kaspersky

# Kaspersky Endpoint Security for Windows 11.0.0

# 目錄

- 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
- 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
- 釣魚網頁位址資料庫
- 防護範圍
- 驗證代理

有關協力廠商代碼的資訊

商標通知

# 關於 Kaspersky Endpoint Security for Windows

該部分介紹 Kaspersky Endpoint Security 11 for Windows（以下簡稱 Kaspersky Endpoint Security）的功能、元件和分發套件，並提供 Kaspersky Endpoint Security 的硬體和軟體要求清單。

## 新聞

Kaspersky Endpoint Security for Windows 提供了以下功能和提升：

1. 整合端點感應器，它是 Kaspersky Anti Targeted Attack Platform 的元件：
   - IoC（入侵指標）掃描器
   - 意外事件回應工具
   - 意外事件調查功能
2. 行為偵測、修復引擎和弱點利用防禦元件支援伺服器作業系統。
3. 行為偵測元件支援共用資料夾對遠端加密的防護。
4. 使用者介面改進：
   - 防護元件按以下區域分組：
     - 進階威脅防護。
     - 關鍵威脅防護。
   - 元件命名與目前資訊安全狀況相符：
     - “檔案防護”元件已重新命名為“檔案威脅防護”。
     - “郵件防護”元件已重新命名為“郵件威脅防護”。
     - “Web 防護”元件已重新命名為“Web 威脅防護”。
     - “網路攻擊防護”元件已重新命名為“網路威脅防護”。
     - “系統監控”元件已分成以下元件：行為偵測、修復引擎、弱點利用防禦。
     - “應用程式權限控制”元件已重命名為“主機入侵防禦”。
     - “應用程式啟動控制”元件已重命名為“應用程式控制”。
5. 威脅防護雲端模式：使用卡巴斯基安全網路時，簡潔的病毒資料庫只需要較少的 RAM 和硬碟空間。
6. 裝置控制：
   - 新增橋接防護功能（封鎖網路間的未授權交換）
   - 新增匯入/匯出信任裝置清單的功能（XML 格式，便於人工閱讀和修改）

7. 應用程式控制：
    - 為單個規則啟用測試模式
    - "黃金映像"類別中包含新的 KL 類別：受信任憑證。
8. 您可以使用 Kaspersky Endpoint Security 的簡化介面：可以在工作列中彈出應用程式圖示的上下文功能表。但應用程式主視窗無法從這裡開啟。
9. 所偵測檔案的校驗和（哈希）將傳送到卡巴斯基安全管理中心管理伺服器並在報告中指示，可用於配置排除項目（受信任區域）。
10. 受信任區域設定中支援遮罩（*、?、**）。
11. 卡巴斯基安全管理中心政策的防護等級指示器，一旦至關重要的防護元件被停用就會發出通知。
12. 多種實用性改進：
    - 簡化了初始化設定精靈
    - 最佳化了產品授權管理

在 Kaspersky Endpoint Security 11 for Windows 中，不再支援以下功能：隔離、IM 防護、弱點掃描。

## 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，可用於檢視最終使用者產品授權協議和隱私政策。
- 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。
- **裝置控制**。此元件可讓您對資料儲存裝置（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。
- **Web 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：

- “應用程式控制”使用應用程式控制規則。
- “主機入侵防禦”使用應用程式權限控制規則。
- 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：

- **行為偵測**。此元件收集您電腦上的應用程式操作的資訊，並將此資訊提供給其他元件以實現更有效的防護。
- **弱點利用防禦**。該元件跟蹤由易於感染的應用程式執行的可執行檔。當存在從易於感染的應用程式執行可執行檔的嘗試，並且該嘗試並非由使用者發起時，Kaspersky Endpoint Security 將封鎖該檔案執行。
- **主機入侵防禦**。此元件可記錄應用程式在作業系統中的行為，並根據受信任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。
- **修復引擎**。該元件允許 Kaspersky Endpoint Security 復原惡意軟體在作業系統中執行的操作。
- **檔案威脅防護**。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。此元件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。
- **Web 威脅防護**。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。
- **郵件威脅防護**。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。
- **網路威脅防護**。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 。

- **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。此元件根據兩類規則篩選網路活動：應用程式網路規則和網路封包規則。

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

- **網路監控**。此元件可讓您即時瀏覽電腦網路活動。

Kaspersky Endpoint Security 提供以下工作：

- **完整性檢查**。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磁碟機和卸除式磁碟。

- **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。

- **回溯**。Kaspersky Endpoint Security 將回溯最新更新的資料庫和模組。

- **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。

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

## 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，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已感染的檔案，它會封鎖那些檔案。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 將由於某種原因未被處理的檔案移動至*活動威脅清單*。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 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);

Microsoft Small Business Server 2011 Standard（64 位元）僅在安裝了 Service Pack 1 for Microsoft Windows Server 2008 R2 時才受支援

- 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。

受支援的虛擬平台：

- VMware Workstation 12。
- VMware ESXi 6.5。
- Microsoft Hyper-V 2016 Server。
- Citrix XenServer 7.2
- Citrix XenDesktop 7.14。
- Citrix Provisioning Services 7.14。

## 特別考慮

您可以在技術支援知識庫的文章 14210 中檢視 Kaspersky Endpoint Security 目前版本中的已知限制和錯誤清單：https://support.kaspersky.com/.

# 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 for Windows。

可以按照以下模式本機安裝 Kaspersky Endpoint Security 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件（有關詳細資訊，請參閱《卡巴斯基安全管理中心說明手冊》）
- 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. 執行分發套件中包括的 setup_kes.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 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 Lab 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 11 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 Endpoint Security 10 Service Pack 1 for Windows (build 10.2.2.10535)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Windows (build 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（版本 10.2.5.3201）
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 4 for Windows（版本 10.2.6.3733）
- Kaspersky Endpoint Security 10 Service Pack 2 for Windows (版本 10.3.0.6294)

## 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》和《隱私政策》

在"安裝精靈"的這一步中，您必須閱讀您與 Kaspersky 之間將簽訂的《使用者產品授權協議》和《隱私政策》。

請仔細閱讀《使用者產品授權協議》和《隱私政策》。如果您同意《使用者產品授權協議》和《隱私政策》的所有條款，則在"**我確認我已完整閱讀、理解並接受**"區域，選擇以下核取方塊：

- **本 EULA 的條款及條件**
- **描述資料處理的《隱私政策》**

在選擇上述兩個核取方塊後，將會在您的裝置上繼續安裝應用程式。

如果您不接受《使用者產品授權協議》和《隱私政策》，可點擊**"取消"**按鈕取消安裝。

## 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**。如果您選擇這一類型的安裝，除"BadUSB攻擊防護"元件之外的所有防護元件都將以 Kaspersky 專家的推薦設定安裝在電腦上。
- **標準安裝**。如果您選擇這一類型的安裝，除"BadUSB攻擊防護"元件之外的所有防護和控制元件都將以 Kaspersky 專家的推薦設定安裝在電腦上。
- **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。"檔案威脅防護"元件是必須安裝的必備元件。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。
- 檔案加密。
- 完整磁碟加密。
- BitLocker 管理。
- 端點感應器。

*BitLocker 管理* 執行以下功能：

- Manages BitLocker 加密構建在 Windows 作業系統中。
- 在卡巴斯基安全管理中心政策設定中配置加密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。

*端點感應器*是 Kaspersky Anti Targeted Attack Platform 的元件。此解決方案用於快速偵測目的攻擊之類的威脅。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磁碟機上可用空間的資訊，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。

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. 新增掃描排除項目

如果您選擇*"自訂安裝"*將可使用此設定

在這一步，您可以指定新增病毒掃描中的排除項目。

**"將 Microsoft 所建議的信任物件排除在掃描範圍外/將 Kaspersky 所建議的信任物件排除在掃描範圍外"**核取方塊，將在/從受信任區域中包括/排除 Microsoft 或 Kaspersky 所建議的區域。

如果選中這些核取方塊中的一個，Kaspersky Endpoint Security 會將 Microsoft 或 Kaspersky 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。

當 Kaspersky Endpoint Security 安裝在執行 Microsoft Windows 以作檔案伺服器之用的電腦上時，**"將 Microsoft 所建議的信任物件排除在掃描範圍外"**方塊將可用。

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 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。

**"將 avp.com 檔案路徑新增至系統變數 %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的路徑。輸入可執行檔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. 應用程式安裝

