ESET SMART SECURITY 9

使用者手冊

(適用於產品版品 9.0 和更新版本)

Microsoft® Windows® 10 / 8.1 / 8 / 7 / Vista / XP

按一下這裡以下載此文件的最新版本。

ENJOY SAFER TECHNOLOGY™

ESET SMART SECURITY

全球客戶支援 :www.eset.com/support

修訂 :10/6/2015

內容

1. ESET Smart Security

ESET Smart Security 代表確實整合電腦安全性的新方法。最新版的 ThreatSense® 掃描引擎結合了量身訂做的個人防火牆與反垃圾郵件模組，增進速度及精確度同時確保電腦受到防護。 其成品就是能夠持續監控可能危害您電腦的攻擊及惡意軟體的智慧型系統。

ESET Smart Security 是完整的安全性解決方案，結合最大防護與最低系統使用量。我們進階的技術使用人工智慧預防病毒、間諜程式、特洛伊木馬、蠕蟲、廣告程式、Rootkit 及其他威脅的入侵，而且不會妨礙系統效能或中斷電腦運作。

功能與優點

重新設計的使用者介面	第 9 版的使用者介面已根據使用性測試的結果大幅重新設計並簡化。所有 GUI 文字內容和通知均已謹慎檢閱，使用者介面現在支援由右至左書寫的語言，例如希伯來文和阿拉伯文。**線上說明**現已整合至 ESET Smart Security 並提供動態更新支援內容。
病毒及間諜程式防護	主動偵測及清除多種已知和未知的病毒、蠕蟲、特洛伊木馬程式及 Rootkit。**進階啟發式**甚至可標記前所未見的惡意軟體，讓您避免不明威脅的危害，並在威脅造成任何傷害之前使其失去效力。**Web 存取防護**和**網路釣魚防護**會監視 Web 瀏覽器與遠端伺服器 (含 SSL) 之間的通訊。**電子郵件用戶端防護**可控制透過 POP3(S) 和 IMAP(S) 通訊協定收到的電子郵件通訊。
定期更新	定期更新病毒資料庫與程式模組是確保電腦有最高度安全性的最佳方法。
ESET LiveGrid® (具有雲端功能聲譽)	您可以直接從 ESET Smart Security 檢查執行中處理程序與檔案的聲譽。
裝置控制	自動掃描所有 USB 隨身碟、記憶卡及 CD/DVD。根據媒體類型、製造商、大小與其他特性封鎖可移除的媒體。
HIPS 功能	您可以更詳細地自訂系統的行為，並為系統登錄、作用中的處理程序與程式指定規則，也可以微調您的安全性狀態。
玩家模式	讓所有快顯視窗、更新或其他佔用大量系統資源的活動延後顯示或進行，保留系統資源供遊戲和其他全螢幕活動使用。

ESET Smart Security 中的功能

銀行和付款防護	銀行和付款防護提供安全瀏覽器供您在存取線上銀行交易或付款閘道時使用，以確保所有線上交易均在受信任且安全的環境下進行。
支援網路簽章	網路簽章可讓您快速識別並封鎖進入及離開使用者裝置的惡意流量，例如 Bot 和弱點封包。此功能可視為殭屍網路防護的增強功能。
智慧型防火牆	可防止未授權使用者存取您的電腦，並利用您的個人資料。
ESET 垃圾郵件防護	垃圾郵件佔所有電子郵件通訊的 80 %。垃圾郵件防護可用來針對此問題進行防護。
ESET 防盜	ESET 防盜 當電腦遺失或遭竊能夠擴大使用者層級的安全性。一旦使用者安裝 ESET Smart Security 及 ESET 防盜，Web 介面將列出其裝置。Web 介面可讓使用者管理其裝置上的 ESET 防盜 配置和管理員及防盜功能。
家長控制	阻擋各種網站類別，讓您的家人免受潛在冒犯性網站內容的危害。

您需要啟用授權才可使用 ESET Smart Security 的功能。建議您在 ESET Smart Security 過期前數週即更新授權。

1.1 第 9 版中的新增功能

ESET Smart Security 的第 9 版具備下列改良功能：

- **銀行和付款防護** - 為線上交易提供額外一層保護。
- **支援網路簽章** - 網路簽章可讓您快速識別並封鎖進入及離開使用者裝置、與 Bot 和弱點封包相關的惡意流量。
- **重新設計的使用者介面** - ESET Smart Security 的圖形使用者介面已全部重新設計，可視度更高，而且使用起來更直覺化。介面現在支援由右至左書寫的語言，例如希伯來文和阿拉伯文。**線上說明**現已整合至 ESET Smart Security 並提供動態更新支援內容。
- **更快且更可靠的安裝**- 包含在安裝後 20 分鐘或電腦重新開機時會自動執行的初次掃描。

如需關於 ESET Smart Security 功能的詳細資訊，請閱讀以下 ESET 知識庫文章：
ESET Smart Security 9 和 ESET NOD32 Antivirus 9 有哪些新增功能？

1.2 系統需求

為使 ESET Smart Security作業順暢，系統應符合下列軟硬體需求：

支援的處理器：Intel® 或 AMD x86-x64
作業系統：Microsoft® Windows® 10/8.1/8/7/Vista/XP SP3 32 位元/XP SP2 64 位元/Home Server 2003 SP2 32 位元/Home Server 2011 64 位元

1.3 預防

當您使用電腦時，尤其是在瀏覽網際網路時，請記得世界上沒有任何防毒系統可以完全消除 入侵 與攻擊. 為達到最大的保護性及方便性，正確地使用防毒解決方案並遵守數項有用的規則是很重要的：

定期更新

根據 ThreatSense 的統計資料顯示，每天都有好幾千種新奇的入侵活動被創造出來，目的為通過現有的安全措施，為其作者帶來利益，而且全由其他使用者買帳。ESET 研究實驗室的專家每天都會分析那些威脅，準備並發佈更新，以不斷提高對我們使用者的防護層級。為確保這些更新能發揮最大效益，您系統上的更新必須正確配置。如需有關如何設定更新的資訊，請參閱更新設定一章。

下載安全修補程式

惡意軟體的作者通常會利用各種系統弱點來增加散播惡意程式碼的效力。軟體公司瞭解這一點，因此密切注意其應用程式是否出現任何弱點，並定期發佈安全更新，以排除潛在的威脅。當這些安全更新發佈時請務必下載。Microsoft Windows 與 Internet Explorer 等 Web 瀏覽器就是會有安全更新定期發佈的兩個範例程式。

備份重要資料

惡意程式的作者通常不在乎使用者的需求，且惡意程式的活動常會導致作業系統整體故障，並遺失重要資料。請定期將重要及敏感資料備份至外部來源，例如：DVD 或外接硬碟機，這是很重要的。當系統發生故障時，這可讓您更容易且更快復原資料。

定期掃描電腦中的病毒

即時檔案系統防護模組會偵測更多已知與未知的病毒、蠕蟲、特洛伊木馬程式及 Rootkit。這表示每次您存取或開啟檔案時，便會掃描檔案中是否有惡意軟體活動。建議您每個月執行電腦完整掃描至少一次，因為惡意軟體簽章會不斷改變，病毒資料庫也會每天自行更新。

遵循基本安全規則

這是最有用且最有效的規則 - 務必要小心謹慎。現在有很多入侵活動都需要使用者介入才能執行及散佈。如果您在開啟新檔案時能夠小心謹慎，就不需耗費龐大的時間和精力來清除入侵活動。以下是一些實用的方針：

- 不要造訪具有多重快顯視窗及閃動廣告的可疑網站。
- 安裝免費程式、轉碼器封裝等時，要很小心。僅使用安全的程式，僅造訪安全的網際網路網站。
- 開啟電子郵件附件時，要很謹慎，尤其是大量傳送的郵件，以及來自不明寄件者的郵件。
- 不要使用系統管理員帳戶來處理電腦的日常工作。

2. 安裝

：

有許多方法可以在您的電腦上安裝 ESET Smart Security。安裝的方法各式各樣，取決於各國家和各種經銷方式：

- Live Installer 可以從 ESET 網站上下載。此安裝套件普遍適用於所有語言 (請選擇想要的語言)。Live Installer 本身是一個小型的檔案；安裝 ESET Smart Security 時所需要的其他檔案都將自動下載。

- 離線安裝 - 從 CD/DVD 安裝時則使用這種檔案類型。其所使用的 *.msi* 檔案比 Live Installer 更大，且不需要網際網路連線或是其他檔案即可完成安裝。

重要 在您安裝 ESET Smart Security 之前，請確定電腦上未安裝任何其他防毒程式。如果在單一電腦上安裝兩個或兩個以上的防毒解決方案，會造成彼此衝突。我們建議您解除安裝系統上的任何其他防毒程式。請參閱 ESET 知識庫文章以取得一般防毒軟體的解除安裝程式工具清單 (提供英文與其他語言版本)。

2.1 Live Installer

：

當您下載 *Live Installer* 安裝套件後，按兩下安裝檔案，並遵循安裝程式視窗中的逐步指示。

重要 此安裝類型需要連接至網際網路。

從下拉式功能表中選取您所需的語言，並按一下 **[下一步]**。需要一點時間下載安裝檔。

同意 **[使用者授權合約]** 後，系統會提示您設定 **[ESET LiveGrid®]**。ESET LiveGrid® 有助於確保迅速持續通知 ESET 新入侵的相關資訊，以快速保護其客戶。此系統允許您將新威脅提交到 ESET 研究實驗室，並對其進行分析、處理及新增到病毒資料庫。

依預設，**[我想要參加 ESET LiveGrid® (建議)]** 選項會選取，這將啟動此功能。

安裝程序的下一步是配置潛在不需要應用程式的偵測作業。潛在不需要應用程式不一定是惡意的，但是可能會對作業系統的行為造成負面影響。請參閱潛在不需要應用程式一章以取得詳細資訊。

按一下 **[安裝]** 以啟動安裝程序。

2.2 離線安裝

一旦啟動離線安裝程式 (.msi) 套件，安裝精靈將引導您進行設定程序。

首先，程式會檢查是否有 ESET Smart Security 的新版本可使用。如果找到更新版本，則會在安裝程序的第一個步驟通知您。如果您選取 **[下載並安裝新版本]** 選項，則系統會下載新版本，並且繼續安裝。只有存在比安裝中版本更新的版本時才會顯示此核取方塊。

下一個步驟便會顯示「使用者授權合約」。請閱讀合約並按一下 **[接受]** 以認知您已接受使用者授權合約。在接受後，會繼續安裝。

如需有關安裝步驟 **[ThreatSense]** 及 **[潛在不需要應用程式偵測]** 的指示，請遵循先前所提之章節的指示 (請參閱「Live Installer」)。

2.2.1 進階設定

在選取 **[進階設定]** 之後，系統將提示您選取安裝的位置。依預設，程式會安裝至以下目錄：

C:\Program Files\ESET\ESET Smart Security

按一下 **[瀏覽...]** 變更此位置 (不建議)。

按一下 **[下一步]** 以配置您的網際網路連線。如果您使用 Proxy 伺服器，必須予以正確配置，才能使病毒資料庫運作。如果不確定您是否使用 Proxy 伺服器連線至網際網路，請選取 **[使用與 Internet Explorer 相同的設定 (建議)]**，並按一下 **[下一步]**。如果您未使用 Proxy 伺服器，請選取 **[我不使用 Proxy 伺服器]**。

若要配置 Proxy 伺服器設定，請選取 **[我使用 Proxy 伺服器]**，然後按一下 **[下一步]**。將 Proxy 伺服器的 IP 位址或 URL 輸入到 **[位址]** 欄位中。在 **[連接埠]** 欄位中，指定 Proxy 伺服器接受連線所在的連接埠 (依預設為 3128)。如果 Proxy 伺服器需要驗證，則必須輸入有效的 **[使用者名稱]** 及 **[密碼]**，授與 Proxy 伺服器的存取權限。如果需要，也可以從 Internet Explorer 複製 Proxy 伺服器設定。若要這樣做，請按一下 **[套用]** 並確認選項。

自訂安裝可讓您定義如何在系統上處理自動程式更新。按一下 **[變更...]** 以存取進階設定。

如果您不想要更新程式元件，請選取 **[絕不更新程式元件]**。選取 **[下載程式元件前詢問]**，以便在每次系統嘗試下載程式元件時顯示確認視窗。若要自動下載程式元件升級，請選取 **[一律更新程式元件]**。

附註： 程式元件更新後，通常需要重新啟動。我們建議選取 **[必要時不通知即重新啟動電腦]**。

下一個安裝視窗提供設定密碼以保護程式設定的選項。選取 **[使用密碼保護配置設定]**，並在 **[新密碼]** 與 **[確認新密碼]** 欄位中輸入您的密碼。需要此密碼才能變更或存取 ESET Smart Security 的設定。兩個密碼欄位相符時，按一下 **[下一步]** 以繼續進行。

若要完成接下來的安裝步驟 **[ThreatSense]** 及 **[潛在不需要應用程式偵測]**，請遵循「Live Installer」一節中的指示進行 (請參閱「Live Installer」)。

接下來，請選取 ESET 個人防火牆的過濾模式。ESET Smart Security 個人防火牆提供四種過濾模式。防火牆行為的變更係以選取的模式為根據。過濾模式還影響需要使用者介入的層級。

若要停用在安裝完成後通常會執行的安裝完成後先掃描以檢查惡意程式碼，請取消選取 **[啟用安裝後掃描]** 旁的核取方塊。按一下 **[準備安裝]** 視窗中的 **[安裝]** 完成安裝。

2.3 常見安裝問題

若安裝期間發生問題，請參閱我們的常見安裝錯誤和解決方案以尋找您問題的解決方案。

2.4 產品啟動

完成 安裝之後，系統將提示您啟動您的產品。

有數個方法可啟動您的產品。啟動視窗中可使用的特定啟動狀況會視國家及發行方法 (CD/DVD、ESET 網頁等) 而異：

- 如果您購買零售版本的產品，請使用 **授權金鑰** 來啟動產品。授權金鑰通常位於產品包裝內或背部。您必須輸入提供的授權金鑰，才能成功啟動產品。授權金鑰 - 採用格式為 XXXX-XXXX-XXXX-XXXX-XXXX 或 XXXX-XXXXXXXX 的唯一字串，可供您識別授權擁有者和啟動授權。
- 如果您在購買之前想要評估 ESET Smart Security，請選取 **[免費試用版授權]**。請輸入您的電子郵件地址和國家，以在有限的時間內啟動 ESET Smart Security。測試授權將傳送至您的電子郵件。每位客戶只能啟動一次試用版授權。
- 如果您沒有授權但想要購買授權，請按一下 [購買授權]。此選項會將您重新引導至當地的 ESET 經銷商網站。

如果您想要快速評估我們的產品，而不想立即啟動，或您想要稍後啟動您的產品，請選取 **[稍後啟動]**。

您可以直接從程式啟動 ESET Smart Security 的副本。以滑鼠右鍵按一下系統匣中的 ESET Smart Security 圖示  ，並從程式功能表選取 **[啟動產品]**。

2.5 輸入授權金鑰

若要取得最佳功能，自動更新程式是很重要的。唯有在 **[更新設定]** 中輸入正確的 **[授權金鑰]**，才能達到此目的。

如果您未在安裝期間輸入您的授權金鑰，您現在可以輸入。在主要程式功能表視窗中，按一下 **[說明及支援]**，再按一下 **[啟動授權]**，然後將接收隨附於 ESET 安全性產品的授權資料輸入到 [產品啟動] 視窗中。

當您輸入**授權金鑰**時，請務必照實輸入：

- 格式為 XXXX-XXXX-XXXX-XXXX-XXXX 的唯一字串，可供您用來識別授權擁有者和啟動授權。

我們建議您從您的註冊電子郵件中複製並貼上授權金鑰以確保正確無誤。

2.6 升級至最新版本

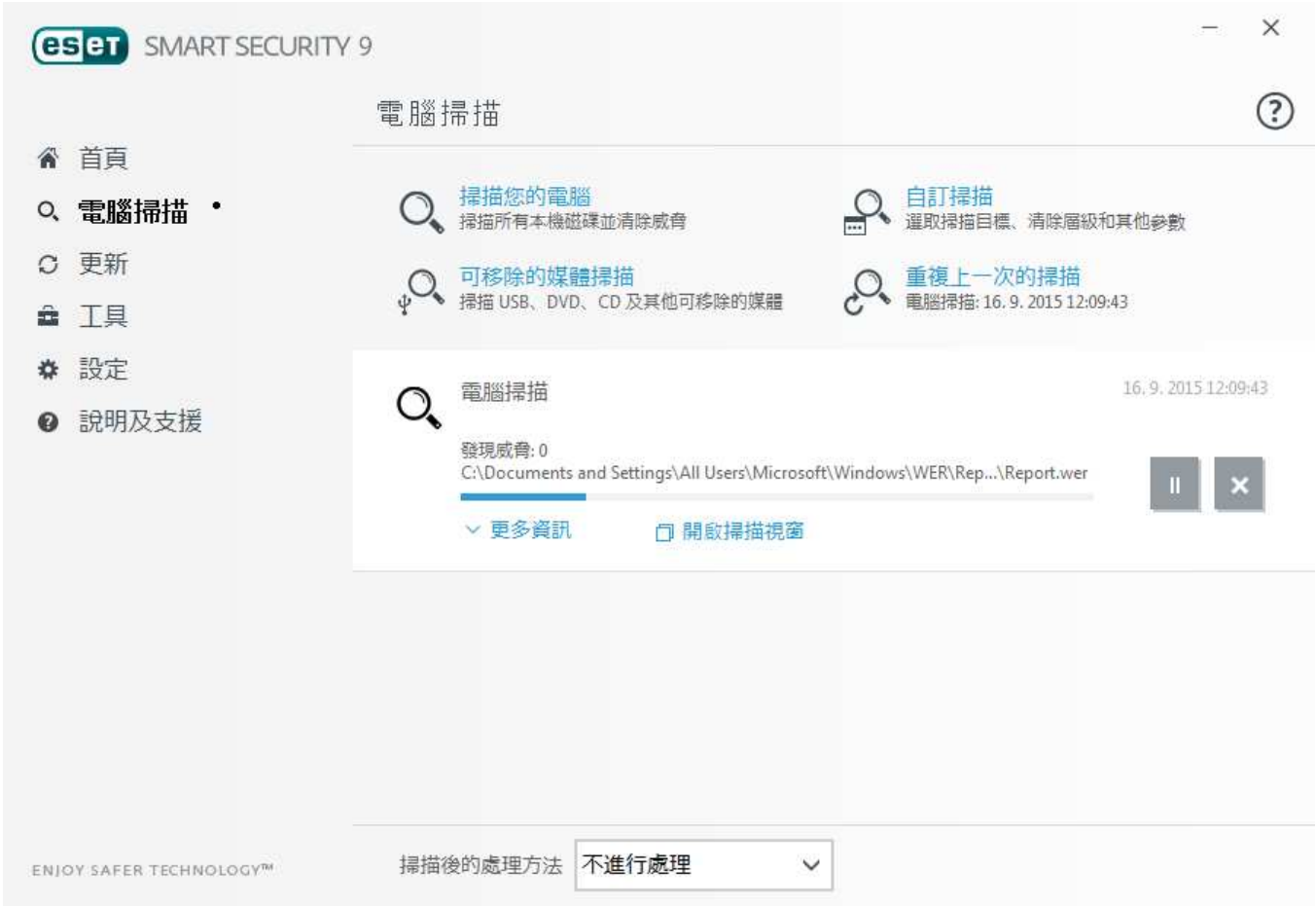
新推出的 ESET Smart Security 版本已改善或修正自動程式模組更新無法解決的問題。透過以下幾種方式即可升級為新版：

1. 透過程式更新自動升級。
   由於程式更新會散佈至所有使用者，而且可能影響某些系統配置，因此會在經過長時間測試後才發行，以針對所有可能的系統配置完成平順的運作。如果您需要在此發行後立即升級為新版本，請使用以下其中一種方法。
2. 在主要程式視窗中，按一下**檢查更新]** (位於 **[更新]** 區段)。
3. 透過下載新版本並安裝覆蓋舊版的方式手動升級。

2.7 安裝完成後先掃描

在安裝 ESET Smart Security 之後，電腦會在安裝或重新啟動後的 20 分鐘進行掃描以檢查惡意程式碼。

您也可以按一下 **[電腦掃描]** > **[掃描您的電腦]** 從主要程式視窗手動啟動電腦掃描。如需有關電腦掃描的詳細資訊，請參閱電腦掃描一節。



3. 初學者手冊

本章提供 ESET Smart Security 及其基本設定的初始概觀。

3.1 主要程式視窗

ESET Smart Security 的主要程式視窗分為兩個主要區段。右側的主要視窗顯示對應從左側的主要功能表中所選取選項的資訊。

以下為主要功能表中選項的說明：

首頁 - 提供與 ESET Smart Security 的防護狀態有關的資訊。

[電腦掃描] - 配置並啟動電腦掃描，或建立自訂掃描。

更新 - 顯示有關病毒資料庫更新的資訊。

工具 - 可存取防護記錄檔案、防護統計、即時監控、執行中的處理程序、網路連線、、排程器 ESET SysInspector 及 ESET SysRescue。

設定 - 選取此選項以調整您電腦、網際網路、網路防護和安全性工具的安全性層級。.

