kaspersky

Kaspersky Security Center Cloud Console

目錄

不相容應用程式
事件儲存區
事件嚴重等級
修補程式重要等級
備用訂購金鑰
卡巴斯基安全管理中心雲端主控台上的帳戶
卡巴斯基安全管理中心雲端主控台操作者
卡巴斯基安全管理中心雲端主控台管理員
卡巴斯基安全網路 (KSN)
卡巴斯基私有安全網路（KPSN）
受管理裝置
可用更新
安裝套件
工作
工作區
工作設定
廣播網域
弱點
強制安裝
應用程式標籤
指定裝置的工作
授權檔案
政策
政策設定檔
啟動產品授權
更新
本機安裝
本機工作
歸屬管理伺服器
產品授權期限
病毒活動臨界值
病毒爆發
病毒資料庫
發佈點
直接應用程式管理
程式設定
管理 Web 外掛程式
管理伺服器
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
裝置標記
身分和存取管理 (IAM)
身分驗證代理

卡巴斯基安全管理中心雲端主控台說明

	**新增內容** 在最新應用程式版本中的新增內容。		**配置網路防護** 透過依組織的需求設定 Kaspersky 應用程式政策與工作，管理組織的安全。
	**硬體和軟體需求** 檢查支援什麼作業系統和應用程式版本。		**Kaspersky 應用程式：定期更新資料庫和軟體模組** 維持防護系統的可靠性。
	**卡巴斯基安全管理中心雲端主控台的產品授權** 瞭解卡巴斯基安全管理中心雲端主控台以試用模式與正式模式運作時的詳細資訊。		**監控和報告** 檢視您的基礎架構、網路裝置防護狀態以及統計資訊，以便管理您組織目前的防護狀態。您也可以使用報告。
	**初始化設定** 開始使用您的工作區，依您的需求設定卡巴斯基安全管理中心雲端主控台。		**弱點和修補程式管理** 尋找和修復協力廠商軟體中的弱點。
	**移轉至卡巴斯基安全管理中心雲端主控台** 將您現有的管理群組和相關物件從內部部署的卡巴斯基安全管理中心移轉到卡巴斯基安全管理中心雲端主控台。		**匯出事件到 SIEM 系統** 設定透過 Syslog 通訊協定，將事件匯出至 SIEM 系統。
	**發現網路裝置** 發現您組織網路中現有與新的裝置。		**使用雲端環境** 保護雲端環境（Amazon Web Services™、Microsoft Azure™、Google™ Cloud Platform）中的虛擬機器。
	**發佈點和/或連線閘道的調整** 配置發佈點。		**給受管理服務提供商 (MSP) 的快速入門指南** 如果您是 MSP 的管理員，請由此瞭解如何使用卡巴斯基安全管理中心雲端主控台。
	**Kaspersky 應用程式：集中化部署** 佈署 Kaspersky 應用程式。		

新增內容

2024 年 4 月更新

本次卡巴斯基安全管理中心雲端主控台更新包含以下新功能和改進功能：

- 一項 Cloud Discovery 新功能。此功能可讓您監控執行 Windows 的受管理裝置上使用雲端服務的情況，甚至封鎖您認為不需要的雲端服務存取活動。Cloud Discovery 會追蹤使用者嘗試透過瀏覽器和桌面應用程式對這些服務進行的存取活動。

2024 年 2 月更新

本次卡巴斯基安全管理中心雲端主控台更新包含以下新功能和改進功能：

- 現在，您可以從受管理裝置清單中選擇一個或多個裝置，然後指派現有工作以在所選裝置上執行。工作的目前裝置範圍將被替換為您選擇的裝置。
- 現在您可以將裝置標籤指派給多個裝置或一次從多個裝置中刪除裝置標籤。從受管理裝置清單中，選擇裝置，然後指定要指派給所選裝置或從所選裝置中刪除的標籤。
- 最佳化受管理裝置清單的外觀和使用者體驗。新增了新列**標籤**以及按裝置標籤過濾裝置的功能。

2024 年 1 月更新

卡巴斯基安全管理中心雲端主控台現在支援 Kaspersky Endpoint Security 12.4 for Windows。

2023 年 12 月更新

本次卡巴斯基安全管理中心雲端主控台更新包含以下新功能和改進功能：

- 您現在可以檢查 SIEM 系統連線。
- 卡巴斯基安全管理中心雲端主控台現在支援透過基於 Linux 的發佈點，輪詢 Microsoft Active Directory 網域控制器和 Samba 網域控制器。
- 遠端診斷基於 Linux 的受管理裝置。
- 卡巴斯基安全管理中心雲端主控台現在支援以下 Kaspersky 應用程式：
  - Kaspersky Endpoint Security for Windows 版本 12.3 修補程式 A
  - Kaspersky Endpoint Security 12.0 for Linux
  - Kaspersky Endpoint Security 12.0 for Mac
  - Kaspersky Endpoint Agent 3.16
  - Kaspersky Embedded Systems Security 3.3 for Windows
- 兩個介面區段由於超出應用程式的功能涵蓋範圍，在主功能表中已被隱藏：

- 加密事件（**操作** → **資料加密與防護** → **加密事件**）
- IP 範圍（**發現和佈署** → **發現** → **IP 範圍**）

- 卡巴斯基安全管理中心雲端主控台的資料處理協議文字已有所更新。
- 不再支援一些舊版瀏覽器（比版本 102 還早的 Firefox ESR）。

2023 年 9 月更新

本次卡巴斯基安全管理中心雲端主控台更新包含以下新功能和改進功能：

- 卡巴斯基安全管理中心雲端主控台現在支援 Kaspersky Embedded Systems Security 3.3 for Linux。
- 卡巴斯基安全管理中心雲端主控台現在支援 Kaspersky Endpoint Security 12.2 for Windows。
- 將 **資產（裝置）** 區段中使用者清單的使用者介面最佳化。

2023 年 6 月更新

本次卡巴斯基安全管理中心雲端主控台更新包含以下新功能和改進功能：

- 發佈新的強化指南。強烈建議您仔細閱讀該指南，並按照安全建議來設定卡巴斯基安全管理中心雲端主控台和您的網路基礎架構。
- 卡巴斯基安全管理中心雲端主控台現在支援 Kaspersky Endpoint Security 11.3 for Mac。
- 卡巴斯基安全管理中心雲端主控台現在支援 Kaspersky Endpoint Security 11.4 for Linux。
- 您可以使用卡巴斯基安全管理中心雲端主控台將事件分類匯出到一個檔案，然後將這些事件分類匯入到卡巴斯基安全管理中心 Windows 或卡巴斯基安全管理中心 Linux。
- 您現在可以針對受網路代理管理的裝置，使用發佈點作為推送伺服器。此功能可讓您確保受管理裝置與管理伺服器之間會持續建立連線。
- 重新組織含有設定的區段，以便將卡巴斯基安全管理中心雲端主控台與其他 Kaspersky 應用程式整合在一起。
- 重新組織**遠端診斷**區段的使用者介面。
- 您現在可以將裝置分類中所含所有裝置的資訊一次儲存到 CSV 檔案。
- 使用者介面和易用性有了一些改進，包括能夠選取表格中的所有項目。

2023 年 3 月更新

本次卡巴斯基安全管理中心雲端主控台更新包含以下新功能和改進功能：

- 卡巴斯基安全管理中心雲端主控台現在支援將叢集和伺服器陣列作為受管理裝置。如果有 Kaspersky 應用程式安裝到叢集節點上，網路代理會將這些資訊傳送給管理伺服器。在網頁主控台中，叢集和伺服器陣列會獨立於其他受管理裝置來列出。您可以將每個叢集或伺服器陣列各當成一個獨立、不可分割的物件來管理。
- 卡巴斯基安全管理中心雲端主控台現在支援 Kaspersky Endpoint Security 12.0 for Windows。

- 報告可以包含的最大項目筆數已增加至 2500 筆（網頁主控台中顯示的報告）和 10,000 筆（您匯出到檔案的報告）。
- 您現在可以選擇是否要在防護狀態報告中納入狀態為*正常*的受管理裝置。
- 您現在可以使用以下其中一種產品授權啟動卡巴斯基安全管理中心雲端主控台，或是將所列產品授權的產品授權金鑰新增至現有工作區：
  - Kaspersky Symphony Security
  - Kaspersky Symphony EDR
  - Kaspersky Symphony MDR
  - Kaspersky Symphony XDR
- 發佈一個適用於 Windows XP 的網路代理特別版本。
- Network Agent for Linux 經過更新，可支援 KSN 代理服務。除了可使用基於 Windows 的發佈點，您現在還可以使用基於 Linux 的發佈點，轉發來自受管理裝置的卡巴斯基安全網路 (KSN) 請求。此功能可讓您進行網路流量的重新分配與最佳化。
- Network Agent for Linux 經過更新，可支援應用程式登錄資料功能。網路代理可以將基於 Linux 的裝置上已安裝的應用程式彙整成清單，然後將這份清單傳送給管理伺服器。
- 您可以使用卡巴斯基安全管理中心雲端主控台將政策和工作匯出到一個檔案，然後將這些政策和工作匯入到卡巴斯基安全管理中心 Windows 或卡巴斯基安全管理中心 Linux。

2022 年 11 月更新

本次 Kaspersky Security Center Cloud Console 更新包含以下新功能和改進功能：

- 卡巴斯基安全管理中心雲端主控台現在支援 Kaspersky Endpoint Security 11.3 for Linux。
- 卡巴斯基安全管理中心雲端主控台現在支援 Kaspersky Managed Detection and Response 2.1.18。
- 卡巴斯基安全管理中心雲端主控台現在支援 Kaspersky Endpoint Security for Mac 11.2 和 11.2.1 更新後的版本，以便支援 macOS 13。
- **介紹與教程**區段中的影片已更新。

2022 年 10 月更新

本次卡巴斯基安全管理中心雲端主控台更新包含以下新功能和改進功能：

- Kaspersky Security Center Cloud Console 適用的資料處理協議文字已更新。
- 現在，當工作區中不含作用中產品授權金鑰，而您若不新增產品授權金鑰，將可能會令該工作區遭刪除時，卡巴斯基安全管理中心雲端主控台基礎架構會通知您。
- 卡巴斯基安全管理中心雲端主控台現在支援 Kaspersky Endpoint Security 11.11.0 for Windows。
- 卡巴斯基安全管理中心雲端主控台現在支援 Kaspersky Endpoint Detection and Response Optimum 2.3。

- 支援 Kaspersky Embedded Systems Security 3.2 for Windows。

2022 年 9 月更新

本次卡巴斯基安全管理中心雲端主控台更新包含以下新功能和改進功能：

- 您現在可以為虛擬管理伺服器分配專門的管理員。您要先為管理員建立使用者帳戶，然後再向該管理員授予對虛擬管理伺服器的存取權限。所分配的管理員僅能存取所選的虛擬管理伺服器，而無法連線到主管理伺服器或其他從屬管理伺服器（無論是實體還是虛擬管理伺服器皆然）。
- 已將您刪除卡巴斯基安全管理中心雲端主控台產品授權金鑰時的使用者體驗最佳化。新機制可防止您意外刪除最後一個啟動產品授權金鑰。
- 您現在可以使用基於 Linux 的發佈點，透過*將更新下載至發佈點儲存區*工作來下載 Kaspersky 安全應用程式的病毒資料庫。
- 網路代理現已提供日語本地化版本。
- 在卡巴斯基安全管理中心雲端主控台介面中，區段名稱的全部大寫樣式已變更為句子樣式的大小寫。

2022 年 8 月更新

新語言支援：卡巴斯基安全管理中心雲端主控台現已提供全日語版本。

2022 年 7 月更新

本次卡巴斯基安全管理中心雲端主控台更新包含以下新功能和改進功能：

- 新支援的 Kaspersky 應用程式版本清單：
  - Kaspersky Endpoint Agent 3.13
  - Kaspersky Endpoint Security 11.2.1 for Mac
  - Kaspersky Security for iOS 1.0.0
  - Kaspersky Endpoint Security 11.10.0 for Windows
- 我們為卡巴斯基安全管理中心雲端主控台更新了協議與資料處理協議的文字。
- 新語言支援：卡巴斯基安全管理中心雲端主控台基礎架構現已提供日語版本。卡巴斯基安全管理中心雲端主控台工作區內對日語的支援即將推出。

2022 年 4 月更新

本次卡巴斯基安全管理中心雲端主控台更新包含以下新功能和改進功能：

- 卡巴斯基安全管理中心雲端主控台現在支援 Kaspersky Endpoint Security 11.9.0 for Windows。
- 卡巴斯基安全管理中心雲端主控台現在支援 Kaspersky Embedded Systems Security 的日語本地化版本。

2022 年 3 月 9 日更新

本次卡巴斯基安全管理中心雲端主控台更新包含以下新功能和改進功能：

- 已實行與 Kaspersky Endpoint Detection and Response Expert 的整合。
- 已實行事件回應平台 (IRP)。現在，您可以透過卡巴斯基安全管理中心雲端主控台來管理安全事件。
- 卡巴斯基安全管理中心雲端主控台現在接受 Kaspersky Endpoint Detection and Response Expert 的產品授權金鑰。產品授權可用於的最小裝置數量為 50 個。

2022 年 2 月 11 日更新

本次卡巴斯基安全管理中心雲端主控台更新包含以下新功能和改進功能：

- 現在支援 Kaspersky Embedded Systems Security for Windows 的產品授權。
- 支援 Kaspersky Endpoint Security 11.8.0 for Windows。
- 您可以使用日語版分發套件，安裝 Kaspersky Endpoint Security 11.8.0 for Windows。
- 支援 Kaspersky Endpoint Agent 3.12。

2021 年 12 月 10 日更新

本次卡巴斯基安全管理中心雲端主控台更新包含以下新功能和改進功能：

- 與內部使用者相關的功能已改進：
  - 您現在可以在入口中新增內部使用者。
  - 應用程式現在會防止您降低自己的權限。

2021 年 10 月 18 日更新

本次卡巴斯基安全管理中心雲端主控台更新包含以下新功能和改進功能：

- 卡巴斯基安全管理中心雲端主控台現在支援 Kaspersky Endpoint Detection and Response Optimum 2.0。
- 您現在可以使用卡巴斯基安全管理中心雲端主控台管理執行 Android 的行動裝置。
- 卡巴斯基市場成為新的功能表區段：您現在可以使用卡巴斯基安全管理中心雲端主控台搜尋 Kaspersky 應用程式。
- 提供新的功能表區段：卡巴斯基公告。「卡巴斯基公告」會提供受管理裝置上所安裝 Kaspersky 應用程式的相關資訊，讓您隨時掌握最新情況。卡巴斯基安全管理中心雲端主控台會定期更新該區段中的資訊。
- 您現在可以透過卡巴斯基安全管理中心雲端主控台，管理在 Linux 作業系統上執行的從屬管理伺服器。

2021 年 9 月 7 日更新

本次卡巴斯基安全管理中心雲端主控台更新包含以下新功能和改進功能：

- 您現在可以透過 Active Directory 同盟服務 (ADFS)，直接使用 Active Directory 帳戶登入卡巴斯基安全管理中心雲端主控台，而無需建立新的使用者帳戶。
- 卡巴斯基安全管理中心雲端主控台現在可搭配以下雲端環境運作：Amazon Web Services、Microsoft Azure 和 Google Cloud。若要保護雲端環境中的虛擬機器（或實例），您需要具有其中一種 Kaspersky Hybrid Cloud Security 產品授權。提供雲端環境設定精靈。
- 每一工作區的最大裝置數量現在是 25,000 個。
- 卡巴斯基安全管理中心雲端主控台中現已提供與 SIEM 系統的整合。您可以使用 Syslog 通訊協定，將事件匯出到 SIEM 系統。
- 您現在可以建立虛擬管理伺服器。每個虛擬管理伺服器都能有自己的管理群組結構、政策、工作、報告和事件。您可以利用虛擬管理伺服器，在工作區內管理工作流程複雜的用戶端組織。不過，您無法將虛擬管理伺服器從內部部署運作的卡巴斯基安全管理中心移轉到卡巴斯基安全管理中心雲端主控台。
- 您現在可以調整表格中的欄寬，並且對資料進行排序和搜尋。
- Kaspersky Business Hub 與卡巴斯基安全管理中心雲端主控台的穩定性與可用性已有所改進。

2020 年 10 月 27 日更新

本次卡巴斯基安全管理中心雲端主控台更新包含以下新功能和改進功能：

- 卡巴斯基安全管理中心雲端主控台現在支援 Kaspersky Endpoint Security 11.6.0 for Windows、Kaspersky Endpoint Security 11.1 for Mac 修補程式 A 和Kaspersky Endpoint Agent 3.10（隨附於 Kaspersky Endpoint Detection and Response Optimum）。
- 您現在可以使用以下產品授權：
  - Kaspersky Endpoint Detection and Response Optimum
  - Kaspersky Endpoint Security for Business Advanced
  - Kaspersky Total Security for Business
- 已實行以下功能：
  - 弱點和修補程式管理功能
  - 加密管理
  - 應用程式控制
  - 自適應異常控制
  - RDP 工作階段，包括 Windows 桌面共用
- 導覽功能表現在為垂直排列，類似於卡巴斯基安全管理中心基於 Microsoft Management Console 的介面。
- 現已提供技術訓練影片，協助您瞭解應用程式的使用方式。

2020 年 6 月 30 日更新

本次卡巴斯基安全管理中心雲端主控台更新包含以下新功能和改進功能：

- 卡巴斯基安全管理中心雲端主控台現在支援 Kaspersky Security 11 for Windows Server（自 2020 年 9 月起）。
- 卡巴斯基安全管理中心雲端主控台現在支援 Kaspersky Endpoint Agent 3.9 和 Kaspersky Endpoint Security 11.4.0 for Windows。
- 快速啟動精靈已改進：移除了一些步驟、稍微變更了步驟順序並且編輯了一些文字，以提高易用性。
- 卡巴斯基安全管理中心雲端主控台現已提供義大利語版本。
- 您現在可以透過卡巴斯基安全管理中心雲端主控台介面，撤銷任何受管理 Kaspersky 應用程式的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。
- 您現在可以刪除工作區。如果您將工作區標記為刪除，則該工作區預設會在 7 天後自動刪除。不過，您可以強制刪除工作區，使其立即刪除。
- 已實行透過雙步驟驗證登入主控台。

卡巴斯基安全管理中心雲端主控台

本節說明卡巴斯基安全管理中心雲端主控台的用途和其主要功能特色和元件。

卡巴斯基安全管理中心雲端主控台是一款由 Kaspersky 架設並維護的應用程式。您無需在自己的電腦或伺服器上安裝卡巴斯基安全管理中心雲端主控台。卡巴斯基安全管理中心雲端主控台可讓管理員將 Kaspersky 安全應用程式安裝到企業網路內的裝置上、遠端執行掃描與更新工作，以及管理受管理應用程式適用的安全政策。管理員可以使用詳細的儀表板，查看企業裝置的狀態快照、詳細報告，以及防護政策中的細項設定。

關於 Kaspersky Security Center Cloud Console

卡巴斯基安全管理中心雲端主控台是一款方便企業網路管理員以及各組織中負責為裝置提供防護的員工使用的應用程式。

卡巴斯基安全管理中心雲端主控台可讓您執行以下工作：

- 將 Kaspersky 應用程式安裝到您網路中的裝置並管理所安裝的應用程式。
- 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。
- 建立虛擬管理伺服器並加以排列成階層。
- 保護您的網路裝置，包括工作站和伺服器：
  - 管理以 Kaspersky 應用程式構建的惡意軟體防護系統。
  - 使用偵測和回應（EDR 和 MDR）功能（需有 Kaspersky Endpoint Detection and Response 與/或 Kaspersky Managed Detection and Response 的產品授權），包括：
    - 分析和調查事件
    - 透過建立威脅發展鏈圖表，將事件做視覺化呈現
    - 手動接受或拒絕回應，或是設定自動接受所有回應
- 以多租戶應用程式的形式使用卡巴斯基安全管理中心雲端主控台。
- 遠端管理用戶端裝置上安裝的 Kaspersky 應用程式。
- 以集中化方式將 Kaspersky 應用程式的產品授權金鑰部署到用戶端裝置。
- 為您網路中的裝置建立和管理安全政策。
- 建立和管理使用者帳戶。
- 建立和管理使用者角色 (RBAC)。
- 為您網路裝置上安裝的應用程式建立和管理工作。
- 個別檢視每個用戶端組織的安全系統狀態報告。

您管理卡巴斯基安全管理中心雲端主控台時，是使用雲端型管理主控台，該主控台會確保透過瀏覽器就能讓您的裝置與管理伺服器彼此互動。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。當您使用瀏覽器連線至卡巴斯基安全管理中心雲端主控台時，瀏覽器會與卡巴斯基安全管理中心雲端主控台伺服器建立連線。

管理伺服器和所連接的資料庫管理系統 (DBMS) 是部署在雲端環境中，以服務的形式提供給您。管理伺服器與 DBMS 的維護亦涵蓋在服務中。卡巴斯基安全管理中心雲端主控台的所有軟體元件均會維持在最新版本。管理伺服器和建立的物件（例如政策和工作）會定期受到備份以確保安全。

卡巴斯基安全管理中心雲端主控台是一款多語言的應用程式。您可以在任意時刻變更介面語言，而不重新開啟應用程式。

卡巴斯基安全管理中心雲端主控台的硬體和軟體需求

管理主控台

對客戶而言，只要有瀏覽器，就能使用卡巴斯基安全管理中心雲端主控台。

> 您僅能在單一瀏覽器視窗或頁籤中使用卡巴斯基安全管理中心雲端主控台。

裝置的硬體和軟體需求，就與用於存取卡巴斯基安全管理中心雲端主控台的瀏覽器相同。

瀏覽器：

- 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
- 「Yandex」瀏覽器 23.5.0.2271
- Mozilla Firefox 延伸支援版本 102.0 或更高版本

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：512MB。
- 可用磁碟空間：1 GB。

弱點和修補程式管理的最低硬體需求：

- 執行頻率為 1.4 GHz 或更高的 CPU。需要 64 位元作業系統。
- RAM：8 GB。

- 可用磁碟空間：1 GB。

網路代理支援的作業系統

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

Microsoft Windows 10 教育版 RS5（2018 年 10 月）32 位元/64 位元
Microsoft Windows 10 家庭版 19H1 32 位元 / 64 位元
Microsoft Windows 10 專業版 19H1 32 位元/64 位元
Microsoft Windows 10 工作站專業版 19H1 32 位元/64 位元
Microsoft Windows 10 企業版 19H1 32 位元/64 位元
Microsoft Windows 10 教育版 19H1 32 位元/64 位元
Microsoft Windows 10 教育版 19H2 32 位元 / 64 位元
Microsoft Windows 10 專業版 19H2 32 位元/64 位元
Microsoft Windows 10 Pro for Workstations 19H2 32 位元 / 64 位元
Microsoft Windows 10 Enterprise 19H2 32 位元 / 64 位元
Microsoft Windows 10 Education 19H2 32 位元 / 64 位元
Microsoft Windows 10 家用版 20H1（2020 年 5 月更新）32 位元/64 位元
Microsoft Windows 10 專業版 20H1（2020 年 5 月更新）32 位元/64 位元
Microsoft Windows 10 企業版 20H1（2020 年 5 月更新）32 位元/64 位元
Microsoft Windows 10 教育版 20H1（2020 年 5 月更新）32 位元/64 位元
Microsoft Windows 10 家用版 20H2（2020 年 10 月更新）32 位元/64 位元
Microsoft Windows 10 專業版 20H2（2020 年 10 月更新）32 位元/64 位元
Microsoft Windows 10 企業版 20H2（2020 年 10 月更新）32 位元/64 位元
Microsoft Windows 10 教育版 20H2（2020 年 10 月更新）32 位元/64 位元
Microsoft Windows 10 家用版 21H1（2021 年 5 月更新）32 位元/64 位元
Microsoft Windows 10 專業版 21H1（2021 年 5 月更新）32 位元/64 位元
Microsoft Windows 10 企業版 21H1（2021 年 5 月更新）32 位元/64 位元
Microsoft Windows 10 教育版 21H1（2021 年 5 月更新）32 位元/64 位元
Microsoft Windows 10 家用版 21H2（2021 年 10 月更新）32 位元/64 位元
Microsoft Windows 10 專業版 21H2（2021 年 10 月更新）32 位元/64 位元
Microsoft Windows 10 企業版 21H2（2021 年 10 月更新）32 位元/64 位元
Microsoft Windows 10 教育版 21H2（2021 年 10 月更新）32 位元/64 位元
Microsoft Windows 10 家用版 22H2（2023 年 10 月更新）32 位元/64 位元
Microsoft Windows 10 專業版 22H2（2023 年 10 月更新）32 位元/64 位元
Microsoft Windows 10 企業版 22H2（2023 年 10 月更新）32 位元/64 位元
Microsoft Windows 10 教育版 22H2（2023 年 10 月更新）32 位元/64 位元
Microsoft Windows 11 家用版 64 位元
Microsoft Windows 11 專業版 64 位元
Microsoft Windows 11 企業版 64 位元
Microsoft Windows 11 教育版 64 位元
Microsoft Windows 11 22H2
Microsoft Windows 8.1 專業版 32 位元/64 位元
Microsoft Windows 8.1 企業版 32 位元/64 位元
Microsoft Windows 8 專業版 32 位元/64 位元
Microsoft Windows 8 Enterprise 32 位元 / 64 位元
Microsoft Windows 7 專業版（Service Pack 1 和更高版本）32 位元/64 位元
Microsoft Windows 7 專業版/旗艦版（Service Pack 1 和更高版本）32 位元/64 位元

	Microsoft Windows 7 家用基本版/進階版（Service Pack 1 和更高版本）32 位元/64 位元 Microsoft Windows XP Professional Service Pack 3 以上 32 位元 Microsoft Windows XP Professional for Embedded Systems Service Pack 3 32 位元 Windows MultiPoint™ Server 2011 Standard/Premium 64 位元 Windows Server 2008 Foundation (Service Pack 2) 32 位元 / 64 位元 Windows Server 2008 Service Pack 2（所有版本）32 位元/64 位元 Windows Server 2008 R2 Datacenter Service Pack 1 和更高版本 64 位元 Windows Server 2008 R2 Enterprise Service Pack 1 和更高版本 64 位元 Windows Server 2008 R2 Foundation（Service Pack 1 和更高版本）64 位元 Windows Server 2008 R2 內核模式 Service Pack 1 和更高版本 64 位元 Windows Server 2008 R2 Standard Service Pack 1 和更高版本 64 位元 Windows Server 2008 R2 Service Pack 1（所有版本）64 位元 Windows Server 2012 Server Core 64 位元 Windows Server 2012 Datacenter 64 位元 Windows Server 2012 Essentials 64 位元 Windows Server 2012 Foundation 64 位元 Windows Server 2012 Standard 64 位元 Windows Server 2012 R2 Server Core 64 位元 Windows Server 2012 R2 Datacenter 64 位元 Windows Server 2012 R2 Essentials 64 位元 Windows Server 2012 R2 Foundation 64 位元 Windows Server 2012 R2 Standard 64 位元 Windows Server 2016 Datacenter (LTSB) 64 位元 Windows Server 2016 Standard (LTSB) 64 位元 Windows Server 2016 Server Core（安裝選項）(LTSB) 64 位元 Windows Server 2019 Standard 64 位元 Windows Server 2019 Datacenter 64 位元 Windows Server 2019 Core 64 位元 Windows Server 2022 Standard 64 位元 Windows Server 2022 Datacenter 64 位元 Windows Server 2022 Core 64 位元
作業系統。Linux	Debian GNU/Linux 12 (Bookworm) Debian GNU/Linux 11.x (Bullseye) 32 位元/64 位元 Debian GNU/Linux 10.x (Buster) 32 位元 / 64 位元 Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 位元 Ubuntu Server 20.04 LTS (Focal Fossa) 32 位元/64 位元 Ubuntu Server 18.04 LTS (Bionic Beaver) 32 位元 / 64 位元 CentOS Stream 9 64 位元 CentOS 7.x 64 位元 Red Hat Enterprise Linux Server 9.x 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 openSUSE 15 64 位元 Oracle Linux 7 64 位元 Oracle Linux 8 64 位元 Oracle Linux 9 64 位元 Linux Mint 20.x 64 位元
作業系統。macOS	macOS Big Sur (11.x) macOS Monterey (12.x) macOS Ventura (13.x)

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

支援以下虛擬平台：

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- VMware Workstation 16 Pro
- VMware Workstation 17 Pro
- Microsoft Hyper-V Server 2012 位元
- Microsoft Hyper-V Server 2012 R2 64 位元
- Microsoft Hyper-V Server 2016 64 位元
- Microsoft Hyper-V Server 2019 64 位元
- Microsoft Hyper-V Server 2022 64 位元
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 17
- Oracle VM VirtualBox 6.x
- Oracle VM VirtualBox 7.x
- 基於內核的虛擬機（網絡代理支援的所有 Linux 作業系統）

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

不支援的作業系統和平台

網路代理

不支援以下作業系統：

- Microsoft Windows Embedded POSReady 7 32 位元/64 位元
- Microsoft Windows Embedded 8 Industry Pro 32 位元/64 位元
- Microsoft Windows Embedded 8 Industry Enterprise 32 位元/64 位元
- Microsoft Windows Embedded 8 Standard 32 位元/64 位元
- Microsoft Windows Embedded 8.1 Industry Enterprise 32 位元/64 位元
- Microsoft Windows Embedded 8.1 Industry Update 32 位元/64 位元
- Microsoft Windows 10 家用版（Threshold 1，1507）32 位元/64 位元
- Microsoft Windows 10 專業版（Threshold 1，1507）32 位元/64 位元
- Microsoft Windows 10 企業版（Threshold 1，1507）32 位元/64 位元
- Microsoft Windows 10 教育版（Threshold 1，1507）32 位元/64 位元
- Microsoft Windows 10 行動裝置版（Threshold 1，1507）32 位元
- Microsoft Windows 10 行動裝置企業版（Threshold 1，1507）32 位元
- Microsoft Windows 10 家用版 Threshold 2（2015 年 11 月更新，1511）32 位元/64 位元
- Microsoft Windows 10 專業版 Threshold 2（2015 年 11 月更新，1511）32 位元/64 位元
- Microsoft Windows 10 企業版 Threshold 2（2015 年 11 月更新，1511）32 位元/64 位元
- Microsoft Windows 10 教育版 Threshold 2（2015 年 11 月更新，1511）32 位元/64 位元
- Microsoft Windows 10 行動裝置版 Threshold 2（2015 年 11 月更新，1511）32 位元
- Microsoft Windows 10 行動裝置企業版 Threshold 2（2015 年 11 月更新，1511）32 位元
- Microsoft Windows 10 家用版 RS1（週年紀念更新，1607）32 位元/64 位元
- Microsoft Windows 10 專業版 RS1（週年紀念更新，1607）32 位元/64 位元
- Microsoft Windows 10 企業版 RS1（週年紀念更新，1607）32 位元/64 位元
- Microsoft Windows 10 教育版 RS1（週年紀念更新，1607）32 位元/64 位元
- Microsoft Windows 10 行動裝置版 RS1（週年紀念更新，1607）32 位元

- Microsoft Windows 10 行動裝置企業版 RS1（週年紀念更新，1607）32 位元
- Microsoft Windows 10 家用版 RS2（創作者更新，1703）32 位元/64 位元
- Microsoft Windows 10 專業版 RS2（創作者更新，1703）32 位元/64 位元
- Microsoft Windows 10 企業版 RS2（創作者更新，1703）32 位元/64 位元
- Microsoft Windows 10 教育版 RS2（創作者更新，1703）32 位元/64 位元
- Microsoft Windows 10 行動裝置版 RS2（創作者更新，1703）32 位元
- Microsoft Windows 10 行動裝置企業版 RS2（創作者更新，1703）32 位元
- Microsoft Windows 10 行動裝置版 RS3 32 位元
- Microsoft Windows 10 行動裝置企業版 RS3 32 位元
- Microsoft Windows 10 行動裝置版 RS4 32 位元
- Microsoft Windows 10 行動裝置企業版 RS4 32 位元
- Microsoft Windows 10 行動裝置版 RS5 32 位元
- Microsoft Windows 10 行動裝置企業版 RS5 32 位元
- Microsoft Windows 8 (Core) 32 位元/64 位元
- Microsoft Windows 7 專業版 32 位元/64 位元
- Microsoft Windows 7 專業版/旗艦版 32 位元/64 位元
- Microsoft Windows 7 家用基本版/進階版 32 位元/64 位元
- Microsoft Windows Vista Business (Service Pack 1) 32 位元/64 位元
- Microsoft Windows Vista Enterprise (Service Pack 1) 32 位元/64 位元
- Microsoft Windows Vista Ultimate (Service Pack 1) 32 位元/64 位元
- Microsoft Windows Vista Business（Service Pack 2 和更高版本）32 位元/64 位元
- Microsoft Windows Vista Enterprise（Service Pack 2 和更高版本）32 位元/64 位元
- Microsoft Windows Vista Ultimate（Service Pack 2 和更高版本）32 位元/64 位元
- Microsoft Windows XP Professional Service Pack 2 32 位元/64 位元
- Microsoft Windows XP Home Service Pack 3 及以上 32 位元
- Windows Essential Business Server 2008 Standard 64 位元
- Windows Essential Business Server 2008 Premium 64 位元
- Windows Small Business Server 2003 Standard (Service Pack 1) 32 位元

- Windows Small Business Server 2003 Premium (Service Pack 1) 32 位元
- Windows Small Business Server 2008 Standard 64 位元
- Windows Small Business Server 2008 Premium 64 位元
- Windows Small Business Server 2011 Premium Add-on 64 位元
- Windows Small Business Server 2011 Standard 64 位元
- Windows Small Business Server 2011 Essentials 64 位元
- Windows Home Server 2011 64 位元
- Windows MultiPoint Server 2010 Standard 64 位元
- Windows MultiPoint Server 2010 Premium 64 位元
- Windows MultiPoint™ Server 2012 Standard/Premium 64 位元
- Microsoft Windows 2000 Server 32 位元
- Windows Server 2003 Enterprise (Service Pack 2) 32 位元/64 位元
- Windows Server 2003 Standard (Service Pack 2) 32 位元/64 位元
- Windows Server 2003 R2 Enterprise (Service Pack 2) 32 位元/64 位元
- Windows Server 2003 R2 Standard (Service Pack 2) 32 位元/64 位元
- Windows Server 2008 Datacenter (Service Pack 1) 32 位元/64 位元
- Windows Server 2008 Enterprise (Service Pack 1) 32 位元/64 位元
- Windows Server 2008 Service Pack 1 Server Core 32 位元/64 位元
- Windows Server 2008 Standard Service Pack 1 32 位元/64 位元
- Windows Server 2008 Standard 32 位元/64 位元
- Windows Server 2008 Enterprise 32 位元/64 位元
- Windows Server 2008 Datacenter 32 位元/64 位元
- Windows Server 2008 R2 Server Core 64 位元
- Windows Server 2008 R2 Datacenter 64 位元
- Windows Server 2008 R2 Enterprise 64 位元
- Windows Server 2008 R2 Foundation 64 位元
- Windows Server 2008 R2 Standard 64 位元
- Windows Server 2016 Nano（安裝選項）(CBB)

- Windows Storage Server 2008 32 位元/64 位元
- Windows Storage Server 2008 Service Pack 2 64 位元
- Windows Storage Server 2008 R2 64 位元
- Windows Storage Server 2012 64 位元
- Windows Storage Server 2012 R2 64 位元
- Windows Storage Server 2016 64 位元
- Windows Storage Server 2019 64 位元
- Debian GNU/Linux 7.x（最高 7.8）32 位元/64 位元
- Debian GNU/Linux 8.x (Jessie) 32 位元/64 位元
- Debian GNU / Linux 9.x (Stretch) 32 位元 / 64 位元
- Ubuntu Server 14.04 LTS (Trusty Tahr) 32 位元/64 位元
- Ubuntu Server 16.04 LTS (Xenial Xerus) 32 位元/64 位元
- Ubuntu Desktop 14.04 LTS (Trusty Tahr) 32 位元/64 位元
- Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32 位元/64 位元
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 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 6.x（至 6.6）64 位元
- CentOS 7.x ARM 64 位元
- CentOS 8.x 64 位元
- SUSE Linux Enterprise Desktop 12（所有 SP）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
- 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
- EulerOS 2.0 SP8 ARM
- Pardus OS 19.1 64 位元
- Astra Linux 特別版 RUSB.10015-01（操作更新 1.7）64 位元
- Astra Linux 特別版 RUSB.10015-01（操作更新 1.6）64 位元
- Astra Linux 通用版（操作更新 2.12）64 位元
- Astra Linux 特別版 RUSB.10152-02（操作更新4.7）ARM 64 位元
- Linux Mint 19.x 64 位元
- AlterOS 7.5 及更高版本 64 位元
- Lotos (Linux 核心版本 4.19.50, DE: MATE) 64 位元
- Mageia 4 32 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 COBALT 7.9 64 位元
- ROSA CHROME 12 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
- OS X 10.10 (Yosemite)
- OS X 10.11 (El Capitan)
- macOS Sierra (10.12)

- macOS High Sierra (10.13)
- macOS Mojave (10.14)
- macOS Catalina (10.15)

不支援以下虛擬平台：

- VMware vSphere 4.1
- VMware vSphere 5.0
- VMware vSphere 5.1
- VMware vSphere 5.5
- VMware vSphere 6
- VMware vSphere 6.5
- VMware Workstation 9.x
- VMware Workstation 10.x
- VMware Workstation 11.x
- VMware Workstation 12.x Pro
- VMware Workstation Pro 14
- VMware Workstation Pro 15
- Microsoft Hyper-V Server 2008 64 位元
- Microsoft Hyper-V Server 2008 R2 64 位元
- Microsoft Hyper-V Server 2008 R2 Service Pack 1 和更高版本 64 位元
- Citrix XenServer 6.0
- Citrix XenServer 6.1
- Citrix XenServer 6.2
- Citrix XenServer 6.5
- Citrix XenServer 7

相容的卡巴斯基應用程式和解決方案

不同產品的產品授權所授權的 Kaspersky 應用程式與解決方案組合各不相同。

您可以透過卡巴斯基安全管理中心雲端主控台部署和管理以下 Kaspersky 應用程式與解決方案：

- Kaspersky Security for Windows Server 11.0.1
- Kaspersky Endpoint Security 12.4 for Windows
- Kaspersky Endpoint Security 12.0 for Linux
- Kaspersky Endpoint Security 12.0 for Mac
- Kaspersky Embedded Systems Security 3.3 for Windows
- Kaspersky Embedded Systems Security 3.3 for Linux
- Kaspersky Endpoint Agent 3.16
- Kaspersky Endpoint Security for Android
- Kaspersky Security for iOS

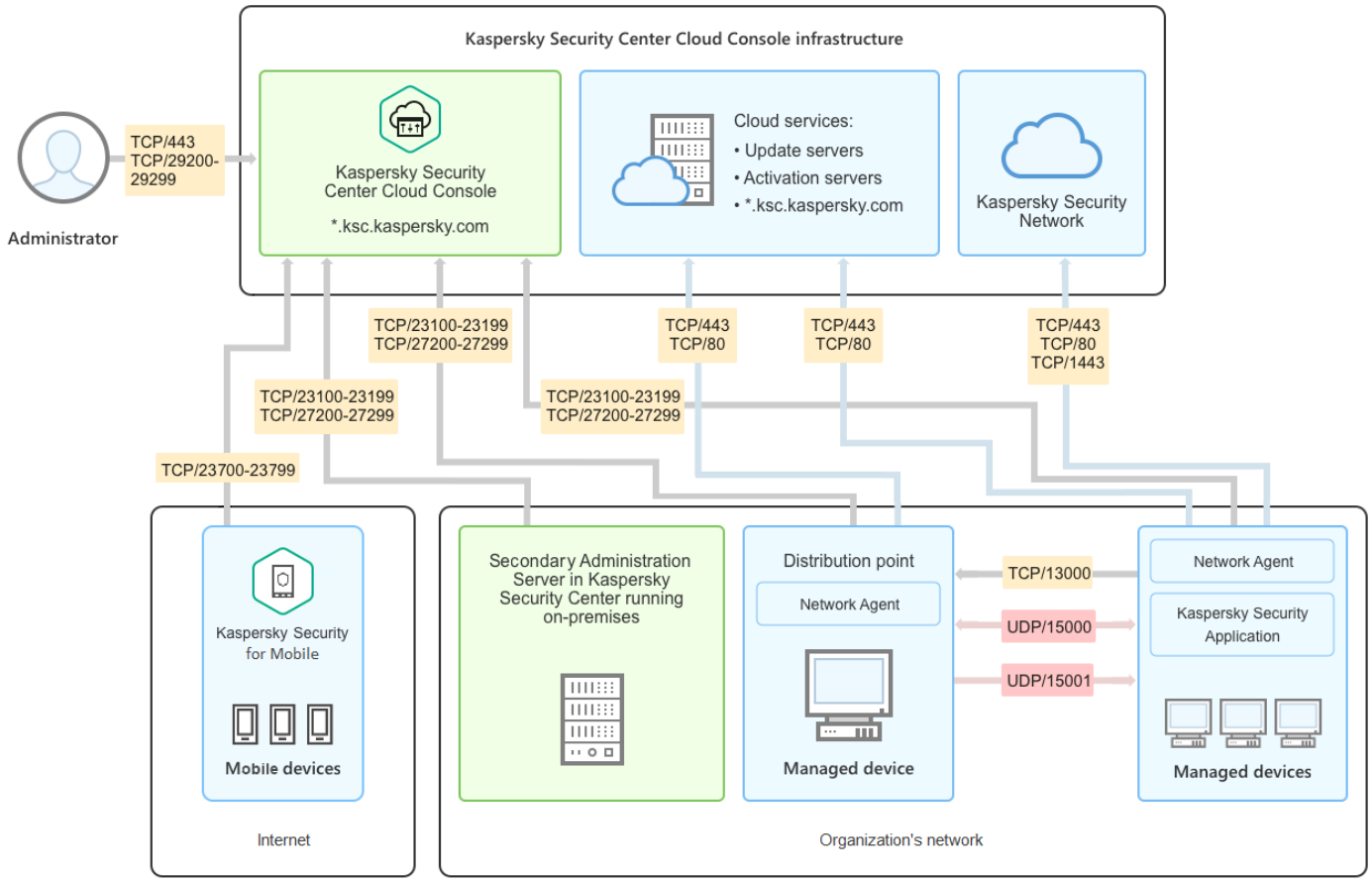
您可以整合以下解決方案以檢視和處理安全事件：

- Kaspersky Managed Detection and Response
- Kaspersky Endpoint Detection and Response Optimum 2.3
- Kaspersky Endpoint Detection and Response Expert

如果您在受管理裝置上安裝新的應用程式版本，但對新的應用程式版本使用過時的政策而不更新政策，則應用程式仍會提供資料給卡巴斯基安全管理中心雲端主控台，但卡巴斯基安全管理中心雲端主控台無法對這些資料進行說明文件的為受管理應用程式處理的資料一節所述的處理。為了讓卡巴斯基安全管理中心雲端主控台能夠處理這些資料，您必須為新版本的應用程式建立新政策。

架構

本節說明卡巴斯基安全管理中心雲端主控台各元件和其之間的互動。



卡巴斯基安全管理中心雲端主控台架構

透過雲端型主控台管理的卡巴斯基安全管理中心雲端主控台主要由兩部分元件組成，即：卡巴斯基安全管理中心雲端主控台基礎架構，以及客戶的基礎架構。

卡巴斯基安全管理中心雲端主控台基礎架構由以下部分組成：

- **雲端型管理主控台**。提供 Web 介面，用以為用戶端組織的網路建立和維護受卡巴斯基安全管理中心雲端主控台管理的防護系統。
- **雲端服務**。包含更新伺服器和啟動伺服器。
- **卡巴斯基安全網路 (KSN)**。一群包含 Kaspersky 資料庫的伺服器，這些資料庫含有持續更新的檔案、網路資源與軟體信譽資訊。卡巴斯基安全網路確保在遇到未知威脅時 Kaspersky 應用程式能夠做出更快速的回應，提高某些防護元件的效能並降低誤報的可能性。

客戶的基礎架構可能會由以下部分組成：

- **發佈點**。指安裝了網路代理的電腦，用以分發更新、輪詢網路、遠端安裝應用程式、取得管理群組（與/或廣播網域）內電腦的資訊。管理員需選取適當的裝置，然後手動將該裝置分配為發佈點。
- **受管理裝置**。客戶的網路內透過卡巴斯基安全管理中心雲端主控台來保護的電腦。每個受管理裝置上均必須安裝網路代理和 Kaspersky 安全應用程式。
- **內部部署運作的從屬管理伺服器**（可選）。您可以使用一台內部部署的管理伺服器來建立管理伺服器階層。

卡巴斯基安全管理中心雲端主控台使用的連接埠

若要使用卡巴斯基安全管理中心雲端主控台（位於 Kaspersky 基礎架構中），您必須在用戶端裝置開啟下列連接埠，以便允許網際網路連線（請參閱下表）：

為了允許網際網路連線，用戶端裝置上必須開啟的連接埠

連接埠（或連接埠範圍）	協定	連接埠（或連接埠範圍）的用途
23100-23199	TCP/TLS	在卡巴斯基安全管理中心雲端主控台管理伺服器（位於 *.ksc.kaspersky.com）接收來自網路代理和從屬管理伺服器的連線。 Kaspersky 基礎架構可能會使用此範圍內的任何連接埠以及此遮罩內的任何網址。此連接埠與網址可能會不時變更。
23700-23799 （僅當您在管理行動裝置時）	TCP/TLS	接收來自行動裝置的連線。 與卡巴斯基安全管理中心雲端主控台管理伺服器（位於 *.ksc.kaspersky.com）連線。 Kaspersky 基礎架構可能會使用此範圍內的任何連接埠以及此遮罩內的任何網址。此連接埠與網址可能會不時變更。
27200-27299	TCP/TLS	接收來自受管理裝置（但不包括行動裝置）的應用程式啟動連線。 與 Kaspersky Security Center Cloud Console 管理伺服器（位於 *.ksc.kaspersky.com）連線。 Kaspersky 基礎架構可能會使用此範圍內的任何連接埠以及此遮罩內的任何網址。連接埠和網址可能會不時變更。
29200-29299	TCP/TLS	使用 klsctunnel 公用程式，借道卡巴斯基安全管理中心雲端主控台管理伺服器（位於 *.ksc.kaspersky.com）來開闢與受管理裝置的連線通道。 Kaspersky 基礎架構可能會使用此範圍內的任何連接埠以及此遮罩內的任何網址。此連接埠與網址可能會不時變更。
443	HTTPS	與卡巴斯基安全管理中心雲端主控台發現服務（位於 *.ksc.kaspersky.com）連線。 Kaspersky 基礎架構可能會使用此遮罩內的任何網址。
1443	TCP	與卡巴斯基安全網路連線
80	TCP	連線會用於在 *.digicert.com 檢查卡巴斯基安全管理中心憑證的有效性。 Kaspersky 基礎架構可能會使用此遮罩內的任何網址。

下表顯示了在安裝了網路代理的用戶端裝置上必須開啟的連接埠。

用戶端裝置上必須開啟的連接埠

連接埠號	協定	連接埠目的	範圍
15000	UDP	接收來自連線閘道（如有使用）的資料	管理用戶端裝置
15000	UDP 廣播	取得同一個廣播網域內其他網路代理的相關資料	傳送更新和安裝套件
15001	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

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

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

下表列出在安裝了網路代理作為發佈點的用戶端裝置上，必須額外開啟的連接埠。

作為發佈點之網路代理所用的連接埠

連接埠號	協定	連接埠目的	範圍
13000	TCP/TLS	接收從網路代理的連線	管理用戶端裝置以及傳送更新和安裝套件
13111 （僅在裝置上執行了 KSN 代理服務時）	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
13295 （僅當您將發佈點用作推送伺服器時）	TCP/TLS	向受管理裝置傳送推送通知	用作推送伺服器的發佈點
15111 （僅在裝置上執行了 KSN 代理服務時）	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
17111 （僅在裝置上執行了 KSN 代理服務時）	HTTPS	接收從受管理裝置到 KSN 代理伺服器的請求	KSN 代理伺服器

如果主管理伺服器是位於 Kaspersky 基礎架構，而您網路中的一或多台管理伺服器是作為從屬管理伺服器，則請參閱內部部署運作的卡巴斯基安全管理中心所用的連接埠清單。請使用其中所列的連接埠，讓您的從屬管理伺服器與用戶端裝置之間能夠進行互動。

卡巴斯基安全管理中心雲端主控台的介面

您是透過 Web 介面管理卡巴斯基安全管理中心雲端主控台。

應用程式視窗中會包含以下項目：

- 視窗左側的主功能表
- 視窗右側的工作區

主功能表

主功能表會包含以下區段：

- **介紹與教程**。包含有關如何設定和使用卡巴斯基安全管理中心雲端主控台與安全應用程式的影片。

  在 Mozilla Firefox 瀏覽器中，如果您以彈出視窗播放**介紹與教程**區段中的影片，接著以子母畫面模式開啟該影片，再關閉彈出視窗中的影片，則子母畫面模式的影片也會跟著關閉。

- **管理伺服器**。顯示您目前所連管理伺服器的名稱。點擊設定圖示 () 會開啟管理伺服器內容。
- **監控和報告**。提供您基礎架構、防護狀態和統計資訊的總覽。
- **資產（裝置）**。包含用於管理用戶端裝置的工具，並且包含工作和 Kaspersky 應用程式政策。
- **使用者和角色**。可讓您管理使用者和角色、透過向使用者分配角色來設定使用者權限，以及為角色設定關聯的政策設定檔。

- **操作**。包含應用程式產品授權、修補程式管理、協力廠商應用程式管理等各種操作。其中還可讓您存取應用程式儲存區。
- **發現和佈署**。可讓您輪詢網路來發現用戶端裝置，以及手動或自動分發裝置到管理群組。其中還包含快速啟動精靈和防護佈署精靈。
- **市場**。包含完整 Kaspersky 業務解決方案系列的資訊，可讓您選取所需的解決方案，然後繼續在 Kaspersky 網站購買這些解決方案。
- **設定**。包含將卡巴斯基安全管理中心雲端主控台與其他 Kaspersky 應用程式整合的設定。其中還包含您個人的介面外觀相關設定，例如介面語言或主題。
- **您的帳戶功能表**。包含線上說明的連結以及 Kaspersky 技術支援的資訊。其中還能讓您登出卡巴斯基安全管理中心雲端主控台。

工作區

工作區會顯示您在應用程式 Web 介面視窗的區段中所選擇檢視的資訊。其中還會包含供您設定資訊顯示方式的控制元素。

卡巴斯基安全管理中心雲端主控台的本地化版本

卡巴斯基安全管理中心雲端主控台的介面和說明文件以下列語言提供：

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

卡巴斯基安全管理中心與卡巴斯基安全管理中心雲端主控台的比較

您可以以下列方式使用卡巴斯基安全管理中心：

- 以雲端解決方案的形式

  卡巴斯基安全管理中心是為您安裝在雲端環境中，而 Kaspersky 會以服務的形式讓您存取管理伺服器。您可以透過以雲端為基礎名為卡巴斯基安全管理中心雲端主控台的管理主控台來管理網路安全系統。此主控台的介面與卡巴斯基安全管理中心網頁主控台類似。

- 以內部部署的解決方案形式（基於 Windows 或基於 Linux）

  卡巴斯基安全管理中心由您安裝在本機裝置上後，您透過以 Microsoft Management Console 為基礎的管理主控台或是卡巴斯基安全管理中心網頁主控台來管理網路安全系統。

  除了基於 Windows 的應用程式，還有卡巴斯基安全管理中心 Linux 可用。卡巴斯基安全管理中心 Linux 乃專為滿足純 Linux 環境的需求而造，會使用基於 Linux 的管理伺服器在 Linux 裝置上部署和管理防護。基於 Windows 的卡巴斯基安全管理中心和卡巴斯基安全管理中心 Linux 所含的功能組合各有不同。

下表可供您比較卡巴斯基安全管理中心和卡巴斯基安全管理中心雲端主控台的主要功能特色。

內部部署運作與雲端解決方案形式的卡巴斯基安全管理中心功能比較

功能或內容	內部部署運作的卡巴斯基安全管理中心 14	卡巴斯基安全管理中心雲端主控台
管理伺服器地點	內部部署	雲端
資料庫管理系統 (DBMS) 地點	內部部署	雲端
網頁型管理主控台	✓	✓
維護管理伺服器和 DBMS	由客戶管理	由 Kaspersky 管理
管理伺服器階層	✓	✓（卡巴斯基安全管理中心雲端主控台的管理伺服器在階層中只能擔任主管理伺服器，並且只能用於政策和工作監控）
管理群組階層	✓	✓
將受管理裝置和相關物件從內部部署的卡巴斯基安全管理中心移轉到卡巴斯基安全管理中心雲端主控台	✓	✓
網路輪詢	✓	✓（僅能由發佈點進行）
受管理裝置的最大數量	100,000	25,000
保護 Windows、Linux 和 macOS 受管理裝置	✓	✓
對行動裝置的防護	✓	✓（僅支援 Kaspersky Endpoint Security for Android 和 Kaspersky Security for iOS）
對公有雲端基礎結構的防護	✓	✓
以裝置為中心的安全管理	✓	✓
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 代理伺服器	✓	✓（僅限在發佈點上）
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	✓	✓
將受管理裝置切換給另一台管理伺服器	✓	–

		（您必須在受管理裝置上重新安裝網路代理，才能將它們切換給另一台管理伺服器）
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	✓	✓ （目的為修正協力廠商軟體弱點，僅能安裝建議的修正程式）
受管理裝置上所發生事件的通知	✓	✓
建立和管理使用者帳戶	✓	✓
資料庫中的最大事件數量	400,000 （最多可增加至 45,000,000）	400,000 （取決於受管理裝置的數量）
與 SIEM 系統整合	✓	✓ （僅限使用 Syslog 格式和 TLS over TCP 通訊協定）
使用管理伺服器作為 WSUS 伺服器	✓	–
監控政策和工作的狀態	✓	✓
支援管理群組中的叢集和伺服器陣列	✓ （僅限基於 MMC 的管理主控台）	–
遠端安裝作業系統	✓	–
SNMP 支援	✓	–

基本概念

本節解釋與卡巴斯基安全管理中心雲端主控台相關的基本概念。

網路代理

管理伺服器與裝置之間的互動是由卡巴斯基安全管理中心雲端主控台的*網路代理*元件執行。所有裝置只要安裝了要用卡巴斯基安全管理中心雲端主控台管理的 Kaspersky 應用程式，均還必須安裝網路代理。

網路代理是以服務的形式安裝在裝置上，並設有以下屬性：

- 名稱為"卡巴斯基安全管理中心網路代理"
- 設定為在作業系統啟動時自動啟動
- 使用 LocalSystem 帳戶

安裝了網路代理的裝置被稱為*受管理裝置*或*裝置*。您可以在 Windows、Linux 或 Mac 裝置上安裝網路代理。

網路代理啟動的處理程序名稱叫 *klnagent.exe*。

網路代理同步管理伺服器的受管理裝置。卡巴斯基安全管理中心雲端主控台每小時都會自動讓管理伺服器與受管理裝置之間同步多次。管理伺服器會視受管理裝置的數量來設定同步間隔（簡稱*心跳*）。

管理群組

管理群組（以下簡稱*群組*）是一種將符合特定特徵的受管理裝置集結在一起的邏輯集合，目的是要在卡巴斯基安全管理中心雲端主控台內將這些裝置作為單一單位來管理。

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。

管理伺服器階層

管理伺服器可互相排列成「主/從屬」階層。每個管理伺服器都可以有多個從屬管理伺服器位於階層內的不同嵌套等級。從屬管理伺服器可位於的嵌套等級不受限制。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。

卡巴斯基安全管理中心雲端主控台管理伺服器只能擔任主管理伺服器，而其從屬伺服器只能是內部部署運作的管理伺服器。

要從內部部署運作的管理伺服器移轉到卡巴斯基安全管理中心雲端主控台管理伺服器時，您可以將管理伺服器排列成階層。然後，您可以只將一部分的受管理裝置轉移給卡巴斯基安全管理中心雲端主控台管理伺服器管理，藉以減少移轉的影響。其餘受管理裝置則仍由內部部署的管理伺服器管理。透過這種方式，您可以用有限數量的受管理裝置測試卡巴斯基安全管理中心雲端主控台的管理功能。同時，您還可以設定政策、工作、報告和其他物件，以便測試對您整個網路進行管理和監控的效果。必要時，您可以切換回內部部署的管理伺服器上所設定的物件。

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。請使用相關功能，根據網路特徵來在不同管理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（簡稱*虛擬伺服器*）是卡巴斯基安全管理中心雲端主控台的一個元件，可用於需要對個別用戶端組織的網路進行病毒防護管理時。每個虛擬管理伺服器都可以有自己的管理群組結構以及管理與監控方式（例如政策、工作、報告和事件）。虛擬管理伺服器的功能特性很適合工作流程複雜的組織。

虛擬管理伺服器具有以下限制：

- 僅有在正式模式的卡巴斯基安全管理中心雲端主控台中，才支援使用虛擬管理伺服器。
- 虛擬管理伺服器不支援建立從屬管理伺服器（包括虛擬伺服器在內）。
- 您無法將虛擬管理伺服器從卡巴斯基安全管理中心移轉到卡巴斯基安全管理中心雲端主控台。
- 虛擬管理伺服器無法有專門的管理員來管理。管理主管理伺服器的管理員預設還會管理所有的虛擬管理伺服器。
- 在虛擬伺服器上建立的使用者在管理伺服器上無法被分配到角色。
- 在虛擬管理伺服器內容視窗中，能調整的區域是有限的。

發佈點

*發佈點*是指安裝了網路代理的裝置，用於分發更新、遠端安裝應用程式，以及擷取網路裝置的資訊。發佈點可執行以下功能：

- 將更新和安裝套件分發到群組內的用戶端裝置上（包括透過 UDP 進行多點傳送分發）。所分發的更新可以是透過執行為發佈點建立的更新工作，從卡巴斯基更新伺服器接收而來。

  執行 macOS 的發佈點裝置無法從 Kaspersky 更新伺服器下載更新。

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

- 使用 UDP 透過多點傳送發佈政策和群組工作。

- 用作管理群組中的裝置與管理伺服器的連線閘道。

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

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

- 輪詢網路以偵測新裝置並更新現有裝置的資訊。

- 透過 Microsoft Windows 工具執行協力廠商軟體和 Kaspersky 程式的遠端安裝，包括在無網路代理的用戶端裝置上的安裝。

  此功能可讓您向管理伺服器無法直接觸及的網路中的用戶端裝置，遠端傳輸網路代理安裝套件。

- 作為代理伺服器參與卡巴斯基安全網路。

  > 執行 Linux 或 macOS 的發佈點裝置並不支援此功能。

  您可以在發佈點端啟用 KSN 代理伺服器，使裝置化身為 KSN 代理伺服器。在此情況下，裝置上會執行 KSN 代理服務 (ksnproxy)。

檔案透過 HTTP（如果啟用了 SSL 連線，則透過 HTTPS）從管理伺服器傳輸到發佈點。使用 HTTP 或 HTTPS 時，流量會較使用 SOAP 少，因此效能等級會更高。

在裝置上安裝網路代理後，就必須依管理群組手動將裝置分配為發佈點。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。不過，擔任發佈點的裝置可以不位於所獲配的管理群組中。如果已在管理群組的階層中分配幾個發佈點，則受管理裝置的網路代理會連線在階層上最近的發佈點。

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

> 卡巴斯基安全管理中心雲端主控台會向每個網路代理各分配一個與其他位址不同的唯一 IP 多點傳送位址。這可讓您避免可能會因 IP 重疊而起的網路超載。

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

> 發佈點狀態 (*Active/Standby*) 會顯示在 klnagchk 報告中，旁邊還附帶一個核取方塊。

一個發佈點需要至少 4 GB 的可用磁碟空間。如果發佈點的可用磁碟空間少於 2 GB，卡巴斯基安全管理中心雲端主控台會建立重要性等級為 *警告*的安全問題。安全問題會發佈於裝置內容中的**事件區域**。

在分配為發佈點的裝置上，執行遠端安裝工作將需要額外的可用磁碟空間。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將需要額外的可用磁碟空間。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。

管理 Web 外掛程式

透過卡巴斯基安全管理中心雲端主控台遠端管理 Kaspersky 軟體時，需使用一種特殊元件，即*管理 Web 外掛程式*。在下方，管理 Web 外掛程式又稱為*管理外掛程式*。管理外掛程式是一種讓卡巴斯基安全管理中心雲端主控台與特定 Kaspersky 應用程式相互銜接的介面。使用管理外掛程式，您可以配置應用程式工作和政策。

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雲端主控台中用於顯示應用程式的操作資料與事件以及用戶端裝置所提供統計資訊的功能

政策

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

政策狀態

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

政策會根據以下規則執行：

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

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

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

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

政策設定檔會根據以下規則執行：

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

政策設定檔

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

為了協助您避免重複建立相同的政策，卡巴斯基安全管理中心雲端主控台可讓您建立*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。

本機應用程式設定與政策的關係

您可以使用政策為群組中的所有裝置設定完全相同的應用程式設定值。

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

應用程式在用戶端裝置上使用的設定的值由政策設定的鎖定（🔒）位置確定：

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

用戶端裝置上執行工作時，應用程式以兩種不同的方式決定使用的設定：

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

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

授權使用應用程式

本節提供與應用程式產品授權相關的資訊。

卡巴斯基安全管理中心雲端主控台產品授權：情境

依此情境操作後，您將可以獲得產品授權來開始使用卡巴斯基安全管理中心雲端主控台以及受管理的安全應用程式。

卡巴斯基安全管理中心雲端主控台可讓您以集中化方式將 Kaspersky 應用程式的產品授權金鑰分發到用戶端裝置上、監控其使用情況，以及續訂產品授權。

如果您已在使用卡巴斯基安全管理中心雲端主控台，可以造訪卡巴斯基市場檢視完整系列的 Kaspersky 業務解決方案、選取所需的解決方案，然後繼續在 Kaspersky 網站進行購買。

在購買產品授權之前，先以試用模式觀察卡巴斯基安全管理中心雲端主控台的功能

卡巴斯基安全管理中心雲端主控台可先讓您免費試用。若要如此做，請建立一個試用工作區，該工作區過 30 天後即會終止。如果您想要有一個可以無限使用的正式工作區，則必須購買產品授權。

試用模式之後無法讓您切換為正式模式。等 30 天期限一到，任何試用工作區和其所有內容都將自動刪除。

階段

此情境分幾個階段進行：

1. **取得啟動碼來獲得讓卡巴斯基安全管理中心雲端主控台以正式模式運作的產品授權。購買一或多種產品授權**

   不同的產品授權所授權的 Kaspersky 應用程式與服務各有不同，因此您可能會需要購買多種產品授權。

   查看您可以購買哪些產品授權以及每種產品授權的最小裝置數量。

   有多項 Kaspersky 解決方案都會隨附卡巴斯基安全管理中心雲端主控台。請選擇您想要使用的解決方案，然後購買該解決方案的產品授權。如果您想要購買涵蓋 10,000 台（含）以上裝置的產品授權，則需要聯絡 Kaspersky 或 Kaspersky 的合作夥伴來提出特殊請求。

   使用此表格查看各產品授權所授權的弱點和修補程式管理功能有哪些。

   如果您想要在 Microsoft Azure 等雲端環境中使用卡巴斯基安全管理中心雲端主控台，請閱讀瞭解雲端環境適用的產品授權選項。

   如果您是管理服務提供商 (MSP)，請閱讀 MSP 適用的卡巴斯基安全管理中心雲端主控台產品授權資訊。

2. **在建立工作區時啟動卡巴斯基安全管理中心雲端主控台**

   您需在建立工作區時，指定產品授權金鑰來啟動卡巴斯基安全管理中心雲端主控台。

   如果您有多個產品授權金鑰，請指定其中任何一個產品授權金鑰，之後您必須在卡巴斯基安全管理中心雲端主控台中新增其他產品授權金鑰，以便啟動受管理的 Kaspersky 應用程式。

3. **將受管理應用程式的產品授權金鑰新增至管理伺服器儲存區**

   您必須先將產品授權金鑰新增至管理伺服器儲存區，才能部署這些產品授權金鑰。

   您在建立工作區時指定的產品授權金鑰會自動新增至管理伺服器儲存區。

如果您有多個產品授權金鑰，請逐一將這些產品授權金鑰新增至卡巴斯基安全管理中心雲端主控台管理伺服器儲存區。

4. **部署受管理應用程式的產品授權金鑰**

   選擇一種方法來將產品授權金鑰部署至所有要保護的裝置：

   - 自動佈署

     如果您使用多種不同的受管理應用程式，且必須為應用程式部署特定啟動碼，請選擇另一種方式部署該啟動碼。

     卡巴斯基安全管理中心可讓您自動將可用的產品授權金鑰部署到受管理應用程式。例如，三個產品授權金鑰被儲存在管理伺服器儲存區。您對這三個產品授權金鑰都啟用了**自動分發產品授權金鑰到受管理裝置**核取方塊。Kaspersky 安全應用程式—例如，Kaspersky Endpoint Security for Windows—被安裝到組織裝置。系統發現裝置上新出現了需要部署產品授權金鑰的受管理應用程式。假設儲存區中有兩個可部署到受管理裝置上的產品授權金鑰：名為 *Key_1*的產品授權金鑰和名為 *Key_2*的產品授權金鑰。其中只有一個產品授權金鑰會被部署到受管理應用程式。在此情況下，並無法預測這兩個產品授權金鑰中的哪一個會被部署到裝置，因為產品授權金鑰的自動部署程序並未為管理員提供任何進行管理活動的機會。

     產品授權金鑰每部署一次，該產品授權金鑰的安裝數量就會重計一次。您必須確保部署產品授權金鑰的應用程式數量不超過產品授權限制。如果安裝數量超過產品授權限制，則所有未獲產品授權涵蓋的裝置都會被分配為*緊急*狀態。

     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

   - 透過為受管理應用程式新增產品授權金鑰工作佈署。

     如果您選擇對受管理應用程式使用「新增產品授權金鑰」工作，您可以選取必須部署到裝置的產品授權金鑰，然後以任何對您方便的方式選取裝置（例如，透過選取管理群組或裝置分類）。

     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。

5. **檢查受管理 Kaspersky 應用程式已在哪些裝置上啟動**

   為了確保產品授權金鑰已獲正確部署，請檢視特定應用程式所用產品授權金鑰的清單。

6. **設定與產品授權到期相關的事件**

   設定事件，以便在您的產品授權金鑰用完或即將到期時收到通知：

   - 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

關於卡巴斯基安全管理中心雲端主控台的試用模式

*試用模式*是卡巴斯基安全管理中心雲端主控台的一種特殊模式，目的在讓使用者能夠先觀察熟悉卡巴斯基安全管理中心雲端主控台的功能。在此模式下，您可以在具有 30 天效期限制的工作區內執行活動。試用模式會在您建立試用工作區的當下自動啟動。試用模式提供的功能組合與標準 Kaspersky Endpoint Security for Business Advanced 產品授權完全相同。

因為需要特殊產品授權的功能並不受支援，所以您無需在卡巴斯基安全管理中心雲端主控台中取得管理伺服器的產品授權。如果您想以試用模式使用卡巴斯基安全管理中心雲端主控台，您在建立第一個工作區時，即會自動獲得試用產品授權。

之後，您無法直接從試用模式切換為正式模式。等 30 天期限一到，任何試用工作區和其所有內容都會自動刪除。

以試用模式使用卡巴斯基安全管理中心雲端主控台功能時，具有以下限制：

- 您無法建立管理伺服器階層。您無法建立虛擬管理伺服器。
- **產品授權**區段為唯讀狀態。您在此區段無法進行任何操作，包括新增和移除產品授權金鑰。
- 您無法建立自訂安裝套件。
- 您無法為使用者建立自訂角色。
- 「病毒爆發」功能無法使用。不會儲存病毒爆發事件，也不會傳送任何通知。
- **刪除的物件**儲存區無法使用。
- 您無法啟用將批次處理事件（大量發佈的事件）新增至資料庫。
- 不支援將管理伺服器從內部部署模式移轉到雲端主控台模式。
- 來自管理伺服器元件（例如管理伺服器或網路代理）的 KSN 統計資訊不會傳送給 Kaspersky。

建立應用程式的某些物件時，也會有一些限制（請參閱下表）。如果嘗試建立這類物件時，超過了其中任何限制，則會無法建立物件，而且會顯示關於該限制的錯誤訊息。

以試用模式建立卡巴斯基安全管理中心雲端主控台物件時的限制

限制類型	參數值
政策	8
工作	17
產品授權金鑰	1
安裝套件	5
裝置分類（不包括預先設好的實例）	5
事件分類（不包括預先設好的實例）	5
裝置移動規則	3
相同類型的報告範本	10

內部安全群組	20
受管理裝置	20

使用卡巴斯基市場選擇卡巴斯基商業解決方案

市場是主功能表中的一個區段，可讓您檢視整個 Kaspersky 業務解決方案範圍，選擇您需要的解決方案，然後在 Kaspersky 網站上進行購買。您可以使用篩選器僅檢視適合您的組織和資訊安全系統要求的那些解決方案。當您選取解決方案後，卡巴斯基安全管理中心雲端主控台會將您重新導向 Kaspersky 網站上的相關網頁，以瞭解該解決方案的更多資訊。每個網頁都可讓您繼續購買或包含有關購買流程的指示。

在 **市場** 區段，您可以使用以下條件篩選 Kaspersky 解決方案：

- 您想要防護的裝置（端點、伺服器和其他類型的資產）數量：
  - 50–250
  - 250–1000
  - 大於 1000
- 貴組織資訊安全團隊的成熟度：
  - **基金會**

    此級別對於只有一個 IT 團隊的企業來說很典型。自動封鎖最大可能數量的威脅。
  - **最佳**

    此級別對於在 IT 團隊內具有特定 IT 安全功能的企業很典型。在此級別，公司需要能夠讓他們應對商品威脅和繞過現有預防機制的威脅的解決方案。
  - **專家**

    此級別對於具有復雜和分佈式 IT 環境的企業來說很典型。IT 安全團隊成熟或公司有 SOC（安全運營中心）團隊。所需解決方案使公司能夠應對複雜的威脅和有針對性的攻擊。
- 您想要防護的資產類型：
  - **端點**：員工工作站、實體和虛擬機、內嵌系統
  - **伺服器**: 實體和虛擬伺服器
  - **雲端**：公有、私有或混合雲端環境；雲端服務
  - **網路**：區域網路，IT 基礎結構
  - **服務**：Kaspersky 提供的安全相關服務

若要查找和購買 Kaspersky 業務解決方案：

1. 在主功能表中，轉至 **市場**。

   預設情況下，該區段顯示所有可用的 Kaspersky 業務解決方案。
2. 要僅檢視適合您組織的解決方案，請在篩選器中選擇所需的值。

3. 點擊您想要購買或了解更多資訊的解決方案。

您將被重新導向到解決方案網頁。您可以按照熒幕上的指示進行購買。

各種產品授權和其最小裝置數量

如果您想以正式模式使用卡巴斯基安全管理中心雲端主控台，則必須在建立第一個工作區前就購買產品授權。下表顯示了您可以購買的產品授權以及每種產品授權的最小裝置數量（即便您想要保護的裝置數量小於該數量也一樣）：

會授予卡巴斯基安全管理中心雲端主控台使用權限的產品授權

產品授權	最小裝置數量（即便您想保護的裝置數量較少也一樣）
Kaspersky Endpoint Security for Business Select	如為正式產品授權：300 如為正式（訂購）產品授權：100
Kaspersky Endpoint Security for Business Advanced	如為正式產品授權：300 如為正式（訂購）產品授權：100
Kaspersky Total Security for Business	300
Kaspersky Endpoint Detection and Response Optimum	如為正式產品授權：300 如為正式（訂購）產品授權：100
Kaspersky Endpoint Detection and Response Expert	50
Kaspersky Hybrid Cloud Security（電腦）	如為正式產品授權：300 如為正式（訂購）產品授權：100
Kaspersky Hybrid Cloud Security（伺服器）	50
Kaspersky Hybrid Cloud Security（核心）	20
Kaspersky Hybrid Cloud Security (CPU)	20
Kaspersky Hybrid Cloud Security Enterprise（電腦）	如為正式產品授權：300 如為正式（訂購）產品授權：100
Kaspersky Hybrid Cloud Security Enterprise（伺服器）	50
Kaspersky Hybrid Cloud Security Enterprise (CPU)	20
Kaspersky Embedded Systems Security	300
Kaspersky Embedded Systems Security Compliance Edition	300
Kaspersky Symphony（目前僅在俄羅斯提供）	300
Kaspersky Next EDR Foundations	300 位使用者（每個使用者產品授權各可套用於 1 台 PC/Mac 裝置和 2 台行動裝置）
Kaspersky Next EDR Optimum	300 位使用者（每個使用者產品授權各可套用於 1 台

	PC/Mac 裝置和 2 台行動裝置）
Kaspersky Next XDR Expert	250 位使用者（每個使用者產品授權各可套用於 1 台 PC/Mac 裝置和 2 台行動裝置）

每一工作區的最大裝置數量為 25,000 台。如果要保護超過 10,000 台裝置，則需要建立不同的工作區。若要如此做，請向 Kaspersky 技術支援傳送請求。請求中必須包含以下資訊：

- **使用者電子郵件** — 使用者在卡巴斯基安全管理中心雲端主控台註冊的電子郵件地址。此使用者會被授予所建立工作區的管理員權限。

  您在卡巴斯基安全管理中心雲端主控台建立帳戶後，無需註冊公司和為其建立工作區。請在請求中指明公司與工作區的資訊。

- **公司名稱** — 您要將卡巴斯基安全管理中心雲端主控台用於的公司本身的名稱。
- **公司所在國家/地區** — 公司所在的國家/地區。
- **工作區名稱** — 要為公司建立的工作區名稱。
- **預估端點計數** — 您要在新工作區中保護的用戶端裝置（包括行動裝置）總數。
- **工作區所在國家/地區** — 您要讓新工作區位於的國家/地區。此參數會影響選擇來儲存工作區的資料中心。

  請注意，如果您想要讓工作區位於美國或加拿大，請指定州或省來決定資料中心地區。

  公司所在國家/地區和**工作區所在國家/地區**參數可以相同。

- **啟動碼** — 您購買卡巴斯基安全管理中心雲端主控台後收到的啟動碼。請確定您要購買的產品授權可涵蓋所有必須保護的用戶端裝置。

傳送請求後，Kaspersky 專家會註冊指定的公司，然後為該公司建立工作區。當工作區建立完成時，您會收到一封電子郵件通知。您可以在卡巴斯基安全管理中心雲端主控台登入自己的帳戶來檢視結果。

超出了產品授權限制事件

卡巴斯基安全管理中心雲端主控台可讓您在用戶端裝置上安裝的 Kaspersky 應用程式數目超過一些產品授權限制時，取得該等事件的資訊。

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。

向受管理裝置分發啟動碼的方法

在受管理裝置上安裝 Kaspersky 應用程式後，這每個應用程式都必須套用啟動碼，才能取得產品授權。您無法使用金鑰檔案來取得受管理應用程式的產品授權；接受的僅有啟動碼。部署啟動碼的方式有以下幾種：

- 自動佈署
- 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

Kaspersky 應用程式可以同時使用多個產品授權金鑰。例如，Kaspersky Endpoint Security for Windows 可以使用兩個產品授權金鑰 — 一個用於 Kaspersky Endpoint Security for Windows，另一個用於啟動 Endpoint Detection and Response 功能。

此外，Kaspersky 應用程式不僅可以有作用中產品授權金鑰，還可以有備用產品授權金鑰。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。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。

新增產品授權金鑰到管理伺服器儲存區

使用卡巴斯基安全管理中心雲端主控台新增產品授權金鑰時，該金鑰的設定會儲存在管理伺服器上。應用程式會根據該資訊產生一份產品授權金鑰使用情況的報告，並通知管理員產品授權金鑰內容中指定的產品授權期滿日期，以及是否違反此限制。您可以在管理伺服器設定內配置產品授權金鑰使用情況的通知。

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. 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

Kaspersky Security Center Cloud Console 允許您自動或是透過新增金鑰工作，將產品授權金鑰分發至用戶端裝置。

部署前，請新增產品授權金鑰到管理伺服器儲存區。

若要透過新增金鑰工作，將產品授權金鑰分發至用戶端裝置：

1. 在主功能表中，轉至 **資產（裝置） → 工作**。
2. 點擊**新增**。
   新工作精靈啟動。使用**下一步**按鈕進行精靈。
3. 在**應用程式**下拉清單，選取要為其新增產品授權金鑰的應用程式。

4. 在**工作類型**清單，選取**新增金鑰**工作。

5. 在**工作名稱**欄位，指定新工作的名稱。

6. 選取要將工作分配到的裝置。

7. 在精靈的**選取產品授權金鑰**步驟，點擊**新增金鑰**連結以新增產品授權金鑰。

8. 在金鑰新增窗格，使用以下選項之一新增產品授權金鑰：

   如果您在建立新增金鑰工作之前，就已將產品授權金鑰新增至管理伺服器儲存區，則不需要新增產品授權金鑰。

   - 選取**輸入啟動碼**選項以輸入啟動碼，然後執行下列操作：

     a. 指定啟動碼，然後點擊**傳送**按鈕。
     金鑰新增窗格中即會顯示產品授權金鑰的資訊。

     b. 點擊**儲存**按鈕。

     如果要自動將產品授權金鑰分發至受管理裝置，請啟用**自動分發產品授權金鑰到受管理裝置**選項。

     金鑰新增窗格即會關閉。

   - 選取**新增金鑰檔案**選項以新增金鑰檔案，然後執行以下操作：

     a. 點擊**選取金鑰檔案**按鈕。

     b. 在開啟的視窗中，選取金鑰檔案，然後點擊**開啟**按鈕 。
     產品授權金鑰新增窗格中即會顯示產品授權金鑰的資訊。

     c. 點擊**儲存**按鈕。

     如果要自動將產品授權金鑰分發至受管理裝置，請啟用**自動分發產品授權金鑰到受管理裝置**選項。

     金鑰新增窗格即會關閉。

9. 在金鑰表格中選取產品授權金鑰。

10. 如果要將此金鑰用作備用金鑰，請在精靈的**產品授權資訊**步驟中，啟用**作為備用金鑰使用**選項。
    在這種情況下，備用金鑰將在活動金鑰過期後被套用。

11. 在精靈的**完成工作建立**步驟中啟用**建立完成時開啟工作詳情**選項，即可修改預設工作設定。
    如果您不啟用該選項，工作將以預設設定來建立。您可以稍後再修改預設設定。

12. 點擊**完成**按鈕。
    精靈即會建立物件。如果您啟用了**建立完成時開啟工作詳情**選項，工作內容視窗即會自動開啟。在此視窗中，您可以指定一般工作設定，並視需要變更在工作建立期間指定的設定。

您也可以透過在工作清單中點擊所建立工作的名稱，開啟工作內容視窗。

工作隨即受到建立、設定，並顯示在工作清單。

13. 若要執行工作，請在工作清單選取該工作，然後點擊**開始**按鈕。
    您也可以在工作內容視窗的**排程**頁籤上，設定工作啟動排程。
    如需排程啟動設定的詳細說明，請參閱一般工作設定。

工作完成後，產品授權金鑰即會佈署到所選裝置。

自動分發產品授權金鑰

如果產品授權金鑰位於管理伺服器上的產品授權金鑰儲存區，則卡巴斯基安全管理中心雲端主控台可以自動將這些金鑰分發至受管理裝置。

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，將切換按鈕切換至**自動分發產品授權金鑰到受管理裝置**。
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期間，系統會將產品授權的裝置數量限制納入考慮。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。

如果您對某個訂購產品授權金鑰指定**自動分發產品授權金鑰到受管理裝置**選項來啟動受管理裝置上的任何應用程式，同時您又具有有效的試用產品授權金鑰，那麼該試用產品授權金鑰將在到期日的八天前，自動被訂購產品授權金鑰取代。

檢視管理伺服器儲存區內使用中產品授權金鑰的資訊

若要檢視已新增至管理伺服器儲存區的產品授權金鑰清單，請

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

顯示的清單會包含已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

檢視特定 Kaspersky 應用程式所用產品授權金鑰的資訊

要了解在為 Kaspersky 應用程式使用哪些產品授權金鑰：

1. 在主功能表中，轉至 **資產（裝置）→ 受管理裝置**。
   若裝置屬於「未配置的裝置」群組，請改為前往 **發現和佈署 → 未配置的裝置**。
2. 點擊所需裝置的名稱。
3. 在開啟的裝置內容視窗中，選取**應用程式**區域。
4. 在開啟的應用程式清單中，選取您要檢視其產品授權金鑰的應用程式。
5. 在開啟的管理伺服器內容視窗中的**一般**頁籤，選取**產品授權金鑰**區段。
   該資訊將顯示在此區段的工作區中。

從儲存區刪除產品授權金鑰

您可以從管理伺服器儲存區中刪除產品授權金鑰。請注意，在以下情況下，卡巴斯基安全管理中心雲端主控台將在 90 天後自動刪除您的工作區：

- 您刪除了在儲存區中手動新增的最後一個產品授權金鑰（無論是作用中、備用還是未使用的金鑰）。
- 最後一個產品授權金鑰到期。

一旦您的工作區被刪除，您即無法透過卡巴斯基安全管理中心雲端主控台管理對您網路的防護。您在卡巴斯基安全管理中心雲端主控台中的資料也將永久遺失。如有必要，您可以手動刪除您的工作區。否則，我們建議您在管理伺服器儲存區中至少保留一個產品授權金鑰。

如果您刪除了產品授權金鑰，但您先前已新增備用產品授權金鑰，則在原先的作用中金鑰被刪除或到期後，備用產品授權金鑰將自動成為作用中產品授權金鑰。

如果您刪除的作用中產品授權金鑰已部署到受管理裝置上，應用程式將繼續在受管理裝置上運作。

若要從管理伺服器儲存區中刪除產品授權金鑰：

1. 檢查管理伺服器並未使用您要刪除的產品授權金鑰。如果管理伺服器使用了您將刪除的金鑰，您將無法刪除該金鑰。若要執行檢查：
   a. 在主功能表中，按一下管理伺服器旁邊的設定圖示（ ）。
      管理伺服器內容視窗將開啟。

b. 在**一般**頁簽上，選取**產品授權金鑰**區段。

c. 如果開啟的區段中顯示了所需的產品授權金鑰檔案，請點擊**刪除啟動產品授權金鑰**按鈕，然後確認操作。在此之後，管理伺服器將不會使用刪除的產品授權金鑰，但該金鑰仍保留在管理伺服器儲存區中。如果未顯示所需的產品授權金鑰，則管理伺服器並未使用該產品授權金鑰。

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

3. 選取所需的產品授權金鑰，然後點擊**刪除**按鈕。

4. 在出現的視窗中，選取**我理解風險並想要刪除產品授權金鑰**核取方塊。這表示您明白，如果您刪除最後一個產品授權金鑰，工作區之後也會遭刪除，而您將對受管理裝置失去控制能力。接著，點擊**刪除**按鈕。

如此一來，所選的產品授權金鑰即會將自儲存區中刪除。

您可以將已刪除的產品授權金鑰新增回來，或是新增新的產品授權金鑰。如果您刪除了最後一個產品授權金鑰，只要您的工作區尚未被刪除，您都還能新增產品授權金鑰。卡巴斯基安全管理中心雲端主控台會在刪除的 30 天、7 天與 1 天前，通知工作區的管理員。

檢視 Kaspersky 應用程式未獲啟動的裝置清單

您可以檢視所有已安裝某個 Kaspersky 應用程式但未加以啟動（例如，產品授權遺失或到期）之裝置的清單。

若要檢視未啟動某個 Kaspersky 應用程式的裝置：

1. 在主功能表中，轉至 **資產（裝置）→ 工作**。

   工作清單隨即顯示。

2. 點擊與所關心 Kaspersky 應用程式相關之更新工作的名稱。

   工作內容視窗會一起顯示數個命名的頁籤。

3. 在工作內容視窗中，選取**結果**區段。

   裝置欄中會顯示已成功執行該工作的裝置。

4. 將**裝置**欄進行排序。

   裝置欄中會顯示工作執行成功的裝置。因缺少產品授權而執行工作失敗的裝置，即為未將該應用程式啟動的裝置。

撤銷最終使用者產品授權協議的許可

若您決定停止防護您的一些用戶端裝置，您可針對任何受管理的 Kaspersky 應用程式撤銷最終使用者產品授權協議 (EULA)。您必須先解除安裝所選的應用程式和其安裝套件，才能撤銷其 EULA。安裝套件必須自管理伺服器和其虛擬管理伺服器中刪除。

在虛擬管理伺服器上接受的 EULA 可以在虛擬管理伺服器或主管理伺服器上撤銷。在主管理伺服器上接受的 EULA 只能在主管理伺服器上撤銷。

若要撤銷 Kaspersky 受管理應用程式的 EULA：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。

2. 在管理伺服器內容視窗的**一般**頁籤上，選取**最終使用者產品授權協議**區段。
   隨即會顯示在建立安裝套件期間或在無縫安裝更新期間接受的 EULA 清單。

3. 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
   - EULA 是否可供撤銷

4. 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
   - 與 EULA 連結的物件（安裝套件、無縫更新）及其名稱與類型的清單

5. 在 EULA 內容視窗的下部，點擊**撤銷產品授權協議**按鈕。
   如果所選的 EULA 只能透過解除安裝應用程式來撤銷，或是此 EULA 只能自主管理伺服器上撤銷，則顯示的會是關於該限制的通知，而非**撤銷產品授權協議**按鈕。

   > 若存在任何物件（安裝套件和其相關工作）使 EULA 無法撤銷，則會顯示相關通知。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。

6. 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。

如果最後一個產品授權金鑰到期，則卡巴斯基安全管理中心雲端主控台會在 90 天後自動刪除您的工作區。因此，您將無法透過卡巴斯基安全管理中心雲端主控台管理對您網路的防護。您在卡巴斯基安全管理中心雲端主控台中的資料也將永久遺失。我們建議您續訂過期的產品授權金鑰，或是將新的產品授權金鑰新增至管理伺服器儲存區，以保住您的工作區。

若要檢視產品授權到期或即將到期的通知：

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，前往**監控和報告 → 控制板**，然後點擊通知旁邊的**檢視將到期的產品授權**連結。

   Kaspersky 產品授權視窗即會開啟，供您檢視和續訂即將到期和已到期的產品授權。

2. 如果要續訂產品授權，請點擊所需產品授權旁邊的**續約產品授權**連結。

   點擊產品授權續訂連結，即表示您同意向 Kaspersky 傳送以下資料：軟體 ID、軟體版本、軟體本地化版本、產品授權 ID，以及一個指出了產品授權是否由合作夥伴公司提供的屬性。這些資料為決定您產品授權的續訂期時所需。

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。

   產品授權即已續訂。

在卡巴斯基安全管理中心雲端主控台中，產品授權即將到期的通知會依以下排程顯示：

- 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

在產品授權到期後使用卡巴斯基安全管理中心雲端主控台

在產品授權到期後，Kaspersky 可能會授權您正常使用無功能限制的卡巴斯基安全管理中心雲端主控台最多 90 天。在這段期間，管理伺服器、網路代理和卡巴斯基安全管理中心雲端主控台Web 介面都會正常運作而未無功能限制。卡巴斯基安全管理中心雲端主控台也會根據目前的 KSN 存取設定，向 Kaspersky 傳送 KSN 統計資訊。受管理應用程式則僅會以有限功能運作（如需詳細資訊，請參閱這些應用程式的說明文件）。

當產品授權到期達 90 天時，卡巴斯基安全管理中心雲端主控台即會自動刪除您的工作區。如果您想保住工作區，請續訂至少一個到期的產品授權金鑰，或是將新的產品授權金鑰新增至儲存區。

卡巴斯基安全網路 (KSN)

該區域敘述如何使用卡巴斯基安全網路 (KSN) 的線上服務基礎架構。該區域提供了關於 KSN 的詳細敘述，介紹了如何啟用 KSN，設定對 KSN 的存取，並檢視 KSN 代理伺服器的使用統計。

關於 KSN

卡巴斯基安全網路 (KSN) 是一種線上服務組織結構，可提供對 Kaspersky 網路知識庫的存取，其中包含與檔案信譽、網路資源和軟體相關的資訊。使用卡巴斯基安全網路中的資料可確保在遇到未知威脅時 Kaspersky 程式能夠做出更快速的回應，提高某些防護元件的效能可降低誤報的風險。KSN 可讓您從 Kaspersky 信譽資料庫擷取用戶端裝置上所安裝應用程式的資訊。

如果您加入 KSN，即表示您同意以自動模式，向 Kaspersky 傳送透過卡巴斯基安全管理中心雲端主控台管理的用戶端裝置上所安裝 Kaspersky 應用程式的操作資訊。依照目前 KSN 存取設定傳送資訊。卡巴斯基分析師會另外分析收到的資訊，並將其包含在卡巴斯基安全網路的信譽和統計資料庫中。

在執行快速設定精靈時，應用程式會提示您加入 KSN。您使用應用程式時，隨時都可以開始或停止使用 KSN。

啟用 KSN 時，應根據閱讀與接受的 KSN 聲明啟用 KSN。如果 KSN 聲明已更新，則在更新或升級管理伺服器時會顯示給您。您可以接受更新的 KSN 聲明，也可以拒絕。如果您拒絕了它，那麼您將按照之前接受的 KSN 聲明的先前版本繼續使用 KSN。

啟用 KSN 後，卡巴斯基安全管理中心雲端主控台會檢查 KSN 伺服器是否可供存取。如果無法使用系統 DNS 存取伺服器，則應用程式使用公用 DNS 伺服器。這是為了確保維護受管理裝置的安全級別。

管理伺服器管理的用戶端裝置透過 KSN 代理伺服器與 KSN 互動。KSN 代理伺服器提供以下功能：

- 即使無法直接連線網際網路，用戶端裝置也可向 KSN 傳送請求以及向 KSN 傳送資訊。
- KSN 代理可暫存已處理的資料，進而減少對外頻寬消耗以及用戶端裝置等待 KSN 回覆而花費的時間。

您可以在發佈點端啟用 KSN 代理伺服器，使裝置化身為 KSN 代理伺服器。在此情況下，裝置上會執行 KSN 代理服務 (ksnproxy)。

啟用和停用 KSN

要啟用 KSN：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取 **KSN 設定**區段。
3. 將切換按鈕切換到**使用卡巴斯基安全網路 已啟用**位置。
   KSN 即會啟用。
   如果啟用了此切換按鈕，用戶端裝置將傳送修補程式安裝結果到卡巴斯基。啟用此切換按鈕時，您應閱讀並接受 KSN 聲明的條款。
4. 點擊**儲存**按鈕。

要停用 KSN：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取 **KSN 設定**區段。
3. 將切換按鈕切換至**使用卡巴斯基安全網路 已停用**位置。
   KSN 即會停用。
   如果停用此切換按鈕，用戶端裝置將不會傳送修補程式安裝結果到卡巴斯基。

4. 點擊**儲存**按鈕。

檢視接受的 KSN 聲明

啟用卡巴斯基安全網路 (KSN) 時，必須閱讀並接受 KSN 聲明。您可以隨時檢視已接受的 KSN 聲明。

若要檢視已接受的 KSN 聲明：

1. 在主功能表中，按一下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 **KSN settings**區段。
3. 點擊**檢視卡巴斯基安全網路聲明**連接。

在開啟的視窗中，您可以檢視接受的 KSN 聲明的文字。

接受更新的 KSN 聲明

啟用 KSN 時，應根據閱讀與接受的 KSN 聲明啟用 KSN。如果 KSN 聲明有所更新，則當您開啟卡巴斯基安全管理中心雲端主控台時，會自動顯示更新後的聲明。您可以接受更新的 KSN 聲明，也可以拒絕。如果您拒絕了它，那麼您將按照之前接受的 KSN 聲明的版本繼續使用 KSN。您可以稍後再檢視並接受更新後的 KSN 聲明。

若要檢視並接受或拒絕更新後的 KSN 聲明，請執行以下操作：

1. 點擊**檢視通知**主應用程式視窗右上角的連結。
   通知 視窗隨即開啟。
2. 點擊**檢視更新的 KSN 聲明**連結。
   卡巴斯基安全網路聲明更新視窗開啟。
3. 閱讀 KSN 聲明，然後透過按一下以下其中一個按鈕做出決定：
   - **我接受更新的 KSN 聲明**
   - **在舊聲明下使用 KSN**

根據您的選擇，KSN 會按照目前或更新的 KSN 聲明條款繼續有效。您可以隨時在管理伺服器屬性中檢視已接受的 KSN 聲明文字。

檢查發佈點是否作為 KSN 代理伺服器運作

在分配作為發佈點運作的受管理裝置上，可以啟用 KSN 代理伺服器。當 ksnproxy 服務在裝置上執行時，受管理裝置會作為 KSN 代理伺服器運作。您可以在本機裝置上檢查、開啟或關閉此服務。

您可以將基於 Windows 或基於 Linux 的裝置分配為發佈點。檢查發佈點的方法取決於該發佈點的作業系統。

若要檢查基於 Windows 的發佈點是否作為 KSN 代理伺服器運作，請執行以下操作：

1. 在發佈點裝置上的 Windows 系統中，開啟**服務**（**所有程序 → 管理工具 → 服務**）。

2. 在服務清單，檢查 ksnproxy 服務是否正在執行。

   如果 ksnproxy 服務正在執行，則裝置上的網路代理會加入卡巴斯基安全網路，並作為發佈點範圍內所管理裝置的 KSN 代理伺服器運作。

如果您想，您可以關閉 ksnproxy 服務。在這種情況下，發佈點上的網路代理停止參與卡巴斯基安全網路。該需要本機管理員權限。

若要檢查基於 Linux 的發佈點是否作為 KSN 代理伺服器運作，請執行以下操作：

1. 在發佈點裝置上，顯示正在執行的處理程序清單。

2. 在正在執行的處理程序清單中，檢查 `/opt/kaspersky/ksc64/sbin/ksnproxy` 處理程序是否正在執行。

如果 `/opt/kaspersky/ksc64/sbin/ksnproxy` 處理程序正在執行，則裝置上的網路代理會加入卡巴斯基安全網路，並作為發佈點範圍內所管理裝置的 KSN 代理伺服器運作。

產品授權定義

本節包含與針對透過卡巴斯基安全管理中心雲端主控台管理的 Kaspersky 應用程式取得產品授權相關的概念定義。

關於產品授權

*產品授權*是指依所簽署產品授權合約（《最終使用者產品授權協議》）的條款所授予在有限時間內使用卡巴斯基安全管理中心雲端主控台的權利。

服務範圍和有效期取決於用於根據其使用該應用程式的產品授權。

我們提供下列授權類型：

- *試用*

  用於試用此程式的免費產品授權。試用版產品授權通常擁有較短的有效期。

  當試用產品授權到期時，卡巴斯基安全管理中心雲端主控台所有功能都會停用。要繼續使用程式，您需要獲得正式版的產品授權。

  您只能在試用產品授權下使用該應用程式一個試用期。

- *正式*

  付費產品授權。

  當正式產品授權到期時，應用程式的主要功能將被停用。若要繼續使用卡巴斯基安全管理中心雲端主控台，您必須續訂正式產品授權。正式產品授權過期後，您將無法繼續使用該應用程式，必須將其從裝置中刪除。

  我們建議在產品授權到期之前進行續約，以確保防護不受中斷，抵禦所有安全威脅。

關於產品授權憑證

*產品授權憑證*是隨著您收到的一個金鑰檔案和啟動碼一起的檔案。

產品授權憑證提供以下的產品授權資訊：

- 產品授權金鑰或訂購號
- 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。

您可以透過在應用程式中輸入*啟動碼*來新增產品授權金鑰。為程式新增金鑰後，將在程式介面中顯示該產品授權金鑰的唯一字母數字序列。

如果違反產品授權協議的條款，Kaspersky 可能會封鎖產品授權金鑰。如果金鑰已被封鎖，要使用程式，您需要新增另外一個金鑰。

產品授權金鑰可以是啟用或備用的金鑰（或預留）。

*啟動產品授權金鑰*是應用程式目前使用的產品授權金鑰。啟動產品授權金鑰可以被新增為正式產品授權。應用程式只能擁有一個啟動產品授權金鑰。

*備用（或預留）產品授權金鑰*是允許使用者使用應用程式，但是目前未使用的產品授權金鑰。與目前產品授權金鑰相關聯的產品授權到期時，備用產品授權金鑰將自動成為目前產品授權金鑰。只有在新增啟動產品授權金鑰之後，才可以新增備用產品授權金鑰。

試用產品授權金鑰僅可以被當作啟動產品授權金鑰新增。試用產品授權金鑰不可以被當作備用產品授權金鑰新增。

關於啟動碼

*啟動碼*是一串由 20 個字元數字組成的唯一序列。您是透過輸入啟動碼來新增用於啟動卡巴斯基安全管理中心雲端主控台的產品授權金鑰。您是透過購買卡巴斯基安全管理中心雲端主控台時或預約試用版卡巴斯基安全管理中心雲端主控台後指定的電子郵件地址收到啟動碼。

若要使用啟動碼啟動應用程式，您需要網際網路來建立與 Kaspersky 啟動伺服器的連線。如果無法使用系統 DNS 存取伺服器，則應用程式使用公用 DNS 伺服器。

當程式被啟動碼啟動後，程式有時傳送有規律的請求到 Kaspersky 啟動伺服器，以便檢查目前產品授權金鑰狀態。您必須提供給程式網際網路連線以使其能夠傳送請求。

如果您在安裝應用程式後丟失了啟動碼，請聯繫從其購買產品授權的卡巴斯基合作夥伴。

您不能使用金鑰檔案來啟動受管理的應用程式，僅接受以啟動碼啟動受管理的應用程式。

關於訂購

*卡巴斯基安全管理中心雲端主控台訂購*是一種依所選設定（訂購到期日、受防護裝置數量）來使用應用程式的訂單。您可以向您的服務提供商（例如，網際網路提供商）註冊您的卡巴斯基安全管理中心雲端主控台訂購。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。若要在限期訂購到期後繼續使用卡巴斯基安全管理中心雲端主控台，您必須續訂訂購。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。

若要以訂購方式使用卡巴斯基安全管理中心雲端主控台，您必須套用服務提供商提供的啟動碼。

您必須在訂購到期後或您取消訂購後，才能為卡巴斯基安全管理中心雲端主控台套用不同的啟動碼。

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。

以訂購形式購買的啟動碼無法用於啟動更舊版本的卡巴斯基安全管理中心雲端主控台。

以訂購形式使用應用程式時，卡巴斯基安全管理中心雲端主控台會自動依指定的時間間隔嘗試存取啟動伺服器，直到訂購到期為止。如果無法存取使用系統 DNS 的伺服器，則應用程式使用公用 DNS 伺服器。您可以在服務提供商網站續約您的訂購。

資料提供

卡巴斯基安全管理中心雲端主控台可讓使用者識別和控制透過受管理應用程式的功能連線到卡巴斯基安全管理中心雲端主控台的裝置（以及該裝置擁有者）。

資料提供方法：

1. 使用者會在卡巴斯基安全管理中心雲端主控台介面中輸入資料。
2. 網路代理從裝置收到資料，然後將這些資料傳輸給管理伺服器。
3. 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。在 Kaspersky 受管理應用程式的說明中，會提供該應用程式所處理資料的清單。
4. 由內部部署運作的從屬管理伺服器傳資料過來。

卡巴斯基安全管理中心雲端主控台會在試用產品授權期限到期的 30 天後或是正式產品授權期限到期的 90 天後，自動刪除工作區。

在產品授權期限到期後，Kaspersky 會將使用者在使用者工作區中的警示與事件相關資料儲存 30 天。

在目前的產品授權下，警示和事件的儲存期限為 360 天。過了此期限之後，較舊的警示與事件會自動刪除。

最終刪除本節列出的資料，可能最多需要 24 小時的時間。

傳送至 Kaspersky 伺服器的資料

在啟動期間傳送的資料

使用者在使用啟動碼啟動軟體時，同意定期向 Kaspersky 提供以下資訊，以供確認使用該軟體的合法性：

- 啟動碼
- 目前產品授權的唯一啟動識別碼

Kaspersky 還可能會使用這些資訊產生 Kaspersky 軟體的分佈與使用統計資訊。

在更新期間傳送的資料

為了改善更新機制的品質，使用者一旦從權利持有人的更新伺服器收到更新，即表示同意定期向 Kaspersky 提供以下資訊：

- 從產品授權得來的軟體 ID
- 完整版本的軟體
- 軟體產品授權 ID
- 軟體安裝 ID (PCID)

- 軟體更新啟動 ID

Kaspersky 還可能會使用這些資訊產生 Kaspersky 軟體的分發與使用統計資訊。

確保不間斷運作、高效運作以及確認使用卡巴斯基安全管理中心雲端主控台的合法性時所需的資料

以下資訊可能會用於該指定目的：

- 與工作區連線的 Kaspersky 安全應用程式本身的名稱與版本，以及安裝了這些安全應用程式的裝置數量。
- 安裝了 Kaspersky 安全應用程式並與所有工作區連線的裝置數量，以及這些連線裝置的類型分佈。
- 工作區識別碼、公司識別碼、工作區所在國家與地區，以及工作區建立日期。
- 工作區中的使用者數量、工作區中上次執行身分驗證的日期。
- 目前所用產品授權的詳細資訊（產品授權類型、產品授權的裝置數量限制、連線的裝置數量，以及先前所用產品授權的到期日）。

點擊卡巴斯基安全管理中心雲端主控台介面中的連結時會傳輸的資料

使用者一旦點擊管理主控台或卡巴斯基安全管理中心雲端主控台中的連結，即表示同意自動傳輸以下資料：

- 卡巴斯基安全管理中心雲端主控台本地化版本
- 產品授權 ID
- 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。

工作區運作所需的資料

卡巴斯基安全管理中心雲端主控台會處理以下資料：

1. 在組織的網路中所偵測到裝置的詳細資訊

   網路代理會從網路裝置接收以下資料，然後將這些資料傳輸給管理伺服器：

   a. 所偵測到裝置暨其元件的技術規格（透過輪詢網路而得，為識別裝置所需）：

   - Active Directory 輪詢：

     Active Directory 裝置：裝置的區分名稱；從網域控制器收到的 Windows 網域名稱； Windows 環境中的裝置名稱；NetBIOS 網域名稱；裝置的 DNS 網域與 DNS 名稱；Security Account Manager (SAM) 帳戶（登入系統時所用的名稱，用於支援執行早期作業系統版本的用戶端和伺服器，例如 Windows NT 4.0、Windows 95、Windows 98 和 LAN Manager）；網域的區分名稱；裝置所屬群組的區分名稱；管理裝置的使用者本身的區分名稱；以及裝置的全域唯一識別碼 (GUID) 與父 GUID。

     輪詢 Active Directory 網路時，還會處理以下類型的資料，以便顯示受管理基礎架構的資訊以及使用者使用這些資訊（例如，在進行防護佈署期間）的情況：

- Active Directory 組織單位：組織單位的區分名稱；網域名稱的區分名稱；組織單位的 GUID 與父 GUID。
- Active Directory 網域：從網域控制器收到的 Windows 網域名稱； DNS 網域；網域的 GUID。
- Active Directory 使用者：使用者的顯示名稱；使用者的區分名稱；網域的區分名稱；使用者的組織名稱；使用者工作的部門名稱；擔任使用者主管的另一位使用者的區分名稱；使用者的全名；SAM 帳戶；電子郵件地址；備用電子郵件地址；主要電話號碼；備用電話號碼；行動電話號碼；使用者的職位名稱；使用者所屬群組的區分名稱；使用者全域唯一識別碼 (GUID)；使用者安全識別碼 (SID)（用於將使用者識別為安全主體的唯一二進位值）；以及使用者主體名稱 (UPN)，即使用者符合網際網路標準 RFC 822 格式的網際網路樣式登入名稱。UPN 較區分名稱更短、更好記。依照慣例，UPN 會對應到使用者電子郵件名稱。
- Active Directory 群組：群組的區分名稱；電子郵件地址；網域的區分名稱；SAM 帳戶；群組所屬其他群組的區分名稱；SID 群組；群組 GUID。

b. Samba 網域輪詢：

Samba 裝置：裝置的區分名稱；從網域控制器收到的網域名稱；NetBIOS 裝置名稱；NetBIOS 網域名稱；裝置的 DNS 網域名稱與 DNS 名稱；Security Account Manager (SAM) 帳戶；網域的區分名稱；裝置所屬群組的區分名稱；管理裝置的使用者本身的區分名稱；裝置的全域唯一識別碼 (GUID) 與父 GUID。

- Samba 組織單位：組織單位的區分名稱；網域的區分名稱；組織單位的 GUID 與父 GUID。
- Samba 網域：從網域控制器收到的網域名稱；DNS 網域；網域的 GUID。
- Samba 使用者：使用者的顯示名稱；使用者的區分名稱；使用者的組織名稱；使用者工作的部門名稱；擔任使用者主管的另一位使用者的區分名稱；使用者的全名；SAM 帳戶；電子郵件地址；備用電子郵件地址；主要電話號碼；備用電話號碼；行動電話號碼；使用者的職位名稱；使用者所屬群組的區分名稱；使用者全域唯一識別碼 (GUID)；使用者安全識別碼 (SID)（用於將使用者識別為安全主體的唯一二進位值）；以及使用者主體名稱 (UPN)，即使用者符合網際網路標準 RFC 822 格式的網際網路樣式登入名稱。UPN 較區分名稱更短、更好記。傳統上，UPN 會對應到使用者電子郵件名稱。
- Samba 群組：群組的區分名稱；電子郵件地址；網域的區分名稱；SAM 帳戶；群組所屬其他群組的區分名稱；SID 群組；群組 GUID。

c. Windows 網域輪詢：

- Windows 網域或工作群組的名稱
- 裝置 NetBIOS 名稱
- 裝置的 DNS 網域與 DNS 名稱
- 裝置名稱和說明
- 裝置在網路中可見
- 裝置 IP 位址
- 裝置類型（工作站、伺服器、SQL Server、網域控制器等）
- 裝置上的作業系統類型
- 裝置的作業系統版本
- 上次更新裝置資訊的時間

- 裝置上次在網路中可見的時間

d. IP 範圍輪詢：

- 裝置 IP 位址
- 裝置 DNS 名稱或 NetBIOS 名稱
- 裝置名稱和說明
- 裝置 MAC 位址
- 裝置上次在網路中可見的時間

2. 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雲端主控台介面中輸入裝置的顯示名稱和說明：

a. 受管理裝置及其元件的技術規格（識別裝置時所需）：

- 裝置的顯示名稱（依 NetBIOS 名稱產生，可手動修改）和說明（手動輸入）
- Windows 網域名稱和類型（Windows NT 網域 / Windows 工作群組）
- Windows 環境中的裝置名稱
- 裝置的 DNS 網域與 DNS 名稱
- 裝置 IP 位址
- 裝置子網路遮罩
- 裝置網路位置
- 裝置 MAC 位址
- 裝置上的作業系統類型
- 裝置是否為 hypervisor 類型的虛擬機器
- 裝置是否為位於虛擬桌面基礎架構 (VDI) 中的動態虛擬機器
- 裝置 GUID
- 網路代理實例 ID
- 網路代理安裝 ID
- 網路代理永久 ID

b. 稽核受管理裝置以及決定特定修補程式和更新是否適用時所需的受管理裝置及其元件的其他規格：

- Windows 更新代理 (WUA) 狀態
- 作業系統架構

- 作業系統生產商
- 作業系統組建編號
- 作業系統發佈 ID
- 作業系統位置資料夾
- 如果裝置是虛擬機器，則為虛擬機器類型
- 裝置回應等待時間
- 網路代理是否以獨立模式運作

c. 與受管理裝置上的活動有關的詳細資訊：

- 上次更新的日期和時間
- 裝置上次在網路中可見的日期和時間
- 待重新啟動狀態（「需要重新啟動。」）
- 開啟裝置的時間

d. 裝置使用者帳戶和其工作階段的詳細資訊

e. 若裝置是發佈點，則還包括發佈點操作統計資訊：

- 發佈點的建立日期和時間
- 工作資料夾名稱
- 工作資料夾大小
- 與管理伺服器同步的次數
- 裝置上次與管理伺服器同步的日期和時間
- 傳輸的檔案數量和總大小
- 用戶端下載的檔案數量和總大小
- 用戶端使用傳輸控制協定 (TCP) 下載的資料量
- 透過多點傳送向用戶端傳送的資料量
- 用戶端透過多點傳送下載的資料量
- 多點傳送分發數量
- 多點傳送分發的總量
- 上次與管理伺服器同步後，與用戶端同步的次數

f. 用於管理裝置的虛擬管理伺服器本身的名稱

g. 雲端裝置的詳細資訊：

- 雲端區域
- 虛擬私有雲端 (VPC)
- 雲端可用性區域
- 雲端子網路
- 雲端置放群組

h. 行動裝置的詳細資訊。受管理應用程式會將行動裝置中的這些資料傳輸給管理伺服器。在受管理應用程式的說明文件中，會提供完整資料清單。

3. 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：

a. 裝置上安裝的 Kaspersky 受管理應用程式和卡巴斯基安全管理中心雲端主控台元件

b. 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
- 上次掃描裝置的日期和時間
- 偵測到的威脅數量
- 解毒失敗的物件數量
- 對 Kaspersky 安全應用程式使用的工作
- 應用程式元件的可用性和狀態
- 病毒資料庫的上次更新時間和版本
- Kaspersky 應用程式設定的詳細資訊
- 作用中產品授權金鑰的資訊
- 備用產品授權金鑰的資訊
- 應用程式安裝日期
- 應用程式安裝 ID

c. 應用程式操作統計資訊：與受管理裝置上的 Kaspersky 應用程式元件狀態變更相關的事件，以及與應用程式元件所發動工作的效能相關的事件

d. Kaspersky 應用程式定義的裝置狀態

e. 由 Kaspersky 應用程式分配的標記

f. Kaspersky 應用程式之已安裝與適用的更新集：

- 應用程式的顯示名稱、版本和語言
- 應用程式的內部名稱
- 登錄機碼中的應用程式名稱和版本
- 應用程式的安裝資料夾
- 修補程式版本
- 所安裝應用程式自動修補程式的清單
- 應用程式是否受卡巴斯基安全管理中心雲端主控台支援
- 應用程式是否安裝在叢集上

g. 裝置上資料加密錯誤的詳細資訊：錯誤 ID、發生時間、操作類型（加密/解密）、錯誤說明、檔案路徑、加密規則說明、裝置 ID 以及使用者名稱

4. 卡巴斯基安全管理中心雲端主控台元件與 Kaspersky 受管理應用程式的事件。

網路代理將資料從裝置傳輸至管理伺服器。

事件的說明可能會包含以下資料：

a. 裝置名稱

b. 裝置使用者名稱

c. 遠端連線到裝置的管理員本身的名稱

d. 裝置上所安裝應用程式的名稱、版本和供應商

e. 裝置上的應用程式安裝資料夾路徑

f. 檔案在裝置上的路徑以及檔案名稱

g. 應用程式名稱以及執行應用程式時使用的命令列參數

h. 修補程式名稱、修補程式檔案名稱、修補程式 ID、修補程式修復的弱點等級、修補程式安裝錯誤的說明

i. 裝置 IP 位址

j. 裝置 MAC 位址

k. 裝置重新啟動狀態

l. 發佈事件的工作本身的名稱

m. 裝置是否已切換到獨立模式以及切換原因

n. 裝置上安全問題的資訊：安全問題類型、安全問題名稱、嚴重等級、安全問題說明、Kaspersky 應用程式傳送的安全問題詳細資訊

o. 裝置上的可用磁碟空間大小

p. Kaspersky 應用程式是否以有限功能模式運作，以及功能範圍的 ID

q. Kaspersky 應用程式設定的舊值和新值

r. Kaspersky 應用程式或其任何元件執行操作時，所發生錯誤的說明

5. 存在於政策和政策設定檔中的卡巴斯基安全管理中心雲端主控台元件與 Kaspersky 受管理應用程式設定。
使用者會在 Kaspersky Security Center Cloud Console 介面中輸入資料。