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下從命令列安裝 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=<用戶名> /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=<用戶名> KLPASSWD=<密碼> KLPASSWDAREA=<密碼範圍>] [ENABLETRACES=1|0 TRACESLEVEL=<偵錯等級>] /qn
```

| | |
|---|---|
| `EULA` | 接受或拒絕最終使用者產品授權協議的條款。可用值：<br>• `1` – 接受最終使用者產品授權協議的條款。<br>• `0` – 拒絕最終使用者產品授權協議的條款。<br>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：<br>• `1` – 接受隱私政策。<br>• `0` – 拒絕隱私政策。<br>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：<br>• `1` – 同意加入 KSN。<br>• `0` – 拒絕加入 KSN（預設值）。<br>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。 |
| `ALLOWREBOOT=1` | 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。<br>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。 |
| `ADDLOCAL` | 選取要安裝的應用程式附加元件。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“端點感應器”。可用值：<br>• `MSBitLockerFeature`。安裝“BitLocker 管理”元件。<br>• `AntiAPTFeature`。端點感應器元件已安裝。 |
| `SKIPPRODUCTCHECK=1` | 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。 |
| SKIPPRODUCTUNINSTALL=1 | 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。 |
| 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。預設使用使用者名稱 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）。<br>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：<br>• SET – 修改應用程式設定。<br>• EXIT – 結束應用程式。<br>• DISPROTECT – 停用防護元件並停止掃描工作。<br>• DISPOLICY – 停用卡巴斯基安全管理中心政策。<br>• UNINST – 從電腦中移除應用程式。<br>• DISCTRL – 停用控制元件。<br>• REMOVELIC – 刪除金鑰。<br>• 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：<br>• 1 – 啟用應用程式偵錯。<br>• 0 – 停用應用程式偵錯（預設值）。 |
| TRACESLEVEL | 偵錯詳細等級。可用值：<br>• 100（關鍵）。僅包含有關致命錯誤的訊息。<br>• 200（高）。有關所有錯誤的訊息，包括致命錯誤。<br>• 300（診斷）。有關所有錯誤的訊息，以及選定的包含警告的訊息。<br>• 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。<br>• 500（一般）。關於一般和致命錯誤的所有警告和訊息，以及包含有關一般操作的詳細資訊的訊息（預設值）。<br>• 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。試用版授權僅提供短時間的測試使用。當試用版授權到期，所有卡巴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 – 應用程式安裝的一般設定
- install.cfg – Kaspersky Endpoint Security 的執行設定
- 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]` – 應用程式安裝的一般設定。
- `[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。“檔案威脅防護”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 | 敘述 |
|---|---|---|
| `[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：<br>• `1` – 接受最終使用者產品授權協議的條款。<br>• `0` – 拒絕最終使用者產品授權協議的條款。<br>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：<br>• `1` – 接受隱私政策。<br>• `0` – 拒絕隱私政策。<br>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：<br>• `1` – 同意加入 KSN。<br>• `0` – 拒絕加入 KSN（預設值）。<br>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。預設使用使用者名稱 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"參數一起指定）。<br>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 KLAdmin 使用者名稱。 |
| | PasswordArea | 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：<br>• SET – 修改應用程式設定。<br>• EXIT – 結束應用程式。<br>• DISPROTECT – 停用防護元件並停止掃描工作。<br>• DISPOLICY – 停用卡巴斯基安全管理中心政策。<br>• UNINST – 從電腦中移除應用程式。<br>• DISCTRL – 停用控制元件。<br>• REMOVELIC – 刪除金鑰。<br>• REPORTS – 檢視報告。 |
| | SelfProtection | 啟用或停用應用程式安裝防護機制。可用值：<br>• 1 – 啟用程式安裝防護機制。<br>• 0 – 停用程式安裝防護機制。<br>您可以停用安裝防護。安裝防護包括防止分發套件被更換為惡意程式、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部分的存取。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。 |
| | Reboot=1 | 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。<br>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。 |
| | AddEnvironment | 在 %PATH% 系統變數中，新增位於 Kaspersky Endpoint Security 安裝資料夾的可執行檔的路徑。可用值：<br>• 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。 |
| | AMPPL | 啟用或停用 Kaspersky Endpoint Security 服務使用 AM-PPL 技術（惡意軟體防護受防護輕型處理程序）提供的防護。可用值：<br>• 1 – 啟用 Kaspersky Endpoint Security 服務使用 AM-PPL 技術提供的防護。<br>• 0 – 停用 Kaspersky Endpoint Security 服務使用 AM-PPL 技術提供的防護。 |
| | SetupReg | 啟用將 setup.reg 檔案中的登錄機碼寫入登錄檔。SetupReg：setup.reg 參數值。 |
| | EnableTraces | 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：<br>• 1 – 啟用應用程式安裝偵錯。<br>• 0 – 停用應用程式安裝偵錯（預設值）。 |
| | TracesLevel | 偵錯詳細等級。可用值：<br>• 100（關鍵）。僅包含有關致命錯誤的訊息。<br>• 200（高）。有關所有錯誤的訊息，包括致命錯誤。<br>• 300（診斷）。有關所有錯誤的訊息，以及選定的包含警告的訊息。<br>• 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。<br>• 500（一般）。關於一般和致命錯誤的所有警告和訊息，以及包含有關一般操作的詳細資訊的訊息（預設值）。<br>• 600（低）。所有可能的訊息。 |
| [Components] | ALL | 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。 |
| | MailThreatProtection | 郵件威脅防護。 |
| | WebThreatProtection | Web 威脅防護。 |
| | | |
| | HostIntrusionPrevention | 主機入侵防禦。 |
| | BehaviorDetection | 行為偵測。 |
| | ExploitPrevention | 弱點利用防禦。 |
| | RemediationEngine | 修復引擎。 |
| | 防火牆 | 防火牆 |

| | | |
|---|---|---|
| | NetworkThreatProtection | 網路威脅防護。 |
| | WebControl | Web 控制。 |
| | DeviceControl | 裝置控制。 |
| | ApplicationControl | 應用程式控制。 |
| | FileEncryption | "檔案級加密"庫。 |
| | DiskEncryption | "完整磁碟加密"庫。 |
| | BadUSBAttackPrevention | BadUSB 攻擊防護。 |
| | AntiAPT | 端點感應器。 |
| | 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：<br>• 1 – 安裝網路代理連線器。<br>• 0 – 不安裝網路代理連線器。 |
| [Tasks] | ScanMyComputer | 完整掃描工作。可用值：<br>• 1 – 該工作將包含在 Kaspersky Endpoint Security 工作清單中。<br>• 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：<br>• 1 – 該工作將包含在 Kaspersky Endpoint Security 工作清單中。<br>• 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：<br>• 1 – 該工作將包含在 Kaspersky Endpoint Security 工作清單中。<br>• 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。

## 步驟 1. 應用程式啟動

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，卡巴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**"。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"檔案威脅防護"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。

## 步驟 2. 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 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。

## 步驟 3. 使用金鑰檔案啟動

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。

## 步驟 4. 選擇要啟動的功能

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和"主機入侵防禦"元件可用。
- **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。

## 步驟 5. 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。

## 步驟 6. 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。

如果要結束初始化配置精靈且不啟動 Kaspersky Endpoint Security，請清除**"啟動 Kaspersky Endpoint Security for Windows"**核取方塊，然後點擊**"完成"**。

## 步驟 7. 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。

## 步驟 8. 卡巴斯基安全網路聲明

在這一步，我們邀請您透過執行以下操作來接受加入卡巴斯基安全網路：

1. 閱讀卡巴斯基安全網路聲明。
2. 從以下選項中選取一個選項：
   - 如果您接受所有條款，請選擇**"我同意使用卡巴斯基安全網路"**選項。
   - 如果您不接受加入卡巴斯基安全網路的條款，請選擇**"我不同意使用卡巴斯基安全網路"**選項。

     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。
3. 要確認選擇，請點擊**"確定"**。

# 更新到新版本的應用程式

將以前版本的應用程式更新為較新版本時，請考慮以下事項：

- 將以前版本更新到 Kaspersky Endpoint Security for Windows 11.0.0 時，不需要移除以前版本的應用程式。
- 建議在開始更新之前結束所有活動的應用程式。
- 要將 Kaspersky Endpoint Security 從版本 10 更新到版本 11，需要解密所有已加密的硬碟磁碟機。

  在更新之前，Kaspersky Endpoint Security 會封鎖完整磁碟加密功能。如果無法封鎖完整磁碟加密，更新安裝將不會啟動。更新應用程式後，將還原完整磁碟加密功能。

您可以將以下應用程式更新到 Kaspersky Endpoint Security 11.0.0 for Windows：

- Kaspersky Endpoint Security 10 Service Pack 1 for Windows (build 10.2.2.10535)
- 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（版本 10.2.5.3201）
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 4 for Windows（版本 10.2.6.3733）
- Kaspersky Endpoint Security 10 Service Pack 2 for Windows (版本 10.3.0.6294)
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 1 for Windows（版本 10.3.0.6294）
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 2 for Windows（版本 10.3.0.6294）
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 for Windows（版本 10.3.3.275）。

.

將 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 更新到 Kaspersky Endpoint Security 11.0.0 for Windows 時，舊版本應用程式的備份區或隔離區中的檔案將傳送到新版本應用程式的備份區中。對於 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 之前的版本，放入先前版本中的備份區或隔離區的檔案不會移轉到新版本。

可以透過以下方式在電腦上更新 Kaspersky Endpoint Security：

- 本機使用安裝精靈。
- 本機使用命令列。
- 遠端使用卡巴斯基安全管理中心軟體套件（有關詳細資訊，請參閱*卡巴斯基安全管理中心說明*）。
- 遠端透過 Microsoft Windows 群組政策管理編輯器（有關詳細資訊，請參閱 *Microsoft 技術支援網站*）。
- 遠端使用系統中心配置管理器。

# 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
- 使用卡巴斯基安全管理中心軟體套件遠端執行（有關詳細資訊，請參閱《卡巴斯基安全管理中心說明手冊》）
- 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. 透過以下方式之一開啟"**控制台**"視窗：
   - 如果您正在使用 Windows 7，請在"**開始**"功能表中選取"**控制台**"。
   - 如果您正在使用 Windows 8 或 Windows 8.1，請按 **Win+I** 組合鍵並選擇"**控制台**"。
   - 如果您正在使用 Windows 10，請按 **Win+X** 組合鍵並選擇"**控制台**"。
2. 在"**控制台**"視窗中，選取"**應用程式和功能**"。
3. 在已安裝的應用程式清單中，選擇"**Kaspersky Endpoint Security for Windows**"。
4. 點擊"**修改/移除**"按鈕。
   應用程式安裝精靈的"**自訂安裝**"視窗將開啟。
5. 在安裝精靈的"**修改、修復或刪除**"視窗中，點擊"**刪除**"按鈕。
6. 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。
- **備份檔案** – 程式掃描且置於"備份區"中的物件。

  在移除應用程式之後儲存的備份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物件，必須在移除應用程式之前將這些檔案從儲存中還原。但是，Kaspersky 專家不建議從備份區中還原物件，因為這可能會損害電腦。
- **程式的操作設定** – 應用程式配置過程中選取的程式設定值。
- **本機儲存的加密金鑰** – 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. 應用程式移除完成移除

在此步驟中，"安裝精靈"將從電腦中移除程式。請等待，直到程式移除操作完成。

當移除程式時，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，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

您可以在包含分發套件的資料夾中透過命令列執行指令來啟動應用程式移除過程。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_kes.exe /x` 或 `msiexec.exe /x {E7012AFE-DB97-4B8B-9513-E98C0C3AACE3}`。

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_kes.exe /s /x` 或 `msiexec.exe /x {E7012AFE-DB97-4B8B-9513-E98C0C3AACE3} /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：*

在命令列中鍵入 `setup_kes.exe /pKLLOGIN=<使用者名稱> /pKLPASSWD=***** /x` 或

`msiexec.exe KLLOGIN=<使用者名稱> KLPASSWD=***** /x {E7012AFE-DB97-4B8B-9513-E98C0C3AACE3}`。

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_kes.exe /pKLLOGIN=<使用者名稱> /pKLPASSWD=***** /s /x` 或

`msiexec.exe /x {E7012AFE-DB97-4B8B-9513-E98C0C3AACE3} KLLOGIN=<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巴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：

- 使用卡巴斯基安全管理中心政策。
- 使用還原工具。

*若要使用卡巴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巴斯基安全管理中心政策套用至電腦。
2. 啟動 Kaspersky Endpoint Security。

*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"檔案威脅防護"元件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 for Windows**.開啟應用程式主視窗。在此視窗中，您可以調節應用程式元件和工作的執行，並檢視已處理的檔案和偵測到的威脅的統計資料。
- **設定**。開啟"**設定**"視窗。"**設定**"標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。

  無論防護元件和控制元件的執行處於暫停狀態還是復原狀態，Kaspersky Endpoint Security 都將使用卡巴斯基安全網路。

- **停用政策/啟用政策**。停用/啟用卡巴斯基安全管理中心政策。如果某個政策已套用於安裝了 Kaspersky Endpoint Security 的電腦，並且設定了用於停用卡巴斯基安全管理中心政策的密碼，則該上下文功能表項可用。
- **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。


應用程式圖示的右鍵選單

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。

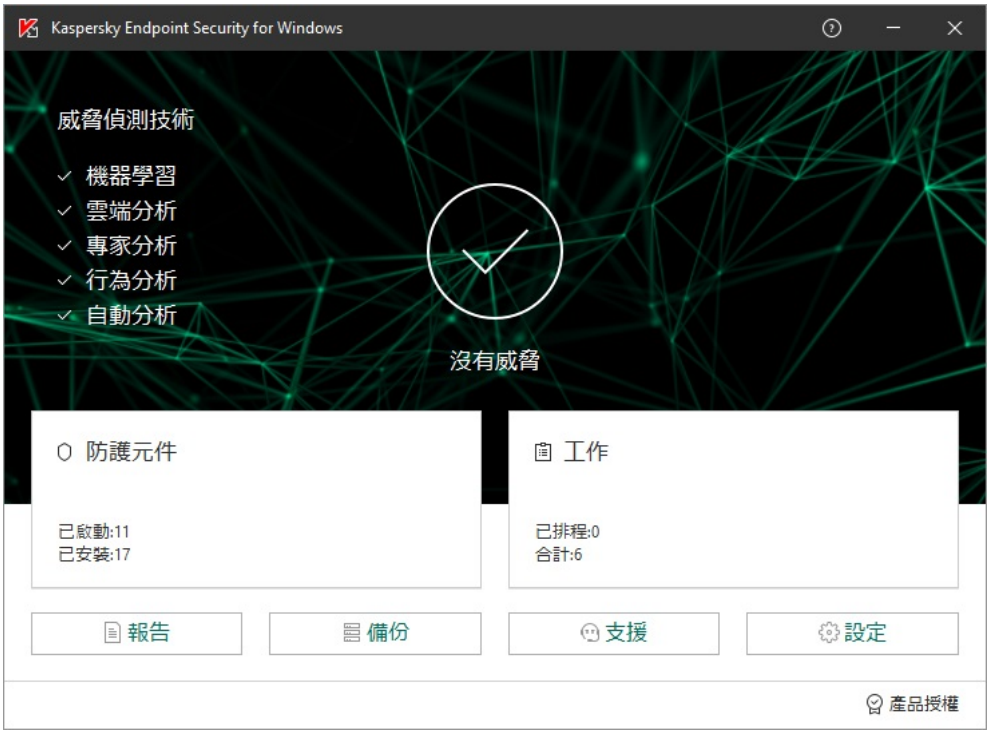
## 應用程式主視窗

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。

應用程式主視窗包含下列項目：

- **Kaspersky Endpoint Security for Windows** 的連結。點擊該連結將開啟"**關於**"視窗，其中包含應用程式版本的資訊。
- 按鈕 ⓘ。點擊此按鈕，將會開啟 Kaspersky Endpoint Security 說明文件。
- "**威脅偵測技術**"區域。該區域包含以下資訊：
  - 該區域的左側部分顯示威脅偵測技術的清單。使用特定技術偵測到的威脅數量顯示在每種威脅偵測技術名稱的右側。
  - 根據活動威脅的出現情況，該區域的中心顯示以下說明之一：
    - **沒有威脅**。如果顯示此說明，點擊"**威脅偵測技術**"區域將開啟"**威脅偵測技術**"視窗，此視窗提供威脅偵測技術的簡要說明以及卡巴斯基安全網路雲端服務基礎結構的狀態和全域統計資訊。
    - **N 個活動威脅**。如果顯示此說明，點擊"**威脅偵測技術**"區域將開啟"**活動威脅**"視窗，該視窗顯示與由於某些原因未被處理的受感染檔案相關的事件清單。
- "**防護元件**"區域。點擊此區域將開啟"**防護元件**"視窗。在此視窗中，您可以檢視已安裝元件的執行狀態。透過此視窗，還可以在包含除加密元件外的所有已安裝元件的設定的"**設定**"視窗中開啟一個子區域。
- "**工作**"區域。點擊此按鈕將開啟"**工作**"視窗。在此視窗中，您可以管理 Kaspersky Endpoint Security 工作的執行，這些工作用於更新應用程式模組和資料庫、掃描檔案中的病毒和其他惡意軟體，以及執行完整性檢查。
- "**報告**"按鈕。點擊該按鈕將開啟"**報告**"視窗，其中包含應用程式整體或單獨元件執行期間或者工作執行期間發生的事件資訊。
- "**儲存**"按鈕。點擊此按鈕將開啟"**備份**"視窗。在此視窗中，您可以檢視應用程式已移除的受感染檔案的副本清單。
- "**支援**"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。
- "**設定**"按鈕。點擊該按鈕將開啟"**設定**"視窗，在其中可以修改應用程式的預設設定。

- 按鈕 / / 。點擊此按鈕將開啟**"事件"**視窗，其中包含有關可用更新以及存取加密檔案和裝置的請求的資訊。
- **"產品授權"**連結。點擊該連結將開啟**"產品授權"**視窗，其中包含目前啟動授權檔案的詳細資訊。




應用程式主視窗

*若要開啟 Kaspersky Endpoint Security 主視窗，請執行以下操作：*

- 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 for Windows**。

## 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授權。

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。

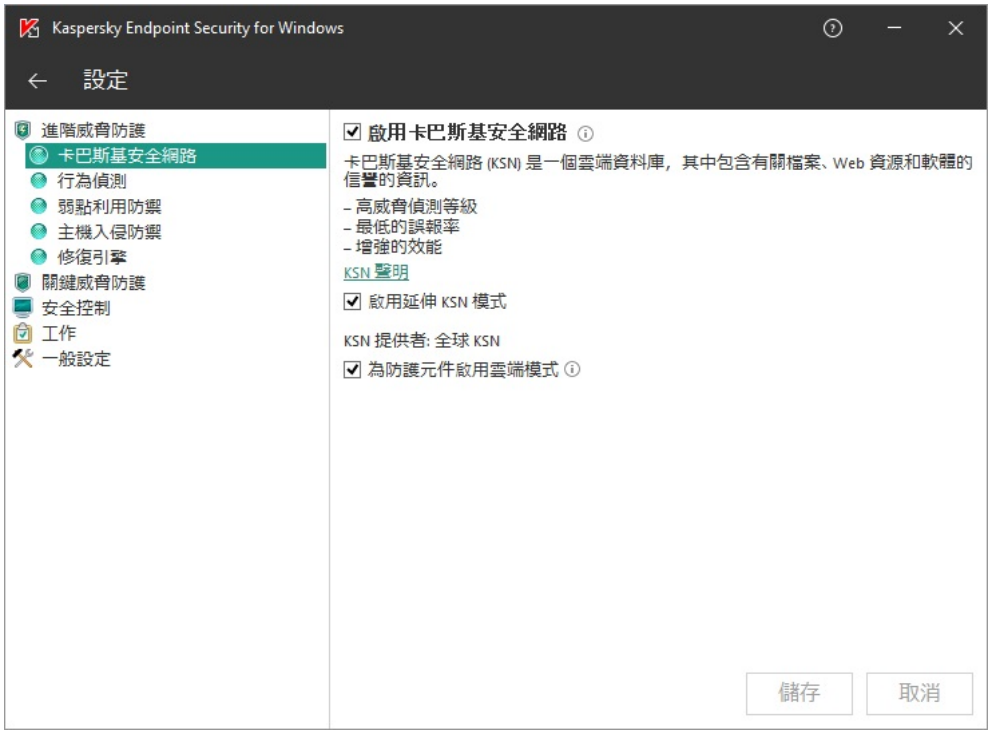
根據啟動伺服器的負載分佈情況，產品授權的狀態從"備用"變為"啟動"，可能會需要一段時間。

## 應用程式設定視窗

Kaspersky Endpoint Security 設定視窗允許您設定整體應用程式設定、單個元件、報告和儲存區、掃描工作和更新工作以及與卡巴斯基安全網路伺服器的通訊。

應用程式設定視窗包含兩個部分（見下圖）：

- 左側包括應用程式元件、工作和包含多個子區域的進階設定區域。
- 右側包含可以用於配置視窗左側選定工作或元件設定的控制元素以及進階設定。




應用程式設定視窗

*若要開啟應用程式設定視窗，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**”。

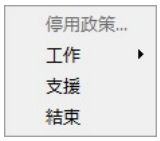
# 簡化的應用程式介面

如果將配置了“顯示簡化應用程式介面”的卡巴斯基安全管理中心政策應用於已安裝 Kaspersky Endpoint Security 的用戶端電腦，則在此用戶端電腦上不能使用應用程式主視窗。右鍵點擊 Kaspersky Endpoint Security 圖示可開啟上下文功能表（如下圖），其中包含以下項目：

- **停用政策**。在已安裝 Kaspersky Endpoint Security 的用戶端電腦上停用卡巴斯基安全管理中心政策。如果某個政策已套用於電腦並且設定了用於停用卡巴斯基安全管理中心政策的密碼，則此上下文功能表項目可用。
- **工作**。包含以下項的下拉清單：
  - **更新**。
  - **回溯**。
  - **完整掃描**。

- **自訂掃描**。
- **關鍵區域掃描**。
- **完整性檢查**。

- **支援**。開啟包含聯絡 Kaspersky 技術"**支援**"所需資訊的視窗。
- **結束**。結束 Kaspersky Endpoint Security。




顯示簡化介面時應用程式圖示的右鍵選單

# 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（如訂購到期日期和受防護裝置數量）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。

有限訂購到期時，您可能得到訂購續費寬限期，在此期間應用程式繼續執行。寬限期的可用性和期限由服務提供者決定。

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。

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 Lab 的啟動伺服器。

當應用程式使用啟動碼啟動時，將安裝啟動授權。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。

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 Lab 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 Lab 可以封鎖此金鑰。如果金鑰被封鎖，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 Lab 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 Lab 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：

- 聯絡產品授權銷售商。
- 基於您現有的啟動碼在 Kaspersky 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

如果啟動碼套用於啟動 Kaspersky Endpoint Security，則您同意為驗證應用程式的正確使用而自動定期傳送以下資訊：

- Kaspersky Endpoint Security 的類型、版本和在地化
- Kaspersky Endpoint Security 已安裝更新的版本
- 電腦 ID 和該電腦上的特定 Kaspersky Endpoint Security 安裝的 ID
- 啟動碼和目前產品授權特定啟動的唯一 ID
- 作業系統的類型、版本和比特率，以及虛擬環境的名稱（如果 Kaspersky Endpoint Security 安裝在虛擬環境中）
- 傳送資訊時活動的 Kaspersky Endpoint Security 元件的 ID

Kaspersky 也可以使用這些資訊來生成關於 Kaspersky 軟體傳播和使用的統計資訊。

使用啟動碼，即表明您同意自動傳送以上列出的資料。如果您不同意傳送這些資訊至 Kaspersky，則應該使用金鑰檔案來啟動 Kaspersky Endpoint Security。

同意最終使用者授權協議的條款，表示您同意自動傳送以下資訊：

- 升級 Kaspersky Endpoint Security 時：
  - Kaspersky Endpoint Security 的版本
  - 啟動產品授權的 ID
  - Kaspersky Endpoint Security 的 ID
  - 啟動產品授權的序列號
  - 升級工作啟動的唯一 ID
  - Kaspersky Endpoint Security 安裝的唯一 ID
- 點擊 Kaspersky Endpoint Security 介面中的連結時：
  - Kaspersky Endpoint Security 的版本
  - 作業系統版本
  - Kaspersky Endpoint Security 啟動日期
  - 產品授權到期日期
  - 金鑰建立日期
  - Kaspersky Endpoint Security 安裝日期

- Kaspersky Endpoint Security 的 ID
- 啟動產品授權的 ID
- 作業系統中偵測到的弱點的 ID
- 為 Kaspersky Endpoint Security 安裝的最新更新的 ID
- 掃描易於感染的應用程式時發現的弱點的 ID
- 偵測到的威脅的哈希值，以及按照 Kaspersky 分類別確定的威脅名稱
- Kaspersky Endpoint Security 啟動錯誤類別
- 錯誤代碼
- Kaspersky Endpoint Security 啟動錯誤代碼
- 金鑰到期前的天數
- 新增金鑰後經過的天數
- 產品授權到期後經過的天數
- 套用活動的產品授權的電腦數量
- 啟動產品授權的序列號
- Kaspersky Endpoint Security 產品授權條款
- 產品授權目前狀態
- 啟動的產品授權的類型
- 應用程式類型
- 升級工作啟動的唯一 ID
- Kaspersky Endpoint Security 安裝的唯一 ID
- 電腦上是唯一軟體安裝 ID
- Kaspersky Endpoint Security 介面語言

- 關於加入卡巴斯基安全網路：
  - 是接受還是拒絕卡巴斯基安全網路聲明
  - 接受或拒絕卡巴斯基安全網路聲明的日期和時間
  - 使用者接受或拒絕的卡巴斯基安全網路聲明的 ID 和版本
  - 有關是選中還是清除“**啟用卡巴斯基安全網路**”核取方塊的資訊
  - 有關是選中還是清除“**啟用延伸 KSN 模式**”核取方塊的資訊

- 個人電腦和使用者的唯一 ID
- 應用程式的完整版和應用程式類型

如果卡巴斯基安全網路被完全停用，這些統計資料將在停用後的 24 小時內每 4 個小時傳送一次。如果您在安裝 Kaspersky Endpoint Security 期間拒絕加入卡巴斯基安全網路，則在電腦上停用卡巴斯基安全網路後的 24 小時內，這些統計資料也將每 4 小時傳送一次。

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

請閱讀最終使用者產品授權協議並存取 Kaspersky 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_<語言 ID>.txt 檔案包含最終使用者授權協議的文字，卡巴斯基安全網路聲明包含在應用程式分發套件中。

## 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。

*購買授權：*

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"**產品授權管理**"區域中執行下列操作之一：
   - 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"**續約產品授權**"按鈕。

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

## 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，在訂購到期之日（或訂購續約寬限期到期之日），Kaspersky Endpoint Security 將通知您，並停止嘗試自動續約訂購。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巴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。如果在寬限期後對訂購進行續約並且訂購狀態未自動更新時，您可能需要執行此操作。

## 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授權和備用授權。
- 透過建立和啟動金鑰新增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金鑰儲存中的金鑰和啟動碼分發到用戶端電腦來遠端進行（詳細資訊請參見《卡巴斯基安全管理中心說明手冊》）。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。

啟動金鑰過程需要一些時間 (在非互動式或遠端安裝)，存取卡巴斯基啟動伺服器。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。

根據電腦效能，啟動作業系統後下載 Kaspersky Endpoint Security 病毒資料庫會花費最多兩分鐘時間。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. 在視窗左側的**"一般設定"**區域中選取**"應用程式設定"**。
3. 請執行以下操作之一：
   - 如果要使應用程式自動執行，請選中**"在電腦啟動時啟動 Kaspersky Endpoint Security for Windows"**核取方塊。
   - 要停用程式自動執行，請清空**"在電腦啟動時執行 Kaspersky Endpoint Security 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 Lab 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**"應用程式"**→**"Kaspersky Endpoint Security 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. 在上下文功能表中，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。

# 參與卡巴斯基安全網路

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 使用從全球使用者處接收的資料。*卡巴斯基安全網路*設計用於收集此類資料。

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。

根據基礎架構的位置，分為全球 KSN 服務（基礎架構由 Kaspersky 伺服器託管）和私有 KSN 服務。

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。否則將無法與私有 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。

使用延伸 KSN 模式時，應用程式會自動將產生的操作統計資訊傳送給 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 進行額外掃描。

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分發套件中。

為了降低 KSN 伺服器的負荷，Kaspersky 可能會發佈應用程式病毒資料庫，臨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說明手冊》。

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。

卡巴斯基安全網路的使用是自願的。應用程式將在初始化設定期間提示您使用 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. 在應用程式主視窗中，點擊**"設定"**按鈕。
2. 在應用程式設定視窗中，選取**"進階威脅防護"**→**"卡巴斯基安全網路"**。
3. 如果您希望 Kaspersky Endpoint Security 使用從卡巴斯基安全網路資料庫收到的檔案信譽、網路資源信譽和應用程式信譽，請選中**"卡巴斯基安全網路"**核取方塊。

   Kaspersky Endpoint Security 將顯示卡巴斯基安全網路聲明。請閱讀卡巴斯基安全網路 (KSN) 聲明的條款，如果您同意這些條款，則請接受。

   預設情況下，Kaspersky Endpoint Security 使用延伸 KSN 模式。*延伸 KSN 模式*是 Kaspersky Endpoint Security 向 Kaspersky 傳送附加資料的一種模式。
4. 如果需要，請清除**"啟用延伸 KSN 模式"**核取方塊。
5. 存儲變更。

## 關於使用卡巴斯基安全網路時的資料提供

同意卡巴斯基安全網路聲明，表示您同意自動傳送以下資訊：

- 如果選中**"啟用卡巴斯基安全網路"**核取方塊並且清除**"啟用延伸 KSN 模式"**核取方塊，則傳送以下資訊：
  - 使用者被引導至所掃描網址前所在頁面的網址
  - 其信譽被請求的網址
  - 用於連線 Kaspersky 服務的協定的版本
  - 病毒資料庫的 ID
  - 偵測到威脅的掃描工作的 ID
  - 發起請求的子系統的 ID
  - 連線協定的 ID 和使用的埠號
  - 已安裝的更新的 ID
  - 偵測到的威脅在 Kaspersky 分類中的名稱和 ID
  - 公共憑證金鑰
  - Kaspersky Endpoint Security 的類型和完整版本
  - 用於對所掃描物件進行簽章的憑證的雜湊值 (SHA256)
  - 所掃描檔案的雜湊 (MD5、SHA2-256 和 SHA1) 和檔案範本 (MD5)
- 如果除**"啟用卡巴斯基安全網路 "**核取方塊外還選中了**"啟用延伸 KSN 模式"**核取方塊，則除上面列出的資訊外，還會傳送以下資訊：
  - 受信任的可執行檔和不可執行檔（或部分檔案），為防止誤報而傳送。

- 應用程式活動報告中包括的以下資訊將被傳送：
  - 應用程式調用的網址和 IP 位址
  - 接收到的已開機檔案所來自的網址和 IP 位址
  - 憑證期限的開始和到期日期和時間，如果傳送的檔案有數位簽章 - 簽章的日期時間，憑證發佈者的名稱，憑證所有者的相關資訊，指紋和公共憑證金鑰及其計算演算法，以及憑證的序號
  - 處理程序視窗的標題
  - 病毒資料庫的 ID，偵測到的威脅在權利持有人分類中的名稱
  - 處理程序存取的檔案的名稱和路徑
  - 處理程序存取的登錄檔項的名稱和值
  - 用於啟動處理程序的帳戶名稱
  - 傳輸的檔案的名稱、大小和版本，檔案的說明和校驗和 (MD5、SHA2-256、SHA1)，格式 ID，開發者名稱，檔案所屬的產品的名稱，檔案在電腦上的完整路徑及路徑範本代碼，以及建立和修改檔案的日期和時間。
  - 有關軟體中安裝的產品授權的資訊、產品授權 ID、其類型及到期日期
  - 啟動處理程序的電腦的名稱的校驗和 (MD5、SHA2-256、SHA1)
  - 傳送資訊時的電腦本機時間
- 此外還將傳送以下資訊：
  - 請求的網路資源的網址和 IP 位址，有關存取該網路資源的檔和 Web 用戶端的資訊，檔案的名稱、大小和校驗和 (MD5、SHA2-256、SHA1)，檔案的完整路徑和路徑範本代碼，檢查其數位簽章的結果，及其在 KSN 中的狀態
  - 如果偵測到潛在的惡意物件，將提供以下有關處理程序記憶體資料的資訊：系統物件層級的元素 (ObjectManager)，UEFI BIOS 記憶體資料，以及登錄檔項的名稱和值。
  - 包含可疑和惡意物件的網頁和電子郵件。
  - 軟體更新元件的版本，在元件執行期間執行更新工作時軟體更新元件當機的次數，更新工作類型的 ID，軟體更新元件的未成功更新工作終止的次數。
  - 有關軟體元件執行中發生的錯誤的資料：軟體狀態的 ID，錯誤代碼和類型以及發生時間，元件的 ID，發生錯誤的產品的模組和處理程序，發生錯誤時的更新工作或類別的 ID，軟體使用的驅動程式的日誌（錯誤代碼、模組名稱、原始檔案的名稱和發生錯誤的字串），用於識別軟體執行中發生的錯誤的方法的 ID，以及發起流量攔截或交換而導致軟體執行出錯的處理程序的名稱。
  - 有關系統傾印 (BSOD) 的資料：電腦上發生 BSOD 的指示器、導致 BSOD 的驅動程式的名稱、驅動程式中的記憶體堆疊和位址、BSOD 之前的作業系統連線持續時間的指示器、驅動程式當機的記憶體堆疊、儲存的記憶體傾印的類型、指示 BSOD 之前作業系統連線持續 10 分鐘以上的指示器、傾印的唯一 ID，以及 BSOD 的日期和時間。
  - 有關軟體的病毒資料庫和元件更新的資料：作為上次更新的結果並在目前更新中載入的索引檔案的名稱、日期和時間，以及上次更新的完成日期和時間，更新的檔案類別的名稱及校驗和 (MD5、SHA2-256、SHA1)。

- 偵測到威脅的掃描工作的 ID。

- 有關檔案簽章使用的身份驗證憑證的資訊：憑證指紋，校驗和信譽演算法，憑證的公開金鑰和序號，憑證發佈者的名稱，憑證檢查結果，以及憑證資料庫的 ID。

- 有關電腦上安裝的作業系統 (OS) 的版本以及安裝的更新套件的資訊，位元數，修訂，作業系統執行模式的設定，以及作業系統內核檔案的版本和校驗和 (MD5、SHA2-256、SHA1)。

- 有關惡意軟體操作回溯的資訊：有關其活動被回溯的檔案的資料（檔案名稱、檔案的完整路徑、檔案的大小和校驗和 (MD5、SHA2-256、SHA1)），有關刪除、重新命名和複製檔案以及還原登錄檔中的值（登錄檔項的指令和值）的成功和失敗操作的資料，有關惡意軟體修改的系統檔案的資訊（回溯前後）。

- 有關可執行檔類比的資訊：檔案的大小和校驗和 (MD5、SHA2-256、SHA1)，類比元件的版本，類比深度，類比期間獲取的邏輯塊的特徵向量及邏輯塊內的功能，以及可執行檔 PE 檔案頭結構中的資料。

- 有關電腦上的軟體的安裝和啟動日期的資訊：安裝的產品授權的類型及有效期，出售產品授權的合作夥伴的 ID，產品授權序號，電腦上軟體安裝的類型（新安裝、升級等），指示成功安裝的指示器或安裝錯誤編號，電腦上的軟體安裝的唯一 ID，執行更新的應用程式的類型和 ID，以及更新工作的 ID。

- 有關載入的軟體模組的資訊：模組檔案的名稱、大小和校驗和 (MD5、SHA2-256、SHA1)，模組檔案的完整路徑和路徑範本代碼，模組檔案的數位簽章設定，簽章建立資料和時間，為模組檔案簽章的主體和組織的名稱，載入模組的處理程序的 ID，模組供應商的名稱，以及載入佇列中模組的序號。

- 有關使用者下載的檔案的資訊：下載的檔案的網址和 IP 位址，下載的網頁，下載協定的 ID 和連線埠號，位址的惡意活動指示器，檔案的內容和大小及其校驗和 (MD5、SHA2-256、SHA1)，下載檔案的處理程序的相關資訊（校驗和 (MD5、SHA2-256、SHA1)，建立和連結的日期和時間，自動執行指示器，內容，封裝程式的名稱，簽章資訊，可執行檔指示器，格式 ID，熵），檔案名稱，電腦上的檔案路徑，檔案的數位簽章及簽章資訊，進行偵測的 URL，頁面上被認為可疑或惡意的指令碼數量，對這些指令碼的已完成 http 請求及回應的相關資訊。

- 有關正在執行的應用程式及其模組的資訊：系統中正在執行的處理程序的資料（處理程序 ID (PID)），處理程序名稱，啟動處理程序的帳戶的詳細資訊，啟動處理程序的應用程式和指令，以及此應用程式或處理程序是否可信的指示器，處理程序檔案的完整路徑和命令列，處理程序完整性級別，處理程序所屬產品的描述（產品名稱和發佈者詳細資訊），以及目前使用的數位憑證的相關資訊，驗證憑證所需的資訊或表示檔案缺少數位簽章的指示器，有關載入到處理程序中的模組資訊（名稱，大小，類型，建立日期，內容，校驗和 (MD5、SHA2-256、SHA1) 以及路徑），PE 檔案頭資訊以及封裝程式的名稱（如果檔案已封裝）。

- 有關所有已安裝的更新集的資訊以及最近安裝的更新和/或遠端更新集的資訊，導致傳送更新資訊的事件的類型，上次更新安裝後經過的時間，傳送資訊時載入的病毒資料庫的相關資訊。

- 有關最作業系統上次重新啟動失敗的資訊：作業系統安裝以來重新啟動失敗的次數，系統傾印資料（錯誤代碼和參數，導致作業系統出錯的模組的名稱、版本和校驗和 (CRC32)，模組內偏移量形式的錯誤位址，以及系統傾印的校驗和 (MD5、SHA2-256、SHA1)）。

- 有關權利持有者的軟體的資訊：所用軟體的完整版本、類型、中文化和執行狀態，已安裝的軟體元件的版本和執行狀態，有關已安裝的軟體更新的資料，TARGET 篩檢程式值，以及用於連線權利持有者服務的協定的版本。

- 有關掃描的物件的資訊：檔案移入或移出的指定信任群組，將檔案移入指定類別的理由，類別 ID，有關類別源的資訊和類別資料庫版本，表示檔案是否有受信任憑證的指示器，檔案開發者名稱，檔案版本，以及檔案所屬的應用程式的名稱和版本。

- 有關掃描的檔案和 URL 的資訊：掃描的檔案的校驗和 (MD5、SHA2-256、SHA1) 和檔案模式 (MD5)，模式大小，偵測到的威脅的類型及其在權利持有者分類中的名稱，病毒資料庫的 ID，其信譽被查詢的 URL，以及使用者被引導至掃描的 URL 時所在頁面的 URL，連線協定的 ID，以及使用的埠號。

- 有關對軟體的自我防護發起攻擊的處理程序的資訊：處理程序檔案的名稱和大小，其校驗和 (MD5、SHA2-256、SHA1)，檔案完整路徑和路徑範本代碼，處理程序檔案建立和連線的日期和時間，可執行檔指示器，處理程序檔案內容，用於對處理程序檔案簽章的憑證的相關資訊，用於啟動處理程序的帳戶的代碼，為存取處理程序所執行的操作的 ID，用於執行操作的資源的類型（處理程序，檔案，登錄檔物件，使用 FindWindow 函數的視窗搜尋），用於執行操作的資源的名稱，操作成功指示器，處理程序檔案的狀態及其在 KSN 中的簽章。

- 有關防護元件執行的資訊：元件的完整版本，導致事件佇列溢出的事件的代碼，此類事件數量，事件佇列溢出總次數，發起該事件的處理程序檔案的相關資訊（檔案名稱，檔案在電腦上的路徑，路徑範本代碼，與檔案關聯的處理程序的校驗和 (MD5、SHA2-256、SHA1)，檔案版本），完整事件捕獲的 ID，捕獲篩檢程式的完整版本，所捕獲事件類型的 Id，事件佇列大小和佇列中第一個事件與目前事件之間的事件數量，佇列中到期事件的數量，發起目前事件的處理程序的資訊（處理程序檔案名稱，檔案在電腦上的路徑，路徑範本代碼，處理程序的校驗和 (MD5、SHA2-256、SHA1)），事件處理時間，事件處理最大容許時間，以及資料傳輸概率值。

- 有關電腦上的軟體執行的資訊：CPU 使用率資料，記憶體使用率資料（專用位元組，未分頁緩衝集區，分頁緩衝集區），軟體處理程序中的活動執行緒數和掛起執行緒數，以及錯誤發生前的軟體執行時間。

- 有關對請求的包含主機的被掃描 URL 和 IP 位址的 Web 資源進行分類的結果的資訊，執行分類的軟體元件的版本，分類方法，以及針對 Web 資源確定的類別集。

- 有關網路攻擊的資訊：發起攻擊的電腦的 IP 位址（Ipv4 和 Ipv6），網路攻擊目標的電腦埠號，攻擊註冊的 IP 封包的協定的 ID，攻擊目標（公司名稱，網站），攻擊回應標記，攻擊的權重等級，以及信任等級值。

- 有關網路連線的資訊：開啟連接埠的處理程序的檔案版本和校驗和 (MD5、SHA2-256、SHA1)，處理程序檔案的路徑和數位簽章，本機和遠端 IP 位址，本機和遠端連線埠號，連線狀態和連接埠開啟時間。

- 有關系統日誌中的事件的資訊：事件時間，偵測到事件的日誌的名稱，事件類型和類別，事件來源的名稱和說明。

- 有關電腦病毒防護狀態的資訊：使用的病毒資料庫的版本及發佈日期和時間，權利持有者服務的更新和連線的統計資料，工作的 ID 以及執行掃描的軟體元件的 ID。

- 有關導致出錯的協力廠商應用程式的資訊：應用程式名稱、版本和中文化，系統應用程式日誌中關於該程式的錯誤代碼和資訊，發生錯誤的位址和協力廠商應用程式的記憶體堆疊，軟體元件中的錯誤指示器，出錯之前協力廠商應用程式的執行時間，出錯的應用程式處理程序映射的校驗和 (MD5、SHA2-256、SHA1)，此應用程式處理程序映射的路徑和路徑範本代碼，作業系統日誌中與該應用程式相關的錯誤說明資訊，發生錯誤的應用程式模組的相關資訊（錯誤 ID，模組中偏移量形式的錯誤位址，模組的名稱和版本，權利持有者外掛程式中的應用程式當機的 ID 及當機的記憶體堆疊，以及出現故障之前應用程式的執行時間）。

- 有關軟體當機的資訊：建立傾印的日期和時間，傾印類型，與傾印關聯的處理程序的名稱，版本和透過傾印傳送統計資訊時的時間，導致軟體當機的事件的類型（意外斷電，協力廠商權利持有者的應用程式當機，攔截處理錯誤），以及異常斷電的日期和時間。

- 有關與欺詐網路資源相關的攻擊的資訊，以及所存取網站的 DNS 和 IP 位址（Ipv4 或 Ipv6）。

- 有關驗證數位憑證真實性所需的所用數位憑證的資訊：用於對掃描物件簽章的憑證的校驗和 (SHA256) 和公共憑證金鑰。

- 有關偵測到的弱點的資訊：弱點資料庫中的弱點 ID，弱點危險等級，以及偵測狀態。

- 有關電腦上安裝的硬體的資訊：固件的類型、名稱、型號和版本，嵌入的裝置與連線的裝置的規格，以及安裝軟體的電腦的唯一 ID。

- 有關電腦上安裝的軟體的資訊：軟體及其開發者的名稱，使用的登錄檔項及其值，已安裝的軟體的檔案資訊（校驗和 (MD5、SHA2-256、SHA1)，名稱，檔案在電腦上的路徑，大小，版本和數位簽章），有關內核物件的資訊，驅動程式，服務，Microsoft Internet Explorer 延伸，列印系統延伸，Windows 資源管理器延伸，智慧安裝元素，控制台小程式，hosts 檔案項目和系統登錄檔，以及瀏覽器和郵件用戶端的版本。

- 有關所有潛在惡意物件和活動的資訊：偵測到的物件的名稱，電腦上物件的完整路徑，所處理檔案的校驗和 (MD5、SHA2-256、SHA1)，偵測日期和時間，感染檔案的名稱、大小和路徑，路徑範本代碼，表示物件是否為容器的指示器，封裝程式名稱（如果檔案已封裝），檔案類型代碼，檔案格式 ID，惡意軟體執行的操作清單以及軟體和使用者針對其做出的回應決策，用於制定決策的病毒資料庫的 Id，偵測到的威脅在權利持有者分類中的名稱，危險等級，偵測狀態和偵測方法，包含在已分析內容中的原因及內容中檔案的序號，校驗和 (MD5、SHA2-256、SHA1)，用於傳送感染訊息或連結的應用程式的可執行檔的名稱和內容，被封鎖物件的主機的去個性化 IP 位址 (IPv4 和 IPv6)，檔案熵，檔案自動執行指示器，在系統中首次偵測到檔案的時間，上次傳送統計資訊後檔案被執行的次數，透過其收到惡意物件的郵件用戶端的名稱、校驗和 (MD5、SHA2-256、SHA1) 和大小，執行掃描的軟體工作的 ID，表示檔案信譽或簽章是否經過檢查的指示器，檔案處理結果，為物件收集的模式的校驗和 (MD5)，模式大小（以位元組為單位），以及使用的偵測技術的技術規格。

- 可執行檔和不可執行檔（全部或部分）。

- 自軟體安裝以來和上次更新以來軟體傾印和系統傾印 (BSOD) 的次數，發生故障的軟體模組的 ID 和版本，軟體處理程序的記憶體堆疊，以及發生故障時的病毒資料庫的相關資訊。

- WMI 儲存庫類的說明和類實例。

- 關於應用程式活動的報告。

- 網路流量封包。

- 參與作業系統載入處理程序的磁區。

- 有關軟體操作的服務資訊：編譯器版本，所掃描物件的惡意活動的指示器，傳送的統計資訊集的版本，有關統計資料可用性和有效性的資訊，用於生成所傳送統計資料的條件的 ID，以及表示軟體是否以互動模式執行的指示器。

- 電腦 RAM 段。

## 為防護元件啟用和停用雲端模式

從卡巴斯基專屬安全網路版本 3.0 開始，在使用卡巴斯基專屬安全網路時，雲端模式功能可用。

*要為防護元件啟用或停用雲端模式：*

1. 開啟程式設定視窗。
2. 在視窗左側的"**進階威脅防護**"區域中，選擇"**卡巴斯基安全網路**"。
   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：
   - 選擇"**為防護元件啟用雲端模式**"核取方塊。

如果選中該核取方塊，Kaspersky Endpoint Security 將使用病毒資料庫的輕量級版本，這可以減少作業系統資源上的負載。

選中該核取方塊後，Kaspersky Endpoint Security 在下次更新期間下載病毒資料庫的輕量級版本。

如果病毒資料庫的輕量級版本不可用，Kaspersky Endpoint Security 會自動轉換到病毒資料庫的進階版本。

- 清除“**為防護元件啟用雲端模式**”核取方塊。
  如果清除該核取方塊，Kaspersky Endpoint Security 將使用病毒資料庫的完全版本。

  清除該核取方塊後，Kaspersky Endpoint Security 在下次更新期間下載病毒資料庫的完全版本。

如果選中“**啟用卡巴斯基安全網路**”核取方塊，則此核取方塊可用。

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“**威脅偵測技術**”區域。
   將開啟“**威脅偵測技術**”視窗。
   以下有關卡巴斯基安全網路效能的資訊顯示在“**威脅偵測技術**”視窗的下部：
   - Kaspersky Endpoint Security 與卡巴斯基安全網路的連線的下列狀態值之一顯示在“**卡巴斯基安全網路 (KSN)**”行下：
     - *已啟用。可用。*
       該狀態表示 Kaspersky Endpoint Security 執行中使用卡巴斯基安全網路，且 KSN 伺服器可用。
     - *已啟用。不可用。*
       該狀態表示 Kaspersky Endpoint Security 執行中使用卡巴斯基安全網路，但 KSN 伺服器不可用。
     - *已停用。*
       該狀態表示 Kaspersky Endpoint Security 執行中不使用卡巴斯基安全網路。
   - “**列入白名單的物件**”、“**列入白名單的物件**”和“**過去 24 小時內消除的威脅**”行顯示卡巴斯基安全網路雲端服務基礎結構的狀態和全域統計資訊。
   - “**上次同步**”行顯示 Kaspersky Endpoint Security 與 KSN 伺服器最近一次同步的日期和時間。

     “**威脅偵測技術**”視窗開啟時，應用程式收集 KSN 使用統計資訊。卡巴斯基安全網路雲端服務基礎結構的全域統計資訊以及“**上次同步**”行不會即時重新整理。

如果自上次與 KSN 伺服器同步以來經過的時間超過 15 分鐘或顯示“*未知*”狀態，則 Kaspersky Endpoint Security 與卡巴斯基安全網路的連線的狀態值將設為“*啟用*”。*不可用*。

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。
- 應用程式未啟動。
- 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）。

如果與卡巴斯基安全網路伺服器的連線無法復原，建議聯絡服務提供商的技術支援。

## 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。
- **產品版本**。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 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 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 網站上檢視有關 Kaspersky Endpoint Security 增強防護的詳細資訊。

# 應用程式行為偵測

本章節介紹應用程式行為偵測的資訊，以及如何設定元件。

## 關於行為偵測

應用程式“行為偵測”元件收集您電腦上的應用程式操作的資訊，並將此資訊提供給其他防護元件以提高效能。

應用程式“行為偵測”元件利用行為流特徵碼 (BSS)。這些特徵碼包含 Kaspersky Endpoint Security 分類為危險的操作序列。如果應用程式操作比對危險活動行為特徵碼，Kaspersky Endpoint Security 將執行選定的回應操作。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。

## 啟用和停用行為偵測

預設情況下，行為偵測已啟用並在 Kaspersky 專家建議的模式下執行。您可以根據需要停用行為偵測。

除非絕對必要，否則不建議停用行為偵測，因為這樣做會降低防護元件的有效性。防護元件可請求“行為偵測”元件收集的資料以偵測威脅。

*要啟用或停用“行為偵測”：*

1. 開啟程式設定視窗。
2. 在視窗左側的“**進階威脅防護**”區域中選取“**行為偵測**”子區域。
   在視窗右側，將顯示“行為偵測”元件的設定。
3. 請執行以下操作之一：
   - 如果您希望 Kaspersky Endpoint Security 使用危險活動行為特徵碼來分析作業系統中的應用程式活動，請選中“**啟用行為偵測**”核取方塊。
   - 如果您不希望 Kaspersky Endpoint Security 使用危險活動行為特徵碼來分析作業系統中的應用程式活動，請清除“**啟用行為偵測**”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操作

當 Kaspersky Endpoint Security 偵測到惡意活動時，它會記錄一個項目，其中包含偵測到的應用程式活動的資訊。

*為了選擇程式進行惡意活動時的操作，請執行以下步驟:*

1. 開啟程式設定視窗。
2. 在視窗左側的“**進階威脅防護**”區域中選取“**行為偵測**”子區域。
   在視窗右側，將顯示“行為偵測”元件的設定。

3. 在“**偵測惡意軟體活動時**”下拉清單中選擇必要操作：

- **刪除檔案**。

  如果選擇此項目，在偵測到惡意活動時，Kaspersky Endpoint Security 會刪除惡意程式的可執行檔，同時在備份區建立該檔案的備份副本。

- **終止程式**。

  如果選擇此項目，在偵測到惡意活動時，Kaspersky Endpoint Security 會終止該應用程式。

- **通知**。

  如果選擇此項目並且偵測到應用程式的惡意軟體活動，Kaspersky Endpoint Security 將應用程式惡意軟體活動的相關資訊新增至活動威脅清單。

4. 要儲存變更，請點擊“**儲存**”按鈕。

## 設定共用資料夾對外部加密的防護

此元件只能監控針對儲存在檔案系統為 NTFS 的大型儲存裝置上並且未使用 EFS 加密的檔案所進行的操作。

分享資料夾對外部加密的防護會分析分享資料夾中的活動。如果該活動與外部加密的典型行為流特徵碼比對，Kaspersky Endpoint Security 將執行選定操作。

您可以按如下方式設定共用資料夾對外部加密的防護：

- 選擇在偵測到共用資料夾外部加密時採取的操作。
- 設定共用資料夾對外部加密的防護的排除項目位址。

## 啟用和停用共用資料夾對外部加密的防護

預設情況下，停用共用資料夾對外部加密的防護。

安裝 Kaspersky Endpoint Security 後，共用資料夾對外部加密的防護將受到限制，直到電腦重新啟動為止。

*要啟用或停用共用資料夾對外部加密的防護：*

1. 開啟程式設定視窗。
2. 在視窗左側的“**進階威脅防護**”區域中選取“**行為偵測**”子區域。

   在視窗右側，將顯示“行為偵測”元件的設定。

3. 請執行以下操作之一：

- 如果您希望 Kaspersky Endpoint Security 分析外部加密的典型活動，請在“**共用資料夾對外部加密的防護**”區域中選中“**啟用共用資料夾對外部加密的防護**”核取方塊。

- 如果您希望 Kaspersky Endpoint Security 分析外部加密的典型活動，請在**"共用資料夾對外部加密的防護"**區域中清除**"啟用共用資料夾對外部加密的防護"**核取方塊。

4. 要儲存變更，請點擊**"儲存"**按鈕。

## 選擇在偵測到共用資料夾外部加密時採取的操作

偵測到修改共用資料夾內檔案的嘗試時，Kaspersky Endpoint Security 將記錄一個項目，其中包含偵測到的修改共用資料夾內檔案的嘗試的相關資訊。

*要選擇在偵測到共用資料夾外部加密時採取的操作：*

1. 開啟程式設定視窗。

2. 在視窗左側的**"進階威脅防護"**區域中選取**"行為偵測"**子區域。

   在視窗右側，將顯示"行為偵測"元件的設定。

3. 在**"共用資料夾對外部加密的防護"**區域的**"偵測共用資料夾的外部加密時"**下拉清單中，選擇必要操作：

   - **封鎖連線**。

     如果選擇此項目，在偵測到修改共用資料夾中的檔案的嘗試時，Kaspersky Endpoint Security 將封鎖來自嘗試修改檔案的電腦的網路活動，建立被修改檔案的備份副本，並產生一條包含修改共用資料夾中的檔案的嘗試的相關資訊的日誌項目。此外，如果啟用了"修復引擎"元件，Kaspersky Endpoint Security 會從備份副本還原被修改的檔案。

     如果選擇**"封鎖連線"**，則可以在**"封鎖連線持續時間"**欄位中指定封鎖網路連線的時間（以分鐘為單位）。

   - **通知**。

     如果選擇此項目，在偵測到修改共用資料夾中的檔案的嘗試時，Kaspersky Endpoint Security 會將修改共用資料夾中的檔案的嘗試的相關資訊新增到活動威脅清單中。

4. 要儲存變更，請點擊**"儲存"**按鈕。

## 設定共用資料夾對外部加密的防護的排除項目位址

必須啟用稽核登入服務，才能從共用資料夾對外部加密的防護中排除位址。預設情況下，稽核登入服務已停用（有關啟用稽核登入服務的詳細資訊，請存取 Microsoft 網站）。

如果遠端電腦在 Kaspersky Endpoint Security 啟動前啟動，從共用資料夾防護中排除位址的功能將不適用於該遠端電腦。您可以在 Kaspersky Endpoint Security 啟動後重啟該遠端電腦，確保從共用資料夾防護中排除位址的功能在此遠端電腦上有效。

*要排除對共用資料夾執行外部加密的遠端電腦：*

1. 開啟程式設定視窗。

2. 在視窗左側的**"進階威脅防護"**區域中選取**"行為偵測"**子區域。

在視窗右側，將顯示“行為偵測”元件的設定。

3. 在“**共用資料夾對外部加密的防護**”區域中，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：

   - 如果您要向排除清單新增 IP 位址或電腦名稱，請點擊“**新增**”按鈕。
   - 如果您希望編輯 IP 位址或電腦名稱，請在排除清單中選定它，然後點擊“**編輯**”按鈕。

   “**電腦**”視窗將開啟。

5. 輸入不應處理其外部加密嘗試的電腦的 IP 位址或名稱。

6. 在“**電腦**”視窗中點擊“**確定**”。

7. 在“**排除**”視窗中點擊“**確定**”。

8. 要儲存變更，請點擊“**儲存**”按鈕。

# 弱點利用防禦

本章節介紹"弱點利用防禦"的資訊，以及如何設定元件。

## 關於弱點利用防禦

"弱點利用防禦"元件跟蹤由易於感染的應用程式執行的可執行檔。當存在從易於感染的應用程式執行可執行檔的嘗試，並且該嘗試並非由使用者執行時，Kaspersky Endpoint Security 將封鎖該檔案執行。有關被封鎖的可執行檔啟動的資訊儲存在"弱點利用防禦"報告中。

## 啟用和停用弱點利用防禦

預設情況下，"弱點利用防禦"已啟用並在 Kaspersky 專家建議的模式下執行。您可以根據需要停用"弱點利用防禦"。

*要啟用或停用弱點利用防禦：*

1. 開啟程式設定視窗。
2. 在視窗左側的"**進階威脅防護**"區域中選取"**弱點利用防禦**"子區域。

   "弱點利用防禦"元件的設定顯示在視窗右方。
3. 請執行以下操作之一：
   - 如果您希望 Kaspersky Endpoint Security 監控由易於感染的應用程式執行的可執行檔，請選中"**啟用弱點利用防禦**"核取方塊。

     如果 Kaspersky Endpoint Security 偵測到某個易於感染的應用程式的可執行檔被除使用者以外的事物執行，Kaspersky Endpoint Security 將執行在"**偵測弱點時**"下拉清單中選擇的操作。
   - 如果您不希望 Kaspersky Endpoint Security 監控由易於感染的應用程式執行的可執行檔，請清除"**啟用弱點利用防禦**"核取方塊。
4. 要儲存變更，請點擊"**儲存**"按鈕。

## 設定弱點利用防禦

您可以執行以下操作來設定"弱點利用防禦"元件：

- 選擇在偵測到弱點時執行的操作
- 啟用或停用系統處理程序記憶體防護。

## 選擇在偵測到弱點時執行的操作

預設情況下，在偵測到弱點時，Kaspersky Endpoint Security 將封鎖利用弱點所嘗試的操作。

*要選擇在偵測到弱點時執行的操作：*

1. 開啟程式設定視窗。
2. 在視窗左側的**"進階威脅防護"**區域中選取**"弱點利用防禦"**子區域。

   "弱點利用防禦"元件的設定顯示在視窗右方。
3. 在**"偵測弱點時"**下拉清單中選擇必要操作：

   - **封鎖操作**。

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

   - **通知**。

     如果選擇此項目，Kaspersky Endpoint Security 將在偵測到弱點時記錄包含弱點相關資訊的項目，並將此弱點的相關資訊新增至活動威脅清單。
4. 要儲存變更，請點擊**"儲存"**按鈕。

# 啟用和停用系統處理程序記憶體防護

預設情況下，啟用系統處理程序記憶體防護。

*要啟用或停用系統處理程序記憶體防護：*

1. 開啟程式設定視窗。
2. 在視窗左側的**"進階威脅防護"**區域中選取**"弱點利用防禦"**子區域。

   "弱點利用防禦"元件的設定顯示在視窗右方。
3. 請執行以下操作之一：

   - 如果您希望 Kaspersky Endpoint Security 封鎖試圖存取系統處理程序的外部處理程序，請在**"系統處理程序記憶體防護"**區域中選中**"啟用系統處理程序記憶體防護"**核取方塊。
   - 如果您不希望 Kaspersky Endpoint Security 封鎖試圖存取系統處理程序的外部處理程序，請在**"系統處理程序記憶體防護"**區域中清除**"啟用系統處理程序記憶體防護"**核取方塊。
4. 要儲存變更，請點擊**"儲存"**按鈕。

# 主機入侵防禦

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"主機入侵防禦"的資訊，以及如何設定元件。

## 關於主機入侵防禦

"主機入侵防禦"元件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和個人資料的存取。

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。應用程式權限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

當應用程式首次啟動時，"主機入侵防禦"元件會檢查此應用程式的安全性並將其置於某個信任群組中。信任群組定義在控制應用程式活動時 Kaspersky Endpoint Security 所套用的規則。

建議您加入卡巴斯基安全網路以協助"主機入侵防禦"元件更有效地工作。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權限控制規則。

再次啟動應用程式時，"主機入侵防禦"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權限控制規則。如果應用程式已經過修改，"主機入侵防禦"會分析應用程式，就像它初次開機時一樣。

## 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：

- 必須啟用"主機入侵防禦"元件，此功能才有效。
- 如果在"主機入侵防禦"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"主機入侵防禦"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、攜帶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 Lab 不保證支援不在清單中的鏡頭。

## 啟用和停用主機入侵防禦

預設情況下，"主機入侵防禦"元件已啟用並在 Kaspersky 專家建議的模式下執行。如有必要，您可以停用"主機入侵防禦"元件。

*要啟用或停用"主機入侵防禦"元件：*

1. 開啟程式設定視窗。
2. 在視窗左側的"**進階威脅防護**"區域中，選取"**主機入侵防禦**"。
   在視窗右側，將顯示"主機入侵防禦"元件的設定。
3. 在視窗右側，執行下列操作：
   - 如果您要啟用"主機入侵防禦"元件，請選中"**啟用主機入侵防禦**"核取方塊。
   - 如果您要停用"主機入侵防禦"元件，請清除"**啟用主機入侵防禦**"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

每個應用程式首次啟動時，"主機入侵防禦"元件都會檢查此應用程式的安全性並將其置於某個信任群組中。

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項目， 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：隨後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 資料庫中此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 自動將所有未知應用程式分配到的信任群組。 Kaspersky Endpoint Security 啟動之前啟動的應用程式將自動移至在"**選擇信任群組**"視窗中指定的信任群組。

對於先于 Kaspersky Endpoint Security 啟動的應用程式，只有網路活動受到控制。程式根據防火牆設定中指定的網路規則進行控制。

## 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。根據收到的回應，應用程式可能會被移動至與"主機入侵防禦"元件設定中指定的信任群組不同的信任群組中。

Kaspersky Endpoint Security 總是將帶有 Microsoft 憑證簽章或 Kaspersky 憑證簽章的應用程式放入信任群組。

*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"**進階威脅防護**"區域中，選取"**主機入侵防禦**"。
   在視窗右側，將顯示"**主機入侵防禦**"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软体供應商。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. 要將所有未知應用程式移至指定的信任群組，請從"**如果無法定義信任群組，則自動將應用程式移至**"下拉清單中選擇所需工作群組。

   出於安全原因，**信任**群組未包括在"**如果無法定義信任群組，則自動將應用程式移至**"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 Lab 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，您可以根據需要編輯單個應用程式的活動控制規則。

*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"**進階威脅防護**"區域中，選取"**主機入侵防禦**"。

   在視窗右側，將顯示"主機入侵防禦"元件的設定。

3. 點擊"**應用程式**"按鈕。

   將開啟"**應用程式**"視窗，並顯示"**應用程式權限控制**"標籤。

4. 在"**應用程式權限控制**"標籤上選取相關的應用程式。
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"**信任群組**"/"**低限制群組**"/"**高限制群組**"/"**不信任群組**"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信任群組

對於先于 Kaspersky Endpoint Security 啟動的應用程式，只有網路活動受到控制。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**"進階威脅防護"**區域中，選取**"主機入侵防禦"**。
   在視窗右側，將顯示"主機入侵防禦"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權限控制規則來控制。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權限控制規則。

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權限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，"主機入侵防禦"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權限控制規則。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**"進階威脅防護"**區域中，選取**"主機入侵防禦"**。
   在視窗右側，將顯示"主機入侵防禦"元件的設定。
3. 點擊**"應用程式"**按鈕。
   這將開啟**"主機入侵防禦"**視窗中的**"應用程式權限控制"**標籤。
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"**標籤。
   - 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"**標籤。

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**"進階威脅防護"**區域中，選取**"主機入侵防禦"**。

   在視窗右側，將顯示"主機入侵防禦"元件的設定。

3. 點擊**"應用程式"**按鈕。

   這將開啟**"主機入侵防禦"**視窗中的**"應用程式權限控制"**標籤。

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**"應用程式權限控制"**標籤的右下角，點擊**"附加"**按鈕。

**"應用程式控制規則"**視窗將開啟。

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"**標籤。
   - 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"**標籤。

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**"進階威脅防護"**區域中，選取**"主機入侵防禦"**。

   在視窗右側，將顯示"主機入侵防禦"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，"主機入侵防禦"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受信任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**"進階威脅防護"**區域中，選取**"主機入侵防禦"**。
   在視窗右側，將顯示"主機入侵防禦"元件的設定。
3. 點擊**"應用程式"**按鈕。
   這將開啟**"主機入侵防禦"**視窗中的**"應用程式控制規則"**標籤。
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"**。
   **"應用程式控制規則"**視窗將開啟。
6. 在開啟的**"應用程式控制規則"**視窗中，選取**"排除"**標籤。
7. 選取**"不要繼承父處理程序限制（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**"進階威脅防護"**區域中，選取**"主機入侵防禦"**。
   在視窗右側，將顯示"主機入侵防禦"元件的設定。
3. 點擊**"應用程式"**按鈕。
   這將開啟**"主機入侵防禦"**視窗中的**"應用程式控制規則"**標籤。
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"**。
   **"應用程式控制規則"**視窗將開啟。
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**"進階威脅防護"**區域中，選取**"主機入侵防禦"**。
   在視窗右側，將顯示"主機入侵防禦"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的控制規則"**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的控制規則"**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

"主機入侵防禦"元件管理應用程式處理各種不同類別作業系統資源和個人資料的權限。

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防護資源，請執行以下操作：*

1. 開啟程式設定視窗。
2. 在視窗左側的**"進階威脅防護"**區域中，選取**"主機入侵防禦"**。
   在視窗右側，將顯示"主機入侵防禦"元件的設定。
3. 點擊 **資源** 按鈕。
   這將開啟**"主機入侵防禦"**視窗中的**"受防護資源"**標籤。
4. 在**"受防護資源"**標籤的左側，選取您要向其新增新類別受防護資源的受防護資源區域或類別。
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，輸入受防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防護資源類別。
8. 在**"主機入侵防禦"**視窗中點擊**"確定"**。
9. 要儲存變更，請點擊**"儲存"**按鈕。

新增某個類別的受防護資源後，您可以透過點擊**"受防護資源"**標籤的左上角的**"編輯"**或**"移除"**按鈕來編輯或刪除此類別。

## 新增受防護資源

*若要新增受防護資源，請執行以下操作：*

1. 開啟程式設定視窗。
2. 在視窗左側的**"進階威脅防護"**區域中，選取**"主機入侵防禦"**。
   在視窗右側，將顯示"主機入侵防禦"元件的設定。
3. 點擊 **資源** 按鈕。

這將開啟"**主機入侵防禦**"視窗中的"**受防護資源**"標籤。

4. 在"**受防護資源**"標籤的左側，選取您要向其新增新類別受防護資源的受防護資源類別。
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"**受防護資源**"視窗。
6. 在"**受防護資源**"視窗的"**名稱**"欄位中輸入受防護資源的名稱。
7. 點擊"**瀏覽**"按鈕。
8. 在開啟的視窗中，根據您要新增的受防護資源的類型指定必要的設定。點擊"**確定**"。
9. 在"**受防護資源**"視窗中，點擊"**確定**"。
   在"**受防護資源**"標籤上選取類別的受防護資源清單中。
10. 在"**主機入侵防禦**"視窗中點擊"**確定**"。
11. 要儲存變更，請點擊"**儲存**"按鈕。

新增受防護資源後，您可以透過在"**受防護資源**"標籤的左上角點擊"**編輯**"或"**移除**"按鈕來編輯或刪除受防護資源。

## 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"**進階威脅防護**"區域中，選取"**主機入侵防禦**"。
   在視窗右側，將顯示"主機入侵防禦"元件的設定。
3. 在視窗右側，點擊"**資源**"按鈕。
   這將開啟"**主機入侵防禦**"視窗中的"**受防護資源**"標籤。
4. 請執行以下操作之一：
   - 在該標籤左側的受防護資源清單中，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"主機入侵防禦"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"**受防護資源**"視窗。

b. 在“**受防護資源**”視窗的“**名稱**”欄位中輸入受防護資源的名稱。

c. 點擊“**瀏覽**”按鈕。

d. 在開啟的視窗中，根據要新增到“主機入侵防禦”元件防護的排除清單的受防護資源類型，指定必需的設定。

e. 點擊“**確定**”。

f. 在“**受防護資源**”視窗中，點擊“**確定**”。

在排除在“主機入侵防禦”元件防護範圍之外的資源的清單中將顯示一個新項目。

> 將資源新增到“主機入侵防禦”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“**移除**”按鈕來編輯或移除此資源。

g. 在“**排除**”視窗中點擊“**確定**”。

5. 在“**主機入侵防禦**”視窗中點擊“**確定**”。

6. 要儲存變更，請點擊“**儲存**”按鈕。

# 修復引擎

本部分包含有關"修復引擎"的資訊以及有關啟用或停用此元件的說明。

## 關於修復引擎

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

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

- 檔案活動。

  Kaspersky Endpoint Security 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。

  Kaspersky Endpoint Security 將刪除已被惡意程式入侵的程式所建立的可執行檔。

  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。

檔案威脅防護元件可以在病毒掃描期間啟動惡意操作回溯。

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。

## 啟用和停用修復引擎

*要啟用或停用修復引擎：*

1. 開啟程式設定視窗。
2. 在視窗左側的"**進階威脅防護**"區域中選取"**修復引擎**"子區域。
3. 請執行以下操作之一：
   - 如果您希望 Kaspersky Endpoint Security 在偵測到惡意軟體時回溯惡意軟體在作業系統中執行的操作，請選中視窗右側"**啟用修復引擎**"核取方塊。

