kaspersky

Kaspersky Endpoint Security for Mac

© 2026 AO Kaspersky Lab

目錄

Kaspersky Endpoint Security 概覽
此版本中的新功能
取決於卡巴斯基安全管理中心管理工具的 Kaspersky Endpoint Security 功能比較
安裝和移除應用程式
  分發套件
  硬體和軟體需求
  準備安裝
  安裝 Kaspersky Endpoint Security
  準備要使用的應用程式
  解除安裝 Kaspersky Endpoint Security
首次啟動應用程式
Kaspersky Endpoint Security 應用程式介面
  應用程式主視窗
  Kaspersky Endpoint Security 圖示
  應用程式設定視窗
關於通知
Kaspersky Endpoint Security 應用程式許可
  關於最終使用者產品授權協議
  關於授權
  關於訂購
  關於產品授權憑證
  關於金鑰
  關於啟動碼
  關於金鑰檔案
  關於資料提供
  啟動 Kaspersky Endpoint Security
  檢視產品授權資訊
  管理產品授權和訂購
  根據工作站產品授權類型比較應用程式功能
執行一般工作
  開啟和結束應用程式
  檢視電腦防護的狀態
  檢視已安裝元件的運行狀態
  停用和還原電腦防護
  使用防護中心
  執行掃描工作
  配置排程掃描工作的自動啟動
  更新應用程式資料庫
  檔案存取被封鎖時如何應對
  還原已經被應用程式刪除或解毒的檔案
  檢視應用程式操作報告
  如果出現通知視窗該怎麼辦

應用程式的進階設定
- 電腦防護範圍
- 檔案威脅防護
- Web 威脅防護
- 郵件威脅防護
- 網路威脅防護
- 防火牆
- 行為偵測
- 掃描
- 更新工作
- 本機工作
  - 外部磁碟掃描工作
- 備份
- 報告
- Managed Detection and Response
- Endpoint Detection and Response Expert（內部部署）
- Endpoint Detection and Response Optimum
  - 與 Endpoint Detection and Response Optimum 整合
  - 掃描查找入侵指標
  - 移動檔案到隔離
  - 獲取檔案
  - 刪除檔案
  - 啟動處理程序
  - 停止處理程序
  - 執行防禦
  - 電腦網路隔離
  - Cloud Sandbox
- FileVault 磁碟加密
- 密碼防護
- 弱點利用防禦
- 修復引擎
- Web 控制
- 裝置控制

加入卡巴斯基安全網路
檢查應用程式元件的完整性
透過卡巴斯基安全管理中心管理主控台管理應用程式
- 在企業網路上部署 Kaspersky Endpoint Security
- 將 Kaspersky Endpoint Security 版本 11.1 或更高版本更新至版本 12.2.1
- 準備遠端安裝 Kaspersky Endpoint Security
  - 安裝 Kaspersky Endpoint Security 管理外掛程式
  - 本機安裝網路代理
  - 使用 Apple 遠端桌面安裝網路代理
  - 使用卡巴斯基安全管理中心安裝網路代理
  - 使用 SSH 協定安裝網路代理
  - 本機解除安裝網路代理

從命令列管理網路代理
在遠端電腦上啟動/停止網路代理
手動檢查用戶端電腦和管理伺服器之間的連線。Klnagchk 公用程式
手動將遠端電腦連線到管理伺服器。Klmover 公用程式
解除安裝網路代理
安裝和解除安裝 Kaspersky Endpoint Security
使用 SSH 協定安裝應用程式
用卡巴斯基安全管理中心安裝應用程式
建立安裝套件
用卡巴斯基安全管理中心解除安裝應用程式
透過卡巴斯基安全管理中心啟動和停止應用程式
建立和管理工作
建立工作
手動啟動和停止工作
匯入和匯出工作
檢視工作
管理特定於工作的設定
建立和管理政策
建立政策
檢視政策清單
配置政策設定
變更政策狀態
將政策匯出到 KLP 檔案
從 KLP 檔案匯入政策
建立和管理政策設定檔
產生有關偵測到的物件的報告
取得加密磁碟機的還原金鑰
透過卡巴斯基安全管理中心網頁主控台和雲端主控台遠端管理應用程式
安裝 Kaspersky Endpoint Security Web 外掛程式
建立政策
主機威脅防護
配置檔案威脅防護元件
配置卸除式磁碟機掃描
配置行為偵測
配置加密軟體防護
配置弱點利用防禦元件
配置修復引擎元件
通訊和 Web 防護
配置"郵件威脅防護"
配置 Web 威脅防護元件
配置網路威脅防護
配置防火牆元件
安全控制
配置裝置控制元件
配置 Web 控制元件
資料加密

一般設定
偵測設定
卡巴斯基安全網路
使用者互動
自我防護
效能
報告和儲存
網路設定
遙測設定
事件設定
更新設定
內建代理
配置 Managed Detection and Response
配置 Endpoint Detection and Response
配置 Endpoint Detection and Response Expert（內部部署）
建立工作
配置掃描工作設定
配置"新增金鑰"工作設定
配置"更新"工作
取得加密磁碟機的還原金鑰
從命令列管理應用程式
檢視命令列說明
執行惡意軟體掃描
更新應用程式
回溯最近更新
啟動/停止元件或工作
檢視元件或工作的狀態和統計訊息
匯出防護設定
啟動應用程式
安裝系統延伸程式
設定網路連線
刪除產品授權金鑰
命令列返回碼
結束應用程式
移除應用程式
Detection and Response 管理指令
管理執行防禦
管理網路隔離
聯絡技術支援服務
如何獲得技術支援
透過 Kaspersky CompanyAccount 提供技術支援
獲取技術支援資訊
使用偵錯檔案
建立偵錯檔案
有關應用程式的資訊來源

附錄
已知問題和限制
已修正問題
按副檔名掃描的物件清單
檔案和資料夾路徑中的遮罩
IOC 檔案要求
受支援的執行防禦的指令碼解釋器
如何將 Kaspersky Endpoint Security 憑證新增至 Mozilla Firefox 憑證儲存
與外部服務交互的網路設定
有關協力廠商代碼的資訊
商標聲明

Kaspersky Endpoint Security 概覽

Kaspersky Endpoint Security 應用程式會防護執行 macOS 的電腦免遭惡意軟體和其他電腦安全威脅的侵害。

檔案威脅防護

威脅防護透過防護和分析任何檔案存取嘗試來即時守衛電腦的檔案系統。更多資訊。

Web 威脅防護

Web 威脅防護可防護電腦透過 HTTP 和HTTPS 協定在 Safari、Google Chrome™ 和 Firefox™ 中傳送和接收的資訊。更多資訊。

郵件威脅防護

郵件威脅防護會掃描傳入和傳出的電子郵件訊息的附件以查找病毒和其他威脅。該元件借助惡意軟體防護資料庫、卡巴斯基安全網路雲端服務和啟發式分析提供電腦保護。更多資訊。

網路威脅防護

網路威脅防護可防止對作業系統的入侵。此元件可防範網路攻擊者（使用連接埠掃描和暴力破解的攻擊者）和網路攻擊者安裝的惡意軟體（包括試圖向犯罪分子傳送個人資料的惡意軟體）。更多資訊。

防火牆

防火牆可在網際網路或者本機網路上工作時封鎖未經授權連線到電腦。這使您可以防護企業區域網路免受身分盜竊和其他攻擊。該元件借助惡意軟體防護資料庫、卡巴斯基安全網路雲端服務和預定義網路規則提供電腦保護。更多資訊。

行為偵測

行為偵測元件接收有關電腦上應用程式操作的資訊，並將此資訊提供給其他防護元件以提高其效能。它還執行選定的操作作為對惡意軟體活動的回應。更多資訊。

弱點利用防禦

弱點利用防禦元件可偵測利用電腦上的弱點來擅用管理員權限或者執行惡意活動的程式代碼。更多資訊。

修復引擎

修復引擎允許 Kaspersky Endpoint Security 復原惡意軟體在作業系統中執行的操作。更多資訊。

掃描

Kaspersky Endpoint Security 應用程式可以按需偵測並消除指定掃描範圍中的惡意軟體和其他電腦安全威脅。Kaspersky Endpoint Security 可以執行電腦的完整掃描、關鍵區域的快速掃描以及指定範圍的掃描。更多資訊。

更新

Kaspersky Endpoint Security 從卡巴斯基更新伺服器、發佈點或系統管理員指定的其他來源更新應用程式資料庫和模組，並建立所有更新檔案的備份副本以允許回溯上次更新。更多資訊。

備份

Kaspersky Endpoint Security 在嘗試解毒或刪除受感染檔案之前會建立受感染檔案的備份副本，以便您可以還原它們。更多資訊。

報告

Kaspersky Endpoint Security 可以生成涉及到應用程式元件的事件和操作的報告。更多資訊。

通知

Kaspersky Endpoint Security 使用通知來通知您 Kaspersky Endpoint Security 操作中的某些事件。通知可以伴隨聲音。更多資訊。

防護中心

Kaspersky Endpoint Security 在防護中心中顯示防護狀態訊息。防護中心顯示有關電腦防護狀態以及如何消除電腦安全問題和威脅的資訊。更多資訊。

透過卡巴斯基安全管理中心遠端管理應用程式

您可以遠端管理安裝了 Kaspersky Endpoint Security 的電腦的防護：接收有關目前電腦防護狀態的資訊、遠端修復問題、回應電腦安全威脅、啟用或停用防護元件（檔案威脅防護、Web 威脅防護、網路威脅防護、行為偵測）、啟用或停用 Web 控制、Managed Detection and Response 和 Endpoint Detection and Response Expert（內部部署）、執行掃描工作、更新應用程式資料庫、執行啟動磁碟加密以及管理 Kaspersky Endpoint Security 產品授權和訂購。您可以使用以下工具來管理 Kaspersky Endpoint Security：

- 卡巴斯基安全管理中心管理主控台。更多資訊。
- 卡巴斯基安全管理中心網頁主控台和雲端主控台。更多資訊。

注意： Kaspersky Endpoint Security 支援的功能取決於您使用的管理工具。

FileVault 磁碟加密

Kaspersky Endpoint Security 允許遠端管理 FileVault 加密。加密可防止未經授權的使用者存取儲存在使用者電腦啟動磁碟上的敏感資料。

Web 控制

您可以遠端管理對使用者造訪的網站的存取。您可以允許或封鎖對特定網址或網址群組的存取。您也可以根據其內容允許或封鎖存取某些類別的網站。更多資訊。

裝置控制

裝置控制可管理使用者對安裝在電腦上或者連線到電腦的裝置的存取。這樣，當連線此類裝置時，您就可以防護電腦免受感染，並防止資料遺失或外洩。更多資訊。

Managed Detection and Response

Managed Detection and Response 元件提供與 Kaspersky Managed Detection and Response 服務的活動，該服務會不斷偵測和消除針對您組織的安全威脅。更多資訊。

Endpoint Detection and Response

Endpoint Detection and Response 元件有助於與 Kaspersky Endpoint Detection and Response 解決方案進行互動。此解決方案結合了自動偵測威脅和回應這些威脅的能力，以抵消包括新漏洞、勒索軟體、無檔案攻擊以及使用合法系統工具的方法。更多資訊。

Endpoint Detection and Response Expert（內部部署）

Endpoint Detection and Response Expert（內部部署）元件有助於與 Kaspersky Anti Targeted Attack Platform 解決方案進行互動。此解決方案可及時偵測進階威脅，例如定向攻擊、進階持續性威脅、零日攻擊等。更多資訊。

此版本中的新功能

該說明套用至適用於 Kaspersky Endpoint Security for Mac 版本 12.2.1。

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

- 現在支援新的 macOS 27 Golden Gate。
- 網頁主控台中的政策管理介面得到了更新。政策中的區域結構進行了變更，以確保與 Kaspersky Endpoint Security for Windows 和 Linux 外掛程式介面保持一致。
- 您現在可以檢視某一段期間對政策進行了哪些修改，以及將這些修改的相關資訊儲存在檔案中。
- 我們新增了新的郵件威脅防護、裝置控制、防火牆、修復引擎和弱點利用防禦元件。
- 現在您可以從 Kaspersky Endpoint Security 應用程式啟動 Managed Detection and Response元件。
- 提高了警示詳細資訊的回應操作的可見性。
- 現在您可以在 Web 主控台中管理行為偵測元件。
- 我們新增了警示摘要。
- 現在，在執行任何回應操作之前，您將收到通知，告知該物件是關鍵系統物件。
- 現在，您可以在建立或編輯 IOC 掃描工作設定時直接在 Web 主控台中編輯 IOC 檔案。
- 現在，您可以將偵測到的物件從警示詳細資訊移至隔離區。
- 我們新增了針對網路隔離工作的限制操作的警告。
- 一般問題修復和改善。

取決於卡巴斯基安全管理中心管理工具的 Kaspersky Endpoint Security 功能比較

Kaspersky Endpoint Security 支援的功能取決於您使用的管理工具（請參閱下表）。

您可以使用以下工具來管理 Kaspersky Endpoint Security：

- 卡巴斯基安全管理中心管理主控台。卡巴斯基安全管理中心管理員工作站上安裝的 Microsoft 管理主控台 (MMC) 管理單元。
- 卡巴斯基安全管理中心網頁主控台。管理伺服器上安裝的卡巴斯基安全管理中心元件。您可以在任何可存取管理伺服器的電腦上使用瀏覽器來使用網頁主控台。
- 卡巴斯基安全管理中心雲端主控台。卡巴斯基安全管理中心的雲端版本。

Kaspersky Endpoint Security 功能比較

功能	卡巴斯基安全管理中心		
	管理主控台	網頁主控台	雲端主控台
進階威脅防護			
卡巴斯基安全網路	✓	✓	✓
行為偵測	✓	✓	
弱點利用防禦	✓	✓	
修復引擎	✓	✓	
關鍵威脅防護			
檔案威脅防護	✓	✓	✓
Web 威脅防護	✓	✓	✓
網路威脅防護	✓	✓	✓
郵件威脅防護	✓	✓	
防火牆	✓	✓	
安全控制			
Web 控制	✓	✓	✓
裝置控制	✓	✓	
資料加密			
FileVault 磁碟加密	✓	✓	✓
還原金鑰	✓	✓	✓
Detection and Response			
Managed Detection and Response	✓	✓	✓
Endpoint Detection and Response		✓	
Endpoint Detection and Response Expert（內部部署）	✓	✓	✓
工作			
新增金鑰	✓	✓	✓
更新	✓	✓	✓
快速掃描	✓	✓	

功能	卡巴斯基安全管理中心		
	管理主控台	網頁主控台	雲端主控台
回溯	✓	✓	✓
掃描	✓	✓	✓

安裝和移除應用程式

分發套件

分發套件包含 Kaspersky Endpoint Security 安裝套件，其包含以下檔案：

- 透過任一可用方法安裝應用程式所需的檔案。
- 包含最終使用者產品授權協議的license_<loc>.txt 檔案。
  最終使用者產品授權協議指定了應用程式的使用條款。

解壓縮壓縮的安裝套件以存取其檔案。

硬體和軟體需求

Kaspersky Endpoint Security 對硬體和軟體有以下要求：

- 處理器類型：Intel, Apple silicon
- 4 GB 記憶體 (RAM)
- 5 GB 可用磁碟空間
- macOS 14、15、26、27
- 網際網路連線

支援的瀏覽器：

- Safari
- Chrome
- Firefox

Kaspersky Endpoint Security 與以下虛擬化工具相容：

- Parallels Desktop 16 for Mac 商業版或更新版本
- VMware Fusion™ 11.5 專業版
- VMware Fusion 12 專業版
- VMware Fusion 13 Pro

MDM 設定檔可以與 Jamf 和 Apple 伺服器一起部署。如果您使用其他伺服器，請參閱技術支援網站（知識庫）上的文章。

您可以透過卡巴斯基安全管理中心遠端管理 Kaspersky Endpoint Security。使用卡巴斯基安全管理中心管理主控台的管理外掛程式和卡巴斯基安全管理中心網頁主控台的 Web 外掛程式來管理 Kaspersky Endpoint Security 需要卡巴斯基安全管理中心 14.2 或更高版本。

注意：要透過卡巴斯基安全管理中心管理 Kaspersky Endpoint Security for Mac 12.2.1，您必須在遠端電腦上安裝網路代理版本 15。

準備安裝

在電腦上安裝應用程式之前，建議您執行以下操作：

- 確保您的電腦滿足硬體和軟體需求。
- 刪除卡巴斯基安全軟體 Mac 版或任何其他反惡意軟體應用程式，以避免系統衝突並最大限度地提高系統效能。

注意：在遠端安裝 Kaspersky Endpoint Security 之前，我們建議您從卡巴斯基技術支援網站下載 KES_for_macOS11_and_later.zip 壓縮檔案，並使用 Apple 遠端管理工具在用戶端電腦上套用 KES_for_macOS11_and_later_profile.mobileconfig 設定檔。這將允許 Kaspersky Endpoint Security 獲得以下權限：安裝核心延伸功能和系統延伸功能的權限、完整磁碟存取權限以及配置網路連線的權限。要了解有關配置檔和其他選項的更多資訊，請造訪技術支援網站。

安裝 Kaspersky Endpoint Security

重要提示： 卡巴斯基專家建議僅按照本說明中的敘述安裝 Kaspersky Endpoint Security。

您可以通過以下方式之一安裝 Kaspersky Endpoint Security：

- 本機，利用從卡巴斯基網站下載的分發套件。
- 遠端使用 Apple 遠端桌面
- 遠端透過卡巴斯基安全管理中心管理主控台。
- 遠端透過卡巴斯基安全管理中心網頁主控台或卡巴斯基安全管理中心雲端主控台。

  有關使用卡巴斯基安全管理中心網頁主控台部署 卡巴斯基應用程式的詳細資訊，請參閱卡巴斯基安全管理中心說明。有關使用卡巴斯基安全管理中心雲端主控台部署 卡巴斯基應用程式的詳細資訊，請參閱卡巴斯基安全管理中心雲端主控台說明。

執行 Kaspersky Endpoint Security 的標準安裝

1. 從分發套件中解壓縮 ZIP 檔案。
2. 從解壓縮的壓縮檔案內容中開啟 .dmg 檔案。

3. 在開啟的視窗中，按兩下**安裝 Kaspersky Endpoint Security**。

   Kaspersky Endpoint Security 安裝助手將開啟。

4. 點擊**安裝**。

5. 按照安裝助手的步驟完成安裝。

安裝完成後，Kaspersky Endpoint Security 將自動啟動。您不必重新啟動電腦。

注意：如果使用此安裝方法，則不會安裝Endpoint Detection and Response Expert（內部部署）、Endpoint Detection and Response (Optimum) 和 Cloud Sandbox 元件。

執行 Kaspersky Endpoint Security 的自訂安裝

1. 從分發套件中解壓縮 ZIP 檔案。

2. 從解壓縮的壓縮檔案內容中開啟 .dmg 檔案。

3. 在開啟的視窗中，按兩下**安裝 Kaspersky Endpoint Security**。

   Kaspersky Endpoint Security 安裝助手將開啟。

4. 點擊**自訂**，選取或取消選取您不想安裝的元件旁的核取方塊，然後點擊**繼續**。

5. 按照安裝助手的步驟完成安裝。

安裝完成後，Kaspersky Endpoint Security 將自動啟動。您不必重新啟動電腦。

使用 Apple 遠端桌面遠端安裝 Kaspersky Endpoint Security

1. 在 Mac 上，選取 **Apple 功能表>系統設定>一般>共用**。

2. 選擇**遠端管理**核取方塊。

3. 在您想要作為伺服器的另一台 Mac 上，安裝 Apple 遠端桌面。有關 Apple 遠端桌面的更多資訊，請參閱 Apple 支援。

4. 開啟 Apple 遠端桌面。

5. 在**遠端桌面**視窗中，點擊左側的**掃描器**，然後選擇要安裝 Kaspersky Endpoint Security 的裝置。

6. 點擊**安裝**。

7. 在管理員憑據提示中，輸入管理員名稱和密碼，然後點擊**新增**。

8. 點擊 + 並選擇 Kaspersky Endpoint Security 安裝套件中的 .dmg 檔案。

9. 點擊**安裝**。

Kaspersky Endpoint Security 開始在所選裝置上安裝。

準備要使用的應用程式

安裝 Kaspersky Endpoint Security 後，您可以執行下列操作：

- 啟動 Kaspersky Endpoint Security。應用程式啟動後，Kaspersky Endpoint Security 開始防護您的電腦，您可以定期更新應用程式資料庫和模組、執行惡意軟體掃描工作並向技術支援傳送請求。

  > Managed Detection and Response 元件在卡巴斯基安全管理中心管理或網頁主控台中單獨啟動。

  如果您目前的產品授權不支援 Endpoint Detection and Response 元件，您需要單獨啟動 Kaspersky Endpoint Detection and Response。

- 評估電腦防護的狀態。
- 更新 Kaspersky Endpoint Security。
- 掃描您的電腦是否有惡意軟體。

解除安裝 Kaspersky Endpoint Security

1. 開啟應用程式分發套件的 DMG 檔案。
2. 在包含分發套件內容的視窗中，按兩下**解除安裝 Kaspersky Endpoint Security**。
   Kaspersky Endpoint Security 解除安裝程式啟動。
3. 在解除安裝程式視窗中，點擊**移除**。
4. 當系統提示您輸入管理員憑據時，輸入管理員名稱和密碼並確認您要解除安裝 Kaspersky Endpoint Security。
   解除安裝 Kaspersky Endpoint Security 啟動。
5. 閱讀有關完成解除安裝的資訊並點擊**結束**以結束移除程式。

Kaspersky Endpoint Security 現已從您的電腦中解除安裝。解除安裝應用程式後不必重新啟動電腦。

首次啟動應用程式

Kaspersky Endpoint Security 在安裝後立即在您的電腦上啟動。要立即防護您的 Mac，應用程式提示您執行基本安裝：

- 向 Kaspersky Endpoint Security 授予必要的權限，以防護您的 Mac 抵禦惡意軟體、網路攻擊和網路威脅。
  對于您授予的權限的更多資訊，點擊 ?。
- 啟動 Kaspersky Endpoint Security。

注意：需要網際網路連線以進行 Kaspersky Endpoint Security 的基本安裝。

首次啟動 Kaspersky Endpoint Security

1. 在**基本防護**視窗，執行以下操作以確保檔案威脅防護和 Web 威脅防護工作正常：
   - 如果您想让 Kaspersky Endpoint Security 應用程式正常工作，允許應用程式掃描您的 Mac 上的每個檔案。為此，請點擊**完全取用磁碟**項旁邊的**允許**並遵照熒幕上的說明操作。
   - 如果想要 Kaspersky Endpoint Security 檢查 URL 和網路封包以防它們損壞您的 Mac，請安裝系統延伸程式。為此，請點擊**系統延伸程式**項旁邊的**安裝**，並遵照熒幕上的說明操作。
   - 如果想要系統延伸程式正常工作，請允許網路內容過濾。為此，請點擊**網路內容過濾**項旁邊的**允許**，並遵照熒幕上的說明。
   - 如果您希望 Kaspersky Endpoint Security 在加密的 HTTPS 流量中搜尋惡意軟體和網際網路威脅，請安裝受信任的憑證。為此，請點擊**安裝**項旁邊的**受信任憑證**，並遵照熒幕上的說明操作。

   重要：如果不授予這些權限，Kaspersky Endpoint Security 應用程式將工作不正常。您必須在**基本防護**視窗授予所有權限。
2. 點擊**繼續**。

將開啟應用程式視窗。

Kaspersky Endpoint Security 應用程式介面

應用程式主視窗

開啟應用程式主視窗

在功能表列中，點擊應用程式圖示，並選擇**Kaspersky Endpoint Security**。

Kaspersky Endpoint Security 的主應用程式視窗包含提供對應用程式主要功能進行存取的介面元素。

主應用程式主視窗分為兩部分：

- 左側部分包含側邊欄，允許您導航應用程式並快速存取其主要功能。
- 中心部分顯示側邊欄中所選區域的內容，並允許您管理資料。

側邊欄

主應用程式視窗的側邊欄具有以下選項：

正在監控	點擊可開啟**正在監控**頁面，該頁面提供有關 Kaspersky Endpoint Security 為防護您的電腦而採取的措施的資訊。
防護中心	點擊以檢視您的電腦防護狀態。更多資訊。
安全	點擊可檢視已安裝元件的運作狀態。更多資訊。
掃描	點擊以管理掃描工作。更多資訊。
更新	點擊以管理更新工作。更多資訊。
產品授權	點擊以啟動應用程式或檢視有關您的產品授權的資訊。更多資訊。

正在監控頁面的控件

正在監控頁面顯示防護狀態指示器，提供有關 Kaspersky Endpoint Security 為防護您的電腦所做的操作的資訊，並包含以下控件。

防護中心	通知您有關電腦防護的問題。更多資訊。
報告	可讓您檢視應用程式運行期間發生的事件、單個元件和工作。更多資訊。
備份	可讓您檢視應用程式已刪除的感染檔案的已儲存副本的清單。瞭解更多。更多資訊。
威脅偵測	允許您檢視有關 Kaspersky Endpoint Security 套用的威脅偵測技術以及這些技術偵測到的威脅數量的資訊。
卡巴斯基安全網路	顯示 Kaspersky Endpoint Security 和卡巴斯基安全網路之間的連線狀態，以及全球卡巴斯基安全網路統計資料。

Kaspersky Endpoint Security 圖示

一旦安裝 Kaspersky Endpoint Security，Kaspersky Endpoint Security 圖示就會出現在功能表列中。當應用程式啟動時，應用程式圖示顯示應用程式的狀態。如果應用程式圖示處於活動狀態（ ），表示全部或某些防護元件已啟用。如果應用程式圖示處於非活動狀態（ ），則所有防護元件均停用。

開啟應用程式圖示功能表

在功能表列中，點擊應用程式圖示。

預設情況下，應用程式圖示始終顯示在功能表列中。您可以從功能表列中刪除應用程式圖示。

從功能表列中刪除應用程式圖示

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在**介面**標籤上的**應用程式圖示**部分中，取消選取**在功能表列中顯示**核取方塊。

當您開啟應用程式視窗時，應用程式圖示也會出現在**Dock**中。

從應用程式圖示功能表中，您可以存取主應用程式視窗並執行以下操作：

- 停用電腦防護。
- 還原電腦防護。
- 開啟防護中心。
- 啟動快速掃描。
- 執行更新。
- 開啟應用程式設定視窗。
- 結束 Kaspersky Endpoint Security。

應用程式設定視窗

開啟應用程式設定視窗

執行以下操作之一：

- 在功能表列中，點擊應用程式圖示，並選擇**設定**。
- 在功能表列中，點擊**Kaspersky Endpoint Security >設定**。
- 如果 Kaspersky Endpoint Security 正在執行，請點擊**Dock**中的應用程式圖示並選擇**設定**。

可以使用設定視窗上部的以下索引標籤快速存取應用程式設定：

- **基本**。在此標籤上，您可以啟用或停用電腦防護並設定檔威脅防護、Web 威脅防護和網路威脅防護設定。
- **掃描**。在此標籤上，您可以設定掃描工作的設定以及掃描工作的排程啟動。
- **威脅**。在此標籤上，您可以選擇要偵測的物件的類別、建立受信任區域以及配置備份設定。
- **進階**。在此標籤上，您可以加入或選擇不參與卡巴斯基安全網路。
- **更新**。在此標籤上，您可以配置應用程式更新設定或回溯到應用程式資料庫的先前版本。
- **介面**。在此標籤上，您可以配置 Kaspersky Endpoint Security 圖示、通知和報告的設定，以及啟用或停用在偵錯檔案中記錄偵錯資訊。

使用  按鈕，您可以封鎖沒有管理員權限的使用者編輯 Kaspersky Endpoint Security 設定。此按鈕位於應用程式設定視窗的下部。若要編輯設定，您必須輸入管理員憑據。

點選?按鈕將開啟 Kaspersky Endpoint Security 說明，其描述了目前應用程式視窗中的所有設定。您也可以透過在**開啟此視窗的說明**功能表中選擇**說明**來開啟活動應用程式視窗的說明主題。

關於通知

Kaspersky Endpoint Security 會顯示通知以告知您應用程式事件。根據電腦上安裝的作業系統版本，通知會顯示在作業系統的通知中心中。通知的外觀取決於作業系統通知設定中設定的選項。

Kaspersky Endpoint Security 事件依其重要性分為三種類型：

- *緊急* – 對電腦安全構成危險威脅的事件（偵測到惡意物件、弱點、Kaspersky Endpoint Security 問題）。緊急事件需要您立即關注。我們建議您不要停用緊急事件的通知。
- *重要* – 不需要您立即關注但可能對未來電腦安全構成威脅的事件。
- *資訊性* – 報告供您參考的事件。

停用通知

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。

   此時會開啟應用程式設定視窗。

2. 在**介面**標籤的**通知**部分，取消選中**啟用通知**核取方塊。

啟用記錄非緊急事件

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。

   此時會開啟應用程式設定視窗。

2. 在**介面**標籤的**報告**部分中，勾選**記錄非緊急事件**核取方塊以接收 Kaspersky Endpoint Security 資訊事件的通知。

無論通知是啟用還是停用，應用程式報告都包含有關 Kaspersky Endpoint Security 執行時發生的事件的資訊。

通知可以伴隨聲音（例如，有關偵測到的惡意軟體的通知）。您可以停用提示音。

記錄非緊急事件顯著增加報告檔案總大小。請注意，此設定僅適用於檔案威脅防護。

停用伴隨通知的提示音

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。

   此時會開啟應用程式設定視窗。

2. 在**介面**標籤的**通知**區域中，取消選中**偵測到惡意軟體時開啟警報音**核取方塊。

如果需要執行操作來回應事件，Kaspersky Endpoint Security 會顯示通知視窗。例如，當應用程式偵測到惡意物件時，它會提示您刪除或解毒該物件。僅在選擇其中一項操作後，通知視窗才會從螢幕上消失。

Kaspersky Endpoint Security 應用程式許可

關於最終使用者產品授權協議

最終使用者產品授權協議（產品授權協議）是您和 AO Kaspersky Lab 之間簽訂的具有約束力的協議，規定了有關使用該應用程式的相關條款。

重要：在開始使用應用程式之前，請認真閱讀產品授權協議。

您可以使用以下方式檢視《最終使用者產品授權協議》的條款：

- 在安裝 Kaspersky Endpoint Security 的過程中
- 閱讀應用程式安裝資料夾中的 license.txt 文件

安裝 Kaspersky Endpoint Security 即表示您確認您已瞭解並接受最終使用者產品授權協議的條款。如果您不接受最終使用者產品授權協議的條款，請取消安裝 Kaspersky Endpoint Security 並且不使用該應用程式。

關於授權

*產品授權*是根據已簽署的產品授權合約（最終使用者產品授權協議）的條款授予的使用 Kaspersky Small Office Security 的限時權利。

服務範圍和有效期取決於使用該應用程式的產品授權。

提供以下產品授權類型：

- *試用版*。用於試用該應用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。當試用版產品授權到期時，所有 Kaspersky Endpoint Security 功能將轉為停用。要繼續使用此程式，您需要購買正式版產品授權。

  您只能在試用版產品授權下使用該應用程式一個試用期。

- *正式版*。付費產品授權。

  當正式版產品授權到期時，應用程式的關鍵功能將被停用。要繼續使用 Kaspersky Endpoint Security，您必須續約正式版產品授權。正式版產品授權過期後，您將無法繼續使用該應用程式，必須將其從裝置中移除。

  我們建議在產品授權到期之前進行續約，以確保不間斷防護所有安全威脅。

關於訂購

*Kaspersky Endpoint Security 訂購*是一項帶有特定參數（到期日期，受防護裝置數量）的應用程式購買訂單。您可以從服務供應商（範例您的 ISP）處訂購 Kaspersky Endpoint Security 訂購。您可以在服務提供商網站上的會員區域中管理您的訂購。例如，您可以續約或取消訂購、縮短期限或變更訂購防護的裝置數量。

訂購可能受限制（例如，一年時間）或不受限製（無到期時間）。若要在有限訂購期限到期後繼續使用 Kaspersky Endpoint Security，您必須手動續約。只要您提前向服務提供者付款，無限訂購就會自動續約。

如果您在有限訂購下使用該應用程式，當訂購到期時，您將有一段寬限期來續約訂購。在寬限期內，應用程式功能保持不變。

在您的更新訂購到期以及訂購續約寬限期結束後，Kaspersky Endpoint Security 仍保持功能，但會停止更新應用程式資料庫。

在您的更新和防護訂購到期以及訂購續約寬限期結束後，Kaspersky Endpoint Security 將停止防護您的電腦。

要在訂購下使用 Kaspersky Endpoint Security，您必須新增從服務供應商處接收到的啟動碼。當在訂購下使用應用程式時，您不能使用不同的啟動碼來續約訂購。只有在訂購到期或取消訂購後，您才可以套用不同的啟動碼。要取消您的訂購，請聯絡您從其購買 Kaspersky Endpoint Security 的服務提供商。

注意：只有刪除使用中的金鑰後才能套用不同的訂購啟動碼。訂購沒有金鑰檔案。您無法將訂購新增為備用金鑰。使用訂購時無法新增備用金鑰。

如果您已經在有效產品授權下使用 Kaspersky Endpoint Security，但想要在訂購下使用應用程式，請刪除目前的活動金鑰，以便您可以使用訂購金鑰啟動應用程式。先前用於在此電腦上啟動應用程式的啟動碼可以在另一台電腦上使用。

注意：可能的訂購選項可能因服務提供者而異。一些服務提供者也可能選擇不提供續約訂購的寬限期。

關於產品授權憑證

*產品授權憑證*是您隨金鑰檔案或啟動碼一起收到的文件。

產品授權憑證包含所提供產品授權的以下資訊：

- 產品授權金鑰或訂單號
- 有關已被授予產品授權的使用者的資訊
- 有關可根據提供的產品授權啟動的應用程式的資訊
- 授權單元（例如，可以在所提供的產品授權下使用應用程式的裝置）的數量限制
- 產品授權有效開始日期
- 產品授權到期日期或產品授權期限
- 產品授權類型

關於金鑰

*金鑰*是一個序號，您可用於根據最終使用者產品授權協議條款啟動和使用應用程式。金鑰由卡巴斯基專家產生。

您可以使用下列方法之一為應用程式新增金鑰：透過套用*金鑰檔案*或輸入*啟動碼*。將金鑰新增到應用程式後，該金鑰將作為唯一的字母數字序列顯示在應用程式介面中。

如果違反產品授權協議的條款，卡巴斯基可能會封鎖金鑰。如果金鑰已被封鎖，您需要新增其他金鑰才能繼續使用應用程式。

金鑰可以是啟動金鑰或備用金鑰。

*啟動金鑰*是程式目前正在使用的金鑰。可以為試用版或商業授權或訂購新增活動金鑰。本應用程式不能擁有兩個及以上啟動金鑰。

*備用金鑰*使用者可新增一組目前尚未使用的金鑰。當與目前啟動金鑰關聯的產品授權到期時，備用金鑰將自動變為啟動狀態。僅當已新增啟動金鑰時才能新增備用金鑰。

試用版產品授權或正式版產品授權金鑰可以被新增為啟動金鑰。試用產品授權的金鑰無法新增為備用金鑰。當試用產品授權金鑰處於活動狀態時，無法新增備用金鑰。

關於啟動碼

*啟動碼*是由 20 個字母和數字組成的唯一序號。您必須輸入啟動碼以新增用於啟動 Kaspersky Endpoint Security 的產品授權金鑰。在購買 Kaspersky Endpoint Security 或請求 Kaspersky Endpoint Security 試用版後，您會在您提供的電子郵件地址收到啟動碼。

要使用啟動碼啟動應用程式，您需要訪問網際網路才能連線到卡巴斯基啟動伺服器。

如果您在安裝應用程式後遺失了啟動碼，請聯絡您購買產品授權的卡巴斯基合作夥伴。

關於金鑰檔案

*金鑰檔案*是卡巴斯基提供給您的具有 .key 副檔名的檔案。金鑰檔案旨在透過新增產品授權金鑰來啟動應用程式。

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

使用金鑰檔案無需連線至卡巴斯基啟動伺服器以啟動應用程式。

如果金鑰檔案被意外刪除，則您可以還原它。您可能需要金鑰檔案註冊諸如 Kaspersky CompanyAccount 之類的服務。

若要還原金鑰檔案，請執行下列任一操作：

- 聯絡產品授權銷售商。
- 使用您可用的啟動碼透過卡巴斯基網站接收金鑰檔案。

關於資料提供

最終使用者產品授權協議

當透過啟動碼啟動 Kaspersky Endpoint Security 時，為了驗證應用程式的合法使用並提供有關卡巴斯基產品分發和使用的統計資訊，您同意在使用 Kaspersky Endpoint Security 期間自動提供以下資訊：

- 已安裝軟體的類型、版本和當地語係化。
- 安裝的更新版本。
- 電腦的識別碼和電腦上安裝的軟體的識別碼。
- 目前產品授權的啟動碼和唯一啟動識別碼。
- 作業系統類型、版本以及字組大小。
- 當軟體安裝在虛擬環境時，虛擬環境的名稱。
- 提供資訊時處於活動狀態的軟體元件的識別碼。
- 支援的資料來源。
- 逾時。
- 使用者電腦上的日期和時間。
- 協定版本。
- 協定內容類型。
- 協定內容長度。
- 使用的資料壓縮類型。
- 啟動票證上的簽名類型。
- 區域啟動中心識別碼。
- 使用 SHA1 演算法計算的啟動碼雜湊值。
- 使用 SHA1 演算法計算的票證內容雜湊。
- 產品授權票證建立日期和時間。
- 產品授權啟動識別碼。
- 目前產品授權票證識別碼。
- 產品授權票證序列識別碼。
- 產品授權啟動日期和時間。

- 產品授權到期的日期及時間。
- 產品授權狀態。
- 產品授權版本。
- 使用者電腦的唯一識別碼。
- 產品授權票證標頭版本。
- 應用程式名稱。
- 傳輸的資料類型。
- 傳輸的資料方案版本。
- 作業系統完整版本。
- 所使用的虛擬機器的描述。
- 相容於應用程式的 ID 清單。

當您使用卡巴斯基更新伺服器下載更新時，為了提高更新過程的效率，您同意在資料庫和模組更新期間定期提供以下資訊用於應用程式識別：

- 軟體 ID (AppID)。
- 啟動的產品授權 ID。
- 唯一軟體安裝 ID（安裝 ID）。
- 唯一的更新工作啟動 ID (SessionID)。
- 應用程式版本 (BuildInfo)。

卡巴斯基安全網路 (KSN) 聲明

KSN 的使用可能可提高軟體對於資訊及網路安全威脅的反應速度。KSN 透過以下方法達到本項目的：

- 判斷受掃描物件的信譽。
- 識別難以偵測的新資安威脅及其來源。
- 立即採取適當措施，以加強防護使用者在電腦中儲存與處理的資料。
- 降低誤報可能性。
- 提升應用程式元件效能。
- 調查使用者電腦感染事件。
- 增進卡巴斯基產品效能。
- 收取有關已知信譽物件數量的參考資訊。
- 及時識別並更正與產品安裝、移除和更新相關的錯誤。

在使用 KSN 期間，卡巴斯基將自動接收和處理資料。使用者傳輸的資料取決於安裝的產品授權類型和指定的卡巴斯基安全網路使用設定。

如果您使用適用於 1-4 個節點的產品授權，卡巴斯基在使用卡巴斯基安全網路期間會自動接收並處理下列資料：

- 所使用授權的相關資訊： 授權的類型和有效期、授權失效前的天數、向其購買授權的合作夥伴的識別碼、區域啟動中心識別碼、啟動碼的總和檢查碼、SHA1 演算法計算的票證內容雜湊、授權票證建立日期與時間、授權資訊識別碼、授權票證識別碼、授權票證順序識別碼、使用者電腦的唯一識別碼、授權票證有效開始日期、授權票證有效結束日期、授權票證目前狀態、票證標題版本、授權版本、票證標題簽章憑證識別碼、金鑰檔案的總和檢查碼、票證標題簽署者序號、身分驗證權杖。

- 所安裝軟體的完整版本； 已安裝軟體的類型； 軟體更新 ID； 聲譽服務的 ID； 協定類型 ID； 區域啟動中心的 ID； 已撤銷軟體服務決策清單版本； 軟體病毒資料庫中的已觸發記錄 ID； 軟體病毒資料庫中的已觸發記錄時間戳記； 觸發的軟體病毒資料庫記錄類型； 電腦上應用程式安裝實例的唯一 ID； 產品授權啟動日期； 授權失效日期； 授權識別碼； 軟體所使用授權的狀態； 目前處理中物件的總和檢查碼類型； 偵測到的惡意軟體名稱或是可能用於傷害使用者裝置或資料的合法軟體名稱； 目前處理中物件的總和檢查碼； 軟體啟動碼的總和檢查碼； 軟體的完整版本； 唯一裝置 ID； 軟體 ID； 軟體金鑰檔案的總和檢查碼； 用於提供軟體授權的資訊模型 ID； 用於簽署軟體授權票證標頭的憑證識別碼； 軟體授權票證建立日期和時間； 軟體授權票證總和檢查碼； 軟體授權票證版本； 軟體啟動碼版本； 權利持有人基礎架構請求資料格式； 啟動的產品授權票證 ID； 軟體元件 ID； 軟體動作結果； 錯誤代碼； 網路服務的已存取位址（URL、IP）； 通訊埠編號； 網路服務請求來源（推薦者）的網址； 認證的公開金鑰； 所掃描物件與雜湊演算法的數位憑證指紋。

如果您使用適用於 5 個或更多節點的產品授權，卡巴斯基在使用卡巴斯基安全網路期間會自動接收並處理下列資料：

- 作業系統版本和已安裝在電腦上的服務套件版本的相關資訊；目前和預設的作業系統語言設定；作業系統內核檔案的版本和總和檢查碼（MD5、SHA2-256、SHA1）；作業系統執行模式的參數； 作業系統版本、作業系統組建編號、作業系統更新編號、作業系統版本、作業系統版本延伸資訊； 作業系統服務包版本； 作業系統啟動的日期和時間； 行為分析子系統中關於作業系統的事件處理延遲時間； 延遲的目前類型作業系統動作事件數； 主動式防禦子系統中關於作業系統的事件處理延遲時間； 已處理的作業系統動作事件數； 已處理的同步作業系統動作事件數； 延遲的目前類型作業系統動作事件總數； 常設事件儲存子系統中關於作業系統的事件處理延遲時間； 延遲的作業系統動作事件總數； 等待中的同步作業系統動作事件數； 作業系統中一項動作收到事件的日期和時間。

- 有關上次作業系統重新啟動失敗的資訊： 重新啟動失敗的次數。

- 權利持有人之已安裝應用程式和病毒防護狀態的相關資訊： 軟體安裝 ID（PCID）； 軟體資料庫記錄版本； 電腦上應用程式安裝實例的唯一識別碼、應用程式類型、應用程式類型 ID、所安裝的應用程式的完整版本、應用程式設定版本的識別碼、電腦類型的識別碼、已安裝應用程式的電腦的唯一識別碼、權利持有人服務中的唯一使用者識別碼、本機語言和操作狀態、所安裝軟體元件的版本及其操作狀態、用於連線權利持有人服務的協定版本； 所安裝軟體的完整版本； 已安裝軟體的類型； 軟體更新 ID； 聲譽服務的 ID； 協定類型 ID； 區域啟動中心的 ID； 已撤銷軟體服務決策清單版本； 軟體病毒資料庫中的已觸發記錄 ID； 軟體病毒資料庫中的已觸發記錄時間戳記； 觸發的軟體病毒資料庫記錄類型； 電腦上應用程式安裝實例的唯一 ID； 產品授權啟動日期； 授權失效日期； 授權識別碼； 軟體所使用授權的狀態； 目前處理中物件的總和檢查碼類型； 偵測到的惡意軟體名稱或是可能用於傷害使用者裝置或資料的合法軟體名稱； 目前處理中物件的總和檢查碼； 軟體啟動碼的總和檢查碼； 軟體的完整版本； 軟體 ID； 軟體金鑰檔案的總和檢查碼； 用於提供軟體授權的資訊模型 ID； 用於簽署軟體授權票證標頭的憑證識別碼； 軟體授權票證建立日期和時間； 軟體授權票證總和檢查碼； 軟體授權票證版本； 軟體啟動碼版本； 權利持有人基礎架構請求資料格式； 啟動的產品授權票證 ID； 軟體元件 ID； 軟體動作結果； 錯誤代碼； 網路服務的已存取位址（URL、IP）； 通訊埠編號； 網路服務請求來源（推薦者）的網址； 防毒資料庫的更新適用週期數； 防毒資料庫上次更新和套用的日期和時間； 軟體資料庫的發佈日期與時間； 軟體元件版本； 軟體更新 ID； 已安裝軟體的類型； System Watcher 開始的日期和時間； 軟體的安裝日期和時間； 由 System Watcher 傳送統計資料的可能性； 由 System Watcher 處理，需時超過標準時間的事件碼； 由 System Watcher 處理，需時超過標準時間的事件的資料庫處理時間； 由 System Watcher 處理一項事件的最大允許時間； 由 System Watcher 處理，需時超過標準時間的事件處理時間； 由 System Watcher 處理，需時超過標準時間的事件總數。

- 所有被處理物件與操作的相關資訊： 軟體對被處理物件的判定； 目錄碼； 處理中物件的大小； 處理中物件的總和檢查碼 (SHA256)； 系統監控環境中偵測到的軟體數量； 被系統監控偵測到的軟體的日期和時間； 偵測特徵； 軟體病毒資料庫中的已觸發記錄 ID； 系統監控偵測軟體的原因； 處理中物件的總和檢查碼 (MD5)； 模組完整性檢查的結果； 目前處理中物件的名稱； 觸發的軟體病毒資料庫記錄類型； 所處理物件的路徑； 被掃描物件的名稱； 掃描的日期和時間； 從其下載的 URL 和 Referrer 位址； 被掃描檔案的大小及其路徑； 壓縮檔案標誌； 檔案建立日期與時間； 封包程式的名稱、大小和總和檢查碼（MD5、SHA2-256）（如果檔案被封包）； 檔案的熵； 檔案的類型； 檔案類型代碼； 可執行檔的標誌、ID 和格式； 物件的總和檢查碼（MD5、SHA2-256）； 物件的補充總和檢查碼的類型和值； 有關物件的數位簽章（憑證）的資料： 憑證發行者相關資料、自上一次傳送統計資料後物件的啟動次數、應用程式掃描工作的 ID、收取有關物件信譽的資訊的方式、目標篩選條件值、適用偵測技術的技術參數； 所處理物件的路徑； 目錄碼。

- 對於可執行檔： 檔案區段熵、聲譽驗證旗標或檔案簽署旗標、名稱、類型、ID 類型、總和檢查碼 (MD5)、經驗證物件所載入應用程式的大小、應用程式路徑和範本路徑、自動執行清單中表明狀態的屬性、登錄日期、屬性清單、封裝程式名稱、應用程式數位簽章相關資訊： 發行商憑證、以 MIME 格式上傳的檔案名稱、檔案組建日期與時間。

- 啟動的應用程式及其模組的相關資訊： 總和檢查碼（MD5、SHA2-256）、大小、屬性、建立日期、加殼器名稱（如果檔案已加殼）、檔案名稱、有關係統上執行的處理程序的資訊（處理程序 ID (PID)、處理程序名稱、有關啟動處理程序的帳戶的資訊、啟動處理程序的應用程式和命令、處理程序檔案的完整路徑以及啟動命令列、處理程序所屬應用程式的敘述（處理程序的名稱）應用程式和有關發布者的資訊），以及正在使用的數位憑證和驗證其真實性所需的資訊或有關缺少檔案數位簽章的資訊），以及有關載入到處理程序中的模組的資訊： 它們的名稱、大小、類型、建立日期、屬性、總和檢查碼（MD5、SHA2-256、SHA1）、它們的路徑、PE 檔案標頭資訊、加殼器名稱（如果檔案已加殼）、有關可用性的資訊以及這些統計資料的有效性、產生正在傳送的統計資料的模式的識別碼。

- 若偵測到威脅或弱點，除了所偵測物件的相關資訊以外，還需提供下列資訊：識別碼、版本及病毒資料庫中的記錄類型、根據卡巴斯基分類的威脅名稱、病毒資料庫上一次更新的日期與時間、可執行檔名稱、要求威脅偵測 URL 之應用程式檔案的總和檢查碼 (MD5)、已偵測威脅的 IP 位址（IPv4 或 IPv6）、弱點識別碼及其威脅等級、偵測到弱點的網頁的 URL 與參照位址。

- 若偵測到潛在惡意物件，提供的相關資訊包括程序記憶體中的資料。

- 網路攻擊資訊： 發動攻擊的電腦 IP 位址、網路攻擊指向的使用者電腦連接埠號、攻擊協定的 ID、攻擊的名稱和類型。

- 網路連線相關資訊： 啟動程序而開啟連接埠的檔案版本及總和檢查碼 (MD5、SHA2-256、SHA1)、程序檔案的路徑及其數位簽章、本機及遠端 IP 位址、本機及遠端連接埠號、連線狀態、連接埠開啟的時間戳記。

- 偵測到有害或可疑內容的網頁 URL 和 IP 位址、要求該 URL 的檔案名稱、大小和總和檢查碼、用來達到判定結果之規則的識別碼、加權與程度、攻擊目標。

- 有關已安裝應用程式和病毒資料庫更新的資訊： 更新工作的完成狀態、更新期間可能發生的錯誤類型、更新失敗的次數、執行更新之應用程式元件的識別碼。

- 卡巴斯基安全網路 (KSN) 的使用相關資訊： KSN 識別碼、軟體識別碼、應用程式完整版本、使用者裝置的去個人化 IP 位址、KSN 要求履行品質指標、KSN 封包處理品質指標、KSN 要求數目指標與 KSN 要求類型相關資訊、開始傳送統計資料的日期與時間、結束傳送統計資料的日期與時間、KSN 配置更新相關資訊： 活動配置的識別碼、收到的配置的識別碼、配置更新的錯誤代碼。

- 系統記錄事件相關資訊： 偵測到事件的記錄檔名稱、事件的類型與分類、事件來源名稱以及事件描述。

- 用於確定檔案和 URL 位址信譽的資訊： 請求信譽的 URL 位址和參照位址、連線的協定類型、應用程式類型的內部識別碼、正在使用的連接埠號、使用者識別碼、掃描檔案的總和檢查碼 (MD5)、偵測到的威脅的類型、用於偵測威脅的記錄的資訊（病毒資料庫的記錄識別碼、記錄時間戳記和類型）； 認證的公開金鑰； 所掃描物件與雜湊演算法的數位憑證指紋。

- 應用程式地區分佈相關資料： 應用程式安裝和啟動日期、提供應用程式啟動授權的合作夥伴 ID、應用程式 ID、應用程式語言本機化 ID、應用程式啟動授權序號、KSN 加入簽章。

- 所使用授權的相關資訊： 授權的類型和有效期、授權失效前的天數、向其購買授權的合作夥伴的識別碼、區域啟動中心識別碼、啟動碼的總和檢查碼、SHA1 演算法計算的票證內容雜湊、授權票證建立日期與時間、授權資訊識別碼、授權票證識別碼、授權票證順序識別碼、使用者電腦的唯一識別碼、授權票證有效開始日期、授權票證有效結束日期、授權票證目前狀態、票證標題版本、授權版本、票證標題簽章憑證識別碼、金鑰檔案的總和檢查碼、票證標題簽署者序號、身分驗證權杖。

- 電腦上所安裝的硬體相關資訊： 內建和已連線裝置的類型、名稱、型號名稱、韌體版本、參數。

- 裝置資訊： 裝置 ID。

- Web 控制元件的作業資訊： 元件版本、分類原因、其他分類原因的相關資訊、分類 URL、被封鎖 / 分類物件的主機 IP 位址。

為加強軟體所提供的防護，卡巴斯基所收到的物件可能遭入侵者用於傷害電腦，並對資訊安全造成威脅。這類物件包括：

- 可執行或不可執行檔或其部分

- 電腦的 RAM 區

- 涉及 OS 啟動程序的區段

- 網路流量資料封包

- 含有可疑或惡意物件的網頁及電子郵件

- WMI 儲存的類別說明及類別實例

- 應用程式活動報告

應用程式活動報告含有以下檔案及處理程序相關資料：

- 發送檔案名稱、大小、版本、說明及總和檢查碼（MD5、SHA2-256、SHA1）、格式 ID、廠商名稱、檔案所屬應用程式名稱、檔案在電腦上的完整路徑和路徑範本代碼、檔案建立和更新的日期與時間。

- 憑證有效期的開始及終止日期與時間（若傳送的檔案含有數位簽章）、憑證簽章日期與時間、憑證發行者名稱、憑證持有人相關資訊、憑證的曝光數和公開金鑰，以及用來進行憑證運算的演算法、憑證序號。

- 執行程序的帳戶名稱。

- 執行程序的電腦名稱的總和檢查碼（MD5、SHA2-256、SHA1）。

- 處理程序視窗標題。

- 病毒資料庫 ID、已識別威脅在卡巴斯基分類下的名稱。

- 用於應用程式之授權的相關資訊、授權 ID、類型和失效日期。

- 提供資訊時電腦的當地時間。

- 程序存取的檔案名稱和路徑。

- 程序存取的 URL 及 IP 位址。

- 下載所執行檔案的 URL 及 IP 位址。

此外，為了實現聲明中所述的避免誤報之目的，權利持有人可能收取受信任的可執行及不可執行檔案或其部分。

閱讀卡巴斯基安全網路聲明

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在**進階**標籤上，點擊**顯示 KSN 聲明**。

Kaspersky Endpoint Security 將以下資訊儲存在偵錯檔案中：

- 有關裝置和作業系統的資訊（唯一的裝置 ID、裝置類型、網路裝置的 MAC 位址、作業系統類型、作業系統版本）。
- 有關應用程式及其模組的操作的資訊。
- 有關訂購（訂購類型、區域）的資訊。
- 有關語言區域設定、應用程式 ID、應用程式自訂、應用程式版本、唯一的應用程式安裝 ID、唯一電腦 ID 的資訊。
- 有關電腦惡意軟體防護狀態，以及所有已處理和已偵測到的物件的資訊（包含已偵測到的物件名稱、偵測的日期和時間、物件的下載網址、已感染檔案的名稱和大小及其路徑、攻擊電腦的 IP 位址和網路攻擊的目標電腦埠號、惡意軟體活動清單和不需要的網址），以及應用程式和使用者所做相關操作和決定的資訊。
- 有關使用者下載的應用程式的資訊（網址、內容、檔案大小、下載檔案的處理程序的相關資訊）。
- 有關啟動的應用程式及應用程式模組的資訊（大小、內容、建立日期、PE 標頭詳細資訊、區域、名稱、位置、封裝應用程式）。
- 有關介面錯誤和已安裝卡巴斯基的應用程式介面用法的資訊。
- 有關網路連線的資訊：遠端電腦和使用者電腦的 IP 位址、用於建立連線的埠號和連線的網路協定。
- 有關電腦透過 IT 與電信網路接收和傳送的網路封包的資訊。
- 有關傳送和接收的電子郵件和即時訊息的資訊。
- 有關存取的網址的資訊：使用開放式協定建立連線的時間、有關網站存取登入名稱和密碼的資料以及 Cookie 內容。
- 伺服器的公開憑證。

偵錯檔案只包含修復應用程式中的缺陷所需的資訊。卡巴斯基使用偵錯檔案調查與 Kaspersky Endpoint Security 操作中的錯誤相關的事件。

預設情況下，停用偵錯檔案的建立。您可以在應用程式設定中啟用偵錯檔案的建立。

偵錯檔案只能手動傳送到卡巴斯基。應用程式不會自動向卡巴斯基傳送偵錯檔案。

您可以選擇如何將偵錯檔案傳送到卡巴斯基。

在向卡巴斯基傳送偵錯檔案之前，請檢視它們包含的資料。

重要：偵錯檔案可能包含個人資訊或機密資訊。透過向卡巴斯基傳送偵錯檔案，您同意向卡巴斯基提供您傳送的偵錯檔案中包含的所有資料，並且您同意用於傳送它們的方法。

此外，可能會被入侵者用於危害電腦或資料的檔案或其某些部分也可傳送到卡巴斯基進行檢查。

卡巴斯基防護根據法律和適用的卡巴斯基規則收到的任何資訊。資料透過安全的管道傳輸。

加入卡巴斯基安全網路完全出於自願。在安裝應用程式時決定是否加入。您之後可隨時變更決定。

啟動 Kaspersky Endpoint Security

重要：在啟動 Kaspersky Endpoint Security 之前，請確保您電腦上設定的日期和時間與實際日期和時間相符。

啟動應用程式涉及向應用程式新增金鑰。

注意：啟動應用程式需要網際網路連線。

啟動試用版

1. 開啟應用程式主視窗。
2. 在主應用程式視窗的側欄上，點擊**產品授權**。

   產品授權視窗將開啟。
3. 在**產品授權**視窗中，點擊**啟動**。

   Kaspersky Endpoint Security 連線到卡巴斯基啟動伺服器並傳送資料進行驗證。如果驗證成功，應用程式將接收並新增免費試用訂購的金鑰。

   重要：只有在之前未曾在電腦上啟動 Kaspersky Endpoint Security 的前提下，才可以啟動該應用程式的試用版本。

使用啟動碼啟動應用程式

1. 開啟應用程式主視窗。
2. 在主應用程式視窗的側欄上，點擊**產品授權**。

   產品授權視窗將開啟。
3. 在**產品授權**視窗中，輸入您在購買 Kaspersky Endpoint Security 時收到的啟動碼。
4. 點擊**啟動**。

注意：啟動碼是一個由 20 個拉丁字母和數位組成的唯一組合，採用 xxxxx-xxxxx-xxxxx-xxxxx 形式。

應用程式連線到卡巴斯基啟動伺服器並傳送啟動碼以確認確實性。如果已成功驗證啟動碼，應用程式將自動接收並新增產品授權金鑰。

注意：根據您收到的啟動碼，您可能需要填寫註冊表。

如果啟動碼驗證失敗，則會顯示相應的通知。此時，請聯絡向您提供此啟動碼的軟體供應商。

使用啟動碼啟動應用程式後，您可在**產品授權**視窗中檢視以下資訊：

- 產品授權或訂購狀態
- 使用中的金鑰
- 備用金鑰（如果有）
- 產品授權類型以及您可以在目前產品授權或訂購下使用該應用程式的電腦數量
- 目前產品授權或訂購下可用的應用程式功能
- 產品授權到期日期和時間
- 距離產品授權到期的天數

檢視產品授權資訊

檢視產品授權資訊

1. 開啟應用程式主視窗。
2. 在主應用程式視窗的側欄上，點擊**產品授權**。

產品授權視窗將開啟。

產品授權視窗可能包含以下資訊：

- 產品授權或訂購狀態
- 使用中的金鑰
- 備用金鑰（如果有）
- 產品授權類型以及您可以在目前產品授權或訂購下使用該應用程式的電腦數量
- 目前產品授權或訂購下可用的應用程式功能
- 產品授權到期日期和時間
- 距離產品授權到期的天數

管理產品授權和訂購

如果與使用中的金鑰關聯的產品授權已過期且未新增備用金鑰，則必須續約產品授權。產品授權過期後，應用程式將繼續以有限的功能運作（更新、卡巴斯基安全網路、Web 控制和透過卡巴斯基安全管理中心進行的 FileVault 磁碟加密將無法使用）。您仍然可以使用所有應用程式元件和執行惡意軟體掃描，但只能使用產品授權到期之前安裝的惡意軟體防護資料庫。

重要提示：如果您的惡意軟體防護資料庫過時，您的電腦受到感染的風險就會增加。

續約產品授權

1. 在主應用程式視窗的側欄上，點擊**"防護中心"**。

   防護中心視窗開啟。

2. 在**防護中心**視窗中，點擊**續約**。

   一個網頁將開啟，顯示如何透過卡巴斯基線上商店或卡巴斯基合作夥伴續約產品授權的相關資訊。如果透過線上商店續約產品授權，在完成付款後，Kaspersky Endpoint Security 的啟動碼將被傳送到訂單中指定的電子郵件信箱。

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

如果您在無限制訂購下使用該應用程式，Kaspersky Endpoint Security 會續約您的訂購，無需您執行任何操作。

如果您在有限訂購下使用應用程式，且續約訂購的寬限期已結束，Kaspersky Endpoint Security 會通知您並停止嘗試自動續約訂購和更新應用程式資料庫。

您可以聯絡向您出售 Kaspersky Endpoint Security 的供應商來手動續約訂購。

續約訂購

1. 開啟應用程式主視窗。

2. 在主應用程式視窗的側欄上，點擊**產品授權**。

   產品授權視窗將開啟。

3. 在**產品授權**視窗中，點擊**造訪服務供應商網站**。

   您的服務提供者的網站將開啟。

您的訂購狀態可能變成已到期。此時，您需要手動更新訂購狀態。如果您目前沒有訂購，Kaspersky Endpoint Security 將停止更新應用程式資料庫（如果您訂購了更新）或停止防護電腦（如果您訂購了更新和防護）。

更新訂購狀態

1. 開啟應用程式主視窗。
2. 在主應用程式視窗的側欄上，點擊**產品授權**。
   產品授權視窗將開啟。
3. 在**產品授權**視窗中，點擊↻按鈕。

根據工作站產品授權類型比較應用程式功能

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

Kaspersky Endpoint Security 功能比較

功能	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert
進階威脅防護						
卡巴斯基安全網路	✓	✓	✓	✓	✓	✓
行為偵測	✓	✓	✓	✓	✓	✓
弱點利用防禦	✓	✓	✓	✓	✓	✓
修復引擎	✓	✓	✓	✓	✓	✓
關鍵威脅防護						
檔案威脅防護	✓	✓	✓	✓	✓	✓
Web 威脅防護	✓	✓	✓	✓	✓	✓
郵件威脅防護	✓	✓	✓	✓	✓	✓
防火牆	✓	✓	✓	✓	✓	✓
網路威脅防護	✓	✓	✓	✓	✓	✓
安全控制						
裝置控制	✓	✓	✓	✓	✓	✓
Web 控制	✓	✓	✓	✓	✓	✓
資料加密						
FileVault 磁碟加密	–	✓	✓	✓	✓	✓
Detection and Response						
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓
Kaspersky Sandbox *（Kaspersky Sandbox 產品授權必須單獨購買）*	✓	✓	✓	✓	✓	✓

執行一般工作

開啟和結束應用程式

安裝完畢後，應用程式將自動啟動，應用程式圖示會出現在功能表列中。

開啟應用程式

在功能表列中，點擊應用程式圖示，並選擇**Kaspersky Endpoint Security**。

結束應用程式

在功能表列上，點擊應用程式圖示並選擇**結束**。

結束應用程式後，應用程式處理程序將從電腦記憶體中刪除。

重要：結束 Kaspersky Endpoint Security 應用程式後，電腦將不再受防護，並可能感染病毒，從而使您的資料面臨遺失的危險。

檢視電腦防護的狀態

防護狀態指示器會告知您電腦防護方面的問題。這個指示器形狀像盾牌，位於 應用程式主視窗。此標誌的顏色可能隨電腦防護狀態而改變。如果 Kaspersky Endpoint Security 偵測到任何安全威脅，應用程式主視窗中會出現一條有關威脅的訊息，指示標誌的顏色也會改變。

指示標誌的顏色會發生如下變化：

- **綠色**。您的電腦受到適當的防護。

  綠色標誌表示惡意軟體防護資料庫為最新版本，所有應用程式元件已根據卡巴斯基建議進行設定。未偵測到惡意物件，或已解毒偵測到的任何惡意物件。

- **黃色**。電腦的防護層級下降。

  黃色標誌表示 Kaspersky Endpoint Security 發現問題。此類問題包括與建議的防護設定輕微差異或應用程式資料庫剛過期。

- **紅色**。電腦面臨感染危險。

  紅色標誌表示存在可能導致電腦感染和資料遺失的危險問題。例如，此惡意軟體防護應用程式資料庫嚴重過期、此應用程式未啟動或偵測到惡意物件。

  我們建議您盡快解決任何問題並處理安全威脅。

檢視已安裝元件的運行狀態

Kaspersky Endpoint Security 可讓您在**安全**視窗中檢查已安裝應用程式元件的狀態。每個元件名稱旁邊的指示器反映了其狀態。

檢視元件狀態

1. 開啟應用程式主視窗。
2. 在主應用程式視窗的側欄上，點擊**安全**。

   安全將開啟。

可能會顯示以下狀態指示器：

	元件正在執行。
	元件正在執行，由安全政策管理。
	元件發生故障。
	元件發生故障，由安全政策管理。
	元件已關閉。
	元件被關閉，由安全政策管理。
	元件已暫停。
	目前產品授權不支援該元件。

注意：對於某些元件，您也可以使用元件名稱旁邊的三點功能表來開啟報表或配置元件設定。

停用和還原電腦防護

預設情況下，Kaspersky Endpoint Security 會在作業系統啟動後啟動，並在關閉之前始終防護您的電腦。所有防護元件（檔案威脅防護、Web 威脅防護和網路威脅防護）均已啟用並正在執行。

您可以完全停用防護或停用特定的防護元件。

重要：卡巴斯基強烈建議不要停用防護或防護元件，因為停用可能導致電腦感染和資料遺失。

當電腦防護被停用時：

- 功能表列中的應用程式圖示為非活動狀態。
- 應用程式主視窗中的防護狀態指示標誌為紅色。

當一個或多個防護元件被停用時，防護狀態指示標誌為紅色或黃色。

注意：停用或暫停防護元件不會影響掃描工作或更新工作。

您可以透過採用以下方法之一停用/還原電腦防護：

- 從應用程式圖示
- 從應用程式設定視窗
- 從**防護**功能表

從應用程式圖示停用/還原電腦防護

1. 在功能表列中，點擊應用程式圖示並選擇**關閉防護/開啟防護**。
   當您關閉防護時，將出現管理員憑證的提示。
2. 當系統提示您輸入管理員憑證時，輸入管理員名稱和密碼並確認您要關閉防護。

從應用程式設定視窗停用/還原電腦防護

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在**基本**標籤的**一般**區域中，取消選中/選中**啟用防護**核取方塊。

從功能表列停用/還原電腦防護

在功能表列中，點擊**防護** > **關閉防護 / 開啟防護**。

重要：如果您停用電腦防護，Kaspersky Endpoint Security 再次啟動時它不會被自動重新啟用。您必須手動重新啟用防護元件。

停用防護元件

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在**基本**標籤上的**<元件名稱>**部分，取消選中**啟用<元件名稱>**核取方塊。

重要：如果停用防護元件，當 Kaspersky Endpoint Security 再次啟動時，該元件不會被自動重新啟用。您必須手動重新啟用防護元件。

啟用防護元件

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在**基本**標籤上的**<元件名稱>**部分，選中**啟用<元件名稱>**核取方塊。

要啟用電腦防護或防護元件，您還可以使用防護中心。停用電腦防護或停用防護元件會使您的電腦面臨更高的感染風險。這是電腦防護停用時防護中心會進行通知的原因。

使用防護中心

*防護中心*是 Kaspersky Endpoint Security 的功能，可幫助您分析並修復問題和電腦安全威脅。

開啟防護中心

在主應用程式視窗的側欄上，點擊**"防護中心"**。

在防護中心中，您可以查找有關活動威脅的資訊、檢視應用程式資料庫的狀態以及尋找是否已停用了任何元件防護。

注意：如果您組織的系統管理員啟用 Web 控制來封鎖對危險 Web 資源的存取，Kaspersky Endpoint Security 會在防護中心中顯示**Web 控制已啟用。**通知。

對於每個問題或威脅，Kaspersky Endpoint Security 會建議您可以執行的操作來解決問題或威脅。例如，如果 Kaspersky Endpoint Security 在電腦上偵測到受感染檔案，您可以點擊**解毒**。如果惡意軟體資料庫已過期，您可以點擊**更新**。您可立即修復問題或解毒威脅，也可以稍後執行操作。

立即修復問題或解毒威脅

點擊具有建議操作名稱的按鈕，以修復問題或解毒威脅。

應用程式即會執行所選操作。

如果不消除危險威脅就關閉防護中心，應用程式主視窗中的防護狀態指示標誌將保持為紅色，提醒您存在這些威脅。

執行掃描工作

Kaspersky Endpoint Security 中包含預設的完整掃描工作。在執行此工作時，該應用程式將掃描電腦的記憶體、啟動物件和所有內部磁碟機以確定是否存在病毒和其他惡意軟體。

執行電腦完整掃描

1. 在主應用程式視窗的側欄上，點擊**"掃描"**。

   掃描視窗將開啟。

2. 點擊 **完整掃描**按鈕。

   電腦的完整掃描將開啟。

Kaspersky Endpoint Security 中包含預設的快速掃描工作。在執行此工作時，該應用程式將掃描電腦的關鍵區域（記憶體、啟動物件和系統資料夾）以確定是否存在病毒和其他惡意軟體。

執行電腦快速掃描

1. 在主應用程式視窗的側欄上，點擊**"掃描"**。

   掃描視窗將開啟。

2. 點擊 **快速掃描**按鈕。

電腦的快速掃描將開啟。

如果您想要掃描單個物件（例如內部磁碟、資料夾、檔案或卸除式磁碟）是否有病毒和其他惡意軟體，您可以執行自訂掃描工作。

掃描所選項目

執行以下操作之一：

- 右鍵點擊選中的項目並選擇**掃描惡意軟體**。
- 將所選項目拖到 Dock 中的應用程式圖示。
- 拖動選中的項到**掃描**視窗。

可以在**報告**視窗中檢視已完成的掃描工作的結果。

注意： Kaspersky Endpoint Security 不會掃描位於 OneDrive 或 iCloud 儲存或其他雲端儲存中的檔案。請將這些檔案從掃描範圍中排除。否則，掃描工作可能會以*受感染檔案未刪除*錯誤結束。

配置排程掃描工作的自動啟動

您可以建立啟動快速掃描和完整掃描工作的排程。Kaspersky Endpoint Security 會根據配置的排程自動掃描整個電腦或電腦的指定區域。

從掃描視窗排程掃描工作

1. 在主應用程式視窗的側欄上，點擊**"掃描"**。

   掃描視窗將開啟。

2. 點擊**排程掃描**。

   將會開啟一個對話方塊，您可以在其中設定排程。

3. 選中**完整掃描**或**快速掃描**核取方塊。

4. 指定掃描頻率和掃描開始時間。

5. 點擊**OK**。

從額定視窗排程掃描工作

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。

   此時會開啟應用程式設定視窗。

2. 在**掃描**標籤上，點擊**排程**。

3. 在開啟的視窗中，選擇您要按排程掃描的工作名稱旁邊的核取方塊。

4. 設定掃描工作頻率和時間。

5. 點擊**OK**儲存變更。

您可以在**報告**視窗中檢視掃描工作結果。

更新應用程式資料庫

專用卡巴斯基更新伺服器是 Kaspersky Endpoint Security 更新的主要來源。Kaspersky Endpoint Security 也可以使用發佈點、本機資料夾或其他 Web 伺服器作為*更新來源*。

注意：從更新伺服器下載更新必須連線到網際網路。

預設情況下，Kaspersky Endpoint Security 定期檢查卡巴斯基更新伺服器上的更新。如果伺服器上有新的更新，Kaspersky Endpoint Security 將在背景下載更新，並將它們安裝到您的電腦上。

開始 Kaspersky Endpoint Security 更新

1. 在主應用程式視窗的側欄上，點擊**更新**。
   更新視窗將開啟。

2. 點擊**更新**。
   應用程式將檢查更新。如果更新可用，應用程式將下載並安裝到您的電腦上。

您也可以用以下方法之一啟動更新工作：

- 點擊應用程式圖示並選擇**更新**。
- 在功能表列中，選擇**防護 > 更新**。

您可以變更 Kaspersky Endpoint Security 更新應用程式資料庫的方式。預設情況下，應用程式會自動更新資料庫。

啟用/停用自動下載 Kaspersky Endpoint Security 資料庫更新

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。

2. 在**更新**標籤上的**資料庫**區域中，選中/取消選中**自動下載更新**核取方塊。

可以在**報告**視窗中檢視已完成的更新工作的結果。

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

檔案存取被封鎖時如何應對

Kaspersky Endpoint Security 可封鎖存取已感染的檔案和應用程式。如果某個檔案受到感染，必須先對其進行解毒才能存取該檔案。

解毒已偵測到的物件

1. 在功能表列中，**防護 > 偵測到的物件**。

   偵測到的物件視窗將開啟。

2. 在**偵測到的物件**部分，點擊所選檔案旁邊的 ••• ，然後選擇**解毒**。

   應用程式開始解毒選擇的物件。在進行解毒時，應用程式會顯示一個對話方塊，可以選擇將向物件執行的操作。

解毒所有已偵測到的物件

1. 在功能表列中，**防護 > 偵測到的物件**。

   偵測到的物件視窗將開啟。

2. 在**偵測到的物件**部分，點擊**解毒全部**按鈕。

   應用程式開始解毒已偵測到的物件。在進行解毒時，應用程式會顯示一個對話方塊，可以選擇將向物件執行的操作。在選擇了操作之後，如果在通知視窗中選中**套用到全部**核取方塊，則應用程式會將此操作套用到所有此類型的檔案。

