操作：
   - 啟用 **警示聚合** 切換開關，然後選擇用來聚合警示的一個或多個屬性：
     - **裝置名稱**
     - **帳戶**
     - **檔案雜湊值**雜湊名稱 （SHA256）

     預設選擇**裝置名稱** 和 **帳戶**屬性。
   - 按一下設定圖示 (⚙)。在開啟的**表格設定**窗格中，前往 **分組**頁簽。選擇 **聚合群組 ID** 並點擊 **套用**。

啟用聚合後，警示將按**事件時間**從最新到最舊進行排序。不支援其他排序選項。選擇不同的分組選項將停用聚合。

該表顯示按屬性匯總的警示。未匯總的警示顯示在表格的底部。

聚合後，每個警示僅被指派給一個群組。

卡巴斯基安全管理中心網頁主控台和其他卡巴斯基解決方案之間的互動

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。

建立背景連線

例如，為了設定卡巴斯基安全管理中心 Linux 與另一個卡巴斯基應用程式或解決方案之間的互動，例如 Kaspersky Managed Detection and Response（也稱為 MDR），則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。

> 您只能配置 Kaspersky Managed Detection and Response 與基於 Windows 的卡巴斯基安全管理中心版本之間的互動。

要建立背景連線：

1. 在主功能表中，轉至**設定** → **整合**。
2. 選擇**網頁主控台代理伺服器設定**頁簽。
3. 在**整合**區域，將用於建立背景連線的切換按鈕切換到位置：**整合的背景連線 已啟用**。
4. 在開啟的**啟用背景連線**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 Linux 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卡巴斯基安全管理中心 網頁主控台和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 Linux 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。

配置代理伺服器連線

若要為卡巴斯基安全管理中心網頁主控台和 Web 外掛程式配置代理伺服器連線：

1. 在主功能表中，轉至**設定** → **整合**。
2. 選擇**網頁主控台伺服器設定**頁簽。
3. 啟用**使用代理伺服器**選項。

4. 指定代理伺服器連線設定：

- **代理伺服器位址**
- **埠號**
- **代理伺服器身分驗證**
- **使用者名稱**（如果啟用**代理伺服器驗證**選項則需要）
- **密碼**（如果啟用**代理伺服器驗證**選項則需要）

5. 點擊「**儲存**」以儲存代理伺服器連線設定。

如果您有管理伺服器層級結構，代理伺服器連線設定不會傳播到用於管理從屬管理伺服器的網頁主控台。您必須為每個卡巴斯基安全管理中心網頁主控台單獨設定代理伺服器連線。

用戶端裝置的遠端診斷

您可在 Windows 和 Linux 用戶端裝置上遠端執行遠端診斷：

- 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。

開啟遠端診斷視窗

若要執行對 Windows 和 Linux 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操作：
   - 若裝置屬於管理群組，請在主功能表中，前往**資產管理 → 資產（裝置）**。
   - 若裝置屬於「未指派的裝置」群組，請在主功能表中，轉至**資產管理→未指派的裝置**。
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**進階**頁籤上，點擊**遠端診斷**。
   這會開啟用戶端裝置的**遠端診斷** 視窗。如果管理伺服器和用戶端裝置之間未建立連線，則會顯示錯誤訊息。

或者，如果您需要立即獲取有關基於 Linux 的用戶端裝置的所有診斷資訊，您可以在此裝置上執行 collect.sh 指令碼。

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. 在遠端診斷視窗中，選擇**卡巴斯基應用程式**頁簽。

   在**應用程式管理**區域中，裝置上安裝的卡巴斯基應用程式清單得以顯示。
3. 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開啟。
4. 若您要啟用偵錯：

   a. 在**偵錯**區域中，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。

   > 在基於 Linux 的用戶端裝置上，網路代理元件更新程式的偵錯由網路代理設定管理。因此，在執行 Linux 的用戶端裝置上，此元件的**啟用偵錯**和**修改偵錯等級**"選項被停用。

5. 若您要停用對選取的應用程式偵錯，請點擊**停用偵錯**按鈕。

   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。

要啟用和配置 Xperf 偵錯或停用它：

1. 開啟用戶端裝置的遠端診斷視窗。

2. 在遠端診斷視窗中，選擇**卡巴斯基應用程式**頁簽。

   在**應用程式管理**區域中，裝置上安裝的卡巴斯基應用程式清單得以顯示。

3. 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。

4. 在**Xperf 偵錯**區域中，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。如果您想要停用 Kaspersky Endpoint Security for Windows 的 Xperf 偵錯，請點擊此按鈕。

5. 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操作：

   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。

6. 如果您想要停用 Kaspersky Endpoint Security for Windows 的 Xperf 偵錯，請點擊**Xperf 偵錯**區域中的**停用 Xperf 偵錯**。

   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. 在遠端診斷視窗中，選擇**卡巴斯基應用程式**頁簽。
   在**應用程式管理**區域中，裝置上安裝的卡巴斯基應用程式清單得以顯示。
3. 在應用程式清單中，選取您要為其下載偵錯檔案的應用程式。
4. 在**偵錯**部分中，點擊**偵錯檔案**按鈕。
   這會開啟**裝置偵錯記錄**視窗，其中會顯示偵錯檔案清單。
5. 在偵錯檔案清單中，選取您要下載的檔案。
6. 執行以下操作之一：
   - 點擊**下載**來下載所選檔案。您可以選擇一個或多個檔案進行下載。
   - 下載部分選取的檔案：
     a. 點擊**下載一部分**。
     您無法同時下載多個檔案的部分內容。如果您選擇多個偵錯檔案，**下載一部分**按鈕將被停用。
     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。
     對於基於 Linux 的裝置，無法編輯檔案部分名稱。
     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，選擇**事件記錄**頁簽。
3. 在**偵錯檔案**區段中，點擊**Windows Update 記錄**或**遠端安裝記錄**，視您要刪除的偵錯檔案而定。

   Windows Update 記錄連接僅適用於基於 Windows 的用戶端裝置。

   這會開啟**裝置偵錯記錄**視窗，其中會顯示偵錯檔案清單。

4. 在偵錯檔案清單中，選取一個或多個您要刪除的檔案。

5. 點擊**移除**按鈕。

   選取的偵錯檔案被刪除。

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. 在遠端診斷視窗中，選擇**卡巴斯基應用程式**頁簽。

3. 在**應用程式設定**區段中，點擊**下載**按鈕，下載用戶端裝置上已安裝應用程式設定的資訊。

包含資訊的 ZIP 存檔將被下載到指定位置。

從用戶端裝置下載系統資訊

從用戶端裝置下載系統資訊：

1. 開啟用戶端裝置的遠端診斷視窗。

2. 在遠端診斷視窗中，選擇**系統資訊**頁簽。

3. 點擊**下載**按鈕可下載有關用戶端裝置的系統資訊。

   如果您獲取有關基於 Linux 的裝置的系統資訊，則緊急終止的應用程式的傾印檔案會被新增到結果檔案中。

   該封存檔案可能包含純文字形式的敏感資料（例如金鑰和密碼）。建議您在將封存檔案傳送給卡巴斯基技術支援之前，先檢查封存檔案中的檔案並移除此類資料。

包含資訊的檔案將下載到指定位置。

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. 在遠端診斷視窗的**事件記錄**頁簽上，點擊**所有裝置記錄**。

3. 在**所有裝置記錄**視窗中，選取多個相關記錄。

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**。
  您無法同時下載多個日誌的部分內容。如果您選擇多個事件記錄，**下載一部分**按鈕將被停用。

  b. 在開啟的視窗中，根據您的需求指定要下載的名稱與記錄部分。
  對於基於 Linux 的裝置，無法編輯記錄部分名稱。

  c. 點擊**下載**。

選取的事件記錄或其部分，會下載至指定的位置。

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. 在遠端診斷視窗中，選擇**卡巴斯基應用程式**頁簽。
   在**應用程式管理**區域中，裝置上安裝的卡巴斯基應用程式清單得以顯示。
3. 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。
4. 點擊以下其中一個按鈕以選取操作：

   - **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。

   視您選取的操作而定，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 Linux 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 Linux 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. 在遠端診斷視窗中，選擇**卡巴斯基應用程式**頁簽。

   在**應用程式管理**區域中，裝置上安裝的卡巴斯基應用程式清單得以顯示。
3. 在應用程式清單中，選擇**卡巴斯基安全管理中心 Linux 網路代理**。

   遠端診斷選項清單隨即開啟。
4. 在**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。
5. 按一下“ **下載診斷報告**”按鈕下載報告。

報告將下載到指定位置。

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 Kaspersky 支援專家要求您這樣做的時候。您無需在該裝置上安裝該應用程式。

如果想在用戶端裝置上執行自訂指令碼，您可以使用`KLACDT_SAVE_SETTING`環境變數來確定儲存執行結果的路徑。例如：

- 對於基於 Windows 的裝置：

  ```
  @echo some result > %KLACDT_SAVE_SETTING%\res.log
  ```
- 對於基於 Linux 的裝置：

  ```
  [[echo some result > $KLACDT_SAVE_SETTING/res.log
  ```

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. 在遠端診斷視窗中，選擇**執行遠端應用程式**頁簽。
3. 在**物件類型**欄位中，選取要上傳的物件類型：
   - 選取**檔案**以上傳可執行檔。
   - 選取**資料夾**以上傳包含要在用戶端裝置上執行的應用程式的資料夾。

     如果選取此物件類型，則會出現**要執行的可執行檔名稱**欄位。在此欄位中，指定資料夾中可執行檔的名稱。您也可以指定檔案的相對路徑。

- 選取**存檔** 以上傳包含要在用戶端裝置上執行的應用程式的 ZIP 存檔。

  如果選取此物件類型，則會出現**要執行的可執行檔名稱**欄位。在此欄位中，指定資料夾中可執行檔的名稱。您也可以指定檔案的相對路徑。

  > ZIP 存檔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。

4. 透過在系統視窗中選取物件或將其拖曳到上傳欄位來上傳物件。
5. 如果需要，在**命令列參數**欄位中指定執行可執行檔時要傳遞的命令列參數。
6. 點擊**上傳和執行**按鈕以在用戶端裝置上執行選定的應用程式。
7. 應用程式執行成功完成後，點擊**下載應用程式執行結果**按鈕即可下載執行結果。

> 會儲存應用程式執行結果，直到您執行新的診斷或關閉視窗。

使用該應用程式對用戶端裝置進行遠端診斷已完成。

在基於 Linux 的用戶端裝置上執行遠端診斷

卡巴斯基安全管理中心 Linux 允許您從用戶端裝置下載基本診斷資訊。或者，您可以使用卡巴斯基的 collect.sh 指令碼獲取關於 Linux 裝置的診斷資訊。該指令碼在需要診斷的基於 Linux 的用戶端裝置上執行，然後產生一個檔案，其中包含診斷資訊、該裝置的系統資訊、應用程式的跟踪檔案、裝置日誌以及被緊急終止的應用程式的傾印檔案。

> 我們建議您使用 collect.sh 指令碼一次性獲取有關 Linux 用戶端裝置的所有診斷資訊。如果通過卡巴斯基安全管理中心 Linux 遠端下載診斷資訊，您將需要經過遠端診斷介面的所有部分。此外，Linux 裝置的診斷資訊可能無法完全獲得。

> 如果您需要將產生的包含診斷資訊的檔案傳送給卡巴斯基技術支援，請在傳送檔案之前刪除所有機密資訊。

要使用 collect.sh 指令碼從基於 Linux 的用戶端裝置下載診斷資訊：

1. 下載 collect.sh 指令碼，其封裝在 collect.tar.gz 壓縮檔案中。
2. 將下載的存檔複製到需要診斷的 Linux 用戶端裝置上。
3. 執行以下指令解壓 collect.tar.gz 存檔：

