卡巴斯基安全管理中心 14 Linux

目錄

卡巴斯基安全管理中心 14 Linux 說明
新增內容
關於卡巴斯基安全管理中心 Linux
- 分發套件
- 硬體和軟體需求
- 關於卡巴斯基安全管理中心 14 網頁主控台
- 支援的 Kaspersky 應用程式清單
- 卡巴斯基安全管理中心比較：基於 Windows 與基於 Linux

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
- 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

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
- 檢視隱私權政策。
- 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
- 超出了產品授權限制事件

架構
卡巴斯基安全管理中心管理伺服器佈署圖表和卡巴斯基安全管理中心 14 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 14 網頁主控台使用的連接埠
安裝
- 主要安裝情境
- 按住資料庫管理系統。
- 設定 MariaDB x64 伺服器以與卡巴斯基安全管理中心 14 Linux 一起使用
- 安裝卡巴斯基安全管理中心
- 安裝卡巴斯基安全管理中心 14 網頁主控台
- 卡巴斯基安全管理中心 14 網頁主控台安裝參數
- 使用 DBMS 的帳戶
- 部署 Kaspersky 容錯移轉叢集
  - 情境：部署 Kaspersky 容錯移轉叢集
  - 關於 Kaspersky 容錯移轉叢集
  - 為 Kaspersky 容錯移轉叢集準備檔案伺服器
  - 為 Kaspersky 容錯移轉叢集準備節點
  - 在 Kaspersky 容錯移轉叢集節點上安裝卡巴斯基安全管理中心
  - 手動啟動和停止叢集節點
- 用於卡巴斯基安全管理中心的憑證
  - 關於卡巴斯基安全管理中心憑證
  - 卡巴斯基安全管理中心中使用的自訂憑證要求
  - 重新發佈卡巴斯基安全管理中心 14 網頁主控台憑證
  - 取代卡巴斯基安全管理中心 14 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
- 定義共用資料夾

關於升級卡巴斯基安全管理中心 Linux
- 使用安裝檔案升級卡巴斯基安全管理中心 Linux
- 通過備份升級卡巴斯基安全管理中心 Linux

登入到卡巴斯基安全管理中心 14 網頁主控台並登出

快速啟動精靈
- 步驟 1：指定網際網路連線設定
- 步驟 2：選取應用程式啟動方式
- 步驟 3：建立基本的網路保護設定
- 步驟 4：設定電子郵件通知
- 步驟 5：關閉快速設定精靈

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

設定管理伺服器
- 配置卡巴斯基安全管理中心 14 網頁主控台到管理伺服器的連線
- 設定 IP 位址允許清單以登入卡巴斯基安全管理中心
- 檢視連線到管理伺服器的記錄
- 設定事件儲存區中的最大事件數量
- 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
  - 資料備份和還原實用程式 (klbackup)
  - 互動模式下的資料備份和還原
  - 靜默模式下的資料備份和還原
- 將管理伺服器和資料庫伺服器移動到另一台裝置
- 建立虛擬管理伺服器
- 管理伺服器的階層
- 建立管理伺服器階層：新增次要管理伺服器
- 檢視次要管理伺服器清單
- 啟用帳戶防護以防止未經授權的修改
- 兩步驟驗證
  - 情境：為所有使用者配置兩步驟驗證
  - 關於帳戶的兩步驟驗證
  - 對您自己的帳戶啟用兩步驟驗證
  - 對所有使用者啟用兩步驟驗證
  - 對使用者帳戶停用兩步驟驗證
  - 對所有使用者停用兩步驟驗證
  - 從兩步驟驗證中排除帳戶
  - 產生新的金鑰
  - 編輯安全碼簽發者的名稱
- 變更允許的密碼輸入嘗試次數
- 變更 DBMS 憑證
- 刪除管理伺服器階層
- 配置介面

發現網路裝置
- 情境：發現網路裝置
- IP 範圍輪詢
- 新增和修改 IP 範圍
- Zeroconf 輪詢
- 裝置標籤
  - 關於裝置標籤
  - 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
- 應用程式標籤
  - 關於應用程式標籤
  - 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
- 卡巴斯基應用程式部署
  - 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
  - 從檔案建立安裝套件
  - 建立獨立安裝套件
  - 檢視獨立安裝套件清單
  - 使用遠端軟體安裝工作安裝應用程式
    - 安裝應用程式到特定裝置
    - 透過 Active Directory 群組政策安裝應用程式
    - 在從屬管理伺服器上安裝應用程式
  - 指定在 Unix 裝置上進行遠端安裝的設定
  - 取代協力廠商安全應用程式
  - 遠端刪除應用程式或軟體更新
  - 準備一部執行 SUSE Linux Enterprise Server 15 的裝置以安裝網路代理
- Kaspersky 應用程式：產品授權和啟動
  - 受管理應用程式的產品授權
  - 新增產品授權金鑰到管理伺服器儲存區
  - 佈署產品授權金鑰到用戶端裝置
  - 自動分發產品授權金鑰
  - 檢視使用中產品授權金鑰的相關資訊
  - 從儲存區刪除產品授權金鑰
  - 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
- 配置網路防護
  - 情境：配置網路防護
  - 關於以裝置為中心和以使用者為中心的安全管理方法
  - 政策設定和傳播：以裝置為中心的方法
  - 政策設定和傳播：以使用者為中心的方法
  - Kaspersky Endpoint Security 更新群組工作的手動設定
  - 網路代理政策設定
  - 變更裝置移動規則的優先順序
  - 工作
    - 關於工作
    - 關於工作範圍
    - 建立工作
    - 手動啟動工作
    - 檢視工作清單
    - 一般工作設定
    - 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
  - 管理用戶端裝置
    - 受管理裝置設定
    - 建立管理群組
    - 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
- 將裝置手動移動至管理群組
- 變更用戶端裝置的管理伺服器
- 當裝置顯示不活動時檢視和配置操作
- 關於裝置狀態
- 設定裝置狀態轉換
- 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
- 政策層級
- 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
- 強制同步
- 檢視政策發佈狀態圖表
- 刪除政策
- 管理政策設定檔
- 檢視政策設定檔
- 變更政策設定檔優先順序
- 建立政策設定檔
- 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
- 使用者和使用者角色
- 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
- 新增內部使用者帳戶
- 建立使用者群組
- 編輯內部使用者帳戶
- 編輯使用者群組
- 新增使用者帳戶到內部群組
- 指派使用者作為裝置所有者
- 刪除使用者或安全群組
- 建立使用者角色
- 編輯使用者角色
- 編輯使用者角色範圍
- 刪除使用者角色
- 關聯政策設定檔到角色
- 管理物件修訂
- 關於物件修訂
- 回溯物件到先前修訂
- 物件刪除
- 使用 klscflag 實用程式開啟連接埠 13291

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
- 瀏覽已下載的更新
- 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
- 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：方案
- 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
- 發佈點和連線閘道器的調整
  - 發佈點的標準配置：單一辦公室
  - 發佈點的標準配置：多個小遠端分辦公室
  - 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
  - 修改管理群組的發佈點清單
  - 啟用推送伺服器
- 管理用戶端裝置上的協力廠商應用程式
  - 情境：應用程式管理
  - 關於應用程式控制
  - 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
  - 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
- 監控和報告
  - 情境：監控和報告
  - 關於監控和報告的類型
  - 儀表板和小部件
    - 使用儀表板
    - 新增小部件到儀表板
    - 從儀表板隱藏小部件
    - 移動儀表板上的小部件
    - 變更部件尺寸或樣子
    - 變更部件設定
    - 關於"僅儀表板"模式
    - 配置"僅儀表板"模式
  - 報告
    - 使用報告
    - 建立報告範本
    - 檢視和編輯報告範本內容
    - 匯出報告到檔案
    - 生成和瀏覽報告
    - 建立報告傳送工作
    - 刪除報告範本
  - 事件和事件選擇
    - 使用事件分類
    - 建立事件分類
    - 編輯事件分類
    - 查看事件分類清單
    - 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
    - 事件類型
      - 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
        - 網路代理警告事件
        - 網路代理資訊事件
    - 封鎖頻發事件
      - 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
- 匯出到 SIEM 系統的事件
  - 情境：設定事件匯出到 SIEM 系統
  - 在您開始之前
  - 卡巴斯基安全管理中心 Linux 中的事件
  - 關於事件匯出
  - 配置在 SIEM 系統中的事件匯出
  - 標記事件，將其以 Syslog 格式匯出到 SIEM 系統
    - 關於標記事件並將其以 Syslog 格式匯出到 SIEM 系統
    - 將 Kaspersky 應用程式的事件標記為以 Syslog 格式匯出
    - 標記一般事件，將其以 Syslog 格式匯出
  - 關於使用 Syslog 格式匯出事件
  - 配置卡巴斯基安全管理中心 Linux 以將事件匯出到 SIEM 系統
  - 直接從資料庫匯出事件
    - 使用 klsql2 實用程式建立 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
- 裝置分類
  - 建立裝置分類
  - 配置裝置分類

API 參考手冊

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

- 配置到 KATA / KEDR 網頁主控台的存取
- 建立背景連線

聯絡技術支援

- 如何取得技術支援
- 透過電話取得技術支援
- 透過 Kaspersky CompanyAccount 取得技術支援

有關程式的資訊來源

已知問題

詞彙表

- HTTPS
- 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
- 備份資料夾
- 備用訂購金鑰
- 內部使用者
- 共用憑證
- 卡巴斯基安全管理中心操作員
- 卡巴斯基安全管理中心管理員
- 卡巴斯基安全管理中心系統健康驗證程式 (SHV)
- 卡巴斯基安全管理中心網頁伺服器
- 卡巴斯基私有安全網路（私有 KSN）
- 受管理裝置
- 可用更新
- 安裝套件
- 工作
- 工作設定
- 廣播網域

- 應用程式商店
- 手動安裝
- 指定裝置的工作
- 授權檔案
- 授權的應用程式群組
- 政策
- 啟動產品授權
- 更新
- 服務供應商管理員
- 本機安裝
- 本機工作
- 歸屬管理伺服器
- 產品授權期限
- 用戶端管理員
- 病毒資料庫
- 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
- 身分驗證代理
- 連線閘道
- 遠端安裝
- 還原
- 還原管理伺服器資料
- 防護狀態
- 隔離區域 (DMZ)
- 集中式應用程式管理

有關協力廠商代碼的資訊

商標聲明

卡巴斯基安全管理中心 14 Linux 說明

新增內容

在最新應用程式版本中的新增內容。

硬體和軟體需求

檢查支援什麼作業系統和應用程式版本。

安裝

安裝管理伺服器和卡巴斯基安全管理中心 14 網頁主控台。

發現網路裝置

發現您組織網路中的現有裝置和新裝置。

Kaspersky 應用程式。集中佈署

佈署 Kaspersky 應用程式。

Kaspersky 應用程式。產品授權和啟動

幾步啟動 Kaspersky 應用程式。

配置網路防護

管理組織的安全。

Kaspersky 應用程式。更新資料庫和軟體模組

維持防護系統的可靠性。

監控和報告

檢視您的基礎架構、防護狀態和統計資訊。

發佈點和/或連線閘道的調整

配置發佈點。

新增內容

卡巴斯基安全管理中心 14 Linux

卡巴斯基安全管理中心 14 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*工作進行下載。
- 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。

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 的用途及其主要功能特色和元件。

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 Linux® 裝置的防護，以符合純 Linux 環境的要求。

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。
- 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。

分發套件

您可以透過 Kaspersky 或其合作夥伴公司的線上商店（例如，https://www.kaspersky.com.tw）購買應用程式。

如果您在線上商店購買卡巴斯基安全管理中心 Linux ，則可以從該商店的網站複製程式。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。

硬體和軟體需求

管理伺服器

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：4 GB。
- 可用磁碟空間：10 GB。

支援以下作業系統：

- Debian GNU/Linux 11.x (Bullseye) 32 位元 / 64 位元
- Debian GNU/Linux 10.x (Buster) 32 位元 / 64 位元
- Debian GNU / Linux 9.x (Stretch) 32 位元 / 64 位元
- Ubuntu Server 20.04 LTS (Focal Fossa) 64 位元
- Ubuntu Server 18.04 LTS (Bionic Beaver) 64 位元
- CentOS 7.x 64 位元
- Red Hat Enterprise Linux Server 8.x 64 位元
- Red Hat Enterprise Linux Server 7.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 1.7（包括封閉軟體環境模式和強制模式）64 位元
- Astra Linux 特別版 1.6（包括封閉軟體環境模式和強制模式）64 位元
- Astra Linux 通用版 2.12 64 位元
- Alt Server 10 64 位元
- Alt Server 9.2 64 位元
- Alt 8 SP Server (LKNV.11100-01) 64 位元
- Alt 8 SP Server (LKNV.11100-02) 64 位元
- Alt 8 SP Server (LKNV.11100-03) 64 位元
- Oracle Linux 7 64 位元
- Oracle Linux 8 64 位元
- RED OS 7.3 Server 64 位元
- RED OS 7.3 Certified Edition 64 位元

支援以下虛擬平台：

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware Workstation 16 Pro
- Microsoft Hyper-V Server 2012 64 位元
- Microsoft Hyper-V Server 2012 R2 64 位元
- Microsoft Hyper-V Server 2016 64 位元
- Microsoft Hyper-V Server 2019 64 位元
- Microsoft Hyper-V Server 2022 64 位元
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 17
- 基於內核的虛擬機。支援以下作業系統：
  - Alt 8 SP Server (LKNV.11100-01) 64 位元
  - Alt Server 10 64 位元

- Astra Linux 特別版 1.7（包括封閉軟體環境模式 和強制模式）64 位元
- Debian GNU/Linux 11.x (Bullseye) 32 位元 / 64 位元
- Ubuntu Server 20.04 LTS (Focal Fossa) 64 位元
- RED OS 7.3 Server 64 位元
- RED OS 7.3 Certified Edition 64 位元

支援以下資料庫伺服器（可以安裝在不同的裝置上）：

- MySQL 5.7 社區 32 位元/64 位元
- MySQL 8.0 64 位元
- MariaDB 10.5.x 64 位元
- MariaDB 10.4.x 64 位元
- MariaDB 10.3.22 及更高版本 32 位元/64 位元
- MariaDB Server 10.3 32 位元 / 64 位元，搭配 InnoDB 儲存引擎
- MariaDB 10.1.30 及更高版本 32 位元/64 位元

卡巴斯基安全管理中心 14 網頁主控台

卡巴斯基安全管理中心 14 網頁主控台伺服器

最小硬體條件：

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

以下作業系統之一（僅限 64 位元版本）：

- Debian GNU/Linux 11.x (Bullseye)
- Debian GNU/Linux 10.x (Buster)
- Debian GNU/Linux 9.x (Stretch)
- Ubuntu Server 20.04 LTS (Focal Fossa)
- Ubuntu Server 18.04 LTS (Bionic Beaver)
- CentOS 7.x
- Red Hat Enterprise Linux Server 8.x
- Red Hat Enterprise Linux Server 7.x
- SUSE Linux Enterprise Server 12（所有服務套件）
- SUSE Linux Enterprise Server 15（所有服務套件）
- SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM 64 位元
- Astra Linux 特別版 1.7（包括封閉軟體環境模式 和強制模式）
- Astra Linux 特別版 1.6（包括封閉軟體環境模式和強制模式）
- Astra Linux Common Edition 2.12
- Alt Server 10
- Alt Server 9.2

- Alt 8 SP Server (LKNV.11100-01)
- Alt 8 SP Server (LKNV.11100-02)
- Alt 8 SP Server (LKNV.11100-03)
- Oracle Linux 8
- Oracle Linux 7
- RED OS 7.3 Server
- RED OS 7.3 認證版

在虛擬化平台中，以下作業系統支援基於內核的虛擬機：

- Alt 8 SP Server (LKNV.11100-01) 64 位元
- Alt Server 10 64 位元
- Astra Linux 特別版 1.7（包括封閉軟體環境模式 和強制模式）64 位元
- Debian GNU/Linux 11.x (Bullseye) 32 位元 / 64 位元
- Ubuntu Server 20.04 LTS (Focal Fossa) 64 位元
- RED OS 7.3 Server 64 位元
- RED OS 7.3 Certified Edition 64 位元

用戶端裝置

對於用戶端，卡巴斯基安全管理中心 14 網頁主控台的使用僅需要一個瀏覽器。

裝置的硬體和軟體需求和卡巴斯基安全管理中心 14 網頁主控台所使用的瀏覽器的需求是相同的。

瀏覽器：

- Mozilla Firefox 延伸程式支援版本 91.8.0 或更高版本（91.8.0 於 2022 年 4 月 5 日發布）
- Mozilla Firefox 99.0 或更高版本（99.0 於 2022 年 4 月 5 日發布）
- Google Chrome 100.0.4896.88 或更高版本（官方版本）
- Microsoft Edge 100 或更高版本
- macOS 的 Safari 15

網路代理

最小硬體條件：

- 執行頻率為 1 GHz 或更高的 CPU。若為 64 位元作業系統，CPU 最低頻率為 1.4 GHz。
- RAM：512 MB。
- 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。

支援以下作業系統：

- Debian GNU/Linux 11.x (Bullseye) 32 位元 / 64 位元
- Debian GNU/Linux 10.x (Buster) 32 位元 / 64 位元
- Debian GNU / Linux 9.x (Stretch) 32 位元 / 64 位元
- Ubuntu Server 20.04 LTS (Focal Fossa) 32 位元/64 位元
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64 位元

- Ubuntu Server 18.04 LTS (Bionic Beaver) 32 位元 / 64 位元
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32 位元/64 位元
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32 位元 / 64 位元
- CentOS 8.x 64 位元
- CentOS 7.x 64 位元
- CentOS 7.x ARM 64 位元
- Red Hat Enterprise Linux Server 8.x 64 位元
- Red Hat Enterprise Linux Server 7.x 64 位元
- Red Hat Enterprise Linux Server 6.x 32 位元/64 位元
- SUSE Linux Enterprise Server 12（所有服務套件）64 位元
- SUSE Linux Enterprise Server 15（所有服務套件）64 位元
- SUSE Linux Enterprise Desktop 15（所有服務套件）64 位元
- SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM 64 位元
- openSUSE 15 64 位元
- EulerOS 2.0 SP8 ARM
- Leopard OS 19.1 64 位元
- Astra Linux 特別版 1.7（包括封閉軟體環境模式和強制模式）64 位元
- Astra Linux 特別版 1.6（包括封閉軟體環境模式和強制模式）64 位元
- Astra Linux 通用版 2.12 64 位元
- Astra Linux 特別版 4.7 ARM
- Alt Server 10 64 位元
- Alt Server 9.2 64 位元
- Alt Workstation 10 32 位元/64 位元
- Alt Workstation 9.2 32 位元/64 位元
- Alt 8 SP Server (LKNV.11100-01) 64 位元
- Alt 8 SP Server (LKNV.11100-02) 64 位元
- Alt 8 SP Server (LKNV.11100-03) 64 位元
- Alt 8 SP Workstation (LKNV.11100-01) 32 位元/64 位元
- Alt 8 SP Workstation (LKNV.11100-02) 32 位元/64 位元
- Alt 8 SP Workstation (LKNV.11100-03) 32 位元/64 位元
- Mageia 4 32 位元
- Oracle Linux 7 64 位元
- Oracle Linux 8 64 位元
- Linux Mint 19.x 32 位元
- Linux Mint 20.x 64 位元
- AlterOS 7.5 及更高版本 64 位元
- GosLinux IC6 64 位元

- RED OS 7.3 64 位元
- RED OS 7.3 Server 64 位元
- RED OS 7.3 Certified Edition 64 位元
- ROSA Enterprise Linux Server 7.3 64 位元
- ROSA Enterprise Linux Desktop 7.3 64 位元
- ROSA COBALT Workstation 7.3 64 位元
- ROSA COBALT Server 7.3 64 位元
- Lotos（Linux 核心版本 4.19.50，DE：MATE) 64 位元

支援以下虛擬平台：

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware Workstation 16 Pro
- Microsoft Hyper-V Server 2012 64 位元
- Microsoft Hyper-V Server 2012 R2 64 位元
- Microsoft Hyper-V Server 2016 64 位元
- Microsoft Hyper-V Server 2019 64 位元
- Microsoft Hyper-V Server 2022 64 位元
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- 基於內核的虛擬機。支援以下作業系統：
  - Alt 8 SP Server (LKNV.11100-01) 64 位元
  - Alt Server 10 64 位元
  - Astra Linux 特別版 1.7（包括封閉軟體環境模式 和強制模式）64 位元
  - Debian GNU/Linux 11.x (Bullseye) 32 位元 / 64 位元
  - Ubuntu Server 20.04 LTS (Focal Fossa) 64 位元
  - RED OS 7.3 64 位元
  - RED OS 7.3 Server 64 位元
  - RED OS 7.3 Certified Edition 64 位元

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。

關於卡巴斯基安全管理中心 14 網頁主控台

卡巴斯基安全管理中心 14 網頁主控台是一個網路應用程式，設計用於管理由 Kaspersky 應用程式防護的網路的安全系統狀態。

使用該應用程式，您可以執行以下操作：

- 管理組織的安全系統狀態。
- 將 Kaspersky 程式安裝到您網路上的裝置並管理已安裝的應用程式。
- 管理為您網路中的裝置所建立的政策。
- 管理使用者帳戶。

- 管理安裝在您的網路裝置上的應用程式工作。
- 檢視關於安全系統狀態的報告。
- 管理向系統管理員和其他 IT 專家傳送報告的行為。

卡巴斯基安全管理中心 14 網頁主控台是一個網路頁面，可確保您的裝置和管理伺服器能夠透過瀏覽器進行通訊。管理伺服器是一個旨在對您網路中的裝置上安裝的 Kaspersky 應用程式管理的應用程式。管理伺服器透過安全通訊協定（SSL）防護的通道連線到您的網路裝置。當您使用瀏覽器連線至卡巴斯基安全管理中心 14 網頁主控台時，瀏覽器會建立與卡巴斯基安全管理中心 14 網頁主控台伺服器的連線。

你按以下方式操作卡巴斯基安全管理中心 14 網頁主控台：

1. 使用瀏覽器連線至卡巴斯基安全管理中心 14 網頁主控台，其中顯示了 Web 入口的介面。
2. 使用網頁入口控件選取您想要執行的指令。卡巴斯基安全管理中心 14 網頁主控台執行以下操作：
   - 如果您已選取用於接收資訊的指令（例如，檢視裝置清單），卡巴斯基安全管理中心 14 網頁主控台會向管理伺服器傳送一個資訊請求，接收必要資料，然後將其以適合檢視的格式傳送到瀏覽器。
   - 如果您已選取用於管理的指令（例如，遠端安裝應用程式），卡巴斯基安全管理中心 14 網頁主控台會從瀏覽器接收該指令並將其傳送至管理伺服器。然後，應用程式從管理伺服器接收結果並以易於檢視的格式將其傳送到瀏覽器。

卡巴斯基安全管理中心 14 網頁主控台是一個多語言的應用程式。您可以在任意時刻變更介面語言，而不重新開啟應用程式。當您將卡巴斯基安全管理中心 14 網頁主控台與卡巴斯基安全管理中心一起安裝時，卡巴斯基安全管理中心 14 網頁主控台具有和安裝檔案一樣的介面語言。當您僅安裝卡巴斯基安全管理中心 14 網頁主控台時，應用程式具有和您的作業系統一樣的介面語言。若卡巴斯基安全管理中心 14 網頁主控台不支援安裝檔案或作業系統的語言，預設會設定為英文。

支援的 Kaspersky 應用程式清單

卡巴斯基安全管理中心 Linux 支援集中部署和管理 Kaspersky Endpoint Security for Linux。此應用程式允許防護工作站和檔案伺服器。請參閱適用於應用程式版本的產品支援生命週期網頁。

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。

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	
	基於 Windows 的解決方案	基於 Linux 的解決方案
管理伺服器地點	內部部署	內部部署
資料庫管理系統 (DBMS) 地點	內部部署	內部部署
在其上安裝管理伺服器的作業系統	Windows	Linux
管理主控台類型	內部部署和基於 Web	基於 Web
在其上安裝基於 Web 的管理主控台的作業系統	Windows 或 Linux	Windows 或 Linux
管理伺服器階層	✓	✓
管理群組階層	✓	✓
網路輪詢	✓	✓（僅按 IP 範圍）
受管理裝置的最大數量	100000	20000
對受 Windows、macOS 和 Linux 管理的裝置的防護	✓	—（僅防護 Linux 裝置）
對行動裝置的防護	✓	—
對虛擬機的防護	✓	—
對公有雲端基礎結構的防護	✓	—
以裝置為中心的安全管理	✓	✓
以使用者為中心的安全管理	✓	✓
應用程式政策	✓	✓

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	✓	✓
支援虛擬管理伺服器	✓	✓
安裝協力廠商軟體更新和修復協力廠商軟體弱點	✓	— （僅透過使用遠端安裝工作）
有關發生在受管裝置上的事件的通知	✓	✓
建立和管理使用者帳戶	✓	✓
監控政策和工作狀態	✓	✓
部署 Kaspersky 容錯移轉叢集	✓	✓

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

管理伺服器會執行下列功能：

- 儲存管理群組結構
- 儲存關於用戶端裝置設定的資訊
- 應用程式分發套件的儲存結構
- 將應用程式遠端安裝至用戶端裝置和遠端移除應用程式
- 更新 Kaspersky 應用程式的程式資料庫和軟體模組
- 管理用戶端裝置上的政策和工作
- 儲存有關用戶端裝置上已發生事件的資訊
- 產生有關 Kaspersky 應用程式操作的報告
- 向用戶端裝置佈署授權金鑰並儲存授權金鑰資訊
- 有關工作處理程序的通知轉發（例如在用戶端裝置上偵測到病毒）

在應用程式介面命名管理伺服器

在卡巴斯基安全管理中心 14 網頁主控台介面中，管理伺服器可以擁有以下名稱：

- 管理伺服器裝置的名稱，例如："*device_name*" 或 "Administration Server: *device_name*"。
- 管理伺服器裝置的 IP 位址，例如："*IP_address*" 或 "Administration Server: *IP_address*"。
- 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 14 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 14 網頁主控台連線到管理伺服器。

管理伺服器階層

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

*虛擬管理伺服器*是次要管理伺服器的一個特例。

在階層架構中，卡巴斯基安全管理中心 Linux 管理伺服器只能作為從屬伺服器工作，由基於 Windows 的卡巴斯基安全管理中心或卡巴斯基安全管理中心雲端主控台的主管理伺服器管理。

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。
- 服務提供商如何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 14 網頁主控台。為了管理大量的多個不同體系和公司的用戶端裝置，更可在管理伺服器階級中新增虛擬管理伺服器。

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任務，以及更新掃描和下載任務。
- 虛擬伺服器無法建立次要管理伺服器（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。

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://<網頁伺服器名稱>:<HTTPS 連接埠>/public/<物件>

其中：

- <網頁伺服器名稱>為卡巴斯基安全管理中心網頁伺服器的名稱。
- <HTTPS 連接埠>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。
- <物件>是使用者可以存取的檔案或子資料夾。

管理員可以以任意方式例如電子郵件等方式將新連結傳送給使用者。

透過點擊連結，使用者可將所需資訊下載至本機裝置。

網路代理

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

網路代理作為系統服務安裝在裝置上，且具有以下內容：

- 名稱為"卡巴斯基安全管理中心 13.1 Linux 網路代理"
- 設定隨作業系統啟動而自動啟動
- 使用 LocalSystem 帳戶

安裝了網路代理的裝置被稱為*受管理裝置*或*裝置*。您可以從以下來源之一安裝網路代理：

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

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

網路代理啟動的處理程序名稱如下：

- klnagent64.service（對於 64 位元作業系統）
- klnagent.service（對於 32 位元作業系統）

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

管理群組

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

管理群組內的所有受管理裝置都被配置以做如下事情：

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

受管理裝置只能屬於一個管理群組。

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

受管理裝置

一個*受管理裝置*是一台執行 Linux 並安裝了網路代理的電腦。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。一個管理伺服器可以管理最多 20,000 台裝置。

未配置的裝置

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

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

管理員工作站

安裝了卡巴斯基安全管理中心 14 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 14 網頁主控台對 Kaspersky 軟體進行遠端管理。在下文中，管理 Web 外掛程式也稱為*管理外掛程式*。管理外掛程式是卡巴斯基安全管理中心 14 網頁主控台和特定 Kaspersky 應用程式之間的介面。使用管理外掛程式，您可以配置應用程式工作和政策。

您可以從卡巴斯基客戶服務網頁 下載管理 Web 外掛程式。

管理外掛程式提供以下：

- 建立並編輯應用程式工作和設定的介面
- 建立和編輯政策和政策設定檔以便遠端和集中配置 Kaspersky 應用程式和裝置的介面
- 應用程式事件傳輸
- 卡巴斯基安全管理中心 14 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，當不同場合僅假設更改多個設定時，您可以使用政策設定檔。

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

政策設定檔會根據以下規則執行：

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

- 政策可以包含最多 100 個設定檔。

政策設定檔

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

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

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

工作

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

特定應用程式的工作僅在安裝了該應用程式的管理外掛程式時可以被建立。

工作可以在管理伺服器和裝置上執行。

以下工作管理伺服器上執行：

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

以下類型的工作在裝置上執行：

- *本機工作* — 在特定裝置上執行的工作。

  本機工作可以被管理員使用卡巴斯基安全管理中心 14 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次要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。

- 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。

所有用戶端裝置是否使用相同的設定（請參閱下圖）可由政策內容項目的鎖定（🔒）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。

政策和本機應用程式設定

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。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。

檔案透過 HTTP 或者 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*的事件。事件將被發佈在裝置內容中，在**事件註記**區域。

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

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

作為發佈點的裝置必須被防護，包括實體防護，以防範非授權的存取。

連線閘道

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

連線閘道最多可以接收來自 10,000 台裝置的連線。

您可以使用兩個選項來使用連線閘道：

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

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

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

所有連線閘道都包含在管理伺服器內容的發佈點清單中。

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

產品授權

本節提供關於卡巴斯基安全管理中心 14 Linux 產品授權的一般概念資訊。

關於最終使用者產品授權協議

最終使用者產品授權協議（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。

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。

  請注意，當您安裝 Linux 網路代理時，網路代理的最終使用者產品授權協議以英文顯示。在安裝過程中，在接受最終使用者產品授權協議的條款之前，您可以在 /opt/kaspersky/klnagent64/share/license 資料夾中查看其他語言的網路代理最終使用者產品授權協議。

- 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。

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*根據使用者授權協議條款授予在有限時間內使用本程式的權限。

產品授權賦予您以下類型的服務：

- 請按照最終使用者產品授權協議中的條款使用該應用程式
- 取得技術支援

服務範圍和有效期取決於用於啟動該程式的產品授權類型。

我們提供下列授權類型：

- *試用版* – 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。

  您只能為此應用程式啟動一次試用授權。

- *正式版* – 購買該程式時取得的付費產品授權。

  正式版產品授權期限到期後，該程式將在受限功能模式下繼續執行（範例，卡巴斯基安全管理中心資料庫更新將不可用）。要繼續使用卡巴斯基安全管理中心的所有功能，您必須續費您的正式產品授權。

我們建議在產品授權到期之前進行續約，以確保對您的電腦持續保有最佳防護。

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文件。

產品授權憑證提供以下的產品授權資訊：

- 產品授權金鑰或訂購號
- 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安裝資料夾的 license.txt 檔案中。
- privacy_policy.txt 檔案可在受管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作為卡巴斯基應用程式的一部分提供，用於防護企業網路。您也可以從 Kaspersky 網站下載。

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。
- 建立一個管理組層級結構，作為一個單一實體管理特定裝置。
- 控制群組的病毒防護狀態。
- 遠端安裝應用程式。
- 檢視可用於遠端安裝的作業系統映像檔的清單。
- 對安裝在用戶端裝置上的應用程式的集中配置。
- 檢視和編輯現有的已授權的應用程式群組。

- 擷取統計資料和應用程式執行報告，以及緊急事件通知。
- 手動檢視和編輯網路偵測到的硬體裝置清單。
- 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。
- 管理使用者角色。

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

傳輸至權利所有人的資料

在卡巴斯基安全管理中心14 Linux 最終使用者產品授權協議中提供。

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
- 在裝置上啟動 Kaspersky 應用程式
- 管理使用者帳戶
- 檢視卡巴斯基應用程式在裝置上的操作相關資訊
- 檢視報告

若要執行其主要功能，卡巴斯基安全管理中心 Linux 可以接收、儲存和處理下列資訊：

- 組織網路中的裝置相關資訊，在網路中作為裝置發現結果透過掃描 IP 間隔來接收。管理伺服器自行取得資料或接收來自網路代理的資料。
- 受管理裝置的詳細資料。網路代理將下列資料從裝置傳輸至管理伺服器。使用者在卡巴斯基安全管理中心 14 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、DNS 網域和 DNS 名稱、IPv4 位址、IPv6 位址、網路位置、MAC 位址、作業系統類型、裝置是否為虛擬機以及 hypervisor 類型、以及裝置是否為屬於 VDI 的動態虛擬機。
  - 稽核受管理裝置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。
  - 受管理裝置的動作詳細資訊：上次更新的日期和時間、網路中上次顯示裝置的時間、重新啟動等待狀態以及裝置開啟時間。
  - 裝置使用者帳戶和其工作階段的詳情。
- 若裝置是發佈點，也包括發佈點操作統計資料。網路代理將資料從裝置傳輸至管理伺服器。

- 使用者在卡巴斯基安全管理中心 14 網頁主控台中輸入的發佈點設定。
- 安裝到裝置的 Kaspersky 應用程式詳情。受管理應用程式透過網路代理將資料從裝置傳輸至管理伺服器：
  - 安裝在受管理裝置上的 Kaspersky 應用程式設定：Kaspersky 應用程式名稱和版本、狀態、即時防護狀態、上次裝置掃描日期和時間、威脅偵測數量、物件消毒失敗數量、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。
- 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 14 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 14 網頁主控台介面中輸入資料。
- 弱點和修補程式管理功能處理的資料。網路代理將有關受管理裝置上偵測到的硬體相關資訊（硬體登錄資料）從裝置傳輸到管理伺服器。
- 應用程式使用者類別。使用者在卡巴斯基安全管理中心 14 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。
- 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。
- 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。
- 輸入的啟動碼詳細資訊。使用者在管理主控台或卡巴斯基安全管理中心 14 網頁主控台介面中輸入資料。
- 使用者帳戶：名稱、說明、全名、電子郵件地址、主要電話號碼和密碼。使用者在卡巴斯基安全管理中心 14 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 14 網頁主控台介面中輸入資料。
- 已刪除之管理物件的登錄資料。使用者在卡巴斯基安全管理中心 14 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 14 網頁主控台介面中輸入資料。
- 在卡巴斯基安全管理中心 14 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 14 網頁主控台介面中輸入資料。
- 卡巴斯基安全管理中心 14 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 14 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 14 網頁主控台介面中輸入資料。
- 卡巴斯基安全管理中心 Linux 元件的卡巴斯基事件記錄和卡巴斯基受管理應用程式。卡巴斯基事件記錄儲存在各裝置上，從未傳輸至管理伺服器。
- 與受管理裝置和卡巴斯基安全管理中心 Linux 元件的安全連線憑證。使用者在卡巴斯基安全管理中心 14 網頁主控台介面中輸入資料。
- 使用者在卡巴斯基安全管理中心 14 網頁主控台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 14 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 14 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。
- 發佈點指派的管理伺服器和網路代理取得關於網路裝置的資訊。

列出的資料儲存在管理伺服器資料庫。使用者名稱和密碼以加密格式儲存。

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。

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。

依照管理主控台或卡巴斯基安全管理中心 14 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。您可以在服務提供商網站續約您的訂購。

超出了產品授權限制事件

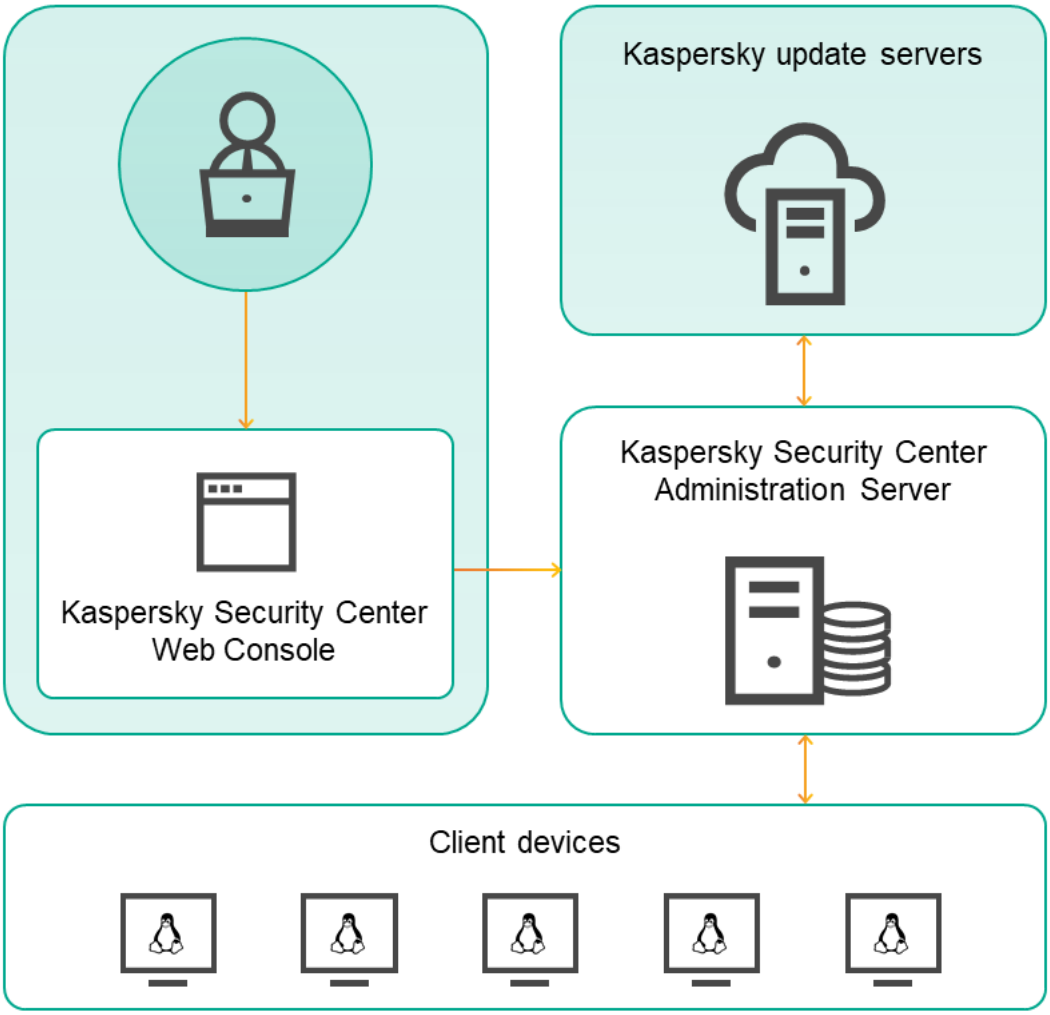
卡巴斯基安全管理中心 Linux 允許您獲取用戶端裝置上安裝的 Kaspersky 應用程式的產品授權達到限制的事件資訊。

產品授權達到限制的此類事件的重要級別依據以下規則定義：

- 如果目前使用單一產品授權的單元的數量達到該產品授權所覆蓋的單元總數的 90% 和 100% 之間，事件等級就是**資訊**重要等級。
- 如果目前使用單一產品授權的單元的數量達到該產品授權所覆蓋的單元總數的 100% 和 110% 之間，事件等級就是**警告**重要等級。
- 如果目前使用單一產品授權的單元的數量超過該產品授權所覆蓋的單元總數的 110%，事件等級就是**緊急事件**重要級別。

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。



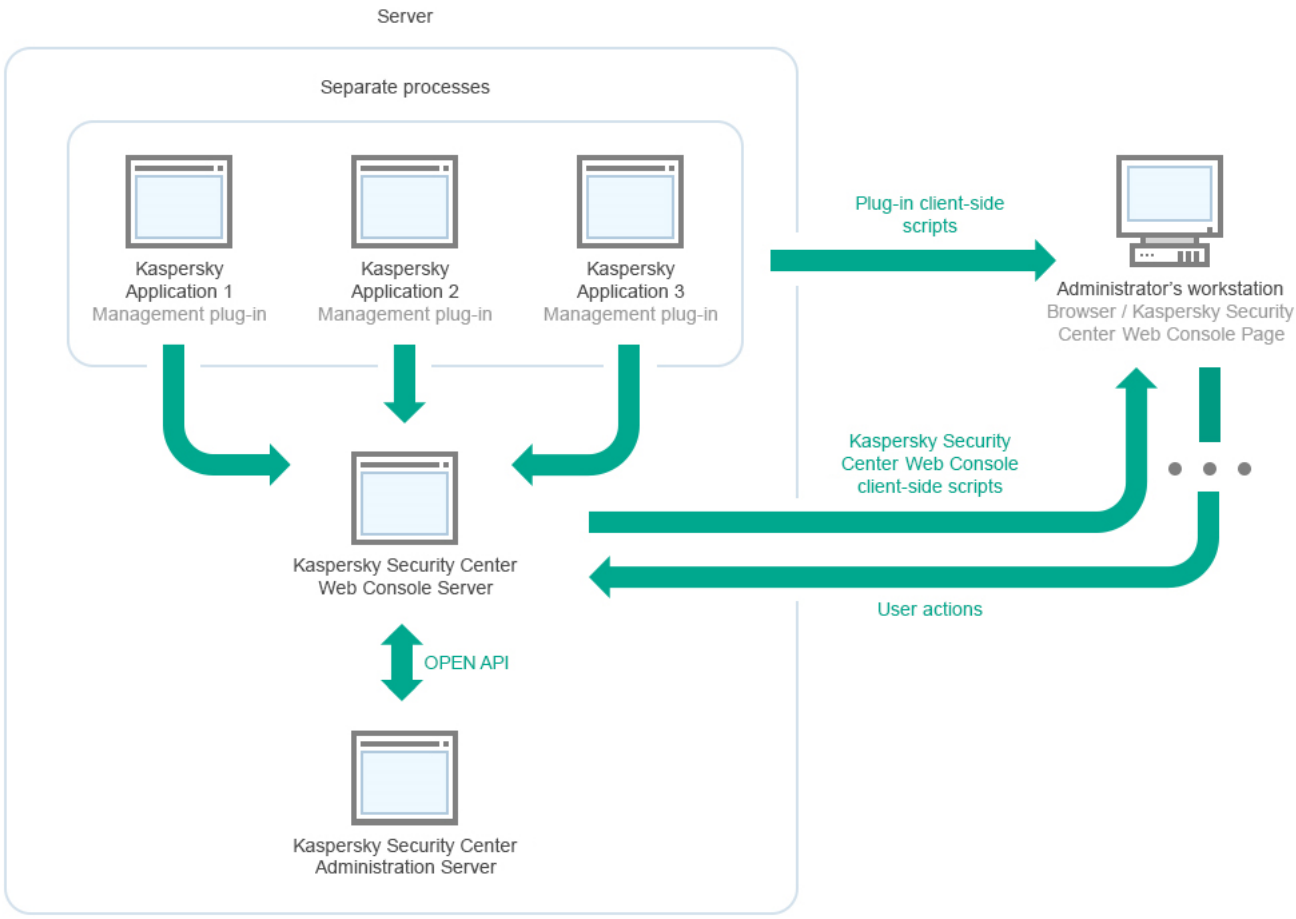
卡巴斯基安全管理中心 14 Linux 架構

卡巴斯基安全管理中心 14 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 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 14 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管理伺服器佈署圖表和卡巴斯基安全管理中心 14 網頁主控台

下圖顯示卡巴斯基安全管理中心管理伺服器佈署圖表和卡巴斯基安全管理中心 14 網頁主控台



卡巴斯基安全管理中心管理伺服器佈署圖表和卡巴斯基安全管理中心 14 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 14 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 14 網頁主控台。

當您在卡巴斯基安全管理中心 14 網頁主控台中執行特定操作時，卡巴斯基安全管理中心 14 網頁主控台伺服器會與卡巴斯基安全管理中心管理伺服器透過 OpenAPI 通訊。卡巴斯基安全管理中心 14 網頁主控台伺服器會從卡巴斯基安全管理中心管理伺服器要求必要資訊，並在卡巴斯基安全管理中心 14 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

下表顯示在管理伺服器和用戶端裝置上必須開啟的預設連接埠。如果願意，您可以變更每個預設連接埠號。

卡巴斯基安全管理中心 Linux 管理伺服器使用的連接埠

埠號	開啟連接埠的處理程序名稱	協定	連接埠目的	範圍
8060	klcsweb	TCP	傳輸發佈的安裝套件到用戶端裝置	發佈安裝套件 您可以在管理伺服器內容視窗的**網頁伺服器**區域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**區域中變更預設連接埠號。
13000	klserver	TCP (TLS)	從網路代理和次要管理伺服器接收連線；也用於在次要管理伺服器上從主管理伺服器接收連線（例如，如果次要管理伺服器在 DMZ 中）	管理用戶端裝置和從屬管理伺服器 您可以在安裝 Kaspersky Security Center 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。
13299	klserver	TCP (TLS)	接收從卡巴斯基安全管理中心 14 網頁主控台到管理伺服器的連線；接收透過	卡巴斯基安全管理中心 14 網頁主控台，OpenAPI。

			OpenAPI 到管理伺服器的連線	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 Kaspersky Security Center 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。
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屬性視窗中更改預設埠號。
15111（僅在裝置上執行 KSN 代理服務時）	ksnproxy	UDP	接收從受管理裝置到 KSN 代理伺服器的請求	KSN 代理伺服器。 您可以在管理伺服器屬性視窗中更改預設埠號。
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）。
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 14 網頁主控台遠端連線受管理裝置。 您可以使用 klscflag 實用程式變更預設連接埠號。

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

下表顯示了必須在 Kaspersky Security Center Linux 網頁主控台伺服器開啟的連接埠。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 Linux 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 14 網頁主控台的連線	卡巴斯基安全管理中心 14 網頁主控台。 您可以在安裝卡巴斯基安全管理中心 14 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 14 網頁主控台，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。

下表顯示了在安裝了網路代理的受管理裝置上必須開啟的連接埠。

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。

下表顯示在安裝了網路代理作為發佈點的受管理裝置上必須開啟的連接埠。除了網路代理使用的連接埠外，列出的連接埠必須在發佈點裝置上開啟（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)	接收從網路代理的連線	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。

卡巴斯基安全管理中心 14 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 14 網頁主控台伺服器（又稱為卡巴斯基安全管理中心 14 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 14 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	KSCWebConsolePlugin	HTTPS	被管理外掛程式處理程序用來接收來自 KSCWebConsoleManagementService 的請求的 API 連接埠	執行管理外掛程式的 node.exe 處理程序
1329，2003	KSCWebConsoleManagementService	HTTPS	用來接收在相同裝置上執行之 KSCWebConsole 服務的要求的 API 連接埠	更新卡巴斯基安全管理中心 14 網頁主控台元件
2005	KSCWebConsole	HTTPS	用來接收在相同裝置上執行之 KSCWebConsoleManagementService service 的要求的 API 連接埠	執行卡巴斯基安全管理中心 14 網頁主控台的 node.exe 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 14 網頁主控台並更新卡巴斯基安全管理中心 14 網頁主控台元件
4150, 4151, 4152	KSCWebConsoleMessageQueue	HTTPS	處理卡巴斯基安全管理中心 14 網頁主控台和管理外掛程式之間通訊所用的訊息代理 API 連接埠	卡巴斯基安全管理中心 14 網頁主控台和管理外掛程式之間的互動

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 14 網頁主控台的安裝。

主要安裝情境

透過遵循此情境，您可以安裝卡巴斯基安全管理中心 14 Linux 管理伺服器和卡巴斯基安全管理中心 14 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 14 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將使用的 DBMS，或者使用現有資料庫。

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**

   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中心在裝置上。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 14 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14 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 14 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14 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生成報告，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。

按住資料庫管理系統。

安裝卡巴斯基安全管理中心將使用的資料庫管理系統（DBMS）。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。

如果使用 MariaDB，您需要配置建議的設定以便 DBMS 與卡巴斯基安全管理中心工作最佳。

設定 MariaDB x64 伺服器以與卡巴斯基安全管理中心 14 Linux 一起使用

如果您將 MariaDB 伺服器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

要設定 my.cnf 檔案：

1. 在文字編輯器中開啟 my.cnf 檔案。

2. 在 my.cnf 檔案中輸入以下幾行：
```
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=< value >
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
```
"innodb_buffer_pool_size"的值必須不少於預期之 KAV 資料庫大小的 80%。

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。

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

要檢查是否啟用了最佳化程式附加元件：

1. 在 MariaDB 用戶端主控台中，執行以下命令：
```
SELECT @@optimizer_switch;
```

2. 確保其輸出包含以下幾行：
```
join_cache_incremental=on
join_cache_hashed=on
join_cache_bka=on
```
如果存在這幾行並啟用了這些值，則會啟用最佳化程式附加元件。

如果這幾行不見了或其值為 off，您需要執行以下幾點：

   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'
```

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

安裝卡巴斯基安全管理中心

該過程描述了如何安裝卡巴斯基安全管理中心。

安裝前：

- 安裝資料庫管理系統。
- 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 版本。

使用安裝檔案—ksc-[版本號]_amd64.deb 或 ksc-[版本號].x86_64.rpm—對應於您裝置上的 Linux 版本。您透過從 Kaspersky 網站下載來接收安裝檔案。

要卡巴斯基安全管理中心：

1. 在命令行中，在具有 root 權限的帳戶下執行本指令中提供的命令。

2. 建立一個群組"kladmins"和一個無權限帳戶"ksc"。該帳戶必須是"kladmins"群組的成員。為此，請依次執行以下命令：
```
# adduser ksc
# groupadd kladmins
# gpasswd -a ksc kladmins
# usermod -g kladmins ksc
```

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

   - `# apt install /<path>/ksc64_[ version_number ]_amd64.deb`
   - `# yum install /<path>/ksc64-[ version_number ].x86_64.rpm -y`

4. 執行卡巴斯基安全管理中心配置：

   ```
   # /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，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，您必須接受隱私政策的條款。

