

kaspersky

Kaspersky Endpoint Security 10 Service Pack 2 for Windows

© 2022 AO Kaspersky Lab

目錄

[關於 Kaspersky Endpoint Security 10 Service Pack 2 for Windows](#)

[新聞](#)

[分發套件](#)

[組織電腦防護](#)

[硬體和軟體需求](#)

[安裝和移除應用程式](#)

[安裝程式](#)

[程式安裝方法](#)

[使用安裝精靈安裝程式](#)

[步驟 1. 確認電腦符合安裝需求](#)

[步驟 2. 安裝過程的歡迎頁面](#)

[步驟 3. 檢視產品授權協議](#)

[步驟 4. 選取安裝類型](#)

[步驟 5. 選取要安裝的程式元件](#)

[步驟 6. 選取目的資料夾](#)

[步驟 7. 新增物件排除病毒掃描](#)

[步驟 8. 應用程式安裝的準備工作](#)

[步驟 9. 安裝應用程式](#)

[透過命令列安裝程式](#)

[使用系統中心設定管理器遠端安裝應用程式](#)

[setup.ini 檔案安裝設定說明](#)

[初始化設定精靈](#)

[啟動應用程式](#)

[使用啟動碼啟動](#)

[使用授權檔案啟動](#)

[選擇啟動功能](#)

[完成啟動](#)

[分析作業系統](#)

[完成應用程式的初始化配置](#)

[卡巴斯基安全網路聲明](#)

[升級舊版本程式的方法](#)

[移除程式](#)

[移除程式的方法](#)

[使用安裝精靈移除程式](#)

[步驟 1. 儲存程式資料以備後用](#)

[步驟 2. 確認應用程式移除](#)

[步驟 3. 移除應用程式。完成移除](#)

[透過命令列移除程式](#)

[刪除測試執行身分驗證代理後的剩餘物件與資料](#)

[程式介面](#)

[工作列通知區域中的程式圖示](#)

[應用程式圖示的右鍵選單](#)

[應用程式主視窗](#)

[配置應用程式設定標籤](#)

[應用程式防護和控制頁籤](#)

[應用程式產品授權](#)

[關於最終使用者產品授權協議](#)

[關於產品授權](#)

[關於產品授權憑證](#)

[關於訂購](#)

[關於啟動碼](#)

[關於產品授權](#)

[關於產品授權檔案](#)

[關於資料提交](#)

[檢視產品授權資訊](#)

[購買產品授權](#)

[續約授權](#)

[續約訂購](#)

[存取服務提供者網站](#)

[關於程式啟動方法](#)

[使用啟動精靈啟動程式](#)

[透過命令列啟動程式](#)

[啟動和停止應用程式](#)

[啟動和停用應用程式自動啟動](#)

[手動啟動和停止程式](#)

[暫停和還原電腦防護和控制](#)

[防護電腦檔案系統檔案防護](#)

[關於檔案防護](#)

[啟用和停用檔案防護](#)

[自動暫停檔案防護](#)

[設定檔案防護](#)

[變更安全防護等級](#)

[變更檔案防護對受感染檔案執行的操作](#)

[編輯檔案防護的防護範圍](#)

[配合啟發式分析使用檔案防護](#)

[在檔案防護操作中使用掃描技術](#)

[最佳化檔案掃描](#)

[掃描複合檔案](#)

[變更掃描模式](#)

[電子郵件防護。郵件防護](#)

[關於郵件防護](#)

[啟動和停用郵件防護](#)

[設定郵件防護](#)

[變更郵件安全防護等級](#)

[變更對受感染電子郵件採取的操作](#)

[編輯郵件防護的防護範圍](#)

[掃描附加於電子郵件中的複合檔案](#)

[篩選電子郵件附件](#)

[掃描 Microsoft Office Outlook 中的電子郵件](#)

[設定在 Outlook 中的郵件掃描](#)

[使用卡巴斯基安全管理中心設定郵件掃描](#)

[電腦的網際網路防護網頁防護](#)

[關於網頁防護](#)

[啟用和停用網頁防護](#)

[設定網頁防護](#)

[變更網頁流量安全等級](#)

[變更對惡意網路流量物件採取的操作](#)

[根據可疑及釣魚網站資料庫掃描網址](#)

[搭配啟發式分析使用網頁防護](#)

[編輯受信任網址清單](#)

[防護即時通訊用戶端流量。即時通訊防護](#)

[關於即時通訊防護](#)

[啟用和停用即時通訊防護](#)

[配置即時通訊防護](#)

[建立即時通訊防護的防護範圍](#)

[使用即時通訊防護根據惡意和釣魚網址資料庫掃描網址](#)

[系統監控](#)

[關於系統監控](#)

[啟用和停用系統監控](#)

[設定系統監控](#)

[啟用或停用弱點防護](#)

[選擇程式中偵測到惡意活動時的操作](#)

[啟動或停用解毒期間回溯惡意操作](#)

[防火牆](#)

[關於防火牆](#)

[啟用或停用防火牆](#)

[關於網路規則](#)

[關於網路連線狀態](#)

[變更網路連線狀態](#)

[管理網路封包規則](#)

[建立和編輯網路封包規則](#)

[啟動或停用網路封包規則](#)

[更改網路封包規則的防火牆操作](#)

[更改網路封包規則的優先順序](#)

[管理應用程式網路規則](#)

[建立和編輯應用程式網路規則](#)

[啟用和停用應用程式網路規則](#)

[變更應用程式網路規則的防火牆操作](#)

[變更應用程式網路規則的優先順序](#)

[網路監控](#)

[關於網路監控](#)

[啟動網路監控](#)

[網路攻擊防護](#)

[關於網路攻擊防護](#)

[啟動或停用網路攻擊防護](#)

[網路攻擊防護設定](#)

[編輯用於封鎖攻擊電腦的設定](#)

[設定排除在封鎖外的位址](#)

[BadUSB 攻擊防護](#)

[關於 BadUSB 攻擊防護](#)

[安裝 BadUSB 攻擊防護元件](#)

[啟用和停用 BadUSB 攻擊防護。](#)

[允許和禁止使用螢幕鍵盤進行授權](#)

[鍵盤授權](#)

[應用程式啟動控制](#)

[關於應用程式啟動控制](#)

[啟用和停用應用程式啟動控制](#)

[應用程式啟動控制功能限制](#)

[關於應用程式啟動控制規則](#)

[管理應用程式啟動控制規則](#)

[新增和編輯應用程式啟動控制規則](#)

[為應用程式啟動控制規則新增觸發條件](#)

[變更應用程式啟動控制規則的狀態](#)

[測試應用程式啟動控制規則](#)

[編輯應用程式啟動控制訊息範本](#)

[關於應用程式啟動控制的操作模式](#)

[選取應用程式啟動控制模式](#)

[使用卡巴斯基安全管理中心管理應用程式啟動控制規則](#)

[收集關於安裝在區域網路電腦上的應用程式資訊](#)

[建立應用程式類別](#)

[使用卡巴斯基安全管理中心建立應用程式啟動控制規則](#)

[使用卡巴斯基安全管理中心變更應用程式啟動控制規則的狀態](#)

[應用程式權限控制](#)

[關於應用程式權限控制](#)

[音訊和視頻裝置控制限制](#)

[啟用和停用應用程式權限控制](#)

[管理應用程式信任群組](#)

[配置將應用程式分配到信任群組的設定](#)

[修改信任群組](#)

[選取在 Kaspersky Endpoint Security 啟動之前啟動的應用程式受信任群組](#)

[管理應用程式控制規則](#)

[變更受信任群組和應用程式群組的應用程式控制規則](#)

[編輯應用程式控制規則](#)

[從卡巴斯基安全網路資料庫下載和更新應用程式控制規則](#)

[停用繼承父程序限制](#)

[從應用程式控制規則中排除特定的應用程式操作](#)

[刪除過時的應用程式控制規則](#)

[防護作業系統資源和身分資料](#)

[新增受防護資源的類別](#)

[新增受防護資源](#)

[停用資源防護](#)

[弱點監控](#)

[關於弱點監控](#)

[啟用和停用弱點監控](#)

[裝置控制](#)

[關於裝置控制](#)

[啟用和停用裝置控制](#)

[關於存取裝置和連接介面的規則](#)

[關於信任的裝置](#)

[關於對裝置存取權限的決定標準](#)

[編輯裝置存取規則](#)

[在事件記錄中新增或排除記錄](#)

[將 Wi-Fi 網路新增至受信任清單](#)

[編輯連接介面存取規則](#)

[對信任的裝置的操作](#)

[在應用程式介面中向信任清單新增裝置](#)

[基於裝置型號或 ID 將裝置新增至信任清單](#)

[基於裝置 ID 遮罩將裝置新增至信任清單](#)

[設定使用者對信任的裝置的存取權限](#)

[從信任裝置的清單中刪除裝置](#)

[編輯裝置控制訊息範本](#)

[獲得存取被封鎖裝置的權限](#)

[使用卡巴斯基安全管理中心建立存取被封鎖裝置的金鑰](#)

[網頁控制](#)

[關於網頁控制](#)

[啟動和停用網頁控制](#)

[網頁資源內容類別](#)

[關於網路資源存取規則](#)

[網路資源存取規則操作](#)

[新增和編輯網頁存取規則](#)

[為網頁存取規則分配優先順序](#)

[測試網頁存取規則](#)

[啟動和停用網頁存取規則](#)

[從舊版本應用程式遷移網頁資源存取規則](#)

[匯出和匯入網頁資源位址清單](#)

[編輯網頁資源位址的遮罩](#)

[編輯網頁控制訊息範本](#)

[KATA Endpoint Sensor](#)

[關於 KATA Endpoint Sensor](#)

[啟用和停用 KATA Endpoint Sensor 元件](#)

[資料加密](#)

[啟用在卡巴斯基安全管理中心政策中實現加密設置](#)

[關於資料加密](#)

[加密功能限制](#)

[變更加密演算法](#)

[啟用單點登入 \(SSO\) 技術](#)

[檔案加密特殊考慮](#)

[加密本機電腦磁碟中的檔案](#)

[加密本機電腦磁碟中的檔案](#)

[為應用程式建立加密檔案存取規則](#)

[加密特定應用程式建立或修改的檔案](#)

[生成解密規則](#)

[在本機電腦磁碟機上解密檔案](#)

[建立加密資料](#)

[解壓縮加密資料](#)

[加密卸除式磁碟](#)

[啟動卸除式磁碟機加密](#)

[新增卸除式磁碟加密規則](#)

[編輯卸除式磁碟的加密規則](#)

[啟用攜帶模式存取卸除式磁碟上的加密檔案](#)

[解密卸除式磁碟](#)

加密硬碟

[關於硬碟加密](#)

[使用 Kaspersky Disk Encryption 技術加密硬碟](#)

[使用 BitLocker 磁碟機加密技術加密硬碟](#)

[建立硬碟加密排除清單](#)

[硬碟解密](#)

管理身分驗證代理

[配合身分驗證代理使用令牌和智慧卡](#)

[編輯身分驗證代理說明郵件](#)

[身分驗證代理說明郵件中字串的有限支援](#)

[選取身分驗證代理偵錯等級](#)

[管理身分驗證代理帳戶](#)

[新增用於建立身分驗證代理帳戶的指令](#)

[選取身分驗證代理帳戶編輯指令](#)

[新增用於刪除身分驗證代理帳戶的指令](#)

[還原身分驗證代理帳戶憑證](#)

[回應使用者請求以還原身分驗證代理帳戶憑證](#)

檢視資料加密詳細資訊

[關於加密狀態](#)

[檢視加密狀態](#)

[在卡巴斯基安全管理中心的詳細視窗中檢視加密統計資訊](#)

[檢視本機電腦磁碟機上檔案加密錯誤](#)

[檢視資料加密報告](#)

管理加密檔案與檔案加密功能限制

[不連接卡巴斯基安全管理中心存取加密檔案](#)

[授予使用者在不連線卡巴斯基安全管理中心時存取加密檔案的權限](#)

[編輯加密檔案存取訊息範本](#)

無法存取加密裝置時的裝置使用

[透過應用程式介面獲得加密裝置的存取權限](#)

[授予使用者存取加密裝置的權限](#)

[為使用者提供使用 BitLocker 加密的硬碟磁碟機還原金鑰](#)

[建立還原實用工具的可執行檔](#)

[使用“還原實用工具”還原加密裝置上的資料](#)

[回應使用者請求以還原加密裝置上的資料](#)

作業系統故障後還原對加密檔案的存取

建立作業系統緊急修復光碟

網路防護

[關於網路防護](#)

[設定網路流量監控設定](#)

[啟動對所有網路連接埠的監控](#)

[建立受監控網路連接埠的清單](#)

[建立所有網路連接埠受監控的應用程式清單](#)

更新資料庫和程式模組

[關於資料庫和程式模組更新](#)

[關於更新來源](#)

[調整更新設定](#)

[新增更新來源](#)

[選擇更新資料庫區域](#)

[設定從共用資料夾更新](#)

[選取更新工作執行模式](#)

[在不同使用者帳戶權限下開始更新工作](#)

[設定應用程式模組更新](#)

[開始和停止更新工作](#)

[回溯上次更新](#)

[配置代理伺服器設定](#)

[掃描電腦](#)

[關於掃描工作](#)

[開始或停止掃描工作](#)

[設定掃描工作設定](#)

[變更安全防護等級](#)

[變更對受感染檔案執行的操作](#)

[產生要掃描的物件清單](#)

[選取要掃描的檔案類型](#)

[最佳化檔案掃描](#)

[掃描複合檔案](#)

[選擇掃描方式](#)

[使用掃描技術](#)

[選取掃描工作執行模式](#)

[使用不同使用者帳戶啟動掃描工作](#)

[掃描連線到電腦的卸除式磁碟](#)

[處理未處理的檔案](#)

[關於未處理的檔案](#)

[管理未處理檔案清單](#)

[啟動未處理檔案自訂掃描](#)

[刪除未處理檔案清單中的檔案](#)

[弱點掃描](#)

[檢視執行中應用程式的弱點資訊](#)

[關於弱點掃描工作](#)

[啟動或停止弱點掃描工作](#)

[配置弱點掃描設定](#)

[建立弱點掃描範圍](#)

[選取弱點掃描工作的執行模式](#)

[使用不同使用者帳戶的權限啟動弱點掃描工作](#)

[管理弱點清單](#)

[關於弱點清單](#)

[再次啟動弱點掃描工作](#)

[修復弱點](#)

[隱藏弱點清單中的項目](#)

[按嚴重性等級篩選弱點清單](#)

[按已修復和隱藏狀態值篩選弱點清單](#)

[檢查應用程式模組的完整性](#)

[關於完整性檢查工作](#)

[啟動或停止完整性檢查工作](#)

[選取完整性檢查工作的執行模式](#)

[管理報告](#)

[管理報告的原則](#)

[配置報告設定](#)

[設定最大報告儲存時間](#)

[設定報告檔案的最大容量](#)

[檢視報告](#)

[檢視報告中的事件資訊](#)

[將報告儲存到檔案](#)

[清理報告](#)

[通知服務](#)

[關於 Kaspersky Endpoint Security 通知](#)

[設定通知服務](#)

[設定事件日誌設定](#)

[設定通知的顯示和傳送](#)

[設定應用程式狀態警告在通知區域的顯示](#)

[管理隔離區和備份區](#)

[關於隔離區和備份區](#)

[配置隔離區和備份區設定](#)

[設定備份和隔離區檔案儲存最長時間](#)

[設定隔離區和備份區的最大容量](#)

[管理隔離區](#)

[啟用和禁用更新後掃描隔離區中的檔案](#)

[啟動隔離區檔案自訂掃描](#)

[從隔離區中還原檔案](#)

[從隔離區中刪除檔案](#)

[管理備份](#)

[從備份區中還原檔案](#)

[從備份區中刪除檔案副本備份。](#)

[進階程式設定](#)

[建立和使用設定檔](#)

[信任區域](#)

[關於信任區域](#)

[建立掃描排除項目](#)

[修改掃描排除項目](#)

[刪除掃描排除項目](#)

[啟用和停用掃描排除項目](#)

[編輯信任應用程式清單](#)

[為受信任應用程式清單中的應用程式啟用或停用受信任區域規則](#)

[使用受信任的系統憑證儲存](#)

[Kaspersky Endpoint Security 自我防護](#)

[關於 Kaspersky Endpoint Security 自我防護](#)

[啟用或停用自我防護](#)

[啟用或停用遠端控制防護](#)

[支援遠端管理應用程式](#)

[Kaspersky Endpoint Security 效能以及與其他應用程式的相容性](#)

[關於 Kaspersky Endpoint Security 效能以及與其他應用程式的相容性](#)

[選擇可偵測的威脅類型](#)

[啟用或停用進階解毒技術 \(工作站 \)](#)

[啟用或停用進階解毒技術 \(檔案伺服器 \)](#)

[啟用或停用省電模式](#)

[啟用或停用允許其他應用程式使用資源](#)

[密碼防護](#)

[關於存取 Kaspersky Endpoint Security 的限制](#)

[啟用和停用密碼防護](#)

[修改 Kaspersky Endpoint Security 存取密碼](#)

[關於使用暫時密碼](#)

[使用卡斯基安全管理中心管理主控台建立暫時密碼](#)

[在 Kaspersky Endpoint Security 介面中應用暫時密碼](#)

[透過卡斯基安全管理中心遠端系統管理](#)

[關於透過卡斯基安全管理中心管理應用程式](#)

[使用其他版本管理外掛程式時的特別考慮](#)

[啟動和停止用戶端電腦上的應用程式](#)

[設定 Kaspersky Endpoint Security 設定](#)

[管理工作](#)

[關於 Kaspersky Endpoint Security 工作](#)

[設定工作管理模式](#)

[建立本機工作](#)

[建立群組工作](#)

[為裝置集合建立工作](#)

[啟動、停止、暫停和還原工作](#)

[編輯工作設定](#)

[管理政策](#)

[關於政策](#)

[建立政策](#)

[編輯政策設定](#)

[選取要顯示在卡斯基安全管理中心政策中的設定](#)

[將使用者訊息傳送至卡斯基安全管理中心伺服器](#)

[在卡斯基安全管理中心事件儲存中檢視使用者訊息](#)

[加入卡斯基安全網路](#)

[關於加入卡斯基安全網路](#)

[啟用和停用卡斯基安全網路](#)

[檢查與卡斯基安全網路的連線](#)

[在卡斯基安全網路中檢查檔案信譽](#)

[使用卡斯基安全網路增強防護](#)

[關於應用程式的資訊源](#)

[聯絡技術支援](#)

[如何取得技術支援](#)

[電話技術支援](#)

[透過 Kaspersky CompanyAccount 取得技術支援](#)

[為技術支援部門收集資訊](#)

[建立偵錯檔案](#)

[偵錯檔案的內容和儲存](#)

[啟用和停用提示向卡斯基實驗室發送傾印和偵錯檔案](#)

[將檔案傳送給技術支援伺服器](#)

[啟用和停用防護傾印檔案和偵錯檔案](#)

詞彙表

[OLE 物件](#)

[位址黑名單](#)

[備份](#)

[備用授權](#)

[受信任平台模組](#)

[受感染的檔案](#)

[可感染檔案](#)

[可疑網頁位址資料庫](#)

[存檔](#)

[將檔案移至隔離區](#)

[工作](#)

[工作設定](#)

[憑證](#)

[憑證指紋](#)

[憑證物件](#)

[憑證發佈者](#)

[應用程式設定](#)

[掃描範圍](#)

[授權憑證](#)

[攜帶式檔案管理器。](#)

[攻擊](#)

[啟動授權](#)

[啟發式分析](#)

[更新](#)

[檔案遮罩](#)

[特徵碼分析](#)

[疑似受感染的檔案](#)

[病毒資料庫](#)

[程式模組](#)

[管理伺服器](#)

[管理群組](#)

[網路代理](#)

[網路代理連線程式。](#)

[網路服務](#)

[網路釣魚](#)

[網頁資源位址的正規表示式](#)

[補丁](#)

[解毒](#)

[誤報](#)

[身分驗證代理](#)

[釣魚網頁位址資料庫](#)

[防護範圍](#)

[隔離](#)

[有關協力廠商代碼的資訊](#)

[商標聲明](#)

關於 Kaspersky Endpoint Security 10 Service Pack 2 for Windows

該部分將說明 Kaspersky Endpoint Security 的功能、元件和安裝套件，並提供安裝 Kaspersky Endpoint Security 所需的硬體和軟體清單。

新聞

Kaspersky Endpoint Security 10 Service Pack 2 for Windows 提供了以下功能和提升：

1. 應用程式啟動控制：

- 支援伺服器作業系統
- 控制 DLL 模組和驅動程式的下載。
- 管理清查工作中的物件清單（DLL 模組和指令碼檔案）。
- 基於新標準控制物件 - 按數位簽章憑證的內容。
- 產生有關被封鎖應用程式測試驅動的報告。
- 支援兩種應用程式啟動控制執行模式：“黑名單”和“白名單”。
- 使用沙 256 雜湊值控制和清查物件。
- 從 PowerShell 解釋器控制指令碼執行。
- 使用受信任的系統憑證儲存。

2. Microsoft BitLocker 管理借助 Microsoft 的 BitLocker 技術啟用硬碟磁碟機加密：

- 遠端管理加密。
- 監控加密裝置。
- 建立裝置加密報告。
- 還原對加密裝置的存取。

3. Kaspersky Disk Encryption：

- 支援使用虛擬鍵盤在身分驗證代理預啟動環境中輸入憑證。
- 支援僅加密裝置上已佔空間的加密模式。
- 支援加密平板電腦 (MS Surface 版本 3 和 4)。

4. 應用程式權限控制：

- 控制應用程式對音訊和視頻錄製裝置的存取。

5. 網頁控制：

- 組態其他類別網路資源的網路資源存取規則。

6. 裝置控制：

- 在 USB 裝置上記錄與刪除和儲存檔案相關的事件。
- 基於以下設定產生受信任 W-Fi 網路清單：名稱、加密類型和身分驗證類型。
- 管理使用者對於 CD/DVD 光碟上檔案讀寫操作的存取權限。

7. 郵件防護：

- 能夠刪除和重新命名郵件防護要掃描的壓縮檔案內的指定類型的檔案。

8. 卡巴斯基安全網路：

- 在 Kaspersky Endpoint Security 報告和卡巴斯基安全管理中心報告中顯示 KSN 為物件處理方法決定的原因。
- 向 KSN 傳送有關選定檔案聲譽的查詢。
- 對於已安裝 Kaspersky Endpoint Security 的用戶端電腦，顯示 KSN 伺服器的可用狀態。

分發套件

Kaspersky Endpoint Security 安裝套件包含以下檔案：

- 透過任何可用方式[安裝程式](#)所需的檔案：
- 更新應用程式安裝期間使用的安裝套件檔案。
- 透過卡巴斯基安全管理中心安裝 Kaspersky Endpoint Security 管理外掛程式的 klcfginst.msi 檔案。
- ksn_<language ID>.txt 檔案，您可以透過其檢視[參與卡巴斯基安全網路](#)的條款。
- license.txt 檔案，您可以透過其檢視[最終使用者產品授權協議](#)。
- incompatible.txt 檔包含了不相容檔案的清單。
- 包含安裝套件內部設定的 installer.ini 檔案。

不建議變更這些設定的值。如果您希望變更安裝選項，請使用 [setup.ini 檔案](#)。

您必須解壓縮安裝套件才能存取這些檔案。

組織電腦防護

Kaspersky Endpoint Security 為電腦提供綜合性防護，封鎖各種類型的威脅、網路和釣魚攻擊、垃圾郵件以及其他不受信任的內容。

每種類型的威脅是由專門的元件處理。各個元件均能夠獨立啟用或停用，並可調整設定。

除了應用程式元件提供的即時防護外，我們建議您定期 *掃描* 電腦病毒和其他威脅。這有助於排除防護元件因安全防護等級設定過低或者其他原因而尚未偵測到的惡意程式傳播可能性。

為維持最新 Kaspersky Endpoint Security 的更新版本，您必須 *更新* 應用程式資料庫和模組。在預設設定下，應用程式將會自動更新，但視情況所需，您亦可手動更新資料庫和應用程式模組。

下列為應用程式的控制元件：

- **應用程式啟動控制**。此元件可記錄使用者啟動應用程式和管理應用程式啟動的操作。
- **應用程式權限控制**。此元件可記錄應用程式在作業系統中的行為，並根據信任的應用程式群組管理應用程式活動。每各應用程式均有可指定相關規則。這些規則將管理應用程式存取使用者個人資料和作業系統資源。這些資料封包括使用者檔案（“我的檔案”資料夾、cookies、使用者活動資訊）和檔案、資料夾、含有常用應用程式設定和重要資訊的登錄檔項目。
- **弱點監控**。弱點監控元件對使用者電腦上啟動或正在執行的應用程式進行即時弱點掃描。
- **裝置控制**。此元件可讓您對資料存放裝置（例如硬碟、卸除式磁碟、磁帶機、CD/DVD）、資料傳輸裝置（例如數據機）、將資訊轉為實體的裝置（例如印表機）或者將其他裝置連接電腦的介面（例如USB、藍芽和紅外線）的存取設定靈活限制。
- **網頁控制**。此元件可讓您對不同的使用者群組進行存取網頁資源的限制設定。

控制元件根據以下規則執行：

- 應用程式啟動控制使用 [應用程式啟動控制規則](#)。
- 應用程式權限控制使用 [應用程式控制規則](#)。
- 裝置控制使用 [裝置存取規則和連接介面存取規則](#)。
- Web 控制使用 [網路資源存取規則](#)。

下列為應用程式的防護元件：

- **檔案防護**。此元件負責防護電腦的檔案系統避免感染。檔案防護在作業系統啟動時啟動，然後一直常駐在電腦記憶體中，將掃描電腦或連接裝置上所有開啟、儲存或啟動的檔案。檔案防護會攔截所有存取檔案的企圖，並掃描此檔案是否包含病毒和其他威脅。
- **系統監控**。此元件記錄電腦上的應用程式活動並將這些資訊提供給其他元件，確保為電腦提供更加有效的防護。
- **郵件防護**。此元件掃描將傳入和傳出的電子郵件訊息是否含有病毒和其他惡意程式。
- **網頁防護**。此元件會掃描透過 HTTP 和 FTP 協議到達使用者電腦的流量，並檢查 URL 是否出現在惡意網址或釣魚網站清單中。
- **即時通訊防護**。此元件為透過即時通訊協定到達電腦的資訊提供防護。此元件確保您安全使用眾多即時通訊用戶端。
- **防火牆**。當電腦連接到網際網路或本機網路時，此元件可防護儲存於電腦上的個人資料，並封鎖大多數針對作業系統的威脅。而元件將根據下列兩種規則篩選網路活動：[應用程式網路規則](#)和[網路封包規則](#)。
- **網路監控**。此元件可讓您即時瀏覽電腦網路活動。

- **網路攻擊防護**。此元件將掃描接收的網路流量以尋找常見的網路攻擊活動。偵測到企圖針對您電腦進行網路攻擊時，Kaspersky Endpoint Security 將封鎖來自攻擊電腦的網路活動。

Kaspersky Endpoint Security 提供以下工作：

- **完整掃描**。Kaspersky Endpoint Security 將完整掃描作業系統，包括 RAM、電腦啟動時載入的物件、作業系統備份以及所有的硬碟和卸除式磁碟。
- **自訂掃描**。Kaspersky Endpoint Security 將掃描使用者選擇的物件。
- **關鍵區域掃描**。Kaspersky Endpoint Security 掃描作業系統啟動時載入的物件、RAM和 Rootkits 目標物件。
- **更新**。Kaspersky Endpoint Security 下載更新應用程式資料庫和模組。更新可以確保電腦防護最新的病毒和其他威脅。
- **弱點掃描**。Kaspersky Endpoint Security 將掃描作業系統和已安裝軟體是否有弱點。此掃描，可即時偵測和清除入侵者可利用的潛在弱點。

資料加密功能可以加密儲存在本機硬碟中的檔案和資料夾。硬碟加密功能可以加密硬碟和卸除式磁碟機。

透過卡巴斯基安全管理中心進行遠端系統管理

卡巴斯基安全管理中心可以遠端啟動和停止用戶端電腦上的 Kaspersky Endpoint Security，並且可以遠端系統管理和設定應用程式設定。

應用程式的服務功能

Kaspersky Endpoint Security 包含了大量的服務功能。它們用於確保應用程式為最新版本、擴充應用程式功能和協助使用者操作。

- **報告**。在其操作過程中，應用程式將儲存一份關於每個應用程式元件和工作的報告。此報告包含 Kaspersky Endpoint Security 事件和應用程式執行的所有行為的清單。在發生意外事件時，您可以將此報告傳送至 Kaspersky Lab，供技術支援專家更加深入地查尋問題。
- **資料儲存**。如果應用程式在掃描電腦以尋找病毒和其他威脅時偵測到受感染的或疑似受感染的檔案，它會封鎖那些檔案。Kaspersky Endpoint Security 將疑似受感染的檔案移動至一個稱為“*隔離*”的專門儲存區。Kaspersky Endpoint Security 將已解毒的和刪除的檔案備份儲存在“*備份區*”中。Kaspersky Endpoint Security 將未處理的檔案移動至“*未處理檔案*”清單。您可以掃描檔案、將檔案還原至原資料夾以及清空資料儲存區。
- **通知服務**。通知服務可讓使用者瞭解電腦目前的防護狀態和 Kaspersky Endpoint Security 的操作。通知可直接顯示在螢幕上，或透過電子郵件進行傳送。
- **卡巴斯基安全網路**。使用者加入卡巴斯基安全網路可即時收集全球使用者的檔案、網頁資源和軟體信譽資訊來加強電腦防護的有效性。
- **產品授權**。使用授權檔案可以解鎖應用程式完整功能、提供應用程式資料庫和模組更新的存取權限、提供應用程式詳細資訊以及提供 Kaspersky Lab 技術支援協助。
- **支援**。所有 Kaspersky Endpoint Security 註冊使用者都可聯絡技術支援專家取得相關協助。您可以透過技術支援網站上的“我的卡巴斯基帳戶”傳送問題，或者透過電話尋求支援人員的協助。

如果此應用程式回傳錯誤，或者在執行期間關閉，它將自動重新啟動。

如果程式遇到反覆導致程式異常關閉的錯誤，它將執行以下操作：

1. 停用控制和防護功能（加密功能仍啟用）。
2. 通知使用者某些功能已被停用。
3. 更新病毒資料庫或應用程式模組更新之後嘗試還原程式的功能。

此應用程式將使用 Kaspersky Lab 專家定義的特殊用途的演算法接收經常性錯誤和系統故障的資訊。

硬體和軟體需求

為確保 Kaspersky Endpoint Security 的正常執行，您的電腦必須符合以下需求：

最低一般要求：

- 2 GB 磁碟可用空間
- 時鐘速度為 1 GHz 的處理器（支援 SSE2 指令集）
- RAM:
 - 1 GB（32 位元作業系統）；
 - 2 GB（64 位元作業系統）。

受支援的個人電腦作業系統：

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 或更高版本；
- Windows 8 Professional / Enterprise;
- Windows 8.1 Professional / Enterprise;
- Windows 10 Home / Pro / Education / Enterprise.

有關對 Microsoft Windows 10 作業系統的支援的詳細資訊，請參閱[技術支援知識庫](#)。

受支援的檔案伺服器作業系統：

- Windows Small Business Server 2008 Standard / Premium (64-bit);
- Windows Small Business Server 2011 Essentials / Standard (64-bit);
- Windows MultiPoint Server 2011 (64-bit);
- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2 或更高版本；
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 或更高版本；
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2016 Essentials / Standard / Datacenter;

- Windows Server 2019 Essentials / Standard / Datacenter.

有關對 Microsoft Windows Server 2016 和 Microsoft Windows Server 2019 作業系統的支援的詳細資訊，請參閱 [技術支援知識庫](#)。

安裝和移除應用程式

本章節將指導您如何在您的電腦上安裝 Kaspersky Endpoint Security、完成初始化設定、從上一版本的應用程式升級、以及將該程式從電腦上移除。

安裝程式

本章節介紹如何在您的電腦上安裝 Kaspersky Endpoint Security 以及如何完成程式的初始化設定。

程式安裝方法

您可以本機安裝（直接在使用者電腦上）或者從管理員工作站遠端安裝 Kaspersky Endpoint Security 10 for Windows。

可以按照以下模式本機安裝 Kaspersky Endpoint Security 10 for Windows：

- 使用應用程式安裝精靈互動模式。
此交互模式您必須參與安裝過程。
- 使用“[命令列](#)”以靜默模式安裝。
以靜默模式啟動安裝後，安裝過程不再需要您的參與。

可以使用以下方式遠端在網路電腦上安裝應用程式：

- 卡巴斯基安全管理中心軟體套裝（請參閱《[卡巴斯基安全管理中心佈署手冊](#)》）。
- Microsoft Windows 群組政策編輯器（請參閱作業系統說明檔案）。
- [系統中心配置管理器](#)。

我們建議您在啟動 Kaspersky Endpoint Security 安裝（包括遠端安裝）之前關閉所有活動的應用程式。

使用安裝精靈安裝程式

應用程式安裝精靈的介面包含了對應於應用程式安裝步驟的一系列視窗。您可以透過使用“**上一步**”和“**下一步**”按鈕在“安裝精靈”頁面之間瀏覽。安裝工作完成後，若要關閉“安裝精靈”，請點擊“**終止**”按鈕。要在安裝過程中停止安裝精靈，請點擊“**取消**”按鈕。

使用安裝精靈來安裝應用程式或從上一版本升級應用程式：

1. 執行[安裝套件](#)中包括的 setup.exe 檔案。
啟動“安裝精靈”。
2. 請按照“安裝精靈”的指示操作。

當啟動 `setup.exe` 檔案後，Kaspersky Endpoint Security 檢查電腦的不相容軟體。預設下，在偵測到不相容軟體時，應用程式處理序被終止並且與 Kaspersky Endpoint Security 不相容的應用程式顯示在螢幕。要繼續安裝，請從電腦移除這些應用程式。

步驟 1. 確認電腦符合安裝需求

在電腦上安裝 Kaspersky Endpoint Security 10 for Windows 或從上一版本應用程式升級之前，請確認符合下列需求：

- 無論作業系統和安裝套件是否滿足 [產品安裝軟體要求](#)。
- 無論是否滿足 [軟硬體要求](#)。
- 確認使用者是否有權限進行安裝。

如果不符合以上任何需求，系統將在電腦螢幕上顯示相關通知。

如果電腦符合列出的需求，“安裝精靈”將搜尋應用程式安裝期間可能導致衝突的 Kaspersky 應用程式。如果發現衝突的程式，系統將提示您手動移除它們。

如果偵測到的應用包括以前版本的 Kaspersky Endpoint Security，所有可以被移轉的資料（如啟動資料和應用程式設定）會在安裝 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 時被保留和使用，以前版本的應用程式將被自動刪除。這適用於以下應用程式版本：

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 CF1 / MP4 CF2
- Kaspersky Anti-Virus 6.0 for Windows Servers MP4 / MP4 CF2
- Kaspersky Endpoint Security 10 Service Pack 1 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 for Windows

步驟 2. 安裝過程的歡迎頁面

如果滿足安裝程式的所有條件，當您開始安裝時程式將顯示歡迎介面。歡迎頁面通知您開始在電腦上安裝 Kaspersky Endpoint Security。

要繼續安裝精靈，請點擊“**下一步**”按鈕。

步驟 3. 檢視產品授權協議

在此步驟中，請閱讀您與 Kaspersky Lab 之間的最終使用者產品授權協議。

請仔細閱讀產品授權協議，如果您同意所有協議，請選取“**我接受授權協議的條款**”核取方塊。

要返回安裝精靈先前的步驟，請點擊“**上一步**”按鈕。要繼續安裝精靈，請點擊“**下一步**”按鈕。要停止安裝精靈，請點擊“**取消**”按鈕。

步驟 4. 選取安裝類型

在此步驟中，您可以選取最合適的 Kaspersky Endpoint Security 安裝類型：

- **基本安裝**。如果您選取該類型安裝，則防護元件、應用程式權限控制和弱點偵測將與 Kaspersky Lab 專家建議的設定一起安裝在電腦上。
- **標準安裝**。若您選擇此安裝類型，將安裝 Kaspersky Lab 的預設防護和控制元件在電腦上。
- **自訂安裝**：如果您選取該類型的安裝，您將獲得提示選取“[要安裝的元件](#)”並指定“[應用程式目的資料夾](#)”。此類型的安裝將安裝不包括在基本和標準安裝中的元件。

簡易安裝是使用預設設定。

要返回安裝精靈先前的步驟，請點擊“**上一步**”按鈕。要繼續安裝精靈，請點擊“**下一步**”按鈕。要停止安裝精靈，請點擊“**取消**”按鈕。

步驟 5. 選取要安裝的程式元件

如果您選取“[自訂](#)”安裝程式，將執行此步驟。

在此步驟中，您可以選取想要安裝的 Kaspersky Endpoint Security 元件。檔案防護是必須安裝的元件。您無法取消其安裝。

預設情況下，除了以下元件之外選定安裝所有應用程式元件：

- [BadUSB 攻擊防護](#)。
- [磁碟機加密](#)。
- [檔案加密](#)。
- [Microsoft BitLocker Manager](#)。
- [KATA Endpoint Sensor](#)。

Microsoft BitLocker Manager 執行以下功能：

- Manages BitLocker 加密構建在 Windows 作業系統中。
- 配置加密政策設定並檢查其與受管電腦的適用性。
- 啟動加密和解密過程。
- 監控受管電腦上加密狀態。
- 集中儲存卡巴斯基安全管理中心管理伺服器上的還原金鑰。

KATA Endpoint Sensor 是卡巴斯基攻擊防護平台。此解決方案用於快速偵測目標攻擊之類的威脅。此元件將持續監控處理程序、活動網路連線和被修改的檔案，並將此資訊中繼給卡巴斯基攻擊防護平台。

若要選取要安裝的元件，點擊調出上下文功能表的元件名稱旁邊的圖示，選取**“功能將安裝在本機磁碟上”**。關於哪些工作由所選元件執行以及安裝此元件所需的磁碟空間大小的詳細資訊，請參閱目前安裝精靈頁面下方的內容。

要檢視關於本機硬碟上可用空間的資訊，請點擊**“磁碟”**按鈕。開啟的**“可用磁碟空間”**視窗中將顯示相關資訊。

若要取消元件安裝，在右鍵選單中選取**“功能將不可用”**選項。

要返回預設元件清單，請點擊**“重設”**按鈕。

要返回安裝精靈先前的步驟，請點擊**“上一步”**按鈕。要繼續安裝精靈，請點擊**“下一步”**按鈕。要停止安裝精靈，請點擊**“取消”**按鈕。

步驟 6. 選取目的資料夾

如果您選擇**“自訂安裝”**將可使用此設定

在此步驟中，您可以指定安裝程式的目的資料夾的路徑。要選取應用程式的目的資料夾，請點擊**“瀏覽”**按鈕。

要檢視關於本機硬碟上可用空間的資訊，請點擊**“磁碟”**按鈕。開啟**“可用磁碟空間”**視窗中將顯示相關資訊。

要返回安裝精靈先前的步驟，請點擊**“上一步”**按鈕。要繼續安裝精靈，請點擊**“下一步”**按鈕。要停止安裝精靈，請點擊**“取消”**按鈕。

步驟 7. 新增物件排除病毒掃描

如果您選擇**“自訂安裝”**將可使用此設定

在此設定中，您可以指定新增病毒掃描中的排除項目。

選取“將 Microsoft 所建議的信任物件排除在病毒掃描範圍外/將 Kaspersky Lab 所建議的信任物件排除在病毒掃描範圍外”核取方塊，排除區域設定將依照 Microsoft 或 Kaspersky Lab 受信任的區域進行排除掃描工作。

如果選中這些核取方塊中的一個，Kaspersky Endpoint Security 會將 Microsoft 或 Kaspersky Lab 建議的區域分別包含在受信任區域中。Kaspersky Endpoint Security 將不針對此區域進行掃描。

選取**“將 Microsoft 所建議的信任物件排除在病毒掃描範圍外”**項目，則將可在 Microsoft Windows 的檔案伺服器電腦上，使用 Kaspersky Endpoint Security。

要返回安裝精靈先前的步驟，請點擊**“上一步”**按鈕。要繼續安裝精靈，請點擊**“下一步”**按鈕。要停止安裝精靈，請點擊**“取消”**按鈕。

步驟 8. 應用程式安裝的準備工作

建議防護安裝過程，因為您的電腦可能已經感染了會干擾 Kaspersky Endpoint Security 10 for Windows 安裝的惡意程式。

預設情況下，啟用安裝過程防護。

但是，如果無法安裝應用程式（例如，使用 Windows 遠端桌面協助執行遠端安裝），我們建議您停用安裝過程的防護。如果出現這種情況，則終止安裝並再次啟動應用程式設定精靈。在“程式安裝的準備工作”中，請取消選取**安裝過程防護**核取方塊。

“確保與 Citrix PVS 相容”核取方塊將啟用/停用以 Citrix PVS 相容模式安裝驅動程式的功能。

僅當您使用 Citrix Provisioning Service 時選取該核取方塊。

“新增 avp.com 檔案路徑到系統變數 %PATH%”核取方塊將啟用/停用一個選項，該選項可將到 avp.com 檔案的路徑新增到 %PATH% 系統變數中。

如果選取該核取方塊，則從命令列啟動 Kaspersky Endpoint Security 或其工作不需要輸入到可執行檔案的路徑。輸入可執行檔案的名稱和啟動特定工作的指令即可。

要返回安裝精靈先前的步驟，請點擊**“上一步”**按鈕。要安裝該程式，請點擊**“安裝”**按鈕。要停止安裝精靈，請點擊**“取消”**按鈕。

當程式安裝在電腦上時，目前網路連線可能會中斷。應用程式安裝完成後大多數被終止的網路連線將被還原。

步驟 9. 安裝應用程式

安裝程式可能需要花費一些時間。請等待安裝完成。

如果您正在升級上一版本應用程式，此步驟還包括設定遷移以及移除上一版本應用程式。

Kaspersky Endpoint Security 安裝完成後，[“初始化設定精靈”](#)將啟動。

透過命令列安裝程式

可以在以下模式之一從命令列安裝 Kaspersky Endpoint Security：

- 使用應用程式安裝精靈互動模式。
- 在靜默模式下。以靜默模式啟動安裝後，安裝過程不再需要您的參與。要在靜默模式下安裝應用程式，請使用 `/s` 和 `/qn` 鍵。

要安裝應用程式或升級應用程式版本：

1. 以管理員身分執行命令列解譯器 (cmd.exe)。
2. 轉到 Kaspersky Endpoint Security 分發套件所在資料夾。
3. 執行以下指令：

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pALLOWREBOOT=1|0] [/pADDLOCAL=<
元件>] [/pSKIPPRODUCTCHECK=1|0] [/pSKIPPRODUCTUNINSTALL=1|0] [/pKLLOGIN=<使用者名稱>
/pKLPASSWD=<密碼> /pKLPASSWDAREA=<密碼範圍>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<偵錯等級
>] /s
```

或

```
msiexec /i <分發套件名稱> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [ALLOWREBOOT=1|0] [ADDLOCAL=
<元件>] [SKIPPRODUCTCHECK=1|0] [SKIPPRODUCTUNINSTALL=1|0] [KLLOGIN=<使用者名稱>
KLPASSWD=<密碼> KLPASSWDAREA=<密碼範圍>] [ENABLETRACES=1|0 TRACESLEVEL=<偵錯等級>] /qn
```

EULA	<p>接受或拒絕最終使用者產品授權協議的條款。可用值：</p> <ul style="list-style-type: none"> • 1 – 接受最終使用者產品授權協議的條款。 • 0 – 拒絕最終使用者產品授權協議的條款。 <p>授權協議的內容包括在 Kaspersky Endpoint Security 分發套件中。必須接受最終使用者授權協議才能安裝應用程式或升級應用程式版本。</p>
PRIVACYPOLICY	<p>接受或拒絕隱私政策。可用值：</p> <ul style="list-style-type: none"> • 1 – 接受隱私政策。 • 0 – 拒絕隱私政策。 <p>隱私政策的文字包含在 Kaspersky Endpoint Security 分發套件 中。要安裝應用程式或升級應用程式版本，您必須接受隱私政策。</p>
KSN	<p>接受或拒絕參與卡巴斯基安全網路。如果沒有為此參數設定任何值，在首次啟動 Kaspersky Endpoint Security 時，Kaspersky Endpoint Security 將提示您確認同意或拒絕加入 KSN。可用值：</p> <ul style="list-style-type: none"> • 1 – 同意加入 KSN。 • 0 – 拒絕加入 KSN (預設值)。 <p>Kaspersky Endpoint Security 分發套件已針對與卡巴斯基安全網路配合使用進行最佳化。如果您選擇不加入卡巴斯基安全網路，則應該在安裝完成後立即更新 Kaspersky Endpoint Security。</p>
ALLOWREBOOT=1	<p>自動重新啟動電腦 (如果安裝或升級應用程式後需要重新啟動)。如果未為此參數設定任何值，則阻止電腦自動重新啟動。</p> <p>安裝 Kaspersky Endpoint Security 時，不需要重新啟動。僅當在安裝前必須移除不相容的應用程式時，才需要重新啟動。更新應用程式版本時也可能需要重新啟動。</p>
ADDLOCAL	<p>選取要安裝的其他元件。預設情況下，將選取安裝除以下元件外的所有應用程式元件：“BadUSB 攻擊防護”、“檔案級加密”、“完整磁碟加密”、“BitLocker 管理”和“KATA 端點感應器”。可用值：</p> <ul style="list-style-type: none"> • MSBitLockerFeature。BitLocker Manager 元件已安裝。 • AntiAPTFeature。KATA Endpoint Sensor 元件已安裝。
SKIPPRODUCTCHECK=1	<p>停用不相容軟體檢查。分發套件 中包含的 incompatible.txt 檔案提供了不相容軟體清單。如果沒有為此參數設定任何值，並且偵測到不相容軟體，則將終止 Kaspersky Endpoint Security 的安裝。</p>
SKIPPRODUCTUNINSTALL=1	<p>停用自動移除偵測到的不相容軟體。如果沒有為此參數設定任何值，則 Kaspersky Endpoint Security 將嘗試刪除不相容軟體。</p>

KLLOGIN	設定用於存取 Kaspersky Endpoint Security 功能和設定的使用者名稱 (“密碼防護” 元件) 。該使用者名稱與 “KLPASSWD” 和 “KLPASSWDAREA” 設定一起進行設定。預設使用者名為 KLAdmin 。
KLPASSWD	指定用於存取 Kaspersky Endpoint Security 功能和設定的密碼 (該密碼與 “KLLOGIN” 和 “KLPASSWDAREA” 參數一起指定) 。 如果您指定了口令，但沒有指定帶有 KLLOGIN 參數的使用者名稱，將預設使用 KLAdmin 使用者名稱。
KLPASSWDAREA	指定用於存取 Kaspersky Endpoint Security 的密碼範圍。當使用者嘗試執行包含在此範圍中的操作時，Kaspersky Endpoint Security 將提示使用者輸入帳戶憑證 (“KLLOGIN” 和 “KLPASSWD” 參數) 。使用 “;” 字元以指定多個值。可用值： <ul style="list-style-type: none"> • SET – 修改應用程式設定。 • EXIT – 結束應用程式。 • DISPROTECT – 停用防護元件並停止掃描工作。 • DISPOLICY – 停用卡巴斯基安全管理中心政策。 • UNINST – 從電腦中移除應用程式。 • DISCTRL – 停用控制元件。 • REMOVELIC – 刪除金鑰。 • REPORTS – 檢視報告。
ENABLETRACES	啟用或停用應用程式偵錯。Kaspersky Endpoint Security 在啟動後將偵錯檔案儲存在資料夾 %ProgramData%/Kaspersky Lab 中。可用值： <ul style="list-style-type: none"> • 1 – 啟用應用程式偵錯。 • 0 – 停用應用程式偵錯 (預設值) 。
TRACESLEVEL	偵錯詳細等級。可用值： <ul style="list-style-type: none"> • 100 (關鍵) 。僅嚴重錯誤訊息。 • 200 (高) 。有關所有錯誤的訊息，包括致命錯誤。 • 300 (診斷) 。有關所有錯誤的訊息，以及選定的包含警告的訊息。 • 400 (重要) 。關於普通和嚴重錯誤的所有警告和訊息，以及選取的一些包含進階資訊的訊息。 • 500 (一般) 。關於普通和嚴重錯誤的所有警告和訊息，以及帶有標準模式應用程式的更詳細資訊的訊息 (預設值) 。 • 600 (低) 。所有可能的訊息。

範例：

```
setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1 /s
```



```
msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1 KSN=1
KLLOGIN=Admin KLPASSWD=Password
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn

setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

安裝應用程式後，Kaspersky Endpoint Security 會啟動試用版產品授權，除非您在 [setup.ini 檔案](#) 中指示啟動碼。試用版產品授權通常擁有較短的有效期。當試用版授權到期，所有卡斯基安全防護功能將轉為停用。要繼續使用程式，您必須 [啟動正式版產品授權](#)。

以靜默模式安裝應用程式或升級應用程式版本時，支援以下檔案的使用：

- [setup.ini](#) – 一般應用程式安裝設定
- [install.cfg](#) – Kaspersky Endpoint Security 的本機設定；
- [setup.reg](#) – 登錄機碼。
只有在 [setup.ini](#) 檔案中為 [SetupReg](#) 參數設定 [setup.reg](#) 值時，[setup.reg](#) 檔案中的登錄機碼才會寫入登錄檔。[setup.reg](#) 檔案由 Kaspersky 專家生成。不建議修改該檔案的內容。

要應用 [setup.ini](#)、[install.cfg](#) 和 [setup.reg](#) 檔案中的設定，請將這些檔案放入包含 Kaspersky Endpoint Security 分發套件的資料夾。

使用系統中心設定管理器遠端安裝應用程式

這些手冊適用於 System Center Configuration Manager 2012 R2。

若要使用系統中心設定管理器遠端安裝應用程式：

1. 開啟設定管理器控制台。
2. 在主控制台右側，在“**應用程式管理**”區域中選取“**軟體套件**”。
3. 在控制台中主控制台右上部分，點擊“**建立軟體套件**”按鈕。
這會啟動“*新建軟體套件和應用程式精靈*”。
4. 在新建軟體套件和應用程式精靈中：
 - a. 在“**軟體套件**”區域中：
 - 在“**名稱**”欄位中輸入安裝套件名稱。
 - 在“**原始資料夾**”欄位中指定包含 Kaspersky Endpoint Security 安裝套件的資料夾的路徑。
 - b. 在“**應用程式類型**”區域中選取“**標準應用程式**”選項。
 - c. 在“**標準應用程式**”區域中：

- 在“名稱”欄位中，輸入安裝套件的唯一名稱（例如包含版本的應用程式名稱）。
- 在“命令列”欄位中從命令列中指定 Kaspersky Endpoint Security 安裝選項。
- 點擊“瀏覽”按鈕指定應用程式可執行檔案的路徑。
- 確保執行模式清單選擇了以管理員權限執行項目。

d. 在“要求”區域中：

- 如果您希望在安裝 Kaspersky Endpoint Security 之前啟用其他應用程式，則選取“首先啟動其他應用程式”核取方塊。
從“應用程式”下拉清單中選取此應用程式，或者點擊“瀏覽”按鈕指定此應用程式可執行檔案的路徑。
- 如果您希望只在指定作業系統中安裝此應用程式，則選取“平台要求”區域中的“只能在指定平台上啟動此應用程式”選項。
在此清單中選取要安裝 Kaspersky Endpoint Security 的作業系統旁的核取方塊。

此步驟為可選項。

e. 在“摘要”區域中選中所有輸入的設定值，點擊“下一步”。

建立的安裝套件將顯示在可用安裝套件清單的“軟體套件”區域中。

5. 在安裝套件右鍵選單中，選取“佈署”。

這將啟動“佈署手冊”。

6. 在佈署精靈中：

a. 在“一般”區域中：

- 在“軟體”欄位中輸入安裝套件的唯一名稱或者點擊“瀏覽”按鈕從清單中選取安裝套件。
- 在“集合”欄位中輸入要安裝應用程式的電腦集合的名稱，或者點擊“瀏覽”按鈕選取集合。

b. 在“包括”區域中，新增分發點（有關詳情，請參閱系統中心設定管理器的說明文件）。

c. 如有必要，在佈署精靈中指定其他設定的值。這些設定是 Kaspersky Endpoint Security 遠端安裝的可選項。

d. 在“摘要”區域中選中所有輸入的設定值，點擊“下一步”。

佈署精靈完成後將建立遠端安裝 Kaspersky Endpoint Security 的工作。

setup.ini 檔案安裝設定說明

從命令列安裝程式或使用 Microsoft Windows 的群組政策編輯器安裝程式時需要使用 setup.ini 檔案。要應用 setup.ini 檔案中的設定，請將該檔案放入包含 Kaspersky Endpoint Security 分發套件的資料夾。

setup.ini 檔案包含以下部分：

- [Setup] – 一般程式安裝選項。

- [Components] – 選取要安裝的應用程式元件。至少需選取一個元件進行安裝，未選取的元件將不會進行安裝。檔案防護是強制性元件，無論此區域中表明的是哪種設定都會安裝在電腦上。
- [Tasks] – 選取要包含在 Kaspersky Endpoint Security 工作清單中的工作。如果沒有指定工作，所有工作都包含在 Kaspersky Endpoint Security 的工作清單中。

1 值的替代值可為 yes、on、enable 和 enabled。

0 值的替代值可為 no、off、disable 和 disabled。

setup.ini 檔案的設定

區域	參數	描述
[Setup]	InstallDir	應用程式安裝資料夾的路徑。
	ActivationCode	Kaspersky Endpoint Security 啟動碼。
	Eula	接受或拒絕最終使用者產品授權協議的條款。可用值： <ul style="list-style-type: none"> • 1 – 接受最終使用者產品授權協議的條款。 • 0 – 拒絕最終使用者產品授權協議的條款。授權協議的內容包括在 Kaspersky Endpoint Security 分發套件 中。必須接受最終使用者授權協議才能安裝應用程式或升級應用程式版本。
	PrivacyPolicy	接受或拒絕隱私政策。可用值： <ul style="list-style-type: none"> • 1 – 接受隱私政策。 • 0 – 拒絕隱私政策。隱私政策的文字包含在 Kaspersky Endpoint Security 分發套件 中。要安裝應用程式或升級應用程式版本，您必須接受隱私政策。
	KSN	接受或拒絕參與卡巴斯基安全網路。如果沒有為此參數設定任何值，在首次啟動 Kaspersky Endpoint Security 時，Kaspersky Endpoint Security 將提示您確認同意或拒絕加入 KSN。可用值： <ul style="list-style-type: none"> • 1 – 同意加入 KSN。 • 0 – 拒絕加入 KSN (預設值)。 Kaspersky Endpoint Security 分發套件已針對與卡巴斯基安全網路配合使用進行最佳化。如果您選擇不加入卡巴斯基安全網路，則應該在安裝完成後立即更新 Kaspersky Endpoint Security。
	Login	設定用於存取 Kaspersky Endpoint Security 功能和設定的使用者名稱 ("密碼防護" 元件)。該使用者名稱與 "Password" 和 "PasswordArea" 設定一起進行設定。預設使用者名稱為 KLAdmin。
	密碼	指定用於存取 Kaspersky Endpoint Security 功能和設定的密碼 (該密碼與 "Login" 和 "PasswordArea")

		<p>參數一起指定)。</p> <p>如果您指定了口令，但沒有指定帶有 登入 參數的使用者名稱，將預設使用 KAdmin 使用者名稱。</p>
	<p>PasswordArea</p>	<p>指定用於存取 Kaspersky Endpoint Security 的密碼範圍。當使用者嘗試執行包含在此範圍中的操作時，Kaspersky Endpoint Security 將提示使用者輸入帳戶憑證 (“登入名稱”和“密碼”參數)。使用“;”字元以指定多個值。可用值：</p> <ul style="list-style-type: none"> • SET – 修改應用程式設定。 • EXIT – 結束應用程式。 • DISPROTECT – 停用防護元件並停止掃描工作。 • DISPOLICY – 停用卡巴斯基安全管理中心政策。 • UNINST – 從電腦中移除應用程式。 • DISCTRL – 停用控制元件。 • REMOVE LIC – 刪除金鑰。 • REPORTS – 檢視報告。
	<p>SelfProtection</p>	<p>啟用或停用應用程式安裝防護機制。可用值：</p> <ul style="list-style-type: none"> • 1 – 啟用程式安裝防護機制。 • 0 – 停用程式安裝防護機制。 您可以停用安裝防護。安裝防護包括防止用惡意程式偽造分發套件、封鎖對 Kaspersky Endpoint Security 安裝資料夾的存取，以及封鎖對包含應用程式金鑰的系統登錄檔登錄區的存取。但是，如果無法安裝應用程式 (例如，使用 Windows 遠端桌面協助執行遠端安裝)，我們建議您停用安裝過程的防護。
	<p>Reboot=1</p>	<p>自動重新啟動電腦 (如果安裝或升級應用程式後需要重新啟動)。如果未為此參數設定任何值，則阻止電腦自動重新啟動。</p> <p>安裝 Kaspersky Endpoint Security 時，不需要重新啟動。僅當在安裝前必須移除不相容的應用程式時，才需要重新啟動。更新應用程式版本時也可能需要重新啟動。</p>
	<p>AddEnvironment</p>	<p>指定此值表示將以位於 Kaspersky Endpoint Security 安裝資料夾的可執行檔案的路徑補充 %PATH% 系統變數。可用值：</p> <ul style="list-style-type: none"> • 1 – 以位於 Kaspersky Endpoint Security 安裝資料夾的可執行檔的路徑補充 %PATH% 系統變數。 • 0 – 不以位於 Kaspersky Endpoint Security 安裝資料夾的可執行檔的路徑補充 %PATH% 系統變數。

		數。
	AMPPL	<p>啟用或停用 Kaspersky Endpoint Security 服務使用 AM-PPL (惡意軟體防護受防護輕型處理程序) 技術提供的防護。可用值：</p> <ul style="list-style-type: none"> • 1 – 啟用 Kaspersky Endpoint Security 服務使用 AM-PPL 技術提供的防護。 • 0 – 停用 Kaspersky Endpoint Security 服務使用 AM-PPL 技術提供的防護。
	SetupReg	<p>啟用將 setup.reg 檔案中的登錄機碼寫入登錄檔。 SetupReg : setup.reg 參數值。</p>
	EnableTraces	<p>啟用或停用應用程式安裝偵錯。Kaspersky Endpoint Security 將偵錯檔案儲存在資料夾 %ProgramData%/Kaspersky Lab 中。可用值：</p> <ul style="list-style-type: none"> • 1 – 啟用應用程式安裝偵錯。 • 0 – 停用應用程式安裝偵錯 (預設值)。
	TracesLevel	<p>偵錯詳細等級。可用值：</p> <ul style="list-style-type: none"> • 100 (關鍵)。僅嚴重錯誤訊息。 • 200 (高)。有關所有錯誤的訊息，包括致命錯誤。 • 300 (診斷)。有關所有錯誤的訊息，以及選定的包含警告的訊息。 • 400 (重要)。關於普通和嚴重錯誤的所有警告和訊息，以及選取的一些包含進階資訊的訊息。 • 500 (一般)。關於普通和嚴重錯誤的所有警告和訊息，以及帶有標準模式應用程式的更詳細資訊的訊息 (預設值)。 • 600 (低)。所有可能的訊息。
[Components]	ALL	<p>安裝所有元件。如果指定了參數值 1，所有元件都將安裝，與單個元件的安裝設定無關。</p>
	MailAntiVirus	郵件防護。
	IMAntiVirus	即時通訊防護。
	WebAntiVirus	網頁防護。
	ApplicationPrivilegeControl	應用程式權限控制。
	SystemWatcher	系統監視器。
	防火牆	防火牆。
	NetworkAttackBlocker	網路攻擊防護。
	WebControl	Web 控制。

	DeviceControl	裝置控制。
	ApplicationStartupControl	應用程式啟動控制。
	FileEncryption	“檔案級加密”庫。
	DiskEncryption	“完整磁碟加密”庫。
	VulnerabilityAssessment	弱點監控。
	KeyboardAuthorization	BadUSB 攻擊防護。
	AntiAPT	KATA Endpoint Sensor。
	MSBitLocker	Microsoft BitLocker Manager。
	AdminKitConnector	網路代理連線器 ，用於透過卡巴斯基安全管理中心遠端管理應用程式。可用值： <ul style="list-style-type: none"> • 1 – 安裝網路代理連線器。 • 0 – 不安裝網路代理連線器。
[Tasks]	ScanMyComputer	完整掃描工作。可用值： <ul style="list-style-type: none"> • 1 – 該工作將包含在 Kaspersky Endpoint Security 工作清單中。 • 0 – 該工作不會包含在 Kaspersky Endpoint Security 工作清單中。
	ScanCritical	關鍵區域掃描工作。可用值： <ul style="list-style-type: none"> • 1 – 該工作將包含在 Kaspersky Endpoint Security 工作清單中。 • 0 – 該工作不會包含在 Kaspersky Endpoint Security 工作清單中。
	Updater	更新工作。可用值： <ul style="list-style-type: none"> • 1 – 該工作將包含在 Kaspersky Endpoint Security 工作清單中。 • 0 – 該工作不會包含在 Kaspersky Endpoint Security 工作清單中。

初始化設定精靈

Kaspersky Endpoint Security 的初始化設定精靈在程式安裝過程結束後開始。初始化設定精靈允許您啟動程式並收集關於作業系統中包含的應用程式的資訊。這些應用程式將被新增到信任應用程式清單中，它們在作業系統中的操作不受任何限制。

初始化設定精靈介面由一系列畫面（步驟）組成。您可以透過使用“**上一步**”和“**下一步**”按鈕，在初始化設定精靈頁面之間瀏覽。要完成“初始化設定精靈”，請點擊“**終止**”按鈕。要在任何時候停止“初始化設定精靈”，請點擊“**取消**”。

如果因某種原因使得“初始化設定精靈”中斷，系統不會儲存已指定的設定。當您下一次開始使用程式時，“初始化設定精靈”將再次啟動，屆時需要您再次進行設定。

啟動應用程式

應用程式必須在具有目前系統日期和時間的電腦上啟動。如果在應用程式啟動後變更系統日期和時間，金鑰將不可用。應用程式將切換至無更新執行模式，卡斯基安全網路將不可用。只有重新調整作業系統，才能使金鑰再變為可用狀態。

在此步驟中，選取以下 Kaspersky Endpoint Security 啟動選項：

- **使用啟動碼啟動**。若要使用 [啟動碼](#) 啟動應用程式，則選取該選項並輸入啟動碼。
- **使用金鑰檔案啟動**。選取該選項可使用金鑰檔案啟動應用程式。
- **“啟動試用版本”**。要啟動應用程式的試用版本，請選取此選項。使用者可透過有時間限制的試用版授權，使用全功能版本應用程式。在授權到期後，將封鎖應用程式功能，您不能再次啟用試用版授權。
- **“稍後啟動”**。若您想略過 Kaspersky Endpoint Security 啟動程式，請選取此選項。使用者將只能使用檔案防護和防火牆元件。使用者將只能於程式安裝完成後，執行一次更新工作。“稍後啟動”選項僅在程式安裝後第一次啟動“初始配置精靈”時可用。

啟動試用版本，或使用啟動碼啟動，皆需要與網際網路連線。

要執行初始化設定精靈，請選取啟動選項並點擊“**下一步**”按鈕。要停止初始化設定精靈，請點擊“**取消**”按鈕。

使用啟動碼啟動

此步驟僅適用於使用啟動碼啟動程式。啟動試用版程式或使用授權檔案啟動程式時，可略過此步驟。

在此步驟中，Kaspersky Endpoint Security 會將啟動資料傳送到啟動伺服器，以驗證輸入的啟動碼。

- 如果啟動碼驗證成功，則初始化設定精靈會收到可自動安裝的授權檔案。然後，初始化設定精靈會繼續進行到下一視窗。
- 如果啟動碼驗證失敗，程式將會顯示對應的訊息。發生此狀況時，建議您諮詢向您銷售 Kaspersky Endpoint Security 授權的軟體供應商。
- 如果超過啟動碼的啟動次數，程式會顯示對應的通知。初始化設定精靈將會中斷，並且程式會建議您聯絡 Kaspersky Lab 技術支援。

要返回到初始化設定精靈的上一步，請點擊“**上一步**”按鈕。要停止初始化設定精靈，請點擊“**取消**”按鈕。

使用授權檔案啟動

此步驟僅適用於使用授權檔案啟動程式的正式版本。

在此步驟中，您必須指定授權檔案。若要執行操作，請點擊“**瀏覽**”按鈕，選取副檔名為 <File ID>.key 的檔案。

選取授權檔案後，視窗下方將顯示以下授權資訊：

- 金鑰
- 授權類型（正式版或試用版）和該授權可用的電腦數。
- 電腦上應用程式啟動日期
- 產品授權到期日期
- 在此產品授權下程式功能可用
- 如果存在，則通知關於產品授權的問題。例如，*產品授權黑名單檔案已損壞*。

要返回到初始化設定精靈的上一步，請點擊“**上一步**”按鈕。要繼續執行初始化設定精靈，請點擊“**下一步**”按鈕。要停止初始化設定精靈，請點擊“**取消**”按鈕。

選擇啟動功能

此步驟僅適用於啟動試用版本時使用。

在該步驟中您可以選取啟動應用程式後可用的功能：

- **基本安裝**。若選取此選項，啟動應用程式後，僅可使用基本的防護元件、應用程式權限控制和弱點監控。
- **標準安裝**。若選取此選項，啟動應用程式後，僅可使用標準配置的防護與控制元件。
- **完整安裝**。若選取此選項，啟動應用程式後，可使用所有安裝的應用程式元件，包含加密功能。

如果您在安裝過程中選取了所擁有產品授權允許的更多元件，這些元件可以安裝但是在應用程式啟動後無法使用。如果購買的產品授權允許使用比目前安裝的元件更多的元件，在應用程式被啟動後，未安裝的元件將會列在在“**產品授權**”區域中。

簡易安裝是使用預設設定。

要返回到初始化設定精靈的上一步，請點擊“**上一步**”按鈕。要繼續執行初始化設定精靈，請點擊“**下一步**”按鈕。要停止初始化設定精靈，請點擊“**取消**”按鈕。

完成啟動

在此步驟中，初始化設定精靈會通知您關於 Kaspersky Endpoint Security 成功啟動的資訊。並為您提供授權資訊：

- 授權類型（正式版或試用版）和該授權可用的電腦數。
- 產品授權到期日期
- 在此產品授權下程式功能可用

要繼續執行初始化設定精靈，請點擊“**下一步**”按鈕。要停止初始化設定精靈，請點擊“**取消**”按鈕。

分析作業系統

在該步驟中，程式將收集系統中所包含應用程式的資訊。這些應用程式將被新增到信任應用程式清單中，它們在作業系統中的操作不受任何限制。

Kaspersky Endpoint Security 安裝之後，其他應用程式首次啟動時會被分析。

要停止初始化設定精靈，請點擊“**取消**”按鈕。

完成應用程式的初始化配置

初始化設定精靈完成視窗包含關於 Kaspersky Endpoint Security 完成安裝過程的資訊。

如果要啟動 Kaspersky Endpoint Security，請點擊“**完成**”按鈕。

如果要結束初始設定精靈且不啟動 Kaspersky Endpoint Security，請清除“**啟動 Kaspersky Endpoint Security 10 for Windows**”核取方塊，然後點擊“**完成**”。

卡巴斯基安全網路聲明

在此步驟中，我們邀請您參加卡巴斯基安全網路。

閱讀卡巴斯基安全網路資料收集聲明：

- 如果您接受所有條款，則選取初始配置精靈視窗中的“**我接受參見卡巴斯基安全網路的條款**”選項。
- 如果您不接受參與卡巴斯基安全網路的條款，則選取初始配置精靈視窗中的“**我不接受卡巴斯基安全網路的參與條款**”選項。

若要繼續初始配置精靈，請點擊“**確定**”。

升級舊版本程式的方法

要將舊版本應用程式升級至 Kaspersky Endpoint Security 10 Service Pack 2 for Windows，請將所有加密的硬碟解密。

您可以將以下應用程式升級為 Kaspersky Endpoint Security 10 Service Pack 2 for Windows：

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 CF1（版本 6.0.4.1424）/MP4 CF2（版本 6.0.4.1611）。

- Kaspersky Anti-Virus 6.0 for Windows Servers MP4 (版本 6.0.4.1424) / MP4 CF2 (版本 6.0.4.1611) 。
- Kaspersky Endpoint Security 10 Service Pack 1 for Windows (版本 10.2.2.10535)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Windows (版本 10.2.2.10535 (MR1))
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows (版本 10.2.4.674)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 for Windows (build 10.2.5.3201)

當任何前版的應用程式升級到 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 時，系統不會轉換“隔離區”和“備份區”的內容。

您可以按照以下操作升級舊版本的程式：

- 使用應用程式安裝精靈的本機互動模式。
- 使用“[命令列](#)”以非互動模式本機安裝
- 卡巴斯基安全管理中心遠端軟體套裝的說明 (請參閱《卡巴斯基安全管理中心佈署手冊》)
- 透過 Microsoft Windows 群組政策編輯器遠端執行 (請參閱作業系統說明檔案)

當從上一版本應用程式升級到 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 時，不需要移除上一版本的應用程式。我們建議您在升級上一版本應用程式之前停止所有活動的應用程式。

移除程式

本章節介紹如何從您的電腦中移除 Kaspersky Endpoint Security 。

移除程式的方法

移除 Kaspersky Endpoint Security 將導致電腦和使用者資訊失去防護。

可以從電腦中以多種方式刪除 Kaspersky Endpoint Security：

- 使用[安裝精靈](#)以互動模式本機進行
- 使用“[命令列](#)”以非互動模式本機安裝
- 透過卡巴斯基安全管理中心軟體套裝的說明遠端執行 (有關詳細資訊，請參閱《卡巴斯基安全管理中心佈署手冊》)
- 透過 Microsoft Windows 群組政策編輯器遠端執行 (請參閱作業系統說明檔案)

使用安裝精靈移除程式

要使用安裝精靈移除 Kaspersky Endpoint Security，請執行以下操作：

1. 在“開始”選單中，選取“應用程式”→“Kaspersky Endpoint Security 10 for Windows”→“修改、修復或移除”。
啟動“安裝精靈”。
2. 在安裝精靈的“修改、修復或移除”視窗中，點擊“移除”按鈕。
3. 請按照“安裝精靈”的指示操作。

步驟 1. 儲存程式資料以備後用

在該步驟中，您可以指定您要保留哪些應用程式所使用的資料以便在接下來的應用程式安裝中使用（例如安裝新版本時）。如果您並未指定任何資料，應用程式將被完全刪除。

要儲存程式資料以備後用，

選取您想要保留的資料類型的核取方塊：

- **啟動資料** – 透過自動使用目前的授權檔案。只要它在下次安裝前授權檔案不到期，即可用來啟動程式資料。
- **備份區和隔離檔案** – 程式掃描且置於“備份區”或“隔離區”中的物件。

在移除應用程式之後儲存的備份區和隔離區檔案只能在用於儲存這些檔案的同一版本應用程式中存取。

如果您排程在移除應用程式之後使用備份區和隔離區物件，必須在移除應用程式之前將這些檔案從它們的儲存中還原。但是，Kaspersky Lab 專家不建議從備份和隔離中還原檔案，因為這可能會損害電腦。

- **應用程式的執行設定** – 應用程式配置過程中選取的程式設定值。
- **儲存本機加密金鑰** – 在移除應用程式之前可存取加密檔案和加密功能。重新安裝應用程式與加密功能後，將可再存取加密檔案和進行加密。
預設情況下已勾選此核取方塊。

要繼續安裝精靈，請點擊“下一步”按鈕。要停止安裝精靈，請點擊“取消”按鈕。

步驟 2. 確認應用程式移除

由於移除程式會危害您電腦的安全，系統會詢問您是否確實想要移除該程式。若要執行操作，請點擊“刪除”按鈕。

要在任何時候停止程式移除，您可以點擊“取消”取消此操作。

步驟 3. 移除應用程式。完成移除

在此步驟中，“安裝精靈”將從電腦中移除程式。請等待，直到應用程式移除操作完成。

當移除應用程式時，您的作業系統可能會要求重新啟動電腦。如果您決定不立即重新啟動電腦，應用程式移除過程的完成將在作業系統重新啟動或者直到電腦關閉並重新開啟後才能完成。

透過命令列移除程式

您可以從命令列啟動應用程式移除處理程序。可以使用互動模式或者靜默模式（無需啟動應用程式安裝精靈）進行移除。

要以互動模式啟動程式移除模式，

在命令列中鍵入 `setup.exe /x` 或 `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275}`。

啟動“安裝精靈”。按照“[安裝精靈](#)”的指示操作。

要以靜默模式啟動程式移除模式，

在命令列中鍵入 `setup.exe /s /x` 或 `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} /qn`。

這會以靜默模式啟動應用程式移除過程（無需啟動安裝精靈）。

如果應用程式移除操作受密碼防護，則應必須在命令列中輸入相應的使用者名稱和密碼。

為 *Kaspersky Endpoint Security* 移除、修改或修復的身分驗證設定使用者名稱和密碼時，若要使用命令列以互動模式移除程式，請執行以下操作：

在命令列中輸入 `setup.exe /pKLLLOGIN=<使用者名稱> /pKLPASSWD=***** /x` 或

`msiexec.exe KLLLOGIN=<User name> KLPASSWD=***** /x {7911E943-32CC-45D0-A29C-56E6EF762275}`。

啟動“安裝精靈”。按照“[安裝精靈](#)”的指示操作。

為 *Kaspersky Endpoint Security* 移除、修改或修復的身分驗證設定使用者名稱和密碼時，若要使用命令列以靜默模式移除程式，請執行以下操作：

在命令列中輸入 `setup.exe /pKLLLOGIN=<使用者名稱> /pKLPASSWD=***** /s /x` 或

`msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} KLLLOGIN=<User name> KLPASSWD=***** /qn`。

刪除測試執行身分驗證代理後的剩餘物件與資料

應用程式移除期間，如果 Kaspersky Endpoint Security 在身分驗證代理測試執行後偵測到系統硬碟上遺留物件和資料，則應用程式移除將被中斷且在刪除此類物件和資料之前無法繼續。

僅在例外情況下，當身分驗證代理測試執行後，遺留的物件和資料才能留在系統硬碟上。舉例來說，這可能發生在已套用卡斯基安全管理中心加密政策時，如果沒有重新啟動電腦，或者如果身分驗證代理測試執行後應用程式啟動失敗。

您可使用以下兩種方式來刪除測試執行身分驗證代理後剩餘的資料與物件：

- 使用卡斯基安全管理中心政策。
- 使用還原工具。

若要使用卡斯基安全管理中心政策，刪除測試身分驗證代理後剩餘資料與物件：

1. 將帶有配置為[解密](#)所有電腦硬碟設定的卡斯基安全管理中心政策套用至電腦。
2. 啟動 Kaspersky Endpoint Security。

若要使用還原工具，刪除測試身分驗證代理後剩餘資料與物件：

1. 在帶有身分驗證測試執行後存留物件和資料的系統硬碟的電腦上執行[使用 Kaspersky Endpoint Security 建立的 fdert.exeon](#) 可執行檔案啟動還原實用工具。
2. 在還原工具視窗中，在“**選擇裝置**”下拉清單中，選取物件和資料所在的系統硬碟。
3. 點擊“**掃描**”按鈕。
4. 點擊“**刪除 AA 物件與資料**”按鈕。

測試驗證代理操作後刪除物件與剩餘資料。

刪除物件與剩餘資料之後，您可能需要另外刪除與驗證代理不相容的應用程式資訊。

若要刪除與驗證代理不相容的應用程式資訊，請執行以下操作：

請在命令列中輸入 `avp pbatestreset`。

若要執行 `avp pbatestreset` 指令，必須安裝加密元件。

程式介面

該部分將說明程式介面的主要元素。

工作列通知區域中的程式圖示




Kaspersky Endpoint Security 安裝完成後，程式圖示將立即出現在 Microsoft Windows 工作列通知區域。

本圖示有以下功能：

- 顯示應用程式的活動。
- 是存取右鍵選單和應用程式主視窗的快速方式。

顯示應用程式的活動

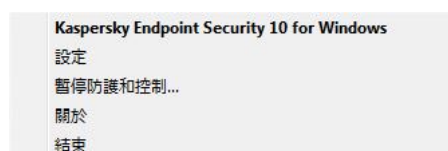
應用程式圖示可顯示應用程式的活動：

-  圖示表示應用程式的所有防護元件均已啟用。
-  圖示表示 Kaspersky Endpoint Security 目前有發生重要事件需要您的注意。例如，已關閉“檔案防護”或應用程式資料庫已過期。
-  圖示表示 Kaspersky Endpoint Security 目前有發生嚴重事件。範例，某個元件（或多個元件）的操作失敗或者程式資料庫損壞。