   ```
   # tar -xzf collect.tar.gz
   ```

4. 執行以下指令以指定指令碼執行權限：

   ```
   # chmod +x collect.sh
   ```

5. 使用具有管理員權限的帳戶執行 collect.sh 指令碼：

   ```
   # ./collect.sh
   ```

一個包含診斷資訊的檔案產生並被儲存到 /tmp/$HOST_NAME-collect.tar.gz 資料夾中。

管理用戶端裝置上的協力廠商應用程式和可執行檔

本區域旨在說明卡巴斯基安全管理中心 Linux 的功能如何管理用戶端裝置上的協力廠商應用程式與可執行檔執行。

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 Linux 作業系統，從 Kaspersky Endpoint Security 11.2 for Linux 開始提供應用程式控制元件。

先決條件

- 系統會將 卡巴斯基安全管理中心 Linux 佈署在您的組織中。
- Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Windows 的政策已建立並處於使用中狀態。政策中啟用了「應用程式控制」元件。

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。

   操作說明：取得並檢視儲存在用戶端裝置上的可執行檔清單

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。

   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 Linux 中，有三種類型的可執行檔類別：

- 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、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。

3. **在 Kaspersky Endpoint Security 政策設定應用程式控制**

   使用您在先前階段建立的類別，在 Kaspersky Endpoint Security for Linux 政策中設定「應用程式控制」元件。

   操作說明：在 Kaspersky Endpoint Security for Windows 政策中配置應用程式控制

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。

   操作說明：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。

如須應用程式控制的詳細資訊，請參閱 Kaspersky Endpoint Security for Linux 說明 和 Kaspersky Endpoint Security for Windows 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

對於 Kaspersky Endpoint Security for Linux，清查可執行檔的功能從 11.2 版本開始可用。

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。

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 **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**新工作設定**頁面的**應用程式**下拉清單中，根據用戶端裝置的作業系統選擇 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Windows。

4. 在**工作類型**下拉清單中，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。

如須清查工作的詳細描述，請參閱 Kaspersky Endpoint Security for Linux 說明 和 Kaspersky Endpoint Security for Windows 說明。

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**軟體管理→第三方應用程式→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**軟體管理→第三方應用程式→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**軟體管理→第三方應用程式→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**選取類別建立方法**步驟，指定應用程式類別名稱並選擇**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**」步驟中，執行以下操作：

   a. 選取要建立類別的規則類型：

   - **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。

   - **從儲存區選取憑證**

     如果選中此選項，則可以指定來自儲存區的憑證。類別條件僅符合指定憑證簽署的可執行檔。

     如果您建立並啟動了清查工作，或在 Kaspersky Endpoint Security 政策中選取了「**關於已啟動的應用程式**」核取方塊，則憑證將新增至儲存區。您可以同時執行兩項操作。

     > 只能從 PE 格式（.exe、.dll、.sys）的可執行檔擷取憑證資訊。

   - **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資料夾路徑。

   - **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**：

     - **從可執行檔清單選取**

       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取**

       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，您應該為此類別中的檔案選取卡巴斯基安全管理中心使用 Linux 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 for Linux 支援 SHA256 計算。

  為該類別中的檔案選取任意 卡巴斯基安全管理中心 Linux 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 for Linux，請選擇 **SHA256**核取方塊。
  - 僅當您使用 Kaspersky Endpoint Security for Windows 時才選擇**MD5 雜湊值**。Kaspersky Endpoint Security for Linux 不支援 MD5 雜湊函數。

  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區的憑證。類別條件僅符合指定憑證簽署的可執行檔。

  如果您建立並啟動了清查工作，或在 Kaspersky Endpoint Security 政策中選取了「**關於已啟動的應用程式**」核取方塊，則憑證將新增至儲存區。您可以同時執行兩項操作。

- **從封存資料夾**

  如果選擇此選項，您可以指定封存資料夾的檔案，然後選擇要使用哪個條件將應用程式新增到使用者類別。封存資料夾將被解壓縮，您選擇的條件將被套用於資料夾中的檔案。作為條件，您可以選取以下標準之一：

  - **檔案雜湊值**

    您選取要用於計算雜湊值的雜湊函數（MD5 或 SHA256）。和封存資料夾裡的檔案具有相同雜湊的應用程式被新增到自訂應用程式類別。

    僅當您使用 Kaspersky Endpoint Security for Windows 時才選擇 MD5 雜湊函數。Kaspersky Endpoint Security for Linux 不支援 MD5 雜湊函數。

  - **檔案內容**

    您選擇要用作標準的中繼資料。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。

- **憑證**

  您選擇要用作標準的憑證內容（憑證主旨、指紋或頒發者）。已用具有同樣內容的憑證簽章的可執行檔將被新增到使用者類別。

> 如果您想使用這些標準，必須在上傳檔案或存檔資料夾後手動指定**檔案內容**和**憑證**標準。

如果選擇此選項，您可以指定封存資料夾的檔案，然後選擇要使用哪個條件將應用程式新增到使用者類別。封存資料夾將被解壓縮，您選擇的條件將被套用於資料夾中的檔案。作為條件，您可以選取以下標準之一：

- **檔案雜湊值**

  您選取要用於計算雜湊值的雜湊函數（MD5 或 SHA256）。和封存資料夾裡的檔案具有相同雜湊的應用程式被新增到自訂應用程式類別。

  僅當您使用 Kaspersky Endpoint Security for Windows 時才選擇 MD5 雜湊函數。Kaspersky Endpoint Security for Linux 不支援 MD5 雜湊函數。

- **檔案內容**

  您選擇要用作標準的中繼資料。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。

- **憑證**

  您選擇要用作標準的憑證內容（憑證主旨、指紋或頒發者）。已用具有同樣內容的憑證簽章的可執行檔將被新增到使用者類別。

> 如果您想使用這些標準，必須在上傳檔案或存檔資料夾後手動指定**檔案內容**和**憑證**標準。

b. 如有必要，可在「**描述**」欄位中新增註解。符號數量不得超過 1000 個。

之後，可以開啟「應用程式類別內容」中的「**條件**」索引標籤，然後在「**條件標準**」欄中，點擊與要編輯或刪除其註解的條件連結，以編輯或刪除該註解。

> 選取「**從 KL 類別**」規則類型時，可以為所有將基於此規則類型建立的條件新增一條註解。可以單獨編輯或刪除每個條件的註解。

選取的準則會新增至條件清單。

可以為正在建立的應用程式類別新增所需的任意數量的條件。

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。

   如有必要，可以在「**描述**」欄位中新增註解。符號數量不得超過 1000 個。

   之後，可以開啟「**應用程式類別內容**」中的「排除」索引標籤，然後在「**條件標準**」欄中，點擊與要編輯或刪除其註解的條件連結，以編輯或刪除該註解。

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。

精靈完成後，應用程式類別即建立完成，並將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。

如須應用程式控制的詳細資訊，請參閱 Kaspersky Endpoint Security for Linux 說明 和 Kaspersky Endpoint Security for Windows 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，您可建立應用程式類別並在應用程式控制元件組態中加以使用。

請確保滿足以下先決條件：

- 在 Kaspersky Endpoint Security 政策中已啟用「應用程式控制」元件。
- 已取得受管理裝置上儲存的可執行檔的清單。

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. 在主功能表中，轉至**軟體管理** → **第三方應用程式** → **應用程式類別**。

   顯示包含可執行檔類別清單的頁面。

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**選取類別建立方法**步驟中，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應用程式類別的裝置。

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，您應該為此類別中的檔案選取卡巴斯基安全管理中心使用 Linux 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 for Linux 支援 SHA256 計算。

     為該類別中的檔案選取任意 卡巴斯基安全管理中心 Linux 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 for Linux，請選擇**SHA256**核取方塊。

     僅當您使用 Kaspersky Endpoint Security for Windows 時才選擇**MD5 雜湊值**。Kaspersky Endpoint Security for Linux 不支援 MD5 雜湊函數。

     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**軟體管理** → **第三方應用程式** → **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**選取類別建立方法**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 SHA256（在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本中支援）/ 為該類別中的檔案計算 MD5（在早於 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 的版本中支援）**

  取決於您網路裝置上安裝的安全應用程式版本，您應該為此類別中的檔案選取卡巴斯基安全管理中心使用 Linux 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 for Linux 支援 SHA256 計算。

  為該類別中的檔案選取任意 卡巴斯基安全管理中心 Linux 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 for Linux，請選擇**SHA256**核取方塊。

  僅當您使用 Kaspersky Endpoint Security for Windows 時才選擇**MD5 雜湊值**。Kaspersky Endpoint Security for Linux 不支援 MD5 雜湊函數。

  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」組態使用類別。

如須應用程式控制的詳細資訊，請參閱 Kaspersky Endpoint Security for Linux 說明 和 Kaspersky Endpoint Security for Windows 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**軟體管理 → 第三方應用程式 → 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。

新增事件相關的可執行檔到應用程式類別

當您在 Kaspersky Endpoint Security 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** → **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**指派到類別**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採取的名稱**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：

     - **新增為包含項目的規則**
     - **新增為排除項目的規則**

- 在**用作條件的參數**區段中，選擇以下選項之一：

  - **憑證詳情（如果檔案沒有憑證，則為 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（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 SHA256（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，僅適用於 Kaspersky Endpoint Security 10 Service Pack 1 版本）**

    > 僅當您使用 Kaspersky Endpoint Security for Windows 時才選擇此選項。Kaspersky Endpoint Security for Linux 不支援 MD5 雜湊函數。

    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。

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。

如須應用程式控制的詳細資訊，請參閱 Kaspersky Endpoint Security for Linux 說明 和 Kaspersky Endpoint Security for Windows 說明 。

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 **資產管理** → **政策**。

   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。切換切換按鈕**應用程式控制已停用**來停用該選項。

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。

如須應用程式控制的詳細資訊，請參閱 Kaspersky Endpoint Security for Linux 說明 和 Kaspersky Endpoint Security for Windows 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 Linux 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。

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→ 第三方應用程式 → 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。

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**列設定**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 **資產管理 → 資產（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。

如須應用程式控制的詳細資訊，請參閱 Kaspersky Endpoint Security for Linux 說明 和 Kaspersky Endpoint Security for Windows 說明 。

關於協力廠商應用程式

卡巴斯基安全管理中心 Linux 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 Linux 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 Linux 檢查是否可以更新第三方軟體 (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 Linux 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。

若要檢視可以使用卡巴斯基安全管理中心 Linux 更新的協力廠商軟體清單：

1. 在主功能表中，轉至 **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**新工作設定**步驟中，指定以下設定：
   a. 在**應用程式**下拉清單中，選取**卡巴斯基安全管理中心 Linux**。
   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**選取規則類型**步驟中，選取**第三方更新的規則**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 Linux 可讓您管理受管理裝置上安裝的協力廠商軟體的更新，並透過安裝所需的更新來修復此類軟體中的弱點。

卡巴斯基安全管理中心 Linux 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，管理伺服器會收到您在工作內容中指定的裝置上安裝之軟體中偵測到的弱點清單，以及所需的更新。在檢視有關可用更新的資訊後，您可以將它們安裝到您的裝置。

卡巴斯基安全管理中心 Linux 透過移除先前的應用程式版本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。

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*安裝所需更新並修復弱點*工作將更新安裝在用戶端裝置。

> 只有當您有弱點和修補程式管理功能的產品授權時，才可建立*安裝所需更新並修復弱點*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 Linux 會檢查更新是否符合更新規則中指定的標準。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。

情境：更新協力廠商軟體

本節提供更新安裝在用戶端裝置上的協力廠商軟體的情境。協力廠商軟體包含來自其他軟體供應商的應用程式。

先決條件

管理伺服器必須連接到網路才能安裝協力廠商軟體更新。

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 Linux 會收到您在工作內容中指定的裝置上安裝之軟體中偵測到的弱點清單，以及所需的更新。

   *弱點掃描和所需更新*工作會由管理伺服器快速啟動精靈自動建立。若您未執行該精靈，請*建立弱點掃描和所需更新工作*或立即執行快速啟動精靈。

   > 您只能為 Windows 裝置建立*弱點掃描和所需更新*工作。您無法為在其他作業系統上執行的裝置建立此工作。

2. **檢視已知更新清單**

   檢視有關可用協力廠商軟體更新的資訊並決定要安裝哪些更新。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。