說明及支援 - 可存取說明檔案、ESET 知識庫、ESET 網站和連結，以提交支援要求。

[首頁] 畫面包含您電腦目前防護層級的重要相關資訊。此狀態視窗會顯示經常使用的 ESET Smart Security 功能。您也可以在此處找到有關程式最新更新以及到期日的資訊。

綠色圖示和綠色的 **[最嚴格的防護]** 狀態表示已確保最嚴格的防護。

如果程式運作不正常怎麼辦？

如果作用中的防護模組運作正常，其防護狀態圖示會顯示為綠色。紅色驚嘆號或橙色通知圖示表示不確定為最嚴格的防護。同時還會在 **[首頁]** 下方顯示各模組防護狀態的額外資訊，以及還原完整防護的建議解決方案。若要變更個別模組的狀態，請按

一下 **[設定]** 並選取所需的模組。

紅色圖示及紅色的「最嚴格的防護」狀態不一定表示嚴重問題。
有幾個原因會顯示此狀態，例如：

- **產品未啟動** - 您可以按一下防護狀態下方的 **[啟動產品]** 或 **[立即購買]** 從 **[首頁]** 啟動 ESET Smart Security。
- **病毒資料庫已過期** - 在數次嘗試更新病毒資料庫失敗之後，就會出現此錯誤。我們建議您檢查更新設定。此錯誤最常見的原因是輸入的驗證資料錯誤或連線設定的配置錯誤。
- **病毒及間諜程式防護已停用** - 您可以按一下 **[啟動所有病毒及間諜程式防護模組]**，以重新啟用病毒及間諜程式防護。
- **ESET 個人防火牆已停用** - 此問題也會在桌面上的 **[網路]** 項目旁邊以安全性通知表示。您可以按一下 **[啟用防火牆]**，以重新啟用網路防護。
- **授權已到期** - 這是由紅色的防護狀態圖示所表示。您的授權過期後即無法更新程式。請按照警告視窗中的指示更新您的授權。

橙色圖示表示防護有限。例如，程式更新可能發生問題或授權可能接近到期日期。
有幾個原因會顯示此狀態，例如：

- **防盜最佳化警告** - 裝置未針對 ESET 防盜 進行最佳化。例如，您的電腦可能未建立幽靈帳戶 (當您將裝置標記為遺失時自動觸發的安全性功能)。您可使用 ESET 防盜 Web 介面中的最佳化功能建立一個幽靈帳戶。
- **玩家模式已啟用** - 啟用玩家模式有潛在的安全性風險。啟用此功能會停用所有快顯視窗並停止任何已排程的工作。
- **您的授權即將到期** - 這是由在系統時鐘旁顯示驚嘆號的防護狀態圖示所表示。您的授權到期後，程式將無法更新，[防護] 狀態圖示將變成紅色。

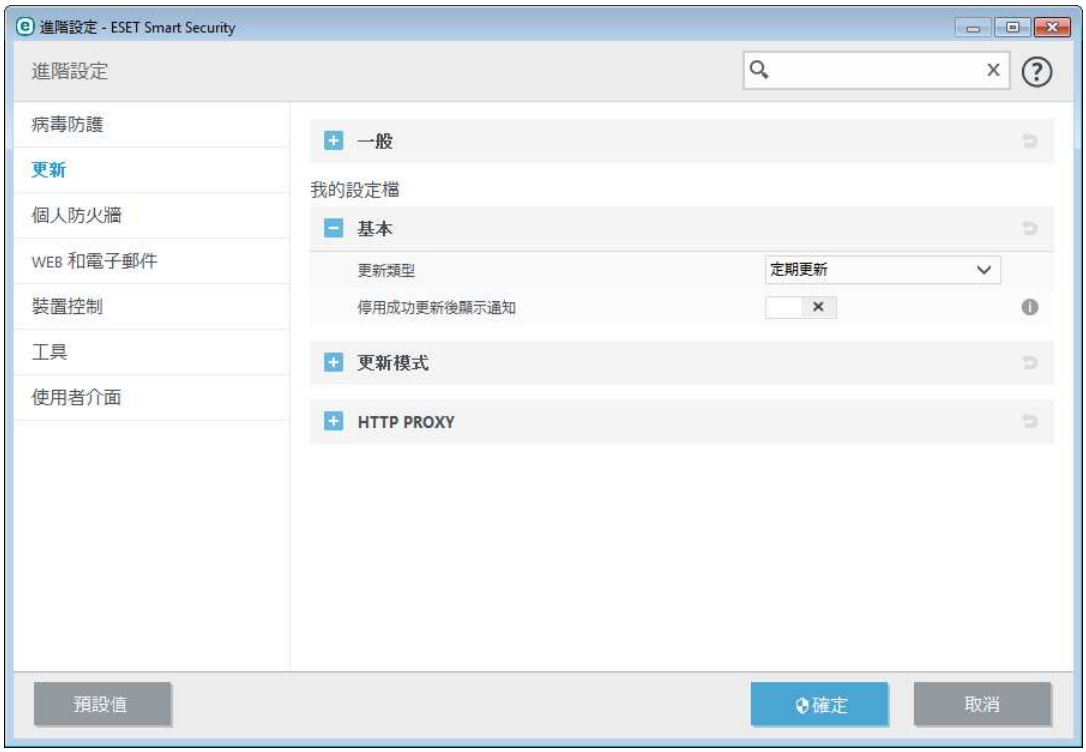
如果您無法使用建議的解決方案解決問題，請按一下 **[說明及支援]** 以存取說明檔案或搜尋 ESET 知識庫。如果您仍需要協助，可提出支援要求。「ESET 客戶服務」將快速回答您的問題並協助尋找解決方法。

3.2 更新

更新病毒資料庫及更新程式元件是保護系統不受惡意代碼威脅的一個重要部分。請注意其配置與作業。從主要功能表中，按一下 **[更新]**，然後按一下 **[立即更新]**，檢查是否有病毒資料庫更新。

如果在啟用 ESET Smart Security 期間沒有輸入使用者名稱及密碼，系統會提示您輸入。

[進階設定] 視窗 (從主要功能表按一下 **[設定]**，然後按一下 **[進階設定]**，或按鍵盤上的 **F5**) 包含其他的更新選項。若要配置例如更新模式、Proxy 伺服器存取、LAN 連線之類的進階更新選項，請按一下 **[更新]** 視窗中的特定索引標籤。



3.3 信任區域設定

：

您必須配置「信任區域」，才能在網路環境中保護您的電腦。您可以配置「信任區域」允許共用，來允許其他使用者存取您的電腦。按一下 **[設定]** > **[網路防護]** > **[已連線的網路]** 並按一下已連線的網路下方的連結。視窗隨即顯示選項，讓您選擇電腦在網路上需要的防護模式。

安裝 ESET Smart Security 之後以及電腦每次連接至新網路之後，都會進行「信任區域」偵測。因此，通常無需定義「信任區域」。依預設，偵測到新區域時會顯示對話方塊視窗以提示您設定該區域的防護層級。

警告 不正確的「信任區域」配置可能會對電腦造成安全風險。

附註： 依預設，會授與「信任區域」中工作站對共用檔案及印表機的存取權、啟用對內 RPC 通訊，還可以使用遠端桌面共用。

如需關於此功能的詳細資訊，請閱讀以下 ESET 知識庫文章：
在 ESET Smart Security 中偵測到新網路連線

3.4 防盜

若要在電腦遺失或遭竊時保護電腦，請選擇以下選項向 ESET 防盜 系統註冊您的電腦。

1. 成功啟動後，請按一下 **[啟用防盜]** 啟動剛剛所註冊電腦的 ESET 防盜 功能。

2. 如果您在 ESET Smart Security 的**首頁**窗格中，看見 **ESET 防盜 可用**訊息，請考慮為您的電腦啟用此功能。按一下 **[啟用 ESET 防盜]** 以向 ESET 防盜 註冊您的電腦。

3. 從主要程式視窗中，按一下 **[設定]** > **[安全性工具]**。按一下 **ESET 防盜** 旁邊的  ，並遵循快顯視窗中的指示進行。

附註： ESET 防盜 不會在 Microsoft Windows Home Servers 上執行。

如需建立 ESET 防盜 電腦關聯的詳細指示，請參閱如何新增新裝置。

3.5 家長控制工具

如果您已經啟用 ESET Smart Security 中的家長控制功能，您也必須設定要用來執行家長控制的使用者帳戶，才能正常運作。

當家長控制已經啟用，而使用者帳戶卻尚未設定時，**[家長控制未設定]** 將顯示於主要程式視窗的 **[首頁]** 窗格。按一下 **[立即設定規則]** 並參閱家長控制一章，並依指示為孩子建立特殊限制，以保護他們不受潛在的資訊威脅。

4. 使用 ESET Smart Security

ESET Smart Security 設定選項可讓您調整電腦的防護層級 與網路。.

[設定] 功能表分為下列區段：

電腦防護
網際網路防護
網路防護
安全性工具

按一下元件，以調整相對應防護模組的進階設定。

[電腦防護] 設定可讓您啟用或停用下列元件：

- **即時檔案系統防護** - 開啟、建立或在電腦上執行所有檔案時，都會掃描這些檔案是否具有惡意程式碼。
- **HIPS** - HIPS 系統監控作業系統中的事件，並根據自訂的規則集合執行反應動作。
- **玩家模式** - 啟用或停用玩家模式。啟用玩家模式之後，您將收到警告訊息 (潛在的安全性風險)，接著主視窗會轉為橙色。

[網際網路防護] 設定可讓您啟用或停用下列元件：

- **Web 存取防護** - 啟如果啟用，則會掃描透過 HTTP 的所有流量以尋找惡意軟體。
- **電子郵件用戶端防護** - 可監視透過 POP3 和 IMAP 通訊協定收到的通訊。
- **垃圾郵件防護** - 掃描來路不明電子郵件，即垃圾郵件。
- **網路釣魚防護** - 過濾疑似散佈內容以操控使用者提交機密資訊的網站。

網路防護 區段可讓您啟用或停用 個人防火牆，網路攻擊防護 (IDS) 及 殭屍網路防護。

安全性工具 設定可讓您調整下列模組：

- 銀行和付款防護
- 家長控制
- 防盜

家長控制功能可讓您封鎖可能包含潛在冒犯性資訊的網頁。此外，家長可禁止存取超過 40 個預先定義的網站類別及 140 多個子類別。

若要重新啟用已停用的安全性元件，請按一下滑桿 ，便會顯示綠色的核取標誌 。

附註： 使用此方法停用防護時，所有停用的防護模組將在電腦重新啟動後啟用。

設定視窗最下方提供其他選項。使用 **[進階設定]** 連結，為每個模組設定詳細參數。使用 **[匯入/匯出設定]** 選項可使用 *.xml* 配置檔案載入設定參數，或將目前的設定參數儲存至配置檔案。

4.1 電腦防護

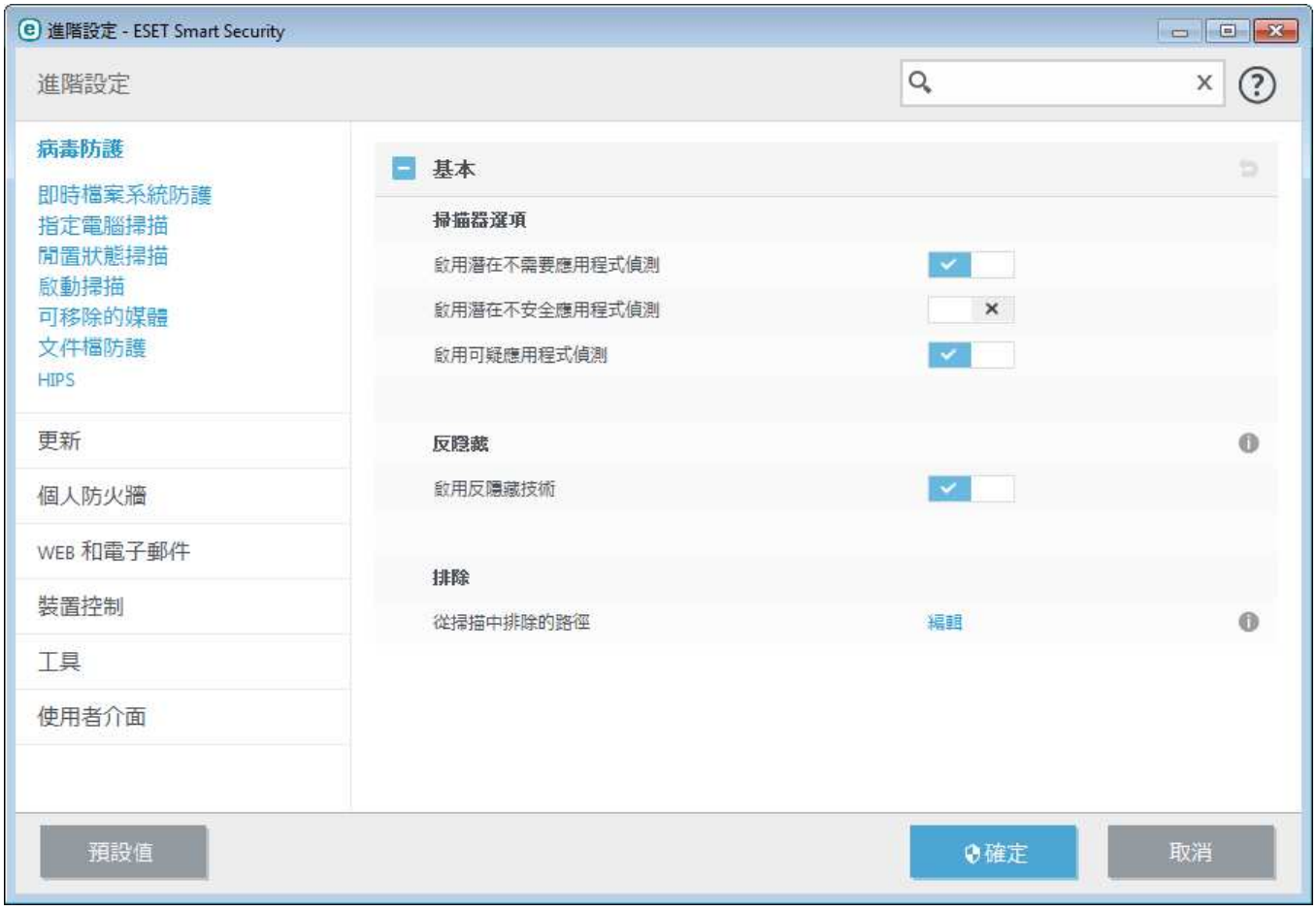
從設定視窗按一下 [電腦防護] 以查看所有防護模組概要。若要暫時關閉個別模組，請按一下 。請注意，這會降低電腦的防護層級。按一下 (位於防護模組旁) 以存取該模組的進階設定。

按一下 > 按一下**[即時檔案系統防護]** 旁邊的 **[編輯例外]** 來開啟 [排除] 設定視窗，您可從掃描中排除檔案與資料夾。

暫停病毒及間諜程式防護 - 停用所有病毒及間諜程式防護模組。當您停用防護之後，視窗將會開啟，您可在該處使用 **[時間間隔]** 下拉式功能表來決定停用防護的時間長度。按一下 **[確定]** 以確認。

4.1.1 病毒防護

病毒防護可藉由控制檔案、電子郵件及網際網路通訊來防止惡意系統攻擊。如果偵測到含有惡意代碼的威脅，「防毒」模組可透過封鎖，接著清除、刪除或將其移至隔離區來消滅它。



所有防護模組的掃描器選項 (例如即時檔案系統防護、Web 存取防護 ...) 皆可讓您啟用或停用以下項目的偵測功能：

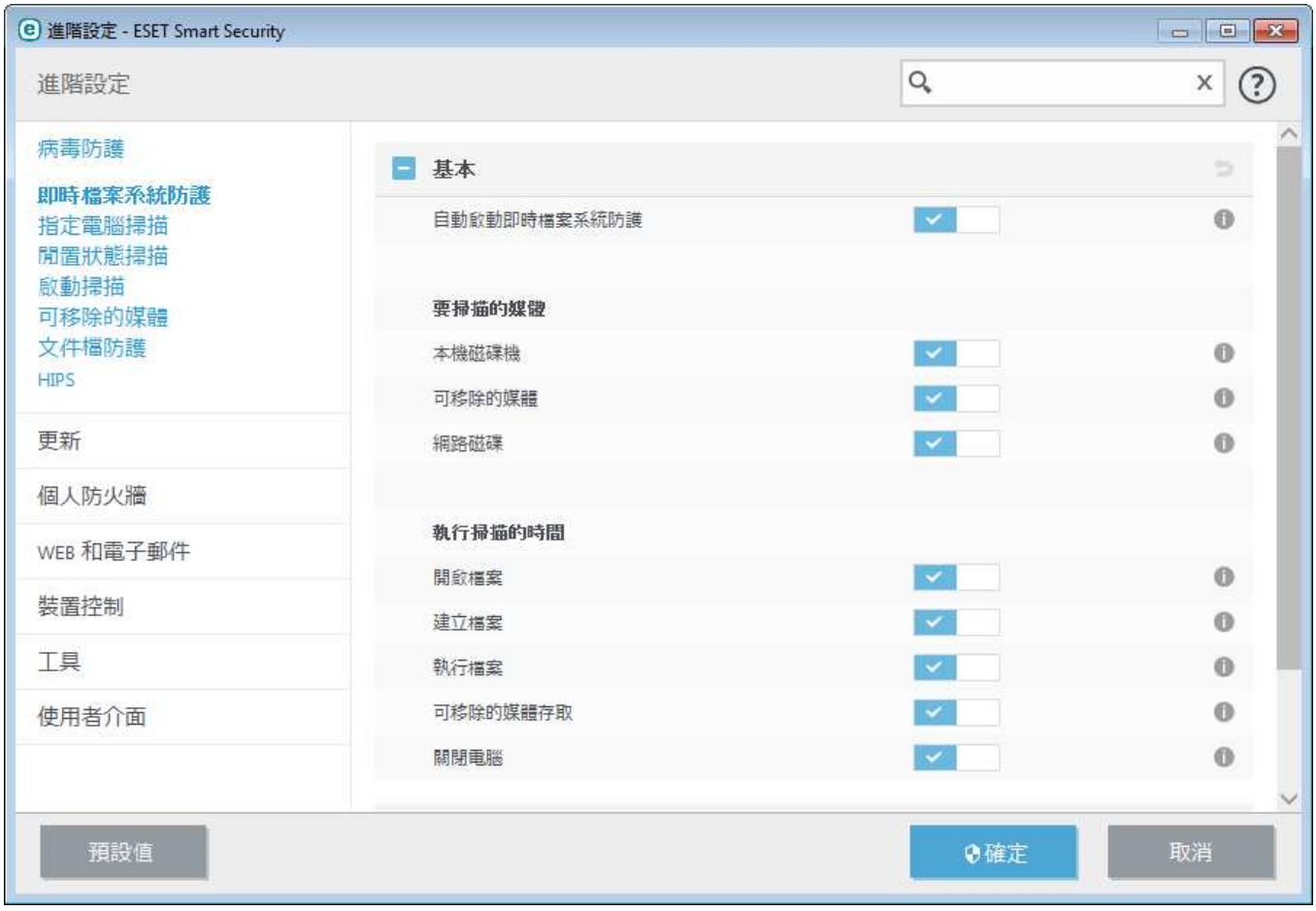
- **潛在不需要應用程式** (PUA) 不一定是惡意的，但是對電腦效能可能會造成負面影響。
  請在字彙中閱讀更多有關這些類型應用程式的資訊。
- **潛在不安全的應用程式**是指合法但可能不當用於惡意用途的商業軟體。例如遠端存取工具、密碼破解應用程式及鍵盤記錄程式 (記錄每次使用者按鍵的程式) 等，皆為潛在不安全的應用程式。依預設會停用此選項。
  請在字彙中閱讀更多有關這些類型應用程式的資訊。
- **[可疑的應用程式]** 包括以壓縮器或保護程式壓縮的程式。惡意軟體作者通常會使用這些類型的保護程式規避偵測。

[反隱藏技術] 是一種精密的系統，能偵測例如 rootkits 等危險程式。這些危險程式可隱藏於作業系統中。這就意味著使用一般測試技術無法偵測到它們。

[排除] 可讓您從掃描中排除檔案及資料夾。為確保所有物件已掃描是否存在威脅，我們建議您只有在絕對必要時建立排除。在某些情況下，您可能需要排除可能包含掃描大型資料庫項目的物件，因其在掃描期間或是軟體與掃描衝突時，可能會降低電腦速度。若要從掃描中排除物件，請參閱排除。

4.1.1.1 即時檔案系統防護

即時檔案系統防護控制系統中與防毒相關的所有事件。開啟、建立或在電腦上執行所有檔案時，都會掃描這些檔案是否具有惡意程式碼。在系統啟動時會啟動即時檔案系統防護。



依預設，即時檔案系統防護會在系統啟動時同時啟動，並持續提供不間斷地掃描。在特殊情況下 (例如，如果與其他即時掃描器發生衝突)，則可以解除 **[即時檔案系統防護]** > **[基本]** 下 **[進階]** 設定中的 **[自動啟動即時檔案系統防護]**，以停用即時防護。

要掃描的媒體

依預設，會掃描所有媒體類型是否有潛在的威脅：

本機磁碟 - 控制所有系統硬碟。
[可移除的媒體] - 控制 CD/DVD、USB 儲存裝置、藍芽裝置等。
網路磁碟 - 掃描所有對應的磁碟機。

我們建議使用預設值設定，只有在特殊情況下才修改這些設定，例如，掃描某些媒體而明顯減慢資料傳送時。

執行掃描的時間

依預設，在開啟、建立或執行時會掃描所有檔案。我們建議您保留預設設定，因為這些預設值會為電腦提供最高等級的即時防護：

- **[開啟檔案]** - 啟用/停用在開啟檔案時掃描。
- **[建立檔案]** - 啟用/停用在建立檔案時掃描。
- **[執行檔案]** - 啟用/停用在執行檔案時掃描。
- **可移除媒體存取** - 啟用或停用存取有儲存空間的特定可移除媒體所觸發的掃描。
- **[關閉電腦]** - 啟用或停用關閉電腦所觸發的掃描。

即時檔案系統防護會檢查所有媒體類型，而且各種系統事件 (例如存取檔案) 都會觸發掃描。使用 ThreatSense 技術偵測方法 (如 ThreatSense 引擎參數設定一節所述)，即時檔案系統防護可設定為將新建立檔案視為與現有檔案不同。例如，您可以設定即時檔案系統防護以更密切監視新建立的檔案。