6. 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 個聯網裝置，請輸入 1。
      - 如果您有 101 到 1000 個聯網裝置，請輸入 2。
      - 如果您有超過 1000 台聯網裝置，請輸入 3。

   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. 輸入在其上安裝資料庫的裝置的 IP 位址。

   i. 輸入資料庫連接埠號。此連接埠用於與管理伺服器通信。預設情況下使用連接埠 3306。

   j. 輸入資料庫名稱。

   k. 輸入您用於存取資料庫的資料庫根帳戶的登入名稱。

   l. 輸入您用於存取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`

   m. 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 16 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 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

使用者已新增，卡巴斯基安全管理中心已安裝。

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`

安裝卡巴斯基安全管理中心 14 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 14 網頁主控台伺服器（也叫卡巴斯基安全管理中心 14 網頁主控台）到執行 Linux 作業系統的裝置。安裝之前，您必須安裝了資料庫管理系統和卡巴斯基安全管理中心管理伺服器。

使用與您裝置上安裝的 Linux 發佈相對應的以下安裝檔案之一：

- 對於 Debian—ksc-web-console-[build_number].x86_64.deb
- 對於基於 RPM 的作業系統—ksc-web-console-[build_number].x86_64.rpm
- 對於 Alt 8—SP-ksc-web-console-[build_number]-alt8p.x86_64.rpm

您透過從 Kaspersky 網站下載來接收安裝檔案。

要安裝卡巴斯基安全管理中心 14 網頁主控台：

1. 確保您要安裝卡巴斯基安全管理中心 14 網頁主控台的裝置執行支援的 Linux 分類。
2. 閱讀安裝套件中的最終使用者產品授權協議 (EULA)（file /var/opt/kaspersky/ksc-web-console/license-<XX>.txt，其中<XX>是語言代碼）。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 14 網頁主控台到管理伺服器。命名該檔案為 ksc-web-console-setup.json 並將其放置到以下目錄：/etc/ksc-web-console-setup.json。

   回應檔案的一個例子，它包含最小參數集以及預設位址和連接埠：

   ```
   {
     "address": "127.0.0.1",
     "port": 8080,
     "trusted": "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC Server",
     "acceptEula": true
   }
   ```

   在 Linux ALT 作業系統上安裝卡巴斯基安全管理中心 14 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 14 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 14 網頁主控台，執行以下指令：
     ```
     $ sudo dpkg -i ksc-web-console-[build_number].x86_64.deb
     ```
   - 要從 .rpm 檔案安裝卡巴斯基安全管理中心 14 網頁主控台，執行以下指令之一：
     ```
     $ sudo rpm -ivh --nodeps ksc-web-console-[build_number].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 rpm -Uvh --nodeps --force ksc-web-console-[build_number].x86_64.rpm
       ```

- 對於執行基於 Debian 的作業系統的裝置：
  ```
  $ sudo dpkg -i ksc-web-console-[build_number].x86_64.deb
  ```

這會開始解壓縮安裝檔案。請等待安裝完成。卡巴斯基安全管理中心 14 網頁主控台被安裝到以下目錄：/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 14 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 14 網頁主控台。

卡巴斯基安全管理中心 14 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 14 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 14 網頁主控台到管理伺服器的參數的 .json 檔案。

這裡是回應檔案的一個例子，它包含最小參數集以及預設位址和連接埠：

```
{
  "address": "127.0.0.1",
  "port": 8080,
  "defaultLangId": 1049,
  "enableLog": false,
  "trusted": "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC Server",
  "acceptEula": true,
  "certPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer",
  "webConsoleAccount": "Group1:User1",
  "managementServiceAccount": "Group1:User2",
  “serviceWebConsoleAccount”："Group1:User3",
  "pluginAccount"："Group1:User4",
  "messageQueueAccount"： "Group1:User5"
}
```

在 Linux ALT 作業系統上安裝卡巴斯基安全管理中心 14 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 14 網頁主控台到執行 Linux 的裝置的參數

參數	敘述	可用值
`address`	卡巴斯基安全管理中心 14 網頁主控台伺服器（必需）。	字串值。
連接埠	卡巴斯基安全管理中心 14 網頁主控台將用於連線到管理伺服器的連接埠號（必需）。	數值。
`defaultLangId`	使用者介面語言（預設，`1033`）。	語言數位： • 德語：`1031` • 英語：`1033` • 西班牙語：`3082` • 西班牙語（墨西哥）：`2058` • 法語：`1036` • 日語：`1041` • 哈薩克語：`1087` • 波蘭語：`1045` • 葡萄牙語（巴西）：`1046` • 俄語：`1049` • 土耳其語：`1055` • 簡體中文：`4`

		• 繁體中文：31748 如果沒有指定值，則使用 English（en-US）語言
enableLog	是否要啟用卡巴斯基安全管理中心 14 網頁主控台活動記錄。	布爾值： • true—啟用記錄（預設選中）。 • false—停用記錄。
trusted	允許連線卡巴斯基安全管理中心 14 網頁主控台的信任的管理伺服器清單。各管理伺服器必須以下列參數定義： • 管理伺服器位址 • 卡巴斯基安全管理中心 14 網頁主控台用以連線到管理伺服器的 OpenAPI 連接埠（預設是 13299） • 管理伺服器憑證路徑 • 將顯示在登入視窗的管理伺服器名稱 參數使用豎線分隔。如果指定了幾個管理伺服器，使用兩個豎線將它們分隔。	以下格式的字串值： " "伺服器位址|連接埠|憑證路徑|伺服器名稱" "。 例如： "X.X.X.X|13299|/cert/server-1.cer|Server 1||Y.Y.Y.Y|13299|/cert/server-2.cer|Server 2"。
acceptEula	您是否要接受最終使用者產品授權協議（EULA）的條款。包含 EULA 條款的檔案和安裝檔案一起下載。	布爾值： • true—我已完整閱讀、瞭解和接受最終使用者產品授權協議的條款。 • false—我不接受產品授權協議的條款（預設選取）。
certDomain	如果您要產生新憑證，使用該參數指定產生新憑證的網域名稱。	字串值。
certPath	如果您要使用現有憑證，使用該參數指定憑證檔案位置	字串值。 指定路徑 “/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer” 以使用現有憑證。對於自訂憑證，請指定儲存此自訂憑證的路徑。
keyPath	如果您要使用現有憑證，使用該參數指定金鑰檔案位置	字串值。
webConsoleAccount	KSCWebConsole服務執行時使用的帳戶的名稱。	以下格式的字串值：“群組名稱:使用者名稱”。 例如："Group1:User1"。 如果未指定任何值，卡巴斯基安全管理中心 14 網頁主控台安裝程式會建立一個預設名稱為 user_management_%uid% 的新帳戶。
managementServiceAccount	KSCWebConsole服務執行時使用的權限帳戶的名稱。	以下格式的字串值：“群組名稱:使用者名稱”。 例如："Group1:User1"。 如果未指定任何值，卡巴斯基安全管理中心 14 網頁主控台安裝程式會建立一個預設名稱為 user_nodejs_%uid% 的新帳戶。
serviceWebConsoleAccount	KSCSvcWebConsole服務執行時使用的帳戶的名稱。	以下格式的字串值：“群組名稱:使用者名稱”。 例如："Group1:User1"。 如果未指定任何值，卡巴斯基安全管理中心 14 網頁主控台安裝程式會建立一個預設名稱為 user_svc_nodejs_%uid% 的新帳戶。
pluginAccount	KSCWebConsolePlugin服務執行時使用的帳戶的名稱。	以下格式的字串值：“群組名稱:使用者名稱”。 例如："Group1:User1"。 如果未指定任何值，卡巴斯基安全管理中心 14 網頁主控台安裝程式會建立一個預設名稱為 user_web_plugin_%uid% 的新帳戶。
messageQueueAccount	KSCWebConsoleMessageQueue服務執行時使用的帳戶的名稱。	以下格式的字串值：“群組名稱:使用者名稱”。 例如："Group1:User1"。 如果未指定任何值，卡巴斯基安全管理中心 14 網頁主控台安裝程式會建立一個預設名稱為 user_message_queue_%uid% 的新帳戶。

如果您指定 `webConsoleAccount`、`managementServiceAccount`、`serviceWebConsoleAccount`、`pluginAccount` 或 `messageQueueAccount` 參數，請確保自訂使用者帳戶屬於同一安全組。如果未指定這些參數，卡巴斯基安全管理中心 14 網頁主控台安裝程式會建立一個預設安全組，然後在該組中建立具有預設名稱的使用者帳戶。

使用 DBMS 的帳戶

下表提供了有關選擇用於 MariaDB DBMS 的帳戶內容的資訊。

本機 DBMS 是安裝在管理伺服器裝置的 DBMS。*遠端 DBMS* 是安裝在其他裝置上的 DBMS。

請在啟動管理伺服器服務之前授予管理伺服器帳戶所需的所有權限。

DBMS：MariaDB

DBMS 位置	本機或遠端。	本機或遠端。
誰建立 KAV 資料庫	安裝程式（自動）。	管理員（手動）。
執行安裝程式的帳戶	本機或網域，具有本機管理員權限。	本機或網域，具有本機管理員權限。
管理伺服器服務帳戶	本機或網域。	本機或網域。
安裝程式和管理伺服器服務用於存取 DBMS 的 DBMS 內部帳戶的權限	需要根存取權限。	對於 KAV 資料庫，全部授予；對於系統表，選擇, 顯示視圖, 處理。

部署 Kaspersky 容錯移轉叢集

本節包含關於 Kaspersky 容錯移轉叢集的一般信息，以及有關在您的網路中準備和部署 Kaspersky 容錯移轉叢集的指示。

情境：部署 Kaspersky 容錯移轉叢集

Kaspersky 容錯移轉叢集提供卡巴斯基安全管理中心的高可用性，並在出現故障時最大限度地減少管理伺服器的停機時間。容錯移轉叢集基於安裝在兩台電腦上的兩個相同的卡巴斯基安全管理中心例項。其中一個例項用作主動節點，另一個例項用作被動節點。主動節點負責管理用戶端裝置的防護，而被動節點則準備在主動節點出現故障時承擔主動節點的所有功能。當發生故障時，被動節點變為主動節點，主動節點變為被動節點。

先決條件

您擁有滿足容錯移轉叢集要求的硬體。

Kaspersky 應用程式佈署分步驟進行：

1. **為卡巴斯基安全管理中心服務建立帳戶**

   建立一個新的網域使用者帳戶或選擇一個現有的網域使用者帳戶，在該帳戶下執行卡巴斯基安全管理中心服務。在每個節點和檔案伺服器上的本機管理員群組中新增所選帳戶。

2. **檔案伺服器準備**

   準備檔案伺服器作為 Kaspersky 容錯移轉叢集的一個元件。確保檔案伺服器滿足硬體和軟體要求，為卡巴斯基安全管理中心 資料建立兩個共用資料夾，並配置存取共用資料夾的權限。

   說明：為 Kaspersky 容錯移轉叢集準備檔案伺服器

3. **準備主動和被動節點**

   準備兩台具有相同硬體和軟體的電腦作為主動節點和被動節點。

   說明：為 Kaspersky 容錯移轉叢集準備節點

4. **資料庫管理系統 (DBMS) 安裝**

   您有兩種選擇：

   - 如果您想使用 MariaDB Galera Cluster，則不需要專門的電腦來執行 DBMS。在每個節點上安裝 MariaDB Galera Cluster。
   - 如果您想使用任何其他受支援的 DBMS，在專用電腦上安裝選定的 DBMS。

5. **卡巴斯基安全管理中心安裝**

   在兩個節點上以容錯移轉叢集模式安裝卡巴斯基安全管理中心。您必須先在主動節點上安裝卡巴斯基安全管理中心，然後再將其安裝在被動節點上。

6. **測試容錯移轉叢集**

檢查您是否正確配置了容錯移轉叢集以及它是否正常工作。例如，您可以在主動節點上停止卡巴斯基安全管理中心服務之一：kladminserver、klnagent、ksnproxy、klactprx 或 klwebsrv。服務停止後，防護管理必須自動切換到被動節點。

結果

卡巴斯基容錯移轉叢集已部署。請熟悉導致主動節點和被動節點之間切換的事件。

關於 Kaspersky 容錯移轉叢集

Kaspersky 容錯移轉叢集提供卡巴斯基安全管理中心的高可用性，並在出現故障時最大限度地減少管理伺服器的停機時間。容錯移轉叢集基於安裝在兩台電腦上的兩個相同的卡巴斯基安全管理中心例項。其中一個例項用作主動節點，另一個例項用作被動節點。主動節點負責管理用戶端裝置的防護，而被動節點則準備在主動節點出現故障時承擔主動節點的所有功能。當發生故障時，被動節點變為主動節點，主動節點變為被動節點。

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

硬體和軟體需求

若要部署 Kaspersky 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電腦。這些電腦將充當主動節點和被動節點。
- 執行 Linux 的檔案伺服器，具有 EXT4 檔案系統。您必須提供一台用作檔案伺服器的專用電腦。

  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) 的電腦。如果您使用 MariaDB Galera Cluster 作為 DBMS，則不需要為此目的的專用電腦。

切換條件

如果主動節點上發生以下任何事件，容錯移轉叢集會將用戶端裝置的防護管理從主動節點切換到被動節點：

- 主動節點由於軟體或者硬體故障而損壞。
- 主動節點因為維護活動被暫時停止。
- 至少一項卡巴斯基安全管理中心服務（或處理程序）失敗或被使用者故意終止。卡巴斯基安全管理中心服務如下：kladminserver、klnagent、klactprx 和 klwebsrv。
- 主動節點與檔案伺服器上的儲存之間的網路連線被中斷或終止。

為 Kaspersky 容錯移轉叢集準備檔案伺服器

檔案伺服器是 Kaspersky 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）
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的資料和設定。您將在配置卡巴斯基安全管理中心的安裝時指定共用資料夾的路徑。

   執行以下指令：

   ```
   sudo yum install nfs-utils
   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 777 /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 cat /etc/exports
sudo exportfs -a
sudo systemctl start rpcbind
sudo service nfs start
```

透過執行以下命令啟用自動啟動：

```
sudo systemctl enable rpcbind
```

4. 重新啟動檔案伺服器。

檔案伺服器已準備就緒。若要部署 Kaspersky 容錯移轉叢集，請按照此情境中的進一步說明進行操作。

為 Kaspersky 容錯移轉叢集準備節點

準備兩台電腦作為卡巴斯基容錯移轉叢集的主動和被動節點。

要為卡巴斯基容錯移轉叢集準備節點：

1. 確保您有兩台滿足硬體和軟體需求的電腦。這些電腦將充當容錯移轉叢集的主動節點和被動節點。

2. 要使節點充當 NFS 用戶端，請在每個節點上安裝 nfs-utils 套件。

   執行以下指令：

   ```
   sudo yum install nfs-utils
   ```

3. 透過執行以下命令建立掛接點：

   ```
   sudo mkdir -p /mnt/KlFocStateShare
   sudo mkdir -p /mnt/KlFocDataShare_klfoc
   ```

4. 檢查共用資料夾是否可以成功掛載。[可選步驟]

   執行以下指令：

   ```
   sudo mount -t nfs -o vers=4,nolock,local_lock=none,auto,user,rw {server}:{KlFocStateShare 資料夾的路徑}
   /mnt/KlFocStateShare
   sudo mount -t nfs -o vers=4,nolock,local_lock=none,noauto,user,rw {server}:{KlFocDataShare_klfoc 資料夾的路徑}
   /mnt/KlFocDataShare_klfoc
   ```

   此處，{server}:{KlFocStateShare 資料夾的路徑} 和 {server}:{KlFocDataShare_klfoc 資料夾的路徑} 是檔案伺服器上共用資料夾的網路路徑。

   成功掛接共用資料夾後，透過執行以下命令將其卸載：

   ```
   sudo umount /mnt/KlFocStateShare
   sudo umount /mnt/KlFocDataShare_klfoc
   ```

5. 匹配掛接點和共用資料夾：

   ```
   sudo vi /etc/fstab
   {server}:{KlFocStateShare 資料夾的路徑} /mnt/KlFocStateShare nfs vers=4,nolock,local_lock=none,auto,user,rw 0 0
   {server}:{KlFocDataShare_klfoc 資料夾的路徑} /mnt/KlFocDataShare_klfoc nfs
   vers=4,nolock,local_lock=none,noauto,user,rw 0 0
   ```

   此處，{server}:{KlFocStateShare 資料夾的路徑} 和 {server}:{KlFocDataShare_klfoc 資料夾的路徑} 是檔案伺服器上共用資料夾的網路路徑。

6. 重新啟動兩個節點。

7. 透過執行以下命令掛載共用資料夾：

   ```
   mount /mnt/KlFocStateShare
   mount /mnt/KlFocDataShare_klfoc
   ```

8. 確保存取共用資料夾的權限屬於 ksc:kladmins。

   執行以下指令：

   ```
   sudo ls -la /mnt/
   ```

9. 執行以下操作之一：

   - 在每個節點上，建立一個虛擬網路介面卡。例如，執行以下命令：

     a. 透過執行以下命令發現介面名稱：

     ```
     ifconfig
     ```

b. 執行以下指令碼（以下以介面名稱為例）：

```
#!/bin/bash
PHYSICAL_IFACE=ens160
VIRTUAL_IFACE=macvlan1
ip link del $VIRTUAL_IFACE > /dev/null 2>&1
ip link add link $PHYSICAL_IFACE $VIRTUAL_IFACE type macvlan
if [ "$?"-ne "0" ]; then
    echo ERROR adding new virtual adapter $VIRTUAL_IFACE!
    exit $?
fi
ip link set $VIRTUAL_IFACE down
if [ "$?"-ne "0" ]; then
    echo ERROR disabling virtual adapter $VIRTUAL_IFACE!
    exit $?
fi
```

c. 執行以下指令：

```
ip addr add {虛擬網路介面卡的 IP 位址} dev {虛擬網路介面卡的名稱}
```

建立虛擬網路介面卡時，IP 位址必須為空。兩個節點上的虛擬網路介面卡必須具有相同的 IP 位址。

d. 檢查虛擬網路介面卡是否已成功建立。

執行以下指令：

```
ip link set macvlan1 up
ifconfig
```

e. 透過執行以下命令停用虛擬網路介面卡：

```
ip link set macvlan1 down
```

- 使用協力廠商負載均衡器。例如，您可以使用 nginx 伺服器。在這種情況下，請執行以下操作：

  a. 提供一台安裝了 nginx 的基於 Linux 的專用電腦。

  b. 配置負載均衡。設定主動節點為主伺服器，被動節點為備份伺服器。

  c. 在 nginx 伺服器上，開啟所有管理伺服器連接埠：TCP 13000, UDP 13000, TCP 13291, TCP 13299, TCP 17000.

節點已準備就緒。若要部署 Kaspersky 容錯移轉叢集，請按照情境中的進一步說明進行操作。

在 Kaspersky 容錯移轉叢集節點上安裝卡巴斯基安全管理中心

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

使用安裝檔案—ksc-[版本號]_amd64.deb 或 ksc-[版本號].x86_64.rpm—對應於您裝置上的 Linux 版本。您透過從 Kaspersky 網站下載來接收安裝檔案。

只有來自 KLAdmins 網域群組的使用者才能在每個節點上安裝 卡巴斯基安全管理中心。

在主（主動）節點上安裝

要在主節點上安裝卡巴斯基安全管理中心：

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 版本。
2. 在命令行中，在具有 root 權限的帳戶下執行本指令中提供的命令。
3. 執行卡巴斯基安全管理中心安裝。根據您的 Linux 版本，執行以下命令之一：
   - `sudo apt install /<path>/ksc64_[ version_number ]_amd64.deb`
   - `sudo yum install /<path>/ksc64-[ version_number ].x86_64.rpm -y`
4. 執行卡巴斯基安全管理中心配置：

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

5. 閱讀 最終使用者產品授權協議 (EULA) 和隱私權政策。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，您必須接受 EULA 的條款。

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

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，輸入以下設定：

a. 輸入狀態共用掛接點的本機路徑。

b. 輸入資料共用掛接點的本機路徑。

c. 選擇容錯移轉叢集連線模式：透過虛擬網路介面卡或外部負載平衡器。

d. 如果您使用虛擬網路介面卡，請輸入其名稱。

e. 當系統提示您輸入管理伺服器 DNS 名稱或靜態 IP 位址時，請輸入虛擬網路介面卡的 IP 位址或外部負載平衡器的 IP 位址。

f. 輸入管理伺服器連接埠號。預設情況下使用連接埠 14000。

g. 輸入管理伺服器 SSL 連接埠號。預設情況下使用連接埠 13000。

h. 評估您打算管理的裝置的大致數量：

- 如果您有 1 到 100 個聯網裝置，請輸入 1。
- 如果您有 101 到 1000 個聯網裝置，請輸入 2。
- 如果您有超過 1000 台聯網裝置，請輸入 3。

i. 輸入服務的安全群組名稱。預設情況下，使用"kladmins"群組。

j. 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。

k. 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。

l. 輸入在其上安裝資料庫的裝置的 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。預設情況下使用連接埠 3306。

n. 輸入資料庫名稱。

o. 輸入您用於存取資料庫的資料庫根帳戶的登入名稱。

p. 輸入您用於存取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

q. 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 16 個字元。

使用者已新增，卡巴斯基安全管理中心已安裝在主節點上。

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：

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 版本。

2. 在命令行中，在具有 root 權限的帳戶下執行本指令中提供的命令。

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

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

4. 執行卡巴斯基安全管理中心配置：

   ```
   sudo /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，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，您必須接受隱私政策的條款。

6. 選擇 **次要集群節點**作為管理伺服器安裝模式。

7. 出現提示時，輸入狀態共用掛接點的本機路徑。

卡巴斯基安全管理中心安裝在次要節點上。

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`

現在，您可以測試卡巴斯基容錯移轉叢集，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 Kaspersky 容錯移轉叢集或臨時分離叢集的一個節點進行維護。如果是這種情況，請按照此節中的說明進行操作。請勿嘗試透過任何其他方式啟動或停止與容錯移轉叢集相關的服務或處理程序。這可能會導致資料丟失。

啟動和停止整個容錯移轉叢集以進行維護

若要啟動或停止整個容錯移轉叢集：

1. 在主動節點上，轉到 /opt/kaspersky/ksc64/sbin。
2. 開啟命令行，然後執行以下命令之一：
   - 若要停止叢集，請執行：`klfoc -stopcluster --stp klfoc`
   - 若要啟動叢集，請執行：`klfoc -startcluster --stp klfoc`

容錯移轉叢集的啟動或停止取決於您執行的命令。

維護節點之一

若要維護節點之一：

1. 在啟動節點上，使用`klfoc -stopcluster --stp klfoc`命令停止容錯移轉叢集。
2. 在您要維護的節點上，轉到 /opt/kaspersky/ksc64/sbin。
3. 開啟命令行，然後透過執行`detach_node.sh`命令將節點從叢集中分離。
4. 在啟動節點上，使用`klfoc -startcluster --stp klfoc`命令啟動容錯移轉叢集。
5. 執行維護活動。
6. 在啟動節點上，使用`klfoc -stopcluster --stp klfoc`命令停止容錯移轉叢集。
7. 在維護的節點上，轉到 /opt/kaspersky/ksc64/sbin。
8. 開啟命令行，然後透過執行`attach_node.cmd` 命令將節點附著到叢集。

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

該節點得到維護並被附著到容錯移轉叢集。

用於卡巴斯基安全管理中心的憑證

本節包含與卡巴斯基安全管理中心憑證相關的資訊，介紹如何發佈和替代卡巴斯基安全管理中心 14 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 14 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
- 網頁伺服器憑證
- 卡巴斯基安全管理中心 14 網頁主控台憑證

預設情況下，卡巴斯基安全管理中心使用自我簽署憑證（即由卡巴斯基安全管理中心本身頒發的憑證），但是您可以用自訂憑證加以替換，以更好地滿足組織網路的要求並符合安全標準。在管理伺服器驗證自訂憑證是否滿足所有適用要求之後，該憑證將承擔與自我簽署憑證相同的功能範圍。唯一的區別是自訂憑證在到期後不會自動重新發行。您可以透過 klsetsrvcert 公用程式或透過卡巴斯基安全管理中心 14 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。

管理伺服器憑證

管理伺服器憑證需要用於以下目的：

- 連線卡巴斯基安全管理中心 14 網頁主控台時驗證管理伺服器的身分
- 受管裝置上管理伺服器和網路代理之間的安全交互
- 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14 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，公用保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。

如果您為管理伺服器憑證指定了超過 397 天的有效期，則 Web 瀏覽器會傳回錯誤。

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。

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置獨立的備份管理伺服器憑證，以在將管理伺服器從一部裝置移至另一部裝置時不會遺失資料。

網頁伺服器憑證

網頁伺服器（卡巴斯基安全管理中心管理伺服器的元件）使用的一種特殊類型憑證。發布網路代理安裝套件（隨後將其下載到受管理裝置）需要此憑證。基於此用途，網頁伺服器可以使用各種憑證。

網頁伺服器按優先級順序使用以下憑證之一：

1. 您透過卡巴斯基安全管理中心 14 網頁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")

卡巴斯基安全管理中心 14 網頁主控台憑證

卡巴斯基安全管理中心 14 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。

卡巴斯基安全管理中心中使用的自訂憑證要求

下表顯示了為卡巴斯基安全管理中心的不同元件指定的自訂憑證的要求。

卡巴斯基安全管理中心憑證要求

憑證類型	要求	註解
一般憑證，一般備用憑證（「C」、「CR」）	最小金鑰長度：2048。 基本限制： • CA：真 • 路徑長度限制：沒有 金鑰使用情況： • 電子簽名 • 憑證籤名 • 金鑰加密 • CRL 簽署 延伸金鑰使用（選填）：伺服器身分驗證、用戶端身分驗證。	延伸金鑰使用參數為選填。 路徑長度限制值可以有別於「無」，但不能小於「1」。
網頁伺服器憑證	延伸金鑰使用：伺服器身分驗證 從中指定憑證的 PKCS # 12 / PEM 容器會包括整個公共金鑰鏈。 出現憑證的主題替代名稱 (SAN)；也就是說， `subjectAltName` 欄位值有效。 該憑證符合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。	不適用。
卡巴斯基安全管理中心 14 網頁主控台憑證	從中指定憑證的 PEM 容器會包括整個公共金鑰鏈。 出現憑證的主題替代名稱 (SAN)；也就是說， `subjectAltName` 欄位值有效。 該憑證符合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 14 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 14 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 14 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 14 網頁主控台憑證。

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

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

若要重新發佈已過期卡巴斯基安全管理中心 14 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 14 網頁主控台：

- 如果想要使用卡巴斯基安全管理中心14 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14 網頁主控台，然後安裝相同的卡巴斯基安全管理中心14 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 14 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 14 網頁主控台憑證

預設下，當您安裝卡巴斯基安全管理中心 14 網頁主控台伺服器（也叫卡巴斯基安全管理中心 14 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 14 網頁主控台的憑證：

1. 建立一個卡巴斯基安全管理中心14 網頁主控台安裝需要的新回應檔案。
2. 在此檔案中，使用 `certPath` 參數和 `keyPath` 參數指定自訂憑證檔案和金鑰檔案的路徑。
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 14 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14 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14 網頁主控台，然後安裝相同的卡巴斯基安全管理中心14 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 14 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 14 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 <filename.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <filename.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 14 網頁主控台不支援受密碼防護的憑證。因此，在基於 OpenSSL 的跨平台實用程式中執行以下命令以從 .pem 文件中刪除複雜密碼：

   ```
   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 14 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。

> 如果您為管理伺服器憑證指定了超過 397 天的有效期，則 Web 瀏覽器會傳回錯誤。

先決條件

新憑證必須以 PKCS#12 格式（例如，透過組織的 PKI）建立，並且必須由受信任的憑證頒發機構 (CA) 頒發。此外，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。對於新憑證，必須滿足以下列出的要求。

憑證類型：一般憑證，一般備用憑證(「C」、「CR」)

要求：

- 最小金鑰長度：2048
- 基本限制：
  - CA：真
  - 路徑長度限制：沒有

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
  - 憑證籤名
  - 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。

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。

結果

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

使用 klsetsrvcert 公用程式替換管理伺服器憑證

要取代管理伺服器憑證：

在命令列下，執行以下公用程式：

```
klsetsrvcert [-t <type> {-i <inputfile> [-p <password>] [-o <chkopt>] | -g <dnsname>}][-f <time>][-r <calistfile>][-l <logfile>]
```

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

下表列出了 klsetsrvcert 公用程式參數的說明。

klsetsrvcert 實用工具參數值

參數	參數值
`-t <type>`	要取代的憑證類型。`<type>` 參數的可能值： • `C` – 取代連接埠 13000 和 13291 的普通憑證。 • `CR` – 取代連接埠 13000 和 13291 的普通預留憑證。
`-f <time>`	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）。 如果要在到期前取代普通或普通儲備證書，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 <輸入檔案>`	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 <chkopt>`	憑證驗證參數（以冒號區隔）。

	要在沒有簽名權限的情況下使用自訂憑證，請在 klsetsrvcert 公用程式中指定 `-o NoCA`。這對於公共 CA 頒發的憑證很有用。
`-g <DNS 名稱>`	新憑證將為指定 DNS 名稱建立。
`-r <calistfile>`	信任的根憑證授權機構清單，格式 PEM。
`-l <記錄檔案>`	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 <inputfile> -p <password> -o NoCA
```

證書被取代後，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。

使用 klmover 公用程式將網路代理連線到管理伺服器

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

要指定新管理伺服器憑證並還原連線：

在命令列下，執行以下公用程式：

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

當網路代理安裝在用戶端裝置上時，此公用程式會自動複製到網路代理安裝資料夾。

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 <連接埠號>`	用來建立與管理伺服器非加密連線的埠號。 預設埠號為 14000。
`-ps <SSL 連接埠號>`	使用 SSL 與管理伺服器建立加密連線時使用的 SSL 埠號。 預設埠號為 13000。
`-nossl`	使用非加密方式連線管理伺服器。 如果未使用該鍵值，網路代理將透過使用加密的 SSL 協定連線至管理伺服器。
`-cert <憑證檔案的路徑>`	存取管理伺服器時使用指定的憑證檔案作為身分驗證。

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。

關於升級卡巴斯基安全管理中心 Linux

您可以安裝版本 14 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 14 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。

> 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。

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安裝文件
- 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

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。

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。

使用安裝檔案升級卡巴斯基安全管理中心 Linux

要將管理伺服器從以前的版本（從版本 13 開始）升級到版本 14，您可以使用卡巴斯基安全管理中心安裝檔案在早期版本的基礎上安裝新版本。

要透過使用安裝檔案將早期版本的管理伺服器升級到版本 14：

1. 從卡巴斯基網站下載包含版本 14 的完整套件的卡巴斯基安全管理中心安裝檔案：
   - 對於執行基於 RPM 的作業系統的裝置 — ksc64-<version number>-11247.x86_64.rpm
   - 對於執行基於 Debian 的作業系統的裝置 — ksc64_<version number>-11247_amd64.deb
2. 使用您在管理伺服器上使用的套件管理程式升級安裝套件。例如，您可以在具有 root 權限的帳戶下的命令行終端中使用以下命令：
   - 對於執行基於 RPM 的作業系統的裝置：
     `$ sudo rpm -Uvh --nodeps --force ksc64-<版本號>-11247.x86_64.rpm`
   - 對於執行基於 Debian 的作業系統的裝置：
     `$ sudo dpkg -i ksc64_<版本號>-11247_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。
3. 執行 /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl 指令碼來配置升級的管理伺服器。
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. 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。

通過備份升級卡巴斯基安全管理中心 Linux

要將管理伺服器從以前的版本（從版本 13 開始）升級到版本 14，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後還原此資料。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。

要透過備份升級早期版本的管理伺服器到版本 14：

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。
3. 在以前的管理伺服器上安裝卡巴斯基安全管理中心版本 14。
4. 從升級前建立的備份還原管理伺服器資料。
5. 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。

登入到卡巴斯基安全管理中心 14 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 14 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。

要登入卡巴斯基安全管理中心 14 網頁主控台，請執行以下操作：

1. 在您的瀏覽器中，轉到<管理伺服器 Web 位址>:<埠號>。
   登入頁面被顯示。
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。
   如果您僅新增了一個管理伺服器，僅登入和密碼欄位被顯示。
3. 執行以下操作之一：
   - 要登入到物理管理伺服器，請輸入本機管理員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**進階設定**。
     b. 建立虛擬伺服器時輸入您指定的虛擬管理伺服器名稱。
     c. 輸入對虛擬管理伺服器具有權限的管理員的使用者名稱和密碼。

登入後，儀表板使用您最後使用的語言和主題顯示。您可以透過卡巴斯基安全管理中心 14 網頁主控台導航並使用其操作卡巴斯基安全管理中心 Linux。

要登出卡巴斯基安全管理中心 14 網頁主控台，請執行以下操作：

1. 點擊位於視窗右上角的您的使用者名稱。
2. 在下拉清單中，選取**登出**。

卡巴斯基安全管理中心 14 網頁主控台被關閉，且登入頁面被顯示。

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。
- 為管理伺服器和受管理應用程式的操作事件通知設定郵件傳送設定（成功的通知傳送需要訊息服務在管理伺服器和所有接收端裝置上執行）。
- 為工作站和伺服器建立防護政策，以及為受管理裝置階層的最上層群組建立病毒掃描工作、更新下載工作和資料備份工作。

  快速啟動精靈僅為其**受管理裝置**資料夾不包含任何政策的應用程式建立政策。如果已經為受管理裝置階層的最上層群組建立相同名稱的工作，則快速啟動精靈不會建立同名工作。

在安裝管理伺服器後，在第一次連線時，應用程式自動提示您執行快速設定精靈。您還可以在任意時刻手動啟動快速設定精靈。

要手動啟動快速啟動精靈：

1. 在應用程式主視窗，點擊管理伺服器名稱旁邊的**設定圖示**（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**一般**區段。
3. 點擊**開始快速啟動精靈**。

精靈提示您執行管理伺服器初始化設定。遵照精靈的說明。使用**下一步**按鈕進行精靈。

步驟 1：指定網際網路連線設定

延伸所有 | 折疊所有

指定卡巴斯基安全管理中心 Linux 的網際網路連線設定。

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**核取方塊。如果選取此方塊，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**
- **連接埠號**
- **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**（如果選取**代理伺服器身分驗證**核取方塊，則可使用該欄位）

  用來建立前往 Proxy 伺服器之連線的使用者帳戶（若選取了**代理伺服器身分驗證**核取方塊，則此欄位可用）。

- **密碼**（如果選取**代理伺服器身分驗證**核取方塊，則可使用該欄位）

  其帳戶用來建立 Proxy 伺服器連線的使用者所設定的密碼（若選取了**代理伺服器身分驗證**核取方塊，則此欄位可用）。
  若要檢視輸入的密碼，依您所需的時間長度點擊並按住**顯示**按鈕。

步驟 2：選取應用程式啟動方式

延伸所有 | 折疊所有

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。

  如果此選項被停用，您可以稍後在主功能表的 **操作 → 產品授權 → Kaspersky 產品授權** 區域將產品授權金鑰部署到受管理裝置。

- **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。

如果此選項被停用，您可以稍後在主功能表的 **操作 → 產品授權 → Kaspersky 產品授權** 區域將產品授權金鑰部署到受管理裝置。

- 透過高推遲應用程式啟動

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 3：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。

步驟 4：設定電子郵件通知

延伸所有 | 折疊所有

設定如何傳遞 Kaspersky 應用程式在用戶端裝置上操作期間記錄的事件通知。這些設定將被用作應用程式政策的預設設定。

要配置發生在 Kaspersky 應用程式上的事件的通知傳送，使用以下設定：

- **收件者（電子郵件信箱）**

  應用程式將給其傳送通知的使用者的郵件位址。您可以輸入一個或更多位址；如果您輸入多個位址，使用分號分隔。

- **SMTP 伺服器位址**

  您組織郵件伺服器的位址。
  如果您輸入多個位址，使用分號分隔。您可以使用以下參數：
  - IPv4 或 Ipv6 位址
  - SMTP 伺服器的 DNS 名稱

- **SMTP 伺服器連接埠**

  SMTP 伺服器的通訊埠號。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，該核取方塊被清除，ESMTP 身分驗證設定不可用。

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 5：關閉快速設定精靈

要關閉精靈，請點擊**完成**按鈕。

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安全程式或網路代理。

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。

防護佈署精靈執行以下操作：

- 為應用程式安裝下載安裝套件（如果之前未建立）。該安裝套件位於**發現和佈署 → 佈署和分配 → 安裝套件**。您可以使用這些套件進行遠端安裝。
- 您可以為您指定的裝置或是管理群組，建立並啟動遠端安裝工作。新建立的遠端安裝工作會儲存在**工作**區段。您可以稍後自行執行此工作。工作類型為**遠端安裝應用程式**。

如果您想在裝有 SUSE Linux Enterprise Server 15 作業系統的裝置上安裝網路代理，請首先安裝 insserv-compat 套件配置網路代理。

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，

在主應用程式視窗，點擊**發現和佈署 → 佈署和分配 → 防護佈署精靈**。

防護佈署精靈啟動。使用**下一步**按鈕進行精靈。

步驟 1：選取安裝套件

選取您要安裝的應用程式安裝套件。

若未列出必要應用程式的安裝套件，請點擊**新增**按鈕，接著從清單中選取應用程式。

步驟 2：選取金鑰檔案或啟動碼的發佈方式

延伸所有 | 折疊所有

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詳細資料。

步驟 3：選取網路代理版本

如果您選取了非網路代理安裝套件，您也必須安裝網路代理，它連線應用程式到卡巴斯基安全管理中心管理伺服器。

選取網路代理的最新版本。

步驟 4：選取裝置

延伸所有 | 折疊所有

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分類中的裝置。您可以指定現有分類之一。
  例如，您可能要使用該選項在特定作業系統版本的裝置上執行工作。

步驟 5：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 Linux 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。

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。

步驟 6：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 7：移動裝置到受管理裝置

指定裝置是否在安裝網路代理後必須被移動到管理群組。

- **不移動裝置**

  裝置保留在目前所在群組中。未被放置在任何群組的裝置保持未分配。

- **將未配置的裝置移動到群組**

  裝置被移動到您選取的管理群組。

預設情況下已選取**不移動裝置** 選項。為了安全，您可能會希望手動移動裝置。

步驟 8：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）**

  如果該選項被選中，您可以指定一個帳戶，並在該帳戶下執行程式的安裝。如果網路代理未安裝在被分配工作的裝置上，您可以指定帳戶。

  您可以根據情況指定多個帳戶，例如，沒有一個帳戶擁有分配工作所對應裝置上全部所需權限時。在此情況下，已經新增的所有帳戶都用於從上到下按順序執行該工作。

  如果尚未新增任何帳戶，將使用執行管理伺服器服務的帳戶執行該工作。

步驟 9：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。

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 Linux 管理伺服器的內容。

配置卡巴斯基安全管理中心 14 網頁主控台到管理伺服器的連線

要設定管理伺服器連線連接埠：

1. 在螢幕上方，點擊所需管理伺服器名稱旁邊的**設定**圖示（ ）。

   管理伺服器內容視窗將開啟。

2. 在**一般**頁籤，選取**連線連接埠**區段。

   應用程式顯示所選伺服器的主要連線設定。

設定 IP 位址允許清單以登入卡巴斯基安全管理中心

預設情況下，使用者可以用任何可以開啟卡巴斯基安全管理中心 14 網頁主控台（以下簡稱 網頁主控台）的裝置登入卡巴斯基安全管理中心。但是，您可以配置管理伺服器，以便使用者只能從具有允許 IP 位址的裝置連線到它。在這種情況下，即使入侵者竊取了卡巴斯基安全管理中心帳戶，他或她也將無法登入卡巴斯基安全管理中心，因為入侵者裝置的 IP 位址不在允許清單中。

當使用者登入卡巴斯基安全管理中心或執行透過卡巴斯基安全中心 OpenAPI 與管理伺服器互動的應用程式時，IP 位址會得到驗證。此時，使用者的裝置嘗試與管理伺服器建立連線。如果裝置的 IP 位址不在允許清單中，則會發生身分驗證錯誤，KLAUD_EV_SERVERCONNECT 事件會通知您尚未建立與管理伺服器的連線。

IP 位址允許清單的要求

僅當以下應用程式嘗試連線到管理伺服器時才會驗證 IP 位址：

- 網頁主控台伺服器

  如果您透過網頁主控台登入卡巴斯基安全管理中心，可以使用作業系統的標準方式在安裝了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但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 klekaut 自動化物件與管理伺服器互動的應用程式
- 透過 OpenAPI（例如 Kaspersky Anti Targeted Attack Platform 或 Kaspersky Security for Virtualization）與管理伺服器互動的應用程式

因此，請指定安裝了上述應用程式的裝置的位址。

您可以設定 IPv4 和 IPv6 位址。您不能指定 IP 位址的範圍。

如何建立 IP 位址的允許清單

如果您之前沒有設定允許清單，請按照以下說明進行操作。

若要建立 IP 位址允許清單以登入卡巴斯基安全管理中心：

1. 在管理伺服器裝置上，在具有管理員權限的帳戶下執行命令提示符。
2. 將當前目錄變更為卡巴斯基安全管理中心安裝資料夾（通常為 /opt/kaspersky/ksc64/sbin）。

3. 使用管理員權限輸入以下命令：
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP 位址>" -t s`

   指定滿足上述要求的 IP 位址。多個 IP 位址必須用分號隔開。

   如何只允許一台裝置連線到管理伺服器的示例：

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s`

   如何允許多個裝置連線到管理伺服器的示例：

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 198.51.100.0; 203.0.113.0" -t s`

4. 重新啟動管理伺服器服務。

您可以在管理伺服器上的 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. 使用管理員權限在命令提示符處輸入以下指令：
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`

2. 重新啟動管理伺服器服務。

之後，不再驗證 IP 位址。

檢視連線到管理伺服器的記錄

操作期間的連線歷程和到管理伺服器的連線嘗試可以被儲存到檔案。檔案中的資訊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. 在應用程式主視窗，點擊所需管理伺服器名稱旁邊的**設定圖示**（ ）。

   管理伺服器內容視窗將開啟。

2. 在**一般**頁籤，選取**連線連接埠**區段。

3. 啟用**記錄管理伺服器連線事件**選項。

所有連入管理伺服器的後續事件、身分驗證結果和 SSL 錯誤將被儲存到 %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog。

設定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。

如果資料庫的事件數量達到管理員指定的最大值，程式刪除最舊的的事件並用新事件將其重寫。若管理伺服器刪除舊事件，則無法儲存新事件到資料庫。在此時間段內，拒絕事件的資訊被寫入卡巴斯基事件記錄。新事件被列隊，然後在刪除操作後被儲存到資料庫。

要限制儲存在管理伺服器事件儲存區中的事件的數量：

1. 在螢幕上方，點擊所需管理伺服器名稱旁邊的**設定**圖示（ ）。

   管理伺服器內容視窗將開啟。

2. 在**一般**頁籤，選取**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。

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。

請注意，已安裝的管理外掛程式沒有備份。從備份副本還原管理伺服器資料後，您需要下載並重新安裝受管應用程式的外掛程式。

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。

只用使用 klbackup 實用程式才能進行管理伺服器還原。

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。如果由快速設定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. 前往**裝置 → 工作**。
2. 點擊**新增**。
   新增工作精靈啟動。
3. 在精靈首頁上的**應用程式**清單中，選取**卡巴斯基安全管理中心 14**並在**工作類型**清單中選取**備份管理伺服器資料**。
4. 在精靈的對應頁面，指定以下資訊：
   - 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**頁面啟用**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。

資料備份和還原實用程式 (klbackup)

您可以使用卡巴斯基安全管理中心發佈套件中隨附的 klbackup 實用程式複製管理伺服器資料以作備份和將來還原之用。

klbackup 實用程式可用以下兩種模式執行：

- 互動

- 靜默

互動模式下的資料備份和還原

若要以互動模式建立管理伺服器資料備份，請執行以下操作：

1. 執行位於卡巴斯基安全管理中心安裝資料夾（通常為 /opt/kaspersky/ksc64/sbin/klbackup）中的 klbackup 實用程式。
   這樣將啟動備份和還原精靈。
2. 在精靈的第一個視窗中，選取**執行管理伺服器資料備份**。
   如果您選取**僅還原或備份管理伺服器憑證**選項，將只儲存管理伺服器憑證的備份副本。
   點擊**"下一步"**。
3. 在下一個精靈視窗中，指定密碼和備份的目標資料夾，然後點擊**下一步**按鈕開始備份。

若要以互動模式還原管理伺服器資料，請執行以下操作：

1. 執行位於卡巴斯基安全管理中心安裝資料夾（通常為 /opt/kaspersky/ksc64/sbin/klbackup）中的 klbackup 實用程式。使用與安裝管理伺服器時相同的帳戶啟動 klbackup 實用程式。
   這樣將啟動備份和還原精靈。
2. 在精靈的第一個視窗中，選取**還原管理伺服器資料**。
   若您選取**僅還原或備份管理伺服器憑證**選項，則只會還原管理伺服器憑證。
   點擊**"下一步"**。
3. 在精靈的**還原設定**視窗中：
   - 指定包含管理伺服器資料備份副本的資料夾。您必須確保該檔案名稱為 backup.zip。
   - 指定資料備份中輸入的密碼。
     在還原資料時，您必須指定在備份過程中輸入的密碼。如果某個共用資料夾的路徑在備份工作完成後發生變更，請檢查使用還原資料工作的操作（還原工作和遠端安裝工作）。必要時，編輯這些工作的設定。當從備份檔案還原資料時，沒有人可以存取管理伺服器的共用資料夾。啟動 klbackup 實用程式所使用的帳戶必須對該共用資料夾具有完全存取權限。
4. 點擊**"下一步"**按鈕，還原資料。

靜默模式下的資料備份和還原

若要以靜默模式建立備份副本或還原管理伺服器，

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 實用程式。

實用程式的命令列語法：