如果您確信被檔案威脅防護封鎖的檔案是安全的，可以將其加入信任區域中。

還原已經被應用程式刪除或解毒的檔案

有時無法在解毒過程中完整儲存檔案。如果已解毒的檔案包含重要資訊，且這些資訊在解毒之後部分或完全無法存取，您可以嘗試從備份副本還原原始檔案。

還原已經被應用程式在解毒過程中刪除或修改的檔案

1. 在功能表列中，**防護 > 偵測到的物件**。

   偵測到的物件視窗將開啟。

2. 在**備份**部分中，點擊您要還原的檔案旁邊的 ••• 。

   彈出功能表將開啟。

3. 選擇**還原檔案**。

   一個視窗將開啟，用於指定檔案名稱、標籤以及檔案將被還原到的資料夾。預設情況下，已指定原始檔案名稱和位置。

4. 指定檔案名稱和檔案將被還原到的資料夾。

5. 點擊**儲存**。

應用程式將把檔案還原到具有指定名稱的指定位置。

還原檔案後，您需要立即掃描該檔案是否有惡意軟體。可以使用更新的資料庫對該物件進行解毒而不會損壞。

重要：建議您不要還原檔案的備份副本，除非還原它們是絕對必要的，因為這樣做可能會導致電腦感染。

檢視應用程式操作報告

您可以在**已處理的物件**標籤上檢視列出所有偵測到的物件的 Kaspersky Endpoint Security 報告。系統事件顯示在**系統事件**標籤上。此外，還會為以下每個應用程式元件建立單獨的詳細報告：檔案威脅防護、Web 威脅防護、網路威脅防護、行為偵測以及掃描和更新工作。

開啟報告視窗

在功能表列中，選擇**防護 > 報告**。

如果出現通知視窗該怎麼辦

應用程式通知以通知視窗的形式通知您需要注意的應用程式事件。

如果螢幕上出現通知，請選擇建議的選項之一。最佳選項是卡巴斯基專家設定的預設選項。

應用程式的進階設定

電腦防護範圍

Kaspersky Endpoint Security 偵測的物件按不同內容劃分為多種類別。應用程式始終會搜尋病毒、蠕蟲、木馬和惡意工具。這些應用程式可能會對電腦造成嚴重危害。為確保對您的電腦提供更可靠的防護，您可以透過允許應用程式檢查可能被入侵者利用來危害您的電腦或個人資料的合法軟體，來延伸可偵測物件的清單。

Kaspersky Endpoint Security 可防禦的物件按以下類別組成群組：

- **病毒、蠕蟲、木馬、惡意工具、廣告軟體和自動撥號軟體**

  此類別包括：

  - 所有類型的惡意軟體。
  - 透過在您的電腦上顯示廣告（例如，橫幅）或將瀏覽器中的搜尋結果取代為廣告網站，而給您造成不便的軟體。
  - 透過電腦的數據機偷偷建立電話連線的應用程式。

  對所有類型的惡意軟體進行防禦是最低的必需安全等級。按照卡巴斯基專家的建議，Kaspersky Endpoint Security 將始終監控屬於此類別的物件。

- **可以被入侵者利用以破壞您的電腦或個人資料的合法軟體**此類別包括可以被入侵者利用來危害您的電腦或個人資料的合法軟體，例如遠端管理應用程式。

選擇要偵測的物件類別

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。

   此時會開啟應用程式設定視窗。

2. 在**威脅**標籤的**要偵測的物件**部分，選中要偵測的物件類別旁邊的核取方塊。

> **注意：**Kaspersky Endpoint Security 會始終防護您的電腦免受病毒、蠕蟲、木馬、惡意工具、廣告軟體和自動撥號軟體的侵害。因此，無法取消選中此類別的核取方塊。

根據所選的要偵測的物件類別，Kaspersky Endpoint Security 在執行檔案威脅防護、 Web 威脅防護和掃描工作時使用部分或全部惡意軟體防護資料庫。

> **注意：**如果Kaspersky Endpoint Security 將某個應用程式歸類為惡意軟體，但您認為該應用程式是安全的，則可以將其新增到信任區域中。

*受信任區域*是一個物件清單，Kaspersky Endpoint Security 不會掃描或監控該清單中的物件。例如，如果 Kaspersky Endpoint Security 封鎖存取某個檔案、應用程式或網站，但您確信此檔案、應用程式或網址絕對安全，則需要將其新增到受信任區域中。

將某個應用程式新增到受信任區域後，將不再監控其檔案和網路活動（包括可疑活動）。但是， Kaspersky Endpoint Security 將仍然對受信任應用程式的可執行檔案和處理程序進行掃描。

注意：當管理員配置政策禁止編輯信任區域時，使用者無法進入信任區域設定。

向信任檔案和資料夾清單新增/刪除檔案或資料夾

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在**威脅**標籤的**排除項目**區域中，點擊**信任區域**。
   將會開啟受信任區域設定視窗。
3. 在**檔案和資料夾**索引標籤上，編輯受信任檔案和資料夾清單：
   - 向清單中新增檔案或資料夾：
     a. 點擊 + 。
     將會開啟一個可在其中選擇檔案或資料夾的對話方塊。
     b. 選擇要新增的檔案或資料夾。
     c. 點擊**開啟**。
   - 從清單中刪除檔案或資料夾：
     a. 選擇要從信任檔案和資料夾清單中刪除的檔案或資料夾。
     b. 點擊 – 。
4. 點擊**OK**。

向信任網址清單新增/刪除信任網址

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在**威脅**標籤的**排除項目**區域中，點擊**信任區域**。
   將會開啟受信任區域設定視窗。
   您也可以透過點擊**基本**索引標籤**一般**部分中的**信任區域**按鈕來開啟此視窗。
3. 在**網址**索引標籤上，編輯受信任網址的清單：
   - 向清單中新增網址：
     a. 點擊 + 。
     b. 輸入您想新增到清單中的網址。
     c. 點擊**OK**。

- 從清單中刪除網址：

  a. 選擇要刪除的網址。

  b. 點擊 – 。

4. 點擊**OK**。

預設情況下，信任網址清單為空。

新增/刪除信任應用程式到信任應用程式清單

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。

2. 在**威脅**標籤的**排除項目**區域中，點擊**信任區域**。
   將會開啟受信任區域設定視窗。
   您也可以透過點擊**基本**索引標籤**一般**部分中的**信任區域**按鈕來開啟此視窗。

3. 在**受信任應用程式**索引標籤上，編輯受信任應用程式清單：

   - 若要向清單中新增應用程式：

     a. 點擊 + 。
     一個視窗將開啟，您可以在其中指定所需應用程式的參數。

     b. 指定要新增的應用程式的以下參數：

     - **路徑**
     - **代碼簽章要求**

     > **注意：**您可以手動輸入這兩個參數的值，也可以點擊**選擇**按鈕並在開啟的視窗中選擇要新增的應用程式。在此情況下，這些參數的值會自動插入。

     c. 在**選項**部分中，至少選擇一種您不希望 Kaspersky Endpoint Security 應用程式監控的活動類型：

     - **不監控檔案活動**
     - **不監控網路活動**

     d. 點擊**OK**。

   - 要從清單中移除應用程式：

     a. 選擇您想要刪除的應用程式。

     b. 點擊 – 。

預設情況下，受信任應用程式清單為空。

編輯受信任應用程式

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在**威脅**標籤的**排除項目**區域中，點擊**信任區域**。
   將會開啟受信任區域設定視窗。
   您也可以透過點擊**基本**索引標籤**一般**部分中的**信任區域**按鈕來開啟此視窗。
3. 在**受信任應用程式**索引標籤上，選擇要編輯的應用程式。
4. 點擊**編輯**。
5. 在開啟的視窗中，編輯應用程式的參數。
6. 點擊**OK**。

啟用信任網址的監控

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在**威脅**標籤的**排除項目**區域中，點擊**信任區域**。
   將會開啟受信任區域設定視窗。
3. 在**網址**索引標籤上，取消選中您希望 Kaspersky Endpoint Security 應用程式監控的網址旁邊的核取方塊。
4. 點擊**OK**。

檔案威脅防護

檔案威脅防護可避免電腦的檔案系統受感染。該元件隨作業系統一起啟動，保留在電腦的記憶體中，會針對在您的電腦和所有連線的磁碟上開啟、儲存或執行的所有檔案進行惡意軟體掃描。如果您停用檔案威脅防護，它將不會在作業系統啟動時啟動。您必須手動重新啟用檔案威脅防護。

啟用/停用檔案威脅防護

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在**基本**標籤的**檔案威脅防護**部分，選中/取消選中**啟用檔案威脅防護**核取方塊。
   您也可以在防護中心中啟用檔案威脅防護。停用電腦防護或停用防護元件會使您的電腦面臨更高的感染風險。這是電腦防護停用時防護中心會進行通知的原因。

您可以建立檔案威脅防護的防護範圍。

向防護範圍中新增/從中刪除檔案或資料夾

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。

2. 在**基本**標籤的**檔案威脅防護**部分中，點擊**防護範圍**。

   一個視窗將開啟，其中包含檔案威脅防護掃描的物件清單。預設情況下，檔案威脅防護會掃描連線到您的電腦的內置磁碟、卸除式磁碟和網路磁碟中的所有物件。

   備註：您可以略過對只讀系統磁碟區的掃描以显著降低掃描時間。預設情況下，檔案威脅防護不掃描只讀系統磁碟區。

3. 在**防護範圍**區域，新增/刪除物件：

   - 向防護範圍中新增檔案或資料夾：

     a. 點擊+。

     將會開啟一個彈出功能表，可在其中選擇要新增到防護範圍中的物件。

     b. 在彈出功能表中，選擇**檔案和資料夾**項目。

     將會開啟一個可在其中選擇檔案或資料夾的對話方塊。

     c. 選擇您想新增到防護範圍中的檔案或資料夾。

     d. 點擊**開啟**。

   - 從防護範圍中刪除檔案或資料夾：

     a. 選擇防護範圍物件清單中的物件。

     b. 將所選物件從視窗中拖出或點擊–。

4. 如果您要掃描只讀系統磁碟區，在**最佳化**區域，取消選擇**略過掃描唯讀系統磁碟區**核取方塊。

   重要：最佳化可能由于安全原因而停用。

5. 點擊**儲存**。

在防護範圍中新增/刪除預設物件清單中的物件

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。

   此時會開啟應用程式設定視窗。

2. 在**基本**標籤的**檔案威脅防護**部分中，點擊**防護範圍**。

   一個視窗將開啟，其中包含檔案威脅防護掃描的物件清單。預設情況下，檔案威脅防護會掃描連線到您的電腦的內置磁碟、卸除式磁碟和網路磁碟中的所有物件。

   備註：您可以略過對只讀系統磁碟區的掃描以显著降低掃描時間。預設情況下，檔案威脅防護不掃描只讀系統磁碟區。

3. 在**防護範圍**區域，新增/刪除預設物件清單中的物件：

   - 將預設物件清單中的物件新增到防護範圍：

     a. 點擊 + 。
     將會開啟一個彈出功能表，可在其中選擇要新增到防護範圍中的物件。

     b. 在彈出功能表中，選擇您想要新增到防護範圍中的物件（例如**所有內置磁碟**）。

   - 在防護範圍中刪除預設物件清單中的物件：

     a. 選擇防護範圍物件清單中的物件。

     b. 將所選物件從視窗中拖出或點擊 – 。

4. 如果您要掃描只讀系統磁碟區，在**最佳化**區域，取消選擇**略過掃描唯讀系統磁碟區**核取方塊。

   重要：最佳化可能由于安全原因而停用。

5. 點擊**儲存**。

停用防護範圍中的物件防護

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。

2. 在**基本**標籤的**檔案威脅防護**部分中，點擊**防護範圍**。
   一個視窗將開啟，其中包含檔案威脅防護掃描的物件清單。預設情況下，檔案威脅防護會掃描連線到您的電腦的內置磁碟、卸除式磁碟和網路磁碟中的所有物件。

   備註：您可以略過對只讀系統磁碟區的掃描以显著降低掃描時間。預設情況下，檔案威脅防護不掃描只讀系統磁碟區。

3. 取消選中防護範圍物件清單中物件旁邊的核取方塊。

4. 點擊**儲存**。

啟用對只讀系統磁碟區的掃描

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。

2. 在**基本**標籤的**檔案威脅防護**部分中，點擊**防護範圍**。
   一個視窗將開啟，其中包含檔案威脅防護掃描的物件清單。預設情況下，檔案威脅防護會掃描連線到您的電腦的內置磁碟、卸除式磁碟和網路磁碟中的所有物件。

   備註：您可以略過對只讀系統磁碟區的掃描以显著降低掃描時間。預設情況下，檔案威脅防護不掃描只讀系統磁碟區。

3. 在**最佳化**區域，取消選擇**略過掃描唯讀系統磁碟區**核取方塊。

重要：最佳化可能由于安全原因而停用。

4. 點擊**儲存**。

當您或應用程式嘗試存取防護範圍內的某個檔案時，檔案威脅防護會檢查 iSwift 資料庫是否包含有關此檔案的資訊，並使用此資訊確定是否需要掃描檔案。

由於使用了*特徵碼分析*（一種基於惡意軟體防護資料庫中的威脅描述來搜尋威脅的方法），因此可識別惡意物件。除特徵碼分析外，檔案威脅防護還使用啟發式分析和其他掃描技術。

如果在檔案中偵測到威脅，Kaspersky Endpoint Security 會識別偵測到的惡意軟體的類型（例如*病毒*或*木馬*）。然後，應用程式會顯示有關偵測到的物件的通知，並根據您的檔案威脅防護設定對該物件執行操作。

選擇檔案威脅防護在偵測到受感染檔案後執行的操作

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在**基本**部分的**檔案威脅防護**標籤，選擇檔案威脅防護在偵測到受感染檔案後執行的操作。

嘗試解毒或刪除受感染檔案之前，卡巴斯基應用程式會儲存檔案的備份副本，以供在以後還原或刪除該檔案。

有關檔案威脅防護和已偵測到的物件資訊會記錄在報告中。

注意：如果檔案威脅防護在出現錯誤後停止執行，您可檢視報告並嘗試重新啟動此元件。如果問題未解決，您可以聯絡卡巴斯基技術支援。

檢視檔案威脅防護報告

1. 在功能表列中，選擇**防護 > 報告**。
   報告視窗將開啟。
2. 開啟**檔案威脅防護**標籤。

Web 威脅防護

使用網際網路時，您的電腦會暴露於受惡意軟體和其他電腦安全威脅感染的風險之中。在您下載免費應用程式或存取已被駭客攻擊的網站時，電腦安全威脅可能會滲透到您的電腦中。此外，網路蠕蟲甚至可以在您開啟網址或下載檔案之前，在您的電腦連線到網際網路時立即攻擊您的電腦。

Kaspersky Endpoint Security 防護您的電腦透過 Safari、Chrome 或 Firefox 以 HTTP 和 HTTPS 協定傳送和接收的資訊。

注意： Kaspersky Endpoint Security 監控最常用於 HTTP 和 HTTPS 資料傳輸的連接埠上的 Web 流量。只有在選取**檢查安全連線 (HTTPS)**部分中的**一般** HTTPS)。

啟用/停用 Web 威脅防護

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。

   此時會開啟應用程式設定視窗。

2. 在**基本**標籤的**Web 威脅防護**部分，選中/取消選中**啟用Web 威脅防護**核取方塊。

您也可以透過防護中心啟用 Web 威脅防護。停用電腦防護或停用防護元件會使您的電腦面臨更高的感染風險。這是電腦防護停用時防護中心會進行通知的原因。

重要：如果您停用 Web 威脅防護，在重新啟動 Kaspersky Endpoint Security 或作業系統後不會自動重新啟用該功能。您必須手動重新啟用 Web 威脅防護。

Web 威脅防護使用卡巴斯基建議的設定來掃描Web 流量。透過使用特徵碼分析、啟發式分析和來自卡巴斯基安全網路的資料識別惡意物件。

透過檢查網站上的連結是否為釣魚威脅和惡意網址，可以避免受到*釣魚攻擊*。*釣魚攻擊*通常以入侵者的電子郵件形式或入侵者假裝成金融機構（例如銀行），並傳送詐欺網站的連結。在這些電子郵件中，入侵者試圖誘騙使用者存取釣魚網站和輸入機密資訊（例如，金融卡號或您的網上銀行帳戶的名稱和密碼）。例如，釣魚攻擊可以偽裝成來自您銀行的、包含其官網連結的訊息，但實際上連結會將您帶到由騙子建立的以假亂真的假冒銀行官網。

Web 威脅防護可以監控 Web 流量以確定存取釣魚網站的嘗試，並封鎖對此類網站的存取。Kaspersky Endpoint Security 使用應用程式資料庫、啟發式分析和來自卡巴斯基安全網路的資料檢查網站上的連結是否釣魚威脅和惡意網址。

Web 流量掃描演算法

Web 威脅防護會防護您或應用程式透過 HTTP 和 HTTPS 協定存取的每個網頁或檔案，並對其進行惡意代碼掃描：

- 如果網站或檔案包含惡意代碼，Kaspersky Endpoint Security 將會封鎖它並顯示通知，指出請求的檔案或網站已被感染。
- 如果檔案或網頁不包含惡意代碼，您可立即存取。

選擇 Web 威脅防護在偵測到危險 Web 流量物件後執行的操作

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。

   此時會開啟應用程式設定視窗。

2. 在**基本**標籤的**Web 威脅防護**部分中，選擇 Web 威脅防護在偵測到危險 Web 流量物件後執行的操作。

有關 Web 威脅防護和所有偵測到的危險 Web 流量物件的資訊記錄在報告中。

注意：如果 Web 威脅防護在出現錯誤後停止執行，您可檢視 Web 威脅防護報告並嘗試重新啟動此元件。如果問題未解決，您可以聯絡卡巴斯基技術支援。

檢視 Web 威脅防護報告

1. 在功能表列中，選擇**防護** > **報告**。

   報告視窗將開啟。

2. 開啟**Web 威脅防護**標籤。

郵件威脅防護

郵件威脅防護元件會掃描傳入和傳出的電子郵件訊息的附件以查找病毒和其他威脅。該元件借助惡意軟體防護資料庫、卡巴斯基安全網路雲端服務和啟發式分析提供電腦保護。

該應用程式支援以下郵件用戶端：Apple Mail、Microsoft Outlook、Mozilla Thunderbird、Canary Mail、Spark、Mimestream、Airmail、Post Box、Boxy Suite 2、Twobird、Shift、Clean Email、eM Client、Superhuman、Polymail、HEY、Mail+ for Gmail、Spike mail。

預設啟用郵件威脅防護。如有必要，您可以停用郵件威脅防護。

根據所選的作業模式，郵件威脅防護將執行以下操作：

- **自動刪除惡意物件**。如果選擇此選項，當 Kaspersky Endpoint Security 在電子郵件中偵測到受感染物件時，它會刪除受感染物件，並用文字"The requested file infected with<virus name>has been deleted"取代物件的內容。

- **自動封鎖惡意物件**。如果選擇此選項，當 Kaspersky Endpoint Security在電子郵件中偵測到受感染物件時，它會將電子郵件主旨替換為"Message is infected:<original subject>"，其中<original subject>是原始主旨。僅為 POP3 協定取代電子郵件訊息主旨。

使用網頁主控台啟用/停用郵件威脅防護

1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。

2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。

3. 選取"**應用程式設定**"標籤。

4. 前往 **通訊與 Web 防護 → 郵件威脅防護**。

5. 使用**郵件威脅防護**撥動開關啟用或停用該元件。

6. 如果啟用了郵件威脅防護，請選擇偵測到惡意軟體時應用程式執行的操作：

   - **刪除**

   - **封鎖**

7. 如果有必要，在 **進階設定** 部分配置檢查檔案的時間限製或掃描檔案的最大大小。

8. 存儲變更。

使用管理主控台啟用/停用郵件威脅防護

1. 啟動管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，點擊**"受管理裝置"**。
4. 在工作區選擇**"政策"**標籤。
5. 右鍵點擊要設定的政策並選擇**內容**。
6. 在 **屬性** 視窗中，選擇 **關鍵威脅防護** > **郵件威脅防護**。
7. 選擇或取消選擇 **啟用郵件威脅防護** 核取方塊。
8. 在 **偵測到威脅後的動作** 部分，選擇當 Kaspersky Endpoint Security 偵測到威脅時要執行的操作。
9. 如果有必要，在 **郵件威脅防護設定** 部分配置檢查檔案的時間限製或掃描檔案的最大大小。
10. 點擊**"確定"**儲存變更。
11. 執行下列操作之一以套用政策變更：
    - 儲存變更後，點擊**套用**以保留在**內容：<政策名稱>**視窗中。
    - 儲存變更後，點擊**確定**關閉**內容：<政策名稱>**視窗。

使用 Kaspersky Endpoint Security 應用程式啟用/停用郵件威脅防護

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在**基本**標籤的**郵件威脅防護**部分，選中/取消選中**啟用郵件威脅防護**核取方塊。
3. 如果選擇 **啟用郵件威脅防護** 核取方塊，選擇當 Kaspersky Endpoint Security 偵測到威脅時要執行的操作。
4. 如果有必要，配置檢查檔案的時間限製或掃描檔案的最大大小。

檢視郵件威脅防護報告

1. 在功能表列中，選擇**防護** > **報告**。
   報告視窗將開啟。
2. 開啟**郵件威脅防護**標籤。

網路威脅防護

Kaspersky Endpoint Security 可防護您的電腦免受網路攻擊。

*網路攻擊*是為了入侵遠端電腦的作業系統。入侵者進行網路攻擊是為了建立對作業系統的控制，導致作業系統拒絕服務或存取機密資訊。為了實現這些目的，入侵者可以發動直接攻擊，例如連接埠掃描和暴力破解，也可以使用安裝在受攻擊電腦上的惡意軟體。

網路攻擊可以分為以下類型：

- *連接埠掃描*。此類網路攻擊通常是為進行更加危險的網路攻擊做準備。入侵者掃描在目標電腦上使用網路服務的 UDP/TCP 連接埠，並確定目標電腦受到其他更危險類型的網路攻擊的弱點。透過連接埠掃描，入侵者還可以確定目標電腦上的作業系統，選擇適用於此類作業系統的網路攻擊。

- *DoS 攻擊*，即導致拒絕服務的網路攻擊。此類網路攻擊使目標作業系統變得不穩定或完全無法執行。

  存在以下主要的 DoS 攻擊類型：

  - 傳輸經過專門設計但並非目標電腦所需要的網路封包，導致目標作業系統執行出錯或崩潰。

  - 短時間內向遠端電腦傳送大量網路封包。目標電腦的所有資源都用於處理入侵者傳送的網路封包。從而導致電腦停止執行其功能。

- *網路入侵攻擊*。此類網路攻擊用於"劫持"目標電腦的作業系統。這是最危險的一類網路攻擊，因為如果成功，入侵者可以完全控制作業系統。

  當入侵者需要從遠端電腦獲取機密資料（例如，金融卡號和密碼），或將遠端電腦秘密用於入侵目的（例如，透過該電腦對其他電腦發起攻擊）時，會使用此類網路攻擊。

啟用/停用網路威脅防護

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。

   此時會開啟應用程式設定視窗。

2. 在**基本**標籤的**網路威脅防護**部分，選中/取消選中**啟用網路威脅防護**核取方塊。

您也可以在防護中心中啟用網路威脅防護。停用電腦防護或停用防護元件會使您的電腦面臨更高的感染風險。這是電腦防護停用時防護中心會進行通知的原因。

重要：如果您停用網路威脅防護，在重新啟動 Kaspersky Endpoint Security 或作業系統後不會自動重新啟用該功能。您必須手動重新啟用網路威脅防護。

當應用程式偵測到危險的網路活動時，Kaspersky Endpoint Security 會自動將發動攻擊的電腦 IP 位址新增到被封鎖的電腦清單，除非發動攻擊的電腦位於受信任電腦清單。

編輯被封鎖的電腦清單

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。

   此時會開啟應用程式設定視窗。

2. 在**基本**標籤的**網路威脅防護**部分中，勾選**啟用網路威脅防護**核取方塊。

3. 點擊**設定**。

   開啟一個包含受信任電腦清單和被封鎖電腦清單的視窗。

4. 開啟**被封鎖的電腦**標籤。

5. 如果您確定被封鎖電腦不是威脅，則在清單中選擇該電腦 IP 位址，然後點擊**解除封鎖**。

   將開啟確認對話方塊。

6. 在確認視窗中，執行以下操作之一：

   - 要解除對電腦的封鎖，請點擊**解除封鎖**。

     Kaspersky Endpoint Security 將解鎖 IP 位址。

   - 如果您希望 Kaspersky Endpoint Security 從不封鎖選定的 IP 位址，請點擊**解除封鎖並排除**。

     Kaspersky Endpoint Security 會解除對 IP 位址的封鎖，並將其新增到受信任電腦清單。

7. 點擊**儲存**。

您可以建立和編輯受信任電腦清單。Kaspersky Endpoint Security 應用程式不會封鎖這些電腦 IP 位址，甚至在這些電腦上偵測到危險網路活動時也是如此。

編輯受信任電腦清單

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。

   此時會開啟應用程式設定視窗。

2. 在**基本**標籤的**網路威脅防護**部分中，勾選**啟用網路威脅防護**核取方塊。

3. 點擊**設定**。

   開啟一個包含受信任電腦清單和被封鎖電腦清單的視窗。

4. 開啟**受信任電腦**標籤。

5. 編輯受信任電腦清單：

   - 將 IP 位址新增到受信任電腦清單中：

     a. 點擊 + 。

     b. 在出現的欄位中，輸入您認為是安全的電腦 IP 位址。

   - 從受信任電腦清單中刪除 IP 位址：

     a. 選擇清單中的 IP 位址。

     b. 點擊 – 。

   - 編輯受信任電腦清單中的 IP 位址：

     a. 選擇清單中的 IP 位址。

     b. 點擊**編輯**。

     c. 變更 IP 位址。

6. 點擊**儲存**。

偵測到網路攻擊時，Kaspersky Endpoint Security 會在報告中記錄有關攻擊的資訊。

注意：如果網路威脅防護元件在出現錯誤後停止執行，可檢視報告並嘗試重新啟動此元件。如果問題未解決，您可以聯絡卡巴斯基技術支援。

檢視網路威脅防護報告

1. 在功能表列中，選擇**防護** > **報告**。

   報告視窗將開啟。

2. 開啟**網路威脅防護**標籤。

防火牆

防火牆可在網際網路或者本機網路上工作時封鎖未經授權連線到電腦。這使您可以防護企業區域網路免受身分盜竊和其他攻擊。該元件借助惡意軟體防護資料庫、卡巴斯基安全網路雲端服務和預定義網路規則提供電腦保護。

網路規則優先順序

每條規則都有一個優先順序。規則在清單中的位置越高，其優先順序就越高。如果將網路活動新增至多條規則中，防火牆將根據優先順序最高的規則來規範網路活動。

網路連線類型

防火牆可讓您根據網路連線類型控製網路活動。您可以在 Kaspersky Endpoint Security 設定中變更網路連線的類型。

有以下網路連線類型可用：

- **公共網路**。網路不受惡意軟體防護應用程式、防火牆或過濾器（例如咖啡館中的 Wi-Fi）的防護。當使用者操作連線到此類網路的電腦時，防火牆會阻止對該電腦的檔案和印表機的存取。外部使用者也無法透過共用資料夾和遠端存取此電腦的桌面來存取資料。防火牆預設將公共網路類型指派給網際網路。您無法變更網際網路的類型。

- **本機網路**。為對此電腦上的檔案和印表機具有受限存取權限的使用者提供的網路（例如企業 LAN 或家庭網路）。

- **受信任網路**。安全的網絡，其中的電腦不會受到攻擊或未經授權的資料存取嘗試。防火牆允許具有此狀態的網路內的任何網路活動。

在管理主控台中管理防火牆元件

1. 啟動管理主控台。

2. 最大化**管理伺服器<伺服器名稱>**節點。

3. 在主控台樹狀目錄中，點擊**"受管理裝置"**。

4. 在工作區選擇**"政策"**標籤。

5. 右鍵點擊要設定的政策並選擇**內容**。

6. 在 **屬性** 視窗中，選擇 **關鍵威脅防護 > 防火牆**。

7. 選擇或取消選擇**啟用防火牆**核取方塊。

8. 在 **防火牆設定** 部分，點擊 **設定** 按鈕並新增、編輯、刪除或變更規則的優先順序。

9. 在 **可用網路** 部分，點擊 **設定** 按鈕並新增、編輯、刪除或變更網路類型。

10. 點擊**"確定"**儲存變更。

11. 執行下列操作之一以套用政策變更：

    - 儲存變更後，點擊**套用**以保留在**內容：<政策名稱>**視窗中。
    - 儲存變更後，點擊**確定**關閉**內容：<政策名稱>**視窗。

在 Web 主控台中管理防火牆元件

1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。

2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。

3. 選取"**應用程式設定**"標籤。

4. 前往 **通訊與 Web 防護 → 防火牆**。

5. 使用**防火牆**撥動開關啟用或停用該元件。

6. 在 **防火牆設定** 部分，點擊 **網路封包規則** 按鈕並新增、編輯、刪除或變更規則的優先順序。

7. 在 **可用網路** 部分，點擊 **網路設定** 按鈕並新增、編輯或變更網路類型。

8. 存儲變更。

管理 Kaspersky Endpoint Security 應用程式中的防火牆元件

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。

2. 在**基本**標籤的**防火牆**區域中，取消選中/選中**啟用防火牆**核取方塊。

3. 如果需要，點擊 **設定** 按鈕並配置防火牆設定：

    - 在 **網路封包規則** 頁簽上，您可以新增、編輯、刪除或變更規則的優先順序。
    - 在 **可用網路** 頁簽上，您可以新增、編輯或變更網路的類型。

因此，如果啟用了防火牆，Kaspersky Endpoint Security 將會控製網路活動並阻止未經授權的網路連線您的電腦。

檢視防火牆報告

1. 在功能表列中，選擇**防護** > **報告**。

   報告視窗將開啟。

2. 開啟**防火牆**頁簽。

行為偵測

行為偵測元件接收有關電腦上應用程式操作的資料，並將此資訊提供給其他防護元件以提高其效能。行為偵測元件使用應用程式的行為串流簽章 (BSS)。如果應用程式活動與行為串流簽章比對，Kaspersky Endpoint Security 將執行選定的回應操作。根據危險活動行為流簽章的 Kaspersky Endpoint Security 功能為電腦提供主動防禦。

預設情況下，行為偵測已啟用並以卡巴斯基專家建議的模式執行。如有必要，您可以停用行為偵測。

使用網頁主控台啟用/停用行為偵測

1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。

2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。

3. 選取"**應用程式設定**"標籤。

4. 前往 **主機威脅防護 → 行為分析 → 行為偵測** 部分。

5. 使用**行為偵測**撥動開關啟用或停用該元件。

6. 如果啟用了行為偵測，請選擇在偵測到惡意軟體活動時執行下列操作之一：

   - **封鎖**

     如果選擇此選項，Kaspersky Endpoint Security 應用程式將在偵測惡意活動時終止應用程式。

   - **刪除**

     如果選擇此選項，Kaspersky Endpoint Security 會在偵測惡意活動時刪除惡意應用程式的可執行檔案，並在備份中建立該檔案的備份副本。

   - **提示操作**

     如果選擇此選項，則當偵測到惡意軟體活動時，Kaspersky Endpoint Security 應用程式將顯示一個通知視窗，其中包含有關惡意物件的資訊，並提示使用者選擇 Kaspersky Endpoint Security 應用程式要採取的操作。可用的操作可能因物件狀態的不同而有所不同。

7. 如果啟用了行為偵測和防護共用資料夾抵禦外部加密，請選擇在偵測到外部加密時要執行的以下操作之一：

   - **通知**

     如果選擇此選項，當偵測到嘗試修改共用資料夾中的檔案時，Kaspersky Endpoint Security 應用程式將新增關於此嘗試的資訊到活動威脅清單，新增項目到本機應用程式報告，並將偵測到的惡意活動的相關資訊傳送到卡巴斯基安全管理中心。

- **封鎖攻擊裝置**

  如果選擇此選項，當 Kaspersky Endpoint Security 應用程式偵測到嘗試修改共用資料夾中的檔案時，它將封鎖存取發起惡意活動的工作階段的檔案修改（只讀），並建立被修改檔案的備份副本。

8. 存儲變更。

使用管理主控台啟用/停用行為偵測

1. 啟動管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，點擊**"受管理裝置"**。
4. 在工作區選擇**"政策"**標籤。
5. 右鍵點擊要設定的政策並選擇**內容**。
6. 在**屬性**視窗中，選擇**進階威脅防護>行為偵測**
7. 選擇或取消選擇**啟用行為偵測**核取方塊。
8. 如有必要，在**偵測到惡意軟體活動時的動作**部分中，選擇偵測到惡意軟體活動時要執行的操作。
9. 點擊**"確定"**儲存變更。
10. 執行下列操作之一以套用政策變更：

    - 儲存變更後，點擊**套用**以保留在**內容：<政策名稱>**視窗中。
    - 儲存變更後，點擊**確定**關閉**內容：<政策名稱>**視窗。

使用 Kaspersky Endpoint Security 應用程式啟用/停用行為偵測

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在**進階**索引標籤的"行為偵測"部分中，選擇或取消選擇**啟用行為偵測**核取方塊。
3. 如果勾選**啟用行為偵測**核取方塊，請選擇在偵測到惡意軟體活動時要執行的下列操作之一：

    - **封鎖**

      如果選擇此選項，Kaspersky Endpoint Security 應用程式將在偵測惡意活動時終止應用程式。

    - **刪除**

      如果選擇此選項，Kaspersky Endpoint Security 會在偵測惡意活動時刪除惡意應用程式的可執行檔案，並在備份中建立該檔案的備份副本。

    - **提示操作**

      如果選擇此選項，則當偵測到惡意軟體活動時，Kaspersky Endpoint Security 應用程式將顯示一個通知視窗，其中包含有關惡意物件的資訊，並提示使用者選擇 Kaspersky Endpoint Security 應用程式要採取的操作。可用的操作可能因物件狀態的不同而有所不同。

因此，如果啟用行為偵測，Kaspersky Endpoint Security 將使用行為串流簽章來分析應用程式在作業系統中的活動。

重要提示：除非絕對必要，否則我們不建議停用行為偵測，因為這樣做會降低防護元件的有效性。為了偵測威脅，防護元件可以請求行為偵測元件收集的資料。

掃描

檔案威脅防護 和 Web 威脅防護 提供即時電腦防護。我們也建議您定期掃描電腦，以檢查是否有惡意軟體和其他電腦安全威脅。執行電腦掃描對於防止未被防護元件偵測到的惡意軟體的擴張十分必要。

Kaspersky Endpoint Security 包含以下內建的掃描工作：

- **完整掃描**。

  電腦記憶體、啟動物件和所有內置磁碟的惡意軟體掃描。

- **快速掃描**。

  僅對電腦的關鍵區域執行惡意軟體掃描：記憶體、啟動物件和系統資料夾。

- **自訂掃描**。

  對指定物件（檔案、資料夾、內置磁碟或可拆卸磁碟）執行惡意軟體掃描。

- **外部磁碟掃描**

  當電腦連線到外部磁碟時，將執行外部磁碟惡意軟體掃描。

當應用程式執行病毒掃描時，將透過特徵碼分析識別惡意物件。除特徵碼分析外，Kaspersky Endpoint Security 還使用啟發式分析和其他掃描技術。

掃描視窗顯示有關每個正在執行的掃描工作的進度資訊（完成百分比和剩餘時間）以及掃描歷史記錄（100 個最近的掃描工作）。

開始完整掃描和快速掃描工作

1. 在主應用程式視窗的側欄上，點擊**"掃描"**。

   掃描視窗將開啟。

2. 在**掃描**視窗中，點擊**完整掃描**或**快速掃描**按鈕。

掃描工作開始。

啟動自訂掃描工作

1. 在主應用程式視窗的側欄上，點擊**"掃描"**。

   掃描視窗將開啟。

2. 若要啟動**自訂掃描**工作，請執行下列操作之一：

   - 將檔案或資料夾拖曳到視窗上。
   - 點擊**選擇**並開啟檔案或資料夾。

   掃描工作開始。

停止掃描工作

1. 在主應用程式視窗的側欄上，點擊**"掃描"**。
   掃描視窗將開啟。
2. 在**掃描**視窗中，點擊您想要停止的掃描工作旁邊的停止按鈕 ( )。
   將開啟確認對話方塊。
3. 在確認對話方塊中，點擊**停止**。

   掃描工作將停止。

您可以安排完整掃描或快速掃描工作。

從掃描視窗排程掃描工作

1. 在主應用程式視窗的側欄上，點擊**"掃描"**。
   掃描視窗將開啟。
2. 點擊**排程掃描**。
   將會開啟一個對話方塊，您可以在其中設定排程。
3. 選中**完整掃描**或**快速掃描**核取方塊。
4. 指定掃描頻率和掃描開始時間。
5. 點擊**OK**。

從額定視窗排程掃描工作

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在**掃描**標籤上，點擊**排程**。
3. 在開啟的視窗中，選擇您要按排程掃描的工作名稱旁邊的核取方塊。
4. 設定掃描工作頻率和時間。
5. 點擊**OK**儲存變更。

當電腦連線到外部磁碟時，Kaspersky Endpoint Security 應用程式將會自動開始掃描、提示掃描或不執行任何操作。您可以在外部磁碟掃描工作的設定中選擇一個選項。

選擇當電腦連線到外部磁碟時，Kaspersky Endpoint Security 應用程式執行的操作

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在**掃描**標籤左側的清單中，選擇**外部磁碟掃描**。
3. 在**連線了外部磁碟時**部分，選擇連線到外部磁碟時 Kaspersky Endpoint Security 執行的操作。

完整掃描和快速掃描工作已包含掃描範圍。在執行完整掃描工作時，Kaspersky Endpoint Security 應用程式將掃描電腦的記憶體、啟動物件和所有內置磁碟。在執行快速掃描工作時，應用程式將掃描電腦記憶體、啟動物件和系統資料夾。您可以變更快速掃描工作的掃描範圍。

備註：您可以略過對只讀系統磁碟區的掃描以显著降低掃描時間。預設情況下，Kaspersky Endpoint Security 在執行快速掃描工作時不掃描只讀系統磁碟區，但在執行完整掃描工作時掃描只讀系統磁碟區。

注意： Kaspersky Endpoint Security 不會掃描位於 OneDrive 或 iCloud 儲存或其他雲端儲存中的檔案。請將這些檔案從掃描範圍中排除。否則，掃描工作可能會以*受感染檔案未刪除*錯誤結束。

啟用/停用對只讀系統磁碟區的掃描

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在**掃描**標籤左側的清單中，選擇**完整掃描**或**快速掃描**工作。
3. 在**最佳化**區域，取消選擇/選擇**略過掃描唯讀系統磁碟區**核取方塊。

重要：最佳化可能由于安全原因而停用。

在快速掃描工作的掃描範圍中新增/刪除檔案或資料夾

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在**掃描**標籤左側的清單中，選擇**快速掃描**工作。
3. 在**掃描範圍**部分，點擊**編輯**。
   一個視窗將會開啟，其中包含快速掃描工作掃描範圍中的物件清單。
4. 編輯掃描範圍物件的清單：
   - 向快速掃描工作的掃描範圍新增檔案或資料夾：
     a. 點擊 + 。
        將會出現一個彈出功能表，可在其中選擇要新增到掃描範圍中的物件。
     b. 選擇**檔案和資料夾**項目。
        將會開啟一個可在其中選擇檔案或資料夾的對話方塊。

c. 選擇您想要新增到快速掃描工作的掃描範圍中的檔案或資料夾。

d. 點擊**開啟**。

- 從快速掃描工作的掃描範圍中刪除檔案或資料夾：

a. 選擇您想要刪除的物件。

b. 將所選物件從視窗中拖出或點擊 _ 。

5. 點擊**儲存**。

將預設快速掃描清單上的物件新增到快速掃描工作的掃描範圍

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在**掃描**標籤左側的清單中，選擇**快速掃描**工作。
3. 在**掃描範圍**部分，點擊**編輯**。
   一個視窗將開啟，其中包含掃描範圍物件的清單。
4. 點擊 + 。
   將會出現一個彈出功能表，可在其中選擇要新增到掃描範圍中的物件。
5. 在彈出功能表中，選擇您想要新增到掃描範圍中的物件（例如**記憶體**）。
6. 點擊**OK**。

停用快速掃描工作掃描範圍中的物件的防護

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在**掃描**標籤左側的清單中，選擇**快速掃描**工作。
3. 在**掃描範圍**部分，點擊**編輯**。
   一個視窗將開啟，其中包含掃描範圍物件的清單。
4. 取消選中掃描範圍物件清單中物件旁邊的核取方塊。
5. 點擊**OK**。

如果在檔案中偵測到威脅，應用程式將顯示一個通知並對此物件執行指定的操作。您可以修訂偵測到物件時要執行的操作。

選擇 Kaspersky Endpoint Security 在偵測到已感染檔案後的操作

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在**掃描**標籤，選擇工作清單中的一項工作。
3. 在**動作**部分，選擇應用程式在偵測到已感染檔案後的操作。

在解毒或刪除受感染檔案之前，Kaspersky Endpoint Security 會在備份中儲存該檔案的副本，以便您可以在必要時還原原始檔案。

有關掃描工作的結果和所有已偵測到的物件的資訊記錄在報告中。

注意：如果執行惡意軟體掃描工作時遇到任何錯誤，請重新啟動該工作。如果重新嘗試執行掃描仍然導致錯誤，請與卡巴斯基技術支援聯絡。

檢視掃描工作報告

1. 在功能表列中，選擇**防護 > 報告**。

   報告視窗將開啟。

2. 開啟**掃描**標籤。

更新工作

及時更新應用程式資料庫可確保您的電腦始終處於受防護狀態。檔案威脅防護、Web 威脅防護和掃描工作使用應用程式資料庫來偵測和消除電腦上的惡意軟體。應用程式資料庫定期更新，並加入不同種類的威脅資訊和解毒威脅的方法，因此定時更新資料庫非常重要。

Kaspersky Endpoint Security 將從卡巴斯基更新伺服器下載應用程式資料庫和新的應用程式模組，並安裝到您的電腦。Kaspersky Endpoint Security 也可以使用發佈點、本機資料夾或其他 Web 伺服器。

注意：連線到更新伺服器和下載更新必須存取網際網路。如果透過代理伺服器連線到網際網路，則可能需要設定網路設定。

可以採用以下方法之一下載應用程式資料庫更新：

- **自動**。Kaspersky Endpoint Security 會定期檢查卡巴斯基更新伺服器上的更新。如果更新伺服器上存在新的更新，Kaspersky Endpoint Security 將在背景下載此更新，並將其安裝到您的電腦。預設啟用此選項。
- **手動**。您可以隨時手動檢查 Kaspersky Endpoint Security 更新。

啟用/停用自動下載 Kaspersky Endpoint Security 資料庫更新

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。

   此時會開啟應用程式設定視窗。

2. 在**更新**標籤上的**資料庫**區域中，選中/取消選中**自動下載更新**核取方塊。

檢查 Kaspersky Endpoint Security 資料庫更新

1. 在主應用程式視窗的側欄上，點擊**更新**。

   更新視窗將開啟。

2. 點擊**更新**。

   應用程式開始更新資料庫。

您也可以用以下方法之一啟動更新工作：

- 點擊應用程式圖示並選擇**更新**。
- 在功能表列中，選擇**防護 > 更新**。

更新過程中，應用程式資料庫和模組將與更新伺服器上目前可用的應用程式資料庫和模組進行對比。如果電腦上已經安裝了最新版本的資料庫，則**更新**視窗將顯示一條訊息，告知您應用程式資料庫為最新版本。如果應用程式版本和應用程式資料庫與更新伺服器上目前可用的不一致，在電腦上將只下載和安裝缺少的更新元件。應用程式資料庫的增量更新所用時間更短，所需的 Web 流量也更少。

如果透過代理伺服器連線到網際網路，則可以設定代理伺服器連線設定。Kaspersky Endpoint Security 使用這些設定來更新應用程式資料庫並下載應用程式模組更新。

配置與代理伺服器的連線

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 選擇**更新**索引標籤。
3. 在**代理**部分中，選取**使用代理伺服器**核取方塊，然後點擊**設定**。
   一個視窗將開啟，您可以在其中配置代理伺服器連線設定。
4. 配置與代理伺服器的連線。
5. 點擊**儲存**以儲存對代理伺服器連線設定所做的變更。

在更新應用程式資料庫之前，Kaspersky Endpoint Security 會建立它們的備份副本，以便在必要時執行回溯。如果新版本的應用程式資料庫包含不正確的簽名，導致 Kaspersky Endpoint Security 封鎖安全應用程式，則回溯功能非常有用。

注意：如果 Kaspersky Endpoint Security 資料庫損壞，我們建議您開始更新以下載並安裝最新版本的應用程式資料庫。

回溯最近更新

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 選擇**更新**索引標籤。
3. 在**回溯**部分中，點擊**回溯更新**。

Kaspersky Endpoint Security 也在**報告**視窗提供有關更新工作結果的詳細報告。

檢視更新工作報告

1. 在功能表列中，選擇**防護** > **報告**。
2. **報告**視窗將開啟。
3. 選擇**資料庫更新**頁簽。

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

本機工作

外部磁碟掃描工作

Kaspersky Endpoint Security 可以掃描您執行或複製的所有檔案，即使該檔案位於外部磁碟上。若要防止惡意軟體的傳播，您可以配置當外部磁碟連線到裝置時對其自動掃描。

以下外部磁碟掃描設定可以進行配置：

- **連線了外部磁碟時 Kaspersky Endpoint Security 執行的操作。**

  掃描

  如果選擇此選項，Kaspersky Endpoint Security 將為連線的外部磁碟啟動惡意軟體掃描工作。

  預設選擇此選項。

  什麼都不做

  如果選擇此選項，Kaspersky Endpoint Security 不會掃描已連線的外部磁碟。

- **Kaspersky Endpoint Security 在偵測到惡意物件時執行的操作。**

  解毒；若解毒失敗則刪除

  如果選擇此選項，Kaspersky Endpoint Security 封鎖存取受感染物件並嘗試在不請求使用者確認的情況下解毒檔案。

  如果物件已解毒，Kaspersky Endpoint Security 會用原始的檔案名儲存在原來的位置。如果解毒失敗，Kaspersky Endpoint Security 將刪除無法解毒的受感染物件。

  預設選擇此選項。

  提示操作

  如果選擇此選項，Kaspersky Endpoint Security 將顯示一個通知視窗，其中包含有關惡意物件的資訊，並提示使用者選擇 Kaspersky Endpoint Security 要採取的操作。可用的操作可能因物件狀態的不同而有所不同。

您可以在管理主控台、網頁主控台或 Kaspersky Endpoint Security 應用程式中設定外部磁碟掃描。

如何在管理主控台 (MMC) 中設定外部磁碟掃描

1. 啟動卡巴斯基安全管理中心管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，點擊**"受管理裝置"**。
4. 在工作區選擇**"政策"**標籤。
5. 右鍵點擊要設定的政策並選擇**內容**。
6. 在**屬性**視窗中，選擇**本機工作 > 外部磁碟掃描**。
7. 配置工作設定。
8. 點擊**"確定"**儲存變更。

如何在網頁主控台和雲端主控台中配置執行外部磁碟掃描

1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選取**"應用程式設定"**標籤。
4. 前往 **主機威脅防護 → 卸除式磁碟機掃描**。
5. 使用**卸除式磁碟機掃描**撥動開關啟用或停用該元件。
6. 存儲變更。

如何在應用程式介面中配置執行外部磁碟掃描

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在**掃描**標籤左側的清單中，選擇**外部磁碟掃描**。
3. 在**連線了外部磁碟時**部分，選擇連線到外部磁碟時 Kaspersky Endpoint Security 執行的操作。

備份

有時，在解毒過程中無法保留受感染檔案的完整性。如果已解毒的檔案包含重要資訊，且這些資訊在解毒之後部分或完全無法存取，您可以嘗試從備份還原原始檔案。

*備份副本*是在解毒或刪除檔案時所建立的危險檔案的副本。它儲存在備份區中。

*備份區*是一個特殊儲存區，包含解毒過程中被刪除或修改的檔案的備份副本。備份區的主要功能是使使用者可以隨時還原原始檔案。備份區中的檔案以特殊格式儲存，對電腦不具有危險性。

檢視備份區內容

1. 在功能表列中，**防護** > **偵測到的物件**。

   偵測到的物件視窗將開啟。

2. 在**備份**部分中，檢視已備份檔案的清單。

您可以從備份區還原或刪除檔案備份副本。

從備份區中還原檔案的備份副本

1. 在功能表列中，**防護** > **偵測到的物件**。

   偵測到的物件視窗將開啟。

2. 在**備份**部分中，點擊您要還原的檔案旁邊的 ••• 。

   彈出功能表將開啟。

3. 選擇**還原檔案**。

   一個視窗將開啟，用於指定檔案名稱、標籤以及檔案將被還原到的資料夾。預設情況下，已指定原始檔案名稱和位置。

4. 指定檔案名稱和檔案將被還原到的資料夾。

5. 點擊**儲存**。

   應用程式將把檔案還原到具有指定名稱的指定位置。

還原檔案後，您需要立即掃描該檔案是否有惡意軟體。可以使用更新的資料庫對該物件進行解毒而不會損壞。

重要：建議您不要還原檔案的備份副本，除非還原它們是絕對必要的，因為這樣做可能會導致電腦感染。

從備份中刪除檔案的備份副本

1. 在功能表列中，**防護** > **偵測到的物件**。

   偵測到的物件視窗將開啟。

2. 在**備份**部分中，執行以下操作：

   - 若要刪除檔案的所有備份副本，請點擊**刪除全部**。
   - 若要刪除選定的備份副本，請點擊它旁邊的 ••• ，然後選擇**刪除備份副本**。

預設情況下，備份檔案的儲存期限為 30 天。當該期限到期時，檔案將被刪除。您可以變更檔案最長的備份儲存期限或取消儲存期限的限制。

設定備份區中的檔案儲存期

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。

   此時會開啟應用程式設定視窗。

2. 在**威脅**標籤的**備份**部分中，勾選**<number> 天後刪除備份物件**核取方塊，並指定在此後自動刪除備份中儲存的檔案的時間段。

報告

您可以在**已處理的物件**標籤上檢視列出所有偵測到的物件的 Kaspersky Endpoint Security 報告。系統事件顯示在**系統事件**標籤上。此外，還會為以下每個應用程式元件建立單獨的詳細報告：檔案威脅防護、Web 威脅防護、網路威脅防護、行為偵測以及掃描和更新工作。

開啟報告視窗

在功能表列中，選擇**防護 > 報告**。

Kaspersky Endpoint Security 可以儲存文字格式的報告。如果應用程式元件或工作產生您無法自行修復的錯誤，並且需要卡巴斯基技術支援的說明，則此功能可能會發揮作用。在這種情況下，可將文字格式的報告傳送給卡巴斯基技術支援人員，以便我們的專家能夠研究問題並儘快修復。

將 Kaspersky Endpoint Security 元件報告或工作報告匯出到文字檔案

1. 在功能表列中，選擇**防護 > 報告**。

   報告視窗將開啟。

2. 在左側窗格中，選擇包含所需報告的標籤。

3. 在右上角，點擊 ⍐ 。

4. 在開啟的視窗中，指定報告的檔案名、標籤和目的資料夾。

5. 點擊**儲存**。

預設情況下，Kaspersky Endpoint Security 不在報告中記錄資訊性事件。您可以允許記錄資訊性事件。

允許在報告中記錄資訊性事件

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。

   此時會開啟應用程式設定視窗。

2. 在**介面**標籤的**報告**部分中，勾選**記錄非緊急事件**核取方塊以接收 Kaspersky Endpoint Security 資訊事件的通知。

Managed Detection and Response

Kaspersky Endpoint Security 版本 11.2 中新增了 Managed Detection and Response 元件。該元件與稱為 Kaspersky Managed Detection and Response 的解決方案進行交互。*Kaspersky Managed Detection and Response (MDR)*持續搜尋、偵測和消除針對您組織的威脅。如欲瞭解該解決方案如何工作的詳細資訊，請參閱 *Kaspersky Managed Detection and Response 說明*。

與 Kaspersky Managed Detection and Response 互動時，該應用程式可讓您執行以下功能：

- 使用 BLOB 設定檔啟動 Managed Detection and Response。
- 從 Kaspersky Managed Detection and Response 執行命令。
- 將遙測資料傳送到 Kaspersky Managed Detection and Response 以進行威脅偵測。

Managed Detection and Response 元件有以下附加要求：

- macOS 14 或更新版本
- 基於 Intel 的 Mac、Apple 晶片
- 啟動的 Kaspersky Endpoint Security 產品授權條款

您必須啟用延伸以下元件才能使 Managed Detection and Response 正常工作：

- 檔案威脅防護
- Web 威脅防護
- 郵件威脅防護

啟用這些元件是強制性的。否則，Kaspersky Managed Detection and Response 將無法正常運作，因為它無法接收所需的遙測資料。

此外，Kaspersky Managed Detection and Response 也使用從其他應用程式元件接收的資料。啟用這些元件可選。提供額外資料的元件包括：

- 行為偵測

與 Kaspersky Managed Detection and Response 整合

與 Kaspersky Managed Detection and Response 整合包括以下步驟：

1. **設定卡巴斯基安全網路代理伺服器**

   卡巴斯基安全網路代理伺服器透過管理伺服器促進電腦和卡巴斯基安全網路雲端服務基礎架構之間的資料交換，而不是直接交換。

   在管理伺服器屬性中加載卡巴斯基安全網路設定檔。卡巴斯基安全網路設定檔位於 MDR 設定檔的 ZIP 壓縮檔案中。您可以在 Kaspersky Managed Detection and Response 主控台中獲取 ZIP 壓縮檔案。有關配置卡巴斯基安全網路代理伺服器的詳細資訊，請參閱*卡巴斯基安全管理中心說明*。

   結果，Kaspersky Endpoint Security 將使用私有 KSN 來確定檔案、應用程式和網站的信譽。*基礎架構：卡巴斯基私人安全網路*運作狀態將在卡巴斯基安全網路部分的政策設定中指示。

   將私有 KSN 與 Kaspersky Managed Detection and Response 結合使用可確保將遙測資料傳送到符合 GDPR（一般資料防護規範）的伺服器。如果未使用私有 KSN，則可以將遙測資料傳送到全球 KSN。這可能違反您所在國家/地區的法律。

   重要：您必須啟用延伸 KSN 模式才能使 Managed Detection and Response 正常工作。

2. **啟動 Kaspersky Managed Detection and Response**

您可以使用以下方法在端點裝置上啟動 Managed Detection and Response 元件：

- **使用 Kaspersky Endpoint Security 應用程式中的啟動碼進行啟動**。

  1. 開啟應用程式主視窗。
  2. 在主應用程式視窗的側欄上，點擊**產品授權**。

     產品授權視窗將開啟。
  3. 在**產品授權**視窗中，輸入您在購買時收到的啟動碼。

     注意：啟動碼是一個由 20 個拉丁字母和數位組成的唯一組合，採用 xxxxx-xxxxx-xxxxx-xxxxx 形式。
  4. 點擊**啟動**。

     應用程式連線到卡巴斯基啟動伺服器並傳送啟動碼以確認確實性。如果已成功驗證啟動碼，應用程式將自動接收並新增產品授權金鑰。

     注意：根據您收到的啟動碼，您可能需要填寫註冊表。

  如果啟動碼驗證失敗，則會顯示相應的通知。此時，請聯絡向您提供此啟動碼的軟體供應商。

- **使用 BLOB 檔案啟動**。

  在 Kaspersky Endpoint Security 政策中加載 BLOB 設定檔（請參閱以下說明）。BLOB 檔案包含用戶端 ID 以及有關 Kaspersky Managed Detection and Response 產品許可的資訊。BLOB 檔案位於 MDR 設定檔的 ZIP 壓縮檔案中。您可以在 Kaspersky Managed Detection and Response 主控台中獲取 ZIP 壓縮檔案。有關 BLOB 檔案的詳細資訊，請參閱 *Kaspersky Managed Detection and Response 說明*。

  在管理主控台 (MMC) 中啟動 Kaspersky Managed Detection and Response

  1. 啟動卡巴斯基安全管理中心管理主控台。
  2. 最大化**管理伺服器<伺服器名稱>**節點。
  3. 在主控台樹狀目錄中，點擊**"受管理裝置"**。
  4. 在工作區選擇**"政策"**標籤。
  5. 右鍵點擊要設定的政策並選擇**內容**。
  6. 在**內容**視窗中，選擇 **Detection and Response → Managed Detection and Response**。
  7. 選擇**啟用 Managed Detection and Response**核取方塊。
  8. 在**MDR 設定檔**區塊中，點擊**匯入**並選擇 Kaspersky Managed Detection and Response 主控台中收到的 BLOB 檔案。該檔案具有 .P7 副檔名。
  9. 點擊**"確定"**儲存變更。

在網頁主控台和雲端主控台中啟動 Kaspersky Managed Detection and Response

1. 在網頁主控台的主視窗中，選取**"裝置"→"政策和設定檔"**。
2. 點擊 Kaspersky Endpoint Security for Mac 政策的名稱。
3. 政策內容視窗將開啟。
4. 選取**"應用程式設定"**標籤。
5. 選擇**Detection and Response > Managed Detection and Response**。
6. 開啟 **Managed Detection and Response (KATA)** 切換開關。
7. 點擊**"匯入"**，然後選擇在 Kaspersky Managed Detection and Response 主控台中獲取的 BLOB 檔案。該檔案具有 .P7 副檔名。
8. 存儲變更。

結果，Kaspersky Endpoint Security 將驗證 BLOB 檔案。BLOB 檔案驗證包括檢查數位簽章和產品授權期限。如果 BLOB 檔案驗證成功，在與卡巴斯基安全管理中心進行下一次同步時，Kaspersky Endpoint Security 將加載該檔案並將其傳送到電腦。

- **使用"新增金鑰"工作啟動**。

  - **在管理主控台 (MMC) 中啟動 Kaspersky Managed Detection and Response**

    1. 在**選擇工作類型**視窗中，最大化 **Kaspersky Endpoint Security for Mac (12.2.1)**節點。
    2. 若要建立新增金鑰的工作，請選擇**新增金鑰**。
    3. 在**應用程式啟動**視窗中，執行以下操作：

       a. 從卡巴斯基安全管理中心儲存中選擇啟動碼或金鑰，或新增一個電腦上儲存的金鑰檔案。

       b. 若要將指定金鑰新增為備用金鑰，請選取**新增為備用金鑰**核取方塊。

       當目前的啟動金鑰到期時，備用金鑰將變為活動狀態。

       有關指定金鑰的資訊（金鑰、金鑰類型和金鑰到期日期）顯示在**應用程式啟動**視窗中。

    4. 在選擇將工作指派到的裝置視窗中，選擇要用於指定用戶端電腦的方法：

       - 若要從管理伺服器在網路上偵測到的電腦中進行選擇，請選擇**選擇管理伺服器偵測到的網路裝置**選項。
       - 若要手動指定電腦的 IP 位址或從檔案匯入電腦的 IP 位址，請選擇**手動指定裝置位址或從清單匯入位址**選項。
       - 若要根據預設條件為所選的裝置建立工作，請選擇**將工作指派給裝置選擇**選項。
       - 若要從特定管理群組中選擇電腦，請選擇**將工作指派給管理群組**選項。

5. 在開啟的視窗中（**選擇裝置**、**裝置選擇**或**選擇管理群組**，取決於您在上一個步驟中選擇的選項），選擇用戶端電腦、指定電腦的 IP 位址、指定電腦選擇、或選擇工作將被套用到的管理群組。

   注意：此步驟與本機或群組工作無關。

6. 在**設定工作排程**視窗中，在**排程啟動**下拉清單中選擇啟動模式。

7. 如有必要，將排程工作配置為自動啟動（透過指定工作開始日期和時間）。

8. 如果您想要執行應用程式無法依照排程啟動的工作（例如，因為電腦在排程時間關閉），請勾選**執行錯過的工作**核取方塊。

   一旦阻止工作啟動的障礙被消除，Kaspersky Endpoint Security 就會啟動工作。

9. 如果您希望卡巴斯基安全管理中心自動決定不同電腦上工作啟動之間的時間間隔，請勾選**對工作啟動使用自動隨機延遲**核取方塊。

   這有助於減少卡巴斯基安全管理中心管理伺服器上的負載。

10. 若要手動設定在不同電腦上啟動工作之間的時間間隔，請勾選**在（分鐘）間隔內使用隨機延遲啟動工作**核取方塊並指定分鐘數。

    這有助於減少卡巴斯基安全管理中心管理伺服器上的負載。

11. 在**定義工作名稱**視窗的**名稱**欄位中，輸入您正在建立的工作的名稱。

1. 在**完成工作建立**視窗中，執行以下操作：

   a. 如果您希望工作在精靈完成後立即啟動，請勾選**精靈完成後執行工作**核取方塊。

   b. 點擊**結束**關閉精靈。

- **在網頁主控台和雲端主控台中啟動 Kaspersky Managed Detection and Response**

1. 在網頁主控台的主視窗中，選取"**資產（裝置）**">"**工作**"。

   工作清單開啟。

2. 點擊**新增**。

   新工作精靈啟動。

3. 配置工作設定：

   a. 在"**應用程式**"下拉清單中，選取"Kaspersky Endpoint Security for Mac (12.2.1)"。

   b. 在"**工作類型**"下拉式清單中，選取"**新增金鑰**"。

   c. 在"**工作名稱**"欄位中，輸入簡要說明。

   d. 選擇以下選項之一：

   - **將工作分配給管理群組**

     此工作被指派給管理群組中包含的裝置。您可以指定現有群組之一或建立新群組。

例如，如果訊息特定於特定管理群組中包含的裝置，您可能想要使用此選項來執行向使用者傳送訊息的工作。

如果工作唄指派給管理群組，則工作屬性視窗中不會顯示**「安全性」**索引標籤，因為群組工作受其所套用的群組的安全性設定的約束。

- **手動指定裝置位址或從清單中匯入位址**

  您可以指定您要將工作分配給的裝置的 NetBIOS 名稱、DNS 名稱、IP 位址和 IP 子網路。

  您可能希望使用此選項來執行特定子網路的工作。例如，您可能想要在會計師的裝置上安裝特定應用程式或掃描可能受感染的子網路中的裝置。

- **將工作指派給裝置分類**

  此工作被指派給裝置分類中包含的裝置。您可以指定現有選擇之一。

  例如，您可能希望使用此選項在具有特定作業系統版本的裝置上執行工作。

4. 按照所選工作範圍選項選取裝置。

5. 從清單中選擇產品授權金鑰。如果清單中沒有合適的產品授權，您可以將新的產品授權金鑰新增至管理伺服器儲存庫。

6. 輸入您希望用其權限執行工作的使用者的帳戶認證。點擊**下一步**。

   備足：預設情況下，Kaspersky Endpoint Security 作為系統使用者帳戶 (root) 啟動工作。

7. 在**完成工作建立**步驟中，點擊**完成**按鈕以建立工作並關閉精靈。

   如果您啟用了**建立完成後開啟工作詳情**選項，則工作設定視窗會開啟。在此視窗中，您可以檢查工作參數、修改它們，或根據需要設定工作啟動排程。

8. 點擊新工作。

   工作內容視窗將開啟。

9. 選取**"排程"**標籤。

10. 設定工作排程。

    注意：確保電腦已開啟以執行工作。

11. 點擊**儲存**。

12. 若要立即執行工作而不管配置的排程如何，請執行下列操作：

    a. 選中工作旁邊的核取方塊。

    b. 點擊**"執行"**按鈕。

Endpoint Detection and Response Expert（內部部署）

Kaspersky Endpoint Security 支援與 Kaspersky Endpoint Detection and Response元件整合，作為 Kaspersky Anti Targeted Attack Platform 解決方案的一部分。此解決方案只在及時偵測進階威脅，例如定向攻擊、進階持續性威脅、零日攻擊等。有關解決方案運作方式的詳細資訊，請參閱 *Kaspersky Anti Targeted Attack Platform 說明*。

在設定與 Endpoint Detection and Response (KATA) 的整合時，KATA 伺服器會接收有關 Kaspersky Endpoint Security 操作中發生的事件、應用程式發現的威脅以及有關處理這些威脅的資訊。為了對偵測到的威脅做出反應，Kaspersky Endpoint Security 可能會執行在 Kaspersky Anti Targeted Attack Platform Web 介面中啟動的工作。

Endpoint Detection and Response Expert（內部部署）有以下附加要求：

- Kaspersky Anti Targeted Attack Platform 6.0 或更高版本。
- 卡巴斯基安全管理中心版本 14.2 或更高版本。
- 可以在卡巴斯基安全管理中心管理主控台 (MMC)、網頁主控台或雲端主控台中設定與 Endpoint Detection and Response Expert（7.1 或者更高版本）的整合。
- 可以在卡巴斯基安全管理中心管理主控台 (MMC)、網頁主控台或雲端主控台中設定與Endpoint Detection and Response Expert（8.0 或者更高版本）的整合。

與 Kaspersky Endpoint Detection and Response (KATA) 整合

與 Kaspersky Managed Detection and Response (KATA) 整合包括以下步驟：

1. **安裝 Endpoint Detection and Response 元件**

   您可以在安裝 Kaspersky Endpoint Security 期間選擇 Endpoint Detection and Response 元件。

2. **啟動 Endpoint Detection and Response**

   如果您目前的產品授權不支援 Endpoint Detection and Response 元件，您需要單獨啟動 Kaspersky Endpoint Detection and Response。

   您可以在**產品授權**視窗中檢查目前產品授權是否支援 Endpoint Detection and Response 功能。

3. **連線到 KATA 伺服器**

   Kaspersky Anti Targeted Attack Platform 要求在 Kaspersky Endpoint Security 和 KATA 伺服器之間建立可信連線。要配置可信連線，您需要使用 TLS 憑證。您可以在 Kaspersky Anti Targeted Attack Platform Web 介面中下載 TLS 憑證。有關下載憑證的詳細資訊，請參閱 *Kaspersky Anti Targeted Attack Platform 說明*。

   預設情況下，Kaspersky Endpoint Security 僅檢查 KATA 伺服器的 TLS 憑證。為了使連線更加安全，您可以啟用雙向驗證。要使用雙向驗證，您需要使用受密碼防護的加密容器。有關下載加密容器的詳細資訊，請參閱 *Kaspersky Anti Targeted Attack Platform 說明*。

   使用管理主控台將裝有 Kaspersky Endpoint Security 的電腦連線到 KATA 伺服器

   1. 啟動管理主控台。
   2. 最大化**管理伺服器<伺服器名稱>**節點。

3. 在主控台樹狀目錄中，點擊**"受管理裝置"**。

4. 在工作區選擇**"政策"**標籤。

5. 右鍵點擊要設定的政策並選擇**內容**。

6. 在**內容**視窗中，選擇**Detection and Response** > **Endpoint Detection and Response Expert (on-premise)**。

7. 選擇 **啟用 Endpoint Detection and Response Expert（7.1 或者更早版本）** 核取方塊。

8. 點擊**伺服器連線設定**。

9. 在開啟的**伺服器連線設定**視窗中，配置以下設定：

   - 點擊**上傳 TLS 憑證**以選擇將用於與 KATA 伺服器建立可信任連線的 TLS 憑證。
   - 如果要變更 KATA 伺服器回應逾時，請在**逾時（秒）**欄位中指定逾時。當逾時用完時，Kaspersky Endpoint Security 會嘗試連線到不同的 KATA 伺服器。
   - 如果要使用雙向驗證，請選取**使用雙向身分驗證**核取方塊。點擊**載入加密容器**以選擇加密容器檔案，並在**加密容器密碼**欄位中輸入密碼。

10. 點擊**儲存**。

11. 若要新增 KATA 伺服器，請點擊**新增**。

12. 在開啟的**KATA 伺服器**視窗中，指定伺服器位址和連接埠，然後點擊**儲存**。

13. 點擊**"確定"**儲存變更。

使用網頁主控台將裝有 Kaspersky Endpoint Security 的電腦連線到 KATA 伺服器

1. 在網頁主控台的主視窗中，選取**"裝置"**→**"政策和設定檔"**。

2. 點擊 Kaspersky Endpoint Security for Mac 政策的名稱。
   政策內容視窗將開啟。

3. 選取**"應用程式設定"**標籤。

4. 選擇**Detection and Response** > **Endpoint Detection and Response Expert (on-premise)**。

5. 開啟 **Endpoint Detection and Response Expert（內部部署）**切換開關。

6. 點擊**連線設定**。

7. 在開啟的**伺服器連線設定**視窗中，配置以下設定：

   - 點擊**新增 TLS 憑證**以選擇將用於與 KATA 伺服器建立可信任連線的 TLS 憑證。
   - 如果要變更 KATA 伺服器回應逾時，請在**逾時（秒）**欄位中指定逾時。當逾時用完時，Kaspersky Endpoint Security 會嘗試連線到不同的 KATA 伺服器。
   - 如果要使用雙向驗證，請選取**使用雙向身分驗證**核取方塊。點擊**載入加密容器**以選擇加密容器檔案，並在**加密容器密碼**欄位中輸入密碼。

8. 點擊**OK**。

9. 若要新增 KATA 伺服器，請點擊**新增**。

10. 在開啟的對話方塊中，指定伺服器位址和連接埠，然後點擊**確定**。

11. 存儲變更。

結果，電腦將出現在 Kaspersky Anti Targeted Attack Platform 的 Web 介面中。

Endpoint Detection and Response Optimum

從版本 12.1 開始，Kaspersky Endpoint Security for Mac 包括 Kaspersky Endpoint Detection and Response Optimum 解決方案（以下也稱為 “EDR Optimum”）的內建代理。此解決方案旨在防護企業 IT 基礎架構免受進階網路威脅。解決方案的功能結合了自動偵測威脅和回應這些威脅的能力，以抵消包括新漏洞、勒索軟體、無檔案攻擊以及使用合法系統工具的方法。有關這些解決方案的詳細資訊，請參閱Kaspersky Endpoint Detection and Response Optimum 說明。

Kaspersky Endpoint Detection and Response 會審查和分析威脅發展並向*安全人員*或者*管理員*提供有關需要作出及時回應的潛在攻擊的資訊。Kaspersky Endpoint Detection and Response 會在單獨視窗中顯示偵測詳情。*偵測詳情*是一款用來檢視有關被偵測的威脅的整個收集資訊的工具。偵測詳情包括，例如，出現在電腦上的檔案的歷史。有關管理警示詳情的更多資訊，請參閱Kaspersky Endpoint Detection and Response Optimum 說明。

注意：您可以在網頁主控台中配置 EDR Optimum 元件。

Endpoint Detection and Response 設定

參數	描述
網路隔離	回應偵測到的威脅自動將電腦從網路中隔離。 當開啟網路隔離時，應用程式會斷開電腦上的所有活動連線並封鎖所有新的 TCP/IP 連線。應用程式只會讓以下連線處於活動狀態： • 網路隔離排除項目中列出的連線。 • Kaspersky Endpoint Security 服務安裝的連線。 • 卡巴斯基安全管理中心網路代理啟動的連線。
距離自動解鎖被隔離的電腦 N 小時	指定時間後可以自動或者手動關閉網路隔離。預設情況下，Kaspersky Endpoint Security 會在隔離啟動 8 小時後關閉網路隔離。
網路隔離排除項目	從網路隔離中排除的規則清單當開啟網路隔離時，電腦上匹配規則的網路連線不會被封鎖。 要配置網路隔離排除項目，您可以使用標準網路設定檔清單。預設情況下，排除項目包括包含確保裝置（具有 DNS/DHCP 伺服器和 DNS/DHCP 用戶端角色）不中斷操作的規則的網路設定檔。您也可以修改標準網路設定檔的設定或者手動定義排除項目。 **重要：**只有當網路隔離回應偵測到的威脅自動開啟時，政策內容中指定的排除項目才會套用。只有當網路隔離在卡巴斯基安全管理中心主控台的電腦內容或者警示詳情中手動開啟時，電腦內容中指定的排除項目才會套用。
執行防止	執行防禦可讓人管理可執行檔和指令碼的執行，以及開啟 Office 格式的檔案。這樣的話，您可以（例如）防止執行您認為不安全的應用程式。因此，威脅擴散可以被停止。執行防禦支援一組指令碼解釋器。 所要使用執行防禦元件，您需要新增執行防禦規則。執行防禦規則是應用程式對物件執行進行回應（例如，封鎖物件執行時）時考慮的一組條件。應用程式根據檔案路徑或者使用 MD5 和 SHA256 雜湊演算法計算的總和檢查碼來識別檔案。