應用程式圖示的右鍵選單

應用程式圖示的右鍵選單包含下列項目：

- **Kaspersky Endpoint Security 10 for Windows**。開啟應用程式主視窗的“防護和控制”頁籤。“防護和控制”頁籤允許您調整應用程式元件執行工作和瀏覽已處理的檔案，及偵測到威脅的相關統計資料。
- **設定**。開啟程式主視窗的“設定”頁籤。“設定”頁籤允許您變更應用程式的預設設定。
- **暫停防護和控制/還原防護和控制**。此項目可暫時停止/還原應用程式防護元件的執行。此頁不會影響應用程式資料庫和模組更新工作或者為偵測病毒和其他威脅而進行的掃描工作。
- **停用政策/啟用政策**。停用/啟用卡巴斯基安全管理中心政策。此右鍵選單中，可以使用 Kaspersky Endpoint Security 工作政策，亦可關閉卡巴斯基安全中心政策已設定的密碼。
- **關於**。此項目可開啟一個包含應用程式詳細資訊的視窗。
- **結束**。本項目可結束 Kaspersky Endpoint Security。點擊右鍵選單中的“結束”項目會導致應用程式結束記憶體。



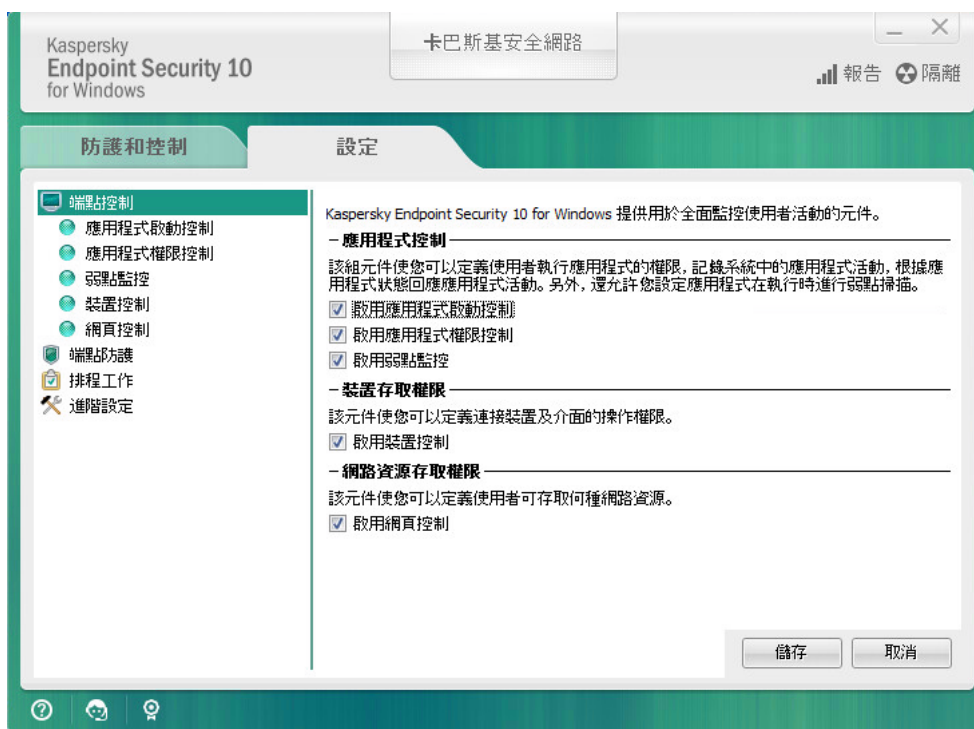
您可以將滑鼠指標放在 Microsoft Windows 工作列通知區域的程式圖示上並右鍵點擊開啟程式圖示的右鍵選單。

應用程式主視窗

Kaspersky Endpoint Security 主視窗包含的介面元素可讓使用者存取應用程式的主要功能。

主視窗分為四個部分（見下圖）：

- 位於視窗上半部的介面元素包含可讓您瀏覽以下資訊的介面元素：
 - 應用程式詳細資訊
 - 卡巴斯基安全網路統計資訊
 - 未處理的檔案清單
 - 偵測到的弱點清單
 - 隔離的檔案清單
 - 程式偵測到受感染的檔案的備份副本
 - 應用程式整體或個別元件執行期間或者工作執行期間發生的事件報告
- “**防護和控制**”頁籤可允許您調整應用程式元件和工作的執行和完成。開啟應用程式主視窗時即會出現“**防護和控制**”頁籤。
- “**設定**”頁籤允許您編輯應用程式預設設定。
- 視窗下方包含以下元素：
 - **按鈕** 。點擊此按鈕，將會開啟 Kaspersky Endpoint Security 說明文件。
 - **按鈕** 。點擊本按鈕，將開啟“**支援**”視窗，此視窗含有作業系統資訊、及目前 Kaspersky Endpoint Security 版本和 Kaspersky Lab 資源連結等資訊。
 - **按鈕**  / 。點擊本按鈕將開啟“**授權管理**”視窗，其中包含目前啟動授權檔案的詳細資訊。
 - **按鈕**  /  / 。點擊此按鈕將開啟 **事件** 視窗，包含有關可用更新以及請求存取加密檔案和裝置的資訊。按鈕只有在有存取和刪除更新的請求時才可用。



配置應用程式設定標籤

若要開啟應用程式設定標籤，執行以下操作之一：

- 在主應用程式視窗中，選取“設定”標籤。
- 在應用程式圖示的右鍵選單中，選取“設定”。

應用程式防護和控制頁籤

Kaspersky Endpoint Security 的防護和控制標籤用於提供有關所有工作執行的一般資訊和所有應用程式元件執行的一般資訊。在該標籤上，您也可以管理元件的執行和工作的操作。

應用程式防護和控制標籤包含三個部分（見下圖）：

- “**端點控制**”區域包含控制元件的清單。
- “**管理防護**”區域包含病毒防護元件的清單。
- “**工作**”區域包含電腦上所執行本機工作的清單。

每個區域都包含控制元素，您可以用以啟用或停用元件的執行，轉至選定元件或工作的設定，檢視選定元件或工作的操作統計資訊。



應用程式防護和控制頁籤

若要開啟應用程式防護和控制標籤，執行以下操作之一：

- 在應用程式主視窗中，選取“防護和控制”頁籤。
- 點擊 Microsoft Windows 工作通知欄上的應用程式圖示。
- 在應用程式圖示的上下文功能表中選取 **Kaspersky Endpoint Security 10 for Windows**。

應用程式產品授權

本部分提供了應用程式產品授權相關一般概念的資訊。

關於最終使用者產品授權協議

*最終使用者授權協議*是您與 Kaspersky Lab 之間達成的法律協議，它規定了您在使用所購買的應用程式時須遵循的條款。

建議您在使用應用程式前認真閱讀《產品授權協議》條款。

您可透過下列方式檢視此授權協議的條款：

- 以[互動模式](#)安裝 Kaspersky Endpoint Security 時。
- 透過閱讀 license.txt 檔案。此文件包括在[應用程式安裝套件](#)中。

安裝程式時確認您同意最終使用者產品授權協議即表示您同意最終使用者產品授權協議中的條款。如果您不同意最終使用者授權的協議，將會中止安裝。

關於授權

*產品授權*是根據最終使用者產品授權協議授予的在有限時間內使用本應用程式的權限。

有效的授權使您可獲得以下服務：

- 根據最終使用者產品授權協議的條款使用本應用程式
- 技術支援

程式功能及附加服務的使用期限取決於您的授權類型而定。

我們提供下列授權類型：

- **試用版** – 目的在於讓使用者熟悉該應用程式的免費授權。
試用版產品授權通常擁有較短的有效期。當試用版授權到期，所有 Kaspersky Endpoint Security 功能將轉為停用。要繼續使用此應用程式，您必須購買一個正式授權。
您只能使用試用產品授權啟動應用程式一次。
- **正式版** – 購買 Kaspersky Endpoint Security 的付費授權。
正式產品授權中所能使用的應用程式功能取決於所選產品。所選的產品指定在[產品授權憑證](#)中。可用產品的資訊可以在 [Kaspersky 網站](#) 上找到。
當正式版產品授權到期時，應用程式的關鍵功能將被停用。要繼續使用此應用程式，您必須續約正式產品授權。如果不打算續約產品授權，您必須從電腦移除應用程式。

關於產品授權憑證

產品授權憑證是傳送給使用者的一個帶有金鑰檔案或啟動碼的文件。

產品授權憑證包含以下產品授權資訊：

- 訂購號
- 被授予產品授權的使用者詳情
- 可以使用產品授權啟動的應用程式詳情
- 授權單元的數量限制（例如，可以在此產品授權下使用應用程式的裝置數量）
- 產品授權期限開始日期
- 產品授權到期日期或產品授權期限
- 產品授權類型

關於訂購

Kaspersky Endpoint Security 訂購是一項帶有特定參數（訂購到期日期，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。您可以手動或自動對訂購進行續約，也可以取消訂購。您可以在[服務供應商網站](#)上管理您的訂購。

訂購可以是有限訂購（範例一年時間）或無限訂購（無到期時間）。訂購到期後，若要使 *Kaspersky Endpoint Security* 繼續工作，您必須續約訂購。如果按時預支付供應商服務，則可以自動續約無限訂購。

對於有限訂購，訂購到期後您將獲得訂購續約寬限期，在此期間應用程式將繼續發揮全功能。服務供應商決定是否提供寬限期，如果提供，供應商將確定寬限期長度。

若要在訂購下使用 *Kaspersky Endpoint Security*，您需要套用從服務供應商處接收到的啟動碼。套用了啟動碼之後，將安裝啟動產品授權。啟動產品授權定義了在訂購中使用應用程式的產品授權。僅在使用啟動碼時可安裝其他產品授權。在使用產品授權檔案或在訂購中，不能安裝其他產品授權。

訂購中可用的應用程式功能取決於下列正式產品授權類型下的應用程式功能：標準、*Kaspersky Business Space Security*、*Kaspersky Enterprise Space Security* 此授權類型主要是為防護檔案伺服器、工作站與行動裝置而設計，並且支援使用管理元件管理工作站與行動裝置。

根據每個供應商的不同，可能的訂購管理選項亦有所不同。服務供應商可能不會提供用於續約訂購的寬限期，在此寬限期內程式仍發揮其功能。

在訂購下購買的啟動碼可能無法用於啟動先前版本的 *Kaspersky Endpoint Security*。

關於啟動碼

啟動碼為您購買 *Kaspersky Endpoint Security* 正式授權後取得的唯一的一串二十位元的拉丁字母和數位組合。

要用啟動碼啟動應用程式，需要網際網路接入連線到 Kaspersky 的啟動伺服器。

當應用程式使用啟動碼啟動時，將安裝啟動金鑰。僅在使用啟動碼時可安裝其他產品授權。在使用產品授權檔案或在訂購中，不能安裝其他產品授權。

如果啟動應用程式後遺失了啟動碼，則您可以還原啟動碼。您可能會需要啟動碼，例如用於註冊卡巴斯基公司帳戶。若要還原啟動碼，您必須[聯絡 Kaspersky 技術支援](#)。

關於產品授權

金鑰 一個特殊的字母數字序列。金鑰將依據最終使用者授權協議提供相應的產品功能（包含授權類型、授權有效期、授權限制）。

對於訂購中安裝的金鑰，不提供產品授權憑證。

您可以使用啟動碼或金鑰檔案將金鑰新增至應用程式。

您也可新增編輯或刪除金鑰。若違反了最終使用者授權協議的條款，則 Kaspersky 可以封鎖此金鑰。如果金鑰被列入黑名單，則您必須新增其他金鑰以繼續使用應用程式。

如果把到期產品授權的金鑰刪除掉，應用程式功能將不可用。您在刪除金鑰後無法再次新增此類別金鑰。

有兩種類型的金鑰：啟動金鑰和備用金鑰。

啟動金鑰是程式目前正在使用的金鑰。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。本應用程式不能擁有兩個及以上啟動金鑰。

備份金鑰使用者可新增一組目前尚未使用的金鑰。啟動金鑰到期後，備用金鑰將自動生效。在目前已有金鑰啟用下才能新增備用金鑰。

只能將試用版產品授權的金鑰以啟動金鑰的形式進行新增。無法將其新增為備用金鑰。試用版產品授權金鑰無法替換正式版產品授權的啟動金鑰。

如果某個金鑰被列入黑名單，[啟動應用程式所用的授權所覆蓋](#)的應用程式功能將可以執行八天。卡巴斯基安全網路和資料庫、程式模組更新不受限制，仍可以使用。通知使用者此金鑰已被列入黑名單。八天後程式功能將受限，僅限於產品授權到期後可使用的功能：程式可以執行，但是無法更新，卡巴斯基安全網路不可用。

關於產品授權檔案

金鑰檔案是您在購買 Kaspersky Endpoint Security 之後從 Kaspersky 接收到的 .key 副檔名的檔案。金鑰檔案的目的是新增能夠啟動應用程式的金鑰。

使用金鑰檔案無需連線至 Kaspersky 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卡巴斯基公司帳戶之類的服務。

若要還原金鑰檔案，請執行以下操作：

- 聯絡產品授權供應商。

- 基於您現有的啟動碼在 [Kaspersky Lab 網站上](#) 獲得金鑰檔案。

當使用金鑰檔案啟動應用程式時，將新增啟動金鑰。備用授權許可密鑰只能使用密鑰文件添加，而不能使用激活碼添加。

關於資料提交

接受《最終使用者產品授權協議》即表示您同意自動傳輸以下資訊：您對產品使用，所安裝程式的類型、版本和語言中文化，程式安裝程式的唯一識別碼和安裝類型，活動和備用金鑰上的資料（包括產品授權類型、有效期、程式啟動日期和產品授權到期日期，產品授權編號，產品授權的目前狀態，啟動伺服器互動協議版本）。

如果程式是用啟動碼啟動的，為了接收產品授權持有者的產品的分發和使用統計資訊，您同意自動提供正在使用的程式版本（包括已安裝程式更新的資訊、程式安裝識別碼和產品授權資訊），作業系統版本，和提供資訊時活動的程式元件識別碼。

Kaspersky Lab 將根據法律和 Kaspersky Lab 應用程式管理規定防護收到的資訊。

Kaspersky Lab 完全匿名使用收到的資訊並僅做一般統計之用。系統將使用原始收集的資訊自動產生一般統計資訊，不包含任何個人資料或其他機密資訊。原始收集的資訊將隨著資訊的積累而銷毀（每年一次）。一般統計資料永久儲存。

請閱讀最終使用者產品授權協議並存取 [Kaspersky Lab 網站](#) 瞭解當您接受《最終使用者產品授權協議》和同意《KSN 聲明》之後我們如何收集、儲存和銷毀有關程式使用的資訊。license.txt 和 ksn.txt 檔案包含《最終使用者產品授權協議》和《KSN 聲明》，是 [分發軟體套件](#) 的一部分。

檢視產品授權資訊

若要檢視授權資訊，請執行以下操作：

1. 開啟“[程式主視窗](#)”。
2. 點擊主應用程式視窗下方的  /  按鈕。

“**授權管理**”視窗將開啟。產品授權相關資訊將顯示在“**授權管理**”視窗的上部。

購買產品授權

您可以在安裝程式後購買授權。購買產品授權後，您將收到用於 [啟動應用程式](#) 的啟動碼或金鑰檔案。

要購買產品授權：

1. 開啟“[程式主視窗](#)”。
2. 點擊主應用程式視窗下方的  /  按鈕。
“**授權管理**”視窗將開啟。
3. 在“**授權管理**”視窗中，執行下列操作：
 - 如果您已安裝試用版授權，請點擊“**購買授權**”按鈕。
 - 如果您已安裝正式版授權，請點擊“**續約授權**”按鈕。

這時瀏覽器將開啟 Kaspersky 線上商店的視窗，您可以在此網站中購買產品授權。

續約授權

如果您的授權即將到期，您可以進行續約。這將確保在現有授權到期後，使用新的授權啟動應用程式前，您的電腦仍處於防護之中。

要續約授權，請執行以下操作：

1. [接收](#)新應用程式啟動碼或金鑰檔案。
2. 使用您接收的啟動碼或金鑰檔案 [新增備用金鑰](#)。

這就新增了 [備用金鑰](#)。它將在產品授權到期後變為 [啟動](#) 狀態。

根據 Kaspersky 啟動伺服器的負載分佈情況，金鑰從備用金鑰更新為啟動金鑰可能會需要一段時間。

續約訂購

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。

如果您在無限訂購下使用應用程式，Kaspersky Endpoint Security 將自動檢查啟動伺服器，以背景模式獲取續約的產品授權。如果啟動伺服器上有可用產品授權，應用程式會替換先前產品授權繼而新增此產品授權。透過這種方式，使用無限訂購的 Kaspersky Endpoint Security 無需使用者介入進行更新。

如果您在有限訂購下使用本應用程式，在訂購（或在訂購續約可用時，在訂購到期寬限期）到期之日，Kaspersky Endpoint Security 會顯示相應通知，並停止自動續約嘗試。在這種情況下，Kaspersky Endpoint Security 將與 [正式版應用程式](#) 到期一樣的方式執行：應用程式執行但是沒有更新且卡斯基安全網路不可用。

您可以在 [服務提供者的網站上續約訂購](#)。

您可以在“[產品授權](#)”視窗中手動更新訂購狀態。如果在寬限期到期後對訂購進行續約並且訂購狀態未自動更新時，您需要執行此操作。

存取服務提供者網站

若要從程式介面中存取服務供應商網站，請執行以下操作：

1. 開啟“[程式主視窗](#)”。
2. 點擊主應用程式視窗下方的  /  按鈕。
“[授權管理](#)”視窗將開啟。
3. 在“[產品授權](#)”視窗中點擊“[聯絡您的訂購供應商](#)”。

關於程式啟動方法

啟動是一種啟動授權的過程，允許您在授權到期前使用完整的產品功能。在程式啟動過程中新增授權。

您可以採用以下方式啟動應用程式：

- 安裝應用程式時，使用[初始化配置精靈的說明](#)。您可以透過以下方式來新增啟動授權。
- 透過使用[啟動精靈](#)從應用程式介面本機完成，您可以使用這種方式新增啟動金鑰和備用金鑰。
- 透過[建立](#)和[啟動](#)新增金鑰工作遠端使用卡巴斯基安全管理中心軟體套件。您可使用此方式同時新增啟動與備用金鑰。
- 透過將儲存在卡巴斯基安全管理中心管理伺服器的金鑰儲存中的金鑰和啟動碼自動分發到用戶端電腦上進行遠端管理（詳細資訊請參見《[卡巴斯基安全管理中心管理手冊](#)》）。您可使用此方式同時新增啟動與備用金鑰。



在訂購下購買的啟動碼位於第一位。

- 使用[命令列](#)。

根據 Kaspersky 的啟動伺服器的負載分佈情況，（在遠端安裝或非互動安裝時）程式用啟動碼啟動可能會花一定時間。若您需要立即啟動應用程式，您可能需要中斷正在進行的啟動過程，並使用啟動精靈進行啟動。

使用啟動精靈啟動程式

要使用啟動精靈啟動 Kaspersky Endpoint Security，請執行以下操作：

1. 點擊主應用程式視窗下方的  /  按鈕。
“授權管理”視窗將開啟。
2. 在“授權管理”視窗，點擊“使用新授權啟動應用程式”按鈕。
應用程式啟動精靈將啟動。
3. 按照啟動精靈的指示操作。

有關應用程式啟動步驟的詳細資訊，請參閱[初始化配置精靈](#)區域。

透過命令列啟動程式

透過命令列安裝程式。

在命令列中輸入 `avp.com license /add <啟動碼或金鑰檔案> /password=<密碼>`。

啟動和停止應用程式

本章節包含關於如何設定程式的自動啟動、如何手動啟動或停止程式以及如何暫停或繼續執行防護和控制元件的資訊。

啟動和停用應用程式自動啟動

自動啟動表示在作業系統啟動後會立即開啟 Kaspersky Endpoint Security，無需使用者另外操作。此程式啟動選項為預設的啟動狀態。

安裝 Kaspersky Endpoint Security 後，它會在首次執行時自動啟動。之後，每次作業系統啟動後該程式都會自動啟動。

根據電腦效能，啟動作業系統後下載 Kaspersky Endpoint Security 病毒防護軟體會花費兩分鐘時間。在該期間電腦防護等級降低。當 Kaspersky Endpoint Security 已經在載入的作業系統中啟動時下載病毒資料庫不會導致電腦防護等級的降低。

要啟用或停用程式自動啟動，請執行下列操作：

1. 開啟[程式設定視窗](#)。
2. 選取左側的“**端點防護**”區域。
端點防護設定將顯示在視窗右方。
3. 請執行以下操作之一：
 - 要啟程式自動執行，請選定“**在電腦啟動時執行 Kaspersky Endpoint Security 10 for Windows**”核取方塊。
 - 要停程式自動執行，請清除“**在電腦啟動時執行 Kaspersky Endpoint Security 10 for Windows**”核取方塊。
4. 要儲存變更，請點擊“**儲存**”按鈕。

手動啟動和停止程式

Kaspersky 專家建議您不要手動停止 Kaspersky Endpoint Security，因為這樣做會使電腦和您的個人資料曝露於威脅之中。如有必要，您可以根據需要[暫停電腦防護](#)而無需停止應用程式。

如果您先前停用了[應用程式自動啟動](#)，則 Kaspersky Endpoint Security 需要手動啟動。

要手動啟動程式，請執行下列操作：

在“**開始**”功能表中選取“**程式**”→“ Kaspersky Endpoint Security 10 for Windows”。



要手動停止程式，請執行下列操作：

1. 在工作列通知區域按右鍵程式圖示，開啟右鍵選單中。
2. 在右鍵選單中，選取“**結束**”。

暫停和還原電腦防護和控制

暫停電腦防護和控制表示停用 Kaspersky Endpoint Security 的所有防護和控制元件一段時間。

應用程式狀態使用[工作列通知區域中應用程式圖示進行顯示](#)。

-  圖示表示電腦防護和控制已暫停。
-  圖示表示電腦防護和控制已還原。

暫停或還原電腦防護和控制不影響掃描工作或程式更新工作。

如果在暫停或還原電腦防護和控制時已建立任何網路連線，系統會顯示關於終止這些網路連線的通知。

暫停電腦防護和控制：

1. 在工作列通知區域按右鍵程式圖示，開啟右鍵選單中。
2. 在右鍵選單中，選取“**暫停防護和控制**”。
系統將開啟開啟“**暫停防護**”視窗。
3. 從以下選項中選取一個選項：
 - **暫停防護時間** – 經過下面的下拉清單中所指定的時間後還原電腦防護和控制。
 - **重新啟動程式後還原防護** – 結束並重新開啟應用程式或重新啟動作業系統後還原電腦防護和控制。若要使用此選項，必須啟用應用程式的自動啟動。
 - **暫停** – 在您決定重新啟用時還原電腦防護和控制。
4. 如果您在上一步驟中選取了“**暫停指定時間**”選項，則在下拉清單中選取所需的間隔。

還原電腦防護和控制：

1. 在工作列通知區域按右鍵程式圖示，開啟右鍵選單中。
2. 在右鍵選單中，選取“**還原防護和控制**”。

如果您決定還原電腦防護和控制，可以隨時進行該操作，這與您之前選取的防護暫停選項無關。

防護電腦檔案系統檔案防護

本章節介紹關於檔案防護的資訊以及如何設定元件的說明。

關於檔案防護

檔案防護可避免電腦的檔案系統受感染。預設情況下，檔案防護將與作業系統一起啟動，一直停留在記憶體中，掃描所有電腦和磁碟上附加到檔案防護的開啟、儲存或執行的檔案，偵測是否存在病毒和其他威脅。

如果 Kaspersky Endpoint Security 在檔案中偵測到威脅，它將向該檔案分配下列狀態：

1. 指示偵測到惡意程式類型（例如 *病毒* 或 *木馬*）的狀態。
2. 如果掃描無法確定檔案是否受感染，則將其標記為 *疑似感染*。電子郵件可能包含典型病毒或其他惡意程式的代碼序列，或已知病毒的變種。
3. 該應用程式將顯示在檔案中偵測到的惡意物件的 [通知](#)（如果配置了通知），並按照檔案防護設定中指定的 [動作](#) 處理檔案。





啟用和停用檔案防護

預設情況下，將會啟用檔案防護功能。您可以在必要時停用檔案防護。

有兩種啟動或停用該元件的方式：

- 透過 [應用程式主視窗](#) 的“**防護和控制**”頁籤。
- 開啟 [程式設定視窗](#)。

要啟用或停用檔案防護，請在程式主視窗的防護和控制頁籤中執行以下操作：

1. 開啟“程式主視窗”。
2. 選擇“**防護和控制**”頁籤。
3. 點擊“**防護**”區域。
開啟“**防護**”區域。
4. 右鍵點擊“檔案防護”元件，開啟有資訊說明的右鍵選單。
系統將開啟一個用於選擇對該元件的操作功能表。
5. 請執行以下操作之一：
 - 要啟用檔案防護，請在功能表中選取“**開始**”。
“**檔案防護**”行左側的元件狀態圖示  將變為圖示 .
 - 要停用檔案防護，請在功能表中選取“**停止**”。
“**檔案防護**”行左側的元件狀態圖示  將變為圖示 .

要從程式設定視窗中啟用或停用檔案防護，請執行下列操作：

1. 開啟程式設定視窗。
2. 在視窗左側的“端點防護”區域中，選取“檔案防護”子區域。
在視窗右側，將顯示檔案防護元件的設定。
3. 請執行以下操作之一：
 - 如果要啟用檔案防護，請選取“**啟用檔案防護**”核取方塊。
 - 如果要停用檔案防護，請選取“**停用檔案防護**”核取方塊。
4. 要儲存變更，請點擊“**儲存**”按鈕。

自動暫停檔案防護

您可以設定檔案防護在特定時間或處理特定程式時自動暫停。

檔案防護功能因衝突而暫停是一種緊急措施。如果在元件執行過程中發生任何衝突，建議您與 Kaspersky Lab 技術支援服務 (<https://companyaccount.kaspersky.com>) 聯絡。支援專家將幫助您設定檔案防護，使其能與電腦上的其他程式同時執行。

自動暫停檔案防護：

1. 開啟 [程式設定視窗](#)。
2. 在視窗左側的“端點防護”區域中，選取“檔案防護”子區域。
在視窗右側，將顯示檔案防護元件的設定。
3. 在“安全防護等級”區域中點擊“設定”按鈕。
開啟“檔案防護”視窗。
4. 在“檔案防護”視窗中，選擇“附加”頁籤。
5. 在“暫停工作”區域：
 - 要設定檔案防護在特定時間自動暫停，請選取“**根據排程**”然後點擊“**排程**”按鈕。
開啟“**暫停工作**”視窗。
 - 要設定檔案防護在特定程式啟動時自動暫停，請選取“**在程式啟動後**”核取方塊，然後點擊“**選取**”按鈕。
開啟“**應用程式**”視窗。
6. 請執行以下操作之一：
 - 如果要設定檔案防護在特定時間自動暫停，請在“**暫停工作**”視窗中，使用“**暫停工作時間**”和“**還原工作時間**”欄位中指定檔案防護的暫停時間（格式為小時：分鐘）。點擊“**確定**”。
 - 如果要設定檔案防護在特定程式啟動時自動暫停，請在“**應用程式**”視窗中，使用“**新增**”、“**編輯**”和“**刪除**”按鈕，建立一個應用程式清單，以便使這些應用程式在執行時暫停“檔案防護”功能。點擊“**確定**”。

7. 在“檔案防護”視窗中點擊“確認”。
8. 要儲存變更，請點擊“儲存”按鈕。

設定檔案防護

您可以執行以下操作來設定檔案防護：

- 變更安全防護等級。
您可以選擇某種預設的安全防護等級或手動配置安全性等級的設定。如果您改變了檔案安全防護等級設定，仍可隨時還原到建議的檔案安全防護等級設定。
- 變更檔案防護對受感染檔案執行的偵測操作。
- 編輯檔案防護的防護範圍
您可以透過新增或刪除掃描物件，或透過變更掃描檔案類型擴充或限制防護範圍。
- 設定啟發式分析。
檔案防護使用一種稱為特徵碼分析的技術。在特徵碼分析中，檔案防護將偵測物件與其程式防護資料庫中的記錄進行相符。根據 Kaspersky Lab 專家的建議，特徵分析將處於常時啟動狀態。
您可以使用啟發式分析提高防護效率。在啟發式分析中，檔案防護在作業系統中分析物件的行為。啟發式分析啟用偵測那些在程式防護資料庫中目前不存在的可用記錄的惡意物件。
- 優化掃描。
您可以最佳化檔案防護執行的檔案掃描以便減少掃描時間，提高 Kaspersky Endpoint Security 的執行速度。這可以透過僅掃描新檔案和上次掃描後經過修改的檔案來實現。此模式適用於簡單檔案和複合檔案。
您也可以啟用 iChecker 和 iSwift 技術，在掃描中排除最近一次掃描後未修改的檔案，從而最佳化檔案掃描速度。
- 設定複合檔案的掃描。
- 變更檔案掃描模式。

變更安全防護等級

為了防護電腦檔案系統，檔案防護應用各種不同的設定組。這些設定組稱為 *安全防護等級*。有三種預設的安全防護等級：**高**、**建議**和**低**。**建議防護**安全防護等級設定將被視為 Kaspersky 專家建議的最佳設定。

要變更安全防護等級：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點防護”區域中，選取“檔案防護”子區域。
在視窗右側，將顯示檔案防護元件的設定。
3. 在“安全防護等級”區域中執行下列操作：
 - 如果您希望設定一種預設的安全防護等級（**高**、**建議**或**低**），請使用移動滑桿選取。

- 如果您希望設定自訂安全防護等級，則點擊“**設定**”按鈕，在開啟的“**檔案防護**”視窗中輸入自訂設定。您設定自訂安全防護等級之後，“**安全防護等級**”區域中安全防護等級的名稱將變更為“**自訂**”。
- 如果您希望將安全防護等級變更為“**建議**”，點擊“**預設**”按鈕。

4. 要儲存變更，請點擊“**儲存**”按鈕。

變更檔案防護對受感染檔案執行的操作

若要變更檔案防護對受感染檔案執行的操作，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**端點防護**”區域中，選取“**檔案防護**”子區域。
在視窗右側，將顯示檔案防護元件的設定。
3. 在“**偵測到威脅後的動作**”區域，選取所需的模式：

- **自動選擇動作**。
- **執行操作：解毒**。如果解毒失敗刪除。
- **執行操作：解毒**。

若選取此選項，Kaspersky Endpoint Security 則會將 Windows Store 應用程式，套用在“**刪除**”行動中。

- **執行操作：刪除**。
- **執行操作：封鎖**。

4. 要儲存變更，請點擊“**儲存**”按鈕。

編輯檔案防護的防護範圍

防護範圍是指元件啟用時的掃描物件。不同元件的防護範圍有不同的參數。檔案防護的防護範圍的內容即所掃描檔案的位置和類型。檔案防護預設只掃描儲存於硬碟、網路磁碟或卸除式媒體中的[可感染檔案](#)。

要建立防護範圍，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**端點防護**”區域中，選取“**檔案防護**”子區域。
在視窗右側，將顯示檔案防護元件的設定。
3. 在“**安全防護等級**”區域中點擊“**設定**”按鈕。
開啟“**檔案防護**”視窗。

4. 在“**檔案防護**”視窗中，選取“**一般**”頁籤。

5. 在“**檔案類型**”區域中，請指定您希望檔案防護掃描的檔案的類型：

- 如果您希望掃描所有檔案，請選取“**所有檔案**”。
- 如果您希望根據其格式掃描最易被感染的檔案，請選取“**依格式掃描檔案**”。
- 如果您希望依據其副檔名掃描最容易受感染的檔案，請選取“**依副檔名掃描檔案**”。

選取需要掃描的檔案類型時，請注意：

- 部分檔案格式（如 .txt），惡意程式碼入侵並執行的可能性相當低。同時，部分檔案格式會包含或可能會包含惡意程式碼（如 .exe、.dll 和 .doc）。這些檔案中，惡意程式碼入侵並執行的可能性相當高。
- 入侵者可能會把可執行檔案的副檔名重新命名為 .txt，然後將其中的病毒或其他惡意程式傳送到您的電腦中。如果您選取按副檔名掃描檔案，掃描中會略過這類檔案。如果您選取依格式掃描檔案，而不考慮副檔名，檔案防護將分析檔案頭。這種分析可以顯示該檔案為 .exe 格式。程式將徹底掃描此類檔案以尋找病毒和其他惡意程式。

6. 在“**防護範圍**”區域中執行下列操作：

- 若要將新物件新增至掃描範圍，請點擊“**新增**”按鈕。
- 如果您希望變更一個物件的位置，請從掃描範圍中選取此物件，然後點擊“**編輯**”按鈕。

開啟“**選取掃描範圍**”。

- 如果您希望從掃描物件清單中刪除一個物件，請在掃描物件清單中選取此物件，然後點擊“**刪除**”按鈕。螢幕上將開啟確認刪除視窗。

7. 請執行以下操作之一：

- 如果您希望在掃描物件清單中新增一個新的物件，或者變更一個物件的位置，請在“**選取掃描範圍**”視窗中選取一個物件，然後點擊“**新增**”按鈕。
“**選取掃描範圍**”視窗中選取的所有物件都將顯示在“**檔案防護**”視窗中的“**防護範圍**”清單內。
點擊“**確定**”。
- 如果您希望刪除一個物件，請在確認刪除視窗中點擊“**是**”按鈕。

8. 如有必要，可重複第 6-7 步以便掃描物件清單中新增物件、變更位置，或刪除物件。

9. 要從掃描物件清單中排除一個物件，請在“**防護範圍**”清單中清空此物件旁邊的核取方塊。但是，此物件仍保留在掃描物件清單中，但不在檔案防護掃描中。

10. 在“**檔案防護**”視窗中點擊“**確認**”。

11. 要儲存變更，請點擊“**儲存**”按鈕。

配合啟發式分析使用檔案防護

若要在檔案防護執行中設定使用啟發式分析，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點防護”區域中，選取“檔案防護”子區域。
在視窗右側，將顯示檔案防護元件的設定。
3. 在“安全防護等級”區域中點擊“設定”按鈕。
開啟“檔案防護”視窗。
4. 在“檔案防護”視窗中選擇“效能”頁籤。
5. 在“掃描方式”區域中：
 - 如果您希望檔案防護使用啟發式分析，請選取“啟發式分析”核取方塊，使用滑塊設定啟發式分析具體等級：輕度掃描、中度掃描或深度掃描。
 - 如果您不希望檔案防護使用啟發式分析，請清空“啟發式分析”核取方塊。
6. 點擊“確定”。
7. 要儲存變更，請點擊“儲存”按鈕。

在檔案防護操作中使用掃描技術

配置在檔案防護操作中使用掃描技術：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點防護”區域中，選取“檔案防護”子區域。
在視窗右側，將顯示檔案防護元件的設定。
3. 在“安全防護等級”區域中點擊“設定”按鈕。
開啟“檔案防護”視窗。
4. 在“檔案防護”視窗中，選擇“附加”頁籤。
5. 在“暫停工作”區域中：
 - 選取您在檔案防護操作中要使用的技術名稱所對應的核取方塊。
 - 清除您不想在檔案防護操作中使用的技術名稱所對應的核取方塊。
6. 點擊“確定”。
7. 要儲存變更，請點擊“儲存”按鈕。

最佳化檔案掃描

要最佳化檔案掃描，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**端點防護**”區域中，選取“**檔案防護**”子區域。
在視窗右側，將顯示檔案防護元件的設定。
3. 點擊“**設定**”按鈕。
開啟“**檔案防護**”視窗。
4. 在“**檔案防護**”視窗中選擇“**效能**”頁籤。
5. 在“**掃描最佳化**”區域中選取“**只掃描新增及變更的檔案**”核取方塊。
6. 點擊“**確定**”。
7. 要儲存變更，請點擊“**儲存**”按鈕。

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，例如存檔案或電子郵件資料庫中。為了偵測以這種方式隱藏的病毒和其他惡意程式，必須將複合檔案解壓縮，但是這可能會降低掃描速度。您可以限制掃描複合檔案的設定，從而加快掃描速度。

用於處理受感染複合檔案（解毒或刪除）的方法取決於檔案類型。

檔案防護會解毒 RAR、ARJ、ZIP、CAB 和 LHA 格式的複合檔案並刪除所有其他格式的檔案（郵件資料庫除外）。

若要設定複合檔案的掃描，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**端點防護**”區域中，選取“**檔案防護**”子區域。
在視窗右側，將顯示檔案防護元件的設定。
3. 在“**安全防護等級**”區域中點擊“**設定**”按鈕。
開啟“**檔案防護**”視窗。
4. 在“**檔案防護**”視窗中選擇“**效能**”頁籤。
5. 在“**掃描複合檔案**”區域中指定您希望掃描的複合檔案類型：壓縮檔案、安裝套件或 Office 格式檔案。
6. 若要僅掃描新增和變更的複合檔案，請選取“**僅掃描新增和變更的檔案**”核取方塊。
檔案防護將僅掃描所有類型的新增和變更的複合檔案。
7. 點擊 **附加** 按鈕。
螢幕上將開啟**複合檔案** 視窗。

8. 在“**背景掃描**”區域中執行下列操作：

- 若要封鎖檔案防護在背景解壓縮複合檔案，請清空“**在背景解壓複合檔案**”核取方塊。
- 如果允許檔案防護在背景模式解壓縮大型複合檔案，請選取“**在背景解壓複合檔案**”核取方塊，並在“**檔案大小下限**”欄位中指定所需值。

9. 在 **容量限制** 區域中可執行下列操作：

- 如果封鎖檔案防護解壓縮大型複合檔案，請選中“**不解壓大型複合檔案**”核取方塊，並在“**最大檔案容量**”欄位中指定所需值。檔案防護不會解壓縮大於指定大小的複合檔案。
- 若要允許檔案防護解壓縮大型複合檔案，請清空“**不解壓大型複合文件**”核取方塊。
如果檔案容量超出“**最小檔案容量**”欄位的值，則此檔案將被分類為大型檔案。

無論是否選取“**複合檔案大於指定值時不解壓縮**”核取方塊，檔案防護均會掃描從壓縮檔案解壓縮出的大型檔案。

10. 點擊“**確定**”。

11. 在“**檔案防護**”視窗中點擊“**確認**”。

12. 要儲存變更，請點擊“**儲存**”按鈕。

變更掃描模式

*掃描模式*是指檔案防護開始掃描檔案的條件。預設情況下，Kaspersky Endpoint Security 以智慧模式掃描檔案。在此檔案掃描模式下，檔案防護將確定是否在使用者、應用程式（以使用者身分在登入的帳戶下或用不同帳戶）或作業系統對檔案執行分析操作後掃描檔案。例如，當操作某個 Microsoft Office Word 手冊時，Kaspersky Endpoint Security 將在其首次開啟和最後一次關閉時掃描該檔案。覆蓋檔案的操作過程不會掃描檔案。

若要變更檔案掃描模式，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**端點防護**”區域中，選取“**檔案防護**”子區域。
在視窗右側，將顯示檔案防護元件的設定。
3. 在“**安全防護等級**”區域中點擊“**設定**”按鈕。
開啟“**檔案防護**”視窗。
4. 在“**檔案防護**”視窗中，選擇“**附加**”頁籤。
5. 在“**掃描模式**”區域，選取所需的模式：
 - 智慧模式。
 - 存取及修改。
 - 存取。

- 執行。

6. 點擊“**確定**”。

7. 要儲存變更，請點擊“**儲存**”按鈕。

電子郵件防護。郵件防護

如果將 Kaspersky Endpoint Security 安裝在執行 Microsoft Windows for workstations 的電腦上，則可使用此元件。如果將 Kaspersky Endpoint Security 安裝在執行 [Microsoft Windows 以做檔案伺服器之用](#) 的電腦上，則此元件無法使用。

本章節介紹郵件防護資訊，以及如何設定元件。

關於郵件防護

郵件防護掃描將傳送和接收電子郵件訊息是否有病毒和其他威脅。它與 Kaspersky Endpoint Security 一起開始執行，一直保留在記憶體中，掃描所有透過 POP3、SMTP、IMAP、MAPI 和 NNTP 協定傳送或接收的電子郵件。如果沒有在郵件中偵測到安全威脅，則使用者可以接收或處理該郵件。

如果在檔案中偵測到威脅，Kaspersky Endpoint Security 將向該檔案分配下列狀態：

1. 識別電子郵件中所偵測物件的類型（例如木馬）。
2. 電子郵件分配到以下狀態之一：
 - **疑似感染**。如果掃描無法確定電子郵件是否被感染，則分配該狀態。電子郵件訊息可能包含典型病毒或惡意軟體的程式碼片段，或已知病毒的變種。
 - **已感染**。如果電子郵件掃描發現了包括了 Kaspersky Endpoint Security 資料庫中已知的病毒代碼片段，則將該狀態分配給物件。
 - **未發現**。如果電子郵件掃描未偵測到病毒或其他威脅，則將該狀態分配給物件。

應用程式將封鎖該電子郵件，顯示有關已偵測物件的[通知](#)（如果在通知設定中進行了指定），並執行郵件防護設定中指定的操作。

此元件安裝將與電腦上的電子郵件用戶端進行相互運作。Microsoft Office Outlook® 郵件用戶端可使用可嵌入的延伸外掛程式讓您精調郵件掃描設定。“郵件防護”外掛程式在安裝 Kaspersky Endpoint Security 期間已嵌入在 Microsoft Office Outlook 郵件用戶端中。

工作列通知區域中顯示的郵件防護圖示可指示程式正在執行。每當掃描電子郵件時，該圖示都顯示為 。

啟動和停用郵件防護





預設情況下，郵件防護功能已啟用並且以 Kaspersky Lab 專家建議的模式執行。您可以在必要時停用郵件防護。

有兩種啟動或停用該元件的方式：

- 透過 [應用程式主視窗](#) 的“防護和控制”頁籤。
- 開啟 [程式設定視窗](#)。

要啟用或停用郵件防護，請在程式主應用視窗的“防護和控制”頁籤中執行以下操作：

1. 開啟“程式主視窗”。

2. 選擇“**防護和控制**”頁籤。
3. 點擊“**防護**”區域。
開啟“**防護**”區域。
4. 右鍵點擊“郵件防護”元件，開啟有資訊說明的右鍵選單。
系統將開啟一個用於選擇對該元件的操作功能表。
5. 請執行以下操作之一：
 - 要啟用郵件防護，請在功能表中選取“**開始**”。
郵件防護左側顯示的元件狀態圖示  將變為圖示 。
 - 要停用郵件防護，請在功能表中選取“**停止**”。
郵件防護左側顯示的元件狀態圖示  將變為圖示 。

若要從應用程式設定視窗中啟用或停用郵件防護，請執行以下操作：

1. 開啟程式設定視窗。
2. 在視窗左側的“**端點防護**”區域中，選取“**郵件防護**”區域。
在視窗右側將顯示“郵件防護”元件的設定。
3. 請執行以下操作之一：
 - 如果要啟用郵件防護，請選取“**啟用郵件防護**”核取方塊。
 - 如果要停用郵件防護，請清空“**啟用郵件防護**”核取方塊。
4. 要儲存變更，請點擊“**儲存**”按鈕。

設定郵件防護

您可以執行下列操作來設定郵件防護：

- 變更郵件安全等級。
您可以選取某個預設的電子郵件安全防護等級，也可以設定自訂電子郵件安全防護等級。
如果您變更了電子郵件安全防護等級，您可以隨時還原為建議的電子郵件安全防護等級設定。
- 變更 Kaspersky Endpoint Security 對受感染電子郵件的操作。
- 編輯郵件防護的防護範圍。
- 設定電子郵件複合檔案附件的掃描。
您可以啟用或停用掃描郵件附件，限制要掃描的郵件附件的最大大小並限制郵件附件最大掃描時長。
- 按電子郵件附件類型設定篩選。
按類型篩選郵件附件允許自動重新命名或刪除指定類型的檔案。

- 設定啟發式分析。

您可以使用**啟發式分析**提高防護效率。在啟發式分析中，Kaspersky Endpoint Security 將分析應用程式在作業系統中的活動。啟發式分析可偵測在 Kaspersky Endpoint Security 資料庫中目前不存在記錄的電子郵件訊息中的威脅。

- 在 Microsoft Office Outlook 中設定電子郵件掃描。

使用為 Microsoft Office Outlook 電子郵件用戶端設計的可嵌入延伸外掛程式，您可以輕鬆地配置電子郵件掃描設定。

使用其他電子郵件用戶端（包括 Microsoft Outlook Express®、Windows Mail 和 Mozilla™ Thunderbird™）時，郵件防護元件將掃描 SMTP、POP3、IMAP 和 NNTP 郵件協定的流量。

使用 Mozilla Thunderbird 郵件用戶端時，如果使用篩檢程式將訊息移出“**收件箱**”資料夾，郵件防護將不能掃描病毒、其他惡意程式或經由 IMAP 協定傳送的電子郵件。

變更郵件安全防護等級

郵件防護應用各種不同的設定組以防護郵件。這些設定組稱為**電子郵件安全防護等級**。有三種電子郵件安全防護等級：**高**、**建議**和**低**。**建議防護**檔案安全防護等級可視為最佳設定，是 Kaspersky 建議採用的等級。

要變更電子郵件安全防護等級，請執行以下操作：

1. 開啟**程式設定視窗**。
2. 在視窗左側的“**端點防護**”區域中，選取“**郵件防護**”區域。
在視窗右側將顯示“郵件防護”元件的設定。
3. 在“**安全防護等級**”區域中執行下列操作：
 - 如果您希望安裝一種預設的電子郵件安全等級（**高**、**建議**或**低**），請使用捲軸選取一個等級。
 - 如果您希望設定一種自訂電子郵件安全防護等級，請點擊“**設定**”按鈕，在開啟的“**郵件防護**”視窗中指定設定。
您設定自訂郵件安全防護等級之後，“**安全防護等級**”區域中郵件安全防護等級的名稱將變更為“**自訂**”。
 - 如果您希望將電子郵件安全防護等級變更為“**建議**”，請點擊“**預設**”按鈕。
4. 要儲存變更，請點擊“**儲存**”按鈕。

變更對受感染電子郵件採取的操作

若變更對受感染電子郵件執行的操作，請執行以下操作：

1. 開啟**程式設定視窗**。
2. 在視窗左側的“**端點防護**”區域中，選取“**郵件防護**”區域。
在視窗右側將顯示“郵件防護”元件的設定。
3. 在“**偵測到威脅後的動作**”區域中選取 Kaspersky Endpoint Security 對偵測到受感染郵件執行的操作：

- 自動選擇動作。
- 執行操作：解毒。如果解毒失敗刪除。
- 執行操作：解毒。
- 執行操作：刪除。
- 執行操作：封鎖。

4. 要儲存變更，請點擊“儲存”按鈕。

編輯郵件防護的防護範圍

防護範圍是指活動時被該元件掃描的物件。不同元件的防護範圍有不同的參數。“郵件防護”的防護範圍內容包括將郵件防護整合至電子郵件用戶端的設定、電子郵件訊息類型，以及被“郵件防護”掃描流量的電子郵件類型和電子郵件協定。預設情況下，Kaspersky Endpoint Security 將掃描透過 POP3、SMTP、NNTP 和 IMAP 協定進出的電子郵件和流量，並且該掃描與 Microsoft Office Outlook 電子郵件用戶端相整合。

若要建立防護範圍，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點防護”區域中，選取“郵件防護”區域。
在視窗右側將顯示“郵件防護”元件的設定。
3. 點擊“設定”按鈕。
螢幕上將開啟“郵件防護”視窗。
4. 選取“一般”標籤。
5. 在“防護範圍”區域中執行以下操作：
 - 如果希望“郵件防護”掃描電腦上的所有接收的電子郵件和傳送的電子郵件，請選取“接收和傳送的郵件”選項。
 - 如果希望郵件防護只掃描電腦中的接收電子郵件，請選取“僅接收的郵件”選項。

如果您選取僅掃描接收的郵件，建議為所有傳送的郵件執行一次性掃描，因為有可能您的電腦存有郵件蠕蟲病毒並且會透過郵件傳播。這有助於避免因未監控電腦大量電子郵件散播而造成的問題。

6. 在“網路可用性”區域中執行下列操作：
 - 如果您希望“郵件防護”在經由 POP3、SMTP、NNTP 和 IMAP 協議傳送的電子郵件到達電腦之前進行掃描，請選取“POP3 / SMTP / NNTP / IMAP 流量”核取方塊。
如果您不希望“郵件防護”在經由 POP3、SMTP、NNTP 和 IMAP 協議傳送的電子郵件到達電腦之前進行掃描，請清空“POP3 / SMTP / NNTP / IMAP 流量”核取方塊。在這種情況下，如果選定了“附加：Microsoft Office Outlook 延伸”核取方塊，使用者電腦上接收到郵件時，郵件將經過 Microsoft Office Outlook 郵件用戶端中嵌入的郵件防護延伸外掛程式的掃描。

如果您使用非 Microsoft Office Outlook 電子郵件用戶端，當清空“POP3 / SMTP / NNTP / IMAP 流量”核取方塊後，經由 POP3、SMTP、NNTP 和 IMAP 協議傳送的郵件將不被郵件防護掃描。

- 如果您希望從 Microsoft Office Outlook 存取“郵件防護”設定並且希望經由 POP3、SMTP、NNTP、IMAP 和 MAPI 協議傳送的郵件在到達電腦後由嵌入在 Microsoft Office Outlook 的延伸外掛程式進行掃描，請選取“附加：Microsoft Office Outlook 延伸外掛程式”核取方塊。

如果您想封鎖從 Microsoft Office Outlook 存取“郵件防護”設定並且停用經由 POP3、SMTP、NNTP、IMAP 和 MAPI 協議傳送的郵件在到達電腦後由嵌入在 Microsoft Office Outlook 的延伸外掛程式進行掃描，請清空“附加：Microsoft Office Outlook 延伸外掛程式”核取方塊。

“郵件防護”外掛程式在安裝 Kaspersky Endpoint Security 期間已嵌入在 Microsoft Office Outlook 郵件用戶端中。

7. 點擊“確定”。
8. 要儲存變更，請點擊“儲存”按鈕。

掃描附加於電子郵件中的複合檔案

若要設定對附加於電子郵件中的複合檔案掃描：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“病毒防護”區域中，選取“郵件防護”子區域。
在視窗右側將顯示“郵件防護”元件的設定。
3. 點擊“設定”按鈕。
螢幕上將開啟“郵件防護”視窗。
4. 選取“一般”標籤。
5. 在“掃描複合檔案”區域執行以下操作：
 - 如果您希望郵件防護略過電子郵件附件的存檔，請取消選取“掃描附件中的存檔”核取方塊。
 - 如果您希望“郵件防護”略過大小超過 N MB 的電子郵件附件，請選取“略過掃描，若檔案大小超過 N MB”核取方塊。如果您選取此核取方塊，請在核取方塊名稱對應的欄位中指定最大物件容量。
 - 如果您希望“郵件防護”掃描所需掃描時間超過 N 秒的電子郵件附件，請選取“不對掃描時間長於 N 秒的壓縮檔案進行掃描”核取方塊。
6. 點擊“確定”。
7. 要儲存變更，請點擊“儲存”按鈕。

篩選電子郵件附件

惡意程式會以電子郵件附件的形式傳播。您可以根據郵件附件類型設定篩選，指定類型的檔案可以被自動重新命名或刪除。透過重新命名某種類型的附件，Kaspersky Endpoint Security 可以防護您的電腦，防禦惡意程式的自動執行。

若要設定附件的篩選，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**端點防護**”區域中，選取“**郵件防護**”區域。
在視窗右側將顯示“郵件防護”元件的設定。
3. 在“**安全防護等級**”區域中點擊“**設定**”按鈕。
螢幕上將開啟“**郵件防護**”視窗。
4. 在“**郵件防護**”視窗中，選取“**附件篩選**”頁籤。
5. 請執行以下操作之一：
 - 如果您不希望郵件防護篩選電子郵件附件，請選取“**停用篩選**”選項。
 - 如果您希望郵件防護重新命名**[特定類型](#)**的電子郵件附件，請選取“**重新命名指定的附件類型**”設定。

請注意檔案的實際格式可能不比對其檔案名副檔名。

如果您啟用了篩選郵件附件中的物件，則郵件防護將重新命名或刪除帶有以下副檔名的檔案：

com – 不超過 64 KB 的應用程式的執行檔案

exe – 可執行檔案或自解壓存檔

sys – Microsoft Windows 系統檔案

prg – dBase™、Clipper、Microsoft Visual FoxPro® 或 WAVmaker 程式的程式文字

bin – 二進位檔案

bat – 批次檔案

cmd – Microsoft Windows NT (類似於 DOS 的 bat 檔案)、OS/2 的指令檔案

dpl – 壓縮的 Borland Delphi 庫

dll – 動態連結程式庫

scr – Microsoft Windows 啟動畫面

cpl – Microsoft Windows 控制台模組

ocx – Microsoft OLE (物件連結與嵌入) 物件

tsp – 以分段計時模式執行的程式

drv – 裝置驅動程式

vxd – Microsoft Windows 虛擬裝置驅動程式

pif – 程式資訊檔案

sys – Microsoft Windows 連結檔案

reg – Microsoft Windows 系統登錄機碼檔案

ini – 設定檔，包含 Microsoft Windows、Windows NT 和一些應用程式的設定資料

cla – Java 類

vbs – Visual Basic® 指令碼

vbe – BIOS 影片延伸

js, jse – JavaScript 源文字

htm – 超文字文件

htt – Microsoft Windows 超文字標頭檔

hta – Microsoft Internet Explorer 超文字程式®

asp – 動態伺服器頁面指令碼

chm – 已編譯的 HTML 檔案

pht – 集成 PHP 指令碼的 HTML 檔案

php – 集成到 HTML 檔案中的指令碼

wsh – Microsoft Windows 指令碼主檔案

wsf – Microsoft Windows 指令碼

the – Microsoft Windows 95 桌面牆紙檔案

hlp – Win 說明檔案

eml – Microsoft Outlook Express 電子郵件

nws – 新型 Microsoft Outlook Express 電子郵件

msg – Microsoft Mail 電子郵件

plg – 電子郵件

mbx – 已儲存的 Microsoft Office Outlook 電子郵件的副檔名

doc* – Microsoft Office Word 文件，如：doc 為 Microsoft Office Word 文件，docx 為支援 XML 的 Microsoft Office Word 2007 文件，docm 為支援巨集的 Microsoft Office Word 2007 文件

dot* – Microsoft Office Word 文件範本，如：dot 為 Microsoft Office Word 文件範本，dotx 為 Microsoft Office Word 2007 文件範本，dotm 為支援巨集的 Microsoft Office Word 2007 文件範本

fpm – 資料庫程式、Microsoft Visual FoxPro 開機檔案

rtf – 富文字格式文件

shs – Windows Shell Scrap Object Handler 片段

dwg – AutoCAD® 圖形資料庫

msi – Microsoft Windows 安裝套裝程式

otm – Microsoft Office Outlook 的 VBA 項目

pdf – Adobe Acrobat 文件

swf – Shockwave® Flash 封包物件

jpg, jpeg – 壓縮圖片格式

emf – 增強型圖中繼檔案格式檔案。下一代 Microsoft Windows OS 圖中繼檔案。16位 Microsoft Windows 不支援 EMF 檔案。

ico – 物件圖示檔案

ov? – Microsoft Office Word 可執行檔案

xl* – Microsoft Office Excel 文件和檔案，如：Microsoft Office Excel 延伸 xla 檔案，圖表 xlc，文件範本 xlt，Microsoft Office Excel 2007 工作簿.xlsx，支援巨集的 Microsoft Office Excel 2007 工作簿 xlsm，二進位（非 XML）格式的 Microsoft Office Excel 2007 工作簿 xlsb，Microsoft Office Excel 2007 範本 xltm，支援巨集的 Microsoft Office Excel 2007 範本 xlsm，支援巨集的 Microsoft Office Excel 2007 外掛程式 xlam

pp* – Microsoft Office PowerPoint® 文件和檔案，如：Microsoft Office PowerPoint 幻燈片 pps，幻燈片演示文稿 ppt，Microsoft Office PowerPoint 2007 幻燈片演示文稿 pptx，支援巨集的 Microsoft Office PowerPoint 2007 幻燈片演示文稿 pptm，Microsoft Office PowerPoint 2007 幻燈片演示文稿範本 potx，支援巨集的 Microsoft Office PowerPoint 2007 幻燈片演示文稿範本 potm，Microsoft Office PowerPoint 2007 放映幻燈片 ppsx，支援巨集的 Microsoft Office PowerPoint 2007 放映幻燈片 ppsm，支援巨集的 Microsoft Office PowerPoint 2007 外掛程式 ppam

md* – Microsoft Office Access® 文件和檔案，如：Microsoft Office Access 工作組 mda，資料庫 mdb

sldx – Microsoft PowerPoint 2007 幻燈片

sldm – 支援巨集的 Microsoft PowerPoint 2007 幻燈片

thmx – Microsoft Office 2007 主旨

- 如果您希望郵件防護刪除特定類型的電子郵件附件，請選取“**刪除指定的附件類型**”選項。
6. 如果您在上個步驟中選取了“**重新命名指定的附件類型**”選項或者“**刪除指定的附件類型**”選項，則選取相應類型檔案旁的核取方塊。
- 您可以使用“**新增**”、“**編輯**”和“**刪除**”按鈕來變更檔案類型清單。
7. 點擊“**確定**”。
8. 要儲存變更，請點擊“**儲存**”按鈕。

掃描 Microsoft Office Outlook 中的電子郵件

在 Kaspersky Endpoint Security 安裝期間，郵件防護外掛程式嵌入到 Microsoft Office Outlook（以下簡稱 Outlook）中。您可從 Outlook 內部快速開啟郵件防護設定，指定在何時掃描電子郵件以尋找掃描病毒和其他威脅。Outlook 的郵件防護外掛程式可掃描透過 POP3、SMTP、NNTP、IMAP 和 MAPI 協定傳送或接收的電子郵件。

如果在 Kaspersky Endpoint Security 介面中選定了“**附加：Microsoft Office Outlook 外掛程式**”核取方塊，則可以直接在 Outlook 中配置電子郵件防護設定。

在 Outlook 中，接收的電子郵件首先由郵件防護進行掃描（在 Kaspersky Endpoint Security 介面中選定了“POP3 / SMTP / NNTP / IMAP 流量”核取方塊），然後由嵌入 Outlook 的郵件防護外掛程式進行掃描。如果郵件防護在電子郵件訊息中偵測到惡意物件，會就此事件向您發出警訊。

您在通知視窗中選取的操作決定用於清除郵件中威脅的元件。郵件防護或嵌入到 Outlook 中的郵件防護外掛程式。

- 如果您在通知視窗中選取“**清除**”或“**刪除**”，則由“郵件防護”刪除威脅。
- 如果您在通知視窗中選取“**略過**”，則由 Outlook 的郵件防護外掛程式解毒威脅。

傳送的電子郵件首先由嵌入 Outlook 的電子郵件外掛程式進行掃描，然後由郵件防護進行掃描。

設定在 Outlook 中的郵件掃描

要在 Outlook 2007 中設定郵件掃描：

1. 開啟 Outlook 2007 的主視窗。
2. 從功能表列中選取“**服務** → **設定**”。
開啟“**選項**”視窗。
3. 在“**選項**”視窗中選取“**電子郵件防護**”頁籤。

要在 Outlook 2010/2013 中設定郵件掃描：

1. 開啟 Outlook 程式主視窗。
選取左上角的“**檔案**”頁籤。
2. 點擊“**選項**”按鈕。
開啟“**Outlook 選項**”視窗。
3. 選取“**外掛程式**”區域。
嵌入到 Outlook 的外掛程式設定將顯示在視窗右側。
4. 點擊“**外掛程式選項**”按鈕。

使用卡巴斯基安全管理中心設定郵件掃描

如果使用 Outlook 的郵件防護延伸外掛程式，則建議使用緩衝區的交換模式。有關交換緩存模式和使用建議資訊，請參閱 Microsoft 知識庫：<https://technet.microsoft.com/zh-cn/library/cc179175.aspx>。

若要使用卡巴斯基安全管理中心設定 Outlook 的郵件防護延伸外掛程式：

1. 開啟卡巴斯基安全管理中心的管理主控台。

2. 在管理主控台樹狀目錄中，「**受管裝置**」資料夾下，開啟您希望為其設定郵件掃描的相關管理群組名稱所對應的資料夾。
3. 在工作區選擇**「政策」**頁籤。
4. 選擇所需政策。
5. 使用以下方式開啟**「內容: <政策名稱>」**視窗：
 - 在所選定項目右鍵選單中，選擇**「內容」**。
 - 點擊位於管理主控台工作區右側的**「設定政策」**連線。
6. 在**「端點防護」**區域中，選取**「郵件防護」**子區域。
7. 在**「安全防護等級」**區域中點擊**「設定」**按鈕。
螢幕上將開啟**「郵件防護」**視窗。
8. 在**「連線」**區域中，點擊**「設定」**按鈕。
系統將開啟**「郵件防護」**視窗。
9. 在**「郵件防護」**視窗中：
 - 如果您希望 Outlook 的郵件防護延伸外掛程式掃描郵件到達時進行掃描，選取**「接收時掃描」**核取方塊。
 - 如果您希望 Outlook 的郵件防護延伸外掛程式在使用者開啟郵件時掃描內進郵件，選取**「閱讀時掃描」**核取方塊。
 - 如果您希望 Outlook 的郵件防護延伸外掛程式在傳送郵件時掃描外出郵件，選取**「傳送時掃描」**核取方塊。
10. 在**「電子郵件防護」**的視窗上，點擊**「確定」**。
11. 在**「郵件防護」**視窗中點擊**「確認」**。
12. 套用政策。
有關實施卡巴斯基安全管理中心政策的詳細資訊，請查閱《*卡巴斯基安全管理中心管理手冊*》。

電腦的網際網路防護網頁防護

如果將 Kaspersky Endpoint Security 安裝在執行 Microsoft Windows for workstations 的電腦上，則可使用此元件。如果將 Kaspersky Endpoint Security 安裝在執行 [Microsoft Windows 以做檔案伺服器之用](#) 的電腦上，則此元件無法使用。

本章節介紹網頁防護資訊，以及如何設定元件。

關於網頁防護

每次您上網時，儲存在您的電腦上的資訊將會曝露給病毒和其他惡意程式。當您下載免費軟體或瀏覽受駭客攻擊的網站時，它們可以侵入您的電腦。當您的電腦建立網際網路連線，甚至在開啟網頁或下載檔案之前，網路蠕蟲就可以找到攻擊的方法。

網頁防護可以防護透過 HTTP 和 FTP 協定傳入和傳出電腦的資料，並根據可疑或釣魚網頁位址清單檢查網址。

網頁防護偵測並分析使用者或應用程式透過 HTTP 或 FTP 協定存取的每個網頁或檔案的病毒和其他惡意程式。將會以下使用情況：

- 如果發現網頁或檔案不包含惡意程式碼，使用者可以立即存取它們。
- 如果使用者存取包含惡意程式碼的網頁或檔案，應用程式將執行網頁防護設定中指定的操作。

啟用和停用網頁防護



預設情況下，網頁防護功能已啟用並且以 Kaspersky Lab 專家建議的模式運行。您可以在必要時停用網頁防護。

有兩種啟動或停用該元件的方式：



- 透過 [應用程式主視窗](#) 的“防護和控制”頁籤。
- 開啟 [程式設定視窗](#)。

要啟用或停用網頁防護，請在程式主視窗的“防護和控制”頁籤中執行以下操作：

1. 開啟“程式主視窗”。
2. 選擇“防護和控制”頁籤。
3. 點擊“防護”區域。
開啟“防護”區域。
4. 右鍵點擊“網頁防護”元件，開啟有資訊說明的右鍵選單。
系統將開啟一個用於選擇對該元件的操作功能表。
5. 請執行以下操作之一：
 - 要啟用“網頁防護”，請在功能表中選取“開始”。

“網頁防護”左側顯示的元件狀態圖示  將變為圖示 。

- 要停用“網頁防護”，請在功能表中選取“**停止**”。

“網頁防護”左側顯示的元件狀態圖示  將變為圖示 。

若要從應用程式設定視窗中啟用或停用網頁防護，請執行以下操作：

1. 開啟程式設定視窗。
2. 在視窗左側的“端點防護”區域中，選取“**網頁防護**”區域。
在視窗右側，將顯示網頁防護元件的設定。
3. 請執行以下操作之一：
 - 如果要啟用網頁防護，請選取“**啟用網頁防護**”核取方塊。
 - 如果要停用網頁防護，請清空“**啟用網頁防護**”核取方塊。
4. 要儲存變更，請點擊“**儲存**”按鈕。

設定網頁防護

您可以按照以下步驟設定網頁防護：

- 變更網頁流量安全等級。
您可以為透過 HTTP 和 FTP 協定接收或傳送的網頁流量選取一個預先設定的安全等級，或者也可以設定一個自訂網頁流量安全等級。
如果您對網頁流量安全等級進行了變更，以後隨時可以還原至建議的網頁流量安全等級設定。
- 變更 Kaspersky Endpoint Security 針對受病毒感染的網頁流量物件所採取的處理措施。
如果對某 HTTP 物件的分析顯示其包含惡意程式碼，網頁防護將根據您指定的處理措施採取操作。
- 根據釣魚網站和可疑網址資料庫設定網頁防護對網址的掃描。
- 設定在掃描網頁流量中的病毒和其他惡意程式時使用啟發式分析。
您可以使用啟發式分析提高防護效率。在啟發式分析中，Kaspersky Endpoint Security 將分析應用程式在作業系統中的活動。啟發式分析可以偵測 Kaspersky Endpoint Security 資料庫中尚無記錄的安全威脅。
- 設定在掃描網頁中的釣魚連結時使用啟發式分析。
- 最佳化網頁防護掃描透過 HTTP 和 FTP 協定傳送和接收的網頁流量。
- 建立信任網址的清單。
您可以為您信任其內容的網址建立一個清單。網頁防護不會對來自受信任網址的資訊進行病毒或其他威脅分析。在一些情況下本選項十分有用，例如，當網頁防護干擾您從一個已知網站上下載檔案時。

網址可以是某特定網頁的位址，也可以是某網站的位址。

變更網頁流量安全等級

要防護經由 HTTP 和 FTP 協定傳輸和接收的資料，網頁防護可套用多種設定群組。這些設定組被稱為網頁流量安全防護等級。有三種預先安裝的網頁流量安全防護等級：**高**、**建議**和**低**。**建議防護**網頁流量安全防護等級可視為最佳設定，是 Kaspersky 建議採用的等級。

要變更網頁流量安全防護等級：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**端點防護**”區域中，選取“**網頁防護**”區域。
在視窗右側，將顯示網頁防護元件的設定。
3. 在“**安全防護等級**”區域中執行下列操作：
 - 如果您希望安裝一種預設的網頁流量安全防護等級（**高**、**建議**或**低**），請使用捲軸選取一個等級。
 - 如果您希望設定一種自訂網頁流量安全防護等級，請在“**網頁防護**”視窗中點擊“**設定**”按鈕並指定設定。
您設定自訂網頁流量安全防護等級之後，“**安全防護等級**”區域中網頁流量安全防護等級的名稱將變更為“**自訂**”。
 - 如果您希望將網頁流量安全防護等級變更為“**建議**”，請點擊“**預設**”按鈕。
4. 要儲存變更，請點擊“**儲存**”按鈕。

變更對惡意網路流量物件採取的操作

若要變更對惡意網路流量物件採取的操作，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**端點防護**”區域中，選取“**網頁防護**”區域。
在視窗右側，將顯示網頁防護元件的設定。
3. 在“**偵測到威脅後的動作**”區域，選取 Kaspersky Endpoint Security 對惡意網頁流量物件所採取的操作：
 - **自動選擇動作**。
 - **封鎖下載**。
 - **允許下載**。
4. 要儲存變更，請點擊“**儲存**”按鈕。

根據可疑及釣魚網站資料庫掃描網址

掃描連結以檢視其是否包含在釣魚網址清單中，以避免網路釣魚攻擊。釣魚攻擊常常帶有偽裝，比如從您銀行發來的帶有銀行官方網站連結的電子郵件訊息。點擊此連結，您將進入銀行網站的完整複製網站，甚至可以在瀏覽器位址欄看到其真實位址，即使您在假網站上。從此刻起，您在網站上的所有操作都將被追蹤，進而用來竊取您的金錢。

由於連線釣魚網站的連結不僅能透過電子郵件訊息傳送，而且還可能來自其他來源，（比如 ICQ 訊息），網頁防護功能將在網頁流量等級監視您存取釣魚網站的操作並封鎖您存取此類網站。Kaspersky Endpoint Security 安裝套件中包含釣魚網址清單。

若要根據可疑和釣魚網址資料庫設定網頁防護以掃描網址，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點防護”區域中，選取“網頁防護”區域。
在視窗右側，將顯示網頁防護元件的設定。
3. 點擊“設定”按鈕。
開啟“網頁防護”視窗。
4. 在“網頁防護”視窗中，選取“一般”頁籤。
5. 請執行以下操作：
 - 如果您希望網頁防護根據惡意網址資料庫檢查網址，請在“掃描方法”區域中選取“檢查連結是否在惡意連結資料庫中列出”核取方塊。
 - 如果您希望網頁防護根據釣魚網址資料庫檢查網址，請在“網路釣魚防護設定”區域中選取“檢查連結是否在惡意連結資料庫中列出”核取方塊。

您也可以根據[卡巴斯基安全網路](#)信譽資料庫檢查連結。

6. 點擊“確定”。
7. 要儲存變更，請點擊“儲存”按鈕。

搭配啟發式分析使用網頁防護

若要設定啟發式分析的使用，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點防護”區域中，選取“網頁防護”區域。
在視窗右側，將顯示網頁防護元件的設定。
3. 在“安全防護等級”區域中點擊“設定”按鈕。
開啟“網頁防護”視窗。
4. 選取“一般”標籤。
5. 如果您希望網頁防護使用啟發式分析掃描網頁流量中的病毒和其他惡意程式，在“掃描方式”中，請選取“使用啟發式分析偵測病毒”選框並使用捲軸設定啟發式分析的具體等級：輕度掃描、中度掃描或深度掃描。

6. 如果您希望網頁防護使用啟發式分析掃描網頁尋找釣魚連結，則在“**網路釣魚防護設定**”區域中選取“**偵測釣魚連結的啟發式分析**”核取方塊。
7. 點擊“**確定**”。
8. 要儲存變更，請點擊“**儲存**”按鈕。

編輯受信任網址清單

若要建立受信任網頁位址的清單：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**端點防護**”區域中，選取“**網頁防護**”區域。
在視窗右側，將顯示網頁防護元件的設定。
3. 點擊“**設定**”按鈕。
開啟“**網頁防護**”視窗。
4. 選取“**信任網址**”頁籤。
5. 選取“**不掃描受信任網址的 Web 流量**”核取方塊。
6. 為您信任其內容的網頁或網址建立清單。若要建立清單：
 - a. 點擊“**新增**”按鈕。
開啟“**網址/網址遮罩**”視窗。
 - b. 輸入網站/網頁位址或位址遮罩。
 - c. 點擊“**確定**”。
一條新記錄將出現在信任網址的清單中。
7. 點擊“**確定**”。
8. 要儲存變更，請點擊“**儲存**”按鈕。

防護即時通訊用戶端流量。即時通訊防護

如果將 Kaspersky Endpoint Security 安裝在執行 Microsoft Windows for workstations 的電腦上，則可使用此元件。如果將 Kaspersky Endpoint Security 安裝在執行 [Microsoft Windows 以做檔案伺服器之用](#) 的電腦上，則此元件無法使用。

本章節介紹即時通訊防護資訊，以及如何設定元件。

關於即時通訊防護

即時通訊防護將掃描即時通訊用戶端（也稱 *即時通訊用戶端*）的流量。

即時通訊防護不會掃描透過加密通道傳輸的郵件。

透過即時通訊用戶端傳送的訊息可能含有以下安全威脅：

- 企圖將惡意程式下載至電腦的網址
- 入侵者用於釣魚攻擊的惡意程式和網站的網址
釣魚攻擊的目的是竊取使用者個人資訊，例如銀行號碼、護照資訊、銀行支付系統及其線上服務（例如社群網站或電子郵件帳戶）密碼的釣魚攻擊。

可以透過即時通訊用戶端傳送的檔案。嘗試儲存此類檔案時，檔案將由 [檔案防護](#) 元件進行掃描。

即時通訊防護可攔截使用者透過即時通訊用戶端傳送或接收的所有訊息並掃描其中會對電腦安全產生威脅的網址。

- 如果訊息中沒有危險網址，該郵件將傳送給使用者。
- 如果訊息中偵測到危險連結，即時通訊防護會在活動的即時通訊用戶端的訊息視窗中將該訊息替換成關於該威脅的通知。

啟用和停用即時通訊防護





即時通訊防護已預設啟用並採用 Kaspersky Lab 專家建議的模式執行。您可以在必要時停用即時通訊防護。

有兩種啟動或停用該元件的方式：

- 透過 [應用程式主視窗](#) 的“防護和控制”頁籤。
- 開啟 [程式設定視窗](#)。

要啟用或停用即時通訊防護，請在程式主視窗的防護和控制頁籤中執行以下操作：

1. 開啟“程式主視窗”。

2. 選擇“**防護和控制**”頁籤。
3. 點擊“**防護**”區域。
開啟“**防護**”區域。
4. 右鍵點擊“**即時通訊防護**”以開啟元件操作的右鍵選單。
5. 請執行以下操作之一：
 - 要啟用即時通訊防護，請在功能表中選取“**開始**”。
顯示在“**即時通訊防護**”左側顯示的元件狀態圖示  將變為圖示 。
 - 要停用即時通訊防護，請在功能表中選取“**停止**”。
顯示在“**即時通訊防護**”左側顯示的元件狀態圖示  將變為圖示 。

透過程式設定視窗啟用或停用即時通訊防護：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**端點防護**”區域中，選取“**即時通訊防護**”子區域。
即時通訊防護元件將顯示在視窗右邊。
3. 請執行以下操作之一：
 - 如果要啟用即時通訊防護，請選取“**啟用即時通訊防護**”核取方塊。
 - 如果您想停用即時通訊防護，請清除“**啟用即時通訊防護**”核取方塊。
4. 要儲存變更，請點擊“**儲存**”按鈕。

配置即時通訊防護

您可以執行下列操作來設定即時通訊防護：

- 設定防護範圍。
您可以透過指定掃描的即時通訊用戶端訊息類型來擴大或縮小防護範圍。
- 根據可疑網址和釣魚網站資料庫設定即時通訊防護以掃描即時通訊用戶端訊息中的連結。

建立即時通訊防護的防護範圍

防護範圍是指元件啟用時的掃描物件。不同元件的防護範圍有不同的參數。對傳送或接收的即時通訊用戶端訊息進行掃描屬於即時通訊防護的防護範圍。即時通訊防護預設既掃描傳送的訊息又掃描接收的訊息。您可以停用掃描傳送的流量。

要建立防護範圍，請執行以下操作：

1. 開啟[程式設定視窗](#)。

2. 在視窗左側的“端點防護”區域中，選取“即時通訊防護”子區域。
即時通訊防護元件將顯示在視窗右邊。
3. 在“防護範圍”區域中執行以下操作：
 - 如果您希望即時通訊防護掃描所有傳送和接收的即時通訊用戶端訊息，請選取“傳送和接收的訊息”選項。
 - 如果希望“即時通訊防護”只掃描即時通訊用戶端接收的電子郵件，請選取“僅接收的郵件”選項。
4. 要儲存變更，請點擊“儲存”按鈕。

使用即時通訊防護根據惡意和釣魚網址資料庫掃描網址

若要根據可疑和釣魚網址資料庫設定即時通訊防護以掃描網址，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點防護”區域中，選取“即時通訊防護”子區域。
即時通訊防護元件將顯示在視窗右邊。
3. 在“掃描方式”區域中選取您希望即時通訊防護使用的掃描方式：
 - 如果您希望根據可疑網址資料庫檢查即時通訊用戶端訊息中的網址，請選取“檢查網站是否位於可疑網址資料庫”核取方塊。
 - 如果您希望根據釣魚網址資料庫檢查即時通訊用戶端訊息中的網址，請選取“檢查連結是否位於釣魚連結資料庫”核取方塊。
4. 要儲存變更，請點擊“儲存”按鈕。