3. **配置更新的安裝**

當卡巴斯基安全管理中心 Linux 收到協力廠商軟體更新清單時，您可藉由建立*安裝所需更新並修復弱點*工作，以在用戶端裝置安裝這些更新。

> 您只能為 Windows 裝置建立*安裝所需更新並修復弱點*工作。您無法為在其他作業系統上執行的裝置建立此工作。

*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產品授權時，才可建立 *安裝所需更新並修復弱點*工作。

若要安裝某些軟體更新，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。

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。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. **核准與拒絕協力廠商軟體更新（選用）**

若您建立的是*安裝所需更新並修復弱點*工作，您可在工作內容視窗中指定更新安裝規則。

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*、*已批准*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，以允許僅安裝有*已批准*狀態的更新。然後，將您想要安裝的這些更新手動設定為*已批准*狀態。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標準的特定更新設定*已批准*狀態。如果您手動核准大量更新，管理伺服器的效能會降低，這可能會導致管理伺服器過載。

預設情況下，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*已批准*或*已拒絕*。

有關更多詳細信息，請參閱有關核准和拒絕協力廠商軟體更新的說明。

6. **執行更新安裝工作**

啟動*安裝所需更新並修復弱點*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*成功完成*狀態。

7. **建立有關更新安裝結果的報告 (可選)**

若要檢視更新安裝的詳細統計，請建立第三方軟體更新安裝結果報告。

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 Linux 會檢查更新是否符合更新規則中指定的標準。系統會將符合條件的所有新更新在下次工作執行時安裝。

協力廠商軟體更新安裝選項

您可以透過建立並執行*安裝所需更新並修復弱點*工作，在受管理裝置上安裝協力廠商軟體更新和來自 Windows Update 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*安裝所需更新並修復弱點*工作。您可以使用此工作來安裝其他廠商軟體的更新。

> 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。

您可以建立工作，透過以下方式作為安裝所需更新的選擇：

- 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，並可避免您重複建立含有相同更新安裝清單的工作。

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. 使用下列路徑之一開啟更新清單：

   - **軟體管理→修補程式管理→軟體更新**。
   - **資產管理 → 資產（裝置）** → <裝置名稱> → **進階** → **可用更新**.
   - **軟體管理→第三方應用程式 → 應用程式登錄資料**→<應用程式名稱>→ **可用更新**。

   已顯示可用外掛程式清單。

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。如果未顯示此按鈕，請點擊省略符號按鈕，然後從下拉式清單中選取**安裝更新**。

   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。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。所選的更新會新增到工作內容。

  工作內容視窗隨即開啟。按一下**儲存**按鈕以儲存變更。

如果您選擇建立新工作，則會建立該新工作並顯示在**工作**的工作清單中。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，您必須啟動*安裝所需更新並修復弱點*工作。您可以透過點擊工作清單中的**開始**按鈕或在您啟動的工作的內容中指定排程設定來啟動此工作。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。

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**軟體管理→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*
   - *修復弱點*

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：

   - 若要啟動現有工作，請勾選*安裝所需更新並修復弱點*工作旁的複選框，然後點擊**開始**按鈕。

     該工作將在後台模式下完成。不需要進一步操作。

   - 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。

     > 如果選擇多個工作，**新增規則**按鈕將被停用。

     您無法為*修復弱點*工作新增規則。如果選擇*修復弱點*工作，則會顯示以下通知：*欲安裝更新，請使用「安裝所需更新並修復弱點」工作。*

b. 在精靈的**建立更新安裝規則**步驟中，設定新規則：

- **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。

  若所選更新的重要性等級為*未知*，則不會顯示此規則。

- **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。

  僅針對 Microsoft 軟體更新顯示此規則。若所選更新的重要性等級為*未知*，則不會顯示。

- **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 Linux 僅安裝由與所選更新相同之供應商提供的應用程式相關的更新。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。

  僅針對協力廠商軟體更新顯示此規則。

- **類型更新的安裝規則**

- **所選應用程式的更新的安裝規則**

  僅針對協力廠商軟體更新顯示此規則。

- **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。

- **安裝所選更新時，自動安裝所有必要的先前應用程式更新**

  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。

工作內容視窗隨即開啟。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。

- 要建立工作：

a. 點擊**新工作**按鈕。

b. 在精靈的**建立更新安裝規則**步驟中，設定新規則：

- **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。

  若所選更新的重要性等級為*未知*，則不會顯示此規則。

- **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。

  僅針對 Microsoft 軟體更新顯示此規則。若所選更新的重要性等級為*未知*，則不會顯示。

- **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 Linux 僅安裝由與所選更新相同之供應商提供的應用程式相關的更新。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。

  僅針對協力廠商軟體更新顯示此規則。

- **類型更新的安裝規則**

- **所選應用程式的更新的安裝規則**

  僅針對協力廠商軟體更新顯示此規則。

- **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。

- **安裝所選更新時，自動安裝所有必要的先前應用程式更新**

  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。

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。

「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 Linux 會使用有關適用 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。

- **連線更新伺服器以更新資料**

  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：

  - 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以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**連線更新伺服器以更新資料**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**連線更新伺服器以更新資料**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**，Kaspersky Security Center Linux 便不會請求任何更新資訊。

如果您的組織網路中使用了 WSUS 伺服器（本機 WSUS 伺服器），並且您希望將其與卡巴斯基安全管理中心管理伺服器一起使用，則必須先確保卡巴斯基安全管理中心管理伺服器未用作 WSUS 伺服器，然後執行下列操作：

1. 在執行 Windows 的受管理裝置上，為 Windows 更新伺服器服務指定本機 WSUS 伺服器。您可以在 Windows 登錄檔中手動執行此操作，也可以使用 Windows 群組原則執行此操作。

2. 在本機 WSUS 伺服器上，指定所需的更新分類以及要在其上分發更新的應用程式。

3. 將您的 WSUS 伺服器與上游伺服器同步（這可以是 Microsoft WSUS 伺服器，也可以是另一個本地上游 WSUS 伺服器）。

在裝置上執行*尋找弱點和所需更新*工作後，網路代理將使用 Windows 更新服務發起適用於該裝置的 Windows 更新請求。Windows 更新服務從登錄檔獲取外部 WSUS 伺服器的位址，並直接從該外部 WSUS 伺服器搜尋更新。然後，Windows 更新服務透過網路代理將此清單轉送到管理伺服器。因此，管理伺服器具有最新的庫。

- **搜尋卡巴斯基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 Linux 會在 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的所需更新（由非卡巴斯基和 Microsoft 的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 Linux 不會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 Linux 在此資料夾中搜尋需要修復弱點和安裝更新之協力廠商應用程式。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 Linux 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。這些檔案可供在遠端診斷公用程式中存取，您可以在該處下載或刪除這些檔案。

  如果停用該功能，網路代理將根據卡巴斯基安全管理中心 Linux 遠端診斷實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**執行錯過的工作**與**使用工作啟動自動隨機化延遲**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「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 Linux 會收到已偵測弱點清單，與安裝在受管理裝置上的協力廠商軟體的所需更新清單。

> 您只能為 Windows 裝置建立*弱點掃描和所需更新*工作。您無法為在其他作業系統上執行的裝置建立此工作。

*弱點掃描和所需更新*工作會在快速啟動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 **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**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. 選取要將工作分配到的裝置。
6. 指定掃描弱點和需要更新的應用程式之方法：

   - **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 Linux 會使用有關適用 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。

- **連線更新伺服器以更新資料**

  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：

  - 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以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**連線更新伺服器以更新資料**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**連線更新伺服器以更新資料**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**，Kaspersky Security Center Linux 便不會請求任何更新資訊。

  如果您的組織網路中使用了 WSUS 伺服器（本機 WSUS 伺服器），並且您希望將其與卡巴斯基安全管理中心管理伺服器一起使用，則必須先確保卡巴斯基安全管理中心管理伺服器未用作 WSUS 伺服器，然後執行下列操作：

  1. 在執行 Windows 的受管理裝置上，為 Windows 更新伺服器服務指定本機 WSUS 伺服器。您可以在 Windows 登錄檔中手動執行此操作，也可以使用 Windows 群組原則執行此操作。
  2. 在本機 WSUS 伺服器上，指定所需的更新分類以及要在其上分發更新的應用程式。
  3. 將您的 WSUS 伺服器與上游伺服器同步（這可以是 Microsoft WSUS 伺服器，也可以是另一個本地上游 WSUS 伺服器）。

  在裝置上執行*尋找弱點和所需更新*工作後，網路代理將使用 Windows 更新服務發起適用於該裝置的 Windows 更新請求。Windows 更新服務從登錄檔獲取外部 WSUS 伺服器的位址，並直接從該外部 WSUS 伺服器搜尋更新。然後，Windows 更新服務透過網路代理將此清單轉送到管理伺服器。因此，管理伺服器具有最新的庫。

- **搜尋卡巴斯基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 Linux 會在 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的所需更新（由非卡巴斯基和 Microsoft 的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 Linux 不會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。

您可以在建立工作後在工作內容視窗的**應用程式設定**頁籤上停用這些選項。

7. **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 Linux 在此資料夾中搜尋需要修復弱點和安裝更新之協力廠商應用程式。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。

   您可以在建立工作後在工作內容視窗的**應用程式設定**頁籤上變更指定的路徑。

8. 如果需要，**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 Linux 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。這些檔案可供在遠端診斷公用程式中存取，您可以在該處下載或刪除這些檔案。

   如果停用該功能，網路代理將根據卡巴斯基安全管理中心 Linux 遠端診斷實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。

   您可以在建立工作後在工作內容視窗的**應用程式設定**頁籤上停用此選項。

9. 指定**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。

   如果您在上一個步驟中啟用了進階診斷，則必須指定此值。您可以在建立工作後在工作內容視窗的**應用程式設定**頁籤上變更此值。

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。

    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。

工作被建立和配置。若要執行工作，請在工作清單選取該工作，並點擊**開始**按鈕。

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**執行錯過的工作**與**使用工作啟動自動隨機化延遲**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。

您也可以安排*弱點掃描和所需更新*工作在特定時間啟動。例如，您可以從工作內容視窗的**每 N 小時**頁籤上的**開始工作**下拉式功能表中選擇**排程**排程開始。在這種情況下，請注意，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時執行。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。您必須根據組織採用的工作規則為該工作設定最方便的排程。

如需排程啟動設定的詳細說明，請參閱一般工作設定。

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上的協力廠商應用程式的可用更新清單，

在主功能表中，轉至**軟體管理→修補程式管理→軟體更新**。

可用更新清單隨即顯示。

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）
     - 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

- **屬性**

  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。點擊狀態會開啟具有所選狀態的裝置清單。

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。

檢視選取的受管理裝置上安裝的協力廠商軟體可用更新清單：

1. 在主功能表中，轉至 **資產管理 → 資產（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**區域。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 (包含 Microsoft 軟體) 更新清單為 CSV 或 TXT 檔案格式。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**。

   可用更新清單隨即顯示。

   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。

   如果您只想匯出特定更新，請選取清單中所需更新旁邊的核取方塊。

2. 點擊**匯出到 TXT** 或**匯出到 CSV** 按鈕，視您偏好的匯出格式而定。如果未顯示這些按鈕中的任何一個按鈕，請點選省略符號按鈕，然後從下拉式清單中選取需要的選項。

包含協力廠商軟體 (包括 Microsoft 軟體) 可用更新清單的檔案將下載到您目前的裝置。

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。

   可用更新清單隨即顯示。

   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。

   如果您只想匯出特定更新，請選取清單中所需更新旁邊的核取方塊。

   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。

2. 點擊**匯出到 TXT** 或**匯出到 CSV** 按鈕，視您偏好的匯出格式而定。如果未顯示這些按鈕中的任何一個按鈕，請點選省略符號按鈕，然後從下拉式清單中選取需要的選項。

包含所選受管理裝置上安裝之協力廠商軟體 (包含 Microsoft 軟體) 可用的更新清單的檔案，將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*工作內容中配置的規則。建議您僅為那些不符合規則中標準的更新設定*已批准*狀態。當您手動核准大量更新時，管理伺服器的效能會降低，這可能會導致管理伺服器過載。