```
klbackup -path BACKUP_PATH [-logfile LOGFILE] [-use_ts]|[-restore] [-password PASSWORD] [-online]
```

> 如果在 klbackup 實用程式的命令列中沒有指定密碼，該實用程式將提示您輸入密碼。

參數敘述：

- `-path BACKUP_PATH` – 在 BACKUP_PATH 資料夾中儲存資訊或使用 BACKUP_PATH 資料夾中的資料進行還原（必填參數）。
- `-logfile LOGFILE` – 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 實用程式需要獲得變更 BACKUP_PATH 資料夾中資料的權限。
- `-use_ts` – 儲存資料時，將資料複製到 BACKUP_PATH 資料夾，將其複製到以 `klbackup YYYY-MM-DD # HH-MM-SS` 格式命名為包含目前系統日期和操作時間的子資料夾。如果未指定鍵，資訊將儲存在 BACKUP_PATH 資料夾的根目錄。
  當您嘗試將資訊儲存至已儲存備份副本的資料夾時，系統會回傳錯誤訊息。不會更新任何資訊。
  `-use_ts` 鍵允許您維護管理伺服器資料壓縮檔案。例如，如果 `-path` 鍵指明資料夾 `C:\KLBackups`，資料夾 `klbackup 2022/6/19 # 11-30-18`，那麼程式將儲存管理伺服器截止 2022 年 6 月 19 日 11:30:18 AM. 的狀態資訊。
- `-restore` – 還原管理伺服器資料。系統將基於 BACKUP_PATH 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 BACKUP_PATH 資料夾內。
- `-password PASSWORD` – 使用 PASSWORD 參數指定的密碼儲存或還原管理伺服器憑證、加密或解密憑證。

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 實用程式所使用的帳戶必須對該共用資料夾具有完全存取權限。

- `-online`—透過建立卷快照來備份管理伺服器資料以最小化管理伺服器的離線時間。當您使用實用程式恢復資料時，該選項被略過。

將管理伺服器和資料庫伺服器移動到另一台裝置

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。
- 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 14 網頁主控台執行資料備份任務或執行klbackup 實用程式。

2. 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 14 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。

3. 在新裝置上，安裝管理伺服器將使用的資料庫管理系統 (DBMS)。

   選擇 DBMS 時，請考慮管理伺服器涵蓋的裝置數量。

4. 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新裝置上，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操作說明的“h”項目中輸入前一個裝置的 IP 位址。

5. 安裝完成後，使用 klbackup 實用程式在新裝置上還原管理伺服器資料。

   如果您在舊裝置和新裝置上使用 SQL Server 作為 DBMS，請注意新裝置上安裝的 SQL Server 版本必須與舊裝置上安裝的 SQL Server 版本相同或更高。否則，您將無法在新裝置上還原管理伺服器資料。

6. 開啟卡巴斯基安全管理中心 14 網頁主控台然後連線到管理伺服器。

7. 驗證所有用戶端裝置都已連線到管理伺服器。

8. 從之前的裝置中解除安裝管理伺服器和資料庫伺服器。

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。

要建立和新增虛擬管理伺服器：

1. 在應用程式主視窗，點擊所需管理伺服器名稱旁邊的**設定圖示**（ ）。

2. 在開啟的頁面中，前往**管理伺服器**頁籤。

3. 選取您要新增虛擬管理伺服器到的管理群組。
   虛擬管理伺服器將管理所選群組（包括子群組）中的裝置。

4. 在功能表行上，點擊**新虛擬管理伺服器**。

5. 在開啟的頁面上，定義新虛擬管理伺服器的內容：

   - **虛擬管理伺服器名稱**.
   - **管理伺服器連線位址**

     您可指定管理伺服器的名稱或 IP 位址。

6. 從使用者清單中，選擇虛擬管理伺服器管理員。如果您想，您可以編輯現有帳戶之一，然後分配其管理員角色，或建立一個新使用者帳戶。

7. 點擊**儲存**。

新虛擬管理伺服器會建立並新增至管理群組，同時顯示在**管理伺服器**頁籤上。

如果您在卡巴斯基安全管理中心 14 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 14 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 14 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 14 網頁主控台的裝置上，在具有管理員權限的帳戶下執行 ksc-web-console-<版本號>.exe 安裝檔案。
  2. 安裝精靈將啟動。
  3. 在精靈的第一頁，選擇**升級**選項。
  4. 在**修改類型**頁面，選擇**編輯連線設定**選項。
  5. 在**受信任的管理伺服器**頁面，新增所需的從屬管理伺服器。
  6. 在精靈的最後一頁，點擊**修改**以套用設定。
  7. 在應用程式重新設定成功完成後，點擊**完成**按鈕。

- 使用卡巴斯基安全管理中心 14 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 14 網頁主控台中的虛擬管理伺服器。

- 使用基於 MMC 的管理主控台直接連線到虛擬伺服器。

管理伺服器的階層

一個 MSP 可能執行多個管理伺服器。可能不方便管理幾個不同的管理伺服器，因此可以應用階層結構。

在階層架構中，卡巴斯基安全管理中心 Linux 管理伺服器只能作為從屬伺服器工作，由基於 Windows 的卡巴斯基安全管理中心或卡巴斯基安全管理中心雲端主控台的主管理伺服器管理。

兩個管理伺服器的"主要/從屬"組態提供了以下選項：

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

建立管理伺服器階層：新增次要管理伺服器

延伸所有 | 折疊所有

在階層架構中，卡巴斯基安全管理中心 Linux 管理伺服器只能作為從屬伺服器工作，由基於 Windows 的卡巴斯基安全管理中心或卡巴斯基安全管理中心雲端主控台的主管理伺服器管理。

新增次要管理伺服器（在未來的主要管理伺服器上執行）

您可以新增管理伺服器作為次要管理伺服器，進而建立"主要 / 次要"層級。

要新增可以透過卡巴斯基安全管理中心 14 網頁主控台連線的從屬管理伺服器：

1. 確保未來主要管理伺服器的連接埠 13000 可用於從次要管理伺服器接收連線。
2. 在未來主要管理伺服器上，點擊**設定**圖示（ ）。
3. 在開啟的內容頁面中，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**。
   "連線次要管理伺服器"精靈啟動。
6. 在精靈的第一頁，填充以下欄位：
   - **從屬管理伺服器顯示名稱**

次要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 的次要伺服器"之類的名稱。

- **從屬管理伺服器位址（可選）**

  指定次要管理伺服器的 IP 位址或網域名稱。

- **管理伺服器 SSL 連接埠號**

  指定主要管理伺服器上的 SSL 埠號。預設埠號為 13000。

- **管理伺服器 API 連接埠**

  指定主要管理伺服器上的埠號以透過 OpenAPI 接收連線。預設埠號為 13299。

- **將主管理伺服器連線到 DMZ 中的從屬管理伺服器**

  如果次要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次要管理伺服器的連線。否則，次要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：
  - **位址**
  - **使用者名稱**
  - **密碼**

7. 遵照精靈的後續說明。

精靈結束後，"主要/次要"層級被建立。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。主要管理伺服器的工作和政策被接收和套用。次要管理伺服器顯示在主要管理伺服器上，在新增其的管理群組中。

新增次要管理伺服器（執行在未來從屬管理伺服器）

如果您無法連線到未來次要管理伺服器（例如，它臨時被斷開或無法連線），您仍可以新增次要管理伺服器。

要新增不可以透過卡巴斯基安全管理中心 14 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. 提示未來次要管理伺服器的責任系統管理員做以下事情：
   a. 點擊**設定**圖示（ ）。
   b. 在開啟的內容頁面中，前往**一般**頁籤的**管理伺服器階層**區段。
   c. 選取**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. 透過點擊**瀏覽**選取先前儲存的帶有未來主要管理伺服器憑證的檔案。
   f. 如有需要，請選取**將主管理伺服器連線到 DMZ 中的從屬管理伺服器**核取方塊。
   g. 若未來次要管理伺服器的連線會透過代理伺服器執行，請選取**使用代理伺服器**選項並指定連線設定。
   h. 點擊**儲存**。

"主要 / 次要"層級被建立。主要管理伺服器開始使用連接埠 13000 從次要管理伺服器接收連線。主要管理伺服器的工作和政策被接收和套用。次要管理伺服器顯示在主要管理伺服器上，在新增其的管理群組中。

檢視次要管理伺服器清單

要檢視次要（包括虛擬）管理伺服器清單：

在主應用程式視窗中，點擊管理伺服器名稱，此資訊位於**設定**圖示旁邊（ ）。

次要（包括虛擬）管理伺服器下拉清單被顯示。

您可透過點及其名稱前往這些管理伺服器的任何一個。

管理群組也會予以顯示，但是灰色的，無法在此功能表中進行管理。

如果您在卡巴斯基安全管理中心 14 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 14 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 14 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 14 網頁主控台的裝置上，在具有管理員權限的帳戶下執行 ksc-web-console-<版本號>.exe 安裝檔案。
  2. 安裝精靈將啟動。
  3. 在精靈的第一頁，選擇**升級**選項。
  4. 在**修改類型**頁面，選擇**編輯連線設定**選項。
  5. 在**受信任的管理伺服器**頁面，新增所需的從屬管理伺服器。
  6. 在精靈的最後一頁，點擊**修改**以套用設定。
  7. 在應用程式重新設定成功完成後，點擊**完成**按鈕。

- 使用卡巴斯基安全管理中心 14 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 14 網頁主控台中的虛擬管理伺服器。
- 使用基於 MMC 的管理主控台直接連線到虛擬伺服器。

啟用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. 前往**使用者和角色 → 使用者**。
2. 點擊您要為其指定帳戶防護免受未經授權修改的內部使用者帳戶名稱。
3. 在開啟的使用者設定視窗中，選取**驗證安全性**頁籤。
4. 在**驗證安全性**頁籤中，如果您希望每次變更或修改帳戶設定時都要請求憑證，請選取**請求身分驗證以檢查權限來修改使用者帳戶**選項。否則，請選取**允許使用者無需其他身分驗證即可修改此帳戶**選項。
5. 點擊**"儲存"**按鈕。

兩步驟驗證

本節介紹如何使用兩步驟驗證來減少未授權存取卡巴斯基安全管理中心 14 網頁主控台的風險。

情境：為所有使用者配置兩步驟驗證

此情境說明如何為所有使用者啟用兩步驟驗證，以及如何從兩步驟驗證中排除使用者帳戶。如果在為其他使用者啟用帳戶前未啟用帳戶的兩步驟驗證，則應用程式會先開啟用於為帳戶啟用兩步驟驗證的視窗。此方案還說明如何為您自己的帳戶啟用兩步驟驗證。

如果您為帳戶啟用了兩步驟驗證，則可以進入為所有使用者啟用兩步驟驗證的階段。

先決條件

開始之前：

- 請確保您的使用者帳戶在以下功能區具有 修改物件 ACL的權限：**一般功能：使用者權限**，以修改其他使用者帳戶的安全設定的功能區域。
- 確保管理伺服器的其他使用者在其裝置上安裝驗證應用程式。

階段

為所有使用者啟用兩步驟驗證將分階段進行：

1. **在裝置上安裝驗證應用程式**

   您可以安裝 Google Authenticator、Microsoft Authenticator 或任何其他支援時效型一次性密碼演算法的驗證應用程式。

2. **將驗證應用程式時間與安裝了管理伺服器的裝置時間同步**

   驗證應用程式中設定的時間必須與管理伺服器的時間同步。

3. **對您的帳戶啟用兩步驟驗證，並為您的帳戶接收金鑰**

   為帳戶啟用兩步驟驗證後，您可以為所有使用者啟用兩步驟驗證。

4. **對所有使用者啟用兩步驟驗證**

   啟用了兩步驟驗證的使用者必須使用它登入管理伺服器。

5. **編輯安全碼簽發者的名稱**

   如果您有多個具有相似名稱的管理伺服器，則可能必須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。

6. **排除不需要啟用兩步驟驗證的使用者帳戶**

   如有需要，您可以從兩步驟驗證中排除使用者。具有被排除帳戶的使用者不必使用兩步驟驗證即可登入管理伺服器。

結果

完成此情境後：

- 對帳戶啟用兩步驟驗證
- 為管理伺服器的所有使用者帳戶啟用了兩步驟驗證，但已排除的使用者帳戶除外。

關於帳戶的兩步驟驗證

卡巴斯基安全管理中心 Linux 為卡巴斯基安全管理中心 14 網頁主控台的使用者提供兩步驟驗證。為帳戶啟用兩步驟驗證後，每次登入到卡巴斯基安全管理中心 14 網頁主控台時，都將輸入使用者名稱、密碼和其他一次性安全碼。若要接收一次性使用的安全碼，您的電腦或行動裝置上必須具有驗證應用程式。

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。簽發者名稱用作驗證應用程式中管理伺服器的識別碼。如果變更了安全碼簽發者名稱，則必須簽發新的金鑰並將其傳遞給驗證應用程式。安全碼為一次性，有效期最長為 90 秒（具體時間可能會有所不同）。

啟用了兩步驟驗證的任何使用者都可以重新簽發自己的金鑰。當使用者使用重新發布的金鑰進行身分驗證並將其用於登錄時，管理伺服器將為使用者帳戶儲存新的金鑰。如果使用者輸入的新金鑰不正確，則管理伺服器不會儲存新的金鑰，而將目前的金鑰保留為對進一步的驗證有效。

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驗證應用程式，例如 Google Authenticator。為了產生安全碼，必須將在驗證應用程式中設定的時間與為管理伺服器設定的時間同步。

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。

強烈建議您在多個裝置上安裝驗證應用程式。儲存密碼或 QR 碼，並將其儲存在安全的地方。如果您遺失了行動裝置，這有助於您復原對卡巴斯基安全管理中心 14 網頁主控台的存取。

為了確保使用卡巴斯基安全管理中心，您可以為自己的帳戶啟用兩步驟驗證，並為所有使用者啟用兩步驟驗證。

您可以從兩步驟驗證中排除帳戶。對於無法接收身分驗證安全碼的服務帳戶，這可能是必需的。

兩步驟驗證根據以下規則進行：

- 只有在**一般功能中擁有修改物件 ACL 權限的使用者帳戶：使用者權限**功能區，可以為所有使用者啟用兩步驟驗證。
- 只有為自己的帳戶啟用了兩步驟驗證的使用者才能為所有使用者啟用兩步驟驗證的選項。
- 只有為自己的帳戶啟用了兩步驟驗證的使用者，才能從為所有使用者啟用的兩步驟驗證清單中排除其他使用者帳戶。
- 使用者僅可以為其帳戶啟用兩步驟驗證。
- 在**一般功能中擁有修改物件 ACL 權限的使用者帳戶：使用者權限**功能區，並使用兩步驟驗證登入到卡巴斯基安全管理中心 14 網頁主控台的使用者帳戶，可停用兩步驟驗證：適用於僅當停用所有使用者的兩步驟驗證時的其他任何使用者，與從所有使用者啟用的兩步驟驗證清單中排除的使用者。
- 使用兩步驟驗證登入卡巴斯基安全管理中心 14 網頁主控台的任何使用者，都可以重新簽發自己的金鑰。
- 您可以為目前使用的管理伺服器，啟用對所有使用者進行兩步驟驗證選項。如果在管理伺服器上啟用此選項，則還將為其虛擬管理伺服器的使用者帳戶啟用此選項，並且不要對輔助管理伺服器的使用者帳戶啟用兩步驟驗證。

如果在卡巴斯基安全管理中心管理伺服器 13 或者更改版本上為使用者帳戶啟用了兩步驟驗證，則該使用者將無法登入卡巴斯基安全管理中心網頁主控台版本 12、12.1 或 12.2。

對您自己的帳戶啟用兩步驟驗證

您只能為自己的帳戶啟用兩步驟驗證。

在開始為帳戶啟用兩步驟驗證之前，請確保在行動裝置上安裝了驗證應用程式。確保驗證應用程式中設定的時間必須與管理伺服器上設定的裝置時間同步。

要啟用使用者帳戶的兩步驟驗證：

1. 前往**使用者和角色 → 使用者**。
2. 請點擊帳戶的名稱。
3. 在開啟的使用者設定視窗中，選取**帳戶防護**頁籤。
4. 在**帳戶防護**頁籤：
   - 如果您要為使用者帳戶啟用兩步驟驗證，請選取**請求使用者名稱、密碼和安全碼（兩步驟驗證）**選項。
     - 在開啟的兩步驟驗證視窗中，在驗證應用程式中輸入金鑰或掃描 QR 碼並接收一次性安全碼。
       您可以在驗證應用程式中手動指定金鑰，也可以透過行動裝置掃描 QR 碼。
     - 在開啟的兩步驟驗證視窗中，指定由身分驗證器應用程式產生的安全碼，然後點擊**確認並套用**按鈕。
5. 點擊**儲存**按鈕。

對帳戶啟用兩步驟驗證

對所有使用者啟用兩步驟驗證

如果您的帳戶具有在 **一般功能的修改對象 ACL權限，您可以為管理伺服器的所有使用者啟用兩步驟驗證：使用者權限**功能區域，如果您透過兩步驟驗證進行身份驗證。如果在為所有使用者啟用帳戶之前未啟用帳戶的兩步驟驗證，則該應用程式將開啟一個視窗，以為您自己的帳戶啟用兩步驟驗證。

若要為多個使用者啟用或停用兩步驟驗證，請執行以下操作：

1. 在應用程式主視窗，點擊所需管理伺服器名稱旁邊的**設定圖示**（ ）。
   管理伺服器內容視窗將開啟。
2. 在屬性視窗的**驗證安全性**頁籤上，切換**所有使用者的兩步驟驗證**選項設定按鈕為啟用位置。

為所有使用者啟用了兩步驟驗證。從現在開始，除了其帳戶不包括在兩步驟驗證中的使用者之外，管理伺服器的使用者（包括在啟用此選項後新增的使用者）都必須為其帳戶設定兩步驟驗證。

對使用者帳戶停用兩步驟驗證

您可以為自己的帳戶以及任何其他使用者的帳戶停用兩步驟驗證。

您可以停用對另一使用者帳戶的兩步驟驗證，前提是您的帳戶在**一般功能中具有修改物件 ACL 權限：使用者權限**功能區域。

要停用使用者帳戶的兩步驟驗證：

1. 前往**使用者和角色 → 使用者**。
2. 點擊您想要為其停用兩步驟驗證之內部使用者帳戶的名稱。這可以是您自己的帳戶，也可以是任何其他使用者的帳戶。
3. 在開啟的使用者設定視窗中，選取**帳戶防護**頁籤。
4. 如果您要為使用者帳戶停用兩步驟驗證，請在**帳戶防護**頁籤上選取**僅請求使用者名稱和密碼**選項。
5. 點擊**儲存**按鈕。

該使用者帳戶已停用兩步驟驗證。

對所有使用者停用兩步驟驗證

您可為所有使用者停用兩步驟驗證，前提是您的帳戶啟用了兩步驟驗證，並且您的的帳戶在**一般功能中具有修改物件 ACL 權限：使用者權限**功能區域。如果您的帳戶未啟用兩步驟驗證，則必須先為帳戶啟用兩步驟驗證，然後再為所有使用者停用該功能。

若要為所有使用者啟用和停用兩步驟驗證：

1. 在應用程式主視窗，點擊所需管理伺服器名稱旁邊的**設定圖示**（ ）。
   管理伺服器內容視窗將開啟。
2. 在屬性視窗的**驗證安全性** 頁籤上，將**所有使用者的兩步驟驗證**選項切換至停用的位置。
3. 在身分驗證視窗中輸入您的帳戶憑證。

所有使用者均停用兩步驟驗證。

從兩步驟驗證中排除帳戶

您可以從兩步驟驗證中排除使用者帳戶，前提是您在**一般功能中有修改物件 ACL 權限：使用者權限**功能區域。

如果某個使用者帳戶被排除在所有使用者的兩步驟驗證清單之外，則該使用者不必使用兩步驟驗證。

對於在身分驗證期間無法通過安全碼驗證的服務帳戶，可能有必要從兩步驟驗證中排除帳戶。

如果排除某些使用者帳戶的兩步驟驗證：

1. 在應用程式主視窗，點擊所需管理伺服器名稱旁邊的**設定圖示**（ ）。
   管理伺服器內容視窗將開啟。
2. 在屬性視窗的**驗證安全性**頁籤上的兩步驟驗證排除表中，點擊**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. 點擊**確定**按鈕。

所選取的使用者帳戶將排除在兩步驟驗證之外。

產生新的金鑰

僅當您透過兩步驟驗證獲得授權時，才能為帳戶的兩步驟驗證產生新的金鑰。

要為使用者帳戶產生新的金鑰：

1. 前往**使用者和角色 → 使用者**。
2. 點擊您想要為其產生新的兩步驟驗證金鑰的使用者帳戶名稱。
3. 在開啟的使用者設定視窗中，選取**帳戶防護**頁籤。
4. 在**帳戶防護**頁籤中，點擊**產生新的金鑰**連結。
5. 在開啟的兩步驟驗證視窗中，指定由身分驗證應用程式產生的新安全金鑰。
6. 點擊**確認並套用**按鈕。

為使用者產生一個新的金鑰。

如果丟失了行動裝置，您可以在另一台行動裝置上安裝身分驗證器應用程式並產生新金鑰以還原對卡巴斯基安全管理中心 14 網頁主控台的存取。

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）。以防萬一，您可以更改安全碼簽發者的名稱，例如，管理伺服器已經為另一台管理伺服器使用了類似的安全碼簽發者名稱。預設情況下，安全碼簽發者的名稱與管理伺服器的名稱相同。

更改安全碼簽發者名稱後，您必須重新簽發新的金鑰並將其傳遞給驗證應用程式。

若要指定安全碼簽發者的新名稱：

1. 在應用程式主視窗，點擊所需管理伺服器名稱旁邊的**設定圖示**（ ）。
   管理伺服器內容視窗將開啟。
2. 在開啟的使用者設定視窗中，選取**帳戶防護**頁籤。
3. 在**帳戶防護**頁籤上，點擊**編輯**連結。
   編輯安全碼簽發者區段隨即開啟。
4. 指定新的安全碼簽發者名稱。
5. 點擊**確定**按鈕。

為管理伺服器指定了新的安全碼簽發者名稱。

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。

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。

若要使用 klsrvconfig 實用程式在 Linux 環境中變更 DBMS 憑據，請執行以下操作：

1. 啟動 Linux 命令行。
2. 在開啟的命令行視窗中指定 klsrvconfig 實用程式：
   ```
   sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred
   ```
3. 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。
4. 輸入新密碼。
5. 指定新密碼進行確認。

DBMS 憑據已變更。

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. 在螢幕上方，點擊主要管理伺服器名稱旁邊的**設定**圖示（ ）。
2. 在開啟的頁面中，前往**管理伺服器**頁籤。
3. 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. 在功能表行上，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。

配置介面

您可設定卡巴斯基安全管理中心 14 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 14 網頁主控台介面：

1. 在主應用程式視窗，點擊帳戶功能表。
2. 在下拉清單中，選取**介面選項**。
3. 在開啟的**介面選項**視窗中，啟用或停用所需選項。
4. 點擊**儲存**。

之後，主控台會根據啟用的選項在主功能表中顯示相關區域。例如，如果您啟用 **顯示 EDR 警示**，則 **監控和報告 → 警示** 區域將出現在主功能表中。

發現網路裝置

該部分描述網路裝置的搜尋和發現。

卡巴斯基安全管理中心允許您按照指定規則尋找裝置。您可以儲存搜尋結果到文字檔案。

搜尋和發現功能允許您尋找以下裝置：

- 卡巴斯基安全管理中心管理伺服器及其從屬管理伺服器的管理群組中的受管理裝置。
- 由卡巴斯基安全管理中心管理伺服器及其從屬管理伺服器管理的未配置裝置。

情境：發現網路裝置

您必須在安裝安全應用程式之前執行裝置發現。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。

3. **設定規則以新增發現的裝置到管理群組（可選）**

   如果新裝置出現在您的網路，它們會在常規輪詢中被發現並被自動包含在**未配置的裝置**群組。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**未配置的裝置**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

完成方案可以導致如下：

- 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。

新發現的裝置根據設定的規則被安排。（或者，如果未設定任何規則，裝置保留在**未配置的裝置**群組）。

IP 範圍輪詢

卡巴斯基安全管理中心嘗試使用標準 DNS 請求為指定範圍的每個 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從其所在裝置的網路設定獲取 IP 輪詢範圍。如果裝置位址是 192.168.0.1 且子網路遮罩是 255.255.255.0，卡巴斯基安全管理中心自動包含網路 192.168.0.0/24 到輪詢位址。卡巴斯基安全管理中心從 192.168.0.1 到 192.168.0.254 之間輪詢所有位址。

如果僅啟用 IP 範圍輪詢，卡巴斯基安全管理中心將僅發現具有 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。

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. 前往**發現和佈署 → 發現 → IP 範圍**。
2. 點擊**內容**按鈕。

   IP 輪詢內容視窗將開啟。
3. 透過使用**允許輪詢**切換按鈕來啟用或停用 IP 輪詢。
4. 設定輪詢排程。預設下，IP 輪詢每 420 分鐘（七小時）執行一次。

   當指定輪詢間隔時，確保該設定不超過 IP 位址生命週期參數值。如果 IP 位址在 IP 位址生命週期中不被輪詢所驗證，該 IP 位址被從輪詢結果中自動刪除。預設下，輪詢結果的生命期是 24 小時，因為動態 IP 位址（使用 Dynamic Host Configuration Protocol（DHCP））分配每 24 小時變更一次。

   輪詢排程選項：

   - **每 N 天**

     輪詢定期執行，按照指定天數間隔，從指定的日期和時間開始。

     預設下，輪詢每天執行一次，從目前系統日期和時間開始。

   - **每 N 分鐘**

     輪詢定期執行，按照指定分鐘間隔，從指定的時間開始。

- **按每星期中的指定日**

  輪詢定期執行，在指定星期的指定時間。

- **每個月在所選週的指定天**

  輪詢定期執行，在指定月日的指定時間。

- **執行略過的工作**

  如果在排程輪詢期間管理伺服器被切換掉或不可用，管理伺服器可以在切換回來後立即啟動輪詢，或者等待下次排程輪詢。
  如果啟用該選項，管理伺服器在它切換回來後立即啟動輪詢。
  如果停用該選項，管理伺服器等待下一次排程輪詢。
  預設情況下已停用該選項。

5. 點擊**儲存**按鈕。

內容封包儲存並套用到所有 IP 範圍。

手動執行輪詢

要立即執行輪詢，

點擊**開始輪詢**。

新增和修改 IP 範圍

延伸所有 | 折疊所有

開始，卡巴斯基安全管理中心從其所在裝置的網路設定獲取 IP 輪詢範圍。如果裝置位址是 192.168.0.1 且子網路遮罩是 255.255.255.0，卡巴斯基安全管理中心自動包含網路 192.168.0.0/24 到輪詢位址。卡巴斯基安全管理中心從 192.168.0.1 到 192.168.0.254 之間輪詢所有位址。您可以修改自動定義的 IP 範圍或新增自訂 IP 範圍。

您只能為 IPv4 位址建立範圍。如果您啟用 Zeroconf 輪詢，卡巴斯基安全管理中心將輪詢整個網路。

要新增新 IP 範圍：

1. 前往**發現和佈署 → 發現 → IP 範圍**。
2. 若要建立新的 IP 範圍，請點擊**新增**按鈕。
3. 在開啟的視窗，指定以下設定：

- **IP 範圍名稱**

  IP 範圍名稱。您可能想指定 IP 範圍本身作為名稱，例如，"192.168.0.0/24"。

- **IP 間隔或子網路位址和遮罩**

  透過指定開始和結束位址或子網路位址和子網路遮罩設定 IP 範圍。您也可透過點擊**瀏覽**按鈕選取其中一個已存在的 IP 範圍。

- **IP 位址使用期限（小時）**

  當指定該參數時，確保它超過輪詢排程中設定的輪詢間隔。如果 IP 位址在 IP 位址生命週期中不被輪詢所驗證，該 IP 位址被從輪詢結果中自動刪除。預設下，輪詢結果的生命期是 24 小時，因為動態 IP 位址（使用 Dynamic Host Configuration Protocol—DHCP）分配每 24 小時變更一次。

4. 若您要輪詢子網路或您已新增間隔，請選取**啟用 IP 範圍輪詢**。否則，您新增的子網路或間隔將不被輪詢。
5. 點擊**儲存**按鈕。

新 IP 範圍被新增到 IP 範圍清單。

您可使用**開始輪詢**按鈕分別執行各 IP 範圍的輪詢。輪詢完成時，您可使用**裝置**按鈕檢視已發現裝置的清單。預設下，輪詢結果的壽命是 24 小時，且等於 IP 位址生命週期設定。

要新增子網路到現有 IP 範圍：

1. 前往**發現和佈署 → 發現 → IP 範圍**。
2. 點擊您要新增到子網路的 IP 範圍名稱。
3. 在開啟的視窗中，點擊**新增**按鈕。
4. 透過使用位址或者遮罩指定子網路，或者透過使用 IP 範圍中的第一個和最後一個 IP 位址。或者，透過點擊**瀏覽**按鈕新增現有子網路。
5. 點擊**儲存**按鈕。
   新子網路被新增到 IP 範圍。
6. 點擊**儲存**按鈕。

IP 範圍的新設定被儲存。

您可以新增無限多的子網路。命名 IP 範圍不被允許重疊，IP 範圍中的非命名子網路沒有此限制。您可以對每個 IP 範圍獨立啟用和停用輪詢。

Zeroconf 輪詢

僅基於 Linux 的分發點支援此輪詢類型。

卡巴斯基安全管理中心可以輪詢具有 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. 前往**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開始輪詢您的網路。在這種情況下，指定的 IP 範圍將被忽略。

裝置標籤

該部分描述了裝置標籤，提供了建立和修改它們以及手動或自動標記裝置的說明。

關於裝置標籤

卡巴斯基安全管理中心允許您*標記*裝置。標籤是裝置標誌，可以用於分群組、描述或尋找裝置。分配到裝置的標籤可以用於建立分類、尋找裝置以及分發裝置到管理群組。

您可以手動或自動標記裝置。當您要標記單個裝置時可以使用手動標記。自動標記由卡巴斯基安全管理中心利用指定標記規則來執行。

當指定條件被滿足時，裝置被自動標記。單個規則對應於每個標記。規則應用到裝置網路內容、作業系統、裝置上安裝的應用程式以及其他裝置內容。例如，您可以設定規則以分配 [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 裝置並給它們分配工作。

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，包括主要管理伺服器和從屬虛擬管理伺服器。規則僅被套用到來自建立規則的相同管理伺服器的裝置。

建立裝置標籤

要建立裝置標籤：

1. 在主功能表中，轉至 **裝置 → 標籤 → 裝置標籤**。
2. 點擊**新增**。

新標籤視窗開啟。

3. 在**標籤**欄位中，輸入頁籤名稱。
4. 點擊**儲存**儲存變更。

新標籤出現在裝置標籤清單。

重命名裝置標籤

要重命名裝置標籤：

1. 在主功能表中，轉至 **裝置** → **標籤** → **裝置標籤**。
2. 點擊您要重命名的標籤名稱。
   標籤內容視窗開啟。
3. 在**標籤**欄位，輸入頁籤名稱。
4. 點擊**儲存**儲存變更。

更新的標籤出現在裝置標籤清單。

刪除裝置標籤

要刪除裝置標籤：

1. 在主功能表中，轉至 **裝置** → **標籤** → **裝置標籤**。
2. 在清單中，選取您要刪除的裝置標籤旁邊的方塊。
3. 點擊**刪除**按鈕。
4. 在開啟的視窗中，點擊**是**按鈕。

裝置標籤被刪除。刪除的標籤被從其分配的所有裝置上自動刪除。

> 您刪除的標籤不會自動從自動標記規則中刪除。標籤被刪除後，它僅在裝置第一次滿足標籤分配條件時被分配到新裝置。

檢視分配了標籤的裝置

要檢視分配了標籤的裝置：

1. 在主功能表中，轉至 **裝置** → **標籤** → **裝置標籤**。
2. 點擊您要檢視已指派裝置之標籤的**檢視裝置**連結。
   若您沒有在標籤房看見**檢視裝置**連結，該標籤不會指派給任何裝置。

裝置清單僅顯示分配了標籤的裝置。

要返回裝置標籤清單，點擊您瀏覽器的**後退**按鈕。

檢視分配到裝置的標籤

要檢視分配到裝置的標籤：

1. 在主功能表中，轉至 **裝置** → **受管理裝置**。
2. 點擊您要檢視其標籤的裝置名稱。
3. 在開啟的裝置內容視窗中，選取**標籤**頁籤。

分配給所選裝置的標籤清單被顯示。

您可以分配其他標籤到裝置或刪除已經分配的標籤。您也可以檢視管理伺服器上存在的所有裝置標籤。

手動標記裝置

要手動分配標籤到裝置：

1. 檢視分配到您要分配其他標籤的裝置的標籤。
2. 點擊**新增**。
3. 在開啟的視窗中，執行以下操作之一：
   - 若要建立並指派新標籤，請選取**建立新標籤**，之後指定新標籤的名稱。
   - 若要選取現有標籤，請選取**分配現有標籤**，之後在下拉清單選取必要標籤。
4. 點擊**確定**以套用變更。
5. 點擊**儲存**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. 檢視分配到您要刪除標籤的裝置的標籤。
2. 選取您要刪除的項目旁邊的核取方塊。
3. 點擊**取消分配標籤**按鈕。
4. 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。

檢視自動標記裝置規則

要檢視自動標記裝置規則，

做以下任意：

- 在主功能表中，轉至 **裝置 → 標籤 → 自動標記規則**。
- 在主功能表中，轉至**裝置 → 標籤**，然後點擊**設定自動標記規則**連接。
- 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**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。
   - **應用程式**—網路代理在裝置上的出現，和作業系統類型、版本和架構。
   - **虛擬機**—裝置屬於虛擬機的特定類型。
   - **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**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。

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。

關於應用程式標籤

卡巴斯基安全管理中心 Linux 可讓您標記協力廠商應用程式（非 Kaspersky 的供應商製作的應用程式）。標籤是應用程式標誌，可以用於分組或尋找應用程式。分配給應用程式的標籤可以作為裝置分類中的條件。

例如，您可以建立 [瀏覽器] 標籤並分配其到所有瀏覽器（諸如 Microsoft Internet Explorer、Google Chrome、Mozilla Firefox。）

建立應用程式標籤

要建立應用程式標籤：

1. 在主功能表中，轉至**操作 → 協力廠商應用程式 → 應用程式標籤**。
2. 點擊**新增**。
   新標籤視窗開啟。
3. 輸入標籤名稱。
4. 點擊**確定**儲存變更。

新標籤出現在應用程式標籤清單。

重命名應用程式標籤

要重命名應用程式標籤：

1. 在主功能表中，轉至 **操作 → 協力廠商應用程式 → 應用程式標籤**。

2. 選取您要重新命名之標籤旁的核取方塊，接著點擊**編輯**。
   標籤內容視窗開啟。
3. 變更標籤名稱。
4. 點擊**確定**儲存變更。

更新的標籤出現在應用程式標籤清單。

分配標籤到應用程式

要分配一個或多個標籤到一個應用程式：

1. 在主功能表中，轉至 **操作 → 協力廠商應用程式 → 應用程式登錄資料**。
2. 點擊您要分配標籤的應用程式名稱。
3. 選取 **標籤**頁籤。
   標籤顯示所有存在於管理伺服器的應用程式標籤。對於指派給選取的應用程式的標記，系統會選取**分配的標籤**欄中的核取方塊。
4. 對於要指派的標籤，請在**分配的標籤**欄中選取核取方塊。
5. 點擊**儲存**儲存變更。

標籤被分配到應用程式。

從應用程式上刪除分配的標籤

要從應用程式刪除一個或多個標籤：

1. 在主功能表中，轉至 **操作 → 協力廠商應用程式 → 應用程式登錄資料**。
2. 點擊您要刪除標籤的應用程式名稱。
3. 選取 **標籤**頁籤。
   標籤顯示所有存在於管理伺服器的應用程式標籤。對於指派給選取的應用程式的標記，系統會選取**分配的標籤**欄中的核取方塊。
4. 對於您要移除的標記，請不要選取**分配的標籤**欄中的核取方塊。
5. 點擊**儲存**儲存變更。

標籤被從應用程式刪除。

> 已移除應用程式的標籤不被刪除。如果您想，您可以手動刪除它們。

刪除應用程式標籤

要刪除應用程式標籤：

1. 在主功能表中，轉至 **操作 → 協力廠商應用程式 → 應用程式標籤**。
2. 在清單中，選取您想要刪除的應用程式標籤。
3. 點擊**刪除**按鈕。
4. 在開啟的視窗中，點擊**確定**按鈕。

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。

卡巴斯基應用程式部署

本節說明如何透過卡巴斯基安全管理中心 14 網頁主控台在貴組織內的用戶端裝置上佈署 Kaspersky 應用程式。

情境：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 14 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。

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**

   從卡巴斯基網站下載 Kaspersky Endpoint Security for Linux 的管理 Web 外掛程式，然後將外掛程式新增到卡巴斯基安全管理中心14 網頁主控台。

2. **下載和建立網路代理的安裝套件**

   從卡巴斯基網站下載網路代理分發套件，然後建立網路代理安裝套件。

   您可以使用下載的分發套件在本機安裝網路代理。為此，請按照Kaspersky Endpoint Security for Linux 文件中提供的指示操作。

3. **下載和建立 Kaspersky Endpoint Security for Linux 的安裝套件**

   從卡巴斯基網站下載 Kaspersky Endpoint Security for Linux 分發套件，然後 建立 Kaspersky Endpoint Security for Linux 安裝套件。

4. **建立獨立安裝套件（可選）**

   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。若您使用獨立式套件來安裝 Kaspersky 應用程式，可忽略下方的階段 5 和階段 6。

5. **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。

6. **建立和配置工作**

   Kaspersky Endpoint Security for Windows 的*更新*工作必須被配置。

   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，確保工作排程滿足您的需求。（預設下，工作的排程啟動被設定為**手動**，但是您可能要選取其他選項。）

7. **建立政策**

   手動或透過快速啟動精靈為 Kaspersky Endpoint Security for Linux 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。

8. **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

完成方案可以導致如下：

- 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，您必須新增和下載此應用程式的管理外掛程式。

要新增和下載卡巴斯基應用程式的管理外掛程式：

1. 從卡巴斯基網站下載 Kaspersky Endpoint Security for Linux 的管理 Web 外掛程式。
2. 開啟卡巴斯基安全管理中心 14 網頁主控台。
3. 在**主控台設定**下拉清單中，選取**Web 外掛程式**。
   可用管理外掛程式清單被顯示。
4. 點擊**從檔案新增**按鈕。

系統將顯示**從檔案新增**視窗。

5. 點擊**上傳 Zip 檔案**按鈕。
6. 指定下載的 Web 外掛程式的 ZIP 檔案。
7. 點擊**上傳簽章**按鈕。
8. 指定下載的 Web 外掛程式簽章的 TXT 檔案。
9. 點擊**新增**按鈕。
   卡巴斯基安全管理中心將驗證上傳的檔案，然後新增並安裝 Web 外掛程式。
10. 安裝完成時，點擊**確定**。

管理 Web 外掛程式使用預設配置被安裝並顯示在管理 Web 外掛程式清單中。

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。

若要建立應用程式安裝套件：

1. 執行以下操作之一：
   - 前往**發現和佈署 → 佈署和分配 → 安裝套件**。
   - 前往**操作 → 儲存區 → 安裝套件**。

   系統會顯示可在管理伺服器使用的安裝套件清單。
2. 點擊**新增**。
   新套件精靈啟動。使用**下一步**按鈕進行精靈。
3. 在精靈的第一個頁面中，選取**從檔案建立安裝套件**
4. 在精靈的下個頁面，指定檔案名稱並點擊**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。
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**。
   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. 在精靈的下個頁面，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行參數。
   您可指定命令行參數以靜默模式從安裝應用程式來安裝套件。您可選擇指定命令行參數。
   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。

- **來源**.應用程式供應商名稱。
- **應用程式**.封裝在自訂安裝套件的應用程式名稱。
- **版本**.應用程式版本。
- **語言**.封裝在自訂安裝套件的應用程式語言。
- **大小 (MB)**.安裝套件大小。
- **作業系統**.適用安裝套件的作業系統類型。
- **建立日期**.安裝套件建立日期。
- **已修改**.安裝套件修改日期。
- **類型**.安裝套件的類型。

- 變更命令行參數。

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（Installer.exe），您可將其儲存在網頁伺服器或共用資料夾、由電子郵件傳送，或以其他方式傳輸至用戶端裝置。在用戶端裝置上，使用者會本機執行已接收檔案而不透過卡巴斯基安全管理中心 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。

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. 執行以下操作之一：
   - 前往**發現和佈署 → 佈署和分配 → 安裝套件**。
   - 前往**操作 → 儲存區 → 安裝套件**。

   系統會顯示可在管理伺服器使用的安裝套件清單。
2. 在安裝套件的清單中，選取安裝套件並在上列清單中，點擊**佈署**按鈕。
3. 選取**使用獨立安裝套件**選項。

   獨立安裝套件建立精靈啟動。使用**下一步**按鈕進行精靈。
4. 在精靈的第一頁，請確保已啟用**網路代理與該應用程式一同安裝**選項，若您要安裝與選取的應用程式一起安裝網路代理。

   預設情況下已啟用該選項。若您不確認裝置是否安裝網路代理，建議啟用此選項。若網路代理已在裝置上安裝，在安裝含網路代理的獨立安裝套件後，網路代理將會更新至新版本。

   若您停用此選項，網路代理將不會安裝在裝置上，且裝置不會受到管理。

   若管理伺服器已存在所選應用程式的獨立安裝套件，精靈會告知您此資訊。在此情況下，您必須選取以下其中一個動作：
   - **建立獨立安裝套件**.若您要針對新應用程式版本建立獨立安裝套件，並同時希望保留針對先前應用程式版本建立的獨立安裝套件，請選取此選項。新獨立安裝套件會放在另一個資料夾中。
   - **使用存在的獨立安裝套件**.若要使用現有獨立安裝套件，請選取此選項。建立套件的程序將不會啟動。
   - **重新建立存在的獨立安裝套件**.如果您要再次針對相同應用程式建立獨立安裝套件，請選取此選項。獨立安裝套件會放在相同資料夾。
5. 在精靈的**移動到受管理裝置清單**頁面，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，請不要變更選擇的選項。

   如果要在網路代理安裝後移動用戶端裝置，請選取**將未配置的裝置移動到此群組**選項並指定要將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。
6. 在精靈的次頁上，完成獨立安裝套件時，請點擊**完成**按鈕。

   獨立安裝套件建立精靈會關閉。

系統會在管理伺服器共用資料夾的 PkgInst 子資料夾建立和放置獨立安裝套件。您可透過點擊在安裝套件清單上的**檢視獨立安裝套件清單**按鈕檢視獨立安裝套件的清單。

檢視獨立安裝套件清單

您可檢視獨立安裝套件的清單以及各獨立安裝套件的內容。

若要所有安裝套件的獨立安裝套件清單：

在上述清單中，點擊**檢視獨立安裝套件清單**按鈕。

在獨立安裝套件清單中會顯示其以下內容：

- **檔案名稱**.自動形成為包含在套件與應用程式版本中之應用程式名稱的獨立安裝套件名稱。
- **應用程式名稱**.包含在獨立安裝套件中的應用程式名稱。
- **應用程式版本**.
- **網路代理的安裝檔案名稱**.僅在網路代理包含在獨立安裝套件中時才會顯示內容。
- **網路代理版本**.僅在網路代理包含在獨立安裝套件中時才會顯示內容。
- **大小**.檔案大小為 MB。
- **群組**.網路代理安裝後要將用戶端裝置移動過去的群組名稱。
- **建立日期**.建立獨立安裝套件的日期和時間。
- **已修改**.修改獨立安裝套件的日期和時間。
- **路徑**.獨立安裝套件所在資料夾的完整路徑。
- **網址**.獨立安裝套件位置的網址。
- **檔案雜湊值**.該內容會用來驗證獨立安裝套件不是由協力廠商變更，且使用者有您建立與傳輸給使用者的相同檔案。

若要檢視特定安裝套件的獨立安裝套件清單：

選取清單中的安裝套件，並在清單上點擊**檢視獨立安裝套件清單**按鈕。

在獨立安裝套件清單中，您可：

- 點擊**發佈**按鈕，在網路伺服器上發佈獨立安裝套件。收到您傳送之獨立安裝套件連結的使用者，可下載已發佈的獨立安裝套件。
- 點擊**取消發佈**按鈕，取消網路伺服器上獨立安裝套件的發佈。只有您與其他管理員可下載取消發佈的獨立安裝套件。
- 點擊**下載**按鈕，下載獨立安裝套件至您的裝置。
- 點擊**透過電子郵件傳送**按鈕，傳送含有連至獨立安裝套件的連結。
- 點擊**刪除**按鈕，移除獨立安裝套件。

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到裝置，您可以在精靈視窗中指定裝置，使用以下方式之一：

- **選取管理伺服器偵測到的網路裝置**.此種情況下，工作被分配到指定裝置。特定裝置可以包含管理群組的裝置和未配置的裝置。
- **手動指定裝置位址或從清單匯入位址**.您可以指定您要為其分配工作的裝置的 DNS 名稱、IP 位址和 IP 子網路。
- **分配工作到裝置分類**.此種情況下，工作被分配到先前建立的分類中的裝置。您可以指定預設分類或您所建立的自訂分類。
- **分配工作到管理群組**.此種情況下，工作被分配到先前建立的管理群組中的裝置。

若您要在為安裝網路代理的裝置上正確進行遠端安裝，您必須開啟以下的連接埠：a) TCP 139 和 445；b) UDP 137 和 138。依預設，網域中所有裝置將自動開啟這些連接埠。它們被使用遠端安裝準備實用程式自動開啟。

安裝應用程式到特定裝置

本節包含有關如何在管理組、具有特定 IP 位址的裝置或選擇的受管裝置上遠端安裝應用程式的資訊。

若要安裝應用程式到特定裝置：

1. 要進行此項工作的裝置必須連線至管理伺服器。
2. 在主功能表中，轉至 **裝置 → 工作**。
3. 點擊**新增**。
   新增工作精靈啟動。
4. 在**工作類型**欄位中，選取**遠端安裝應用程式**。
5. 您可以選取以下其中一個方法：
   - **分配工作到管理群組**

     工作被分配到包含在管理群組中的裝置。您可以指定現有群組之一或者建立新群組。
     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。
   - **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分類中的裝置。您可以指定現有分類之一。
     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. 遵照精靈的說明。
   新增工作精靈會在特定裝置上建立精靈中所選應用程式的遠端安裝工作。如果您選擇了**分配工作到管理群組**選項，工作將是一個組工作。
7. 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。

遠端安裝任務完成後，所選應用程式將安裝在指定裝置上。

透過 Active Directory 群組政策安裝應用程式

卡巴斯基安全管理中心可以讓您在受管理裝置上使用 Active Directory 群組政策安裝 Kaspersky 應用程式。

> 您必須連同安裝套件中的網路代理一起安裝，才使用 Active Directory 的群組政策進行安裝應用程式。

使用 Active Directory 的群組政策安裝應用程式，請執行以下操作：

1. 執行防護部署精靈。遵照精靈的說明。
2. 在防護部署精靈的**遠端安裝工作設定**頁面，啟用**在 Active Directory 群組政策中指定安裝套件的安裝**選項。
3. 在選取帳戶以存取裝置頁面上選取**需要帳戶（不使用網路代理）**選項。
4. 在安裝了卡巴斯基安全管理中心的裝置上新增帶有管理員權限的帳戶或包含在"群組政策建立器所有者"網域群組的帳戶。
5. 將權限授予所選帳戶：
   a. 轉到**控制面板→管理工具**，然後開啟**群組政策管理**。
   b. 點擊具有所需網域的節點。
   c. 點擊**委派**區段。
   d. 在**權限**下拉功能表中，選取**連結 GPO**。
   e. 點擊**新增**。
   f. 在開啟的**選取使用者、電腦或群組**視窗中，選取所需的帳戶。

g. 點擊**"確定"**關閉**"選取使用者、電腦或群組**視窗。

h. 在**群組和使用者**清單中，選取剛剛新增的帳戶，然後點擊**進階 → 進階**。

i. 在**權限項目**清單中，按兩下剛剛新增的帳戶。

j. 授予以下權限：

- **建立群組物件**
- **刪除群組物件**
- **建立群組政策容器物件**
- **刪除群組政策容器物件**

k. 點擊**"確定"**儲存變更。

6. 按照精靈的說明定義其他設定。

7. 手動執行建立的遠端安裝工作，或等待排程啟動。

啟動該工作之後，將會進行遠端安裝的流程：

1. 工作執行時，以下的物件將會建立在指定裝置上的網域中：
   - 名稱 **Kaspersky_AK{GUID}** 下的群組政策物件（GPO）。
   - 對應於 GPO 的安全群組。該安全群組包含工作覆蓋的用戶端裝置。安全群組的內容定義了 GPO 的範圍。
2. 在這種情況下，卡巴斯基安全管理中心會直接從程式名為「共享」的共用網路資料夾在使用者端裝置上安裝程式。在卡巴斯基安全管理中心的安裝資料夾中，系統將建立一個輔助嵌套資料夾，其中包含安裝應用程式所需的 .msi 檔案。
3. 當新裝置新增到此工作範圍內時，這些新電腦將會在下個工作啟動時，自動加入到安全性群組。如果在工作排程中選定**"執行略過的工作"**選項，則裝置將立即加入安全群組。
4. 當從工作範圍中刪除了裝置，在下個工作啟動時，將會將其安全性群組中刪除。
5. 當您從 Active Directory 中刪除了此工作，GPO、連至 GPO 的連結，還有安全性群組都會刪除。

如果您要透過 Active Directory 安裝其他的程式，您可以手動的進行調整這些設定。例如，這可能會發生在以下狀況：

- 當病毒防護管理員沒有權限進行更動網域中的 Active Directory 時
- 原始安裝套件必須儲存在單獨的網路資源上時
- 當需要將 GPO 連結到特定的 Active Directory 單元時

在 Active Directory 中有以下情況，可使用下列另一種安裝方式：

- 如果直接從卡巴斯基安全管理中心共用資料夾進行安裝，您必須在 GPO 內容中為所需應用程式指定 .msi 檔案（位於安裝套件的 exec 子資料夾中）。
- 如果必須將安裝套件放置在其他網路資源上，您必須將整個 exec 資料夾的內容複製過去，因為除了副檔名為 .msi 的檔案外，該資料夾還包含建立安裝套件時建立的設定檔。要安裝與該程式相關聯的產品授權金鑰，請將金鑰檔案一起複製到該資料夾中。

在從屬管理伺服器上安裝應用程式

在從屬管理伺服器上安裝應用程式：

1. 若要進行此項工作的從屬管理伺服器，必須連線至管理伺服器。
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。為此目的，請建立**發佈安裝套件**類型的工作。
3. 在從屬管理伺服器上建立一個遠端應用程式安裝工作。選取**將應用程式遠端安裝到從屬管理伺服器**工作類型。

   新增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。

遠端安裝任務完成後，所選應用程式將安裝在從屬管理伺服器上。

指定在 Unix 裝置上進行遠端安裝的設定

使用遠端安裝工作在 Unix 裝置上安裝應用程式時，可以為工作指定 Unix 特定的設定。建立工作後，這些設定可在工作屬性中使用。

要為遠端安裝工作指定特定於 Unix 的設定，請執行以下操作：

1. 在主功能表中，轉至 **裝置 → 工作**。
2. 點擊您要為其指定 Unix 特定設定的遠端安裝工作名稱。
   工作內容視窗隨即開啟。
3. 前往**應用程式設定 → Unix 特定設定**。
4. 指定下列設定：
   - **設定根帳戶密碼（僅適用於透過 SSH 佈署）**

     如果不指定密碼，無法在目標裝置上使用 sudo 指令，選擇此選項，然後指定 root 帳戶的密碼。卡巴斯基安全管理中心 14 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 14 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 14 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。

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在安裝安全應用程式到受管理裝置之前移除不相容的應用程式。

說明：安裝前移除不相容的應用程式

透過專用工作移除不相容的應用程式

要移除不相容的應用程式，使用**遠端移除應用程式**工作。該工作應該在安全應用程式安裝工作執行之前執行在裝置。例如，在安裝工作中，您可以選取**在完成其它工作時**作為排程類型，其中的其他工作為**遠端移除應用程式**。

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。

說明：建立工作

遠程刪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. 在主應用程式視窗，點擊**裝置 → 工作**。
2. 點擊**新增**。
   新增工作精靈啟動。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，請選取**遠端解除安裝應用程式**工作類型。

4. 指定您正建立的工作的名稱。

   工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元（ *<>-_?:\"| ）。

5. 選取要分配工作的裝置。

6. 選擇要刪除的軟體類型，然後選擇要刪除的特定應用程式，更新或修補程式：

   - **解除安裝受管理應用程式**

     顯示 Kaspersky 應用程式清單。選取您要移除的弱點。

   - **解除安裝不相容的應用程式**

     顯示與 Kaspersky 安全應用程式或卡巴斯基安全管理中心不相容的應用程式清單。選取您要刪除之項目旁的核取方塊。

   - **從應用程式登錄資料中解除安裝應用程式**

     預設情況下，網路代理會傳送管理伺服器有關受管理裝置上安裝的應用程式資訊。已安裝的應用程式清單會儲存在應用程式登錄資料中。

     要從應用程式登錄資料中選取一個應用程式：

     a. 點擊**要解除安裝的應用程式**欄位，然後選擇要刪除的應用程式。

     b. 指定移除選項：

     - **解除安裝模式**

       選取您要如何移除該應用程式：

       - **自動定義解除安裝指令**

         如果應用程式具有應用程式供應商定義的解除安裝命令，則卡巴斯基安全管理中心將使用此命令。我們建議您選取此選項。

       - **指定解除安裝指令**

         如果要為解除安裝應用程式指定自己的命令，請選取此選項。

         建議您先嘗試使用**自動定義解除安裝指令**選項。如果透過自動定義的解除安裝命令失敗，請使用自己的命令。

         在該欄位中鍵入安裝命令，然後指定以下選項：

         除非未自動偵測預設指令，否則將使用此指令進行解除安裝

         卡巴斯基安全管理中心會檢查所選應用程式是否具有應用程式供應商定義的解除安裝命令。如果找到該命令，則卡巴斯基安全管理中心將使用該命令，而不是**應用程式解除安裝指令**欄位中指定的命令。

         我們建議您啟用該選項。

     - **應用程式成功解除安裝後執行重新啟動**

       如果應用程式要求成功移除後在受管理裝置上重新啟動作業系統，則作業系統將會自動重新啟動。

7. 指定用戶端裝置將如何下載解除安裝公用程式：

   - **使用網路代理**

     檔案會透過安裝在這些用戶端裝置上的網路代理傳遞到用戶端裝置。

     如果停用此選項，則會使用 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。使用 **使用網路代理** 或者 **透過發佈點使用作業系統資源** 選項。

檔案將被使用管理伺服器作業系統工具傳輸到用戶端裝置。如果使用者端裝置上未安裝網路代理，但是使用者端裝置與管理伺服器在同一網路，則您可以啟用此選項。

- **透過發佈點使用作業系統資源**

使用作業系統工具透過發佈點將檔案傳輸到用戶端裝置。如果網路中存在不止一個發佈點，那麼您可以選取此選項。

如果啟用**使用網路代理**方塊，僅在網路代理工具不可使用時才會透過作業系統工具傳送檔案。

- **同時下載的最大數量**

管理伺服器可以同時向其傳輸檔案的最大用戶端裝置數量。此數字越大，應用程式解除安裝的速度越快，但是管理伺服器上的負載會更高。

- **解除安裝嘗試次數上限**

若是在執行*遠端解除安裝應用程式*工作時，卡巴斯基安全管理中心解除安裝受管理裝置的應用程式失敗超過指定次數，卡巴斯基安全管理中心會停止傳送解除安裝公用程式到該受管理裝置，且不再在該裝置上啟動安裝程式。

解除安裝嘗試次數上限參數允許您節省受管理裝置資源，以及減少流量（移除、MSI 檔案執行和錯誤訊息）。

重複的工作啟動嘗試可能提示裝置具有妨礙解除安裝的問題。管理員應在指定的移除嘗試次數內解決問題，然後重新啟動工作（手動或按排程）。

如果解除安裝始終未完成，問題被視為無法解決且後續工作啟動被認為是不必要的資源和流量浪費。

建立該工作時，嘗試技術會設定為 `0`。返回錯誤的安裝程式的每次執行都增加計數。

如果超過指定的嘗試次數且裝置已準備好解除安裝應用程式，您可以增加**解除安裝嘗試次數上限**參數的值並啟動工作以解除安裝應用程式。或者，您可以建立新的*遠端解除安裝應用程式*工作。

- **下載之前驗證作業系統類型**

在將檔案傳輸到用戶端裝置之前，卡巴斯基安全管理中心將檢查「解除安裝公用程式」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，也不會嘗試解除安裝應用程式。例如，要從包括執行各種作業系統之裝置的管理群組裝置中移除某些應用程式，您可以將解除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。

8. 指定作業系統重新啟動設定：

- **不重新啟動裝置**

用戶端電腦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。

- **強制關閉已鎖定連線的應用程式**

執行應用程式可能會阻止用戶端裝置重新啟動。例如，如果文件在文書處理應用程式中編輯且未儲存，應用程式不會允許裝置重新啟動。

如果啟用該選項，鎖定裝置上的此類應用程式在裝置重新啟動前被強制關閉。結果，使用者可能遺失他們未儲存的變更。

如果停用該選項，鎖定裝置不被重新啟動。此裝置上的工作狀態表示裝置需要重新啟動。使用者必須手動關閉所有執行在鎖定裝置上的應用程式並重新啟動這些裝置。

預設情況下已停用該選項。

9. 如果必要，請新增要用於啟動遠端解除安裝工作的帳戶：

- **不需要帳戶（網路代理已安裝）**

如果該選項被選中，您不是必須指定一個帳戶，並在該帳戶下執行程式的安裝。將使用執行管理伺服器服務的帳戶執行該工作。

如果網路代理未安裝在用戶端裝置，該選項不可用。

- **需要帳戶（不使用網路代理）**

  如果該選項被選中，您可以指定一個帳戶，並在該帳戶下執行程式的安裝。如果網路代理未安裝在被分配工作的裝置上，您可以指定帳戶。

  您可以根據情況指定多個帳戶，例如，沒有一個帳戶擁有分配工作所對應裝置上全部所需權限時。在此情況下，已經新增的所有帳戶都用於從上到下按順序執行該工作。

  如果尚未新增任何帳戶，將使用執行管理伺服器服務的帳戶執行該工作。

10. 若要修改預設工作設定，請啟用**完成工作建立**頁面的**建立完成時開啟工作詳情**選項。如果您不啟用該選項，工作使用預設設定建立。您可以稍後隨時修改預設設定。
11. 點擊**完成**按鈕。

    工作被建立並顯示在工作清單。
12. 點擊建立的工作的名稱以開啟工作內容視窗。
13. 在工作內容視窗中，指定一般工作設定。
14. 點擊**儲存**按鈕。
15. 您可以手動執行此工作，或等候工作設定中指定的排程將其啟動。

    遠端解除安裝工作完成時，所選應用程式從特定的裝置中移除。

準備一部執行 SUSE Linux Enterprise Server 15 的裝置以安裝網路代理

要在裝有 SUSE Linux Enterprise Server 15 作業系統的裝置上安裝網路代理：

在安裝網路代理之前，執行以下指令：