系統監控

如果將 Kaspersky Endpoint Security 安裝在執行 Microsoft Windows for workstations 的電腦上，則可使用此元件。如果將 Kaspersky Endpoint Security 安裝在執行 [Microsoft Windows 以做檔案伺服器之用](#) 的電腦上，則此元件無法使用。

本章節介紹系統監控的相關資訊並說明如何配置該元件的設定。

關於系統監控

系統監控將收集您的電腦上應用程式操作的資料，將這類資訊傳送給其他元件，以實現更可靠的防護。

危險活動行為特徵碼

危險活動行為特徵碼(BSS) 包含 Kaspersky Endpoint Security 將其分類為危險操作的一系列應用程式操作。如果應用程式操作符合危險活動行為特徵碼，Kaspersky Endpoint Security 將執行指定操作。根據危險活動行為特徵碼的 Kaspersky Endpoint Security 功能為電腦提供主動防禦。

預設情況下，如果應用程式活動比對行為流特徵碼，系統監控會將該應用程式的可執行檔案移動至 [隔離](#)。

回溯惡意程式執行的操作

根據系統監控收集的資訊，Kaspersky Endpoint Security 在執行解毒期間可 [回溯惡意程式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 將對以下類型的惡意軟體活動採取操作：

- 檔案活動。
Kaspersky Endpoint Security 將刪除由惡意程式建立的位於任何媒介（除了網路媒介）上的可執行檔案。
Kaspersky Endpoint Security 將刪除惡意程式入侵的某個程式建立的可執行檔案。
Kaspersky Endpoint Security 不會還原已變更或刪除的檔案。
- 登錄檔活動。
Kaspersky Endpoint Security 將刪除惡意軟體建立的分區和登錄機碼。
Kaspersky Endpoint Security 不會還原被修改或刪除的分區和登錄機碼。
- 系統活動。
Kaspersky Endpoint Security 將終止惡意程式發起的處理程序。
Kaspersky Endpoint Security 將終止惡意程式入侵的處理程序。
Kaspersky Endpoint Security 不會還原由惡意程式掛起的處理程序。
- 網路活動。
Kaspersky Endpoint Security 將封鎖惡意程式的網路活動。
Kaspersky Endpoint Security 將封鎖惡意程式入侵的處理程序的網路活動。

[檔案防護](#)可以在[病毒掃描](#)期間發起惡意操作回溯。

回溯惡意程式操作的過程將會影響一組嚴格限定的資料。回溯對於作業系統或您的電腦中資料的完整性不會產生負面影響。

啟用和停用系統監控





預設情況下，系統監控已啟用並在 Kaspersky Lab 建議的模式下執行。您可以在必要時停用“系統監控”。

除非絕對必要，否則不建議停用系統監控，因為這會影響防護元件的效能。防護元件可能會請求由系統監控所收集的資料，以更加準確地確認所發現的威脅。

有兩種方式可啟用或停用系統監控：

- 透過[應用程式主視窗](#)的“**防護和控制**”頁籤。
- 開啟[程式設定視窗](#)。

要啟用或停用系統監控，請在主應用程式視窗的“**防護和控制**”頁籤中執行以下操作：

1. 開啟“程式主視窗”。
2. 選擇“**防護和控制**”頁籤。
3. 點擊“**防護**”區域。
開啟“**防護**”區域。
4. 右鍵點擊以顯示包含“系統監控”元件資訊說明的右鍵選單。
系統將開啟一個用於選擇對該元件的操作功能表。
5. 請執行以下操作之一：
 - 要啟用系統監控，請選取“**開始**”。
“**系統監控**”左側顯示的元件狀態圖示  將變為圖示 。
 - 要停用系統監控，請選取“**停止**”。
“**系統監控**”左側顯示的元件狀態圖示  將變為圖示 。

若要從應用程式設定視窗中啟用或停用“系統監控”，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**端點防護**”區域中選取“**系統監控**”。
在視窗右側，將會顯示“**系統監控**”元件的設定。
3. 請執行以下操作之一：
 - 要啟用系統監控，請選取“**啟用系統監控**”核取方塊

- 要停用系統監控，請清空“**停用系統監控**”核取方塊。
4. 要儲存變更，請點擊“**儲存**”按鈕。

設定系統監控

您可以執行下列操作來設定系統監控：

- 啟用或停用攻擊防護；
- 選擇程式中偵測到惡意活動時的動作；
- 啟用或停用解毒期間回溯惡意操作。

啟用或停用弱點防護

要啟用或停用弱點防護：

1. 開啟 [程式設定視窗](#)。
2. 在視窗左側的“**端點防護**”區域中選取“**系統監控**”。
在視窗右側，將會顯示“**系統監控**”元件的設定。
3. 請執行以下操作之一：
 - 如果您想要讓 Kaspersky Endpoint Security 監控由弱點程式使用的檔案，請選擇 **啟用弱點防護** 核取方塊。
如果 Kaspersky Endpoint Security 偵測到被弱點程式使用的檔案被意外開啟，則它將按照您在 **偵測到威脅後的動作** 彈出清單的選擇操作。
 - 如果您想要讓 Kaspersky Endpoint Security 監控由弱點程式使用的檔案，請選擇 **啟用弱點防護** 核取方塊。
4. 要儲存變更，請點擊“**儲存**”按鈕。

選擇程式中偵測到惡意活動時的動作

為了選擇程式進行惡意活動時的動作，請執行以下步驟：

1. 開啟 [程式設定視窗](#)。
2. 在視窗左側的“**端點防護**”區域中選取“**系統監控**”。
在視窗右側，將會顯示“**系統監控**”元件的設定。
3. 在 **關於偵測惡意活動** 彈出清單的 **偵測到威脅時的動作** 區域中，選擇以下操作：
 - **自動選擇動作**。
 - **移動檔案到隔離區**。

- 終止惡意程式。
- 略過。

4. 要儲存變更，請點擊“儲存”按鈕。

啟動或停用解毒期間回溯惡意操作

若要啟用或停用解毒期間回溯惡意操作，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點防護”區域中選取“系統監控”。
- 在視窗右側，將會顯示“系統監控”元件的設定。
3. 請執行以下操作之一：
 - 如果您希望 Kaspersky Endpoint Security 在執行解毒期間回溯惡意程式在作業系統中執行的操作，請選取“在解毒過程中回溯惡意軟體所做過的動作”核取方塊。
 - 如果您希望 Kaspersky Endpoint Security 在執行解毒期間略過惡意軟體在作業系統中執行的操作，請清空“在解毒過程中回溯惡意軟體所做過的動作”核取方塊。
4. 要儲存變更，請點擊“儲存”按鈕。

防火牆

本章節介紹防火牆的詳細資訊，以及如何設定元件。

關於防火牆

使用區域網路和網際網路的過程中，電腦曝露於病毒、其他惡意程式、以及一系列針對作業系統和軟體弱點的攻擊環境中。

當電腦連接到網際網路或區域網路時，防火牆可防護儲存於使用者電腦上的個人資料，並封鎖最可能針對作業系統的威脅。防火牆可偵測使用者電腦的所有網路連線、提供 IP 位址清單，並指示預設網路連線的狀態。

防火牆元件將根據[網路規則](#)篩選所有網路活動。設定網路規則允許您指定想要的電腦防護等級，例如從封鎖所有應用程式的網際網路存取到允許無限制存取權限。





啟用或停用防火牆

預設情況下，防火牆為啟動狀態，各種功能均設定為最佳化。如有需要，您可以停用防火牆。

有兩種啟動或停用該元件的方式：

- 透過[應用程式主視窗](#)的“**防護和控制**”頁籤。
- 開啟[程式設定視窗](#)。

要啟用或停用防火牆，請在應用程式主視窗的“**防護和控制**”頁籤中執行以下操作：

1. 開啟“程式主視窗”。
2. 選擇“**防護和控制**”頁籤。
3. 點擊“**防護**”區域。
開啟“**防護**”區域。
4. 右鍵點擊“**防火牆**”以開啟元件操作的右鍵選單。
5. 請執行以下操作之一：
 - 要啟用防火牆，在右鍵選單中選取“**開始**”。
顯示在“**防火牆**”行左側的元件狀態圖示  將變為圖示 。
 - 要停用防火牆，請在右鍵選單中選取“**停止**”。
顯示在“**防火牆**”行左側的元件狀態圖示  將變為圖示 。

若要從應用程式設定視窗中啟用或停用防火牆，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**端點防護**”區域中，選取“**防火牆**”。
在視窗右側，將顯示防火牆元件的設定。

3. 請執行以下操作之一：

- 要啟用防火牆，請選取“**啟用防火牆**”核取方塊。
- 要停用防火牆，請選取“**停用防火牆**”核取方塊。

4. 要儲存變更，請點擊“**儲存**”按鈕。

關於網路規則

*網路規則*是指防火牆在偵測網路連線嘗試時採取的允許或封鎖操作。

防火牆針對不同類型的網路攻擊提供兩種等級的防護：網路等級和程式等級。套用網路封包規則即提供網路等級的防護。套用應用程式可以存取網路資源的規則即提供程式等級的防護。

根據這兩種防火牆防護等級，您可以建立：

- *網路封包規則*。網路封包規則將對網路封包進行限制，與程式無關。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。預設情況下，防火牆已指定某些網路封包規則。
- *應用程式網路規則*。應用程式網路規則將對特定應用程式的網路活動進行限制。它們不僅將網路封包的特徵列入重要參考因素，還把接收或傳送此網路封包的應用程式列入重要參考因素中。這些規則讓您可以微調網路活動篩選設定：例如，封鎖某些應用程式進行某些網路連線，而不封鎖其他應用程式則進行這些網路連線。

網路封包規則的優先順序比應用程式網路規則高。如果網路封包規則和應用程式網路規則指定了同一類別的網路活動，則該網路活動將根據網路封包規則進行處理。

您可以為每種網路封包規則和應用程式網路規則指定執行優先順序。

網路封包規則的優先順序比應用程式網路規則高。如果網路封包規則和應用程式網路規則指定了同一類別的網路活動，則該網路活動將根據網路封包規則進行處理。

應用程式網路規則的運作方式如下：應用程式網路規則包括基於網路狀態（*公用*、*本機*或*受信任*）的存取規則。例如，預設情況下，“高限制群組”信任群組中的應用程式在所有狀態的網路中均不允許進行任何網路活動。如果為單個應用程式（父應用程式）指定了網路規則，則其他應用程式的子處理程序將依據父應用程式的網路規則執行。如果應用程式沒有網路規則，則子程序將根據應用程式信任組的網路存取規則執行。

例如，對於瀏覽器 X 以外的所有應用程式，您已禁止所有狀態的網路中的任何網路活動。如果從瀏覽器 X（父應用程式）開始安裝瀏覽器 Y（子處理程序），則瀏覽器 Y 安裝程式將存取網路並下載必要的檔案。安裝後，根據防火牆設定，瀏覽器 Y 將被拒絕執行任何網路連線。要禁止作為子處理程序的瀏覽器 Y 安裝程式的網路活動，必須為瀏覽器 Y 的安裝程式新增網路規則。

關於網路連線狀態

防火牆控制使用者電腦上的所有網路連線，並且自動為監測到的每個網路連線分配一個狀態。

網路連線可具有下列狀態類型：

- **公用網路**。公共網路 該狀態用於不受任何防毒應用程式、防火牆或篩選器防護的網路（例如網咖網路）。當使用者操作連接到此類網路的電腦時，防火牆可封鎖對此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存取資料，以及遠端存取該電腦的桌面。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。

防火牆預設為網際網路分配公用網路狀態。您無法變更網際網路的狀態。

- **區域網路**。區域網路 該狀態將分配給使用者可存取電腦的檔案和印表機的網路 (例如，區域或家用網路) 。
- **信任網路**。信任網路 該狀態將分配給電腦不會曝露於攻擊或未經授權的資料存取嘗試的安全網路。防火牆允許在具有此狀態的網路中進行任何網路活動。

變更網路連線狀態

若要變更網路連線狀態，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點防護”區域中，選取“防火牆”子區域。
在視窗右側，將顯示防火牆元件的設定。
3. 點擊“可用網路”按鈕。
將開啟“防火牆”視窗。
4. 選取您想要變更其狀態的網路連線。
5. 在右鍵選單中選取[網路連線狀態](#)：
 - 公用網路。
 - 區域網路。
 - 信任網路。
6. 在“防火牆”視窗中點擊“確認”。
7. 要儲存變更，請點擊“儲存”按鈕。

管理網路封包規則

您在管理網路封包規則時可執行以下操作：

- 建立新的網路封包規則。
您可以透過建立一個可應用於網路封包和資料流程的條件集和操作集來建立新的網路封包規則。
- 啟用或停用網路封包規則。
預設情況下，由防火牆建立的所有網路封包規則處於“*開*”狀態。當啟用網路封包規則時，防火牆應用此規則。您可以停用網路封包規則清單中選取的任何網路封包規則。當停用網路封包規則時，防火牆將暫時不套用此規則。


預設情況下，新增到網路封包規則清單中的自訂網路封包規則處於“*開*”狀態。

- 編輯現有網路封包規則的設定。
當您建立新的網路封包規則之後，您始終可以重新編輯其設定並根據需要進行修改。
- 變更網路封包規則的防火牆操作。
在網路封包規則清單中，您可以編輯防火牆在偵測到與特定網路封包規則相符的網路活動時的操作。
- 變更網路封包規則的優先順序。
您可以提高或降低清單中選取的網路封包規則的優先順序。
- 刪除網路封包規則。
您可以刪除網路封包規則以停止防火牆將此規則應用於偵測網路活動，並停止將此規則顯示在“**關**”狀態的網路封包規則清單中。

建立和編輯網路封包規則

在建立網路封包規則時，請記得，它們的優先順序比應用程式網路規則高。

若要建立和編輯網路封包規則，請執行以下操作：

1. 開啟[程式設定視窗](#)。
 2. 在視窗左側的“**端點防護**”區域中，選取“**防火牆**”。
 3. 點擊“**網路封包規則**”按鈕。
 4. “**防火牆**”視窗將開啟“**網路封包規則**”頁籤。
此頁籤將顯示防火牆設定的預設網路封包規則清單。
 5. 請執行以下操作之一：
 - 要建立一個新的網路封包規則，請點擊“**新增**”按鈕。
 - 要編輯一個網路封包規則，請在清單中選取此規則，並點擊“**編輯**”按鈕。
- 開啟“**網路規則**”視窗。
6. 在“**動作**”下拉清單中選取防火牆在偵測到此類網路活動後的操作：
 - **允許**
 - **封鎖**
 - **根據應用程式規則**。
 7. 在“**名稱**”欄位中透過以下方式填寫此[網路服務](#)的名稱：
 - 點擊位於“**名稱**”欄位右側的  圖示，然後從下拉清單中選取網路服務的名稱。
此下拉清單中含有定義最常用的網路連線的網路服務。

- 在“**名稱**”欄位中手動輸入網路服務名稱。
8. 指定資料傳輸協定：
- a. 勾選“**協定**”方塊。
 - b. 在下拉清單中選取監控網路活動的協定種類。
防火牆將監控使用 TCP、UDP、ICMP、ICMPv6、IGMP 和 GRE 協定的網路連線。
如果您從“**名稱**”下拉清單中選取網路服務，那麼“**協定**”核取方塊將自動勾選，並且在核取方塊旁邊的下拉清單中自動填寫與所選網路服務相對應的協定類型。預設情況下將會選取“**協定**”方塊。
9. 在“**方向**”下拉清單中選取受監控的網路活動方向。
防火牆將對以下方向的網路連線進行監控：
- **接收 (封包)**。
 - **接收**。
 - **接收/傳送**
 - **傳送 (封包)**。
 - **傳送**。
10. 如果選取的是 ICMP 或 ICMPv6 埠，您可以指定 ICMP 封包類型和代碼：
- a. 勾選“**ICMP 類型**”方塊並在下拉清單中選取 ICMP 封包類型。
 - b. 勾選“**ICMP 代碼**”方塊並在下拉清單中選取 ICMP 封包代碼。
11. 如果選取的是 TCP 或 UDP 協定類型，您可以指定其連線受監控的本機和遠端電腦逗號分隔的連接埠：
- a. 在“**遠端連接埠**”欄位中輸入遠端連接埠。
 - b. 在“**本機連接埠**”欄位中輸入本機連接埠。
12. 在“**網路介面卡**”表中，指定傳送或接收網路封包的網路介面卡設定。若要執行操作，請使用“**新增**”、“**編輯**”和“**刪除**”按鈕。
13. 如果您希望限制控制基於網路封包存活時間 (TTL)，則選取 **TTL** 核取方塊並在旁邊的欄位中指定進出網路封包的時間範圍值。
網路規則將控制其時間不會超過指定值的網路封包的傳輸。
否則，清空 **TTL** 核取方塊。
14. 指定傳送和/或接收網路封包的遠端電腦的網路位址。若要執行操作，請選取“**遠端位址**”下拉清單中的任一以下值：
- **任何位址**。網路規則將控制任意 IP 位址的遠端電腦接收和/或傳送的網路封包。
 - **子網路位址**。網路規則將控制擁有與選定網路類型相關的 IP 位址的電腦傳送和/或接收的網路封包：**信任網路**、**區域網路**或**公用網路**。
 - **來自群組位址**。網路規則將控制擁有可使用“**新增**”、“**編輯**”和“**刪除**”按鈕指定的清單中 IP 位址的遠端電腦傳送和/或接收的網路封包。

15. 指定安裝了 Kaspersky Endpoint Security 的可以傳送和/或接收網路封包的電腦的網路位址。若要執行操作，請選取“**本機位址**”下拉清單中的任一以下值：

- **任何位址**。網路規則將控制任意 IP 位址的安裝了 Kaspersky Endpoint Security 的遠端電腦接收和/或傳送的網路封包。
- **來自群組位址**。網路規則將控制擁有可使用“**新增**”、“**編輯**”和“**刪除**”按鈕指定的清單中 IP 位址的已安裝 Kaspersky Endpoint Security 的遠端電腦傳送和/或接收的網路封包。

有時候無法獲得使用網路封包的應用程式的本機位址。如果出現這種情況，則“**本機位址**”設定值將被略過。

16. 如果您希望將網路規則的操作反映在**報告**中，請選取“**記錄事件**”核取方塊。

17. 在“**網路規則**”視窗中點擊“**確定**”。

如果建立新的網路規則，此規則將顯示在“**防火牆**”視窗中的“**網路封包規則**”頁籤中。新規則預設位於網路封包規則清單的最末端。

18. 在“**防火牆**”視窗中點擊“**確認**”。

19. 要儲存變更，請點擊“**儲存**”按鈕。

啟動或停用網路封包規則

若要啟用或停用網路封包規則，請執行以下操作：

1. 開啟**程式設定視窗**。
2. 在視窗左側的“**端點防護**”區域中，選取“**防火牆**”子區域。
在視窗右側，將顯示防火牆元件的設定。
3. 點擊“**網路封包規則**”按鈕。
“**防火牆**”視窗將開啟“**網路封包規則**”頁籤。
4. 在清單中選取所需的網路封包規則。
5. 請執行以下操作之一：
 - 要啟用網路封包規則，請選取此規則名稱旁邊的核取方塊。
 - 要停用網路封包規則，請清空此規則名稱旁邊的核取方塊。
6. 點擊“**確定**”。
7. 要儲存變更，請點擊“**儲存**”按鈕。

更改網路封包規則的防火牆操作

若要變更應用於網路封包規則的防火牆操作，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點防護”區域中，選取“防火牆”子區域。
在視窗右側，將顯示防火牆元件的設定。
3. 點擊“網路封包規則”按鈕。
“防火牆”視窗將開啟“網路封包規則”頁籤。
4. 在清單中選取您希望變更其操作的網路封包規則。
5. 在“權限”列中，點擊右鍵顯示右鍵選單，然後選擇您要分配的操作：
 - 允許
 - 封鎖
 - 根據應用程式規則
 - 記錄事件
6. 在“防火牆”視窗中點擊“確認”。
7. 要儲存變更，請點擊“儲存”按鈕。

更改網路封包規則的優先順序

網路封包規則的優先順序取決於其在網路包規則清單中的位置。封包規則清單中位於最上方的優先等級最高。

每個手動建立的網路封包規則都將被新增到封包規則清單尾部，擁有最低的優先等級。

防火牆將按照網路封包規則清單中規則的顯示順序自上而下執行規則。根據套用於特定網路連線的每個已處理網路封包規則，防火牆會允許或封鎖對該網路連線設定中指定的位址和通訊埠的網路存取。

若要變更網路封包規則優先順序，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點防護”區域中，選取“防火牆”子區域。
在視窗右側，將顯示防火牆元件的設定。
3. 點擊“網路封包規則”按鈕。
“防火牆”視窗將開啟“網路封包規則”頁籤。
4. 在清單中選取您希望變更其優先順序的網路封包規則。
5. 使用**上移**和**下移**按鈕將該規則移動到網路封包規則清單中您想要的位置：
6. 點擊“確定”。
7. 要儲存變更，請點擊“儲存”按鈕。

管理應用程式網路規則

預設情況下，Kaspersky Endpoint Security 將按照其所監控的檔案或網路活動所對應的軟體的供應商名稱對安裝在電腦上的所有應用程式進行群組分配。應用程式群組將依次被歸類到“信任群組”中。所有應用程式和應用程式群組都將繼承來自其父群組的內容：應用程式控制規則、應用程式網路規則及其執行優先順序。

預設情況下，當篩選群組中所有應用程式的網路活動時，防火牆模組將套用應用程式群組的網路規則，這與[應用程式權限控制](#)元件相似。應用程式群組網路規則將定義群組中應用程式存取不同網路連線的權限。

預設情況下，防火牆將為電腦上的 Kaspersky Endpoint Security 偵測到的每個應用程式群組建立網路規則集。您可以變更套用於預設建立的應用程式群組網路規則的防火牆操作。您不能編輯、刪除、停用或變更預設情況下建立的應用程式群組網路規則的優先等級。

您也可以為單個應用程式建立網路規則。此類規則將擁有比該應用程式所屬網路規則群組高的優先順序。

您在管理應用程式網路封包規則時可執行以下操作：

- 建立新網路規則。
您可以建立新網路規則，防火牆必須按照該規則管理應用程式或屬於選定應用程式群組的應用程式的網路活動。
- 啟用或停用網路規則。
所有網路規則都將新增到具有“*閒*”狀態的應用程式網路規則清單中。當啟用網路規則時，防火牆套用此規則。您可以停用手動建立的網路規則。如果網路規則被停用，防火牆將暫時不套用此規則。
- 變更網路規則的設定。
當您建立新的網路規則之後，您始終可以返回其設定並根據需要進行修改。
- 變更網路規則的防火牆操作。
在網路規則清單中，您可以編輯防火牆在該應用程式或應用程式群組中偵測到網路活動時對網路規則施加的操作。
- 變更網路規則的優先順序。
您可以提高或降低自訂網路規則的優先順序。
- 刪除網路規則。
您可以刪除自訂網路規則，以使防火牆停止在偵測到網路活動時將此網路規則套用於選取的應用程式或應用程式群組，並停止在該應用程式網路規則清單中顯示此規則。

建立和編輯應用程式網路規則

若要為應用程式群組建立和編輯網路規則，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點防護”區域中，選取“防火牆”子區域。

3. 點擊“應用程式網路規則”按鈕。

在“防火牆”視窗開啟“應用程式控制規則”頁籤。

4. 在應用程式清單中，選取您想為其建立或編輯網路規則的應用程式或應用程式群組。

5. 點擊右鍵調出上下文功能表，根據您的需要選取“應用程式規則”或“群組規則”。

這會開啟“應用程式控制規則”或“應用程式群組控制規則”視窗。

6. 在開啟的視窗中選取“網路規則”頁籤。

7. 請執行以下操作之一：


- 要建立一個新的網路規則，請點擊“新增”按鈕。
- 要編輯一個網路規則，請在網路規則清單中選取此規則，並點擊“編輯”按鈕。

開啟“網路規則”視窗。

8. 在“動作”下拉清單中選取防火牆在偵測到此類網路活動後的操作：

- 允許
- 封鎖

9. 在“名稱”欄位中透過以下方式填寫此網路服務  的名稱：

- 點擊位於“名稱”欄位右側的  圖示，然後從下拉清單中選取網路服務的名稱。此下拉清單中含有定義最常用的網路連線的網路服務。
- 在“名稱”欄位中手動輸入網路服務名稱。

10. 指定資料傳輸協定：

a. 勾選“協定”方塊。

b. 在下拉式功能表中選取監控網路活動的協定種類。

防火牆將監控使用 TCP、UDP、ICMP、ICMPv6、IGMP 和 GRE 協定的網路連線。

如果您從“名稱”下拉清單中選取網路服務，那麼“協定”核取方塊將自動勾選，並且在核取方塊旁邊的下拉清單中自動填寫與所選網路服務相對應的協定類型。預設情況下將會選取“協定”方塊。

11. 在“方向”下拉清單中選取受監控的網路活動方向。

防火牆將對以下方向的網路連線進行監控：

- 接收。
- 接收/傳送：
- 傳送。

12. 如果選取的是 ICMP 或 ICMPv6 埠，您可以指定 ICMP 封包類型和代碼：

a. 勾選“ICMP 類型”方塊並在下拉清單中選取 ICMP 封包類型。

b. 勾選“ICMP 代碼”方塊並在下拉清單中選取 ICMP 封包代碼。

13. 如果選取的是 TCP 或 UDP 協定類型，您可以指定其連線受監控的本機和遠端電腦逗號分隔的連接埠：
 - a. 在“**遠端連接埠**”欄位中輸入遠端連接埠。
 - b. 在“**本機連接埠**”欄位中輸入本機連接埠。
14. 指定傳送和/或接收網路封包的遠端電腦的網路位址。若要執行操作，請選取“**遠端位址**”下拉清單中的任一以下值：
 - **任何位址**。網路規則將控制任意 IP 位址的遠端電腦接收和/或傳送的網路封包。
 - **子網路位址**。網路規則將控制擁有與選定網路類型相關的 IP 位址的電腦傳送和/或接收的網路封包：**信任網路**、**區域網路**或**公用網路**。
 - **來自群組位址**。網路規則將控制擁有可使用“**新增**”、“**編輯**”和“**刪除**”按鈕指定的清單中 IP 位址的遠端電腦傳送和/或接收的網路封包。
15. 指定安裝了 Kaspersky Endpoint Security 的可以傳送和/或接收網路封包的電腦的網路位址。若要執行操作，請選取“**本機位址**”下拉清單中的任一以下值：
 - **任何位址**。網路規則將控制任意 IP 位址的安裝了 Kaspersky Endpoint Security 的遠端電腦接收和/或傳送的網路封包。
 - **來自群組位址**。網路規則將控制擁有可使用“**新增**”、“**編輯**”和“**刪除**”按鈕指定的清單中 IP 位址的已安裝 Kaspersky Endpoint Security 的遠端電腦傳送和/或接收的網路封包。

有時候無法獲得使用網路封包的應用程式的本機位址。如果出現這種情況，則“**本機位址**”設定值將被略過。

16. 如果您希望將網路規則的操作反映在**報告**中，請選取“**記錄事件**”核取方塊。
17. 在“**網路規則**”視窗中點擊“**確定**”。

如果建立新的網路規則，此規則將顯示在“**網路規則**”頁籤中。
18. 如果規則用於應用程式群組則點擊“**應用程式群組控制規則**”視窗中的“**確定**”，或者如果規則用於某個應用程式則點擊“**應用程式群組控制規則**”視窗中的“**確定**”。
19. 在“**防火牆**”視窗中點擊“**確認**”。
20. 要儲存變更，請點擊“**儲存**”按鈕。

啟用和停用應用程式網路規則

若要啟用或停用應用程式網路規則，請執行以下操作：

1. 開啟**程式設定視窗**。
2. 在視窗左側的“**端點防護**”區域中，選取“**防火牆**”子區域。

在視窗右側，將顯示防火牆元件的設定。
3. 點擊“**應用程式網路規則**”按鈕。

在“**防火牆**”視窗開啟“**應用程式控制規則**”頁籤。

4. 在清單中選取您想為其啟用或停用網路規則的應用程式或應用程式群組。
5. 點擊右鍵調出上下文功能表，根據您的需要選取“**應用程式規則**”或“**群組規則**”。
這會開啟“**應用程式控制規則**”或“**應用程式群組控制規則**”視窗。
6. 在開啟的視窗中選取“**網路規則**”頁籤。
7. 在應用程式群組的網路規則清單中，選取相關的網路規則。
8. 請執行以下操作之一：
 - 如果您希望啟用規則，請選取網路規則名稱旁邊的核取方塊。
 - 如果您希望停用規則，請清空網路規則名稱旁邊的核取方塊。

您不能停用預設情況下由防火牆建立的應用程式群組網路規則。

9. 如果規則用於應用程式群組則點擊“**應用程式群組控制規則**”視窗中的“**確定**”，或者如果規則用於某個應用程式則點擊“**應用程式群組控制規則**”視窗中的“**確定**”。
10. 在“**防火牆**”視窗中點擊“**確認**”。
11. 要儲存變更，請點擊“**儲存**”按鈕。

變更應用程式網路規則的防火牆操作

您可以變更應用於應用程式或應用程式群組的網路規則的預設建立的防火牆操作，也可以為應用程式或應用程式群組變更單個自訂網路規則的防火牆操作。

若要為應用程式或應用程式群組變更所有網路規則的防火牆操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**端點防護**”區域中，選取“**防火牆**”子區域。
在視窗右側，將顯示防火牆元件的設定。
3. 點擊“**應用程式網路規則**”按鈕。
在“**防火牆**”視窗開啟“**應用程式控制規則**”頁籤。
4. 如果您希望變更預設建立的應用至所有網路規則的防火牆操作，則選取清單中應用程式或應用程式群組。手動建立的網路規則將保持不變。
5. 在“**網路**”列中，點擊右鍵顯示右鍵選單，然後選取您要分配的操作：
 - **繼承**
 - **允許**
 - **封鎖**

6. 點擊“**確定**”。

7. 要儲存變更，請點擊“**儲存**”按鈕。

若要變更一個應用程式或應用程式群組網路規則的防火牆操作，請執行以下操作：

1. 開啟[程式設定視窗](#)。

2. 在視窗左側的“**端點防護**”區域中，選取“**防火牆**”。

在視窗右側，將顯示防火牆元件的設定。

3. 點擊“**應用程式網路規則**”按鈕。

在“**防火牆**”視窗開啟“**應用程式控制規則**”頁籤。

4. 在清單中選取您想為其變更一個網路規則操作的應用程式或應用程式群組。

5. 點擊右鍵調出上下文功能表，根據您的需要選取“**應用程式規則**”或“**群組規則**”。

這會開啟“**應用程式控制規則**”或“**應用程式群組控制規則**”視窗。

6. 在開啟的視窗中選取“**網路規則**”頁籤。

7. 選取您要為其變更防火牆操作的網路規則。

8. 在“**權限**”列中，點擊右鍵顯示右鍵選單，然後選擇您要分配的操作：

- 允許
- 封鎖
- 記錄事件

9. 如果規則用於應用程式群組則點擊“**應用程式群組控制規則**”視窗中的“**確定**”，或者如果規則用於某個應用程式則點擊“**應用程式群組控制規則**”視窗中的“**確定**”。

10. 在“**防火牆**”視窗中點擊“**確認**”。

11. 要儲存變更，請點擊“**儲存**”按鈕。

變更應用程式網路規則的優先順序

網路規則的優先順序取決於其在網路規則清單中的位置。防火牆執行按照網路規則清單中規則的顯示順序自上而下執行規則。根據套用於特定網路連線的每個已處理網路規則，防火牆會允許或封鎖對該網路連線設定中指定的位址和連接埠的網路存取。

手動建立的網路規則擁有比預設網路規則高的優先順序。

您不能變更預設應用程式群組網路規則的優先順序。

若要變更網路規則的優先順序，請執行以下操作：

1. 開啟[程式設定視窗](#)。

2. 在視窗左側的“端點防護”區域中，選取“**防火牆**”子區域。
在視窗右側，將顯示防火牆元件的設定。
3. 點擊“**應用程式網路規則**”按鈕。
在“**防火牆**”視窗開啟“**應用程式控制規則**”頁籤。
4. 在應用程式群組網路規則清單中，選取您要變更網路規則優先順序的應用程式或應用程式群組。
5. 點擊右鍵調出上下文功能表，根據您的需要選取“**應用程式規則**”或“**群組規則**”。
這會開啟“**應用程式控制規則**”或“**應用程式群組控制規則**”視窗。
6. 在開啟的視窗中選取“**網路規則**”頁籤。
7. 選取您想要變更其優先順序的網路規則。
8. 使用**上移**和**下移**按鈕將該規則移動到網路規則清單中您想要的位置：
9. 如果規則用於應用程式群組則點擊“**應用程式群組控制規則**”視窗中的“**確定**”，或者如果規則用於某個應用程式則點擊“**應用程式群組控制規則**”視窗中的“**確定**”。
10. 在“**防火牆**”視窗中點擊“**確認**”。
11. 要儲存變更，請點擊“**儲存**”按鈕。

網路監控

本章節介紹網路監控資訊，並介紹如何啟動網路監控。

關於網路監控

*網路監控*是一個用於即時檢視網路活動資訊的工具。

啟動網路監控

若要啟動網路監控，請執行以下操作：

1. 開啟“[程式主視窗](#)”。
2. 選擇“**防護和控制**”頁籤。
3. 點擊“**防護**”區域。
開啟“**防護**”區域。
4. 右鍵點擊“**防火牆**”以開啟元件操作的右鍵選單。
5. 在右鍵選單中選取“**網路監控**”。
開啟“**網路監控**”視窗。在該視窗中，將以四個頁籤顯示電腦網路活動的相關資訊：

- “**網路活動**”頁籤顯示電腦目前所有活動的網路連線。接收和傳送的網路連線都將同時顯示。
- “**開啟連接埠**”頁籤列出電腦所有開啟的網路連接埠。
- “**網路流量**”頁籤顯示使用者電腦目前連接其他電腦之間傳送和接收的網路流量。
- “**封鎖的電腦**”頁籤列出網路攻擊防護元件在偵測到網路攻擊後封鎖該網路活動的遠端電腦 IP 位址。

網路攻擊防護

本章節介紹網路攻擊防護資訊，以及如何設定元件。

關於網路攻擊防護

網路攻擊防護將掃描接收的網路流量以偵測常見的網路攻擊活動。偵測到企圖針對您電腦進行網路攻擊時，Kaspersky Endpoint Security 將封鎖來自攻擊電腦的網路活動。您的螢幕將顯示有關網路攻擊嘗試的警告說明並顯示攻擊電腦的資訊。

來自攻擊電腦的網路流量將被封鎖一小時。您可以編輯封鎖電腦攻擊的設定。

Kaspersky Endpoint Security 資料庫提供目前已知類型的網路攻擊以及解決方法。網路攻擊防護元件偵測到的網路攻擊清單在[資料庫和應用程式模組更新](#)期間更新。


啟動或停用網路攻擊防護

預設情況下將啟用網路攻擊防護，並設定為最佳模式。您可以在必要時停用網路攻擊防護。

有兩種啟動或停用該元件的方式：

- 透過[應用程式主視窗](#)的“**防護和控制**”頁籤。
- 開啟[程式設定視窗](#)。

要啟用或停用網路攻擊防護，請在應用程式主視窗的“**防護和控制**”頁籤中執行以下操作：

1. 開啟“程式主視窗”。
2. 選擇“**防護和控制**”頁籤。
3. 點擊“**防護**”區域。
開啟“**防護**”區域。
4. 右鍵點擊“**網路攻擊防護**”以開啟元件操作的右鍵選單。
5. 請執行以下操作之一：
 - 要啟用網路攻擊防護，請在功能表中選取“**啟動**”。
網路攻擊防護 行左側顯示的元件狀態圖示  將變為圖示 。
 - 要停用網路攻擊防護，請在功能表中選取“**停止**”。
網路攻擊防護 行左側顯示的元件狀態圖示  將變為圖示 。

若要從應用程式設定視窗中啟用或停用網路攻擊防護，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**端點防護**”區域中，選取“**網路攻擊防護**”區域。
網路攻擊防護設定將顯示在視窗右方。

3. 請執行以下操作：

- 要啟用網路攻擊防護，請勾選“**啟用網路攻擊防護**”核取方塊。
- 要停用網路攻擊防護，請取消“**啟用網路攻擊防護**”核取方塊。

4. 要儲存變更，請點擊“**儲存**”按鈕。

網路攻擊防護設定

您可以執行下列操作來配置網路攻擊防護設定：

- 配置用於封鎖攻擊電腦的設定。
- 生成排除封鎖的位址清單。

編輯用於封鎖攻擊電腦的設定

若要編輯封鎖電腦攻擊的設定，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**端點防護**”區域中，選取“**網路攻擊防護**”區域。

網路攻擊防護設定將顯示在視窗右方。

3. 選取“**將攻擊電腦新增到封鎖電腦清單**”核取方塊。

如果勾選該核取方塊，在偵測到網路攻擊時，網路攻擊防護將在指定時間內封鎖來自攻擊電腦的網路流量。此功能將自動防護電腦避免以後來自同一位址的攻擊。

如果未勾選該核取方塊，在偵測到網路攻擊意圖時，網路攻擊防護不會啟動對以後來自同一位址的攻擊進行自動防護。

4. 在“**將攻擊電腦新增到封鎖電腦清單**”核取方塊旁邊的欄位中變更封鎖攻擊電腦的持續時間。

5. 要儲存變更，請點擊“**儲存**”按鈕。

設定排除在封鎖外的位址

若要設定排除在封鎖外的位址：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**端點防護**”區域中，選取“**網路攻擊防護**”區域。

網路攻擊防護設定將顯示在視窗右方。

3. 點擊“**排除項目**”按鈕。

開啟“**排除項目**”視窗。

4. 請執行以下操作之一：

- 如果您要新增新的 IP 位址，請點擊**“新增”**按鈕。
- 如果您希望編輯之前新增的 IP 位址，請在規則清單中選定它，然後點擊**“編輯”**按鈕。

“IP 位址”視窗將開啟。

5. 輸入不封鎖網路攻擊的電腦的 IP 位址。

6. 在**“IP 位址”**視窗中點擊**“確定”**。

7. 在**“排除”**視窗中點擊**“確認”**。

8. 要儲存變更，請點擊**“儲存”**按鈕。

BadUSB 攻擊防護

本部分包含有關 BadUSB 攻擊防護元件的資訊。

關於 BadUSB 攻擊防護

某些病毒會修改 USB 裝置的固件以欺騙作業系統，將 USB 偽裝為鍵盤。

BadUSB 攻擊防護元件可以防止受感染的模擬鍵盤的 USB 裝置連線至電腦。

當 USB 裝置連線至電腦並被程式識別為鍵盤時，程式將提示使用者使用該鍵盤或螢幕鍵盤（如果可用）輸入程式生成的數位代碼。這個步驟稱為鍵盤授權。程式將允許使用經過授權的鍵盤並封鎖未經授權的鍵盤。

BadUSB 攻擊防護在安裝之後將在後台運行。如果應用程式不受卡巴斯基安全管理中心政策管理，您可以透過[臨時暫停和還原電腦保護和控制](#)的方式啟用或停用 BadUSB 攻擊防護。

安裝 BadUSB 攻擊防護元件

如果您在 Kaspersky Endpoint Security 安裝期間選取了[基本或標準安裝](#)，則 BadUSB Attack Prevention 元件將不可用。若要進行安裝，您必須變更應用程式元件的設定。

若要安裝 *BadUSB* 攻擊防護元件，請執行以下操作：

1. 在“開始”選單中，選取“應用程式”→“Kaspersky Endpoint Security 10 for Windows”→“修改、修復或移除”。
啟動“安裝精靈”。
2. 在應用程式安裝精靈的“修改、修復或移除程式”視窗中，點擊“修改”按鈕。
應用程式安裝精靈的“自訂安裝”視窗將開啟。
3. 在“BadUSB 攻擊防護”元件名稱旁邊圖示的右鍵選單中，選取“功能將安裝在本機硬碟上”選項。
4. 點擊 **下一步** 按鈕。
5. 請按照“安裝精靈”的指示操作。

啟用和停用 BadUSB 攻擊防護。

要啟用或停用 *BadUSB* 攻擊防護：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點防護”區域中，選取“BadUSB 攻擊防護”子區域。
BadUSB 攻擊防護設定將顯示在視窗右邊。
3. 請執行以下操作之一：
 - 要啟用 BadUSB 攻擊防護，請勾選“**啟用 BadUSB 攻擊防護**”核取方塊。

- 要停用 BadUSB 攻擊防護，請取消勾選“**啟用 BadUSB 攻擊防護**”核取方塊。

4. 要儲存變更，請點擊“**儲存**”按鈕。

允許和禁止使用螢幕鍵盤進行授權

應當僅在 USB 裝置授權不支援輸入隨機字元時（例如條碼掃描器）使用螢幕鍵盤授權。不建議使用螢幕鍵盤授權未知的 USB 裝置。

若要允許或封鎖使用螢幕鍵盤進行授權：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**端點防護**”區域中，選取“**BadUSB 攻擊防護**”子區域。
此元件設定將顯示在視窗右方。
3. 請執行以下操作之一：
 - 選取“**禁止使用螢幕鍵盤進行授權**”核取方塊封鎖使用螢幕鍵盤進行授權。
 - 清空“**禁止使用螢幕鍵盤進行授權**”核取方塊封鎖使用螢幕鍵盤進行授權。
4. 要儲存變更，請點擊“**儲存**”按鈕。

鍵盤授權

在 BadUSB 攻擊防護元件安裝前被電腦識別為鍵盤的 USB 裝置在該元件安裝後仍將被認定為經過授權。

僅當啟用了提示 USB 鍵盤授權時程式才會要求認證作業系統識別為鍵盤的 USB 裝置。鍵盤經過授權前使用者無法使用該鍵盤。

如果停用了提示 USB 鍵盤授權，則使用者可以使用所有連線的鍵盤。啟用提示 USB 鍵盤授權之後，應用程式將立即提示授權每個連線的未經授權的鍵盤。

若要授權鍵盤，請執行以下操作：

1. 啟用了 USB 鍵盤授權後，將鍵盤連線至 USB 連接埠。
“<鍵盤名>鍵盤授權”視窗將開啟並帶有所連線鍵盤和授權所需的數位代碼。
 2. 使用所連線的鍵盤或螢幕鍵盤（如果可用）在授權視窗中輸入隨機生成的數位代碼。
 3. 點擊“**確定**”。
- 如果正確輸入代碼，程式將在授權鍵盤清單中儲存識別參數 - 鍵盤的 VID/PID 和其所連接的連接埠號。重新啟動作業系統後重新連接鍵盤時無需重複授權。

經授權的鍵盤連接至該電腦不同連接埠時，程式將再次提示為該鍵盤授權。

如果錯誤輸入數位代碼，則程式將生成新的代碼。輸入數位代碼時有三種方式：如果連續三次都沒有正確輸入數字代碼或者“<鍵盤名>鍵盤授權”視窗關閉了，程式將封鎖該鍵盤的輸入。重新連接鍵盤或者作業系統重新啟動後，程式將再次提示使用者重新執行鍵盤授權。

應用程式啟動控制

本章節介紹應用程式啟動控制的資訊，以及如何設定元件。

關於應用程式啟動控制

應用程式啟動控制元件使用 [應用程式啟動控制規則](#) 監控使用者嘗試啟動應用程式的操作並管理應用程式的啟動。

其設定不符合任何應用程式啟動控制規則的應用程式啟動將由選定的元件執行模式進行管理。預設情況下選定了 [黑名單模式](#)。該規則允許任何使用者啟動任何應用程式。

所有使用者嘗試啟動應用程式的操作都記錄在 [報告](#) 中。





啟用和停用應用程式啟動控制

儘管應用程式啟動控制被預設停用，您仍可以根據需要啟用應用程式啟動控制。

有兩種啟動或停用該元件的方式：

- 透過 [應用程式主視窗](#) 的“防護和控制”頁籤。
- 開啟 [程式設定視窗](#)。

要啟用或停用應用程式啟動控制，請在應用程式主視窗的“防護和控制”頁籤中執行以下操作：

1. 開啟“程式主視窗”。
2. 選擇“防護和控制”頁籤。
3. 點擊“端點控制”區域。
開啟“端點控制”區域。
4. 右鍵點擊應用程式啟動控制開啟元件相關資訊的右鍵選單。
系統將開啟一個用於選擇對該元件的操作功能表。
5. 請執行以下操作之一：
 - 要啟用應用程式啟動控制，請在功能表中選取“開始”。
應用程式啟動控制左側顯示的元件狀態圖示  將變為圖示 。
 - 要停用應用程式啟動控制，請在功能表中選取“停止”。
應用程式啟動控制左側顯示的元件狀態圖示  將變為圖示 。

若要從應用程式設定視窗中啟用或停用應用程式啟動控制，請執行以下操作：

1. 開啟 [程式設定視窗](#)。
2. 在視窗左側的“端點控制”區域中，選取“應用程式啟動控制”子區域。
在視窗右側，將顯示應用程式啟動控制元件的設定。

3. 請執行以下操作之一：

- 要啟用應用程式啟動控制，請選取“**啟用應用程式啟動控制**”核取方塊。
- 要停用應用程式啟動控制，請取消“**啟用應用程式啟動控制**”核取方塊。

4. 要儲存變更，請點擊“**儲存**”按鈕。

應用程式啟動控制功能限制

在以下情況中應用程式啟動控制元件的執行受到限制：

- 應用程式版本升級時，不支援匯入應用程式啟動控制元件設定。

若要還原應用程式啟動控制的功能，您必須重新配置元件設定。

- 如果沒有與 KSN 伺服器連線，則 Kaspersky Endpoint Security 將僅從本機資料庫中接收關於應用程式及其模組信譽的資訊。如果本機資料庫不包含有關應用程式的資訊，則此應用程式無法被放入信任群組中。

與 KSN 連線時應用程式的類別與沒有 KSN 連線時的類別可能不同。

- 在卡斯基安全管理中心資料庫中可以儲存 150,000 份已處理檔案的資訊。一旦達到這一數量的記錄，新的檔案將不會被處理。要還原清單操作，您必須從安裝了 Kaspersky Endpoint Security 的電腦上刪除之前存在卡斯基安全管理中心資料庫中的檔案。
- 此元件不會控制指令碼的啟動，除非透過命令列將指令碼傳送給解譯器。

如果應用程式啟動控制允許解譯器的啟動，則此元件將不會封鎖從此解譯器啟動指令碼。

- 此元件不會封鎖從不受 Kaspersky Endpoint Security 支援的解譯器啟動指令碼。

Kaspersky Endpoint Security 支援以下解譯器：

- Java
- PowerShell

支援以下類型的解譯器：

- { cCmdLineParser::itCmd, _T("%ComSpec%")};
- { cCmdLineParser::itReg, _T("%SystemRoot%\system32\reg.exe")};
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\system32\regedit.exe")};
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\regedit.exe")};
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\system32\regedt32.exe")};

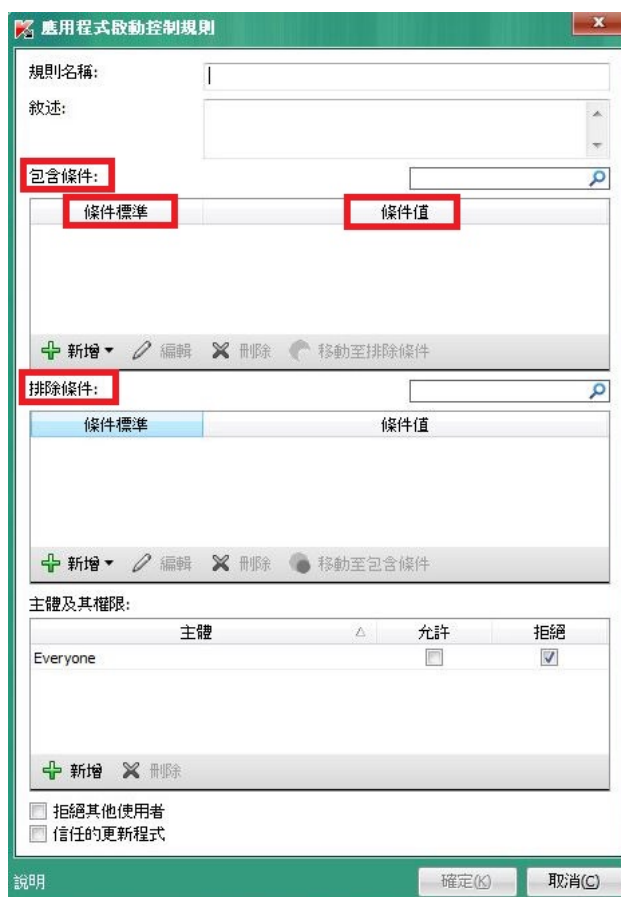
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\cscript.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\wscript.exe") };
- { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\system32\\msiexec.exe") };
- { cCmdLineParser::itMmc, _T("%SystemRoot%\\system32\\mmc.exe") };
- { cCmdLineParser::itMshta, _T("%SystemRoot%\\system32\\mshta.exe") };
- { cCmdLineParser::itRundll, _T("%SystemRoot%\\system32\\rundll32.exe") };
- { cCmdLineParser::itMetro, _T("%SystemRoot%\\system32\\wwahost.exe") };
- { cCmdLineParser::itCmd, _T("%SystemRoot%\\syswow64\\cmd.exe") };
- { cCmdLineParser::itReg, _T("%SystemRoot%\\syswow64\\reg.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedt32.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\cscript.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\wscript.exe") };
- { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\syswow64\\msiexec.exe") };
- { cCmdLineParser::itMmc, _T("%SystemRoot%\\syswow64\\mmc.exe") };
- { cCmdLineParser::itMshta, _T("%SystemRoot%\\syswow64\\mshta.exe") };
- { cCmdLineParser::itRundll, _T("%SystemRoot%\\syswow64\\rundll32.exe") };
- { cCmdLineParser::itMetro, _T("%SystemRoot%\\syswow64\\wwahost.exe") }.

關於應用程式啟動控制規則

Kaspersky Endpoint Security 根據規則按照使用者控制應用程式的啟動。應用程式啟動控制規則將指定觸發條件以及條件被觸發時應用程式啟動控制指定的操作（按使用者允許或封鎖應用程式啟用）。

規則觸發條件

觸發規則的條件擁有以下對應：“條件類型 - 條件標準 - 條件值”（參見下圖）。根據規則觸發條件，Kaspersky Endpoint Security 將對應用程式應用（或不應用）規則。



應用程式啟動控制規則。規則觸發條件參數

規則使用包括和排除條件：

- **包含條件**。如果應用程式比對至少一個包括條件，Kaspersky Endpoint Security 會將規則應用至此應用程式。
- **排除條件**。如果應用程式比對至少一個排除條件並且不比對任何包括條件，Kaspersky Endpoint Security 不會將規則套用至此應用程式。

規則觸發條件使用標準進行建立。Kaspersky Endpoint Security 中使用以下標準建立規則：

- 應用程式可執行檔案所在資料夾的路徑
- 檔案內容 (應用程式可執行檔名稱、磁碟上應用程式的可執行檔名稱、應用程式可執行檔的版本、應用程式名稱以及應用程式供應商)
- 應用程式可執行檔案的雜湊值。
- 憑證：發佈者、主體、指紋。
- 應用程式是否屬於某 KL 類別。
- 卸除式磁碟上可執行檔案的位置。

必須為條件中使用的每個標準制定標準值。如果要啟動的應用程式參數符合包括條件中指定的標準值，則觸發規則。在這種情況下，應用程式啟動控制將執行規則中指定的操作。如果應用程式參數比對排除條件中指定的值，應用程式啟動控制不會控制應用程式的啟動。

觸發規則後由應用程式啟動控制元件作出決定。

觸發操作後，應用程式啟動控制將允許使用者（或使用者群組）啟動應用程式或根據規則封鎖啟動。您可以選取允許或不允許比對規則的應用程式啟動的使用者或使用者群組。

如果一個規則未指定那些被允許啟動符合此規則的應用程式使用者，則此規則稱為“**封鎖**”規則。

如果一個規則未指定任何不允許啟動符合此規則的應用程式使用者，則此規則稱為“**允許**”規則。

封鎖規則的優先等級高於允許規則的優先等級。例如，如果已經為一個使用者群組指定應用程式啟動控制允許規則，但也為此使用者群組中的使用者指定一個應用程式啟動控制封鎖規則，則此使用者將被封鎖啟動應用程式。

規則執行狀態

應用程式啟動控制規則可為以下兩個狀態值之一：

- **開**。
此規則執行狀態表示已啟用規則。
- **關**。
此規則狀態表示已停用規則。

預設應用程式啟動控制規則

預設情況下，應用程式啟動控制以黑名單模式執行。此元件允許所有使用者啟動所有應用程式。當使用者嘗試啟動由應用程式啟動控制規則封鎖的應用程式時，**Kaspersky Endpoint Security** 將封鎖此應用程式啟動（如果選取了“**封鎖**”操作）或者在報告中儲存此應用程式啟動的資訊（如果選取了“**通知**”操作）。

管理應用程式啟動控制規則

您可以為應用程式網路規則執行以下操作：

- 新增新規則
- 建立或變更觸發規則的條件
- 編輯規則狀態
應用程式啟動控制規則可以被啟用（勾選規則旁邊的核取方塊）或停用（清空規則對應的核取方塊）。預設情況下建立應用程式啟動控制規則後即被啟用。
- 刪除規則

新增和編輯應用程式啟動控制規則

若要新增或編輯應用程式啟動控制規則，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**端點控制**”區域中，選取“**應用程式啟動控制**”子區域。

在視窗右側，將顯示應用程式啟動控制元件的設定。

3. 選擇“**啟用應用程式啟動控制**”以使元件設定可以供編輯。

4. 請執行以下操作之一：

- 要新增規則，請點擊“**新增**”按鈕。
- 如果您希望編輯現有規則，請選取在規則清單中選定它，然後點擊“**編輯**”按鈕。

開啟“**應用程式啟動控制規則**”視窗。

5. 指定或編輯規則的設定：

- a. 在“**規則名稱**”欄位中輸入或編輯規則的名稱。
- b. 在“**包含條件**”表中 [建立](#) 或編輯觸發規則的包含條件清單，方法是點擊“**新增**”、“**編輯**”、“**刪除**”和“**移動至排除條件**”按鈕。
- c. 在“**排除條件**”表中建立或編輯觸發規則的排除條件清單，方法是點擊“**新增**”、“**編輯**”、“**刪除**”和“**移動至包含條件**”按鈕。
- d. 如有必要，您可以變更規則觸發條件的類型：
 - 要將條件類型從包含條件變更為排除條件，請在“**包含條件**”表中選取一個條件，然後點擊“**移動至排除條件**”按鈕。
 - 要將條件類型從排除條件變更為包含條件，請在“**排除條件**”表中選取一個條件，然後點擊“**移動至包含條件**”按鈕。
- e. 編譯或編輯允許或不允許其啟動符合規則觸發條件的應用程式的使用者和/或使用者群組的清單。若要執行操作，請點擊“**使用者及其權限**”表中的“**新增**”按鈕。

將開啟 Microsoft Windows 中的“**選擇使用者或群組**”視窗。您透過該視窗可以選取使用者和/或使用者群組。

預設情況下，“**每個人**”值已新增至使用者清單。該規則適用於所有使用者。

如果該表中沒有指定使用者，則無法儲存該規則。

- f. 在“**使用者及其權限**”表中，選取使用者和/或使用者群組對應的“**允許**”或“**封鎖**”核取方塊以確定其啟動應用程式的權限。
預設選定的核取方塊取決於“[應用程式啟動控制執行模式](#)”。
- g. 如果您希望在應用程式啟動時封鎖比對規則觸發條件的“**使用者**”欄中沒有出現的使用者和不屬於“**使用者**”欄中指定使用者群組的所有使用者，則選取“**拒絕其他使用者**”核取方塊。

如果清空了“**拒絕其他使用者**”核取方塊，則 Kaspersky Endpoint Security 不會控制“**使用者及其權限**”清單中指定的使用者以及不屬於“**使用者及其權限**”表中指定使用者群組的使用者啟動應用程式。

- h. 如果您希望 Kaspersky Endpoint Security 將比對規則觸發條件的應用程式視為信任的更新程式，並且希望允許它們啟動未定義應用程式啟動控制規則的其它應用程式，請選取“**信任的更新程式**”核取方塊。

6. 點擊“**確定**”。

7. 要儲存變更，請點擊“儲存”按鈕。

為應用程式啟動控制規則新增觸發條件

若要為應用程式啟動控制規則新增觸發條件：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點控制”區域中，選取“應用程式啟動控制”子區域。
在視窗右側，將顯示應用程式啟動控制元件的設定。
3. 選擇“啟用應用程式啟動控制”以使元件設定可以供編輯。
4. 請執行以下操作之一：
 - 如果您要為應用程式建立一個新的網路規則並為其新增觸發條件，請點擊“新增”按鈕。
 - 如果您要將觸發條件新增至現有規則，則在規則清單中選取您所需的規則，然後點擊“編輯”按鈕。

開啟“應用程式啟動控制規則”視窗。

5. 在“包含條件”或“排除條件”表中，點擊“新增”按鈕。

您可以使用“新增”下拉清單將各種觸發條件新增至規則（請參見以下說明）。

若要根據檔案的內容在指定資料夾中新增規則觸發條件：

1. 在“新增”按鈕的下拉清單中，選取“指定資料夾中檔案內容的條件”。
Microsoft Windows 的標準“選取資料夾”視窗將開啟。
2. 在“選取資料夾”視窗中，選取包含可執行應用程式檔案的資料夾，您將這些檔案的內容做為觸發規則的一個或多個條件的基礎。
3. 點擊“確定”。
開啟“新增條件”視窗。
4. 在“顯示標準”下拉清單中，根據您要建立的一個或多個規則觸發條件選取標準：**檔案雜湊值**、**憑證**、**KL 類別**、**檔案內容**或**資料夾路徑**。

Kaspersky Endpoint Security 不支援擁有雜湊代碼的 MD5 檔案並且不會基於 MD5 雜湊代碼控制應用程式的啟動。規則觸發條件使用了 SHA256 雜湊代碼。

5. 如果您在“顯示標準”下拉清單中選取“檔案內容”請選取要在觸發規則的條件中使用的可執行檔案內容所對應的核取方塊：**檔案名稱**、**檔案版本**、**應用程式名稱**、**應用程式版本**和**軟體廠商**。
如果未選取任何指定內容，則無法儲存規則。
6. 如果您在“顯示標準”下拉清單中選取了“[憑證](#)”，則選取在規則觸發條件中要使用的設定對應的核取方塊：[發佈者](#)、[主體](#)和[指紋](#)。
如果未選取任何指定設定，則無法儲存規則。

不建議只將**發佈者**和**主體**標準設定為規則觸發條件。使用這些標準不可靠。

7. 選取您要將其內容包括在觸發規則的條件中的應用程式可執行資料夾名稱旁邊的核取方塊。
8. 點擊 **下一步** 按鈕。
系統將顯示程式化的規則觸發條件清單。
9. 在程式化的規則觸發條件清單中，選取您要新增到應用程式啟動控制規則的規則觸發條件所對應的核取方塊。
10. 點擊“**終止**”按鈕。

若要根據電腦上啟動的應用程式內容新增規則觸發條件：

1. 在“**新增**”按鈕的下拉功能表中，選取“**執行應用程式的內容的條件**”。
2. 在“**新增條件**”視窗的“**顯示標準**”下拉清單中，根據您要建立的一個或多個規則觸發條件選取標準：**檔案雜湊值**、**憑證**、**KL 類別**、**檔案內容**或**資料夾路徑**。
3. 如果您在“**顯示標準**”下拉清單中選取“**檔案內容**”請選取要在觸發規則的條件中使用的可執行檔案內容所對應的核取方塊：**檔案名稱**、**檔案版本**、**應用程式名稱**、**應用程式版本**和**軟體廠商**。
如果未選取任何指定內容，則無法儲存規則。
4. 如果您在“**顯示標準**”下拉清單中選取了“**憑證**”，則選取在規則觸發條件中要使用的設定對應的核取方塊：**發佈者**、**主體**和**指紋**。
如果未選取任何指定設定，則無法儲存規則。

不建議只將**發佈者**和**主體**標準設定為規則觸發條件。使用這些標準不可靠。

5. 選取您要將其內容包括在觸發規則的條件中的應用程式可執行資料夾名稱旁邊的核取方塊。
6. 點擊 **下一步** 按鈕。
系統將顯示程式化的規則觸發條件清單。
7. 在程式化的規則觸發條件清單中，選取您要新增到應用程式啟動控制規則的規則觸發條件所對應的核取方塊。
8. 點擊“**終止**”按鈕。

若要根據 **KL 類別** 新增規則觸發條件：

1. 在“**新增**”按鈕下的下拉清單中，選取“**KL 類別**條件”。
KL 類別是具有相同主旨內容的應用程式清單。該清單由 Kaspersky 專家維護。例如，“**Office 應用程式**” **KL 類別**就包含了 **Microsoft Office** 套裝的所有應用程式、**Adobe® Acrobat®** 和其他應用程式。
2. 在“**KL 類別**條件”視窗中，選中您要建立規則觸發條件所依據的 **KL 類別**的名稱旁邊的核取方塊。
3. 點擊“**確定**”。

若要新增自訂的規則觸發條件：

1. 在“**新增**”按鈕的下拉清單中，選取“**自訂條件**”。

2. 在“**自訂條件**”視窗中，點擊“**選取**”按鈕並指定應用程式可執行檔案的路徑。
3. 根據您要建立的規則觸發條件選取標準：**檔案雜湊值**、**憑證**、**檔案內容**或**檔案或資料夾路徑**。

如果您在 **檔案或資料夾路徑** 欄位中使用符號連結，建議您解析符號連結以正確操作“應用程式啟動控制”規則。要這樣做，點擊“**解析符號連結**”按鈕。

4. 如有需要，可配置選定標準的設定。
5. 點擊“**確定**”。

若要根據儲存應用程式可執行檔的磁碟機的資訊新增規則觸發條件：

1. 在“**新增**”按鈕的下拉清單中，選取“**檔案磁碟機條件**”。
2. 在“**檔案磁碟機條件**”視窗中，開啟“**磁碟機**”下拉清單，以選取控制其中應用程式啟動的磁碟機類型。
3. 點擊“**確定**”。

變更應用程式啟動控制規則的狀態

若要變更應用程式啟動控制規則的狀態，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**端點控制**”區域中，選取“**應用程式啟動控制**”子區域。
在視窗右側，將顯示應用程式啟動控制元件的設定。
3. 選擇“**啟用應用程式啟動控制**”以使元件設定可以供編輯。
4. 選取您想要編輯其狀態的規則。
5. 在 **狀態** 列中，執行以下操作：
 - 如果您希望啟用使用規則，則選取規則旁邊的核取方塊。
 - 如果您希望停用使用規則，則清空規則旁邊的核取方塊。
6. 要儲存變更，請點擊“**儲存**”按鈕。

測試應用程式啟動控制規則

若要確保應用程式啟動控制規則不會封鎖需要執行的應用程式，建議將新建立的規則加至測試模式並分析其執行。

在測試模式下分析應用程式啟動控制規則的執行及傳送應用程式啟動控制事件給卡巴斯基安全管理中心。如果允許所有電腦使用者需要使用的應用程式啟動，則這些規則已被正確建立。否則，建議您修改您所建立規則的設定。

預設情況下已停用應用程式啟動控制規則的測試模式。

若要應用程式啟動控制規則：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點控制”區域中，選取“應用程式啟動控制”子區域。
在視窗右側，將顯示應用程式啟動控制元件的設定。
3. 選擇“啟用應用程式啟動控制”以使元件設定可以供編輯。
4. 在“應用程式啟動控制規則”下拉清單中選取以下選項之一：
 - **黑名單**，如果您希望允許除封鎖規則中指定的應用程式之外的所有應用程式執行。
 - **白名單**，如果您希望封鎖除允許規則中指定的應用程式之外的所有應用程式執行。
5. 在“動作”下拉清單中選取“通知”。
6. 要儲存變更，請點擊“儲存”按鈕。

Kaspersky Endpoint Security 不會封鎖被應用程式啟動控制規則封鎖啟動的應用程式，但是會將它們的啟動報告給管理伺服器。

編輯應用程式啟動控制訊息範本

使用者嘗試啟動被應用程式啟動控制規則封鎖的應用程式時，Kaspersky Endpoint Security 會顯示訊息，指明該應用程式被封鎖啟動。如果您認為該應用程式被錯誤地封鎖啟動，可使用訊息內容中的連結向公司區域網路管理員傳送訊息。

針對應用程式被封鎖啟動時顯示的訊息和傳送給管理員的訊息可使用特殊的範本。您可以修改訊息範本。

若要編輯訊息範本，請執行下列操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點控制”區域中，選取“應用程式啟動控制”子區域。
在視窗右側，將顯示應用程式啟動控制元件的設定。
3. 選擇“啟用應用程式啟動控制”以使元件設定可以供編輯。
4. 點擊 **範本** 按鈕。
開啟“範本”視窗。
5. 請執行以下操作之一：
 - 如果您要編輯應用程式被封鎖啟動時顯示的訊息範本，請選取“**封鎖**”頁籤。
 - 如果您要修改傳送給區域網路管理員的回報訊息的範本，請選取“**傳送給管理員的資訊**”頁籤。
6. 編輯應用程式被封鎖啟動時或傳送給管理員的訊息範本。若要執行該操作，請使用根據“**預設**”和“**變數**”按鈕。
7. 點擊“**確定**”。

8. 要儲存變更，請點擊“儲存”按鈕。

關於應用程式啟動控制的操作模式

應用程式啟動端點控制模組有以下兩種工作模式：

- **黑名單**。在此模式下，應用程式啟動控制允許所有使用者啟動所有應用程式，除非它們已經在[應用程式啟動控制的封鎖規則](#)中指定。

預設情況下，應用程式啟動控制啟用此模式。

- **白名單**。在此模式下，應用程式啟動控制封鎖所有使用者啟動任何應用程式，除非它們已經在應用程式啟動控制的允許規則中指定。

如果完全設定應用程式啟動控制的允許規則，該元件會封鎖所有尚未經過區域網路管理員驗證的新應用程式啟動，但允許作業系統和使用者工作所依賴的信任群組應用程式執行。

每種模式都有兩種可對執行應用程式採取的操作：Kaspersky Endpoint Security 可以封鎖應用程式的啟動或者通知使用者比對應用程式啟動控制規則條件的應用程式的啟動。

您可以同時使用 Kaspersky Endpoint Security 本機介面和卡斯基安全管理中心端設定應用程式啟動控制以使其在這些模式下操作。

但是，卡斯基安全管理中心提供 Kaspersky Endpoint Security 本機介面所沒有的工具，如以下工作所需的工具：

- [建立應用程式類別](#)。

卡斯基安全管理中心管理主控台端建立的應用程式啟動控制規則根據自訂應用程式類別，但不像 Kaspersky Endpoint Security 本機介面那樣根據包括和排除條件。

- [收集關於安裝在區域網路電腦上的應用程式的相關資訊](#)。

這就是為什麼建議使用卡斯基安全管理中心設定應用程式啟動控制元件的執行。

選取應用程式啟動控制模式

若要選取應用程式啟動控制模式：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點控制”區域中，選取“**應用程式啟動控制**”子區域。
在視窗右側，將顯示應用程式啟動控制元件的設定。
3. 選擇“**啟用應用程式啟動控制**”以使元件設定可以供編輯。
4. 在“**應用程式啟動控制規則**”下拉清單中選取以下選項之一：

- **黑名單**，如果您希望允許除封鎖規則中指定的應用程式之外的所有應用程式執行。
- **白名單**，如果您希望封鎖除允許規則中指定的應用程式之外的所有應用程式執行。

選定此模式時，預設情況下建立兩個應用程式啟動控制規則：**黃金映像**和**信任的更新程式**。您無法刪除這些規則。這些規則的設定無法編輯。您可以透過選取或清除相關規則旁邊的核取方塊啟用或停用這些規則。預設情況下，啟用了**黃金映像**規則，**信任的更新程式**規則被停用。所有使用者允許啟動比對這些規則的觸發條件的應用程式。

選定模式期間建立的所有規則將在模式變更後儲存，以便可以再次使用這些規則。若要再次使用這些規則，您只需要在**應用程式啟動控制規則**下拉清單中選取所需的模式即可。

5. 在**動作**下拉清單中，選取使用者嘗試啟動應用程式啟動控制規則封鎖的應用程式時元件要執行的操作。
6. 如果您希望 Kaspersky Endpoint Security 在使用者啟動應用程式時監控載入 DLL 模組，則選取**監控 DLL 和驅動程式**核取方塊。

有關模組和載入模組的應用程式的資訊將儲存至報告。

如果選定此核取方塊，則 Kaspersky Endpoint Security 啟動之前即開始監控 DLL 模組和驅動程式。要設定在應用程式啟動前對所有 DLL 模組和驅動程式進行後續監控，請在選擇 **監控 DLL 和驅動程式** 核取方塊後重新啟動電腦。如果您無法重新啟動電腦，您可以在選擇 **監控 DLL 和驅動程式** 核取方塊後在 Kaspersky Endpoint Security 執行時載入 DLL 模組和驅動程式。在此情況下，監控僅對 Kaspersky Endpoint Security 執行時載入的 DLL 模組和驅動程式有效。

監控 DLL 模組和驅動程式時，不建議使用基於 KL 類別建立的“應用程式啟動控制”規則。確定 DLL 模組和驅動程式的 KL 類別（包括在“作業系統及其元件”規則中）可能會工作不正確。特別是，“作業系統及其元件”規則是預設建立的，並不是在 DLL 模組和驅動程式啟動時分配的。當開啟此功能時，必須為 DLL 模組和驅動程式建立單獨的允許規則。如果這種允許規則不存在使用此**控制 DLL 和驅動程式**功能可能會使系統不穩定。

我們建議開啟密碼防護來配置程式設定，以便可以關閉封鎖啟動極為重要的 DLL 模組和驅動程式的允許規則而在過程中變更卡巴斯基安全管理中心的政策設定。

7. 要儲存變更，請點擊**儲存**按鈕。

使用卡巴斯基安全管理中心管理應用程式啟動控制規則

該部分包含有關使用卡巴斯基安全管理中心設定應用程式啟動控制規則的資訊，並提供優化使用應用程式啟動控制的建議。

收集關於安裝在區域網路電腦上的應用程式資訊

若要建立優化的應用程式啟動控制規則，建議首先思考一下本機網路中電腦上所使用的應用程式。若要執行操作，您可以獲得以下資訊：

- 格式區域網路電腦上使用的應用程式供應商、版本和中文語言。
- 程式更新頻率。
- 公司中所使用的應用程式使用政策（這可能是安全性政策或管理政策）。

- 應用程式分發資料封包的儲存位置。

有關在公司區域網路電腦上使用的應用程式的資訊可在“**應用程式登錄檔**”資料夾和“**可執行檔案**”資料夾中找到。“**應用程式登錄檔**”資料夾和“**可執行檔案**”資料夾位於卡斯基安全管理中心主控台樹狀目錄中的“**應用程式管理**”資料夾中。

“**應用程式登錄檔**”資料夾包含在用戶端電腦上安裝的[網路代理](#)所偵測到的應用程式清單。

“**可執行檔案**”資料夾包含曾經在用戶端電腦上啟動的或者在 [Kaspersky Endpoint Security 清單工作](#)中偵測到的可執行檔案的清單。

要檢視該應用程式及其可執行檔的一般資訊以及安裝了該應用程式的電腦的清單，請開啟在“**應用程式登錄檔**”資料夾或“**可執行檔**”資料夾中選取的應用程式的內容視窗。

建立應用程式類別

為了建立規則時的方便，您可以建立應用程式類別並在建立應用程式啟動控制規則時使用它們。

建議您建立涵蓋公司內所使用的標準應用程式集的“工作應用程式”類別。如果工作中不同的使用者群組使用不同的應用程式集，則可以為每個使用者群組建立單獨的應用程式類別。

若要建立應用程式類別，請執行以下操作：

1. 開啟卡斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄中，選取“**附加** → **應用程式管理** → **應用程式類別**”資料夾。
3. 在工作區中點擊“**建立類別**”按鈕。
使用者類別建立精靈將啟動。
4. 請按照使用者類別建立精靈的指示操作。

使用卡斯基安全管理中心建立應用程式啟動控制規則

若要使用卡斯基安全管理中心建立應用程式啟動控制規則：

1. 開啟卡斯基安全管理中心的管理主控台。
2. 在主控台樹狀目錄的“**管理電腦**”資料夾中，開啟相關用戶端電腦所屬的管理群組名稱的資料夾。
3. 在工作區選擇“**政策**”頁籤。
4. 選擇所需政策。
5. 使用以下方式開啟“**內容: <政策名稱>**”視窗：
 - 在所選定項目右鍵選單中，選擇“**內容**”。
 - 點擊位於管理主控台工作區右側的“**設定政策**”連線。
6. 在“**端點控制**”區域中，選取“**應用程式啟動控制**”子區域。

在視窗右側，將顯示應用程式啟動控制元件的設定。

7. 點擊“**新增**”按鈕。

開啟“**應用程式啟動控制規則**”視窗。

8. 在“**類別**”下拉清單中，選取您要依據其建立規則的應用程式類別。

9. 指定您要配置其權限啟動選定類別中應用程式的使用者和使用者群組清單。若要執行操作，應在“**主體及其權限**”表中點擊“**新增**”按鈕。

Microsoft Windows 中將開啟“**選取使用者或群組**”視窗。您透過該視窗可以選取使用者和/或使用者群組。

10. 在“**主體及其權限**”表中：

- 如果您希望允許使用者和/或使用者群組啟動屬於選定類別的應用程式，則選取這些使用者旁邊的“**允許**”核取方塊。
- 如果您希望封鎖使用者和/或使用者群組啟動屬於選定類別的應用程式，則選取這些使用者旁邊的“**封鎖**”核取方塊。

11. 如果您希望在應用程式啟動時封鎖屬於選定類別的應用程式的“**使用者**”欄中沒有出現的使用者和不屬於“**使用者**”欄中指定使用者群組的所有使用者，則選取“**拒絕其他使用者**”核取方塊。

12. 如果您希望 Kaspersky Endpoint Security 將屬於規則中指定類別的應用程式視為信任的更新程式，並且希望允許它們啟動未定義應用程式啟動控制規則的其他應用程式，請選取“**信任的更新程式**”核取方塊。

13. 點擊“**確定**”。

14. 在政策內容視窗的“**應用程式啟動控制**”區域中，點擊“**套用**”按鈕。

使用卡巴斯基安全管理中心變更應用程式啟動控制規則的狀態

若要變更應用程式啟動控制規則的狀態，請執行以下操作：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在主控台樹狀目錄的“**管理電腦**”資料夾中，開啟相關用戶端電腦所屬的管理群組名稱的資料夾。
3. 在工作區選擇“**政策**”頁籤。
4. 選擇所需政策。
5. 使用以下方式開啟“**內容: <政策名稱>**”視窗：
 - 在所選定項目右鍵選單中，選擇“**內容**”。
 - 點擊位於管理主控台工作區右側的“**設定政策**”連線。
6. 在“**端點控制**”區域中，選取“**應用程式啟動控制**”子區域。

在視窗右側，將顯示應用程式啟動控制元件的設定。
7. 選取要變更其狀態的應用程式啟動控制規則。
8. 在“**狀態**”列中執行以下操作之一：

- 如果您希望啟用使用規則，則選取規則旁邊的核取方塊。
- 如果您希望停用使用規則，則清空規則旁邊的核取方塊。

9. 點擊 **套用** 按鈕。

應用程式權限控制

如果將 Kaspersky Endpoint Security 安裝在執行 Microsoft Windows for workstations 的電腦上，則可使用此元件。如果將 Kaspersky Endpoint Security 安裝在執行 [Microsoft Windows 以做檔案伺服器之用](#) 的電腦上，則此元件無法使用。

本章節介紹應用程式權限控制的資訊，以及如何設定元件。

關於應用程式權限控制

應用程式權限控制可避免應用程式執行可能給作業系統帶來危險的操作，並確保控制對作業系統資源以及您身分資料的存取。

該元件可使用 [應用程式控制規則](#) 來控制應用程式的活動，包括對受防護資源（例如檔案和資料夾、登錄機碼以及網路位址）的存取。應用程式控制規則是應用於作業系統中各種應用程式操作以及對電腦資源的存取權限的一組限制。

防火牆元件監控應用程式的網路活動

在電腦上首次啟動某應用程式時，應用程式權限控制元件會驗證應用程式的安全，並將其置於一個信任群組中。信任群組定義在控制應用程式活動時 Kaspersky Endpoint Security 所應用的應用程式控制規則。

建議僅 [參加卡巴斯基安全網路](#) 以便使應用程式權限控制執行更有效。透過卡巴斯基安全網路獲得的資料使您可以將應用程式更加準確地分類在組中，並應用最佳應用程式控制規則。