為確保在使用即時防護時佔用最低的系統使用量，已掃描的檔案不予重複掃描 (除非已經過修改)。每次更新病毒資料庫之後，會立即重新掃描檔案。使用 **[智慧型最佳化]** 可控制此行為。如果停用此 **[智慧型最佳化]**，則所有檔案都會在每次存取時進行掃描。若要修改此設定，請按 **F5** 以開啟 [進階設定] 並展開 **[病毒防護]** > **[即時檔案系統防護]** 。請按一下 **[ThreatSense 參數]** > **[其他]** 並選取或取消選取 **[啟用智慧型最佳化]**。

4.1.1.1.1 其他 ThreatSense 參數

用於新建立及已修改檔案的其他 ThreatSense 參數

新建立或已修改檔案感染的可能性高於現有的檔案。這正是為何程式會以額外的掃描參數檢查這些檔案的原因。ESET Smart Security 配合病毒碼式掃描方式，使用可在病毒碼資料庫更新發行前 先行偵測新威脅的啟發式。除了新建立的檔案之外，也可針對 **[自我解壓檔]** (.sfx) 及 **[加殼技術虛擬機偵測]** (內部壓縮的執行檔案) 執行掃描。依預設，至多可以掃描至保存檔的第 10 層巢狀層級，並不論其實際大小都會進行檢查。若要修改壓縮檔掃描設定，請取消選取 **[預設壓縮檔掃描設定]**。

用於已執行檔案的其他 ThreatSense 參數

執行檔案時的進階啟發式 - 依預設，執行檔案時使用進階啟發式。啟用時，我們強烈建議您保持啟用智慧型最佳化和 ESET LiveGrid® 以減輕對系統效能的影響。

執行來自可移除的媒體之檔案時的進階啟發式 - 進階啟發式會在虛擬環境中模擬程式碼，並在允許執行可移除媒體中的程式碼前先評估其行為。

4.1.1.1.2 清除層級

即時防護具有三個清除層級 (若要存取清除層級設定，請按一下 **[即時檔案系統防護]** 區段中的 **[ThreatSense 引擎參數設定]**，然後按一下 **[清除]**)。

不清除 - 不會自動清除受感染的檔案。程式會顯示警告視窗並允許使用者選擇處理方法。此層級針對進階使用者而設計，進階使用者瞭解出現入侵時需採取哪些步驟。

標準清除 - 程式會根據預先定義的處理方法 (視入侵的類型而定) 嘗試自動清除或刪除受感染檔案。畫面右下角會顯示通知，表示受感染檔案的偵測及刪除。如果無法自動選取正確的處理方法，則程式會提供其他的後續處理方法。無法完成預先定義的處理方法時，程式也會提供後續處理方法的選項。

完全清除 - 程式會清除或刪除所有受感染檔案。只有系統檔案例外。如果無法清除受感染的檔案，則系統會提示使用者在警告視窗中選取一個處理方法。

警告 如果壓縮檔包含受感染的檔案，則您可以選用兩個選項來處理壓縮檔。在標準模式 (標準清除) 中，如果壓縮檔內所有檔案均受感染，則刪除整個壓縮檔。在 **[完全清除]** 模式中，當壓縮檔內含有至少一個受感染的檔案時，即會刪除壓縮檔，無論壓縮檔中其他檔案的狀態為何。

4.1.1.1.3 何時修改即時防護配置

即時防護是維護系統安全的最重要組成部分。修改其參數時請務必小心。建議您僅在特定情況中修改其參數。

安裝 ESET Smart Security之後，所有設定都已最佳化，為使用者提供最高層級的系統安全。若要還原預設值，請按一下視窗中每個索引標籤旁的 ↩ (**[進階設定]** > **[病毒防護]** > **[即時檔案系統防護]**)。

4.1.1.1.4 檢查即時防護

若要驗證即時防護正在運作並偵測病毒，請使用來自 eicar.com 的測試檔案。此測試檔案是所有防毒程式都可偵測到的無害檔案。該檔案由 EICAR (European Institute for Computer Antivirus Research) 公司建立，以測試防毒程式的功能。此檔案的下載連結為 http://www.eicar.org/download/eicar.com

附註： 執行即時防護檢查之前，必須停用防火牆。如果已啟用防火牆，則其會偵測到檔案並防止下載測試檔案。

4.1.1.1.5 即時防護無法運作時怎麼辦

在本章中，我們說明使用即時防護時可能發生的問題，以及如何疑難排解這些問題。

已停用即時防護

如果使用者不小心停用即時防護，則需要重新啟動它。若要重新啟動即時防護，請瀏覽至主要程式視窗的 **[設定]** ，並且按一下 **[電腦防護]** > **[即時檔案系統防護]**。

如果在系統啟動時未啟動即時保護，則通常是由於已停用 **[自動啟動即時檔案系統防護]** 的緣故。若要確保啟用此選項，請瀏覽至 [進階設定] (**F5**) 並按一下 **[防毒]** > **[即時檔案系統防護]**。

如果即時防護不會偵測及清除入侵

請確定電腦上未安裝任何其他防毒程式。若您同時安裝兩個防毒程式，它們可能會與彼此衝突。我們建議您先解除安裝系統上的任何其他防毒程式，再安裝 ESET。

即時防護未啟動

如果在系統啟動時未啟動即時保護 (且已啟用 **[自動啟動即時檔案系統保護]**)，則可能是由於與其他程式發生衝突。如需解決此問題的協助，請連絡 ESET 客戶服務。

4.1.1.2 電腦掃描

指定掃描器是防毒解決方案中的一個重要部分。它可用來針對電腦中的檔案及資料夾執行掃描。從安全性來看，不應該僅在懷疑有感染時才執行電腦掃描，出於常規安全性考量也應定期執行掃描。我們建議您定期為系統執行深入掃描，以偵測有否於寫入磁碟時未遭 [即時檔案系統防護] 所攔截的病毒。資料寫入磁碟時，若即時檔案系統防護已停用、病毒資料庫已過時，或是檔案儲存至磁碟時未偵測為病毒，就可能發生上述情況。

可以使用兩種 **[電腦掃描]** 類型。**[掃描您的電腦]** 可快速掃描系統，無須指定掃描參數。**[自訂掃描]** 可讓您選取針對目標特定位置所設計的預先定義掃描設定檔，也會讓您選擇特定的掃描目標。

掃描您的電腦

掃描您的電腦可讓您快速啟動電腦掃描並清除感染的檔案，無需使用者介入。掃描您的電腦的優點在於可以輕鬆執行作業，而不需要詳細的掃描配置。掃描會檢查本機磁碟中所有的檔案，且會自動清除或刪除偵測到的入侵。清除層級會自動設為預設值。如需更多有關清除類型的資訊，請參閱清除。

自訂掃描

自訂掃描可讓您指定掃描參數，例如掃描目標與掃描方法。自訂掃描的優點是可以詳細地配置參數。您可以將配置儲存為使用者定義的掃描設定檔，以利於使用相同參數重複執行掃描。

可移除的媒體掃描

與「掃描您的電腦」類似 - 可快速啟動掃描目前與電腦連接的可移除媒體 (如 CD/DVD/USB)。當您將 USB 隨身碟連接到電腦時，並想要掃描其內容是否有潛在威脅，這功能十分有用。

按一下 **[自訂掃描]** ？ 再選取 **[掃描目標]** 下拉式功能表中的 **可移除的媒體** 移，並按一下 **[掃描]**，也可啟動這類型掃描。

重複上次掃描

可讓您使用先前執行時所使用的相同設定，快速啟動先前執行的掃描。

請參閱掃描進度，取得更多關於掃描進度的資訊。

附註: 我們建議您一個月至少執行一次電腦掃描。您可以透過 **[工具]** > **更多工具** > **[排程器]**，將掃描配置為排程工作。如何安排每週電腦掃描?

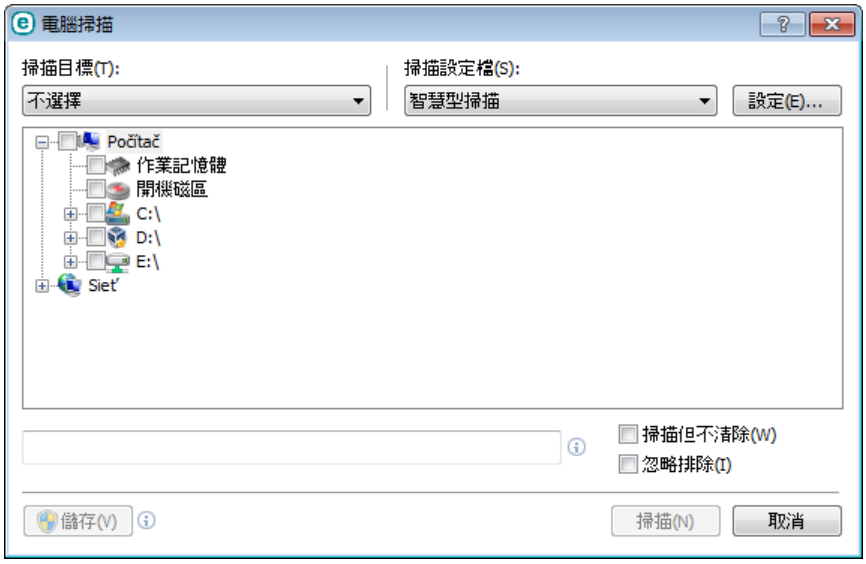
4.1.1.2.1 自訂掃描啟動器

如果只要掃描特的目標，不要掃描整個磁碟空間，您可以按一下 **[電腦掃描]** > **[自訂掃描]** 以使用 [自訂掃描]，然選取 **[掃描目標]** 下拉式功能表中的選項，或從資料夾 (樹狀) 結構中選取特定的目標。

[掃描目標] 視窗可讓您定義掃描入侵的物件 (記憶體、磁碟機、磁區、檔案及資料夾)。從列出電腦上所有可用裝置的樹狀結構中選取目標。**[掃描目標]** 下拉式功能表可讓您選取預先定義的掃描目標。

- **使用設定檔設定** - 選取所選掃描設定檔中設定的目標。
- **可移除媒體** - 選取磁碟片、USB 儲存裝置、CD/DVD。
- **本機磁碟機** - 選取所有系統硬碟。
- **網路磁碟機** - 選取所有對應的網路磁碟機。
- **不選擇** - 取消所有選擇。

若要快速瀏覽至掃描目標，或直接新增想要的目標 (資料夾或檔案)，請將其輸入資料夾清單下方的空白欄位。僅當樹狀結構中沒有選取任何目標，且 **[掃描目標]** 功能表設為 **[不選擇]** 時才可以這樣做。



感染項目不會自動清除。「掃描但不清除」可用來取得目前防護狀態的概觀。如果您只對掃描系統有興趣，且不使用其他清除處理方式，請選取 **[掃描但不清除]**。您亦可進一步使用下列方法選用三種清除層級：按一下 **[設定...]**> **[清除]**。掃描的相關資訊會儲存在掃描防護記錄中。

當選取 **[忽略例外]** 時，先前從掃描排除的包含副檔名檔案將會進行掃描而沒有例外。

您可以從 **[掃描設定檔]** 下拉式功能表中選擇用於掃描所選目標的設定檔。預設的設定檔是 **[掃描您的電腦]**。還有兩個預先定義的掃描設定檔，名稱分別是 **[深入掃描]** 與 **[內容功能表掃描]**。這些掃描設定檔會使用不同的 ThreatSense 參數。按一下 **[設定...]** 可詳細設定從 [掃描設定檔] 功能表中選擇的掃描設定檔。在 ThreatSense 參數中的 **[其他]** 區段下有可用選項的說明。

按一下**[儲存]** 以儲存目標選項中所執行的變更 (包括在資料夾樹狀結構內所進行的選取)。

按一下 **[掃描]** 使用您已設定的自訂參數來執行掃描。

[以管理員身分掃描] 可讓您在管理員帳戶下執行掃描。若目前的使用者權限不足，無法存取要掃描的適當檔案時，請按一下此選項。請注意，如果目前的使用者無法以管理員身分呼叫 UAC 作業，則無法使用此按鈕。

4.1.1.2.2 掃描進度

掃描進度視窗顯示掃描的目前狀態，以及發現包含惡意程式碼的檔案數目。

附註：通常無法掃瞄某些檔案，例如密碼保護的檔案或系統專用的檔案 (一般是 *pagefile.sys* 及某些防護記錄檔案)。

掃描進度 - 進度列可顯示已掃描物件與待掃描物件的狀態。此掃描進度狀態衍生自掃描中包括的物件總數。
目標 - 目前掃描的物件名稱及其位置。
發現的威脅 - 顯示掃描期間已掃描檔案、找到的威脅與已清除威脅的總數。
暫停 - 暫停掃描。
繼續 - 當掃描進度暫停時，則可看見此選項。按一下 **[繼續]** 以繼續掃描。
停止 - 終止掃描。
捲動掃描防護記錄 - 如果啟用，掃描防護記錄將在加入新項目時自動向下捲動，以顯示最新的項目。

提示：

按一下放大鏡或箭號以顯示目前執行中掃描的相關詳細資訊。
您可以按一下 **[掃描您的電腦]** 或 **[自訂掃描]**，以執行另一個平行掃描。

掃描後的處理方法 - 當電腦掃描完成後，觸發已排程的關機或重新開機。完成掃描後，關閉確認對話方塊視窗將開啟並於 60 秒後逾時。

4.1.1.2.3 掃描設定檔

您偏好的掃描參數可儲存供未來掃描時使用。我們建議您盡量為定期進行的掃描建立不同設定檔 (含有各種掃描目標、掃描方法及其他參數)。

若要建立新的設定檔，請開啟 [進階設定] 視窗 (F5)，然後按一下 **[病毒防護]** > **[指定電腦掃描]** > **[基本]** > **[設定檔清單]**。**[設定檔管理員]** 視窗包括 **[已選取的設定檔]** 下拉式功能表，其中列出現有的掃描設定檔與可建立新設定檔的選項。若要協助您建立掃描設定檔以符合您的需求，請參閱 ThreatSense 引擎參數設定一節，以取得每個掃描設定參數的說明。

範例： 假設您要建立您自己的掃描設定檔且 **[掃描您的電腦]** 配置有部份適用，但不要掃描 運行時間壓縮器 或潛在不安全的應用程式，並且要套用 **[完全清除]**。在 **[設定檔管理程式]** 視窗中輸入新設定檔的名稱並按一下 **[新增]**。從 **[已選取的設定檔]** 下拉式功能表中選取新設定檔，並調整剩餘的參數以符合您的需求，接著按一下 **[確定]** 以儲存新的設定檔。

4.1.1.3 啟動掃描

依預設，在系統啟動和病毒資料庫更新時，將執行啟動檔案自動檢查。這項掃描取決於排程器配置及工作。

啟動掃描選項是 **[系統啟動檔案檢查]** 排程器工作的一部分。若要修改其設定，請瀏覽至 **[工具]** > **更多工具** > **排程器**，按一下 **[自動啟動檔案檢查]** ，接著 **[編輯]**。在最後一個步驟中，[啟動檔案自動檢查] 視窗將出現 (請參閱下一章以取得詳細資訊)。

如需排程器工作建立及管理的詳細指示，請參閱建立新工作。

4.1.1.3.1 啟動檔案自動檢查

建立「系統啟動檔案檢查」排程工作時，有數個選項可供您調整下列參數：

[一般使用的檔案] 下拉式功能表根據精密的演算法指定系統啟動時檔案的掃描深度。系統會根據下列條件依遞減順序排列檔案：

- **所有登錄的檔案** (掃描的檔案最多)
- **很少使用的檔案**
- **一般使用的檔案**
- **經常使用的檔案**
- **僅最常使用的檔案** (掃描的檔案最少)

此外也包含兩個特定的群組：

- **使用者登入前執行的檔案** - 包含在使用者不用登入即可存取之位置中的檔案 (包含幾乎所有的啟動位置，例如服務、瀏覽器 Helper 物件、Winlogon 通知、Windows 排程器項目、已知 DLL 等)。
- **使用者登入後執行的檔案** - 包含在只有使用者登入後才能存取之位置中的檔案 (包含僅針對特定使用者執行的檔案，一般是 *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run* 中的檔案)。

每個上述群組的待掃描檔案清單是固定的。

掃描優先順序 - 用於決定何時開始掃描的優先順序層級：

- **閒置時** - 只有在系統閒置時才會執行工作、
- **最低** - 系統負載可能最低時、
- **較低** - 低系統負載、
- **正常** - 平均系統負載。

4.1.1.4 閒置狀態掃描

您可以在 **[病毒防護]** > **閒置狀態掃描**> **[基本]** 下的 **[進階設定]** 中啟用閒置狀態掃描器。將 **[啟用閒置狀態掃描]** 旁的切換選項設定為 **[開啟]** 以啟用此功能。電腦在閒置狀態時，會在所有本機磁碟機上執行無訊息電腦掃描。請參閱閒置狀態偵測觸發取得觸發閒置狀態掃描器所必須符合的完整條件清單。

依預設，當電腦 (筆記型電腦) 使用電池的電源時，閒置狀態掃描器不會執行。您可以在 [進階] 設定中啟動 **[即使電腦電源來自電池仍然要執行]** 旁的切換選項以覆寫此設定。

在 **[進階設定]** > **[工具]** > **ESET LiveGrid®**中開啟 **[啟用記錄]**，即可在防護記錄檔案區段中記錄電腦掃描輸出 (在主要程式視窗中按一下 **[工具]** > **[防護記錄檔案]**，並從 **[防護記錄]** 中選取 **[電腦掃描]**)。

閒置狀態偵測將在您的電腦處於以下狀態時執行:

- 螢幕保護程式
- 電腦鎖定
- 使用者登出

按一下 ThreatSense 引擎參數設定來為閒置狀態掃描修改掃描參數 (例如，偵測方法)。

4.1.1.5 排除

[排除] 可讓您從掃描中排除檔案及資料夾。為確保所有物件已掃描是否存在威脅，我們建議您只有在絕對必要時建立排除。然而，在某些情況下，您可能需要排除物件。例如，大型資料庫項目在掃描期間或是軟體與掃描衝突時，可能會降低電腦速度。

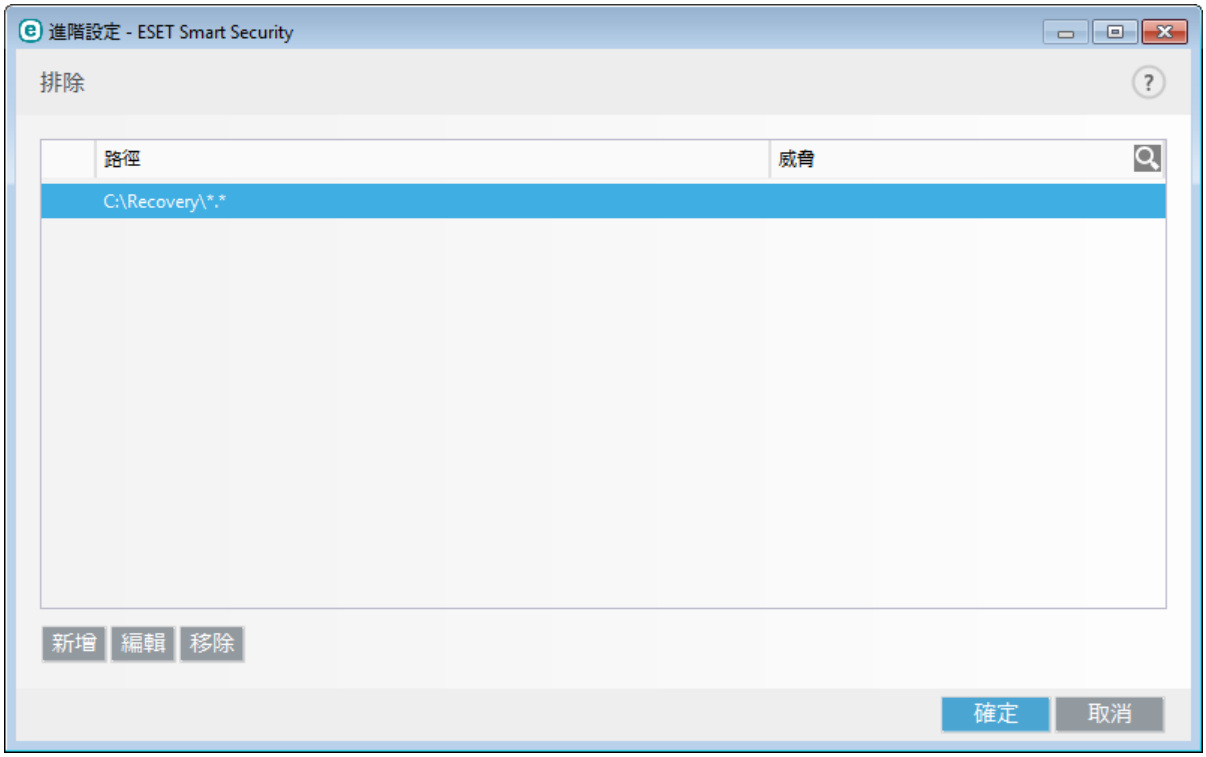
若要從掃描中排除物件：

1. 按一下 **[新增]**?
2. 輸入物件的路徑或在樹狀結構中進行選取。

您可以使用萬用字元來涵蓋一組檔案。問號 (?) 代表一個變數字元，而星號 (*) 代表含有零或多個字元的變數字串。

範例

- 如果您想要排除資料夾中的所有檔案，請輸入資料夾的路徑並使用遮罩「*.*」。
- 若要排除包含所有檔案與子資料夾的整個磁碟機，請使用遮罩「D:*」。
- 如果您只想要排除 doc 檔案，請使用遮罩「*.doc」。
- 如果執行檔的名稱具有特定數目的字元 (且字元不同)，但您只確切瞭解第一個字元 (例如 D)，請使用下列格式：D???? .exe。問號取代遺漏 (未知) 字元。