6. 卡巴斯基安全管理中心雲端主控台元件與 Kaspersky 受管理應用程式的工作設定
使用者會在 Kaspersky Security Center Cloud Console 介面中輸入資料。

7. 弱點和修補程式管理功能處理的資料。
網路代理將下列資料從裝置傳輸至管理伺服器：

a. 安裝在受管理裝置（應用程式登錄資料）的應用程式和修補程式的詳細資訊。應用程式可能是依應用程式控制功能在受管理裝置上所偵測到可執行檔的資訊來受到識別：

- 應用程式/修補程式 ID
- 父應用程式 ID（如為修補程式）
- 應用程式/修補程式名稱和版本
- 應用程式/修補程式是否為 Windows Installer 的 .msi 檔案
- 應用程式/修補程式供應商
- 本土化版本語言 ID
- 應用程式/修補程式安裝日期
- 應用程式安裝路徑
- 應用程式/修補程式供應商的技術支援網站
- 技術支援電話號碼
- 所安裝應用程式實例的 ID
- 注釋
- 解除安裝金鑰
- 以靜默模式安裝時所用的金鑰
- 修補程式分類
- 提供了修補程式相關額外資訊的網址
- 應用程式的登錄機碼
- 應用程式組建編號
- 使用者 SID

- 作業系統類型（Windows、Unix）

b. 在受管理裝置上所偵測到硬體的資訊（硬體登錄資料）：

- 裝置 ID
- 裝置類型（主機板、CPU、RAM、大容量儲存裝置、顯示卡、音效卡、網路介面控制器、顯示器、光碟裝置）
- 裝置名稱
- 敘述
- 供應商
- 序號
- 修訂
- 驅動程式的資訊：開發者、版本、說明和發佈日期
- BIOS 的資訊：開發者、版本、序號和發佈日期
- 晶片
- 時鐘頻率
- CPU 核心數量
- CPU 執行緒數量
- CPU 平台
- 儲存裝置轉速
- RAM：類型、零件號碼
- 顯存
- 音效卡解碼器

c. 在受管理裝置上的協力廠商軟體中所偵測到弱點的詳細資訊：

- 弱點識別碼
- 弱點嚴重等級（警告、高度、緊急）
- 弱點類型（Microsoft、協力廠商）
- 提供了弱點說明的網頁位址
- 弱點項目的建立時間
- 供應商名稱
- 供應商的本地化名稱

- 供應商 ID
- 應用程式名稱
- 應用程式的本地化名稱
- 應用程式安裝代碼
- 應用程式版本
- 應用程式本地化版本語言
- 弱點說明中所提 CVE 識別碼的清單
- 將弱點封鎖的 Kaspersky 防護技術（檔案威脅防護、行為偵測、Web 威脅防護、郵件威脅防護、主機入侵防護、ZETA Shield）
- 偵測到弱點的物件檔案路徑
- 弱點偵測時間
- 弱點說明中的知識庫文章 ID
- 弱點說明中的安全公告 ID
- 弱點適用的更新清單
- 弱點是否存在被利用的情況
- 是否有針對該弱點的惡意軟體存在

d. 受管理裝置上所安裝協力廠商應用程式之可用更新的詳細資訊：

- 應用程式名稱和版本
- 供應商
- 應用程式本地化版本語言
- 作業系統
- 修補程式的清單（依安裝順序列出）
- 套用修補程式的應用程式本身的原始版本
- 安裝修補程式後的應用程式版本
- 修補程式 ID
- 版本編號
- 安裝旗標
- 修補程式的產品授權協議
- 修補程式是否為安裝其他修補程式的先決條件

- 已安裝之必要應用程式及其更新的清單
- 修補程式資訊的來源
- 修補程式的額外資訊（網頁位址）
- 修補程式的下載網址、檔案名稱、版本、修訂和 SHA-256

e. WSUS 功能所找到 Microsoft 更新的詳細資訊：

- 更新修訂編號
- Microsoft 更新類型（驅動程式、軟體、類別、Detectoid）
- 依 Microsoft Security Response Center (MSRC) 公告而言的更新重要性等級（低度、中度、高度、緊急）
- 與更新相關之 MSRC 公告的 ID
- MSRC 知識庫文章 ID
- 更新名稱（標題）
- 更新說明
- 更新安裝程式是否為互動式
- 安裝旗標
- 更新分類（重大更新、定義更新、驅動程式、功能套件、安全更新、服務套件、工具、更新匯總、更新、升級）
- 套用應用程式更新的應用程式本身的資訊
- 最終使用者產品授權協議 (EULA) ID
- EULA 文字
- 是否必須接受 EULA 才能安裝更新
- 相關更新的資訊（ID 和修訂編號）
- 更新 ID（全域 Microsoft Windows 更新身分識別）
- 所取代的更新 ID
- 更新是否為隱藏性質
- 更新是否為強制性質
- 更新安裝狀態（不適用、未指定安裝、已分配、正在安裝、已安裝、失敗、需要重新啟動、未指定安裝（新版本））
- 更新的 CVE ID
- 發佈更新的公司，或是「缺少公司」一值

f. WSUS 功能找到且必須安裝在裝置上的 Microsoft 更新清單。

8. 應用程式控制功能在受管理裝置上所偵測到可執行檔的資訊（可能與應用程式登錄資料中的資訊相關聯）。在針對透過相對應應用程式來管理的裝置提供資料說明的章節中，會提供完整資料清單。

   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。

9. 備份區中所放入檔案的資訊。在為透過相對應應用程式管理的裝置提供資料說明的區段中，會提供完整的資料清單。

   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。

10. Kaspersky 專家為了進行詳細分析而索取之檔案的資訊。如需完整的資料清單，請見針對透過相對應應用程式管理的裝置進行資料說明的區段。

    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。

11. 自適應異常控制規則的狀態與觸發資訊。在針對透過相應應用程式管理的裝置來提供說明的區段中，會提供完整的資料清單。

    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。

12. 因安裝或連接至受管理裝置而被裝置控制功能偵測到的裝置本身的資訊（記憶體單位、資訊傳輸工具、資訊實體工具和連接匯流排）。在針對透過相應應用程式管理的裝置來說明資料的區段中，會提供完整的資料清單。

    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。

13. 警示資料：

    - 警示中第一個遙測事件的日期和時間
    - 警示中最後一個遙測事件的日期和時間
    - 所觸發規則的名稱（由使用者在卡巴斯基安全管理中心雲端主控台介面中輸入）
    - 警示狀態
    - 解析結果（誤報、確判為真、低優先順序）
    - 獲派解決警示的使用者本身的 ID 和名稱
    - 與警示來源事件相關的裝置在卡巴斯基安全管理中心雲端主控台資料庫中的唯一 ID 以及名稱
    - 警示來源事件相關裝置的使用者本身的 SID 和名稱
    - 可觀察物件，即與警示來源事件相關的可觀察資料：
      - IP 位址
      - 檔案的 MD5 雜湊總和以及檔案路徑
      - 網址
      - 網域
    - 與警示相關的物件本身的額外詳細資訊（從應用程式得到）
    - 對警示的註解：

- 新增註解的日期和時間
- 新增註解的使用者
- 註解文字

- 警示變更記錄：
  - 變更日期和時間
  - 執行變更的使用者
  - 變更說明

14. 安全問題的資料：

- 安全問題中第一個事件的日期和時間
- 安全問題中最後一個事件的日期和時間
- 安全問題名稱（由使用者在卡巴斯基安全管理中心雲端主控台介面中輸入）
- 安全問題的簡要說明
- 安全問題優先順序
- 安全問題狀態
- 獲派解決安全問題的使用者本身的 ID 和名稱
- 解析結果（誤報、確判為真、低優先順序、已合併）
- 對安全問題的註解：
  - 新增註解的日期和時間
  - 新增註解的使用者
  - 註解文字
- 安全問題變更記錄：
  - 變更日期和時間
  - 執行變更的使用者
  - 變更說明

15. Kaspersky 應用程式的資料加密功能會處理的資料。

受管理應用程式會透過網路代理，將資料從裝置傳輸至管理伺服器。磁碟機說明是由使用者在卡巴斯基安全管理中心雲端主控台介面中輸入：

a. 裝置上磁碟機的清單：

- 磁碟機名稱

- 加密狀態
- 磁碟機類型（開機磁碟機、磁碟機）
- 磁碟機序號
- 敘述

b. 裝置上所發生資料加密錯誤的詳細資訊：

- 發生錯誤的日期和時間
- 操作類型（加密、解密）
- 錯誤敘述
- 檔案路徑
- 規則說明
- 裝置 ID
- 使用者名稱
- 錯誤 ID

c. Kaspersky 應用程式的資料加密設定。
在針對透過相對應應用程式來管理的裝置提供資料說明的章節中，會提供完整資料清單。

16. 所輸入啟動碼的詳細資訊。
使用者會在 Kaspersky Security Center Cloud Console 介面中輸入資料。

17. 使用者帳戶。
使用者會在卡巴斯基安全管理中心雲端主控台介面中輸入以下資料：

a. 名稱

b. 敘述

c. 完整名稱

d. 郵件信箱

e. 主電話號碼

f. 密碼

18. 使用 Active Directory 進行使用者身分驗證時所需的資料：

a. Active Directory 同盟服務 (ADFS) 設定：

- 身分驗證提供商的主 URL
- ADFS 的受信任根憑證

- ADFS 中產生的用戶端 ID
- 用於 ADFS 存取防護的秘密金鑰
- 權杖的範圍
- 執行了整合的 Active Directory 網域
- 包含使用者 SID 的權杖欄位本身的名稱
- 包含使用者群組 SID 陣列的權杖欄位本身的名稱

使用者會在卡巴斯基安全管理中心雲端主控台介面中輸入資料。

b. 卡巴斯基安全管理中心雲端主控台自動從 ADFS 伺服器收到的資料：

- 簽發者 (issuer)
- 使用者授權端點 (authorization_endpoint)
- 權杖端點 (token_endpoint)
- JSON Web 金鑰集 URI (jwks_uri)
- 存取權杖簽發者 (access_token_issuer)
- 使用者資訊端點 (userinfo_endpoint)
- 終點工作階段端點 (end_session_endpoint)
- 權杖簽署憑證

19. 以下管理物件的修訂歷程：管理伺服器、管理群組、政策、工作、使用者 / 安全群組、安裝套件。
使用者會在卡巴斯基安全管理中心雲端主控台介面中輸入以下資料：

a. 管理伺服器

b. 管理群組

c. 政策

d. 工作

e. 使用者 / 安全群組

f. 安裝套件

20. 所刪除管理物件的登錄資料。
使用者會在卡巴斯基安全管理中心雲端主控台介面中輸入資料。

21. 從檔案建立的安裝套件以及安裝設定。
使用者會在卡巴斯基安全管理中心雲端主控台介面中輸入資料。

22. 在卡巴斯基安全管理中心雲端主控台中顯示卡巴斯基公告時所需的資料：

a. 使用者所用受管理 Kaspersky 應用程式的資訊：應用程式 ID、完整版本編號。

b. 使用者的卡巴斯基安全管理中心雲端主控台介面本地化版本。

c. 裝置上軟體的啟動資訊：軟體產品授權 ID；軟體產品授權期限；軟體產品授權到期的日期和時間；使用的軟體產品授權類型；軟體訂購類型；軟體訂購到期的日期和時間；軟體訂購的目前狀態；軟體訂購目前/變更狀態的原因；購買軟體產品授權時所透過價目表項目的 ID。

d. 使用者在使用軟體時所接受法律協議的資訊：法律協議類型；法律協議的版本；用於指出使用者是否已接受法律協議條款的旗標。

e. 從權利持有人所收到公告的資訊：公告 ID；收到公告的時間；收到公告的狀態。

使用者會在卡巴斯基安全管理中心雲端主控台介面中輸入資料。

23. 卡巴斯基安全管理中心雲端主控台使用者設定。

使用者會在卡巴斯基安全管理中心雲端主控台介面中輸入以下資料：

a. 使用者介面本地化版本語言

b. 使用者介面主題

c. 監控面板的顯示設定

d. 通知狀態的資訊：已讀 / 尚未讀取

e. 試算表欄位的狀態：顯示/隱藏

f. 教程進度

24. 在受管理裝置上執行遠端診斷功能時收到的資料：偵錯檔案、系統資訊、裝置上所安裝 Kaspersky 應用程式的詳細資訊、傾印檔案、記錄檔案、執行技術支援提供的診斷指令碼後得到的結果。

25. 使用者在卡巴斯基安全管理中心雲端主控台介面中輸入的資料：

a. 建立管理群組階層時的管理群組名稱

b. 設定電子郵件通知時的電子郵件地址

c. 對裝置加上的標記以及標記規則

d. 對應用程式加上的標記

e. 應用程式使用者類別

f. 為使用者分配角色時的角色名稱

g. 子網路的資訊：子網路名稱、說明、位址和遮罩

h. 報告和分類的設定

i. 使用者輸入的任何其他資料

26. 從內部部署的從屬管理伺服器收到的資料。

欲知卡巴斯基安全管理中心管理伺服器會處理的資料，請參閱卡巴斯基安全管理中心線上說明。

當連接內部部署的卡巴斯基安全管理中心管理伺服器作為與卡巴斯基安全管理中心雲端主控台相關的從屬伺服器時，卡巴斯基安全管理中心雲端主控台會處理來自該從屬管理伺服器的下類資料：

a. 透過在 Active Directory 網路或 Windows 網路中執行裝置偵測，或透過掃描 IP 間隔，而在組織的網路中發現之裝置的資訊

b. 透過執行 Active Directory 網路輪詢，而發現之 Active Directory 組織單位、網域、使用者和群組的資訊

c. 受管理裝置、其技術規格（包括識別裝置所需的規格）、裝置使用者的帳戶以及其工作階段的資訊

d. 透過 Exchange ActiveSync 通訊協定傳輸的行動裝置資訊

e. 透過 iOS MDM 通訊協定傳輸的行動裝置資訊

f. 裝置上所安裝 Kaspersky 應用程式的詳細資訊：設定、操作統計資訊、應用程式定義的裝置狀態、已安裝與適用的更新、標記

g. 根據卡巴斯基安全管理中心元件中與 Kaspersky 受管理應用程式中的事件設定來傳輸的資訊

h. 存在於政策和政策設定檔中的卡巴斯基安全管理中心元件與 Kaspersky 受管理應用程式設定

i. 卡巴斯基安全管理中心元件與 Kaspersky 受管理應用程式的工作設定

j. 弱點和修補程式管理功能處理的資料：應用程式和修補程式的詳細資訊；硬體的資訊；在受管理裝置上的協力廠商軟體中所偵測到弱點的詳細資訊；可用之協力廠商應用程式更新的詳細資訊；WSUS 功能所發現 Microsoft 更新的詳細資訊

k. 應用程式的使用者類別

l. 應用程式控制功能在受管理裝置上所偵測到可執行檔的詳細資料

m. 備份區中所放入檔案的詳細資訊

n. 隔離區中所放入檔案的詳細資訊

o. Kaspersky 專家為了進行詳細分析而索取的檔案的資訊

p. 自適應異常控制規則的狀態與觸發資訊

q. 安裝或連接至受管理裝置並且由應用程式控制功能偵測到的裝置的詳細資訊（記憶體單位、資訊傳輸工具、資訊實體工具和連接匯流排）

r. Kaspersky 應用程式的加密設定：加密金鑰的儲存區、裝置加密狀態

s. 使用 Kaspersky 應用程式的資料加密功能在裝置上執行資料加密時所發生錯誤的資訊

t. 受管理可程式設計邏輯控制器 (PLC) 的清單

u. 所輸入啟動碼的詳細資訊

v. 使用者帳戶

w. 管理物件的修訂歷程

x. 所刪除管理物件的登錄資料

y. 從檔案建立的安裝套件以及安裝設定

z. 卡巴斯基安全管理中心網頁主控台使用者設定

aa. 使用者在管理主控台或卡巴斯基安全管理中心雲端主控台介面中輸入的任何資料

ab. 受管理裝置對卡巴斯基安全管理中心元件進行安全連線時所用的憑證

27. 使用遠端診斷功能時從受管理裝置上傳的資訊：診斷檔案（傾印檔案、記錄檔案、偵錯檔案等）以及這些檔案中包含的資料。

28. 將卡巴斯基安全管理中心雲端主控台與 SIEM 系統進行整合以便匯出事件時所需的資料：

- 連線和身分驗證所需的資料：
  - SIEM 系統連線位址和連接埠
  - SIEM 伺服器身分驗證憑證
  - 在 SIEM 系統中進行卡巴斯基安全管理中心雲端主控台的用戶端身分驗證時所需的受信任憑證與私密金鑰

  使用者會在卡巴斯基安全管理中心雲端主控台介面中輸入資料。
- 卡巴斯基安全管理中心雲端主控台從 SIEM 系統收到的資料：進行 SIEM 伺服器身分驗證時所用 SIEM 伺服器憑證的公開金鑰。

29. 卡巴斯基安全管理中心雲端主控台與雲端環境互動時所需的資料：

a. Amazon Web Services (AWS)：

- IAM 使用者帳戶的存取金鑰 ID
- IAM 使用者帳戶的秘密金鑰

b. Microsoft Azure：

- Azure 應用程式 ID
- Azure 訂購 ID
- Azure 應用程式密碼
- 用於 Azure 儲存區的帳戶名稱
- 用於 Azure 儲存區的帳戶存取金鑰

c. Google Cloud：

- Google 用戶端電子郵件
- 專案 ID
- 私密金鑰

使用者會在卡巴斯基安全管理中心雲端主控台介面中輸入資料。

30. 由不支援的 Kaspersky 應用程式傳輸的資料

當您在已安裝 Kaspersky 應用程式的裝置上安裝網路代理，但該應用程式不受卡巴斯基安全管理中心雲端主控台支援時，則該 Kaspersky 應用程式仍會向卡巴斯基安全管理中心雲端主控台傳輸資料（在應用程式說明系統的「關於資料提供」一節中，會提供這些資料的清單）。不過，卡巴斯基安全管理中心雲端主控台無法以針對卡巴斯基安全管理中心雲端主控台的主要功能所說明的程序，對不受支援的應用程式所傳輸的資料進行處理。

如需受支援的 Kaspersky 應用程式清單，請參閱卡巴斯基安全管理中心雲端主控台線上說明。

受管理應用程式運作所需的資料

以下受管理應用程式會透過網路代理，將資料從裝置傳輸至管理伺服器：

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Mac
- Kaspersky Endpoint Agent
- Kaspersky Security for Windows Server
- Kaspersky Security for Mobile
- Kaspersky Embedded Systems Security for Windows
- Kaspersky Embedded Systems Security for Linux

所處理的資料清單公佈於 https://ksc.kaspersky.com/Home/LegalDocuments 中的卡巴斯基安全管理中心雲端主控台資料處理協議部分。在該法律文件網頁上，找到名為 Kaspersky Security Center Cloud Console Agreement 的文字區塊，然後將該文字區塊向下捲動到 Data for devices managed through the relevant managed application。您也可以使用瀏覽器的標準「尋找」功能來達到相同目的。

本機處理的使用者資料

在卡巴斯基安全管理中心雲端主控台中，唯一可部署到本機的卡巴斯基安全管理中心元件便是網路代理。

會在本機處理之使用者資料的清單：

- 「使用者資料」區段中所列出在 Kaspersky 的框架與基礎架構內處理的所有資料（但不包括管理員透過卡巴斯基安全管理中心雲端主控台介面輸入的資料）
- 網路代理的 Kaspersky 事件記錄
- 網路代理的偵錯
- 記錄，包括由網路代理安裝程式、卡巴斯基安全管理中心公用程式建立的記錄

網路代理的傾印、記錄與偵錯檔案包含了隨機資料，因此可能會包含個人資料。檔案會以未加密的方式儲存在安裝了網路代理的裝置上。檔案不會被自動傳輸給 Kaspersky。使用者可以應技術支援的要求，手動將這些資料傳輸給 Kaspersky，以解決操作卡巴斯基安全管理中心時發生的問題。

個人資料的額外處理方

以下列出除 Kaspersky 外，其他會為卡巴斯基安全管理中心雲端主控台處理工作區相關個人資料的處理方。

組織名稱和地址：
Microsoft Ireland Operations Limited
One Microsoft Place, South County Business Park, Leopardstown
Dublin 18 D18 P521

服務：
Microsoft Azure（資料託管）

〈選取用於儲存卡巴斯基安全管理中心雲端主控台資訊的資料中心〉一節會列出資料處理所在的國家/地區。

關於卡巴斯基安全管理中心雲端主控台的法律文件

若要使用卡巴斯基安全管理中心雲端主控台，您必須閱讀並明確同意卡巴斯基安全管理中心雲端主控台網站上的法律文件所載的條款和條件。您可以在登入卡巴斯基安全管理中心雲端主控台來管理工作區時，檢視 AO Kaspersky Lab 為網站提供的隱私權政策條款和條件。您可以在建立公司工作區時，閱讀卡巴斯基安全管理中心雲端主控台協議以及卡巴斯基安全管理中心雲端主控台資料處理協議。

請先仔細閱讀所有這些法律文件的文字，再開始使用卡巴斯基安全管理中心雲端主控台。

Kaspersky 應用程式的最終使用者產品授權協議

最終使用者產品授權協議（以下簡稱「產品授權協議」或 EULA）是您和 AO Kaspersky Lab 之間具有約束力的協議，其中規定了您使用 Kaspersky 應用程式時應遵守的條款。

您可透過以下方式，檢視最終使用者產品授權協議的條款：

- 在建立 Kaspersky 應用程式安裝套件期間顯示的視窗中。
- 在受管理裝置上 Kaspersky 應用程式安裝資料夾內的 license.txt 檔案中。

您可以隨時撤銷接受最終使用者產品授權協議。

如果您不接受 Kaspersky 應用程式的產品授權協議條款，即無法使用該應用程式。

硬化指南

卡巴斯基安全管理中心雲端主控台是一款由 Kaspersky 架設並維護的應用程式。您無需在自己的電腦或伺服器上安裝卡巴斯基安全管理中心雲端主控台。卡巴斯基安全管理中心雲端主控台可讓管理員將 Kaspersky 安全應用程式安裝到企業網路內的裝置上、遠端執行掃描與更新工作，以及管理受管理應用程式適用的安全政策。

卡巴斯基安全管理中心雲端主控台是專為以集中化方式在組織的網路中執行基本的管理和維護工作而設計。該應用程式使管理員可以存取有關組織網路安全級別的詳細資訊。卡巴斯基安全管理中心雲端主控台可讓您設定所有以 Kaspersky 應用程式建構的防護元件。

卡巴斯基安全管理中心雲端主控台可用於對用戶端裝置進行完整的防護管理，是組織的安全系統中最重要的元件。因此，對於卡巴斯基安全管理中心雲端主控台，需要採取更高階的防護方法。

本強化指南針對卡巴斯基安全管理中心雲端主控台和其元件的設定，說明了相關建議與功能，藉以降低其遭駭的風險。

硬化指南包含以下資訊：

- 設定帳戶來存取卡巴斯基安全管理中心雲端主控台
- 管理用戶端裝置防護
- 配置受管理應用程式的防護
- 將資訊傳輸到協力廠商應用程式

在您開始使用卡巴斯基安全管理中心雲端主控台之前，系統會提示您閱讀簡要版本的強化指南。

請注意，您必須確認已閱讀強化指南，方能使用卡巴斯基安全管理中心雲端主控台。

要閱讀硬化指南：

1. 開啟卡巴斯基安全管理中心雲端主控台並進行登入。卡巴斯基安全管理中心雲端主控台會檢查您是否確認閱讀了目前版本的強化指南。

   如果您尚未閱讀硬化指南，則一個視窗會開啟並顯示它的簡要版本。

2. 執行以下操作之一：

   - 如果想要以文字文件形式檢視硬化指南的簡要版本，請點擊**在新視窗中開啟**連接。
   - 如果您想檢視完整版本的強化指南，請點擊**在線上說明中開啟強化指南**連結。

3. 閱讀硬化指南後，選擇**我確認我已完全閱讀並理解硬化指南**核取方塊，然後點擊**接受**按鈕。

現在，您可以使用卡巴斯基安全管理中心雲端主控台。

當有新版本的強化指南出現時，卡巴斯基安全管理中心雲端主控台會提示您加以閱讀。

卡巴斯基安全管理中心雲端主控台架構

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

在初步發展架構的階段，我們建議您熟悉卡巴斯基安全管理中心雲端主控台各元件和其之間的互動方式，以及背後的資料流量與連接埠使用架構。

基於此資訊，您可以形成一個架構，指定：

- 管理員的工作區組織，以及連線到卡巴斯基安全管理中心雲端主控台的方法
- 網路代理和防護軟體的部署方法
- 使用發佈點
- 使用虛擬管理伺服器
- 使用管理伺服器階層
- 病毒資料庫更新方案
- 其他資訊流

帳戶和身分驗證

對卡巴斯基安全管理中心雲端主控台使用雙步驟驗證

Kaspersky Security Center Cloud Console 為使用者提供了雙步驟驗證機制。

雙步驟驗證有助於讓您的卡巴斯基安全管理中心雲端主控台帳戶更加安全。啟用此功能後，您每次使用電子郵件地址和密碼登入卡巴斯基安全管理中心雲端主控台時，都必須額外輸入一次性安全碼。您可以透過簡訊接收一次性安全碼，或是在身份驗證器應用程式中產生該代碼（視您設定的雙步驟驗證方法而定）。

我們強烈建議不要將身份驗證器應用程式安裝到用於與卡巴斯基安全管理中心雲端主控台建立連線的同一台裝置上。您可以在行動裝置上安裝驗證器應用程式。

禁止儲存管理員密碼

如果您使用卡巴斯基安全管理中心雲端主控台，**我們強烈建議不要**將管理員密碼儲存到使用者裝置上所安裝的瀏覽器中。

如果瀏覽器遭駭，入侵者就可以取得其中儲存的密碼。此外，如果儲存了密碼的使用者裝置失竊，入侵者就可以取得受保護的資料。

限制主要管理員角色成員資格

我們建議對主管理員角色的成員資格進行限制。

使用者在建立工作區後，預設會獲配主管理員角色。此角色在進行管理時很有用，但從安全角度來看也很重大，因為主管理員角色具有廣泛的權限。在將此角色分配給使用者這方面，應進行嚴格管制。

您可以利用預先定義的使用者角色（已預先設有一組權限）來管理卡巴斯基安全管理中心雲端主控台。

設定應用程式功能的存取權限

我們建議為每個使用者或使用者群組靈活設定對卡巴斯基安全管理中心雲端主控台功能的存取權限。

基於角色的存取控制方式可讓您以一組預先定義的權限建立標準使用者角色，然後視使用者的職責範圍將這些角色分配給使用者。

基於角色的存取控制模型的主要優點：

- 易於管理
- 角色階層
- 最少特權方法
- 職責分離

您可以根據職位向某些員工分配內建角色，或是建立全新的角色。

設定角色時，需要注意與變更管理伺服器裝置的防護狀態以及遠端安裝協力廠商軟體相關聯的權限：

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

為遠端安裝應用程式使用單獨的帳戶

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

我們建議為遠端安裝應用程式使用單獨的帳戶。您可以將某個角色或某些權限分配給該單獨的帳戶。

管理用戶端裝置防護

在管理群組之間移動裝置的自動規則

我們建議限制使用自動規則在管理群組之間行動裝置。

如果您使用自動規則移動裝置，這可能會導致政策遭擴大套用，使得裝置在移動後比移動前擁有更多的權限。

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

此建議不適用於將裝置一次性初始分配給管理群組。

發佈點和連線閘道的安全要求

安裝了網路代理的裝置可以擔任發佈點並執行以下功能：

- 將從管理伺服器收到的更新和安裝套件發佈到群組內的用戶端裝置。
- 在用戶端裝置上執行協力廠商軟體和卡巴斯基應用程式的遠端安裝。
- 輪詢網路以偵測新裝置並更新現有裝置的資訊。
- 擔任用戶端裝置的 KSN 代理伺服器。

考慮到可用的功能，我們建議對擔任發佈點的裝置進行保護，以免其遭受任何類型的未經授權存取（包括物理存取）。

配置受管理應用程式的防護

配置網路防護

請確定您已完成卡巴斯基安全管理中心雲端主控台初始化設定情境。該情境還包含執行快速啟動精靈的步驟。

快速啟動精靈執行時，會以預設參數建立政策和工作。這些參數可能不是最佳選擇，甚至可能為您的組織所禁止。因此，我們建議對建立的政策和工作進行設定，並且根據您組織網路的需求，建立額外的政策和工作。

指定用於停用防護和解除安裝應用程式的密碼

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

指定將用戶端裝置手動連線到管理伺服器（klmover 公用程式）的密碼

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

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

啟用**使用解除安裝密碼**還會啟用卡巴斯基安全管理中心網頁主控台刪除工具 (cleaner.exe) 的密碼防護。

使用卡巴斯基安全網路

我們建議在受管理應用程式的所有政策以及卡巴斯基安全管理中心雲端主控台的內容中，啟用卡巴斯基安全網路 (KSN) 並接受 KSN 聲明。您可以在更新或升級卡巴斯基安全管理中心雲端主控台時，接受更新後的 KSN 聲明。

發現新裝置

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

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

事件傳輸到第三方系統

監控和報告

為了及時回應安全問題，我們建議配置監控和報告功能。

匯出到 SIEM 系統的事件

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

稽核事件的電子郵件通知

為便在發生緊急情況時及時做出回應，我們建議將卡巴斯基安全管理中心雲端主控台設定為針對稽核事件、緊急事件、故障事件和警告，傳送事件通知。

由於這些事件是系統內事件，因此可以預期它們的數量很少，這非常適用於郵件。

卡巴斯基安全管理中心雲端主控台的初始化設定

本節概述了卡巴斯基安全管理中心雲端主控台從建立工作區到監控網路防護狀態的各種主要部署情境。

如需部署內部部署運作的卡巴斯基安全管理中心，請參閱卡巴斯基安全管理中心線上說明。

建議您至少分配一個工作天來完成此情境。

此情境將引導您完成以下操作：

- 以管理員身分開始使用您公司的工作區
- 發現您網路中的裝置（如有必要，您會分配發佈點並手動在其上安裝分發套件）
- 將受管理 Kaspersky 應用程式部署到用戶端裝置上；設定工具來進行網路防護、監控以及定期更新 Kaspersky 資料庫、軟體模組和應用程式

完成此情境後，以 Kaspersky 應用程式建構的網路防護即設定完成。您將能夠繼續監控網路防護狀態。

先決條件

開始之前：

- 檢視卡巴斯基安全管理中心雲端主控台的架構，以瞭解主要應用程式元件之間的互動方式。
- 閱讀卡巴斯基安全管理中心雲端主控台和受管理應用程式的產品授權資訊。
- 確保您具有卡巴斯基安全管理中心雲端主控台的有效啟動碼（如果您是要建立正式工作區）。

階段

卡巴斯基安全管理中心雲端主控台設定是分多個階段進行：

1. **設定連接埠**

   確保所有必要的連接埠均已開啟，讓您的網路與 Kaspersky 基礎架構之間能夠進行互動。此外，如果您計畫使用管理伺服器階層，請確保所有必要的連接埠均已開啟，讓涉及從屬管理伺服器和用戶端裝置的互動能夠進行。

2. **為您的公司建立工作區**

   建立帳戶，然後為您的公司建立工作區。

3. **執行快速啟動精靈**

   開啟並登入卡巴斯基安全管理中心雲端主控台。首次登入時，系統會自動提示您執行快速啟動精靈。您還可以在任意時刻手動啟動快速啟動精靈。

   當快速啟動精靈完成時，您將得到網路代理與安全應用程式的安裝套件。進一步部署卡巴斯基安全管理中心雲端主控台時，需要有這些安裝套件。

4. **部署 Kaspersky 應用程式**

   執行 Kaspersky 應用程式初始化部署情境。該情境的其中一個步驟會提到網路輪詢操作。該操作十分必要，因為這樣才能發現您網路中的用戶端裝置。如需網路輪詢和其設定的說明，請參閱發現網路裝置的情境。

   如果您是要部署 Kaspersky Security for Windows Server，請確保用於該應用程式的資料庫為最新版本。

5. **Kaspersky 安全應用程式產品授權**

   在受管理裝置上部署 Kaspersky 安全應用程式後，這每個應用程式均必須套用啟動碼以獲得產品授權。請將您的啟動碼部署到受管理裝置上安裝的 Kaspersky 應用程式。您有多種選擇來對 Kaspersky 安全應用程式套用產品授權。

6. **配置網路防護**

   執行網路防護設定，以對透過快速啟動精靈建立的政策和工作進行微調。

7. **定期更新 Kaspersky 資料庫、軟體模組和應用程式**

   為了保護您的網路免受病毒和其他威脅的親慨，您必須設定定期更新 Kaspersky 資料庫、軟體模組和應用程式。

8. **更新協力廠商軟體並修復協力廠商軟體弱點（可選）**

   卡巴斯基安全管理中心雲端主控台可讓您管理用戶端裝置上所安裝 Microsoft 應用程式的更新。您也可以透過安裝所需更新，修復 Microsoft 應用程式的弱點。

9. **設定工具來監控網路防護狀態**

   選取並設定小工具、報告和其他工具，讓您能夠監控網路防護狀態。

部署並設定卡巴斯基安全管理中心雲端主控台後，您就可以開始監控網路防護狀態。

工作區管理

本節說明在卡巴斯基安全管理中心雲端主控台中，您可以如何使用帳戶和工作區。

關於卡巴斯基安全管理中心雲端主控台中的工作區管理

在卡巴斯基安全管理中心雲端主控台中，您可以執行以下操作：

- 建立帳戶。
- 編輯帳戶。
- 註冊公司並建立工作區。
- 編輯公司和工作區的資訊。
- 刪除工作區和公司。
- 刪除帳戶。

開始使用卡巴斯基安全管理中心雲端主控台

本節說明如何註冊並開始使用卡巴斯基安全管理中心雲端主控台。

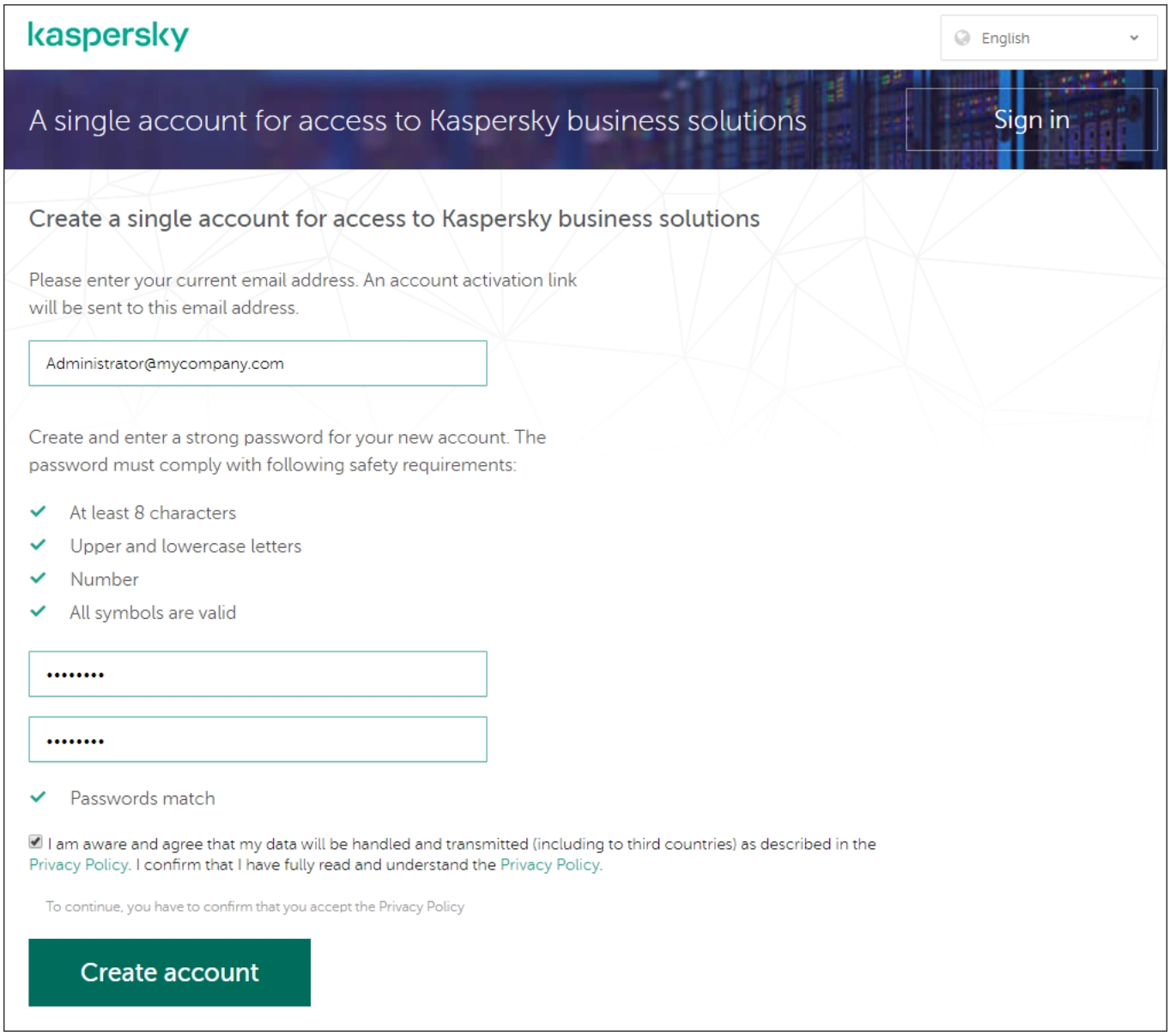
註冊卡巴斯基安全管理中心雲端主控台的過程包括以下步驟：

1. 建立並確認帳戶。
2. 註冊公司並建立工作區。

建立帳戶

若要在卡巴斯基安全管理中心雲端主控台中建立帳戶：

1. 在您的瀏覽器中，前往卡巴斯基安全管理中心雲端主控台。
2. 點擊卡巴斯基安全管理中心雲端主控台開始頁面上的**創建帳戶**按鈕。
3. 在**建立單一帳戶來獲取 Kaspersky 業務解決方案**頁面上，輸入您帳戶的電子郵件地址、密碼以及密碼確認欄位（請參閱下圖）。



在卡巴斯基安全管理中心雲端主控台中建立帳戶

4. 點擊**隱私權政策**連結，然後仔細閱讀隱私政策文字。
5. 如果您明白並同意您的資料將會受到隱私政策所述的處理和傳輸（包括傳輸到第三個國家/地區），並且確認您已完全閱讀並瞭解隱私權政策，請選取讓資料受到隱私權政策所述處理的同意文字旁邊的核取方塊，然後點擊**創建帳戶**按鈕。

   如果您不接受隱私權政策，請勿使用卡巴斯基安全管理中心雲端主控台。

   僅有當您選取該核取方塊後，該按鈕才會變得可用。

   隨即會顯示一個頁面，提示您查看電子郵件。Kaspersky 會傳送一封郵件到您指定的電子郵件地址。該郵件會包含完成帳戶建立程序的連結。
6. 關閉該頁面，然後到您的信箱中開啟該電子郵件。
7. 點擊 Kaspersky 所傳送郵件中的連結以前往您的帳戶頁面。
8. 在**使用者帳戶啟用**頁面上，點擊**繼續**按鈕完成帳戶啟動。

在卡巴斯基安全管理中心雲端主控台中建立帳戶的程序即告完成。

註冊公司並建立工作區

建立帳戶後，您可以立即註冊公司並為其建立工作區。

如果要保護的裝置超過 10,000 台，則您無需依下述方式在卡巴斯基安全管理中心雲端主控台註冊公司並建立工作區。請改為向 Kaspersky 技術支援傳送請求。在該請求中，請指明您的公司和所要建立工作區的資訊。

目前您僅能註冊一家公司並建立一個工作區。在未來版本的卡巴斯基安全管理中心雲端主控台中，您將能夠為您的公司建立額外的工作區。這將有助您建立與公司結構相對應的工作區，因為您將能為每個分公司各建立不同的工作區。

在開始之前，請先確保您知道以下資訊：

- 您計畫將軟體解決方案用於的公司本身的名稱。
- 公司所在的國家/地區。如果公司位於美國或加拿大，您還必須知道所在的州或省。
- 您想要保護的公司電腦與行動裝置總數。

若要在卡巴斯基安全管理中心雲端主控台中註冊公司並建立工作區：

1. 在您的瀏覽器中，前往卡巴斯基安全管理中心雲端主控台。
2. 點擊卡巴斯基安全管理中心雲端主控台開始頁面上的**登入**按鈕。
3. 輸入您在建立帳戶時指定的電子郵件地址和密碼，然後點擊**登入**按鈕。
   「創建工作區」精靈即會啟動。使用**下一步**按鈕進行精靈。
4. 在精靈的**步驟 01：卡巴斯基安全管理中心雲端主控台的使用條款**頁面上，執行以下操作：
   a. 仔細閱讀軟體解決方案的協議、隱私權政策和資料處理協議。
   b. 如果您同意該等協議與資料處理協議的條款和條件，並且明白並同意您的資料將會受到隱私權政策所述的處理和傳輸（包括傳輸給第三個國家/地區），而且確認您已完全閱讀並瞭解隱私權政策，請選取所列三份文件旁邊的核取方塊，然後點擊**接受**按鈕。

   如果您不同意其中的條款和條件，請勿使用卡巴斯基安全管理中心雲端主控台。

   如果您點擊**拒絕**按鈕，工作區建立程序即會終止。
5. 在精靈的**步驟 02：公司資訊**頁面上，指定您公司的主要詳細資訊。
   填充以下欄位：
   - **您公司的名稱**（必填）

指定您計畫將軟體解決方案用於的公司本身的名稱。您可以輸入最長 255 個字元的字串。該字串可以包含大寫與小寫字元、數字、空格、句點、逗點、減號、破折號和底線。指定的公司名稱將會顯示在卡巴斯基安全管理中心雲端主控台中。

- **額外公司描述**欄位（可選）

  您可以指定所註冊公司的額外資訊。您可以輸入最長 255 個字元的字串。該字串可以包含大寫與小寫字元、數字、空格、句點、逗點、減號、破折號和底線。

6. 在精靈的**步驟 03：工作區資訊**頁面上，指定您要為公司建立的工作區本身的資訊。

   填入以下必填欄位：

   - **工作區名稱**。指定您計畫將軟體解決方案用於的工作區本身的名稱。您可以輸入最長 255 個字元的字串。該字串可以包含大寫與小寫字元、數字、空格、句點、逗點、減號、破折號和底線。指定的工作區名稱將會顯示在卡巴斯基安全管理中心雲端主控台中。

   - **國家**。在下拉清單中，選取您的工作區所在的國家/地區。如果您選取美國或加拿大，亦請在此欄位下方出現的**省份**下拉清單中指定州或省。

   - **裝置數量**。輸入您要在此工作區中保護的電腦與行動裝置總數。

     在輸入欄位中，您可以輸入 300 到 10,000 之間的數字。

7. 在精靈的**步驟 04：新工作區的授權**頁面上，執行以下其中一項操作：

   - 如果您想試用卡巴斯基安全管理中心雲端主控台，請點擊**我想申請試用工作區**連結。

     我們建議您將自己的裝置連線到試用工作區、測試對設定進行任何修改，然後記下結果。

     > 您將無法透過輸入啟動碼，直接將試用工作區切換為正式模式。若要切換為正式模式，您必須刪除工作區，然後重新建立工作區。

   - 如果您想以正式模式使用卡巴斯基安全管理中心雲端主控台，請輸入啟動碼，然後點擊**驗證**按鈕。

在卡巴斯基安全管理中心雲端主控台中註冊公司並建立工作區的程序即告完成。

準備好工作區後，您會收到一封電子郵件，其中包含工作區的存取連結。

開啟您的卡巴斯基安全管理中心雲端主控台工作區

您為卡巴斯基安全管理中心雲端主控台建立工作區之後，該工作區即會自動開啟。之後，您可以依本節所述的方式開啟工作區。

如果您是某個虛擬管理伺服器的管理員，則您只對該虛擬管理伺服器具有存取權限。在您登入並開啟工作區後，卡巴斯基安全管理中心雲端主控台會向您提供該虛擬管理伺服器的介面。您無法切換到主管理伺服器或其他從屬管理伺服器。

> 虛擬管理伺服器的管理員必須具有單一虛擬管理伺服器的存取權限。如果您沒有主伺服器的存取權限，但有多個虛擬伺服器的存取權限，則您無法登入卡巴斯基安全管理中心雲端主控台。

若要開啟卡巴斯基安全管理中心雲端主控台工作區：

1. 在您的瀏覽器中，前往卡巴斯基安全管理中心雲端主控台。

2. 在卡巴斯基安全管理中心雲端主控台指定您的使用者名稱和密碼來登入帳戶。

3. 如果您設定了雙步驟驗證，請輸入透過簡訊傳送給您或是身份驗證器應用程式中產生的一次性安全碼（視您設定的雙步驟驗證方法而定）。

   入口頁面會顯示您擔任管理員的公司和其工作區清單。

4. 點擊所需工作區的名稱或**前往工作區**連結以前往工作區。

   有時，工作區可能會因維護因素而無法使用。如果是這種情況，您將無法前往您的卡巴斯基安全管理中心雲端主控台工作區。

   > 您無法開啟標記為刪除的工作區。

5. 如果卡巴斯基安全管理中心雲端主控台有任何法律文件自您上次接受其條款和條件後有了變更，則入口頁面會顯示變更後的文件。

   請執行下列操作：

   a. 仔細閱讀所顯示的文件。

   b. 如果您同意所顯示文件的條款和條件，請選取所列文件旁邊的核取方塊，然後點擊**我接受條款**按鈕。

   > 如果您不同意其中的條款和條件，請停止使用所選的 Kaspersky 軟體解決方案。

   > 如果您點擊**我拒絕**按鈕，操作將會終止。

您的卡巴斯基安全管理中心雲端主控台工作區即會開啟。

登出卡巴斯基安全管理中心雲端主控台

您在完成工作後，應該要登出卡巴斯基安全管理中心雲端主控台來以安全的方式關閉目前的工作階段。

若要登出卡巴斯基安全管理中心雲端主控台，請

在主功能表中，轉到您的帳戶設定，然後選擇**登出**。

卡巴斯基安全管理中心雲端主控台即會關閉，並顯示帳戶頁面。如有必要，您可以關閉該瀏覽器頁面。您工作區中的所有資料都會儲存。

管理公司和工作區清單

本節說明如何在卡巴斯基安全管理中心雲端主控台中，檢視在您帳戶下註冊的公司資訊和工作區清單、變更公司和工作區的資訊，以及刪除工作區和公司。

目前您僅能註冊一家公司並建立一個工作區。在未來版本的卡巴斯基安全管理中心雲端主控台中，您將能夠為您的公司建立額外的工作區。這將有助您建立與公司結構相對應的工作區，因為您將能為每個分公司各建立不同的工作區。

編輯公司和工作區的資訊

您可以修改您將公司新增至卡巴斯基安全管理中心雲端主控台時，所指定公司與工作區的資訊。

若要修改公司和/或工作區的資訊：

1. 在您的瀏覽器中，前往卡巴斯基安全管理中心雲端主控台。
2. 在卡巴斯基安全管理中心雲端主控台指定您的使用者名稱和密碼來登入帳戶。
3. 如果您設定了雙步驟驗證，請輸入透過簡訊傳送給您或是身份驗證器應用程式中產生的一次性安全碼（視您設定的雙步驟驗證方法而定）。

   入口頁面會顯示您擔任管理員的公司和其工作區清單。
4. 若要編輯公司名稱和說明，請執行以下操作：
   a. 在包含公司資訊的區域中，點擊**編輯** (✎) 圖示。
   b. 視需要修改公司名稱和/或說明。
   c. 點擊**儲存**按鈕。

      若要取消變更，請點擊**取消**按鈕。
5. 若要編輯工作區名稱，請執行以下操作：
   a. 在包含工作區資訊的區域中，點擊**編輯** (✎) 圖示。
   b. 視需要修改工作區名稱。
   c. 點擊**儲存**按鈕。

      若要取消變更，請點擊**取消**按鈕。

卡巴斯基安全管理中心雲端主控台中即會顯示修改後的資訊。

刪除工作區和公司

您可以手動或自動刪除公司的工作區。刪除最後一個工作區後，公司資訊也會自動刪除。

手動刪除

如果公司決定停止使用某個工作區，您可以刪除公司的該工作區。

> 刪除工作區後，所有安全應用程式都會保留在受管理裝置上。因此，建議您在刪除工作區之前，先停用所有安全應用程式的密碼防護，或是解除安裝受管理裝置上的安全應用程式。

若要刪除工作區和公司：

1. 在您的瀏覽器中，前往卡巴斯基安全管理中心雲端主控台。

2. 在卡巴斯基安全管理中心雲端主控台指定您的使用者名稱和密碼來登入帳戶。

3. 如果您設定了雙步驟驗證，請輸入透過簡訊傳送給您或是身份驗證器應用程式中產生的一次性安全碼（視您設定的雙步驟驗證方法而定）。

   口頁面會顯示您擔任管理員的公司和其工作區的清單。

4. 選取您要刪除的工作區。

5. 在右側包含所選工作區的區段中，點擊**刪除** (🗑) 圖示。

   刪除工作區視窗即會開啟。

6. 在**刪除工作區**視窗中，確認您要刪除工作區。

   工作區即會被標記為刪除。工作區的資訊區塊會以紅色邊框醒目顯示。

   工作區的資訊區塊會複製到頁面底部的**標記為刪除**區段。

> 您無法前往標記為刪除的工作區進行管理。

> 如果您無法將工作區標記為刪除，請聯絡 Kaspersky 技術支援。Kaspersky 的技術支援工程師會在收到您的請求後，將工作區和公司刪除。

工作區在被標記為刪除後，可能會保持該狀態 7 天。7 天後即會自動刪除。

在這段期間，您可以將標記為刪除的工作區強制刪除，或是取消刪除工作區。

若要強制刪除工作區：

1. 在您的瀏覽器中，前往卡巴斯基安全管理中心雲端主控台。

2. 在卡巴斯基安全管理中心雲端主控台指定您的使用者名稱和密碼來登入帳戶。

3. 如果您設定了雙步驟驗證，請輸入透過簡訊傳送給您或是身份驗證器應用程式中產生的一次性安全碼（視您設定的雙步驟驗證方法而定）。

   入口頁面會顯示您擔任管理員的公司和其工作區清單。

4. 在**標記刪除**區段中，在標記為刪除的工作區本身的資訊區塊中，點擊**強制刪除**選項。

   刪除工作區視窗即會開啟。

5. 在**刪除工作區**視窗中，輸入所要刪除工作區的 ID。

   系統會提示您確認工作區的 ID，確保您不會誤刪工作區。工作區一經刪除，即無法還原。

   工作區 ID 會顯示在工作區資訊區段中的工作區名稱下。

6. 在**刪除工作區**視窗中，點擊**確定**。

   工作區即會刪除。所有關於使用者、受管理裝置和其設定的資料都會刪除。

自動刪除

在以下情況，卡巴斯基安全管理中心雲端主控台會自動刪除工作區：

- 試用產品授權到期的 30 天後。
- 管理伺服器儲存區中所有正式或訂購產品授權都到期的 90 天後。
- 您刪除了在儲存區中手動新增的最後一個產品授權金鑰（無論是有效、備用還是未使用中的金鑰）的 90 天後。

Kaspersky Security Center Cloud Console 會在刪除的 30 天、7 天與 1 天前，通知工作區的管理員。

取消刪除工作區

您可以取消刪除已標記為刪除的工作區。

您無法取消刪除已刪除的工作區。

若要取消刪除工作區：

1. 在您的瀏覽器中，前往卡巴斯基安全管理中心雲端主控台。
2. 在卡巴斯基安全管理中心雲端主控台指定您的使用者名稱和密碼來登入帳戶。
3. 如果您設定了雙步驟驗證，請輸入透過簡訊傳送給您或是身份驗證器應用程式中產生的一次性安全碼（視您設定的雙步驟驗證方法而定）。

   入口頁面會顯示您擔任管理員的公司和其工作區清單。
4. 在**標記刪除**區段中，在標記為刪除的工作區本身的資訊區塊中，點擊**取消刪除**連結。

工作區即會取消刪除。您現在可以前往工作區並繼續加以使用。

管理對公司和其工作區的存取權限

本節包含與授予和撤銷對您公司和其工作區的存取權限有關的資訊。

卡巴斯基安全管理中心雲端主控台為您提供了兩種存取權限等級：

- **管理員**

  具有此存取權限等級的使用者可以對公司和其工作區進行完整管理。
- **使用者**

  具有此存取權等級的使用者可以檢視可用工作區的清單並進入這些工作區。

授予對您公司和其工作區的存取權限

如果您想讓其他使用者登入您的公司並依所選的存取權限等級加以管理，您可以向其授予對您公司和其工作區的存取權限。

若要向使用者授予存取權限，該使用者必須在卡巴斯基安全管理中心雲端主控台中建立帳戶。

若要授予對您公司和其工作區的存取權限：

1. 在您的瀏覽器中，前往卡巴斯基安全管理中心雲端主控台。
2. 在卡巴斯基安全管理中心雲端主控台指定您的使用者名稱和密碼來登入帳戶。
3. 如果您設定了雙步驟驗證，請輸入透過簡訊傳送給您或是身份驗證器應用程式中產生的一次性安全碼（視您設定的雙步驟驗證方法而定）。

   入口頁面會顯示您擔任管理員的公司和其工作區清單。
4. 點擊**顯示存取權控制**連結。

   對公司具有存取權限的帳戶清單即會展開。
5. 點擊**授予存取權限**連結。
6. 在**郵件信箱**欄位中，指定您要授予存取權限之帳戶的電子郵件地址。
7. 在**存取權級別**清單中，選取要向輸入的帳戶分配的存取權限等級：

   - **管理員**

     具有此存取權限等級的使用者可以對公司和其工作區進行完整管理。
   - **使用者**

     具有此存取權限等級的使用者可以檢視可用工作區的清單並進入這些工作區。

   您無法向同一個公司內的同一個帳戶授予多個存取權限等級。
8. 點擊**授予**按鈕。

指定的帳戶即已獲得對您公司和其工作區的存取權限。該使用者可以登入公司並依所選的存取權限等級加以管理。

如果您向帳戶授予了**使用者**存取權限等級，則必須分配角色給該新增的使用者。否則，該使用者將無法進入工作區。

撤銷對您公司和其工作區的存取權限

如果您不想再讓使用者登入您的公司加以管理（例如，在使用者離職後），您可以撤銷其對您公司和其工作區的存取權限。

您無法撤銷自己對公司的存取權限。

若要撤銷對您公司和其工作區的存取權限：

1. 在您的瀏覽器中，前往卡巴斯基安全管理中心雲端主控台。
2. 在卡巴斯基安全管理中心雲端主控台指定您的使用者名稱和密碼來登入帳戶。
3. 如果您設定了雙步驟驗證，請輸入透過簡訊傳送給您或是身份驗證器應用程式中產生的一次性安全碼（視您設定的雙步驟驗證方法而定）。

   入口頁面會顯示您擔任管理員的公司和其工作區清單。
4. 點擊**顯示存取權控制**連結。

   對公司具有存取權限的帳戶清單即會展開。
5. 在您要撤銷存取權限的帳戶旁邊，點擊**撤銷** (🗑) 圖示。
6. 在開啟的**撤銷對公司的存取權**視窗中，點擊**確定**確認操作。

所選帳戶對您公司和其工作區的存取權限即已被撤銷。使用者無法再登入公司進行管理。

重設您的密碼

如果您忘記卡巴斯基安全管理中心雲端主控台帳戶的密碼，可以重設密碼來恢復存取帳戶。

若要重設帳戶密碼：

1. 在您的瀏覽器中，前往卡巴斯基安全管理中心雲端主控台。
2. 點擊**登入**按鈕，然後點擊**忘記密碼？**連結。
3. 輸入您在建立帳戶時指定的電子郵件地址。
4. 點擊**重設密碼**。

   一封包含重設密碼連結的電子郵件即會傳送到指定的地址。
5. 點擊該電子郵件中的連結。
6. 在開啟的視窗中，輸入新密碼並進行確認。
7. 如果您設定了秘密問題，請回答該問題。

   如果您設定了雙步驟驗證，請輸入透過簡訊傳送給您或是身份驗證器應用程式中產生的一次性安全碼（視您設定的雙步驟驗證方法而定）。
8. 點擊**繼續**。

   新的卡巴斯基安全管理中心雲端主控台登入密碼即已儲存。

如果您並未收到電子郵件，請檢查所輸入的電子郵件地址和您的垃圾郵件資料夾，然後再試一次。如果重試後仍未收到郵件，則指定的電子郵件地址可能並未在網站上註冊。請聯絡 Kaspersky 技術支援。

在卡巴斯基安全管理中心雲端主控台中編輯帳戶的設定

本節提供關於如何在卡巴斯基安全管理中心雲端主控台中編輯和刪除帳戶的指示。

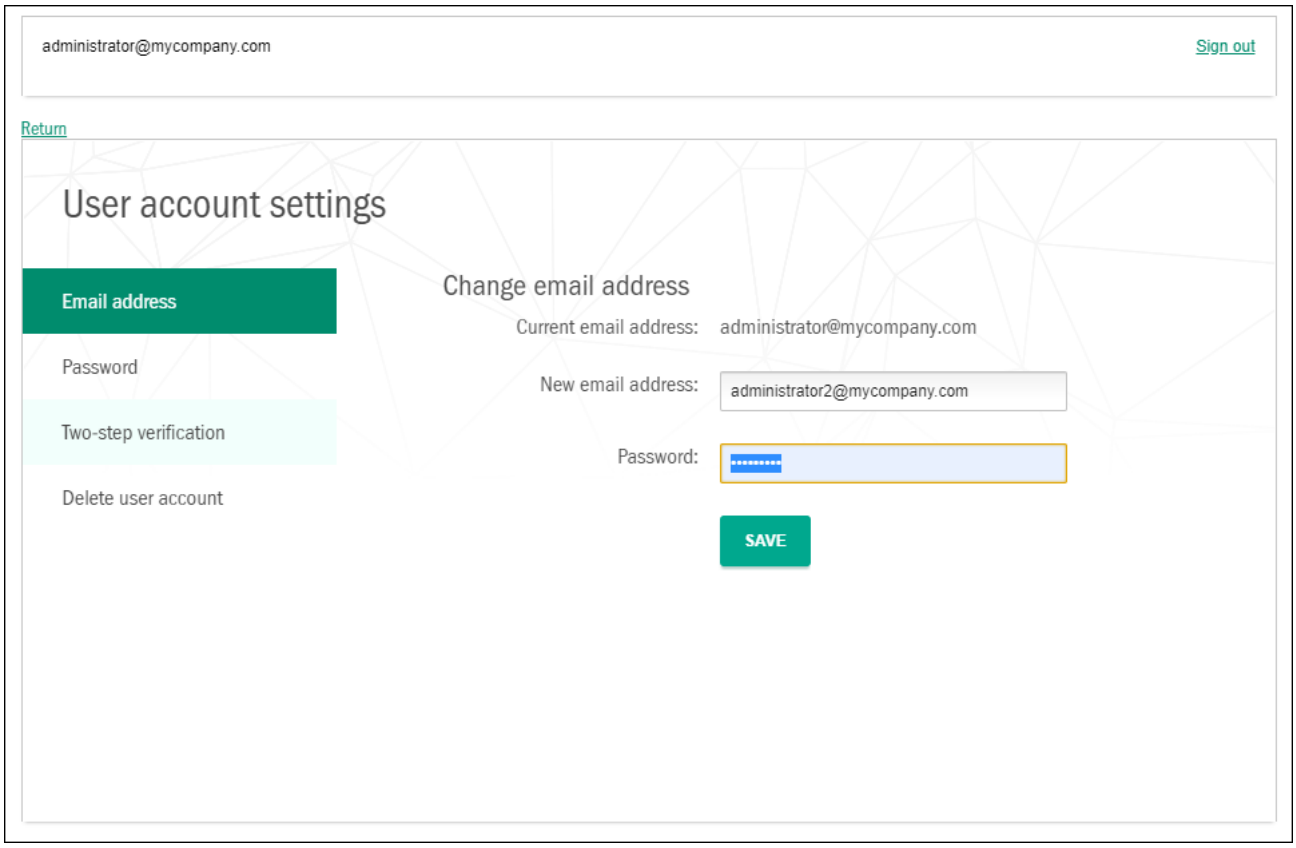
變更電子郵件地址

若要在卡巴斯基安全管理中心雲端主控台的帳戶設定中變更您的電子郵件地址：

1. 在卡巴斯基安全管理中心雲端主控台中，點擊包含您帳戶名稱的連結，然後選取**管理使用者帳戶**。

   使用者帳戶設定視窗即會開啟。

2. 選擇**郵件信箱**區段（請參閱下圖）。



在卡巴斯基安全管理中心雲端主控台的帳戶設定中變更電子郵件地址

郵件信箱區段會顯示您目前的電子郵件地址、一個用於輸入新地址的輸入欄位、一個用於輸入密碼的輸入欄位，以及**儲存**按鈕。

3. 在**新電郵地址**輸入欄位中，輸入您新的電子郵件。

   請小心輸入地址。如果輸入的地址無效，您將無法進入帳戶並使用卡巴斯基安全管理中心雲端主控台。

4. 在**密碼**輸入欄位中，輸入您目前的密碼。

5. 點擊**儲存**按鈕。

6. 點擊**返回**連結返回卡巴斯基安全管理中心雲端主控台，或是點擊**登出**連結離開入口。

您在卡巴斯基安全管理中心雲端主控台帳戶設定與我的卡巴斯基帳戶設定中的電子郵件地址現已變更。一封郵件會傳送到您新的電子郵件地址，通知您用於存取帳戶的電子郵件地址已變更。您下次登入卡巴斯基安全管理中心雲端主控台時，必須指定新的電子郵件地址。

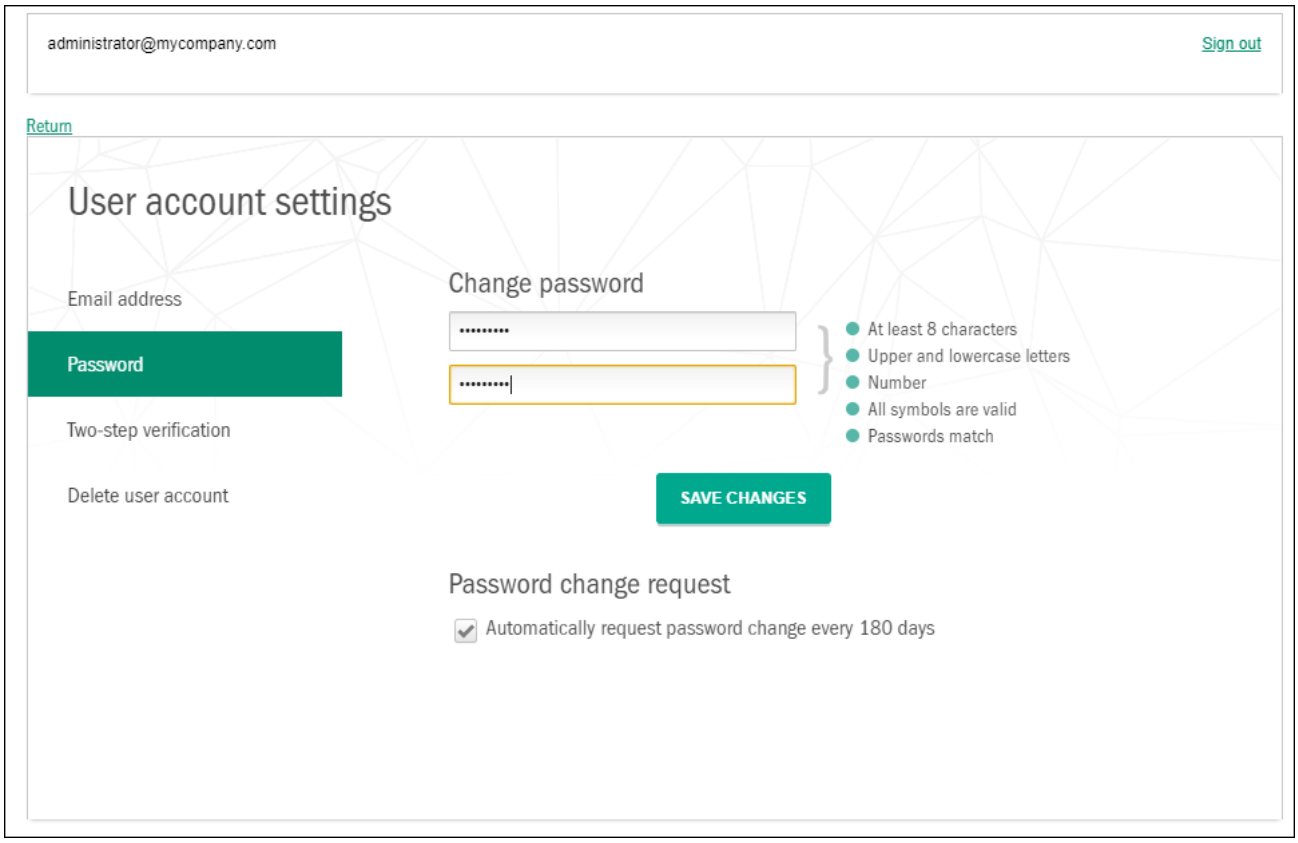
變更密碼

若要在卡巴斯基安全管理中心雲端主控台的帳戶設定中變更您的密碼：

1. 在卡巴斯基安全管理中心雲端主控台中，點擊包含您帳戶名稱的連結，然後選取**管理使用者帳戶**。

   使用者帳戶設定視窗即會開啟。

2. 選取**密碼**區段（請參閱下圖）。



在卡巴斯基安全管理中心雲端主控台中變更帳戶密碼

   此區段會顯示用於輸入新密碼和進行確認的欄位，以及**儲存變更**按鈕。

3. 輸入新密碼並在對應的輸入欄位中進行確認。

   密碼輸入欄位的右側會顯示對密碼的要求。您必須遵守這些要求，才能儲存新密碼。

4. 選取或清除**每 180 天自動請求變更密碼**核取方塊。

   預設情況下已選取此方塊。

5. 點擊**儲存變更**按鈕。

6. 點擊**返回**連結返回卡巴斯基安全管理中心雲端主控台，或是點擊**登出**連結離開入口。

   您的密碼現已變更。您登入卡巴斯基安全管理中心雲端主控台和登入我的卡巴斯基時，都將必須輸入新密碼。

使用雙步驟驗證

本節說明有助於讓您的卡巴斯基安全管理中心雲端主控台帳戶更加安全的雙步驟驗證。

關於雙步驟驗證

雙步驟驗證有助於讓您在 Kaspersky Security Center Cloud Console 中的帳戶更為安全。啟用此功能後，您每次使用電子郵件地址和密碼登入 Kaspersky Security Center Cloud Console 時，都必須額外輸入一次性安全碼。使用雙步驟驗證時，竊得或猜到您密碼的罪犯還必須能夠查看您的行動電話，否則無法登入您的帳戶。此外，啟用雙步驟驗證後，如果您忘記密碼，還必須額外輸入一次性安全碼。

設定雙步驟驗證後，接下來您要做的事就是保護您行動電話的實體安全，並維護對您行動電話號碼的存取安全。

您可以透過以下任一方式取得一次性安全碼：

- 透過簡訊將安全碼傳送到您的行動電話號碼。

  在此情況下，如果您無法存取您的行動電話，您將無法登入您的卡巴斯基安全管理中心雲端主控台帳戶，直到您又能恢復存取該電話號碼為止。

- 在您行動電話上安裝的身份驗證器應用程式中產生安全碼。

  我們強烈建議您設定透過身份驗證器應用程式進行的雙步驟驗證。在此情況下，即使您的行動電話未連上網際網路或行動網路，您仍能登入您的帳戶。

  我們僅測試過 Google Authenticator 和 Microsoft Authenticator 對卡巴斯基安全管理中心雲端主控台的相容性，而這些應用程式在當時是免費使用的。這些應用程式的介面可能並無您偏好的語言版本。在使用應用程式之前，亦請查看應用程式的 GDPR 合規性和隱私權政策。Kaspersky 與這些應用程式的發行者之間完全無任何贊助、背書或任何其他關係。

  > Microsoft Authenticator 僅能安裝到行動裝置上。

  我們還建議您在自己行動電話以外的裝置上安裝身份驗證器應用程式。如此一來，如果您的行動電話失竊，您仍能登入您的帳戶。

  如果您的行動電話失竊，造成您無法存取該行動電話，而您在其他裝置上又無身份驗證器應用程式，您將無法登入您的卡巴斯基安全管理中心雲端主控台帳戶，直到您又能恢復存取該電話號碼為止。屆時請使用透過簡訊傳送的安全碼。

> 如果您先前設定了祕密問題，好在想不起密碼時用於找回密碼，則設定雙步驟驗證後，祕密問題功能將永久停用。

情境：設定雙步驟驗證

雙步驟驗證有助於讓您的卡巴斯基安全管理中心雲端主控台帳戶更加安全。完成本節的情境後，您的帳戶將已設定雙步驟驗證。

此情境分多個階段進行：

1. **新增您的電話號碼**

   在此階段，您會設定透過簡訊進行的雙步驟驗證。

2. **安裝和設定身份驗證器應用程式**

   安裝和設定身份驗證器應用程式。

我們強烈建議您設定透過身份驗證器應用程式進行的雙步驟驗證。在此情況下，即使您的行動電話未連上網際網路或行動網路，您仍能登入您的帳戶。

我們還建議您在自己行動電話以外的裝置安裝身份驗證器應用程式。如此一來，如果您的行動電話失竊，您仍能登入您的帳戶。

3. **變更您的電話號碼**

   如有必要，您可以變更雙步驟驗證使用的電話號碼。

設定透過簡訊進行的雙步驟驗證

若要設定透過簡訊進行的雙步驟驗證：

1. 在卡巴斯基安全管理中心雲端主控台中，點擊包含您帳戶名稱的連結，然後選取**管理使用者帳戶**。

   使用者帳戶設定視窗即會開啟。

2. 選取**雙步驟驗證**區段。

3. 點擊**設定**按鈕。

4. 在**輸入現時密碼**下，指定您卡巴斯基安全管理中心雲端主控台帳戶的密碼，然後點擊**繼續**按鈕。

5. 在**指定您的流動電話號碼**下，指定您想要在雙步驟驗證中使用的行動電話號碼，然後點擊**下一步**按鈕。

   > 您可以將同一個電話號碼用於最多五個帳戶。

   一組 6 位數安全碼即會傳送到指定的電話號碼。

6. 在**確認您的電話號碼**下，輸入收到的安全碼。

雙步驟驗證即已設定完成。現在，您每次使用電子郵件地址和密碼進行登入或是忘記密碼時，都需要輸入透過簡訊傳送到所指定電話號碼的一次性安全碼。

您現在可以安裝並設定身份驗證器應用程式、變更您的電話號碼，或是停用雙步驟驗證。

設定透過身份驗證器應用程式進行的雙步驟驗證

在卡巴斯基安全管理中心雲端主控台中，身份驗證器應用程式不能作為獨立的驗證方法來使用。您必須先設定透過簡訊進行的雙步驟驗證。如果您停用透過行動電話號碼進行的雙步驟驗證，則透過身份驗證器應用程式進行的驗證會自動關閉。當透過簡訊和透過應用程式進行的驗證都設定好後，您就能在登入頁面或在忘記密碼時選取驗證方法。

若要設定透過身份驗證器應用程式進行的雙步驟驗證：

1. 設定透過簡訊進行的雙步驟驗證。

2. 下載、安裝並執行您要使用的身份驗證器應用程式。

我們僅測試過 Google Authenticator 和 Microsoft Authenticator 對卡巴斯基安全管理中心雲端主控台的相容性，而這些應用程式在當時是免費使用的。這些應用程式的介面可能並無您偏好的語言版本。在使用應用程式之前，亦請查看應用程式的 GDPR 合規性和隱私權政策。Kaspersky 與這些應用程式的發行者之間完全無任何贊助、背書或任何其他關係。

Microsoft Authenticator 僅能安裝到行動裝置上。

如有需要，您可以使用其他應用程式，但風險自負。您使用的應用程式必須支援 6 位數安全碼。

我們還建議您在自己行動電話以外的裝置安裝身份驗證器應用程式。如此一來，如果您的行動電話失竊，您仍能登入您的帳戶。

3. 在卡巴斯基安全管理中心雲端主控台中，點擊包含您帳戶名稱的連結，然後選取**管理使用者帳戶**。

   使用者帳戶設定視窗即會開啟。

4. 選取**雙步驟驗證**區段。

5. 點擊**獲取密鑰**按鈕。

6. 在**輸入現時密碼**下，指定您卡巴斯基安全管理中心雲端主控台帳戶的密碼，然後點擊**繼續**按鈕。

   入口頁面會顯示一組 16 個字元的秘密金鑰和一個 QR code。

7. 在每個裝置上的身份驗證器應用程式中，建立帳戶並輸入所顯示的秘密金鑰。或者，您也可以使用行動電話掃描 QR code。在此情況下，帳戶將會自動建立。如需更多資訊，請參閱您應用程式的說明文件。

   您的身份驗證器應用程式中即會產生一組 6 位數安全碼。

8. 確認您在每個裝置上的應用程式中產生的安全碼都相同。

9. 在卡巴斯基安全管理中心雲端主控台中，輸入所產生的安全碼。

透過身份驗證器應用程式進行的雙步驟驗證即已設定完成。現在，您每次使用電子郵件地址和密碼登入或是忘記密碼時，都需要輸入身份驗證器應用程式中產生的一次性安全碼。

您現在可以停用身份驗證器應用程式或完全停用雙步驟驗證。

變更您的行動電話號碼

若要變更透過簡訊進行的雙步驟驗證所用的行動電話號碼：

1. 在卡巴斯基安全管理中心雲端主控台中，點擊包含您帳戶名稱的連結，然後選取**管理使用者帳戶**。

   使用者帳戶設定視窗即會開啟。

2. 選取**雙步驟驗證**區段。

3. 在**電話號碼**下，點擊**變更電話號碼**連結。

4. 在**指定您的流動電話號碼**下，指定要在雙步驟驗證中使用的新行動電話號碼，然後點擊**下一步**按鈕。

5. 在**輸入現時密碼**下，指定您卡巴斯基安全管理中心雲端主控台帳戶的密碼，然後點擊**繼續**按鈕。

   一組 6 位數安全碼即會傳送到指定的電話號碼。

6. 在**確認您的電話號碼**下，輸入收到的安全碼。

您的行動電話號碼即已變更。現在，一次性安全碼將傳送到新的電話號碼。

停用雙步驟身分驗證

如果您不想再使用雙步驟驗證，可依本節所述方式加以停用。

停用雙步驟驗證將會降低您帳戶的安全性。我們強烈建議您繼續使用雙步驟驗證。

如果您設定了透過簡訊進行的雙步驟驗證，則可以停用雙步驟驗證。如果您設定了透過身份驗證器應用程式進行的雙步驟驗證，則可以停用該應用程式，或是完全停用雙步驟驗證。

若要停用身份驗證器應用程式：

1. 在卡巴斯基安全管理中心雲端主控台中，點擊包含您帳戶名稱的連結，然後選取**管理使用者帳戶**。

   使用者帳戶設定視窗即會開啟。

2. 選取**雙步驟驗證**區段。

3. 在**身份驗證器應用程式**下，點擊**停用身份驗證器應用程式**連結。

4. 在**輸入現時密碼**下，指定您卡巴斯基安全管理中心雲端主控台帳戶的密碼，然後點擊**繼續**按鈕。

   身份驗證器應用程式即會停用。透過身份驗證器應用程式進行雙步驟驗證的設定亦會刪除。您現在可以刪除您在身份驗證器應用程式中的帳戶。

   之後，您可以重新設定透過身份驗證器應用程式進行的雙步驟驗證。

若要完全停用雙步驟驗證：

1. 在卡巴斯基安全管理中心雲端主控台中，點擊包含您帳戶名稱的連結，然後選取**管理使用者帳戶**。

   使用者帳戶設定視窗即會開啟。

2. 選取**雙步驟驗證**區段。

3. 在**電話號碼**下，點擊**停用雙步驟驗證**連結。

4. 在**輸入現時密碼**下，指定您卡巴斯基安全管理中心雲端主控台帳戶的密碼，然後點擊**繼續**按鈕。

   雙步驟驗證即會停用。如果您使用了透過身份驗證器應用程式進行的雙步驟驗證，則雙步驟驗證的設定將會刪除。您現在可以刪除您在身份驗證器應用程式中的帳戶。

   之後，您可以重新設定雙步驟驗證。

在卡巴斯基安全管理中心雲端主控台中刪除帳戶

如果您想停止使用卡巴斯基安全管理中心雲端主控台，可以刪除您的帳戶。

刪除帳戶時，該帳戶的所有相關資料都會遺失。

刪除帳戶後，您即無法再存取您在 Kaspersky Endpoint Security Cloud、Kaspersky Security for Microsoft Office 365 和卡巴斯基安全管理中心雲端主控台中的工作區。如果您是工作區中唯一的管理員，則該工作區將會刪除。此外，您將無法存取我的卡巴斯基帳戶。

若要在卡巴斯基安全管理中心雲端主控台中刪除帳戶：

1. 在卡巴斯基安全管理中心雲端主控台中，點擊包含您帳戶名稱的連結，然後選取**管理使用者帳戶**。
   使用者帳戶設定視窗即會開啟。
2. 選取**刪除使用者帳戶**區段。
   刪除使用者帳戶區段會顯示關於帳戶刪除後果的資訊，而在這些資訊的下方，會顯示**刪除**按鈕。
3. 請閱讀這些帳戶刪除資訊，然後點擊**刪除**按鈕。
   輸入您的使用者帳戶密碼視窗即會開啟。
4. 在密碼輸入欄位中，輸入您的密碼，然後點擊**繼續**按鈕。

   您的帳戶即會刪除。

選取用於儲存卡巴斯基安全管理中心雲端主控台資訊的資料中心

卡巴斯基安全管理中心雲端主控台中的工作區是使用以 Microsoft Azure 雲端平台為基礎的全球資料中心網路內的伺服器來建立。所選用於架設受管理工作區的資料中心，取決於您在卡巴斯基安全管理中心雲端主控台中註冊工作區時所指定的國家/地區（請參閱下表）。安全應用程式的分發套件會提供於工作區所在的同一部伺服器上。

公司位置與 Microsoft Azure 區域的對應

公司所在國家/地區	Microsoft 資料中心區域
阿根廷	巴西南部
玻利維亞	巴西南部
巴西	巴西南部
智利	巴西南部
哥倫比亞	巴西南部
厄瓜多	巴西南部
蓋亞那	巴西南部
秘魯	巴西南部
巴拉圭	巴西南部
蘇利南	巴西南部
烏拉圭	巴西南部
委內瑞拉	巴西南部
安地卡及巴布達	美國東部
安圭拉	美國東部
阿魯巴	美國東部

巴貝多	美國東部
聖巴泰勒米島	美國東部
博奈爾島、聖尤斯特歇斯島和薩巴島	美國東部
貝里斯	美國東部
哥斯大黎加	美國東部
古巴	美國東部
庫拉索	美國東部
多米尼克	美國東部
多明尼加共和國	美國東部
格瑞那達	美國東部
瓜德羅普	美國東部
瓜地馬拉	美國東部
宏都拉斯	美國東部
海地	美國東部
牙買加	美國東部
聖克里斯多福與尼維斯	美國東部
開曼群島	美國東部
聖露西亞	美國東部
聖馬丁島	美國東部
馬丁尼克	美國東部
蒙塞拉特島	美國東部
尼加拉瓜	美國東部
巴拿馬	美國東部
波多黎各	美國東部
荷屬聖馬丁	美國東部
千里達及托巴哥	美國東部
聖文森及格瑞那丁	美國東部
英屬維京群島	美國東部
美屬維京群島	美國東部
日本	美國東部
加拿大（新布倫瑞克省）	美國東部
加拿大（紐芬蘭與拉布拉多省）	美國東部
加拿大（諾瓦斯科西亞省）	美國東部
加拿大（安大略省）	美國東部
加拿大（愛德華王子島省）	美國東部
加拿大（魁北克省）	美國東部

美國（阿拉巴馬州）	美國東部
美國（阿肯色州）	美國東部
美國（康乃狄克州）	美國東部
美國（哥倫比亞特區）	美國東部
美國（德拉瓦州）	美國東部
美國（佛羅里達州）	美國東部
美國（喬治亞州）	美國東部
美國（愛荷華州）	美國東部
美國（伊利諾州）	美國東部
美國（印第安納州）	美國東部
美國（肯塔基州）	美國東部
美國（路易斯安那州）	美國東部
美國（麻薩諸塞州）	美國東部
美國（馬里蘭州）	美國東部
美國（緬因州）	美國東部
美國（密西根州）	美國東部
美國（明尼蘇達州）	美國東部
美國（密蘇里州）	美國東部
美國（密西西比州）	美國東部
美國（北卡羅來納州）	美國東部
美國（新罕布夏州）	美國東部
美國（新澤西州）	美國東部
美國（紐約州）	美國東部
美國（俄亥俄州）	美國東部
美國（賓夕維尼亞州）	美國東部
美國（羅德島州）	美國東部
美國（南卡羅來納州）	美國東部
美國（田納西州）	美國東部
美國（維吉尼亞州）	美國東部
美國（佛蒙特州）	美國東部
美國（威斯康辛州）	美國東部
美國（西維吉尼亞州）	美國東部
阿爾巴尼亞	北歐（愛爾蘭）
波士尼亞與赫塞哥維納	北歐（愛爾蘭）
保加利亞	北歐（愛爾蘭）
白俄羅斯	北歐（愛爾蘭）

捷克	北歐（愛爾蘭）
丹麥	北歐（愛爾蘭）
愛沙尼亞	北歐（愛爾蘭）
芬蘭	北歐（愛爾蘭）
英國	北歐（愛爾蘭）
格陵蘭	北歐（愛爾蘭）
希臘	北歐（愛爾蘭）
克羅埃西亞	北歐（愛爾蘭）
匈牙利	北歐（愛爾蘭）
愛爾蘭島	北歐（愛爾蘭）
冰島	北歐（愛爾蘭）
吉爾吉斯斯坦	北歐（愛爾蘭）
哈薩克	北歐（愛爾蘭）
立陶宛	北歐（愛爾蘭）
拉脫維亞	北歐（愛爾蘭）
摩爾多瓦	北歐（愛爾蘭）
蒙特內哥羅共和國	北歐（愛爾蘭）
馬其頓共和國	北歐（愛爾蘭）
蒙古	北歐（愛爾蘭）
挪威	北歐（愛爾蘭）
波蘭	北歐（愛爾蘭）
羅馬尼亞	北歐（愛爾蘭）
塞爾維亞共和國	北歐（愛爾蘭）
俄羅斯	北歐（愛爾蘭）
瑞典	北歐（愛爾蘭）
斯洛維尼亞	北歐（愛爾蘭）
斯洛伐克	北歐（愛爾蘭）
塔吉克	北歐（愛爾蘭）
土庫曼	北歐（愛爾蘭）
烏茲別克	北歐（愛爾蘭）
加拿大（亞伯達省）	美國西部
加拿大（不列顛哥倫比亞省）	美國西部
加拿大（緬尼托巴省）	美國西部
加拿大（西北特區）	美國西部
加拿大（努納福特區）	美國西部
加拿大（育空特區）	美國西部

加拿大（薩克其萬省）	美國西部
墨西哥	美國西部
美國（阿拉斯加州）	美國西部
美國（亞利桑那州）	美國西部
美國（加利福尼亞州）	美國西部
美國（科羅拉多州）	美國西部
美國（夏威夷州）	美國西部
美國（愛達荷州）	美國西部
美國（堪薩斯州）	美國西部
美國（蒙大拿州）	美國西部
美國（北達科他州）	美國西部
美國（內布拉斯加州）	美國西部
美國（新墨西哥州）	美國西部
美國（內華達州）	美國西部
美國（奧克拉荷馬州）	美國西部
美國（奧勒岡州）	美國西部
美國（南達科他州）	美國西部
美國（德克薩斯州）	美國西部
美國（猶他州）	美國西部
美國（華盛頓州）	美國西部
美國（懷俄明州）	美國西部
美國（其他行政區）	美國東部
其他國家/地區	西歐（荷蘭）

存取公用 DNS 伺服器

卡巴斯基安全管理中心雲端主控台如果無法透過系統 DNS 存取 Kaspersky 伺服器，則可能會依所列順序使用以下公用 DNS 伺服器：

1. Google Public DNS (8.8.8.8)
2. Cloudflare DNS (1.1.1.1)
3. Alibaba Cloud DNS (223.6.6.6)
4. Quad9 DNS (9.9.9.9)
5. CleanBrowsing (185.228.168.168)

因為網路代理是與 DNS 伺服器建立 TCP/UDP 連線，所以對這些 DNS 伺服器的請求可能會包含用戶端裝置的網域位址與公用 IP 位址。如果卡巴斯基安全管理中心雲端主控台是使用公用 DNS 伺服器，則資料處理會受相關服務的隱私權政策所約束。

情境：為透過卡巴斯基安全管理中心雲端主控台管理的管理伺服器建立階層

此情境說明您在為透過卡巴斯基安全管理中心雲端主控台（建立階層時會擔任主管理伺服器的角色）管理的管理伺服器建立階層時，所必須執行的操作。之後，該階層可用於將受管理裝置和物件從卡巴斯基安全管理中心移轉到卡巴斯基安全管理中心雲端主控台，以及透過卡巴斯基安全管理中心雲端主控台管理從屬管理伺服器和裝置。

卡巴斯基安全管理中心雲端主控台僅能擔任主管理伺服器，而內部部署運作的管理伺服器則僅能擔任從屬管理伺服器。其他階層模式均無法使用。

先決條件

在開始之前，請確保滿足以下先決條件：

- 將內部部署運作的管理伺服器升級至版本 12 或以上版本。
- 在內部部署運作的管理伺服器上，安裝卡巴斯基安全管理中心網頁主控台。
- 為您計畫透過卡巴斯基安全管理中心雲端主控台管理的應用程式安裝專用的 Web 外掛程式。
- 將受管理應用程式升級至卡巴斯基安全管理中心雲端主控台支援的版本。
- 在內部部署運作的管理伺服器上，確定「將更新下載至管理伺服器儲存區」工作中指定的更新來源並非主管理伺服器；如有必要，請適當修改工作設定。

建立階層後，卡巴斯基安全管理中心雲端主控台中有效的政策與工作會套用到從屬管理伺服器，進而取代其上現有的政策與工作。若要避免此行為，請在建立階層之前先刪除卡巴斯基安全管理中心雲端主控台的所有政策與工作。或者，您也可以到每個卡巴斯基安全管理中心雲端主控台政策的設定中將狀態變更為 **非作用中**，並且到每個卡巴斯基安全管理中心雲端主控台工作的設定中停用**分發到從屬和虛擬管理伺服器**選項。

如有必要，您可以隨時刪除管理伺服器階層。

階層建立的各階段

本基本情境是針對從屬管理伺服器在網際網路上無法供存取的情況來提供。不過，如果從屬管理伺服器在網際網路上可供存取，則以下所述部分步驟中的操作可能會有所不同。此外，在此種情況下還必須略過某些步驟。

管理伺服器階層的建立包括以下階段：

1. **擷取從屬管理伺服器的憑證**

   如果從屬管理伺服器在網際網路上可供存取，請略過此步驟。

   在內部部署運作的卡巴斯基安全管理中心網頁主控台中，開啟管理伺服器內容，然後開啟**一般**頁籤上的**一般**區段。點擊**檢視管理伺服器憑證**連結。在您瀏覽器設定中所指定的資料夾內會自動儲存 CER 格式的憑證檔案。

2 從卡巴斯基安全管理中心雲端主控台擷取連線設定和憑證

如果從屬管理伺服器在網際網路上可供存取，請略過此步驟。

在卡巴斯基安全管理中心雲端主控台中，開啟管理伺服器內容，然後開啟**一般**頁籤上的**管理伺服器階層**區段。畫面上即會顯示以下連線設定：

- **HDS 位址**

  顯示用於進行 Hosted Discovery Service (HDS) 連線的網址。

- **HDS 連接埠**

  顯示用於進行 HDS 連線的連接埠號。

該區段還包含兩個連結：

- **檢視管理伺服器憑證**

  點擊此連結會開始下載卡巴斯基安全管理中心雲端主控台實例憑證的公開金鑰。

- **HDS 根 CA 憑證**

  點擊此連結會開始下載 .pem 格式的檔案，其中會包含憑證機構 (CA) 所簽發受信任根憑證的清單。此檔案是專為供從屬管理伺服器使用而設計：需要有它才能驗證 HDS 憑證。

手動複製連線設定（使用剪貼簿或透過任何其他您方便的方式），然後儲存到任何格式（您方便就好）的檔案。點擊**檢視管理伺服器憑證**連結，然後等待憑證檔案下載完成。點擊 **HDS 根 CA 憑證**連結，然後等待含有憑證機構所簽發受信任根憑證之清單的檔案下載完成。這兩個檔案都會儲存到您的瀏覽器設定中所指定的資料夾內。

3 選取要連線的從屬管理伺服器

在管理伺服器內容中，前往**管理伺服器**頁籤。在管理群組階層中，選取要包含從屬管理伺服器及其所有受管理裝置的管理群組旁邊的核取方塊。點擊**連線從屬管理伺服器**按鈕。

在開啟的頁面上，在**從屬管理伺服器顯示名稱**欄位中指定從屬管理伺服器在階層中必須顯示的名稱。這純粹是方便您辨識之用，因此可視需要設為與從屬管理伺服器的實際名稱不同的名稱。點擊**"下一步"**。

如果從屬管理伺服器在網際網路上可供存取，則您還必須在 **從屬管理伺服器位址（可選）** 欄位中指定從屬管理伺服器的位址。

在下一頁，點擊**瀏覽**按鈕，然後指定您從從屬管理伺服器儲存的 .pem 檔案。點擊**"下一步"**。

4 啟用並設定代理伺服器

此步驟中所述的操作為可選的操作。僅有當您的連線需要使用代理伺服器時，才需要執行這些操作。

點擊**"下一步"**。在**定義如何將從屬管理伺服器連線到主管理伺服器**頁面上，您可以視需要啟用並設定代理伺服器。選取**使用代理伺服器**核取方塊，然後指定以下代理設定：

- **位址**

代理伺服器位址。

- **使用者名稱**

  用於登入代理伺服器的使用者名稱。

- **密碼**

  用於登入代理伺服器的密碼。

5. **指定身分驗證設定，然後將從屬管理伺服器新增至階層中**

   點擊**"下一步"**。在**從屬管理伺服器憑證**頁面上，指定以下設定：

   - **使用者名稱**

     您用於登入從屬管理伺服器的使用者名稱。

   - **密碼**

     用於登入從屬管理伺服器的密碼。

   點擊**下一步**，然後等待從屬管理伺服器出現在階層中。

   如果從屬管理伺服器在網際網路上可供存取，則它會連線到主管理伺服器。

   如果從屬管理伺服器在網際網路上可供存取，且這兩個管理伺服器之間的連線建立成功，則請略過所有進一步的步驟。

   如果從屬管理伺服器在網際網路上無法供存取，則它會變得可見，但您必須在從屬管理伺服器上執行額外操作，才能對其進行控制。

6. **在內部部署運作的卡巴斯基安全管理中心網頁主控台中設定連線**

   在內部部署運作的卡巴斯基安全管理中心網頁主控台中，開啟管理伺服器內容，然後開啟**一般**頁籤上的**管理伺服器階層**區段。選取**此管理伺服器是階層中的從屬伺服器**核取方塊。在**主管理伺服器類型**清單中，選取**Kaspersky Security Center Cloud Console**選項。

   卡巴斯基安全管理中心網頁主控台會檢查*將更新下載至管理伺服器儲存區*工作中指定的更新來源是否為主管理伺服器。如果指定的更新來源是主管理伺服器，則您會收到相對應的警告訊息以及工作設定連結。您可以先修改設定再回來建立階層，也可以略過此操作，直接繼續建立階層。

   在**用於在從屬管理伺服器與主管理伺服器之間建立連線的設定**群組中，指定以下設定：

   - **HDS 伺服器位址（從 Cloud Console 上的主管理伺服器）**

     輸入您從卡巴斯基安全管理中心雲端主控台的管理伺服器內容中複製並儲存之完全限定網域名稱 (FQDN) 格式的 HDS 伺服器位址。

   - **HDS 伺服器連接埠**

輸入您從卡巴斯基安全管理中心雲端主控台的管理伺服器內容中複製並儲存的 HDS 伺服器連接埠號。

7. **將憑證新增到從屬管理伺服器中**

   點擊**指定主管理伺服器憑證**按鈕，然後指定您從卡巴斯基安全管理中心雲端主控台的管理伺服器內容中儲存的憑證檔案。

   點擊**指定 Hosted Discovery Service 憑證**按鈕，然後指定您從卡巴斯基安全管理中心雲端主控台的管理伺服器內容中儲存的 .pem 檔案。

   如果您在卡巴斯基安全管理中心雲端主控台中連接從屬管理伺服器時啟用了代理伺服器，請選取**使用代理伺服器**核取方塊，然後指定與卡巴斯基安全管理中心雲端主控台中相同的代理設定。

   如果從屬管理伺服器是位於非警戒區 (DMZ)，您還可以選取**將主管理伺服器連線到 DMZ 中的從屬管理伺服器**核取方塊。

   從屬管理伺服器即會連線到主管理伺服器。

結果

執行上述步驟後，您可以透過以下跡象，確認階層建立成功：

- 主管理伺服器的作用中政策在從屬管理伺服器上生效。主管理伺服器的工作獲分發給從屬管理伺服器。如果某個群組工作的設定中啟用了**分發到從屬和虛擬管理伺服器**選項，則每個該等工作也會獲分發給從屬管理伺服器。
- 在主管理伺服器上被鎖定而無法變更的政策設定，在從屬管理伺服器上的所有原則中都顯示為被鎖定而無法變更。
- 主管理伺服器套用的政策顯示在從屬管理伺服器的政策清單中（**資產（裝置）→政策和設定檔**）。
- 主管理伺服器分發的群組工作顯示在從屬管理伺服器的工作清單中（**資產（裝置）→工作**）。
- 在主管理伺服器上建立的政策和工作，在從屬管理伺服器上無法被修改。
- 在卡巴斯基安全管理中心雲端主控台中的管理群組結構內，從屬管理伺服器顯示在您新增該管理伺服器時所選的群組內。

移轉至卡巴斯基安全管理中心雲端主控台

本節說明從內部部署執行的卡巴斯基安全管理中心網頁主控台（版本 12 或更新版本）移轉到卡巴斯基安全管理中心雲端主控台的程序。

移轉至卡巴斯基安全管理中心雲端主控台的方法

本節提供資訊，說明將以內部部署執行之卡巴斯基安全管理中心移轉到卡巴斯基安全管理中心雲端主控台的適用方法。

透過移轉功能，您可以將網路裝置從卡巴斯基安全管理中心轉移到卡巴斯基安全管理中心雲端主控台的管理之下。您的受管理裝置將會切換而不會遺失主要設定，例如管理群組的會員身分以及基本物件，例如與受管理應用程式相關的政策和工作。

您可以選擇兩種可用方法的其中一種，以將管理伺服器移轉到卡巴斯基安全管理中心雲端主控台：

- 在沒有管理伺服器階層的情況下移轉：
  - 即使內部部署的管理伺服器不是卡巴斯基安全管理中心雲端主控台的從屬伺服器，也可以將受管理裝置和相關物件傳輸到卡巴斯基安全管理中心雲端主控台。
  - 如果在不同的實體裝置上開啟卡巴斯基安全管理中心網頁主控台和卡巴斯基安全管理中心雲端主控台，則可能需要傳輸檔案（在卸除式磁碟機上、透過電子郵件、透過共享資料夾或以其他任何方便使用的形式）。

  如果您的網路包含虛擬管理伺服器，也可以執行在有虛擬管理伺服器的情況下進行移轉。

- 使用管理伺服器階層移轉：
  - 僅使用卡巴斯基安全管理中心雲端主控台的介面就可以將受管理裝置和相關物件傳輸到卡巴斯基安全管理中心雲端主控台，因此不需要實體檔案傳輸。
  - 需要將在內部部署執行的管理伺服器作為卡巴斯基安全管理中心雲端主控台的從屬伺服器運作。您可以在開始移轉之前建立這類階層。

對於完整磁碟加密，卡巴斯基安全管理中心雲端主控台僅支援 BitLocker。

情境：在沒有管理伺服器階層的情況下移轉

本節說明從內部部署中執行的卡巴斯基安全管理中心網頁主控台將受管理裝置及相關物件（例如政策、工作、報告）移轉到卡巴斯基安全管理中心雲端主控台的方法。您可在移轉範圍中包含單一管理群組，以在卡巴斯基安全管理中心雲端主控台還原相同的管理群組。

該群組必須包含單個作業系統的受管理裝置。如果您的網路包含不同作業系統或 Linux 發行版的裝置，請將這些裝置分配到不同的管理群組，然後分別移轉每個群組。

完成移轉後，將透過卡巴斯基安全管理中心雲端主控台升級和管理移轉範圍內群組中的所有網路代理。

本節列出的步驟涵蓋了在沒有管理伺服器階層下執行的移轉過程，意即未在內部部署執行的卡巴斯基安全管理中心雲端主控台和卡巴斯基安全管理中心網頁主控台間建立連線。

先決條件

開始之前，請執行以下操作：

- 將執行內部佈署的管理伺服器升級至以下版本：
  - 對於 Windows 裝置 — 版本 12 或更高版本
  - 對於 Linux 裝置 — 版本 12 修補程式或更高版本
- 安裝卡巴斯基安全管理中心雲端主控台版本 12.1 或更高版本。
- 將受管理裝置上的網路代理升級到版本 12 或更高版本。
- 在 Windows 裝置上，使用沒有卸除安裝密碼的網路代理。
  如果已設定密碼，請在卡巴斯基安全管理中心雲端控制台中執行以下操作之一：
  - 停用**網路代理政策設定使用解除安裝密碼**Use uninstallation password選項。
  - 使用*遠端解除安裝應用程式*工作來遠端解除安裝網路代理。在工作的**要解除安裝的應用程式**欄位，選取**卡巴斯基安全管理中心網路代理**。不要忘記輸入卸除安裝密碼。
- 將受管理應用程式升級至卡巴斯基安全管理中心雲端主控台所支援的版本。
- 確保您有最新版本的受管理應用程式的政策。如果您使用過時的政策，為卡巴斯基安全管理中心雲端主控台支援的應用程式版本建立新的政策。
- 若要使用實際政策，請將您計畫透過卡巴斯基安全管理中心雲端主控台管理的應用程式專用的 Web 外掛程式進行升級。
- 如果卡巴斯基應用程式不受卡巴斯基安全管理中心雲端主控台支援，從受管理裝置卸除安裝這些應用程式，然後將卸除安裝的應用程式替換為受支援的應用程式。
- 解密執行 Windows 作業系統的受管理裝置上被 Kaspersky Endpoint Security for Windows 加密的所有資料（磁碟層級或檔案層級），並透過應用程式政策或透過本機將受管理裝置上的加密功能停用。有關詳細資訊，請參閱 Kaspersky Endpoint Security for Windows 的說明。

  若 Windows 裝置仍存有透過 Kaspersky Endpoint Security for Windows 加密的任何檔案或資料夾，則網路代理升級將在移轉程序期間取消。系統將會傳送通知提示您解密裝置上的所有資料並停用該加密功能。

卡巴斯基安全管理中心雲端主控台最多允許每部管理伺服器管理 25,000 部裝置。

移轉階段

移轉至卡巴斯基安全管理中心雲端主控台由下列階段組成：

1. **規劃移轉範圍與檢查先決條件**

   預估移轉程序的範圍，意即審核要匯出的管理群組及評估其中的受管理裝置數量。另外，請確認移轉先決條件中所列的所有活動都已成功完成。

2. **從卡巴斯基安全管理中心網頁主控台匯出受管理裝置、物件及設定**

   使用內部部署運作的卡巴斯基安全管理中心網頁主控台中的移轉精靈，將您的受管理裝置連同其物件一起匯出。

   匯出檔案大小上限為 4 GB。

3. **將匯出的檔案匯入到卡巴斯基安全管理中心雲端主控台**

   將受管理裝置和物件的相關資訊傳送到卡巴斯基安全管理中心雲端主控台。為此，請使用卡巴斯基安全管理中心雲端主控台移轉精靈來匯入匯出檔案並建立網路代理獨立安裝套件。

4. **在受管理裝置上重新安裝網路代理**

   返回內部部署運作的卡巴斯基安全管理中心網頁主控台中的移轉精靈，以建立遠端安裝工作。您將能夠（立即或稍後）使用此工作在受管理裝置上重新安裝網路代理並完成移轉過程。

結果

完成移轉後，您可確認它是否成功：

- 網路代理會重新安裝在所有受管理裝置上。
- 所有裝置都會透過卡巴斯基安全管理中心雲端主控台進行管理。
- 所有移轉前生效的物件設定都將保留。

移轉精靈

本節會為卡巴斯基安全管理中心雲端主控台與卡巴斯基安全管理中心網頁主控台版本 12 或以上版本中的移轉精靈提供相關資訊。

步驟 1。從卡巴斯基安全管理中心網頁主控台匯出受管理裝置、物件及設定

從卡巴斯基安全管理中心網頁主控台移轉受管理裝置至卡巴斯基安全管理中心雲端主控台時，您需要先建立匯出檔案，其中包含以內部部署執行之管理伺服器上存在的管理群組階層資訊。匯出檔案還必須包含有關物件及其設定的資訊。匯出檔案將會用來後續匯入卡巴斯基安全管理中心雲端主控台。

匯出檔案大小上限為 4 GB。

若要從卡巴斯基安全管理中心網頁主控台匯出物件與其設定：

1. 在卡巴斯基安全管理中心網頁主控台的主功能表中，前往**操作→移轉**。

2. 在移轉精靈的歡迎頁面中，選取**下一步**。**要匯出的受管理裝置**頁面隨即開啟，並顯示對應管理伺服器的整個管理群組階層

3. 在**要匯出的受管理裝置**頁面上，點擊**受管理裝置**群組名稱旁的臂章圖示 (>) 以展開管理群組階層。選取您要匯出的管理群組。

   對兩個管理群組執行從內部部署運作的卡巴斯基安全管理中心移轉到卡巴斯基安全管理中心雲端主控台的動作後，這些群組的遠端安裝工作會以相同的名稱顯示。

4. 選取其政策與工作必須一起與群組物件移轉至卡巴斯基安全管理中心雲端主控台的受管理應用程式。若要選取其物件要匯出的受管理應用程式，請選取清單中其名稱旁的核取方塊。

   儘管清單中顯示了卡巴斯基安全管理中心管理伺服器，但是選取相應的核取方塊不會導致匯出其政策。

   要確保卡巴斯基安全管理中心雲端主控台支援您的受管理應用程式，請點擊相應的連結。它將使您重新定向到包含卡巴斯基安全管理中心雲端主控台管理的應用程式清單的"線上說明"主題。

   若您選取的應用程式不受卡巴斯基安全管理中心雲端主控台支援，這些應用程式的政策與工作仍會匯出之後匯入，但您將無法在卡巴斯基安全管理中心雲端主控台管理，因為專屬外掛程式無法使用。

5. 檢視預設匯出的群組物件清單，並指定要與所選管理群組一起匯出之非群組物件，如有必要。透過包含或排出各種物件來配置匯出範圍，例如全域工作、自訂裝置分類、報告、自訂角色、內部使用者與安全群組，以及自訂應用程式類別。此頁面包含以下區段：

   - **全域工作**

     受管理應用程式的全域工作清單，以及網路代理的全域工作。

     若您所選的全域工作會套用至特定物件分類，系統也會匯出此分類。

     儘管清單中顯示了管理伺服器的全域工作，但是您無法將其匯出。選取這些工作不會影響匯出範圍。遠端安裝工作也保留在匯出範圍之外，因為無法匯出它們各自的安裝套件。

   - **裝置分類**

     自訂裝置分類的清單。

   - **報告**

     要匯出的可編輯清單報告實例。

     若您所選的報告會套用至特定物件分類，系統也會匯出此分類。

     卡巴斯基安全管理中心雲端主控台包含與卡巴斯基安全管理中心網頁主控台相同的報告範本集，因此您可以選取僅匯出手動建立或重新配置的報告。

   - **群組物件**

依預設要匯出群組物件的清單。與所選管理群組相關的以下物件會依預設匯出其整體：

- 管理群組結構，即所選管理群組的所有子群組
- 包含在要匯出之管理群組的裝置
- 指派給裝置以匯出的標籤

  若標籤已在卡巴斯基安全管理中心網頁主控台但從未指派給任何裝置，則不會匯出該標籤。自動標記規則也不會匯出。

- 所選的受管理應用程式的群組政策

  管理伺服器政策與網路代理政策不會匯出。

- 所選的受管理應用程式的群組工作與網路代理群組工作

  管理伺服器工作不會匯出。

抵也可以預防特定類型的非群組物件遭到匯出：

- 若要取消匯出自訂角色 (意即僅由使用者建立的那些角色)，請選取**將自訂角色排除在匯出範圍外**核取方塊。
- 若要取消匯出內部使用者與安全群組，請選取**將內部使用者和安全群組排除在匯出範圍外**核取方塊。
- 若要取消匯出有手動新增內容的自訂應用程式類別，請選取**將自訂應用程式類別排除在匯出範圍外**核取方塊。

如果您將各種作業系統的裝置轉移到卡巴斯基安全管理中心雲端主控台，則非群組物件只需移轉一次。

移轉精靈會檢查所選管理群組中所含受管理裝置的數量。如果此數字超過 10,000，則會出現錯誤訊息。**下一步**按鈕會保持無法使用（變暗），直到所選管理群組中受管理裝置的數量在限制範圍內為止。

6. 定義好移轉範圍後，請點擊**下一步**開始匯出程序。**建立匯出檔案**頁面即會開啟，供您檢視在移轉範圍中所加入每類物件的匯出進度。請等待片刻，直到物件清單中所有物件旁的重新整理圖示 (🔄) 更換為綠色勾號標記 (✓)。匯出程序完成且匯出檔案會自動下載至您瀏覽器設定的預設下載位置。匯出檔案名稱會顯示在瀏覽器視窗的底部。

7. 顯示**匯出已成功完成**頁面時，您可繼續在卡巴斯基安全管理中心雲端主控台執行的下個階段。

若您在不同裝置使用卡巴斯基安全管理中心網頁主控台和卡巴斯基安全管理中心雲端主控台，您需將匯出檔案複製至卸除式磁碟機或選擇其他傳輸檔案的方式。

步驟 2。將匯出的檔案匯入到卡巴斯基安全管理中心雲端主控台

若要傳輸將您從卡巴斯基安全管理中心 網頁主控台匯出之受管理裝置、物件與其設定的相關資訊，您需將其匯入佈署在您工作空間的卡巴斯基安全管理中心雲端主控台。這可讓您建立獨立安裝套件，並將其用來在受管理裝置上重新安裝網路代理。

在啟動卡巴斯基安全管理中心雲端主控台中的移轉精靈前，請確保其目前的本地化版本語言與匯出過程中所用卡巴斯基安全管理中心網頁主控台的語言相同。如有必要，請切換語言。

如果您先前已在卡巴斯基安全管理中心雲端主控台工作區完成快速啟動精靈，則**受管理裝置**群組會包含以預設設定建立的政策和工作。在匯入從卡巴斯基安全管理中心網頁主控台匯出的政策和任務之前，請先刪除這些政策和任務。

若要將匯出檔案匯入卡巴斯基安全管理中心雲端主控台：

1. 在卡巴斯基安全管理中心雲端主控台的主功能表中，前往**操作 → 移轉**。
2. 在移轉精靈的歡迎頁面中，點擊**匯入**。在開啟的 Windows 檔案總管視窗中，透過儲存匯出檔案的瀏覽資料夾選取匯出檔案，並點擊**開啟**。請等待檔案上傳狀態旁的重新整理圖示 (🔄) 更換為綠色勾號標記 (✓)。
3. 點擊**"下一步"**。下一頁隨即開啟，顯示卡巴斯基安全管理中心雲端主控台中管理伺服器管理群組的整個階層。
4. 針對必須還原之群組物件的目標管理群組選取在旁邊的核取方塊，接著點擊**下一步**。移轉精靈即會顯示卡巴斯基安全管理中心雲端主控台中可用之網路代理安裝套件的清單。
5. 選取內含網路代理相關版本與本地化的安裝套件，並點擊**下一步**。

   僅當您先前已在卡巴斯基安全管理中心雲端主控台工作區完成快速啟動精靈，而且您是執行 Windows 裝置移轉時，才選取 Kaspersky Network Agent for Windows 安裝套件。

   請等移轉精靈建立好獨立安裝套件。網路代理獨立安裝套件的檔案大小上限為 200 MB。

   檔案被解壓並自動下載到瀏覽器設定中定義的預設下載位置。非群組物件和群組物件將還原到目標管理群組。

   完成匯入時，管理群組的匯出結構，包含裝置的詳細資料，會顯示在所選目標管理群組下。若您還原的物件名稱與現有物件名稱相同，前者會使用增量尾碼新增。

   如果您已導入整個**受管理裝置**群組，建議您重新命名新導入的子群組以避免混淆：

   a. 前往**群組的階層**區域。

   b. 在群組樹狀目錄中點擊子群組的名稱。

   c. 在開啟的內容中，在**名稱**欄位中輸入其他名稱（例如，"已移轉的裝置"）。

   建議您檢查導出範圍中包含的物件（政策、工作和受管理裝置）是否已成功導入到卡巴斯基安全管理中心雲端主控台。為此，請前往**資產（裝置）**區段，並查看導入的物件是否出現在**政策和設定檔**、**工作**和**受管理裝置**子區段。

您無法最小化移轉精靈並在匯入期間執行任何並行作業。請等待片刻，直到物件清單中所有物件旁的重新整理圖示 (🔄) 更換為綠色勾號標記 (✓)，匯入隨即完成。之後，裝置會開始切換到卡巴斯基安全管理中心雲端主控台。

6. 點擊**完成**以關閉移轉精靈視窗。

7. 如果要再次查找和下載獨立安裝套件，請轉到**發現和佈署→佈署和分配→安裝套件**，然後點擊**檢視獨立安裝套件清單**按鈕。在開啟的清單中，選取已建立的獨立安裝套件，然後點擊**下載**按鈕。