- 如果您不希望 Kaspersky Endpoint Security 在偵測到惡意軟體時回溯惡意軟體在作業系統中執行的操作，請清除視窗右側**"啟用修復引擎"**核取方塊。

4. 要儲存變更，請點擊**"儲存"**按鈕。

# 檔案威脅防護

本章節介紹檔案威脅防護資訊，以及如何設定元件。

## 關於檔案威脅防護

"檔案威脅防護"元件允許您防止電腦的檔案系統受到感染。預設情況下，"檔案威脅防護"元件與 Kaspersky Endpoint Security 一起啟動，持續停留在電腦的記憶體中，掃描在電腦及其連線的磁碟機上開啟或執行的檔案以偵測是否存在病毒和其他威脅。掃描根據應用程式設定執行。

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. 偵測檔案中物件的類型（例如*病毒*或*木馬*）。
2. 該應用程式將顯示關於在檔案中偵測到的惡意物件的通知（如果配置了通知），並採取在"檔案威脅防護"元件設定中指定的動作來處理檔案。

## 啟用和停用檔案威脅防護

預設情況下，"檔案威脅防護"元件已啟用並在 Kaspersky 專家建議的模式下執行。如有必要，您可以停用"檔案威脅防護"。

*要啟用和停用"檔案威脅防護"：*

1. 開啟程式設定視窗。
2. 在視窗左側的"**關鍵威脅防護**"區域中選擇"**檔案威脅防護**"。
   "檔案威脅防護"元件的設定顯示在視窗右方。
3. 請執行以下操作之一：
   - 如果要啟用"檔案威脅防護"，請選中"**啟用檔案威脅防護**"核取方塊。
   - 如果要停用"檔案威脅防護"，請清除"**啟用檔案威脅防護**"核取方塊。
4. 要儲存變更，請點擊"**儲存**"按鈕。

## 自動暫停檔案威脅防護

您可以設定"檔案威脅防護"在指定時間或處理特定應用程式時自動暫停。

只有"檔案威脅防護"與某些應用程式衝突時，才應將其暫停作為最後手段。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"檔案威脅防護"元件以便與您的電腦上的其他應用程式同時執行。

*要設定"檔案威脅防護"的自動暫停：*

1. 開啟程式設定視窗。
2. 在視窗左側的**"關鍵威脅防護"**區域中選擇**"檔案威脅防護"**。

   **"檔案威脅防護"**元件的設定顯示在視窗右方。
3. 在**"安全防護等級"**區域中點擊**"設定"**按鈕。

   **"檔案威脅防護"**視窗將開啟。
4. 在**"檔案威脅防護"**視窗中，選擇**"附加"**標籤。
5. 在**"暫停工作"**區域：

   - 如果要設定"檔案威脅防護"在指定時間自動暫停，請選取**"根據排程"**然後點擊**"排程"**按鈕。

     開啟**"暫停工作"**視窗。

   - 如果要設定"檔案威脅防護"在指定應用程式啟動時自動暫停，請選取**"在程式啟動時"**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"檔案威脅防護"在指定時間自動暫停，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"檔案威脅防護"的暫停時間（格式為 HH:MM）。點擊**"確定"**。

   - 如果要設定"檔案威脅防護"在指定應用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**"移除"**按鈕建立一個應用程式清單，以便"檔案威脅防護"在這些應用程式執行時暫停。點擊**"確定"**。
7. 在**"檔案威脅防護"**視窗中，點擊**"確定"**。
8. 要儲存變更，請點擊**"儲存"**按鈕。

## 檔案威脅防護設定

您可以執行以下操作來設定"檔案威脅防護"元件：

- 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"檔案威脅防護"元件在偵測到受感染的檔案時執行的操作。

- 構成"檔案威脅防護"元件的防護範圍。

  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。

  "檔案威脅防護"元件使用一種稱為機器學習和特徵碼分析的掃描技術 。在特徵碼分析過程中，"檔案威脅防護"元件將偵測到的物件與應用程式病毒資料庫中的記錄進行比較。根據 Kaspersky 專家的建議，機器學習和特徵碼分析始終啟用。

  您可以使用啟發式分析提高防護效率。在啟發式分析中，"檔案威脅防護"元件將分析物件在作業系統中的活動。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。

  您可以透過減少掃描時間和提高 Kaspersky Endpoint Security 的執行速度來最佳化"檔案威脅防護"元件執行的檔案掃描。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，"檔案威脅防護"元件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：**高防護**，**建議防護**和**低防護**。**建議防護**安全防護等級設定將被視為 Kaspersky Lab 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"**關鍵威脅防護**"區域中選擇"**檔案威脅防護**"。

   "檔案威脅防護"元件的設定顯示在視窗右方。
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（**高防護**，**建議防護**或**低防護**），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"**檔案威脅防護**"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"**建議防護**"，點擊"**預設**"按鈕。
4. 要儲存變更，請點擊"**儲存**"按鈕。

## 變更"檔案威脅防護"元件對受感染檔案執行的操作

預設情況下，"檔案威脅防護"元件將自動嘗試對已經偵測到的所有受感染檔案執行解毒操作。如果解毒失敗，"檔案威脅防護"元件將刪除這些檔案。

*要變更"檔案威脅防護"元件對受感染檔案執行的操作：*

1. 開啟程式設定視窗。
2. 在視窗左側的"**關鍵威脅防護**"區域中選擇"**檔案威脅防護**"。

   "檔案威脅防護"元件的設定顯示在視窗右方。
3. 在"**偵測到威脅後的動作**"區域，選取所需的模式：

- **解毒，如果解毒失敗則刪除**。

  如果選擇該選項，“檔案威脅防護”元件將自動嘗試對已經偵測到的所有受感染檔案執行解毒操作。如果解毒失敗，“檔案威脅防護”元件將刪除這些檔案。

- **解毒，如果解毒失敗則封鎖**。

  如果選擇該選項，“檔案威脅防護”元件將自動嘗試對已經偵測到的所有受感染檔案執行解毒操作。如果解毒失敗，“檔案威脅防護”元件將封鎖這些檔案。

- **封鎖**。

  如果選擇該選項，“檔案威脅防護”元件將自動封鎖所有受感染的檔案，而不對其進行解毒處理。

4. 要儲存變更，請點擊“**儲存**”按鈕。

## 構成“檔案威脅防護”元件的防護範圍

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。要掃描的檔案的位置和類型是“檔案威脅防護”元件防護範圍的內容。預設情況下，“檔案威脅防護”元件僅掃描從硬碟、抽取式磁碟機和網路磁碟機執行的潛在受感染檔案。

*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“**關鍵威脅防護**”區域中選擇“**檔案威脅防護**”。

   “檔案威脅防護”元件的設定顯示在視窗右方。
3. 在“**安全防護等級**”區域中點擊“**設定**”按鈕。

   “**檔案威脅防護**”視窗將開啟。
4. 在“**檔案威脅防護**”視窗中，選取“**一般**”標籤。
5. 在“**檔案類型**”區域中，指定您希望“檔案威脅防護”元件掃描的檔案類型：

   - 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。如果選擇按格式掃描檔案，則“檔案威脅防護”元件會分析檔案標頭，和副檔名無關。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**"檔案威脅防護"**視窗的**"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"檔案威脅防護"元件的掃描範圍中。
10. 在**"檔案威脅防護"**視窗中，點擊**"確定"**。
11. 要儲存變更，請點擊**"儲存"**按鈕。

## 在"檔案威脅防護"元件的執行中使用啟發式分析

*要設定"檔案威脅防護"元件執行中啟發式分析的使用：*

1. 開啟程式設定視窗。
2. 在視窗左側的**"關鍵威脅防護"**區域中選擇**"檔案威脅防護"**。

   "檔案威脅防護"元件的設定顯示在視窗右方。
3. 在**"安全防護等級"**區域中點擊**"設定"**按鈕。

   **"檔案威脅防護"**視窗將開啟。
4. 在**"檔案威脅防護"**視窗中選擇**"效能"**標籤。
5. 在**"掃描方式"**區域中：
   - 如果您希望"檔案威脅防護"元件使用啟發式分析，請選取**"啟發式分析"**核取方塊， 使用滑塊設定啟發式分析等級：**輕度掃描**、**中度掃描**或**深度掃描**。
   - 如果您不希望"檔案威脅防護"元件使用啟發式分析，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“檔案威脅防護”元件的執行中使用掃描技術

*要設定“檔案威脅防護”元件執行中掃描技術的使用：*

1. 開啟程式設定視窗。
2. 在視窗左側的“**關鍵威脅防護**”區域中選擇“**檔案威脅防護**”。
   “檔案威脅防護”元件的設定顯示在視窗右方。
3. 在“**安全防護等級**”區域中點擊“**設定**”按鈕。
   “**檔案威脅防護**”視窗將開啟。
4. 在“**檔案威脅防護**”視窗中，選擇“**附加**”標籤。
5. 在“**掃描技術**”區域中：
   - 選取您在“檔案威脅防護”元件執行中要使用的技術名稱旁邊的核取方塊。
   - 清除您在“檔案威脅防護”元件執行中不想使用的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。

## 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“**關鍵威脅防護**”區域中選擇“**檔案威脅防護**”。
   “檔案威脅防護”元件的設定顯示在視窗右方。
3. 點擊“**設定**”按鈕。
   “**檔案威脅防護**”視窗將開啟。
4. 在“**檔案威脅防護**”視窗中選擇“**效能**”標籤。
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軟體，必須將複合檔案解壓縮，但是這可能會降低掃描速度。您可以限制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。

"檔案威脅防護"元件會解毒 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**"關鍵威脅防護"**區域中選擇**"檔案威脅防護"**。

   "檔案威脅防護"元件的設定顯示在視窗右方。
3. 在**"安全防護等級"**區域中點擊**"設定"**按鈕。

   **"檔案威脅防護"**視窗將開啟。
4. 在**"檔案威脅防護"**視窗中選擇**"效能"**標籤。
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. 若要僅掃描新增和已變更的複合檔案，請選取**"只掃描新增及變更的檔案"**核取方塊。

   "檔案威脅防護"元件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：

   - 要封鎖"檔案威脅防護"元件在背景解壓縮複合檔案，請清除**"在背景解壓縮複合檔案"**核取方塊。
   - 要允許"檔案威脅防護"元件在背景掃描時解壓縮複合檔案， 請選取**"在背景解壓縮複合檔案"**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：

   - 要封鎖"檔案威脅防護"元件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。"檔案威脅防護"元件不會解壓縮大於指定大小的複合檔案。
   - 要允許"檔案威脅防護"元件解壓縮大型複合檔案，請清除**"不解壓大型復合文件"**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**"不解壓大型複合檔案"**核取方塊，"檔案威脅防護"元件均會掃描從存檔中提取的大型檔案。

10. 點擊**"確定"**。

11. 在**"檔案威脅防護"**視窗中，點擊**"確定"**。

12. 要儲存變更，請點擊**"儲存"**按鈕。

## 變更掃描模式

*掃描模式*是指觸發"檔案威脅防護"元件進行檔案掃描的條件。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，"檔案威脅防護"元件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**"關鍵威脅防護"**區域中選擇**"檔案威脅防護"**。
   "檔案威脅防護"元件的設定顯示在視窗右方。

3. 在**"安全防護等級"**區域中點擊**"設定"**按鈕。
   **"檔案威脅防護"**視窗將開啟。

4. 在**"檔案威脅防護"**視窗中，選擇**"附加"**標籤。

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。

# Web 威脅防護

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 Web 威脅防護資訊，以及如何設定元件。

## 關於 Web 威脅防護

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軟體。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。

"Web 威脅防護"元件可以防護透過 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。

"Web 威脅防護"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，並分析其中是否存在病毒和其他威脅。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"Web 威脅防護"元件設定中指定的操作。

## 啟用和停用 Web 威脅防護

預設情況下，"Web 威脅防護"元件已啟用並在 Kaspersky 專家建議的模式下執行。如有必要，您可以停用"Web 威脅防護"元件。

*要啟用或停用"Web 威脅防護"元件：*

1. 開啟程式設定視窗。
2. 在視窗左側的"**關鍵威脅防護**"區域中選擇"**Web 威脅防護**"。
   "Web 威脅防護"元件的設定顯示在視窗右方。
3. 請執行以下操作之一：
   - 如果要啟用"Web 威脅防護"元件，請選中"**啟用 Web 威脅防護**"核取方塊。
   - 如果要停用"Web 威脅防護"元件，請清除"**啟用 Web 威脅防護**"核取方塊。
4. 要儲存變更，請點擊"**儲存**"按鈕。

## Web 威脅防護設定

您可以執行以下操作來配置“Web 威脅防護”元件：

- 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“Web 威脅防護”元件執行的物件 Web 流量掃描表明該物件包含惡意程式碼，則“Web 威脅防護”元件對該物件的回應取決於您指定的操作。

- 配置“Web 威脅防護”元件的連結掃描以根據釣魚和惡意網址資料庫檢查連結。

- 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“Web 威脅防護”對透過 HTTP 和 FTP 協定傳送和接收的 Web 流量進行的掃描。

- 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。“Web 威脅防護”元件不會分析來自受信任網址的資訊，不會檢查它們中是否含有病毒或其他威脅。在一些情況下本選項十分有用，例如，當“Web 威脅防護”元件干擾您從一個已知網站上下載檔案時。

  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

為防護經由 HTTP 和 FTP 協定傳送和接收的資料，“Web 威脅防護”元件套用多個設定群組。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：**高防護**，**建議防護**和**低防護**。**建議防護**網頁流量安全防護等級可視為最佳設定，是 Kaspersky Lab 建議採用的等級。

*變更網頁流量安全等級：*

1. 開啟程式設定視窗。
2. 在視窗左側的“**關鍵威脅防護**”區域中選擇“**Web 威脅防護**”。

   “Web 威脅防護”元件的設定顯示在視窗右方。
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（**高防護**、**建議防護**或**低防護**），請使用捲軸選取一個等級。
   - 如果您希望設定一種自訂 Web 流量安全防護等級，請在“**Web 威脅防護**”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**"建議防護"**，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

預設情況下，在 Web 流量中偵測到受感染物件後，"Web 威脅防護"元件將封鎖存取物件並顯示有關此操作的通知。

*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**"關鍵威脅防護"**區域中選擇**"Web 威脅防護"**。

   "Web 威脅防護"元件的設定顯示在視窗右方。

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：

   - **封鎖下載**。

     如果選擇此選項，在 Web 流量中偵測到受感染物件後，"Web 威脅防護"元件將封鎖存取物件並顯示有關此操作的通知。

   - **通知**。

     如果選擇此選項並且在 Web 流量中偵測到受感染物件，"Web 威脅防護"元件將允許此物件下載到電腦；Kaspersky Endpoint Security 會記錄包含受感染物件相關資訊的事件，並將受感染物件相關資訊新增到活動威脅清單中。

4. 要儲存變更，請點擊**"儲存"**按鈕。

## "Web 威脅防護"掃描連結，根據釣魚和惡意網址資料庫檢查連結

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），因此"Web 威脅防護"元件將在 Web 流量掃描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 分發套件中包含釣魚網址清單。

*要配置"Web 威脅防護"元件根據釣魚和惡意網址資料庫檢查連結：*

1. 開啟程式設定視窗。

2. 在視窗左側的**"關鍵威脅防護"**區域中選擇**"Web 威脅防護"**。

   "Web 威脅防護"元件的設定顯示在視窗右方。

3. 點擊**"設定"**按鈕。

"**Web 威脅防護**"視窗將開啟。

4. 在"**Web 威脅防護**"視窗中選取"**一般**"標籤。

5. 請執行以下操作：

   - 如果您希望"Web 威脅防護"元件根據惡意網址資料庫檢查連結，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"Web 威脅防護"元件根據釣魚網址資料庫檢查連結，請在"**網路釣魚防護設定**"區域中選取"**檢查連結是否在釣魚連結資料庫中列出**"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。

## 在"Web 威脅防護"元件的執行中使用啟發式分析

*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"**關鍵威脅防護**"區域中選擇"**Web 威脅防護**"。

   "Web 威脅防護"元件的設定顯示在視窗右方。

3. 在"**安全防護等級**"區域中點擊"**設定**"按鈕。

   "**Web 威脅防護**"視窗將開啟。

4. 選取"**一般**"標籤。

5. 如果您希望"Web 威脅防護"元件使用啟發式分析掃描網頁流量中的病毒和其他惡意程式，請在"**掃描方式**"中，請選取"**用於偵測病毒的啟發式分析**"方塊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"Web 威脅防護"元件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"**用於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

*若要建立受信任網址的清單：*

1. 開啟程式設定視窗。

2. 在視窗左側的**"關鍵威脅防護"**區域中選擇**"Web 威脅防護"**。
   "Web 威脅防護"元件的設定顯示在視窗右方。

3. 點擊**"設定"**按鈕。
   **"Web 威脅防護"**視窗將開啟。

4. 選取**"受信任網址"**標籤。

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。

# 郵件威脅防護

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。

本章節介紹郵件威脅防護資訊，以及如何設定元件。

## 關於郵件威脅防護

"郵件威脅防護"元件掃描傳送和接收電子郵件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。

在電子郵件中偵測到威脅，"郵件威脅防護"元件將執行以下操作：

1. 將"*已感染*"狀態指定給電子郵件。

   在以下情況下，此狀態指定給電子郵件：

   - 電子郵件掃描發現了 Kaspersky Endpoint Security 病毒資料庫中包括的已知病毒代碼的片段。
   - 電子郵件包含典型病毒或其他惡意軟體的程式碼片段，或已知病毒的變種。

2. 識別電子郵件中所偵測物件的類型（例如*木馬*）。
3. 封鎖該電子郵件。
4. 顯示關於偵測的物件的通知（如果在通知設定中配置為顯示通知）。
5. 執行"郵件威脅防護"元件設定中定義的操作。

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。"郵件威脅防護"外掛程式在安裝 Kaspersky Endpoint Security 時嵌入在 Microsoft Office Outlook 郵件用戶端中。

## 啟用和停用郵件威脅防護

預設情況下，"郵件威脅防護"元件已啟用並在 Kaspersky 專家建議的模式下執行。如有必要，您可以停用"郵件威脅防護"元件。

*要啟用或停用"郵件威脅防護"元件：*

1. 開啟"調整應用程式設定"視窗。
2. 在視窗左側的"**關鍵威脅防護**"區域中選擇"**郵件威脅防護**"。

   "郵件威脅防護"元件的設定顯示在視窗右方。

3. 請執行以下操作之一：

- 如果要啟用“郵件威脅防護”元件，請選中“**啟用郵件威脅防護**”核取方塊。
- 如果要停用“郵件威脅防護”元件，請清除“**啟用郵件威脅防護**”核取方塊。

4. 要儲存變更，請點擊“**儲存**”按鈕。

## 郵件威脅防護設定

您可以執行以下操作來設定“郵件威脅防護”元件：

- 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。
- 構成“郵件威脅防護”元件的防護範圍。
- 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，“郵件威脅防護”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，“郵件威脅防護”元件將不能掃描病毒、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

“檔案威脅防護”元件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：**高防護**，**建議防護**和**低防護**。**建議防護**檔案安全防護等級可視為最佳設定，是 Kaspersky Lab 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**"關鍵威脅防護"**區域中選擇**"郵件威脅防護"**。

   "郵件威脅防護"元件的設定顯示在視窗右方。
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（**高防護**，**建議防護**或**低防護**），請使用捲軸選取一個等級。
   - 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**"郵件威脅防護"**視窗中輸入自訂設定。

     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**"建議防護"**，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

預設情況下，"郵件威脅防護"元件將自動嘗試對已經偵測到的所有受感染電子郵件執行解毒操作。如果解毒失敗，"郵件威脅防護"元件會刪除感染的電子郵件。

*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**"關鍵威脅防護"**區域中選擇**"郵件威脅防護"**。

   "郵件威脅防護"元件的設定顯示在視窗右方。
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：

   - **解毒，如果解毒失敗則刪除**。

     如果選擇此選項，"郵件威脅防護"將自動對偵測到的所有受感染的電子郵件訊息進行解毒。如果解毒失敗，"郵件威脅防護"元件會刪除感染的電子郵件。
   - **解毒，如果解毒失敗則封鎖**。

     如果選擇此選項，"郵件威脅防護"將自動對偵測到的所有受感染的電子郵件訊息進行解毒。如果解毒失敗，"郵件威脅防護"元件會封鎖感染的電子郵件。
   - **封鎖**。

     如果選擇此選項，"郵件威脅防護"將自動封鎖所有受感染的電子郵件，不進行解毒。
4. 要儲存變更，請點擊**"儲存"**按鈕。

## 構成"郵件威脅防護"元件的防護範圍

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。"郵件威脅防護"元件的防護範圍內容包括將"郵件威脅防護"元件整合至郵件用戶端的設定，以及被"郵件威脅防護"元件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。

*要構成"郵件威脅防護"元件的防護範圍：*

1. 開啟程式設定視窗。
2. 在視窗左側的"**關鍵威脅防護**"區域中選擇"**郵件威脅防護**"。

   "郵件威脅防護"元件的設定顯示在視窗右方。
3. 點擊"**設定**"按鈕。

   "**郵件威脅防護**"視窗將開啟。
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"郵件威脅防護"元件掃描電腦上的所有接收和傳送的郵件，請選取"**接收和傳送的電子郵件**"選項。
   - 如果希望"郵件威脅防護"元件只掃描電腦中的接收電子郵件，請選取"**僅接收的訊息**"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"郵件威脅防護"元件在經由 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"郵件威脅防護"元件在經由 POP3、SMTP、NNTP 和 IMAP 協議傳送的電子郵件到達電腦之前進行掃描，請清除"**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 延伸程式**"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"郵件威脅防護"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"郵件威脅防護"元件掃描。
   - 如果您希望允許從 Microsoft Office Outlook 存取"郵件威脅防護"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 延伸程式**"核取方塊。

     如果您希望封鎖從 Microsoft Office Outlook 存取"郵件威脅防護"設定並且禁止經由 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，請清除"**附加：Microsoft Office Outlook 延伸程式**"核取方塊。

     "郵件威脅防護"外掛程式在安裝 Kaspersky Endpoint Security 時嵌入在 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**"基本威脅防護"**區域中，選取**"主機入侵防禦"**。

   "郵件威脅防護"元件的設定顯示在視窗右側。
3. 點擊**"設定"**按鈕。

   **"郵件威脅防護"**視窗將開啟。
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"郵件威脅防護"元件略過電子郵件附件的存檔，請取消選取**"掃描附件中的壓縮檔案"**核取方塊。
   - 如果您希望"郵件威脅防護"元件略過附加到郵件的 Office 格式檔案，請清除**"掃描附件 Office 格式"**核取方塊。
   - 如果您希望"郵件威脅防護"元件略過大小超過 N MB 的電子郵件附件，請選取**"不掃描大小大於 N MB 的壓縮檔案"**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"郵件威脅防護"元件掃描郵件附件的時間不超過 N 秒，請清除**"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

附件篩選功能不適用於發出的電子郵件。

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**"關鍵威脅防護"**區域中選擇**"郵件威脅防護"**。

   "郵件威脅防護"元件的設定顯示在視窗右方。
3. 在**"安全防護等級"**區域中點擊**"設定"**按鈕。

"**郵件威脅防護**"視窗將開啟。

4. 在"**郵件威脅防護**"視窗中選取"**附件篩選**"標籤。

5. 請執行以下操作之一：

- 如果您不希望"郵件威脅防護"元件篩選郵件附件，請選取"**停用篩選**"選項。
- 如果您希望"郵件威脅防護"元件重新命名**特定類型**的郵件附件，請選取"**重新命名選取類型的附件**"設定。

請注意檔案的實際格式可能不比對其檔案名副檔名。

如果您啟用了電子郵件附件篩選，則"郵件威脅防護"元件可能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 – 自解壓存檔或可執行檔

sys – Microsoft Windows 系統檔案

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

bin – 二進位檔案

bat – 批檔案

cmd – Microsoft Windows NT 的指令檔案（與 DOS 批次檔案類似）、OS/2

dpl – 壓縮的 Borland Delphi 庫

dll – 動態連結程式庫

scr – Microsoft Windows 屏保

cpl – Microsoft Windows 控制台模組

ocx – Microsoft OLE（物件連結和嵌入）物件

tsp – 以分時模式執行的程式

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

lnk – Microsoft Windows 連結檔案

reg – Microsoft Windows 系統登錄機碼檔案

ini – 包含 Microsoft Windows、Windows NT 和某些應用程式配置資料的設定檔

cla – Java 類

vbs – Visual Basic® 指令碼

vbe – BIOS 影片延伸外掛程式

js, jse – JavaScript source text

htm – 超文字文件

htt – Microsoft Windows 超文字標頭

hta – Microsoft Internet Explorer® 超文字程式

asp – Active Server Pages 指令碼

chm – 編撰的 HTML 檔案

pht – 帶有 PHP 指令碼的 HTML 檔案

php – 集成到 HTML 檔案的指令碼

wsh – Microsoft Windows Script Host 檔案

wsf – Microsoft Windows 指令碼

the – Microsoft Windows 95 桌面壁紙檔案

hlp – Win 說明檔案

eml – Microsoft Outlook Express 郵件

nws – 新 Microsoft Outlook Express 郵件

msg – Microsoft Mail 郵件

plg – 郵件

mbx – 已儲存的 Microsoft Office Outlook 郵件

doc* – Microsoft Office Word 文件，例如：doc（Microsoft Office Word 文件）、docx（帶 XML 支援的 Microsoft Office Word 2007 文件）、docm（帶巨集支援的 Microsoft Office Word 2007 文件）

dot* – Microsoft Office Word 文件模組，例如 dot（Microsoft Office Word 文件範本）、dotx（Microsoft Office Word 2007 文件範本）、dotm（帶巨集支援的 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® 圖紙資料庫

msi – Microsoft Windows Installer 安裝套件

otm – 適用於 Microsoft Office Outlook 的 VBA 項目

pdf – Adobe Acrobat 文件

swf – Shockwave® Flash 資料封包文件

jpg, jpeg – 壓縮影像格式

emf – 增強中繼檔案格式檔案。下一代 Microsoft Windows OS 中繼檔案 16 位元 Microsoft Windows 不支援 EMF 檔案。

ico – 物件圖示檔案

ov? – Microsoft Office Word 可執行檔

xl* – Microsoft Office Excel 文件和檔案，例如：xla 對應 Microsoft Office Excel、xlc 對應圖表、xlt 對應文件範本、xlsx 對應 Microsoft Office Excel 2007 工作簿、xltm 對應支援巨集的 Microsoft Office Excel 2007 工作簿、xlsb 對應二進位格式（非 XML）的 Microsoft Office Excel 2007 工作簿、xltx 對應於 Microsoft Office Excel 2007 範本、xlsm 對應於支援巨集的 Microsoft Office Excel 2007 範本、xlam 對應於支援巨集的 Microsoft Office Excel 2007 外掛程式

pp* – Microsoft Office PowerPoint® 文件和檔案，例如：pps 代表 Microsoft Office PowerPoint 幻燈片、ppt 代表幻燈片、pptx 代表 Microsoft Office PowerPoint 2007 幻燈片、pptm 代表支援巨集的 Microsoft Office PowerPoint 2007 幻燈片、potx 代表 Microsoft Office PowerPoint 2007 幻燈片範本、potm 代表支援巨集的 Microsoft Office PowerPoint 2007 幻燈片、ppsx 代表 Microsoft Office PowerPoint 2007 幻燈片、ppsm 代表支援巨集的 Microsoft Office PowerPoint 2007 幻燈片、ppam 代表支援巨集的 Microsoft Office PowerPoint 2007 外掛程式

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

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“郵件威脅防護”元件刪除特定類型的郵件附件，請選取“**刪除選取類型的附件**”設定。

6. 如果您在上個步驟中選取了“**重新命名選取類型的附件**”選項或者“**刪除選取類型的附件**”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“**移除**”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，“郵件威脅防護”延伸程式嵌入到 Microsoft Office Outlook（以下簡稱 Outlook）中。您可從 Outlook 內部快速開啟“郵件威脅防護”元件設定，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“郵件威脅防護”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。

郵件威脅防護延伸支援 Outlook 2010、2013、2016的操作。

如果在 Kaspersky Endpoint Security 介面中選定了**"附加：Microsoft Office Outlook 延伸程式"**核取方塊，則可以直接在 Outlook 中配置"郵件威脅防護"元件設定。

在 Outlook 中，接收的電子郵件首先由"郵件威脅防護"元件進行掃描（如果在 Kaspersky Endpoint Security 介面中選定了**"POP3/SMTP/NNTP/IMAP 流量"**核取方塊），然後由 Outlook 的"郵件威脅防護"延伸程式進行掃描。如果"郵件威脅防護"元件在郵件中偵測到惡意物件，會就此事件向您發出警訊。

傳送的電子郵件首先由 Outlook 的"郵件威脅防護"延伸程式進行掃描，然後由"郵件威脅防護"元件進行掃描。

## 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"**標籤。

*要在 Outlook 2010/2013/2016 中設定郵件掃描：*

1. 開啟 Outlook 程式主視窗。
   選取左上角的**"檔案"**標籤。
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"郵件威脅防護"延伸外掛程式掃描郵件，建議使用緩衝區的交換模式。有關交換快取模式和使用建議資訊，請參閱 Microsoft 知識庫：https://technet.microsoft.com/en-us/library/cc179175.aspx。

*要使用卡巴斯基安全管理中心設定 Outlook 的"郵件威脅防護"延伸外掛程式的執行模式：*

1. 開啟卡巴斯基安全管理中心管理主控台。

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"**標籤。

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**"關鍵威脅防護"**區域中選擇**"郵件威脅防護"**。

7. 在**"安全防護等級"**區域中點擊**"設定"**按鈕。

   **"郵件威脅防護"**視窗將開啟。

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"郵件威脅防護"延伸外掛程式在郵件到達信箱時進行掃描，選取**"接收時掃描"**核取方塊。
   - 如果您希望 Outlook 的"郵件威脅防護"延伸外掛程式在使用者開啟郵件時進行掃描，請選中**"讀取時掃描"**核取方塊。
   - 如果您希望 Outlook 的"郵件威脅防護"延伸外掛程式在傳送郵件時掃描郵件，請選中**"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**"郵件威脅防護"**的視窗上，點擊**"確定"**。

12. 套用政策。

    有關套用卡巴斯基安全管理中心政策的詳細資訊，請參閱《*卡巴斯基安全管理中心說明手冊*》。

# 網路威脅防護

本章節介紹網路攻擊防護資訊，以及如何設定元件。

## 關於網路威脅防護

“網路威脅防護”元件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。您可以編輯用於封鎖攻擊電腦的設定。

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。“網路威脅防護”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。

## 啟用和停用網路威脅防護

預設情況下，“網路威脅防護”已啟用並在最佳化模式下執行。如有必要，您可以停用“網路威脅防護”。

*要啟用或停用“網路威脅防護”：*

1. 開啟程式設定視窗。
2. 在視窗左側的“**關鍵威脅防護**”區域中選擇“**網路威脅防護**”。
   “網路威脅防護”元件設定將顯示在視窗右方。
3. 請執行以下操作：
   - 如果要啟用“網路威脅防護”，請選中“**啟用網路威脅防護**”核取方塊。
   - 如果要停用“網路威脅防護”，請清除“**啟用網路威脅防護**”核取方塊。
4. 要儲存變更，請點擊“**儲存**”按鈕。

## 網路威脅防護設定

您可以執行下列操作來配置“網路威脅防護”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**"關鍵威脅防護"**區域中選擇**"網路威脅防護"**。

   "網路威脅防護"元件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。

   如果選中此核取方塊，在偵測到網路攻擊意圖時，"網路威脅防護"元件將在指定時間內封鎖來自攻擊電腦的網路活動。這將自動防護電腦避免以後來自同一位址的網路攻擊。

   如果清除此核取方塊，在偵測到網路攻擊意圖時，"網路威脅防護"元件不會啟用對以後來自同一位址的網路攻擊的自動防護。
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**"關鍵威脅防護"**區域中選擇**"網路威脅防護"**。

   "網路威脅防護"元件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**"確定"**。
8. 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。

*要啟用或停用防火牆：*

1. 開啟程式設定視窗。
2. 在視窗左側的**"關鍵威脅防護"**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，請取消選取**"啟用防火牆"**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。

- **本機網路**。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“**關鍵威脅防護**”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“**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**。
   - **本機網路**。
   - **信任網路**。

6. 在"**防火牆**"視窗中點擊"**確定**"。

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**"關鍵威脅防護"**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"**標籤。
   此標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之一指定網路服務的名稱：

   - 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**、**本機網路**或**公用網路**。
    - **來自清單的位址**。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。
    - **來自清單的位址**。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"**標籤中。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**"確定"**。

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**"關鍵威脅防護"**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**"網路封包規則"**按鈕。
   **"防火牆"**視窗將開啟**"網路封包規則"**標籤。
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**"關鍵威脅防護"**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**"網路封包規則"**按鈕。
   **"防火牆"**視窗將開啟**"網路封包規則"**標籤。
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**"確定"**。

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**"關鍵威脅防護"**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**"網路封包規則"**按鈕。
   **"防火牆"**視窗將開啟**"網路封包規則"**標籤。
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。

像"主機入侵防禦"元件一樣，預設情況下，"防火牆"元件在篩選應用程式群組內所有應用程式的網路活動時將套用應用程式群組的網路規則。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"*開*"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"**關鍵威脅防護**"區域中，選取"**防火牆**"。
3. 點擊"**應用程式規則**"按鈕。

   在"**防火牆**"視窗開啟"**應用程式網路規則**"標籤。
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"**應用程式控制規則**"或"**應用程式群組控制規則**"視窗中選擇"**網路規則**"標籤。
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之一指定網路服務的名稱：
   - 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**、**本機網路**或**公用網路**。
    - **來自清單的位址**。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。
- **來自清單的位址**。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"**標籤中。
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**"應用程式控制規則"**視窗中的"確定"。
19. 在**"防火牆"**視窗中點擊**"確定"**。
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**"關鍵威脅防護"**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**"應用程式規則"**按鈕。
   在**"防火牆"**視窗開啟**"應用程式網路規則"**標籤。
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"**標籤。
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**"應用程式控制規則"**視窗中的"確定"。

10. 在**"防火牆"**視窗中點擊**"確定"**。

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**"關鍵威脅防護"**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**"應用程式規則"**按鈕。
   在**"防火牆"**視窗開啟**"應用程式網路規則"**標籤。

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**"關鍵威脅防護"**區域中，選取**"防火牆"**區域。
   在視窗右側，將顯示防火牆元件的設定。

3. 點擊**"應用程式規則"**按鈕。
   在**"防火牆"**視窗開啟**"應用程式網路規則"**標籤。

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"**標籤。

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**"應用程式控制規則"**視窗中的"確定"。

10. 在**"防火牆"**視窗中點擊**"確定"**。

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。

*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**"關鍵威脅防護"**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**"應用程式規則"**按鈕。
   在**"防火牆"**視窗開啟**"應用程式網路規則"**標籤。

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"**標籤。

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**"應用程式控制規則"**視窗中的"確定"。

10. 在**"防火牆"**視窗中點擊**"確定"**。

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. 點擊**"防護元件"**區域。
   將開啟**"防護元件"**視窗。

3. 點擊視窗下部的**"網路監控"**連結。
   開啟**"網路監控"**視窗。在該視窗中，將以四個標籤顯示電腦網路活動的相關資訊：

   - **"網路活動"**標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"**標籤列出電腦所有開啟的網路連接埠。
   - **"網路流量"**標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"**標籤列出"網路威脅防護"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。

# 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。如果未將卡巴斯基安全管理中心政策套用於安裝了 Kaspersky Endpoint Security 的電腦，您可以透過臨時暫停和還原電腦防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. 透過以下方式之一開啟**"控制台"**視窗：
   - 如果您正在使用 Windows 7，請在**"開始"**功能表中選取**"控制台"**。
   - 如果您正在使用 Windows 8 或 Windows 8.1，請按 **Win+I** 組合鍵並選擇**"控制台"**。
   - 如果您正在使用 Windows 10，請按 **Win+X** 組合鍵並選擇**"控制台"**。
2. 在**"控制台"**視窗中，選取**"應用程式和功能"**。
3. 在已安裝的應用程式清單中，選擇**"Kaspersky Endpoint Security for Windows"**。
4. 點擊**"修改/移除"**按鈕。
5. 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。
6. 在**"BadUSB 攻擊防護"**元件名稱旁邊圖示的內容功能表中的**"關鍵威脅防護"**元件群組中，選取**"功能將安裝在本機硬碟磁碟機上"**選項。
7. 點擊**"下一步"**按鈕。
8. 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**"關鍵威脅防護"**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**"關鍵威脅防護"**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：
   - 如果您希望封鎖使用螢幕鍵盤進行授權，請選中**"禁止使用螢幕鍵盤授權 USB 裝置"**核取方塊。
   - 如果您希望允許使用螢幕鍵盤進行授權，請清除**"禁止使用螢幕鍵盤授權 USB 裝置"**核取方塊。
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嘗試機會：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。

# 應用程式控制

本章節介紹應用程式控制的資訊，以及如何設定元件。

## 關於應用程式控制

應用程式控制元件使用*應用程式控制規則*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。

預設情況下，“應用程式控制”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）。

## 啟用和停用應用程式控制

儘管應用程式控制被預設停用，您仍可以根據需要啟用應用程式控制。

*要啟用或停用“應用程式控制”：*

1. 開啟程式設定視窗。
2. 在視窗左側的“**安全控制**”區域中，選取“**應用程式控制**”子區域。
   在視窗右側，顯示了“應用程式控制”元件的設定。
3. 請執行以下操作之一：
   - 如果您想要啟用“應用程式控制”，請選中“**啟用應用程式控制**”核取方塊。
   - 如果您想要停用“應用程式控制”，請清除“**啟用應用程式控制**”核取方塊。
4. 要儲存變更，請點擊“**儲存**”按鈕。

## 應用程式控制功能限制

在以下情況中“應用程式控制”元件的執行受到限制：

- 應用程式版本升級時，不支援匯入“應用程式控制”元件設定。
- 升級應用程式版本時，只有從 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 升級到 Kaspersky Endpoint Security 11 for Windows，才支援匯入“應用程式控制”設定。

> 升級除 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 以外的應用程式版本時，必須重新配置“應用程式控制”設定才能使此元件還原為執行狀態。

- 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。

  Kaspersky Endpoint Security 在連線到 KSN 伺服器時分配到 KL 類別"**根據 KSN 中的聲譽受受信任應用程式**"的應用程式清單與在未連線到 KSN 時分配到 KL 類別"**根據 KSN 中的聲譽受受信任應用程式**"的應用程式清單可能有所不同。

- 在卡巴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巴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"應用程式控制"規則允許解譯器的啟動，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：

  - %ComSpec%;
  - %SystemRoot%\\system32\\regedit.exe;
  - %SystemRoot%\\regedit.exe;
  - %SystemRoot%\\system32\\regedt32.exe;
  - %SystemRoot%\\system32\\cscript.exe;
  - %SystemRoot%\\system32\\wscript.exe;
  - %SystemRoot%\\system32\\msiexec.exe;
  - %SystemRoot%\\system32\\mshta.exe;
  - %SystemRoot%\\system32\\rundll32.exe;
  - %SystemRoot%\\system32\\wwahost.exe;
  - %SystemRoot%\\syswow64\\cmd.exe;
  - %SystemRoot%\\syswow64\\regedit.exe;
  - %SystemRoot%\\syswow64\\regedt32.exe;
  - %SystemRoot%\\syswow64\\cscript.exe;
  - %SystemRoot%\\syswow64\\wscript.exe;

- %SystemRoot%\\syswow64\\msiexec.exe;
- %SystemRoot%\\syswow64\\mshta.exe;
- %SystemRoot%\\syswow64\\rundll32.exe;
- %SystemRoot%\\syswow64\\wwahost.exe.

# 關於應用程式控制規則

Kaspersky Endpoint Security 根據規則按照使用者控制應用程式的啟動。應用程式控制規則指定觸發條件以及條件被觸發時"應用程式控制"元件指定的操作（使用者允許或封鎖應用程式啟動）。

## 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）
- 應用程式可執行檔的雜湊值 。
- 憑證：發佈者、主題、指紋。
- 應用程式是否屬於某 KL 類別。
- 卸除式磁碟上可執行檔的位置。

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，"應用程式控制"不會控制應用程式的啟動。

### 觸發規則後由"應用程式控制"元件作出決定。

觸發操作後，"應用程式控制"將允許使用者（或使用者群組）啟動應用程式或封鎖啟動。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

應用程式控制規則可為以下兩個狀態值之一：

- **開**。此狀態表示執行"應用程式控制"時使用該規則。
- **關**。此狀態表示"應用程式控制"啟用時略過此規則。
- **測試**。此狀態表示 Kaspersky Endpoint Security 允許啟動套用了規則的應用程式，但會在報告中記錄與啟動此類別應用程式有關的資訊。

## 管理應用程式控制規則

您可以為應用程式控制規則執行以下操作：

- 新增新規則
- 建立或變更觸發規則的條件
- 編輯規則狀態

可以啟用、停用應用程式控制規則或將其轉換到測試模式。預設情況下建立應用程式控制規則後將其啟用。

- 刪除規則

## 新增和編輯應用程式控制規則

*要新增或編輯應用程式控制規則：*

1. 開啟程式設定視窗。
2. 在視窗左側的**"安全控制"**區域中，選取**"應用程式控制"**子區域。
   在視窗右側，顯示了"應用程式控制"元件的設定。
3. 選擇**"啟用應用程式控制"**核取方塊以使元件設定可供編輯。
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。

   **"應用程式控制規則"**視窗將開啟。
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**"主體及其權限"**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“**主體及其權限**”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“**主體**”欄中沒有出現的使用者和不屬於“**主體**”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“**主體及其權限**”清單中指定的使用者以及不屬於“**主體及其權限**”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，並且希望允許它們建立將被允許隨後執行的其它可執行檔，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。

## 為應用程式控制規則新增觸發條件

*要為應用程式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“**安全控制**”區域中，選取“**應用程式控制**”子區域。

在視窗右側，顯示了“應用程式控制”元件的設定。

3. 選擇“**啟用應用程式控制**”核取方塊以使元件設定可供編輯。

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。

“**應用程式控制規則**”視窗將開啟。

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**”按鈕下的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“**根據特定資料夾的應用程式內容建立條件**”。

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擇標準：**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**”，請選中要在觸發規則條件中使用的可執行檔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**供應商**。

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**”，請選中要在規則觸發條件中使用的設定所對應的核取方塊：**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“**根據已執行過的應用程式內容建立條件**”。

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擇標準：**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。

3. 如果您在“**顯示標準**”下拉清單中選取“**檔案內容**”，請選中要在觸發規則條件中使用的可執行檔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**供應商**。

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**”，請選中要在規則觸發條件中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。由 Kaspersky Lab 專家維護的網頁位址清單。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，根據您要建立規則觸發條件選取 KL 類別名稱旁邊的核取方塊。

   您可以點擊 KL 類別名稱左側的 按鈕來有選擇地標記嵌套的 KL 類別。

3. 點擊**"確定"**。

*若要新增自訂的規則觸發條件：*

1. 在**"新增"**按鈕下的下拉清單中，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的路徑。

3. 根據您要建立的規則觸發條件選擇標準：**檔案雜湊值**、**憑證**、**檔案內容**或**檔案或資料夾路徑**。

   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。

   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"應用程式控制"規則。要執行此操作，請點擊**"解析符號連結"** 按鈕。

4. 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"**按鈕下的下拉清單中，選取**"檔案磁碟機條件"**。

2. 在**"檔案磁碟機條件"**視窗的**"磁碟機"**下拉清單中，選取在其中將應用程式啟動作為規則觸發條件的儲存裝置類型。

3. 點擊**"確定"**。

## 變更應用程式控制規則的狀態

*要變更應用程式控制規則的狀態：*

1. 開啟程式設定視窗。
2. 在視窗左側的“**安全控制**”區域中，選取“**應用程式控制**”子區域。
   在視窗右側，顯示了“應用程式控制”元件的設定。
3. 選擇“**啟用應用程式控制**”核取方塊以使元件設定可供編輯。
4. 在“**狀態**”列中，點擊左鍵顯示上下文功能表，並選擇以下選項之一：
   - **開**。此狀態表示執行“應用程式控制”時使用該規則。
   - **關**。此狀態表示“應用程式控制”啟用時略過此規則。
   - **測試**。此狀態表示 Kaspersky Endpoint Security 允許啟動套用了規則的應用程式，但會在報告中記錄與啟動此類別應用程式有關的資訊。

     如果在“**動作**”下拉清單中選擇“**封鎖**”選項，則可以使用“**測試**”狀態為部分規則指定等同於“**通知**”選項的動作。
5. 要儲存變更，請點擊“**儲存**”按鈕。

## 測試應用程式控制規則

要確保“應用程式控制”規則不會封鎖工作所需的應用程式，建議啟用“應用程式控制”規則的測試並在建立新規則後分析其執行。

分析應用程式控制規則的執行需要檢視報告給卡巴斯基安全管理中心的已發生的應用程式控制事件。如果對於電腦使用者工作所需的所有應用程式，測試模式都不會產生封鎖啟動事件，則說明建立了正確的規則。否則，建議您更新已建立的規則的設定，建立附加規則或刪除現有規則。

預設情況下已停用應用程式控制規則的測試模式。

*要啟用“應用程式控制”規則的測試或為“應用程式控制”選擇封鎖操作：*

1. 開啟程式設定視窗。
2. 在視窗左側的“**安全控制**”區域中，選取“**應用程式控制**”子區域。
   在視窗右側，顯示了“應用程式控制”元件的設定。
3. 選擇“**啟用應用程式控制**”核取方塊以使元件設定可供編輯。
4. 在“**應用程式控制模式**”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. 請執行以下操作之一：
   - 如果要為“應用程式控制”規則啟用測試模式，請在“**動作**”下拉清單中選擇“**通知**”選項。
   - 如果要為“應用程式控制”規則啟用封鎖模式，請在“**動作**”下拉清單中選擇“**封鎖**”選項。

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。

## 編輯應用程式控制訊息範本

使用者嘗試啟動被應用程式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**"安全控制"**區域中，選取**"應用程式控制"**子區域。

   在視窗右側，顯示了"應用程式控制"元件的設定。
3. 選擇**"啟用應用程式控制"**核取方塊以使元件設定可供編輯。
4. 點擊**"範本"**按鈕。

   開啟**"訊息範本"**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"**標籤。
   - 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**"傳送給管理員的訊息"**標籤。
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。

## 關於應用程式控制執行模式

"應用程式控制"模組有以下兩種執行模式：

- **黑名單**。在此模式下，"應用程式控制"允許所有使用者啟動所有應用程式，但在"應用程式控制"封鎖規則中指定的應用程式除外。

  預設情況下，應用程式控制啟用此模式。
- **白名單**。在此模式下，"應用程式控制"禁止所有使用者啟動任何應用程式，但在"應用程式控制"允許規則中指定的應用程式除外。

  如果完全設定"應用程式控制"的允許規則，此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。

  您可以閱讀針對在白名單模式下配置應用程式控制規則的建議。

每種模式都有兩種可對已啟動的符合"應用程式控制"規則的應用程式所採取的操作：Kaspersky Endpoint Security 可以封鎖應用程式啟動或者通知使用者應用程式啟動。

您可以同時使用 Kaspersky Endpoint Security 本機介面和卡巴斯基安全管理中心設定"應用程式控制"以使其在這些模式下操作。

但是，卡巴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。

  卡巴斯基安全管理中心管理主控台端建立的"應用程式控制"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巴斯基安全管理中心設定"應用程式控制"元件的執行。

## 選取應用程式控制模式

*要選取應用程式控制模式：*

1. 開啟程式設定視窗。
2. 在視窗左側的"**安全控制**"區域中，選取"**應用程式控制**"子區域。

   在視窗右側，顯示了"應用程式控制"元件的設定。
3. 選擇"**啟用應用程式控制**"核取方塊以使元件設定可供編輯。
4. 在"**應用程式控制模式**"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。

     最初為白名單模式定義的規則為"**黃金映像**"規則，它允許啟動的應用程式包含在"黃金映像"類別中，而"**信任的更新程式**"規則允許啟動"信任的更新程式"KL 類別中的應用程式。"黃金映像"KL 類別包含確保作業系統正常執行的程式。"信任的更新程式"KL類別包含最具信譽的軟體廠商的更新程式。您無法刪除這些規則。這些規則的設定無法編輯。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。要再次使用這些規則，您只需要在"**應用程式控制模式**"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 DDL 模組，則選取"**控制 DDL 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。

   Kaspersky Endpoint Security 僅監控自選中"**控制 DLL 和驅動程式**"核取方塊後載入的 DLL 模組和驅動程式。如果您希望 Kaspersky Endpoint Security 監控所有 DLL 模組和驅動程式（包括在 Kaspersky Endpoint Security 啟動之前載入的 DLL 模組和驅動程式），請在選中"**控制DLL 和驅動程式**"核取方塊後重新啟動電腦。

當啟用用於控制載入哪些 DLL 模組的功能時，請確保**"應用程式控制"**區域已啟用預設**黃金映像**規則或其他包含受信任憑證 KL 類別的規則，並確保在啟動 Kaspersky Endpoint Security 之前載入受信任的 DLL 模組和驅動程式。如果在停用**"黃金映像"**規則時啟用對載入 DLL 模組和驅動程式的控制，可能導致作業系統不穩定。

基於其他 KL 類別（受信任憑證 KL 類別除外）建立的應用程式控制規則不能用於 DLL 模組和驅動程式的啟動控制。

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不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控制規則

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

## 收集關於安裝在區域網路電腦上的應用程式資訊

要建立優化的應用程式控制規則，建議首先思考一下公司 LAN 中電腦上使用的應用程式。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、版本和中文化語言。
- 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"**資料夾中找到。**"應用程式登錄檔"**資料夾和**"可執行檔"**資料夾位於卡巴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"**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。

*要開啟**"應用程式登錄檔"**資料夾中的應用程式的內容視窗：*

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄的**"附加"**資料夾的**"應用程式管理"**資料夾中，選取**"應用程式登錄檔"**資料夾。

3. 選取應用程式。
4. 在應用程式的右鍵選單中，選取**"內容"**。
   **"內容：<應用程式名稱>"**視窗將開啟。

*要開啟**"可執行檔"**資料夾中的可執行檔的內容視窗：*

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄的**"附加"**資料夾的**"應用程式管理"**資料夾中，選取**"可執行檔"**資料夾。
3. 選取可執行檔。
4. 在可執行檔的右鍵選單中，選擇**"內容"**。
   **"內容：<可執行檔名稱>"**視窗將開啟。

## 收集關於在使用者電腦上啟動的應用程式的相關資訊

*要啟用將已安裝 Kaspersky Endpoint Security 的電腦上啟動的應用程式的相關資訊轉發到管理伺服器的功能：*

1. 開啟卡巴斯基安全管理中心管理主控台。
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"**標籤。
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**"一般設定"**區域中，選取**"報告和儲存"**子區域。
7. 在視窗右側部分的**"到管理伺服器的資料傳輸"**區域中點擊**"設定"**按鈕。
   **"通知"**視窗將開啟。
8. 選擇**"關於已啟動的應用程式"**核取方塊。
9. 在**"通知"**視窗中點擊**"確定"**。
10. 在**"內容：<政策名稱>"**視窗中點擊**"確定"**。

## 建立應用程式類別

您可以建立應用程式類別，以便建立應用程式控制規則。

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. 開啟卡巴斯基安全管理中心管理主控台。
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。

## 步驟 1. 選擇類別類型

在此步驟中，選擇以下應用程式類別之一：

- **包含手動新增內容的類別**。如果選擇此類型的類別，您可以在"配置將應用程式包括在類別中的條件"步驟和"配置將應用程式從類別中排除的條件"步驟中定義將可執行檔包括到已建立類別中所依據的標準。
- **包含選定裝置的可執行檔的類別**。如果選擇此類型的類別，您可以在"設定"步驟中指定必須包括在此類別中的可執行檔所屬的裝置。
- **包含自動新增內容的類別**。如果選擇此類型的類別，您可以在"儲存庫資料夾"步驟中指定將自動包括在已建立的類別中的可執行檔所來自的資料夾。

  建立包含自動新增內容的類別時，卡巴斯基安全管理中心對以下格式的檔案執行清查：EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX 和 SCR。

## 步驟 2. 輸入使用者類別名稱

在此步驟中，為應用程式類別指定一個名稱。

要繼續安裝精靈，請點擊"**下一步**"按鈕。

## 步驟 3. 配置將應用程式包括在類別中的條件

如果您選擇"**包含手動新增內容的類別**"類別類型，此步驟可用。

在此步驟中，在"**新增**"下拉清單中選擇以下一個或多個用於將應用程式包括到類別中的條件：

- **從可執行檔清單**。將用戶端裝置上的可執行檔清單中的應用程式新增到自訂類別。
- **透過檔案內容**。指定可執行檔的詳細資料，作為將應用程式新增到自訂類別的條件。

- **資料夾內檔案的中繼資料**。選擇用戶端裝置上包含可執行檔的資料夾。卡巴斯基安全管理中心會將這些可執行檔的中繼資料作為將應用程式新增到自訂類別的條件。
- **資料夾內檔案的雜湊值**。選擇用戶端裝置上包含可執行檔的資料夾。卡巴斯基安全管理中心會將這些可執行檔的雜湊值作為將應用程式新增到自訂類別的條件。
- **資料夾內檔案的憑證**。選擇用戶端裝置上包含帶憑證簽章的可執行檔的資料夾。卡巴斯基安全管理中心會將這些可執行檔的憑證作為將應用程式新增到自訂類別的條件。

  不建議使用其內容中未指定**憑證指紋**參數的條件。

- **MSI 安裝檔案中繼資料**。選擇 MSI 安裝套件。卡巴斯基安全管理中心會將 MSI 安裝套件內封裝的可執行檔的中繼資料作為將應用程式新增到自訂類別的條件。
- **應用程式的 MSI 安裝程式的檔案校驗和**。選擇 MSI 格式的安裝套件。卡巴斯基安全管理中心會將此安裝套件內封裝的可執行檔的雜湊值作為將應用程式新增到自訂類別的條件。
- **KL 類別**。指定 KL 類別作為將應用程式新增到自訂類別的條件。

  KL 類別是具有相同主旨內容的應用程式清單。由 Kaspersky Lab 專家維護的網頁位址清單。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。

  您可以選擇所有 KL 類別來生成受信任應用程式的延伸清單。
- **應用程式資料夾**。選擇用戶端裝置上的資料夾。卡巴斯基安全管理中心會將此資料夾下的可執行檔新增到自訂類別。
- **憑證儲存庫內的憑證**。選擇憑證儲存庫內的憑證作為將應用程式新增到自訂類別的條件。

  不建議使用其內容中未指定**憑證指紋**參數的條件。

- **磁碟機類型**。指定儲存裝置類型（所有硬碟磁碟機和卸除式磁碟機，或者僅限卸除式磁碟機）作為將應用程式新增到自訂類別的條件。

要繼續安裝精靈，請點擊“**下一步**”按鈕。

## 步驟 4. 配置將應用程式從類別中排除的條件

如果您選擇“**包含手動新增內容的類別**”類別類型，此步驟可用。

在此步驟指定的應用程式將從類別中排除，即使在“配置將應用程式包括在類別中的條件”步驟指定了這些應用程式。

在此步驟中，在“**新增**”下拉清單中選擇以下用於將應用程式從類別中排除的條件之一：

- **從可執行檔清單**。將用戶端裝置上的可執行檔清單中的應用程式新增到自訂類別。
- **透過檔案內容**。指定可執行檔的詳細資料，作為將應用程式新增到自訂類別的條件。

- **資料夾內檔案的中繼資料**。選擇用戶端裝置上包含可執行檔的資料夾。卡巴斯基安全管理中心會將這些可執行檔的中繼資料作為將應用程式新增到自訂類別的條件。

- **資料夾內檔案的雜湊值**。選擇用戶端裝置上包含可執行檔的資料夾。卡巴斯基安全管理中心會將這些可執行檔的雜湊值作為將應用程式新增到自訂類別的條件。

- **資料夾內檔案的憑證**。選擇用戶端裝置上包含帶憑證簽章的可執行檔的資料夾。卡巴斯基安全管理中心會將這些可執行檔的憑證作為將應用程式新增到自訂類別的條件。

- **MSI 安裝檔案中繼資料**。選擇 MSI 安裝套件。卡巴斯基安全管理中心會將 MSI 安裝套件內封裝的可執行檔的中繼資料作為將應用程式新增到自訂類別的條件。

- **應用程式的 MSI 安裝程式的檔案校驗和**。選擇 MSI 格式的安裝套件。卡巴斯基安全管理中心會將此安裝套件內封裝的可執行檔的雜湊值作為將應用程式新增到自訂類別的條件。

- **KL 類別**。指定 KL 類別作為將應用程式新增到自訂類別的條件。

  KL 類別是具有相同主旨內容的應用程式清單。由 Kaspersky Lab 專家維護的網頁位址清單。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。

  您可以選擇所有 KL 類別來生成受信任應用程式的延伸清單。

- **應用程式資料夾**。選擇用戶端裝置上的資料夾。卡巴斯基安全管理中心會將該資料夾內的可執行檔新增到自訂應用程式類別。

- **憑證儲存庫內的憑證**。選擇憑證儲存庫內的憑證作為將應用程式新增到自訂類別的條件。

- **磁碟機類型**。指定儲存裝置類型（所有硬碟磁碟機和卸除式磁碟機，或者僅限卸除式磁碟機）作為將應用程式新增到自訂類別的條件。

要繼續安裝精靈，請點擊“**下一步**”按鈕。

## 步驟 5. 設定

如果您選取**包含選定裝置的可執行檔的類別**類別類型，此步驟可用。

在此步驟中，點擊“**新增**”按鈕，指定將由卡巴斯基安全管理中心新增到該應用程式類別的可執行檔所屬的電腦。“**可執行檔**”資料夾中指定電腦的所有可執行檔都將由卡巴斯基安全管理中心新增到此應用程式類別。

在此步驟還可以配置以下設定：

- 卡巴斯基安全管理中心雜湊函數計算的演算法。要選擇演算法，您必須選中以下至少一個核取方塊：

  - “**為此類別下的檔案計算 SHA-256（Kaspersky Endpoint Security 10 Service Pack 2 for Windows 及更高版本支援）**”核取方塊。

  - “**為此類別下的檔案計算 MD5（低於 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 的版本支援）**”核取方塊。

- “**與管理伺服器儲存區同步資料**”核取方塊。如果您希望卡巴斯基安全管理中心定期清除應用程式類別並將“**可執行檔**”資料夾中指定電腦的所有可執行檔新增到該類別，請選取該核取方塊。

  如果清除“**與管理伺服器儲存庫同步資料**”核取方塊，卡巴斯基安全管理中心在建立應用程式類別之後將不會對其進行任何修改。

- "**掃描週期（小時）**"欄位。在這一欄位中，您可以指定卡巴斯基安全管理中心定期清除應用程式類別並將"**可執行檔**"資料夾中指定電腦的所有可執行檔新增到該類別的時間間隔（小時）。

  如果選取"**與管理伺服器儲存區同步資料**"核取方塊，此欄位可用。

要繼續安裝精靈，請點擊"**下一步**"按鈕。

## 步驟 6. 儲存庫資料夾

如果您選擇"**包含自動新增內容的類別**"類別類型，此步驟可用。

在此步驟中，點擊"**瀏覽**"按鈕，指定卡巴斯基安全管理中心將在其中搜尋可執行檔的資料夾，以便自動將應用程式新增到該應用程式類別。

在此步驟還可以配置以下設定：

- "**在此類別中包含動態連結程式庫 (DLL)**"核取方塊。如果您希望應用程式類別包含動態連結程式庫（DLL 格式的檔案），並且應用程式控制元件記錄系統中執行的此類程式庫的行為，請選擇此核取方塊。

  在應用程式類別中包含 DLL 檔案可能降低卡巴斯基安全管理中心的效能。

- "**在此類別中包含指令碼資料**"核取方塊。如果您希望應用程式類別包含指令碼資料，並且防止指令碼被"Web 威脅防護"元件封鎖，請選擇此核取方塊。

  在應用程式類別中包含指令碼資料可能降低卡巴斯基安全管理中心的效能。

- 卡巴斯基安全管理中心雜湊函數計算的演算法。要選擇演算法，您必須選中以下至少一個核取方塊：

  - "**為此類別下的檔案計算 SHA-256（Kaspersky Endpoint Security 10 Service Pack 2 for Windows 及更高版本支援）**"核取方塊。

  - "**為此類別下的檔案計算 MD5（低於 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 的版本支援）**"核取方塊。

- "**強制掃描資料夾變更**"核取方塊。如果您希望卡巴斯基安全管理中心在用於自動新增到應用程式類別的資料夾中定期搜尋可執行檔，請選擇此核取方塊。

  如果清除"**強制掃描資料夾變更**"核取方塊，卡巴斯基安全管理中心僅在用於自動新增到應用程式類別的資料夾有變更、該資料夾內新增或刪除了檔案時才在該資料夾中搜尋可執行檔。

- "**掃描週期（小時）**"欄位。在此欄位中，您可以指定卡巴斯基安全管理中心在用於自動新增到應用程式類別的資料夾中搜尋可執行檔的時間間隔（以小時為單位）。

  如果選取了"**強制掃描資料夾變更**"核取方塊，該欄位可用。

要繼續安裝精靈，請點擊"**下一步**"按鈕。

## 步驟 7. 建立自訂類別

要結束"應用程式安裝精靈"，請點擊"**完成**"按鈕。