參數	描述
執行或開啟被禁止物件時的動作	**封鎖並寫入報告**。在此模式中，應用程式會封鎖執行物件或者開啟匹配防護規則條件的文件。應用程式也會將嘗試執行物件或者開啟文件的事件發佈到卡巴斯基安全管理中心事件記錄和統一記錄系統。 **僅記錄事件**。在此模式中，Kaspersky Endpoint Security 會將嘗試執行可執行物件或者開啟匹配防護規則條件的文件的事件發佈到卡巴斯基安全管理中心事件記錄和統一記錄系統，但是不會封鎖執行或者開啟物件或者文件的嘗試。預設情況下已選擇此項。
Cloud Sandbox	Cloud Sandbox 技術可讓您偵測電腦上的進階威脅。Kaspersky Endpoint Security 自動將被偵測檔案轉寄到 Cloud Sandbox 進行分析。Cloud Sandbox 在隔離環境中執行這些檔案以識別惡意活動和決定其信譽。有關這些檔案的資料然後被傳送到卡巴斯基安全網路。因此，如果 Cloud Sandbox 偵測到一個惡意檔案，Kaspersky Endpoint Security 將執行適當操作在偵測到該檔案的所有電腦上消除該威脅。 **注意：**Cloud Sandbox 技術永久啟用，對所有卡巴斯基安全網路使用者可用，與他們使用的產品授權類型無關。

與 Endpoint Detection and Response Optimum 整合

要與 Kaspersky Endpoint Detection and Response 集成，您必須 新增 Endpoint Detection and Response Optimum (EDR Optimum) 元件並配置 Kaspersky Endpoint Security。

注意： EDR Optimum 和 Endpoint Detection and Response (KATA) 元件彼此不相容。

Endpoint Detection and Response 要工作必須滿足以下條件：

- 卡巴斯基安全管理中心版本 13.2 或更高版本。在早期版本的卡巴斯基安全管理中心中，無法啟動 Endpoint Detection and Response 功能。
- Kaspersky Endpoint Detection and Response 管理外掛程式已安裝。這是用於在 Windows、Mac 和 Linux 作業係統上使用代理的單一外掛程式。當使用 Endpoint Detection and Response Optimum 時，您需要 Kaspersky Endpoint Security 管理外掛程式來建立威脅回應工作，EDR 管理外掛程式來檢視警示詳情。
- EDR Optimum 元件作為 Kaspersky Endpoint Security 的一部分支援與 Kaspersky Endpoint Detection and Response Optimum 3.0 解決方案的交互。不支援與早期版本的 Kaspersky Endpoint Inspection and Response Optimum 互動。
- EDR Optimum 可以在網頁主控台中進行管理。
- 應用程式被啟動，功能受產品授權覆蓋。
- Endpoint Detection and Response 元件已開啟。

與 Kaspersky Endpoint Detection and Response Optimum 整合

與 Kaspersky Managed Detection and Response Optimum 整合包括以下步驟：

1. **安裝 Endpoint Detection and Response Optimum 元件**

   您可以在安裝 Kaspersky Endpoint Security 期間選擇 Endpoint Detection and Response 元件。

2. **啟動 Endpoint Detection and Response**

   如果您目前的產品授權不支援 Endpoint Detection and Response 元件，您需要單獨啟動 Kaspersky Endpoint Detection and Response。

   您可以在**產品授權**視窗中檢查目前產品授權是否支援 Endpoint Detection and Response 功能。

3. **啟用 Endpoint Detection and Response 元件**

   您可以在 Kaspersky Endpoint Security for Mac 政策設定中啟用或者停用該元件。

   如何在網頁主控台中啟用或停用 Endpoint Detection and Response 元件

   1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
   2. 點擊 Kaspersky Endpoint Security 政策的名稱。

      政策內容視窗將開啟。
   3. 選取"**應用程式設定**"標籤。
   4. 轉到**Detection and Response** > **Endpoint Detection and Response**。
   5. 開啟 **Endpoint Detection and Response Expert（內部部署）**切換開關。
   6. 存儲變更。

掃描查找入侵指標

洩露指示器 (IOC)是一個物件或者活動的資料集合，表明對電腦的未經授權存取（資料洩露）。例如，許多登入系統的不成功嘗試可以構成一個洩露指示器。"**IOC 掃描**"工作可發現電腦上的洩露指示器並採取威脅回應措施。

Kaspersky Endpoint Security 可使用 IOC 檔案搜尋洩露指示器。IOC 檔案是包含應用程式試圖匹配以計數偵測的指示器集合的檔案。IOC 檔案必須符合 IOC 檔案的要求。

IOC 掃描工作執行模式

Kaspersky Endpoint Detection and Response 可讓您建立標準 IOC 掃描工作以偵測洩露的資料。"標準 IOC 掃描工作"是一個在網頁主控台中手動建立和配置的群組或本機工作。工作使用使用者準備的 IOC 檔案執行。如果您想要手動新增洩露指示器，請閱讀IOC 檔案要求。

建立 IOC 掃描工作

您可以手動建立"IOC 掃描"工作：

- 在偵測詳情中（僅適用於 EDR Optimum）。

  *偵測詳情*是一款用來檢視有關被偵測的威脅的整個收集資訊的工具。偵測詳情包括，例如，出現在電腦上的檔案的歷史。有關管理警示詳情的更多資訊，請參閱Kaspersky Endpoint Detection and Response Optimum 說明。
- 使用工作精靈。

要建立 IOC 掃描工作：

1. 在網頁主控台的主視窗中，選取“**資產（裝置）**”>“**工作**”。

   工作清單開啟。

2. 點擊**新增**。

   新工作精靈啟動。

3. 配置工作設定：

   a. 在“**應用程式**”下拉清單中，選取“Kaspersky Endpoint Security for Mac (12.2.1)”。

   b. 在“**工作類型**”下拉式清單中，選取“**IOC 掃描**”。

   c. 在“**工作名稱**”欄位中，輸入簡要說明。

   d. 在“**選取要對其分配工作的裝置**”塊中，選取工作範圍。

4. 按照所選工作範圍選項選取裝置。

5. 在**IOC 掃描設定**部分中，載入 IOC 檔案以搜尋入侵指標。您可以新增 IOC 檔案或從包含檔案雜湊或 IP 位址的檔案產生一個 IOC 檔案。

   加載 IOC 檔案後，您可以從 IOC 檔案檢視和編輯指示器清單。

   注意：不建議在執行工作後新增或刪除 IOC 檔案。這可能會導致 IOC 掃描結果對於先前執行的工作顯示不正確。要根據新的 IOC 檔案搜尋洩露指示器，建議新增工作。

6. 配置偵測到 IOC 後的動作：

   - **將電腦從網路隔離**。如果選擇該選項，Kaspersky Endpoint Security 會從網路隔離電腦以防止威脅傳播。您可以在“Endpoint Detection and Response Optimum 元件設定”中配置隔離時長。
   - **將副本移動到隔離區並刪除物件**。如果選擇該選項，Kaspersky Endpoint Security 會刪除在電腦上發現的惡意物件。在刪除物件之前，Kaspersky Endpoint Security 會建立備份副本以防物件以後需要還原。Kaspersky Endpoint Security 會將備份副本移動到隔離。
   - **執行關鍵區域掃描**。如果選擇該選項，Kaspersky Endpoint Security 將執行“快速掃描”工作。預設情況下，Kaspersky Endpoint Security 掃描記憶體、啟動物件和系統資料夾。

7. 轉到“**進階**”區域。

8. 選擇必須作為工作的一部分進行分析的資料類型（IOC 文件）。

   注意：Kaspersky Endpoint Security 根據載入的 IOC 檔案的內容自動選擇 IOC 掃描 工作的資料類型（IOC 文件）。不建議取消選擇資料類型。

   您還可以為以下資料類型配置掃描範圍：

   - **處理程序 – ProcessItem**
   - **檔案 – FileItem**

- **網路連接埠 – PortItem**
- **使用者帳戶 – UserItem**
- **ARP 表 – ArpEntryItem**
- **主機 – SystemInfoItem**
- **URLs – UrlHistoryItem**
- **Routes – RouteEntryItem**

9. 點擊**OK**。
10. 輸入您希望用其權限執行工作的使用者的帳戶認證。點擊**下一步**。

    備足：預設情況下，Kaspersky Endpoint Security 作為系統使用者帳戶 (root) 啟動工作。

11. 在**完成工作建立**步驟中，點擊**完成**按鈕以建立工作並關閉精靈。

    如果您啟用了**建立完成後開啟工作詳情**選項，則工作設定視窗會開啟。在此視窗中，您可以檢查工作參數、修改它們，或根據需要設定工作啟動排程。

12. 點擊新工作。

    工作內容視窗將開啟。

13. 選取"**排程**"標籤。
14. 設定工作排程。

    注意：確保電腦已開啟以執行工作。

15. 點擊**儲存**。
16. 若要立即執行工作而不管配置的排程如何，請執行下列操作：

    a. 選中工作旁邊的核取方塊。

    b. 點擊"**執行**"按鈕。

17. 因此，Kaspersky Endpoint Security 將執行搜尋電腦上的洩露指示器。您可以在工作內容的"**結果**"區域中檢視工作結果。您可以在工作內容中檢視偵測到的洩露指示器的有關資訊：**應用程式設定 > IOC 掃描結果**。

注意：IOC 掃描結果保留 30 天。在此期間之後，Kaspersky Endpoint Security 將自動移除最舊條目。

移動檔案到隔離

當回應威脅時，Kaspersky Endpoint Detection and Response 可以建立“*移動檔案到隔離區*”工作。這對於最小化威脅的後果是必需的。*隔離區*是電腦上的一個特別本機儲存區域。使用者可以隔離使用者認為對電腦有危險的檔案。隔離檔案以加密狀態儲存，不會威脅裝置安全。Kaspersky Endpoint Security 使用備份作為檔案儲存。有關將隔離區作為解決方案的一部分進行管理的詳細信息，請參閱Kaspersky Endpoint Inspection and Response Optimum 說明。

您可以用以下方式建立“*移動檔案到隔離區*”工作：

- 在偵測詳情中（僅適用於 EDR Optimum）。

  *偵測詳情*是一款用來檢視有關被偵測的威脅的整個收集資訊的工具。偵測詳情包括，例如，出現在電腦上的檔案的歷史。有關管理警示詳情的更多資訊，請參閱Kaspersky Endpoint Detection and Response Optimum 說明。

- 使用工作精靈。

  您必須輸入檔案路徑或者雜湊（SHA256 或者 MD5），或者檔案路徑和檔案雜湊二者。

“*將檔案移動到隔離區*”工作有以下限制：

- 檔案大小不得超過 100 MB。
- 您可以在網頁主控台中配置 EDR Optimum 的工作。
- 備份容量受可用磁碟空間的限制。

若要建立“移動檔案到隔離區”工作：

1. 在網頁主控台的主視窗中，選取“**資產（裝置）**”>“**工作**”。

   工作清單開啟。

2. 點擊**新增**。

   新工作精靈啟動。

3. 配置工作設定：

   a. 在“**應用程式**”下拉清單中，選取“Kaspersky Endpoint Security for Mac (12.2.1)”。

   b. 在“**工作類型**”下拉式清單中，選取“**移動檔案到隔離**”。

   c. 在“**工作名稱**”欄位中，輸入簡要說明。

   d. 選擇以下選項之一：

   - **將工作分配給管理群組**

     此工作被指派給管理群組中包含的裝置。您可以指定現有群組之一或建立新群組。

     例如，如果訊息特定於特定管理群組中包含的裝置，您可能想要使用此選項來執行向使用者傳送訊息的工作。

     如果工作唄指派給管理群組，則工作屬性視窗中不會顯示**「安全性」**索引標籤，因為群組工作受其所套用的群組的安全性設定的約束。

   - **手動指定裝置位址或從清單中匯入位址**

     您可以指定您要將工作分配給的裝置的 NetBIOS 名稱、DNS 名稱、IP 位址和 IP 子網路。

您可能希望使用此選項來執行特定子網路的工作。例如，您可能想要在會計師的裝置上安裝特定應用程式或掃描可能受感染的子網路中的裝置。

- **將工作指派給裝置分類**

  此工作被指派給裝置分類中包含的裝置。您可以指定現有選擇之一。

  例如，您可能希望使用此選項在具有特定作業系統版本的裝置上執行工作。

4. 按照所選工作範圍選項選取裝置。
5. 在**工作範圍**步驟中，指定管理群組、具有特定位址的裝置或裝置分類。

   可用設定取決於上一個步驟中選擇的選項。
6. 在檔案清單中，點擊**"新增"**。

   檔案新增精靈啟動。
7. 在**請指定要移動到隔離區的檔案**下拉清單中，選擇選項之一並填寫必填欄位。若要新增檔案，您必須輸入檔案的的完整路徑、或雜湊和路徑二者。
8. 如果您希望該工作適用於關鍵系統物件，請選擇 **套用到關鍵系統物件** 核取方塊。
9. 輸入您希望用其權限執行工作的使用者的帳戶認證。點擊**下一步**。

   備足：預設情況下，Kaspersky Endpoint Security 作為系統使用者帳戶 (root) 啟動工作。
10. 在**完成工作建立**步驟中，點擊**完成**按鈕以建立工作並關閉精靈。

    如果您啟用了**建立完成後開啟工作詳情**選項，則工作設定視窗會開啟。在此視窗中，您可以檢查工作參數、修改它們，或根據需要設定工作啟動排程。
11. 點擊新工作。

    工作內容視窗將開啟。
12. 選取**"排程"**標籤。
13. 設定工作排程。

    注意：確保電腦已開啟以執行工作。
14. 點擊**儲存**。
15. 若要立即執行工作而不管配置的排程如何，請執行下列操作：

    a. 選中工作旁邊的核取方塊。

    b. 點擊**"執行"**按鈕。

結果，Kaspersky Endpoint Security 會將檔案移動到隔離區。

如果您試圖隔離一個目前在執行的可執行檔，*"移動檔案到隔離區"*工作可能完成但有*"存取被拒絕"*錯誤。為檔案建立終止處理程序工作然後重試。

如果您試圖隔離一個太大的檔案，“*移動檔案到隔離區*”工作將以“*隔離儲存中空間不足*”錯誤而失敗。釋放磁碟空間並重試。

獲取檔案

您可以從使用者的電腦獲取檔案。例如，您可以配置獲取由協力廠商應用程式建立的事件記錄檔案。若要獲取檔案，您必須建立專用工作。因為執行工作，檔案被儲存在備份中。您可以使用網頁主控台從備份下載此檔案到電腦。在使用者的電腦上，檔案將保留在原始資料夾中。

重要：檔案大小不得超過 100 MB。備份容量受可用磁碟空間的限制。

若要建立“獲取檔案”工作：

1. 在網頁主控台的主視窗中，選取“**資產（裝置）**”>“**工作**”。
   工作清單開啟。
2. 點擊**新增**。
   新工作精靈啟動。
3. 配置工作設定：
   a. 在“**應用程式**”下拉清單中，選取“Kaspersky Endpoint Security for Mac (12.2.1)”。
   b. 在“**工作類型**”下拉式清單中，選取“**獲取檔案**”。
   c. 在“**工作名稱**”欄位中，輸入簡要說明。
   d. 選擇以下選項之一：
   - **將工作分配給管理群組**

     此工作被指派給管理群組中包含的裝置。您可以指定現有群組之一或建立新群組。

     例如，如果訊息特定於特定管理群組中包含的裝置，您可能想要使用此選項來執行向使用者傳送訊息的工作。

     如果工作唄指派給管理群組，則工作屬性視窗中不會顯示**「安全性」**索引標籤，因為群組工作受其所套用的群組的安全性設定的約束。
   - **手動指定裝置位址或從清單中匯入位址**

     您可以指定您要將工作分配給的裝置的 NetBIOS 名稱、DNS 名稱、IP 位址和 IP 子網路。

     您可能希望使用此選項來執行特定子網路的工作。例如，您可能想要在會計師的裝置上安裝特定應用程式或掃描可能受感染的子網路中的裝置。
   - **將工作指派給裝置分類**

     此工作被指派給裝置分類中包含的裝置。您可以指定現有選擇之一。

     例如，您可能希望使用此選項在具有特定作業系統版本的裝置上執行工作。

4. 按照所選工作範圍選項選取裝置。在**獲取檔案**視窗中，點擊**新增**。

   "**獲取檔案**"對話方塊將開啟。

5. 在**指定需要獲取的檔案**下拉清單中，選擇選項之一併填寫必填欄位。

   若要新增檔案，您必須輸入檔案的的完整路徑、或檔案雜湊和路徑二者。

6. 點擊**OK**。

   要新增的檔案的設定將顯示在檔案清單中。

7. 點擊**下一步**。

8. 輸入您希望用其權限執行工作的使用者的帳戶認證。點擊**下一步**。

   備足：預設情況下，Kaspersky Endpoint Security 作為系統使用者帳戶 (root) 啟動工作。

9. 在**完成工作建立**步驟中，點擊**完成**按鈕以建立工作並關閉精靈。

   如果您啟用了**建立完成後開啟工作詳情**選項，則工作設定視窗會開啟。在此視窗中，您可以檢查工作參數、修改它們，或根據需要設定工作啟動排程。

10. 點擊新工作。

    工作內容視窗將開啟。

11. 選取"**排程**"標籤。

12. 設定工作排程。

    注意：確保電腦已開啟以執行工作。

13. 點擊**儲存**。

14. 若要立即執行工作而不管配置的排程如何，請執行下列操作：

    a. 選中工作旁邊的核取方塊。

    b. 點擊"**執行**"按鈕。

結果，Kaspersky Endpoint Security 將建立一個檔案副本並將此副本移動到備份區。您可以在網頁主控台中從備份區下載檔案。

刪除檔案

您可以使用"*刪除檔案*"工作遠端刪除檔案。例如，您可以在回應威脅時遠端刪除檔案。

若要建立"刪除檔案"工作：

1. 在網頁主控台的主視窗中，選取"**資產（裝置）**">"**工作**"。

   工作清單開啟。

2. 點擊**新增**。

   新工作精靈啟動。

3. 配置工作設定：

   a. 在"**應用程式**"下拉清單中，選取"Kaspersky Endpoint Security for Mac (12.2.1)"。

   b. 在"**工作類型**"下拉式清單中，選取"**刪除檔案**"。

   c. 在"**工作名稱**"欄位中，輸入簡要說明。

   d. 選擇以下選項之一：

   - **將工作分配給管理群組**

     此工作被指派給管理群組中包含的裝置。您可以指定現有群組之一或建立新群組。

     例如，如果訊息特定於特定管理群組中包含的裝置，您可能想要使用此選項來執行向使用者傳送訊息的工作。

     如果工作唄指派給管理群組，則工作屬性視窗中不會顯示**「安全性」**索引標籤，因為群組工作受其所套用的群組的安全性設定的約束。

   - **手動指定裝置位址或從清單中匯入位址**

     您可以指定您要將工作分配給的裝置的 NetBIOS 名稱、DNS 名稱、IP 位址和 IP 子網路。

     您可能希望使用此選項來執行特定子網路的工作。例如，您可能想要在會計師的裝置上安裝特定應用程式或掃描可能受感染的子網路中的裝置。

   - **將工作指派給裝置分類**

     此工作被指派給裝置分類中包含的裝置。您可以指定現有選擇之一。

     例如，您可能希望使用此選項在具有特定作業系統版本的裝置上執行工作。

4. 按照所選工作範圍選項選取裝置。

5. 在**指定需要刪除的檔案**下拉清單中，選擇選項之一併填寫必填欄位。若要新增檔案，您必須輸入檔案的的完整路徑、或雜湊和路徑二者。

6. 如果您希望該工作適用於關鍵系統物件，請選擇 **套用到關鍵系統物件** 核取方塊。

7. 輸入您希望用其權限執行工作的使用者的帳戶認證。點擊**下一步**。

   備足：預設情況下，Kaspersky Endpoint Security 作為系統使用者帳戶 (root) 啟動工作。

8. 在**完成工作建立**步驟中，點擊**完成**按鈕以建立工作並關閉精靈。

   如果您啟用了**建立完成後開啟工作詳情**選項，則工作設定視窗會開啟。在此視窗中，您可以檢查工作參數、修改它們，或根據需要設定工作啟動排程。

9. 點擊新工作。

   工作內容視窗將開啟。

10. 選取“**排程**”標籤。

11. 設定工作排程。

> **注意：**確保電腦已開啟以執行工作。

12. 點擊**儲存**。

13. 若要立即執行工作而不管配置的排程如何，請執行下列操作：

    a. 選中工作旁邊的核取方塊。

    b. 點擊“**執行**”按鈕。

結果，Kaspersky Endpoint Security 會從電腦刪除檔案。如果檔案被其它處理程序鎖定，工作將顯示為“*已完成*”，但是檔案本身只有在電腦重啟後才會被刪除。重啟電腦後，請確認檔案已刪除。

如果您試圖刪除一個目前在執行的可執行檔，“*刪除檔案*”工作可能完成但有“*存取被拒絕*”錯誤。為檔案建立終止處理程序工作然後重試。

啟動處理程序

您可以使用“*啟動處理程序*”工作遠端執行檔案。

> **重要：**您可以在網頁主控台中配置 EDR Optimum 的工作。

若要建立啟動處理程序工作：

1. 在網頁主控台的主視窗中，選取“**資產（裝置）**”>“**工作**”。
   工作清單開啟。

2. 點擊**新增**。
   新工作精靈啟動。

3. 配置工作設定：

    a. 在“**應用程式**”下拉清單中，選取“Kaspersky Endpoint Security for Mac (12.2.1)”。

    b. 在“**工作類型**”下拉式清單中，選取“**啟動處理程序**”。

    c. 在“**工作名稱**”欄位中，輸入簡要說明。

    d. 選擇以下選項之一：

    - **將工作分配給管理群組**

      此工作被指派給管理群組中包含的裝置。您可以指定現有群組之一或建立新群組。

      例如，如果訊息特定於特定管理群組中包含的裝置，您可能想要使用此選項來執行向使用者傳送訊息的工作。

如果工作唄指派給管理群組，則工作屬性視窗中不會顯示**「安全性」**索引標籤，因為群組工作受其所套用的群組的安全性設定的約束。

- **手動指定裝置位址或從清單中匯入位址**

  您可以指定您要將工作分配給的裝置的 NetBIOS 名稱、DNS 名稱、IP 位址和 IP 子網路。

  您可能希望使用此選項來執行特定子網路的工作。例如，您可能想要在會計師的裝置上安裝特定應用程式或掃描可能受感染的子網路中的裝置。

- **將工作指派給裝置分類**

  此工作被指派給裝置分類中包含的裝置。您可以指定現有選擇之一。

  例如，您可能希望使用此選項在具有特定作業系統版本的裝置上執行工作。

4. 按照所選工作範圍選項選取裝置。
5. 在**工作範圍**步驟中，指定管理群組、具有特定位址的裝置或裝置分類。

   可用設定取決於上一個步驟中選擇的選項。
6. 配置工作設定：
   a. 在**可執行指令**欄位中，指定要在本機裝置上執行的命令。
   b. 如有必要，請在**命令列參數（可選）**欄位中指定命令列參數。
   c. 如有必要，請在**工作資料夾路徑（可選）**欄位中指定可執行檔的路徑。
7. 在**完成工作建立**步驟中，點擊**完成**按鈕以建立工作並關閉精靈。

   如果您啟用了**建立完成後開啟工作詳情**選項，則工作設定視窗會開啟。在此視窗中，您可以檢查工作參數、修改它們，或根據需要設定工作啟動排程。
8. 點擊新工作。

   工作內容視窗將開啟。
9. 選取**"排程"**標籤。
10. 設定工作排程。

> **注意：**確保電腦已開啟以執行工作。

11. 點擊**儲存**。
12. 若要立即執行工作而不管配置的排程如何，請執行下列操作：
    a. 選中工作旁邊的核取方塊。
    b. 點擊**"執行"**按鈕。

結果，Kaspersky Endpoint Security 將在靜默模式下執行指令和啟動處理程序。您可以在工作內容的**"執行結果"**區域中檢視工作結果。

停止處理程序

您可以使用"*終止處理程序*"工作遠端終止處理程序。例如，您可以遠端終止一個使用"啟動處理程序工作"啟動的網際網路速度測試公用程式。

如果想要禁止執行檔案，您可以配置"執行防禦元件"。您可以禁止執行可執行檔、指令碼、Office 格式的檔案。

"*終止處理程序*"工作有以下限制：

- 您只可以在網頁主控台中配置 EDR Optimum 的工作。

若要建立"終止處理程序"工作：

1. 在網頁主控台的主視窗中，選取"**資產（裝置）**">"**工作**"。
   工作清單開啟。
2. 點擊**新增**。
   新工作精靈啟動。
3. 配置工作設定：
   a. 在"**應用程式**"下拉清單中，選取"Kaspersky Endpoint Security for Mac (12.2.1)"。
   b. 在"**工作類型**"下拉式清單中，選取"**終止處理程序**"。
   c. 在"**工作名稱**"欄位中，輸入簡要說明。
   d. 選擇以下選項之一：
      - **將工作分配給管理群組**

        此工作被指派給管理群組中包含的裝置。您可以指定現有群組之一或建立新群組。

        例如，如果訊息特定於特定管理群組中包含的裝置，您可能想要使用此選項來執行向使用者傳送訊息的工作。

        如果工作唄指派給管理群組，則工作屬性視窗中不會顯示**「安全性」**索引標籤，因為群組工作受其所套用的群組的安全性設定的約束。

      - **手動指定裝置位址或從清單中匯入位址**

        您可以指定您要將工作分配給的裝置的 NetBIOS 名稱、DNS 名稱、IP 位址和 IP 子網路。

        您可能希望使用此選項來執行特定子網路的工作。例如，您可能想要在會計師的裝置上安裝特定應用程式或掃描可能受感染的子網路中的裝置。

      - **將工作指派給裝置分類**

        此工作被指派給裝置分類中包含的裝置。您可以指定現有選擇之一。

        例如，您可能希望使用此選項在具有特定作業系統版本的裝置上執行工作。
4. 按照所選工作範圍選項選取裝置。

5. 在**工作範圍**步驟中，指定管理群組、具有特定位址的裝置或裝置分類。

   可用設定取決於上一個步驟中選擇的選項。

6. 在精靈的此步驟中，在**請指定處理程序應該被終止的檔案**下拉清單中，選擇選項之一併填寫必填欄位。若要指定檔案，您必須輸入檔案的的完整路徑、或檔案雜湊和路徑二者。

   注意：如果您為本機裝置建立此工作，則可以透過 PID 指定處理程序。

7. 如果您希望該工作適用於關鍵系統物件，請選擇 **套用到關鍵系統物件** 核取方塊。

8. 輸入您希望用其權限執行工作的使用者的帳戶認證。點擊**下一步**。

   備足：預設情況下，Kaspersky Endpoint Security 作為系統使用者帳戶 (root) 啟動工作。

9. 在**完成工作建立**步驟中，點擊**完成**按鈕以建立工作並關閉精靈。

   如果您啟用了**建立完成後開啟工作詳情**選項，則工作設定視窗會開啟。在此視窗中，您可以檢查工作參數、修改它們，或根據需要設定工作啟動排程。

10. 點擊新工作。

    工作內容視窗將開啟。

11. 選取"**排程**"標籤。

12. 設定工作排程。

    注意：確保電腦已開啟以執行工作。

13. 點擊**儲存**。

14. 若要立即執行工作而不管配置的排程如何，請執行下列操作：

    a. 選中工作旁邊的核取方塊。

    b. 點擊"**執行**"按鈕。

結果，Kaspersky Endpoint Security 會終止電腦上的處理程序。例如，如果*遊戲*應用程式正在執行，而您終止了 *遊戲*處理程序，應用程式將不儲存資料即關閉。您可以在工作內容的"**結果**"區域中檢視工作結果。

執行防禦

執行防禦可讓人管理可執行檔和指令碼的執行，以及開啟 Office 格式的檔案。這樣的話，您可以（例如）防止執行您認為不安全的應用程式。因此，威脅擴散可以被停止。執行防禦支援一組指令碼解釋器。

執行防禦規則

執行防禦使用執行防禦規則管理使用者對檔案的存取。執行防禦規則是應用程式對物件執行進行回應（例如，封鎖物件執行時）時考慮的一組條件。應用程式根據檔案路徑或者使用 MD5 和 SHA256 雜湊演算法計算的總和檢查碼來識別檔案。

您可以建立執行防禦規則：

- 在偵測詳情中（僅適用於 EDR Optimum）。

  *偵測詳情*是一款用來檢視有關被偵測的威脅的整個收集資訊的工具。偵測詳情包括，例如，出現在電腦上的檔案的歷史。有關管理警示詳情的更多資訊，請參閱Kaspersky Endpoint Detection and Response Optimum 說明。

- 使用群組政策或者本機應用程式設定。您必須輸入檔案路徑或者雜湊（SHA256 或者 MD5），或者檔案路徑和檔案雜湊二者。

您也可以使用命令列本機管理執行防禦。

注意：無法封鎖系統關鍵物件 (SCO) 的啟動。SCO 是作業系統和 Kaspersky Endpoint Security for Mac 應用程式要求能夠執行的檔案。

執行防禦規則模式

執行防禦元件可以在兩種模式下工作：

- **僅統計**

  在此模式中，Kaspersky Endpoint Security 會將嘗試執行可執行物件或者開啟匹配防護規則條件的文件的事件發佈到卡巴斯基安全管理中心事件記錄和統一記錄系統，但是不會封鎖執行或者開啟物件或者文件的嘗試。預設情況下已選擇此項。

- **啟動**

  在此模式中，應用程式會封鎖執行物件或者開啟匹配防護規則條件的文件。應用程式也會將嘗試執行物件或者開啟文件的事件發佈到卡巴斯基安全管理中心事件記錄和統一記錄系統。

管理執行防禦

重要：您只可以在網頁主控台中配置元件設定。

要防止執行：

1. 在網頁主控台的主視窗中，選取**"裝置"→"政策和設定檔"**。
2. 點擊 Kaspersky Endpoint Security for Mac 政策的名稱。

   政策內容視窗將開啟。

3. 選取“**應用程式設定**”標籤。

4. 轉到**Detection and Response** > **Endpoint Detection and Response**。

5. 開啟**執行防禦**切換開關。

6. 在“**執行或開啟被禁止物件時的動作**”塊中，選擇元件操作模式：

   - **封鎖並寫入報告**。在此模式中，應用程式會封鎖執行物件或者開啟匹配防護規則條件的文件。應用程式也會將嘗試執行物件或者開啟文件的事件發佈到卡巴斯基安全管理中心事件記錄和統一記錄系統。

   - **僅記錄事件**。在此模式中，Kaspersky Endpoint Security 會將嘗試執行可執行物件或者開啟匹配防護規則條件的文件的事件發佈到卡巴斯基安全管理中心事件記錄和統一記錄系統，但是不會封鎖執行或者開啟物件或者文件的嘗試。預設情況下已選擇此項。

7. 建立執行防禦規則清單：

   a. 點擊**新增**。

   b. 在開啟的對話方塊中，輸入執行防禦規則的名稱（例如應用程式 A）。

   c. 在**類型**下拉清單中，選擇要封鎖的物件：“**應用程式**”、“**指令碼**”、“**文件**”。

   如果您選擇了錯誤的物件類型，則 Kaspersky Endpoint Security 不封鎖檔案或者指令碼。

   d. 若要新增檔案，您必須輸入檔案的雜湊（SHA256 或者 MD5）、檔案的完整路徑、或雜湊和路徑二者。

   注意：如果檔案位於網路磁碟機上，請按以下列方式輸入檔案路徑：/Volumes/shared_folder_name/filename。如果檔案路徑包含網路磁碟機字母，則 Kaspersky Endpoint Security 不封鎖檔案或者指令碼。

   a. 點擊**OK**。

8. 存儲變更。

結果，Kaspersky Endpoint Security 會封鎖執行物件：執行可執行檔和指令碼，開啟 Office 格式檔案。不過，您可以（例如）在文本編輯器中開啟指令碼檔案（即使執行指令碼被禁止）。當封鎖執行物件時，如果在應用程式設定中啟用了通知，則 Kaspersky Endpoint Security 會顯示一個標準通知。

電腦網路隔離

電腦網路隔離可自動從網路中隔離電腦以回應偵測到洩露指示器 (IOC)，這就是自動模式。您可以在研究偵測到的威脅時手動開啟網路隔離，這就是手動模式。

當開啟網路隔離時，應用程式會斷開電腦上的所有活動連線並封鎖所有新的 TCP/IP 連線，以下連線除外：

- 網路隔離排除項目中列出的連線。
- Kaspersky Endpoint Security 服務安裝的連線。
- 卡巴斯基安全管理中心網路代理啟動的連線。

重要：您只可以在網頁主控台中配置元件設定。

自動網路隔離模式

您可以配置網路隔離自動開啟以回應 IOC 偵測。您可以使用群組政策配置自動網路隔離模式。

如何配置網路隔離自動開啟以回應 IOC 偵測

1. 在網頁主控台的主視窗中，選取**"裝置"**>**"工作"**。
2. 工作清單開啟。
3. 點擊 Kaspersky Endpoint Security 的**"IOC 掃描"**工作。
   工作內容視窗將開啟。
   如有必要，建立IOC 掃描工作。
4. 選取**"應用程式設定"**標籤。
5. 在**"偵測到 IOC 後的動作"**塊中，選擇**"發現 IOC 後發出警報並採取回應操作"**選項，然後是**"將電腦從網路隔離（8 小時）"**核取方塊。
6. 存儲變更。
7. 結果，當偵測到 IOC 時，應用程式會從網路中隔離電腦以防止威脅散佈。

您可以配置在指定時間經過後自動關閉網路隔離。預設情況下，應用程式在開啟網路隔離 8 小時後將其關閉。您也可以手動關閉網路隔離（請參閱下面的指示）。關閉網路隔離後，電腦可以不受限制地使用網路。

如何配置在自動模式中延遲關閉電腦的網路隔離

1. 在網頁主控台的主視窗中，選取**"裝置"**→**"政策和設定檔"**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選取**"應用程式設定"**標籤。
4. 轉到**Detection and Response** > **Endpoint Detection and Response**。
5. 在**"網路隔離"**塊中，點擊**"配置電腦解鎖設定"**。

6. 在開啟的視窗中，選取**距離自動解鎖被隔離的電腦**核取方塊，然後輸入自動關閉網路隔離的延遲時間。

7. 存儲變更。

手動網路隔離模式

您也可以手動開啟和關閉網路隔離。您可以使用卡巴斯基安全管理中心主控台中的電腦屬性配置手動網路隔離模式。

您可以開啟網路隔離：

- 在偵測詳情中（僅適用於 EDR Optimum）。

  *偵測詳情*是一款用來檢視有關被偵測的威脅的整個收集資訊的工具。偵測詳情包括，例如，出現在電腦上的檔案的歷史。有關管理警示詳情的更多資訊，請參閱Kaspersky Endpoint Detection and Response Optimum 說明。

- 使用本機應用程式設定。

如何手動開啟電腦的網路隔離

1. 在網頁主控台的主視窗中，選取**"裝置"**>**"受管理裝置"**。

2. 選取要為其配置本機應用程式設定的電腦。

   這將開啟電腦內容。

3. 選取**"應用程式"**標籤。

4. 點擊 **Kaspersky Endpoint Security for Mac**。

   這將開啟本機應用程式設定。

5. 選取**"應用程式設定"**標籤。

6. 轉到**Detection and Response** > **Endpoint Detection and Response**。

7. 在**"網路隔離"**塊中，點擊**"將電腦從網路隔離"**。

您可以配置在指定時間經過後自動關閉網路隔離。預設情況下，應用程式在開啟網路隔離 8 小時後將其關閉。關閉網路隔離後，電腦可以不受限制地使用網路。

如何配置延遲手動關閉電腦的網路隔離

1. 在網頁主控台的主視窗中，選取**"裝置"**>**"受管理裝置"**。

2. 選取要為其配置本機應用程式設定的電腦。

   這將開啟電腦內容。

3. 選取**"工作"**標籤。

   這將顯示電腦上可用的工作清單。

4. 選擇**網路隔離**。

5. 選取"**應用程式設定**"標籤。

6. 在開啟的視窗中，選擇關閉網路隔離的延遲。

7. 存儲變更。

如何手動關閉電腦的網路隔離

1. 在網頁主控台的主視窗中，選取"**裝置**">"**受管理裝置**"。

2. 選取要為其配置本機應用程式設定的電腦。

3. 這將開啟電腦內容。

4. 選取"**應用程式**"標籤。

5. 點擊 Kaspersky Endpoint Security for Mac。

6. 這將開啟本機應用程式設定。

7. 選取"**應用程式設定**"標籤。

8. 轉到**Detection and Response** > **Endpoint Detection and Response**。

9. 在"**網路隔離**"塊中，點擊"**解除封鎖被從網路隔離的電腦**"。

您也可以使用命令列本機停用網路隔離。

網路隔離排除項目

您可以配置網路隔離排除項目。當開啟網路隔離時，電腦上匹配規則的網路連線不會被封鎖。

要配置網路隔離排除項目，您可以使用標準網路設定檔清單。預設情況下，排除項目包括包含確保裝置（具有 DNS/DHCP 伺服器和 DNS/DHCP 用戶端角色）不中斷操作的規則的網路設定檔。您也可以修改標準網路設定檔的設定或者手動定義排除項目（請見以下指示）。

重要：只有當網路隔離回應偵測到的威脅自動開啟時，政策內容中指定的排除項目才會套用。只有當網路隔離在卡巴斯基安全管理中心主控台的電腦內容中手動開啟時，電腦內容中指定的排除項目才會套用。

注意：活動政策不會阻止套用在電腦內容中配置的網路隔離的排除項目，因為這些參數有不同的使用案例。

如何自動新增網路隔離排除項目

1. 在網頁主控台的主視窗中，選取"**裝置**"→"**政策和設定檔**"。

2. 點擊 Kaspersky Endpoint Security 政策的名稱。

3. 政策內容視窗將開啟。

4. 選取"**應用程式設定**"標籤。

5. 轉到**Detection and Response** > **Endpoint Detection and Response**。

6. 在**"網路隔離排除項目"**塊中，點擊**"排除項目"**。

7. 在下一個視窗中，點擊**從設定檔新增**，然後選擇標準網路設定檔以設定排除項目。

8. 來自設定檔的網路隔離排除項目被新增至網路隔離排除項目清單。您可以檢視網路連線的內容。如有必要，您可以修改網路連線設定。

9. 如有必要，手動新增網路隔離排除項目。為此，在排除項目清單視窗中點擊**"新增"**並手動編輯網路連線設定。

10. 存儲變更。

如何手動新增網路隔離排除項目

1. 在網頁主控台的主視窗中，選取**"裝置"**>**"受管理裝置"**。

2. 選取要為其配置本機應用程式設定的電腦。

3. 這將開啟電腦內容。

4. 選取**"工作"**標籤。

5. 這將顯示電腦上可用的工作清單。

6. 選擇**網路隔離**工作。

7. 選取**"應用程式設定"**標籤。

8. 在開啟的視窗中，點擊**排除項目**。

9. 在下一個視窗中，點擊**從設定檔新增**，然後選擇標準網路設定檔以設定排除項目。

10. 來自設定檔的網路隔離排除項目被新增至網路隔離排除項目清單。您可以檢視網路連線的內容。如有必要，您可以修改網路連線設定。

11. 如有必要，手動新增網路隔離排除項目。為此，在排除項目清單視窗中點擊**"新增"**並手動編輯網路連線設定。

12. 存儲變更。

您也可以使用命令列本機檢視網路隔離排除項目清單。在這種情況下，電腦必須被隔離。

Cloud Sandbox

Cloud Sandbox 技術可讓您偵測電腦上的進階威脅。Kaspersky Endpoint Security 自動將被偵測檔案轉寄到 Cloud Sandbox 進行分析。Cloud Sandbox 在隔離環境中執行這些檔案以識別惡意活動和決定其信譽。有關這些檔案的資料然後被傳送到卡巴斯基安全網路。因此，如果 Cloud Sandbox 偵測到一個惡意檔案，Kaspersky Endpoint Security 將執行適當操作在偵測到該檔案的所有電腦上消除該威脅。

重要：若要 Cloud Sandbox 作業，您必須啟用使用卡巴斯基安全網路。

備註：如果您正在使用卡巴斯基私有安全網路，則 Cloud Sandbox 技術不可使用。

若要啟用 Cloud Sandbox：

1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選取"**應用程式設定**"標籤。
4. 前往 **內置代理設定 → Endpoint Detection and Response** 部分。
5. 選擇 **Cloud Sandbox** 頁簽。
6. 開啟**Cloud Sandbox**撥動開關。
7. 存儲變更。

每當有威脅，Kaspersky Endpoint Security 就會在"**威脅偵測**"部分的"應用程式主視窗"中為使用 Cloud Sandbox 偵測到的威脅啟動計數器。Kaspersky Endpoint Security 也會在卡巴斯基安全管理中心主控台的威脅報告中指明 Cloud Sandbox 威偵測技術。

FileVault 磁碟加密

Kaspersky Endpoint Security 允許遠端管理 FileVault 加密。加密可防止未經授權的使用者存取儲存在使用者電腦啟動磁碟上的敏感資料。

當管理員從卡巴斯基安全管理中心在電腦上啟動 FileVault 加密時，Kaspersky Endpoint Security 會提示此電腦的使用者輸入他或她的憑據。只有在使用者提供憑據、電腦重新啟動、電腦上收到策略設定已過去 30 分鐘後，磁碟加密才會啟動。提示輸入憑據的最小間隔也是 30 分鐘。

為了防止使用者在啟用 FileVault 加密時解密 Mac 的啟動磁碟，管理員需要使用 JAMF 部署禁止磁碟解密的 MDM 設定檔。若要使用禁止磁碟解密的 MDM 設定檔解密 Mac 的啟動磁碟，管理員首先需要刪除該設定檔。

注意：如果卡巴斯基安全管理中心中未啟用 FileVault 加密管理，具有管理員權限的使用者可以從系統設定加密和解密其 Mac 啟動磁碟。有關 FileVault 的更多資訊，請參閱 Apple 文件。

如果電腦有多個電腦帳戶，FileVault 加密會使除輸入其憑據的使用者之外的所有使用者都無法存取該磁碟。

允許其他使用者解鎖磁碟

1. 選擇**Apple 功能表>系統設定>隱私權與安全**。
2. 點選 **FileVault**。
   FileVault 視窗將開啟。
3. 點擊**啟用使用者**。
4. 在開啟的視窗中，選擇授權解鎖電腦的使用者。
5. 輸入使用者電腦帳戶的密碼，然後點擊**確定**。
6. 點擊**繼續**。

使用者可以存取加密的磁碟。

注意：需要管理員權限才能允許其他使用者解鎖磁碟。

如果管理員透過卡巴斯基安全管理中心管理主控台、網頁主控台或雲端主控台管理 Kaspersky Endpoint Security，該電腦的使用者忘記或遺失其憑據並且無法存取加密磁碟，則管理員可以獲得還原金鑰。

如何使用卡巴斯基安全管理中心管理主控台取得還原金鑰

如何使用卡巴斯基安全管理中心網頁主控台和雲端主控台取得還原金鑰

密碼防護

Kaspersky Endpoint Security 允許透過設定管理員密碼來限制使用者裝置上不需要的操作。

如果啟用了密碼防護，Kaspersky Endpoint Security 在嘗試執行下列任一操作時需要密碼：

- 配置應用程式設定
- 結束應用程式
- 刪除產品授權金鑰
- 移除應用程式

注意：密碼防護僅限制透過解除安裝程式執行 Kaspersky Endpoint Security 的刪除。

- 從備份還原隔離檔案
- 檢視報告

停用密碼防護不會停用政策設定。如果政策中禁止編輯設定，則即使停用密碼防護也無法編輯該設定。

使用管理主控台啟用密碼防護

1. 啟動管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，點擊**"受管理裝置"**。
4. 在工作區選擇**"政策"**標籤。
5. 右鍵點擊要設定的政策並選擇**內容**。
6. 在**屬性**視窗中，選擇**其他設定>使用者互動**。
7. 在**密碼防護**部分中，選取**啟用密碼防護**核取方塊。
8. 在開啟的**密碼防護設定**視窗中，配置以下設定：
   - 在**密碼**欄位中輸入密碼，然後在**確認密碼**欄位中再次輸入該密碼。
   - 在**要求密碼以**部分中，選取所需的核取方塊以防護使用者裝置上的對應操作。
9. 點擊**"確定"**儲存變更。
10. 執行下列操作之一以套用政策變更：
    - 儲存變更後，點擊**套用**以保留在**內容：<政策名稱>**視窗中。
    - 儲存變更後，點擊**確定**關閉**內容：<政策名稱>**視窗。

使用管理主控台編輯密碼防護設定

1. 啟動管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，點擊**"受管理裝置"**。
4. 在工作區選擇**"政策"**標籤。
5. 右鍵點擊要設定的政策並選擇**內容**。
6. 在**屬性**視窗中，選擇**其他設定>使用者互動**。
7. 在**密碼防護**部分中，點擊**設定**按鈕。
8. 在開啟的**密碼防護設定**視窗中，編輯要變更的設定。
9. 點擊**"確定"**儲存變更。

使用網頁主控台啟用密碼防護

1. 在網頁主控台的主視窗中，選取**"裝置"**→**"政策和設定檔"**。
2. 點擊 Kaspersky Endpoint Security for Mac 政策的名稱。

3. 政策內容視窗將開啟。

4. 選取"**應用程式設定**"標籤。

5. 選擇**其他設定** > **使用者互動**。

6. 打開**密碼防護**切換開關。

7. 在開啟的**密碼防護設定**視窗中，配置以下設定：

   - 在**密碼**欄位中輸入密碼，然後在**確認密碼**欄位中再次輸入該密碼。預設情況下，出於安全原因會隱藏密碼字元。若要檢視密碼，請點擊**顯示**。

   - 在**要求密碼**部分中，選取所需的核取方塊以防護使用者裝置上的對應操作。

8. 點擊**確定**關閉**密碼防護設定**對話方塊。

9. 點擊**確定**關閉**使用者互動**部分。

10. 按一下**儲存**以儲存對政策的變更。

使用網頁主控台編輯密碼防護

1. 在網頁主控台的主視窗中，選取"**裝置**"→"**政策和設定檔**"。

2. 點擊 Kaspersky Endpoint Security for Mac 政策的名稱。

3. 政策內容視窗將開啟。

4. 選取"**應用程式設定**"標籤。

5. 選擇**其他設定** > **使用者互動**。

6. 在**密碼防護**部分中，點擊**設定**按鈕。

7. 在開啟的**密碼防護設定**對話方塊中，編輯要變更的設定。

8. 點擊**確定**關閉**密碼防護設定**對話方塊。

9. 點擊**確定**關閉**使用者互動**部分。

10. 按一下**儲存**以儲存對政策的變更。

使用 Kaspersky Endpoint Security 應用程式啟用密碼防護

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。

2. 在**介面**標籤的**密碼防護**部分中，選中**啟用密碼防護**核取方塊。

3. 在開啟的視窗中，配置以下設定：

   - 在**密碼**欄位中輸入密碼，然後在**確認密碼**欄位中再次輸入該密碼。

   - 在**要求密碼以**部分中，選取所需的核取方塊以防護使用者裝置上的對應操作。

4. 點擊**OK**。

> **注意：**如果您選擇變**變更應用程式設定**作為密碼防護操作，則需要輸入密碼兩次才能變更密碼防護設定。

使用 Kaspersky Endpoint Security 應用程式編輯密碼防護

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在**介面**標籤的**密碼防護**部分中，點擊**設定**。
3. 在開啟的視窗中，編輯要變更的設定。
4. 點擊**OK**。

弱點利用防禦

弱點利用防禦元件可偵測利用電腦上的弱點來擅用管理員權限或者執行惡意活動的程式代碼。例如，弱點利用可以利用緩衝區溢位攻擊。為了實現這一點，弱點利用程式會向易受攻擊的應用程式傳送大量資料。在處理這些資料時，存在弱點的應用程式會執行惡意程式碼。這次攻擊的結果是，弱點可以啟動未經授權的惡意軟體安裝。當存在從易於感染的應用程式執行可執行檔的嘗試，並且該嘗試並非由使用者執行時，Kaspersky Endpoint Security 將封鎖該檔案執行或通知使用者。

預設情況下，弱點利用防禦處於啟用狀態。如有必要，您可以停用弱點利用防禦。

使用網頁主控台啟用/停用弱點利用防禦

1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選取"**應用程式設定**"標籤。
4. 前往 **主機威脅防護 → 行為分析 → 弱點利用防禦** 部分。
5. 使用**弱點利用防禦**撥動開關啟用或停用該元件。
6. 如果弱點利用防禦已啟用，請選擇在偵測到弱點利用時執行下列操作之一：
   - **封鎖**
     如果選擇此項，在偵測到弱點時，Kaspersky Endpoint Security 會封鎖此弱點的操作，並生成一條包含此弱點相關資訊的日誌項目。
   - **通知**
     如果選擇此項目，當 Kaspersky Endpoint Security 偵測到弱點利用時，它將記錄一條包含弱點利用資訊的項目並將此弱點利用的相關資訊新增到活動威脅清單。
7. 存儲變更。

使用管理主控台啟用/停用弱點利用防禦

1. 啟動管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，點擊**"受管理裝置"**。
4. 在工作區選擇**"政策"**標籤。
5. 右鍵點擊要設定的政策並選擇**內容**。
6. 在**屬性**視窗中，選擇**進階威脅防護>弱點利用防禦**。
7. 選擇或取消選擇**啟用弱點利用防禦**核取方塊。
8. 如果有必要，在 **偵測到弱點利用時** 部分，選擇當 Kaspersky Endpoint Security 偵測到弱點利用時要執行的操作。
9. 點擊**"確定"**儲存變更。
10. 執行下列操作之一以套用政策變更：
    - 儲存變更後，點擊**套用**以保留在**內容：<政策名稱>**視窗中。
    - 儲存變更後，點擊**確定**關閉**內容：<政策名稱>**視窗。

使用 Kaspersky Endpoint Security 應用程式啟用/停用弱點利用防禦

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。

   此時會開啟應用程式設定視窗。
2. 在**進階**頁簽的"弱點利用防禦"部分中，選擇或取消選擇**啟用弱點利用防禦**核取方塊。
3. 如果勾選**啟用行為偵測**核取方塊，請選擇在偵測到惡意軟體活動時要執行的下列操作之一：
    - **自動封鎖危險惡意軟體活動**

      如果選擇此項，在偵測到弱點時，Kaspersky Endpoint Security 會封鎖此弱點的操作，並生成一條包含此弱點相關資訊的日誌項目。
    - **通知**

      如果選擇此項目，當 Kaspersky Endpoint Security 偵測到弱點利用時，它將記錄一條包含弱點利用資訊的項目並將此弱點利用的相關資訊新增到活動威脅清單。

檢視弱點利用防禦報告

1. 在功能表列中，選擇**防護 > 報告**。

   報告視窗將開啟。
2. 開啟 **弱點利用防禦** 索引標簽。

修復引擎

修復引擎允許 Kaspersky Endpoint Security 復原惡意軟體在作業系統中執行的操作。

回溯作業系統中的惡意軟體活動時，Kaspersky Endpoint Security 將處理以下類型的惡意軟體活動：

- **檔案活動**
  Kaspersky Endpoint Security 執行以下操作：
  - 刪除惡意軟體建立的可執行檔（在網路磁碟機以外的所有媒體上）。
  - 刪除已被惡意軟體滲透的程式所建立的可執行檔。
  - 還原已被惡意軟體修改或刪除的檔案。
- **系統活動**
  Kaspersky Endpoint Security 執行以下操作：
  - 終止由惡意軟體啟動的處理程序。
  - 終止惡意應用程式滲透的處理程序。
  - 不會恢復已被惡意軟體停止的處理程序。
- **網路活動**
  Kaspersky Endpoint Security 執行以下操作：
  - 封鎖惡意軟體的網路活動。

惡意軟體操作的回溯可以由檔案威脅防護或行為偵測元件啟動，也可以在惡意軟體掃描期間啟動。

回溯惡意軟體操作會影響嚴格定義的資料集。回溯不會對作業系統或電腦資料的完整性產生不利影響。

在管理主控台中啟用/停用修復引擎

1. 啟動管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，點擊**"受管理裝置"**。
4. 在工作區選擇**"政策"**標籤。
5. 右鍵點擊要設定的政策並選擇**內容**。
6. 在**屬性**視窗中，選擇**進階威脅防護>修復引擎**。
7. 選擇或取消選擇**啟用修復引擎**核取方塊。
8. 點擊**"確定"**儲存變更。

9. 執行下列操作之一以套用政策變更：

- 儲存變更後，點擊**套用**以保留在**內容：<政策名稱>**視窗中。
- 儲存變更後，點擊**確定**關閉**內容：<政策名稱>**視窗。

在 Web 主控台中啟用/停用修復引擎

1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選取"**應用程式設定**"標籤。
4. 前往 **主機威脅防護 → 行為分析 → 修復引擎** 部分。
5. 使用**修復引擎**撥動開關啟用或停用該元件。
6. 存儲變更。

在應用程式介面中啟用/停用修復引擎

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在**進階**索引標籤的"**修復引擎**部分中，選擇或取消選擇**啟用修復引擎**核取方塊。

因此，如果啟用了修復引擎，則 Kaspersky Endpoint Security 將復原由作業系統中的惡意應用程式執行的操作。

Web 控制

Web 控制可管理使用者對 Web 資源的存取。這有助於減少流量和對工作時間的不當使用。當使用者嘗試開啟受 Web 控制限制的網站時，Kaspersky Endpoint Security 將阻止存取或顯示警告。

您可以封鎖對特定網站或選定類別網站的存取。

註： Kaspersky Endpoint Security 應用程式只能阻止存取使用 HTTPS 進行連線的網站。只有在選取**基本**部分中**一般**頁簽上 的**檢查安全連線 (HTTPS)** 核取方塊時，該應用程式才會掃描加密連線 (HTTPS)。

在管理主控台中新增規則

1. 啟動管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，點擊"**受管理裝置**"。
4. 在工作區選擇"**政策**"標籤。
5. 右鍵點擊要設定的政策並選擇**內容**。

6. 在 **屬性** 視窗中，選擇 **安全控制** > **Web 控制**。
7. 選擇 **啟用 Web 控制** 核取方塊。
8. 點擊**新增**。
9. 在開啟的視窗中，輸入規則名稱。
10. 如果您希望規則生效，請選擇 **啟動的規則** 核取方塊。
11. 執行以下操作之一：
    - 如果您希望規則套用於特定網址，請選擇 **按遮罩分類的網址或一組網址** 選項。
    - 如果您希望規則套用於特定網站類別，請選擇 **網站類別** 選項。
12. 點選 **指定**。
13. 在開啟的視窗中，指定規則範圍。
14. 執行以下操作之一：
    - 如果您希望 Kaspersky Endpoint Security 封鎖存取，請選擇 **封鎖** 選項。
    - 如果您希望 Kaspersky Endpoint Security 允許存取，請選擇 **允許** 選項。
    - 如果您希望 Kaspersky Endpoint Security 顯示警告，請選擇 **顯示警告** 選項。
15. 點擊**"確定"**儲存變更。
16. 執行下列操作之一以套用政策變更：
    - 儲存變更後，點擊**套用**以保留在**內容：<政策名稱>**視窗中。
    - 儲存變更後，點擊**確定**關閉**內容：<政策名稱>**視窗。

在 Web 主控台中新增規則

1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選取"**應用程式設定**"標籤。
4. 前往 **安全控制 → Web 控制**。
5. 打開 **Web 控制** 開關。
6. 點擊**新增**。
7. 在開啟的視窗中，輸入規則名稱。

8. 執行以下操作之一：

   - 如果您希望規則生效，請選擇 **啟動** 選項。
   - 如果您希望規則處於非活動狀態，請選擇 **未啟動** 選項。

9. 執行以下操作之一：

   - 如果您希望 Kaspersky Endpoint Security 允許存取，請選擇 **允許** 選項。
   - 如果您希望 Kaspersky Endpoint Security 封鎖存取，請選擇 **封鎖** 選項。
   - 如果您希望 Kaspersky Endpoint Security 顯示警告，請選擇 **顯示警告** 選項。

10. 執行以下操作之一：

    - 如果您希望規則套用於特定網站類別，請選擇 **類別** 選項並點擊 **選擇類別** 來選擇類別。
    - 如果您希望規則套用於特定網址，請選擇 **單個位址** 選項並將它們新增到下表中。

11. 存儲變更。

註： 無法在 Kaspersky Endpoint Security 應用程式中管理 Web 控制設定。

裝置控制

裝置控制可管理使用者對安裝在電腦上或者連線到電腦的裝置的存取。這樣，當連線此類裝置時，您就可以防護電腦免受感染，並防止資料遺失或外洩。

裝置存取級別

裝置控制在以下級別控制存取：

- **裝置類型**。您可以控制對硬碟、卸除式磁碟、軟碟、CD/DVD 磁碟機和 Wi-Fi 網路的存取。
  您可以如下設定裝置存取：
  - 允許。
  - 封鎖。
  - 封鎖但有例外（僅限 Wi-Fi）。
- **受信任裝置**。受信任裝置是受信任裝置設定中指定的使用者始終具有完全存取權限的裝置。

您可以根據以下資料新增受信任裝置：

- **按 ID 分類裝置**。每個裝置都有一個唯一的 ID（硬體 ID，HWID）。您可以使用作業系統工具在裝置屬性中檢視該 ID。裝置 ID 範例：SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000。如果您想新增多個特定裝置，透過 ID 新增裝置會很方便。

- **按型號分類裝置**。每個裝置都有一個供應商 ID (VID) 和一個產品 ID (PID)。您可以使用作業系統工具在裝置屬性中檢視這些 ID。用於輸入VID 和 PID 的範本：VID_1234&PID_5678。如果您在組織中使用某種型號的裝置，按型號添加裝置會很方便。這樣，您就可以新增該型號的所有裝置了。

- **按 ID 遮罩分類裝置**。如果您使用具有相似 ID 的多個裝置，則可以使用遮罩將裝置新增至受信任清單。`*` 字元可替換任意字元集。輸入遮罩時，Kaspersky Endpoint Security 不支援 `?` 字元。例如， `WDC_C*`。

- **按型號遮罩分類裝置**。如果您使用具有相似 VID 或 PID 的多個裝置（例如，來自相同製造商的裝置），則可以使用遮罩將裝置新增至受信任清單。`*` 字元可替換任意字元集。輸入遮罩時，Kaspersky Endpoint Security 不支援 `?` 字元。例如，`VID_05AC&PID_*`。

在管理主控台中管理裝置控制元件

1. 啟動管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，點擊**"受管理裝置"**。
4. 在工作區選擇**"政策"**標籤。
5. 右鍵點擊要設定的政策並選擇**內容**。
6. 在 **屬性** 視窗中，選擇 **安全控制** > **裝置控制**。
7. 選擇 **啟用裝置控制** 核取方塊。
8. 在 **裝置類型** 頁簽上，設定裝置類型和 Wi-Fi 網路的存取規則。
9. 在 **受信任裝置** 頁簽上，配置單個裝置或者裝置群組的存取規則。
10. 點擊**"確定"**儲存變更。
11. 執行下列操作之一以套用政策變更：
    - 儲存變更後，點擊**套用**以保留在**內容：<政策名稱>**視窗中。
    - 儲存變更後，點擊**確定**關閉**內容：<政策名稱>**視窗。

在網頁主控台中管理裝置控制元件

1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選取**"應用程式設定"**標籤。
4. 前往 **安全控制** > **裝置控制**。

5. 打開 **裝置控制** 開關。

6. 在 **裝置控制設定** 頁簽上，配置裝置、裝置類型和 Wi-Fi 網路的存取規則。

7. 存儲變更。

註： 無法在 Kaspersky Endpoint Security 應用程式中管理裝置控制設定。

因此，如果啟用了裝置控制，應用程式會將已連線裝置的資訊傳遞到卡巴斯基安全管理中心。您可以在卡巴斯基安全管理中心的 **進階 → 儲存庫 → 硬體資料夾**中檢視已連線裝置的清單。

檢視裝置控制報告

1. 在功能表列中，選擇**防護 > 報告**。

   報告視窗將開啟。

2. 開啟**裝置控制**頁簽。

加入卡巴斯基安全網路

當您參與卡巴斯基安全網路時，Kaspersky Endpoint Security 統計資訊將自動傳送到卡巴斯基，以加強對您的 Mac 的防護。

注意：卡巴斯基不會在沒有您明確同意的情況下收集、處理或儲存任何個人資料。

加入卡巴斯基安全網路完全出於自願。在安裝應用程式時決定是否加入。您之後可隨時變更決定。

啟用卡巴斯基安全網路

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在 **進階** 索引標籤的**KSN**部分，點擊**顯示 KSN 聲明**檢視卡巴斯基安全網路聲明。
3. 如果您希望 Kaspersky Endpoint Security 使用從卡巴斯基安全網路收到的有關檔案、Web 資源和應用程式的信譽資訊，並且您接受聲明的所有條款，請選中**加入卡巴斯基安全網路**核取方塊。
4. 在開啟的視窗中，點擊**確認**。

   加入卡巴斯基安全網路和**啟用延伸 KSN 模式**核取方塊將被選取。

注意：預設情況下，Kaspersky Endpoint Security 使用延伸 KSN 模式。*延伸 KSN 模式*是 Kaspersky Endpoint Security 向 Kaspersky 傳送附加資料的一種模式。如果您不想向卡巴斯基提供這些資料，請取消選取**啟用延伸 KSN 模式**核取方塊。

當使用卡巴斯基安全網路時向卡巴斯基提供的資料

如果勾選**加入卡巴斯基安全網路**核取方塊並且取消勾選**啟用延伸 KSN 模式**核取方塊，Kaspersky Endpoint Security 將向卡巴斯基提供以下資料：

- 所使用授權的相關資訊： 授權的類型和有效期、授權失效前的天數、向其購買授權的合作夥伴的識別碼、區域啟動中心識別碼、啟動碼的總和檢查碼、SHA1 演算法計算的票證內容雜湊、授權票證建立日期與時間、授權資訊識別碼、授權票證識別碼、授權票證順序識別碼、使用者電腦的唯一識別碼、授權票證有效開始日期、授權票證有效結束日期、授權票證目前狀態、票證標題版本、授權版本、票證標題簽章憑證識別碼、金鑰檔案的總和檢查碼、票證標題簽署者序號、身分驗證權杖。

- 所安裝軟體的完整版本；
  已安裝軟體的類型；
  軟體更新 ID； 聲譽服務的 ID； 協定類型 ID； 區域啟動中心的 ID； 已撤銷軟體服務決策清單版本； 軟體病毒資料庫中的已觸發記錄 ID； 軟體病毒資料庫中的已觸發記錄時間戳記； 觸發的軟體病毒資料庫記錄類型； 電腦上應用程式安裝實例的唯一 ID； 產品授權啟動日期； 授權失效日期； 授權識別碼； 軟體所使用授權的狀態； 目前處理中物件的總和檢查碼類型； 偵測到的惡意軟體名稱或是可能用於傷害使用者裝置或資料的合法軟體名稱； 目前處理中物件的總和檢查碼； 軟體啟動碼的總和檢查碼； 軟體的完整版本； 唯一裝置 ID； 軟體 ID； 軟體金鑰檔案的總和檢查碼； 用於提供軟體授權的資訊模型 ID； 用於簽署軟體授權票證標頭的憑證識別碼； 軟體授權票證建立日期和時間； 軟體授權票證總和檢查碼； 軟體授權票證版本； 軟體啟動碼版本； 權利持有人基礎架構請求資料格式； 啟動的產品授權票證 ID； 軟體元件 ID； 軟體動作結果； 錯誤代碼； 網路服務的已存取位址（URL、IP）； 通訊埠編號； 網路服務請求來源（推薦者）的網址； 認證的公開金鑰； 所掃描物件與雜湊演算法的數位憑證指紋。

如果勾選**加入卡巴斯基安全網路**和**啟用延伸 KSN 模式**核取方塊，Kaspersky Endpoint Security 會向卡巴斯基提供以下資料：

- 作業系統版本和已安裝在電腦上的服務套件版本的相關資訊；目前和預設的作業系統語言設定；作業系統內核檔案的版本和總和檢查碼（MD5、SHA2-256、SHA1）；作業系統執行模式的參數； 作業系統版本、作業系統組建編號、作業系統更新編號、作業系統版本、作業系統版本延伸資訊； 作業系統服務包版本； 作業系統啟動的日期和時間； 行為分析子系統中關於作業系統的事件處理延遲時間； 延遲的目前類型作業系統動作事件數； 主動式防禦子系統中關於作業系統的事件處理延遲時間； 已處理的作業系統動作事件數； 已處理的同步作業系統動作事件數； 延遲的目前類型作業系統動作事件總數； 常設事件儲存子系統中關於作業系統的事件處理延遲時間； 延遲的作業系統動作事件總數； 等待中的同步作業系統動作事件數； 作業系統中一項動作收到事件的日期和時間。

- 有關上次作業系統重新啟動失敗的資訊： 重新啟動失敗的次數。

- 權利持有人之已安裝應用程式和病毒防護狀態的相關資訊： 軟體安裝 ID（PCID）； 軟體資料庫記錄版本； 電腦上應用程式安裝實例的唯一識別碼、應用程式類型、應用程式類型 ID、所安裝的應用程式的完整版本、應用程式設定版本的識別碼、電腦類型的識別碼、已安裝應用程式的電腦的唯一識別碼、權利持有人服務中的唯一使用者識別碼、本機語言和操作狀態、所安裝軟體元件的版本及其操作狀態、用於連線權利持有人服務的協定版本； 所安裝軟體的完整版本； 已安裝軟體的類型； 軟體更新 ID； 聲譽服務的 ID； 協定類型 ID； 區域啟動中心的 ID； 已撤銷軟體服務決策清單版本； 軟體病毒資料庫中的已觸發記錄 ID； 軟體病毒資料庫中的已觸發記錄時間戳記； 觸發的軟體病毒資料庫記錄類型； 電腦上應用程式安裝實例的唯一 ID； 產品授權啟動日期； 授權失效日期； 授權識別碼； 軟體所使用授權的狀態； 目前處理中物件的總和檢查碼類型； 偵測到的惡意軟體名稱或是可能用於傷害使用者裝置或資料的合法軟體名稱； 目前處理中物件的總和檢查碼； 軟體啟動碼的總和檢查碼； 軟體的完整版本； 軟體 ID； 軟體金鑰檔案的總和檢查碼； 用於提供軟體授權的資訊模型 ID； 用於簽署軟體授權票證標頭的憑證識別碼； 軟體授權票證建立日期和時間； 軟體授權票證總和檢查碼； 軟體授權票證版本； 軟體啟動碼版本； 權利持有人基礎架構請求資料格式； 啟動的產品授權票證 ID； 軟體元件 ID； 軟體動作結果； 錯誤代碼； 網路服務的已存取位址（URL、IP）； 通訊埠編號； 網路服務請求來源（推薦者）的網址； 防毒資料庫的更新適用週期數； 防毒資料庫上次更新和套用的日期和時間； 軟體資料庫的發佈日期與時間； 軟體元件版本； 軟體更新 ID； 已安裝軟體的類型； System Watcher 開始的日期和時間； 軟體的安裝日期和時間； 由 System Watcher 傳送統計資料的可能性； 由 System Watcher 處理，需時超過標準時間的事件碼； 由 System Watcher 處理，需時超過標準時間的事件的資料庫處理時間； 由 System Watcher 處理一項事件的最大允許時間； 由 System Watcher 處理，需時超過標準時間的事件處理時間； 由 System Watcher 處理，需時超過標準時間的事件總數。

- 所有被處理物件與操作的相關資訊： 軟體對被處理物件的判定； 目錄碼； 處理中物件的大小； 處理中物件的總和檢查碼 (SHA256)； 系統監控環境中偵測到的軟體數量； 被系統監控偵測到的軟體的日期和時間； 偵測特徵； 軟體病毒資料庫中的已觸發記錄 ID； 系統監控偵測軟體的原因； 處理中物件的總和檢查碼 (MD5)； 模組完整性檢查的結果； 目前處理中物件的名稱； 觸發的軟體病毒資料庫記錄類型； 所處理物件的路徑； 被掃描物件的名稱； 掃描的日期和時間； 從其下載的 URL 和 Referrer 位址； 被掃描檔案的大小及其路徑； 壓縮檔案標誌； 檔案建立日期與時間； 封包程式的名稱、大小和總和檢查碼（MD5、SHA2-256）（如果檔案被封包）； 檔案的熵； 檔案的類型； 檔案類型代碼； 可執行檔的標誌、ID 和格式； 物件的總和檢查碼（MD5、SHA2-256）； 物件的補充總和檢查碼的類型和值； 有關物件的數位簽章（憑證）的資料： 憑證發行者相關資料、自上一次傳送統計資料後物件的啟動次數、應用程式掃描工作的 ID、收取有關物件信譽的資訊的方式、目標篩選條件值、適用偵測技術的技術參數； 所處理物件的路徑； 目錄碼。

- 對於可執行檔： 檔案區段熵、聲譽驗證旗標或檔案簽署旗標、名稱、類型、ID 類型、總和檢查碼 (MD5)、經驗證物件所載入應用程式的大小、應用程式路徑和範本路徑、自動執行清單中表明狀態的屬性、登錄日期、屬性清單、封裝程式名稱、應用程式數位簽章相關資訊： 發行商憑證、以 MIME 格式上傳的檔案名稱、檔案組建日期與時間。

- 啟動的應用程式及其模組的相關資訊： 總和檢查碼（MD5、SHA2-256）、大小、屬性、建立日期、加殼器名稱（如果檔案已加殼）、檔案名稱、有關係統上執行的處理程序的資訊（處理程序 ID (PID)、處理程序名稱、有關啟動處理程序的帳戶的資訊、啟動處理程序的應用程式和命令、處理程序檔案的完整路徑以及啟動命令列、處理程序所屬應用程式的敘述（處理程序的名稱）應用程式和有關發布者的資訊），以及正在使用的數位憑證和驗證其真實性所需的資訊或有關缺少檔案數位簽章的資訊），以及有關載入到處理程序中的模組的資訊： 它們的名稱、大小、類型、建立日期、屬性、總和檢查碼（MD5、SHA2-256、SHA1）、它們的路徑、PE 檔案標頭資訊、加殼器名稱（如果檔案已加殼）、有關可用性的資訊以及這些統計資料的有效性、產生正在傳送的統計資料的模式的識別碼。

- 若偵測到威脅或弱點，除了所偵測物件的相關資訊以外，還需提供下列資訊：識別碼、版本及病毒資料庫中的記錄類型、根據卡巴斯基分類的威脅名稱、病毒資料庫上一次更新的日期與時間、可執行檔名稱、要求威脅偵測 URL 之應用程式檔案的總和檢查碼 (MD5)、已偵測威脅的 IP 位址（IPv4 或 IPv6）、弱點識別碼及其威脅等級、偵測到弱點的網頁的 URL 與參照位址。

- 若偵測到潛在惡意物件，提供的相關資訊包括程序記憶體中的資料。

- 網路攻擊資訊： 發動攻擊的電腦 IP 位址、網路攻擊指向的使用者電腦連接埠號、攻擊協定的 ID、攻擊的名稱和類型。

- 網路連線相關資訊： 啟動程序而開啟連接埠的檔案版本及總和檢查碼 (MD5、SHA2-256、SHA1)、程序檔案的路徑及其數位簽章、本機及遠端 IP 位址、本機及遠端連接埠號、連線狀態、連接埠開啟的時間戳記。