```
$ sudo zypper install insserv-compat
```

這使您能夠安裝 insserv-compat 套件並正確配置網路代理。

執行 `rpm -q insserv-compat` 指令來檢查套件是否已經安裝。

如果您的網路包含大量執行 SUSE Linux Enterprise Server 15 的裝置，您可以使用用來配置和管理公司基礎結構的特殊軟體。透過使用此軟體，您可以一次在所有必要的裝置上自動安裝 insserv-compat 套件。例如，您可以使用 Puppet、Ansible、Chef，可以製作自己的指令碼 — 使用任何方便的方法。

準備好 SUSE Linux Enterprise Server 15 裝置後，部署和安裝網路代理。

Kaspersky 應用程式：產品授權和啟動

本章節說明使用受管理的 Kaspersky 應用程式產品授權金鑰的卡巴斯基安全管理中心功能。

卡巴斯基安全管理中心 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生成一份產品授權金鑰使用情況的報告，並通知管理員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

新增金鑰檔案或啟動碼至受管理應用程式安裝套件

對於安全應用程式，該選項不被建議。新增至安裝套件的產品授權金鑰或啟動碼可能會有安全風險。

如果您使用安裝套件安裝受管理應用程式，您可以在該安裝套件中或在應用程式政策中指定啟動碼或金鑰檔案。產品授權金鑰將在下一次裝置與管理伺服器同步時被佈署到受管理裝置。

說明：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 → Kaspersky 產品授權**。
2. 點擊**新增**按鈕。
3. 選取您要新增的內容：
   - **新增金鑰檔案**
     點擊**選取金鑰檔案**按鈕並瀏覽至要新增的金鑰檔案。
   - **輸入啟動碼**
     指定文字欄位中的啟動碼並點擊**傳送**按鈕。

4. 點擊**關閉**按鈕。

產品授權金鑰或幾個產品授權金鑰被新增到管理伺服器儲存區。

佈署產品授權金鑰到用戶端裝置

卡巴斯基安全管理中心 14 網頁主控台可讓您使用*產品授權金鑰分發*工作將產品授權金鑰分發至用戶端裝置。

要將產品授權金鑰發佈至用戶端裝置，請執行以下操作：

1. 在主功能表中，轉至 **裝置 → 工作**。
2. 點擊**新增**。
   新增工作精靈啟動。
3. 選取您要新增產品授權金鑰的應用程式。
4. 從**工作類型**清單選取**新增產品授權金鑰**。
5. 請按照精靈的步驟進行操作。
6. 若要修改預設工作設定，請啟用**完成工作建立**頁面的**建立完成時開啟工作詳情**選項。如果您不啟用該選項，工作使用預設設定建立。您可以稍後隨時修改預設設定。
7. 點擊**建立**按鈕。
   工作被建立並顯示在工作清單。
8. 若要執行工作，請在工作清單選取該工作，並點擊**開始**按鈕。

當工作完成時，產品授權金鑰被佈署到所選裝置。

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 → Kaspersky 產品授權**。
2. 選取您要自動發佈到裝置的產品授權金鑰名稱。
3. 在開啟的產品授權金鑰內容視窗中，選取**自動分發產品授權金鑰到受管理裝置**核取方塊。
4. 點擊**儲存**按鈕。

產品授權金鑰將被自動分發到所有相容的裝置。

產品授權金鑰發佈是使用網路代理執行的。沒有為應用程式建立產品授權金鑰發佈工作。

在自動分發產品授權金鑰過程中，系統會考慮產品授權對裝置數量的限制。授權限制會在產品授權金鑰的內容中設定。若達授權限制，則會自動停止分發此裝置上的產品授權金鑰。

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，您可以之後手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

要檢視新增到管理伺服器儲存區的產品授權金鑰清單：

在主功能表中，轉至 **操作 → 產品授權 → Kaspersky 產品授權**。

顯示清單包含新增至管理伺服器儲存區的金鑰檔案與啟動碼。

要檢視關於產品授權金鑰的詳細資訊：

1. 在主功能表中，轉至 **操作 → 產品授權 → Kaspersky 產品授權**。
2. 點擊所需產品授權金鑰的名稱。

在開啟的產品授權金鑰內容視窗，您可以檢視：

- 在**一般**頁籤—產品授權金鑰的主資訊
- 在**裝置**頁籤—用戶端裝置清單，裝置中的產品授權金鑰用來啟動已安裝的 Kaspersky 應用程式

要檢視哪些產品授權金鑰被佈署到特定用戶端裝置：

1. 在主功能表中，轉至 **裝置 → 受管理裝置**。
2. 點擊所需裝置的名稱。
3. 在開啟的裝置內容視窗中，選取**應用程式**頁籤。
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，點擊**一般**頁籤，然後開啟**產品授權**區段。

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。

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. 前往**操作 → 產品授權 → Kaspersky 產品授權**。
2. 選取您要從儲存區刪除的金鑰檔案或啟動碼。
3. 點擊**刪除**按鈕。
4. 請點擊**確定**按鈕來確認操作。

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

若您決定停止保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。
2. 在清單中，選取您要撤銷協議的 EULA。
   您可以檢視 EULA 的下列內容：
   - 接受 EULA 的日期
   - 接受 EULA 的使用者名稱
3. 點擊任何 EULA 的接受日期以開啟其顯示以下資料的內容視窗：
   - 接受 EULA 的使用者名稱
   - 接受 EULA 的日期
   - EULA 的唯一識別碼 (UID)
   - EULA 的完整內容
   - EULA 連結的物件清單（安裝套件、無縫更新、行動應用程式），以及其各自的名稱與類型
4. 在 EULA 內容視窗的下部，點擊**撤銷產品授權協議**按鈕。

若存在任何物件（安裝套件與其各自工作）防止撤銷 EULA，則會顯示對應的通知。刪除這些物件前，您無法處理撤銷。

在開啟的視窗中，系統會告知您必須先解除安裝對應至 EULA 的 Kaspersky 應用程式。

5. 按一下按鈕以確認撤銷。

EULA 已撤銷。這不會在顯示於 **最終使用者產品授權協議** 區段的產品授權協議清單中。EULA 內容視窗關閉；應用程式將不再繼續安裝。

續約 Kaspersky 應用程式的產品授權

您可以續約已過期或即將過期（少於 30 天）的 Kaspersky 應用程式產品授權。

要續約過期的產品授權或即將過期的產品授權：

1. 做以下之一：
   - 在主功能表中，轉至 **操作 → 產品授權 → Kaspersky 產品授權**。
   - 在主功能表中，轉至**監控和報告 → 控制板**，然後點擊通知旁邊的"**檢視即將到期的產品授權**"連接。

   Kaspersky 產品授權 視窗將開啟，您可以在其中檢視和續約產品授權。
2. 點擊所需產品授權旁邊的 **續約產品授權** 連接。

   點擊產品授權續約連接，即表示您同意向 Kaspersky 傳輸關於卡巴斯基安全管理中心的以下資訊：其版本、您使用的當地語係化版本、軟體產品授權 ID（即您要續約的產品授權 ID）以及您是否透過合作夥伴公司購買了產品授權。
3. 在開啟的產品授權續約服務視窗中，按照說明續約產品授權。

   產品授權已續約。

在卡巴斯基安全管理中心 14 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 商務解決方案範圍，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 14 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**

此級別對於具有複雜和分佈式 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 商務解決方案：

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 商務解決方案。
2. 要僅檢視適合您組織的解決方案，請在篩選器中選擇所需的值。
3. 點擊您想要購買或了解更多資訊的解決方案。

您將被重新導向到解決方案網頁。您可以按照熒幕上的指示進行購買。

配置網路防護

本節包含有關政策和工作的手動配置、使用者角色、建構管理群組結構和工作階層的資訊。

情境：配置網路防護

快速啟動精靈會建立含預設設定的政策與工作。這些設定可能對組織來說並不是最佳設定，甚至不被允許。因此，建議您微調這些政策與工作，並在您網路有需求時，建立其他政策與工作。

先決條件

在您開始之前，確保您已做了如下：

- 已安裝卡巴斯基安全管理中心管理伺服器
- 已安裝卡巴斯基安全管理中心 14 網頁主控台
- 已完成卡巴斯基安全管理中心主安裝情境
- 完成快速設定精靈，或在**受管理裝置**管理群組手動建立以下政策和工作：
  - Kaspersky Endpoint Security 政策
  - 更新 Kaspersky Endpoint Security 的群組工作
  - 網路代理政策

設定要以階段進行的網路防護：

1. **設定和傳播 Kaspersky 應用程式政策和政策設定檔**

   要為安裝在受管理裝置上的 Kaspersky 應用程式配置和傳播設定，您可以使用兩種不同的安全管理方法—以裝置為中心或以使用者為中心。這兩種方法也可以被合併。

2. **配置工作以遠端管理 Kaspersky 應用程式**

   檢查使用快速啟動精靈建立的工作並調整它們，如有必要。

   說明：為 Kaspersky Endpoint Security 設定群組工作。

   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**

   這些資料是由被管理的用戶端電腦傳送，並儲存至管理伺服器的資料庫當中。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：設定事件最大數量。

結果

當您完成該方案時，您將透過配置 Kaspersky 應用程式、工作和管理伺服器接收的事件來防護您的網路：

- Kaspersky 應用程式會根據政策與政策設定檔設定。
- 應用程式會透過一組工作管理。
- 儲存在資料庫的事件數量上限已設定。

當網路防護配置完成時，您可以繼續配置 Kaspersky 資料庫和應用程式的一般更新。

關於以裝置為中心和以使用者為中心的安全管理方法

您可以從裝置功能的立場和從使用者角色的立場管理安全設定。第一種方法叫做*以裝置為中心的安全管理*，第二種叫做*以使用者為中心的安全管理*。要應用不同的應用程式設定到不同的裝置，您可以使用兩種方法的任意或組合。

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，您可以應用特別應用程式設定到單個使用者。這可能用在員工在公司有獨一角色或您要監控與個別人的裝置相關的安全事故時。取決於該員工在公司的角色，您可以延伸或限制該員工變更應用程式設定的權限。例如，您可能要延伸在本機辦公室管理用戶端裝置的系統管理員的權限。

您也可以組合以裝置為中心的安全管理和以使用者為中心的安全管理方法。例如，您可以為每個管理群組設定特別的應用程式政策，然後為一個或幾個使用者角色建立政策設定檔。在此情況下，政策和政策設定檔會按照以下優先順序加以套用：

1. 為以裝置為中心的安全管理建立的政策被應用。
2. 政策設定檔會根據政策設定檔優先順序內容加以修改。
3. 政策被與使用者角色關聯的政策設定檔修改。

政策設定和傳播：以裝置為中心的方法

當您完成該方案後，應用程式將在所有受管理裝置上被設定，與您定義的應用程式政策和政策設定檔一致。

先決條件

開始前，請確保您已安裝了卡巴斯基安全管理中心管理伺服器和卡巴斯基安全管理中心 14 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設定您網路的防護時，卡巴斯基安全管理中心為 Kaspersky Endpoint Security for Linux 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次要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**

預設下，卡巴斯基安全管理中心每 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

當以裝置為中心的方案完成時，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管理伺服器和卡巴斯基安全管理中心 14 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次要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。

Kaspersky Endpoint Security 更新群組工作的手動設定

Kaspersky Endpoint Security 最佳與建議的排程選項為**當新更新下載至儲存區時**（如果選取了**使用工作啟動自動隨機延遲**核取方塊。）

網路代理政策設定

延伸所有 | 折疊所有

若設定網路代理政策：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。
2. 點擊網路代理政策的名稱。

網路代理政策的內容視窗開啟。

一般

在此頁簽上，您可以修改政策狀態並指定政策設定的繼承：

- 在**政策狀態**區塊，您可以選取政策的模式：
  - **啟用政策**

    如果選取該選項，政策將變為啟用狀態。
    預設情況下已選定此選項。

  - **停用政策**

    如果選取該選項，政策將變為不啟用狀態，但它仍然儲存在**"政策"**資料夾中。如果需要，您可以啟動該政策。

- 在**設定繼承**設定群組中，您可以配置政策繼承：
  - **從父政策繼承設定**

    如果啟用此選項，則政策設定值將繼承上一級群組政策，因而會受到鎖定。
    預設情況下已啟用該選項。

  - **在子政策中強制繼承設定**

如果啟用此選項，則在套用政策變更之後，程式將執行以下操作：

- 政策設定的值將被傳送到階層管理群組的政策，也就是孩子政策。
- 在每個子政策內容視窗的**一般**區域的**設定繼承**區塊，系統將自動選取**從父政策繼承設定**核取方塊。

如果啟用此方塊，則會鎖定子政策設定。

預設情況下已停用該選項。

事件配置

在此頁簽上，您可以配置事件記錄和事件通知。事件根據重要性級別分佈在在以下部分中的 **事件配置** 頁簽上：

- **功能失效**
- **警告**
- **資訊**

在每個區域，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** 部分，您可以配置 **發生了事件。** 事件類型。例如，當發佈點的可用磁碟空間小於 2 GB（遠端安裝應用程式和下載更新至少需要 4 GB）時，此類事件可能發生。若要配置 **發生了事件。** 事件，點擊它並指定儲存發生的事件的位置以及如何通知它們。

如果網路代理偵測到事件，您可以使用受管理裝置設定。

應用程式設定

設定

在**設定**區域，您可以配置網路代理政策：

- **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或漫遊政策的名稱
  - 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
  - 政策設定檔

    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。

儲存區

在**儲存區**區域，您可以選取將其資訊從網路代理傳送到管理伺服器的物件類型。如果網路代理政策禁止本區域中某些設定，則您無法修改這些設定。

- **已安裝應用程式詳情**

  如果啟用此選項，會將安裝在用戶端裝置上的應用程式資訊傳送至管理伺服器。

  預設情況下已啟用該選項。

- **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。

網路

網路區域包含三個子區域：

- **連線**
- **連線設定檔**
- **連線排程**

在**連線**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。
    若同步間隔社為少於 15 分鐘，同步會每 15 分鐘執行一次。若同步間隔設為 15 分鐘或更多，同步會以特定同步間隔執行。

  - **壓縮網路流量**

    如果啟用此選項，則透過減少所傳輸的流量進而減少管理伺服器的負載來提高網路代理的資料傳輸速度。

    用戶端裝置上的 CPU 負載可能會增加。

    預設情況下會啟用此核取方塊。

  - **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。連線到 KSN 代理伺服器的預設 UDP 連接埠是 15111。

- **UDP 連接埠號**

  在該欄位中，您可以輸入 UDP 埠號。預設埠號為 15000。
  使用十進位系統記錄。

在 **網路** 區域的 **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。**連線設定檔**區域的設定僅在執行 Windows 的裝置上可用：

- **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**

連線設定檔僅支援執行 Windows 的裝置。我們不建議使用該選項。

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

在 **連線設定檔** 設定群組中，不能新增新項目到 **管理伺服器連線設定檔** 清單，所以 **新增** 按鈕無效。預設的連線設定檔也不能修改。

- **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：

- **Zeroconf**

如果啟用此選項，發佈點將使用零配置網路（也稱為 *Zeroconf*）用 IPv6 裝置自動輪詢網路。在這種情況下，啟用的 IP 範圍輪詢將被忽略，因為發佈點會輪詢整個網路。

要開始使用 Zeroconf，必須滿足以下條件：

- 發佈點必須執行 Linux。
- 您必須在發佈點上安裝 avahi-browse 公用程式。

如果停用此選項，則發佈點不會使用 IPv6 裝置輪詢網路。

預設情況下已停用該選項。

- **IP 範圍**

如果啟用此選項，則管理伺服器將按照您按一下**設定輪詢排程**連結所配置的排程自動輪詢 IP 範圍。

如果停用此選項，則管理伺服器將不輪詢 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。

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**

  如果啟用該方塊，您可以在輸入欄位中為代理伺服器身分驗證指定憑證。
  預設情況下會停用此核取方塊。

- **使用者名稱**
- **密碼**

更新（發佈點）

在**更新（發佈點）**部分，您可以啟用下載差異檔案功能，以便發佈點以差異檔案的形式從卡巴斯基更新伺服器獲取更新。

變更歷程

在此頁籤上，您可以檢視政策修訂的清單並復原對政策進行的變更（如有必要）。

變更裝置移動規則的優先順序

所有裝置移動規則都有優先順序。

要提高或降低移動規則的優先順序，

使用滑鼠分別在清單中向上或向下移動規則。

工作

該部分描述了卡巴斯基安全管理中心使用的工作。

關於工作

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

特定應用程式的工作可以使用卡巴斯基安全管理中心 14 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 14 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 14 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次要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。

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

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

- 指定裝置分類。

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

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

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

建立工作

要建立工作：

1. 在主功能表中，轉至 **裝置 → 工作**。
2. 點擊**新增**。

   新增工作精靈啟動。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。

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。您可以隨時手動啟動工作。

若要手動啟動工作：

1. 在主功能表中，轉至 **裝置 → 工作**。

2. 在工作清單中，請選取您要啟動之工作旁的核取方塊。

3. 點擊**開始**按鈕。

工作啟動。您可在**狀態**欄中查看工作狀態或點擊**結果**按鈕。

檢視工作清單

您可檢視在卡巴斯基安全管理中心 Linux 建立的工作清單。

若要檢視工作清單，

前往**裝置 → 工作**。

工作清單隨即顯示。工作會依與應用程式名稱的關聯來分組。例如，*遠端安裝應用程式*工作會與管理伺服器相關，*更新*工作則指 Kaspersky Endpoint Security for Linux。

若要檢視工作內容，

請點擊工作的名稱。

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

延伸所有 | 折疊所有

此區段會列出您可檢視與為工作指定的清單。

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**

    用戶端電腦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。

  - **強制關閉已鎖定連線的應用程式**

    執行應用程式可能會阻止用戶端裝置重新啟動。例如，如果文件在文書處理應用程式中編輯且未儲存，應用程式不會允許裝置重新啟動。

    如果啟用該選項，鎖定裝置上的此類應用程式在裝置重新啟動前被強制關閉。結果，使用者可能遺失他們未儲存的變更。

    如果停用該選項，鎖定裝置不被重新啟動。此裝置上的工作狀態表示裝置需要重新啟動。使用者必須手動關閉所有執行在鎖定裝置上的應用程式並重新啟動這些裝置。

    預設情況下已停用該選項。

- 工作排程設定：
  - **排程開始**

    選取工作執行排程並設定所選排程。

    - **每 N 小時**

      工作定期執行，按照指定小時數間隔，從指定的日期和時間開始。

      預設下，工作每六小時執行一次，從目前系統日期和時間開始。

- **每 N 天**

  工作定期執行，按照指定天數間隔。此外，您可指定第一個工作執行的日期與時間。這些額外選項會在您建立的工作受到應用程式支援時可用。

  預設下，工作每天執行一次，從目前系統日期和時間開始。

- **每 N 星期**

  工作定期執行，按照指定星期數間隔，從指定的星期和時間開始。

  預設下，工作每星期一於目前系統時間執行一次。

- **每 N 分鐘**

  工作定期執行，按照指定分鐘數間隔，從工作建立日期的指定時間開始。

  預設下，工作每 30 分鐘執行一次，從目前系統時間開始。

- **每天（不支援日光節約時間）**

  工作定期執行，按照指定天數間隔。排程不支援日光節約時間 (DST)。這意味著在夏令時開始和結束時當時鐘向前或向後撥動一小時時，實際工作啟動時間不變更。

  我們不建議您使用該排程。它用於向後相容卡巴斯基安全管理中心 Linux。

  預設下，工作每天於目前系統時間執行一次。

- **每週**

  工作每週在指定星期和指定時間執行。

- **按每星期中的指定日**

  工作定期執行，在指定星期的指定時間。

  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。

  預設情況下已啟用該選項。

- **每個月在所選週的指定天**

  工作定期在指定月日的指定時間執行。

  預設下，未選取月日；預設啟動時間是 6:00:00 P.M.。

- **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。您可以選取先前工作如何結束（成功或帶有錯誤）以觸發目前工作的啟動。

- **執行略過的工作**

  該選項決定在工作要啟動時用戶端裝置在網路中不可見時工作的行為。

  如果啟用該選項，系統將在下一次在用戶端裝置上執行 Kaspersky 應用程式時嘗試啟動工作。如果工作排程是**手動**、**一次**或**立即**，裝置在網路中可見或包含在工作範圍後，工作會立即啟動。

  如果停用該選項，則只有已排程的工作會在用戶端裝置上啟動，而對於**手動**、**一次**與**立即**而言，僅在網路中可見的用戶端裝置上會啟動。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。

  預設情況下已啟用該選項。

- **使用工作啟動自動隨機延遲**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動，即是，*分佈式工作啟動*。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  當工作被建立時，根據工作中包含用戶端裝置的數量，分發啟動時間被自動計算。然後，工作總是在計算的開始時間啟動。然後當工作設定被編輯或者工作被手動啟動時，計算的工作啟動時間值被變更。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

- **使用工作啟動隨機延遲間隔（分鐘）**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

  預設情況下已停用該選項。預設時間間隔為一分鐘。

- 要分配工作的裝置：

  - **選取管理伺服器偵測到的網路裝置**

    工作被分配到指定裝置。特定裝置可以包含管理群組的裝置和未配置的裝置。

    例如，您可能要在安裝網路代理到未配置的裝置的工作中使用該選項。

  - **手動指定裝置位址或從清單匯入位址**

    您可以指定您要為其分配工作的裝置的 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分類中的裝置。您可以指定現有分類之一。

    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。您可以指定現有群組之一或者建立新群組。

    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。

- 帳戶設定：

  - **預設帳戶**

    在與執行該工作的應用程式相同的帳戶下執行該工作。

    預設情況下已選定此選項。

  - **指定帳戶**

    填寫**帳戶**與**密碼**欄位以指定工作要在其下執行的帳戶詳情。帳戶必須對此工作有足夠的權限。

  - **帳戶**

執行該工作的帳戶。

- **密碼**

  工作執行時使用的帳戶的密碼。

工作建立後指定的設定

您可以在建立工作後指定以下設定。

- 群組工作設定：
  - **分發到子群組**

    此選項僅在群組工作的設定中可用。
    啟用此選項時，工作範圍包括：
    - 您在建立工作時選擇的管理群組。
    - 依據群組層次結構從屬於所選管理群組的任何級別下的管理群組。

    停用此選項時，工作範圍僅包括您在建立工作時選擇的管理群組。
    預設情況下已啟用該選項。

  - **分發到從屬和虛擬管理伺服器**

    啟用此選項時，在主管理伺服器上有效的工作也將套用於從屬管理伺服器（包括虛擬伺服器）。如果從屬管理伺服器上已經存在相同類型的工作，則這兩個工作都將套用到從屬管理伺服器上 — 現有的工作和從主管理伺服器繼承的工作。
    此選項僅在**分發到子群組**選項已啟用的情況下可用。
    預設情況下已停用該選項。

- 進階排程設定：
  - **透過 Wake-On-LAN 在工作啟動之前啟動裝置（分鐘）**

    裝置上的作業系統在工作開始之前的指定時間啟動。預設時間段為五分鐘。

    如果您想要工作在工作範圍內的所有用戶端裝置上執行，包括工作要啟動時關閉的裝置，則啟用該選項。

    若要裝置在工作完成後自動關閉，請啟用**完成工作後關閉裝置**選項。此選項可在相同視窗中找到。

    預設情況下已停用該選項。

  - **工作完成後關閉裝置**

    例如，您可能想為每週五工作時間後安裝更新到用戶端裝置的更新安裝工作啟用該選項，然後在週末關閉這些裝置。

    預設情況下已停用該選項。

  - **如果工作執行長於此時間則停止工作（分鐘）**

    在指定時間段過後，工作被自動停止，無論它是否完成。
    如果您想要中斷或停止執行時間太長的工作，則啟用該選項。
    預設情況下已停用該選項。預設工作執行時間是 120 分鐘。

- 通知設定：
  - **儲存工作歷程記錄**塊:
    - **儲存在管理伺服器資料庫上（天）**

有關工作範圍內所有用戶端裝置上的工作執行的應用程式事件在指定的天數內被儲存在管理伺服器。當該時間段過後，資訊被從管理伺服器刪除。

預設情況下已啟用該選項。

- **儲存在裝置的作業系統事件記錄中**

  有關工作執行的應用程式事件被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**。

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**裝置**頁面上，選取**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

延伸所有 | 折疊所有

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 14 網頁主控台的帳戶名稱。接著在**在工作中使用的目前密碼**欄位手動指定帳戶密碼。

- **指定不同帳戶**

  指定必須啟動工作的帳戶名稱。接著在**在工作中使用的目前密碼**欄位指定帳戶密碼。

若您填寫**先前密碼(可選，如果您要使用目前密碼更換它)**欄位，卡巴斯基安全管理中心僅會對已找到帳戶名稱與密碼的工作取代密碼。取代會自動執行。在所有其他情況下，您必須選擇進行精靈的下個步驟。

步驟 2：選取要採取的動作

若您未在精靈的第一步指定舊密碼或指定的舊密碼與工作內容中的密碼不符，您必須對已找到的工作選擇要採取的動作。

若要為工作選擇操作：

1. 選取您要為其選擇操作之工作旁邊的核取方塊。
2. 執行以下操作之一：
   - 若要移除工作內容中的密碼，請點擊**刪除憑證**。
     工作會切換為在預設帳戶下執行。
   - 若要用新的密碼取代，請點擊**即便舊密碼錯誤或未指定也強制密碼變更**。
   - 若要取消密碼變更，請點擊**未選擇操作**。

所選操作會在您移至精靈的下一步時套用。

步驟 3：檢視結果

在精靈的最後步驟中，檢視各個已找到工作的結果。要完成精靈，請點擊**"完成"**按鈕。

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。但無法瀏覽本機工作的執行結果。

要檢視工作結果：

1. 在工作內容視窗中，選取**一般**區域。

2. 點擊**結果**連結開啟**工作結果**視窗。

管理用戶端裝置

該部分說明如何管理管理群組中的裝置。

受管理裝置設定

延伸所有 | 折疊所有

要檢視受管理裝置設定：

1. 選取**裝置 → 受管理裝置**。
   受管理裝置清單隨即顯示。
2. 在受管理裝置清單中，點擊有所需裝置名稱的連結。

所選裝置的內容視窗隨即顯示。

一般

一般區域顯示有關用戶端裝置的一般資訊。資訊基於上一次用戶端裝置與管理伺服器之間的同步接收的資料來提供：

- **名稱**

  在該欄位中，您可以檢視和修改管理群組中的用戶端裝置名稱。

- **敘述**

  在該欄位中，您可以輸入用戶端裝置的附加敘述。

- **群組**

  包括了用戶端裝置的管理群組。

- **上次更新**

  裝置上資料庫或應用程式最後更新日期。

- **上一次可見**

  裝置在網路中最後可見的日期和時間。

- **連線至管理伺服器**

  裝置上的網路代理上一次連線到管理伺服器的日期和時間。

- **不斷開與管理伺服器的連線**

  如果啟用此選項，受管裝置和管理伺服器之間將保持持續連線。如果您使用的不是推送伺服器，您可能想要使用此選項，它提供了這樣的連線。

  如果停用此選項且不在使用推送伺服器，則受管理裝置將僅在同步資料或傳輸資訊時連線至管理伺服器。

  選取**不斷開與管理伺服器的連線**選項時的裝置數量上限是 300。

  預設情況下，受管裝置上停用此選項。預設情況下，此選項在安裝了管理伺服器的裝置上處於啟用狀態，即使您嘗試停用它也會保持啟用狀態。

網路

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。

系統

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。

防護

防護區域將通知您用戶端裝置上病毒防護的目前狀態：

- **裝置狀態**

  根據管理員針對裝置病毒防護狀態定義之條件，以及網路上裝置的活動所指派的用戶端裝置狀態。

- **所有問題**

  該表格包含了用戶端裝置上安裝的受管理應用程式偵測到的問題的完整清單。每個問題都伴有一個狀態，應用程式建議您分配該狀態到該問題的裝置。

- **即時防護**

  該欄位顯示目前的用戶端裝置即時防護狀態。
  當裝置狀態變更時，新狀態僅在用戶端裝置與管理伺服器同步之後顯示在裝置內容視窗。

- **上一次自訂掃描**

  用戶端裝置上執行的最後一次掃描的日期和時間。

- **偵測到的威脅總數**

  自安裝安全應用程式（第一次掃描）或自上次重設威脅計數器以來，在用戶端裝置上偵測到的威脅總數。

- **活動威脅**

  用戶端裝置上的未處理檔案數量。
  該欄位行動裝置上的未處理檔案數量。

由應用程式定義的裝置狀態

由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

應用程式區域列出用戶端裝置上安裝的所有 Kaspersky 應用程式。您可以點擊應用程式名稱以查看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。

啟用的政策和政策設定檔

啟用的政策和政策設定檔區段會列出受管理裝置上啟用的政策和政策設定檔。

工作

在**工作**區域，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。管理伺服器請求用戶端裝置的工作狀態詳情。如果未建立連線，則不顯示狀態。

事件

事件區域將顯示選定用戶端裝置在管理伺服器上所記錄事件的資訊。

標籤

在**標籤**區域，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。

可執行檔

可執行檔區域會顯示在用戶端裝置上發現的可執行檔。

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**

  點擊**匯出至檔案**按鈕儲存裝置與之互動的發佈點清單檔案。預設下，程式匯出裝置清單到 CSV 檔案。

- **內容**

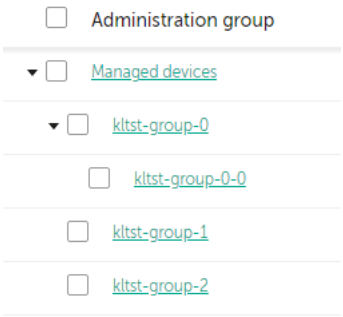
  點擊**內容**按鈕檢視和配置裝置與之互動的發佈點。

硬體登錄資料

在**硬體登錄資料**區域，您可以檢視安裝在用戶端裝置上的硬體資訊。

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新增到**受管理裝置**群組中，並新增嵌套群組（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. 前往**裝置 → 群組的階層**。
2. 在管理群組結構中，選取要加入新管理群組的管理群組。
3. 點擊**新增**按鈕。
4. 在開啟的**新管理群組名稱**視窗中，輸入群組名稱，然後點擊**新增**按鈕。

管理群組階層中將顯示帶有指定名稱的新管理群組。

要建立管理群組的架構：

1. 前往**裝置 → 群組的階層**。
2. 點擊**匯入**按鈕。

新管理群組架構精靈啟動。遵照精靈的說明。

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**裝置 → 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。

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，等等。

建立裝置移動規則

延伸所有 | 折疊所有

您可以設定裝置移動規則，即自動分配裝置到管理群組的規則。

要建立移動規則：

1. 在主功能表中，轉至**裝置 → 移動規則**頁簽。
2. 點擊**新增**。
3. 在開啟的視窗中，在**一般**頁籤指定以下資訊：

- **規則名稱**

  輸入新規則名稱。
  如果您正複製規則，新規則與來源規則名稱相同，但是索引格式（ ）被新增到名稱，例如：（1）。

- **管理群組**

選取要自動移動裝置的管理群組。

- **套用規則**

  您可以選取以下選項之一：
  - 對每台裝置執行一次。
    規則對比對標準的每台裝置套用一次。
  - 對每台裝置執行一次，然後在每次更新代理重新安裝時。
    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。
  - 規則被持續套用。
    規則根據管理伺服器自動設定的排程被套用（通常每幾個小時）。

- **僅移動不屬於任何管理群組的裝置**

  如果啟用該選項，僅未配置的裝置將被移動到所選群組。
  如果停用該選項，已經屬於其他管理群組的裝置以及未配置的裝置將被移動到所選群組。

- **啟用規則**

  如果啟用該選項，規則被啟用並在被儲存後開始工作。
  如果停用該選項，規則被建立，但不被啟用。直到您啟用該選項它才工作。

4. 在 **規則條件**頁簽上，指定至少一個標準，裝置將根據該標準被移至管理組。
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。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. 在主功能表中，轉至**裝置 → 移動規則**頁簽。
   您也可選取**發現和佈署 → 佈署和分配**，然後在功能表中選取**移動規則**。
   移動規則清單被顯示。
2. 選取您要複製的規則旁邊的核取方塊。
3. 點擊**複製**。
4. 在開啟的視窗中，變更在**一般**頁籤的以下資訊，若您緊要複製規則而不改變其設定，請不要進行任何變更：

- **規則名稱**

  輸入新規則名稱。
  如果您正複製規則，新規則與來源規則名稱相同，但是索引格式（）被新增到名稱，例如：（1）。

- **管理群組**

  選取要自動移動裝置的管理群組。

- **套用規則**

  您可以選取以下選項之一：
  - 對每台裝置執行一次。

規則對比對標準的每台裝置套用一次。

- 對每台裝置執行一次，然後在每次更新代理重新安裝時。
  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。
- 規則被持續套用。
  規則根據管理伺服器自動設定的排程被套用（通常每幾個小時）。

- **僅移動不屬於任何管理群組的裝置**

  如果啟用該選項，僅未配置的裝置將被移動到所選群組。
  如果停用該選項，已經屬於其他管理群組的裝置以及未配置的裝置將被移動到所選群組。

- **啟用規則**

  如果啟用該選項，規則被啟用並在被儲存後開始工作。
  如果停用該選項，規則被建立，但不被啟用。直到您啟用該選項它才工作。

5. 在**規則條件**標籤上，為要自動移動的裝置指定至少一個條件。
6. 點擊**儲存**。

新移動規則被建立。它顯示在移動規則清單。

裝置移動規則的條件

延伸所有 | 折疊所有

當您建立或者複製 將用戶端裝置移動到管理組的規則時，在**規則條件**頁簽上，設定移動裝置的條件。weile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。

標籤頁籤

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。

網路頁籤

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：

- **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。

- **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。

- **連線設定檔已變更**

  您可以選取以下值之一：
  - **是**.裝置移動規則僅套用於連線設定檔已變更的用戶端裝置。
  - **否**.裝置移動規則僅套用於連線設定檔未變更的用戶端裝置。
  - **未選取值**。該條件不適用。

- **由不同管理伺服器管理**

  您可以選取以下值之一：
  - **是**.裝置移動規則僅套用於由其他管理伺服器管理的用戶端裝置。這些伺服器與您配置裝置移動規則的伺服器不同。
  - **否**.裝置移動規則僅套用於由目前管理伺服器管理的用戶端裝置。
  - **未選取值**。該條件不適用。

應用程式頁籤

在此頁簽上，您可以根據用戶端裝置上安裝的受管應用程式和作業系統設定裝置移動規則：

- **網路代理已安裝**

  您可以選取以下值之一：
  - **是**.裝置移動規則僅適用於安裝了網路代理的用戶端裝置。
  - **否**.裝置移動規則僅適用於未安裝網路代理的用戶端裝置。
  - **未選取值**。該條件不適用。

- **應用程式**

  指定應在用戶端裝置上安裝哪些受管應用程式，以便裝置移動規則套用於這些裝置。例如，您可以選擇**卡巴斯基安全管理中心 14 網路代理**或者**卡巴斯基安全管理中心 14 管理伺服器**。
  如果您不選擇任何受管應用程式，則該條件不適用。

- **作業系統版本**

  您可以根據作業系統版本剔除用戶端裝置。為此，請指定應安裝在用戶端裝置上的作業系統。因此，裝置移動規則將套用到具有所選作業系統的用戶端裝置。
  如果您不啟用此選項，則條件不適用。依預設已停用該選項。

- **作業系統 bit 大小**

  您可以透過作業系統位元大小來剔除用戶端裝置。在**作業系統 bit 大小**欄位，您可以選擇以下一個值：
  - **未知**
  - **x86**
  - **AMD64**
  - **IA64**

  要檢查用戶端裝置的作業系統位元大小：

  1. 在主功能表中，轉至 **裝置** → **受管理裝置**區域。
  2. 點擊右側的**欄設定**按鈕（ ）。
  3. 選取**作業系統 bit 大小**選項並點擊**儲存**按鈕。
     之後，將顯示每個受管裝置的作業系統位元大小。

- **作業系統服務套件版本**

  在該欄位中，可以指定作業系統的更新套件版本（採用 *X.Y* 格式），這將決定將移動規則套用到裝置的方式。預設情況下，不指定版本值。

- **使用者憑證**

  您可以選取以下值之一：
  - **已安裝**.裝置移動規則僅套用到具有行動憑證的行動裝置。
  - **未安裝**.裝置移動規則僅套用到沒有行動憑證的行動裝置。
  - **未選取值**。該條件不適用。

- **作業系統版本**

  該設定僅套用到 Windows 作業系統。

  您可以指定所選作業系統是否必須具有相等、更早或更晚的版本號。您也可以設定對所有版本號的裝置移動規則，除了指定的版本號。

- **作業系統發佈號**

  該設定僅套用到 Windows 作業系統。

  您可以指定所選作業系統是否必須具有相等、更早或更晚的發行版本號。您也可以設定對所有發行版本號的裝置移動規則，除了指定的版本號。

虛擬機頁籤

在此頁籤上，您可以根據用戶端是否是虛擬機或虛擬桌面基礎架構 (VDI) 的一部分來設定裝置移動規則：

- **這是一台虛擬機**

  在該下拉清單中，您可以選取以下一個值：
  - **N/A**.該條件不適用。
  - **否**.移動不是虛擬機的裝置。
  - **是**.移動是虛擬機的裝置。

- **虛擬機類型**
- **虛擬桌面基礎架構的一部分**

  在該下拉清單中，您可以選取以下一個值：
  - **N/A**.該條件不適用。
  - **否**.移動不屬於 VDI 的裝置。
  - **是**.移動屬於 VDI 的裝置。

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. 前往**裝置 → 受管理裝置**。
2. 點擊 **目前路徑：**清單上方的<目前路徑>連接。
3. 在開啟的視窗中，選取您要向其新增裝置的管理群組。
4. 點擊**新增裝置**按鈕。
   行動裝置精靈啟動。
5. 列出您希望新增裝置的管理群組。

   您只可新增建立裝置時或裝置發現後已將資訊新增至管理伺服器資料庫的裝置。

   選取您希望將裝置新增至清單的方式：
   - 點擊**新增裝置**按鈕，接著以下列其中一種方式指定裝置：
     - 從管理伺服器偵測到的裝置清單中選取該裝置。
     - 指定裝置 IP 位址或 IP 範圍。
     - 指定裝置 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，以及以下禁用字元：, \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %
6. 檢視要新增至管理群組的裝置清單。您可新增或移除裝置來編輯清單。
7. 確認清單正確後，請點擊**下一步**按鈕。

精靈會處理裝置清單並顯示結果。系統會將已成功處理的裝置新增至管理群組，並顯示在管理伺服器產生的名稱下的裝置清單中。

將裝置手動移動至管理群組

您可將裝置從一個管理群組移至另一個，或從未配置的裝置群組移至另一個管理群組。

要把一台或多台裝置新增至一個選定的管理群組中，請執行以下操作：

1. 從您要移動裝置的位置開啟管理群組。要這麼做，請執行以下操作之一：
   - 若要開啟管理群組，請前往 **裝置 → 群組 → <群組名稱> → 受管理裝置**。
   - 若要開啟**未配置的裝置**群組，請前往**發現和佈署 → 未配置的裝置**。

2. 選取您要移至不同群組之裝置旁的核取方塊。
3. 點擊**移至群組**按鈕。
4. 在管理群組階層中，選取您要將選取的裝置移至管理群組旁的核取方塊。