再次啟動應用程式時，應用程式權限控制會檢查其完整性。如果應用程式未變更，則該元件會對其應用目前應用程式控制規則。如果應用程式已經過修改，則應用程式權限控制會對其進行重新掃描，就像它首次啟動時一樣。

音訊和視頻裝置控制限制

關於音訊流防護

音訊流防護需要以下特殊考慮：

- 必須為該功能啟用應用程式權限控制元件才能執行。
- 如果在應用程式權限控制元件啟動之前該應用程式開始接受音訊流，則 Kaspersky Endpoint Security 允許該應用程式接收音訊流且不顯示任何通知。
- 如果您在應用程式開始接收音訊流之後將該應用程式移動至“**不受信任**”群組或“**高限制**”群組，Kaspersky Endpoint Security 將允許應用程式接收音訊流且不顯示任何通知。
- 應用程式存取錄音裝置的設定被變更後（例如，如果在應用程式控制設定視窗中封鎖了該應用程式接收音訊流），則必須重新啟動該應用程式才能封鎖其繼續接收音訊流。
- 控制對錄音裝置音訊流的存取不取決於應用程式的鏡頭存取設定。

- Kaspersky Endpoint Security 僅防護對內建麥克風和外建麥克風的存取。不支援其他音訊流裝置。
- Kaspersky Endpoint Security 無法防護對其他諸如單反相機、可攜式錄影機和動作捕捉相機中音訊流的防護。

在 Kaspersky Endpoint Security 安裝和升級期間應特別考慮音訊和視頻裝置的執行。

當您在安裝 Kaspersky Endpoint Security 之後首次執行音訊和視頻錄製或播放應用程式時，音訊和視頻播放或錄製可能會被中斷。為了確保該功能能夠控制應用程式對錄音裝置的存取，這是必要的。Kaspersky Endpoint Security 首次執行時控制音訊硬體的系統裝置將重新開機。

關於應用程式對鏡頭的存取

鏡頭存取保護功能擁有以下特別考慮和限制：

- 應用程式將控制從處理鏡頭資料而來的視頻和靜止影像。
- 應用程式將控制視頻流，如果其作為鏡頭接收視頻流的一部分。
- 應用程式僅控制在 Windows 裝置管理員中顯示為“**影像處理裝置**”透過 USB 或 IEEE1394 連線的鏡頭。

支援的鏡頭

Kaspersky Endpoint Security 支援以下鏡頭：

- Logitech HD Webcam C270
- Logitech HD Webcam C310
- Logitech Webcam C210
- Logitech Webcam Pro 9000
- Logitech HD Webcam C525
- Microsoft LifeCam VX-1000
- Microsoft LifeCam VX-2000
- Microsoft LifeCam VX-3000
- Microsoft LifeCam VX-800
- Microsoft LifeCam Cinema

Kaspersky 不保證支援不在清單中的鏡頭。





啟用和停用應用程式權限控制

預設情況下已啟用應用程式權限控制並且以 Kaspersky Lab 專家建議的模式執行。如有需要，您可以停用應用程式權限控制。

有兩種啟動或停用該元件的方式：

- 透過[應用程式主視窗](#)的“**防護和控制**”頁籤。
- 開啟[程式設定視窗](#)。

要啟用或停用應用程式權限控制，請在應用程式主視窗的“**防護和控制**”頁籤中執行以下操作：

1. 開啟“程式主視窗”。
2. 選擇“**防護和控制**”頁籤。
3. 點擊“**端點控制**”區域。
開啟“**端點控制**”區域。
4. 右鍵點擊應用程式權限控制開啟元件相關資訊的右鍵選單。
系統將開啟一個用於選擇對該元件的操作功能表。
5. 請執行以下操作之一：
 - 若要啟用應用程式權限控制，請選取“**開始**”。
顯示在“應用程式權限控制”行左側的元件狀態圖示將變為圖示。
 - 要停用應用程式權限控制元件，請在功能表中選取“**停止**”。
顯示在“應用程式權限控制”行左側的元件狀態圖示將變為圖示。

若要透過應用程式設定視窗啟用或停用應用程式權限控制，請執行以下操作：

1. 開啟程式設定視窗。
2. 在視窗左側的“**端點控制**”區域中，選擇“**應用程式權限控制**”。
在視窗右側，將顯示應用程式權限控制元件的設定。
3. 在視窗右側，執行下列操作：
 - 要啟用應用程式啟動控制，請選取“**啟用應用程式權限控制**”核取方塊。
 - 要停用應用程式啟動控制，請取消“**啟用應用程式權限控制**”核取方塊。
4. 要儲存變更，請點擊“**儲存**”按鈕。

管理應用程式信任群組

在電腦上首次啟動應用程式時，應用程式權限控制元件會驗證應用程式的安全，並將其置於一個[信任群組](#)中。

在應用程式掃描的第一階段，Kaspersky Endpoint Security 將搜尋已知應用程式的內部資料庫檢視是否存在相符的條目，然後同時向[卡巴斯基安全網路](#)資料庫傳送請求（如果網際網路連線可用）。根據內部資料庫和卡巴斯基安全網路資料庫的搜尋結果，應用程式將被放置到某個信任群組中。每次應用程式啟動時，Kaspersky Endpoint Security 會向 KSN 資料庫傳送新查詢，如果 KSN 中該應用程式的信譽發生變化則將應用程式放置到不同信任群組中。

您可以選擇 Kaspersky Endpoint Security 將所有未知應用程式自動分配到其中的受信任群組。在 Kaspersky Endpoint Security 之前啟動的應用程式將被自動移至“[選擇受信任群組](#)”視窗中指定的受信任群組。

該元件將只根據防火牆設定中設定的網路規則控制 Kaspersky Endpoint Security 啟動前啟動的應用程式的網路活動。

配置將應用程式分配到信任群組的設定

如果啟用了參與卡巴斯基安全網路，Kaspersky Endpoint Security 會在每次應用程式啟動時向 KSN 傳送有關應用程式信譽的查詢。根據收到的 KSN 回復，應用程式可能會被移動至應用程式權限控制設定中指定的信任群組不同的信任群組中。

若要配置將應用程式置於信任群組中的設定，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點控制”區域中，選擇“**應用程式權限控制**”子區域。
在視窗右側，將顯示應用程式權限控制元件的設定。
3. 如果您想要將來自受信任供應商的經過數位簽章的應用程式自動置於“信任”群組中，請選取“**信任具有數位簽章的應用程式**”核取方塊。

受信任供應商是卡巴斯基包含在受信任群組中的那些軟體供應商。您還[可以手動將供應商憑證新增到受信任系統憑證儲存中](#)。

4. 選取將未知的應用程式分配到信任群組的方式：
 - 若要使用啟發式分析將未知應用程式分配至信任群組，請選取“**使用啟發式分析以定義群組**”選項並在“**定義群組最大時間**”欄位中指定分配給掃描啟動應用程式的時間量。
 - 如果您希望將所有未知的應用程式分配到一個指定的群組，請選取“**自動移至群組**”，並在下拉清單中選取適當的信任群組。

出於安全考慮，“信任”群組不會包括在“自動移動至群組”設定的值中。

5. 要儲存變更，請點擊“**儲存**”按鈕。

修改信任群組

在應用程式首次執行時，Kaspersky Endpoint Security 會自動將其分配到一個指定的信任群組。您可以根據需要將此應用程式手動移動到另一個信任群組。

Kaspersky 專家建議您不要將應用程式從自動分配的信任群組移動到不同的信任群組。相反，您可以編輯單個應用程式的規則。

若要變更應用程式首次執行時由 *Kaspersky Endpoint Security* 自動分配的信任群組：

1. 開啟 [程式設定視窗](#)。
2. 在視窗左側的“端點控制”區域中，選擇“應用程式權限控制”。
在視窗右側，將顯示應用程式權限控制元件的設定。
3. 點擊“應用程式”按鈕。
開啟“應用程式控制規則”頁籤上的“應用程式”視窗。
4. 在“應用程式控制規則”頁籤上選取應用程式。
5. 請執行以下操作之一：
 - 右鍵點擊以顯示應用程式的右鍵選單。在應用程式的上下文功能表中，選取“移至群組 → <群組名稱>”。
 - 要開啟該右鍵選單，請點擊“受信任”/“低限制”/“高限制”/“不信任”連結。在右鍵選單中選取所需的信任群組。
6. 點擊“確定”。
7. 要儲存變更，請點擊“儲存”按鈕。

選取在 *Kaspersky Endpoint Security* 啟動之前啟動的應用程式受信任群組

該元件只控制在 *Kaspersky Endpoint Security* 啟動前啟動的應用程式的網路活動。程式根據 [防火牆設定](#) 中指定的網路規則進行控制。若要指定必須為此類應用程式的網路活動應用哪些網路規則，您必須選取受信任群組。

若要選取在 *Kaspersky Endpoint Security* 啟動之前啟動的應用程式信任群組：

1. 開啟 [程式設定視窗](#)。
2. 在視窗左側的“端點控制”區域中，選擇“應用程式權限控制”。
在視窗右側，將顯示應用程式權限控制元件的設定。
3. 點擊“編輯”按鈕。
這將開啟“選擇信任群組”視窗。
4. 選取所需的信任群組。
5. 點擊“確定”。
6. 要儲存變更，請點擊“儲存”按鈕。

管理應用程式控制規則

在預設情況下，應用程式的活動將由 **Kaspersky Endpoint Security** 在此應用程式第一次啟動時分配的信任群組指定的應用程式控制規則來控制。根據需要，您可以為信任群組中的單個應用程式或一組應用程式編輯整個信任群組的應用程式控制規則。

信任群組中為單個應用程式或一組應用程式指定的應用程式控制規則所擁有的優先順序別要高於為信任群組指定的應用程式控制規則。換句話說，如果信任群組中單個應用程式或一組應用程式的應用程式控制規則設定與信任群組的應用程式控制規則設定不同，應用程式權限控制元件將根據為單個應用程式或一組應用程式定義的應用程式控制規則來控制信任群組內應用程式或應用程式群組的活動。

變更受信任群組和應用程式群組的應用程式控制規則

預設情況下已為不同的信任群組建立最佳的應用程式控制規則。應用程式群組控制規則的設定從信任群組控制規則的設定中繼承。您可以編輯預設的信任群組控制規則和應用程式群組控制規則。

若要編輯預設的信任群組控制規則或應用程式群組控制規則，請執行以下操作：

1. 開啟[程式設定視窗](#)。

2. 在視窗左側的“端點控制”區域中，選擇“**應用程式權限控制**”。

在視窗右側，將顯示應用程式權限控制元件的設定。

3. 點擊“**應用程式**”按鈕。

這將開啟“**應用程式權限控制**”視窗中的“**應用程式控制規則**”核取方塊。

4. 選取所需的信任群組或應用程式群組。

5. 從信任群組或應用程式群組的右鍵選單中，選取“**群組規則**”。

程式將開啟“**應用程式群組控制規則**”視窗。

6. 在“**應用程式群組控制規則**”視窗中，執行下列操作：

- 要編輯控制信任群組或應用程式群組存取作業系統登錄檔、使用者檔案、應用程式設定的權限的信任群組控制規則或應用程式群組控制規則，請選取“**檔案和系統登錄檔**”頁籤。
- 要編輯控制信任群組或應用程式群組存取作業系統處理程序和物件的權限的信任群組控制規則或應用程式群組控制規則，請選取“**權限**”頁籤。

7. 按右鍵在相關資源的相關操作列中顯示右鍵選單。

8. 選擇相關功能表項目。

- 繼承
- 允許
- 封鎖
- 記錄事件

如果您正在編輯信任群組控制規則，“**繼承**”選項將不可用。

9. 點擊“**確定**”。

10. 在“**應用程式**”視窗中點擊“**確定**”。

11. 要儲存變更，請點擊“**儲存**”按鈕。

編輯應用程式控制規則

預設情況下，屬於一個應用程式群組或信任群組的應用程式，其應用程式控制規則的設定從信任群組控制規則的設定中繼承。您可以編輯應用程式控制規則的設定。

若要變更應用程式控制規則：

1. 開啟[程式設定視窗](#)。

2. 在視窗左側的“**端點控制**”區域中，選擇“**應用程式權限控制**”。

在視窗右側，將顯示應用程式權限控制元件的設定。

3. 點擊“**應用程式**”按鈕。

這將開啟“**應用程式權限控制**”視窗中的“**應用程式控制規則**”核取方塊。

4. 選取需要的應用程式。

5. 請執行以下操作之一：

- 在應用程式的右鍵選單中，選取“**應用程式規則**”。
- 在“**應用程式控制規則**”頁籤的右下角，點擊“**附加**”按鈕。

開啟“**應用程式控制**”視窗。

6. 在“**應用程式控制規則**”視窗中，執行下列操作：

- 要編輯控制應用程式存取作業系統登錄檔、使用者檔案、應用程式設定的權限的應用程式控制規則，請選取“**檔案和系統登錄檔**”頁籤。
- 要編輯應用程式存取作業系統處理程序和物件的權限的應用程式控制規則，請選取“**權限**”頁籤。

7. 按右鍵在相關資源的相關操作列中顯示右鍵選單。

8. 選擇相關功能表項目。

- **繼承**
- **允許**
- **封鎖**
- **記錄事件**

9. 點擊“**確定**”。

10. 在“**應用程式**”視窗中點擊“**確定**”。

11. 要儲存變更，請點擊“儲存”按鈕。

從卡巴斯基安全網路資料庫下載和更新應用程式控制規則

預設情況下，當卡巴斯基安全網路資料庫中偵測到某個應用程式新資訊時，Kaspersky Endpoint Security 會將從 KSN 資料庫下載的控制規則套用至該應用程式。您之後可以為該應用程式手動編輯控制規則。

如果一個應用程式首次執行時不存在於卡巴斯基安全網路資料庫中，但之後新增了相關資訊，預設情況下 Kaspersky Endpoint Security 會自動更新此應用程式的控制規則。

您可以停用從卡巴斯基安全網路資料庫下載應用程式控制規則以及自動更新之前未知應用程式的控制規則。

若您要停用從卡巴斯基安全網路資料庫下載和更新應用程式控制規則，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點控制”區域中，選擇“應用程式權限控制”。
在視窗右側，將顯示應用程式權限控制元件的設定。
3. 取消“根據卡巴斯基安全網路(KSN)資料庫更新未知應用程式的控制規則”核取方塊。
4. 要儲存變更，請點擊“儲存”按鈕。

停用繼承父程序限制

應用程式可能由使用者啟動，也可能由另一個執行中的應用程式啟動。由另一個應用程式啟動時，系統將建立一個啟動序列，其中包含父程序和子程序。

當應用程式嘗試獲得存取受防護資源的權限時，應用程式權限控制將分析此應用程式的所有父級程序的權限。然後遵循最小優先順序規則：比較應用程式與父程序的存取權限時，擁有最小優先順序的存取權限應用於此應用程式的活動。

存取權限的優先順序如下：

1. **允許** 此存取權限擁有最高優先順序。
2. **封鎖** 此存取權限擁有最低優先順序。

此機制能夠防止不信任的應有程式或權限受限的應用程式使用信任的應用程式來執行需要一定權限的操作。

如果由於缺少授予父處理程序的權限應用程式的活動被封鎖，您可以編輯這些權限或者停用父處理程序繼承限制。

若要停用繼承父程序限制

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點控制”區域中，選擇“應用程式權限控制”。
在視窗右側，將顯示應用程式權限控制元件的設定。

3. 點擊“**應用程式**”按鈕。

這將開啟“**應用程式權限控制**”視窗中的“**應用程式控制規則**”核取方塊。

4. 選取需要的應用程式。

5. 在應用程式的右鍵選單中，選取“**應用程式規則**”。

開啟“**應用程式控制**”視窗。

6. 在開啟的“**應用程式控制規則**”視窗中，選取“**排除**”頁籤。

7. 選取“**不要繼承父程序 (應用程式的限制)**”核取方塊。

8. 點擊“**確定**”。

9. 在“**應用程式**”視窗中點擊“**確定**”。

10. 要儲存變更，請點擊“**儲存**”按鈕。

從應用程式控制規則中排除特定的應用程式操作

若要從應用程式控制規則中排除特定應用程式操作，請執行以下操作：

1. 開啟[程式設定視窗](#)。

2. 在視窗左側的“**端點控制**”區域中，選擇“**應用程式權限控制**”。

在視窗右側，將顯示應用程式權限控制元件的設定。

3. 點擊“**應用程式**”按鈕。

這將開啟“**應用程式權限控制**”視窗中的“**應用程式控制規則**”核取方塊。

4. 選取需要的應用程式。

5. 在應用程式的右鍵選單中，選取“**應用程式規則**”。

開啟“**應用程式控制**”視窗。

6. 選取“**排除項目**”標籤。

7. 選取不監控應用程式活動操作旁的核取方塊。

8. 點擊“**確定**”。

9. 在“**應用程式**”視窗中點擊“**確定**”。

10. 要儲存變更，請點擊“**儲存**”按鈕。

刪除過時的應用程式控制規則

預設情況下，對於 60 天內未啟動的應用程式，其控制規則將自動移除。您可以變更未用應用程式的控制規則的儲存持續時間，或停用自動刪除規則。

若要刪除過時的應用程式控制規則：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點控制”區域中，選擇“應用程式權限控制”。
在視窗右側，將顯示應用程式權限控制元件的設定。
3. 請執行以下操作之一：
 - 如果您希望 Kaspersky Endpoint Security 刪除未用應用程式的控制規則，請選取“刪除超過以下時間未啟動的應用程式規則”核取方塊並指定相關的天數。
 - 要停用未用應用程式的控制規則的自動刪除，請取消“刪除超過以下時間未啟動的應用程式規則”核取方塊。
4. 要儲存變更，請點擊“儲存”按鈕。

防護作業系統資源和身分資料

應用程式權限控制將管理應用程式處理各種不同類別作業系統資源和身分資料的權限。

Kaspersky Lab 專家已建立受防護資源的預設類別。您無法編輯或刪除受防護資源的預設類別，或這些類別中的受防護資源。

但您可以執行下列操作：

- 新增新的受防護資源的類別。
- 新增新的受防護資源。
- 停用對某個資源的防護。

新增受防護資源的類別

若要新增新類別的受保護資源，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點控制”區域中，選擇“應用程式權限控制”。
在視窗右側，將顯示應用程式權限控制元件的設定。
3. 點擊 **資源** 按鈕。
這將開啟“應用程式權限控制”視窗中的“受保護資源”頁籤。
4. 在“受保護資源”頁籤的左側，選取您要向其新增新類別受保護資源的受保護資源區域或類別。
5. 點擊“新增”按鈕並在下拉清單中選取“類別”。
開啟“受防護資源的類別”視窗。

6. 在開啟的“**受防護資源的類別**”視窗中，輸入受保護資源新類別的名稱。
7. 點擊“**確定**”。
- 一個新項目會顯示在清單中的受保護資源類別。
8. 在“**應用程式權限控制**”視窗中點擊“**確定**”。
9. 要儲存變更，請點擊“**儲存**”按鈕。

新增某個類別的受保護資源後，您可以透過點擊“**受保護資源**”頁籤的左上角的“**編輯**”或“**刪除**”按鈕來編輯或刪除該類別。

新增受防護資源

若要新增受保護資源，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**端點控制**”區域中，選擇“**應用程式權限控制**”。
- 在視窗右側，將顯示應用程式權限控制元件的設定。
3. 點擊 **資源** 按鈕。
- 這將開啟“**應用程式權限控制**”視窗中的“**受保護資源**”頁籤。
4. 在“**受保護資源**”頁籤的左側，選取您要向其新增新類別受保護資源的受保護資源類別。
5. 點擊“**新增**”按鈕並在下拉清單中選取您要新增的資源類型：
 - **檔案或資料夾**。
 - **登錄機碼**。
- 開啟“**受保護資源**”視窗。
6. 在“**受保護資源**”視窗的“**名稱**”欄位中輸入受保護資源的名稱。
7. 點擊 **瀏覽** 按鈕。
8. 在開啟的視窗中，根據您要新增的受保護資源的類型指定必要的設定。點擊“**確定**”。
9. 在“**受保護資源**”視窗中，點擊“**確定**”。
- 在“**受保護資源**”頁籤上選取類別的受保護資源清單中。
10. 在“**應用程式權限控制**”視窗中點擊“**確定**”。
11. 要儲存變更，請點擊“**儲存**”按鈕。

新增受保護資源後，您可以透過在“**受保護資源**”頁籤的左上角點擊“**編輯**”或“**刪除**”按鈕來編輯或刪除受保護資源。

停用資源防護

若要停用資源防護，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點控制”區域中，選擇“應用程式權限控制”。
在視窗右側，將顯示應用程式權限控制元件的設定。
3. 在視窗右側，點擊“資源”按鈕。
這將開啟“應用程式權限控制”視窗中的“受保護資源”頁籤。
4. 請執行以下操作之一：
 - 在該頁籤左側的受保護資源清單中，選取您要為其停用防護的資源，並取消資源名稱旁邊的核取方塊。
 - 點擊“排除”並執行以下操作：
 - a. 在“排除”視窗中，點擊“新增”按鈕。在下拉清單中選取您想要新增到不受應用程式權限控制元件防護的排除清單的資源類型：“檔案或資料夾”或“登錄機碼”。
開啟“受保護資源”視窗。
 - b. 在“受保護資源”視窗的“名稱”欄位中輸入受保護資源的名稱。
 - c. 點擊 **瀏覽** 按鈕。
 - d. 在開啟的視窗中，根據要新增到應用程式權限控制元件防護的排除清單的受保護資源類型，指定必需的設定。
 - e. 點擊“確定”。
 - f. 在“受保護資源”視窗中，點擊“確定”。
在排除在應用程式權限控制元件防護範圍之外的資源的清單中將顯示一個新元素。

將資源新增到應用程式權限控制元件的防護排除清單後，您可以透過點擊“排除”視窗上方的“編輯”或“刪除”按鈕來編輯或刪除該資源。
 - g. 在“排除”視窗中點擊“確認”。
5. 在“應用程式權限控制”視窗中點擊“確定”。
6. 要儲存變更，請點擊“儲存”按鈕。

弱點監控

如果將 Kaspersky Endpoint Security 安裝在執行 Microsoft Windows for workstations 的電腦上，則可使用此元件。如果將 Kaspersky Endpoint Security 安裝在執行 Microsoft Windows for File Servers 的電腦上，則可使用此元件。

此區域包含有關弱點監控和如何啟用和停用此元件的說明。

關於弱點監控

“弱點監控”元件對使用者電腦上執行的應用程式進行即時弱點掃描，並在應用程式啟動時也執行即時弱點掃描。啟用“弱點監控”元件後，您無需再啟動“弱點掃描”工作。如果尚未對使用者電腦上安裝的應用程式進行掃描或很長時間沒有進行掃描，則該掃描與“[弱點掃描工作](#)”相關。





啟用和停用弱點監控

預設情況下已啟動弱點監控元件。您可以在必要時停用弱點監控。

有兩種啟動或停用該元件的方式：

- 透過[應用程式主視窗](#)的“**防護和控制**”頁籤。
- 開啟[程式設定視窗](#)。

若要啟用或停用弱點監控，請在主應用程式視窗的“防護和控制”頁籤中執行以下操作：

1. 開啟“[程式主視窗](#)”。
2. 選擇“**防護和控制**”頁籤。
3. 點擊“**端點控制**”區域。
開啟“**端點控制**”區域。
4. 右鍵點選包含有關弱點監控元件的資訊的行以顯示右鍵選單。
系統將開啟一個用於選擇對該元件的操作功能表。
5. 請執行以下操作之一：
 - 要啟用弱點監控，請選取“**開始**”。
弱點監控左側顯示的元件狀態圖示  將變為圖示 。
 - 要停用弱點監控，請選取“**停止**”。
弱點監控左側顯示的元件狀態圖示  將變為圖示 。

若要從程式設定視窗中啟用或停用弱點監控，請執行以下操作：

1. 開啟[程式設定視窗](#)。

2. 在視窗左側的“端點控制”區域中，選取“弱點監控”。

在視窗右側，將顯示“弱點監控”元件的設定。

3. 在視窗右側，執行下列操作：

- 如果您希望 Kaspersky Endpoint Security 啟動電腦正在執行的應用程式的弱點掃描，或針對使用者所啟動的應用程式的弱點掃描，請選取“**啟用弱點監控**”核取方塊。
- 如果您不希望 Kaspersky Endpoint Security 啟動電腦正在執行的應用程式的弱點掃描，或針對使用者所啟動的應用程式的弱點掃描，請取消“**啟用弱點監控**”核取方塊。

4. 要儲存變更，請點擊“**儲存**”按鈕。

裝置控制

如果將 Kaspersky Endpoint Security 安裝在執行 Microsoft Windows for workstations 的電腦上，則可使用此元件。如果將 Kaspersky Endpoint Security 安裝在執行 [Microsoft Windows 以做檔案伺服器之用](#) 的電腦上，則此元件無法使用。

本章節介紹裝置控制的資訊，以及如何設定元件。

關於裝置控制

裝置控制透過限制使用者存取安裝在電腦上的裝置或與電腦連線的裝置，確保保密資料的安全，這些裝置包括：

- 資料儲存裝置（硬碟、卸除式磁碟、磁帶裝置、CD/DVD 磁碟機）
- 資料傳輸工具（數據機、外接式網路卡）
- 將資料轉換為實體的裝置（印表機）
- 連接介面（也簡稱“介面”），是指將裝置連接至電腦的介面（範例 USB、FireWire 和紅外線）

裝置控制透過套用 [裝置存取規則](#)（也稱為“存取規則”）和“[連接介面存取規則](#)”（也稱為“介面存取規則”）管理使用者對裝置的存取。

啟用和停用裝置控制

預設情況下將啟用裝置控制。您可以根據需要停用裝置控制。

有兩種啟動或停用該元件的方式：

- 透過 [應用程式主視窗](#) 的“**防護和控制**”頁籤。
- 開啟 [程式設定視窗](#)。

要啟用或停用網路攻擊防護，請在應用程式主視窗的“**防護和控制**”頁籤中執行以下操作：

1. 開啟“程式主視窗”。
2. 選擇“**防護和控制**”頁籤。
3. 點擊“**端點控制**”區域。
開啟“**端點控制**”區域。
4. 右鍵點擊裝置控制開啟元件相關資訊的右鍵選單。
系統將開啟一個用於選擇對該元件的操作功能表。
5. 請執行以下操作之一：
 - 要啟用裝置控制，請在功能表中選取“**開始**”。

- 要停用裝置控制，請在功能表中選取“**停止**”。

若要在程式設定視窗中啟用或停用裝置控制，請執行下列操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**端點控制**”區域中，選擇“**裝置控制**”。
在視窗右側，將顯示裝置控制元件的設定。
3. 請執行以下操作之一：
 - 如果要啟用裝置控制，請選取“**啟用裝置控制**”核取方塊。
 - 如果要停用裝置控制，請清除“**啟用裝置控制**”核取方塊。
4. 要儲存變更，請點擊“**儲存**”按鈕。

關於存取裝置和連接介面的規則

裝置存取規則是定義裝置控制元件以下功能的參數組合：

- 允許所選使用者和/或使用者的群組在特定時段存取特定類型的裝置。
您可以選取使用者和/或使用者的群組，並為它們建立裝置存取排程。
- 設定讀取儲存裝置內容的權限。
- 設定編輯儲存裝置內容的權限。

預設情況下，程式將在裝置控制元件分類中為所有裝置類型建立存取規則。所有使用者隨時對裝置進行完全存取，只要允許存取各種類型裝置的連接介面即可。

連接介面存取規則可允許或封鎖對連接介面的存取。

預設情況下，程式將為裝置控制元件分類中存在的所有連接介面建立允許存取的規則。

您不能建立或刪除裝置或連接介面存取規則，而只能編輯它們。

關於信任的裝置

*信任的裝置*是指在信任裝置設定中指定的使用者可隨時進行完全存取的裝置。

以下操作適用於信任的裝置：

- 將裝置新增至信任的裝置的清單。
- 變更允許存取信任的裝置的使用者和/或使用者的群組。
- 從信任的裝置的清單中刪除裝置。

如果您將一個裝置新增到信任的裝置的清單，並為該類型的裝置建立封鎖或限制存取的存取規則，Kaspersky Endpoint Security 會根據信任的裝置清單中是否存在該裝置來決定是否授權對該裝置的存取權限。信任的裝置清單中裝置存在情況的優先順序高於存取規則。

關於對裝置存取權限的決定標準

Kaspersky Endpoint Security 在使用者將裝置連接到電腦之後做出是否允許存取該裝置的決定。

關於對裝置存取權限的決定標準

編號	初始條件	在做出關於對裝置的存取權限的決定之前採取的步驟			對裝置存取權限的結果
		檢查該裝置是否包括在信任的裝置的清單中	根據存取規則測試對裝置的存取權限	根據匯流排存取規則測試對匯流排的存取權限	
1	該裝置不存在於裝置控制元件的裝置分類中。	未包括在信任的裝置的清單中。	沒有存取規則。	不接受掃描。	允許存取。
2	該裝置為信任裝置。	包括在信任的裝置的清單中。	不接受掃描。	不接受掃描。	允許存取。
3	允許存取裝置	未包括在信任的裝置的清單中。	允許存取。	不接受掃描。	允許存取。
4	對裝置的存取權限取決於匯流排。	未包括在信任的裝置的清單中。	存取權限取決於匯流排。	允許存取。	允許存取。
5	對裝置的存取權限取決於匯流排。	未包括在信任的裝置的清單中。	存取權限取決於匯流排。	封鎖存取。	封鎖存取。
6	允許存取裝置沒有匯流排存取規則。	未包括在信任的裝置的清單中。	允許存取。	沒有匯流排存取規則。	允許存取。
7	封鎖存取裝置。	未包括在信任的裝置的清單中。	封鎖存取。	不接受掃描。	封鎖存取。
8	找不到裝置存取規則或匯流排存取規則。	未包括在信任的裝置的清單中。	沒有存取規則。	沒有匯流排存取規則。	允許存取。
9	沒有裝置存取規則。	未包括在信任的裝置的清單中。	沒有存取規則。	允許存取。	允許存取。
10	沒有裝置存取規則。	未包括在信任的裝置	沒有存取規則。	封鎖存取。	封鎖存

		的清單中。			取。
--	--	-------	--	--	----

您可以在連接裝置之後編輯裝置存取規則。如果裝置已連接並且存取規則允許存取它，但是您稍後編輯了該存取規則並且封鎖存取，則 Kaspersky Endpoint Security 將在該裝置下一次被請求執行任何檔案操作（瀏覽資料夾樹狀目錄、讀取、寫入）時封鎖存取該裝置。沒有檔案系統的裝置僅在該裝置下一次連接時被封鎖。

如果已安裝有 Kaspersky Endpoint Security 的電腦上的使用者需要請求被錯誤封鎖的裝置的存取權限，則向該使用者傳送[請求存取說明](#)。

編輯裝置存取規則

根據裝置類型，您可以修改各種存取設定，例如接收裝置存取權限的使用者的清單、存取排程和存取黑名單/存取白名單。

若要編輯裝置存取規則，請執行下列操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點控制”區域中，選擇“裝置控制”。
在視窗右側，將顯示裝置控制元件的設定。
3. 在視窗右側，選擇“裝置類型”頁籤。
“裝置類型”頁籤包含裝置控制元件分類中包括的所有裝置的存取規則。
4. 選取您想要編輯的存取規則。
5. 點擊“編輯”按鈕。該按鈕僅可用於具有檔案系統的裝置類型。

開啟“設定裝置存取規則”視窗。

預設情況下，裝置存取規則授權所有使用者隨時存取指定類型裝置的最大權限。此類存取規則在“使用者和/或使用者群組”清單中包括“所有”群組。在“根據使用者群組選擇的存取排程所擁有的權限”表中包括“預設排程”的時間間隔，並且授權使用者對裝置執行任何操作的權限。

6. 若要編輯裝置存取規則的設定，請執行下列操作：
 - a. 從“使用者和/或使用者群組”清單中選取使用者和/或使用者群組。
要編輯“使用者和/或使用者群組”清單，請使用“新增”、“編輯”和“刪除”按鈕。
 - b. 在“根據使用者群組選擇的存取排程所擁有的權限”表中，設定選取的使用者和/或使用者群組存取裝置的排程。為此，請選取您想在要編輯的裝置存取規則中使用的裝置的存取排程名稱旁邊的核取方塊。
若要編輯裝置存取排程的清單，請使用“根據使用者群組選擇的存取排程所擁有的權限”表中的“建立”、“編輯”、“複製”和“刪除”按鈕。
 - c. 對於正在編輯的規則中所用裝置的每個存取排程，指定使用裝置時允許的操作。為此，請在“根據使用者群組選擇的存取排程所擁有的權限”表中，選取包含相關操作的名稱列中的核取方塊。
 - d. 點擊“確定”。

編輯了裝置存取規則的預設設定後，“裝置類型”標籤上的“存取”欄內的裝置類型的存取設定將變為“根據規則限制”值。

7. 要儲存變更，請點擊“儲存”按鈕。

在事件記錄中新增或排除記錄

事件記錄僅對執行卸除式磁碟上的檔案可用。

若要啟用或停用事件記錄，請執行下列操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點控制”區域中，選擇“裝置控制”。
- 在視窗右側，將顯示裝置控制元件的設定。
3. 在視窗右側，選擇“裝置類型”頁籤。
- “裝置類型”頁籤包含裝置控制元件分類中包括的所有裝置的存取規則。
4. 選取裝置表中的“卸除式磁碟機”。
- 表上方的“日誌記錄”按鈕將可用。
5. 點擊“日誌記錄”按鈕。
- 這會開啟“日誌記錄設定”視窗。
6. 請執行以下操作之一：
 - 如果您希望啟用記錄卸除式磁碟上的檔案刪除和寫入操作，請選取“啟用日誌記錄”核取方塊。
 - Kaspersky Endpoint Security 會將事件儲存在建立檔案中並傳送訊息至卡巴斯基安全管理中心管理伺服器，無論使用者是否在卸除式磁碟上寫入或刪除檔案。
 - 否則，清空“啟用日誌記錄”核取方塊。
7. 指定必須記錄的操作。若要進行操作，請執行下列操作之一：
 - 如果您希望 Kaspersky Endpoint Security 記錄所有事件，則選取“儲存所有檔案資訊”核取方塊。
 - 如果您希望 Kaspersky Endpoint Security 只記錄有關特定格式檔案的資訊，請在“檔案格式篩選”區域中選取相關檔案格式對應的核取方塊。
8. 指定必須記錄為事件的 Kaspersky Endpoint Security 使用者操作。為此，請參閱以下執行操作：
 - a. 在“使用者”區域，點擊“選取”按鈕。
 - Microsoft Windows 中將開啟“選取使用者或群組”視窗。
 - b. 指定或編輯使用者和使用者群組清單。
- “使用者”區域中指定的使用者在卸除式磁碟上寫入檔案或刪除檔案時，Kaspersky Endpoint Security 會將此類操作的資訊寫入事件記錄並將訊息傳送至卡巴斯基安全管理中心管理伺服器。
9. 在“日誌記錄設定”視窗中，點擊“確定”。
10. 要儲存變更，請點擊“儲存”按鈕。

您可以在卡斯基安全管理中心管理主控台中檢視移動磁碟機上與檔案關聯的事件，其位於**事件標籤**上**管理伺服器節點**的工作區中。要使事件顯示在本機 Kaspersky Endpoint Security 事件日誌中，您必須選擇“裝置控制”元件的[通知設定](#)中的**執行檔操作**核取方塊。

將 Wi-Fi 網路新增至受信任清單

您可以允許使用者連線至您認為安全的 Wi-Fi 網路，例如公司 Wi-Fi 網路。若要執行操作，您必須將該網路新增至受信任 Wi-Fi 網路清單。裝置控制將封鎖存取除受信任清單中指定的 Wi-Fi 網路之外的所有網路。

若要將 Wi-Fi 網路新增至受信任清單：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點控制”區域中，選擇“裝置控制”。
在視窗右側，將顯示裝置控制元件的設定。
3. 在視窗右側，選擇“裝置類型”頁籤。
“裝置類型”頁籤包含裝置控制元件分類中包括的所有裝置的存取規則。
4. 在“Wi-Fi”裝置對應的“存取”欄中，點擊右鍵開啟上下文功能表。
5. 選取“封鎖但不包括”選項。
6. 在裝置清單中，選取“Wi-Fi”並點擊“編輯”按鈕。
這會開啟“受信任 Wi-Fi 網路”視窗。
7. 點擊“新增”按鈕。
這會開啟“受信任 Wi-Fi 網路”視窗。
8. 在“受信任 Wi-Fi 網路”視窗中：
 - 在“網路名稱”欄位中，指定您要新增至受信任清單的 Wi-Fi 網路。
 - 在“身分驗證類型”下拉清單中，選取連線至受信任 Wi-Fi 網路時使用的身分驗證類型。
 - 在“加密類型”下拉清單中，選取用於確保受信任 Wi-Fi 網路流量安全的加密類型。
 - 在“備註”欄位中，您可以指定有關所新增 Wi-Fi 網路的任何資訊。

如果某個 Wi-Fi 網路的設定比對規則中指定的所有設定則其被認為受信任。

9. 在“受信任 Wi-Fi 網路”視窗中點擊“確定”。
10. 在“受信任的 Wi-Fi 網路”視窗中點擊“確定”。

編輯連接介面存取規則

若要編輯連接介面存取規則，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點控制”區域中，選擇“裝置控制”。
在視窗右側，將顯示裝置控制元件的設定。
3. 選取“**連接介面**”頁籤。
“**連接介面**”頁籤會顯示分類在裝置控制元件中的所有連接介面的存取規則。
4. 選取您要編輯的介面連接規則。
5. 可變更存取參數的值：
 - 要允許對連接介面的存取，請點擊“**存取**”列以開啟右鍵選單，然後選取“**允許**”。
 - 要封鎖對連接介面的存取，請點擊“**存取**”列以開啟右鍵選單，然後選取“**封鎖**”。
6. 要儲存變更，請點擊“**儲存**”按鈕。

對信任的裝置的操作

本章節介紹關於信任的裝置操作的資訊。

在應用程式介面中向信任清單新增裝置

預設情況下，在將裝置新增到信任的裝置清單中後，所有用戶端（“Everyone”使用者群組）都被授權存取該裝置的權限。

若要在應用程式介面中向信任清單新增裝置，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點控制”區域中，選擇“裝置控制”。
在視窗右側，將顯示裝置控制元件的設定。
3. 在視窗右側，選擇“**信任的裝置**”頁籤。
4. 點擊“**選取**”按鈕。
“**選取信任的裝置**”視窗將開啟。
5. 選取您想要新增到信任的裝置清單中的裝置名稱旁邊的核取方塊。
“**裝置**”列中顯示的清單項目取決於在“**顯示已連接的裝置**”下拉清單中選取的值。
6. 點擊“**選取**”按鈕。
將開啟 Microsoft Windows 中的“**選擇使用者或群組**”視窗。
7. 在 Microsoft Windows 中的“**選取使用者或群組**”視窗中，指定 Kaspersky Endpoint Security 為其將選定裝置識別為信任的裝置的使用者和/或使用者群組。

在 Microsoft Windows 的“**選取使用者和/或使用者群組**”視窗中指定的使用者和/或使用者群組的名稱顯示在“**允許使用者和/或使用者群組存取**”欄位中。

8. 在“**選取信任的裝置**”視窗中，點擊“**確定**”。

在“**裝置控制**”元件設定視窗的“**信任的裝置**”頁籤，其中將會顯示新增的信任的裝置參數（“裝置”和“使用者”）。

9. 對於您想要為指定使用者和/或使用者群組新增到信任的裝置清單中的每個裝置，重複執行步驟 4–7。

10. 要儲存變更，請點擊“**儲存**”按鈕。

基於裝置型號或 ID 將裝置新增至信任清單

預設情況下，在將裝置新增到信任的裝置清單中後，所有用戶端（“Everyone”使用者群組）都被授權存取該裝置的權限。

若要基於裝置型號或 ID 將裝置新增至信任清單，請執行以下操作：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄中的“**受管裝置**”資料夾下，開啟您希望為其建立信任群組清單的管理員同名資料夾。
3. 在工作區選擇“**政策**”頁籤。
4. 選擇所需政策。
5. 使用以下方式開啟“**內容: <政策名稱>**”視窗：
 - 在所選定項目右鍵選單中，選擇“**內容**”。
 - 點擊位於管理主控台工作區右側的“**設定政策**”連線。
6. 在“**端點控制**”區域中，選取“**裝置控制**”子區域。
7. 在視窗右側，選擇“**信任的裝置**”頁籤。
8. 點擊“**新增**”按鈕。

系統將開啟該按鈕的右鍵功能表。
9. 在“**新增**”按鈕的右鍵功能表中，執行下列操作之一：
 - 如果您要將帶有已知唯一 ID 的裝置新增至受信裝置清單中，則選取“**透過 ID 選取裝置**”按鈕。
 - 選取“**按型號選取裝置**”項新增其 VID（供應商 ID）和 PID（產品 ID）已知的信任裝置的清單。
10. 在開啟的視窗中，在“**裝置類型**”下拉清單中選取要在下表中顯示的裝置類型。
11. 點擊 **重新整理** 按鈕。

該表將顯示其裝置 ID 和/或型號已知且屬於“**裝置類型**”下拉清單中選定類型的裝置清單。
12. 選取您想要新增到信任的裝置清單中的裝置名稱旁邊的核取方塊。
13. 點擊“**選取**”按鈕。

將開啟 Microsoft Windows 中的“選擇使用者或群組”視窗。

14. 在 Microsoft Windows 中的“選取使用者或群組”視窗中，指定 Kaspersky Endpoint Security 為其將選定裝置識別為信任的裝置的使用者和/或使用群組。

在 Microsoft Windows 的“選取使用者和/或使用群組”視窗中指定的使用者和/或使用群組的名稱顯示在“允許使用者和/或使用群組存取”欄位中。

15. 點擊“確定”。

“信任的裝置”頁籤的清單中將顯示新增了信任裝置參數的行。

16. 點擊“確定”或“套用”儲存變更。

基於裝置 ID 遮罩將裝置新增至信任清單

預設情況下，在將裝置新增到信任的裝置清單中後，所有用戶端（“Everyone”使用者群組）都被授權存取該裝置的權限。

只可以在卡巴斯基安全管理中心管理主控台中根據裝置 ID 遮罩將裝置新增至受信任清單。

要根據裝置 ID 遮罩將裝置新增至信任清單，請執行以下操作：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄中的“受管裝置”資料夾下，開啟您希望為其建立信任群組清單的管理員同名資料夾。
3. 在工作區選擇“政策”頁籤。
4. 選擇所需政策。
5. 使用以下方式開啟“內容: <政策名稱>”視窗：
 - 在所選定項目右鍵選單中，選擇“內容”。
 - 點擊位於管理主控台工作區右側的“設定政策”連線。
6. 在“端點控制”區域中，選取“裝置控制”子區域。
7. 在視窗右側，選擇“信任的裝置”頁籤。
8. 點擊“新增”按鈕。

系統將開啟該按鈕的右鍵功能表。
9. 在“新增”按鈕的右鍵功能表中，選取“透過裝置 ID 遮罩”。
- “透過 ID 遮罩新增信任的裝置”視窗將開啟。
10. 在“透過 ID 遮罩新增信任的裝置”視窗中，在“遮罩”欄位中輸入裝置 ID 遮罩。
11. 點擊“選取”按鈕。

將開啟 Microsoft Windows 中的“選擇使用者或群組”視窗。

12. 在 Microsoft Windows 中的“**選取使用者或群組**”視窗中，指定 Kaspersky Endpoint Security 會將其型號或 ID 匹配指定遮罩的識別為受信裝置。

在 Microsoft Windows 的“**選取使用者和/或使用者群組**”視窗中指定的使用者和/或使用者群組的名稱顯示在“**允許使用者和/或使用者群組存取**”欄位中。

13. 點擊“**確定**”。

在“**裝置控制**”元件設定視窗中的“**信任的裝置**”頁籤中，某行中將顯示將裝置安裝 ID 遮罩新增至信任的裝置清單的規則設定。

14. 要儲存變更，請點擊“**儲存**”按鈕。

設定使用者對信任的裝置的存取權限

預設情況下，在將裝置新增到信任的裝置清單中後，所有用戶端（“**Everyone**”使用者群組）都被授權存取該裝置的權限。您可以設定使用者（或使用者群組）對信任的裝置的存取。

若要設定使用者對信任的裝置的存取權限：

1. 開啟[程式設定視窗](#)。

2. 在視窗左側的“**端點控制**”區域中，選擇“**裝置控制**”。

在視窗右側，將顯示裝置控制元件的設定。

3. 在視窗右側，選擇“**信任的裝置**”頁籤。

4. 從信任的裝置的清單中，選取您想要編輯其存取規則的裝置。

5. 點擊“**編輯**”按鈕。

開啟“**設定信任的裝置存取規則**”視窗。

6. 點擊“**選取**”按鈕。

將開啟 Microsoft Windows 中的“**選擇使用者或群組**”視窗。

7. 在 Microsoft Windows 中的“**選取使用者或群組**”視窗中，指定 Kaspersky Endpoint Security 為其將選定裝置識別為信任的裝置的使用者和/或使用者群組。

8. 點擊“**確定**”。

在 Microsoft Windows 的“**選取使用者和/或使用者群組**”視窗中指定的使用者和/或使用者群組的名稱顯示在“**設定信任的裝置存取規則**”視窗的“**允許使用者和/或使用者群組存取**”欄位中。

9. 點擊“**確定**”。

10. 要儲存變更，請點擊“**儲存**”按鈕。

從信任裝置的清單中刪除裝置

若要從受信裝置清單中刪除裝置，請執行以下操作：

1. 開啟[程式設定視窗](#)。

2. 在視窗左側的“端點控制”區域中，選擇“裝置控制”。
- 在視窗右側，將顯示裝置控制元件的設定。
3. 在視窗右側，選擇“信任的裝置”頁籤。
4. 選取要從信任的裝置清單中刪除的裝置。
5. 點擊“刪除”按鈕。
6. 要儲存變更，請點擊“儲存”按鈕。

Kaspersky Endpoint Security 會根據裝置存取規則和連接介面存取規則，確定您已從信任的裝置清單中刪除裝置的存取權限。

編輯裝置控制訊息範本

當使用者嘗試存取被封鎖的裝置時，Kaspersky Endpoint Security 會顯示一條訊息，說明對該裝置的存取被封鎖，或封鎖對該裝置內容的操作。如果使用者相信對裝置的存取被錯誤地封鎖了，或者對裝置內容的操作被錯誤封鎖了，使用者可以透過點擊被封鎖操作顯示訊息中的連結向公司區域網路管理員傳送訊息。

使用者可以使用範本來撰寫關於封鎖存取裝置或封鎖對裝置內容執行操作的訊息以及傳送給管理員的回報訊息。您可以修改訊息範本。

若要編輯裝置控制訊息範本，請執行下列操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點控制”區域中，選擇“裝置控制”。
- 在視窗右側，將顯示裝置控制元件的設定。
3. 在視窗右側，點擊“範本”按鈕。
- 開啟“範本”視窗。
4. 請執行以下操作之一：
 - 要修改關於封鎖存取裝置或封鎖對裝置內容執行操作的訊息的範本，請選取“封鎖”頁籤。
 - 要修改傳送給區域網路管理員的回報訊息的範本，請選取“傳送給管理員的資訊”頁籤。
5. 編輯資訊範本。您也可以使用以下按鈕：變數、預設值和連結（該按鈕僅在“封鎖”標籤上可用。）
6. 點擊“確定”。
7. 要儲存變更，請點擊“儲存”按鈕。

獲得存取被封鎖裝置的權限

這些說明的目標讀者是用戶端電腦上安裝有 Kaspersky Endpoint Security 的使用者。

僅當 Kaspersky Endpoint Security 根據卡巴斯基安全管理中心的政策操作時，Kaspersky Endpoint Security 授權存取裝置權限的功能才能使用（請參閱 *卡巴斯基安全管理中心管理手冊*）。

若要從裝置控制元件設定視窗中請求存取被封鎖裝置的權限，請執行下列操作：

1. 在主應用程式視窗中，選取“**防護和控制**”頁籤。
2. 點擊“**端點控制**”區域。
開啟“**端點控制**”區域。
3. 右鍵點擊裝置控制開啟元件相關資訊的右鍵選單。
系統將開啟一個用於選擇對該元件的操作功能表。
4. 點擊“**存取裝置**”按鈕。
開啟“**臨時存取裝置**”視窗。
5. 從已連線的裝置清單中，選取您想要取得其存取權限的裝置。
6. 點擊“**產生請求存取檔案**”按鈕。
這將開啟“**建立請求存取檔案**”視窗。
7. 在“**存取持續時間**”欄位中，指定您想要存取裝置的時長。
8. 點擊**儲存** 按鈕。
Microsoft Windows 的標準“**儲存請求存取檔案**”視窗將開啟。
9. 在 Microsoft Windows 的“**儲存請求存取檔案**”視窗中，選取您需要儲存包含裝置存取檔案的資料夾，然後點選“**儲存**”按鈕。
10. 將該裝置請求存取檔案傳送給區域網路管理員。
11. 接收來自區域網路管理員的裝置存取金鑰檔案。
12. 在“**臨時存取裝置**”視窗中，點擊“**啟用存取金鑰**”按鈕。
Microsoft Windows 的標準“**開啟存取金鑰**”視窗將開啟。
13. 在 Microsoft Windows 的“**開啟存取金鑰**”視窗中，選取從區域網路管理員那裡收到的裝置存取金鑰檔案，然後點選“**開啟**”。
“**啟動裝置存取金鑰**”視窗將開啟，並且顯示關於所提供的存取權限的資訊。
14. 在“**啟動裝置存取金鑰**”視窗中，點擊“**確定**”。

要透過通知裝置被封鎖的資訊中的連結來請求存取被封鎖裝置的權限，請執行下列操作：

1. 在包含通知裝置或連接介面被封鎖的資訊視窗中，點擊“**請求存取**”連結。
這將開啟“**建立請求存取檔案**”視窗。
2. 在“**存取持續時間**”欄位中，指定您想要存取裝置的時長。
3. 點擊**儲存** 按鈕。
Microsoft Windows 的標準“**儲存請求存取檔案**”視窗將開啟。

4. 在 Microsoft Windows 的“**儲存請求存取檔案**”視窗中，選取您需要儲存包含裝置存取檔案的資料夾，然後點選“**儲存**”按鈕。
5. 將該裝置請求存取檔案傳送給區域網路管理員。
6. 接收來自區域網路管理員的裝置存取金鑰檔案。
7. 在“**臨時存取裝置**”視窗中，點選“**啟用存取金鑰**”按鈕。
Microsoft Windows 的標準“**開啟存取金鑰**”視窗將開啟。
8. 在 Microsoft Windows 的“**開啟存取金鑰**”視窗中，選取從區域網路管理員那裡收到的裝置存取金鑰檔案，然後點選“**開啟**”。
- “**啟動裝置存取金鑰**”視窗將開啟，並且顯示關於所提供的存取權限的資訊。
9. 在“**啟動裝置存取金鑰**”視窗中，點選“**確定**”。

當對裝置的存取被授予多項的時間週期時，可能會與您設定時間有所不同。授權裝置控制的期限由區域網路管理員在產生裝置存取密碼時指定。

使用卡巴斯基安全管理中心建立存取被封鎖裝置的金鑰

要授予使用者臨時存取被封鎖裝置的權限，需要裝置存取金鑰。您可以使用卡巴斯基安全管理中心建立存取金鑰。

若要建立被封鎖裝置的存取金鑰：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在主控台樹狀目錄的“**受管裝置**”資料夾中，開啟相關用戶端電腦所屬的管理群組名稱的資料夾。
3. 在工作區選取“**裝置**”頁籤。
4. 在用戶端電腦清單中，選取其使用者需要取得裝置臨時存取權限的電腦。
5. 在用戶端電腦的右鍵選單中選取在“**允許離線模式下存取裝置和資料**”。
- 開啟“**允許離線模式下存取裝置和資料**”視窗。
6. 選取“**裝置控制**”頁籤。
7. 在“**裝置控制**”頁籤上點選“**瀏覽**”按鈕。
Microsoft Windows 的標準“**選擇要求存取檔案**”視窗將開啟。
8. 在“**選取請求存取金鑰**”視窗中，選取您從使用者那裡收到的存取金鑰，然後點選“**開啟**”按鈕。
在“**裝置控制**”顯示對於其使用者請求存取封鎖裝置的詳細資料。
9. 指定“**存取持續時間**”設定的值。
您授予使用者裝置存取權限的時間長度。預設值與使用者在建立請求存取金鑰時指定的值相同。
10. 指定“**啟用時間範圍**”設定的值。
定義使用者可透過使用提供的啟用代碼啟用被封鎖裝置存取權限的時間範圍。

11. 點擊**儲存** 按鈕。

Microsoft Windows 的標準**“儲存存取金鑰”**視窗將開啟。

12. 選取您想要儲存包含被封鎖裝置存取金鑰的檔案目標資料夾。

13. 點擊**儲存** 按鈕。

網頁控制

如果將 Kaspersky Endpoint Security 安裝在執行 Microsoft Windows for workstations 的電腦上，則可使用此元件。如果將 Kaspersky Endpoint Security 安裝在執行 [Microsoft Windows 以做檔案伺服器之用](#) 的電腦上，則此元件無法使用。

本章節包含有關 Web 控制的資訊，以及有關如何配置元件設定的說明。

關於網頁控制

網頁控制透過限制或封鎖存取網頁資源來控制使用者在區域網路中的操作。

網路資源是單個網頁或多個網頁，或是一個網站或多個具有共同特性的網站。

網頁控制提供以下選項：

- 節省流量。
它透過限制或封鎖多媒體檔案的下載、或限制封鎖與使用者工作職責無關的網頁資源存取來控制流量。
- 根據網頁資源的內容類別限制存取。
為了節省流量並減少由於員工不正確使用而造成的潛在流量損失，您可以限制或封鎖對特定網頁資源類別的存取（例如，封鎖存取屬於“網際網路溝通媒體”類別的網頁資源）。
- 集中控制對網頁資源的存取。
當使用卡巴斯基安全管理中心時，對存取網頁資源的個人和群組的設定可使用。

所有套用到網頁資源存取權限的限制和封鎖都將實施為[網路資源存取規則](#)。

啟動和停用網頁控制

預設情況下將啟用網頁控制。您可以根據需要停用網頁控制。

有兩種啟動或停用該元件的方式：

- 透過[應用程式主視窗](#)的“防護和控制”頁籤。
- 開啟[程式設定視窗](#)。

要啟用或停用網頁控制，請在應用程式主視窗的“**防護和控制**”頁籤中執行以下操作：

1. 開啟“程式主視窗”。
2. 選擇“**防護和控制**”頁籤。
3. 點擊“**端點控制**”區域。
開啟“**端點控制**”區域。

4. 右鍵點擊網頁控制開啟元件相關資訊的右鍵選單。
系統將開啟一個用於選擇對該元件的操作功能表。
5. 請執行以下操作之一：
 - 要啟用網頁控制，請在功能表中選取“**啟動**”。
 - 要停用網頁控制，請在功能表中選取“**停止**”。

若要在程式設定視窗中啟用或停用網頁控制，請執行下列操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**端點控制**”區域中，選取“**網頁控制**”子區域。
在視窗右側，將顯示網頁控制元件的設定。
3. 請執行以下操作之一：
 - 如果要啟用網頁控制，請選取“**啟用網頁控制**”核取方塊。
 - 如果要停用網頁控制，請取消“**啟用網頁控制**”核取方塊。

如果網頁控制被停用，則 Kaspersky Endpoint Security 不會控制對網頁資源的存取。

4. 要儲存變更，請點擊“**儲存**”按鈕。

網頁資源內容類別

下列網頁資源類別均已選定，以便更完整的透過功能和主題來敘述網頁資源封鎖資料內容類別（以下簡稱“類別”）封鎖資料。清單中的資源顯示順序並不反應網際網路中這些類別的相關重要性和普及性。類別名稱是臨時的，只用於 Kaspersky Lab 產品和網站。這些名稱並不一定反映法律所指的含義。一個網頁資源可以分屬多個不同類別。

色情

此類別包含下列類型的網頁資源：

- 包含描繪人類生殖器或人形生物、人類性交或人類自我刺激行為的照片或視頻材料的任何網頁資源。
- 包含描繪人類生殖器或人形生物、人類性交或人類自我刺激行為的文字材料的網頁資源。
- 用於討論人類性關係的網頁資源。

與網際網路傳媒類別重疊

- 包含色情材料、實際描繪人類性行為的作品，或旨在刺激性興奮的藝術作品的網頁資源。
- 既定目標且具有包含性關係內容的特殊部分和/或單個文章的官方媒體和線上社區網頁資源。
- 包含性變態內容的網頁資源。

- 宣傳和出售用於性和刺激性沖動、性服務和親密約會（包含透過色情視訊聊天提供線上服務、“電話性愛”、“性簡訊”（“虛擬性”）提供的服務）的網頁資源。
- 具有以下內容的 Web 資源：
 - 包含科學和熱門主題的性教育的文章和網誌。
 - 醫學百科全書，特別是關於有性生殖的部分。
 - 醫療機構的資源，特別是涉及性器官治療的部分。

軟體、音樂、影片

此類別包括您可以單獨選取的以下子類別：

- **音訊和視訊。**
此子類別包括用於分發音樂和視頻資料的網頁資源：電影、體育廣播錄音錄像、音樂會錄音錄像、歌曲、電影剪輯、視頻、音頻和視訊教程錄音錄像等。
- **下載種子。**
此類別包括用於共用無限大小的檔案種子的網站。
- **檔案共用。**
此子類別包括檔案共用網站，與分發檔案的實際位置無關。

酒精、煙草、毒品

此類別包含內容與酒精或酒精產品、煙草製品、麻醉、精神和/或毒品直接或間接相關的網頁資源。

- 宣傳和銷售這類物質和這類物質消費用品的網頁資源。

與“電子商務”類別重疊

- 具有如何消費和生產麻醉、精神和/或毒品物質說明的網頁資源。

此類包含關於科學和醫療主題的網頁資源。

暴力

此類包含敘述對人類或動物進行殘忍對待的物理或心理暴力行為的任何照片、視頻或文字材料。

- 帶有對處決、折磨或虐待，以及相關工具進行描繪或說明的網頁資源。

與“武器、爆炸物和煙火”類別重疊。

- 包含對人、動物或虛擬生物進行虐待或羞辱的謀殺、戰鬥、毆打或強姦場景進行描繪和說明的網頁資源。

- 包含煽動生命冒險和/或死亡冒險（包括自我傷害或自殺）行為資訊的網頁資源。
- 包含對人或動物進行或煽動暴力和/或虐待行為資訊的網頁資源。
- 包含對戰爭受害者和戰爭暴行、武裝衝突、事故、災難、自然災害、工業或社會災難或人類痛苦進行真實敘述的網頁資源。
- 包含暴力和虐待（包括所謂的“槍手”、“打鬥”、“槍械”等）場景的瀏覽器電腦遊戲。

與“電腦遊戲”類別重疊。

武器、爆藥、煙火

此類別包含帶有武器、爆炸和煙火產品資訊的網頁資源：

- 武器、爆炸物和煙火產品製造商和商店的網站。

與“電子商務”類別重疊

- 關於製造或使用武器、爆炸物和焰火產品的網頁資源。
- 包含針對武器、爆炸物和煙火產品進行分析、歷史介紹、製造和百科全書式資料介紹的網頁資源。

“武器”是指旨在傷害人類和動物的生命或健康和/或損壞製造和結構的裝置、物品和方法。

不雅詞彙

此類別包含發現具有污穢語言的網頁資源。

與“色情內容”類別重疊。

此類別還包含帶有以褻瀆為研究主題的語言和語言學材料的網頁資源。

賭博、彩票、抽獎

此類別包含為使用者提供賭博參與（即使這樣的參與並不是存取網頁的強制性條件）機會的網頁資源。此類別包含提供下列內容的網頁資源：

- 要求參與者使用金錢的賭博。

與“電腦遊戲”類別重疊。

- 涉及賭錢的賭博比賽。

- 涉及購買獎券或號碼的彩票。
- 可引起參與賭博、抽獎或彩票的資訊。

與“電子商務”類別重疊

此類別包含那些以提供免費參與作為獨立模式的網頁資源，以及對未進入本類別的使用者進行積極宣傳的網頁資源。

網路通信

此類別包含促使使用者（註冊使用者或未註冊使用者）在特定情況下將個人資訊傳送至相關網頁資源或其他線上服務的其他使用者，以及/或者將內容（公開內容或限制內容）傳送至相關網頁資源的網頁資源。您可以單獨選取以下子類別：

- **聊天和論壇。**
此子類別包括用於使用特殊網頁程式公共討論各種主旨的網頁資源，以及啟用了即時溝通用於分發或支援即時通訊的應用程式。
- **網誌。**
此子類別包括了網誌平台，包括了收費或免費提供建立和維護網誌服務的網站。
- **社群網路。**
此子類別包括各種旨在建立、組織和政府之間聯絡人的網站（需要註冊使用者帳戶作為參與條件）。
- **約會網站。**
此子類別包括收費或免費提供各種社交網路服務的網頁資源。

與“色情內容”和“電子商務”類別重疊。

- **基於 Web 的郵件。**
此子類別包含電子郵件和相關資料（如個人聯絡人）的電子郵件服務和郵箱頁面的專門登入頁面。此類別不包含提供電子郵件服務的網際網路服務供應商的其他頁面。

電子零售商、銀行和支付系統

此類別包含設計用於使用特定網頁應用程式進行非現金貨幣線上交易的網頁資源。您可以單獨選取以下子類別：

- **購物和拍賣。**
此子類別包括用於銷售任何商品、工作或服務的個人和/或法律實體的線上商店和線上拍賣商店，包括專門的顯示商店網站和接受線上支付的實體商店的網站。
- **銀行。**
此子類別包含具有網上銀行功能的專門的銀行網頁，包括銀行帳戶之間的（電子）轉帳、銀行存款、貨幣兌換、協力廠商服務支付等。
- **支付系統。**

此子類別包含提供使用者個人帳戶存取電子貨幣系統的網頁。

從技術角度來說，支付可影響任何類型的金融卡（實際卡或虛擬卡、借記卡或信用卡、本國或國際）和電子貨幣。無論網路資源是否在 SSL 協議上進行資料傳輸和使用 3D 安全身分驗證等技術，均屬於此類別。

求職網站

此類別包括旨在匯聚僱主和求職者的網頁資源：

- 個人求職機構（職業介紹所和/或獵頭機構）網站。
- 僱主提供職位空缺並介紹其優勢的網站。
- 僱主和招聘機構提供職位空缺的獨立網站。
- 可發佈或檢視並不積極尋求就業的專業人員資訊的專業社群網路。

與網際網路傳媒類別重疊

匿名存取系統

此類別包括使用特定網頁應用程式下載其他網頁資源作為中介的網頁資源，其目的為：

- 繞過網域網路對網頁位址或 IP 位址的限制；
- 匿名存取網頁資源，包括專門拒絕來自特定 IP 位址或位址群組（例如以所在國分組的 IP 位址）的 HTTP 請求的網頁資源。

此類別包括具有特定目的的上述網頁資源（“匿名網站”）和技術上具有類似功能的網頁資源。

休閒遊戲

此類別包括包含各類風格電腦遊戲的網頁資源：

- 電腦遊戲開發商網站。
- 用於討論電腦遊戲的網頁資源。

與網際網路傳媒類別重疊

- 能夠提供線上參與遊戲的技術功能（可讓參與者與其他參與者一起或單獨進行遊戲），可本機安裝應用程式或無需安裝（“瀏覽器遊戲”）的網頁資源。
- 旨在宣傳、分發和支援遊戲軟體的網頁資源。

宗教活動

此類別包含帶有宗教意識形態和/或任何形式崇拜的公共活動、協會和組織的材料的網頁資源。

- 不同等級的宗教組織官方網站，從國際宗教到本機宗教社團均包含在內。
- 從主流宗教協會或社團分離出來的未登記的宗教組織和社團的網站。
- 獨立於傳統宗教活動的宗教組織和社團（包括在某個特定創始人的倡議下獨立的宗教組織和社團）的網站。
- 追求不同傳統宗教間合作的相互認同的組織的網站。
- 帶有學術、歷史和宗教主題的各種材料的網頁資源。
- 詳細描繪或敘述宗教崇拜（包括儀式和涉及神、造物主和/或具有超自然力量物品的崇拜儀式）的網頁資源。

新聞媒體

此類別包含具有主流媒體或（讓使用者自行新增其新聞報道的）網路發佈網站所建立的公開新聞內容的網頁資源。

- 官方媒體網站。
- 提供官方來源資訊服務的網站。
- 提供從各種官方和非官方新聞資訊匯聚服務的網站。
- 使用者自身（“社群新聞網站”）建立新聞內容的網站。

廣告欄

此類別包含帶有廣告欄的網頁資源：廣告欄上的廣告資訊可能會在使用者活動時分散他們的注意力，同時廣告下載會新增下載流量。

關於網路資源存取規則

網路資源存取規則是使用者在規則排程中指定的時間範圍內存取規則中描述的網頁資源時，Kaspersky Endpoint Security 執行的一組篩選和操作。透過篩選，您可以精確指定由網頁控制元件控制其存取權限的網頁資源。

系統提供以下篩選功能選項：

- **按內容篩選**。網頁控制將按照[內容和資料類型分類網頁資源](#)。您可以按特定類別的內容和資料類型控制使用者對網頁資源的存取權限。使用者存取屬於選取內容類別和/或資料類型類別的網頁資源時，Kaspersky Endpoint Security 會執行規則中指定的操作。

- **按網頁資源位址篩選**。您可以控制使用者對所有網頁資源位址或單個網頁資源位址和/或網頁資源位址群組的存取權限。

如果指定按內容篩選和按網頁資源位址篩選，而指定的網頁資源位址和/或網頁資源位址群組屬於選取的內容類別或資料類型類別，Kaspersky Endpoint Security 不會控制對選取內容類別和/或資料類型類別中所有網頁資源的存取權限。相反，應用程式僅控制對指定網頁資源位址和/或網頁資源位址群組的存取權限。

- **按名稱篩選**。您可以指定可存取根據規則控制的網頁資源使用者和/或使用者群組的名稱。
- **規則排程**。您可以指定下列規則排程。規則排程為 Kaspersky Endpoint Security 監控對該規則涵蓋網路資源的存取時間範圍。

安裝 Kaspersky Endpoint Security 後，網頁端點控制模組的規則清單將不為空白。該清單中存在兩個規則：

- “方案和式樣表”規則，該規則授權所有使用者在任何時間都可存取其位址包含檔案名稱具有 css、js 或 vbs 副檔名的網頁資源。例如，<http://www.example.com/style.css>、<http://www.example.com/style.css?mode=normal>。
- “預設”規則，該規則授權所有使用者在任何時候存取任何網頁資源。

網路資源存取規則操作

您可以對網路資源存取規則執行下列操作：

- 新增新規則
- 編輯規則
- 為規則分配優先順序

某個規則的優先順序按照網頁控制元件設定視窗中存取規則表中此規則簡要說明行所在的位置決定。這表示在存取規則表中位置較高的規則擁有較高的優先順序。

如果使用者嘗試存取的網路資源與多個規則的參數相符，則 Kaspersky Endpoint Security 會按照擁有最高優先順序的規則執行操作。

- 測試規則。

您可以使用規則診斷功能檢查規則的一致性。

- 啟用和停用規則。

可以啟用（執行狀態：*開*）或停用（執行狀態：*關*）網路資源存取規則。預設情況下，建立規則之後，此規則已被啟用（操作狀態：*開啟*）。您可以停用此規則。

- 刪除規則

新增和編輯網頁存取規則

若要新增或編輯網路資源存取規則，請執行下列操作

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點控制”區域中，選取“網頁控制”子區域。

在視窗右側，將顯示網頁控制元件的設定。

3. 請執行以下操作之一：

- 要新增規則，請點擊**“新增”**按鈕。
- 如果您希望編輯規則，選取表中的規則並點擊**“編輯”**按鈕。

開啟 **按存取規則的優先排序** 視窗。

4. 指定或編輯規則的設定。為此，請參閱以下執行操作：

a. 在**“名稱”**欄位中輸入或編輯規則的名稱。

b. 在**“篩選內容”**下拉清單中，選取需要的選項：

- **任何內容**。
- **根據內容類別**。
- **根據資料類型**。
- **根據內容類別和資料類型**。

c. 如果選定了**“任何內容”**之外的其它選項，則可以開啟用於選取內容類別和/或資料類型的選取視窗。選取所需內容類別和/或資料類型名稱旁邊的核取方塊。

選取某個內容類別和/或資料類型類別旁邊的核取方塊則表示 Kaspersky Endpoint Security 將套用規則以控制對屬於選取的內容類別和/或資料類型類別的網頁資源存取。

d. 在**“套用於位址”**下拉清單中，選取需要的選項：

- **套用至所有網址**。
- **套用至指定網址**。

e. 如果選取**“套用至指定網址”**選項，程式將開啟一個區域以供您建立網頁資源清單。您可以使用**“新增”**、**“編輯”**和**“刪除”**按鈕新增或編輯網頁資源位址。

f. 選取**“指定使用者和/或群組”**核取方塊。

g. 點擊**“選取”**按鈕。

將開啟 Microsoft Windows 中的**“選擇使用者或群組”**視窗。

h. 指定或編輯將允許或封鎖其存取此規則所敘述網頁資源的使用者和/或使用群組清單。

i. 在**“動作”**下拉清單中，選取需要的選項：

- **允許**，如果選取此值，Kaspersky Endpoint Security 將允許存取與此規則設定相符的網頁資源。
- **封鎖**，如果選取此值，Kaspersky Endpoint Security 將封鎖存取與此規則設定相符的網頁資源。
- **警告**。如果選定此值，Kaspersky Endpoint Security 將在使用者嘗試存取比對此規則的網頁資源時顯示此網頁內容令人不快的警告。透過使用警告訊息中的連結，使用者可取得請求的網頁資源存取權限。

j. 在**“規則排程”**下拉清單中，選取所需排程的名稱，或根據選取的規則排程產生新排程。為此，請參閱以下執行操作：

1. 在“規則排程”下拉清單中，點擊“設定”按鈕。
系統將開啟“規則排程”視窗。
2. 要用規則不適用的時間跨度新增此規則排程，請在顯示規則排程的表格中，點擊與您想要選取的時間和星期幾對應的表格單元。
這些儲存格的顏色將變為灰色。
3. 要將此規則適用的時間跨度替換為此規則不適用的時間跨度，請點擊與您想要選取的時間和星期幾對應的灰色表格單元。
這些單元的顏色將變為綠色。
4. 點擊“另存為”按鈕。
開啟“規則排程名稱”視窗。
5. 鍵入規則排程名稱或保留建議的預設名稱。
6. 點擊“確定”。

5. 在“網頁存取規則”視窗，點擊“確定”。

6. 要儲存變更，請點擊“儲存”按鈕。

為網頁存取規則分配優先順序

您可以為規則清單中的每個規則分配優先順序，方法是按照某種順序排列這些規則。

要為網路資源存取規則分配優先順序，請執行下列操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點控制”區域中，選取“網頁控制”子區域。
在視窗右側，將顯示網頁控制元件的設定。
3. 在視窗右側，選取您想要變更其優先順序的規則。
4. 使用 **上移** 和 **下移** 按鈕將該規則移至規則清單中所需的排名。
5. 對於您想要變更其優先順序的所有規則，重複執行步驟 3-4。
6. 要儲存變更，請點擊“儲存”按鈕。

測試網頁存取規則

要檢查網頁控制規則的一致性，您可以測試它們。為此，網頁控制元件包括了規則診斷功能。

要測試網路資源存取規則，請執行下列操作：

1. 開啟[程式設定視窗](#)。

2. 在視窗左側的“端點控制”區域中，選取“網頁控制”子區域。

在視窗右側，將顯示網頁控制元件的設定。

3. 在視窗右側，點擊“診斷”按鈕。

系統將開啟“規則診斷”視窗。

4. 填寫“條件”區域中的欄位：

- a. 如果您想要測試 Kaspersky Endpoint Security 用於控制特定網頁資源存取權限的規則，請選取“指定的網址”核取方塊。然後在下面的欄位中輸入網頁資源的位址。
- b. 如果您想要測試 Kaspersky Endpoint Security 用於為指定使用者和/或使用者群組控制網頁資源存取權限的規則，請指定使用者和/或使用者群組清單。
- c. 如果您想要測試 Kaspersky Endpoint Security 用於控制指定內容類別和/或資料類型類別的網頁資源存取權限的規則“篩選內容”下拉式選單，選取需要的選項（“根據內容類別”，“根據資料類型”，或“根據內容類別和資料類型”）。
- d. 如果您要在測試規則時考慮嘗試存取規則診斷條件中指定的網頁資源的時間和星期幾，請選取“測試規則的時間”核取方塊。然後，請指定星期幾和時間。

5. 點擊“測試”按鈕。

測試完成後將顯示一條訊息，其中包含關於 Kaspersky Endpoint Security 採取的操作（允許、封鎖或警告）的資訊，該操作是程式根據存取指定網路資源的嘗試所觸發的第一個規則而採取的。要觸發的第一個規則是在網頁控制規則清單中具有比其他滿足診斷條件的規則更高排名的規則。該訊息顯示在“測試”按鈕的右側。下表包含 Kaspersky Endpoint Security 根據其優先順序低於所觸發的第一個規則的規則而採取的操作的相關資訊。規則點擊降優先順序列出。

啟動和停用網頁存取規則

若要啟用或停用網路資源存取規則，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點控制”區域中，選取“網頁控制”子區域。
在視窗右側，將顯示網頁控制元件的設定。
3. 在視窗右側，選取要啟用或停用的規則。
4. 在 **狀態** 列中，執行以下操作：
 - 如果要啟用規則，請選取“*開啟*”值。
 - 如果要停用規則，請選取“*關閉*”值。
5. 要儲存變更，請點擊“儲存”按鈕。

從舊版本應用程式遷移網頁資源存取規則

當 Service Pack 1 Maintenance Release 1 或更早版本應用程式升級至 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 時，基於網頁內容類別的網頁資源控制規則將按照下列政策進行移轉：

- 來自“論壇和聊天”、“網頁郵件”和“社群網路”清單的基於一個或多個網頁資源內容的網路資源存取規則將轉換至“網際網路傳媒”網頁資源內容類別。
- 來自“電子商店”和“支付系統”清單的基於一個或多個網頁資源內容類別的網路資源存取規則將移轉至“電子商務”網頁資源內容類別。
- 基於“賭博”網頁資源內容類別的網路資源存取規則將轉換至“賭博、彩票和抽獎”內容類別。
- 基於“瀏覽器遊戲”網頁資源內容類別的網路資源存取規則將轉換至“電腦遊戲”內容類別。
- 對於上表未列出的各種網頁資源內容類別，轉換時將不發生任何變更。

匯出和匯入網頁資源位址清單

如果您在網路資源存取規則中建立了網路資源位址清單，則可將其匯出到 .txt 檔案。隨後，您可以從該檔案匯入清單，從而不必在設定存取規則時建立新的網頁位址清單。例如，在建立具有相似參數的存取規則時，用於匯出和匯入網頁位址清單的選項會非常有用。

若要將網頁資源位址清單匯出到檔案，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點控制”區域中，選取“網頁控制”子區域。
在視窗右側，將顯示網頁控制元件的設定。
3. 選取您要將其網頁位址清單匯出到檔案的規則。
4. 點擊“編輯”按鈕。
開啟 **按存取規則的優先排序** 視窗。
5. 如果您不希望匯出整個網頁位址清單，而只是要匯出清單的一部分，請選取所需的網頁位址。
6. 在包含網頁資源位址清單的欄位的右側，點擊  按鈕。
系統將開啟操作確認視窗。
7. 請執行以下操作之一：
 - 如果您要只匯出網頁位址清單中的選取內容，請在操作確認視窗中，點擊“是”按鈕。
 - 如果您要匯出網頁位址清單中的選取內容，請在操作確認視窗中，點選“否”按鈕。
標準的 Microsoft Office “另存為”視窗將開啟。
8. 在 Microsoft Windows 的“另存為”視窗中，選取您要匯出網頁位址清單的檔案。點擊**儲存** 按鈕。

若要從一個檔案將網頁資源位址清單匯出到規則，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“端點控制”區域中，選取“網頁控制”子區域。

在視窗右側，將顯示網頁控制元件的設定。


3. 請執行以下操作之一：

- 如果您要建立新的網路資源存取規則，請點擊**“新增”**按鈕。
- 選取您要編輯的網路資源存取規則。然後點擊**“編輯”**按鈕。

開啟 **按存取規則的優先排序** 視窗。

4. 請執行以下操作之一：

- 如果建立新的網路資源存取規則，請從**“套用於位址”**下拉清單中選取**“指定的位址”**。
- 如果編輯網路資源存取規則，請轉到這些操作說明中的第 5 步。