要批准或拒絕一個或幾個更新：

1. 在主功能表中，轉至 **軟體管理→修補程式管理 →軟體更新**。

   可用更新清單隨即顯示。

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。如果未顯示這些按鈕中的任何一個按鈕，請點選省略符號按鈕，然後從下拉式清單中選取需要的選項。

   更新的預設狀態是*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**軟體管理→修補程式管理→軟體更新**。

   可用更新清單隨即顯示。

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**區域，於**更新核准狀態**下拉式清單中選取更新狀態。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，則這些更新不會安裝在已計畫但未安裝的裝置上。更新將保持在已將其安裝的裝置上。如果需要，您可以在本機手動刪除它們。

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安裝在受管理裝置上協力廠商軟體中的弱點。此工作可讓您根據工作設定中指定的規則，安裝多個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 **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**下拉清單中，選擇卡巴斯基安全管理中心。
4. 在**工作類型**清單中，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*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. 在精靈的**指定安裝更新規則** 步驟，新增更新安裝規則。

   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。對於具有規則的操作的資訊，請參閱更新安裝規則。

   這些規則被套用到用戶端裝置上的更新安裝。如果您不指定任何規則，則該工作無需執行任何操作。
8. 指定下列設定：

   - **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**下載更新到**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。

  - **下載更新到**

    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 Linux 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。這些檔案可供在遠端診斷公用程式中存取，您可以在該處下載或刪除這些檔案。

  如果停用該功能，網路代理將根據卡巴斯基安全管理中心 Linux 遠端診斷實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。

轉到精靈的下一個步驟。

9. 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。

- **提示使用者動作**

  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。

- **強制關閉封鎖工作階段中應用程式前的等待時間（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。

10. 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。

11. 點擊**完成**按鈕。

    新工作精靈即會建立工作。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。

12. 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，將安裝所需的更新並修復弱點。

如果您的組織網路中使用了 WSUS 伺服器（本機 WSUS 伺服器），並且您希望將其與卡巴斯基安全管理中心管理伺服器一起使用，則必須先確保卡巴斯基安全管理中心管理伺服器未用作 WSUS 伺服器，然後執行下列操作：

a. 在執行 Windows 的受管理裝置上，為 Windows 更新伺服器服務指定本機 WSUS 伺服器。您可以在 Windows 登錄檔中手動執行此操作，也可以使用 Windows 群組原則執行此操作。

b. 在本機 WSUS 伺服器上，指定所需的更新分類以及要在其上分發更新的應用程式。

c. 將您的 WSUS 伺服器與上游伺服器同步（這可以是 Microsoft WSUS 伺服器，也可以是另一個本地上游 WSUS 伺服器）。

在裝置上執行*安裝所需更新和修復弱點*工作後，網路代理使用 Windows 更新服務安裝 Windows 更新。Windows 更新服務從登錄檔獲取外部 WSUS 伺服器的位址，並直接從該外部伺服器下載更新。

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為所有更新建立規則、為 Windows Update 中的更新建立規則，或為協力廠商應用程式（由非卡巴斯基和 Microsoft 軟體供應商製作的應用程式）更新建立規則而定。當新增 Windows Update 更新或協力廠商應用程式的更新規則時，您可以選取您要為其安裝更新的特定應用程式和應用程式版本。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：

- 透過在建立新的*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*工作內容視窗的**應用程式設定**頁籤上新增規則。
- 透過更新安裝精靈或弱點修復精靈。

為所有更新增設規則

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. 在精靈的**選取規則類型**步驟中，選擇**所有更新的規則**。

3. 在精靈的**一般標準**步驟中，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）**。這會安裝帶有*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。

轉到精靈的下一個步驟。

4. 選取要安裝的更新：

- **安裝所有合適的更新**

  安裝滿足在精靈**一般標準**步驟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。

  - **安裝所選更新時，自動安裝所有必要的先前應用程式更新**

    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。

轉到精靈的下一個步驟。

5. 選取將由安裝所選更新而修復的弱點：

- **修復所有符合其他標準的弱點**

  修復滿足在精靈**一般標準**步驟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。

轉到精靈的下一個步驟。

6. 指定您要新增的規則名稱。您可以稍後在所建立工作的內容視窗的**應用程式設定**頁籤變更該名稱。

新規則已建立、設定並顯示在新工作精靈的規則表中。

為 Windows Update 中的更新新增規則

為 Windows Update 中的更新新增規則：

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. 選擇 **Windows Update 的規則**。

   轉到精靈的下一個步驟。

3. 在精靈的**一般標準**步驟中，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）**。這會安裝帶有*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。

為協力廠商應用程式的更新新增規則

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. 在精靈的**選取規則類型**步驟中，選擇**第三方更新的規則**。

3. 在精靈的**一般標準**步驟中，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）**。這會安裝帶有*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。

   轉到精靈的下一個步驟。

4. 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。

   轉到精靈的下一個步驟。

5. 指定您要新增的規則名稱。您可以稍後在所建立工作的內容視窗的**應用程式設定**頁籤變更該名稱。

新規則已建立、設定並顯示在新工作精靈的規則表中。

建立工作後安裝所需更新和弱點修復工作之設定

建立*安裝所需更新並修復弱點*工作後，您可以在工作內容視窗的**應用程式設定**頁籤上指定以下設定：

- 在**測試安裝**區域：
  - **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更新測試安裝的裝置。
  - **在指定群組中的裝置上執行掃描**。如果要在一組裝置上測試更新安裝，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**。如果要在一部份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。

  選取除**不掃描**以外的任意選項時，在**決定是否繼續進行安裝的所需時間（小時）**欄位中指定從更新測試安裝到開始將更新安裝到所有裝置上必須間隔的時數。
- 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。

如需工作設定的詳細說明，請參閱一般工作設定。

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援自動更新功能。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，此設定不會以更新核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*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 **軟體管理 → 第三方應用程式→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**欄和**管理自動更新**欄篩選清單。

   應用程式屬性視窗隨即開啟。
3. 在**一般**區域中，為以下功能選取一個值：

   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 Linux 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*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 Linux 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*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。

修復協力廠商軟體弱點

本節說明卡巴斯基安全管理中心 Linux 中與修復受管理裝置上安裝的軟體之弱點相關的功能。

關於尋找與修復軟體弱點

卡巴斯基安全管理中心 Linux 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 Linux 會使用來自已知弱點資料庫的特徵。該資料庫由卡巴斯基專家建立並保持更新。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。您可以在卡巴斯基網站上搜尋軟體弱點詳情。

卡巴斯基安全管理中心 Linux 會使用*弱點掃描和所需更新*工作尋找軟體弱點。

修復軟體弱點

為了修復軟體弱點，卡巴斯基安全管理中心 Linux 會使用由軟體供應商提供的軟體更新。作為執行將更新下載至管理伺服器儲存區工作的結果，軟體更新的元數據將被下載到管理伺服器儲存區。此工作是為了下載卡巴斯基與協力廠商軟體更新之中繼資料。該工作由卡巴斯基安全管理中心 Linux 快速啟動精靈自動建立。您也能手動*建立將更新下載至管理伺服器儲存區工作*。

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 Linux 產品授權，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 Linux 產品授權，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。

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 Linux 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。
  - 修復非 Microsoft 軟體的協力廠商軟體中的弱點。

階段

用以下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**

   若要在受管理裝置上安裝的軟體中尋找弱點，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 Linux 會收到偵測到的弱點清單，以及您在工作內容中指定的裝置上安裝的軟體需要的更新。

*弱點掃描和所需更新*工作會由卡巴斯基安全管理中心 Linux 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。

> 您只能為 Windows 裝置建立*弱點掃描和所需更新*工作。您無法為在其他作業系統上執行的裝置建立此工作。

2. **檢視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。對於清單中的各個弱點，您也可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，您必須手動指定對工作設定中列出之協力廠商軟體弱點的使用者修復項目。*修復弱點*工作會使用適用於 Microsoft 軟體的建議修復項目和適用於協力廠商軟體的使用者修復項目。

   > 您可以僅為 Windows 裝置建立*安裝所需更新並修復弱點*工作和*修復弱點*工作。您無法為在其他作業系統上執行的裝置建立這些工作。

   您可啟動修復弱點精靈，精靈會自動建立以下其中一個這類工作或您可手動建立其中一個這類工作。

   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，系統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。符合規則中標準的所有軟體更新都將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，則僅 Microsoft 軟體中的弱點會被修復。

4. **排程工作**

   排程*弱點掃描和所需更新*工作定期自動執行，以保持弱點清單最新。建議頻率為每週一次。

   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，請確保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）**

   您可在所有受管理裝置或僅在選取的受管理裝置中忽略軟體弱點。

6. **執行修復弱點工作**

   啟動*安裝所需更新並修復弱點*或*修復弱點*工作。工作完成時，請確保工作清單的工作為*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。報告會顯示未修復軟體弱點的資訊。它允許您識別和解決組織中使用的協力廠商軟體（包括 Microsoft 軟體）中的弱點。

8. **檢查用於尋找與修復協力廠商軟體弱點的配置**

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。
- 如果需要，可以忽略某些軟體弱點。
- 設定修復弱點的工作。
- 排程尋找並修復軟體弱點的工作，以便其依序啟動。
- 檢查修復軟體弱點工作是否已啟動。

修復協力廠商軟體弱點

若要尋找協力廠商軟體弱點，您可以建立並執行*弱點掃描和所需更新*工作並接收軟體弱點清單。取得軟體弱點清單後，您可在受管理的 Windows 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作業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，並為您省去繁雜的工作建立操作。

使用弱點清單修復軟體弱點

使用弱點清單修復軟體弱點：

1. 透過執行下列操作之一開啟弱點清單：

   - 在主功能表中，轉至**軟體管理→修補程式管理→軟體弱點**。
   - 在主功能表中，轉至**資產管理→ 資產（裝置）** → <裝置名稱> → **進階** → **軟體弱點**。
   - 在主功能表中，轉至**軟體管理→第三方應用程式→應用程式登錄資料**→ <應用程式名稱>→**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. 在弱點清單中，選取欲修復弱點旁的複選框，然後點擊**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管理產品授權，則會預先選取安裝所需更新並修復弱點工作。如果您沒有產品授權，則會預先選取修復弱點工作。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。如果您擁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。所選弱點已新增到工作內容中。

     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，則會建立該工作並顯示在 **工作** 的工作清單中。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，您需手動指定工作設定中列出的軟體弱點。

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**軟體管理→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表格隨即顯示。

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。

   > 如果您選擇多個弱點，該按鈕將被停用。

   弱點修復精靈啟動。現有工作清單隨即顯示。清單可能含有以下工作類型：

   - 安裝所需更新並修復弱點
   - 修復弱點

   不能修改修復弱點工作以安裝新更新。要安裝新更新，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. 執行以下操作之一：

- 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。

  不需要進一步操作。可以關閉精靈。該工作將在後台模式下完成。

- 對現有安裝所需更新並修復弱點工作新增規則：

  a. 選取工作名稱旁邊的核取方塊，然後點擊**新增規則**按鈕。

  > 如果選擇多個工作，**新增規則**按鈕將被停用。

  您無法為修復弱點工作新增規則。如果選擇一個修復弱點工作，則會顯示以下通知：「欲安裝更新，請使用『安裝所需更新並修復弱點』工作。」

  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。

  - **透過使用其類型與建議用於所選弱點之更新相同的更新來修復弱點的規則**

    僅針對 Microsoft 軟體弱點顯示此規則。

  - **修復所選供應商應用程式中的弱點規則**

    僅針對協力廠商軟體弱點顯示此規則。

  - **修復所選應用程式的所有版本中的弱點的規則**

    僅針對協力廠商軟體弱點顯示此規則。

  - **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。

  工作內容視窗隨即開啟。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。

- 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。

  - **透過使用其類型與建議用於所選弱點之更新相同的更新來修復弱點的規則**

    僅針對 Microsoft 軟體弱點顯示此規則。

  - **修復所選供應商應用程式中的弱點規則**

    僅針對協力廠商軟體弱點顯示此規則。

  - **修復所選應用程式的所有版本中的弱點的規則**

    僅針對協力廠商軟體弱點顯示此規則。

  - **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。

  d. 在新工作精靈中繼續建立工作。

  您在修復弱點精靈中新增的規則將顯示在新工作精靈的**指定安裝更新規則**步驟中。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。