5. 點擊**移動**按鈕。

選取的裝置會移至選取的管理群組。

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，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。

   新增工作精靈啟動。遵照精靈的說明。在新增工作精靈的**新工作**視窗中，選擇**卡巴斯基安全管理中心 14**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：

   - **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。您可以指定現有群組之一或者建立新群組。
     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。

   - **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分類中的裝置。您可以指定現有分類之一。
     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。

為其建立工作的用戶端裝置，在工作執行完畢後，將被工作設定中指定的管理伺服器管理。

當裝置顯示不活動時檢視和配置操作

如果組中的用戶端裝置不活動，您可以獲取關於它的通知。您也可以自動刪除此類裝置。

要在組中裝置顯示不活動時檢視或設定操作：

1. 在主功能表中，轉至 **裝置 → 群組的階層**。
2. 點擊所需管理群組的名稱。
   管理群組內容視窗將開啟。
3. 在內容視窗中，前往**設定**頁籤。
4. 在**繼承**區段，啟用或停用以下選項：

   - **從父群組繼承**

     該區域的設定將從包含用戶端裝置的父群組繼承。如果啟用此選項，**網路中的裝置活動**下的設定會禁止任何變更。
     該選項僅在管理群組擁有父群組時可用。
     預設情況下已啟用該選項。

- **在子群組中強制繼承設定**

  該設定值將被分發到子群組，但在子群組的內容中這些設定被鎖定。
  預設情況下已停用該選項。

5. 在**裝置活動**區段，啟用或停用以下選項：

- **若裝置未活動超過下列天數，則通知管理員**

  如果啟用該選項，管理員接收不活動裝置的通知。您可以指定**裝置在網路上已長時間沒有活動**事件被建立的時間間隔。預設時間間隔為 7 天。
  預設情況下已啟用該選項。

- **若裝置未活動超過下列天數，則從群組刪除裝置**

  如果啟用該選項，您可以指定從組中自動移除裝置的時間間隔。預設時間間隔為 60 天。
  預設情況下已啟用該選項。

6. 點擊**儲存**。

您的變更已儲存並套用。

關於裝置狀態

卡巴斯基安全管理中心 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。在有些情況下，指派狀態給裝置時，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）。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，病毒掃描工作，且發現的病毒數量超過指定值。	大於 0。
即時防護不符合管理員的設定等級	裝置在網路中可見，但即時防護等級與管理員在裝置狀態條件中設定的等級不同。	• 已停止。 • 已暫停。 • 執行中。
病毒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，但病毒掃描工作在指定時間內未執行。條件僅套用到於 7 天之前或更早新增到管理伺服器資料庫的裝置。	多於 1 天。
資料庫已過期	裝置在網路中可見且安全應用程式已安裝到裝置，但病毒資料庫在指定時間內未在該裝置上更新。條件僅套用到於 1 天之前或更早新增到管理伺服器資料庫的裝置。	多於 1 天。
長時間未連線	網路代理已安裝到裝置，但由於裝置關閉，裝置在指定時間段內未連線到管理伺服器。	多於 1 天。

偵測到活動威脅	**活動威脅**資料夾中的未處理的物件的數量超過指定的值。	多於 0 個項目。
需要重新啟動	裝置在網路中可見，但應用程式基於所選原因之一在指定時間之前請求裝置重新啟動。	多於 0 分鐘。
安裝了不相容的應用程式	裝置在網路中可見，但透過網路代理執行的軟體清查在裝置上偵測到了不相容的應用程式。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
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。
偵測到未處理的事件	裝置上發現了一些未處理的事故。事件可以透過安裝在用戶端裝置上的受管理 Kaspersky 應用程式自動建立，也可以由管理員手動建立。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
應用程式定義的裝置狀態	裝置狀態由受管理應用程式定義。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
裝置磁碟空間不足	裝置剩餘磁碟空間少於指定值或裝置無法與管理伺服器同步。當裝置已與管理伺服器成功同步且裝置上的剩餘空間大於或等於指定值時，*緊急*或*警告*狀態被變更為*正常*狀態。	大於 0 MB
裝置已失去管理	在裝置發現過程中，裝置在網路中可見，但是超過三次嘗試與管理伺服器同步都失敗了。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
防護已停用	裝置在網路中可見，但裝置上的安全應用程式已被停用大於指定的時間段。	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。當指定條件滿足時，用戶端裝置被分配以下狀態之一：*緊急* 或 *警告*。未滿足特定條件時，系統會為用戶端裝置指派*正常*狀態。

一個條件的不同值可對應於不同的狀態。例如，依預設，若**資料庫已過期**條件有**多於 3 天**的值，則用戶端裝置會被指派*警告*狀態，逾值為**多於 7 天**，則會指派*緊急*狀態。

如果您從以前的版本升級卡巴斯基安全管理中心 Linux，指定*緊急*或*警告*狀態的 **資料庫已過期** 條件的值不會改變。

當卡巴斯基安全管理中心 Linux 指派狀態給裝置時，對於有些條件（請參閱條件說明欄），系統會將能見度標記列入考量。例如，若受管理裝置因符合資料庫已過期條件而被指派*緊急*狀態，之後能見度標記也已針對該裝置設定，則裝置會被指派*正常*狀態。

設定裝置狀態轉換

您可變更條件以為裝置配置*緊急*或*警告*狀態。

要啟用變更裝置狀態到緊急：

1. 使用下列方式之一開啟內容視窗：
   - 在**政策**資料夾，在管理伺服器政策的上下文功能表中，選取**內容**。
   - 在管理群組的右鍵選單中選取**內容**。
2. 在開啟的內容視窗中，在**區域**視窗選取**裝置狀態**。
3. 在工作區，在**若指定以下條件，則設為"緊急"** 區域，從清單中選取條件核取方塊。

   然而，您可以變更在父政策中未鎖定的設定。

4. 為所選條件設定所需的值。
   您可針對部分（非全部）條件設定值。
5. 點擊**確定**。

未滿足特定條件時，系統會為受管理裝置配置*緊急*狀態。

要啟用變更裝置狀態到警告：

1. 使用下列方式之一開啟內容視窗：
   - 在**政策**資料夾，在管理伺服器政策的上下文功能表中，選取**內容**。
   - 在管理群組的右鍵選單中選取**內容**。
2. 在開啟的內容視窗中，在**區域**視窗選取**裝置狀態**。
3. 在工作區，在**若指定以下條件，則設為"警告"**區域，從清單中選取條件核取方塊。

   然而，您可以變更在父政策中未鎖定的設定。

4. 為所選條件設定所需的值。
   您可針對部分（非全部）條件設定值。
5. 點擊**確定**。

未滿足特定條件時，系統會為受管理裝置配置*警告*狀態。

政策和政策設定檔

在卡巴斯基安全管理中心 14 網頁主控台，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，當不同場合僅假設更改多個設定時，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
Undefined	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：

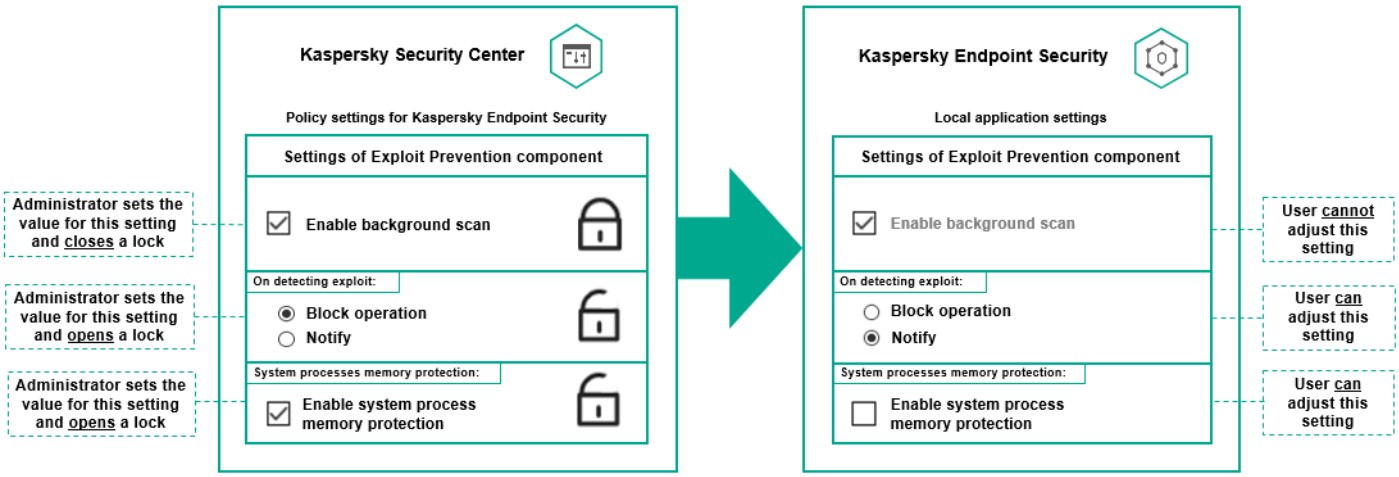
- 鎖定管理子群組政策的設定
- 在受管理裝置上鎖定卡巴斯基應用程式的設定

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。

政策和本機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

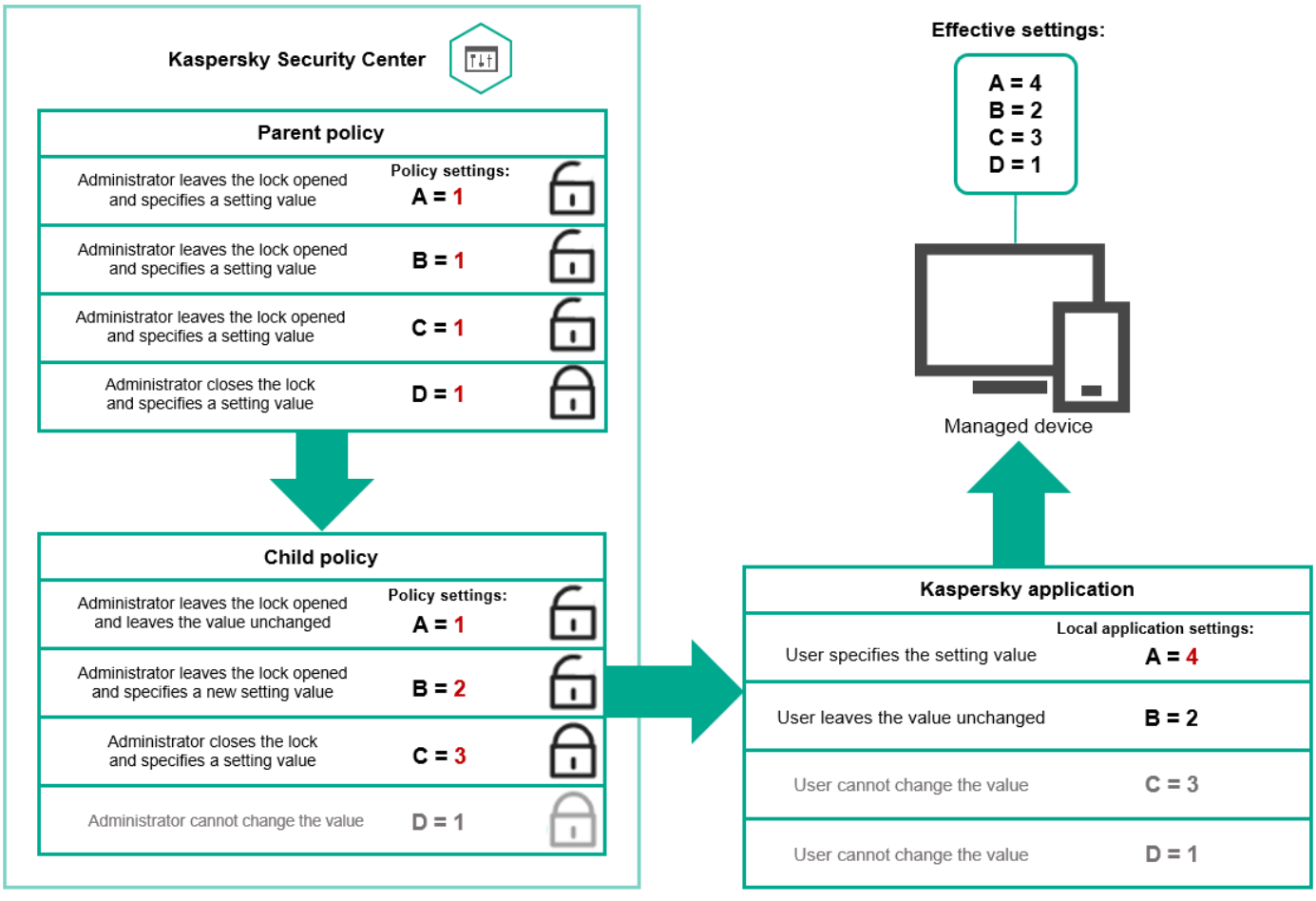
如果不同的裝置需要不同的設定，則可以將裝置組織到管理群組中。

您可以為單一管理群組指定政策。您可以*繼承政策設定*。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組。如果要建立自訂組，它們將作為受管理裝置組內的子群組（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）。

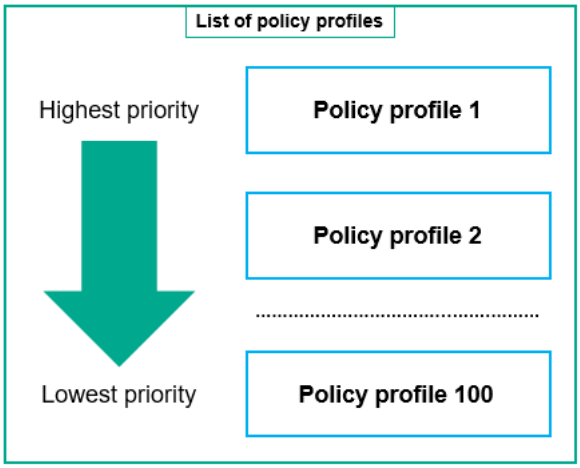


政策層級

政策層次結構中的政策設定檔

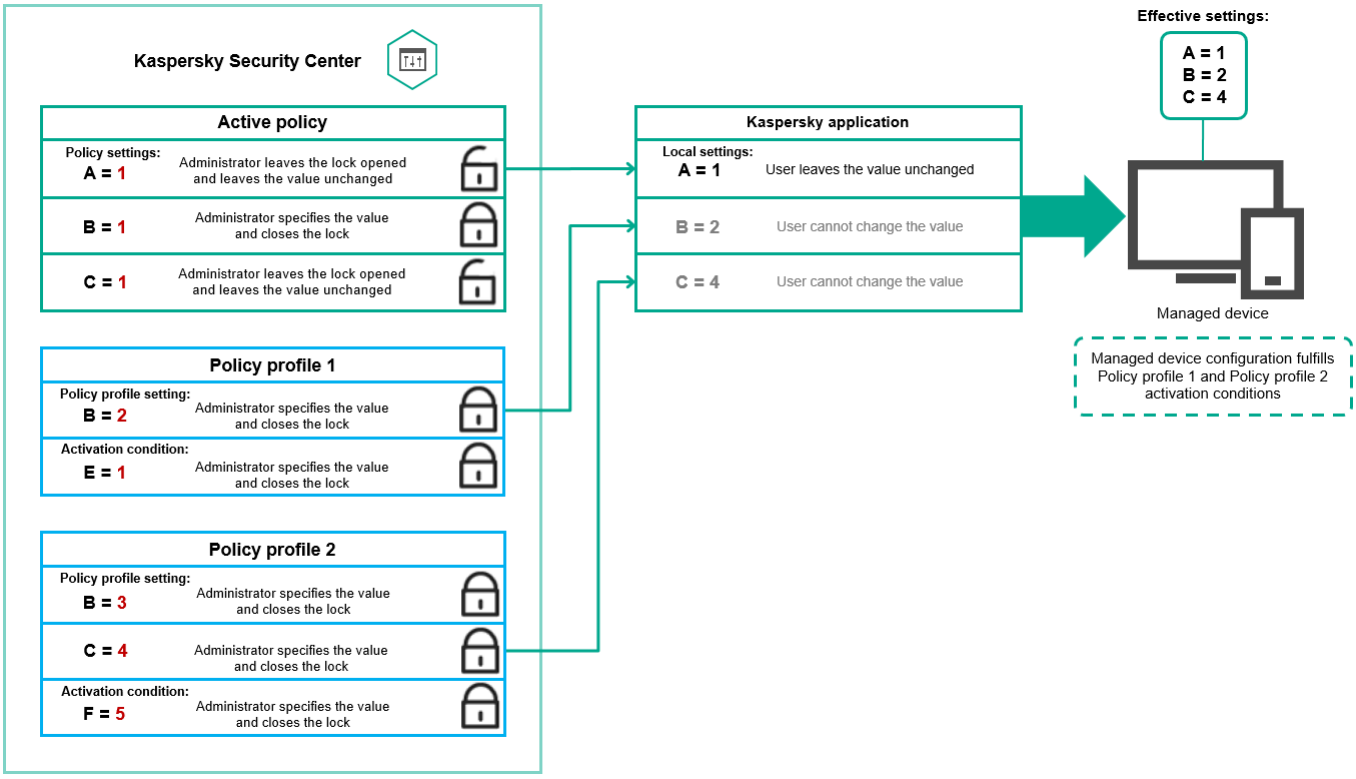
政策設定檔具有以下優先等級分配條件：

- 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）。

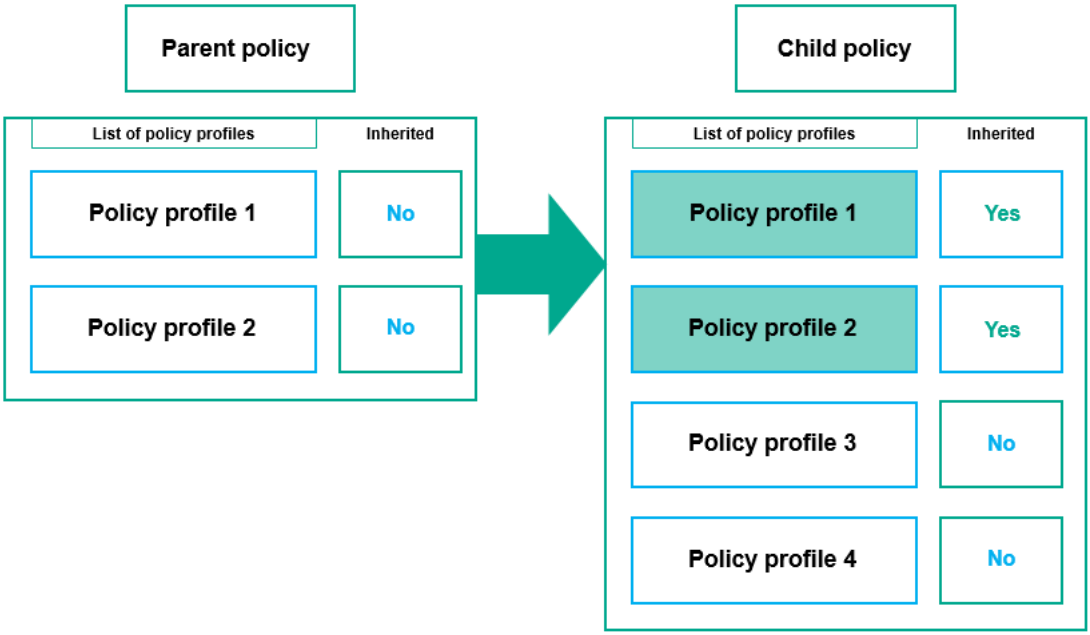


受管理裝置配置滿足幾個政策設定檔的啟動條件

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）。

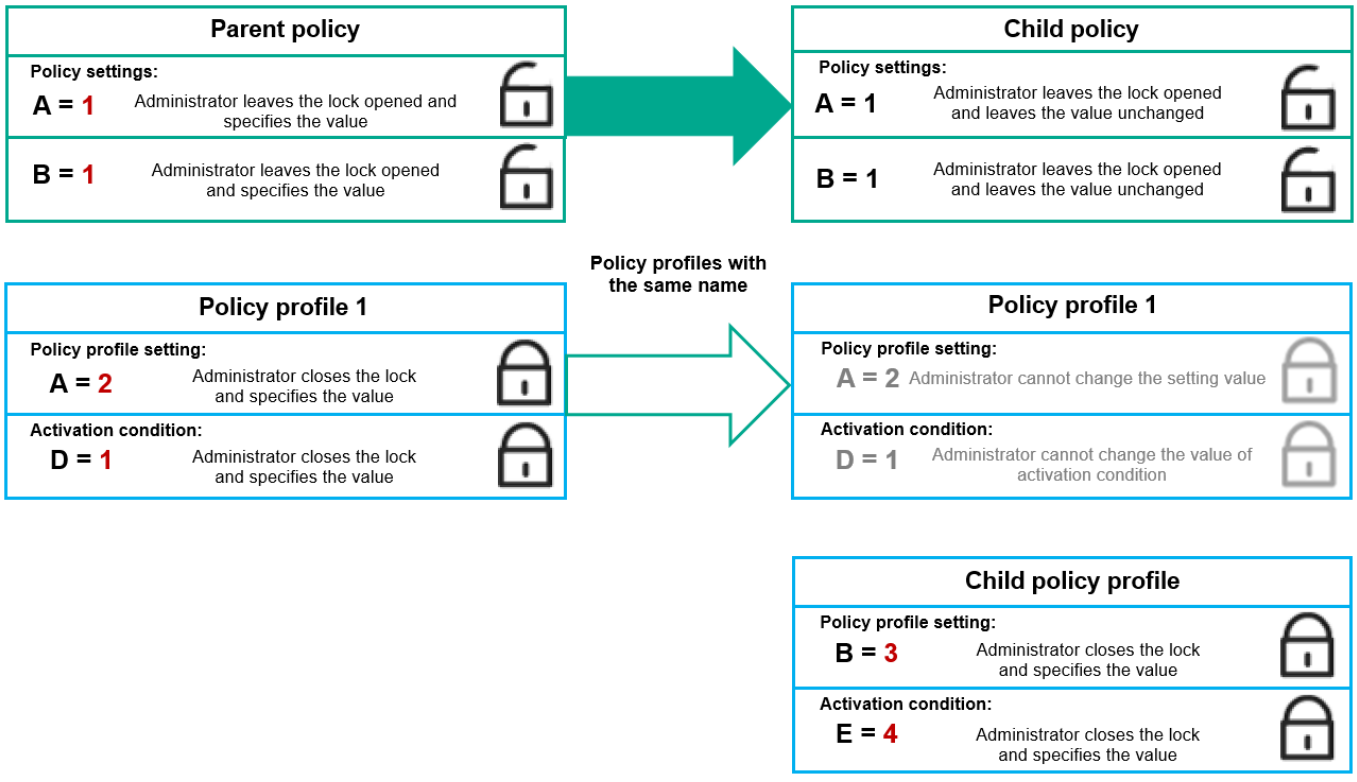


政策設定檔繼承

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更改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更改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、查看政策分發狀態圖，以及刪除政策的資訊。

檢視政策清單

您可以檢視為管理伺服器或任何管理群組建立的政策清單。

要檢視政策清單，請執行以下操作：

1. 在主功能表中，轉至 **裝置 → 群組的階層**。
2. 在管理群組結構中，選擇您要檢視其政策清單的管理群組。

政策清單以表格格式出現。如果沒有政策，表格為空。您可以顯示或隱藏表格的列，變更它們的順序，僅檢視包含指定值的行，或者使用尋找。

建立政策

您可以建立政策；您也可以修改和刪除現有政策。

要建立政策：

1. 前往**裝置 → 政策和設定檔**。
2. 點擊**新增**。
   選取應用程式視窗隨即開啟。
3. 選取您要建立政策的應用程式。
4. 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。
5. 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。
6. 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。
7. 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

   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。
8. 點擊**儲存**儲存政策。

該政策將顯示在政策清單中。

一般政策設定

延伸所有 | 折疊所有

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，您可以選取政策的模式：
  - **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階層管理群組的政策，也就是孩子政策。
    - 在每個子政策內容視窗的**一般**區域的**設定繼承**區塊，系統將自動選取**從父政策繼承設定**核取方塊。

    如果啟用此方塊，則會鎖定子政策設定。
    預設情況下已停用該選項。

事件配置

事件配置區域可讓您配置事件記錄和事件通知。事件根據嚴重等級用下面的標籤分佈：

- **緊急**
  緊急頁籤不會顯示在網路代理政策內容中。
- **功能失效**
- **警告**
- **資訊**

在每個區域，清單顯示在管理伺服器上事件類型和預設事件儲存的期限（天）。點擊事件類型允許您指定以下設定：

- **事件註冊**
  您可以指定儲存事件的天數和選取儲存事件的位置：
  - **使用 Syslog 匯出到 SIEM 系統**
  - **儲存在裝置的作業系統事件記錄中**
  - **儲存在管理伺服器的作業系統事件記錄中**
- **事件通知**
  您可以選取您是否想由以下方法之一被通知事件：
  - **透過郵件通知**
  - **透過簡訊通知**
  - **透過執行可執行檔或指令碼通知**
  - **透過 SNMP 通知**

  預設下，使用在管理伺服器內容標籤中指定的通知設定（例如收件者位址）。如有需要，您可在**電子郵件**、**SMS**與**要執行的可執行檔**頁籤變更這些設定。

變更歷程

變更歷程頁籤可讓您檢視政策修訂的清單，並復原對政策進行的變更（如有必要）。

修改政策

要修改政策：

1. 前往**裝置 → 政策和設定檔**。
2. 點擊您要修改的政策。
   政策設定視窗隨即開啟。
3. 指定通用設定和為其建立政策的應用程式的設定。如需詳細資訊，請參閱以下內容：
   - 管理伺服器配置
   - 網路代理政策設定
   - Kaspersky Endpoint Security for Linux 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**。

對政策所做的變更將儲存在政策內容中，並且會顯示在**變更歷程**區段。

啟用和停用政策繼承選項

若要啟用或停用政策中的繼承選項：

1. 開啟所需的政策。
2. 開啟**一般**頁籤。
3. 啟用或停用政策繼承：
   - 如果您對子群組啟用**從父政策繼承設定**，並在父政策中鎖定一些設定，那麼您無法在子政策中變更這些設定。
   - 如果您對子政策停用**從父政策繼承設定**，那麼您可以變更子政策中的所有設定，即便一些設定在父政策中是鎖定的。
   - 如果您在父群組啟用**在子政策中強制繼承設定**，這將為每個子政策啟用**從父政策繼承設定**。此種情況下，您無法為任何子政策停用該選項。所有在父政策中被鎖定的設定被強制繼承到子群組，且您無法在子群組中變更這些設定。
4. 點擊**儲存** 按鈕儲存更改，或點擊**取消** 按鈕拒絕更改。

依預設，政策會啟用**從父政策繼承設定**選項。

如果政策有設定檔，所有子政策都會繼承這些設定檔。

複製政策

您可以從一個管理群組複製政策到另一個。

要複製政策到其他管理群組：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。
2. 選取您要複製的政策旁邊的核取方塊。
3. 點擊**複製**按鈕。
   在螢幕的右側，管理群組樹狀目錄被顯示。
4. 在樹狀目錄中，選取目的群組，意即您要複製政策到該群組。
5. 點擊畫面底部的**複製**按鈕。
6. 點擊**確定**以確認操作。

政策將連帶其所有設定檔被複製到目的群組。目標群組中各個複製的政策將會**非作用中**。您可隨時變更狀態至**作用中**。

如果目的群組中已包含名稱與新移動政策的名稱一致的政策，那麼會在新移動政策的名稱後附加一個（<下一個序號>）的索引，例如：（1）。

移動政策

您可以從一個管理群組移動政策到另一個。例如，您要刪除一個群組，但您要為其他群組使用其政策。在此情況下，您可能要先將政策從舊群組移動至新群組，再刪除舊群組。

要移動政策到其他管理群組：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。
2. 選取您要移動的政策旁邊的核取方塊。
3. 點擊**移動**按鈕。
   在螢幕的右側，管理群組樹狀目錄被顯示。
4. 在樹狀目錄中，選取目的群組，例如，您要將政策移動到該群組。
5. 點擊畫面底部的**移動**按鈕。
6. 點擊**確定**以確認操作。

如果政策不是從資源群組繼承的，它連帶所有設定檔被移動到目的群組。目標群組中的政策狀態是**非作用中**。您可隨時變更狀態至**作用中**。

如果政策繼承自資源群組，它將保持在資源群組中。它連帶所有其設定檔被複製到目的群組。目標群組中的政策狀態是**非作用中**。您可隨時變更狀態至**作用中**。

如果目的群組中已包含名稱與新移動政策的名稱一致的政策，那麼會在新移動政策的名稱後附加一個（<下一個序號>）的索引，例如：（1）。

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. 前往**裝置 → 受管理裝置**。
2. 點擊要與管理伺服器同步的裝置名稱。
   政策內容視窗會開啟，並含有所選的**一般**區段。
3. 點擊**強制同步**按鈕。

應用程式將所選裝置與管理伺服器同步。

同步多部裝置

強制同步管理伺服器和受管理裝置：

1. 開啟管理群組的裝置清單或裝置分類：
   - 前往**裝置 → 受管理裝置 → 群組**，接著選取包含要同步裝置的管理群組。
   - 執行裝置分類以檢視裝置清單。
2. 選取您要與管理伺服器同步之裝置旁的核取方塊。
3. 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，查看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. 前往**裝置 → 受管理裝置**。
2. 點擊要與管理伺服器同步的裝置名稱。
   政策內容視窗會開啟，並含有所選的**一般**區段。
3. 點擊**應用程式**頁籤。
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. 前往**裝置→政策和設定檔** 。
2. 選取要在裝置上檢視分配狀態之政策名稱旁的核取方塊。
3. 在出現的選單中，選取**分發**連結。
   <政策名稱>分發結果視窗隨即開啟。
4. 在開啟的**<政策名稱>分發結果**視窗中，顯示政策的**狀態描述**。

您可以使用政策分發更改清單中顯示的裝置數量。裝置最高數量是 100000。

若要使用政策發佈結果更改清單中顯示的裝置數量：

1. 前往工具列中的**介面選項**區段。
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 100000）。
   預設情況下，數量為 5000。
3. 點擊**儲存**。
   設定已儲存並套用。

刪除政策

如果您不再需要一個政策，您可以刪除它。您僅可以刪除一個在指定管理群組中繼承的政策。如果一個政策是繼承的，您僅可以在其被建立的上級群組刪除它。

要刪除政策，請執行以下操作：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。
2. 選取您要刪除之政策旁的核取方塊並點擊**刪除**。
   若您選取繼承的政策，則**刪除**按鈕會變成無法使用（暗顯）。
3. 點擊**確定**以確認操作。

政策連帶其所有設定檔被刪除。

管理政策設定檔

本節說明管理政策設定檔，並提供查看政策設定檔、變更政策設定檔優先等級、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，以及刪除政策設定檔的資訊。

檢視政策設定檔

要檢視政策設定檔：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。

2. 點擊您要檢視其設定檔的政策名稱。
   政策內容視窗會開啟，並含有所選的**一般**頁籤。
3. 開啟**政策設定檔**頁籤。

政策設定檔清單以表格格式出現。如果政策沒有設定檔，將出現空表。

變更政策設定檔優先順序

要變更政策設定檔優先順序：

1. 轉到您要的政策的設定檔清單。
   將出現政策設定檔清單。
2. 在**政策設定檔**頁籤，選取您要變更優先權之政策設定檔旁的核取方塊。
3. 透過點擊**提高優先順序**或**降低優先順序**，在清單中設定政策設定檔的新位置。
   政策設定檔在清單中的位置越高，其優先順序越高。
4. 點擊**儲存**按鈕。

所選政策設定檔的優先順序被變更並套用。

建立政策設定檔

要建立政策設定檔：

1. 轉到您要的政策設定檔清單。
   將出現政策設定檔清單。如果政策沒有設定檔，將顯示空表。
2. 點擊**新增**。
3. 如果您需要，變更設定檔的預設名稱和預設繼承設定。
4. 選取 **應用程式設定**頁籤。
   或者，您可點擊**儲存**並結束。您建立的設定檔將出現在政策設定檔清單，且您可以稍後編輯其設定。
5. 在**應用程式設定**頁籤的左窗格與右邊的結果窗格中選取您要的類別，接著編輯設定檔的設定。您可以在每個類別中（區域）編輯政策設定檔設定。
   編輯設定時，您可點擊**取消**來取消最後的操作。
6. 點擊**儲存**以儲存設定檔。

該設定檔顯示在政策設定檔清單中。

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

延伸所有 | 折疊所有

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**頁籤，點擊**新增**按鈕。
   政策設定檔啟動規則視窗開啟。
4. 指定規則的名稱。
5. 選取影響您目前建立的政策設定檔的啟動的條件的核取方塊：

- **政策設定檔啟動一般規則**

  選取該核取方塊依據裝置行動模式狀態設定裝置上的政策設定檔啟動規則、連線管理伺服器規則和分配給裝置的標記。

  對於該選項，指定在下一步：

  - **裝置狀態**

    定義裝置出現在網路的條件：
    - **線上**—裝置位在網路中，因此可使用管理伺服器。
    - **離線**—裝置位在網路外，因此無法使用管理伺服器。
    - **N/A**—將不套用標準。

  - **本裝置上已啟動管理伺服器連線規則**

    選取政策設定檔啟動條件（規則是否被執行）並選取規則名稱。
    規則定義裝置網路位置以便連線到管理伺服器，它的條件必須被滿足（或不滿足）以便啟動政策設定檔。
    用於連線到管理伺服器的裝置網路位置敘述可以在網路代理轉換規則中被建立或設定。

- **特別裝置所有者規則**
  對於該選項，指定在下一步：

  - **裝置所有者**

    啟用此選項依據裝置所有者在其上設定和啟用設定檔啟動規則。在此方塊下的下拉清單，你可以選取設定檔啟動標準：
    - 裝置屬於指定的擁有者（"="符號）。
    - 裝置不屬於指定的擁有者（"#"符號）。
      如果啟用該選項，設定檔根據配置的標準在裝置上啟動。啟用此選項時，您可以指定裝置所有者。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

  - **裝置所有者在內部安全群組中**

    啟用此選項以卡巴斯基安全管理中心 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。

- **硬體說明書規則**

  選取該核取方塊依據記憶體和邏輯處理器數量設定裝置上的政策設定檔啟動規則。

  對於該選項，指定在下一步：

  - **記憶體大小 (MB)**

    啟用此選項透過裝置上可用 RAM 容量在裝置上設定和啟用設定檔啟動規則。在此方塊下的下拉清單，你可以選取設定檔啟動標準：

    - 該裝置記憶體大小小於指定值（"<" 符號）。
    - 該裝置記憶體大小大於指定值（">" 符號）。

    如果啟用該選項，設定檔根據配置的標準在裝置上啟動。您可以指定裝置上的 RAM 容量。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

  - **邏輯處理器數量**

    啟用此選項透過裝置上邏輯處理器數量在裝置上設定和啟用設定檔啟動規則。在此方塊下的下拉清單，你可以選取設定檔啟動標準：

    - 裝置上邏輯處理器數量少於或等於指定值（"<" 符號）。
    - 裝置上邏輯處理器數量大於或等於指定值（">" 符號）。

    如果啟用該選項，設定檔根據配置的標準在裝置上啟動。您可以指定裝置上的邏輯處理器數量。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

- **角色分配規則**

  對於該選項，指定在下一步：

  - **由裝置所有者特定角色啟動政策設定檔**

    選取該選項以在裝置上根據所有者角色配置和啟用設定檔啟動規則。 從現有角色清單手動新增角色。

    如果啟用該選項，設定檔根據配置的標準在裝置上啟動。

- **標籤使用規則**

  選取該核取方塊根據分配到裝置的標籤設定裝置上的政策設定檔啟動規則。您可以在有選取標籤或沒有選取標籤的裝置啟動政策設定檔。

  對於該選項，指定在下一步：

  - **標籤清單**

    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。

精靈的附加頁面數量取決於您在第一步選取的設定。您可以稍後修改政策設定檔啟動規則。

6. 檢查所配置參數的清單。若清單正確，請點擊**建立**。

設定檔將被儲存。當觸發啟動規則時，將在裝置上啟動該設定檔。

針對顯示在**啟動規則**頁籤中政策設定檔內容的設定檔，所建立的政策設定檔啟動規則。您可以修改或刪除任何政策設定檔啟動規則。

多個啟動規則可以被一起觸發。

刪除政策設定檔

要刪除政策設定檔：

1. 轉到您要的政策的設定檔清單。
   將出現政策設定檔清單。
2. 在**政策設定檔**頁籤上，選取要刪除之政策設定檔旁的核取方塊，接著點擊**刪除**。
3. 在開啟的視窗中，再次點擊**刪除**按鈕。

政策設定檔被刪除。如果政策從低級別群組繼承，設定檔保持在該群組，但變成該群組的政策設定檔。這可以消除低級別群組裝置上安裝的受管理應用程式的設定的顯著修改。

使用者和使用者角色

該部分描述了使用者和使用者角色，並提供建立和修改它們、分配角色和群組到使用者以及關聯政策設定檔到角色的說明。

關於用於角色

使用者角色（也叫*角色*）是包含一組權限集的物件。角色可以與安裝在使用者裝置上的 Kaspersky 應用程式設定關聯。您可以分配角色到使用者集，或者到管理伺服器階層的任何等級的安全群組集。

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、**修改**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	**修改**	• 將裝置新增到管理群組：**修改** • 從管理群組中刪除裝置：**修改** • 將管理群組新增到另一個管理群組：**修改** • 從另一個管理群組中刪除管理群組：**修改**	沒有	沒有	沒有
一般功能：存取物件而不考慮它們的 ACLs	**讀取**	獲得對所有物件的存取權限：**讀取**	沒有	沒有	沒有
一般功能：基本功能	• **讀取** • **修改** • **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）：**修改**、**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：**修改** • 檢視群組的存取控制清單：**讀取** • 查看卡巴斯基事件記錄：**讀取**	• 「將更新下載至管理伺服器儲存區」 • 「提交報告」 • 「分發安裝套件」 • 「在次要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」 • 「已安裝的外圍防禦應用程式的摘要報告」 • 「已安裝的應用程式類型概要報告」 • 「受感染的裝置使用者報告」 • 「事件報告」 • 「事件報告」 • 「發佈點活動報告」 • 「從屬管理伺服器的報告」 • 「裝置控制事件報告」 • 「禁止的應用程式報告」 • 「Web 控制報告」 • 「有效使用者權限報告」 • 「權限報告」	沒有

一般功能：刪除物件	• **讀取** • **修改**	• 查看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：**修改**	沒有	沒有	沒有
一般功能：事件處理	• **刪除事件** • **編輯事件通知設定** • **編輯事件記錄設定** • **修改**	• 變更事件註冊設定：**編輯事件記錄設定** • 變更事件通知設定：**編輯事件通知設定** • 刪除事件：**刪除事件**	沒有	沒有	設定： • 儲存在資料庫中的最大事件數量 • 儲存已刪除裝置中的事件時段
一般功能：管理伺服器上的操作	• **讀取** • **修改** • **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：**修改** • 指定在管理管理伺服器上啟動的啟動代理連接埠：**修改** • 指定在管理伺服器上啟動的行動啟動代理連接埠：**修改** • 指定用於發佈獨立套件之網頁伺服器的連接埠：**修改** • 指定用於發佈 MDM 設定檔的網頁伺服器的連接埠：**修改** • 指定管理伺服器的 SSL 連接埠以透過網頁主控台進行連線：**修改** • 指定用於行動連線之管理伺服器的管理連接埠：**修改** • 指定儲存在管理管理伺服器資料庫的事件最大數量：**修改** • 指定管理伺服器可以傳送的最大事件數：**修改** • 指定管理伺服器可以傳送事件的時段：**修改**	• 「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** • **修改** • **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** • **修改**	• 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：**修改**	沒有	沒有	沒有

一般功能：**強制報告管理**	• **讀取** • **修改**	• 建立報告，而不考慮其 ACL：**寫入** • 不論報告的 ACL 為何都加以執行：**讀取**	沒有	沒有	沒有
一般功能：**管理伺服器階層**	**配置管理伺服器的階層**	• 註冊、更新或刪除輔助管理伺服器：**配置管理伺服器的階層**	沒有	沒有	沒有
一般功能：**使用者權限**	**修改物件 ACL**	• 變更任何物件的安全屬性：**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** • **修改** • **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

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。

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。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	允許對所有類型報告的所有操作、所有檢視操作，包含檢視已刪除的物件（在**已刪除的物件**區域授予**讀取**與**修改**權限）。不允許其他操作。您可以分配該角色到執行您組織的稽核的人。
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；在以下區域授予有限的權限：**系統管理**：**連線**區域。您可以分配該角色到負責您組織的 IT 安全的安全官。

下表顯示分配給每個預定義使用者角色的存取權限。

功能區的功能**行動裝置管理：一般**和**系統管理**在卡巴斯基安全管理中心 Linux 中不可用。具有**弱點和修補程式管理管理員/操作員**和**行動裝置管理管理員/操作員**角色的使用者只能存取來自**一般功能**的權限：**基本**功能區域。

預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，在**一般功能**： • **基本功能** • **事件處理** • **管理伺服器階層**

	• **虛擬管理伺服器**
管理伺服器憑證運算子	授予以下所有功能區域的**讀取**和**執行**權限，位於**一般功能**中： • **基本功能** • **虛擬管理伺服器**
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，在**一般功能**： • **基本功能** • **Kaspersky 軟體部署** • **產品授權金鑰管理** 授予**讀取**和**執行**權利，位於**一般功能：虛擬管理伺服器**功能區域。
安裝運算子	授予以下所有功能區域的**讀取**和**執行**權限，位於**一般功能**中： • **基本功能** • **Kaspersky 軟體部署**（也會在此區域授予**管理 Kaspersky Lab 修補程式**權限） • **虛擬管理伺服器**
Kaspersky Endpoint Security 管理員	允許在以下功能區域中進行所有操作： • **一般功能：基本功能** • Kaspersky Endpoint Security 區域，包括所有功能
Kaspersky Endpoint Security 運算子	授予以下所有功能區域的**讀取**和**執行**權限： • **一般功能：基本功能** • Kaspersky Endpoint Security 區域，包括所有功能
主要管理員	允許功能區域內的所有操作，以下區域*除外*，在**一般功能**： • **存取物件而不考慮它們的 ACLs** • **強制報告管理**
主要運算子	授予以下所有功能區域的**讀取**和**執行**（如適用）權限： • **一般功能**： • **基本功能** • **刪除物件** • **管理伺服器上的操作** • **Kaspersky Lab 軟體佈署** • **虛擬管理伺服器** • Kaspersky Endpoint Security 區域，包括所有功能
行動裝置管理管理員	允許**一般功能中的所有操作：基本功能**的功能區域。
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** 授予**讀取**、**修改**、**執行**、**將來自裝置的檔案儲存到管理員的工作站**，以及**對裝置分類執行操作**的權限，位於**系統管理：連線**功能區域。 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	允許以下區域的所有操作：**移動裝置管理：自助服務入口網站**功能區域。此功能僅適用於卡巴斯基安全管理中心 11 或更新版本。
管理者	授予 **讀取**權限，位於**一般功能**：**存取物件而不管它們的 ACL** 和 **一般功能**：**強制報告管理**功能區域。 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。

新增內部使用者帳戶

要新增新內部使用者帳戶到卡巴斯基安全管理中心 Linux：

1. 在主功能表中，轉至 **使用者和角色 → 使用者**。
2. 點擊**新增**。
3. 在開啟的**新實體**視窗，指定新使用者帳戶設定：
   - 保留預設選項 **使用者**。
   - **名稱**.
   - 連線到卡巴斯基安全管理中心 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 16 位字元長度。
     - 密碼必須包含以下組中三組的字元：
       - 大寫字母 (A-Z)
       - 小寫字母 (a-z)
       - 數字 (0-9)
       - 特殊字元 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - 密碼不可以包含任何空白、Unicode 字元或 ":" 和「@」的組合，並且「@」前不可有「.」。

     若要查看您輸入的字元，請按住**顯示**按鈕。

     > 輸入密碼的嘗試次數有限。預設下，允許的最大密碼輸入嘗試次數是 10。您可以管理允許的密碼輸入嘗試次數，敘述在"變更允許的密碼輸入嘗試次數"。

     > 如果使用者輸入無效的密碼指定次數，使用者被鎖定一小時。您僅可以透過變更密碼解鎖封鎖使用者。
   - **完整名稱**
   - **敘述**
   - **郵件信箱**
   - **電話**
4. 點擊**確定**儲存變更。

新使用者帳戶出現在使用者和使用者群組清單。

建立使用者群組

要建立使用者群組：

1. 在主功能表中，轉至 **使用者和角色 → 使用者**。
2. 點擊**新增**。
3. 在開啟的**新實體**視窗中，選取**群組**。
4. 為新使用者群組指定以下設定：
   - **群組名稱**
   - **敘述**
5. 點擊**確定**儲存變更。

新使用者群組出現在使用者和使用者群組清單。

編輯內部使用者帳戶

要在卡巴斯基安全管理中心 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**。
2. 點擊您要編輯的使用者帳戶名稱。
3. 在開啟的使用者設定視窗中的**一般**頁籤，變更使用者帳戶設定：
   - **敘述**
   - **完整名稱**
   - **郵件信箱**
   - **主電話**
   - 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 16 位字元長度。
     - 密碼必須包含以下組中三組的字元：
       - 大寫字母 (A-Z)
       - 小寫字母 (a-z)
       - 數字 (0-9)
       - 特殊字元 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - 密碼不可以包含任何空白、Unicode 字元或 "." 和「@」的組合，並且「@」前不可有「.」。

     要檢視輸入的密碼，點擊並按住**顯示**按鈕。

     > 輸入密碼的嘗試次數有限。預設下，允許的最大密碼輸入嘗試次數是 10。您可以變更允許的嘗試次數；但是，出於安全原因，我們不建議您減少此數字。如果使用者輸入無效的密碼指定次數，使用者被鎖定一小時。您僅可以透過變更密碼解鎖封鎖使用者。
   - 如有必要，請切換開關按鈕至**已停用**，以禁止使用者連線到應用程式。您可以停用帳戶，例如，在員工離職後。
4. 在**驗證安全性**頁籤中，您可以指定此帳戶的安全設定。
5. 在**群組**頁籤，您可新增使用者至安全群組。
6. 在**裝置**頁籤，您可指派裝置給使用者。
7. 在**角色**頁籤，您可指派角色給使用者。
8. 點擊**儲存**儲存變更。

更新的使用者帳戶出現在使用者和安全群組清單。

編輯使用者群組

您僅可以編輯內部群組。

要編輯使用者群組:

1. 在主功能表中，轉至 **使用者和角色 → 使用者**。
2. 點擊您要編輯的使用者群組名稱。
3. 在開啟的群組設定視窗中，變更使用者群組設定：
   - **名稱**
   - **敘述**
4. 點擊**儲存**儲存變更。

更新的使用者群組出現在使用者和使用者群組清單。

新增使用者帳戶到內部群組

您僅可以新增內部使用者帳戶到內部群組。

要新增使用者帳戶到內部群組：

1. 在主功能表中，轉至 **使用者和角色 → 使用者**。
2. 選取您要新增到群組的使用者帳戶旁邊的核取方塊。
3. 點擊**分配群組**按鈕。
4. 在開啟的**分配群組**視窗中，選取您要新增使用者帳戶的群組。
5. 點擊**分配**按鈕。

使用者帳戶被新增到群組。

指派使用者作為裝置所有者

有關指派使用者為行動裝置擁有者的資訊，請參閱Kaspersky Security for Mobile 說明。

要指派使用者作為裝置所有者：

1. 在主功能表中，轉至 **使用者和角色 → 使用者**。
2. 點擊您要分配為裝置所有者的使用者帳戶名稱。
3. 在開啟的使用者設定視窗中，選取**裝置**頁籤。
4. 點擊**新增**。
5. 從裝置清單中，選取您要分配給使用者的裝置。
6. 點擊**確定**。

所選的裝置被新增到分配給使用者的裝置清單。

您可在**裝置 → 受管理裝置**執行相同操作，方法是點擊您要指派之裝置的名稱，之後點擊**管理裝置所有者**連結。

刪除使用者或安全群組

您僅可以刪除內部使用者或內部安全群組。

要刪除使用者或安全群組：

1. 在主功能表中，轉至 **使用者和角色 → 使用者**。
2. 選取您要刪除的使用者或安全群組旁邊的核取方塊。
3. 點擊**刪除**。
4. 在開啟的視窗中，點擊**確定**按鈕。

使用者或安全群組被刪除。

建立使用者角色

要建立使用者角色：

1. 在主功能表中，轉至 **使用者和角色 → 角色**。
2. 點擊**新增**。
3. 在開啟的**新角色名稱**視窗中，輸入新角色的名稱。
4. 點擊**確定**以套用變更。
5. 在開啟的角色內容視窗中，變更角色設定：
   - 在**一般**頁籤，編輯角色名稱。
     您無法編輯預定義角色名稱。
   - 在**設定**頁籤，編輯角色範圍和政策以及與角色相關的設定檔。
   - 在**存取權限**頁籤，編輯存取 Kaspersky 應用程式的權限。
6. 點擊**儲存**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**儲存變更。

更新的角色出現在使用者角色清單。

編輯使用者角色範圍

*使用者角色範圍*是使用者和管理群組的組合。與使用者角色關聯的設定僅套用到屬於該角色使用者的裝置，以及僅在這些裝置屬於與該角色關聯的群組（包括子群組）時。

要新增使用者、安全群組和管理群組到使用者角色範圍，您可以使用以下其中一種方法：

方法 1：

1. 在主功能表中，轉至 **使用者和角色** → **使用者**。
2. 選取您要新增到使用者角色範圍的使用者和安全群組旁邊的核取方塊。
3. 點擊**分配角色**按鈕。
   角色分配精靈啟動。使用**下一步**按鈕進行精靈。
4. 在精靈的**選擇角色**頁面，選取您要指派的使用者角色。
5. 在精靈的**定義範圍**頁面，選取您要新增至使用者角色範圍的管理群組。
6. 點擊**分配角色**按鈕以關閉精靈。

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. 點擊您要定義範圍的角色名稱。
3. 在開啟的角色內容視窗中，選取**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. 在精靈的**定義範圍**頁面，選取您要新增至使用者角色範圍的管理群組。
6. 在精靈的**選取使用者**頁面，選取您要新增到使用者角色範圍的使用者和安全群組。
7. 點擊**分配角色**按鈕以關閉精靈。
8. 點擊**關閉**按鈕（ ✕ ）以關閉角色內容視窗。

所選使用者或安全群組和所選管理群組被新增到使用者角色範圍。

刪除使用者角色

要刪除使用者角色：

1. 在主功能表中，轉至 **使用者和角色** → **角色**。
2. 選取您要刪除的角色旁邊的核取方塊。
3. 點擊**刪除**。
4. 在開啟的視窗中，點擊**確定**按鈕。

使用者角色被刪除。

關聯政策設定檔到角色

您可以關聯使用者角色到政策設定檔。此種情況下，該政策設定檔的啟動規則基於角色：政策設定檔對具有指定角色的使用者可用。

例如，政策禁止在管理群組的所有裝置上執行 GPS 導航軟體。GPS 導航軟體僅在"使用者"管理群組中的單個裝置上是必須的——該裝置屬於導遊。此種情況下，您可以分配"導遊"角色給其所有者，然後建立一個政策設定檔，允許 GPS 導航軟體僅在分配了"導遊"角色的使用者的裝置上執行。所有其他政策設定被保留。僅帶有"導遊"角色的使用者將被允許執行 GPS 導航軟體。然後，如果其他員工被分配了"導遊"角色，該新員工也在組織的裝置上執行導航軟體。執行 GPS 導航軟體在相同管理群組的其他裝置上仍將被禁止。

要關聯角色到政策設定檔：

1. 在主功能表中，轉至 **使用者和角色** → **角色**。
2. 選取您要關聯政策設定檔的角色名稱。
   角色內容視窗會開啟，並含有所選的**一般**頁籤。
3. 選取**設定**頁籤，之後向下捲動至**政策和設定檔**區段。
4. 點擊**編輯**。
5. 要關聯角色到：

- **現有政策設定檔**—點擊所學政策名稱旁邊的臂章圖示（ ）， 然後選取您要關聯角色的設定檔旁邊的核取方塊。
- **新政策設定檔**：
    a. 選取您要建立設定檔的政策旁邊的核取方塊。
    b. 點擊**新政策設定檔**。
    c. 為新設定檔指定名稱並配置設定檔設定。
    d. 點擊**儲存**按鈕。
    e. 選取新設定檔旁邊的核取方塊。

6. 點擊**分配到角色**。

設定檔被關聯到角色並顯示在角色內容中。設定檔自動應用到分配了該角色的使用者的任意裝置。

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。

支援修訂管理的應用程式物件包括：

- 管理伺服器
- 政策
- 工作
- 管理群組
- 使用者帳戶
- 安裝套件

您可以對物件修訂採取以下操作：

- 將所選修訂與目前進行比較
- 比較所選的修訂
- 將物件與相同類型的其他物件的所選修訂進行比較
- 檢視所選修訂
- 回溯對物件所做的變更到所選的修訂
- 儲存修訂到 .txt 檔案

在支援修訂管理的任何物件的內容視窗中，**變更歷程**區域會顯示含有以下詳情的物件修訂清單：

- 物件修訂版本
- 物件修改的日期和時間
- 修改物件的使用者的名稱
- 執行在物件上的操作
- 與物件設定變更相關的修訂敘述
  預設下，物件修訂敘述為空。若要新增敘述到修訂，選取相關修訂並點擊**敘述**按鈕。在**物件修訂敘述**視窗，輸入修訂敘述的部分文字。

關於物件修訂

您可以對物件修訂採取以下操作：

- 將所選修訂與目前進行比較
- 比較所選的修訂

- 將物件與相同類型的其他物件的所選修訂進行比較
- 檢視所選修訂
- 回溯對物件所做的變更到所選的修訂
- 儲存修訂到 .txt 檔案

在支援修訂管理的任何物件的內容視窗中，**變更歷程**區域會顯示含有以下詳情的物件修訂清單：

- 物件修訂版本
- 物件修改的日期和時間
- 修改物件的使用者的名稱
- 執行在物件上的操作
- 與物件設定變更相關的修訂敘述

回溯物件到先前修訂

如果必要，您可以回溯對物件所做的變更。例如，您可能必須轉換政策設定到特定日期的狀態。

要回溯對物件所做的變更：

1. 在物件的內容視窗中，開啟**變更歷程**頁籤。
2. 在物件修訂清單中，選取您必須復原的修訂。
3. 點擊**回溯**按鈕。
4. 點擊**確定**以確認操作。

該物件被回溯到所選修訂。物件修訂清單顯示所做的操作記錄。修訂敘述顯示了您轉換物件所到的修訂號的資訊。

復原操作僅適用於政策和工作物件。

物件刪除

該部分提供了關於刪除物件和檢視已刪除物件的資訊。

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

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。

使用 klscflag 實用程式開啟連接埠 13291

管理伺服器上的連接埠 13291 用於接收來自管理主控台的連線。在非 Windows 電腦上，此連接埠預設不開啟。如果想要使用基於 MMC 的管理主控台或 klakaut 實用程式，可以使用 klscflag 實用程式開啟此連接埠。此實用程式可變更 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：