5. 在包含網頁資源位址清單的欄位的右側，點擊  按鈕。

如果您正建立新規則，程式將開啟標準的Microsoft Windows**“開啟檔案”**視窗。

如果您正編輯規則，將開啟一個視窗需求請您進行確認。

6. 請執行以下操作之一：

- 如果編輯網路資源存取規則，請轉到這些操作說明中的第 7 步。
- 如果您正編輯網路資源存取規則，請在操作確認視窗中執行以下操作：
 - 如果您要將從網頁資源位址清單中匯入的內容新增到現有清單，請點選**“是”**按鈕。
 - 如果您要刪除網頁位址清單中的現有內容及新增匯入的，請點擊**“否”**按鈕。

開啟Microsoft Windows 的**“開啟檔案”**視窗。

7. 在 Microsoft Windows 的**“開啟檔案”**視窗中，選取包含要匯入的網頁位址清單的檔案。

8. 點擊**“開啟”**按鈕。

9. 在**“網頁存取規則”**視窗，點擊**“確定”**。

編輯網頁資源位址的遮罩

如果您在建立網路資源存取規則時需要輸入多個相似的網頁位址，則使用**網路資源位址遮罩**（也稱為“位址遮罩”）會較為便利。如果建立得當，一個位址遮罩可以替換多項的網頁位址。

建立位址遮罩時遵循以下規則：

1. * 字元將替換包含零或任意個字元的任何序列。

例如，如果輸入 *abc* 位址遮罩，則存取規則將應用於包含序列 abc 的所有網頁。範例：
http://www.example.com/page_0-9abcdef.html。

若要在位址遮罩中包括 * 字元，則輸入兩個 * 字元。

2. 位於位址遮罩開頭的 www. 字元序列被解釋為 *. 序列。

範例：位址遮罩 www.example.com 將作為 *.example.com 進行處理。

3. 如果位址遮罩不以 * 字元開頭，則位址遮罩的內容等同於以 * 為首碼的內容。
4. 位址遮罩開頭的字元序列 * 將被解釋為 * 或空字串。
範例：位址遮罩 `http://www*.example.com` 涵蓋位址 `http://www2.example.com`。
5. 如果位址遮罩以 / 或 * 之外的字元結尾，則位址遮罩的內容等同於以 /* 為尾碼的內容。
範例：位址遮罩 `http://www.example.com` 涵蓋像 `http://www.example.com/abc` 這樣的位址，其中 a、b 和 c 為任意字元。
6. 如果位址遮罩不以 / 字元開頭，則位址遮罩的內容等同於以 /* 為首碼的內容。
7. 字元序列 /* 將被解釋為 /* 或空字串。
8. 網頁資源位址根據位址遮罩進行驗證，同時會考慮使用的協定 (http 或 https) :
 - 如果位址遮罩不含網路通訊協定，該位址遮罩將涵蓋使用任意網路通訊協定的位址。
範例：位址遮罩 `example.com` 涵蓋位址 `http://example.com` 和 `https://example.com`。
 - 如果位址遮罩包含網路通訊協定，該位址僅涵蓋使用位址遮罩中網路通訊協定的位址。
範例：位址遮罩 `http://*.example.com` 涵蓋位址 `http://www.example.com`，但不涵蓋 `https://www.example.com`。
9. 用雙引號引起來的位址遮罩表示除 * 字元 (如果初始包含在位址遮罩中) 外，不考慮其他任何替代項目。規則 5 和 7 不會應用至雙引號中的位址遮罩 (請參閱下表中的範例 14-18) 。
10. 在比較網頁資源的位址遮罩時，不會考慮使用者名稱和密碼、連接埠以及字元大小寫。

關於如何使用規則建立位址遮罩的示範

編號	位址遮罩	要驗證的網頁資源位址	是位址遮罩涵蓋的位址	註解
1	<code>*.example.com</code>	<code>http://www.123example.com</code>	否	參閱規則 1。
2	<code>*.example.com</code>	<code>http://www.123.example.com</code>	是	參閱規則 1。
3	<code>*example.com</code>	<code>http://www.123example.com</code>	是	參閱規則 1。
4	<code>*example.com</code>	<code>http://www.123.example.com</code>	是	參閱規則 1。
5	<code>http://www*.example.com</code>	<code>http://www.123example.com</code>	否	參閱規則 1。
6	<code>www.example.com</code>	<code>http://www.example.com</code>	是	參閱規則 2、1。
7	<code>www.example.com</code>	<code>https://www.example.com</code>	是	參閱規則 2、1。
8	<code>http://www*.example.com</code>	<code>http://123.example.com</code>	是	參閱規則 2、4、1。
9	<code>www.example.com</code>	<code>http://www.example.com/abc</code>	是	參見規則 2、5、1。
10	<code>example.com</code>	<code>http://www.example.com</code>	是	參見規則 3、1。
11	<code>http://example.com/</code>	<code>http://example.com/abc</code>	是	參見規則 6。
12	<code>http://example.com/*</code>	<code>http://example.com</code>	是	參閱規則 7。
13	<code>http://example.com</code>	<code>https://example.com</code>	否	參閱規則 8。
14	<code>"example.com"</code>	<code>http://www.example.com</code>	否	參閱規則 9。
15	<code>"http://www.example.com"</code>	<code>http://www.example.com/abc</code>	否	參閱規則 9。

16	"*.example.com"	http://www.example.com	是	參閱規則 1、9。
17	"http://www.example.com/*"	http://www.example.com/abc	是	參閱規則 1、9。
18	"www.example.com"	http://www.example.com; https://www.example.com	是	參閱規則 9、8。
19	www.example.com/abc/123	http://www.example.com/abc	否	位址遮罩包含的信息量多於網頁位址。

編輯網頁控制訊息範本

根據在網頁控制規則內容中指定的操作的類型，當使用者嘗試存取網際網路資源時，Kaspersky Endpoint Security 顯示下列類型的訊息（應用程式用 HTTP 伺服器回應訊息替換 HTML 頁面）：

- 警告訊息。該訊息將警告存取該網頁資源的使用者該網頁資源不受歡迎並且/或者違反公司安全政策。如果在描述該網頁規則中的設定，從“**動作**”下拉清單中選取了“**警告**”選項，則 Kaspersky Endpoint Security 將會顯示警告訊息。

如果使用者認為該警告是錯誤的，使用者可以點擊警告訊息中的連結，開啟預先產生的回報訊息並將其傳送給公司區域網路管理員。

- 通知封鎖網頁資源的訊息。如果在描述該網頁規則的設定中，從“**動作**”下拉清單中選取了“**封鎖**”選項，則 Kaspersky Endpoint Security 顯示一條訊息，通知您封鎖了一個網頁。

如果使用者相信該網頁被封鎖是錯誤的，可以點選網頁資源封鎖通知中的連結，開啟預先產生的訊息並將其傳送給公司區域網路管理員。

我們為警告訊息、通知網頁資源被封鎖的訊息以及要傳送給管理員的訊息提供了專用範本。您可以修改其中內容。

要變更網路控制訊息範本，請執行下列操作：

- 開啟[程式設定視窗](#)。
- 在視窗左側的“**端點控制**”區域中，選取“**網頁控制**”子區域。
在視窗右側，將顯示網頁控制元件的設定。
- 在視窗右側，點擊“**範本**”按鈕。
開啟“**範本**”視窗。
- 請執行以下操作之一：
 - 如果您想要編輯警告使用者某個網頁資源是潛在威脅的範本訊息，請選取“**警告**”頁籤。
 - 如果您想要編輯通知使用者對某個網頁資源的存取被封鎖的範本訊息，請選取“**封鎖**”頁籤。
 - 要修改傳送給區域網路管理員的訊息的範本，請選取“**傳送給管理員的資訊**”頁籤。
- 編輯資訊範本。您也可以使用**變數**下拉清單和**預設**以及**連結**（在“**給管理員發訊息**”標籤上該按鈕不可用）按鈕。
- 點擊“**確定**”。

7. 要儲存變更，請點擊**儲存**按鈕。

KATA Endpoint Sensor

KATA Endpoint Sensor 元件只能在卡巴斯基安全管理中心管理主控台中可用。若要使用該元件，您必須安裝管理外掛程式。

該區域包含有關 KATA Endpoint Sensor 和如何啟用和停用該元件的說明。

關於 KATA Endpoint Sensor

KATA Endpoint Sensor 是卡巴斯基攻擊防護平台。此解決方案用於快速偵測目標攻擊之類的威脅。

該元件安裝在用戶端電腦上。在這些電腦上，該元件將持續監控處理程序、活動網路連線和被修改的檔案，並將該資訊中繼給卡巴斯基攻擊防護平台。

元件功能在以下作業系統中可用：

- Microsoft Windows 7 Professional / Enterprise / Ultimate x86 Edition SP1、Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition SP1。
- Microsoft Windows 8.1 Enterprise x86 Edition、Microsoft Windows 8.1 Enterprise x64 Edition。
- Microsoft Windows 10 Pro / Enterprise x86 Edition、Microsoft Windows 10 Pro / Enterprise x64 Edition。
- Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition SP1。
- Microsoft Windows Server 2012 Standard / Foundation / Essentials x64 Edition、Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials x64 Edition。
- Microsoft Windows Server 2016

有關本文件中未提供的卡巴斯基反針對性攻擊平台的其他資訊，請參閱卡巴斯基反針對性攻擊平台說明。

應在卡巴斯基攻擊防護平台伺服器上直接允許電腦與 KATA Endpoint Sensor 的連線，不使用代理伺服器。

啟用和停用 KATA Endpoint Sensor 元件

若要啟用和停用 KATA Endpoint Sensor 元件：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄的“**受管裝置**”資料夾中，開啟您希望為其編輯政策設定的相關管理群組所在的資料夾。
3. 在工作區選擇“**政策**”頁籤。
4. 選擇所需政策。
5. 使用以下方式開啟“**內容: <政策名稱>**”視窗：

- 在所選定項目右鍵選單中，選擇“內容”。
 - 點擊位於管理主控台工作區右側的“設定政策”連線。
6. 在“進階設定”區域中選取“KATA Endpoint Sensor”子區域。
7. 請執行以下操作之一：
- 如果您希望啟用 KATA Endpoint Sensor，選取“KATA Endpoint Sensor”核取方塊。
 - 如果您希望停用 KATA Endpoint Sensor，清空“KATA Endpoint Sensor”核取方塊。
8. 如果您在上個步驟中選定了“KATA 端點感測器”核取方塊，在“伺服器位址”欄位中指定包含以下部分的 Kaspersky Anti Targeted Attack Platform 伺服器位址：
- a. 協定名稱
 - b. 伺服器的 IP 位址或全限定功能變數名稱 (FQDN)
 - c. 伺服器上 Windows 事件收集器的路徑
9. 點擊“確定”。
10. 套用政策。

有關實施卡巴斯基安全管理中心政策的詳細資訊，請查閱《卡巴斯基安全管理中心管理手冊》。

資料加密

如果 Kaspersky Endpoint Security 安裝在執行 Microsoft Windows for workstations 的電腦上，則資料加密功能完全可用。如果將 Kaspersky Endpoint Security 安裝在執行 Microsoft Windows 以做檔案伺服器之用的電腦上，則僅使用 BitLocker 磁碟機加密技術的硬碟磁碟機加密可用。

本章節包括對硬碟及卸除式磁碟和本機磁碟上檔案和資料夾加密的資訊，並提供說明如何使用 Kaspersky Endpoint Security 和 Kaspersky Endpoint Security 管理外掛程式設定並執行資料加密和解密。

如果沒有加密資料的存取權限，請參閱如何使用加密資料的特別說明（[在檔案加密功能受限情況下使用加密檔案](#)，[在存取權限不存在的情況下使用加密裝置](#)）。

啟用在卡巴斯基安全管理中心政策中實現加密設置

若要啟用在卡巴斯基安全管理中心政策中顯示加密設定，請執行以下操作：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄的“**管理主控台 - <電腦名稱>**”節點的右鍵選單中選取“**檢視→ 介面設定**”。“**介面設定**”視窗將開啟。
3. 在“**介面設定**”視窗中，選取“**顯示加密和資料防護**”核取方塊。
4. 點擊“**確定**”。

關於資料加密

Kaspersky Endpoint Security 允許您加密儲存在本機和卸除式磁碟上的檔案和資料夾，或者整個卸除式磁碟和硬碟磁碟機。筆記型電腦、卸除式磁碟或硬碟遺失或被竊取時，又或者在未經許可的使用者或應用程式存取資料時，資料加密功能能夠將資訊洩露的危險降至最低。

如果產品授權已到期，本程式不會加密新資料，舊的已加密資料仍保持加密狀態並且可用。在此情況下，加密新資料將要求用允許使用加密的新產品授權來啟動程式。

如果產品授權已到期，或違反了終端使用者產品授權協議，亦或電腦上已刪除此金鑰、Kaspersky Endpoint Security 或加密元件，則先前加密檔案的加密狀態將得不到保證。這是因為某些應用程式，例如 Microsoft Office Word，會在編輯期間建立暫存檔案副本。原始檔案儲存後，暫存檔案副本將會替換原始檔案。因此，在沒有或無法存取資料加密功能的電腦上檔案仍未受到防護。

Kaspersky Endpoint Security 提供了以下幾個方面的資料防護：

- **加密本機電腦磁碟中的檔案**。您可以根據副檔名或副檔名群組編制檔案清單，和儲存在本機電腦磁碟機上的資料夾清單，並為特定應用程式建立的檔案建立加密規則。套用卡巴斯基安全管理中心政策後，Kaspersky Endpoint Security 將加密和解密以下檔案：
 - 單獨新增到加密和解密清單中的檔案。

- 儲存在新增到加密和解密清單中的資料夾內的檔案。
- 單獨應用程式建立的檔案。

有關實施卡巴斯基安全管理中心政策的詳細資訊，請查閱《[卡巴斯基安全管理中心管理手冊](#)》。

- **卸除式磁碟加密。**您可以指定預設加密規則，應用程式將根據該規則對所有卸除式磁碟套用相同操作，您也可以為個別卸除式磁碟指定加密規則。

預設加密規則低於為個別卸除式磁碟建立的加密規則的優先順序。為擁有特定裝置型號的卸除式磁碟建立的加密規則的優先順序低於為擁有特定裝置 ID 的卸除式磁碟建立的檔案加密規則的優先順序。

若要為卸除式磁碟中的檔案選取加密規則，Kaspersky Endpoint Security 將會檢查裝置的型號和 ID 是否已知。然後此程式將執行以下操作之一：

- 如果只有裝置型號已知，程式將為特定裝置型號的卸除式磁碟建立加密規則（如果先行已建立）。
- 如果裝置 ID 已知，程式將為特定裝置 ID 的卸除式磁碟配置加密規則（如果先行已建立）。
- 如果裝置型號和 ID 已知，程式將為特定裝置 ID 的卸除式磁碟建立加密規則（如果先行已建立）。如果不存在此類規則，但是存在為特定裝置型號的卸除式磁碟建立的加密規則，則應用程式將套用此規則。如果沒有為特定的裝置 ID 或特定的裝置型號指定加密規則，應用程式將應用預設的加密規則。
- 如果裝置型號和裝置 ID 都未知，程式將使用預設的加密規則。

程式可以讓您準備卸除式磁碟以攜帶模式使用上儲存的加密資料。啟用模式後，您可以存取連接到沒有加密功能的電腦上的卸除式磁碟中的加密檔。

應用卡巴斯基安全管理中心政策後，應用程式將執行加密規則內指定的操作。

- **管理應用程式存取加密檔案的規則。**對於任何應用程式，您可以建立加密檔案存取規則，封鎖對加密檔案的存取或者允許僅使用加密文字（應用加密時獲得的字串）存取加密檔案。
- **建立加密檔案。**您可以建立加密檔案，使用密碼防護針對此檔案的存取。只有輸入您防護此檔案的密碼才能存取加密檔案中的內容。此類檔案可以安全的透過網路或透過卸除式磁碟傳輸。
- **加密硬碟。**您可以選取加密技術：Kaspersky Disk Encryption 或 BitLocker 磁碟機加密（以下簡稱“BitLocker”）。

BitLocker 技術是 Windows 作業系統的一部分。如果電腦配備了 Trusted Platform Module (TPM)，BitLocker 將用其儲存提供加密硬碟存取的還原金鑰。電腦啟動時，BitLocker 將從 Trusted Platform Module 請求硬碟還原金鑰並解鎖磁碟。您可以設定存取還原金鑰使用密碼和/或 PIN 碼。

您可以指定預設的硬碟加密規則，並建立要從加密中排除的硬碟清單。套用卡巴斯基安全管理中心政策後，Kaspersky Endpoint Security 將按照磁區加密硬碟。應用程式加密將同時套用至硬碟的所有邏輯分區上。有關實施卡巴斯基安全管理中心政策的詳細資訊，請查閱《[卡巴斯基安全管理中心管理手冊](#)》。

加密系統硬碟後，在下次電腦啟動時，使用者要能夠存取硬碟並且作業系統載入前，使用者必須透過[身分驗證代理](#)的驗證。這需要輸入連線至電腦的令牌或智慧卡的密碼，或者本機區域網路管理員使用身分驗證代理帳戶管理工作建立的身分驗證代理帳戶的使用者名稱或密碼。這些帳戶以使用者登入作業系統的 Microsoft Windows 帳戶為基礎。這些帳戶以使用者登入作業系統的 Microsoft Windows 帳戶為基礎。您可以管理身分驗證代理帳戶並使用單點登入 (SSO) 技術，該技術使您可以使用身分驗證代理帳戶的使用者名稱和密碼自動登入至作業系統。

如果您備份電腦，然後對電腦資料進行加密，之後還原電腦備份副本並再次加密電腦資料，Kaspersky Endpoint Security 將會建立相同的身分驗證代理帳戶。要刪除重複帳戶，請使用帶有 **dupfix** 金鑰的 **klmover** 實用程式。Klmover 實用程式含在卡巴斯基安全管理中心安裝程式中。您可以在 [卡巴斯基安全管理中心管理手冊](#) 中瞭解有關其操作的更多資訊。

將應用程式版本升級到 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 時，系統不會儲存身分驗證代理帳戶清單。

只能在安裝了帶有**硬碟磁碟機加密功能**的 Kaspersky Endpoint Security 電腦上存取已加密的硬碟磁碟機。當出現公司區域網路之外的連接嘗試存取加密檔案時，此功能會大大降低加密硬碟中的檔案洩露的風險。

若要加密硬碟磁碟機和卸除式磁碟機，您可以使用**“僅加密使用的磁碟空間”**功能。建議您僅為先前未使用的新裝置使用此功能。如果您在已使用的裝置上套用加密，建議您加密整個裝置。這將確保所有資料受到防護 - 即使刪除了仍包含可檢索資訊的資料。

開始加密之前，Kaspersky Endpoint Security 將獲得檔案系統磁區圖。第一波加密包括開始加密時檔案佔用的磁區。第二波加密包括加密開始後寫入的磁區。加密完成後，所有包含資料的磁區都將被加密。

加密完成並且使用者刪除檔案後，儲存刪除檔案的磁區可以在檔案系統等級儲存新的資訊但是仍保持為加密狀態。因此，隨著在電腦上開啟 **僅加密已使用的磁碟空間** 功能的情況下啟動定期加密時向新裝置寫入新檔案，一段時間後所有磁區將被加密。

解密檔案所需的檔案由加密時控制電腦的卡斯基安全管理中心管理伺服器提供。如果包含加密檔案的電腦發現自己由於某種原因處於另外一個管理伺服器的控制下，並且這些加密檔案從未受到存取，則可以透過下列方式之一獲得存取權限：

- 從區域網路管理員那裡請求存取加密物件的權限；
- 使用“還原實用工具”還原對加密硬碟的存取權限；
- 從備份還原在加密時控制電腦的卡斯基安全管理中心管理伺服器的配置，並且在現在控制包含加密物件的電腦的管理伺服器上使用此配置。

程式將在加密期間建立服務檔案。需要硬碟上大約 2-3% 的非碎片的磁碟空間來儲存這些檔案。如果硬碟上的可用磁碟空間不足，加密操作不會運行，直至您清理出足夠的空間。

SUGGESTED CORRECTION: Kaspersky Endpoint Security 加密功能和 Kaspersky Anti-Virus for UEFI 不相容。對安裝了 Kaspersky Anti-Virus for UEFI 的電腦硬碟進行加密會使得 Kaspersky Anti-Virus for UEFI 無法執行。

加密功能限制

在加密硬碟磁碟機上建立新分區，以及格式化加密硬碟磁碟機的現有分區可能會導致這些硬碟磁碟機上的資料遺失。

對於不滿足軟硬體要求的硬碟，其無法使用 Kaspersky Disk Encryption 技術加密硬碟。

Kaspersky Endpoint Security 不支援以下配置：

- 引導載入程式位於某個磁碟上而作業系統位於其他磁碟上。
- 系統包含 UEFI 32 標準的嵌入式軟體。

- Intel® 快速啟動技術和擁有休眠分區的磁碟，即使 Intel® 快速啟動技術被停用。
- MBR 格式的磁碟擁有超過四個延伸分區。
- 交換檔案位於非系統磁碟上。
- 同時安裝有多個作業系統的多啟動系統。
- 動態分區（僅支援主要磁碟分割）。
- 未經過磁碟整理可用空間少於 2% 的磁碟。
- 磁區大小不是 512 位元組或類比 512 位元組的 4096 位元組的磁碟。
- 混合磁碟。

變更加密演算法

Kaspersky Endpoint Security 使用的資料加密演算法取決於安裝套件中包括的加密庫。

若要變更加密演算法，請執行以下操作：

1. 開始變更加密演算法之前解密 Kaspersky Endpoint Security 加密的物件。

改變加密演算法後，先前加密的物件將變為不可使用。

2. [移除 Kaspersky Endpoint Security](#)。
3. 從包含不同位數的加密庫的安裝套件中[安裝 Kaspersky Endpoint Security](#)。

啟用單點登入 (SSO) 技術

單點登入 (SSO) 技術與帳戶憑證協力廠商提供者不相容。

若要啟用單點登入 (SSO) 技術，請執行以下操作：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄中“**受管裝置**”資料夾下，開啟您希望為其啟用單點登入 (SSO) 技術的管理群組名稱所對應的資料夾。
3. 在工作區選擇“**政策**”頁籤。
4. 選擇所需政策。
5. 使用以下方式開啟“**內容: <政策名稱>**”視窗：

- 在所選定項目右鍵選單中，選擇“內容”。
 - 點擊位於管理主控台工作區右側的“設定政策”連線。
6. 在“資料加密”區域中，選取“公共加密設定”子區域。
 7. 在“公共加密設定”子區域中，點擊“密碼設定”區域中的“設定”按鈕。
將開啟“加密密碼設定”視窗中的“身分驗證代理”視窗。
 8. 選取“使用單點登入 (SSO) 技術”核取方塊。
 9. 點擊“確定”。
 10. 若要儲存您的設定，請在“內容：<政策名稱>”視窗，點擊“確定”按鈕。
 11. 套用政策。
有關實施卡巴斯基安全管理中心政策的詳細資訊，請查閱《卡巴斯基安全管理中心管理手冊》。

檔案加密特殊考慮

使用檔案加密功能時，請記住以下幾點：

- 已經為指定受管電腦組建立了針對卸除式磁碟資料加密的帶有預設設定的卡巴斯基安全管理中心政策。因此，卸除式磁碟上的檔案加密/解密政策應用程式結果取決於其所連接的電腦。
- Kaspersky Endpoint Security 不會加密/解密卸除式磁碟上儲存狀態為唯讀的檔案。
- Kaspersky Endpoint Security 僅為作業系統本機使用者設定資料加密/解密標準資料夾內的檔案。Kaspersky Endpoint Security 不會加密/解密標準資料夾內的行動使用者設定檔、強制使用者設定檔、臨時使用者設定檔和重新定位的資料夾。由 Kaspersky 建議加密的標準資料夾中包含以下資料夾：
 - 我的檔案
 - 我的最愛
 - Cookies
 - 桌面
 - Internet Explorer 暫存檔案
 - 暫存檔案
 - Outlook 檔案
- 如果加密檔案和資料夾會損壞作業系統或所安裝的應用程式時，Kaspersky Endpoint Security 不會執行加密操作。例如，加密排除項清單中包含以下檔案和包含所有內嵌物件內的檔案：
 - %WINDIR%。
 - %PROGRAMFILES%、%PROGRAMFILES(X86)%。
 - Windows 登錄檔。

您無法檢視或編輯這個加密排除清單。加密排除清單中的檔案和資料夾被新增至加密清單時，在檔案和資料夾加密期間，它們不會被加密。

- 支援以下裝置類型的卸除式磁碟：
 - 透過 USB 介面連接的資料媒體
 - 透過 USB 和 FireWire 介面連接的固定磁碟機
 - 透過 USB 和 FireWire 介面連接的 SSD 磁碟機

加密本機電腦磁碟中的檔案

如果將 Kaspersky Endpoint Security 安裝在運行 Microsoft Windows 以做工作站用的電腦上，則本機電腦磁碟中的檔案可用加密。如果將 Kaspersky Endpoint Security 安裝在[執行 Microsoft Windows 以做伺服器之用](#)的電腦上，則本機電腦磁碟中的檔案可用加密。

該部分涵蓋對本機電腦磁碟上資料加密的資訊，並提供說明如何使用 Kaspersky Endpoint Security 和 Kaspersky Endpoint Security 主控台外掛程式設定並執行對本機電腦磁碟上的檔案進行加密。

加密本機電腦磁碟中的檔案

若要在本機磁碟機上加密檔案，請執行以下操作：

1. 開啟卡斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄的“**受管裝置**”資料夾下，開啟您希望為其配置本機磁碟機資料加密的管理群組所在的資料夾。
3. 在工作區選擇“**政策**”頁籤。
4. 選擇所需政策。
5. 使用以下方式開啟“**內容: <政策名稱>**”視窗：
 - 在所選定項目右鍵選單中，選擇“**內容**”。
 - 點擊位於管理主控台工作區右側的“**設定政策**”連線。
6. 在“**資料加密**”區域中，選取“**檔案及資料夾加密**”區域。
7. 在視窗右側，選擇 **加密** 頁籤。
8. 在“**加密模式**”下拉清單中，選取“**預設規則**”項。
9. 在“**加密**”標籤下，點擊“**新增**”按鈕，在下拉清單中選取以下項目之一：
 - a. 選取“**預定義資料夾**”項目將 Kaspersky 專家建議的本機使用者設定檔資料夾的檔案新增至加密規則。
“**選擇預定義資料夾**”視窗將開啟。

b. 選取“**自訂資料夾**”項目手動將資料夾路徑輸入至加密規則。

“**新增自訂資料夾**”視窗將開啟。

c. 選取“**按副檔名新增檔案**”項目將檔案副檔名新增至加密規則。Kaspersky Endpoint Security 將加密電腦本機磁碟機中所有指定副檔名的檔案。

“**新增/編輯檔案副檔名清單**”視窗將開啟。

d. 選取“**按副檔名群組新增檔案**”項將成組的檔案副檔名新增至加密規則。Kaspersky Endpoint Security 會加密電腦上所有本機磁碟機上副檔名群組中列出副檔名的檔案。

“**選擇檔案副檔名群組**”視窗將開啟。

10. 若要儲存您的設定，請在“**內容：<政策名稱>**”視窗，點擊“**確定**”按鈕。

11. 套用政策。

有關實施卡斯基安全管理中心政策的詳細資訊，請查閱《**卡斯基安全管理中心管理手冊**》。

一旦套用該政策，Kaspersky Endpoint Security 將加密所有加密規則中包括的和[解密規則](#)中不包括的檔案。

如果同一個的檔案被新增至加密規則和解密規則中，Kaspersky Endpoint Security 不會加密已加密的檔案，但是會解密已經加密的檔案。

如果檔案內容（檔案路徑/檔案名稱/檔案副檔名）在修改後仍然滿足加密規則條件，則 Kaspersky Endpoint Security 將加密已解密的檔案。

Kaspersky Endpoint Security 將會延遲加密已開啟的檔案，直至其關閉。

當使用者建立其內容複合加密規則條件的新檔案時，Kaspersky Endpoint Security 將在檔案開啟時加密檔案。

如果您在本機磁碟上將加密檔案移動至另一個資料夾，該檔案仍保持為加密狀態，而與該資料夾是否包含在加密規則中無關。

為應用程式建立加密檔案存取規則

為應用程式建立加密檔案存取規則：

1. 開啟卡斯基安全管理中心的管理主控台。

2. 在管理主控台樹狀目錄中，“**受管裝置**”資料夾下，開啟您希望為應用程式建立加密檔案存取規則的相關管理群組所在的資料夾。

3. 在工作區選擇“**政策**”頁籤。

4. 選擇所需政策。

5. 使用以下方式開啟“**內容：<政策名稱>**”視窗：

- 在所選定項目右鍵選單中，選擇“**內容**”。
- 點擊位於管理主控台工作區右側的“**設定政策**”連線。

6. 在“**資料加密**”區域中，選取“**檔案及資料夾加密**”區域。

7. 在“**加密模式**”下拉清單中，選取“**預設規則**”項。

存取規則僅在“**預設規則**”模式下可以應用。在“**預設值**”模式中執行存取規則後，如果您切換到“**保持不變**”模式。Kaspersky Endpoint Security 將略過所有存取規則。所有應用程式將能夠存取所有加密檔案。

8. 在視窗右側，選取“**應用程式規則**”頁籤。

9. 如果您只希望從卡巴斯基安全管理中心清單中選取應用程式，則點擊“**新增**”按鈕並在下拉清單中選取“**卡巴斯基安全管理中心清單中的應用程式**”項目。

“**卡巴斯基安全管理中心清單中的應用程式**”視窗將開啟。

請執行以下操作：

a. 指定篩選條件以縮小表中的應用程式清單。若要執行操作，指定“**應用程式**”、“**軟體廠商**”和“**已新增期間**”參數的值和“**群組**”區域中所有核取方塊。

b. 點擊 **重新整理** 按鈕。

清單將列出比對所套用篩選條件的應用程式。

c. 在“**應用程式**”列中，選取您要為其建立加密檔案存取規則的應用程式旁邊的核取方塊。

d. 在“**應用程式規則**”下拉清單中，選取確定應用程式對加密檔案存取權限的規則。

e. 在“**為先前選定應用程式指定的操作**”下拉清單中，選取根據先前為應用程式所建立加密檔案存取規則 Kaspersky Endpoint Security 所執行的操作。

f. 點擊“**確定**”。

應用程式加密檔案存取規則的詳情將顯示在 **應用程式規則** 頁籤中。

10. 如果您希望手動選取應用程式，則點擊“**新增**”按鈕並在下拉清單中選取“**自訂應用程式**”項目。

“**新增/編輯應用程式可執行檔案名稱**”視窗將開啟。

請執行以下操作：

a. 在輸入欄位中，輸入應用程式可執行檔案的名稱或名稱清單，包括其副檔名。

您也可以從卡巴斯基安全管理中心清單中新增應用程式可執行檔案的名稱，請點擊“**從卡巴斯基安全管理中心清單中新增**”按鈕。

b. 如有必要，在“**敘述**”欄位中輸入應用程式清單的說明。

c. 在“**應用程式規則**”下拉清單中，選取確定應用程式對加密檔案存取權限的規則。

d. 點擊“**確定**”。

應用程式加密檔案存取規則的詳情將顯示在 **應用程式規則** 頁籤中。

11. 點擊“**確定**”儲存變更。

加密特定應用程式建立或修改的檔案

您可以建立規則，Kaspersky Endpoint Security 將加密此規則內指定的應用程式建立或修改的檔案。

加密規則應用前指定應用程式建立或修改的檔案將不會被加密。

若要加密特定應用程式建立或修改的檔案：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄的“**受管裝置**”資料夾下，開啟您要設定指定應用程式所建立檔案加密的相關管理群組對應的同名資料夾。
3. 在工作區選擇“**政策**”頁籤。
4. 選擇所需政策。
5. 使用以下方式開啟“**內容: <政策名稱>**”視窗：
 - 在所選定項目右鍵選單中，選擇“**內容**”。
 - 點擊位於管理主控台工作區右側的“**設定政策**”連線。
6. 在“**資料加密**”區域中，選取“**檔案及資料夾加密**”區域。
7. 在“**加密模式**”下拉清單中，選取“**預設規則**”項。

加密規則僅在“**預設規則**”模式下可以套用。在“**預設規則**”模式中套用加密規則後，如果您切換到“**保持不變**”模式，Kaspersky Endpoint Security 將略過所有加密規則。先前加密的檔案將保持為加密。

8. 在視窗右側，選取“**應用程式規則**”頁籤。
9. 如果您只希望從卡巴斯基安全管理中心清單中選取應用程式，則點擊“**新增**”按鈕並在下拉清單中選取“**卡巴斯基安全管理中心清單中的應用程式**”項目。

“**卡巴斯基安全管理中心清單中的應用程式**”視窗將開啟。

請執行以下操作：

- a. 指定篩選條件以縮小表中的應用程式清單。若要執行操作，指定“**應用程式**”、“**軟體廠商**”和“**已新增期間**”參數的值和“**群組**”區域中所有核取方塊。
- b. 點擊 **重新整理** 按鈕。
清單將列出比對所套用篩選條件的應用程式。
- c. 在“**應用程式**”欄中選取其建立的檔案需要加密的應用程式旁的核取方塊。
- d. 在“**應用程式規則**”下拉清單中，選取“**加密所有已建立檔案**”。
- e. 在“**為先前選定應用程式指定的操作**”下拉清單中，選取根據先前為應用程式所建立加密檔案存取規則 Kaspersky Endpoint Security 所執行的操作。
- f. 點擊“**確定**”。

選定應用程式建立或修改檔案的加密規則的資訊將顯示在“**應用程式規則**”標籤上的表中。

10. 如果您希望手動選取應用程式，則點擊“**新增**”按鈕並在下拉清單中選取“**自訂應用程式**”項目。
“**新增/編輯應用程式可執行檔案名稱**”視窗將開啟。

請執行以下操作：

- a. 在輸入欄位中，輸入應用程式可執行檔案的名稱或名稱清單，包括其副檔名。
您也可以從卡巴斯基安全管理中心清單中新增應用程式可執行檔案的名稱，請點擊**“從卡巴斯基安全管理中心清單中新增”**按鈕。
- b. 如有必要，在**“敘述”**欄位中輸入應用程式清單的說明。
- c. 在**“應用程式規則”**下拉清單中，選取**“加密所有已建立檔案”**。
- d. 點擊**“確定”**。

選定應用程式建立或修改檔案的加密規則的資訊將顯示在**“應用程式規則”**標籤上的表中。

11. 點擊**“確定”**儲存變更。

生成解密規則

若要生成解密規則：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄中，**“受管裝置”**資料夾下，開啟您希望為其建立檔案解密清單的管理群組名稱所對應的資料夾。
3. 在工作區選擇**“政策”**頁籤。
4. 選擇所需政策。
5. 使用以下方式開啟**“內容: <政策名稱>”**視窗：
 - 在所選定項目右鍵選單中，選擇**“內容”**。
 - 點擊位於管理主控台工作區右側的**“設定政策”**連線。
6. 在**“資料加密”**區域中，選取**“檔案及資料夾加密”**區域。
7. 在視窗右側，選取**“解密”**頁籤。
8. 在**“加密模式”**下拉清單中，選取**“預設規則”**項。
9. 在**“解密”**標籤下，點擊**“新增”**按鈕，在下拉清單中選取以下項目之一：
 - a. 選取**“預定義資料夾”**項目將 Kaspersky 專家建議的本機使用者設定檔資料夾的檔案新增至解密規則。
“選擇預定義資料夾”視窗將開啟。
 - b. 選取**“自訂資料夾”**項目手動將資料夾路徑輸入至解密規則。
“新增自訂資料夾”視窗將開啟。
 - c. 選取**“按副檔名新增檔案”**項目將檔案副檔名新增至解密規則。Kaspersky Endpoint Security 不會加密電腦本機磁碟機中所有指定副檔名的檔案。
“新增/編輯檔案副檔名清單”視窗將開啟。

d. 選取“**按副檔名群組新增檔案**”項將成組的檔案副檔名新增至解密規則。Kaspersky Endpoint Security 不會解密電腦上所有本機磁碟機上副檔名群組中列出副檔名的檔案。

“**選擇檔案副檔名群組**”視窗將開啟。

10. 若要儲存您的設定，請在“**內容：<政策名稱>**”視窗，點擊“**確定**”按鈕。

11. 套用政策。

有關實施卡巴斯基安全管理中心政策的詳細資訊，請查閱《*卡巴斯基安全管理中心管理手冊*》。

如果同一個的檔案被新增至加密規則和解密規則中，Kaspersky Endpoint Security 不會加密已加密的檔案，但是會解密已經加密的檔案。

在本機電腦磁碟機上解密檔案

若要在本機磁碟機上解密檔案，請執行以下操作：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在主控台樹狀目錄的“**受管裝置**”資料夾下，開啟您希望為其設定本機磁碟機檔案加密的管理群組所在的資料夾。
3. 在工作區選擇“**政策**”頁籤。
4. 選擇所需政策。
5. 使用以下方式開啟“**內容：<政策名稱>**”視窗：
 - 在所選定項目右鍵選單中，選擇“**內容**”。
 - 點擊位於管理主控台工作區右側的“**設定政策**”連線。

6. 在“**資料加密**”區域中，選取“**檔案及資料夾加密**”區域。

7. 在視窗右側，選擇 **加密** 頁籤。

8. 從清單中刪除您要解密的檔案和資料夾。若要執行操作，請選取檔案，然後在“**刪除**”按鈕的右鍵選單中選取“**刪除規則和解密檔案**”。

您可以一次從加密清單中刪除數個專案。為此，請在按住 **CTRL** 的同時透過點擊來選擇所需的檔案，然後選擇“**刪除**”按鈕的右鍵選單中的“**刪除規則並解密檔案**”項。

從加密清單中刪除的檔案和資料夾將自動新增至解密清單中。

9. [建立檔案解密清單](#)。

10. 若要儲存您的設定，請在“**內容：<政策名稱>**”視窗，點擊“**確定**”按鈕。

11. 套用政策。

有關實施卡巴斯基安全管理中心政策的詳細資訊，請查閱《*卡巴斯基安全管理中心管理手冊*》。

套用政策後，Kaspersky Endpoint Security 將會解密被新增至解密清單的已加密檔案。

如果未加密檔案的參數（檔案路徑/檔案名稱/檔案副檔名）已變更為比對已新增至解密清單的物件的參數時，Kaspersky Endpoint Security 將會解密這些加密檔案。

Kaspersky Endpoint Security 將會延遲解密已開啟的文件，直至其關閉。

建立加密資料

Kaspersky Endpoint Security 建立加密資料時不會執行檔案壓縮。

若要建立加密的資料封包，請執行以下操作：

1. 在已安裝 Kaspersky Endpoint Security 並且已啟用加密功能的電腦上使用任意檔案管理程式選取您要新增至加密檔案的檔案和/或資料夾。右鍵點擊以開啟其右鍵選單。
 2. 在右鍵選單中，選取“**新增至加密檔案**”。
 - Microsoft Windows 對話方塊“**選擇儲存加密檔案的路徑**”將開啟。
 3. 在標準的 Microsoft Windows 對話方塊“**選擇儲存加密檔案的路徑**”中，選取卸除式磁碟上儲存加密資料的目標位置。點擊**儲存** 按鈕。
 - “**新增至加密檔案**”視窗將會開啟。
 4. 在“**新增至加密檔案**”視窗中輸入密碼並確認密碼。
 5. 點擊 **建立** 按鈕。
- 加密資料建立過程將啟動。加密資料封包建立過程完畢後，卸除式磁碟上選定的目的檔案夾中將建立一個受密碼防護的自解壓加密資料。

如果您取消建立加密資料，Kaspersky Endpoint Security 會執行以下操作：

1. 終止將檔案複製到壓縮檔案中，結束所有目前正在進行的壓縮資料加密操作，如果有正在進行的操作。
2. 刪除在建立和加密資料的過程中建立的所有暫存檔案以及壓縮檔案自身。
3. 通知使用者加密資料建立過程已被強制終止。

解壓縮加密資料

若要解壓縮加密的壓縮檔案，請執行以下操作：

1. 在任意檔案管理員中選取已加密壓縮檔案。點擊啟動已加密壓縮檔案解壓縮精靈。
- “**輸入密碼**”視窗將開啟。
2. 輸入保護加密壓縮檔案的密碼。
3. 在“**輸入密碼**”視窗中點選“**確認**”。
- 如果密碼輸入成功，“**瀏覽**”Microsoft Windows 對話視窗將開啟。
4. 在“**瀏覽**”Microsoft Windows 對話視窗中，選取解壓縮加密壓縮檔案的目的資料夾，然後點擊“**確定**”。

將加密壓縮檔案解壓縮至目的資料夾的過程將開始。

如果該加密壓縮之前已經解壓縮至指定目的資料夾，該資料夾內現有的檔案將被加密壓縮檔案中的檔案覆蓋。

如果您取消解壓縮加密資料，Kaspersky Endpoint Security 會執行以下操作：

1. 停止壓縮檔案解密過程，終止從加密壓縮檔案中複製檔案的所有操作，如果正在進行此類操作。
2. 刪除在解密和解壓縮加密壓縮檔案的過程中建立的所有暫存檔案，以及已經從加密壓縮檔案總複製到目的檔案夾中的所有檔案。
3. 通知使用者加密資料解壓縮過程已被強制終止。

加密卸除式磁碟

如果將 Kaspersky Endpoint Security 安裝在運行 Microsoft Windows for workstations 的電腦上，則可使用卸除式磁碟機加密功能。如果將 Kaspersky Endpoint Security 安裝在執行 [Microsoft Windows 以做檔案伺服器](#) 之用的電腦上，則不可使用卸除式磁碟加密功能。

該部分包含卸除式磁碟加密的資訊，以及使用 Kaspersky Endpoint Security 和 Kaspersky Endpoint Security 管理外掛程式配置和執行卸除式磁碟的加密資訊。

啟動卸除式磁碟機加密

若要加密卸除式磁碟，請執行以下操作：

1. 開啟卡斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄中，“受管裝置”資料夾下，開啟您希望為其建立卸除式磁碟機加密的相關管理群組名稱所對應的資料夾。
3. 在工作區選擇“政策”頁籤。
4. 選擇所需政策。
5. 使用以下方式開啟“內容: <政策名稱>”視窗：
 - 在所選定項目右鍵選單中，選擇“內容”。
 - 點擊位於管理主控台工作區右側的“設定政策”連線。
6. 在“資料加密”區域中，選取“卸除式磁碟加密”子區域。
7. 在“加密模式”下拉清單中，選取在選定受管理群組中電腦上連線卸除式磁碟時，Kaspersky Endpoint Security 對其執行的預設操作。

- **加密整個磁碟機**。如果選定了該選項，為卸除式磁碟有指定加密設定的卡巴斯基安全管理中心政策時，Kaspersky Endpoint Security 將會按磁區加密卸除式磁碟上的儲存內容。因此，應用程式加密不僅僅是卸除式磁碟上的檔案，還加密了包括資料夾結構在內的卸除式磁碟系統檔案。Kaspersky Endpoint Security 不會重新加密已經加密的卸除式磁碟。

該加密功能屬於 Kaspersky Endpoint Security 的硬碟加密功能。

- **加密所有檔案**。如果選定了該選項，為卸除式磁碟應用帶有指定加密設定的卡巴斯基安全管理中心政策時，Kaspersky Endpoint Security 將會加密卸除式磁碟上儲存的所有檔案。Kaspersky Endpoint Security 不會再次加密已經加密的檔案。程式不會加密包括已加密檔案和資料夾結構的名稱在內的卸除式磁碟中的系統檔案。
- **僅加密新檔案**。如果選定了該選項，為卸除式磁碟應用帶有指定加密設定的卡巴斯基安全管理中心政策時，Kaspersky Endpoint Security 將只會加密在上次應用卡巴斯基安全管理中心政策之後新增至卸除式磁碟的檔案或者卸除式磁碟之後儲存的和修改的所有檔案。
- **解密整個硬碟**。如果選定了該選項，為卸除式磁碟應用帶有指定加密設定的卡巴斯基安全管理中心政策時，Kaspersky Endpoint Security 將會解密卸除式磁碟上儲存的先前加密的所有已加密檔案和檔案系統。

該加密特點使得資料加密功能和由 Kaspersky Endpoint Security 提供的硬碟加密功能。

- **保留不變**。如果選定了該選項，為卸除式磁碟應用帶有指定加密設定的卡巴斯基安全管理中心政策時，Kaspersky Endpoint Security 不會加密或解密卸除式磁碟上的檔案。

8. 在卸除式磁碟上為需要加密其內容的檔案[建立](#)加密規則。

9. 套用政策。

有關實施卡巴斯基安全管理中心政策的詳細資訊，請查閱《卡巴斯基安全管理中心管理手冊》。

套用政策之後，當使用者連接卸除式磁碟時或者已經連接卸除式磁碟時，Kaspersky Endpoint Security 將會通知使用者卸除式磁碟將應用加密規則：該卸除式磁碟上儲存的資料將被加密。

如果卸除式磁碟上的加密資料應用 *保留不變* 規則，程式不會通知使用者任何資訊。

程式將警告使用者加密過程可能會花費些時間。

程式將通知使用者確定加密操作並執行以下操作：

- 如果使用者同意加密，程式將根據政策設定加密資料。
- 如果使用者拒絕加密，程式將不會加密資料，將卸除式磁碟上的檔案限定為唯讀。
- 如果使用者略過加密提示，程式將不會加密資料，並將卸除式磁碟上的檔案限定為唯讀，應用卡巴斯基安全管理中心政策時或連線卸除式磁碟時，程式將再次提示使用者確認資料加密。

已經為指定受管電腦組建立了針對卸除式磁碟機資料加密的帶有預設設定的卡巴斯基安全管理中心政策。因此，卸除式磁碟上的資料加密結果取決於其所連接的電腦。

如果在資料加密期間，使用者安全刪除卸除式磁碟，Kaspersky Endpoint Security 將會在加密過程完成前中斷資料加密過程，允許刪除卸除式磁碟。

如果對卸除式磁碟機的加密失敗，請在 Kaspersky Endpoint Security 介面中查看“資料加密”報告。對檔案的存取可能被其他應用程式拒絕。在這種情況下，請嘗試從電腦上拔下卸除式磁碟機，然後重新連接。

新增卸除式磁碟加密規則

若要為卸除式磁碟機新新增密規則，請執行以下操作：

1. 開啟卡斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄中的“受管裝置”資料夾內，開啟您希望為其新增卸除式磁碟機加密規則的相關管理群組對應的同名資料夾。
3. 在工作區選擇“政策”頁籤。
4. 選擇所需政策。
5. 使用以下方式開啟“內容: <政策名稱>”視窗：
 - 在所選定項目右鍵選單中，選擇“內容”。
 - 點擊位於管理主控台工作區右側的“設定政策”連線。
6. 在“資料加密”區域中，選取“卸除式磁碟加密”子區域。
7. 左鍵點擊“新增”按鈕並在下拉清單中選取以下項目之一：
 - 如果您希望為裝置控制元件的受信任裝置清單中的卸除式磁碟新增加密規則，則選取“從該政策受信任裝置清單中”。
 - “新增受信任裝置清單中的裝置”視窗將開啟。
 - 如果您希望為卡斯基安全管理中心清單中卸除式磁碟新增加密規則，則選取“從裝置的卡斯基安全管理中心清單中”。
 - “新增卡斯基安全管理中心裝置清單”視窗將開啟。
8. 如果您在上個步驟中選取了“從裝置的卡斯基安全管理中心 清單中”，則指定表中顯示裝置的篩選器。為此，請參閱以下執行操作：
 - a. 指定以下參數值：為已定義的表顯示裝置、裝置類型、名稱、電腦和 Kaspersky Disk Encryption。
 - b. 點擊 重新整理 按鈕。
9. 在“裝置類型”欄位中，選取您要為其建立加密規則的卸除式磁碟名稱旁邊的核取方塊。
10. 在“選定裝置加密模式”下拉清單中，選取 Kaspersky Endpoint Security 對選定卸除式磁碟上檔案執行的操作。
11. 如果您希望 Kaspersky Endpoint Security 在加密前準備卸除式磁碟，請選取“攜帶模式”核取方塊，這將能夠在攜帶模式中使用上面儲存的加密檔案。

攜帶模式可以在存有加密檔案的卸除式磁碟連線至沒有加密功能的電腦時能夠存取卸除式磁碟中的加密檔案。

12. 如果您希望 Kaspersky Endpoint Security 只加密包含有檔案的磁碟磁區，則選取“**僅加密已使用的磁碟空間**”核取方塊。

如果您在已使用的磁碟上應用加密，建議加密整個磁碟。這將確保所有資料受到防護 - 即使刪除了仍包含可檢索資訊的資料。建議為先前未使用的新磁碟使用“**僅加密已使用的磁碟空間**”功能。

如果先前使用“**僅加密已使用的磁碟空間**”功能加密了裝置，則在“**加密整個卸除式磁碟**”模式中套用政策，未包含檔案的磁區將不會被加密。

13. 在“**為先前選定裝置指定的操作**”下拉清單中，選取根據先前為卸除式磁碟所建立加密檔案存取規則 Kaspersky Endpoint Security 所執行的操作：

- 如果您希望先前為卸除式磁碟建立的加密規則不變，則選取“**略過**”。
- 如果您希望先前為卸除式磁碟建立的加密規則由新規則代替，則選取“**更新**”。

14. 點擊“**確定**”。

包含已建立加密規則的參數將顯示在“**自訂規則**”頁籤中。

15. 點擊“**確定**”儲存變更。

新增的卸除式磁碟加密規則，套用於卡巴斯基安全管理中心修改後的政策用以控制任何電腦的可攜式裝置。

編輯卸除式磁碟的加密規則

若要為卸除式磁碟機編輯加密規則，請執行以下操作：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在主控台樹狀目錄中的“**受管裝置**”資料夾內，開啟您希望為其編輯卸除式磁碟機加密的相關管理群組對應的同名資料夾。
3. 在工作區選擇“**政策**”頁籤。
4. 選擇所需政策。
5. 使用以下方式開啟“**內容: <政策名稱>**”視窗：
 - 在所選定項目右鍵選單中，選擇“**內容**”。
 - 點擊位於管理主控台工作區右側的“**設定政策**”連線。
6. 在“**資料加密**”區域中，選取“**卸除式磁碟加密**”子區域。
7. 已配置加密規則的卸除式磁碟清單中，選擇對應您所需卸除式磁碟的項目。
8. 點擊**指定規則**按鈕為卸除式磁碟編輯加密規則。
系統將開啟“**指定規則**”按鈕的功能表。
9. 在“**設定規則**”按鈕的右鍵選單中，選取 Kaspersky Endpoint Security 對選定卸除式磁碟機上檔案執行的操作。
10. 點擊“**確定**”儲存變更。

已修改的卸除式磁碟加密規則，套用於卡巴斯基安全管理中心修改後的政策用以控制任何電腦的卸除式磁碟。

啟用攜帶模式存取卸除式磁碟上的加密檔案

若要啟用攜帶模式以便存取卸除式磁碟機上的加密檔案，請執行以下操作：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄中，在“**受管裝置**”資料夾中，開啟您要啟用攜帶模式以便存取卸除式磁碟上加密檔案的管理群組名稱所對應的資料夾。
3. 在工作區選擇“**政策**”頁籤。
4. 選擇所需政策。
5. 使用以下方式開啟“**內容: <政策名稱>**”視窗：
 - 在所選定項目右鍵選單中，選擇“**內容**”。
 - 點擊位於管理主控台工作區右側的“**設定政策**”連線。
6. 在“**資料加密**”區域中，選取“**卸除式磁碟加密**”子區域。
7. 勾選“**攜帶模式**”核取方塊。

攜帶模式可用於加密所有檔案，也可用於僅加密新檔案。

8. 點擊“**確定**”。
 9. 套用政策。

有關實施卡巴斯基安全管理中心政策的詳細資訊，請查閱《*卡巴斯基安全管理中心管理手冊*》。
 10. 連線卸除式磁碟機到套用了卡巴斯基安全管理中心政策的裝置。
 11. 確認卸除式磁碟機加密操作。

這會開啟一個視窗，您可以在其中為 [攜帶式檔案管理器](#) 建立密碼。
 12. 指定滿足強度要求的密碼並確認。
 13. 點擊“**確定**”。
- Kaspersky Endpoint Security 根據卡巴斯基安全管理中心政策中定義的加密規則加密卸除式磁碟機上的檔案。用來操作加密檔案的攜帶式檔案管理器也將被寫入卸除式磁碟機。

啟用模式後，您可以存取連接到沒有加密功能的電腦上的卸除式磁碟中的加密檔。

解密卸除式磁碟

若要解密卸除式磁碟機，請執行以下操作：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄中，「**受管裝置**」資料夾下，開啟您希望為其建立卸除式磁碟機加密的相關管理群組名稱所對應的資料夾。
3. 在工作區選擇「**政策**」頁籤。
4. 選擇所需政策。
5. 使用以下方式開啟「**內容: <政策名稱>**」視窗：
 - 在所選定項目右鍵選單中，選擇「**內容**」。
 - 點擊位於管理主控台工作區右側的「**設定政策**」連線。
6. 在「**資料加密**」區域中，選取「**卸除式磁碟加密**」子區域。
7. 如果您希望解密所有儲存在卸除式磁碟上的加密檔案，請在「**加密模式**」下拉清單中選取「**解密整個卸除式磁碟機**」。
8. 若要解密儲存在個人卸除式磁碟上的資料，請為您要解密其資料的卸除式磁碟編輯加密規則。為此，請參閱以下執行操作：
 - a. 已配置加密規則的卸除式磁碟清單中，選擇對應您所需卸除式磁碟的項目。
 - b. 點擊**指定規則**按鈕為卸除式磁碟編輯加密規則。
系統將開啟「**指定規則**」按鈕的功能表。
 - c. 選取「**設定規則**」項目右鍵選單中的「**解密所有檔案**」按鈕。
9. 點擊「**確定**」儲存變更。
10. 套用政策。

有關實施卡巴斯基安全管理中心政策的詳細資訊，請查閱《*卡巴斯基安全管理中心管理手冊*》。

套用政策之後，當使用者連接卸除式磁碟時或者已經連接卸除式磁碟時，Kaspersky Endpoint Security 將會通知使用者卸除式磁碟將應用加密規則：卸除式磁碟上加密的檔案以及卸除式磁碟的檔案系統（如果已加密）將被解密。程式將警告使用者解密過程可能會花費些時間。

已經為指定受管電腦組建立了針對卸除式磁碟機資料加密的帶有預設設定的卡巴斯基安全管理中心政策。因此，卸除式磁碟上的資料解密結果取決於其連接的電腦。

如果在資料解密期間，使用者安全刪除卸除式磁碟，Kaspersky Endpoint Security 將會在解密過程完成前中斷資料解密過程，並且允許刪除卸除式磁碟。

如果對卸除式磁碟機的解密失敗，請在 Kaspersky Endpoint Security 介面中查看「**資料加密**」報告。對檔案的存取可能被其他應用程式拒絕。在這種情況下，請嘗試從電腦上拔下卸除式磁碟機，然後重新連接。

加密硬碟

如果 Kaspersky Endpoint Security 安裝在執行 Microsoft Windows for Workstations 的電腦上，則可使用 BitLocker 磁碟機加密和 Kaspersky 磁碟加密技術進行加密。如果 Kaspersky Endpoint Security 安裝在運行 [Microsoft Windows for File Servers](#) 的電腦上，則僅 BitLocker 磁碟機加密技術可用。

此部分包含硬碟加密的資訊，以及使用 Kaspersky Endpoint Security 和 Kaspersky Endpoint Security 主控台外掛程式設定和執行硬碟加密的資訊。

關於硬碟加密

啟動硬碟加密之前，應用程式會執行一些檢查，以確定裝置是否可以被加密，其中包括檢查系統硬碟與驗證代理和 BitLocker 加密元件的相容性。若要檢查相容性，電腦必須重新啟動。重新啟動電腦後，應用程式會自動執行所有必需的檢查。如果相容性檢查不成功，則在啟動作業系統和應用程式後開始硬碟磁碟機加密。如果系統硬碟不相容驗證代理或 BitLocker 加密元件不相容，必須按下硬體重置按鈕，重新啟動電腦。Kaspersky Endpoint Security 將會記錄有關不相容的資訊記錄。在此情況下，程式將無法在系統啟動時進行硬碟加密。有關此資訊的事件將會記錄在卡巴斯基安全管理中心的報告中。

如果電腦硬體設定已經變更，先前不相容的檢查記錄資訊將會予以刪除，以重新檢查系統硬碟與身分驗證代理和 BitLocker 加密元件的相容性。執行此操作前，請先在命令列執行加密類型的 `avp pbatestreset` 指令。如果作業系統未能在檢查系統硬碟是否與身分驗證代理相容之後載入，[您必須在身分驗證代理測試執行之後使用還原實用工具刪除剩餘物件和資料](#)，然後啟動 Kaspersky Endpoint Security 並再次執行 `avp pbatestreset` 指令。

啟動硬碟加密工作後，Kaspersky Endpoint Security 將加密硬碟上的所有資料。

如果用戶在硬碟解密期間關閉或重新啟動電腦，下次啟動作業系統之前系統將載入身分驗證。成功透過身分驗證並在作業系統啟動後，Kaspersky Endpoint Security 將還原硬碟加密。

如果作業系統在加密硬碟期間切換至休眠模式，作業系統結束休眠模式時將載入身分驗證。成功透過身分驗證並在作業系統啟動後，Kaspersky Endpoint Security 將還原硬碟加密。

如果作業系統在硬碟加密期間進入休眠模式，則當作業系統結束休眠模式時，Kaspersky Endpoint Security 將還原硬碟加密，且無需載入身分驗證。

可以透過兩種方式在身分驗證代理中執行使用者身分驗證：

- 輸入區域網路管理員使用卡巴斯基安全管理中心工具建立的身分驗證代理帳戶的使用者名稱和密碼。
- 輸入連線至電腦的令牌的密碼或智慧卡的密碼。

身分驗證代理支援以下語言的鍵盤配置：

- 英語 (英國)
- 英語 (美國)
- 阿拉伯語 (阿爾及利亞、摩洛哥、突尼斯、AZERTY 佈局)
- 西班牙語 (拉丁美洲)
- 意大利語
- 德語 (德國和奧地利)

- 德語 (瑞士)
- 葡萄牙語 (巴西、ABNT2 佈局)
- 俄語 (針對帶有 QWERTY 佈局的 105 鍵 IBM / Windows 鍵盤)
- 土耳其語 (QWERTY 佈局)
- 法語 (法國)
- 法語 (瑞士)
- 法語 (比利時 AZERTY 佈局)
- 日語 (針對帶有 QWERTY 佈局的 106 鍵鍵盤)

如果作業系統的語言和區域標準設定中新增了此佈局，則在身分驗證代理中可以使用此鍵盤佈局。

如果身分驗證代理帳戶名稱包含身分驗證代理中無法使用鍵盤配置輸入的符號，則只能使用[還原實用工具](#)還原後或[還原身分驗證代理帳戶名稱和密碼還原後](#)存取加密的硬碟。

Kaspersky Endpoint Security 支援以下 eToken、智慧卡讀卡器和智慧卡：

- SafeNet eToken PRO 64K (4.2b) (USB)
- SafeNet eToken PRO 72K Java (USB)
- SafeNet eToken PRO 72K Java (智慧卡)
- SafeNet eToken 4100 72K Java (智慧卡)
- SafeNet eToken 5100 (USB)
- SafeNet eToken 5105 (USB)
- SafeNet eToken 7300 (USB)
- EMC RSA SecurID 800 (USB).
- Rutoken EDS (USB)
- Rutoken EDS (Flash)
- Aladdin-RD JaCarta PKI (USB)
- Aladdin-RD JaCarta PKI (智慧卡)
- Athena IDProtect Laser (USB)
- Gemalto IDBridge CT40 (讀卡器)
- Gemalto IDPrime .NET 511

使用 Kaspersky Disk Encryption 技術加密硬碟

加密電腦硬碟之前，建議您確保電腦未遭受感染。若要執行操作，應啟動[完整掃描或關鍵區域掃描工作](#)。如果加密被 rootkit 感染的電腦硬碟，將可能導致電腦無法操作。

若要使用 Kaspersky Disk Encryption 技術加密硬碟：

1. 開啟卡斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄中，“**受管裝置**”資料夾下，開啟您希望為其設定硬碟加密的相關管理群組名稱所對應的資料夾。
3. 在工作區選擇“**政策**”頁籤。
4. 選擇所需政策。
5. 使用以下方式開啟“**內容: <政策名稱>**”視窗：
 - 在所選定項目右鍵選單中，選擇“**內容**”。
 - 點擊位於管理主控台工作區右側的“**設定政策**”連線。
6. 在“**資料加密**”區域中，選取“**硬碟加密**”子區域。
7. 在“**加密技術**”下拉清單中，選取“**Kaspersky Disk Encryption**”選項。

如果電腦的硬碟先前使用 BitLocker 加密，則無法使用 Kaspersky Disk Encryption。

8. 在“**加密模式**”下拉清單中，選取“**加密所有磁碟機**”。

如果您需要從加密中排除某些硬碟，則[建立此類硬碟的清單](#)。

9. 選取以下加密模式之一：
 - 如果您只希望將加密應用至包含檔案的硬碟，則選取“**僅加密已使用的磁碟空間**”核取方塊。
如果您在已使用的磁碟上應用加密，建議加密整個磁碟。這將確保所有資料受到防護 - 即使刪除了仍包含可檢索資訊的資料。建議為先前未使用的新磁碟使用“**僅加密已使用的磁碟空間**”功能。
 - 如果您希望將加密應用至這個硬碟，則清空“**僅加密已使用的磁碟空間**”核取方塊。

此功能僅適用於未加密的磁碟。如果裝置先前使用**僅加密已使用的磁碟空間**功能加密，則在**加密所有硬碟**模式下套用政策後，未包含檔案的磁區不會被加密。

10. 點擊“**確定**”儲存變更。

11. 套用政策。

有關實施卡斯基安全管理中心政策的詳細資訊，請查閱《[卡斯基安全管理中心管理手冊](#)》。

使用 BitLocker 磁碟機加密技術加密硬碟

加密電腦硬碟之前，建議您確保電腦未遭受感染。若要執行操作，應啟動[完整掃描或關鍵區域掃描工作](#)。如果加密被 rootkit 感染的電腦硬碟，將可能導致電腦無法操作。

在安裝有伺服器作業系統的電腦上使用 BitLocker 磁碟機加密技術可能要求使用“新增角色和元件”精靈安裝 **BitLocker 磁碟機加密** 元件。

若要使用 BitLocker 磁碟機加密技術加密硬碟：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄中，“**受管裝置**”資料夾下，開啟您希望為其設定硬碟加密的相關管理群組名稱所對應的資料夾。
3. 在工作區選擇“**政策**”頁籤。
4. 選擇所需政策。
5. 使用以下方式開啟“**內容: <政策名稱>**”視窗：
 - 在所選定項目右鍵選單中，選擇“**內容**”。
 - 點擊位於管理主控台工作區右側的“**設定政策**”連線。
6. 在“**資料加密**”區域中，選取“**硬碟加密**”子區域。
7. 在“**加密技術**”下拉清單中，選取“**BitLocker 磁碟機加密**”選項。
8. 在“**加密模式**”下拉清單中，選取“**加密所有硬碟**”選項。
9. 如果您希望在預啟動環境中使用觸控式螢幕鍵盤輸入資訊，則選取“**允許在平板電腦上使用需要預啟動鍵盤輸入的身分驗證**”核取方塊。

建議在預啟動環境中僅對擁有備用資料登錄工具的裝置（例如 USB 鍵盤）使用此設定。

10. 選取以下加密類型之一：
 - 如果您希望使用硬體加密，則選取“**使用硬體加密**”核取方塊。
 - 如果您希望停用硬體加密，則清空“**使用硬體加密**”核取方塊。
11. 選取以下加密模式之一：
 - 如果您只希望將加密應用至包含檔案的硬碟，則選取“**僅加密已使用的磁碟空間**”核取方塊。
 - 如果您希望將加密應用至這個硬碟，則清空“**僅加密已使用的磁碟空間**”核取方塊。

此功能僅適用於未加密的磁碟。如果裝置先前使用**僅加密已使用的磁碟空間**功能加密，則在**加密所有硬碟**模式下套用政策後，未包含檔案的磁區不會被加密。

12. 選取存取使用 BitLocker 加密的硬碟方式。

- 如果您希望使用“[受信任平台模組 \(TPM\)](#)”儲存加密金鑰，則選取“**使用受信任平台模組 (TPM)**”選項。
- 如果您使用受信任平台模組 (TPM) 加密硬碟，則選取“**使用密碼**”選項，在“**密碼最小長度**”欄位中指定密碼必須包括的最少字元數。

Windows 7 和 Windows 2008 R2 作業系統以及更早的版本必須有受信任的平台模組 (TPM)。

13. 如果在上個步驟中，您選取了“**使用受信任平台模組 (TPM)**”選項：

- 如果您要設定在使用者嘗試存取加密金鑰時需提供的 PIN 碼，則選取“**使用 PIN**”核取方塊並在“**最小 PIN 長度**”欄位中指定 PIN 代碼必須包含的最少數位位元數。
- 如果您想使用密碼存取電腦上沒有受信任的平台模組的加密硬碟磁碟機，請選擇“**如果受信任的平台模組 (TPM) 不可用則使用密碼**”核取方塊，並在“**最短密碼長度**”欄位中指定密碼應包含的最少字元數。在這種情況下，使用給定的密碼存取加密金鑰將就如同**使用密碼**核取方塊被選中。

如果**如果受信任的平台模組 (TPM) 不可用則使用密碼**核取方塊未被選中且受信任的平台模組不可用，則硬碟磁碟機加密將不會啟動。

14. 點擊“**確定**”儲存變更。

15. 套用政策。

有關實施卡巴斯基安全管理中心政策的詳細資訊，請查閱《[卡巴斯基安全管理中心管理手冊](#)》。

在安裝有 Kaspersky Endpoint Security 的用戶端電腦上套用政策後，將進行以下查詢：

- 如果加密原則被套用到系統硬碟磁碟機，則如果受信任的平台模組在使用的話將會出現“PIN 代碼”視窗，或將會出現預載入授權的密碼請求視窗。
- 如果電腦的作業系統開啟了聯邦資訊處理標準的相容模式，則在 Windows 8 和更高版本中作業系統將顯示 USB 裝置連線請求視窗以儲存還原金鑰檔案。

如果無法存取加密金鑰，使用者可以請求本機網路管理員提供[還原金鑰](#)（如果還原金鑰在較早前沒有被儲存在 USB 裝置上或已遺失）。

建立硬碟加密排除清單

您可以僅為 Kaspersky Disk Encryption 技術建立加密排除項清單。

若要建立硬碟排除清單，請執行以下操作：

1. 開啟卡巴斯基安全管理中心的管理主控台。

2. 在管理主控台樹狀目錄中的“**受管裝置**”資料夾下，開啟您希望為其建立硬碟排除清單的管理群組名稱所對應的資料夾。

3. 在工作區選擇“**政策**”頁籤。

4. 選擇所需政策。

5. 使用以下方式開啟“**內容: <政策名稱>**”視窗：

- 在所選定項目右鍵選單中，選擇“**內容**”。
- 點擊位於管理主控台工作區右側的“**設定政策**”連線。

6. 在“**資料加密**”區域中，選取“**硬碟加密**”子區域。

7. 在“**加密技術**”下拉清單中，選取“**Kaspersky Disk Encryption**”選項。

從加密項目中排除的硬碟所對應的項目將顯示在“**不加密以下硬碟**”清單中。如果您先前並未建立硬碟加密排除清單，此清單將是空白。

8. 若要向硬碟排除清單中新增硬碟，請執行以下操作：

a. 點擊“**新增**”按鈕。

“**新增卡巴斯基安全管理中心裝置清單**”視窗將開啟。

b. 在“**從卡巴斯基安全管理中心清單中新增裝置**”視窗中，指定以下參數值：**名稱**、**電腦**、**磁碟類型**和**Kaspersky Disk Encryption**。

c. 點擊 **重新整理** 按鈕。

d. 在“**名稱**”列中，在表行中選擇與您要新增到硬碟磁碟機加密排除清單中的硬碟磁碟機對應的核取方塊。

e. 點擊“**確定**”。

對應於選定硬碟的項目將顯示在“**不加密以下硬碟**”清單中。

9. 如果您希望從排除項清單中刪除硬碟，則在“**不加密以下硬碟**”表中選取一個或多個行並點擊“**刪除**”按鈕。

若要選取表中多個行，請按住“**CTRL**”鍵依次選取。

10. 點擊“**確定**”儲存變更。

硬碟解密

即使沒有允許資料加密的啟動授權，您也可以解密硬碟磁碟機。

若要解密硬碟，請執行以下操作：

1. 開啟卡巴斯基安全管理中心的管理主控台。

2. 在管理主控台樹狀目錄中，「**受管裝置**」資料夾下，開啟您希望為其設定硬碟解密的相關管理群組名稱所對應的資料夾。
3. 在工作區選擇**「政策」**頁籤。
4. 選擇所需政策。
5. 使用以下方式開啟**「內容: <政策名稱>」**視窗：
 - 在所選定項目右鍵選單中，選擇**「內容」**。
 - 點擊位於管理主控台工作區右側的**「設定政策」**連線。
6. 在**「資料加密」**區域中，選取**「硬碟加密」**子區域。
7. 在**「加密技術」**下拉清單中選取加密硬碟的技術。
8. 請執行以下操作之一：
 - 在**「加密模式」**下拉清單中，選取**「解密所有硬碟」**選取方塊，如果您希望解密所有加密的硬碟。
 - 將您希望解密的加密硬碟**新增至不加密以下硬碟表**。

該選項僅對卡巴斯基磁碟加密技術有效。

9. 點擊**「確定」**儲存變更。
10. 套用政策。

有關實施卡巴斯基安全管理中心政策的詳細資訊，請查閱《*卡巴斯基安全管理中心管理手冊*》。

如果使用者在解密使用卡巴斯基磁碟加密技術進行了加密的硬碟磁碟機期間關閉了或重新啟動了電腦，下次啟動作業系統之前系統將載入身分驗證代理。成功透過身分驗證並在作業系統啟動後，Kaspersky Endpoint Security 將還原硬碟解密。

如果作業系統在在解密使用卡巴斯基磁碟加密技術進行了加密的硬碟磁碟機期間切換至休眠模式，作業系統退出休眠模式時將載入身分驗證代理。成功透過身分驗證並在作業系統啟動後，Kaspersky Endpoint Security 將還原硬碟解密。進行硬碟解密後，在第一次重新開機作業系統之前，休眠模式將不可用。

如果作業系統在硬碟解密期間進入休眠模式，則當作業系統結束休眠模式時，Kaspersky Endpoint Security 將還原硬碟加密，且無需載入身分驗證。

管理身分驗證代理

如果系統硬碟被加密，則身分驗證代理在作業系統啟動之前載入。使用身分驗證代理完成身分驗證以便存取加密的系統硬碟並載入作業系統。

在成功完成身分驗證過程後，作業系統將載入。身分驗證過程將在每次作業系統重新啟動時重新開始。

在某些情況下，使用者可能無法透過身分驗證。例如，當使用者忘記身分驗證代理帳戶的帳戶憑證，或忘記令牌或智慧卡的密碼，或遺失了令牌或智慧卡時則無法透過身分驗證。

如果使用者忘記了身分驗證代理帳戶憑證或者令牌或智慧卡密碼，您必須聯絡企業區域網路管理員以 [還原](#) 他們。

如果使用者遺失了令牌或智慧卡，管理員必須[新增令牌或智慧卡電子憑證檔案](#)到指令以建立身分驗證代理帳戶。然後使用者必須完成 [在加密裝置上還原資料](#) 過程。

配合身分驗證代理使用令牌和智慧卡

存取加密硬碟時可將令牌或智慧卡用於身分驗證。若要執行操作，您必須將令牌檔案或智慧卡電子憑證新增至建立身分驗證代理帳戶的指令。

如果電腦硬碟磁碟機使用 AES256 加密演算法進行加密，則可以使用令牌或智慧卡。如果使用 AES256 演算法加密了電腦硬碟磁碟機，新增電子憑證檔案到指令將被拒絕。

要把令牌檔案或智慧卡電子憑證檔案新增到用於建立身分驗證代理帳戶的指令中，請首先使用用於管理憑證的協力廠商軟體儲存檔案。

eToken 或智慧卡憑證必須具有下列內容：

- 憑證必須相容 X.509 標準，並且憑證必須具有 DER 編碼。
如果令牌或智慧卡憑證檔案不滿足此需求，此管理外掛程式將會拒絕將此檔案載入至用於建立身分驗證代理帳戶的指令，並會顯示錯誤訊息。
- “KeyUsage”參數定義了憑證的目的，它的值必須為 `keyEncipherment` 或 `dataEncipherment`。
如果令牌或智慧卡的電子憑證檔案不滿足此需求，此外掛程式將會把此憑證檔案載入至用於建立身分驗證代理帳戶的指令，並顯示警告訊息。
- 此憑證包含至少 1024 位長度的 RSA 金鑰。
如果令牌或智慧卡憑證檔案不滿足此需求，此管理外掛程式將會拒絕將此檔案載入至用於建立身分驗證代理帳戶的指令，並會顯示錯誤訊息。

編輯身分驗證代理說明郵件

編輯身份驗證代理說明訊息之前，請檢查[預啟動環境中受支援字元清單](#)。

若要編輯身分驗證說明郵件，請執行以下操作：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄中的“**受管裝置**”資料夾下，開啟您希望為其編輯身分驗證代理說明郵件的管理群組所在的資料夾。
3. 在工作區選擇“**政策**”頁籤。
4. 選擇所需政策。
5. 使用以下方式開啟“**內容: <政策名稱>**”視窗：
 - 在所選定項目右鍵選單中，選擇“**內容**”。
 - 點擊位於管理主控台工作區右側的“**設定政策**”連線。

6. 在“資料加密”區域中，選取“公共加密設定”子區域。

7. 在“範本”區域，點擊“訊息”按鈕。

這會開啟“身分驗證代理說明郵件”視窗。

8. 請執行以下操作：

- 輸入帳戶憑證時選取“身分驗證”標籤編輯身分驗證代理視窗中顯示的說明。
- 選取“變更密碼”頁籤可編輯在變更身分驗證代理帳戶密碼時顯示在身分驗證視窗中的說明。
- 選取“還原密碼”頁籤可編輯在還原身分驗證代理帳戶密碼時顯示在身分驗證視窗中的說明。

9. 編輯說明訊息。

如果您希望還原原始文字，則點擊“預設”按鈕。

10. 點擊“確定”。

11. 若要儲存您的設定，請在“內容：<政策名稱>”視窗，點擊“確定”按鈕。

身分驗證代理說明郵件中字串的有限支援

在預啟動環境下，支援以下 Unicode 字元：

- 基本拉丁字母 (0000 - 007F)
- 附加 Latin-1 字元 (0080 - 00FF)
- 延伸 Latin-A (0100 - 017F)
- 延伸 Latin-B (0180 - 024F)
- 未組合的延伸 ID 字元 (02B0 - 02FF)
- 組合變音標記 (0300 - 036F)
- 希臘和科普特字母 (0370 - 03FF)
- 西瑞爾字母 (0400 - 04FF)
- 希伯來語 (0590 - 05FF)
- 阿拉伯語 (0600 - 06FF)
- 附加延伸拉丁語 (1E00 - 1EFF)
- 標點符號 (2000 - 206F)
- 貨幣符號 (20A0 - 20CF)
- 類似字母的符號 (2100 - 214F)

- 幾何符號 (25A0 - 25FF)
- 阿拉伯語 Script-B (FE70 - FEFF)

該清單中未指定的字元在預啟動環境中不受支援。不建議在身分驗證代理說明訊息中使用此類字元。

選取身分驗證代理偵錯等級

偵錯檔案中關於身分驗證代理的應用程式記錄服務資訊和關於身分驗證代理使用者操作的資訊。當您需要還原對加密硬碟磁碟機上的資料的存取時，身分驗證代理偵錯檔案將非常有用。

要選取身分驗證代理偵錯等級：

1. 當帶有加密硬碟的電腦啟動後，請按 **F3** 按鈕，調出用於設定身分驗證代理設定的視窗。
2. 在身分驗證代理設定視窗中，選取偵錯等級：
 - **停用調試日誌記錄 (預設)**。如果選定此選項，應用程式不會在偵錯檔案中記錄有關身分驗證代理事件的資訊。
 - **啟用調試日誌記錄**。如果選取此選項，應用程式在偵錯檔案中記錄身分驗證代理的操作和身分驗證代理的使用者執行操作。
 - **啟用詳細日誌記錄**。如果選取此選項，應用程式將把身分驗證代理的操作輸入和身分驗證代理的使用者執行操作納入偵錯等級。