附註： 如果檔案符合條件排除掃描的條件，即時檔案系統防護模組或電腦掃描模組便無法偵測到該檔案內的威脅。

直欄

路徑 - 排除檔案及資料夾的路徑。

威脅 - 如果排除檔案旁有威脅的名稱，則代表該檔案只是因為指定威脅而排除，不是完全排除。如果該檔案在稍後被其他惡意軟體感染，則防毒模組仍會偵測到它。此類排除僅適用於特定類型的入侵，並可在報告入侵的威脅警告視窗 (按一下 **[顯示進階選項]**，然後選取 **[從偵測中排除]**)，或按一下 **[工具]** > **更多工具** > **[隔離]**，用滑鼠右鍵按一下隔離檔案，並選取內容功能表中的 **[還原並從偵測中排除]**。

控制項元素

新增 - 從偵測中排除物件。

編輯 - 可讓您編輯已選取的項目。

移除 - 移除已選取的項目。

4.1.1.6 ThreatSense 參數

ThreatSense 是由許多複雜威脅偵測方法組成之技術。此技術是主動式的，也就是說該技術也可在新威脅擴散初期提供防護。其使用代碼分析、代碼模擬、一般資料庫和病毒資料庫的組合，共同合作以大幅增強系統安全性。掃描引擎可以同時控制數個資料串流，以最大化效能及偵測率。ThreatSense 技術還可以順利消除 rootkit。

ThreatSense 引擎設定選項可讓您指定數個掃描參數：

- 要掃描的檔案類型及副檔名、
- 各種偵測方法的組合、
- 清除層級等。

若要進入設定視窗，請按一下任何使用 ThreatSense 技術之模組進階設定視窗中的 **ThreatSense[參數]** (如下所示)。不同的安全情況可能需要不同的設定。瞭解這一點之後，就可針對下列防護模組，分別進行 ThreatSense 配置：

- 即時檔案系統防護、
- 閒置狀態掃描、
- 啟動掃描、
- 文件防護、
- 電子郵件用戶端防護、
- Web 存取防護，
- 電腦掃描。

每個模組的 ThreatSense 參數都已高度最佳化，其修改對系統作業有很大影響。例如，將參數變更為一律掃描運行時間壓縮器，或在即時檔案系統防護模組中啟用進階啟發式可能會導致系統速度減慢 (通常，使用這些方法僅掃描新建立的檔案)。除了「電腦掃描」之外，我們建議您不要變更任何模組的預設 ThreatSense 參數。

要掃描的物件

此區段可讓您定義要掃描是否有入侵的電腦元件及檔案。

[作業記憶體] - 掃描攻擊系統作業記憶體的威脅。

開機磁區 - 掃描開機磁區的主要開機記錄中是否有病毒。

電子郵件檔案 - 程式支援下列副檔名：DBX (Outlook Express) 及 EML。

壓縮檔 - 程式支援下列副檔名：ARJ、BZ2、CAB、CHM、DBX、GZIP、ISO/BIN/NRG、LHA、MIME、NSIS、RAR、SIS、TAR、TNEF、UUE、WISE、ZIP、ACE 及許多其他副檔名。

自解壓縮檔 - 自我解壓檔 (SFX) 是不需要特定程式 (壓縮程式) 即可自行解壓縮的壓縮檔。

加殼技術虛擬機偵測 - 執行之後，加殼技術虛擬機偵測 (不同於標準壓縮檔類型) 會在記憶體中解壓縮。除了標準靜態壓縮器 (UPX、yoda、ASPack、FSG 等)，掃描器還能透過使用代碼模擬，辨識幾種其他類型的壓縮器。

掃描選項

選取在掃描系統是否有入侵時使用的方法。可用選項如下：

啟發式 - 啟發式是分析程式 (惡意) 活動的演算法。這項技術的主要優點是可以識別不存在或先前病毒資料庫不瞭解的惡意軟體。缺點是有錯誤警示的可能性 (很小)。

進階啟發式/DNA/智慧型簽章 - 進階啟發式是由 ESET 開發的獨特啟發式演算法所組成，經過最佳化以偵測電腦蠕蟲及特洛伊木馬程式，並以高階程式設計語言撰寫。使用進階啟發式能大幅提高 ESET 產品的威脅偵測功能。簽章可以可靠地偵測及識別病毒。採用自動更新系統，發現威脅數個小時之後便有可用的新病毒碼。病毒碼的缺點是僅偵測瞭解的病毒 (或這些病毒略微修改的版本)。

潛在不需要應用程式是含有廣告軟體、安裝工具列或具有其他不明企圖的程式。在某些情況下，使用者可能會認為潛在不需要應用程式的優點大於風險。因此，相較於其他例如特洛伊木馬或蠕蟲惡意軟體的類型，ESET 將此類應用程式指定為低風險的類別。

警告 - 發現潛在的威脅

偵測到潛在不需要應用程式時，您可以決定要採取的處理方法：

1. **清除/中斷連線**：此選項結束動作，並且防止潛在的威脅進入系統。
2. **略過**：此選項會允許潛在威脅進入您的系統。
3. 若要讓應用程式以後在電腦上不中斷地執行，請按一下 **[進階選項]**，然後選取 **[從偵測中排除]** 旁的核取方塊。

偵測到潛在不需要應用程式且無法清除時，**[位址已被封鎖]** 通知視窗會在畫面右下角顯示。如需有關此事件的詳細資訊，請從主功能表瀏覽至 **[工具]** > **更多工具** > 從主要功能表中的 **[防護記錄檔案]** > **[過濾的網站]**。

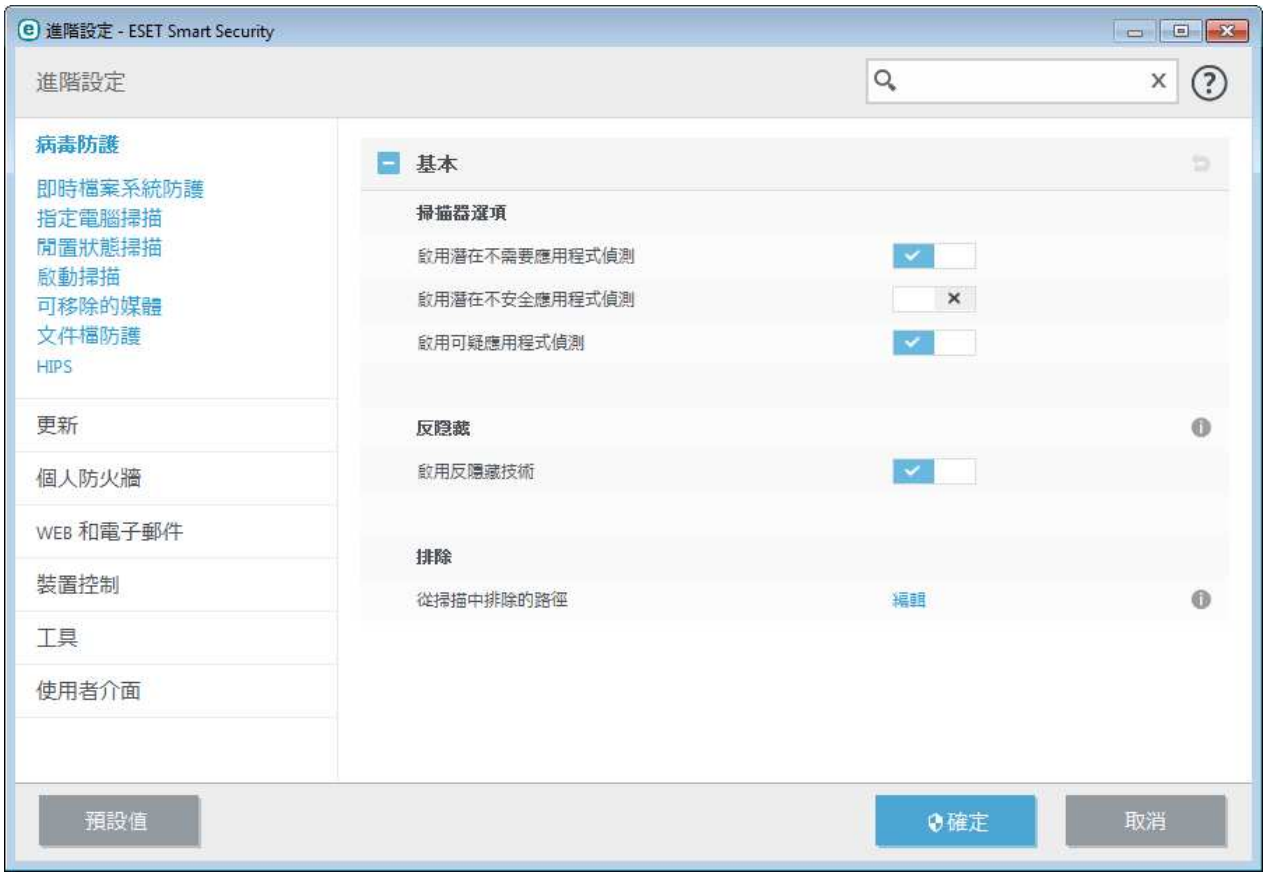
潛在不需要應用程式 - 設定

安裝您的 ESET 產品時，可以決定是否要啟用不需要應用程式的偵測，如下所示：

潛在不需要應用程式可能會安裝廣告軟體、工具列，或者具有其他不安全和不需要的程式功能。

您隨時可以在程式設定裡修改這些設定。若要啟用或停用潛在不需要、不安全或可疑應用程式的偵測，請遵循下列指示：

1. 開啟您的 ESET 產品。如何開啟我的 ESET 產品？
2. 按 **F5** 鍵以存取 **[進階設定]**。
3. 按一下 **[防毒]**，根據您的喜好啟用或停用 **[啟用潛在不需要應用程式偵測]**？**[啟用潛在不安全應用程式偵測]** 和 **[啟用可疑應用程式偵測]** 選項。按一下 **[確定]** 以確認。



潛在不需要應用程式 - 軟體包裝函式

軟體包裝函式是檔案裝載網站使用的一種特殊應用程式修改類型。其為第三方工具，會安裝您要下載的程式，但也會新增其他軟體，例如工具列或廣告軟體。這些其他軟體可能會變更您網頁瀏覽器的首頁和搜尋設定。除此之外，檔案裝載網站通常不會通知軟體廠商或接收下載的用戶其已經執行修改，且不會輕易允許取消修改。因為上述原因，ESET 將軟體包裝函式分類為一種潛在不需要應用程式，讓使用者選擇接受或不接受下載。

請參閱這份 ESET 知識庫文章以取得此說明頁面的更新版本。

[潛在不安全的應用程式] - [潛在不安全的應用程式] 是用於商業、合法程式的分類，例如遠端存取工具、密碼破解應用程式及鍵盤記錄程式 (記錄每次使用者按鍵的程式)。依預設會停用此選項。

清除設定會決定在掃描器清除受感染檔案期間的行為。有 3 個清除層級。

排除

副檔名是檔案名稱中以句點隔開的部份。副檔名定義檔案的類型及內容。ThreatSense 參數設定的此區段可讓您定義要掃描的檔案類型。

其他

配置 [指定電腦掃描] 的 ThreatSense 引擎參數設定時，**[其他]** 區段也有以下可用選項：

掃描替代資料串流 (ADS) NTFS 檔案系統使用的替代資料串流是使用一般掃描技術無法看到的檔案及資料夾關聯。許多入侵會透過將自己偽裝為替代資料串流來嘗試躲避偵測。

以低優先順序執行背景掃描 - 每個掃描序列都會消耗大量的系統資源。如果處理的程式佔有大量的系統資源，則可以啟動低優先順序背景掃描，從而節省應用程式的資源。

記錄所有物件 - 如果已選取此選項，則防護記錄檔案會顯示所有已掃描的檔案 (包括未受感染的檔案)。例如，如果壓縮檔內發現入侵，防護記錄將同時清除壓縮檔內的其他檔案。

啟用智慧型最佳化 - 啟用「智慧型最佳化」時，會使用最佳設定以確保最有效率的掃描層級，同時維持最快的掃描速度。各種防護模組都會聰明地掃描，利用不同的掃描方式並將其套用至特定的檔案類型。如果停用「智慧型最佳化」，則當執行掃描時，只會套用特定模組的 ThreatSense 核心中使用者定義的設定。

保存最後一次的存取時間郵戳 - 選取此選項，以保留掃描檔案的原始存取時間，而不會更新該時間 (例如，以用於資料備

份系統)。

限制

[限制] 區段可讓您指定物件的大小上限，以及要掃描的巢狀保存檔層級：

物件設定

物件大小上限 - 定義要掃描的物件大小上限。然後，指定的防毒模組只會掃描小於所指定大小的物件。只有進階使用者基於特定的理由，才應變更此選項來排除掃描較大物件。預設值：*無限制*。

物件的掃描時間上限 (秒) - 定義掃描物件的時間值上限。如果已在這裡輸入使用者定義的值，則當該時間到期，防毒模組會停止掃描物件，無論掃描是否完成。預設值：*無限制*。

壓縮檔掃描設定

壓縮檔巢狀層級 - 指定壓縮檔掃描的深度上限。預設值： *10*.

壓縮檔中檔案的大小上限 - 此選項可讓您指定要掃描的壓縮保存檔中，所包含檔案的大小上限 (解壓縮時)。預設值：*無限制*。

附註： 我們不建議變更預設值；在正常情況下，應該沒有要修改的理由。

4.1.1.6.1 清除

清除設定會決定在掃描器清除受感染檔案期間的行為。有 3 個清除層級。

4.1.1.6.2 從掃描中排除的檔案副檔名

副檔名是檔案名稱中以句點隔開的部份。副檔名定義檔案的類型及內容。ThreatSense 參數設定的此區段可讓您定義要掃描的檔案類型。

依預設，會掃描所有檔案，無論它們的副檔名為何。可以將任何副檔名新增至從掃描中排除的檔案清單。

如果掃描某些檔案類型會造成使用副檔名的程式無法正常執行，有時必須排除這種檔案不予掃描。例如，使用 Microsoft Exchange 伺服器時，可能建議排除 .edb、.eml 及 .tmp 等副檔名。

使用 **[新增]** 及 **[移除]** 按鈕，您可以允許或禁止指定檔案副檔名的掃描。若要將新的副檔名新增至清單，請按一下 **[新增]**，在空白欄位輸入副檔名並按一下 **[確定]**。當您選取 **[輸入多個值]** 時，您可新增多個以行、逗號或分號分隔的檔案副檔名。當您啟用多個選項時，副檔名將於清單中顯示。選取清單中的副檔名，並按一下 **[移除]** 以從清單中刪除副檔名。若您想要編輯已選取的副檔名，請按一下 **[編輯]**。

可以使用特殊符號 *(星號) 及 ?(問號)。星號代表任何字元字串，而問號代表任何字符。

4.1.1.7 偵測到入侵

入侵可以從網頁、共用資料夾等不同的進入點透過電子郵件，或從可移除的裝置 (USB、外部磁碟、CD、DVD、磁碟片等) 到達系統。

標準行為

做為 ESET Smart Security 處理入侵的一般範例，入侵的偵測可使用：

- 即時檔案系統防護
- Web 存取防護
- 電子郵件用戶端防護
- 指定電腦掃描

個別使用標準清除層級，並且將嘗試清除檔案並移至隔離區或終止連線。通知視窗會顯示在畫面右下角的通知區域中。如需有關清除層級和行為的詳細資訊，請參閱清除。

清除及刪除

如果沒有要針對即時檔案系統防護採取的預先定義處理方法，則會提示您在警告視窗中選取一個選項。通常可以使用 **[清除]**？**[刪除]** 及 **[不進行處理]** 選項。不建議選取 **[不進行處理]**，因為它不會清除受感染的檔案。但若您確定檔案無害，只是因失誤而偵測為入侵，則可破例選用此選項。

如果已將惡意程式碼連接至檔案的病毒已攻擊檔案，則套用清除。如果是這種情況，則請先嘗試清除受感染的檔案，以將其還原為原始狀態。如果該檔案僅由惡意程式碼組成，則會刪除該檔案。

如果受感染的檔案「已鎖定」或正由系統程序使用，則通常只會在釋放之後才會刪除它 (通常在系統重新啟動後)。

多種威脅

如果在電腦掃描期間沒有清除任何受感染的檔案 (或清除層級設為 **[不清除]**)，則警告視窗會提示您針對顯示的那些檔案選取處理方法。先針對檔案選取處理方法 (為清單中的每個檔案個別設定處理方法)，然後按一下 **[完成]**。

刪除壓縮檔中的檔案

在預設清除模式中，只有在整個壓縮檔包含受感染的檔案而不包含未感染檔案時，才會刪除它。也就是說，如果壓縮檔還包含

無害的未感染檔案，則不會進行刪除。執行完全清除掃描時請小心，因為啟用完全清除後，當壓縮檔內含有至少一個受感染的檔案時，即會刪除壓縮檔，無論壓縮檔中其他檔案的狀態為何。

如果您的電腦正在顯示惡意程式感染的信號 (例如，速度更慢、頻繁凍結等)，我們建議您執行下列各項：

- 開啟 ESET Smart Security，然後按一下 [電腦掃描]
- 按一下 **[掃描您的電腦]** (如需詳細資訊，請參閱電腦掃描)
- 完成掃描之後，請檢閱已掃描、受感染及已清除的防護記錄

如果您僅想要掃描磁碟的某一部分，請按一下 **[自訂掃描]**，並選取要進行病毒掃描的目標。

4.1.1.8 文件防護

文件防護功能可在 Microsoft Office 文件開啟前先行掃描文件，以及掃描 Internet Explorer 自動下載的檔案 (如 Microsoft ActiveX 元素)。文件防護在即時檔案系統防護之外再提供一層防護，若停用可增強無須處理大量 Microsoft Office 文件的系統效能。

[整合至系統] 可啟動防護系統。若要修改此選項，請按 F5 開啟 [進階設定] 視窗，然後從 **[進階設定]** 視窗中，按一下 **[病毒防護]** > **[文件防護]**。

使用 Microsoft Antivirus API 的應用程式 (如 Microsoft Office 2000 與更新版本，或 Microsoft Internet Explorer 5.0 與更新版本) 可啟動此功能。

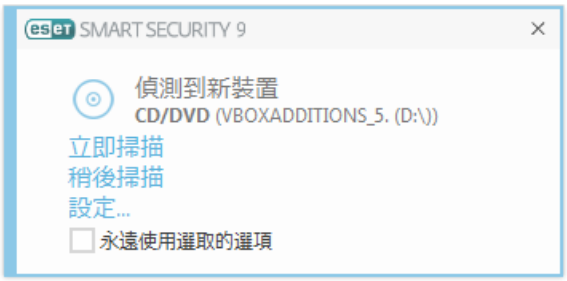
4.1.2 可移除的媒體

ESET Smart Security 提供自動可移除媒體 (CD/DVD/USB/...) 掃描。此模組可讓您掃描插入的媒體。若電腦管理員想要避免使用者使用含有來路不明內容的可移除媒體時，這功能便非常實用。

插入可移除媒體之後要採取的處理方法 - 選取預設處理方法，在將可移除媒體裝置插入電腦之後執行 (CD/DVD/USB)。如果選取 **[顯示掃描選項]**，則會顯示通知，讓您選擇想要的處理方法：

- **不掃描** - 不執行任何處理方法，且會關閉 **[偵測到新裝置]** 視窗。
- **自動裝置掃描** - 將針對已插入的可移除媒體裝置執行指定電腦掃描。
- **顯示掃描選項** - 開啟 [可移除的媒體設定] 區段。

插入可移除的媒體後會顯示下列對話方塊：



立即掃描 - 將會觸發掃描可移除的媒體。

稍後掃描 - 將延後掃描可移除的媒體。

設定 - 開啟 [進階設定]。

永遠使用選取的選項 - 選取後，在其他時間插入可移除媒體後會執行相同的處理方法。

此外，ESET Smart Security 具備裝置控制功能，能夠讓您定義在指定的電腦使用外部裝置的規則。在裝置控制一節中可找到裝置控制的詳細資訊。

4.1.3 裝置控制

ESET Smart Security 提供自動裝置 (CD/DVD/USB/...) 控制項。此模組可讓您掃描、封鎖或調整擴充的過濾器/權限，以及定義使用者存取和使用指定裝置的方式。若電腦管理員想要避免使用者使用含有來路不明內容的裝置時，這功能便非常實用。

支援的外部裝置：

- 磁碟儲存裝置 (HDD、USB 卸除式磁碟)
- CD/DVD
- USB 印表機
- FireWire 儲存裝置
- 藍牙裝置
- 智慧卡讀卡機
- 影像裝置
- 數據機
- LPT/COM 連接埠
- 可攜式裝置
- 所有裝置類型

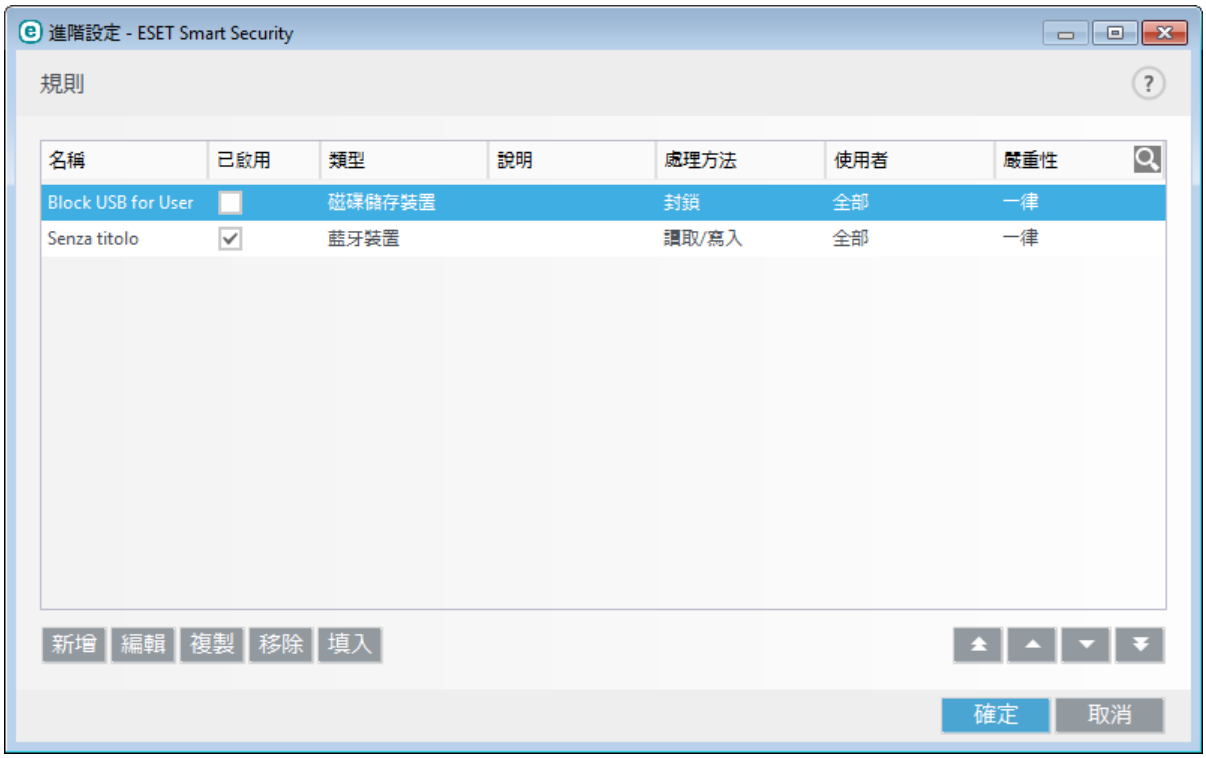
選取 **[進階設定]** (F5) > **[裝置控制]**，即可修改裝置控制設定選項。