```
$ 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：

```
$ 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
```

真 值表示連接埠已開啟。否則，系統將顯示 假 值。

更新 Kaspersky 資料庫和應用程式

該部分敘述了定期更新以下內容必須採取的步驟：

- 卡巴斯基資料庫和軟體模組
- 已安裝的 Kaspersky 應用程式，包括卡巴斯基安全管理中心元件和安全應用程式

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方案。完成設定網路防護情境後，您必須維持防護系統的可靠性，確保管理伺服器和受管理裝置受到多種威脅的防護，包含病毒、網路攻擊與釣魚攻擊。

網路防護透過更新以下內容保持最新：

- 卡巴斯基資料庫和軟體模組
- 已安裝的 Kaspersky 應用程式，包括卡巴斯基安全管理中心元件和安全應用程式

當您完成此情境，您可確保以下事項：

- 您的網路被最近的卡巴斯基軟體防護，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 14 網頁主控台佈署 Kaspersky 應用程式的方案佈署 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，根據網路防護配置方案。
3. 分配了適當數量的發佈點，與受管理裝置和網路拓撲一致。

更新 Kaspersky 資料庫和應用程式分步驟進行：

1 選取更新方案

您可使用多種方案為卡巴斯基安全管理中心元件和安全應用程式安裝更新。選取一個或多個滿足您網路需求的方案。

2 建立管理伺服器的“將更新下載至儲存區”工作

該工作由卡巴斯基安全管理中心快速啟動精靈自動建立。如果您未執行精靈，立即建立工作。

需要該工作以從 Kaspersky 更新伺服器下載更新到管理伺服器儲存區，以及為卡巴斯基安全管理中心更新 Kaspersky 資料庫和軟體模組。更新被下載後，它們可以被傳播到受管理裝置。

如果您的網路被分配了發佈點，更新被從管理伺服器儲存區自動下載到發佈點儲存區。此種情況下，發佈點所在範圍的受管理裝置從發佈點儲存區下載更新，而不是從管理伺服器儲存區。

說明：建立管理伺服器的"將更新下載至儲存區"工作

3. **建立"將更新下載至發佈點儲存區"工作（可選）**

   預設下，更新被從管理伺服器下載到發佈點。您可以配置卡巴斯基安全管理中心直接從 Kaspersky 更新伺服器下載更新到發佈點。您可以下載到發佈點儲存區，例如，如果管理伺服器和發佈點之間的流量比發佈點和 Kaspersky 更新伺服器之間的流量貴，或者如果您的管理伺服器沒有網際網路存取。

   當您的網路獲得指派的發佈點並且建立了*將更新下載至發佈點儲存區*工作後，發佈點會從 Kaspersky 更新伺服器下載更新，而非管理伺服器儲存區。

   說明：建立「將更新下載至發佈點儲存區」工作

4. **配置發佈點**

   當您的網路有指派的發佈點時，請確保**佈署更新**選項已在所有必要發佈點中啟用。當該選項對發佈點停用時，包含在發佈點範圍中的裝置從管理伺服器儲存區下載更新。

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裝置之間的流量。當該功能被啟用時，管理伺服器或發佈點下載 diff 檔案，而不是整個 Kaspersky 資料庫或軟體模組檔案。diff 檔案敘述了資料庫或軟體模組的檔案的兩個版本之間的差異。因此，diff 檔案比整個檔案佔用更少的空間。這導致降低管理伺服器之間或發佈點和受管理裝置之間的流量。若要使用此功能，請啟用*將更新下載至管理伺服器儲存區*工作和/或*將更新下載至發佈點儲存區*工作內容中的**下載差異檔案**選項。

   說明：使用 diff 檔案更新 Kaspersky 資料庫和軟體模組

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。

   如果您的網路包括僅支援 IPv6 的裝置，並且您想要定期更新安裝在這些裝置上的安全應用程式，請確保管理伺服器 13.2 版和網路代理 13.2 版安裝在受管理裝置上。

   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。

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。這是為了確保更新病毒資料庫並維護受管裝置的安全級別。

- 已安裝的 Kaspersky 應用程式，包括卡巴斯基安全管理中心元件和安全應用程式

  卡巴斯基安全管理中心無法自動更新卡巴斯基應用程式。要更新應用程式，請從卡巴斯基網站下載最新的應用程式版本，然後手動安裝它們：

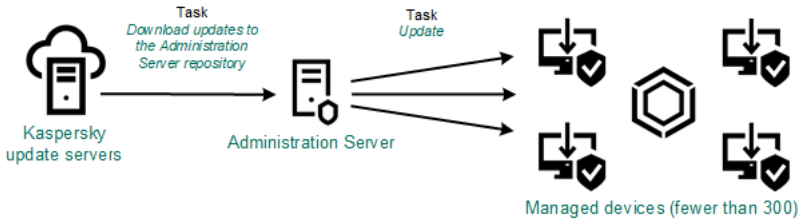
  - 卡巴斯基安全管理中心管理伺服器和卡巴斯基安全管理中心 14 網頁主控台
  - 網路代理、Kaspersky Endpoint Security for Linux、管理 Web 外掛程式

取決於您網路的配置，您可以使用以下方案來下載和分發所需更新到受管理裝置：

- 透過使用單個工作：*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 for Linux
- 如果管理伺服器沒有網際網路連線，則透過本機或網路資料夾

使用將更新下載至管理伺服器儲存區工作

在此方案中，卡巴斯基安全管理中心會透過*將更新下載至管理伺服器儲存區*工作下載更新。在單一網段包含少於 300 台受管理裝置或每個網段包含少於 10 台受管理裝置的小網路中，更新直接從管理伺服器儲存區被分發到受管理裝置（參見下圖）。



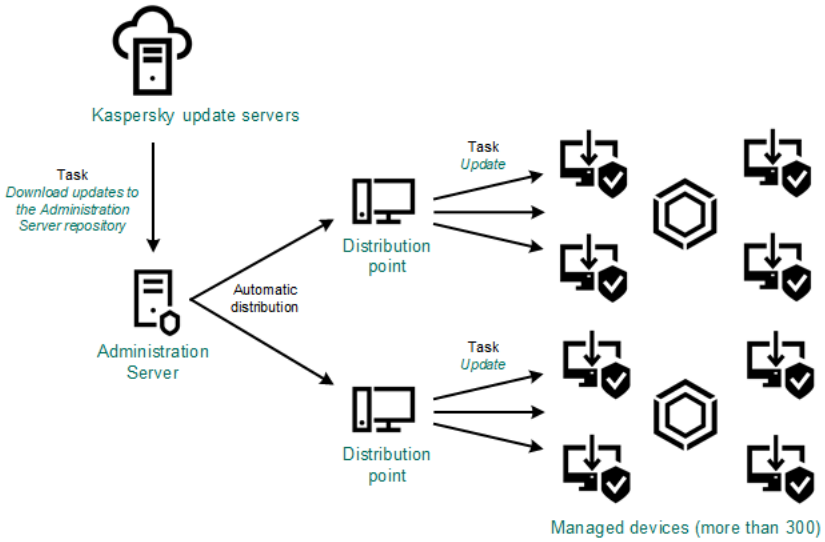
使用將更新下載至管理伺服器儲存區工作在沒有發佈點狀態下更新

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 更新伺服器通信並使用 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 for Linux 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 for Linux 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。

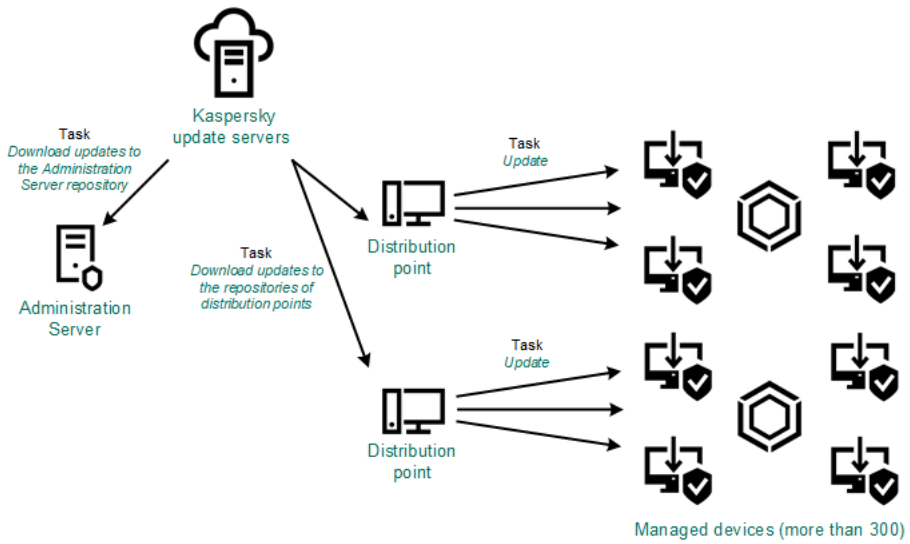
每個 Kaspersky 應用程式都從管理伺服器請求所需更新。管理伺服器集合這些更新並僅下載應用程式請求的更新。這確保了相同更新不被下載多次，且不必要更新不被下載。當執行*將更新下載至管理伺服器儲存區*工作時，管理伺服器自動傳送以下資訊到 Kaspersky 更新伺服器以便確保相關版本的 Kaspersky 資料庫和軟體模組的下載：

- 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

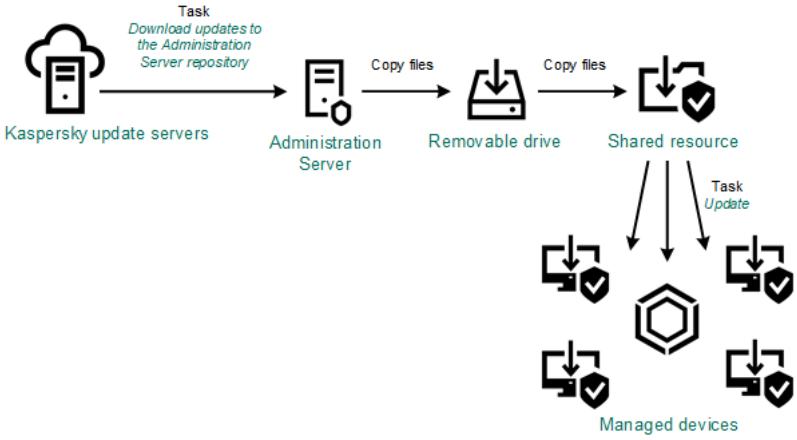
預設下，管理伺服器和發佈點與 Kaspersky 更新伺服器通信並使用 HTTPS 協定下載更新。您可以配置管理伺服器和/或發佈點使用 HTTP 協定，而不是 HTTPS。

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。

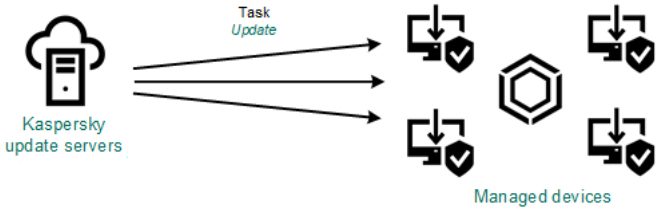
如果裝置未連線到管理伺服器，您可以使用本機資料夾或共用資料夾作為更新 Kaspersky 資料庫、軟體模組和應用程式的更新來源。在此方案中，您需要從管理伺服器儲存區複製所需更新到卸除式磁碟機，然後複製更新到在 Kaspersky Endpoint Security for Linux 設定 中指定的本機資料夾或共用資料夾作為更新來源（參見下圖）。



透過本機資料夾、共用資料夾或 FTP 伺服器更新

直接從卡巴斯基更新伺服器到受管理裝置上的 Kaspersky Endpoint Security for Linux

在受管理裝置上，您可以配置 Kaspersky Endpoint Security for Linux 直接從卡巴斯基更新伺服器接收更新（參見下圖）。



直接從卡巴斯基更新伺服器更新安全應用程式

在此方案中，安全應用程式不使用卡巴斯基安全管理中心提供的儲存區。要直接從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。對於這些設定的完整描述，請參考 Kaspersky Endpoint Security for Linux 文件 。

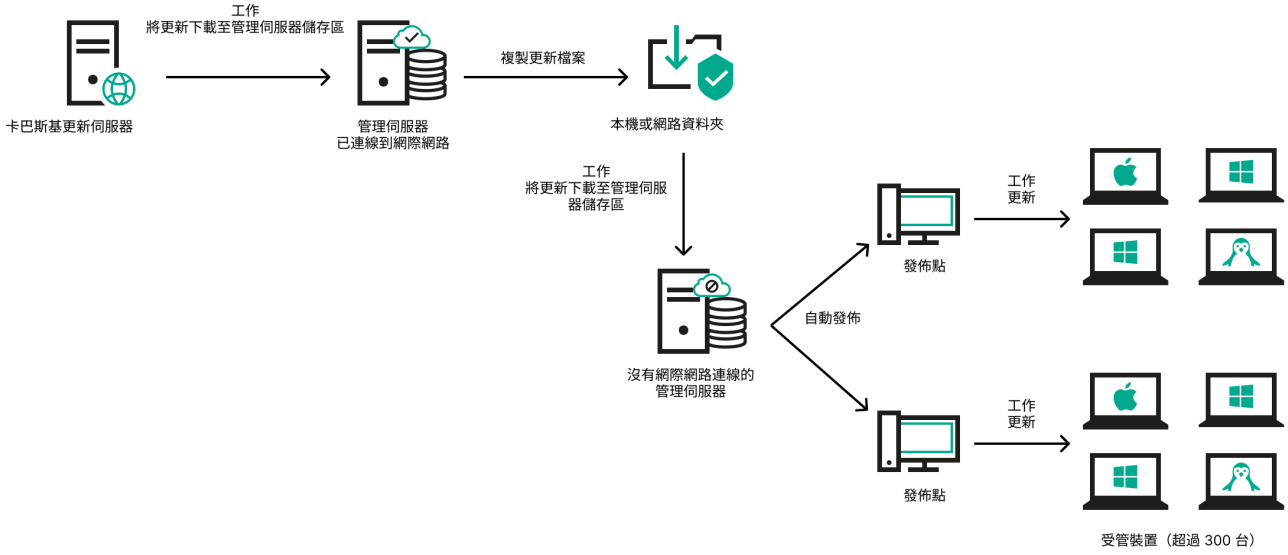
如果管理伺服器沒有網際網路連線，則透過本機或網路資料夾

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*從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

  由於此實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*工作的屬性，然後啟用*使用舊配置下載更新*選項。

建立“將更新下載至管理伺服器儲存區”工作

延伸所有 | 折疊所有

*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。要在分發之前對其進行驗證，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. 前往**裝置** → **工作**。
2. 點擊**新增**。

"新增工作"精靈啟動。遵照精靈的步驟操作。

3. 對於卡巴斯基安全管理中心應用程式，請選取**將更新下載至管理伺服器儲存區**工作類型。

4. 指定您正建立的工作的名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元（ *<>-_?:\"| ）。

5. 在**完成工作建立**頁面，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並修改預設工作設定。否則，您可以稍後隨時配置工作設定。

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、本機或網路資料夾或主管理伺服器。

   - **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。

   - **複製下載的更新至其他資料夾**

     管理伺服器接收更新後，它複製它們到指定資料夾。如果您想要在您的網路上手動管理更新的分發，則使用該選項。

     例如，您可能要在以下情況下使用該選項：您組織的網路包含幾個獨立子網路，且每個子網路的裝置不能存取其他子網路。然而，所有子網路中的裝置都可以存取通用網路共用。此種情況下，您在子網路之一設定管理伺服器從 Kaspersky 更新伺服器下載更新，啟用該選項，然後指定該網路共用。對於其他管理伺服器的"將更新下載至儲存區"工作中，指定與更新來源相同的網路共用。

     預設情況下已停用該選項。

   - **下載差異檔案**

     該選項啟用下載 diff 檔案功能。

     預設情況下已停用該選項。

   - **使用舊配置下載更新**

     從版本 14 開始，卡巴斯基安全管理中心使用新方案下載資料庫和軟體模組的更新。對於使用新方案下載更新的應用程式，更新來源必須包含具有與新方案相容的中繼資料的更新檔案。如果更新來源包含的更新檔案的中繼資料僅與舊方案相容，請啟用 **使用舊配置下載更新** 選項。否則，更新下載工作將失敗。

     例如，當本機或網路資料夾被指定為更新來源並且此資料夾中的更新檔案由以下應用程式之一下載時，您必須啟用此選項：

     - Kaspersky Update Utility

       此實用程式使用舊方案下載更新。

     - 卡巴斯基安全管理中心 13.2 或更早版本

       例如，您的管理伺服器 1 沒有網際網路連線。在這種情況下，您可以使用具有網際網路連線的管理伺服器 2 下載更新，然後將更新放置到本機或網路資料夾以將其用作管理伺服器 1 的更新來源。如果管理伺服器 2 的版本為 13.2 或更早，請啟用管理伺服器 1 的工作中的 **使用舊配置下載更新** 選項。

     預設情況下已停用該選項。

   - **執行更新驗證**

     管理伺服器會從源下載更新並將其儲存到暫時儲存區，之後執行**更新驗證工作**欄位中定義的工作。如果工作成功完成，系統會從暫時儲存區將更新複製到管理伺服器共用資料夾，然後分發到所有以管理伺服器作為更新來源的裝置（系統會啟動有**當新更新下載至儲存區時**排程類型的工作）。"將更新下載至儲存區"工作僅在*更新驗證*工作完成後結束。

     預設情況下已停用該選項。

9. 在工作內容視窗的**排程**頁籤，建立工作開始的排程。如果必要，指定以下設定：

   - **排程開始**:

選取工作執行排程並設定所選排程。

- **手動**（預設選取）

  工作不自動執行。您僅可以手動啟動。
  預設情況下已啟用該選項。

- **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，工作每六小時執行一次，從目前系統日期和時間開始。

- **每 N 天**

  工作定期執行，按照指定天數間隔。此外，您可指定第一個工作執行的日期與時間。這些額外選項會在您建立的工作受到應用程式支援時可用。
  預設下，工作每天執行一次，從目前系統日期和時間開始。

- **每 N 星期**

  工作定期執行，按照指定星期數間隔，從指定的星期和時間開始。
  預設下，工作每星期一於目前系統時間執行一次。

- **每天（不支援日光節約時間）**

  工作定期執行，按照指定天數間隔。排程不支援日光節約時間 (DST)。這意味著在夏令時開始和結束時當時鐘向前或向後撥動一小時時，實際工作啟動時間不變更。
  我們不建議您使用該排程。它用於向後相容卡巴斯基安全管理中心 Linux。
  預設下，工作每天於目前系統時間執行一次。

- **每週**

  工作每週在指定星期和指定時間執行。

- **按每星期中的指定日**

  工作定期執行，在指定星期的指定時間。
  預設下，工作每週五 6:00:00 P.M. 執行。

- **每月**

  工作定期執行，在指定月日的指定時間。
  在缺少指定日的月份，工作在最後一天執行。
  預設下，工作在每月的第一天執行，在目前系統時間。

- **每個月在所選週的指定天**

  工作定期在指定月日的指定時間執行。
  預設下，未選取月日；預設啟動時間是 6:00:00 P.M.。

- **在完成其它工作時**

  目前工作在其他工作完成後啟動。您可以選取先前工作如何結束（成功或帶有錯誤）以觸發目前工作的啟動。

- 其它工作設定：

  - **執行略過的工作**

    該選項決定在工作要啟動時用戶端裝置在網路中不可見時工作的行為。

    如果啟用該選項，系統將在下一次在用戶端裝置上執行 Kaspersky 應用程式時嘗試啟動工作。如果工作排程是**手動**、**一次**或**立即**，裝置在網路中可見或包含在工作範圍後，工作會立即啟動。

    如果停用該選項，則只有已排程的工作會在用戶端裝置上啟動，而對於**手動**、**一次**與**立即**而言，僅在網路中可見的用戶端裝置上會啟動。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。

    預設情況下已啟用該選項。

  - **使用工作啟動自動隨機延遲**

    如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動，即是，*分佈式工作啟動*。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

    當工作被建立時，根據工作中包含用戶端裝置的數量，分發啟動時間被自動計算。然後，工作總是在計算的開始時間啟動。然後當工作設定被編輯或者工作被手動啟動時，計算的工作啟動時間值被變更。

    如果該選項被停用，工作依據排程在用戶端裝置上啟動。

  - **使用工作啟動隨機延遲間隔（分鐘）**

    如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。

    如果該選項被停用，工作依據排程在用戶端裝置上啟動。

    預設情況下已停用該選項。預設時間間隔為一分鐘。

  - **如果工作執行長於此時間則停止工作（分鐘）**

    在指定時間段過後，工作被自動停止，無論它是否完成。

    如果您想要中斷或停止執行時間太長的工作，則啟用該選項。

    預設情況下已停用該選項。預設工作執行時間是 120 分鐘。

10. 點擊**儲存**按鈕。

    工作被建立和配置。

當管理伺服器執行*將更新下載至管理伺服器儲存區*工作時，資料庫和軟體模組更新將從更新來源下載並儲存在管理伺服器共用資料夾中。如果您為管理群組建立此工作，它將僅被套用到包含在指定管理群組中的網路代理。

這些更新將從管理伺服器共用資料夾分發至用戶端裝置和次要管理伺服器。

瀏覽已下載的更新

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。您可以在**Kaspersky 資料庫和軟體模組更新**區域中檢視下載的更新。

要檢視已下載的更新，

在主功能表中，轉至 **操作 → Kaspersky 應用程式 → Kaspersky 資料庫和軟體模組更新**。

可用更新清單被顯示。

驗證已下載的更新

安裝更新到受管理裝置之前，您可以先透過*更新驗證*工作檢查更新。*更新驗證*工作會自動作為*將更新下載至管理伺服器儲存區*工作的一部分執行。管理伺服器從更新來源下載更新、將其儲存在臨時儲存區並執行*更新驗證*工作。如果工作成功完成，更新將從臨時儲存區複製到管理伺服器共用資料夾。它們被分發到所有以該管理伺服器為更新來源的用戶端裝置。

如果*更新驗證*工作的結果顯示位於臨時儲存區中的更新是錯誤的，或*更新驗證*工作發生錯誤，這些更新不會被複製到共用資料夾。管理伺服器保留之前的更新集。此外，有**當新更新下載至儲存區時**排程類型的工作也不會啟動。若新更新的掃描成功完成，這些操作會在*將更新下載至管理伺服器儲存區*工作下次啟動時執行。

如果在一台或多台測試裝置上出現以下情況，那麼更新就被認為是無效的：

- 發生了更新工作錯誤。
- 安全應用程式的即時防護狀態在套用更新後變更。
- 執行自訂掃描工作過程中發現一個被感染的物件。
- Kaspersky 程式出現執行階段錯誤。

如果在任何測試裝置上未出現以上情況，則此更新集就被認為是有效的，*更新驗證*工作被認為已成功完成。

在開始建立*更新驗證*工作之前 ，執行先決條件：

1. 用幾個測試裝置建立管理群組。您將需要該組來驗證更新。

   我們建議使用網路中防護最可靠、應用程式設定最常用的裝置作為測試裝置。這種方法提高了掃描期間病毒偵測的品質和概率，將誤報的風險降至最低。如果在測試裝置上偵測到病毒，*更新驗證*工作將被判定為不成功。

2. 為卡巴斯基安全管理中心支援的應用程式（例如 Kaspersky Endpoint Security for Linux）建立更新和病毒掃描工作。當建立更新和病毒掃描工作時，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病毒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，您需要指定更新和病毒掃描工作。

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 **裝置 → 工作**。
2. 點擊**將更新下載至管理伺服器儲存區**工作。
3. 在開啟的內容視窗中，轉至**應用程式設定**頁籤，然後啟用**執行更新驗證**選項。
4. 如果*更新驗證*工作存在，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擇*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"新增工作精靈"中，如果要變更預設名稱，請指定工作名稱。

   c. 選擇您之前建立的具有測試裝置的管理群組。

   d. 首先，選擇卡巴斯基安全管理中心支援的所需應用程式的更新工作，然後選擇病毒掃描工作。

   之後，將出現以下選項。我們建議啟用它們：

   - **在資料庫更新後重新啟動裝置**

     在裝置上更新病毒資料庫後，我們建議重新啟動裝置。

     依預設已啟用該選項。

   - **在資料庫更新和裝置重新啟動後檢查即時防護狀態**

     如果啟用此選項，則*更新驗證*工作將檢查下載到管理伺服器儲存區的更新是否有效，以及在病毒資料庫更新和裝置重啟後防護等級是否降低了。

     預設情況下已啟用該選項。

   e. 指定一個帳戶，*更新驗證*工作將從該帳戶執行。您可以使用您的帳戶並啟用**預設帳戶**選項。或者，您可以指定工作應在具有必要存取權限的另一個帳戶下執行。為此，請選擇 **指定帳戶** 選項，然後輸入該帳戶的憑據。

6. 點擊**儲存**關閉*將更新下載至管理伺服器儲存區*工作的內容視窗。

自動更新驗證被啟用。現在，您可以執行*將更新下載至管理伺服器儲存區*工作，它將從更新驗證開始。

建立「將更新下載至發佈點儲存區」工作

您可以為管理群組建立*將更新下載至發佈點儲存區*工作。該工作將為包含在指定管理群組中的發佈點執行。

您可以使用該工作，例如，如果管理伺服器和發佈點之間的流量比發佈點和 Kaspersky 更新伺服器之間的流量貴，或者如果您的管理伺服器沒有網際網路存取。

該工作用在從 Kaspersky 更新伺服器下載更新到發佈點儲存區時。更新清單包含：

- Kaspersky 安全應用程式資料庫和軟體模組更新
- 卡巴斯基安全管理中心元件更新
- Kaspersky 安全應用程式更新

更新被下載後，它們可以被傳播到受管理裝置。

*若要針對選取的管理群組建立**將更新下載至發佈點儲存區**工作：*

1. 在主功能表中，轉至 **裝置 → 工作**。
2. 點擊**新增**按鈕。
   新增工作精靈啟動。遵照精靈的步驟操作。
3. 若為卡巴斯基安全管理中心應用程式，請在**工作類型**欄位選取**將更新下載至發佈點儲存區**。
4. 指定您正建立的工作的名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元（ *<>-_?:\"| ）。
5. 選取一個選項按鈕以指定管理群組、裝置分類或應用程式工作的裝置。
6. 在 **完成工作建立** 步驟，如果要修改預設工作設定，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. 點擊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 程式可以從 Kaspersky 的 HTTP(S) 伺服器下載資料庫和程式模組更新。
       預設情況下已選取此選項。
     - 主管理伺服器
       該資源套用到為次要或虛擬管理伺服器建立的工作。
     - 本機或網路資料夾
       包含最新更新的本機或網路資料夾。網路資料夾可以是 FTP 或 HTTP 伺服器，或者 SMB 共用。如果網路資料夾需要身分驗證，則僅支援 SMB 通訊協定。在選取本機資料夾時，您必須在安裝了管理伺服器的裝置上指定一個資料夾。

       更新來源所使用的 FTP 或 HTTP 伺服器或網路資料夾必須包含比對 Kaspersky 更新伺服器所建立的結構的資料夾結構（帶有更新）。

     如果為卡巴斯基更新伺服器或本機或網路資料夾更新來源啟用**不使用代理伺服器**選項，則即使您為發佈點啟用了網路代理政策設定的**使用代理伺服器**選項，發佈點也不使用代理伺服器下載更新。

   - **更新儲存資料夾**

     用於儲存已儲存更新的指定資料夾的路徑。您可以將指定的資料夾路徑複製到剪貼簿。您不能變更群組工作的指定資料夾的路徑。

   - **下載差異檔案**

     該選項啟用下載 diff 檔案功能。

預設情況下已停用該選項。

- **使用舊配置下載更新**

  從版本 14 開始，卡巴斯基安全管理中心使用新方案下載資料庫和軟體模組的更新。對於使用新方案下載更新的應用程式，更新來源必須包含具有與新方案相容的中繼資料的更新檔案。如果更新來源包含的更新檔案的中繼資料僅與舊方案相容，請啟用 **使用舊配置下載更新** 選項。否則，更新下載工作將失敗。

  例如，當本機或網路資料夾被指定為更新來源並且此資料夾中的更新檔案由以下應用程式之一下載時，您必須啟用此選項：

  - Kaspersky Update Utility

    此實用程式使用舊方案下載更新。

  - 卡巴斯基安全管理中心 13.2 或更早版本

    例如，發佈點被配置為從本機或網路資料夾獲取更新。在這種情況下，您可以使用具有網際網路連線的管理伺服器下載更新，然後將更新放在發佈點上的本機資料夾中。如果管理伺服器的版本為 13.2 或更早，請啟用*將更新下載到發佈點的儲存區* 工作中的**使用舊配置下載更新**選項。

  預設情況下已停用該選項。

10. 為工作啟動建立排程。如果必要，指定以下設定：

- **排程開始**：

  選取工作執行排程並設定所選排程。

  - **手動**（預設選取）

    工作不自動執行。您僅可以手動啟動。

    預設情況下已啟用該選項。

  - **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，工作每六小時執行一次，從目前系統日期和時間開始。

  - **每 N 天**

    工作定期執行，按照指定天數間隔。此外，您可指定第一個工作執行的日期與時間。這些額外選項會在您建立的工作受到應用程式支援時可用。

    預設下，工作每天執行一次，從目前系統日期和時間開始。

  - **每 N 星期**

    工作定期執行，按照指定星期數間隔，從指定的星期和時間開始。

    預設下，工作每星期一於目前系統時間執行一次。

  - **每天（不支援日光節約時間）**

    工作定期執行，按照指定天數間隔。排程不支援日光節約時間 (DST)。這意味著在夏令時開始和結束時當時鐘向前或向後撥動一小時時，實際工作啟動時間不變更。

    我們不建議您使用該排程。它用於向後相容卡巴斯基安全管理中心 Linux。

    預設下，工作每天於目前系統時間執行一次。

  - **每週**

工作每週在指定星期和指定時間執行。

- **按每星期中的指定日**

  工作定期執行，在指定星期的指定時間。
  預設下，工作每週五 6:00:00 P.M. 執行。

- **每月**

  工作定期執行，在指定月日的指定時間。
  在缺少指定日的月份，工作在最後一天執行。
  預設下，工作在每月的第一天執行，在目前系統時間。

- **每個月在所選週的指定天**

  工作定期在指定月日的指定時間執行。
  預設下，未選取月日；預設啟動時間是 6:00:00 P.M.。

- **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防毒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分類。

- **在完成其它工作時**

  目前工作在其他工作完成後啟動。您可以選取先前工作如何結束（成功或帶有錯誤）以觸發目前工作的啟動。

- **執行略過的工作**

  該選項決定在工作要啟動時用戶端裝置在網路中不可見時工作的行為。
  如果啟用該選項，系統將在下一次在用戶端裝置上執行 Kaspersky 應用程式時嘗試啟動工作。如果工作排程是**手動**、**一次**或**立即**，裝置在網路中可見或包含在工作範圍後，工作會立即啟動。
  如果停用該選項，則只有已排程的工作會在用戶端裝置上啟動，而對於**手動**、**一次**與**立即**而言，僅在網路中可見的用戶端裝置上會啟動。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。
  預設情況下已啟用該選項。

- **使用工作啟動自動隨機延遲**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動，即是，*分佈式工作啟動*。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。
  當工作被建立時，根據工作中包含用戶端裝置的數量，分發啟動時間被自動計算。然後，工作總是在計算的開始時間啟動。然後當工作設定被編輯或者工作被手動啟動時，計算的工作啟動時間值被變更。
  如果該選項被停用，工作依據排程在用戶端裝置上啟動。

- **使用工作啟動隨機延遲間隔（分鐘）**

  如果該選項被啟用，工作將在用戶端裝置啟動，而是在一定的時間間隔內隨機啟動。當分佈式工作執行時，分發的工作可以幫助避免從用戶端裝置到管理伺服器同時大量的請求。
  如果該選項被停用，工作依據排程在用戶端裝置上啟動。
  預設情況下已停用該選項。預設時間間隔為一分鐘。

11. 點擊**儲存**按鈕。

工作被建立和配置。

除了您在工作建立過程中指定的設定，您還可以變更所建立工作的其他內容。

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
  該資源套用到為次要或虛擬管理伺服器建立的工作。
- 本機或網路資料夾

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。作為本機資料夾，您只能使用管理伺服器上的一個資料夾；作為網路資料夾，您只能使用 FTP 或 HTTP 伺服器。

如果您同時新增卡巴斯基更新伺服器和本機或網路資料夾，更新將首先從該資料夾下載。如果下載時出錯，將使用卡巴斯基更新伺服器。

如果包含更新的共用資料夾受密碼防護，請啟用**指定帳戶以存取更新來源的共用資料夾（如果有）**選項並輸入存取所需的帳戶憑據。

要新增更新來源：

1. 前往**裝置 → 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**行，點擊**設定**按鈕。
5. 在開啟的視窗中，點擊**新增**按鈕。
6. 在更新來源清單中，新增必要的來源。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。
7. 點擊**確定**，然後關閉更新來源內容視窗。
8. 在更新來源視窗中，點擊**確定**。
9. 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。

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：方案

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

延伸所有 | 折疊所有

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. 在應用程式主視窗，點擊所需管理伺服器名稱旁邊的**設定圖示**（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**發佈點**區段。
3. 點擊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，請點擊**建立工作**連接以建立工作。新增工作精靈啟動。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：\\<server name>\KLSHARE\Updates。

   或者，您可以配置卡巴斯基安全管理中心定期複製更新到您選取的資料夾。為此，請使用*將更新下載至管理伺服器儲存區*工作內容中的**複製下載的更新至其他資料夾**選項。如果您指定快閃記憶體磁碟機或外部硬碟磁碟機上的資料夾作為該選項的目的資料夾，該大容量裝置將總是包含更新的最新版本。
3. 在離線裝置上，配置 Kaspersky Endpoint Security for Windows 以從本機資料夾或共用資料夾接收更新，例如 FTP 伺服器或共用資料夾。
4. 從卸除式磁碟機複製更新到您想用作更新來源的本機資料夾或共用資源。
5. 在需要安裝更新的離線裝置上，開始 Kaspersky Endpoint Security for Linux 的更新工作。

在更新工作完成後，Kaspersky 資料庫和軟體模組在裝置上變為最新。

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。

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。

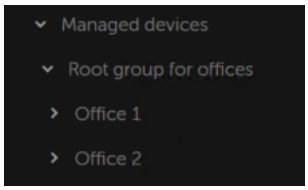
有以下構建管理群組結構的方法：

- 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 實用程式偵錯。

發佈點的標準配置：多個小遠端分辦公室

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/10,000 + 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。

要自動分配發佈點：

1. 在應用程式主視窗，點擊所需管理伺服器名稱旁邊的**設定圖示**（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**發佈點**區段。
3. 選取**自動分配發佈點**選項。

   如果自動指派裝置作為發佈點被啟用，您無法手動配置發佈點，也不能編輯發佈點清單。

4. 點擊**儲存**按鈕。

管理伺服器便自動指派和配置發佈點。

手動分配發佈點

延伸所有 | 折疊所有

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分配發佈點（例如，如果您要使用單獨分配的伺服器），您可以在計算數量和配置後手動分配發佈點。

作為發佈點的裝置必須被防護，包括實體防護，以防範非授權的存取。

要手動指派裝置作為發佈點：

1. 在應用程式主視窗，點擊所需管理伺服器名稱旁邊的**設定圖示**（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**發佈點**區段。
3. 選取**手動分配發佈點**選項。
4. 點擊**分配**按鈕。
5. 選擇您要製作發佈點的裝置。
   選取裝置時，請牢記發佈點的操作功能以及裝置作為發佈點的需求。
6. 選擇您要包含在所選發佈點範圍的管理群組。
7. 點擊**確定**按鈕。
   您新增的發佈點將顯示在**發佈點**區域的發佈點清單。
8. 在清單中選擇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 埠號**

       用戶端裝置與發佈點之間，使用 SSL 進行安全連線的 SSL 埠號。
       預設情況下使用連接埠 13000。

     - **使用多點傳送**

       如果啟用此選項，程式會使用 IP 多點傳送，在群組中的各用戶端裝置上自動發佈安裝套件。
       IP 多點傳送會減少從安裝套件安裝應用程式至一組用戶端裝置的時間，但當您安裝應用程式至單一用戶端裝置時會增加安裝時間。

     - **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 多點傳輸埠號**

  IP 多點傳輸的埠號。

  預設情況下，埠號指定為 15001。如果執行管理伺服器的裝置指定為發佈點，連接埠 13001 預設用於 SSL 連線。

- **佈署更新**

  更新被從以下來源分發到受管理裝置：

  - 此發佈點（如果啟用此選項）。
  - 其他發佈點、管理伺服器或卡巴斯基更新伺服器（如果停用此選項）。

  使用發佈點來佈署更新可以節省流量，因為您減少了下載次數。此外，您可以減輕管理伺服器上的負載並在發佈點之間重新定位負載。您可以計算網路的發佈點數量以最佳化流量和負載。

  如果停用此選項，管理伺服器上的更新下載和負載數量可能會增加。預設情況下已啟用該選項。

- **佈署安裝套件**

  安裝套件被從以下來源分發到受管理裝置：

  - 此發佈點（如果啟用此選項）。
  - 其他發佈點、管理伺服器或卡巴斯基更新伺服器（如果停用此選項）。

  使用發佈點來佈署安裝套件可以節省流量，因為您減少了下載次數。此外，您可以減輕管理伺服器上的負載並在發佈點之間重新定位負載。您可以計算網路的發佈點數量以最佳化流量和負載。

  如果停用此選項，管理伺服器上的安裝套件下載和負載數量可能會增加。預設情況下已啟用該選項。

- 在"**範圍**"區域，指定發佈點將向其分發更新的管理組。
- 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，請點擊**建立工作**連接以建立工作。新增工作精靈啟動。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。

- 配置發佈點對 IP 範圍的輪詢。

  - **IP 範圍**

    您可以為 IPv4 範圍和 Ipv6 網路啟用裝置發現。

    如果啟用"**啟用範圍輪詢**"核取方塊，您可以新增掃已描範圍並為其設定排程。您可以新增 IP 範圍到已掃描範圍清單。

    如果啟用 **啟用輪詢與 Zeroconf 技術** 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。

- 在**進階**區域，指定發佈點必須使用以儲存發佈資料的資料夾。

  - **使用預設的資料夾**

如果您選取此選項，應用程式使用發佈點上的網路代理安裝資料夾。

- **使用指定的資料夾**

  如果您選取該選項，則可以在下面的欄位中指定該資料夾的路徑。它可以是發佈點上的本機資料夾，也可以是企業網路上任何裝置的資料夾。

  發佈點上用於執行網路代理的帳戶必須具有對指定資料夾的存取權限以進行讀寫操作。

10. 點擊**確定**按鈕。

所選裝置作為發佈點執行。

修改管理群組的發佈點清單

您可以檢視為特定管理群組分配的發佈點清單並透過新增或刪除發佈點來修改清單。

要檢視和修改分配給管理群組的發佈點清單：

1. 前往**裝置 → 群組**。
2. 在管理群組結構中，選擇您要檢視其分配的發佈點的管理群組。
3. 點擊**發佈點**頁籤。
4. 使用**分配**按鈕新增管理群組的發佈點，或使用**取消分配**按鈕移除已指派的發佈點。

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。

要在分發點上啟用推入伺服器：

1. 點擊所需管理伺服器名稱旁邊的**設定**圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**發佈點**區段。
3. 點擊要在其上啟用推入伺服器的分發點的名稱。
   分發點內容視窗將開啟。
4. 在**一般**區段上啟用**執行推入伺服器**選項。
5. 在 **推入伺服器連接埠** 欄位中，鍵入連接埠編號。您可以指定任何未佔用連接埠的編號。
6. 在 **遠端主機位址** 欄位中，指定分發點裝置的 IP 位址或名稱。
7. 點擊**確定**按鈕。

推入伺服器將在所選分發點上啟用。

管理用戶端裝置上的協力廠商應用程式

本節說明卡巴斯基安全管理中心 Linux 功能如何管理在用戶端裝置上執行的協力廠商應用程式。

情境：應用程式管理

您可在使用者裝置上管理應用程式啟動。您可允許或封鎖要在受管理裝置上執行的應用程式。此功能會由應用程式控制元件執行。

應用程式控制元件適用於 Kaspersky Endpoint Security 11.2 for Linux 及更高版本。

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 政策已建立並啟動。

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。若您知道受管理裝置確切安裝的可執行檔，您可略過此階段。

   說明：取得並檢視儲存在用戶端裝置上的可執行檔清單

2. **針對在您組織中使用的應用程式建立應用程式類別**

   分析受管理裝置上儲存的可執行檔清單。根據分析，建立應用程式類別。建議您建立涵蓋您組織使用之應用程式標準集的「工作應用程式」類別。若不同的使用者群組在其工作中使用不同的應用程式集，則可針對各使用者群組建立獨立的應用程式類別。

   說明：建立含有手動新增內容的應用程式類別

3. **在 Kaspersky Endpoint Security for Linux 政策配置應用程式控制**

   使用您在先前階段已建立的應用程式類別在 Kaspersky Endpoint Security for Linux 政策中配置應用程式控制元件。

4. **確認應用程式控制組態**

   請確保您已完成以下項目：

   - 建立應用程式類別。
   - 使用應用程式類別配置應用程式控制。

結果

當情境完成時，受管理裝置上的應用程式啟動會受到控制。使用者僅可啟動組織中允許的這些應用程式，不可啟動被禁止的應用程式。

有關應用程式控制的詳細資訊，請參閱 Kaspersky Endpoint Security for Linux 線上說明。

關於應用程式控制

應用程式控制元件會監控使用者啟動應用程式的嘗試，並使用應用程式控制規則規管應用程式的啟動。

應用程式控制元件適用於 Kaspersky Endpoint Security 11.2 for Linux 及更高版本。

與任何應用程式控制規則不符的應用程式啟動的設定，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應用程式（除了封鎖規則中指定的應用程式），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應用程式（除了允許規則中指定的應用程式），則會使用此模式。

應用程式控制規則會透過應用程式類別執行。您建立定義特定條件的應用程式類別。在卡巴斯基安全管理中心Linux 中，您只能建立手動新增內容的類別.您會定義條件，例如檔案中繼資料、檔案雜湊碼、檔案憑證、KL 類別、檔案路徑，以在類別中包含可執行檔。

有關應用程式控制的詳細資訊，請參閱 Kaspersky Endpoint Security for Linux 線上說明。

取得並檢視儲存在用戶端裝置上的可執行檔清單

您可取得儲存在受管理裝置上的可執行檔清單。若要清查可執行檔，您必須建立清查工作。

清查可執行檔的功能適用於 Kaspersky Endpoint Security 11.2 for Linux 及更高版本。

要在用戶端裝置上為可執行檔建立清查工作：

1. 前往**裝置 → 工作**。
   工作清單隨即顯示。
2. 點擊**新增**按鈕。
   新增工作精靈啟動。遵照精靈的步驟操作。
3. 在**新工作**頁籤的**應用程式**下拉清單，選取 Kaspersky Endpoint Security for Linux。
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，點擊**完成**按鈕。

在新工作精靈完成後，**清單**工作或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。

有關清查工作的詳細說明，請參閱 Kaspersky Endpoint Security for Linux 線上說明。

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。

清查過程中，應用程式偵測以下格式的可執行檔：MZ、COM、PE、NE、SYS、CMD、BAT、PS1、JS、VBS、REG、MSI、CPL、DLL、JAR 和 HTML。

要檢視儲存在用戶端裝置的所有可執行檔清單：

在**操作 → 協力廠商應用程式**下拉清單中，選取**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。

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**操作 → 協力廠商應用程式**下拉清單中，選取**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。遵照精靈的步驟操作。
3. 在精靈的**選擇類別建立方法**頁面，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. 在精靈的**條件**頁面，點擊**新增**按鈕以新增條件準則以在建立類別中包含檔案。
5. 在**條件標準**頁面，選取要從清單建立類別的規則類型：

   - **從儲存區選擇憑證**

     如果選中此選項，則可以指定來自儲存空間的憑證。已按照指定的憑證簽章的可執行檔將被新增到使用者類別。

   - **指定應用程式路徑（支援遮罩）**

     如果選中此選項，您可以指定包含了要新增到自訂應用程式類別的可執行檔的用戶端裝置上的資料夾。

   - **卸除式磁碟機**

     如果選中此選項，您可以指定應用程式在其上執行的媒體類型（任意裝置或行動裝置）。在所選驅動類型上執行的應用程式被新增到使用者應用程式類別。

   - **雜湊、檔案內容或憑證**：

- **從可執行檔清單選擇**

  如果選中此選項，可以使用用戶端裝置上的可執行檔清單來選取可執行檔並將應用程式新增到類別。

- **從應用程式登錄資料選擇**

  若已選取此選項，會顯示應用程式登錄資料。您可從登錄資料選取應用程式，並指定以下檔案中繼資料：

  - 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。

- **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。計算的雜湊值資訊儲存在管理伺服器資料庫。雜湊值的儲存不顯著增加資料庫尺寸。

  SHA-256 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 SHA-256 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 **SHA-256** 核取方塊。
  - 僅當您使用 Kaspersky Endpoint Security for Windows 時選擇 **MD5 雜湊值** 核取方塊。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。中繼資料將會傳送至管理伺服器。包含相同中繼資料的可執行檔將新增至應用程式類別。

  憑證

  如果選中此選項，則可以指定來自儲存空間的憑證。已按照指定的憑證簽章的可執行檔將被新增到使用者類別。

- **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**

    您選擇要用於計算雜湊值的雜湊函數（MD5 或 SHA-256）。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。

選取的準則會新增至條件清單。

您可視需要新增所需數量的應用程式類別。

6. 在精靈的**排除**頁面精靈，點擊**新增**按鈕至限定條件準則，以從建立的類別排除檔案。

7. 在**條件標準**頁面，從清單選取規則類型，與您為類別建立選取規則類型的方式一樣。

當精靈結束時就會建立自訂應用程式類別。它顯示在應用程式類別清單中。當您設定應用程式控制時，您可使用建立的應用程式類別。

有關應用程式控制的詳細資訊，請參閱 Kaspersky Endpoint Security for Linux 線上說明 。

檢視應用程式類別清單

您可檢視已配置應用程式類別清單以及各應用程式類別的設定。

要檢視應用程式類別清單，

在**操作**頁籤的**協力廠商應用程式**下拉清單中，選取**應用程式類別**。

應用程式類別清單頁面隨即顯示。

若要檢視應用程式類別內容，

點擊應用程式類別的名稱。

應用程式類別的內容視窗開啟。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

延伸所有 | 折疊所有

當您在 Kaspersky Endpoint Security for Linux 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。
- **給管理員的應用程式啟動封鎖訊息**（*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. 前往**監控和報告 → 事件分類**。
   事件分類清單已顯示。
2. 選取事件分類來檢視與應用程式控制相關的事件並啟動此事件分類。
   若您尚未建立與應用程式控制相關的事件分類，您可選取並啟動預先定義的分類，例如**最近的事件**。
   事件清單隨即顯示。
3. 選取其中有您要新增至應用程式類別之可執行檔的事件，接著點擊**分配到類別**按鈕。
   新類別精靈啟動。使用**下一步**按鈕進行精靈。
4. 在精靈頁面上，指定相關設定：
   - 在**對事件相關可執行檔所採取的操作**區段，選取以下其中一個選項：
     - **新增到新的應用程式類別**

       如果您需要根據事件相關的可執行檔建立新的應用程式類別，請選取此選項。
       預設情況下已選定此選項。
       若您已選取此選項，請指定新類別名稱。

     - **新增到現有應用程式類別**

       如果您需要新增事件相關可執行檔至現有應用程式類別，請選取此選項。
       預設情況下未選定此選項。
       若您已選取此選項，請選取您要新增可執行檔且有手動新增內容的應用程式類別。

   - 在**規則類型**區段，選取以下其中一個選項：

- **新增到包含的規則**
- **新增到排除的規則**

- 在**用作條件的參數**區段，選取以下其中一個選項：
  - **憑證詳情（或沒有憑證的檔案的 SHA-256 雜湊）**

    檔案可能使用憑證簽署。多個檔案可能使用相同的憑證簽署。例如，相同應用程式的不同版本可能使用相同的憑證簽署，或者相同供應商的多個不同應用程式可能使用相同憑證簽署。當您選取憑證時，應用程式的多個版本或相同供應商的多個應用程式可能組成一個類別。