若您在不同裝置使用卡巴斯基安全管理中心網頁主控台和卡巴斯基安全管理中心雲端主控台，您需將獨立安裝套件複製至卸除式磁碟機或選擇其他傳輸檔案的方式。

步驟 3。透過卡巴斯基安全管理中心雲端主控台管理的裝置重新安裝網路代理

建立網路代理獨立安裝套件後，您可繼續建立遠端安裝工作。執行該工作可讓您在所有受管理裝置上重新安裝網路代理，以將這些裝置切換到卡巴斯基安全管理中心雲端主控台的管理之下。

為了減少資料遺失的風險，建議您先對小型管理群組執行操作，該管理群組最多可對在公司網路內但不包含實體伺服器的 20 個受管理裝置進行計數。完成這些操作後，請確定重新安裝成功完成，然後才全面進行重新安裝。

若要建立遠端安裝工作並重新安裝網路代理：

1. 返回內部部署運作的卡巴斯基安全管理中心網頁主控台中的移轉精靈。

我們建議依下述方式，使用移轉精靈建立遠端安裝工作來重新安裝網路代理。如果需要使用自訂的遠端安裝工作，您需要先以網路代理獨立安裝套件為基礎，手動建立自訂安裝套件。請注意，建立自訂安裝套件時，必須在可執行檔命令列中指定「-s」參數。否則，以該自訂安裝套件重新安裝網路代理時，會出現錯誤。

您可視移轉精靈的目前狀態，進行以下其中一種操作：

- 若您匯出後並未關閉移轉精靈，而工作階段尚未到期，請點擊**前往移轉精靈的步驟 3** 按鈕。選取**上傳獨立安裝套件**核取方塊並點擊**選擇獨立安裝套件**按鈕。在開啟的瀏覽器視窗中，指定網路代理獨立安裝套件。

- 如果您因故必須重新啟動移轉精靈，請選取**上傳獨立安裝套件**核取方塊，然後點擊**選擇獨立安裝套件**按鈕。在開啟的瀏覽器視窗中，指定網路代理獨立安裝套件。之後，移轉精靈會再次顯示該管理伺服器的管理群組階層。選取與您已建立之匯出檔案相同的群組並點擊**下一步**。

移轉精靈會再次檢查所選管理群組中包含的受管理裝置數量。如果此數字超過 10,000，則會出現錯誤訊息。**下一步**按鈕會保持無法使用（變暗），直到所選管理群組中受管理裝置的數量在限制範圍內為止。

2. 請等待獨立安裝套件上傳，接著按一下**下一步**。移轉精靈即會建立自訂安裝套件和其適用的遠端安裝工作。工作範圍將包含您在**要匯出的受管理裝置**頁面上所選的管理群組；工作啟動排程依預設會設定在**手動**。移轉

精靈會顯示建立進度。請等待重新整理圖示 (🔄) 更換為綠色勾號標記 (✓)，接著點擊**下一步**。

3. 如有需要，請針對以內部部署執行之管理伺服器的所選管理群組與其所有子群組中的裝置，選取該裝置的**執行新建立的遠端安裝工作**核取方塊 (依預設會取消選取)。在此情況下，裝置會在卡巴斯基安全管理中心雲端主控台的管理下切換，但僅在網路代理安裝完成後進行。執行工作的管理群組會顯示完整路徑。

   請注意，工作必須在匯入卡巴斯基安全管理中心雲端主控台完成後啟動。否則，裝置名稱可能會在清單中重複。

4. 點擊**完成**關閉移轉精靈並啟動遠端安裝工作來達成以下目的：

   - 升級網路代理實例
   - 透過卡巴斯基安全管理中心雲端主控台切換管理的網路代理實例

   若您不選取**執行新建立的遠端安裝工作** 核取方塊，您可之後手動啟動工作，如有必要。

您可以檢查現在是否可以透過卡巴斯基安全管理中心雲端主控台管理移轉的網路代理實例。為此，請轉至**資產（裝置）→受管理裝置**。確保移轉的受管理裝置在**可見**中，**網路代理已安裝**和**網路代理正在執行**列具有確認圖標 (✓)。此外，請確保這些裝置沒有"*長時間未連線*"狀態描述。

在有管理伺服器階層的情況下移轉

本節說明如何將受管理裝置和相關物件從內部部署運作的卡巴斯基安全管理中心網頁主控台移轉到卡巴斯基安全管理中心雲端主控台。此過程與一個階層有關：內部部署執行的卡巴斯基安全管理中心網頁主控台會以從屬管理伺服器運作，而卡巴斯基安全管理中心雲端主控台會以主管理伺服器運作。

每個轉移到卡巴斯基安全管理中心雲端主控台的管理群組所含的受管理裝置，都必須是同一種作業系統。如果您的網路包含不同作業系統的裝置，請將這些裝置分配到不同的管理群組中，然後分別移轉每個群組。

完成移轉後，將透過卡巴斯基安全管理中心雲端主控台升級和管理移轉範圍內群組中的所有網路代理。

開始之前，請執行以下操作：

- 將執行內部佈署的管理伺服器升級至以下版本：
  - 對於 Windows 裝置 — 版本 12 或更高版本
  - 對於 Linux 裝置 — 版本 12 修補程式或更高版本
- 安裝卡巴斯基安全管理中心雲端主控台版本 12.1 或更高版本。
- 將受管理裝置上的網路代理升級到版本 12 或更高版本。
- 在 Windows 裝置上，使用沒有卸除安裝密碼的網路代理。
  如果已設定密碼，請在卡巴斯基安全管理中心雲端控制台中執行以下操作之一：
  - 停用**網路代理政策設定使用解除安裝密碼**Use uninstallation password選項。

- 使用*遠端解除安裝應用程式*工作來遠端解除安裝網路代理。在工作的**要解除安裝的應用程式**欄位，選取**卡巴斯基安全管理中心網路代理**。不要忘記輸入卸除安裝密碼。

- 將受管理應用程式升級至卡巴斯基安全管理中心雲端主控台所支援的版本。
- 確保您有最新版本的受管理應用程式的政策。如果您使用過時的政策，為卡巴斯基安全管理中心雲端主控台支援的應用程式版本建立新的政策。
- 若要使用實際政策，請將您計畫透過卡巴斯基安全管理中心雲端主控台管理的應用程式專用的 Web 外掛程式進行升級。
- 如果卡巴斯基應用程式不受卡巴斯基安全管理中心雲端主控台支援，從受管理裝置卸除安裝這些應用程式，然後將卸除安裝的應用程式替換為受支援的應用程式。
- 解密執行 Windows 作業系統的受管理裝置上被 Kaspersky Endpoint Security for Windows 加密的所有資料（磁碟層級或檔案層級），並透過應用程式政策或透過本機將受管理裝置上的加密功能停用。有關詳細資訊，請參閱 Kaspersky Endpoint Security for Windows 的說明。

  若 Windows 裝置仍存有透過 Kaspersky Endpoint Security for Windows 加密的任何檔案或資料夾，則網路代理升級將在移轉程序期間取消。系統將會傳送通知提示您解密裝置上的所有資料並停用該加密功能。

卡巴斯基安全管理中心雲端主控台最多允許每部管理伺服器管理 25,000 部裝置。

若要執行移轉到卡巴斯基安全管理中心雲端主控台：

1. 預估移轉程序的範圍，意即審核要匯出的管理群組及評估其中的受管理裝置數量。請確認所有列為移轉先決條件的活動都已成功完成。
2. 在卡巴斯基安全管理中心雲端主控台中，前往要移轉受管理裝置的從屬管理伺服器。
3. 在主功能表中，前往**操作 → 移轉**。

   移轉精靈的歡迎頁面即會開啟。
4. 在歡迎頁面上，點擊**下一步**。

   要匯出的受管理裝置頁面隨即開啟，並顯示從屬管理伺服器的整個管理群組階層。
5. 在**要匯出的受管理裝置**頁面上，點擊**受管理裝置**群組名稱旁邊的箭頭圖示 (>) 以展開管理群組階層。選取您要匯出的管理群組。

   移轉精靈會檢查所選管理群組中包含的受管理裝置數量。如果此數字超過 10,000，則會出現錯誤訊息。**下一步**按鈕會保持無法使用（變暗），直到所選管理群組中受管理裝置的數量在限制範圍內為止。
6. 選取其政策與工作必須一起與群組物件移轉至卡巴斯基安全管理中心雲端主控台的受管理應用程式。若要選取其物件要匯出的受管理應用程式，請選取清單中其名稱旁的核取方塊。

   儘管清單中顯示了卡巴斯基安全管理中心管理伺服器，但是選取相應的核取方塊不會導致匯出其政策。

   要確保卡巴斯基安全管理中心雲端主控台支援您的受管理應用程式，請點擊相應的連結。它將使您重新定向到包含卡巴斯基安全管理中心雲端主控台管理的應用程式清單的"線上說明"主題。

若所選的應用程式不受卡巴斯基安全管理中心雲端主控台支援，則這些應用程式的政策與工作仍會移轉，但礙於無專用的外掛程式可用，您將無法在卡巴斯基安全管理中心雲端主控台加以管理。

7. 依預設要匯出群組物件的清單。如有需要，您還可以指定要與選定管理群組一起匯出的非群組物件，例如全域工作、自訂裝置分類、報告、自訂角色、內部使用者和安全群組，以及帶有手動新增內容的自訂應用程式類別。此頁面包含以下區段：

- **全域工作**

  受管理應用程式的全域工作清單，以及網路代理的全域工作。

  若您所選的全域工作會套用至特定物件分類，系統也會匯出此分類。

  儘管清單中顯示了管理伺服器的全域工作，但是您無法將其匯出。選取這些工作不會影響匯出範圍。遠端安裝工作也保留在匯出範圍之外，因為無法匯出它們各自的安裝套件。

- **裝置分類**

  自訂裝置分類的清單。

- **報告**

  要匯出的可編輯清單報告實例。

  若您所選的報告會套用至特定物件分類，系統也會匯出此分類。

  卡巴斯基安全管理中心雲端主控台包含與卡巴斯基安全管理中心網頁主控台相同的報告範本集，因此您可以選取僅匯出手動建立或重新配置的報告。

- **群組物件**

依預設要匯出群組物件的清單。與所選管理群組相關的以下物件會依預設匯出其整體：

- 管理群組結構，即所選管理群組的所有子群組
- 包含在要匯出之管理群組的裝置
- 指派給裝置以匯出的標籤

  若標籤已在卡巴斯基安全管理中心網頁主控台但從未指派給任何裝置，則不會匯出該標籤。自動標記規則也不會匯出。

- 所選的受管理應用程式的群組政策

  管理伺服器政策與網路代理政策不會匯出。

- 所選的受管理應用程式的群組工作與網路代理群組工作

  管理伺服器工作不會匯出。

抵也可以預防特定類型的非群組物件遭到匯出：

- 若要取消匯出自訂角色 (意即僅由使用者建立的那些角色)，請選取**將自訂角色排除在匯出範圍外**核取方塊。
- 若要取消匯出內部使用者與安全群組，請選取**將內部使用者和安全群組排除在匯出範圍外**核取方塊。
- 若要取消匯出有手動新增內容的自訂應用程式類別，請選取**將自訂應用程式類別排除在匯出範圍外**核取方塊。

如果您將各種作業系統的裝置轉移到卡巴斯基安全管理中心雲端主控台，則非群組物件只需移轉一次。

8. 定義好移轉範圍後，請點擊**下一步**開始匯出程序。**建立匯出檔案**頁面即會開啟，供您檢視您在移轉範圍中所納入每類物件的匯出進度。請等待片刻，直到物件清單中所有物件旁的重新整理圖示 (🔄) 更換為綠色勾號標記 (✓)。匯出完成，匯出檔案會自動儲存到一個臨時資料夾。開啟下一頁，顯示卡巴斯基安全管理中心雲端主控台中的管理群組的整個階層結構，該主控台會以主管理伺服器運作。

9. 針對群組物件必須匯入至的管理群組，選取在旁邊的核取方塊，接著點擊**下一步**。將檔案解壓縮，並將非群組物件和群組物件還原到目標管理群組。

若您還原的物件名稱與現有物件名稱相同，前者會使用增量尾碼新增。

完成匯入時，管理群組的匯出結構，包含裝置的詳細資料，會顯示在所選目標管理群組下。非群組物件也會匯入。

您無法最小化移轉精靈並在匯入期間執行任何並行作業。請等待片刻，直到物件清單中所有物件旁的重新整理圖示 (🔄) 更換為綠色勾號標記 (✓)，匯入隨即完成。之後，裝置會開始切換到卡巴斯基安全管理中心雲端主控台。

10. 匯入完成後，移轉精靈會顯示卡巴斯基安全管理中心雲端主控台中適當作業系統專用之網路代理安裝套件的清單。請選取版本與本地化版本皆適當的網路代理安裝套件。

    僅當您先前已在卡巴斯基安全管理中心雲端主控台工作區完成快速啟動精靈，而且您是執行 Windows 裝置移轉時，才選取 Kaspersky Network Agent for Windows 安裝套件。

11. 點擊"**下一步**"。

    移轉精靈即會建立一個新的獨立安裝套件（或使用現有安裝套件）和一個以其為基礎建立的自訂安裝套件，以及相對應的遠端安裝工作。工作範圍包括您在**要匯出的受管理裝置**選取的管理群組。依預設，工作啟動排程會設定為**手動**。移轉精靈會顯示建立進度。

12. 請等待重新整理圖示 (🔄) 更換為綠色勾號標記 (✓)，接著點擊**下一步**。

13. 如有需要，請針對以內部部署執行之卡巴斯基安全管理中心網頁主控台內的所選管理群組與其所有子群組中的裝置，選取該裝置的**執行新建立的遠端安裝工作**核取方塊 (依預設會取消選取)。網路代理安裝完成後，您可以透過卡巴斯基安全管理中心雲端主控台管理選定的裝置。執行工作的管理群組會顯示完整路徑。

    遠端安裝工作必須在匯入卡巴斯基安全管理中心雲端主控台完成後啟動。否則該裝置會遭系統複製。

14. 點擊**完成**關閉移轉精靈並啟動遠端安裝工作以達成以下目的：

    - 升級網路代理實例
    - 透過卡巴斯基安全管理中心雲端主控台管理網路代理實例

    若您不選取**執行遠端安裝工作**核取方塊，您可之後手動啟動工作，如有必要。

您可以檢查現在是否可以透過卡巴斯基安全管理中心雲端主控台管理移轉的網路代理實例。為此，請轉至**資產（裝置）→受管理裝置**。確保移轉的受管理裝置在**可見**中，**網路代理已安裝**和**網路代理正在執行**列具有確認圖標 (✓)。此外，請確保這些裝置沒有"*長時間未連線*"狀態描述。

情境：移轉執行 Linux 或 macOS 作業系統的裝置

本節介紹如何將執行 Linux 或 macOS 作業系統的裝置從內部執行的卡巴斯基安全管理中心網頁主控台移轉到卡巴斯基安全管理中心雲端主控台。在沒有管理伺服器階層的情況下進行移轉和在有管理伺服器階層的情況下進行移轉的基本情境，可用以將所有裝置和相關物件都轉移到卡巴斯基安全管理中心雲端主控台。但是，如果您的網路不僅包含執行 Windows 的裝置，還包含執行 Linux 或 macOS 的裝置，則您需要分別針對每種類型的作業系統來轉移裝置。因此，您必須多次執行移轉。

先決條件

開始之前，請執行以下操作：

- 將內部部署運作的管理伺服器升級至版本 12 修補程式 A 或以上版本。
- 安裝卡巴斯基安全管理中心網頁主控台 12.1 或更新版本。

- 將受管理裝置上的網路代理升級到版本 12 或以上。
- 將受管理應用程式升級至卡巴斯基安全管理中心雲端主控台所支援的版本。
- 確保您有最新版本的受管理應用程式的政策。如果您使用過時的政策，為卡巴斯基安全管理中心雲端主控台支援的應用程式版本建立新的政策。
- 若要使用實際政策，請將您計畫透過卡巴斯基安全管理中心雲端主控台管理的應用程式專用的 Web 外掛程式進行升級。
- 如果卡巴斯基應用程式不受卡巴斯基安全管理中心雲端主控台支援，從受管理裝置卸除安裝這些應用程式，然後將卸除安裝的應用程式替換為受支援的應用程式。

卡巴斯基安全管理中心雲端主控台最多允許每部管理伺服器管理 25,000 部裝置。

移轉階段

移轉至卡巴斯基安全管理中心雲端主控台由下列階段組成：

1. **按作業系統對受管理裝置進行分組**

   如果您的網路包括執行不同作業系統（Windows、Linux 或 macOS）的裝置，請將每個作業系統的裝置放在卡巴斯基安全管理中心網頁主控台中單獨管理群組中。此外，為每個 Linux 發佈建立一個管理群組。例如，如果您有 Debian 和 Red Hat Linux 裝置，請將它們分配到不同的管理群組中。這將使您能夠成功執行移轉，因為不同的作業系統需要不同的網路代理安裝套件。

2. **分別對每個管理群組和其應用程式物件執行移轉**

   每種作業系統的受管理裝置必須分別移轉，以便納入其政策和工作。例如，如果您有 Windows、macOS、Ubuntu 和 CentOS 裝置，可先讓執行 Windows 作業系統的裝置轉移到卡巴斯基安全管理中心雲端主控台，接著是 macOS 裝置，再來是 Ubuntu 裝置，最後才是 CentOS 裝置。您可以按任意順序轉移受管理裝置。

   若要如此做，請視您的網路是否包含從屬管理伺服器，執行在沒有管理伺服器階層的情況下進行移轉或在有管理伺服器階層的情況下進行移轉。在移轉期間，請使用與所轉移裝置的作業系統相對應的網路代理安裝套件。例如，為 Linux 裝置選擇卡巴斯基安全管理中心13.2 網路代理以成功執行移轉。

   請注意，非群組物件（例如全域工作、自訂裝置分類或報告）只需移轉一次。

結果

完成移轉後，您可確認它是否成功：

- 在每個執行 Linux 或 macOS 作業系統的受管理裝置上重新安裝正確版本的網路代理。
- 所有 Linux 或 macOS 裝置都會透過卡巴斯基安全管理中心雲端主控台進行管理。
- 所有移轉前生效的物件設定都將保留。

情境：從卡巴斯基安全管理中心雲端主控台反向移轉至卡巴斯基安全管理中心

您可能會想將受管理裝置從卡巴斯基安全管理中心雲端主控台移轉到卡巴斯基安全管理中心管理伺服器。例如，如果您不想移轉到卡巴斯基安全管理中心雲端主控台了，就可以使用此程序。

先決條件

在開始之前，請確保滿足以下先決條件：

- 卡巴斯基安全管理中心雲端主控台可用而且已連接受管理裝置。
- 有卡巴斯基安全管理中心 14.2（或以上版本）管理伺服器可用，而且有版本 13 或以上版本的網路代理安裝套件。

反向移轉階段

反向移轉包括以下階段：

1. **在內部部署的卡巴斯基安全管理中心管理伺服器中建立網路代理獨立安裝套件**

   在內部部署運作的卡巴斯基安全管理中心管理伺服器中，建立網路代理獨立安裝套件。

   在建立期間，您可以選取**將未配置的裝置移動到此群組**選項，以指定網路代理在安裝後要移至的管理群組。如果您指定了管理群組，則會建立一項自動移動規則，將所有以此獨立安裝套件安裝的網路代理都移至目標管理群組。

   為了確保正確進行反向移轉，請確定所選的網路代理版本等於或高於卡巴斯基安全管理中心雲端主控台中使用的版本。

2. **在卡巴斯基安全管理中心雲端主控台中建立自訂安裝套件**

   在卡巴斯基安全管理中心雲端主控台中，以您從內部部署運作的卡巴斯基安全管理中心管理伺服器建立並儲存的獨立安裝套件為基礎，建立自訂安裝套件。

   若要啟用以靜默模式安裝套件，請在**可執行檔命令列**欄位中指定 `-s` 參數。

3. **建立遠端安裝工作**

   在卡巴斯基安全管理中心雲端主控台中，使用所建立的自訂安裝套件建立遠端安裝工作。

4. **執行遠端安裝工作**

   啟動所建立的遠端安裝工作。該工作會發動重新安裝所指定管理群組中的所有網路代理；它還會變更連線位址和修改其他連線設定，以便將網路代理切換到內部部署的卡巴斯基安全管理中心管理伺服器的管理之下。

   如果您在建立獨立安裝套件的期間並未指定任何目標管理群組，則所有裝置都會移至**未配置的裝置**群組。

結果

完成移轉後，您可確認它是否成功：

- 所有落在遠端安裝工作的涵蓋範圍內、先前透過卡巴斯基安全管理中心雲端主控台來管理的裝置，現在均已由內部部署的卡巴斯基安全管理中心管理伺服器來管理。
- 裝置已自動移至安裝套件設定中所指定的管理群組。

卡巴斯基安全管理中心雲端主控台中的遠端安裝工作會無法完成：它不再具有目標裝置，因為所有目標裝置的連線設定均已被修改。您在確認所有落在移轉範圍內的裝置在受管理裝置清單中的**可見**欄都出現錯誤圖示(!)後，必須手動停止該工作。

在有虛擬管理伺服器的情況下移轉

如果您現有內部部署的卡巴斯基安全管理中心基礎架構中有虛擬管理伺服器存在，您即無法使用移轉精靈從內部部署的卡巴斯基安全管理中心移轉至卡巴斯基安全管理中心雲端主控台。此外，您將僅能移轉您客戶的裝置。您將必須手動建立政策、工作和報告。

您可以執行以下其中一種移轉情境：

- 將您的用戶端裝置從虛擬管理伺服器移至主管理伺服器
- 手動執行從虛擬管理伺服器移轉出來

情境：在有虛擬管理伺服器的情況下，移動裝置來進行移轉

若要從內部部署運作的卡巴斯基安全管理中心網頁主控台移轉至卡巴斯基安全管理中心雲端主控台，您可以將裝置從虛擬管理伺服器移至主管理伺服器。

先決條件

在移轉之前，您必須先執行多項操作，包括將內部部署的管理伺服器升級到版本 12 或以上版本，以及將受管理應用程式升級到卡巴斯基安全管理中心雲端主控台支援的版本。

移轉情境

此情境分多個階段進行：

1. **為您每個虛擬管理伺服器各建立一個管理群組**

   您需在內部部署運作的卡巴斯基安全管理中心建立群組。

2. **移動您客戶的裝置**

   在內部部署運作的卡巴斯基安全管理中心，將您客戶的裝置從每個虛擬管理伺服器移至在上一個階段建立的相關管理群組。

3. **移轉**

   依針對不含管理伺服器階層的網路所述的方式執行移轉。

4. **將裝置移到虛擬管理伺服器的管理之下（可選步驟）**

   如果您想要透過虛擬管理伺服器管理您的客戶，請將裝置從管理群組移到虛擬管理伺服器的管理之下。

5. **建立政策、工作和報告**

   視需要建立政策、工作和報告。

結果

完成移轉後，您可確認它是否成功：

- 網路代理會重新安裝在所有受管理裝置上。
- 所有裝置都會透過卡巴斯基安全管理中心雲端主控台進行管理。
- 所有移轉前生效的物件設定都將保留。

情境：在有虛擬管理伺服器的情況下，手動進行移轉

您可以從內部部署運作的卡巴斯基安全管理中心網頁主控台移轉到卡巴斯基安全管理中心雲端主控台。

先決條件

在移轉之前，您必須先執行多項操作，包括將內部部署的管理伺服器升級到版本 12 或以上版本，以及將受管理應用程式升級到卡巴斯基安全管理中心雲端主控台支援的版本。

移轉情境

此情境分多個階段進行：

1. **為您每個虛擬管理伺服器各建立一個管理群組**

   在卡巴斯基安全管理中心雲端主控台中，為您每個虛擬管理伺服器各建立一個相對應的管理群組。

2. **建立網路代理的獨立安裝套件**

   建立網路代理的獨立安裝套件。在建立期間，請指定您在上一個階段建立的管理群組。這表示您必須為每個管理群組各建立一個獨立安裝套件。

   此階段是在您的卡巴斯基安全管理中心雲端主控台中進行。

3. **下載獨立安裝套件**

   下載您在上一個階段建立的獨立安裝套件。此階段是在您的卡巴斯基安全管理中心雲端主控台中進行。

4. **以每個獨立安裝套件各建立一個封存檔**

   可用的封存檔類型有：ZIP、CAB、TAR 或 TAR.GZ。

5. **建立網路代理的自訂安裝套件**

   建立網路代理的自訂安裝套件。在建立期間，請使用您在上一個階段建立的檔案。

   此階段是在您內部部署運作的卡巴斯基安全管理中心進行。

6. **建立遠端安裝工作**

   建立遠端安裝工作以使用所建立的自訂安裝套件安裝網路代理。

   建立工作時，請指定相對應的管理群組。

   此階段是在您內部部署的卡巴斯基安全管理中心進行。

7. **執行所建立的遠端安裝工作**

   網路代理會更新。卡巴斯基安全管理中心雲端主控台管理伺服器會接手管理它們。

   所有裝置都會移轉到卡巴斯基安全管理中心雲端主控台，並加到您建立網路代理的獨立安裝套件時所指定的管理群組中。

8. **將裝置移到虛擬管理伺服器的管理之下（可選步驟）**

   如果您想要透過虛擬管理伺服器管理您的客戶，請將裝置從管理群組移到虛擬管理伺服器的管理之下。

9. **建立政策、工作和報告**

   視需要建立政策、工作和報告。

結果

完成移轉後，您可確認它是否成功：

- 網路代理會重新安裝在所有受管理裝置上。
- 所有裝置都會透過卡巴斯基安全管理中心雲端主控台進行管理。

  所有移轉前生效的物件設定都將保留。

情境：將裝置從管理群組移到虛擬伺服器的管理之下

您可能會想透過虛擬管理伺服器來管理您的客戶。如果您已將裝置和其他項目從內部部署的卡巴斯基安全管理中心移轉到卡巴斯基安全管理中心雲端主控台，則這些裝置會位於管理群組中。若要透過虛擬管理伺服器來管理客戶的裝置，您必須將裝置從管理群組移到虛擬管理伺服器的管理之下。

先決條件

您已為每個客戶各建立一個虛擬管理伺服器。

每個客戶的所有裝置都位於該客戶專屬的一個管理群組中。

階段

此情境分幾個階段進行：

1. **建立網路代理的獨立安裝套件**

   切換到每個建立的虛擬管理伺服器，然後建立網路代理的獨立安裝套件。若要切換管理伺服器，您可以在主功能表中點擊目前管理伺服器名稱右側的箭頭圖示 (>) 到，然後選取所需的管理伺服器。

2. **下載獨立安裝套件**

   下載您在上一個階段建立的獨立安裝套件。

3. **以每個獨立安裝套件各建立一個封存檔**

   可用的封存檔類型有：ZIP、CAB、TAR 或 TAR.GZ。

4. **建立網路代理的自訂安裝套件**

   建立網路代理的自訂安裝套件。在建立期間，請使用您在上一個階段建立的檔案。

   此階段是主管理伺服器上進行。

5. **建立遠端安裝工作**

   建立遠端安裝工作以使用所建立的自訂安裝套件安裝網路代理。

   建立工作時，請指定相對應的管理群組。

   此階段是主管理伺服器上進行。

6. **執行所建立的遠端安裝工作**

   網路代理即會更新。裝置會移到虛擬管理伺服器的管理之下。

7. **建立政策、工作和報告**

   視需要建立政策、工作和報告。

結果

您現在可以使用虛擬管理伺服器來管理移轉後的客戶裝置。

快速啟動精靈

本節提供卡巴斯基安全管理中心雲端主控台快速啟動精靈的相關資訊。

關於快速啟動精靈

卡巴斯基安全管理中心雲端主控台中的快速啟動精靈讓您只需建立少少的必要工作和政策並調整少少的設定，就能開始建立 Kaspersky 應用程式的安裝套件。使用精靈時，您可以對卡巴斯基安全管理中心雲端主控台進行以下變更：

- 發動下載受管理 Kaspersky 應用程式的安裝套件。
- 為執行 Windows、Linux 或 macOS 的裝置建立網路代理獨立安裝套件。
- 建立卡巴斯基安全管理中心網路代理政策。
- 建立*將更新下載至發佈點儲存區*工作。
- 為受管理 Kaspersky 應用程式設定政策和工作。
- 設定與卡巴斯基安全網路 (KSN) 的互動。

快速啟動精靈完成後，網路代理與受管理 Kaspersky 應用程式的安裝套件即會出現在**發現和佈署** → **佈署和分配** → **安裝套件**清單中。

快速啟動精靈會建立受管理應用程式（例如 Kaspersky Endpoint Security for Windows）適用的政策（但若已為「受管理裝置」群組建立該等政策，則不適用）。快速啟動精靈會建立工作（但若「受管理裝置」群組有同名的工作存在，則不適用）。

在您建立公司工作區並首次啟動卡巴斯基安全管理中心雲端主控台後，卡巴斯基安全管理中心雲端主控台會自動提示您執行快速啟動精靈。您還可以在任意時刻手動啟動快速啟動精靈。

啟動快速啟動精靈

在您建立公司工作區並首次啟動卡巴斯基安全管理中心雲端主控台後，卡巴斯基安全管理中心雲端主控台會自動提示您執行快速啟動精靈。您還可以在任意時刻手動啟動快速啟動精靈。

若您再次啟動快速啟動精靈，則先前執行精靈時建立過的工作和政策不會再建立一次。

要手動啟動快速啟動精靈：

1. 在主功能表中，按一下管理伺服器名稱旁邊的設定圖示（ ）。

   管理伺服器內容視窗將開啟。

2. 在**一般**頁籤，選取**一般**區段。

3. 點擊 **開始快速啟動精靈**。

或者，您也可以選取**發現和佈署** → **佈署和分配** → **快速啟動精靈**來啟動快速啟動精靈。

精靈會提示您執行卡巴斯基安全管理中心雲端主控台的初始化設定。遵照精靈的說明。使用**下一步**按鈕進行精靈。使用**上一步**按鈕返回精靈的上一步。

步驟 1：選取要下載的安裝套件

在清單中，選取要在用戶端裝置上安裝的 Kaspersky 應用程式。卡巴斯基安全管理中心雲端主控台會建立所選應用程式的安裝套件。您之後將會使用所建立的安裝套件安裝應用程式。

選取安裝套件來下載時，請注意語言：安裝套件會有多種語言版本可選。

請選取以下應用程式：

- 卡巴斯基安全管理中心網路代理

  選取網路代理安裝套件時，請注意以下幾點：

  - 每個用戶端裝置上都必須安裝網路代理。因此，請為用戶端裝置上執行的每種作業系統各選取適當的網路代理。

  - 您必須使用獨立安裝套件，手動將網路代理安裝到您選來擔任發佈點的裝置上。發佈點為執行網路輪詢以及遠端在用戶端裝置上安裝 Kaspersky 安全應用程式時所不可或缺。因此，您必須至少選取一個網路代理安裝套件。隨著您繼續執行精靈的後續步驟，卡巴斯基安全管理中心雲端主控台會建立網路代理獨立安裝套件。

    與基於 Windows 的發佈點相比，基於 Linux 和 macOS 的發佈點功能有限。強烈建議您選擇基於 Windows 的電腦擔任發佈點。

    您可以選取 Windows、Linux 和 macOS 專用的網路代理。如果您僅選取某種作業系統（例如 macOS）專用的網路代理，則會建立所選作業系統專用的獨立安裝套件。如果您同時選取多種作業系統專用的網路代理，則卡巴斯基安全管理中心雲端主控台會依以下優先順序，僅建立一個獨立安裝套件：Windows 最優先，Linux 次之，最後是 macOS。例如，如果您同時選取 Network Agents for Linux 和 for macOS，則卡巴斯基安全管理中心雲端主控台會建立 Network Agent for Linux 的獨立安裝套件。您可以隨時針對任何這些作業系統，手動建立網路代理獨立安裝套件。

- Kaspersky 安全應用程式

  請為您組織中的用戶端裝置上安裝的作業系統，選取適當的安裝套件。

步驟 2：設定代理伺服器

如果您的組織會使用代理伺服器連線到網際網路，請在精靈的此步驟指定代理伺服器設定。這些設定會新增至網路代理安裝套件中。安裝後，網路代理會自動在每個用戶端裝置上使用這些設定。

為代理伺服器連線指定以下設定：

- **使用代理伺服器**
- **位址**
- **連接埠號**
- **代理伺服器身分驗證**

如果啟用此選項，則您可以在輸入欄位中指定進行代理伺服器身分驗證時所用的憑證。
我們建議您指定僅具有代理伺服器身分驗證所需的最低權限的帳戶的憑據。
預設情況下已停用該選項。

- **使用者名稱**

  建立連線代理伺服器的帳戶的使用者名稱。
  我們建議您指定僅具有代理伺服器身分驗證所需的最低權限的帳戶的憑據。

- **密碼**

  建立連線代理伺服器的帳戶的密碼。
  我們建議您指定僅具有代理伺服器身分驗證所需的最低權限的帳戶的憑據。

步驟 3。設定卡巴斯基安全網路

如果您在精靈的第一個步驟下載了 Kaspersky Endpoint Security for Windows 安裝套件，則會顯示以下應用程式的 KSN 聲明文字：

- Kaspersky Endpoint Security for Windows
- 安裝在本機裝置上的卡巴斯基安全管理中心
- 安裝在雲端環境中的卡巴斯基安全管理中心雲端主控台

如果您並未下載 Kaspersky Endpoint Security for Windows 安裝套件，則不會顯示該應用程式的 KSN 聲明。

在試用模式下，僅會顯示 Kaspersky Endpoint Security for Windows 的 KSN 聲明。

請仔細閱讀卡巴斯基安全網路聲明。您可以選取以下其中一個方法：

- **我同意使用卡巴斯基安全網路**

  卡巴斯基安全管理中心雲端主控台以及用戶端裝置上安裝的受管理應用程式會自動將其操作詳細資訊傳輸至卡巴斯基安全網路。參與卡巴斯基安全網路確保了包含病毒和其他威脅的資料庫的快速更新，該資料庫確保了對緊急安全威脅的快速回應。

- **我不同意使用卡巴斯基安全網路**

  卡巴斯基安全管理中心雲端主控台和受管理應用程式不會提供資訊給卡巴斯基安全網路。
  若您選取此選項，則會停用卡巴斯基安全網路。

KSN 預設為停用狀態。您之後如果對於是否使用 KSN 改變心意，可以在管理伺服器內容視窗的 **KSN 設定**區段中啟用（或停用）相對應的選項。

步驟 4：設定管理第三方更新的方式

如果*弱點掃描和所需更新*工作已存在，則不會顯示此步驟。

如果您想要取得受管理裝置上所安裝應用程式的更新清單以及所發現弱點與建議修復項目的清單，請啟用**搜尋第三方軟體更新和修復弱點程式**選項。如果啟用此選項，卡巴斯基安全管理中心雲端主控台會建立*弱點掃描和所需更新*工作。

步驟 5。建立基本的網路防護設定

在精靈的此步驟，請點擊**建立**按鈕，建立所需的物件來對您的用戶端裝置加上初始防護。

卡巴斯基安全管理中心雲端主控台會執行兩項操作：

- 以預設設定建立基本的政策和工作

  會建立的政策如下：

  - 卡巴斯基安全管理中心網路代理政策
  - 受管理的 Kaspersky 應用程式政策

  會建立的工作如下：

  - *將更新下載至發佈點儲存區*工作
  - *弱點掃描和所需更新*工作

    僅當您在精靈的上一個步驟啟用了**搜尋第三方軟體更新和修復弱點程式**選項時，才會建立此工作。
  - 受管理 Kaspersky 應用程式適用的工作
- 建立網路代理的獨立安裝套件

  您會使用此套件在發佈點上安裝網路代理。卡巴斯基安全管理中心雲端主控台會以您在精靈的上一個步驟選取的網路代理安裝套件為基礎，建立獨立安裝套件。在套件建立期間，您必須閱讀並接受網路代理 EULA 的條款。建立獨立安裝套件後，系統會提示您將其下載到您目前使用的裝置上。

  建立網路代理獨立安裝套件可能會需要一些時間。您可以繼續進入精靈的下一個步驟。該程序將以背景模式繼續執行。您可以在**安裝套件**區段（**發現和佈署 → 佈署和分配 → 安裝套件**）的**進行中 ()**頁籤追蹤該程序。

  基於驗證身分的原因，每個獨立安裝套件都會經憑證簽署。此憑證會不時重新簽發。每次重新簽發憑證的程序一結束，卡巴斯基安全管理中心雲端主控台便會自動對所有已建立的獨立安裝套件更新簽章。此自動更新簽章的動作無法對下載的獨立安裝套件執行。因此，其憑證會到期，屆時當您以獨立安裝套件安裝應用程式時，可能會出現憑證錯誤。在此情況下，請重新下載獨立安裝套件。

步驟 6：關閉快速啟動精靈

請在快速啟動精靈的完成頁面上，閱讀您還必須執行哪些操作，將 Kaspersky 安全應用程式部署到用戶端裝置上。請依照 Kaspersky 應用程式初始化部署的情境中提供的各階段進行操作。

Kaspersky 應用程式初始化部署

本節說明如何在您組織中的用戶端裝置上初始化部署 Kaspersky 應用程式。

情境：Kaspersky 應用程式初始化部署

此情境說明如何在卡巴斯基安全管理中心雲端主控台中，將 Kaspersky 應用程式安裝到用戶端裝置上。首先，您必須在您的網路中部署發佈點。然後，您必須透過發佈點，執行網路輪詢並發現您網路中的網路裝置。其後，您便可以將 Kaspersky 應用程式部署到網路裝置上。

完成此情境時，Kaspersky 應用程式會已部署到您組織網路中所選的用戶端裝置上。您可以管理所有安裝了 Kaspersky 應用程式的裝置。

先決條件

在開始之前，請確保滿足以下先決條件：

- 快速啟動精靈已完成。
- 已建立網路代理與安全應用程式的安裝套件。
- 在受管理裝置的防火牆中，已將網址 https://aes.s.kaspersky-labs.com/endpoints/ 加為例外。
- 您知道您組織中用戶端裝置的網際網路設定資訊、閘道的資訊，以及代理伺服器設定。

階段

Kaspersky 應用程式的初始化部署是分多個階段進行：

1. **選擇一台要擔任發佈點的裝置**

   在卡巴斯基安全管理中心雲端主控台中，發佈點的功用為：

   - 輪詢網路以及發現裝置
   - 遠端將網路代理安裝到用戶端裝置上
   - 使用戶端裝置能夠連線到管理伺服器（當發佈點是擔任連線閘道時）

   請選擇您組織網路中的某個裝置擔任管理群組的發佈點。所選裝置必須符合對發佈點的要求。請視您組織網路中的用戶端裝置數量，選擇正確數量的裝置擔任發佈點。

2. **建立網路代理的獨立安裝套件**

   建立網路代理的獨立安裝套件，以供安裝到發佈點上。

   如果您的用戶端裝置無法直接透過網際網路連線到管理伺服器，請在網路代理安裝套件設定中設定連線閘道和代理伺服器設定。

3. **在所選擔任發佈點的裝置上安裝網路代理**

   透過任何方式，將網路代理的獨立安裝套件傳送到所選裝置。例如，您可以將獨立安裝套件複製到卸除式磁碟機（例如隨身碟）或是加到共用資料夾中。

在獨立安裝套件檔案的**內容**視窗中，確認網路代理的獨立安裝套件經過 Kaspersky 簽署。

在所選裝置上執行網路代理獨立安裝套件來進行安裝。網路代理現在即已根據網路代理安裝套件的設定安裝完成，並已連線到管理伺服器。裝有網路代理的裝置會被加到建立網路代理的獨立安裝套件時所指定的管理群組中。

如果在執行 Microsoft Windows XP Professional for Embedded Systems 32 位元的裝置上使用獨立安裝套件來安裝網路代理，安裝將會失敗。若要解決此問題，請從 Microsoft 網站預先安裝 Windows XP 適用的 KB2868626 更新：https://www.catalog.update.microsoft.com/Search.aspx?q=KB2868626。

4. **將安裝了網路代理的裝置分配為發佈點**

   將安裝了網路代理的裝置分配為發佈點。

5. **為發佈點設定並執行網路輪詢**

   為安裝了網路代理的發佈點設定網路輪詢。您可以選擇在網路代理政策中設定網路輪詢。

   待網路輪詢依排程完成後，連線到您組織網路的用戶端裝置即會獲發現並加到**未配置的裝置**群組中。

6. **建立網路代理與受管理 Kaspersky 應用程式的安裝套件**

   如果您並未啟動快速啟動精靈，或是略過了建立安裝套件的步驟，請建立 Kaspersky 應用程式的安裝套件。您必須就您組織網路中的用戶端裝置上安裝的作業系統，建立適當的網路代理與受管理 Kaspersky 應用程式安裝套件。

7. **移除協力廠商安全應用程式**

   如果您組織網路中的用戶端裝置上安裝了協力廠商安全應用程式，請加以移除後，再安裝 Kaspersky 應用程式。

8. **在用戶端裝置上安裝 Kaspersky 應用程式**

   建立一些工作來將網路代理和受管理 Kaspersky 應用程式安裝到您組織網路中的用戶端裝置上。建立工作時，請使用**遠端安裝應用程式**工作類型。對於用於安裝網路代理的工作，請使用**透過發佈點使用作業系統資源**選項。對於用於安裝受管理 Kaspersky 應用程式的工作，請使用**使用網路代理**選項。建立好工作後，您可以對工作進行設定。請確保各項工作的排程符合您的需求。安裝網路代理的工作必須先執行。將網路代理安裝到用戶端裝置後，接著就必須執行用於安裝受管理 Kaspersky 應用程式的工作。

   您可以選擇建立一個遠端安裝工作，以將網路代理和受管理 Kaspersky 應用程式安裝到您組織網路中的用戶端裝置上。在此情況下，請在**安裝套件區塊**中使用**選取安裝套件**選項和**選取網路代理**選項，並在**強制下載安裝套件**區塊中使用**透過發佈點使用作業系統資源**選項。

   您也可以建立多個遠端安裝工作，針對不同的管理群組或不同的裝置分類安裝受管理 Kaspersky 應用程式。

   如果您有用戶端裝置不在設有發佈點的網路內（例如，遠端使用者的筆記型電腦），您必須建立網路代理獨立安裝套件，然後透過任何方法將這些獨立安裝套件傳送到這些用戶端裝置。將網路代理獨立安裝套件安裝到這些用戶端裝置的本機上。然後，您便可以依照與發佈點發現的其他裝置適用的相同指示，將受管理 Kaspersky 應用程式安裝到這些遠端使用者的裝置上。

   執行遠端安裝工作。

   要安裝 Kaspersky 應用程式時，您可以選擇啟動防護佈署精靈。

9. **安裝 Kaspersky Security for Mobile**

   如果您計劃管理公司行動裝置，請按照 Kaspersky Security for Mobile 說明 中提供的指示瞭解有關 Kaspersky Endpoint Security for Android 部署的資訊。

10. **確認 Kaspersky 應用程式的初始化部署成功**

    產生並檢視 **Kaspersky 軟體版本報告**。確認您組織中的所有用戶端裝置上皆已安裝受管理 Kaspersky 應用程式。

對於完整磁碟加密，卡巴斯基安全管理中心雲端主控台僅支援 BitLocker。

為 Kaspersky 應用程式建立安裝套件

若要將 Kaspersky 應用程式部署到您組織中的網路裝置上，您必須在卡巴斯基安全管理中心雲端主控台中建立 Kaspersky 應用程式的安裝套件。

若要建立 Kaspersky 應用程式安裝套件：

1. 執行以下操作之一：

   - 在主功能表中，轉至 **發現和佈署 → 佈署和分配 → 安裝套件**。
   - 在主功能表中，轉至 **操作 → 儲存區 → 安裝套件**。

   您也可以在螢幕通知清單中檢視關於新套件的通知。如果有關於新安裝套件的通知，您可以按一下通知旁邊的連結並轉到可用安裝套件清單。

   系統會顯示可在管理伺服器使用的安裝套件清單。

2. 點擊**新增**。

   新套件精靈啟動。使用**下一步**按鈕進行精靈。

3. 在精靈的第一個頁面中，選取**為 Kaspersky 應用程式建立安裝套件**。

   Kaspersky 網頁伺服器上可用之分發套件的清單即會顯示。

4. 點擊分發套件的名稱，例如 **Kaspersky Endpoint Security for Windows (<版本編號>)**。

   內含分發套件資訊的視窗即會開啟。

5. 請閱讀資訊並點擊**下載並建立安裝套件**按鈕。

   若分發套件無法自動轉換為安裝套件，則顯示的按鈕會是**下載分發套件**而非**下載並建立安裝套件**。在此情況下，請下載分發套件，然後使用下載的檔案建立自訂安裝套件。

   下載安裝套件的作業即會開始。您可以關閉精靈視窗或繼續執行指示的下一步。如果關閉精靈視窗，下載程序將在後台模式下繼續。

   如果要追蹤安裝套件的下載程序，請執行以下操作：

   a. 在主功能表中，轉至 **操作 → 儲存區 → 安裝套件 → 進行中 ()**。

   b. 追蹤操作進度**下載進度**欄和**下載狀態**表的欄。

   該程序完成後，請安裝套件將新增到**已下載**頁籤的清單。如果下載程序停止並且下載狀態切換為**接受 EULA**，然後點擊安裝套件名稱，然後繼續進行指示的下一步。

   如果您計畫從卡巴斯基安全管理中心網頁主控台移轉到卡巴斯基安全管理中心雲端主控台，而您組織卻設有必須透過代理來存取企業網路的安全規定，則這可能會影響移轉程序。您在建立網路代理安裝套件後，必須指定代理設定，以便確保受管理裝置上的網路代理實例與您卡巴斯基安全管理中心雲端主控台工作區之間能夠連線：

   a. 定義安裝套件名稱。

   b. 在開啟的安裝套件內容視窗中，前往**設定**頁籤。

c. 開啟**連線**區段。

d. 選取**使用代理伺服器**選項，然後填寫**代理伺服器位址**和**代理伺服器連接埠**欄位。

6. 對於一些 Kaspersky 應用程式，下載過程中，**顯示 EULA**按鈕被顯示。如果它不顯示，做以下操作：

a. 點擊**顯示 EULA**按鈕以閱讀最終使用者產品授權協議 (EULA)。

b. 閱讀螢幕上顯示的 EULA，然後點擊**同意**按鈕。

您接受 EULA 後，下載便會繼續。若您點擊**拒絕**，下載便會暫停。

7. 當下載完成時，請點擊**關閉**按鈕 (✕) 關閉內含分發套件資訊的視窗。

安裝套件即已建立。該安裝套件會出現在安裝套件清單中。

分發安裝套件至從屬管理伺服器

若要分發安裝套件至從屬管理伺服器：

1. 與控制相關從屬管理伺服器的管理伺服器建立連線。

2. 使用以下其中一種方式，建立向從屬管理伺服器發佈安裝套件的工作：

- 如果您要管理群組中的從屬管理伺服器建立發佈套件工作，您可以在群組工作中建立此工作。
- 如果您要為指定的從屬管理伺服器建立發佈套件的工作，您可以在指定裝置工作中建立該工作。

新工作精靈啟動。遵照精靈的說明。

在新工作精靈的**新工作**視窗中，於**工作類型**欄位選取**發佈安裝套件**。您也可以在**工作名稱**欄位中編輯工作的預設名稱。

在下一個步驟，指定從屬管理伺服器作為工作範圍，然後依照新工作精靈的指示進行操作。當您完成時，新工作精靈即會建立用於將所選安裝套件分發到特定從屬管理伺服器的工作。

當您為內部部署運作的從屬管理伺服器建立「發佈安裝套件」工作時，無論選取的分發選項為何（**所有安裝套件**或**選取的安裝套件**），分發範圍都僅包括自訂安裝套件，以及內部部署運作的卡巴斯基安全管理中心網頁主控台所支援 Kaspersky 應用程式的安裝套件。

3. 您可以手動執行此工作，或等候工作設定中指定的排程將其啟動。

所選安裝套件將會複製到指定的從屬管理伺服器上。

建立網路代理的獨立安裝套件

您和您組織中的裝置使用者可使用獨立安裝套件，在裝置的本機上安裝網路代理程式。獨立安裝套件可以針對執行 Windows、Linux 或 macOS 的裝置來建立。

在卡巴斯基安全管理中心雲端主控台中，您只能建立網路代理的獨立安裝套件。

獨立安裝套件是一種可執行檔案，可透過電子郵件傳送或以其他方法傳輸至用戶端裝置上。讓收到的檔案在用戶端裝置本機上執行，即可安裝網路代理，而無需借助卡巴斯基安全管理中心雲端主控台。

Network Agent for Linux 與 Network Agent for macOS 的獨立安裝套件是副檔名為 .sh 的指令碼檔案。當您執行該檔案時，指令碼會將內含安裝套件和其設定的附加封存檔解壓縮，然後啟動安裝。

如果在執行 Microsoft Windows XP Professional for Embedded Systems 32 位元的裝置上使用獨立安裝套件來安裝網路代理，安裝將會失敗。若要解決此問題，請從 Microsoft 網站預先安裝 Windows XP 適用的 KB2868626 更新：https://www.catalog.update.microsoft.com/Search.aspx?q=KB2868626。

基於驗證身分的原因，每個獨立安裝套件都會經憑證簽署。此憑證會不時重新簽發。每次重新簽發憑證的程序一結束，卡巴斯基安全管理中心雲端主控台便會自動對所有已建立的獨立安裝套件更新簽章。此自動更新簽章的動作無法對下載的獨立安裝套件執行。因此，其憑證會到期，屆時當您以獨立安裝套件安裝應用程式時，可能會出現憑證錯誤。在此情況下，請重新下載獨立安裝套件。

若要建立獨立安裝套件：

1. 執行以下操作之一：

   - 在主功能表中，轉至 **發現和佈署 → 佈署和分配 → 安裝套件**。
   - 在主功能表中，轉至 **操作 → 儲存區 → 安裝套件**。

   系統會顯示可用安裝套件的清單。如果網路代理安裝套件不在清單中，請手動建立該安裝套件。

2. 在安裝套件的清單中，點擊網路代理安裝套件的名稱。

   網路代理安裝套件的內容視窗即會顯示。

3. 如有必要，請修改網路代理安裝套件的設定，然後關閉網路代理安裝套件的內容視窗。

4. 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。

5. 選擇**使用獨立安裝套件**選項。

   獨立安裝套件建立精靈啟動。使用**下一步**按鈕進行精靈。

6. 在精靈的第一頁，若您要隨所選的應用程式安裝網路代理，請確認**網路代理與該應用程式一同安裝**選項已啟用。

   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。

7. 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。

8. 在精靈的下一頁，若您要在精靈完成後顯示獨立安裝套件的清單，請選取**開啟獨立安裝套件清單**選項。

9. 點擊**完成**按鈕。

   獨立安裝套件建立精靈即會關閉。

網路代理獨立安裝套件即已建立。建立的獨立安裝套件會顯示在獨立安裝套件清單中供您檢視。

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：

1. 執行以下操作之一：

   - 在主功能表中，轉至 **發現和佈署 → 佈署和分配 → 安裝套件**。
   - 在主功能表中，轉至 **操作 → 儲存區 → 安裝套件**。

   可用安裝套件的清單即會顯示。

2. 在上述清單中，點擊**檢視獨立安裝套件清單**按鈕。

獨立安裝套件的清單即會顯示。

在獨立安裝套件清單中，其屬性顯示如下：

- **檔案名稱**。自動形成為包含在套件與應用程式版本中之應用程式名稱的獨立安裝套件名稱。
- **網路代理的安裝檔案名稱**。
- **網路代理版本**。
- **大小**。以 MB 為單位的檔案大小。
- **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。
- **已建立**。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。
- **檔案雜湊值**。此屬性用於確認獨立安裝套件未遭第三方人士竄改，使用者手中的檔案就是您所建立並向其傳輸的同一個檔案。

若要檢視特定安裝套件的獨立安裝套件清單：

選取清單中的安裝套件，並在清單上點擊**檢視獨立安裝套件清單**按鈕。

在獨立安裝套件清單中，您可執行以下操作：

- 點擊**下載**按鈕，下載獨立安裝套件至您的裝置。

  基於驗證身分的原因，每個獨立安裝套件都會經憑證簽署。此憑證會不時重新簽發。每次重新簽發憑證的程序一結束，卡巴斯基安全管理中心雲端主控台便會自動對所有已建立的獨立安裝套件更新簽章。此自動更新簽章的動作無法對下載的獨立安裝套件執行。因此，其憑證會到期，屆時當您以獨立安裝套件安裝應用程式時，可能會出現憑證錯誤。在此情況下，請重新下載獨立安裝套件。

- 點擊**移除**按鈕，移除獨立安裝套件。

建立自訂安裝套件

您可以使用自訂安裝套件完成以下動作：

- 將任何應用程式（例如文字編輯器）安裝到卡巴斯基安全管理中心雲端主控台涉及的用戶端裝置上（例如透過工作的方式）。
- 建立獨立安裝套件。

自訂安裝套件是一個含有一組檔案（包括可執行檔）的資料夾。自訂安裝套件的一種建立來源是封存檔案。封存檔案內含需加到自訂安裝套件中的一或多個檔案。您在建立自訂安裝套件時，可以指定命令列選項（例如以靜默模式安裝應用程式的選項）。

若要建立應用程式安裝套件：

1. 執行以下操作之一：
   - 在主功能表中，轉至 **發現和佈署 → 佈署和分配 → 安裝套件**。
   - 在主功能表中，轉至 **操作 → 儲存區 → 安裝套件**。

   系統會顯示可在管理伺服器使用的安裝套件清單。
2. 點擊**新增**。

   新套件精靈啟動。使用**下一步**按鈕進行精靈。
3. 在精靈的第一個頁面中，選取**從檔案建立安裝套件**。
4. 在精靈的下一個頁面，指定安裝套件名稱，然後點擊**瀏覽**按鈕。

   標準的**開啟**視窗即會開啟，供您選擇用於建立安裝套件的封存檔案。
5. 選取位於可用磁碟的封存檔案。

   您可以上傳 ZIP、CAB、TAR 或 TAR.GZ 封存。您無法從 SFX（自行解壓封存）檔案來建立安裝套件。

   檔案即會下載至卡巴斯基安全管理中心雲端主控台管理伺服器。

   如果管理伺服器偵測到封存檔包含 Kaspersky 應用程式，則會顯示錯誤訊息。您可以從 Kaspersky 網頁伺服器下載 Kaspersky 應用程式的安裝套件。選取**操作 → Kaspersky 應用程式 → 最新應用程式版本**即可進行此操作。
6. 在精靈的下一頁，如果所選封存檔案包含多個可執行檔，請選取其中那個需執行才能使用所建立的安裝套件來安裝應用程式的可執行檔。

7. 如有需要，請指定可執行檔的命令列參數。

   您可以指定命令行參數，讓安裝套件以靜默模式安裝應用程式。如需命令列參數的詳細資訊，請參閱應用程式供應商的說明文件。

   建立安裝套件的作業即會開始。

   精靈會通知您程序已完成。

   若安裝套件未能建立，則會顯示錯誤訊息。

   在卡巴斯基安全管理中心雲端主控台中，管理伺服器上所有安裝套件的總大小限制為 500 MB。如果在建立安裝套件的過程中超出了該總大小限制，請刪除先前建立的安裝套件。安裝套件的大小會顯示在安裝套件的內容中。

8. 點擊**完成**按鈕以關閉精靈。

建立的自訂安裝套件即會下載到管理伺服器。下載後，安裝套件出現在安裝套件清單。

在安裝套件的清單中，您可以檢視自訂安裝套件的以下屬性：

- **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)**。自訂安裝套件的大小。
- **作業系統**。建立的自訂安裝套件適用的作業系統。
- **已建立**。安裝套件建立日期。
- **已修改**。安裝套件修改日期。
- **類型**。Kaspersky 應用程式或協力廠商應用程式。

在安裝套件的清單中，點擊顯示了自訂安裝套件名稱的連結，即可變更命令列參數和自訂安裝套件名稱。

發佈點需求

若要處理多達 10,000 部用戶端裝置，發佈點必須至少滿足以下需求（已提供測試機器配置）：

- CPU：Intel® Core™ i7-7700 CPU, 3.60 GHz 4 核心。
- RAM：8 GB。
- 可用儲存空間：120 GB。

此外，發佈點必須具有網際網路存取權限且必須永遠保持連線。

如果管理伺服器上有任何遠端安裝工作等待，帶有發佈點的裝置也會請求一定的剩餘磁碟空間，這些空間與要安裝的安裝套件大小相當。

如果管理伺服器上有一個或多個更新（修補程式）安裝和弱點修復工作實例，帶有發佈點的裝置也會請求一定的剩餘磁碟空間，這些空間相當於兩倍的修補程式總大小。

網路代理政策設定

若設定網路代理政策：

1. 在主功能表中，轉至 **資產（裝置）→ 政策和設定檔**。
2. 按一下網路代理政策的名稱。
   網路代理政策的內容視窗開啟。

考慮到基於 Windows、macOS 和 Linux 的裝置，有各種設定可使用。

一般頁籤

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：
  - **作用中**
  - **非作用中**

    如果選取該選項，政策將變為不啟用狀態，但它仍然儲存在**政策**資料夾中。如果需要，您可以啟動該政策。
- 在**設定繼承**設定群組中，您可以配置政策繼承：
  - **從父政策繼承設定**

    如果啟用此選項，則政策設定值將繼承上一級群組政策，因而會受到鎖定。

    預設情況下已啟用該選項。
  - **在子政策中強制繼承設定**

    如果啟用此選項，則在套用政策變更之後，程式將執行以下操作：
    - 政策設定的值將被傳送到管理子群組的政策，也就是子政策。
    - 在每個子政策內容視窗的**一般**區域的**設定繼承**區塊，系統將自動選取**從父政策繼承設定**核取方塊。

    如果啟用此方塊，則會鎖定子政策設定。

    預設情況下已停用該選項。

事件配置頁籤

給頁簽可讓您配置事件記錄和事件通知。事件根據重要性級別分佈在以下部分中的 **事件配置** 頁簽上：

- **功能失效**
- **警告**
- **資訊**

在每個區域，事件類型清單顯示事件類型和在管理伺服器上的預設事件儲存期限（天）。點擊**內容**按鈕，您可以指定清單中已選中的事件記錄和通知設定。預設下，為整個管理伺服器指定的通用通知設定被用於所有事件類型。然後，您可以變更所需事件類型的特別設定。

應用程式設定頁籤

設定

在**設定**區域，您可以配置網路代理政策：

- **僅透過發佈點分發檔案**

  如果啟用此選項，則用戶端裝置僅會透過發佈點收到更新，而不是直接從更新伺服器收到更新。

  如果停用此選項，則用戶端裝置可以從不同的來源收到更新，即可以直接從更新伺服器收到更新，亦可從本機或網路資料夾收到更新。

  預設情況下已停用該選項。

- **事件佇列最大值 (MB)**
- **應用程式被允許在裝置上獲取政策延伸資料**

  安裝在受管理裝置的網路代理會傳輸已套用安全應用程式政策的相關資訊至安全應用程式（例如 Kaspersky Endpoint Security for Windows）。您可在安全應用程式介面檢視已傳輸的資訊。

  網路代理會傳輸以下資訊：

  - 政策傳送至受管理裝置的時間
  - 政策傳送至受管理裝置時啟用中或漫遊政策的名稱
  - 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
  - 啟用政策設定檔清單

    您也可使用資訊確保套用正確政策至裝置和用於疑難排解。預設情況下已停用該選項。

- **防護網路代理服務免遭非授權的移除或終止，並防止設定變更**

如果啟用該選項，則網路代理被安裝到受管理裝置之後，沒有所需權限元件無法被移除或重新設定。網路代理服務無法被停止。此選項對網域控制器沒有影響。

啟用此選項可防護以本機管理員權限操作的工作站上的網路代理。

預設情況下已停用該選項。

- **使用解除安裝密碼**

  如果選取該方塊，則按一下**修改**按鈕可以指定 klmover 公用程式和網路代理遠端移除的密碼。

  預設情況下已停用該選項。

儲存區

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

- **已安裝應用程式詳情**
- **包括修補程式資訊**

  安裝在用戶端裝置的應用程式修補程式的資訊會傳送至管理伺服器。啟用此選項可能增加管理伺服器和 DBMS 的負載，並造成資料庫的流量增加。

  預設情況下已啟用該選項。它僅適用於 Windows。

- **Windows Update 更新詳情**

  如果啟用此選項，會將用戶端裝置上應該安裝的 Microsoft Windows Update 更新資訊傳送至管理伺服器。

  有時候，即使停用該選項，更新也會顯示在**可用更新**區域的裝置屬性中。例如，若組織的裝置具有可由這些更新修復的弱點，就可能會發生這個情況。

  預設情況下已啟用該選項。它僅適用於 Windows。

- **軟體弱點和對應更新的詳情**

  若啟用此選項，協力廠商的弱點（包含 Microsoft 軟體）、受管理裝置上偵測到的資訊以及修復協力廠商弱點的軟體更新資訊（不含 Microsoft 軟體）都會傳送至管理伺服器。

  選取此選項（**軟體弱點和對應更新的詳情**）會增加網路負載、管理伺服器磁碟負載和網路代理的資源消耗。

  預設情況下已啟用該選項。它僅適用於 Windows。

  若要管理 Microsoft 軟體更新，請使用**Windows Update 更新詳情**選項。

- **硬體登錄資料詳細資訊**

軟體更新和弱點

在**軟體更新和弱點**區段，您可以設定搜尋 Windows 更新的方式，並啟用對可執行檔的弱點掃描。**軟體更新和弱點**區域的設定僅在執行 Windows 的裝置上可用：

- 在**允許使用者管理 Windows Update 更新的安裝**下，您可以限制使用者可以使用 Windows Update 在他們的裝置上手動安裝的 Windows 更新。

  在執行 Windows 10 的裝置上，如果 Windows Update 已為裝置找到更新，您在**允許使用者管理 Windows Update 更新安裝**下選取的新選項將僅在發現的更新被安裝後才被套用。

  在下拉清單中選取項目：

  - **允許使用者安裝所有可套用 Windows Update 更新**

    使用者可以安裝所有可套用到他們裝置的 Microsoft Windows Update 更新。

    如果您不希望干預更新安裝，請選取該選項。

    當使用者手動安裝 Microsoft Windows Update 更新時，更新可能從 Microsoft 伺服器下載，而不是從管理伺服器。如果管理伺服器還未下載這些更新，這是可能的。從 Microsoft 伺服器下載更新導致額外流量。

  - **僅允許使用者安裝批准的 Windows Update 更新**

    使用者可以安裝所有可應用到他們裝置的和您批准的 Microsoft Windows Update 更新。

    例如，您可能想先在測試環境中檢查更新安裝以確保它們不干預裝置操作，僅在這之後允許安裝這些批准的更新到用戶端裝置。

    當使用者手動安裝 Microsoft Windows Update 更新時，更新可能從 Microsoft 伺服器下載，而不是從管理伺服器。如果管理伺服器還未下載這些更新，這是可能的。從 Microsoft 伺服器下載更新導致額外流量。

  - **不允許使用者安裝 Windows Update 更新**

    使用者無法在他們的裝置上手動安裝 Microsoft Windows Update 更新。所有可套用更新根據您的設定而安裝。

    如果您想要集中管理更新的安裝則選則此選項。

    例如，您可以想最佳化更新排程以便網路不超載。您可以計畫稍後更新，以便它們不干預使用者工作。

- 在**Windows Update 搜尋模式**設定群組中，您可以選取更新搜尋模式：

  - **主動**

如果選中該選項，管理伺服器支援使用網路代理在用戶端裝置上從 Windows 更新代理傳送請求至更新來源：Windows 更新伺服器（或簡稱為 WSUS）。然後，網路代理會將從 Windows 更新代理接收到的資訊傳送給管理伺服器。

只有選取*弱點掃描和所需更新*工作的**連線更新伺服器更新資料**選項時，此選項才會發揮效力。

預設情況下已選定此選項。

- **被動**

  如果您選定該選項，網路代理將從上次同步更新來源之後定期從 Windows 更新代理將所擷取更新的資訊傳遞給管理伺服器。如果 Windows 更新代理沒有執行與更新來源同步，在管理伺服器上的更新資訊就不再是最新的。

  若要從更新來源的記憶體快取獲得更新，請選取此選項。

- **已停用**

  如果選中該選項，管理伺服器不會請求任何有關更新的資訊。

  若您要在本機裝置先測試更新，請選取此選項。

- **當執行可執行檔時掃描其弱點**

  如果啟用此選項，系統將在執行可執行檔時掃描弱點。

  預設情況下已停用該選項。

重新啟動管理

如果您的作業系統必須在您使用、安裝或移除安裝應用程式時重新啟動受管理裝置，請在**重新啟動管理**區域指定執行的操作。**重新啟動管理**區域的設定僅在執行 Windows 的裝置上可用：

- **不要重新啟動作業系統**

  用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

- **如果必要，自動重新啟動作業系統**

  如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

- **提示使用者操作**

  用戶端裝置螢幕上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。該選項適用於使用者必須可以選取最方便的時間進行重新啟動的工作站。

  預設情況下已選定此選項。

- **重複提示間隔（分鐘）**

  如果啟用該選項，應用程式以指定頻率提示使用者重新啟動作業系統。

  預設情況下已啟用該選項。預設間隔是 5 分鐘。可用值介於 1 和 1440 分鐘之間。

  如果停用該選項，提示僅顯示一次。

- **在指定時間後強制重新啟動（分鐘）**

  提示使用者之後，應用程式在指定時間間隔後強制作業系統重新啟動。

  預設情況下已啟用該選項。預設延時是 30 分鐘。可用值介於 1 和 1440 分鐘之間。

- **強制關閉被封鎖工作階段中的應用程式**

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

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

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

  預設情況下已停用該選項。

Windows 共用桌面

您可以透過**Windows 共用桌面**區域啟用並設定在使用共用桌面存取時使用者的遠端裝置上執行的管理員操作的稽核。**Windows 共用桌面**區域的設定僅在執行 Windows 的裝置上可用：

- **啟用稽核**

  如果啟用此選項，則會啟用遠端裝置上管理員的操作稽核。遠端裝置上的管理員操作是被一一記錄下來的：

  - 在遠端裝置的事件記錄中
  - 在位於遠端裝置上網路代理安裝資料夾中的副檔名為 syslog 的檔案中
  - 在卡巴斯基安全管理中心雲端主控台的事件資料庫中

  當符合以下條件時，管理員可使用操作稽核：

  - 弱點和修補程式管理授權使用中
  - 管理員有權啟動共用存取遠端裝置的桌面

  如果清除該選項，則會停用遠端裝置上的管理員操作稽核。

  預設情況下已停用該選項。

- **讀取時要監控的檔案遮罩**

清單包含檔案遮罩。啟用稽核時，應用程式會監控管理員的讀取檔案是否與已讀取檔案的遮罩和從屬資訊相符。若已選取**啟用稽核**核取方塊，則可使用該清單。您可編輯檔案遮罩並新增一個至清單。各個新檔案遮罩應在新行的清單中指定。

預設，指定了以下檔案遮罩:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **修改時要監控的檔案遮罩**

  該清單包含遠端裝置上的檔案遮罩。啟用稽核時，應用程式會監控管理員在符合遮罩的檔案中所作的變更，並儲存這些修改的資訊。若已選取**啟用稽核**核取方塊，則可使用該清單。您可編輯檔案遮罩並新增一個至清單。各個新檔案遮罩應在新行的清單中指定。

  預設，指定了以下檔案遮罩:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

管理修補程式和更新

在**管理修補程式和更新**區段，您可以設定下載受管理裝置、分發更新，以及安裝修補程式：請啟用或停用**對未定義狀態的元件自動安裝可套用更新和修補程式**選項。

連線

連線區域包含三個子區域：

- **網路**
- **連線設定檔**
- **連線排程**

在**網路**子區域，您可以設定到管理伺服器的連線、啟用 UDP 連接埠，和指定 UDP 連接埠號。

- 在**到管理伺服器的連線**設定群組中，您可以指定以下設定：
  - **壓縮網路流量**

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

    用戶端裝置上的 CPU 負載可能會增加。

    預設情況下會啟用此核取方塊。

  - **在 Microsoft Windows 防火牆上開啟網路代理連接埠**

    如果啟用此選項，網路代理工作所需的 UDP 連接埠將新增到 Microsoft Windows 防火牆排除清單中。

    預設情況下已啟用該選項。

  - **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 連接埠號。預設埠號為 15000。

  使用十進位系統記錄。

  如果用戶端裝置執行在 Windows XP Service Pack 2 系統下，則整合的防火牆會封鎖 UDP 連接埠 15000。請手動開啟此連接埠。

- **使用發佈點強制連線到管理伺服器**

  如果您在發佈點設定視窗中選取了**執行推入伺服器**選項，請選取此選項。否則，發佈點將不會作為推送伺服器。

在**連線設定檔**子區段中，由於無法將新項目新增到**管理伺服器連線設定檔**清單，所以**新增**按鈕會停用。預設的連線設定檔也不能修改。

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**
- **在指定時間間隔連線**

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。輪詢設定僅在執行 Windows 的裝置上可用。您可以使用以下選項啟用輪詢並設定其頻率：

- **Windows 網路**

如果啟用此選項，則發佈點會按照您點擊**設定快速輪詢排程**和**設定完整輪詢排程**連結後所設定的排程來自動輪詢網路。

如果停用此選項，則管理伺服器將不輪詢網路。

預設情況下已啟用該選項。

- **IP 範圍**

  如果啟用此選項，則發佈點會按照您點擊**設定輪詢排程**連結後所設定的排程來自動輪詢 IP 範圍。

  如果停用此選項，則發佈點將不輪詢 IP 範圍。

  預設情況下已停用該選項。

- **網域控制器**

  如果啟用此選項，則發佈點將按照您按一下**設定輪詢排程**連結所配置的排程自動輪詢網域控制器。

  如果停用此選項，則發佈點將不輪詢網域控制器。

  在 10.2 版之前的網路代理中，可在**輪詢間隔（分鐘）**欄位中配置網域控制器的輪詢頻率。如果啟用此選項，則該欄位可用。

  預設情況下已停用該選項。

發佈點網路設定

在**發佈點網路設定**區域中，您可以指定網際網路存取設定：

- **使用代理伺服器**
- **位址**
- **連接埠號**
- **略過本機位址的代理伺服器**

  如果啟用此選項，則不使用代理伺服器連線本機網路的裝置。

  預設情況下已停用該選項。

- **代理伺服器身分驗證**

  如果選取該方塊，您可以在輸入欄位中為代理伺服器身分驗證指定憑證。

  預設情況下已清空此方塊。

- **使用者名稱**
- **密碼**

KSN 代理（發佈點）

在 **KSN 代理（發佈點）**區域，您可以設定應用程式使用發佈點，以從受管理裝置轉發 KSN 請求。

- **在發佈點端啟用 KSN 代理**

  KSN 代理服務執行在用作發佈點的裝置上。使用該功能重新分發和最佳化網路流量。

  執行 Linux 或 macOS 的發佈點裝置並不支援此功能。

  發佈點傳送列在卡巴斯基安全網路聲明中的統計資訊到 Kaspersky。依預設，KSN 聲明位於 %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula。

  預設情況下已停用該選項。僅當管理伺服器內容視窗中的**我同意使用卡巴斯基安全網路**選項已啟用時，啟用此選項才會有作用。

  您可以指派活動被動叢集節點到發佈點並在該節點上啟用 KSN 代理伺服器。

- **連接埠**

  受管理裝置將用於連線到 KSN 代理伺服器的 TCP 埠號。預設埠號為 13111。

- **UDP 連接埠**

  如果需要受管理裝置透過 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。

按作業系統比較網路代理政策設定

下表顯示了您可以使用哪些網路代理政策設定來配置具有特定作業系統的網路代理。

網路代理政策設定：按作業系統比較

政策區域	Windows	macOS	Linux
一般	✓	✓	✓
事件配置	✓	✓	✓
設定	✓	✓ 但不包括**使用解除安裝密碼**核取方塊。	✓ 撇去 **使用解除安裝密碼**核取方塊。
儲存區	✓	–	✓ 提供以下功能： • 已安裝應用程式詳情 • 硬體登錄資料詳細資訊
軟體更新和弱點	✓	–	–
重新啟動管理	✓	–	–

Windows 共用桌面	✓	–	–
管理修補程式和更新	✓	–	–
連線→網路	✓	✓ 不包括**在 Microsoft Windows 防火牆上開啟網路代理連接埠**核取方塊。	✓ 不包括**在 Microsoft Windows 防火牆上開啟網路代理連接埠**核取方塊。
連線→連線排程	✓	✓	✓
透過發佈點的網路輪詢	✓ 提供以下功能： • **Windows 網路** • **IP 範圍** • **網域控制器**（Microsoft Active Directory）	–	✓ 提供以下功能： • **IP 範圍** • **網域控制器**（Microsoft Active Directory、以 Samba 作為 Active Directory）
發佈點網路設定	✓	✓	✓
KSN 代理（發佈點）	✓	–	✓

網路代理安裝套件設定

要設定網路代理安裝套件：

1. 執行以下操作之一：

   - 在主功能表中，轉至 **發現和佈署 → 佈署和分配 → 安裝套件**。
   - 在主功能表中，轉至 **操作 → 儲存區 → 安裝套件**。

   系統會顯示可在管理伺服器使用的安裝套件清單。

2. 點擊顯示了網路代理安裝套件名稱的連結。

   網路代理安裝套件的內容視窗即會開啟。視窗中的資訊會分組成頁籤和區段。

一般

一般區域顯示有關安裝套件的一般資訊：

- 安裝套件名稱

- 為其建立該安裝套件的應用程式的名稱和版本
- 安裝套件大小
- 安裝套件建立日期
- 安裝套件資料夾的路徑

設定

本區域顯示為確保網路代理在安裝後就能正確工作所需的設定。該區域的設定僅在執行 Windows 的裝置上可用。

在**目的資料夾**設定群組，您可以選取安裝網路代理的用戶端裝置。

- **安裝到預設資料夾**

  如果選取該選項，網路代理將安裝在 <磁碟機>:\Program Files\Kaspersky Lab\NetworkAgent folder 資料夾中。如果該資料夾不存在，系統會自動建立。

  預設情況下已選定此選項。

- **安裝到指定資料夾**

  如果選取該選項，則網路代理將安裝到輸入欄位中指定的資料夾中。

在以下設定群組中，您可以設定網路代理遠端移除工作的密碼：

- **使用解除安裝密碼**

  如果啟用此核取方塊，透過按一下**修改**按鈕，您可以輸入移除密碼（僅對執行 Windows 的裝置上的網路代理可用）。

  預設情況下已停用該選項。

- **狀態**
- **防護網路代理服務免遭非授權的移除或終止，並防止設定變更**

  如果啟用該選項，則網路代理被安裝到受管理裝置之後，沒有所需權限元件無法被移除或重新設定。網路代理服務無法被停止。此選項對網域控制器沒有影響。

  啟用此選項可防護以本機管理員權限操作的工作站上的網路代理。

  預設情況下已停用該選項。

- **對未定義狀態的元件自動安裝可套用更新和修補程式**

  如果勾選此核取方塊，則會自動安裝所有下載的網路代理更新與修補程式。

  如果該核取方塊被清空，所有下載的更新和修補程式僅在您變更其狀態到*已批准*後被更新。帶有*未定義*狀態的更新和修補程式將不被安裝。

  預設情況下已選取此方塊。

連線

在該區域中，您可以配置網路代理至管理伺服器的連線：

- **使用 UDP 連接埠**

  UDP 連接埠號

  在該欄位中，可以指定使用 UDP 協定連線管理伺服器到網路代理的連接埠。
  預設 UDP 連接埠 15000。

- **在 Microsoft Windows 防火牆中開啟網路代理連接埠**

  如果啟用此選項，網路代理使用的 UDP 連接埠將被新增到 Microsoft Windows 防火牆排除項目清單中。
  預設情況下已啟用該選項。

- **不使用代理伺服器**

- **使用代理伺服器**
  代理伺服器位址
  代理伺服器連接埠

- **代理伺服器身分驗證**

  如果啟用此選項，則您可以在輸入欄位中指定進行代理伺服器身分驗證時所用的憑證。
  我們建議您指定僅具有代理伺服器身分驗證所需的最低權限的帳戶的憑據。
  預設情況下已停用該選項。

  使用者名稱

  建立連線代理伺服器的帳戶的使用者名稱。
  我們建議您指定僅具有代理伺服器身分驗證所需的最低權限的帳戶的憑據。

  密碼

  建立連線代理伺服器的帳戶的密碼。
  我們建議您指定僅具有代理伺服器身分驗證所需的最低權限的帳戶的憑據。

進階

在**進階**區域，可以設定如何使用連線閘道：

- **透過使用連線閘道連線到管理伺服器**

- **連線閘道位址**

- **啟用 VDI 動態模式**

如果啟用此選項，虛擬機上安裝的網路代理的虛擬桌面基礎架構 (VDI) 動態模式將會啟用。
預設情況下已停用該選項。

- **最佳化 VDI 設定**

如果啟用此選項，在網路代理設定中將停用以下功能：

- 獲取已安裝軟體的資訊
- 獲取硬體資訊
- 獲取偵測到的弱點資訊
- 獲取需要更新的資訊

預設情況下已停用該選項。

附加元件

在該區域，您可以為網路代理同時安裝選取附加元件。

標籤

標籤區域顯示網路代理安裝後，可以被新增到用戶端裝置的關鍵字清單。您可以在清單中新增和刪除標籤以及重命名它們。

如果標籤旁的核取方塊被選中，該標籤在網路代理安裝過程中被自動新增到受管理裝置。

如果標籤旁的核取方塊被清空，該標籤在網路代理安裝過程中不被自動新增到受管理裝置。您可以手動新增該標籤到裝置。

當從清單中刪除標籤時，它被自動從所有新增了該標籤的裝置上刪除。

變更歷程

在該區域，您可以檢視安裝套件修訂歷程。您可以比較修訂、檢視修訂、儲存修訂到檔案和新增/編輯修訂敘述。

對特別作業系統可用的網路代理安裝套件設定在下表中給出。

網路代理安裝套件設定

內容區域	Windows	Mac	Linux
一般	✓	✓	✓
設定	✓	–	–
連線	✓	✓ * 但不包括**在 Microsoft Windows 防火牆中開啟網路代理連接埠**核取方塊	✓ * 但不包括**在 Microsoft Windows 防火牆中開啟網路代理連接埠**核取方塊
進階	✓	✓	✓
附加	✓	✓	✓

元件			
標籤	✓	✓ * 除了自動標記規則	✓ * 除了自動標記規則
變更歷程	✓	✓	✓

虛擬基礎架構

卡巴斯基安全管理中心雲端主控台支援使用虛擬機器。為了保護您的虛擬基礎架構，您需要在每個虛擬機器上都安裝網路代理。

降低虛擬機負載的竅門

在虛擬機器上安裝網路代理時，建議您考慮停用一些似乎對虛擬機器幾乎無用的卡巴斯基安全管理中心雲端主控台功能。

當在虛擬機或虛擬機範本上安裝網路代理時，我們建議執行以下操作：

- 如果您正執行遠端安裝，在網路代理安裝套件的內容視窗（在**進階**下），選取**最佳化 VDI 設定**選項。
- 如果您正透過精靈在互動式介面上執行，在精靈視窗，選中**為虛擬架構最佳化網路代理設定**選項。

選中這些選項將改變網路代理設定，因此以下功能保持預設被停用（在套用政策之前）：

- 獲取已安裝軟體的資訊
- 獲取硬體資訊
- 獲取偵測到的弱點資訊
- 獲取需要更新的資訊

通常，這些功能對於虛擬機不必要，因為它們使用統一軟體和虛擬硬體。

停用該功能是不可逆的。如果需要任何被停用的功能，您可以透過網路代理政策啟用它，或透過網路代理本機設定。網路代理本機設定透過管理主控台中相關裝置的上下文功能表可用。

對動態虛擬機的支援

卡巴斯基安全管理中心雲端主控台支援動態虛擬機器。如果虛擬架構佈署在組織網路，動態（暫時）虛擬機可以被用在特定情況。動態虛擬機基於管理員提供的範本以獨立名稱建立。使用者工作在虛擬機一定時間，然後關閉虛擬機後，該虛擬機將被從虛擬架構刪除。安裝了網路代理的虛擬機器亦會被新增至管理伺服器資料庫中。在您關閉此虛擬機器後，管理伺服器資料庫中相對應的項目亦必須移除。

要自動刪除虛擬機項目，當安裝網路代理到範本或動態虛擬機時，選取**啟用 VDI 動態模式**選項：

- 對於遠端安裝—在網路代理安裝套件的內容視窗（**進階**區段）

- 對於互動式安裝–在網路代理安裝精靈

當安裝網路代理到實體裝置時，不要選取**啟用 VDI 動態模式**選項。

如果您要在刪除虛擬機後將動態虛擬機的事件儲存在管理伺服器一段時間，那麼，在管理伺服器內容視窗，在**事件儲存區**區域，選取**裝置被刪除後儲存事件**選項並指定事件的最大儲存期限（天）。

對虛擬機複製的支援

卡巴斯基安全管理中心雲端主控台支援將安裝了網路代理的虛擬機器進行複製，或是以安裝了網路代理的範本為基礎建立虛擬機器。

在以下情況，網路代理可以自動偵測虛擬機器的複製：

- 安裝網路代理時勾選**啟用 VDI 動態模式**選項：在每次重新啟動作業系統後，系統會將此虛擬機視為新裝置，無論此虛擬機是否為複製的虛擬機。
- 以下 hypervisors 之一被使用：VMware™, HyperV®, 或 Xen®：網路代理透過變更的虛擬硬體 ID 偵測虛擬機的複製。

虛擬硬體變更分析並不絕對可靠。在廣泛套用該方法之前，您必須在小組虛擬機上測試您組織中使用的目前 hypervisor 版本。

Windows、macOS 和 Linux 網路代理的使用：比較

與 Windows 網路代理相比，macOS 和 Linux 網路代理具有一些功能限制。網路代理政策和安裝套件設定也根據作業系統不同而不同。下表比較適用於 Windows、macOS 和 Linux 作業系統的網路代理功能和使用情境。

網路代理功能比較

網路代理功能	Windows	Linux	macOS
安裝			
自動安裝網路代理的更新與修補程式	✓	–	–
自動發佈金鑰	✓	✓	✓
在裝置上手動執行應用程式安裝程式安裝	✓	✓	✓
強制同步	✓	✓	✓
發佈點			
網路輪詢	✓ • IP 範圍輪詢	✓ • IP 範圍輪詢	–

	• Windows 網路輪詢 • 網域控制器輪詢（Active Directory）	• 網域控制器輪詢（Microsoft Active Directory、以 Samba 作為 Active Directory）	
在發佈點端執行 KSN 代理服務	✓	–	–
通過 Kaspersky 更新伺服器將更新下載到將更新發佈到受管理裝置的發佈點儲存區	✓	✓	– 執行 macOS 的發佈點裝置無法從 Kaspersky 更新伺服器下載更新。 若一或多個執行 macOS 的裝置位於 *下載更新至發佈點儲存區*工作範圍內，該工作會以*失敗*狀態完成，即使工作已在所有 Windows 裝置上成功完成。
應用程式的推送安裝	✓	受限制：無法使用 Linux 發佈點在 Windows 裝置上執行推送安裝。	
處理協力廠商應用程式			
在裝置上遠端安裝應用程式	✓	–	–
軟體更新	✓	–	–
在網路代理政策中配置作業系統更新	✓	–	–
檢視軟體弱點資訊	✓	–	–
掃描應用程式以尋找弱點	✓	–	–
清查裝置上所安裝的軟體	✓	–	–
虛擬機			
在虛擬機上安裝網路代理	✓	✓	✓
虛擬桌面基礎結構 (VDI) 的最佳化設定	✓	✓	✓
對動態虛擬機的支援	✓	✓	✓
其他			
在遠端用戶端裝置使用 Windows 桌面共用稽核操作	✓	–	–

管理裝置重新啟動	✓	–	–
連線管理員	✓	✓	✓
用戶端裝置的遠端桌面連線	✓	–	–

發佈點內容中會顯示以下區段，但 macOS 版網路代理並不支援相對應的功能：

- 更新來源
- KSN 代理伺服器
- Windows 網域
- Active Directory
- IP 範圍
- 進階
- 統計

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 **資產（裝置）→工作**。
2. 按一下您要為其指定 Unix 特定設定的遠端安裝工作名稱。
   工作內容視窗隨即開啟。
3. 前往**應用程式設定 → Unix 特定設定**。
4. 指定下列設定：

   - **設定根帳戶密碼（僅適用於透過 SSH 佈署）**

     如果不指定密碼，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雲端主控台會以加密形式將密碼傳送到目標裝置、解密該密碼，然後使用指定的密碼，代表根帳戶來啟動安裝程序。

     卡巴斯基安全管理中心雲端主控台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雲端主控台會使用指定的目錄作為透過 SSH 進行存取時的臨時目錄。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雲端主控台安裝 Kaspersky 安全應用程式時，可能需要移除與所要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雲端主控台提供了一些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。您可以在防護佈署精靈中找到該選項。啟用該選項後，卡巴斯基安全管理中心雲端主控台會先移除不相容的應用程式，然後才安裝安全應用程式。

透過專用工作移除不相容的應用程式

若要透過工作移除不相容的應用程式，請使用**遠端解除安裝應用程式**工作。該工作應該在安全應用程式安裝工作執行之前執行在裝置。例如，在安裝工作中，您可以選取排程類型**在完成其它工作時**，這裡，其他工作就是**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。

手動安裝應用程式的選項

您可以在本機裝置上安裝網路代理，無需涉及卡巴斯基安全管理中心雲端中控台。為此，請按照以下主題中的描述為網路代理建立一個獨立安裝套件：建立獨立安裝套件。將套件傳輸到您的用戶端裝置並安裝它。網路代理安裝完成後，您可以將該裝置用作發佈點。

防護佈署精靈

要安裝 Kaspersky 應用程式，您可以使用防護佈署精靈。防護佈署精靈允許使用特別建立的安裝套件或直接從分發套件來遠端安裝應用程式。

防護佈署精靈會執行以下操作：

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

開始防護佈署精靈

要手動啟動防護佈署精靈，

在主功能表中，轉至**發現和佈署 → 佈署和分配 → 防護佈署精靈**。

防護佈署精靈啟動。使用**下一步**按鈕進行精靈。

步驟 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 3：選取裝置

指定要安裝應用程式的裝置清單：

- **安裝到受管理裝置**

  如果選取該選項，程式將為該裝置群組建立遠端安裝工作。

- **選取需要安裝的裝置**

  該工作被分配到裝置選項中的裝置。您可以指定其中一個現有選項。
  例如，您可能要使用該選項在特定作業系統版本的裝置上執行工作。

步驟 4：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，指定如何將安裝程式所需的檔案分發到用戶端裝置中：

- **使用網路代理**

  如果啟用此選項，安裝套件透過安裝在裝置上的網路代理傳送到用戶端裝置。

  如果停用此選項，則會使用用戶端裝置的作業系統工具傳送安裝套件。

  如果已指派工作給安裝了網路代理的裝置，建議您選取該核取方塊。

  預設情況下已啟用該選項。

- **透過發佈點使用作業系統資源**

  如果啟用此選項，安裝套件使用作業系統工具透過發佈點傳送到用戶端裝置。如果網路中存在不止一個發佈點，那麼您可以選取本選項。

  如果選取**使用網路代理**方塊，僅在網路代理工具不可用時才透過作業系統工具傳送檔案。

  預設情況下，已經為虛擬管理伺服器上建立的遠端安裝工作選取該選項。

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 5：重新啟動管理

如果安裝應用程式時作業系統必須重新啟動，指定要執行的操作：

- **不重新啟動裝置**

  用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

- **重新啟動裝置**

  如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

- **提示使用者操作**

  用戶端裝置螢幕上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。該選項適用於使用者必須可以選取最方便的時間進行重新啟動的工作站。

  預設情況下已選定此選項。

- **重複提示間隔（分鐘）**

  如果啟用該選項，應用程式以指定頻率提示使用者重新啟動作業系統。

  預設情況下已啟用該選項。預設間隔是 5 分鐘。可用值介於 1 和 1440 分鐘之間。

  如果停用該選項，提示僅顯示一次。

- **在該時間後重新啟動（分鐘）**

  提示使用者之後，應用程式在指定時間間隔後強制作業系統重新啟動。

  預設情況下已啟用該選項。預設延時是 30 分鐘。可用值介於 1 和 1440 分鐘之間。

- **強制關閉被封鎖工作階段中的應用程式**

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

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

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

  預設情況下已停用該選項。

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雲端主控台自動移除與所部署的應用程式不相容的應用程式，請選取此選項。

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）**

  如果您為其分配遠端安裝工作的裝置上未安裝網路代理，請選取此選項。在這種情況下，您可以指定使用者帳戶來安裝應用程式。

  要指定應用程式安裝程式將在其下執行的使用者帳戶，請點擊**新增**按鈕，選擇**本機帳戶**，然後指定使用者帳戶憑據。

  您可以根據情況指定多個帳戶，例如，沒有一個帳戶在分配工作的所有裝置上擁有全部所需權限時。在此情況下，已新增的所有帳戶會用於從上到下按順序執行該工作。

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。

用於與外部服務交互的網路設定

卡巴斯基安全管理中心雲端主控台會使用以下網路設定與外部服務進行互動。

網路設定

網路設定	位址	敘述
連接埠： 443 協定： HTTPS	activation-v2.kaspersky.com/activationservice/activationservice.svc	應用程式啟動。
連接埠：	https://s00.upd.kaspersky.com https://s01.upd.kaspersky.com	更新 Kaspersky 資料庫、軟體模組和應用程式。

443 協定： HTTPS	https://s02.upd.kaspersky.com https://s03.upd.kaspersky.com https://s04.upd.kaspersky.com https://s05.upd.kaspersky.com https://s06.upd.kaspersky.com https://s07.upd.kaspersky.com https://s08.upd.kaspersky.com https://s09.upd.kaspersky.com https://s10.upd.kaspersky.com https://s11.upd.kaspersky.com https://s12.upd.kaspersky.com https://s13.upd.kaspersky.com https://s14.upd.kaspersky.com https://s15.upd.kaspersky.com https://s16.upd.kaspersky.com https://s17.upd.kaspersky.com https://s18.upd.kaspersky.com https://s19.upd.kaspersky.com https://cm.k.kaspersky-labs.com	
連接埠： 443 協定： HTTPS	https://downloads.upd.kaspersky.com	• 更新 Kaspersky 資料庫、軟體模組和應用程式。 • 檢查卡巴斯基伺服器是否可存取。卡巴斯基安全管理中心雲端主控台會在下載 Kaspersky 資料庫和軟體模組之前，先檢查 Kaspersky 伺服器是否可供存取。如果無法使用系統 DNS 存取伺服器，則應用程式使用公用 DNS 伺服器。
連接埠： 80 協定： HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com	更新 Kaspersky 資料庫、軟體模組和應用程式。

	http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	
連接埠： 443 協定： HTTPS	ds.kaspersky.com	使用卡巴斯基安全網路。
連接埠： 443、 1443 協定： HTTPS	ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com	使用卡巴斯基安全網路。
協定： HTTPS	click.kaspersky.com redirect.kaspersky.com	開啟介面中的連接。
連接埠： 80 協定： HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	公有金鑰基礎架構 (PKI)。
連接埠： 443 協定： HTTPS	https://ipm-klca.kaspersky.com	行銷公告。

準備在封閉軟體環境模式下執行 Astra Linux 的裝置以安裝網路代理

在封閉軟體環境模式下執行 Astra Linux 的裝置上安裝網路代理之前，您必須執行兩個準備過程：下面說明中的一個和適用於任何 Linux 裝置的常規準備步驟。

在您開始之前：

- 請確認您要安裝 Network Agent for Linux 的裝置是執行支援的 Linux 版本。
- 從卡巴斯基網站下載必要的網路代理安裝檔案.

在具有 root 權限的帳戶下執行本指令中提供的命令。

準備在封閉軟件環境模式下執行 Astra Linux 的裝置以安裝網路代理：

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

   ```
   DIGSIG_ELF_MODE=1
   ```

2. 在指令行中，執行以下指令來安裝相容套件：

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

3. 為應用程式金鑰建立一個目錄：

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

4. 將應用程式金鑰 /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg 放在上一步建立的目錄中：

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

   如果卡巴斯基安全管理中心雲端主控台分發套件不含 kaspersky_astra_pub_key.gpg 應用程式金鑰，您可以點擊以下連結進行下載：
   https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg。

5. 更新 RAM 瓷碟：

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

   重新啟動系統。

6. 執行對任何 Linux 裝置通用的準備步驟。

裝置已準備。您現在可以繼續安裝網路代理。

準備 Linux 裝置並在 Linux 裝置上遠端安裝網路代理

網路代理安裝包括兩個步驟：

- Linux 裝置準備
- 網路代理遠端安裝

Linux 裝置準備

要準備執行 Linux 的裝置以遠端安裝網路代理：

1. 確保目標 Linux 裝置上已安裝下列軟體：

   - Sudo
   - Perl 語言解譯器 5.10 或更高版本

2. 測試裝置配置：

   a. 檢查是否您可以透過 SSH 用戶端（例如 PuTTY）連線到裝置。

   如果您無法連線到裝置，開啟檔案 /etc/ssh/sshd_config 並確保以下設定具有以下相關值：

   ```
   PasswordAuthentication no
   ChallengeResponseAuthentication yes
   ```

   如果您可以毫無問題地連線到裝置，請不要修改 /etc/ssh/sshd_config 檔案；否則在執行遠端安裝工作時可能會遇到 SSH 認證失敗的情況。

   儲存檔案（如果必要）並使用 `sudo service ssh restart` 命令來重新啟動 SSH 服務。

   b. 停用要連線裝置的使用者帳戶的 sudo 密碼。

   c. 使用 sudo 的 `visudo` 指令開啟 sudoers 設定檔。

   在開啟的檔案中，找到以 `%sudo`（或 `%wheel`，如果您使用的是 CentOS 作業系統）開始的行。在此行下，指定以下內容：`<username> ALL = (ALL) NOPASSWD: ALL`。此種情況下，`<username>`是用於透過 SSH 進行裝置連線的使用者帳戶。如果您使用的是 Astra Linux 作業系統，請在 /etc/sudoers 檔案的最後一行新增以下文字：`%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

   d. 儲存並關閉 sudoers 檔案。

   e. 透過 SSH 再次連線裝置並確保 Sudo 服務不提示您輸入密碼；您可以使用 `sudo whoami` 指令來操作。

3. 開啟 /etc/systemd/logind.conf 檔案，接著執行以下操作之一：

   - 指定 no（否）為 KillUserProcesses 設定的值：`KillUserProcesses=no`。
   - 對於 KillExcludeUsers 設定，請輸入執行遠端安裝之帳戶的使用者名稱，例如：`KillExcludeUsers=root`。

   如果目標裝置正在執行 Astra Linux，在`/home/<`使用者名稱`>/.bashrc`檔案新增`export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin`子串，其中`< username >`是用於使用 SSH 進行裝置連線的使用者帳戶。

   若要套用變更的設定，請重新啟動 Linux 裝置或執行以下命令：

   ```
   $ sudo systemctl restart systemd-logind.service
   ```

4. 如果您想在使用 SUSE Linux Enterprise Server 15 作業系統的裝置上安裝網路代理，請先安裝 insserv-compat 套件以設定網路代理。

5. 如果要在封閉軟體環境模式下執行 Astra Linux 作業系統的裝置上安裝網路代理，請執行額外的步驟來準備 Astra Linux 裝置。

網路代理遠端安裝

要在 Linux 裝置上遠端安裝網路代理：

1. 下載並建立安裝套件：

   a. 在裝置上安裝之前，請確保該安裝套件安裝了所有的先決條件（程式和庫）。

   您可以自己檢視每個安裝套件的先決條件，使用 Linux 分發套件的實用工具。有關更多公用程式的詳情，請參閱您的作業系統文件。

   b. 使用應用程式介面或從卡巴斯基網站下載網路代理安裝套件。

   c. 要建立遠端安裝套件，使用以下檔案：

   - klnagent.kpd
   - akinstall.sh
   - 網路代理的 .deb 或 .rpm 套件

2. 使用以下設定建立遠端安裝工作：

   - 在新工作精靈的**設定**頁面，選取**透過管理伺服器使用作業系統資源**核取方塊。清空所有其他核取方塊。
   - 在**選取要執行此工作的帳戶**頁面，請指定透過 SSH 進行裝置連線的使用者帳戶設定。

3. 執行遠端安裝工作。使用 `su` 指令的選項保護環境：`-m, -p, --preserve-environment`。

如果您在早於 20 版本的 Fedora 裝置上使用 SSH 安裝網路代理，可能返回錯誤。此種情況下，為了成功安裝網路代理，請在 /etc/sudoers 檔案注釋出預設選項（用註釋符號將其圍住以防止其被解析）。對於可能導致 SSH 連線問題的預設選項的詳細說明，請參考 Bugzilla bugtracker 網站。

行動裝置管理

若要透過卡巴斯基安全管理中心雲端主控台管理行動裝置防護，必須使用「行動裝置管理」功能。如果您要管理組織員工擁有的行動裝置，請啟用和配置行動裝置管理。

行動裝置管理可讓您管理員工的 Android 裝置。該防護是由裝置上安裝的 Kaspersky Security for Mobile 應用程式所提供。該行動應用程式會確保保護行動裝置免受 Web 威脅、病毒和其他構成威脅的程式的侵害。

有關行動裝置的防護部署和管理的資訊，請參閱Kaspersky Security for Mobile 說明。

偵測和回應功能

本節包含各項 Kaspersky 解決方案的資訊，這些解決方案可整合到卡巴斯基安全管理中心雲端主控台中，使主控台多出偵測和回應功能。

關於偵測和回應功能

卡巴斯基安全管理中心雲端主控台的主控台介面中可以整合其他 Kaspersky 解決方案的功能。例如，您可以將偵測和回應功能新增至卡巴斯基安全管理中心雲端主控台的功能中。

偵測和回應解決方案是專為保護組織的 IT 基礎架構免受複雜網路威脅的侵害而設計。該解決方案的功能將自動偵測威脅以及對這些威脅做出回應的功能相結合，以抵禦複雜的攻擊，包括新的弱點利用、勒索軟體、無檔案攻擊以及取道合法系統工具的方法。

您可以整合以下解決方案：

- Kaspersky Endpoint Detection and Response Optimum

  在 Kaspersky Endpoint Protection Platform（簡稱 EPP）應用程式偵測到威脅後，卡巴斯基安全管理中心雲端主控台會在警示清單中新增一筆警示。警示中會包含所偵測到威脅的詳細資訊，供您分析並調查威脅。您也可以建立威脅發展鏈圖表，將事件做視覺化呈現。該圖表會及時描述所偵測到攻擊的部署階段。

  作為回應，您可以選擇其中一項預先定義的回應操作，例如，隔離不受信任的物件、將受感染的裝置自網路上隔離，或是為不受信任的物件建立防止執行規則。

  如需有關啟動該解決方案的資訊，請參閱 Kaspersky Endpoint Detection and Response Optimum 說明文件。

- Kaspersky Managed Detection and Response

  在 Kaspersky EPP 應用程式偵測到威脅後，卡巴斯基安全管理中心雲端主控台會在事件清單中新增一筆事件。事件中會包含所偵測到威脅的詳細資訊。Kaspersky 的 MDR 安全運營中心 (SOC) 分析人員或是協力廠商公司會調查事件並提供用於解決事件的回應方式。您可以手動接受或拒絕所提供的措施，或是啟用用於自動接受所有回應的選項。

  如需有關啟動該解決方案的資訊，請參閱 Kaspersky Managed Detection and Response 說明文件。

- Kaspersky Endpoint Detection and Response Expert

  此解決方案適用於擁有 SOC 分析團隊的組織。偵測到的威脅會被標註為警示或事件，以供分配給 SOC 分析人員進行調查。Kaspersky Endpoint Detection and Response Expert 會向您提供每個警示或事件的詳細資訊，以及用於管理警示與事件、搜尋威脅以及開發自訂規則的工具。SOC 分析人員或安全官可以手動選取回應操作，或是採用預先定義的自動化回應措施。

  如需有關啟動該解決方案的資訊，請參閱 Kaspersky Endpoint Detection and Response Expert 說明文件。

整合偵測和回應功能後的介面變更

以下 Kaspersky 解決方案提供的偵測和回應功能可整合到卡巴斯基安全管理中心雲端主控台介面中：

- Kaspersky Endpoint Detection and Response (EDR) Optimum
- Kaspersky Managed Detection and Response (MDR)
- Kaspersky Endpoint Detection and Response (EDR) Expert

下表列出了這些解決方案在經整合後，會對卡巴斯基安全管理中心雲端主控台介面造成的變更。

解決方案	卡巴斯基安全管理中心雲端主控台中的變更
Kaspersky EDR Optimum	新增以下元素： • **警示**區段（**監控和報告 → 警示**）。此解決方案偵測到的警示會列在 **Optimum** 頁籤上。 • **控制板**上的一項小工具（**監控和報告 → 控制板**）。
Kaspersky MDR	新增以下元素： • **MDR**區段（**監控和報告 → MDR**）。 • **顯示 MDR 功能**選項（**設定 → 介面選項 → 顯示 MDR 功能**）。 • **控制板**上的一項小工具（**監控和報告 → 控制板**）。
卡巴斯基 EDR 專家	新增以下元素： • **警示**區段（**監控和報告 → 警示**）。此解決方案偵測到的警示會列在 **Expert** 頁籤上。 • **事件**區段（**監控和報告 → 事件**）。 • **搜尋威脅**區段（**監控和報告 → 搜尋威脅**）。 • **自訂規則**區段（**監控和報告 → 自訂規則**）。 • Kaspersky EDR Expert 的一般設定（**設定 → 整合 → Kaspersky EDR Expert**）。 • **控制板**上的多項小工具（**監控和報告 → 控制板**）。

發現網路裝置以及建立管理群組

本節說明如何搜尋和發現網路裝置，以及為這些裝置建立管理群組。

卡巴斯基安全管理中心雲端主控台可讓您依指定的條件尋找裝置。您可以儲存搜尋結果到文字檔案。

搜尋和發現功能可讓您尋找以下裝置：

- 卡巴斯基安全管理中心雲端主控台管理伺服器（和其從屬管理伺服器）的管理群組中的受管理裝置。
- 受卡巴斯基安全管理中心雲端主控台管理伺服器（和其從屬管理伺服器）管理的未指派的裝置。

情境：發現網路裝置

在初始化部署安全應用程式之前，您必須先執行裝置發現。當所有網路裝置都獲發現後，您就能接收它們的資訊並透過政策加以管理。您需要定期執行網路輪詢，以便發現新裝置並檢查先前發現的裝置是否仍在網路中。

當您完成此情境後，裝置發現作業將已設定完成並會依指定的排程進行。

先決條件

在卡巴斯基安全管理中心雲端主控台中，裝置發現作業是由發佈點執行。開始之前，請執行以下操作：

- 決定要讓哪些裝置擔任發佈點。
- 將網路代理安裝到所選的裝置上。
- 手動將裝置分配為發佈點。

階段

此情境分幾個階段進行：

1. **選擇發現類型**

   決定您要定期使用哪些發現類型。

2. **設定輪詢**

   在每個發佈點的內容中，啟用並設定所選的網路輪詢類型：Windows 網路輪詢、網域控制器輪詢或 IP 範圍輪詢。請確保輪詢排程符合您組織的需求。

   如果網域中包含網路裝置，建議使用網域控制器輪詢。

3. **設定規則以新增發現的裝置到管理群組（可選）**

   如果您的網路上出現了新裝置，這些裝置會在定期輪詢期間獲發現並被自動加到**未配置的裝置**群組。如有需要，您可以設定規則來自動將這些裝置移到**受管理裝置**群組。您也可以建立保留規則。

   如果您略過此規則設定步驟，所有新發現的裝置都會移到**未配置的裝置**群組並留在該處。如有需要，您可以手動將這些裝置移到**受管理裝置**群組。如果您將這些裝置移到**受管理裝置**群組，您可以分析每個裝置的資訊，然後決定是否將裝置移到管理群組（以及是的話，要移到哪個群組）。

當網路輪詢操作完成時，請檢查新發現的裝置是否已依設定的規則受到排列。如果未設定任何規則，則這些裝置會留在**未配置的裝置**群組。

網路輪詢

卡巴斯基安全管理中心雲端主控台會透過定期輪詢 Windows 網路、IP 範圍、Microsoft Active Directory 網域控制器和 Samba 網域控制器，收到與網路結構和該網路所含裝置有關的資訊。以 Samba 網域控制器而言，是使用 Samba 4 作為 Active Directory 網域控制器。網路輪詢可以手動啟動，也可以依排程自動啟動。

卡巴斯基安全管理中心雲端主控台會依輪詢結果，更新未配置的裝置清單。您也可以設定規則來將新發現的裝置自動移到管理群組。

卡巴斯基安全管理中心雲端主控台使用的網路輪詢方法如下：

- *IP 範圍輪詢*。卡巴斯基安全管理中心雲端主控台會使用網際網路控制訊息通訊協定 (ICMP) 封包來輪詢指定的 IP 範圍，然後將這些 IP 範圍內的裝置彙整成一組完整資料。
- *Windows 網路輪詢*。您有兩種 Windows 網路輪詢可以執行：快速輪詢或完整輪詢。在快速輪詢期間，卡巴斯基安全管理中心雲端主控台僅會從所有網域與工作群組中的裝置 NetBIOS 名稱清單擷取資訊。在完整輪詢期間，則會向每個裝置索取以下資訊：作業系統 (OS) 名稱、IP 位址、DNS 名稱和 NetBIOS 名稱。
- *網域控制器輪詢*。與 Active Directory 單位結構以及各 Active Directory 群組中的裝置 DNS 名稱有關的資訊會記錄到卡巴斯基安全管理中心雲端主控台資料庫中。

以*Windows 網路輪詢*和*網域控制器輪詢*方法進行輪詢的結果會另外顯示在**發現和佈署 → 發現**區段中。

以 *IP 範圍輪詢*方法進行輪詢的結果則會顯示在**發現和佈署 → 未配置的裝置** 區段中。

一台裝置可能會顯示在不止一個偵測區域中。如果在 HQ 網域中偵測到某台裝置，而該裝置的位址為 192.168.0.1，則該裝置會同時出現在 **Windows 網域**區段和**未配置的裝置**區段中。您可以修改每種輪詢方法的網路輪詢設定。例如，您可能想要修改輪詢排程或者設定是否輪詢整個 Active Directory 樹系還是僅指定網域。

Windows 網路輪詢

關於 Windows 網路輪詢

在快速輪詢過程中，管理伺服器只會從所有網域和工作群組中裝置的 NetBIOS 名稱清單獲取資訊。在完整輪詢中，以下資訊被從每個用戶端裝置請求：

- 作業系統名稱
- IP 位址
- DNS 名稱
- NetBIOS 名稱

快速輪詢和完整輪詢都需要以下：

- 連接埠 UDP 137/138、TCP 139 在網路中必須可用。

- 必須使用 Microsoft Computer Browser 服務，且主瀏覽器電腦在發佈點上必須為啟用狀態。
- 必須使用 Microsoft Computer Browser 服務，且主瀏覽器電腦必須在用戶端裝置上啟用。
  - 至少一台裝置上，如果網路裝置數量不超過 32。
  - 對每 32 台網路裝置至少一台裝置上。

完整輪詢僅在快速輪詢至少執行了一次時可以執行。

檢視和修改 Windows 網路輪詢設定

要修改 Windows 網路輪詢內容：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**發佈點**區段。
3. 點擊要用於進行輪詢網路的發佈點名稱。
   分發點內容視窗將開啟。
4. 選取 **Windows 網域輪詢**區段。
5. 使用**啟用網路輪詢**切換按鈕啟用或停用 Windows 網路輪詢。
6. 設定快速輪詢和完整輪詢的排程。
7. 點擊**確定**按鈕。

內容被儲存並套用到所有發現的 Windows 網域和工作群組。

網域控制器輪詢

卡巴斯基安全管理中心雲端主控台支援輪詢 Microsoft Active Directory 網域控制器和 Samba 網域控制器。以 Samba 網域控制器而言，是使用 Samba 4 作為 Active Directory 網域控制器。當您輪詢網域控制器時，發佈點會擷取與網域結構、使用者帳戶、安全群組以及網域所含裝置的 DNS 名稱有關的資訊。網域控制器輪詢會依您設定的排程來執行。

先決條件

在輪詢網域控制器之前，請確保啟用以下協定：

- 簡單身分驗證和安全層 (SASL)
- 輕量級目錄訪問協定 (LDAP)

確保網域控制器裝置上的以下連接埠可用：

- 389 用於 SASL

- 636 用於 TLS

使用發佈點進行網域控制器輪詢

您還可以使用發佈點輪詢網域控制器。基於 Windows 或 Linux 的受管理裝置可以充當發佈點。

對於 Linux 發佈點，支援對 Microsoft Active Directory 網域控制器和 Samba 網域控制器進行輪詢。
對於 Windows 發佈點，僅支援對 Microsoft Active Directory 網域控制器的輪詢。
使用 Mac 發佈點進行輪詢不受支援。

要使用發佈點配置網域控制器輪詢：

1. 開啟發佈點屬性。
2. 選擇**網域控制器輪詢**部分。
3. 選取**啟用網域控制器輪詢**選項。
4. 選擇要輪詢的網域控制器。
   如果您使用 Linux 發佈點，請在**輪詢指定網域**部分中點擊**新增**，然後指定網域控制器的位址和使用者憑據。
   如果您使用 Windows 發佈點，則可以選擇以下選項之一：
   - **輪詢目前網域**
   - **輪詢整個網域樹系**
   - **輪詢指定網域**
5. 如果需要，點擊**設定輪詢排程**按鈕以指定輪詢排程選項。
   輪詢僅根據指定的排程開始。無法手動啟動輪詢。

輪詢完成後，網域結構即會顯示在**網域控制器** 區段中。

如果您設定並啟用了裝置移動規則，則新發現的裝置會自動加到**受管理裝置**群組中。如果未啟用移動規則，新發現的裝置被自動包含在**未配置的裝置**群組。

獲發現的使用者帳戶可供在卡巴斯基安全管理中心雲端主控台中用於進行網域身分驗證。

檢視網域控制器輪詢結果

若要檢視網域控制器輪詢結果：

1. 在主功能表中，前往**發現和佈署 → 發現 → 網域控制器**。
   發現的組織單元清單被顯示。
2. 選取組織單位，然後點擊**裝置**按鈕。
   組織單元中的裝置清單被顯示。

您可以搜尋清單和篩選結果。

IP 範圍輪詢

卡巴斯基安全管理中心雲端主控台會嘗試利用標準 DNS 請求，對指定範圍中的每個位址執行反向名稱解析來得出 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。如果裝置有所回應，該裝置的資訊即會被新增到卡巴斯基安全管理中心雲端主控台資料庫中。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。在使用了 Active Directory 的網路中，會自動維護這類網域。但是在這些網路中，IP 子網路輪詢提供的資訊不會比 Active Directory 輪詢多。而且，小網路的管理員經常不配置反向查詢區，因為它對許多網路服務來說是不必要的。由於所有這些原因，IP 子網路輪詢預設被停用。

一開始，卡巴斯基安全管理中心雲端主控台會從用於進行網路輪詢的發佈點裝置本身的網路設定，取得要輪詢的 IP 範圍。如果裝置位址是 192.168.0.1 且子網路遮罩是 255.255.255.0，則卡巴斯基安全管理中心雲端主控台會自動將網路 192.168.0.0/24 加到輪詢位址清單中。卡巴斯基安全管理中心雲端主控台會輪詢 192.168.0.1 到 192.168.0.254 之間的所有位址。