## 將“可執行檔”資料夾中的可執行檔新增到應用程式類別。

*要將“**可執行檔**”資料夾中的可執行檔新增到應用程式類別：*

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄的“**附加**”資料夾的“**應用程式管理**”資料夾中，選取“**可執行檔**”資料夾。
3. 在工作區中，選擇要新增到應用程式類別的可執行檔。
4. 右鍵點擊以開啟選定可執行檔的右鍵選單，然後選取“**新增到類別**”。
   “**選取使用者類別**”視窗將開啟。
5. 在“**選取使用者類別**”視窗中：
   - 在視窗上部，選擇下列選項之一：
     - **建立應用程式類別**。如果您要建立新的應用程式類別並向其中新增可執行檔，則選擇此選項。
     - **將規則新增至指定分類**。如果您要選取現有應用程式類別並向其中新增可執行檔，則選擇此選項。
   - 在“**規則類型**”區域中，選取以下選項之一：
     - **新增包含規則**。如果您要建立將可執行檔新增到應用程式類別的條件，則選擇此選項。
     - **新增排除規則**。如果您要建立將可執行檔從應用程式類別排除的條件，則選擇此選項。
   - 在“**檔案資訊類型**”區域中，選取以下選項之一：
     - **憑證資料或沒有憑證的檔案的 SHA-256**。
     - **憑證資料（沒有憑證的檔案將被略過）**。
     - **僅 SHA-256（沒有 SHA-256 的檔案將被略過）**。
     - **MD5（停止使用的模式，僅針對 Kaspersky Endpoint Security 10 Service Pack 1 版本）**。
6. 點擊“**確定**”。

## 使用卡巴斯基安全管理中心新增和修改應用程式控制規則

*要使用卡巴斯基安全管理中心新增或修改應用程式控制規則：*

1. 開啟卡巴斯基安全管理中心管理主控台。
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**”標籤。
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“**安全控制**”區域中，選取“**應用程式控制**”。
   在視窗右側，顯示了“應用程式控制”元件的設定。

7. 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。

   “**應用程式控制規則**”視窗將開啟。

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. 在“**主體及其權限**”表中點擊“**新增**”按鈕。
   標準 Microsoft Windows“**選擇使用者或群組**”視窗開啟。

10. 在“**選擇使用者或群組**”視窗中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。

11. 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，則選取相關行中的“**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，則選取相關行中的“**封鎖**”核取方塊。

12. 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“**主體**”欄中沒有出現的使用者和不屬於“**主體**”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。

13. 如果您希望 Kaspersky Endpoint Security 將選定應用程式類別中包括的應用程式視為受信任的更新程式，並且希望允許它們建立將被允許隨後執行的其它可執行檔，請選取“**信任的更新程式**”核取方塊。

14. 點擊“**確定**”。

15. 在政策內容視窗的“**應用程式控制**”區域中，點擊“**套用**”按鈕。

## 透過卡巴斯基安全管理中心變更應用程式控制規則的狀態

*要變更應用程式控制規則的狀態：*

1. 開啟卡巴斯基安全管理中心管理主控台。

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**”標籤。

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“**安全控制**”區域中，選取“**應用程式控制**”。
   在視窗右側，顯示了“應用程式控制”元件的設定。

7. 在“**狀態**”列中，點擊左鍵顯示上下文功能表，並選擇以下選項之一：

   - **開**。此狀態表示執行“應用程式控制”時使用該規則。
   - **關**。此狀態表示“應用程式控制”啟用時略過此規則。
   - **測試**。此狀態表示 Kaspersky Endpoint Security 總是允許啟動套用了規則的應用程式，但會在報告中記錄與啟動此類別應用程式有關的資訊。

   > 如果在“**動作**”下拉清單中選擇“**封鎖**”選項，則可以使用“**測試**”狀態為部分規則指定等同於“**通知**”選項的動作。

8. 點擊 **套用** 按鈕。

## 使用卡巴斯基安全管理中心測試應用程式控制規則

要確保“應用程式控制”規則不會封鎖工作所需的應用程式，建議啟用“應用程式控制”規則的測試並在建立新規則後分析其執行。啟用“應用程式控制”規則的測試後，Kaspersky Endpoint Security 不會封鎖被“應用程式控制”封鎖啟動的應用程式，但是會將有關它們啟動的通知傳送給管理伺服器。

分析應用程式控制規則的執行需要檢視報告給卡巴斯基安全管理中心的已發生的應用程式控制事件。如果對於電腦使用者工作所需的所有應用程式，測試模式都不會產生封鎖啟動事件，則說明建立了正確的規則。 否則，建議您更新已建立的規則的設定，建立附加規則或刪除現有規則。

預設情況下已停用“應用程式控制”規則的封鎖模式。

*要在卡巴斯基安全管理中心中啟用“應用程式控制”規則的測試或為“應用程式控制”選擇封鎖操作：*

1. 開啟卡巴斯基安全管理中心管理主控台。
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**”標籤。
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“**安全控制**”區域中，選取“**應用程式控制**”。

在視窗右側，顯示了“應用程式控制”元件的設定。

7. 在“**應用程式控制模式**”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。
8. 請執行以下操作之一：
   - 如果要為“應用程式控制”規則啟用測試模式，請在“**動作**”下拉清單中選擇“**通知**”選項。
   - 如果要為“應用程式控制”規則啟用封鎖模式，請在“**動作**”下拉清單中選擇“**封鎖**”選項。
9. 要儲存變更，請點擊“**儲存**”按鈕。

## 檢視“應用程式控制”元件的測試執行所產生的事件

*要檢視卡巴斯基安全管理中心在測試模式下收到的應用程式控制事件：*

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄的“**管理伺服器**”中選取“**事件**”標籤。
3. 點擊“**建立集合**”按鈕。
   “**內容：<集合名稱>**”視窗將開啟。
4. 開啟“**事件**”區域。
5. 點擊“**清除所有**”按鈕。
6. 在“**事件**”表中選擇“**禁止應用程式在測試模式下啟動**”以及“**允許應用程式在測試模式下啟動**”核取方塊。
7. 點擊“**確定**”。
8. 在“**集合事件**”下拉清單中選擇建立的集合。
9. 點擊“**執行集合**”按鈕。

## 檢視“應用程式控制”元件的執行所產生的事件

*要檢視卡巴斯基安全管理中心收到的由“應用程式控制”元件的執行所產生的事件：*

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄的“**管理伺服器**”中選取“**事件**”標籤。
3. 點擊“**建立集合**”按鈕。
   “**內容：<集合名稱>**”視窗將開啟。

4. 開啟**"事件"**區域。

5. 點擊**"清除所有"**按鈕。

6. 在**"事件"**表中選擇**"封鎖應用程式啟動"**核取方塊。

7. 點擊**"確定"**。

8. 在**"集合事件"**下拉清單中選擇建立的集合。

9. 點擊**"執行集合"**按鈕。

## 將事件相關的可執行檔新增到應用程式類別

*要將與產生的應用程式控制事件關聯的可執行檔新增到應用程式類別：*

1. 開啟卡巴斯基安全管理中心管理主控台。

2. 在管理主控台樹狀目錄的**"管理伺服器"**中選取**"事件"**標籤。

3. 在**"集合事件"**下拉清單中選擇與"應用程式控制"元件執行相關的事件集合（檢視"應用程式控制"元件的執行所產生的事件，檢視"應用程式控制"元件的測試執行所產生的事件）。

4. 點擊**"執行集合"**按鈕。

5. 選擇您要將其相關可執行檔新增到應用程式類別的事件。

6. 右鍵點擊以開啟選定事件的右鍵選單，然後選取**"新增到類別"**。
   **"選取使用者類別"**視窗將開啟。

7. 在**"選取使用者類別"**視窗中：

   - 在視窗上部，選擇下列選項之一：

     - **建立應用程式類別**。如果您要建立新的應用程式類別並向其中新增可執行檔，則選擇此選項。

     - **將規則新增至指定分類**。如果您要選取現有應用程式類別並向其中新增可執行檔，則選擇此選項。

   - 在**"規則類型"**區域中，選取以下選項之一：

     - **新增包含規則**。如果您要建立將可執行檔新增到應用程式類別的條件，則選擇此選項。

     - **新增排除規則**。如果您要建立將可執行檔從應用程式類別排除的條件，則選擇此選項。

   - 在**"檔案資訊類型"**區域中，選取以下選項之一：

     - **憑證資料或沒有憑證的檔案的 SHA-256**。

     - **憑證資料（沒有憑證的檔案將被略過）**。

     - **僅 SHA-256（沒有 SHA-256 的檔案將被略過）**。

     - **MD5（停止使用的模式，僅針對 Kaspersky Endpoint Security 10 Service Pack 1 版本）**。

8. 點擊**"確定"**。

## 檢視測試封鎖執行的報告

*要檢視測試封鎖執行的報告：*

1. 開啟卡巴斯基安全管理中心管理主控台。
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**"選擇報告範本類型"**步驟中，選擇**"其他"**→**"測試封鎖執行的報告"**。
   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. 使用以下方法之一執行在先前說明步驟中建立的報告生成過程：
   - 在報告的右鍵選單中選取**"顯示報告"**。
   - 點擊位於管理主控台工作區右側的**"顯示報告"**連結。
   - 點擊報告將其開啟。

   此報告將顯示在新視窗中。

   報告建立過程將開始。此報告將顯示在新視窗中。

## 檢視被封鎖執行的報告

*要檢視被封鎖執行的報告：*

1. 開啟卡巴斯基安全管理中心管理主控台。
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**"選擇報告範本類型"**步驟中，選擇**"其他"**→**"被封鎖執行的報告"**。
   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. 使用以下方法之一執行在先前說明步驟中建立的報告生成過程：
   - 在報告的右鍵選單中選取**"顯示報告"**。
   - 點擊位於管理主控台工作區右側的**"顯示報告"**連結。
   - 點擊報告將其開啟。

此報告將顯示在新視窗中。

## 實施白名單模式的最佳實踐

本節包含針對實施白名單模式的建議。

## 排程實施白名單模式

排程實施白名單模式時，建議執行以下操作：

1. 形成以下類型的群組：
   - 使用者群組。需要設定為允許使用各種應用程式集的使用者群組。
   - 管理群組。卡巴斯基安全管理中心將白名單模式套用於的一個或多個電腦群組。如果要對電腦群組設定不同的白名單模式，則需要建立多個電腦群組。
2. 建立必須允許啟動的應用程式清單。

   在建立清單前，建議執行以下操作：

   1. 執行清查工作。

      清查工作的建立、重新配置和啟動的相關資訊可在"工作管理"區域檢視。

   2. 啟用向管理伺服器轉發電腦上啟動的應用程式的相關資訊。
   3. 檢視可執行檔清單。

## 設定白名單模式

設定白名單模式時，建議執行以下操作：

1. 建立包含必須允許啟動的應用程式的應用程式類別。

   您可以選擇以下用於建立應用程式類別的方法之一：

   - **包含手動新增內容的類別（步驟 3. 配置將應用程式包括在類別中的條件，步驟 4. 配置將應用程式從類別中排除的條件）**。您可以透過使用以下條件手動新增到此類別：
     - 檔案中繼資料。如果使用此條件，卡巴斯基安全管理中心會將所有附帶指定檔案內容的可執行檔新增到此應用程式類別。
     - 檔案雜湊碼。如果使用此條件，卡巴斯基安全管理中心會將所有具有指定雜湊值的可執行檔新增到該應用程式類別。

       使用此條件將排除自動安裝更新的功能，因為不同版本的檔案雜湊值也不同。

- 檔案憑證。如果使用此條件，卡巴斯基安全管理中心會將所有具有指定憑證簽章的可執行檔新增到此應用程式類別。
- KL 類別。如果使用此條件，卡巴斯基安全管理中心會將所有屬於指定 KL 類別的應用程式新增到此應用程式類別。
- 應用程式資料夾。如果使用此條件，卡巴斯基安全管理中心會將此資料夾中的所有可執行檔新增到該應用程式類別。

使用"應用程式資料夾"條件可能不安全，因為指定資料夾中的任何應用程式都將被允許啟動。建議只將使用具有"應用程式資料夾"條件的應用程式類別的規則套用於那些必須允許為其自動安裝更新的使用者。

您也可以將**可執行檔**資料夾中的可執行檔新增到包含手動新增內容的應用程式類別。

- **包含自動新增內容的類別**。您可以指定將自動分配到已建立的應用程式類別的可執行檔所來自的資料夾。
- **包含選定裝置的可執行檔的類別**。您可以指定其所有可執行檔都將自動分配到已建立的應用程式類別的電腦。

使用這種方法建立應用程式類別時，卡巴斯基安全管理中心透過可執行檔清單接收電腦上的應用程式的相關資訊。

2. 為"應用程式控制"元件選擇白名單模式。
3. 使用已建立的應用程式類別建立應用程式控制規則。

最初為白名單模式定義的規則為"黃金映像"規則，它允許啟動"黃金映像"KL 類別中包含的應用程式，而"信任的更新程式"規則允許啟動"信任的更新程式"KL 類別中包含的應用程式。"黃金映像"KL 類別包含確保作業系統正常執行的程式。"信任的更新程式"KL類別包含最具信譽的軟體廠商的更新程式。您無法刪除這些規則。這些規則的設定無法編輯。預設情況下，啟用"黃金映像"規則，停用"信任的更新程式"規則。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。

4. 確定必須允許為其自動安裝更新的應用程式。

   您可以透過以下任意一種方式允許自動安裝更新：

   - 透過允許屬於任何 KL 類別的所有應用程式啟動來指定允許的應用程式的延伸清單。
   - 透過允許有憑證簽章的所有應用程式啟動來指定允許的應用程式的延伸清單。

     要允許有憑證簽章的所有應用程式啟動，您可以建立一個包含基於憑證的條件的類別，此條件只使用值為"*"的"**主旨**"參數。
   - 對於應用程式控制規則，選擇"**信任的更新程式**"參數。如果選中此核取方塊，Kaspersky Endpoint Security 會將屬於在應用程式類別規則中指定的類別的應用程式視為信任的更新程式。Kaspersky Endpoint Security 允許由類別規則中指定的應用程式所安裝或更新的應用程式啟動（如果沒有封鎖規則套用於它們）。
   - 根據"應用程式資料夾"條件使用應用程式類別建立允許規則。使用此方法時，指定資料夾內的所有可執行檔都將新增到此應用程式類別。

使用“應用程式資料夾”條件可能不安全，因為指定資料夾中的任何應用程式都將被允許啟動。建議只將使用具有“應用程式資料夾”條件的應用程式類別的規則套用於那些必須允許為其自動安裝更新的使用者。

## 測試白名單模式

要確保“應用程式控制”規則不會封鎖工作所需的應用程式，建議啟用“應用程式控制”規則的測試並在建立新規則後分析其執行。啟用測試模式後，Kaspersky Endpoint Security 不會封鎖被應用程式控制規則封鎖啟動的應用程式，但是會將有關它們啟動的通知傳送給管理伺服器。

測試白名單模式時，建議執行以下操作：

1. 確定測試週期（從幾天到兩個月）。
2. 啟用“應用程式控制”規則的測試。
3. 檢查“應用程式控制”的執行測試所產生的事件和測試封鎖執行的報告來分析測試結果。
4. 根據分析結果，變更白名單模式設定。

   尤其是，根據測試結果，您可以將與“應用程式控制”元件的事件相關的可執行檔新增到包含手動新增內容的類別。

## 支援白名單模式

為“應用程式控制”選擇封鎖操作後，建議執行以下操作以繼續支援白名單模式：

- 檢查“應用程式控制”的執行所產生的事件和封鎖執行的報告來分析“應用程式控制”的效果。
- 分析使用者的應用程式存取請求。
- 在卡巴斯基安全網路或 Kaspersky Whitelist 網站中檢查陌生可執行檔的信譽來分析這些檔案。
- 在安裝作業系統或軟體的更新前，請在電腦測試群組中安裝這些更新，以檢查“應用程式控制”規則將如何處理它們。
- 將必要的應用程式新增到“應用程式控制”規則中使用的類別。

# 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。

*要啟用或停用裝置控制：*

1. 開啟程式設定視窗。
2. 在視窗左側的“**安全控制**”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的清單中。 | 沒有存取規則。 | 封鎖存取。 | 封鎖存取。 |

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**"安全控制"**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"**標籤。
   **"裝置類型"**標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**"配置裝置存取規則"**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**"移除"**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**"移除"**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**"安全控制"**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"**標籤。

   **"裝置類型"**標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"**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"**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日誌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。

您可以在卡巴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**"安全控制"**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"**標籤。

   **"裝置類型"**標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**"封鎖但帶有例外"**選項。

6. 在裝置清單中，選取**"Wi-Fi"**並點擊**"編輯"**按鈕。

   這會開啟**"受信任的 Wi-Fi 網路"**視窗。

7. 點擊**"新增"**按鈕。

這會開啟**"受信任的 Wi-Fi 網路"**視窗。

8. 在**"受信任的 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**"註解"**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定為受信任。

9. 在**"受信任的 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"**。

## 編輯連接匯流排存取規則

*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**"安全控制"**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"**標籤。
   **"連接介面"**標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“**安全控制**”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**”標籤。
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**”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**”標籤，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**”標籤。
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**"安全控制"**區域中，選取**"裝置控制"**。
7. 在視窗右側，選擇**"信任的裝置"**標籤。
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**"透過裝置 ID"**按鈕。
   - 選取**"透過裝置型號"**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"**欄位中。
15. 點擊**"確定"**。
    **"信任的裝置"**標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"**標籤。

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“**安全控制**”區域中，選取“**裝置控制**”。

7. 在視窗右側，選擇“**信任的裝置**”標籤。

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**”。

   “**依據 ID 遮罩新增受信任裝置**”視窗將開啟。

10. 在“**依據 ID 遮罩新增受信任裝置**”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**”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**”標籤中，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“**安全控制**”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**”標籤。

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。

"**設定受信任裝置存取規則**"視窗將開啟。

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"**設定受信任裝置存取規則**"視窗的"**允許使用者和/或使用者群組**"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

*若要從信任的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"**安全控制**"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**"標籤。

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。

## 匯入信任的裝置的清單

*要匯入信任的裝置的清單：*

1. 開啟程式設定視窗。

2. 在視窗左側的"**安全控制**"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**"標籤。

4. 點擊"**匯入**"按鈕。

   將開啟"**請選取設定檔**"視窗。

5. 在**"請選取設定檔"**視窗中，選擇您要從中匯入受信任裝置清單的 XML 檔，然後點擊**"開啟"**按鈕。

   如果受信任裝置清單包含一些項目，您將看到一個標題為**"該清單已經包含一些元素"**的視窗。在此視窗中，您可以執行以下操作之一：

   - 如果您要將匯入的項目新增到現有項目中，則點擊**"是"**。
   - 如果您要在新增匯入的項目之前刪除現有項目，則點擊**"否"**。

6. 要儲存變更，請點擊**"儲存"**按鈕。

## 匯出信任的裝置的清單

*要匯出信任的裝置的清單：*

1. 開啟程式設定視窗。
2. 在視窗左側的**"安全控制"**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"**標籤。
4. 選擇您想要匯出的清單項目。
5. 點擊**"匯出"**按鈕。

   將開啟**"請選取設定檔"**視窗。

6. 在**"請選取設定檔"**視窗中，指定您要將受信任裝置清單匯出到的 XML 檔的名稱，選擇要儲存此檔案的資料夾，然後點擊**"儲存"**按鈕。

## 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**"安全控制"**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**"訊息範本"**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"**標籤。
- 要修改傳送給區域網路管理員的回報訊息的範本，請選取**"傳送給管理員的訊息"**標籤。

5. 編輯資訊範本。您還可以使用下列按鈕：**變數**、**預設**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。

## 橋接防護

本節包含有關橋接防護的資訊和如何配置此功能的說明。

## 關於橋接防護

橋接防護提供針對橋接器的防護，防止安裝有 Kaspersky Endpoint Security 的電腦同時建立多個網路連線。

## 啟用和停用橋接防護

預設情況下停用橋接防護。如有必要，您可以啟用此功能。

*要啟用或停用橋接防護：*

1. 開啟程式設定視窗。
2. 在視窗左側的**"安全控制"**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. 點擊**"橋接防護"**按鈕。
   將開啟**"橋接防護"**視窗。
4. 請執行以下操作之一：
   - 選中**"啟用橋接防護"**核取方塊可啟用對網路橋接的防護。
     啟用橋接防護後，Kaspersky Endpoint Security 會按照連線規則封鎖已建立的連線。
   - 清除**"啟用橋接防護"**核取方塊可停用對網路橋接的防護。
5. 在**"橋接防護"**視窗中點擊**"確定"**。
6. 要儲存變更，請點擊**"儲存"**按鈕。

## 關於連線規則

已針對以下預定義的裝置類型建立連線規則：

- 網路介面卡
- Wi-Fi 介面卡
- 數據機

如果啟用連線規則，Kaspersky Endpoint Security 將：

- 在建立新連線時封鎖活動連線（如果規則中指定的裝置類型同時用於這兩個連線）。
- 封鎖透過使用了較低優先順序規則的裝置類型建立的連線。

## 變更連線規則的狀態

*要變更連線規則的狀態：*

1. 開啟程式設定視窗。
2. 在視窗左側的**"安全控制"**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. 點擊**"橋接防護"**按鈕。
   將開啟**"橋接防護"**視窗。
4. 選取您想要編輯其狀態的規則。
5. 在**"控制"**列中，點擊左鍵以彈出上下文功能表，然後執行以下操作之一：
   - 如果要啟用規則，請選取**"開啟"**。
   - 如果要停用規則，請選取**"關閉"**。
6. 在**"橋接防護"**視窗中點擊**"確定"**。
7. 要儲存變更，請點擊**"儲存"**按鈕。

## 變更連線規則的優先順序

*要變更連線規則的優先順序：*

1. 開啟程式設定視窗。
2. 在視窗左側的**"安全控制"**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. 點擊**"橋接防護"**按鈕。
   將開啟**"橋接防護"**視窗。

4. 選取您想要變更其優先順序的規則。

5. 請執行以下操作之一：

   - 點擊**"上移"**按鈕可以使規則在規則清單中上移一級。
   - 點擊**"下移"**按鈕可以使規則在規則清單中下移一級。

規則在規則清單中的位置越高，其優先順序越高。除了透過使用最高級規則的裝置類型所建立的連線外，橋接防護將封鎖所有連線。

1. 在**"橋接防護"**視窗中點擊**"確定"**。

2. 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。

僅當卡巴斯基安全管理中心政策已套用於裝置，並且在政策設定中啟用了相應的功能後，Kaspersky Endpoint Security 的授權暫時存取裝置的權限的功能才可用（有關詳細資訊，請參閱《卡巴斯基安全管理中心說明手冊》）。

*要請求存取被封鎖裝置的權限：*

1. 開啟程式設定視窗。

2. 在視窗左側的**"安全控制"**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**"請求存取"**按鈕。
   開啟**"請求存取裝置"**視窗。

4. 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。

5. 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。

6. 在**"存取持續時間"**欄位中，指定您想要存取裝置的時長。

7. 點擊**儲存** 按鈕。
   Microsoft Windows 的標準**"儲存請求存取檔案"**視窗將開啟。

8. 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。

9. 將該裝置請求存取檔案傳送給區域網路管理員。

10. 接收來自區域網路管理員的裝置存取金鑰檔案。

11. 在**"請求存取裝置"**視窗中，點擊**"啟動存取金鑰"**按鈕。

Microsoft Windows 的標準**"開啟存取金鑰"**視窗將開啟。

12. 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"**。

    **"啟動裝置的存取金鑰"**視窗將開啟，並且顯示關於所提供的存取權限的資訊。

13. 在**"啟動裝置的存取金鑰"**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**"請求存取裝置"**視窗中，點擊**"啟動存取金鑰"**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"**。

   **"啟動裝置的存取金鑰"**視窗將開啟，並且顯示關於所提供的存取權限的資訊。

9. 在**"啟動裝置的存取金鑰"**視窗中，點擊**"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"**標籤。

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**"授予離線模式下的存取權限"**。
   開啟**"授予離線模式下的存取權限"**視窗。

6. 選取**"裝置控制"**標籤。

7. 在**"裝置控制"**標籤上點選**"瀏覽"**按鈕。
   Microsoft Windows 的標準**"選擇請求存取檔案"**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。

# Web 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 Web 控制

使用 Web 控制可以透過限制或封鎖存取網頁資源來控制區域網路使用者的操作。

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。

Web 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指定網頁資源類別的存取（例如，封鎖存取屬於"網際網路溝通"類別的網站）。

- 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。

## 啟用或停用 Web 控制

預設情況下將啟用 Web 控制。您可以根據需要停用 Web 控制。

*要啟用或停用 Web 控制：*

1. 開啟程式設定視窗。
2. 在視窗左側的"**安全控制**"區域中，選擇"**Web 控制**"。

   在視窗右側，顯示了 Web 控制元件的設定。
3. 請執行以下操作之一：
   - 如果要啟用 Web 控制，請選取"**啟用 Web 控制**"核取方塊。
   - 如果要停用 Web 控制，請清除"**啟用 Web 控制**"核取方塊。

   如果 Web 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旨來敘述網頁資源封锁資料內容類別（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 應用程式和網站。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。
- 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。
- 包含以下內容的網路資源：
  - 覆寫科學與大眾主旨的性教育文章與網誌。
  - 醫療百科，尤其是關於有性生殖的部分。
  - 醫療機構資源，尤其是關於性器官治療的部分。

## 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。

- **檔案下載種子**。

  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。
- 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旨的網頁資源。

## 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”、“打斗”、“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。
- 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。

## 褻瀆、淫穢

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旨的語言和語言學材料的網頁資源。

## 網際網路通信

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、論壇與即時通訊**。

  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）。

- **交友網站**。

  此子類別包括收費或免費提供各種社群網路服務的網頁資源。

  與“色情內容”類別重疊。

- **基於網頁的郵件**。

  此子類別僅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。

## 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。

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。

## 線上商店、銀行、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：

- **線上商店**。

  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的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。

## 匿名網站

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。
- 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、歷史和宗教主旨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。

## 地區法律限制

該類別包含**根據俄羅斯聯邦法律要求封鎖**的子類別，其中包含根據俄羅斯聯邦法律封鎖的網路資源。

# 關於網路資源存取規則

不建議建立超過 1000 條的 Web 資源存取規則，因為這可能導致系統變得不穩定。

網路資源存取規則是使用者在規則排程中指明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 Web 控制元件控制其存取權限的網頁資源集區。

系統提供以下篩選功能選項：

- **按內容篩選**。Web 控制將按照內容和資料類型分類網頁資源。對於內容和資料屬於按這些類別定義的類型的網頁資源，您可以控制使用者對它們的存取權限。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，Web 控制元件的規則清單將不為空白。該清單中存在兩個規則：

- “指令碼和式樣表”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 Web 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"**安全控制**"區域中，選擇"**Web 控制**"。

   在視窗右側，顯示了 Web 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：

      - **套用於所有位址**。
      - **套用於單個位址**。

   e. 如果選取"**套用於單個位址**"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和/或位址分組。

   f. 選取"**指定使用者和/或使用者群組**"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/或使用者群組清單。

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**"安全控制"**區域中，選擇**"Web 控制"**。

   在視窗右側，顯示了 Web 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 Web 控制規則的一致性，您可以測試它們。為此，Web 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**"安全控制"**區域中，選擇**"Web 控制"**。
   在視窗右側，顯示了 Web 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 Web 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**"安全控制"**區域中，選擇**"Web 控制"**。
   在視窗右側，顯示了 Web 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 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更早版本應用程式升級至 Kaspersky Endpoint Security 11 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“網際網路溝通”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“線上商城，銀行，支付系統”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“**安全控制**”區域中，選擇“**Web 控制**”。

   在視窗右側，顯示了 Web 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**"安全控制"**區域中，選擇**"Web 控制"**。
   在視窗右側，顯示了 Web 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**"套用於單個位址"**。
   - 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 | *.example.com | http://www.123example.com | 否 | 參見規則 1。 |
| 2 | *.example.com | http://www.123.example.com | 是 | 參見規則 1。 |
| 3 | *example.com | http://www.123example.com | 是 | 參見規則 1。 |

| | | | | |
|---|---|---|---|---|
| 4 | *example.com | http://www.123.example.com | 是 | 參見規則 1。 |
| 5 | http://www.*.example.com | http://www.123example.com | 否 | 參見規則 1。 |
| 6 | www.example.com | http://www.example.com | 是 | 參見規則 2、1。 |
| 7 | www.example.com | https://www.example.com | 是 | 參見規則 2、1。 |
| 8 | http://www.*.example.com | http://123.example.com | 是 | 參見規則 2、4、1。 |
| 9 | www.example.com | http://www.example.com/abc | 是 | 參見規則 2、5、1。 |
| 10 | example.com | http://www.example.com | 是 | 參見規則 3、1。 |
| 11 | http://example.com/ | http://example.com/abc | 是 | 參見規則 6。 |
| 12 | http://example.com/* | http://example.com | 是 | 參見規則 7。 |
| 13 | http://example.com | https://example.com | 否 | 參見規則 8。 |
| 14 | "example.com" | http://www.example.com | 否 | 參見規則 9。 |
| 15 | "http://www.example.com" | http://www.example.com/abc | 否 | 參見規則 9。 |
| 16 | "*.example.com" | http://www.example.com | 是 | 參見規則 1、9。 |
| 17 | "http://www.example.com/*" | http://www.example.com/abc | 是 | 參見規則 1、9。 |
| 18 | "www.example.com" | http://www.example.com; https://www.example.com | 是 | 參見規則 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 Web 控制訊息範本

根據在 Web 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 顯示下列類型之一的訊息（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。

在處理透過 HTTPS 協定接收的 Web 流量時，Kaspersky Endpoint Security 會封鎖已禁止的 Web 資源，而不顯示 Web 控制訊息。

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：*

1. 開啟程式設定視窗。
2. 在視窗左側的**"安全控制"**區域中，選擇**"Web 控制"**。
   在視窗右側，顯示了 Web 控制元件的設定。
3. 在視窗右側，點擊**"範本"**按鈕。
   開啟**"訊息範本"**視窗。
4. 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"**標籤。
   - 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"**標籤。
   - 要修改傳送給區域網路管理員的訊息的範本，請選取**"傳送給管理員的訊息"**標籤。
5. 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。
6. 點擊**"確定"**。
7. 要儲存變更，請點擊**"儲存"**按鈕。

# 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 for File Servers的電腦上，則只有使用 BitLocker 磁碟機加密技術的完整磁碟加密可用。

本章節包含有關對本機電腦磁碟機、硬碟和卸除式磁碟上的檔案進行加密和解密的資訊，並提供有關如何使用 Kaspersky Endpoint Security 和 Kaspersky Endpoint Security 管理外掛程式設定和執行資料加密和解密的說明。

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）。

## 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機和硬碟磁碟機。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：

- **本機電腦磁碟機上檔案級加密**。您可以根據副檔名或副檔名組合編制檔案清單，和儲存在本機電腦磁碟上的資料夾清單，並且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。

  有關套用卡巴斯基安全管理中心政策的詳細資訊，請參閱《卡巴斯基安全管理中心說明手冊》。
- **卸除式磁碟機加密**。您可以指定預設加密規則，應用程式將根據此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。

- **完整磁碟加密**。您可以選取加密技術：卡巴斯基磁碟加密或 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磁碟機存取的還原金鑰。電腦啟動時，BitLocker 將從 Trusted Platform Module 請求硬碟磁碟機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。

  您可以指定預設的完整磁碟加密規則，並建立要從加密中排除的硬碟磁碟機的清單。套用卡巴斯基安全管理中心政策後，Kaspersky Endpoint Security 將按照磁區執行完整磁碟加密。應用程式加密將同時套用至硬碟磁碟機的所有邏輯分區上。有關套用卡巴斯基安全管理中心政策的詳細資訊，請參閱《*卡巴斯基安全管理中心說明手冊*》。

  加密系統硬碟磁碟機後，在下次電腦啟動時，使用者要能夠存取硬碟磁碟機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，此技術使您可以使用身分驗證代理帳戶的使用者帳戶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說明手冊》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 11 for Windows 時，系統不會儲存身分驗證代理帳戶清單。

  只能在安裝了帶有完整磁碟加密功能的 Kaspersky Endpoint Security 的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磁碟機中的檔案洩露的風險。

若要加密硬碟磁碟機和卸除式磁碟，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，在啟用"**僅加密使用的磁碟空間**"功能的情況下，隨著檔案寫入新裝置和定期加密該裝置，在一段時間後所有磁區都將加密。

解密檔案所需的檔案由加密時控制電腦的卡巴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"還原加密裝置上的資料；
- 從備份還原在加密時控制電腦的卡巴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 0.5% 的非碎片的磁碟空間來儲存這些檔案。如果硬碟磁碟機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 的電腦磁碟機進行加密會使得 Kaspersky Anti-Virus for UEFI 無法執行。

## 加密功能限制

對於不滿足軟硬體需求的硬碟磁碟機，無法使用卡巴斯基磁碟加密技術進行完整磁碟加密。

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 0.5% 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分發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. 從包含不同位數加密演算法的分發套件中安裝 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"**標籤。
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**"一般加密設定"**子區域。
7. 在**"一般加密設定"**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. 若要儲存您的變更，請在**"內容：<政策名稱>"**視窗中點擊**"確定"**。
11. 套用政策。
    有關套用卡巴斯基安全管理中心政策的詳細資訊，請參閱《卡巴斯基安全管理中心說明手冊》。

## 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，套用為加密/解密抽取式磁碟磁碟機配置的卡巴斯基安全管理中心政策的結果取決於抽取式磁碟磁碟機連線到的電腦。
- 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 Lab 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
  - 暫存檔案
  - Outlook 檔案
- Kaspersky Endpoint Security 不會加密其修改可能損害作業系統和安裝的應用程式的檔案。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。儘管加密排除項目清單中的檔案和資料夾可以新增至加密清單，但在檔案加密工作期間，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

## 本機電腦磁碟機上檔案級加密

如果將 Kaspersky Endpoint Security 安裝在執行 Microsoft Windows 以做工作站用的電腦上，則本機電腦磁碟機上的檔案級加密可用。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

Kaspersky Endpoint Security 支援加密具有 FAT32 和 NTFS 檔案系統的本機磁碟機中的檔案。

*若要在本機磁碟機上加密檔案，請執行以下操作：*

1. 開啟卡巴斯基安全管理中心管理主控台。
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"**標籤。
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**"檔案級加密"**。
7. 在視窗右側，選擇 **加密** 標籤。
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 Lab 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. 若要儲存您的變更，請在**"內容：<政策名稱>"**視窗中點擊**"確定"**。
11. 套用政策。
    有關套用卡巴斯基安全管理中心政策的詳細資訊，請參閱《*卡巴斯基安全管理中心說明手冊*》。

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. 開啟卡巴斯基安全管理中心管理主控台。
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"**標籤。
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**"檔案級加密"**。
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**"預設規則"**模式中執行存取規則後，如果您轉換到**"保留不變"**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"**標籤。
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應用程式清單"**項目。

   **"從卡巴斯基安全管理中心清單中新增應用程式"**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"**、**"供應商"**和**"新增的時間段"**參數的值和**"群"**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** 標籤中。

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** 標籤中。

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"**標籤。
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**"檔案級加密"**。
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**"保留不變"**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"**標籤。
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應用程式清單"**項目。

   **"從卡巴斯基安全管理中心清單中新增應用程式"**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"**、**"供應商"**和**"新增的時間段"**參數的值和**"群"**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**"之前為應用程式選擇的動作"**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"**標籤。
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**"檔案級加密"**。
7. 在視窗右側，選取**"解密"**標籤。
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 Lab 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. 若要儲存您的變更，請在**"內容：<政策名稱>"**視窗中點擊**"確定"**。
11. 套用政策。
    有關套用卡巴斯基安全管理中心政策的詳細資訊，請參閱《*卡巴斯基安全管理中心說明手冊*》。

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"**標籤。
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**"檔案級加密"**。
7. 在視窗右側，選擇 **加密** 標籤。
8. 從清單中移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**"刪除規則並解密檔案"**。

   您可以一次從加密清單中刪除數個項目。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**"移除"**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. 若要儲存您的變更，請在**"內容：<政策名稱>"**視窗中點擊**"確定"**。
11. 套用政策。

有關套用卡巴斯基安全管理中心政策的詳細資訊，請參閱《卡巴斯基安全管理中心說明手冊》。

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**"確定"**。

   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案，以及已經從加密壓縮檔案總複製到目的檔案案夾中的所有檔案。

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。

## 啟動卸除式磁碟加密

*若要加密卸除式磁碟，請執行以下操作：*

1. 開啟卡巴斯基安全管理中心管理主控台。
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"**標籤。
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**"卸除式磁碟機加密"**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。
   - **加密整個卸除式磁碟機**。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。

     該加密方案由 Kaspersky Endpoint Security 的完整磁碟加密功能提供。

   - **加密所有檔案**。如果選定了該選項，為卸除式磁碟機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機上儲存的所有檔案。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。

- **解密整個卸除式磁碟機**。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。

  Kaspersky Endpoint Security 的檔案級加密功能和完整磁碟加密功能均可以使該加密方案成為可能。

- **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。

Kaspersky Endpoint Security 支援 FAT32 和 NTFS 檔案系統的加密。如果選擇"**加密所有檔案**"或"**僅加密新檔案**"選項，並且帶有不受支援的檔案系統的卸除式磁碟機連線到電腦，則卸除式磁碟機加密工作返回錯誤，Kaspersky Endpoint Security 為此卸除式磁碟機分配唯讀狀態。

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。

有關套用卡巴斯基安全管理中心政策的詳細資訊，請參閱《卡巴斯基安全管理中心說明手冊》。

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

*若要為卸除式磁碟新新增密規則，請執行以下操作：*

1. 開啟卡巴斯基安全管理中心管理主控台。
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"**標籤。
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**"卸除式磁碟機加密"**子區域。
7. 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"**。

     **"從受信任裝置清單中新增裝置"**視窗將開啟。
   - 如果您希望為卡巴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**"從裝置的卡巴斯基安全管理中心清單中"**。

     **"從卡巴斯基安全管理中心清單中新增裝置"**視窗將開啟。
8. 如果您在上個步驟中選取了**"從裝置的卡巴斯基安全管理中心 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. 指定下列參數的值：**在表中顯示已定義以下項的裝置**：**名稱**、**電腦**和 **卡巴斯基磁碟加密**。
   b. 點擊 **重新整理**按鈕。
9. 在**"選定裝置的加密模式"**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。
10. 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。
11. 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機"**模式中套用政策，未包含檔案的磁區將不會被加密。
12. 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"**。

13. 點擊**"確定"**。

    包含已建立加密規則的參數將顯示在**"自訂規則"**標籤中。

14. 點擊**"確定"**儲存變更。

新增的卸除式磁碟機加密規則，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"**標籤。
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**"卸除式磁碟機加密"**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**"設定規則"**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機加密規則，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"**標籤。

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**"卸除式磁碟機加密"**子區域。
7. 勾選**"攜帶模式"**核取方塊。

   僅當在**"選定裝置的加密模式"**下拉清單中選擇了**"加密所有檔案"**或**"僅加密新檔案"**，攜帶模式才可用。

8. 點擊**"確定"**。
9. 套用政策。

   有關套用卡巴斯基安全管理中心政策的詳細資訊，請參閱《卡巴斯基安全管理中心說明手冊》。

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電腦。
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，請執行以下操作：*

1. 開啟卡巴斯基安全管理中心管理主控台。
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"**標籤。
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**"卸除式磁碟機加密"**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**"設定規則"**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。

有關套用卡巴斯基安全管理中心政策的詳細資訊，請參閱《卡巴斯基安全管理中心說明手冊》。

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。

## 完整磁碟加密

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。

本節包含有關完整磁碟加密的資訊，以及使用 Kaspersky Endpoint Security 和 Kaspersky Endpoint Security 管理外掛程式配置和執行完整磁碟加密的說明。

## 關於完整磁碟加密

Kaspersky Endpoint Security 支援 FAT32、NTFS 和 exFat 檔案系統的完整磁碟加密。

啟動完整磁碟加密之前，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磁碟機與驗證代理或 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。如果相容性檢查成功，則在載入作業系統和啟動應用程式後開始完整磁碟加密。如果系統硬碟磁碟機不相容驗證代理或 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。根據此資訊，應用程式在作業系統啟動時不會啟動完整磁碟加密。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磁碟機與身分驗證代理和 BitLocker 加密元件的相容性。要執行此操作，請在完整磁碟加密前，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磁碟機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。

啟動完整磁碟加密後，Kaspersky Endpoint Security 將加密硬碟上的所有資料。

如果使用者在完整磁碟加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 將還原完整磁碟加密。

如果作業系統在完整磁碟加密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 將還原完整磁碟加密。

如果作業系統在完整磁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 將還原完整磁碟加密，且不會載入身分驗證代理。

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。

  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。

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磁碟機。

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

## 使用卡巴斯基磁碟加密技術執行完整磁碟加密

在電腦上開始完整磁碟加密之前，建議您確保電腦未受到感染。若要執行操作，應啟動完整掃描或關鍵區域掃描工作。在已被 rootkit 感染的電腦上執行完整磁碟加密可能導致電腦無法執行。

*要使用卡巴斯基磁碟加密技術執行完整磁碟加密：*

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄的**"受管裝置"**資料夾中，開啟您希望為其設定完整磁碟加密的管理群組的名稱所對應的資料夾。
3. 在工作區選擇**"政策"**標籤。
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**"完整磁碟加密"**。
7. 在**"加密技術"**下拉清單中，選取**"卡巴斯基磁碟加密"**選項。

   如果電腦的硬碟磁碟機先前使用 BitLocker 加密，則無法使用卡巴斯基磁碟加密。

8. 在**"加密模式"**下拉清單中，選取**"加密所有硬碟磁碟機"**。

   如果電腦安裝了多個作業系統，則在加密所有硬碟後，您將只能載入安裝了此應用程式的作業系統。

   如果您需要從加密中排除某些硬碟磁碟機，則建立此類硬碟磁碟機的清單。

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磁碟機，則選取**"僅加密使用的磁碟空間"**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磁碟機，則清空**"僅加密使用的磁碟空間"**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**僅加密使用的磁碟空間**功能加密，則在**加密所有硬碟磁碟機**模式下套用政策後，未包含檔案的磁區不會被加密。

10. 如果在電腦加密過程中遇到硬體不相容問題，可以在 BIOS 中選中**"使用 Legacy USB Support"**核取方塊以在初始電腦啟動階段啟用對 USB 裝置的支援。

    啟用/停用 Legacy USB Support 不會影響作業系統啟動後對 USB 裝置的支援。

    啟用 Legacy USB Support 後，如果電腦以 BIOS 模式執行，身分驗證代理將不支援 USB 權杖操作。建議僅當存在硬體相容性問題時並僅對發生問題的電腦使用此選項。

11. 點擊“**確定**”儲存變更。

12. 套用政策。

    有關套用卡巴斯基安全管理中心政策的詳細資訊，請參閱《卡巴斯基安全管理中心說明手冊》。

## 使用 BitLocker 磁碟機加密技術執行完整磁碟加密

在電腦上開始完整磁碟加密之前，建議您確保電腦未受到感染。若要執行操作，應啟動完整掃描或關鍵區域掃描工作。在已被 rootkit 感染的電腦上執行完整磁碟加密可能導致電腦無法執行。

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。

*要使用 BitLocker 磁碟機加密技術執行完整磁碟加密：*

1. 開啟卡巴斯基安全管理中心管理主控台。

2. 在管理主控台樹狀目錄的“**受管裝置**”資料夾中，開啟您希望為其設定完整磁碟加密的管理群組的名稱所對應的資料夾。

3. 在工作區選擇“**政策**”標籤。

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“**完整磁碟加密**”。

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“**加密所有硬碟磁碟機**”選項。

   如果電腦安裝了多個作業系統，在加密後，您將能夠只載入執行了加密的作業系統。

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磁碟機，則選取**"僅加密使用的磁碟空間"**核取方塊。
    - 如果您希望將加密應用至這個硬碟磁碟機，則清空**"僅加密使用的磁碟空間"**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**僅加密使用的磁碟空間**功能加密，則在**加密所有硬碟磁碟機**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 加密的硬碟磁碟機方式。

    - 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) 進行完整磁碟加密，請選取**"使用密碼"**選項，並在**"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**"密碼最小長度"**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平台模組不可用，則完整磁碟加密將不會啟動。

14. 點擊**"確定"**儲存變更。

15. 套用政策。

    有關套用卡巴斯基安全管理中心政策的詳細資訊，請參閱《卡巴斯基安全管理中心說明手冊》。

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：

- 如果卡巴斯基安全管理中心政策配置為加密系統硬碟磁碟機，則如果受信任平台模組在使用中，將顯示 PIN 代碼提示視窗，否則將顯示用於預啟動身份驗證的密碼請求視窗。
- 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 和更早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）。

## 建立硬碟磁碟機加密排除清單

您可以僅為卡巴斯基磁碟加密技術建立加密排除項目清單。

*若要建立硬碟磁碟機排除清單，請執行以下操作：*

1. 開啟卡巴斯基安全管理中心管理主控台。
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磁碟機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"**標籤。
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**"完整磁碟加密"**。
7. 在**"加密技術"**下拉清單中，選取**"卡巴斯基磁碟加密"**選項。
   從加密項目中排除的硬碟磁碟機所對應的項目將顯示在**"請勿加密以下硬碟磁碟機"**清單中。如果您先前並未建立硬碟磁碟機加密排除清單，此清單將是空白。
8. 若要向硬碟磁碟機排除清單中新增硬碟磁碟機，請執行以下操作：
   a. 點擊**"新增"**按鈕。
   **"從卡巴斯基安全管理中心清單中新增裝置"**視窗將開啟。
   b. 在**"從卡巴斯基安全管理中心清單新增裝置"**視窗中，指定下列參數的值：**名稱**、**電腦**、**磁碟類型**和**卡巴斯基磁碟加密**。
   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"**。
   對應於選定硬碟磁碟機的項目將顯示在**"請勿加密以下硬碟磁碟機"**清單中。
9. 如果您希望從排除項清單中刪除硬碟磁碟機，則在**"請勿加密以下硬碟磁碟機"**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。

## 硬碟磁碟機解密

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。

*若要解密硬碟磁碟機，請執行以下操作：*

1. 開啟卡巴斯基安全管理中心管理主控台。
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磁碟機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"**標籤。
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**"完整磁碟加密"**。
7. 在**"加密技術"**下拉清單中選取加密硬碟磁碟機的技術。
8. 請執行以下操作之一：
   - 在**"加密模式"**下拉清單中，選取**"解密所有硬碟磁碟機"**選取方塊，如果您希望解密所有加密的硬碟磁碟機。
   - 將您希望解密的加密硬碟磁碟機新增至**請勿加密以下硬碟磁碟機**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。

    有關套用卡巴斯基安全管理中心政策的詳細資訊，請參閱《*卡巴斯基安全管理中心說明手冊*》。

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 將還原硬碟磁碟機解密。

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 將還原硬碟磁碟機解密。進行硬碟磁碟機解密後，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磁碟機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 將還原硬碟磁碟機加密，且無需載入身分驗證。

## 使用身分驗證代理

如果系統硬碟磁碟機被加密，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磁碟機並載入作業系統。

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接受加密裝置存取或還原資料的過程。

## 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**"標籤。

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“**一般加密設定**”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**”標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**”標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。

   > 您可以輸入包含 16 行或更少文字的說明文字。一行的最大長度為 64 個字元。

10. 點擊“**確定**”。
11. 若要儲存您的變更，請在“**內容：<政策名稱>**”視窗中點擊“**確定**”。

## 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。

*要選取身分驗證代理偵錯等級：*

1. 當帶有加密硬碟磁碟機的電腦啟動後，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磁碟機的電腦透過 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。

如果電腦上有已加密的硬碟磁碟機或者在完整磁碟加密期間，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，您可以手動將身分驗證代理偵錯檔案傳送至 Kaspersky 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“**用於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。

用於管理新增至工作中的身分驗證代理帳戶的指令將被執行。

## 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 使用者帳戶不存在於電腦或其**加密（帳戶管理）**本機工作正在被修改的受信任域中，身分驗證代理帳戶管理工作將以執行錯誤而結束。

5. 如果您希望將先前為身分驗證代理建立的現有帳戶取代為正在建立的帳戶，請選擇**"更換現有帳戶"**核取方塊。

   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磁碟機。

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磁碟機。

   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**"不要求變更密碼"**選項。

9. 如果您希望在存取加密硬碟磁碟機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**"指令敘述"**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"**選項。
    - 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"**選項。

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“**帳戶編輯指令**”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“**進行身分驗證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“**編輯指令敘述**”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：<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**"刪除帳戶指令"**。

   **"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. 開啟卡巴斯基安全管理中心管理主控台。
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名稱所對應的資料夾。
3. 在工作區選取**"裝置"**標籤。
4. 在**"裝置"**標籤上，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**"授予離線模式下的存取權限"**。

   開啟**"授予離線模式下的存取權限"**視窗。
6. 在**"授予離線模式下的存取權限"**視窗中，選取**"身分驗證代理"**標籤。
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**硬碟磁碟機**下拉清單中，選取您要還原存取的加密硬碟磁碟機。
10. 在**"使用者請求"**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，卡巴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巴斯基安全管理中心。

程式提供了以下加密狀態值：

- *未定義加密政策*。尚未為該電腦定義卡巴斯基安全管理中心加密政策。
- *正在套用政策*。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巴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。

- *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。

## 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"**標籤。
   工作區中的**"裝置"**標籤將顯示選定電腦群組中電腦的內容。
4. 在工作區的**"裝置"**標籤中，將捲軸滑向右側。
5. 如果 **加密狀態** 列未顯示：
   1. 右鍵點擊開啟表頭的右鍵選單。
   2. 在右鍵選單的**"檢視"**下拉清單中，選擇**"新增/刪除列"**。
      **"新增/刪除列"**視窗將開啟。
   3. 在**"新增/刪除列"**視窗中選擇**"加密狀態"**核取方塊。
   4. 點擊**"確定"**。

**"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。該狀態是基於電腦本機磁碟機上的檔案加密資訊和完整磁碟加密的資訊形成的。

## 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：裝置加密"**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**"卸除式磁碟機加密"**項。

所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"**標籤，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. 開啟卡巴斯基安全管理中心管理主控台。
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"**標籤。
4. 在**"裝置"**標籤上，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，卡巴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. 開啟卡巴斯基安全管理中心管理主控台。
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**”視窗中選取以下項目之一：
   - **受管裝置加密狀態報告**。
   - **大容量儲存裝置加密狀態報告**。
   - **檔案加密錯誤報告**。
   - **封鎖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。
6. 在模板的右鍵選單中選取“**顯示報告**”。

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。**"檔案存取被封鎖"**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. 獲取區域網路管理員為你建立並提供的存取加密檔案的金鑰檔案。

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"**標籤。