開啟 **[整合至系統]** 旁的切換以啟動 ESET Smart Security 中的裝置控制功能；若要使變更生效，您需要重新啟動電腦。在啟用裝置控制之後，**[規則]** 將會變成啟用狀態，使您可以開啟規則編輯器視窗。

如果插入的裝置遭到現有規則封鎖，將會顯示通知視窗且不授與裝置的存取權限。

4.1.3.1 裝置控制規則編輯器

[裝置控制規則編輯器] 視窗會顯示現有規則，並允許準確控制使用者連接到電腦的外部裝置。



針對使用者或使用者群組，並按照可在規則設定中指定的其他裝置參數，可允許或封鎖特定裝置。規則清單包含規則的數個說明，例如名稱、外部裝置類型、將外部裝置連接到電腦後要執行的動作，以及防護記錄嚴重性。

按一下 **[新增]** 或 **[編輯]** 以管理規則。按一下 **[複製]** 可使用另一個所選取規則使用的預先定義選項建立新的規則。按一下規則時顯示的 XML 字串會複製到剪貼簿，以協助系統管理員匯出/匯入並使用這些資料，例如在 ESET Remote Administrator 中。

按下 CTRL 並按一下左鍵，您可以選取多個規則並將動作 (例如刪除或在清單中向上或向下移) 套用到所有選取的規則。**[已啟用]** 核取方塊可停用或啟用規則，如果您不希望永久刪除規則以供日後使用，此選項很有用。

控制是由按照決定優先順序的順序進行排序的規則所完成，優先順序較高的規則出現在頂端。

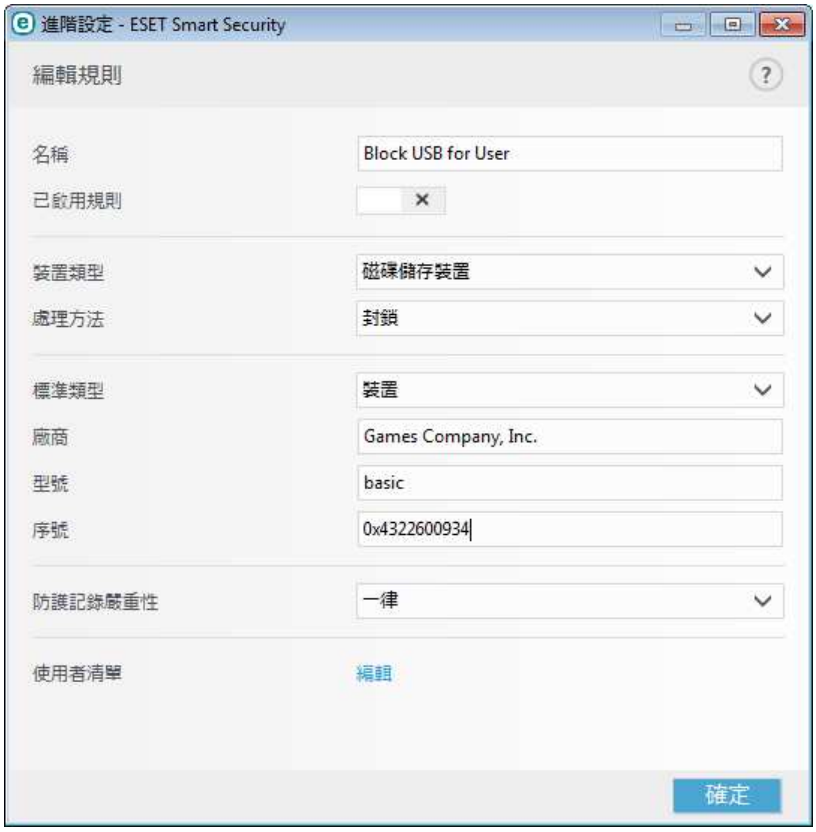
在 ESET Smart Security 的主要視窗中選取 **[工具]**，即可檢視防護記錄項目 > **更多工具** > **防護記錄檔案**。

裝置控制防護記錄會記錄所有裝置控制防護遭到觸發的事件。

按一下 **[填入]** 可為電腦所連接的裝置自動填入可移除媒體裝置參數。

4.1.3.2 新增裝置控制規則

裝置控制規則會定義符合規則條件的裝置連接到電腦時將採取的處理方法。



將規則說明輸入到 **[名稱]** 欄位中，以便進一步識別。按一下 **[已啟用規則]** 旁的切換選項可停用或啟用此規則；如果您不想要永久刪除規則，此選項很有用。

裝置類型

從下拉式功能表選擇外部裝置類型 (磁碟儲存裝置/可攜式裝置/藍牙/FireWire/...)。裝置的類型資訊是從作業系統收集而來，而且，如果裝置連接到電腦，可在系統裝置管理程式中看見裝置的類型資訊。儲存裝置包括透過 USB 或 FireWire 連接的外部磁碟或常見的讀卡機。智慧卡讀卡機包括各種配備內嵌積體電路之智慧卡 (如 SIM 卡或驗證卡) 的讀卡機。掃描器或相機都是影像裝置。因為這些裝置僅提供其行動相關的資訊且不會提供與使用者有關的資訊，無法以全域方式封鎖這些裝置。

處理方法

可允許或封鎖對於非儲存裝置的存取。另一方面，儲存裝置的規則允許選取下列其中一個權限設定：

- **讀取/寫入** - 將允許裝置的完整存取權限。
- **封鎖** - 將封鎖裝置的存取權限。
- **唯讀** - 僅允許讀取裝置的存取權限。
- **警告** - 每次連線到一個裝置就會通知使用者是否允許存取該裝置或是要封鎖，並會建立一筆記錄項目。不會記取裝置，針對相同裝置進行後續連線時仍會顯示通知。

請注意，並非所有裝置類型都適用所有處理方法 (權限)。如果其類型為儲存裝置，則四種處理方法都可以使用。對於非儲存裝置，只可使用三種處理方法 (例如，**[唯讀]** 不適用於藍牙，因此只能允許、封鎖或警告藍牙裝置)。

標準類型- 選取 **[裝置群組]** 或 **[裝置]**。

下面列出可用來微調規則並針對裝置進行調整的其他參數。所有參數均區分大小寫：

- **供應商** - 依供應商名稱或 ID 進行過濾。
- **型號** - 裝置的指定名稱。
- **序號** - 外部裝置通常擁有其專屬的序號。若是 CD/DVD，則是指定的媒體會有序號，而非 CD 光碟機。

附註： 如果並未定義這些參數，規則在比對時就會忽略這些欄位。所有文字欄位中的過濾參數均不區分大小寫，且不支援萬用字元 (* 與 ?)。

提示： 若要檢視關於裝置的資訊，請為該類型的裝置建立規則，將裝置連接到電腦，然後查看裝置控制防護記錄中的裝置詳細資訊。

記錄嚴重性

ESET Smart Security 會將所有重大事件儲存在防護記錄檔案中，您可以從主要功能表直接檢視該檔案。按一下 **[工具]** > **更多工具** > **[防護記錄檔案]**，然後從 **[防護記錄]** 下拉式功能表中選取 **[裝置控制]**。

- **永遠** - 記錄全部的事件。
- **診斷** - 記錄微調程式時所需的資訊。
- **資訊** - 記錄資訊性訊息，包含成功更新訊息及上述所有記錄。
- **警告** - 記錄嚴重錯誤及警告訊息。
- **無** - 不記錄任何防護記錄。

將某些使用者或使用者群組新增至 **[使用者清單]**，即可將規則限制在某些使用者或使用者群組：

- **新增** - 開啟 **[物件類型：使用者或群組]** 對話方塊視窗，可讓您選取所需的使用者。
- **移除** - 從過濾器移除選取的使用者。

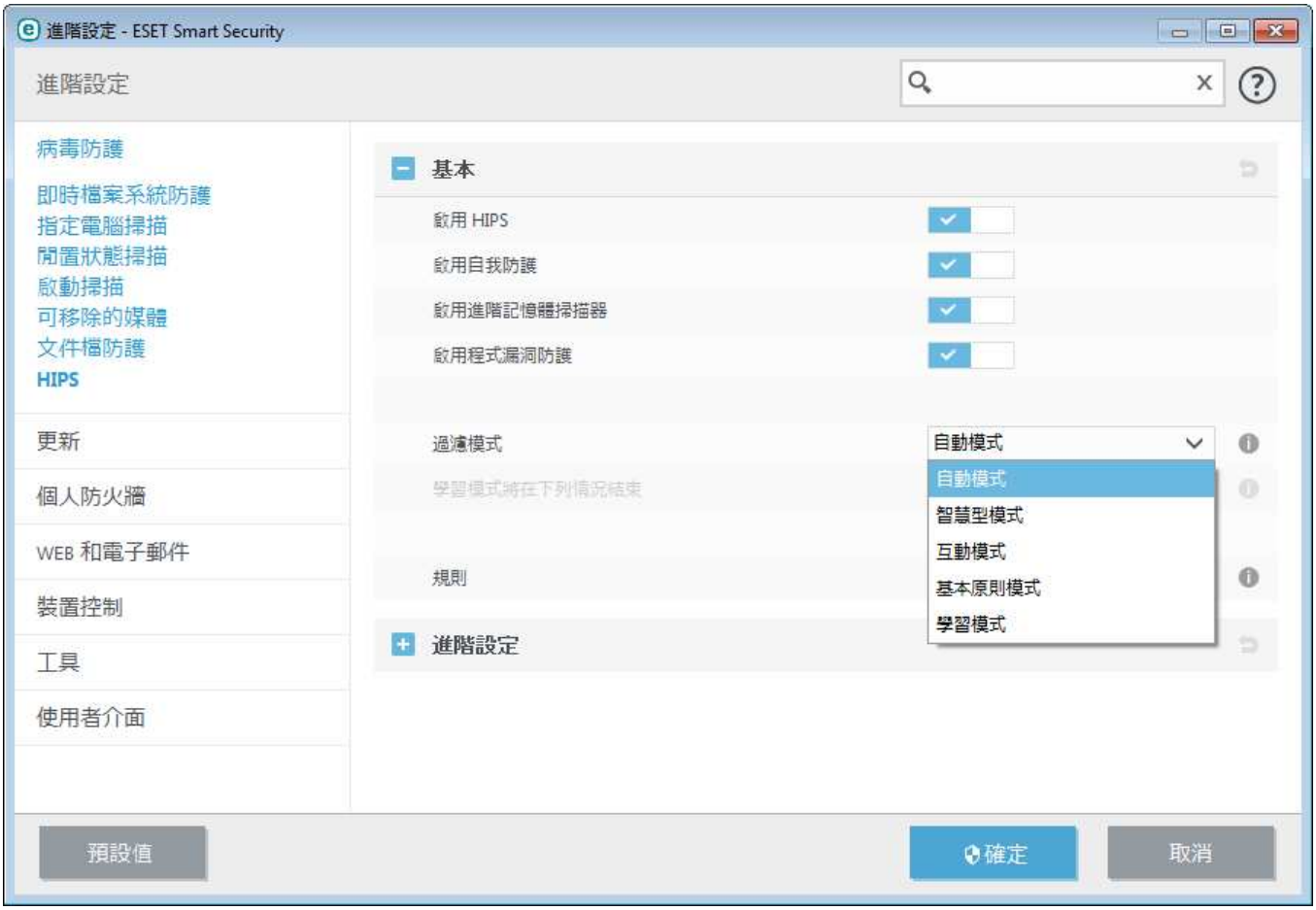
附註：所有裝置都可以使用者規則篩選 (例如，影像裝置不會提供使用者相關資訊，僅提供動作相關資訊)。

4.1.4 主機入侵預防系統 (HIPS)

若要變更 HIPS 設定，僅能由有經驗的使用者執行。未正確配置的 HIPS 設定可能導致系統不穩定。

主機入侵預防系統 (HIPS) 能保護您的系統抵抗惡意軟體以及任何嘗試對電腦產生不良影響的不必要活動。HIPS 利用進階行為分析再加上網路過濾的偵測能力，可監視執行中的程序、檔案及登錄機碼。HIPS 與即時檔案系統防護各自獨立，且不是防火牆，它只會監視在作業系統內執行的處理程序。

按一下 **[進階設定]** (F5) > **[病毒防護]** > **[HIPS]** > **[基本]**，便可找到 HIPS 設定。HIPS 狀態 (啟用/停用) 顯示在 ESET Smart Security 主要程式視窗中的 **[設定]** > **[電腦防護]**。



ESET Smart Security 使用內建的 **[自我保護]** 技術，可防止惡意軟體損毀或停用您的病毒及間諜程式防護，因此能確定系統隨時受到保護。需要重新啟動 Windows 才能停用 HIPS 或 [自我保護]。

[進階記憶體掃描器] 可與惡意探索封鎖程式一起搭配，強化對抗惡意軟體在整個利用欺騙及/或加密時對惡意軟體防護產品所啟用偵測功能的規避動作。進階記憶體掃描器依預設已啟用。請在字彙中閱讀更多有關此類型防護的資訊。

惡意探索封鎖程式是設計用來強化常遭利用的應用程式類型的防護，例如 Web 瀏覽器、PDF 閱讀器、郵件用戶端和 MS Office 元件。惡意探索封鎖程式依預設已啟用。請在字彙中閱讀更多有關此類型防護的資訊。

過濾可使用以下四種模式其中之一執行：

自動模式 - 系統會啟用作業，但受到保護系統的預先定義規則封鎖的作業除外。

智慧型模式 - 僅會通知使用者關於非常可疑的事件。

互動模式 - 系統將提示使用者確認作業。

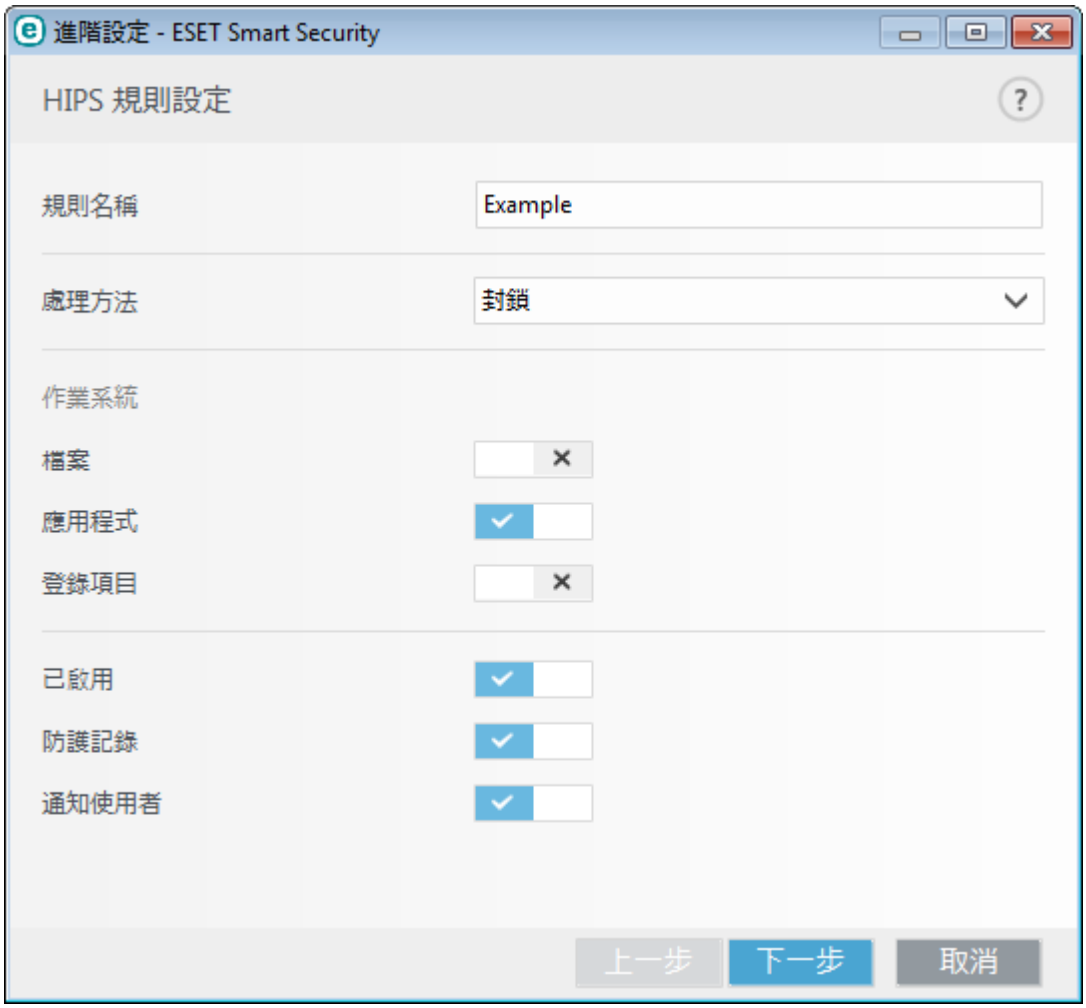
原則型模式 - 系統會封鎖作業。

[學習模式] - 系統會啟用作業，且每次作業後會建立規則。以此模式建立的規則可在 [規則編輯器] 中檢視，但與手動建立的規則或自動模式下建立的規則相較之下，其優先順序較低。當您從 [HIPS 過濾模式] 下拉式功能表選取 [學習模式]，即可使用 **[學習模式將在下列情況結束]** 設定。選取您要啟用學習模式的持續時間，最長為 14 天。過了指定的持續時間之後，會提示您在學習模式中編輯 HIPS 建立的規則。您可以選擇不同的過濾模式，或者延後決定並持續使用學習模式。

HIPS 系統監控作業系統中的事件，並根據類似個人防火牆規則的規則執行反應動作。按一下 **[編輯]** 開啟 HIPS 規則管理視窗。在此您可以選取、建立、編輯或刪除規則。

在下列範例中，我們將說明如何限制應用程式發生不想要的行為：

1. 命名規則，並選取 **[處理方法]** 下拉式功能表中的 **[封鎖]**。
2. 啟用 **[通知使用者]** 切換選項，以在每次套用規則時顯示通知。
3. 請至少選取一個要套用規則的作業。在 **[來源應用程式]** 視窗中，從下拉式功能表選取 **[所有應用程式]**，將您的新規則套用至所有嘗試在您指定的應用程式上執行任何已選取應用程式作業的應用程式。
4. 選取 **[修改另一個應用程式的狀態]** (產品說明中會有所有作業的說明，按下 F1 鍵即可顯示).
5. 從下拉式功能表中選取 **[特定應用程式]**，並 **[新增]** 一個或多個您要保護的應用程式。
6. 按一下 **[完成]** 以儲存您的新規則。



4.1.4.1 進階設定

以下選項可用於除錯及分析應用程式的行為：

一律允許載入驅動程式 - 除非使用者規則明確封鎖，否則一律允許載入選取的驅動程式，無論配置的過濾模式為何。

記錄所有封鎖的作業 - 所有封鎖的作業將寫入至 HIPS 防護記錄。

當啟動應用程式發生變更時通知 - 每次在系統啟動中新增或移除應用程式時，便會顯示桌面通知。

請參閱我們的 知識庫文章以取得此說明頁面的更新版本。

4.1.4.2 HIPS 互動視窗

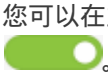
若規則的預設處理方法已設定為 **[詢問]**，每次觸發規則時都會出現對話方塊視窗。您可以選擇 **[拒絕]** 或 **[允許]** 作業。如果您不在指定時間內選擇處理方法，則會根據規則選取新處理方法。

對話視窗可讓您根據 HIPS 偵測的任何新處理方法來建立規則，然後定義允許或拒絕該處理方法所依據的條件。按一下 **[詳細資訊]** 可存取確實的參數設定。系統認定使用此方法建立的規則等於手動建立的規則，因此由對話視窗建立的規則無需像觸發該對話視窗的規則那般明確。這表示，建立此類規則後，同樣的作業可以觸發相同的視窗。

[直到結束應用程式之前都會記住] 會造成使用處理方法 (**[允許/拒絕]**)，直到規則或過濾模式變更、HIPS 模組更新或系統重新啟動為止。在進行上述三個處理方法的任何之一後，則會刪除暫時的規則。

4.1.5 玩家模式

玩家模式是一項專為要求可不間斷地使用軟體、不想受到快顯視窗打擾，而且想要將用量減到最少的 CPU 使用者所設計的功能。玩家模式也可在簡報期間使用，在此期間中病毒活動無法干擾簡報。透過啟用此功能，所有的快顯視窗均會停用，而且排程器的活動也將完全停止。然而，系統保護功能仍會在背景執行，不需要和使用者互動。