- 偵測到有害或可疑內容的網頁 URL 和 IP 位址、要求該 URL 的檔案名稱、大小和總和檢查碼、用來達到判定結果之規則的識別碼、加權與程度、攻擊目標。

- 有關已安裝應用程式和病毒資料庫更新的資訊： 更新工作的完成狀態、更新期間可能發生的錯誤類型、更新失敗的次數、執行更新之應用程式元件的識別碼。

- 卡巴斯基安全網路 (KSN) 的使用相關資訊： KSN 識別碼、軟體識別碼、應用程式完整版本、使用者裝置的去個人化 IP 位址、KSN 要求履行品質指標、KSN 封包處理品質指標、KSN 要求數目指標與 KSN 要求類型相關資訊、開始傳送統計資料的日期與時間、結束傳送統計資料的日期與時間、KSN 配置更新相關資訊： 活動配置的識別碼、收到的配置的識別碼、配置更新的錯誤代碼。

- 系統記錄事件相關資訊： 偵測到事件的記錄檔名稱、事件的類型與分類、事件來源名稱以及事件描述。

- 用於確定檔案和 URL 位址信譽的資訊： 請求信譽的 URL 位址和參照位址、連線的協定類型、應用程式類型的內部識別碼、正在使用的連接埠號、使用者識別碼、掃描檔案的總和檢查碼 (MD5)、偵測到的威脅的類型、用於偵測威脅的記錄的資訊（病毒資料庫的記錄識別碼、記錄時間戳記和類型）； 認證的公開金鑰； 所掃描物件與雜湊演算法的數位憑證指紋。

- 應用程式地區分佈相關資料： 應用程式安裝和啟動日期、提供應用程式啟動授權的合作夥伴 ID、應用程式 ID、應用程式語言本機化 ID、應用程式啟動授權序號、KSN 加入簽章。

- 所使用授權的相關資訊： 授權的類型和有效期、授權失效前的天數、向其購買授權的合作夥伴的識別碼、區域啟動中心識別碼、啟動碼的總和檢查碼、SHA1 演算法計算的票證內容雜湊、授權票證建立日期與時間、授權資訊識別碼、授權票證識別碼、授權票證順序識別碼、使用者電腦的唯一識別碼、授權票證有效開始日期、授權票證有效結束日期、授權票證目前狀態、票證標題版本、授權版本、票證標題簽章憑證識別碼、金鑰檔案的總和檢查碼、票證標題簽署者序號、身分驗證權杖。

- 電腦上所安裝的硬體相關資訊： 內建和已連線裝置的類型、名稱、型號名稱、韌體版本、參數。

- 裝置資訊： 裝置 ID。

- Web 控制元件的作業資訊：
  元件版本、分類原因、其他分類原因的相關資訊、分類 URL、被封鎖 / 分類物件的主機 IP 位址。

注意：根據卡巴斯基安全管理中心設定，您可以參與卡巴斯基私人安全網路而不是卡巴斯基安全網路。當 Kaspersky Endpoint Security 從卡巴斯基私人安全網路切換到卡巴斯基安全網路時，它會通知您並提示您接受卡巴斯基安全網路聲明的條款。有關參與卡巴斯基私人安全網路的詳細資訊，請參閱卡巴斯基安全管理中心說明。

卡巴斯基安全網路基礎架構

Kaspersky Endpoint Security 支援以下卡巴斯基安全網路基礎架構解決方案：

- *全球 KSN* 是大多數 Kaspersky 應用程式使用的解決方案。KSN 參與者從卡巴斯基安全網路接收資訊，並向 Kaspersky 傳送使用者電腦上偵測到的物件的資訊，以便 Kaspersky 分析人員進行額外分析，並包括在卡巴斯基安全網路的信譽和統計資料庫中。
- *私有 KSN* 是讓承載 Kaspersky Endpoint Security 或其他 Kaspersky 應用程式的電腦的使用者獲得卡巴斯基安全網路信譽資料庫以及其他統計資料的存取權限的解決方案，無需從他們自己的電腦向卡巴斯基安全網路傳送資料。私有 KSN 專為因以下任一原因無法參與卡巴斯基安全網路的公司客戶所設計：
  - 本機工作站未連線網際網路。
  - 法律禁止或公司安全政策限制將任何資料傳輸到國家/地區外部或公司 LAN 外部。

預設情況下，卡巴斯基安全管理中心使用全球 KSN。您可以在卡巴斯基安全管理中心管理主控台 (MMC) 和卡巴斯基安全管理中心網頁主控台中設定私有 KSN 的使用。無法在卡巴斯基安全管理中心雲端主控台中設定“私有 KSN”的使用。

KSN 代理

受卡巴斯基安全管理中心管理伺服器管理的電腦可以透過 KSN 代理服務與卡巴斯基安全網路互動。

KSN 代理服務提供以下功能：

- 使用者的電腦可以查詢的 KSN 和將資訊送交 KSN，即使沒有直接連線網際網路。
- KSN 代理服務暫存處理過的資料，從而減少外部網路通訊信道上的負荷，並加快接收使用者的電腦請求的資訊的速度。

有關 KSN 代理服務的更多詳細資訊，請參閱卡巴斯基安全管理中心說明。

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

檢查應用程式元件的完整性

Kaspersky Endpoint Security 包含動態連結程式庫、可執行檔、設定檔和介面檔案形式的各種二進位模組。入侵者可能會用包含惡意代碼的其他檔案取代一個或多個應用程式可執行模組或檔案。為了防止這種情況，Kaspersky Endpoint Security 可以檢查應用程式元件的完整性。該應用程式可檢查模組和檔案是否有未經授權的變更或損壞。如果應用程式模組或檔案的總和檢查碼不正確，則視為已損壞。該應用程式可檢查模組和檔案是否有未經授權的變更或損壞。如果應用程式模組或檔案的總和檢查碼不正確，則視為已損壞。

應用程式元件的完整性使用位於 /Library/Application Support/Kaspersky Lab/KAV/Binaries 目錄中的 integrity_checker 公用程式進行檢查。該公用程式可檢查包含應用程式檔案清單的清單檔案的完整性，這些應用程式檔案的完整性對於應用程式元件的正確操作至關重要。

受卡巴斯基加密簽章防護的 integrity_check.xml 清單檔案位於與 integrity_checker 公用程式相同的目錄中 (/Library/Application Support/Kaspersky Lab/KAV/Binaries)。

注意：執行 integrity_checker 公用程式需要根使用者帳戶權限。

完整性檢查可以使用與應用程式一起安裝的公用程式或使用經過認證的 CD 上的公用程式來執行。

若要檢查應用程式元件的完整性，請執行下列命令：

```
sudo "/Library/Application Support/Kaspersky Lab/KAV/Binaries/integrity_checker"
```

預設情況下，該公用程式使用位於 /Library/Application Support/Kaspersky Lab/KAV/Binaries 目錄中的 integrity_check.xml 檔案。

若要顯示公用程式設定的說明，請執行以下命令：

```
--help
```

檢查每個清單檔案的結果會顯示在清單檔案名稱旁邊，格式如下：

- `SUCCEEDED` — 檔案的完整性已確認（返回碼`0`）
- `FAILED` — 未確認檔案的完整性（返回碼不是`0`）

透過卡巴斯基安全管理中心管理主控台管理應用程式

卡巴斯基安全中心旨在集中管理企業網路安全。有關卡巴斯基安全管理中心的詳細資訊，請參閱卡巴斯基安全管理中心說明。

您也可以透過應用程式的圖形使用者介面、卡巴斯基安全管理中心網頁主控台和雲端主控台以及命令列來管理 Kaspersky Endpoint Security。

在企業網路上部署 Kaspersky Endpoint Security

1. 在網路上部署*管理伺服器*。

   管理伺服器是卡巴斯基安全管理中心的一個元件，它集中儲存有關公司網路中安裝的所有卡巴斯基應用程式的資訊並管理這些應用程式。

2. 在卡巴斯基安全管理中心管理員工作站上安裝*管理主控台*。

   管理主控台是卡巴斯基安全管理中心的一個元件，為管理伺服器和*網路代理*的管理服務提供使用者介面。網路代理協調管理伺服器與安裝在公司網路內電腦上的 Kaspersky Endpoint Security 之間的互動。

3. 在卡巴斯基安全管理中心管理員的工作站上安裝 Kaspersky Endpoint Security 管理外掛程式。

   *管理外掛程式*是一個專用元件，提供透過管理主控台管理卡巴斯基應用程式的介面。每個應用程式都有自己的管理外掛程式。此管理外掛程式適用於所有可從卡巴斯基安全管理中心管理的卡巴斯基應用程式。

4. 透過以下方式之一在遠端 Mac 電腦上安裝網路代理：

   - 本機
   - 遠端使用 Apple 遠端桌面
   - 遠端透過卡巴斯基安全管理中心
   - 遠端使用 SSH 協定

   注意：要透過卡巴斯基安全管理中心管理 Kaspersky Endpoint Security for Mac 12.2.1，您必須在遠端電腦上安裝網路代理版本 15。

5. 透過以下方式之一在遠端 Mac 電腦上安裝 Kaspersky Endpoint Security：

   - 本機
   - 遠端使用 Apple 遠端桌面
   - 遠端使用 SSH 協定
   - 遠端透過卡巴斯基安全管理中心

重要資訊：如果遠端電腦上安裝了 for Mac 版卡巴斯基安全軟體或第三方惡意軟體防護軟體，請在安裝 Kaspersky Endpoint Security 之前將其解除安裝。

有關如何部署管理伺服器和安裝管理主控台的詳細資訊，請參閱卡巴斯基安全管理中心說明。

將 Kaspersky Endpoint Security 版本 11.1 或更高版本更新至版本 12.2.1

注意：要透過卡巴斯基安全管理中心管理 Kaspersky Endpoint Security for Mac 12.2.1，您必須在遠端電腦上安裝網路代理版本 15。

您可以透過以下方式之一將透過卡巴斯基安全管理中心管理的 Kaspersky Endpoint Security 從版本 11.1 或更高版本更新至版本 12.2.1：

- 同時將遠端電腦上的 Kaspersky Endpoint Security 更新至版本 12.2.1，將網路代理更新至版本 15。
- 首先將網路代理更新至版本 15，然後將 Kaspersky Endpoint Security 更新至版本 12.2.1。

當將應用程式更新為較新版本時，請考慮以下事項：

- 要將 Kaspersky Endpoint Security 更新到版本 12.2.1，需要 macOS 14 或更高版本。
- 您需要從技術支援網站下載 KES_11.3_profile.zip 壓縮檔案以套用新的設定檔。
- 將 Kaspersky Endpoint Security 更新至版本 12.2.1 後，網路設定中可能會出現兩個 Kaspersky Filter 和兩個 Kaspersky Monitor 項目。
- 如果您擁有 Kaspersky Endpoint Security 版本 11.0.1 或更早版本，若要將應用程式更新至版本 12.2.1，您需要解除安裝該應用程式並將 macOS 更新至版本 14 或更高版本。然後您可以安裝 Kaspersky Endpoint Security 版本 12.2.1。

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

準備遠端安裝 Kaspersky Endpoint Security

本節包含在卡巴斯基安全管理中心管理員工作站上安裝 Kaspersky Endpoint Security 管理外掛程式以及在遠端電腦上安裝網路代理的資訊。

安裝 Kaspersky Endpoint Security 管理外掛程式和網路代理是透過卡巴斯基安全管理中心安裝 Kaspersky Endpoint Security 的先決條件。

安裝 Kaspersky Endpoint Security 管理外掛程式

Kaspersky Endpoint Security 管理外掛程式提供了一個透過管理主控台管理 Kaspersky Endpoint Security 的介面。

安裝 Kaspersky Endpoint Security 管理外掛程式

1. 在卡巴斯基安全管理中心管理員工作站上，解壓縮包含 Kaspersky Endpoint Security 安裝套件檔案的壓縮檔案。
2. 開啟包含 Kaspersky Endpoint Security 安裝套件檔案的資料夾。
3. 雙擊 klcfginst.exe。

Kaspersky Endpoint Security 管理外掛程式開始安裝。

重要提示：在安裝 Kaspersky Endpoint Security 管理外掛程式之前，請關閉卡巴斯基安全管理中心管理員工作站上的管理主控台。

本機安裝網路代理

網路代理協調管理伺服器與安裝在公司網路內電腦上的 Kaspersky Endpoint Security 之間的互動。

本機安裝網路代理

1. 在遠端電腦上，開啟具有網路代理分發套件的資料夾。
2. 開啟網路代理分發套件（DMG 檔案）。
   一個包含分發套件內容的視窗將開啟。
3. 在包含分發套件內容的視窗中，雙擊**卡巴斯基網路代理**。
4. **點擊繼續**確認您要安裝網路代理。
5. 在**簡介**視窗中，點擊**繼續**。
6. 在**產品授權**視窗中，閱讀您與 AO Kaspersky Lab 之間的網路代理最終使用者產品授權協議的文字。請執行以下操作：
   - 若要接受協議的所有條款並繼續安裝，請**點擊繼續**。
   - 若要列印協議文字，請點擊**列印**。
   - 若要將協定儲存為文字檔案，請點擊**儲存**。

7. 在確認視窗中，執行以下操作之一：

   - 若要繼續安裝網路代理，請點擊**同意**。
   - 若要返回最終使用者產品授權協議的文字，請點擊**閱讀產品授權**。
   - 若要取消安裝，請點擊**不同意**。

8. 在**設定**視窗中，執行以下操作：

   a. 在**伺服器**欄位中，指定安裝卡巴斯基安全管理中心的伺服器的 IP 位址或 DNS 名稱。

   b. 在**連接埠**欄位中，指定與伺服器的未加密連線的連接埠號。

   c. 在**SSL 連接埠**欄位中，指定與伺服器的 SSL 連線的連接埠號。

   d. 如果您想在安裝後立即啟動網路代理，請勾選**安裝後執行**核取方塊。

   如果您不想使用 SSL 連線到伺服器，請取消選擇**使用 SSL**核取方塊。若要繼續安裝，請點擊**繼續**。

9. 在**安裝類型**視窗中，閱讀有關將在其上安裝網路代理的磁碟的資訊。
   若要使用建議的設定安裝網路代理，請點擊**安裝**並輸入管理員密碼以確認您的選擇。
   等待網路代理安裝程式完成應用程式元件的安裝。

10. 點擊**關閉**結束安裝程式。

使用 Apple 遠端桌面安裝網路代理

1. 在遠端電腦上，選取**Apple 功能表>系統設定>一般>共用**。
2. 選擇**遠端管理**核取方塊。
3. 在您想要作為伺服器的另一台 Mac 上，安裝 Apple 遠端桌面。有關 Apple 遠端桌面的更多資訊，請參閱 Apple 支援。
4. 開啟 Apple 遠端桌面。
5. 在**遠端桌面**視窗中，點擊左側的**掃描器**，然後選擇要安裝網路代理的裝置。
6. 點擊**複製**。
7. 點選 + 並選擇網路代理安裝檔案：DMG 檔案、KUD 檔案和 SH 檔案。
8. 在**將項目放入**彈出式功能表中，選擇**磁碟的頂部資料夾**。
9. 點擊**複製**。
10. 檔案複製成功後，點擊**Unix**。
11. 輸入以下命令：

```
cd /;
./install.sh --accept_eula -r <管理伺服器位址>
```

其中<管理伺服器位址>是卡巴斯基安全管理中心管理伺服器的 DNS 名稱或 IP 位址。

注意：輸入此命令即表示您接受最終使用者產品授權協議。

12. 選擇以**使用者**身分執行命令並在欄位中鍵入“root”。
13. 點擊**傳送**。

網路代理安裝在選定的裝置上開始。

使用卡巴斯基安全管理中心安裝網路代理

卡巴斯基安全管理中心使用 SSH 連線在用戶端電腦上安裝網路代理。

在用戶端電腦上安裝網路代理之前，請確保滿足以下條件：

- 卡巴斯基安全管理中心管理伺服器部署在公司網路上。
- 管理主控台安裝在卡巴斯基安全管理中心管理員工作站上。
- 遠端登入在遠端電腦上啟用。
- 將用於執行遠端安裝工作的專用管理員帳戶在遠端電腦上建立。您可以使用網域帳戶進行安裝。
- 專用帳戶的 sudo 密碼已停用。

建立網路代理安裝套件

1. 啟動卡巴斯基安全管理中心管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹中，選擇**“進階”**資料夾，然後選擇**“遠端安裝”**子資料夾，然後選擇**“安裝套件”**子資料夾。
4. 在工作區中，點擊**建立安裝套件**。
5. 在**選擇安裝套件類型**視窗中，點擊**為卡巴斯基應用程式建立安裝套件**。
6. 在**定義安裝套件名稱**視窗中，在**名稱**欄位中輸入新安裝套件的名稱，然後點擊**下一步**。
7. 在**選擇安裝的分發套件**視窗中，點擊**瀏覽**。
   選擇用於建立安裝套件的檔案的視窗將開啟。
8. 開啟包含網頁代理安裝套件內容的資料夾，然後選擇 klnagent.kud 檔案。
   選擇要安裝的分發套件視窗將顯示要使用已新增的檔案遠端安裝的應用程式的名稱和版本。
9. 點擊**下一步**。
   Kaspersky Endpoint Security 安裝套件使用指定設定建立。
10. 在精靈的最後一個視窗中，點擊**結束**退出新建套件精靈。

在用戶端電腦上建立遠端安裝網路代理工作

1. 啟動卡巴斯基安全管理中心管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 選取"**工作**"資料夾。
4. 在工作區中，透過單擊**新工作**啟動新建工作精靈。
5. 按照下面新建工作精靈的步驟操作，建立用於在用戶端電腦上遠端安裝 Kaspersky Endpoint Security 的工作。

若要繼續精靈的下一步，請點擊**下一步**。若要返回精靈的上一步，請點擊←。若要在任何步驟結束精靈，請點擊**取消**。

注意：按鈕的外觀可能會有所不同，具體取決於您的 Windows 版本。

步驟 1.選擇工作類型

1. 在**選擇工作類型**視窗中，最大化**卡巴斯基安全管理中心管理伺服器**節點。
2. 選擇**遠端安裝應用程式**工作。

步驟 2.選擇安裝套件

在**選擇安裝套件**視窗中，執行下列操作之一：

- 如果之前已經建立了具有所需設定的網路代理安裝套件，請在**選擇安裝套件**視窗上部的安裝套件清單中選擇它。
- 如果尚未建立所需的安裝套件，請點擊**新建**啟動新建套件精靈。

步驟 3.配置安裝設定：

在**設定**視窗中，執行以下操作：

1. 選擇**透過管理伺服器使用作業系統資源**核取方塊。
2. 取消選擇所有其他核取方塊。

步驟 4.選擇安裝後要新增電腦的管理群組

在**移至受管理裝置清單**視窗中，選擇安裝後電腦將移至的群組（如有必要）。

步驟 5.定義如何選擇要為其建立工作的用戶端電腦

在**選擇將工作指派到的裝置**視窗中，選擇要用於指定用戶端電腦的方法：

- 若要從管理伺服器在網路上偵測到的電腦中進行選擇，請選擇**選擇管理伺服器偵測到的網路裝置**選項。
- 若要手動指定電腦的 IP 位址或從檔案匯入電腦的 IP 位址，請選擇**手動指定裝置位址或從清單匯入位址**選項。
- 若要根據預設條件為所選的裝置建立工作，請選擇**將工作指派給裝置選擇**選項。
- 若要從特定管理群組中選擇電腦，請選擇**將工作指派給管理群組**選項。

步驟 6.選擇用戶端電腦

在開啟的視窗中（**選擇裝置**、**裝置選擇**或**選擇管理群組**，取決於您在上一個步驟中選擇的選項），選擇用戶端電腦、指定電腦的 IP 位址、指定電腦選擇、或選擇工作將被套用到的管理群組。

步驟 7.選取要執行工作的帳戶

1. 在**選擇執行工作的帳戶**視窗中，選取**所需帳戶（不使用網路代理）**核取方塊。
2. 點擊**新增 > 帳戶**。

   帳戶視窗將開啟。
3. 輸入遠端電腦的專用管理員帳戶的登入名稱和密碼。
4. 點擊**OK**。

步驟 8.設定工作排程

1. 在**設定工作排程**視窗中，在**排程啟動**下拉清單中選擇啟動模式。
2. 如有必要，將排程工作配置為自動啟動（透過指定工作開始日期和時間）。
3. 如果您想要執行應用程式無法依照排程啟動的工作（例如，因為電腦在排程時間關閉），請勾選**執行錯過的工作**核取方塊。

   一旦阻止工作啟動的障礙被消除，Kaspersky Endpoint Security 就會啟動工作。

步驟 9.指定工作名稱

在**定義工作名稱**視窗的**名稱**欄位中，輸入您正在建立的工作的名稱。

步驟 10.完成建立工作

在**完成工作建立**視窗中，執行以下操作：

1. 如果您希望工作在精靈完成後立即啟動，請勾選**精靈完成後執行工作**核取方塊。
2. 點擊**結束**關閉精靈。

使用 SSH 協定安裝網路代理

在遠端電腦上安裝網路代理的一種方法是使用 SSH 協定。

確保滿足以下要求：

- 卡巴斯基安全管理中心管理伺服器部署在公司網路上。
- 管理主控台安裝在卡巴斯基安全管理中心管理員工作站上。
- 網路代理安裝套件已建立並儲存在管理伺服器的共用資料夾中。
- 遠端登入在遠端電腦上啟用。
- 用於安裝網路代理的電腦帳戶包含在 sudoers 中。

有關安裝套件的詳細資訊，請參閱卡巴斯基安全管理中心說明。

使用 SSH 協定安裝網路代理

1. 在管理員工作站上啟動 SSH 用戶端。
2. 連線到遠端電腦。
3. 將管理伺服器的共用資料夾連線為遠端電腦上的網路磁碟機。為此，請在 SSH 用戶端中輸入以下命令：
   ```
   mkdir /Volumes/KLSHARE
   mount_smbfs //<管理員帳戶>:<密碼>@<管理伺服器 IP 位址>/KLSHARE /Volumes/KLSHARE
   ```
   參數敘述：
   - `<administrator account>` – 管理伺服器上的管理員帳戶的名稱。
   - `<password>` – 管理伺服器上管理員的密碼。
   - `<Administration Server IP address>` – 託管卡巴斯基安全管理中心的伺服器的 IP 位址。
4. 執行安裝指令碼。為此，請在 SSH 用戶端中輸入以下命令：
   ```
   cd /Volumes/KLSHARE/<klnagent_package_folder>
   ```
   其中`<klnagent_package_folder>`是網路代理安裝套件所在的資料夾。
   ```
   sudo ./install.sh --accept_eula [-r <伺服器>] [-p <連接埠號>] [-s use_ssl 0|1] [-l <SSL 連接埠號>] [-x use_proxy 0|1] [ -a <代理>] [-n <代理登入名>] [-w <代理密碼>]
   ```
   參數敘述：
   - `<server>` – 在其上安裝卡巴斯基安全管理中心的伺服器的 IP 位址或 DNS 名稱。
   - `<port number>` – 將用於與管理伺服器建立未加密連線的連接埠號。預設情況下使用 14000 連接埠。
   - `use_ssl 0|1` – 定義在網路代理和管理伺服器之間建立連線時是否使用加密的參數。如果值為“0”，則使用未加密的連線。如果值為“1”，則透過 SSL 協定建立連線（預設值）。
   - `<SSL port number>` – 將用於透過 SSL 協定與管理伺服器建立加密連線的連接埠號。預設情況下使用 13000 連接埠。
   - `use_proxy 0|1` – 定義連線到網際網路時是否使用代理伺服器的參數。如果值為“0”，則不使用代理伺服器。如果值為“1”，則透過代理伺服器建立連線（預設值）。
   - `<proxy>` – 代理伺服器的 IP 位址或 DNS 名稱。
   - `<proxy_login>` – 用於連線代理伺服器的使用者帳戶。
   - `<proxy_password>` – 用於連線代理伺服器的密碼。

   重要提示：執行此命令需要管理員權限。
5. 斷開連線遠端電腦上的網路磁碟機。為此，請在 SSH 用戶端中輸入以下命令：
   ```
   umount /Volumes/KLSHARE
   ```
6. 檢查網路代理在遠端電腦上是否正常運作。為此，請在 SSH 用戶端中輸入以下命令：
   ```
   cd /Library/Application\ Support/Kaspersky\ Lab/klnagent/Binaries/
   ```

```
sudo ./klnagchk
```

如果檢查成功，則網路代理功能正常。

本機解除安裝網路代理

1. 在遠端電腦上，開啟具有網路代理分發套件的資料夾。
2. 開啟網路代理分發套件（DMG 檔案）。
   一個包含分發套件內容的視窗將開啟。
3. 在包含分發套件內容的視窗中，雙擊**Network Agent Uninstaller**。
4. 在**介紹**視窗中，點擊**繼續**。
5. 在**資訊**視窗中，點擊**解除安裝**。
6. 當系統提示您輸入管理員憑據時，輸入管理員名稱和密碼並確認您要解除安裝網路代理。
   解除安裝網路代理開始。
7. 閱讀有關解除安裝的資訊並點擊**完成**以結束移除程式。

網路代理現在被從遠端電腦中刪除。

從命令列管理網路代理

本節包含如何在用戶端電腦上使用命令列管理網路代理的資訊。

您可以在用戶端電腦上使用命令列停止網路代理並再次啟動它。

您也可以使用 klmover 公用程式手動將遠端電腦連線到管理伺服器，並使用 klnagchk 公用程式檢查遠端電腦和管理伺服器之間的連線。

您可以解除安裝網路代理。

在遠端電腦上啟動/停止網路代理

您可以使用命令列在用戶端電腦上停止網路代理並重新啟動它。

停止網路代理

在遠端電腦上，從命令列使用 unload 命令啟動 launchctl 公用程式。

指令語法：

```
sudo launchctl unload /Library/LaunchDaemons/com.kaspersky.klnagent.plist
```

啟動網路代理

在遠端電腦上，從命令列使用 load 命令啟動 launchctl 公用程式。

指令語法：

```
sudo launchctl load /Library/LaunchDaemons/com.kaspersky.klnagent.plist
```

重要資訊：需要管理員權限才能停止和啟動網路代理。

手動檢查用戶端電腦和管理伺服器之間的連線。Klnagchk 公用程式

檢查遠端電腦和管理伺服器之間的連線

在遠端電腦上，從命令列執行 klnagchk 公用程式。

klnagchk 公用程式包含在網路代理分發套件中。

安裝網路代理後，klnagchk 公用程式位於 /Library/Application Support/Kaspersky Lab/klnagent/Binaries 資料夾中。

根據您指定的參數，klnagchk 公用程式會在從命令列執行時執行以下操作：

- 顯示為遠端電腦上安裝的網路代理與管理伺服器之間的連線指定的設定，或將它們儲存在檔案中。
- 將網路代理統計資料（自上次啟動網路代理以來）和公用程式執行結果儲存在檔案中，或在螢幕上顯示此資訊。
- 嘗試在網路代理和管理伺服器之間建立連線。
- 如果該公用程式無法建立連線，它將傳送 ICMP 封包來檢查安裝管理伺服器的電腦的狀態。

執行公用程式之前，請在命令列中前往 /Library/Application Support/Kaspersky Lab/klnagent/Binaries。

指令語法：

```
sudo ./klnagchk [-logfile <檔案名>] [-sp] [-savecert <憑證檔案路徑>] [-restart]
```

重要提示：執行該公用程式需要管理員權限。

參數敘述

`-logfile <file name>` – 將網路代理和管理伺服器之間的連線設定以及公用程式執行結果儲存在檔案中。如果不指定該參數，則螢幕上會顯示伺服器連線設定、執行結果和錯誤訊息。

`-sp` – 在螢幕上顯示代理伺服器驗證的密碼或將其儲存在檔案中。如果網路代理透過代理伺服器連線到管理伺服器，則使用此參數。預設不使用該參數。

`-savecert <file name>` – 將用於在管理伺服器上進行身分驗證的憑證儲存在指定檔案中。

`-restart` – 公用程式完成執行後重新啟動網路代理。

範例:
sudo ./klnagchk -logfile klnagchk.log -sp

手動將遠端電腦連線到管理伺服器。Klmover 公用程式

將遠端電腦連線到管理伺服器

在遠端電腦上，從命令列執行 klmover 公用程式。

klmover 公用程式包含在網路代理安裝套件中。

安裝網路代理後，klmover 公用程式位於 /Library/Application Support/Kaspersky Lab/klnagent/Binaries 資料夾中。

根據您指定的參數，klmover 公用程式在從命令列執行時執行以下操作：

- 使用指定參數將網路代理連線到管理伺服器。
- 將公用程式執行結果儲存在檔案中或將其顯示在螢幕上。

執行公用程式之前，請在命令列中前往 /Library/Application Support/Kaspersky Lab/klnagent/Binaries。

命令列語法：

```
sudo ./klmover [-logfile <檔案名稱>] [-address <伺服器位址>] [-pn <連接埠號>] [-ps <SSL 連接埠號>] [-nossl] [-cert <憑證檔案路徑> ] [-silent] [-dupfix]
```

重要提示：執行該公用程式需要管理員權限。

參數敘述

`-logfile <file name>` – 將執行結果儲存在檔案中。如果不指定該參數，則螢幕上會顯示執行結果和錯誤訊息。

`-address <server address>` – 網路代理用於連線到管理伺服器的位址。您可以指定伺服器的 IP 位址或 DNS 名稱。

注意：您也可以使用具有此參數的命令來變更遠端電腦所連線的管理伺服器的位址。

`-pn <port number>` – 將用於與管理伺服器建立未加密連線的連接埠號。預設情況下使用 14000 連接埠。

`-ps <SSL port number>` – 將用於透過 SSL 協定與管理伺服器建立加密連線的連接埠號。預設情況下使用 13000 連接埠。

`-nossl` – 使用管理伺服器的未加密連線。如果未指定此參數，網路代理將透過加密的 SSL 協定與管理伺服器建立安全連線。

`-cert <path to certificate file>` – 使用指定的憑證檔案在新管理伺服器上進行身分驗證。如果未指定此參數，網路代理將在首次連線到管理伺服器時收到憑證。

`-silent` – 以靜默模式執行該公用程式。

`-dupfix` – 如果網路代理的安裝方式與本說明中所述的方法不同（例如，如果從安裝了網路代理的磁碟映像還原網路代理），則使用此參數。如果網路代理的自動自我識別導致管理主控台中原始電腦和其他電腦的圖示重複，請嘗試重新連線重複的電腦。

注意：執行 klmover 公用程式時，建議指定所有參數的值。

範例:
sudo ./klmover -logfile klmover.log -address 192.0.2.12 -ps 13001

透過網路代理連線到管理伺服器的遠端電腦稱為*用戶端電腦*。

解除安裝網路代理

指令語法：

```
sudo '/Library/Application Support/Kaspersky Lab/klnagent/Binaries/UninstallScript'
```

安裝和解除安裝 Kaspersky Endpoint Security

本節介紹在用戶端電腦上遠端安裝和解除安裝 Kaspersky Endpoint Security。

您也可以在本機或透過卡巴斯基安全管理中心網頁主控台或卡巴斯基安全管理中心雲端主控台安裝或解除安裝 Kaspersky Endpoint Security。

使用 SSH 協定安裝應用程式

在遠端電腦上安裝 Kaspersky Endpoint Security 之前，請確保滿足以下條件：

- 卡巴斯基安全管理中心管理伺服器部署在公司網路上。
- 管理主控台安裝在卡巴斯基安全管理中心管理員工作站上。
- Kaspersky Endpoint Security 安裝套件已建立，位於管理伺服器上的共用資料夾中。
- Kaspersky Endpoint Security 的金鑰檔案儲存在管理伺服器上的共用資料夾中（可選）。

- 遠端登入在遠端電腦上啟用。
- 用於安裝應用程式的電腦帳戶包含在 sudoers 中。

使用 SSH 協定在用戶端電腦上安裝 Kaspersky Endpoint Security

1. 在卡巴斯基安全管理中心管理員工作站上啟動 SSH 用戶端。
2. 連線到遠端電腦。
3. 將管理伺服器的共用資料夾連線為遠端電腦上的網路磁碟機。為此，請在 SSH 用戶端中輸入以下命令：
   ```
   mkdir /Volumes/KLSHARE
   mount_smbfs //<管理員帳戶>:<密碼>@<管理伺服器 IP 位址>/KLSHARE /Volumes/KLSHARE
   ```
   參數敘述：
   - `<administrator account>` – 管理伺服器上的管理員帳戶的名稱。
   - `<password>` – 管理伺服器上管理員的密碼。
   - `<Administration Server IP address>` – 託管卡巴斯基安全管理中心的伺服器的 IP 位址。
4. 執行安裝指令碼。為此，請在 SSH 用戶端中輸入以下命令：
   ```
   cd /Volumes/KLSHARE/<KES 套件資料夾>
   ./install.sh --accept_eula
   ```
   其中 `<KES 套件資料夾>` 是 Kaspersky Endpoint Security 安裝套件所在的資料夾。

   重要提示：執行此命令需要管理員權限。
5. 斷開連線遠端電腦上的網路磁碟機。為此，請在 SSH 用戶端中輸入以下命令：
   ```
   umount /Volumes/KLSHARE
   ```

用卡巴斯基安全管理中心安裝應用程式

在用戶端電腦上安裝 Kaspersky Endpoint Security 之前，請確保滿足以下條件：

- 卡巴斯基安全管理中心管理伺服器部署在公司網路上。
- 管理主控台安裝在卡巴斯基安全管理中心管理員工作站上。
- 網路代理安裝在用戶端電腦上。
- Kaspersky Endpoint Security 安裝套件已建立並儲存在管理伺服器上的共用資料夾中。
- Kaspersky Endpoint Security 的金鑰檔案儲存在管理伺服器上的共用資料夾中（可選）。
- 用戶端電腦將會新增至管理伺服器上的**受管理裝置**管理群組（可選）。

有關管理伺服器上管理群組的詳細資訊，請參閱卡巴斯基安全管理中心說明。

若要使用卡巴斯基安全管理中心在用戶端電腦上安裝 Kaspersky Endpoint Security，您必須建立並啟動**遠端安裝應用程式**工作。

建立在用戶端電腦上遠端安裝 Kaspersky Endpoint Security 的工作

1. 啟動卡巴斯基安全管理中心管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 選取"**工作**"資料夾。
4. 在工作區中，透過單擊**新工作**啟動新建工作精靈。
5. 按照下面新建工作精靈的步驟操作，建立用於在用戶端電腦上遠端安裝 Kaspersky Endpoint Security 的工作。

若要繼續精靈的下一步，請點擊**下一步**。若要返回精靈的上一步，請點擊←。若要在任何步驟結束精靈，請點擊**取消**。

注意：按鈕的外觀可能會有所不同，具體取決於您的 Windows 版本。

步驟 1.選擇工作類型

1. 在**選擇工作類型**視窗中，最大化**卡巴斯基安全管理中心管理伺服器**節點。
2. 選擇**遠端安裝應用程式**工作。

步驟 2.選擇安裝套件

在**選擇安裝套件**視窗中，執行下列操作之一：

- 如果先前已建立具有所需設定的 Kaspersky Endpoint Security 安裝套件，請在**選擇安裝套件**視窗上部的安裝套件清單中選擇它。
- 如果尚未建立所需的安裝套件，請點擊**新建**以啟動新建套件精靈。

步驟 3.安裝其他應用程式

如果您還想在用戶端電腦上安裝網路代理，請在**進階**視窗中選取**將網路代理與此應用程式一起安裝**和 **<網路代理安裝套件名稱>**核取方塊。

注意：網路代理的安裝套件必須事先建立。如果尚未建立，請點擊**建立**以啟動新建套件精靈。

步驟 4.配置安裝設定：

在**設定**視窗中，配置應用程式的遠端安裝。

步驟 5.選擇安裝後要新增電腦的管理群組

在**移至受管理裝置清單**視窗中，選擇安裝後電腦將移至的群組（如有必要）。

注意：如果您在步驟 3 中選擇安裝網路代理，則會出現**移至受管理裝置清單**視窗。

步驟 6.定義如何選擇要為其建立工作的用戶端電腦

在**選擇將工作指派到的裝置**視窗中，選擇要用於指定用戶端電腦的方法：

- 若要從管理伺服器在網路上偵測到的電腦中進行選擇，請選擇**選擇管理伺服器偵測到的網路裝置**選項。
- 若要手動指定電腦的 IP 位址或從檔案匯入電腦的 IP 位址，請選擇**手動指定裝置位址或從清單匯入位址**選項。
- 若要根據預設條件為所選的裝置建立工作，請選擇**將工作指派給裝置選擇**選項。
- 若要從特定管理群組中選擇電腦，請選擇**將工作指派給管理群組**選項。

步驟 7.選擇用戶端電腦

在開啟的視窗中（**選擇裝置**、**裝置選擇**或**選擇管理群組**，取決於您在上一個步驟中選擇的選項），選擇用戶端電腦、指定電腦的 IP 位址、指定電腦選擇、或選擇工作將被套用到的管理群組。

步驟 8.選取要執行工作的帳戶

在**選擇執行工作的帳戶**視窗中，選取**不需要帳戶（已安裝網路代理）**核取方塊。

假定您在啟動此精靈之前已安裝網路代理。

步驟 9.設定工作排程

1. 在**設定工作排程**視窗中，在**排程啟動**下拉清單中選擇啟動模式。
2. 如有必要，將排程工作配置為自動啟動（透過指定工作開始日期和時間）。
3. 如果您想要執行應用程式無法依照排程啟動的工作（例如，因為電腦在排程時間關閉），請勾選**執行錯過的工作**核取方塊。

   一旦阻止工作啟動的障礙被消除，Kaspersky Endpoint Security 就會啟動工作。

步驟 10.指定工作名稱

在**定義工作名稱**視窗的**名稱**欄位中，輸入您正在建立的工作的名稱。

步驟 11.完成建立工作

在**完成工作建立**視窗中，執行以下操作：

1. 如果您希望工作在精靈完成後立即啟動，請勾選**精靈完成後執行工作**核取方塊。
2. 點擊**結束**關閉精靈。

您建立的工作將顯示在**工作**資料夾的工作區中。

建立安裝套件

建立**遠端安裝應用程式**工作時，您可以使用現有安裝套件或建立新安裝套件。若要檢視已建立的安裝套件清單，請點擊**進階>遠端安裝>安裝套件**。

在卡巴斯基安全管理中心中建立安裝套件

1. 啟動卡巴斯基安全管理中心管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。

3. 在主控台樹中，選擇**"進階"**資料夾，然後選擇**"遠端安裝"**子資料夾，然後選擇**"安裝套件"**子資料夾。

4. 在工作區中，點擊**建立安裝套件**。

5. 在**選擇安裝套件類型**視窗中，點擊**為卡巴斯基應用程式建立安裝套件**。

6. 在**定義安裝套件名稱**視窗中，在**名稱**欄位中輸入新安裝套件的名稱，然後點擊**下一步**。

7. 在**選擇安裝的分發套件**視窗中，點擊**瀏覽**。

   選擇用於建立安裝套件的檔案的視窗將開啟。

8. 開啟包含 Kaspersky Endpoint Security 安裝套件內容的資料夾，然後選擇 kesmac.kud 檔案。

   選擇要安裝的分發套件視窗將顯示要使用已新增的檔案遠端安裝的應用程式的名稱和版本。

9. 如有必要，請勾選**將更新從儲存庫複製到安裝套件**核取方塊，將應用程式更新從卡巴斯基安全管理中心儲存空間複製到安裝套件，然後點擊**下一步**。

   安裝套件開始上傳到管理伺服器。上傳完成後，**安裝類型**視窗將開啟。

10. 在**安裝類型**視窗的**要安裝的套件**部分中，選取或取消選取要在用戶端電腦上安裝期間跳過的元件名稱旁的核取方塊，然後點擊**下一步**。

    Kaspersky Endpoint Security 安裝套件使用指定設定建立。

11. 在精靈的最後一個視窗中，點擊**結束**以完成新建套件精靈。

用卡巴斯基安全管理中心解除安裝應用程式

在透過卡巴斯基安全管理中心從用戶端電腦刪除 Kaspersky Endpoint Security 之前，請確保滿足以下條件：

- 卡巴斯基安全管理中心管理伺服器部署在公司網路上。
- 管理主控台安裝在卡巴斯基安全管理中心管理員工作站上。
- 網路代理安裝在用戶端電腦上。

若要透過卡巴斯基安全管理中心從用戶端電腦解除安裝 Kaspersky Endpoint Security，您必須建立並啟動**遠端解除安裝應用程式**工作。

重要提示：從用戶端電腦刪除 Kaspersky Endpoint Security 可能會導致感染風險。

建立從用戶端電腦遠端解除安裝 Kaspersky Endpoint Security 的工作

1. 啟動卡巴斯基安全管理中心管理主控台。

2. 最大化**管理伺服器<伺服器名稱>**節點。

3. 選取**"工作"**資料夾。

4. 在工作區中，透過單擊**新工作**啟動新建工作精靈。

5. 依照下面的新建工作精靈的步驟操作，建立用於從用戶端電腦遠端解除安裝 Kaspersky Endpoint Security 的工作。

若要繼續精靈的下一步，請點擊**下一步**。若要返回精靈的上一步，請點擊←。若要在任何步驟結束精靈，請點擊**取消**。

注意：按鈕的外觀可能會有所不同，具體取決於您的 Windows 版本。

步驟 1.選擇工作類型

1. 在**選擇工作類型**視窗中，最大化**卡巴斯基安全管理中心管理伺服器**節點。
2. 展開**進階**子節點。
3. 選擇**遠端解除安裝應用程式**工作。

步驟 2.選擇要解除安裝的應用程式

在**選擇要解除安裝的應用程式**視窗中，選擇**解除安裝卡巴斯基安全管理中心支援的應用程式**。

步驟 3.配置解除安裝設定

在**設定**視窗中，執行以下操作：

1. 在**"要解除安裝的應用程式"**下拉清單中，選取 **Kaspersky Endpoint Security for Mac 12.2.1**。
2. 點擊**下一步**。
3. 配置應用程式的遠端解除安裝。

步驟 4.選擇作業系統重新啟動選項

在**選擇作業系統重新啟動選項**視窗中，選擇**不重新啟動裝置**選項。

步驟 5.定義如何選擇要為其建立工作的用戶端電腦

在**選擇將工作指派到的裝置**視窗中，選擇要用於指定用戶端電腦的方法：

- 若要從管理伺服器在網路上偵測到的電腦中進行選擇，請選擇**選擇管理伺服器偵測到的網路裝置**選項。
- 若要手動指定電腦的 IP 位址或從檔案匯入電腦的 IP 位址，請選擇**手動指定裝置位址或從清單匯入位址**選項。
- 若要根據預設條件為所選的裝置建立工作，請選擇**將工作指派給裝置選擇**選項。
- 若要從特定管理群組中選擇電腦，請選擇**將工作指派給管理群組**選項。

步驟 6.選擇用戶端電腦

在開啟的視窗中（**選擇裝置**、**裝置選擇**或**選擇管理群組**，取決於您在上一個步驟中選擇的選項），選擇用戶端電腦、指定電腦的 IP 位址、指定電腦選擇、或選擇工作將被套用到的管理群組。

步驟 7.選取要執行工作的帳戶

在**選擇執行工作的帳戶**視窗中，選取**不需要帳戶（已安裝網路代理）**核取方塊。

假定您在啟動此精靈之前已安裝網路代理。

步驟 8.設定工作排程

1. 在**設定工作排程**視窗中，在**排程啟動**下拉清單中選擇啟動模式。
2. 如有必要，將排程工作配置為自動啟動（透過指定工作開始日期和時間）。
3. 如果您想要執行應用程式無法依照排程啟動的工作（例如，因為電腦在排程時間關閉），請勾選**執行錯過的工作**核取方塊。

   一旦阻止工作啟動的障礙被消除，Kaspersky Endpoint Security 就會啟動工作。

步驟 9.指定工作名稱

在**定義工作名稱**視窗的**名稱**欄位中，輸入您正在建立的工作的名稱。

步驟 10.完成建立工作

在**完成工作建立**視窗中，執行以下操作：

1. 如果您希望工作在精靈完成後立即啟動，請勾選**精靈完成後執行工作**核取方塊。
2. 點擊**結束**關閉精靈。

您建立的工作將顯示在**工作**資料夾的工作區中。

透過卡巴斯基安全管理中心啟動和停止應用程式

您可以在透過卡巴斯基安全管理中心管理的裝置清單中選取的電腦上啟動或停止 Kaspersky Endpoint Security。

透過卡巴斯基安全管理中心啟動或停止 Kaspersky Endpoint Security

1. 啟動卡巴斯基安全管理中心管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，點擊"**受管理裝置**"。
4. 選擇包含所需用戶端電腦的管理群組。
5. 選擇**裝置**索引標籤。
6. 從用戶端電腦清單中選擇電腦。
7. 透過以下方式之一開啟**內容：<電腦名稱>**視窗：
   - 雙擊用戶端電腦的名稱。
   - 右鍵點擊用戶端電腦，然後從上下文功能表中選擇**內容**。
8. 選取"**應用程式**"部分。

9. 在**裝置上安裝的卡巴斯基應用程式**清單中，以滑鼠右鍵點擊開啟 **Kaspersky Endpoint Security for Mac (12.2.1)**項目的上下文功能表，然後執行下列其中一項操作：

   - 若要啟動應用程式，請選擇**"啟動"**項目。
   - 若要停止應用程式，請選擇**"停止"**項目。

重要提示： Kaspersky Endpoint Security 停止後，用戶端電腦繼續在不受防護的模式下執行，這可能會導致感染風險。

建立和管理工作

本節介紹如何使用卡巴斯基安全管理中心建立和配置 Kaspersky Endpoint Security 在用戶端電腦或一組電腦上執行的工作。

*工作*是 Kaspersky Endpoint Security 在用戶端電腦上執行的一組可配置操作。

在卡巴斯基安全管理中心中，您可以建立以下工作：

- 新增金鑰
- 快速掃描
- 回溯
- 掃描
- 更新

您可以對工作執行以下操作：

- 啟動和停止工作。
- 配置工作設定。
- 追蹤工作的進度。
- 將工作從一組複製並移動到另一組。
- 刪除工作。
- 匯入和匯出工作。

有關工作的更多資訊，請參閱卡巴斯基安全管理中心說明。

建立工作

當透過卡巴斯基安全管理中心管理 Kaspersky Endpoint Security 時，您可以建立以下類型的工作：

- 本機工作。*本機工作*是在單獨的用戶端電腦上執行的工作。
- 群組工作。*群組工作*是在管理群組中的電腦上執行的工作。
- 任意一組電腦的工作。您可以建立要在任何電腦上執行的工作，無論它們是否屬於管理群組或電腦集合。

為單獨的用戶端電腦建立本機工作

1. 啟動卡巴斯基安全管理中心管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，點擊**"受管理裝置"**。
4. 選擇包含所需用戶端電腦的管理群組。
5. 在工作區選取**"裝置"**標籤。
6. 從用戶端電腦清單中選擇電腦。
7. 透過以下方式之一開啟**內容：<電腦名稱>**視窗：
   - 雙擊用戶端電腦的名稱。
   - 右鍵點擊用戶端電腦，然後從上下文功能表中選擇**內容**。
8. 在**內容：<電腦名稱>**視窗中，選擇**工作**部分。
   所選用戶端電腦的系統工作和自訂工作清單顯示在右側的工作區中。
9. 點擊工作區下方的**新增**。
   新工作精靈啟動。
10. 依照新工作精靈的步驟為單獨的用戶端電腦建立本機工作。

為管理群組中的用戶端電腦建立工作

1. 啟動卡巴斯基安全管理中心管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，點擊**"受管理裝置"**。
4. 選擇包含所需用戶端電腦的管理群組。
5. 在工作區選取**"工作"**標籤。
6. 在工作區中，透過單擊**新工作**啟動新建工作精靈。
7. 依照新工作精靈的步驟為管理群組中包含的用戶端電腦建立工作。

有關如何建立群組工作的詳細資訊，請參閱卡巴斯基安全管理中心說明。

為任意一組電腦建立工作

1. 啟動卡巴斯基安全管理中心管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，點擊 **"工作"**。
4. 在工作區中，透過單擊**新工作**啟動新建工作精靈。
5. 依照新建工作精靈的步驟為任意一組電腦建立工作。

若要繼續精靈的下一步，請點擊**下一步**。若要返回精靈的上一步，請點擊←。若要在任何步驟結束精靈，請點擊**取消**。

注意：按鈕的外觀可能會有所不同，具體取決於您的 Windows 版本。

步驟 1.選擇應用程式並定義工作類型

1. 在**選擇工作類型**視窗中，最大化 **Kaspersky Endpoint Security for Mac (12.2.1)**節點。
2. 選擇您要建立的工作類型：
   - 若要建立新增金鑰的工作，請選擇**新增金鑰**。
   - 若要建立關鍵區域掃描工作，請選擇**快速掃描**。
   - 若要建立工作回溯最新更新，請選擇**回溯**。
   - 若要建立惡意軟體掃描工作，請選擇**掃描**。
   - 若要建立更新工作，請選擇**更新**。

步驟 2.配置所選工作類型的設定

根據上一個步驟中選擇的工作類型，設定視窗的內容可能會有所不同。此視窗對於回溯工作不顯示。

應用程式啟動

在**應用程式啟動**視窗中，執行以下操作：

1. 從卡巴斯基安全管理中心儲存中選擇啟動碼或金鑰，或新增一個電腦上儲存的金鑰檔案。
2. 若要將指定金鑰新增為備用金鑰，請選取**新增為備用金鑰**核取方塊。
   當目前的啟動金鑰到期時，備用金鑰將變為活動狀態。

有關指定金鑰的資訊（金鑰、金鑰類型和金鑰到期日期）顯示在**應用程式啟動**視窗中。

更新

專用卡巴斯基更新伺服器是 Kaspersky Endpoint Security 更新的主要來源。Kaspersky Endpoint Security 也可以使用發佈點、本機資料夾或其他 Web 伺服器作為*更新來源*。

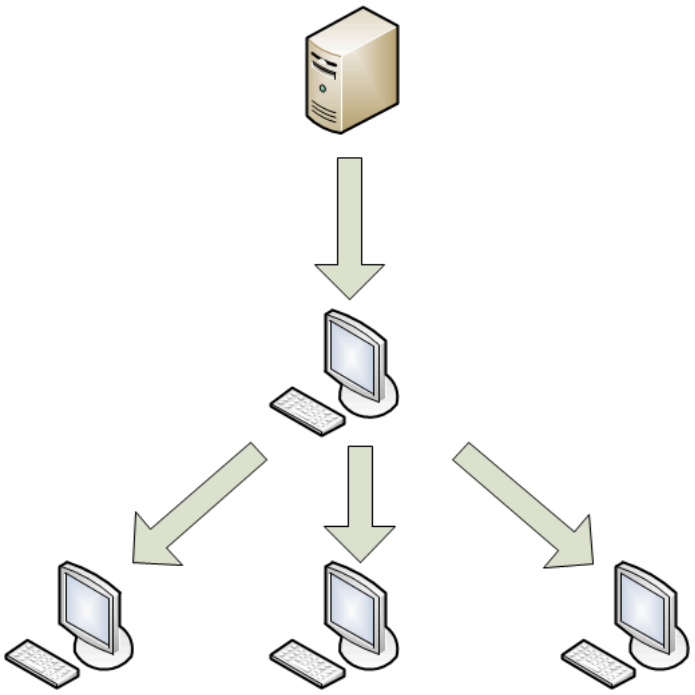
您可以將下載的更新放在本機資料夾中，以更新公司網路中其他電腦上的應用程式資料庫和 Kaspersky Endpoint Security 模組，從而減少網際網路流量。

您可以如下設定更新分發：

1. 網路上的一台電腦從卡巴斯基更新伺服器或其他更新來源接收 Kaspersky Endpoint Security 更新套件。檢索到的更新被放置在共用的本機資料夾中。

   注意：共用的本機資料夾必須提前建立。

2. 網路上的其他電腦將共用的本機資料夾作為更新來源。



透過本機電腦分發更新

如有必要，請在**更新**視窗中編輯更新工作設定：

1. 若要停用應用程式模組更新，請取消選取**更新應用程式模組**核取方塊。
2. 若要變更更新來源：
   a. 點擊**設定**。
      設定：更新視窗將開啟。
   b. 選取您要使用的更新來源旁的核取方塊。
3. 若要指定不同的更新來源，請點擊**新增**。

更新來源視窗將開啟。

a. 指定更新來源的網址或作為更新來源的本機或網路資料夾的路徑，然後點擊**確定**。

b. 點擊**確定**儲存變更並關閉**設定：更新**視窗。

掃描和快速掃描

預設情況下，Kaspersky Endpoint Security 使用**建議**安全等級，在掃描後偵測到感染物件時提示使用者執行操作，並掃描下列物件：

- 所有卸除式磁碟機
- 所有內部磁碟機
- 所有網路磁碟機
- 記憶體

注意： Kaspersky Endpoint Security 不會掃描位於 OneDrive 或 iCloud 儲存或其他雲端儲存中的檔案。請將這些檔案從掃描範圍中排除。否則，掃描工作可能會以*受感染檔案未刪除*錯誤結束。

如有必要，在**掃描**視窗中編輯掃描設定：

1. 選擇預設安全等級之一或自訂安全設定。
2. 指定 Kaspersky Endpoint Security 在偵測到感染物件時執行的操作。
3. 定義掃描範圍。

步驟 3.定義如何選擇要為其建立工作的用戶端電腦

注意：此步驟與本機或群組工作無關。

在**選擇將工作指派到的裝置**視窗中，選擇要用於指定用戶端電腦的方法：

- 若要從管理伺服器在網路上偵測到的電腦中進行選擇，請選擇**選擇管理伺服器偵測到的網路裝置**選項。
- 若要手動指定電腦的 IP 位址或從檔案匯入電腦的 IP 位址，請選擇**手動指定裝置位址或從清單匯入位址**選項。
- 若要根據預設條件為所選的裝置建立工作，請選擇**將工作指派給裝置選擇**選項。
- 若要從特定管理群組中選擇電腦，請選擇**將工作指派給管理群組**選項。

步驟 4.選擇用戶端電腦

注意：此步驟與本機或群組工作無關。

在開啟的視窗中（**選擇裝置**、**裝置選擇**或**選擇管理群組**，取決於您在上一個步驟中選擇的選項），選擇用戶端電腦、指定電腦的 IP 位址、指定電腦選擇、或選擇工作將被套用到的管理群組。

步驟 5.設定工作排程

1. 在**設定工作排程**視窗中，在**排程啟動**下拉清單中選擇啟動模式。
2. 如有必要，將排程工作配置為自動啟動（透過指定工作開始日期和時間）。
3. 如果您想要執行應用程式無法依照排程啟動的工作（例如，因為電腦在排程時間關閉），請勾選**執行錯過的工作**核取方塊。

   一旦阻止工作啟動的障礙被消除，Kaspersky Endpoint Security 就會啟動工作。
4. 如果您希望卡巴斯基安全管理中心自動決定不同電腦上工作啟動之間的時間間隔，請勾選**對工作啟動使用自動隨機延遲**核取方塊。

   這有助於減少卡巴斯基安全管理中心管理伺服器上的負載。
5. 若要手動設定在不同電腦上啟動工作之間的時間間隔，請勾選**在（分鐘）間隔內使用隨機延遲啟動工作**核取方塊並指定分鐘數。

   這有助於減少卡巴斯基安全管理中心管理伺服器上的負載。

步驟 6.指定工作名稱

在**定義工作名稱**視窗的**名稱**欄位中，輸入您正在建立的工作的名稱。

步驟 7.完成建立工作

在**完成工作建立**視窗中，執行以下操作：

1. 如果您希望工作在精靈完成後立即啟動，請勾選**精靈完成後執行工作**核取方塊。
2. 點擊**結束**關閉精靈。

手動啟動和停止工作

排程工作會依照排程自動啟動和停止。但是，您可以隨時手動啟動工作。

注意：工作只有當網路代理正在執行時才會在用戶端電腦上啟動。如果網路代理停止執行，所有活動工作都會中斷。

手動啟動和停止工作

1. 開啟包含要啟動或停止的工作的工作清單。
2. 選擇您要啟動或停止的工作。

3. 透過以下方式之一啟動或停止工作：

   - 右鍵點擊以顯示工作的上下文功能表，然後選擇**“啟動”**或**“停止”**。
   - 在工作區中，點擊**啟動**或**停止**。
   - 右鍵點擊以顯示工作的上下文功能表，然後選擇**內容**。在開啟的視窗中，點擊**啟動**或**停止**。

匯入和匯出工作

您可以將群組工作和任意電腦群組的工作匯出到檔案。

匯出工作

1. 選擇要從中匯出工作的工作清單：

   - 選擇管理群組，然後開啟**工作**索引標籤。
   - 在主控台樹狀目錄中，點擊 **“工作”**。

2. 右鍵點擊要匯出的工作，然後在工作的捷徑功能表中選擇**所有工作 > 匯出**。
3. 在**儲存為**視窗中，指定匯出工作的檔案名稱和儲存位置。
4. 點擊**儲存**。

匯入工作

1. 選擇要將工作匯入的工作清單：

   - 選擇管理群組，然後開啟**工作**索引標籤。
   - 在主控台樹狀目錄中，點擊 **“工作”**。

2. 透過以下任一種方式匯入工作：

   - 在工作清單的捷徑功能表中，選擇**所有工作 > “匯入”**。
   - 點擊**從檔案匯入工作**。

3. 在**開啟**視窗中，指定要匯入的工作檔案的路徑。
4. 點擊**開啟**。

   該工作將顯示在工作清單中。

檢視工作

您可以檢視為特定電腦、特定管理群組中的電腦建立的工作清單或所有非本機工作的清單。

檢視特定管理群組的工作

1. 啟動卡巴斯基安全管理中心管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，點擊**"受管理裝置"**。
4. 選擇包含所需用戶端電腦的管理群組。
5. 在工作區選取**"工作"**標籤。

所選管理群組中電腦的工作清單將顯示。

檢視本機工作

1. 啟動卡巴斯基安全管理中心管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，點擊**"受管理裝置"**。
4. 選擇包含所需用戶端電腦的管理群組。
5. 在工作區選取**"裝置"**標籤。
6. 從用戶端電腦清單中選擇電腦。
7. 透過以下方式之一開啟**內容：<電腦名稱>**視窗：
   - 雙擊用戶端電腦的名稱。
   - 右鍵點擊用戶端電腦，然後從上下文功能表中選擇**內容**。
8. 在**內容：<電腦名稱>**視窗中，選擇**工作**部分。

所選用戶端電腦的系統工作和自訂工作清單顯示在右側的工作區中。

檢視非本機工作

1. 啟動卡巴斯基安全管理中心管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，點擊 **"工作"**。

為可能屬於也可能不屬於管理群組的電腦所建立的非本機工作清單將顯示。

管理特定於工作的設定

檢視本機工作的設定

1. 開啟本機工作清單。
2. 在清單中選擇一個工作，然後透過以下方式之一開啟工作設定：
   - 雙擊工作名稱。
   - 右鍵點擊以顯示工作的捷徑功能表並選擇**內容**。

檢視群組工作的設定

1. 開啟管理群組的群組工作清單。
2. 在清單中選擇一個工作，然後透過以下方式之一開啟工作設定：
   - 雙擊工作名稱。
   - 右鍵點擊以顯示工作的捷徑功能表並選擇**內容**。
   - 點擊工作區中的**配置工作**連結。

檢視非本機工作的設定

1. 開啟非本機工作清單。
2. 在清單中選擇一個工作，然後透過以下方式之一開啟工作設定：
   - 雙擊工作名稱。
   - 右鍵點擊以顯示工作的捷徑功能表並選擇**內容**。
   - 點擊工作區中的**配置工作**連結。

有關工作的更多資訊，請參閱卡巴斯基安全管理中心說明。

對於本機工作、群組工作或任意電腦群組的工作

配置“新增金鑰“工作設定

1. 開啟包含**新增金鑰**工作設定的視窗。
2. 選擇**應用程式啟動**部分。
3. 如有必要，請透過以下方式之一新增另一個金鑰：
   - 若要從新增至卡巴斯基安全管理中心儲存的啟動碼中選擇金鑰或啟動碼：
     a. 選擇**金鑰或啟動碼**選項。
     b. 點擊**瀏覽**。
     “卡巴斯基安全管理中心儲存中的金鑰和啟動碼”視窗將開啟。

c. 選擇金鑰或啟動碼。

d. 點擊**確定**。

- 新增金鑰檔案：

a. 選擇**金鑰檔案**選項。

b. 點擊**新增**。
檔案選擇視窗開啟。

c. 選擇金鑰檔案。

d. 點擊**開啟**。

注意：當新增不同的金鑰時，目前金鑰將被刪除。

4. 若要將指定金鑰新增為備用金鑰，請選取**新增為備用金鑰**核取方塊。
當目前的金鑰到期時，備用金鑰將變為活動狀態。

注意：備用金鑰到期日期必須晚於目前金鑰到期日。

5. 透過以下方式之一儲存變更：

- 儲存變更後，點擊**套用**以保留在**內容：<工作名稱>**視窗中。
- 儲存變更後，點擊**確定**關閉**內容：<工作名稱>**視窗。

管理快速掃描工作設定

1. 開啟包含**快速掃描**工作設定的視窗。
2. 選取"**快速掃描**"部分。
3. 若要變更 Kaspersky Endpoint Security 執行快速掃描工作的安全級別，請在**安全等級**部分中執行下列操作之一：

- 透過向上或向下移動滑桿來選擇預設的安全等級。
您可以選擇以下安全等級之一：

- **最大防護**。Kaspersky Endpoint Security 對已開啟、儲存或執行的檔案執行最大程度的監控。
- **建議**。Kaspersky Endpoint Security 使用卡巴斯基建議的設定監控檔案。
這是預設的安全等級。
- **最高速度**。Kaspersky Endpoint Security 監控最少的檔案集合。如果您想要使用需要大量記憶體資源的其他應用程式，您可以選擇此安全等級。

- 手動配置安全設定：

  a. 點擊**設定**。

  設定：掃描視窗將開啟。

  b. 在**一般**標籤的**檔案類型**部分中，選擇在執行快速掃描工作時 Kaspersky Endpoint Security 應掃描的檔案類型。

  c. 在**一般**標籤的**最佳化**部分中，配置掃描效能設定。

  d. 在**複合檔案**標籤的**一般**部分中，選擇您希望 Kaspersky Endpoint Security 分析哪些複合檔案以尋找可偵測物件。

  e. 在**進階**標籤的**進階設定**部分中，配置 iSwift 技術的使用以及在應用程式統計資料中儲存有關偵測到的物件的資訊。

  f. 在**進階**標籤的**啟發式分析器**部分中，配置啟發式分析器的使用並選擇啟發式分析器在惡意軟體掃描期間套用的防護等級。

  g. 點擊**確定**儲存變更並關閉**設定：掃描**視窗。

  安全等級變更為**自訂**。

- 若要還原預設設定，請點擊**預設**。

  安全等級變更為**建議**。

4. 如有必要，在**操作**部分中，選擇 Kaspersky Endpoint Security 在偵測到感染物件時應執行的操作。

5. 若要指定掃描範圍，請在**掃描範圍**部分中點擊**設定**，然後在開啟的**掃描範圍**視窗中執行下列操作：

   a. 如果您希望 Kaspersky Endpoint Security 掃描電腦記憶體，請選取**記憶體**核取方塊。

   b. 如果您希望 Kaspersky Endpoint Security 掃描啟動物件，請選取**記憶體**核取方塊。

   c. 如果您希望 Kaspersky Endpoint Security 掃描其他附加檔案或資料夾，請點擊**新增**並指定檔案、資料夾、檔案或資料夾名稱遮罩。

   d. 點擊**確定**儲存變更並關閉**掃描範圍**視窗。

6. 透過以下方式之一儲存變更：

   - 儲存變更後，點擊**套用**以保留在**內容：<工作名稱>**視窗中。
   - 儲存變更後，點擊**確定**關閉**內容：<工作名稱>**視窗。

配置掃描工作設定

1. 開啟包含**掃描**工作設定的視窗。

2. 選取"**掃描**"部分。

3. 若要變更 Kaspersky Endpoint Security 執行掃描工作的安全級別，請在**安全等級**部分中執行下列操作之一：

   - 透過向上或向下移動滑桿來選擇預設的安全等級。

您可以選擇以下安全等級之一：

- **最大防護**。Kaspersky Endpoint Security 對已開啟、儲存或執行的檔案執行最大程度的監控。
- **建議**。Kaspersky Endpoint Security 使用卡巴斯基建議的設定監控檔案。

  這是預設的安全等級。
- **最高速度**。Kaspersky Endpoint Security 監控最少的檔案集合。如果您想要使用需要大量記憶體資源的其他應用程式，您可以選擇此安全等級。

- 手動配置安全設定：

  a. 點擊**設定**。

  設定：掃描視窗將開啟。

  b. 在**一般**標籤的**檔案類型**部分中，選擇在執行掃描工作時 Kaspersky Endpoint Security 應掃描的檔案類型。

  c. 在**一般**標籤的**最佳化**部分中，配置掃描效能設定。

  d. 在**複合檔案**標籤的**一般**部分中，選擇您希望 Kaspersky Endpoint Security 分析哪些複合檔案以尋找可偵測物件。

  e. 在**進階**標籤的**進階設定**部分中，配置 iSwift 技術的使用以及在應用程式統計資料中儲存有關偵測到的物件的資訊。

  f. 在**進階**標籤的**啟發式分析器**部分中，配置啟發式分析器的使用並選擇啟發式分析器在惡意軟體掃描期間套用的防護等級。

  g. 點擊**確定**儲存變更並關閉**設定：掃描**視窗。

  安全等級變更為**自訂**。

- 若要還原預設設定，請點擊**預設**。

  安全等級變更為**建議**。

4. 如有必要，在**操作**部分中，選擇 Kaspersky Endpoint Security 在偵測到感染物件時應執行的操作。

5. 若要指定掃描範圍，請在**掃描範圍**部分中點擊**設定**，然後在開啟的**掃描範圍**視窗中執行下列操作：

   a. 如果您希望 Kaspersky Endpoint Security 掃描所有卸除式磁碟機，請選取**所有卸除式磁碟**核取方塊。

   b. 如果您希望 Kaspersky Endpoint Security 掃描所有內部磁碟機，請選取**所有內置磁碟**核取方塊。

   c. 如果您希望 Kaspersky Endpoint Security 掃描所有網路磁碟機，請選取**所有網路磁碟**核取方塊。

   d. 如果您希望 Kaspersky Endpoint Security 掃描電腦記憶體，請選取**記憶體**核取方塊。

   e. 如果您希望 Kaspersky Endpoint Security 掃描啟動物件，請選取**記憶體**核取方塊。

   f. 如果您希望 Kaspersky Endpoint Security 掃描其他檔案或資料夾，請點擊**新增**並指定檔案、資料夾、檔案或資料夾名稱遮罩。

   g. 點擊**確定**儲存變更並關閉**掃描範圍**視窗。

6. 透過以下方式之一儲存變更：

- 儲存變更後，點擊**套用**以保留在**內容：<工作名稱>**視窗中。
- 儲存變更後，點擊**確定**關閉**內容：<工作名稱>**視窗。

管理"更新"工作設定

1. 開啟包含**更新**工作設定的視窗。
2. 選擇**更新**部分。
3. 如果您希望 Kaspersky Endpoint Security 與應用程式資料庫一起更新應用程式模組，請選取**更新應用程式模組**核取方塊。
4. 要選擇更新來源，請執行以下操作：
   a. 點擊**設定**。
   設定：更新視窗將開啟。
   b. 透過以下方式之一指定更新來源：
   - 如果您希望應用程式從管理伺服器下載更新，請選取**卡巴斯基安全管理中心**核取方塊。
   - 如果您希望應用程式從卡巴斯基更新伺服器下載更新，請選取**卡巴斯基更新伺服器**核取方塊。
   - 若要新增不同的更新來源，請點擊**新增**，然後在開啟的視窗中輸入更新來源的路徑。
     預設情況下，Kaspersky Endpoint Security 從卡巴斯基更新伺服器下載更新。
   c. 點擊**確定**儲存變更並關閉**設定：更新**視窗。
5. 透過以下方式之一儲存變更：

- 儲存變更後，點擊**套用**以保留在**內容：<工作名稱>**視窗中。
- 儲存變更後，點擊**確定**關閉**內容：<工作名稱>**視窗。

僅適用於本機工作

管理檔案威脅防護工作設定

1. 開啟用戶端電腦的本機工作清單。
2. 在本機工作清單中，選擇檔案威脅防護工作並透過以下方式之一開啟其內容：

- 雙擊工作名稱。
- 右鍵點擊以顯示工作的捷徑功能表並選擇**內容**。
- 點擊**內容**。

3. 選擇"**檔案威脅防護**"部分。

4. 如有必要，請配置以下設定：

- 在用戶端電腦上啟用或停用檔案威脅防護。
- 若要選擇預設安全等級之一，請使用**安全等級**部分中的滑桿。
- 若要手動設定安全設定，請點擊**設定**，然後在開啟的**設定：檔案威脅防護**視窗中執行下列操作：

  a. 在**一般**標籤的**檔案類型**部分中，選擇 Kaspersky Endpoint Security 開啟、執行或儲存檔案時應掃描的檔案類型。

  b. 在**一般**標籤的**最佳化**部分中，設定掃描效能設定並選擇掃描技術，然後選擇 Kaspersky Endpoint Security 是否跳過對用戶端電腦上的唯讀系統磁碟區的掃描。

  c. 在**一般**標籤的**複合檔案**部分中，選擇應掃描哪些複合檔案以尋找可偵測物件，並設定掃描大型物件的限制。

  d. 在**防護範圍**標籤上，指定檔案威脅防護應掃描的檔案或資料夾。

  預設情況下，位於連線到用戶端電腦的卸除式磁碟機、內部磁碟機和網路磁碟機上的所有物件將被掃描。您可以將物件新增至防護範圍、修改清單中的物件、暫時停用掃描清單中的物件或從清單中刪除物件。

  e. 在**進階**標籤的**掃描模式**部分中，選擇檔案威脅防護模式。

  f. 在**進階**標籤的**暫停工作**部分中，啟用或停用檔案威脅防護的排程暫停，並根據排程配置工作自動暫停。

  g. 在**進階**所有標簽的**啟發式分析器**部分中，配置檔威脅防護對啟發式分析器的使用。

  h. 點擊**確定**儲存變更並關閉**設定：檔案威脅防護**視窗。

- 在**如果偵測到惡意物件**部分中，選擇檔案威脅防護在偵測到感染物件時執行的操作。

5. 透過以下方式之一儲存變更：

- 儲存變更後，點擊**套用**以保留在**內容：檔案威脅防護**視窗中。
- 儲存變更後，點擊**確定**關閉**內容：檔案威脅防護**視窗。

管理 Web 威脅防護工作設定

1. 開啟用戶端電腦的本機工作清單。
2. 在本機工作清單中，選擇 Web 威脅防護工作並透過以下方式之一開啟其內容：

- 雙擊工作名稱。
- 右鍵點擊以顯示工作的捷徑功能表並選擇**內容**。
- 點擊**內容**。

3. 選擇“**Web 威脅防護**”部分。

4. 如有必要，請配置以下設定：

- 在用戶端電腦上啟用或停用 Web 威脅防護。
- 若要選擇預設安全等級之一，請使用**安全等級**部分中的滑桿。
- 若要手動設定安全設定，請點擊**設定**，然後在開啟的**設定： Web 威脅防護**視窗中執行下列操作：

  a. 在**一般**標籤**的掃描模式**部分中，啟用或停用根據惡意網址資料庫檢查網址。

  b. 在**一般**標籤的**網路釣魚防護設定**部分中，啟用或停用根據網路釣魚網址資料庫檢查網址。

  c. 在**一般**標籤的**網路釣魚防護設定**部分中，啟用或停用使用啟發式分析器來偵測網路釣魚連結。

  d. 在**受信任網址**標籤上，啟用或停用對受信任網址的 Web 流量進行掃描，並建立或編輯受信任的網址清單。

  e. 點擊**確定**儲存變更並關閉**設定： Web 威脅防護**視窗。

5. 在**如果偵測到惡意物件**部分中，選擇 Web 威脅防護在偵測到 Web 流量中的危險物件時執行的操作。

6. 透過以下方式之一儲存變更：

- 儲存變更後，點擊**套用**以保留在**內容：Web 威脅防護**視窗中。
- 儲存變更後，點擊**確定**關閉**內容：Web 威脅防護**視窗。

管理快速掃描工作設定

1. 開啟用戶端電腦的本機工作清單。

2. 在本機工作清單中，選擇“快速掃描”工作並透過下列方式之一開啟其內容：

- 雙擊工作名稱。
- 右鍵點擊以顯示工作的捷徑功能表並選擇**內容**。
- 點擊**內容**。

3. 選取“**掃描**”部分。

4. 如有必要，請配置以下設定：

- 若要選擇預設安全等級之一，請使用**安全等級**部分中的滑桿。
- 若要手動設定安全設定，請點擊**設定**，然後在開啟的**設定：掃描**視窗中執行下列操作：

  a. 在**一般**標籤的**檔案類型**部分中，選擇 Kaspersky Endpoint Security 應掃描的檔案類型。

  b. 在**一般**標籤的**最佳化**部分中，配置掃描效能設定。

  c. 在**一般**標籤的**複合檔案**部分中，選擇您希望 Kaspersky Endpoint Security 掃描的複合檔案。

  d. 在**進階**標籤的**進階設定**部分中，配置 iSwift 技術的使用以及在應用程式統計資料中儲存有關偵測到的物件的資訊。

e. 在**進階**標籤的**啟發式分析器**部分中，配置啟發式分析器的使用並選擇啟發式分析器要套用的防護等級。

f. 點擊**確定**儲存變更並關閉**設定：掃描**視窗。

- 在**操作**部分中，選擇 Kaspersky Endpoint Security 在偵測到受感染物件時應該執行的操作。
- 若要指定掃描範圍，請在**掃描範圍**部分中點擊**設定**，然後在開啟的**掃描範圍**視窗中執行下列操作：
  - 如果您希望 Kaspersky Endpoint Security 掃描預設清單中的物件，請選取相關物件旁的核取方塊。
  - 如果您希望 Kaspersky Endpoint Security 掃描其他檔案或資料夾，請點擊**新增**並指定檔案、資料夾、檔案或資料夾名稱遮罩。
  - 點擊**確定**儲存變更並關閉**掃描範圍**視窗。