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**"授予離線模式下的存取權限"**。

   開啟**"授予離線模式下的存取權限"**視窗。
6. 在**"授予離線模式下的存取權限"**視窗中，選擇**"加密"**標籤。
7. 在 **加密** 標籤上點擊 **瀏覽** 按鈕。

   系統將開啟標準的**"選擇請求存取檔案"**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"**標籤上。
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他方法傳送給使用者，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"**標籤。
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**"一般加密設定"**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. 若要儲存您的變更，請在**"內容：<政策名稱>"**視窗中點擊**"確定"**。

# 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 副檔名的請求存取檔案 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 副檔名的請求存取檔案 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前，建議在將執行過程的電腦上取消卡巴斯基安全管理中心政策或停用卡巴斯基安全管理中心政策設定中的加密。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. 開啟卡巴斯基安全管理中心管理主控台。
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"**標籤。
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**"授予離線模式下的存取權限"**。

開啟**"授予離線模式下的存取權限"**視窗。

6. 在**"授予離線模式下的存取權限"**視窗中，選擇**"加密"**標籤。
7. 在 **加密** 標籤上點擊 **瀏覽** 按鈕。

系統將開啟標準的**"選擇請求存取檔案"**Microsoft Windows 視窗。

8. 在**"選擇請求存取檔案"**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。

卡巴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"**標籤上。

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他方法傳送給使用者，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 加密的系統硬碟磁碟機的還原金鑰：*

1. 開啟卡巴斯基安全管理中心管理主控台。
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"**標籤。
4. 在**"裝置"**標籤上，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**"授予離線模式下的存取權限"**。
   開啟**"授予離線模式下的存取權限"**視窗。
6. 在**"授予離線模式下的存取權限"**視窗中，選取**"存取 BitLocker 防護的系統磁碟"**標籤。
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 加密的非系統硬碟磁碟機的還原金鑰：*

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄中，選取**"附加 → 資料加密和防護 → 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，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**”按鈕開啟“**支援**”視窗。
3. 在“**支援**”視窗中，點擊“**加密裝置還原實用程式**”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“**建立獨立還原實用程式**”按鈕。
   “**建立獨立還原實用程式**”視窗將開啟。
5. 在“**儲存至**”視窗中，手動鍵入儲存還原實用程式可執行檔的路徑，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 主視窗內的“**支援**”按鈕開啟“**支援**”視窗，點擊“**加密裝置還原實用程式**”按鈕。
   - 執行建立還原實用工具的 fdert.exe 可執行檔。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. 開啟卡巴斯基安全管理中心管理主控台。

2. 在管理主控台樹狀目錄中，選取"**附加 → 資料加密和防護 → 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**附加 → 資料加密和防護**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"**選擇請求存取檔案**"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他方法傳送給使用者，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. 在電腦與資料被加密時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。
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）。

# 端點感應器

"端點感應器"元件的設定只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。

此區域包含有關"端點感應器"和如何啟用或停用此元件的說明。

## 關於端點感應器

*端點感應器*是 Kaspersky Anti Targeted Attack Platform 的元件。此解決方案用於快速偵測目的攻擊之類的威脅。

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。

此元件的功能在以下作業系統下可用：

- 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 2012 Standard / Foundation / Essentials x64 Edition、Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials x64 Edition。
- Microsoft Windows Server 2016

有關本文件未提供的 Kaspersky Anti Targeted Attack Platform 的其他資訊，請參閱 Kaspersky Anti Targeted Attack Platform 說明。

必須在 Kaspersky Anti Targeted Attack Platform 伺服器上直接允許電腦與"端點感應器"的連線，不使用代理伺服器。

## 啟用和停用端點感應器元件

*要啟用和停用端點感應器元件：*

1. 開啟卡巴斯基安全管理中心管理主控台。
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**"標籤。
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. 選擇“**端點感應器**”區域。
7. 請執行以下操作之一：
   - 如果您希望啟用端點感應器，請選中“**端點感應器**”核取方塊。
   - 如果您希望停用端點感應器，請清除“**端點感應器**”核取方塊。
8. 如果您在上一步選中了核取方塊：
   a. 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：
      1. 協定名稱
      2. 伺服器的 IP 位址或全限定功能變數名稱 (FQDN)
      3. 伺服器上 Windows 事件收集器的路徑
   b. 在“**連接埠**”欄位中，指定用於連線到 Kaspersky Anti Targeted Attack Platform 伺服器的埠號。
9. 點擊“**確定**”。
10. 套用政策。
    有關套用卡巴斯基安全管理中心政策的詳細資訊，請參閱《卡巴斯基安全管理中心說明手冊》。

# 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 Lab 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 Lab 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新威脅記錄。因此，我們建議您定期更新資料庫。

  除了 Kaspersky Endpoint Security 資料庫之外，系統也會更新已啟用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"**工作**"視窗的"**更新**"區域中。

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。

更新來源包括卡巴斯基安全管理中心、 Kaspersky 更新伺服器、以及網路或本機資料夾。

如果您無法存取 Kaspersky 更新伺服器（例如，網際網路存取受到限制），您可以聯絡 Kaspersky 總部以請求 Kaspersky 合作夥伴的聯絡資訊。Kaspersky 合作夥伴將透過卸除式磁碟機向您提供更新。

在訂購位於卸除式磁碟機上的更新時，請指定您是否還需要程式模組更新。

## 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 Lab 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 Lab 更新伺服器區域。

  如果您使用 Kaspersky Lab 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 Lab 更新伺服器的地點。Kaspersky Lab 更新伺服器位於多個國家/地區。使用最近的 Kaspersky Lab 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 Lab 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**"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"**標籤上點擊**"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**"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"**標籤中的**"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**"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“**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**”標籤上點擊“**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**”標籤中，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“**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** 標籤在 **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**"程式啟動後延遲啟動工作時間"**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**"程式啟動後延遲啟動工作時間"**將無法使用。

     d. 如果您希望 Kaspersky Endpoint Security 儘快執行略過的工作，請勾選**"執行略過的工作"**核取方塊。

     如果在**"頻率"**下拉清單中選取**"小時"**、**"分鐘"**或**"在程式啟動後"**，則**"執行略過的工作"**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，或者從沒有設定過代理伺服器身分驗證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**"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** 標籤在 **更新** 視窗中開啟。

4. 在**"執行模式"**標籤的**"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**"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 Lab 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. 點擊應用程式主視窗下方的**"工作"**按鈕。
   **"工作"**視窗將開啟。

3. 點擊具有更新工作名稱的區域。
   所選區域將展開。

4. 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"**。
  更新工作名稱下方顯示的工作進度狀態變更為*"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"**。
  更新工作名稱下方顯示的工作進度狀態變更為*"已停止"*。

*要在顯示簡化的應用程式介面時啟動或停止更新工作：*

1. 在工作列通知區域按右鍵程式圖示，開啟右鍵選單中。
2. 在上下文功能表中的**"工作"**下拉清單中，執行以下操作之一：
   - 選擇未執行的更新工作以將其啟動
   - 選擇正在執行的更新工作以將其停止
   - 選擇暫停的更新工作以將其還原或重新啟動

# 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. 點擊應用程式主視窗下方的**"工作"**按鈕。
   **"工作"**視窗將開啟。
3. 點擊具有更新回溯工作名稱的區域。
   所選區域將展開。
4. 點擊**"啟動"**按鈕。
   這將啟動回溯工作。
   回溯工作名稱下方顯示的工作進度狀態變更為*"正在執行"*。

*要在顯示簡化的應用程式介面時啟動或停止回溯工作：*

1. 在工作列通知區域按右鍵程式圖示，開啟右鍵選單中。
2. 在上下文功能表中的**"工作"**下拉清單中，執行以下操作之一：
   - 選擇未執行的回溯工作以將其啟動
   - 選擇正在執行的回溯工作以將其停止

- 選擇暫停的回溯工作以將其還原或重新啟動

## 配置代理伺服器使用

*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**"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 。

   您也可以在應用程式設定視窗的**"一般設定"**區域的**"應用程式設定"**子區域中開啟**"代理伺服器設定"**視窗。
4. 在**"代理伺服器設定"**標籤中選取**"使用代理伺服器"**核取方塊。
5. 選擇以下選項之一以確定代理伺服器位址：
   - **自動偵測代理伺服器位址**。
     預設情況下已勾選此選項。
   - **使用指定的代理伺服器位址和連接埠**。
6. 如果選擇了**"使用指定的代理伺服器位址和連接埠"**選項，請在**"位址"**和**"連接埠"**欄位中指定值。
7. 如果您希望在代理伺服器上啟用身分驗證，請選中**"設定用於身分驗證的使用者名稱和密碼"**並在以下欄位中指定值：
   - **使用者名稱**。
     該欄位用於輸入在代理伺服器上進行身分驗證時使用的使用者名稱。
   - **密碼**。
     該欄位用於輸入在代理伺服器上進行身分驗證時使用的使用者密碼。
8. 如果您希望在從共用資料夾更新 Kaspersky Endpoint Security 時停用代理伺服器，請選中**"本機位址不使用代理伺服器"**核取方塊。
9. 點擊**"確定"**。
10. 要儲存變更，請點擊**"儲存"**按鈕。

# 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。

掃描工作開始後，在"**工作**"視窗中，工作完成進度顯示正在執行的掃描工作的名稱下方。

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. 點擊應用程式主視窗下方的"**工作**"按鈕。
   "**工作**"視窗將開啟。
3. 點擊具有掃描工作名稱的區域。
   所選區域將展開。
4. 請執行以下操作之一：
   - 如果要執行掃描工作，請點擊"**啟動**"按鈕。
     此掃描工作名稱下方顯示的工作進度狀態變更為"*正在執行*"。
   - 如果您想要停止掃描工作，請在上下文功能表中選取"**停止**"。
     此掃描工作名稱下方顯示的工作進度狀態變更為"*已停止*"。

*要在顯示簡化的應用程式介面時啟動或停止掃描工作：*

1. 在工作列通知區域按右鍵程式圖示，開啟右鍵選單中。
2. 在上下文功能表中的"**工作**"下拉清單中，執行以下操作之一：
   - 選擇未執行的掃描工作以將其啟動
   - 選擇正在執行的掃描工作以將其停止
   - 選擇暫停的掃描工作以將其還原或重新啟動

## 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 Securit 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。
- 設定掃描方式。

  Kaspersky Endpoint Security 使用一種稱為機器學習和特徵碼分析的掃描技術。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 專家的建議，機器學習和特徵碼分析始終啟用。

  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：**高防護**，**建議防護**和**低防護**。**"建議防護"**安全防護等級設定可以看做是最佳化設定。它們由 Kaspersky Lab 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**"工作"**區域中，選擇包含所需掃描工作名稱的子區域（**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（**高防護**，**建議防護**或**低防護**），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**"建議防護"**，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

預設情況下，在偵測到受感染的檔案時，Kaspersky Endpoint Security 將嘗試解毒操作，或者如果無法解毒則移除它們。

*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"**工作**"區域中，選擇包含所需掃描工作名稱的子區域（**完整掃描**、**關鍵區域掃描**、**自訂掃描**、**從上下文功能表掃描**）。

   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，選取以下選項之一：
   - 如果您希望 Kaspersky Endpoint Security 嘗試解毒操作，或者如果無法解毒則刪除它們，請選中"**解毒，如果解毒失敗則刪除**"核取方塊。
   - 如果您希望 Kaspersky Endpoint Security 嘗試解毒操作，如果無法解毒則通知您，請選中"**解毒，如果解毒失敗則通知**"核取方塊。
   - 如果您希望　Kaspersky Endpoint Security 在偵測到受感染檔案時通知您，請選中"**通知**"核取方塊。

   在偵測到屬於 Windows Store 應用程式一部分的受感染檔案時，Kaspersky Endpoint Security 將套用**刪除**操作。
4. 要儲存變更，請點擊"**儲存**"按鈕。

## 產生要掃描的物件清單

*要生成要掃描的物件清單：*

1. 開啟程式設定視窗。
2. 在視窗左側的"**工作**"區域中，選擇包含所需掃描工作名稱的子區域（**完整掃描**、**關鍵區域掃描**、**自訂掃描**、**從上下文功能表掃描**）。

   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. 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**"。
5. 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"**。

6. 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。

7. 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。

8. 點擊**"確定"**。

9. 要儲存變更，請點擊**"儲存"**按鈕。

## 選取要掃描的檔案類型

*要選取要掃描的檔案類型：*

1. 開啟程式設定視窗。

2. 在視窗左側的**"工作"**區域中，選擇包含所需掃描工作名稱的子區域（**完整掃描**、**關鍵區域掃描**、**自訂掃描**、**從上下文功能表掃描**）。
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"**標籤。

5. 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，有些檔案格式包含可執行代碼（例如 EXE 和 DLL 格式）或可能包含可執行代碼（例如 DOC 格式）。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"檔案威脅防護"元件會分析檔案標頭，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。

6. 在掃描工作名稱的視窗中選取"**確定**"按鈕。

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"**工作**"區域中，選擇包含所需掃描工作名稱的子區域（**完整掃描**、**關鍵區域掃描**、**自訂掃描**、**從上下文功能表掃描**）。

   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**"標籤。

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軟體，必須將複合檔案解壓縮，但是這可能會降低掃描速度。您可以限制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**"工作"**區域中，選擇包含所需掃描工作名稱的子區域（**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"**標籤。

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**"只掃描新增及變更的檔案"**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**"工作"**區域中，選擇包含所需掃描工作名稱的子區域（**完整掃描**、**關鍵區域掃描**、**自訂掃描**、**從上下文功能表掃描**）。

   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** 標籤。

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**"工作"**區域中，選擇包含所需掃描工作名稱的子區域（**完整掃描**、**關鍵區域掃描**、**自訂掃描**、**從上下文功能表掃描**）。

   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** 標籤。

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**"工作"**區域中，選擇相關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 儘快執行略過的掃描工作，請勾選**“執行略過的工作”**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。

## 設定在不同使用者帳號下掃描工作的啟動

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**“工作”**區域中，選擇相關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”**標籤的**“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機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. 在視窗左側的**“工作”**區域中選擇**“卸除式磁碟機掃描”**。

視窗右側將顯示掃描抽取式磁碟機的設定。

3. 在"**連接卸除式磁碟機時的動作**"下拉清單中，選擇所需操作：

   - **不掃描**
   - **深度掃描**

     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. 請執行以下操作之一：

   - 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，請選中"**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）。
   - 如果您希望 Kaspersky Endpoint Security 掃描所有硬碟，請清除"**最大抽取式磁碟機大小**"核取方塊。

5. 請執行以下操作之一：

   - 如果您希望 Kaspersky Endpoint Security 在單獨的視窗中顯示抽取式磁碟機掃描進度，請選中"**顯示掃描進度**"核取方塊。
   - 如果您希望 Kaspersky Endpoint Security 在背景執行抽取式磁碟機掃描，請清除"**顯示掃描進度**"核取方塊。

6. 要儲存變更，請點擊"**儲存**"按鈕。

# 處理活動威脅

本章節包含如何處理 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。

## 關於活動威脅

Kaspersky Endpoint Security 將記錄偵測到威活動脅但未處理的檔案的相關資訊。此資訊在活動威脅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。

如果 Kaspersky Endpoint Security 在掃描電腦中的病毒和其他威脅時由於某種原因未能按照指定的應用程式設定對某個檔案執行操作，Kaspersky Endpoint Security 會將該檔案移至活動威脅清單。

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。

但您可以執行下列操作之一：

- 在更新資料庫和程式模組後，對活動威脅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。
- 刪除活動威脅清單中的項目。

## 處理活動威脅清單

活動威脅清單顯示為與由於某些原因未被處理的感染檔案相關的事件表。

您可以對活動威脅清單中的檔案執行以下操作：

- 檢視活動威脅清單
- 使用目前版本的 Kaspersky Endpoint Security 資料庫和模組掃描清單中的活動威脅
- 將檔案從活動威脅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）
- 移除活動威脅清單中的檔案
- 開啟活動威脅清單中的檔案最初所在的資料夾

您也可在管理表中資料時執行以下操作：

- 基於列值或者自訂篩選條件篩選活動威脅。
- 使用活動威脅搜尋功能。
- 對活動威脅排序。
- 變更活動威脅清單中顯示的列的順序和排列
- 對活動威脅分組。

如有必要，您可以將選定的活動威脅的相關資訊複製到剪貼簿。

## 對活動威脅清單中的檔案啟動自訂掃描工作

您可以手動對由於某種原因未被處理的受感染檔案啟動自訂掃描工作。例如，如果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活動威脅清單中的檔案，則可以啟動掃描。

*要對活動威脅清單中的檔案啟動自訂掃描：*

1. 開啟“程式主視窗”。
2. 點擊“**<...> 個活動威脅**”區域。
   將開啟“**活動威脅**”視窗。
3. 在“**活動威脅**”視窗的表格中，選擇一個或多個與要掃描的檔案關聯的項目。
   若要選取多個項目，請按住“**CTRL**”鍵依次選擇項目。
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。

## 刪除活動威脅清單中的項目

*要刪除活動威脅清單中的項目：*

1. 開啟“程式主視窗”。
2. 點擊“**<...> 個活動威脅**”區域。
   將開啟“**活動威脅**”視窗。
3. 在“**活動威脅**”視窗的表中，選擇一個或多個要從活動威脅清單中刪除的項目。
   若要選取多個項目，請按住“**CTRL**”鍵依次選擇項目。
4. 透過下列方式之一刪除項目：
   - 點擊“**刪除**”按鈕。
   - 右鍵點擊以開啟右鍵選單並選取“**刪除**”。

# 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。

在完整性檢查工作啟動後，其進度顯示在“**工作**”視窗中的工作名稱下方的行中。

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. 點擊應用程式主視窗下方的“**工作**”按鈕。
   “**工作**”視窗將開啟。
3. 點擊具有完整性掃描工作名稱的區域。
   所選區域將展開。
4. 請執行以下操作之一：
   - 如果要執行完整性檢查工作，請點擊“**啟動**”按鈕。
     完整性檢查工作名稱下方顯示的工作進度狀態變更為“*正在執行*”。
   - 如果您想要停止完整性檢查工作，請從上下文功能表中選取“**停止**”。
     完整性檢查工作名稱下方顯示的工作進度狀態變更為“*已停止*”。

*要在顯示簡化的應用程式介面時啟動或停止完整性檢查工作：*

1. 在工作列通知區域按右鍵程式圖示，開啟右鍵選單中。
2. 在上下文功能表中的“**工作**”下拉清單中，執行以下操作之一：
   - 選擇未執行的完整性檢查工作以將其啟動
   - 選擇正在執行的完整性檢查工作以將其停止
   - 選擇暫停的完整性檢查工作以將其還原或重新啟動

# 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**"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**"執行略過的工作"**方塊。

      如果從**"頻率"**下拉清單中選取**"小時"**、**"分鐘"**或**"在程式啟動後"**，則**"執行略過的工作"**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. 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。

## 關於報告

每個 Kaspersky Endpoint Security 元件的操作、每次掃描工作、更新工作和完整性檢查工作的效能以及應用程式的整體操作的相關資訊將記錄在報告中。

報告儲存在 ProgramData\Kaspersky Lab\KES\Report 資料夾中。

報告可能包含以下使用者資料：

- Kaspersky Endpoint Security 掃描的檔案的路徑
- Kaspersky Endpoint Security 修改的登錄機碼的路徑
- Microsoft Windows 使用者名稱
- 使用者開啟的網頁的位址。

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。
- 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。

如果 Kaspersky Endpoint Security 在卡巴斯基安全管理中心管理下執行，則有關事件的資訊可能會傳送至卡巴斯基安全管理中心管理伺服器。有關在卡巴斯基安全管理中心管理報告的更多詳細資訊，請參閱《卡巴斯基安全管理中心說明》系統。

## 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. 在視窗的左側的**一般設定** 區域中，選擇 **報告和儲存**。
3. 在視窗右側的"**報告**"區域中，執行下列操作之一：

   - 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. 在視窗左側的**一般設定** 區域中，選擇 **報告和儲存**。
3. 在視窗右側的**"報告"**區域中，執行下列操作之一：
   - 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

如果使用者能檢視報告，該使用者也能檢視報告中反映的所有事件。

*若要檢視報告：*

1. 開啟"程式主視窗"。
2. 點擊應用程式主視窗下方的**"報告"**按鈕。
   **"報告"**視窗將開啟。
3. 在**"報告"**視窗左側的元件和工作清單中，選取一個元件或工作。
   視窗右側部分顯示的報告中包含 Kaspersky Endpoint Security 的選定元件或選定工作執行所生成的事件清單。
   您可以根據其中一列的單元格中的值對報告中的事件進行排序。

預設情況下，報告事件根據**"事件日期"**列中的單元格中的值按照遞增排序。

## 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. 點擊應用程式主視窗下方的**"報告"**按鈕。
   **"報告"**視窗將開啟。
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。若要尋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

使用者個人負責確保儲存為檔案的報告的資訊安全，尤其是控制和限制存取該資訊。

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. 點擊應用程式主視窗下方的“**報告**”按鈕。
   “**報告**”視窗將開啟。
3. 在“**報告**”視窗左側的元件和工作清單中，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。
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. 在視窗的左側的**一般設定** 區域中，選擇 **報告和儲存**。
3. 在視窗右側的**"報告"**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**。
   - **防護元件報告**。包含關於下列 Kaspersky Endpoint Security 元件操作的資訊：
     - 行為偵測。
     - 弱點利用防禦。
     - 主機入侵防禦。
     - 檔案威脅防護。
     - Web 威脅防護。
     - 郵件威脅防護。
     - 網路威脅防護。
     - BadUSB 攻擊防護。
   - **控制元件報告**。包含關於下列 Kaspersky Endpoint Security 元件操作的資訊：
     - 應用程式控制。
     - 裝置控制。
     - Web 控制。
   - **資料加密報告**。包含關於已完成的資料加密工作的資訊。
   - **掃描工作報告**。包含關於以下已完成掃描工作的資訊：
     - 完整掃描。
     - 關鍵區域掃描。
     - 自訂掃描。

     僅當選中**"所有報告"**核取方塊時，才會移除已完成的完整性檢查工作的相關資訊。
   - **"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。

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

*要配置事件日誌設定，請執行以下操作：*

1. 開啟程式設定視窗。
2. 在視窗左側的“**一般設定**”區域中，選取“**介面**”。

Kaspersky Endpoint Security 介面的設定顯示在視窗右側。

3. 在**"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日誌設定的元件或工作。

5. 選定**"儲存於本機日誌中"**和**"儲存於 Windows 事件日誌中"**列中相關事件旁的核取方塊。

   已在**"儲存於本機日誌中"**欄中選中核取方塊的事件將顯示在**"卡巴斯基事件日誌"**區域中的**"應用程式和服務日誌"**中。已在**"儲存於 Windows 事件日誌中"**欄中選中核取方塊的事件將顯示在**"應用程式"**區域中的**"Windows 日誌"**中。若要開啟事件日誌，請點擊**"開始 → 控制台 → 管理 → 事件檢視器"**。

   事件中可能包括以下使用者資料：Kaspersky Endpoint Security 掃描的檔案的路徑；Kaspersky Endpoint Security 修改的登錄檔項的路徑；Microsoft Windows 使用者名稱；使用者開啟的網頁的位址。

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. 在視窗左側的**"一般設定"**區域中，選取**"介面"**。

   Kaspersky Endpoint Security 介面的設定顯示在視窗右側。

3. 在**"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**"在螢幕上通知"**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**"透過電子郵件通知"**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。

   事件中可能包括以下使用者資料：Kaspersky Endpoint Security 掃描的檔案的路徑；Kaspersky Endpoint Security 修改的登錄檔項的路徑；Microsoft Windows 使用者名稱；使用者開啟的網頁的位址。

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. 在**"電子郵件通知設定"**的視窗上，點選**"確定"**。

11. 在**"通知"**視窗中點擊**"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**"一般設定"**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 。

# 管理備份

本節包含有關如何設定和管理備份的說明。

## 關於備份

"*備份*"是在解毒過程中刪除或修改的檔案備份副本的清單。*備份副本*是指對檔案進行病毒清除或移除前建立的檔案副本。檔案的備份副本以特定格式儲存並且不會帶來威脅。

檔案的備份副本儲存在 ProgramData\Kaspersky Lab\KES\QB 資料夾中。

管理員群組中的使用者已被授予存取該資料夾的權限。其帳戶用於安裝 Kaspersky Endpoint Security 的使用者被授予該資料夾的有限存取權限。

Kaspersky Endpoint Security 不提供設定使用者存取權限以備份檔案副本的功能。

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，可以嘗試將檔案從其備份副本還原到其原始資料夾中。

如果 Kaspersky Endpoint Security 在卡巴斯基安全管理中心管理下執行，則檔案的備份副本可能會傳送至卡巴斯基安全管理中心管理伺服器。有關在卡巴斯基安全管理中心管理檔案的備份副本的更多詳細資訊，請參閱《卡巴斯基安全管理中心說明》系統。

## 配置備份設定

您可以按如下方式配置備份區設定：

- 配置備份區中的檔案副本的最長儲存期。

  備份區中的檔案副本的預設最長儲存期限是 30 天。最長儲存期限超出後，Kaspersky Endpoint Security 將刪除備份區中最舊的檔案。您可以取消時間限制或者變更最大檔案儲存期限。

- 設定備份區的最大容量。

  預設情況下，備份區的最大容量為 100 MB。當達到最大容量後，Kaspersky Endpoint Security 將自動刪除備份區中最舊的檔案，以便不會超出最大容量。您可以取消備份區容量限制或者變更最大容量。

## 配置備份區中的檔案的最長儲存期

*要配置備份區中的檔案的最長儲存期：*

1. 開啟程式設定視窗。
2. 在視窗的左側的**一般設定** 區域中，選擇 **報告和儲存**。
3. 請執行以下操作之一：

- 如果您希望限制備份區中的檔案副本的儲存期，請在視窗右側的**"備份"**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，指定備份區中的檔案副本的最長儲存期。備份區中的檔案副本的預設最長儲存期限是 30 天。

- 如果您希望取消備份區中的檔案副本的儲存期限制，請在視窗右側的**"備份"**區域中清除**"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。

## 設定備份區的最大容量

*要設定備份區的最大容量：*

1. 開啟程式設定視窗。

2. 在視窗的左側的**一般設定** 區域中，選擇 **報告和儲存**。

3. 請執行以下操作之一：

   - 如果您希望限制備份區的總容量，可以選取**"備份"**區域中視窗右側的**"最大儲存容量"**核取方塊，在**"最大儲存容量"**核取方塊右側的欄位中指定備份區的最大容量。

     預設情況下，組成檔案備份副本的資料的最大儲存容量是 100 MB。

   - 如果您希望刪除備份區的容量限制，則清空**"備份區設定"**區域中視窗右側的**"最大儲存容量"**核取方塊。

   預設情況下，備份區容量無限制。

4. 要儲存變更，請點擊**"儲存"**按鈕。

## 復原和移除備份區中的檔案

如果在檔案中偵測到惡意程式碼，Kaspersky Endpoint Security 將封鎖此檔案、為其指定*"已感染"*狀態，並將其副本放到"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*）。

當應用程式設定中設定的儲存條件後，Kaspersky Endpoint Security 將自動刪除備份區中的所有檔案副本，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

  對於檔案的備份副本，顯示檔案的原始資料夾位置。檔案原始資料夾位置中可能包含個人資料。

- 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。

您可以將所選備份檔案的相關資訊複製到剪貼簿。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**"全部選取"**。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

如果將位於同一資料夾中具有相同名稱但內容不同的多個檔案移至備份區，則只能復原最後放入備份區的檔案。

*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. 點擊應用程式主視窗下方的**"儲存"**按鈕。

   **"備份"**視窗將開啟。
3. 如果您希望從備份區中還原所有檔案，則在**"備份"**視窗中從任何檔案的內容功能表中選取**"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。
4. 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"**視窗上的表格中，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**"全部選取"**。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. 點擊應用程式主視窗下方的“**儲存**”按鈕。
3. “**備份**”視窗將開啟。
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**”視窗上的表格中，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“**全部選取**”。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

本節包含有關配置 Kaspersky Endpoint Security 一般設定的資訊。

# 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 Lab 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：

- 行為偵測。
- 弱點利用防禦。
- 主機入侵防禦。
- 檔案威脅防護。
- Web 威脅防護。
- 郵件威脅防護。
- 掃描工作

### 受信任應用程式清單

*受信任應用程式清單*包含應用程式的檔案和網路活動（包括可疑活動）以及對系統登錄檔的存取不受 Kaspersky Endpoint Security 的監控。預設情況下，Kaspersky Endpoint Security 將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。

從掃描中排除受信任應用程式可避免 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. 在視窗左側的**"一般設定"**區域中，選取**"排除"**。

   排除設定將顯示在視窗右側。
3. 在**"掃描排除項目和信任區域"**區域中點擊**"設定"**按鈕。

   **"信任區域"**視窗中將開啟，並顯示**"掃描排除項目"**標籤。

4. 點擊**"新增"**按鈕。

**"掃描排除項目"**視窗將開啟。在該視窗中，您可以使用**"內容"**區域中的一個或多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。

   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**"掃描排除項目"**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 Lab 病毒百科全書的分類輸入威脅類型的名稱，或威脅類型名稱的遮罩。

   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. 要從掃描中排除帶有指定名稱的物件：

   a. 在**"內容"**區域中選取**"物件雜湊"**核取方塊。

   b. 點選**"掃描排除項目描述"**區域中的**"輸入物件雜湊"**連結，開啟**"物件雜湊"**視窗。

   c. 按照 Kaspersky 病毒百科全書中的分類輸入物件的 SHA256 哈希，或透過點擊**"瀏覽"**按鈕選擇檔案。

   d. 在**"物件雜湊"**視窗中點選**"確定"**。

   所新增物件雜湊的連結將顯示在**"掃描排除項目"**視窗的**"掃描排除項目描述"**區域中。

8. 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。

9. 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。

10. 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**“信任區域”**視窗中的**“掃描排除項目”**標籤的表中。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。

11. 在**“信任區域”**的視窗上，點選**“確定”**。

12. 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. 在視窗左側的**“一般設定”**區域中，選取**“排除”**。

   排除設定將顯示在視窗右側。

3. 在**“掃描排除項目和信任區域”**區域中點擊**“設定”**按鈕。

   **“信任區域”**視窗中將開啟，並顯示**“掃描排除項目”**標籤。

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。

     **“掃描排除項目”**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. 在視窗左側的**“一般設定”**區域中，選取**“排除”**。

   排除設定將顯示在視窗右側。

3. 在**“掃描排除項目和信任區域”**區域中點擊**“設定”**按鈕。

   **“信任區域”**視窗中將開啟，並顯示**“掃描排除項目”**標籤。

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. 在視窗左側的**"一般設定"**區域中，選取**"排除"**。
   排除設定將顯示在視窗右側。
3. 在**"掃描排除項目和信任區域"**區域中點擊**"設定"**按鈕。
   **"信任區域"**視窗中將開啟，並顯示**"掃描排除項目"**標籤。
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. 在視窗左側的**"一般設定"**區域中，選取**"排除"**。
   排除設定將顯示在視窗右側。
3. 在**"掃描排除項目和信任區域"**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**"受信任應用程式"**標籤。
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路徑，在標準的 Microsoft Windows**"開啟"**視窗中點擊**"開啟"**。

這些操作將開啟**"應用程式掃描排除項目"**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**。
- **不監控應用程式活動**。
- **不繼承父程序限制（應用程式）的限制**。
- **不監控子應用程式活動**。
- **不封鎖與程式介面互動**。
- **不掃描網頁資料流量**。

> 如果使用 Kaspersky Endpoint Security 管理外掛程式新增受信任應用程式，必須在不對**"不掃描網路流量"**設定使用遮罩的情況下指定應用程式才能起作用。

b. 在**"應用程式掃描排除項目"**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. **"應用程式掃描排除項目"**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**"應用程式掃描排除項目"**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**"應用程式掃描排除項目"**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. 在視窗左側的**"一般設定"**區域中，選取**"排除"**。
排除設定將顯示在視窗右側。

3. 在**"掃描排除項目和信任區域"**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**"受信任應用程式"**標籤。

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. 在視窗左側的**"一般設定"**區域中，選取**"排除項目"**。
排除項目設定將顯示在視窗右側。

3. 在“**掃描排除項目和信任區域**”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“**受信任的系統憑證儲存**”下拉清單中，選取必須被 Kaspersky Endpoint Security 視為受信任的系統儲存。
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。

# 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，“郵件威脅防護”和“Web 威脅防護”元件將監控透過特定協定傳輸並經過使用者電腦上開放的特定 TCP 和 UDP 連接埠的資料流。例如，“郵件威脅防護”元件分析透過 SMTP 傳輸的資訊，而“Web 威脅防護”元件分析透過 HTTP 和 FTP 傳輸的資訊。

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。隨後“郵件威脅防護”和“Web 威脅防護”元件在監控網路流量時會特別注意這些連接埠和應用程式。

## 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. 在視窗左側的“**一般設定**”區域中，選取“**排除**”。

排除設定將顯示在視窗右側。

3. 在**"要監控的連接埠"**區域中，選取**"監控全部的連接埠"**選項。

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

*建立受監控的網路連接埠清單*

1. 開啟程式設定視窗。

2. 在視窗左側的**"一般設定"**區域中，選取**"排除"**。
   排除設定將顯示在視窗右側。

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**"監控全部的連接埠"**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 建立監控全部的連接埠的應用程式清單中包含 FTP 協定接收或傳送資料的應用程式。

*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. 在視窗左側的**"一般設定"**區域中，選取**"排除"**。
   排除設定將顯示在視窗右側。
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**"監控指定應用程式的所有連接埠"**核取方塊。
6. 在**"監控指定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。

# 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。

# 啟用和停用自我防護

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. 在視窗左側的"**一般設定**"區域中選取"**應用程式設定**"。
   Kaspersky Endpoint Security 的進階設定顯示在視窗右側。
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。

# 啟用與停用遠端控制防護

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. 在視窗左側的"**一般設定**"區域中選取"**應用程式設定**"。
   Kaspersky Endpoint Security 的進階設定顯示在視窗右側。

3. 請執行以下操作之一：

   - 如果要啟用遠端控制防護，請選取**"停用系統服務的外部管理"**核取方塊。
   - 如果要停用遠端控制防護，請清除**"停用系統服務的外部管理"**核取方塊。

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. 在視窗左側的**"一般設定"**區域中，選取**"排除"**。
   排除設定將顯示在視窗右側。
3. 在**"掃描排除項目和信任區域"**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**"受信任應用程式"**標籤。
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尋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路徑，在標準的 Microsoft Windows**"開啟"**視窗中點擊**"開啟"**。

   這些操作將開啟**"應用程式掃描排除項目"**視窗。

8. 選取**"不監控應用程式活動"**核取方塊。
9. 在**"應用程式掃描排除項目"**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 的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 的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
- 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 和硬碟磁碟機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 將使用特殊的進階解毒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。排程外檔案伺務器的重新啟動，可能會導致檔案伺務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解毒技術的原因。

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. 在視窗左側的"**一般設定**"區域中，選取"**排除**"。
   排除設定將顯示在視窗右側。
3. 在"**需偵測的物件**"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**
   - **可能會帶來危害的封裝檔案**
   - **多重封裝檔案**
5. 點擊"**確定**"。
   "**需偵測的物件**"視窗將關閉。在"**需偵測的物件**"區域中，所選物件類型在"**已啟用對以下類型物件的偵測**"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. 在視窗左側的“**一般設定**”區域中選取“**應用程式設定**”。
   Kaspersky Endpoint Security 的進階設定顯示在視窗右側。
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**”方塊。
   - 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**”方塊。
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. 在政策內容視窗中，開啟“**應用程式設定**”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“**立即執行進階解毒技術**”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. 在政策內容視窗中，開啟“**應用程式設定**”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的病毒掃描群組工作的內容中，取消“**立即執行進階解毒技術**”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. 在視窗左側的"**一般設定**"區域中選取"**應用程式設定**"。
   Kaspersky Endpoint Security 的進階設定顯示在視窗右側。
3. 在"**效能**"區域中：
   - 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
     - 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。
4. 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. 在視窗左側的"**一般設定**"區域中選取"**應用程式設定**"。
   Kaspersky Endpoint Security 的進階設定顯示在視窗右側。
3. 在"**效能**"區域中：
   - 如果您要啟用允許其他應用程式使用資源的模式，請選取"**將資源讓給其他應用程式**"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
- 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**"將資源讓給其他應用程式"**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。

4. 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 11 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 KLAdmin。

## 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. 在視窗左側的**"一般設定"**區域中，選取**"介面"**。

   Kaspersky Endpoint Security 介面的設定顯示在視窗右側。
3. 在**"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**"全部選取"**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：

   - **配置應用程式設定**。
   - **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。

11. 要儲存變更，請在應用程式設定視窗中點擊**"儲存"**按鈕。

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**"記住目前連線的密碼"**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. 在視窗左側的**"一般設定"**區域中，選取**"介面"**。

   Kaspersky Endpoint Security 介面的設定顯示在視窗右側。

3. 在**"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。

6. 要儲存變更，請在應用程式設定視窗中點擊**"儲存"**按鈕。

   **"密碼檢查"**視窗將開啟。

7. 在**"使用者名稱"**欄位中輸入使用者名稱。

8. 在 **密碼** 欄位輸入 Kaspersky Endpoint Security 的存取密碼。

9. 點擊**"確定"**。

## 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. 在視窗左側的**"一般設定"**區域中，選取**"介面"**。

   Kaspersky Endpoint Security 介面的設定顯示在視窗右側。

3. 在**"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。

   **"密碼檢查"**視窗將開啟。

9. 在**"使用者名稱"**欄位中輸入使用者名稱。

10. 在 **密碼** 欄位輸入舊的 Kaspersky Endpoint Security 存取密碼。

11. 點擊**"確定"**。

## 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"**標籤。
4. 在屬於使用者請求暫時密碼的電腦的上下文功能表中，選取**"內容"**。

   **"內容: "<電腦名稱>"**視窗將開啟。
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 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**"應用程式設定 "<應用程式名稱>""**視窗的**"一般設定"**區域中，選取**"介面"**。
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"**視窗的**"暫時密碼"**區域中，點擊**"設定"**按鈕。

   如果在該電腦上執行的卡巴斯基安全管理中心政策中為卡巴斯基安全管理中心啟用了密碼防護，則該按鈕可用。

   **"建立暫時密碼"**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。

## 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。
- 透過卡巴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. 在視窗左側的**"一般設定"**區域中選取**"管理設定"**。
   視窗右側將顯示設定管理功能。
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. 在視窗左側的**"一般設定"**區域中選取**"管理設定"**。
   視窗右側將顯示設定管理功能。
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。

# 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，新增金鑰以及啟動和停止更新和掃描工作。

在有關應用程式控制的章節中，您可以找到有關使用卡巴斯基安全管理中心管理應用程式控制規則的資訊。

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說明》。

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. 開啟卡巴斯基安全管理中心管理主控台。
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**”標籤。
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並選取“**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 Lab 程式清單將顯示在用戶端電腦內容視窗的右側。
7. 選擇“Kaspersky Endpoint Security for Windows”。
8. 請執行以下操作：
   - 啟動應用程式，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 的內容功能表中選取“**內容**”或者點擊 Kaspersky 應用程式清單中下方的“**內容**”按鈕。
     “**Kaspersky Endpoint Security for Windows (11.0.0) 應用程式設定**”視窗開啟。
     b. 在“**一般**”區域中點擊視窗右側的“**執行**”。
   - 要停止 Kaspersky Endpoint Security，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 的內容功能表中選取“**內容**”或者點擊 Kaspersky 應用程式清單中下方的“**內容**”按鈕。
     “**Kaspersky Endpoint Security for Windows (11.0.0) 應用程式設定**”視窗開啟。
     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. 開啟卡巴斯基安全管理中心管理主控台。
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. 選擇"Kaspersky Endpoint Security for Windows"。
8. 請執行以下操作之一：
   - 從 Kaspersky Endpoint Security 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。

   **"Kaspersky Endpoint Security for Windows 應用程式設定"**視窗開啟。
9. 在**"一般設定"**區域中，配置 Kaspersky Endpoint Security 的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"區域"相同。《卡巴斯基安全管理中心說明手冊》提供了這些區域的說明。

   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**"一般設定"**區域中配置應用程式設定時，您將無法編輯它們。
10. 要儲存變更，請在**"Kaspersky Endpoint Security for Windows 應用程式設定"**視窗中點擊**"確定"**。

# 工作管理

本章節介紹如何管理 Kaspersky Endpoint Security 的工作。有關透過卡巴斯基安全管理中心進行工作管理的詳細資訊，請參閱《卡巴斯基安全管理中心說明手冊》。

## 關於 Kaspersky Endpoint Security 工作

卡巴斯基安全管理中心將透過工作控制 Kaspersky Lab 程式活動。這些工作將實施主要的管理功能，例如授權檔案安裝、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。

  如果安裝了 Kaspersky Endpoint Security 的電腦上未安裝"應用程式控制"元件，該電腦上的清單工作將返回錯誤。

- **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"**標籤。
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**"本機工作"**區域中，選擇**"工作管理"**子區域。
7. 在**"工作管理"**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。

   有關套用卡巴斯基安全管理中心政策的詳細資訊，請參閱《卡巴斯基安全管理中心說明手冊》。

# 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"**標籤。
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。

- 在用戶端電腦的右鍵選單中，選取**"內容"**，然後在出現的**"內容：<電腦名稱>"**視窗的**"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"**標籤。
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。

## 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"**標籤。
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** 標籤。
   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"**標籤。
   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"**標籤。
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並選取**"內容"**。
   開啟用戶端電腦的內容視窗。
6. 選擇 **工作** 標籤。
   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. 點擊**"內容"**按鈕。
   **"內容：<本機工作名稱>"**視窗將開啟。
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. 若要儲存變更，請在**"內容：<本機工作名稱>"**視窗中點擊**"確定"**。

12. 若要儲存變更，請在**"內容：<電腦名稱>"**視窗中點擊**"確定"**。

*要編輯群組設定，請執行以下操作：*

1. 開啟卡巴斯基安全管理中心管理主控台。

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"**標籤。
   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. 右鍵點擊以顯示群組工作的右鍵選單並選取**"內容"**。
   **"內容：<群組工作名稱>"**視窗將開啟。

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. 開啟卡巴斯基安全管理中心管理主控台。

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合工作。

3. 右鍵點擊以顯示電腦集合工作的右鍵選單並選取**"內容"**。
   **"內容：<電腦集合工作名稱>"**視窗開啟。

4. 在**"內容：<電腦集合工作名稱>"**視窗，選取**"設定"**選項。

5. 編輯電腦集合的工作設定。

6. 若要儲存變更，請在**"內容：<電腦集合工作名稱>"**視窗中點擊**"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巴斯基安全管理中心是一樣的。有關詳細說明，請參閱《卡巴斯基安全管理中心說明手冊》。**"設定"**區域包含 Kaspersky Endpoint Security for Windows 的具體設定。其內容取決於選定工作或工作類型。

## 清查工作設定

您可以為清查工作配置以下設定：

- **清查範圍**。在此區域中，您可以指定在清查過程中掃描的檔案系統物件。這些物件可以是本機資料夾、網路資料夾、卸除式磁碟機、硬碟磁碟機或整個電腦。

- **清查工作設定**。在此區域中，您可以配置以下設定：

  - **在電腦空閒時掃描**。此核取方塊用於啟用/停用當電腦資源有限時暫停清查工作的功能。如果螢幕防護關閉及電腦解除，Kaspersky Endpoint Security 將暫停清查工作。

- **DLL 模組清查**。此核取方塊用於啟用/停用對 DLL 模組資料進行分析並將分析結果傳遞給管理伺服器的功能。
- **指令碼檔案清查**。此核取方塊用於啟用/停用對包含指令碼的檔案的資料進行分析並將分析結果傳遞給管理伺服器的功能。
- **進階**。點擊此按鈕將開啟"**進階設定**"視窗，在其中可以配置以下設定：
  - **只掃描新增及變更的檔案**。此核取方塊用於啟用/停用只掃描新檔案和自上次清查以來已修改的檔案的模式。
  - **略過掃描時間超過以下值的檔案**。此核取方塊用於啟用/停用掃描單個檔案的時長限制。經過在右側欄位中設定的時間段後，Kaspersky Endpoint Security 停止掃描檔案。
  - **掃描壓縮檔案**。此核取方塊用於啟用/停用掃描 RAR、ARJ、ZIP、CAB、LHA、JAR 和 ICE 壓縮檔是否存在可執行檔。
  - **掃描分發套件**。此核取方塊用於啟用/停用在執行清查工作時掃描分發套件。
  - **不解壓大型複合檔案**。

    如果選擇此核取方塊，Kaspersky Endpoint Security 不會掃描檔案大小超過"**最大檔案大小**"欄位中指定的值的複合檔案。

    如果清除該核取方塊，Kaspersky Endpoint Security 將掃描所有大小的複合檔案。

    > 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。

  - **最大檔案大小**。Kaspersky Endpoint Security 不解壓大小超過此欄位中指定的值的檔案。此值的單位為百萬位元組。

# 管理政策

本章節將敘述如何建立並設定您的 Kaspersky Endpoint Security 政策。有關使用卡巴斯基安全管理中心政策管理 Kaspersky Endpoint Security 的詳細資訊，請參閱《卡巴斯基安全管理中心說明手冊》。

# 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。

變更用戶端電腦上的應用程式設定的能力透過政策內容中這些設定的"鎖"狀態確定：

- 關閉的"鎖"(🔒) 的含義如下：
  - 卡巴斯基安全管理中心會封鎖從用戶端電腦上的 Kaspersky Endpoint Security 介面對與此鎖有關的設定進行變更。在所有用戶端電腦上，Kaspersky Endpoint Security 均使用這些設定的相同值，即，政策內容中

定義的值。

- 對於嵌套的管理群組和啟用了**"繼承頂級政策的設定"**功能的從屬管理伺服器，卡巴斯基安全管理中心會封鎖在這些政策的內容中對與此鎖有關的設定進行變更。將使用頂級政策內容中定義的這些設定的值。

- 開啟的"鎖"( ) 的含義如下：

  - 卡巴斯基安全管理中心允許從用戶端電腦上的 Kaspersky Endpoint Security 介面對與此鎖有關的設定進行變更。在每台用戶端電腦上，Kaspersky Endpoint Security 將根據這些設定的本機值執行（如果該元件已啟用）。

  - 對於嵌套的管理群組和啟用了**"繼承頂級政策的設定"**功能的從屬管理伺服器，卡巴斯基安全管理中心允許在這些政策的內容中對與此鎖有關的設定進行變更。這些設定的值不取決於頂層政策中指定的值。

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：

- 關鍵威脅防護。功能範圍包括"檔案威脅防護"、"郵件威脅防護"、"Web 威脅防護"、"網路威脅防護"、"防火牆"和"掃描工作"元件。

- 應用程式控制。功能範圍包括"應用程式控制"元件。

- 裝置控制。功能範圍包括"裝置控制"元件。

- 加密。功能範圍包括"完整磁碟加密"和"檔案級加密"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。

- 進階威脅防護。功能範圍包括 KSN 設定以及"行為偵測"、"弱點利用防禦"、"主機入侵防禦"和"修復引擎"元件。

- 一般功能。此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、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說明手冊》。

## 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"**標籤。
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"**標籤。
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 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**"進階威脅防護"**、**"關鍵威脅防護"**和**"安全控制"**區域包含防護和控制元件的設定，**"資料加密"**區域包含完整磁碟加密、檔案級加密以及卸除式磁碟機加密的設定，**"端點感應器"**區域包含"端點感應器"元件的設定，**"本機工作"**區域包含本機工作和群組工作的設定，**"一般設定"**區域包含應用程式設定。

   如果在卡巴斯基安全管理中心的**"介面設定"**視窗中選中相應核取方塊，將顯示政策設定中的資料加密和控制元件設定。預設情況下，將選中這些核取方塊。

6. 編輯政策設定。

7. 若要儲存您的變更，請在"**內容：<政策名稱>**"視窗中點擊"**確定**"。

## 政策內容視窗中的安全等級指示器

安全等級指示器顯示在"**內容: <政策名稱>**"視窗的頂部。此指示器的值可能如下：

- **高防護等級**。如果啟用以下類別的所有元件，指示器為此值並變為綠色：
  - **緊急**。此類別包含以下元件：
    - 檔案威脅防護。
    - 行為偵測。
    - 弱點利用防禦。
    - 修復引擎。
  - **重要**。此類別包含以下元件：
    - 卡巴斯基安全網路。
    - Web 威脅防護。
    - 郵件威脅防護。
    - 主機入侵防禦。
- **中防護等級**。如果停用了一個重要元件，指示器為此值並變為黃色。
- **低防護等級**。在以下任意一種情況下，指示器為此值並變為紅色：
  - 一個或多個關鍵元件被停用。
  - 兩個或更多重要元件被停用。

如果指示器顯示**中防護等級**或**低防護等級**，指示器的右側將顯示"**瞭解更多資訊**"連結，此連結將開啟"**建議的防護元件**"視窗。在此視窗中，可以啟用任一建議的防護元件。

## 設定應用程式介面的顯示

*要設定應用程式介面的顯示：*

1. 開啟卡巴斯基安全管理中心管理主控台。

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應用程式介面顯示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**"標籤。

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"**一般設定**"區域中，選取"**介面**"子區域。

7. 在"**使用者互動**"區域中執行以下操作之一：

   - 如果您要在用戶端電腦上顯示以下介面元素，請選擇"**顯示應用程式介面**"核取方塊：
     - 包含"**開始**"功能表中的應用程式名稱的資料夾
     - Microsoft Windows 工作通知列上的 Kaspersky Endpoint Security 圖示。
     - 彈出通知

     如果選中此核取方塊，使用者可以從應用程式介面檢視應用程式設定，並可以根據可用權限變更應用程式設定。

   - 如果您希望在用戶端電腦上隱藏 Kaspersky Endpoint Security 的所有跡象，請清除"**顯示應用程式介面**"核取方塊。

8. 如果您希望在已安裝 Kaspersky Endpoint Security 的用戶端電腦上顯示簡化的應用程式介面，請在"**使用者互動**"區域中選中"**簡化的應用程式介面**"核取方塊。

   如果選中"**顯示應用程式介面**"核取方塊，則此核取方塊可用。

## 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。

- "應用程式控制"封鎖了某個應用程式的啟動。

  請求允許啟動被封鎖的應用程式的郵件範本在 Kaspersky Endpoint Security 介面的"應用程式控制"區域中提供。

- Web 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"Web 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外出政策執行在安裝了 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

"應用程式控制"、"裝置控制"和"Web 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。

  如果安裝了 Kaspersky Endpoint Security 的電腦套用了政策或外出政策，將以電子郵件的形式傳送使用者資訊。

*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"**使用者請求**"。
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。

# 從命令列管理應用程式

您可以從命令列管理 Kaspersky Endpoint Security。可以執行 `HELP` 指令來檢視用於管理應用程式的指令清單。要閱讀特定指令的語法，請輸入 `HELP <指令>`。

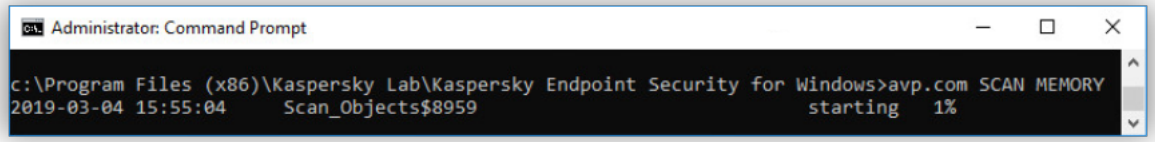
## 指令

*要從命令列管理 Kaspersky Endpoint Security：*

1. 以管理員身分執行命令列解譯器 (cmd.exe)。
2. 轉到 Kaspersky Endpoint Security 可執行檔所在資料夾。
3. 要執行指令，請輸入：