    每個檔案都有單獨的 SHA-256 雜湊。當您選取 SHA-256 雜湊時，僅一個對應的檔案，例如，定義的應用程式版本，組成類別。

    如果您要新增可執行檔的憑證詳情（或者無憑證檔案的 SHA-256 雜湊）到類別規則，請選取此選項。

    預設情況下已選定此選項。

  - **憑證詳情（沒有憑證的檔案將被略過）**

    檔案可能使用憑證簽署。多個檔案可能使用相同的憑證簽署。例如，相同應用程式的不同版本可能使用相同的憑證簽署，或者相同供應商的多個不同應用程式可能使用相同憑證簽署。當您選取憑證時，應用程式的多個版本或相同供應商的多個應用程式可能組成一個類別。

    如果您要新增可執行檔的憑證詳情到類別規則，請選取此選項。如果可執行檔沒有憑證，該檔案將被略過。該檔案的資訊將不被新增到類別。

  - **僅 SHA-256（沒有雜湊的檔案將被略過）**

    每個檔案都有單獨的 SHA-256 雜湊。當您選取 SHA-256 雜湊時，僅一個對應的檔案，例如，定義的應用程式版本，組成類別。

    如果您要僅新增可執行檔的 SHA-256 雜湊詳情，請選取此選項。

  - **僅 MD5（停產模式，僅對 Kaspersky Endpoint Security 10 Service Pack 1 版本）**

    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。

有關應用程式控制的詳細資訊，請參閱 Kaspersky Endpoint Security for Linux 線上說明。

監控和報告

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。

情境：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對其功能運作產生報告。

組織網路中的監控和報告分步驟進行：

1. **設定裝置狀態轉換**

   熟悉取決於特定條件的裝置狀態設定。透過變更這些設定，您可以變更帶有*嚴重*或*警告*嚴重等級的裝置數量。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：

   - 檢閱新裝置小工具
   - 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料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儀表板並加以檢閱
   - 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 14 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

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。

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

事件分類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 14 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分類。

通知

通知會警示您關於事件的資訊，並協助您透過執行建議動作或您認為適當的動作加速回應這些事件。

儀表板和小部件

本部分包含有關儀表板和儀表板提供的小部件的資訊。該部分包括有關如何管理小部件和配置小部件設定的說明。

使用儀表板

控製板透過對資訊進行圖形顯示來允許您監控您組織網路的安全趨勢。

控製板可在卡巴斯基安全管理中心 14 網頁主控台使用，請在**監控和報告**區段點擊**控制板**。

控製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 14 網頁主控台具有以下類別的預設部件集：

- **防護狀態**
- **佈署**
- **更新**
- **威脅統計資料**
- **其他**

一些部件具有帶連結的文字資訊。您可以透過點選連結檢視詳細資訊。

當配置控製板時，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

要新增工具到控製板：

1. 在主功能表中，轉至 **監控和報告 → 控制板**。
2. 點擊**新增或還原 Web 小部件**按鈕。
3. 在可用工具清單，選取您要新增到控製板的工具。
   工具按類別分組。要檢視包含在類別中的工具清單，點擊類別名稱旁邊的臂章圖示（ ）。
4. 點擊**新增**按鈕。

所選的工具被新增到控製板結尾。

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

要從控製板隱藏工具：

1. 在主功能表中，轉至 **監控和報告 → 控制板**。
2. 點擊您要隱藏的工具旁邊的**設定**圖示（⚙）。
3. 選取**隱藏 Web 小部件**。
4. 在開啟的**警告**視窗中，點擊**確定**按鈕。

所選工具被隱藏。稍後，您可以再次新增該工具到控製板。

移動儀表板上的小部件

要移動工具到控製板：

1. 在主功能表中，轉至 **監控和報告 → 控制板**。
2. 點擊您要移動的工具旁邊的**設定**圖示（⚙）。
3. 選取**移動**。
4. 點擊您要移動工具的地方。您僅可以選取其他工具。

所選工具的地方被清掃。

變更部件尺寸或樣子

對於顯示圖表的工具，您可以變更其展示–線條圖或線形圖。對於一些工具，您可以變更其大小：最小、中度或最大。

要變更工具展示：

1. 在主功能表中，轉至 **監控和報告 → 控制板**。
2. 點擊您要編輯的工具旁邊的**設定**圖示（⚙）。
3. 執行以下操作之一：
   - 若要顯示小工具作為條狀圖，請選取 **圖表類型：線條**。
   - 若要顯示小工具作為直線圖，請選取 **圖表類型：線形**。
   - 若要變更由小工具佔據的區域，請選取其中一個值：
     - **最小**
     - **最小（僅線條）**
     - **中度（餅圖）**
     - **中度（線條圖）**
     - **最大**

所選工具的展示被變更。

變更部件設定

要變更工具設定：

1. 在主功能表中，轉至 **監控和報告 → 控制板**。
2. 點擊您要變更的小工具旁邊的**設定**圖示（⚙）。
3. 選取**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**儲存變更。

所選工具的設定被變更。

設定集合取決於特定工具。以下是一些通用設定：

- **Web 小部件範圍**（小工具顯示資訊的物件集）—例如，管理群組或裝置分類。
- **選取工作**（小工具顯示資訊的工作）。
- **時間間隔**（小工具中顯示資訊的時間間隔）—介於兩個指定日期；從指定日期至當前日期；或從當前日期扣除目前日期的指定天數。
- **若指定以下條件，則設為"緊急"**與**若指定以下條件，則設為"警告"**（規判交通號誌燈號的規則）。

關於"僅儀表板"模式

你可以為不管理網路但希望在卡巴斯基安全管理中心中檢視網路防護統計資訊的員工（例如，高級經理）配置僅儀表板模式。當使用者啟用此模式時，只會向使用者顯示帶有一組預定義小工具的儀表板。因此，他或她可以監控小工具中指定的統計資訊，例如，所有受管理裝置的防護狀態、最近檢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 **一般功能中具有修改物件 ACL權限的使用者："使用者權限"**功能區域。

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**一般功能中有修改物件 ACL權限："使用者權限"**功能區域。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**一般功能中有讀取權限：基本功能**的功能區域。

> 如果在您的網路中安排了管理伺服器的層次結構，為了配置僅儀表板模式，請轉到伺服器，其中使用者帳戶可在 **使用者和角色 → 使用者** 部分中使用。它可以是主伺服器或實體從屬伺服器。無法在虛擬伺服器上調整模式。

若要配置僅儀表板模式：

1. 在主功能表中，轉至 **使用者和角色 → 使用者**。
2. 點擊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**儀表盤**標籤上您可以使用小工具執行與在 **監控和報告 → 控制板** 部分一樣的操作：
   - 新增小工具到儀表板。
   - 隱藏使用者不需要的小工具。
   - 移動小工具到特定的順序。
   - 變更小工具的大小或外觀。
   - 變更小工具設定。
6. 轉換切換按鈕以啟用**以僅儀表板模式顯示主控台**選項。

之後，只有儀表板可供使用者使用。他或她可以監控統計資料，但不能變更網路防護設定和儀表板外觀。由於為您顯示的儀表板與為使用者顯示的儀表板相同，您也無法變更儀表板。

如果您保持停用該選項，則會為使用者顯示主功能表，因此他或她可以在卡巴斯基安全管理中心中執行各種操作，包括變更安全設定和小工具。

7. 完成配置僅儀表板模式後點擊**儲存**按鈕。只有在那之後，準備好的儀表板才會顯示給使用者。

8. 如果使用者想要檢視受支援的卡巴斯基應用程式的統計資訊並且需要存取權限來執行此操作，請為使用者配置權限。之後，卡巴斯基應用程式資料將在這些應用程式的小工具中顯示給使用者。

現在使用者可以在自訂帳戶下登入卡巴斯基安全管理中心並在"僅儀表板"模式下監控網路防護統計資訊。

報告

本節介紹如何使用報告、管理自定義報告範本、使用報告範本產生新報告以及建立報告交付工作。

使用報告

報告功能允許您獲取您組織網路的詳細安全數字資訊、儲存該資訊到檔案、透過郵件傳送它和列印它。

報告可在卡巴斯基安全管理中心 14 網頁主控台的**監控和報告**區段，透過點擊**報告**取得。

預設下，報告包含 30 天內的資訊。

卡巴斯基安全管理中心 Linux 具有以下類別的預設報告集：

- **防護狀態**
- **佈署**
- **更新**
- **威脅統計資料**
- **其他**

您可以建立自訂報告範本、編輯報告範本和刪除它們。

您可以基於現有範本建立報告、匯出報告到檔案和建立報告傳送工作。

建立報告範本

要建立報告範本，請執行以下操作：

1. 在主功能表中，轉至 **監控和報告 → 報告**。

2. 點擊**新增**。
   程式將啟動"新報告範本精靈"。使用**下一步**按鈕進行精靈。

3. 在精靈的第一頁，輸入報告名稱並選取報告類型。

4. 在精靈的**範圍**頁面，選取根據此報告範本，其資料會顯示在報告中的用戶端裝置集（管理群組、裝置分類、選取的裝置，或所有網路裝置）。

5. 在精靈的**報告週期**頁面，指定報告期間。有以下可用值：

   - 在兩個指定日期之間
   - 從指定日期到報告建立日期
   - 從報告建立日期減去指定天數

   該頁對一些報告可能不顯示。

6. 點擊 **確定** 以關閉精靈。

7. 執行以下操作之一：

   - 點擊**儲存和執行**按鈕以儲存新報告範本並據此執行報告。
     報告範本被儲存。報告被生成。
   - 點擊**儲存**按鈕以儲存新報告範本精靈。
     報告範本被儲存。

您可以使用新範本來生成和檢視報告。

檢視和編輯報告範本內容

延伸所有 | 折疊所有

您可以檢視和編輯報告範本的基本內容，例如，報告範本名稱或顯示在報告中的欄位。

要檢視和編輯報告範本內容：

1. 在主功能表中，轉至 **監控和報告 → 報告**。
2. 選取您要檢視並編輯其內容的報告範本旁邊的核取方塊。
   或者，您可以先產生報告，然後點擊**編輯**按鈕。
3. 點擊**開啟報告範本內容**按鈕。
   編輯報告 <報告名稱>視窗會開啟，並含有所選的**一般**頁籤。
4. 編輯報告範本內容：
   - **一般**頁籤：
     - 報告範本名稱
     - **顯示項目的最大數量**

       如果啟用該選項，顯示在表格中的帶有詳細報告資料的項目數量不會超過指定值。

       報告項目首先根據指定在報告範本內容的**欄位 → 詳細資料欄位**區域的規則被儲存，然後僅第一個結果項目被儲存。帶有詳細報告資料的表頭展示顯示的項目數量和比對其他報告範本設定的可用項目總數。

       如果停用該選項，帶有詳細報告資料的表顯示所有可用項目。我們不建議您停用該選項。限制顯示的報告項目數量降低資料庫管理系統（DBMS）負載，也降低生成和匯出報告的所需時間。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，您的裝置可能在生成此報告時記憶體不夠，進而您將無法檢視報告。

       預設情況下已啟用該選項。預設值是 1000。
     - **群組**
       點擊**設定**按鈕以變更建立報告的用戶端裝置集。對於一些報告類型，按鈕可能不可用。實際設定取決於建立報告範本時指定的設定。
     - **時間間隔**
       點擊**設定**按鈕以修改報告時段。對於一些報告類型，按鈕可能不可用。有以下可用值：
       - 在兩個指定日期之間
       - 從指定日期到報告建立日期
       - 從報告建立日期減去指定天數
     - **包含來自從屬和虛擬管理伺服器的資料**

       如果啟用該選項，報告包含屬於建立範本的管理伺服器的次要和虛擬管理伺服器的資訊。

       如果您要僅從目前管理伺服器檢視資料，停用該選項。

       預設情況下已啟用該選項。
     - **嵌套等級**

       報告包含位於目前管理伺服器下小於或等於指定巢狀等級的次要和虛擬管理伺服器的資料。

       預設值是 1。如果您必須從樹中位於低等級的從屬管理伺服器接收資訊，您可能要變更該值。
     - **資料等待間隔（分鐘）**

       在產生報告之前，建立報告範本的管理伺服器等待從屬管理伺服器的資料指定分鐘數。如果在該時間段後未從從屬管理伺服器接收到資料，報告依然執行。除了實際資料，報告也會顯示從快取接收的資料（如果**從屬管理伺服器的記憶體暫存資料**選項已啟用），否則為 **N/A**（不可用）。

       預設值是 5 分鐘。
     - **從屬管理伺服器的快取資料**

次要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次要管理伺服器接收資料，報告顯示從快取接收的資料。資料傳輸到快取的日期也被顯示。

啟用該選項允許您檢視從屬管理伺服器資訊，即便即時資料無法被獲取。然而，所顯示資料可能過期。

預設情況下已停用該選項。

- **記憶體緩衝區更新頻率（小時）**

  次要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次要管理伺服器的資料。

  啟用該選項減慢報告生成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**儲存變更。
6. 點擊**關閉**按鈕（✕）關閉**編輯報告 <報告名稱>**視窗。

更新的報告範本顯示在報告範本清單。

匯出報告到檔案

您可以匯出報告到 XML、HTML 或 HTML 檔案。

要匯出報告到檔案：

1. 前往**監控和報告 → 報告**。
2. 選取您要匯出到檔案的報告旁邊的核取方塊。
3. 點擊**"匯出報告"**按鈕。
4. 在開啟的視窗中，變更**名稱**欄位的報告檔案名稱。預設下，檔案名稱與所選的報告範本名稱一致。
5. 選取報告檔案類型：XML、HTML 或 PDF。

   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。

6. 點擊**"匯出報告"**按鈕。

   所選格式的報告將被下載到您的裝置—到您裝置的預設資料夾—或您瀏覽器中開啟的標準**另存為**視窗將允許您儲存檔案到您想要的位置。

報告被儲存到檔案。

生成和瀏覽報告

要建立和瀏覽報告，請執行以下操作：

1. 在主功能表中，轉至 **監控和報告 → 報告**。

2. 點擊要用來建立報告的報告範本名稱。

會產生並顯示使用所選範本的報告。

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. 前往**監控和報告 → 報告**。
2. 【可選】選取您要建立報告傳送工作的報告範本旁邊的核取方塊。
3. 點擊**新報告傳送工作**按鈕。
4. "新增工作"精靈啟動。使用**下一步**按鈕進行精靈。
5. 在精靈的第一頁，輸入工作名稱。預設名稱為 **傳送報告（ <N> ）**，其中 <N> 是工作的序號。
6. 在精靈的工作設定頁面，指定以下設定：
   a. 要使用工作傳送的報告範本。如果您在步驟 2 選取了它們，請略過此步驟。
   b. 報告格式：HTML、XLS 或 PDF。
   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。
   d. 報告是否被儲存到資料夾，先前在該資料夾中儲存的報告是否被覆蓋，以及是否使用特定帳戶存取資料夾（對於共用資料夾）。
7. 若要在建立工作後修改其他工作設定，請精靈的**完成工作建立**頁面啟用**建立完成時開啟工作詳情**選項。
8. 點擊**建立**按鈕以建立工作並關閉精靈。
   報告傳送工作被建立。若您啟用**建立完成時開啟工作詳情**選項，工作設定視窗隨即開啟。

刪除報告範本

要刪除一個或幾個報告範本：

1. 在主功能表中，轉至 **監控和報告 → 報告**。
2. 選取您要刪除的報告範本旁邊的核取方塊。
3. 點擊**刪除**按鈕。
4. 在開啟的視窗中，點擊**確定**以確認您的選取。

所選報告範本被刪除。如果這些報告範本被包含在報告傳送工作中，它們也被從工作刪除。

事件和事件選擇

本節提供有關事件和事件選擇、卡巴斯基安全管理中心 Linux 元件中發生的事件類型以及管理頻繁事件封鎖的資訊。

使用事件分類

事件分類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 14 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分類。

事件分類可在卡巴斯基安全管理中心 14 網頁主控台使用，請在**監控和報告**區段點擊**事件分類**。

預設下，事件分類包含 7 天內的資訊。

卡巴斯基安全管理中心 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**
  - **資訊訊息**
- **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 **監控和報告 → 事件分類**。
2. 點擊**新增**。
3. 在開啟的**新事件分類**視窗，指定新事件分類的設定。在視窗中重複此操作。
4. 點擊**儲存**儲存變更。
   確認視窗開啟。
5. 若要檢視事件分類結果，請持續選取**轉到分類結果**核取方塊。
6. 點擊**儲存**以確認建立事件分類。

若您持續選取**轉到分類結果**核取方塊，會顯示事件分類結果。否則，新事件分類出現在事件分類清單。

編輯事件分類

要編輯事件分類：

1. 在主功能表中，轉至 **監控和報告 → 事件分類**。
2. 選取您要編輯的事件分類旁邊的核取方塊。
3. 點擊**內容**按鈕。
   事件分類設定視窗開啟。
4. 編輯事件分類內容。

   > 對於預定義的事件選擇，您只能編輯以下頁簽上的內容：**一般**（選擇名稱除外），**時間**，和 **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**儲存變更。

編輯的事件分類顯示在清單。

查看事件分類清單

要檢視事件分類，請執行以下操作：

1. 在主功能表中，轉至 **監控和報告 → 事件分類**。
2. 選取您要啟動的事件分類旁邊的核取方塊。
3. 執行以下操作之一：
   - 如果您要在事件分類結果中配置排序，做以下：
     a. 點擊**重新配置排序並啟動**按鈕。
     b. 在顯示的 **重新配置事件分類排序** 視窗中指定排序設定。
     c. 請點擊選項的名稱。
   - 或者，若您要在管理伺服器上排序好事件後檢視事件清單，請點擊選項名稱。

事件分類結果被顯示。

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。
   事件內容視窗隨即開啟。
3. 在顯示的視窗中，您可以做以下：
   - 檢視關於所選事件的資訊
   - 在事件分類結果中轉到上一個事件和下一個事件
   - 轉到發生事件的裝置
   - 轉到包含發生事件的裝置的管理群組
   - 對於工作相關事件，轉到工作內容

匯出事件到檔案

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。

3. 點擊**匯出至檔案**按鈕。

所選事件被匯出到檔案。

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**變更歷程**按鈕。

物件修訂歷程被開啟。

刪除事件

要刪除一個或幾個事件：

1. 啟動事件分類。
2. 選取所需事件旁邊的核取方塊。
3. 點擊**刪除**按鈕。

所選事件被刪除且無法還原。

刪除事件分類

您僅可以刪除使用者定義的事件分類。預定義事件分類無法被刪除。

要刪除一個或幾個事件分類：

1. 在主功能表中，轉至 **監控和報告 → 事件分類**。
2. 選取您要刪除的事件分類旁邊的核取方塊。
3. 點擊**刪除**。
4. 在開啟的視窗中，點擊**確定**按鈕。

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. 選取**裝置 → 政策和設定檔**。
2. 執行以下操作之一：
   - 若要設定網路代理事件或受管理 Kaspersky 應用程式事件的儲存時段，請點擊對應政策的名稱。
     政策內容頁面隨即開啟。
   - 若要設定管理伺服器事件，請在螢幕上方，點擊所需管理伺服器名稱旁邊的**設定**圖示（ ）。
     若您有給管理伺服器的政策，您可改為點擊此政策的名稱。

管理伺服器內容頁面（或管理伺服器政策內容頁面）隨即開啟。

3. 選取 **事件配置**頁籤。
   與**緊急**區段相關的事件類型清單隨即顯示。
4. 選取**功能失效**、**警告**或**資訊**區域。
5. 在右側面板中的事件類型清單中，點擊您要變更其儲存期限的事件的連結。
   在開啟的視窗的**事件註冊**區段，會啟用**儲存在管理伺服器資料庫上（天）**選項。
6. 在該開關按鈕下面的編輯方塊中，輸入儲存事件的天數。
7. 若您要在管理伺服器資料庫儲存事件，請停用**儲存在管理伺服器資料庫上（天）**選項。

   若您在管理伺服器內容視窗中設定管理伺服器事件，以及若事件設定在卡巴斯基安全管理中心 Linux 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。

8. 點擊**確定**。
   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。

事件類型

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 Linux 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。

事件類型描述的資料結構

對於每個事件類型，它的顯示名稱、ID、字母碼、描述和預設儲存期限被提供。

- **事件類型顯示名稱**。該文字當您配置事件時和它們發生時被顯示在卡巴斯基安全管理中心 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。
  您可以變更事件儲存期限：設定事件儲存期限

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。

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
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）。	180 天

			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。	
裝置已失去管理。	4111	KLSRV_HOST_OUT_CONTROL	如果受管理裝置在網路中可見，但一定時間未連線到管理伺服器，則該類型的事件發生。 找到什麼封鎖了裝置上網路代理的正常功能。可能的原因包括網路問題和從裝置移除網路代理。	180 天
裝置狀態為"緊急"。	4113	KLSRV_HOST_STATUS_CRITICAL	當受管理裝置被分配*緊急*狀態時，該類型的事件發生。您可設定裝置狀態要變更為*緊急*的條件。	180 天
金鑰檔案已新增到黑名單。	4124	KLSRV_LICENSE_BLACKLISTED	當 Kaspersky 已新增您使用的啟動碼或金鑰檔案到拒絕清單時，會發生該類型的事件。 聯絡技術支援獲得更多詳情。	180 天
產品授權即將到期。	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	當接近商業授權到期日時，就會發生此類事件。 卡巴斯基安全管理中心每天會檢查一次產品授權是否接近到期日。此類事件會在產品授權到期日期前 30 天、15 天、5 天和 1 天發布。無法變更此天數。如果管理伺服器在許可證到期日期前的指定日期關閉，則事件將在第二天發布。 當商業授權到期時，卡巴斯基安全管理中心 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。 • 如果您使用訂閱方案，請確保續訂該方案。無限制訂購如果已經預付給服務提供商了，則會在到期日自動續約。	180 天
憑證已到期。	4132	KLSRV_CERTIFICATE_EXPIRED	當行動裝置管理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。 您可以透過選取憑證發行設定中的**如果可能，自動重新發佈憑證**核取方塊來設定自動更新憑證。	180 天

管理伺服器功能失效事件

下表顯示具有**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。

管理伺服器功能失效事件

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
執行時錯誤。	4125	KLSRV_RUNTIME_ERROR	由於未知問題，該類型的事件發生。 多數情況下，這些是 DBMS 問題、網路問題和其他軟體和硬體問題。 事件詳情可以在事件描述中找到。	180 天
其中一個已授權應用程式群組已超過最大安裝數量。	4126	KLSRV_INVLICPROD_EXCEDED	管理伺服器定期產生該類型的事件（每小時）。如果在卡巴斯基安全管理中心 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
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 / 或金鑰是否被變更。 • 檢查網際網路連線，因為它可能是事件原因。遵照指示更新資料庫和軟體模組。	180 天

沒有剩餘硬碟空間。	4107	KLSRV_DISK_FULL	當安裝管理伺服器的裝置磁碟空間不足時，就會發生此類事件。 釋出裝置上的磁碟空間。	180 天
共用資料夾無法使用。	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	如果管理伺服器共用資料夾不可用，則該類型的事件發生。 您可以透過以下方式回應事件： • 檢查管理伺服器（共用資料夾所在位置）是否已開啟並可用。 • 檢查資料夾的使用者名稱和 / 或金鑰是否變更。 • 檢查網路連線。	180 天
管理伺服器資料庫無法使用。	4109	KLSRV_DATABASE_UNAVAILABLE	如果管理伺服器資料庫不可用則該類型的事件發生。 您可以透過以下方式回應事件： • 檢查安裝了 SQL Server 的遠端伺服器是否可用。 • 檢視 DBMS 記錄以發現管理伺服器資料庫不可用的原因。例如，因為維護，安裝了 SQL Server 的遠端伺服器可能不可用。	180 天

管理伺服器資料庫空間不足。	4110	KLSRV_DATABASE_FULL	當管理伺服器資料庫沒有剩餘空間時，該類型的事件發生。
			當管理伺服器的資料庫達到其容量，以及當不可能再往資料庫記錄時，管理伺服器不工作。
			以下是根據您使用的 DBMS，該事件的原因，以及到該事件的正確回應：
			• 您使用 SQL Server Express 版本 DBMS：
			  • 在 SQL Server Express 文件中，檢查您使用版本的資料庫大小限制。可能您的管理伺服器資料庫已超過了資料庫大小限制。
			  • 限制儲存在管理伺服器資料庫的事件數量。
			  • 在管理伺服器資料庫中有太多由應用程式控制元件傳送的事件。您可以變更關於管理伺服器資料庫中應用程式事件儲存的 Kaspersky Endpoint Security for Linux 政策設定。
			• 您使用 DBMS 而不是 SQL Server Express Edition：
			  • 不限制儲存在管理伺服器資料庫的事件數量。
			  • 降低儲存在管理伺服器資料庫的事件數量。
			在 DBMS 選項處檢視資訊。
				180 天

管理伺服器警告事件

下表顯示具有**警告**重要等級的卡巴斯基安全管理中心管理伺服器事件。

管理伺服器警告事件

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
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。	90 天

			• 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。	
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 14 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 14 網頁主控台將裝置自動從群組中刪除的時間間隔。	90 天
裝置名稱衝突。	4102	KLSRV_EVENT_HOSTS_CONFLICT	當管理伺服器將兩個或更多受管理裝置視為單一裝置時，會發生此類事件。 當複製的硬碟用在受管理裝置上進行軟體佈署，並且沒有將網路代理切換到參考裝置上的專用磁碟複製模式時，通常會發生這種情況。 為避免此問題，請在複製該裝置硬碟之前將網路代理切換到參考裝置上的磁碟複製模式。	90 天
裝置狀態為“警告”。	4114	KLSRV_HOST_STATUS_WARNING	當受管理裝置被分配 *警告* 狀態時，該類型的事件發生。您可設定裝置狀態要變更為 *警告* 的條件。	90 天
其中一個已授權應用程式群組總數即將超過最大安裝數量。	4127	KLSRV_INVLICPROD_FILLED	當已授權應用程式群組中包含的協力廠商應用程式的安裝數量達到產品授權金鑰屬性中指定之最大允許值的 90% 時，將發生此類事件。 您可以透過以下方式回應事件： • 如果某些受管理裝置上未使用協力廠商應用程式，請從這些裝置上刪除該應用程式。 • 如果您預計協力廠商應用程式的安裝數量將在不久的將來超過允許的最大值，請考慮預先獲取更多裝置的協力廠商授權。 您可以使用已授權應用程式群組的功能管理協力廠商應用程式的產品授權金鑰。	90 天
憑證已被請求。	4133	KLSRV_CERTIFICATE_REQUESTED	當無法自動重新發佈行動裝置管理憑證時，將發生此類事件。 以下可能是事件的原因和適當的回應： • 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
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
APNs 憑證已到期。	4135	KLSRV_APN_CERTIFICATE_EXPIRED	當 APNs 憑證過期時，會發生此類事件。 您需要手動續訂 APNs 憑證並將其安裝在 iOS MDM 伺服器上。	未儲存
APNs 憑證即將到期。	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	當 APNs 憑證剩餘時間不足 14 天時，就會發生此類事件。 當 APNs 憑證到期時，您需要手動續訂 APNs 憑證並將其安裝在 iOS MDM 伺服器上。 建議您在到期日之前安排續訂 APNs 憑證。	未儲存

傳送 FCM 訊息到行動裝置失敗。	4138	KLSRV_GCM_DEVICE_ERROR	當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
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
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
硬碟剩餘空間少。	4105	KLSRV_NO_SPACE_ON_VOLUMES	當安裝管理伺服器的裝置硬碟空間不足時，就會發生此類事件。 釋出裝置上的磁碟空間。	90 天
管理伺服器資料庫的剩餘空間少。	4106	KLSRV_NO_SPACE_IN_DATABASE	如果管理伺服器資料庫受限制則該類型的事件發生。如果您不糾正情況，管理伺服器資料庫就將達到其容量且管理伺服器將不工作。 以下是根據您使用的 DBMS，該事件的原因，以及到該事件的正確回應。 您使用 SQL Server Express 版本 DBMS： • 在 SQL Server Express 文件中，檢閱您使用版本的資料庫大小限制。可能您的管理伺服器資料庫即將超過資料庫大小限制。 • 限制儲存在管理伺服器資料庫的事件數量。 • 在管理伺服器資料庫中有太多由應用程式控制元件傳送的事件。您可以變更關於管理伺服器資料庫中應用程式事件儲存的 Kaspersky Endpoint Security for Linux 政策設定。 您使用 DBMS 而不是 SQL Server Express Edition： • 不限制儲存在管理伺服器資料庫的事件數量 • 降低儲存在管理伺服器資料庫的事件數量 在 DBMS 選項處檢視資訊。	90 天
連到從屬管理伺服器的連線已中斷。	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	當與次要管理伺服器的連線中斷時，會發生此類事件。 在安裝了次要管理伺服器的裝置上讀取卡巴斯基事件記錄，並據此做出回應。	90 天
連到主管理伺服器的連線已中斷。	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	當與主要管理伺服器的連線中斷時，會發生此類事件。	90 天

			在安裝了主要管理伺服器的裝置上讀取卡巴斯基事件記錄，並據此做出回應。	
已註冊 Kaspersky 軟體模組的新更新。	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	當管理伺服器為需要批准安裝的受管理裝置上安裝的 Kaspersky 軟體註冊新更新時，將發生此類事件。 使用卡巴斯基安全管理中心網頁主控台核准或拒絕更新。	90 天
超過資料庫中的事件數量限制，刪除事件開始。	4145	KLSRV_EVP_DB_TRUNCATING	當從管理伺服器資料庫刪除舊事件在管理伺服器資料庫達到容量後開始時，該類型的事件發生。 您可以透過以下方式回應事件： • 變更儲存在管理伺服器資料庫的事件數量上限 • 降低儲存在管理伺服器資料庫的事件數量	未儲存
超過資料庫中的事件數量限制，事件已被刪除。	4146	KLSRV_EVP_DB_TRUNCATED	當從管理伺服器資料庫刪除舊事件在管理伺服器資料庫達到容量後完成時，該類型的事件發生。 您可以透過以下方式回應事件： • 變更允許儲存在管理伺服器資料庫的事件數量上限 • 降低儲存在管理伺服器資料庫的事件數量	未儲存

管理伺服器資訊事件

下表顯示具有**資訊**重要等級的卡巴斯基安全管理中心管理伺服器事件。

管理伺服器資訊事件

事件類型顯示名稱	事件類型 ID	事件類型	預設儲存期限
產品授權金鑰的 90% 已經使用。	4097	KLSRV_EV_LICENSE_CHECK_90	30 天
已偵測到新裝置。	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 天
裝置已被自動新增到群組。	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 天
裝置已從群組中刪除：長時間在網路中不活動。	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 天
已授權應用程式群組之一的安裝即將超過限制（已經使用 95% 以上）。	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 天
找到了要傳送至 Kaspersky 以分析的檔案。	4131	KLSRV_APS_FILE_APPEARED	30 天
此行動裝置上的 FCM 實例 ID 已被變更。	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 天
更新被成功複製至指定的資料夾。	4122	KLSRV_UPD_REPL_OK	30 天
連到從屬管理伺服器的連線已建立。	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 天
連到主管理伺服器的連線已建立。	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 天
資料庫已更新。	4144	KLSRV_UPD_BASES_UPDATED	30 天
稽核：到管理伺服器的連線已建立。	4147	KLAUD_EV_SERVERCONNECT	30 天
稽核：物件已修改。	4148	KLAUD_EV_OBJECTMODIFY	30 天
稽核：物件狀態已修改。	4150	KLAUD_EV_TASK_STATE_CHANGED	30 天
稽核：群組設定已修改。	4149	KLAUD_EV_ADMGROUP_CHANGED	30 天
稽核: 連到管理伺服器的連線已終止。	4151	KLAUD_EV_SERVERDISCONNECT	30 天
稽核：物件內容已修改。	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 天
稽核：使用者權限已修改。	4153	KLAUD_EV_OBJECTACLMODIFIED	30 天

網路代理事件

該部分包含網路代理相關事件資訊。

網路代理警告事件

下表顯示具有**警告**嚴重等級的卡巴斯基安全管理中心 Linux 網路代理事件。

網路代理警告事件

事件類型顯示名稱	事件類型 ID	事件類型	預設儲存期限
發生了事件。	549	GNRL_EV_APP_INCIDENT_OCCURED	30 天

網路代理資訊事件

下表顯示具有**資訊**嚴重等級的卡巴斯基安全管理中心 Linux 網路代理事件。

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
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
裝置已被刪除。	7709	KLNAG_EV_DEVICE_REMOVE	30 天
已偵測到新裝置。	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 天
裝置已被授權。	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 天

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查看該事件是否存在於**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發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. 在應用程式主視窗，點擊所需管理伺服器名稱旁邊的**設定圖示**（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**封鎖頻繁事件**區段。
3. 在**封鎖頻繁事件**區段：
   - 如果要取消封鎖接收頻繁事件，請執行以下操作：
     a. 選取您要封鎖的頻繁事件並點擊**排除**按鈕。
     b. 點擊**"儲存"**按鈕。
   - 如果要封鎖接收頻繁事件：
     a. 選取您要封鎖的頻繁事件並點擊**封鎖**按鈕。

b. 點擊"**儲存**"按鈕。

管理伺服器會接收取消封鎖的頻繁事件，並且不會接收已封鎖的頻繁事件。

移除對頻發事件的封鎖

您可以刪除對頻繁事件的封鎖並開始接收它們，直到管理伺服器再次封鎖這些頻繁事件為止。

要移除對頻繁事件的封鎖：

1. 在應用程式主視窗，點擊所需管理伺服器名稱旁邊的**設定圖示**（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**封鎖頻繁事件**區段。
3. 在**封鎖頻繁事件**區段，選擇要為其移除封鎖的頻繁事件類型。
4. 點擊**移除封鎖**按鈕。

頻繁事件將從頻繁事件清單中移除。管理伺服器將接收此類型的事件。

在管理伺服器上的事件處理和儲存

關於程式和受管理裝置的操作事件資訊儲存在管理伺服器資料庫。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、裝置 OS 事件記錄和管理伺服器電腦 OS 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。

如果資料庫的事件數量達到管理員指定的最大值，程式刪除最舊的的事件並用新事件將其重寫。若管理伺服器刪除舊事件，則無法儲存新事件到資料庫。在此時間段內，拒絕事件的資訊被寫入卡巴斯基事件記錄。新事件被列隊，然後在刪除操作後被儲存到資料庫。

通知和裝置狀態

本節包含有關如何檢視通知、配置通知傳遞、使用裝置狀態和啟用變更裝置狀態的資訊。

使用通知

通知會警示您關於事件的資訊，並協助您透過執行建議動作或您認為適當的動作加速回應這些事件。

根據選取的通知方法，有以下類型的通知可用：

- 螢幕通知
- 透過簡訊通知
- 透過電子郵件通知
- 透過可執行檔或指令碼通知

螢幕通知

螢幕通知提醒您按照重要等級分組的事件（*緊急*、*警告*和*資訊*）。

螢幕通知可以有兩種狀態之一：

- *已檢視*。您已對通知執行了建議操作或您已手動為通知分配了該狀態。
- *未檢視*。您未對通知執行了建議操作或您未手動為通知分配了該狀態。

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查看通知：

- 在**監控和報告** 中 → **通知**區段。這裡，您可以檢視預定義類別的通知。
- 您可以開啟單獨的視窗。此種情況下，您可以標記通知為已檢視。
- 在 **監控和報告** 上的**所選嚴重等級的通知**小工具中 → **控制板**區段。在部件中，您可以僅檢視處在*嚴重*和*警告*重要性等級的事件通知。

您可以執行操作，例如，您可以回應事件。

要檢視預定義類別的通知：

1. 在主功能表中，轉至 **監控和報告** → **通知**。
   系統會選取左窗格中的**所有通知**類別，右窗格會顯示所有通知。
2. 在左側面板，選取類別之一：
   - **佈署**
   - **裝置**
   - **防護**
   - **更新**(這包含可以下載的 Kaspersky 應用程式通知和已下載的病毒資料庫更新通知)
   - **弱點利用防禦**
   - **管理伺服器**(這僅包含管理伺服器相關事件)
   - **有用連結** (這包含到 Kaspersky 資源的連結，例如 Kaspersky 技術支援、Kaspersky 論壇、產品授權續約頁面或 Kaspersky IT 百科全書)
   - **Kaspersky 新聞** (這包含 Kaspersky 應用程式發佈資訊)

   所選類別的通知清單被顯示。清單包含以下：

- 與通知主題相關的圖示：佈署（ ）、保護（ ）、更新（ ）、裝置管理（ ）、防止利用（ ）、管理伺服器（ ）。
- 通知重要性等級。以下重要性等級通知會顯示：**緊急通知** ( )、**警告通知** ( )、**資訊通知**。清單中的通知按重要性等級分組。
- **通知**.這包含通知敘述。
- **操作**.這包含建議您執行的快速操作連結。例如，通知點擊該連結，您可以轉到儲存區並安裝安全應用程式到裝置，或檢視裝置清單或事件清單。您為通知執行建議操作之後，該通知被分配*已檢視*狀態。
- **註冊的狀態**.這包含從通知被註冊到管理伺服器到現在為止過去的天數或小時數。

要按照重要性等級在單獨的視窗中檢視螢幕通知：

1. 在卡巴斯基安全管理中心 14 網頁主控台的右上角，點擊**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，通知會根據重要性等級分組：*緊急*、*警告*和*資訊*。
2. 選取 **系統**頁籤。
   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（ ）、防止利用（ ）、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**頁籤。

   *資訊*重要性等級通知清單被顯示。

   清單的組織會與**系統**頁籤上的清單相同（請參閱以上說明）。僅有的不同是沒有顏色標記。

您可以透過註冊在管理伺服器上的日期間隔來過濾通知。使用**顯示篩選器**核取方塊來管理篩選條件。

要在部件上檢視螢幕通知：

1. 在**控制板**區段上，選取**新增或還原 Web 小部件**。
2. 在開啟的視窗中，點擊**其他**類別，選取**所選嚴重等級的通知**小工具，接著點擊新增。

   小工具現在會顯示在**控制板**頁籤上。預設下，*嚴重*重要性等級的通知顯示在部件。

   您可以點擊部件上的**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（）、保護（）、更新（）、裝置管理（）、防止利用（）、管理伺服器（）。
- 通知敘述和建議操作的連結。您對通知執行建議操作之後，該通知會變成*已檢視*狀態。
- 從通知被註冊到管理伺服器到現在為止過去的天數或小時數。
- 到其他通知的連結。點擊此連結後，系統會將您轉移至**監控和報告**區段中**通知**區段的通知檢視畫面。

關於裝置狀態

卡巴斯基安全管理中心 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。在有些情況下，指派狀態給裝置時，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）。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，病毒掃描工作，且發現的病毒數量超過指定值。	大於 0。
即時防護不符合管理員的設定等級	裝置在網路中可見，但即時防護等級與管理員在裝置狀態條件中設定的等級不同。	• 已停止。 • 已暫停。 • 執行中。

病毒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，但病毒掃描工作在指定時間內未執行。條件僅套用到於 7 天之前或更早新增到管理伺服器資料庫的裝置。	多於1天。
資料庫已過期	裝置在網路中可見且安全應用程式已安裝到裝置，但病毒資料庫在指定時間內未在該裝置上更新。條件僅套用到於1天之前或更早新增到管理伺服器資料庫的裝置。	多於1天。
長時間未連線	網路代理已安裝到裝置，但由於裝置關閉，裝置在指定時間段內未連線到管理伺服器。	多於1天。
偵測到活動威脅	**活動威脅**資料夾中的未處理的物件的數量超過指定的值。	多於 0 個項目。
需要重新啟動	裝置在網路中可見，但應用程式基於所選原因之一在指定時間之前請求裝置重新啟動。	多於 0 分鐘。
安裝了不相容的應用程式	裝置在網路中可見，但透過網路代理執行的軟體清查在裝置上偵測到了不相容的應用程式。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
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。
偵測到未處理的事件	裝置上發現了一些未處理的事故。事件可以透過安裝在用戶端裝置上的受管理 Kaspersky 應用程式自動建立，也可以由管理員手動建立。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
應用程式定義的裝置狀態	裝置狀態由受管理應用程式定義。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
裝置磁碟空間不足	裝置剩餘磁碟空間少於指定值或裝置無法與管理伺服器同步。當裝置已與管理伺服器成功同步且裝置上的剩餘空間大於或等於指定值時，*緊急*或*警告*狀態被變更為*正常*狀態。	大於 0 MB
裝置已失去管理	在裝置發現過程中，裝置在網路中可見，但是超過三次嘗試與管理伺服器同步都失敗了。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
防護已停用	裝置在網路中可見，但裝置上的安全應用程式已被停用大於指定的時間段。	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。當指定條件滿足時，用戶端裝置被分配以下狀態之一：*緊急*或 *警告*。未滿足特定條件時，系統會為用戶端裝置指派*正常*狀態。

一個條件的不同值可對應於不同的狀態。例如，依預設，若**資料庫已過期**條件有**多於 3 天**的值，則用戶端裝置會被指派*警告*狀態，逾值為**多於 7 天**，則會指派*緊急*狀態。

如果您從以前的版本升級卡巴斯基安全管理中心 Linux，指定*緊急*或*警告*狀態的 **資料庫已過期** 條件的值不會改變。

當卡巴斯基安全管理中心 Linux 指派狀態給裝置時，對於有些條件（請參閱條件說明欄），系統會將能見度標記列入考量。例如，若受管理裝置因符合資料庫已過期條件而被指派*緊急*狀態，之後能見度標記也已針對該裝置設定，則裝置會被指派*正常*狀態。

設定裝置狀態轉換

您可變更條件以為裝置配置*緊急*或*警告*狀態。

要啟用變更裝置狀態到緊急：

1. 在主功能表中，轉至 **裝置 → 群組的階層**。
2. 在開啟的群組清單中，針對您要變更切換裝置狀態的群組，點擊有該群組名稱的連結。
3. 在開啟的工作內容視窗中，選取**裝置狀態**頁籤。
4. 在左方窗格中，選取**緊急**。
5. 在右方窗格中的**若指定以下條件，則設為"緊急"**區段，啟用將裝置切換為*緊急*狀態的條件。

   然而，您可以變更在父政策中未鎖定的設定。

6. 在清單中選取條件旁的選項按鈕。
7. 在清單左上角，點擊**編輯**按鈕。
8. 為所選條件設定所需的值。
   可以不為每個條件設定值。
9. 點擊**確定**。

未滿足特定條件時，系統會為受管理裝置配置*緊急*狀態。

要啟用變更裝置狀態到警告：

1. 在主功能表中，轉至 **裝置 → 群組的階層**。
2. 在開啟的群組清單中，針對您要變更切換裝置狀態的群組，點擊有該群組名稱的連結。
3. 在開啟的工作內容視窗中，選取**裝置狀態**頁籤。
4. 在左方窗格中，選取**警告**。
5. 在右方窗格中的**若指定以下條件，則設為"警告"**區段，啟用將裝置切換為*警告*狀態的條件。

   然而，您可以變更在父政策中未鎖定的設定。

6. 在清單中選取條件旁的選項按鈕。
7. 在清單左上角，點擊**編輯**按鈕。
8. 為所選條件設定所需的值。
   可以不為每個條件設定值。
9. 點擊**確定**。

未滿足特定條件時，系統會為受管理裝置配置*警告*狀態。

配置通知傳送

您可以配置發生在卡巴斯基安全管理中心 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. 在螢幕上方，點擊所需管理伺服器名稱旁邊的**設定**圖示（ ）。
   管理伺服器內容視窗會開啟，並含有所選的**一般**頁籤。
2. 點擊**通知**區段，並在右窗格選取您需要之通知方法的頁籤：

- **電子郵件**

  電子郵件標籤允許您透過電子郵件配置事件通知。

  在 **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保護措施。

  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保護與 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**寄件者郵件信箱：如果未指定該設定，則將使用收件者信箱。 警告：我們不建議您使用虛構郵件信箱。**欄位中，指定寄件者的電子郵件位址。如果您將該欄位置空，收件者信箱被使用。不建議使用虛假郵件信箱。

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（通知數量 / 分鐘數）。

- **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保護與 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**寄件者郵件信箱：如果未指定該設定，則將使用收件者信箱。 警告：我們不建議您使用虛構郵件信箱。**欄位中，指定寄件者的電子郵件位址。如果您將該欄位置空，收件者信箱被使用。不建議使用虛假郵件信箱。

在**SMS 訊息接收者電話號碼**欄位中，指定短信通知接收人的手機號碼。

通知訊息欄位中會包含事件發生時應用程式傳送的事件資訊標準文字。該文字可以包含替代參數，例如事件名稱、裝置名稱和網域名稱。

> 如果通知文字包含百分號 (%) 字元，您必須指定兩次以允許訊息傳送。範例，“CPU 負載是 100%”。

點擊**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（通知數量 / 分鐘數）。

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 **事件配置** 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 **監控和報告 → 事件分類**。
2. 點擊**最近事件**選擇名稱。

   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 上下載該測試病毒。

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佔位符。

敘述事件的佔位符

佔位符	佔位符敘述
%SEVERITY%	事件重要性等級
%COMPUTER%	發生事件的裝置的名稱
%DOMAIN%	網域
%EVENT%	事件
%DESCR%	事件敘述
%RISE_TIME%	建立時間
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	工作名稱
%KL_PRODUCT%	卡巴斯基安全管理中心 Linux 網路代理
%KL_VERSION%	網路代理版本號
%HOST_IP%	IP 位址
%HOST_CONN_IP%	電腦 IP 位址

例如：

事件通知由某個可執行檔（例如，script1.bat）發出，在該可執行檔中，將啟動具有 %COMPUTER% 佔位符的另一個可執行檔（例如，script2.bat）。當發生事件時，將在管理員的裝置上執行 script1.bat 檔案，而該檔案隨後執行具有 %COMPUTER% 佔位符的 script2.bat 檔案。管理員將接收到發生事件的裝置的名稱。

卡巴斯基公告

本節說明如何使用、設定和停用卡巴斯基公告。

關於卡巴斯基公告

卡巴斯基公告部分（**監控和報告 → 卡巴斯基公告**）透過提供與您的卡巴斯基安全管理中心版本和受管理裝置上安裝的受管理應用程式相關資訊，讓您隨時了解最新資訊。卡巴斯基安全管理中心會透過刪除過時的公告並新增資訊來定期更新此部分中的資訊。

卡巴斯基安全管理中心僅顯示與目前連線的管理伺服器和安裝在該管理伺服器的受管理裝置上的 Kaspersky 應用程式相關的 Kaspersky 公告。對於任何類型的管理伺服器（主要、次要或虛擬），公告會單獨顯示。

管理伺服器必須具有網際網路連線才能接收卡巴斯基公告。

公告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，卡巴斯基公告已啟用。如果您不想接收卡巴斯基公告，則可以停用此功能。

為了向您顯示與您的網路防護配置相對應的資訊，卡巴斯基安全管理中心將資料傳送到卡巴斯基雲端伺服器，並僅接收與網路中安裝的卡巴斯基應用程式有關的公告。可以傳送到伺服器的資料集在您安裝卡巴斯基安全管理中心管理伺服器時接受的最終使用者產品授權協議中有說明。

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 14 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"部分中點擊標籤以查看此公告。

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 **監控和報告 → 卡巴斯基公告**。
2. 點擊**設定**連結。
   隨即開啟"卡巴斯基公告設定"視窗。
3. 指定下列設定：
   - 選取您要檢視的公告嚴重等級。其他類別的公告將不會顯示。
   - 選擇通知標籤要顯示的位置。該標籤可以顯示在所有主控台部分，也可以顯示在**監控和報告**部分及其子部分。
4. 點擊**確定**按鈕。
   卡巴斯基公告設定已配置完成。

停用卡巴斯基公告

卡巴斯基公告部分（**監控和報告 → 卡巴斯基公告**）透過提供與您的卡巴斯基安全管理中心版本和受管理裝置上安裝的受管理應用程式相關資訊，讓您隨時了解最新資訊。如果您不想接收卡巴斯基公告，則可以停用此功能。

要停用卡巴斯基公告：

1. 在應用程式主視窗，點擊所需管理伺服器名稱旁邊的**設定圖示**（ ）。
   管理伺服器內容視窗將開啟。

2. 在**一般**頁籤，選取**卡巴斯基公告**部分。

3. 將切換按鈕切換到**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。

匯出到 SIEM 系統的事件

本節將介紹如何配置匯出事件到 SIEM 系統。

情境：設定事件匯出到 SIEM 系統

卡巴斯基安全管理中心 Linux 允許透過以下方法之一配置將事件匯出到 SIEM 系統：匯出到使用 Syslog 格式的任何 SIEM 系統或直接從卡巴斯基安全管理中心資料庫匯出事件到 SIEM 系統。完成此場景後，管理伺服器會自動將事件傳送到 SIEM 系統。

先決條件

在卡巴斯基安全管理中心 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場景的步驟。

將事件匯出到 SIEM 系統的過程包括以下步驟：

- **配置 SIEM 系統以接收來自卡巴斯基安全管理中心 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/IP、UDP 或 TLS over TCP 通訊協定
  - 使用從卡巴斯基安全管理中心資料庫直接匯出的事件（一組公共視圖被提供在卡巴斯基安全管理中心資料庫；您可以在 klakdb.chm 文件尋找這些公共視圖的敘述。）

結果

如果您選取了要匯出的事件，配置事件匯出到 SIEM 系統後，您可以查看匯出結果。

在您開始之前

延伸所有 | 折疊所有

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。

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。您可以匯出這些資訊到外部 SIEM 系統。匯出事件資訊到外部 SIEM 系統使 SIEM 系統管理員可以快速回應發生在受管理裝置或裝置群組上的安全系統事件。