5. 透過以下方式之一儲存變更：

- 儲存變更後，點擊**套用**以保留在**內容：快速掃描**視窗中。
- 儲存變更後，點擊**確定**關閉**內容：快速掃描**視窗。

管理"完整掃描"工作設定

1. 開啟用戶端電腦的本機工作清單。
2. 在本機工作清單中，選擇"完整掃描"工作並透過下列方式之一開啟其內容：
   - 雙擊工作名稱。
   - 右鍵點擊以顯示工作的捷徑功能表並選擇**內容**。
   - 點擊**內容**。
3. 選取"**掃描**"部分。
4. 如有必要，請配置以下設定：
   - 若要選擇預設安全等級之一，請使用**安全等級**部分中的滑桿。
   - 若要手動設定安全設定，請點擊**設定**，然後在開啟的**設定：掃描**視窗中執行下列操作：
     a. 在**一般**標籤的**檔案類型**部分中，選擇 Kaspersky Endpoint Security 應掃描的檔案類型。
     b. 在**一般**標籤的**最佳化**部分中，配置掃描效能設定。
     c. 在**一般**標籤的**複合檔案**部分中，選擇您希望 Kaspersky Endpoint Security 掃描的複合檔案。
     d. 在**進階**標籤的**進階設定**部分中，配置 iSwift 技術的使用以及在應用程式統計資料中儲存有關偵測到的物件的資訊。
     e. 在**進階**標籤的**啟發式分析器**部分中，配置啟發式分析器的使用並選擇啟發式分析器要套用的防護等級。
     f. 點擊**確定**儲存變更並關閉**設定：掃描**視窗。
   - 在**操作**部分中，選擇 Kaspersky Endpoint Security 在偵測到受感染物件時應該執行的操作。

- 若要指定掃描範圍，請在**掃描範圍**部分中點擊**設定**，然後在開啟的**掃描範圍**視窗中執行下列操作：
  - 如果您希望 Kaspersky Endpoint Security 掃描預設清單中的物件，請選取相關物件旁的核取方塊。
  - 如果您希望 Kaspersky Endpoint Security 掃描其他檔案或資料夾，請點擊**新增**並指定檔案、資料夾、檔案或資料夾名稱遮罩。
  - 點擊**確定**儲存變更並關閉**掃描範圍**視窗。

5. 透過以下方式之一儲存變更：
   - 儲存變更後，點擊**套用**以保留在**內容：完整掃描**視窗中。
   - 儲存變更後，點擊**確定**關閉**內容：完整掃描**視窗。

管理自訂掃描工作設定

1. 開啟用戶端電腦的本機工作清單。
2. 在本機工作清單中，選擇"自訂掃描"工作並透過下列方式之一開啟其內容：
   - 雙擊工作名稱。
   - 右鍵點擊以顯示工作的捷徑功能表並選擇**內容**。
   - 點擊**內容**。
3. 選取"**掃描**"部分。
4. 如有必要，請配置以下設定：
   - 若要選擇預設安全等級之一，請使用**安全等級**部分中的滑桿。
   - 若要手動設定安全設定，請點擊**設定**，然後在開啟的**設定：掃描**視窗中執行下列操作：
     a. 在**一般**標籤的**檔案類型**部分中，選擇 Kaspersky Endpoint Security 應掃描的檔案類型。
     b. 在**一般**標籤的**最佳化**部分中，配置掃描效能設定。
     c. 在**一般**標籤的**複合檔案**部分中，選擇您希望 Kaspersky Endpoint Security 掃描的複合檔案。
     d. 在**進階**標籤的**進階設定**部分中，配置 iSwift 技術的使用以及在應用程式統計資料中儲存有關偵測到的物件的資訊。
     e. 在**進階**標籤的**啟發式分析器**部分中，配置啟發式分析器的使用並選擇啟發式分析器要套用的防護等級。
     f. 點擊**確定**儲存變更並關閉**設定：掃描**視窗。
   - 在**操作**部分中，選擇 Kaspersky Endpoint Security 在偵測到受感染物件時應該執行的操作。
   - 若要指定掃描範圍，請在**掃描範圍**部分中點擊**設定**，然後在開啟的**掃描範圍**視窗中執行下列操作：
     - 點擊**新增**並指定檔案、資料夾、檔案或資料夾的名稱遮罩。
     - 點擊**確定**儲存變更並關閉**掃描範圍**視窗。

5. 透過以下方式之一儲存變更：

- 儲存變更後，點擊**套用**以保留在**內容：自訂掃描**視窗中。
- 儲存變更後，點擊**確定**關閉**內容：自訂掃描**視窗。

管理網路威脅防護工作設定

1. 開啟用戶端電腦的本機工作清單。
2. 在本機工作清單中，選擇網路威脅防護工作並透過以下方式之一開啟其內容：
   - 雙擊工作名稱。
   - 右鍵點擊以顯示工作的捷徑功能表並選擇**內容**。
   - 點擊**內容**。
3. 選擇"**網路威脅防護**"部分。
4. 如有必要，請配置以下設定：
   - 在用戶端電腦上啟用或停用網路威脅防護。
   - 在**網路威脅防護設定**部分中，勾選或取消勾選**封鎖攻擊電腦<值>分鐘**核取方塊並指定該值。
   - 您也可以指定網路活動不會被封鎖的電腦的 IP 位址。為此，請執行以下步驟：
     a. 點擊**排除項目**。
     排除項目視窗將開啟。
     b. 點擊**新增**。
     "**IP 位址**"視窗將開啟。
     c. 指定網路活動不會被封鎖的電腦的 IP 位址，然後點擊**確定**。
     d. 點擊**確定**儲存變更然後關閉**排除項目**視窗。
5. 透過以下方式之一儲存變更：
   - 儲存變更後，點擊**套用**以保留在**內容：網路威脅防護**視窗中。
   - 儲存變更後，點擊**確定**關閉**內容：網路威脅防護**視窗。

建立和管理政策

本節包含有關如何建立和配置 Kaspersky Endpoint Security 政策的資訊。

政策可決定應用程式的設定並管理在管理群組內的裝置上配置該應用程式的能力。必須為每個應用程式建立單獨的政策。您可以為每個管理群組中的裝置上安裝的應用程式建立無限數量的各種政策，但一次只能將一個政策套用至管理群組中的每個應用程式。

注意：建立和設定政策時，您可以使用和按鈕允許或禁止對政策中的任何設定群組進行變更。

您可以對自訂政策執行以下操作：

- 制定政策。
- 配置政策。
- 將政策從一個群組複製或移動到另一個群組。
- 刪除政策。
- 變更政策的狀態。
- 將政策匯出到檔案。
- 從檔案匯入政策。

有關卡巴斯基安全管理中心政策的詳細資訊，請參閱卡巴斯基安全管理中心說明。

建立政策

本節包含如何啟動新政策精靈來建立政策的操作說明。

從管理群組的資料夾建立政策

1. 啟動卡巴斯基安全管理中心管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，點擊**"受管理裝置"**。
4. 選擇包含所需用戶端電腦的管理群組。
5. 在工作區中，選擇**政策**標籤並點選**新政策**。
   新建政策精靈將會開啟。
6. 請依照新建政策精靈的步驟建立政策。

從政策資料夾建立政策

1. 啟動卡巴斯基安全管理中心管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，點擊 **"政策"**。

4. 在工作區中，點擊**新建政策**。

   新建政策精靈將會開啟。

5. 請依照新建政策精靈的步驟建立政策。

若要繼續精靈的下一步，請點擊**下一步**。若要返回精靈的上一步，請點擊←。若要在任何步驟結束精靈，請點擊**取消**。

注意：按鈕的外觀可能會有所不同，具體取決於您的 Windows 版本。

步驟 1.選取應用程式

在**選擇要為其建立群組政策的應用程式**視窗的應用程式清單中，選擇 **Kaspersky Endpoint Security for Mac (12.2.1)**。

步驟 2.指定政策名稱

1. 在**輸入群組政策名稱**視窗的**名稱**欄位中，指定您要建立的政策的名稱。名稱不能包含以下符號：**“ * < : > ? \ |**。

2. 如果您要將設定從現有 Kaspersky Endpoint Security 政策匯入至新政策，請勾選**使用應用程式早期版本的政策設定**核取方塊。

步驟 3.指定防護設定

如有必要，在**防護**視窗中配置以下設定：

- 配置用戶端電腦上作業系統的防護設定。
- 配置受信任區域。

  您可以建立 Kaspersky Endpoint Security 不掃描或監控的物件清單。
- 配置受信任應用程式。

  您可以建立 Kaspersky Endpoint Security 不會監控其網路和檔案活動的應用程式清單。
- 選擇要偵測的物件類型。
- 當電腦使用電池為電源時，停用或啟用排程工作的啟動。
- 限制掃描工作對 CPU 的使用。

步驟 4.配置檔威脅防護設定

在**檔案威脅防護**視窗中，如有必要，請執行以下操作：

- 開啟/關閉檔案威脅防護。

  預設情況下，檔案威脅防護處於開啟狀態。
- 選擇安全等級。

  預設情況下，選擇卡巴斯基建議的安全等級。

- 配置檔威脅防護設定。
- 選擇偵測到惡意物件時要執行的操作。

步驟 5.配置 Web 威脅防護設定

在 **Web 威脅防護**視窗中，如有必要，請執行以下操作：

- 開啟/關閉 Web 威脅防護。
  預設情況下，Web 威脅防護處於開啟狀態。
- 選擇安全等級。
  預設情況下，選擇卡巴斯基建議的安全等級。
- 配置 Web 威脅防護設定。
- 選擇在 Web 流量中偵測到惡意物件時要執行的動作。

步驟 6.配置網路威脅防護設定

在**網路威脅防護**視窗中，如有必要，請執行以下操作：

- 開啟/關閉網路威脅防護。
  預設啟用网路威胁防護。
- 配置網路威脅防護設定。
- 建立或編輯遠端電腦的 IP 位址清單，其網路活動永遠不會被 Kaspersky Endpoint Security 封鎖。

步驟 7.配置更新設定

在**更新**視窗中，如有必要，請執行以下操作：

- 開啟/關閉應用程式模組的更新。
- 指定更新來源。

步驟 8.配置 KSN 設定

在**卡巴斯基安全網路**視窗中，如有必要，請執行以下操作：

- 點擊 **KSN 聲明**閱讀卡巴斯基安全網路聲明全文。
- 檢視有關卡巴斯基安全管理中心提供的 KSN 基礎架構的資訊。
- 開啟/關閉卡巴斯基安全網路的使用。
- 啟用或停用延伸 KSN 模式。
- 啟用或停用 KSN 代理的使用。
- 當 KSN 代理不可用時啟用或停用卡巴斯基伺服器的使用。

注意：只有當卡巴斯基安全管理中心管理伺服器用作代理伺服器時，才能在遠端電腦上使用卡巴斯基安全網路和 KSN 代理。有關管理伺服器內容的詳細資訊，請參閱卡巴斯基安全管理中心說明。

當卡巴斯基安全管理中心使用全球 KSN 基礎架構並且您在政策設定中選擇參與卡巴斯基安全網路時，对其套用政策的用戶端電腦的 Kaspersky Endpoint Security 統計資料將被自動傳送至卡巴斯基以增強對這些電腦的防護。

注意：卡巴斯基不會在沒有您明確同意的情況下收集、處理或儲存任何個人資料。

在全球 KSN 基礎架構中使用卡巴斯基安全網路時向卡巴斯基提供的資料

如果勾選**我同意使用卡巴斯基安全網路**核取方塊並且取消勾選**啟用延伸 KSN 模式**核取方塊，Kaspersky Endpoint Security 將向卡巴斯基提供以下資料：

- 所使用授權的相關資訊： 授權的類型和有效期、授權失效前的天數、向其購買授權的合作夥伴的識別碼、區域啟動中心識別碼、啟動碼的總和檢查碼、SHA1 演算法計算的票證內容雜湊、授權票證建立日期與時間、授權資訊識別碼、授權票證識別碼、授權票證順序識別碼、使用者電腦的唯一識別碼、授權票證有效開始日期、授權票證有效結束日期、授權票證目前狀態、票證標題版本、授權版本、票證標題簽章憑證識別碼、金鑰檔案的總和檢查碼、票證標題簽署者序號、身分驗證權杖。

- 所安裝軟體的完整版本；
  已安裝軟體的類型；
  軟體更新 ID； 聲譽服務的 ID； 協定類型 ID； 區域啟動中心的 ID； 已撤銷軟體服務決策清單版本； 軟體病毒資料庫中的已觸發記錄 ID； 軟體病毒資料庫中的已觸發記錄時間戳記； 觸發的軟體病毒資料庫記錄類型； 電腦上應用程式安裝實例的唯一 ID； 產品授權啟動日期； 授權失效日期； 授權識別碼； 軟體所使用授權的狀態； 目前處理中物件的總和檢查碼類型； 偵測到的惡意軟體名稱或是可能用於傷害使用者裝置或資料的合法軟體名稱； 目前處理中物件的總和檢查碼； 軟體啟動碼的總和檢查碼； 軟體的完整版本； 唯一裝置 ID； 軟體 ID； 軟體金鑰檔案的總和檢查碼； 用於提供軟體授權的資訊模型 ID； 用於簽署軟體授權票證標頭的憑證識別碼； 軟體授權票證建立日期和時間； 軟體授權票證總和檢查碼； 軟體授權票證版本； 軟體啟動碼版本； 權利持有人基礎架構請求資料格式； 啟動的產品授權票證 ID； 軟體元件 ID； 軟體動作結果； 錯誤代碼； 網路服務的已存取位址（URL、IP）； 通訊埠編號； 網路服務請求來源（推薦者）的網址； 認證的公開金鑰； 所掃描物件與雜湊演算法的數位憑證指紋。

如果選中**我同意使用卡巴斯基安全網路**和**啟用延伸 KSN 模式**核取方塊，Kaspersky Endpoint Security 會向卡巴斯基提供以下資料：

- 作業系統版本和已安裝在電腦上的服務套件版本的相關資訊；目前和預設的作業系統語言設定；作業系統內核檔案的版本和總和檢查碼（MD5、SHA2-256、SHA1）；作業系統執行模式的參數； 作業系統版本、作業系統組建編號、作業系統更新編號、作業系統版本、作業系統版本延伸資訊； 作業系統服務包版本； 作業系統啟動的日期和時間； 行為分析子系統中關於作業系統的事件處理延遲時間； 延遲的目前類型作業系統動作事件數； 主動式防禦子系統中關於作業系統的事件處理延遲時間； 已處理的作業系統動作事件數； 已處理的同步作業系統動作事件數； 延遲的目前類型作業系統動作事件總數； 常設事件儲存子系統中關於作業系統的事件處理延遲時間； 延遲的作業系統動作事件總數； 等待中的同步作業系統動作事件數； 作業系統中一項動作收到事件的日期和時間。

- 有關上次作業系統重新啟動失敗的資訊： 重新啟動失敗的次數。

- 權利持有人之已安裝應用程式和病毒防護狀態的相關資訊： 軟體安裝 ID（PCID）； 軟體資料庫記錄版本； 電腦上應用程式安裝實例的唯一識別碼、應用程式類型、應用程式類型 ID、所安裝的應用程式的完整版本、應用程式設定版本的識別碼、電腦類型的識別碼、已安裝應用程式的電腦的唯一識別碼、權利持有人服務中的唯一使用者識別碼、本機語言和操作狀態、所安裝軟體元件的版本及其操作狀態、用於連線權利持有人服務的協定版本； 所安裝軟體的完整版本； 已安裝軟體的類型； 軟體更新 ID； 聲譽服務的 ID； 協定類型 ID； 區域啟動中心的 ID； 已撤銷軟體服務決策清單版本； 軟體病毒資料庫中的已觸發記錄 ID； 軟體病毒資料庫中的已觸發記錄時間戳記； 觸發的軟體病毒資料庫記錄類型； 電腦上應用程式安裝實例的唯一 ID； 產品授權啟動日期； 授權失效日期； 授權識別碼； 軟體所使用授權的狀態； 目前處理中物件的總和檢查碼類型； 偵測到的惡意軟體名稱或是可能用於傷害使用者裝置或資料的合法軟體名稱； 目前處理中物件的總和檢查碼； 軟體啟動碼的總和檢查碼； 軟體的完整版本； 軟體 ID； 軟體金鑰檔案的總和檢查碼； 用於提供軟體授權的資訊模型 ID； 用於簽署軟體授權票證標頭的憑證識別碼； 軟體授權票證建立日期和時間； 軟體授權票證總和檢查碼； 軟體授權票證版本； 軟體啟動碼版本； 權利持有人基礎架構請求資料格式； 啟動的產品授權票證 ID； 軟體元件 ID； 軟體動作結果； 錯誤代碼； 網路服務的已存取位址（URL、IP）； 通訊埠編號； 網路服務請求來源（推薦者）的網址； 防毒資料庫的更新適用週期數； 防毒資料庫上次更新和套用的日期和時間； 軟體資料庫的發佈日期與時間； 軟體元件版本； 軟體更新 ID； 已安裝軟體的類型； System Watcher 開始的日期和時間； 軟體的安裝日期和時間； 由 System Watcher 傳送統計資料的可能性； 由 System Watcher 處理，需時超過標準時間的事件碼； 由 System Watcher 處理，需時超過標準時間的事件的資料庫處理時間； 由 System Watcher 處理一項事件的最大允許時間； 由 System Watcher 處理，需時超過標準時間的事件處理時間； 由 System Watcher 處理，需時超過標準時間的事件總數。

- 所有被處理物件與操作的相關資訊： 軟體對被處理物件的判定； 目錄碼； 處理中物件的大小； 處理中物件的總和檢查碼 (SHA256)； 系統監控環境中偵測到的軟體數量； 被系統監控偵測到的軟體的日期和時間； 偵測特徵； 軟體病毒資料庫中的已觸發記錄 ID； 系統監控偵測軟體的原因； 處理中物件的總和檢查碼 (MD5)； 模組完整性檢查的結果； 目前處理中物件的名稱； 觸發的軟體病毒資料庫記錄類型； 所處理物件的路徑； 被掃描物件的名稱； 掃描的日期和時間； 從其下載的 URL 和 Referrer 位址； 被掃描檔案的大小及其路徑； 壓縮檔案標誌； 檔案建立日期與時間； 封包程式的名稱、大小和總和檢查碼（MD5、SHA2-256）（如果檔案被封包）； 檔案的熵； 檔案的類型； 檔案類型代碼； 可執行檔的標誌、ID 和格式； 物件的總和檢查碼（MD5、SHA2-256）； 物件的補充總和檢查碼的類型和值； 有關物件的數位簽章（憑證）的資料： 憑證發行者相關資料、自上一次傳送統計資料後物件的啟動次數、應用程式掃描工作的 ID、收取有關物件信譽的資訊的方式、目標篩選條件值、適用偵測技術的技術參數； 所處理物件的路徑； 目錄碼。

- 對於可執行檔： 檔案區段熵、聲譽驗證旗標或檔案簽署旗標、名稱、類型、ID 類型、總和檢查碼 (MD5)、經驗證物件所載入應用程式的大小、應用程式路徑和範本路徑、自動執行清單中表明狀態的屬性、登錄日期、屬性清單、封裝程式名稱、應用程式數位簽章相關資訊： 發行商憑證、以 MIME 格式上傳的檔案名稱、檔案組建日期與時間。

- 啟動的應用程式及其模組的相關資訊： 總和檢查碼（MD5、SHA2-256）、大小、屬性、建立日期、加殼器名稱（如果檔案已加殼）、檔案名稱、有關係統上執行的處理程序的資訊（處理程序 ID (PID)、處理程序名稱、有關啟動處理程序的帳戶的資訊、啟動處理程序的應用程式和命令、處理程序檔案的完整路徑以及啟動命令列、處理程序所屬應用程式的敘述（處理程序的名稱）應用程式和有關發布者的資訊），以及正在使用的數位憑證和驗證其真實性所需的資訊或有關缺少檔案數位簽章的資訊），以及有關載入到處理程序中的模組的資訊： 它們的名稱、大小、類型、建立日期、屬性、總和檢查碼（MD5、SHA2-256、SHA1）、它們的路徑、PE 檔案標頭資訊、加殼器名稱（如果檔案已加殼）、有關可用性的資訊以及這些統計資料的有效性、產生正在傳送的統計資料的模式的識別碼。

- 若偵測到威脅或弱點，除了所偵測物件的相關資訊以外，還需提供下列資訊：識別碼、版本及病毒資料庫中的記錄類型、根據卡巴斯基分類的威脅名稱、病毒資料庫上一次更新的日期與時間、可執行檔名稱、要求威脅偵測 URL 之應用程式檔案的總和檢查碼 (MD5)、已偵測威脅的 IP 位址（IPv4 或 IPv6）、弱點識別碼及其威脅等級、偵測到弱點的網頁的 URL 與參照位址。

- 若偵測到潛在惡意物件，提供的相關資訊包括程序記憶體中的資料。

- 網路攻擊資訊： 發動攻擊的電腦 IP 位址、網路攻擊指向的使用者電腦連接埠號、攻擊協定的 ID、攻擊的名稱和類型。

- 網路連線相關資訊： 啟動程序而開啟連接埠的檔案版本及總和檢查碼 (MD5、SHA2-256、SHA1)、程序檔案的路徑及其數位簽章、本機及遠端 IP 位址、本機及遠端連接埠號、連線狀態、連接埠開啟的時間戳記。

- 偵測到有害或可疑內容的網頁 URL 和 IP 位址、要求該 URL 的檔案名稱、大小和總和檢查碼、用來達到判定結果之規則的識別碼、加權與程度、攻擊目標。

- 有關已安裝應用程式和病毒資料庫更新的資訊： 更新工作的完成狀態、更新期間可能發生的錯誤類型、更新失敗的次數、執行更新之應用程式元件的識別碼。

- 卡巴斯基安全網路 (KSN) 的使用相關資訊： KSN 識別碼、軟體識別碼、應用程式完整版本、使用者裝置的去個人化 IP 位址、KSN 要求履行品質指標、KSN 封包處理品質指標、KSN 要求數目指標與 KSN 要求類型相關資訊、開始傳送統計資料的日期與時間、結束傳送統計資料的日期與時間、KSN 配置更新相關資訊： 活動配置的識別碼、收到的配置的識別碼、配置更新的錯誤代碼。

- 系統記錄事件相關資訊： 偵測到事件的記錄檔名稱、事件的類型與分類、事件來源名稱以及事件描述。

- 用於確定檔案和 URL 位址信譽的資訊： 請求信譽的 URL 位址和參照位址、連線的協定類型、應用程式類型的內部識別碼、正在使用的連接埠號、使用者識別碼、掃描檔案的總和檢查碼 (MD5)、偵測到的威脅的類型、用於偵測威脅的記錄的資訊（病毒資料庫的記錄識別碼、記錄時間戳記和類型）； 認證的公開金鑰； 所掃描物件與雜湊演算法的數位憑證指紋。

- 應用程式地區分佈相關資料： 應用程式安裝和啟動日期、提供應用程式啟動授權的合作夥伴 ID、應用程式 ID、應用程式語言本機化 ID、應用程式啟動授權序號、KSN 加入簽章。

- 所使用授權的相關資訊： 授權的類型和有效期、授權失效前的天數、向其購買授權的合作夥伴的識別碼、區域啟動中心識別碼、啟動碼的總和檢查碼、SHA1 演算法計算的票證內容雜湊、授權票證建立日期與時間、授權資訊識別碼、授權票證識別碼、授權票證順序識別碼、使用者電腦的唯一識別碼、授權票證有效開始日期、授權票證有效結束日期、授權票證目前狀態、票證標題版本、授權版本、票證標題簽章憑證識別碼、金鑰檔案的總和檢查碼、票證標題簽署者序號、身分驗證權杖。

- 電腦上所安裝的硬體相關資訊： 內建和已連線裝置的類型、名稱、型號名稱、韌體版本、參數。

- 裝置資訊： 裝置 ID。

- Web 控制元件的作業資訊： 元件版本、分類原因、其他分類原因的相關資訊、分類 URL、被封鎖 / 分類物件的主機 IP 位址。

當卡巴斯基安全管理中心使用私有 KSN 基礎架構並且您在政策設定中選擇參與卡巴斯基安全網路時，Kaspersky Endpoint Security 不會將對其套用了政策的用戶端電腦的統計資料傳送到卡巴斯基。

政策被刪除或變成非活動狀態後，用戶端電腦上的 KSN 設定將返回初始狀態。

步驟 9.配置使用者互動設定

如有必要，請在**使用者互動**視窗中配置 Kaspersky Endpoint Security 設定以與用戶端電腦的使用者進行互動。

步驟 10.配置網路連線設定

在**網路**視窗中，如有必要，請執行以下操作：

- 配置與代理伺服器的連線。

- 啟用或停用入站和出站 HTTPS 流量掃描。

- 選擇用於在 Mozilla Firefox 瀏覽器中檢查加密 HTTPS 流量的憑證儲存。

- 管理受信任的根憑證清單。

- 配置受監控的連接埠。

您可以建立 Kaspersky Endpoint Security 監控的連接埠清單。

步驟 11.配置報告和備份設定

在**報告和備份**視窗中，如有必要，請執行以下操作：

- 配置報告的產生和儲存設定。
- 配置在備份中儲存物件的設定。

步驟 12.配置 FileVault 磁碟加密

在 **FileVault 磁碟加密**視窗中，如有必要，請執行以下操作：

- 啟用或停用使用者啟動磁碟的 FileVault 磁碟加密管理。

  預設情況下，FileVault 磁碟加密管理處於停用狀態。
- 如果您希望在將政策套用到用戶端電腦時加密使用者的啟動磁碟，請選擇**加密磁碟**選項。

如果 **啟用 FileVault 磁碟加密管理**核取方塊被取消選中，則具有管理員權限的使用者可以從系統設定中加密和解密其 Mac 啟動磁碟。

如果選取**啟用 FileVault 磁碟加密管理**核取方塊和**加密磁碟**選項，則具有管理員權限的使用者無法從系統設定中解密其 Mac 的啟動磁碟。

如果選取**啟用 FileVault 磁碟加密管理**核取方塊和**解密磁碟**選項，則具有管理員權限的使用者無法從系統設定中加密其 Mac 的啟動磁碟。

步驟 13.配置 Web 控制

如有必要，在 **Web 控制**視窗中執行以下操作：

- 开启/關閉 Web 控制。

> **注意：**如果您啟用 Web 控制來封鎖對危險 Web 資源的存取，Kaspersky Endpoint Security 會在遠端電腦上的防護中心中顯示 **Web 控制已啟用。**通知。
> 如果在新建政策精靈的**檢查安全連線 (HTTPS)**視窗中選取**網路**核取方塊，則當使用者存取遠端電腦上被 Web 控制封鎖的 Web 資源時，Kaspersky Endpoint Security 會顯示通知。

- 點擊**新增**為 Web 控制新增規則。

  您可以輸入規則名稱、選擇規則是否處於活動狀態、透過建立特定網址清單或選擇網站類別來指定規則區域，以及選擇當使用者造訪此規則中包含的網站時 Kaspersky Endpoint Security 執行的操作。
- 編輯、刪除或組織清單中所建立的規則。

規則的排序順序決定了 Kaspersky Endpoint Security 對其應用程式排序的優先順序。

步驟 14.配置 Managed Detection and Response

在**Managed Detection and Response**視窗中，如有必要，請執行以下操作：

- 啟用或停用 Managed Detection and Response 元件。

  預設情況下，Managed Detection and Response 處於停用狀態。

- 匯入或刪除用於啟動受管理裝置上的 Managed Detection and Response 元件的設定檔。

如果勾選 **啟用 Managed Detection and Response** 核取方塊並匯入 MDR 設定檔案，則 Managed Detection and Response 元件將處於活動狀態並與 Kaspersky Managed Detection and Response 服務互動。該服務會不斷偵測並消除針對您組織的安全威脅。

步驟 15.配置 Endpoint Detection and Response Expert（內部部署）

在**Endpoint Detection and Response Expert (on-premise)**視窗中，如有必要，請執行以下操作：

- 啟用或停用 Endpoint Detection and Response Expert（內部部署）元件。
  預設情況下，Endpoint Detection and Response Expert（內部部署）元件處於停用狀態。
- 配置伺服器連線設定並新增 TLS 憑證。
- 新增伺服器。

如果選取 **啟用 Endpoint Detection and Response Expert（7.1 或者更早版本）** 核取方塊並新增 TLS 憑證和伺服器，則 Endpoint Detection and Response Expert（內部部署）元件將處於活動狀態並與 Kaspersky Anti Targeted Attack Platform 解決方案進行互動。此解決方案可及時偵測進階威脅，例如定向攻擊、進階持續性威脅、零日攻擊等。

步驟 16.配置外部磁碟掃描

在**外部磁碟掃描**視窗中，配置以下設定：

- 連線了外部磁碟時 Kaspersky Endpoint Security 執行的操作。
- Kaspersky Endpoint Security 在偵測到惡意物件時執行的操作。

步驟 17.配置行為偵測

在**行為偵測**視窗中，如有必要，請執行以下操作：

- 啟用或停用行為偵測。
  預設情況下，行為偵測處於啟用狀態。
- 選擇偵測到惡意軟體活動時要執行的操作。
- 啟用或停用防護共用資料夾抵禦外部加密。
  - 選擇偵測到惡意軟體活動時要執行的操作。

步驟 18.配置“郵件威脅防護”

在**郵件威脅防護**視窗中，如有必要，請執行以下操作：

- 啟用或停用郵件威脅防護。
  預設啟用网路威胁防護。
- 選擇偵測到惡意物件時要執行的操作。
- 配置郵件威脅防護設定。

步驟 19.配置弱點利用防禦

在**弱點利用防禦**視窗中，如有必要，請執行以下操作：

- 啟用或停用弱點利用防禦。
  預設情況下，弱點利用防禦處於啟用狀態。
- 選擇偵測到弱點利用時要執行的操作。

步驟 20.配置修復引擎

在**修復引擎**視窗中，如有必要，請執行以下操作：

- 啟用或停用修復引擎。
  預設情況下，修復引擎處於啟用狀態。

步驟 21.配置裝置控制

如有必要，在 **裝置控制**視窗中執行以下操作：

- 啟用或停用裝置控制。
  預設情況下，裝置控制處於啟用狀態。
- 配置裝置控制設定。

步驟 22.配置防火牆

在**防火牆**視窗中，如有必要，請執行以下操作：

- 啟用或停用防火牆。
  預設情況下，防火牆處於啟用狀態。
- 配置防火牆設定。

步驟 23.定義將對其套用政策的管理群組

在**目標群組**視窗中，點擊**瀏覽**以選擇要對其套用政策的管理群組。

步驟 24.選擇政策狀態並完成政策建立

在**為應用程式建立群組政策**視窗中，執行下列操作：

1. 選擇將指派給政策的狀態：
   - *活動政策*：政策被套用於選定的管理群組。
   - *非活動政策：*不套用政策。
   - *漫遊政策：*當電腦與公司網路斷開連線時，此政策將被套用於選定的管理群組。

   > **注意：**您可以為管理群組中的應用程式建立多個政策，但只有一個可處於活動狀態。

   有關政策狀態的詳細資訊，請參閱卡巴斯基安全管理中心說明。
2. 如果您想在建立政策後檢視政策設定，請選取**建立後立即開啟政策內容**核取方塊。

3. 點擊**結束**關閉新建政策精靈。

   您建立的政策將顯示在相關管理群組工作區的**政策**標籤上。此政策將在用戶端電腦首次與管理伺服器同步後套用到用戶端電腦。

您可以編輯已建立的政策的設定。您也可以使用每組設定的和按鈕禁止或允許從用戶端電腦變更每組設定。一組設定旁邊的按鈕表示不允許用戶端電腦的使用者在使用者的電腦上編輯這些設定。一組設定旁邊的按鈕表示允許用戶端電腦的使用者在使用者電腦上編輯這些設定。

檢視政策清單

您可以為每個管理群組中的電腦上安裝的應用程式建立無限數量的各種政策，但一次只能將一個政策套用至管理群組中的每個應用程式。

檢視管理群組的政策清單

1. 啟動卡巴斯基安全管理中心管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，點擊**"受管理裝置"**。
4. 選擇包含所需用戶端電腦的管理群組。
5. 在工作區選擇**"政策"**標籤。

   政策清單將顯示。

配置政策設定

您可以變更在卡巴斯基安全管理中心中建立的政策，並封鎖對其子群組政策和工作設定中的設定進行任何變更。

Kaspersky Endpoint Security 政策設定包括應用程式設定和工作設定。

配置政策設定

1. 啟動卡巴斯基安全管理中心管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，點擊**"受管理裝置"**。
4. 在工作區選擇**"政策"**標籤。
5. 右鍵點擊要設定的政策並選擇**內容**。
6. 在**內容：<政策名稱>**視窗中，配置政策設定：
   - 在**關鍵威脅防護**部分中

配置以下檔案威脅防護設定

- 開啟/關閉檔案威脅防護。
- 選擇預設安全等級之一或手動配置安全設定。
- 選擇偵測到惡意物件時要執行的操作。

配置以下 Web 威脅防護設定

- 開啟/關閉 Web 威脅防護。
- 選擇預設安全等級之一或手動配置安全設定。
- 啟用/停用根據惡意網址資料庫檢查網址。
- 配置網路釣魚防護設定。
- 新增其流量不會被 Web 威脅防護掃描的可信任位址。
- 選擇在 Web 流量中偵測到惡意物件時要執行的動作。

配置以下郵件威脅防護設定

- 啟用或停用郵件威脅防護。
- 選擇偵測到惡意物件時要執行的操作。
- 配置郵件威脅防護設定。

配置以下網路威脅防護設定

- 開啟/關閉網路威脅防護。
- 配置網路威脅防護設定。
- 指定網路活動不會被封鎖的電腦的 IP 位址。

配置以下防火牆設定

- 啟用或停用防火牆。
- 配置防火牆設定。

- 在**進階威脅防護**部分中

  配置以下 KSN 設定

  - 點擊 **KSN 聲明**閱讀卡巴斯基安全網路聲明全文。
  - 開啟/關閉卡巴斯基安全網路的使用。
  - 啟用或停用延伸 KSN 模式。
  - 開啟/關閉雲端模式。

- 啟用或停用 KSN 代理的使用。
- 當 KSN 代理不可用時啟用或停用卡巴斯基伺服器的使用。

注意：只有當卡巴斯基安全管理中心管理伺服器用作代理伺服器時，才能在遠端電腦上使用卡巴斯基安全網路和 KSN 代理。有關管理伺服器內容的詳細資訊，請參閱卡巴斯基安全管理中心說明。

配置以下行為偵測設定

- 啟用或停用行為偵測。

  預設情況下，行為偵測處於啟用狀態。
- 選擇偵測到惡意軟體活動時要執行的操作。

配置以下弱點利用防禦設定

- 啟用或停用弱點利用防禦。
- 選擇偵測到弱點利用時要執行的操作。

配置以下修復引擎設定

啟用或停用修復引擎。

- 在**安全控制**部分中

  配置以下裝置控制設定
  - 啟用或停用裝置控制。
  - 配置裝置控制設定。

  配置以下 Web 控制設定
  - 开启/關閉 Web 控制。
  - 點擊**新增**為 Web 控制新增規則。
  - 編輯、刪除或組織清單中所建立的規則。
- 在**資料加密**部分中

  配置以下 FileVault 磁碟加密設定
  - 啟用或停用用戶端電腦的 FileVault 磁碟加密管理。
  - 加密或解密用戶端電腦上的啟動磁碟。

    如果 **啟用 FileVault 磁碟加密管理**核取方塊被取消選中，則具有管理員權限的使用者可以從系統設定中加密和解密其 Mac 啟動磁碟。

    如果選取**啟用 FileVault 磁碟加密管理**核取方塊和**加密磁碟**選項，則具有管理員權限的使用者無法從系統設定中解密其 Mac 的啟動磁碟。

    如果選取**啟用 FileVault 磁碟加密管理**核取方塊和**解密磁碟**選項，則具有管理員權限的使用者無法從系統設定中加密其 Mac 的啟動磁碟。
- 在 **Detection and Response** 部分中

配置以下 Managed Detection and Response 設定

- 啟用或停用 Managed Detection and Response 元件。
- 匯入或刪除用於啟動受管理裝置上的 Managed Detection and Response 元件的設定檔。

配置以下 Endpoint Detection and Response (KATA) 設定

- 啟用或停用 Endpoint Detection and Response (KATA) 元件。
- 配置伺服器連線設定並新增 TLS 憑證。
- 新增 KATA 伺服器。

- 在**本機工作**部分
  配置以下外部磁碟掃描設定
  - 連線了外部磁碟時 Kaspersky Endpoint Security 執行的操作。
  - Kaspersky Endpoint Security 在偵測到惡意物件時執行的操作。
- 在"**更新**"部分中
  配置以下更新設定
  - 開啟/關閉應用程式模組的更新。
  - 指定更新來源。
- 在**其他設定**部分中
  配置以下防護設定
  - 啟用或停用對用戶端電腦的即時防護。
  - 啟用或停用 Kaspersky Endpoint Security 在用戶端電腦啟動時啟動。
  - 配置受信任區域。
  - 配置受信任應用程式。
  - 選擇要偵測的物件類型。
  - 當電腦使用電池為電源時，停用或啟用排程工作的啟動。

  配置以下網路設定
  - 啟用或停用代理伺服器的使用。
  - 指定代理伺服器位址。
  - 啟用或停用本機地址的代理伺服器的使用。
  - 指定用於進行代理伺服器身分驗證的使用者名稱和密碼。
  - 啟用或停用入站和出站 HTTPS 流量掃描。

- 選擇用於在 Mozilla Firefox 瀏覽器中檢查加密 HTTPS 流量的憑證儲存。
- 配置受監控的連接埠。

配置以下報告和備份設定

- 啟用或停用在報告中儲存非緊急事件。
- 啟用或停用僅儲存最近事件。
- 啟用或停用在指定時間段後刪除事件。
- 指定儲存事件的期限。
- 啟用或停用在指定時間段後從備份中刪除物件。
- 指定備份中物件的儲存期限。

配置以下使用者互動設定

- 啟用或停用事件通知。
- 選擇 Kaspersky Endpoint Security 如何通知使用者有關事件。
- 啟用或停用在功能表列中顯示 Kaspersky Endpoint Security 圖示。
- 配置使用者是否可以開啟 Kaspersky Endpoint Security 主視窗並使用用戶端電腦上的應用程式介面。
- 在用戶端電腦上 Kaspersky Endpoint Security 圖示的捷徑功能表中啟用或停用**結束**項目的可用性。
- 選擇用於顯示卡巴斯基安全管理中心事件的語言。
- 配置用戶端電腦使用者可用的 Kaspersky Endpoint Security 設定。
- 配置密碼防護以限制使用者裝置上不必要的操作。

7. 點擊**確定**儲存變更並關閉政策內容視窗。

變更政策狀態

政策狀態可定義政策的操作。此政策可以具有活動、漫遊或非活動狀態。您可以在政策設定中變更政策狀態。

變更政策狀態

1. 啟動卡巴斯基安全管理中心管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，點擊**"受管理裝置"**。
4. 選擇包含所需用戶端電腦的管理群組。
5. 在工作區選擇**"政策"**標籤。

6. 右鍵點擊要變更其狀態的政策，然後從上下文功能表中選擇**內容**。
7. 在**內容：<政策名稱>**視窗中，選擇**一般**部分。
8. 在**政策狀態**部分中，選擇下列政策狀態之一：
   - **活動政策**。政策被套用於選定的管理群組。
   - **漫遊政策**。當用戶端電腦與公司網路斷開連線時，此政策將被套用於選定的管理群組。
   - **非活動政策**。政策不被套用於選定的管理群組。
9. 點擊**確定**儲存變更並關閉**內容：<政策名稱>**視窗。

將政策匯出到 KLP 檔案

您可以將自訂政策匯出到檔案以在其他管理伺服器上使用該政策。

將政策匯出到 KLP 檔案

1. 啟動卡巴斯基安全管理中心管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，點擊**"受管理裝置"**。
4. 選擇包含所需用戶端電腦的管理群組。
5. 在工作區選擇**"政策"**標籤。
6. 右鍵點擊政策以顯示其上下文功能表，然後選擇**匯出**。
   "儲存為"視窗將開啟。
7. 選擇要在其中儲存政策的 KLP 檔案的資料夾。
8. 指定檔案名稱。
9. 點擊**儲存**將檔案儲存到所選資料夾中。

從 KLP 檔案匯入政策

您可以從檔案匯入具有預先定義設定的現有政策。

從 KLP 檔案匯入政策

1. 啟動卡巴斯基安全管理中心管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，點擊**"受管理裝置"**。

4. 選擇包含所需用戶端電腦的管理群組。
5. 在工作區選擇"**政策**"標籤。
6. 透過以下方式之一開啟檔案選擇視窗：
   - 點擊**從檔案匯入政策**按鈕。
   - 透過右鍵點擊工作區中的空白區域開啟上下文功能表並選擇**匯入**項目。
7. 選擇包含政策的 KLP 檔案，然後點擊**開啟**。

匯入的政策將被新增到工作區中的政策清單中。

建立和管理政策設定檔

*政策設定檔*是政策的一組命名變數設定，當滿足特定條件時，它會在用戶端電腦上啟動。啟動設定檔會修改啟動政策設定檔時在裝置上生效的政策設定。

建立政策設定檔

1. 在主控台樹狀目錄中，選擇要為其建立政策設定檔的管理群組。
2. 在工作區選擇"**政策**"標籤。
3. 執行下列操作之一以開啟要為其建立設定檔的政策的內容：
   - 雙擊政策的名稱。
   - 右鍵點擊政策名稱以顯示上下文功能表然後選擇**內容**。
   - 點擊**配置政策**連結。
4. 在**內容：<政策名稱>**視窗中，選擇**政策設定檔**部分。
5. 在工作區中，點擊**新增**。
6. 在**指派政策設定檔**視窗中，閱讀有關政策的資訊，然後點擊**下一步**。
   如果您不想在建立新政策設定檔時顯示此視窗，請選取**不再顯示此視窗**核取方塊，然後點擊**下一步**。
7. 在**政策設定檔名稱**視窗中，執行下列操作來配置政策設定檔：
   - 輸入新政策設定檔的名稱。

     注意：設定檔名稱不能超過 100 個字元。

   - 在**政策設定檔狀態**部分中，選擇政策設定檔是啟用還是停用。

- 在**政策設定檔狀態**部分的下拉清單中，選擇是否可以編輯政策設定檔。
- 如果要設定政策設定檔的啟動規則，請勾選**關閉新政策設定檔精靈後，繼續配置政策設定檔啟動規則核取**核取方塊。

8. 點擊**結束**。
9. 如果您已勾選**關閉新政策設定檔精靈後，繼續配置政策設定檔啟動規則**核取方塊，請繼續執行新建政策設定檔啟動規則精靈的步驟。

您建立的政策設定檔將顯示在**內容：<政策名稱>** 視窗的**政策設定檔**部分中。

建立政策設定檔啟動規則

1. 在主控台樹狀目錄中，選擇要在其中建立政策設定檔啟動規則的管理群組。
2. 在工作區選擇"**政策**"標籤。
3. 執行下列操作之一以開啟政策的內容：
   - 雙擊政策的名稱。
   - 右鍵點擊政策名稱以顯示上下文功能表然後選擇**內容**。
   - 點擊**配置政策**連結。
4. 在**內容：<政策名稱>**視窗中，選擇**政策設定檔**部分。
5. 在工作區中，選擇要為其建立啟動規則的政策設定檔，然後點擊**內容**。
   內容：<政策設定檔名稱>視窗開啟。
6. 選擇**啟動規則**部分。
7. 在工作區中，點擊**新增**。
   新政策設定檔啟動規則精靈啟動。

請依照新建政策設定檔啟動規則精靈的步驟進行操作。

修改政策設定檔

1. 在主控台樹狀目錄中，選擇要修改其政策設定檔的管理群組。
2. 在工作區選擇"**政策**"標籤。
3. 執行下列操作之一以開啟要修改設定檔的政策的內容：
   - 雙擊政策的名稱。
   - 右鍵點擊政策名稱以顯示上下文功能表然後選擇**內容**。
   - 點擊**配置政策**連結。
4. 在**內容：<政策名稱>**視窗中，選擇**政策設定檔**部分。

5. 在工作區中，選擇要修改的政策設定檔，然後點擊**內容**。

   內容：<政策設定檔名稱>視窗開啟。

6. 如有必要，配置設定檔：

   - 在**一般**部分中，重新命名設定檔或透過選擇/取消選擇**啟用設定檔**核取方塊來啟用/啟用設定檔。
   - 在**啟動規則**部分中，建立、編輯或刪除啟動規則。
   - 在**裝置**部分中，選擇要套用政策設定檔的裝置。
   - 編輯相關部分中的政策設定。

7. 點擊**OK**。

如果政策設定檔處於活動狀態，則修改的設定將在用戶端電腦與管理伺服器同步後被套用。如果政策設定檔處於非活動狀態，則它們將在啟動規則被觸發後套用。

變更政策設定檔的優先順序

1. 在主控台樹狀目錄中，選擇要變更其政策設定檔優先順序的管理群組。
2. 在工作區選擇**"政策"**標籤。
3. 執行下列操作之一以開啟要變更政策設定檔優先順序的政策的內容：
   - 雙擊政策的名稱。
   - 右鍵點擊政策名稱以顯示上下文功能表然後選擇**內容**。
   - 點擊**配置政策**連結。
4. 在**內容：<政策名稱>**視窗中，選擇**政策設定檔**部分。
5. 在工作區中，選取您希望變更其優先順序的政策設定檔。
6. 透過點選  按鈕提高/降低所選設定檔的優先順序。

刪除政策設定檔

1. 在主控台樹狀目錄中，選擇要刪除其政策設定檔的管理群組。
2. 在工作區選擇**"政策"**標籤。
3. 執行下列操作之一以開啟要刪除設定檔的政策的內容：
   - 雙擊政策的名稱。
   - 右鍵點擊政策名稱以顯示上下文功能表然後選擇**內容**。
   - 點擊**配置政策**連結。
4. 在**內容：<政策名稱>**視窗中，選擇**政策設定檔**部分。
5. 在工作區中，選擇要刪除的設定檔，然後點擊**刪除**。

有關政策設定檔的詳細資訊，請參閱卡巴斯基安全管理中心說明。

產生有關偵測到的物件的報告

產生有關偵測到的物件的報告

1. 啟動卡巴斯基安全管理中心管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，點擊**"受管理裝置"**。
4. 選擇包含所需用戶端電腦的管理群組。
5. 選擇**裝置**索引標籤。
6. 從用戶端電腦清單中選擇電腦。
7. 右鍵點擊所選電腦以開啟上下文功能表，然後選擇**所有工作>檢視威脅報告**。

產生的報告將在瀏覽器視窗中開啟。

您可以在卡巴斯基安全管理中心說明中找到產生關於用戶端電腦上的應用程式偵測到的物件的報告的其他方法的資訊。

取得加密磁碟機的還原金鑰

如果用戶端電腦的使用者忘記或遺失了他或她的憑據並且無法存取加密磁碟機，您可以獲得還原金鑰。

獲取還原金鑰

1. 啟動卡巴斯基安全管理中心管理主控台。
2. 最大化**管理伺服器<伺服器名稱>**節點。
3. 在主控台樹狀目錄中，選擇**"進階"**資料夾，然後選擇**"資料加密和防護"**子資料夾，然後選擇**"加密磁碟機"**子資料夾。
4. 在工作區中，右鍵點擊具有加密磁碟的裝置以顯示捷徑功能表，然後選擇**獲取 macOS 的還原金鑰**。
   一個帶有還原金鑰的視窗將開啟。
5. 以任何方便的方式儲存還原金鑰。

您可以在用戶端電腦上使用此還原金鑰來存取加密磁碟機。

透過卡巴斯基安全管理中心網頁主控台和雲端主控台遠端管理應用程式

卡巴斯基安全管理中心網頁主控台（Web Console）是一個 Web 應用程式，旨在提供集中方式來執行與管理和維護組織的網路安全相關的主要工作。網頁主控台是一個卡巴斯基安全管理中心元件，提供用於在瀏覽器視窗中管理 Kaspersky Endpoint Security 的使用者介面。有關卡巴斯基安全管理中心網頁主控台的詳細資訊，請參閱卡巴斯基安全管理中心說明。

卡巴斯基安全管理中心雲端主控台（雲端主控台）是用於防護和管理群組織網路的基於雲端的解決方案。有關卡巴斯基安全管理中心雲端主控台的詳細資訊，請參閱卡巴斯基安全管理中心雲端主控台說明。

您也可以透過應用程式的圖形使用者介面、卡巴斯基安全管理中心管理主控台和命令列來管理 Kaspersky Endpoint Security。

安裝 Kaspersky Endpoint Security Web 外掛程式

Kaspersky Endpoint Security Web 外掛程式允許在 Kaspersky Endpoint Security 和卡巴斯基安全管理中心之間進行互動。Web 外掛程式必須安裝在安裝了卡巴斯基安全管理中心網頁主控台的裝置上。有權在瀏覽器中存取卡巴斯基安全管理中心網頁主控台的所有管理員都可以使用該 Web 外掛程式的功能。

您可以按如下方式安裝該 Web 外掛程式：

- 使用卡巴斯基安全管理中心網頁主控台的“快速啟動精靈”。

  第一次將網頁主控台連線到管理伺服器時，網頁主控台會自動提示您執行快速啟動精靈。您也可以在網頁主控台介面中執行快速啟動精靈（**“發現和佈署”→“佈署和指派”→“快速啟動精靈”**）。快速啟動精靈還可以檢查已安裝的 Web 外掛程式是否為最新，並下載必需的更新。有關卡巴斯基安全管理中心網頁主控台的“快速啟動精靈”的更多詳細資訊，請參閱卡巴斯基安全管理中心說明。

- 手動，使用從外部來源到網頁主控台的分發套件。

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

若要手動安裝 Kaspersky Endpoint Security Web 外掛程式：

1. 在卡巴斯基安全管理中心網頁主控台的主視窗中，選擇**設定 → Web 外掛程式**。

   已安裝 Web 外掛程式的清單將開啟。

2. 透過以下方式之一開始安裝 Kaspersky Endpoint Security Web 外掛程式：

   - 從卡巴斯基 Web 外掛程式清單安裝：

     a. 點擊**新增**。

     一個所有可用的卡巴斯基 Web 外掛程式的清單將開啟。該清單在新版本的應用程式發佈後會自動更新。

     b. 在清單中找到 Kaspersky Endpoint Security for Mac 12.2.1 Web 外掛程式，然後按一下其名稱。

c. 在包含 Web 外掛程式描述的視窗中，點擊**安裝外掛程式**按鈕。

d. 等待安裝完成，然後在資訊視窗中按一下**確定**。

- 從外部來源安裝 Web 外掛程式（安裝 Web 外掛程式所需的壓縮檔案包含在分發套件中）：

a. 點擊**從檔案新增**按鈕。

b. 在開啟的視窗中，指定包含 Web 外掛程式分發套件的 ZIP 壓縮檔案的路徑以及 TXT 格式的簽章檔案的路徑。該檔案位於 Web 外掛程式的壓縮檔案中。

c. 點擊**新增**。

d. 等待安裝完成，然後在資訊視窗中按一下**「確定」**。

新外掛程式將顯示在已安裝的 Web 外掛程式清單中（**設定 → Web 外掛程式**）。

注意：如果您在卡巴斯基安全管理中心管理伺服器的屬性中選擇 Kaspersky Endpoint Security 分發套件中未包含的語言，則產品授權協議和整個卡巴斯基安全管理中心網頁主控台介面將以英文顯示。

建立政策

本部分包含有關如何使用卡巴斯基安全管理中心網頁主控台和雲端主控台建立和設定 Kaspersky Endpoint Security 政策的資訊。

政策可決定應用程式的設定並管理在管理群組內的裝置上配置該應用程式的能力。必須為每個應用程式建立單獨的政策。您可以為每個管理群組中的裝置上安裝的應用程式建立無限數量的各種政策，但一次只能將一個政策套用至管理群組中的每個應用程式。

注意：建立和設定政策時，您可以使用**強制**切換開關允許或禁止對政策中的任何設定群組進行變更。

建立政策

1. 在左側的**裝置**部分中，選擇**政策和設定檔**部分。
2. 點擊**新增**。
3. 選擇要為其建立政策的應用程式，然後點擊**下一步**。

   新政策視窗將開啟。
4. 在**一般**標籤上，指定政策名稱並配置政策狀態和政策設定繼承選項。
5. 在**應用程式設定**標籤上，設定在強制執行政策時將套用至用戶端電腦上的 Kaspersky Endpoint Security 的應用程式設定。
6. 點擊**儲存**。

您可以對自訂政策執行以下操作：

- 制定政策。
- 配置政策。
- 將政策從一個群組複製或移動到另一個群組。
- 刪除政策。
- 變更政策的狀態。

有關卡巴斯基安全管理中心網頁主控台政策的詳細資訊，請參閱卡巴斯基安全管理中心說明。

有關卡巴斯基安全管理中心雲端主控台政策的詳細資訊，請參閱卡巴斯基安全管理中心雲端主控台說明。

注意：使用卡巴斯基安全管理中心網頁主控台和雲端主控台為 Kaspersky Endpoint Security 政策建立政策設定檔後，您需要檢查這些設定是否正確套用在用戶端電腦上。

主機威脅防護

配置檔案威脅防護元件

您可以透過以下方式之一配置檔案威脅防護元件：

- **使用統一防護和管理外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取"**應用程式設定**"標籤。
  4. 前往 **主機威脅防護 → 檔案威脅防護**。
  5. 使用**檔案威脅防護**撥動開關啟用或停用該元件。
  6. 配置檔案威脅防護元件。
  7. 存儲變更。

- **使用 Kaspersky Endpoint Security 外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。

3. 選取"**應用程式設定**"標籤。

4. 前往 **關鍵威脅防護 → 檔案威脅防護**。

5. 使用**檔案威脅防護**撥動開關啟用或停用該元件。

6. 配置檔案威脅防護元件。

7. 存儲變更。

檔威脅防護設定

設定	描述
掃描排除項目	"*掃描排除項目*"是一組條件，必須滿足這些條件，Kaspersky Endpoint Security 才不會掃描特定物件是否存在病毒和其他威脅。掃描排除項目可確保安全使用可能被入侵者用於損害電腦或使用者資料的合法軟體。儘管這類應用程式並不具備任何惡意功能，它們可能被入侵者利用。有關入侵者可用來破壞電腦或個人資料的合法應用程式的詳細資訊，請參閱 Kaspersky IT 百科全書網站。
偵測到威脅後的動作	**解毒；若解毒失敗則刪除**如果選取該選項，應用程式將自動對偵測到的受感染檔案執行解毒操作。如果解毒失敗，應用程式將刪除檔案。 **提示動作**。Kaspersky Endpoint Security 會顯示一個通知視窗，其中包含有關使檔案受到感染的惡意物件資訊，並提示您選擇 Kaspersky Endpoint Security 要執行的操作。可用的操作可能因物件狀態的不同而有所不同。
防護範圍	包含"檔案威脅防護"元件掃描的物件。掃描物件可能是硬碟、卸除式磁碟機、網路磁碟機、資料夾、檔案或由遮罩定義的多個檔案。 預設情況下，"檔案威脅防護"元件將掃描任何硬碟、網路磁碟機或卸除式磁碟機中啟動的檔案。無法變更或刪除這些物件的防護範圍。您只可以從掃描中排除項（例如卸除式磁碟機）。
掃描最佳化	在 **掃描最佳化**中，您可以配置 Kaspersky Endpoint Security 以便在掃描檔案時獲得更高效能。 • **只掃描新增及修改的檔案**。僅掃描新檔案和自上次掃描以來已被修改的檔案。這有助於縮短掃描的持續時間。此模式適用於簡單檔案和複合檔案。 • **略過唯讀系統磁碟區掃描**。如果選取此核取方塊，應用程式將不會掃描唯讀系統磁碟區。這可大大縮短掃描時間。
掃描複合檔案	隱藏病毒和其他惡意程式的一種常用方法就是將其植入複合檔案中，例如存檔案或資料庫中。為了偵測以這種方式隱藏的病毒和其他惡意軟體，必須將複合檔案解壓縮，但是這可能會降低掃描速度。您可以限制要掃描的複合檔案類型，從而加快掃描速度。 • **掃描壓縮檔案**。掃描 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其它存檔。應用程式不僅依照副檔名而且依照格式掃描存檔。當檢查封存時，應用程式會執行巡迴解壓縮。這可讓人偵測多層封存（封存內的封存）內的威脅。 • **掃描分發套件和自解壓縮檔案**。掃描協力廠商應用程式的安裝套件和自解壓壓縮檔案。自解壓壓縮檔案包含一個可執行的解壓縮模組。若要掃描自解壓壓縮檔案，必須選擇 **掃描壓縮檔案**核取方塊。 • **掃描 Microsoft Office 格式檔案和嵌入式 OLE 物件**。Microsoft Office 檔案（例如 DOC、DOCX、XLS、PPT）和嵌入檔案中的 OLE 物件（例如 Excel 表格、巨集、電子郵件附件）。
允許在背景中解壓縮大於以下大小 (MB) 的壓縮檔案	如果選中該核取方塊，應用程式會提供對大於指定值的複合檔案的存取權限，然後再掃描這些檔案。在這種情況下，Kaspersky Endpoint Security 在背景解壓並掃描複合檔案。 對於小於該值的複合檔案，只有在解壓和掃描這些檔案後，應用程式才會提供對這些檔案的存取權限。 如果未選中該核取方塊，則只有在解壓和掃描任何大小的複合檔案後，應用程式才會提供對這些檔案的存取權限。
不掃描大於該值的壓縮檔案 (MB)	如果選中該核取方塊，應用程式不會掃描其大小超過指定值的複合檔案。 如果清除該核取方塊，應用程式將掃描所有大小的複合檔案。 應用程式會掃描從存檔中提取的大檔案，而不管是否選中該核取方塊。

配置卸除式磁碟機掃描

您可以透過以下方式之一配置卸除式磁碟機掃描元件：

- **使用統一防護和管理外掛程式**

1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。

2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。

3. 選取“**應用程式設定**”標籤。
4. 前往 **主機威脅防護 → 卸除式磁碟機掃描**。
5. 使用**卸除式磁碟機掃描**撥動開關啟用或停用該元件。
6. 配置卸除式磁碟機掃描元件。
7. 存儲變更。

- **使用 Kaspersky Endpoint Security 外掛程式**

1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選取“**應用程式設定**”標籤。
4. 前往**本機工作>外部磁碟掃描**。
5. 配置卸除式磁碟機掃描元件。
6. 存儲變更。

配置行為偵測

您可以透過以下方式之一配置行為偵測元件：

- **使用統一防護和管理外掛程式**

1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選取“**應用程式設定**”標籤。
4. 前往 **主機威脅防護 → 行為分析 → 行為偵測** 部分。
5. 使用**行為偵測**撥動開關啟用或停用該元件。
6. 配置行為偵測元件。
7. 存儲變更。

- **使用 Kaspersky Endpoint Security 外掛程式**

1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。

3. 選取"**應用程式設定**"標籤。
4. 前往**進階威脅防護 → 行為偵測**。
5. 使用**行為偵測**撥動開關啟用或停用該元件。
6. 配置行為偵測元件。
7. 存儲變更。

行為偵測設定

設定	描述
受信任應用程式	*受信任應用程式清單*包含應用程式的檔案和網路活動（包括可疑活動）以及對系統登錄檔的存取不受 Kaspersky Endpoint Security 的監控。預設情況下，Kaspersky Endpoint Security 將監控任何應用程式處理程序開啟、執行或儲存的物件，並控制所有應用程式的活動及其產生的網路流量。應用程式被新增到受信任應用程式清單後，Kaspersky Endpoint Security 將停止監控該應用程式的活動。
掃描排除項目	"*掃描排除項目*"是一組條件，必須滿足這些條件，Kaspersky Endpoint Security 才不會掃描特定物件是否存在病毒和其他威脅。掃描排除項目可確保安全使用可能被入侵者用於損害電腦或使用者資料的合法軟體。儘管這類應用程式並不具備任何惡意功能，它們可能被入侵者利用。有關入侵者可用來破壞電腦或個人資料的合法應用程式的詳細資訊，請參閱 Kaspersky IT 百科全書網站。
偵測到威脅後的動作	**請求操作**。如果偵測到惡意活動，Kaspersky Endpoint Security 會提示使用者選擇偵測到惡意活動時要執行的操作。可用的操作可能因物件狀態的不同而有所不同。 **封鎖**。如果偵測到惡意活動，Kaspersky Endpoint Security 會阻止執行惡意活動的應用程式，並記錄有關偵測到的惡意活動的資訊。 **刪除**。如果選擇此選項，則在偵測到惡意活動時 Kaspersky Endpoint Security 會刪除惡意應用程式的可執行檔案，並在備份中建立該檔案的備份副本。

配置加密軟體防護

您可以透過以下方式之一配置加密軟體防護元件：

- **使用統一防護和管理外掛程式**
  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取"**應用程式設定**"標籤。
  4. 前往 **主機威脅防護 → 行為分析 → 加密軟體防護** 部分。
  5. 使用**加密軟體防護**撥動開關啟用或停用該元件。
  6. 配置加密軟體防護元件。
  7. 存儲變更。
- **使用 Kaspersky Endpoint Security 外掛程式**
  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。

3. 選取“**應用程式設定**”標籤。
4. 前往**進階威脅防護** → **行為偵測**。
5. 使用 **防護共用資料夾免受外部加密攻擊** 撥動開關以啟用或停用該元件。
6. 配置加密軟體防護元件。
7. 存儲變更。

Anti-Cryptor 設定

參數	描述
偵測到威脅後的動作	**通知**.如果選取此選項，在偵測到修改共用資料夾中的檔案的嘗試時，Kaspersky Endpoint Security 會將有關此嘗試的資訊新增到活動威脅清單中，並新增一個項目到報告中。 **封鎖連線（分鐘）**。當偵測到修改共用資料夾中的檔案的嘗試時，Kaspersky Endpoint Security 會封鎖來自執行惡意活動的裝置的網路流量。應用程式會建立一個 *偵測到加密*事件，其中包含有關受感染裝置的資訊。

配置弱點利用防禦元件

您可以透過以下方式之一配置弱點利用防禦元件：

- **使用統一防護和管理外掛程式**
  1. 在網頁主控台的主視窗中，選取**資產管理** → **政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取“**應用程式設定**”標籤。
  4. 前往 **主機威脅防護** → **行為分析** → **弱點利用防禦** 部分。
  5. 使用**弱點利用防禦**撥動開關啟用或停用該元件。
  6. 配置弱點利用防禦元件。
  7. 存儲變更。
- **使用 Kaspersky Endpoint Security 外掛程式**
  1. 在網頁主控台的主視窗中，選取**資產管理** → **政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取“**應用程式設定**”標籤。
  4. 前往**進階威脅防護** → **弱點利用防禦**
  5. 使用**弱點利用防禦**撥動開關啟用或停用該元件。

6. 配置弱點利用防禦元件。
7. 存儲變更。

弱點利用防禦設定

設定	描述
偵測到威脅後的動作	**通知**.。如果選擇此項目，當 Kaspersky Endpoint Security 偵測到弱點利用時，它將記錄一條包含弱點利用資訊的項目並將此弱點利用的相關資訊新增到活動威脅清單。 **封鎖**。如果選擇此項，在偵測到弱點時，Kaspersky Endpoint Security 會封鎖此弱點的操作，並生成一條包含此弱點相關資訊的日誌項目。

配置修復引擎元件

您可以透過以下方式之一配置修復引擎元件：

- **使用統一防護和管理外掛程式**
  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取**"應用程式設定"**標籤。
  4. 前往 **主機威脅防護 → 行為分析 → 修復引擎** 部分。
  5. 使用**修復引擎**撥動開關啟用或停用該元件。
  6. 配置修復引擎元件。
  7. 存儲變更。
- **使用 Kaspersky Endpoint Security 外掛程式**
  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取**"應用程式設定"**標籤。
  4. 前往**進階威脅防護>修復引擎**。
  5. 使用**修復引擎**撥動開關啟用或停用該元件。
  6. 配置修復引擎元件。
  7. 存儲變更。

通訊和 Web 防護

配置“郵件威脅防護”

您可以透過以下方式之一配置郵件威脅防護元件：

- **使用統一防護和管理外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取“**應用程式設定**”標籤。
  4. 前往 **通訊與 Web 防護 → 郵件威脅防護**。
  5. 使用**郵件威脅防護**撥動開關啟用或停用該元件。
  6. 配置郵件威脅防護元件。
  7. 存儲變更。

- **使用 Kaspersky Endpoint Security 外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取“**應用程式設定**”標籤。
  4. 前往 **關鍵威脅防護 → Web 威脅防護**。
  5. 使用**郵件威脅防護**撥動開關啟用或停用該元件。
  6. 配置郵件威脅防護元件。
  7. 存儲變更。

設定	描述
偵測到威脅後的動作	**解毒；若解毒失敗則刪除** 在入站或出站郵件中偵測到受感染的物件時，應用程式會嘗試對偵測到的物件進行解毒。使用者將能夠存取帶安全附件的郵件。如果無法解毒物件，應用程式將刪除受感染的物件。應用程式會將有關已執行操作的資訊新增到郵件主旨，例如，*[郵件已處理]*<*郵件主旨*>。 **封鎖**。如果在入站郵件中偵測到受感染的物件，應用程式會將警告新增到郵件主旨。使用者將能夠存取帶原始附件的郵件。如果在出站郵件中偵測到受感染的物件，應用程式會封鎖郵件的傳輸，郵件使用者端會顯示錯誤。
不掃描大於該值的壓縮檔案 (MB)	如果選擇此方塊，"郵件威脅防護"元件將在掃描中排除大小超過指定值的電子郵件附件。如果清空此方塊，則"郵件威脅防護"元件可以掃描任意尺寸的電子郵件附件。
略過掃描時間超過以下時長的檔案（秒）	如果選擇此方塊，則分配的用於掃描電子郵件壓縮檔案附件的時間將被限制為指定的長度。

配置 Web 威脅防護元件

您可以透過以下方式之一配置網路威脅防護元件：

- **使用統一防護和管理外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取"**應用程式設定**"標籤。
  4. 前往 **通訊與 Web 防護 → Web 威脅防護** 部分。
  5. 使用**Web 威脅防護**撥動開關啟用或停用該元件。
  6. 配置 Web 威脅防護元件。
  7. 存儲變更。

- **使用 Kaspersky Endpoint Security 外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取"**應用程式設定**"標籤。
  4. 前往 **關鍵威脅防護 → Web 威脅防護**。
  5. 使用**Web 威脅防護**撥動開關啟用或停用該元件。
  6. 配置 Web 威脅防護元件。
  7. 存儲變更。

設定	描述
受信任網址	Web 威脅防護認為可信賴的網址清單。此元件不會掃描來自這些位址的傳入和傳出流量以偵測威脅。在一些情況下可以使用受信任網址清單，例如，當"Web 威脅防護"元件干擾您從一個已知網站上下載檔案時。
掃描排除項目	"*掃描排除項目*"是一組條件，必須滿足這些條件，Kaspersky Endpoint Security 才不會掃描特定物件是否存在病毒和其他威脅。掃描排除項目可確保安全使用可能被入侵者用於損害電腦或使用者資料的合法軟體。儘管這類應用程式並不具備任何惡意功能，它們可能被入侵者利用。有關入侵者可用來破壞電腦或個人資料的合法應用程式的詳細資訊，請參閱 Kaspersky IT 百科全書網站。
偵測到威脅後的動作	**封鎖**。如果選擇此選項並且在 Web 流量中偵測到受感染物件，"Web 威脅防護"元件將封鎖存取物件並在瀏覽器中顯示一條訊息。 **提升操作**.Kaspersky Endpoint Security 會顯示一個通知，其中包含有關感染了 Web 流量物件的惡意軟體類型的資訊，並提示您選擇 Kaspersky Endpoint Security 對此物件要採取的操作。可用的操作可能因物件狀態的不同而有所不同。

配置網路威脅防護

您可以透過以下方式之一配置網路威脅防護元件：

- **使用統一防護和管理外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取"**應用程式設定**"標籤。
  4. 前往 **通訊與 Web 防護 → 網路威脅防護** 部分。
  5. 使用**網路威脅防護**撥動開關啟用或停用該元件。
  6. 配置網路威脅防護元件。
  7. 存儲變更。

- **使用 Kaspersky Endpoint Security 外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取"**應用程式設定**"標籤。
  4. 前往 **關鍵威脅防護 → 網路威脅防護**。
  5. 使用**網路威脅防護**撥動開關啟用或停用該元件。
  6. 配置網路威脅防護元件。
  7. 存儲變更。

設定	描述
受信任 IP 位址	受信任裝置的 IP位址清單。網路威脅防護元件不會封鎖來自這些位址的網路活動。
偵測到威脅後的動作	**封鎖**。當偵測到威脅時，網路威脅防護功能會封鎖攻擊。 **封鎖攻擊和攻擊裝置（分鐘）**。如果啟用此選項，"網路威脅防護"元件將把發動攻擊的電腦新增至封鎖清單。這意味著，"網路威脅防護"元件將會在該攻擊電腦的首次網路攻擊嘗試後的指定時間段內，封鎖與該電腦的網路連線。此封鎖操作將會自動防護電腦避免以後來自同一位址的攻擊。攻擊電腦必須待在封鎖清單中的最短時間為一分鐘。最長時間為 999 分鐘。

配置防火牆元件

您可以透過以下方式之一配置防火牆元件：

- **使用統一防護和管理外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取"**應用程式設定**"標籤。
  4. 前往 **通訊與 Web 防護 → 防火牆**。
  5. 使用**防火牆**撥動開關啟用或停用該元件。
  6. 配置防火牆元件。
  7. 存儲變更。

- **使用 Kaspersky Endpoint Security 外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取"**應用程式設定**"標籤。
  4. 前往 **關鍵威脅防護 → 防火牆**部分。
  5. 使用**防火牆**撥動開關啟用或停用該元件。
  6. 配置防火牆元件。
  7. 存儲變更。

設定	描述
網路封包規則	包含網路封包規則清單的表。網路封包規則將對網路封包進行限制，與應用程式無關。此類規則將限制透過特定連接埠的選定資料協定傳送和接收的網路流量。 此表格列出了由 Kaspersky 建議的預配置網路封包規則，它們能最好地為執行 macOS 作業系統的電腦提供網路流量防護。 防火牆將為每條網路封包規則設定執行優先順序。防火牆將按照封包規則清單上的順序從上到下處理網路封包規則。防火牆將找到最適合網路連線的網路封包規則，並套用該規則來允許或封鎖網路活動。然後，防火牆會對特定網路連線略過所有後續網路封包規則。 網路封包規則的優先順序比應用程式網路規則高。
可用網路	此表格包含防火牆在電腦上偵測到的網路連線的資訊。 有以下網路連線類型可用： • 網路不受惡意軟體防護應用程式、防火牆或過濾器（例如咖啡館中的 Wi-Fi）的防護。當使用者操作連線到此類網路的電腦時，防火牆會阻止對該電腦的檔案和印表機的存取。外部使用者也無法透過共用資料夾和遠端存取此電腦的桌面來存取資料。防火牆根據為每一個應用程式設定的網路規則，篩選應用程式的網路活動。 • 為對此電腦上的檔案和印表機具有受限存取權限的使用者提供的網路（例如企業 LAN 或家庭網路）。 • 安全的網絡，其中的電腦不會受到攻擊或未經授權的資料存取嘗試。防火牆允許具有此狀態的網路內的任何網路活動。