如果您使用 Windows 網路輪詢和/或 Active Directory 輪詢，則不建議您使用 IP 範圍輪詢。

瀏覽和修改 IP 範圍輪詢設定

要瀏覽和修改 IP 範圍輪詢設定：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**發佈點**區段。
3. 點擊要用於進行輪詢網路的發佈點名稱。
   分發點內容視窗將開啟。
4. 選取 **IP 範圍輪詢**區段。
5. 使用**啟用範圍輪詢**切換按鈕啟用或停用 IP 輪詢。
6. 設定輪詢排程。預設下，IP 輪詢每 420 分鐘（七小時）執行一次。
7. 如有必要，請新增或修改要輪詢的 IP 範圍。
   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。
8. 點擊**確定**按鈕。

內容封包儲存並套用到所有 IP 範圍。

配置 Samba 網域控制器

卡巴斯基安全管理中心雲端主控台支援僅以 Samba 4 執行的 Linux 網域控制器。

Samba 網域控制器支援與 Microsoft Active Directory 網域控制器相同的架構延伸。您可以使用 Samba 4 架構延伸啟用 Samba 網域控制器與 Microsoft Active Directory 網域控制器的完全相容。這是一個可選操作。

我們建議啟用 Samba 網域控制器與 Microsoft Active Directory 網域控制器的完全相容。這將確保卡巴斯基安全管理中心雲端主控台與 Samba 網域控制器之間能夠正確互動。

要啟用 Samba 網域控制器與 Microsoft Active Directory 網域控制器的完全相容：

1. 執行以下指令以使用 RFC2307 架構延伸：

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. 在 Samba 網域控制器中啟用架構更新。為此，請新增以下行列到 /etc/samba/smb.conf 檔案中：

   ```
   dsdb:schema update allowed = true
   ```

   如果架構更新完成時出現錯誤，則需要對充當架構主機的網域控制器執行完整還原。

如果要正確輪詢 Samba 網域控制器，則必須在 /etc/samba/smb.conf 檔案中指定`netbios` 名稱和工作群組參數。

新增和修改 IP 範圍

一開始，Kaspersky Security Center Cloud Console 會從用於進行網路輪詢的發佈點裝置本身的網路設定，取得要輪詢的 IP 範圍。如果裝置位址是 192.168.0.1 且子網路遮罩是 255.255.255.0，則卡巴斯基安全管理中心雲端主控台會自動將網路 192.168.0.0/24 加到輪詢位址清單中。卡巴斯基安全管理中心雲端主控台會輪詢 192.168.0.1 到 192.168.0.254 之間的所有位址。您可以修改自動定義的 IP 範圍或新增自訂 IP 範圍。

要新增新 IP 範圍：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**發佈點**區段。
3. 點擊要用於進行輪詢網路的發佈點名稱。
   分發點內容視窗將開啟。
4. 選取 **IP 範圍輪詢**區段。
5. 若要建立新的 IP 範圍，請點擊**新增**按鈕。
6. 在開啟的視窗，指定以下設定：

   - **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。

- **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。

7. 點擊**確定**按鈕。

新 IP 範圍被新增到 IP 範圍清單。

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。

發佈點和連線閘道器的調整

在卡巴斯基安全管理中心雲端主控台中，管理群組的結構具有以下功用：

- 設定政策範圍

  套用相關設定到裝置有另一種方式，透過使用*政策設定檔*。在此情況下，政策的涵蓋範圍是依標記、Active Directory 組織單元中的裝置位置、Active Directory 安全群組中的成員資格等等來設定。

- 設定群組工作範圍

  還有一個不基於管理群組層級定義群組工作範圍的方法：使用裝置分類的工作和特定裝置的工作。

- 設定對裝置和從屬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。讓發佈點達最佳分佈，將可節省您組織網路中的流量。

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。

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。請使用下表計算您的網路所需的發佈點數量。

請確認您計畫要指派為發佈點的裝置具有足量的可用磁碟空間、不會經常關機，並且停用了睡眠模式。

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/10000 + 1)，建議：(N/5000 + 2)，N 是網路裝置數量

網路中基於網路裝置數量被專門分配的包含多個網段的發佈點的數量

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

使用標準用戶端裝置（工作站）作為發佈點

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

網路中基於網路裝置數量作為發佈點工作的包含單一網段的工作站的數量

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

網路中基於網路裝置數量作為發佈點工作的包含多個網段的工作站的數量

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

如果某個發佈點無法使用，請手動更新 Kaspersky 伺服器、軟體模組和應用程式或直接從 Kaspersky 更新資料庫更新。

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。

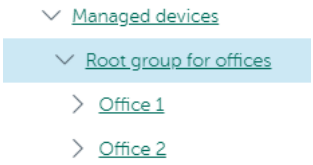
有以下構建管理群組結構的方法：

- 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。
- 不考慮網路拓撲而構建管理群組結構。在此情況下，您必須為網路中每個獨立部分的根管理群組（例如**受管理裝置**群組）各分配一或多個裝置作為發佈點。所有這些發佈點都會位於相同層級，且涵蓋範圍都同樣是組織網路中的所有裝置。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：多個小遠端辦公室

該標準配置用於一定數量的小型遠端辦公室，您可透過網際網路與總部通訊。每個遠端辦公室都位於 NAT 之外，就是說，從一個遠端辦公室到另一個遠端辦公室的連線是不可能的，因為辦公室是彼此隔離的。

配置必須在管理群組中體現：必須為每個遠端辦公室建立各自的管理群組（下圖中的群組**辦公室 1** 和**辦公室 2**）。



遠端辦公室包含在管理群組結構

您必須指定一或多個發佈點給一間辦公室的每個對應管理群組。發佈點必須是遠端辦公室中具有足夠剩餘磁碟空間的裝置。佈署在**辦公室 1** 群組的裝置，例如，將存取分配到**辦公室 1** 管理群組的發佈點。

如果一些使用者在辦公室之間移動他們的攜帶式電腦，您必須在遠端辦公室選取兩個或更多裝置（除了現有的發佈點）並分配它們作為等級管理群組的發佈點（上圖中**辦公室根群組**）。

例如：攜帶式電腦佈署在**辦公室 1** 管理群組，然後被移動到對應於**辦公室 2** 管理群組的辦公室。在移動攜帶式電腦後，網路代理試圖存取分配到**辦公室 1** 群組的發佈點，但是那些發佈點不可用。然後，網路代理開始嘗試存取分配到**辦公室根群組**的發佈點。因為遠端辦公室是彼此隔離的，嘗試存取分配到**辦公室根群組**管理群組的發佈點僅在網路代理嘗試存取**辦公室 2** 群組中的發佈點時才會成功。就是說，攜帶式電腦將保持在原始辦公室對應的管理群組，但是將使用它當時所在辦公室的發佈點。

手動分配發佈點

卡巴斯基安全管理中心雲端主控台可讓您手動將裝置分配為發佈點。建議您計算您網路所需的發佈點數量與配置。

執行 macOS 的發佈點裝置無法從 Kaspersky 更新伺服器下載更新。

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

作為發佈點的裝置必須被防護，包括實體防護，以防範非授權的存取。

要手動指派裝置作為發佈點：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**發佈點**區段。
3. 點擊**分配**按鈕。
4. 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。

5. 選擇您要包含在所選發佈點範圍的管理群組。

6. 點擊**新增**按鈕。

   您新增的發佈點將顯示在**發佈點**區域的發佈點清單。

7. 在清單中選擇新增的發佈點以開啟其內容視窗。

8. 在內容視窗中配置發佈點：

   - **一般**區段中包含發佈點與用戶端裝置之間的互動設定：

     - **SSL 連接埠**

       用戶端裝置與發佈點之間，使用 SSL 進行安全連線的 SSL 埠號。

       預設情況下使用連接埠 13000。

     - **使用多點傳送**

       如果啟用此選項，程式會使用 IP 多點傳送，在群組中的各用戶端裝置上自動發佈安裝套件。

       IP 多點傳送會減少從安裝套件安裝應用程式至一組用戶端裝置的時間，但當您安裝應用程式至單一用戶端裝置時安裝時間會增加。

     - **IP 多點傳送位址**

       用於多點傳送的 IP 位址。您可以定義範圍是 224.0.0.0 – 239.255.255.255 的 IP 位址

       卡巴斯基安全管理中心雲端主控台預設會自動分配一個位於指定範圍內的唯一 IP 多點傳送位址。

     - **IP 多點傳輸連接埠號**

       IP 多點傳輸的埠號。

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

     - **佈署更新**

       更新被從以下來源分發到受管理裝置：

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

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

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

     - **佈署安裝套件**

安裝套件被從以下來源分發到受管理裝置：

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

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

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

- **執行推入伺服器**

在卡巴斯基安全管理中心雲端主控台中，對於以網路代理管理的基於 Windows 和基於 Linux 的裝置，發佈點可以作為推送伺服器使用。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。如果您為同一個管理群組分配了多個發佈點，則可以在每個發佈點上啟用推送伺服器。在這種情況下，管理伺服器會平衡發佈點之間的負載。

- **推入伺服器連接埠**

推送伺服器的連接埠號。您可以指定任何未佔用連接埠的編號。

- 在**範圍**區域中，指定發佈點將發佈更新的範圍（管理群組和/或網路定位）。

僅執行 Windows 作業系統的裝置可以定義網路位置。網路位置無法定義在執行其他作業系統的裝置上。

- 在 **KSN 代理**區域，您可以設定應用程式使用發佈點，以從受管理裝置轉發 KSN 請求：

  在發佈點端啟用 KSN 代理

KSN 代理服務執行在用作發佈點的裝置上。使用該功能重新分發和最佳化網路流量。

執行 Linux 或 macOS 的發佈點裝置並不支援此功能。

發佈點傳送列在卡巴斯基安全網路聲明中的統計資訊到 Kaspersky。依預設，KSN 聲明位於 %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula。

預設情況下已停用該選項。僅當管理伺服器內容視窗中的**我同意使用卡巴斯基安全網路**選項已啟用時，啟用此選項才會有作用。

您可以指派活動被動叢集節點到發佈點並在該節點上啟用 KSN 代理伺服器。

- 透過發佈點配置 Windows 網域、Active Directory 和 IP 範圍的輪詢：

- **Windows 網域輪詢**

您可以啟用 Windows 網域裝置發現並為發現設定排程。

- **Active Directory**

您可以啟用 Active Directory 網域網路輪詢並為輪詢設定排程。

如果您使用 Windows 發佈點，則可以選擇以下選項之一：

- **輪詢目前 Active Directory 網域**。
- **輪詢 Active Directory 網域樹系**。
- **僅輪詢所選 Active Directory 網域**。如果您選取該選項，新增一個或更多 Active Directory 網域到清單。

如果您使用安裝了網路代理版本 15 的 Linux 發佈點，則只能輪詢為其指定位址和使用者憑據的 Active Directory 網域。目前 Active Directory 網域和 Active Directory 網域樹系的輪詢不可用。

- **IP 範圍輪詢**

您可以為 IPv4 範圍和 IPv6 網路啟用裝置發現。

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

如果啟用**使用 Zeroconf 來輪詢 IPv6 網路**選項，發佈點將使用零配置網路（也稱為"*Zeroconf*"）自動輪詢 IPv6 網路。在這種情況下，指定的 IP 範圍將被忽略，因為發佈點會輪詢整個網路。如果發佈點執行 Linux，則**使用 Zeroconf 來輪詢 IPv6 網路**選項可用。要使用 Zeroconf Ipv6 輪詢，您必須在發佈點上安裝 avahi-browse 公用程式。

- 在**進階**區段中，指定發佈點必須用來儲存發佈資料的資料夾：
  - **使用預設資料夾**

如果您選取此選項，應用程式使用發佈點上的網路代理安裝資料夾。

  - **使用指定資料夾**

如果您選取該選項，則可以在下面的欄位中指定該資料夾的路徑。它可以是發佈點上的本機資料夾，也可以是企業網路上任何裝置的資料夾。

發佈點上用於執行網路代理的帳戶必須具有對指定資料夾的存取權限以進行讀寫操作。

9. 點擊**確定**按鈕。

所選裝置作為發佈點執行。

修改管理群組的發佈點清單

您可以檢視為特定管理群組分配的發佈點清單並透過新增或刪除發佈點來修改清單。

要檢視和修改分配給管理群組的發佈點清單：

1. 在主功能表中，前往**資產（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**標籤。

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。

使用發佈點作為推送伺服器

在 Kaspersky Security Center Cloud Console 中，對於以網路代理管理的基於 Windows 和基於 Linux 的裝置，發佈點可以作為推送伺服器使用。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。如果您為同一個管理群組分配了多個發佈點，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。

您可以將發佈點作為推送伺服器，確保受管理裝置與管理伺服器之間會持續連線。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。如果您將發佈點作為推送伺服器，即無需傳送封包到網路代理的 UDP 連接埠。

若要將發佈點用作推送伺服器：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。

   管理伺服器內容視窗將開啟。

2. 在**一般**頁籤，選取**發佈點**區段。

3. 點擊要作為推送伺服器的發佈點。

4. 在所選發佈點的內容清單中，前往**一般**區段，然後啟用**執行推入伺服器**選項。

   推入伺服器連接埠輸入欄位即會變得可用。

5. 在**推入伺服器連接埠**輸入欄位，指定發佈點上供用戶端裝置使用的連接埠。預設情況下使用連接埠 13295。

   若要在擔任推送伺服器的發佈點與受管理裝置之間建立連線，您必須手動將指定的推送伺服器連接埠新增至 Microsoft Windows 防火牆排除清單。

6. 點擊**確定**離開發佈點內容視窗，然後點擊**儲存**套用變更。

   在您啟用**執行推入伺服器**選項後，擔任推送伺服器的發佈點上即會自動啟用**不斷開與管理伺服器的連線**選項。此選項會在網路代理與管理伺服器之間提早提供連線。

7. 開啟網路代理政策設定視窗。

8. 前往**連線 → 網路**，然後啟用**Use distribution point to force connection to the Administration Server**選項。對該選項關閉鎖定。

9. 另外在**網路**子區段，您可以停用**使用 UDP 連接埠**選項。設定的推送伺服器即會在受管理裝置與管理伺服器之間持續提供連線，而非透過 UDP 連接埠傳送封包。

10. 點擊**確定**按鈕以離開視窗。

該發佈點將開始作為 KSN 代理伺服器。它現在可以向用戶端裝置傳送推送通知。

使用"不要中斷與管理伺服器的連線"選項在受管理裝置和管理伺服器之間提供持續連線

如果您不使用推送伺服器，則卡巴斯基安全管理中心雲端主控台不會在受管理裝置與管理伺服器之間持續提供連線。受管理裝置上的網路代理定期建立連線並與管理伺服器同步。這些同步工作階段相隔的間隔是定義在網路代理政策中。如果需要提早同步，則管理伺服器（或發佈點，如有使用）會透過 IPv4 或 IPv6 網路，將經簽署的網路封包傳送到網路代理的 UDP 連接埠。預設情況下，埠號指定為 15000。如果在管理伺服器和受管理裝置之間無法建立 UDP 連線，同步將在下次網路代理和管理伺服器一般連線時在同步間隔內執行。

如果沒有網路代理和管理伺服器之間的提前連線，某些操作將無法執行，例如執行和停止本機工作、接收受管理應用程式的統計資訊或建立隧道。若要解決這個問題但您未在使用推送伺服器，可以使用**不斷開與管理伺服器的連線**選項，確保受管理裝置和管理伺服器之間會持續連線。

要提供受管理裝置與管理伺服器之間的持續連線：

1. 執行以下操作之一：

   - 如果受管理裝置直接（即不透過發佈點）存取管理伺服器：

     a. 在主功能表中，轉至 **裝置 → 受管理裝置**。

     b. 點擊您想要維持持續連線的裝置名稱。
     受管理裝置的內容視窗即會開啟。

   - 如果受管理裝置透過在閘道模式下執行的發佈點存取管理伺服器（不是直接）：

     a. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
     管理伺服器內容視窗將開啟。

     b. 在**一般**頁籤，選取**發佈點**區段。

     c. 在發佈點清單中，點擊所需發佈點的名稱。
     所選發佈點的內容視窗即會開啟。

2. 在所開啟內容視窗的**一般**區段中，選取**不斷開與管理伺服器的連線**選項。

持續連線會在受管理裝置和管理伺服器之間建立。

不斷開與管理伺服器的連線選項所能選取的最大裝置總數是 300。

建立管理群組

一開始，管理群組階層僅會包含名為**受管理裝置**的管理群組。您在建立管理群組階層時，可以將裝置和虛擬機器新增到**受管理裝置**節點和子群組中。對於每個管理群組，內容視窗會包含與群組相關之政策、工作與裝置的資訊。

要建立管理群組，請執行以下操作：

1. 在主功能表中，轉至 **資產（裝置）→ 群組的階層**。
2. 選取您要建立新子群組的管理群組旁邊的核取方塊。
3. 點擊**新增**按鈕。
4. 輸入新管理群組的名稱。
5. 點擊**新增**按鈕。

具有所指定名稱的新管理群組即會顯示在管理群組階層中。

應用程式可讓您根據 Active Directory 的結構或網域的結構建立管理群組階層。您也可以從文字檔案建立群組架構。

要建立管理群組的架構：

1. 在主功能表中，轉至 **資產（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。

建立裝置移動規則

您可以設定裝置移動規則，即自動分配裝置到管理群組的規則。

要建立移動規則：

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

- **規則名稱**

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

- **管理群組**

  選取要自動移動裝置的管理群組。

- **啟動的規則**

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

- **僅移動不屬於任何管理群組的裝置**

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

- **套用規則**

  您可以選取以下選項之一：
  - **對每台裝置執行一次**
    規則對比對標準的每台裝置套用一次。
  - **對每台裝置執行一次，然後在每次網路代理重新安裝時執行**
    規則對比對標準的每台裝置套用一次，然後僅在網路代理被重新安裝到這些裝置時。
  - **持續套用規則**
    規則根據管理伺服器自動設定的排程被套用（通常每幾個小時）。

4. 在**規則條件**頁簽上，指定至少一個標準，裝置將根據該標準被移至管理群組。
5. 點擊**儲存**。

移動規則被建立。它顯示在移動規則清單。

位置在清單中越高，規則的優先順序越高。要提高或降低移動規則的優先順序，請使用滑鼠分別在清單中向上或向下移動規則。

如果裝置內容滿足多個規則的條件，裝置被移動到具有高優先順序的規則的目的群組。

複製裝置移動規則

您可以複製移動規則，例如，如果您要對不同目標管理群組擁有幾個相同規則。

要複製現有移動規則：

1. 執行以下操作之一：
   - 在主功能表中，轉至 **資產（裝置）→ 移動規則**。
   - 在主功能表中，轉至 **發現和佈署 → 佈署和分配 → 移動規則**。

   移動規則清單被顯示。
2. 選取您要複製的規則旁邊的核取方塊。
3. 點擊**複製**。
4. 在開啟的視窗中，變更在**一般**頁籤的以下資訊，若您緊要複製規則而不改變其設定，請不要進行任何變更：

- **規則名稱**

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

- **管理群組**

  選取要自動移動裝置的管理群組。

- **啟動的規則**

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

- **僅移動不屬於任何管理群組的裝置**

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

- **套用規則**

  您可以選取以下選項之一：
  - **對每台裝置執行一次**
    規則對比對標準的每台裝置套用一次。
  - **對每台裝置執行一次，然後在每次網路代理重新安裝時執行**
    規則對比對標準的每台裝置套用一次，然後僅在網路代理被重新安裝到這些裝置時。
  - **持續套用規則**
    規則根據管理伺服器自動設定的排程被套用（通常每幾個小時）。

5. 在**規則條件**頁簽上，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。

將裝置手動新增至管理群組

您可用下列方式將裝置自動移至管理群組：建立裝置移動規則、手動將裝置從某一管理群組移至另一個，或將裝置新增至選取的管理群組。下節說明如何手動將裝置新增至管理群組。

新增一或多個裝置至選取的管理群組：

1. 在主功能表中，轉至 **資產（裝置）→ 受管理裝置**。

2. 按一下清單上方的**目前路徑：<current path>** 連結。

3. 在開啟的視窗中，選取您要向其新增裝置的管理群組。

4. 點擊**新增裝置**按鈕。
   行動裝置精靈啟動。

5. 列出您希望新增裝置的管理群組。

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

   選取您希望將裝置新增至清單的方式：

   - 點擊**新增裝置**按鈕，接著以下列其中一種方式指定裝置：
     - 從管理伺服器偵測到的裝置清單中選取該裝置。
     - 指定裝置 IP 位址或 IP 範圍。
     - 指定裝置 NetBIOS 名稱或 DNS 名稱。

       > 裝置名稱欄位不得包含空格、退格鍵，以及以下禁用字元：:,\/*'“;:&`~!@#$^()=+[]{}|<>%

   - 點擊**從檔案匯入裝置**按鈕以從 .txt 檔案匯入裝置清單。各裝置位址或名稱均需在獨立的資料行中指定。

     > 檔案不得包含空格、退格鍵，以及以下停用字元：:,\/*'“;:&`~!@#$^()=+[]{}|<>%

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。

將裝置或者叢集手動移動至管理群組

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

您還可以將叢集或伺服器陣列從一個管理群組移動到另一個管理群組。當您將叢集或伺服器陣列移動到另一個群組時，其所有節點都會隨之移動，因為叢集及其任何節點始終屬於同一管理群組。當您在**裝置**頁簽上選擇單個叢集節點時，**移至群組**按鈕將變得不可用。

要把一台或多台裝置或者叢集移動至一個選定的管理群組中，請執行以下操作：

1. 從您要移動裝置的位置開啟管理群組。要這麼做，請執行以下操作之一：

   - 若要開啟管理群組，請依序前往主功能表和**資產（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，請在主功能表中前往**發現和佈署 → 未配置的裝置**。

2. 如果管理群組包含叢集或伺服器陣列，則**受管理裝置**部分將分為兩個頁簽：**裝置**頁簽以及**叢集和伺服器陣列**頁簽。開啟要移動的物件的頁簽。

3. 選取您要移至不同群組之裝置或者叢集旁的核取方塊。

4. 點擊**移至群組**按鈕。

5. 在管理群組階層中，選取您要將選取的裝置或者叢集移至管理群組旁的核取方塊。

6. 點擊**移動**按鈕。

選取的裝置或者叢集會移至選取的管理群組。

為未配置的裝置配置保留規則

Windows 網路輪詢完成後，發現的裝置被放置到"未配置的裝置"管理群組的子群組。該管理群組可以在**發現和佈署 → 發現 → Windows 網域**中取得。**Windows 網域**資料夾是父群組。它包含以對應網域為名稱的子群組和在輪詢過程中發現的工作群組。父群組可能也包含行動裝置管理群組。您可以為父群組和每個子群組配置未配置的裝置的保留規則。保留規則不取決於裝置發現設定並在裝置發現被停用時也工作。

裝置保留規則不會影響具有一個或多個使用完整磁碟加密進行加密的磁碟機的裝置。此類裝置不會被自動刪除——您只能手動刪除它們。如果您需要刪除帶有加密磁碟機的裝置，請先解密磁碟機，然後再刪除該裝置。

要為未配置的裝置設定保留規則：

1. 在主功能表中，轉至 **發現和佈署 → 發現 → Windows 網域**。

2. 執行以下操作之一：

   - 要配置父群組的設定，請點擊**內容**按鈕。

     Windows 網域內容視窗將開啟。

   - 要配置子群組設定，點擊其名稱。

     子群組內容視窗將開啟。

3. 定義下列設定：

   - **若裝置未活動超過下列天數，則從群組刪除裝置**

     如果啟用該選項，您可以指定從組中自動移除裝置的時間間隔。預設下，該選項也被分發到子群組。預設時間間隔為 7 天。

     預設情況下已啟用該選項。

   - **從父群組繼承**

如果啟用該選項，裝置在目前群組的保留期從父群組繼承且無法被變更。
該選項僅對子群組可用。
預設情況下已啟用該選項。

- **強制子群組繼承**

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

4. 點擊**同意**按鈕。

您的變更已儲存並套用。

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

在開始之前，請先確認您已完成卡巴斯基安全管理中心雲端主控台初始化設定情境，包括快速啟動精靈。

當快速啟動精靈執行時，**受管理裝置**管理群組中會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
- 弱點掃描和所需更新（網路代理的工作）

階段

設定要以階段進行的網路防護：

1. **設定和傳播 Kaspersky 應用程式政策和政策設定檔**

   若要為受管理裝置上安裝的 Kaspersky 應用程式建立並傳播設定，您有兩種不同的安全管理方法可用，即：裝置導向式以及使用者導向式安全管理。您也可以這兩種方法並用。

2. **配置工作以遠端管理 Kaspersky 應用程式**

   檢查使用快速啟動精靈建立的工作並調整它們，如有必要。

   說明：

   - 為 Kaspersky Endpoint Security 設定群組工作
   - 建立*Find vulnerabilities and required updates*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。

   操作說明：設定事件最大數量。

結果

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

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

當網路防護配置完成時，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。您也可在 Active Directory 根據裝置使用量或其硬體規格來區分裝置。

以使用者為中心的安全性管理可讓您套用不同安全應用程式設定至不同的使用者角色。您可建立一些使用者角色，將適當的使用者角色指派給每位使用者，並將不同的應用程式設定定義至不同角色使用者擁有的裝置。例如，您可能要應用不同的應用程式設定到會計和人力資源 (HR) 人員的裝置。結果，當實現了以使用者為中心的安全管理時，每個部門—財務部門和人事部門—具有自己的 Kaspersky 應用程式設定配置。設定配置定義了哪些應用程式設定可以被使用者變更以及哪些被強制設定並被管理員鎖定。

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

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

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

政策設定和傳播：以裝置為中心的方法

本節提供了以裝置導向式方法，以集中化方式對受管理裝置上安裝的 Kaspersky 應用程式進行設定的情境。當您完成該情境後，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。

除了裝置導向式方法，您還可以考慮改用或加用使用者導向式安全管理情境。

處理程序

以裝置為中心的 Kaspersky 應用程式管理情境包含以下步驟：

1. **管理應用程式政策**

   透過為每個應用程式建立政策來配置安裝在受管理裝置上的 Kaspersky 應用程式設定。政策集將被傳播到用戶端裝置。

   當您在快速啟動精靈中設定對您網路的防護時，卡巴斯基安全管理中心雲端主控台會為 Kaspersky Endpoint Security for Windows 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。請直接手動設定 Kaspersky Endpoint Security 政策。

   如果您擁有由多個管理群組組成的階層結構，則子管理群組預設會繼承主管理伺服器的政策。您可以透過強制子群組繼承設定，禁止上游政策中所做的設定遭到任何修改。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。剩餘未鎖定的設定則可在下游政策中受到修改。建立的政策層級將允許您有效管理管理群組中的裝置。

   說明：建立一個政策

2. **建立政策設定檔（可選）**

   如果您想讓單一管理群組中的裝置在不同政策設定下執行，為這些裝置建立政策設定檔。政策設定檔是政策設定的命名子集。子集會連同政策一起分發至目標裝置，並根據名為*設定檔啟動條件*的特別條件來作為輔助政策。設定檔僅包含與「基本」政策不同的設定，並在受管理裝置上活動。

   透過使用設定檔啟動條件您可以應用不同的政策設定檔，例如，到特定單元中的裝置或到 Active Directory 安全群組，具有特別硬體設定或被特別標籤標記。使用標籤篩選滿足特別標準的裝置。例如，您可以建立叫做 *Windows* 的標籤，使用該標籤標記所有執行 Windows 作業系統的裝置，然後指定該標籤作為政策設定檔啟動條件。結果，安裝在所有 Windows 裝置上的 Kaspersky 應用程式將被使用它們自己的政策設定檔管理。

   說明：

   - 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**

   卡巴斯基安全管理中心雲端主控台每小時都會自動讓管理伺服器與受管理裝置之間同步多次。同步過程中，新的或變更的政策和政策設定檔被傳播到受管理裝置。您可以避免自動同步並透過使用強制同步指令手動執行同步。一旦同步完成，政策和政策設定檔被傳送和應用到安裝的 Kaspersky 應用程式。

   您可以檢查政策和政策設定檔是否被傳送到了裝置。卡巴斯基安全管理中心雲端主控台會在裝置的內容中指定傳送日期和時間。

   說明：強制同步

結果

當以裝置為中心的情境完成時，Kaspersky 應用程式根據指定的設定被設定並透過政策層級傳播。

設定的應用程式政策和政策設定檔將被自動應用到新增到管理群組的新裝置。

政策設定和傳播：以使用者為中心的方法

該部分敘述了以使用者為中心的集中配置安裝到受管理裝置上的 Kaspersky 應用程式的方案。當您完成該情境後，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。

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。請深入瞭解這兩種管理方法。

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。

   當您以快速啟動精靈設定對您網路的防護時，卡巴斯基安全管理中心雲端主控台會為 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。請直接手動設定 Kaspersky Endpoint Security 政策。

   如果您擁有由多個管理群組組成的階層結構，則子管理群組預設會繼承主管理伺服器的政策。您可以透過強制子群組繼承設定，禁止上游政策中所做的設定遭到任何修改。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。剩餘未鎖定的設定則可在下游政策中受到修改。建立的政策層級將允許您有效管理管理群組中的裝置。

   說明：建立一個政策

2. **指定裝置所有者**

   分配受管理裝置到對應使用者。

   說明：指派使用者作為裝置所有者

3. **為您的企業定義使用者角色**

   聯想您企業的員工所做的不同工作。您必須根據他們的角色劃分所有員工。例如，您可以按照部門、專業或職位劃分他們。然後您將需要為每個群組建立使用者角色。記住，每個使用者角色將擁有其自己的政策設定檔，包含該角色特有的應用程式設定。

4. **建立使用者角色**

   為您在上一個步驟定義的每個員工群組，建立使用者角色或是使用預先定義的使用者角色。使用者角色將包含到應用程式功能的存取權限群組。

   說明：建立一個使用者角色

5. **定義每個使用者角色範圍**

   對於每個建立的使用者角色，定義使用者和/或安全群組以及管理群組。與使用者角色關聯的設定僅套用到屬於該角色使用者的裝置，以及僅在這些裝置屬於與該角色關聯的群組（包括子群組）時。

   說明：編輯使用者角色範圍

6. **建立政策設定檔**

   為您企業中的每個使用者角色建立政策設定檔。政策設定檔決定了哪些設定將被根據使用者角色套用到使用者裝置上的應用程式。

   說明：建立一個政策設定檔

7. **關聯政策設定檔與使用者角色**

   關聯建立的政策設定檔與使用者角色。此後：政策設定檔對具有特定角色的使用者活動。政策設定檔中配置的設定將被套用到安裝於使用者裝置上的 Kaspersky 應用程式。

   說明：關聯政策設定檔到角色

8. **傳播政策和政策設定檔到受管理裝置**

   卡巴斯基安全管理中心雲端主控台每小時都會自動讓管理伺服器與受管理裝置之間同步多次。同步過程中，新的或變更的政策和政策設定檔被傳播到受管理裝置。您可以避免自動同步並透過使用強制同步指令手動執行同步。一旦同步完成，政策和政策設定檔被傳送和應用到安裝的 Kaspersky 應用程式。

   您可以檢查政策和政策設定檔是否被傳送到了裝置。卡巴斯基安全管理中心雲端主控台會在裝置的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 政策的手動設定

本節提供有關如何設定 Kaspersky Endpoint Security 政策的建議。您可以在政策內容視窗中執行設定。編輯設定時，請按一下相關設定群組右側的鎖定圖示，將指定的值套用到工作站。

設定卡巴斯基安全網路

卡巴斯基安全網路 (KSN) 是雲端服務的基礎架構，包含檔案、網路資源與軟體的信譽資訊。卡巴斯基安全網路讓 Kaspersky Endpoint Security for Windows 能更快回應不同類型的威脅，增強防護元件的效能，並降低誤報的可能性。如需有關卡巴斯基安全網路的更多資訊，請參閱 Kaspersky Endpoint Security for Windows 說明。

您可以在 Kaspersky Endpoint Security for Windows 的政策內容視窗中，於**應用程式設定 → 進階威脅防護**區段設定讓卡巴斯基安全網路運作。

要指定建議的 KSN 設定：

1. 在主功能表中，轉至 **資產（裝置） → 政策和設定檔**。
2. 按一下 Kaspersky Endpoint Security for Windows 的政策。
   所選政策的內容視窗開啟。
3. 在政策內容中，前往**應用程式設定 → 進階威脅防護 → 卡巴斯基安全網路**。
4. 確保**使用管理伺服器作為 KSN 代理伺服器**選項已啟用。使用該功能有助於重新分發和最佳化網路流量。

   如果您使用Managed Detection and Response，您必須為發佈點啟用**KSN 代理**選項並啟用延伸 KSN 模式。

5. [可選] 如果 KSN 代理服務不可用，啟用對 KSN 伺服器的使用。若要如此做，請啟用**當 KSN 代理伺服器不可用時使用卡巴斯基安全網路伺服器**選項。
   KSN 伺服器可能位於 Kaspersky 端（當 KSN 被使用）或協力廠商端（當 KPSN 被使用）。
6. 點擊**確定**。

建議的 KSN 設定被指定。

檢查受防火牆保護的網路清單

確保 Kaspersky Endpoint Security for Windows 防火牆防護您的所有網路。預設情況下，防火牆防護具有以下連線類型的網路：

- **公用網路**。病毒防護應用程式、防火牆或過濾器不防護此類網路中的裝置。
- **本機網路**。限制此網路中的裝置存取檔案和印表機。
- **受信任的網路**。此類網路中的裝置受到防護，可防止攻擊以及未經授權的檔案和資料存取。

如果您配置了自訂網路，請確保防火牆會防護這個網路。為此，請檢查 Kaspersky Endpoint Security for Windows 政策內容中的網路清單。該清單可能不包含所有網路。

如需有關防火牆的詳細資訊，請參閱 Kaspersky Endpoint Security for Windows 說明。

要檢視網路清單：

1. 在主功能表中，轉至 **資產（裝置）→ 政策和設定檔**。
2. 按一下 Kaspersky Endpoint Security for Windows 的政策。
   所選政策的內容視窗開啟。
3. 在政策內容中，前往**應用程式設定 → 關鍵威脅防護 → 防火牆**。
4. 在**可用網路**下面，按一下**網路設定**連結。
   網路連線視窗將開啟。該視窗顯示網路清單。
5. 如果清單有缺少的網路，請新增它。

從管理伺服器記憶體中排除軟體詳細資訊

我們建議管理伺服器不要儲存有關在網路裝置上啟動的軟體模組資訊。如此，管理伺服器記憶體才不會過度執行。

您可以在 Kaspersky Endpoint Security for Windows 政策內容中停用對此資訊的儲存。

要停用對已安裝軟體模組資訊的儲存：

1. 在主功能表中，轉至 **資產（裝置）→ 政策和設定檔**。
2. 按一下 Kaspersky Endpoint Security for Windows 的政策。
   所選政策的內容視窗開啟。
3. 在政策內容中，前往**應用程式設定 → 一般設定 → 報告與儲存**。
4. 在**到管理伺服器的資料傳輸**下，停用在頂級政策中仍然被啟用的**關於啟動的應用程式**核取方塊。
   當選中該核取方塊時：如果選中此核取方塊，管理伺服器資料庫儲存網路裝置上所有軟體模組的所有版本資訊。這些資訊可能會佔用卡巴斯基安全管理中心雲端主控台資料庫中的大量磁碟空間（數十 GB）。

   已安裝軟體模組的資訊不被儲存到管理伺服器資料庫。

在管理伺服器資料庫中儲存重要的政策事件

為了避免管理伺服器資料溢出，我們建議您僅儲存重要事件到資料庫。

要配置註冊重要事件到管理伺服器資料庫：

1. 在主功能表中，轉至 **資產（裝置）→ 政策和設定檔**。
2. 按一下 Kaspersky Endpoint Security for Windows 的政策。
   所選政策的內容視窗開啟。
3. 在政策內容中，開啟**事件配置**頁籤。
4. 在**緊急**區段，點擊**新增事件**並僅選取以下事件旁的核取方塊：
   - *最終使用者產品授權協議被違反*
   - *應用程式自動執行被停用*
   - *啟動錯誤*
   - *偵測到活動威脅。應該啟動進階解毒*
   - *不可能解毒*
   - *偵測到先前開啟的危險連結*
   - *禁止已終止*
   - *網路活動被封鎖*
   - *偵測到網路攻擊*
   - *應用程式啟動被禁止*
   - *存取被拒絕（本機基準）*
   - *存取被拒絕 (KSN)*
   - *本機更新錯誤*
   - *無法同時啟動兩個工作*
   - *與卡巴斯基安全管理中心互動錯誤*
   - *未更新所有元件*
   - *套用檔案加密/解密規則錯誤*
   - *啟用便攜模式錯誤*
   - *停用便攜模式錯誤*

- *無法載入加密模組*
- *政策無法被套用*
- *變更應用程式元件時出錯*

5. 點擊**確定**。
6. 在**功能失效**區段，點擊**新增事件**並僅選取事件*有效工作設定旁的核取方塊。設定未套用。*
7. 點擊**確定**。
8. 在**警告**區段，點擊**新增事件**並僅選取以下事件旁的核取方塊：
   - *自我防護已停用*
   - *防護元件已停用*
   - *不正確的備用金鑰*
   - *偵測到可以被侵入者用於損害您的電腦或個人資料的合法軟體（本機基準）*
   - *偵測到可以被侵入者用於損害您的電腦或個人資料的合法軟體 (KSN)*
   - *物件已刪除*
   - *物件已解毒*
   - *使用者已退出加密政策*
   - *檔案已由管理員從 Kaspersky Anti Targeted Attack Platform 伺服器上的隔離區還原*
   - *檔案被管理員隔離在 Kaspersky Anti Targeted Attack Platform 伺服器上*
   - *向管理員傳送的有關應用程式啟動禁止的訊息*
   - *向管理員傳送的有關裝置存取禁止的訊息*
   - *向管理員傳送的有關網頁存取禁止的訊息*
9. 點擊**確定**。
10. 在**資訊**區段，點擊**新增事件**並僅選取以下事件旁的核取方塊：
    - *物件備份副本被建立*
    - *應用程式啟動在測試模式中被禁止*
11. 點擊**確定**。

註冊重要事件到管理伺服器資料庫被配置。

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

Kaspersky Endpoint Security 的最佳化和建議排程選項是**當新更新下載至儲存區時**時，當**使用工作啟動自動隨機延遲**核取方塊被選中時。

工作

本節說明卡巴斯基安全管理中心雲端主控台使用的工作。

關於工作

卡巴斯基安全管理中心雲端主控台是透過建立和執行工作來管理裝置上安裝的 Kaspersky 應用程式。無論是安裝、啟動及停止應用程式、掃描檔案、更新資料庫和軟體模組，還是對應用程式執行其他操作，均需要透過*工作*來完成。工作可以在管理伺服器和裝置上執行。

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。

  本機工作可由管理員使用管理工具修改，或是由遠端裝置的使用者透過安全應用程式介面之類的方式修改。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。

- *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。

對於每個應用程式，您都可以建立多個群組工作、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。

工作的執行結果會儲存在每個裝置上的作業系統事件記錄中以及管理伺服器資料庫中。

請勿在工作設定中包含私密資料。例如，避免指定網域管理員密碼。

關於工作範圍

*工作範圍*是執行工作的裝置集合。範圍的類型包括以下：

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

當建立*全域工作*時，您可以使用以下方法指定範圍：

- 手動指定特定裝置。

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

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

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

- 指定裝置分類。

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

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

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

建立工作

您可以在工作清單中建立工作；或在**受管理裝置**清單中選擇裝置，然後建立分配給所選裝置的新工作。

在工作清單中建立工作：

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

   新工作精靈啟動。遵循其說明。

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

工作被建立並顯示在工作清單。

若要建立分配給所選裝置的新工作：

在主功能表中，轉至 **資產（裝置）→受管理裝置**。

受管理裝置清單隨即顯示。

1. 在受管理裝置清單中，選取裝置旁的核取方塊以為其執行工作。您可以使用搜尋和過濾功能來查找您正在尋找的裝置。
2. 點擊**執行工作**按鈕，然後選擇**建立新工作**。

   新工作精靈啟動。

   在精靈的第一步中，您可以刪除被選擇包含在工作範圍中的裝置。請按照精靈的步驟進行操作。

3. 點擊**完成**按鈕。

該工作是為選定的裝置建立的。

檢視工作清單

您可檢視在卡巴斯基安全管理中心雲端主控台中建立之工作的清單。

若要檢視工作清單，

在主功能表中，轉至 **資產（裝置）→工作**。

工作清單隨即顯示。工作會依與應用程式名稱的關聯來分組。例如，遠端解除安裝應用程式工作會與管理伺服器相關，弱點掃描和所需更新工作則與網路代理相關。

若要檢視工作內容，

請按一下工作的名稱。

工作內容視窗會一起顯示數個命名的頁籤。例如，**工作類型**會顯示在**一般**頁籤，以及工作排程—位於**排程**頁籤。

手動啟動工作

該應用程式會根據在各工作內容中指定的排程設定啟動工作。您可以隨時從工作清單手動啟動工作；或在**受管理裝置**清單中選擇裝置，然後為其啟動現有工作。

若要手動啟動工作：

1. 在主功能表中，轉至 **資產（裝置）→工作**。
2. 在工作清單中，請選取您要啟動之工作旁的核取方塊。
3. 點擊**"開始"**按鈕。

工作啟動。您可在**狀態**欄中檢視工作狀態或點擊**結果**按鈕。

為選取的裝置啟動工作

您可以在裝置清單中選擇一台或多台用戶端裝置，然後啟動先前為它們建立的工作。這可讓您執行先前為一組特定裝置建立的工作。

這會將工作被指派到的裝置變更到您在執行工作時選擇的裝置清單。

為選取的裝置啟動工作：

1. 在主功能表中，轉至 **資產（裝置）→受管理裝置**。受管理裝置清單隨即顯示。

在受管理裝置清單中，使用核取方塊選擇要為其執行工作的裝置。您可以使用搜尋和過濾功能來查找您正在尋找的裝置。

1. 按一下**執行工作**按鈕，然後選擇**套用現有工作**。

   現有工作清單隨即顯示。

2. 所選裝置顯示在工作清單上方。如有必要，您可以從此清單中刪除裝置。您可以刪除除一台裝置之外的所有裝置。

3. 在清單中選擇所需的工作。您可以使用清單上方的搜尋框按名稱搜尋所需的工作。只能選擇一項工作。

4. 按一下**儲存並啟動工作**。

所選工作將立即為所選裝置啟動。工作中的排程啟動設定不會變更。

一般工作設定與內容

此區段包含您可檢視與為大多數工作配置的清單。可用設定清單取決於您正在配置的工作。

工作建立過程中指定的設定

您可以在建立工作時指定以下設定。一些設定也可以在所建立工作的內容中修改。

- 要分配工作的裝置：
  - **分配工作到管理群組**

    工作被分配到包含在管理群組中的裝置。您可以指定其中一個現有群組或者建立新群組。

    例如，您可能要使用該選項執行傳送訊息到使用者工作，如果訊息針對包含在特定管理群組中的裝置。

  - **手動指定裝置位址或從清單匯入位址**

    工作被分配到指定裝置。您可以透過以下其中一種方法指定裝置：

    - 指定裝置的 IP 位址、NetBIOS 名稱或 DNS 名稱。
    - 指定 IP 範圍。

      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。
    - 選取管理伺服器偵測到的裝置，包括未指派的裝置。

      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。

  - **分配工作到裝置分類**

該工作被分配到裝置選項中的裝置。您可以指定其中一個現有選項。

例如，您可能要使用該選項在特定作業系統版本的裝置上執行工作。

- 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。

- 作業系統重新啟動設定：
  - **不重新啟動**

    用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

  - **重新啟動裝置**

    如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

  - **提示使用者操作**

    用戶端裝置螢幕上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。該選項適用於使用者必須可以選取最方便的時間進行重新啟動的工作站。

    預設情況下已選定此選項。

  - **重複提示間隔（分鐘）**

    如果啟用該選項，應用程式以指定頻率提示使用者重新啟動作業系統。

    預設情況下已啟用該選項。預設間隔是 5 分鐘。可用值介於 1 和 1440 分鐘之間。

    如果停用該選項，提示僅顯示一次。

  - **在該時間後重新啟動（分鐘）**

    提示使用者之後，應用程式在指定時間間隔後強制作業系統重新啟動。

    預設情況下已啟用該選項。預設延時是 30 分鐘。可用值介於 1 和 1440 分鐘之間。

- **強制關閉被封鎖工作階段中的應用程式**

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

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

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

  預設情況下已停用該選項。

工作建立後指定的設定

您可以在建立工作後指定以下設定。

- 群組工作設定：
  - **分發到子群組**

    此選項僅在群組工作的設定中可用。

    啟用此選項時，工作範圍包括：
    - 您在建立工作時選擇的管理群組。
    - 依據群組階層，所選管理群組底下任何層級的管理群組。

    停用此選項時，工作範圍僅包括您在建立工作時選擇的管理群組。

    預設情況下已啟用該選項。

  - **分發到從屬和虛擬管理伺服器**

    啟用此選項時，在主管理伺服器上有效的工作也將套用於從屬管理伺服器（包括虛擬伺服器）。如果從屬管理伺服器上已經存在相同類型的工作，則這兩個工作都將套用到從屬管理伺服器上 — 現有的工作和從主管理伺服器繼承的工作。

    此選項僅在**分發到子群組**選項已啟用的情況下可用。

    預設情況下已停用該選項。

- 工作排程設定：
  - **排程開始設定：**
    - **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 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。此排程是為了讓卡巴斯基安全管理中心雲端主控台與舊版系統相容而存在。

  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.。

- **當新更新下載至儲存區時**

  當有新的更新下載到發佈點儲存區時，卡巴斯基安全管理中心雲端主控台會執行所有設有此排程的工作。網路代理會在受管理裝置與管理伺服器之間進行定期同步（又稱心跳）時，檢查是否有更新。

  例如，您可能會想對與安全應用程式（例如 Kaspersky Endpoint Security）相關的更新工作使用此排程。

  如果受管理裝置上的網路代理連續 25 小時以上未偵測到新更新，則卡巴斯基安全管理中心雲端主控台會在該裝置上執行所有設有此排程的工作。這些工作會每小時執行一次，直到偵測到新的更新為止。如果受管理裝置與負責將更新下載到儲存區的發佈點之間沒有連線，則卡巴斯基安全管理中心雲端主控台亦會每小時執行這些工作一次。

- **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選項。

- **在完成其它工作時**

  目前工作在其他工作完成後啟動。您可以選取先前工作如何結束（成功或帶有錯誤）以觸發目前工作的啟動。例如，您可能想使用***Turn on the device***選項執行開啟裝置工作，完成後，請執行*惡意軟體掃描*工作。只有當這兩項工作都被分配給相同的裝置時，此參數才會有作用。

- **執行錯過的工作**

  該選項決定在工作要啟動時用戶端裝置在網路中不可見時工作的行為。

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

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

- **透過使用 Wake-On-LAN 功能在啟動工作之前開啟裝置（分鐘）**

  裝置上的作業系統在工作開始之前的指定時間啟動。預設時間段為五分鐘。

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

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

  預設情況下已停用該選項。

- **完成工作後關閉裝置**

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

  預設情況下已停用該選項。

- **停止工作，若時間超過（分鐘）**

  在指定時間段過後，工作被自動停止，無論它是否完成。

  如果您想要中斷或停止執行時間太長的工作，則啟用該選項。

  預設情況下已停用該選項。預設工作執行時間是 120 分鐘。

- 通知：
  - **儲存工作歷程記錄**塊:
    - **儲存所有事件**
    - **儲存工作進度相關事件**
    - **僅儲存工作執行結果**
    - **儲存在管理伺服器資料庫上（天）**

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

預設情況下已啟用該選項。

- **儲存在裝置的作業系統事件記錄中**

  有關工作執行的應用程式事件被儲存在每個用戶端裝置的本機 Windows 事件記錄中。

  預設情況下已停用該選項。

- **僅通知錯誤**
- **透過郵件通知**

- 工作範圍設定：
- **範圍外的排除項目**

  您可以指定套用工作的裝置群組。要排除的群組僅可以是套用工作的管理群組的子群組。

- **變更歷程**

匯出工作

卡巴斯基安全管理中心雲端主控台可讓您將工作及其設定儲存到 KLT 檔案。您可以使用此 KLT 檔案匯入儲存的工作到 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux。

要匯出工作，請執行以下操作：

1. 在主功能表中，轉至 **資產（裝置）→工作**。
2. 選取您要匯出之工作旁邊的核取方塊。

   您不能同時匯出多個工作。如果您選擇了多個工作，**匯出**按鈕將被停用。此外，管理伺服器工作也不供匯出。
3. 點擊**匯出**按鈕。
4. 在開啟的**另存新檔**視窗中，指定工作檔案的名稱和路徑。按一下**儲存**按鈕。

   另存新檔視窗僅當您使用 Google Chrome、Microsoft Edge 或 Opera 時才會顯示。如果您使用其他瀏覽器，工作檔案會自動儲存在**下載**資料夾。

匯入工作

卡巴斯基安全管理中心雲端主控台可讓您從 KLT 檔案匯入工作。KLT 檔案包含匯出工作及其設定。

要匯入工作，請執行以下操作：

1. 在主功能表中，轉至 **資產（裝置）→工作**。
2. 點擊**匯入**按鈕。
3. 點擊**瀏覽**按鈕選擇要匯入的工作檔案。
4. 在開啟的視窗中，指定 KLT 工作檔案的路徑，然後按一下**開啟**按鈕。請注意，您只能選擇一個工作檔案。
   工作處理開始。
5. 工作處理成功後，選擇要將工作分配到哪些裝置。如要這麼做，請選擇以下選項之一：

   - **分配工作到管理群組**

     工作被分配到包含在管理群組中的裝置。您可以指定其中一個現有群組或者建立新群組。
     例如，您可能要使用該選項執行傳送訊息到使用者工作，如果訊息針對包含在特定管理群組中的裝置。

   - **手動指定裝置位址或從清單匯入位址**

     您可以指定您要為其分配工作的裝置的 NetBIOS 名稱、DNS 名稱、IP 位址和 IP 子網路。
     您可能要使用該選項以對特定子網路執行工作。例如，您可能要安裝特定應用程式到會計裝置，或者掃描疑似被感染子網路中的裝置。

   - **分配工作到裝置分類**

     該工作被分配到裝置選項中的裝置。您可以指定其中一個現有選項。
     例如，您可能要使用該選項在特定作業系統版本的裝置上執行工作。

6. 指定工作範圍。
7. 點擊**完成**按鈕以完成工作匯入。

此時會顯示匯入結果通知。如果工作匯入成功，您可以按一下**詳細資訊**連結以檢視工作內容。

匯入成功後，工作會顯示在工作清單中。工作設定和排程也會一起匯入。工作將根據其排程來啟動。

如果新匯入的工作與現有工作的名稱相同，則匯入工作的名稱將加上 **(<next sequence number>)** 索引，例如：**(1)**、**(2)**。

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

要檢視受管理裝置設定：

1. 在主功能表中，轉至 **資產（裝置）→ 受管理裝置**。
   受管理裝置清單隨即顯示。
2. 在受管理裝置清單中，按一下有所需裝置名稱的連結。

   所選裝置的屬性視窗隨即顯示。

以下分頁顯示在屬性視窗的上部，代表主設定群組：

- **一般**

此分頁包含以下區段：

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

    在該欄位中，您可以檢視和修改管理群組中的用戶端裝置名稱。

  - **敘述**

    在該欄位中，您可以輸入用戶端裝置的附加敘述。

  - **裝置狀態**

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

  - **裝置所有者**

    裝置擁有者的名稱。作為裝置擁有者，您可以點擊**管理裝置所有者**連接來分配或刪除使用者。

  - **完整的群組名稱**

    包括了用戶端裝置的管理群組。

  - **上次病毒資料庫更新**

    裝置上病毒資料庫或應用程式最後更新日期。

  - **連線至管理伺服器**

    裝置上的網路代理上一次連線到管理伺服器的日期和時間。

  - **上一次可見**

    裝置在網路中最後可見的日期和時間。

  - **網路代理版本**

    安裝的網路代理的版本。

  - **已建立**

    在 Kaspersky Security Center Cloud Console 中建立裝置的日期。

- **不斷開與管理伺服器的連線**

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

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

  不斷開與管理伺服器的連線選項所能選取的最大裝置總數是 300。

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

- **網路**區段會顯示有關用戶端裝置網路屬性的以下資訊：
  - **IP 位址**

    裝置 IP 位址。

  - **Windows 網域**

    包含裝置的 Windows 網域或工作群組。

  - **DNS 名稱**

    用戶端裝置的 DNS 網域名稱。

  - **NetBIOS 名稱**

    用戶端裝置的 Windows 網路名稱。

  - **IPv6 位址**
- **系統**區段會顯示安裝在用戶端裝置上應用程式的相關資訊。
  - **作業系統**
  - **CPU 架構**
  - **作業系統生產商**
  - **作業系統資料夾**
  - **裝置名稱**
  - **虛擬機類型**

    虛擬機製造商。

  - **作為 VDI 一部分的動態虛擬機**

    此行顯示用戶端裝置是否是作為 VDI 一部分的動態虛擬機。

- **作業系統版本**

- **防護**區域將提供有關用戶端裝置上病毒防護的目前狀態的一下資訊：

  - **可見**

    用戶端裝置的可見性狀態。

  - **裝置狀態**

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

  - **狀態敘述**

    用戶端裝置防護狀態和與管理伺服器的連線。

  - **防護狀態**

    該欄位顯示目前的用戶端裝置即時防護狀態。

    當裝置狀態變更時，新狀態僅在用戶端裝置與管理伺服器同步之後顯示在裝置屬性視窗。

  - **上一次完整掃描**

    用戶端裝置上執行的最後一次惡意軟體掃描的日期和時間。

  - **偵測到的病毒**

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

  - **解毒失敗的物件**

    用戶端裝置上的未處理檔案數量。

    該欄位行動裝置上的未處理檔案數量。

  - **磁碟加密狀態**

    裝置本機磁碟機上的目前檔案加密狀態。有關狀態的說明，請參閱 Kaspersky Endpoint Security for Windows 說明。

- **應用程式定義的裝置狀態**區段會提供相關資訊，說明由裝置上安裝的受管理應用程式所定義的裝置狀態。該裝置狀態可以與卡巴斯基安全管理中心雲端主控台所定義的狀態不同。

- **應用程式**

此分頁列出了用戶端裝置上安裝的所有 Kaspersky 應用程式。您可以按一下應用程式名稱以檢視有關該應用程式的一般資訊、裝置上發生的事件清單以及應用程式設定。

- **啟用政策和政策設定檔**

  此分頁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**標籤中，您可以管理用戶端工作：檢視現有工作清單、建立新工作、移除、啟動和停止工作、修改工作設定以及檢視執行結果。該工作清單會根據用戶端最近一次與管理伺服器同步的連線期間所收到的資料提供。管理伺服器向用戶端裝置請求工作狀態詳情。如果未建立連線，則不顯示狀態。

- **事件**

  事件標籤將顯示選定用戶端裝置在管理伺服器上所記錄事件的資訊。

- **安全問題**

  在**安全問題**頁籤中，您可為用戶端裝置檢視、編輯和建立安全問題。安全問題可以透過安裝在使用者端裝置上的受管理卡巴斯基應用程式自動建立，也可以由管理員手動建立。例如，如果使用者定期將惡意軟體從其卸除式磁碟機移至裝置，則管理員可以建立安全問題。管理員可以在安全問題文字中提供情況的簡要說明和建議的操作（例如對於一個使用者的紀律性操作），還可以新增連結到使用者。

  對其採用了所有必要操作的安全問題稱為*已處理安全問題*。存在的未處理安全問題可被選為將裝置的狀態變更為*緊急*或*警告*的條件。

  此部分包含已為裝置建立的安全問題的清單。安全問題按照幾個等級和類型分類。安全問題的類型是由建立安全問題的 Kaspersky 應用程式定義。選中**已處理**列中的核取方塊即可突出顯示清單上的已處理安全問題。

- **標籤**

  在**標籤**分頁，您可以編輯用來尋找用戶端裝置的關鍵字清單，並可以檢視現有標籤清單、從清單中配置標籤、設定自動標記規則、新增標籤和重新命名舊標籤以及移除標籤。

- **進階**

此分頁包含以下區段：

- **應用程式登錄資料**。在此區域，您可以檢視用戶端裝置上安裝的應用程式及其更新的登錄檔，您還可以設定應用程式登錄資料的顯示方式。

  如果用戶端裝置上安裝的網路代理將所需資訊傳送到管理伺服器，則將提供有關已安裝應用程式的資訊。您可以在網路代理或其政策的內容視窗中的**儲存區**區域，設定將資訊傳送到管理伺服器。

  按一下應用程式名稱會開啟一個視窗，其中包含應用程式詳細資訊以及為該應用程式安裝的更新軟體套件的清單。

- **可執行檔**。此區域會顯示在用戶端裝置上發現的可執行檔案。

- **發佈點**。該區域提供裝置與之互動的發佈點清單。

  - **匯出至檔案**

    按一下**匯出至檔案**按鈕儲存裝置與之互動的發佈點清單檔案。預設下，應用程式匯出裝置清單到 CSV 檔案。

  - **內容**

    按一下**屬性**按鈕檢視和配置裝置與之互動的發佈點。

- **硬體登錄資料**。在此區域，您可以檢視安裝在用戶端裝置上的硬體資訊。

- **可用更新**。該區域顯示在該裝置上發現的未安裝的軟體更新清單。

- **軟體弱點**。此區域會顯示安裝在用戶端裝置上的協力廠商應用程式的弱點資訊。

  若要將弱點儲存到檔案中，請選擇要儲存之弱點旁邊的核取方塊，然後點擊「確定」，接著點擊**匯出到 CSV**按鈕或**匯出到 TXT**按鈕。

  區段會包含以下設定：

  - **僅顯示可以被修復的弱點**

    如果啟用此選項，該區域會顯示可透過使用修補程式修復的弱點。

    如果停用此選項，該區域會同時顯示可透過使用修補程式修復的弱點，以及未發佈修補程式的弱點。

    預設情況下已啟用該選項。

  - **弱點內容**

選取清單中的軟體弱點並按一下名稱，以在個別視窗中檢視所選軟體弱點的屬性。在視窗中，您可以進行以下操作：

- 忽略該受管理裝置上的軟體弱點（在管理主控台或在卡巴斯基安全管理中心雲端主控台進行）。
- 檢視對弱點的建議修復清單。
- 手動指定軟體更新以修復弱點（在管理主控台或在卡巴斯基安全管理中心雲端主控台進行）。
- 檢視弱點實例。
- 檢視要修復弱點的現有工作清單，並建立新工作來修復弱點。

- **遠端診斷**。在本節中，您可以執行用戶端裝置的遠端診斷。

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雲端主控台提供各種*預先定義的分類*（例如，**處於"緊急"狀態的裝置**、**防護已停用**、**偵測到活動威脅**）。預先定義分類無法被刪除。您也可以建立和配置附加*使用者定義分類*。

在使用者定義分類中，您可以設定搜尋範圍並選取所有裝置、受管理裝置、或者未配置的裝置。搜尋參數在條件中指定。在裝置分類中，您可以建立帶有不同搜尋參數的多個條件。例如，您可以建立兩個條件並指定不同的 IP 範圍。如果多個條件被指定，分類顯示滿足任意條件的裝置。相比之下，條件中的搜尋參數是附加的。如果 IP 範圍和已安裝應用程式名稱都被指定在一個條件，僅安裝了應用程式且 IP 位址處於指定範圍的裝置被顯示。

從裝置分類中檢視裝置清單

卡巴斯基安全管理中心雲端主控台可讓您檢視裝置分類中的裝置清單。

從裝置分類中檢視裝置清單：

1. 在主功能表中，轉到**資產（裝置）** → **裝置分類** or **發現和佈署** → **裝置分類**區域。
2. 在選項清單中，按一下裝置分類的名稱。
   該頁面會顯示一個表格，其中包含有關裝置分類中包含的裝置的資訊。
3. 您可以按如下方式對裝置表格資料進行分組和篩選：
   - 點擊設定圖示（ ），然後選擇要在表中顯示的列。
   - 點擊篩選圖示（ ），然後在喚起的功能表中指定並套用篩選條件。
     顯示篩選後的裝置表格。

您可以在裝置分類中選擇一個或多個裝置，然後點擊**新工作**按鈕以建立將套用於這些裝置的工作。

要將裝置分類中的選定裝置移動到另一個管理群組，請點擊**移至群組**按鈕，然後選擇目標管理群組。

建立裝置分類

要建立裝置分類，請執行以下操作：

1. 在主功能表中，轉至 **資產（裝置）→ 裝置分類**。
   裝置選項清單頁面隨即顯示。
2. 點擊**新增**按鈕。
   裝置分類設定視窗開啟。
3. 輸入新選項的名稱。
4. 指定包含要包括在裝置分類中的裝置的群組：
   - **尋找任何裝置**— 搜尋符合選擇標準並被包含在**受管理裝置**或未**未配置的裝置**群組中的裝置。
   - **尋找受管理裝置** — 搜尋符合選擇標準並被包含在**受管理裝置**群組中的裝置。
   - **尋找未配置的裝置**— 搜尋符合選擇標準並被包含在**未配置的裝置**群組中的裝置。

   您可以啟用**包含次要管理伺服器的資料**核取方塊以啟用搜尋滿足選擇條件並由從屬管理伺服器管理的裝置。
5. 點擊**新增**按鈕。
6. 在開啟的視窗中，指定將裝置包括在此選項中時必須符合的條件，然後點擊**確定**按鈕。
7. 點擊**儲存**按鈕。

裝置選項已建立並新增到裝置選項清單中。

配置裝置分類

要配置裝置分類：

1. 在主功能表中，轉至 **資產（裝置）→ 裝置分類**。
   裝置選項清單頁面隨即顯示。
2. 選擇相關的使用者自定義裝置分類，然後點擊**內容**按鈕。
   裝置分類設定視窗開啟。
3. 在**一般**標籤上，點擊**新條件**連接。
4. 指定包含裝置到該分類所必須滿足的條件。
5. 點擊**儲存**按鈕。

裝置被套用並儲存。

以下是分配裝置到分類的條件敘述。多個條件使用 OR 邏輯運算子組合在一起：分類範圍將包含至少符合列出的一個條件的裝置。

一般

在**一般**區域，您可以變更分類條件的名稱，指定是否必須倒轉條件：

反轉分類條件

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。

網路基礎架構

在**網路**子區域，您可以指定依據網路資料裝置納入分類的標準：

- **裝置名稱**

  裝置的 Windows 網路名稱（NetBIOS 名稱），或者 IPv4 或 IPv6 位址。

- **網域**

  顯示指定的 Windows 網域中包括的所有裝置。

- **管理群組**

  顯示指定的管理群組中包括的裝置。

- **敘述**

裝置內容視窗中的文字：在**一般**區域的**敘述**欄位。
您可以使用以下特徵說明**敘述**欄位中的文字：

- 在單詞中：
  - *****。用任意數量的字元更換任何字串。

    例如：
    要敘述單詞 **Server** 或 **Server's**，您可以輸入 **Server***。
  - **?**。更換任意單個字元。

    例如：
    要敘述單詞 **Window** 或 **Windows**，您可以輸入 **Windo?**。
    星號 (*****) 或問號 (**?**) 不能用於查詢中的第一個字元。
- 要尋找多個單詞：
  - 空格。顯示所有在其敘述中包含列出的任何單詞的裝置。

    例如：
    要尋找在其敘述中包含**從屬**或**虛擬**單詞的短語，您可以在查詢中包含**從屬虛擬**等字。
  - **+**。當單詞帶有加號前綴時，所有搜尋結果都將包含該單詞。

    例如：
    要搜尋同時包含**從屬**和**虛擬**的短語，請輸入**+從屬+虛擬**查詢。
  - **-**。當單詞帶有減號前綴時，所有搜尋結果都不包含該單詞。

    例如：
    要尋找包含**從屬**但不包含**虛擬**的短語，請輸入**+從屬-虛擬**查詢。
  - **「<某些文字>」**。引號中圍繞的文字必須存在文字中。

    例如：
    要尋找包含**從屬伺服器**單詞群組合的短語，您可以在查詢中輸入**「從屬伺服器」**。

- **IP 範圍**

  如果啟用此選項，您可以輸入應該包括相關裝置的 IP 範圍的初始和最終 IP 位址。
  預設情況下已停用該選項。

- **由不同管理伺服器管理**

您可以選取以下值之一：

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

在**Active Directory**子區域，您可以根據 Active Directory 資料設定將裝置納入分類的標準：

- **裝置在 Active Directory 組織單元中**

  如果啟用此選項，分類將包括輸入欄位中所指定 Active Directory 組織單位中的裝置。
  預設情況下已停用該選項。

- **包括子組織單元**

  如果啟用此選項，選取範圍將包括指定 Active Directory 組織單元的所有子組織單元中的裝置。
  預設情況下已停用該選項。

- **該裝置是 Active Directory 群組成員**

  如果啟用此選項，選取範圍將包括輸入欄位中指定的 Active Directory 群組中的裝置。
  預設情況下已停用該選項。

在**網路活動**子區域，您可以根據網路活動指定將裝置納入分類的標準：

- **作為發佈點**

  在下拉清單中，可設定執行搜尋時在分類中包括裝置的標準：
  - **是**。選取範圍將包括充當發佈點的裝置。
  - **否**。分類不包含作為發佈點的裝置。
  - **未選取值**。將不套用標準。

- **不斷開與管理伺服器的連線**

  在下拉清單中，可設定執行搜尋時在分類中包括裝置的標準：
  - **已啟用**。分類將包含已選取**不斷開與管理伺服器的連線**核取方塊的裝置。
  - **已停用**。分類將包含未選取**不斷開與管理伺服器的連線**核取方塊的裝置。
  - **未選取值**。將不套用標準。

- **連線設定檔已轉換**

在下拉清單中，可設定執行搜尋時在分類中包括裝置的標準：

- **是**。該分類將包含連線設定檔轉換後連線到管理伺服器的裝置。
- **否**。該分類將不包含連線設定檔轉換後連線到管理伺服器的裝置。
- **未選取值**。將不套用標準。

- **上一次連線到管理伺服器**

  您可使用此方塊設定按上一次連線到管理伺服器的時間搜尋裝置的標準。

  如果選取該方塊，則在輸入欄位中，您可以指定在用戶端裝置上安裝的網路代理和管理伺服器之間建立上一次連線的時間間隔（日期和時間）。選取將包括位於指定間隔的裝置。

  如果清除此方塊，則將不會套用標準。

  預設情況下已清空此方塊。

- **網路輪詢時偵測到新裝置**

  搜尋最近幾天透過網路輪詢偵測到的新裝置。

  如果選取此核取方塊，分類將只包括在**偵測週期（天）**欄位中指定的天數內透過裝置發現偵測到的新裝置。

  如果停用此選項，分類將包括透過裝置發現偵測到的所有裝置。

  預設情況下已停用該選項。

- **裝置可見**

  在下拉清單中，可設定執行搜尋時在分類中包括裝置的標準：

  - **是**。程式在分類中包括網路中目前可見的裝置。
  - **否**。應用程式在分類中包括網路中目前不顯示的裝置。
  - **未選取值**。將不套用標準。

在**雲端區段**子區域中，您可以根據相關雲端區段設定將裝置納入分類的標準：

- **裝置在雲端區段中**

  如果啟用此選項，您可以從 AWS、Azure 和 Google 雲端區段中選擇裝置。

  如果也啟用了**包含子物件**選項，則搜尋會在選取區段的所有子物件上執行。

  搜尋結果僅包含所選段的裝置。

- **使用 API 發現的裝置**

在下拉清單，您可以選取裝置是否由 API 工具偵測：

- **是**。裝置使用 AWS、Azure 或 Google API 進行偵測。
- **否**。裝置無法使用 AWS、Azure 或 Google API 進行偵測。即裝置要么在雲端環境之外，要么在雲端環境中，但無法通過 API 偵測到。
- 沒有值。這項條件不適用。

裝置狀態

在**受管理裝置狀態**子區域，您可以根據受管理應用程式的裝置狀態的敘述設定將裝置納入分類的標準：

- **裝置狀態**

  在該下拉清單中，您可以選取下列裝置狀態之一：*確定*、*緊急*或 *警告*。

- **即時防護狀態**

  您可以在該下拉清單中選取即時防護狀態。具有指定即時防護狀態的裝置將被包括在選取範圍中。

- **裝置狀態敘述**

  在此欄位中，您可以選取條件旁邊的方塊，若滿足這些條件，程式會為裝置分配下列狀態之一： *確定*、*緊急*或 *警告*。

在**受管理應用程式元件的狀態**子區域中，您可以根據受管理應用程式元件狀態設定將裝置納入分類的標準：

- **資料洩漏防護狀態**

  根據資料外洩防護的狀態搜尋裝置（*裝置上無資料*, *已停止*, *正在啟動*, *已暫停*, *執行中*, *失敗*）。

- **協作伺服器防護狀態**

  根據伺服器協作防護狀態搜尋裝置（*裝置上無資料*, *已停止*、*正在啟動*、*已暫停*, *執行中*、*失敗*）。

- **郵件伺服器的病毒防護狀態**

  根據郵件伺服器防護狀態搜尋裝置（*裝置上無資料*、*已停止*、*正在啟動*、*已暫停*、*執行中*、*失敗*）。

- **端點感應器狀態**

  根據端點感應器元件狀態搜尋裝置（*裝置上無資料*、*已停止*、*正在啟動*、*已暫停*、*執行中失敗*）。

在**影響受管理應用程式狀態的問題**子區域，您可以根據由受管理應用程式偵測到的可能問題清單指定將裝置納入分類的標準。如果至少一個您選取的問題存在於裝置，裝置將被包含到分類。當您選取幾個應用程式的問題時，您可以選取在所有清單中自動選取該問題。

您可以選取受管理應用程式狀態敘述的核取方塊；接收這些狀態時，裝置將被包含在分類。當您選取幾個應用程式的狀態時，您可以選取在所有清單中自動選取該狀態。

系統詳情

在**作業系統**區域，您可以根據作業系統指定將裝置納入分類的標準。

- **平台類型**

  如果選中該方塊，您可以從清單中選取一個作業系統。安裝了指定作業系統的裝置會包含在搜尋結果中。

- **作業系統服務套件版本**

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

- **作業系統 bit 大小**

  在該下拉清單中可選取作業系統的架構，這將決定將移動規則套用到裝置（**未知**、**x86**、**AMD64** 或 **IA64**）的方式。預設情況下，不選取清單中的任何選項，這樣就不會對作業系統的架構進行定義。

- **作業系統版本**

  該設定僅套用到 Windows 作業系統。

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

- **作業系統發佈號**

  該設定僅套用到 Windows 作業系統。

  作業系統發佈 ID。您可以指定所選作業系統是否必須具有相等、更早或更晚的發佈 ID。您也可以設定對所有發佈 ID 的搜尋，除了指定的值。

在**虛擬機**區域中，您可以根據它們是否是虛擬機或虛擬桌面基礎架構 (VDI) 的一部分來指定將裝置納入分類的標準：

- **這是一台虛擬機**

在此下拉清單中，您可以選取以下選項：

- **未定義**。
- **否**。尋找不是虛擬機的裝置。
- **是**。搜尋虛擬機裝置。

- **虛擬機類型**

在該下拉清單中，您可以選取虛擬機製造商。
若在**這是一台虛擬機**下清單中選取**是**或**不重要**值，則可使用此下拉清單。

- **虛擬桌面基礎架構的一部分**

在此下拉清單中，您可以選取以下選項：

- **未定義**。
- **否**。尋找不是虛擬桌面基礎架構一部分的裝置。
- **是**。搜尋屬於虛擬桌面基礎架構 (VDI) 一部分的裝置。

在**硬體登錄資料**子區域，您可以根據所安裝的硬體設定將裝置納入分類的標準：

確保在要從中獲取硬體詳細資訊的 Linux 裝置上安裝了 lshw 公用程式。根據所使用的 hypervisor，從虛擬機獲取的硬體詳細資訊可能不完整。

- **裝置**

在該下拉清單中，您可以選取單元類型。所有帶有該單元的裝置被包含在搜尋結果。
該欄位支援完整文字搜尋。

- **供應商**

在該下拉清單中，您可以選取單元生產商的名稱。所有帶有該單元的裝置被包含在搜尋結果。
該欄位支援完整文字搜尋。

- **裝置名稱**

在 Windows 網路中的裝置名稱。具有指定名稱的裝置將包括在該分類中。

- **敘述**

裝置或硬體單元的敘述。帶有該欄位中指定的敘述的裝置將包括在分類範圍內。
可在裝置的內容視窗輸入任何格式的裝置敘述。該欄位支援完整文字搜尋。

- **裝置製造商**

  裝置製造商的名稱。被指定生產商製造的裝置將包括在分類範圍內。

  您可以在裝置的內容視窗中輸入製造商的名稱。

- **序號**

  帶該欄位中指定序號的所有硬體裝置將包括在該分類中。

- **清單號**

  帶有該欄位中指定的清單編號的裝置將包括在選取範圍內。

- **使用者**

  該欄位中指定使用者的所有硬體裝置都將包括在該分類中。

- **位置**

  裝置或硬體單元的位置（例如，在總部或分公司）。在該欄位中指定的位置佈署的電腦或其他裝置將包括在該分類中。

  您可以在該裝置的內容視窗中以任何格式敘述裝置的位置。

- **CPU 時鐘頻率 (MHz)，從**

  CPU 的最小時鐘速率。CPU 與輸入欄位中指定的時鐘速率範圍（含）比對的裝置將被包含在分類中。

- **CPU 時鐘頻率 (MHz)，到**

  CPU 的最大時鐘速率。CPU 與輸入欄位中指定的時鐘速率範圍（含）比對的裝置將被包含在分類中。

- **虛擬 CPU 內核數量，從**

  虛擬 CPU 核心的最小數量。CPU 與輸入欄位中指定的虛擬核心數範圍（含）比對的裝置將被包含在分類中。

- **虛擬 CPU 內核數量，到**

  虛擬 CPU 核心的最大數量。CPU 與輸入欄位中指定的虛擬核心數範圍（含）比對的裝置將被包含在分類中。

- **硬碟磁區，以 GB 為單位，從**

  裝置上硬碟磁碟機的最小容量。硬碟磁碟機與這些輸入欄位中指定的容量範圍（含）比對的裝置將包括在分類範圍內。

- **硬碟磁區，以 GB 為單位，到**

裝置上硬碟磁碟機的最大容量。硬碟磁碟機與這些輸入欄位中指定的容量範圍（含）比對的裝置將包括在分類範圍內。

- **RAM 大小 (MB)，從**

  裝置 RAM 的最小大小。RAM 與輸入欄位中指定的大小範圍（含）比對的裝置將被包含在分類中。

- **記憶體大小 (MB)**

  裝置 RAM 的最大大小。RAM 與輸入欄位中指定的大小範圍（含）比對的裝置將被包含在分類中。

協力廠商軟體詳情

在**應用程式登錄資料**子區域，您可以根據已安裝的應用程式設定搜尋裝置的標準：

- **應用程式名稱**

  在該下拉清單中，您可以選取應用程式。安裝有指定應用程式的裝置將包括在選取範圍中。

- **應用程式版本**

  在該輸入欄位中，您可以指定選定應用程式的版本。

- **供應商**

  在該下拉清單中，您可以選取已安裝應用程式的生產商。

- **應用程式狀態**

  在該下拉清單中，您可以選取應用程式的狀態（*已安裝*、*未安裝*）。已安裝或未安裝指定應用程式的裝置，取決於所選狀態，將被包含在分類。

- **根據更新尋找**

  如果啟用此選項，則搜尋操作將使用相關裝置內應用程式更新的有關資訊來執行。選取核取方塊後，**應用程式名稱**、**應用程式版本**與**應用程式狀態**欄位會各自變成**更新名稱**、**更新版本**和**狀態**。

  預設情況下已停用該選項。

- **不相容安全應用程式名稱**

  在該下拉清單中，您可以選取協力廠商安全應用程式。在搜尋過程中，安裝有指定程式的裝置將包括在選取範圍中。

- **應用程式標籤**

在該下拉清單中，您可以選取應用程式標籤。所有安裝了敘述中帶有所選標籤的應用程式的裝置都被包含在裝置分類。

- **套用到沒有指定標籤的裝置**

  如果啟用此選項，分類將包含未帶有所選標籤的敘述的裝置。

  如果停用該選項，則不套用標準。

  預設情況下已停用該選項。

在**弱點與更新**子區域中，您可以根據 Windows 更新來源指定將裝置納入分類的標準：

WUA 已轉換到管理伺服器

您可以在下拉清單中選取以下搜尋選項之一：

- **是**。如果選中該選項，搜尋結果會包含從管理伺服器收到 Windows Update 更新的裝置。
- **否**。如果選中該選項，結果會包含從其他來源收到 Windows Update 更新的裝置。

Kaspersky 應用程式詳情

在**Kaspersky 應用程式**子區域中，您可以根據所選的受管理應用程式設定將裝置納入分類的標準：

- **應用程式名稱**

  在下拉清單中，可設定按 Kaspersky 應用程式名稱執行搜尋時在分類中包括裝置的標準。

  清單僅提供管理員工作站上已安裝管理外掛程式的應用程式的名稱。

  如果未選取任何應用程式，則將不會套用該標準。

- **應用程式版本**

  在輸入欄位，可設定按 Kaspersky 應用程式版本號執行搜尋時在分類中包括裝置的標準。

  如果未指定版本號，則將不會套用該標準。

- **重大更新名稱**

  在該下拉清單中，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。

  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。

- **選擇上次更新模組的期間**

您可以使用此選項來設定按這些裝置上安裝的程式模組上次更新的時間搜尋裝置的標準。

如果選中此方塊，則您可以在輸入欄位中指定執行這些裝置上安裝的程式模組的上一次更新的時間間隔（日期和時間）。

如果清除此方塊，則將不會套用標準。

預設情況下已清空此方塊。

- **裝置透過管理伺服器進行管理**

在此下拉清單中，您可以將透過卡巴斯基安全管理中心雲端主控台管理的裝置加到分類中：

- **是**。應用程式會將透過卡巴斯基安全管理中心雲端主控台來管理的裝置加到分類中。
- **否**。應用程式會將不是透過卡巴斯基安全管理中心雲端主控台來管理的裝置加到分類中。
- **未選取值**。將不套用標準。

- **安全應用程式已安裝**

在該下拉清單，您可以包含已安裝安全應用程式的裝置到分類：

- **是**。應用程式包含安裝了安全應用程式的裝置到分類。
- **否**。應用程式會在分類中包含未安裝安全應用程式的裝置。
- **未選取值**。將不套用標準。

在**病毒防護**子區域，您可以根據防護狀態設定將裝置納入分類的標準：

- **資料庫發佈日期**

如果啟用此選項，您可以按病毒資料庫發佈日期搜尋用戶端裝置。在該輸入欄位中，您可以設定執行搜尋的時間間隔。

預設情況下已停用該選項。

- **資料庫記錄數**

如果啟用此選項，您可以依據資料庫記錄數量來搜尋用戶端裝置。在輸入欄位中，您可以設定病毒資料庫記錄數的上限值和下限值。

預設情況下已停用該選項。

- **上一次掃描**

如果啟用此選項，您可以按上次惡意軟體掃描時間來搜尋用戶端裝置。在該輸入欄位中，您可以指定執行上一次惡意軟體掃描的時段。

預設情況下已停用該選項。

- **偵測到的威脅**

進階加密標準 (AES) 對稱區塊編碼器演算法。在下拉清單中，您可以選取加密金鑰大小（56-bit、128-bit、192-bit 或 256-bit）。

可用值：*AES56*、*AES128*、*AES192* 和 *AES256*。

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。

應用程式元件子區段會針對在卡巴斯基安全管理中心雲端主控台中安裝了專用管理外掛程式的應用程式，列出該應用程式的元件。

在**應用程式元件**子區域中，您可以根據所選應用程式元件的狀態和版本編號指定將裝置納入分類的標準：

- **狀態**

  根據應用程式傳送到管理伺服器的元件狀態搜尋裝置。您可以選擇以下狀態之一：*N/A*、*Stopped*、*Paused*、*Starting*、*Running*、*Failed*、*Not installed*、*Not supported by license*。如果安裝在受管理裝置上的應用程式的所選元件具有指定狀態，裝置被包含到裝置分類。

  由應用程式傳送的狀態：

  - *已停止* - 元件被停用且不在工作。
  - *已暫停* - 元件被暫停，例如，在使用者在受管理應用程式上停止了防護後。
  - *正在啟動* - 元件處於初始化處理程序中。
  - *執行中* - 元件被啟用且在正常工作。
  - *失敗* — 元件操作中發生錯誤。
  - *未安裝* - 當設定應用程式自訂安裝時，使用者未選取該元件以安裝。
  - *不受產品授權支援* — 產品授權不涵蓋所選元件。

  不同於其他狀態，裝置上*N/A* 狀態不由應用程式傳送。該選項顯示應用程式沒有所選元件狀態的資訊。例如，這可能發生在所選元件不屬於任何在裝置上安裝的應用程式時，或裝置關閉時。

- **版本**

  根據您在清單中選取的版本號搜尋裝置。您可以輸入版本號，例如 `3.4.1.0`，然後指定所選元件是否必須具有相同、更早或更新版本。您也可以設定對所有版本的搜尋，除了指定的值。

標籤

在**標籤**區域中，您可以根據先前新增到受管理裝置的敘述的關鍵字（標籤）設定將裝置納入分類的標準：

如果有至少一個指定的標籤符合則套用

如果啟用此選項，搜尋結果將顯示包含帶有所選標籤的敘述的裝置。

如果停用此選項，搜尋結果將僅顯示包含帶有所有標籤的敘述的裝置。

預設情況下已停用該選項。

要將標籤新增到條件，請點擊**新增**按鈕，然後點擊**標籤**輸入欄位來選擇標籤。指定是否在裝置分類中包括或排除具有所選標籤的裝置。

- **必須被包含**

  如果選取了該選項，搜尋結果將顯示帶有包含了所選標籤的敘述的裝置。要尋找裝置，您可以使用星號，它表示任何字元長度的字串。

  預設情況下已選定此選項。

- **必須被排除**

  如果選取了該選項，搜尋結果將顯示不帶有包含了所選標籤的敘述的裝置。要尋找裝置，您可以使用星號，它表示任何字元長度的字串。

使用者

在**使用者**區域中，您可以根據登入到作業系統的使用者帳戶設定將裝置納入分類的標準。

- **最後一次登入系統的使用者**

  如果啟用此選項，您可以選擇用於配置標準的使用者帳戶。請注意，使用者清單經過篩選，會顯示內部使用者。搜尋結果會包含上一次登入使用者為所選使用者的裝置。

- **登入系統至少一次的使用者**

  如果啟用此選項，您可以選擇用於配置標準的使用者帳戶。請注意，使用者清單經過篩選，會顯示內部使用者。搜尋結果會包含指定的使用者至少登入過一次的裝置。

從裝置分類中匯出裝置清單

卡巴斯基安全管理中心雲端主控台可讓您將裝置分類中裝置的資訊匯出為 CSV 或 TXT 檔案。

從裝置分類中匯出裝置清單：

1. 從裝置分類中開啟包含裝置的表格。
2. 使用以下方法之一選擇要匯出的裝置：
   - 要選擇特定裝置，請選中它們旁邊的核取方塊。
   - 要從當前表頁面選擇所有裝置，請選中裝置表標頭中的核取方塊，然後選中**全選當前頁面**核取方塊。

- 要從表中選擇所有裝置，請選中裝置表標頭中的核取方塊，然後選擇**全選**核取方塊。

點擊**匯出到 CSV**或**匯出到 TXT**按鈕。表中包含的有關所選裝置的所有資訊都將被匯出。

請注意，如果您將篩選條件套用於裝置表，則只有來自顯示列的篩選資料將被匯出。

在分類中從管理群組中刪除裝置

在使用裝置分類時，你可以直接從管理群組中刪除裝置，而不是轉換到包含這些裝置的管理群組。

要從管理群組刪除裝置，請執行以下操作：

1. 在主功能表中，轉到**資產（裝置）→ 裝置分類** or **發現和佈署 → 裝置分類**。
2. 在選項清單中，按一下裝置分類的名稱。
   該頁面會顯示一個表格，其中包含有關裝置分類中包含的裝置的資訊。
3. 選取您要移除的裝置，之後點擊**刪除**。
   所選裝置即從對應管理群組中刪除。

當裝置顯示不活動時檢視和配置操作

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

要在組中裝置顯示不活動時檢視或設定操作：

1. 在主功能表中，轉至 **資產（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雲端主控台會分配狀態給每個受管理裝置。特定狀態會根據是否符合使用者定義的條件而指派。在某些情況下，卡巴斯基安全管理中心雲端主控台在分配狀態給裝置時，會將裝置在網路中的可見性旗標（請參閱下表）列入考量。若卡巴斯基安全管理中心雲端主控台在兩小時內未在網路中找到裝置，該裝置的可見性旗標會設定為*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。
惡意軟體掃描已長時間未執行	裝置在網路中可見且安全應用程式已安裝到裝置，但*惡意軟體掃描*工作在指定時間內未執行。條件僅套用到於 7 天之前或更早新增到管理伺服器資料庫的裝置。	多於 1 天。
資料庫已過期	裝置在網路中可見且安全應用程式已安裝到裝置，但病毒資料庫在指定時間內未在該裝置上更新。條件僅套用到於 1 天之前或更早新增到管理伺服器資料庫的裝置。	多於 1 天。
長時間未連線	網路代理已安裝到裝置，但由於裝置關閉，裝置在指定時間段內未連線到管理伺服器。	多於 1 天。
偵測到活動威脅	**活動威脅**資料夾中的未處理的物件的數量超過指定的值。	多於 0 個項目。
需要重新啟動	裝置在網路中可見，但應用程式基於所選原因之一在指定時間之前請求裝置重新啟動。	多於 0 分鐘。
安裝了不相容的應用程式	裝置在網路中可見，但透過網路代理執行的軟體清查在裝置上偵測到了不相容的應用程式。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
偵測到軟體弱點	裝置在網路中可見且網路代理已安裝到裝置，但*弱點掃描和所需更新*工作在裝置應用程式中偵測到指定嚴重等級的弱點。	• 緊急。 • 高。 • 中等。 • 如果弱點無法被修補則略過。 • 如果為安裝分配了更新則略過。
產品授權已到期	裝置在網路中可見，但產品授權已過期。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
產品授權即將到期	裝置在網路中可見，但裝置上的產品授權即將在指定天數內過期。	多於 0 天。
Windows Update 更新檢查已長時間未執行	裝置在網路中可見，但“執行 Windows 更新同步”工作在指定時間段內未執行。	多於 1 天。

無效的加密狀態	網路代理已安裝到裝置，但裝置加密結果等於指定值。	• 由於使用者拒絕未遵從政策（僅對外部裝置）。 • 由於錯誤未遵從政策。 • 套用政策時需要重新啟動。 • 未指定加密政策。 • 不支援。 • 當套用政策時。
行動裝置設定與政策不同	行動裝置設定不同於 Kaspersky Endpoint Security for Android 政策中指定的設定。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
偵測到未處理的安全問題	裝置上發現了一些未處理的安全問題。安全問題可以透過安裝在使用者端裝置上的受管理卡巴斯基應用程式自動建立，也可以由管理員手動建立。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
應用程式定義的裝置狀態	裝置狀態由受管理應用程式定義。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
裝置磁碟空間不足	裝置剩餘磁碟空間少於指定值或裝置無法與管理伺服器同步。當裝置已與管理伺服器成功同步且裝置上的剩餘空間大於或等於指定值時，*緊急*或*警告*狀態被變更為*正常*狀態。	大於 0 MB
裝置已失去管理	在裝置發現過程中，裝置在網路中可見，但是超過三次嘗試與管理伺服器同步都失敗了。	• 開關按鈕被關閉。 • 開關按鈕被開啟。
防護已停用	裝置在網路中可見，但裝置上的安全應用程式已被停用大於指定的時間段。 在這種情況下，安全應用程式的狀態為*stopped*或*failure*，不同於下列狀態：*starting*、*running*或*suspended*。	多於 0 分鐘。
安全應用程式	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

沒有執行		閉。 • 開關按鈕被開啟。

卡巴斯基安全管理中心雲端主控台可讓您設定在指定條件滿足時，自動轉換管理群組中裝置的狀態。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，逆值為**多於 7 天**，則會指派*緊急*狀態。

卡巴斯基安全管理中心雲端主控台在分配狀態給裝置時，會就某些條件（請參閱「條件敘述」欄）將可見性旗標列入考量。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 **資產（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 **資產（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。

變更用戶端裝置的管理伺服器

您可以使用**"變更管理伺服器"**工作來變更用戶端裝置連線的管理伺服器。工作完成後，所選用戶端裝置將被置於您指定的管理伺服器的管理之下。您可以在以下管理伺服器之間切換裝置管理：

- 主管理伺服器及其虛擬管理伺服器之一
- 同一台主管理伺服器的兩台虛擬管理伺服器

要變更用戶端裝置連線的管理伺服器：

1. 在主功能表中，轉至 **資產（裝置）→工作**。

2. 點擊**新增**。
   新工作精靈啟動。使用**下一步**按鈕進行精靈。

3. 對於卡巴斯基安全管理中心雲端主控台應用程式，請選取**變更管理伺服器**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. 選擇您想要用來管理所選裝置的管理伺服器。

7. 指定帳戶設定：

   - **預設帳戶**

在與執行該工作的應用程式相同的帳戶下執行該工作。
預設情況下已選定此選項。

- **指定帳戶**

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

- **帳戶**

  執行該工作的帳戶。

- **密碼**

  工作執行時使用的帳戶的密碼。

8. 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。
9. 點擊**完成**按鈕。
   工作被建立並顯示在工作清單。
10. 按一下建立的工作的名稱以開啟工作內容視窗。
11. 在工作內容視窗中，依需求指定一般工作設定。
12. 點擊**儲存**按鈕。
    工作被建立和配置。
13. 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。

關於叢集和伺服器陣列

卡巴斯基安全管理中心雲端主控台現在支援叢集技術。如果網路代理向管理伺服器傳送資訊確認組成伺服器陣列的用戶端裝置上已安裝該應用程式，則該用戶端裝置就成為一個叢集節點。

如果管理群組包含叢集或伺服器陣列，則**受管理裝置**頁面將顯示兩個頁簽：一個用於單個裝置，另一個用於叢集和伺服器陣列。受管理裝置被偵測為叢集節點後，叢集將作為單獨物件被新增到**叢集和伺服器陣列**頁簽中。

叢集或伺服器陣列節點與其他受管理裝置一起列在**裝置**頁簽上。您可以將節點作為單個裝置檢視屬性並執行其他操作，但不能刪除叢集節點或將其從叢集中單獨移動到另一個管理群組。您只能刪除或移動整個叢集。

您可以對叢集或伺服器陣列執行以下操作：

- 檢視屬性

- 將叢集或伺服器陣列移至另一個管理群組

  當您將叢集或伺服器陣列移動到另一個群組時，其所有節點都會隨之移動，因為叢集及其任何節點始終屬於同一管理群組。

- 刪除

  僅當組織網路中不再存在叢集或伺服器陣列時，刪除該叢集或伺服器陣列才合理。如果叢集在您的網路上仍然可見，且叢集節點上仍安裝有網路代理和 Kaspersky 安全應用程式，則卡巴斯基安全管理中心雲端主控台會自動將已刪除的叢集及其節點加回受管理裝置清單。

叢集或伺服器陣列的屬性

檢視叢集或伺服器陣列的設定：

1. 在主功能表中，轉至**資產（裝置）→受管理裝置→叢集和伺服器陣列**。

   叢集和伺服器陣列的清單將得以顯示。

2. 點擊所需叢集或伺服器陣列的名稱。

所選叢集或伺服器陣列的屬性視窗將得以顯示。

一般

一般區域顯示有關叢集或伺服器陣列的一般資訊。資訊基於上一次叢集節點與管理伺服器之間的同步接收的資料來提供：

- **名稱**
- **敘述**
- **Windows 網域**

  Windows 網域或工作群組，包含叢集或伺服器陣列。

- **NetBIOS 名稱**

  叢集或伺服器陣列的 Windows 網路名稱。

- **DNS 名稱**

  叢集或伺服器陣列的 DNS 網域名稱。

工作

在**工作**標籤中，您可以管理被分配給叢集或者伺服器陣列的工作：檢視現有工作清單；建立新工作；移除、啟動和停止工作；修改工作設定；以及檢視執行結果。列出的工作與安裝在叢集節點上的卡巴斯基安全應用程式相關。卡巴斯基安全管理中心雲端主控台是從叢集節點收到工作清單和工作狀態詳細資訊。如果未建立連線，則不顯示狀態。

節點

此頁簽顯示叢集或伺服器陣列中包含的節點清單。您可以點擊節點名稱來檢視裝置屬性視窗。

Kaspersky 應用程式

屬性視窗還可包含其他頁簽，其中包含與叢集節點上安裝的卡巴斯基安全應用程式相關的資訊和設定。

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雲端主控台可讓您對裝置加上標記。*標記*是指對裝置加上的標籤，可用於分組、說明或尋找裝置。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。自動標記則是由卡巴斯基安全管理中心雲端主控台依指定的標記規則來執行。

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，如果您的網路包含執行 Windows、Linux 和 macOS 的裝置，您可以設定一條規則，將 `[Linux]` 標記分配給所有基於 Linux 的裝置。然後，您便可以在建立裝置分類時使用該標記；這將有助您整理出所有基於 Linux 的裝置，然後向它們分配工作。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，包括主管理伺服器和從屬虛擬管理伺服器。規則僅被套用到來自建立規則的相同管理伺服器的裝置。

建立裝置標籤

要建立裝置標籤：

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

   新標籤視窗開啟。
3. 在**標籤**欄位中，輸入頁籤名稱。
4. 點擊**儲存**以儲存變更。

新標籤出現在裝置標籤清單。

重命名裝置標籤

要重命名裝置標籤：

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

更新的標籤出現在裝置標籤清單。

刪除裝置標籤

要刪除裝置標籤：

1. 在主功能表中，轉至 **資產（裝置）→標籤→裝置標籤**。
2. 在清單中，選取您想要刪除的裝置標籤。
3. 點擊**刪除**按鈕。
4. 在開啟的視窗中，點擊**是**按鈕。

裝置標籤被刪除。刪除的標籤被從其分配的所有裝置上自動刪除。

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

如果此標記由應用程式或網路代理分配給裝置，則已刪除的標記不會被自動從裝置中刪除。要從您的裝置中刪除標籤，請使用 klscflag 公用程式。

檢視分配了標籤的裝置

要檢視分配了標籤的裝置：

1. 在主功能表中，轉至 **資產（裝置）→標籤→裝置標籤**。
2. 點擊您要檢視已指派裝置之標籤的**檢視裝置**連結。

裝置清單僅顯示分配了標籤的裝置。

要返回裝置標籤清單，點擊您瀏覽器的**後退**按鈕。

檢視分配到裝置的標籤

要檢視分配到裝置的標籤：

1. 在主功能表中，轉至 **資產（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

要分配標籤到裝置：

1. 檢視分配到您要分配其他標籤的裝置的標籤。
2. 點擊**新增**。
3. 在開啟的視窗中，執行以下操作之一：
   - 若要建立並指派新標籤，請選取**建立新標籤**，之後指定新標籤的名稱。
   - 若要選取現有標籤，請選取**分配現有標籤**，之後在下拉清單選取必要標籤。
4. 點擊**確定**以套用變更。
5. 點擊**儲存**以儲存變更。

所選的標籤被分配到裝置。

要分配標籤到多個裝置：

1. 在主功能表中，轉至 **資產（裝置）→受管理裝置**。
2. 選擇要為其分配標籤的裝置。
3. 按一下**標籤**，然後從下拉清單中選擇**分配**。
4. 在開啟的視窗中，從下拉清單中選擇一個標籤。
   如果需要，您可以選擇多個標籤。
   您還可以執行以下操作：
   - 透過點擊**編輯**( ) 圖示輸入標籤的名稱.
     指定標籤的新名稱，然後點擊**儲存**按鈕。

請注意，該標籤也將在裝置標籤清單中被重新命名。

- 透過點擊**刪除**( ) 圖示刪除標籤。
  在開啟的視窗中，點擊**刪除**按鈕。

  請注意，該標籤也將被從管理伺服器中刪除。

5. 點擊**儲存**按鈕。

標籤被分配到選定裝置。您可以刪除已分配的標籤。

從裝置上刪除分配的標籤

未配置的裝置標籤不被刪除。如果您想，您可以手動刪除它。

您不能手動刪除應用程式或網路代理分配給裝置的標籤。要刪除這些標籤，請使用 klscflag 公用程式。

要從裝置上刪除標籤：

1. 在主功能表中，轉至 **資產（裝置）→受管理裝置**。
2. 點擊您要檢視其標籤的裝置名稱。
3. 在開啟的裝置內容視窗中，選取**標籤**頁籤。
4. 選取您要刪除的項目旁邊的核取方塊。
5. 在清單頂部，點擊**取消分配標籤**按鈕。
6. 在開啟的視窗中，點擊**是**按鈕。

標籤從裝置上刪除。

若要從多個裝置中刪除標籤：

1. 在主功能表中，轉至 **資產（裝置）→受管理裝置**。
2. 選擇要刪除其標籤的裝置。
3. 點擊**標籤**，然後從下拉清單中選擇**移除**。
4. 在開啟的視窗中，選取要刪除的標籤旁邊的核取方塊。

   此視窗會顯示分配給您在步驟 2 中選取的所有裝置的所有標籤。

5. 點擊**儲存**按鈕。

標籤被從裝置中刪除。

檢視自動標記裝置規則

要檢視自動標記裝置規則，

做以下任意：

- 在主功能表中，轉至 **資產（裝置）→ 標籤 → 自動標記規則**。
- 在主功能表中，前往**資產（裝置）→ 標籤 → 裝置標籤**，然後點擊**設定自動標記規則**連結。
- 檢視指派給裝置的標籤，接著點擊**設定**按鈕。

自動標記裝置規則清單出現。

編輯自動標記裝置規則

要編輯自動標記裝置規則：

1. 檢視自動標記裝置規則。
2. 點擊您要編輯的規則名稱。
   規則設定視窗開啟。
3. 編輯規則的一般內容：
   a. 在**規則名稱**欄位，輸入規則名稱。
      名稱不能包括 256 個以上字元。
   b. 做以下任意：
      - 透過切換開關按鈕至**規則已啟用**啟用規則。
      - 透過切換開關按鈕至**規則已停用**停用規則。
4. 做以下任意：
   - 如果要新增新條件，請點擊**新增**按鈕，然後在開啟的視窗中指定新條件的設定。
   - 若要編輯現有條件，請點擊您要編輯之條件的名稱，接著編輯條件設定。
   - 若您要刪除條件，請選取您要刪除之條件名稱旁的核取方塊，接著點擊**刪除**。
5. 在條件設定視窗點擊**確定**。
6. 點擊**儲存**以儲存變更。

編輯的規則顯示在清單。

建立自動標記裝置規則

要建立自動標記裝置規則：

1. 檢視自動標記裝置規則。
2. 點擊**新增**。
   新規則設定視窗開啟。
3. 配置規則的一般內容：
   a. 在**規則名稱**欄位中，輸入規則名稱。
      名稱不能包括 256 個以上字元。
   b. 執行以下操作之一：
      - 透過切換開關按鈕至**規則已啟用**啟用規則。
      - 透過切換開關按鈕至**規則已停用**停用規則。
   c. 在**標籤**欄位中，輸入新裝置標籤名稱或從清單中選取其中一個現有裝置標籤。
      名稱不能包括 256 個以上字元。
4. 在條件區段中，點擊**新增**按鈕以新增新條件。
   新條件設定視窗開啟。
5. 輸入條件名稱。
   名稱不能包括 256 個以上字元。名稱必須在規則內唯一。
6. 設定根據以下條件的規則觸發。您可以選取多個條件。
   - **網路**—裝置網路內容，例如 Windows 網路中的裝置名稱，或裝置是否屬於網域或 IP 範圍。

     如果您用於卡巴斯基安全管理中心雲端主控台的資料庫設有區分大小寫的規則，請在指定裝置 DNS 名稱時保留大小寫。否則，自動標記規則將不起作用。

   - **應用程式**—網路代理在裝置上的出現，和作業系統類型、版本和架構。
   - **虛擬機**—裝置屬於虛擬機的特定類型。
   - **Active Directory**—裝置在 Active Directory 組織單元中的出現和裝置在 Active Directory 群組中的成員關係。
   - **應用程式登錄資料**—裝置上不同供應商應用程式的出現。
7. 點擊**確定**儲存變更。
   如果必要，您可以為一個規則設定多個條件。此種情況下，在滿足至少一個條件時，標籤將被分配到裝置。
8. 點擊**儲存**以儲存變更。

新建立的規則會在所選管理伺服器管理的裝置上強制執行。如果裝置的設定滿足規則條件，標籤被分配到裝置。

然後，規則被套用到以下情況：

- 自動和間歇性，取決於伺服器負載
- 在您編輯規則之後
- 當您手動執行規則時
- 在管理伺服器偵測到滿足規則條件的裝置設定的變更或包含此裝置的群組設定的變更後

您可以建立多個標記規則。如果您建立了多個標記規則且規則對應的條件同時被滿足，單個裝置可以被分配多個標籤。您可以在裝置內容中檢視所有分配的標籤清單。

為自動標記裝置執行規則

當規則執行時，規則內容中指定的標籤被分配到滿足相同規則中指定條件的裝置。您僅可以執行活動規則。

要為自動標記裝置執行規則：

1. 檢視自動標記裝置規則。
2. 選取您要執行的活動規則旁邊的核取方塊。
3. 點擊**執行規則**按鈕。

   所選規則被執行。

刪除自動標記裝置規則

要刪除自動標記裝置規則：

1. 檢視自動標記裝置規則。
2. 選取您要刪除的規則旁邊的核取方塊。
3. 點擊**刪除**。
4. 在開啟的視窗中，再次點擊**刪除**按鈕。

   所選規則被刪除。規則內容中指定的標籤從所有所分配的裝置上取消分配。

> 未配置的裝置標籤不被刪除。如果您想，您可以手動刪除它。

隔離區和備份區

安裝在用戶端裝置上的 Kaspersky 防毒應用程式可能在裝置掃描過程中放置檔案到隔離區或備份區。

*隔離區*是一個存放檔案的特殊區域，儲存疑似感染的檔案或偵測時無法解毒的檔案。

*備份區*設定用於儲存在解毒過程中被刪除或被修改的檔案的備份副本。

卡巴斯基安全管理中心雲端主控台會將裝置上被 Kaspersky 應用程式放入隔離區或備份區的檔案建立成一份摘要清單。用戶端裝置上的網路代理將隔離區和備份區檔案的資訊傳輸到管理伺服器。

卡巴斯基安全管理中心雲端主控台並不會將儲存區中的檔案複製到管理伺服器。所有檔案均儲存在裝置儲存區中。

從儲存區下載檔案

卡巴斯基安全管理中心雲端主控台可讓您將用戶端裝置上被安全應用程式放入隔離區或備份區的檔案下載一份副本。檔案會複製到您指定的目的。

僅當滿足以下其中一項條件時，您才能下載檔案：該裝置的設定中啟用了**不斷開與管理伺服器的連線**選項、正在使用推送伺服器，或是正在使用連線閘道。否則，下載將無法進行。

不斷開與管理伺服器的連線選項所能選取的最大裝置總數是 300。

要將隔離區或備份區中的檔案備份儲存到硬碟磁碟機，請執行以下操作：

1. 執行以下操作之一：
   - 如果要從隔離區儲存檔案副本，請在主功能表中，轉到**操作 → 儲存區 → 隔離**。
   - 如果要從備份儲存檔案副本，請在主功能表中，轉到**操作 → 儲存區 → 備份**。
2. 在開啟的視窗中，選擇要下載的檔案，然後點擊**下載**。

下載開始。已放置在用戶端裝置上隔離區中的檔案的副本將被儲存到指定的資料夾中。

從儲存區刪除檔案

要將檔案從隔離區或備份區刪除，請執行以下操作：

1. 執行以下操作之一：
   - 如果要從隔離區儲存檔案副本，請在主功能表中，轉到**操作 → 儲存區 → 隔離**。
   - 如果要從備份儲存檔案副本，請在主功能表中，轉到**操作 → 儲存區 → 備份**。
2. 在開啟的視窗中，選取要刪除的檔案，然後點擊**刪除**。
3. 確認您要刪除該檔案。

已將檔案放入存儲庫（隔離或備份）的用戶端裝置上的安全應用程式會從此存儲庫中刪除相同的檔案。

用戶端裝置的遠端診斷

您可在 Windows 和 Linux 用戶端裝置上遠端執行遠端診斷：

- 啟用和關閉偵錯、變更偵錯等級並下載偵錯檔案
- 下載系統資訊和應用程式設定
- 下載事件記錄
- 為應用程式建立記憶體傾印檔案
- 開始進行診斷並下載診斷報告
- 啟動、停止和重新啟動應用程式

您可以使用從用戶端裝置下載的事件記錄和診斷報告以自行定位問題。同時，若您聯絡 Kaspersky 技術支援，他們可能會請您從用戶端裝置下載偵錯檔案、傾印檔案、事件記錄和診斷報告以讓 Kaspersky 進一步分析。

開啟遠端診斷視窗

若要執行對 Windows 和 Linux 用戶端裝置的遠端診斷，您必須開啟遠端診斷視窗。

開啟遠端診斷視窗：

1. 選取您要開啟遠端診斷視窗的裝置，並執行以下其中一個動作：
   - 若裝置屬於管理群組，請在主功能表中，前往**資產（裝置）→ 群組 → <群組名稱> → 受管理裝置**。
   - 若裝置屬於「未配置的裝置」群組，請在主功能表中，前往**發現和佈署 → 未配置的裝置**。
2. 點擊所需裝置的名稱。
3. 在開啟的裝置內容視窗中，選取**進階**頁籤。
4. 在開啟的視窗中，點擊**遠端診斷**。

   這會開啟用戶端裝置的**遠端診斷** 視窗。如果管理伺服器與用戶端裝置之間並未建立連線，則會顯示錯誤訊息。

或者，如果您需要立即取得某個基於 Linux 的用戶端裝置的所有診斷資訊，您可以在該裝置上執行 collect.sh 指令碼。

啟用與停用應用程式偵錯

您可啟用和停用對應用程式的偵錯，包含 Xperf 偵錯。

啟用和停用偵錯

在遠端裝置上啟用或停用偵錯：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗中，選擇**Kaspersky 應用程式**頁簽。
   在**應用程式管理**區域中，裝置上安裝的卡巴斯基應用程式清單得以顯示。
3. 在應用程式清單上，選取您要啟用或停用偵錯的應用程式。
   遠端診斷選項清單隨即開啟。
4. 若您要啟用偵錯：
   a. 在**偵錯**區域中，點擊**啟用偵錯**。
   b. 在開啟的**修改偵錯等級**視窗中，建議您保留設定的預設值。當需要時，技術支援專家將指導您設定過程。下列設定可用：
      - **偵錯等級**
        偵錯等級定義偵錯檔案包含的詳情資料量。
      - **基於循環的偵錯**
        應用程式覆蓋偵錯資訊以防止偵錯檔案過量增長。指定用於儲存偵錯資訊的檔案最大數量，以及每個檔案的最大大小。如果寫入了最大數量的最大大小的偵錯檔案，最舊的檔案被刪除以便新偵錯檔案可以被寫入。

        此設定僅適用於 Kaspersky Endpoint Security
   c. 點擊**儲存**。

   偵錯會針對選取的應用程式啟用。某些情況下，要啟用偵錯，必須重新啟動安全應用程式及其工作。

   在基於 Linux 的用戶端裝置上，Kaspersky Security Agent 元件更新程式的偵錯由網路代理設定管理。因此，在執行 Linux 的用戶端裝置上，此元件的**啟用偵錯**和**修改偵錯等級**"選項被停用。
5. 若您要停用對選取的應用程式偵錯，請點擊**停用偵錯**。
   系統會針對選取的應用程式停用偵錯。

啟用 Xperf 偵錯

對於 Kaspersky Endpoint Security，技術支援專家可能需求您對系統效能資訊啟用 Xperf 偵錯。

要啟用和配置 Xperf 偵錯或停用它：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗中，選擇**Kaspersky 應用程式**頁簽。
   在**應用程式管理**區域中，裝置上安裝的卡巴斯基應用程式清單得以顯示。
3. 在應用程式清單中，選取 Kaspersky Endpoint Security for Windows。

適用於 Kaspersky Endpoint Security for Windows 遠端診斷選項的清單隨即顯示。

4. 在**Xperf 偵錯**區域中，點擊**啟用 Xperf 偵錯**。

   若已啟用 Xperf 偵錯，則會改為顯示**停用 Xperf 偵錯**按鈕。如果您想要停用 Kaspersky Endpoint Security for Windows 的 Xperf 偵錯，請點擊此按鈕。

5. 在開啟的**變更 Xperf 偵錯等級**視窗，根據技術支援專員的要求執行以下動作：

   a. 選取以下其中一個偵錯等級：

   - **輕度等級**

     該類型的偵錯檔案包含系統最少量資訊。

     預設情況下已選定此選項。

   - **深度等級**

     相比於*輕度*類型的偵錯檔案，該類型的偵錯檔案包含更多詳細資訊，且可能在*輕度*類型偵錯檔案不足以評估效能時被技術支援專家需求。*深度*偵錯檔案包含關於系統的硬體、作業系統、應用程式的啟動和結束處理程序清單、用於效能評估的事件和來自 Windows System Assessment 工具的事件的技術資訊。

   b. 選取以下其中一個 Xperf 偵錯類型：

   - **基本類型**

     偵錯資訊在 Kaspersky Endpoint Security 應用程式執行期間被接收。

     預設情況下已選定此選項。

   - **重新啟動時類型**

     偵錯資訊在作業系統從受管理裝置上啟動時接收。該偵錯類型在影響系統效能的問題發生時，在裝置被開啟後和 Kaspersky Endpoint Security 啟動之前有效。

   系統可能要求您啟用**循環檔案大小 (MB)**選項，以防止偵錯檔案的過量增長。然後指定偵錯檔案的最大大小。當檔案達到最大大小時，最舊的偵錯資訊被新資訊覆蓋。

   c. 定義輪換檔案大小。

   d. 點擊**儲存**。

   系統會啟用並設定 Xperf 偵錯。

6. 如果您想要停用 Kaspersky Endpoint Security for Windows 的 Xperf 偵錯，請點擊**Xperf 偵錯**區域中的**停用 Xperf 偵錯**。

   Xperf 偵錯已停用。

下載應用程式偵錯檔案

僅當滿足以下其中一項條件時，您才能從用戶端裝置下載偵錯檔案：該裝置的設定中啟用了**不斷開與管理伺服器的連線**選項、正在使用推送伺服器，或是正在使用連線閘道。否則，下載將無法進行。