> 您只能為 Windows 裝置建立*修復弱點*工作。您無法為在其他作業系統上執行的裝置建立此工作。

只有當您擁有*弱點和修補程式管理產品授權*時，才可以建立新的修復弱點工作。

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 **工作**。

   > 或者，您可以在裝置內容視窗的**工作**頁籤上建立此工作。

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**下拉清單中，選擇卡巴斯基安全管理中心。

4. 在**工作類型**清單中，選擇**修復弱點**工作類型。

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。

   轉到精靈的下一個步驟。

7. 點擊**新增**按鈕。

   更新清單隨即開啟。

8. 在弱點清單中，選取欲修復弱點旁的複選框，然後點擊**確定**按鈕。

   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。

   轉到精靈的下一個步驟。

9. 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。

- **提示使用者動作**

  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。

- **強制關閉被封鎖工作階段中的應用程式**

  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。

轉到精靈的下一個步驟。

10. 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。

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，工作使用預設設定建立。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。

工作隨即建立、設定，並顯示在**工作**的工作清單中。

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，選定的弱點將被修復。

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和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以修復弱點的軟體更新。

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**軟體管理→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. 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。

   所選弱點的內容視窗開啟。

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. 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對應於**軟體管理→安裝套件**。

   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，您可點擊**新增**按鈕，並啟動新套件精靈以立即建立套件。

5. 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**儲存**按鈕。

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。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

掃描受管理裝置上安裝的軟體之弱點後，您可檢視偵測出的軟體弱點的清單。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。

您也可以產生並檢視弱點報告。

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**。

在用戶端裝置上偵測到的軟體弱點清單隨即顯示。

若要調整軟體弱點列表，

點擊軟體弱點清單右上角的**篩選器**圖示 ( ) 並選擇需要的篩選條件。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 **資產管理 → 資產（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. 選取弱點旁邊的核取方塊。
3. 點擊**裝置弱點統計資訊**按鈕。

   > 如果您選擇多個弱點，則**裝置弱點統計資訊**按鈕將被停用。

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。您可以將這些檔案傳送給您的資訊安全經理或將其依統計目的儲存。

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**。

   受管理裝置上偵測到的應用程式中的軟體弱點清單隨即顯示。

   預設情況下，僅匯出目前頁面顯示的弱點。

   如果您只想匯出特定弱點，請選取這些弱點旁的核取方塊。

2. 點擊**匯出到 TXT** 或**匯出到 CSV** 按鈕，視您偏好的匯出格式而定。如果未顯示這些按鈕中的任何一個按鈕，請點擊省略符號按鈕，然後從下拉式清單中選取需要的選項。

包含軟體弱點清單的檔案將下載到您的裝置。

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 **資產管理 → 資產（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。

預設情況下，僅匯出目前頁面顯示的弱點。

如果您只想匯出特定弱點，請選取這些弱點旁的核取方塊。

1. 點擊**匯出到 TXT** 或**匯出到 CSV** 按鈕，視您偏好的匯出格式而定。如果未顯示這些按鈕中的任何一個按鈕，請點擊省略符號按鈕，然後從下拉式清單中選取需要的選項。

包含軟體弱點清單的檔案將下載到您的裝置。

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**。
   受管理裝置上偵測到的應用程式中的軟體弱點清單隨即顯示。

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。

在選取的受管理裝置上忽略軟體弱點：

1. 在主功能表中，轉至**資產管理 → 資產（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。

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可讓您使用安裝套件來遠端安裝協力廠商應用程式。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*將更新下載至管理伺服器儲存區*工作時，系統會自動建立資料庫。

> 只有當您擁有弱點和修補程式管理產品授權時，才可以從卡巴斯基資料庫建立協力廠商應用程式的安裝套件。

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**軟體管理→安裝套件**。
2. 點擊**新增**按鈕。
   新套件精靈啟動。使用**下一步**按鈕進行精靈。
3. 選擇**從卡巴斯基資料庫中選取一個應用程式來建立安裝套件**選項。

   > 此選項僅在有弱點和修補程式管理產品授權下才可使用。

轉到精靈的下一個步驟。

4. 選取您要為其建立安裝套件的應用程式。
   轉到精靈的下一個步驟。

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安裝產品授權協議，請在精靈的**產品授權協議和隱私政策**步驟中執行以下操作：

   a. 點擊**顯示**連結以閱讀供應商網站上的產品授權協議或檢視產品授權更新。

   b. 選擇**本人確認已完整閱讀、理解並接受本《最終使用者產品授權協議》的條款和條件**之核取方塊。

   c. 點擊**全部接受**按鈕接受清單中顯示的所有產品授權協議和隱私權政策。

7. 在精靈的 **新安裝套件的名稱**步驟中的**套件名稱**欄位，輸入安裝套件的名稱，然後點擊**下一步**。
   新建立的安裝套件將上傳到管理伺服器。新套件精靈會顯示一則訊息，通知您安裝套件已成功建立。

8. 點擊**完成**按鈕。

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。

只有當您擁有弱點和修補程式管理產品授權時，您才可以使用卡巴斯基資料庫中的協力廠商應用程式安裝套件來建立和重新設定*遠端安裝應用程式*工作。

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。

從卡巴斯基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**軟體管理→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。
   內容視窗隨即開啟。

3. 如有必要，請修改設定。

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，並不會顯示下列所有設定。您可以透過點擊**篩選器**按鈕來新增所需的列，然後從清單中選擇相關的列名稱。

- **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。
  - 顯示更新內容並包含以下各列的表格：
    - **名稱**

      更新的名稱。

- **描述**

  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。

- **修補程式重要性等級**

  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（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。

- **更新審批狀態**

  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 描述**

  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。

- **建立日期**

- **設定**頁籤，其中顯示安裝套件設定及其在安裝過程中用來作為命令行參數的名稱、描述和值。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。

- **變更歷史**頁籤，其中顯示安裝套件修訂版號並包含以下各欄：

  - **修訂** — 安裝套件的修訂編號。

  - **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。

  - **使用者裝置 IP 位址** — 從中修改物件之裝置的 IP 位址。

  - **網頁主控台 IP 位址** — 用於修改物件的卡巴斯基安全管理中心網頁主控台的 IP 位址。

  - **動作** — 對修訂中的安裝套件執行的操作。

  - **描述** — 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。

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。透過使用可存取網際網路的管理伺服器，您將能夠下載修補程式 (所需的更新)，然後將其傳輸到隔離管理伺服器。

> 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。

請參閱此處理程序的說明和方案，以了解隔離網路中修復弱點的過程如何運行。

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. 在以下裝置上安裝卡巴斯基安全管理中心 Linux (不早於版本 15.1)：
   - 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**

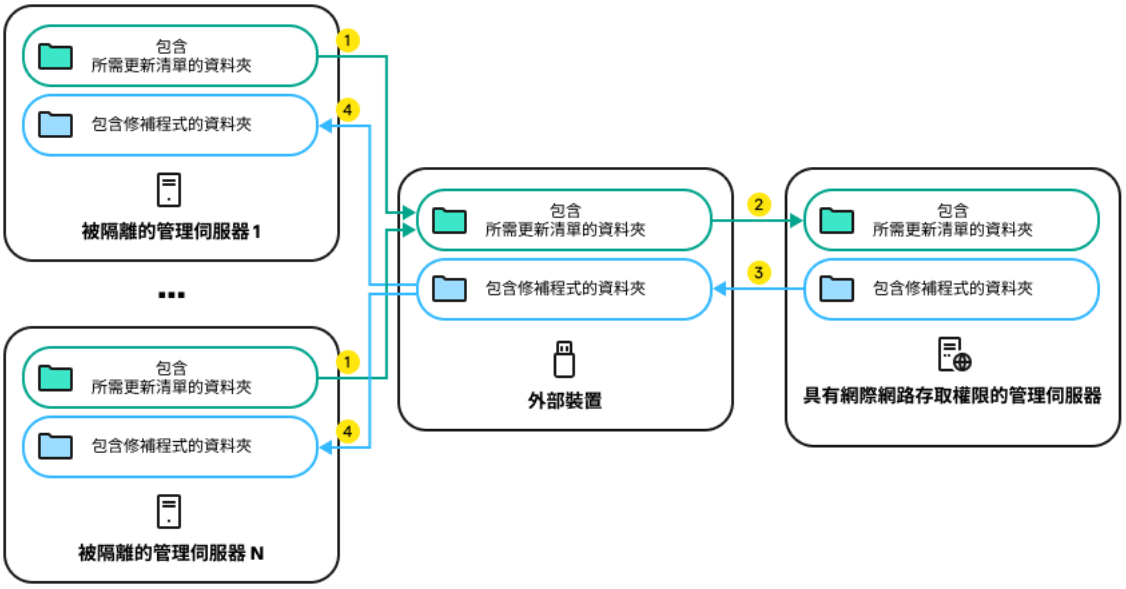
   完成管理伺服器設定後，您可以在具有網際網路存取權限的管理伺服器和隔離管理伺服器之間傳輸所需的更新清單和修補程式。接下來，修補程式的更新將透過使用*安裝所需更新並修復弱點*工作安裝在受管理裝置上。

結果

因此，協力廠商軟體更新將被傳輸到隔離管理伺服器並使用卡巴斯基安全管理中心 Linux 安裝在連接的受管理裝置上。管理伺服器設定一次即可，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

修復隔離網路中協力廠商軟體弱點的過程如下圖所示。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管理伺服器（以下稱為隔離管理伺服器）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理裝置上。此更新清單作為一組二進位檔案儲存在特定資料夾中，每個檔案均以包含必要更新的修補程式 ID 命名。因此，清單中的每個檔案都對應一個特定的修補程式。

由外部裝置將必要更新由被隔離管理伺服器傳輸到具有網際網路存取權限的指定管理伺服器之清單。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設定的資料夾中。

當所有修補程式已下載並放置在指定資料夾中時，它們將回傳每個隔離管理伺服器，並從中取得所需更新的清單。這些修補程式保存在每個獨立管理伺服器上專門為其建立的資料夾中。

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理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，首先需要設定可以存取網際網路的管理伺服器，然後設定隔離管理伺服器。

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

   您可以根據需要重新命名這些資料夾。

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 群組。

3. 使用 klscflag 實用程式將路徑寫入管理伺服器內容中的資料夾。

   執行命令行，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目錄中。預設安裝路徑為/opt/kaspersky/ksc64/sbin。

4. 在命令行中執行以下命令：

   - 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>"`

   範例：`klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "/FolderForPatches"`

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。

   範例：`klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 120`

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隔離管理伺服器。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

完成設定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。

若要設定隔離管理伺服器，請針對每個管理伺服器執行下列步驟：

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

   您可以根據需要重新命名這些資料夾。

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 群組。

4. 使用 klscflag 實用程式將路徑寫入管理伺服器內容中的資料夾。

   執行命令行，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目錄中。預設安裝路徑為/opt/kaspersky/ksc64/sbin。

5. 在命令行中執行以下命令：

   - 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>"`

   範例：`klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "/FolderForPatches"`

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。

   範例：`klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 120`

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 Linux 不計算修補程式的 SHA256 雜湊。如果啟用此選項，則在隔離管理伺服器收到修補程式後，卡巴斯基安全管理中心 Linux 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。