安全控制

配置裝置控制元件

您可以透過以下方式之一配置裝置控制元件：

- **使用統一防護和管理外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取**"應用程式設定"**標籤。
  4. 前往 **安全控制 → 裝置控制**。
  5. 使用**裝置控制**撥動開關啟用或停用該元件。
  6. 配置裝置控制。
  7. 存儲變更。

- **使用 Kaspersky Endpoint Security 外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取**"應用程式設定"**標籤。

4. 前往 **安全控制 → 裝置控制**。
5. 使用**裝置控制**撥動開關啟用或停用該元件。
6. 配置裝置控制。
7. 存儲變更。

裝置控制設定

設定	描述
受信任裝置	被授權存取這些裝置的受信任裝置和使用者的清單。
裝置和 Wi-Fi 網路	符合"裝置控制"元件分類的所有可用裝置類型的清單，包括它們各自的存取狀態。

配置 Web 控制元件

您可以透過下列方式之一配置 Web 控制元件：

- **使用統一防護和管理外掛程式**
  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取"**應用程式設定**"標籤。
  4. 前往 **安全控制 → Web 控制**。
  5. 使用**Web 控制**撥動開關啟用或停用該元件。
  6. 配置 Web 控制元件。
  7. 存儲變更。
- **使用 Kaspersky Endpoint Security 外掛程式**
  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取"**應用程式設定**"標籤。
  4. 前往 **安全控制 → Web 控制**。
  5. 使用**Web 控制**撥動開關啟用或停用該元件。
  6. 配置 Web 控制元件。
  7. 存儲變更。

Web 控制設定

設定	描述
規則清單	包含 Web 資源存取規則的清單。每條規則都有一個優先順序。規則在清單中的位置越高，其優先順序就越高。如果某個網站已新增到多條規則，"Web 控制"會基於優先順序最高的規則來管理對該網站的存取。
預設操作	不被任何其他規則覆蓋的 Web 資源的存取規則。下列選項可用： • **允許除規則清單外的所有內容**。 • **封鎖除規則清單外的所有內容**。

資料加密

您可以透過以下方式之一配置資料加密元件：

- **使用統一防護和管理外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取**"應用程式設定"**標籤。
  4. 前往**資料加密**部分。
  5. 使用**資料加密**撥動開關啟用或停用該元件。
  6. 配置資料加密元件。
  7. 存儲變更。

- **使用 Kaspersky Endpoint Security 外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取**"應用程式設定"**標籤。
  4. 前往**資料加密**部分。
  5. 使用**FileVault 磁碟加密**撥動開關啟用或停用該元件。
  6. 配置資料加密元件。
  7. 存儲變更。

"完整磁碟加密"設定

設定	描述
裝置操作	**加密所有硬碟磁碟機**。如果選擇此選項，套用政策後，應用程式將加密所有硬碟。 **解密所有硬碟磁碟機**。如果選擇此選項，套用政策後，應用程式將解密先前已加密的所有硬碟。

一般設定

偵測設定

您可以透過以下方式之一配置偵測設定：

- **使用統一防護和管理外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理** → **政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取**"應用程式設定"**標籤。
  4. 前往 **一般設定** → **偵測設定**。
  5. 配置偵測設定。
  6. 存儲變更。

- **使用 Kaspersky Endpoint Security 外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理** → **政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取**"應用程式設定"**標籤。
  4. 前往 **其他設定** → **防護**。
  5. 配置偵測設定。
  6. 存儲變更。

偵測設定

偵測設定

設定	描述
偵測其他類型的物件	不管應用程式設定的配置如何，Kaspersky Endpoint Security 始終會偵測並封鎖病毒、蠕蟲、木馬和惡意工具。它們可能會給電腦帶來巨大的損害。 您也可以啟用對以下類型物件的偵測： • **可被入侵者利用以破壞您的電腦或個人資料的合法軟體**儘管這類應用程式並不具備任何惡意功能，它們可能被入侵者利用。有關入侵者可用來破壞電腦或個人資料的合法應用程式的詳細資訊，請參閱 Kaspersky IT 百科全書網站。

卡巴斯基安全網路

您可以透過以下方式之一配置卡巴斯基安全網路設定：

- **使用統一防護和管理外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取**"應用程式設定"**標籤。
  4. 前往 **一般設定 → 卡巴斯基安全網路**。
  5. 使用 **卡巴斯基安全網路（KSN）** 切換開關啟用或停用該元件。
  6. 配置卡巴斯基安全網路元件。
  7. 存儲變更。

- **使用 Kaspersky Endpoint Security 外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取**"應用程式設定"**標籤。
  4. 前往 **進階威脅防護 → 卡巴斯基安全網路**。
  5. 使用 **卡巴斯基安全網路** 切換開關啟用或停用該元件。
  6. 配置卡巴斯基安全網路元件。
  7. 存儲變更。

偵測設定

設定	描述
啟用延伸 KSN 模式	*延伸 KSN 模式*是 Kaspersky Endpoint Security 向 Kaspersky 傳送附加資料的一種模式。 無論切換位置如何，Kaspersky Endpoint Security 皆使用 KSN 偵測威脅。
使用雲端模式	*雲端模式* 是指 Kaspersky Endpoint Security 使用輕量級版本的病毒資料庫的應用程式執行模式。當使用輕量級病毒資料庫時，卡巴斯基安全網路支援應用程式執行。與通常的資料庫相比，輕量級版本的病毒資料庫僅需要大約一半的電腦 RAM。如果您未參與卡巴斯基安全網路或已停用雲端模式，Kaspersky Endpoint Security 會從 Kaspersky 伺服器下載完整版本的病毒資料庫。 如果選擇該核取方塊，Kaspersky Endpoint Security 將使用病毒資料庫的輕量級版本，這可以減少作業系統資源上的負載。 選中該核取方塊後，Kaspersky Endpoint Security 在下次更新期間下載病毒資料庫的輕量級版本。 如果清除該核取方塊，Kaspersky Endpoint Security 將使用病毒資料庫的完全版本。 清除該核取方塊後，Kaspersky Endpoint Security 在下次更新期間下載病毒資料庫的完全版本。
使用管理伺服器為 KSN 代理伺服器	如果選中該核取方塊，Kaspersky Endpoint Security 將使用 KSN 代理服務。您可以在管理伺服器內容中配置 KSN 代理服務設定。
當 KSN 代理伺服器不可用時使用卡巴斯基安全網路伺服器	如果選中該核取方塊，當KSN Proxy服務不可用時，Kaspersky Endpoint Security 將使用 KSN 伺服器。KSN 伺服器可以位於 Kaspersky 側，也可以位於協力廠商一側的伺服器（使用卡巴斯基私有安全網路時）。

使用者互動

您可以透過以下方式之一配置應用程式介面設定以及應用程式與使用者互動的設定：

- **使用統一防護和管理外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取**"應用程式設定"**標籤。
  4. 前往 **一般設定 → 使用者互動**。
  5. 配置使用者互動設定。
  6. 存儲變更。

- **使用 Kaspersky Endpoint Security 外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取**"應用程式設定"**標籤。

4. 前往 **其他設定 → 使用者互動**。

5. 配置使用者互動設定。

6. 存儲變更。

使用者互動設定

設定	描述
電腦啟動時啟動 Kaspersky Endpoint Security（ 建議 ）	如果啟用此功能，Kaspersky Endpoint Security 將隨作業系統啟動，且在整個工作階段保護電腦。 如果停用此功能，Kaspersky Endpoint Security 將不會隨作業系統啟動，需使用者手動啟動。電腦防護已停用，使用者資料可能受到威脅。
顯示應用程式圖示	此核取方塊可啟用/停用遠端電腦上功能表列中應用程式圖示的顯示。 如果選取此核取方塊，應用程式圖示將顯示在功能表列中。 如果清除此核取方塊，應用程式圖示將被從功能表列中隱藏。 預設情況下已選擇此選擇方塊。
本機管理更新	如果選取此核取方塊，則會啟用遠端電腦上 Kaspersky Endpoint Security 更新的本機管理。 如果清除此核取方塊，則只能使用卡巴斯基安全管理中心中的 Kaspersky Endpoint Security 管理外掛程式來管理遠端電腦上的 Kaspersky Endpoint Security 更新。
本機管理金鑰	如果選取該核取方塊，則會啟用遠端電腦上 Kaspersky Endpoint Security 金鑰的本機管理。 如果清除該核取方塊，則只能使用卡巴斯基安全管理中心中的 Kaspersky Endpoint Security 管理外掛程式來管理遠端電腦上的 Kaspersky Endpoint Security 金鑰。
結束應用程式	如果選取此核取方塊，則應用程式圖示的上下文功能表中將出現**結束**命令。遠端電腦的使用者可以結束遠端電腦上的 Kaspersky Endpoint Security。 如果清除此核取方塊，則應用程式圖示的上下文功能表中將不會出現**結束**命令。遠端電腦的使用者無法結束遠端電腦上的 Kaspersky Endpoint Security。

自我防護

您可以透過以下方式之一配置自我防護設定：

- **使用統一防護和管理外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。

  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。

  3. 選取**"應用程式設定"**標籤。

  4. 前往 **一般設定 → 自我防護**。

  5. 使用**密碼防護**撥動開關啟用或停用該元件。

  6. 配置自我防護。

  7. 存儲變更。

- **使用 Kaspersky Endpoint Security 外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。

  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。

3. 選取“**應用程式設定**”標籤。
4. 前往 **其他設定** → **使用者互動**。
5. 使用**密碼防護**撥動開關啟用或停用該元件。
6. 配置密碼防護。
7. 存儲變更。

自我防護設定

設定	描述
密碼防護	如果開啟此切換開關，當使用者嘗試執行密碼防護範圍內的操作時，Kaspersky Endpoint Security 將提示使用者輸入密碼。密碼防護範圍包括禁止的操作（如停用防護元件）和密碼防護範圍適用的使用者帳戶。 啟用密碼防護後，Kaspersky Endpoint Security 會提示您設定 KLAdmin 帳戶的密碼。

效能

您可以透過以下方式之一配置效能設定：

- **使用統一防護和管理外掛程式**
  1. 在網頁主控台的主視窗中，選取**資產管理** → **政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取“**應用程式設定**”標籤。
  4. 前往 **一般設定** → **效能**。
  5. 配置效能設定。
  6. 存儲變更。
- **使用 Kaspersky Endpoint Security 外掛程式**
  1. 在網頁主控台的主視窗中，選取**資產管理** → **政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取“**應用程式設定**”標籤。
  4. 前往 **其他設定** → **防護**。
  5. 配置效能設定。
  6. 存儲變更。

效能設定

設定	描述
使用電池供電時延遲或者略過排程工作	如果啟用此功能，Kaspersky Endpoint Security 將切換到省電模式。 Kaspersky Endpoint Security 會*取消*排程的工作。如果需要，您可以手動啟動掃描和更新工作。
限制掃描工作的 CPU 使用	若要最佳化 Kaspersky Endpoint Security 效能，您可以透過惡意軟體掃描工作限制 CPU 使用率。 如果啟用此功能，則惡意軟體掃描工作的所有 CPU 核心上的平均負載會接近指定的值。

報告和儲存

您可以透過以下方式之一配置報告和儲存設定：

- **使用統一防護和管理外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取**"應用程式設定"**標籤。
  4. 前往 **一般設定 → 報告和儲存**。
  5. 配置報告和儲存設定。
  6. 存儲變更。

- **使用 Kaspersky Endpoint Security 外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取**"應用程式設定"**標籤。
  4. 前往 **其他設定 → 報告和備份**。
  5. 配置報告和儲存設定。
  6. 存儲變更。

報告和儲存設定

設定	描述
以下時間後刪除報告 (天)	如果選中該核取方塊，則最大報告儲存期限制為定義的時間隔。在此時間之後，Kaspersky Endpoint Security 將自動移除報告檔案中的最早項目。
僅保留近期的事件	如果勾選此核取方塊，則每次啟動工作時，Kaspersky Endpoint Security 都會刪除自上次啟動工作以來發生的非關鍵事件的資訊，但會保留報告中的重要註釋（例如，有關偵測到的惡意對象的資訊）。

設定	描述
記錄非緊急事件	如果選擇該選擇方塊，Kaspersky Endpoint Security 將在報告中記錄非關鍵事件（例如資訊事件）。非緊急事件不影響防護。
以下時間後刪除物件 (天)	如果選中該核取方塊，則最大檔案儲存期限制為定義的時間間隔。最長儲存期限超出後，Kaspersky Endpoint Security 將刪除備份區中最舊的檔案。

網路設定

您可以透過以下方式之一配置網路設定：

- **使用統一防護和管理外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取**"應用程式設定"**標籤。
  4. 前往 **一般設定 → 網路設定**。
  5. 配置網路設定。
  6. 存儲變更。

- **使用 Kaspersky Endpoint Security 外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取**"應用程式設定"**標籤。
  4. 前往 **其他設定 → 網路**。
  5. 配置網路設定。
  6. 存儲變更。

網路設定

設定	描述
受信任的根憑證	信任根憑證清單。如果（例如）您需要部署新認證中心，Kaspersky Endpoint Security 可讓您在使用者電腦上安裝受信任根憑證。該應用程式可讓您將憑證新增至一個特殊的 Kaspersky Endpoint Security 憑證商店。在此情況下，該憑證被認為僅對 Kaspersky Endpoint Security 應用程式受信任。換而言之，使用者可以用瀏覽器中的新憑證存取網站。如果其它應用程式嘗試存取網站，你會因為憑證問題得到一個連線錯誤。
代理伺服器	用於用戶端電腦使用者存取網際網路的代理伺服器的設定。Kaspersky Endpoint Security 使用這些設定來配置某些防護元件，包括進行與更新資料庫和程式模組有關的配置。
使用代理伺服器身分驗證	如果選取此核取方塊，則應用程式在連線到代理伺服器時將使用使用者名稱和密碼進行身分驗證。

設定	描述
本機位址略過代理伺服器	如果選擇此方塊，則 Kaspersky Endpoint Security 從共用資料夾執行更新時不使用代理伺服器。
加密連線掃描	此功能可讓 Web 威脅防護、郵件威脅防護和 Web 控制元件監控和處理加密 (HTTPS) 連線。

遙測設定

您可以透過以下方式之一配置遙測設定：

- **使用統一防護和管理外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取**"應用程式設定"**標籤。
  4. 前往 **一般設定 → 遙測設定**。
  5. 配置遙測設定。
  6. 存儲變更。

- **使用 Kaspersky Endpoint Security 外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取**"應用程式設定"**標籤。
  4. 前往 **其他設定 → 受信任區域 → 遙測設定**。
  5. 配置遙測設定。
  6. 存儲變更。

遙測設定

設定	描述
EDR Expert (on-premise) 遙測	**匯入** 和 **匯出**。您可以將 EDR Expert（內部部署）遙測設定匯出至 JSON 檔案。然後，您可以修改檔案，例如，新增大量事件 ID。您還可以使用匯出/匯入功能來備份傳送事件的設定，或將清單遷移到其他政策。
一般排除項目	為了最佳化傳輸的資料，您可以為某些事件類型配置排除規則。Kaspersky Endpoint Security 不會收集屬於此類規則範圍內的遙測資料。這樣可以減少流量，並避免處理來自受信任物件和處理程序的事件。

事件設定

應用程式運行時，會發生各種 *事件*。他們可以是純粹的資訊或包含重要資訊。例如，應用程式可以使用事件來通知資料庫更新成功，或指出需要修復的元件錯誤。

Kaspersky Endpoint Security 事件可分為以下幾個嚴重類別：

- *緊急事件* – 對電腦安全構成危險威脅的事件（偵測到惡意物件、弱點、Kaspersky Endpoint Security 問題）。緊急事件需要您立即關注。我們建議您不要停用緊急事件的通知。
- *功能失效* 是 Kaspersky Endpoint Security 發生故障（處理錯誤、工作設定錯誤）時所發生的事件。此類事件不會直接威脅電腦的安全，但需要您進行幹預，以確保 Kaspersky Endpoint Security 正常運作並防護您的裝置。
- *警告* – 不需要您立即關注但可能對未來電腦安全構成威脅的事件。
- *資訊訊息* – 報告供您參考的事件。

無論是否啟用或者停用通知，Kaspersky Endpoint Security 都會將所有應用程式事件的資訊記錄在應用程式報告中。

更新設定

您可以透過以下方式之一配置更新設定：

- **使用統一防護和管理外掛程式**
  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取**"應用程式設定"**標籤。
  4. 前往 **一般設定 → 更新**。
  5. 配置更新設定。
  6. 存儲變更。
- **使用 Kaspersky Endpoint Security 外掛程式**
  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取**"應用程式設定"**標籤。
  4. 轉到**"更新"**區域。

5. 配置更新設定。

6. 存儲變更。

更新設定

設定	描述
更新來源	*更新來源*是包含 Kaspersky Endpoint Security 的資料庫和程式模組更新的資源。 更新來源包括卡巴斯基安全管理中心、卡巴斯基更新伺服器、以及網路或本機資料夾。 如果卡巴斯基的更新伺服器不可用，Kaspersky Endpoint Security 可以使用備用網域來接收資料庫和應用程式模組更新。有關詳細資訊，請參閱技術支援知識庫。 更新來源的預設清單包括了卡巴斯基安全管理中心和卡巴斯基更新伺服器。您可以在清單中新增其他更新來源。您可以指定 HTTP/FTP 伺服器和共用資料夾作為更新來源。 除非它們是卡巴斯基的更新伺服器，否則 Kaspersky Endpoint Security 不支援來自 HTTPS 伺服器的更新。 如果選取了多個來源作為更新來源，Kaspersky Endpoint Security 將嘗試從清單頂端開始依次連接，使用從第一個可用源檢索到的更新資料執行更新工作。 預設情況下，Kaspersky Endpoint Security 使用卡巴斯基安全管理中心伺服器作為第一個更新來源。這有助於在更新時節省流量。如果政策未被套用到電腦，卡巴斯基伺服器將被選為更新本機工作設定中的第一個更新來源，因為應用程式可能無法存取卡巴斯基安全管理中心伺服器。

內建代理

配置 Managed Detection and Response

您可以透過以下方式之一配置 Managed Detection and Response元件：

- **使用統一防護和管理外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。

  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。

  3. 選取"**應用程式設定**"標籤。

  4. 前往 **內置代理設定 → Managed Detection and Response** 部分。

  5. 使用**Managed Detection and Response** 撥動開關啟用或停用該元件。

  6. 配置 Managed Detection and Response 元件

  7. 存儲變更。

- **使用 Kaspersky Endpoint Security 外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取**"應用程式設定"**標籤。
  4. 轉到**Detection and Response > Managed Detection and Response**。
  5. 使用**Managed Detection and Response** 撥動開關啟用或停用該元件。
  6. 配置 Managed Detection and Response 元件
  7. 存儲變更。

Managed Detection and Response 元件設定

設定	描述
MDR 設定檔	BLOB 檔案包含用戶端 ID 以及有關 Kaspersky Managed Detection and Response 產品許可的資訊。BLOB 檔案位於 MDR 設定檔的 ZIP 壓縮檔案中。您可以在 Kaspersky Managed Detection and Response 主控台中獲取 ZIP 壓縮檔案。有關 BLOB 檔案的詳細資訊，請參閱 Kaspersky Managed Detection and Response 說明。

配置 Endpoint Detection and Response

您可以透過以下方式之一配置 Endpoint Detection and Response元件：

- **使用統一防護和管理外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取**"應用程式設定"**標籤。
  4. 前往 **內置代理設定 → Endpoint Detection and Response** 部分。
  5. 使用**Managed Detection and Response** 撥動開關啟用或停用該元件。
  6. 配置 Endpoint Detection and Response 元件。
  7. 存儲變更。

- **使用 Kaspersky Endpoint Security 外掛程式**

  1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。
  2. 點擊 Kaspersky Endpoint Security 政策的名稱。
     政策內容視窗將開啟。
  3. 選取**"應用程式設定"**標籤。

4. 轉到**Detection and Response** > **Endpoint Detection and Response**。

5. 使用**Endpoint Detection and Response** 撥動開關啟用或停用該元件。

6. 配置 Endpoint Detection and Response 元件。

7. 存儲變更。

Endpoint Detection and Response 設定

設定	描述
網路隔離	回應偵測到的威脅自動將電腦從網路中隔離。 當開啟網路隔離時，應用程式會斷開電腦上的所有活動連線並封鎖所有新的 TCP/IP 連線。應用程式只會讓以下連線處於活動狀態： • 網路隔離排除項目中列出的連線。 • Kaspersky Endpoint Security 服務安裝的連線。 • 卡巴斯基安全管理中心網路代理啟動的連線。
自動解鎖隔離裝置的時間 (小時)	指定時間後可以自動或者手動關閉網路隔離。
網路隔離排除項目	從網路隔離中排除的規則清單當開啟網路隔離時，電腦上匹配規則的網路連線不會被封鎖。 要配置網路隔離排除項目，您可以使用"*標準網路設定檔*"清單。預設情況下，排除項目包括包含確保裝置（具有 DNS/DHCP 伺服器和 DNS/DHCP 用戶端角色）不中斷操作的規則的網路設定檔。您也可以修改標準網路設定檔的設定或者手動定義排除項目。 只有當網路隔離回應偵測到的威脅自動開啟時，政策內容中指定的排除項目才會套用。只有當網路隔離在卡巴斯基安全管理中心主控台的電腦內容或者警示詳情中手動開啟時，電腦內容中指定的排除項目才會套用。
執行防止	控制可執行檔和指令碼的執行以及 Office 格式檔案的開啟。例如，您可以防止執行在選取電腦上被認為不安全的應用程式。執行防護支援 Office 檔案延伸程式集合和指令碼解譯器集合。 所要使用執行防禦元件，您需要新增執行防禦規則。
執行或開啟被禁止的物件時的動作	**封鎖並新增至事件記錄**。在此模式中，應用程式會封鎖執行物件或者開啟匹配防護規則條件的文件。應用程式也會將嘗試執行物件或者開啟文件的事件發佈到系統事件記錄和卡巴斯基安全管理中心事件記錄。 **新增至事件記錄**。在此模式中，Kaspersky Endpoint Security 會將嘗試執行可執行物件或者開啟匹配防護規則條件的文件的事件發佈到系統事件記錄和卡巴斯基安全管理中心，但是不會封鎖執行或者開啟物件或者文件的嘗試。預設情況下已選擇此項。
執行防止規則	*執行防護規則*是應用程式對物件執行進行回應（例如，封鎖物件執行時）時考慮的一組條件。應用程式根據檔案路徑或者使用 MD5 和 SHA256 雜湊演算法計算的總和檢查碼來識別檔案。
Cloud Sandbox	*Cloud Sandbox* 技術可讓您偵測電腦上的進階威脅。Kaspersky Endpoint Security 自動將被偵測檔案轉寄到 Cloud Sandbox 進行分析。Cloud Sandbox 在隔離環境中執行這些檔案以識別惡意活動和決定其信譽。有關這些檔案的資料然後被傳送到卡巴斯基安全網路。因此，如果 Cloud Sandbox 偵測到一個惡意檔案，Kaspersky Endpoint Security 將執行適當操作在偵測到該檔案的所有電腦上消除該威脅。 要取得有關被分析物件的資訊，需要建立 KSN 連線。

配置 Endpoint Detection and Response Expert（內部部署）

您可以透過以下方式之一配置 Endpoint Detection and Response Expert（內部部署）元件：

- **使用統一防護和管理外掛程式**

1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。

2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。

3. 選取"**應用程式設定**"標籤。

4. 前往 **內置代理設定 → Endpoint Detection and Response Expert (on-premise)** 部分。

5. 使用**Managed Detection and Response Expert（內部部署）**撥動開關啟用或停用該元件。

6. 配置 Endpoint Detection and Response Expert（內部部署）元件

7. 存儲變更。

- **使用 Kaspersky Endpoint Security 外掛程式**

1. 在網頁主控台的主視窗中，選取**資產管理 → 政策**。

2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。

3. 選取"**應用程式設定**"標籤。

4. 前往**Detection and Response** > **Endpoint Detection and Response Expert (on-premise)**。

5. 使用**Managed Detection and Response Expert（內部部署）**撥動開關啟用或停用該元件。

6. 配置 Endpoint Detection and Response Expert（內部部署）元件

7. 存儲變更。

Endpoint Detection and Response Expert（內部部署）元件設定

設定	描述
Endpoint Detection and Response Expert 解決方案	Kaspersky Endpoint Security 可與之進行整合的 Endpoint Detection and Response Expert 解決方案。 • **Endpoint Detection and Response Expert（版本 7.1 或者更早版本）** • **Endpoint Detection and Response Expert（版本 8.0 或者更高版本）**
連線設定	管理以下 KATA 或遙測資料收集伺服器連線設定： • **伺服器連線逾時**。Central Node 伺服器響應最大逾時。當超時用完時，Kaspersky Endpoint Security 會嘗試連線到不同的中央節點伺服器。 • **伺服器憑證**。用於與 Central Node 伺服器建立可信連線的 TLS 憑證。您可以在 Kaspersky Anti Targeted Attack Platform 主控台中獲取 TLS 憑證（請參閱 Kaspersky Anti Targeted Attack Platform 說明）。 • **使用雙向身分驗證**。在 Kaspersky Endpoint Security 和中央節點伺服器之間建立安全連線時進行雙向身分驗證。要使用雙向身分驗證，您需要在 Central Node 伺服器設定中啟用雙向身分驗證，然後獲取加密容器並設定密碼以防護加密容器。加密容器是一個帶有憑證和私鑰的 PFX 存檔。您可以在 Kaspersky Anti Targeted Attack Platform 主控台中獲得一個加密容器（請參閱 Kaspersky Anti Targeted Attack Platform 說明）。配置中央節點設定後，您還需要在 Kaspersky Endpoint Security 設定中啟用雙向身分驗證並加載受密碼防護的加密容器。 加密容器必須受密碼防護。無法新增密碼為空的加密容器。
傳送同步請求到伺服器的時間間隔 (分) *（僅適用於 Endpoint Detection and Response Expert 7.1 或更早版本）*	傳送到伺服器的同步請求的頻率。在同步期間，Kaspersky Endpoint Security 傳送有關被修改應用程式設定和工作的資訊。
連線到 KATA 伺服器 / 遙測資料收集伺服器連線	輸入與 Kaspersky Anti Targeted Attack Platform 伺服器或遙測資料收集伺服器連線的 IP 位址和連接埠。 您可以新增 Central Node（用於 KATA）或遙測資料收集伺服器的多個位址。Kaspersky Endpoint Security 嘗試連線到第一個 IP 位址的伺服器。如果無法建立連線，Kaspersky Endpoint Security 將嘗試連線到清單中的第二個 IP 位址，依此類推。 EDR（KATA）和 EDR Expert（內部部署）解決方案具有不同的架構。對於遙測資料處理，EDR Expert（內部部署）使用遙測資料收集伺服器，EDR（KATA）使用 Central Node 伺服器。因此，如果您要將應用程式與 EDR Expert（內部部署）整合，則需要新增遙測資料收集伺服器。

設定	描述
傳送遙測資料到 KATA / 將遙測資料傳送至遙測資料收集伺服器	根據所選方案，此功能可完全阻止遙測資料被傳送至 KATA 伺服器或遙測資料收集伺服器。例如，如果您將 Kaspersky Anti Targeted Attack Platform 與另一個也使用遙測的解決方案一起使用，您可以關閉 KATA (EDR) 的遙測資料傳送。這可讓您最佳化這些解決方案的伺服器負載。 如果您部署了 Managed Detection and Response 解決方案和 KATA (EDR)，則可以使用 MDR 遙測並在 KATA (EDR) 中建立「威脅回應」工作。
最大事件傳輸延遲時間（秒）	應用程式在同步間隔到期後與伺服器同步以傳送事件。
啟用請求節流	該功能有助於最佳化伺服器負載。如果選中該核取方塊，應用程式將限制傳輸的事件。如果事件數量超過配置的限制，Kaspersky Endpoint Security 將停止傳送事件。 **每個小時的最大事件數量**.如果事件流超過配置的每小時事件數限制，應用程式會分析遙測數據流並限制事件的傳送。Kaspersky Endpoint Security 在一小時後還原傳送事件。如果應用程式安裝在伺服器上，則遙測資料流會更高。對於伺服器，建議將該值增加到每小時 60,000 個事件。 **事件限制超過百分比**.該應用程式按類型對事件進行排序（例如，"登錄檔中的變更"事件），如果相同類型的事件佔事件總數的比率超過配置的百分比限制，則限制事件的傳輸。當其他事件與事件總數的比率再次變得足夠大時，Kaspersky Endpoint Security 會還原傳送事件。
連線至回應伺服器 *（僅適用於 Endpoint Detection and Response Expert 8.0 或更高版本）*	連線到回應伺服器設定。請輸入回應伺服器 IP 位址（IPv4 或 IPv6）和連線到伺服器的連接埠。 您可以新增多個回應伺服器位址。Kaspersky Endpoint Security 嘗試連線到第一個 IP 位址的伺服器。如果無法建立連線，Kaspersky Endpoint Security 將嘗試連線到清單中的第二個 IP 位址，依此類推。
連線設定 *（僅適用於 Endpoint Detection and Response Expert 8.0 或更高版本）*	為回應伺服器連線設定以下內容： • **伺服器連線逾時**。回應伺服器回應最大逾時。當逾時用完時，Kaspersky Endpoint Security 會嘗試連線到不同的伺服器。 • **伺服器憑證**。用於與回應伺服器建立可信連線的 TLS 憑證。 • **使用雙向身分驗證**。在 Kaspersky Endpoint Security 和回應伺服器之間建立安全連線時進行雙向身分驗證。要使用雙向身分驗證，您需要在回應伺服器設定中啟用雙向身分驗證，然後獲取加密容器並設定密碼以防護加密容器。*加密容器*是一個帶有憑證和私鑰的 PFX 存檔。您可以在 Kaspersky Anti Targeted Attack Platform 主控台中獲得一個加密容器（請參閱 Kaspersky Anti Targeted Attack Platform 說明）。配置回應伺服器設定後，您還需要在 Kaspersky Endpoint Security 設定中啟用雙向身分驗證並加載受密碼防護的加密容器。 加密容器必須受密碼防護。無法新增密碼為空的加密容器。

建立工作

本節介紹如何使用卡巴斯基安全管理中心網頁主控台和雲端主控台建立和配置 Kaspersky Endpoint Security 在卡巴斯基安全管理中心管理的用戶端電腦或電腦群組上執行的工作。

*工作*是 Kaspersky Endpoint Security 在用戶端電腦上執行的一組可配置操作。

在卡巴斯基安全管理中心網頁主控台和雲端主控台中，您可以建立以下工作：

- 掃描
- 更新
- 回溯
- 新增金鑰

建立工作

1. 在左側的**裝置**部分中，選擇**工作**部分。
2. 點擊**新增**。
   新增工作精靈將啟動。
3. 在"**應用程式**"下拉清單中，選取"**Kaspersky Endpoint Security for Mac (12.2.1)**"。
4. 在"**工作類型**"下拉清單中，選取您想要建立的工作。
5. 如果需要，請在**工作名稱**欄位中編輯工作名稱。
6. 選取將要對其分配工作的裝置。
7. 配置所選工作類型的設定。
8. 點擊**結束**完成新增工作精靈。

> **注意：**如果您在**完成工作建立**視窗中選取**建立完成後開啟工作詳細資料**核取方塊，則可以繼續修改預設工作設定。如果不選取此核取方塊，則會使用預設設定建立工作。您可以在以後隨時修改預設工作設定。

您可以對工作執行以下操作：

- 啟動和停止工作。
- 配置工作設定。
- 追蹤工作的進度。
- 將工作從一組複製並移動到另一組。
- 刪除工作。

有關卡巴斯基安全管理中心網頁主控台工作的詳細資訊，請參閱卡巴斯基安全管理中心說明。

有關卡巴斯基安全管理中心雲端主控台工作的詳細資訊，請參閱卡巴斯基安全管理中心雲端主控台說明。

配置掃描工作設定

在**應用程式設定**標籤上，您可以設定遠端電腦上 Kaspersky Endpoint Security 的**掃描**工作設定。

開啟掃描工作設定

1. 轉至**裝置>工作**。
2. 雙擊工作類型為**掃描**的工作。
3. 選取"**應用程式設定**"標籤。

如有必要，請執行以下操作：

- 定義掃描範圍。
- 指定 Kaspersky Endpoint Security 在偵測到感染物件時執行的操作。
- 選擇執行掃描工作時 Kaspersky Endpoint Security 將掃描的檔案類型。
- 配置掃描效能設定。
- 選擇 Kaspersky Endpoint Security 將分析哪些複合檔案。

注意： Kaspersky Endpoint Security 不會掃描位於 OneDrive 或 iCloud 儲存或其他雲端儲存中的檔案。請將這些檔案從掃描範圍中排除。否則，掃描工作可能會以*受感染檔案未刪除*錯誤結束。

配置“新增金鑰“工作設定

在**應用程式設定**標籤上，您可以為遠端電腦上的 Kaspersky Endpoint Security 設定**新增金鑰**工作設定。

開啟新增金鑰工作設定

1. 轉至**裝置>工作**。
2. 雙擊工作類型為**新增金鑰**的工作。
3. 選取“**應用程式設定**”標籤。

如有必要，請執行以下操作：

- 將目前產品授權金鑰設為備用金鑰。
- 選擇另一個金鑰來啟動使用者電腦上的 Kaspersky Endpoint Security。
- 將新的產品授權金鑰新增至卡巴斯基安全管理中心儲存庫。

配置“更新”工作

在**應用程式設定**標籤上，您可以設定遠端電腦上 Kaspersky Endpoint Security 的**更新**工作設定。

開啟“更新”工作設定

1. 轉至**裝置>工作**。
2. 雙擊工作類型為**更新**的工作。
3. 選取“**應用程式設定**”標籤。

專用卡巴斯基更新伺服器是 Kaspersky Endpoint Security 更新的主要來源。Kaspersky Endpoint Security 也可以使用發佈點、本機資料夾或其他 Web 伺服器作為*更新來源*。

如果您透過卡巴斯基安全管理中心網頁主控台管理 Kaspersky Endpoint Security，則更新來源清單預設包括卡巴斯基更新伺服器和卡巴斯基安全管理中心伺服器。Kaspersky Endpoint Security 首先從卡巴斯基安全管理中心伺服器下載更新，然後從卡巴斯基更新伺服器下載更新。

如果您透過卡巴斯基安全管理中心雲端主控台管理 Kaspersky Endpoint Security，則更新來源清單預設包括卡巴斯基更新伺服器和發佈點。Kaspersky Endpoint Security 首先從發佈點下載更新，然後從 Kaspersky 更新伺服器下載更新。有關發佈點的詳細資訊，請參閱卡巴斯基安全管理中心說明。

如有必要，請執行以下操作：

- 開啟/關閉應用程式模組的更新。
- 新增或刪除將用於更新 Kaspersky Endpoint Security 的更新來源。

取得加密磁碟機的還原金鑰

如果用戶端電腦的使用者忘記或遺失了他或她的憑據並且無法存取加密磁碟機，您可以獲得還原金鑰。

獲取還原金鑰

1. 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選擇 **設定 → 介面選項**。
2. 開啟顯示資料加密與防護切換開關以啟用管理資料加密，然後點擊**儲存**。
3. 轉至**操作 → 資料加密與防護 → 加密磁碟機**。
   加密裝置清單開啟。
4. 選取具有加密磁碟機的裝置旁的核取方塊。
5. 點擊**同意存取離線模式下的裝置**。
6. 在**授予離線模式下裝置的存取權限**對話方塊中，選擇 Kaspersky Endpoint Security 的 Web 外掛程式，然後點擊**確定**。
7. 點擊**獲取還原金鑰**。
   還原金鑰將出現在目前對話視窗中。
8. 以任何方便的方式儲存還原金鑰。

您可以在用戶端電腦上使用此還原金鑰來存取加密磁碟機。

從命令列管理應用程式

您可以從命令列管理 Kaspersky Endpoint Security 應用程式。

注意：安裝 Kaspersky Endpoint Security 模組更新後，命令列中的應用程式用戶端版本可能不同於安裝的應用程式版本。

命令列語法：

```
kav <指令> <參數>
```

每條指令都有各自的受支援參數範圍。

檢視命令列說明

使用以下指令檢視應用程式命令列語法的相關資訊：

```
kav -? | help
```

執行惡意軟體掃描

指令語法：

```
kav scan <掃描範圍> <操作> <檔案類型> <排除項目> <報告參數> <進階參數>
```

注意：要執行惡意軟體掃描，您也可以透過從命令列啟動工作來使用應用程式中建立的工作。此工作使用 Kaspersky Endpoint Security 介面中指定的參數啟動。

參數敘述

<掃描範圍> – 此參數指定要掃描惡意代碼的物件清單。您可以包含多個參數，用空格分隔它們。

注意： Kaspersky Endpoint Security 不會掃描位於 OneDrive 或 iCloud 儲存或其他雲端儲存中的檔案。請將這些檔案從掃描範圍中排除。否則，掃描工作可能會以*受感染檔案未刪除*錯誤結束。

有以下可能的值：

- `<files>` – 要掃描的檔案和/或資料夾的路徑清單。您可以指定檔案的絕對或相對路徑。清單中的項目以空格分隔。

  注意：如果物件的名稱或其路徑包含空格或特殊字元（例如`$`、`&`或`@`），則該名稱應該用單引號(`' '`)括起來，或者每個特殊字元都應該透過立即在前面新增反斜線(`\`)逸出。如果引用特定資料夾，則會掃描該資料夾中的所有檔案和資料夾。

- `-all` – 完整掃描您的電腦。
- `-remdrives` – 所有卸除式磁碟機。
- `-fixdrives` – 所有內部磁碟機。
- `-netdrives` – 所有網路磁碟機。
- `-@:<filelist.lst>` – 包含掃描範圍內的物件和資料夾清單的檔案路徑。該檔案必須採用文字格式，並且每個掃描物件必須在單獨的行中列出。只能輸入檔案的絕對路徑。

`<action>` – 此參數決定對掃描期間偵測到的惡意物件所採取的動作。如果未定義此參數，則預設操作為對應值`-i8`的操作。

有以下可能的值：

- `-i0` – 對物件不採取任何操作，僅在報告中保存有關物件的資訊。
- `-i1` – 對感染物件進行解毒，如果無法解毒則跳過。
- `-i2` – 解毒感染物件，若無法解毒則刪除；不要刪除容器，帶有可執行標頭（SFX 壓縮檔案）的容器除外。
- `-i3` – 解毒感染物件，若無法解毒則刪除；如果無法刪除容器內受感染的檔案，請徹底刪除容器。
- `-i4` – 刪除感染物件；如果無法刪除容器內受感染的檔案，請徹底刪除容器。
- `-i8` – 如果偵測到感染物件，提示使用者採取操作（預設使用）。
- `-i9` – 掃描完成後提示使用者執行操作。

`<file types>` – 此參數定義要接受惡意軟體掃描的檔案類型。預設情況下，如果未定義此參數，則僅掃描可能被感染的檔案（基於檔案內容）。

有以下可能的值：

- `-fe` – 僅掃描可能被感染的檔案（基於檔案副檔名）。
- `-fi` – 僅掃描可能被感染的檔案（基於檔案內容）。預設使用此參數。
- `-fa` – 掃描所有檔案。

`<exclusions>` – 此參數定義要從掃描中排除的物件。您可以包含多個參數，用空格分隔它們。

有以下可能的值：

- `-e:a` – 不掃描壓縮檔案。
- `-e:b` – 不掃描電子郵件資料庫。
- `-e:m` – 不掃描文字格式的電子郵件。
- `-e:<mask>` – 不按遮罩掃描物件。
- `-e:<seconds>` – 跳過掃描時間超過指定時間長度（以秒為單位）的物件。
- `-es:<size>` – 跳過大小大於指定值（以兆位元組為單位）的物件。

`<report parameters>` – 這些參數定義掃描結果報告的格式。您可以指定報告檔案的絕對或相對路徑。如果不定義該參數，則顯示回溯結果和所有事件。

有以下可能的值：

- `-r:<report file>` – 僅將重要事件記錄到指定的報告檔案中。
- `-ra:<report file>` – 將所有事件記錄到指定的報告檔案中。

`<advanced parameters>` – 定義惡意軟體掃描技術和設定檔的使用的參數：

- `-iSwift=<on|off>` – 啟用/停用 iSwift 的使用。
- `-c:<configuration file>` – 定義包含惡意軟體掃描工作的應用程式設定的設定檔的路徑。您可以指定檔案的絕對或相對路徑。如果未指定此參數，則應用程式介面中設定的值將與命令列中已指定的值一起使用。

範例:
開始掃描資料夾 ~/Documents、/Applications 和名為 my test.exe 的檔案：

```
kav scan ~/Documents /Applications 'my test.exe'
```

掃描檔案 objects2scan.txt 中所列的物件。使用 scan_settings.txt 設定檔。掃描完成後，建立一個報告來記錄所有事件：

```
kav scan -@:objects2scan.txt -c:scan_settings.txt -ra:scan.log
```

範例設定檔：

```
-netdrives -@:objects2scan.txt -ra:scan.log
```

更新應用程式

指令語法：

`kav update <更新來源> <報告參數> <進階參數>`

參數敘述

`<update source>` – 從其下載更新的 HTTP 伺服器或網路或本機資料夾。如果未選擇路徑，則將從應用程式更新設定中取得更新來源。

`<report parameters>` – 這些參數定義掃描結果報告的格式。您可以指定報告檔案的絕對或相對路徑。如果不定義該參數，則顯示回溯結果和所有事件。

有以下可能的值：

- `-r: <report file>` – 僅將重要事件記錄到指定的報告檔案中。
- `-ra: <report file>` – 將所有事件記錄到指定的報告檔案中。

`<advanced parameters>` – 定義設定檔使用的參數。

`-c: <configuration file>` – 定義包含用於更新應用程式的應用程式設定的設定檔的路徑。您可以指定檔案的絕對或相對路徑。如果未定義此參數，則使用應用程式介面中設定的值。

範例:
從預設來源更新應用程式資料庫，將所有事件記錄在報告中：

```
kav update -ra:avbases_upd.txt
```

使用 updateapp.ini 設定檔的參數更新 Kaspersky Endpoint Security 模組：

```
kav update -app=on -c:updateapp.ini
```

回溯最近更新

指令語法：

`kav rollback <報告參數>`

重要提示：執行此命令需要管理員權限。

參數敘述

`<report parameters>` – 此參數定義包含更新回溯結果的報告的格式。您可以指定報告檔案的絕對或相對路徑。如果不定義該參數，則顯示回溯結果和所有事件。

有以下可能的值：

- `-r: <report file>` – 僅將重要事件記錄到指定的報告檔案中。
- `-ra: <report file>` – 將所有事件記錄到指定的報告檔案中。

範例:

```
kav rollback -ra:rollback.txt
```

啟動/停止元件或工作

啟動指令語法：

`kav start <工作或元件名稱> <報告參數>`

停止指令語法：

`kav stop <工作或元件名稱>`

重要提示：執行停止命令需要管理員權限。

參數敘述

`<task or component name>` – 指定下列值之一：

- `fm`或`file_monitoring` – 檔案威脅防護
- `wm`或`web_monitoring` – Web 威脅防護
- `mail_monitoring` – 郵件威脅防護
- `ids` – 網路威脅防護
- `firewall` – 防火牆
- `behaviordetection` – 行為偵測
- `exploitprevention` – 弱點利用防禦
- `remediationengine` – 修復引擎
- `devicecontrol` – 裝置控制
- `webcontrol` – Web 控制
- `full`或`scan_my_computer` – 完整掃描工作
- `scan_objects` – 自訂掃描工作
- `quick`或`scan_critical_areas` – 快速掃描工作
- `externalstoragesscanner` – 卸除式磁碟掃描工作
- `updater` – 更新工作
- `rollback` – 回溯工作
- `diskencryption` – FileVault 磁碟加密
- `edroptimum` – Endpoint Detection and Response Optimum
- `edrkata` — Endpoint Detection and Response Expert（內部部署）

- `cloudsandbox` – Cloud Sandbox
- `mdr` – Managed Detection and Response

`<report parameters>` – 這些參數定義元件或工作結果的報告格式。您可以指定報告檔案的絕對或相對路徑。如果未定義此參數，Kaspersky Endpoint Security 將根據圖形使用者介面中配置的參數顯示結果。

注意： <報告參數>僅適用於`scan_objects`、`updater`和`rollback`值。

有以下可能的值：

- `-r: <report file>` – 僅將重要事件記錄到指定的報告檔案中。
- `-ra: <report file>` – 將所有事件記錄到指定的報告檔案中。

注意：從命令提示啟動的元件和工作使用圖形使用者介面中配置的參數來執行。

範例:
若要啟用檔案威脅防護元件，請在命令列中輸入以下命令：

```
kav start fm
```

若要從命令列停止完整掃描工作，請輸入以下命令：

```
kav stop scan_my_computer
```

檢視元件或工作的狀態和統計訊息

狀態指令語法：

```
kav status <工作或元件名稱>
```

統計指令語法：

```
kav statistics <工作或元件名稱>
```

參數敘述

`<task or component name>` – 指定下列值之一：

- `fm`或`file_monitoring` – 檔案威脅防護
- `wm`或`web_monitoring` – Web 威脅防護
- `mail_monitoring` – 郵件威脅防護
- `ids` – 網路威脅防護
- `firewall` – 防火牆

- `behaviordetection` – 行為偵測
- `exploitprevention` – 弱點利用防禦
- `remediationengine` – 修復引擎
- `devicecontrol` – 裝置控制
- `webcontrol` – Web 控制
- `full`或`scan_my_computer` – 完整掃描工作
- `scan_objects` – 自訂掃描工作
- `quick`或`scan_critical_areas` – 快速掃描工作
- `externalstoragesscanner` – 卸除式磁碟掃描工作
- `updater` – 更新工作
- `rollback` – 回溯工作
- `diskencryption` – FileVault 磁碟加密
- `edroptimum` – Endpoint Detection and Response Optimum
- `edrkata` — Endpoint Detection and Response Expert（內部部署）
- `cloudsandbox` – Cloud Sandbox
- `mdr` – Managed Detection and Response

注意：如果執行 status 指令時未指定<工作或元件名稱>參數的值，則會顯示應用程式的所有工作和元件的狀態。對於統計指令，必須為<工作或元件名稱>參數指定一個值。

匯出防護設定

指令語法：

```
kav export <工作或元件名稱> <匯出檔案>
```

參數敘述

`<task or component name>` – 指定下列值之一：

- `fm`或`file_monitoring` – 檔案威脅防護
- `wm`或`web_monitoring` – Web 威脅防護

- `mail_monitoring` – 郵件威脅防護
- `ids` – 網路威脅防護
- `firewall` – 防火牆
- `behaviordetection` – 行為偵測
- `exploitprevention` – 弱點利用防禦
- `remediationengine` – 修復引擎
- `devicecontrol` – 裝置控制
- `webcontrol` – Web 控制
- `full`或`scan_my_computer` – 完整掃描工作
- `scan_objects` – 自訂掃描工作
- `quick`或`scan_critical_areas` – 快速掃描工作
- `externalstoragesscanner` – 卸除式磁碟掃描工作
- `updater` – 更新工作
- `rollback` – 回溯工作
- `diskencryption` – FileVault 磁碟加密
- `edroptimum` – Endpoint Detection and Response Optimum
- `edrkata` — Endpoint Detection and Response Expert（內部部署）
- `cloudsandbox` – Cloud Sandbox
- `mdr` – Managed Detection and Response

`<export file>` – 應用程式設定匯出到的檔案的路徑。您可以指定檔案的絕對或相對路徑。

```
範例:
kav export fm fm_settings.txt
```

啟動應用程式

您可以透過套用金鑰檔案來啟動 Kaspersky Endpoint Security。

指令語法：

```
kav license /add <金鑰檔案或金鑰啟動碼>
```

參數敘述

`<key file>` – 副檔名為 .key 的應用程式金鑰檔案。

`<key activation code>` – XXXX-XXXX-XXXX-XXXX 格式的啟動碼。

範例:

```
kav license /add ./1AA111A1.key
kav license /add A11A1-11111-1A1AA-1A11A
```

安裝系統延伸程式

指令語法：

```
kav activatesystemextension /sysext
```

注意：您需要在**隱私權與安全性**設定中授予 Kaspersky Endpoint Security 權限才能完成延伸功能的安裝。

設定網路連線

您可以為 Web 威脅防護和網路威脅防護元件設定網路連線。

指令語法：

```
kav activatesystemextension /webav
```

注意：您需要授予 Kaspersky Endpoint Security 網路內容過濾權限才能完成設定。

刪除產品授權金鑰

您可以刪除目前新增至應用程式的所有產品授權金鑰。

指令語法：

```
kav license /del
```

重要提示：執行此命令需要管理員權限。

命令列返回碼

命令列中的任何命令都可以傳回一般代碼。回傳代碼包括一般代碼以及特定於某個工作的代碼。

接收回傳碼的指令語法：

```
echo $?
```

一般返回碼：

- `0` – 操作成功完成
- `1` – 參數值無效
- `2` – 未知錯誤
- `3` – 工作完成錯誤
- `4` – 工作取消

惡意軟體掃描工作回傳碼：

- `101` – 所有惡意物件均已處理
- `102` – 偵測到惡意物件

結束應用程式

指令語法：

```
kav exit
```

重要提示：執行此命令需要管理員權限。

移除應用程式

使用下列命令序列從命令列解除安裝 Kaspersky Endpoint Security：

```
sudo /Library/Application\ Support/Kaspersky\ Lab/klnagent/Binaries/UninstallScript
sudo /Library/Application\ Support/Kaspersky\ Lab/KAV/Binaries/UninstallScript
```

```
sudo rm -rf /Library/Application\ Support/Kaspersky\ Lab/ /Applications/Kaspersky
```

重要提示：解除安裝該應用程式需要管理員權限。

Detection and Response 管理指令

您可以使用命令列來管理 Detection and Response 解決方案的內建功能。如果無法使用卡巴斯基安全管理中心主控台進行管理，您可以管理 Detection and Response 解決方案。

管理執行防禦

您可以檢視用戶端電腦的執行防禦設定並停用用戶端電腦上的執行防禦。

指令語法：

```
kav prevention </disable | /show>
```

命令說明

`/disable` - 用於關閉用戶端電腦上的執行防禦的命令。

`/show` - 顯示目前執行防禦設定的指令，包括模式和執行防禦規則清單。

管理網路隔離

您可以檢視主機的網路隔離設定並停用主機上的網路隔離。

指令語法：

```
kav isolation </off | /status>
```

命令說明

`/off` - 關閉網路隔離的命令。

重要提示：執行此命令需要管理員權限。

`/status` - 用於顯示網路隔離狀態和排除項目的命令。

> **注意：**這些命令必須同時執行。

聯絡技術支援服務

本部分說明如何獲得技術支援和可用條款。

如何獲得技術支援

如果您在 Kaspersky Endpoint Security 檔案或任何有關 Kaspersky Endpoint Security 的資訊來源中找不到問題的解決方案，請聯絡卡巴斯基技術支援。技術支援專業人員會為您解答關於安裝和使用 Kaspersky Endpoint Security 的所有問題。

注意：卡巴斯基在 Kaspersky Endpoint Security 的生命週期內提供支援（請參閱應用程式支援生命週期頁面）。在聯絡技術支援之前，請閱讀支援規則。

您可以使用下列方式之一與技術支援聯絡：

- 透過造訪技術支援網站
- 透過 Kaspersky CompanyAccount 入口網站向卡巴斯基技術支援傳送請求

透過 Kaspersky CompanyAccount 提供技術支援

Kaspersky CompanyAccount 是使用卡巴斯基應用程式的公司的入口網站。Kaspersky CompanyAccount 入口網站旨在透過線上請求促進用戶和卡巴斯基專家之間的互動。您可以使用 Kaspersky CompanyAccount 來追蹤線上請求的狀態並儲存它們的歷史記錄。

您可以在 Kaspersky CompanyAccount 上的單一帳戶下註冊組織的所有員工。單一帳戶可讓您集中管理註冊員工向卡巴斯基發出的電子請求，並透過 Kaspersky CompanyAccount 管理這些員工的權限。

Kaspersky CompanyAccount 入口網站提供以下語言版本：

- 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

要了解有關 Kaspersky CompanyAccount 的更多資訊，請造訪技術支援網站。

獲取技術支援資訊

為了更有效地支援和解決應用程式問題，技術支援專業人員可能會要求您臨時變更應用程式設定，以便在診斷期間進行偵錯。這可能需要執行以下操作：

- 啟動用於提取延伸診斷資訊的功能。
- 微調單個應用程式元件的設定，這些設定無法透過標準使用者介面元素獲得。
- 變更提取的診斷資訊的傳輸設定。

技術支援專業人員將為您提供執行所列操作所需的所有資訊，並告知您出於偵錯目的而需要獲取的資料範圍。延伸診斷資訊被提取後，被儲存在使用者電腦上。資料不會被自動傳送到卡巴斯基。

使用偵錯檔案

向卡巴斯基技術支援專業人員報告問題後，他們可能要求您生成包含 Kaspersky Endpoint Security 執行情況的資訊的報告，並將報告傳送給卡巴斯基技術支援。另外，卡巴斯基技術支援專業人員還可能要求您建立*偵錯檔案*。透過偵錯檔案，可以逐步檢查應用程式命令的執行情況，並確定何時发生錯誤。

建立偵錯檔案

偵錯是記錄有關應用程式活動的詳細資訊的有效方式。技術支援專業人員使用偵錯檔案來排查問題。

建立偵錯檔案

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。
   此時會開啟應用程式設定視窗。
2. 在**介面**標籤的**偵錯**部分，選中**啟用偵錯**核取方塊。

重要：建議僅在卡巴斯基技術支援專業人員的要求下啟用偵錯。

偵錯檔案可能需要大量的磁碟空間。當您不再需要偵錯檔案時，請停用偵錯。

停用偵錯

1. 在功能表列中，點擊應用程式圖示，並選擇**設定**。

   此時會開啟應用程式設定視窗。

2. 在**介面**標籤的**偵錯**部分，取消選中**啟用偵錯**核取方塊。

Kaspersky Endpoint Security 將以下資訊儲存在偵錯檔案中：

- 有關裝置和作業系統的資訊（唯一的裝置 ID、裝置類型、網路裝置的 MAC 位址、作業系統類型、作業系統版本）。
- 有關應用程式及其模組的操作的資訊。
- 有關訂購（訂購類型、區域）的資訊。
- 有關語言區域設定、應用程式 ID、應用程式自訂、應用程式版本、唯一的應用程式安裝 ID、唯一電腦 ID 的資訊。
- 有關電腦惡意軟體防護狀態，以及所有已處理和已偵測到的物件的資訊（包含已偵測到的物件名稱、偵測的日期和時間、物件的下載網址、已感染檔案的名稱和大小及其路徑、攻擊電腦的 IP 位址和網路攻擊的目標電腦埠號、惡意軟體活動清單和不需要的網址），以及應用程式和使用者所做相關操作和決定的資訊。
- 有關使用者下載的應用程式的資訊（網址、內容、檔案大小、下載檔案的處理程序的相關資訊）。
- 有關啟動的應用程式及應用程式模組的資訊（大小、內容、建立日期、PE 標頭詳細資訊、區域、名稱、位置、封裝應用程式）。
- 有關介面錯誤和已安裝卡巴斯基的應用程式介面用法的資訊。
- 有關網路連線的資訊：遠端電腦和使用者電腦的 IP 位址、用於建立連線的埠號和連線的網路協定。
- 有關電腦透過 IT 與電信網路接收和傳送的網路封包的資訊。
- 有關傳送和接收的電子郵件和即時訊息的資訊。
- 有關存取的網址的資訊：使用開放式協定建立連線的時間、有關網站存取登入名稱和密碼的資料以及 Cookie 內容。
- 伺服器的公開憑證。

偵錯檔案只包含修復應用程式中的缺陷所需的資訊。卡巴斯基使用偵錯檔案調查與 Kaspersky Endpoint Security 操作中的錯誤相關的事件。

預設情況下，停用偵錯檔案的建立。您可以在應用程式設定中啟用偵錯檔案的建立。

偵錯檔案只能手動傳送到卡巴斯基。應用程式不會自動向卡巴斯基傳送偵錯檔案。

您可以選擇如何將偵錯檔案傳送到卡巴斯基。

在向卡巴斯基傳送偵錯檔案之前，請檢視它們包含的資料。

重要：偵錯檔案可能包含個人資訊或機密資訊。透過向卡巴斯基傳送偵錯檔案，您同意向卡巴斯基提供您傳送的偵錯檔案中包含的所有資料，並且您同意用於傳送它們的方法。

有關應用程式的資訊來源

本節介紹有關該應用程式的資訊來源。

您可以根據手邊問題的重要性和緊迫性選擇最方便的資訊源。

卡巴斯基網站上的 Kaspersky Endpoint Security 頁面

在 卡巴斯基網站的 Kaspersky Endpoint Security 網頁 上，您可以檢視有關應用程式、其功能和特性的一般資訊。

Kaspersky Endpoint Security 頁面包含線上商店的連接。您可以在那裡購買或續約應用程式。

知識庫中的 Kaspersky Endpoint Security 頁面

*知識庫*是卡巴斯基技術支援網站上的一部分。

知識庫中的 Kaspersky Endpoint Security 頁面 內提供的文章可以提供有用的資訊、建議和有關如何購買、安裝和使用應用程式的一般問題回答的資訊。

知識庫中的文章會提供 Kaspersky Endpoint Security 和其他 Kaspersky 應用程式的相關問題的答案。知識庫中的文章也包含來自卡巴斯基技術支援的新聞。

從“說明”下拉式功能表進入知識庫

1. 選擇**說明** → **支援**。
2. 點擊**技術支援**。

在我們的論壇上討論卡巴斯基應用程式

如果您的問題無需立即答覆，您可以在我們的論壇 與卡巴斯基專家和其他使用者一起進行討論。

在此論壇中，您可以檢視討論主題、發表評論並建立新的討論主題。

從“說明”下拉式功能表進入論壇

1. 選擇**說明** → **支援**。
2. 點擊論壇 **社區**。

附錄

本節提供補充文件文字的資訊。

已知問題和限制

Kaspersky Endpoint Security 有以下已知問題和限制：

- 如果您電腦上安裝的某個應用程式收集資訊並將其傳送以供處理，則 Kaspersky Endpoint Security 應用程式可能會將其歸類為惡意軟體。若要避免這種情況，您可以按照文件中所述透過配置 Kaspersky Endpoint Security 應用程式從掃描中排除此應用程式。
- 可透過編輯設定檔修改應用程式功能設定。
- 在卡巴斯基安全管理中心中，本機工作可能會在受管理裝置的屬性中列出兩次。
- 變更本機更新工作的更新來源會停用更新工作的自動執行。
- 如果您透過管理主控台啟動電腦重新啟動工作，並向使用者傳送包含分號 (;) 的訊息，則該工作將顯示為已完成，但使用者不會被提示重新啟動其 Mac。
- 若要從 Kaspersky Endpoint Security 掃描中排除 Safari 網路流量，您需要將下列路徑新增至排除清單：
  - `/System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.N`
  - `/System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.N`
  - `/System/Library/PrivateFrameworks/SafariShared.framework/Versions/A/XPCServices/com.a`
  - `/System/Library/Frameworks/webkit2.framework/versions/a/xpcservices/com.apple.webkit`
- 若要從 Kaspersky Endpoint Security 掃描中排除 Google Chrome 網路流量，您需要將下列路徑新增至排除清單：
  - `/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/<VersionNumber>/Helpers/Google Chrome Helper.app/Contents/MacOS/Google Chrome Helper`
- 使用卡巴斯基安全管理中心網頁主控台和雲端主控台為 Kaspersky Endpoint Security 政策建立政策設定檔後，您需要檢查這些設定是否正確套用在用戶端電腦上。
- 當在政策設定中啟用 FileVault 磁碟加密時，具有管理員權限的使用者可以從系統設定（系統偏好設定）解密其 Mac 的啟動磁碟。
- 代理伺服器選項中的變更僅在 Kaspersky Endpoint Security 重新啟動後才會被套用。
- Safari 可能無法連線到具有不受信任憑證的網站。您可以將此類網站新增至排除項目或使用其他瀏覽器。
- 透過卡巴斯基安全管理中心遠端解除安裝 Kaspersky Endpoint Security 11.2 或更高版本後，應用程式的系統延伸功能之一可能會保留在電腦記憶體中。此後，在極少數情況下，安裝 Kaspersky Endpoint Security 時可能會出現完整磁碟存取權限問題。在這種情況下，我們建議您在本機解除安裝該應用程式並重新安裝。

- 如果 Kaspersky Endpoint Security 正在執行，則可能無法安裝需要 Rosetta 的應用程式。若要解決該問題，請結束 Kaspersky Endpoint Security 並嘗試重新安裝該應用程式。
- 在複合物件中偵測到的威脅的警報詳細資訊僅包含有關偵測到的物件本身的資訊，而不包含威脅發展鏈的圖表。
- 儲存密碼以進行密碼防護時，可能會發生錯誤。在這種情況下，我們建議解除安裝並重新安裝應用程式。
- Kaspersky Endpoint Security 不會掃描位於 OneDrive 或 iCloud 儲存或其他雲端儲存中的檔案。請將這些檔案從掃描範圍中排除。否則，掃描工作可能會以*受感染檔案未刪除*錯誤結束。
- 您無法掃描因為"移動檔案到隔離區"工作而被隔離的物件。
- 在卡巴斯基安全管理中心中，只有當 NetBIOS 名稱、電腦名稱和主機名稱相同時，裝置名稱才會正確顯示。

已修正問題

下表列出了在之前版本的 Kaspersky Endpoint Security 中发现的所有问题，并在当前版本中已修复。

版本 12.2.1 中修复的问题列表

問題 ID	問題描述
10054891	無法在網頁主控台的 Kaspersky Endpoint Security for Mac 政策中將應用程式新增至信任區域。

按副檔名掃描的物件清單

如果在卡巴斯基安全管理中心中建立掃描工作時，您在掃描設定中選擇了**按延伸程式掃描應用程式和文件**選項，Kaspersky Endpoint Security 將對不含副檔名的物件和具有以下副檔名的物件執行惡意軟體掃描：

一般格式：

- txt
- csv
- htm
- html

多媒體（音訊/視訊）檔案：

- flv
- f4v
- avi
- 3gp
- 3g2
- 3gp2
- 3p2
- divx
- mp4
- mkv
- mov
- qt
- asf
- wmv
- rm
- rmvb
- vob
- dat
- mpg
- mpeg
- bik
- fcs
- mp3
- mpeg3
- flac
- ape

- ogg
- aac
- m4a
- wma
- ac3
- wav
- mka
- rm
- ra
- ravb
- mid
- midi
- cda

影像檔案：

- jpg
- jpe
- jpeg
- jff
- gif
- png
- bmp
- tif
- tiff
- emf
- wmf
- eps

- psd
- cdr
- swf

可執行檔和系統檔案：

- exe
- dll
- scr
- ocx
- com
- sys
- class
- o
- so
- elf
- prx
- vb
- vbs
- js
- bat
- cmd
- msi
- deb
- rpm
- sh
- pl
- dylib

文件和範本：

- doc
- dot
- docx
- dotx
- docm
- dotm
- xsl
- xls
- xlsx
- xltx
- xlsm
- xltm
- xlam
- xlsb
- ppt
- pot
- pps
- pptx
- potx
- pptm
- potm
- ppsx
- ppsm
- rtf
- pdf
- msg

- eml
- vsd
- vss
- vst
- vdx
- vsx
- vtx
- xps
- oxps
- one
- onepkg
- xsn
- odt
- ods
- odp
- sxw
- pub
- mdb
- accdb
- accde
- accdr
- accdc
- chm
- mht

壓縮檔案：

- zip
- 7z*
- 7-z
- rar
- iso
- cab
- jar
- bz
- bz2
- tbz
- tbz2
- gz
- tgz
- arj
- dmg
- smi
- img
- xar

請注意：檔案的實際格式可能不比對其檔案名副檔名。

檔案和資料夾路徑中的遮罩

*檔案名稱遮罩或資料夾名稱遮罩*使用通用符號表示檔案的名稱和副檔名或資料夾的名稱。

當您指定防護範圍、掃描範圍和信任區域時，可以使用這些符號：

- 波形符號 `~` 可取代檔案或資料夾路徑中的 `/Users/<使用者名稱>`。例如，路徑`~/Desktop`表示防護範圍包括您要防護的電腦上所有使用者的桌面資料夾。
- 星號 `*` 可取代檔案或資料夾名稱中的任何字元集合，但`\`和`/`字元（它們在檔案和資料夾的路徑中分隔檔案和資料夾的名稱）除外。例如，遮罩“`/*/*.db*`”將包括位於內部磁碟上但是不在子資料夾中所有以 `db` 開始的副檔名的檔案的路徑。
- 兩個連續星號 `**` 在檔案或資料夾名稱中代表任意一組字元（包括空集），包括 `\` 和 `/` 字元（它們可分割檔案和資料夾路徑中的檔案和資料夾名稱）。例如，遮罩`/Folder/**/*.txt`將包括位於名為 `Folder` 的資料夾及其子資料夾中所有帶 `TXT` 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩`/**/*.txt`不是有效遮罩。
- 問號 `?` 可取代檔案或資料夾名稱中的任何單一字元，但 `\` 和 `/` 字元（它們在檔案和資料夾的路徑中分隔檔案和資料夾的名稱）除外。例如，遮罩`/Folder/???.txt`將包括位於 `Folder` 資料夾中所有帶 `TXT` 副檔名且名稱由三個字元構成的檔案的路徑。

IOC 檔案要求

當建立 IOC 掃描工作時，請考量以下 IOC 檔案要求和限制：

- 應用程式在用於描述洩露指示器的開放標準 OpenIOC 版本 1.0 和 1.1 或者 STIX 版本 2.0 和 2.1中支援具有 IOC 和 JSON 延伸程式的 IOC 檔案。
- 如果用命令行建立 IOC 掃描工作時上傳 IOC 檔案而其中一些不受支援，當執行工作時，應用程式將僅使用受支援的 IOC 檔案。如果用命令行建立 IOC 掃描工作時您上傳的所有 IOC 檔案不受支援，工作仍然可以被執行，但是將不會偵測任何洩露指示器。無法使用網頁主控台或雲端主控台上傳不受支援的 IOC 檔案。
- 語義錯誤和不受支援的 IOC 字詞以及 IOC 檔案中的標籤不會引起工作執行失敗。在 IOC 檔案的此類區域中，應用程式會偵測到不符合。
- 在單個 IOC 掃描工作中使用的所有 IOC 檔案的識別碼必須為唯一。如果有識別碼一樣的 IOC 檔案，它可能會影響工作執行結果。
- 單個 IOC 檔案的大小不得超過 2 MB。使用更大的檔案將引起 IOC 掃描工作以錯誤終止。新增至 IOC 集合的所有檔案的總大小不得超過 10 MB。如果所有檔案的總大小超過10 MB，則需要拆分IOC 集合並建立多個 IOC 掃描工作。
- 建議為每個威脅建立一個 IOC 檔案。這會讓分析 IOC 掃描工作的結果更容易。

應用程式對 IOC 檔案支援的功能和限制顯示在下表中。

IOC 文件支援的功能和限制。

受支援條件	OpenIOC 1.0:
	
	`is`
	`isnot`（作為集合中的例外）
	`contains`
	`containsnot`（作為集合中的例外）
	OpenIOC 1.1:
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`
	STIX 2.0 和 2.1：
	
	`=`
	`!=`
	`>`
	`<`
	`=>`
	`<=`
	`in`
	`like`
	`matches`

受支援條件屬性	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

受支援運算子	`AND` `OR`
受支援資料類型	`"date"`:日期（適用條件：`is`、`greater-than`、`less-than`） `"int"`:整數（適用條件：`is`、`greater-than`、`less-than`） `"string"`: 字串（適用條件：`is`、`contains`、`matches`、`starts-with`、`ends-with`） `"duration"`:以秒為單位的持續時間（適用條件：`is`、`greater-than`、`less-than`）

資料類型解譯的功能	`"boolean string"`、`"restricted string"`、`"md5"`、`"IP"`、`"sha256"`、`"base64Binary"` 資料類型被解譯為字串。
	
	當 `int` 和 `date` 資料類型的"內容"設定以間隔的形式設定時，應用程式支援其解譯：
	
	OpenIOC 1.0:
	使用"內容"欄位中的"`TO`"運算子：
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1:
	使用"`greater-than`"和"`less-than`"條件
	使用"內容"欄位中的"`TO`"運算子
	如果指示器設定格式為 `ISO 8601`, `Zulu Time Zone`, `UTC`，則應用程式支援"`date`"和"`duration`"資料類型的解譯。

受支援的執行防禦的指令碼解釋器

執行防禦支援以下指令碼解譯器：

- PkgUtil
- PkgInstaller

- /usr/bin/osascript
- /usr/bin/osacompile
- /usr/local/bin/python
- /usr/local/bin/python3
- /usr/bin/perl
- /usr/bin/ruby
- /bin/bash
- /bin/zsh
- /bin/sh
- /bin/dash
- /bin/csh
- /bin/ksh
- /bin/tcsh

重要提示：如果執行防禦規則中指定的指令碼由已啟動的 PkgUtil 或 PkgInstaller 指令碼解釋器開啟，則該指令碼的執行不會被封鎖。

如何將 Kaspersky Endpoint Security 憑證新增至 Mozilla Firefox 憑證儲存

如果瀏覽器使用 Mozilla Firefox 憑證儲存，您需要手動匯出卡巴斯基憑證並將其新增至該憑證儲存。否則瀏覽器將無法開啟 HTTPS 頁面。

匯出卡巴斯基憑證

1. 在 Mac 上開啟**啟動板>其他>keychain 存取**。
2. 在視窗的左側窗格中，點擊**系統**並開啟**憑證**標籤。
3. 在憑證清單中，找到**Kaspersky Web Anti-Virus Certification Authority**。
4. 右鍵點選該憑證並選擇**匯出"Kaspersky Web Anti-Virus Certification Authority"**。
5. 選擇儲存憑證的位置，然後點擊**儲存**。

   卡巴斯基憑證已儲存。

將卡巴斯基憑證新增至 Mozilla Firefox 憑證儲存

1. 開啟 Mozilla Firefox
2. 在右上角，點擊功能表按鈕並選擇**設定**。
3. 在視窗的左窗格中，選擇**隱私權和安全性**。
4. 向下捲動到**憑證**部分。
5. 點擊**檢視憑證**。
6. 在開啟的視窗中，點擊**匯入**。
7. 選擇卡巴斯基憑證檔案並點擊**開啟**。
8. 選擇**信任此 CA 來識別網站**和**信任此 CA 來識別電子郵件使用者**核取方塊。點擊**OK**。

   卡巴斯基憑證已匯入 Mozilla Firefox 憑證儲存中。它顯示在**憑證管理器**視窗的憑證清單中。

重要提示：每次重新安裝 Kaspersky Endpoint Security 應用程式時，都會產生新的 Kaspersky 根憑證。這意味著，您需要在每次重新安裝 Kaspersky Endpoint Security 應用程式後完成此過程。

與外部服務交互的網路設定

Kaspersky Endpoint Security 用以下網路設定與外部服務進行交互。

網路設定

位址	描述
`activation-v2.kaspersky.com/activationservice/activationservice.svc` 通訊協定：`HTTPS` 連接埠：`443`	啟動應用程式。

位址	描述

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`s08.upd.kaspersky.com`
`s09.upd.kaspersky.com`
`s10.upd.kaspersky.com`
`s11.upd.kaspersky.com`
`s12.upd.kaspersky.com`
`s13.upd.kaspersky.com`
`s14.upd.kaspersky.com`
`s15.upd.kaspersky.com`
`s16.upd.kaspersky.com`
`s17.upd.kaspersky.com`
`s18.upd.kaspersky.com`
`s19.upd.kaspersky.com`
`cm.k.kaspersky-labs.com`
通訊協定：`HTTPS`
連接埠：`443`
	更新資料庫和應用程式軟體模組。