```
avp.com <指令> [選項]
```

結果，Kaspersky Endpoint Security 將執行該指令（參見下圖）。




從命令列管理應用程式

## SCAN。病毒掃描

執行病毒掃描工作。

指令語法

```
SCAN [<掃描範圍>] [<偵測到威脅後的操作>] [<檔案類型>] [<掃描排除項目>] [/R[A]:<報告檔案>] [<掃描技術>] [/C:<掃描設定檔案>]
```

| **掃描範圍** | |
|---|---|
| <要掃描的檔案> | 以空格分隔的檔案和資料夾清單。長路徑必須用引號括起來。短路徑（MS-DOS 格式）不需要用引號括起來。範例：<br>• `"C:\Program Files (x86)\Example Folder"` – 長路徑。<br>• `C:\PROGRA~2\EXAMPL~1` – 短路徑。 |
| `/ALL` | 執行“*完整掃描*”工作。Kaspersky Endpoint Security 掃描以下物件： |

| | |
|---|---|
| | • 內核記憶體<br>• 作業系統啟動時載入的物件<br>• 開機磁區<br>• 作業系統備份儲存區<br>• 所有磁碟機和卸除式裝置 |
| /MEMORY | 掃描內核記憶體。 |
| /STARTUP | 掃描在作業系統啟動時載入的物件。 |
| /MAIL | 掃描 Outlook 郵箱。 |
| /REMDRIVES | 掃描卸除式磁碟機。 |
| /FIXDRIVES | 掃描硬碟磁碟機。 |
| /NETDRIVES | 掃描網路磁碟機。 |
| /QUARANTINE | 掃描 Kaspersky Endpoint Security 備份區中的檔案。 |
| /@:<file list.lst> | 掃描清單中的檔案和資料夾。清單中的每個檔案都必須另起一行。長路徑必須用引號括起來。短路徑（MS-DOS 格式）不需要用引號括起來。範例：<br>• `"C:\Program Files (x86)\Example Folder"` – 長路徑。<br>• `C:\PROGRA~2\EXAMPL~1` – 短路徑。 |

| **偵測到威脅後的動作** | |
|---|---|
| /i0 | 通知。如果選擇此選項，Kaspersky Endpoint Security 會在偵測到受感染檔案時將這些檔案的相關資訊新增到活動威脅清單。 |
| /i1 | 解毒；如果解毒失敗則通知。如果選擇該選項，Kaspersky Endpoint Security 將自動對已經偵測到的所有受感染的檔案執行解毒操作。如果無法進行解毒，Kaspersky Endpoint Security 會將偵測到的受感染檔案的相關資訊新增到活動威脅清單。 |
| /i2 | 解毒；如果解毒失敗則刪除。如果選擇該選項，Kaspersky Endpoint Security 將自動對已經偵測到的所有受感染的檔案執行解毒操作。如果解毒失敗，Kaspersky Endpoint Security 將刪除檔案。<br>預設情況下已選擇此操作。 |
| /i3 | 解毒偵測到的已感染檔案。如果解毒失敗，則刪除已感染檔案。如果無法解毒或刪除已感染檔案，還會刪除複合檔案（例如，存檔）。 |
| /i4 | 刪除已感染檔案。如果無法刪除已感染檔案，還會刪除複合檔案（例如，存檔）。 |
| /i8 | 一偵測到威脅就提示使用者執行操作。 |
| /i9 | 掃描完成後提示使用者執行操作。 |

| **檔案類型** | |
|---|---|
| | |

| | |
|---|---|
| /fe | 根據副檔名掃描檔案。如果啟用該設定，則 Kaspersky Endpoint Security 僅掃描被感染的檔案。此時，系統將根據檔案的副檔名確定檔案格式。 |
| /fi | 根據格式掃描檔案。如果啟用該設定，則 Kaspersky Endpoint Security 僅掃描被感染的檔案。在掃描檔案以尋找惡意程式碼之前，系統將分析檔案的內部頭以確定檔案的格式（例如，.txt、.doc 或 .exe）。在掃描過程中還將考慮檔案的副檔名。 |
| /fa | 所有檔案。如果啟用該設定，Kaspersky Endpoint Security 將毫無例外地掃描所有檔案（所有格式和副檔名）。<br>這是預設設定。 |

| 掃描排除項目 | |
|---|---|
| -e:a | RAR、ARJ、ZIP、CAB、LHA、JAR 和 ICE 壓縮檔案將從掃描範圍中排除。 |
| -e:b | 郵件資料庫、傳入和傳出電子郵件將從掃描範圍中排除。 |
| -E:<檔案遮罩> | 與檔案遮罩比對的檔案將從掃描範圍中排除。範例：<br>• 遮罩 *.exe 將包括具有 exe 副檔名的檔案的所有路徑。<br>• 遮罩 example 將包括名為 EXAMPLE 的檔案的所有路徑。 |
| -e:<秒> | 掃描時間長於指定時間限制（以秒為單位）的檔案將從掃描範圍中排除。 |
| -es:<百萬位元組> | 大於指定大小限制（以百萬位元組為單位）的檔案將從掃描範圍中排除。 |

| 將事件儲存到報告檔案模式 | |
|---|---|
| /R:<報告檔案> | 僅將關鍵事件儲存到報告檔案中。 |
| /RA:<報告檔案> | 將所有事件儲存到報告檔案中。 |

| 掃描技術 | |
|---|---|
| /iChecker=on\|off | 該技術透過將某些檔案排除在掃描範圍外來提高掃描速度。該技術將使用特殊演算法將檔案排除在掃描範圍之外，該演算法會考慮 Kaspersky Endpoint Security 資料庫的發佈日期、檔案的上次掃描日期以及對掃描設定的任何修改。 |
| /iSwift=on\|off | 該技術透過將某些檔案排除在掃描範圍外來提高掃描速度。該技術將使用特殊演算法將檔案排除在掃描範圍之外，該演算法會考慮 Kaspersky Endpoint Security 資料庫的發佈日期、檔案的上次掃描日期以及對掃描設定的任何修改。iSwift 技術是對用於 NTFS 檔案系統的 iChecker 技術的增強版。 |

| 進階設定 | |
|---|---|
| /C:<包含病毒掃描設定的檔案> | 包含病毒掃描工作設定的檔案。必須手動建立該檔案並以 TXT 格式儲存。該檔案可以具有以下內容：[<掃描範圍>] [<偵測到威脅後的操作>] [<檔案類型>] [<掃描排除項目>] [/R[A]:<報告檔案>] [<掃描技術>]。 |

範例：

- avp.com SCAN /R:log.txt /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files" C:\Downloads\test.exe
- avp.com SCAN /C:scan_settings.txt

# UPDATE。更新資料庫和程式模組

執行"*更新*"工作。

指令語法