您可以在主要程式視窗的 **[設定]** > **[電腦防護]** 下啟用或停用玩家模式，方式為按一下  或 **[玩家模式]** 旁的  。啟用玩家模式有潛在的安全性風險，所以工作列上的防護狀態圖示會變成橙色並顯示警告。您也會在主要程式視窗中看見這個警告，**[玩家模式已啟用]** 則以橙色顯示。

您可以展開 **[電腦]**，按一下 **[玩家模式]** 並選取 **[啟用玩家模式]** 旁的核取方塊，在 [進階設定] 樹狀結構 (F5) 中啟用 [玩家模式]。

選取 [進階設定] (F5) 下的 **[以全螢幕執行應用程式時自動啟用玩家模式]**，在您開始全螢幕應用程式時啟動玩家模式，並在離開應用程式後停止。

選取 **[自動停用玩家模式於]** 以定義一段時間，玩家模式會在這段時間過後自動停用。

附註： 如果個人防火牆處於互動模式且啟用玩家模式，您可能就無法順利連接至網際網路。如果您啟動的遊戲會連接至網際網路，就會產生問題。系統通常會要求您確認這類動作 (如果尚未定義任何通訊規則或例外)，但是玩家模式已經停用使用者互動。若要允許通訊，請針對可能發生此問題的任何應用程式定義通訊規則，或使用個人防火牆中的其他過濾模式。請記得，啟用玩家模式之後，如果您造訪的網頁或應用程式可能有安全性風險，則會加以封鎖；但由於使用者互動已經停用，因此您不會看到任何解釋或警告。

4.2 網際網路防護

按一下 **[網際網路防護]** 之後，您便可以在 **[設定]** 窗格中找到 Web 和電子郵件設定。您可以在這裡存取更詳細的程式設定。

網際網路連線是個人電腦中的標準功能。但很糟糕的是，網際網路也成為傳輸惡意程式碼的主要媒介。因為如此，您必須審慎考量您的 **[Web 存取防護]** 設定。

按一下 ⚙ 以開啟進階設定中的 Web/電子郵件/網路釣魚/垃圾郵件 防護設定。

[電子郵件用戶端防護] 可控制透過 POP3 和 IMAP 通訊協定收到的電子郵件通訊。使用電子郵件用戶端的外掛程式，ESET Smart Security 可控制與電子郵件用戶端之間往來的所有通訊 (POP3、MAPI、IMAP、HTTP)。

[垃圾郵件防護] 可過濾來路不明電子郵件。

當按下齒輪 ⚙ (位於 **[垃圾郵件防護]** 旁),將可使用下列選項：

配置... - 開啟電子郵件用戶端和垃圾郵件防護進階設定。

使用者的白名單/黑名單/例外名單 - 開啟對話方塊視窗，供您新增、編輯或刪除視為安全或不安全的電子郵件地址。根據此處定義的規則，從這些地址發出的電子郵件將不會進行掃描，或將當作垃圾郵件處理。按一下 **[使用者的例外清單]** 以新增、編輯或刪除可能受詐騙而被用來傳送垃圾郵件的電子郵件地址。針對例外清單中寄件者地址發出的電子郵件訊息，系統會一律掃描看是否為垃圾郵件。

[網路釣魚防護] 可讓您封鎖已知會散佈網路釣魚內容的網頁。強烈建議您將網路釣魚防護保留為啟用。

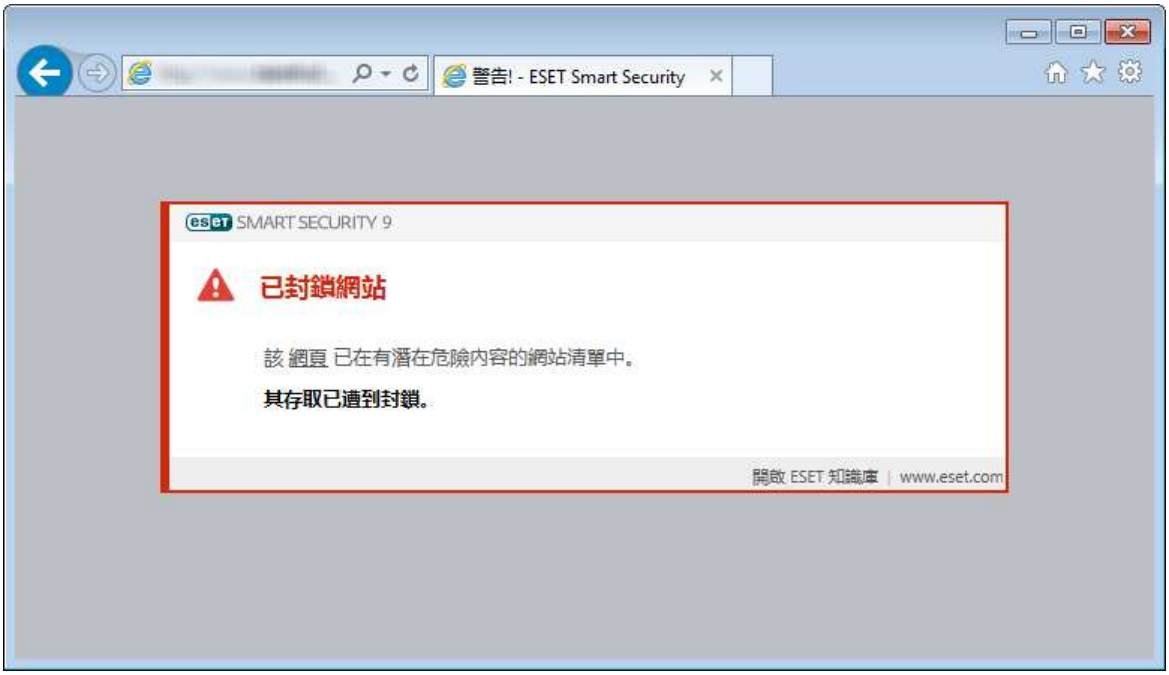
您可以停用 Web/電子郵件/網路釣魚/垃圾郵件 防護模組，方式為按一下  。

4.2.1 Web 存取防護

網際網路連線是個人電腦中的標準功能。不幸的是，它也成為傳輸惡意程式碼的主要媒介。Web 存取的運作方式是監視 Web 瀏覽器與遠端伺服器之間的通訊，並遵循 HTTP (超文字傳輸通訊協定) 及 HTTPs (加密的通訊) 規則。

在內容下載之前封鎖已知含惡意內容網頁的存取權限。所有其他網頁會在下載時由 ThreatSense 掃描引擎進行掃描，並在偵測到其包含惡意內容時加以封鎖。Web 存取防護會提供兩層防護，依黑名單封鎖和依內容封鎖。

強烈建議您啟用 Web 存取防護功能。此選項可從 ESET Smart Security 的主要視窗存取 (瀏覽至 **[設定]** > **[網際網路防護]** > **[Web 存取防護]**。



您可在 **[進階設定]** (F5) > **[Web 和電子郵件]** > **[Web 存取防護]** 中使用下列選項：

- **Web 通訊協定** - 可讓您配置監控大多數網際網路瀏覽器使用的這類標準通訊協定。
- **URL 位址管理**- 可讓您指定要封鎖、允許或從檢查中排除的 HTTP 位址。
- **ThreatSense 參數** - 進階病毒掃描器設定，可讓您配置如要掃描的物件類型 (電子郵件和壓縮檔等)、Web 存取防護的偵測方法等設定。

4.2.1.1 基本

啟用 Web 存取防護 - 停用之後，無法確保得到 Web 存取防護和網路釣魚防護。

附註: 強烈建議您將此選項保留為啟用。

4.2.1.2 Web 通訊協定

依預設，ESET Smart Security 已配置為監視大多數網際網路瀏覽器所使用的 HTTP 通訊協定。

HTTP 掃描器設定

Windows Vista 以及更新版的作業系統會一律監視所有應用程式連接埠上的 HTTP 流量。於 Windows XP，您可以在 **[進階設定]** (F5) > **[Web 和電子郵件]** >**[Web 存取防護]** > **[Web 通訊協定]** 中修改 **[HTTP 通訊協定使用的連接埠]**。系統會監視所有應用程式特定連接埠上的 HTTP 流量，且應用程式的所有連接埠將標記為 [Web 和電子郵件用戶端]。

HTTPS 掃描器設定

ESET Smart Security 也支援 HTTPS 通訊協定檢查。HTTPS 的通訊使用加密的通道以在伺服器與用戶端間傳輸資訊。ESET Smart Security會檢查利用 SSL (安全通訊端層) 與 TLS (傳輸層安全性) 通訊協定的通訊。此程式將只掃描 **[HTTPS 通訊協定使用的連接埠]** 中定義的連接埠流量，無論其作業系統的版本為何。

不掃描加密的通訊。若要掃描加密的通訊並且檢視掃描器設定，請瀏覽至 [進階設定] 區段中的 SSL/TLS，按一下 **[Web 和電**

子郵件] > **[SSL/TLS]**，並啟用 **[啟用 SSL/TLS 通訊協定過濾]** 選項。

4.2.1.3 URL 位址管理

URL 位址管理區段可讓您指定要封鎖、允許或從檢查中排除的 HTTP 位址。

不可以存取 **[封鎖位址清單]** 中的網站，除非它們包含在 **[允許的位址清單]** 中。**[從檢查中排除的位址清單]** 中的網站在存取時將不檢查是否含有惡意程式碼。

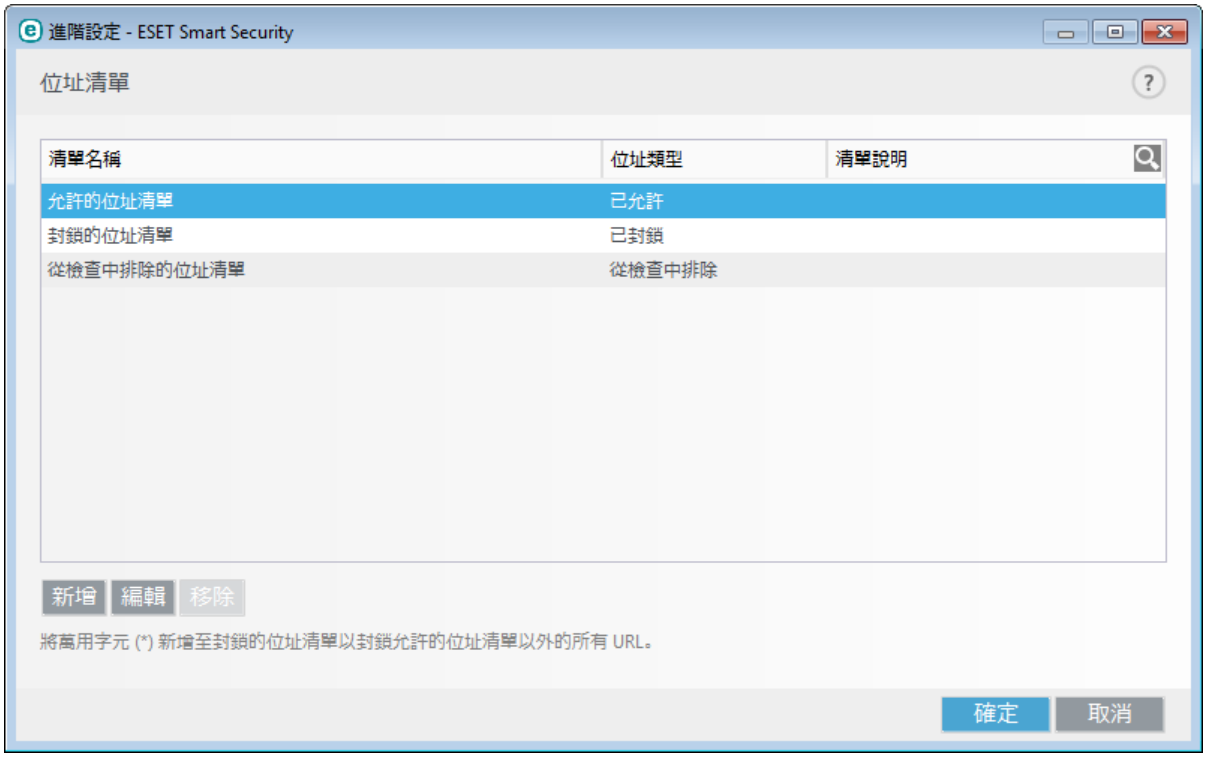
若除了 HTTP 網頁之外，您也想過濾 HTTPS 位址，則必須選取 **[啟用 SSL/TLS 通訊協定過濾]**。否則只有您已造訪 HTTPS 網站的網域將會新增，但完整 URL 則不會新增。

如果您將 URL 位址新增至 **[已從過濾中排除的位址清單]**，則會從掃描中排除該位址。您也可以將特定位址新增至 **[允許的位址清單]** 或 **[封鎖的位址清單]**，以允許或封鎖這些位址。

若您想封鎖所有位於作用中 **[允許的位址清單]** 以外的 HTTP 位址，請將 * 新增至作用中的 **[封鎖的位址清單]**。

可以使用特殊符號 *(星號) 及 ?(問號)。星號可以代替任何字元字串，問號可代替任何符號。在指定排除的位址時應特別注意，因為此清單只能包含受信任且安全的位址。同樣地，必須確定在此清單中正確使用字符 * 及 ?。請參閱 新增 HTTP 位址/網域遮罩 以瞭解如何使整個網域，包含所有子網域能安全地相符。若要啟動清單，請選取 **[作用中的清單]**。如果您想在進入目前清單中的位址時收到通知，請選取 **[套用時通知]**。

提示: URL 位址管理也允許您在瀏覽網際網路時封鎖或允許開啟特定檔案類型。例如，若您不想開啟執行檔，請從下拉式功能表選取您要封鎖這些檔案的清單，接著輸入遮罩「**.exe」。



控制項元素

新增 - 除了預先定義的清單之外，將建立新的清單。若您想有邏輯地分隔不同的位址群組，這樣做很有幫助。例如，一個封鎖的位址清單可能包含外部公用黑名單上的位址，而第二個清單則可能包含您自己黑名單上的位址，這會讓您在保持自己的清單不變時更容易更新外部清單。

編輯 - 修改現有清單。使用它來新增或移除位址。

移除 - 刪除現有清單。僅適用於使用 **[新增]** 建立的清單，預設清單並不適用。

4.2.2 電子郵件用戶端防護

4.2.2.1 電子郵件用戶端

ESET Smart Security 與電子郵件用戶端的整合會針對電子郵件訊息中的惡意代碼，增加作用中的防護層級。如果您的電子郵件用戶端受支援，即可在 ESET Smart Security 中啟用此整合。如果啟用整合，ESET Smart Security 工具列會直接插入電子郵件用戶端 (不插入較新版的 Windows Live Mail 工具列)，以便更有效進行電子郵件防護。整合設定位於 **[設定]** > **[進階設定]** > **[Web 和電子郵件]** > **[電子郵件用戶端防護]** > **[電子郵件用戶端]** 下方。

電子郵件用戶端整合

目前支援的電子郵件用戶端包括 Microsoft Outlook、Outlook Express、Windows Mail 和 Windows Live Mail。電子郵件防護是以外掛程式的形式在這些程式中運作。外掛程式的主要優勢為其獨立於所使用的通訊協定。當電子郵件用戶端接收到加密的郵件，它會將其解密並傳送到病毒掃描器。如需支援的電子郵件用戶端及其版本清單，請參閱以下 ESET 資料庫文章。

即使未啟用整合，電子郵件通訊仍會受到電子郵件用戶端防護模組 (POP3、IMAP) 保護。

如果在處理電子郵件用戶端 (僅限 MS Outlook) 時發生系統速度減慢，請開啟 **[停用收件匣內容變更檢查]**。當從 Kerio Outlook Connector Store 擷取電子郵件時會發生這種狀況。

要掃描的電子郵件

已接收的電子郵件 - 可切換接收郵件的檢查。
已傳送的電子郵件 - 可切換傳送郵件的檢查。
已閱讀的電子郵件 - 可切換讀取郵件的檢查。

針對受感染電子郵件執行的處理方法

不進行處理 - 如果啟用，則程式會識別受感染附件，但不會對電子郵件採取任何處理方法。
刪除電子郵件 - 程式會通知使用者有關入侵的資訊並刪除該訊息。
將受感染電子郵件移到刪除的郵件資料夾 - 自動將受感染電子郵件移至 [刪除的郵件] 資料夾。
將受感染電子郵件移到資料夾 - 自動將受感染電子郵件移至指定的資料夾。

資料夾 - 指定偵測到受感染電子郵件時，要將其移到哪個自訂資料夾。

更新後重複掃描 - 可切換為在病毒資料庫更新後重新掃描。

接受其他模組的掃描結果 - 如果選取此選項，則電子郵件防護模組會接受其他防護模組 (POP3、IMAP 通訊協定掃描) 的掃描結果。

4.2.2.2 電子郵件通訊協定

在電子郵件用戶端應用程式中，IMAP 和 POP3 通訊協定是接收電子郵件通訊使用最廣泛的通訊協定。網際網路訊息存取通訊協定 (IMAP) 是另一種用於擷取電子郵件的網際網路通訊協定。IMAP 有些優點凌駕 POP3，例如多重用戶端可以同時連接到相同信箱，並維持郵件狀態資訊 (例如郵件是否已讀取、回覆或刪除)。無論使用的電子郵件用戶端為何，ESET Smart Security 均可防護這些通訊協定，而無須重新配置電子郵件用戶端。

提供此控制項的防護模組會自動在系統啟動時同時啟動，接著在記憶體中發生作用。IMAP 通訊協定控制會自動執行，不需要重新配置電子郵件用戶端。依預設，系統會掃描連接埠 143 上的所有通訊，不過您可以視需要新增其他通訊連接埠。多個連接埠號必須以逗號分隔。

您可以在 [進階] 設定中配置 IMAP/IMAPS 和 POP3/POP3S 通訊協定檢查。若要存取此設定，請展開 **[Web 和電子郵件]** > **[電子郵件用戶端防護]** > **[電子郵件通訊協定]**。

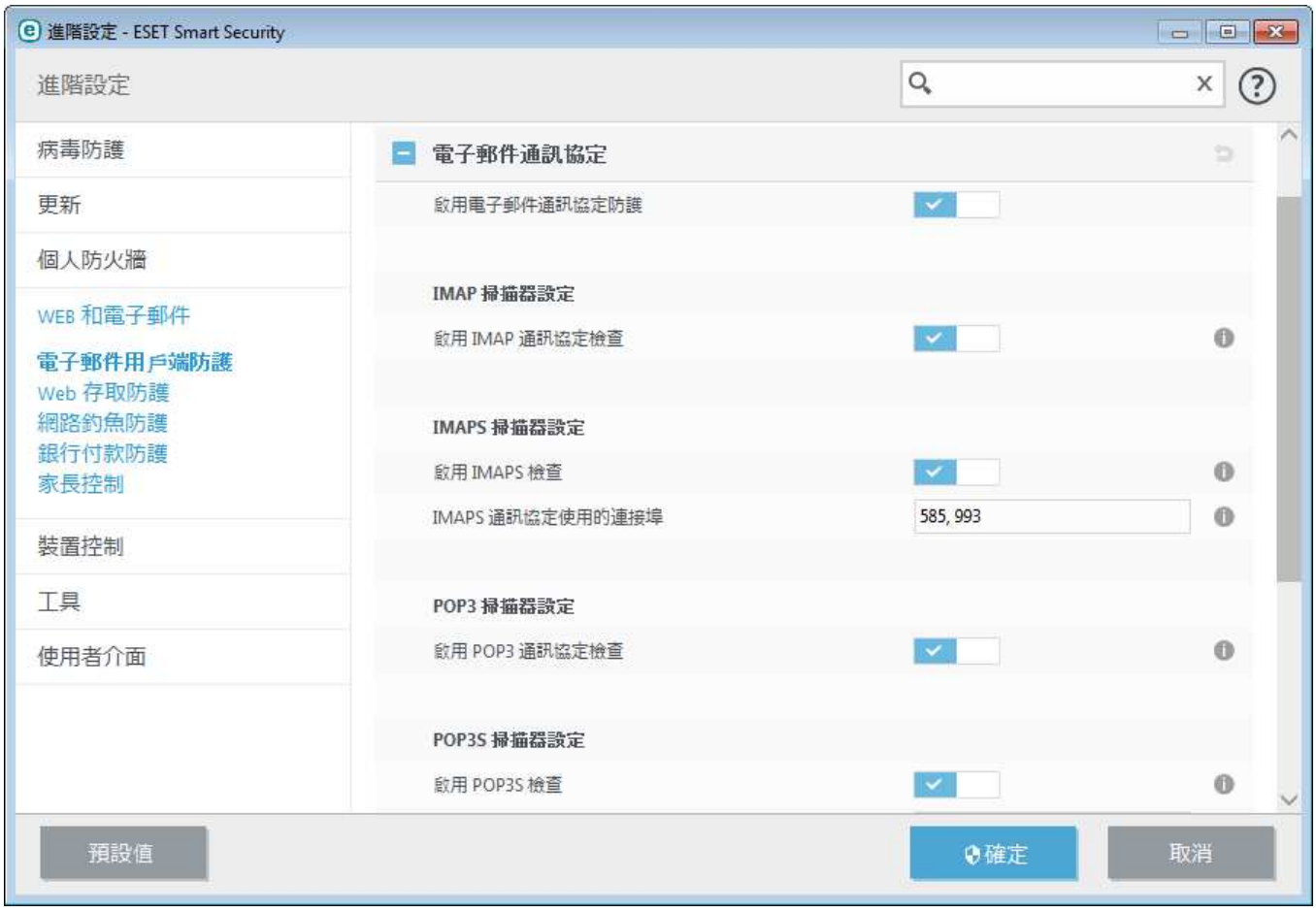
啟用電子郵件通訊協定防護 - 允許檢查電子郵件通訊協定。

在 Windows Vista 和更新版，所有連接埠會自動偵測並掃描 IMAP 和 POP3 通訊協定。在 Windows XP 中，只會針對所有應用程式掃描已配置的 **IMAP/POP3 通訊協定所使用的連接埠**，並且會針對標記為 Web 和電子郵件用戶端的應用程式掃描所有連接埠。