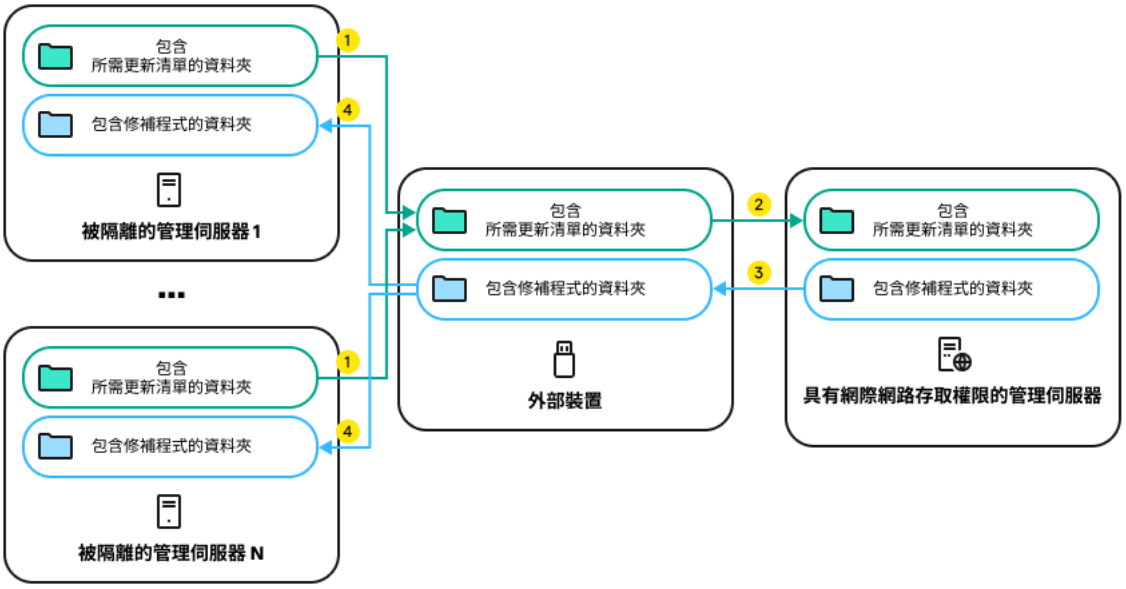
設定完所有管理伺服器後，您可以傳輸修補程式和所需更新清單，並修復隔離網路中受管理裝置上的協力廠商軟體弱點。

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下圖所示：



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。您可以為這些資料夾指定任何您想要的名稱。

   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。這在只需少量修補程式的前提下會比較方便。

   - 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，則會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，更新安裝在受管理裝置上，且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。

禁用在隔離網路中傳輸修補程式和安裝更新

您可以禁用傳輸修補程式到隔離管理伺服器；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。

禁用傳輸修補程式到隔離管理伺服器：

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內容中，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。

   執行命令行，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目錄中。預設安裝路徑為/opt/kaspersky/ksc64/sbin。

   在命令行中執行以下命令：

   - 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. 如果您刪除了資料夾的路徑，請在具有網路存取權限的管理伺服器上重新啟動服務。

3. 在要解除每個隔離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。

   在具有 root 權限的帳戶下在命令列中執行以下命令：

   - 若要刪除修補程式資料夾的路徑：
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_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之服務。

如果您重新設定管理伺服器以存取網路，修補程式將不再透過卡巴斯基安全管理中心 Linux 傳輸。

如果您僅重新設定特定管理伺服器並將其從隔離網路中刪除，它們將不再透過卡巴斯基安全管理中心 Linux 接收修補程式。只有那些保留在隔離網路內的管理伺服器才會繼續接收修補程式。

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。

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手動處理的工作。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。透過使用 OpenAPI，您可以開發用戶端應用程式。

您可以使用螢幕右側的搜尋欄位，在《OpenAPI 參考手冊》中找出您所需的資訊。

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 Linux 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，

從安裝了管理伺服器的裝置上的 KlAkOAPI.tar.gz 存檔安裝 KlAkOAPI 套件。

KlAkOAPI 套件包含一組執行典型操作的範例。您只能在安裝了管理伺服器和 KlAkOAPI 套件的裝置上呼叫 OpenAPI 方法、執行範例和您自己的指令碼。包含此套件的 KlAkOAPI.tar.gz 壓縮檔案位於卡巴斯基安全管理中心 Linux 安裝資料夾中。

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」層次結構	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次結構的連線。	建立管理伺服器的層次結構，新增從屬管理伺服器，刪除管理伺服器的層次結構
透過連線閘道下載網路清單檔案到指定主機	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
啟動裝置工作	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

樣本	樣本目的	情景
為群組中的裝置註冊發佈點	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 • 在群組層次結構中移動 • 獲取完整的、擴展的群組層次結構及其名稱和巢狀結構	設定管理伺服器
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。	管理工作
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。	新增內部使用者帳戶
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。	管理使用者和使用者角色
建立內部使用者，建立並透過電子郵件傳送 Android 安裝套件	您可以使用SecurityPolicy 類別建立內部用戶，建立一個 Android 安裝套件，並透過電子郵件將其傳送給使用者。	新增內部使用者帳戶

透過 OpenAPI 與 卡巴斯基安全管理中心 Linux 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 Linux 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 Linux 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 Linux 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 Linux 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。

計劃 卡巴斯基安全管理中心 Linux 佈署

當在組織網路中排程卡巴斯基安全管理中心 Linux 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 50,000 台裝置。如果組織網路中的裝置總數超過 50,000，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，用於使用卡巴斯基安全管理中心網頁主控台工具發佈獨立套件
- 8060 TCP—HTTP 連接埠，用於使用卡巴斯基安全管理中心網頁主控台工具發佈獨立套件
- 13292 TCP—TLS 連接埠，僅在有需要被管理的行動裝置時需要
- 8080 TCP—HTTPS 連接埠，用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 Linux 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 50,000 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**選項）。如果發佈點總數不超過 300 則持續連線模式可用。

MSP 用戶端可能想要管理員工的 Android 和 iOS 裝置。管理伺服器透過 TLS、TCP 連接埠 13292 管理行動裝置。

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
- 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

一些用戶端公司，例如MSP，可能執行多台管理伺服器。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。在階層結構中，基於 Linux 的管理伺服器既可以作為主伺服器也可以作為從屬伺服器。基於 Linux 的主伺服器可以管理基於 Linux 和基於 Windows 的從屬伺服器。基於 Windows 的主伺服器可以管理基於 Linux 的次要伺服器。

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、工作、使用者角色和安裝套件，從而防止重複設定。
- 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）。
- 主管理伺服器可作為從屬管理伺服器的更新來源。

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。

管理伺服器的層次結構為多組織用戶模式提供支援。此模式允許主管理員獨立地集中管理多個用戶端。每個用戶端組織或辦公室都與其他用戶端組織或辦公室隔離，被稱為租用戶。您可以將多個受管理裝置及其相關資料、設定、政策和工作指派給一個租用戶，並按租用戶配置使用者權限。

安裝在主要組織基礎結構中的主管理伺服器可充當主要租用戶。主管理伺服器使從屬或虛擬管理伺服器（其獨立的租用戶）能夠獨立接收和處理自己的事件並使用自己的資源、服務和配置。

擁有多個用戶端組織的服務提供商可以向每個用戶端組織獨立提供卡巴斯基安全管理中心 Linux 功能，包括警示聚合和回應操作。為了實現這一點，服務提供商將從屬或虛擬管理伺服器作為每個用戶端組織的租用戶進行連線。服務提供商利用自己的人員和資源提供服務。

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。

佈署和初始化設定

卡巴斯基安全管理中心 Linux 是一個分發的應用程式。卡巴斯基安全管理中心 Linux 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。
- 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 Linux 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
- 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

在故障移轉叢集上開始部署卡巴斯基安全管理中心 Linux之前，您必須為卡巴斯基安全管理中心 Linux 服務建立帳戶。

為此，在主動節點、被動節點和檔案伺服器上執行以下步驟：

1. 建立一個名為“kladmins”的群組，並為所有三個群組分配相同的 GID。
2. 建立一個名為“ksc”的網域群組，並為所有三個使用者帳戶分配相同的 UID。將已建立帳戶的主要群組設定為「kladmins」。
3. 建立一個名為“rightless”的網域群組，並為所有三個使用者帳戶分配相同的 UID。將已建立帳戶的主要群組設定為「kladmins」。

選取 DBMS

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
MySQL（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。
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。
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，請使用此 DBMS。
Tantor（檢視受支援的版本）	如果您打算為少於 50,000 台裝置執行單個管理伺服器，請使用此 DBMS。 Tantor DBMS 僅支援在 Astra Linux Special Edition RUSB.10015-01（操作更新 1.8）上執行。

對於如何安裝所選 DBMS 的資訊，請參考其文件。

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式的通知。

> 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。

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

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週期。

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。

指定管理伺服器位址

當安裝管理伺服器時，您必須指定 DNS 名稱或者管理伺服器的靜態 IP 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，您將可以透過使用卡巴斯基安全管理中心網頁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。

維護閒置連線

我們建議您在連線閘道裝置上設定以下 keepalive 參數，以提高連線穩定性：

- `net.ipv4.tcp_keepalive_intvl` 可指定在發送第一條 keepalive 訊息後，後續訊息的發送頻率。將此參數設定為 `1`。
- `net.ipv4.tcp_keepalive_probes` 可指定在判定連線失效前，允許發送的無回應 keepalive 訊息數量。將此參數設定為 `10`。
- `net.ipv4.tcp_keepalive_time` 可指定在最後一個資料封包後，發送第一條 keepalive 訊息前的等待時間。將此參數設定為 `900`。

要設定 keepalive 參數，請執行以下操作：

1. 開啟 /etc/sysctl.conf 檔案。
2. 新增以下參數值：

```
net.ipv4.tcp_keepalive_intvl = 1
net.ipv4.tcp_keepalive_probes = 10
net.ipv4.tcp_keepalive_time = 900
```

3. 執行以下指令，以更新 keepalive 參數：

```
sudo sysctl -p /etc/sysctl.conf
```

4. 執行以下指令，以確保參數值已套用：

```
sudo sysctl net.ipv4.tcp_keepalive_intvl
sudo sysctl net.ipv4.tcp_keepalive_probes
sudo sysctl net.ipv4.tcp_keepalive_time
```

佈署網路代理和安全應用程式

為了管理組織中的受管理裝置並保護它們免受安全威脅，您必須在每個受管理裝置上安裝網路代理和卡巴斯基安全應用程式。

有關防護佈署的資訊，請參閱部署網路代理和安全應用程式部分。

有關行動裝置防護的資訊，請參閱行動裝置管理部分。

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）下載更新並作為 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）。

在用戶端組織網路中設定防護

管理伺服器安裝完成後，卡巴斯基安全管理中心網頁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。

編輯設定時，請記住您可以鎖定或解鎖設定以禁止或允許在工作站上編輯其值。

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 文件。

以下敘述了進階設定操作，我們建議您在 Kaspersky Endpoint Security 的政策內容視窗中執行，在**一般設定**區域中。

一般設定區域，報告和儲存子區域

在“**將資料傳輸到管理伺服器**”部分，請注意“**關於已啟動的應用程式**”核取方塊。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 Linux 資料庫上的大量磁碟空間（幾十 G）。因此，如果**關於已啟動的應用程式**核取方塊依然在頂級政策中被選中，它必須被清空。

一般設定區域，介面子區域

如果組織網路中的威脅防護必須透過卡巴斯基安全管理中心網頁主控台集中管理，您必須停用在工作站上顯示 Kaspersky Endpoint Security 使用者介面（透過在**與使用者互動**區域清空**顯示應用程式介面**核取方塊），並啟用密碼防護（透過在**Password protection**區域選中密碼防護核取方塊）。

在事件配置區域配置政策

在**事件組態**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：
  - *應用程式自動執行被停用*
  - *存取被拒絕*
  - *應用程式啟動被禁止*
  - *不可能解毒*
  - *最終使用者產品授權協議被違反*
  - *無法載入加密模組*
  - *無法同時啟動兩個工作*
  - *偵測到活動威脅 .，應該啟動進階解毒*
  - *偵測到網路攻擊*
  - *未更新所有元件*
  - *啟動錯誤*
  - *啟用便攜模式錯誤*
  - *與卡巴斯基安全管理中心 Linux 互動錯誤*
  - *停用便攜模式錯誤*
  - *更改應用程式元件時出錯*
  - *套用檔案加密/解密規則錯誤*