與“**啟用調試日誌記錄**”選項等級相比，在此選項下，輸入項的詳細資訊程度要更高。輸入項的詳細資訊程度更高將會減慢身分驗證代理和作業系統的啟動。

- **啟用調試日誌記錄並選取串口**。如果選取此選項，應用程式將在偵錯檔案中記錄身分驗證代理的操作輸入和身分驗證代理的使用者執行操作，並透過 COM 連接埠傳輸此檔案。
如果帶有已加密硬碟的電腦透過 COM 連接埠連線至另一台電腦時，可以從另一台電腦檢查身分驗證代理事件。
- **啟用詳細調試日誌記錄並選取串口**。如果選取此選項，應用程式將在偵錯檔案中詳細記錄身分驗證代理的操作輸入和身分驗證代理的使用者操作，並透過 COM 連接埠傳輸此檔案。

與“**啟用調試日誌記錄並選取串口**”選項的等級相比，在此選項下，輸入項的詳細資訊程度要更高。輸入項的詳細資訊程度更高將會減慢身分驗證代理和作業系統的啟動。

如果電腦上擁有已加密的硬碟或者在硬碟加密期間，資料將記錄在身分驗證代理偵錯檔案中。

與其他程式偵錯檔案不一樣，身分驗證代理偵錯檔案不會傳送至 Kaspersky Lab。如有必要，系統管理員可以手動將身分驗證代理偵錯檔案傳送至 Kaspersky Lab 以供分析。

管理身分驗證代理帳戶

以下卡巴斯基安全管理中心工具可用於管理身分驗證代理帳戶：

- 管理身分驗證代理帳戶的群組工作。此工作允許您管理一組用戶端電腦的身分驗證代理帳戶。
- **加密 (帳戶管理)** 本機工作。此工作允許您管理單個用戶端電腦的身分驗證代理帳戶。

若要配置身分驗證代理帳戶管理工作的設定：

1. 建立 ([建立本機工作](#) , [建立群組工作](#)) 身分驗證代理帳戶管理工作。
2. [開啟](#)“內容：<身分驗證代理帳戶管理工作名稱>”視窗中的“設定”區域。
3. [新增用於建立身分驗證代理帳戶的指令](#)。
4. [新增用於編輯身分驗證代理帳戶的指令](#)。
5. [新增用於刪除身分驗證代理使用者帳戶的指令](#)。
6. 如有必要，您可以編輯已新增的用於管理身分驗證代理帳戶的指令。若要執行操作，請在“**管理身分驗證代理帳戶的指令**”清單中選取指令，然後點擊“**編輯**”按鈕。
7. 如有必要，您可以刪除已新增的用於管理身分驗證代理帳戶的指令。若要執行操作，請在“**用於管理身分驗證代理帳戶的指令**”清單中選取一個或多個指令，然後點擊“**移除**”按鈕。

若要選取表中多個行，請按住“CTRL”鍵依次選取。

8. 若要儲存變更，點擊工作內容視窗中的“**確定**”。
9. [執行工作](#)。

新增至工作的身分驗證代理帳戶管理指令將執行。

新增用於建立身分驗證代理帳戶的指令

若要新增用於建立身分驗證代理帳戶的命令，請執行以下操作：

1. [開啟](#)“內容：<身分驗證代理帳戶管理工作名稱>”視窗中的“設定”區域。
2. 點擊“**新增**”按鈕並在下拉清單中選取“**新增帳戶指令**”。“**新增使用者帳戶**”視窗將開啟。
3. 在“**Windows 帳戶**”內的“**新增使用者帳戶**”欄位中，指定建立身分驗證代理所依據的 Microsoft Windows 使用者帳戶。
若要執行操作，請手動輸入帳戶名或點擊**選取** 按鈕。
4. 如果您手動輸入了 Microsoft Windows 帳戶，請點擊“**允許**”按鈕確定帳戶的安全標識符 SID。
如果您點擊“**允許**”按鈕時選取不決定安全標識符 SID，SID 將在工作在電腦上執行時確定。

在新增身分驗證代理帳戶建立指令時決定 Microsoft Windows 使用者帳戶的 SID 以確保手動正確輸入 Microsoft Windows 帳戶名稱最方便的方式。如果輸入的 Microsoft Windows 帳戶不存在，或者屬於一個不受信任域，或者由於正在修改**加密 (帳戶管理)**本機工作而不存在，身分驗證代理帳戶管理工作將以執行錯誤而結束。

5. 選取**“變更目前使用者帳戶”**核取方塊，使正在建立的帳戶替換先前為身分驗證代理建立的同名的帳戶。

當您在管理身分驗證代理帳戶的群組工作中新增身分驗證代理建立命令時，此步驟將可用。當您在**加密 (帳戶管理)**本機工作中新增身分驗證代理建立指令時，此步驟將無法使用。

6. 在**“使用者名稱”**欄位中，輸入在身分驗證過程中必須輸入的身分驗證代理帳戶名，以便存取加密的硬碟。

7. 如果您希望在身分驗證期間應用程式提示使用者輸入身分驗證代理帳戶以便存取加密硬碟，請選取**“允許基於密碼的驗證”**。

8. 如果您在上個步驟中選取了**“允許基於密碼的驗證”**核取方塊：

a. 在**“密碼”**欄位中，輸入在身分驗證過程中必須輸入的身分驗證代理帳戶密碼，以便存取加密的硬碟。

b. 在**“確認密碼”**欄位中，確認在先前步驟中輸入的身分驗證代理帳戶。

c. 請執行以下操作之一：

- 如果您希望 Kaspersky Endpoint Security 在使用者第一次透過指令中指定帳戶的身分驗證時顯示密碼變更提示，請選取**“首次身分驗證時變更密碼”**選項。
- 否則，選取**“不請求密碼變更”**選項。

9. 如果您希望在存取加密硬碟身分驗證期間應用程式提示使用者輸入連線至電腦的令牌或智慧卡，請選取**“允許基於憑證的驗證”**。

10. 如果在上個步驟中，您選取了**“允許基於憑證的驗證”**核取方塊，則點擊**“瀏覽”**按鈕並在**“選擇憑證檔案”**視窗中選取令牌檔案或智慧卡電子憑證。

11. 如有必要，在**“命令敘述”**欄位中輸入您需要管理指令的身分驗證代理帳戶的詳細資料。

12. 請執行以下操作之一：

- 如果您希望應用程式允許使用者在指令中指定帳戶下存取身分驗證中的身分驗證對話方塊，請選取**“允許身分驗證”**方塊。
- 如果您希望應用程式拒絕使用者在指令中指定帳戶下存取身分驗證中的身分驗證對話方塊，請選取**“封鎖身分驗證”**方塊。

13. 在**“新增使用者帳戶”**視窗中，點擊**“確定”**。

選取身分驗證代理帳戶編輯指令

若要新增用於編輯身分驗證代理帳戶的命令，請執行以下操作：

1. 在“內容：<管理身分驗證代理帳戶管理工作名稱>”視窗的“設定”區域中，開啟“新增”按鈕的右鍵選單，然後選取“編輯帳戶命令”項。

“編輯使用者帳戶”視窗將開啟。

2. 在“編輯使用者帳戶”視窗內的“Windows 帳戶”欄位中，指定用於建立您要編輯的身分驗證代理帳戶的 Microsoft Windows 使用者帳戶名稱。若要執行操作，請手動輸入帳戶名或點擊選取 按鈕。

3. 如果您手動輸入了 Microsoft Windows 使用者帳戶，請點擊“允許”按鈕確定使用者帳戶的 SID。

如果您點擊“允許”按鈕時選取不決定安全標識符 SID，SID 將在工作在電腦上執行時確定。

在新增身分驗證代理帳戶編輯指令時決定 Microsoft Windows 使用者帳戶的 SID 是確保手動正確輸入 Microsoft Windows 使用者帳戶名稱最方便的方式。如果輸入的 Microsoft Windows 使用者帳戶不存在或屬於不受信任的網域，管理身分驗證代理帳戶的群組工作將以執行錯誤而結束。

4. 如果您希望 Kaspersky Endpoint Security 為所有基於 Microsoft Windows 的以下欄位中輸入的“Windows 帳戶”的身分驗證代理帳戶變更密碼，請選取“變更使用者名稱”核取方塊，然後為身分驗證使用者帳戶輸入密碼。

5. 選取“修改基於密碼的驗證設定”核取方塊使基於密碼的身分驗證設定變為可用。

6. 如果您希望在身分驗證期間應用程式提示使用者輸入身分驗證代理帳戶以便存取加密硬碟，請選取“允許基於密碼的驗證”。

7. 如果您在上個步驟中選取了“允許基於密碼的驗證”核取方塊：

a. 在“密碼”欄位中，輸入身分驗證代理帳戶的新密碼。

b. 在“確認密碼”欄位中，確認在先前步驟中輸入的密碼。

8. 如果您希望 Kaspersky Endpoint Security 為所有基於 Microsoft Windows 的以下欄位中輸入的“Windows 帳戶”的身分驗證代理帳戶變更密碼，請選取“在身分驗證中驗證身分時編輯密碼變更規則”核取方塊。

9. 在身分驗證中驗證身分時指定密碼變更設定的值。

10. 選取“修改基於憑證的驗證設定”核取方塊以便編輯基於 eToken 或智慧卡電子憑證的驗證設定。

11. 如果您希望在身分驗證期間應用程式提示使用者輸入連線至電腦的 eToken 或智能卡以便存取加密硬碟，請選取“允許基於憑證的驗證”。

12. 如果在上個步驟中，您選取了“允許基於憑證的驗證”核取方塊，則點擊“瀏覽”按鈕並在“選擇憑證檔案”視窗中選取令牌檔案或智慧卡電子憑證。

13. 如果您希望 Kaspersky Endpoint Security 為所有使用 Microsoft Windows 的以下欄位中輸入的“Windows 帳戶”的身分驗證代理帳戶變更命令描述，請選取“編輯命令描述”核取方塊。

14. 如果您希望 Kaspersky Endpoint Security 為所有 Windows 帳戶欄位中指定的 Microsoft Windows 帳戶建立的所有身分驗證代理帳戶將身分驗證中身分驗證使用者存取規則變更為以下指定值，請選取“編輯身分驗證中身分驗證存取規則”核取方塊。

15. 在身分驗證代理中指定存取身分驗證對話方塊的規則。

16. 在“編輯使用者帳戶”視窗中，點擊“確定”。

新增用於刪除身分驗證代理帳戶的指令

若要新增用於刪除身分驗證代理帳戶的指令：

1. 在“內容：<管理身分驗證代理帳戶的工作名稱>”視窗的“設定”區域中，開啟“新增”按鈕的右鍵選單，然後選取“刪除帳戶命令”。
- “刪除使用者帳戶”視窗將開啟。
2. 在“刪除使用者帳戶”視窗內的“Windows 帳戶”欄位中，指定已建立的您要刪除的身分驗證代理帳戶的 Microsoft Windows 使用者帳戶名稱。若要執行操作，請手動輸入帳戶名或點擊**選取** 按鈕。
3. 如果您手動輸入了 Microsoft Windows 使用者帳戶，請點擊“允許”按鈕確定使用者帳戶的 SID。
- 如果您點擊“允許”按鈕時選取不決定安全標識符 SID，SID 將在工作在電腦上執行時確定。

在新增身分驗證代理帳戶刪除指令時決定 Microsoft Windows 使用者帳戶的 SID 是確保手動正確輸入 Microsoft Windows 使用者帳戶名稱的方便方式。如果輸入的 Microsoft Windows 使用者帳戶不存在或屬於不受信任的網域，管理身分驗證代理帳戶的群組工作將以執行錯誤而結束。

4. 在“刪除使用者帳戶”視窗中，點擊“確定”。

還原身分驗證代理帳戶憑證

這些說明的目標讀者是用戶端電腦上安裝有 Kaspersky Endpoint Security 的使用者。

若要還原身分驗證代理帳戶的使用者名稱和密碼，請執行以下操作：

1. 身分驗證將在作業系統載入前在擁有加密硬碟的電腦上載入。在身分驗證代理的介面上點擊“忘記密碼”按鈕初始化還原身分驗證代理的使用者名稱和密碼的流程。
2. 按照身分驗證代理的說明進行操作，以獲得用於還原身分驗證代理帳戶使用者名稱和密碼的請求單元。
3. 請求欄位中為區域網路管理員指示您的企業和電腦名稱。
4. 在身分驗證代理區域輸入區域網路管理員[生成並提供](#)的帳戶使用者名稱和密碼還原請求。
5. 為身分驗證代理帳戶輸入新密碼，並進行確認。

身分驗證代理帳戶的使用者名稱定義在還原身分驗證代理帳戶使用者名稱和密碼請求回應區域中。

當您輸入並確認身分驗證代理帳戶的新密碼後，該密碼將被儲存，您將獲得存取加密硬碟的存取權限。

回應使用者請求以還原身分驗證代理帳戶憑證

若要建立並傳送給請求還原身分驗證代理帳戶使用者名稱和密碼的使用者的回應區域，請執行以下操作：

1. 開啟卡斯基安全管理中心的管理主控台。

2. 在管理主控台樹狀目錄的“**受管理裝置**”資料夾中，開啟包含請求還原身分驗證代理帳戶使用者名稱和密碼的使用者電腦所在的管理群組對應的資料夾。
3. 在工作區選取“**裝置**”頁籤。
4. 在“**裝置**”頁籤上，選取請求身分驗證代理帳戶使用者名稱和密碼的使用者電腦所在的清單，點擊右鍵開啟右鍵選單。
5. 在右鍵選單中，選取“**在允許離線模式下存取裝置和資料**”選項。
開啟“**允許離線模式下存取裝置和資料**”視窗。
6. 在“**允許離線模式下存取裝置和資料的存取權限**”視窗中，選取“**身分驗證代理**”頁籤。
7. 在“**正在使用的加密演算法**”區域中選取加密演算法的類型。
8. 在“**帳戶**”下拉清單中，選取為請求還原身分驗證代理帳戶名稱和密碼的使用者建立的身分驗證代理帳戶的名稱。
9. 在“**硬碟**”下拉清單中，選取您要還原存取的加密硬碟。
10. 在“**使用者要求**”區域輸入使用者填寫的請求框。
對使用者請求還原身分驗證代理帳戶的使用者名稱和密碼的回應部分的內容將顯示“**存取金鑰**”欄位中。
11. 向使用者指示回應框的內容。

檢視資料加密詳細資訊

本章節介紹如何檢視資料加密詳細資訊。

關於加密狀態

當正在執行加密或解密工作時，卡斯基安全管理中心會將應用於用戶端電腦的加密參數狀態的相關資訊轉發給卡斯基安全管理中心。

程式提供了以下加密狀態值：

- **未定義政策**。尚未為該電腦定義卡斯基安全管理中心政策。
- **正在加密/解密**。正在這台電腦上進行資料加密和/或解密。
- **錯誤**。在電腦上進行資料加密和/或解密期間發生錯誤。
- **需要重新啟動**。必須重新啟動作業系統才能在該電腦上啟動或完成資料加密或解密。
- **根據政策**。已使用該電腦上應用的卡斯基安全管理中心政策中指定的加密設定完成該電腦上的資料加密和/或解密。
- **使用者已取消**。使用者拒絕確認卸除式磁碟上的檔案加密操作。
- **未支援**。資料加密功能在該電腦上無法使用。

檢視加密狀態

若要檢視電腦資料的加密狀態，請執行以下操作：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄的“**受管裝置**”資料夾中，開啟相關電腦所屬的管理群組名稱的資料夾。
3. 在工作區選取“**裝置**”頁籤。
工作區中的“**裝置**”頁籤將顯示選定電腦群組中電腦的內容。
4. 在工作區的“**裝置**”頁籤中，將捲軸滑向右側。

“**加密狀態**”列將顯示選定管理群組中電腦上資料的加密狀態。此狀態是依據有關電腦本機上的資料加密、電腦硬碟加密以及連接至電腦的卸除式磁碟的加密資訊確定的。

在卡巴斯基安全管理中心的詳細視窗中檢視加密統計資訊

若要在卡巴斯基安全管理中心的詳細視窗中檢視加密狀態，請執行以下操作：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在主控台樹狀目錄中，選取“**管理伺服器 – <電腦名稱>**”節點。
3. 在管理主控台樹狀目錄的右側工作區中選取“**統計資訊**”標籤。
4. 使用包含資料加密統計資訊的詳細視窗建立新頁面。為此，請參閱以下執行操作：
 - a. 在“**統計**”標籤上點擊“**自訂檢視**”按鈕。
“**內容：統計**”視窗將開啟。
 - b. 在“**內容：統計**”視窗，點擊“**新增**”。
“**內容：新頁面**”視窗將開啟。
 - c. 在“**內容：新頁面**”視窗的“**一般**”區域中輸入頁面名稱。
 - d. 在“**詳情視窗**”區域中點擊“**新增**”按鈕。
“**新詳細視窗**”視窗將開啟。
 - e. 在“**防護狀態**”群組的“**新詳情視窗**”區域中選取“**裝置加密**”項。
 - f. 點擊“**確定**”。
“**內容：加密控制**”視窗將開啟。
 - g. 如有必要，可編輯詳細視窗設定。若要執行操作，請使用“**內容：電腦加密**”視窗中的“**檢視**”和“**裝置**”區域。
 - h. 點擊“**確定**”。
 - i. 重複執行說明中的步驟 d – h，在“**新詳細視窗**”視窗中的“**防護狀態**”區域中，選取“**卸除式磁碟加密**”項。

新增的詳情面板將顯示在“內容：新頁面”視窗的“詳情面板”清單中。

j. 在“內容：新頁面”視窗中點擊“確定”。

在先前步驟中建立的帶有詳情面板的頁面名稱將顯示在“內容：統計”視窗的“頁面”清單中。

k. 在“內容：統計”視窗，點擊“關閉”。

5. 在“統計”頁籤，開啟在此說明的先前步驟中建立的頁面。

詳情頁面將出現，其中顯示了電腦和卸除式磁碟的加密狀態。

檢視本機電腦磁碟機上檔案加密錯誤

若要檢視本機電腦磁碟上檔案加密錯誤：

1. 開啟卡斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄中，在“受管裝置”資料夾中，開啟包含您要檢視其資料加密錯誤清單的用戶端電腦的管理群組名稱所對應的資料夾。
3. 在工作區選取“裝置”頁籤。
4. 在“裝置”頁籤上，選取清單中電腦的名稱，點擊右鍵開啟右鍵選單。
5. 請執行以下操作之一：
 - 在用戶端電腦的右鍵選單中選取“防護”。
 - 在電腦的右鍵選單中選取“內容”項。在“內容：<電腦名稱>”視窗中，選取“防護”區域。
6. 在“內容：<電腦名稱>”視窗的“防護”區域中，點擊“檢視資料加密錯誤清單”連結開啟“資料加密錯誤”視窗。
該視窗將顯示本機電腦磁碟機上資料加密錯誤的詳情。錯誤被修正後，卡斯基安全管理中心會將該錯誤詳情從“資料加密錯誤”視窗中刪除。

檢視資料加密報告

若要檢視資料加密報告，請執行以下操作：

1. 開啟卡斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄的“管理伺服器”節點中選取“報告”標籤。
3. 點擊“建立報告範本”按鈕。
“報告範本精靈”將啟動。
4. 按照“報告範本精靈”的說明進行操作。在“其他”區域的“選取報告範本類型”視窗中選取以下專案之一：
 - 受管裝置加密狀態報告。
 - 儲存的裝置資料加密報告。

- 加密錯誤報告。
- 封鎖加密檔案存取的報告。

完成新建報告範本精靈之後，新報告範本將出現在“報告”標籤上。

5. 選取在說明的上個步驟中建立的報告範本。

報告建立過程將開始。此報告將顯示在新視窗中。

管理加密檔案與檔案加密功能限制

在套用卡巴斯基安全管理中心政策並隨後加密檔案時，Kaspersky Endpoint Security 會收到用於直接存取加密檔案的金鑰。如果使用者在資料加密過程中處於活動狀態的任何 Windows 帳戶下工作，則可以使用此金鑰直接存取加密檔案。如果使用者在資料加密過程中處於非活動狀態的 Windows 帳戶下工作，則必須連接至卡巴斯基安全管理中心才能存取加密檔案。

在以下情況下可能無法存取加密檔案：

- 使用者電腦上儲存了加密金鑰，但是未連線卡巴斯基安全管理中心以管理這些加密金鑰。在這種情況下，要存取加密檔案，使用者必須從區域網路管理員處請求加密檔案存取權限。

如果不存在對卡巴斯基安全管理中心的存取權限，您必須：

- 請求存取金鑰以存取電腦硬碟磁碟機上的加密檔案；
- 若要存取卸除式磁碟上所儲存的加密檔案，請為每個卸除式磁碟上加密的檔案請求單獨的存取金鑰。
- 加密元件被從使用者電腦上移除。在此情況下，使用者可以開啟本機和移動磁碟上的加密檔案，但是檔案內容將顯示為加密。

在以下情況下，使用者可以使用加密檔案：

- 檔案放置在建立於安裝了 Kaspersky Endpoint Security 的電腦上的 [加密檔案](#) 里。
- 檔案儲存在允許 [攜帶式模式](#) 的卸除式磁碟機上。

不連接卡巴斯基安全管理中心存取加密檔案

這些說明的目標讀者是用戶端電腦上安裝有 Kaspersky Endpoint Security 的使用者。

若要不連接卡巴斯基安全管理中心存取加密檔案，請執行以下操作：

1. 嘗試存取您所需的加密檔案。

當您嘗試存取電腦本機磁碟機上所儲存的檔案時，如果沒有連接卡巴斯基安全管理中心，Kaspersky Endpoint Security 將會為本機電腦磁碟機上所有加密檔案的存取權限建立一個請求檔案。如果您嘗試存取儲存在卸除式磁碟上的檔案，Kaspersky Endpoint Security 將會為卸除式磁碟上所有加密檔案的存取權限建立一個請求檔案。“存取檔案被封鎖”視窗將開啟。

2. 將加密檔案存取權限請求傳送給本機區域網路管理員。若要進行操作，請執行下列操作之一：

- 若要將加密檔案存取權限請求傳送給本機區域網路管理員，請點擊“[透過電子郵件傳送](#)”按鈕。

- 若要儲存請求存取加密檔案的檔案並將使用其他方法傳送給區域網路管理員，則點擊“儲存”按鈕。
3. 獲取金鑰檔案存取區域網路管理員為你[建立並提供](#)的加密檔案。
 4. 使用以下方式之一啟動加密檔案存取金鑰：
 - 在任意檔案管理程式中選取加密檔案存取金鑰檔案。點擊開啟此檔案。
 - 請執行以下操作：
 - a. 開啟 Kaspersky Endpoint Security 的主視窗。
 - b. 點擊  按鈕。
這會開啟“事件”視窗。
 - c. 選取“檔案及裝置存取權限狀態”標籤。
此標籤將顯示所有加密檔案存取請求的清單。
 - d. 選取獲得存取加密檔案金鑰檔案的請求。
 - e. 若要載入獲得的加密檔案存取金鑰檔案，請點擊“瀏覽”。
系統將開啟標準的“選擇存取金鑰檔案” Microsoft Windows 對話視窗。
 - f. 在標準的 Microsoft Windows “選擇存取金鑰檔案”視窗中，選取帶有 .kesdr 副檔名的並比對存取請求檔案檔案名的管理員提供的檔案。
 - g. 點擊“開啟”按鈕。
 - h. 在“事件”視窗中點擊“確定”。

如果嘗試存取電腦本機磁碟上檔案時建立加密檔案存取請求檔案，Kaspersky Endpoint Security 會授予本機電腦磁碟上所儲存所有加密檔案的存取權限。如果嘗試存取卸除式磁碟上檔案時建立加密檔案存取請求檔案，Kaspersky Endpoint Security 會授予卸除式磁碟上所儲存所有加密檔案的存取權限。若要存取其他卸除式磁碟上所儲存的加密檔案，您必須為每個卸除式磁碟請求單獨的存取金鑰檔案。

授予使用者在不連線卡巴斯基安全管理中心時存取加密檔案的權限

若要授予使用者在不連線卡巴斯基安全管理中心時存取加密檔案的權限：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在主控台樹狀目錄中，在“受管裝置”資料夾中，開啟您要在為其請求加密檔案存取權限的電腦使用者所屬管理群組名稱所對應的資料夾。
3. 在工作區選取“裝置”頁籤。
4. 在“裝置”標籤上，選取使用者正在請求加密檔案存取權限的電腦，然後點擊滑鼠右鍵開啟右鍵選單。
5. 在右鍵選單中，選取“在允許離線模式下存取裝置和資料”選項。
開啟“允許離線模式下存取裝置和資料”視窗。
6. 在“允許離線模式下存取裝置和資料的存取權限”視窗中，選擇“加密”頁籤。

7. 在 **加密** 頁籤上點擊 **瀏覽** 按鈕。

系統將開啟標準的“**選取請求存取權限檔案**”Microsoft Windows 視窗。

8. 在“**選取請求存取權限檔案**”視窗中，指定請求加密檔案存取權限的使用者接收到的請求檔案的路徑，然後點擊“**開啟**”。

卡巴斯基安全管理中心將建立存取加密檔案的金鑰檔案。使用者請求的詳情將顯示在**加密** 頁籤上。

9. 請執行以下操作之一：

- 若要將建立的存取金鑰檔案傳送給使用者，請點擊**透過電子郵件傳送** 按鈕。
- 若要為加密裝置儲存存取金鑰檔案並透過其它方法傳送給使用者，請點擊“**儲存**”按鈕。

編輯加密檔案存取訊息範本

若要編輯加密檔案存取訊息範本，請執行以下操作：

1. 開啟卡巴斯基安全管理中心的管理主控台。

2. 在管理主控台樹狀目錄中，“**受管裝置**”資料夾下，開啟您希望編輯加密檔案存取請求郵件範本的管理群組名稱所對應的資料夾。

3. 在工作區選擇“**政策**”頁籤。

4. 選擇所需政策。

5. 使用以下方式開啟“**內容: <政策名稱>**”視窗：

- 在所選定項目右鍵選單中，選擇“**內容**”。
- 點擊位於管理主控台工作區右側的“**設定政策**”連線。

6. 在“**資料加密**”區域中，選取“**公共加密設定**”子區域。

7. 在“**範本**”區域，點擊“**範本**”按鈕。

開啟“**範本**”視窗。

8. 請執行以下操作：

- 如果您希望編輯使用者郵件範本，則選取“**使用者郵件**”標籤。使用者電腦上沒有可用金鑰用於存取加密檔案而存取加密檔案時，“**檔案存取被拒絕**”視窗將開啟。點擊“**檔案存取被拒絕**”視窗中的“**透過電子郵件傳送**”按鈕將自動建立使用者電子郵件訊息。該郵件會將請求存取加密檔案存取權限的檔案一起傳送給公司區域網路管理員。
- 如果您希望編輯管理員郵件範本，則選取“**管理員郵件**”標籤。當已選定“**授予已加密檔案的存取權限**”視窗中的“**透過電子郵件傳送**”按鈕，該電子郵件將自動被建立，並在使用者獲得加密檔案存取權限之後傳送給使用者。

9. 編輯資訊範本。

您可以使用“**預設**”按鈕和“**變數**”下拉清單。

10. 點擊“**確定**”。

11. 若要儲存您的設定，請在“內容：<政策名稱>”視窗，點擊“確定”按鈕。

無法存取加密裝置時的裝置使用

獲取存取加密裝置的權限

在以下情況下使用者可能被要求請求存取加密裝置：

- 硬碟磁碟機在其他電腦上進行的加密。
- 裝置的加密金鑰不在電腦上（例如，首次嘗試存取電腦上的加密卸除式磁碟機時），電腦未連線到卡巴斯基安全管理中心。
使用者套用存取金鑰到加密裝置後，Kaspersky Endpoint Security 將把加密金鑰儲存在使用者的電腦上，允許在隨後的存取嘗試時存取此裝置（即使未連線到卡巴斯基安全管理中心）。

可用以下方式獲得加密裝置的存取權限：

1. 使用者 [使用 Kaspersky Endpoint Security 應用程式介面建立帶有 kesdc 副檔名的請求存取檔案](#) 並把它傳送給公司區域網路管理員。
2. 管理員 [使用卡巴斯基安全管理中心管理員主控台建立帶有 kesdc 副檔名的存取金鑰檔案](#) 並把它傳送給使用者。
3. 使用者 [套用存取金鑰](#)。

還原加密裝置上的資料

使用者可用使用 [加密裝置還原實用工具](#)（以下簡稱“還原實用工具”）使用加密裝置。在下列情況中可能要求這樣做：

- 使用存取金鑰獲取存取權限的過程不成功。
- 帶有加密裝置的電腦上尚未安裝加密元件。

需要使用“還原實用工具”還原對加密裝置存取的資料有一段時間以未加密形式在使用者電腦的記憶體裡。要降低有人未經授權存取此類別資料的風險，建議您在受信任的電腦上還原存取加密裝置。

可用以下方式還原加密裝置上的資料：

1. 使用者 [使用“還原實用工具”建立帶有 fdertc 副檔名的請求存取檔案](#) 並把它傳送給公司區域網路管理員。
2. 管理員 [使用卡巴斯基安全管理中心管理員主控台建立帶有 fdertr 副檔名的存取金鑰檔案](#) 並把它傳送給使用者。
3. 使用者 [套用存取金鑰](#)。

若要還原加密系統硬碟磁碟機上的資料，使用者也可以在“還原實用工具”中指定身分驗證代理帳戶憑證。如果身分驗證代理帳戶的元資料已損壞，使用者必須使用請求存取檔案完成還原過程。


在還原加密裝置上的資料之前，建議您在將執行此操作的電腦上取消卡巴斯基安全管理中心加密政策。這可以防止重新加密磁碟。

透過應用程式介面獲得加密裝置的存取權限

這些說明的目標讀者是用戶端電腦上安裝有 Kaspersky Endpoint Security 的使用者。

要透過應用程式介面獲得加密裝置的存取權限：

1. 嘗試存取您所需的加密裝置。
“存取資料被封鎖”視窗將開啟。
2. 向公司區域網路管理員傳送帶有 kesdc 延伸的請求存取加密裝置的檔案。若要進行操作，請執行下列操作之一：
 - 若要將產生的請求存取加密裝置的檔案電郵給公司區域網路管理員，則點擊 **透過電子郵件傳送** 按鈕。
 - 若要儲存請求存取加密裝置的檔案並將使用其他方法傳送給公司區域網路管理員，則點擊“**儲存**”按鈕。

如果您已關閉 **存取資料被封鎖** 視窗而未儲存請求存取檔案或未將其傳送給公司區域網路管理員，您可以隨時在 **檔案及裝置存取權限狀態** 標籤上的 **事件** 視窗中進行此操作。若要開啟此視窗，則在程式主視窗中點擊  按鈕。

3. 獲取並儲存公司區域網路管理員 [建立和提供](#) 給您的加密裝置存取金鑰檔案。
4. 使用以下方法之一套用存取金鑰以存取加密裝置：
 - 在任何檔案管理員中，找到加密裝置存取金鑰檔案然後按兩下開啟。
 - 請執行以下操作：
 - a. 開啟 Kaspersky Endpoint Security 的主視窗。
 - b. 點擊  按鈕開啟“**事件**”視窗。
 - c. 選取“**檔案及裝置存取權限狀態**”標籤。
此視窗包含所有加密檔案和裝置存取請求的清單。
 - d. 選擇收到用來存取加密裝置的存取金鑰檔案的請求。
 - e. 若要載入收到的加密裝置存取金鑰檔案，請點擊“**瀏覽**”。
系統將開啟標準的“**選擇存取金鑰檔案**” Microsoft Windows 對話視窗。
 - f. 在標準的 Microsoft Windows“**選擇存取金鑰檔案**”視窗中，選取帶有 kesdr 副檔名的並比對加密裝置存取請求檔案檔案名的管理員提供的檔案。
 - g. 點擊“**開啟**”按鈕。
 - h. 在“**檔案及裝置存取權限狀態**”視窗中點擊“**確定**”。

這樣，Kaspersky Endpoint Security 將會提供對加密裝置的存取權限。

授予使用者存取加密裝置的權限

授予使用者存取加密裝置的權限：

1. 開啟卡斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄中，在“**受管裝置**”資料夾中，開啟您要在為其請求裝置存取權限的電腦使用者所屬管理群組名稱所對應的資料夾。
3. 在工作區選取“**裝置**”頁籤。
4. 在“**裝置**”標籤上，選取使用者正在請求加密裝置存取權限的電腦，然後點擊滑鼠右鍵開啟右鍵選單。
5. 在右鍵選單中，選取“**在允許離線模式下存取裝置和資料**”選項。
開啟“**允許離線模式下存取裝置和資料**”視窗。
6. 在“**允許離線模式下存取裝置和資料的存取權限**”視窗中，選擇“**加密**”頁籤。
7. 在 **加密** 頁籤上點擊 **瀏覽** 按鈕。
系統將開啟標準的“**選取請求存取權限檔案**”Microsoft Windows 視窗。
8. 在“**選擇請求存取權限檔案**”視窗中，指定帶有您從使用者接收到的 kesdc 延伸的請求檔案位置。
9. 點擊“**開啟**”按鈕。
卡斯基安全管理中心將產生帶有 kesdr 延伸的加密裝置存取金鑰檔案。使用者請求的詳情將顯示在**加密** 頁籤上。
10. 請執行以下操作之一：
 - 若要將建立的存取金鑰檔案傳送給使用者，請點擊**透過電子郵件傳送** 按鈕。
 - 若要為加密裝置儲存存取金鑰檔案並透過其它方法傳送給使用者，請點擊“**儲存**”按鈕。

為使用者提供使用 BitLocker 加密的硬碟磁碟機還原金鑰

若要向使用者傳送使用 BitLocker 加密的系統硬碟的還原金鑰：

1. 開啟卡斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄中，在“**受管裝置**”資料夾中，開啟您要在為其請求加密磁碟存取權限的電腦使用者所屬管理群組名稱所對應的資料夾。
3. 在工作區選取“**裝置**”頁籤。
4. 在“**裝置**”頁籤上，選取屬於該使用者的正在請求加密卸除式磁碟存取權限的電腦。
5. 點擊右鍵開啟右鍵選單，選取“**允許離線模式下存取裝置和資料**”。
開啟“**允許離線模式下存取裝置和資料**”視窗。

6. 在“允許離線模式下存取裝置和資料的存取權限”視窗中，選取“存取 BitLocker 防護的系統磁碟”頁籤。
7. 提示使用者在 BitLocker 密碼輸入視窗中輸入還原金鑰 ID，然後在“還原金鑰 ID”欄位中對比該 ID。

如果 ID 不比對，該金鑰無法用於還原指定系統磁碟的存取。請確保選定電腦的名稱與使用者電腦的名稱相符合。

8. 向使用者傳送“還原金鑰”欄位中指定的金鑰。

若要向使用者傳送使用 BitLocker 加密的非系統硬碟的還原金鑰：

1. 開啟卡斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄中，選取“附加 → 加密和資料防護 → 加密裝置”資料夾。
工作區中將顯示加密裝置清單。
3. 在工作區中，選取需要還原存取權限的加密裝置。
4. 點擊右鍵調出上下文功能表，並選取“獲得指定加密裝置的存取金鑰”。
這會開啟“還原使用 BitLocker 加密磁碟的存取”視窗。
5. 提示使用者在 BitLocker 密碼輸入視窗中輸入還原金鑰 ID，然後在“還原金鑰 ID”欄位中對比該 ID。


如果 ID 不比對，該金鑰無法用於還原指定磁碟的存取。請確保選定電腦的名稱與使用者電腦的名稱相符合。

6. 向使用者傳送“還原金鑰”欄位中指定的金鑰。

建立還原實用工具的可執行檔

這些說明的目標讀者是用戶端電腦上安裝有 Kaspersky Endpoint Security 的使用者。

若要建立還原工具的可執行檔案，請執行以下操作：

1. 開啟“[程式主視窗](#)”。
2. 點擊主程式視窗左下角的 按鈕開啟“支援”視窗。
3. 在“支援”視窗中，點擊“還原加密磁碟”按鈕。
解密裝置還原實用程式啟動。
4. 在還原實用程式視窗中，點擊“建立獨立還原工具”按鈕。
“建立獨立還原實用程式”視窗將開啟。
5. 在“儲存”視窗中，手動鍵入儲存還原實用程式可執行檔案的路徑，或者點擊“瀏覽”按鈕。
6. 點擊“建立獨立還原實用程式”視窗中的“確定”按鈕。

還原實用工具的可執行檔將儲存在選定資料夾內。

使用“還原實用工具”還原加密裝置上的資料

這些說明的目標讀者是用戶端電腦上安裝有 Kaspersky Endpoint Security 的使用者。

若要使用還原工具還原對加密裝置的存取權限：

1. 按照以下方式之一執行還原工具：

- 點擊 Kaspersky Endpoint Security 主視窗內  按鈕開啟“支援”視窗，點擊“還原加密裝置”按鈕。
- 執行建立還原實用工具的 fdert.exe 可執行檔案。[此檔案由 Kaspersky Endpoint Security 建立。](#)

2. 在還原工具視窗中，從“選擇裝置”下拉清單中選取要還原其存取權限的加密裝置。

3. 點擊“掃描”按鈕允許此實用工具定義應在裝置上執行何種操作：是否應解鎖或者解密。

如果電腦可以存取 Kaspersky Endpoint Security 加密功能，“還原實用工具”將提示您解鎖裝置。解鎖裝置並不進行解密，解鎖的裝置將可以直接存取。如果電腦不可以存取 Kaspersky Endpoint Security 加密功能，“還原實用工具”將提示您解密裝置。

4. 如果加密系統硬碟磁碟機的診斷提示裝置主引導記錄 (MBR) 出現問題，請點擊“修復 MBR”按鈕。

修復裝置的主引導記錄將可加快解鎖或解密裝置時所需的資訊收集速度。

5. 根據診斷結果點擊解鎖或解密按鈕。

“裝置解鎖設定 或 裝置解密設定”視窗將開啟。

6. 如果您想要使用身分驗證代理帳戶還原資料：

- a. 請選擇使用身分驗證代理帳戶設定選項。
- b. 在名稱和密碼欄位，指定身分驗證代理帳戶憑證。

這種方法僅當還原系統硬碟磁碟機上的資料時可用。如果系統硬碟磁碟機損壞且身分驗證代理帳戶資料已遺失，您必須從公司區域網路管理員獲得存取金鑰才能還原加密裝置上的資料。

7. 如果您想要使用存取金鑰還原資料：

- a. 請選擇手動指定裝置存取金鑰選項。
- b. 點擊接收存取金鑰按鈕。
- c. “接收裝置存取金鑰”視窗將開啟。
- d. 點擊儲存按鈕，選擇要在其中儲存帶有 fdertc 副檔名的請求存取檔案的資料夾。
- e. 將此請求存取檔案傳送給公司區域網路管理員。

在接收到存取金鑰前不要關閉**接收裝置存取金鑰**視窗。當此視窗再次開啟時，您將無法套用之前由管理員建立的存取金鑰。

f. 獲取並儲存公司區域網路管理員 [建立和提供](#) 給您的存取金鑰檔案。

g. 點擊**載入**按鈕然後在開啟的視窗中選擇帶有 fdertr 副檔名的存取金鑰檔案。

8. 如果您要解密裝置，您必須在**裝置解密設定**視窗中也指定其他解密設定。為此，請參閱以下執行操作：

- 指定解密區域：
 - 如果您想要解密整個裝置，請選擇**解密整個裝置**選項。
 - 如果您想要解密裝置上的部分資料，請選擇**解密裝置中單一區域**選項然後使用**開始**和**結束**欄位指定解密區域範圍。
- 選擇寫入解密資料的位置：
 - 如果您想要用解密資料複寫原裝置上的資料，請清除**解密後將資料儲存至檔案**核取方塊。
 - 如果您想要把解密資料和原加密資料另存，請選擇**解密後將資料儲存至檔案**核取方塊然後使用**瀏覽**按鈕指定儲存資料的路徑。

9. 點擊**確定**。

裝置解鎖/解密過程將啟動。

回應使用者請求以還原加密裝置上的資料

若要建立存取裝置的金鑰檔案並將其傳送給使用者，請執行以下操作：

1. 開啟卡斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄中，選取**附加 → 加密和資料防護 → 加密裝置**資料夾。
3. 在工作區中選擇您想要為其建立存取金鑰檔案的加密裝置，然後在裝置的上下文功能表中選擇**獲取指定加密裝置的存取金鑰**。

如果您不確定請求存取檔案是為哪個電腦產生的，請在管理主控台樹狀目錄中選擇**附近 → 加密和資料防護**資料夾，然後在工作區中點擊**獲取裝置加密金鑰**連結。

“允許存取裝置”視窗將開啟。

4. 選擇使用中的加密演算法。若要進行操作，請選取下列選項之一：

- **AES256**，如果 Kaspersky Endpoint Security 已從位於加密裝置的電腦上的 AES256 資料夾中的分發套件安裝；
- **AES56**，如果 Kaspersky Endpoint Security 已從位於加密裝置的電腦上的 AES56 資料夾中的分發套件安裝；

5. 點擊 **瀏覽** 按鈕。

系統將開啟標準的“**選取請求存取權限檔案**”Microsoft Windows 視窗。

6. 在“**選擇請求存取權限檔案**”視窗中，指定帶有您從使用者接收到的 `fdertc` 延伸的請求檔案位置。

7. 點擊“**開啟**”按鈕。

卡巴斯基安全管理中心產生帶有 `fdertc` 副檔名的存取金鑰檔案用來存取加密裝置。

8. 請執行以下操作之一：

- 若要將建立的存取金鑰檔案傳送給使用者，請點擊**透過電子郵件傳送** 按鈕。
- 若要為加密裝置儲存存取金鑰檔案並透過其它方法傳送給使用者，請點擊“**儲存**”按鈕。

作業系統故障後還原對加密檔案的存取

只有使用了檔案級加密 (FLE) 時，才能在作業系統故障後還原對資料的存取。如果使用了完整磁碟加密 (FDE)，則無法還原對資料的存取。

要在作業系統故障後還原對加密資料的存取：

1. 不格式化硬碟的情況下重新安裝作業系統。
2. [安裝 Kaspersky Endpoint Security](#)。
3. 在電腦與資料加密期間控制電腦的卡巴斯基安全管理中心管理伺服器之間建立連線。

授予加密資料存取權限的條件與作業系統發生故障之前適用的條件相同。

建立作業系統緊急修復光碟

當加密硬碟由於某種原因而無法存取，因而作業系統無法載入時，作業系統救援光碟可能就會很有用。

您可以使用救援光碟載入 Windows 作業系統的映像，並且使用作業系統映像中包括的還原工具還原對加密硬碟的存取。

若要建立作業系統救援光碟：

1. [建立加密裝置還原實用工具的可執行檔案](#)。
2. 建立 Windows 預啟動環境的自訂映像。在建立 Windows 預啟動環境的自訂映像的同時，將還原實用工具的可執行檔新增至映像。
3. 將 Windows 預安裝環境的自訂映像儲存至開機磁碟機，如 CD 或卸除式磁碟。

有關建立 Windows 預啟動環境的自訂映像的說明，請參閱 Microsoft 說明檔案（例如，[Microsoft TechNet 資源](#)）。

網路防護

本章節介紹網路流量監控相關資訊，並將介紹如何設定受監控的網路連接埠設定。

關於網路防護

在 Kaspersky Endpoint Security 執行期間，[郵件防護](#)、[網頁防護](#)和[即時通訊防護](#)將監控透過您電腦上特定開放 TCP 和 UDP 連接埠和透過特殊協議傳輸的資料流。例如，郵件防護會掃描透過 SMTP 傳輸的資料，而網頁防護會掃描透過 HTTP 和 FTP 協定傳輸的資料。

Kaspersky Endpoint Security 將作業系統的 TCP 和 UDP 通訊埠根據其群組成方式分成多個群組。某些網路連接埠保留用於可能存在弱點的服務。我們建議您加強監控這些連接埠，因為這些連接埠遭受攻擊的可能性更大。如果使用非標準網路連接埠的非標準服務，這些網路連接埠也可能成為攻擊電腦的目標。您可以指定網路連接埠清單和請求網路存取的應用程式清單。這些連接埠和應用程式即可收到來自郵件防護、網頁防護和即時通訊防護元件在監控網路流量時的資訊。

設定網路流量監控設定

您可以執行以下操作以設定網路流量監控設定：

- 啟用對所有網路連接埠的監控。
- 建立受監控網路連接埠的清單。
- 建立所有網路連接埠受監控的應用程式清單。

啟動對所有網路連接埠的監控

若要啟用對所有網路連接埠的監控，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側，選擇 **端點防護** 區域。
端點防護設定將顯示在視窗右方。
3. 在“**要監控的連接埠**”區域中，選取“**監控所有連接埠**”。
4. 要儲存變更，請點擊“**儲存**”按鈕。

建立受監控網路連接埠的清單

建立受監控網路連接埠的清單

1. 開啟[程式設定視窗](#)。

2. 在視窗左側，選擇 **端點防護** 區域。

端點防護設定將顯示在視窗右方。

3. 在“**要監控的連接埠**”區域中，選取“**僅監控選擇的連接埠**”。

4. 點擊“**設定**”按鈕。

開啟“**網路連接埠**”視窗。**網路連接埠** 視窗中將顯示一個常用於傳送電子郵件和網路流量的網路連接埠清單。該網路連接埠清單包含在 Kaspersky Endpoint Security 安裝套件中。

5. 在網路連接埠清單中可執行以下操作：

- 勾選您希望加入到受監控網路連接埠清單的網路連接埠相對應的核取方塊。
預設情況下，將會選取“**網路連接埠**”視窗中列出的所有網路連接埠所對應的核取方塊。
- 清除您不希望加入到受監控網路連接埠清單的網路連接埠所對應的核取方塊。

6. 如果某網路連接埠未在網路連接埠清單中，請按照以下步驟新增：

- a. 在網路連接埠清單中，點擊“**新增**”連結開啟“**網路連接埠**”視窗。
- b. 在“**連接埠**”欄位中輸入網路連接埠號。
- c. 在“**敘述**”欄位中手動輸入網路連接埠名稱。
- d. 點擊“**確定**”。

關閉“**網路連接埠**”視窗。新增的網路連接埠將顯示在網路連接埠清單的末端。

7. 在“**網路連接埠**”視窗中點擊“**確定**”。

8. 要儲存變更，請點擊“**儲存**”按鈕。

若是 FTP 協定執行被動模式，透過隨機建立的網路連接埠，不會被新增到監控連接埠清單中。若要防護此類連線，則選取“**受監控連接埠**”區域中“**監控所有網路連接埠**”核取方塊，或者[設定監控建立 FTP 連線的應用程式的所有連接埠](#)。

建立所有網路連接埠受監控的應用程式清單

您可以使用 Kaspersky Endpoint Security 建立監控全部的連接埠的應用程式清單。

建議您在 Kaspersky Endpoint Security 建立監控所有網路連接埠的應用程式清單中包含 FTP 協定接收或傳輸資料的應用程式。

若要建立所有網路連接埠受監控的應用程式清單，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側，選擇 **端點防護** 區域。
端點防護設定將顯示在視窗右方。

3. 在“**要監控的連接埠**”區域中，選取“**僅監控選擇的連接埠**”。
 4. 點擊“**設定**”按鈕。
開啟“**網路連接埠**”視窗。
 5. 選取“**監控所選應用程式的所有連接埠**”核取方塊。
 6. 在“**監控所選應用程式的所有連接埠**”核取方塊下的應用程式清單中，執行以下操作：
 - 選取位於您希望監控其所有連接埠的應用程式名稱旁邊的核取方塊。
預設情況下，將會選取“**網路連接埠**”視窗中列出的所有網路連接埠旁邊的核取方塊。
 - 取消位於您不希望監控其所有連接埠的應用程式名稱旁邊的核取方塊。
 7. 如果清單中未包含某應用程式，請按照以下步驟新增：
 - a. 點擊位於應用程式清單下方的“**新增**”連結，開啟右鍵選單。
 - b. 在右鍵選單中，選取新增應用程式的方法：
 - 要從電腦安裝的應用程式清單中選取此應用程式，請在功能表中選取“**應用程式**”指令。此時將開啟“**選取應用程式**”視窗，可以讓您指定應用程式名稱。
 - 若要指定應用程式的可執行檔案位置，請選取“**瀏覽**”指令。此時程式將開啟 Microsoft Windows 的“**開啟**”視窗，可以讓您指定應用程式的可執行檔案名稱。

在您選取應用程式後，系統將開啟“**應用程式**”視窗。
 - c. 在“**名稱**”欄位，輸入應用程式名稱。
 - d. 點擊“**確定**”。
將關閉“**應用程式**”視窗。您新增的應用程式將出現在應用程式清單的末端。
8. 在“**網路連接埠**”視窗中點擊“**確定**”。
9. 要儲存變更，請點擊“**儲存**”按鈕。

更新資料庫和程式模組

本章節包含關於資料庫和程式模組更新（也稱為“更新”）的資訊，以及配置更新設定的說明。

關於資料庫和程式模組更新

更新 Kaspersky Endpoint Security 的資料庫和程式模組可為您的電腦提供最新防護。新病毒和其他類型的惡意程式每天都在全世界出現。Kaspersky Endpoint Security 資料庫包含關於威脅的資訊和解毒的方法。要快速偵測到威脅，建議您定期更新資料庫和應用程式模組。

定期更新需要一份程式要使用的活動授權檔案。如果目前沒有產品授權，您將只能執行一次更新。

Kaspersky Endpoint Security 的主要更新來源是 Kaspersky 更新伺服器。

您的電腦必須連線到網際網路才能成功下載來自 Kaspersky 更新伺服器的更新資料。預設情況下，系統將自動確定網際網路連線設定。如果您使用代理伺服器，則需要[調整連線設定](#)。

當執行更新時，以下物件將下載並安裝到您的電腦中：

- **Kaspersky Endpoint Security 資料庫。**由於資料庫包含了威脅簽章和關於如何刪除威脅的資訊，電腦因此而獲得防護。當搜尋並為受感染檔案解毒時，防護元件將使用此資訊。資料庫將不斷更新應對它們的方法和威脅記錄。因此，我們建議您定期更新資料庫。

除了 Kaspersky Endpoint Security 資料庫之外，系統也會更新已啟程式元件以攔截網路流量的網路驅動程式。

- **程式模組。**除了 Kaspersky Endpoint Security 資料庫，您也可以更新程式模組。更新程式模組可以修復 Kaspersky Endpoint Security 中的弱點、新增新功能或強化現有功能。

更新時，您的電腦上的程式模組和資料庫將與最新版本更新來源進行對比。如果您目前資料庫和程式模組與對應的最新版本不同，缺少的更新部分將安裝在您的電腦上。

上下文說明檔案可以與應用程式模組更新一起更新。

如果資料庫過期，更新量可能會很大，這可能會花費更多的網際網路流量（最多達幾十 MB）。

有關 Kaspersky Endpoint Security 資料庫目前狀態的資訊顯示在[應用程式主視窗](#)的“防護和控制”頁籤上“工作”區域的“更新”中。

有關更新工作執行期間更新結果和所有發生事件的資訊將記錄在 [Kaspersky Endpoint Security 報告](#)中。

關於更新來源

更新來源是包含 Kaspersky Endpoint Security 的資料庫和程式模組更新的資源。

更新來源包括卡斯基安全管理中心、Kaspersky 更新伺服器、以及網路或本機資料夾。

調整更新設定

您可以執行下列操作來設定更新設定：

- 新增新的更新來源。

更新來源的預設清單包括了卡巴斯基安全管理中心和 Kaspersky 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。

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。

如果您選取了區域網路之外的來源作為更新來源，您必須有網路連線才能進行更新。

- 選取 Kaspersky 更新伺服器區域。

如果您使用 Kaspersky 更新伺服器作為更新來源，您可選取用於下載更新資料的 Kaspersky 更新伺服器的地點。Kaspersky 更新伺服器位於多個國家/地區。使用最近的 Kaspersky 更新伺服器有助於縮短檢索更新資料所用的時間。

預設情況下，程式使用從作業系統登錄檔獲得的目前區域的資訊。

- 設定 Kaspersky Endpoint Security 從共用資料夾更新。

為了節約網際網路流量，您可以對 Kaspersky Endpoint Security 更新進行對應的設定，以便您的區域網路中的電腦從共用資料夾接收更新。為此目的，您的區域網路中一台電腦將從卡巴斯基安全管理中心伺服器或 Kaspersky 接收最新的更新資料，然後將檢索到的更新資料複製到一個共用資料夾中。然後，區域網路其他電腦可從此共用資料夾中接收更新資料。

- 選取更新工作執行模式。

如果無法執行更新工作（例如，電腦當時沒有開啟），您可以設定工作在其他時間立即自動開始執行錯過的工作。

如果您選取了“**根據排程**”更新工作執行模式，而且 Kaspersky Endpoint Security 的啟動時間與更新工作啟動排程相符，您可以在程式啟動後延遲更新工作的執行。更新工作只能在 Kaspersky Endpoint Security 啟動後經過特定時間間隔後執行。

- 設定更新工作在不同的使用者帳戶下執行。

新增更新來源

要新增更新來源，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**排程工作**”區域中，選取“**更新**”。
程式更新設定將顯示在視窗右方。
3. 在“**執行模式和更新來源**”區域中點擊“**更新來源**”按鈕。
開啟“**更新**”視窗的“**來源**”視窗。
4. 在“**來源**”頁籤上點擊“**新增**”按鈕。

開啟“**選取更新來源**”視窗。

5. 在“**選取更新來源**”視窗中選取含有更新資料的資料夾，或者在“**來源**”欄位中輸入完整路徑。
6. 點擊“**確定**”。
7. 在“**更新**”視窗中點擊“**確定**”。
8. 要儲存變更，請點擊“**儲存**”按鈕。

選擇更新資料庫區域

若要選取更新伺服器區域，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**排程工作**”區域中，選取“**更新**”。
程式更新設定將顯示在視窗右方。
3. 在“**執行模式和更新來源**”區域中點擊“**更新來源**”按鈕。
開啟“**更新**”視窗的“**來源**”視窗。
4. 在“**來源**”頁籤中的“**區域設定**”區域中選取“**從清單中選取**”。
5. 從下拉清單中選取離您目前位置最近的國家或地區。
6. 點擊“**確定**”。
7. 要儲存變更，請點擊“**儲存**”按鈕。

設定從共用資料夾更新

設定 Kaspersky Endpoint Security 從共用資料夾更新資料須執行以下幾個步驟：

1. 啟用將更新資料複製到位於區域網路上的一台電腦的共用資料夾中。
2. 設定為從指定共用資料夾中將 Kaspersky Endpoint Security 更新資料更新至區域網路中的其他電腦上。

若要啟用複製更新來源到共用資料夾，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**排程工作**”區域中，選取“**更新**”。
程式更新設定將顯示在視窗右方。
3. 在“**附加**”區域中選取“**將更新複製到資料夾**”核取方塊。
4. 指定放置更新資料的共用資料夾。您可以採用以下方式之一：

- 在“將更新複製到資料夾”核取方塊下的欄位中輸入共用資料夾路徑。
- 點擊 **瀏覽** 按鈕。在開啟的“選取資料夾”視窗中，選取需要的資料夾並點擊“**確定**”。

5. 要儲存變更，請點擊“**儲存**”按鈕。

若要設定 *Kaspersky Endpoint Security* 從共用資料夾更新，請執行以下操作：

1. 開啟 [程式設定視窗](#)。
2. 在視窗左側的“**排程工作**”區域中，選取“**更新**”。
程式更新設定將顯示在視窗右方。
3. 在“**執行模式和更新來源**”區域中點擊“**更新來源**”按鈕。
開啟“**更新**”視窗的“**來源**”視窗。
4. 在“**來源**”頁籤上點擊“**新增**”按鈕。
開啟“**選取更新來源**”視窗。
5. 在“**選取更新來源**”視窗中選取含有更新資料的共用資料夾，或者在“**來源**”欄位中輸入完整路徑。
6. 點擊“**確定**”。
7. 在“**來源**”頁籤中，取消您沒有將其指定為共用資料夾的更新來源名稱旁邊的核取方塊。
8. 點擊“**確定**”。
9. 要儲存變更，請點擊“**儲存**”按鈕。

選取更新工作執行模式

若要選取更新工作執行模式，請執行以下操作：

1. 開啟 [程式設定視窗](#)。
2. 在視窗左側的“**排程工作**”區域中，選取“**更新**”。
程式更新設定將顯示在視窗右方。
3. 點擊 **執行模式** 按鈕。
執行模式 頁籤在 **更新** 視窗中開啟。
4. 在“**執行模式**”區域中為開始更新工作選取以下選項：
 - 如果您希望 *Kaspersky Endpoint Security* 根據是否能夠從更新來源獲得更新資料進行更新，請選取“**自動更新**”。*Kaspersky Endpoint Security* 檢查更新資料的頻率在病毒爆發時會新增，在其他時候會減少。
 - 如果您希望手動開始更新工作，請選取“**手動更新**”。
 - 如果您希望為更新工作設定一個啟動排程，請選取“**根據排程**”。
5. 請執行以下操作之一：

- 如果您已經選取“自動”或“手動”選項，請轉至本說明中的第 6 步。
- 如果選取“根據排程”選項，請指定更新工作執行排程的設定。為此，請參閱以下執行操作：
 - a. 在“頻率”下拉清單中指明何時開始更新工作。從以下選項中選取一個選項：分鐘、小時、天、每週、在指定時間、每月或者在程式啟動後。
 - b. 根據“頻率”下拉清單中選取的項目，指定更新工作開始時間的值。
 - c. 在“延遲執行在程式啟動後”欄位中，指定更新工作在 Kaspersky Endpoint Security 啟動後的開始時間間隔。

如果在“頻率”下拉清單中選取“在程式啟動後”選項，那麼“延遲執行在程式啟動後”將無法使用。

- d. 如果您希望 Kaspersky Endpoint Security 儘快執行錯過的工作，請勾選“執行錯過的工作”核取方塊。

如果在“頻率”下拉清單中選取“小時”、“分鐘”或“應用程式啟動之後”，則“執行略過的工作”選框無法使用。

6. 點擊“確定”。
7. 要儲存變更，請點擊“儲存”按鈕。

在不同使用者帳戶權限下開始更新工作

預設情況下，Kaspersky Endpoint Security 使用您用來登入作業系統的帳戶執行更新工作。但是，Kaspersky Endpoint Security 可以從使用者沒有存取權限的更新來源（例如，含有更新資料的共用資料夾）進行更新，或者沒有授權代理伺服器使用者而無法存取的更新來源進行更新。在 Kaspersky Endpoint Security 設定中，您可以指定一個擁有以上權限的使用者，然後使用此使用者帳戶開始 Kaspersky Endpoint Security 更新工作。

若要使用不同的使用者帳戶開始更新工作，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“排程工作”區域中，選取“更新”。
程式更新設定將顯示在視窗右方。
3. 在“執行模式和更新來源”區域中點擊“執行模式”按鈕。
執行模式 頁籤在 更新 視窗中開啟。
4. 在“執行模式”頁籤的“使用者”區域中勾選“工作執行身分”選項。
5. 在“名稱”欄位中，輸入需要使用其權限存取更新來源的使用者帳戶。
6. 在“密碼”欄位中，輸入需要使用其權限存取更新來源的使用者密碼。
7. 點擊“確定”。
8. 要儲存變更，請點擊“儲存”按鈕。

設定應用程式模組更新

若要設定應用程式模組更新：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**排程工作**”區域中，選取“**更新**”。
程式更新設定將顯示在視窗右方。
3. 在“**附加**”區域中執行下列操作：
 - 如果希望應用程式將應用程式模組更新包含在更新軟體套件中，請選定“**下載應用程式模組更新**”核取方塊。
 - 否則，清空“**下載應用程式模組更新**”核取方塊。
4. 如果在上個步驟中選取了“**下載應用程式模組更新**”核取方塊，則指定應用程式安裝應用程式模組更新的條件：
 - 如果希望程式在本機透過程式介面或使用卡巴斯基安全管理中心，自動安裝程式模組的重要更新和其他更新（在其獲得批准後），請選取“**安裝重要更新和批准的更新**”選項。
 - 如果希望程式在本機透過程式介面或使用卡巴斯基安全管理中心安裝程式模組更新（在其獲得批准後），請選取“**僅安裝指定的更新**”選項。
5. 要儲存變更，請點擊“**儲存**”按鈕。

開始和停止更新工作

無論選取的何種更新工作執行模式，您都可以隨時啟動或停止 Kaspersky Endpoint Security 更新工作。

要從 Kaspersky 伺服器下載更新軟體套件，需要網際網路連線。

若要啟動或停止更新工作，請執行以下操作：

1. 開啟“程式主視窗”。
2. 選擇“**防護和控制**”頁籤。
3. 點擊 **工作** 區域。
開啟 **工作** 區域。
4. 右鍵點擊顯示包含更新工作名稱相關資訊的右鍵選單。
點擊選單可開啟要對更新工作採取的操作功能表。
5. 請執行以下操作之一：

- 如果您想要啟動更新工作，請從該功能表中選取“**啟動更新**”。
顯示在“**更新**”按鈕右側的更新工作進度狀態將變更為 *正在執行*。
- 如果您想要停止更新工作，請從該功能表中選取“**停止更新**”。
顯示在“**更新**”按鈕右側的更新工作進度狀態將變更為 *已停止*。

回溯上次更新

在資料庫和程式模組進行第一次更新以後，就能夠將資料庫和程式模組回溯至前一版本的功能。

每次使用者開始更新程式時，Kaspersky Endpoint Security 會為目前資料庫和程式模組建立一個備份副本。讓您能夠在必要時將資料庫和程式模組回溯至它們的前一版本。回溯至前一版本這個功能十分有用，例如，當新資料庫版本包含一個無效的簽章而導致 Kaspersky Endpoint Security 封鎖某個安全的應用程式時，回溯操作就會十分有用。

若要回溯到最近更新，請執行以下操作：

1. 開啟“程式主視窗”。
2. 選擇“**防護和控制**”頁籤。
3. 點擊 **工作** 區域。
開啟 **工作** 區域。
4. 右鍵點擊開啟“**更新**”的右鍵選單。
5. 選取“**回溯更新**”。

配置代理伺服器設定

若要設定代理伺服器設定，請執行以下操作：

1. 開啟 [程式設定視窗](#)。
2. 在視窗左側的“**排程工作**”區域中，選取“**更新**”。
程式更新設定將顯示在視窗右方。
3. 在“**代理伺服器**”區域中點擊“**設定**”按鈕。
開啟“**代理伺服器設定**”視窗。
4. 在“**代理伺服器設定**”頁籤中選取“**使用代理伺服器**”核取方塊。
5. 指定代理伺服器設定。
6. 點擊“**確定**”。
7. 要儲存變更，請點擊“**儲存**”按鈕。

您還可以在主應用程式視窗**設定**頁籤上的**進階設定**區域中配置代理伺服器設定。

掃描電腦

病毒對於電腦安全至關重要。定期進行病毒掃描有助於防止因安全等級設定過低或者其他原因導致防護元件未能偵測到惡意軟體進行傳播。

本部分將介紹掃描工作的要求和設定、安全等級、掃描方式和技術，以及如何處理在病毒掃描時 Kaspersky Endpoint Security 尚未處理的檔案。

關於掃描工作

Kaspersky Endpoint Security 將透過以下工作尋找病毒和其他惡意程式並檢查程式模組的完整性：

- **完整掃描**。徹底地掃描整個電腦。Kaspersky Endpoint Security 預設掃描以下物件：
 - 內核記憶體
 - 作業系統啟動時載入的物件
 - 開機磁區
 - 作業系統備份儲存區
 - 所有磁碟機和卸除式裝置
- **關鍵區域掃描**。預設情況下，Kaspersky Endpoint Security 會掃描內核記憶體、執行處理序和磁碟的開啟磁區。
- **自訂掃描**。Kaspersky Endpoint Security 將掃描使用者選擇的物件。您可以掃描下表中的任意物件：
 - 內核記憶體
 - 作業系統啟動時載入的物件
 - 作業系統備份儲存區
 - Outlook 郵箱
 - 所有磁碟機、卸除式和網路磁碟
 - 任何選取的檔案
- **完整性檢查**。Kaspersky Endpoint Security 將檢查程式的模組是否損壞或者被修改。

完整掃描和關鍵區域掃描工作與其他掃描方式有所不同。對於這兩者來說，不建議使用者編輯掃描範圍。

[掃描工作啟動後](#)，它們的完成進度將顯示在正在執行工作的名稱旁邊的欄位中，在 Kaspersky Endpoint Security 主視窗的**防護和控制**標籤的**工作**區域中。

掃描結果和執行掃描工作時發生的事件都將記錄在一個 Kaspersky Endpoint Security 報告中。

開始或停止掃描工作

無論選取的何種掃描工作執行模式，您都可以隨時啟動或停止更新工作。

若要啟動或停止掃描工作，請執行以下操作：

1. 開啟“[程式主視窗](#)”。
2. 選擇“**防護和控制**”頁籤。
3. 點擊 **工作** 區域。
開啟 **工作** 區域。
4. 右鍵點擊顯示包含掃描工作名稱相關資訊的右鍵選單。
操作功能表將顯示在掃描工作上方。
5. 請執行以下操作之一：
 - 如果您想要啟動掃描工作，請從該功能表中選取“**啟動掃描**”。
帶有該掃描工作名稱按鈕右方的工作處理程序狀態將變為“*正在進行*”。
 - 如果您想要停止掃描工作，請從該功能表中選取“**停止掃描**”。
帶有該掃描工作名稱按鈕右方的工作處理程序狀態將變為“*已停止*”。

設定掃描工作設定

若要配置掃描工作設定，請執行以下操作：

- 變更安全防護等級。
您可以選擇某種預設的安全防護等級或手動配置安全性等級的設定。如果您改變了檔案安全防護等級設定，仍可隨時還原到建議的檔案安全防護等級設定。
- 如果偵測到受感染的檔案，請變更 **Kaspersky Endpoint Security** 執行的操作。
- 編輯掃描範圍。
您可以透過新增或刪除掃描物件，或透過變更掃描檔案類型擴充或限制掃描範圍。
- 優化掃描。
您可以最佳化檔案掃描：縮短掃描時間並提高 **Kaspersky Endpoint Security** 的執行速度。這可以透過僅掃描新檔案和上次掃描後經過修改的檔案來實現。此模式適用於簡單檔案和複合檔案。您還可以設定單個檔案的掃描限制。當指定的時間間隔到期時，**Kaspersky Endpoint Security** 將從目前掃描中排除此檔案（除包含多個檔案的存檔和物件之外）。
您也可以啟用 **iChecker** 和 **iSwift** 技術。這些技術可以透過排除上次掃描後未修改的檔案來最佳化檔案掃描速度。
- 設定複合檔案的掃描。
- 設定使用掃描方式。

處於活動狀態時，Kaspersky Endpoint Security 將使用特徵碼分析。在特徵碼分析中，Kaspersky Endpoint Security 會將偵測物件與其資料庫中的記錄進行比對。根據 Kaspersky Lab 專家的建議，特徵分析將處於常時啟動狀態。

您可以使用啟發式分析提高防護效率。在啟發式分析中，Kaspersky Endpoint Security 將分析物件在作業系統中的活動。啟發式分析可以偵測 Kaspersky Endpoint Security 資料庫中尚無記錄的新惡意物件。

- 選取掃描工作執行模式。

如果由於任何原因無法執行掃描工作（例如，當時電腦處於關機狀態），則可以設定錯過的工作，使其在電腦可用時儘快自動執行。

如果已選取“**根據排程**”更新工作執行模式，而且 Kaspersky Endpoint Security 啟動時間與掃描工作執行排程相符，則可以在應用程式啟動後延遲掃描工作的開始。掃描工作只能在 Kaspersky Endpoint Security 啟動後指定時間之後執行。

- 設定以不同使用者帳戶執行掃描工作。
- 指定在連接卸除式磁碟機後對卸除式磁碟機的掃描設定。

變更安全防護等級

Kaspersky Endpoint Security 使用各種設定組合來執行掃描工作。這些儲存在應用程式中的設定組合稱為 *安全防護等級*。有三種預設的安全防護等級：**高**、**建議**和**低**。“**建議**”安全防護等級設定可以看做是最佳化設定。它們由 Kaspersky 專家建議。

要變更安全防護等級：

1. 開啟 [程式設定視窗](#)。
2. 在視窗左側的“**排程工作**”區域中，選擇所需掃描工作的名稱所在的子區域 (**完整掃描**、**關鍵區域掃描**或**自訂掃描**)。
在視窗右側，將顯示掃描工作的設定。
3. 在“**安全防護等級**”區域中執行下列操作：
 - 如果您希望套用一種預設的安全防護等級（**高**、**建議**或**低**），請使用移動滑桿選取。
 - 如果您希望設定自訂安全防護等級，則點擊“**設定**”按鈕，在出現的視窗中指定掃描工作名稱的設定。
您設定自訂安全防護等級之後，“**安全防護等級**”區域中安全防護等級的名稱將變更為“**自訂**”。
 - 如果您希望將安全防護等級變更為“**建議**”，點擊“**預設**”按鈕。
4. 要儲存變更，請點擊“**儲存**”按鈕。

變更對受感染檔案執行的操作

若要變更對受感染檔案執行的操作，請執行以下操作：

1. 開啟 [程式設定視窗](#)。
2. 在視窗左側的“**排程工作**”區域中，選擇所需掃描工作的名稱所在的子區域 (**完整掃描**、**關鍵區域掃描**或**自訂掃描**)。

在視窗右側，將顯示掃描工作的設定。

3. 在“偵測到威脅後的動作”區域，選取所需的模式：

- 自動選擇動作。
- 執行動作。

4. 如果您在先前步驟中選取了“執行動作”，則選取以下核取方塊：

- 如果您希望 Kaspersky Endpoint Security 清除偵測到的威脅，則選取“清除”核取方塊。

若選取此選項，Kaspersky Endpoint Security 則會將 Windows Store 應用程式，套用在“刪除”行動中。

- 如果您希望 Kaspersky Endpoint Security 刪除偵測到威脅的物件，則選取“刪除”核取方塊。
- 如果您希望 Kaspersky Endpoint Security 嘗試對偵測到威脅的物件解毒並且無法解毒時刪除檔案，則選取“解毒”和“刪除”兩個核取方塊。
- 如果您希望 Kaspersky Endpoint Security 在偵測到帶有威脅的物件時不採取任何操作而僅僅是通知使用者這些物件的掃描結果，則清空“解毒”和“刪除”核取方塊。

5. 要儲存變更，請點擊“儲存”按鈕。

產生要掃描的物件清單

若要產生要掃描的物件清單，您可以使用以下兩種方法之一：

- 透過[應用程式主視窗](#)的“防護和控制”頁籤。
- 開啟[程式設定視窗](#)。

此方法僅可用於**完整掃描**和**關鍵區域掃描**工作。只有在**防護和控制**標籤上才可以建立**自訂掃描**工作要掃描的物件清單。

要在應用程式主視窗的“防護和控制”標籤中建立要掃描的物件清單，請執行以下操作：

1. 開啟“程式主視窗”。
2. 選擇“防護和控制”頁籤。
3. 點擊 **工作** 區域。
開啟 **工作** 區域。
4. 右鍵點擊開啟包含工作名稱的行的上下文功能表，然後選擇 **掃描範圍**。
開啟“**掃描範圍**”。
5. 如果您希望將新物件新增至掃描範圍：

- a. 點擊**“新增”**按鈕。
開啟**“選取掃描範圍”**。
 - b. 選取物件並點擊**“新增”**。
“選取掃描範圍”視窗中選取的所有物件都將顯示在**“掃描範圍”**清單內。
 - c. 點擊**“確定”**。
6. 如果您希望變更掃描範圍中某個物件的路徑：
- a. 在掃描範圍中選取此物件。
 - b. 點擊**“編輯”**按鈕。
開啟**“選取掃描範圍”**。
 - c. 在掃描範圍中輸入物件新路徑。
 - d. 點擊**“確定”**。
7. 如果您希望從掃描範圍中刪除某個物件：
- a. 從掃描範圍中選取要刪除的物件。
若要選取多個物件，請按住**“CTRL”**鍵依次選取。
 - b. 點擊**“刪除”**按鈕。
螢幕上將開啟確認刪除視窗。
 - c. 在刪除確認視窗中點擊**“是”**。

您無法刪除或編輯包括在預設掃描範圍中的物件。

8. 要從掃描物件清單中排除一個物件，請在**“掃描範圍”**清單中清空此物件旁邊的核取方塊。
此物件仍保留在要掃描的物件清單中，但當掃描工作執行時，它不會被掃描。
9. 點擊**“確定”**。
10. 要儲存變更，請點擊**“儲存”**按鈕。

要從應用程式設定視窗建立要掃描的物件清單：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的**“排程工作”**區域中，選取所需掃描工作的名稱所在的子區域**“完整掃描”**，或**“關鍵區域掃描”**。
在視窗右側，將顯示掃描工作的設定。
3. 點擊**“掃描範圍”**按鈕。
開啟**“掃描範圍”**。
4. 根據之前說明的步驟 5-10 建立要掃描的物件清單。

選取要掃描的檔案類型

您可以使用以下兩種方法選擇要掃描的檔案類型：

- 透過[應用程式主視窗](#)的“**防護和控制**”頁籤。
- 開啟[程式設定視窗](#)。

此方法僅可用於**完整掃描**和**關鍵區域掃描**工作。只有在**防護和控制**標籤上才可以選擇**自訂掃描**工作要掃描的檔案類型。

要在程式主視窗的“**防護和控制**”標籤中選擇要掃描的檔案類型，請執行以下操作：

1. 開啟“程式主視窗”。
2. 選擇“**防護和控制**”頁籤。
3. 點擊 **工作** 區域。
開啟 **工作** 區域。
4. 右鍵點擊開啟包含工作名稱的行的上下文功能表，然後選擇 **設定**。
開啟所選掃描工作名稱的視窗。
5. 在所選掃描工作名稱的視窗中選取“**範圍**”頁籤。
6. 在“**檔案類型**”區域中，請指定您想要在所選掃描工作執行時掃描的檔案類型：
 - 如果您希望掃描所有檔案，請選取“**所有檔案**”。
 - 如果您希望根據其格式掃描最易被感染的檔案，請選取“**依格式掃描檔案**”。
 - 如果您希望依據其副檔名掃描通常最容易受感染的檔案，請選取“**依副檔名掃描檔案**”。

選取需要掃描的檔案類型時，請考慮以下資訊：

- 部分檔案格式（如 TXT），惡意程式碼入侵並執行的可能性相當低。同時，部分檔案格式會包含或可能會包含惡意程式碼（如 .exe、.dll 和 .doc）。這些檔案中，惡意程式碼入侵並執行的可能性高。
 - 入侵者可能會把可執行檔案的副檔名重新命名為 .txt，然後將其中的病毒或其他惡意程式傳送到您的電腦中。如果您按照副檔名選取掃描檔案，程式將在掃描期間略過此檔案。如果選擇按格式掃描檔案，則檔案病毒防護會分析檔案標頭，和副檔名無關。如果這一分析表明此檔案的格式為 EXE，應用程式會掃描它。
7. 在掃描工作名稱的視窗中選取“**確定**”按鈕。
 8. 要儲存變更，請點擊“**儲存**”按鈕。

要從應用程式設定視窗選擇要掃描的檔案類型：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**排程工作**”區域中，選取所需掃描工作的名稱所在的子區域“**完整掃描**”，或“**關鍵區域掃描**”。

在視窗右側，將顯示掃描工作的設定。

3. 在“**安全防護等級**”區域中點擊“**設定**”按鈕。
開啟所選掃描工作名稱的視窗。
4. 在所選掃描工作名稱的視窗中選取“**範圍**”頁籤。
5. 完成先前說明中的步驟 5-7。

最佳化檔案掃描

要最佳化檔案掃描，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**排程工作**”區域中，選擇所需掃描工作的名稱所在的子區域 (**完整掃描**、**關鍵區域掃描**或**自訂掃描**)。
在視窗右側，將顯示掃描工作的設定。
3. 在“**安全防護等級**”區域中點擊“**設定**”按鈕。
開啟所選掃描工作名稱的視窗。
4. 在開啟的視窗中選取“**範圍**”頁籤。
5. 在“**掃描最佳化**”區域中執行下列操作：
 - 選取“**只掃描新增及變更的檔案**”核取方塊。
 - 選取“**略過掃描時間超過以下值的檔案**”核取方塊，並指定單個檔案掃描時間長度（以秒為單位）。
6. 點擊“**確定**”。
7. 要儲存變更，請點擊“**儲存**”按鈕。