事件類型

在卡巴斯基安全管理中心 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**事件配置**頁簽中檢視可以由應用程式生產的事件的完整清單。對於管理伺服器，您還可以在管理伺服器屬性中檢視事件清單。

事件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執行過程中發生了嚴重問題、錯誤或功能異常。
- *警告*是不緊急的事件，但是也指示了今後可能發生的潛在問題。如果在事件發生後應用程式可以被還原而不遺失資料或功能，則這些事件是警告等級。
- *資訊*事件用於提示成功完成操作、應用程式的正常功能或完成了某過程。

每個事件都有一個儲存期限，在這時間內您可以在卡巴斯基安全管理中心 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。

關於事件匯出

您可以將事件匯出用在處理組織和技術級別的安全問題的中心系統中，提供安全監控服務，以及從不同解決方案合併資訊。即是提供對網路硬體和應用程式生成的安全警告的即時分析的 SIEM 系統，或者安全操作中心 (SOC)。

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。

事件匯出的 Syslog 格式

您可以將 Syslog 格式的事件傳送到任何 SIEM 系統。使用 Syslog 格式，您可以轉發發生在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。當以 Syslog 格式匯出事件時，您可以精確選取轉發哪些事件種類到 SIEM 系統。

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**

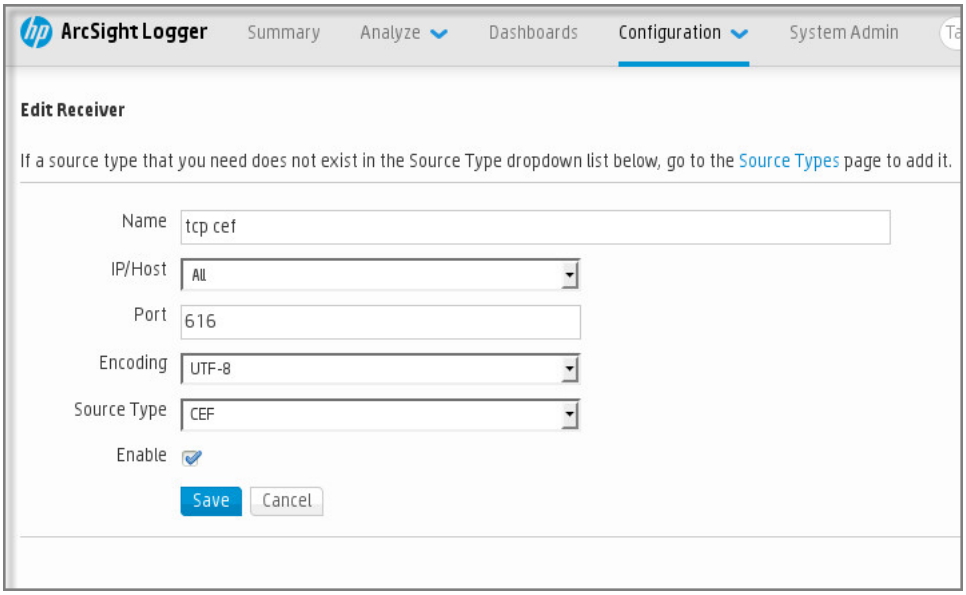
  指定連線到卡巴斯基安全管理中心 Linux 的連接埠號。此連接埠必須與您在配置 SIEM 系統期間在卡巴斯基安全管理中心 Linux 中指定的連接埠相同。

- **資料格式**

  指定 Syslog 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、參數等等。 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。

每個 SIEM 系統都有標準訊息解析器集合。Kaspersky 也為一些 SIEM 系統提供訊息解析器，例如 QRadar 和 ArcSight。您可以從對應的 SIEM 系統的網站下載這些訊息解析器。當設定接收者時，您可以選取使用標準訊息解析器或 Kaspersky 訊息解析器。

標記事件，將其以 Syslog 格式匯出到 SIEM 系統

本節介紹如何標記事件，以將用 Syslog 格式匯出到 SIEM 系統。

關於標記事件並將其以 Syslog 格式匯出到 SIEM 系統

在啟用自動匯出事件後，您必須選取將被匯出到外部 SIEM 系統的事件。

您可以根據以下條件之一，設定以 Syslog 格式將事件匯出到外部系統：

- 標記一般事件。如果您在政策、事件設定或在管理伺服器設定中，標記要匯出的事件，SIEM 系統將接收由特定政策管理的所有應用程式上發生的所選事件。如果匯出的事件在政策中被選中，您將不能為由該政策管理的個別應用程式重新定義所選事件。
- 標記受管理應用程式的事件。如果您在受管理裝置上為安裝的受管理應用程式標記要匯出的事件，SIEM 系統將僅接收發生在該應用程式中的事件。

將 Kaspersky 應用程式的事件標記為以 Syslog 格式匯出

如果您要匯出發生在特定受管理裝置上安裝的個別受管理應用程式中的事件，標記要在應用程式政策中匯出的時間。在這種情況下，標記的事件將從注冊範圍內的所有裝置中匯出。

若要為特定受管理應用程式標記要匯出的事件：

1. 在主功能表中，轉至 **裝置 → 政策和設定檔**。
2. 點擊您要爲其標記事件的應用程式的政策。
   政策設定視窗隨即開啟。
3. 前往**事件配置**區域。
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。

   您也可以在**事件註冊**部分中標記匯出到 SIEM 系統的事件，它可透過點擊事件連結開啟。

6. 一個複選標記 (✓) 出現在您標記為匯出到 SIEM 系統的一個或多個事件的欄的 **Syslog** 中。
7. 點擊**儲存**按鈕。

受管理應用程式中的標記事件已準備好匯出到 SIEM 系統。

您可以為特定受管理裝置標記要匯出到 SIEM 系統的事件。如果先前匯出的事件在應用程式的政策中標記過，您將不能為受管理的裝置重新定義標記的事件。

若要為受管理裝置標記要匯出的事件：

1. 在主功能表中，轉至 **裝置 → 受管理裝置**。
   受管理裝置清單隨即顯示。
2. 點擊所需裝置名稱在受管理裝置清單中的連結。
   所選裝置的內容視窗隨即顯示。
3. 前往**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. 前往**事件配置**區域。
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，如果配置了到 SIEM 系統的匯出，管理伺服器會向 SIEM 系統傳送標記的事件。

標記一般事件，將其以 Syslog 格式匯出

您可以使用 Syslog 格式標記管理伺服器將匯出到 SIEM 系統的一般事件。

標記一般事件以匯出到 SIEM 系統：

1. 執行以下操作之一：
   - 點擊所需管理伺服器名稱旁邊的**設定圖示**（ ）。
   - 在主功能表中，轉至**裝置 → 政策和設定檔**，然後點擊某個政策的連接。
2. 在開啟的視窗中，請前往**事件配置**頁籤。
3. 點擊**透過使用 Syslog 標記為匯出到 SIEM 系統**。

   此外，您可以在 **事件註冊** 部分中標記匯出到 SIEM 系統的事件，它可透過點擊事件連結開啟。
4. 一個複選標記 (✓) 出現在您標記為匯出到 SIEM 系統的一個或多個事件的欄的 **Syslog** 中。

從現在開始，如果配置了到 SIEM 系統的匯出，管理伺服器會向 SIEM 系統傳送標記的事件。

關於使用 Syslog 格式匯出事件

您可以使用 Syslog 格式匯出管理伺服器和受管理裝置上安裝的其他 Kaspersky 應用程式中發生的事件到 SIEM 系統。

Syslog 是訊息記錄協定的標準。它允許分離生成訊息的軟體、儲存訊息的系統和報告和分析訊息的軟體。每個訊息都帶有裝置代碼標籤，指示生成訊息的軟體類型，並被分配嚴重等級。

Syslog 格式由 Request for Comments (RFC) 文件定義，該文件由 Internet Engineering Task Force（網際網路標準）發佈。RFC 5424 標準用於從卡巴斯基安全管理中心 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。

若要在卡巴斯基安全管理中心 14 網頁主控台中配置匯出到 SIEM 系統：

1. 在**主控台設定**下拉清單中，選取**整合**。

   主控台設定視窗隨即開啟。
2. 選取 **整合**頁籤。
3. 在**整合** 頁簽，選取**SIEM**區段。
4. 透過點擊**設定**連結。

   匯出設定區段將開啟。
5. 在**匯出設定**區域指定以下設定：
   - **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/IP、UDP 或 TLS over TCP 通訊協定。

  如果您透過 TCP 通訊協定選取 TLS，則可以指定以下 TLS 設定：

  - **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) 接收帶有憑證清單的檔案，然後將該檔案上傳到卡巴斯基安全管理中心 Linux。卡巴斯基安全管理中心會檢查 SIEM 系統伺服器的憑證是否也由受信任的 CA 簽署。

      要新增受信任的憑證，請點擊**瀏覽 CA 憑證檔案**按鈕，然後上傳憑證。

    - **SHA 指紋**。您可以在卡巴斯基安全管理中心中指定 SIEM 系統憑證的 SHA-1 指紋。要新增 SHA-1 指紋，請將其輸入**指紋**欄位，然後點擊**新增**按鈕。

    透過使用**新增用戶端身分驗證**設定，您可以產生憑證來驗證卡巴斯基安全管理中心。因此，您將使用卡巴斯基安全管理中心發佈的自簽章憑證。在此情況下，您可以同時使用受信任的憑證和 SHA 指紋來驗證 SIEM 系統伺服器。

  - **新增主體名稱/主體別名**

    主體名稱是接收憑證的網域。如果 SIEM 系統伺服器的網域與 SIEM 系統伺服器憑證的主體名稱不符，卡巴斯基安全管理中心 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**新增主體名稱/主體別名**欄位中指定主體名稱。如果任何指定的主體名稱與 SIEM 系統憑證的主體名稱匹配，卡巴斯基安全管理中心 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**.將帶有憑證的檔案上傳到**包含憑證的檔案**欄位，將帶有私密金鑰的檔案上傳到**包含金鑰的檔案**欄位。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。檔案上傳後，在**密碼或者憑證驗證**欄位中指定解碼私密金鑰的密碼。如果未編碼私密金鑰未編碼，則密碼可以為空值。

    - **生產金鑰**.您可以在卡巴斯基安全管理中心中產生自簽章憑證。結果，卡巴斯基安全管理中心 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。

6. 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. 透過點擊**設定匯出開始日期**連結。

   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。

7. 將選項切換到 **自動匯出事件至 SIEM 系統資料庫 已啟用** 位置。

8. 點擊**儲存**按鈕。

匯出到 SIEM 系統已配置。從現在開始，如果您在 SIEM 系統中配置了事件接收，管理伺服器將匯出標記的事件到 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。

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 實用程式建立 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 實用程式建立 SQL 查詢

該部分敘述了如何下載和使用 klsql2 實用程式，以及如何使用該實用程式建立 SQL 查詢。當您使用 klsql2 實用程式建立 SQL 查詢時，您不必提供資料庫名稱和存取參數，因為查詢直接定位卡巴斯基安全管理中心 Linux 公共視圖。

要下載和使用 klsql2 實用程式：

1. 從 Kaspersky 網站下載 klsql2 實用程式。
2. 複製和解壓下載的 klsql2.zip 檔案到卡巴斯基安全管理中心 Linux 管理伺服器裝置的任意資料夾。
   klsql2.zip 套件包含以下檔案：
   - klsql2.exe
   - src.sql
   - start.cmd
3. 在任意文字編輯器中開啟 src.sql。
4. 在 src.sql 檔案中，鍵入所需的 SQL 查詢，然後儲存該檔案。
5. 在卡巴斯基安全管理中心 Linux 管理伺服器裝置上，在命令列，輸入以下指令以從 src.sql 檔案執行 SQL 查詢並儲存結果到 result.xml 檔案：
   ```
   klsql2 -i src.sql -o result.xml
   ```
6. 開啟新建立的 result.xml 檔案以檢視查詢結果。

您可以編輯 src.sql 檔案並建立到公共視圖的任意查詢。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 實用程式建立。

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，最近的事件最先顯示。

例如：

```
SELECT
e.nId,                                                  /* 事件標識 */
e.tmRiseTime,                                           /* 事件發生的時間 */
e.strEventType,                                         /* 事件類型的內部名稱 */
e.wstrEventTypeDisplayName,                             /* 事件的顯示名稱 */
e.wstrDescription,                                      /* 事件的顯示敘述 */
e.wstrGroupName,                                        /* 事件所在的群組名稱 */
h.wstrDisplayName,                                      /* 發生事件的裝置的顯示名稱 */
CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.'+
CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.'+
CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.'+
CAST(((h.nIp) & 255) AS varchar(4)) as strIp            /* 發生事件的裝置的 IP 位址 */
FROM v_akpub_ev_event e
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

檢視卡巴斯基安全管理中心 Linux 資料庫名稱

如果您要透過 SQL Server、MySQL 或 MariaDB 資料庫管理工具存取卡巴斯基安全管理中心 Linux ，您必須知道資料庫的名稱以便從您的 SQL 指令碼編輯器連線。

要檢視卡巴斯基安全管理中心 Linux 資料庫名稱：

1. 點擊所需管理伺服器名稱旁邊的**設定**圖示（ ）。
   管理伺服器內容視窗將開啟。

2. 在**一般**頁籤，然後選取**目前資料庫詳情**區段。

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。

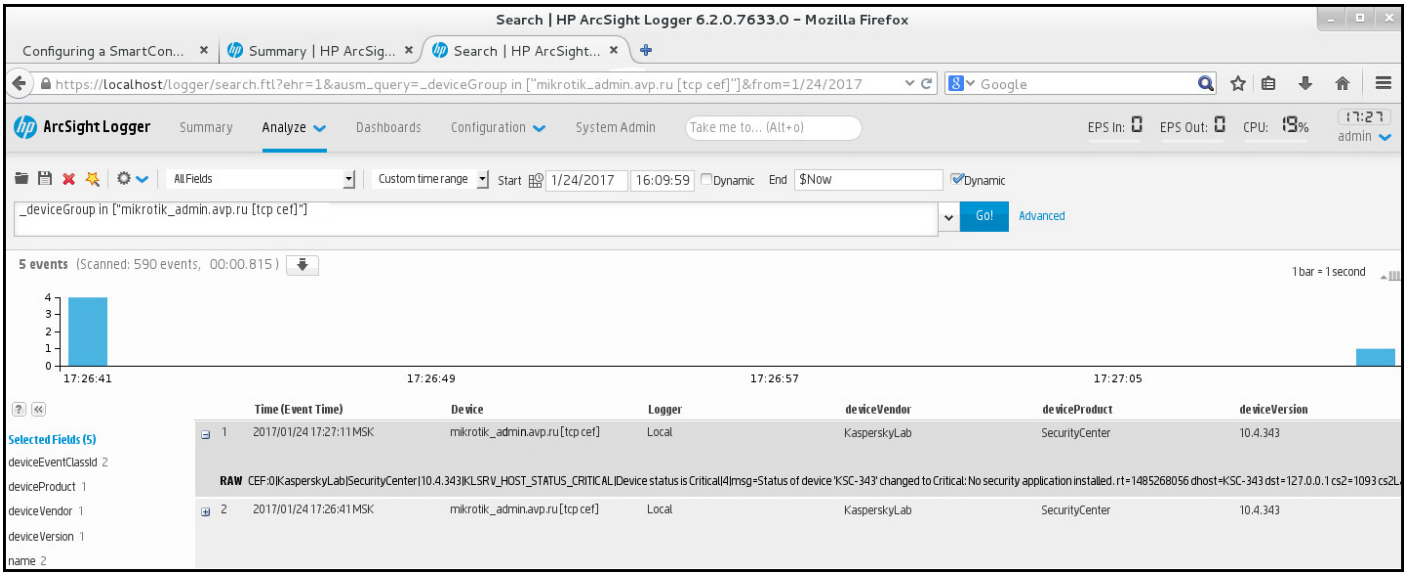
檢視匯出結果

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，第一個事件是關鍵的管理伺服器事件："*裝置狀態為緊急*"。

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

裝置分類

*裝置分類*是根據特定條件篩選裝置的工具。您可以使用裝置分類管理幾個裝置：例如，檢視僅檢視這些裝置的報告或移動所有這些裝置到其他群組。

卡巴斯基安全管理中心提供大範圍的*預先定義分類*（例如，**處於"緊急"狀態的裝置**，**防護已停用**，**偵測到活動威脅**）。預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。

要檢視裝置分類，請執行以下操作：

1. 在功能表中，轉至 **裝置 → 裝置分類** 要么 **發現和佈署 → 裝置分類** 區域。
2. 在選項清單中，點擊相關選項的名稱。

隨即顯示裝置選項結果。

建立裝置分類

要建立裝置分類，請執行以下操作：

1. 在主功能表中，轉至 **裝置 → 裝置分類**。
   裝置選項清單頁面隨即顯示。
2. 點擊**新增**按鈕。
   裝置分類設定視窗隨即開啟。
3. 輸入新選項的名稱。
4. 指定要包括在裝置選項中的裝置類型。

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

延伸所有 | 折疊所有

要配置裝置分類：

1. 前往**裝置 → 裝置分類**。
   裝置選項清單頁面隨即顯示。
2. 點擊使用者定義的相關裝置選項。
   裝置分類設定視窗隨即開啟。
3. 在**一般**頁籤，指定包含裝置到該分類必須符合的條件。
4. 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：選取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

> 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。
> 預設情況下已停用該選項。

網路

在**網路**區域，您可以指定依據網路資料裝置納入分類的標準：

- **裝置名稱或 IP 位址**
- **Windows 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。

- **敘述**

  > 裝置內容視窗中的文字：在**一般**區域的**敘述**欄位。
  > 您可以使用以下特徵說明**敘述**欄位中的文字：
  > - 在單詞中：
  >   - *****。用任意數量的字元更換任何字串。
  >
  > **例如**：
  > 要敘述單詞 **Server** 或 **Server's**，您可以輸入 **Server***。
  >
  > - **?.**更換任意單個字元。
  >
  > **例如**：

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。

標籤

在**標籤**區域中，您可以根據先前新增到受管理裝置的敘述的關鍵字（標籤）設定將裝置納入分類的標準：

- **如果有至少一個指定的標籤符合則套用**

  如果啟用此選項，搜尋結果將顯示包含帶有所選標籤的敘述的裝置。
  如果停用此選項，搜尋結果將僅顯示包含帶有所有標籤的敘述的裝置。
  預設情況下已停用該選項。

- **必須包含標籤**

  如果選取了該選項，搜尋結果將顯示帶有包含了所選標籤的敘述的裝置。要尋找裝置，您可以使用星號，它表示任何字元長度的字串。
  預設情況下已選定此選項。

- **必須排除標籤**

  如果選取了該選項，搜尋結果將顯示不帶有包含了所選標籤的敘述的裝置。要尋找裝置，您可以使用星號，它表示任何字元長度的字串。

網路活動

在**網路活動**區域，您可以根據網路活動指定將裝置納入分類的標準：

- **該裝置是發佈點**

  在下拉清單中，可設定執行搜尋時在分類中包括裝置的標準：
  - **是**.選取範圍將包括充當發佈點的裝置。
  - **否**.分類不包含作為發佈點的裝置。
  - **未選取值**。將不套用標準。

- **不斷開與管理伺服器的連線**

  在下拉清單中，可設定執行搜尋時在分類中包括裝置的標準：
  - **已啟用**.分類將包含已選取**不斷開與管理伺服器的連線**核取方塊的裝置。
  - **已停用**.分類將包含未選取**不斷開與管理伺服器的連線**核取方塊的裝置。
  - **未選取值**。將不套用標準。

- **連線設定檔已轉換**

  在下拉清單中，可設定執行搜尋時在分類中包括裝置的標準：
  - **是**.該分類將包含連線設定檔轉換後連線到管理伺服器的裝置。
  - **否**.該分類將不包含連線設定檔轉換後連線到管理伺服器的裝置。
  - **未選取值**。將不套用標準。

- **上一次連線到管理伺服器**

  您可使用此方塊設定按上一次連線到管理伺服器的時間搜尋裝置的標準。

  如果選取該方塊，則在輸入欄位中，您可以指定在用戶端裝置上安裝的網路代理和管理伺服器之間建立上一次連線的時間間隔（日期和時間）。選取將包括位於指定間隔的裝置。

  如果清除此方塊，則將不會套用標準。

  預設情況下已清空此方塊。

- **網路輪詢時偵測到新裝置**

  搜尋最近幾天透過網路輪詢偵測到的新裝置。

  如果選取此核取方塊，分類將只包括在**偵測週期（天）**欄位中指定的天數內透過裝置發現偵測到的新裝置。

  如果停用此選項，分類將包括透過裝置發現偵測到的所有裝置。

  預設情況下已停用該選項。

- **裝置可見**

  在下拉清單中，可設定執行搜尋時在分類中包括裝置的標準：
  - **是**.程式在分類中包括網路中目前可見的裝置。
  - **否**.程式在分類中包括網路中目前不顯示的裝置。
  - **未選取值**。將不套用標準。

應用程式

在**應用程式**區域中，您可以根據所選的受管理應用程式設定將裝置納入分類的標準：

- **應用程式名稱**

  在下拉清單中，可設定按 Kaspersky 應用程式名稱執行搜尋時在分類中包括裝置的標準。

  清單僅提供管理員工作站上已安裝管理外掛程式的應用程式的名稱。

  如果未選取任何應用程式，則將不會套用該標準。

- **應用程式版本**

  在輸入欄位，可設定按 Kaspersky 應用程式版本號執行搜尋時在分類中包括裝置的標準。

  如果未指定版本號，則將不會套用該標準。

- **重大更新名稱**

在輸入欄位中，可設定按應用程式名稱或更新套件編號執行搜尋時在分類中包括裝置的標準。
如果欄位留空，則將不會套用該標準。

- **上一次模組更新**

  您可以使用此選項來設定按這些裝置上安裝的程式模組上次更新的時間搜尋裝置的標準。
  如果選中此方塊，則您可以在輸入欄位中指定執行這些裝置上安裝的程式模組的上一次更新的時間間隔（日期和時間）。
  如果清除此方塊，則將不會套用標準。
  預設情況下已清空此方塊。

- **裝置透過卡巴斯基安全管理中心 14 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。

作業系統

在**作業系統**區域，您可以根據作業系統指定將裝置納入分類的標準。

- **作業系統版本**

  如果選中該方塊，您可以從清單中選取一個作業系統。安裝了指定作業系統的裝置會包含在搜尋結果中。

- **作業系統 bit 大小**

  在該下拉清單中可選取作業系統的架構，這將決定將移動規則套用到裝置（**未知**、**x86**、**AMD64** 或 **IA64**）的方式。預設情況下，不選取清單中的任何選項，這樣就不會對作業系統的架構進行定義。

- **作業系統服務套件版本**

  在該欄位中，可以指定作業系統的更新套件版本（採用 *X.Y* 格式），這將決定將移動規則套用到裝置的方式。預設情況下，不指定版本值。

- **作業系統版本**

  該設定僅套用到 Windows 作業系統。

  作業系統版本號。您可以指定所選作業系統是否必須具有相等、更早或更晚的版本號。您也可以設定對所有版本號的搜尋，除了指定的值。

- **作業系統發佈 ID**

該設定僅套用到 Windows 作業系統。

作業系統發佈 ID。您可以指定所選作業系統是否必須具有相等、更早或更晚的發佈 ID。您也可以設定對所有發佈 ID 的搜尋，除了指定的值。

裝置狀態

在**裝置狀態**區域，您可以根據受管理應用程式的裝置狀態的敘述設定將裝置納入分類的標準：

- **裝置狀態**

  在該下拉清單中，您可以選取下列裝置狀態之一：*確定*"*緊急*"、"*警告*"。

- **裝置狀態敘述**

  在該欄位中，您可以選中條件旁邊的方塊，這些條件如果被滿足，程式會為裝置分配下列狀態之一："*確定*"，"*緊急*"，"*警告*"。

- **應用程式定義的裝置狀態**

  您可以在該下拉清單中選取即時防護狀態。具有指定即時防護狀態的裝置將被包括在選取範圍中。

防護元件

在**防護元件**區域，您可以根據防護狀態設定將裝置納入分類的標準：

- **資料庫發佈日期**

  如果啟用此選項，您可以按病毒資料庫發佈日期搜尋用戶端裝置。在該輸入欄位中，您可以設定執行搜尋的時間間隔。
  預設情況下已停用該選項。

- **上一次掃描**

  如果啟用此選項，您可以按上次病毒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病毒掃描的時段。
  預設情況下已停用該選項。

- **偵測到的威脅總數**

  如果啟用此選項，您可以依據發現的病毒數量來搜尋用戶端裝置。在輸入欄位中，您可以設定發現病毒總數的上限值和下限值。
  預設情況下已停用該選項。

應用程式登錄資料

在**應用程式登錄資料**區域，您可以根據已安裝的應用程式設定搜尋裝置的標準：

- **應用程式名稱**

  在該下拉清單中，您可以選取應用程式。安裝有指定應用程式的裝置將包括在選取範圍中。

- **應用程式版本**

  在該輸入欄位中，您可以指定選定應用程式的版本。

- **供應商**

在該下拉清單中，您可以選取已安裝應用程式的生產商。

- **應用程式狀態**

  在該下拉清單中，您可以選取應用程式的狀態（*已安裝*、*未安裝*）。已安裝或未安裝指定應用程式的裝置，取決於所選狀態，將被包含在分類。

- **根據更新尋找**

  如果啟用此選項，則搜尋操作將使用相關裝置內應用程式更新的有關資訊來執行。選取核取方塊後，**應用程式名稱**、**應用程式版本**與**應用程式狀態**欄位會各自變成**更新名稱**、**更新版本**和**狀態**。
  預設情況下已停用該選項。

- **不相容的安全應用程式名稱**

  在該下拉清單中，您可以選取協力廠商安全應用程式。在搜尋過程中，安裝有指定程式的裝置將包括在選取範圍中。

- **應用程式標籤**

  在該下拉清單中，您可以選取應用程式標籤。所有安裝了敘述中帶有所選標籤的應用程式的裝置都被包含在裝置分類。

- **套用到沒有指定標籤的裝置**

  如果啟用此選項，分類將包含未帶有所選標籤的敘述的裝置。

  如果停用該選項，則不套用標準。
  預設情況下已停用該選項。

硬體登錄資料

在**硬體登錄資料**區域，您可以根據所安裝的硬體設定將裝置納入分類的標準：

- **裝置**

  在該下拉清單中，您可以選取單元類型。所有帶有該單元的裝置被包含在搜尋結果。
  該欄位支援完整文字搜尋。

- **供應商**

  在該下拉清單中，您可以選取單元生產商的名稱。所有帶有該單元的裝置被包含在搜尋結果。
  該欄位支援完整文字搜尋。

- **裝置名稱**

  具有指定名稱的裝置將包括在該分類中。

- **敘述**

  裝置或硬體單元的敘述。帶有該欄位中指定的敘述的裝置將包括在分類範圍內。
  可在裝置的內容視窗輸入任何格式的裝置敘述。該欄位支援完整文字搜尋。

- **裝置製造商**

  裝置製造商的名稱。被指定生產商製造的的裝置將包括在分類範圍內。
  您可以在裝置的內容視窗中輸入製造商的名稱。

- **序號**

  帶該欄位中指定序號的所有硬體裝置將包括在該分類中。

- **清單號**

  帶有該欄位中指定的清單編號的裝置將包括在選取範圍內。

- **使用者**

  該欄位中指定使用者的所有硬體裝置都將包括在該分類中。

- **位置**

  裝置或硬體單元的位置（例如，在總部或分公司）。在該欄位中指定的位置佈署的電腦或其他裝置將包括在該分類中。
  您可以在該裝置的內容視窗中以任何格式敘述裝置的位置。

- **CPU 頻率 (MHz)**

  CPU 的頻率範圍。CPU 與這些輸入欄位（含）中頻率範圍比對的裝置將包括在分類範圍內。

- **虛擬 CPU 核心**

  CPU 中虛擬內核的數量範圍。CPU 與這些輸入欄位（含）中範圍比對的裝置將包括在分類範圍內。

- **硬碟磁區 (GB)**

  裝置硬碟容量值的範圍。硬碟與這些輸入欄位（含）中範圍比對的裝置將包括在分類範圍內。

- **記憶體大小 (MB)**

  裝置 RAM 大小的值的範圍。RAM 與這些輸入欄位（含）中範圍比對的裝置將包括在分類範圍內。

虛擬機

在**虛擬機**區域中，您可以根據它們是否是虛擬機或虛擬桌面基礎架構 (VDI) 的一部分來指定將裝置納入分類的標準：

- **這是一台虛擬機**

  在此下拉清單中，您可以選取以下選項：
  - **不重要**.
  - **否**.搜尋不是虛擬機的裝置。
  - **是**.搜尋虛擬機裝置。

- **虛擬機類型**

  在該下拉清單中，您可以選取虛擬機製造商。
  若在**這是一台虛擬機**下清單中選取**是**或**不重要**值，則可使用此下拉清單。

- **虛擬桌面基礎架構的一部分**

  在此下拉清單中，您可以選取以下選項：
  - **不重要**.
  - **否**.尋找不是虛擬桌面基礎架構一部分的裝置。

- **是**,搜尋屬於虛擬桌面基礎架構 (VDI) 一部分的裝置。

使用者

在**使用者**區域中，您可以根據登入到作業系統的使用者帳戶設定將裝置納入分類的標準。

- **最後一次登入系統的使用者**

  如果啟用此選項，按一下**瀏覽**按鈕可以指定使用者帳戶。搜尋結果包含其上一次登入使用者為指定使用者的裝置。

- **登入系統至少一次的使用者**

  如果啟用此選項，按一下**瀏覽**按鈕可以指定使用者帳戶。搜尋結果包含指定使用者至少登入一次的裝置。

影響受管理應用程式狀態的問題

在**影響受管理應用程式狀態的問題**區域，您可以根據由受管理應用程式偵測到的可能問題清單指定將裝置納入分類的標準。如果至少一個您選取的問題存在於裝置，裝置將被包含到分類。當您選取幾個應用程式的問題時，您可以選取在所有清單中自動選取該問題。

裝置狀態敘述

您可以選取受管理應用程式狀態敘述的核取方塊；接收這些狀態時，裝置將被包含在分類。當您選取幾個應用程式的狀態時，您可以選取在所有清單中自動選取該狀態。

受管理應用程式元件的狀態

在**受管理應用程式元件的狀態**區域中，您可以根據受管理應用程式元件狀態設定將裝置納入分類的標準：

- **資料洩漏防護狀態**

  根據資料外洩防護的狀態搜尋裝置（*裝置上無資料*, *已停止*, *正在啟動*, *已暫停*, *執行中*, *失敗*）。

- **協作伺服器防護狀態**

  根據伺服器協作防護狀態搜尋裝置（*裝置上無資料*, *已停止*、*正在啟動*、*已暫停*, *執行中*、*失敗*）。

- **郵件伺服器的病毒防護狀態**

  根據郵件伺服器防護狀態搜尋裝置（*裝置上無資料*、*已停止*、*正在啟動*、*已暫停*、*執行中*、*失敗*）。

- **端點感應器狀態**

  根據端點感應器元件狀態搜尋裝置（*裝置上無資料*、*已停止*、*正在啟動*、*已暫停*、*執行中失敗*）。

應用程式元件

該區域包含了在管理主控台中安裝了管理外掛程式的這些應用程式的元件清單。

在**應用程式元件**區域中，您可以根據所選應用程式元件的狀態和版本編號指定將裝置納入分類的標準：

- **狀態**

  根據應用程式傳送到管理伺服器的元件狀態搜尋裝置。您可以選取以下狀態之一：*沒有來自裝置的資料*、*停止*、*開始*、*暫停*、*跑步*、*故障*，或者*未安裝*。如果安裝在受管理裝置上的應用程式的所選元件具有指定狀態，裝置被包含到裝置分類。

  由應用程式傳送的狀態：

- *正在啟動* - 元件處於初始化處理程序中。
- *執行中* - 元件被啟用且在正常工作。
- *已暫停* - 元件被暫停，例如，在使用者在受管理應用程式上停止了防護後。
- *故障* - 元件操作中發生錯誤。
- *已停止* - 元件被停用且不在工作。
- *未安裝* - 當設定應用程式自訂安裝時，使用者未選取該元件以安裝。

不同於其他狀態，*裝置上無資料*狀態不由應用程式傳送。該選項顯示應用程式沒有所選元件狀態的資訊。例如，這可能發生在所選元件不屬於任何在裝置上安裝的應用程式時，或裝置關閉時。

- **版本**

根據您在清單中選取的版本號搜尋裝置。您可以輸入版本號，例如 `3.4.1.0`，然後指定所選元件是否必須具有相同、更早或更新版本。您也可以設定對所有版本的搜尋，除了指定的值。

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執行工作，或分配發佈點。您可以按原樣執行範例，也可以根據範例建立自己的指令碼。

要調用 OpenAPI 方法並執行指令碼：

1. 下載 KlAkOAPI.tar.gz 存檔。此存檔包括 KlAkOAPI 套件和範例（您可以從存檔或 OpenAPI 參考指南中復制它們）。
2. 從安裝了管理伺服器的裝置上的 KlAkOAPI.tar.gz 存檔安裝 KlAkOAPI 套件。
   您只能在安裝了管理伺服器和 KlAkOAPI 套件的裝置上調用 OpenAPI 方法、執行範例和您自己的指令碼。

符合使用者方案和卡巴斯基安全管理中心 OpenAPI 方法的樣本

樣本	樣本目的	情景
記錄 KlAkParams	您可以使用 `KlAkParams` 資料結構來擷取與處理資料。該範例顯示如何使用此資料結構。 範例輸出可以以不同的方式呈現。您可以取得資料來傳送 HTTP 方法或在您的程式碼中使用它。	監控和報告
建立和刪除"主要/從屬"層級結構	您可以新增次要管理伺服器，進而建立「主要 / 次要」層級。或者，您可以中斷次要管理伺服器與層級結構的連線。	建立管理伺服器的層級結構，新增從屬管理伺服器，刪除管理伺服器的層級結構
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

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 • 在群組階層結構中移動 • 獲取完整的、擴展的群組階層結構及其名稱和嵌套	設定管理伺服器
列舉工作、查詢工作統計並執行工作	您可以找到以下資訊： • 工作進度記錄 • 目前工作狀態 • 不同狀態的工作數量 您還可以執行工作。預設情況下，範例會在輸出統計資訊後執行工作。	監視工作執行
建立並執行工作	您可以建立工作。在範例中指定以下工作參數： • 類型 • 執行方法 • 名稱 • 將使用工作的裝置群組 預設情況下，範例會建立一個「顯示訊息」類型的工作。您可以為管理伺服器的所有受管理裝置執行此工作。如有需要，您可以指定自己的工作參數。	建立工作
列舉產品授權金鑰	您可以獲得安裝在管理伺服器受管理裝置上之卡巴斯基應用程式的所有啟動產品授權金鑰的清單。該清單包含關於每個產品授權金鑰的詳細資料，例如名稱、類型或到期日期。	檢視使用中產品授權金鑰的相關資訊
建立與尋找內部使用者	您可以建立一個帳戶以進行進一步的工作。	選取帳戶以啟動管理伺服器
建立一個自訂類別	您可以根據需要建立應用程式類別參數。	建立含有手動新增內容的應用程式類別
使用 SrvView 列舉使用者	您可以使用 SrvView 類別請求獲得管理伺服器的詳細資料。例如，您可以使用此範例取得使用者清單。	管理使用者帳戶

透過 OpenAPI 與卡巴斯基安全管理中心互動的應用程式

一些應用程式透過 OpenAPI 與卡巴斯基安全管理中心互動。例如，此類應用程式包括 Kaspersky Anti Targeted Attack Platform 或 Kaspersky Security for Virtualization。這也可以是您基於 OpenAPI 開發的自訂用戶端應用程式。

透過 OpenAPI 與卡巴斯基安全管理中心互動的應用程式連線至管理伺服器。如果您配置了一個連線至管理伺服器的 IP 位址允許清單，請新增安裝了使用卡巴斯基安全管理中心 OpenAPI 的應用程式的裝置的 IP 位址。要了解您使用的應用程式是否透過 OpenAPI 工作，請參閱此應用程式的說明。

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 Optimum 和 Kaspersky Managed Detection and Response。

配置到 KATA / KEDR 網頁主控台的存取

Kaspersky Anti Targeted Attack（KATA）和 Kaspersky Endpoint Detection and Response（KEDR）是 Kaspersky Anti Targeted Attack Platform 的兩個功能塊。您可以透過 Kaspersky Anti Targeted Attack Platform 的網頁主控台（KATA / KEDR 網頁主控台）管理這些功能塊。如果您使用卡巴斯基安全管理中心 14 網頁主控台和 KATA / KEDR 網頁主控台，您可以從卡巴斯基安全管理中心 14 網頁主控台介面直接配置到 KATA / KEDR 網頁主控台的存取。

要配置到 KATA / KEDR 網頁主控台的存取：

1. 在主應用程式視窗中，點擊螢幕上方的**主控台設定**。
2. 在下拉清單中，選取**整合**。

   主控台設定視窗隨即開啟。

3. 在 **整合** 頁簽上，在 **KATA / KEDR 網頁主控台的網址** 欄位中輸入 KATA/KEDR 網頁主控台的 URL。

4. 點擊**儲存**按鈕。

進階管理 下拉清單被新增到主應用程式視窗中。您可以使用該功能表開啟 KATA / KEDR 網頁主控台。您點擊 **進階網路安全** 後，帶有您指定網址的新頁籤在您的瀏覽器開啟。

建立背景連線

例如，為了設定卡巴斯基安全管理中心與另一個卡巴斯基應用程式或解決方案之間的互動，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。您可以建立此連線，前提是您的帳戶具有**一般功能的修改物件 ACL 權限：使用者權限**功能區域。

> 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**主控台設定**下拉清單中，選取**整合**。
   主控台設定視窗隨即開啟。

2. 選取 **整合**頁籤。

3. 在**整合**頁籤，選取**整合**區段。

4. 將建立背景連線的切換按鈕切換到以下位置：**為整合建立背景連線 已啟用**.

5. 在開啟的**建立背景連線的服務將在卡巴斯基安全管理中心網頁主控台伺服器上啟動。**區段中，點擊**確定**按鈕。

在卡巴斯基安全管理中心網頁主控台和管理伺服器之間建立背景連線。管理伺服器會為背景連線建立一個帳戶，該帳戶會當作服務帳戶使用，以維護卡巴斯基安全管理中心與另一個卡巴斯基應用程式或解決方案之間的互動。該服務帳戶的名稱包含 NWCSvcUser 前置碼。出於安全考量，管理伺服器每 30 天會自動變更一次服務帳戶的密碼。您無法手動刪除此服務帳戶。當您停用跨服務連線時，管理伺服器會自動刪除此帳戶。管理伺服器會為每個卡巴斯基安全管理中心 14 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。

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 文件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。

> 卡巴斯基在此卡巴斯基安全管理中心 Linux 的生命週期內提供支援（請參見產品支援生命週期頁面）。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

透過電話取得技術支援

您可以從世界大多數區域撥打技術支援專家電話。您可以找到如何在您的國家獲取技術支援的資訊，並且可以在 卡巴斯基客戶服務網站 聯絡技術支援。

> 與技術支援部門聯絡之前，請閱讀支援規則。

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。

有關程式的資訊來源

Kaspersky 網站上的卡巴斯基安全管理中心頁面

在 Kaspersky 網站的卡巴斯基安全管理中心頁面上，您可以檢視有關程式、程式功能和特性的一般資訊。

知識庫中的卡巴斯基安全管理中心頁

*知識庫*是 Kaspersky 技術支援網站的一部分。

在知識庫的卡巴斯基安全管理中心 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。

已知問題

卡巴斯基安全管理中心 Linux 具有許多限制，這些限制對於應用程式的執行並不重要：

- 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不會要求您輸入憑據。
- 您在工作排程中設定**立即**選項並儲存變更後，*變更管理伺服器*工作不會自動啟動。
- 如果在管理伺服器內容中指定代理伺服器設定，然後在*將更新下載至管理伺服器儲存區*工作中啟用**不要使用代理伺服器**選項，此選項將被忽略並透過代理伺服器建立連線。
- 如果您在不同的瀏覽器中開啟卡巴斯基安全管理中心14 網頁主控台並在管理伺服器內容視窗中下載管理伺服器憑證檔案，則下載的檔案具有不同名稱。
- 當您嘗試從**備份**儲存區（**操作 → 儲存區 → 備份**）還原物件或將物件傳送到卡巴斯基時，將發生錯誤。
- Kaspersky Endpoint Security for Linux 的父策略中鎖定的設定會被繼承，但不會鎖定在子策略中。
- 從受管裝置傳送到管理伺服器的硬體資訊可能不完整；某些硬體項目可能未指定。

- 可以刪除您在 Kaspersky Endpoint Security for Linux 策略中新增到應用程式控制功能的應用程式類別。
- 具有多個網路介面卡的受管裝置可傳送有關網路介面卡 MAC 位址的管理伺服器資訊，該網路介面卡不是用於連線到管理伺服器的網路介面卡。
- 如果您在回應檔案中的 webConsoleAccount 和 managementServiceAccount 參數中指定自訂使用者帳戶以安裝卡巴斯基安全管理中心14 網頁主控台，並且這些帳戶屬於不同的安全群組，則卡巴斯基安全管理中心 14 網頁主控台在安裝後將不起作用。
- 在 Astra Linux 64 位版本中，klnagent-astra 套件不能用 klnagent64_14 套件升級：舊套件 klnagent64-astra 將被刪除，新套件 klnagent64 將被安裝而不是升級，所以將新增包含 klnagent64_14 套件的裝置的新圖示。您可以刪除此裝置的舊圖示。

詞彙表

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。

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 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。

備份資料夾

用於儲存使用備份實用程式建立的管理伺服器資料副本的專用資料夾。

備用訂購金鑰

程式已驗證可使用，但是目前還未使用的金鑰。

內部使用者

內部使用者的帳戶可用於管理虛擬管理伺服器。卡巴斯基安全管理中心授權應用程式的內部使用者擁有真實使用者的所有權限。

只能在卡巴斯基安全管理中心內建立和使用內部使用者帳戶。內部使用者的資料不會傳送到作業系統上。卡巴斯基安全管理中心將驗證內部使用者。

共用憑證

憑證用於識別使用者的行動裝置。

卡巴斯基安全管理中心操作員

對透過卡巴斯基安全管理中心管理的防護系統的狀態和操作進行監視的使用者。

卡巴斯基安全管理中心管理員

透過卡巴斯基安全管理中心遠端集中管理系統來管理應用程式操作的人。

卡巴斯基安全管理中心系統健康驗證程式 (SHV)

在卡巴斯基安全管理中心和 Microsoft NAP 並行執行時，用於檢查作業系統執行能力的卡巴斯基安全管理中心的一個元件。

卡巴斯基安全管理中心網頁伺服器

卡巴斯基安全管理中心元件，與管理伺服器一同安裝。網頁伺服器用於透過網路傳輸獨立安裝套件、iOS MDM 設定檔、以及共用資料夾的檔案。

卡巴斯基私有安全網路（私有 KSN）

私有卡巴斯基安全網路允許已安裝 Kaspersky 應用程式裝置的使用者，存取卡巴斯基安全網路信譽資料庫和其他統計資料，而不從他們的裝置傳送資料到卡巴斯基安全網路。私有卡巴斯基安全網路用於由於以下原因無法參與卡巴斯基安全網路的企業客戶：

- 使用者裝置未連線到網際網路。
- 傳輸任何資料到國家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。

應用程式商店

卡巴斯基安全管理中心元件。應用程式商店用於安裝應用程式到使用者 Android 裝置。應用程式商店允許您發佈應用程式 APK 檔案和連結到 Google Play。

手動安裝

從分發套件安裝安全應用程式到企業網路中的裝置。手動安裝需要管理員或其他 IT 專家的參與。通常情況下，如果遠端安裝發生錯誤，則執行手動安裝。

指定裝置的工作

從任意管理群組分配給一批用戶端裝置並且在那些裝置上執行的工作。

授權檔案

帶有 .key 副檔名的檔案，可以用來以試用或正式產品授權使用 Kaspersky 應用程式。

授權的應用程式群組

由管理員根據的標準設定（範例，根據供應商）建立的應用程式群組，系統將維護已安裝至用戶端裝置的應用程式的統計資訊。

政策

政策決定應用程式設定並管理應用程式在管理群組中電腦上的配置。必須為每個應用程式都建立單獨的政策。您可以為安裝在每個管理群組中之電腦的應用程式建立多個政策，但是對於管理群組中的每個應用程式，一次只能套用一個政策。

啟動產品授權

應用程式目前使用的金鑰。

更新

替換或者新增從 Kaspersky 更新伺服器接收到的新檔案（資料庫或應用程式模組）的過程。

服務供應商管理員

病毒防護服務提供者的員工。該管理員為基於 Kaspersky 病毒防護產品的病毒防護系統執行安裝和維護工作，並且向客戶提供技術支援。

本機安裝

將安全應用程式安裝在企業網路的裝置上，手動安裝會從安全應用程式分發套件開始，或者從預先下載到裝置的已發佈安裝套件開始。

本機工作

在單台用戶端電腦上定義和執行的工作。

歸屬管理伺服器

主管理伺服器是網路代理安裝過程中指定的管理伺服器。主管理伺服器可在網路代理連線設定檔中被使用。

產品授權期限

您可以存取程式功能並且有權使用進階服務的時間段。您可以使用的服務取決於產品授權的類型。

用戶端管理員

客戶組織中負責監控病毒防護狀態的員工。

病毒資料庫

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 14 網頁主控台。

管理伺服器

卡巴斯基安全管理中心的一個元件，可集中儲存公司網路安裝的所有 Kaspersky 應用程式相關資訊。它也可用於管理這些應用程式。

管理伺服器憑證

管理伺服器用於以下目的的憑證：

- 連線卡巴斯基安全管理中心 14 網頁主控台時驗證管理伺服器的身分
- 受管裝置上管理伺服器和網路代理之間的安全交互
- 將主管理伺服器連線到輔助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的 Kaspersky 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 14 網頁主控台的裝置。該元件提供了卡巴斯基安全管理中心管理介面。

管理員工作站用於設定和管理卡巴斯基安全管理中心的伺服器部分。使用管理員工作站，管理員基於 Kaspersky 應用程式為企業區域網路建立和管理一個集中的病毒防護系統。

管理員權限

在 Exchange 組織內管理 Exchange 物件所需的使用者權限。

管理群組

一組按照功能和已安裝的 Kaspersky 應用程式分組的裝置。裝置被分組成一個單一實體以便管理。群組可以包含其他群組。群組政策和群組工作可以為群組中每個安裝的應用程式建立。

網路代理

卡巴斯基安全管理中心的一個元件，它對管理伺服器和特定網路節點（工作站或伺服器）上安裝的 Kaspersky 程式之間的互動進行協調。該元件是公司內所有 Microsoft® Windows® 應用程式的通用元件。對於為 Unix 和 MacOS 之類別的平台開發的 Kaspersky 產品，分別有不同版本的網路代理。

網路病毒防護

一組技術和組織措施，能降低病毒和垃圾郵件可能感染組織網路的機會並防止網路攻擊、釣魚和其他威脅。當您使用安全應用程式和服務和應用企業資料安全政策時，網路安全被增加。

網路防護狀態

目前防護狀態，它定義了企業網路裝置的安全。網路防護狀態包括已安裝的安全應用程式、產品授權金鑰的使用及偵測到的威脅數量和類型等項目。

群組工作

為某個管理群組定義並且在該組織中所有用戶端裝置上執行的工作。

虛擬管理伺服器

卡巴斯基安全管理中心元件，其用途是管理用戶端組織網路的防護系統。

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

- 只能在主管理伺服器上建立虛擬管理伺服器。
- 虛擬管理伺服器在其操作中使用主管理伺服器資料庫。虛擬管理伺服器不支援資料備份和還原任務，以及更新掃描和下載任務。
- 虛擬伺服器無法建立次要管理伺服器（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。

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電腦的架構的配置詳情
- 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。

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

Firebird 是 Firebird Foundation 的註冊商標。

Foxit 是 Foxit Corporation 的註冊商標。

FreeBSD 是 FreeBSD foundation 的註冊商標。

Google、Android、Chrome、Chromium、Dalvik、Firebase、Google Chrome、Google Earth、Google Play、Google Maps、Hangouts 和 YouTube 是 Google LLC 的商標。

FusionCompute、FusionSphere 是華為技術有限公司在中國和其他國家的註冊商標。

Intel、Core 和 Xeon 是 Intel Corporation 在美國和其他國家/地區註冊的商標。

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 在美國和其他國家的註冊商標。

Micro Focus 是 Micro Focus (IP) Limited 或其附屬公司在英國、美國和其他國家/地區的商標或註冊商標。

Microsoft、Active Directory、ActiveSync、BitLocker、Excel、Forefront、Internet Explorer、InfoPath、Hyper-V、Microsoft Edge、MultiPoint、MS-DOS、PowerShell、PowerPoint、SharePoint、SQL Server、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 和 Thunderbird 是 Mozilla Foundation 的商標。

Novell 是 Novell Enterprises Inc. 在美國和其他國家的註冊商標。

Oracle、Java、JavaScript 和 TouchDown 是 Oracle 和/或其附屬公司的註冊商標。

Parallels 和 Parallels 標誌是 Parallels International GmbH 在加拿大、美國和/或其他地方的商標或註冊商標。

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、Ansible、CentOS、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。

BlackBerry 是 Research In Motion Limited 所有的商標，在美國和/或其他國家註冊。

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。

VMware、VMware vSphere 和 VMware Workstation 是 VMware, Inc. 在美國和/或其他國家的註冊商標或商標。

UNIX 是在美國和其他國家的註冊商標，透過 X/Open Company Limited 授權。

Zabbix 是 Zabbix SIA 的註冊商標。