- *政策無法被套用*
- *禁止已終止*
- *網路活動被封鎖*

- 在**功能失效**頁籤上：*無效工作設定 .，設定未套用*
- 在**警告**頁籤：
  - *自我防護已停用*
  - *不正確的備用金鑰*
  - *使用者已退出加密政策*
- 在**資訊**頁籤：*在測試模式下禁止應用程式啟動*

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

快速啟動精靈建立掃描裝置的群組工作。如果自動指定的群組掃描工作排程不適合您的組織，您必須根據組織採用的工作場所規則手動設定最方便的排程。

例如，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。在這種情況下，您需要手動設定群組掃描工作。

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 Linux 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。在這種情況下，政策的範圍透過（例如）裝置標籤或者使用者角色來設定。

- 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：

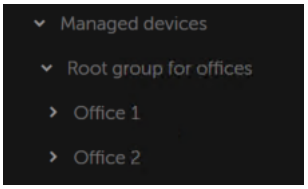
- 構建管理群組結構涉及到網路拓撲。管理群組結構可能不精確反映網路拓撲。網路各部分之間以及特定管理群組相互比對。您可以使用發佈點自動分配或手動分配它們。

- 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 實用程式或者 traceroute 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 Linux，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 Linux 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 Linux 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

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使用卡巴斯基安全管理中心 網頁主控台修改，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 Syslog 事件記錄和卡巴斯基安全管理中心 Linux 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

建議您，將裝置設定為透過*裝置移動規則*自動指派到管理群組。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 Linux 管理員明確建立，在**資產管理 → 移動規則**區域中。

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。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。這些方案也與卡巴斯基安全管理中心 Linux 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。

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 Linux 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。

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 Linux，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資料夾 /var/opt/kaspersky/KSC_Backups* 中。

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。

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。

在執行還原的管理伺服器上的實例，必須使用相同類型的 DBMS 和相同或更新版本。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：

- 必須為新的管理伺服器指派相同的 DNS 名稱。

  如果在部署網路代理時，網路代理安裝套件中設定了靜態 IP 位址，則也必須將相同的 IP 位址指派給新的管理伺服器。或者，您可以使用確定網路代理連線到的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）。

- 在 IAM 設定檔 `var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml` 中，將 `server_iam.ksc_address` 參數設定為與先前使用的管理伺服器憑證的主題備用名稱 (SAN) 中指定的管理伺服器位址完全相同。有關詳細信息，請參閱以下文章：將管理伺服器位址新增至IAM伺服器組態。

- 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。

- 執行 klbackup 實用程式並執行還原。還原成功後，請重新安裝網頁主控台。

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. 執行 klbackup 實用程式並執行還原。

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 Linux 分發節點上的資料的不一致和應用程式操作不正常。

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。

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 Linux 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。

關於將網路代理切換到其他管理伺服器

如果變更了下列網路設定，卡巴斯基安全管理中心 Linux 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。

  DHCP 伺服器位址條件設定目前無法使用。

- **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 名稱已變更。
- **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。您必須使用專用伺服器，並且軟體能夠處理高負載和頻繁的網路代理請求。請勿指定管理伺服器的連接埠。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。

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。

為漫遊使用者建立連線設定檔

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 **資產管理 → 政策**。
   b. 選擇要為其建立連線設定檔的管理群組：
      - 對於根群組，您可以繼續下一步。
      - 對於子群組，請按一下頁面頂部的**顯示階層**按鈕，然後在開啟的視窗中按一下所需子群組的名稱。

      所選群組的路徑將顯示在頁面頂部。如果需要，您可以點擊帶有管理群組名稱的連結進入該群組。預設情況下，路徑中的最後一個連結不活動。您也可以點擊**隱藏階層**按鈕關閉層次結構視窗。
   c. 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 **資產管理 → 資產（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**設定設定檔**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 Linux 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。

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 Linux 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、或接收受管理應用程式的統計資訊。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. 在主功能表中，轉至 **資產管理 → 資產（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。

3. 在裝置屬性視窗的**一般**部分中，啟用**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。在卡巴斯基安全管理中心網頁主控台中，該裝置顯示為已關閉。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**屬性（屬性值會顯示在卡巴斯基安全管理中心網頁主控台的裝置內容中的**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 Linux 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。

受管理裝置的屬性視窗包含**強制同步**按鈕。當卡巴斯基安全管理中心 Linux 執行同步指令時，管理伺服器會試圖連線到裝置。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。

度量手冊

該部分提供了卡巴斯基安全管理中心 Linux 尺寸資訊。

關於本手冊

卡巴斯基安全管理中心 Linux （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 軟體的裝置的防護的網路。

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

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。

建議在裝置上安裝管理伺服器和 DBMS 後，在這些裝置上安裝 Kaspersky Endpoint Security for Linux。對於 Kaspersky Endpoint Security的硬體需求，請參閱 Kaspersky Endpoint Security for Linux 說明。

Kaspersky Endpoint Security for Linux 與 Managed Detection and Response 及 Kaspersky Endpoint Detection and Response Expert（內部部署）整合時產生的負載，未納入卡巴斯基安全管理中心 Linux 與 Kaspersky Endpoint Security for Linux 併發安裝的計算中。

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。

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。

> 您需要在安裝了管理伺服器的裝置上啟用交換檔案。交換檔案的最小大小必須大於 RAM 容量的 1.5 倍。

建議在裝置上安裝管理伺服器和 DBMS 後，在這些裝置上安裝 Kaspersky Endpoint Security for Linux。
若要進行併發安裝，您必須至少具備 225 IOPS，並且在管理伺服器與 DBMS 的需求之外，另外增加 1.5 GB RAM。
如需 Kaspersky Endpoint Security 的硬體需求，請參閱 Kaspersky Endpoint Security for Linux 說明。

該網路包括 50,000 台裝置

安裝了管理伺服器的裝置的配置。

硬體	參數值
CPU	8 核（建議 12 核），2500 MHz
RAM	16 GB
磁碟空間	300 GB、150 IOPS 或更高

安裝了 PostgreSQL DBMS 的裝置組態

硬體	參數值
CPU	16 核心，2 500 MHz
RAM	32 GB
磁碟空間	300 GB、150 IOPS 或更高

容錯移轉叢集的節點配置

硬體	參數值
CPU	16 核心，2 500 MHz
RAM	32 GB
磁碟空間	500 GB、300 IOPS 或更高
網路介面控制器	1 Gbps

安裝了管理伺服器和 PostgreSQL DBMS 的裝置的配置

硬體	參數值
CPU	24 核（建議 28 核），2500 MHz
RAM	48 GB
磁碟空間	600 GB、300 IOPS 或更高

該網路包括 30,000 台裝置

安裝了管理伺服器的裝置的配置。

硬體	參數值
CPU	6 核（建議 8 核），2500 MHz
RAM	12 GB
磁碟空間	200 GB、150 IOPS 或更高

安裝了 PostgreSQL DBMS 的裝置組態

硬體	參數值
CPU	12 核心，2 500 MHz
RAM	22 GB
磁碟空間	250 GB、150 IOPS 或更高

容錯移轉叢集的節點配置

硬體	參數值
CPU	16 核心，2 500 MHz
RAM	32 GB
磁碟空間	500 GB、300 IOPS 或更高
網路介面控制器	1 Gbps

安裝了管理伺服器和 PostgreSQL DBMS 的裝置的配置

硬體	參數值
CPU	16 核（建議 20 核），2500 MHz
RAM	34 GB
磁碟空間	450 GB、300 IOPS 或更高

該網路包括 10,000 台裝置

安裝了管理伺服器的裝置的配置。

硬體	參數值
CPU	4 核（建議 6 核），2500 MHz
RAM	8 GB
磁碟空間	100 GB、150 IOPS 或更高

安裝了 PostgreSQL DBMS 的裝置組態

硬體	參數值
CPU	6 核，2500 MHz
RAM	10 GB
磁碟空間	200 GB、150 IOPS 或更高

容錯移轉叢集的節點配置

硬體	參數值
CPU	16 核心，2 500 MHz
RAM	32 GB
磁碟空間	500 GB、300 IOPS 或更高
網路介面控制器	1 Gbps

安裝了管理伺服器和 PostgreSQL DBMS 的裝置的配置

硬體	參數值
CPU	8 核（建議 14 核），2500 MHz
RAM	18 GB
磁碟空間	300 GB、300 IOPS 或更高

該網路包括 1000 台裝置

安裝了管理伺服器的裝置的配置。

硬體	參數值
CPU	2 核，2500 MHz
RAM	6 GB
磁碟空間	10 GB、150 IOPS 或更高

安裝了 PostgreSQL DBMS 的裝置組態

硬體	參數值
CPU	2 核，2500 MHz
RAM	4 GB
磁碟空間	20 GB、150 IOPS 或更高

容錯移轉叢集的節點配置

硬體	參數值
CPU	16 核心，2 500 MHz
RAM	32 GB

硬體	參數值
磁碟空間	500 GB、300 IOPS 或更高
網路介面控制器	1 Gbps

安裝了管理伺服器和 PostgreSQL DBMS 的裝置的配置

硬體	參數值
CPU	4 核心，2 500 MHz
RAM	10 GB
磁碟空間	30 GB、300 IOPS 或更高

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。
- PostgreSQL DBMS 不包含 plpgsql 以外的任何擴充元件。

在安裝了 DBMS 的裝置上，資料庫大約會消耗 100 GB 的磁碟空間，交易日誌大約會消耗 200 GB 的磁碟空間。

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。

操作期間，一定的*未佔用時間*總是出現在資料庫。因此，資料庫檔案的實際大小通常約為資料庫所佔空間量的兩倍。

不建議明確限制事務記錄的大小。建議保留 MAXSIZE 參數的預設值。

磁碟空間計算

/var/opt/kaspersky/klnagent_srv/ 資料夾在管理伺服器上需要的磁碟空間，大致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。

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 Linux 會在卡巴斯基安全管理中心網頁主控台中為該動態 VM 建立一個記錄並將動態 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 Linux 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 Linux 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 Linux 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 Linux。

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 Linux。

變更動態 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

本文介紹基於 Windows 和 Linux 發佈點的硬體和軟體要求。

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。

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。

基於 Windows 發佈點的硬體需求

基於 Windows 發佈點的最低硬體要求

用戶端裝置數量	處理器	RAM	RAM，啟用修補程式管理	磁碟空間
10,000	4 核心，2 500 MHz	8 GB	8 GB	120 GB

5000	4 核心，2 500 MHz	6 GB	8 GB	120 GB
1000	2 核，2500 MHz	4 GB	8 GB	120 GB

基於 Linux 發佈點的硬體需求

Linux 型發佈點的最低硬體要求

用戶端裝置數量	處理器	RAM	磁碟空間
10,000	4 核心，2 500 MHz	10 GB	120 GB
5000	4 核心，2 500 MHz	8 GB	120 GB
1000	2 核心，2500 MHz	6 GB	120 GB

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。

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 Linux 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，作業係統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）。

管理大量裝置的管理伺服器的最佳實踐

使用 DBMS 的最佳實踐

將**管理伺服器維護**工作配置為定期執行，尤其是當您使用 PostgreSQL DBMS 時。

從 IOC 掃描中排除 DBMS 資料夾。

政策和設定檔的最佳實踐

減少元件（例如 Kaspersky Endpoint Security for Windows）的活動政策數量。您可以用政策設定檔替換政策。

管理大量裝置的管理伺服器的最佳實踐

減少同時執行的工作數量，尤其是遠端安裝和修補程式管理。

減少與裝置選擇相關的工作數量並最佳化其排程。

在政策設定的**事件組態**部分，最大限度地減少儲存的事件類型的數量。

儲存事件的最佳實踐

降低應用程式控制元件中單一類型事件的頻率。有關詳細資訊，請參閱以下文章：關於封鎖頻繁事件。

縮短來自元件（例如 Kaspersky Endpoint Security for Windows）的事件和有關已修復弱點的資訊事件的儲存期限。

在常見工作（例如更新工作）的工作設定中，啟用 **儲存工作進度相關事件**選項。有關詳細資訊，請參閱以下文章：記錄有關工作和政策的事件的資訊。

最佳化清查工作設定。有關詳細資訊，請參閱以下文章：清查工作。

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、資料庫維護工作和更新 Kaspersky Endpoint Security 的群組工作是卡巴斯基安全管理中心 Linux 的基本功能部分。