`downloads.upd.kaspersky.com` 通訊協定：`HTTPS` 連接埠：`443`	• 更新資料庫和應用程式軟體模組。 • 驗證對卡巴斯基伺服器的存取。如果無法使用系統 DNS 存取伺服器，則應用程式將使用公用 DNS。為了確保更新病毒資料庫和維持電腦的安全水平，這很有必要。Kaspersky Endpoint Security 按以下順序使用下列公用 DNS 伺服器清單： 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)。 **重要資訊：**應用程式發出的請求可能包含使用者的網域位址和公用 IP 位址，因為應用程式使用 DNS 伺服器建立 TCP/UDP 連線。該資訊需要用來（例如）在使用 HTTPS 時驗證網頁資源的憑證。如果 Kaspersky Endpoint Security 使用的是公共 DNS 伺服器，則資料處理受相關服務的隱私權政策約束。 **如何阻止 Kaspersky Endpoint Security 使用公共 DNS 伺服器** 1. 結束使用者裝置上的 Kaspersky Endpoint Security 應用程式。 2. 在位於 `/Library/Application Support/Kaspersky Lab/KAV/Binaries/config.xml` 的 Kaspersky Endpoint Security 應用程式的設定檔中新增 `ForceUseSystemDNS` 變數，並將值設為 `1`。 3. 啟動 Kaspersky Endpoint Security 應用程式。 結果，Kaspersky Endpoint Security 應用程式將僅使用系統 DNS。

位址	描述
touch.kaspersky.com 通訊協定：HTTP	• 接收檢查憑證有效期的受信任時間（TLS 連線）。 • 當 Web 威脅防護執行時在瀏覽器中警告被拒絕的 Web 資源存取。
p00.upd.kaspersky.com p01.upd.kaspersky.com p02.upd.kaspersky.com p03.upd.kaspersky.com p04.upd.kaspersky.com p05.upd.kaspersky.com p06.upd.kaspersky.com p07.upd.kaspersky.com p08.upd.kaspersky.com p09.upd.kaspersky.com p10.upd.kaspersky.com p11.upd.kaspersky.com p12.upd.kaspersky.com p13.upd.kaspersky.com p14.upd.kaspersky.com p15.upd.kaspersky.com p16.upd.kaspersky.com p17.upd.kaspersky.com p18.upd.kaspersky.com p19.upd.kaspersky.com downloads.kaspersky-labs.com cm.k.kaspersky-labs.com 通訊協定：HTTP 連接埠：80	更新資料庫和應用程式軟體模組。
ds.kaspersky.com dc1.ksn.kaspersky-labs.com dc1-file.ksn.kaspersky-labs.com dc1-pp.ksn.kaspersky-labs.com dc1-st.ksn.kaspersky-labs.com 通訊協定：HTTPS 連接埠：443	使用卡巴斯基安全網路。
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 通訊協定：KSN 連接埠：443, 1443	使用卡巴斯基安全網路。
click.kaspersky.com redirect.kaspersky.com 通訊協定：HTTPS 連接埠：443	跟隨介面中的連接。

用於加密的設定

位址	描述

`crl.kaspersky.com`
`ocsp.kaspersky.com`
通訊協定：`HTTP`
連接埠：`80`
	公鑰基礎結構（PKI）。

有關協力廠商代碼的資訊

有關協力廠商代碼的資訊包含在應用程式安裝資料夾中的 legal_notices.txt 內。

商標聲明

註冊商標及服務標誌均為其各自所有人的財產。

ActiveSync、Active Directory、Excel, IIS、Microsoft、Outlook、Windows、Windows Installer 和 WMI 是 Microsoft 集團公司的商標。

Apple、Apple Remote Desktop、FileVault、iCloud、Keychain、Launchpad、Mac、macOS、Rosetta、Safari 和 Xcode 是 Apple Inc. 的商標。

Chrome, Gmail, Google 和 Google Chrome 是 Google LLC 的商標。

Composer 和 JAMF 是 JAMF SOFTWARE, LLC 在美國和其他國家的註冊商標或普通法商標。

Firefox、Mozilla 和 Thunderbird 是 Mozilla Foundation 在美國和其他國家的商標。

Intel 是 Intel 公司或其子公司的商標。

JavaScript 是 Oracle 和/或其附屬公司的註冊商標。

Linux 是 Linus Torvalds 在美國和其它國家地區的註冊商標。

Parallels、Parallels 標誌和 Coherence 是 Parallels International GmbH 的商標或註冊商標。

Vmware 和 VMware Fusion 是 VMware, Inc. 在美國和/或其他地區的註冊商標和/或商標。

“使用者支援”視窗

該視窗提供以下資訊：

- Kaspersky Endpoint Security 的版本
- Kaspersky Endpoint Security 目前使用的資料庫的發佈日期
- 電腦上安裝的作業系統版本

技術支援

點擊此按鈕開啟卡巴斯基技術支援知識庫，您可以在那裡找到卡巴斯基專家發佈的 Kaspersky Endpoint Security 相關文章。

社區

點擊此按鈕開啟社區，您可以在那裡和卡巴斯基專家和其他使用者討論 Kaspersky Endpoint Security。

關閉

點擊此按鈕關閉使用者支援視窗。

“憑證設定”視窗

在**一般**標籤上，您可以選擇用於在 Mozilla Firefox 瀏覽器中檢查加密 HTTPS 流量的憑證儲存：

- **System Roots keychain (建議)**
- **來自 Mozilla Firefox 瀏覽器設定的憑證儲存**

  在此情況下，您需要手動將 Kaspersky Endpoint Security 憑證新增至 Mozilla Firefox 瀏覽器的憑證儲存中。有關更多資訊，請參閱如何將 Kaspersky Endpoint Security 憑證新增至 Mozilla Firefox 憑證儲存。

在**受信任憑證**索引標籤上，您可以建立一個受信任的根憑證清單，无需通知即可連線到相應的伺服器。

預設情況下該清單為空。

+

點擊此按鈕將開啟一個對话方塊，用於新增將被視為受信任的憑證。

–

點擊該按鈕可以從受信任憑證清單中刪除選定的憑證。

憑證名稱

此列顯示受信任的根憑證的名稱。

取消

點擊此按鈕將關閉視窗而不儲存變更。

儲存

點擊此按鈕將儲存受信任根憑證的目前清單，並關閉視窗。

“驗證憑證”視窗

顯示憑證

點擊此按鈕可開啟一個系統視窗，其中包含有關憑證的資訊。

取消

點擊此按鈕關閉該視窗。

新增到受信任

點擊此按鈕將憑證新增到受信任憑證清單中。因此，您將能夠在沒有通知的情況下連線到相應的伺服器。

連線

點擊此按鈕可將您連線到伺服器。

注意：可用的按鈕可能因憑證類型而異。

“選擇憑證”視窗

可用憑證清單

選中憑證旁邊的核取方塊，以便在連線到伺服器時使用該憑證。

顯示憑證

點擊此按鈕可開啟一個系統視窗，其中包含有關憑證的資訊。

取消

點擊此按鈕關閉該視窗。

繼續

點擊此按鈕將繼續使用所選憑證連線到伺服器。

“偵測到受密碼防護的壓縮檔案”視窗

在執行檔案威脅防護或掃描工作時，如果 Kaspersky Endpoint Security 需要掃描受密碼防護的壓縮檔案，則會顯示一個通知視窗。

壓縮檔案

壓縮檔案的路徑。

密碼

用於輸入密碼的欄位。

如果輸入密碼，Kaspersky Endpoint Security 將對該壓縮檔案執行惡意軟體和其他電腦安全威脅掃描。

略過受防護的壓縮檔案

點擊此按鈕將略過該物件以及相同類型的所有物件。

略過

點擊此按鈕可略過物件。

“已偵測到的物件”對話方塊

當 Kaspersky Endpoint Security 偵測到病毒或其他電腦安全威脅時，螢幕上會出現通知視窗。

偵測到

根據卡巴斯基病毒百科全書分類的物件名稱。

詳細資訊

點擊此按鈕將開啟一個卡巴斯基病毒百科全書頁面，其中包含有關偵測到的物件的資訊。

物件

包含偵測到的物件的資料夾的路徑，或在其中偵測到物件的網址。

套用到全部

在檔案防護、Web 威脅防護或病毒掃描工作的目前工作階段期間，此核取方塊可用於啟用/停用針對相同類型的全部物件所選的操作。

預設取消選中此核取方塊。

檔案防護或 Web 威脅防護的目前工作階段是指從元件啟動到其停止執行或此應用程式關閉或重新啟動期間的時間。惡意軟體掃描工作的目前工作階段是指從惡意軟體掃描工作開始到完成之間的時間。

具有可對偵測到的物件執行的操作的按鈕會根據偵測到的物件的類型而變化。

您可以選擇以下操作之一：

- **解毒**。解毒該物件。在執行解毒之前，Kaspersky Endpoint Security 會建立檔案的備份副本，以便您需要還原原始檔案。
- **刪除**。刪除該物件。在執行刪除之前，Kaspersky Endpoint Security 會建立檔案的備份副本，以便您需要還原原始檔案。
- **不封鎖**。允許存取被視為危險 Web 流量物件的網站。
- **封鎖**。拒絕存取被視為危險 Web 流量物件的網站。
- **刪除壓縮檔案**。刪除包含已偵測到的物件的壓縮檔案。
- **略過受防護的壓縮檔案**。惡意軟體掃描期間略過受密碼防護的壓縮檔案。
- **略過**。封鎖存取該物件，但不對其執行任何操作。

“掃描”視窗

點擊此按鈕可返回到上一個 Kaspersky Endpoint Security 視窗。

點擊此按鈕可前進到下一個 Kaspersky Endpoint Security 視窗。

點擊此按鈕可刪除**掃描**視窗中所有惡意軟體掃描工作的所有記錄。

排程掃描

點擊此按鈕將會開啟一個對話方塊，您可以在其中安排完整掃描或快速掃描工作。

快速掃描

點選開始按鈕（ ）在本節中執行快速掃描工作。

完整掃描

點選開始按鈕（ ）在本節中執行完整掃描工作。

點擊此按鈕可停止所選的惡意軟體掃描工作。

如果惡意軟體掃描工作正在執行，將顯示此按鈕。

設定

點擊此按鈕將開啟 **掃描**索引標籤，您可以在其中配置掃描工作設定。

選擇

點擊此按鈕將會開啟一個對話方塊，您可以在其中選擇要掃描的檔案或資料夾。

在**檔案和資料夾**部分的下部，您可以檢視對所選檔案或資料夾執行的所有惡意軟體掃描工作的記錄。

詳細資訊

點擊此按鈕可開啟惡意軟體掃描工作報告視窗。

將指標懸停在掃描工作上時，將顯示此按鈕。

清除掃描歷史記錄

點擊此按鈕將刪除所有惡意軟體掃描工作的所有記錄。

顯示全部

點擊此按鈕可開啟**偵測到的物件**視窗，可在其中檢視所有已偵測到的物件。

注意： Kaspersky Endpoint Security 不會掃描位於 OneDrive 或 iCloud 儲存或其他雲端儲存中的檔案。請將這些檔案從掃描範圍中排除。否則，掃描工作可能會以*受感染檔案未刪除*錯誤結束。

“已偵測到的物件”視窗

偵測到的物件部分包含被應用程式偵測到的惡意物件。

解毒全部

點擊此按鈕啟動對已偵測到的所有惡意物件的解毒。

略過全部

點擊此按鈕可從**偵測到的物件**區域的惡意物件清單中刪除所有惡意物件。

•••

點擊此按鈕可開啟一個彈出功能表，可從中選擇對惡意物件執行以下操作之一：

- **解毒**。解毒該物件。在解毒之前，Kaspersky Endpoint Security 應用程式會建立檔案的備份副本，以便可以在以後還原或解毒此檔案，而不影響其完整性。
- **略過**。從偵測到的物件清單中刪除物件。

其他物件區域包含偵測到的非惡意但會被駭客利用損害您的電腦或資料的物件。

刪除全部

點擊此按鈕可從電腦中刪除所有已偵測到的物件。

略過全部

點擊此按鈕可從**其他物件**區域的偵測到的物件清單中刪除所有偵測到的物件。

•••

點擊此按鈕將會開啟一個彈出功能表，可從中選擇要對已偵測到的物件執行的以下操作之一：

- **刪除**。從電腦中刪除已偵測到的物件。
- **略過**。從偵測到的物件清單中刪除物件。

備份部分包含已偵測到的物件的備份副本。

刪除全部

點擊此按鈕可從電腦中刪除已偵測到的物件的所有備份副本。

•••

點擊此按鈕將會開啟一個彈出功能表，可從中選擇要對隔離物件執行的以下操作之一：

- **刪除備份副本**。從電腦中刪除已偵測到的物件的備份副本。
- **還原檔案**。將清單中選定檔案的備份副本還原到其原始位置，並使用與解毒或刪除之前的原始檔案相同的名稱。如果原始位置存在同名的物件（例如，在解毒前Kaspersky Endpoint Security 已建立原始檔案副本或已解毒原始檔案），將會顯示警告。您可以變更要將物件還原到的位置或者重命名物件。

產品授權視窗



點擊此按鈕可返回到上一個 Kaspersky Endpoint Security 視窗。



點擊此按鈕可前進到下一個 Kaspersky Endpoint Security 視窗。

注意：此視窗會根據 Kaspersky Endpoint Security 是否啟動以及所使用的產品授權或訂購類型而有所不同。

該視窗可能包含以下資訊：

- 產品授權或訂購狀態
- 使用中的金鑰
- 備用金鑰（如果有）
- 產品授權類型以及您可以在目前產品授權或訂購下使用該應用程式的電腦數量
- 目前產品授權或訂購下可用的應用程式功能
- 產品授權到期日期和時間
- 距離產品授權到期的天數

在該視窗中，您可以執行以下操作：

- 透過輸入啟動應啟動應用程式。
- 造訪包含如何在卡巴斯基線上商店購買產品授權資訊的網站。
- 開啟 Kaspersky Endpoint Security 供應商網站，其中包含有關訂購續約的資訊。
- 更新您的訂購狀態。

有關 Kaspersky Endpoint Security 產品授權的更多資訊，請聯絡您組織中的系統管理員。

“防護範圍”視窗

在**防護範圍**區域，您可以檢視和編輯防護範圍。

所有卸除式磁碟

此核取方塊可啟用/停用所有卸除式磁碟的即時防護。

預設選中此核取方塊。

所有內置磁碟

此核取方塊可啟用/停用所有內置磁碟的即時防護。

預設選中此核取方塊。

所有網路磁碟

此核取方塊可啟用/停用所有網路磁碟的即時防護。

預設選中此核取方塊。

+

點擊此按鈕會開啟一個清單，您可以在其中選擇項以建立防護範圍：

- **檔案和資料夾**。選擇此項目可開啟一個用於向防護範圍中新增檔案或資料夾的對話方塊。
- **所有磁碟**。選擇此項目可將電腦的所有卸除式磁碟、內置磁碟和網路磁碟新增到防護範圍。
- **所有卸除式磁碟**。選擇此項目可將電腦的所有卸除式磁碟新增到防護範圍。
- **所有內置磁碟**。選擇此項目可將電腦的所有內置磁碟新增到防護範圍。
- **所有網路磁碟**。選擇此項目可將電腦的所有網路磁碟新增到防護範圍。
- **記憶體**。選擇此項目可將電腦記憶體新增到防護範圍。
- **啟動物件**。選擇此項目可將在作業系統啟動時啟動的所有可執行檔案新增到防護範圍。掃描啟動物件可以偵測 Rootkit。

使用清單項目旁邊的核取方塊，可啟用/停用與此項目關聯的物件的即時防護。

–

點擊此按鈕可從防護範圍清單中刪除選定的項目。

預設無法刪除防護範圍清單中包含的項目。

在**最佳化**區域，您可以配置 Kaspersky Endpoint Security 是否掃描只讀系統磁碟區。

略過掃描唯讀系統磁碟區

該核取方塊可停用/啟用 Kaspersky Endpoint Security 掃描唯讀系統磁碟區。

預設選中此核取方塊。

重要：最佳化可能由于安全原因而停用。

“掃描範圍”視窗

在此視窗中，您可以檢視和編輯快速掃描工作的掃描範圍。

使用清單中的物件旁邊的核取方塊可啟用/停用該物件的掃描。

+
點擊此按鈕可開啟一個用於調整掃描範圍的清單：

- **檔案和資料夾**。選擇此項將會開啟一個對話方塊，用於向掃描範圍新增檔案或資料夾。
- **所有磁碟**。選擇此項目可將電腦的所有卸除式磁碟、內置磁碟和網路磁碟新增到掃描範圍。
- **所有外部磁碟**。選擇此項目可將電腦的所有卸除式磁碟新增到掃描範圍。
- **所有內置磁碟**。選擇此項目可將電腦的所有內置磁碟新增到掃描範圍。
- **所有網路磁碟**。選擇此項目可將電腦的所有網路磁碟新增到掃描範圍。
- **記憶體**。選擇此項目可將電腦記憶體新增到掃描範圍。
- **啟動物件**。選擇此項目可將在作業系統啟動時啟動的所有可執行檔案新增到掃描範圍。掃描啟動物件可以偵測 Rootkit。

–
點擊此按鈕可以從掃描範圍清單中刪除選定的項目。

預設無法刪除掃描範圍清單中包含的項目。

在**最佳化**區域，您可以配置 Kaspersky Endpoint Security 應用程式在執行掃描工作時是否掃描只讀系統磁碟區。

略過掃描唯讀系統磁碟區

該核取方塊可停用/啟用 Kaspersky Endpoint Security 掃描唯讀系統磁碟區。

如果選擇此核取方塊，Kaspersky Endpoint Security 將不掃描唯讀系統磁碟區。這可大大縮短掃描時間。

如果清除此核取方塊，Kaspersky Endpoint Security 將掃描唯讀系統磁碟區。

預設情況下已選擇此選擇方塊。

注意： Kaspersky Endpoint Security 不會掃描位於 OneDrive 或 iCloud 儲存或其他雲端儲存中的檔案。請將這些檔案從掃描範圍中排除。否則，掃描工作可能會以*受感染檔案未刪除*錯誤結束。

“基本”索引標籤

在**一般**部分中，您可以啟用或停用防護電腦抵禦惡意軟體和其他電腦安全威脅。

啟用防護

此核取方塊可啟用/停用即時防護以抵禦惡意軟體和其他電腦安全威脅侵害。

預設選中此核取方塊。

檢查安全連線 (HTTPS)

此核取方塊可啟用/停用 Kaspersky Endpoint Security 掃描加密連線 (HTTPS)，並在 Web 控制封鎖使用者存取危險 Web 資源時顯示通知。

預設取消選中此核取方塊。

信任區域

點擊此按鈕將開啟一個視窗，您可以在其中透過建立您信任、不希望掃描惡意軟體的物件清單來編輯受信任區域。

設定

點擊此按鈕將開啟一個視窗，您可以在其中管理受信任的根憑證清單並選擇憑證儲存以在 Mozilla Firefox 瀏覽器中檢查加密的 HTTPS 流量。

在**檔案威脅防護**部分，您可以啟用或停用檔案威脅防護，並選擇 Kaspersky Endpoint Security 在偵測到受感染檔案時執行的操作。

啟用檔案威脅防護

此核取方塊可啟用/停用檔案威脅防護。

預設選中此核取方塊。

防護範圍

點擊此按鈕可關閉一個視窗，您可在其中建立防護範圍。

自動解毒或刪除惡意物件

Kaspersky Endpoint Security 封鎖存取受感染檔案並嘗試在不請求使用者確認的情況下解毒檔案。在執行解毒之前，Kaspersky Endpoint Security 會在備份中儲存檔案的備份副本。如果解毒成功，Kaspersky Endpoint Security 會以原始檔案名稱將檔案儲存在原始位置。如果解毒失敗，Kaspersky Endpoint Security 會使受感染的檔案在其原來的位置保持封鎖狀態。有關偵測感染物件的資訊記錄在**已處理的物件**報告中。

提示動作

Kaspersky Endpoint Security 會顯示一個通知視窗，其中包含有關被懷疑感染檔案的惡意物件資訊，並提示您選擇 Kaspersky Endpoint Security 要執行的操作。可用的操作可能因物件狀態的不同而有所不同。

預設選擇此操作。

在**Web 威脅防護**部分，您可以啟用或停用 Web 威脅防護，並選擇 Kaspersky Endpoint Security 在偵測到危險的 Web 流量物件時執行的操作。

啟用Web 威脅防護

此核取方塊可啟用/停用 Web 威脅防護。

預設選中此核取方塊。

自動封鎖危險網路通訊物件

Kaspersky Endpoint Security 會鎖對對偵測到危險 Web 流量物件的網站的存取，無需請求確認。

提示動作

Kaspersky Endpoint Security 會顯示一個通知視窗，其中包含有關偵測到危險 Web 流量物件的資訊，並提示您選擇 Kaspersky Endpoint Security 要執行的操作。可用的操作可能因物件狀態的不同而有所不同。

預設選擇此操作。

在**郵件威脅防護**部分，您可以啟用或停用郵件威脅防護，並選擇 Kaspersky Endpoint Security 在偵測到受感染物件時執行的操作。

啟用郵件威脅防護

此核取方塊可啟用/停用郵件威脅防護。

預設選中此核取方塊。

自動刪除惡意物件

當 Kaspersky Endpoint Security 在電子郵件中偵測到受感染物件時，它會刪除受感染物件，並用文字"The requested file infected with <virus name> has been deleted"取代物件的內容。

自動封鎖惡意物件

當 Kaspersky Endpoint Security在電子郵件中偵測到受感染物件時，它會將電子郵件主旨替換為"Message is infected: <original subject>"，其中<original subject>是原始主旨。僅為 POP3 協定取代電子郵件訊息主旨。

在**網路威脅防護**部分，您可以啟用或停用網路威脅防護。

啟用網路威脅防護

此核取方塊可啟用/停用網路威脅防護。

預設選中此核取方塊。

設定

點擊此按鈕可開啟一個視窗，您可在其中建立受信任電腦清單或檢視和編輯被封鎖的電腦清單。



點擊此按鈕可防止沒有管理員權限的使用者變更 Kaspersky Endpoint Security 應用程式的設定。



點擊此按鈕會提示您輸入管理員憑證。輸入管理員憑證後，應用程式設定將可編輯。

"受信任應用程式"索引標籤

在**受信任應用程式**索引標籤上，您可以建立不希望 Kaspersky Endpoint Security 應用程式監控的應用程式清單。

預設情況下，受信任區域物件清單為空。

+

點擊此按鈕將開啟一個視窗，您可以在其中輸入應用程式的路徑、指定代碼簽章要求和選擇 Kaspersky Endpoint Security 不監控的活動類型。

–

點擊該按鈕可以從受信任區域中刪除選定的應用程式。

編輯

點擊此按鈕可開啟一個視窗，您可在其中編輯受信任應用程式的參數。

"新增受信任應用程式"視窗

路徑

Kaspersky Endpoint Security 不會監控其網路或檔案活動的應用程式的路徑。

注意：不能使用符號連結來指定此欄位中的路徑。

選擇

點擊此按鈕將開啟一個視窗，您可以在其中選擇 Kaspersky Endpoint Security 不會監控其活動的應用程式。在這種情況下，將自動插入**路徑**和**代碼簽章要求**欄位的值。

代碼簽章要求

Kaspersky Endpoint Security 不會監控其活動的應用程式的代碼簽章要求。

這是一個可選參數。

在**選項**部分中，您可以選擇不希望 Kaspersky Endpoint Security 應用程式監控的活動類型。

不監控檔案活動

此核取方塊可啟用/停用監控用戶端電腦上應用程式的檔案操作。

如果選取此核取方塊，Kaspersky Endpoint Security 不監控應用程式的檔案活動。

如果清除此核取方塊，Kaspersky Endpoint Security 將監控應用程式的檔案活動。

預設情況下已選擇此選擇方塊。

不監控網路活動

此核取方塊可啟用/停用對用戶端電腦上應用程式的入站和出站網際網路流量的監控。

如果選取此核取方塊，Kaspersky Endpoint Security 不監控應用程式的網路活動。

如果清除此核取方塊，Kaspersky Endpoint Security 將監控應用程式的網路活動。

預設情況下已選擇此選擇方塊。

取消

點擊此按鈕將關閉視窗而不儲存變更。

OK

點擊此按鈕將保存受信任應用程式的參數並關閉視窗。

“受信任檔案和資料夾”頁簽

在**檔案和資料夾**索引標籤上，您可以建立不希望 Kaspersky Endpoint Security 應用程式監控的檔案和資料夾清單。

預設情況下，受信任區域物件清單為空。

+

點擊此按鈕將開啟一個用於選擇檔案或資料夾的對話方塊。

–

點擊此按鈕可以從信任區域移除選中的物件。

“受信任網址”頁簽

在**網址**索引標籤上，您可以建立不希望 Kaspersky Endpoint Security 應用程式監控的網址清單。

預設情況下，受信任區域物件清單為空。

+

點擊此按鈕可新增一個用於輸入網址的欄位。

當指定網站位址時，您可以使用以下符號：

- 星號 (*) 代替任意字元集，除了 \ 和 / 字元。
- 兩個連續的星號 (**) 代替任意字元集（包括空集），包括 \ 和 / 字元。
- 問號 (？) 代替檔案或資料夾名稱中的任何單一字元，但 \ 和 / 字元除外。

–

點擊該按鈕可以從信任網域中刪除選定的網址。

“郵件威脅防護設定”視窗

跳過壓縮檔案，如果其大於 <value> MB

如果選擇此核取方塊，如果電子郵件附件壓縮檔案的大小超過指定值，郵件威脅防護將把壓縮檔案排除在掃描之外。

如果選擇此核取方塊，郵件威脅防護將掃描任何大小的電子郵件附件壓縮檔案。

預設值是 8 MB。

預設選中此核取方塊。

限制壓縮檔案的檢查時間為 <value> 秒

如果選擇此核取方塊，為掃描電子郵件附件壓縮檔案分配的時間將被限制為指定時段。

如果清除此核取方塊，為掃描壓縮檔案分配的時間將不受限制。

預設值是 5 秒。

預設選中此核取方塊。

“設定”視窗

在**受信任電腦**標籤，您可以建立受信任電腦的清單。Kaspersky Endpoint Security 應用程式不會封鎖這些電腦 IP 位址，甚至在這些電腦上偵測到危險網路活動時也是如此。

受信任電腦清單預設為空。

+

點擊此按鈕可新增一個欄位，用於輸入受信任電腦 IP 位址。

–

點擊該按鈕可以從受信任電腦清單中刪除選定的 IP 位址。

編輯

點擊此按鈕將使所選 IP 位址可編輯。

在**被封鎖的電腦**標籤，您可以檢視和編輯被封鎖的電腦清單。

偵測到來自此電腦的危險網路活動後，Kaspersky Endpoint Security 會將具有此 IP 位址的電腦封鎖一個小時。

IP 位址

此欄顯示被封鎖的電腦 IP 位址。

事件發生時間

此欄顯示在電腦上偵測到危險網路活動的日期和時間。

解除封鎖

點擊該按鈕可以從被封鎖的電腦清單中刪除選定的 IP 位址。

網路封包規則頁簽

規則名稱

網路封包規則名稱。

在**操作**部分，您可以選擇 Kaspersky Endpoint Security在偵測到網路活動時要執行的操作。

在**協定**部分，您可以指定網路規則適用的協定。

在**方向**部分，您可以指定被監控的網路活動的方向。

在**TTL**部分，您可以指定被監控的網路封包的壽命。

在**網路介面卡**部分，您可以指定網路規則適用的網路介面卡。

在**遠端位址**部分，您可以指定可以傳送和接收網路封包的遠端裝置的網路位址。

在**本機位址**部分，您可以指定可以傳送和接收網路封包的裝置的本機網路位址。

記錄事件

使用此核取方塊可啟用/停用記錄防火牆事件。

如果選擇該核取方塊，Kaspersky Endpoint Security 將在報告中記錄防火牆事件。

如果清除此核取方塊，Kaspersky Endpoint Security 將不會在報告中記錄防火牆事件。

預設取消選中此核取方塊。

網路介面卡視窗

介面卡名稱

網路介面卡名稱。

介面類型

從此下拉清單中，您可以選擇網路介面卡的介面類型。

IP 位址

IP 位址清單。

MAC 位址

MAC 位址清單。

網路介面卡視窗

名稱

此列包含網路介面卡名稱。

介面類型

此列包含網路介面卡的介面類型。

IP 位址

此列包含網路介面卡的 IP 位址。

MAC 位址

此欄顯示網路介面卡的 MAC 位址。

“本機位址”視窗

本機位址

此列包含本機位址。

“本機位址”視窗

類型

此下拉清單可讓您指定網路規則要套用的本機 IP 條目的類型。

IP 位址

IP 位址輸入欄位。此欄位僅當您在**類型**下拉清單中選擇 **IP 位址**時可以使用 。

範圍起始

IP 位址範圍起始輸入欄位。此欄位僅當您在**類型**下拉清單中選擇 **IP 位址範圍**時可以使用 。

範圍結束

IP 位址範圍結束輸入欄位。此欄位僅當您在**類型**下拉清單中選擇 **IP 位址範圍**時可以使用 。

“遠端位址”視窗

遠端位址

此列包含遠端位址。

“遠端位址”視窗

類型

此下拉清單可讓您指定網路規則要套用的遠端位址條目的類型。

位址

IP 位址或 DNS 名稱輸入欄位。此欄位僅當您在**類型**下拉清單中選擇 **IP 位址或 DNS 名稱**時可以使用 。

範圍起始

IP 位址範圍起始輸入欄位。此欄位僅當您在**類型**下拉清單中選擇 **IP 位址範圍**時可以使用 。

範圍結束

IP 位址範圍結束輸入欄位。此欄位僅當您在**類型**下拉清單中選擇 **IP 位址範圍**時可以使用 。

範本視窗

網路規則範本

此列包含網路規則範本。

網路封包規則頁簽

名稱

網路規則名稱。

操作

防火墻在偵測到網路活動種類時執行的動作。

位址

套用網路規則的網路位址。

可用網路頁簽

名稱

此列包含網路名稱。

網路狀態

此列包含網路的網路狀態。

IP 位址

此列包含網路 IP 位址。

可用網路視窗

網路名稱

網路名稱。

網路狀態

網路狀態下拉清單。

IP 位址

網路 IP 位址。

“MAC 位址”視窗

類型

此下拉清單可讓您指定網路規則要套用的 MAC 位址條目的類型。

MAC 位址

MAC 位址輸入欄位。此欄位僅當您在**類型**下拉清單中選擇 **MAC 位址**時可以使用。

遮罩

MAC 位址遮罩輸入欄位。此欄位僅在您選擇 **MAC 位址遮罩** 在 **類型** 下拉清單。

範圍起始

MAC 位址範圍起始輸入欄位。此欄位僅當您在**類型**下拉清單中選擇 **MAC 位址範圍**時可以使用 。

範圍結束

MAC 位址範圍結束輸入欄位。此欄位僅當您在**類型**下拉清單中選擇 **MAC 位址範圍**時可以使用 。

“進階”頁簽

在**KSN**區域中，您可以閱讀卡巴斯基安全網路聲明的條款並選擇是否加入卡巴斯基安全網路。

顯示 KSN 聲明

點擊此按鈕會開啟一個視窗，其中顯示卡巴斯基安全網路聲明的文字。

Kaspersky Endpoint Security 可以使用全球或私有 KSN 基礎架構。如果您加入卡巴斯基安全網絡，Kaspersky Endpoint Security 將使用從卡巴斯基安全網絡接收的有關檔案、Web 資源和應用程式的信譽資訊，並提供卡巴斯基安全網絡運行偵測服務所需的資料。

加入卡巴斯基安全網路

使用此核取方塊可啟用/停用加入卡巴斯基安全網路的選項。

加入卡巴斯基私人安全網路

此核取方塊可啟用/停用加入卡巴斯基私人安全網路。有關參與卡巴斯基私人安全網路的更多資訊，請聯絡您組織中的系統管理員。

啟用延伸 KSN 模式

此核取方塊用於啟用/停用向卡巴斯基安全網路提供其他資料。這些資料用於提高對您的電腦的防護和 Kaspersky Endpoint Security 的易用性。·您可以在卡巴斯基安全網路聲明和 Kaspersky Endpoint Security 說明中找到資料清單。

如果選取**加入卡巴斯基安全網路**核取方塊，則會自動選取此核取方塊，但您可以取消選取它。

啟用雲端模式

雲端模式 是指 Kaspersky Endpoint Security 使用輕量級版本的惡意軟體防護資料庫的應用程式執行模式。僅當啟用卡巴斯基安全網路參與時，此模式才可用。與通常的資料庫相比，輕量級版本的惡意軟體防護資料庫僅需要大約一半的電腦 RAM。如果您未參與卡巴斯基安全網路或已停用雲端模式，Kaspersky Endpoint Security 會從 Kaspersky 伺服器下載完整版本的惡意軟體防護資料庫。

如果開啟該切換按鈕，Kaspersky Endpoint Security 將使用惡意軟體防護資料庫的輕量級版本，這可以減少作業系統資源上的負載。

注意：選中該核取方塊後，Kaspersky Endpoint Security 在下次更新期間下載惡意軟體防護資料庫的輕量級版本。

如果關閉該切換按鈕，Kaspersky Endpoint Security 將使用惡意軟體防護資料庫的完全版本。

注意：選中該核取方塊後，Kaspersky Endpoint Security 在下次更新期間下載惡意軟體防護資料庫的完整版本。

在**行為偵測**區域中，您可以啟用/停用行為偵測元件，並選擇偵測到惡意軟體活動時要執行的動作。

啟用行為偵測

此核取方塊可啟用/停用行為偵測元件，該元件接收有關電腦上應用程式操作的資訊並將其提供給其他防護元件以提高其效能。

封鎖惡意軟體活動

如果選擇此選項，Kaspersky Endpoint Security 將在偵測到惡意活動時終止應用程式。

刪除偵測到的危險物件

如果選擇此選項，Kaspersky Endpoint Security 會在偵測到惡意活動時刪除惡意應用程式的可執行檔案，並在備份中建立該檔案的備份副本。

提示動作

如果選擇此選項，則當偵測到惡意軟體活動時，Kaspersky Endpoint Security 應用程式將顯示一個通知視窗，其中包含有關惡意物件的資訊，並提示使用者選擇 Kaspersky Endpoint Security 應用程式要採取的操作。可用的操作可能因物件狀態的不同而有所不同。



點擊此按鈕可防止沒有管理員權限的使用者變更 Kaspersky Endpoint Security 應用程式的設定。



點擊此按鈕會提示您輸入管理員憑證。輸入管理員憑證後，應用程式設定將可編輯。

“掃描”頁簽

惡意軟體掃描工作清單

包含預設惡意軟體掃描工作：

- **完整掃描**。電腦記憶體、啟動物件和所有內置磁碟的惡意軟體掃描。
- **快速掃描**。僅對電腦的關鍵區域執行惡意軟體掃描：記憶體、啟動物件和系統資料夾。
- **自訂掃描**。對指定物件（檔案、資料夾、內置磁碟或可拆卸磁碟）執行惡意軟體掃描。
- **外部磁碟掃描**。當電腦連線到外部磁碟時，將執行外部磁碟惡意軟體掃描。

注意： Kaspersky Endpoint Security 不會掃描位於 OneDrive 或 iCloud 儲存或其他雲端儲存中的檔案。請將這些檔案從掃描範圍中排除。否則，掃描工作可能會以*受感染檔案未刪除*錯誤結束。

在**掃描範圍**區域中，可以檢視和編輯快速掃描工作的掃描範圍。

編輯

點擊此按鈕可開啟一個視窗，您可在該視窗中檢視和編輯掃描範圍。

僅當在清單中選擇了快速掃描工作時，此按鈕才可用。

在**動作**部分中，您可以選擇 Kaspersky Endpoint Security 在偵測到受感染檔案時執行的操作，並排程工作。

自動解毒或刪除惡意物件

Kaspersky Endpoint Security 封鎖存取受感染檔案並嘗試在不請求使用者確認的情況下解毒檔案。在執行解毒之前，Kaspersky Endpoint Security 會在備份中儲存檔案的備份副本。如果解毒成功，Kaspersky Endpoint Security 會以原始檔案名稱將檔案儲存在原始位置。如果解毒失敗，Kaspersky Endpoint Security 會使受感染的檔案在其原來的位置保持封鎖狀態。有關偵測感染物件的資訊記錄在**已處理的物件**報告中。

當掃描完成時提示動作

Kaspersky Endpoint Security 會推遲處理被偵測到的已感染檔案到掃描結束。掃描完成後，Kaspersky Endpoint Security 將顯示通知視窗，通知您偵測到已感染物件並提供您進一步操作的選擇。可用的操作可能因物件狀態的不同而有所不同。

預設選擇此操作。

在**連線了外部磁碟時**標籤的**外部磁碟掃描**部分，您可以選擇當連線到外部磁碟時 Kaspersky Endpoint Security 執行的操作。

掃描

如果選擇此選項，Kaspersky Endpoint Security 將為連線的外部磁碟啟動惡意軟體掃描工作。

預設選擇此選項。

什麼都不做

如果選擇此選項，Kaspersky Endpoint Security 不會掃描已連線的外部磁碟。

在**最佳化**區域，您可以配置 Kaspersky Endpoint Security 在執行快速掃描或全盤掃描時是否掃描只讀系統磁碟區。

略過掃描唯讀系統磁碟區

該核取方塊可停用/啟用 Kaspersky Endpoint Security 掃描唯讀系統磁碟區。

該核取方塊對快速掃描工作預設選中，對完整掃描工作預設不選。

重要：最佳化可能由于安全原因而停用。

CPU 使用

點擊此按鈕將開啟一個對話方塊，您可以在其中啟用或停用限制應用程式使用受防護裝置的 CPU 來執行掃描工作。如果選擇**將掃描的 CPU 利用限制為**選項，您可以在對應欄位中指定允許的最大 CPU 使用率。

注意：這是所有 CPU 核心的累積限制。活動監控器中顯示的 CPU 使用率是每個 CPU 核心使用率的總和，因此可能會超過 100%。

啟用此選項會對 Kaspersky Endpoint Security 的效能產生負面影響。

預設情況下，此選項處於停用狀態。

排程

點擊此按鈕將會開啟一個對話方塊，您可以在其中安排完整掃描或快速掃描工作。



點擊此按鈕可防止沒有管理員權限的使用者變更 Kaspersky Endpoint Security 應用程式的設定。



點擊此按鈕會提示您輸入管理員憑證。輸入管理員憑證後，應用程式設定將可編輯。

“威脅”頁簽

您可以在**要偵測的物件**部分中設定要偵測的物件清單。

病毒、蠕蟲、木馬、惡意工具、廣告軟體和自動撥號軟體

此類別包括以下類型的程式：

- 所有類型的惡意軟體。
- 在您的電腦上顯示廣告（例如，橫幅）或使用廣告網站替換瀏覽器中的搜尋結果的應用程式。
- 透過電腦的數據機偷偷建立電話連線的應用程式。

Kaspersky Endpoint Security 始終控制此類程式。

此核取方塊始終處於選中狀態，無法取消選中。

可以被入侵者利用以破壞您的電腦或個人資料的合法軟體

使用此核取方塊可啟用/停用對合法應用程式的管理，入侵者可能會利用這些應用程式對使用者的電腦或資料造成危害（例如，遠端管理應用程式）。

預設取消選中此核取方塊。

在**備份**部分中，您可以指定物件可以在“備份”中儲存多長時間。

距離刪除備份物件還有 <value> 天

此核取方塊可啟用/停用在指定時間段後從備份中刪除物件。

如果選中此核取方塊，應用程式會在該核取方塊旁邊的數位輸入欄位中特定的期限到期後刪除備份區中的物件。如果取消選中此核取方塊，物件將無限期地儲存在備份區中。

預設選中此核取方塊，物件將在備份區中儲存 30 天。

在**排除項目**區域中，可以建立能夠信任而無需進行惡意軟體掃描的檔案、資料夾、應用程式和網站的清單。

信任區域

點擊此按鈕將開啟一個視窗，您可以在其中透過建立您信任、不希望掃描惡意軟體的物件清單來編輯受信任區域。

注意：當管理員配置政策禁止編輯信任區域時，使用者無法進入信任區域設定。



點擊此按鈕可防止沒有管理員權限的使用者變更 Kaspersky Endpoint Security 應用程式的設定。



點擊此按鈕會提示您輸入管理員憑證。輸入管理員憑證後，應用程式設定將可編輯。

“更新”頁簽

在**資料庫**部分，您可以設定 Kaspersky Endpoint Security 資料庫的更新模式。

自動下載更新

此核取方塊可啟用/停用應用程式資料庫的自動更新。

預設選中此核取方塊。

在**代理**部分，您可以設定使用代理伺服器來更新 Kaspersky Endpoint Security。

使用代理伺服器

此核取方塊可啟用/停用當更新惡意軟體防護資料庫和應用程式模組時使用代理伺服器連線到網際網路。

預設選中此核取方塊。

設定

點擊此按鈕將開啟一個視窗，您可以在其中配置 代理伺服器連線設定。

在**回溯**部分，您可以回溯到應用程式資料庫的先前版本。當新版本的應用程式資料庫包含導致 Kaspersky Endpoint Security 封鎖安全應用程式的不正確簽名時，您可能需要回溯更新。

回溯更新

點擊此按鈕將執行應用程式資料庫的回溯。



點擊此按鈕可防止沒有管理員權限的使用者變更 Kaspersky Endpoint Security 應用程式的設定。



點擊此按鈕會提示您輸入管理員憑證。輸入管理員憑證後，應用程式設定將可編輯。

“代理伺服器設定”視窗

使用系統的代理伺服器設定

Kaspersky Endpoint Security 使用在 Mac 的作業系統設定中指定的代理伺服器設定。

預設選擇此操作。

使用指定的代理伺服器設定

Kaspersky Endpoint Security 使用在此視窗中指定的代理伺服器設定。

位址

用於輸入代理伺服器的 IP 位址或網域名稱的欄位。

如果選擇**使用指定的代理伺服器設定**”選項，則此欄位可用。

連接埠

用於更新 Kaspersky Endpoint Security 的代理伺服器連接埠號的輸入欄位。

如果選擇**使用指定的代理伺服器設定**”選項，則此欄位可用。

預設值是 80。

使用代理伺服器驗證

*身分驗證*是在連線到代理伺服器時驗證使用者名稱和密碼的過程。

此核取方塊可在連線到代理伺服器時啟用/停用身分驗證。

預設取消選中此核取方塊。

使用者名稱

用於當連線到代理伺服器時輸入使用者名稱進行身分驗證的欄位。

如果選取**使用代理伺服器驗證**核取方塊，則該欄位可用。

密碼

用於當連線到代理伺服器時輸入密碼進行身分驗證的欄位。

如果選取**使用代理伺服器驗證**核取方塊，則該欄位可用。

如果您未指定使用者名稱和密碼，或者指定的使用者名稱和密碼被代理伺服器拒絕，則一個視窗將開啟，您必須在其中輸入使用者名稱和密碼以在代理伺服器上進行身分驗證。如果身分驗證成功，並且在請求視窗中選取**記住密碼**核取方塊，則您指定的使用者名稱和密碼將在以後的所有情況下套用。如果未選取使用者名稱和密碼輸入視窗中的**記住密碼**核取方塊，則下次連線代理伺服器時系統將再次提示您輸入使用者名稱和密碼。

對本機位址不使用代理伺服器

此核取方塊可啟用/停用當從本機或網路資料夾更新應用程式時對代理伺服器的使用。

預設選中此核取方塊。

“需要代理伺服器驗證”對話方塊

使用者名稱

用於輸入連線到代理伺服器的使用者名稱的欄位。

密碼

用於輸入密碼的欄位。

記住密碼

此核取方塊啟用/停用將來在代理伺服器上使用指定的使用者名稱和密碼進行身分驗證。

預設取消選中此核取方塊。

“介面”索引標籤

在**通知**部分，您可以設定 Kaspersky Endpoint Security 顯示的通知，以通知您各類別事件。

啟用通知

此核取方塊可啟用/停用有關應用程式事件的通知。

預設選中此核取方塊。

偵測到惡意軟體時開啟警報音

使用此核取方塊將啟用/停用 Kaspersky Endpoint Security 偵測到惡意物件時的提示音。

預設選中此核取方塊。

在**應用程式圖示**部分，您可以設定要在功能表列中顯示的應用程式圖示。

在功能表列中顯示

此核取方塊啟用/停用功能表列中應用程式圖示的顯示。

在**報告**部分，您可以啟用/停用在 Kaspersky Endpoint Security 報告中的非緊急事件記錄。

記錄非緊急事件

使用此核取方塊可啟用/停用在報告中記錄資訊性事件。通常，這些事件對於電腦安全性而言並不重要。

在**偵錯**區域中，可啟用或停用偵錯。

偵錯是記錄有關應用程式活動的詳細資訊的方式。卡巴斯基技術支援專業人員使用偵錯檔案來排查問題。您可以啟用應用程式事件記錄以建立偵錯檔案並將其傳送到技術支援。預設情況下，應用程式事件記錄被停用。

重要：只有在技術支援專業人員要求您開啟偵錯時才這樣做。

啟用偵錯

使用此核取方塊允許/禁止建立偵錯檔案。

預設取消選中此核取方塊。

在**密碼防護**部分，您可以啟用密碼防護以防止電腦上不需要的操作。

啟用密碼防護

此核取方塊可啟用/停用對不需要的操作的密碼防護。

預設取消選中此核取方塊。

選擇此核取方塊將開啟一個視窗，您可以在其中設定和配置管理員密碼。

設定

點擊此按鈕可開啟一個視窗，您可在此視窗中編輯管理員密碼參數。



點擊此按鈕可防止沒有管理員權限的使用者變更 Kaspersky Endpoint Security 應用程式的設定。



點擊此按鈕會提示您輸入管理員憑證。輸入管理員憑證後，應用程式設定將可編輯。

設定管理員密碼視窗

密碼

用於輸入密碼以限制裝置上不需要的操作的欄位。

確認密碼

透過再次輸入密碼來確認密碼的欄位。

選項

可以受密碼防護的操作清單。選取所需的核取方塊以防護裝置上的對應操作。您必須至少選擇一個核取方塊。

取消

點擊此按鈕將關閉視窗而不儲存變更。

OK

點擊此按鈕將儲存管理員密碼設定並關閉視窗。儲存變更後，當嘗試在裝置上執行不需要的操作時，您會被提示輸入密碼。

“系統事件”報告

視窗右窗格包含有關 Kaspersky Endpoint Security 操作的報告。

時間

此列顯示事件的日期和時間。

事件

此列顯示事件狀態。

程式名稱

此列顯示在其中發生事件的程式的名稱。

使用者

此列顯示發起此事件的使用者的名稱。

使用者類型

此列顯示發起此事件的使用者類型。



點擊此按鈕可開啟一個視窗，您可以在此視窗中將報告儲存為 TXT 檔案。

“已處理的物件”報告

視窗的右側窗格包含 Kaspersky Endpoint Security 應用程式偵測到的所有感染物件和危險 Web 流量物件的清單。

時間

此欄顯示偵測到物件的時間。

物件

此欄顯示偵測到物件的位置的路徑或物件的網址。

狀態

此欄顯示應用程式在偵測到物件後執行的操作。

已偵測

此欄根據卡巴斯基病毒百科全書中的分類顯示偵測到的物件的類型。

名稱

此欄根據卡巴斯基病毒百科全書中的分類顯示偵測到的物件的名稱。



點擊此按鈕可開啟一個視窗，您可以在此視窗中將報告儲存為 TXT 檔案。

“資料庫更新”報告

視窗的右側窗格包含應用程式執行的更新工作的報告。

啟動時間

此欄顯示每個更新工作的開始日期和時間。如果展開操作清單，此列也會列出更新應用程式時執行的操作以及執行這些操作的時間。

狀態

此欄顯示更新工作的狀態。

大小

此欄顯示所下載的更新檔案的大小。

平均速度

此欄顯示更新檔案的下載速度。

結束時間

此欄顯示更新工作的完成時間。

點擊此按鈕可展開更新工作中包含的操作的清單。

點擊此按鈕可摺疊更新工作中包含的操作的清單。



點擊此按鈕可開啟一個視窗，您可以在此視窗中將報告儲存為 TXT 檔案。

“掃描”報告

視窗的右側窗格包含 Kaspersky Endpoint Security 執行的掃描工作的報告。

工作

此列顯示掃描工作的名稱。

狀態

此列顯示掃描工作的狀態或已掃描物件的狀態。

日期

此列顯示掃描工作的日期和時間。

發起者

此列顯示發起掃描工作的使用者、應用程式或處理程序。

>

點擊此按鈕將展開掃描物件清單。

⌄

點擊此按鈕將折疊掃描物件清單。



點擊此按鈕可開啟一個視窗，您可以在此視窗中將報告儲存為 TXT 檔案。

“檔案威脅防護”報告

視窗右窗格包含有關檔案威脅防護操作的報告。

日期

此列顯示應用程式存取已掃描物件的日期和時間。

路徑

此列顯示已掃描物件的原始位置的路徑。

狀態

此列顯示掃描物件的狀態。

程式名稱

此列顯示存取已掃描物件的應用程式。



點擊此按鈕可開啟一個視窗，您可以在此視窗中將報告儲存為 TXT 檔案。

“Web 威脅防護”報告

視窗右窗格包含有關 Web 威脅防護操作的報告。

日期

此列顯示偵測到的 Web 流量物件的日期和時間。

URL

此列顯示 Web 威脅防護偵測到的 Web 流量物件。對於偵測到的每個 Web 流量物件，此欄指定偵測到此類物件的網址。

狀態

此列顯示偵測到的 Web 流量物件的狀態。

程式名稱

此列顯示存取偵測到的 Web 流量物件的程式。



點擊此按鈕可開啟一個視窗，您可以在此視窗中將報告儲存為 TXT 檔案。

“郵件威脅防護”報告

視窗右窗格包含有關郵件威脅防護操作的報告。

日期

此欄顯示在電子郵件訊息中偵測到感染物件時的日期和時間。

路徑

此列顯示有關在其中偵測到感染對象的電子郵件的資訊。

狀態

此欄顯示在偵測到感染物件後 Kaspersky Endpoint Security 執行的操作。

程式名稱

此列顯示電子郵件用戶端名稱。



點擊此按鈕可開啟一個視窗，您可以在此視窗中將報告儲存為 TXT 檔案。

“網路威脅防護”報告

視窗右窗格包含有關網路威脅防護操作的報告。

日期

此欄顯示在電腦上偵測到危險網路活動的日期和時間。

IP 位址

此欄顯示 Kaspersky Endpoint Security 偵測到存在危險的網路活動的電腦 IP 位址。

狀態

此欄顯示在偵測到危險網路活動後 Kaspersky Endpoint Security 執行的操作。

攻擊類型

此欄顯示偵測到的網路攻擊類型。

本機連接埠

此欄顯示嘗試透過其入侵的本機連接埠號。

協定

此列顯示用於執行攻擊的協定類型。



點擊此按鈕可開啟一個視窗，您可以在此視窗中將報告儲存為 TXT 檔案。

Endpoint Detection and Response 報告

視窗右窗格包含有關 Endpoint Detection and Response 元件操作的報告。

日期

此列顯示事件的日期和時間。

事件

此列顯示事件狀態。



點擊此按鈕可開啟一個視窗，您可以在此視窗中將報告儲存為 TXT 檔案。

防火牆報告

視窗右窗格包含有關防火牆操作的報告。

日期

此列顯示事件的日期和時間。

事件

此列顯示事件狀態。



點擊此按鈕可開啟一個視窗，您可以在此視窗中將報告儲存為 TXT 檔案。

弱點利用防禦報告

視窗右窗格包含有關弱點利用防禦操作的報告。

日期

此列顯示事件的日期和時間。

事件

此列顯示事件狀態。



點擊此按鈕可開啟一個視窗，您可以在此視窗中將報告儲存為 TXT 檔案。

裝置控制報告

視窗右窗格包含有關裝置控制操作的報告。

日期

此列顯示事件的日期和時間。

事件

此列顯示事件狀態。



點擊此按鈕可開啟一個視窗，您可以在此視窗中將報告儲存為 TXT 檔案。

“系統監控”報告

視窗右窗格包含有關系統監控元件操作的報告。

日期

此列顯示事件的日期和時間。

事件

此列顯示事件狀態。



點擊此按鈕可開啟一個視窗，您可以在此視窗中將報告儲存為 TXT 檔案。

“安裝類型”視窗

在**要安裝的套件**部分中，您可以選擇將安裝在用戶端電腦上的應用程式元件。

掃描

此核取方塊可將掃描元件新增至 Kaspersky Endpoint Security 安裝套件。

此核取方塊預設被選取且無法被清除。

檔案威脅防護

此核取方塊可啟用/停用將檔案威脅防護元件新增至 Kaspersky Endpoint Security 安裝套件。

如果勾選此核取方塊，檔案威脅防護元件將被包含在 Kaspersky Endpoint Security 安裝套件中。

如果清除此核取方塊，檔案威脅防護元件將不被包含在 Kaspersky Endpoint Security 安裝套件中。

預設情況下已選擇此選擇方塊。

Web 威脅防護

此核取方塊可啟用/停用將 Web 威脅防護元件新增至 Kaspersky Endpoint Security 安裝套件。

如果勾選此核取方塊，Web 威脅防護元件將被包含在 Kaspersky Endpoint Security 安裝套件中。

如果清除此核取方塊，Web 威脅防護元件將不被包含在 Kaspersky Endpoint Security 安裝套件中。

預設情況下已選擇此選擇方塊。

網路威脅防護

此核取方塊可啟用/停用將網路威脅防護元件新增至 Kaspersky Endpoint Security 安裝套件。

如果勾選此核取方塊，網路威脅防護元件將被包含在 Kaspersky Endpoint Security 安裝套件中。

如果清除此核取方塊，則網路威脅防護元件不會被包含在 Kaspersky Endpoint Security 安裝套件中。

預設情況下已選擇此選擇方塊。

網路代理連線器

此核取方塊可將網路代理連線程式元件新增至 Kaspersky Endpoint Security 安裝套件中。

此核取方塊預設被選取且無法被清除。

密碼防護設定視窗

密碼

用於輸入密碼以限制裝置上不需要的操作的欄位。
點擊**顯示**可檢視輸入的符號。

確認密碼

透過再次輸入密碼來確認密碼的欄位。
點擊**顯示**可檢視輸入的符號。

要求密碼

可以受密碼防護的操作清單。選取所需的核取方塊以防護使用者裝置上的對應操作。

“授予存取權限”對話方塊

獲取還原金鑰

點擊此按鈕會產生存取用戶端電腦上的加密磁碟所需的還原金鑰。

“進階威脅防護”部分

在**KSN 設定**部分，您可以設定卡巴斯基安全網路的使用。

卡巴斯基安全網路

卡巴斯基安全網路切換開關可啟用/停用參與卡巴斯基安全網路。

如果**卡巴斯基安全網路**切換開關開啟，套用應用程式政策的用戶端電腦將參與卡巴斯基安全網路。

如果**卡巴斯基安全網路**切換開關關閉，套用應用程式政策的用戶端電腦不會參與卡巴斯基安全網路。

此切換開關預設關閉。

延伸 KSN 模式

延伸 KSN 模式切換開關可啟用/停用從遠端電腦向卡巴斯基傳送附加資料。這些資料用於提高用戶端電腦的防護和 Kaspersky Endpoint Security 的易用性。

如果開啟**延伸 KSN 模式**，則該政策下的用戶端電腦將向卡巴斯基安全網路提供偵測服務運作所需的資料和附加資料。

如果關閉**延伸 KSN 模式**，則該政策下的用戶端電腦將僅提供偵測服務運作所需的資料。不會向卡巴斯基安全網路提供任何額外資料。

延伸 KSN 模式切換開關預設為關閉。

如果您開啟**卡巴斯基安全網路**切換開關，切換開關會自動開啟，但您也可以將其關閉。

在全球 KSN 基礎架構中使用卡巴斯基安全網路時向卡巴斯基提供的資料

如果啟用**卡巴斯基安全網路**切換開關並停用**延伸 KSN 模式**切換開關，在用戶端電腦上執行的 Kaspersky Endpoint Security 會向卡巴斯基提供以下資料：

- 所使用授權的相關資訊： 授權的類型和有效期、授權失效前的天數、向其購買授權的合作夥伴的識別碼、區域啟動中心識別碼、啟動碼的總和檢查碼、SHA1 演算法計算的票證內容雜湊、授權票證建立日期與時間、授權資訊識別碼、授權票證識別碼、授權票證順序識別碼、使用者電腦的唯一識別碼、授權票證有效開始日期、授權票證有效結束日期、授權票證目前狀態、票證標題版本、授權版本、票證標題簽章憑證識別碼、金鑰檔案的總和檢查碼、票證標題簽署者序號、身分驗證權杖。

- 所安裝軟體的完整版本；
  已安裝軟體的類型；
  軟體更新 ID； 聲譽服務的 ID； 協定類型 ID； 區域啟動中心的 ID； 已撤銷軟體服務決策清單版本； 軟體病毒資料庫中的已觸發記錄 ID； 軟體病毒資料庫中的已觸發記錄時間戳記； 觸發的軟體病毒資料庫記錄類型； 電腦上應用程式安裝實例的唯一 ID； 產品授權啟動日期； 授權失效日期； 授權識別碼； 軟體所使用授權的狀態； 目前處理中物件的總和檢查碼類型； 偵測到的惡意軟體名稱或是可能用於傷害使用者裝置或資料的合法軟體名稱； 目前處理中物件的總和檢查碼； 軟體啟動碼的總和檢查碼； 軟體的完整版本； 唯一裝置 ID； 軟體 ID； 軟體金鑰檔案的總和檢查碼； 用於提供軟體授權的資訊模型 ID； 用於簽署軟體授權票證標頭的憑證識別碼； 軟體授權票證建立日期和時間； 軟體授權票證總和檢查碼； 軟體授權票證版本； 軟體啟動碼版本； 權利持有人基礎架構請求資料格式； 啟動的產品授權票證 ID； 軟體元件 ID； 軟體動作結果； 錯誤代碼； 網路服務的已存取位址（URL、IP）； 通訊埠編號； 網路服務請求來源（推薦者）的網址； 認證的公開金鑰； 所掃描物件與雜湊演算法的數位憑證指紋。

如果啟用**卡巴斯基安全網路**和**延伸 KSN 模式**切換開關，在用戶端電腦上執行的 Kaspersky Endpoint Security 會向卡巴斯基提供以下資料：

- 作業系統版本和已安裝在電腦上的服務套件版本的相關資訊；目前和預設的作業系統語言設定；作業系統內核檔案的版本和總和檢查碼（MD5、SHA2-256、SHA1）；作業系統執行模式的參數； 作業系統版本、作業系統組建編號、作業系統更新編號、作業系統版本、作業系統版本延伸資訊； 作業系統服務包版本； 作業系統啟動的日期和時間； 行為分析子系統中關於作業系統的事件處理延遲時間； 延遲的目前類型作業系統動作事件數； 主動式防禦子系統中關於作業系統的事件處理延遲時間； 已處理的作業系統動作事件數； 已處理的同步作業系統動作事件數； 延遲的目前類型作業系統動作事件總數； 常設事件儲存子系統中關於作業系統的事件處理延遲時間； 延遲的作業系統動作事件總數； 等待中的同步作業系統動作事件數； 作業系統中一項動作收到事件的日期和時間。

- 有關上次作業系統重新啟動失敗的資訊： 重新啟動失敗的次數。

- 權利持有人之已安裝應用程式和病毒防護狀態的相關資訊： 軟體安裝 ID（PCID）； 軟體資料庫記錄版本； 電腦上應用程式安裝實例的唯一識別碼、應用程式類型、應用程式類型 ID、所安裝的應用程式的完整版本、應用程式設定版本的識別碼、電腦類型的識別碼、已安裝應用程式的電腦的唯一識別碼、權利持有人服務中的唯一使用者識別碼、本機語言和操作狀態、所安裝軟體元件的版本及其操作狀態、用於連線權利持有人服務的協定版本； 所安裝軟體的完整版本； 已安裝軟體的類型； 軟體更新 ID； 聲譽服務的 ID； 協定類型 ID； 區域啟動中心的 ID； 已撤銷軟體服務決策清單版本； 軟體病毒資料庫中的已觸發記錄 ID； 軟體病毒資料庫中的已觸發記錄時間戳記； 觸發的軟體病毒資料庫記錄類型； 電腦上應用程式安裝實例的唯一 ID； 產品授權啟動日期； 授權失效日期； 授權識別碼； 軟體所使用授權的狀態； 目前處理中物件的總和檢查碼類型； 偵測到的惡意軟體名稱或是可能用於傷害使用者裝置或資料的合法軟體名稱； 目前處理中物件的總和檢查碼； 軟體啟動碼的總和檢查碼； 軟體的完整版本； 軟體 ID； 軟體金鑰檔案的總和檢查碼； 用於提供軟體授權的資訊模型 ID； 用於簽署軟體授權票證標頭的憑證識別碼； 軟體授權票證建立日期和時間； 軟體授權票證總和檢查碼； 軟體授權票證版本； 軟體啟動碼版本； 權利持有人基礎架構請求資料格式； 啟動的產品授權票證 ID； 軟體元件 ID； 軟體動作結果； 錯誤代碼； 網路服務的已存取位址（URL、IP）； 通訊埠編號； 網路服務請求來源（推薦者）的網址； 防毒資料庫的更新適用週期數； 防毒資料庫上次更新和套用的日期和時間； 軟體資料庫的發佈日期與時間； 軟體元件版本； 軟體更新 ID； 已安裝軟體的類型； System Watcher 開始的日期和時間； 軟體的安裝日期和時間； 由 System Watcher 傳送統計資料的可能性； 由 System Watcher 處理，需時超過標準時間的事件碼； 由 System Watcher 處理，需時超過標準時間的事件的資料庫處理時間； 由 System Watcher 處理一項事件的最大允許時間； 由 System Watcher 處理，需時超過標準時間的事件處理時間； 由 System Watcher 處理，需時超過標準時間的事件總數。

- 所有被處理物件與操作的相關資訊： 軟體對被處理物件的判定； 目錄碼； 處理中物件的大小； 處理中物件的總和檢查碼 (SHA256)； 系統監控環境中偵測到的軟體數量； 被系統監控偵測到的軟體的日期和時間； 偵測特徵； 軟體病毒資料庫中的已觸發記錄 ID； 系統監控偵測軟體的原因； 處理中物件的總和檢查碼 (MD5)； 模組完整性檢查的結果； 目前處理中物件的名稱； 觸發的軟體病毒資料庫記錄類型； 所處理物件的路徑； 被掃描物件的名稱； 掃描的日期和時間； 從其下載的 URL 和 Referrer 位址； 被掃描檔案的大小及其路徑； 壓縮檔案標誌； 檔案建立日期與時間； 封包程式的名稱、大小和總和檢查碼（MD5、SHA2-256）（如果檔案被封包）； 檔案的熵； 檔案的類型； 檔案類型代碼； 可執行檔的標誌、ID 和格式； 物件的總和檢查碼（MD5、SHA2-256）； 物件的補充總和檢查碼的類型和值； 有關物件的數位簽章（憑證）的資料： 憑證發行者相關資料、自上一次傳送統計資料後物件的啟動次數、應用程式掃描工作的 ID、收取有關物件信譽的資訊的方式、目標篩選條件值、適用偵測技術的技術參數； 所處理物件的路徑； 目錄碼。

- 對於可執行檔： 檔案區段熵、聲譽驗證旗標或檔案簽署旗標、名稱、類型、ID 類型、總和檢查碼 (MD5)、經驗證物件所載入應用程式的大小、應用程式路徑和範本路徑、自動執行清單中表明狀態的屬性、登錄日期、屬性清單、封裝程式名稱、應用程式數位簽章相關資訊： 發行商憑證、以 MIME 格式上傳的檔案名稱、檔案組建日期與時間。

- 啟動的應用程式及其模組的相關資訊： 總和檢查碼（MD5、SHA2-256）、大小、屬性、建立日期、加殼器名稱（如果檔案已加殼）、檔案名稱、有關係統上執行的處理程序的資訊（處理程序 ID (PID)、處理程序名稱、有關啟動處理程序的帳戶的資訊、啟動處理程序的應用程式和命令、處理程序檔案的完整路徑以及啟動命令列、處理程序所屬應用程式的敘述（處理程序的名稱）應用程式和有關發布者的資訊），以及正在使用的數位憑證和驗證其真實性所需的資訊或有關缺少檔案數位簽章的資訊），以及有關載入到處理程序中的模組的資訊： 它們的名稱、大小、類型、建立日期、屬性、總和檢查碼（MD5、SHA2-256、SHA1）、它們的路徑、PE 檔案標頭資訊、加殼器名稱（如果檔案已加殼）、有關可用性的資訊以及這些統計資料的有效性、產生正在傳送的統計資料的模式的識別碼。

- 若偵測到威脅或弱點，除了所偵測物件的相關資訊以外，還需提供下列資訊：識別碼、版本及病毒資料庫中的記錄類型、根據卡巴斯基分類的威脅名稱、病毒資料庫上一次更新的日期與時間、可執行檔名稱、要求威脅偵測 URL 之應用程式檔案的總和檢查碼 (MD5)、已偵測威脅的 IP 位址（IPv4 或 IPv6）、弱點識別碼及其威脅等級、偵測到弱點的網頁的 URL 與參照位址。

- 若偵測到潛在惡意物件，提供的相關資訊包括程序記憶體中的資料。

- 網路攻擊資訊： 發動攻擊的電腦 IP 位址、網路攻擊指向的使用者電腦連接埠號、攻擊協定的 ID、攻擊的名稱和類型。

- 網路連線相關資訊： 啟動程序而開啟連接埠的檔案版本及總和檢查碼 (MD5、SHA2-256、SHA1)、程序檔案的路徑及其數位簽章、本機及遠端 IP 位址、本機及遠端連接埠號、連線狀態、連接埠開啟的時間戳記。

- 偵測到有害或可疑內容的網頁 URL 和 IP 位址、要求該 URL 的檔案名稱、大小和總和檢查碼、用來達到判定結果之規則的識別碼、加權與程度、攻擊目標。

- 有關已安裝應用程式和病毒資料庫更新的資訊： 更新工作的完成狀態、更新期間可能發生的錯誤類型、更新失敗的次數、執行更新之應用程式元件的識別碼。

- 卡巴斯基安全網路 (KSN) 的使用相關資訊： KSN 識別碼、軟體識別碼、應用程式完整版本、使用者裝置的去個人化 IP 位址、KSN 要求履行品質指標、KSN 封包處理品質指標、KSN 要求數目指標與 KSN 要求類型相關資訊、開始傳送統計資料的日期與時間、結束傳送統計資料的日期與時間、KSN 配置更新相關資訊： 活動配置的識別碼、收到的配置的識別碼、配置更新的錯誤代碼。

- 系統記錄事件相關資訊： 偵測到事件的記錄檔名稱、事件的類型與分類、事件來源名稱以及事件描述。

- 用於確定檔案和 URL 位址信譽的資訊： 請求信譽的 URL 位址和參照位址、連線的協定類型、應用程式類型的內部識別碼、正在使用的連接埠號、使用者識別碼、掃描檔案的總和檢查碼 (MD5)、偵測到的威脅的類型、用於偵測威脅的記錄的資訊（病毒資料庫的記錄識別碼、記錄時間戳記和類型）； 認證的公開金鑰； 所掃描物件與雜湊演算法的數位憑證指紋。

- 應用程式地區分佈相關資料： 應用程式安裝和啟動日期、提供應用程式啟動授權的合作夥伴 ID、應用程式 ID、應用程式語言本機化 ID、應用程式啟動授權序號、KSN 加入簽章。

- 所使用授權的相關資訊： 授權的類型和有效期、授權失效前的天數、向其購買授權的合作夥伴的識別碼、區域啟動中心識別碼、啟動碼的總和檢查碼、SHA1 演算法計算的票證內容雜湊、授權票證建立日期與時間、授權資訊識別碼、授權票證識別碼、授權票證順序識別碼、使用者電腦的唯一識別碼、授權票證有效開始日期、授權票證有效結束日期、授權票證目前狀態、票證標題版本、授權版本、票證標題簽章憑證識別碼、金鑰檔案的總和檢查碼、票證標題簽署者序號、身分驗證權杖。

- 電腦上所安裝的硬體相關資訊： 內建和已連線裝置的類型、名稱、型號名稱、韌體版本、參數。

- 裝置資訊： 裝置 ID。

- Web 控制元件的作業資訊：
  元件版本、分類原因、其他分類原因的相關資訊、分類 URL、被封鎖 / 分類物件的主機 IP 位址。

雲端模式

雲端模式切換開關可啟用/停用 Kaspersky Endpoint Security 在其中使用輕量級版本的惡意軟體防護資料庫的應用程式運行模式。僅當啟用卡巴斯基安全網路參與時，此模式才可用。與通常的資料庫相比，輕量級版本的惡意軟體防護資料庫僅需要大約一半的電腦 RAM。如果您未參與卡巴斯基安全網路或已停用雲端模式，Kaspersky Endpoint Security 會從 Kaspersky 伺服器下載完整版本的惡意軟體防護資料庫。

如果開啟該切換按鈕，Kaspersky Endpoint Security 將使用惡意軟體防護資料庫的輕量級版本，這可以減少作業系統資源上的負載。

注意：選中該核取方塊後，Kaspersky Endpoint Security 在下次更新期間下載惡意軟體防護資料庫的輕量級版本。

如果關閉該切換按鈕，Kaspersky Endpoint Security 將使用惡意軟體防護資料庫的完全版本。

注意：選中該核取方塊後，Kaspersky Endpoint Security 在下次更新期間下載惡意軟體防護資料庫的完整版本。

KSN 聲明

點擊此連結將開啟一個視窗，您可以在其中閱讀卡巴斯基安全網路聲明的文字並接受卡巴斯基安全網路參與條款。

注意：如果您透過卡巴斯基安全管理中心網頁主控台管理 Kaspersky Endpoint Security，並且根據卡巴斯基安全管理中心設定，您可以加入卡巴斯基私人安全網路而不是卡巴斯基安全網路。如果您透過卡巴斯基安全管理中心雲端主控台管理 Kaspersky Endpoint Security，則無法參與卡巴斯基私人安全網路。有關參與卡巴斯基私人安全網路的詳細資訊，請參閱卡巴斯基安全管理中心說明。

在**KSN 代理設定**部分中，您可以設定 KSN 代理設定。

使用 KSN 代理

此核取方塊可在連線到卡巴斯基安全網路時啟用/停用代理伺服器的使用。

如果選取該核取方塊，Kaspersky Endpoint Security 將使用代理伺服器連線到卡巴斯基安全網路。

如果清除該核取方塊，Kaspersky Endpoint Security 會直接連線到卡巴斯基安全網路。

預設情況下已清空此核取方塊。

當 KSN 代理不可用時使用卡巴斯基伺服器

如果 KSN 代理不可用，此核取方塊可啟用/停用卡巴斯基服務器的使用。

如果選中該核取方塊，當 KSN 代理不可用時，Kaspersky Endpoint Security 將使用 KSN 伺服器。

如果清除此核取方塊，當 KSN 代理不可用時，Kaspersky Endpoint Security 不會使用卡巴斯基伺服器。

預設情況下已清空此核取方塊。

如果選取**使用 KSN 代理**核取方塊，則此核取方塊可用。

強制執行

當**強制執行**切換開關開啟時，Kaspersky Endpoint Security 禁止變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

當**強制執行**切換開關關閉時，Kaspersky Endpoint Security 允許變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

“參與卡巴斯基安全網路/卡巴斯基私人安全網路”視窗

瞭解更多

點擊此連結將開啟一個新的瀏覽器視窗，您可以在其中閱讀卡巴斯基安全網路聲明或卡巴斯基私人安全網路聲明的文字。

我接受卡巴斯基安全網路/卡巴斯基私人安全網路的參與條款

套用政策的電腦參與卡巴斯基安全網路/卡巴斯基私人安全網路。

我不接受卡巴斯基安全網路/卡巴斯基私人安全網路的參與條款

套用此政策的電腦不參與卡巴斯基安全網路/卡巴斯基私人安全網路。

注意：如果您透過卡巴斯基安全管理中心雲端主控台管理 Kaspersky Endpoint Security，則無法參與卡巴斯基私人安全網路。有關參與卡巴斯基私人安全網路的詳細資訊，請參閱卡巴斯基安全管理中心說明。