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程式，必須將複合檔案解壓縮，但是這可能會降低掃描速度。您可以限制掃描複合檔案的設定，從而加快掃描速度。

若要設定複合檔案的掃描，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**排程工作**”區域中，選擇所需掃描工作的名稱所在的子區域 (**完整掃描**、**關鍵區域掃描**或**自訂掃描**)。
在視窗右側，將顯示掃描工作的設定。
3. 在“**安全防護等級**”區域中點擊“**設定**”按鈕。

開啟所選掃描工作名稱的視窗。

4. 在開啟的視窗中選取“**範圍**”頁籤。
5. 在“**掃描複合檔案**”區域中，指定要掃描的複合檔案：存檔、安裝套裝程式、Office 格式檔案、電子郵件格式檔案或密碼防護的存檔。
6. 如果在“**掃描優化**”區域中清空了“**僅掃描新的變更的檔按**”核取方塊，如果您希望為每個類型的複合檔案指定掃描該類型的所有檔案還是只掃描新檔案，則點擊複合檔案類型名稱旁邊的“**全部/新建**”。
點擊連結會變更它的值。
如果選取“**只掃描新增及變更的檔案**”核取方塊，則只掃描新檔案。
7. 點擊 **附加** 按鈕。
螢幕上將開啟**複合檔案** 視窗。
8. 在 **容量限制** 區域中可執行下列操作：
 - 如果不希望解壓縮大型複合檔案，請選取“**複合檔案大於指定值時不解壓縮**”核取方塊，並在“**最大檔案容量**”欄位中指定所需值。
 - 如果希望解壓縮大型複合檔案而不考慮其容量，請取消選取“**複合檔案大於指定值時不解壓縮**”核取方塊。

無論是否選取“**不解壓大型複合檔案**”核取方塊，Kaspersky Endpoint Security 均會掃描從存檔案中提取的大型檔案。

9. 點擊“**確定**”。
10. 在掃描工作名稱的視窗中選取“**確定**”按鈕。
11. 要儲存變更，請點擊“**儲存**”按鈕。

選擇掃描方式

若要選取掃描方式，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**排程工作**”區域中，選擇所需掃描工作的名稱所在的子區域 (**完整掃描**、**關鍵區域掃描**或**自訂掃描**)。
在視窗右側，將顯示掃描工作的設定。
3. 在“**安全防護等級**”區域中點擊“**設定**”按鈕。
開啟所選掃描工作名稱的視窗。
4. 在開啟的視窗中選擇**附加** 頁籤。
5. 如果您希望應用程式在執行掃描工作時使用啟發式分析，請在“**掃描方式**”區域中，選取“**啟發式分析**”核取方塊。然後使用捲軸設定啟發式分析等級：**輕度掃描**、**中度掃描**或**深度掃描**。
6. 點擊“**確定**”。

7. 要儲存變更，請點擊“儲存”按鈕。

使用掃描技術

若要使用掃描技術，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**排程工作**”區域中，選擇所需掃描工作的名稱所在的子區域 (**完整掃描**、**關鍵區域掃描**或**自訂掃描**)。
在視窗右側，將顯示掃描工作的設定。
3. 在“**安全防護等級**”區域中點擊“**設定**”按鈕。
開啟所選掃描工作名稱的視窗。
4. 在開啟的視窗中選擇**附加** 頁籤。
5. 在“**掃描技術**”區域，選取您要在掃描期間使用技術名稱旁邊的核取方塊。
6. 點擊“**確定**”。
7. 要儲存變更，請點擊“儲存”按鈕。

選取掃描工作執行模式

若要選取掃描工作執行模式，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**排程工作**”區域中，選擇所需工作的名稱所在的子區域 (**完整掃描**、**關鍵區域掃描**或**自訂掃描**)。
在視窗右側，將顯示掃描工作的設定。
3. 點擊 **執行模式** 按鈕。
“**執行模式**”標籤中將顯示帶有選定工作內容的視窗。
4. 在“**執行模式**”區域中，選取工作執行模式：**手動**或**根據排程**。
5. 如果您選取了“**根據排程**”選項，則指定排程設定。為此，請參閱以下執行操作：
 - a. 在“**頻率**”下拉式功能表清單中，選取工作執行頻率 (**分鐘**、**小時**、**天**、**每週**、**在指定時間**、**每個月**或者在**程式啟動後**、**每次更新後**)。
 - b. 根據選定的頻率，配置指定工作執行排程的進階設定。
 - c. 如果您希望 Kaspersky Endpoint Security 儘快執行錯過的掃描工作，請勾選“**執行錯過的工作**”核取方塊。

如果在“**頻率**”下拉清單中選取“**分鐘**”、“**小時**”、“**在程式啟動後**”或“**每次更新後**”，則“**執行略過的工作**”核取方塊無法使用。

- a. 如果在電腦資源有限時希望 Kaspersky Endpoint Security 暫停工作，請選取“**僅在電腦空閒時執行**”核取方塊。

此排程選項有助於節省電腦資源。

6. 點擊“**確定**”。

7. 要儲存變更，請點擊“**儲存**”按鈕。

使用不同使用者帳戶啟動掃描工作

預設情況下，掃描工作在登入到作業系統的使用者帳戶權限下執行。但您可能需要使用不同使用者帳戶執行掃描工作。您可以在掃描工作的設定中指定一個擁有適當權限的使用者，然後使用此使用者帳戶執行掃描工作。

若要設定使用不同使用者帳戶啟動掃描工作，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**排程工作**”區域中，選擇所需工作的名稱所在的子區域 (**完整掃描**、**關鍵區域掃描**或**自訂掃描**)。在視窗右側，將顯示掃描工作的設定。
3. 點擊 **執行模式** 按鈕。
“**執行模式**”標籤中將顯示帶有選定工作內容的視窗。
4. 在“**執行模式**”頁籤的“**使用者**”區域中勾選“**工作執行身分**”選項。
5. 在“**名稱**”欄位中，輸入需要使用其權限啟動掃描工作的使用者帳戶名稱。
6. 在“**密碼**”欄位中，輸入需要使用其權限啟動掃描工作的使用者密碼。
7. 點擊“**確定**”。
8. 要儲存變更，請點擊“**儲存**”按鈕。

掃描連線到電腦的卸除式磁碟

某些惡意程式會透過區域網路和卸除式磁碟攻擊作業系統的弱點複製自身。Kaspersky Endpoint Security 允許您掃描連線到電腦的卸除式磁碟有無病毒和其他惡意程式。

若要設定掃描連線的卸除式磁碟，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側，選擇“**排程工作**”區域。
工作設定將顯示在視窗右方。

3. 在“**連接時掃描卸除式磁碟**”區域，請從“**連接卸除式磁碟時的動作**”下拉清單中設定操作：

- **不掃描**
- **詳細掃描**

在此模式中，Kaspersky Endpoint Security 將掃描卸除式磁碟中所有檔案，包括複合物件在內的檔案。

- **快速掃描**

在此模式中，Kaspersky Endpoint Security 僅掃描疑似感染檔案，不會解壓縮複合物件。

4. 如果您希望 Kaspersky Endpoint Security 只掃描其大小不超過指定值的卸除式裝置，請選取“**卸除式裝置最大容量**”核取方塊，並在旁邊的欄位中指定一個值（以百萬位元組為單位）。

5. 要儲存變更，請點擊“**儲存**”按鈕。

處理未處理的檔案

本章節介紹如何處理 Kaspersky Endpoint Security 在掃描電腦以尋找有無病毒和其他威脅時未處理的受感染檔案和疑似感染的檔案。

關於未處理的檔案

Kaspersky Endpoint Security 將記錄偵測到威脅活動但未處理的檔案的相關資訊。此資訊在未處理檔案清單中以事件的形式記錄。

Kaspersky Endpoint Security 在掃描電腦檢視有無病毒和其他威脅時，根據指定應用程式設定對於受感染的檔案執行下列操作，則受感染的檔案視為 *已處理*：

- 解毒。
- 刪除。
- 無法解毒則刪除。

Kaspersky Endpoint Security 在掃描電腦檢視有無病毒和其他威脅時，由於任何原因，根據指定的應用程式設定未能對受感染檔案執行操作時，受感染的檔案將視為 *無法處理*。

在下列情況中可能出現此狀況：

- 掃描的檔案無法使用（例如，檔案位於網路磁碟或沒有讀寫權限的卸除式磁碟上）。
- 在掃描工作的“**偵測到威脅後的動作**”區域中選取的操作為“**通知**”，當顯示關於受感染檔案的通知時，使用者選取“**略過**”操作。

您可在更新資料庫和程式模組後，對未處理檔案清單中的檔案手動啟動自訂掃描工作。掃描後檔案狀態可能會改變。根據檔案狀態，您可對其執行所需操作。

例如，您可以執行下列操作：

- **刪除帶有感染狀態的檔案。**

- 還原包含重要資訊的受感染檔案，並還原標記為 *已解毒* 或 *未解毒*。
- 隔離帶有 *疑似感染* 狀態的檔案。

管理未處理檔案清單

未處理檔案清單將以表格的形式顯示。

您可以對未處理的檔案執行以下操作：

- 檢視未處理檔案清單。
- 使用目前的 **Kaspersky Endpoint Security** 資料庫和模組掃描未處理檔案。
- 將檔案從未處理檔案清單還原到原資料夾或者根據您的選取還原到其他資料夾（當原資料夾無法寫入時）。
- 刪除未處理檔案清單中的檔案。
- 開啟未處理的檔案原來所在的資料夾。

您也可在管理表中資料時執行以下操作：

- 透過條件值或者自訂篩選條件篩選未處理檔案事件。
- 使用未處理檔案事件搜尋功能。
- 排序未處理檔案事件。
- 變更未處理檔案事件清單中的顯示順序和條件列設定。
- 為未處理檔案事件分組。

如有需要，您可以將所選未處理檔案事件複製到剪貼簿。

啟動未處理檔案自訂掃描

您可以手動啟動未處理檔案的自訂掃描工作。如果，例如由於某種原因上次掃描被中斷，或者如果您希望在最近更新資料庫和應用程式模組後重新掃描未處理的檔案則可以啟動掃描。

啟動未處理檔案的自訂掃描

1. 開啟“[程式主視窗](#)”。
2. 在程式主視窗上半部分，點擊“**隔離區**”連結開啟“**儲存**”視窗。
3. 在“**儲存**”視窗中，選擇“**未處理的檔案**”標籤。
4. 在“**未處理的檔案**”頁籤上的表格中，選取您想要掃描的一個或多個檔案事件。
若要選擇多個事件，請按住“**CTRL**”鍵依次選擇事件。

5. 以下列方式啟動自訂掃描工作：

- 點擊“**重新掃描**”按鈕。
- 點擊右鍵顯示右鍵選單，然後選取“**重新掃描**”項。

刪除未處理檔案清單中的檔案

若要刪除未處理檔案清單中的檔案，請執行以下操作：

1. 開啟“[程式主視窗](#)”。
2. 在程式主視窗上半部分，點擊“**隔離區**”連結開啟“**儲存**”視窗。
3. 在“**儲存**”視窗中，選擇“**未處理的檔案**”標籤。
4. 在“**未處理的檔案**”頁籤上的表格中，選取要刪除的一個或多個檔案事件。
若要選擇多個事件，請按住“**CTRL**”鍵依次選擇事件。
5. 透過下列方式之一刪除檔案：
 - 點擊“**刪除**”按鈕。
 - 右鍵點擊以開啟右鍵選單並選取“**刪除**”。

弱點掃描

本章節介紹關於弱點掃描工作的細節和設定，並且說明如何管理 Kaspersky Endpoint Security 在執行弱點掃描工作時偵測到的弱點清單。

檢視執行中應用程式的弱點資訊

如果將 Kaspersky Endpoint Security 安裝在執行 Microsoft Windows 以做工作站之用的電腦上，則關於正在執行程式的弱點資訊可使用。如果將 Kaspersky Endpoint Security 安裝在執行 [Microsoft Windows 以做檔案伺服器之用](#)的電腦上，則該資訊可使用。

若要檢視執行中應用程式的弱點資訊，請執行以下操作：

1. 開啟“[程式主視窗](#)”。
2. 選擇“**防護和控制**”頁籤。
3. 開啟“**端點控制**”區域。
4. 點選“**應用程式活動監控**”按鈕。

“**應用程式活動監控**”標籤上的“**應用程式權限控制視窗**”將開啟。“**應用程式活動監控**”包含作業系統中執行的應用程式活動的概要資訊。由“弱點監控”元件確定的執行中應用程式的弱點狀態將顯示在“**弱點嚴重性**”列中。

關於弱點掃描工作

弱點掃描主要是針對於操作系統時產生的弱點，例如，在開發程式時的疏忽、強度較弱的密碼或者惡意軟體導致的弱點。在掃描弱點時，應用程式將分析作業系統並搜尋 Microsoft 和其他生產廠家的應用程式的異常情況和損壞設定。

弱點掃描可執行作業系統安全診斷並偵測那些可能會被入侵者用於傳播惡意物件並獲得個人資訊的軟體功能。

[弱點掃描工作啟動](#)後，它們的完成進度將顯示在工作名稱旁邊的“**弱點掃描**”工作中，在 Kaspersky Endpoint Security 主視窗的“**防護和控制**”標籤的“**工作**”區域中。

弱點掃描工作的結果記錄在[報告](#)中。

啟動或停止弱點掃描工作

不管為弱點掃描工作選取的執行模式為何，您都可以在任意時間啟動或停止工作。

若要啟動或停止弱點掃描工作，請執行以下操作：

1. 開啟“[程式主視窗](#)”。
2. 選擇“**防護和控制**”頁籤。

3. 點擊 **工作** 區域。
開啟 **工作** 區域。
4. 右鍵點擊顯示包含弱點掃描工作名稱相關資訊的右鍵選單。
操作功能表將顯示在弱點掃描工作上方。
5. 請執行以下操作之一：
 - 要啟動弱點掃描工作，請在功能表中選取“**啟動掃描**”。
帶有該弱點掃描工作名稱的按鈕右方的工作處理程序狀態將變為“**正在執行**”。
 - 要停止弱點掃描工作，請在功能表中選取“**停止掃描**”。
帶有該弱點掃描工作名稱的按鈕右方的工作處理程序狀態將變為“**已停止**”。

配置弱點掃描設定

若要配置弱點掃描設定，請執行以下操作：

- 建立弱點掃描範圍。
您可以透過新增或刪除要掃描弱點的應用程式的方式延伸或縮小掃描範圍。
- 選取弱點掃描工作的執行模式。
如果由於任何原因無法執行掃描工作（例如，當時電腦處於關機狀態），則可以設定錯過的工作，使其在電腦可用時儘快自動執行。
- 設定工作在不同的使用者帳戶的權限下執行。
預設情況下，掃描工作在登入到作業系統的使用者帳戶權限下執行。但您可能需要使用不同使用者帳戶執行掃描工作。您可以在工作設定中指定一個擁有適當權限的使用者，然後使用此使用者帳戶執行工作。

建立弱點掃描範圍

弱點掃描範圍是軟體供應商和指向軟體安裝資料夾的路徑（例如，所有 Microsoft 應用程式都安裝在 Program Files 資料夾中）。

若要建立弱點掃描範圍，請執行以下操作：

1. 開啟 [程式設定視窗](#)。
2. 在視窗左側的“**排程工作**”區域中選擇“**弱點掃描**”。
弱點掃描工作設定將顯示在視窗右方。
3. 在“**掃描範圍**”區域中：
 - a. 要使用 Kaspersky Endpoint Security 尋找電腦上安裝的 Microsoft 應用程式的弱點，請選取“**Microsoft**”核取方塊。
 - b. 要使用 Kaspersky Endpoint Security 尋找電腦上安裝的除 Microsoft 應用程式外的所有應用程式的弱點，請選取“**其他軟體廠商**”核取方塊。

- c. 在“附加弱點掃描範圍”視窗中點選“設定”按鈕。
“弱點掃描範圍”視窗將開啟。
 - d. 建立弱點掃描範圍，可使用“新增”和“刪除”按鈕。
 - e. 在“弱點掃描範圍”視窗中點擊“確定”。
4. 要儲存變更，請點擊“儲存”按鈕。

選取弱點掃描工作的執行模式

若要選取弱點掃描工作執行模式，請執行以下操作：

1. 開啟[程式設定視窗](#)。
 2. 在視窗左側的“排程工作”區域中選擇“弱點掃描”。
弱點掃描工作設定將顯示在視窗右方。
 3. 點擊 **執行模式** 按鈕。
這將開啟“弱點掃描”視窗的“執行模式”頁籤。
 4. 在“執行模式”區域中為開始掃弱點描工作選取以下執行模式：
 - 如果您希望手動開始弱點掃描工作，請選取“**手動**”。
 - 如果您希望為弱點掃描工作設定一個啟動排程，請選取“**根據排程**”。
 5. 請執行以下操作之一：
 - 如果選取“**手動**”選項，請前往本說明的第 6 步。
 - 如果您選取“**根據排程**”選項，請指定該弱點掃描工作的具體啟動設定。為此，請參閱以下執行操作：
 - a. 在“**頻率**”下拉清單中指明何時開始弱點掃描工作。選取以下選項之一：“**天**”、“**每週**”、“**在指定時間**”、“**每月**”、“**在程式啟動後**”或“**在每次更新後**”。
 - b. 根據“**頻率**”下拉清單中的選取項，指定弱點掃描工作啟動時間的值。
 - c. 如果您希望 Kaspersky Endpoint Security 盡快開始錯過的弱點掃描工作，請選取“**執行錯過的工作**”核取方塊。
- 如果在“**頻率**”下拉清單中選取“**在程式啟動後**”或“**每次更新後**”，則“**執行錯過的工作**”核取方塊無法使用。
6. 點擊“**確定**”。
 7. 要儲存變更，請點擊“**儲存**”按鈕。

使用不同使用者帳戶的權限啟動弱點掃描工作

預設情況下，弱點掃描工作在登入到作業系統的使用者帳戶下啟動。但您可能需要使用不同使用者帳戶執行弱點掃描工作。您可以在弱點掃描工作的設定中指定一個擁有適當權限的使用者，然後使用該使用者帳戶執行弱點掃描工作。

若要設定在不同使用者帳戶下弱點掃描工作的啟動，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**排程工作**”區域中選擇“**弱點掃描**”。
- 弱點掃描工作設定將顯示在視窗右方。
3. 點擊 **執行模式** 按鈕。
- 這將開啟“**弱點掃描**”視窗的“**執行模式**”頁籤。
4. 在“**執行模式**”頁籤的“**使用者**”區域中勾選“**工作執行身分**”選項。
5. 在“**名稱**”欄位中輸入您希望用來啟動弱點掃描工作的使用者帳戶的名稱。
6. 在“**密碼**”欄位中輸入您希望用來啟動弱點掃描工作的使用者帳戶的密碼。
7. 點擊“**確定**”。
8. 要儲存變更，請點擊“**儲存**”按鈕。

管理弱點清單

管理弱點清單時，您可以執行下列操作：

- 檢視弱點清單。
- 更新資料庫和程式模組後再次啟動弱點掃描工作。
- 在單獨的區域中檢視弱點的詳細資訊及其修復建議。
- 隱藏弱點清單中選取的項目。
- 篩選弱點清單的危險層級。
- 按重要性等級，以及 *已修復* 和 *隱藏* 狀態篩選弱點清單。

您也可在管理表中資料時執行以下操作：

- 透過使用自訂篩選條件刪選弱點清單。
- 使用弱點搜尋功能。
- 將弱點清單中的項目排序。

- 變更弱點清單中顯示的順序和列設定。
- 將弱點清單中的項目分類。




關於弱點清單

Kaspersky Endpoint Security 將在弱點清單中記錄[弱點掃描工作](#)的結果。

在您檢視特定弱點並執行建議的修復操作之後，Kaspersky Endpoint Security 會將弱點的狀態變更為 *已修復*。

如果您不希望在弱點清單中顯示指定弱點項目，您可選取隱藏這些項目。Kaspersky Endpoint Security 將其狀態變更為 *隱藏*。

弱點清單以表格的形式顯示。每個表格行包含下列資訊：

- 指示弱點嚴重性等級的圖示。有以下弱點嚴重性等級：
 - 圖示 。“**緊急**”。此嚴重性等級將套用於必須立即修補的高度危險的弱點。入侵者會攻擊此等級的弱點以感染作業系統或存取使用者的個人資料。Kaspersky Lab 建議您迅速修復所有所需的步驟修復“緊急”安全等級的弱點。
 - 圖示 。“**重要**”。此嚴重性等級將套用於需要儘快修補的重要弱點。入侵者可以入侵該等級的弱點。入侵者目前不會主動入侵“重要”安全等級的弱點。Kaspersky Lab 建議您採取所有步驟修復“重要”安全等級的弱點。
 - 圖示 。“**警告**”。此嚴重性等級套用於可延遲修補的弱點。但是此類弱點在將來會對電腦的安全造成威脅。
- 弱點 ID。
- 偵測到存在弱點的應用程式名稱。
- 弱點簡要介紹。
- 數位簽章中指定的軟體發佈者相關資訊。
- 修復弱點所採取操作的結果。

再次啟動弱點掃描工作

要更新有關先前所檢查弱點的資訊，您可以重新啟動弱點掃描工作。如果由於其他原因弱點掃描被中斷或者如果您希望在[資料庫和應用程式模組更新後](#)掃描電腦查找弱點，則您需要重新開機掃描工作。

要再次啟動弱點掃描工作，請執行以下操作：

1. 開啟“[程式主視窗](#)”。
2. 在程式主視窗上半部分，點擊“**隔離區**”連結開啟“**儲存**”視窗。
3. 在“**儲存**”視窗中選擇“**弱點**”標籤。

在“**弱點**”頁籤中含有一個 Kaspersky Endpoint Security 在弱點掃描工作中已偵測到的弱點清單。

4. 在“儲存”視窗下方，點擊“重新掃描”按鈕。

Kaspersky Endpoint Security 將在弱點清單中更新詳細的弱點資訊。

透過安裝建議的修補程式修補的弱點的狀態在再次執行弱點掃描後不會變更。

修復弱點

您可以透過安裝作業系統更新、變更應用程式設定或者安裝應用程式補丁等方式修復弱點。

偵測到的弱點可能不應用於已安裝的應用程式而適用於它們的副本。只有在已經安裝應用程式的情況下補丁才能夠修復弱點。

要修復弱點，請執行以下操作：

1. 開啟“[程式主視窗](#)”。
2. 在程式主視窗上半部分，點擊“**隔離區**”連結開啟“**儲存**”視窗。
3. 在“**儲存**”視窗中選擇“**弱點**”標籤。

在“**弱點**”頁籤中含有一個 Kaspersky Endpoint Security 在弱點掃描工作中已偵測到的弱點清單。

4. 在弱點清單中選取與對應弱點對應的項目。

帶有此弱點資訊和建議如何修復弱點的區域將出現在弱點清單的底部。

每個所選弱點均包含下列資訊：

- 偵測到存在弱點的應用程式名稱。
 - 偵測到存在弱點的應用程式版本。
 - 弱點安全性等級。
 - 弱點 ID。
 - 上一次弱點偵測的日期和時間。
 - 關於如何修復此弱點的建議（例如：指向某作業系統更新或應用程式修復的連結）。
 - 指向某含有此弱點敘述的網站連結。
5. 要瀏覽此弱點的詳細敘述，請點擊“**附加資訊**”連結開啟一個網站頁面，此頁面中將含有與所選弱點相關的威脅的詳細敘述。您可從 <http://www.secunia.com> 網站上下載目前程式版本所需更新並進行安裝。
 6. 選取以下方式修復弱點：
 - 如果此應用程式有可用的一個或多個修補程式，請按照位於修補程式名稱旁邊的說明安裝必需修補程式。
 - 如果有可用的作業系統更新，請按照位於更新名稱旁邊的說明安裝必需更新。

當您完成修復或更新安裝後，弱點即修復完成。Kaspersky Endpoint Security 將為此弱點分配一個表明其已修復的狀態。已修復的弱點項目在弱點清單中會顯示為灰色。

7. 如果視窗下部沒有提供關於如何修復某弱點的資訊，您可以在 Kaspersky Endpoint Security 資料庫和模組更新後重新啟動弱點掃描工作。因為 Kaspersky Endpoint Security 根據弱點資料庫掃描系統中的弱點，在應用程式更新後可能會出現含有某個已修復的弱點的項目。

隱藏弱點清單中的項目

您可以隱藏弱點清單中選取的項目。Kaspersky Endpoint Security 將為弱點清單中選定並標記為隱藏的項目分配“**隱藏**”狀態。然後您可以按照 [隱藏](#) 狀態值 [篩選弱點清單](#)。

要隱藏弱點清單中的項目，請執行以下操作：

1. 開啟“[程式主視窗](#)”。
2. 在程式主視窗上半部分，點擊“**隔離區**”連結開啟“**儲存**”視窗。
3. 在“**儲存**”視窗中選擇“**弱點**”標籤。
在“**弱點**”頁籤中含有一個 Kaspersky Endpoint Security 在弱點掃描工作中已偵測到的弱點清單。
4. 在弱點清單中，選取您希望隱藏的弱點項目。
帶有此弱點資訊和建議如何修復弱點的區域將出現在弱點清單的底部。
5. 點擊“**隱藏**”按鈕。
Kaspersky Endpoint Security 將為所選弱點分配“**隱藏**”狀態。帶有“**隱藏**”狀態的弱點項目將移動至弱點清單的末尾並淡出。
6. 若要在弱點清單中隱藏有關弱點的項目，請選取清單頂部的“**隱藏**”核取方塊。

按嚴重性等級篩選弱點清單

如果您希望按嚴重性等級篩選弱點清單，請執行以下操作：

1. 開啟“[程式主視窗](#)”。
2. 在程式主視窗上半部分，點擊“**隔離區**”連結開啟“**儲存**”視窗。
3. 在“**儲存**”視窗中選擇“**弱點**”標籤。
在“**弱點**”頁籤中含有一個 Kaspersky Endpoint Security 在弱點掃描工作中已偵測到的弱點清單。三種弱點嚴重性等級的圖示（警告、重要、關鍵）將顯示在“**顯示嚴重性**”列的弱點清單上部。透過點擊這些圖示，您可以按嚴重性等級篩選弱點清單。
4. 點擊一個、兩個或三個弱點嚴重性等級。比對選定嚴重等級的弱點將顯示在清單中。若要停止在清單中顯示比對特定嚴重性等級的弱點，請再次點擊相關嚴重性等級圖示。如果未選取嚴重性等級，則弱點清單為空。

您關閉“**儲存**”視窗時，程式將儲存指定的弱點項目篩選條件。

按已修復和隱藏狀態值篩選弱點清單

如果您希望按已修復和隱藏狀態值篩選弱點清單，請執行以下操作：

1. 開啟“[程式主視窗](#)”。
2. 在程式主視窗上半部分，點擊“**隔離區**”連結開啟“**儲存**”視窗。
3. 在“**儲存**”視窗中選擇“**弱點**”標籤。
在“**弱點**”頁籤中含有一個 Kaspersky Endpoint Security 在弱點掃描工作中已偵測到的弱點清單。
4. 表示弱點狀態的核取方塊顯示在“**顯示軟體弱點**”設定旁邊。您可以採用以下方式篩選 *已修復* 狀態的弱點清單：
 - 如果您希望在弱點清單中顯示已修復弱點項目，請選取“**已修復**”核取方塊。已修復弱點的項目在弱點清單中將顯示為灰色。
 - 如果您希望在弱點清單中隱藏已修復弱點項目，請清空“**已修復**”核取方塊。
5. 您可以採用以下方式篩選 *隱藏* 狀態的弱點清單：
 - 如果您希望在弱點清單中顯示隱藏弱點項目，請選取“**隱藏**”核取方塊。隱藏弱點的項目在弱點清單中將顯示為灰色。
 - 如果您希望在弱點清單中隱藏掉隱藏弱點項目，請清空“**隱藏**”核取方塊。

您關閉“**儲存**”視窗後，程式將不儲存指定的弱點項目篩選條件。

檢查應用程式模組的完整性

該區域包含完整性檢查工作的技術規範和設定的資訊。

關於完整性檢查工作

Kaspersky Endpoint Security 將檢查應用程式安裝資料夾內的應用程式模組以檢查任何損壞或修改。如果應用程式模組擁有錯誤的數位簽章，則此模組被認定為損壞。

[完整性檢查工作啟動後](#)，它們的完成進度將顯示在**工作名稱**旁邊的欄位中，在 Kaspersky Endpoint Security 主視窗的**防護和控制**標籤的工作區域中。

完整性檢查工作的結果將記錄在[報告](#)中。

啟動或停止完整性檢查工作

無論選取的何種執行模式，您都可以隨時啟動或停止完整性檢查工作。

若要啟動或停止完整性檢查工作，請執行以下操作：

1. 開啟[程式主視窗](#)。
2. 選擇**防護和控制**頁籤。
3. 開啟**工作**區域。
4. 右鍵點擊顯示包含完整性檢查工作名稱相關資訊的右鍵選單。
5. 請執行以下操作之一：
 - 要啟動完整性檢查工作，請在功能表中選取**啟動掃描**。
帶有該工作名稱按鈕右方的工作處理程序狀態將變為**正在進行**。
 - 如果您想要停止完整性檢查工作，請從該功能表中選取**停止掃描**。
帶有該工作名稱按鈕右方的工作處理程序狀態將變為**已停止**。

選取完整性檢查工作的執行模式

若要選取完整性檢查工作的執行模式：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的**排程工作**區域中，選取**完整性檢查**。
完整性檢查工作設定將顯示在視窗右方。

3. 在“**執行模式**”區域中，選取以下選項之一：

- 如果您希望手動開始完整性檢查工作，請選取“**手動**”。
- 如果您希望為完整性檢查工作設定一個啟動排程，請選取“**根據排程**”。

4. 如果您在上個步驟中選取了“**根據排程**”選項，則指定工作執行排程的設定。為此，請參閱以下執行操作：

- a. 在“**頻率**”下拉清單中，指定啟動完整性檢查工作的時間。從以下選項中選取一個選項：**分鐘**、**小時**、**天**、**每週**、**在指定時間**、**每月**或者**在程式啟動後**。
- b. 根據從“**頻率**”下拉清單中選取的項目，指定定義工作啟動時間的設定值。
- c. 如果您希望 Kaspersky Endpoint Security 儘快執行錯過的完整性檢查工作，請勾選“**執行錯過的工作**”選框。

如果從“**頻率**”下拉清單中選取“**小時**”、“**分鐘**”或“**應用程式啟動之後**”，則“**執行錯誤的工作**”核取方塊無法使用。

- d. 如果在電腦資源有限時希望 Kaspersky Endpoint Security 暫停工作，請選取“**僅在電腦空閒時執行**”核取方塊。

此排程選項有助於節省電腦資源。

5. 點擊“**確定**”。


6. 要儲存變更，請點擊“**儲存**”按鈕。

管理報告

本章節介紹如何配置報告設定和管理報告。

管理報告的原則




每個 Kaspersky Endpoint Security 元件的操作、每次掃描工作、完整性控制工作、更新工作和弱點掃描工作的表現以及應用程式的整體操作的相關資訊將記錄在報告中。

報告資料將以表格的形式呈現，此表格中包含一個事件清單。每個表格行都含有一個單獨事件的相關資訊。事件內容位元於表格列中。部分列為複合列，包含有帶附加內容的嵌套列。若要檢視附加內容，您必須按圖表名稱旁邊的  按鈕。在各種不同元件或各種工作執行過程中記錄下來的事件擁有不同的內容整合。

以下報告可用：

- **系統稽核**報告。包含在應用程式操作和與使用者互動時記錄的事件的相關資訊。
- **所有防護元件**報告。包含以下 Kaspersky Endpoint Security 元件執行時記錄的事件的相關資訊：
 - 檔案防護。
 - 郵件防護。
 - 網頁防護。
 - 即時通訊防護。
 - 系統監視器。
 - 防火牆。
 - 網路攻擊防護。
 - BadUSB 攻擊防護。
- Kaspersky Endpoint Security 元件或工作執行報告。
- **“加密”**報告。包含資料加密和解密期間所發生事件的資訊。

報告使用以下事件重要性等級：

- **資訊事件**。圖示 。通常不包含重要資訊的一般事件。
- **“重要事件”**。圖示 。顯示了 Kaspersky Endpoint Security 操作上的重要情況而需要注意的事件。
- **“緊急事件”**。圖示 。十分重要的事件以及 Kaspersky Endpoint Security 執行問題或在防護使用者電腦時的弱點。

為便於處理報告，您可以透過以下幾種方法修改資料的顯示方式：

- 透過各種不同的規則篩選事件清單。
- 使用搜尋功能尋找特定的事件。

- 在單獨的區域中檢視所選事件。
- 按照每個表格列的值排列事件清單。
- 顯示和隱藏按照事件篩選群組的事件。
- 變更報告中表格列的順序和排列。

如有需要，您可以將產生的報告儲存為文字檔案。

您還可以[刪除合併成組的 Kaspersky Endpoint Security 元件和工作的報告資訊](#)。此時，Kaspersky Endpoint Security 將刪除選取報告從開始到目前時間的所有項目。

配置報告設定

您可以透過以下方式管理報告設定：

- 設定最長報告儲存時間。

Kaspersky Endpoint Security 記錄的事件報告的最長儲存時間預設為 30 天。在此時間之後，Kaspersky Endpoint Security 將自動移除報告檔案中的最早項目。您可以取消時間限制或者變更最大報告儲存期限。

- 設定報告檔案的最大容量。

您可以指定包含報告的檔案的最大容量。預設情況下，最大報告檔案容量為 1024 MB。要避免超過最大報告檔案容量，當達到最大報告檔案容量時，Kaspersky Endpoint Security 將自動刪除報告檔案中的最早項目。您可以取消報告檔案容量限制或設定不同值。

設定最大報告儲存時間

要修改報告的最大儲存期限，請執行下列操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗的左側上，點選**進階設定** 選擇 **報告和儲存**。
3. 在視窗右側的**報告參數**區域中，執行下列操作：
 - 要限制報告儲存期限，請選取**儲存報告不超過**核取方塊。在**儲存報告不超過**核取方塊旁邊的欄位中，指定報告的最長儲存期限。
預設的報告最長儲存期限是 30 天。
 - 要取消對報告儲存期限的限制，請清除**儲存報告不超過**按鈕。

預設情況下啟用對報告儲存期限的限制。

4. 要儲存變更，請點擊**儲存**按鈕。

設定報告檔案的最大容量

要設定報告檔案的最大容量，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗的左側上，點選**進階設定** 選擇 **報告和儲存**。
3. 在視窗右側的**“報告參數”**區域中，執行下列操作：
 - 要限制報告檔案大小，請選取**“儲存報告不超過”**核取方塊。在**“最大檔案大小”**核取方塊右邊的欄位中，指定報告檔案的最大大小。
預設情況下，報告檔案大小被限制為 1024 MB。
 - 要刪除報告檔案大小的限制，請清空**“最大檔案大小”**核取方塊。
預設情況下，啟用報告檔案大小限制。
4. 要儲存變更，請點擊**“儲存”**按鈕。

檢視報告

若要檢視報告：

1. 開啟[“程式主視窗”](#)。
2. 在主程式視窗上半部分，點擊**“報告”**連結開啟**“報告”**視窗。
3. 要產生“所有防護元件”報告，請在**“報告”**視窗的左側的元件和工作清單中選取**“所有防護元件”**。
“所有防護元件”報告顯示在視窗的右側，其中包含 Kaspersky Endpoint Security 所有防護元件操作中事件的清單。
4. 要產生元件或工作操作的報告，請在**“報告”**視窗左側，元件和工作清單中選取一個元件或工作。
報告顯示在視窗的右側，其中包含所選 Kaspersky Endpoint Security 元件或工作操作中事件的清單。
預設情況下，報告事件根據**“事件日期”**列中的值來排序。

檢視報告中的事件資訊

您可以在報告中檢視每個事件的詳細概述。

若要檢視報告中每個事件的詳細概述，請執行以下操作：

1. 開啟[“程式主視窗”](#)。
2. 在主程式視窗上半部分，點擊**“報告”**連結開啟**“報告”**視窗。
3. 在左側視窗中選取元件或工作的相關報告。
報告範圍中的事件將顯示在視窗右側的表中。若要查找報告中的特定事件，請使用篩選、搜尋和排序功能。
4. 選取報告中的相關事件。

帶有事件概覽的區域將顯示在視窗的底部。

將報告儲存到檔案

您可以將所產生的報告儲存到內容格式 (TXT) 檔案或 CSV 檔案中。

Kaspersky Endpoint Security 在報告中記錄事件的方式與其在螢幕上的顯示方式相同，換言之，兩者使用相同的事件內容和序列。

要將報告儲存到檔案中，請執行下列操作：

1. 開啟“[程式主視窗](#)”。
2. 在主程式視窗上半部分，點擊“**報告**”連結開啟“**報告**”視窗。
3. 請執行以下操作之一：
 - 要產生“所有防護元件”報告，請在元件和工作清單中，選取“**所有防護元件**”。
所有防護元件報告顯示在視窗的右側，其中包含所有防護元件操作中事件的清單。
 - 要產生關於特定元件或工作操作的報告，請在元件和工作清單中選取對應的元件或工作。
一般防護報告將顯示在視窗的右側，其中包含所有防護元件操作中事件的清單。
4. 如有必要，您可以透過下列方法修改報告中的資料呈現方式：
 - 篩選事件
 - 執行事件搜尋
 - 欄位重新排列
 - 事件排序
5. 點選視窗右上部的“**儲存報告**”按鈕。
一個右鍵選單將開啟。
6. 在右鍵選單中，選取儲存報告檔案的編碼方式：**另存為 ANSI**或**另存為 Unicode**。
標準的 Microsoft Office“**另存為**”視窗將開啟。
7. 在“**另存為**”視窗中，指定報告檔案的目的資料夾。
8. 在“**檔案名稱**”欄位中，輸入報告檔案名稱。
9. 在“**檔案類型**”欄位中，選取所需的報告檔案格式：TXT 或 CSV。
10. 點擊**儲存** 按鈕。

清理報告

要刪除報告中的資訊，請執行下列操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗的左側上，點選**進階設定** 選擇 **報告和儲存**。
3. 在視窗右側的“**報告參數**”區域中，點選“**刪除報告**”按鈕。
“**刪除報告**”視窗將開啟。
4. 選取您想要刪除其資訊的報告旁的核取方塊：
 - “**所有報告**”。
 - **基本防護報告**。包含關於下列 Kaspersky Endpoint Security 元件操作的資訊：
 - 檔案防護
 - 郵件防護。
 - 網頁防護。
 - 即時通訊防護。
 - 系統監視器。
 - 防火牆。
 - 網路攻擊防護。
 - BadUSB 攻擊防護。
 - **掃描工作報告**。包含關於已完成掃描工作的資訊：
 - 完整掃描
 - 關鍵區域掃描
 - 自訂掃描
 - 完整性檢查。
 - “**更新工作報告**”。包含關於已完成更新工作的資訊：
 - **防火牆報告**。包含關於防火牆操作的資訊。
 - **控制元件報告**。包含關於下列 Kaspersky Endpoint Security 元件操作的資訊：
 - 應用程式啟動控制。
 - 應用程式權限控制。
 - 弱點監控。
 - 裝置控制。

- Web 控制。
- 資料加密報告。

5. 點擊“確定”。

通知服務

本部分包含有關使用者在 Kaspersky Endpoint Security 操作中發生事件的通知服務的資訊，並且包含有關如何設定通知參數的說明。

關於 Kaspersky Endpoint Security 通知

Kaspersky Endpoint Security 執行操作時發生的所有類型的事件。這些事件通知可以是純粹的資訊或包含重要資訊。例如，通知可以告知成功更新了資料庫和應用程式模組或記錄需要糾正的元件錯誤。

Kaspersky Endpoint Security 支援記錄 Microsoft Windows 應用程式日誌和 / 或 Kaspersky Endpoint Security 事件日誌操作中的事件資訊。

Kaspersky Endpoint Security 透過下列方式傳送通知：

- 使用 Microsoft Windows 工作列通知區域中的彈窗通知；
- 透過電子郵件。

您可以設定事件通知的傳送方式。您可以為每一類事件設定通知傳送方式。

設定通知服務

您可以執行下列操作來設定通知服務：

- 設定 Kaspersky Endpoint Security 在其中記錄通知服務事件的事件記錄的設定。
- 設定如何顯示螢幕通知。
- 設定電子郵件通知

使用事件表設定通知服務時，您可以執行以下操作：

- 按列值或者自訂篩選條件篩選通知服務事件。
- 使用搜尋功能搜尋通知服務事件。
- 對通知服務事件進行排序。
- 變更通知服務事件清單中的顯示順序和列設定。

設定事件日誌設定

要配置事件記錄設定，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗的左側上，點選**進階設定** 選擇 **報告和儲存**。

視窗右側將顯示報告和儲存設定。

3. 在“通知”區域中，點擊“設定”按鈕。

這會開啟“通知”視窗。

Kaspersky Endpoint Security 元件和工作顯示在該視窗的左側。該視窗的右側列出了為選取元件或工作產生的事件。

4. 在視窗左側，選取您要為其設定事件記錄設定的元件或工作。

5. 選定“儲存於本機日誌中”和“在 Windows 事件記錄中儲存”列中相關事件旁的核取方塊。

已在“儲存於本機記錄”欄中選中核取方塊的事件將顯示在“卡巴斯基事件記錄”區域中的“應用程式和服務記錄”中。已在“儲存在 Windows 事件記錄”欄中選中核取方塊的事件將顯示在“應用程式”區域中的“Windows 記錄”中。若要開啟事件記錄，請點擊“開始 → 控制台 → 管理 → 事件檢視器”。

6. 點擊“確定”。

7. 要儲存變更，請點擊“儲存”按鈕。

設定通知的顯示和傳送

若要設定通知的顯示和傳送：

1. 開啟[程式設定視窗](#)。

2. 在視窗的左側上，點選**進階設定** 選擇 **報告和儲存**。

視窗右側將顯示報告和儲存設定。

3. 在“通知”區域中，點擊“設定”按鈕。

這會開啟“通知”視窗。

Kaspersky Endpoint Security 元件和工作顯示在該視窗的左側。該視窗的右側列出了為選取元件或選定工作產生的事件。

4. 在視窗的左側，選取要為其設定螢幕通知傳送的元件或工作。

5. 在“提示視窗通知”列中，選取所需事件旁的核取方塊。

關於選取事件的資訊會以 Microsoft Windows 工作列通知區域中彈出訊息的形式顯示在螢幕上。

6. 在“電子郵件通知”列中，選取所需事件旁的核取方塊。

如果配置了郵件通知傳遞設定，則透過電子郵件傳送選定事件的資訊。

7. 點選“電子郵件通知設定” 按鈕。

“電子郵件通知設定”視窗將開啟。

8. 選取“傳送事件通知”核取方塊以啟用傳送有關在“透過電子郵件通知”列中選定的 Kaspersky Endpoint Security 事件資訊的功能。

9. 指定電子郵件事件通知傳送設定。

10. 點擊“確定”。

11. 在“電子郵件通知設定”的視窗上，點選“確定”。

12. 要儲存變更，請點擊“儲存”按鈕。

設定應用程式狀態警告在通知區域的顯示

若要設定通知區域中應用程式狀態警告的顯示：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“進階設定”區域中，選取“介面”。
Kaspersky Endpoint Security 介面的設定顯示在視窗右側。
3. 在“警告”區域中，選取您要在 Microsoft Windows 通知區域中看到通知的事件類型旁的核取方塊。
4. 要儲存變更，請點擊“儲存”按鈕。

發生與選定類別關聯的事件時，通知區域的[應用程式圖示](#)將根據警告的嚴重性變更為  或 。

管理隔離區和備份區

本章節將介紹如何設定和管理隔離區和備份。

關於隔離區和備份區

*隔離*是疑似受病毒和其他惡意程式感染的檔案清單。*疑似受感染檔案*是懷疑受病毒和其他惡意程式及其變種感染的檔案。

當 Kaspersky Endpoint Security 隔離疑似感染的檔案時不會複製該檔案，而是移動它：程式將從硬碟或電子郵件訊息中刪除該檔案並將其儲存在特定的資料儲存中。“隔離區”中的檔案以特定格式儲存並且不會帶來威脅。

Kaspersky Endpoint Security 可以在[病毒掃描](#)期間或者[檔案防護](#)、[郵件防護](#)和[系統監控](#)元件執行期間偵測和隔離疑似感染檔案。

在下列情況下，Kaspersky Endpoint Security 將檔案置於“隔離區”中：

- 檔案代碼看上去像已知但部分修改的威脅，或者包含類似惡意程式的結構，並且未在 Kaspersky Endpoint Security 資料庫中列出。在這種情況下，檔案防護和郵件防護過程中，或者在病毒掃描間執行了啟發式分析，檔案將被置於“隔離區”中。啟發式分析很少會導致誤報。
- 檔案執行的一系列操作包含可疑行為。在此例中，在“系統監控”元件分析檔案的行為後，該檔案將置於“隔離區”中。

“*備份*”是在解毒過程中刪除或修改的檔案備份副本的清單。*備份區副本*是檔案的副本，第一次試圖解毒或刪除該檔案時建立並作為潛在受感染檔案儲存在同一儲存區中。檔案的備份副本以特定格式儲存並且不會帶來威脅。

有時，在清除過程中無法維護檔案的完整性。如果您在解毒後失去對受感染檔案重要資訊的部分或全部存取權限，可以嘗試將該檔案的受感染副本還原到其原始資料夾中。

如有可能，經過另一次資料庫或程式模組更新後，Kaspersky Endpoint Security 有可能真正識別並消除威脅。因此，我們建議您在每次資料庫和程式模組更新後掃描隔離的檔案。

配置隔離區和備份區設定

資料儲存由隔離區和備份構成您可以透過以下操作設定隔離區和備份設定：

- 為隔離區檔案和備份的檔案副本設定最大儲存期限。
隔離區檔案和備份的檔案副本預設最大儲存期限是 30 天。當最大儲存期限超出後，Kaspersky Endpoint Security 將刪除資料儲存中時間最久的檔案。您可以取消時間限制或者變更最大檔案儲存期限。
- 您可以設定隔離區和備份區的最大容量
預設情況下，隔離區和備份區的最大容量為 100 MB。當資料儲存達到最大容量時，Kaspersky Endpoint Security 將自動刪除資料儲存中時間最久的檔案，確保不超出最大資料儲存容量。您可以取消隔離區和備份區容量限制或者變更它們的最大容量。

設定備份和隔離區檔案儲存最長時間

要設定備份和隔離區檔案儲存最長時間，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗的左側上，點選**進階設定** 選擇 **報告和儲存**。
3. 請執行以下操作之一：
 - 要限制檔案儲存時間限制，請在該視窗右側的“**隔離區和備份區設定**”區域中選取“**儲存物件的時間不超過**”核取方塊。在“**儲存物件的時間不超過**”核取方塊右側的欄位中，指定隔離區檔案和備份區檔案副本的最長儲存時間。隔離區檔案和備份的檔案副本的儲存時間預設限制為 30 天。
 - 要取消隔離區和備份去檔案儲存時間限制，請在該視窗右側的“**隔離區和備份區設定**”區域中選取“**儲存物件的時間不超過**”核取方塊。
4. 要儲存變更，請點擊“**儲存**”按鈕。

設定隔離區和備份區的最大容量

要設定隔離區和備份區的最大容量，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗的左側上，點選**進階設定** 選擇 **報告和儲存**。
3. 請執行以下操作之一：
 - 如果您希望限制隔離區和備份區的總容量，可以選取“**隔離區和備份區設定**”區域中右側視窗中“**最大儲存容量**”核取方塊，在“**最大儲存容量**”核取方塊右側欄位中指定隔離區和備份區的最大容量。
預設情況下，組成隔離區目錄和檔案備份副本的資料最大儲存容量是 100 MB。
 - 如果您希望限制隔離區和備份區的容量，則清空“**隔離區和備份區設定**”區域右側視窗中的“**最大儲存容量**”核取方塊。
預設情況下隔離區和備份區容量無限制。
4. 要儲存變更，請點擊“**儲存**”按鈕。

管理隔離區

當達到進階設定中設定的儲存條件後，Kaspersky Endpoint Security 將[自動刪除](#)隔離區中的所有檔案，不管它們的狀態是什麼。

在管理隔離區時，您可進行以下檔案操作：

- 檢視從 Kaspersky Endpoint Security 隔離的檔案。
- 使用目前版本的 Kaspersky Endpoint Security 資料庫和模組掃描存在潛在感染可能的檔案。
- 將檔案從隔離區還原到原始位置。

- 將檔案從隔離區刪除。
- 開啟檔案原來所在的資料夾。

已隔離檔案集合以表格顯示。

您也可在管理表中資料時執行以下操作：

- 根據行和自訂篩選條件隔離檔案。
- 使用隔離檔案搜尋功能。
- 為隔離檔案排序。
- 變更已隔離檔案事件表格中的顯示順序和列設定。

您可以將所選隔離事件複製到剪貼簿。若要選取多個隔離的檔案，點擊右鍵開啟任何檔案的上下文功能表，選取“**全選**”。若要取消選取不希望掃描的檔案，則在按住 **CTRL** 鍵的同時點擊它們。

啟用和禁用更新後掃描隔離區中的檔案

如果 Kaspersky Endpoint Security 偵測感染的跡象時，會掃描該檔案，但無法確定是否有惡意程式感染，這時候 Kaspersky Endpoint Security 就會把這檔案移動到**隔離**。Kaspersky Endpoint Security 可能稍後在資料庫和程式模組更新後準確識別和解毒這些威脅。您可以在每次更新的資料庫和程式模組後自動掃描隔離區。

我們建議您定期掃描隔離區中的檔案。掃描可能會改變檔案的狀態。有些檔案可以進行解除，並還原到原來的狀態，您可以繼續使用乾淨的檔案。

啟用更新後掃描隔離的檔案，執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗的左側上，點選**進階設定** 選擇 **報告和儲存**。
報告和儲存的管理設定就會顯示在右邊的視窗上。
3. 在“**隔離和備份**”中，執行以下操作：
 - 為了讓隔離的檔案每次在更新之後能夠掃描，所以每次更新後建議點選“**在更新後重新掃描**”核取方塊。
 - 要停止每次檔案在更新後掃描的話，您可以將“**在更新後重新掃描**”的核取方塊取消。
4. 要儲存變更，請點擊“**儲存**”按鈕。

啟動隔離區檔案自訂掃描

在資料庫和程式模組更新後，Kaspersky Endpoint Security 也許能夠識別位於隔離區中的檔案的威脅類型並進行解毒。如果沒有將應用程式設定為在每次完成資料庫和程式模組更新後自動掃描隔離的檔案，您可以手動啟動隔離的檔案自訂掃描工作。

要啟動隔離區檔案自訂掃描，請執行以下操作：

1. 開啟“[程式主視窗](#)”。
2. 在程式主視窗上半部分，點擊“**隔離區**”連結開啟“**儲存**”視窗。
開啟“**儲存**”視窗的“**隔離區**”頁籤。
3. 在“**隔離**”中，選取包含您希望掃描的檔案的一個或多個。
若要選取多個隔離的檔案，點擊右鍵開啟任何檔案的上下文功能表，選取“**全選**”。若要取消選取不希望掃描的檔案，則在按住 **CTRL** 鍵的同時點擊它們。
4. 以下列方式啟動自訂掃描工作：
 - 點擊“**重新掃描**”按鈕。
 - 點擊右鍵顯示右鍵選單，然後選取“**重新掃描**”項。掃描工作完成後，程式將以通知顯示掃描的檔案和偵測到的威脅數量。

從隔離區中還原檔案

要從隔離區中還原檔案，請執行以下操作：

1. 開啟“[程式主視窗](#)”。
2. 在程式主視窗上半部分，點擊“**隔離區**”連結開啟“**儲存**”視窗。
開啟“**儲存**”視窗的“**隔離區**”頁籤。
3. 如果您希望還原所有隔離的檔案，則從任何檔案的上下文功能表中選取“**全部還原**”。
Kaspersky Endpoint Security 將所有檔案從隔離區還原至其原資料夾。
4. 要還原一個或多個隔離區檔案，請執行以下操作：
 - a. 在“**隔離**”標籤中選取一個或多個您希望從隔離區還原的檔案。
若要選取多個隔離的檔案，點擊右鍵開啟任何檔案的上下文功能表，選取“**全選**”。若要取消選取不希望掃描的檔案，則在按住 **CTRL** 鍵的同時點擊它們。
 - b. 請按照以下方式還原檔案：
 - 點擊 **還原** 按鈕。
 - 右鍵點擊以開啟右鍵選單並選取“**還原**”。

Kaspersky Endpoint Security 會將把所選檔案還原至它們原來所在的資料夾。

從隔離區中刪除檔案

要從隔離區中刪除檔案，請執行以下操作：

1. 開啟“[程式主視窗](#)”。
2. 在程式主視窗上半部分，點擊“**隔離區**”連結開啟“**儲存**”視窗。

開啟“儲存”視窗的“隔離區”頁籤。

3. 如果您希望從隔離區中刪除所有檔案，則從任何檔案的上下文功能表中選取“全部刪除”。

Kaspersky Endpoint Security 將從隔離區中刪除所有檔案。

4. 要刪除一個或多個隔離區檔案，請執行以下操作：

a. 在“隔離”標籤的表中，選取您希望從隔離區中刪除的一個或多個疑似感染檔案。

若要選取多個隔離的檔案，點擊右鍵開啟任何檔案的上下文功能表，選取“全選”。若要取消選取不希望掃描的檔案，則在按住 **CTRL** 鍵的同時點擊它們。

b. 透過下列方式之一刪除檔案：

- 點擊“刪除”按鈕。
- 右鍵點擊以開啟右鍵選單並選取“刪除”。

Kaspersky Endpoint Security 將把所選檔案從隔離區刪除。

管理備份

如果在檔案中偵測到惡意程式碼，Kaspersky Endpoint Security 將封鎖此檔案、將其副本放到“備份區”中並嘗試對其解毒。成功解毒後，此備份副本的狀態將變為 *已解毒*。檔案在原始資料夾中將不可用。如果檔案無法被解毒，Kaspersky Endpoint Security 將把它從原始資料夾中刪除。您可以將此檔案從它的備份副本還原到它的原資料夾。

在屬於 Windows Store 應用程式的檔案中偵測到惡意程式碼以後，Kaspersky Endpoint Security 將立即刪除檔案，而不會將其備份副本移至備份區。您可以使用 Windows 8 作業系統的適當工具還原 Windows Store 應用程式的完整性（有關還原 Windows Store 應用程式的詳細資訊，請參閱 *Windows 8 說明檔案*）。

當應用程式設定中定義的儲存期限到期後，Kaspersky Endpoint Security 將 [自動刪除](#) 備份區中的所有檔案備份副本，而不管它們的狀態是什麼。

您也可以手動從備份區中刪除檔案的副本。

檔案備份副本集合以表格顯示。

在管理備份時，您可以對檔案備份執行以下操作：

- 檢視檔案備份副本的集合
- 將檔案備份副本還原至原資料夾。
- 從備份區中刪除檔案副本備份。

您也可在管理表中資料時執行以下操作：

- 透過列值或者自訂篩選條件篩選備份副本。
- 使用備份副本搜尋功能。
- 為備份副本排序。

- 變更備份副本表格中的顯示順序和列設定。

如有需要，您可以將所選備份事件複製到剪貼簿。若要選取多個備份區檔案，點擊右鍵開啟任何檔案的上下文功能表，選取“**全選**”。若要取消選取不希望掃描的檔案，則在按住 **CTRL** 鍵的同時點擊它們。

從備份區中還原檔案

要從備份區中還原檔案，請執行以下操作：

1. 開啟“[程式主視窗](#)”。
2. 在程式主視窗上半部分，點擊“**隔離區**”連結開啟“**儲存**”視窗。
3. 在“**儲存**”視窗中，選取“**備份區**”頁籤。
4. 如果您希望從備份區中還原所有檔案，則從任何檔案的上下文功能表中選取“**全部還原**”。
Kaspersky Endpoint Security 將把所有檔案的備份副本還原至它們原來所在的資料夾。
5. 要還原備份區中的一個或多個檔案，請執行以下操作：
 - a. 在“**備份區**”頁籤上的表格中，選取一個或多個備份區檔案。
若要選取多個隔離的檔案，點擊右鍵開啟任何檔案的上下文功能表，選取“**全選**”。若要取消選取不希望掃描的檔案，則在按住 **CTRL** 鍵的同時點擊它們。
 - b. 請按照以下方式還原檔案：
 - 點擊 **還原** 按鈕。
 - 右鍵點擊以開啟右鍵選單並選取“**還原**”。

Kaspersky Endpoint Security 會將把所選檔案的備份副本還原至它們原來所在的資料夾。

從備份區中刪除檔案副本備份。

要從備份區中刪除檔案副本備份：

1. 開啟“[程式主視窗](#)”。
2. 在程式主視窗上半部分，點擊“**隔離區**”連結開啟“**儲存**”視窗。
3. 在“**儲存**”視窗中，選取“**備份區**”頁籤。
4. 如果您想要從備份區刪除所有檔案，請執行以下操作中的其中一項：
 - 在任何檔案的上下文功能表中，選擇 **全部刪除**。
 - 點擊**清除儲存**按鈕。

Kaspersky Endpoint Security 將從備份區中刪除所有檔案備份副本。

5. 如果您希望從備份區中刪除一個或多個檔案：

a. 在“**備份區**”頁籤上的表格中，選取一個或多個備份區檔案。

若要選取多個備份區檔案，點擊右鍵開啟任何檔案的上下文功能表，選取“**全選**”。若要取消選取不希望掃描的檔案，則在按住 **CTRL** 鍵的同時點擊它們。

b. 透過下列方式之一刪除檔案：

- 點擊“**刪除**”按鈕。
- 右鍵點擊以開啟右鍵選單並選取“**刪除**”。

Kaspersky Endpoint Security 將把所選備份從隔離區刪除。

進階程式設定

本章節介紹 Kaspersky Endpoint Security 的進階設定以及如何配置這些設定。

建立和使用設定檔

帶有 Kaspersky Endpoint Security 設定的設定檔允許您完成以下工作：

- 透過命令列使用自訂的設定本機安裝 Kaspersky Endpoint Security。
若要執行操作，您必須在安裝套件所在的相同資料夾內儲存設定檔。
- 透過卡斯基安全管理中心使用自訂的設定遠端安裝 Kaspersky Endpoint Security。
- 從一台電腦上將 Kaspersky Endpoint Security 設定遷移至其他電腦上。

若要建立設定檔，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側，選取“**進階設定**”區域。
進階程式設定將顯示在視窗右側。
3. 在“**管理設定**”區域中點擊“**儲存**”按鈕。
Microsoft Windows 的標準“**請選取設定檔**”視窗將開啟。
4. 指定您要儲存設定檔的路徑並輸入其名稱。

若要使用設定檔本機或遠端安裝 Kaspersky Endpoint Security，您必須將其命名為 install.cfg。

5. 點擊**儲存** 按鈕。

若要從設定檔匯入 Kaspersky Endpoint Security 設定：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側，選取“**進階設定**”區域。
進階程式設定將顯示在視窗右側。
3. 在“**管理設定**”區域中點擊“**載入**”按鈕。
Microsoft Windows 的標準“**請選取設定檔**”視窗將開啟。
4. 指定設定檔的路徑。
5. 點擊“**開啟**”按鈕。

Kaspersky Endpoint Security 設定的所有值都將根據選定設定檔進行設定。

信任區域

本章節包含信任區域的資訊以及設定掃描排除項目和建立信任應用程式清單的說明。

關於信任區域

*信任區域*是在其有效時，管理員建立的 Kaspersky Endpoint Security 不進行監控的物件和應用程式的清單。換句話說，它就是掃描排除項目集合。

考慮到所處理物件的特點和安裝在電腦上的應用程式，管理員可以自主建立信任區域。當 Kaspersky Endpoint Security 封鎖存取特定物件或應用程式時，如果您確定此物件或應用程式是無害的，則有必要將其包含在信任區域中。

您可以將下列類型的物件排除在掃描範圍外：

- 特定格式的檔案
- 透過遮罩選取的檔案
- 選定檔案
- 資料夾
- 應用程式處理程序

掃描排除項目

“*掃描排除項目*”是一組條件，根據此條件 Kaspersky Endpoint Security 不掃描物件的病毒和其他惡意程式。

掃描排除項目可確保使用者安全地使用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，它們可在惡意程式中作為輔助元件。這類應用程式的例子包括遠端系統管理工具、IRC 用戶端、FTP 伺服器、各種暫停或隱藏處理程序的實用工具、鍵盤記錄程式、密碼破解工具、自動撥號器。此類應用程式不會被歸類為病毒。可被犯罪分子用來破壞您的電腦或個人資料的合法軟體的詳細資訊可以在 Kaspersky 病毒百科全書找到，網址是 <https://encyclopedia.kaspersky.com/knowledge/riskware/>。

這類應用程式可以被 Kaspersky Endpoint Security 封鎖。若要防止它們被封鎖，您可以為正在使用的應用程式排除掃描排除項目。為此，請將 Kaspersky Lab 病毒百科全書中列出的名稱或名稱遮罩新增到受信任區域。例如，您可能經常使用遠端控制程式。這是一種遠端存取應用程式，使您能夠控制遠端的電腦。Kaspersky Endpoint Security 會將這些活動看做潛在危險並進行封鎖。若要防止應用程式被封鎖，請使用 Kaspersky 病毒百科全書中列出的名稱或名稱遮罩建立掃描排除項目。

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 可能會將其歸類為惡意軟體。若要避免此資訊，您可以按照文件所述透過配置 Kaspersky Endpoint Security 從掃描中排除此應用程式。

排除規則可用於下列特定應用程式元件和系統管理員設定的工作：

- 檔案防護
- 郵件防護。
- 網頁防護。
- 應用程式權限控制。

- 掃描工作
- 系統監視器。

信任的應用程式清單

*信任的應用程式清單*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 將掃描任何程式處理程序開啟、執行或儲存的物件，並控制所有應用程式的行動及其產生的網頁流量。Kaspersky Endpoint Security 將從掃描中排除[受信任應用程式清單](#)中的應用程式。

例如，如果您認為由標準 Microsoft Windows 記事本使用的物件不需掃描並且可確認是安全的，也即您信任此應用程式，則您可將 Microsoft Windows 記事本新增到受信任應用程式清單中。掃描會略過此應用程式使用的物件。

此外，Kaspersky Endpoint Security 分類為危險的特定操作，在很多應用程式的功能環境中可能是安全的。例如，攔截鍵盤輸入的內容，是自動鍵盤設定切換器中的一種例行程式（例如 Punto Switcher）。考慮到此類程式的特點並將其行為從監控中排除，我們建議您可將此類程式新增到信任應用程式清單中。

從掃描中排除信任的應用程式可避免 Kaspersky Endpoint Security 和其他程式的相容性衝突（例如，Kaspersky Endpoint Security 和另一個防毒應用程式對協力廠商電腦網頁流量的掃描問題），同時也能強化電腦效能，這在使用伺服器版應用程式時十分重要。

同時，信任應用程式的可執行檔案和處理程序仍然會掃描病毒和其他惡意程式。您可以透過掃描排除項目將應用程式從 Kaspersky Endpoint Security 掃描中完全排除。

建立掃描排除項目

如果包含某個物件的磁碟或資料夾在掃描工作啟動時包括在掃描範圍中，則 Kaspersky Endpoint Security 將不對此物件進行掃描。但是，當啟動了針對該特殊物件的自訂掃描工作時，掃描排除項目將不應用。

若要編輯掃描排除項目，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 選取左側的“端點防護”區域。
端點防護設定將顯示在視窗右方。
3. 在“排除項和信任的應用程式”區域中點擊“設定”按鈕。
“受信任區域”視窗中將開啟，並顯示“掃描排除項”頁籤。
4. 點擊“新增”按鈕。
“掃描排除項”視窗將開啟。在該視窗中，您可以使用“內容”區域中的一個或兩個條件建立掃描排除項目。
5. 要從掃描中排除某個檔案或資料夾，請執行以下操作：
 - a. 在“內容”區域中選取“檔案或資料夾”選取方塊。
 - b. 點選“掃描排除項目說明”區域中的“選取檔案或資料夾”連結，開啟“檔案或資料夾名稱”視窗。

c. 輸入檔案或資料夾名稱，或者檔案或資料夾名稱遮罩，或者點擊“**瀏覽**”選取資料夾樹狀目錄中的檔案或資料夾。

在檔案或資料夾名稱遮罩中，您可以使用星號 (*) 代替檔案名稱中的任何字集。

例如，您可以使用遮罩新增以下路徑：

- 位於任何資料夾的檔案位置：
 - “*.exe” 遮罩將包括具有 EXE 副檔名檔案的所有路徑。
 - “test” 遮罩將包括以 “test” 命名的所有檔案的路徑。
- 位於指定資料夾的檔案的路徑：
 - “C:\dir*.*” 遮罩將包括位於 C:\dir\ 資料夾的所有檔案的路徑，但不包括 C:\dir\ 的子資料夾。
 - 遮罩“C:\dir*”將包括位於 C:\dir\ 資料夾的檔案的所有路徑，但不包括 C:\dir\ 的子資料夾中的檔案的路徑。
 - 遮罩“C:\dir\”將包括位於 C:\dir\ 資料夾的檔案的所有路徑，但不包括 C:\dir\ 的子資料夾中的檔案的路徑。
 - “C:\dir*.exe” 遮罩將包括 C:\dir\ 資料夾中帶有 EXE 副檔名的所有檔案的路徑，但不包括 C:\dir\ 的子資料夾。
 - “C:\dir\test” 遮罩將包括 C:\dir\ 資料夾中以 “test” 命名的所有檔案的路徑，但不包括 C:\dir\ 的子資料夾。
 - “C:\dir*\test” 遮罩將包括 C:\dir\ 資料夾及其子資料夾中以 “test” 命名的所有檔案的路徑。
- 位於指定名稱的所有資料夾中的檔案的路徑：
 - “dir*.*” 遮罩將包括以 “dir” 命名的資料夾中的所有檔案的路徑，但不包括這些資料夾的子資料夾。
 - 遮罩“dir*”將包括名為“dir”的資料夾中的檔案的所有路徑，但不包括這些資料夾的子資料夾中的檔案的路徑。
 - 遮罩“dir\”將包括名為“dir”的資料夾中的檔案的所有路徑，但不包括這些資料夾的子資料夾中的檔案的路徑。
 - “dir*.exe” 遮罩將包括以 “dir” 命名的資料夾中帶有 EXE 副檔名的所有檔案的路徑，但不包括這些資料夾的子資料夾。
 - “dir\test” 遮罩將包括以 “dir” 命名的資料夾中名為 “test” 的所有檔案的路徑，但不包括這些資料夾的子資料夾。

d. 在“**檔案或資料夾名稱**”視窗中點選“**確定**”。

已新增檔案或資料夾的連結將出現在“**排除排除項目**”視窗中的“**掃描排除項目描述**”區域。

6. 要從掃描中排除帶有指定名稱的物件，請執行以下操作：

- a. 在“**內容**”區域中選取“**物件名稱**”核取方塊。
- b. 點選“**掃描排除項目描述**”區域中的“**輸入物件名稱**”連結，開啟“**物件名稱**”視窗。
- c. 根據 Kaspersky 病毒百科全書的分類輸入物件名稱或名稱遮罩：

d. 在“物件名稱”視窗中點選“確定”。

所新增物件名稱的連結將顯示在“掃描排除項目”視窗的“掃描排除項目描述”區域中。

7. 如有必要，在“註解”欄位，輸入您建立的掃描排除項目的簡要說明。

8. 指定應該使用掃描排除項目的 Kaspersky Endpoint Security 元件：

a. 點選“掃描排除項目描述”區域中的“任何”連結可開啟“選取元件”連結。

b. 點擊“選取元件”連結以開啟“防護元件”視窗。

c. 選取必須應用掃描排除項目的元件旁的核取方塊。

d. 在“防護元件”視窗中點擊“確定”。

如果在掃描排除項目設定中指定了元件，則只有 Kaspersky Endpoint Security 的這些元件不對此物件進行掃描。

如果在掃描排除項目的設定中沒有指定元件，Kaspersky Endpoint Security 的所有元件執行掃描時會應用該排除規則。

9. 在“掃描排除項目”視窗中，點選“確定”。

您新增的掃描排除項目將出現在“受信任區域”視窗中的“掃描排除項目”頁籤的表中。設定的該掃描排除項目設定將顯示在“掃描排除項目描述”區域中。

10. 在“信任區域”的視窗上，點選“確定”。

11. 要儲存變更，請點擊“儲存”按鈕。

修改掃描排除項目

要修改掃描排除項目，請執行以下操作：

1. 開啟[程式設定視窗](#)。

2. 選取左側的“端點防護”區域。

端點防護設定將顯示在視窗右方。

3. 在“排除項和信任的應用程式”區域中點擊“設定”按鈕。

“受信任區域”視窗中將開啟，並顯示“掃描排除項”頁籤。

4. 在清單中選取您要修改的掃描排除項目。

5. 使用以下方法之一變更掃描排除項目設定：

- 點擊“編輯”按鈕。

“掃描排除項”視窗將開啟。

- 點擊“掃描排除項目描述”欄位中的連結開啟視窗編輯所需的設定。

6. 如果在上個步驟中點擊了“編輯”按鈕，則在“掃描排除項目”視窗中點擊“確定”。

該掃描排除項目的修改的設定將顯示在“掃描規則項目描述”區域中。

7. 在“**信任區域**”的視窗上，點選“**確定**”。
8. 要儲存變更，請點擊“**儲存**”按鈕。

刪除掃描排除項目

若要刪除掃描排除項目，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 選取左側的“**端點防護**”區域。
端點防護設定將顯示在視窗右方。
3. 在“**排除項和信任的應用程式**”區域中點擊“**設定**”按鈕。
“**受信任區域**”視窗中將開啟，並顯示“**掃描排除項**”頁籤。
4. 在掃描排除項目清單中選取您所需的掃描排除項目。
5. 點擊“**刪除**”按鈕。
被刪除的掃描排除項目將從清單中消失。
6. 在“**信任區域**”的視窗上，點選“**確定**”。
7. 要儲存變更，請點擊“**儲存**”按鈕。

啟用和停用掃描排除項目

若要啟用和停用掃描排除項目，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 選取左側的“**端點防護**”區域。
端點防護設定將顯示在視窗右方。
3. 在“**排除項和信任的應用程式**”區域中點擊“**設定**”按鈕。
“**受信任區域**”視窗中將開啟，並顯示“**掃描排除項**”頁籤。
4. 在掃描排除項目清單中選取您所需的排除項目。
5. 請執行以下操作之一：
 - 要啟用某個掃描排除項目，請勾選該掃描排除項目名稱旁邊的核取方塊。
 - 要停用某個掃描排除項目，請清除該掃描排除項目名稱旁邊的核取方塊。
6. 點擊“**確定**”。
7. 要儲存變更，請點擊“**儲存**”按鈕。

編輯信任應用程式清單

若要編輯信任應用程式清單，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 選取左側的“**端點防護**”區域。
端點防護設定將顯示在視窗右方。
3. 在“**排除項和信任的應用程式**”區域中點擊“**設定**”按鈕。
開啟“**信任區域**”視窗。
4. 在“**信任區域**”視窗中選取“**信任的應用程式**”頁籤。
5. 若要將應用程式新增到信任應用程式清單中：
 - a. 點擊“**新增**”按鈕。
 - b. 在開啟的右鍵選單中執行以下操作：
 - 如果您要在電腦安裝的應用程式清單中找到此應用程式，請在功能表中選取“**應用程式**”。
開啟“**選擇應用程式**”。
 - 如果您要指定相關應用程式可執行檔案的路徑，請選取“**瀏覽**”。
將開啟標準的 Microsoft Windows“**開啟檔案**”視窗。
 - c. 採用以下方式之一選取程式：
 - 如果您在上個步驟中選取了“**應用程式**”，則在電腦上已安裝應用程式清單中選取應用程式，在**選取應用程式**視窗中點擊“**確定**”。
 - 如果您在先前步驟中選取了“**瀏覽**”，則指定相關應用程式的可執行檔案路徑，在標準的 Microsoft Windows“**開啟**”視窗中點擊“**開啟**”。

這些操作將開啟“**掃描應用程式排除項目**”視窗。

- a. 選取選定應用程式相關受信任區域規則對應的核取方塊：
 - 不掃描開啟的檔案。
 - 不監控應用程式行為。
 - 不繼承父程序（應用程式）的限制。
 - 不監控應用程式活動。
 - 不要封鎖與應用程式介面的互動。
 - 不掃描網頁資料流量。
 - b. 在“**掃描應用程式排除項目**”視窗中點擊“**確定**”。
- 您已新增的信任群組應用程式將出現在信任群組應用程式清單中。

6. 要編輯信任群組應用程式的設定：

- a. 選取信任群組應用程式清單中的信任群組應用程式。
- b. 點擊“**編輯**”按鈕。
- c. “**掃描應用程式排除項目**”視窗將開啟。
- d. 選取或清除選定應用程式相關受信任區域規則對應的核取方塊：

如果在“**掃描應用程式排除項目**”視窗中沒有選取受信任區域規則，則受信任應用程式包括在掃描中。在這種情況下，信任應用程式不會從信任應用程式清單中刪除，但其核取方塊被清除。

- e. 在“**掃描應用程式排除項目**”視窗中點擊“**確定**”。

7. 要從信任應用程式清單中刪除信任應用程式：

- a. 選取信任群組應用程式清單中的信任群組應用程式。
- b. 點擊“**刪除**”按鈕。

8. 在“**信任區域**”的視窗上，點選“**確定**”。

9. 要儲存變更，請點擊“**儲存**”按鈕。

為受信任應用程式清單中的應用程式啟用或停用受信任區域規則

如果要在受信任應用程式清單中啟用或停用應用至應用程式的受信任區域規則：

1. 開啟程式設定視窗。
2. 選取左側的“**端點防護**”區域。
端點防護設定將顯示在視窗右方。
3. 在“**排除項和信任的應用程式**”區域中點擊“**設定**”按鈕。
開啟“**信任區域**”視窗。
4. 在“**信任區域**”視窗中選取“**信任的應用程式**”頁籤。
5. 在信任應用程式清單中，選取必要的信任應用程式。
6. 請執行以下操作之一：
 - 要從 Kaspersky Endpoint Security 掃描中排除信任應用程式，請選取其名稱旁邊的核取方塊。
 - 要在 Kaspersky Endpoint Security 掃描中包含信任應用程式，請取消其名稱旁邊的核取方塊。
7. 點擊“**確定**”。
8. 要儲存變更，請點擊“**儲存**”按鈕。

使用受信任的系統憑證儲存

使用系統憑證儲存允許您從病毒掃描中排除由受信任數位簽章簽發的應用程式。Kaspersky Endpoint Security 會自動將此類應用程式分配給受信任群組。

若要使用受信任的系統憑證儲存：

1. 開啟[程式設定視窗](#)。
2. 選取左側的“**病毒防護**”區域。
病毒防護設定將顯示在視窗右方。
3. 在“**掃描排除項目和受信任應用程式**”區域中點擊“**設定**”按鈕。
“**信任區域**”視窗將開啟。
4. 在“**信任區域**”視窗中選取“**受信任的系統憑證儲存**”標籤。
5. 選取“**使用受信任的系統憑證儲存**”核取方塊。
6. 在“**信任的系統憑證儲存**”下拉清單中，選取 Kaspersky Endpoint Security 必須將哪個系統儲存為受信任儲存。
7. 在“**受信任區域**”視窗中點擊“**確定**”。
8. 要儲存變更，請點擊“**儲存**”按鈕。

Kaspersky Endpoint Security 自我防護

本章節介紹 Kaspersky Endpoint Security 自我防護和遠端控制防護機制，並且說明如何配置這些機制的設定。

關於 Kaspersky Endpoint Security 自我防護

Kaspersky Endpoint Security 防護電腦避免惡意程式（包括試圖封鎖 Kaspersky Endpoint Security 操作或將其從電腦上刪除的惡意程式）的威脅。

透過 Kaspersky Endpoint Security 的自我防護和遠端控制防護機制可確保電腦上安全系統的穩定性。

*自我防護*可防止變更或刪除在硬碟、記憶體處理程序和系統登錄檔中的應用程式檔案。

*遠端控制防護*可封鎖遠端電腦控制應用程式服務的一切嘗試。

在執行 64 位元作業系統的電腦上，只有 Kaspersky Endpoint Security 自我防護可防止變更或刪除在硬碟、記憶體處理程序和系統登錄機碼中的應用程式檔案。

啟用或停用自我防護

預設情況下已啟用 Kaspersky Endpoint Security 的自我防護機制。您可以根據需要停用自我防護。

若要啟用或停用自我防護，請執行下列操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側，選取“**進階設定**”區域。
進階程式設定將顯示在視窗右側。
3. 請執行以下操作之一：
 - 要啟用自我防護機制，請選取“**啟用自我防護**”核取方塊。
 - 要停用自我防護機制，請清除“**啟用自我防護**”核取方塊。
4. 要儲存變更，請點擊“**儲存**”按鈕。