```
UPDATE [local] ["<更新來源>"] [/R[A]:<報告檔案>] [/C:<包含更新設定的檔案>]
```

| **更新工作設定** | |
|---|---|
| 本機 | 開始安裝應用程式後自動建立的*更新*工作。您可以在本機應用程式介面或卡巴斯基安全管理中心的主控台中變更"*更新*"工作的設定。如果未配置此設定，則 Kaspersky Endpoint Security 會使用預設設定或命令中指定的設定來開始"*更新*"工作。您可以按以下方式配置"更新"工作設定：<br>• `UPDATE` 使用預設設定啟動"*更新*"工作：更新來源是 Kaspersky 更新伺服器，帳戶是 System 以及其他預設設定。<br>• `UPDATE local` 啟動安裝後自動建立的"*更新*"工作（預定義工作）。<br>• `UPDATE <更新設定>` 使用手動定義的設定（如下）啟動"*更新*"工作。 |

| **更新來源** | |
|---|---|
| "<更新來源>" | HTTP 或 FTP 伺服器的位址，或具有更新套件的共用資料夾的位址。只能指定一個更新來源。如果未指定更新來源，則 Kaspersky Endpoint Security 將使用預設來源 – Kaspersky 更新伺服器。 |

| **將事件儲存到報告檔案模式** | |
|---|---|
| `/R:<報告檔案>` | 僅將關鍵事件儲存到報告檔案中。 |
| `/RA:<報告檔案>` | 將所有事件儲存到報告檔案中。 |

| **進階設定** | |
|---|---|
| `/C:<包含更新設定的檔案>` | 包含"*更新*"工作設定的檔案。必須手動建立該檔案並以 TXT 格式儲存。該檔案可以具有以下內容：`["<更新來源>"] [/R[A]:報告檔案>]`。 |

範例：