“基本威脅防護”部分

檔案威脅防護

點擊此連接將開啟一個視窗，您可以在其中設定檔案威脅防護設定。

Web 威脅防護

點擊此連接將開啟一個視窗，您可以在其中設定 Web 威脅防護設定。

網路威脅防護

點擊此連接將開啟一個視窗，您可以在其中設定網路威脅防護設定。

郵件威脅防護

點擊此連接將開啟一個視窗，您可以在其中設定郵件威脅防護設定。

防火牆

點擊此連接將開啟一個視窗，您可以在其中設定防火牆設定。

“檔案威脅防護”視窗

檔案威脅防護

檔案威脅防護切換開關可啟用/停用檔案威脅防護。

如果開啟**檔案威脅防護**切換開關，Kaspersky Endpoint Security 將對套用政策的用戶端電腦的檔案系統執行即時監控。

如果**檔案威脅防護**切換開關關閉，則 Kaspersky Endpoint Security 不會防護套用政策的用戶端電腦的檔案系統。

此切換開關預設為開啟。

在**防護範圍**部分，您可以透過選擇預設項目之一或新增您選擇的檔案或資料夾來設定防護範圍。

新增

點擊此按鈕將開啟一個對話方塊，您可以在其中指定要新增至防護範圍中包含的物件清單中的檔案、資料夾或遮罩。

刪除

點擊此按鈕會將物件從防護範圍中移除。

如果在受防護物件清單中選擇了某個物件，則此按鈕可用。

您無法刪除包含在防護範圍內的預設物件。

防護範圍

此列包含啟用檔案威脅防護時 Kaspersky Endpoint Security 掃描的物件。

預設情況下，Kaspersky Endpoint Security 掃描以下物件：

- **所有卸除式磁碟**。Kaspersky Endpoint Security 掃描所有卸除式磁碟機。
- **所有內置磁碟**。Kaspersky Endpoint Security 掃描所有內部磁碟機。
- **所有網路磁碟**。Kaspersky Endpoint Security 掃描所有網路磁碟機。

狀態

如果開啟此列中的切換開關，Kaspersky Endpoint Security 將在啟用檔案威脅防護時掃描**防護範圍**列中的對應物件。

如果此列中的切換開關被關閉，則在啟用檔案威脅防護時，Kaspersky Endpoint Security 不會掃描**防護範圍**欄位中的對應物件。

附加

此列指示 Kaspersky Endpoint Security 是否掃描對應物件的子資料夾。

在**如果偵測到惡意物件**部分中，您可以選擇 Kaspersky Endpoint Security 在偵測到惡意物件時執行的操作。

提示操作

Kaspersky Endpoint Security 會顯示一個通知視窗，其中包含有關使檔案受到感染的惡意物件資訊，並提示您選擇 Kaspersky Endpoint Security 要執行的操作。可用的操作可能因物件狀態的不同而有所不同。

預設選擇此選項。

解毒；若解毒失敗則刪除

Kaspersky Endpoint Security 封鎖存取受感染檔案並嘗試在不請求使用者確認的情況下解毒檔案。

如果解毒成功，Kaspersky Endpoint Security 會以原始檔案名稱將檔案儲存在原始位置。如果解毒失敗，Kaspersky Endpoint Security 將刪除感染檔案。

解毒；若解毒失敗則封鎖

Kaspersky Endpoint Security 封鎖存取受感染檔案並嘗試在不請求使用者確認的情況下解毒檔案。

如果解毒成功，Kaspersky Endpoint Security 會以原始檔案名稱將檔案儲存在原始位置。如果解毒失敗，Kaspersky Endpoint Security 會使受感染的檔案在其原來的位置保持封鎖狀態。

在**最佳化**部分，您可以配置掃描效能並選擇掃描演算法。

只掃描新增及修改的檔案

此核取方塊可啟用/停用僅掃描 Kaspersky Endpoint Security 識別為新檔案或自上次掃描以來已修改的檔案。

如果選取此核取方塊，Kaspersky Endpoint Security 將僅掃描其識別為新檔案或自上次掃描以來已修改的檔案。

如果清除該核取方塊，Kaspersky Endpoint Security 將掃描所有檔案。

預設情況下已選擇此選擇方塊。

略過掃描唯讀系統磁區

該核取方塊可停用/啟用 Kaspersky Endpoint Security 掃描唯讀系統磁碟區。

如果選擇此核取方塊，Kaspersky Endpoint Security 將不掃描唯讀系統磁碟區。這可大大縮短掃描時間。

如果清除此核取方塊，Kaspersky Endpoint Security 將掃描唯讀系統磁碟區。

預設情況下已選擇此選擇方塊。

使用 iSwift

此核取方塊可啟用/停用在掃描過程中使用 iSwift 技術。iSwift 允許 Kaspersky Endpoint Security 使用特殊演算法從掃描中排除某些物件，這有助於提高掃描速度。

如果選取此核取方塊，Kaspersky Endpoint Security 將在掃描期間使用 iSwift。

如果取消選擇該框，Kaspersky Endpoint Security 將將在掃描期間不使用 iSwift。

預設情況下已選擇此選擇方塊。

在**檔案類型**部分中，您可以選擇當檔案威脅防護被啟用時 Kaspersky Endpoint Security 將掃描哪些檔案。

掃描所有檔案

Kaspersky Endpoint Security 掃描所有被執行、開啟或儲存的檔案系統物件。

按內容掃描應用程式和文件

Kaspersky Endpoint Security 僅掃描可能被感染的物件（根據其內容）。

按延伸程式掃描應用程式和文件

Kaspersky Endpoint Security 僅掃描可能被感染的物件（根據其副檔名）。

延伸程式清單由卡巴斯基定義並包含在 Kaspersky Endpoint Security 資料庫中。

Kaspersky Endpoint Security 總是掃描不含副檔名的檔案。

在**複合檔案**部分，您可以選擇當檔案威脅防護被啟用時 Kaspersky Endpoint Security 掃描的複合檔案類型。

掃描存檔

此核取方塊可啟用/停用壓縮檔案掃描。有關延伸程式清單，請參閱 Kaspersky Endpoint Security 說明。

如果勾選此核取方塊，Kaspersky Endpoint Security 將掃描壓縮檔案。

如果清除此核取方塊，Kaspersky Endpoint Security 將在掃描期間跳過壓縮檔案。

掃描安裝套件

此核取方塊可啟用/停用對安裝套件的掃描。

如果勾選此核取方塊，Kaspersky Endpoint Security 將掃描安裝套件。

如果清除此核取方塊，Kaspersky Endpoint Security 將在掃描期間跳過安裝套件。

掃描嵌入的 OLE 物件

此核取方塊可啟用/停用掃描檔案中嵌入的物件，例如 Excel 電子表格、巨集或電子郵件附件。

如果勾選此核取方塊，Kaspersky Endpoint Security 將掃描嵌入的 OLE 物件。

如果清除此核取方塊，Kaspersky Endpoint Security 將在掃描期間跳過嵌入的 OLE 物件。

不擷取大於 <值> MB 的壓縮檔案

此核取方塊可啟用/停用對要掃描的壓縮檔案大小的限制。

如果選取此核取方塊，Kaspersky Endpoint Security 將在掃描期間跳過大於指定值的壓縮檔案。

如果清除此核取方塊，Kaspersky Endpoint Security 會擷取並掃描壓縮檔案，無論其大小為何。

如果選取**掃描存檔**核取方塊，則此核取方塊可用。

延遲擷取大於 MB 的檔案

限制要掃描的壓縮檔案大小的選項。

如果勾選此核取方塊，Kaspersky Endpoint Security 會掃描大小超過設定限制的所有壓縮檔案，但會在偵測到此類壓縮檔案兩分鐘後以較低優先順序執行掃描。

如果清除此核取方塊，Kaspersky Endpoint Security 將以同等優先順序掃描所有壓縮檔案。

如果選取**掃描存檔**核取方塊，則此核取方塊可用。

強制執行

當**強制執行**切換開關開啟時，Kaspersky Endpoint Security 禁止變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

當**強制執行**切換開關關閉時，Kaspersky Endpoint Security 允許變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

“新增防護範圍”對話方塊

輸入檔案名稱、資料夾名稱或遮罩輸入欄位

檔案、資料夾或檔案/資料夾遮罩的路徑。

物件是資料夾

此核取方塊可啟用/停用將物件作為資料夾來掃描。

如果勾選此核取方塊，Kaspersky Endpoint Security 會將您在**輸入檔案名稱、資料夾名稱或遮罩**欄位中指定的物件作為資料夾來掃描。

如果清除此核取方塊，Kaspersky Endpoint Security 會將您在**輸入檔案名稱、資料夾名稱或遮罩**欄位中指定的物件作為檔案來掃描。

預設情況下已選擇此選擇方塊。

包含子資料夾

此核取方塊可啟用/停用掃描在**輸入檔案名稱、資料夾名稱或遮罩**欄位中指定的資料夾中的子資料夾。

如果選取此核取方塊，Kaspersky Endpoint Security 將在惡意軟體掃描期間掃描子資料夾。

如果清除此核取方塊，Kaspersky Endpoint Security 在惡意軟體掃描期間僅掃描直接位於**輸入檔案名稱、資料夾名稱或遮罩**欄位中指定的資料夾中的檔案。

預設情況下已選擇此選擇方塊。

“Web 威脅防護”視窗

Web 威脅防護

Web 威脅防護切換開關可啟用/停用 Web 威脅防護。

如果**Web 威脅防護**切換開關被開啟，Web 威脅防護將掃描您的電腦在 Safari、Google Chrome 或 Firefox 中透過 HTTP 和 HTTPS 協定傳送和接收的資料。

如果**Web 威脅防護**切換開關被關閉，Web 威脅防護不會掃描您的電腦透過 Web 瀏覽器傳送和接收的資料。

此切換開關預設為開啟。

在**如果偵測到惡意物件**部分中，您可以選擇 Kaspersky Endpoint Security 在偵測到惡意物件時執行的操作。

提示操作

Kaspersky Endpoint Security 會顯示一個通知視窗，其中包含有關感染了 Web 流量物件的惡意軟體類型的資訊，並提示您選擇 Kaspersky Endpoint Security 對此物件要採取的操作。可用的操作可能因物件狀態的不同而有所不同。

預設選擇此操作。

自動封鎖

Kaspersky Endpoint Security 會自動封鎖對危險Web 流量物件的存取。

在**受信任網址**部分中，您可以建立或編輯受信任的網址清單，並啟用或停用掃描此清單中的網址的流量。

不掃描受信任網址的 Web 流量

此核取方塊可啟用/停用掃描來自受信任網址的 Web 流量。

如果勾選此核取方塊，則 Kaspersky Endpoint Security 不會掃描來自受信任網址的 Web 流量。

如果清除此核取方塊，Kaspersky Endpoint Security 將掃描來自受信任網址的 Web 流量。

預設情況下已清空此核取方塊。

網址清單

此清單包含受信任的網址。

您可以清除清單中網址旁的核取方塊。如果清除該核取方塊，Web 威脅防護將掃描來自從該網址的 Web 流量。

如果勾選**不掃描受信任網址的 Web 流量**核取方塊，則該清單可用。

新增

點擊此按鈕將開啟一個對話方塊，您可以在其中輸入要新增至受信任網址清單中的網址或網址遮罩。

刪除

按一下此按鈕將從清單中刪除選定的網址或網址遮罩。

如果在受信任網址清單中選擇網址或網址遮罩，則此按鈕可用。

網址

此列包含受信任的網址。

狀態

如果開啟此列中的切換開關，則在啟用 Web 威脅防護並勾選**網址**核取方塊的情況下，Kaspersky Endpoint Security 不會掃描**不掃描受信任網址的 Web 流量**列中的對應物件。

如果關閉此列中的切換開關，則在啟用 Web 威脅防護並勾選**網址**核取方塊的情況下，Kaspersky Endpoint Security 會掃描**不掃描受信任網址的 Web 流量**列中的對應物件。

強制執行

當**強制執行**切換開關開啟時，Kaspersky Endpoint Security 禁止變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

當**強制執行**切換開關關閉時，Kaspersky Endpoint Security 允許變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

"新增網址"對話方塊

網址輸入欄位

Web 威脅防護不會掃描其流量的網址或網址遮罩。

在**狀態**部分中，您可以定義 Kaspersky Endpoint Security 是否掃描來自該網址或網址群組的流量。

停用

網址或網址遮罩將會被新增到**受信任網址**清單中，但 Kaspersky Endpoint Security 會掃描其流量。

啟用

網址或網址遮罩將會被新增到**受信任網址**清單中，Kaspersky Endpoint Security 不會掃描其流量。

“網路威脅防護”視窗

網路威脅防護

網路威脅防護切換開關可啟用/停用網路威脅防護。

如果**網路威脅防護**切換開關開啟，Kaspersky Endpoint Security 會防護遠端電腦免受網路攻擊。

如果**網路威脅防護**切換開關關閉，Kaspersky Endpoint Security 不會防護遠端電腦抵禦網路攻擊。

此切換開關預設為開啟。

在**網路威脅防護設定**部分，您可以修改 Kaspersky Endpoint Security 封鎖攻擊電腦的期限。

封鎖攻擊電腦 分鐘

此核取方塊可啟用/停用將攻擊電腦新增至指定時間段內封鎖的電腦清單。

如果選取此核取方塊，Kaspersky Endpoint Security 會將攻擊電腦新增至指定時間內封鎖的電腦清單。

如果不選擇此選擇方塊，Kaspersky Endpoint Security 將不會封鎖攻擊電腦。

預設情況下已選擇此選擇方塊。

預設情況下，攻擊電腦會被封鎖 60 分鐘。

在**排除項目**部分中，您可以建立或編輯遠端電腦的 IP 位址清單，這些電腦的網路活動永遠不會被 Kaspersky Endpoint Security 封鎖。

IP 位址清單

此清單包含其網路活動永遠不會被 Kaspersky Endpoint Security 封鎖的遠端電腦的 IP 位址。

新增

點擊此按鈕將開啟一個對話方塊，您可以在其中輸入遠端電腦的 IP 位址。

刪除

點擊此按鈕可從清單中刪除選擇的 IP 位址。

如果在 IP 位址清單中選擇了遠端電腦的 IP 位址，則此按鈕可用。

強制執行

當**強制執行**切換開關開啟時，Kaspersky Endpoint Security 禁止變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

當**強制執行**切換開關關閉時，Kaspersky Endpoint Security 允許變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

“新增排除項目”對話方塊

IP 位址輸入欄位

遠端電腦的 IP 位址。

“安全控制”部分

Web 控制

Web 控制切換開關可啟用/停用 Web 控制。

如果開啟**Web 控制**切換開關，您可以建立規則來管理使用者在遠端電腦上造訪的網站。

如果關閉**Web 控制**切換開關，您將無法管理使用者在遠端電腦上造訪的網站。

此切換開關預設關閉。

規則清單

此清單包含您為管理使用者在遠端電腦上造訪的網站而建立的規則。

規則的排序順序決定了 Kaspersky Endpoint Security 對其應用程式排序的優先順序。

新增

點擊此按鈕將開啟一個視窗，您可以在其中為 Web 控制建立新規則。

刪除

點擊此按鈕可以從規則清單中移除選擇的規則。

如果選取規則旁邊的核取方塊，則此按鈕可用。

向上

點擊此按鈕會將所選規則在規則清單中向上移動，並提高 Kaspersky Endpoint Security 對其應用程式的優先順序。

向下

點擊此按鈕會將所選規則在規則清單中向下移動，並降低 Kaspersky Endpoint Security 對其應用程式的優先順序。

名稱

規則名稱。

狀態

此列中的切換開關可定義規則是否處於活動狀態。

您可以開啟/關閉對應規則旁邊的切換開關來變更規則的狀態。

操作

當使用者造訪特定網址、網址群組或受規則影響的網站類別時 Kaspersky Endpoint Security 執行的操作。

您可以透過選擇此列對應快捷功能表中的另一個選項來變更指派的操作。

強制執行

當**強制執行**切換開關開啟時，Kaspersky Endpoint Security 禁止變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

當**強制執行**切換開關關閉時，Kaspersky Endpoint Security 允許變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

“編輯規則”視窗

規則名稱輸入欄位

規則名稱。

在**狀態**部分中，您可以將規則設定為活動或非活動。

啟動

如果選取此選項，您將建立一個活動的規則。它將在政策實施後立即被套用於遠端電腦。

未啟動

如果選取此選項，您將建立一個非活動的規則。它將在政策執行時處於待定狀態。

在**操作**部分中，您可以選擇 Kaspersky Endpoint Security 在使用者存取受規則影響的特定網址、網址群組或網站類別時執行的操作。

允許

如果選擇此選項，Kaspersky Endpoint Security 將允許使用者造訪受規則影響的網址、網址群組或網站類別。

注意：如果在“新建政策”精靈的**網路**中開啟**安全連線 (HTTPS) 檢查**切換開關，Kaspersky Endpoint Security 將允許造訪遠端電腦上的 Web 資源。

預設選擇此選項。

封鎖

如果選擇此選項，Kaspersky Endpoint Security 將防止使用者造訪受規則影響的網址、網址群組或網站類別。

注意：如果在“新建政策”精靈的**網路**視窗中開啟**安全連線 (HTTPS) 檢查**切換開關，則當使用者存取遠端電腦上 Web 控制所封鎖的 Web 資源時，Kaspersky Endpoint Security 會顯示通知。

顯示警告

如果選擇此選項，當使用者嘗試造訪受規則影響的網址、網址群組或網站類別時，Kaspersky Endpoint Security 會顯示警告。

在**規則區域**部分中，您可以選擇為某個特定網址或一組網址、或網站類別建立規則。

類別

如果選擇此選項，您將為網站類別建立規則。

選擇類別

點擊此連結將開啟一個對話方塊，您可以在其中選擇受規則影響的網站類別。

單個位址

如果選擇此選項，您將為某個特定網址或一組網址建立規則。

預設選擇此選項。

新增

點擊此按鈕將開啟一個對話方塊，您可以在其中指定受規則影響的網址或網址遮罩。

刪除

點擊此按鈕將從受規則影響的網址清單中刪除選定的網址或網址遮罩。
如果選取網址或網址遮罩旁的核取方塊，則此按鈕可用。

位址

受規則影響的網址或網址遮罩。

“新增網址”對話方塊

網址輸入欄位

將受規則影響的網址或網址遮罩。

“內容類別”對話方塊

內容類別清單

此清單包含您可以新增至規則的網站類別清單。

網站類別名稱旁的核取方塊可將屬於該類別的網站新增至規則或從規則中刪除。

預設情況下，所有核取方塊均處於清除狀態。

“Detection and Response” 部分

Managed Detection and Response

點擊此連結將開啟一個視窗，您可以在其中配置Managed Detection and Response 設定。

Endpoint Detection and Response

點擊此連結將開啟一個視窗，您可以在其中配置 Endpoint Detection and Response 設定。

Endpoint Detection and Response Expert (on-premise)

點擊此連結將開啟一個視窗，您可以在其中配置 Endpoint Detection and Response Expert（內部部署）。

“Managed Detection and Response“ 視窗

Managed Detection and Response

Managed Detection and Response 切換開關可啟用/停用與 Kaspersky Managed Detection and Response 服務互動的 Managed Detection and Response 元件。該服務會不斷偵測並消除針對您組織的安全威脅。

如果**Managed Detection and Response** 切換開關已開啟，MDR 設定檔案已匯入，則Managed Detection and Response 元件被啟用。

如果**Managed Detection and Response**切換開關被關閉，則 Managed Detection and Response 元件被停用。

此切換開關預設關閉。

匯入

點擊此按鈕將開啟一個視窗，您可以在其中匯入 Kaspersky Endpoint Security 政策中的 MDR 設定檔。

刪除設定檔

點擊此按鈕可從 Kaspersky Endpoint Security 政策中刪除 MDR 設定檔。

強制執行

當**強制執行**切換開關開啟時，Kaspersky Endpoint Security 禁止變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

當**強制執行**切換開關關閉時，Kaspersky Endpoint Security 允許變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

“Endpoint Detection and Response” 視窗

Endpoint Detection and Response

Endpoint Detection and Response 切換開關可啟用/停用與 Endpoint Detection and Response 元件，它與 Kaspersky Endpoint Detection and Response 解決方案互動。此解決方案可防護電腦抵禦複雜威脅，包括新的弱點利用、勒索軟體和無檔案攻擊。

如果**Endpoint Detection and Response**切換開關開啟，則 Endpoint Detection and Response 元件將會啟用。

如果**Endpoint Detection and Response**切換開關關閉，則 Endpoint Detection and Response 元件將會停用。

此切換開關預設關閉。

在**網路隔離**部分中，您可以設定將電腦與網路隔離的設置，以回應入侵指標偵測。

配置電腦解鎖設定

點擊此連結將開啟一個視窗，您可以在其中指定自動關閉網路隔離的延遲。

排除項目

點擊此連結將開啟一個視窗，您可以在其中指定自動啟用網路隔離後電腦上不被封鎖的網路連線。

在**執行防止**部分中，您可以配置用於執行執行檔和指令碼以及開啟 Office 格式檔案的設定。

執行防止

執行防止切換開關可啟用/停用執行防禦。

如果**執行防止**切換開關打開，您可以建立和編輯執行防禦規則清單，並選擇執行或開啟禁止物件時要執行的操作。

如果關閉**執行防止**切換開關，您將無法管理使用者在其裝置上執行或開啟的物件。

此切換開關預設關閉。

執行或開啟被禁止物件時的動作

封鎖並寫入報告

如果選擇此模式，應用程式會封鎖執行物件或者開啟匹配防護規則條件的文件。應用程式也會將嘗試執行物件或者開啟文件的事件發佈到卡巴斯基安全管理中心事件記錄和統一記錄系統。

僅記錄事件

如果選擇此模式，Kaspersky Endpoint Security 會將嘗試執行可執行物件或者開啟匹配防護規則條件的文件的事件發佈到卡巴斯基安全管理中心事件記錄和統一記錄系統，但是不會封鎖執行或者開啟物件或者文件的嘗試。預設情況下已選擇此項。

新增

點擊此按鈕將開啟一個對話方塊，您可以在其中建立新的執行防禦規則。

編輯

點擊此按鈕可開啟一個對話方塊，您可在此視窗中編輯現有的執行防禦規則。

如果選定規則清單中的規則，則該按鈕可用。

刪除

點擊此按鈕可以從規則清單中移除執行防禦規則。

如果選定規則清單中的規則，則該按鈕可用。

在**Cloud Sandbox 設定**部分，您可以啟用或停用Cloud Sandbox元件。

Cloud Sandbox

Cloud Sandbox切換開關可啟用/停用 Cloud Sandbox 技術，有助於偵測電腦上的進階威脅。Kaspersky Endpoint Security 自動將被偵測檔案轉寄到 Cloud Sandbox 進行分析。Cloud Sandbox 在隔離環境中執行這些檔案以識別惡意活動和決定其信譽。有關這些檔案的資料然後被傳送到卡巴斯基安全網路。因此，如果 Cloud Sandbox 偵測到一個惡意檔案，Kaspersky Endpoint Security 將執行適當操作在偵測到該檔案的所有電腦上消除該威脅。

如果開啟**Cloud Sandbox**切換開關，則啟用 Cloud Sandbox 技術。

如果關閉**Cloud Sandbox**切換開關，則 Cloud Sandbox 技術被停用。

此切換開關預設關閉。

強制執行

當**強制執行**切換開關開啟時，Kaspersky Endpoint Security 禁止變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

當**強制執行**切換開關關閉時，Kaspersky Endpoint Security 允許變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

電腦解鎖設定視窗

距離自動解鎖被隔離的電腦

此核取方塊可啟用/停用在指定時間後自動關閉網路隔離。

如果勾選此核取方塊，您可以指定自動關閉電腦網路隔離的延遲時間。

如果清除此核取方塊，Kaspersky Endpoint Security 將在隔離開始 8 小時後關閉網路隔離。

預設情況下已選擇此選擇方塊。

小時

網路隔離將在此後被自動關閉的時間間隔。

僅當選取**距離自動解鎖被隔離的電腦**核取方塊時，此欄位才可編輯。

網路隔離排除項目視窗

網路隔離排除項目

此清單包含您新增為網路隔離排除項目的網路連線。

新增

點擊此按鈕將開啟一個視窗，您可以在其中手動指定要新增為排除項目的網路連線的設定。

從個人檔案新增

點擊此按鈕將開啟一個視窗，您可以在其中選擇用於配置排除項目的標準網路設定檔。

刪除

點擊此按鈕將從網路隔離排除項目清單中刪除網路連線。

如果選擇了網路隔離排除項目清單中的連線，則該按鈕可用。

規則屬性視窗

規則名稱

網路隔離排除規則的名稱。

這是一個可選參數。

方向

流量方向。

協定

協定類型。

編號

協定編號。

該值必須符合IANA 分配的網際網路協定號碼清單。

如果選擇**自訂**協定類型，則此欄位可用。

本機連接埠或範圍

正在為其配置網路隔離排除項目的電腦的本機連接埠或範圍。

遠端連接埠或範圍

正在為其配置網路隔離排除項目的電腦的遠端連接埠或範圍。

遠端位址

正在為其配置網路隔離排除項目的電腦的網路位址。

應用程式

此核取方塊可讓您新增被允許啟動網路連線的應用程式，該網路連線已被新增至隔離電腦上的網路隔離排除項目。

如果選取此核取方塊，您可以新增此類應用程式。

如果清除此核取方塊，則隔離電腦上的任何應用程式都可以啟動被新增至網路隔離排除項目中的網路連線。

預設情況下已清空此核取方塊。

新增

點擊此按鈕將開啟一個視窗，您可以在其中指定被允許啟動新增至網路隔離排除項目的網路連線的應用程式的路徑。

編輯

點擊此按鈕將開啟一個視窗，您可以在其中編輯新增應用程式的路徑。

如果選定清單中的應用程式，則該按鈕可用。

刪除

點擊此按鈕將刪除已新增的應用程式。

如果選定清單中的應用程式，則該按鈕可用。

防禦規則視窗

名稱

規則名稱。

類型

您要封鎖的物件的類型。

在**物件路徑**部分中，您可以選擇是否指定要禁止的物件的完整路徑。如果選擇指定路徑，請在對應欄位中輸入其值。

在**物件總和檢查碼**部分中，您可以選擇是否指定要禁止的物件的總和檢查碼。如果您選擇指定總和檢查碼，請選擇其類型並在對應欄位中輸入其值。

Endpoint Detection and Response (KATA) 視窗

Endpoint Detection and Response Expert (on-premise)

Endpoint Detection and Response Expert (on-premise)切換開關可啟用/停用與 Kaspersky Anti Targeted Attack Platform 解決方案互動的 Endpoint Detection and Response Expert（內部部署）元件。此解決方案可及時偵測進階威脅，例如定向攻擊、進階持續性威脅、零日攻擊等。

如果**Endpoint Detection and Response Expert (on-premise)**切換開關開啟，則 Endpoint Detection and Response Expert（內部部署）元件將會啟用。

如果**Endpoint Detection and Response Expert (on-premise)**切換開關關閉，則 Endpoint Detection and Response Expert（內部部署）元件將會停用。

此切換開關預設關閉。

Endpoint Detection and Response Expert（7.1 或者更早版本）

如果選擇此選項，則 Endpoint Detection and Response Expert（內部部署）元件將以與 Endpoint Detection and Response Expert（版本 7.1 或更早版本）相容的模式運作。

Endpoint Detection and Response Expert（8.0 或者更高版本）

如果選擇此選項，則 Endpoint Detection and Response Expert（內部部署）元件將以與 Endpoint Detection and Response Expert（版本 8.0 或更高版本）相容的模式運作。

繼承政策的連線設定

如果選擇此選項，則遙測資料收集伺服器連線設定、遙測資料收集伺服器、遙測資料收集伺服器資料傳輸設定、傳送至遙測資料收集伺服器的事件數量限制、回應伺服器連線設定以及回應伺服器將從父政策繼承，並且將無法編輯。

如果選擇**Endpoint Detection and Response Expert（8.0 或者更高版本）**模式，則此選項可用。

預設選擇此選項。

使用自訂連線設定

如果選擇此選項，則遙測資料收集伺服器連線設定、遙測資料收集伺服器、遙測資料收集伺服器資料傳輸設定、傳送至遙測資料收集伺服器的事件數量限制、回應伺服器連線設定以及回應伺服器將不從父政策繼承，仍然可以編輯。

如果選擇**Endpoint Detection and Response Expert（8.0 或者更高版本）**模式，則此選項可用。

根據在**連線至 KATA 伺服器**或者 **遙測資料收集伺服器連線**部分中選擇的模式，您可以配置伺服器連線設定。

連線設定

點擊此連接將開啟一個對話方塊，您可以在其中配置連線到伺服器的設定。

傳送同步請求至伺服器的間隔（分）

傳送到 KATA 伺服器的同步請求之間的時間間隔。

預設值是 5 分鐘。

如果選擇**Endpoint Detection and Response Expert（8.0 或者更高版本）**模式，則此選項可用。

新增

點擊此按鈕將開啟一個視窗，您可以在其中配置與伺服器的連線。

編輯

點擊此按鈕將開啟一個視窗，您可以在其中編輯與伺服器的現有連線。

如果伺服器選定清單中的伺服器，則該按鈕可用。

刪除

點擊此按鈕可從清單中刪除選擇的伺服器。

如果選定清單中的伺服器，則該按鈕可用。

位址

伺服器的 IP 位址。

連接埠

伺服器的連接埠號。

在**資料傳輸設定**部分中，您可以設定將資料傳送到伺服器的設定。

傳送遙測資料至 KATA

此核取方塊用於啟用/停用向 KATA 伺服器傳送事件。

如果選取此核取方塊，則會將事件傳送至 KATA 伺服器。

如果取消選取此核取方塊，則不會將事件傳送至 KATA 伺服器。

如果選擇**Endpoint Detection and Response Expert（7.1 或者更早版本）**模式，則此選項可用。

預設清除此核取方塊。

傳送遙測資料至遙測資料收集伺服器

此核取方塊用於啟用/停用向遙測資料收集伺服器傳送事件。

如果選取此核取方塊，則會將事件傳送至遙測資料收集伺服器。

如果取消選取此核取方塊，則不會將事件傳送至遙測資料收集伺服器。

如果選擇**Endpoint Detection and Response Expert（8.0 或者更高版本）**核取方塊，則此選項可用。

預設清除此核取方塊。

最大事件傳輸延遲時間（秒）

Kaspersky Endpoint Security 向伺服器傳送事件的時間間隔。

預設值是 30 秒。

在**請求節流**部分，您可以限制傳輸事件的數量。

啟用請求節流

此核取方塊可啟用/停用限制 Kaspersky Endpoint Security 傳送至 KATA 伺服器的事件數量。

如果選取此核取方塊，則應用程式傳送的事件數將受到限制。

如果清除此核取方塊，則應用程式傳送的事件數量不受限制。

預設情況下已選擇此選擇方塊。

每個小時的最大事件數量

Kaspersky Endpoint Security 每小時傳送到 KATA 伺服器的最大事件數。Kaspersky Endpoint Security 在一小時後還原傳送事件。

預設值是每小時 3000 個事件。

事件限制超過百分比

相同類型事件的閾值（以百分比表示）。

如果特定類型的事件與事件總數的比率超過配置的閾值，Kaspersky Endpoint Security 將限制該類型事件的傳輸。

預設值是 15%。

在 **連線至回應伺服器** 部分，您可以配置與回應伺服器的連線設定。

連線設定

點擊此連接將開啟一個對話方塊，您可以在其中配置連線到伺服器的設定。

傳送同步請求至伺服器的間隔（分）

傳送到 KATA 伺服器的同步請求之間的時間間隔。

預設值是 5 分鐘。

如果選擇**Endpoint Detection and Response Expert（8.0 或者更高版本）**模式，則此選項可用。

新增

點擊此按鈕將開啟一個視窗，您可以在其中配置與伺服器的連線。

編輯

點擊此按鈕將開啟一個視窗，您可以在其中編輯與伺服器的現有連線。

如果伺服器選定清單中的伺服器，則該按鈕可用。

刪除

點擊此按鈕可從清單中刪除選擇的伺服器。

如果選定清單中的伺服器，則該按鈕可用。

位址

伺服器的 IP 位址。

連接埠

伺服器的連接埠號。

強制執行

當**強制執行**切換開關開啟時，Kaspersky Endpoint Security 禁止變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

當**強制執行**切換開關關閉時，Kaspersky Endpoint Security 允許變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

KATA 伺服器視窗

位址

KATA 伺服器的 IP 位址。

連接埠

KATA 伺服器的連接埠號。

預設值是 443。

"伺服器連線設定"視窗

逾時（秒）

KATA 伺服器回應逾時。當逾時用完時，Kaspersky Endpoint Security 會嘗試連線到不同的 KATA 伺服器。

預設值是 10 秒。

在**伺服器 TLS 憑證**部分中，您可以新增或刪除 TLS 憑證並查看有關所新增的憑證的資訊。

新增 TLS 憑證

點擊此按鈕將開啟一個視窗，您可以在其中選擇將用於與 KATA 伺服器建立可信任連線的 TLS 憑證。

移除

點擊此按鈕將刪除目前的 TLS 憑證。

如果已新增 TLS 憑證，則此按鈕可用。

在**附加連線安全**部分中，您可以為 Kaspersky Endpoint Security 和 KATA 伺服器之間的連線配置增強防護。

使用雙向身分驗證

此核取方塊可啟用/停用雙向驗證，使 Kaspersky Endpoint Security 和 KATA 伺服器之間的連線更加安全。要使用雙向驗證，您需要載入加密容器。

如果勾選此核取方塊，Kaspersky Endpoint Security 將使用雙向驗證連線到 KATA 伺服器。

如果清除此核取方塊，則 Kaspersky Endpoint Security 不會使用雙向驗證來連線到 KATA 伺服器。

預設情況下已清空此核取方塊。

載入加密容器

點擊此按鈕將開啟一個視窗，您可以在其中選擇將用於雙向驗證的加密容器。加密容器檔案的副檔名為 .PFX。

注意：加密容器必須受密碼防護。無法新增密碼為空的加密容器。

加密容器密碼

用於雙向驗證的加密容器的密碼。

“更新”部分

更新應用程式模組

此核取方塊可啟用/停用應用程式模組的更新。應用程式資料庫始終更新。

如果勾選此核取方塊，Kaspersky Endpoint Security 會更新應用程式模組。

如果清除此選擇方塊，則 Kaspersky Endpoint Security 不會更新應用程式模組。

預設情況下已選擇此選擇方塊。

更新來源

此清單包含 Kaspersky Endpoint Security 從其下載和安裝應用程式資料庫和模組更新的資源位址。您可以指定本機或網路資料夾、FTP 或 HTTP 伺服器作為更新來源。

預設更新來源清單包含 Kaspersky 更新伺服器。

如果您透過卡巴斯基安全管理中心網頁主控台管理 Kaspersky Endpoint Security，則更新來源清單預設也包括卡巴斯基安全管理中心伺服器。

如果您透過卡巴斯基安全管理中心雲端主控台管理 Kaspersky Endpoint Security，則更新來源清單預設還包括發佈點。有關發佈點的詳細資訊，請參閱卡巴斯基安全管理中心說明。

您無法從清單中刪除預設更新來源。

新增

點擊此按鈕將開啟一個對話方塊，您可以在其中指定本機或網路資料夾的路徑，或要新增至更新來源清單的網址。

刪除

點擊此按鈕可從清單中刪除選擇的更新來源。

如果選取更新來源旁的核取方塊，則此按鈕可用。

更新來源

此列包含 Kaspersky Endpoint Security 的更新來源。

狀態

如果此列中的切換開關開啟，Kaspersky Endpoint Security 將使用**更新來源**列中對應的更新來源來接收更新。

如果此列中的切換開關關閉，則 Kaspersky Endpoint Security 不會使用**更新來源**列中對應的更新來源來接收更新。

強制執行

當**強制執行**切換開關開啟時，Kaspersky Endpoint Security 禁止變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

當**強制執行**切換開關關閉時，Kaspersky Endpoint Security 允許變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

“新增更新來源”對話方塊

輸入本機或網路資料夾的路徑，或網址輸入欄位

Kaspersky Endpoint Security 從其複製更新的資源位址。

您可以指定本機或網路資料夾的路徑、或 FTP 或 HTTP 伺服器的網址或 IP 位址作為資源的位址。

您可以按以下格式指定 FTP 伺服器的網址：ftp://<使用者名稱>:<密碼>@<主機>:<連接埠>。

在**狀態**部分中，您可以定義 Kaspersky Endpoint Security 是否使用指定的網址作為更新來源。

已停用

該網址已新增至更新來源清單中，但 Kaspersky Endpoint Security 未使用該網址作為更新來源。

已啟用

該網址被新增至更新來源清單中，並且 Kaspersky Endpoint Security 使用該網址作為更新來源。

“資料加密”部分

FileVault 磁碟加密

FileVault 磁碟加密切換開關可啟用/停用 FileVault 磁碟加密管理。

如果**FileVault 磁碟**加密切換開關開啟，則 FileVault 磁碟加密可以被從卡巴斯基安全管理中心套用到用戶端電腦。

如果**FileVault 磁碟加密**切換開關關閉，FileVault 磁碟加密將無法被從卡巴斯基安全管理中心套用到用戶端電腦。

此切換開關預設關閉。

注意：如果**FileVault 磁碟加密**切換開關被關閉，則具有管理員權限的使用者可以從系統設定中加密和解密其 Mac 啟動磁碟。有關 FileVault 的更多資訊，請參閱 Apple 文件。

加密磁碟

Kaspersky Endpoint Security 在對其套用政策的用戶端電腦上顯示輸入電腦帳戶憑據的提示。當使用者輸入憑據時，Kaspersky Endpoint Security 將開始加密使用者的啟動磁碟。

如果**FileVault 磁碟加密**切換開關被開啟且**“加密磁碟”**選項被選取，則具有管理員權限的使用者無法從系統設定中解密其 Mac 的啟動磁碟。

解密磁碟

Kaspersky Endpoint Security 在對其套用政策的用戶端電腦上顯示輸入電腦帳戶憑據的提示。當使用者輸入憑據時，Kaspersky Endpoint Security 將開始解密使用者的啟動磁碟。

如果**FileVault 磁碟加密**切換開關被開啟且**“解密磁碟”**選項被選取，則具有管理員權限的使用者無法從系統設定中加密其 Mac 的啟動磁碟。

強制執行

當**強制執行**切換開關開啟時，Kaspersky Endpoint Security 禁止變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

當**強制執行**切換開關關閉時，Kaspersky Endpoint Security 允許變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

“遙測設定”視窗

新增

點擊此按鈕將會開啟一個視窗，您可以在其中將規則新增到受信任區域。

編輯

點擊此按鈕可開啟一個視窗，您可在此編輯所選規則。

刪除

點擊該按鈕可以從受信任區域中刪除選定的規則。

狀態

此列中的切換開關用於停用/啟用新增至受信任區域的規則。

如果撥動開關已啟用，則該規則生效。

如果切換開關已停用，則該規則處於非活動狀態。

規則名稱

此列包含新增至受信任區域的規則名稱。

敘述

包含被新增至受信任區域的規則資訊的註解。

新增/編輯排除規則視窗

狀態

此切換開關用於啟用/停用新增至受信任區域的規則。

如果撥動開關已啟用，則該規則生效。

如果切換開關已停用，則該規則處於非活動狀態。

規則名稱

新增到受信任區域的規則名稱。

敘述

包含被新增至受信任區域的規則資訊的註解。

攻擊指標 (IOA)

用於輸入攻擊指標的 GUID 的欄位。

“其他設定”部分

防護

點擊此連結將開啟**防護**視窗，您可以在其中管理使用者電腦上安裝的 Kaspersky Endpoint Security 的一般設定，並選擇 Kaspersky Endpoint Security 將偵測的物件類型。

報告和備份

點擊此連結將開啟**報告和備份**視窗，您可以在其中管理報告和備份設定。

使用者互動

點擊此連結將開啟**使用者互動**視窗，您可以在其中設定 Kaspersky Endpoint Security 顯示的通知、卡巴斯基安全管理中心中顯示的事件的顯示語言以及 Kaspersky Endpoint Security 的其他設定。

網路

點擊此連結將開啟**網路**視窗，您可以在其中管理代理伺服器設定、啟用或停用加密連線 (HTTPS) 掃描、選擇用於在 Mozilla Firefox 瀏覽器中檢查加密 HTTPS 流量的憑證儲存以及配置受監控連接埠。

受信任區域

點擊此連結將開啟**受信任區域**視窗，您可以在其中新增檔案威脅防護或掃描工作的排除項目並配置受信任應用程式。

“防護”視窗

在**一般**部分中，您可以啟用或停用遠端電腦上的檔案防護，並設定在電腦開啟或作業系統重新啟動時自動啟動應用程式。

在電腦啟動時啟動應用程式

此核取方塊可啟用/停用當遠端電腦開啟或作業系統重新啟動時 Kaspersky Endpoint Security 自動啟動。

如果選取該核取方塊，Kaspersky Endpoint Security 將在遠端電腦開啟或其作業系統重新啟動時自動啟動。

如果清除該核取方塊，當遠端電腦開啟或其作業系統重新啟動時，Kaspersky Endpoint Security 不會自動啟動。

預設情況下已選擇此選擇方塊。

重要提示：如果您在 Kaspersky Endpoint Security 未執行時選取此核取方塊，則只有在本機啟動應用程式或使用卡巴斯基安全管理中心後才會套用變更。

啟用防護

此核取方塊可啟用/停用對安裝了 Kaspersky Endpoint Security 的遠端電腦的防護。

如果選取此核取方塊，則會啟用對遠端電腦的防護。

如果清除此核取方塊，則會停用對遠端電腦的防護。

預設情況下已選擇此選擇方塊。

在**被偵測的物件的類型**部分中，您可以選擇 Kaspersky Endpoint Security 將偵測的物件類型。

病毒，蠕蟲，木馬，惡意工具，廣告軟體和自動撥號程式

此核取方塊可啟用/停用對以下類型程式的偵測：

- 所有類型的惡意軟體。
- 在您的電腦上顯示廣告（例如，橫幅）或使用廣告網站替換瀏覽器中的搜尋結果的應用程式。
- 透過電腦的數據機偷偷建立電話連線的應用程式。

此核取方塊預設被選取且無法被清除。

可被入侵者利用以破壞使用者的電腦或個人資料的合法軟體

此核取方塊可啟用/停用對非惡意或有危險但在某些情況下可能被用於損害使用者電腦的應用程式的偵測。

如果選定了該核取方塊，Kaspersky Endpoint Security 會偵測可以被犯罪份子利用以破壞使用者的電腦或個人資料的合法軟體。

如果清除該核取方塊，則 Kaspersky Endpoint Security 不會偵測入侵者可用於損壞使用者電腦或個人資料的合法軟體。

預設情況下已清空此核取方塊。

進階部分可讓您啟用節能模式。

使用電池供電時略過排程工作

此核取方塊可啟用/停用在使用電池供電的電腦上啟動排程掃描工作。

如果勾選此核取方塊，則 Kaspersky Endpoint Security 不會在使用電池供電的電腦上啟動排程掃描工作。

如果清除此核取方塊，Kaspersky Endpoint Security 將在使用電池供電的電腦上啟動排程掃描工作。

預設情況下已選擇此選擇方塊。

限制掃描工作對 CPU 的使用

Kaspersky Endpoint Security 將對受防護裝置 CPU 執行按需掃描工作的使用相應輸入欄位中指定的值。

啟用此選項會對 Kaspersky Endpoint Security 的效能產生負面影響。

預設情況下，此選項處於停用狀態。

上限（百分比）

Kaspersky Endpoint Security 掃描工作允許的最大 CPU 使用率。

如果選擇了**限制掃描工作對 CPU 的使用**選項，則該輸入欄位可用。

注意：這是所有 CPU 核心的累積限制。活動監控器中顯示的 CPU 使用率是每個 CPU 核心使用率的總和，因此可能會超過 100%。

強制執行

當**強制執行**切換開關開啟時，Kaspersky Endpoint Security 禁止變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

當**強制執行**切換開關關閉時，Kaspersky Endpoint Security 允許變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

“報告與備份”視窗

在**報告**部分中，您可以設定用於產生和儲存有關 Kaspersky Endpoint Security 執行時發生的事件的報告的設定。

<值> 天後刪除報告

此核取方塊可啟用/停用在指定時間段後刪除報告。

如果選取此核取方塊，Kaspersky Endpoint Security 將在指定時間段後刪除報告。預設情況下，Kaspersky Endpoint Security 會將報表儲存 30 天。

如果清除此核取方塊，Kaspersky Endpoint Security 將無限期儲存報告。

預設情況下已選擇此選擇方塊。

記錄非緊急事件

此核取方塊可啟用/停用報告中非緊急事件（例如資訊事件）的記錄。非緊急事件不影響安全。

如果選擇該選擇方塊， Kaspersky Endpoint Security 將在報告中記錄資訊事件。

如果清除此核取方塊，Kaspersky Endpoint Security 將不會在報告中記錄資訊事件。

預設情況下已清空此核取方塊。

僅保留最近的事件

此核取方塊可啟用/停用僅保留有關上次執行工作的重要事件的資訊。

如果選取此核取方塊，則每次工作啟動時，Kaspersky Endpoint Security 都會從上次執行的工作中刪除有關非緊急事件的資訊，但會在報告中保留重要資訊（例如，有關偵測到的惡意軟體的訊息）。

如果清除此核取方塊，Kaspersky Endpoint Security 將保留上次執行工作的所有資訊。

預設情況下已清空此核取方塊。

在**備份**部分中，您可以指定物件可以在“備份”中儲存多長時間。

在 天後刪除物件

此核取方塊可啟用/停用在指定時間段後從備份中刪除物件。

如果選取此核取方塊，Kaspersky Endpoint Security 會在指定時間段後從備份中刪除物件。預設儲存期限為 30 天。

如果清除此核取方塊，Kaspersky Endpoint Security 將無限期地將物件儲存在備份中。

預設情況下已選擇此選擇方塊。

強制執行

當**強制執行**切換開關開啟時，Kaspersky Endpoint Security 禁止變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

當**強制執行**切換開關關閉時，Kaspersky Endpoint Security 允許變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

“使用者互動”視窗

在**應用程式介面**部分中，您可以設定應用程式圖示是否顯示在遠端電腦上的功能表列中，以及使用者是否可以開啟 Kaspersky Endpoint Security 主視窗並使用應用程式介面。

在功能表列中顯示應用程式圖示

此核取方塊可啟用/停用遠端電腦上功能表列中應用程式圖示的顯示。

如果選取此核取方塊，應用程式圖示將顯示在功能表列中。

如果清除此核取方塊，應用程式圖示將被從功能表列中隱藏。

預設情況下已選擇此選擇方塊。

允許使用者開啟應用程式

此核取方塊可啟用/停用使用者開啟 Kaspersky Endpoint Security 主視窗並使用遠端電腦上的應用程式介面的能力。

如果選取此核取方塊，使用者可以開啟 Kaspersky Endpoint Security 主視窗並使用遠端電腦上的應用程式介面。

如果清除此核取方塊，Kaspersky Endpoint Security 會阻止使用者開啟主應用程式視窗並隱藏遠端電腦上的應用程式介面。

預設情況下已選擇此選擇方塊。

在**通知**部分，您可以啟用有關 Kaspersky Endpoint Security 事件的通知並選擇首選通知類型。

通知

通知切換開關可啟用/停用有關 Kaspersky Endpoint Security 事件的通知。

如果**通知**切換開關開啟，Kaspersky Endpoint Security 將顯示 Kaspersky Endpoint Security 元件執行期間發生的事件的通知。

如果**通知**切換開關關閉，則 Kaspersky Endpoint Security 不會顯示 Kaspersky Endpoint Security 元件執行期間發生的事件的通知。

此切換開關預設為開啟。

使用者通知

點擊此連接將開啟一個視窗，您可以在其中選擇要用於所有事件類型的通知類型。

在**允許使用者結束應用程式**部分中，您可以設定遠端電腦上的使用者是否可以關閉 Kaspersky Endpoint Security。

在應用程式圖示的上下文功能表中顯示結束

此核取方塊可啟用/停用功能表列中顯示的應用程式圖示的上下文功能表中的**結束**項目的可用性。

如果選取此核取方塊，則應用程式圖示的上下文功能表中將提供**結束**”項目。遠端電腦的使用者可以結束遠端電腦上的 Kaspersky Endpoint Security。

如果清除此核取方塊，則應用程式圖示的上下文功能表中的**結束**"項目不可用。遠端電腦的使用者無法結束遠端電腦上的 Kaspersky Endpoint Security。

預設情況下已選擇此選擇方塊。

在**卡巴斯基安全管理中心中的事件**部分中，您可以選擇卡巴斯基安全管理中心中 Kaspersky Endpoint Security 事件的顯示語言。

顯示語言

從此下拉清單中，您可以選擇卡巴斯基安全管理中心中 Kaspersky Endpoint Security 事件的顯示語言。

在**限制**部分中，您可以允許在遠端電腦上本機管理 Kaspersky Endpoint Security 金鑰和更新。

允許使用者本機管理更新

此核取方塊可啟用/停用遠端電腦上 Kaspersky Endpoint Security 更新的本機管理。

如果選取此核取方塊，則會啟用遠端電腦上 Kaspersky Endpoint Security 更新的本機管理。

如果清除此核取方塊，則只能使用卡巴斯基安全管理中心中的 Kaspersky Endpoint Security 管理外掛程式來管理遠端電腦上的 Kaspersky Endpoint Security 更新。

預設情況下已選擇此選擇方塊。

允許使用者本機管理金鑰

此核取方塊可啟用/停用遠端電腦上 Kaspersky Endpoint Security 金鑰的本機管理。

如果選取該核取方塊，則會啟用遠端電腦上 Kaspersky Endpoint Security 金鑰的本機管理。

如果清除該核取方塊，則只能使用卡巴斯基安全管理中心中的 Kaspersky Endpoint Security 管理外掛程式來管理遠端電腦上的 Kaspersky Endpoint Security 金鑰。

預設情況下已選擇此選擇方塊。

在**密碼防護**部分中，您可以設定和配置密碼以限制使用者裝置上不需要的操作。

密碼防護

密碼防護切換開關可啟用/停用對使用者裝置上不必要的操作的密碼防護。

如果**密碼防護**切換開關打開，您可以設定和配置密碼以限制使用者在其裝置上的操作。

如果**密碼防護**切換開關關閉，使用者無需輸入密碼即可執行不需要的操作。

此切換開關預設關閉。

打開此切換開關將開啟一個視窗，您可以在其中配置密碼以限制用戶裝置上不需要的操作。

設定

點擊此按鈕將開啟一個視窗，您可以在其中配置密碼以限制用戶裝置上不需要的操作。

強制執行

當**強制執行**切換開關開啟時，Kaspersky Endpoint Security 禁止變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

當**強制執行**切換開關關閉時，Kaspersky Endpoint Security 允許變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

“使用者通知”視窗

事件

此列列出了 Kaspersky Endpoint Security 執行時可能發生的事件：

- **緊急事件**。對安全至關重要的事件。
- **功能失效**。導致系統失敗的事件。
- **重要事件**。使用者應該注意的事件。
- **資訊事件**。本質上是資訊性的事件。

通知

通知是通知使用者有關事件的快閃訊息。

通知列中的核取方塊可啟用/停用有關特定類別事件的快閃通知。

音訊

與事件相關的聲音通知。

音訊列中的核取方塊可啟用/停用特定類別事件的聲音通知。

“受信任區域”視窗：“檔案與資料夾”部分

新增

點擊此按鈕將會開啟一個對話方塊，您可以在其中將檔案或資料夾新增到受信任區域。

刪除

點擊此按鈕可以從排除項目清單中移除選定檔案或資料夾。

如果選取檔案或資料夾旁的核取方塊，則此按鈕可用。

檔案或資料夾

此列包含新增至受信任區域的檔案或資料夾。

狀態

此列中的切換開關可停用/啟用對新增至受信任區域的檔案或資料夾的掃描。

如果切換開關開啟，Kaspersky Endpoint Security 將不掃描對應的檔案或資料夾。

如果切換開關關閉，Kaspersky Endpoint Security 將掃描對應的檔案或資料夾。

註釋

有關新增至受信任區域的檔案或資料夾的資訊。

強制執行

當**強制執行**切換開關開啟時，Kaspersky Endpoint Security 禁止變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

當**強制執行**切換開關關閉時，Kaspersky Endpoint Security 允許變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

“新增排除項目”對話方塊

輸入檔案名稱、資料夾名稱或遮罩輸入欄位

將被排除在防護範圍之外的檔案或資料夾的路徑，或檔案/資料夾遮罩。

包含子資料夾

此核取方塊可啟用/停用掃描在**輸入檔案名稱、資料夾名稱或遮罩**欄位中指定的資料夾中的子資料夾。

如果選取此核取方塊，Kaspersky Endpoint Security 在惡意軟體掃描期間將不掃描指定資料夾的子資料夾。

如果清除此核取方塊，Kaspersky Endpoint Security 在惡意軟體掃描期間僅排除直接位於**輸入檔案名稱、資料夾名稱或遮罩**欄位中指定的資料夾中的檔案。指定資料夾的子資料夾將被掃描。

預設情況下已選擇此選擇方塊。

在**元件**部分中，您可以選擇不掃描指定檔案或資料夾的元件。

任何

掃描元件和檔案威脅防護元件都不會掃描指定的檔案或資料夾。

來自清單

此選項可讓您選擇元件。

檔案威脅防護

如果選取此核取方塊，檔案威脅防護元件將不會掃描指定的檔案或資料夾。
如果選擇**來自清單**選項，則此核取方塊可用。

掃描

如果選取此核取方塊，掃描元件將不會掃描指定的檔案或資料夾。
如果選擇**來自清單**選項，則此核取方塊可用。

注釋輸入欄位

有關新增至受信任區域的檔案或資料夾的資訊。

在**狀態**部分中，您可以選擇排除項目是否處於活動狀態。

已停用

Kaspersky Endpoint Security 掃描對應的檔案或資料夾。

已啟用

Kaspersky Endpoint Security 不掃描對應的檔案或資料夾。

“受信任區域”視窗：“受信任應用程式”部分

受信任應用程式清單

Kaspersky Endpoint Security 不會監控其網路活動的受信任應用程式清單。

新增

點擊此按鈕將開啟一個對話方塊，您可以在其中輸入 Kaspersky Endpoint Security 不會監控其網路活動的應用程式的路徑。

刪除

點擊此按鈕可以從清單中移除選擇的受信任應用程式。

如果選取受信任應用程式旁的核取方塊，則此按鈕可用。

應用程式

此列包含應用程式名稱或應用程式路徑的最後一段。

狀態

此列包含一個切換開關，指示對應用程式網路活動的監控狀態。

如果狀態為**已啟用**，則 Kaspersky Endpoint Security 不會監控對應應用程式的網路活動。

如果狀態為**已停用**，則 Kaspersky Endpoint Security 會監控對應應用程式的網路活動。

路徑

此列包含您手動新增的用戶端電腦上的應用程式路徑。

強制執行

當**強制執行**切換開關開啟時，Kaspersky Endpoint Security 禁止變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

當**強制執行**切換開關關閉時，Kaspersky Endpoint Security 允許變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

“新增應用程式”對話方塊

路徑輸入欄位

Kaspersky Endpoint Security 應用程式不會監控其網路或檔案活動的應用程式的路徑。

代碼簽章要求

Kaspersky Endpoint Security 不會監控其活動的應用程式的代碼簽章要求。

這是一個可選參數。

選項

在此部分中，您可以選擇不希望 Kaspersky Endpoint Security 應用程式監控的活動類型。

不監控檔案活動

此核取方塊可啟用/停用監控用戶端電腦上應用程式的檔案操作。

如果選取此核取方塊，Kaspersky Endpoint Security 不監控應用程式的檔案活動。

如果清除此核取方塊，Kaspersky Endpoint Security 將監控應用程式的檔案活動。

預設情況下已選擇此選擇方塊。

不監控網路活動

此核取方塊可啟用/停用對用戶端電腦上應用程式的入站和出站網際網路流量的監控。

如果選取此核取方塊，Kaspersky Endpoint Security 不監控應用程式的網路活動。

如果清除此核取方塊，Kaspersky Endpoint Security 將監控應用程式的網路活動。

預設情況下已選擇此選擇方塊。

“網路”視窗

在**代理伺服器設定**部分，您可以設定代理伺服器的使用以及用於連線到代理伺服器的設定。

不使用代理伺服器

如果選擇此選項，則 Kaspersky Endpoint Security 不使用代理伺服器連線到應用程式資料庫和模組的更新來源。

使用係統代理伺服器設定

如果選擇此選項，Kaspersky Endpoint Security 將使用在作業系統中配置的代理伺服器設定來連線到應用程式資料庫和模組的更新來源。

預設選擇此選項。

使用指定的代理伺服器設定

如果選擇此選項，Kaspersky Endpoint Security 將使用您指定的代理伺服器設定連線到應用程式資料庫和模組的更新來源。

位址

代理伺服器的 IP 位址或符號名稱。

如果選擇**使用指定的代理伺服器設定**”選項，則此欄位可用。

連接埠

代理伺服器連接埠號。

預設連接埠號為 8080。

如果選擇**使用指定的代理伺服器設定**”選項，則此欄位可用。

使用身分驗證

此核取方塊可啟用/停用當連線到代理伺服器時使用身分驗證。

如果選取此核取方塊，Kaspersky Endpoint Security 需要使用者憑證才能連線到代理伺服器。

如果清除此核取方塊，Kaspersky Endpoint Security 不需要使用者憑證即可連線到代理伺服器。

預設情況下已選擇此選擇方塊。

如果選擇**使用指定的代理伺服器設定**”選項，則此核取方塊可用。

使用者名稱

用於連線代理伺服器的使用者名稱。

如果選擇**使用指定的代理伺服器設定**選項和**使用身分驗證**核取方塊，則此欄位可用。

密碼

指定使用者名稱的密碼。

如果選擇**使用指定的代理伺服器設定**選項和**使用身分驗證**核取方塊，則此欄位可用。

顯示

點擊此按鈕將顯示您在**密碼**欄位中輸入的密碼字元。

本機位址不使用代理伺服器

此核取方塊可啟用/停用從本機或網路資料夾更新應用程式資料庫和模組時對代理伺服器的使用。

如果選中此核取方塊，Kaspersky Endpoint Security 從本機或網路資料夾更新應用程式資料庫和應用程式模組時，不使用代理伺服器。

如果清除此核取方塊，Kaspersky Endpoint Security 從本機或網路資料夾更新應用程式資料庫和應用程式模組時將使用代理伺服器。

預設情況下已選擇此選擇方塊。

如果選擇**使用指定的代理伺服器設定**"選項，則此核取方塊可用。

在**檢查安全連線**部分，您可以定義 Kaspersky Endpoint Security 是否掃描安全連線 (HTTPS)。

安全連線 (HTTPS) 檢查

安全連線 (HTTPS) 檢查切換開關可啟用/停用掃描透過 HTTPS 協定建立的安全連線，並在 Web 控制封鎖使用者存取危險 Web 資源時顯示通知。

如果**安全連線 (HTTPS) 檢查**切換開關已開啟，Kaspersky Endpoint Security 會執行下列操作：

- Web 威脅防護會掃描您的電腦在 Safari、Google Chrome 或 Firefox 中透過 HTTPS 協定傳送和接收的資料。
- 當使用者存取遠端電腦上 Web 控制封鎖的 Web 資源時，應用程式會顯示通知。

如果**安全連線 (HTTPS) 檢查**切換開關關閉，Kaspersky Endpoint Security 將執行下列操作：

- Web 威脅防護不會掃描您的電腦透過 HTTPS 協定傳送和接收的資料。
- 當使用者存取遠端電腦上 Web 控制封鎖的 Web 資源時，應用程式不會顯示通知。

此切換開關預設為開啟。

在**選擇供 Firefox 使用的憑證儲存**部分中，您可以選擇用於在 Mozilla Firefox 瀏覽器中檢查加密 HTTPS 流量的憑證儲存。

System Roots keychain (建議)

如果選擇此選項，Kaspersky Endpoint Security 將使用系統根 keychain 中的根憑證檢查 Mozilla Firefox 瀏覽器中的加密 HTTPS 流量。

預設選擇此選項。

來自 Mozilla Firefox 瀏覽器設定的憑證儲存

如果選擇此選項，Kaspersky Endpoint Security 將使用瀏覽器憑證儲存中的憑證。

在此情況下，您需要手動將 Kaspersky Endpoint Security 憑證新增至 Mozilla Firefox 瀏覽器的憑證儲存中。有關更多資訊，請參閱如何將卡巴斯基憑證新增至 Mozilla Firefox 憑證儲存。

在**受信任的根憑證**部分中，您可以管理受信任的根憑證清單。

管理受信任的根憑證

點擊此連接將開啟一個視窗，您可以在其中建立一個受信任的根憑證清單，无需通知即可連線到相應的伺服器。

在**被監控的連接埠**部分中，您可以設定 Kaspersky Endpoint Security 監控的連接埠。

所選連接埠

點擊此連接將開啟一個視窗，您可以在其中配置 Kaspersky Endpoint Security 監控的連接埠清單。

強制執行

當**強制執行**切換開關開啟時，Kaspersky Endpoint Security 禁止變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

當**強制執行**切換開關關閉時，Kaspersky Endpoint Security 允許變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

“管理受信任的根憑證”視窗

新增

點擊此按鈕將開啟一個對话方塊，用於新增將被視為受信任的憑證。

刪除

點擊此按鈕可將選定憑證從清單中刪除。

受信任憑證清單

一個顯示受信任根憑證的名稱的清單。

預設情況下該清單為空。

強制執行

當**強制執行**切換開關開啟時，Kaspersky Endpoint Security 禁止變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

當**強制執行**切換開關關閉時，Kaspersky Endpoint Security 允許變更本機電腦上的工作設定、應用程式設定、子群組政策和從屬管理伺服器的值。

“受監控連接埠”視窗

受監控連接埠清單

您可以為其配置傳輸資料監控的連接埠清單。

預設情況下，連接埠清單包含最常見服務經常使用的連接埠。

新增

點擊此按鈕將開啟一個對話方塊，您可以在其中新增要由 Kaspersky Endpoint Security 監控的連接埠。

刪除

點擊此按鈕可將選定連接埠從清單中刪除。

如果選取連接埠旁的核取方塊，則此按鈕可用。

連接埠

此列包含連接埠號。

狀態

此列包含一個切換開關，指示對透過連接埠傳輸的資料的監控狀態。

如果狀態為**已監控**，則 Kaspersky Endpoint Security 會掃描透過對應連接埠傳輸的流量。

如果狀態為**未監控**，則 Kaspersky Endpoint Security 不會掃描透過對應連接埠傳輸的流量。

敘述

此列包含連接埠的敘述。

“新增連接埠”對話方塊

連接埠輸入欄位

您希望 Kaspersky Endpoint Security 為其掃描所傳輸資料的連接埠號。

敘述輸入欄位

有關連接埠的附加資訊，例如連接埠類型。

“產品授權資訊”視窗

在**產品授權資訊**視窗中，您可以檢視有關產品授權的資訊，包括其到期日期、可以在該產品授權下使用 Kaspersky Endpoint Security 的電腦數量以及產品授權類型。

新增為備用金鑰

此核取方塊可啟用/停用將特定金鑰檔案或啟動碼新增為備用金鑰。

如果選取此核取方塊，Kaspersky Endpoint Security 將把指定的金鑰檔案或啟動碼新增為備用金鑰。

如果清除此核取方塊，Kaspersky Endpoint Security 將把指定的金鑰檔案或啟動碼新增為活動金鑰。

預設情況下已清空此核取方塊。

“掃描”視窗

掃描範圍

點擊此連接可開啟一個視窗，您可在其中建立掃描範圍。

在**如果偵測到惡意物件**部分中，您可以選擇 Kaspersky Endpoint Security 在偵測到感染物件時執行的操作。

提示使用者在掃描後採取行動

在掃描完成之前，Kaspersky Endpoint Security 不會處理物件。此時，Kaspersky Endpoint Security 會顯示一條通知，其中包含有關每個感染物件的資訊，並提示使用者選擇要採取的操作。可用選項取決於物件的類型。

預設選擇此選項。

提示使用者立即採取行動

Kaspersky Endpoint Security 會顯示一條通知，其中包含有關應用程式偵測的每個感染物件的資訊，並提示使用者選擇進一步的操作。可用選項取決於物件的類型。

不提示採取行動

Kaspersky Endpoint Security 會在報告中記錄有關偵測到的物件的資訊，而不對其進行處理。

自動解毒

此核取方塊可啟用/停用 Kaspersky Endpoint Security 解毒偵測到的感染物件，而不提示使用者確認。

如果勾選此核取方塊，Kaspersky Endpoint Security 會自動解毒受感染的物件。

如果清除此核取方塊，Kaspersky Endpoint Security 將跳過受感染的物件。

如果選擇**不提示採取行動**選項，則此核取方塊可用。

預設情況下已選擇此選擇方塊。

解毒；若解毒失敗則刪除

此核取方塊可啟用/停用在嘗試解毒失敗後移除受感染或可能受感染的物件。

如果選取此核取方塊，Kaspersky Endpoint Security 會自動移除無法被解毒的感染物件。

如果清除此核取方塊，則 Kaspersky Endpoint Security 不會移除無法被解毒的感染物件。

如果選擇**不提示採取行動**選項並選擇**自動解毒**核取方塊，則此核取方塊會顯示。

預設情況下已選擇此選擇方塊。

在**檔案類型**部分，您可以選擇 Kaspersky Endpoint Security 掃描的檔案格式。

掃描所有檔案

Kaspersky Endpoint Security 掃描所有被執行、開啟或儲存的檔案系統物件。

按內容掃描應用程式和文件

Kaspersky Endpoint Security 僅根據檔案格式掃描可能被感染的物件。

檔案格式清單由卡巴斯基定義，是 Kaspersky Endpoint Security 資料庫的一部分。

按延伸程式掃描應用程式和文件

Kaspersky Endpoint Security 僅掃描可能被感染的物件（根據其副檔名）。

檔案副檔名清單由卡巴斯基定義，是 Kaspersky Endpoint Security 資料庫的一部分。

Kaspersky Endpoint Security 總是掃描不含副檔名的檔案。

在**最佳化**部分中，您可以設定掃描效能。

只掃描新增及修改的檔案

此核取方塊可啟用/停用僅掃描 Kaspersky Endpoint Security 識別為新檔案或自上次掃描以來已修改的檔案。

如果選取此核取方塊，Kaspersky Endpoint Security 將僅掃描其識別為新檔案或自上次掃描以來已修改的檔案。

如果清除該核取方塊，Kaspersky Endpoint Security 將掃描所有檔案。

略過掃描唯讀系統磁區

該核取方塊可停用/啟用 Kaspersky Endpoint Security 掃描唯讀系統磁碟區。

如果選擇此核取方塊，Kaspersky Endpoint Security 將不掃描唯讀系統磁碟區。這可大大縮短掃描時間。

如果清除此核取方塊，Kaspersky Endpoint Security 將掃描唯讀系統磁碟區。

預設情況下已選擇此選擇方塊。

跳過大於 <值> MB 的檔案

此核取方塊可啟用/停用從掃描中排除大於指定大小的檔案。

如果選取此核取方塊，Kaspersky Endpoint Security 將跳過大於指定大小的檔案。

如果清除此核取方塊，則無論檔案大小為何 Kaspersky Endpoint Security 都會掃描檔案。

預設情況下已清空此核取方塊。

預設情況下，大小設定為 100 MB。

如果掃描時間超過 秒則跳過

此核取方塊可啟用/停用檔案掃描持續時間的限制。如果掃描檔案超過指定的時間限制，Kaspersky Endpoint Security 將跳過該檔案。

如果選取此核取方塊，當掃描檔案超過指定時間限制時，Kaspersky Endpoint Security 將跳過該檔案。

如果清除此核取方塊，無論掃描可能需要多長時間Kaspersky Endpoint Security 都將掃描檔案。

預設值是 30 秒。

在**複合檔案**部分，您可以選擇 Kaspersky Endpoint Security 掃描的複合檔案類型。

掃描存檔

此核取方塊可啟用/停用壓縮檔案掃描。

如果勾選此核取方塊，Kaspersky Endpoint Security 將掃描壓縮檔案。

如果清除此核取方塊，Kaspersky Endpoint Security 將在掃描期間跳過壓縮檔案。

所有

Kaspersky Endpoint Security 將掃描所有檔案。

如果選取**掃描存檔**核取方塊，則此選項可用。

僅新建

Kaspersky Endpoint Security 將僅掃描新壓縮檔案。

如果選取**掃描存檔**核取方塊，則此選項可用。

掃描受密碼防護的存檔

此核取方塊可啟用/停用掃描受密碼防護的壓縮檔案。

如果勾選此核取方塊，Kaspersky Endpoint Security 將掃描受密碼防護的檔案。

如果清除此核取方塊，Kaspersky Endpoint Security 將在掃描期間跳過受密碼防護的檔案。

掃描嵌入的 OLE 物件

此核取方塊可啟用/停用掃描檔案中嵌入的物件，例如 Excel 電子表格、巨集或電子郵件附件。

如果勾選此核取方塊，Kaspersky Endpoint Security 將掃描嵌入的 OLE 物件。

如果清除此核取方塊，Kaspersky Endpoint Security 將在掃描期間跳過嵌入的 OLE 物件。

所有

Kaspersky Endpoint Security 將掃描所有 OLE 物件。

如果選取**掃描嵌入的 OLE 物件**核取方塊，則此選項可用。

僅新建

Kaspersky Endpoint Security 將僅掃描新的嵌入 OLE 物件。

如果選取**掃描嵌入的 OLE 物件**核取方塊，則此選項可用。

掃描電子郵件格式檔案

此核取方塊可啟用/停用掃描電子郵件格式的檔案和電子郵件資料庫。

如果勾選此核取方塊，Kaspersky Endpoint Security 將掃描電子郵件格式的檔案和電子郵件資料庫。

如果清除此核取方塊，Kaspersky Endpoint Security 將在掃描期間跳過電子郵件格式的檔案和電子郵件資料庫。

“掃描範圍”視窗

新增

點擊此按鈕將開啟一個對話方塊，您可以在其中指定要新增至掃描範圍的檔案、資料夾或檔案/資料夾遮罩。

刪除

按一下該按鈕將從掃描範圍中移除物件。

如果選取物件旁邊的核取方塊，則此按鈕可用。

您無法刪除掃描範圍中包含的預設物件。

掃描範圍

此列包含惡意軟體掃描期間掃描的物件。

狀態

此列中的切換開關可啟用/停用掃描新增至掃描範圍的物件。

如果此切換開關開啟，Kaspersky Endpoint Security 將掃描對應的物件。

如果此切換開關關閉，Kaspersky Endpoint Security 將不會掃描對應的物件。

附加

此列指示 Kaspersky Endpoint Security 是否掃描對應物件的子資料夾。

注意： Kaspersky Endpoint Security 不會掃描位於 OneDrive 或 iCloud 儲存或其他雲端儲存中的檔案。請將這些檔案從掃描範圍中排除。否則，掃描工作可能會以*受感染檔案未刪除*錯誤結束。

“新增掃描範圍”對話方塊

輸入檔案名稱、資料夾名稱或遮罩

檔案、資料夾或檔案/資料夾遮罩的路徑。

物件是資料夾

此核取方塊可啟用/停用將物件作為資料夾來掃描。

如果勾選此核取方塊，Kaspersky Endpoint Security 會將您在**輸入檔案名稱、資料夾名稱或遮罩**欄位中指定的物件作為資料夾來掃描。

如果清除此核取方塊，Kaspersky Endpoint Security 會將您在**輸入檔案名稱、資料夾名稱或遮罩**欄位中指定的物件作為檔案來掃描。

預設情況下已選擇此選擇方塊。

包含子資料夾

此核取方塊可啟用/停用掃描在**輸入檔案名稱、資料夾名稱或遮罩**欄位中指定的資料夾中的子資料夾。

如果選取此核取方塊，Kaspersky Endpoint Security 將在惡意軟體掃描期間掃描子資料夾。

如果清除此核取方塊，Kaspersky Endpoint Security 在惡意軟體掃描期間僅掃描直接位於**輸入檔案名稱、資料夾名稱或遮罩**欄位中指定的資料夾中的檔案。

預設情況下已選擇此選擇方塊。

注意： Kaspersky Endpoint Security 不會掃描位於 OneDrive 或 iCloud 儲存或其他雲端儲存中的檔案。請將這些檔案從掃描範圍中排除。否則，掃描工作可能會以*受感染檔案未刪除*錯誤結束。

檔案參數視窗

以下類型的檔案雜湊受支援：

- **MD5**
  這種類型的雜湊必須為 32 個字元長，並包含 0-9、af、AF。
- **SHA256**
  這種類型的雜湊必須為 64 個字元長，並包含 0-9、af、AF。