啟用或停用遠端控制防護

預設情況下已啟用遠端控制防護機制。您可以根據需要停用遠端控制防護機制。

若要啟用或停用遠端控制防護機制，請執行下列操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側，選取“**進階設定**”區域。
進階程式設定將顯示在視窗右側。
3. 請執行以下操作之一：
 - 要啟用遠端控制防護機制，請選取“**停用系統服務的外部管理**”。
 - 要停用遠端控制防護機制，請清除“**停用系統服務的外部管理**”。
4. 要儲存變更，請點擊“**儲存**”按鈕。

支援遠端管理應用程式

啟用外部控制防護後，您可能偶爾會需要使用遠端管理應用程式。

若要啟用遠端系統管理應用程式的操作，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 選取左側的“**端點防護**”區域。
端點防護設定將顯示在視窗右方。
3. 在“**排除項和信任的應用程式**”區域中點擊“**設定**”按鈕。
開啟“**信任區域**”視窗。

4. 在“信任區域”視窗中選取“信任的應用程式”頁籤。
5. 點擊“新增”按鈕。
6. 在開啟的右鍵選單中執行以下操作：
 - 要在電腦安裝的應用程式清單中找到查找遠端管理應用程式，請在功能表中選取“應用程式”。開啟“選擇應用程式”。
 - 要指定相關應用程式可執行檔案的路徑，請選取“瀏覽”。將開啟標準的 Microsoft Windows“開啟檔案”視窗。
7. 採用以下方式之一選取程式：
 - 如果您在上個步驟中選取了“應用程式”，則在電腦上已安裝應用程式清單中選取應用程式，在選取應用程式視窗中點擊“確定”。
 - 如果您在先前步驟中選取了“瀏覽”，則指定相關應用程式的可執行檔案路徑，在標準的 Microsoft Windows“開啟”視窗中點擊“開啟”。這些操作將開啟“掃描應用程式排除項目”視窗。
8. 選取“不監控應用程式活動”核取方塊。
9. 在“掃描應用程式排除項目”視窗中點擊“確定”。

您已新增的信任群組應用程式將出現在信任群組應用程式清單中。
10. 要儲存變更，請點擊“儲存”按鈕。

Kaspersky Endpoint Security 效能以及與其他應用程式的相容性

本章節除了包含如何選取可偵測威脅類型和 Kaspersky Endpoint Security 操作模式的資訊之外，還包含關於 Kaspersky Endpoint Security 效能以及與其他應用程式相容性的資訊。

關於 Kaspersky Endpoint Security 效能以及與其他應用程式的相容性

Kaspersky Endpoint Security 效能

Kaspersky Endpoint Security 效能指可偵測的威脅類型、電量消耗以及電腦資源使用。

選擇可偵測的威脅類型

Kaspersky Endpoint Security 將讓您精調電腦防護並選取執行期間應用程式偵測的物件類型。Kaspersky Endpoint Security 將持續掃描作業系統中的病毒、蠕蟲和木馬。您不能停用對這些威脅類型的掃描。此類惡意程式可能會給電腦帶來巨大的損害。為了更好地防護您的電腦，您可以透過啟動對合法應用程式的監控來擴大可偵測的威脅類型範圍，因為入侵者可能侵入這些應用程式損害電腦或使用者資料。

使用省電模式

對於行動式電腦來說，應用程式的電量消耗是一個關鍵的考慮因素。Kaspersky Endpoint Security 的排程工作通常會消耗可觀的資源。當電腦使用電池執行時，您可以使用省電模式，更加節省電量。

在省電模式下，以下排程工作將自動延遲：

- [更新工作](#)
- [完整掃描工作](#)
- [關鍵區域掃描工作](#)
- [自訂掃描工作](#)
- [弱點掃描工作](#)
- [完整性檢查工作](#)

無論是否啟用省電模式，Kaspersky Endpoint Security 將在筆記型電腦切換到電池電源時暫停加密工作。及當筆記型電腦從電池電源切換到主電源還原應用程式的加密工作。

允許其他應用程式使用電腦資源

Kaspersky Endpoint Security 使用電腦資源可能會影響到其他應用程式的效能表現。為了解決在 CPU 和硬碟子系統上的負載新增的條件下發生的同步執行的問題，Kaspersky Endpoint Security 可以暫停排程工作並將資源讓給其他應用程式。

不過，很多應用程式都會在 CPU 資源剛剛可用時立即載入，然後以背景模式執行。為了防止 Kaspersky Endpoint Security 根據其他應用程式的效能進行掃描，最好不要允許其他應用程式使用作業系統資源。

如有必要，您可以手動啟動這些工作。

使用進階解毒技術

如今的惡意程式能夠入侵作業系統的最底層，繼而無法順利清除。在作業系統中偵測到惡意活動之後，Kaspersky Endpoint Security 將使用特殊的[進階清除技術](#)執行廣泛的清除步驟。[進階解毒技術](#)致力於清除 RAM 中已啟動處理程序，以及封鎖 Kaspersky Endpoint Security 使用其他方式刪除它們的惡意程式。這些威脅將從電腦中清除。執行進階解毒過程時，我們建議您不要開啟新的程式或者編輯作業系統登錄檔。進階解毒技術會佔用相當多的作業系統資源，這可能會降低其他應用程式的執行速度。

在執行 Microsoft Windows for workstations 的電腦上執行完進階解毒過程後，Kaspersky Endpoint Security 將請求使用者授權，重新啟動電腦。系統重新啟動後 Kaspersky Endpoint Security 將刪除惡意軟體檔案並啟動“快速”電腦完整掃描。

由於 Kaspersky Endpoint Security for file servers 的具體設定，在執行 Microsoft Windows for file servers 的電腦上，將不會提示重新啟動。排程外檔案伺服器重新啟動，可能會導致檔案伺服器未儲存的資料遺失或暫時不可使用的情況。我們建議您在電腦重新啟動後開始一次尋找病毒和其他威脅的完整掃描工作。這就是為什麼預設情況下檔案伺服器[關](#)進階清除技術的原因。

如果偵測到檔案伺服器上有病毒感染，事件通知將傳遞到卡巴斯基安全管理中心，採取主動消毒。要對檔案伺服器進行解毒，請對檔案伺服器啟用活動解毒技術，並在檔案伺服器使用者合適的時間啟動“[病毒掃描](#)”群組工作。

選擇可偵測的威脅類型

若要選取可偵測的威脅類型，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側，選擇 **端點防護** 區域。
端點防護設定將顯示在視窗右方。
3. 在“物件”：區域中點擊“設定”按鈕。
“需偵測的物件”視窗將開啟。
4. 請選取您想要 Kaspersky Endpoint Security 偵測威脅類型旁邊的核取方塊。
 - 惡意工具
 - 廣告軟體
 - 自動撥號程式
 - 其他
 - 可能導致損壞的套件檔案
 - 多重封裝物件
5. 點擊“確定”。
“需偵測的物件”視窗將關閉。在“物件”區域中，所選威脅類型在“已啟用對以下物件類型的偵測”下方列出。
6. 要儲存變更，請點擊“儲存”按鈕。

啟用或停用進階解毒技術（工作站）

若要啟用或停用進階解毒技術（工作站），請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側，選擇 **端點防護** 區域。
端點防護設定將顯示在視窗右方。
3. 在視窗右側，執行下列操作：
 - 如果您希望 Kaspersky Endpoint Security 執行電腦進階解毒，請選取“**啟用進階解毒技術**”選框。
 - 如果您不希望 Kaspersky Endpoint Security 執行電腦進階解毒，請清除“**啟用進階解毒技術**”選框。
4. 要儲存變更，請點擊“儲存”按鈕。

透過卡巴斯基安全管理中心啟動進階解毒工作時，使用者無法使用作業系統的大多數功能。工作完成後工作站將重新啟動。

啟用或停用進階解毒技術 (檔案伺服器)

若要停用檔案伺服器的進階解毒技術，請執行下列操作之一：

- 在活動卡巴斯基安全管理中心政策內容中，啟用進階解毒技術。為此，請參閱以下執行操作：
 - a. 政策內容視窗開啟**一般防護設定**區域。
 - b. 選取“**啟用進階解毒技術**”核取方塊。
 - c. 若要儲存變更，點擊政策內容視窗中的“**確定**”。
- 在卡巴斯基安全管理中心的“病毒掃描”群組工作的內容中，選取“**執行進階解毒技術**”核取方塊。

若要停用檔案伺服器的進階解毒技術，請執行下列操作之一：

- 在卡巴斯基安全管理中心政策內容啟用進階解毒技術。為此，請參閱以下執行操作：
 - a. 政策內容視窗開啟**一般防護設定**區域。
 - b. 清除“**啟用進階解毒技術**”核取方塊。
 - c. 若要儲存變更，點擊政策內容視窗中的“**確定**”。
- 在卡巴斯基安全管理中心群組工作內容視窗的病毒掃描中，取消“**執行進階解毒技術**”核取方塊。

啟用或停用省電模式

若要啟用或停用省電模式，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側，選取“**進階設定**”區域。
進階程式設定將顯示在視窗右側。
3. 在“**執行模式**”區域中點擊“**設定**”按鈕。
“**執行模式**”視窗將開啟。
4. 在“**動作模式**”區域中執行以下操作：
 - 要啟用省電模式，請選取“**使用電池供電時推遲排程工作**”核取方塊。
啟用節能模式且電腦使用電池執行時，即使排程了以下工作，以下工作也不會執行：
 - 更新工作

- 完整掃描工作
 - 關鍵區域掃描工作
 - 自訂掃描工作
 - 弱點掃描工作
 - 完整性檢查工作
- 如果要停用省電模式，請清空“**使用電池供電時推遲排程工作**”核取方塊。在這種情況下，不論電腦電源供應如何，Kaspersky Endpoint Security 都將執行排程工作。

5. 要儲存變更，請點擊“**儲存**”按鈕。

啟用或停用允許其他應用程式使用資源

若要啟用或停用允許其他應用程式使用資源，請執行以下操作：

1. 開啟 [程式設定視窗](#)。
2. 在視窗左側，選取“**進階設定**”區域。
進階程式設定將顯示在視窗右側。
3. 在“**執行模式**”區域中點擊“**設定**”按鈕。
“**執行模式**”視窗將開啟。
4. 在“**動作模式**”區域中執行以下操作：
 - 如果您要啟用允許其他應用程式使用資源的模式，請選取“**將資訊讓給其他應用程式**”核取方塊。
當設定為允許其他應用程式使用資源時，Kaspersky Endpoint Security 將延遲會拖慢其他其他應用程式的排程工作：
 - 更新工作
 - 完整掃描工作
 - 關鍵區域掃描工作
 - 自訂掃描工作
 - 弱點掃描工作
 - 完整性檢查工作
 - 要停用其他應用程式使用資源的模式，請取消選定“**將資訊讓給其他應用程式**”核取方塊。在這種情況下，不論其他應用程式的操作如何，Kaspersky Endpoint Security 都將執行排程工作。

預設情況下，應用程式已設定為允許其他應用程式使用資源。

5. 要儲存變更，請點擊“**儲存**”按鈕。

密碼防護

本章節介紹關於限制使用密碼存取 Kaspersky Endpoint Security 的資訊。

關於存取 Kaspersky Endpoint Security 的限制

多個不同電腦知識水準的使用者可以共用一台電腦。如果使用者可以無限制存取 Kaspersky Endpoint Security 及其設定，則電腦防護的層級可能會下降。

您可以透過設定使用者名稱和密碼和指定應用程式提示使用者輸入驗證資訊進行操作來限制存取 Kaspersky Endpoint Security：

當先前版本應用程式升級到 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 時，系統不會儲存密碼（如果設定了密碼）。如果是首次編輯密碼防護設定，則使用預設使用者名 KAdmin。

啟用和停用密碼防護

我們建議您謹慎使用應用程式存取時所應用的密碼限制。如果您忘記密碼，請聯絡 [Kaspersky Lab 技術支援](#) 獲取有關停用密碼防護的說明。

若要啟用密碼防護，請執行下列操作：

1. 開啟 [程式設定視窗](#)。
2. 在視窗左側，選取“**進階設定**”區域。
應用程式設定將顯示在視窗右側。
3. 在“**密碼防護**”區域中點擊“**設定**”按鈕。
開啟“**密碼防護**”。
4. 選取“**啟用密碼防護**”核取方塊。
5. 在 **使用者名稱** 欄位中，輸入執行後續密碼防護的操作時必須在 **密碼檢查** 視窗中指定的使用者名稱。
6. 在“**新密碼**”欄位中輸入用於存取應用程式的密碼。
7. 確認“**確認密碼**”欄位中的密碼。
8. 如果您希望限制對應用程式所有操作的存取，請在“**密碼範圍**”區域中點擊“**全選**”按鈕。
9. 如果您希望選擇性地限制使用者存取，請在“**密碼範圍**”區域中選取相關操作名稱旁邊的核取方塊：
 - **調整應用程式設定**。

- 結束應用程式。
- 停用防護元件。
- 停用控制元件。
- 刪除金鑰。
- 移除/修改/還原應用程式。
- 還原存取加密裝置上的資料。
- 檢視報告。

10. 點擊“確定”按鈕。

然後程式將檢查輸入的密碼。如果密碼比對，應用程式將應用此密碼。如果密碼不比對，則程式將提示您再次在“**確認密碼**”欄位中確認密碼。

啟用密碼防護後，應用程式將在每次執行密碼範圍中的操作時提示輸入密碼。如果您不希望在目前連線中每當您嘗試執行密碼防護的操作時提示您輸入密碼，您可以在**密碼檢查**視窗中選中“**記住目前連線的密碼**”核取方塊。

取消“**記住密碼**”核取方塊後，表示應用程式將在您每次嘗試此操作時提示您輸入密碼。

若要停用密碼防護，請執行下列操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側，選取“**進階設定**”區域。
應用程式設定將顯示在視窗右側。
3. 在“**密碼防護**”區域中點擊“**設定**”按鈕。
開啟“**密碼防護**”。
4. 清空“**啟用密碼防護**”核取方塊。

僅當您以 KLAdmin 身分登入時，才能停用密碼防護。如果您使用任何其他使用者帳戶或臨時密碼，則無法停用密碼防護。

5. 點擊“確定”按鈕。

禁用密碼防護後，下次啟動 Kaspersky Endpoint Security 時將取消對應用程式的存取限制。

修改 Kaspersky Endpoint Security 存取密碼

若要修改 Kaspersky Endpoint Security 存取密碼，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側，選取“**進階設定**”區域。

3. 在“**密碼防護**”區域中點擊“**設定**”按鈕。
開啟“**密碼防護**”。
4. 在“**使用者名稱**”欄位中輸入使用者名稱。
5. 在“**新密碼**”欄位中輸入新的程式存取密碼。
6. 在“**確認密碼**”欄位再次輸入新密碼。

7. 點擊“**確定**”。

然後程式將檢查輸入的密碼。如果密碼對比，則程式將應用新密碼並關閉“**密碼防護**”視窗。如果密碼不比對，則程式將提示您再次在“**確認密碼**”欄位中確認密碼。

8. 要儲存變更，請在應用程式設定視窗中點擊“**儲存**”按鈕。

關於使用暫時密碼

使用受卡巴斯基安全管理中心政策管理的用戶端電腦時，使用者可能需要使用在政策等級密碼防護的 **Kaspersky Endpoint Security** 執行操作。啟用密碼防護時，只有卡巴斯基安全管理中心管理員可以執行密碼範圍內指定的操作。但是如果與卡巴斯基安全管理中心的連線遺失（例如當使用者不在公司網路內時），使用卡巴斯基安全管理中心本機介面進行的功能有限。

若要為使用者提供執行所需操作的能力而無需給予政策設定中設定的密碼，卡巴斯基安全管理中心管理員可以建立暫時密碼。暫時密碼擁有有限的有效期和有限的操作範圍。使用者在應用程式介面中輸入暫時密碼時，卡巴斯基安全管理中心管理員允許的操作將變為可用。

暫時密碼到期後，**Kaspersky Endpoint Security** 將繼續根據卡巴斯基安全管理中心政策的設定執行。在政策等級受密碼防護的操作將對使用者無效。

使用卡巴斯基安全管理中心管理主控台建立暫時密碼

若要建立暫時密碼並將其傳送給使用者：

1. 開啟卡巴斯基安全管理中心的管理主控台。
 2. 在主控台樹狀目錄中，在“**受管裝置**”資料夾中，開啟您要在為其請求暫時密碼的電腦使用者所屬管理群組名稱所對應的資料夾。
 3. 在工作區選取“**裝置**”頁籤。
 4. 在屬於使用者請求暫時密碼的電腦的右鍵選單中，選取“**內容**”。
- “**內容：<電腦名稱>**”視窗將會開啟。
5. 在“**內容：<電腦名稱>**”視窗中，選取“**應用程式**”區域。
 6. 選取 **Kaspersky Endpoint Security Service Pack 2 for Windows** 並使用以下方式之一開啟應用程式內容視窗：
 - 點擊螢幕底部的“**內容**”按鈕。
 - 在應用程式的右鍵選單中，選取“**內容**”。

這會開啟“應用程式設定<應用程式名稱>”視窗。

7. 在“進階設定”區域中， “應用程式設定<應用程式名稱>”視窗中選取“應用程式設定”子區域。
8. 在“密碼防護”區域中點擊“設定”按鈕。
開啟“密碼防護”。
9. 在“密碼防護”視窗中， 在“暫時密碼”區域中， 點擊“設定”按鈕。

如果在該電腦上執行的卡斯基安全管理中心政策中為卡斯基安全管理中心啟用了密碼防護，則該按鈕可用。

“建立臨時存取碼”視窗將開啟。

10. 在“到期日期”欄位中， 指定使用者不能再使用暫時密碼的日期。
在此日期， 暫時密碼將變為無效。必須建立新的暫時密碼才能在 Kaspersky Endpoint Security 本機介面中執行操作。
11. 在“暫時密碼範圍”表中， 選取暫時密碼有效時使用者可以使用的操作旁的核取方塊。
12. 點擊 **建立** 按鈕。
這會開啟包含加密密碼的“暫時密碼”視窗。
13. 複製密碼和 [使用說明](#) 並將其傳送給使用者。

在 Kaspersky Endpoint Security 介面中應用暫時密碼

這些說明的目標讀者是用戶端電腦上安裝有 Kaspersky Endpoint Security 的使用者。

若要套用暫時密碼：

1. 開啟 [程式設定視窗](#)。
2. 在視窗左側， 選取“進階設定”區域。
應用程式設定將顯示在視窗右側。
3. 在“密碼防護”區域中點擊“暫時密碼”按鈕。
“暫時密碼”視窗將開啟。
4. 選中“啟用暫時密碼”核取方塊。
5. 在該輸入欄位中指定從卡斯基安全管理中心管理員處獲得的密碼。
6. 點擊“確定”儲存變更。

應用暫時密碼後， 卡斯基安全管理中心管理員指定的操作將可用。“暫時密碼”視窗將顯示暫時密碼和允許操作的到期時間。

透過卡巴斯基安全管理中心遠端系統管理

本章節介紹如何透過卡巴斯基安全管理中心管理應用程式。

關於透過卡巴斯基安全管理中心管理應用程式

卡巴斯基安全管理中心允許您遠端安裝和移除、啟動和停止 Kaspersky Endpoint Security，配置應用程式設定，變更可用應用程式元件的集合，新增鍵以及啟動更新和掃描工作。

有關該文件中未提供的透過卡巴斯基安全管理中心管理應用程式的附加資訊，請參閱 *卡巴斯基安全管理中心管理手冊*。

可以使用卡巴斯基安全管理中心管理外掛程式透過 Kaspersky Endpoint Security 管理應用程式。

管理外掛程式的版本會根據用戶端電腦上所安裝 Kaspersky Endpoint Security 版本的不同而有所不同。如果所安裝的管理外掛程式版本比已安裝版本的 Kaspersky Endpoint Security 的功能少，則管理外掛程式不會管理缺失功能的設定。使用者可以在 Kaspersky Endpoint Security 本機介面修改這些設定。

使用其他版本管理外掛程式時的特別考慮

您可以使用管理外掛程式變更以下項：

- 政策
- 政策內容
- 群組工作
- 本機工作
- Kaspersky Endpoint Security 的本機設定

只有當您擁有的管理外掛程式版本等於或大於帶管理外掛程式的 Kaspersky Endpoint Security 相容資訊中指定的版本時才能透過卡巴斯基安全管理中心管理 Kaspersky Endpoint Security。您可以在 [安裝套件的 installer.ini](#) 檔案中檢視管理外掛程式的最低所需版本。

如果開啟了任何元件，管理外掛程式將檢查其相容資訊。如果管理外掛程式的版本等於或晚於相容資訊中指定的版本，您可以變更該元件的設定。否則您無法使用管理外掛程式變更選定元件的設定。建議升級管理外掛程式。

使用後續版本的管理外掛程式變更先前定義的設定

您可以使用後續版本的管理外掛程式變更所有先前定義的設定，並配置先前所使用版本的管理外掛程式中沒有的新設定。

對於新設定，後續版本的管理外掛程式會在第一次儲存政策、政策設定檔或工作時分配預設值。

使用後續版本的管理外掛程式變更政策、政策設定檔或群組工作時，這些元件將對先前版本的管理外掛程式不可用。Kaspersky Endpoint Security 的本機設定和本機工作的設定仍然對先前版本的管理外掛程式可用。

啟動和停止用戶端電腦上的應用程式

要在用戶端電腦上啟動或停止應用程式，請執行以下操作：

1. 開啟卡斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄的“**受管裝置**”資料夾中，開啟相關用戶端電腦所屬的**管理群組**名稱的資料夾。
3. 在工作區選取“**裝置**”頁籤。
4. 選取您想要啟動或停止應用程式的電腦。
5. 右鍵點擊以顯示用戶端電腦的右鍵選單并選取“**內容**”。
開啟用戶端電腦的內容視窗。
6. 在用戶端電腦內容視窗中，選取“**應用程式**”區域。
安裝在用戶端電腦上的 Kaspersky 應用程式清單將顯示在用戶端電腦內容視窗的右側。
7. 選取 Kaspersky Endpoint Security 10 for Windows。
8. 請執行以下操作：
 - 啟動應用程式，請點擊 Kaspersky 應用程式清單右側的  按鈕或執行以下操作：
 - a. 在 Kaspersky Endpoint Security 的右鍵選單中選取“**內容**”或點擊 Kaspersky Lab 應用程式清單下方的“**內容**”按鈕。
開啟“**Kaspersky Endpoint Security 10 for Windows 應用程式設定**”視窗。
 - b. 在“**一般**”區域中點擊視窗右側的“**正在執行**”。
 - 要停止 Kaspersky Endpoint Security，請點擊 Kaspersky Lab 應用程式清單右側的  按鈕或執行以下操作：
 - a. 在 Kaspersky Endpoint Security 的右鍵選單中選取“**內容**”或點擊 Kaspersky Lab 應用程式清單下方的“**內容**”按鈕。
開啟“**Kaspersky Endpoint Security 10 for Windows 應用程式設定**”視窗。
 - b. 在“**一般**”區域中點擊視窗右側的“**停止**”。

設定 Kaspersky Endpoint Security 設定

要設定 Kaspersky Endpoint Security 設定：

1. 開啟卡斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄的“**受管理裝置**”資料夾中，開啟相關用戶端電腦所屬的**管理群組**名稱的資料夾。
3. 在工作區選取“**裝置**”標籤。

4. 選取您想要為其配置 Kaspersky Endpoint Security 設定的電腦。
5. 在用戶端電腦的內容功能表中，選取“內容”。
開啟用戶端電腦的內容視窗。
6. 在用戶端電腦內容視窗中選取“應用程式”區域。
安裝在用戶端電腦上的 Kaspersky 應用程式清單將顯示在用戶端電腦內容視窗的右側。
7. 選取應用程式 Kaspersky Endpoint Security 10 for Windows。
8. 請執行以下操作之一：
 - 從 Kaspersky Endpoint Security 10 for Windows 的內容功能表中選取“內容”。
 - 點擊 Kaspersky 應用程式清單下方的“內容”按鈕。

開啟“Kaspersky Endpoint Security 10 for Windows 應用程式設定”視窗。

9. 在“進階設定”區域中，設定 Kaspersky Endpoint Security 設定以及報告和儲存設定。

“Kaspersky Endpoint Security for Windows 應用程式設定”視窗中的其他區域與卡巴斯基安全管理中心的標準應用程式區域相同。卡巴斯基安全管理中心管理手冊中提供這些部分的說明。

如果某個應用程式受到禁止變更特定設定的政策的限制，則在“進階設定”區域中配置應用程式設定時，您將無法編輯它們。

10. 若要儲存變更，請在“Kaspersky Endpoint Security 10 for Windows 應用程式設定”視窗中點選“確定”。

管理工作

本章節介紹如何管理 Kaspersky Endpoint Security 的工作。關於透過卡巴斯基安全管理中心進行工作管理的詳細資訊，請參見《卡巴斯基安全管理中心管理手冊》。

關於 Kaspersky Endpoint Security 工作

卡巴斯基安全管理中心透過工作控制用戶端電腦上的 Kaspersky 應用程式的活動。這些工作將實施主要的管理功能，例如金鑰安裝、電腦掃描以及資料庫和程式模組更新等。

您可以建立以下類型的工作來透過卡巴斯基安全管理中心管理 Kaspersky Endpoint Security。

- 為單獨的用戶端電腦設定的本機工作。
- 為一個或多個管理群組中的用戶端電腦設定的群組工作。
- 為不屬於管理群組的一組電腦設定的工作。

為管理群組之外的電腦整合設定的工作，僅應用於工作設定中指定的用戶端電腦。如果在設定某工作的電腦整合中加入了新的用戶端電腦，該工作將不套用於這些新的電腦。要使該工作套用於這些電腦，您可以建立一個新的工作或者編輯現有工作的設定。

若要遠端系統管理 Kaspersky Endpoint Security，您可以使用以下列出的任意類型的工作：

- **新增金鑰**。Kaspersky Endpoint Security 將安裝用於啟動程式的金鑰，包括備用金鑰。
- **變更應用程式元件**。Kaspersky Endpoint Security 將根據工作設定中指定元件清單在用戶端電腦上安裝和刪除元件。
- **清查**。Kaspersky Endpoint Security 將收集安裝在電腦上的所有應用程式的資訊以及儲存在電腦上的可執行應用程式資訊。

您可以啟用 DLL 模組和指令檔案清單。在這種情況下，卡巴斯基安全管理中心將接收已安裝 Kaspersky Endpoint Security 的電腦上已載入 DLL 模組的資訊和包含指令碼的檔案的資訊。

啟用清單 DLL 模組和指令檔案會顯著增加清單工作時長和資料庫大小。

- **更新**。Kaspersky Endpoint Security 將根據設定的更新工作來更新資料庫和應用程式模組。
- **回溯**。Kaspersky Endpoint Security 將回溯最新更新的資料庫和模組。
- **病毒掃描**。Kaspersky Endpoint Security 將對工作設定中指定的電腦區域執行病毒掃描。
- **檢查與 KSN 的連線**。Kaspersky Endpoint Security 將傳送有關 KSN 伺服器可使用性的查詢並更新 KSN 連線狀態。
- **完整性檢查**。Kaspersky Endpoint Security 將獲得有關用戶端電腦上已安裝應用程式模組的設定並掃描每個模組的數位簽章。
- **管理身分驗證代理帳戶**。執行該工作時，Kaspersky Endpoint Security 將生成指令，刪除、新增或修改身分驗證代理帳戶。

您可以對工作執行以下操作：

- 啟動、停止、暫停和還原工作。
- 建立新的工作。
- 編輯工作設定。

透過設定 Kaspersky Endpoint Security 的功能區存取權限，為每個擁有卡巴斯基安全管理中心管理伺服器存取權的使用者定義 Kaspersky Endpoint Security 工作設定的存取權限（讀取、寫入、執行）。若要配置存取 Kaspersky Endpoint Security 功能區的權限，請轉至卡巴斯基安全管理中心管理伺服器內容視窗“**安全**”區域中。

設定工作管理模式

若要在 Kaspersky Endpoint Security 本機介面中設定使用工作的模式：

1. 開啟卡巴斯基安全管理中心的管理主控台。

2. 在管理主控台樹狀目錄中，在“**受管裝置**”資料夾中，開啟您在 Kaspersky Endpoint Security 本機介面中為其設定工作使用模式的管理員群組名稱的資料夾。
3. 在工作區選擇“**政策**”頁籤。
4. 選擇所需政策。
5. 使用以下方式開啟“**內容: <政策名稱>**”視窗：
 - 在所選定項目右鍵選單中，選擇“**內容**”。
 - 點擊位於管理主控台工作區右側的“**設定政策**”連線。
6. 在“**進階設定**”區域中選取“**進階設定**”子區域。
7. 在“**執行模式**”區域中：
 - 如果您希望使用者在 Kaspersky Endpoint Security 的介面中和命令列中使用本機工作，則選取“**允許使用本機工作**”核取方塊。


如果該核取方塊被清空，則本機工作功能被停止。在此模式中，本機工作不根據排程執行。本機工作也無法在 Kaspersky Endpoint Security 本機介面中啟動或編輯，使用命令列工作時也無法進行。

 - 如果您希望使用者檢視群組工作清單，則選取“**允許顯示群組工作**”核取方塊。
 - 如果您希望使用者修改群組工作設定，則選取“**允許管理群組工作**”核取方塊。
8. 點擊“**確定**”儲存變更。
9. 套用政策。

有關實施卡巴斯基安全管理中心政策的詳細資訊，請查閱《*卡巴斯基安全管理中心管理手冊*》。

建立本機工作

若要建立本機工作，請執行以下操作：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄的“**受管裝置**”資料夾中，開啟相關用戶端電腦所屬的**管理群組** 名稱的資料夾。
3. 在工作區選取“**裝置**”頁籤。
4. 選取要建立本機工作的電腦。
5. 請執行以下操作之一：
 - 在用戶端電腦的右鍵選單中選取“**所有工作**”“**建立工作**”選項。
 - 在用戶端電腦的上下文功能表中，選取“**內容**”，並在顯示的“**內容: <電腦名稱>**”視窗中在“**工作**”標籤上點擊“**新增**”按鈕。
 - 在“**執行動作**”下拉清單中選取“**建立工作**”。

啟動“工作精靈”。

6. 請按照工作精靈的指示操作。

建立群組工作

若要建立群組工作，請執行以下操作：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 請執行以下操作之一：
 - 在管理主控台樹狀目錄中選取“**受管裝置**”資料夾，為卡巴斯基安全管理中心管理的所有電腦建立群組工作。
 - 在管理主控台樹狀目錄的“**受管裝置**”資料夾中，開啟相關用戶端電腦所屬的管理群組名稱的資料夾。
3. 在工作區選擇“**工作**”頁籤。
4. 點擊“**建立工作**”按鈕。
啟動“工作精靈”。
5. 請按照工作精靈的指示操作。

為裝置集合建立工作



要為裝置集合建立工作，請執行以下步驟：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 選取管理主控台樹狀目錄中的“**工作**”資料夾。
3. 點擊“**建立工作**”按鈕。
啟動“工作精靈”。
4. 請按照工作精靈的指示操作。
5. 在精靈的“**選取要分配工作的裝置**”視窗中，點擊“**將工作分配給裝置集合**”按鈕。
6. 在精靈視窗的右側，點擊“**選取**”按鈕。
“**裝置集合**”視窗將開啟。
7. 選擇所需的裝置。
8. 在“**裝置集合**”視窗中點擊“**確定**”。
9. 請按照工作精靈的指示操作。

啟動、停止、暫停和還原工作


如果用戶端電腦上正在執行 Kaspersky Endpoint Security [應用程式](#)，您可以透過卡巴斯基安全管理中心啟動、停止、暫停和還原此用戶端電腦上的工作。當 Kaspersky Endpoint Security 暫停時，執行工作將暫停並無法透過卡巴斯基安全管理中心啟動、停止、暫停或還原此工作。

若要啟動、停止、暫停或還原本機工作，請執行以下操作：


1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄的“**受管裝置**”資料夾中，開啟相關用戶端電腦所屬的**管理群組**名稱的資料夾。
3. 在工作區選取“**裝置**”頁籤。
4. 選取您想要啟動、停止、暫停或還原本機工作的電腦。
5. 右鍵點擊以顯示用戶端電腦的右鍵選單並選取“**內容**”。
開啟用戶端電腦的內容視窗。
6. 選擇 **工作** 頁籤。
本機工作清單將顯示在此視窗的右側。
7. 選取您想要啟動、停止、暫停或還原的本機工作。
8. 使用以下方式之一對工作執行必要的操作：
 - 右鍵點擊開啟本機工作上下文功能表，選取“**正在執行 / 停止 / 暫停 / 還原**”。
 - 要啟動或停止本機工作，請點擊本機工作清單右側的  /  按鈕。
 - 請執行以下操作：
 - a. 點擊本機工作清單中的“**內容**”按鈕，或者選取工作上下文功能表中的“**內容**”。
“**內容：<工作名稱>**”視窗將會開啟。
 - b. 在“**一般**”標籤中，點擊“**正在執行 / 停止 / 暫停 / 還原**”按鈕。

若要啟動、停止、暫停或還原群組工作，請執行以下操作：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄的“**受管裝置**”資料夾中，選取您想要啟動、停止、暫停或還原群組工作的管理群組名稱資料夾。
3. 在工作區選擇“**工作**”頁籤。
群組工作將顯示在視窗右側。
4. 選取您想要啟動、停止、暫停或還原的群組工作。
5. 使用以下方式之一對工作執行必要的操作：

- 在群組工作的上下文功能表中，選取“正在執行 / 停止 / 暫停 / 還原”。
- 點擊視窗右側的  按鈕可啟動或停止群組工作。
- 請執行以下操作：
 - a. 點擊管理主控台工作區右側中的“工作設定”連結，或者在工作上下文功能表中選取“內容”。“內容：<工作名稱>”視窗將會開啟。
 - b. 在“一般”標籤中，點擊“正在執行 / 停止 / 暫停 / 還原”按鈕。

若要啟動、停止、暫停或還原選取電腦的工作，請執行以下操作：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄的“工作”資料夾中，選取您想要啟動、停止、暫停或刪除的選取電腦工作。
3. 請執行以下操作之一：
 - 在工作上下文功能表中，選取“正在執行 / 停止 / 暫停 / 還原”。
 - 點擊視窗右側的  按鈕可啟動或停止特定電腦的工作。
 - 請執行以下操作：
 - a. 點擊管理主控台工作區右側中的“工作設定”連結，或者在工作上下文功能表中選取“內容”。“內容：<工作名稱>”視窗將會開啟。
 - b. 在“一般”標籤中，點擊“正在執行 / 停止 / 暫停 / 還原”按鈕。

編輯工作設定

要編輯本機工作設定，請執行以下操作：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄的“受管裝置”資料夾中，開啟相關用戶端電腦所屬的管理群組 @名稱的資料夾。
3. 在工作區選取“裝置”頁籤。
4. 選取您想要為其配置應用程式設定的電腦。
5. 右鍵點擊以顯示用戶端電腦的右鍵選單并選取“內容”。
開啟用戶端電腦的內容視窗。
6. 選擇 **工作** 頁籤。
本機工作清單將顯示在此視窗的右側。
7. 在本機工作清單中選取所需的本機工作。
8. 使用以下方式開啟“內容：<政策名稱>”視窗：

- 在所選定項目右鍵選單中，選擇“內容”。
- 點擊位於管理主控台工作區右側的“設定政策”連線。

9. 在“內容：<本機工作名稱>”視窗中，選取“設定”區域。

10. 編輯本機工作設定

11. 若要儲存設定，請在“內容：<本機工作名稱>”視窗中，點擊“確定”。

12. 若要儲存設定，請在“內容：<政策名稱>”視窗，點擊“確定”按鈕。

要編輯群組設定，請執行以下操作：

1. 開啟卡斯基安全管理中心的管理主控台。
2. 在“受管裝置”的資料夾中，開啟相關管理群組名稱的資料夾。
3. 在工作區選擇“工作”頁籤。
群組工作顯示在管理主控台工作區中。
4. 選取所需的群組工作。
5. 使用以下方式開啟“內容：<政策名稱>”視窗：

- 在所選定項目右鍵選單中，選擇“內容”。
- 點擊位於管理主控台工作區右側的“設定政策”連線。

6. 在“內容：<群組工作名稱>”視窗中，選取“設定”區域。

7. 編輯群組工作設定：

8. 若要儲存變更，請在“內容：<群組工作名稱>”視窗中，點擊“確定”。

要編輯電腦集中工作設定，請執行以下操作：

1. 開啟卡斯基安全管理中心的管理主控台。
2. 在主控台樹狀目錄的“工作”資料夾中，選取您想要編輯其設定的電腦集工作。
3. 使用以下方式開啟“內容：<政策名稱>”視窗：

- 在所選定項目右鍵選單中，選擇“內容”。
- 點擊位於管理主控台工作區右側的“設定政策”連線。

4. 在“內容：<電腦集工作名稱>”視窗，選取“設定”選項。

5. 編輯電腦集的工作設定。

6. 若要變更設定，請在“內容：<電腦集工作名稱>”視窗中點選“確定”。

除了“設定”部份之外，工作內容視窗中的所有其他部份都與卡斯基安全管理中心是一樣的。有關詳細說明，請參閱 *卡斯基安全管理中心管理手冊*。“設定”區域包含 Kaspersky Endpoint Security 10 for Windows 特定設定。其內容取決於選定工作或工作類型。

管理政策

本章節將敘述如何建立並設定您的 Kaspersky Endpoint Security 政策。關於使用卡巴斯基安全管理中心政策管理 Kaspersky Endpoint Security 的詳情，請參閱 *卡巴斯基安全管理中心管理手冊*。

關於政策

您可以使用政策讓同一 Kaspersky Endpoint Security 設定應用於一個管理群組的所有用戶端電腦中。

您可以使用 Kaspersky Endpoint Security 在管理群組中本機變更為每個電腦指定的設定值。您可以本機變更那些政策未封鎖其變更的設定。

政策的設定中是否顯示“鎖定”決定使用者電腦的應用程式設定是否可以編輯。

- 如果設定被“鎖定” (🔒)，您無法本機編輯該設定的值。政策中指定的設定值將用於管理群組中所有用戶端中。
- 當設定被“解鎖”(🔓)後，您可以在本機編輯該設定。如果在本機編輯某設定，重新設定的設定將套用於管理群組中的該用戶端電腦。不套用由政策配置的設定。

首次套用政策後，本機應用程式的設定將根據政策設定進行改變。

為每個擁有卡巴斯基安全管理中心管理伺服器存取權限的使用者指定存取政策設定的權限（讀取、寫入、執行），並為 Kaspersky Endpoint Security 的每個功能範圍單獨指定政策設定。若要設定存取政策設定的權限，請轉至卡巴斯基安全管理中心 Administration Server 內容視窗“安全”區域中。

Kaspersky Endpoint Security 的以下功能範圍將出現：

- 病毒防護。功能範圍包括檔案防護、郵件防護、網頁防護、即時通訊防護、弱點掃描和掃描工作。
- 應用程式啟動控制。功能範圍包括“應用程式啟動控制”元件。
- 裝置控制。功能範圍包括“裝置控制”元件。
- 加密。該功能範圍包含硬碟、檔案和資料夾加密元件。
- 信任區域。該功能範圍包括信任區域。
- Web 控制。功能範圍包括“Web 控制”元件。
- 入侵防護。該功能範圍包括應用程式活動監控、弱點監控、防火牆、網路攻擊防護和應用程式權限控制。
- 一般功能。該功能範圍包括沒有為其他功能範圍指定的一般應用程式設定，包括：產品授權、KSN 設定、清查工作、應用程式資料庫和模組更新工作、自我防護、進階應用程式設定、報告和儲存、密碼防護設定和應用程式介面設定。

您可以對政策執行以下操作：

- 建立政策。
- 編輯政策設定。

如果您存取管理伺服器所用的使用者帳戶沒有權限編輯某些功能範圍，則無法編輯這些功能範圍的設定。

- 刪除政策。
- 變更政策狀態。

有關與 Kaspersky Endpoint Security 互動無關的政策使用資訊，請參閱 *卡巴斯基安全管理中心管理手冊*。

建立政策

若要建立政策，請執行以下操作：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 請執行以下操作之一：
 - 如果您希望為卡巴斯基安全管理中心管理的所有電腦建立政策，在管理主控台樹狀目錄中選取“**受管裝置**”資料夾。
 - 在管理主控台樹狀目錄的“**受管裝置**”資料夾中，開啟相關用戶端電腦所屬的管理群組名稱的資料夾。
3. 在工作區選擇“**政策**”頁籤。
4. 請執行以下操作之一：
 - 點擊“**建立政策**”按鈕。
 - 右鍵點擊開啟上下文功能表並選取“**建立政策**”。

啟動“政策精靈”。

5. 按照“政策精靈”的說明進行操作。

編輯政策設定

若要編輯政策設定，請執行以下操作：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄的“**受管裝置**”資料夾中，開啟您希望為其編輯政策設定的相關管理群組所在的資料夾。
3. 在工作區選擇“**政策**”頁籤。
4. 選擇所需政策。
5. 使用以下方式開啟“**內容: <政策名稱>**”視窗：
 - 在所選定項目右鍵選單中，選擇“**內容**”。

- 點擊位於管理主控台工作區右側的“**設定政策**”連線。

Kaspersky Endpoint Security 10 for Windows 政策設定包括元件設定和[應用程式設定](#)。“內容：<政策名稱>”視窗的“**端點防護**”和“**端點控制**”區域將顯示防護和控制元件的設定，“**資料加密**”區域將顯示檔案和資料夾的加密設定，“**進階設定**”區域將顯示應用程式設定。

若要啟用在政策設定中顯示資料加密設定和控制元件設定，您必須選取卡巴斯基安全管理中心的“**介面設定**”視窗中相應的核取方塊。

6. 編輯政策設定。
7. 若要儲存您的設定，請在“內容：<政策名稱>”視窗，點擊“**確定**”按鈕。

選取要顯示在卡巴斯基安全管理中心政策中的設定

若要選取要顯示在卡巴斯基安全管理中心政策中的設定：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄的“**管理主控台 - <電腦名稱>**”節點的右鍵選單中選取“**檢視→ 介面設定**”。“**介面設定**”視窗將開啟。
3. 在“**介面設定**”視窗中，選取需要顯示在卡巴斯基安全管理中心政策建立設定和政策內容中的設定旁的核取方塊。
 - 選取“**顯示端點功能設定**”核取方塊啟用在卡巴斯基安全管理中心的政策精靈，並在政策內容視窗顯示控制元件的設定。
 - 選取“**顯示加密與資料防護**”核取方塊啟用在卡巴斯基安全管理中心的新政策精靈，並在政策內容中顯示“資料加密”設定。
4. 點擊“**確定**”。

將使用者訊息傳送至卡巴斯基安全管理中心伺服器

在以下情況下，使用者可能需要向本機公司網路系統管理員傳送郵件：

- 裝置控制封鎖對此裝置的存取。
請求被封鎖裝置存取權限的郵件範本在“[裝置控制](#)”區域中 Kaspersky Endpoint Security 介面內。
- 應用程式啟動控制封鎖了某個應用程式的啟動。
請求被封鎖裝置存取權限的郵件範本在“[應用程式啟動控制](#)”區域中 Kaspersky Endpoint Security 介面內。
- 網頁控制封鎖對網頁資源的存取。
請求被封鎖網頁資源存取權限的郵件範本在“[網頁控制](#)”區域中 Kaspersky Endpoint Security 介面內。

用於傳送訊息的方式和所使用的範本取決於安裝 Kaspersky Endpoint Security 的電腦上執行卡巴斯基安全管理中心政策，是否連線了卡巴斯基安全管理中心管理伺服器。有以下情景：

- 如果安裝了卡巴斯基安全管理中心的電腦上沒有執行卡巴斯基安全管理中心政策，使用者的訊息將透過電子郵件傳送給本機區域網路管理員。
訊息欄位的內容將來自 Kaspersky Endpoint Security 本機介面中定義的範本。
- 如果安裝了卡巴斯基安全管理中心的電腦上執行著卡巴斯基安全管理中心政策，標準訊息將傳送至卡巴斯基安全管理中心管理伺服器。
在這種情況下，可以在[卡巴斯基安全管理中心事件儲存中](#)檢視使用者訊息。訊息欄位的內容將來自卡巴斯基安全管理中心政策中定義的範本。
- 卡巴斯基安全管理中心漫遊政策執行在安裝了 Kaspersky Endpoint Security 的電腦上，用於傳送郵件的方法將取決於是否連線了卡巴斯基安全管理中心。
 - 如果建立了與卡巴斯基安全管理中心的連線，Kaspersky Endpoint Security 會將標準郵件傳送至卡巴斯基安全管理中心管理伺服器。
 - 如果沒有卡巴斯基安全管理中心連線，則使用者的訊息透過電子郵件傳送給本機區域網路管理員。
 在這兩種情況中，訊息欄位的內容將來自卡巴斯基安全管理中心政策中定義的範本。

在卡巴斯基安全管理中心事件儲存中檢視使用者訊息

[“應用程式啟動控制”](#)、[“裝置控制”](#)和[“網頁控制”](#)元件允許區域網路使用者使用已安裝 Kaspersky Endpoint Security 的電腦向管理員傳送訊息。

使用者可以使用兩種方法將訊息傳送給管理員：

- 作為卡巴斯基安全管理中心事件儲存中的事件。
如果安裝在使用者電腦上的 Kaspersky Endpoint Security 應用程式在活動政策下工作，則使用者事件將傳送到 Kaspersky 安全中心事件儲存中。
- 作為電子郵件資訊。
如果使用者電腦上安裝的 Kaspersky Endpoint Security 應用程式並沒有使用政策或者使用不在辦公室政策，則使用者資訊透過電子郵件傳送。

若要在卡巴斯基安全管理中心事件儲存中檢視使用者訊息，請執行以下操作：

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄的“**管理伺服器**”中選取“**事件**”標籤。
卡巴斯基安全管理中心工作區將顯示 Kaspersky Endpoint Security 執行期間發生的所有事件，包括接收自區域網路使用者傳送給管理員的郵件。
3. 若要設定事件篩選，則在“**選取事件**”下拉清單中選取“**使用者要求**”。
4. 在事件清單中選取傳送給管理員的訊息。
5. 透過以下方式之一開啟“**事件設定**”視窗：
 - 右鍵點擊。以顯示事件的右鍵選單並選取“**內容**”。
 - 點擊管理主控台工作區右側的“**開啟事件內容視窗**”按鈕。

加入卡巴斯基安全網路

本章節介紹關於如何加入卡巴斯基安全網路的資訊以及如何啟動和停用卡巴斯基安全網路。

關於加入卡巴斯基安全網路

為了更有效地防護您的電腦，Kaspersky Endpoint Security 將使用從全球使用者收集的資料。卡巴斯基安全網路設計用於收集此資料。

卡巴斯基安全網路 (KSN) 是一個雲端服務的基礎架構。它可以存取線上 Kaspersky Lab 知識庫。該知識庫中包含了檔案信譽、網頁資源和軟體的相關資訊。使用卡巴斯基安全網路的資料可確保 Kaspersky Endpoint Security 能夠更快地對新型威脅作出回應，提高一些防護元件的效能，並減少誤報風險。

根據基礎架構的具體位址，有全球 KSN 服務（基礎架構由 Kaspersky Lab 伺服器託管）和地區 KSN 服務（基礎架構由協力廠商伺服器託管，如在網際網路服務供應商的網路中）。

變更產品授權後，為了能使用地區 KSN，請將新產品授權的資訊提交給服務供應商。否則將無法與 KSN 交換資料。

感謝加入卡巴斯基安全網路的使用者，使 Kaspersky Lab 能夠即時快速地接收威脅的類型資訊和來源資訊，研發出使其失效的方法，並最大限度地降低應用程式元件顯示的誤報。

參與 KSN 期間，程式會自動將程式運行期間生成的統計資訊傳送給 KSN。應用程式也會將駭客用來損壞電腦或資料的某些特定檔案（或部分檔案）傳送給 Kaspersky Lab 進行額外掃描。

個人資料將不會被收集、處理或儲存。有關在參與 KSN 期間生成的 Kaspersky Lab 統計資訊的傳送詳情，以及有關此類資訊的儲存和銷毀，請參閱卡巴斯基安全網路聲明和 [Kaspersky Lab 網站](#)。ksn_<language ID>.txt 檔案和卡巴斯基安全網路聲明包含在應用程式安裝套件中。

為了降低 KSN 伺服器的負荷，Kaspersky 可能會發佈應用程式防毒資料庫，暫時停用或部分限制對卡巴斯基安全網路的請求。在這種情況下，[KSN 的連線狀態](#)將顯示為 [有限制啟用](#)。

受卡巴斯基安全管理中心管理伺服器管理的使用者電腦可以透過 KSN 代理服務與 KSN 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 代理暫存處理過的資料，從而減少外部網路連接上的負荷，並加快使用者接收資料的速度。

有關 KSN 代理服務的詳細資訊，請參閱《卡巴斯基安全管理中心管理手冊》。

可以在 [卡巴斯基安全管理中心政策](#)的內容中配置 KSN 代理服務設定。

加入卡巴斯基安全網路是自發性的。應用程式將在初始化設定期間邀請使用者參加 KSN。使用者可以隨時開始或停止加入 KSN。

啟用和停用卡巴斯基安全網路

若要啟用和停用卡巴斯基安全網路，請執行以下操作：

1. 開啟[程式設定視窗](#)。
2. 在視窗左側的“**進階設定**”區域中選取“**KSN 設定**”子區域。
卡巴斯基安全網路設定將顯示在視窗右方。
3. 請執行以下操作之一：
 - 如果要啟用卡巴斯基安全網路，請選取“**我接受 KSN 聲明與參與條款**”核取方塊。
 - 如果要停用卡巴斯基安全網路，請清空“**我接受 KSN 聲明與參與條款**”核取方塊。
4. 要儲存變更，請點擊“**儲存**”按鈕。

檢查與卡巴斯基安全網路的連線

若要檢查與卡巴斯基安全網路的連接，請執行以下操作：

1. 開啟“[程式主視窗](#)”。
2. 在此視窗的上部，點擊“**卡巴斯基安全網路**”按鈕。

開啟“**卡巴斯基安全網路**”視窗。

在“**卡巴斯基安全網路**”視窗的左側，以圓形**KSN**按鈕形式顯示連接卡巴斯基安全網路的模式：

- 如果 Kaspersky Endpoint Security 未連線至卡巴斯基安全網路，**KSN** 按鈕呈灰色。**KSN** 按鈕下方顯示的狀態為“*停用*”。
- 如果 Kaspersky Endpoint Security 連線於卡巴斯基安全網路並且 KSN 伺服器可用，**KSN** 按鈕呈綠色。在“**KSN**”按鈕下方顯示下列資訊：*啟用*狀態，使用的 KSN 類型 – **私有 KSN** 或**全球 KSN**，以及與 KSN 伺服器的上一次同步日期和時間。該視窗的右側顯示檔案、網頁資源和軟體的信譽。

當您開啟“**卡巴斯基安全網路**”視窗時，Kaspersky Endpoint Security 將收集 KSN 視窗使用情況統計資料。此統計資料並不即時更新。

- 如果 Kaspersky Endpoint Security 連線於卡巴斯基安全網路但是 KSN 伺服器不可用，**KSN** 按鈕呈綠色。**KSN** 按鈕下方顯示的狀態為“*已啟用*”。

如果與 KSN 伺服器的上一次同步時間超過 15 分鐘，或者“*未知*”狀態，這表示 KSN 伺服器不可用。在此狀態下，建議您聯絡技術支援或您的服務提供者。

下列原因可導致無法連線卡巴斯基安全網路伺服器：

- 電腦未連線網際網路。

- 程式尚未啟動或產品授權已到期。
- 偵測到產品授權相關問題（例如產品授權已進入黑名單）。

在卡巴斯基安全網路中檢查檔案信譽

KSN 服務允許您獲取 Kaspersky Lab 信譽資料庫中包括的有關應用程式的資訊。這會在公司等級啟用彈性管理應用程式的啟動政策，以此防止犯罪分子用來損害您電腦或個人資料的惡意軟體和其他程式的啟動。

若要在卡巴斯基安全網路中檢查檔案信譽：

1. 點擊右鍵調出您要檢查其信譽的檔案的內容功能表。
2. 選取“**檢查 KSN 中的信譽**”選項。

如果您接受了“[卡巴斯基安全網路聲明](#)”條款則該核取方塊可用。

這會開啟“<檔案名稱> - KSN 中的信譽”視窗。“<檔案名稱> - KSN 中的信譽”視窗將顯示有關檔案的以下資訊：

- **路徑**。檔案儲存在磁碟上的路徑。
- **版本**。應用程式版本（僅顯示可執行檔的資訊）。
- **數位簽章**。顯示檔案的數位簽章。
- **已簽章**。對數位簽章的憑證簽章的日期。
- **建立日期**。檔案建立日期。
- **修改日期**。檔案上次修改日期。
- **大小**。檔案所佔用磁碟空間。
- 有關多少使用者信任該檔案或封鎖該檔案的資訊。

使用卡巴斯基安全網路增強防護

Kaspersky Lab 透過卡巴斯基安全網路為使用者提供進階的防護。這項防護措施設計用於處理進階永久的威脅和零日攻擊。整合了雲端技術和 Kaspersky Lab 專業的病毒分析的 Kaspersky Endpoint Security，將成為防護最複雜的網路威脅的不二選取。

可在 Kaspersky Lab 網站上檢視有關 Kaspersky Endpoint Security 增強防護的詳細資訊。

關於應用程式的資訊源

Kaspersky 網站上的 Kaspersky Endpoint Security 頁面

在 [Kaspersky Endpoint Security 網頁](#) 上，您可以檢視有關應用程式及其功能和特性的一般資訊。

Kaspersky Endpoint Security 頁面包含線上商店連結。您可以在此購買或續約應用程式。

知識庫中的 Kaspersky Endpoint Security 頁面

*知識庫*是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。

知識庫文章不僅僅可以回答有關 Kaspersky Endpoint Security 的問題，也能解決其他 Kaspersky Lab 應用程式的問題。知識庫中的文章也包含技術支援發布的新聞。

在網路論壇上討論 Kaspersky Lab 的應用程式

如果您的問題尚未需要迫切性的答案，您可以與下列卡巴斯基官方論壇上的專家及其他使用者進行 [討論](#)。在這個論壇中您可以觀看現有的主題，留下您的建議，與建立新主題。

在這個論壇中您可以觀看現有的主題，留下您的建議，與建立新主題。

聯絡技術支援

本部分說明了獲得技術支援的方式和適用的條款。

如何取得技術支援

如果您無法在應用程式文件中或[應用程式相關資訊源](#)中找到您問題的解決方案，建議您聯絡技術支援。技術支援服務專家會為您解答關於安裝和使用該應用程式的任何問題。

技術支援僅提供給購買了正式版產品授權的使用者。使用試用版產品授權的使用者無法獲得技術支援。

與技術支援部門聯絡之前，請閱讀[支援規則](#)。

您可以透過以下方式取得技術支援

- [致電技術支援](#)
- 透過 [Kaspersky CompanyAccount 網站](#) 向 Kaspersky Lab 技術支援傳送請求

電話技術支援

您可以在世界大多數區域致電技術支援代表。您可以在 [Kaspersky 技術支援網站](#) 上找到在您區域獲得技術支援和技術支援聯絡方式的資訊。

與技術支援部門聯絡之前，請閱讀[支援規則](#)。

透過 Kaspersky CompanyAccount 取得技術支援

[Kaspersky CompanyAccount](#) 是為使用 Kaspersky 應用程式的公司提供的網站。Kaspersky CompanyAccount 網站旨在透過電子請求促進使用者與 Kaspersky 專家之間的互動。您可以使用 Kaspersky CompanyAccount 網站跟蹤您的線上請求和狀態並儲存這些請求的歷史。

您可以在一個 Kaspersky CompanyAccount 帳戶下註冊您所有的公司員工。單個帳戶能讓您集中管理註冊員工向 Kaspersky 傳送的電子請求單，同時透過 Kaspersky CompanyAccount 管理這些員工的權限。

Kaspersky CompanyAccount 網站擁有以下語言版本：

- 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

若要瞭解有關 Kaspersky CompanyAccount 的更多資訊，請存取[技術支援網站](#)。

為技術支援部門收集資訊

在您告知技術支援專家您的問題之後，他們可能請您建立一個 *偵錯檔案*。使用偵錯檔案可以偵錯逐步執行應用程式命令的過程，並確定應用程式操作中發生錯誤的階段。

技術支援專家可能需要更多相關資訊，關於作業系統、電腦中執行的處理程序、應用程式元件操作的詳細報告，以及應用程式故障傾印。

您可在 Kaspersky Endpoint Security 的說明下收集必要的資訊。收集的資訊可以儲存在硬碟上並在您最方便的時候上傳。

執行診斷時，技術支援專家將要求您透過以下方式變更應用程式設定：

- 收集啟動功能的詳細診斷資訊。
- 微調某些無法透過標準使用者介面進行調整的程式元件設定。
- 變更所收集資訊的儲存和傳輸設定。
- 設定網路流量擷取和記錄。

技術支援專家將提供一切所需的資訊來執行這些操作（包含描述步驟順序進行修改設定，設定檔，scripts，額外的命令功能，除錯模組，特殊工具等），並告知您調整的目的與收集的資料範圍。收集擴充的診斷資訊儲存在使用者的電腦上。收集的資料將不會自動傳輸給 Kaspersky Lab。

用於確定傳送給 Kaspersky Lab 的轉儲檔案所在轉儲伺服器位址的設定儲存在使用者電腦上。如果需要可在作業系統登錄檔 "DumpServerConfigUrl"="https://dmppcfg.kaspersky-labs.com/dumpserver/config.xml" 中編輯這些設定的值。

以上列出的操作請在技術支援專家的引導下，按照指示操作。沒有依照管理手冊或技術支援專家的指導方式變更應用程式設定可能造成系統損壞，影響電腦安全性危及正在處理的檔案可用性和完整性。

建立偵錯檔案

若要建立偵錯檔案，請執行以下操作：

1. 開啟[「程式主視窗」](#)。
2. 在主應用程式視窗中，點擊  按鈕。

“支援”視窗將開啟。

3. 在“支援”視窗中，點擊“系統偵錯”按鈕。

開啟“技術支援資訊”視窗。

4. 要啟動偵錯處理程序，請選取“啟用偵錯”核取方塊。

5. 在“等級”下拉清單中，選取偵錯等級。

我們建議您透過技術支援專家瞭解所需偵錯等級。如果技術支援專家未提供指導，請將偵錯等級設定為“普通(500)”。

6. 再現發生問題的狀況。

7. 若要停止偵錯處理程序，返回至“技術支援資訊”視窗並清空“啟用偵錯”核取方塊。

建立偵錯檔案後，您可繼續執行[將偵錯結果上傳至 Kaspersky Lab 伺服器](#)。

偵錯檔案的內容和儲存

使用者個人應對所收集資料的安全負責，特別是監控和限制對電腦上所收集資料的存取，直至將其提交至 Kaspersky Lab。

應用程式在使用期間，偵錯檔案以修正的格式儲存在電腦中。當應用程式被移除後，偵錯檔案將被永久刪除。

偵錯檔案儲存在 ProgramData\Kaspersky Lab 資料夾中。

偵錯檔案擁有以下名稱格式：KES<version number_dateXX.XX_timeXX.XX_pidXXX.><偵錯檔案類型>.log.enc1。

身分驗證代理偵錯檔案儲存在系統卷資訊資料夾中，並且擁有以下名稱：KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin。

您可以檢視偵錯檔案中儲存的資料。請聯絡 Kaspersky Lab 技術支援獲得如何檢視資料的說明。

所有偵錯檔案都包含下列通用資料：

- 事件時間。
- 執行線程編號。

身分驗證代理偵錯檔案不包含該資訊。

- 引起該事件的應用程式元件。
- 事件嚴重程度（通知性事件、警告、嚴重事件、錯誤）。
- 關於應用程式元件命令執行和命令執行結果的事件說明。

SRV.log、GUI.log 和 ALL.log 偵錯檔案的內容

SRV.log、GUI.log 和 ALL.log 偵錯檔案可儲存一般資料之外的下列資訊：

- 個人資料，包括姓氏、名字和中間名，如果此資料封包含在本機電腦檔案的路徑中。
- 使用者名稱和密碼，如果它們公開傳輸。在網際網路流量掃描期間，此資料可被記錄偵錯檔案中。偵錯檔案只記錄來自 trafmon2.ppl 的流量。
- 使用者名稱和密碼，如果它們包含在 HTTP 標題中。
- Microsoft Windows 帳戶名稱，如果該帳戶名稱包含在檔案名中。
- 包含您的帳戶名和密碼的電子郵件位址或網頁位址，如果它們包含在被偵測的物件名中。
- 您存取的網站和從這些網站被重定向的網站。當應用程式掃描網路時，將會把此資料寫入偵錯檔案。
- 登入代理伺服器的代理伺服器位址、電腦名稱、連接埠、IP 位址和使用者名稱。當應用程式使用代理伺服器時，將會把此資料寫入偵錯檔案。
- 您的電腦要與其建立連接的遠端 IP 位址。
- 郵件主題、ID、社群網路寄件者網頁的寄件者名稱和位址。當啟用網頁控制元件時，將會把此資料寫入偵錯檔案。

HST.log、BL.log、Dumpwriter.log、WD.log 和 AVPCon.dll.log 偵錯檔案的內容

除了一般資料之後，HST.log 偵錯檔案包含關於資料庫執行和程式模組更新工作的資訊。

除了一般資料之外，BL.log 偵錯檔案包含應用程式執行期間發生的事件資訊，以及對應用程式錯誤進行故障排除所需的資料。如果使用 avp.exe -bl 參數啟動應用程式，將建立此檔案。

除了一般資料之外，當進行應用程式記憶體傾印時，Dumpwriter.log 偵錯檔案包含對錯誤進行故障排除時必要服務資訊。

除了一般資料之外，WD.log 偵錯檔案包含 avpsus 服務執行期間所發生的事件資訊，包括應用程式模組更新事件。

除了一般資料之外，AVPCon.dll.log 偵錯檔案包含卡斯基安全管理中心連接模組執行期間所發生的事件資訊。

應用程式外掛程式偵錯檔案的內容

除了一般資料之外，應用程式外掛程式偵錯檔案包含下列資訊：

- 從右鍵功能表開啟掃描的外掛程式的 shellex.dll.log 偵錯檔案包含掃描工作執行資訊和調試外掛程式所需的資料。
- 郵件防護外掛程式 mcou.OUTLOOK.EXE 偵錯檔案包含電子郵件的部分內容，包括電子郵件位址。

身分驗證代理偵錯檔案的內容

除了一般資料之外，身分驗證代理偵錯檔案包含身分驗證代理執行資訊和使用者使用身分驗證代理所執行操作的資訊。

啟用和停用提示向卡巴斯基實驗室發送傾印和偵錯檔案

若要啟用或停用向 Kaspersky Lab 傳送傾印和偵錯檔案：

1. 開啟 [程式設定視窗](#)。
2. 在視窗左側，選取“**進階設定**”區域。
進階程式設定將顯示在視窗右側。
3. 在“**執行模式**”區域中點擊“**設定**”按鈕。
“**執行模式**”視窗將開啟。
4. 在“**執行模式**”視窗中，選取“**啟用傾印寫入**”核取方塊啟用應用程式寫入應用程式轉儲檔案。
5. 請執行以下操作之一：
 - 如果您希望應用程式在下次應用程式啟動時在“**上傳技術支援資訊至伺服器**”視窗中提示您將傾印和偵錯檔案傳送至 Kaspersky Lab，以分析應用程式關閉原因，請選定“**向 Kaspersky Lab 傳送傾印和偵錯檔案進行分析**”核取方塊。
 - 否則清空“**向 Kaspersky Lab 傳送傾印和偵錯檔案**”核取方塊。
6. 在“**執行模式**”視窗中點擊“**確定**”。
7. 若要儲存變更，則在主程式視窗中點擊“**儲存**”按鈕。

將檔案傳送給技術支援伺服器

包含作業系統、偵錯檔案和轉儲檔案資訊的檔案必須被傳送給 Kaspersky Lab 技術支援專家。

若要將檔案傳送給技術支援伺服器：

1. 在 Kaspersky Endpoint Security 任何時候出現執行故障時重新開機。
這會開啟“**上次應用程式啟動失敗**”視窗。

Kaspersky Endpoint Security 每次啟動時都會顯示“**上次應用程式啟動失敗**”視窗（包括重新啟動電腦後），直至您將傾印檔案或跟蹤檔案傳送給技術支援或您點擊**不傳送**按鈕為止。

2. 在“**先前應用程式啟動失敗**”視窗中，點擊**此處**開啟所產生檔案清單。
3. 選取您要傳送給技術支援的檔案旁邊的核取方塊。
4. 點擊“**顯示聲明條款**”按鈕。
“**資料提供聲明**”視窗將開啟。
5. 閱讀資料提供聲明的內容，然後點擊“**關閉**”按鈕。
6. 在“**上次應用程式啟動失敗**”視窗中，選取“**我同意資料提供聲明**”核取方塊。

7. 點擊“**傳送**”按鈕。

這會開啟“**請求編號**”視窗。

8. 在“**請求編號**”視窗中，指定在透過卡巴斯基公司帳戶聯絡技術支援時獲得的編號。

9. 點擊“**確定**”。

選定資料檔案將被封包並傳送至技術支援伺服器。

啟用和停用防護傾印檔案和偵錯檔案

轉儲檔案和偵錯檔案包含有關作業系統的資訊以及[使用者保密資料](#)。為了防止未經授權地存取此類資料，您可以啟用防護轉儲檔案和偵錯檔案。

如果啟用了傾印檔案和偵錯檔案防護，則以下使用者可以存取這些檔案：

- 系統管理員和本機管理員以及啟用寫入轉儲檔案和偵錯檔案的使用者可以存取轉儲檔案。
- 只有系統管理員和本機管理員可以存取偵錯檔案。

若要啟用和停用防護轉儲檔案和偵錯檔案：

1. 開啟[程式設定視窗](#)。

2. 選取左側的“**進階設定**”區域。

應用程式設定將顯示在視窗右側。

3. 在“**執行模式**”區域中點擊“**設定**”按鈕。

“**執行模式**”視窗將開啟。

4. 請執行以下操作之一：

- 如果您希望啟用防護，則選取“**啟用傾印和跟蹤檔案保護**”核取方塊。
- 如果您希望停用防護，則清空“**啟用傾印和跟蹤檔案保護**”核取方塊。

5. 在“**執行模式**”視窗中點擊“**確定**”。

6. 若要儲存變更，則在主程式視窗中點擊“**儲存**”按鈕。

防護有效期間寫入的轉儲檔案和偵錯檔案即使該功能被停用也會保持為防護狀態。

詞彙表

OLE 物件

附加的檔案或嵌入到其他檔案中的檔案。Kaspersky 應用程式允許掃描 OLE 物件以尋找病毒。例如，如果您在 Microsoft Office Word 手冊中插入一個 Microsoft Office Excel® 表格，此表格將作為 OLE 物件被掃描。

位址黑名單

一個電子郵件信箱清單，從這些位址發來的所有郵件無論其訊息內容如何，均被 Kaspersky Lab 程式封鎖。

備份

嘗試解毒或刪除前建立的儲存備份檔案的特殊儲存空間。

備用授權

程式已驗證可使用，但是目前還未使用的授權。

受信任平台模組

一個與安全相關的提供基本功能的微晶片（例如用於儲存加密金鑰）。受信任平台模組通常安裝在電腦主機板上並且透過硬體匯流排與其他所有系統元件進行互動。

受感染的檔案

包含惡意程式碼（在掃描檔案時偵測到已知惡意軟體的代碼）的檔案。Kaspersky 建議您不要使用此類別檔案，原因是它們可能會感染您的電腦。

可感染檔案

根據檔案的結構或格式，某些檔案可能會作為儲存和傳播惡意程式碼的"內容"而成為入侵者的工具。一般來說，此類檔案是可執行檔案，例如副檔名為 .com、.exe 和 .dll 的檔案。這類檔案中，惡意程式碼入侵的風險相當高。

可疑網頁位址資料庫

其網頁內容被認為可能具有危險的網頁位址清單。該清單由 Kaspersky 專家建立。它會定期更新，並且會包含在 Kaspersky 應用程式分發套件中。

存檔

封裝到單一壓縮檔案的一個或幾個檔案。需要一個名叫 archiver 的應用程式以開啟和解包資料。

將檔案移至隔離區

一種處理疑似感染檔案的方法，此方法封鎖存取檔案，並且將檔案從其原始位置移動到隔離區資料夾，在此以加密形式存放此檔案以排除感染威脅。

工作

Kaspersky 應用程式作為工作要執行的功能，例如：即時檔案防護、完整裝置掃描、資料庫更新。

工作設定

特定於每個類型工作的程式設定。

憑證

包含私密金鑰和金鑰所有者資訊以及金鑰範圍，以及確認公共金鑰屬於此所有者的電子文件。憑證必須由發佈它的認證中心簽章。

憑證指紋

用於識別憑證金鑰的資訊。透過對金鑰值應用密碼雜湊功能即可建立指紋。

憑證物件

連結至憑證的私密金鑰的容器。這可以是使用者、應用程式、任何虛擬物件、電腦或服務。

憑證發佈者

發佈憑證的認證中心。

應用程式設定

所有類型的工作共有並且控制應用程式整體操作的應用程式設定，如應用程式效能設定、報告設定和備份設定。

掃描範圍

Kaspersky Endpoint Security 在執行掃描工作時掃描的物件。

授權憑證

與金鑰檔案或啟動碼一起由 Kaspersky 傳輸給使用者的文件。此文件包含授予使用者的產品授權資訊。

攜帶式檔案管理器。

這是一種應用程式,可讓您在電腦上沒有加密功能的情況下透過其提供的介面使用卸除式磁碟機上的加密檔案。

攻擊

使用系統或軟體中某種弱點的程式程式碼。攻擊經常被用來在使用者不知情的情況下在電腦上安裝惡意軟體。

啟動授權

程式目前正在使用的授權。

啟發式分析

開發此技術的目的是偵測使用 Kaspersky Lab 程式資料庫無法偵測到的威脅。它可以偵測受未知病毒或已知病毒新變種感染的可疑檔案。

更新

替換/新增從 Kaspersky Lab 更新伺服器上擷取的新檔案 (資料庫或應用程式模組) 的程式。

檔案遮罩

使用萬用字元表示檔案名稱和副檔名。

檔案遮罩可包含檔案名稱中允許使用的任何字元，包括萬用字元：

- * – 代替零個或多個字元。
- ? – 代替任一個字元。

請注意，檔案名稱和副檔名始終透過英文句號分開。

特徵碼分析

一種威脅偵測技術，這種偵測技術將使用包含病毒敘述和解毒方法的 **Kaspersky Endpoint Security** 資料庫。使用特徵碼分析的防護可為您提供可接受的最低等級的安全。根據 **Kaspersky Lab** 專家的建議，此防護方式永遠處於啟用狀態。

疑似受感染的檔案

包含經修改的已知病毒代碼或 **Kaspersky Lab** 尚不清楚的疑似病毒代碼的物件。啟發式分析可偵測到疑似感染的檔案。

病毒資料庫

資料庫包含在 **Kaspersky** 發佈病毒資料庫時已知的電腦安全威脅的資訊。病毒資料庫簽章有助於偵測掃描物件中的惡意代碼。病毒資料庫由 **Kaspersky** 建立並且每小時都會更新。

程式模組

包括在程式安裝檔案中的檔案，這些檔案實現程式的核心功能。程式執行的各種工作類型（即時防護、自訂掃描、更新）都對應於獨立的可執行模組。從應用程式主視窗中啟動電腦完整掃描時，您便啟動此工作的模組。

管理伺服器

卡斯基安全管理中心的一個元件，可集中儲存公司網路內安裝的所有 **Kaspersky Lab** 程式的資訊。它也可用於管理這些應用程式。

管理群組

一組共用一般功能的裝置和一組在這些裝置上安裝的 **Kaspersky** 應用程式。將裝置歸類在群組是為了讓您輕易的把電腦群當作一台電腦進行管理。一個群組可能包含其他的群組。您可以為群組中每個安裝的應用程式建立群組政策和群組工作。

網路代理

一個卡斯基安全管理中心模組，它實現了管理伺服器和特定網路節點（工作站或伺服器）上安裝的 **Kaspersky Lab** 應用程式之間的互動。此元件對在 Windows 下執行的所有 **Kaspersky** 應用程式通用。網路代理的獨立版本是為在其他作業系統下執行的應用程式而設計。

網路代理連線程式。

連線應用程式和網路代理的應用程式功能。使用網路代理，您可以透過卡巴斯基安全管理中心來遠端管理應用程式。

網路服務

定義網路活動的參數集合。針對此網路活動，您可以建立管理防火牆執行的網路規則。

網路釣魚

網路詐騙的一種，傳送電子郵件竊取機密資訊，最常見的財務資料。

網頁資源位址的正規表示式

網頁資源的正規表示式位址是透過正規化獲得的網頁資源位址的文字表達。正規化是一個網頁資源位址文字表達根據特定規則而改變的過程，例如從網頁資源位址的文字表示中排除 HTTP 登入、密碼和連線通訊埠；此外網頁資源位址的字元將從大寫變更為小寫。

在病毒防護中，正規化網頁資源位址的目的是為了防止再次掃描實際上等效但是語法不同的網站位址。

範例：

非正規表示式的位址: `www.Example.com\`。

正規表示式的位址: `www.example.com`。

補丁

在程式運行或安裝更新期間可以修復小缺陷的附加檔案。

解毒

能夠完全或部分還原物件資料的一種處理已感染物件的處理方式。並非所有受感染的物件都能被解毒。

誤報

當 Kaspersky 應用程式由於未受感染檔案的簽章與病毒的簽章類似而將其報告為受感染的檔案時，稱為誤報。

身分驗證代理

驗證加密存取的程序，透過驗證以取得存取加密硬碟，即在作業系統啟動後，執行系統硬碟的加密。

釣魚網頁位址資料庫

Kaspersky 專家確定與釣魚相關的網址清單。此資料庫會定期更新，並且會包含在 Kaspersky 應用程式分發套件中。

防護範圍

在執行時被病毒防護持續掃描的物件。不同元件的防護範圍有不同的參數。

隔離

Kaspersky Endpoint Security 會將疑似感染的物件存放在此資料夾中。被隔離的檔案以加密格式儲存。

有關協力廠商代碼的資訊

有關協力廠商的代碼被包含在一個檔案名為 `legal_notices.txt` 的檔案，並儲存在應用程式的安裝資料夾中。

商標聲明

註冊商標和服務標誌均屬於各自所有者。

Adobe、Acrobat 和 Shockwave 是 Adobe Systems Incorporated 在美國和其他國家/地區的商標或註冊商標。

Mac 和 FireWire 是 Apple Inc. 在美國和其他區域註冊的商標。

AutoCAD 在 Autodesk, Inc. 和/或其子公司/附屬公司在美國和/或其他國家/地區的商標或註冊商標。

wordmark Bluetooth 及其商標是 Bluetooth SIG, Inc. 的財產。

Borland 是 Borland Software Corporation 在美國和其他國家/地區的商標或註冊商標。

Citrix 和 Citrix Provisioning Services 是 Citrix Systems, Inc. 和/或其附屬公司在美國和其他國家和地區專利局的註冊商標。

dBase 是 dataBased Intelligence, Inc. 的商標。

EMC 和 SecurID 是 EMC Corporation 的商標或在美國或其他國家/地區註冊的 EMC Corporation 的商標。

ICQ 是 ICQ LLC 的商標和/或服務標記。

Intel 和 Pentium 是 Intel Corporation 在美國和其他國家/地區註冊的商標。

Logitech 是 Logitech Company 在美國和其他國家/地區的註冊商標或商標。

Mail.ru 是 Mail.Ru LLC. 的註冊商標。

Microsoft、Windows、Internet Explorer、Access、Excel、PowerPoint、Outlook、Outlook Express、Windows Server、Visual Basic、Visual FoxPro、BitLocker, LifeCam Cinema, PowerShell 和 Surface 是 Microsoft Corporation 在美國和其他國家/地區註冊的商標。

Mozilla 和 Thunderbird 是 Mozilla Foundation 的商標。

Novell 是 Novell, Inc 在美國和其他國家/地區的註冊商標。

Java 和 JavaScript 是 Oracle Corporation 和/或其分公司的註冊商標。

SafeNet 是 SafeNet, Inc. 的註冊商標。

UNIX 是在美國和其他國家註冊的商標，經 X/Open Company Limited 授權使用。