```
avp.com UPDATE local

avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

# ROLLBACK。回溯上次更新

回溯上次病毒資料庫更新。這允許您在必要時將資料庫和應用程式模組回溯到以前的版本，例如，當新資料庫版本包含無效簽章而導致 Kaspersky Endpoint Security 封鎖了安全的應用程式時。

指令語法

```
ROLLBACK [/R[A]:<報告檔案>]
```

| 將事件儲存到報告檔案模式 | |
|---|---|
| /R:<報告檔案> | 僅將關鍵事件儲存到報告檔案中。 |
| /RA:<報告檔案> | 將所有事件儲存到報告檔案中。 |

範例：

```
avp.com ROLLBACK /RA:rollback.txt
```

## TRACES。偵錯

啟用/停用偵錯。預設情況下，停用偵錯。

指令語法

```
TRACES on|off [<偵錯等級>] [<進階設定>]
```

| 偵錯等級 | |
|---|---|
| <偵錯等級> | 偵錯詳細等級。可用值：<br>• `100`（關鍵）。僅包含有關致命錯誤的訊息。<br>• `200`（高）。有關所有錯誤的訊息，包括致命錯誤。<br>• `300`（診斷）。有關所有錯誤的訊息以及警告。<br>• `400`（重要）。所有錯誤訊息、警告和其他資訊。<br>• `500`（一般）。有關所有錯誤的訊息和警告，以及有關正常模式下應用程式操作的詳細資訊（預設）。<br>• `600`（低）。所有訊息。 |

| 進階設定 | |
|---|---|
| `all` | 使用 `dbg`、`file` 和 `mem` 參數執行指令。 |
| `dbg` | 使用 OutputDebugString 函數並儲存偵錯檔案。OutputDebugString 函數將字串傳送到應用程式調試器以在螢幕上顯示。有關詳細資訊，請存取 *MSDN 網站*。 |
| `file` | 儲存一個偵錯檔案（無大小限制）。 |
| `rot` | 將偵錯儲存到有限數量的大小有限的檔案中，並在達到最大大小時覆蓋舊檔案。 |

| | |
|---|---|
| mem | 將偵錯儲存到 dump 檔案。 |

範例：

- avp.com TRACES on 500
- avp.com TRACES on 500 dbg
- avp.com TRACES off
- avp.com TRACES on 500 dbg mem
- avp.com TRACES off file

## START。啟動設定檔

啟動設定檔（例如，更新資料庫或啟用防護元件）。

指令語法

START <設定檔> [/R[A]:<報告檔案>]

| **設定檔** | |
|---|---|
| <設定檔> | 設定檔名稱。*設定檔*是 Kaspersky Endpoint Security 元件、工作或功能。您可以執行 HELP START 指令來檢視可用設定檔清單。 |

| **將事件儲存到報告檔案模式** | |
|---|---|
| /R:<報告檔案> | 僅將關鍵事件儲存到報告檔案中。 |
| /RA:<報告檔案> | 將所有事件儲存到報告檔案中。 |

範例：

avp.com START Scan_Objects

## STOP。停止設定檔

停止執行設定檔（例如，停止掃描、停止卸除式磁碟機掃描或停用防護元件）。

要執行此指令，必須啟用密碼防護。使用者必須具有以下權限：**配置應用程式設定**、**停用防護元件**和**停用控制元件**。

指令語法

STOP <設定檔> /login=<使用者名稱> /password=<密碼>

| 設定檔 | |
|---|---|
| <設定檔> | 設定檔名稱。*設定檔*是 Kaspersky Endpoint Security 元件、工作或功能。您可以執行 `HELP STOP` 指令來檢視可用設定檔清單。 |

| 身分驗證 | |
|---|---|
| `/login=<使用者名稱> /password=<密碼>` | 有關被授予所需密碼防護權限的使用者帳戶的資訊。 |

## STATUS。設定檔狀態

顯示應用程式設定檔的狀態資訊（例如，`正在執行`或`已完成`）。您可以輸入 `HELP STATUS` 指令來檢視可用設定檔清單。

Kaspersky Endpoint Security 還會顯示有關服務設定檔狀態的資訊。聯絡卡巴斯基技術支援時，可能需要有關服務設定檔狀態的資訊。

指令語法

```
STATUS [<設定檔>]
```

## STATISTICS。設定檔操作統計

檢視有關應用程式設定檔的統計資訊（例如，掃描持續時間或偵測到的威脅數）。您可以執行 `HELP STATISTICS` 指令來檢視可用設定檔清單。

指令語法

```
STATISTICS <設定檔>
```

## RESTORE。還原檔案

您可以將檔案從備份區還原到原始資料夾。如果指定路徑中已存在具有相同名稱的檔案，則檔案名會附加尾碼"-copy"。要還原的檔案將保留其原始名稱進行複製。

要執行此指令，必須啟用密碼防護。使用者必須具有"**從備份區還原**"權限。

*備份區*儲存保留在解毒過程中刪除或修改的檔案的副本。*備份副本*是指對檔案進行病毒清除或移除前建立的檔案副本。檔案的備份副本以特定格式儲存並且不會帶來威脅。

檔案的備份副本儲存在 C:\ProgramData\Kaspersky Lab\KES\QB 資料夾中。

管理員群組中的使用者被授予存取該資料夾的完整權限。其帳戶用於安裝 Kaspersky Endpoint Security 的使用者被授予該資料夾的有限存取權限。

Kaspersky Endpoint Security 不提供設定使用者存取權限以備份檔案副本的功能。

指令語法

```
RESTORE [/REPLACE] <檔案名稱> /login=<使用者名稱> /password=<密碼>
```

| **進階設定** | |
|---|---|
| /REPLACE | 覆蓋現有檔案。 |
| <檔案名稱> | 要還原的檔案的名稱。 |

| **身分驗證** | |
|---|---|
| /login=<使用者名稱> /password=<密碼> | 有關被授予所需密碼防護權限的使用者帳戶的資訊。 |

範例：

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

## EXPORT。匯出應用程式設定

將 Kaspersky Endpoint Security 設定匯出到檔案。該檔案將位於 C:\Windows\SysWOW64 資料夾。

指令語法

```
EXPORT <設定檔> <檔案名稱>
```

| **設定檔** | |
|---|---|
| <設定檔> | 設定檔名稱。*設定檔*是 Kaspersky Endpoint Security 元件、工作或功能。您可以執行 `HELP EXPORT` 指令來檢視可用設定檔清單。 |

| **要匯出的檔案** | |
|---|---|
| <檔案名稱> | 應用程式設定將匯出到的檔案的名稱。您可以將 Kaspersky Endpoint Security 設定匯出為 DAT 或 CFG 設定檔、TXT 文字檔案或 XML 檔。 |

範例：

- `avp.com EXPORT ids ids_config.dat`
- `avp.com EXPORT fm fm_config.txt`

## IMPORT。匯入應用程式設定

從使用 `EXPORT` 指令建立的檔案中匯入 Kaspersky Endpoint Security 的設定。

要執行此指令，必須啟用密碼防護。使用者必須具有以下權限：**配置應用程式設定**、**停用防護元件**和**停用控制元件**。

指令語法

```
IMPORT <檔案名稱> /login=<使用者名稱> /password=<密碼>
```

| **要匯入的檔案** | |
|---|---|
| <檔案名稱> | 將從中匯入應用程式設定的檔案的名稱。您可以從 DAT 或 CFG 設定檔、TXT 文字檔案或 XML 檔匯入 Kaspersky Endpoint Security 設定。 |

| **身分驗證** | |
|---|---|
| `/login=<使用者名稱> /password=<密碼>` | 有關被授予所需密碼防護權限的使用者帳戶的資訊。 |

範例：

```
avp.com IMPORT config.dat /login=KLAdmin /password=!Password1
```

## ADDKEY。套用金鑰檔案。

套用金鑰檔案以啟動 Kaspersky Endpoint Security。如果應用程式已啟動，則該金鑰將作為備用金鑰新增。

指令語法

```
ADDKEY <檔案名稱> /login=<使用者名稱> /password=<密碼>
```

| **金鑰檔案** | |
|---|---|
| <檔案名稱> | 金鑰檔案名稱。 |

| **身分驗證** | |
|---|---|
| `/login=<使用者名稱> /password=<密碼>` | 使用者帳戶憑證。只有啟用了密碼防護時，才需要輸入這些憑證。 |

範例：

```
avp.com ADDKEY file.key
```

## LICENSE。產品授權

對 Kaspersky Endpoint Security 產品授權金鑰執行操作。

要執行此指令並刪除產品授權金鑰，必須啟用密碼防護。使用者必須具有**"刪除金鑰"**權限。

指令語法

```
LICENSE <操作> [/login=<使用者名稱> /password=<密碼>]
```

| **動作** | |
|---|---|
| /ADD <檔案名稱> | 套用金鑰檔案以啟動 Kaspersky Endpoint Security。如果應用程式已啟動，則該金鑰將作為備用金鑰新增。 |
| /ADD <啟動碼> | 使用啟動碼啟動 Kaspersky Endpoint Security。如果應用程式已啟動，則該金鑰將作為備用金鑰新增。 |
| /REFRESH <檔案名稱> | 使用金鑰檔案續約產品授權。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。不能透過執行此指令新增啟動金鑰。 |
| /REFRESH <啟動碼> | 使用啟動碼續約產品授權。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。不能透過執行此指令新增啟動金鑰。 |
| /DEL /login=<使用者名稱> /password=<密碼> | 刪除產品授權金鑰。備用金鑰也將被刪除。 |

| **身分驗證** | |
|---|---|
| /login=<使用者名稱> /password=<密碼> | 有關被授予所需密碼防護權限的使用者帳戶的資訊。 |

範例：

- avp.com LICENSE /ADD file.key
- avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
- avp.com LICENSE /DEL /login=KLAdmin /password=!Password1

## RENEW。購買產品授權

開啟卡巴斯基網站以購買或續約產品授權。

## PBATESTRESET。重設預加密檢查結果

重設對 BitLocker 加密技術相容性的檢查結果。這些結果還包括對電腦與身分驗證代理的相容性的檢查。

在執行完整磁碟加密之前，應用程式會執行大量檢查以驗證是否可以使用 BitLocker 技術對電腦進行加密。如果無法加密電腦，Kaspersky Endpoint Security 會記錄有關不相容性的資訊。下次嘗試加密時，應用程式不會執行此檢查，並警告您無法進行加密。如果電腦的硬體設定已變更，則必須重設應用程式先前記錄的相容性檢查結果，以重新檢查系統硬碟磁碟機與身分驗證代理的相容性以及 BitLocker 加密技術支援。

## EXIT。結束應用程式

結束 Kaspersky Endpoint Security。應用程式將從電腦的 RAM 中移除。

要執行此指令，必須啟用密碼防護。使用者必須具有"**結束應用程式**"權限。

指令語法

```
EXIT /login=<使用者名稱> /password=<密碼>
```

## EXITPOLICY。停用政策

在電腦上停用卡巴斯基安全管理中心政策。所有 Kaspersky Endpoint Security 設定均可進行配置，包括政策中已上鎖的設定 (🔒)。

要執行此指令，必須啟用密碼防護。使用者必須具有"**停用卡巴斯基安全管理中心政策**"權限。

指令語法

```
EXITPOLICY /login=<使用者名稱> /password=<密碼>
```

## STARTPOLICY。啟用政策

在電腦上啟用卡巴斯基安全管理中心政策。將根據政策配置應用程式設定。

## DISABLE。停用防護

停用具有過期 Kaspersky Endpoint Security 產品授權的電腦上的檔案威脅防護。無法在未啟動應用程式或具有有效產品授權的電腦上執行此指令。

## SPYWARE。間諜軟體偵測

啟用/停用間諜軟體偵測。預設情況下已啟用間諜軟體偵測。

指令語法

```
SPYWARE on|off
```

## 附錄。應用程式設定檔

*設定檔*是 Kaspersky Endpoint Security 元件、工作或功能。設定檔用於從命令列管理應用程式。您可以使用設定檔執行 `START`、`STOP`、`STATUS`、`STATISTICS`、`EXPORT` 和 `IMPORT` 指令。使用設定檔，您可以配置應用程式設定（例如，`STOP DeviceControl`）或執行工作（例如，`START Scan_My_Computer`）。

以下設定檔可用：

- `BehaviorDetection` – 行為偵測。
- `DeviceControl` – 裝置控制。
- `EntAppControl` - 應用程式控制。
- `File_Monitoring` 或 `FM` – 檔案威脅防護。
- `Firewall` 或 `FW` – 防火牆。
- `HIPS` – 主機入侵防禦。
- `IDS` – 關於網路威脅防護。
- `IntegrityCheck` – 完整性檢查。
- `Mail_Monitoring` 或 `EM` – 郵件威脅防護。
- `Rollback` – 更新回溯。
- `Scan_ContextScan` – 從內容功能表掃描。
- `Scan_IdleScan` – 背景掃描。
- `Scan_Memory` - 內核記憶體掃描。
- `Scan_My_Computer` – 完整掃描。
- `Scan_Objects` – 自訂掃描。
- `Scan_Qscan` - 掃描在作業系統啟動時載入的物件。
- `Scan_Removable_Drive` – 卸除式磁碟機掃描。
- `Scan_Startup` 或 `STARTUP` – 關鍵區域掃描。
- `Updater` – 更新。
- `Web_Monitoring` 或 `WM` – Web 威脅防護。
- `WebControl` – Web 控制。

Kaspersky Endpoint Security 還支援服務設定檔。聯絡卡巴斯基技術支援時，可能需要服務設定檔。

# 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 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。

## 在使用者社區中討論卡巴斯基應用程式

如果您的問題並不急迫需要回答，您可以在我們的社區 中與 Kaspersky 專家和其他使用者討論。

在此社區中，您可以檢視現有主題，發表評論以及建立新的討論主題。

# 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。

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 Lab 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 是一個為使用 Kaspersky Lab 應用程式的公司提供的網站入口。Kaspersky CompanyAccount 入口網站設計用於透過線上請求便利使用者和 Kaspersky Lab 專家之間溝通的網頁服務。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 Lab 傳送的電子請求單，也能夠透過 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。

技術支援專家可能還需要更多相關資訊，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。

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。
- 變更所收集診斷資訊的儲存設定。
- 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送至 Kaspersky。

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。

## 建立應用程式偵錯檔案

*應用程式偵錯* - 是應用程式所執行的各種動作的詳細記錄和應用程式執行期間的各種事件的訊息。

*要建立應用程式偵錯檔案：*

1. 在應用程式主視窗中，點擊**"支援"**按鈕。

   **"支援"**視窗將開啟。

2. 在**"支援"**視窗中，點擊**"系統偵錯"**按鈕。

   開啟**"技術支援資訊"**視窗。

3. 要啟動偵錯過程，請在**"應用程式偵錯"**下拉清單中選取以下項目之一：

   - **已啟用**

     選取此項目可啟用偵錯。

- **使用循環**。

  選擇此項目可啟用偵錯並限制偵錯檔案的最大數量以及每個偵錯檔案的最大大小。如果已寫入最大數量的最大大小的偵錯檔案，最早的偵錯檔案將被刪除，以便可以寫入新的偵錯檔案。

  如果選擇此項目，您可以為以下欄位指定值：

  - **用於迴圈的最大檔案數**

    在此欄位中可以指定寫入的偵錯檔案的最大數量。

  - **每個檔案的最大大小**

    在此欄位中可以指定寫入的每個偵錯檔案的最大容量。

4. 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)**”。

5. 重新啟動 Kaspersky Endpoint Security。

6. 要停止偵錯過程，請返回“**技術支援資訊**”視窗，並在“**應用程式偵錯**”下拉清單中選取“**已停用**”。

您也可以在從命令列安裝應用程式時（包括使用 setup.ini 檔案）建立偵錯檔案。

## 啟用和停用傾印寫入

*要啟用和停用傾印寫入：*

1. 開啟程式設定視窗。

2. 在左側，選擇“**一般設定**”區域中的“**應用程式設定**”。

   應用程式設定將顯示在視窗右側。

3. 在“**偵錯資訊**”區域中點擊“**設定**”按鈕。

   將開啟“**偵錯資訊**”視窗。

4. 請執行以下操作之一：

   - 如果您希望應用程式寫入應用程式的傾印，請選中“**啟用傾印寫入**”核取方塊。

   - 如果您不希望應用程式寫入應用程式的傾印，請清除“**啟用傾印寫入**”核取方塊。

5. 在“**偵錯資訊**”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。

## 啟用和停用防護傾印檔案和偵錯檔案

傾印檔案和偵錯檔案包含作業系統的資訊,可能還包含使用者資料。為了防止未經授權地存取此類資料，您可以啟用防護傾印檔案和偵錯檔案。

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傾印檔案和偵錯檔案的使用者可以存取傾印檔案。
- 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傾印檔案和偵錯檔案：*

1. 開啟程式設定視窗。
2. 在左側，選擇**"一般設定"**區域中的**"應用程式設定"**。
   應用程式設定將顯示在視窗右側。
3. 在**"偵錯資訊"**區域中點擊**"設定"**按鈕。
   將開啟**"偵錯資訊"**視窗。
4. 請執行以下操作之一：
   - 如果您希望啟用防護，則選取**"啟用傾印和偵錯檔案防護"**核取方塊。
   - 如果您希望停用防護，則清空**"啟用傾印和偵錯檔案防護"**核取方塊。
5. 在**"偵錯資訊"**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傾印檔案和偵錯檔案即使該功能被停用也會保持為防護狀態。

## 傾印檔案的內容和儲存

使用者個人應對所收集資料的安全負責，特別是控制和限制對電腦上儲存的所收集資料的存取。

只要應用程式在使用中，就會在電腦中儲存傾印檔案，當應用程式被移除後，傾印檔案將被永久移除。傾印檔案儲存在 ProgramData\Kaspersky Lab 資料夾中。

傾印檔案包含此檔案建立時 Kaspersky Endpoint Security 處理程序的工作記憶體的所有相關資訊。傾印檔案中還可能包含個人資料。

## 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。

只要應用程式在使用中，就會在電腦中儲存偵錯檔案，當應用程式被移除後，偵錯檔案將被永久移除。

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`。

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。

所有偵錯檔案都包含下列一般資料：

- 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，如果它們公開傳送。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。
- 郵件主旨、ID、社群網路寄件者網頁的寄件者名稱和位址。當啟用 Web 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 偵錯檔案包含卡巴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。
- "郵件威脅防護"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。

# 詞彙表

## OLE 物件

附加的檔案或嵌入到其他檔案中的檔案。使用 Kaspersky Lab 程式可掃描 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 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，此類別檔案是可執行檔，例如副檔名為 .com、.exe 和 .dll 的檔案。這類別檔案中，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。由 Kaspersky Lab 專家建立的網頁位址清單。它會定期更新，並且會包含在 Kaspersky Lab 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。

## 工作

Kaspersky Lab 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

Kaspersky Lab 提供給使用者一個包含啟動檔案或啟動碼的文件。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 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 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 專家的建議，此防護方式永遠處於啟用狀態。

## 病毒資料庫

資料庫包含在 Kaspersky Lab 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 Lab 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

卡巴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 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 Lab 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

一個卡巴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使用者登入、密碼和連線連接埠；此外網頁資源位址的字元將從大寫變更為小寫。

在防護元件的執行中，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 Lab 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。

## 釣魚網頁位址資料庫

Kaspersky Lab 專家確定與釣魚相關的網頁位址清單。此資料庫會定期更新，並且會包含在 Kaspersky Lab 應用程式分發套件中。

## 防護範圍

在執行時被基本威脅防護元件持續掃描的物件。不同元件的防護範圍有不同的參數。

## 驗證代理

可啟動硬碟磁碟機加密後，讓您完成身分驗證以存取加密的硬碟磁碟機並載入作業系統啟動的介面。

# 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稱為 legal_notices.txt 的檔案，並儲存在應用程式的安裝資料夾中。

# 商標通知

註冊商標和服務標誌均屬於各自所有者。

Adobe、Acrobat、Flash 和 Shockwave 是 Adobe Systems Incorporated 在美國和/或其他國家/地區的商標或註冊商標。

FireWire 是 Apple, Inc. 在美國和其他國家/地區註冊的商標。

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/或其他國家/地區的商標或註冊商標。

Citrix 和 Citrix Provisioning Services 是 Citrix Systems, Inc. 和/或其子公司在美國和/或其他國家/地區的專利局註冊的商標。

dBase 是 dataBased Intelligence, Inc. 的商標

EMC 和 SecurID 是 EMC Corporation 在美國和/或其他國家/地區註冊的商標。

IBM 是 International Business Machines Corporation 在世界多個地區註冊的商標。

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。

Microsoft、Access、BitLocker、Excel、Internet Explorer、LifeCam Cinema、MultiPoint、Outlook、PowerPoint、PowerShell、Visual C++、Visual Basic、Visual FoxPro、Windows、Windows Store 和 Windows Server 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。

Java 和 JavaScript 是 Oracle Corporation 和/或其分公司的註冊商標。