不斷開與管理伺服器的連線選項所能選取的最大裝置總數是 300。

要下載應用程式的偵錯檔案：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗中，選擇**Kaspersky 應用程式**頁簽。
   在**應用程式管理**區域中，裝置上安裝的卡巴斯基應用程式清單得以顯示。
3. 在應用程式清單中，選取您要為其下載偵錯檔案的應用程式。
4. 在**偵錯**部分中，點擊**偵錯檔案**按鈕。
   這會開啟**裝置偵錯記錄**視窗，其中會顯示偵錯檔案清單。
5. 在偵錯檔案清單中，選取您要下載的檔案。
6. 執行以下操作之一：
   - 點擊**下載**來下載所選檔案。您可以選擇一個或多個檔案進行下載。
   - 下載部分選取的檔案：
     a. 點擊**下載一部分**。
        您無法同時下載多個檔案的部分內容。如果您選擇多個偵錯檔案，**下載一部分**按鈕將被停用。
     b. 在開啟的視窗中，根據您的需求指定要下載的名稱與檔案部分。
        對於基於 Linux 的裝置，無法編輯檔案部分名稱。
     c. 點擊**下載**。

選取的檔案或其部分會下載至您指定的位置。

刪除偵錯檔案

您可刪除不再需要的偵錯檔案。

若要刪除偵錯檔案：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在開啟的遠端診斷視窗中，選擇**事件記錄**頁簽。
3. 在**偵錯檔案**區段中，點擊**Windows Update 記錄**或**遠端安裝記錄**，視您要刪除的偵錯檔案而定。
   這會開啟**裝置偵錯記錄**視窗，其中會顯示偵錯檔案清單。
4. 在偵錯檔案清單中，選取一個或多個您要刪除的檔案。
5. 點擊**移除**按鈕。

選取的偵錯檔案被刪除。

下載應用程式設定

僅當滿足以下其中一項條件時，您才能從用戶端裝置下載應用程式設定：該裝置的設定中啟用了**不斷開與管理伺服器的連線**選項、正在使用推送伺服器，或是正在使用連線閘道。否則，下載將無法進行。

不斷開與管理伺服器的連線選項所能選取的最大裝置總數是 300。

從用戶端裝置下載應用程式設定：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗中，選擇**Kaspersky 應用程式**頁簽。
3. 在**應用程式設定**區段中，點擊**下載**按鈕，下載用戶端裝置上已安裝應用程式設定的資訊。

包含資訊的 ZIP 存檔將被下載到指定位置。

從用戶端裝置下載系統資訊

僅當滿足以下其中一項條件時，您才能從用戶端裝置下載系統資訊到您的裝置：該裝置的設定中啟用了**不斷開與管理伺服器的連線**選項、正在使用推送伺服器，或是正在使用連線閘道。否則，下載將無法進行。

不斷開與管理伺服器的連線選項所能選取的最大裝置總數是 300。

從用戶端裝置下載系統資訊：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗中，選擇**系統資訊**頁簽。
3. 點擊**下載**按鈕可下載有關用戶端裝置的系統資訊。

包含資訊的檔案將下載到指定位置。

下載事件記錄

僅當滿足以下其中一項條件時，您才能從用戶端裝置下載事件記錄到您的裝置：該裝置的設定中啟用了**不斷開與管理伺服器的連線**選項、正在使用推送伺服器，或是正在使用連線閘道。否則，下載將無法進行。

不斷開與管理伺服器的連線選項所能選取的最大裝置總數是 300。

要從遠端裝置下載事件記錄：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗的**事件記錄**頁簽上，點擊**所有裝置記錄**。
3. 在**所有裝置記錄**視窗中，選取多個相關記錄。
4. 執行以下操作之一：

- 點擊**下載整個檔案**來下載所選日誌。
- 下載部分選取的記錄：
  a. 點擊**下載一部分**。
  您無法同時下載多個日誌的部分內容。如果您選擇多個事件記錄，**下載一部分**按鈕將被停用。
  b. 在開啟的視窗中，根據您的需求指定要下載的名稱與記錄部分。
  c. 點擊**下載**。

選取的事件記錄或其部分，會下載至指定的位置。

啟動、停止、重新啟動應用程式

您可在用戶端裝置啟動、停止、重新啟動應用程式。

若要啟動、停止和重新啟動應用程式，請執行以下操作：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗中，選擇**Kaspersky 應用程式**頁簽。
   在**應用程式管理**區域中，裝置上安裝的卡巴斯基應用程式清單得以顯示。
3. 在應用程式清單中，選取您要啟動、停止或重新啟動的應用程式。
4. 點擊以下其中一個按鈕以選取動作：
   - **停止應用程式**
     此按鈕僅在應用程式正在執行時可供使用。
   - **重新啟動應用程式**
     此按鈕僅在應用程式正在執行時可供使用。
   - **啟動應用程式**
     此按鈕僅在應用程式不是正在執行時可供使用。

視您選取的動作而定，系統會啟動、停止或重新啟動應用程式。

若您重新啟動網路代理，系統會顯示訊息表示將失去裝置對管理伺服器的目前連線。

執行應用程式的遠端診斷並下載結果

要為某遠端裝置應用程式啟動診斷並下載其執行結果，請執行以下操作：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗中，選擇**Kaspersky 應用程式**頁簽。
   在**應用程式管理**區域中，裝置上安裝的卡巴斯基應用程式清單得以顯示。

3. 在應用程式清單中，選取您要執行遠端診斷的應用程式。

   遠端診斷選項清單隨即開啟。

4. 在**診斷報告**區段中，點擊**執行診斷** 按鈕。

   這會啟動遠端診斷程序並產生診斷報告。診斷程序完成時，您就能使用**下載診斷報告**按鈕。

5. 按一下**“ 下載診斷報告”**按鈕下載報告。

報告將下載到指定位置。

在用戶端裝置執行應用程式

您可能需要在用戶端裝置上執行應用程式，若 Kaspersky 支援專家要求您這樣做的時候。您無需在該裝置上安裝該應用程式。您無需在該裝置上安裝該應用程式。

若要在用戶端裝置上執行應用程式：

1. 開啟用戶端裝置的遠端診斷視窗。

2. 在遠端診斷視窗中，選擇**執行遠端應用程式**頁簽。

3. 在**應用程式檔案**部分中，點擊**瀏覽**按鈕以選擇包含要在用戶端裝置上執行的應用程式的 ZIP 存檔。

   > ZIP 存檔必須包含公用程式資料夾。此資料夾包含要在遠端裝置上執行的可執行檔。

   如有必要，您可以指定可執行檔名稱和命令行參數。為此，請填寫**要在遠端裝置上執行的封存中的可執行檔**和**命令列參數**欄位。

4. 點擊**上傳和執行**按鈕以在用戶端裝置上執行指定的應用程式。

5. 請遵循卡巴斯基支援專業人員的指示。

為應用程式建立記憶體傾印檔案

應用程式傾印檔案允許您檢視某個時間點在用戶端裝置上執行的應用程式的參數。該檔案還包含有關為應用程式加載的模組的資訊。

> 產生傾印檔案僅適用於在基於 Windows 的用戶端裝置上執行的 32 位元處理程序。對於執行 Linux 的用戶端裝置和 64 位元處理程序，此功能不受支援。

要為應用程式建立傾印檔案：

1. 開啟用戶端裝置的遠端診斷視窗。

2. 在遠端診斷視窗中，選擇**執行遠端應用程式**頁簽。

3. 在**正在產生處理程序記憶體傾印檔案**區域中，指定要為其產生傾印檔案的應用程式的可執行檔。

4. 點擊**下載**按鈕以儲存指定應用程式的傾印檔案。

   如果指定的應用程式未在用戶端裝置上執行，則會顯示錯誤消息。

用戶端裝置的遠端桌面連線

您可以透過用戶端裝置上安裝的網路代理，遠端存取該裝置的桌面。如果裝置的 TCP 和 UDP 連接埠關閉，也可透過網路代理遠端連線至用戶端裝置。

與裝置建立連線後，您即會對該裝置上儲存的資訊具有完整存取權限，並且可以管理該裝置上安裝的應用程式。

您必須在目標受管理裝置的作業系統設定中允許目標遠端連線。例如，在 Windows 10 中，此選項名為**允許遠端協助連線至此電腦**（您可在**主控台 → 系統和安全性 → 系統 → 遠端設定**找到此選項）。若您有「弱點和修補程式管理」的授權，您可建立與受管理裝置的連線時強制啟用此選項。若您沒有授權，請在目標受管理裝置上啟用此選項。如果停用此選項，則無法使用遠端連線。

若要建立遠端裝置連線，您需有兩個公用程式：

- Kaspersky 公用程式，名稱為 klsctunnel。此公用程式必須儲存在您的工作站上。您可使用此公用程式進行用戶端裝置與管理伺服器之間的通道連線。

  卡巴斯基安全管理中心雲端主控台允許以先途經管理伺服器、再途經網路代理的方式，開闢從管理主控台到受管理裝置上所指定連接埠的 TCP 連線通道。通道設計用於連線安裝管理主控台的裝置上的用戶端應用程式到受管理裝置上的 TCP 連接埠—如果管理主控台和目的裝置之間沒有直接連線可用。

  如果用於連線到管理伺服器的連接埠在裝置上不可用，則需要遠端用戶端裝置和管理伺服器之間的連線隧道。在以下情況下裝置連接埠可能無法使用：

  - 遠端裝置使用 NAT 機制連線到本機網路。
  - 遠端裝置是本機網路管理伺服器的一部分，但是它的連接埠已被防火牆關閉。

- 名為「遠端桌面連線」的標準 Microsoft Windows 元件。根據標準 Windows 公用程式 mstsc.exe 的設定建立遠端桌面的連線。

  在使用者不知道的情況下遠端連線到使用者目前的桌面。一旦您連線上，裝置使用者即會在未獲事先通知的情況下被中斷連線。

若要連線到用戶端裝置的桌面，必須符合以下其中一項條件：

- 用戶端裝置所屬的管理群組具有的發佈點啟用了**不斷開與管理伺服器的連線**選項。
- 在用戶端裝置設定中，**不斷開與管理伺服器的連線**選項已啟用。

  啟用了**不斷開與管理伺服器的連線**選項的用戶端裝置數量上限為 300 台。

若要連線至用戶端裝置的桌面：

1. 在主功能表中，轉至 **資產（裝置）→ 受管理裝置**。
2. 選取您要取得存取權限之裝置名稱旁邊的核取方塊。
3. 點擊**連線到遠端桌面**按鈕。

   遠端桌面（僅限 Windows）視窗隨即開啟。

4. 點擊**下載**按鈕以下載 klsctunnel 實用程式。

5. 點擊**複製到剪貼簿**按鈕以複製文字欄位的文字。此文字為二進位大型物件 (BLOB)，其中包含建立管理伺服器與受管理裝置間連線的設定。

   BLOB 有效時間為 3 分鐘。若 BLOB 已到期，請重新開啟遠端桌面（僅限 Windows）視窗以產生新的 BLOB。

6. 執行 klsctunnel 公用程式。

   公用程式視窗隨即開啟。

7. 貼上複製的文字至文字欄位。

8. 若您使用代理伺服器，請選取**使用代理伺服器**核取方塊，接著指定代理伺服器連線設定。

9. 點擊**開啟連接埠**按鈕。

   「遠端桌面連線」登入視窗隨即開啟。

10. 指定您目前用來登入卡巴斯基安全管理中心雲端主控台的帳戶憑證。

11. 點擊**連線**按鈕。

與裝置建立連線後，您將能在 Microsoft Windows 的遠端連線視窗中使用桌面。

透過 Windows 桌面共用連線到用戶端裝置

您可以透過用戶端裝置上安裝的網路代理，遠端存取該裝置的桌面。如果裝置的 TCP 和 UDP 連接埠關閉，也可透過網路代理遠端連線至用戶端裝置。

您可以連線至用戶端裝置上的現有工作階段，而不使該工作階段中的使用者中斷連線。在此情況下，您和裝置上的工作階段使用者將共享對桌面的存取。

若要建立遠端裝置連線，您需有兩個公用程式：

- Kaspersky 公用程式，名稱為 klsctunnel。此公用程式必須儲存在您的工作站上。您可使用此公用程式進行用戶端裝置與管理伺服器之間的通道連線。

  卡巴斯基安全管理中心雲端主控台允許以先途經管理伺服器、再途經網路代理的方式，開闢從管理主控台到受管理裝置上所指定連接埠的 TCP 連線通道。通道設計用於連線安裝管理主控台的裝置上的用戶端應用程式到受管理裝置上的 TCP 連接埠—如果管理主控台和目的裝置之間沒有直接連線可用。

  如果用於連線到管理伺服器的連接埠在裝置上不可用，則需要遠端用戶端裝置和管理伺服器之間的連線隧道。在以下情況下裝置連接埠可能無法使用：

  - 遠端裝置使用 NAT 機制連線到本機網路。
  - 遠端裝置是本機網路管理伺服器的一部分，但是它的連接埠已被防火牆關閉。

- Windows 桌面共用。當連線到現有的遠端桌面工作階段時，裝置上的工作階段使用者會收到您的連線請求。在卡巴斯基安全管理中心雲端主控台建立的報告中，不會儲存有關裝置上的遠端操作及其結果有關的任何資訊。

您可以設定對遠端用戶端裝置上的使用者活動進行稽核。在稽核期間，應用程式會儲存用戶端裝置上經管理員開啟並/或修改過之檔案的資訊。

使用 Windows 桌面共用連線到用戶端裝置必須符合以下需求：

- 您的工作站上安裝了 Microsoft Windows Vista 或以上版本。

  若要檢查 Windows 桌面共用功能是否隨附於您的 Windows 版本中，請確保 32 位元的登錄檔中包含 CLSID {32BE5ED2-5C86-480F-A914-0FF8885A1B3F}。

- 用戶端裝置安裝了 Microsoft Windows Vista 或更新版本。

- 卡巴斯基安全管理中心雲端主控台使用的是支援弱點和修補程式管理的產品授權。

- 用戶端裝置所屬的管理群組具有的發佈點啟用了**不斷開與管理伺服器的連線**選項，或是用戶端裝置設定中啟用了該選項。

  請注意，啟用了**不斷開與管理伺服器的連線**選項的用戶端裝置數量上限為 300 個。

若要透過 Windows 桌面共用連線到用戶端裝置的桌面：

1. 在主功能表中，轉至 **資產（裝置）→受管理裝置**。
2. 選取您要取得存取權限之裝置名稱旁邊的核取方塊。
3. 點擊**Windows 共用桌面**按鈕。

   Windows 共用桌面精靈隨即開啟。
4. 點擊**下載**按鈕下載 klsctunnel 實用程式，接著等待下載程序完成。

   若您已有 klsctunnel 公用程式，請略過此步驟。
5. 點擊**下一步**按鈕。
6. 選取裝置上您要連線的工作階段，接著點擊**下一步**按鈕。
7. 在目標裝置上開啟的對話方塊中，使用者必須允許共用工作階段。否該工作階段將無法完成。

   裝置使用者確認桌面共用的工作階段後，精靈的下一頁面隨即開啟。
8. 點擊**複製到剪貼簿**按鈕以複製文字欄位的文字。此文字為二進位大型物件 (BLOB)，其中包含建立管理伺服器與受管理裝置間連線的設定。

   > BLOB 有效時間為 3 分鐘。若已過期，請產生全新 BLOB。

9. 執行 klsctunnel 公用程式。

   公用程式視窗隨即開啟。
10. 貼上複製的文字至文字欄位。
11. 若您使用代理伺服器，請選取**使用代理伺服器**核取方塊，接著指定代理伺服器連線設定。
12. 點擊**開啟連接埠**按鈕。

桌面共用會在新視窗啟動。若您要與裝置互動，請點擊視窗左上角的功能表圖示 ( )，接著選取**互動模式**。

智慧培訓模式中的規則觸發

該部分提供了用戶端裝置上的 Kaspersky Endpoint Security for Windows 中的適應性異常控制規則執行的偵測資訊。

規則偵測用戶端裝置上的異常行為並可能封鎖它。規則如果是以智慧培訓模式運作，則會偵測異常行為，然後將所偵測到每個異常行為的報告傳送給卡巴斯基安全管理中心雲端主控台管理伺服器。此資訊會以清單儲存在**儲存區**資料夾的**智慧培訓狀態中的規則觸發**子資料夾中。您可以確認偵測為正確或新增它們為排除，因此該行為類型不再被認為是異常。

偵測資訊儲存在管理伺服器的事件記錄中（與其他事件一起）和適應性異常控制報告中。

如需自適應異常控制、規則以及規則模式與狀態的更多資訊，請參閱 Kaspersky Endpoint Security 說明。

檢視使用適應性異常控制規則執行的偵測清單

要檢視使用適應性異常控制規則執行的偵測清單：

1. 在主功能表中，前往**操作 → 儲存區**。
2. 點擊**智慧培訓狀態中的規則觸發**連結。

   清單顯示使用適應性異常控制規則執行的偵測的以下資訊：

   - **管理群組**

     裝置所屬管理群組的名稱。

   - **裝置名稱**

     套用規則的用戶端裝置名稱。

   - **名稱**

     套用的規則名稱。

   - **狀態**

     正在排除 — 如果管理員處理該項目並新增其到排除規則清單。該狀態保持到下一次用戶端電腦與管理伺服器同步時，同步之後，該項目從清單消失。

     正在確認 — 如果管理員處理該項目並確認。該狀態保持到下一次用戶端電腦與管理伺服器同步時，同步之後，該項目從清單消失。

     空 — 如果管理員不處理該項目。

   - **使用者名稱**

執行產生偵測之處理程序的用戶端裝置使用者名稱。

- **已處理**

  異常被偵測的日期。

- **來源處理程序路徑**

  處理程序來源路徑，例如，執行操作的處理程序路徑（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

- **來源處理程序雜湊**

  處理程序來源檔案的 SHA-256 雜湊（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

- **來源物件路徑**

  啟動處理程序的物件路徑（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

- **來源物件雜湊**

  原始檔案的 SHA-256 雜湊（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

- **目的處理程序路徑**

  目的處理程序的路徑（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

- **目的處理程序雜湊**

  目的檔案的 SHA-256 雜湊（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

- **目的物件路徑**

  目的物件的路徑（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

- **目的物件雜湊**

  目的檔案的 SHA-256 雜湊（更多資訊請參閱 Kaspersky Endpoint Security 說明）。

要檢視每個資訊元素的內容：

1. 在主功能表中，前往**操作 → 儲存區**。
2. 點擊**智慧培訓狀態中的規則觸發**連結。

3. 在開啟的視窗中，選取您需要的物件。

4. 點擊**內容**連結。

物件的內容視窗即會開啟，其中會顯示所選元素的資訊。

您可以確認或新增到排除適應性異常控制規則偵測清單的任何元素。

要確認元素，

在偵測清單中選取元素並點擊**確認**按鈕。

元素的狀態被變更為正在**正在確認**。

您的確認將被統計到規則所用的統計資訊中（如需更多資訊，請參閱 Kaspersky Endpoint Security for Windows 說明文件）。

要新增元素作為排除，

選取偵測清單中的一或多個元素，然後點擊**排除**按鈕。

新增排除精靈啟動。遵照精靈的說明。

如果您拒絕或確認偵測，它將在下一次用戶端裝置與管理伺服器同步時被從偵測清單中排除，且它將不再出現在清單。

從適應性異常控制規則新增排除

「新增排除精靈」可讓您為 Kaspersky Endpoint Security for Windows 的自適應異常控制規則新增排除項目。

要透過適應性異常控制節點啟動新增排除精靈：

1. 在主功能表中，前往**操作 → 儲存區 → 智慧培訓狀態中的規則觸發**。

2. 在開啟的視窗中，選取偵測清單中的一或多個元素，然後點擊**排除**按鈕。
   您可以一次新增 1000 個排除項目。如果您選取更多元素且嘗試新增它們到排除，將顯示錯誤訊息。

新增排除精靈啟動。

政策和政策設定檔

在卡巴斯基安全管理中心雲端主控台中，您可以為 Kaspersky 應用程式建立政策。該部分描述了政策和政策設定檔，並提供建立和修改它們的說明。

關於政策

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

政策狀態

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

政策會根據以下規則執行：

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

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

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

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

政策設定檔會根據以下規則執行：

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

> 您無法建立管理伺服器政策。

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*。
Enforce	如果設定旁邊顯示關閉的鎖頭，並且啟用了切換按鈕，則該設定將套用於強制執行政策的裝置。使用者無法在受管理應用程式介面中修改這些設定的值。這些類型的設定稱為*鎖定*。

我們強烈建議您關閉要在受管理裝置上套用的政策設定的鎖定。解鎖的政策設定可以由卡巴斯基應用程式設定在受管理裝置上重新分配。

您可以使用鎖定按鈕執行以下操作：

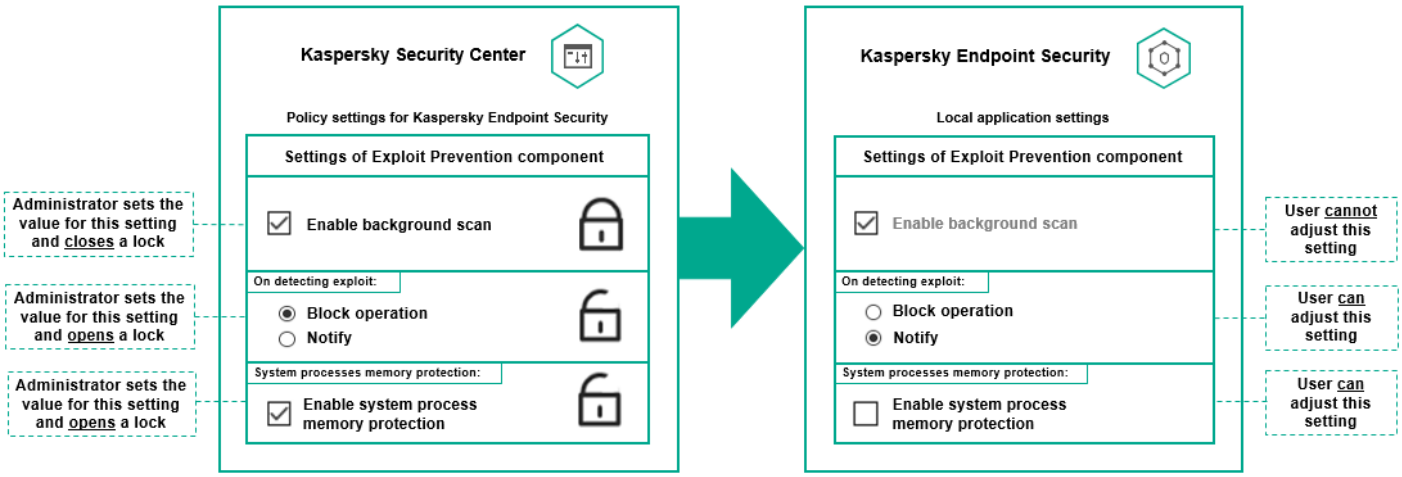
- 鎖定管理子群組政策的設定
- 在受管理裝置上鎖定卡巴斯基應用程式的設定

因此，鎖定設定可用於在受管理裝置上實作有效的設定。

有效設定的實作程序包括以下操作：

- 受管理裝置會套用卡巴斯基應用程式的設定值。
- 受管理裝置會套用政策的鎖定設定值。

政策和受管理卡巴斯基應用程式包含相同的設定集。配置政策設定時，卡巴斯基應用程式設定會變更受管理裝置上的值。您無法調整受管理裝置上的鎖定設定（請參閱下圖）：



鎖定和卡巴斯基應用程式設定

政策繼承和政策設定檔

本節提供政策和政策設定檔的階層和繼承資訊。

政策層級

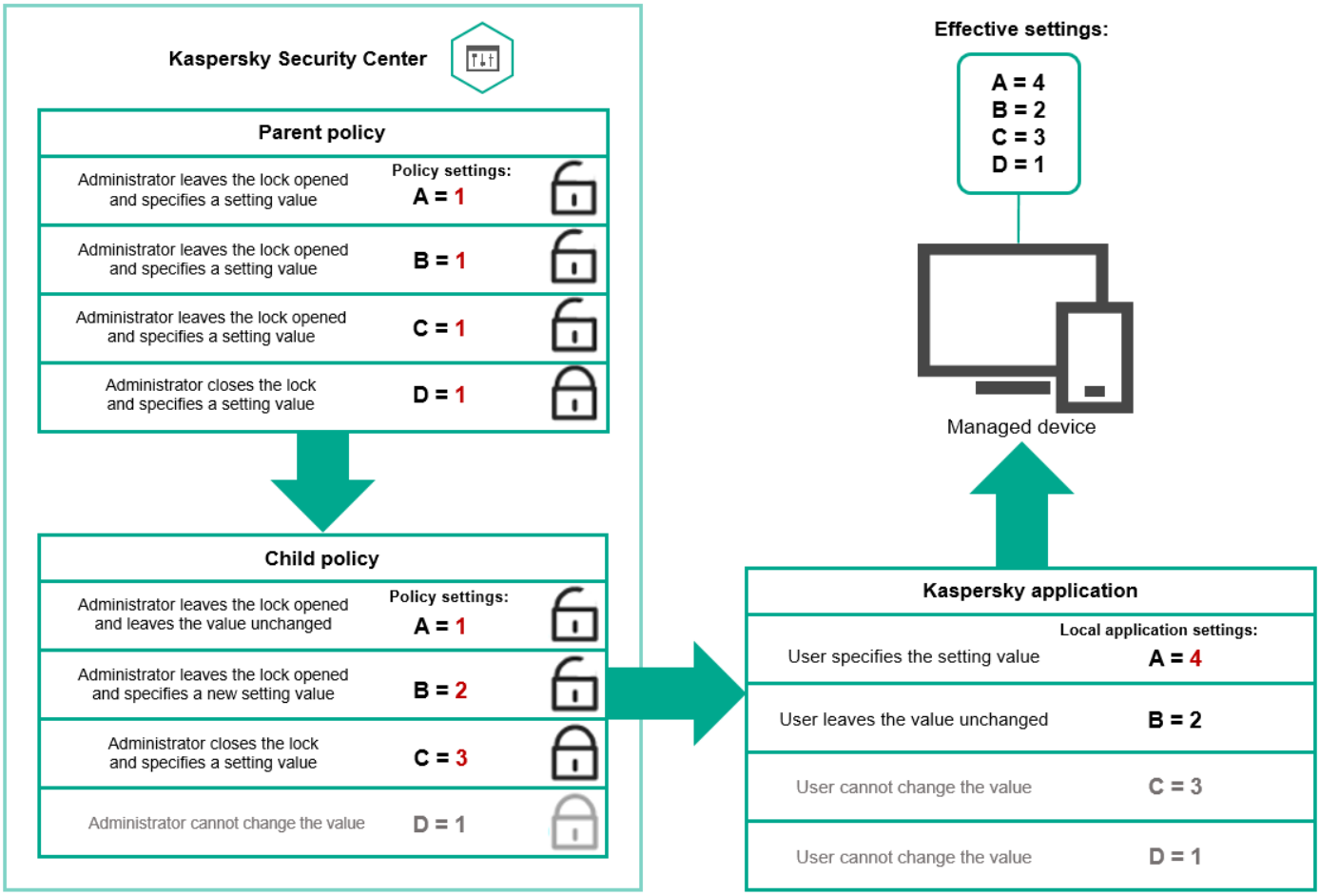
如果不同的裝置需要不同的設定，則可以將裝置組織到管理群組中。

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

根據管理群組的層次結構，相同應用程式的政策會互相作用。上級（父）管理群組政策的鎖定設定將重新分配子群組的政策設定值（請參閱下圖）。

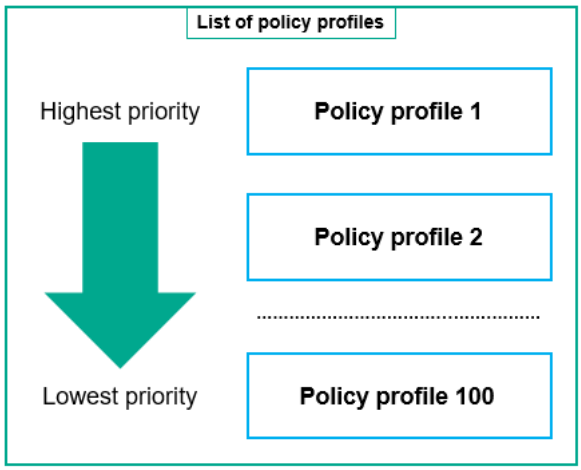


政策層級

政策層次結構中的政策設定檔

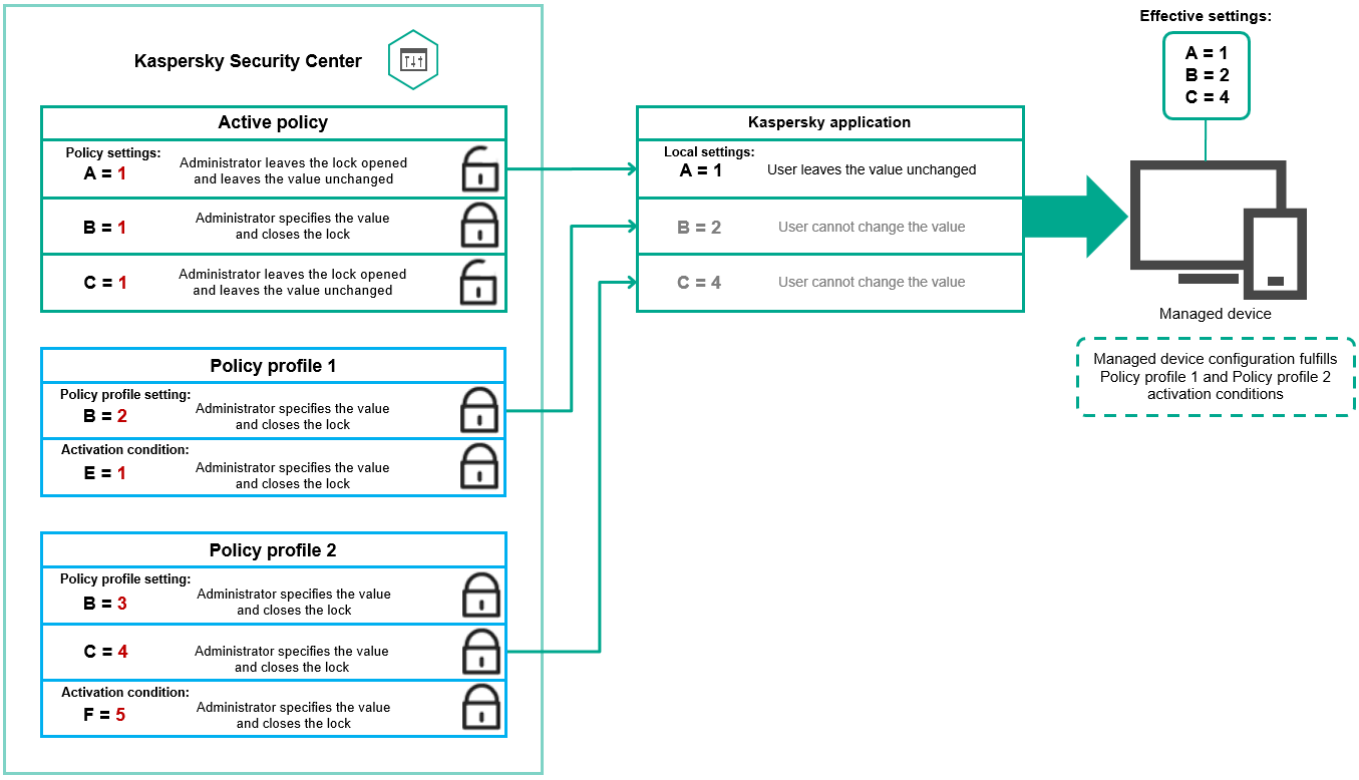
政策設定檔具有以下優先等級分配條件：

- 設定檔在政策設定檔清單中的位置指示其優先等級。您可變更政策設定檔的優先順序。清單中的最高位置表示最高優先等級（請參閱下圖）。



政策設定檔的優先等級定義

- 政策設定檔的啟動條件互不依賴。您可以同時啟動多個政策設定檔。如果多個政策設定檔影響相同設定，則裝置將從政策設定檔中取得具有最高優先等級的設定值（請參閱下圖）。



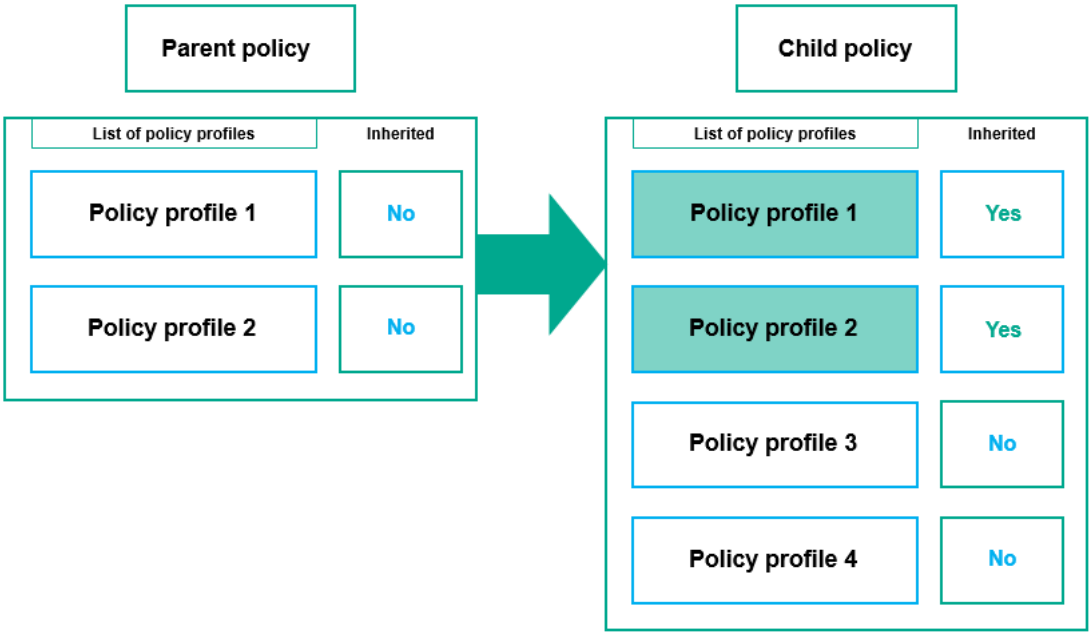
受管理裝置配置滿足幾個政策設定檔的啟動條件

繼承層次結構中的政策設定檔

來自不同層次結構層級政策的政策設定檔符合以下條件：

- 較低層級的政策從較高層級的政策繼承政策設定檔。從較高級政策繼承的政策設定檔比原始政策設定檔的層級具有更高的優先等級（請參閱下圖）。

- 您不能變更繼承之政策設定檔的優先等級（請參見下圖）。

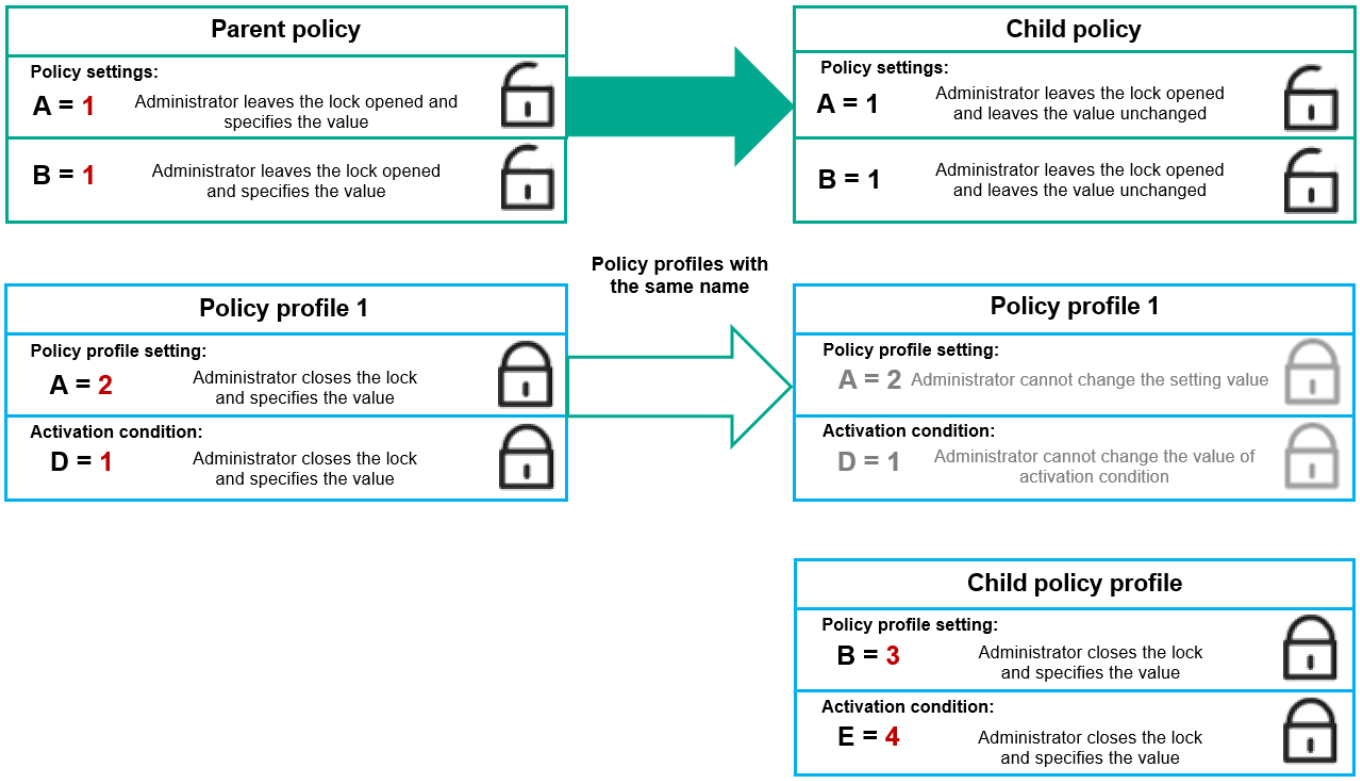


政策設定檔繼承

具有相同名稱的政策設定檔

如果在不同的層次結構層級中有兩個名稱相同的政策，則這些政策將根據以下規則執行：

- 上級政策設定檔的鎖定設定和設定檔啟動條件會變更下級政策設定檔的設定和設定檔啟動條件（請參閱下圖）。



子設定檔從父政策設定檔繼承設定值

- 上級政策設定檔的解鎖設定和設定檔啟動條件不會變更下級政策設定檔的設定和設定檔啟動條件。

如何在受管理裝置上實作設定

以下提供在受管理裝置上實作有效設定的說明：

- 所有未被鎖定的設定值都取自於政策。
- 然後，這將被受管理應用程式設定的值覆寫。
- 接著，將套用有效政策中被鎖定的設定值。鎖定的設定值會變更未鎖定的有效設定值。

管理政策

本節說明管理政策，並提供檢視政策清單、建立政策、修改政策、複製政策、移動政策、強制同步、檢視政策分發狀態圖，以及刪除政策的資訊。

檢視政策清單

您可以檢視為管理伺服器或任何管理群組建立的政策清單。

要檢視政策清單，請執行以下操作：

1. 在主功能表中，轉至 **資產（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。

> 您無法建立管理伺服器政策。

要建立政策：

1. 在主功能表中，轉至 **資產（裝置）→ 政策和設定檔**。
2. 點擊**新增**。
   選取應用程式視窗將開啟。
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**標籤。

   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。

   應用程式設定取決於您是為何種應用程式建立政策。如需詳細資訊，請參閱以下內容：

   - 管理伺服器配置
   - 網路代理政策設定
   - Kaspersky Endpoint Security for Windows 文件

   如需設定其他安全應用程式設定的詳細資訊，請參閱對應應用程至的文件。

   編輯設定時，您可點擊**取消**來取消最後的操作。

8. 點擊**儲存**儲存政策。

該政策將顯示在政策清單中。

修改政策

要修改政策：

1. 在主功能表中，轉至 **資產（裝置）→ 政策和設定檔**。

2. 點擊您要修改的政策。

   政策設定視窗隨即開啟。

3. 指定通用設定和為其建立政策的應用程式的設定。如需詳細資訊，請參閱以下內容：

   - 管理伺服器配置
   - 網路代理政策設定
   - Kaspersky Endpoint Security for Windows 文件

   如需設定其他安全應用程式設定的詳細資訊，請參閱對應應用程式的文件。

4. 點擊**儲存**。

對政策所做的變更將儲存在政策內容中，並且會顯示在**變更歷程**區段。

一般政策設定

一般

在**一般**頁籤，您可以修改政策狀態並指定政策設定的繼承方式：

- 在**政策狀態**區塊中，您可以選取一種政策模式：
  - **作用中**
  - **漫遊**

    如果選取該選項，政策將在裝置離開企業網路時變為啟用狀態。
  - **非作用中**

    如果選取該選項，政策將變為不啟用狀態，但它仍然儲存在**政策**資料夾中。如果需要，您可以啟動該政策。
- 在**設定繼承**設定群組中，您可以配置政策繼承：
  - **從父政策繼承設定**

    如果啟用此選項，則政策設定值將繼承上一級群組政策，因而會受到鎖定。

    預設情況下已啟用該選項。
  - **在子政策中強制繼承設定**

    如果啟用此選項，則在套用政策變更之後，程式將執行以下操作：
    - 政策設定的值將被傳送到管理子群組的政策，也就是子政策。
    - 在每個子政策內容視窗的**一般**區域的**設定繼承**區塊，系統將自動選取**從父政策繼承設定**核取方塊。

    如果啟用此方塊，則會鎖定子政策設定。

    預設情況下已停用該選項。

事件配置

事件配置區域可讓您設定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：

  - **儲存在管理伺服器資料庫上（天）**
  - **儲存在裝置的作業系統事件記錄中**

- **事件通知**

  您可以選取是否要透過電子郵件收到事件通知。

  預設情況下，將使用在管理伺服器內容標籤上指定的通知設定（例如收件者信箱等）。如有需要，您可以在**電子郵件**頁籤上變更這些設定。

變更歷程

變更歷程頁籤可讓您檢視政策修訂清單，並視需要復原對政策進行的變更。

啟用和停用政策繼承選項

若要啟用或停用政策中的繼承選項：

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

依預設，政策會啟用**從父政策繼承設定**選項。

如果政策有設定檔，所有子政策都會繼承這些設定檔。

複製政策

您可以從一個管理群組複製政策到另一個。

要複製政策到其他管理群組：

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

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

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

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

匯出政策

卡巴斯基安全管理中心雲端主控台可讓您將政策和其設定以及政策設定檔儲存到 KLP 檔案。您可以使用此 KLP 檔案匯入儲存的政策到 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux。

要匯出政策，請執行以下操作：

1. 在主功能表中，轉至 **資產（裝置）→政策和設定檔**。
2. 選取您要匯出之政策旁邊的核取方塊。

   您不能同時匯出多個政策。如果您選擇了多個政策，**匯出**按鈕將被停用。
3. 點擊**匯出**按鈕。
4. 在開啟的**另存新檔**視窗中，指定政策檔案的名稱和路徑。按一下**儲存**按鈕。

   另存新檔視窗僅當您使用 Google Chrome、Microsoft Edge 或 Opera 時才會顯示。如果您使用其他瀏覽器，政策檔案會自動儲存在**下載**資料夾。

匯入政策

卡巴斯基安全管理中心雲端主控台可讓您從 KLP 檔案匯入政策。KLP 檔案包含匯出的政策及其設定和政策設定檔。

要匯入政策，請執行以下操作：

1. 在主功能表中，轉至 **資產（裝置）→政策和設定檔**。
2. 點擊**匯入**按鈕。
3. 點擊**瀏覽**按鈕選擇要匯入的政策檔案。
4. 在開啟的視窗中，指定 KLP 政策檔案的路徑，然後按一下**開啟**按鈕。請注意，您只能選擇一個政策檔案。

   政策處理開始。
5. 政策處理完畢後，選擇要將政策套用到哪些管理群組。
6. 點擊**完成**按鈕以完成政策匯入。

此時會顯示匯入結果通知。如果政策匯入成功，您可以按一下**詳細資訊**連結以檢視政策內容。

匯入成功後，政策會顯示在政策清單中。政策的設定和設定檔也會一併匯入。無論匯出期間選取的政策狀態如何，匯入的政策都處於非使用中狀態。您可以在政策內容中變更政策狀態。

如果新匯入政策的名稱與現有政策的名稱相同，則匯入政策的名稱將加上 **(<next sequence number>)** 索引，例如：**(1)**、**(2)**。

檢視政策發佈狀態圖表

在卡巴斯基安全管理中心雲端主控台中，您可以透過政策發佈狀態圖表檢視每個裝置上的政策套用狀態。

要檢視每個裝置上的政策發佈狀態：

1. 在主功能表中，轉至 **資產（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. 在出現的功能表中，點擊**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> 分佈結果**視窗中，會顯示政策的**狀態敘述（如適用）**。

您可以使用政策分發變更清單中顯示的結果數量。裝置最高數量是 100,000。

若要使用政策發佈結果變更清單中顯示的裝置數量：

1. 在主功能表中，轉到您的帳戶設定，然後選擇**介面選項**。
2. 在**政策發佈結果中顯示的裝置上限**中，輸入裝置數量（最多 100,000）。
   預設情況下，數量為 5000。
3. 點擊**儲存**。

設定已儲存並套用。

在出現病毒爆發事件時自動啟用政策

要使政策在出現病毒爆發事件時自動啟用，請執行以下操作：

1. 在主功能表中，按一下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. 選擇**病毒爆發**區段。
3. 在右側面板中，點擊**配置在病毒爆發事件發生時要啟動的政策**連結。
   啟動政策視窗將開啟。
4. 在與偵測到病毒爆發的該元件相關區段中—適用於工作站與檔案伺服器的防毒軟體、適用於郵件伺服器的防毒軟體，或適用於週邊防護的防毒軟體—選取您要輸入項旁的選項按鈕，之後點擊**新增**。
   內含**受管理裝置**管理群組的視窗隨即開啟。
5. 點擊**受管理裝置**旁的 V 型圖示（ ）。
   管理群組層級和它們的政策被顯示。
6. 在管理群組層級和它們的政策中，點擊政策名稱或偵測到病毒爆發時啟動的政策的名稱。

要在清單或群組中選擇所有政策，選擇所需名稱旁邊的核取方塊。

7. 點擊**儲存**按鈕。

管理群組層級和它們的政策的視窗被關閉。

所選的政策被新增到偵測到病毒爆發時啟動的政策清單。所選政策在病毒爆發中被啟動，無論它們是活動的還是非活動的。

如果政策在病毒爆發事件中啟動，您僅可以使用手動模式返回到先前政策。

強制同步

儘管卡巴斯基安全管理中心雲端主控台會自動同步受管理裝置的狀態、設定、工作和政策，但有時候，您需要當下就確知是否已在指定的裝置上執行同步。

同步單一裝置

要強制同步管理伺服器和受管理裝置：

1. 在主功能表中，轉至 **資產（裝置）→ 受管理裝置**。
2. 點擊要與管理伺服器同步的裝置名稱。

政策內容視窗會開啟，並含有所選的**一般**區段。

3. 點擊**強制同步**按鈕。

應用程式將所選裝置與管理伺服器同步。

同步多部裝置

強制同步管理伺服器和受管理裝置：

1. 開啟管理群組的裝置清單或裝置分類：
   - 在主功能表中，前往**資產（裝置）→ 受管理裝置 → 群組**，然後選取要同步的裝置所在的管理群組。
   - 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，檢視上次連線管理伺服器的時間已針對選取的裝置變更為目前時間。若時間未變更，請點擊**重新整理**按鈕更新頁面內容。

所選裝置會與管理伺服器同步。

檢視政策交付的時間

在管理伺服器上變更 Kaspersky 應用程式適用的政策後，您可以檢查變更後的政策是否已傳輸到特定的受管理裝置中。政策可以在定期同步或者強制同步中傳輸。

若要檢視應用程式政策交付至受管理裝置的日期與時間：

1. 在主功能表中，轉至 **資產（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**標籤。
4. 選取您要檢視政策同步日期的應用程式。

應用程式政策視窗會開啟，並含有所選的**一般**區段，並且顯示政策交付日期與時間。

刪除政策

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

要刪除政策，請執行以下操作：

1. 在主功能表中，轉至 **資產（裝置）→ 政策和設定檔**。
2. 選取您要刪除之政策旁的核取方塊並點擊**刪除**。

   若您選取繼承的政策，則**刪除**按鈕會變成無法使用（暗顯）。
3. 點擊**確定**以確認操作。

政策連帶其所有設定檔被刪除。

管理政策設定檔

本節說明管理政策設定檔，並提供查看政策設定檔、更改政策設定檔優先等級、建立政策設定檔、修改政策設定檔、複製政策設定檔、建立政策設定檔啟動規則，以及刪除政策設定檔的資訊。

檢視政策設定檔

要檢視政策設定檔：

1. 在主功能表中，轉至 **資產（裝置）→ 政策和設定檔**。
2. 點擊您要檢視其設定檔的政策名稱。

政策內容視窗會開啟，並含有所選的**一般**頁籤。

3. 開啟**政策設定檔**頁籤。

政策設定檔清單以表格格式出現。如果政策沒有設定檔，將顯示空表。

變更政策設定檔優先順序

要變更政策設定檔優先順序：

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

所選政策設定檔的優先順序被變更並套用。

建立政策設定檔

要建立政策設定檔：

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

該設定檔顯示在政策設定檔清單中。

修改政策設定檔

只有 Kaspersky Endpoint Security for Windows 的政策才支援編輯政策設定檔。

修改政策設定檔：

1. 轉到您要的政策的設定檔清單。
   將出現政策設定檔清單。
2. 在**政策設定檔**頁籤，選取您要修改的政策設定檔。
   "政策設定檔"視窗開啟。
3. 在內容視窗中設定設定檔：
   - 如有需要，請在**一般**區域中變更設定檔名稱，並啟用或停用設定檔。
   - 編輯設定檔啟動規則。
   - 編輯應用程式設定。

   對於其他安全應用程式設定詳情，請參閱對應應用程式文件。
4. 點擊**儲存**。

您已變更的設定將在裝置與管理伺服器同步之後生效（如果政策設定檔處於活動狀態），或在啟動規則觸發後生效（如果政策設定檔處於非活動狀態）。

複製政策設定檔

您可以複製政策設定檔到目前政策或其他政策，例如，如果您要對不同政策擁有相同設定檔。您也可以使用複製，如果您想擁有兩個或更多僅在少數設定不同的設定檔。

要複製政策設定檔：

1. 轉到您要的政策的設定檔清單。
   將出現政策設定檔清單。如果政策沒有設定檔，將顯示空表。
2. 在**政策設定檔**頁籤，選取您要複製的政策設定檔。
3. 點擊**複製**。
4. 在開啟的視窗中，選取您要複製設定檔的政策。
   您可以複製政策設定檔到相同政策或您指定的政策。
5. 點擊**複製**。

   政策設定檔被複製到您選取的政策。新複製的設定檔具有最低優先順序。如果您複製設定檔到相同政策，新複製的設定檔名稱將附加（）索引，例如：（1）、（2）。

稍後，您可以變更設定檔設定，包括它的名稱和內容；原始政策設定檔此種情況下將不被變更。

建立政策設定檔啟動規則

要建立政策設定檔啟動規則：

1. 轉到您要的政策的設定檔清單。
   將出現政策設定檔清單。
2. 在**政策設定檔**頁籤，點擊您需在其中建立啟動規則的政策設定檔。
   如果政策設定檔清單為空，您可以建立政策設定檔。
3. 在**啟動規則**標籤上，點擊**新增**按鈕。
   政策設定檔啟動規則視窗開啟。
4. 指定規則的名稱。
5. 選取影響您目前建立的政策設定檔的啟動的條件的核取方塊：

   - **政策設定檔啟動一般規則**

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

     對於該選項，指定在下一步：

     - **裝置狀態**

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

     - **本裝置上已啟動管理伺服器連線規則**

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

   - **特別裝置所有者規則**
     對於該選項，指定在下一步：
     - **裝置所有者**

啟用此選項依據裝置所有者在其上設定和啟用設定檔啟動規則。在此方塊下的下拉清單，你可以選取設定檔啟動標準：

- 裝置屬於指定的擁有者（“=”符號）。
- 裝置不屬於指定的擁有者（"≠"符號）。

  請注意，使用者清單經過篩選，會顯示身分為內部使用者的裝置擁有者。

  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**

  啟用此選項後，可依裝置擁有者在卡巴斯基安全管理中心雲端主控台內部安全群組的成員資格，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）。
  - 裝置擁有者不是指定安全群組的成員（"≠"符號）。

    請注意，使用者清單經過篩選，會顯示身分為內部使用者的裝置擁有者。

    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雲端主控台的安全群組。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

- **硬體說明書規則**

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

  對於該選項，指定在下一步：

  - **記憶體大小 (MB)**

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

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

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

  - **邏輯處理器數量**

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

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

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

- **角色分配規則**

  對於該選項，指定在下一步：

  由裝置所有者特定角色啟動政策設定檔

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

  如果啟用該選項，設定檔根據配置的標準在裝置上啟動。

- **標籤使用規則**

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

  對於該選項，指定在下一步：

  - **標籤**

    在標籤清單中，透過選中與相應標籤對應的方塊，可以指定政策設定檔中的裝置包含規則。

    您可以透過清單上方的欄位新增新標籤到清單，並點擊**新增**按鈕。

    政策設定檔包含具有選定標籤的裝置。如果清除方塊，則將不套用該標準。預設情況下已清除這些方塊。

  - **套用到沒有指定標籤的裝置**

    如果您必須轉換您的標籤選項則啟用此選項。

    如果啟用此選項，政策設定檔將包含未帶有所選標籤的敘述的裝置。如果停用該選項，則不套用標準。

    預設情況下已停用該選項。

- **Active Directory 使用規則**

  選取該核取方塊依據裝置在 Active Directory 組織單元中的出現或者裝置在 Active Directory 安全性群組中的成員關係設定裝置上的政策設定檔啟動規則。

  對於該選項，指定在下一步：

  - **裝置所有者在 Active Directory 安全群組中的身分**

    如果啟用此選項，當裝置屬於指定的安全群組或指定安全群組的子群組時，裝置上的政策設定檔被啟動。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

  - **裝置列入 Active Directory 安全群組**

    如果選取此核取方塊，則會在裝置上啟動政策設定檔。如果停用此選項，則不套用設定檔啟動標準。預設情況下已停用該選項。

  - **在 Active Directory 組織單元中的裝置分配**

如果啟用此選項，包含在指定 Active Directory 組織單元 (OU) 中的裝置上的政策設定檔將會啟動。如果停用此選項，則不套用設定檔啟動標準。

預設情況下已停用該選項。

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

6. 檢查所配置參數的清單。若清單正確，請點擊**建立**。

設定檔將被儲存。當觸發啟動規則時，將在裝置上啟動該設定檔。

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

多個啟動規則可以被一起觸發。

刪除政策設定檔

要刪除政策設定檔：

1. 轉到您要的政策的設定檔清單。

   將出現政策設定檔清單。

2. 在**政策設定檔**頁籤上，選取要刪除之政策設定檔旁的核取方塊，接著點擊**刪除**。

3. 在開啟的視窗中，再次點擊**刪除**按鈕。

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

資料加密與防護

在筆記型電腦或硬碟磁碟機被竊取或遺失，或未經授權的使用者和應用程式存取資料時，資料加密能夠降低資料意外洩漏的風險。

以下 Kaspersky 應用程式支援加密：

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Mac

您可以使用使用者介面設定來顯示或隱藏與加密管理功能相關的某些介面元素。

Kaspersky Endpoint Security for Windows 中的資料加密

您可以在作為伺服器或工作站的 Windows 作業系統裝置上管理 BitLocker 磁碟機加密技術。

例如，透過使用這些 Kaspersky Endpoint Security for Windows 元件，您可以啟用或停用加密、檢視加密磁碟機清單、或產生和檢視有關加密的報告。

您可以透過在卡巴斯基安全管理中心雲端主控台中定義 Kaspersky Endpoint Security for Windows 的政策來設定加密。Kaspersky Endpoint Security for Windows 會根據使用的政策執行加密和解密。關於如何設定規則和加密功能說明的詳細說明，請參閱 Kaspersky Endpoint Security for Windows 說明。

Kaspersky Endpoint Security for Mac 中的資料加密

您可以在執行 macOS 的裝置上使用 FileVault 加密。在使用 Kaspersky Endpoint Security for Mac 時，您可以啟用或停用此加密。

您可以透過在卡巴斯基安全管理中心雲端主控台中定義 Kaspersky Endpoint Security for Mac 的政策來設定加密。Kaspersky Endpoint Security for Mac 將根據使用中的政策執行加密和解密。有關加密功能的詳細說明，請參閱 Kaspersky Endpoint Security for Mac 說明。

檢視加密磁碟機的清單

在卡巴斯基安全管理中心雲端主控台中，您可以檢視有關加密磁碟機和加密磁碟機所屬裝置的詳細資訊。磁碟機上的資訊解密後，該裝置會自動從該清單中移除。

檢視加密磁碟機的清單，

在主功能表中，轉至 **操作 → 資料加密與防護 → 加密磁碟機**。

如果功能表上沒有這個區段，表示它隱藏起來了。在使用者介面設定中，啟用**顯示資料加密與防護**選項即可顯示該區段。

匯出加密磁碟機清單為 CSV 或 TXT 檔案。為此，請點擊**匯出到 CSV**或**匯出到 TXT**按鈕。

建立和檢視加密報告

您可以建立以下報告：

- 受管理裝置加密狀態報告。此報告提供有關各種受管理裝置的資料加密詳細資訊。例如，該報告顯示套用已設定加密規則之政策的裝置數量。此外，您還可以找出需要重新啟動的裝置數量。該報告還包含每台裝置的加密技術和演算法相關資訊。
- 大容量儲存裝置加密狀態報告。此報告包含的資訊與受管理裝置加密狀態報告類似，但它僅提供大容量儲存裝置和卸除式磁碟機的資料。
- 加密磁碟機存取權限報告。此報告會顯示哪些使用者帳戶可以存取加密磁碟機。
- 檔案加密錯誤報告。此報告包含在裝置上執行資料加密或解密工作時所發生錯誤的相關資訊。
- 封鎖存取加密檔案的報告。該報告包含了封鎖應用程式存取加密檔案的資訊。如果未經授權的使用者或應用程式試圖存取加密檔案或磁碟機，則此報告很有用。

您可在**監控和報告 → 報告**區域中產生任何報告。或者，在**操作→資料加密與防護**區域中，您可以產生以下加密報告：

- 大容量儲存裝置加密狀態報告
- 加密磁碟機存取權限報告
- 檔案加密錯誤報告

*要在**資料加密與防護**部分產生加密報告：*

1. 請確保您在介面選項啟用了**顯示資料加密與防護**選項。
2. 在主功能表中，轉至 **操作 → 資料加密與防護**。
3. 開啟**加密磁碟機**區段，以產生大容量儲存裝置加密狀態報告或是加密磁碟機存取權限報告。
4. 按一下您要產生的報告名稱。

報告產生將開始。

以離線模式授予加密磁碟機的存取權限

使用者可要求對加密裝置的存取權限，例如，當 Kaspersky Endpoint Security for Windows 未安裝在受管理裝置時。收到要求後，您可建立存取金鑰檔案並將其傳送給使用者。所有使用案例和詳細指示都會在 Kaspersky Endpoint Security for Windows 說明中提供。

若要以離線模式授予加密磁碟機的存取權限：

1. 從使用者那裡取得要求存取檔案（副檔名為 FDERTC 的檔案）。按照 Kaspersky Endpoint Security for Windows 說明 中的指示，在 Kaspersky Endpoint Security for Windows 中產生該檔案。
2. 在主功能表中，轉至 **操作 → 資料加密與防護 → 加密磁碟機**。

   加密磁碟機清單隨即顯示。
3. 選取使用者要求存取權限的磁碟機。
4. 點擊**同意存取離線模式下的裝置**按鈕。
5. 在開啟的視窗中，選取對應 Kaspersky 應用程式用來加密已選取磁碟機的外掛程式。

   若磁碟機是以卡巴斯基安全管理中心雲端主控台不支援的 Kaspersky 應用程式加密，請使用基於 Microsoft Management Console 的管理主控台授予離線存取權限。
6. 按照 Kaspersky Endpoint Security for Windows 說明 提供的說明操作（請參閱本節最後的展開區塊）。

之後，使用者套用收到的檔案來存取加密磁碟機，並讀取儲存在磁碟機上的資料。

使用者和使用者角色

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

關於使用者帳戶

卡巴斯基安全管理中心雲端主控台可讓您管理使用者帳戶以及帳戶群組。該程式支援兩種帳戶類型：

- 組織員工的帳戶。在輪詢組織網路時管理伺服器擷取資料的本機使用者帳戶。
- 卡巴斯基安全管理中心雲端主控台內部使用者的帳戶。您可以在入口建立內部使用者的帳戶。這些帳戶僅供在卡巴斯基安全管理中心雲端主控台內使用。

要檢視使用者帳戶和安全群組表：

1. 在主功能表中，轉至**使用者和角色** → **使用者和群組**。
2. 選擇**使用者**或**群組**頁簽。

使用者或安全群組表將開啟。開啟的表格預設會依**子類型**和**已分配角色**欄受到篩選。表格中會顯示已分配角色的內部使用者或群組。

如果您想檢視僅包含本機使用者帳戶的表格，請將**子類型**篩選條件設定為**本機**。

如果您切換到從屬管理伺服器版本 14.2 或更早版本，然後開啟使用者或安全群組的清單，則開啟的表格僅會依**子類型**欄受到篩選。預設不會依**已分配角色**欄套用篩選。篩選後的表格會包含所有的內部使用者或安全群組（無論是否已分配角色皆然）。

新增內部使用者帳戶

如有需要，您可以在入口新增工作區的內部使用者。新增內部使用者後，您可以在卡巴斯基安全管理中心雲端主控台中向其分配角色。

關於用於角色

使用者角色（也叫*角色*）是包含一組權限集的物件。角色可以與安裝在使用者裝置上的 Kaspersky 應用程式設定關聯。您可以在管理伺服器階層中任何層級或在指定物件層級，指派角色給使用者集或安全群組集。

如果您透過包含虛擬管理伺服器的管理伺服器階層管理裝置，請注意您只能從實體管理伺服器建立、修改或刪除使用者角色。然後，您可以將使用者角色傳播到從屬管理伺服器，包括虛擬伺服器。

您可以關聯使用者角色到政策設定檔。若使用者獲派一個角色，此使用者會取得執行工作職能必要的安全設定。

一個使用者角色可以與特定管理群組中的裝置使用者關聯。

使用者角色範圍

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

使用角色的好處

使用角色的好處之一是您不必為每個受管理裝置或使用者指定安全設定。公司內使用者與裝置的數量可能很多，但不同的工作職能所需的不同安全設定則很小。

與使用政策設定檔的不同點

政策設定檔是為每個 Kaspersky 應用程式建立的政策的內容。角色與許多為不同應用程式建立的政策設定檔相關聯。因此，角色是聯合特定使用者類型的設定到一處的方法。

設定應用程式功能的存取權限。角色型存取控制

在控制對卡巴斯基安全管理中心雲端主控台功能與受管理 Kaspersky 應用程式功能的存取權限方面，卡巴斯基安全管理中心雲端主控台提供了基於角色的控制機制。

您可以透過以下其中一種方式，為卡巴斯基安全管理中心雲端主控台使用者設定對應用程式功能的存取權限：

- 透過為每個使用者或使用者群組單獨設定權限。
- 透過使用一群組預先定義的權限建立標準使用者角色並根據使用者的職責範圍將這些角色分配給使用者。

使用者角色的應用旨在簡化和縮短配置使用者對應應用程式功能存取權限的常規過程。角色內的存取權限根據標準工作和使用者的職責範圍設定。

可為使用者角色分配與其各自的目的對應的名稱。您可在程式中建立無限數量的角色。

您可以將預定義的使用者角色與已配置的一組權限一起使用，或者建立新角色並自己配置所需的權限。

應用程式功能的存取權

下表顯示使用卡巴斯基安全管理中心雲端主控台各功能時需要具備的存取權限，以便管理相關聯的工作、報告、設定以及執行相關聯的使用者操作。

要執行表中列出的使用者操作，使用者必須具有操作旁邊指定的權限。

讀取、**寫入**和**執行**權限適用於任何工作、報告或設定。除了這些權限外，使用者還必須具有**對裝置分類執行操作**的權限，才能管理裝置分類上的工作、報告或設定。

表中缺少的所有工作、報告、設定和安裝套件均屬於**一般功能：基本功能**的功能區域。

應用程式功能的存取權

功能區域	權限	使用者操作：執行操作所需的權限	工作	報告	其他
一般功能：對管理群組的管理功能	**寫入**	• 將裝置新增到管理群組：**寫入** • 從管理群組中刪除裝置：**寫入**	沒有	沒有	沒有

		• 將管理群組新增到另一個管理群組：**寫入** • 從另一個管理群組中刪除管理群組：**寫入**			
一般功能：存取物件而不考慮它們的 ACL	**讀取**	獲得對所有物件的存取權限：**讀取**	沒有	沒有	沒有
一般功能：基本功能	• **讀取** • **寫入** • **執行** • **對裝置分類執行操作**	• 虛擬伺服器的裝置移動規則（建立、修改或刪除）：**寫入**、**對裝置分類執行操作** • 取得行動 (LWNGT) 通訊協定自訂憑證：**讀取** • 設定行動 (LWNGT) 通訊協定自訂憑證：**寫入** • 獲取 NLA 定義的網路清單：**讀取** • 新增、修改或刪除 NLA 定義的網路清單：**寫入** • 檢視群組的存取控制清單：**讀取** • 檢視卡巴斯基事件日誌：**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」 • 「在從屬管理伺服器上遠端安裝應用程式」	• 「防護狀態報告」 • 「威脅報告」 • 「受感染最嚴重的裝置報告」 • 「病毒資料庫狀態報告」 • 「錯誤報告」 • 「網路攻擊報告」 • 「已安裝郵件系統保護應用程式的摘要報告」 • 「已安裝的外圍防禦應用程式的摘要報告」 • 「已安裝的應用程式類型概要報告」 • 「受感染的裝置使用者報告」 • 「安全問題報告」 • 「事件報告」	沒有

				• 「發佈點活動報告」 • 「從屬管理伺服器的報告」 • 「裝置控制事件報告」 • 「弱點報告」 • 「禁止的應用程式報告」 • 「Web 控制報告」 • 「受管理裝置加密狀態報告」 • 「大容量儲存裝置加密狀態報告」 • 「檔案加密錯誤報告」 • 「封鎖存取加密檔案的報告」 • 「加密磁碟機存取權限報告」 • 「有效使用者權限報告」 • 「權限報告」	
一般功能：**刪除的物件**	• **讀取** • **寫入**	• 檢視資源回收桶中已刪除的物件：**讀取** • 從資源回收桶中刪除物件：**寫入**	沒有	沒有	沒有
一般功能：**事件處理**	• **刪除事件**	• 變更事件註冊設定：**編輯事件記錄設定**	沒有	沒有	設定： • 病毒爆發設定：建立病

	• **編輯事件通知設定** • **編輯事件記錄設定** • **寫入**	• 變更事件通知設定：**編輯事件通知設定** • 刪除事件：**刪除事件**			毒爆發事件所需的病毒偵測次數 • 病毒爆發設定：評估病毒偵測的時段 • 儲存在資料庫中的最大事件數量 • 儲存已刪除裝置中的事件時段
一般功能：**Kaspersky 軟體部署**	• **管理 Kaspersky 修補程式** • **讀取** • **寫入** • **執行** • **對裝置分類執行操作**	核准或拒絕安裝修補程式：**管理 Kaspersky 修補程式**	沒有	• 「虛擬管理伺服器產品授權金鑰使用報告」 • 「Kaspersky 軟體版本報告」 • 「不相容的應用程式報告」 • 「Kaspersky 軟體模組更新版本報告」 • 「防護部署報告」	安裝套件：「Kaspersky」
一般功能：**產品授權金鑰管理**	• **匯出金鑰檔案** • **寫入**	• 匯出金鑰檔案：**匯出金鑰檔案** • 修改管理伺服器產品授權金鑰設定：**寫入**	沒有	沒有	沒有
一般功能：**強制報告管理**	• **讀取** • **寫入**	• 建立報告，而不考慮其 ACL：**寫入** • 不論報告的 ACL 為何都加以執行：**讀取**	沒有	沒有	沒有
一般功能：**管理伺服器的階**	**配置管理伺服器的階層**	註冊、更新或刪除從屬管理伺服器：**配置**	沒有	沒有	沒有

層		**管理伺服器的階層**			
一般功能：使用者權限	**修改物件 ACL**	• 變更任何物件的「安全性」屬性：**修改物件 ACL** • 管理使用者角色：**修改物件 ACL** • 管理內部使用者：**修改物件 ACL** • 管理安全群組：**修改物件 ACL** • 管理別名：**修改物件 ACL**	沒有	沒有	沒有
一般功能：虛擬管理伺服器	• **管理虛擬管理伺服器** • **讀取** • **寫入** • **執行** • **對裝置分類執行操作**	• 取得理虛擬管理伺服器的清單：**讀取** • 取得虛擬管理伺服器的資訊：**讀取** • 建立、更新或刪除虛擬管理伺服器：**管理虛擬管理伺服器** • 將虛擬管理伺服器移動到另一個群組：**管理虛擬管理伺服器** • 設定管理虛擬伺服器權限：**管理虛擬管理伺服器**	沒有	「協力廠商軟體更新安裝結果報告」	沒有
一般功能：加密金鑰管理	**寫入**	匯入加密金鑰：**寫入**	沒有	沒有	沒有
系統管理：連線性	• **開始 RDP 工作階段** • **連線到現有的 RDP 工作階段** • **啟動通道建立功能** • **將來自裝置的檔案儲存到管理員的工作站**	• 建立桌面共用工作階段：**建立桌面共用工作階段的權限** • 建立 RDP 工作階段：**連線到現有的 RDP 工作階段** • 建立通道：**啟動通道建立功能** • 儲存內容網路清單：**將來自裝置的檔案儲存到管理員的工作站**	沒有	「裝置使用者報告」	沒有

	• **讀取** • **寫入** • **執行** • **對裝置分類執行操作**				
系統管理：**硬體詳細目錄**	• **讀取** • **寫入** • **執行** • **對裝置分類執行操作**	• 取得或匯出硬體詳細目錄物件：**讀取** • 新增、設定或刪除硬體詳細目錄物件：**寫入**	沒有	• 「硬體登錄資料的報告」 • 「組態更改的報告」 • 「硬體報告」	沒有
系統管理：**網路存取控制**	• **讀取** • **寫入**	• 檢視 CISCO 設定：**讀取** • 更改 CISCO 設定：**寫入**	沒有	沒有	沒有
系統管理：**作業系統部署**	• **部署 PXE 伺服器** • **讀取** • **寫入** • **執行** • **對裝置分類執行操作**	• 部署 PXE 伺服器：**部署 PXE 伺服器** • 檢視 PXE 伺服器清單：**讀取** • 在 PXE 用戶端上啟動或停止安裝程序：**執行** • 管理 WinPE 和作業系統映像的驅動程式：**寫入**	「在參考裝置作業系統映像上建立安裝套件」	沒有	安裝套件：「作業系統映像檔」
系統管理：**弱點和修補程式管理**	• **讀取** • **寫入** • **執行** • **對裝置分類執行操作**	• 檢視協力廠商修補程式屬性：**讀取** • 更改協力廠商修補程式屬性：**寫入**	• 「執行 Windows Update 同步」 • 「安裝 Windows Update 更新」 • 「修復弱點」	「軟體更新報告」	沒有

			• 「安裝必要更新並修復弱點」		
系統管理：**遠端安裝**	• **讀取** • **寫入** • **執行** • **對裝置分類執行操作**	• 檢視協力廠商弱點和修補程式管理的安裝套件屬性：**讀取** • 更改協力廠商弱點和修補程式管理的安裝套件屬性：**寫入**	沒有	沒有	安裝套件： • 「自訂應用程式」 • 「VAPM 套件」
系統管理：**軟體詳細目錄**	• **讀取** • **寫入** • **執行** • **對裝置分類執行操作**	沒有	沒有	• 「已安裝應用程式的報告」 • 「應用程式登錄資料歷程報告」 • 「已授權應用程式群組狀態報告」 • 「協力廠商軟體產品授權金鑰報告」	沒有

預先定義的使用者角色

向卡巴斯基安全管理中心雲端主控台使用者分配使用者角色，可讓使用者對應用程式功能具備一組存取權限。

在虛擬伺服器上建立的使用者，在管理伺服器上無法被分配到角色。

您可以將預定義的使用者角色與已配置的一組權限一起使用，或者建立新角色並自己配置所需的權限。卡巴斯基安全管理中心雲端主控台中提供的一些預先定義的使用者角色可能會與特定職位相關聯，例如**稽核員**、**安全官**、**管理者**（這些角色自卡巴斯基安全管理中心雲端主控台版本 11 起即已存在）。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**寫入**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	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

者	管理員。
安全官	允許所有檢視操作，允許報告管理；在**系統管理**：**連線**區域授予有限的權限。您可以分配該角色到負責您組織的 IT 安全的安全官。

下表顯示指派給每個預先定義使用者角色的存取權限。

預先定義使用者角色的存取權限

角色	敘述

管理伺服器管理員	允許在以下功能區域中進行所有操作：
	• **一般功能**：
	  • **基本功能**
	  • **事件處理**
	  • **管理伺服器階層**
	  • **虛擬管理伺服器**
	• **系統管理**：
	  • **連線**
	  • **硬體清單**
	  • **軟體清查**
	在**一般功能：加密金鑰管理**功能區域中授予**讀取**和**寫入**權限。

管理伺服器憑證運算子	授予以下所有功能區域的**讀取**和**執行**權限：
	• **一般功能**：
	  • **基本功能**
	  • **虛擬管理伺服器**
	• **系統管理**：
	  • **連線**
	  • **硬體清單**
	  • **軟體清查**

稽核員	允許在以下功能區域中進行所有操作，在**一般功能**： • **存取物件而不考慮它們的 ACLs** • **刪除物件** • **強制報告管理** 您可以分配該角色到執行您組織的稽核的人。

安裝管理員	允許在以下功能區域中進行所有操作：
	• **一般功能**：
	  • **基本功能**
	  • **Kaspersky 軟體部署**
	  • **產品授權金鑰管理**
	• **系統管理**：
	  • **作業系統部署**
	  • **弱點和修補程式管理**
	  • **遠端安裝**
	  • **軟體清查**
	在**一般功能：虛擬管理伺服器**功能區域中授予**讀取**和**執行**權限。

安裝運算子	授予以下所有功能區域的**讀取**和**執行**權限：
	• **一般功能**：
	  • **基本功能**
	  • **Kaspersky 軟體佈署**（也會在此區域授予**管理 Kaspersky 修補程式**權限）
	  • **虛擬管理伺服器**
	• **系統管理**：
	  • **作業系統部署**
	  • **弱點和修補程式管理**
	  • **遠端安裝**
	  • **軟體清查**

Kaspersky Endpoint Security 管理員	允許在以下功能區域中進行所有操作： • **一般功能：基本功能** • Kaspersky Endpoint Security 區域，包括所有功能 在**一般功能：加密金鑰管理**功能區域中授予**讀取**和**寫入**權限。
Kaspersky Endpoint Security 運算子	授予以下所有功能區域的**讀取**和**執行**權限： • **一般功能：基本功能** • Kaspersky Endpoint Security 區域，包括所有功能
主要管理員	允許在各功能區域內進行所有操作，但這*不包括***一般功能**中的以下區域： • **存取物件而不考慮它們的 ACLs**

	• **強制報告管理** 在**一般功能：加密金鑰管理**功能區域中授予**讀取**和**寫入**權限。

主要運算子	授予以下所有功能區域的**讀取**和**執行**（如適用）權限：
	• **一般功能**：
	  • **基本功能**
	  • **刪除物件**
	  • **管理伺服器上的操作**
	  • **Kaspersky 軟體佈署**
	  • **虛擬管理伺服器**
	• **行動裝置管理：一般**
	• **系統管理**，包括所有功能
	• Kaspersky Endpoint Security 區域，包括所有功能

行動裝置管理管理員	允許在以下功能區域中進行所有操作： • **一般功能：基本功能** • **行動裝置管理：一般**
行動裝置管理運算子	在**一般功能**：**基本功能**的功能區域中授予**讀取**和**執行**權限。 在**行動裝置管理**：**一般**功能區域中授予**讀取**和**僅向行動裝置傳送資訊命令**。
安全官	允許在以下功能區域中進行所有操作，在**一般功能**： • **存取物件而不考慮它們的 ACLs** • **強制報告管理** 在**系統管理：連線**功能區域中，授予**讀取**、**寫入**、**執行**、**將來自裝置的檔案儲存到管理員的工作站**以及**對裝置分類執行操作**的權限。 您可以分配該角色到負責您組織的 IT 安全的安全官。
高級安全分析師	在**一般功能**：**基本功能**功能區域中授予**讀取**權限。 在**系統管理：連線**功能區域中，授予**讀取**、**寫入**、**執行**、**將來自裝置的檔案儲存到管理員的工作站**以及**對裝置分類執行操作**的權限。 授予對 Kaspersky Endpoint Detection and Response Expert 解決方案的存取權限。
自助服務入口使用者	允許**行動裝置管理：自助服務入口**功能區域中的所有操作。此功能在卡巴斯基安全管理中心 11 和以上版本中不受支援。
管理者	授予在**一般功能**：**存取物件而不考慮它們的 ACL** 與**一般功能**：**強制報告管理**功能區域中的**讀取**權限。 您可以分配該角色到負責您組織的 IT 安全的安全官和其他管理員。
弱點和修補程式管理管理員	允許在**一般功能**：**基本功能**與**系統管理**（包括所有功能）功能區域中的所有操作。

弱點和修補程式管理操作者	授予在**一般功能**：**基本功能**和**系統管理**（包括所有功能）功能區域中的**讀取**和**執行**權限（如適用）。

為特定物件分配存取權限

除了分配伺服器層級的存取權限，您可以設定對特定物件的存取，例如，對特定工作的存取。該應用程式允許您指定對以下物件類型的存取權限：

- 管理群組
- 工作
- 報告
- 裝置分類
- 事件分類

若要為特定物件分配存取權限：

1. 根據物件類型，在主功能表中，轉至相對應的部分：
   - **資產（裝置）→ 群組的階層**
   - **資產（裝置）→工作**
   - **監控和報告→報告**
   - **資產（裝置）→裝置分類**
   - **監控和報告 → 事件分類**
2. 開啟物件的內容，以將存取權限指派給物件。

   要開啟管理群組或工作的內容視窗，請按一下物件名稱。您可以使用工具列上的按鈕開啟其他物件的內容。
3. 在內容視窗中，開啟**存取權限**部分。

   使用者清單開啟。列出的使用者和安全群組具有物件的存取權限。預設情況下，如果您使用管理群組或伺服器的階層，則清單和存取權限是從父管理群組或主伺服器繼承的。
4. 為了能夠修改清單，啟用**使用自訂權限**選項。
5. 設定存取權限：
   - 使用**新增**和**刪除**按鈕修改清單。
   - 指定使用者或安全群組的存取權限。執行以下操作之一：
     - 如果要手動指定存取權限，請選擇使用者或安全群組，按一下**存取權限**按鈕，然後指定存取權限。
     - 如果你想分配使用者角色到使用者或安全群組，請選擇使用者或安全群組，按一下**角色**按鈕，然後選擇要分配的角色。

6. 點擊**儲存**按鈕。

物件的存取權限已設定好。

為使用者或安全群組分配角色

對使用者或安全群組分配角色：

1. 在主功能表中，轉至**使用者和角色→使用者和群組**，然後選擇**使用者**或**群組**頁簽。
2. 選擇要對其分配角色的使用者或安全群組的名稱。

   您可以選取多個名稱。
3. 在功能表行中，點擊**分配角色**按鈕。

   角色分配精靈啟動。
4. 按照精靈的說明進行操作：選擇要分配給所選使用者或安全群組的角色，然後選擇角色的範圍。

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

擁有處理管理伺服器權限集合的角色將被指派給使用者（或者多個使用者，或者安全群組）。在使用者或安全群組清單中，**已分配角色**列中會出現一個核取方塊。

建立使用者角色

要建立使用者角色：

1. 在主功能表中，轉至 **使用者和角色 → 角色**。
2. 點擊**新增**。
3. 在開啟的**新角色名稱**視窗中，輸入新角色的名稱。
4. 點擊**確定**以套用變更。
5. 在開啟的角色內容視窗中，變更角色設定：
   - 在**一般**頁籤，編輯角色名稱。

     您無法編輯預定義角色名稱。
   - 在**設定**頁籤，編輯角色範圍和政策以及與角色相關的設定檔。
   - 在**存取權限**頁籤，編輯存取 Kaspersky 應用程式的權限。
6. 點擊**儲存**以儲存變更。

新角色出現在使用者角色清單。

編輯使用者的存取權限

您可以編輯使用者對以下物件的存取權限：

- 管理伺服器
- 管理群組
- 工作
- 報告
- 事件分類
- 裝置分類

若要編輯使用者的存取權限：

1. 前往所選物件的**存取權限**頁籤。
2. 選取要編輯存取權限的使用者。

   如果您選取了自己的使用者帳戶，您無法撤銷自己的存取權限。變更將不會儲存。

3. 點擊**存取權限**按鈕。
4. 在開啟的視窗中，編輯所選使用者的存取權限。
5. 點擊**確定**按鈕。

該使用者的存取權限即已變更。

編輯使用者角色

要編輯使用者角色：

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

更新的角色出現在使用者角色清單。

編輯使用者角色範圍

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

若要將使用者、使用者群組和管理群組新增到使用者角色的涵蓋範圍中，您可以使用以下任一方法：

方法 1：

1. 在主功能表中，轉至**使用者和角色→使用者和群組**，然後選擇**使用者**或**群組**頁簽。
2. 選取您要新增到使用者角色涵蓋範圍中的使用者或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**按鈕以關閉視窗。

所選的使用者（或使用者群組）以及所選的管理群組即會新增到使用者角色的涵蓋範圍中。

方法 2：

1. 在主功能表中，轉至 **使用者和角色 → 角色**。
2. 按一下您要定義範圍的角色名稱。
3. 在開啟的角色內容頁面中，選擇**設定**頁籤。
4. 在**角色範圍**區段中，點擊**新增**。
   角色分配精靈啟動。使用**下一步**按鈕進行精靈。
5. 在精靈的**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中的使用者和使用者群組。
7. 點擊**分配角色**按鈕以關閉視窗。
8. 關閉角色內容視窗。

所選的使用者（或使用者群組）以及所選的管理群組即會新增到使用者角色的涵蓋範圍中。

刪除使用者角色

要刪除使用者角色：

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

使用者角色被刪除。

關聯政策設定檔到角色

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

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

要關聯角色到政策設定檔：

1. 在主功能表中，轉至 **使用者和角色 → 角色**。
2. 選取您要關聯政策設定檔的角色名稱。
   角色內容視窗會開啟，並含有所選的**一般**頁籤。
3. 選取**設定**頁籤，之後向下捲動至**政策和設定檔**區段。
4. 點擊**編輯**。
5. 要關聯角色到：
   - **現有政策設定檔**—點擊所學政策名稱旁邊的臂章圖示（ > ），然後選取您要關聯角色的設定檔旁邊的核取方塊。
   - **新政策設定檔**：
     a. 選取您要建立設定檔的政策旁邊的核取方塊。
     b. 點擊**新政策設定檔**。
     c. 為新設定檔指定名稱並配置設定檔設定。
     d. 點擊**儲存**按鈕。
     e. 選取新設定檔旁邊的核取方塊。
6. 點擊**分配到角色**。

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

建立安全群組

要建立安全群組：

1. 在主功能表中，轉至**使用者和角色** → **使用者和群組**，然後選擇**群組**頁簽。
2. 點擊**新群組**。
3. 在**新群組**視窗中，為新的安全群組指定以下設定：
   - **名稱**
   - **敘述**
4. 點擊**確定**儲存變更。

新的安全群組即已新增到安全群組清單中。

編輯安全群組

要編輯安全群組：

1. 在主功能表中，轉至**使用者和角色** → **使用者和群組**，然後選擇**群組**頁簽。
2. 點擊您要編輯的安全群組名稱。
3. 在開啟的群組設定視窗中，變更安全群組設定：
   - 在**一般**頁簽上，您可以變更**名稱**和**敘述**設定。這些設定僅適用於內部安全群組。
   - 在**使用者**頁籤，您可新增使用者至安全群組。此設定僅適用於內部使用者和內部安全群組。
   - 在**角色**頁籤，您可指派角色給安全群組。
4. 點擊**儲存**以儲存變更。

變更被套用於安全群組。

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** → **使用者和群組**，然後選擇**使用者**頁簽。
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。您還可以使用群組設定，將內部使用者新增到群組。

刪除安全群組

您僅可以刪除內部安全群組。

若要刪除使用者群組：

1. 在主功能表中，轉至**使用者和角色** → **使用者和群組**，然後選擇**群組**頁簽。
2. 選取您要刪除的使用者群組旁邊的核取方塊。
3. 點擊**刪除**，然後在開啟的視窗中確認刪除。

該使用者群組即會刪除。

設定 ADFS 整合

若要讓在組織中的 Active Directory (AD) 中註冊的使用者能夠登入卡巴斯基安全管理中心雲端主控台，您必須設定與 Active Directory 同盟服務 (ADFS) 的整合。

卡巴斯基安全管理中心雲端主控台支援 ADFS 3 (Windows Server 2016) 或以上版本。

若要變更 ADFS 整合設定，您必須具有變更使用者權限的存取權限。

在繼續之前，請先確認您已完成 Active Directory 輪詢。

若要設定 ADFS 整合：

1. 在主功能表中，按一下管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取 **ADFS 整合設定**區段。
3. 複製回撥 URL。

您將需要有該 URL，才能在 ADFS 管理主控台中設定整合。

4. 在 ADFS 管理主控台中，新增應用程式群組，然後選取 **Server application** 範本（Microsoft 介面元素是顯示英文名稱）來新增應用程式。

   ADFS 管理主控台即會為新的應用程式產生用戶端 ID。您將需要有該用戶端 ID，才能在卡巴斯基安全管理中心雲端主控台中設定整合。

5. 在重新導向 URI 部分，指定您在管理伺服器內容視窗中複製的回撥 URL。

6. 產生用戶端密碼。您將需要有該用戶端密碼，才能在卡巴斯基安全管理中心雲端主控台中設定整合。

7. 儲存所新增應用程式的內容。

8. 將新的應用程式新增到建立的應用程式群組中。這次請選取 **Web API** 範本。

9. 在 **Identifiers** 頁籤的 **Relying party identifiers** 清單中，新增您稍早所新增伺服器應用程式的用戶端 ID。

10. 在 **Client Permissions** 頁籤的 **Permitted scopes** 清單中，選取 **allatclaims** 和 **openid** 涵蓋範圍。

11. 在 **Issuance Transform Rules** 頁籤，選取 **Send LDAP Attributes as Claims** 範本來新增規則：

    a. 為規則命名。例如，您可以將其命名為「Group SID」。

    b. 選取 **Active Directory** 作為屬性儲存區，然後以 LDAP 屬性的形式將 **Token-Groups as SIDs** 對應到「Group SID」作為連出的宣告類型。

12. 在 **Issuance Transform Rules** 頁籤，選取 **Send Claims Using a Custom Rule** 範本來新增規則：

    a. 為規則命名。例如，您可以將其命名為「ActiveDirectoryUserSID」。

    b. 在 **Custom rule** 欄位中，輸入：

    ```
    c:[Type ==
    "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
    Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types =
    ("http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"), query =
    ";objectSID;{0}", param = c.Value);
    ```

13. 在卡巴斯基安全管理中心雲端主控台中，再次開啟 **ADFS 整合設定**區段。

14. 將切換按鈕切換到 **ADFS 整合 已啟用**位置。

15. 點擊**設定**連結，然後指定含有同盟伺服器一或多個憑證的檔案。

16. 點擊 **ADFS 整合設定**連結，然後指定以下設定：

- **簽發者 URL**

  在您組織中運作的同盟伺服器本身的 URL 位址。

  具體而言，卡巴斯基安全管理中心雲端主控台會在簽發者 URL 位址中加上「/.well-known/openid-configuration」，然後嘗試開啟得到的 URL 位址 (issuer_URL/.well-known/openid-configuration)，以便自動發現簽發者設定。

- **用戶端 ID**

同盟伺服器所產生用於識別卡巴斯基安全管理中心雲端主控台的用戶端 ID。您可以在 ADFS 管理主控台中與卡巴斯基安全管理中心雲端主控台相對應的伺服器應用程式本身的內容視窗內，找到用戶端 ID。

- **用戶端密碼**

  您是在 ADFS 管理主控台中指定與卡巴斯基安全管理中心雲端主控台相對應的伺服器應用程式本身的內容時，產生用戶端密碼。

- **對使用者進行身分驗證的網域**

  您所選網域的成員將能夠使用其網域帳戶憑證登入卡巴斯基安全管理中心雲端主控台。網域名稱會在您完成網路輪詢後，出現在清單中。

- **ID 權杖中使用者 SID 的欄位名稱**

  ID 權杖中引用了使用者 SID 的欄位本身的名稱。需要有該欄位名稱，才能在卡巴斯基安全管理中心雲端主控台中識別使用者。在 ID 權杖中，該欄位預設名為「primarysid」。

- **ID 權杖中使用者群組的 SID 陣列的欄位名稱**

  引用了使用者所屬 Active Directory 安全群組 SID 陣列的欄位本身的名稱。在 ID 權杖中，該欄位預設名為「groupsid」。

17. 點擊**儲存**按鈕。

與 ADFS 的整合程序即告完成。若要使用 AD 帳戶憑證登入卡巴斯基安全管理中心雲端主控台，請使用 **ADFS 整合設定**區段中提供的連結（**含有 ADFS 的 Kaspersky Security Center Cloud Console 的登入連接**）。

當您首次透過 ADFS 登入卡巴斯基安全管理中心雲端主控台時，主控台的回應速度可能會較慢。

指派使用者作為裝置所有者

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

要指派使用者作為裝置所有者：

1. 如果要指派連線到虛擬管理伺服器的裝置所有者，請先切換到虛擬管理伺服器：
   a. 在主功能表中，按一下目前管理伺服器名稱右側的 v 形箭號圖示（ ）。
   b. 選取所需的管理伺服器。
2. 在主功能表中，轉至**使用者和角色 → 使用者和群組**，然後選擇**使用者**頁簽。

使用者清單開啟。如果您目前已連線到虛擬管理伺服器，該清單會包括來自目前虛擬管理伺服器和主管理伺服器的使用者。

3. 按一下您要指派為裝置所有者的使用者帳戶名稱。

4. 在開啟的使用者設定視窗中，選擇**裝置**頁籤。

5. 點擊**新增**。

6. 從裝置清單中，選取您要分配給使用者的裝置。

7. 點擊**確定**。

所選的裝置被新增到分配給使用者的裝置清單。

您可在**資產（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。

管理物件修訂

該區域包含了物件修訂管理的資訊。

支援修訂管理的物件包括：

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

關於物件修訂

卡巴斯基安全管理中心雲端主控台可讓您追蹤物件修改歷程。您每次儲存變更到物件時，*修訂*被建立。每個修訂都有一個數字。

您可以對物件修訂採取以下操作：

- 檢視所選修訂
- 回溯對物件所做的變更到所選的修訂

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

- 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。若要為某次修訂新增說明，請選取該修訂，然後點擊**編輯描述**按鈕。在開啟的視窗中，輸入一些文字作為修訂說明。

回溯變更

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

要回溯對物件所做的變更：

1. 前往物件的**變更歷程**區段。
2. 在物件修訂清單中，選取您要回溯的修訂號。
3. 點擊**回溯**按鈕。

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

新增修訂敘述

您可以為修訂新增敘述以簡化在清單中的修訂搜尋。

要新增修訂敘述：

1. 前往物件的**變更歷程**區段。
2. 在物件修訂清單中，選取您想要新增敘述的修訂。
3. 點擊**編輯描述**按鈕。
4. 在開啟的視窗中，輸入一些文字作為修訂說明。

   預設下，物件修訂敘述為空。
5. 點擊**儲存**。

新的說明即會顯示在修訂歷程記錄表的**敘述**欄位中。

物件刪除

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。

關於刪除用戶端裝置

當您從管理群組中刪除受管理裝置時，應用程式會將裝置移至未分配的裝置群組。刪除裝置後，已安裝的卡巴斯基應用程式——網路代理和任何安全應用程式，例如 Kaspersky Endpoint Security——將保留在裝置上。

卡巴斯基安全管理中心雲端主控台會依以下規則處理「未配置的裝置」群組中的裝置：

- 如果您配置了裝置移動規則，並且裝置符合移動規則的條件，則該裝置會被根據規則自動移動到管理群組。
- 裝置會被儲存在未分配的裝置群組中，並被根據裝置保留規則自動從群組中刪除。

  裝置保留規則不會影響具有一個或多個使用完整磁碟加密進行加密的磁碟機的裝置。此類裝置不會被自動刪除——您只能手動刪除它們。如果您需要刪除帶有加密磁碟機的裝置，請先解密磁碟機，然後再刪除該裝置。

  當您刪除帶有加密磁碟機的裝置時，解密磁碟機所需的資料也會被刪除。在這種情況下，要解密磁碟機，必須滿足以下條件：

  - 裝置被重新連線到管理伺服器以還原解密磁碟機所需的資料。
  - 裝置使用者記得解密密碼。
  - 用於加密磁碟機的安全應用程式（例如 Kaspersky Endpoint Security for Windows）仍安裝在裝置上。

  如果磁碟機由 Kaspersky Disk Encryption 技術加密，您還可以嘗試使用 FDERT Restore Utility 還原資料.

當您從未分配的裝置群組中手動刪除裝置時，應用程式會從清單中刪除該裝置。刪除裝置後，已安裝的卡巴斯基應用程式（如果有）將保留在裝置上。之後，如果該裝置對管理伺服器而言仍然可見，而您又設定了定期網路輪詢，則在網路輪詢期間，卡巴斯基安全管理中心雲端主控台會發現該裝置並將其新增回「未配置的裝置」群組。因此，最好僅當裝置對管理伺服器不可見時再手動刪除該裝置。

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雲端主控台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情境。您在完成設定網路防護的情境後，必須維護防護系統的可靠性。這些維護可確保受管理裝置持續受到牢靠的防護，能夠抵禦病毒、網路攻擊和網路釣魚攻擊等各種威脅。

您有多種模式可用來為卡巴斯基安全管理中心雲端主控台元件和安全應用程式安裝更新。請選擇一或多個最符合您網路需求的模式。

以下情境所述的更新模式，需要將更新下載至發佈點儲存區。如果受管理裝置未連線到發佈點，請考慮手動更新 Kaspersky 資料庫、軟體模組和應用程式或直接從卡巴斯基更新伺服器更新。

當您完成此情境後，會發生以下結果：

- 卡巴斯基安全管理中心雲端主控台元件會自動更新，或是僅在您將更新指定為*已批准*狀態後更新。
- Kaspersky 安全應用程式、Kaspersky 資料庫與軟體模組會依您指定的排程更新。Kaspersky 安全應用程式預設僅會安裝您批准的更新。

您可以設定更新程序，以便用下述兩種方式之一下載和安裝更新：

- 自動地

  在此情況下，您僅需執行此情境一次。您將必須排定*將更新下載至發佈點儲存區*工作（如果有）、Kaspersky 安全應用程式的更新工作，並且保留網路代理內容中的預設更新設定。

- 手動

  您可以設定更新程序，以便手動執行*將更新下載至發佈點儲存區*工作（如果有）以及 Kaspersky 安全應用程式的更新工作。您也可以將網路代理設定為僅在卡巴斯基安全管理中心雲端主控台元件的更新獲您指定為*已批准*狀態後，才安裝該更新。

先決條件

在您開始之前，確保您已做了如下：

1. 依透過卡巴斯基安全管理中心雲端主控台部署 Kaspersky 應用程式的情境，將 Kaspersky 安全應用程式部署到受管理裝置。您在執行該情境時，已依受管理裝置的數量以及網路拓撲，分配了適當數量的發佈點。
2. 建立了配置了所有所需政策、政策設定檔和工作，根據網路防護配置情境。

階段

設定定期更新 Kaspersky 資料庫與應用程式，是分多個階段進行：

1. **建立「將更新下載至發佈點儲存區」工作**

   建立*將更新下載至發佈點儲存區*工作。執行該工作時，卡巴斯基安全管理中心雲端主控台會直接將卡巴斯基更新伺服器上的更新下載到發佈點。

   操作說明：建立「將更新下載至發佈點儲存區」工作

2. **配置發佈點**

   請確認所有所需發佈點的內容中都啟用了**佈署更新**選項。當有發佈點停用該選項時，位於該發佈點涵蓋範圍內的裝置將僅能從本機資源或直接從卡巴斯基更新伺服器下載更新。

   若您要受管理裝置僅從發佈點接收更新，請啟用網路代理政策的**僅透過發佈點分發檔案**選項。

3. **使用差異檔案最佳化更新程序（可選）**

   啟用此功能可讓發佈點與受管理裝置之間的流量減少。若要使用此功能，請在*將更新下載至發佈點儲存區*工作的內容中啟用**下載差異檔案**選項。

   如何使用 diff 檔案：使用 diff 檔案更新 Kaspersky 資料庫和軟體模組

4. **定義要安裝哪些更新**

   預設下，下載的軟體更新具有*未定義*狀態。請將狀態變更為*已批准*或*已拒絕*，藉以定義是否應將該更新安裝到網路裝置上。批准的更新總是被安裝。未定義的更新僅能依網路代理政策設定，安裝到網路代理和其他卡巴斯基安全管理中心雲端主控台元件中。您設定了*已拒絕*狀態的更新將不被安裝到裝置。

   說明：

   - 關於更新狀態
   - 批准和拒絕軟體更新

5. **設定自動安裝卡巴斯基安全管理中心雲端主控台元件的更新和修補程式**

   為網路代理和其他卡巴斯基安全管理中心雲端主控台元件下載的更新和修補程式預設會自動安裝。若您在網路代理內容中保持啟用**對未定義狀態的元件自動安裝可套用更新和修補程式**選項，則所有更新都會在下載至儲存區後自動安裝（或數個儲存區）。如果停用此選項，被下載和標注為*未定義*狀態的 Kaspersky 修補程式將僅在您改變其狀態為*已批准*是被安裝。

   操作說明：啟用和停用卡巴斯基安全管理中心雲端主控台元件的自動更新和修補

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，以提供對應用程式、軟體模組和 Kaspersky 資料庫（包括病毒資料庫）的及時更新。建議您在設定工作排程時，選取**When new updates are downloaded to the repository**選項。這將確保新的更新會盡快受到安裝。

   受管理應用程式的更新預設僅會在您將更新狀態變更為*已批准*後安裝。對於 Kaspersky Endpoint Security for Windows，您可以在更新工作中變更該更新設定。

   如果更新需要檢視和接受最終使用者產品授權協議的條款，您需要先接受它們。此後，更新可以被傳播到受管理裝置。

   操作說明：在裝置上自動安裝 Kaspersky Endpoint Security 更新

完成此情境後，您即可繼續監控網路狀態。

關於更新 Kaspersky 資料庫、軟體模組和應用程式

為確保您的受管理裝置隨時享有最新防護，您必須及時提供以下項目的更新：

- 卡巴斯基資料庫和軟體模組

Kaspersky Security Center Cloud Console 會在下載 Kaspersky 資料庫和軟體模組之前，先檢查 Kaspersky 伺服器是否可供存取。如果無法使用系統 DNS 存取伺服器，則應用程式使用公用 DNS 伺服器。這是為了確保更新病毒資料庫並維護受管理裝置的安全級別。

- 已安裝的 Kaspersky 應用程式，包括卡巴斯基安全管理中心雲端主控台元件和安全應用程式

取決於您網路的配置，您可以使用以下方案來下載和分發所需更新到受管理裝置：

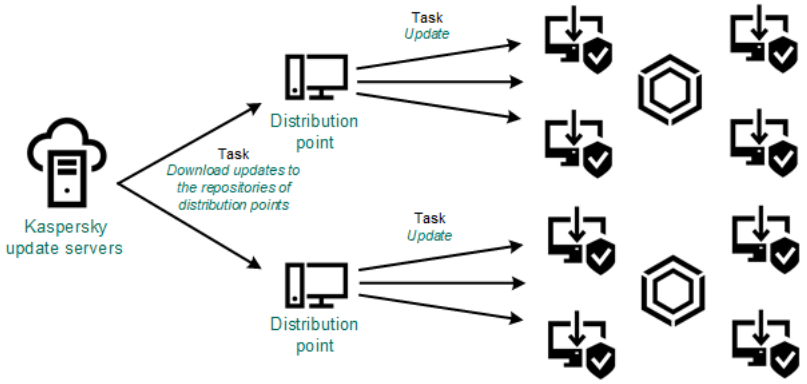
- 使用*將更新下載至發佈點儲存區*工作
- 透過本機資料夾、共用資料夾或 FTP 伺服器手動。
- 直接從卡巴斯基更新伺服器下載到受管理裝置上的安全應用程式

使用將更新下載至發佈點儲存區工作

在此模式中，卡巴斯基安全管理中心雲端主控台是透過*將更新下載至發佈點儲存區*工作來下載更新。位於發佈點涵蓋範圍內的受管理裝置會該從發佈點的儲存區下載更新（參見下圖）。

執行 macOS 的發佈點裝置無法從 Kaspersky 更新伺服器下載更新。

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



使用將更新下載至發佈點儲存區工作進行更新

當*將更新下載至發佈點儲存區*工作完成時，以下更新即已下載到發佈點儲存區：

- Kaspersky 資料庫和受管理裝置上安全應用程式的軟體模組

  這些更新透過 Kaspersky Endpoint Security for Windows 更新工作安裝。

- 卡巴斯基安全管理中心雲端主控台元件的更新

  預設下，這些更新被自動安裝。您可以在網路代理政策中變更設定。

- 安全應用程式更新

  預設下，Kaspersky Endpoint Security for Windows 僅安裝您批准的更新。更新透過更新工作安裝且可以在工作內容中被配置。

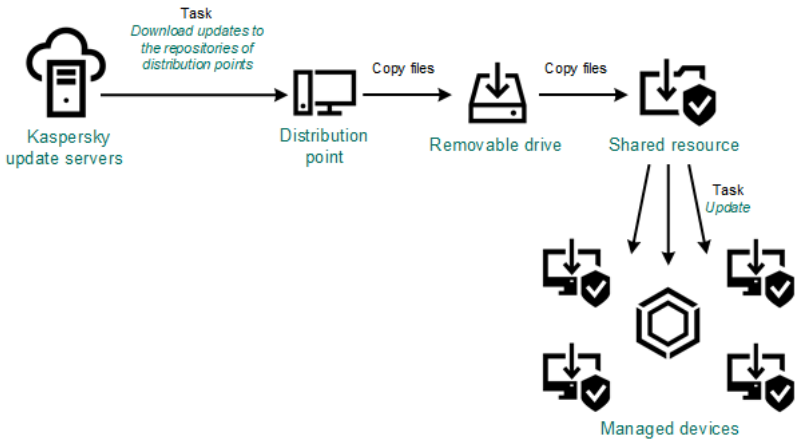
每個 Kaspersky 應用程式都從管理伺服器請求所需更新。管理伺服器會彙整這些請求，然後僅將應用程式所請求的更新下載到發佈點儲存區。這確保了相同更新不被下載多次，且不必要更新不被下載。執行*將更新下載至發佈點儲存區*工作時，管理伺服器會自動向卡巴斯基更新伺服器傳送以下資訊，以確保下載的是相關版本的 Kaspersky 資料庫和軟體模組：

- 應用程式 ID 和版本
- 應用程式安裝 ID
- 啟動金鑰 ID
- 下載工作執行 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。

透過本機資料夾、共用資料夾或 FTP 伺服器手動。

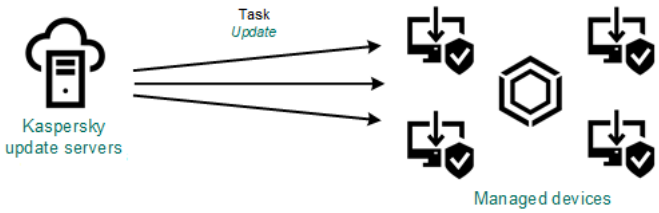
如果用戶端裝置未連線到發佈點，您可以使用本機資料夾或共用資料夾作為更新 Kaspersky 資料庫、軟體模組和應用程式的來源。在此模式中，您需要從發佈點儲存區複製所需更新到卸除式磁碟機，然後將這些更新複製到 Kaspersky Endpoint Security for Windows 設定中所指定作為更新來源的本機資料夾或共用資料夾（請參閱下圖）。



透過本機資料夾、共用資料夾或 FTP 伺服器更新

直接從 Kaspersky 更新伺服器到受管理裝置上的 Kaspersky Endpoint Security for Windows

在受管理裝置上，您可以配置 Kaspersky Endpoint Security for Windows 直接從 Kaspersky 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

在此模式中，安全應用程式並不會用到卡巴斯基安全管理中心雲端主控台所提供的儲存區。要直接從 Kaspersky 更新伺服器接收更新，在安全應用程式介面中指定 Kaspersky 更新伺服器作為更新來源。對於這些設定的完整描述，請參考 Kaspersky Endpoint Security for Windows 檔案。

建立「將更新下載至發佈點儲存區」工作

執行 macOS 的發佈點裝置無法從 Kaspersky 更新伺服器下載更新。

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

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

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雲端主控台元件的更新
- 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。

若要為所選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 **資產（裝置）→工作**。
2. 點擊**新增**按鈕。
   新工作精靈啟動。遵照精靈的說明。
3. 對於卡巴斯基安全管理中心雲端主控台應用程式，請在**工作類型**欄位選取**將更新下載至發佈點儲存區**。
4. 指定您正建立的工作的名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。
5. 選取一個選項按鈕以指定管理群組、裝置分類或應用程式工作的裝置。
6. 在**完成工作建立**步驟中，若您啟用**建立完成時開啟工作詳情**選項，您可修改預設工作設定。如果您不啟用該選項，工作使用預設設定建立。您可以稍後隨時修改預設設定。
7. 點擊**建立**按鈕。
   工作被建立並顯示在工作清單。
8. 按一下建立的工作的名稱以開啟工作內容視窗。
9. 在工作內容視窗的**應用程式設定**頁籤，指定以下設定：
   - **更新來源**

以下資源可作為發佈點的更新來源：

- Kaspersky 更新伺服器

  Kaspersky 應用程式可以從 Kaspersky 的 HTTP(S) 伺服器下載資料庫和程式模組更新。

  預設情況下已選取此選項。

- 主管理伺服器

  該資源套用到為從屬或虛擬管理伺服器建立的工作。

- 本機或網路資料夾

  包含最新更新的本機或網路資料夾。網路資料夾可以是 FTP 或 HTTP 伺服器，或者 SMB 共用。如果網路資料夾需要身分驗證，則僅支援 SMB 通訊協定。在選取本機資料夾時，您必須在安裝了管理伺服器的裝置上指定一個資料夾。

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

- **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**

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

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

  - Kaspersky Update Utility

    此公用程式使用舊方案下載更新。

  - 卡巴斯基安全管理中心 13.2 或更早版本

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

  預設情況下已停用該選項。

10. 為工作啟動建立排程。如果必要，指定以下設定：

- **排程開始**

選取工作執行排程並設定所選排程。

- **手動**（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。此排程是為了讓卡巴斯基安全管理中心雲端主控台與舊版系統相容而存在。

  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選項。

- **在完成其它工作時**

  目前工作在其他工作完成後啟動。您可以選取先前工作如何結束（成功或帶有錯誤）以觸發目前工作的啟動。例如，您可能想使用***Turn on the device***選項執行開啟裝置工作，完成後，請執行*惡意軟體掃描*工作。只有當這兩項工作都被分配給相同的裝置時，此參數才會有作用。

- **執行錯過的工作**

  該選項決定在工作要啟動時用戶端裝置在網路中不可見時工作的行為。

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

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

執行*將更新下載至發佈點儲存區*工作時，資料庫和軟體模組更新從更新來源下載並儲存在共用資料夾。下載的更新將僅被包含在指定管理群組的發佈點和沒有更新下載工作的更新代理使用。

將受管理裝置設定為僅從發佈點接收更新

受管理裝置可以從多種來源擷取 Kaspersky 資料庫、軟體模組和 Kaspersky 應用程式的更新：直接從更新伺服器、從發佈點，或是從本地或網路資料夾擷取更新。您可以將發佈點指定為唯一可能的更新來源。

若要將受管理裝置設定為僅從發佈點接收更新：

1. 在主功能表中，轉至 **資產（裝置）→ 政策和設定檔**。
2. 點擊網路代理政策。
3. 在政策內容視窗中，開啟**應用程式設定**頁籤。
4. 在**設定**區段中，開啟**僅透過發佈點分發檔案**切換按鈕。
5. 為該開關按鈕設定鎖（🔒）。
6. 點擊**儲存**按鈕。

   該政策即會套用到所選裝置，讓這些裝置僅從發佈點接收更新。

啟用和停用卡巴斯基安全管理中心雲端主控台元件的自動更新和修補

在裝置上安裝網路代理期間，預設會啟用自動安裝卡巴斯基安全管理中心雲端主控台元件的更新和修補程式。您可以在安裝網路代理期間加以停用，或稍後透過政策來停用。

若要於在裝置本機上安裝網路代理期間，停用自動更新和修補卡巴斯基安全管理中心雲端主控台元件：

1. 啟動在裝置本機上安裝網路代理。
2. 在**進階設定**步驟，清空**自動安裝元件的未定義狀態的可應用更新和修補程式**核取方塊。
3. 遵照精靈的說明。

   裝置上即會安裝停用了自動更新和修補卡巴斯基安全管理中心雲端主控台元件的網路代理。您可以稍後使用政策啟用自動更新和修補程式。

若要在透過安裝套件在裝置上安裝網路代理期間，停用自動更新和修補卡巴斯基安全管理中心雲端主控台元件：

1. 在主功能表中，轉至 **操作 → 儲存區 → 安裝套件**。
2. 點擊**卡巴斯基安全管理中心網路代理 <版本號>** 套件。
3. 在內容視窗中，開啟**設定**頁籤。
4. 關閉**對未定義狀態的元件自動安裝可套用更新和修補程式**開關按鈕。

   此套件即會安裝停用了自動更新和修補卡巴斯基安全管理中心雲端主控台元件的網路代理。您可以稍後使用政策啟用自動更新和修補程式。

如果於在裝置上安裝網路代理期間選取（或清空）了第 4 步的核取方塊，您之後可以透過網路代理政策啟用（或停用）自動更新。

若要透過網路代理政策來啟用或停用自動更新和修補卡巴斯基安全管理中心雲端主控台元件：

1. 在主功能表中，轉至 **資產（裝置）→ 政策和設定檔**。
2. 點擊網路代理政策。
3. 在政策內容視窗中，選取**應用程式設定**頁籤。
4. 在**管理修補程式和更新**區段中，開啟或關閉**對未定義狀態的元件自動安裝可套用更新和修補程式**開關按鈕以個別啟用或停用自動更新和修補。
5. 確認對此切換按鈕設定（**強制執行**）鎖定 (🔒)。

   該政策即會套用到所選裝置，在這些裝置上啟用（或停用）自動更新和修補卡巴斯基安全管理中心雲端主控台元件。

自動安裝 Kaspersky Endpoint Security for Windows 的更新

您可以在用戶端裝置上配置 Kaspersky Endpoint Security for Windows 自動更新資料庫和軟體模組。

要在裝置上配置下載和自動安裝 Kaspersky Endpoint Security for Windows 更新：

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

   新工作精靈啟動。遵照精靈的說明。
3. 對於 Kaspersky Endpoint Security for Windows 應用程式，選取**更新**作為工作子類型。
4. 指定您正建立的工作的名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。
5. 選取工作範圍。
6. 指定管理群組、裝置分類或應用程式工作的裝置。
7. 在**完成工作建立**步驟中，若您啟用**建立完成時開啟工作詳情**選項，您可修改預設工作設定。如果您不啟用該選項，工作使用預設設定建立。您可以稍後隨時修改預設設定。
8. 點擊**建立**按鈕。