ESET Smart Security 也支援掃描 IMAPS 和 POP3S 通訊協定，其使用加密的通道以在伺服器與用戶端間傳輸資訊。ESET Smart Security 會檢查利用 SSL (安全通訊端層) 與 TLS (傳輸層安全性) 通訊協定的通訊。此程式將只掃描 **IMAPS/POP3S**

通訊協定使用的連接埠中定義的連接埠之流量，無論其作業系統的版本為何。

不掃描加密的通訊。若要掃描加密的通訊並且檢視掃描器設定，請瀏覽至 [進階設定] 區段中的 SSL/TLS，按一下 **[Web 和電子郵件]** > **[SSL/TLS]**，並啟用 **[啟用 SSL/TLS 通訊協定過濾]** 選項。



4.2.2.3 警告及通知

電子郵件防護可控制透過 POP3 及 IMAP 通訊協定收到的電子郵件通訊。使用 Microsoft Outlook 及其他電子郵件用戶端的外掛程式，ESET Smart Security 可控制來自電子郵件用戶端的所有通訊 (POP3、MAPI、IMAP、HTTP)。當檢查對內的郵件時，程式會使用包含在 ThreatSense 掃描引擎中的所有進階掃描方法。這表示即使針對病毒資料庫進行比較之前，也會發生惡意程式的偵測。POP3 及 IMAP 通訊協定的掃描獨立於所使用的電子郵件用戶端。

在 **[Web 和電子郵件]** > **[電子郵件用戶端防護]** > **[警告及通知]** 下的 **[進階設定]** 可找到此功能的選項。

ThreatSense 參數 - 進階病毒掃描器設定，可讓您配置掃描目標、偵測方法等。按一下以顯示詳細的病毒掃描器設定視窗。

檢查電子郵件之後，帶有掃描結果的通知會附加到訊息。您可以選取 **[將標籤訊息附加到已接收並已閱讀的郵件]**？**[將附註附加到已接收、已閱讀且受感染電子郵件的主旨]** 或 **[將標籤訊息附加到已傳送的郵件]**。請注意，雖然這些情況不常發生，但是標籤訊息有可能會在有問題 HTML 訊息中省略，或訊息由惡意程式所產生。標籤訊息可以新增至已接收及已讀取的電子郵件或已傳送的電子郵件 (或兩者)。可用的選項是：

- **絕不** - 不會新增任何標籤訊息。
- **僅針對受感染電子郵件** - 只有包含惡意軟體的訊息才會標示為已勾選 (預設值)。
- **針對所有已掃描的電子郵件** - 程式會將訊息附加到所有已掃描的電子郵件。

將附註附加到已傳送之受感染電子郵件的主旨 - 如果您不要讓電子郵件防護在受感染電子郵件的主旨中包含病毒警告，請停用這項功能。此功能允許對受感染電子郵件進行簡單、基於主旨的過濾 (如果電子郵件程式支援的話)。它也會增加收件者的可靠性，而且如果偵測到入侵，則會提供有關指定電子郵件或寄件者的重要資訊。

新增到受感染電子郵件主旨的範本 - 如果您想修改受感染電子郵件的主旨字首格式，請編輯此範本。此功能會將字首值為 *"[virus]"* 的郵件主旨 *"Hello"* 取代成下列格式：*"[virus] Hello"*。變數 *%VIRUSNAME%* 代表偵測到的威脅。

4.2.2.4 與電子郵件用戶端整合

ESET Smart Security 與電子郵件用戶端的整合會針對電子郵件訊息中的惡意代碼，增加作用中的防護層級。如果您的電子郵件用戶端受支援，即可在 ESET Smart Security 中啟用此整合。如果啟用整合，ESET Smart Security 工具列會直接插入電子郵件用戶端，以便更有效進行電子郵件防護。可以透過 **[設定]** > **[進入進階設定...]** 使用整合設定。> **[Web 和電子郵件]** > **[電子郵件用戶端防護]** > **[電子郵件用戶端整合]** 中變更整合設定。

目前支援的電子郵件用戶端包括 Microsoft Outlook、Outlook Express、Windows Mail、Windows Live Mail。如需支援的電子郵件用戶端及其版本清單，請參閱以下 ESET 資料庫文章。

如果在處理電子郵件用戶端時系統速度減慢，請選取 **[停用收件匣內容變更檢查]** 旁的核取方塊。當從 Kerio Outlook Connector Store 擷取電子郵件時會發生這種狀況。

即使未啟用整合，電子郵件通訊仍會受到電子郵件用戶端防護模組 (POP3、IMAP) 保護。

4.2.2.4.1 電子郵件用戶端防護配置

電子郵件用戶端防護模組支援下列電子郵件用戶端：Microsoft Outlook、Outlook Express、Windows Mail、Windows Live Mail 及 Mozilla Thunderbird。電子郵件防護是以外掛程式的形式在這些程式中運作。外掛程式的主要優勢為其獨立於所使用的通訊協定。當電子郵件用戶端接收到加密的郵件，它會將其解密並傳送到病毒掃描器。

4.2.2.5 POP3、POP3S 過濾器

在電子郵件用戶端應用程式中，POP3 通訊協定是接收電子郵件通訊使用最廣泛的通訊協定。無論使用的電子郵件用戶端為何，ESET Smart Security 均可防護此通訊協定。

提供此控制項的防護模組會自動在系統啟動時同時啟動，接著在記憶體中發生作用。若要讓模組正確運作，請確定已啟用它 - 系統會自動執行 POP3 通訊協定檢查，而無需重新配置電子郵件用戶端。依預設，通訊埠 110 中的所有通訊均會經過檢查；必要時，您也可以新增其他通訊埠。多個連接埠號必須以逗號分隔。

不掃描加密的通訊。若要掃描加密的通訊並且檢視掃描器設定，請瀏覽至 [進階設定] 區段中的 SSL/TLS，按一下 **[Web 和電子郵件]** > **[SSL/TLS]**，並啟用 **[啟用 SSL/TLS 通訊協定過濾]** 選項。

您可以在此區段中配置 POP3 與 POP3S 通訊協定檢查。

啟用 POP3 通訊協定檢查 - 如果啟用，則會監視通過 POP3 的所有流量以尋找惡意軟體。

POP3 通訊協定使用的連接埠 - POP3 通訊協定使用的連接埠清單 (預設為 110)。

ESET Smart Security 也支援 POP3S 通訊協定檢查。這類型的通訊使用加密的通道以在伺服器與用戶端間傳輸資訊。ESET Smart Security 會檢查利用 SSL (安全通訊端層) 與 TLS (傳輸層安全性) 加密方法的通訊。

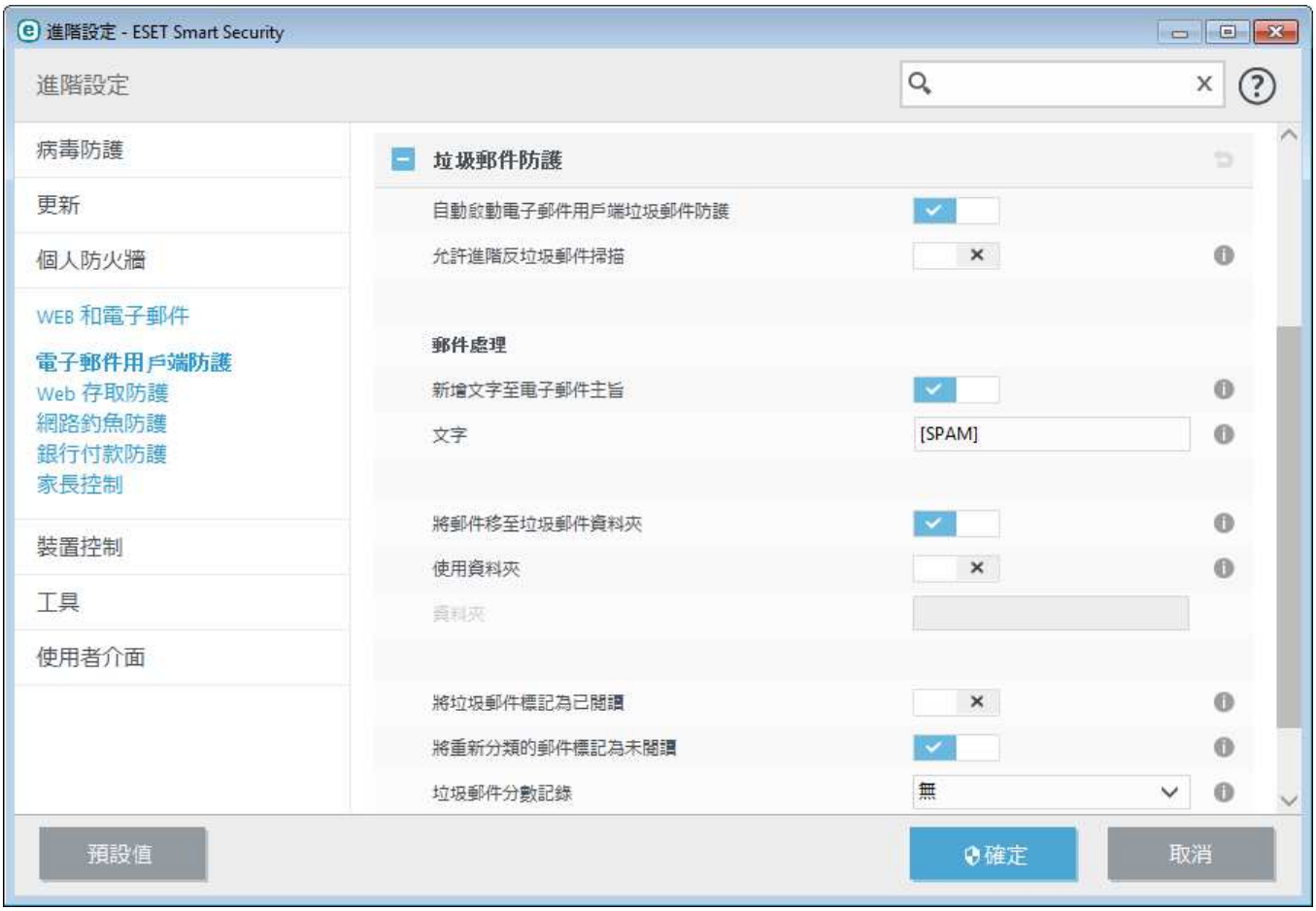
不使用 POP3S 檢查 - 不會檢查加密的通訊。

針對選取的連接埠使用 POP3S 通訊協定檢查 - 勾選此選項以只針對在 **[POP3S 通訊協定使用的連接埠]** 中定義的連接埠啟用 POP3S 檢查。

POP3S 通訊協定使用的連接埠 - 要檢查的 POP3S 連接埠清單 (預設為 995)。

4.2.2.6 垃圾郵件防護

來路不明的電子郵件 (又稱為垃圾郵件) 已成為電子通訊的最大問題。垃圾郵件佔所有電子郵件通訊的 80 %。垃圾郵件防護可用來針對此問題進行防護。垃圾郵件防護模組結合數種電子郵件安全性原則，能夠提供卓越的過濾結果讓收件匣免除垃圾郵件。



垃圾郵件偵測中的一個重要原則是：可以根據預先定義的信任地址 (白名單) 及垃圾郵件地址 (黑名單)，識別來路不明的電子郵件。連絡人清單中的所有地址及您標記為安全的所有其他地址，都會自動新增至白名單。

用於偵測垃圾郵件的主要方法是掃描電子郵件訊息屬性。針對基本垃圾郵件防護條件 (郵件定義、統計啟發式、識別演算法及其他唯一方法) 掃描收到的郵件，而且產生的索引值會決定郵件是否為垃圾郵件。

自動啟動電子郵件用戶端垃圾郵件防護 - 啟用時，將在系統啟動時自動啟動垃圾郵件防護。

允許進階反垃圾郵件掃描 - 將定期下載其他反垃圾郵件資料，以提高反垃圾郵件能力，並達到較好的結果。

ESET Smart Security 的垃圾郵件防護可讓您設定不同的參數來處理郵件清單。選項如下：

郵件處理

新增文字至電子郵件主旨 - 可讓您將自訂字首字串新增至已分類為垃圾郵件的郵件主旨行中。預設值是 [SPAM]。

將郵件移至垃圾郵件資料夾 - 啟用時，垃圾郵件將移至預設垃圾電子郵件資料夾，而重新分類為非垃圾郵件的訊息會移至收件匣。在電子郵件上按一下滑鼠右鍵並從內容功能表選取 ESET Smart Security 後，您可以從應用程式選項中選擇。

使用資料夾 - 此選項會將垃圾郵件移至使用者定義的資料夾。

將垃圾郵件標記為已閱讀 - 啟用此選項，以自動將垃圾郵件標記為已閱讀。這將有助您著眼於「非垃圾」郵件。

將重新分類的郵件標記為未閱讀 - 起初分類為垃圾郵件而稍後標記為「清除」的郵件將顯示為未閱讀。

垃圾郵件分數記錄- ESET Smart Security 垃圾郵件防護引擎會將垃圾郵件分數指派給各個掃描的郵件。郵件將記錄於垃圾郵件防護記錄 中 (**[ESET Smart Security]** > **[工具]** > **[防護記錄檔案]** > **[垃圾郵件防護]**)。

- **無** - 垃圾郵件掃描的分數將不記錄。
- **重新分類並標示為垃圾郵件** - 如果想要記錄已標示為「垃圾郵件」之郵件的垃圾郵件分數，請選取此選項。
- **所有** - 所有郵件及其垃圾郵件分數都會記錄至防護記錄中。

附註: 按一下垃圾電子郵件資料夾中的郵件時，您可以選擇 **[將選取的郵件重新分類為非垃圾郵件]**，郵件即會移至收件匣。按一下收件匣中您認為是垃圾郵件的郵件後，您可以選取 **[將郵件重新分類為垃圾郵件]**，郵件即會移至垃圾電子郵件資料夾。您可以選取多封電子郵件，然後同時對這些郵件執行動作。

附註：ESET Smart Security 針對 Microsoft Outlook、Outlook Express、Windows Mail 和 Windows Live Mail 支援垃圾郵件防護。

4.2.3 通訊協定過濾

應用程式通訊協定的病毒防護由 ThreatSense 掃描引擎控制，該引擎可密切地整合所有進階惡意程式掃描技術。無論是使用網際網路瀏覽器或電子郵件用戶端，通訊協定過濾都會自動運作。想編輯加密 (SSL/TLS) 設定，請移至 **[Web 和電子郵件]** > **[SSL/TLS]**。

啟用應用程式通訊協定內容過濾 - 可用於停用通訊協定過濾。請注意，許多 ESET Smart Security 元件 (Web 存取防護、電子郵件通訊協定防護、網路釣魚防護、Web 控制) 必須啟用此選項才能正常運作。

排除的應用程式 - 允許您從通訊協定過濾排除特定的應用程式。對於通訊協定過濾導致相容性問題時很有幫助。

排除的 IP 位址 - 允許您從通訊協定過濾排除特定的遠端位址。對於通訊協定過濾導致相容性問題時很有幫助。

Web 和電子郵件用戶端 - 只適用於 Windows XP 作業系統，可讓您選取所有流量皆經過通訊協定過濾的應用程式，無論使用何種連接埠。

4.2.3.1 Web 和電子郵件用戶端

附註：從 Windows Vista Service Pack 1 與 Windows Server 2008 起，新的 Windows 過濾平台 (WFP) 架構就被用來檢查網路通訊。由於 WFP 技術使用特殊監視技術，因此無法使用 **[Web 和電子郵件用戶端]** 區段。

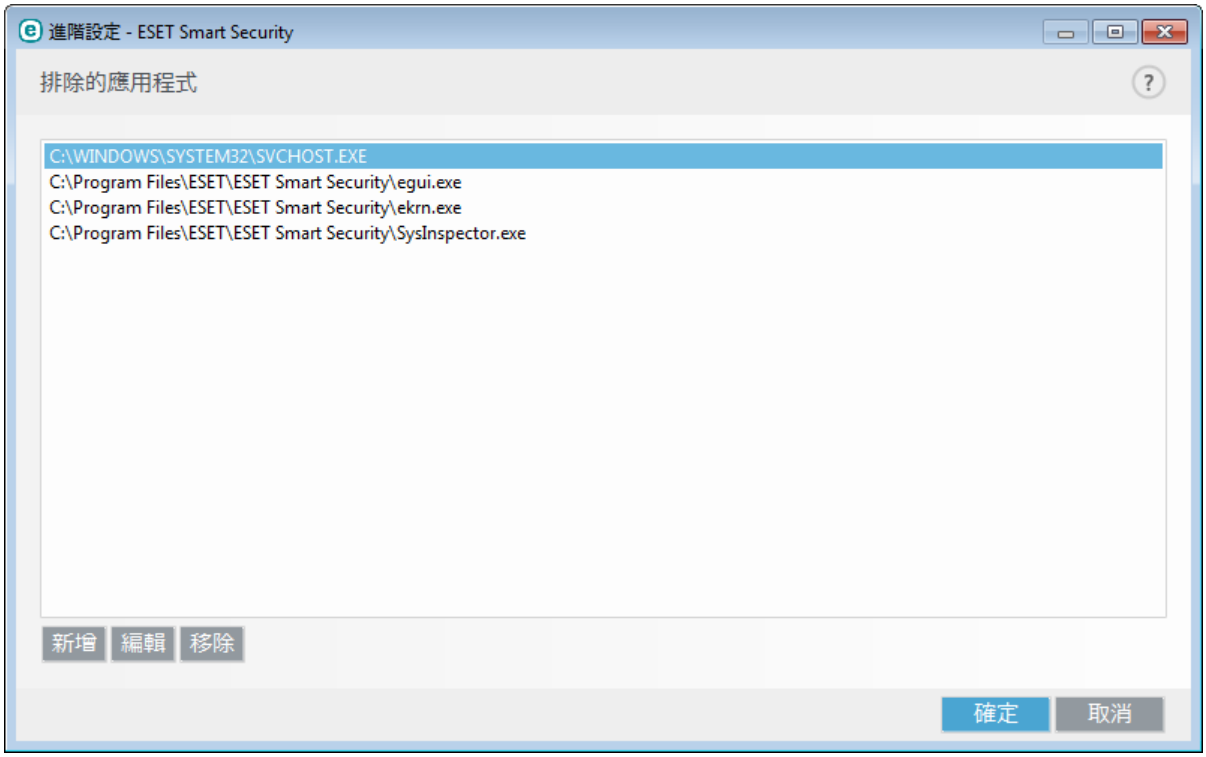
由於在網際網路周圍散佈著大量的惡意代碼，因此能安全地瀏覽網際網路是電腦防護非常重要的面向。網路瀏覽器的弱點和詐騙連結會幫助惡意代碼在不被察覺的情況下進入系統，這也就是 ESET Smart Security 著重在網路瀏覽器安全性的原因之一。每個存取網路的應用程式都可以標記為網際網路瀏覽器。核取方塊有兩種狀態：

- **取消選取** - 只過濾使用指定連接埠的應用程式通訊。
- **已選取** - 永遠過濾通訊 (設定不同的連接埠時亦同)。

4.2.3.2 排除的應用程式

若要將特定的網路識別應用程式排除在內容過濾之外，請在清單中選取這些應用程式。屆時將不會針對所選應用程式的 HTTP/POP3/IMAP 通訊檢查是否存在威脅。建議僅針對在檢查通訊時無法正常運作的應用程式使用此選項。

執行中的應用程式及服務會自動顯示在此處。按一下 **[新增]**，手動新增未顯示於通訊協定過濾清單上的應用程式。

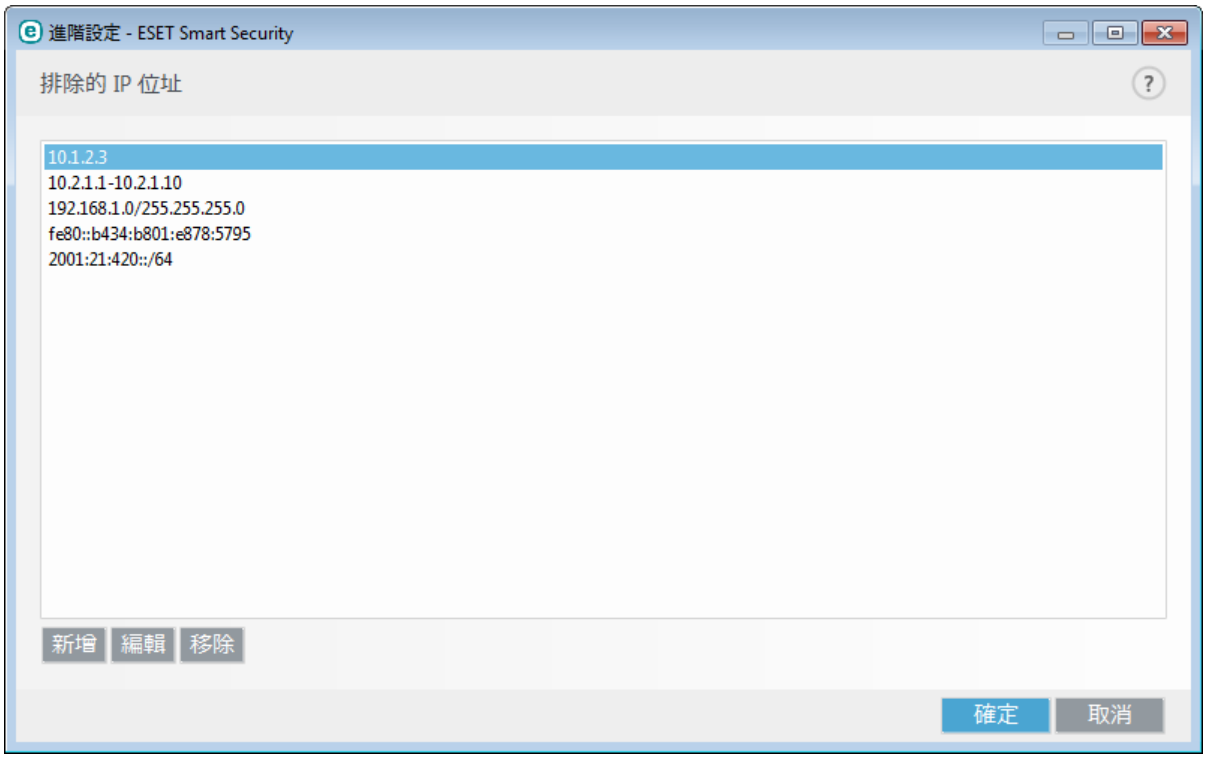


4.2.3.3 排除的 IP 位址

在清單中的項目將排除於通訊協定內容過濾之外。屆時將不會針對所選位址的 HTTP/POP3/IMAP 往來通訊檢查是否存在威脅。我們建議只將此選項用於已知值得信賴的位址。