清查工作是弱點和修補程式管理功能的一部分，且在該功能未啟動時不可用。

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資料庫維護工作

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 Linux 達到了該限制，它將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。

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 for Linux	390 MB	3.3 MB
網路代理安裝	75 MB	397 KB
網路代理與 Kaspersky Endpoint Security for Linux 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 for Linux。
- 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。

已知問題

卡巴斯基安全管理中心 Linux 具有以下限制，但這些限制對於應用程式的運作並無大礙：

- 10373324：如果所有節點均未安裝網路代理，則在計算指標狀態時，僅會考慮目前作用中的節點。如果其中一個節點上安裝了網路代理，則只有在該節點變成作用中時，才會考慮該節點。因此，若要在計算指標狀態時考慮所有節點，您必須在每個節點上安裝網路代理，且每個節點都必須至少曾處於作用中狀態一次。

- 8994760：如果您擁有虛擬管理伺服器的存取權限，但沒有主管理伺服器的存取權限，並且嘗試登入卡巴斯基安全管理中心 Linux，則會發生錯誤，且錯誤訊息 **目前無法處理您的要求，請稍後再試** 不正確。錯誤文字必須為以下內容：**檢查您的存取權限。您必須在主伺服器上或者只能在一台虛擬伺服器上擁有存取權限。請聯絡主管理員，然後再試**

- 10085767：遷移至卡巴斯基安全管理中心 Linux 時，報告範圍可能會顯示不正確。

- 10292104：在卡巴斯基安全管理中心網頁主控台 15.1 或 15.2 版本中，如果您將 Kaspersky Endpoint Detection and Response Optimum 外掛程式更新至 16.3 版本，**警示** 區段可能不會顯示警示。

- 10308380：建立應用程式類別後，如果您嘗試按一下確認對話方塊中的 **確定** 按鈕來開啟其屬性，屬性視窗不會開啟。

- 10253149：針對應用程式政策，如果您在 **事件組態** 索引標籤上選取大量事件，則包含有關此類事件對管理伺服器或資料庫管理系統效能影響之警告的 **顯示更多** 展開區塊不會顯示。

- 10127434：如果您登入主管理伺服器上的卡巴斯基安全管理中心網頁主控台時開啟 **工作** 區段，然後開啟 階層視窗，虛擬伺服器會顯示為主伺服器。

- 9302142：Microsoft Windows on Arm不支援**使用網路代理作為 DMZ 連線閘道**選項。

- 9065814: 嘗試從Samba 4網域中的Windows裝置進行網域身分驗證時，可能會發生錯誤。

- 9335676: 在高可用性資料庫管理系統叢集切換主節點後，卡巴斯基安全管理中心網頁主控台可能無法存取或存取速度顯著降低。如果卡巴斯基安全管理中心網頁主控台超過10分鐘仍無法訪問，請使用以下命令重新啟動IAM服務：

  ```
  systemctl restart kliam_srv.service
  ```

- 9157005, 9157085: 在啟用了*安裝所需更新並修復弱點*選項的 Windows受管理裝置上執行**在裝置重新啟動或關閉時開始安裝**工作時，該工作可能會失敗並出現錯誤。當排定安裝大量更新時，可能會出現此問題。若要解決此問題，請在不啟用**在裝置重新啟動或關閉時開始安裝**選項的情況下執行此工作。

- 9272534: 如果使用者表包含超過 50,000 個使用者，則僅顯示前 50,000 個使用者，其餘使用者將不顯示。

- 9291235: 在管理伺服器版本 16.1 上還原備份後，卡巴斯基安全管理中心網頁主控台會顯示登入頁面。身分驗證成功後，系統會要求用於雙因素驗證的一次性安全代碼。如果輸入有效的一次性安全代碼，則會顯示錯誤訊息，提示代碼不正確。在這種情況下，請稍等幾分鐘，然後手動重新整理頁面，重試登入卡巴斯基安全管理中心網頁主控台。備份還原處理程序完成後，下次嘗試登入時身分驗證即可成功。

- 7939561: 嘗試修改受防護的使用者帳戶時，按一下帳戶防護**帳戶防護取消**按鈕會導致錯誤。

- 8562938: 在管理伺服器政策屬性中開啟行動裝置連接埠不會啟用行動裝置管理功能，也不會觸發行動憑證的產生。若要啟用行動裝置管理功能，必須在管理伺服器屬性中開啟行動裝置的連接埠。

- 8732282: 對於在 Active Directory 的帳戶屬性中啟用了**使用者無法變更密碼**選項的使用者，將不會執行 Active Directory 中的**重設密碼**回應操作。網域控制站管理員必須停用此使用者的**使用者無法變更密碼**選項或手動重設密碼。如果您擁有 Kaspersky Next XDR Optimum 產品授權、啟用了與 Active Directory 的整合且使用者包含在 Active Directory 安全群組中，則會發生此問題。

- 8688182: 如果使用者在 Active Directory 中的帳戶屬性中啟用了**密碼永不過期**選項，則在執行**重設密碼**回應操作後， **密碼永不過期**選項將被停用，且使用者將需要在下次登入時變更其網域密碼。如果您擁有 Kaspersky Next XDR Optimum 產品授權、啟用了與 Active Directory 的整合且使用者包含在 Active Directory 安全群組中，則會發生此問題。

- 8703857: 只有當代理伺服器支援基本驗證時，才會建立卡巴斯基安全管理中心網頁主控台和管理 Web 外掛程式的代理伺服器連線。

- 7911778: 當您執行**遠端解除安裝應用程式**工作以從執行 Arm 架構作業系統且與管理伺服器時間不同步的裝置解除安裝網路代理時，工作狀態不會從**執行中**變更為**已完成** ，即使在網路代理已被成功從裝置解除安裝後。若要解決此問題，請在**遠端解除安裝應用程式**之前將裝置上的時間與已安裝的網路代理同步，並將裝置上的時間與管理伺服器同步。

- 6896585: 如果卡巴斯基安全管理中心 Linux 安裝在名稱中包含西里爾符號的裝置上，則受管理裝置無法透過 KSN 代理服務連線到 KSN。

- 7523299: 網路代理在執行 CentOS 6.6 的受管理裝置上終止進程後不會重新啟動。

- 7835858: 如果您在卡巴斯基安全管理中心網頁主控台 15.2 或更高版本中使用**每 N 天**和**按星期幾**排程設定建立工作，然後在早期版本的卡巴斯基安全管理中心網頁主控台或管理主控台中開啟該工作（例如，當該工作也套用於從屬管理伺服器（可以是 Linux 和 Windows 版）時，排程設定可能會顯示不正確，或者可能發生錯誤。

- 7208621: 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。

- 6511063: 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。

- 5915107: 在信紙格式的報告中，分頁符可能會水平切割文字行。

- 5556109: 具有多個網路介面卡的受管理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。

- 9093038: 如果卡巴斯基安全管理中心 Linux 管理伺服器安裝後未啟動，且作業系統日誌包含與 kladminserver_srv.service 相關的錯誤 213/SECUREBITS，請以超級使用者身分執行下列命令：

  ```
  mkdir -p /etc/systemd/system/kladminserver_srv.service.d
  echo "[Service]" > /etc/systemd/system/kladminserver_srv.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/kladminserver_srv.service.d/override.conf
  mkdir -p /etc/systemd/system/klwebsrv_srv.service.d
  echo "[Service]" > /etc/systemd/system/klwebsrv_srv.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/klwebsrv_srv.service.d/override.conf
  ```

  如果卡巴斯基安全管理中心網頁主控台安裝後未啟動，且作業系統日誌包含與 KSCWebConsole.service 相關的錯誤 213/SECUREBITS，請以超級使用者身分執行下列命令：

  ```
  mkdir -p /etc/systemd/system/KSCSvcWebConsole.service.d
  echo "[Service]" > /etc/systemd/system/KSCSvcWebConsole.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCSvcWebConsole.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsoleManagement.service.d
  echo "[Service]" > /etc/systemd/system/KSCWebConsoleManagement.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsoleManagement.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsoleNATS.service.d
  echo "[Service]" > /etc/systemd/system/KSCWebConsoleNATS.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsoleNATS.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsolePlugin.service.d
  echo "[Service]" > /etc/systemd/system/KSCWebConsolePlugin.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsolePlugin.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsole.service.d
  echo "[Service]" > /etc/systemd/system/KSCWebConsole.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsole.service.d/override.conf
  ```

  如果安裝後 kliam_srv 服務未能啟動，且作業系統記錄中出現與該服務相關的 213/SECUREBITS 錯誤，請以超級使用者身分執行以下命令：

  ```
  mkdir -p /etc/systemd/system/kliam_srv.service.d
  echo "[Service]" > /etc/systemd/system/kliam_srv.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/kliam_srv.service.d/override.conf
  ```

- 9165434: NTLM 身分驗證不適用於受保護使用者群組中的使用者帳戶。

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 Linux 檔案或其中一個有關卡巴斯基安全管理中心 Linux 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 Linux 安裝和使用的所有問題。

Kaspersky 在此卡巴斯基安全管理中心 Linux 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 /var/lib/systemd/coredump 目錄中。只要卡巴斯基安全管理中心 Linux 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。

如果管理伺服器當機，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發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 Linux 頁面

在 Kaspersky 網站的 卡巴斯基安全管理中心 Linux 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 Linux 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 Linux 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 Linux 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

Cloud Discovery

Cloud Discovery 管理使用者對雲端服務的存取。雲端服務包括 Microsoft Teams、Salesforce、Microsoft Office 365 等。雲端服務按類別分組，例如*檔案共用*、*通訊軟體*、*電子郵件*。

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。

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。

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。

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。

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 Linux 管理的卡巴斯基應用程式。

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 Linux 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 Linux 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 Linux 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 Linux 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 Linux 管理員

透過卡巴斯基安全管理中心 Linux 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 Linux 網頁伺服器

卡巴斯基安全管理中心 Linux 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系統健康驗證程式 (SHV)

在卡巴斯基安全管理中心 Linux 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 Linux 的一個元件。

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。Kaspersky Private Security Network用於由於以下原因無法加入Kaspersky Security Network的企業用戶端：

- 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。

應用程式商店

卡巴斯基安全管理中心 Linux 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。

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。管理主控台類似於卡巴斯基安全管理中心網頁主控台。

管理伺服器

卡巴斯基安全管理中心 Linux 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：

- 連線卡巴斯基安全管理中心 網頁主控台時驗證管理伺服器的身分
- 受管理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

從其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 Linux 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 Linux 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 Linux 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 Linux 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）。

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

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。

設定檔

包含設定集合和 iOS MDM 行動裝置限制的政策。

身分識別與存取管理器 (IAM)

管理伺服器的元件，可讓您使用網域身份驗證（單一登入）。單一登入功能可讓使用者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，而無需在公司網路上重新輸入密碼。

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 Linux 提供的服務安裝卡巴斯基應用程式。

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。

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，在應用程式安裝目錄內。

商標聲明

註冊商標及服務標誌均為其各自所有人的財產。

Adobe、Acrobat、Flash、PostScript 和 Shockwave 是 Adobe 在美國和/或其他國家/地區的註冊商標或商標。

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軟體基金會在美國和/或其他國家的註冊商標或商標。

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、Cisco Jabber、Cisco Systems、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、Google Public DNS、Hangouts 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。

Microsoft、Active Directory、ActiveSync、BitLocker、Excel、Forefront、Internet Explorer、InfoPath、Hyper-V、Microsoft Edge、MultiPoint、MS-DOS、PowerShell、PowerPoint、SharePoint、SQL Server、Office 365、OneNote、Outlook、Skype、Tahoma、Visio、Win32、Windows、Windows PowerShell、Windows Media、Windows Server、Windows Phone、Windows Vista 和 Windows Azure 是 Microsoft 集團公司的商標。

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。

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。

Rocky Linux 是 Rocky Enterprise Software Foundation 的商標。

Samsung是SAMSUNG在美國或其他國家的商標。

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。