   工作被建立並顯示在工作清單。
9. 按一下建立的工作的名稱以開啟工作內容視窗。
10. 在工作內容視窗的**應用程式設定**頁籤，定義本機或行動模式的更新工作設定：
    - **本機模式**：此頁籤上的設定定義了當裝置與管理伺服器之間建立了連線時，裝置要如何接收更新。
    - **行動模式**：此頁籤上的設定定義了當卡巴斯基安全管理中心雲端主控台與裝置之間未建立連線時（例如，當裝置未連線到網際網路時），裝置要如何接收更新。
11. 啟用您要用來更新 Kaspersky Endpoint Security for Windows 資料庫與應用程式模組的更新來源。如有必要，請使用**向上移動**與**向下移動**按鈕將清單中的來源變更位置。若啟用數個更新來源，Kaspersky Endpoint Security for Windows 會嘗試逐一連線，從清單頂端開始，並透過第一個可用來源的更新套件執行更新工作。

    當更新來源是設定為卡巴斯基安全管理中心雲端主控台時，更新下載來源會是發佈點儲存區，而不是管理伺服器儲存區。請確定您分配了發佈點並建立了*將更新下載至發佈點儲存區*工作。
12. 啟用**安裝批准的應用程式模組更新**選項，在更新應用程式資料庫同時下載和安裝軟體模組。

    如果啟用該選項，Kaspersky Endpoint Security for Windows 在執行更新工作時，會通知使用者有可用的軟體模組更新並且更新套件包含軟體模組更新。Kaspersky Endpoint Security for Windows 僅會安裝經您設定為*已批准*狀態的更新；這些更新將透過應用程式介面或透過卡巴斯基安全管理中心雲端主控台安裝到本機上。

    您也可以啟用**自動安裝關鍵應用程式模組更新**選項。如果軟體模組有任何更新，Kaspersky Endpoint Security for Windows 自動安裝*關鍵*狀態的更新；其餘的更新會在您批准後安裝。

    如果軟體模組更新需要審查並接受產品授權協議的隱私政策，程式將在使用者接受最終使用者產品授權協議的條款和隱私政策後安裝更新。
13. 選取**複製更新到資料夾**核取方塊，程式將已下載的更新儲存到指定的資料夾。
14. 排程工作。若要確保定期更新，建議您選取**當新更新下載至儲存區時**選項。
15. 點擊**儲存**。

更新工作在執行時，程式傳送請求到 Kaspersky 更新伺服器。

一些更新需要安裝最新版本的管理外掛程式。

關於更新狀態

*狀態*是軟體更新的一項屬性，定義了特定的軟體更新是否必須安裝到網路裝置上。

更新可以具有以下狀態：

- *未定義*

  預設下，下載的軟體更新具有*未定義*狀態。未定義的更新僅能依網路代理政策設定，安裝到網路代理和其他卡巴斯基安全管理中心雲端主控台元件中。

- *已批准*

  批准的更新總是被安裝。如果更新需要檢視和接受最終使用者產品授權協議的條款，您需要先接受它們。

- *已拒絕*

  您設定了*已拒絕*狀態的更新將不被安裝到裝置。

對於以下軟體的更新，您可以變更更新的狀態：

- 網路代理和其他卡巴斯基安全管理中心雲端主控台元件

  為卡巴斯基安全管理中心雲端主控台元件下載的更新和修補程式預設會自動安裝。若您在網路代理內容中保持啟用**對未定義狀態的元件自動安裝可套用更新和修補程式**選項，則所有更新都會在下載至儲存區後自動安裝（或數個儲存區）。如果停用此選項，被下載和標注為*未定義*狀態的 Kaspersky 修補程式將僅在您改變其狀態為*已批准*是被安裝。

  卡巴斯基安全管理中心雲端主控台元件的更新無法解除安裝，即使您將更新設定為*已拒絕*狀態也一樣。

- Kaspersky 安全應用程式

  受管理應用程式的更新預設僅會在您將更新狀態變更為*已批准*後，才會安裝。如果先前為安全應用程式安裝了已拒絕的更新，卡巴斯基安全管理中心雲端主控台會嘗試在所有裝置解除安裝該更新。

批准和拒絕軟體更新

更新安裝工作的設定可能需要對要安裝的更新進行批准。您可以批准必須安裝的更新並拒絕不能安裝的更新。

例如，您可能想先在測試環境中檢查更新安裝以確保它們不干預裝置操作，僅在這之後允許安裝這些更新到用戶端裝置。

要批准或拒絕一個或幾個更新：

1. 在主功能表中，轉到**操作 → Kaspersky 應用程式 → 無縫更新**。

   可用更新清單被顯示。

受管理應用程式的更新可能需要安裝卡巴斯基安全管理中心特定的最低版本。如果此版本晚於目前版本，則顯示這些更新，但無法核准。同樣，在升級卡巴斯基安全管理中心之前，無法從此類更新中建立安裝軟體套件。提示您將卡巴斯基安全管理中心執行個體升級到所需的最低版本。

2. 選取您要批准或拒絕的更新。

3. 點擊**批准**以核准選取的更新或**拒絕**以拒絕選取的更新。

   預設值是*未定義*。

您分配了*已批准*狀態的更新被放置在安裝佇列。

您分配了*已拒絕*狀態的更新被從先前將其安裝的裝置上移除（如果可能）。而且，它們將來也不會被安裝到其他裝置。

Kaspersky 應用程式的一些更是無法被移除。如果您將其設定為*Declined*狀態，卡巴斯基安全管理中心雲端主控台並不會在先前已安裝這些更新的裝置解除安裝這些更新。然而，這些更新將來也不會被安裝到其他裝置。

如果您為協力廠商軟體更新設定了*已拒絕*狀態，則已計畫但未安裝這些更新的裝置將不會安裝這些更新。更新將保持在已將其安裝的裝置上。如果您必須刪除更新，您可以在本機手動刪除它們。

使用 diff 檔案更新 Kaspersky 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。使用差異檔案可節省您公司網路中的流量，因為比起使用資料庫和軟體模組的完整檔案，差異檔案佔用的空間更少。如果發佈點上啟用了*下載差異檔案*的功能，則差異檔案會儲存到該發佈點上。因此，從該發佈點取得更新的裝置便可以使用儲存的差異檔案來更新自身的資料庫和軟體模組。

為了讓差異檔案獲得最佳利用，我們建議您將裝置的更新頻率以及裝置取得更新的發佈點本身的更新排程進行同步。不過，即便裝置的更新頻率低於裝置取得更新的發佈點本身的更新頻率好幾倍，流量還是會比較省。

發佈點不對 diff 檔案的自動分發使用 IP 多點傳送。

若要啟用下載差異檔案的功能：

1. 在主功能表中，轉至 **資產（裝置）→ 工作**。

2. 點擊*將更新下載至發佈點儲存區*工作以開啟工作內容。

3. 在**應用程式設定**頁籤，啟用**下載差異檔案**選項。

4. 點擊**儲存**按鈕。

   下載差異檔案的功能即會啟用。每次執行*將更新下載至發佈點儲存區*工作時，除了會下載更新檔案，還會下載更新的差異檔案。

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。

在離線裝置上更新 Kaspersky 資料庫和軟體模組

在受管理裝置上更新 Kaspersky 資料庫和軟體模組是個重要的工作，它維持裝置的防護以防範病毒和其他威脅。管理員設定的定期更新通常是透過使用發佈點的儲存區進行。

當您需要在一或多個未連線到發佈點或網際網路的裝置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。

您可以從以下來源複製所需更新：

- 發佈點。

  為確保發佈點儲存區包含所需的更新來用於離線裝置上安裝的安全應用程式，在發佈點的涵蓋範圍內，至少要有一台受管理的線上裝置安裝了相同的安全應用程式。該應用程式必須設定為透過*將更新下載至發佈點儲存區*工作，從發佈點儲存區接收更新。

- 任何安裝了相同的安全應用程式、並且設定為從發佈點儲存區或直接從卡巴斯基更新伺服器接收更新的裝置。

以下是從發佈點儲存區複製更新，然後再加以設定來更新資料庫與軟體模組的例子。

要在離線裝置上更新 Kaspersky 資料庫和軟體模組：

1. 將卸除式磁碟機連接到發佈點裝置。
2. 複製更新檔案到卸除式磁碟機。

   更新預設會位於：%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\Updates。
3. 在離線裝置上，配置安全應用程式（例如，Kaspersky Endpoint Security for Windows）以從本機資料夾或共用資料夾接收更新，例如 FTP 伺服器或共用資料夾。
4. 從卸除式磁碟機複製更新到您想用作更新來源的本機資料夾或共用資源。
5. 在需要安裝更新的離線裝置上，開始 Kaspersky Endpoint Security for Windows 的更新工作。

在更新工作完成後，Kaspersky 資料庫和軟體模組在裝置上變為最新。

更新 Kaspersky Security for Windows Server 資料庫

您可以在受管理裝置上安裝 Kaspersky Security for Windows Server，而您或許想要啟動該應用程式的即時檔案防護工作。不過，該應用程式本身並未隨附正常運作所需的資料庫。這些資料庫要等*將更新下載至發佈點儲存區*工作完成後，才會下載到受管理裝置。

如果您想在受管理裝置上安裝 Kaspersky Security for Windows Server 後，立即啟動即時檔案防護工作，您必須確保該應用程式的資料庫已下載並已是最新版本。否則，該工作可能無法會正常運作。

若要確保 Kaspersky Security for Windows Server 資料庫是最新版本：

1. 確保管理伺服器上已完成*將更新下載至發佈點儲存區*工作。

2. 執行以下操作之一：

   - 在即時檔案防護工作的設定中，將啟動時機設定為*應用程式啟動時*，然後重新啟動受管理裝置。
   - 在即時檔案防護工作的設定中，手動將開始時間設定為您想要的時間。

Kaspersky Security for Windows Server 中的即時檔案防護工作即已準備好正常運作。

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雲端主控台中，與管理用戶端裝置上安裝的協力廠商應用程式相關的功能。

關於協力廠商應用程式

卡巴斯基安全管理中心雲端主控台可以幫助您更新用戶端裝置上安裝的協力廠商軟體並修復協力廠商軟體的弱點。卡巴斯基安全管理中心雲端主控台只能將協力廠商軟體從目前版本更新到最新版本。以下清單列出您可透過卡巴斯基安全管理中心雲端主控台更新的協力廠商軟體：

協力廠商軟體清單可以用新的應用程式進行更新和延伸。您可以檢視卡巴斯基安全管理中心雲端主控台中的可用更新清單，看看您是否可透過卡巴斯基安全管理中心雲端主控台更新使用者裝置上的協力廠商軟體。

- 7-Zip Developers: 7-Zip
- Adobe Systems:
  - Adobe Acrobat DC
  - Adobe Acrobat Reader DC
  - Adobe Acrobat
  - Adobe Reader
  - Adobe Shockwave Player
- AIMPDevTeam: AIMP
- ALTAP: Altap Salamander
- Apache Software Foundation: Apache Tomcat
- Apple:
  - Apple iTunes
  - Apple QuickTime
- Armory Technologies, Inc.: Armory
- Cerulean Studios: Trillian Basic
- Ciphrex Corporation: mSIGNA
- Cisco: Cisco Jabber
- Code Sector: TeraCopy
- Codec Guide:

    - K-Lite Codec Pack Basic
    - K-Lite Codec Pack Full
    - K-Lite Codec Pack Mega
    - K-Lite Codec Pack Standard
- DbVis Software AB: DbVisualizer
- Decho Corp.:
    - Mozy Enterprise
    - Mozy Home
    - Mozy Pro
- Dominik Reichl: KeePass Password Safe
- Don HO don.h@free.fr: Notepad++
- DoubleGIS: 2GIS
- Dropbox, Inc.: Dropbox
- EaseUs: EaseUS Todo Backup Free
- Electrum Technologies GmbH: Electrum
- Enter Srl: Iperius Backup
- Eric Lawrence: Fiddler
- EverNote: EverNote
- Exodus Movement Inc: Exodus
- EZB Systems: UltraISO
- Famatech:
    - Radmin
    - 遠端管理員
- Far Manager: FAR Manager
- FastStone Soft: FastStone Image Viewer
- FileZilla Project: FileZilla
- Firebird Developers: Firebird
- Foxit Corporation:

    - Foxit Reader
    - Foxit Reader Enterprise
- Free Download Manager.ORG: Free Download Manager
- GIMP project: GIMP
- GlavSoft LLC.: TightVNC
- GNU Project: Gpg4win
- Google:
    - Google Earth
    - Google Chrome
    - Google Chrome Enterprise
    - Google Earth Pro
- Inkscape Project: Inkscape
- IrfanView: IrfanView
- iterate GmbH: Cyberduck
- Logitech: SetPoint
- LogMeIn, Inc.:
    - LogMeIn
    - Hamachi
    - LogMeIn Rescue Technician Console
- Martin Prikryl: WinSCP
- Mozilla Foundation:
    - Mozilla Firefox
    - Mozilla Firefox ESR
    - Mozilla SeaMonkey
    - Mozilla Thunderbird
- New Cloud Technologies Ltd: MyOffice Standard.Home Edition
- OpenOffice.org: OpenOffice
- Opera Software: Opera

- Oracle Corporation:
  - Oracle Java JRE
  - Oracle VirtualBox
- PDF44: PDF24 MSI/EXE
- Piriform:
  - CCleaner
  - Defraggler
  - Recuva
  - Speccy
- Postgresql: PostgreSQL
- RealNetworks: RealPlayer Cloud
- RealVNC:
  - RealVNC Server
  - RealVNC Viewer
- Right Hemisphere Inc.: SAP Visual Enterprise Viewer (Complete/Minimum)
- Simon Tatham: PuTTY
- Skype Technologies: Skype for Windows
- Sober Lemur S.a.s.:
  - PDFsam Basic
  - PDFsam Visual
- Softland: FBackup
- Splashtop Inc.: Splashtop Streamer
- Stefan Haglund, Fredrik Haglund, Florian Schmitz: CDBurnerXP
- Sublime HQ Pty Ltd: Sublime Text
- TeamViewer GmbH:
  - TeamViewer Host
  - TeamViewer
- Telegram Messenger LLP: Telegram Desktop

- The Document Foundation:
  - LibreOffice
  - LibreOffice HelpPack
- The Git Development Community:
  - Git for Windows
  - Git LFS
- The Pidgin developer community: Pidgin
- TortoiseSVN Developers: TortoiseSVN
- VideoLAN: VLC media player
- VMware:
  - VMware Player
  - VMware Workstation
- WinRAR Developers: WinRAR
- WinZip: WinZip
- Wireshark Foundation: Wireshark
- Wrike: Wrike
- Zimbra: Zimbra Desktop

弱點和修補程式管理的限制

視您使用的產品授權以及卡巴斯基安全管理中心雲端主控台運作的模式而定，弱點和修補程式管理功能會具有一些限制。

不支援弱點和修補程式管理的產品授權如下：

- Kaspersky Endpoint Security for Business Select
- Kaspersky Hybrid Cloud Security

支援弱點和修補程式管理的產品授權如下：

- Kaspersky Endpoint Security for Business Advanced
- Kaspersky Endpoint Detection and Response Optimum
- Kaspersky Total Security for Business

- Kaspersky Hybrid Cloud Security Enterprise

下表比較了卡巴斯基安全管理中心雲端主控台在試用模式下、使用不支援弱點和修補程式管理的產品授權時，以及使用支援弱點和修補程式管理的產品授權時，會具有的限制。

弱點和修補程式管理的限制

限制	試用模式	正式模式：不支援弱點和修補程式管理的產品授權	正式模式：支援弱點和修補程式管理的產品授權
*安裝 Windows Update 更新*工作或*修復弱點*工作的最大數量	4	4	0（無法建立這些類型的新工作）
*安裝所需更新並修復弱點*工作的最大數量	2	不支援	4
所有*安裝所需更新並修復弱點*工作中的最大規則數量	10	不支援	50
可同時處於*已批准*狀態的軟體更新最大數量	100	不支援	1000
可手動新增到工作中的軟體更新最大數量	500	1000	1000
可手動新增到工作中的軟體弱點最大數量	500	1000	1000

弱點和修補程式管理功能在試用模式與正式模式下以及各種產品授權選項下的可用性

卡巴斯基安全管理中心雲端主控台中弱點和修補程式管理功能的可用性，取決於您是在試用模式還是正式模式下使用，以及您所選的產品授權選項。請使用下表查看可用的弱點和修補程式管理功能。

弱點和修補程式管理功能的可用性

弱點和修補程式管理功能	試用模式	正式模式：Kaspersky Endpoint Security for Business Select	正式模式：Kaspersky Endpoint Security for Business Advanced、Kaspersky Endpoint Detection and Response Optimum、Kaspersky Total Security for Business
手動在執行 Windows 的受管理裝置上修復 Microsoft 軟體中的弱點 建立*修復弱點*工作	✓	✓	–
在執行 Windows 的受管理裝置上手動安裝 Microsoft 軟體更新 透過*安裝 Windows Update 更新*工作安裝協力廠商軟體更新	–	✓	✓

自動根據規則來安裝協力廠商軟體更新並修復協力廠商軟體弱點 建立*安裝所需更新並修復弱點*工作並安裝更新 新增安裝更新的規則	✓	–	✓

安裝協力廠商軟體更新

本節說明卡巴斯基安全管理中心雲端主控台中，與在用戶端裝置上安裝協力廠商應用程式的更新相關的功能。

情境：更新協力廠商軟體

本節提供在用戶端裝置安裝更新協力廠商軟體的情境。該協力廠商軟體中包含來自 Microsoft 和其他軟體供應商的應用程式。Microsoft 應用程式的更新會由 Windows Update 服務提供。

階段

更新協力廠商軟體採分階段進行：

1. **搜尋所需更新**

   若要尋找受管理裝置必要的協力廠商軟體更新，請執行*弱點掃描和所需更新*工作。當該工作完成時，卡巴斯基安全管理中心雲端主控台會收到在您工作內容中所指定裝置上已安裝的軟體中偵測到的弱點與所需更新的清單。

   *弱點掃描和所需更新*工作會由管理伺服器快速設定精靈自動建立。若您未執行該精靈，請建立工作或立即執行快速啟動精靈。

   說明：

   - 建立弱點掃描和所需更新工作
   - 「弱點掃描和所需更新」工作設定

2. **分析已知更新清單**

   檢視**軟體更新**清單並決定要安裝的更新。若要檢視各更新的詳細資訊，請按一下清單中的更新名稱。您可以針對清單中的每項更新，檢視該更新在各受管理裝置上的安裝統計資訊。例如，您可以檢視未安裝、將安裝或是無法安裝所選更新的裝置數量。

   操作說明：檢視可用協力廠商軟體更新的資訊

3. **配置更新的安裝**

   當卡巴斯基安全管理中心雲端主控台收到協力廠商軟體更新的清單時，您可使用*安裝所需更新並修復弱點*工作或*安裝 Windows Update 更新*工作，將這些更新安裝到用戶端裝置上。建立其中一種這類工作。您可在**工作**頁籤或使用**軟體更新**清單建立這類工作。

   *安裝所需更新並修復弱點*工作用來安裝 Microsoft 應用程式的更新，包括由 Windows Update 服務提供的更新，以及其他供應商產品的更新。

*安裝 Windows Update 更新*工作則僅能用來安裝 Windows Update 更新。

軟體更新安裝工作具有一些限制。這些限制取決於您對卡巴斯基安全管理中心雲端主控台使用的產品授權以及卡巴斯基安全管理中心雲端主控台運作的模式。

若要安裝一些軟體更新，您必須接受安裝軟體的最終使用者產品授權協議 (EULA)。若您拒絕 EULA，則無法安裝該軟體更新。

說明：

- 建立安裝所需更新並修復弱點工作
- 建立安裝 Windows Update 更新工作
- 檢視可用協力廠商軟體更新的資訊

4. **排程工作**

   為確定更新清單永遠處於最新狀態，請排程*弱點掃描和所需更新*工作以不時自動執行。預設頻率為每週一次。

   若您已建立*安裝所需更新並修復弱點*工作，您可排程與*弱點掃描和所需更新*工作的執行頻率相同會更少。排定*安裝 Windows Update 更新*工作時請注意，您在每次啟動該工作之前，都必須為該工作定義更新清單。

   排程工作時，請確定修復弱點的工作會在*弱點掃描和所需更新*工作完成後啟動。

   操作說明：一般工作設定

5. **核准和拒絕軟體更新（選用）**

   若您建立的是*安裝所需更新並修復弱點*工作，您可在工作內容中，指定更新安裝規則。若您建立的是*安裝 Windows Update 更新*工作，請略過此步驟。

   對於各規則，您可定義更新來根據更新狀態進行安裝：*未定義*、*已核准*或*已拒絕*。例如，您可能要針對伺服器建立特定工作，並針對此工作設定規則，以允許僅安裝 Windows Update 更新，以及僅安裝有*已核准*狀態的更新。針對您要安裝的這些更新手動設定*已核准*狀態後。在此情況下，處於*未定義*或*已拒絕*狀態的 Windows Update 更新將不會安裝到您在工作中指定的伺服器。

   預設下，下載的軟體更新具有*未定義*狀態。您可在**軟體更新**清單（**操作 → 修補程式管理 → 軟體更新**）變更狀態至*已核准*或*已拒絕*。

   操作說明：核准與拒絕協力廠商軟體更新

6. **執行更新安裝工作**

   啟動*安裝所需更新並修復弱點*工作或*安裝 Windows Update 更新*工作。啟動這類工作時，更新會自動下載並安裝至受管理裝置。工作完成後，請確保工作清單出現*已成功完成*狀態。

   操作說明：手動啟動工作

7. **建立協力廠商軟體更新安裝結果的報告（選用）**

   為了確認工作已建立並且安裝了更新，請建立**協力廠商軟體更新安裝結果報告**，然後在該報告中檢視詳細的更新安裝統計資訊。

   操作說明：產生和檢視報告

關於協力廠商軟體更新

卡巴斯基安全管理中心雲端主控台可讓您管理受管理裝置上安裝的協力廠商軟體更新，並且安裝所需更新來修復 Microsoft 應用程式和其他軟體廠商產品中的弱點。

卡巴斯基安全管理中心雲端主控台是透過*弱點掃描和所需更新*工作搜尋更新。完成此工作時，管理伺服器會收到偵測到的弱點清單，以及安裝於您在工作內容指定裝置上已安裝軟體需要的更新。在檢視可用更新資訊後，您可以將它們安裝到裝置。

卡巴斯基安全管理中心雲端主控台更新某些應用程式的方式，是先移除舊版應用程式再安裝新版應用程式。

在受管理裝置上更新協力廠商應用程式或修復協力廠商應用程式中的弱點時，可能需要使用者互動。例如，若協力廠商應用程式目前開啟，可能會提示使用者關閉協力廠商應用程式。

出於安全原因，卡巴斯基技術會自動掃描您使用弱點和修補程式管理功能安裝的任何協力廠商軟體更新以查找惡意軟體。這些技術用於自動檢查檔案，包括病毒掃描、靜態分析、動態分析、沙箱環境中的行為分析和機器學習。

卡巴斯基專家不會對可以使用弱點和修補程式管理功能安裝的協力廠商軟體更新進行手動分析。此外，卡巴斯基專家不會在此類更新中搜尋弱點（已知或未知）或未記錄的功能，也不會對上述段落中指定的更新以外的其他類型的更新進行分析。

用於安裝協力廠商軟體更新的工作

當系統將協力廠商軟體更新的中繼資料下載至儲存區後，您可使用以下工作將更新安裝在用戶端裝置：

- *安裝所需更新並修復弱點*工作

  此工作用來安裝 Microsoft 應用程式的更新，包括由 Windows Update 服務提供的更新，以及其他供應商產品的更新。

  此工作完成時，更新會自動安裝在受管理裝置上。當有新更新的中繼資料下載至管理伺服器儲存區時，卡巴斯基安全管理中心雲端主控台會檢查更新是否符合更新規則中指定的條件。系統會下載符合條件的所有新更新，並在下次工作執行時安裝。

- *安裝 Windows Update 更新*工作

  此工作只能用於安裝 Windows Update 更新。

  完成此工作時，僅會安裝這些工作內容中指定的更新。未來您若要安裝新更新，必須將所需更新新增至現有工作的更新清單，或是建立*安裝 Windows Update 更新*工作。

軟體更新安裝工作具有一些限制。這些限制取決於您對卡巴斯基安全管理中心雲端主控台使用的產品授權以及卡巴斯基安全管理中心雲端主控台運作的模式。

安裝協力廠商軟體更新

您可建立並執行以下其中一項工作在受管理裝置上安裝協力廠商軟體更新：

- *安裝所需更新並修復弱點*

  您可以使用此工作來安裝 Microsoft 提供的 Windows Update 更新和其他供應商的產品更新。

- *安裝 Windows Update 更新*

  您僅能將此工作用來安裝 Windows Update 更新。

軟體更新安裝工作具有一些限制。這些限制取決於您對卡巴斯基安全管理中心雲端主控台使用的產品授權以及卡巴斯基安全管理中心雲端主控台運作的模式。

在受管理裝置上更新協力廠商應用程式或修復協力廠商應用程式中的弱點時，可能需要使用者互動。例如，若協力廠商應用程式目前開啟，可能會提示使用者關閉協力廠商應用程式。

您可以建立工作，透過以下方式作為安裝所需更新的選擇：

- 透過開啟更新清單並指定要安裝的更新。

  這會建立安裝所選更新的新工作。您也可以選擇將選定的更新新增到現有工作。

- 透過執行更新安裝精靈。

  更新安裝精靈的可用性取決於卡巴斯基安全管理中心雲端主控台模式以及您目前的產品授權。

  該精靈簡化了更新安裝工作的建立與設定，並可避免您重複建立含有相同更新安裝清單的工作。

使用更新清單安裝協力廠商軟體更新

若要使用更新清單安裝協力廠商軟體更新：

1. 開啟更新清單之一：

   - 要開啟一般更新清單，請在主功能表中，前往**操作 → 修補程式管理 → 軟體更新**。
   - 若要開啟受管理裝置的更新清單，請在主功能表中，前往**資產（裝置） → 受管理裝置 → <裝置名稱> → 進階 → 可用更新**。
   - 若要開啟特定應用程式的更新清單，請在主功能表中，前往**操作 → 協力廠商應用程式 → 應用程式登錄資料 → <應用程式名稱> → 可用更新**。

   可用更新清單被顯示。

2. 選取您要安裝之更新旁邊的核取方塊。

3. 點擊**安裝更新**按鈕。

   若要安裝一些軟體更新，您必須接受最終使用者產品授權協議 (EULA)。若您拒絕 EULA，則無法安裝該軟體更新。

4. 您可以選取以下其中一個方法：

   - **新工作**

     新工作精靈啟動。畫面中會預先選取*安裝所需更新並修復弱點*工作或*安裝 Windows Update 更新*工作（視卡巴斯基安全管理中心雲端主控台模式以及您目前的產品授權而定）。請按照精靈的步驟完成工作建立。

   - **安裝更新（新增規則到指定工作）**

     選取要向其新增所選更新的工作。選取*安裝所需更新並修復弱點*工作或*安裝 Windows Update 更新*工作。如果您選取*安裝所需更新並修復弱點*工作，則系統會自動將用於安裝所選更新的新規則新增到所選工作中。如果您選取*安裝 Windows Update 更新*工作，則系統會將所選更新新增到工作內容中。

     工作內容視窗隨即開啟。按一下**儲存**按鈕以儲存變更。

如果您選擇建立工作，則會建立該工作並將其顯示在以下位置的工作清單中：**資產（裝置）→工作**。如果您選擇將更新新增到現有工作，則這些更新將儲存在工作屬性中。

若要安裝協力廠商軟體更新，請啟動*安裝所需更新並修復弱點*工作或*安裝 Windows Update 更新*工作。您可手動啟動任何這類工作，或在您啟動的工作內容中指定排程設定。指定工作排誠實，請確保更新安裝工作會在*弱點掃描和所需更新*工作完成後啟動。

使用更新安裝精靈安裝協力廠商軟體更新

此功能的可用性取決於卡巴斯基安全管理中心雲端主控台模式以及您目前的產品授權。

若要建立工作以使用「更新安裝精靈」安裝協力廠商軟體更新：

1. 在主功能表中，轉至 **操作 → 修補程式管理 → 軟體更新**。
   可用更新清單被顯示。
2. 選取您要安裝之更新旁邊的核取方塊。
3. 點擊**執行更新安裝精靈**按鈕。
   更新安裝精靈開始。**選取更新安裝工作**頁面會列出所有以下類型的現有工作：
   - *安裝所需更新並修復弱點*
   - *安裝 Windows Update 更新*
   - *修復弱點*

   您不能修改後兩種類型的工作來安裝新更新。要安裝新更新，您只能使用*安裝所需更新並修復弱點*工作。
4. 如果希望精靈僅顯示用於安裝所選更新的工作，請啟用**僅顯示安裝此更新的工作**選項。
5. 選取您要新增的內容：
   - 若要啟動工作，請選取工作名稱旁邊的核取方塊，然後點擊**開始**按鈕。
   - 若要將新規則新增到現有工作：
     a. 選取工作名稱旁邊的核取方塊，然後點擊**新增規則**按鈕。
     b. 在開啟的頁面上，配置新規則：
     - **此嚴重等級之更新的安裝規則**

       有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

       如果啟用該選項，更新僅修復 Kaspersky 設定的嚴重等級等於或高於所選更新之嚴重性（**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

       如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

       預設情況下已停用該選項。

- **根據 MSRC 此嚴重等級之更新的安裝規則**（僅適用於 Windows Update 更新）

  有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

  如果啟用該選項（僅適用於 Windows Update 更新），更新僅修復 Microsoft Security Response Center (MSRC) 設定的安全等級等於或高於清單中選定的值（**低**、**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

  如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

  預設情況下已停用該選項。

- **該供應商的更新的安裝規則**（僅適用於協力廠商應用程式的更新）

  此選項僅適用於協力廠商應用程式的更新。卡巴斯基安全管理中心雲端主控台僅會安裝由所選更新的同一個供應商提供的應用程式相關更新。未安裝拒絕更新和其他供應商提供的應用程式更新。

  預設情況下已停用該選項。

- **類型更新的安裝規則**

- **所選更新的安裝規則**

- **核准所選更新**

  所選更新將被批准安裝。如果一些應用的更新安裝規則僅允許安裝批准的更新，啟用該選項。

  預設情況下已停用該選項。

- **自動安裝所選更新安裝時需要的所有先前應用程式更新**

  如果在安裝所選更新需要時，您同意安裝暫時應用程式版本，保持該選項被啟用。

  如果停用該選項，僅選定的應用程式版本被安裝。如果您想直截了當地更新應用程式，而不嘗試安裝增量版本，請停用該選項。如果安裝所選更新不能不安裝先前版本的應用程式，應用程式更新失敗。

  例如，您在裝置上安裝了應用程式的版本 3，您想更新它到版本 5，但是該應用程式的版本 5 僅可以在版本 4 之上安裝。如果啟用該選項，軟體先安裝版本 4，然後安裝版本 5。如果停用該選項，軟體更新應用程式失敗。

  預設情況下已啟用該選項。

c. 點擊**新增**按鈕。

- 要建立工作：

  a. 點擊**新工作**按鈕。

  b. 在開啟的頁面上，配置新規則：

  - **此嚴重等級之更新的安裝規則**

有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

如果啟用該選項，更新僅修復 Kaspersky 設定的嚴重等級等於或高於所選更新之嚴重性（**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

預設情況下已停用該選項。

- **根據 MSRC 此嚴重等級之更新的安裝規則**（僅適用於 Windows Update 更新）

  有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

  如果啟用該選項（僅適用於 Windows Update 更新），更新僅修復 Microsoft Security Response Center (MSRC) 設定的安全等級等於或高於清單中選定的值（**低**、**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

  如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

  預設情況下已停用該選項。

- **該供應商的更新的安裝規則**（僅適用於協力廠商應用程式的更新）

  此選項僅適用於協力廠商應用程式的更新。卡巴斯基安全管理中心雲端主控台僅會安裝由所選更新的同一個供應商提供的應用程式相關更新。未安裝拒絕更新和其他供應商提供的應用程式更新。

  預設情況下已停用該選項。

- **類型更新的安裝規則**
- **所選更新的安裝規則**
- **核准所選更新**

  所選更新將被批准安裝。如果一些應用的更新安裝規則僅允許安裝批准的更新，啟用該選項。

  預設情況下已停用該選項。

- **自動安裝所選更新安裝時需要的所有先前應用程式更新**

  如果在安裝所選更新需要時，您同意安裝暫時應用程式版本，保持該選項被啟用。

  如果停用該選項，僅選定的應用程式版本被安裝。如果您想直截了當地更新應用程式，而不嘗試安裝增量版本，請停用該選項。如果安裝所選更新不能不安裝先前版本的應用程式，應用程式更新失敗。

  例如，您在裝置上安裝了應用程式的版本 3，您想更新它到版本 5，但是該應用程式的版本 5 僅可以在版本 4 之上安裝。如果啟用該選項，軟體先安裝版本 4，然後安裝版本 5。如果停用該選項，軟體更新應用程式失敗。

  預設情況下已啟用該選項。

c. 點擊**新增**按鈕。

如果選擇啟動工作，則可以關閉精靈。該工作將在後台模式下完成。不需要進一步操作。

如果您選擇將規則新增到現有工作，則會開啟工作內容視窗。新規則已新增到工作屬性中。您可以檢視或修改規則或其他工作設定。按一下**儲存**按鈕以儲存變更。

如果選擇建立工作，請在「新工作精靈」中繼續建立工作。您在更新安裝精靈中新增的規則將顯示在「新建工作精靈」中。當您完成新工作精靈時，*安裝所需更新並修復弱點*工作將已新增到工作清單中。

建立「尋找弱點和所需更新」工作

卡巴斯基安全管理中心雲端主控台會透過弱點掃描和所需更新工作，收到在受管理裝置上已安裝的協力廠商軟體中偵測到的弱點與所需更新的清單。

弱點掃描和所需更新工作會在快速設定精靈執行時自動建立。如果您未執行精靈，您可手動建立該工作。

若要建立弱點掃描和所需更新工作：

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

   新工作精靈啟動。遵照精靈的說明。
3. 對於卡巴斯基安全管理中心雲端主控台應用程式，請選取**弱點掃描和所需更新**工作類型。
4. 指定您正建立的工作的名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。
5. 選取要分配工作的裝置。
6. 若要修改預設工作設定，請啟用**完成工作建立**頁面的**建立完成時開啟工作詳情**選項。如果您不啟用該選項，工作使用預設設定建立。您可以稍後隨時修改預設設定。
7. 點擊**建立**按鈕。

   工作被建立並顯示在工作清單。
8. 按一下建立的工作的名稱以開啟工作內容視窗。
9. 在工作內容視窗中，指定一般工作設定。
10. 在**應用程式設定**頁籤中，指定以下設定：

    - **搜尋 Microsoft 列出的弱點和更新**

      搜尋弱點與更新時，卡巴斯基安全管理中心雲端主控台會使用向 Microsoft 更新來源所取得關於當時可用之適用 Microsoft 更新的資訊。

      例如，如果您對 Microsoft 更新和協力廠商應用程式更新有不同設定與不同工作，您可能會需要停用此選項。

      預設情況下已啟用該選項。

    - **連線更新伺服器更新資料**

受管理裝置上的 Windows Update 代理程式會連線至 Microsoft 更新來源。以下伺服器會以 Microsoft 更新來源運作：

- 卡巴斯基安全管理中心雲端主控台管理伺服器（請參閱網路代理政策的設定）
- 具備 Microsoft Windows Server Update Services (WSUS) 的 Windows 伺服器會佈署在貴組織的網路中
- Microsoft Updates 伺服器

如果啟用該選項，受管理裝置上的 Windows Update 代理程式會連線至 Microsoft 更新來源，以重新整理可應用的 Microsoft Windows Update 資訊。

若停用此選項，受管理裝置上的 Windows Update 代理程式會使用適用 Microsoft Windows 更新的資訊，此資訊先前從 Microsoft 更新來源取得，儲存在裝置的快取中。

到 Microsoft 更新來源的連線可能消耗資源。若您的其他工作或網路代理政策內容中的**軟體更新和弱點**區域設定一般連線至此更新來源，您可能需要停用此選項。若您不要停用此選項，為了降低伺服器過載，您可設定工作排程來隨機使工作在 360 分鐘內延遲啟動。

預設情況下已啟用該選項。

網路代理政策設定的以下選項組合會定義取得更新的模式：

- 只有在**Windows Update 搜尋模式**設定群組中啟用**連線更新伺服器更新資料**選項與 **主動**選項時，才會選取受管理裝置上的 Windows Update 代理程式會連線更新伺服器以取得更新。
- 受管理裝置上的 Windows Update 代理程式會使用適用的 Microsoft Windows 更新資訊，此資訊先前從 Microsoft 更新來源取得，儲存在裝置的快取中，若在**Windows Update 搜尋模式**設定群組啟用**連線更新伺服器更新資料**選項，則會選取**被動**選項，或若在**Windows Update 搜尋模式**設定群組停用**連線更新伺服器更新資料**選項，則會選取**主動**選項。
- 無論**連線更新伺服器更新資料**選項為啟用還是停用狀態，只要選取了 **Windows Update 搜尋模式**群組設定中的**已停用**選項，卡巴斯基安全管理中心雲端主控台便不會請求任何更新資訊。

- **搜尋 Kaspersky 列出的第三方弱點和更新**

如果啟用此選項，卡巴斯基安全管理中心雲端主控台會在 Windows 登錄檔以及**指定檔案系統中應用程式進階搜尋的路徑**下指定的資料夾中，搜尋協力廠商應用程式（由 Kaspersky 和 Microsoft 以外的其他軟體供應商提供的應用程式）的弱點與所需更新。支援的協力廠商應用程式的完整清單由 Kaspersky 管理。

如果停用此選項，則卡巴斯基安全管理中心雲端主控台不會搜尋協力廠商應用程式的弱點與所需更新。例如，如果您有帶有不同 Microsoft Windows 更新和協力廠商應用程式更新設定的不同工作，您可能想要停用該選項。

預設情況下已啟用該選項。

- **指定檔案系統中應用程式進階搜尋的路徑**

卡巴斯基安全管理中心雲端主控台要到哪些資料夾中搜尋需要修復弱點和安裝更新的協力廠商應用程式。您可以使用系統變數。

指定應用程式安裝資料夾。此清單預設會空白。

- **啟用進階診斷**

如果啟用此功能，即便在卡巴斯基安全管理中心雲端主控台遠端診斷公用程式中對網路代理停用了偵錯，網路代理也會寫入偵錯。偵錯輪流寫入兩個檔案中；兩個檔案的最大大小由**進階診斷檔案的最大大小 (MB)**值決定。當兩個檔案都滿時，網路代理再次開始寫入它們。帶有偵錯的檔案儲存在 %WINDIR%\Temp 資料夾。這些檔案可供在遠端診斷公用程式中存取，您可以在該處下載或刪除這些檔案。

如果停用此功能，則網路代理會根據卡巴斯基安全管理中心雲端主控台遠端診斷公用程式中的設定寫入偵錯。沒有附加偵錯被寫入。

當建立工作時，您不必啟用進階診斷。您可能想要使用該功能，如果，例如，工作在一些裝置上失敗且您想要在另一個工作執行期間獲取額外資訊。

預設情況下已停用該選項。

- **進階診斷檔案的最大大小 (MB)**

  預設值是 100 MB，可用值介於 1 MB 和 2,048 MB 之間。當您所傳送的進階診斷檔案資訊不足以定位問題時，您可能被 Kaspersky 技術支援專家需求變更預設值。

11. 點擊**儲存**按鈕。

工作被建立和配置。

若工作結果包含 0x80240033「Windows 更新代理錯誤 80240033（「無法下載產品授權期限」）」警告，您可以透過 Windows 登錄資料解決此問題。

「尋找弱點和所需更新」工作設定

*弱點掃描和所需更新*工作會在快速設定精靈執行時自動建立。如果您未執行精靈，您可手動建立該工作。

除了一般工作設定外，您可在建立*弱點掃描和所需更新*工作，或在之後設定已建立工作的內容時，指定以下設定：

- **搜尋 Microsoft 列出的弱點和更新**

  搜尋弱點與更新時，卡巴斯基安全管理中心雲端主控台會使用向 Microsoft 更新來源所取得關於當時可用之適用 Microsoft 更新的資訊。

  例如，如果您對 Microsoft 更新和協力廠商應用程式更新有不同設定與不同工作，您可能會需要停用此選項。

  預設情況下已啟用該選項。

- **連線更新伺服器更新資料**

受管理裝置上的 Windows Update 代理程式會連線至 Microsoft 更新來源。以下伺服器會以 Microsoft 更新來源運作：

- 卡巴斯基安全管理中心雲端主控台管理伺服器（請參閱網路代理政策的設定）
- 具備 Microsoft Windows Server Update Services (WSUS) 的 Windows 伺服器會佈署在貴組織的網路中
- Microsoft Updates 伺服器

如果啟用該選項，受管理裝置上的 Windows Update 代理程式會連線至 Microsoft 更新來源，以重新整理可應用的 Microsoft Windows Update 資訊。

若停用此選項，受管理裝置上的 Windows Update 代理程式會使用適用 Microsoft Windows 更新的資訊，此資訊先前從 Microsoft 更新來源取得，儲存在裝置的快取中。

到 Microsoft 更新來源的連線可能消耗資源。若您的其他工作或網路代理政策內容中的**軟體更新和弱點**區域設定一般連線至此更新來源，您可能需要停用此選項。若您不要停用此選項，為了降低伺服器過載，您可設定工作排程來隨機使工作在 360 分鐘內延遲啟動。

預設情況下已啟用該選項。

網路代理政策設定的以下選項組合會定義取得更新的模式：

- 只有在**Windows Update 搜尋模式**設定群組中啟用**連線更新伺服器更新資料**選項與 **主動**選項時，才會選取受管理裝置上的 Windows Update 代理程式會連線更新伺服器以取得更新。
- 受管理裝置上的 Windows Update 代理程式會使用適用的 Microsoft Windows 更新資訊，此資訊先前從 Microsoft 更新來源取得，儲存在裝置的快取中，若在**Windows Update 搜尋模式**設定群組啟用**連線更新伺服器更新資料**選項，則會選取**被動**選項，或若在**Windows Update 搜尋模式**設定群組停用**連線更新伺服器更新資料**選項，則會選取**主動**選項。
- 無論**連線更新伺服器更新資料**選項為啟用還是停用狀態，只要選取了 **Windows Update 搜尋模式**群組設定中的**已停用**選項，卡巴斯基安全管理中心雲端主控台便不會請求任何更新資訊。

- **搜尋 Kaspersky 列出的第三方弱點和更新**

如果啟用此選項，卡巴斯基安全管理中心雲端主控台會在 Windows 登錄檔以及**指定檔案系統中應用程式進階搜尋的路徑**下指定的資料夾中，搜尋協力廠商應用程式（由 Kaspersky 和 Microsoft 以外的其他軟體供應商提供的應用程式）的弱點與所需更新。支援的協力廠商應用程式的完整清單由 Kaspersky 管理。

如果停用此選項，則卡巴斯基安全管理中心雲端主控台不會搜尋協力廠商應用程式的弱點與所需更新。例如，如果您有帶有不同 Microsoft Windows 更新和協力廠商應用程式更新設定的不同工作，您可能想要停用該選項。

預設情況下已啟用該選項。

- **指定檔案系統中應用程式進階搜尋的路徑**

卡巴斯基安全管理中心雲端主控台要到哪些資料夾中搜尋需要修復弱點和安裝更新的協力廠商應用程式。您可以使用系統變數。

指定應用程式安裝資料夾。此清單預設會空白。

- **啟用進階診斷**

如果啟用此功能，即便在卡巴斯基安全管理中心雲端主控台遠端診斷公用程式中對網路代理停用了偵錯，網路代理也會寫入偵錯。偵錯輪流寫入兩個檔案中；兩個檔案的最大大小由**進階診斷檔案的最大大小 (MB)**值決定。當兩個檔案都滿時，網路代理再次開始寫入它們。帶有偵錯的檔案儲存在 %WINDIR%\Temp 資料夾。這些檔案可供在遠端診斷公用程式中存取，您可以在該處下載或刪除這些檔案。

如果停用此功能，則網路代理會根據卡巴斯基安全管理中心雲端主控台遠端診斷公用程式中的設定寫入偵錯。沒有附加偵錯被寫入。

當建立工作時，您不必啟用進階診斷。您可能想要使用該功能，如果，例如，工作在一些裝置上失敗且您想要在另一個工作執行期間獲取額外資訊。

預設情況下已停用該選項。

- **進階診斷檔案的最大大小 (MB)**

  預設值是 100 MB，可用值介於 1 MB 和 2,048 MB 之間。當您所傳送的進階診斷檔案資訊不足以定位問題時，您可能被 Kaspersky 技術支援專家需求變更預設值。

工作排程的建議

排程*弱點掃描和所需更新*工作時，請確保啟用**執行錯過的工作**與**使用工作啟動自動隨機延遲**兩個選項。

依預設，*弱點掃描和所需更新*工作設定為手動啟動。如果組織的工作規則要在此時關閉所有裝置，*弱點掃描和所需更新*工作將在裝置再次開啟電源時執行，意即，在星期三早上。此活動可能不是必須的，因為弱點掃描可能增加 CPU 和磁碟子系統負載。您必須根據組織的工作規則為該工作設定最方便的排程。

建立安裝必要更新並修復弱點工作

*安裝所需更新並修復弱點*工作的可用性取決於卡巴斯基安全管理中心雲端主控台模式以及您目前的產品授權。

*安裝所需更新並修復弱點*工作會用來更新與修復協力廠商軟體中的弱點，包含安裝在受管理裝置上的 Microsoft 軟體。此工作可讓您根據特定規則安裝多項更新並修復多個弱點。

若要使用*安裝所需更新並修復弱點*工作安裝更新或修復弱點，您可進行以下一項操作：

- 執行更新安裝精靈或弱點修復精靈。
- 建立*安裝所需更新並修復弱點*工作。
- 對現有*安裝所需更新並修復弱點*工作新增安裝更新規則。

軟體更新安裝工作具有一些限制。這些限制取決於您對卡巴斯基安全管理中心雲端主控台使用的產品授權以及卡巴斯基安全管理中心雲端主控台運作的模式。

要建立安裝所需更新並修復弱點工作：

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

新工作精靈啟動。遵照精靈的說明。

3. 對於卡巴斯基安全管理中心雲端主控台應用程式，請選取**安裝所需更新並修復弱點**工作類型。

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

5. 選取要分配工作的裝置。

6. 指定更新安裝的規則，然後指定以下設定：

- **在裝置重新啟動或關閉時開始安裝**

  如果啟用該選項，更新在裝置被重新啟動或關閉時安裝。否則，更新根據排程安裝。

  如果安裝更新可能影響裝置效能則使用該選項。

  預設情況下已停用該選項。

- **安裝所需的一般系統元件**

  如果啟用該選項，在安裝更新之前，應用程式自動安裝所需的所有一般系統元件（先決條件）。例如，這些先決條件可以是作業系統更新。

  如果停用該選項，您可能必須手動安裝先決條件。

  預設情況下已停用該選項。

- **更新過程中允許安裝新的應用程式版本**

  如果啟用該**選項**，如果更新導致軟體應用程式新版本的安裝，更新將被允許。

  如果停用該選項，軟體不被升級。您可以稍後手動或透過其他工作安裝軟體的新版本。例如，如果公司基礎架構不被新軟體版本支援，或者如果您想要在測試基礎架構中檢查升級，您可能使用該選項。

  預設情況下已啟用該選項。

  升級應用程式可能導致安裝在用戶端裝置上的獨立應用程式功能異常。

- **下載更新到裝置而不安裝**

  如果啟用該選項，應用程式下載更新到裝置但是不自動安裝它們。您可以稍後手動安裝下載的更新。

  Microsoft 更新被下載到系統 Windows 儲存。協力廠商應用程式更新（由非 Kaspersky 和 Microsoft 軟體供應商製作的應用程式）會下載到在**下載更新資料夾**欄位指定的資料夾。

  如果停用該選項，更新被自動安裝到裝置。

  預設情況下已停用該選項。

- **下載更新資料夾**

  該資料夾用於下載協力廠商應用程式（由非 Kaspersky 和 Microsoft 軟體供應商製作的應用程式）更新。

- **啟用進階診斷**

如果啟用此功能，即便在卡巴斯基安全管理中心雲端主控台遠端診斷公用程式中對網路代理停用了偵錯，網路代理也會寫入偵錯。偵錯輪流寫入兩個檔案中；兩個檔案的最大大小由**進階診斷檔案的最大大小 (MB)**值決定。當兩個檔案都滿時，網路代理再次開始寫入它們。帶有偵錯的檔案儲存在 %WINDIR%\Temp 資料夾。這些檔案可供在遠端診斷公用程式中存取，您可以在該處下載或刪除這些檔案。

如果停用此功能，則網路代理會根據卡巴斯基安全管理中心雲端主控台遠端診斷公用程式中的設定寫入偵錯。沒有附加偵錯被寫入。

當建立工作時，您不必啟用進階診斷。您可能想要使用該功能，如果，例如，工作在一些裝置上失敗且您想要在另一個工作執行期間獲取額外資訊。

預設情況下已停用該選項。

- **進階診斷檔案的最大大小（MB）**

  預設值是 100 MB，可用值介於 1 MB 和 2,048 MB 之間。當您所傳送的進階診斷檔案資訊不足以定位問題時，您可能被 Kaspersky 技術支援專家需求變更預設值。

7. 指定作業系統重新啟動設定：

- **不重新啟動裝置**

  用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

- **重新啟動裝置**

  如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

- **提示使用者操作**

  用戶端裝置螢幕上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。該選項適用於使用者必須可以選取最方便的時間進行重新啟動的工作站。

  預設情況下已選定此選項。

- **重複提示間隔（分鐘）**

  如果啟用該選項，應用程式以指定頻率提示使用者重新啟動作業系統。

  預設情況下已啟用該選項。預設間隔是 5 分鐘。可用值介於 1 和 1440 分鐘之間。

  如果停用該選項，提示僅顯示一次。

- **在該時間後重新啟動（分鐘）**

  提示使用者之後，應用程式在指定時間間隔後強制作業系統重新啟動。

  預設情況下已啟用該選項。預設延時是 30 分鐘。可用值介於 1 和 1440 分鐘之間。

- **強制關閉封鎖工作階段中應用程式前的等待時間（分鐘）**

  使用者裝置鎖定時，程式以強制模式關閉（指定不活動間隔之後自動鎖定，或手動鎖定）。
  如果啟用此選項，一旦輸入區域指定的時間間隔結束，鎖定裝置上的程式以強制模式關閉。
  如果停用此選項，鎖定裝置上的程式將不會關閉。
  預設情況下已停用該選項。

8. 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。

9. 點擊**完成**按鈕。
   工作被建立並顯示在工作清單。

10. 按一下建立的工作的名稱以開啟工作內容視窗。

11. 在工作內容視窗中，依需求指定一般工作設定。

12. 點擊**儲存**按鈕。
    工作被建立和配置。

若工作結果包含 0x80240033「Windows 更新代理錯誤 80240033（「無法下載產品授權期限」）」警告，您可以透過 Windows 登錄資料解決此問題。

新增安裝更新的規則

此功能的可用性取決於卡巴斯基安全管理中心雲端主控台模式以及您目前的產品授權。

使用*安裝所需更新並修復弱點*工作安裝軟體更新或修復軟體弱點時，您必須指定安裝更新的規則。這些規則決定要安裝的更新和要修復的弱點。

精確設定會視您是否建立 Microsoft 應用程式、協力廠商應用程式（由非 Kaspersky 和 Microsoft 軟體供應商製作的應用程式）、或所有應用程式更新的規則而定。當新增 Windows Update 更新或協力廠商應用程式的更新規則時，您可以選取特定的應用程式和您要安裝更新的應用程式版本。當新增所有更新的規則時，您可以選取要安裝的特定更新，以及要透過安裝更新而修復的弱點。

您可以透過以下方式建立更新的安裝規則：

- 透過在建立新的安裝所需更新並修復弱點工作時新增規則。
- 透過在現有*安裝所需更新並修復弱點*工作屬性視窗的**應用程式設定**索引標籤上新增規則。
- 透過更新安裝精靈或弱點修復精靈。

若要為所有更新建立新規則：

1. 點擊**新增**按鈕。
   規則建立精靈開始。使用**下一步**按鈕進行精靈。

2. 在**規則類型**頁面上，選擇**所有更新的規則**。

3. 在**一般標準**頁面，使用下拉清單指定以下設定：

- **要安裝的更新集**

  選取必須在用戶端裝置上安裝的更新：

  - **僅安裝批准的更新**。這僅安裝批准的更新。
  - **安裝所有更新（除了拒絕的）**。這安裝帶有*已批准*或*未定義*批准狀態的更新。
  - **安裝所有更新（包含拒絕的）**。這安裝所有更新，無論什麼批准狀態。警惕選取該選項。例如，如果您想要在測試基礎架構中檢查一些被拒絕的更新的安裝，使用該選項。

- **修復弱點的時機為嚴重等級大於或等於**

  有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

  如果啟用該選項，更新僅修復 Kaspersky 設定的安全等級等於或高於清單中選定的值（**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

  如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

  預設情況下已停用該選項。

4. 在**更新**頁面，選取要安裝的更新：

- **安裝所有合適的更新**

  安裝滿足在精靈中**一般標準**頁面指定標準的所有軟體更新。預設選取。

- **僅安裝清單中的更新**

  僅安裝您從清單中手動選取的軟體更新。該清單包含所有可用軟體更新。

  例如，您可能想要在以下情況下選取特定更新：要在測試環境中檢查它們的安裝、要僅更新嚴重應用程式、或者要僅更新特定應用程式。

- **自動安裝所選更新安裝時需要的所有先前應用程式更新**

  如果在安裝所選更新需要時，您同意安裝暫時應用程式版本，保持該選項被啟用。

  如果停用該選項，僅選定的應用程式版本被安裝。如果您想直截了當地更新應用程式，而不嘗試安裝增量版本，請停用該選項。如果安裝所選更新不能不安裝先前版本的應用程式，應用程式更新失敗。

  例如，您在裝置上安裝了應用程式的版本 3，您想更新它到版本 5，但是該應用程式的版本 5 僅可以在版本 4 之上安裝。如果啟用該選項，軟體先安裝版本 4，然後安裝版本 5。如果停用該選項，軟體更新應用程式失敗。

  預設情況下已啟用該選項。

5. 在**弱點**頁面，選取將由安裝所選更新修復的弱點。

- **修復所有符合其他標準的弱點**

修復滿足在精靈中**一般標準**頁面指定標準的所有弱點。預設選取。

- **僅修復清單中的弱點**

  僅修復您手動從清單中選取的弱點。清單包含所有偵測到的弱點。

  例如，您可能想要在以下情況下選取特定弱點：要在測試環境中檢查它們的修復、要僅修復嚴重應用程式中的弱點、或者要僅修復特定應用程式中的弱點。

6. 在**名稱**頁面，指定您正在建立的規則名稱。您可以稍後在所建立工作的內容視窗的**設定**區域變更該名稱。

「規則建立精靈」完成操作後，系統會建立新規則並顯示在「新工作精靈」或工作屬性的欄位中。

若要為 Windows Update 更新建立新規則：

1. 點擊**新增**按鈕。

   規則建立精靈開始。使用**下一步**按鈕進行精靈。

2. 在**規則類型**頁面上，選擇 **Windows Update 的規則**。

3. 在**一般標準**頁面中，指定以下設定：

- **要安裝的更新集**

  選取必須在用戶端裝置上安裝的更新：

  - **僅安裝批准的更新**。這僅安裝批准的更新。
  - **安裝所有更新（除了拒絕的）**。這安裝帶有*已批准*或*未定義*批准狀態的更新。
  - **安裝所有更新（包含拒絕的）**。這安裝所有更新，無論什麼批准狀態。警惕選取該選項。例如，如果您想要在測試基礎架構中檢查一些被拒絕的更新的安裝，使用該選項。

- **修復弱點的時機為嚴重等級大於或等於**

  有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

  如果啟用該選項，更新僅修復 Kaspersky 設定的安全等級等於或高於清單中選定的值（**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

  如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

  預設情況下已停用該選項。

- **修復弱點的時機為 MSRC 嚴重等級大於**

  有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

  如果啟用該選項，更新僅修復 Microsoft Security Response Center (MSRC) 設定的安全等級等於或高於清單中選定的值（**低**、**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

  如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

  預設情況下已停用該選項。

4. 在**應用程式**頁面，選取您要安裝更新的應用程式和應用程式版本。預設情況下選定所有應用程式。

5. 在**更新類別**頁面，選取要安裝的更新類別。這些類別與 Microsoft Update Catalog 中的類別相同。預設情況下選定所有類別。

6. 在**名稱**頁面，指定您正在建立的規則名稱。您可以稍後在所建立工作的內容視窗的**設定**區域變更該名稱。

「規則建立精靈」完成操作後，系統會建立新規則並顯示在「新工作精靈」或工作屬性的欄位中。

若要為協力廠商應用程式更新建立規則：

1. 點擊**新增**按鈕。

   規則建立精靈開始。使用**下一步**按鈕進行精靈。

2. 在**規則類型**頁面上，選擇**協力廠商更新的規則**。

3. 在**一般標準**頁面中，指定以下設定：

   - **要安裝的更新集**

     選取必須在用戶端裝置上安裝的更新：

     - **僅安裝批准的更新**。這僅安裝批准的更新。
     - **安裝所有更新（除了拒絕的）**。這安裝帶有*已批准*或*未定義*批准狀態的更新。
     - **安裝所有更新（包含拒絕的）**。這安裝所有更新，無論什麼批准狀態。警惕選取該選項。例如，如果您想要在測試基礎架構中檢查一些被拒絕的更新的安裝，使用該選項。

   - **修復弱點的時機為嚴重等級大於或等於**

     有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

     如果啟用該選項，更新僅修復 Kaspersky 設定的安全等級等於或高於清單中選定的值（**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

     如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

     預設情況下已停用該選項。

4. 在**應用程式**頁面，選取您要安裝更新的應用程式和應用程式版本。預設情況下選定所有應用程式。

5. 在**名稱**頁面，指定您正在建立的規則名稱。您可以稍後在所建立工作的內容視窗的設定區域變更該名稱。

「規則建立精靈」完成操作後，系統會建立新規則並顯示在「新工作精靈」或工作屬性的欄位中。

建立安裝 Windows Update 更新工作

「安裝 Windows Update 更新」工作可讓您在用戶端裝置上，安裝由 Windows Update 服務提供的軟體更新。

軟體更新安裝工作具有一些限制。這些限制取決於您對卡巴斯基安全管理中心雲端主控台使用的產品授權以及卡巴斯基安全管理中心雲端主控台運作的模式。

若要建立安裝 Windows Update 更新的工作：

1. 在主功能表中，轉至 **資產（裝置）→ 工作**。
2. 點擊**新增**。
   新工作精靈啟動。使用**下一步**按鈕進行精靈。
3. 對於卡巴斯基安全管理中心雲端主控台應用程式，請選取**安裝 Windows Update 更新**工作類型。
4. 指定您正建立的工作的名稱。
   工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。
5. 選取要分配工作的裝置。
6. 點擊**新增**按鈕。
   更新清單隨即開啟。
7. 選取您要安裝的 Windows Update，之後點擊**確定**。
8. 指定作業系統重新啟動設定：

- **不重新啟動裝置**

  用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

- **重新啟動裝置**

  如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

- **提示使用者操作**

  用戶端裝置螢幕上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。該選項適用於使用者必須可以選取最方便的時間進行重新啟動的工作站。

  預設情況下已選定此選項。

- **重複提示間隔（分鐘）**

  如果啟用該選項，應用程式以指定頻率提示使用者重新啟動作業系統。

  預設情況下已啟用該選項。預設間隔是 5 分鐘。可用值介於 1 和 1440 分鐘之間。

  如果停用該選項，提示僅顯示一次。

- **在該時間後重新啟動（分鐘）**

  提示使用者之後，應用程式在指定時間間隔後強制作業系統重新啟動。

  預設情況下已啟用該選項。預設延時是 30 分鐘。可用值介於 1 和 1440 分鐘之間。

- **強制關閉被封鎖工作階段中的應用程式**

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

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

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

  預設情況下已停用該選項。

9. 指定帳戶設定：

   - **預設帳戶**

     在與執行該工作的應用程式相同的帳戶下執行該工作。

     預設情況下已選定此選項。

   - **指定帳戶**

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

   - **帳戶**

     執行該工作的帳戶。

   - **密碼**

     工作執行時使用的帳戶的密碼。

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

11. 點擊**完成**按鈕。

    工作被建立並顯示在工作清單。

12. 按一下建立的工作的名稱以開啟工作內容視窗。

13. 在工作內容視窗中，依需求指定一般工作設定。

14. 點擊**儲存**按鈕。

工作被建立和配置。

檢視可用協力廠商軟體更新的資訊

您可檢視安裝在用戶端裝置之協力廠商軟體可用更新的清單，包含 Microsoft 軟體。

若要檢視安裝在用戶端裝置之協力廠商應用程式的可用更新清單，

在主功能表中，轉至 **操作 → 修補程式管理 → 軟體更新**。

可用更新清單被顯示。

您可指定篩選條件以檢視軟體更新的清單。點擊軟體更新清單右上角的**篩選器**圖示（ ）來管理篩選條件。您也可從軟體弱點清單上方的**預設篩選器** 下拉清單選取其中一個預設篩選條件。

要檢視更新的內容：

1. 點擊所需軟體更新的名稱。
2. 更新的屬性視窗隨即開啟，並顯示透過以下索引標籤分組的資訊：

- **一般**

  此索引標籤顯示所選更新的一般詳細資料：

  - 更新批准狀態（您可以透過在下拉清單中選取新狀態來手動更改）
  - 此更新所屬的 Windows Server Update Services (WSUS) 類別
  - 登錄更新的日期和時間
  - 建立更新的日期和時間
  - 更新的重要層級
  - 更新要求的安裝要求
  - 更新所屬的應用程式系列
  - 更新適用的應用程式
  - 更新修訂編號

- **內容**

此索引標籤會顯示一組屬性，您可將其用來取得所選更新的詳細資訊。此集合將視更新是由 Microsoft 還是協力廠商供應商發布的而有所不同。

該索引標籤會顯示 Microsoft 更新的以下資訊：

- Microsoft 安全回應中心 (MSRC) 定義的更新嚴重等級
- 連結到 Microsoft 知識庫中說明更新的文章
- 連結到 Microsoft 安全公告中說明此更新的文章
- 更新識別碼 (ID)

該索引標籤顯示以下協力廠商更新的相關資訊：

- 此更新是修補程式還是完整分發套件
- 更新的本地化語言
- 是自動安裝還是手動安裝更新
- 套用後是否撤銷該更新
- 下載更新的連結

- **裝置**

  此索引標籤顯示已安裝所選更新裝置的清單。

- **已修復弱點**

  此索引標籤顯示所選更新可以修復的漏洞清單。

- **更新融合**

  此索引標籤顯示相同應用程式發佈之各種更新間的可能交集，即所選更新是否可以取代其他更新，反之是否可以由其他更新取代（僅適用於 Microsoft 更新）。

- **安裝該更新的工作**

  此索引標籤顯示工作清單，其範圍包括所選更新的安裝。該索引標籤還使您可以為更新建立新的遠端安裝工作。

若要檢視更新安裝的統計：

1. 選取所需軟體更新旁邊的核取方塊。
2. 點擊**更新安裝狀態統計資訊**按鈕。

更新安裝狀態圖表隨即顯示。點擊狀態會開啟裝置清單，其更新為所選狀態。

在所選取且執行 Windows 的受管理裝置上，您可檢視已安裝之協力廠商軟體可用軟體更新的資訊，包含 Microsoft 軟體。

若要在選取的受管理裝置上，檢視已安裝的協力廠商軟體可用更新清單：

1. 在主功能表中，轉至 **資產（裝置）→ 受管理裝置**。
   受管理裝置清單隨即顯示。
2. 在受管理裝置清單中，點擊有您要檢視之協力廠商軟體更新的裝置名稱連結。
   所選裝置的屬性視窗隨即顯示。
3. 在所選裝置的內容視窗中，選取**進階**頁籤。
4. 在左窗格中，選取**可用更新**區段。若要只檢視已安裝的更新，請啟用**顯示已安裝的更新**選項。

選取的裝置上可用協力廠商軟體更新的清單隨即顯示。

將可用軟體更新清單匯出至檔案

您可匯出協力廠商軟體更新清單，包含 Microsoft 軟體，目前可以 CSV 或 TXT 檔案顯示。您可使用這些檔案，例如將它們傳送至您的資訊安全經理，或儲存起來以供統計使用。

若要將所有受管理裝置安裝之協力廠商軟體的可用更新清單匯出為文字檔案：

1. 在主功能表中，轉至 **操作 → 修補程式管理 → 軟體更新**。
   此頁面會顯示在所有受管理裝置上已安裝之協力廠商軟體的可用更新清單。
2. 點擊**匯出到 TXT**或**匯出到 CSV**按鈕，視您偏好的匯出格式而定。

內含協力廠商軟體可用更新清單的檔案，包含 Microsoft 軟體，會現在至您目前使用的裝置。

若要將所選受管理裝置安裝之協力廠商軟體的可用更新清單匯出為文字檔案：

1. 開啟所選受管理裝置之協力廠商軟體更新的清單。
2. 選取您要匯出的軟體更新。
   若要匯出完整的軟體更新清單請略過此步驟。
   若要匯出軟體更新的完整清單，僅會匯出顯示在目前頁面的更新。
   若要僅匯出安裝的更新，請選取 **顯示已安裝的更新** 核取方塊。
3. 點擊**匯出到 TXT**或**匯出到 CSV**按鈕，視您偏好的匯出格式而定。

含在所選受管理裝置安裝之協力廠商軟體更新清單的檔案，包含 Microsoft 軟體，會下載至您目前使用的裝置。

核准與拒絕協力廠商軟體更新

當您設定*安裝必要更新並修正弱點*工作時，您可建立要安裝之更新需要的更新特定狀態規則。例如，更新規則可允許以下安裝：

- 僅核准的更新
- 僅核准且未定義的更新
- 無論更新狀態為何的所有更新

您可以批准必須安裝的更新並拒絕不能安裝的更新。

對於少量更新而言，使用*已批准*狀態來管理更新安裝非常有效。若要安裝多個更新，請使用可在*安裝所需的更新和修復漏洞*工作中配置的規則。建議您僅為那些不符合規則中指定條件的特定更新設定*已批准*狀態。當您手動批准大量更新時，管理伺服器的效能下降，這可能導致伺服器過載。

要批准或拒絕一個或幾個更新：

1. 在主功能表中，轉至 **操作 → 修補程式管理 → 軟體更新**。
   可用更新清單被顯示。
2. 選取您要批准或拒絕的更新。
3. 點擊**批准**以核准選取的更新或**拒絕**以拒絕選取的更新。
   預設值是*未定義*。

選取的更新有您定義的狀態。

您也可以選擇在特定更新的屬性中更改批准狀態。

批准或拒絕其屬性中的更新：

1. 在主功能表中，轉至 **操作 → 修補程式管理 → 軟體更新**。
   可用更新清單被顯示。
2. 點擊您要批准或拒絕的更新名稱。
   更新屬性視窗隨即開啟。
3. 在**一般**區段，透過更改**更新批准狀態**選項來選取更新狀態。您可以選取*已批准*、*已拒絕*或*未定義*狀態。
4. 按一下**儲存**按鈕以儲存變更。

選取的更新有您定義的狀態。

如果您為協力廠商軟體更新設定了**已拒絕**狀態，則已計畫但未安裝這些更新的裝置將不會安裝這些更新。更新將保持在已將其安裝的裝置上。如果您必須刪除它們，您可以在本機手動刪除它們。

自動更新協力廠商應用程式

某些協力廠商應用程式可以自動更新。應用程式供應商會定義應用程式是否支持自動更新功能。如果受管理裝置上安裝的協力廠商應用程式支援自動更新，則可以在應用程式屬性中指定自動更新設定。更改自動更新設定後，網路代理會在安裝了應用程式的每個受管理裝置上套用新設定。

自動更新設定獨立於其他物件和弱點和修補程式管理功能的設定。例如，此設定會以更新批准狀態或更新安裝工作為依據，例如*安裝所需更新並修復弱點*，*安裝 Windows Update 更新*和*修復弱點*。

若要為協力廠商應用程式配置自動更新設定：

1. 在主功能表中，轉至 **操作 → 協力廠商應用程式 → 應用程式登錄資料**。
2. 點擊要為其更改自動更新設定的應用程式名稱。

   若要簡化搜尋，您可以依照**自動更新狀態**欄篩選清單。

   應用程式屬性視窗隨即開啟。
3. 在**一般**區段中，為以下設定選取一個值：

   自動更新狀態

   您可以選取以下其中一個方法：

   - **未定義**

     自動更新功能已停用。卡巴斯基安全管理中心雲端主控台會透過以下工作來安裝協力廠商應用程式更新：*安裝所需更新並修復弱點*、*安裝 Windows Update 更新*以及*修復弱點*。
   - **允許**

     供應商發布該應用程式的更新後，此更新將自動安裝在受管理裝置上。不需要進一步操作。
   - **已封鎖**

     這些更新不會自動安裝。卡巴斯基安全管理中心雲端主控台會透過以下工作來安裝協力廠商應用程式更新：*安裝所需更新並修復弱點*、*安裝 Windows Update 更新*以及*修復弱點*。
4. 按一下**儲存**按鈕以儲存變更。

自動更新設定將套用在所選應用程式。

修復協力廠商軟體弱點

本節說明卡巴斯基安全管理中心雲端主控台中，與修復受管理裝置上所安裝軟體中的弱點相關的功能。

情境：尋找並修復軟體弱點

本節說明在執行 Windows 的受管理裝置上尋找與修復弱點的情境。您可在作業系統與協力廠商軟體（包含 Microsoft 軟體）中尋找並修復軟體弱點。

先決條件

- 卡巴斯基安全管理中心雲端主控台已部署到您的組織中。
- 您組織中有執行 Windows 的受管理裝置。

階段

分階段尋找並修復軟體弱點：

1. **掃描用戶端裝置上所安裝軟體中的弱點**

   若要在受管理裝置已安裝軟體中尋找弱點，請執行*弱點掃描和所需更新*工作。當該工作完成時，Kaspersky Security Center Cloud Console 會收到在您工作內容中指定的裝置上已安裝的軟體中偵測到的弱點與所需更新的清單。

   卡巴斯基安全管理中心雲端主控台快速啟動精靈會自動建立*弱點掃描和所需更新*工作。如果您未執行精靈，請立即將其啟動或手動建立工作。

   操作說明：建立弱點掃描和所需更新工作

2. **分析偵測到的軟體弱點清單**

   檢視**軟體弱點**清單並決定要修復的弱點。若要檢視各弱點的詳細資訊，請按一下清單中的弱點名稱。對於清單中的各個，您也可檢視受管理裝置上弱點的統計資料。

   說明：

   - 檢視軟體弱點資訊
   - 檢視受管理裝置的弱點統計資料

3. **設定弱點修復**

   偵測到軟體弱點時，您可使用*安裝所需更新並修復弱點*工作或*修復弱點*工作修復受管理裝置上的軟體弱點。

   *安裝所需更新並修復弱點*工作會用來更新與修復協力廠商軟體中的弱點，包含安裝在受管理裝置上的 Microsoft 軟體。該工作可讓您根據特定規則安裝多項更新並修復多個弱點。該工作的可用性取決於卡巴斯基安全管理中心雲端主控台模式以及您目前的產品授權。為了修復軟體弱點，*安裝所需更新並修復弱點*工作會使用建議的軟體更新。

   *修復弱點*工作會使用 Microsoft 軟體的建議修復項目。

   您可啟動弱點修復精靈，精靈會自動建立以下其中一種這類工作或您可手動建立其中一種這類工作。

   操作說明：修復協力廠商軟體中的弱點、建立「安裝必要更新並修復弱點」工作

4. **排程工作**

   為確定弱點清單永遠處於最新狀態，請排程*弱點掃描和所需更新*工作以不時自動執行。建議平均頻率為每週一次。

   若您已建立*安裝所需更新並修復弱點*工作，您可排程與*弱點掃描和所需更新*工作的執行頻率相同會更少。排定*修復弱點*工作時請注意，您在每次啟動工作之前，都必須選取 Microsoft 軟體的修復項目。

   排程工作時，請確定修復弱點的工作會在*弱點掃描和所需更新*工作完成後啟動。

5. **忽略軟體弱點（選用）**

   如有需要，您可忽略所有受管理裝置，或僅忽略已選受管理裝置上要修復的軟體弱點。

   操作說明：忽略軟體弱點

6. **執行修復弱點工作**

   啟動*安裝所需更新並修復弱點*或*修復弱點*工作。工作完成後，請確保工作清單出現*已成功完成*狀態。

7. **建立修復軟體弱點的結果報告（選用）**

   若要檢視弱點修復的詳細統暨，請產生弱點報告。報告會顯示未修復之軟體弱點的資訊。您已知道如何在組織中尋找與修復協力廠商軟體中的弱點（包含 Microsoft 軟體）。

   操作說明：產生和檢視報告

8. **檢查尋找與修復協力廠商軟體中的弱點的配置**

   請確認以下出現跡象：

   - 受管理裝置上的軟體弱點清單並未空白。
   - 工作清單中有修復弱點的工作。
   - 各項用於尋找並修復軟體弱點的工作是依能讓它們循序執行的順序排程。請檢視這些工作的內容來比較其排程。
   - 修復軟體弱點的工作已成功完成。請到工作內容視窗的**結果**頁籤上檢視資訊。

結果

若您已建立並設定*安裝所需更新並修復弱點*工作，弱點會自動在受管理裝置上修復。當工作執行時，會將可用軟體更新的清單與工作設定中指定的規則建立關聯。所有符合規則中所訂條件的軟體更新，都會下載至發佈點的儲存區並受到安裝，以便修復軟體弱點。

若您已建立*修復弱點*工作，僅 Microsoft 軟體中的軟體弱點會被修復。

關於尋找與修復軟體弱點

卡巴斯基安全管理中心雲端主控台會在執行 Microsoft Windows 系列作業系統的受管理裝置上偵測並修復軟體弱點。作業系統和協力廠商軟體（包含 Microsoft 軟體）會偵測弱點。

尋找軟體弱點

為了尋找軟體弱點，卡巴斯基安全管理中心雲端主控台會運用已知弱點資料庫與 Windows Update 資料庫中的特徵。已知弱點資料庫是由 Kaspersky 專家建立並維護。資料庫會包含弱點的資訊，例如弱點敘述、弱點偵測日期、弱點嚴重等級。您可以在 Kaspersky 網站上搜尋軟體弱點詳情。

卡巴斯基安全管理中心雲端主控台是使用*弱點掃描和所需更新*工作尋找軟體弱點。

修復軟體弱點

為了修復軟體弱點，卡巴斯基安全管理中心雲端主控台會使用由軟體供應商簽發的軟體更新。您可以隨時檢視軟體弱點的清單。執行*將更新下載至發佈點儲存區*工作時，會自動將軟體更新的中繼資料下載到管理伺服器儲存區以及發佈點的儲存區。您可以透過卡巴斯基安全管理中心雲端主控台快速啟動精靈或以手動方式建立該工作。

修復弱點的軟體更新可使用完整分發套件或修補程式代表。修復軟體弱點的軟體更新又稱為*修復項目*。在卡巴斯基安全管理中心雲端主控台中，您會使用*建議的修復項目*來修復弱點。建議的修復項目是指由 Kaspersky 專家建議安裝的軟體更新。

視卡巴斯基安全管理中心雲端主控台模式以及您目前的產品授權而定，您可以使用*安裝所需更新並修復弱點*工作或*修復弱點*工作來修復軟體弱點。

*安裝所需更新並修復弱點*工作會在安裝建議的修復項目時，自動修復多個弱點。針對此工作，您可手動設定特定規則來修復多個弱點。

您可以透過*修復弱點*工作，安裝 Microsoft 軟體的建議修復項目來修復弱點。

出於安全原因，卡巴斯基技術會自動掃描您使用弱點和修補程式管理功能安裝的任何協力廠商軟體更新以查找惡意軟體。這些技術用於自動檢查檔案，包括病毒掃描、靜態分析、動態分析、沙箱環境中的行為分析和機器學習。

卡巴斯基專家不會對可以使用弱點和修補程式管理功能安裝的協力廠商軟體更新進行手動分析。此外，卡巴斯基專家不會在此類更新中搜尋弱點（已知或未知）或未記錄的功能，也不會對上述段落中指定的更新以外的其他類型的更新進行分析。

軟體更新安裝工作具有一些限制。這些限制取決於您對卡巴斯基安全管理中心雲端主控台使用的產品授權以及卡巴斯基安全管理中心雲端主控台運作的模式。

在受管理裝置上更新協力廠商應用程式或修復協力廠商應用程式中的弱點時，可能需要使用者互動。例如，若協力廠商應用程式目前開啟，可能會提示使用者關閉協力廠商應用程式。

若要修復一些軟體弱點，您必須接受安裝軟體的最終使用者產品授權協議 (EULA)（若系統要求您接受 EULA）。若您拒絕 EULA，則無法修復軟體弱點。

每個所修復弱點的資訊都會在管理伺服器上儲存 90 天。過了這段時間，即會自動刪除。

修復軟體弱點

取得軟體弱點清單後，您可在執行 Windows 的受管理裝置上修復軟體弱點。您可以透過建立並執行*修復弱點*工作或*安裝所需更新並修復弱點*工作來修復操作系統和協力廠商軟體（包括 Microsoft 軟體）中的軟體弱點。

軟體更新安裝工作具有一些限制。這些限制取決於您對卡巴斯基安全管理中心雲端主控台使用的產品授權以及卡巴斯基安全管理中心雲端主控台運作的模式。

在受管理裝置上更新協力廠商應用程式或修復協力廠商應用程式中的弱點時，可能需要使用者互動。例如，若協力廠商應用程式目前開啟，可能會提示使用者關閉協力廠商應用程式。

您可以建立工作，透過以下方式作為修復軟體弱點的選擇：

- 透過開啟弱點清單並指定要修復的弱點。

  結果，建立了修復軟體弱點的新工作。作為選擇，您可以將所選弱點新增到現有工作。

- 透過執行「弱點修復精靈」。

  此功能的可用性取決於卡巴斯基安全管理中心雲端主控台模式以及您目前的產品授權。

  該精靈簡化了修復弱點工作的建立與設定，並可避免您重複建立含有相同更新安裝清單的工作。

使用弱點清單修復軟體弱點

若要修復軟體弱點：

1. 開啟弱點清單之一：

   - 要開啟一般弱點清單，請在主功能表中，前往**操作 → 修補程式管理 → 軟體弱點**。
   - 若要開啟受管理裝置的弱點清單，請在主功能表中，前往**資產（裝置） → 受管理裝置 → <裝置名稱> → 進階 → 軟體弱點**。
   - 若要開啟特定應用程式的弱點清單，請在主功能表中，前往**操作 → 協力廠商應用程式 → 應用程式登錄資料 → <應用程式名稱> → 弱點**。

   在協力廠商軟體的弱點清單頁面隨即顯示。

2. 選取清單中的一或多個弱點並點擊**修復弱點**按鈕。

   若沒有要修復其中一個所選弱點的建議軟體更新，則會顯示通知訊息。

   若要修復一些軟體弱點，您必須接受安裝軟體的最終使用者產品授權協議 (EULA)（若系統要求您接受 EULA）。若您拒絕 EULA，則無法修復軟體弱點。

3. 您可以選取以下其中一個方法：

   - **新工作**

     新工作精靈啟動。畫面中會預先選取*安裝所需更新並修復弱點*工作或*修復弱點*工作（視卡巴斯基安全管理中心雲端主控台模式以及您目前的產品授權而定）。請按照精靈的步驟完成工作建立。

   - **修復弱點（新增規則到指定工作）**

     選取要向其中新增所選弱點的工作。視卡巴斯基安全管理中心雲端主控台模式以及您目前的產品授權而定，請選取*安裝所需更新並修復弱點*工作或*修復弱點*工作。如果您選取*安裝所需更新並修復弱點*工作，則系統會自動將用於修復所選弱點的新規則新增到所選工作中。如果您選取*修復弱點*工作，則系統會將所選弱點新增到工作內容中。

     工作內容視窗隨即開啟。按一下**儲存**按鈕以儲存變更。

   如果您選擇建立工作，則會建立該工作並將其顯示在以下位置的工作清單中：**資產（裝置） → 工作**。如果您選擇將弱點新增到現有工作中，則這些弱點將儲存在工作屬性中。

要修復協力廠商軟體弱點，請啟動*安裝所需更新並修復弱點*工作或*修復弱點*工作。若您已建立*修復弱點*工作，您需手動指定軟體更新來修復工作設定中的軟體弱點清單。

使用「弱點修復精靈」修復軟體弱點

弱點修復精靈的可用性取決於您使用的產品授權以及卡巴斯基安全管理中心雲端主控台運作的模式。

要使用「弱點修復精靈」來修復軟體弱點：

1. 在主功能表中，轉至 **操作 → 修補程式管理 → 軟體弱點**。

   安裝在受管理裝置之協力廠商軟體的弱點清單頁面隨即顯示。

2. 選取您要移除之規則旁邊的核取方塊。

3. 點擊**執行修復弱點精靈**按鈕。

   弱點修復精靈啟動。**選取修復弱點工作**頁面顯示以下類型的所有現有工作清單：

- *安裝所需更新並修復弱點*
- *安裝 Windows Update 更新*
- *修復弱點*

您不能修改最後兩種工作來安裝新更新。要安裝新更新，您只能使用*安裝所需更新並修復弱點*工作。

4. 如果您希望精靈僅顯示修復所選弱點的工作，請啟用**僅顯示修復此弱點的工作**選項。
5. 選取您要新增的內容：
   - 若要啟動工作，請選取工作名稱旁邊的核取方塊，然後點擊**開始**按鈕。
   - 若要將新規則新增到現有工作：
     a. 選取工作名稱旁邊的核取方塊，然後點擊**新增規則**按鈕。
     b. 在開啟的頁面上，配置新規則：
     - **修復該嚴重等級的弱點規則**

       有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

       如果啟用該選項，更新僅修復 Kaspersky 設定的嚴重等級等於或高於所選更新之嚴重性（**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

       如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

       預設情況下已停用該選項。

     - **透過與所選弱點建議定義的更新類型相同的更新來修復弱點的規則**（僅適用於 Microsoft 軟體弱點）
     - **修復所選供應商應用程式中的弱點規則**（僅適用於協力廠商軟體弱點）
     - **修復所選應用程式的所有版本中的弱點的規則**（僅適用於協力廠商軟體弱點）
     - **修復所選弱點的規則**
     - **批准修復該弱點的更新**

       所選更新將被批准安裝。如果一些應用的更新安裝規則僅允許安裝批准的更新，啟用該選項。

       預設情況下已停用該選項。

     c. 點擊**新增**按鈕。
   - 要建立工作：
     a. 點擊**新工作**按鈕。
     b. 在開啟的頁面上，配置新規則：
     - **修復該嚴重等級的弱點規則**

有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

如果啟用該選項，更新僅修復 Kaspersky 設定的嚴重等級等於或高於所選更新之嚴重性（**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

預設情況下已停用該選項。

- **透過 類型的更新修復弱點的規則**（僅適用於 Microsoft 軟體弱點）
- **修復所選供應商應用程式中的弱點規則**（僅適用於協力廠商軟體弱點）
- **修復所選應用程式的所有版本中的弱點的規則**（僅適用於協力廠商軟體弱點）
- **修復所選弱點的規則**
- **批准修復該弱點的更新**

所選更新將被批准安裝。如果一些應用的更新安裝規則僅允許安裝批准的更新，啟用該選項。

預設情況下已停用該選項。

c. 點擊**新增**按鈕。

如果選擇啟動工作，則可以關閉精靈。該工作將在後台模式下完成。不需要進一步操作。

如果您選擇將規則新增到現有工作，則會開啟工作內容視窗。新規則已新增到工作屬性中。您可以檢視或修改規則或其他工作設定。按一下**儲存**按鈕以儲存變更。

如果選擇建立工作，請在「新工作精靈」中繼續建立工作。您在「弱點修復精靈」中新增的規則將顯示在「新工作精靈」中。當您完成新工作精靈時，*安裝必要更新並修復弱點*工作將已新增到工作清單中。

建立修復弱點工作。

*修復弱點*工作可讓您在執行 Windows 的受管理裝置上修復 Microsoft 軟體中的弱點。

此功能的可用性取決於卡巴斯基安全管理中心雲端主控台模式以及您目前的產品授權。建議您使用*安裝所需更新並修復弱點*工作而不是*修復弱點*工作。*安裝所需更新並修復弱點*工作可讓您根據定義的規則自動安裝多個更新並修復多個弱點。

軟體更新安裝工作具有一些限制。這些限制取決於您對卡巴斯基安全管理中心雲端主控台使用的產品授權以及卡巴斯基安全管理中心雲端主控台運作的模式。

在受管理裝置上更新協力廠商應用程式或修復協力廠商應用程式中的弱點時，可能需要使用者互動。例如，若協力廠商應用程式目前開啟，可能會提示使用者關閉協力廠商應用程式。

建立修復弱點工作：

1. 在主功能表中，轉至 **資產（裝置）→工作**。

2. 點擊**新增**。

   新工作精靈啟動。使用**下一步**按鈕進行精靈。

3. 對於卡巴斯基安全管理中心雲端主控台應用程式，請選取**修復弱點**工作類型。

4. 指定您正建立的工作的名稱。

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

5. 選取要分配工作的裝置。

6. 點擊**新增**按鈕。

   更新清單隨即開啟。

7. 選取您要修復的弱點，之後點擊**確定**。

8. 指定作業系統重新啟動設定：

   - **不重新啟動裝置**

     用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

   - **重新啟動裝置**

     如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

   - **提示使用者操作**

     用戶端裝置螢幕上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。該選項適用於使用者必須可以選取最方便的時間進行重新啟動的工作站。

     預設情況下已選定此選項。

   - **重複提示間隔（分鐘）**

     如果啟用該選項，應用程式以指定頻率提示使用者重新啟動作業系統。

     預設情況下已啟用該選項。預設間隔是 5 分鐘。可用值介於 1 和 1440 分鐘之間。

     如果停用該選項，提示僅顯示一次。

   - **在該時間後重新啟動（分鐘）**

     提示使用者之後，應用程式在指定時間間隔後強制作業系統重新啟動。

     預設情況下已啟用該選項。預設延時是 30 分鐘。可用值介於 1 和 1440 分鐘之間。

   - **強制關閉被封鎖工作階段中的應用程式**

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

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

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

預設情況下已停用該選項。

9. 指定帳戶設定：

- **預設帳戶**

  在與執行該工作的應用程式相同的帳戶下執行該工作。

  預設情況下已選定此選項。

- **指定帳戶**

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

- **帳戶**

  執行該工作的帳戶。

- **密碼**

  工作執行時使用的帳戶的密碼。

10. 若在**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。

11. 點擊**完成**按鈕。

    工作被建立並顯示在工作清單。

12. 按一下建立的工作的名稱以開啟工作內容視窗。

13. 在工作內容視窗中，依需求指定一般工作設定。

14. 點擊**儲存**按鈕。

工作被建立和配置。

建立安裝必要更新並修復弱點工作

*安裝所需更新並修復弱點*工作的可用性取決於卡巴斯基安全管理中心雲端主控台模式以及您目前的產品授權。

*安裝所需更新並修復弱點*工作會用來更新與修復協力廠商軟體中的弱點，包含安裝在受管理裝置上的 Microsoft 軟體。此工作可讓您根據特定規則安裝多項更新並修復多個弱點。

若要使用*安裝所需更新並修復弱點*工作安裝更新或修復弱點，您可進行以下一項操作：

- 執行更新安裝精靈或弱點修復精靈。
- 建立*安裝所需更新並修復弱點*工作。
- 對現有*安裝所需更新並修復弱點*工作新增安裝更新規則。

軟體更新安裝工作具有一些限制。這些限制取決於您對卡巴斯基安全管理中心雲端主控台使用的產品授權以及卡巴斯基安全管理中心雲端主控台運作的模式。

要建立安裝所需更新並修復弱點工作：

1. 在主功能表中，轉至 **資產（裝置）→工作**。
2. 點擊**新增**。
   新工作精靈啟動。遵照精靈的說明。
3. 對於卡巴斯基安全管理中心雲端主控台應用程式，請選取**安裝所需更新並修復弱點**工作類型。
4. 指定您正建立的工作的名稱。工作名稱不能包含多於 100 個字元並且不能包括任何特殊字元 ("*<>?\:|)。
5. 選取要分配工作的裝置。
6. 指定更新安裝的規則，然後指定以下設定：

   - **在裝置重新啟動或關閉時開始安裝**

     如果啟用該選項，更新在裝置被重新啟動或關閉時安裝。否則，更新根據排程安裝。
     如果安裝更新可能影響裝置效能則使用該選項。
     預設情況下已停用該選項。

   - **安裝所需的一般系統元件**

     如果啟用該選項，在安裝更新之前，應用程式自動安裝所需的所有一般系統元件（先決條件）。例如，這些先決條件可以是作業系統更新。
     如果停用該選項，您可能必須手動安裝先決條件。
     預設情況下已停用該選項。

   - **更新過程中允許安裝新的應用程式版本**

如果啟用該**選項**，如果更新導致軟體應用程式新版本的安裝，更新將被允許。

如果停用該選項，軟體不被升級。您可以稍後手動或透過其他工作安裝軟體的新版本。例如，如果公司基礎架構不被新軟體版本支援，或者如果您想要在測試基礎架構中檢查升級，您可能使用該選項。

預設情況下已啟用該選項。

升級應用程式可能導致安裝在用戶端裝置上的獨立應用程式功能異常。

- **下載更新到裝置而不安裝**

如果啟用該選項，應用程式下載更新到裝置但是不自動安裝它們。您可以稍後手動安裝下載的更新。

Microsoft 更新被下載到系統 Windows 儲存。協力廠商應用程式更新（由非 Kaspersky 和 Microsoft 軟體供應商製作的應用程式）會下載到在**下載更新資料夾**欄位指定的資料夾。

如果停用該選項，更新被自動安裝到裝置。

預設情況下已停用該選項。

- **下載更新資料夾**

該資料夾用於下載協力廠商應用程式（由非 Kaspersky 和 Microsoft 軟體供應商製作的應用程式）更新。

- **啟用進階診斷**

如果啟用此功能，即便在卡巴斯基安全管理中心雲端主控台遠端診斷公用程式中對網路代理停用了偵錯，網路代理也會寫入偵錯。偵錯輪流寫入兩個檔案中；兩個檔案的最大大小由**進階診斷檔案的最大大小 (MB)**值決定。當兩個檔案都滿時，網路代理再次開始寫入它們。帶有偵錯的檔案儲存在 %WINDIR%\Temp 資料夾。這些檔案可供在遠端診斷公用程式中存取，您可以在該處下載或刪除這些檔案。

如果停用此功能，則網路代理會根據卡巴斯基安全管理中心雲端主控台遠端診斷公用程式中的設定寫入偵錯。沒有附加偵錯被寫入。

當建立工作時，您不必啟用進階診斷。您可能想要使用該功能，如果，例如，工作在一些裝置上失敗且您想要在另一個工作執行期間獲取額外資訊。

預設情況下已停用該選項。

- **進階診斷檔案的最大大小（MB）**

預設值是 100 MB，可用值介於 1 MB 和 2,048 MB 之間。當您所傳送的進階診斷檔案資訊不足以定位問題時，您可能被 Kaspersky 技術支援專家需求變更預設值。

7. 指定作業系統重新啟動設定：

- **不重新啟動裝置**

用戶端裝置在操作後不被自動重新啟動。要完成操作，您必須重新啟動裝置（例如，手動或透過裝置管理工作）。所需重新啟動的資訊被儲存在工作結果和裝置狀態。該選項適用於在需要持續操作的伺服器和其他裝置上的工作。

- **重新啟動裝置**

如果完成安裝需要重新啟動，用戶端裝置總是被自動重新啟動。該選項適用於允許中斷操作（關機或重新啟動）的裝置上的工作。

- **提示使用者操作**

  用戶端裝置螢幕上將顯示重新啟動提醒，提示使用者手動重新啟動裝置。可以為該選項定義一些進階設定：使用者訊息文字、訊息顯示頻率以及強制重新啟動（不需要使用者確認）的時間間隔。該選項適用於使用者必須可以選取最方便的時間進行重新啟動的工作站。

  預設情況下已選定此選項。

- **重複提示間隔（分鐘）**

  如果啟用該選項，應用程式以指定頻率提示使用者重新啟動作業系統。

  預設情況下已啟用該選項。預設間隔是 5 分鐘。可用值介於 1 和 1440 分鐘之間。

  如果停用該選項，提示僅顯示一次。

- **在該時間後重新啟動（分鐘）**

  提示使用者之後，應用程式在指定時間間隔後強制作業系統重新啟動。

  預設情況下已啟用該選項。預設延時是 30 分鐘。可用值介於 1 和 1440 分鐘之間。

- **強制關閉封鎖工作階段中應用程式前的等待時間（分鐘）**

  使用者裝置鎖定時，程式以強制模式關閉（指定不活動間隔之後自動鎖定，或手動鎖定）。

  如果啟用此選項，一旦輸入區域指定的時間間隔結束，鎖定裝置上的程式以強制模式關閉。

  如果停用此選項，鎖定裝置上的程式將不會關閉。

  預設情況下已停用該選項。

8. 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。

9. 點擊**完成**按鈕。

   工作被建立並顯示在工作清單。

10. 按一下建立的工作的名稱以開啟工作內容視窗。

11. 在工作內容視窗中，依需求指定一般工作設定。

12. 點擊**儲存**按鈕。

    工作被建立和配置。

若工作結果包含 0x80240033「Windows 更新代理錯誤 80240033（「無法下載產品授權期限」）」警告，您可以透過 Windows 登錄資料解決此問題。

新增安裝更新的規則

此功能的可用性取決於卡巴斯基安全管理中心雲端主控台模式以及您目前的產品授權。

使用*安裝所需更新並修復弱點*工作安裝軟體更新或修復軟體弱點時，您必須指定安裝更新的規則。這些規則決定要安裝的更新和要修復的弱點。

精確設定會視您是否建立 Microsoft 應用程式、協力廠商應用程式（由非 Kaspersky 和 Microsoft 軟體供應商製作的應用程式）、或所有應用程式更新的規則而定。當新增 Windows Update 更新或協力廠商應用程式的更新規則時，您可以選取特定的應用程式和您要安裝更新的應用程式版本。當新增所有更新的規則時，您可以選取要安裝的特定更新，以及要透過安裝更新而修復的弱點。

您可以透過以下方式建立更新的安裝規則：

- 透過在建立新的安裝所需更新並修復弱點工作時新增規則。
- 透過在現有*安裝所需更新並修復弱點*工作屬性視窗的**應用程式設定**索引標籤上新增規則。
- 透過更新安裝精靈或弱點修復精靈。

若要為所有更新建立新規則：

1. 點擊**新增**按鈕。
   規則建立精靈開始。使用**下一步**按鈕進行精靈。
2. 在**規則類型**頁面上，選擇**所有更新的規則**。
3. 在**一般標準**頁面，使用下拉清單指定以下設定：
   - **要安裝的更新集**

     選取必須在用戶端裝置上安裝的更新：
     - **僅安裝批准的更新**。這僅安裝批准的更新。
     - **安裝所有更新（除了拒絕的）**。這安裝帶有*已批准*或*未定義*批准狀態的更新。
     - **安裝所有更新（包含拒絕的）**。這安裝所有更新，無論什麼批准狀態。警惕選取該選項。例如，如果您想要在測試基礎架構中檢查一些被拒絕的更新的安裝，使用該選項。
   - **修復弱點的時機為嚴重等級大於或等於**

     有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

     如果啟用該選項，更新僅修復 Kaspersky 設定的安全等級等於或高於清單中選定的值（**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

     如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

     預設情況下已停用該選項。
4. 在**更新**頁面，選取要安裝的更新：

- **安裝所有合適的更新**

  安裝滿足在精靈中**一般標準**頁面指定標準的所有軟體更新。預設選取。

- **僅安裝清單中的更新**

  僅安裝您從清單中手動選取的軟體更新。該清單包含所有可用軟體更新。

  例如，您可能想要在以下情況下選取特定更新：要在測試環境中檢查它們的安裝、要僅更新嚴重應用程式、或者要僅更新特定應用程式。

- **自動安裝所選更新安裝時需要的所有先前應用程式更新**

  如果在安裝所選更新需要時，您同意安裝暫時應用程式版本，保持該選項被啟用。

  如果停用該選項，僅選定的應用程式版本被安裝。如果您想直截了當地更新應用程式，而不嘗試安裝增量版本，請停用該選項。如果安裝所選更新不能不安裝先前版本的應用程式，應用程式更新失敗。

  例如，您在裝置上安裝了應用程式的版本 3，您想更新它到版本 5，但是該應用程式的版本 5 僅可以在版本 4 之上安裝。如果啟用該選項，軟體先安裝版本 4，然後安裝版本 5。如果停用該選項，軟體更新應用程式失敗。

  預設情況下已啟用該選項。

5. 在**弱點**頁面，選取將由安裝所選更新修復的弱點。

- **修復所有符合其他標準的弱點**

  修復滿足在精靈中**一般標準**頁面指定標準的所有弱點。預設選取。

- **僅修復清單中的弱點**

  僅修復您手動從清單中選取的弱點。清單包含所有偵測到的弱點。

  例如，您可能想要在以下情況下選取特定弱點：要在測試環境中檢查它們的修復、要僅修復嚴重應用程式中的弱點、或者要僅修復特定應用程式中的弱點。

6. 在**名稱**頁面，指定您正在建立的規則名稱。您可以稍後在所建立工作的內容視窗的**設定**區域變更該名稱。

「規則建立精靈」完成操作後，系統會建立新規則並顯示在「新工作精靈」或工作屬性的欄位中。

若要為 Windows Update 更新建立新規則：

1. 點擊**新增**按鈕。

   規則建立精靈開始。使用**下一步**按鈕進行精靈。

2. 在**規則類型**頁面上，選擇 **Windows Update 的規則**。

3. 在**一般標準**頁面中，指定以下設定：

- **要安裝的更新集**

選取必須在用戶端裝置上安裝的更新：

- **僅安裝批准的更新**。這僅安裝批准的更新。
- **安裝所有更新（除了拒絕的）**。這安裝帶有*已批准*或*未定義*批准狀態的更新。
- **安裝所有更新（包含拒絕的）**。這安裝所有更新，無論什麼批准狀態。警惕選取該選項。例如，如果您想要在測試基礎架構中檢查一些被拒絕的更新的安裝，使用該選項。

- **修復弱點的時機為嚴重等級大於或等於**

  有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

  如果啟用該選項，更新僅修復 Kaspersky 設定的安全等級等於或高於清單中選定的值（**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

  如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

  預設情況下已停用該選項。

- **修復弱點的時機為 MSRC 嚴重等級大於**

  有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

  如果啟用該選項，更新僅修復 Microsoft Security Response Center (MSRC) 設定的安全等級等於或高於清單中選定的值（**低**、**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

  如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

  預設情況下已停用該選項。

4. 在**應用程式**頁面，選取您要安裝更新的應用程式和應用程式版本。預設情況下選定所有應用程式。
5. 在**更新類別**頁面，選取要安裝的更新類別。這些類別與 Microsoft Update Catalog 中的類別相同。預設情況下選定所有類別。
6. 在**名稱**頁面，指定您正在建立的規則名稱。您可以稍後在所建立工作的內容視窗的**設定**區域變更該名稱。

「規則建立精靈」完成操作後，系統會建立新規則並顯示在「新工作精靈」或工作屬性的欄位中。

若要為協力廠商應用程式更新建立規則：

1. 點擊**新增**按鈕。

   規則建立精靈開始。使用**下一步**按鈕進行精靈。
2. 在**規則類型**頁面上，選擇**協力廠商更新的規則**。
3. 在**一般標準**頁面中，指定以下設定：

- **要安裝的更新集**

選取必須在用戶端裝置上安裝的更新：

- **僅安裝批准的更新**。這僅安裝批准的更新。
- **安裝所有更新（除了拒絕的）**。這安裝帶有*已批准*或*未定義*批准狀態的更新。
- **安裝所有更新（包含拒絕的）**。這安裝所有更新，無論什麼批准狀態。警惕選取該選項。例如，如果您想要在測試基礎架構中檢查一些被拒絕的更新的安裝，使用該選項。

- **修復弱點的時機為嚴重等級大於或等於**

有時候，軟體更新可能損害使用者的軟體體驗。此種情況下，您可能決定僅安裝軟體操作的關鍵更新並略過其他更新。

如果啟用該選項，更新僅修復 Kaspersky 設定的安全等級等於或高於清單中選定的值（**中度**、**高危**或**嚴重**）的弱點。安全等級低於選定值的弱點不被修復。

如果停用該選項，更新修復所有弱點，無論它們的安全等級是什麼。

預設情況下已停用該選項。

4. 在**應用程式**頁面，選取您要安裝更新的應用程式和應用程式版本。預設情況下選定所有應用程式。
5. 在**名稱**頁面，指定您正在建立的規則名稱。您可以稍後在所建立工作的內容視窗的設定區域變更該名稱。

「規則建立精靈」完成操作後，系統會建立新規則並顯示在「新工作精靈」或工作屬性的欄位中。

檢視在所有受管理裝置上偵測到的軟體弱點

掃描受管理裝置上軟體的弱點後，您可檢視在所有受管理裝置上軟體弱點的清單。

要檢視在所有受管理裝置上偵測的軟體弱點清單，

在主功能表中，轉至 **操作 → 修補程式管理 → 軟體弱點**。

此頁會顯示在用戶端裝置中偵測到的軟體弱點清單。

您也可產生並檢視弱點報告。

您可指定檢視軟體弱點清單的篩選器。點擊軟體弱點清單右上角的**篩選器**圖示（ ）來管理篩選條件。您也可從軟體弱點清單上方的**預設篩選器** 下拉清單選取其中一個預設篩選條件。

您可從清單取得關於任何弱點的詳細資訊。

若要取得軟體弱點資訊：

在軟體弱點清單中，按一下有弱點名稱的連結。

軟體弱點內容視窗隨即開啟。

檢視在受管理裝置上偵測到的軟體弱點的資訊

您可檢視在所選且執行 Windows 的受管理裝置上偵測到的軟體弱點資訊。

若要檢視在選取的受管理裝置偵測的軟體弱點：

1. 在主功能表中，轉至 **資產（裝置）→ 受管理裝置**。
   受管理裝置清單隨即顯示。
2. 在受管理裝置清單中，按一下您要檢視之已偵測軟體弱點的裝置名稱連結。
   所選裝置的屬性視窗隨即顯示。
3. 在所選裝置的內容視窗中，選取**進階**頁籤。
4. 在左窗格中，選取**軟體弱點**區段。
   若要僅檢視可修正的軟體弱點，請選取 **僅顯示可以被修復的弱點** 選項。

在所選受管理裝置上偵測到的軟體弱點清單隨即顯示。

若要檢視所選軟體弱點的內容，

按一下軟體弱點清單中軟體弱點名稱的連結。

所選軟體弱點的內容視窗隨即顯示。

檢視受管理裝置的弱點統計資料

您可檢視受管理裝置上各軟體弱點的統計資料。統計資料會以圖表顯示。圖表會顯示裝置數量搭配以下狀態：

- *已忽略：<裝置數量>*。若您在弱點內容中手動設定選項以忽略弱點，則會配置此狀態。
- *已修復：<裝置數量>*。若修復弱點的工作完成，則會配置此狀態。
- *修復已排程：<裝置數量>*。若您已建立工作修復弱點，但該工作尚未執行，則會配置此狀態。
- *修補程式已套用：<裝置數量>*。若您已手動選取軟體更新來修復弱點，但此更新的軟體尚未修復弱點，則會配置此狀態。
- *需要修復：<裝置數量>*。若僅在受管理裝置部分修復弱點，並且需要在受管理裝置的剩餘部分修部弱點，則會配置此狀態。

若要檢視受管理裝置的弱點統計資料：

1. 在主功能表中，轉至 **操作 → 修補程式管理 → 軟體弱點**。
   此頁會顯示受管理裝置中偵測到的應用程式弱點清單。
2. 選取所需弱點旁邊的核取方塊。

3. 點擊**裝置弱點統計資訊**按鈕。

弱點狀態圖表隨即顯示。按一下狀態會開啟裝置清單，其中會顯示有所選狀態弱點的裝置。

將軟體弱點匯出至檔案中

您可將顯示的弱點清單匯出為 CSV 或 TXT 檔案。您可使用這些檔案，例如將它們傳送至您的資訊安全經理，或儲存起來以供統計使用。

若要匯出所有受管理裝置上偵測到的軟體弱點清單為文字檔案：

1. 在主功能表中，轉至 **操作 → 修補程式管理 → 軟體弱點**。
   此頁會顯示受管理裝置中偵測到的應用程式弱點清單。
2. 點擊**匯出到 TXT**或**匯出到 CSV**按鈕，視您偏好的匯出格式而定。

內含軟體弱點清單的檔案會下載至您目前使用的裝置。

若要匯出所選受管理裝置上偵測到的軟體弱點清單為文字檔案：

1. 開啟所選受管理裝置偵測到的軟體弱點清單。
2. 選取您要匯出的軟體弱點。
   若您要匯出在受管理裝置偵測到的軟體弱點完整清單，請略過此步驟。
   若您要匯出在受管理裝置偵測到的軟體弱點完整清單，僅會匯出顯示在目前頁面的弱點。
3. 點擊**匯出到 TXT**或**匯出到 CSV**按鈕，視您偏好的匯出格式而定。

含檔案所選受管理裝置偵測到的軟體弱點清單的檔案會下載至您目前使用的裝置。

忽略軟體弱點

您可忽略要修復的軟體弱點。忽略軟體弱點的原因可能如下：

- 您認為軟體弱點對您組織不緊急。
- 您瞭解軟體弱點修復會損壞需弱點修復之軟體的相關資料。
- 您確定軟體弱點對您組織網路並不危險，因為您使用其他措施防護您的受管理裝置。

您可在所有受管理裝置或僅在選取的受管理裝置忽略軟體弱點。

若要在所有受管理裝置上忽略軟體弱點：

1. 在主功能表中，轉至 **操作 → 修補程式管理 → 軟體弱點**。
   此頁會顯示在受管理裝置中偵測到的軟體弱點清單。
2. 在軟體弱點清單中，按一下有要忽略的軟體弱點名稱連結。

軟體弱點內容視窗開啟。

3. 在**一般**頁籤，點擊**略過弱點**選項。
4. 點擊**儲存**按鈕。
   軟體弱點內容視窗關閉。

軟體弱點會在所有受管理裝置遭到忽略。

若要在選取的受管理裝置忽略軟體弱點：

1. 在主功能表中，轉至 **資產（裝置）→ 受管理裝置**。
   受管理裝置清單隨即顯示。
2. 在受管理裝置清單中，按一下有您要忽略之軟體弱點的裝置名稱連結。
   弱點內容視窗隨即開啟。
3. 在裝置內容視窗中，選取**進階**頁籤。
4. 在左窗格中，選取**軟體弱點**區段。
   在裝置上偵測到的軟體弱點清單隨即顯示。
5. 在軟體弱點清單中，選取您要在選取裝置上忽略的弱點。
   軟體弱點內容視窗開啟。
6. 在軟體弱點內容視窗中的**一般**頁籤，啟用**略過弱點**選項。
7. 點擊**儲存**按鈕。
   軟體弱點內容視窗關閉。
8. 關閉裝置內容視窗。

軟體弱點會在選取的裝置上遭到忽略。

忽略的軟體弱點在完成*修復弱點*工作或*安裝所需更新並修復弱點*工作將不會修復。您可從弱點清單以篩選方式排除忽略的軟體弱點。

設定修復弱點資訊的最長儲存期間

若要在資料庫中設定已在受管理裝置上修復的弱點的資訊的最長儲存期間：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在開啟的頁面中，前往**事件儲存區**頁籤。
3. 指定所修復弱點的資訊在資料庫中的最大儲存期限。
   在試用模式下，預設儲存期限為 7 天，而在正式模式下，預設儲存期限為 60 天。在試用模式下，最大限制為 14 天，而正式模式下，最大限制為 365 天。

4. 點擊**儲存**。

修復弱點資訊的最長儲存期間為指定天數。

管理用戶端裝置上的應用程式執行

本節說明卡巴斯基安全管理中心雲端主控台中，與管理用戶端裝置上執行的應用程式相關的功能。

情境：應用程式管理

您可以管理用戶端裝置上的應用程式啟動情形。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。您可管理安裝在 Windows 或 Linux 裝置的應用程式。

對於 Linux 作業系統，從 Kaspersky Endpoint Security 11.2 for Linux 開始提供應用程式控制元件。

先決條件

- 您的組織中已部署 Kaspersky Security Center Cloud Console。
- Kaspersky Endpoint Security for Windows 或 Kaspersky Endpoint Security for Linux 的政策已建立並處於使用中狀態。

階段

應用程式控制使用情境是分多個階段進行：

1. **形成和檢視應用戶端裝置上應用程式清單**

   此階段可提供您受管理裝置上安裝哪些應用程式的資訊。您可檢視應用程式清單，並根據組織的安全政策決定要允許和禁止的應用程式。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應用程式，您可略過此階段。

   操作說明：取得並檢視安裝在用戶端裝置的應用程式清單

2. **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。

   操作說明：取得並檢視用戶端裝置上所安裝可執行檔的清單

3. **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應用程式清單與可執行檔。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。若不同的安全群組在其工作中使用不同的應用程式集，則可針對各安全群組建立獨立的應用程式類別。

   根據建立應用程式類別的條件集，您可建立兩種類型的應用程式類別。

   操作說明：建立含有手動新增內容的應用程式類別，建立包含來自選定裝置的可執行檔的應用程式類別

4. **在 Kaspersky Endpoint Security for Windows 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 Windows 政策中配置應用程式控制元件。

   操作說明：在 Kaspersky Endpoint Security for Windows 政策中配置應用程式控制

5. **在測試模式中開啟應用程式控制元件**

   若要確定應用程式控制規則沒有封鎖使用者工作必要的應用程式，建議啟用測試應用程式控制規則，並在建立新規則後分析其運作。測試啟用時，Kaspersky Endpoint Security for Windows 不會封鎖應用程式控制規則封鎖啟動的應用程式，但會改為傳送有關其啟動的資訊至管理伺服器。

   測試應用程式控制規則時，建議執行以下動作：

   - 決定測試期間。測試期間可從數日到兩個月。
   - 檢查因應用程式控制作業產生的測試事件。

   操作說明：在 Kaspersky Endpoint Security for Windows 政策中設定應用程式控制。請依照其中的指示，在設定程序中啟用測試模式。

6. **變更應用程式控制元件的應用程式類別設定**

   如有必要，請變更應用程式控制設定。根據測試結果，您可新增與應用程式控制元件事件相關的可執行檔致函手動新增內容的應用程式類別。

   操作說明：將與事件相關的可執行檔新增到應用程式類別

7. **在操作模式套用應用程式控制規則**

   測試應用程式控制規則且完成應用程式類別組態後，您可在操作模式中套用應用程式控制規則。

   操作說明：在 Kaspersky Endpoint Security for Windows 政策中設定應用程式控制。請依照其中的指示，在設定程序中停用測試模式。

8. **確認應用程式控制組態**

   請確認以下出現跡象：

   - 應用程式類別清單並未空白。請檢視應用程式類別清單，確定其中包含您已設定的類別。
   - 應用程式控制已設定為使用所建立的應用程式類別。請檢視 Kaspersky Endpoint Security for Windows 政策的設定，並確保您已在**應用程式設定** → **安全控制** → **應用程式控制**中設定應用程式控制。
   - 應用程式控制的規則是以操作模式套用。請檢查 Kaspersky Endpoint Security for Windows 政策中的模式，並確保您已在**應用程式設定** → **安全控制** → **應用程式控制**中停用**測試模式**。

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。使用者僅可啟動您的組織中允許的應用程式，而無法啟動您的組織中禁止的應用程式。

如需有關應用程式控制的詳細資訊，請參閱以下說明主題：

- Kaspersky Endpoint Security for Windows 線上說明
- Kaspersky Endpoint Security for Linux 線上說明

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 for Windows 和 Kaspersky Endpoint Security for Linux（版本 11.2 或以上版本）。本節所有指示都在說明 Kaspersky Endpoint Security 的應用程式控制設定。

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。預設會選取*拒絕清單*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雲端主控台中，應用程式類別分兩種類型：

- 含有手動新增內容的類別。您會定義條件，例如檔案中繼資料、檔案雜湊碼、檔案憑證、KL 類別、檔案路徑，以在類別中包含可執行檔。
- 包含來自所選服務的可執行檔的類別。您指定之裝置的可執行檔會自動包含在類別中。

如需有關應用程式控制的詳細資訊，請參閱以下說明主題：

- Kaspersky Endpoint Security for Windows 線上說明
- Kaspersky Endpoint Security for Linux 線上說明

取得並檢視安裝在用戶端裝置的應用程式清單

卡巴斯基安全管理中心雲端主控台會在執行 Linux 和 Windows 的受管理用戶端裝置上清查所有安裝的軟體。

網路代理編輯安裝在裝置上的應用程式清單，並把該清單傳給管理伺服器。網路代理更新應用程式清單大約需要 10-15 分鐘。

對於 Windows 用戶端裝置，網路代理從 Windows 登錄接收有關已安裝應用程式的大部分資訊。對於 Linux 用戶端裝置，套件管理工具會向網路代理提供有關已安裝應用程式的資訊。

若要檢視安裝在受管理裝置上的應用程式清單：

1. 在主功能表中，轉至 **操作 → 協力廠商應用程式 → 應用程式登錄資料**。

   該頁面顯示一個表格，其中包含安裝在受管理裝置上的應用程式。選取應用程式以檢視其內容，例如，供應商名稱、版本號、可執行檔清單、安裝了該應用程式的裝置清單、可用軟體更新清單和偵測到的軟體弱點清單。

2. 您可以按如下方式對包含已安裝應用程式的表格資料進行分組和篩選：

   - 按一下表格右上角的設定圖示（ ）。

在叫用的**欄設定**功能表中，選擇要在表格中顯示的欄。要檢視安裝應用程式的用戶端裝置的作業系統類型，請選擇**作業系統類型**欄。

- 按一下表格右上角的篩選圖示（ ）， 然後在叫用的功能表中指定並套用篩選條件。
  顯示篩選後的已安裝應用程式表格。

若要檢視安裝在特定受管理裝置上的應用程式清單：

在主功能表中，轉至 **裝置 → 受管理裝置 → <裝置名稱> → 進階 → 應用程式登錄資料**。在此功能表中，您可將應用程式清單匯出為 CSV 檔案或 TXT 檔案。

如需有關應用程式控制的詳細資訊，請參閱以下說明主題：

- Kaspersky Endpoint Security for Windows 線上說明
- Kaspersky Endpoint Security for Linux 線上說明

取得並檢視用戶端裝置上所安裝可執行檔的清單

您可以取得受管理裝置上所安裝可執行檔的清單。若要清查可執行檔，您必須建立清查工作。

清查可執行檔的功能可用於以下應用程式：

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux（版本 11.2 和以上版本）

您可以在獲取已安裝應用程式的資訊時降低資料庫的負載。為此，我們建議您在安裝了標準軟體集合的參考裝置上執行清查工作。

要在用戶端裝置上為可執行檔建立清查工作：

1. 在主功能表中，轉至**資產（裝置）→ 工作**。
   工作清單隨即顯示。
2. 點擊**新增**按鈕。
   新工作精靈啟動。遵照精靈的說明。
3. 在**新工作**頁面的**應用程式**下拉清單中，根據用戶端裝置的作業系統類型選擇 Kaspersky Endpoint Security for Linux 或 Kaspersky Endpoint Security for Windows。
4. 在**工作類型**下拉式清單中，選取**清單**。
5. 在**完成工作建立**頁面上，點擊**完成**按鈕。

在新工作精靈完成後，**清單**工作即已建立並設定完成。如有需要，您可變更已建立工作的設定。新建立的工作會顯示在工作清單。

關於清查工作的詳細說明，請參考以下說明：

- Kaspersky Endpoint Security for Windows 說明

- Kaspersky Endpoint Security for Linux 說明

在執行**清單**工作後，受管理裝置上安裝的可執行檔即已建立成清單，可供您檢視。

清查期間會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。

若要檢視用戶端裝置上所儲存可執行檔的清單，請

在主功能表中，轉至 **操作 → 協力廠商應用程式 → 可執行檔**。

該頁面會顯示用戶端裝置上所儲存可執行檔的清單。

您也可以將受管理裝置中的可執行檔傳送給 Kaspersky 來檢查是否有潛在威脅。

要將受管理裝置的可執行檔傳送到卡巴斯基：

1. 在主功能表中，轉至 **操作 → 協力廠商應用程式 → 可執行檔**。
2. 按一下要傳送到卡巴斯基的可執行檔的連結。
3. 在開啟的視窗中，轉至**裝置**區域，然後選擇要從其傳送可執行檔的受管理裝置的核取方塊。

   在傳送可執行檔之前，請確保受管理裝置與管理伺服器有直接連線，方法是選擇**不斷開與管理伺服器的連線** 核取方塊。**不斷開與管理伺服器的連線**選項所能選取的最大裝置總數是 300。

4. 點擊**傳送到 Kaspersky**按鈕。

選定的可執行檔被下載以進一步傳送到卡巴斯基。

建立含有手動新增內容的應用程式類別

您可指定一組準則作為可執行檔的範本，這些範本是您希望在組織中允許或封鎖的啟動範本。根據對應該準則的可執行檔，您可建立應用程式類別並在應用程式控制元件組態中加以使用。

要建立含有手動新增內容的應用程式類別：

1. 在主功能表中，轉至 **操作 → 協力廠商應用程式 → 應用程式類別**。
   應用程式類別清單頁面隨即顯示。
2. 點擊**新增**按鈕。
   新類別精靈啟動。遵照精靈的說明。
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 KL 類別**

  如果選中此選項，作為新增應用程式到使用者類別的條件，您可以為應用程式指定 Kaspersky 類別。來自指定 Kaspersky 類別的應用程式將被新增到自訂應用程式類別。

- **從儲存區選取憑證**

  如果選中此選項，則可以指定來自儲存空間的憑證。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，您可以指定包含要新增到使用者應用程式類別的可執行檔的用戶端裝置上的資料夾路徑。

- **卸除式磁碟機**

  如果選中此選項，您可以指定應用程式在其上執行的媒體類型（任意裝置或行動裝置）。在所選驅動類型上執行的應用程式被新增到使用者應用程式類別。

- **雜湊、檔案內容或憑證**：

  - **從可執行檔清單選擇**

    如果選中此選項，可以使用用戶端裝置上的可執行檔清單來選取應用程式並將其新增到類別。

  - **從應用程式登錄資料選擇**

    若已選取此選項，會顯示應用程式登錄資料。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

視您網路裝置中安裝的安全應用程式版本而定，您必須選取卡巴斯基安全管理中心雲端主控台用於為此類別中的檔案計算雜湊值的演算法。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 10 Service Pack 2 for Windows 和更新版本支援 SHA-256 計算。計算 MD5 雜湊被所有 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 的早期版本支援。

請為卡巴斯基安全管理中心雲端主控台用於為該類別中的檔案計算雜湊值的方法，選取以下任一選項：

- 如果您網路上安裝的所有安全應用程式實例都是 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更高版本，請選取**SHA-256**核取方塊。對於 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 早期版本，我們不建議您新增根據可執行檔 SHA-256 雜湊值為標準建立的類別。這將導致安全應用程式操作失敗。此種情況下，您可以為類別中的檔案使用 MD5 加密演算法。
- 如果您的網路上安裝了 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 之前的任何版本，請選取**MD5 雜湊值**。對於 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本，您無法新增基於可執行檔的 MD5 總和檢查碼的條件所建立的類別。此種情況下，您可以為類別中的檔案使用 SHA-256 加密演算法。
- 如果您網路上的不同裝置同時使用早期和更新版本的 Kaspersky Endpoint Security 10，請選中**SHA-256**核取方塊和**MD5 雜湊值**核取方塊。

檔案內容

若已選取此選項，您可指定檔案中繼資料作為檔案名稱、檔案版本、供應商。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。

- **從檔案或從 MSI 套件 / 存檔資料夾**

如果選中此選項，作為新增應用程式到使用者類別的一個條件，您可以指定 MSI 安裝程式的檔。應用程式安裝程式的檔案內容將被傳送到管理伺服器。與指定的 MSI 安裝程式具有相同檔案內容的應用程式被新增到自訂應用程式類別。

選取的準則會新增至條件清單。

您可視需要新增所需數量的應用程式類別。

6. 在精靈的**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。

如需有關應用程式控制的詳細資訊，請參閱以下說明主題：

- Kaspersky Endpoint Security for Windows 線上說明

- Kaspersky Endpoint Security for Linux 線上說明

若要建立應用程式類別以包含來自所選裝置的可執行檔

您可從選取的裝置使用可執行檔作為您希望允許或封鎖的可執行檔範本。根據選取裝置的可執行檔，您可建立應用程式類別並在應用程式控制元件組態中加以使用。

若要建立應用程式類別以包含來自所選裝置的可執行檔：

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

   應用程式類別清單頁面隨即顯示。

2. 點擊**新增**按鈕。

   新類別精靈啟動。使用**下一步**按鈕進行精靈。

3. 在精靈的**選擇類別建立方法**頁面，指定類別名稱並選取**包含所選裝置上可執行檔的類別。這些可執行檔被自動處理，它們的計量被新增到類別中**選項。

4. 點擊**新增**。

5. 在開啟的視窗中，選取一部裝置，或其中的可執行檔將用來建立應用程式類別的裝置。

6. 指定下列設定：

   - **雜湊值計算方法**

     視您網路裝置中安裝的安全應用程式版本而定，您必須選取卡巴斯基安全管理中心雲端主控台用於為此類別中的檔案計算雜湊值的演算法。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 10 Service Pack 2 for Windows 和更新版本支援 SHA-256 計算。計算 MD5 雜湊被所有 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 的早期版本支援。

     請為卡巴斯基安全管理中心雲端主控台用於為該類別中的檔案計算雜湊值的方法，選取以下任一選項：

     - 如果您網路上安裝的所有安全應用程式實例都是 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更高版本，請選取**SHA-256**核取方塊。對於 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 早期版本，我們不建議您新增根據可執行檔 SHA-256 雜湊值為標準建立的類別。這將導致安全應用程式操作失敗。此種情況下，您可以為類別中的檔案使用 MD5 加密演算法。

     - 如果您的網路上安裝了 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 之前的任何版本，請選取**MD5 雜湊值**。對於 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本，您無法新增基於可執行檔的 MD5 總和檢查碼的條件所建立的類別。此種情況下，您可以為類別中的檔案使用 SHA-256 加密演算法。

     如果您網路上的不同裝置同時使用早期和更新版本的 Kaspersky Endpoint Security 10，請選中**SHA-256**核取方塊和**MD5 雜湊值**核取方塊。

     為該類別中的檔案計算 SHA-256（在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本中支援）核取方塊被預設選中。

     為該類別中的檔案計算 MD5（在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 更早版本中支援）核取方塊被預設清空。

- **與管理伺服器儲存區同步資料**

  選取此選項，若您希望管理伺服器定期在指定資料夾（或資料夾）檢查變更。

  預設情況下已停用該選項。

  若您啟用此選項，請指定時段（小時）以檢查指定資料夾（或資料夾）中的變更。依預設，掃描間隔為 24 小時。

- **檔案類型**

  在此區段內，您可指定用來建立應用程式類別的檔案類型。

  所有檔案。所有檔案都會在建立類別時納入考量。預設情況下已選定此選項。

  僅應用程式類別之外的檔案。僅應用程式類別外的檔案會在建立類別時納入考量。

- **資料夾**

  在此區段中，您可要指定已選取裝置中要用來建立應用程式類別的資料夾。

  所有資料夾。所有資料夾都會納入建立類別的考量。預設情況下已選定此選項。

  指定資料夾。僅指定的資料夾會納入建立類別的考量。若您選取此選項，您必須指定連至資料夾的路徑。

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。

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，

在主功能表中，轉至 **操作 → 協力廠商應用程式 → 應用程式類別**。

應用程式類別清單頁面隨即顯示。

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。

在 Kaspersky Endpoint Security for Windows 政策配置應用程式控制

建立應用程式控制類別後，您可將其用來在 Kaspersky Endpoint Security for Windows 政策配置應用程式控制。

若要在 Kaspersky Endpoint Security for Windows 政策設定應用程式控制：

1. 在主功能表中，轉至 **資產（裝置）→ 政策和設定檔**。

   政策清單頁面隨即顯示。

2. 點擊 **Kaspersky Endpoint Security for Windows** 政策。

   政策設定視窗隨即開啟。

3. 轉到**應用程式設定→安全控制→應用程式控制**。

   含應用程式控制設定的**應用程式控制**視窗隨即顯示。

4. **應用程式控制**選項預設為啟用。切換切換按鈕**應用程式控制已停用**來停用該選項。

5. 在**應用程式控制設定**封鎖設定中，啟用操作模式以套用應用程式控制規則，並允許 Kaspersky Endpoint Security for Windows 封鎖應用程式啟動。

   如果要測試應用程式控制規則，請在**應用程式控制設定**區域啟用測試模式。在測試模式下，Kaspersky Endpoint Security for Windows 不會封鎖應用程式啟動，但會在報告中記錄有關觸發規則的資訊。點擊**檢視報告**連接可檢視此資訊。

6. 若您希望在使用者啟動應用程式時，要 Kaspersky Endpoint Security for Windows 監控 DLL 模組載入情況，請啟用**控制 DLL 模組載入**選項。

   模組與載入模組之應用程式的相關資訊將儲存至報告中。

   選取**控制 DLL 模組載入**選項後，Kaspersky Endpoint Security for Windows 僅會監控 DLL 模組和載入的驅動程式。選取**控制 DLL 模組載入**選項後，若您要 Kaspersky Endpoint Security for Windows 監控所有 DLL 模組合驅動程式，包含那些在 Kaspersky Endpoint Security for Windows 啟動前就已載入的項目，請重新啟動電腦。

7. （選用）在**訊息範本**區塊中，變更應用程式被封鎖啟動時顯示的訊息範本，以及會傳送給您的電子郵件訊息範本。

8. 在**應用程式控制模式**封鎖設定中，選取**拒絕清單**或**允許清單**模式。

   依預設會選取**拒絕清單**模式。

9. 按一下**規則清單設定**連結。

   拒絕清單與允許清單視窗隨即開啟以供您新增應用程式類別。選取**拒絕清單**模式時，依預設會選取**拒絕清單**頁籤，選取**允許清單**模式時會選取**允許清單**頁籤。

10. 在**拒絕清單與允許清單**視窗中，點擊**新增**按鈕。

    應用程式控制規則視窗將啟動。

11. 按一下**請選擇一個類別**連結。

    應用程式類別視窗隨即開啟。

12. 新增您先前建立的應用程式類別。

    您可按一下**編輯**按鈕來編輯已建立類別的設定。

    您可按一下**新增**按鈕建立新類別。

    您可按一下**刪除**按鈕從清單中刪除類別。

13. 完成應用程式類別清單後，請點擊**確定**按鈕。

    應用程式類別視窗隨即關閉。

14. 在**應用程式控制規則**視窗的**物件與其權限**區段中，建立要套用應用程式控制規則的使用者與使用者群組清單。

15. 點擊**確定**按鈕以儲存設定並關閉**應用程式控制規則**視窗。

16. 點擊 **確定** 按鈕以儲存設定並關閉**拒絕清單與允許清單**視窗。

17. 點擊**確定**按鈕以儲存設定並關閉**應用程式控制**視窗。

18. 關閉包含 Kaspersky Endpoint Security for Windows 政策設定的視窗。

    應用程式控制已設定。政策填入用戶端裝置後，可執行檔啟動就會受管理。

如需有關應用程式控制的詳細資訊，請參閱以下說明主題：

- Kaspersky Endpoint Security for Windows 線上說明
- Kaspersky Endpoint Security for Linux 線上說明

新增事件相關的可執行檔到應用程式類別

當您在 Kaspersky Endpoint Security for Windows 政策中配置應用程式控制，以下事件會顯示在事件清單中：

- **應用程式遭禁止啟動**（*緊急*事件）。若您已設定應用程式控制來套用規則，則會顯示此事件。
- **應用程式在測試模式中遭禁止啟動**（*資訊*事件）。若您已設定用程式控制來測試規則，則會顯示此事件。
- **向管理員傳送的有關應用程式啟動禁止的訊息**（*警告*事件）。若您已設定應用程式控制來套用規則，則會顯示此事件，並且使用者已要求存取在啟動時遭封鎖的應用程式。

建議您建立事件分類來檢視與應用程式控制操作相關的事件。

您可新增與應用程式控制事件相關的可執行檔至現有應用程式類別或新的應用程式類別。您僅可將可執行檔，新增至透過手動新增內容的應用程式類別。

若要新增與應用程式控制事件相關的可執行檔到應用程式類別：

1. 在主功能表中，轉至 **監控和報告 → 事件分類**。

   事件分類清單已顯示。

2. 選取事件分類來檢視與應用程式控制相關的事件並啟動此事件分類。

   若您尚未建立與應用程式控制相關的事件分類，您可選取並啟動預先定義的分類，例如**最近的事件**。

   事件清單隨即顯示。

3. 選取其中有您要新增至應用程式類別之可執行檔的事件，接著點擊**分配到類別**按鈕。

   新類別精靈啟動。使用**下一步**按鈕進行精靈。

4. 在精靈頁面上，指定相關設定：

   - 在**對事件相關可執行檔所採取的操作**區段，選取以下其中一個選項：

     - **新增到新的應用程式類別**

如果您需要根據事件相關的可執行檔建立新的應用程式類別，請選取此選項。

預設情況下已選定此選項。

若您已選取此選項，請指定新類別名稱。

- **新增到現有應用程式類別**

  如果您需要新增事件相關可執行檔至現有應用程式類別，請選取此選項。

  預設情況下未選定此選項。

  若您已選取此選項，請選取您要新增可執行檔且有手動新增內容的應用程式類別。

- 在**規則類型**區域，選取以下選項之一：
  - **新增到包含的規則**
  - **新增到排除的規則**
- 在**用作條件的參數**區段中，選擇以下選項之一：
  - **憑證詳情（或沒有憑證的檔案的 SHA-256 雜湊）**

    檔案可能使用憑證簽署。多個檔案可能使用相同的憑證簽署。例如，相同應用程式的不同版本可能使用相同的憑證簽署，或者相同供應商的多個不同應用程式可能使用相同憑證簽署。當您選取憑證時，應用程式的多個版本或相同供應商的多個應用程式可能組成一個類別。

    每個檔案都有單獨的 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，僅適用 Kaspersky Endpoint Security 10 Service Pack 1 版本）**

每個檔案都有單獨的 MD5 雜湊。當您選取 MD5 雜湊時，僅一個對應的檔案，例如，定義的應用程式版本，組成類別。

如果您要僅新增可執行檔的 MD5 雜湊詳情，請選取此選項。MD5 雜湊碼計算功能被 Kaspersky Endpoint Security 10 Service Pack 1 for Windows 和所有早期版本支援。

5. 點擊**確定**。

當精靈完成時，系統會新增與應用程式控制事件相關的可執行檔至現有應用程式類別或新的應用程式類別。您可檢視已修改或建立的應用程式類別的設定。

如需有關應用程式控制的詳細資訊，請參閱以下說明主題：

- Kaspersky Endpoint Security for Windows 線上說明
- Kaspersky Endpoint Security for Linux 線上說明

從卡巴斯基資料庫建立協力廠商應用程式的安裝套件

卡巴斯基安全管理中心網頁主控台可讓您使用安裝套件來遠端安裝協力廠商應用程式。此類協力廠商應用程式會隨附於專用的 Kaspersky 資料庫中。

若要根據 Kaspersky 資料庫建立協力廠商應用程式安裝套件，必須具有「弱點和修補程式管理」產品授權。

若要從 Kaspersky 資料庫建立協力廠商應用程式的安裝套件，請執行以下操作：

1. 在主功能表中，轉至 **發現和佈署 → 佈署和分配 → 安裝套件**。
2. 點擊**新增**按鈕。
3. 在開啟的「新安裝套件精靈」頁面上，選取**從 Kaspersky 資料庫中選取一個應用程式來建立安裝套件**選項並點擊**下一步**。
4. 在開啟的應用程式清單中，選取相關應用程式，然後點擊**下一步**。
5. 在下拉清單中選擇相關的本地化語言，然後點擊**下一步**。

僅當應用程式提供多種語言選項的選擇時，才顯示此步驟。

6. 如果系統提示您接受產品授權協議，請在**最終使用者產品授權協議**開啟頁面，點擊連結以讀取供應商網站上的產品授權協議，然後選取**本人确认已完全阅读、理解并接受本《最终用户授权许可协议》的条款和条件**核取方塊。
7. 在開啟的**新安裝套件的名稱**頁面中的**檔案名稱**欄位，輸入安裝套件的名稱，然後點擊**下一步**。

等待直到新建立的安裝套件上傳到管理伺服器。當「新套件精靈」顯示訊息通知您套件建立過程成功時，請點擊**完成**。

新建立的安裝套件會出現在安裝套件清單。您可以在建立或重新配置*遠端安裝應用程式*工作時選取此套件。

從卡巴斯基資料庫檢視和修改協力廠商應用程式的安裝套件設定

如果您先前已經建立 Kaspersky 資料庫中列出之協力廠商應用程式的任何安裝套件，則可以隨後檢視和修改這些軟體套件的設定。

從 Kaspersky 資料庫修改協力廠商應用程式安裝套件的設定僅在「弱點和修補程式管理」產品授權下可用。

要從 Kaspersky 資料庫檢視和修改協力廠商應用程式的安裝套件的設定，請執行以下操作：

1. 在主功能表中，轉至 **發現和佈署 → 佈署和分配 → 安裝套件**。
2. 在開啟的安裝套件清單中，點擊相關套件的名稱。
3. 如有必要，在開啟的屬性頁面上修改設定。
4. 點擊**儲存**按鈕。

您修改的設定隨即保存。

Kaspersky 資料庫協力廠商應用程式的安裝套件設定

協力廠商應用程式的安裝套件設定會用以下頁籤分組：

預設情況下，僅顯示下面列出的一部分設定，因此您可以透過點擊**篩選器**按鈕，然後從清單中選取相關的欄名稱。

- **一般**頁籤：
  - 包含可以手動編輯的安裝套件名稱的輸入欄位
  - **應用程式**

    為其建立安裝套件的協力廠商應用程式名稱。
  - **版本**

    為其建立安裝套件的協力廠商應用程式的版本編號。
  - **大小**

    協力廠商安裝套件的大小（以 KB 為單位）。
  - **已建立**

    協力廠商安裝套件的建立日期和時間。

- **路徑**

  儲存獨立安裝套件網路資料夾的路徑。

- **安裝處理程序**頁籤：

  - **安裝所需的一般系統元件**

    如果啟用該選項，在安裝更新之前，應用程式自動安裝所需的所有一般系統元件（先決條件）。例如，這些先決條件可以是作業系統更新。

    如果停用該選項，您可能必須手動安裝先決條件。

    預設情況下已停用該選項。

  - 顯示更新屬性並包含以下各列的表格：

    - **名稱**

      更新的名稱。

    - **敘述**

      更新的說明。

    - **來源**

      更新的來源，由 Microsoft 或其他第三方開發人員發布。

    - **類型**

      更新的類型，適用於驅動程式還是應用程式。

    - **類別**

      顯示 Microsoft 更新（關鍵更新、定義更新、驅動程式、功能套件、安全更新、Service Pack、工具、更新匯總、更新或升級）的 Windows Server Update Services (WSUS) 類別。

    - **根據 MSRC 的嚴重等級**

      Microsoft 安全回應中心 (MSRC) 定義的更新嚴重等級。

    - **嚴重等級**

      Kaspersky 定義的更新嚴重等級。

    - **修補程式重要性等級**

      修補程式的嚴重等級（如果適用於 Kaspersky應用程式）。

    - **文章**

知識庫中描述更新的文章識別碼 (ID)。

- **公告**

  說明更新的安全公告 ID。

- **未指定安裝（新版本）**

  顯示更新是否具有未指派安裝狀態。

- **即將安裝**

  顯示更新是否具有「待安裝」狀態。

- **正在安裝**

  顯示更新是否具有「安裝中」狀態。

- **已安裝**

  顯示更新是否具有「已安裝」狀態。

- **失敗**

  顯示更新是否具有「已失敗」狀態。

- **需要重新啟動**

  顯示更新是否具有「需要重新啟動」狀態。

- **已註冊**

  顯示註冊更新的日期和時間。

- **以互動模式安裝**

  顯示更新是否需要在安裝期間與使用者進行互動。

- **已撤銷**

  顯示撤銷更新的日期和時間。

- **更新批准狀態**

  顯示更新是否獲准安裝。

- **修訂**

顯示更新的當前修訂版號。

- **更新 ID**

  顯示更新的 ID。

- **應用程式版本**

  顯示應用程式要更新的版號。

- **被替代的**

  顯示可以取代更新的其他更新。

- **替代**

  顯示可以由更新取代的其他更新。

- **您必須接受產品授權協議的條款**

  顯示更新是否需要接受最終使用者產品授權協議 (EULA) 的條款。

- **URL 敘述**

  顯示更新供應商的名稱。

- **應用程式系列**

  顯示更新所屬的應用程式系列名稱。

- **應用程式**

  顯示更新所屬的應用程式名稱。

- **中文化語言**

  顯示更新本地化的語言。

- **未指定安裝（新版本）**

  顯示更新是否具有「未指派安裝（新版本）」的狀態。

- **需要安裝的先決條件**

  顯示更新是否具有「需要先決條件」的安裝狀態。

- **下載模式**

顯示更新下載的模式。

- **是一個修補程式**

  顯示更新是否為修補程式。

- **未安裝**

  顯示更新是否具有「未安裝」狀態。

- 顯示安裝套件設定（包含名稱、描述和值）的**設定**頁簽，在安裝過程中用來作為命令行參數。如果套件未提供此類設定，則會顯示相應的訊息。您可以修改這些設定的值。
- **變更歷程**頁籤，顯示安裝套件修訂版號並包含以下各欄：
  - **修訂**

    顯示安裝套件修訂版號。

  - **時間**

    顯示建立修訂版號的時間。

  - **使用者**

    顯示用於建立修訂版號的使用者帳戶名稱。

  - **操作**

    列出對修訂版號中的安裝套件執行的操作。

  - **敘述**

    顯示為修訂版本新增的文字描述。

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雲端主控台可讓您對協力廠商應用程式（由 Kaspersky 以外的其他軟體供應商製作的應用程式）加上標記。標籤是應用程式標誌，可以用於分組或尋找應用程式。分配給應用程式的標籤可以作為裝置分類中的條件。

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

建立應用程式標籤

要建立應用程式標籤：

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

新標籤出現在應用程式標籤清單。

重命名應用程式標籤

要重命名應用程式標籤：

1. 在主功能表中，轉至 **操作 → 協力廠商應用程式 → 應用程式標籤**。
2. 選取您要重新命名之標籤旁的核取方塊，接著點擊**編輯**。
   標籤內容視窗開啟。
3. 變更標籤名稱。
4. 點擊**確定**儲存變更。

更新的標籤出現在應用程式標籤清單。

分配標籤到應用程式

要分配一個或多個標籤到一個應用程式：

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

5. 點擊**儲存**以儲存變更。

標籤被分配到應用程式。

從應用程式上刪除分配的標籤

要從應用程式刪除一個或多個標籤：

1. 在主功能表中，轉至 **操作 → 協力廠商應用程式 → 應用程式登錄資料**。
2. 點擊您要刪除標籤的應用程式名稱。
3. 選取**標籤**頁簽。

   標籤顯示所有存在於管理伺服器的應用程式標籤。對於指派給選取的應用程式的標記，系統會選取**分配的標籤**欄中的核取方塊。
4. 對於您要移除的標記，請不要選取**分配的標籤**欄中的核取方塊。
5. 點擊**儲存**以儲存變更。

標籤被從應用程式刪除。

已移除應用程式的標籤不被刪除。如果您想，您可以手動刪除它們。

刪除應用程式標籤

要刪除應用程式標籤：

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

應用程式標籤被刪除。刪除的標籤被從其分配的所有應用程式上自動刪除。

設定管理伺服器

此區段說明設定過程與卡巴斯基安全管理中心管理伺服器的內容。

建立管理伺服器階層：新增次要管理伺服器

您可以讓內部部署運作的管理伺服器以從屬管理伺服器的形式運作，進而在您的網路上建立「主/從屬」階層。對 Kaspersky 基礎架構中的管理伺服器而言，您網路中的主管理伺服器和從屬管理伺服器都是從屬伺服器。您可以新增基於 Windows 的管理伺服器，亦可新增基於 Linux 的管理伺服器。

若要新增可供連線的從屬管理伺服器：

1. 確定未來的從屬管理伺服器安裝了卡巴斯基安全管理中心雲端主控台網頁主控台。
2. 在未來的從屬管理伺服器上，下載並儲存管理伺服器憑證，以供您在新增從屬管理伺服器精靈的其中一個步驟新增到主管理伺服器。
3. 在未來的從屬管理伺服器上透過卡巴斯基安全管理中心雲端主控台網頁主控台執行以下操作（或者，您也可以提示未來的從屬管理伺服器本身的管理員執行這些操作）：
   a. 在主功能表中，在未來的從屬管理伺服器名稱旁邊點擊設定圖示 ()。
   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**核取方塊。
   d. 選擇**雲端主控台**作為主管理伺服器的類型。
      用於在從屬管理伺服器與主管理伺服器之間建立連線的設定欄位即會變得可用。
   e. 在 **HDS 伺服器位址（從 Cloud Console 上的主管理伺服器）**和 **HDS 伺服器連接埠**欄位，輸入卡巴斯基安全管理中心雲端主控台主管理伺服器的位址與連接埠。
      您可以在卡巴斯基安全管理中心雲端主控台管理伺服器內容視窗**一般**頁籤的**管理伺服器階層**區段中，找到 HDS 伺服器位址和 HDS 伺服器連接埠。您可以將這些資料複製並貼到從屬管理伺服器視窗的欄位中。
   f. 點擊**指定主管理伺服器憑證**按鈕，然後選取憑證。
      您可以從卡巴斯基安全管理中心雲端主控台管理伺服器的內容視窗**一般**頁籤中，於**管理伺服器階層**區段點擊**檢視管理伺服器憑證**按鈕來下載該憑證。
   g. 點擊**指定 Hosted Discovery Service 憑證**按鈕，然後選取憑證。
      您可以從卡巴斯基安全管理中心雲端主控台管理伺服器的內容視窗**管理伺服器階層**頁籤，於**一般**區段點擊**HDS 根 CA 憑證**按鈕來下載該憑證。
   h. 如果您會使用代理伺服器連線到卡巴斯基安全管理中心雲端主控台管理伺服器（即您所建立階層中的主伺服器），請加以指明，然後輸入代理伺服器憑證。
   i. 如果從屬管理伺服器是位於非警戒區，請選取**將主管理伺服器連線到 DMZ 中的從屬管理伺服器**選項。
   j. 點擊**儲存**以儲存變更並離開視窗。
4. 在主功能表中，在未來的主管理伺服器名稱旁邊點擊設定圖示 ()。
5. 在開啟的內容頁面中，點擊**管理伺服器**頁籤。

6. 在您要將從屬管理伺服器新增到的管理群組名稱旁邊點擊核取方塊。

7. 在功能表行中，點擊**連線從屬管理伺服器**。

   新增從屬管理伺服器精靈啟動。

8. 在精靈的第一頁，填充以下欄位：

   - **從屬管理伺服器顯示名稱**

     從屬管理伺服器將顯示在層級的名稱。如果需要，您可以輸入 IP 位址作為名稱，也可以使用例如「群組 1 的從屬伺服器」之類的名稱。

   - **從屬管理伺服器位址（可選）**

     指定從屬管理伺服器的 IP 位址或網域名稱。

9. 如果您會使用代理伺服器連線到卡巴斯基安全管理中心雲端主控台管理伺服器（即未來的主伺服器），請加以指明，然後輸入代理伺服器憑證。

10. 依照精靈的進一步指示進行操作。

    精靈結束後，“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。主管理伺服器的工作和政策被接收和套用。從屬管理伺服器顯示在主管理伺服器上，在新增其的管理群組中。

建立管理群組

一開始，管理群組階層僅會包含一個名為**受管理裝置**群組的管理群組。您可以在**受管理裝置**群組中新增裝置和子群組。

要建立管理群組，請執行以下操作：

1. 在主功能表中，轉至 **資產（裝置）→ 群組的階層**。

2. 在階層中，選取要讓新管理群組位於的管理群組。

3. 點擊**新增**按鈕。

4. 在開啟的視窗視窗中，輸入群組的名稱，然後點擊**Add**。

   具有所指定名稱的新管理群組即會顯示在管理群組階層中。

程式允許基於 Active Directory 的架構或域網架構建立管理群組結構。您也可以從文字檔案建立群組架構。

要建立管理群組的架構：

1. 在主功能表中，轉至 **資產（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。

為與已刪除的裝置相關的事件設定儲存期限

在卡巴斯基安全管理中心雲端主控台中，事件是儲存在事件儲存區。您無法設定事件儲存區中可儲存的事件數量。

在管理伺服器內容視窗的**事件儲存區**區段，您可以為與已刪除的裝置相關的事件設定最大儲存期限。最大儲存期限是 1000 天。

若要為與已刪除的裝置相關的事件設定儲存天數：

1. 在主功能表中，點擊卡巴斯基安全管理中心雲端主控台管理伺服器旁邊的設定圖示 ( )。

   管理伺服器內容視窗將開啟。

2. 在**一般**標籤，選取**事件儲存區**區段。

3. 啟用**裝置被刪除後儲存事件**選項。

4. 在**最大儲存期間（天）**編輯方塊中，為與已刪除的裝置相關的事件指定儲存天數。

   與已刪除的裝置相關的事件將會儲存的天數即會以指定的值為限。

此外，您可以更改任何工作的設定，以儲存與工作進度相關的事件，或者只儲存工作執行結果。為此，您將降低資料庫中的事件數量，提高與資料庫中事件表分析相關之情境的執行速度，並降低緊急事件被大數量事件覆寫的風險。

彙整事件相關電子郵件

在運作期間，卡巴斯基安全管理中心雲端主控台和受管理 Kaspersky 應用程式會產生事件。每個事件都會歸為特定類型和嚴重等級（*緊急*、*功能失效*、*警告*或*資訊*）。視發生事件的狀況而定，卡巴斯基安全管理中心雲端主控台可能會對相同類型的事件分配不同的嚴重等級。

卡巴斯基安全管理中心雲端主控台會自動傳送事件的電子郵件通知。卡巴斯基安全管理中心雲端主控台會針對**管理伺服器內容**視窗的**事件配置**頁籤所列的事件，傳送事件通知。共用的通知設定會用於所有類型的事件。

為了限制必須傳送的電子郵件數量，卡巴斯基安全管理中心雲端主控台會將特定期間內所發生相同嚴重等級的事件進行彙整。期間的值是由 Kaspersky 專家管理。因此，收件者會收到沿用以下訊息範本的彙整電子郵件：「已發生 <Number> <Severity_level>（和低層級）活動」。

透過 Kaspersky Security Center Cloud Console 管理內部部署運作的從屬管理伺服器時會有的限制

在您於卡巴斯基安全管理中心雲端主控台使用相關選項來切換到在內部部署運作的從屬管理伺服器之後，應用程式即會對該從屬管理伺服器的管理加上特定限制。以下與卡巴斯基安全管理中心雲端主控台操作相關的設定將不供使用者使用：

- 在網路代理政策和管理伺服器政策的設定中，**事件配置**和**應用程式設定**頁籤會無法使用；無法建立任何新政策。

- 在網路代理工作和管理伺服器工作的設定中，**事件配置**和**應用程式設定**頁籤會無法使用；無法建立任何新工作。
- 無法對網路代理和管理伺服器進行管理，從屬管理伺服器的內容視窗亦變得無法使用。
- 快速啟動精靈會無法使用。
- 無法修改網路代理與管理伺服器事件儲存與通知設定。
- **最新應用程式版本**區段會無法使用。
- **安裝套件**區段會無法使用。

檢視次要管理伺服器清單

要檢視從屬（包括虛擬）管理伺服器清單：

在主功能表中，按一下管理伺服器名稱，其位於設定圖示 () 旁邊。

從屬（包括虛擬）管理伺服器下拉清單被顯示。

您可透過點及其名稱前往這些管理伺服器的任何一個。

刪除管理伺服器階層

如果不再想擁有管理伺服器階層，您可以從該階層將其斷開連線。

要刪除管理伺服器階層：

1. 在主功能表中，按一下主管理伺服器名稱旁邊的設定圖示（  ）。
2. 在開啟的頁面中，前往**管理伺服器**標籤。
3. 在您要刪除次要管理伺服器的管理群組，選取次要管理伺服器。
4. 在功能表中，點擊**刪除**。
5. 在開啟的視窗中，點擊**確定**以確認您要刪除該從屬管理伺服器。

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。

設定介面

您可以根據您會使用的功能，設定卡巴斯基安全管理中心雲端主控台介面來顯示和隱藏區段與介面元素。

若要根據目前使用的一組功能來設定卡巴斯基安全管理中心雲端主控台介面：

1. 在主功能表中，轉到您的帳戶設定，然後選擇**介面選項**。
2. 在開啟的**介面選項**視窗中，啟用或停用以下選項：
   - **顯示資料加密與防護**

     您可以使用此選項，隱藏或顯示介面中的**操作 → 資料加密與防護**區段。卡巴斯基安全管理中心雲端主控台僅會為您自己的使用者帳戶儲存此選項的值，其他使用者可以設定不同的值。

   - **顯示 MDR 功能**

     您可以使用此選項，隱藏或顯示介面中的**監控和報告 → Incidents** 區段。卡巴斯基安全管理中心雲端主控台僅會為您自己的使用者帳戶儲存此選項的值，其他使用者可以設定不同的值。
3. 設定卡巴斯基安全管理中心雲端主控台在政策分發結果中顯示的裝置數量。
4. 點擊**儲存**。

主控台介面設定即會依您的偏好來配置。

管理虛擬管理伺服器

本章節說明用來管理虛擬管理伺服器的以下操作：

- 建立虛擬管理伺服器
- 啓用和停用虛擬管理伺服器
- 為虛擬管理伺服器指派管理員
- 變更用戶端裝置的管理伺服器
- 刪除虛擬管理伺服器

建立虛擬管理伺服器

您可以建立虛擬管理伺服器並新增它們到管理群組。

要建立和新增虛擬管理伺服器：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
2. 在開啟的頁面中，前往**管理伺服器**頁籤。
3. 選取您要新增虛擬管理伺服器到的管理群組。
4. 在功能表行中，點擊**新虛擬管理伺服器**。
5. 在開啟的頁面上，定義**虛擬管理伺服器名稱**。

6. 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。

啓用和停用虛擬管理伺服器

當您建立新的虛擬管理伺服器時，預設情況下會啟用它。您可以隨時停用或再次啟用它。停用或啟用虛擬管理伺服器等同於關閉或開啓實體管理伺服器。

要啓用或停用虛擬管理伺服器：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
2. 在開啟的頁面中，前往**管理伺服器**頁籤。
3. 選擇要啟用或停用的虛擬管理伺服器。
4. 在功能表行上，點擊**啟用 / 停用虛擬管理伺服器**按鈕。

虛擬管理伺服器狀態被變更為啟用或停用，具體取決於其先前的狀態。更新後的狀態顯示在管理伺服器名稱旁邊。

為虛擬管理伺服器指派管理員

當您的組織使用虛擬管理伺服器時，您可能希望為每個虛擬管理伺服器指派一個專用管理員。例如，當您建立虛擬管理伺服器來管理您組織內不同獨立的辦公室或部門時，或者如果您是 MSP 提供商並是透過虛擬管理伺服器管理您的租用戶時，這可能會很有用。

當您建立虛擬管理伺服器時，它會繼承主管理伺服器的使用者清單和所有使用者權限。如果使用者有權存取主伺服器，則該使用者也有權存取虛擬伺服器。建立後，您可以分別設定對伺服器的存取權限。如果您只想為虛擬管理伺服器分配管理員，請在主管理伺服器的內容中確定該管理員未被加到**存取權限**清單。

您可以授予管理員對虛擬管理伺服器的存取權限，來為虛擬管理伺服器指派管理員。您可以透過以下方式之一授予所需的存取權限：

- 手動設定管理員的存取權限
- 為管理員指派一個或多個使用者角色

分配管理員時，請確保您授予的是對單一虛擬管理伺服器的存取權限。對多個虛擬管理伺服器具有存取權限的管理員會無法登入卡巴斯基安全管理中心雲端主控台。

虛擬管理伺服器的管理員登入卡巴斯基安全管理中心雲端主控台的方式與登入主管理伺服器的方式相同。卡巴斯基安全管理中心雲端主控台會對管理員進行身分驗證，然後開啟管理員具有存取權限的虛擬管理伺服器。管理員不能在管理伺服器之間切換。

先決條件

在開始之前，請確保滿足以下條件：

- 已建立虛擬管理伺服器。
- 在主管理伺服器上，您已為虛擬管理伺服器指派的管理員建立一個帳戶。
- 建立的虛擬伺服器管理員帳戶在任何伺服器（無論是主伺服器還是從屬伺服器）的內容中，均未被加到**存取權限**清單中。
- 您在**一般功能**：**使用者權限**功能區域中有**修改物件 ACL** 權限。

手動設定存取權限

為虛擬管理伺服器指派管理員：

1. 在主功能表中，切換到所需的虛擬管理伺服器：
   a. 按一下目前管理伺服器名稱右側的 > 形箭號圖示（ ）。
   b. 選取所需的管理伺服器。
2. 在主功能表中，按一下管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
3. 在**存取權限**頁簽上，點擊**新增**按鈕。
   主管理伺服器和當前虛擬管理伺服器的統一使用者清單開啟。
4. 從使用者清單中，選擇要指派給虛擬管理伺服器的管理員帳戶，然後按一下**確定**按鈕。
   應用程式將選取的使用者新增到**存取權限**頁籤上的使用者清單。
5. 選取新增帳戶旁邊的核取方塊，然後點擊**存取權限**按鈕。
6. 設定管理員對虛擬管理伺服器的權限。
   要成功進行身分驗證，管理員至少必須具有以下權限：
   - **一般功能** → **基本功能**功能區域中的**讀取**權限。
   - **一般功能** → **虛擬管理伺服器**功能區域中的**讀取**權限。

應用程式將修改後的使用者權限儲存到管理員帳戶中。

指派使用者角色來設定存取權限

或者，您可以透過使用者角色，將存取權限授予虛擬管理伺服器管理員。例如，如果您想在同一個虛擬管理伺服器上指派多個管理員，這可能很有用。如果是這種情況，您可以為管理員帳戶指派相同的一個或多個使用者角色，而不是為多個管理員設定相同的使用者權限。

要指派使用者角色來為虛擬管理伺服器指派管理員：

1. 在主管理伺服器上，建立一個新的使用者角色，然後指定管理員必須在虛擬管理伺服器上擁有的所有必需存取權限。您可以建立多個角色，例如，如果您想要單獨存取不同的功能區域。
2. 在主功能表中，切換到所需的虛擬管理伺服器：

a. 按一下目前管理伺服器名稱右側的 > 形箭號圖示（ ）。

b. 選取所需的管理伺服器。

3. 將新角色或多個角色指派給管理員帳戶。

應用程式即會將新角色分配給管理員帳戶。

在物件層級設定存取權限

除了指派功能區域層級的存取權限，您還可以在虛擬管理伺服器上設定對特定物件的存取，例如，特定的管理群組或工作。為此，請切換到虛擬管理伺服器，然後在物件的屬性中設定存取權限。

刪除虛擬管理伺服器

當您刪除虛擬管理伺服器時，在管理伺服器上建立的所有物件（包括政策和工作）也將被刪除。由虛擬管理伺服器管理的管理群組中的受管理裝置將被從管理群組中移除。若要讓裝置回到卡巴斯基安全管理中心雲端主控台的管理之下，請執行網路輪詢，然後將找到的裝置從「未配置的裝置」群組移動到管理群組。

要刪除虛擬管理伺服器：

1. 在主功能表中，按一下管理伺服器名稱旁邊的設定圖示（ ）。

2. 在開啟的頁面中，前往**管理伺服器**頁籤。

3. 選擇要刪除的虛擬管理伺服器。

4. 在功能表行中，點擊 **刪除**按鈕。

虛擬管理伺服器將被刪除。

監控和報告

本節說明卡巴斯基安全管理中心雲端主控台的監控和報告功能。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雲端主控台獲部署之後或運作期間，您可以根據您的需要來設定監控和報告功能。

方案：監控和報告

本節提供了在卡巴斯基安全管理中心雲端主控台中設定監控和報告功能的情境。

先決條件

您在組織網路中部署卡巴斯基安全管理中心雲端主控台後，即可開始加以監控並產生運作報告。

階段

設定在組織網路中進行監控和報告，是分多個階段進行：

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「緊急」或「警告」重要性等級的事件數量。當配置裝置狀態切換時，確保以下：

   - 新設定不與您組織的安全政策資訊衝突。
   - 您可以及時對您組織網路中的重要安全事件做出反應。

2. **配置用戶端裝置上的事件通知**

   操作說明：為用戶端裝置上發生的事件設定電子郵件通知

3. **變更安全網路對病毒爆發事件的回應**

   您可以在管理伺服器內容中變更特定閾值。您也可以建立要啟動的更嚴格政策，或者建立要在事件發生時執行的工作。

4. **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：

   - 產生並檢閱**防護狀態**和**威脅統計資料**類別的報告
   - 啟動並檢閱**緊急**事件分類

7. **檢視產品授權資訊**

   說明：

   - 在儀表板中新增**產品授權金鑰使用**小工具並加以檢閱
   - 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

組織網路中所發生安全事件的資訊是儲存在管理伺服器資料庫。卡巴斯基安全管理中心雲端主控台會根據這些事件，為您的組織網路提供以下類型的監控和報告：

- 儀表板
- 報告
- 事件分類

控製板

儀表板透過對資訊進行圖形顯示來允許您監控您組織網路的安全趨勢。

報告

報告功能允許您獲取您組織網路的詳細安全數字資訊、儲存該資訊到檔案、透過郵件傳送它和列印它。

事件分類

事件選項提供從管理伺服器資料庫中選取的事件的命名集合的螢幕視圖。這些事件集會根據以下類別分組：

- 依嚴重等級—**緊急事件**、**功能失效**、**警告**和**資訊事件**
- 依時間—**最近事件**
- 依類型—**使用者請求**和**稽核事件**

您可以基於卡巴斯基安全管理中心雲端主控台介面中可供配置的設定，建立和檢視使用者定義的事件分類。

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。

在卡巴斯基安全管理中心雲端主控台中存取儀表板的方式，是在**監控和報告**區段點擊**控制板**。

儀表板提供可以自訂的部件。您可以選取大量不同的部件，顯示為圓形圖、表格、圖表和清單。小部件中顯示的資訊會自動更新，更新周期為一到兩分鐘。更新間隔根據不同部件而不同。您可以在任意時刻透過設定功能表在部件上手動重新整理資料。

預設下，部件包含儲存在管理伺服器資料庫中的所有事件的資訊。

卡巴斯基安全管理中心雲端主控台預設會提供一組以下類別的小工具：

- **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。

當配置儀表板時，您可以新增您需要的部件或隱藏您不需要的部件，變更部件的大小或外觀，移動部件以及變更它們的設定。

新增小部件到儀表板

要新增工具到儀表板：

1. 在主功能表中，轉至 **監控和報告 → 控制板**。
2. 點擊**新增或還原 Web 小部件**按鈕。
3. 在可用工具清單，選取您要新增到儀表板的工具。
   工具按類別分組。要檢視包含在類別中的工具清單，點擊類別名稱旁邊的臂章圖示（ > ）。
4. 點擊**新增**按鈕。

所選的工具被新增到儀表板結尾。

您現在可以編輯所新增工具的展示和參數。

從儀表板隱藏小部件

要從儀表板隱藏工具：

1. 在主功能表中，轉至 **監控和報告** → **控制板**。
2. 點擊您要隱藏的工具旁邊的設定圖示（⚙）。
3. 選擇**隱藏 Web 小部件**。
4. 在開啟的**警告**視窗中，點擊**確定**。

所選工具被隱藏。稍後，您可以再次新增該工具到儀表板。

移動儀表板上的小部件

要移動工具到儀表板：

1. 在主功能表中，轉至 **監控和報告** → **控制板**。
2. 點擊您要移動的工具旁邊的設定圖示（⚙）。
3. 選擇**移動**。
4. 點擊您要移動工具的地方。您僅可以選取其他工具。

所選工具的地方被清掃。

變更部件尺寸或樣子

對於顯示圖表的工具，您可以變更其展示–線條圖或線形圖。對於一些工具，您可以變更其大小：最小、中度或最大。

要變更工具展示：

1. 在主功能表中，轉至 **監控和報告** → **控制板**。
2. 點擊您要編輯的工具旁邊的設定圖示（⚙）。
3. 執行以下操作之一：
   - 若要顯示小工具作為條狀圖，請選取 **圖表類型：線條**。
   - 若要顯示小工具作為直線圖，請選取 **圖表類型：線形**。

- 若要變更由小工具佔據的區域，請選取其中一個值：
  - **最小**
  - **最小（僅線條）**
  - **中度（餅圖）**
  - **中度（線條圖）**
  - **最大**

所選工具的展示被變更。

變更部件設定

要變更工具設定：

1. 在主功能表中，轉至 **監控和報告 → 控制板**。
2. 點擊您要變更的小工具旁邊的設定圖示（⚙）。
3. 選擇**顯示設定**。
4. 在開啟的工具設定視窗，變更所需的工具設定。
5. 點擊**儲存**以儲存變更。

所選工具的設定被變更。

設定集合取決於特定工具。以下是一些通用設定：

- **Web 小部件範圍**（小工具顯示資訊的物件集）—例如，管理群組或裝置分類。
- **選取工作**（小工具顯示資訊的工作）。
- **時間間隔**（小工具中顯示資訊的時間間隔）—介於兩個指定日期；從指定日期至當前日期；或從當前日期扣除目前日期的指定天數。
- **若指定以下條件，則設為"緊急"**與**若指定以下條件，則設為"警告"**（規判交通號誌燈號的規則）。

更改小部件設定後，您可以手動重新整理小部件上的資料。

要重新整理小部件上的資料：

1. 在主功能表中，轉至 **監控和報告 → 控制板**。
2. 點擊您要移動的工具旁邊的設定圖示（⚙）。
3. 選擇**重新整理**。

小部件上的資料已重新整理。

關於“僅儀表板”模式

您可以為不負責管理網路但需要在卡巴斯基安全管理中心雲端主控台中檢視網路防護統計資訊的員工（例如，高階經理）設定僅儀表板模式。當使用者啟用此模式時，只會向使用者顯示帶有一組預定義小工具的儀表板。因此，他或她可以監控小工具中指定的統計資訊，例如，所有受管理裝置的防護狀態、最近偵測到的威脅數量或網路中最常見的威脅清單。

當使用者在僅儀表板模式下工作時，將套用以下限制：

- 主功能表不向使用者顯示，因此他或她無法變更網路防護設定。
- 使用者不能用小工具執行任何操作，例如，新增或隱藏它們。因此，您需要將使用者所需的所有小工具都放在儀表板上並進行配置，例如，設定計數物件的規則或指定時間間隔。

您不能將僅儀表板模式分配給自己。如果要在此模式下工作，請聯絡系統管理員、受管理服務提供商 (MSP) 或在**一般功能：使用者權限**功能區域中具有**修改物件 ACL** 權限的使用者。

配置“僅儀表板”模式

在開始配置僅儀表板模式之前，請確保滿足以下先決條件：

- 您在**一般功能：使用者權限**功能區域中有**修改物件 ACL** 權限。如果您沒有此權限，則用於配置模式的標籤將缺失。
- 使用者在「**一般功能：基本功能**」功能區域中有**讀取**權限。

如果您網路中的管理伺服器已排列成階層，請在使用者帳戶位於的伺服器上，前往**使用者和角色 → 使用者和群組**區段**使用者**頁籤設定僅儀表板模式。它可以是主伺服器或實體從屬伺服器。無法在虛擬伺服器上調整模式。

若要配置僅儀表板模式：

1. 在主功能表中，轉至**使用者和角色 → 使用者和群組**，然後選擇**使用者**頁簽。
2. 按一下要使用小工具調整儀表板的使用者帳戶名稱。
3. 在開啟的帳戶設定視窗中，選取**儀表板**標籤。

   在開啟的標籤上，為您和使用者顯示相同的儀表板。
4. 如果**以僅儀表板模式顯示主控台**選項已啟用，用切換按鈕停用它。

   啟用此選項後，您也無法變更儀表板。停用該選項後，您可以管理小工具。
5. 配置儀表板外觀。在**儀表盤**標籤上準備的小工具集合可供具有可自訂帳戶的使用者使用。他或她不能變更小工具的任何設定或大小，也不能從儀表板新增或刪除任何小工具。因此，為使用者調整它們，以便他或她可以檢視網路防護統計資訊。為此，在**儀表板**標籤上，您可以對小部件執行於在**監控和報告→控制板**部分中相同的操作：
   - 新增小工具到儀表板。

- 隱藏使用者不需要的小工具。
- 移動小工具到特定的順序。
- 變更小工具的大小或外觀。
- 變更小工具設定。

6. 轉換切換按鈕以啟用**以僅儀表板模式顯示主控台**選項。

   之後，只有儀表板可供使用者使用。他或她可以監控統計資料，但不能變更網路防護設定和儀表板外觀。由於為您顯示的儀表板與為使用者顯示的儀表板相同，您也無法變更儀表板。

   如果您讓該選項保持停用，則主功能表會向該使用者顯示，供他或她在卡巴斯基安全管理中心雲端主控台中執行各種操作，包括變更安全設定和小工具。

7. 完成配置僅儀表板模式後按一下**儲存**按鈕。只有在那之後，準備好的儀表板才會顯示給使用者。

8. 如果使用者想要檢視受支援的卡巴斯基應用程式的統計資訊並且需要存取權限來執行此操作，請為使用者配置權限。之後，卡巴斯基應用程式資料將在這些應用程式的小工具中顯示給使用者。

現在，使用者可用經自訂的帳戶登入卡巴斯基安全管理中心雲端主控台並以僅儀表板模式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。

在卡巴斯基安全管理中心雲端主控台中存取報告的方式，是在**監控和報告**區段點擊**報告**。

預設下，報告包含 30 天內的資訊。

卡巴斯基安全管理中心雲端主控台預設會提供一組以下類別的報告：

- **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：

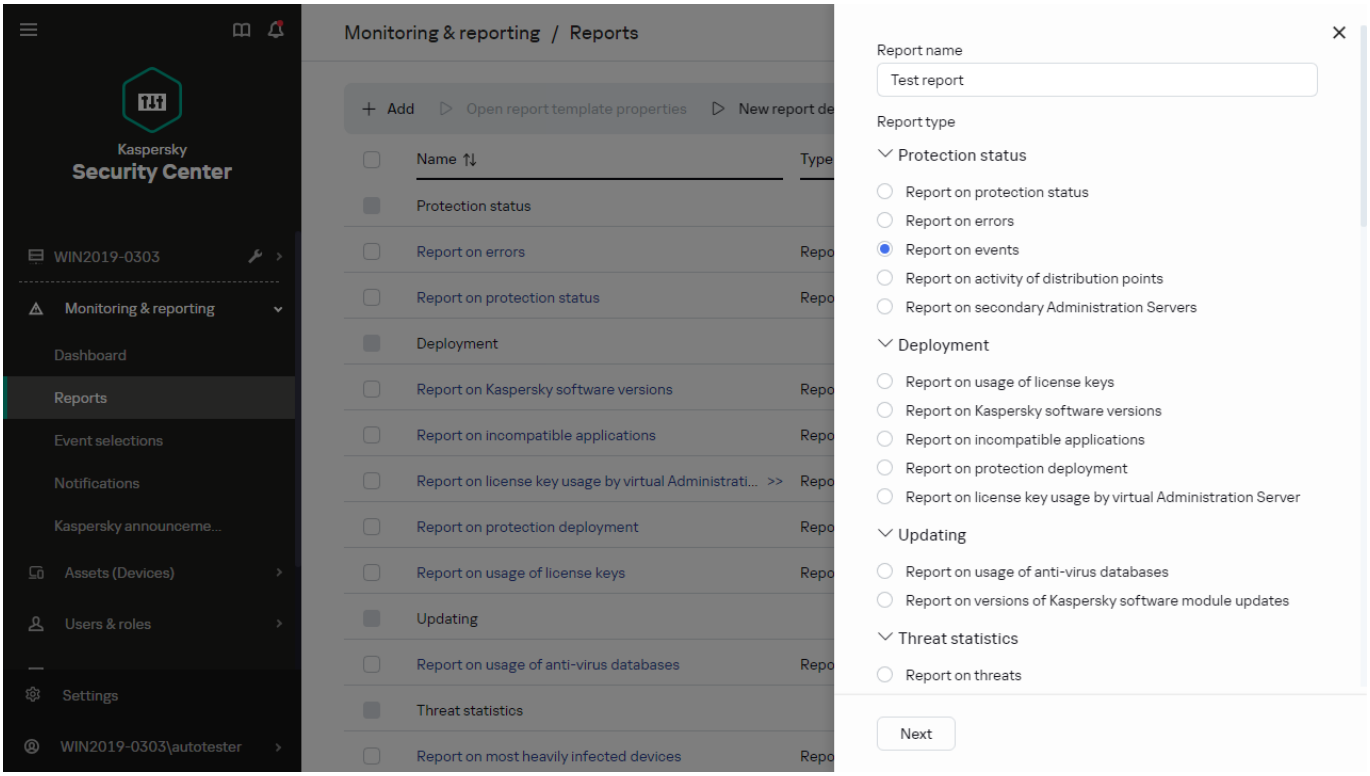
1. 在主功能表中，轉至 **監控和報告 → 報告**。

報告子區域中的報告範本清單

2. 點擊**新增**。

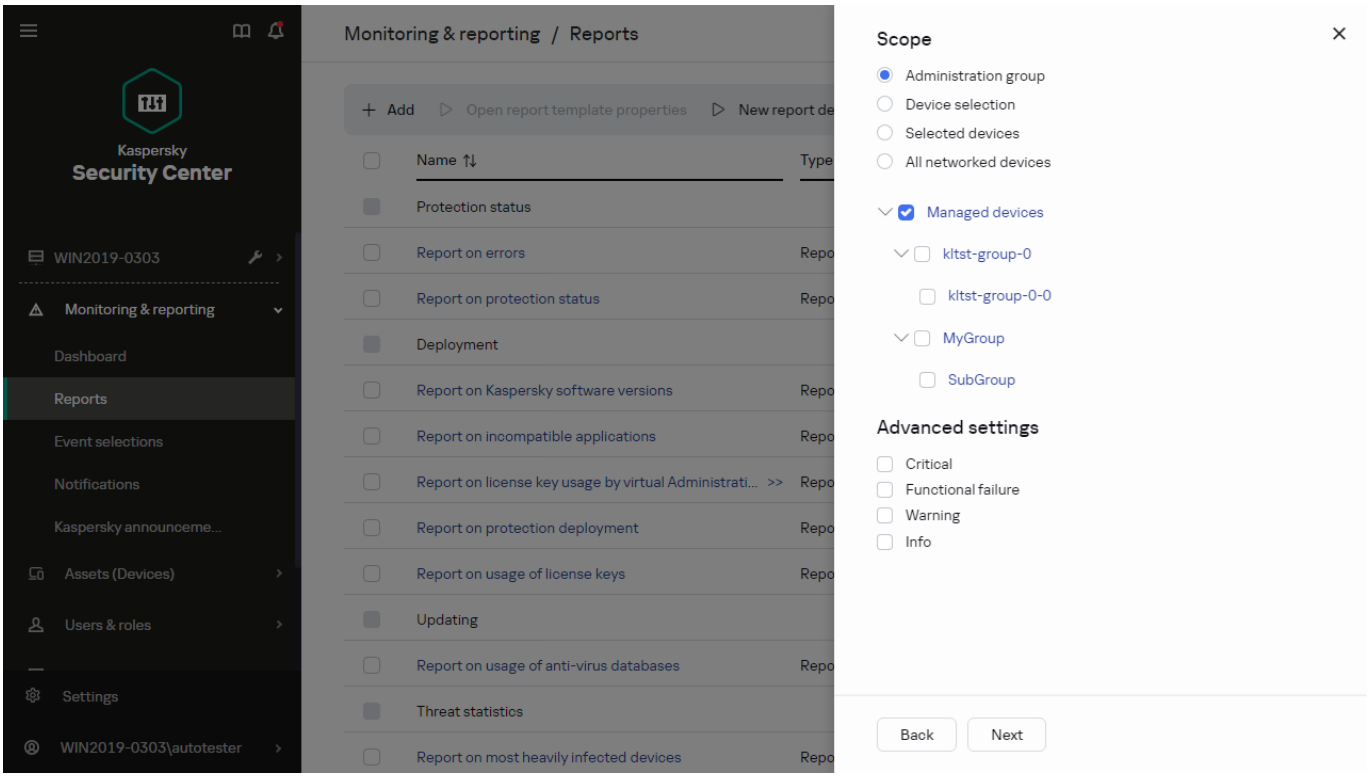
   程式將啟動"新報告範本精靈"。使用**下一步**按鈕進行精靈。

3. 在精靈的第一頁，輸入報告名稱並選取報告類型。



新報告範本精靈。指定報告範本的名稱和類型

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）。

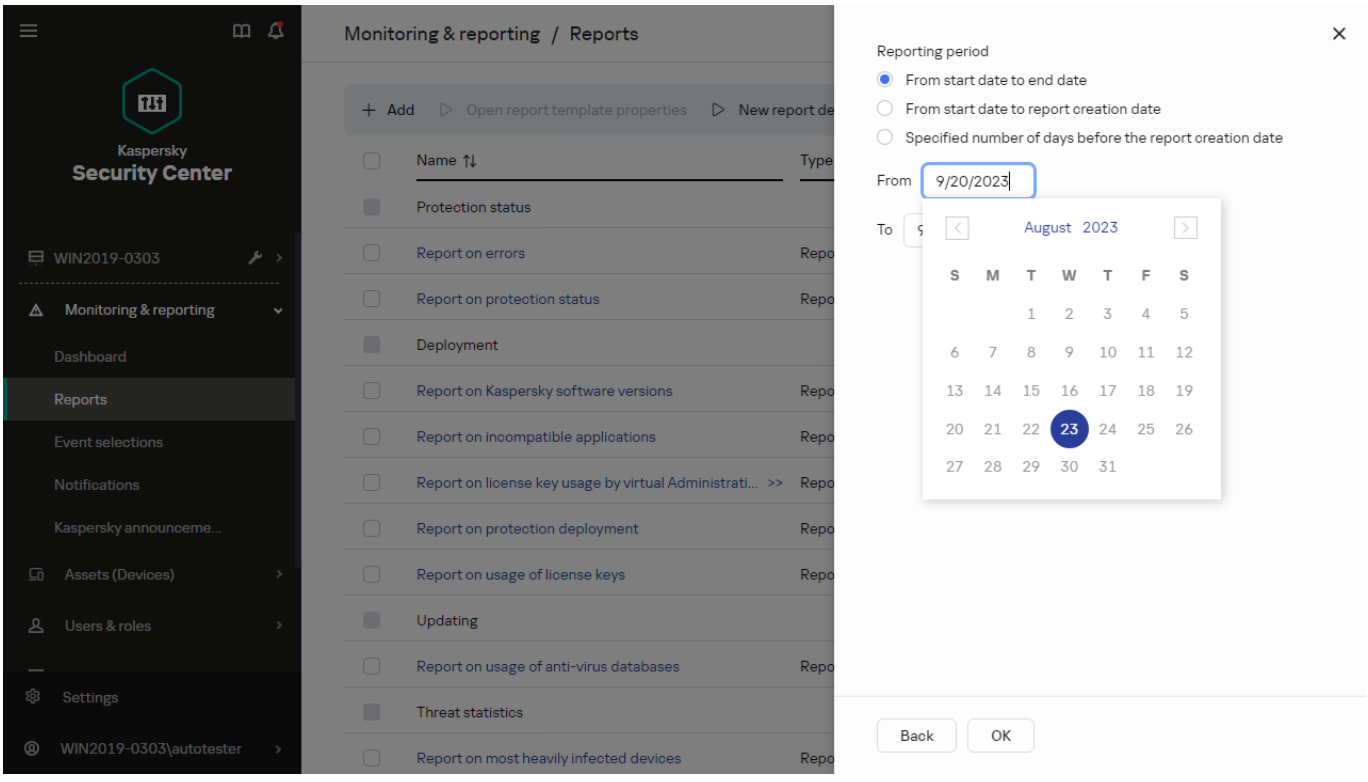


新報告範本精靈。指定報告範本範圍

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。



新報告範本精靈。指定報告期間

6. 點擊**確定**以關閉精靈。

7. 執行以下操作之一：

   - 點擊**儲存和執行**按鈕以儲存新報告範本並據此執行報告。
     報告範本被儲存。報告被生成。

   - 點擊**儲存**按鈕以儲存新報告範本精靈。
     報告範本被儲存。

您可以使用新範本來生成和檢視報告。

檢視和編輯報告範本內容

您可以檢視和編輯報告範本的基本內容，例如，報告範本名稱或顯示在報告中的欄位。

要檢視和編輯報告範本內容：

1. 在主功能表中，轉至 **監控和報告 → 報告**。

2. 選取您要檢視並編輯其內容的報告範本旁邊的核取方塊。
   或者，您可以先產生報告，然後點擊**編輯**按鈕。

3. 點擊**開啟報告範本內容**按鈕。
   編輯報告 <報告名稱>視窗會開啟，並含有所選的**一般**頁籤。

4. 編輯報告範本內容：

   - **一般**頁籤：

     - 報告範本名稱

     - **顯示項目的最大數量**

       如果啟用該選項，顯示在表格中的帶有詳細報告資料的項目數量不會超過指定值。請注意，此選項不會影響將報告匯出到檔案時可包含在報告中的最大事件數。

       報告項目首先根據指定在報告範本內容的**欄位 → 詳細資料欄位**區域的規則被儲存，然後僅第一個結果項目被儲存。帶有詳細報告資料的表頭展示顯示的項目數量和比對其他報告範本設定的可用項目總數。

       如果停用該選項，帶有詳細報告資料的表顯示所有可用項目。我們不建議您停用該選項。限制顯示的報告項目數量會降低資料庫管理系統 (DBMS) 負載，也會降低產生和匯出報告所需的時間。一些報告包含太多項目。如果是這樣，您可能難於閱讀和分析所有。而且，您的裝置可能在產生此報告時記憶體不夠，進而您將無法檢視報告。

       預設情況下已啟用該選項。預設值是 1000。

       請注意，卡巴斯基安全管理中心雲端主控台介面最多可顯示 2500 筆項目。如果您需要檢視更多數量的事件，請使用報告匯出功能。

     - **群組**

       點擊**設定**按鈕以變更建立報告的用戶端裝置集。對於一些報告類型，按鈕可能不可用。實際設定取決於建立報告範本時指定的設定。

- **時間間隔**

  點擊**設定**按鈕以修改報告時段。對於一些報告類型，按鈕可能不可用。有以下可用值：

  - 在兩個指定日期之間
  - 從指定日期到報告建立日期
  - 從報告建立日期減去指定天數

- **包含來自從屬和虛擬管理伺服器的資料**

  如果啟用該選項，報告包含屬於建立範本的管理伺服器的從屬和虛擬管理伺服器的資訊。

  如果您要僅從目前管理伺服器檢視資料，停用該選項。

  預設情況下已啟用該選項。

- **嵌套等級**

  報告包含位於目前管理伺服器下小於或等於指定巢狀等級的從屬和虛擬管理伺服器的資料。

  預設值是 1。如果您必須從樹中位於低等級的從屬管理伺服器接收資訊，您可能要變更該值。

- **資料等待間隔（分鐘）**

  在產生報告之前，建立報告範本的管理伺服器等待從屬管理伺服器的資料指定分鐘數。如果在該時間段後未從從屬管理伺服器接收到資料，報告依然執行。除了實際資料，報告也會顯示從快取接收的資料（如果**從屬管理伺服器的快取資料**選項已啟用），否則為 **N/A**（不可用）。

  預設值是 5 分鐘。

- **從屬管理伺服器的快取資料**

  從屬管理伺服器定期傳輸資料到建立報告範本的管理伺服器。傳輸的資料儲存在快取。

  如果在產生報告時目前管理伺服器無法從從屬管理伺服器接收資料，報告顯示從快取接收的資料。資料傳輸到快取的日期也被顯示。

  啟用該選項允許您檢視從屬管理伺服器資訊，即便即時資料無法被獲取。然而，所顯示資料可能過期。

  預設情況下已停用該選項。

- **快取更新頻率（小時）**

  從屬管理伺服器會在一定間隔時間傳輸資料到建立報告範本的管理伺服器。您可以以小時為單位指定此期間。如果指定值是 0 小時，資料僅會在產生報告時被傳輸。

  預設值是 0。

- **從從屬管理伺服器傳輸詳細資訊**

在產生的報告中，帶有詳細報告資料的表格包含建立報告範本的管理伺服器的從屬管理伺服器的資料。

啟用該選項會減慢報告產生並增加管理伺服器之間的流量。然而，您可以在一個報告中檢視所有資料。

除了啟用該選項，您可能想分析詳細報告資料以偵測故障從屬管理伺服器，然後僅為該故障管理伺服器產生相同報告。

預設情況下已停用該選項。

- **欄位**頁籤

  選取要在報告上顯示的欄位，並使用**向上移動**按鈕與**向下移動**按鈕變更這些欄位的順序。使用**新增**按鈕或**編輯** 按鈕指定報告中的資訊是否必須根據每個欄位排序或篩選。

  在**詳細欄位篩選器**區段，您也可以點擊**轉換篩選器**按鈕以開始使用延伸的篩選格式。此格式使您可以使用邏輯 OR 運算子來組合在各個欄位中指定的篩選條件。點擊該按鈕後，會開啟 **轉換篩選器** 面板。點擊 **轉換篩選器** 按鈕以確認轉換。現在，您可以使用邏輯 OR 運算子從套用的 **詳細資料欄位** 區段定義轉換篩選條件。

  將報告轉換為支援複雜篩選條件的格式將使該報告與卡巴斯基安全管理中心的早期版本（11 和更早版本）不相容。另外，轉換後的報告將不包含來自執行此類不相容版本的從屬管理伺服器的任何資料。

5. 點擊**儲存**以儲存變更。

6. 關閉**編輯報告<報告名稱>**視窗。

更新的報告範本顯示在報告範本清單。

匯出報告到檔案

您可以將一或多份報告儲存為 XML、HTML 或 PDF 檔案。卡巴斯基安全管理中心雲端主控台可讓您同時將最多 10 份報告匯出為指定格式的檔案。

要匯出報告到檔案：

1. 在主功能表中，轉至 **監控和報告 → 報告**。

2. 選擇您要匯出的報告。

   如果您選擇超過 10 個報告，**匯出報告**按鈕將被停用。

3. 點擊**匯出報告**按鈕。

4. 在開啟的視窗中，指定以下匯出參數：

   - **檔案名稱**。

     如果您選擇匯出一份報告，請指定報告檔案名稱。

     如果您選擇多個報告，報告檔案名稱將與所選報告模板的名稱一致。

   - **項目最大數量**。

     指定報告檔案中包含的最大項目數。預設值是 10,000。

- **檔案格式**。

  選取報告檔案格式：XML、HTML 或 PDF。如果匯出多個報告，所有選定的報告都會以指定的格式儲存為單獨檔案。

5. 點擊**匯出報告**按鈕。

報告以指定格式儲存到檔案中。

生成和瀏覽報告

要建立和瀏覽報告，請執行以下操作：

1. 在主功能表中，轉至 **監控和報告 → 報告**。
2. 點擊要用來建立報告的報告範本名稱。

   會產生並顯示使用所選範本的報告。

報告資料僅會以英文顯示，而無其他本地化版本。

此報告將顯示下列資料：

- 在**概要**頁籤：
  - 報告名稱和類型、簡要說明和報告時間區段，以及該報告為哪個裝置群組產生的相關資訊。
  - 圖表顯示最有代表性的報告資料。
  - 帶有計算好的報告指示器的加固表格。
- 在**詳細資訊**頁籤會顯示包含詳細報告資料的表格。

建立報告傳送工作

您可以建立傳送所選報告的工作。

要建立報告傳送工作：

1. 在主功能表中，轉至 **監控和報告 → 報告**。
2. 【可選】選取您要建立報告傳送工作的報告範本旁邊的核取方塊。
3. 點擊**新報告傳送工作**按鈕。
4. 新工作精靈啟動。使用**下一步**按鈕進行精靈。
5. 在精靈的第一頁，輸入工作名稱。預設名稱為 **傳送報告（<N>）**，其中 <N> 是工作的序號。

6. 在精靈的工作設定頁面，指定以下設定：

   a. 要使用工作傳送的報告範本。如果您在步驟 2 選取了它們，請略過此步驟。

   b. 報告格式：HTML、XLS 或 PDF。

   c. 報告是否使用電子郵件連同郵件通知設定一起傳送。

7. 若要在建立工作後修改其他工作設定，請精靈的**完成工作建立**頁面啟用**建立完成時開啟工作詳情**選項。

8. 點擊**建立**按鈕以建立工作並關閉精靈。

   報告傳送工作被建立。若您啟用**建立完成時開啟工作詳情**選項，工作設定視窗隨即開啟。

刪除報告範本

要刪除一個或幾個報告範本：

1. 在主功能表中，轉至 **監控和報告 → 報告**。

2. 選取您要刪除的報告範本旁邊的核取方塊。

3. 點擊**刪除**按鈕。

4. 在開啟的視窗中，點擊**確定**按鈕以確認您的選取。

   所選報告範本被刪除。如果這些報告範本被包含在報告傳送工作中，它們也被從工作刪除。

事件和事件選擇

本節提供以下方面的相關資訊：事件和事件分類、卡巴斯基安全管理中心雲端主控台元件中發生的事件類型以及對頻繁事件的封鎖管理。

關於卡巴斯基安全管理中心雲端主控台中的事件

卡巴斯基安全管理中心雲端主控台可讓您接收管理伺服器和受管理裝置上所安裝 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雲端主控台中，事件分以下類型：

- 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雲端主控台元件：
  - 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，在這期限內您都可以在卡巴斯基安全管理中心雲端主控台中加以檢視或修改。一些事件預設下不儲存在管理伺服器資料庫，因為它們的儲存期限是零。僅可以在管理伺服器資料庫中儲存至少一天的事件可以被匯出到外部系統。

卡巴斯基安全管理中心雲端主控台元件的事件

每個卡巴斯基安全管理中心雲端主控台元件都各有一組自己的事件類型。本節列出了卡巴斯基安全管理中心雲端主控台管理伺服器和網路代理中會發生的事件類型。Kaspersky 應用程式中發生的事件類型不在此區域列出。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。對於管理伺服器，您還可以在管理伺服器屬性中檢視和設定事件清單。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

事件類型描述的資料結構

對於每個事件類型，它的顯示名稱、ID、字母碼、描述和預設儲存期限被提供。

- **事件類型顯示名稱**。在卡巴斯基安全管理中心雲端主控台中，這段文字會在您設定事件以及事件發生時顯示。

- **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）。會用到此代碼的時機為當您使用卡巴斯基安全管理中心雲端主控台資料庫中提供的公用視圖瀏覽和處理事件時。
- **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。

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

下表顯示了重要性等級為**緊急**的卡巴斯基安全管理中心雲端主控台管理伺服器事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。對於管理伺服器，您還可以在管理伺服器屬性中檢視和設定事件清單。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

管理伺服器緊急事件

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	卡巴斯基安全管理中心雲端主控台會每天檢查一次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）。 在超過產品授權限制時產生事件的規則是由卡巴斯基安全管理中心雲端主控台決定。	180 天
病毒爆發	26（對於檔案	GNRL_EV_VIRUS_OUTBREAK	當短時間內在若干受管理裝置上偵測到的惡意物件數量超過	180 天

	威脅防護）		上限值時，該類型的事件發生。 您可以透過以下方式回應事件： • 您可以在管理伺服器內容中配置上限值。 • 您也可以建立嚴格政策以便被啟動，或者建立工作以便在事件發生時執行。	
病毒爆發	27（對於郵件威脅防護）	GNRL_EV_VIRUS_OUTBREAK	當短時間內在若干受管理裝置上偵測到的惡意物件數量超過上限值時，該類型的事件發生。 您可以透過以下方式回應事件： • 您可以在管理伺服器內容中配置上限值。 • 您也可以建立嚴格政策以便被啟動，或者建立工作以便在事件發生時執行。	180天
病毒爆發	28（對於防火牆）	GNRL_EV_VIRUS_OUTBREAK	當短時間內在若干受管理裝置上偵測到的惡意物件數量超過上限值時，該類型的事件發生。 您可以透過以下方式回應事件： • 您可以在管理伺服器內容中配置上限值。 • 您也可以建立嚴格政策以便被啟動，或者建立工作以便在事件發生時執行。	180天
裝置已失去管理	4111	KLSRV_HOST_OUT_CONTROL	如果受管理裝置在網路中可見，但一定時間未連線到管理伺服器，則該類型的事件發生。 找到什麼封鎖了裝置上網路代理的正常功能。可能的原因包括網路問題和從裝置移除網路代理。	180天
裝置狀態為"緊急"	4113	KLSRV_HOST_STATUS_CRITICAL	當受管理裝置被分配*緊急*狀態時，該類型的事件發生。您可設定將裝置狀態變更為*緊急*的條件。	180天
受限功能模式	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	當卡巴斯基安全管理中心雲端主控台開始以基本功能運作，而不提供「弱點和修補程式管	180天

			理」和「行動裝置管理」功能時，會發生此類型的事件。 以下是事件發生的原因和正確回應： • 產品授權期限已到期。請提供產品授權（在管理伺服器上新增有效的啟動碼或金鑰檔案），以便使用以完整運作模式的卡巴斯基安全管理中心雲端主控台。 • 管理伺服器管理比產品授權限制更多的裝置。從管理伺服器的管理群組移動裝置到其他管理伺服器的管理群組（如果其他管理伺服器的產品授權限制允許）。	
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。如果管理伺服器在產品授權到期日期前的指定日期關閉，則事件將在第二天發布。 當正式授權到期時，卡巴斯基安全管理中心雲端主控台僅會提供基本功能。 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	資訊將於近期補上。	180 天
Kaspersky 軟體模組更新已撤銷	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	如果無縫更新被 Kaspersky 技術專家撤銷（這些更新顯示*已撤銷*狀態）；例如，它們必須被更新到新版本，則該類型的事件發生。此事件與卡巴斯基安全管理中心雲端主控台修補程式有關，而與 Kaspersky 受管理應用程式的模組無關。事	180 天

			件提供無縫更新未被安裝的原因。	
稽核：匯出到 SIEM 失敗	5130	KLAUD_EV_SIEM_EXPORT_ERROR	當匯出事件到 SIEM 系統因 SIEM 系統連線錯誤而失敗時，會發生此類型的事件。	180 天

管理伺服器功能失效事件

下文的表格了顯示重要性等級為**功能失效**的卡巴斯基安全管理中心雲端主控台管理伺服器事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。對於管理伺服器，您還可以在管理伺服器屬性中檢視和設定事件清單。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

管理伺服器功能失效事件

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
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雲端主控台中，您會管理協力廠商應用程式的授權金鑰，而安裝數量超過了協力廠商應用程式的授權金鑰所設定的限制，則會發生此類型的事件。 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

管理伺服器警告事件

下文的表格顯示了重要性等級為**警告**的卡巴斯基安全管理中心雲端主控台管理伺服器事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。對於管理伺服器，您還可以在管理伺服器屬性中檢視和設定事件清單。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

管理伺服器警告事件

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	卡巴斯基安全管理中心雲端主控台會每天檢查一次是否超過產品授權限制。	90 天

			當管理伺服器發現安裝在用戶端裝置上的 Kaspersky 應用程式超過了產品授權限制，以及由單一產品授權覆寫的目前使用的產品授權單元數量達到了該產品授權覆寫的單元總數的 100% 到 110%，則該類型的事件發生。 即便當該事件發生時，用戶端裝置是被防護的。 您可以透過以下方式回應事件： • 檢視受管理裝置清單。刪除不在使用的裝置。 • 為更多裝置提供產品授權（新增有效的啟動碼或金鑰檔案至管理伺服器）。在超過產品授權限制時產生事件的規則是由卡巴斯基安全管理中心雲端主控台決定。	
裝置在網路上已長時間沒有活動	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	資訊即將補上。	90 天
裝置名稱衝突	4102	KLSRV_EVENT_HOSTS_CONFLICT	資訊即將補上。	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。您可設定將裝置狀態變更為 *警告* 的條件。	90 天
已授權應用程式群組之一的安裝即將達到限制	4127	KLSRV_INVLICPROD_FILLED	資訊即將補上。	90 天
憑證已被請求	4133	KLSRV_CERTIFICATE_REQUESTED	資訊即將補上。	90 天
憑證已刪除	4134	KLSRV_CERTIFICATE_REMOVED	資訊即將補上。	90 天
APNs 憑證已到期	4135	KLSRV_APN_CERTIFICATE_EXPIRED	資訊即將補上。	90 天
APNs 憑證即將到期	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	資訊即將補上。	90 天
傳送 FCM 訊息到行動裝置失敗	4138	KLSRV_GCM_DEVICE_ERROR	資訊即將補上。	90 天
傳送 FCM 訊息到 FCM 伺服	4139	KLSRV_GCM_HTTP_ERROR	資訊即將補上。	90 天

器時發生 HTTP 錯誤				
傳送 FCM 訊息到 FCM 伺服器失敗	4140	KLSRV_GCM_GENERAL_ERROR	資訊即將補上。	90 天
連到從屬管理伺服器的連線已中斷	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	資訊即將補上。	90 天
連到主管理伺服器的連線已中斷	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	資訊即將補上。	90 天
KSN 代理已啟動。檢查 KSN 可用性失敗	7719	KSNPROXY_STARTED_CON_CHK_FAILED	資訊即將補上。	90 天
已註冊 Kaspersky 軟體模組的新更新	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	資訊即將補上。	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： • 變更管理伺服器資料庫中儲存的最大事件數量。 • 降低儲存在管理伺服器資料庫的事件數量。	90 天
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： • 變更允許管理伺服器資料庫中儲存的最大事件數量。 • 降低儲存在管理伺服器資料庫的事件數量。	90 天
產品授權即將到期	4128	KLSRV_INVLICPROD_EXPIRED_SOON	資訊即將補上。	90 天
稽核：SIEM 伺服器連線測試失敗	5120	KLAUD_EV_SIEM_TEST_FAILED	當 SIEM 伺服器自動連線測試失敗時，會發生此類型的事件。	90 天

管理伺服器資訊事件

下文的表格顯示了重要性等級為**資訊**的卡巴斯基安全管理中心雲端主控台管理伺服器事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。對於管理伺服器，您還可以在管理伺服器屬性中檢視和設定事件清單。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

管理伺服器資訊事件

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
根據規則自動移動裝置	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 （在卡巴斯基安全管理中心雲端主控台中，此事件類型僅適用於從屬管理伺服器。）	4144	KLSRV_UPD_BASES_UPDATED	30 天
KSN 代理已啟動。KSN 可用性檢查已成功完成	7718	KSNPROXY_STARTED_CON_CHK_OK	30 天
KSN 代理已停止	7720	KSNPROXY_STOPPED	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：加密金鑰已從管理伺服器匯入或者匯出	5100	KLAUD_EV_DPEKEYSEXPORT	30 天
稽核：SIEM 伺服器連線測試成功	5110	KLAUD_EV_SIEM_TEST_SUCCESS	30 天

網路代理事件

該部分包含網路代理相關事件資訊。

網路代理功能失效事件

下表顯示具有**功能失效**嚴重等級的卡巴斯基安全管理中心網路代理事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

網路代理功能失效事件

事件類型顯示名稱	事件類型 ID	事件類型	敘述	預設儲存期限
更新安裝錯誤	7702	KLNAG_EV_PATCH_INSTALL_ERROR	如果自動更新和修補卡巴斯基安全管理中心雲端主控台元件不成功，則會發生此類型的事件。事件不包含受管理的 Kaspersky 應用程式的更新。 閱讀事件描述。管理伺服器上的 Windows 問題可能是該事件的原因。如果描述提到 Windows 配置的任何問題，解決該問題。	30 天
安裝協力廠商軟體更新失敗	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	如果正在使用「弱點和修補程式管理」和「行動裝置管理」而協力廠商軟體更新不成功，則會發生此類型的事件。 檢查到協力廠商軟體的連結是否合法。閱讀事件描述。	30 天
安裝 Windows Update 更新失敗	7717	KLNAG_EV_WUA_INSTALL_ERROR	如果 Windows 更新未成功，則該類型的事件發生。請在網路代理政策中設定 Windows 更新。 閱讀事件描述。在 Microsoft 知識庫中尋找錯誤。如果您無法自己解決問題，請聯絡 Microsoft 技術支援。	30 天

網路代理警告事件

下表顯示具有**警告**嚴重等級的卡巴斯基安全管理中心網路代理事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

網路代理警告事件

事件類型顯示名稱	事件類型 ID	事件類型	預設儲存期限
在安裝軟體模組更新期間返回了警告	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 天
協力廠商軟體更新安裝已完成但存在警告	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 天
協力廠商軟體更新已延時	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 天
發生了安全問題	549	GNRL_EV_APP_INCIDENT_OCCURED	30 天
KSN 代理已啟動。檢查 KSN 可用性失敗	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 天

網路代理資訊事件

下表顯示具有**資訊**嚴重等級的卡巴斯基安全管理中心網路代理事件。

對於應用程式可以產生的每個事件，您可以在應用程式政策的**事件配置**標籤上指定通知設定和儲存設定。如果要一次為所有事件設定通知設定，請在管理伺服器內容中設定常規通知設定。

網路代理資訊事件

事件類型顯示名稱	事件類型 ID	事件類型	預設儲存期限
軟體模組更新已成功安裝	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 天
軟體模組更新安裝已啟動	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 天
應用程式已安裝	7703	KLNAG_EV_INV_APP_INSTALLED	30 天
應用程式已解除安裝	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 天
已安裝監控的應用程式	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 天
已解除安裝監控的應用程式	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 天
已安裝協力廠商應用程式	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 天
已新增裝置	7708	KLNAG_EV_DEVICE_ARRIVAL	30 天
裝置已被刪除	7709	KLNAG_EV_DEVICE_REMOVE	30 天
裝置已被偵測	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30

			天
裝置已被授權	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 天
Windows 共用桌面：檔案已讀取	7712	KLUSRLOG_EV_FILE_READ	30 天
Windows 共用桌面：檔案已修改	7713	KLUSRLOG_EV_FILE_MODIFIED	30 天
Windows 共用桌面：應用程式已啟動	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 天
Windows 共用桌面：已啟動	7715	KLUSRLOG_EV_WDS_BEGIN	30 天
Windows 共用桌面：已停止	7716	KLUSRLOG_EV_WDS_END	30 天
協力廠商軟體更新已成功安裝	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 天
協力廠商軟體更新安裝已開始	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 天
KSN 代理已啟動。KSN 可用性檢查已成功完成	7719	KSNPROXY_STARTED_CON_CHK_OK	30 天
KSN 代理已停止	7720	KSNPROXY_STOPPED	30 天

使用事件分類

事件選項提供從管理伺服器資料庫中選取的事件的命名集合的螢幕視圖。這些事件集會根據以下類別分組：

- 依嚴重等級—**緊急事件**、**功能失效**、**警告**和**資訊事件**
- 依時間—**最近事件**
- 依類型—**使用者請求**和**稽核事件**

您可以基於 Kaspersky Security Center Cloud Console 介面中可供配置的設定，建立和檢視使用者定義的事件分類。

在卡巴斯基安全管理中心雲端主控台中存取事件分類的方式，是在**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雲端主控台預設會提供一組預先定義的事件分類：

- 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**

  在卡巴斯基安全管理中心雲端主控台中，會顯示與您工作區中的服務運作相關的稽核事件。這些事件的發生條件是由 Kaspersky 專家操作設定。這些事件包括像是：變更管理伺服器連接埠、備份管理伺服器資料庫，以及建立、修改和刪除使用者帳戶。

您也可以建立和配置附加使用者定義分類。在使用者定義分類中，您可以根據裝置內容（裝置名稱、IP 範圍和管理群組）、根據事件類型和嚴重等級、根據應用程式和元件名稱、以及根據時間間隔來篩選事件。也可以包含工作結果到搜尋範圍。您也可以單一搜尋欄位，可以輸入一個詞或幾個詞。所有內容（例如事件名稱、描述、元件名稱）中包含任意所輸入詞的事件被顯示。

對於預先定義和使用者定義的分類，您可以限制顯示事件的數量或者要搜尋的記錄的數量。這兩種選項都會影響卡巴斯基安全管理中心雲端主控台顯示事件所花費的時間。資料庫越大，過程越耗時。

您可以執行以下操作：

- 編輯事件分類的內容
- 產生事件分類
- 檢視事件分類的詳細資訊
- 刪除事件分類
- 從管理伺服器資料庫中刪除事件

建立事件分類

要建立事件分類，請執行以下操作：

1. 在主功能表中，轉至 **監控和報告 → 事件分類**。
2. 點擊**新增**。
3. 在開啟的**新事件分類**視窗，指定新事件分類的設定。在視窗中重複此操作。
4. 點擊**儲存**以儲存變更。

   確認視窗開啟。
5. 若要檢視事件分類結果，請持續選取**轉到分類結果**核取方塊。
6. 點擊**儲存**以確認建立事件分類。

若您持續選取**轉到分類結果**核取方塊，會顯示事件分類結果。否則，新事件分類出現在事件分類清單。

編輯事件分類

要編輯事件分類：

1. 在主功能表中，轉至 **監控和報告 → 事件分類**。
2. 選取您要編輯的事件分類旁邊的核取方塊。
3. 點擊**內容**按鈕。
   事件分類設定視窗開啟。
4. 編輯事件分類內容。

   > 對於預先定義的事件分類，您盡可編輯以下頁籤的內容：**一般**（分類名稱除外）、**時間**以及**存取權限**。

   對於使用者定義分類，您可以編輯所有內容。
5. 點擊**儲存**以儲存變更。

編輯的事件分類顯示在清單。

查看事件分類清單

要檢視事件分類，請執行以下操作：

1. 在主功能表中，轉至 **監控和報告 → 事件分類**。
2. 選取您要啟動的事件分類旁邊的核取方塊。
3. 執行以下操作之一：
   - 如果您要在事件分類結果中配置排序，做以下：
     a. 點擊**重新配置排序並啟動**按鈕。
     b. 在顯示的 **重新配置事件分類排序** 視窗中指定排序設定。
     c. 請點擊選項的名稱。
   - 或者，若您要在管理伺服器上排序好事件後檢視事件清單，請點擊選項名稱。

事件分類結果被顯示。

匯出事件分類

卡巴斯基安全管理中心雲端主控台可讓您將事件分類及其設定儲存到 KLO 檔案。您可以使用此 KLO 檔案匯入儲存的事件分類到 Kaspersky Security Center Windows 和 Kaspersky Security Center Linux。

請注意，您只能匯出使用者定義的事件分類。卡巴斯基安全管理中心雲端主控台預設會提供的一組事件分類（預先定義的分類）無法儲存到檔案。

要匯出事件分類，請執行以下操作：

1. 在主功能表中，轉至**監控和報告 → 事件分類**。
2. 選取您要匯出的事件分類旁邊的核取方塊。
   您不能同時匯出多個事件分類。如果您選擇了多個分類，**匯出**按鈕將被停用。
3. 點擊**匯出**按鈕。
4. 在開啟的**另存為**視窗中，指定事件分類檔案名稱和路徑，然後點擊**儲存**按鈕。
   另存新檔視窗僅當您使用 Google Chrome、Microsoft Edge 或 Opera 時才會顯示。如果您使用其他瀏覽器，事件分類檔案會自動儲存在**下載**資料夾中。

匯入事件分類

卡巴斯基安全管理中心雲端主控台可讓您從 KLO 檔案匯入事件分類。KLO 檔案包含匯出事件分類及其設定。

要匯入事件分類，請執行以下操作：

1. 在主功能表中，轉至**監控和報告 → 事件分類**。
2. 點擊**匯入**按鈕，然後選擇要匯入的事件分類檔案。
3. 在開啟的視窗中，指定 KLO 檔案的路徑，然後按一下**開啟**按鈕。請注意，您只能選擇一個事件分類檔案。
   事件分類處理開始。

此時會顯示匯入結果通知。如果事件分類匯入成功，您可以點擊**檢視匯入詳細資訊**連接來檢視事件分類屬性。

匯入成功後，事件分類會顯示在分類清單中。事件分類的設定也會被匯入。

如果新匯入事件分類的名稱與現有事件分類的名稱相同，則匯入分類的名稱將加上 **(<next sequence number>)** 索引，例如：**(1)**、**(2)**。

檢視事件詳情

要檢視事件詳情：

1. 啟動事件分類。
2. 點擊所需事件的時間。

事件內容視窗開啟。

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。

記錄工作與政策的事件資訊

本節提供關於如何將卡巴斯基安全管理中心雲端主控台資料庫中儲存的工作與政策事件數量降到最低的建議。每 1000 個裝置預設可以有 100,000 個事件。如果超過這項限制，新事件將會覆寫舊事件。緊急事件可能會因此而消失。此外，還可能會發生名為**超過資料庫中的事件數量限制，事件已被刪除**的管理伺服器警告事件。在這些情況下，我們建議您依本節中的指示進行操作。

您執行事件分析相關情境的速度將能因此而提高。此外，這些建議還可幫助您減少緊急事件因大量事件而遭覆寫的風險。

預設下，每個工作和政策的內容可以用於儲存所有工作執行和政策施加的相關事件。不過，某項工作如果執行頻率太頻繁（例如，每週不止一次），則產生的事件數量可能會太多，進而淹沒整個事件資料庫。在此情況下，建議您在工作設定中選取以下兩個選項之一：

- **儲存工作進度相關事件**。在此情況下，卡巴斯基安全管理中心雲端主控台僅會儲存每個執行工作的裝置所傳來有關工作啟動、進度和完成狀態（成功、存在警告或存在錯誤）的資訊。
- **僅儲存工作執行結果**。在此情況下，卡巴斯基安全管理中心雲端主控台僅會儲存每個執行工作的裝置所傳來有關工作完成狀態（成功、存在警告或存在錯誤）的資訊。

所定義的政策如果適用的裝置為數相當大（例如，超過 10,000 台），則產生的事件可能會太多，進而淹沒整個事件資料庫。在此情況下，我們建議您在政策設定中僅選取最緊急的事件並啟用對它們的記錄。建議您停用所有其他事件的記錄。

您也可以降低工作或政策相關事件的儲存期限。預設期限是工作相關事件 7 天和政策相關事件 30 天。當變更事件儲存期限時，請考慮您組織的工作過程和系統管理員可以分析每個事件的時間。

如果在卡巴斯基安全管理中心雲端主控台資料庫內的所有事件中，群組工作中間狀態變更事件以及政策套用事件佔據了很大比例，則建議您可以修改事件儲存設定。

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**。

   事件分類被刪除。

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。

關於通知

卡巴斯基安全管理中心雲端主控台可就任何您認為重要的事件傳送事件通知，方便您監控您組織的網路。您可以為任何事件設定電子郵件通知。

您在收到電子郵件通知時，可以決定要如何對事件做出回應。該回應必須是對您的組織網路而言最適當的回應。

設定裝置狀態轉換

您可變更條件以為裝置配置*緊急*或*警告*狀態。

要啟用變更裝置狀態到緊急：

1. 在主功能表中，轉至 **資產（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 **資產（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

您可以為卡巴斯基安全管理中心雲端主控台中發生的事件設定電子郵件通知。

若要設定在卡巴斯基安全管理中心雲端主控台中發生事件時傳送事件通知：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗會開啟，並含有所選的**一般**頁籤。

2. 點擊**通知**區段，然後在右側窗格中定義電子郵件通知設定：
   收件者（電子郵件信箱）

   要讓卡巴斯基安全管理中心雲端主控台將通知傳送到的電子郵件地址。您可以在該欄位指定多個位址，以分號分隔。

   您最多可以指定 24 個電子郵件地址。

3. 點擊**傳送測試訊息**按鈕以檢查您是否正確設定了通知：應用程式會將測試通知傳送到您指定的電子郵件地址。

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即會套用到卡巴斯基安全管理中心雲端主控台中發生的所有事件。

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。

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

卡巴斯基公告區段 (**監控和報告 → 卡巴斯基公告**) 會提供卡巴斯基安全管理中心雲端主控台以及受管理裝置上所安裝受管理應用程式的相關資訊，方便您隨時掌握最新情況。卡巴斯基安全管理中心雲端主控台會定期更新該區段中的資訊，也就是刪除過時的公告並加入新資訊。

卡巴斯基安全管理中心雲端主控台僅會針對目前連線的管理伺服器以及在該管理伺服器的受管理裝置上安裝的 Kaspersky 應用程式，顯示相關的卡巴斯基公告。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。

如果有多個管理員使用卡巴斯基安全管理中心雲端主控台，但他們各自設定了不同的介面語言，則卡巴斯基安全管理中心雲端主控台會以這些管理員使用的每種語言顯示卡巴斯基公告。當您在變更介面語言後登出再登入主控台，所選語言的卡巴斯基公告即會自動新增至該區段。

公告包括以下類型的資訊：

- 與安全相關的公告

  與安全相關的公告旨在使網路中安裝的卡巴斯基應用程式保持最新狀態並具有完整功能。公告可能包括有關卡巴斯基應用程式的重要更新、已發現弱點的修復以及解決卡巴斯基應用程式中其他問題的方法資訊。預設情況下，與安全相關的公告是啟用的。如果您不想接收卡巴斯基公告，則可以停用此功能。

  > 在試用模式的卡巴斯基安全管理中心雲端主控台中，您無法停用安全相關公告。

  為了向您顯示與您的網路防護設定相對應的資訊，卡巴斯基安全管理中心雲端主控台會向 Kaspersky 雲端伺服器傳送資料，然後僅接收與您網路中安裝的 Kaspersky 應用程式相關的公告。您在建立公司工作區時接受的卡巴斯基安全管理中心雲端主控台協議中，會說明可能會向伺服器傳送的資料集。

- 行銷公告

  行銷公告包括有關卡巴斯基應用程式的特別優惠、廣告和卡巴斯基新聞的資訊。預設情況下，會停用行銷公告。僅在啟用卡巴斯基安全網路 (KSN) 的情況下，您才會收到此類公告。您可以透過停用 KSN 停用行銷公告。

  為了僅向您顯示可能有助於您保護網路裝置和進行日常工作的相關資訊，卡巴斯基安全管理中心雲端主控台會向 Kaspersky 雲端伺服器傳送資料，然後接收適當的公告。可傳送到伺服器的資料集在 KSN 聲明的"已處理資料"區段中有說明。

根據重要性，新資訊分為以下幾類：

1. 重要資訊
2. 重要新聞
3. 警告
4. 資訊

當卡巴斯基公告區段中出現新資訊時，卡巴斯基安全管理中心雲端主控台會顯示一個與公告的重要性等級相對應的通知標籤。您可以在"卡巴斯基公告"部分中點擊標籤以檢視此公告。

停用卡巴斯基公告

卡巴斯基公告區段（**監控和報告 → 卡巴斯基公告**）會提供與您卡巴斯基安全管理中心雲端主控台版本以及受管理裝置上安裝的受管理應用程式相關的資訊，方便您隨時掌握最新情況。如果您不想接收卡巴斯基公告，則可以停用此功能。

卡巴斯基公告包括兩種類型的資訊：與安全相關的公告和行銷公告。您可以分別停用每種類型的公告。

在試用模式的卡巴斯基安全管理中心雲端主控台中，您無法停用安全相關公告。

停用與安全性有關的公告：

1. 在主功能表中，按一下管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取**卡巴斯基公告**部分。
3. 將切換按鈕切換到**與安全相關的公告 已停用**位置。
4. 點擊**儲存**按鈕。
   卡巴斯基的公告已停用。

預設情況下，會停用行銷公告。僅在啟用卡巴斯基安全網路 (KSN) 的情況下，您才會收到行銷公告。您可以透過停用 KSN 來停用此類型的公告。

停用行銷公告：

1. 在主功能表中，按一下管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**標籤上，選取**KSN 設定**區段。
3. 停用**我同意使用卡巴斯基安全網路**選項。
4. 點擊**儲存**按鈕。
   行銷公告隨即停用。

接收產品授權到期警告

若要在管理伺服器中新增 Kaspersky Endpoint Security for Business Select 產品授權金鑰：

1. 在主功能表中，按一下管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁簽上，選取**License keys**區段。

3. 點擊**選取**。

4. 在開啟的視窗中，選取您的產品授權，然後點擊**確定**。

   或者，如果未顯示產品授權，您可以點擊**新增新的產品授權金鑰**，然後使用您的啟動碼。

該產品授權金鑰即已新增到管理伺服器儲存區中。這會讓管理伺服器在產品授權期限到期的一天前產生*產品授權即將到期*的緊急事件，並在產品授權期限到期之後產生*受限功能模式*的緊急事件。如有需要，您可以設定傳送通知。

如果您將 Kaspersky Endpoint Security for Business Select 產品授權金鑰新增至管理伺服器儲存區，則該產品授權將被視為已在一台裝置上使用。

Cloud Discovery

卡巴斯基安全管理中心雲端主控台可讓您監控執行 Windows 的受管理裝置上使用雲端服務的情況，甚至封鎖您認為不需要的雲端服務存取活動。Cloud Discovery 會追蹤使用者嘗試透過瀏覽器和桌面應用程式對這些服務進行的存取活動。它還會追蹤使用者嘗試透過未加密連線（例如，使用 HTTP 通訊協定）對雲端服務進行的存取活動。此功能可協助您偵測並制止「影子 IT」使用雲端服務。

僅當您購買了其中一種 Kaspersky NEXT 產品授權時，Cloud Discovery 功能才可使用。如需詳細資訊，請參閱各種產品授權和其最小裝置數量。

您可以啟用 Cloud Discovery 功能，然後選取要啟用該功能的安全政策或設定檔。您也可以分別在每個安全政策或設定檔中啟用或停用該功能。對於您不想讓使用者存取的雲端服務，您可以封鎖對這些雲端服務進行的存取活動。

為了能夠封鎖對不需要的雲端服務進行的存取活動，請確保滿足以下先決條件：

- 使用 Kaspersky Endpoint Security 11.2 for Windows 或更高版本。該安全應用程式的更早版本僅能讓您監控雲端服務的使用情況。
- 已購買其中一種 Kaspersky NEXT 產品授權，該產品授權能夠封鎖對不需要的雲端服務進行的存取活動。

Cloud Discovery 小工具和 Cloud Discovery 報告會顯示與嘗試存取雲端服務時成功與遭封鎖的活動有關的資訊。該小工具還會顯示每項雲端服務的風險等級。卡巴斯基安全管理中心雲端主控台會從所有受安全政策或設定檔（啟用了該功能）保護的受管理裝置，取得雲端服務使用情況資訊。

使用小工具啟用 Cloud Discovery

Cloud Discovery 功能可讓您向所有受安全政策（啟用了該功能）保護的受管理裝置，取得雲端服務使用情況資訊。僅能對 Kaspersky Endpoint Security for Windows 政策啟用或停用 Cloud Discovery。

有兩種方式啟用 Cloud Discovery 功能：

- 透過使用 Cloud Discovery 小工具。
- 在 Kaspersky Endpoint Security for Windows 政策內容中完成。

  有關如何在 Kaspersky Endpoint Security for Windows 政策內容中啟用 Cloud Discovery 功能的詳細信息，請參閱 Kaspersky Endpoint Security for Windows 幫助的 Cloud Discovery 部分。

請注意，只能在 Kaspersky Endpoint Security for Windows 策略參數中停用 Cloud Discovery 功能。

要能夠啟用 Cloud Discovery，您必須在**一般功能：基本功能**功能區域中具有**寫入**權限。

要使用 Cloud Discovery 小工具啟用 Cloud Discovery 功能：

1. 前往卡巴斯基安全管理中心雲端主控台。
2. 在主功能表中，轉至 **監控和報告 → 控制板**。
3. 在 **Cloud Discovery** 小工具上，點擊**啟用**按鈕。

4. 在開啟的**啟用 Cloud Discovery** 視窗中，選取要啟用該功能的安全政策，然後點擊**啟用**按鈕。
   以下政策設定將自動啟用：**將指令碼注入Web 流量以與網頁互動**、 **Web 工作階段監控**和**加密連線掃描**。

Cloud Discovery 功能已啟用，且小工具已新增至儀表板中。

在儀表板中新增 Cloud Discovery 小工具

您可以在儀表板中新增 **Cloud Discovery** 小工具，以監控受管理裝置上使用雲端服務的情況。

若要能夠在儀表板中新增 Cloud Discovery 小工具，您必須在**一般功能：基本功能**功能區域中具有**寫入**權限。

若要在儀表板中新增 Cloud Discovery 小工具：

1. 前往卡巴斯基安全管理中心雲端主控台。
2. 在主功能表中，轉至 **監控和報告 → 控制板**。
3. 點擊**新增或還原 Web 小部件**按鈕。
4. 在可用小工具的清單中，點擊**其他**類別旁邊的箭頭圖示 (>)。
5. 選取 **Cloud Discovery** 小工具，然後點擊**新增**按鈕。
   如果 Cloud Discovery 功能已停用，請依照使用小工具啟用 Cloud Discovery 部分中的說明進行操作。

所選的小工具即會新增到儀表板的尾端。

檢視雲端服務使用情況資訊

您可以檢視 **Cloud Discovery** 小工具，其中會顯示與嘗試對雲端服務進行的存取活動有關的資訊。該小工具還會顯示每項雲端服務的風險等級。卡巴斯基安全管理中心雲端主控台會從所有受安全政策（啟用了該功能）保護的受管理裝置，取得雲端服務使用情況資訊。

在檢視之前，請確定：

- Cloud Discovery 小工具已新增至儀表板中。
- Cloud Discovery 功能已啟用。
- 您在**一般功能：基本功能**功能區域中具有 **讀取** 權限。

若要檢視 Cloud Discovery 小工具：

1. 前往卡巴斯基安全管理中心雲端主控台。
2. 在主功能表中，轉至 **監控和報告 → 控制板**。
   Cloud Discovery 小工具會顯示在儀表板中。
3. 在 **Cloud Discovery** 小工具的左側，選取雲端服務類別。

小工具右側的表格會顯示所選類別中，最多五項最常為使用者所嘗試存取的服務。所謂的嘗試，同時包括了成功和遭封鎖的嘗試。

4. 在小工具的右側，選取特定服務。

   下方的表格會顯示最多十台最常嘗試存取該服務的裝置。

小工具即會顯示所請求的資訊。

在顯示的小工具中，您可以執行以下操作：

- 前往**監控和報告** → **報告**區段以檢視 Cloud Discovery 報告。
- 封鎖或允許存取所選的雲端服務。

僅當您購買了其中一種 Kaspersky NEXT 產品授權時，Cloud Discovery 功能才可使用。如需詳細資訊，請參閱各種產品授權和其最小裝置數量。

雲端服務的風險等級

對於每項雲端服務，Cloud Discovery 會向您顯示風險等級。風險等級可幫助您判斷不符合您組織安全要求的服務。例如，您在決定是否封鎖對特定服務進行的存取活動時，可以將風險等級納入考慮。

風險等級是一項估計的指數，並未指出任何與雲端服務品質或服務製造商有關的資訊。風險等級純粹為來自 Kaspersky 專家的建議。

在 Cloud Discovery 小工具以及所有受監控雲端服務的清單中，會顯示雲端服務的風險等級。

封鎖對不需要的雲端服務進行的存取活動

對於您不想讓使用者存取的雲端服務，您可以封鎖對這些雲端服務進行的存取活動。您也可以允許對先前封鎖的雲端服務進行存取。

您在決定是否封鎖對特定服務進行的存取活動時，除了其他眾多考量，還可以將風險等級納入考慮。

您可以在安全政策或設定檔中封鎖或允許對雲端服務進行的存取活動。

有兩種方法封鎖對不需要的雲端服務進行的存取活動：

- 透過使用 Cloud Discovery 小工具。

  在這種情況下，您可以逐一封鎖對服務的存取。

- 在 Kaspersky Endpoint Security for Windows 政策內容中完成。

  在這種情況下，您可以逐一封鎖對服務的存取，或一次性封鎖整個類別。

  有關如何在 Kaspersky Endpoint Security for Windows 政策內容中啟用 Cloud Discovery 功能的詳細信息，請參閱 Kaspersky Endpoint Security for Windows 幫助的 Cloud Discovery 部分。

要封鎖或允許透過小工具對雲端服務的存取：

1. 開啟 Cloud Discovery 小工具，然後選取所需的雲端服務。

2. 在**使用服務的前 10 名裝置**面板中，找到要用於封鎖或允許該服務的安全政策或設定檔。

3. 在所需那行的**政策或設定檔中的存取狀態**欄位，執行以下任一操作：

   - 若要封鎖服務，請在下拉清單中選取**已封鎖**。
   - 若要允許服務，請在下拉清單中選取**允許**。

4. 點擊**儲存**按鈕。

安全政策或設定檔即會封鎖或允許對所選服務進行的存取活動。

用戶端裝置的遠端診斷

您可在 Windows 和 Linux 用戶端裝置上遠端執行遠端診斷：

- 啟用和關閉偵錯、變更偵錯等級並下載偵錯檔案
- 下載系統資訊和應用程式設定
- 下載事件記錄
- 為應用程式建立記憶體傾印檔案
- 開始進行診斷並下載診斷報告
- 啟動、停止和重新啟動應用程式

您可以使用從用戶端裝置下載的事件記錄和診斷報告以自行定位問題。同時，若您聯絡 Kaspersky 技術支援，他們可能會請您從用戶端裝置下載偵錯檔案、傾印檔案、事件記錄和診斷報告以讓 Kaspersky 進一步分析。

開啟遠端診斷視窗

若要執行對 Windows 和 Linux 用戶端裝置的遠端診斷，您必須開啟遠端診斷視窗。

開啟遠端診斷視窗：

1. 選取您要開啟遠端診斷視窗的裝置，並執行以下其中一個動作：
   - 若裝置屬於管理群組，請在主功能表中，前往**資產（裝置）→ 群組 → <群組名稱> → 受管理裝置**。
   - 若裝置屬於「未配置的裝置」群組，請在主功能表中，前往**發現和佈署 → 未配置的裝置**。
2. 點擊所需裝置的名稱。
3. 在開啟的裝置內容視窗中，選取**進階**頁籤。
4. 在開啟的視窗中，點擊**遠端診斷**。
   這會開啟用戶端裝置的**遠端診斷** 視窗。如果管理伺服器與用戶端裝置之間並未建立連線，則會顯示錯誤訊息。

或者，如果您需要立即取得某個基於 Linux 的用戶端裝置的所有診斷資訊，您可以在該裝置上執行 collect.sh 指令碼。

啟用與停用應用程式偵錯

您可啟用和停用對應用程式的偵錯，包含 Xperf 偵錯。

啟用和停用偵錯

在遠端裝置上啟用或停用偵錯：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗中，選擇**Kaspersky 應用程式**頁簽。
   在**應用程式管理**區域中，裝置上安裝的卡巴斯基應用程式清單得以顯示。
3. 在應用程式清單上，選取您要啟用或停用偵錯的應用程式。
   遠端診斷選項清單隨即開啟。
4. 若您要啟用偵錯：
   a. 在**偵錯**區域中，點擊**啟用偵錯**。
   b. 在開啟的**修改偵錯等級**視窗中，建議您保留設定的預設值。當需要時，技術支援專家將指導您設定過程。下列設定可用：
      - **偵錯等級**
        偵錯等級定義偵錯檔案包含的詳情資料量。
      - **基於循環的偵錯**
        應用程式覆蓋偵錯資訊以防止偵錯檔案過量增長。指定用於儲存偵錯資訊的檔案最大數量，以及每個檔案的最大大小。如果寫入了最大數量的最大大小的偵錯檔案，最舊的檔案被刪除以便新偵錯檔案可以被寫入。

        此設定僅適用於 Kaspersky Endpoint Security
   c. 點擊**儲存**。

   偵錯會針對選取的應用程式啟用。某些情況下，要啟用偵錯，必須重新啟動安全應用程式及其工作。

   在基於 Linux 的用戶端裝置上，Kaspersky Security Agent 元件更新程式的偵錯由網路代理設定管理。因此，在執行 Linux 的用戶端裝置上，此元件的**啟用偵錯**和**修改偵錯等級**"選項被停用。
5. 若您要停用對選取的應用程式偵錯，請點擊**停用偵錯**。
   系統會針對選取的應用程式停用偵錯。

啟用 Xperf 偵錯

對於 Kaspersky Endpoint Security，技術支援專家可能需求您對系統效能資訊啟用 Xperf 偵錯。

要啟用和配置 Xperf 偵錯或停用它：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗中，選擇**Kaspersky 應用程式**頁簽。
   在**應用程式管理**區域中，裝置上安裝的卡巴斯基應用程式清單得以顯示。
3. 在應用程式清單中，選取 Kaspersky Endpoint Security for Windows。
   適用於 Kaspersky Endpoint Security for Windows 遠端診斷選項的清單隨即顯示。

4. 在**Xperf 偵錯**區域中，點擊**啟用 Xperf 偵錯**。

   若已啟用 Xperf 偵錯，則會改為顯示**停用 Xperf 偵錯**按鈕。如果您想要停用 Kaspersky Endpoint Security for Windows 的 Xperf 偵錯，請點擊此按鈕。

5. 在開啟的**變更 Xperf 偵錯等級**視窗，根據技術支援專員的要求執行以下動作：

   a. 選取以下其中一個偵錯等級：

   - **輕度等級**

     該類型的偵錯檔案包含系統最少量資訊。

     預設情況下已選定此選項。

   - **深度等級**

     相比於*輕度*類型的偵錯檔案，該類型的偵錯檔案包含更多詳細資訊，且可能在*輕度*類型偵錯檔案不足以評估效能時被技術支援專家需求。*深度*偵錯檔案包含關於系統的硬體、作業系統、應用程式的啟動和結束處理程序清單、用於效能評估的事件和來自 Windows System Assessment 工具的事件的技術資訊。

   b. 選取以下其中一個 Xperf 偵錯類型：

   - **基本類型**

     偵錯資訊在 Kaspersky Endpoint Security 應用程式執行期間被接收。

     預設情況下已選定此選項。

   - **重新啟動時類型**

     偵錯資訊在作業系統從受管理裝置上啟動時接收。該偵錯類型在影響系統效能的問題發生時，在裝置被開啟後和 Kaspersky Endpoint Security 啟動之前有效。

   系統可能要求您啟用**循環檔案大小 (MB)**選項，以防止偵錯檔案的過量增長。然後指定偵錯檔案的最大大小。當檔案達到最大大小時，最舊的偵錯資訊被新資訊覆蓋。

   c. 定義輪換檔案大小。

   d. 點擊**儲存**。

   系統會啟用並設定 Xperf 偵錯。

6. 如果您想要停用 Kaspersky Endpoint Security for Windows 的 Xperf 偵錯，請點擊**Xperf 偵錯**區域中的**停用 Xperf 偵錯**。

   Xperf 偵錯已停用。

下載應用程式偵錯檔案

僅當滿足以下其中一項條件時，您才能從用戶端裝置下載偵錯檔案：該裝置的設定中啟用了**不斷開與管理伺服器的連線**選項、正在使用推送伺服器，或是正在使用連線閘道。否則，下載將無法進行。

不斷開與管理伺服器的連線選項所能選取的最大裝置總數是 300。

要下載應用程式的偵錯檔案：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗中，選擇**Kaspersky 應用程式**頁簽。
   在**應用程式管理**區域中，裝置上安裝的卡巴斯基應用程式清單得以顯示。
3. 在應用程式清單中，選取您要為其下載偵錯檔案的應用程式。
4. 在**偵錯**部分中，點擊**偵錯檔案**按鈕。
   這會開啟**裝置偵錯記錄**視窗，其中會顯示偵錯檔案清單。
5. 在偵錯檔案清單中，選取您要下載的檔案。
6. 執行以下操作之一：
   - 點擊**下載**來下載所選檔案。您可以選擇一個或多個檔案進行下載。
   - 下載部分選取的檔案：
     a. 點擊**下載一部分**。
        您無法同時下載多個檔案的部分內容。如果您選擇多個偵錯檔案，**下載一部分**按鈕將被停用。
     b. 在開啟的視窗中，根據您的需求指定要下載的名稱與檔案部分。
        對於基於 Linux 的裝置，無法編輯檔案部分名稱。
     c. 點擊**下載**。

選取的檔案或其部分會下載至您指定的位置。

刪除偵錯檔案

您可刪除不再需要的偵錯檔案。

若要刪除偵錯檔案：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在開啟的遠端診斷視窗中，選擇**事件記錄**頁簽。
3. 在**偵錯檔案**區段中，點擊**Windows Update 記錄**或**遠端安裝記錄**，視您要刪除的偵錯檔案而定。
   這會開啟**裝置偵錯記錄**視窗，其中會顯示偵錯檔案清單。
4. 在偵錯檔案清單中，選取一個或多個您要刪除的檔案。
5. 點擊**移除**按鈕。

選取的偵錯檔案被刪除。

下載應用程式設定

僅當滿足以下其中一項條件時，您才能從用戶端裝置下載應用程式設定：該裝置的設定中啟用了**不斷開與管理伺服器的連線**選項、正在使用推送伺服器，或是正在使用連線閘道。否則，下載將無法進行。

不斷開與管理伺服器的連線選項所能選取的最大裝置總數是 300。

從用戶端裝置下載應用程式設定：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗中，選擇**Kaspersky 應用程式**頁簽。
3. 在**應用程式設定**區段中，點擊**下載**按鈕，下載用戶端裝置上已安裝應用程式設定的資訊。

包含資訊的 ZIP 存檔將被下載到指定位置。

從用戶端裝置下載系統資訊

僅當滿足以下其中一項條件時，您才能從用戶端裝置下載系統資訊到您的裝置：該裝置的設定中啟用了**不斷開與管理伺服器的連線**選項、正在使用推送伺服器，或是正在使用連線閘道。否則，下載將無法進行。

不斷開與管理伺服器的連線選項所能選取的最大裝置總數是 300。

從用戶端裝置下載系統資訊：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗中，選擇**系統資訊**頁簽。
3. 點擊**下載**按鈕可下載有關用戶端裝置的系統資訊。

包含資訊的檔案將下載到指定位置。

下載事件記錄

僅當滿足以下其中一項條件時，您才能從用戶端裝置下載事件記錄到您的裝置：該裝置的設定中啟用了**不斷開與管理伺服器的連線**選項、正在使用推送伺服器，或是正在使用連線閘道。否則，下載將無法進行。

不斷開與管理伺服器的連線選項所能選取的最大裝置總數是 300。

要從遠端裝置下載事件記錄：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗的**事件記錄**頁簽上，點擊**所有裝置記錄**。
3. 在**所有裝置記錄**視窗中，選取多個相關記錄。
4. 執行以下操作之一：

- 點擊**下載整個檔案**來下載所選日誌。
- 下載部分選取的記錄：
  a. 點擊**下載一部分**。
  您無法同時下載多個日誌的部分內容。如果您選擇多個事件記錄，**下載一部分**按鈕將被停用。
  b. 在開啟的視窗中，根據您的需求指定要下載的名稱與記錄部分。
  c. 點擊**下載**。

選取的事件記錄或其部分，會下載至指定的位置。

啟動、停止、重新啟動應用程式

您可在用戶端裝置啟動、停止、重新啟動應用程式。

若要啟動、停止和重新啟動應用程式，請執行以下操作：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗中，選擇**Kaspersky 應用程式**頁簽。
   在**應用程式管理**區域中，裝置上安裝的卡巴斯基應用程式清單得以顯示。
3. 在應用程式清單中，選取您要啟動、停止或重新啟動的應用程式。
4. 點擊以下其中一個按鈕以選取動作：
   - **停止應用程式**
     此按鈕僅在應用程式正在執行時可供使用。
   - **重新啟動應用程式**
     此按鈕僅在應用程式正在執行時可供使用。
   - **啟動應用程式**
     此按鈕僅在應用程式不是正在執行時可供使用。

視您選取的動作而定，系統會啟動、停止或重新啟動應用程式。

若您重新啟動網路代理，系統會顯示訊息表示將失去裝置對管理伺服器的目前連線。

執行應用程式的遠端診斷並下載結果

要為某遠端裝置應用程式啟動診斷並下載其執行結果，請執行以下操作：

1. 開啟用戶端裝置的遠端診斷視窗。
2. 在遠端診斷視窗中，選擇**Kaspersky 應用程式**頁簽。
   在**應用程式管理**區域中，裝置上安裝的卡巴斯基應用程式清單得以顯示。

3. 在應用程式清單中，選取您要執行遠端診斷的應用程式。

   遠端診斷選項清單隨即開啟。

4. 在**診斷報告**區段中，點擊**執行診斷** 按鈕。

   這會啟動遠端診斷程序並產生診斷報告。診斷程序完成時，您就能使用**下載診斷報告**按鈕。

5. 按一下**“ 下載診斷報告”**按鈕下載報告。

報告將下載到指定位置。

在用戶端裝置執行應用程式

您可能需要在用戶端裝置上執行應用程式，若 Kaspersky 支援專家要求您這樣做的時候。您無需在該裝置上安裝該應用程式。您無需在該裝置上安裝該應用程式。

若要在用戶端裝置上執行應用程式：

1. 開啟用戶端裝置的遠端診斷視窗。

2. 在遠端診斷視窗中，選擇**執行遠端應用程式**頁簽。

3. 在**應用程式檔案**部分中，點擊**瀏覽**按鈕以選擇包含要在用戶端裝置上執行的應用程式的 ZIP 存檔。

   > ZIP 存檔必須包含公用程式資料夾。此資料夾包含要在遠端裝置上執行的可執行檔。

   如有必要，您可以指定可執行檔名稱和命令行參數。為此，請填寫**要在遠端裝置上執行的封存中的可執行檔**和**命令列參數**欄位。

4. 點擊**上傳和執行**按鈕以在用戶端裝置上執行指定的應用程式。

5. 請遵循卡巴斯基支援專業人員的指示。

為應用程式建立記憶體傾印檔案

應用程式傾印檔案允許您檢視某個時間點在用戶端裝置上執行的應用程式的參數。該檔案還包含有關為應用程式加載的模組的資訊。

> 產生傾印檔案僅適用於在基於 Windows 的用戶端裝置上執行的 32 位元處理程序。對於執行 Linux 的用戶端裝置和 64 位元處理程序，此功能不受支援。

要為應用程式建立傾印檔案：

1. 開啟用戶端裝置的遠端診斷視窗。

2. 在遠端診斷視窗中，選擇**執行遠端應用程式**頁簽。

3. 在**正在產生處理程序記憶體傾印檔案**區域中，指定要為其產生傾印檔案的應用程式的可執行檔。

4. 點擊**下載**按鈕以儲存指定應用程式的傾印檔案。

   如果指定的應用程式未在用戶端裝置上執行，則會顯示錯誤消息。

在基於 Linux 的用戶端裝置上執行遠端診斷

卡巴斯基安全管理中心雲端主控台可讓您從用戶端裝置下載基本診斷資訊。或者，您可以使用卡巴斯基的 collect.sh 指令碼獲取關於 Linux 裝置的診斷資訊。該指令碼在需要診斷的基於 Linux 的用戶端裝置上執行，然後產生一個檔案，其中包含診斷資訊、該裝置的系統資訊、應用程式的跟踪檔案、裝置日誌以及被緊急終止的應用程式的傾印檔案。

我們建議您使用 collect.sh 指令碼一次性獲取有關 Linux 用戶端裝置的所有診斷資訊。如果是透過卡巴斯基安全管理中心雲端主控台遠端下載診斷資訊，則您需要逐一看完遠端診斷介面的所有區段。此外，Linux 裝置的診斷資訊可能無法完全獲得。

如果您需要將產生的包含診斷資訊的檔案傳送給卡巴斯基技術支援，請在傳送檔案之前刪除所有機密資訊。

要使用 collect.sh 指令碼從基於 Linux 的用戶端裝置下載診斷資訊：

1. 下載 collect.sh 指令碼 封存在collect.tar.gz 存檔中。
2. 將下載的存檔複製到需要診斷的 Linux 用戶端裝置上。
3. 執行以下指令解壓 collect.tar.gz 存檔：

   ```
   # tar -xzf collect.tar.gz
   ```

4. 執行以下指令以指定指令碼執行權限：

   ```
   # chmod +x collect.sh
   ```

5. 使用具有管理員權限的帳戶執行 collect.sh 指令碼：

   ```
   # ./collect.sh
   ```

一個包含診斷資訊的檔案產生並被儲存到 /tmp/$HOST_NAME-collect.tar.gz 資料夾中。

匯出事件到 SIEM 系統

本節將介紹如何配置匯出事件到 SIEM 系統。

情境：設定事件匯出到 SIEM 系統

本節提供了設定從管理伺服器匯出事件到外部 SIEM 系統的情境。將事件資訊匯出到外部 SIEM 系統後，SIEM 的管理員就能對受管理的裝置或裝置群組上發生的安全系統事件快速做出回應。

先決條件

在卡巴斯基安全管理中心雲端主控台中開始為匯出事件進行設定之前：

- 深入了解事件匯出的方法。
- 確保您知道系統設定的值。

您可以按任何順序執行此情境的步驟。

階段

將事件匯出到 SIEM 系統的程序包括以下階段：

- **將 SIEM 系統設定為接收來自卡巴斯基安全管理中心雲端主控台的事件**

  您必須在 SIEM 系統中設定接收來自卡巴斯基安全管理中心雲端主控台的事件。

- **標記要匯出的事件**

  您必須標記要匯出到 SIEM 系統的事件。首先，請標記所有受管理 Kaspersky 應用程式中會發生的一般事件。您可以額外標記特定受管理 Kaspersky 應用程式會發生的事件。

- **將卡巴斯基安全管理中心雲端主控台設定為匯出事件到 SIEM 系統**

  您必須設定卡巴斯基安全管理中心雲端主控台以開始匯出事件到 SIEM 系統。

結果

如果您選取了要匯出的事件，則在設定匯出事件到 SIEM 系統後，您可以檢視匯出結果。

在您開始之前

在卡巴斯基安全管理中心雲端主控台中為自動匯出事件進行設定時，您必須指定 SIEM 系統中的一些設定。建議您事前查看這些設定，為設定卡巴斯基安全管理中心雲端主控台預做準備。

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**

  在卡巴斯基安全管理中心雲端主控台與您的 SIEM 系統伺服器之間建立連線時所用的連接埠號。您需在卡巴斯基安全管理中心雲端主控台設定中和您 SIEM 系統的接收器設定中指定此值。

- **協定**

  從卡巴斯基安全管理中心雲端主控台傳輸訊息到您的 SIEM 系統時所用的通訊協定。您需在卡巴斯基安全管理中心雲端主控台設定中和您 SIEM 系統的接收器設定中指定此值。

關於事件匯出

卡巴斯基安全管理中心雲端主控台可讓您接收管理伺服器和受管理裝置上所安裝 Kaspersky 應用程式的操作事件資訊。事件資訊儲存在管理伺服器資料庫。

您可以將事件匯出用在處理組織和技術級別的安全問題的中心系統中，提供安全監控服務，以及從不同解決方案合併資訊。即是提供對網路硬體和應用程式生成的安全警告的即時分析的 SIEM 系統，或者安全操作中心 (SOCs)。

這些系統可以從許多來源接收資料，包括網路、安全、伺服器、資料庫和應用程式。SIEM 系統也提供功能以集成監控的資料，以便說明您避免遺失關鍵事件。而且，系統執行相關事件和警告的自動分析以通知管理員安全問題。警告可以透過儀表板實現，或可以透過協力廠商管道傳送，例如郵件。

從卡巴斯基安全管理中心雲端主控台匯出事件到外部 SIEM 系統的程序涉及兩個當事方：事件傳送方 (卡巴斯基安全管理中心雲端主控台) 以及事件接收方（SIEM 系統）。若要成功匯出事件，您必須在您的 SIEM 系統和卡巴斯基安全管理中心雲端主控台中進行設定。您可以先設定任意一端。您可以在卡巴斯基安全管理中心雲端主控台中設定傳送事件，並在 SIEM 系統中設定接收事件（執行順序並不重要）。

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 系統必須要收到並正確解析來自卡巴斯基安全管理中心雲端主控台的事件。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。

在 SIEM 系統中設定事件匯出

從 Kaspersky Security Center Cloud Console 匯出事件到外部 SIEM 系統的程序涉及兩個當事方：事件傳送方 (Kaspersky Security Center Cloud Console) 以及事件接收方（SIEM 系統）。您必須在您的 SIEM 系統和卡巴斯基安全管理中心雲端主控台中為匯出事件進行設定。

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雲端主控台傳送的事件，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：

- **連接埠**

  指定連線到卡巴斯基安全管理中心雲端主控台時所用的連接埠號。此連接埠必須與您在卡巴斯基安全管理中心雲端主控台中設定 SIEM 系統時指定的連接埠相同。

- **訊息協定或來源類型**

  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。

訊息接收器

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，用於將訊息內容拆分到相關欄位，例如事件 ID、嚴重等級、描述、參數等等。這可讓 SIEM 系統處理從卡巴斯基安全管理中心雲端主控台收到的事件，以便儲存在 SIEM 系統資料庫中。

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

啟用自動匯出事件後，您必須標記要匯出到外部 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 **資產（裝置）→政策和設定檔**。
2. 點擊您要爲其標記事件的應用程式的政策。
   政策設定視窗隨即開啟。
3. 轉到**事件配置**部分。
4. 選取您要匯出到 SIEM 系統的事件旁邊的核取方塊。
5. 點擊**透過使用 Syslog 標記為匯出到 SIEM 系統**按鈕。

   您還可以在 **事件註冊** 部分中標記匯出到 SIEM 系統的事件，它可透過點擊事件連結開啟。

6. 一個複選標記 (✓) 出現在您標記為匯出到 SIEM 系統的一個或多個事件的欄的 **Syslog** 中。
7. 點擊**儲存**按鈕。

受管理應用程式中的標記事件已準備好匯出到 SIEM 系統。

您可以為特定受管理裝置標記要匯出到 SIEM 系統的事件。如果先前匯出的事件在應用程式的政策中標記過，您將不能為受管理的裝置重新定義標記的事件。

若要為受管理裝置標記要匯出的事件：

1. 在主功能表中，轉至 **資產（裝置）→受管理裝置**。
   受管理裝置清單隨即顯示。
2. 點擊所需裝置名稱在受管理裝置清單中的連結。
   所選裝置的屬性視窗隨即顯示。
3. 轉到**應用程式**區域。
4. 點擊所需應用程式名稱在應用程式清單中的連結。
5. 轉到**事件配置**部分。
6. 選取您要匯出到 SIEM 的事件旁邊的核取方塊。
7. 點擊**透過使用 Syslog 標記為匯出到 SIEM 系統**按鈕。

   此外，您可以在 **事件註冊** 部分中標記匯出到 SIEM 系統的事件，它可透過點擊事件連結開啟。

8. 一個複選標記 (✓) 出現在您標記為匯出到 SIEM 系統的一個或多個事件的欄的 **Syslog** 中。

從現在開始，如果配置了到 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：
   - 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   - 轉到**資產（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。從卡巴斯基安全管理中心雲端主控台匯出事件到外部系統時，使用的是 RFC 5424 標準。

在卡巴斯基安全管理中心雲端主控台中，您可以設定將事件以 Syslog 格式匯出到外部系統。

匯出過程包含兩個步驟：

1. 啟用自動事件匯出。此步驟是要將卡巴斯基安全管理中心雲端主控台設定為傳送事件到 SIEM 系統。卡巴斯基安全管理中心雲端主控台會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。

將卡巴斯基安全管理中心雲端主控台設定為匯出事件到 SIEM 系統

若要將事件匯出到 SIEM 系統，您必須在卡巴斯基安全管理中心雲端主控台中設定匯出程序。

若要在卡巴斯基安全管理中心雲端主控台中設定匯出到 SIEM 系統：

1. 在主功能表中，按一下所需管理伺服器名稱旁邊的設定圖示（ ）。
   管理伺服器內容視窗將開啟。
2. 在**一般**頁籤，選取 **SIEM** 區段。
3. 點擊**設定**連結。
   匯出設定區域將開啟。
4. 在**匯出設定**區域中指定設定：
   - **SIEM 系統伺服器位址**
     安裝了目前使用的 SIEM 系統的伺服器的 IP 位址。在您的 SIEM 系統設定中檢查此值。
   - **SIEM 系統連接埠**
     在卡巴斯基安全管理中心雲端主控台與您的 SIEM 系統伺服器之間建立連線時所用的連接埠號。您需在卡巴斯基安全管理中心雲端主控台設定中和您 SIEM 系統的接收器設定中指定此值。
   - **協定**

若要傳送訊息到 SIEM 系統，您只能使用 TLS over TCP 通訊協定。若要如此做，請指定 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機構 (CA) 接收含有憑證清單的檔案，然後將該檔案上傳到卡巴斯基安全管理中心雲端主控台。卡巴斯基安全管理中心雲端主控台會檢查 SIEM 系統伺服器的憑證是否同樣經受信任的 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雲端主控台中指定 SIEM 系統憑證的 SHA-1 指紋。要新增 SHA-1 指紋，請在**指紋**欄位中輸入它，然後點擊**新增**按鈕。

  > 您可以使用**新增用戶端身分驗證**設定，產生驗證卡巴斯基安全管理中心雲端主控台時所用的憑證。如此一來，您使用的將是由卡巴斯基安全管理中心雲端主控台簽發的自我簽署憑證。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 系統伺服器的網域名稱與 SIEM 系統伺服器憑證的主體名稱不符，則卡巴斯基安全管理中心雲端主控台會無法連線到 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。如有任何指定的主體名稱與 SIEM 系統憑證的主體名稱相符，則卡巴斯基安全管理中心雲端主控台會視 SIEM 系統伺服器憑證為有效。

- **新增用戶端身分驗證**

  在用戶端身分驗證部分，您可以插入您的憑證或是在卡巴斯基安全管理中心雲端主控台中產生憑證。

  - **插入憑證**。您可以使用從任何來源（例如，從任何受信任的憑證頒發機構）收到的憑證。您必須使用以下憑證類型之一指定憑證及其私密金鑰：

    - **X.509 憑證 PEM**。在**包含憑證的檔案**欄位中上傳帶有憑證的檔案，在**包含金鑰的檔案**欄位中上傳帶有私密金鑰的檔案。這兩個檔案互不相依，檔案的載入順序並不重要。當兩個檔案都上傳後，在**密碼或者憑證驗證**欄位中指定解碼私密金鑰的密碼。如果未編碼私密金鑰未編碼，則密碼可以為空值。

    - **X.509 憑證 PKCS12**。上傳包含憑證及其私密金鑰的單個檔案到**包含憑證的檔案**欄位。當兩個檔案都上傳後，在**密碼或者憑證驗證**欄位中指定解碼私密金鑰的密碼。如果未編碼私密金鑰未編碼，則密碼可以為空值。

  - **生產金鑰**。您可以在卡巴斯基安全管理中心雲端主控台中產生自我簽署憑證。卡巴斯基安全管理中心雲端主控台將因此儲存所產生的自我簽署憑證，而您可以將憑證的公開部分或 SHA1 指紋傳遞給 SIEM 系統。

5. 如果需要，您可以從管理伺服器資料庫中匯出封存事件，並設定開始匯出封存事件的開始日期：

   a. 點擊**設定匯出開始日期**連接。

   b. 在開啟的部分中，在**啟動匯出日期自**欄位中指定開始日期。

   c. 點擊**確定**按鈕。

6. 將選項切換到 **自動匯出事件至 SIEM 系統資料庫 已啟用** 位置。

7. 若要檢查 SIEM 系統連線是否設定成功，請點擊**偵測連線**按鈕。

   連線狀態即會顯示。

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。

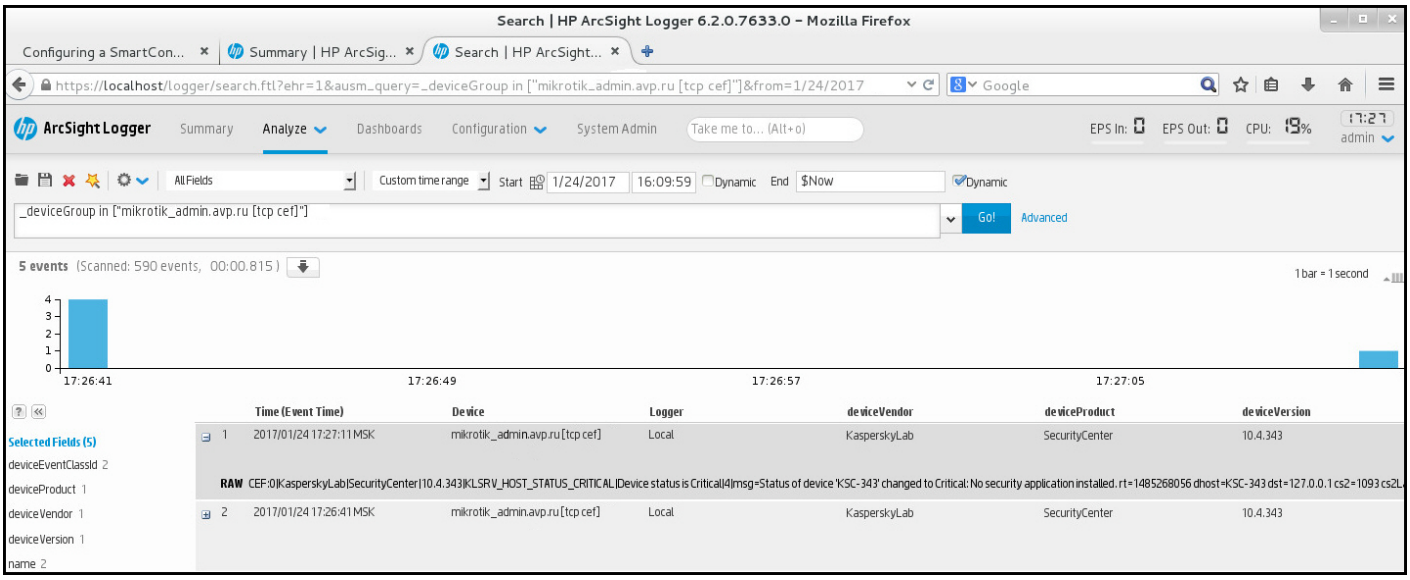
檢視匯出結果

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。

如果您的 SIEM 系統收到來自卡巴斯基安全管理中心雲端主控台的事件並加以正確解析，即表示兩端皆已正確完成設定。否則，請檢查您在卡巴斯基安全管理中心雲端主控台中指定的設定是否與您 SIEM 系統中的設定一致。

下圖顯示匯出到 ArcSight 的事件。例如，第一個事件是緊急的管理伺服器事件：「*Device status is Critical*」。

匯出事件在您 SIEM 系統中的顯示隨您使用的 SIEM 系統而不同。



例子事件

受管理服務提供商 (MSP) 適用的快速入門指南

本快速入門指南旨在供受管理服務提供商 (MSP) 的管理員使用。

卡巴斯基安全管理中心雲端主控台支援多組織用戶。本指南包含管理您客戶（租用戶）的帳戶以及在其裝置上安裝安全應用程式的提示和最佳實務。

關於 Kaspersky Security Center Cloud Console

卡巴斯基安全管理中心雲端主控台是一款由 Kaspersky 架設並維護的應用程式。您無需在自己的電腦或伺服器上安裝卡巴斯基安全管理中心雲端主控台。卡巴斯基安全管理中心雲端主控台可讓管理員將 Kaspersky 安全應用程式安裝到企業網路內的裝置上、遠端執行掃描與更新工作，以及管理受管理應用程式適用的安全政策。管理員可以使用詳細的儀表板，查看企業裝置的狀態快照、詳細報告，以及防護政策中的細項設定。

卡巴斯基安全管理中心雲端主控台的主要功能特色

卡巴斯基安全管理中心雲端主控台可讓您執行以下工作：

- 將 Kaspersky 應用程式安裝到您網路中的裝置並管理所安裝的應用程式。
- 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。
- 建立虛擬管理伺服器並加以排列成階層。
- 保護您的網路裝置，包括工作站和伺服器：
  - 管理以 Kaspersky 應用程式構建的惡意軟體防護系統。
  - 使用偵測和回應（EDR 和 MDR）功能（需有 Kaspersky Endpoint Detection and Response 與/或 Kaspersky Managed Detection and Response 的產品授權），包括：
    - 分析和調查事件
    - 透過建立威脅發展鏈圖表，將事件做視覺化呈現
    - 手動接受或拒絕回應，或是設定自動接受所有回應
- 以多租戶應用程式的形式使用卡巴斯基安全管理中心雲端主控台。
- 遠端管理用戶端裝置上安裝的 Kaspersky 應用程式。
- 以集中化方式將 Kaspersky 應用程式的產品授權金鑰部署到用戶端裝置。
- 為您網路中的裝置建立和管理安全政策。
- 建立和管理使用者帳戶。
- 建立和管理使用者角色 (RBAC)。
- 為您網路裝置上安裝的應用程式建立和管理工作。

- 個別檢視每個用戶端組織的安全系統狀態報告。

關於 MSP 適用的卡巴斯基安全管理中心雲端主控台產品授權

當您開始使用卡巴斯基安全管理中心雲端主控台時，您可以申請試用工作區（在此情況下，您將獲得您工作區中內嵌的 30 天試用產品授權），或是輸入正式產品授權的啟動碼。

您無法將試用工作區轉換為正式工作區。若要在試用產品授權到期後繼續使用卡巴斯基安全管理中心雲端主控台，您必須刪除試用工作區，然後使用正式授權建立另一個工作區。

之後，您可以將一或多個正式產品授權金鑰新增至管理伺服器儲存區。

關於 MSP 適用的偵測和回應功能

卡巴斯基安全管理中心雲端主控台的主控台介面中可以整合其他 Kaspersky 應用程式的功能。例如，您可以整合以下應用程式，以便將偵測和回應功能新增至卡巴斯基安全管理中心雲端主控台的功能中：

- Kaspersky Endpoint Detection and Response Optimum

  Kaspersky Endpoint Detection and Response Optimum 是專為保護組織的 IT 基礎架構免受複雜網路威脅侵害而設計的解決方案。該解決方案的功能將自動偵測威脅以及對這些威脅做出回應的功能相結合，以抵禦複雜的攻擊，包括新的弱點利用、勒索軟體、無檔案攻擊以及取道合法系統工具的方法。

  在 Kaspersky Endpoint Protection Platform (EPP) 應用程式偵測到安全事件後，卡巴斯基安全管理中心雲端主控台中會一張產生含有安全事件詳細重要資料的卡片。事件卡片是由以下其中一種應用程式產生：

  - 隨 Kaspersky EPP 應用程式一起安裝的 Kaspersky Endpoint Agent
  - Kaspersky Endpoint Security 11.7.0 for Windows 或以上版本（已內建 EDR Optimum 功能而無需額外安裝 Kaspersky Endpoint Agent）

  您可以利用事件卡片分析和調查事件。此外，您還可以建立威脅發展鏈圖表，將事件做視覺化呈現。該圖表會及時描述所偵測到攻擊的部署階段。建立的圖表中會包含有關攻擊了涉及哪些模組以及這些模組執行了哪些操作的資訊。

  您也可以發動一連串動作作為回應：為不受信任的物件建立防止執行規則；根據所選的入侵指標 (IOC) 在裝置群組中搜尋類似事件；隔離不受信任的物件；將受感染的裝置自網路隔離。

  如需應用程式的啟動資訊，請參閱 Kaspersky Endpoint Detection and Response Optimum 說明文件。

  如果整合此應用程式，卡巴斯基安全管理中心雲端主控台的介面中即會新增**警示**區段（**監控和報告** → **警示**）。

- Kaspersky Managed Detection and Response

  隨著規避自動化安全屏障的威脅日益增多，Kaspersky Managed Detection and Response 可為苦於尋找專業技術與人員或是內部資源有限的組織，提供全天候的防護。Kaspersky 的 MDR SOC 分析人員或是協力廠商公司會調查事件並提供用於解決事件的回應方式。您可以手動接受或拒絕所提供的措施，或是啟用用於自動接受所有回應的選項。

  如需應用程式的啟動資訊，請參閱 Kaspersky Managed Detection and Response 說明文件。

  如果整合此應用程式，卡巴斯基安全管理中心雲端主控台的介面中會新增**事件**區段（**監控和報告** → **事件**）。

您可以隨時在卡巴斯基安全管理中心雲端主控台的**介面選項**區段，顯示或隱藏引用 Kaspersky Endpoint Detection and Response 或 Kaspersky Managed Detection and Response 功能的介面元素。

開始使用卡巴斯基安全管理中心雲端主控台

完成本節的情境後，卡巴斯基安全管理中心雲端主控台將已可供使用。

開始使用情境

此情境分多個階段進行：

1. **建立帳戶**

   若要開始使用卡巴斯基安全管理中心雲端主控台，您需要有一個帳戶。

   若要建立帳戶：

   1. 開啟您的瀏覽器，然後輸入以下位址：https://ksc.kaspersky.com。
   2. 點擊**創建帳戶**按鈕。
   3. 依照螢幕上的指示進行操作。

2. **建立工作區**

   建立帳戶後，您即可註冊您的公司並建立工作區。

   當您開始使用卡巴斯基安全管理中心雲端主控台時，您可以申請試用工作區（在此情況下，您將獲得您工作區中內嵌的 30 天試用產品授權），或是輸入正式產品授權的啟動碼。

   > 您無法將試用工作區轉換為正式工作區。若要在試用產品授權到期後繼續使用卡巴斯基安全管理中心雲端主控台，您必須刪除試用工作區，然後使用正式授權建立另一個工作區。

   若要註冊公司並建立工作區：

   1. 開啟您的瀏覽器，然後輸入以下位址：https://ksc.kaspersky.com。
   2. 點擊**登入**按鈕。
   3. 依照螢幕上的指示進行操作。

3. **執行卡巴斯基安全管理中心雲端主控台的初始化設定**

   當您首次進入建立的工作區時，系統會自動提示您執行快速啟動精靈。快速啟動精靈會提供引導，讓您只需建立少少的必要工作和政策並調整少少的設定，就能開始建立 Kaspersky 應用程式的安裝套件。依照螢幕上的指示進行操作。

當初始化設定完成時，卡巴斯基安全管理中心雲端主控台即已可供使用。

關於管理您客戶裝置的建議

本節包含將您要保護的客戶裝置進行組織的建議。

適用的建議取決於您是首次使用卡巴斯基安全管理中心雲端主控台，還是已在使用內部部署版本：

- 如果您以前從未使用過卡巴斯基安全管理中心雲端主控台，您有兩個選項：

- 為每個客戶各建立一個虛擬管理伺服器來管理其裝置（建議選項）。在此情況下，每個客戶的裝置都可透過一個獨立於其他客戶的專用虛擬管理伺服器來受到管理。同時，您可以使用主管理伺服器來建立所有客戶共用的政策和工作。主管理伺服器上產生的報告可以納入所有虛擬管理伺服器上的資料。

- 為每個客戶各建立一個管理群組來管理其裝置。如果您想要進一步劃分客戶裝置，可以在每個父群組底下建立從屬管理群組的階層。例如，如果您想要對不同部門員工的裝置使用不同的防護設定，就可以使用從屬群組。

- 如果您已在使用內部部署運作的卡巴斯基安全管理中心雲端主控台，可以將內部部署的卡巴斯基安全管理中心雲端主控台中現有的管理群組和相關物件移轉到卡巴斯基安全管理中心雲端主控台。

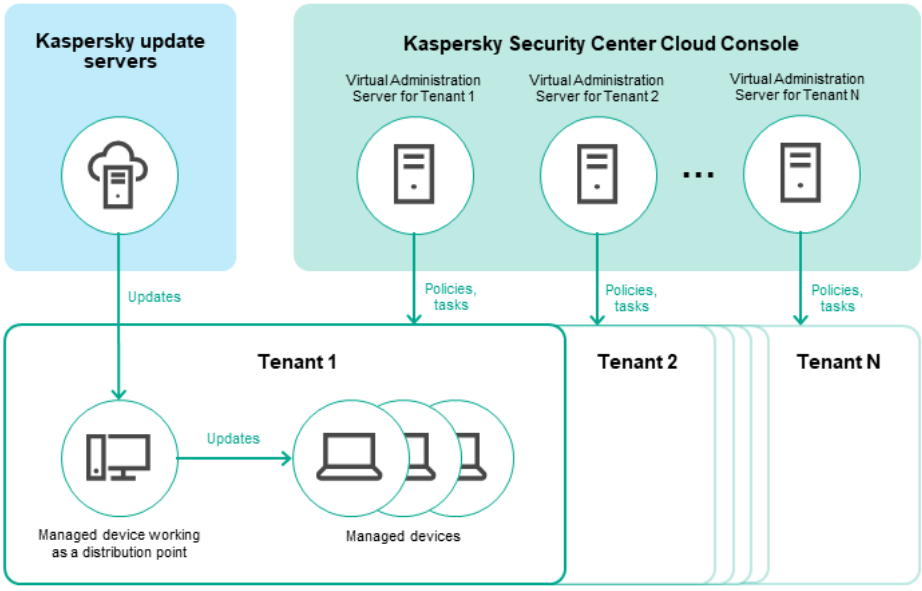
  您無法移轉虛擬管理伺服器。您可以在移轉管理群組和其他物件後，在卡巴斯基安全管理中心雲端主控台中建立虛擬管理伺服器。

  請繼續進行移轉設定。

在主管理伺服器中，虛擬管理伺服器的管理員僅能前往自己的虛擬伺服器。在主管理伺服器上建立的所有物件（例如，小工具、報告或使用者角色），都可供虛擬管理伺服器的管理員讀取。

MSP 一般適用的部署配置

本節說明 MSP 在管理多個租用戶時，通常會採用的部署模式。該模式的基本原理是透過為每個租用戶個別建立的虛擬管理伺服器進行管理。



MSP 適用的典型部署模式

該模式主要包括以下組成元件：

- *卡巴斯基安全管理中心雲端主控台*。提供使用者介面來使用您工作區的管理服務。您是使用卡巴斯基安全管理中心雲端主控台來為用戶端組織的網路部署、管理和維護防護系統。

- *Kaspersky 更新伺服器*。Kaspersky 應用程式可以從 Kaspersky 的 HTTP(S) 伺服器下載資料庫和程式模組更新。

- *虛擬管理伺服器*。MSP 管理員通常會為每個租用戶各建立一個虛擬管理伺服器，藉以為相對應用戶端組織的網路部署、管理和維護防護系統。

- *租用戶*。指需要保護裝置的用戶端組織。

- *受管理裝置*。客戶公司中受卡巴斯基安全管理中心雲端主控台保護的裝置。每個必須保護的裝置都必須安裝網路代理和其中一項 Kaspersky 安全應用程式。

- *作為發佈點來運作的受管理裝置*。指安裝了網路代理的電腦，用以分發更新、輪詢網路、遠端安裝應用程式、取得管理群組（與/或廣播網域）內電腦的資訊。管理員需選取適當的裝置，然後手動將該裝置指派為發佈點。

情境：防護佈署（透過虛擬管理伺服器來管理租用戶）

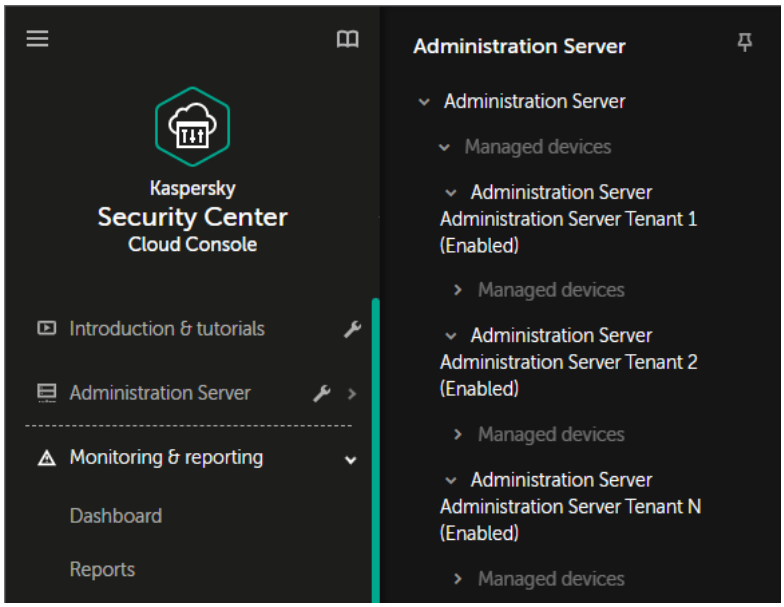
如果您從未使用過卡巴斯基安全管理中心雲端主控台，並且想要透過虛擬管理伺服器管理您的租用戶，請依照本節所述方式進行操作。完成此情境後，您客戶的裝置將已受到保護。

如果您管理多個租用戶，請分別為每個租用戶執行此情境。

此情境分多個階段進行：

1 建立虛擬管理伺服器

為您的客戶建立虛擬管理伺服器。新的虛擬管理伺服器即會出現在管理伺服器階層中：



管理伺服器階層中的虛擬管理伺服器

2 選擇一台要擔任發佈點的裝置

在客戶的裝置當中，決定要一台要擔任發佈點的裝置。

> 一個工作區內的發佈點不能超過 100 個。

3 建立網路代理的獨立安裝套件

切換到建立的虛擬管理伺服器，然後建立網路代理的獨立安裝套件。若要切換管理伺服器，您可以在主功能表中點擊目前管理伺服器名稱右側的箭頭圖示 ( )，然後選取所需的管理伺服器。在建立獨立安裝套件的期間，請指定要將裝置移到的「受管理裝置」管理群組。

4 在所選作為發佈點的裝置上安裝網路代理

您可以使用任何適合您的方法：

- 手動安裝

  為了將獨立安裝套件傳送到裝置上，您可以將套件複製到卸除式磁碟機（例如快閃磁碟機）或是加到共用資料夾中。

- 使用 Active Directory 進行部署

- 使用您的遠端監控和管理 (RMM) 軟體解決方案進行部署

5. **分配發佈點**

   將安裝了網路代理的裝置分配為發佈點。

6. **網路輪詢**

   透過發佈點設定並執行網路輪詢。

   卡巴斯基安全管理中心雲端主控台提供以下網路輪詢方法：

   - IP 範圍輪詢
   - Windows 網路輪詢
   - Active Directory 輪詢

   在依排程完成網路輪詢後，您客戶的裝置將已獲發現並加到**未配置的裝置**群組中。

7. **將發現的裝置移到管理群組**

   設定規則來將自動將發現的裝置移至所需的管理群組，或是手動將這些裝置移至所需的管理群組。如果您計畫在單一管理群組中管理客戶的裝置，可以將裝置移至「受管理裝置」群組。

8. **建立網路代理與受管理 Kaspersky 應用程式的安裝套件**

   下載和建立 Kaspersky 應用程式的安裝套件。

9. **移除協力廠商安全應用程式**

   如果您客戶的裝置上安裝了協力廠商安全應用程式，請先加以移除再安裝 Kaspersky 應用程式。

10. **在用戶端裝置上安裝 Kaspersky 應用程式**

    建立遠端安裝工作來在您客戶的裝置上安裝網路代理和受管理 Kaspersky 應用程式。

    如有必要，您可以建立多個遠端安裝工作來為不同的管理群組或不同的裝置分類安裝受管理 Kaspersky 應用程式。

    待工作建立後，您可對其進行設定。請確保各項工作的排程符合您的需求。安裝網路代理的工作必須先執行。在客戶的裝置上安裝網路代理後，就必須執行安裝受管理 Kaspersky 應用程式的工作。

11. **確認 Kaspersky 應用程式的初始化部署成功**

    產生並檢視 **Kaspersky 軟體版本報告**。請確認您客戶的所有裝置上皆已安裝受管理 Kaspersky 應用程式。

12. **為 Kaspersky 應用程式建立政策**

    為所需的 Kaspersky 應用程式建立政策。如果您想要建立所有客戶都適用的通用政策，請將目前的虛擬管理伺服器切換為主管理伺服器，然後為所需的 Kaspersky 應用程式建立政策。

情境：部署防護（透過管理群組來管理租用戶）

如果您從未使用過卡巴斯基安全管理中心雲端主控台，並且想要透過管理群組管理您的租用戶，請依照本節所述方式進行操作。完成此情境後，您客戶的裝置將已受到保護。

此情境分多個階段進行：

1. **建立管理群組**

   為您每個客戶各建立一個管理群組。

2. **規劃發佈點結構**

   在每個客戶的裝置當中，各決定一台要擔任發佈點的裝置。

   > 一個工作區內的發佈點不能超過 100 個。

3. **建立網路代理的獨立安裝套件**

   建立網路代理的獨立安裝套件。

4. **在所選擔任發佈點的裝置上安裝網路代理**

   在所選擔任發佈點的裝置上安裝網路代理。

   您可以使用任何適合您的方法：

   - 手動安裝

     為了將獨立安裝套件傳送到裝置上，您可以將套件複製到卸除式磁碟機（例如快閃磁碟機）或是放到共用資料夾中。

   - 使用 Active Directory 進行部署
   - 使用您的遠端監控和管理 (RMM) 軟體解決方案進行部署

5. **分配發佈點**

   將安裝了網路代理的裝置分配為發佈點。

6. **網路輪詢**

   透過發佈點設定並執行網路輪詢。

   卡巴斯基安全管理中心雲端主控台提供以下網路輪詢方法：

   - IP 範圍輪詢
   - Windows 網路輪詢
   - Active Directory 輪詢

   在依排程完成網路輪詢後，您客戶的裝置將已獲發現並加到**未配置的裝置**群組中。

7. **將發現的裝置移到管理群組**

   設定規則來將自動將發現的裝置移至所需的管理群組，或是手動將這些裝置移至所需的管理群組。

8. **建立網路代理與受管理 Kaspersky 應用程式的安裝套件**

   如果您並未啟動快速啟動精靈，或是略過了建立安裝套件的步驟，請建立 Kaspersky 應用程式的安裝套件。

9. **移除協力廠商安全應用程式**

如果您客戶的裝置上安裝了協力廠商安全應用程式，請先加以移除再安裝 Kaspersky 應用程式。

10. **在您客戶的裝置上安裝 Kaspersky 應用程式**

    建立遠端安裝工作來在您客戶的裝置上安裝網路代理和受管理 Kaspersky 應用程式。

    如有必要，您可以建立多個遠端安裝工作來為不同的管理群組或不同的裝置分類安裝受管理 Kaspersky 應用程式。

    待工作建立後，您可對其進行設定。請確保各項工作的排程符合您的需求。安裝網路代理的工作必須先執行。在客戶的裝置上安裝網路代理後，就必須執行安裝受管理 Kaspersky 應用程式的工作。

11. **確認 Kaspersky 應用程式的初始化部署成功**

    產生並檢視 **Kaspersky 軟體版本報告**。請確定您客戶的所有裝置上皆已安裝受管理 Kaspersky 應用程式。

12. **為 Kaspersky 應用程式建立政策**

    前往**資產（裝置）** → **群組**功能表；如果您想要建立所有客戶都適用的通用政策，請選取**管理伺服器**。如果您想要為個別客戶建立特定政策，請選取與該客戶相對應的管理群組。為所需的 Kaspersky 應用程式建立政策。

合併運用內部部署的卡巴斯基安全管理中心以及卡巴斯基安全管理中心雲端主控台

如果您已在使用內部部署運作的卡巴斯基安全管理中心雲端主控台，可依本節所述方式，將現有內部部署運作的管理伺服器轉換為您新卡巴斯基安全管理中心雲端主控台管理伺服器的從屬管理伺服器。

設定將內部部署的卡巴斯基安全管理中心雲端主控台以及卡巴斯基安全管理中心雲端主控台合併運用後，除非您刪除管理伺服器階層，否則無法從內部部署的卡巴斯基安全管理中心雲端主控台移轉到卡巴斯基安全管理中心雲端主控台。

若要建立管理伺服器階層，請

將您現有內部部署運作的管理伺服器新增為從屬管理伺服器。

MSP 適用的 Kaspersky 應用程式產品授權

卡巴斯基安全管理中心雲端主控台可讓您以集中化方式將 Kaspersky 應用程式的產品授權金鑰分發到您客戶的裝置上、監控其使用情況，以及續訂產品授權。

如果您管理多個租用戶，可透過以下方式分發產品授權金鑰：

- 向所有租用戶分發同一個產品授權金鑰。
- 向每個租用戶分發個別的產品授權金鑰。

若要將產品授權金鑰分發到您客戶的裝置上：

1. 將所需的產品授權金鑰新增到管理伺服器儲存區中。
2. 執行以下操作之一：
   - 設定自動分發產品授權金鑰。

在此情況下，卡巴斯基安全管理中心雲端主控台會選取一個適用的產品授權金鑰，然後在每次發現新裝置時都自動部署該產品授權金鑰。

- 設定「新增金鑰」工作以將產品授權金鑰分發到裝置。

  設定工作時，您需選取必須部署到裝置上的授權金鑰，然後選取所需裝置位於的管理群組。

  一個工作僅能分發一個產品授權金鑰。這表示，如果您想要分發多個產品授權金鑰，您必須為每個產品授權金鑰各建立一個工作。

客戶裝置上安裝的 Kaspersky 應用程式即已啟動。

MSP 適用的監控和報告功能

卡巴斯基安全管理中心雲端主控台會為您提供監控和報告功能。這些功能會提供關於您組織基礎架構、防護狀態和統計資訊的總覽。

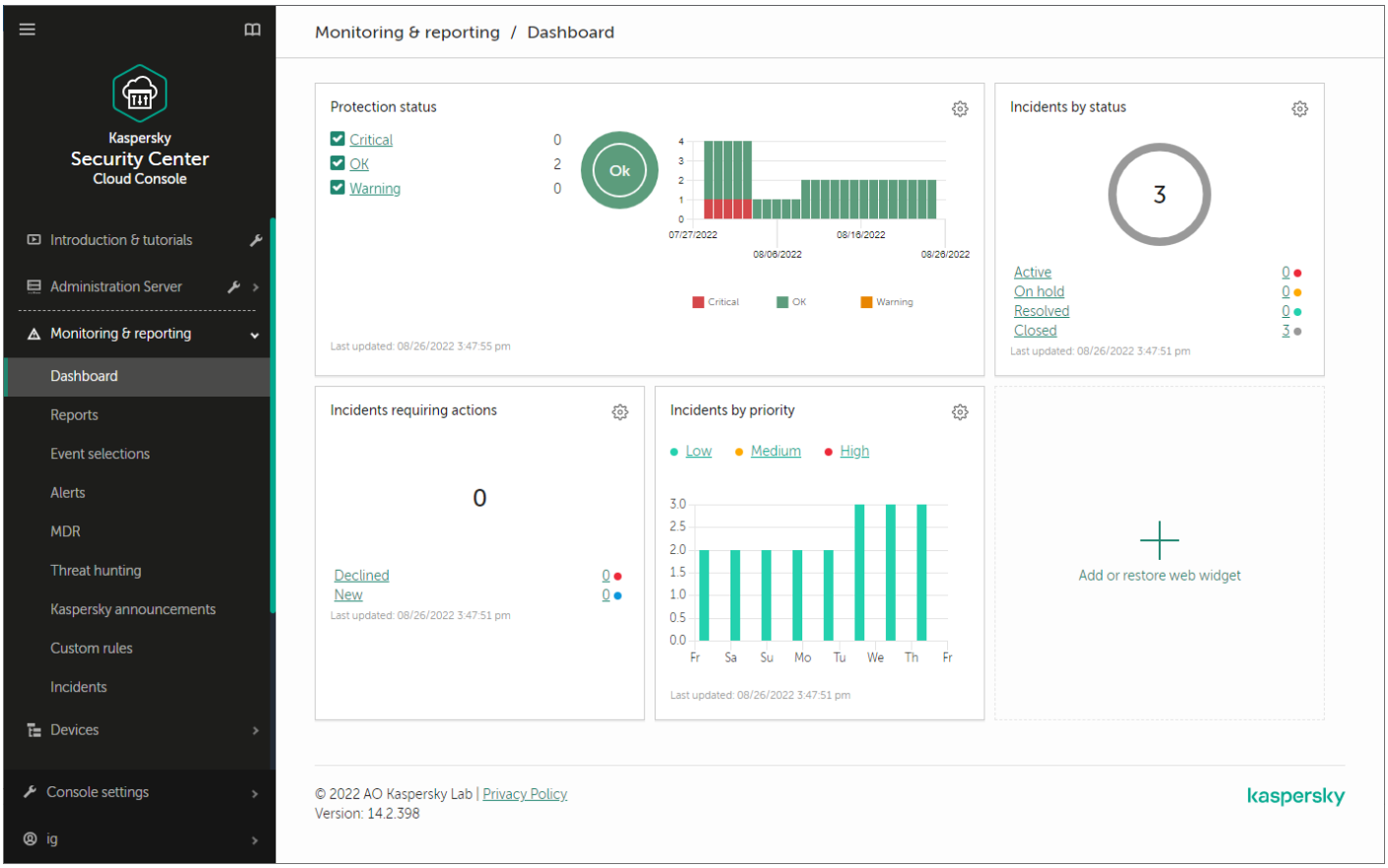
部署卡巴斯基安全管理中心雲端主控台之後，您可以根據您的需要來設定監控和報告功能。

卡巴斯基安全管理中心雲端主控台會提供以下類型的監控和報告功能：

- 儀表板
- 報告
- 事件分類
- 電子郵件通知

儀表板

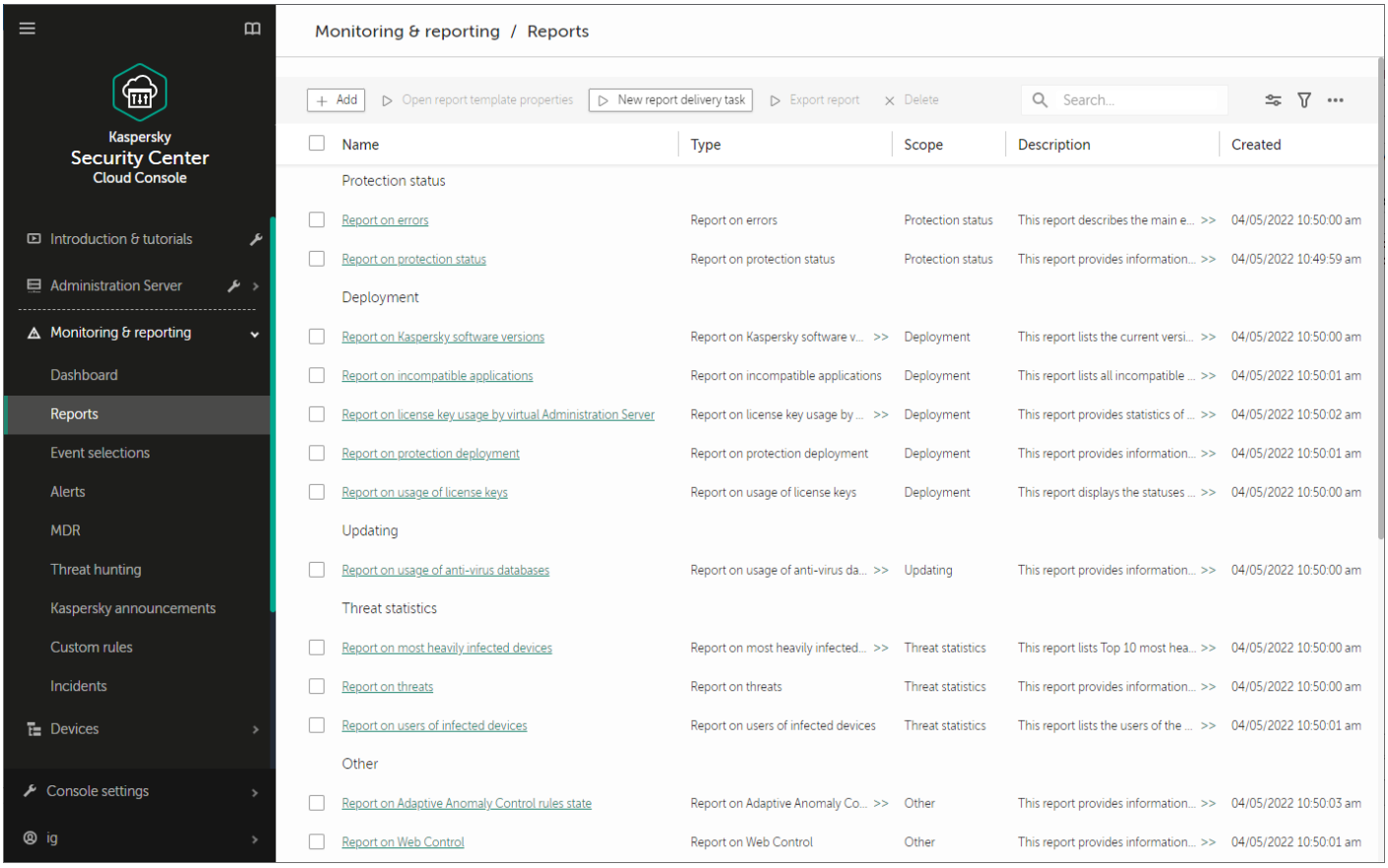
儀表板會為您提供資訊圖表（請參閱下圖），讓您能夠監控您組織網路中的安全趨勢。



「儀表板」區段

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。您也可以排定透過電子郵件傳送報告（請參閱下圖）。



事件分類

事件選項提供從管理伺服器資料庫中選取的事件的命名集合的螢幕視圖。卡巴斯基安全管理中心雲端主控台中包含一些預先定義的事件分類（例如，**最近事件**和**緊急事件**）。您也可以建立自訂事件分類。

電子郵件通知

您可以為卡巴斯基安全管理中心雲端主控台中和您客戶裝置上發生的事件，設定電子郵件通知。

在雲端環境中使用卡巴斯基安全管理中心雲端主控台

本節會為卡巴斯基安全管理中心雲端主控台當中與在雲端環境（例如 Amazon Web Services、Microsoft Azure 或 Google Cloud）中部署和維護卡巴斯基安全管理中心雲端主控台相關的功能，提供相關資訊。

若要在雲端環境中作業，您需要特殊產品授權。如果您並無這類產品授權，則介面中與雲端裝置相關的元素將不供操作。

雲端環境中的產品授權選項

卡巴斯基安全管理中心雲端主控台在試用模式和正式模式下，皆可於雲端環境中運作：

- 在試用模式下，所有雲端環境功能在您工作區的整個有效期間都可供使用。無需有任何產品授權。
- 在正式模式下，僅當管理伺服器內容中已新增作用中的 Kaspersky Hybrid Cloud Security 產品授權金鑰時，雲端環境功能才可供使用。

在這兩種情況下，弱點和修補程式管理都會自動啟動。

嘗試使用 Kaspersky Hybrid Cloud Security 的產品授權啟動雲端環境的功能支援時，可能會發生錯誤。

準備透過 Kaspersky Security Center Cloud Console 在雲端環境中運作

本節介紹如何準備在以下雲端環境中使用卡巴斯基安全管理中心雲端主控台：

- Amazon Web Services
- Microsoft Azure
- Google Cloud

使用 Amazon Web Services 雲端環境

本節介紹如何準備在 Amazon Web Services 中使用卡巴斯基安全管理中心雲端主控台。

本文件中引用的網頁位址在卡巴斯基安全管理中心雲端主控台發佈之日是正確的。

關於使用 Amazon Web Services 雲端環境

若要使用 AWS 平台，特別是建立實例，您需要有 Amazon Web Services 帳戶。您可以在 https://aws.amazon.com/tw/ 建立免費帳戶。您也可以使用現有 Amazon 帳戶。

關於更多 AMI 和 AWS Marketplace 如何工作的詳情，請存取 AWS Marketplace 說明頁面。對於更多使用 AWS 平台、使用實例和相關概念的資訊，請參考 Amazon Web Services 檔案。

本文件中引用的網頁位址在卡巴斯基安全管理中心雲端主控台發佈之日是正確的。

為 Amazon EC2 實例建立 IAM 使用者帳戶

本節說明為了確保卡巴斯基安全管理中心雲端主控台正確運作，所必須執行的操作。這些操作包括使用 AWS Identity and Access Management (IAM) 使用者帳戶。還敘述了為了在用戶端裝置上安裝網路代理和 Kaspersky Security for Windows Server 以及 Kaspersky Endpoint Security for Linux 而必須執行的操作。

確保卡巴斯基安全管理中心雲端主控台對 AWS 具有使用權限

若要在 Amazon Web Services 雲端環境中使用卡巴斯基安全管理中心雲端主控台，您必須建立 *IAM 使用者帳戶*，卡巴斯基安全管理中心雲端主控台將透過該帳戶使用 AWS 服務。在開始使用管理伺服器之前，建立帶有 *AWS IAM 存取金鑰*（也叫 *IAM 存取金鑰*）的 IAM 使用者帳戶。

要建立 IAM 角色或 IAM 使用者帳戶，就需要使用 AWS 管理主控台。要使用 AWS 管理主控台，您將需要 AWS 帳戶的使用者名稱和密碼。

建立搭配卡巴斯基安全管理中心雲端主控台使用的 IAM 使用者帳戶

您需要有 IAM 使用者帳戶來供卡巴斯基安全管理中心雲端主控台使用。您可以建立帶有所有必要權限的 IAM 使用者帳戶，或者您可以建立兩個不同的使用者帳戶。

系統會自動為 IAM 使用者建立 *IAM 存取金鑰*，而您將需要在初始化設定期間向卡巴斯基安全管理中心雲端主控台提供該金鑰。IAM 存取金鑰由存取金鑰 ID 和金鑰組成。關於更多 IAM 服務的詳情，請參考以下 AWS 參考頁面：

- https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html。
- https://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2。

要建立帶有必要權限的 IAM 使用者帳戶：

1. 開啟 AWS 管理主控台並使用您的帳戶登入。
2. 在 AWS 服務清單中，選取 **IAM**。
   包含使用者名稱清單和工具使用功能表的視窗開啟。
3. 在使用者帳戶相關區域導航，並新增新使用者名稱或名字。
4. 對於新增的使用者，指定以下 AWS 內容：
   - 存取類型：**程式設計存取**。
   - 未設定權限邊界。
   - 權限：**ReadOnlyAccess**。
     新增權限後，請檢視該權限是否新增正確。一旦選取錯誤，返回上一個介面並再次做出選取。

5. 您建立使用者帳戶後，包含新 IAM 使用者的 IAM 存取金鑰的表格將出現。存取金鑰 ID 顯示在**存取金鑰 ID** 列。金鑰以星號顯示在**秘密存取金鑰**列。要檢視金鑰，點擊**顯示**。

新建立的帳戶顯示在對應於您的 AWS 帳戶的 IAM 使用者帳戶清單。

本文件中引用的網頁位址在卡巴斯基安全管理中心雲端主控台發佈之日是正確的。

工作在 Microsoft Azure 雲端環境

本節會為提供有關在 Microsoft Azure 提供的雲端環境中操作和維護卡巴斯基安全管理中心雲端主控台的資訊，以及有關將防護佈署到該雲端環境中的虛擬機器上的詳細資訊。

關於使用 Microsoft Azure

要使用 Microsoft Azure 平台，特別是要在 Azure Marketplace 購買應用並建立虛擬機，您將需要一個 Azure 訂購。開始在卡巴斯基安全管理中心雲端主控台中使用 Microsoft Azure 之前，請先建立一個 Azure 應用程式 ID 並讓其具有在虛擬機器上安裝應用程式時所需的權限。

建立訂購、應用程式 ID 和密碼

若要在 Microsoft Azure 環境中使用卡巴斯基安全管理中心雲端主控台，您需要有一份 Azure 訂購、Azure 應用程式 ID 和 Azure 應用程式密碼。您可以使用現有訂購，如果您已經擁有。

Azure 訂購授予其所有者到 Microsoft Azure Platform Management Portal 和 Microsoft Azure 服務的存取權限。所有者可以使用 Microsoft Azure Platform 以管理服務，例如 Azure SQL 和 Azure Storage。

要建立 Microsoft Azure 訂購，

轉到https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/create-subscription並按照那裡的說明進行操作。

關於建立訂購的更多資訊在 Microsoft 網站 可用。您將會得到訂購 ID，而您稍後要將其連同應用程式 ID 和密碼一起提供給卡巴斯基安全管理中心雲端主控台。

要建立和儲存 Azure 應用程式 ID 和密碼，

1. 轉到 https://portal.azure.com 並確保您已登入。
2. 遵照 reference page 的說明，建立您的應用程式 ID。
3. 轉到應用程式設定的**金鑰**區域。
4. 在**金鑰**區域，填充**敘述**和**過期**欄位並置**參數值**欄位為空。
5. 點擊**儲存**。

當您點擊**儲存**，系統自動使用一個長字元序列填充**參數值**欄位。該序列是您的 Azure 應用程式密碼（例如，yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QlfFvdU=）。敘述在您輸入時被顯示。

6. 將密碼複製下來並儲存起來，以便您稍後可以在卡巴斯基安全管理中心雲端主控台中提供應用程式 ID 和密碼。

   您僅可以在密碼被建立時複製它。稍後，密碼不再被顯示且您無法還原它。

本文件中引用的網頁位址在卡巴斯基安全管理中心雲端主控台發佈之日是正確的。

分配角色到 Azure 應用程式 ID

如果您僅想使用裝置發現偵測虛擬機，您的 Azure 應用程式 ID 必須具有閱讀者角色。如果您不僅要偵測虛擬機器，還想透過 Azure API 部署防護，則您的 Azure 應用程式 ID 必須具有虛擬機參與者角色。

按照 Microsoft 網站上的說明分配角色到您的 Azure 應用程式 ID。

在 Google 雲端中使用

本節會為在 Google 提供的雲端環境中使用卡巴斯基安全管理中心雲端主控台提供相關資訊。

您可以透過 Google API，在 Google Cloud 平台中使用卡巴斯基安全管理中心雲端主控台。您需要有 Google 帳戶。如需詳細資訊，請參閱 https://cloud.google.com 上的 Google 文件。

您將需要建立以下憑證並提供給卡巴斯基安全管理中心雲端主控台：

- **用戶端電子郵件**

  輸入您用來在 Google Cloud 註冊專案的電子郵件。

- **專案 ID**

  專案 ID 是您在 Google Cloud 註冊專案時收到的 ID。

- **私密金鑰**

  私密金鑰是您在 Google Cloud 註冊專案時作為私密金鑰收到的字元序列。您可能會想要複製並貼上此序列，以免出錯。

Kaspersky Security Center Cloud Console 中的雲端環境設定精靈

若要使用該精靈設定卡巴斯基安全管理中心雲端主控台，您必須具備以下項目：

- 以下為適用於雲端環境的特定憑證：

- 有權輪詢雲端區段的 IAM 使用者帳戶（用於 Amazon Web Services）
- Azure 應用程式 ID、密碼和訂閱（搭配 Microsoft Azure 使用）
- Google 用戶端電子郵件、Project ID 與私密金鑰（搭配 Google Cloud 使用）

- 安裝套件：
  - Windows 網路輪詢
  - Linux 網路輪詢
  - Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Linux 的 Web 外掛程式
- 至少以下一項：
  - Kaspersky Endpoint Security for Windows 的安裝套件和 Web 外掛程式（建議）
  - Kaspersky Security for Windows Server 的安裝套件和 Web 外掛程式

如果您的工作區是以 Kaspersky Hybrid Cloud Security 產品授權建立，則首次連線到卡巴斯基安全管理中心雲端主控台時，會自動啟動雲端環境設定精靈。您還可以在任意時刻手動啟動雲端環境設定精靈。

要手動啟動雲端環境設定精靈：

在主功能表中，前往**發現和佈署 → 佈署和分配 → 設定雲端環境**。

精靈隨即啟動。

此精靈的平均連線時間是約 15 分鐘。

步驟 1：檢查需要的外掛程式和安裝套件

如果您擁有下面列出的所有必要 Web 外掛程式和安裝套件，則不會顯示此步驟。

要設定雲端環境，您必須具有以下元件：

- 安裝套件：
  - Windows 網路輪詢
  - Linux 網路輪詢
  - Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Linux 的 Web 外掛程式
- 至少以下一項：

- Kaspersky Endpoint Security for Windows 的安裝套件和 Web 外掛程式（建議）
- Kaspersky Security for Windows Server 的安裝套件和 Web 外掛程式

  我們建議您使用 Kaspersky Endpoint Security for Windows 而不是 Kaspersky Security for Windows Server。

卡巴斯基安全管理中心雲端主控台會自動偵測到您已有的元件，而僅列出缺少的元件。按一下**選擇要下載的應用程式**按鈕，然後選擇需要的外掛程式和安裝套件，來下載列出的元件。下載元件後，您可以使用**重新整理**按鈕更新缺少的元件清單。

步驟 2：選取應用程式啟動方式

僅當您是使用 Kaspersky Hybrid Cloud Security 以外的其他產品授權建立工作區，而您從未將 Kaspersky Hybrid Cloud Security 產品授權金鑰新增到管理伺服器的啟動欄位時，才會顯示此步驟。在此情況下，您必須使用 Kaspersky Hybrid Cloud Security 產品授權來啟動管理伺服器。

步驟 3：選取雲端環境與授權

指定下列設定：

- **雲端環境**

  選取您要將卡巴斯基安全管理中心雲端主控台部署於的雲端環境：AWS、Azure 或 Google Cloud。

  若您不只一個雲端環境中工作，請選取一個環境接著再次執行精靈。

- **連線名稱**

  輸入連線名稱。名稱不能包括 256 個以上字元。僅允許 Unicode 字元。

  該名稱也將用作雲端裝置的管理群組名稱。

  若您計畫處理多個雲端環境，您可能想要在連線名稱中納入環境名稱，例如「Azure 區段」、「AWS 區段」或「Google 區段」。

輸入憑證以接收您指定之雲端環境的驗證。

AWS

若您選取 AWS 作為雲端區段類型，請使用 AWS IAM 存取金鑰來進一步輪詢雲端區段。請輸入以下金鑰資料：

- **存取金鑰 ID**

  IAM 存取金鑰 ID 是個字母數字序列。當您在建立 IAM 使用者帳戶時接收金鑰 ID。

  在您選取 AWS IAM 存取金鑰進行授權後，此欄位即可供使用。

- **金鑰**

您建立 IAM 使用者帳戶時接收到的帶有存取金鑰 ID 的金鑰。

金鑰的字元顯示為星號。在您開始輸入金鑰後，**顯示**按鈕被顯示。按一下並按住該按鈕一定時間以檢視輸入的字元。

在您選取 AWS IAM 存取金鑰進行授權後，此欄位即可供使用。

若要檢視您輸入的字元，請按住**顯示**按鈕。

Azure

如果您選取了 Azure 作為雲端區段類型，請為將來輪詢雲端區段所使用的連線指定以下設定：

- **Azure 應用程式 ID**

  您在 Azure 網站建立了該應用程式 ID。

  您僅可以提供一個 Azure 應用程式 ID 用於輪詢和其他目的。如果您要輪詢其他 Azure 段，您必須先刪除現有 Azure 連線。

- **Azure 訂購 ID**

  您在 Azure 網站建立了該訂購。

- **Azure 應用程式密碼**

  當您建立應用程式 ID 時您收到應用程式 ID 的密碼。

  密碼的字元顯示為星號。在您開始輸入密碼後，**顯示**按鈕可用。按一下並按住該按鈕以檢視您輸入的字元。

  若要檢視您輸入的字元，請按住**顯示**按鈕。

- **Azure 儲存帳戶名稱**

  您建立了要搭配卡巴斯基安全管理中心雲端主控台使用之 Azure 儲存帳戶的名稱。

- **Azure 儲存存取金鑰**

  您在建立要搭配卡巴斯基安全管理中心雲端主控台使用的 Azure 儲存帳戶時收到了密碼（金鑰）。

  金鑰在“Azure 儲存帳戶概述”區域可用，在“金鑰”子區域。

  若要檢視您輸入的字元，請按住**顯示**按鈕。

Google Cloud

如果您選取了 Google Cloud 作為雲端區段類型，請為將來輪詢雲端區段所使用的連線指定以下設定：

- **用戶端電子郵件地址**

輸入您用來在 Google Cloud 註冊專案的電子郵件。

- **項目 ID**

  專案 ID 是您在 Google Cloud 註冊專案時收到的 ID。

- **私密金鑰**

  私密金鑰是您在 Google Cloud 註冊專案時作為私密金鑰收到的字元序列。您可能會想要複製並貼上此序列，以免出錯。

  若要檢視您輸入的字元，請按住**顯示**按鈕。

您指定的連線會儲存在應用程式設定。

雲端環境設定精靈僅能讓您指定一個區段。之後，您可以指定更多的連線以管理其他雲端區段。

點擊**下一步**繼續。

步驟 4：輪詢區段並設定與雲端同步

此步驟會啟動雲端區段輪詢，並自動為雲端裝置建立一個特別的管理群組。裝置中發現的實例會放置在此群組。此外，還會設定雲端區段輪詢排程（預設為每 5 分鐘一次，您之後可變更此設定）。

與雲端同步自動移動規則也被建立。之後每次掃描雲端網路時，系統都會將偵測到的虛擬裝置移到**受管理裝置\雲端**群組內相對應的子群組。

定義**與雲端結構同步管理群組**設定。

如果啟用該選項，**雲端**群組被自動建立在**受管理裝置**群組，雲端裝置發現被啟動。在每個雲端網路掃描中偵測到的實例和虛擬機被放置到雲端群組。該群組的管理子群組結構比對您的雲端區段結構（在 AWS 中，可用網域和放置群組不出現在結構中；在 Azure 中，子網路不出現在結構中）。未被識別為雲端環境中實例的裝置在**未配置的裝置**群組。此群組結構可讓您使用群組安裝工作，將病毒防護應用程式安裝到實例上，以及為不同群組設定不同的政策。

如果停用該選項，**雲端**群組也被建立，且雲端裝置發現也被啟動；然而，比對雲端區段結構的子群組不在群組中被建立。所有偵測到的實例都在**雲端**管理群組，因此顯示在單一清單。如果您在 Kaspersky Security Center Cloud Console 中的操作需要同步，可以修改**Synchronize with Cloud**規則的內容並加以強制執行。強加該規則改變雲端群組的子群組結構，以便比對您雲端區段的結構。

預設情況下已停用該選項。

點擊**下一步**繼續。

步驟 5：選擇一個應用程式來為其建立政策和工作

僅當您同時擁有 Kaspersky Endpoint Security for Windows 和 Kaspersky Security for Windows Server 的安裝套件和外掛程式時才會顯示此步驟。如果您只有其中一個應用程式的外掛程式和安裝套件，則會略過此步驟，而卡巴斯基安全管理中心雲端主控台會為現有應用程式建立政策和工作。

選取您要為其建立政策和工作的應用程式：

- Kaspersky Endpoint Security for Windows
- Kaspersky Security for Windows Server

步驟 6：設定適用於卡巴斯基安全管理中心雲端主控台的卡巴斯基安全網路

在試用模式下或在虛擬管理伺服器上執行卡巴斯基安全管理中心雲端主控台時，會略過此步驟。

請指定關於是否將卡巴斯基安全管理中心雲端主控台操作資訊轉發到卡巴斯基安全網路 (KSN) 知識庫的設定。您可以選取以下其中一個方法：

- **我同意使用卡巴斯基安全網路**

  用戶端裝置上安裝的 Kaspersky Security Center Cloud Console 與受管理應用程式會自動將其操作詳細資訊傳輸至卡巴斯基安全網路。參與卡巴斯基安全網路確保了包含病毒和其他威脅的資料庫的快速更新，該資料庫確保了對緊急安全威脅的快速回應。

- **我不同意使用卡巴斯基安全網路**

  Kaspersky Security Center Cloud Console 和受管理應用程式不會提供資訊給卡巴斯基安全網路。

  若您選取此選項，則會停用卡巴斯基安全網路。

Kaspersky 建議您參與卡巴斯基安全網路。

受管理應用程式的 KSN 協議也會隨即顯示。若您同意使用卡巴斯基安全網路，受管理應用程式會將資料傳送至 Kaspersky。若您不同意參與卡巴斯基安全網路，受管理應用程式不會將資料傳送至 Kaspersky。您之後可在應用程式政策中變更此設定。

點擊**下一步**繼續。

步驟 7：建立初始保護設定

您可以檢查建立的政策和工作清單。

等候建立政策與工作完成後，接著點擊**下一步**。在精靈的最後一頁上，點擊**完成**按鈕退出。

透過卡巴斯基安全管理中心雲端主控台輪詢網路區段

與網路結構（和該網路所含裝置）有關的資訊是透過使用 AWS API、Azure API 或 Google API 工具定期輪詢雲端區段而得。卡巴斯基安全管理中心雲端主控台會使用這些資訊來更新「未配置的裝置」和「受管理裝置」資料夾的內容。如果您配置了裝置自動移動到管理群組，偵測到的裝置將被包含在管理群組中。

若要能夠輪詢雲端區段，您的 IAM 使用者帳戶（在 AWS 中）、應用程式 ID 與密碼（在 Azure 中）或是 Google 用戶端電子郵件、Google 專案 ID 與私密金鑰（在 Google Cloud 中）必須提供了相對應的權限。

您可以新增或刪除連線，以及為每個雲端區段設定輪詢排程。

新增透過卡巴斯基安全管理中心雲端主控台輪詢雲端區段時所需的連線

要新增雲端區段輪詢連線到可用連線清單：

1. 在主功能表中，前往**發現和佈署** → **發現** → **雲端**。
2. 在開啟的視窗中，點擊**內容**。
3. 在開啟的**設定**視窗中，點擊**新增**按鈕。
   雲端區段設定視窗開啟。
4. 為將來輪詢雲端區段所使用的連線指定雲端環境名稱：
   - **雲端環境**

     選取要部署 Kaspersky Security Center Cloud Console 的雲端環境：AWS、Azure 或 Google Cloud。
     若您不只一個雲端環境中工作，請選取一個環境接著再次執行精靈。
   - **連線名稱**

     輸入連線名稱。名稱不能包括 256 個以上字元。僅允許 Unicode 字元。
     該名稱也將用作雲端裝置的管理群組名稱。
     若您計畫處理多個雲端環境，您可能想要在連線名稱中納入環境名稱，例如「Azure 區段」、「AWS 區段」或「Google 區段」。
5. 輸入憑證以接收您指定之雲端環境的驗證。
   - 若您選取了 AWS，請指定以下項目：
     - **存取金鑰 ID**

       IAM 存取金鑰 ID 是個字母數字序列。當您在建立 IAM 使用者帳戶時接收金鑰 ID。
       在您選取 AWS IAM 存取金鑰進行授權後，此欄位即可供使用。
     - **金鑰**

       您建立 IAM 使用者帳戶時接收到的帶有存取金鑰 ID 的金鑰。
       金鑰的字元顯示為星號。在您開始輸入金鑰後，**顯示**按鈕被顯示。按一下並按住該按鈕一定時間以檢視輸入的字元。
       在您選取 AWS IAM 存取金鑰進行授權後，此欄位即可供使用。

       若要檢視您輸入的字元，請按住**顯示**按鈕。

- 若您選取了 Azure，請指定下列設定：

  - **Azure 應用程式 ID**

    您在 Azure 網站建立了該應用程式 ID。

    您僅可以提供一個 Azure 應用程式 ID 用於輪詢和其他目的。如果您要輪詢其他 Azure 段，您必須先刪除現有 Azure 連線。

  - **Azure 訂購 ID**

    您在 Azure 網站建立了該訂購。

  - **Azure 應用程式密碼**

    當您建立應用程式 ID 時您收到應用程式 ID 的密碼。

    密碼的字元顯示為星號。在您開始輸入密碼後，**顯示**按鈕可用。按一下並按住該按鈕以檢視您輸入的字元。

    若要檢視您輸入的字元，請按住**顯示**按鈕。

  - **Azure 儲存帳戶名稱**

    您建立了要搭配卡巴斯基安全管理中心雲端主控台使用之 Azure 儲存帳戶的名稱。

  - **Azure 儲存存取金鑰**

    您在建立要搭配卡巴斯基安全管理中心雲端主控台使用的 Azure 儲存帳戶時收到了密碼（金鑰）。

    金鑰在"Azure 儲存帳戶概述"區域可用，在"金鑰"子區域。

    若要檢視您輸入的字元，請按住**顯示**按鈕。

若您選取了 Google Cloud，請指定下列設定：

- **用戶端電子郵件地址**

  輸入您用來在 Google Cloud 註冊專案的電子郵件。

- **項目 ID**

  專案 ID 是您在 Google Cloud 註冊專案時收到的 ID。

- **私密金鑰**

  私密金鑰是您在 Google Cloud 註冊專案時作為私密金鑰收到的字元序列。您可能會想要複製並貼上此序列，以免出錯。

  若要檢視您輸入的字元，請按住**顯示**按鈕。

6. 如有需要，請點擊**設定輪詢排程**接著變更預設設定。

該連線儲存在應用程式設定。

第一次輪詢新雲端區段後，與該段對應的子群組會出現在**受管理裝置\雲端**管理群組。

如果您指定不正確的憑證，在雲端區段輪詢過程中將不會發現實例，且新子群組將不會出現在**受管理裝置\雲端**管理群組。

為雲端區段輪詢刪除連線

如果您不再必須輪詢特定雲端區段，您可以從可用連線清單刪除對應的連線。您還可以刪除連線，如果，例如輪詢雲端區段的權限被轉移給另一個帶有不同憑證的使用者。

要刪除連線：

1. 在主功能表中，前往**發現和佈署 → 發現 → 雲端**。
2. 在開啟的視窗中，點擊**內容**。
3. 在開啟的**設定**視窗中，點擊要刪除之區段的名稱。
4. 點擊**刪除**。
5. 在開啟的視窗中，點擊**確定**按鈕以確認您的選取。

連線已刪除。對應此連線的雲端區段中的裝置會自動從管理群組中刪除。

設定透過卡巴斯基安全管理中心雲端主控台進行輪詢的排程

雲端區段輪詢依據排程執行。您可以設定輪詢頻率。

雲端環境設定精靈會自動將輪詢頻率設定為 5 分鐘。您可以在任意時刻變更該值並設定不同的排程。不過，不建議您設定比每 5 分鐘一次還要頻繁的輪詢頻率，因為這可能會導致 API 運作錯誤。

要設定雲端區段輪詢排程：

1. 在主功能表中，前往**發現和佈署 → 發現 → 雲端**。
2. 在開啟的視窗中，點擊**內容**。
3. 在開啟的**設定**視窗中，點擊要配置輪詢排程的區段名稱。

   雲端區段設定視窗開啟。
4. 在**雲端區段設定**視窗中，點擊**設定輪詢排程**按鈕。

   排程視窗即會開啟。
5. 在**排程**視窗，指定以下設定：

- **排程開始**

  輪詢排程選項：

  - **每 N 天**

    輪詢定期執行，按照指定天數間隔，從指定的日期和時間開始。
    預設下，輪詢每天執行一次，從目前系統日期和時間開始。

  - **每 N 分鐘**

    輪詢定期執行，按照指定分鐘間隔，從指定的時間開始。
    預設下，輪詢每五分鐘執行一次，從目前系統時間開始。

  - **周中天數**

    輪詢定期執行，在指定星期的指定時間。
    預設下，輪詢會每週五下午 6:00:00 執行。

  - **每個月所選週的指定日**

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

- **開始間隔（天）**

  指定 N 等於的值（分鐘或延遲）。

- **開始於**

  指定要完成初次輪群的時間。

- **執行錯過的工作**

  如果您的工作區在排定的輪詢時間無法使用，卡巴斯基安全管理中心雲端主控台可在工作區恢復可用後立即啟動輪詢，或是等下個排定的輪詢時間再啟動輪詢。
  如果啟用此選項，則卡巴斯基安全管理中心雲端主控台會在工作區恢復可用後立即開始輪詢。
  如果停用此選項，則卡巴斯基安全管理中心雲端主控台會等下個排定的輪詢時間再啟動輪詢。
  預設情況下已啟用該選項。

6. 點擊**Save**以儲存變更。

區段的輪詢排程隨即配置並儲存。

檢視透過 Kaspersky Security Center Cloud Console 輪詢雲端區段的結果

您可檢視雲端區段輪詢的結果，意即檢視受管理伺服器管理的雲端裝置清單。

要檢視雲端區段輪詢結果：

在主功能表中，前往**發現和佈署 → 發現 → 雲端**。

可供輪詢的雲端區段即會顯示。

透過卡巴斯基安全管理中心雲端主控台檢視雲端裝置的內容

您可以檢視每一個雲端裝置的內容。

若要檢視雲端裝置內容：

1. 在主功能表中，轉至 **資產（裝置）→ 受管理裝置**。
2. 點擊您要檢視內容的裝置名稱。
   內容視窗開啟，**一般**區域被選中。
3. 若您想檢視特定的雲端裝置內容，請在內容視窗中選擇**系統**區域。
   隨即會視裝置的雲端平台來顯示內容。
   對於 AWS 中的裝置，會顯示以下內容：
   - **使用 API** (值：**AWS**) 發現的裝置
   - **雲端區域**
   - **雲端 VPC**
   - **雲端可用性區域**
   - **雲端子網路遮罩**
   - **雲端位置群組** (此單元只會在實例屬於位置群組時顯示；否則，它將不會顯示)

   對於 Azure 中的裝置，會顯示以下內容：
   - **使用 API** (值：**Microsoft Azure**) 發現的裝置
   - **雲端區域**
   - **雲端子網路**

   對於 Google Cloud 中的裝置，會顯示以下內容：
   - **使用 API** (值：**Google Cloud**) 發現的裝置

- **雲端區域**
- **雲端 VPC**
- **雲端可用性區域**
- **雲端子網路遮罩**

與雲端同步：設定移動規則

在雲端環境設定精靈操作中，與雲端同步規則被自動建立。此規則可讓您自動將每次輪詢時偵測到的裝置從「未配置的裝置」群組移到「受管理裝置」\「雲端」群組，使這些裝置可受到集中化管理。預設下，規則在建立後被啟動。您可以在任意時刻停用、修改或強制規則。

要編輯與雲端同步規則的內容和/或強制規則：

1. 在主功能表中，前往**發現和佈署** → **佈署和分配** → **移動規則**。
   移動規則清單即會開啟。
2. 在移動規則的清單中，選取**與雲端同步**。
   規則內容視窗隨即開啟。
3. 如有需要，請在**規則條件**頁籤的**雲端區段**頁籤中指定以下設定：

- **裝置在雲端區段中**

  該規則僅套用到位於所選雲端區段的裝置。否則，該規則套用到發現的所有裝置。
  預設情況下已選定此選項。

- **包含子物件**

  該規則套用到所選段和其所有嵌套雲端子區域中的所有裝置。否則，該規則僅套用到位於根段的裝置。
  預設情況下已選定此選項。

- **從嵌套物件移動裝置到對應子群組**

  如果啟用該選項，嵌套物件的裝置將被自動移動到對應其結構的子群組。
  如果停用該選項，嵌套物件的裝置將被自動移動到雲端子群組的根，而不再分支。
  預設情況下已啟用該選項。

- **建立對應於新偵測到裝置的容器的子群組**

如果啟用此選項，則當**受管理裝置\雲端**群組的結構中沒有與該裝置所在的區段相對應的子群組時，卡巴斯基安全管理中心雲端主控台會建立相對應的子群組。例如，如果一個子網在裝置發現中被發現，帶有相同名稱的新組將在**受管理裝置\雲端**群組下被建立。

如果停用此選項，則卡巴斯基安全管理中心雲端主控台不會建立任何新的子群組。例如，如果一個子網在網路輪詢中被發現，帶有相同名稱的新群組將不在**受管理裝置雲端**群組下被建立，且該子群組中的裝置將被移動到**受管理裝置雲端**群組。

預設情況下已啟用該選項。

- **刪除在雲端區段中未找到比對的子群組**

  如果啟用該選項，應用程式從雲端群組刪除所有不比對任何現有雲端物件的子群組。

  如果停用該選項，未比對任何現有雲端物件的子群組被保留。

  預設情況下已啟用該選項。

若您在使用雲端環境設定精靈時啟用了**與雲端結構同步管理群組**選項，則會建立**與雲端同步**規則並啟用**建立對應於新偵測到裝置的容器的子群組**與**刪除在雲端區段中未找到比對的子群組**選項。

若您不啟用**與雲端結構同步管理群組** 選項，**與雲端同步**規則會在這些選項停用（未核取）時建立。如果您在卡巴斯基安全管理中心雲端主控台中的操作需要**受管理裝置\雲端**子群組中的子群組結構符合雲端區段的結構，請在規則內容中啟用**建立對應於新偵測到裝置的容器的子群組**與**刪除在雲端區段中未找到比對的子群組**選項，然後強制執行該規則。

4. 在**使用 API 發現的裝置**下拉清單，選取以下值之一：

   - **否**。裝置無法以 AWS、Azure 或 Google API 偵測到，意即裝置是位於雲端環境外，或是位於雲端環境中但無法以 API 偵測到。
   - **AWS**。裝置使用 AWS API 發現，就是，裝置在 AWS 雲端環境中。
   - **Azure**。裝置使用 Azure API 發現，就是，裝置在 Azure 雲端環境中。
   - **Google Cloud**。裝置是以 Google API 發現到，意即裝置絕對是位於 Google 雲端環境中。
   - 沒有值。該標準無法被套用。

5. 如果必要，在其他區域設定其他規則內容。

移動規則隨即配置完成。

將應用程式遠端安裝到 Azure 虛擬機

您必須擁有有效產品授權，才能安裝應用程式到 Microsoft Azure 虛擬機。

卡巴斯基安全管理中心雲端主控台支援以下情境：

- 用戶端裝置會透過 Azure API 探索；安裝也會透過 API 執行。使用 Azure API 意味著您只能安裝以下應用程式：
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Windows

- Kaspersky Security for Windows Server

- 用戶端裝置會透過 Azure API 探索；安裝則透過發佈點執行，如果沒有發佈點，則使用獨立安裝套件手動進行。您可以透過這種方式安裝卡巴斯基安全管理中心雲端主控台支援的任何應用程式。

若要在 Azure 虛擬機上建立遠端安裝應用程式工作：

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

   新工作精靈啟動。
3. 遵照精靈的說明：

   a. 選擇**遠端安裝應用程式**作為工作類型。

   b. 在**安裝套件**頁面上，選擇**Microsoft Azure API 的遠端安裝**。

   c. 選擇存取裝置的帳戶時，請使用現有的 Azure 帳戶，或請按一下**新增**並輸入 Azure 帳戶的憑據：

   - **Azure 帳戶名稱**

     為您指定的憑證輸入任何名稱。此名稱將會顯示在要執行該工作的帳戶清單中。

   - **Azure 應用程式 ID**

     您在 Azure 網站建立了該應用程式 ID。

     您僅可以提供一個 Azure 應用程式 ID 用於輪詢和其他目的。如果您要輪詢其他 Azure 段，您必須先刪除現有 Azure 連線。

   - **Azure 應用程式密碼**

     當您建立應用程式 ID 時您收到應用程式 ID 的密碼。

     密碼的字元顯示為星號。在您開始輸入密碼後，**顯示**按鈕可用。按一下並按住該按鈕以檢視您輸入的字元。

   d. 從**受管理裝置\雲端**群組中選擇相關裝置。

在精靈結束後，應用程式遠端安裝工作會顯示在工作清單中。

變更 Kaspersky Security Center Cloud Console 介面的語言

您可以選取卡巴斯基安全管理中心雲端主控台介面的語言。

要變更介面語言：

1. 在主功能表中，轉至**設定** → **語言**。
2. 選擇一種受支援的當地語係化語言。

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雲端主控台說明文件或任何關於卡巴斯基安全管理中心雲端主控台的資訊來源中找到問題的解決方案，請聯絡 Kaspersky 技術支援中心。技術支援專家將會回答您所有的卡巴斯基安全管理中心雲端主控台安裝與使用問題。

Kaspersky 僅會為生命週期尚未結束的卡巴斯基安全管理中心雲端主控台提供支援（請參閱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 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。

Kaspersky 技術支援專家會需要的資訊

當您聯絡 Kaspersky 技術支援專家時，他們可能會要求您提供以下資訊：

- 關於卡巴斯基安全管理中心雲端主控台的一般資訊
- 工作區 ID
- 產品授權資訊
- 已安裝的應用程式數量
- 租用戶 ID 與狀態

您可以在**帳戶功能表 → 技術支援**區段找到這些資訊。請複製並分享這些資訊，以針對您的問題獲得協助。

有關程式的資訊來源

Kaspersky 網站上的卡巴斯基安全管理中心雲端主控台頁面

在 Kaspersky 網站上的卡巴斯基安全管理中心雲端主控台頁面，您可以檢視關於應用程式及其功能與特性的一般資訊。

知識庫中的卡巴斯基安全管理中心雲端主控台頁面

*知識庫*是 Kaspersky 技術支援網站的一部分。

在知識庫中的卡巴斯基安全管理中心雲端主控台頁面，您可以閱讀文章來瞭解關於如何購買、安裝和使用應用程式的實用資訊、建議與常見問題解答。

知識庫中的文章可能會針對與卡巴斯基安全管理中心雲端主控台和其他 Kaspersky 應用程式相關的問題提供解答。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雲端主控台具有一些對應用程式的運作並無大礙的限制：

- 當您匯入*「將更新下載到發佈點儲存庫」*或*「更新驗證」*工作時，將啟用**「選擇工作將被指派到的裝置」**選項。這些工作不能被指派給裝置分類或特定裝置。如果將*下載更新指派到發佈點儲存庫*或將*更新驗證*工作指派到特定裝置，則工作將無法正確匯入。

- 嘗試將對 Linux 裝置完成*清查掃描*工作後得到的檔案傳送給 Kaspersky 進行分析時，會傳回錯誤。

- 如果您嘗試使用 Active Directory 同盟服務 (ADFS) 登入卡巴斯基安全管理中心雲端主控台，但缺少所需權限，則卡巴斯基安全管理中心雲端主控台仍會傳回「無效憑證」錯誤，而非警告使用者缺少權限。

- 「管理裝置」工作無法對執行 macOS 的裝置正常運作。

- 在「遠端診斷」視窗中點擊**下載整個檔案**按鈕時，可能會無法正常下載。

詞彙表

Amazon EC2 實例

使用 Amazon Web Service 基於 AMI 映像建立的虛擬機。

Amazon 系統映像 (AMI)

範本包含執行虛擬機必要的軟體設定。多個實例可以基於單個 AMI 建立。

AWS Application Program Interface (AWS API)

卡巴斯基安全管理中心雲端主控台所用的 AWS 平台應用程式開發介面。具體來說，AWS API 工具是作為輪詢雲端區段之用。

AWS IAM 存取金鑰

包含金鑰 ID（「AKIAIOSFODNN7EXAMPLE」樣式）和金鑰（「wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY」樣式）的組合。這對屬於 IAM 使用者並用於獲取對 AWS 服務的存取。

AWS 管理主控台

檢視和管理 AWS 資源的 Web 介面。AWS 管理主控台在 https://aws.amazon.com/tw/console/ 可用。

HTTPS

在網路瀏覽器和網路伺服器之間使用加密傳送資料的安全通訊協定。HTTPS 用於存取受限制的資訊，如企業或財務資料。

IAM 使用者

AWS 服務使用者。IAM 使用者可能具有執行雲端區段輪詢的權限。

IAM 角色

請求 AWS 服務的權限設定。IAM 角色不關聯於特定使用者或群組；它們提供不帶 AWS IAM 存取金鑰的存取權限。您可以分配 IAM 角色到 IAM 使用者、EC2 實例和 AWS 應用程式或服務。

JavaScript

一種對網頁功能進行擴充的程式語言。使用 JavaScript 建立的網頁無需使用來自網路伺服器的新資料更新網頁即可執行功能（例如，變更介面元素的圖示或開啟附加視窗）。要檢視使用 JavaScript 建立的頁面，請在您的瀏覽器的設定中啟用 JavaScript 支援。

Kaspersky 更新伺服器

Kaspersky 應用程式可以從 Kaspersky 的 HTTP(S) 伺服器下載資料庫和程式模組更新。

SSL

網際網路和本機網上的使用的資料加密協定。Secure Sockets Layer (SSL) 協定用在網路應用程式中，以便在用戶端和伺服器之間建立安全的連線。

UEFI 防護裝置

在 BIOS 層級整合了 Kaspersky Anti-Virus for UEFI 的裝置。整合的防護從系統啟動時開始確保裝置安全，未整合軟體的裝置僅在安全應用程式啟動後開始防護工作。

不相容應用程式

指不支援透過卡巴斯基安全管理中心雲端主控台來管理的協力廠商病毒防護應用程式或 Kaspersky 應用程式。

事件儲存區

管理伺服器資料庫中的一塊部分，專門用於儲存卡巴斯基安全管理中心雲端主控台中所發生事件的資訊。

事件嚴重等級

在 Kaspersky 程式操作過程中遇到的事件的內容。有以下嚴重等級：

- 緊急事件
- 功能失效
- 警告
- 資訊

根據事件發生時的情況，相同類型的事件可能具有不同的嚴重等級。

修補程式重要等級

修補程式內容。有五個 Microsoft 修補程式和協力廠商修補程式的嚴重等級：

- 緊急
- 高
- 中等
- 低等
- 未知

協力廠商修補程式或 Microsoft 修補程式的嚴重等級由修補程式需要修補的弱點的最不利的嚴重等級決定。

備用訂購金鑰

程式已驗證可使用，但是目前還未使用的金鑰。

卡巴斯基安全管理中心雲端主控台上的帳戶

您在設定 Kaspersky Security Center Cloud Console 時（例如，新增和移除使用者帳戶以及設定安全設定檔（安全政策）時），必須具有的帳戶。該帳戶可讓您使用我的卡巴斯基服務。您是在開始使用卡巴斯基安全管理中心雲端主控台時建立該帳戶。

卡巴斯基安全管理中心雲端主控台操作者

指透過卡巴斯基安全管理中心雲端主控台來監視受管理防護系統之狀態與運作的使用者。

卡巴斯基安全管理中心雲端主控台管理員

指透過卡巴斯基安全管理中心雲端主控台遠端集中管理系統來管理應用程式運作的人員。

卡巴斯基安全網路 (KSN)

一種雲端服務基礎架構，可提供對 Kaspersky 資料庫的存取，其中包含持續更新的檔案、網路資源和軟體信譽資訊。卡巴斯基安全網路確保在遇到未知威脅時 Kaspersky 應用程式能夠做出更快速的回應，提高某些防護元件的效能並降低誤報的可能性。

卡巴斯基私有安全網路（KPSN）

私有卡巴斯基安全網路允許已安裝 Kaspersky 應用程式裝置的使用者，存取卡巴斯基安全網路信譽資料庫和其他統計資料，而不從他們的裝置傳送資料到卡巴斯基安全網路。私有卡巴斯基安全網路用於由於以下原因無法參與卡巴斯基安全網路的企業客戶：

- 裝置未連線到網際網路。
- 傳輸任何資料到國家/地區以外或企業區域網路以外被法律或企業安全政策禁止。

受管理裝置

安裝了網路代理的電腦，或是安裝了 Kaspersky 安全應用程式的行動裝置。

可用更新

Kaspersky 應用程式模組的一組更新，包括在特定期間內積累的重大更新。

安裝套件

一組檔案，專為使用卡巴斯基安全管理中心雲端主控台遠端管理系統來遠端安裝 Kaspersky 程式而建立。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。

工作區

為特定公司建立的卡巴斯基安全管理中心雲端主控台實例。當客戶建立工作區時，Kaspersky 會建立並設定所需的基礎架構和雲端型管理主控台來管理公司裝置上安裝的安全應用程式。

工作設定

對於每個工作類型的特別應用程式設定。

廣播網域

網路的一個邏輯區域，在這裡所有節點可以使用廣播通道在 OSI 層 (Open Systems Interconnection Basic Reference Model) 交換資料。

弱點

作業系統或應用程式存在的弱點，惡意軟體研發者會利用這種弱點入侵系統或應用程式並破壞其完整性。系統中的大量弱點會使系統不安全，因為能夠入侵系統的病毒會導致系統或其所安裝的應用程式發生執行故障。

強制安裝

遠端安裝 Kaspersky 應用程式的方法，允許您安裝軟體到指定用戶端裝置。為了成功完成強制安裝，用於執行該工作的帳戶必須具有足夠的權限，以便在用戶端裝置上遠端啟動應用程式。該方法建議用於安裝應用程式到執行 Microsoft Windows 作業系統並支援該功能的裝置。

應用程式標籤

對協力廠商應用程式加上的標籤，可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的條件。

指定裝置的工作

從任意管理群組分配給一批用戶端裝置並且在那些裝置上執行的工作。

授權檔案

帶有 .key 副檔名的檔案，可以用來以試用或正式產品授權使用 Kaspersky 應用程式。

政策

政策決定應用程式設定並管理應用程式在管理群組中電腦上的配置。必須為每個應用程式都建立單獨的政策。您可以為安裝在每個管理群組中之電腦的應用程式建立多個政策，但是對於管理群組中的每個應用程式，一次只能套用一個政策。

政策設定檔

已命名的政策設定子集。此子集會隨政策一起分發到目標裝置上，並依特殊條件（稱為設定檔啟動條件）輔助政策執行。

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。

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。

病毒活動臨界值

在特定時間內指定類型事件的最大允許數量，當超過該數量時，程式將把其解釋為病毒活動增加並看做是一種病毒爆發。該功能在病毒爆發期間很重要，因為它使管理員能夠即時對病毒攻擊威脅做出反應。

病毒爆發

使裝置感染病毒的一系列蓄意嘗試。

病毒資料庫

包含 Kaspersky 已知的電腦安全威脅資訊。病毒資料庫中的項目使得惡意程式碼在被掃描物件中被偵測。病毒資料庫由 Kaspersky 專家建立並且每小時都會更新。

發佈點

指安裝了網路代理的電腦，用以分發更新、輪詢網路、遠端安裝應用程式、取得管理群組（與/或廣播網域）內電腦的資訊。管理員需選取適當的裝置，然後手動將該裝置分配為發佈點。

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 Web 外掛程式

為了能透過卡巴斯基安全管理中心雲端主控台來遠端管理 Kaspersky 軟體，而使用的一種特殊元件。管理外掛程式是一種讓 Kaspersky Security Center Cloud Console 與特定 Kaspersky 應用程式相互銜接的介面。使用管理外掛程式，您可以配置應用程式工作和政策。

管理伺服器

卡巴斯基安全管理中心雲端主控台的一個元件，用於集中儲存企業網路中所安裝一切 Kaspersky 應用程式的相關資訊。它也可用於管理這些應用程式。

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雲端主控台的一個元件，讓管理伺服器與特定網路節點（工作站或伺服器）上安裝的 Kaspersky 應用程式之間能夠互動。該元件是公司內所有 Microsoft® Windows® 應用程式的通用元件。對於為類 Unix OS 和 macOS 開發的 Kaspersky 應用程式，分別有不同版本的網路代理。

網路病毒防護

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雲端主控台的一個元件，專為管理個別用戶端組織網路的防護系統而設計。

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：

- 虛擬管理伺服器僅能作為從屬管理伺服器。
- 虛擬管理伺服器不支援建立從屬管理伺服器（包括虛擬伺服器）。

裝置所有者

裝置所有者就是管理員需要在裝置上執行操作時可以聯絡的使用者。

裝置標記

對裝置加上的標籤，可用於分組、說明或尋找裝置。

身分和存取管理 (IAM)

啟用了使用者到其他 AWS 服務和資源的存取管理的 AWS 服務。

身分驗證代理

允許您完成存取已加密硬碟磁碟機的身分驗證和在可啟動磁碟機加密後載入作業系統的介面。

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

指使用卡巴斯基安全管理中心雲端主控台提供的服務來安裝 Kaspersky 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。

防護狀態

目前防護狀態，反映了電腦安全等級。

隔離

一個特殊的檔案儲存區，用於存放疑似感染病毒或是在被偵測到時無法被解毒的檔案。

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

指使用卡巴斯基安全管理中心雲端主控台中提供的管理服務來遠端管理應用程式。

有關協力廠商代碼的資訊

legal_notices.txt 檔案中會包含協力廠商程式碼的相關資訊。

Network Agent for Windows 和 Network Agent for Linux 的安裝資料夾中亦會有該 legal_notices.txt 檔案。

如需工作區所用協力廠商程式碼的額外資訊，請參閱 Kaspersky Endpoint Security Cloud 說明文件。

商標聲明

註冊商標及服務標誌均為其各自所有人的財產。

Adobe、Acrobat、Flash、PostScript、Reader、Shockwave 是 Adobe 在美國和/或其他國家/地區的註冊商標或商標。

AMD64 是 Advanced Micro Devices, Inc. 的商標或註冊商標。

Amazon、Amazon EC2、Amazon Web Services、AWS 和 AWS Marketplace 是 Amazon.com, Inc. 或其附屬公司的商標。

Apache 是 Apache Software Foundation 的註冊商標或商標。

Apple、App Store、AppleScript、FileVault、iPhone、iTunes、Mac、Mac OS、macOS、OS X、Safari 和 QuickTime 是 Apple Inc. 的商標。

Arm 是 Arm Limited（或其子公司）在美國和/或其他地方的註冊商標。

Bluetooth 註冊商標和服務標誌皆為 Bluetooth SIG, Inc. 所有。

Ubuntu、LTS 是 Canonical Ltd 的註冊商標。

Cisco、IOS、Cisco Jabber 是 Cisco Systems, Inc. 和/或其附屬公司在美國和其他特定國家/地區的註冊商標或商標。

Citrix 和 XenServer 是 Citrix Systems, Inc. 和/或其附屬公司在美國專利及商標局和其他國家的註冊商標。

Cloudflare、Cloudflare 標誌和 Cloudflare Workers 是 Cloudflare, Inc. 在美國和其他司法管轄區的商標和/或註冊商標。

Corel 和 CorelDRAW 是 Corel Corporation 和/或其子公司在加拿大、美國和/或其他國家/地區的商標或註冊商標。

Dropbox 是 Dropbox, Inc. 的商標。

Radmin 是 Famatech 的註冊商標。

Firebird 是 Firebird Foundation 的註冊商標。

Foxit 是 Foxit Corporation 的註冊商標。

FreeBSD 是 FreeBSD foundation 的註冊商標。

Google、Android、Chrome、Dalvik、Firebase、Google Chrome、Google Earth、Google Maps、Google Play、Google Public DNS 是 Google LLC 的商標。

EulerOS 是華為技術有限公司的商標。

Intel 和 Core 是 Intel Corporation 在美國和/或其他國家/地區的商標。

IBM 和 QRadar 是 International Business Machines Corporation 在全球眾多司法管轄區的註冊商標。

Node.js 是 Joyent, Inc. 的商標。

Linux 是 Linus Torvalds 在美國和其他國家/地區的註冊商標。

Logitech 是 Logitech 在美國和/或其他國家/地區的註冊商標或商標。

Microsoft、Active Directory、ActiveSync、ActiveX、BitLocker、Excel、Hyper-V、InfoPath、Internet Explorer、Microsoft Edge、MS-DOS、MultiPoint、Office 365、OneNote、Outlook、PowerPoint、PowerShell、Segoe、Skype、SQL Server、Tahoma、Visio、Win32、Windows、Windows Azure、Windows Media、Windows Mobile、Windows Phone、Windows Server、and Windows Vista 是 Microsoft 集團公司的商標。

CVE 是 MITRE Corporation 的註冊商標。

Mozilla、Firefox、Thunderbird 是 Mozilla Foundation 在美國和其他國家/地區的商標。

Novell 是 Novell Enterprises Inc. 在美國和其他國家/地區的註冊商標。

NetWare 是 Novell Inc. 在美國和其他國家/地區的註冊商標。

Oracle、Java、JavaScript 是 Oracle 和/或其附屬公司的註冊商標。

Parallels、Parallels 標誌和 Coherence 是 Parallels International GmbH 的商標或註冊商標。

Python 是 Python 軟體基金會的商標或註冊商標。

Red Hat、Red Hat Enterprise Linux、CentOS、Fedora 是 Red Hat Inc. 或其子公司在美國和其他國家/地區的商標或註冊商標。

BlackBerry 是 Research In Motion Limited 所有的商標，在美國和/或其他國家註冊。

SAMSUNG 是 SAMSUNG 在美國或其他國家/地區的商標。

Debian 是 Public Interest, Inc. 公司的軟體的註冊商標。

Splunk 是 Splunk Inc. 在美國和其他國家/地區的商標和註冊商標。

SUSE 是 SUSE LLC 在美國和其他國家/地區的註冊商標。

Symbian 是 Symbian Foundation Ltd. 所擁有的商標。

VMware、VMware vSphere 和 VMware Workstation 是 VMware, Inc. 在美國和/或其他國家/地區的註冊商標或商標。

UNIX 是在美國和其他國家/地區的註冊商標，透過 X/Open Company Limited 授權。