按一下 **[新增]** 以排除通訊協定過濾清單位顯示的遠端位置 IP 位址/位址範圍/子網路。

按一下 **[移除]** 從清單中移除選取的項目。



4.2.3.3.1 新增 IPv4 位址

這可讓您新增要套用規則的遠端位置 IP 位址/位址範圍/子網路。網路通訊協定版本 4 是較舊的版本，但仍被廣為使用。

單一位址 - 新增要套用規則之個別電腦的 IP 位址 (例如 *192.168.0.10*)。

位址範圍 - 輸入第一個及最後一個 IP 位址以指定要套用規則的 (數台電腦) IP 範圍 (例如 *192.168.0.1* 至 *192.168.0.99*)。

子網路 - IP 位址及遮罩定義的子網路 (電腦群組)。

例如，*255.255.255.0* 是 *192.168.1.0/24* 字首的網路遮罩，這表示 *192.168.1.1* 到 *192.168.1.254* 的位址範圍。

4.2.3.3.2 新增 IPv6 位址

這可讓您新增要套用規則的遠端位置 IPv6 位址/子網路。這是最新版本的網際網路通訊協定，該版本即將要取代較舊的第 4 版。

單一位址 - 新增要套用規則的個別電腦 IP 位址 (例如 *2001:718:1c01:16:214:22ff:fec9:ca5*)。

子網路 - IP 位址及遮罩定義的子網路 (例如：*2002:c0a8:6301:1::1/64*)。

4.2.3.4 SSL/TLS

ESET Smart Security 能檢查使用 SSL 通訊協定的通訊中是否存在威脅。對於使用信任的憑證、未知憑證或排除在 SSL 防護通訊檢查之外的憑證進行的 SSL 防護通訊，您可以運用各種掃描模式來檢查。

啟用 SSL/TLS 通訊協定過濾 - 若停用通訊協定過濾，將不會掃描使用 SSL 的通訊。

SSL/TLS 通訊協定過濾模式可選擇下列選項：

自動模式 - 預設模式僅會掃描適當的應用程式，例如網頁瀏覽器和電子郵件用戶端。您可選取要掃描其通訊的應用程式來加以覆寫。

互動模式 - 如果您輸入新的 SSL 防護網站 (含有未知憑證)，則會顯示處理方式選取項目對話方塊。此模式可讓您建立將排除在掃描之外的 SSL 憑證列在其中的清單。

原則模式 - 選取此選項可掃描所有 SSL 防護通訊，但不包括排除在檢查之外的憑證所防護的通訊。如果使用未知的已簽署憑證建立新通訊，則不會通知您出現此情況，而且將自動過濾通訊。存取含有標記為信任的不信任憑證 (在信任憑證清單中) 在其中的伺服器時，將允許對於伺服器的通訊，並且將過濾通訊通道的內容。

SSL 過濾應用程式清單 - 可讓您針對特定應用程式自訂 ESET Smart Security 行為。

已知的憑證清單 - 可讓您為特定的 SSL 憑證自訂 ESET Smart Security 行為。

排除使用擴充驗證憑證 (EV) 保護的通訊 - 啟用後，與此類型 SSL 憑證的通訊將會排除而不進行檢查。擴充驗證 SSL 憑證可確保您實際檢視您的網站，而非看似您網站的假網站 (通常為網路釣魚網站)。

封鎖利用過時通訊協定 SSL 第 2 版的加密通訊 - 自動封鎖使用舊版 SSL 通訊協定的通訊。

系統管理員的憑證

將系統管理員的憑證新增至已知瀏覽器 - 為了使 SSL 通訊能在瀏覽器/電子郵件用戶端中正常運作，您需要將 ESET 的系統管理員憑證新增至已知系統管理員憑證 (發行者) 的清單中。啟用後，ESET Smart Security 可自動將 ESET 系統管理員憑證新增至已知瀏覽器中 (例如 Opera 和 Firefox)。對於使用系統憑證儲存區的瀏覽器來說，憑證會自動新增 (例如 Internet Explorer)。

若要將憑證套用至不支援的瀏覽器，請按一下 **[檢視憑證]** > **[詳情]** > **[複製到檔案...]**，再手動匯入至瀏覽器。

憑證有效性

如果使用 TRCA 憑證儲存區無法驗證憑證 - 在某些情況下，無法使用「信任的根憑證授權」(TRCA) 儲存區驗證網站憑證。這表示憑證已由他人 (例如 Web 伺服器或小型企業的管理員) 簽署，因此將此憑證視為受信任憑證的風險不大。大型企業 (例如銀行) 大多使用 TRCA 簽署的憑證。如果設定 **[詢問憑證有效性]** (預設選取)，系統就會提示使用者選取在建立加密通訊時要採取的處理方法。您可選取 **[封鎖使用憑證的通訊]** 一律終止與使用未驗證憑證的網站之間的加密連線。

如果憑證無效或損毀 - 這表示憑證已到期或簽署方式不正確。在此情況下，我們建議維持選取 **[封鎖使用憑證的通**

訊]。

4.2.3.4.1 憑證

為了使 SSL 通訊能在瀏覽器/電子郵件用戶端中正常運作，您需要將 ESET 的系統管理員憑證新增至已知系統管理員憑證 (發行者) 的清單中。應該啟用 **[將系統管理員的憑證新增至已知瀏覽器]**。選取此選項可自動將 ESET 根憑證新增至已知瀏覽器中 (例如 Opera 和 Firefox)。對於使用系統憑證儲存區的瀏覽器來說，憑證會自動新增 (如 Internet Explorer)。若要將憑證套用至不支援的瀏覽器，請按一下 **[檢視憑證]** > **[詳情]** > **[複製到檔案...]**，然後再手動匯入至瀏覽器。

在某些情況下，無法使用「信任的根憑證授權」儲存區 (例如 VeriSign) 驗證憑證。這表示憑證已由他人 (例如 Web 伺服器或小型企業的管理員) 自我簽署，因此將此憑證視為受信任憑證的風險不大。大型企業 (例如銀行) 大多使用 TRCA 簽署的憑證。如果設定 **[詢問憑證有效性]** (預設選取)，系統就會提示使用者選取在建立加密通訊時要採取的處理方法。這樣會顯示處理方法選取項目對話方塊，讓您能決定將憑證標示為受信任或排除。如果 TRCA 清單中沒有憑證，視窗就會變成紅色。如果 TRCA 清單中有憑證，視窗就會變成綠色。

您可以選取 **[封鎖使用憑證的通訊]**，一律終止與使用未驗證憑證的網站之間的加密連線。

如果憑證無效或損毀，則表示憑證已到期或自我簽署方式不正確。在此情況下，我們建議封鎖使用該憑證的通訊。

4.2.3.4.2 已知的憑證清單

[已知的憑證清單] 可用於為特定的 SSL 憑證自訂 ESET Smart Security 行為，且若在 **[SSL/TLS 通訊協定過濾模式]** 中選取 **[互動模式]**，則可記住選擇的處理方法。您可於**[進階設定]** (F5) > **[Web 和電子郵件]** > **[SSL/TLS]** > **[已知的憑證清單]** 中檢視與編輯清單。

[已知的憑證清單] 視窗包含：

直欄

名稱 - 憑證名稱。

憑證發行者 - 憑證建立者名稱。

憑證主旨 - 主旨欄位可識別與主旨公用金鑰欄位中所儲存公用金鑰相關聯的實體。

存取 - 選取作為 **[存取處理方法]** 的 **[允許]** 或 **[封鎖]** 以允許/封鎖憑證認為安全的通訊，無論憑證的可信任度為何。選取 **[自動]** 以允許信任的憑證並要求不信任的憑證。選取 **[詢問]** 以一律詢問使用者處理方法。

掃描 - 選取作為 **[掃描處理方法]** 的 **[掃描]** 或 **[略過]** ，以掃描或忽略此憑證認為安全的通訊。選取 **[自動]** 以於自動模式中掃描並於互動模式中詢問。選取 **[詢問]** 以一律詢問使用者處理方法。

控制項元素

編輯 - 選取您想配置的憑證並按一下 **[編輯]**。

移除 - 選取您想刪除的憑證並按一下 **[移除]**。

確定/取消 - **若您想儲存變更，請按一下** [確定]**，或若您想離開而不儲存，請按一下** [取消]。

4.2.3.4.3 SSL 過濾應用程式清單

[SSL 過濾應用程式清單] 可用於為特定的應用程式自訂 ESET Smart Security 行為，且若在 **[SSL 通訊協定過濾模式]** 中選取 **[互動模式]**，則可記住選擇的處理方法。您可於**[進階設定]** (F5) > **[Web 和電子郵件]** > **[SSL/TLS]** > **[SSL 過濾應用程式清單]** 中檢視與編輯清單。

[SSL 過濾應用程式清單] 視窗包含：

直欄

應用程式 - 應用程式名稱。

掃描處理方法 - 選取 **[掃描]** 或 **[忽略]** 來掃描或略過通訊。選取 **[自動]** 以於自動模式中掃描並於互動模式中詢問。選取 **[詢問]** 以一律詢問使用者處理方法。

控制項元素

新增 - 新增過濾應用程式。

編輯 - 選取您想配置的憑證並按一下 **[編輯]**。

移除 - 選取您想刪除的憑證並按一下 **[移除]**。

確定/取消 - **若您想儲存變更，請按一下** [確定]，**或若您想離開而不儲存，請按一下** [取消]。

4.2.4 網路釣魚防護

網路釣魚這個詞彙是用來定義利用社交工程 (操縱使用者以取得機密資訊) 的犯罪活動。網路釣魚通常用於存取像是銀行帳號、PIN 碼等敏感資料。請在字彙中閱讀更多有關此活動的資訊。ESET Smart Security 提供網路釣魚防護，封鎖已知會散佈這類內容的網頁。

強烈建議您啟用 ESET Smart Security 中的網路釣魚防護。若要這麼做，請開啟 **[進階設定]** (F5)，然後瀏覽至 **[Web 和電子郵件]** > **[網路釣魚防護]**。

造訪我們的知識庫文章以取得 ESET Smart Security 中網路釣魚防護的詳細資訊。

存取網路釣魚網站

存取已識別的網路釣魚網站時，Web 瀏覽器中會顯示下列對話方塊。如果您仍想存取網站，請按一下 **[略過威脅]** (不建議)。

附註： 已列入白名單的潛在網路釣魚網站會依預設在數小時後過期。若要能永久存取該網站，請使用 URL 位址管理工具。從 **[進階設定]** (F5) 展開 **[Web 和電子郵件]** > **[Web 存取防護]** > **[URL 位址管理]**> **[位址清單]**，按一下 **[編輯]** ，再新增您要編輯的網站至此清單。

網路釣魚網站回報

回報連結可讓您向 ESET 回報網路釣魚/惡意網站以供分析。

附註： 在將網站提交至 ESET 之前，請確定其符合下列一或多個條件：
- 完全未偵測該網站、
- 錯將該網站偵測為威脅。在這個情況下，您可以報告不當封鎖的頁面。

或者您可以使用電子郵件提交該網站。將您的電子郵件傳送至 samples@eset.com。請記得使用敘述性主旨，並盡可能提供網站的相關資訊 (例如，您是從哪一個網站參照至該網站、您如何得知該網站等等)。

4.3 網路防護

個人防火牆可控制所有由系統接收及發出的網路流量。此作業係以過濾規則為根據，藉此達成允許或拒絕個別網路連線。它可提供保護以免於遭受遠端電腦的攻擊，並封鎖某些服務。另可提供 HTTP、POP3 及 IMAP 通訊協定的病毒防護。此功能是電腦安全中非常重要的一個元素。

您可以在**[網路防護]** 下方的 **[設定]** 窗格中找到個人防火牆配置。在此可讓您調整過濾模式、規則及詳細設定。您也可以按一下 **[個人防火牆]** 旁邊的齒輪 ⚙ > **[配置...]** 以存取更多詳細設定，或是按下 **F5** 來存取 [進階設定]。

按一下 **個人防火牆** 旁邊的齒輪 ⚙ 以存取下列設定：

配置... - 開啟 [進階設定] 中的個人防火牆視窗，您可在其中定義防火牆處理網路通訊的方式。

暫停防火牆 (允許所有流量) - 是封鎖所有網路流量的相反配置。如果選取此選項，則會關閉所有個人防火牆過濾選項，允許所有對內及對外連線。當網路流量過濾處於此模式時，按一下 **[啟用防火牆]** 以重新啟用防火牆。

封鎖所有流量 - 個人防火牆會封鎖所有外來及對外通訊。僅當您懷疑存在嚴重安全風險，需要中斷系統與網路連線時才使用此選項。當網路流量過濾處於 **[封鎖所有流量]** 模式時，按一下 **[停止封鎖所有流量]** 將防火牆還原為正常作業。

自動模式 - (啟用其他過濾模式時) - 按一下可變更過濾模式為自動過濾模式 (含使用者定義規則)。

互動模式 - (啟用其他過濾模式時) - 按一下可變更過濾模式為互動過濾模式 (含使用者定義規則)。

網路攻擊防護 (IDS) - 分析網路流量內容以及防護其免於網路攻擊。將封鎖視為有害的流量。

殭屍網路防護 - 快速及準確地發現系統裡的惡意程式。

連線的網路 - 顯示網路介面卡要連線的網路。按一下網路名稱下方的連結之後，系統會提示您選取透過網路介面卡連線的網路防護類型 (完全或允許)。此設定定義網路中其他電腦對您電腦擁有的存取權限。

暫時 IP 位址黑名單 - 檢視已偵測為攻擊來源的 IP 位址清單，並新增至黑名單中以封鎖特定期間的連線。如需詳細資訊，請按一下此選項，然後按 F1。

疑難排解精靈 - 幫助您解決 ESET 個人防火牆所造成的連線問題。如需詳細資訊，請參閱「疑難排解精靈」。

4.3.1 個人防火牆

個人防火牆可控制所有由系統接收及發出的網路流量。此作業係以指定過濾規則為根據，藉此達成允許或拒絕個別網路連線。它可提供保護以免於遭受遠端電腦的攻擊，並封鎖某些服務。另可提供 HTTP、POP3 和 IMAP 通訊協定的病毒防護。此功能是電腦安全中非常重要的一個元素。

啟用個人防火牆 - 我們建議您保持此功能啟用以提高防護程度。如此即可雙向掃描網路流量。

啟用網路攻擊防護 (IDS) - 分析網路流量內容以及防護其免於網路攻擊。將封鎖任何視為有害的流量並防止來自網路的攻擊。

啟用殭屍網路防護 - 在電腦受到感染且 Bot 嘗試通訊時，透過辨識模式偵測並封鎖與惡意指令及控制伺服器相關聯的通訊。

過濾模式 - 防火牆行為的變更係以過濾的模式為根據。過濾模式還影響需要使用者互動的層級。ESET Smart Security 個人防火牆提供下列過濾模式：

自動模式 - 預設模式。此模式適用於喜歡簡便易行的防火牆使用方法而無需定義規則的使用者。雖然可以建立自訂的使用者定義規則，不過自動模式並未強制使用這類規則。自動模式允許指定系統的所有對外流量，並封鎖大多數的外來流量 (除了來自 IDS 及進階選項/允許的服務所指定「信任區域」的某些流量，以及回應最近對外通訊的外來流量)。

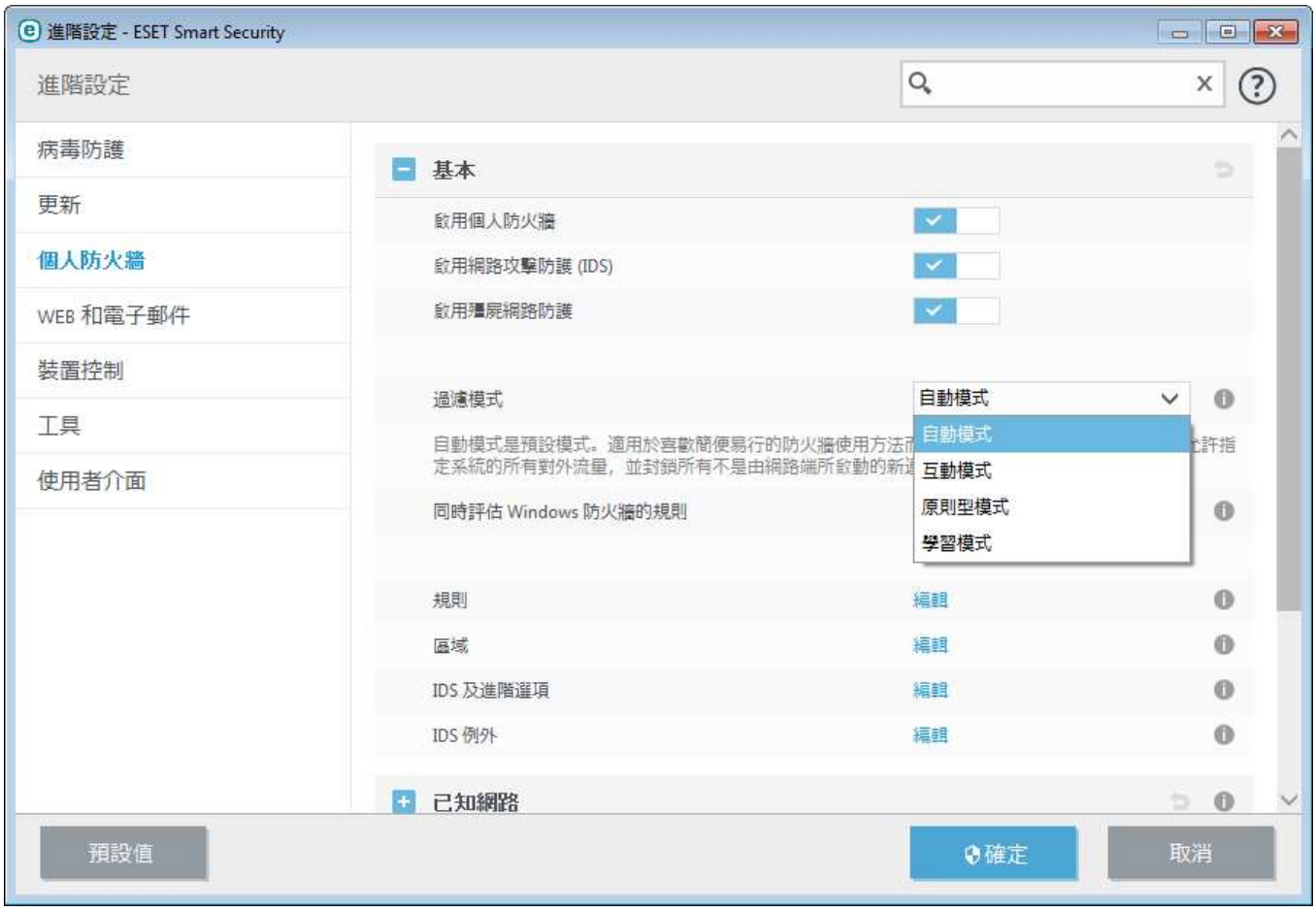
互動模式 - 可讓您針對個人防火牆建置自訂配置。當偵測到通訊但沒有適用的規則時，將會顯示一個對話方塊視窗，報告不明連線。該對話方塊視窗提供允許及拒絕通訊的選項，且該允許或拒絕的決定將儲存成個人防火牆的新規則。如果您選擇建立新規則，則系統會根據該規則，允許或封鎖將來所有此類型的連線。

原則型模式 - 會封鎖所有尚未在特定規則中定義為允許的連線。此模式允許進階使用者定義僅允許所需及安全連線的規則。個人防火牆將會封鎖所有其他未指定的連線。

學習模式 - 自動建立及儲存規則；此模式適用於個人防火牆的起始配置。因為 ESET Smart Security 會根據預先定義的參數來儲存規則，所以不需要與使用者互動。在建立所需通訊的所有規則之後，您應停止使用學習模式以避免安全性風險。

設定檔可透過指定不同情況下的不同規則集，用來自訂 ESET Smart Security 個人防火牆的行為。

同時評估 Windows 防火牆的規則 - 在自動模式中，會允許 Windows 防火牆所允許的傳入流量，除非該流量遭到個人防火牆規則封鎖。



規則 - 在此可讓您新增規則，以及定義個人防火牆處理網路流量的方式。

區域 - 在此您可以建立包含一或多個安全 IP 位址的區域。

IDS 及進階選項 - 讓您配置進階過濾選項以及 IDS 功能 (用來偵測數種類型的攻擊與弱點)。

IDS 例外 - 讓您新增 IDS 例外，並自訂遇到惡意活動時要採取的反應。

附註： 當遭到殭屍網路攻擊時，您可以為電腦建立 IDS 例外。您可以在 **[進階設定]** (F5) > **[個人防火牆]** > **[IDS 例外]** 修改例外。

4.3.1.1 學習模式設定

學習模式可針對系統中已建立的個別通訊自動建立及儲存規則。因為 ESET Smart Security 會根據預先定義的參數來儲存規則，所以不需要與使用者互動。

此模式可能導致您的電腦暴露在風險中，建議您只用於個人防火牆的初始配置。

在 **[進階設定]** (F5) > **[個人防火牆]** > **[學習模式設定]** 中啟動「學習模式」，以顯示「學習模式」選項。此區段含有下列項目：

警告 在「學習模式」中，個人防火牆不會過濾通訊。所有對外與對內通訊均可通行。在此模式中，您的電腦未受到個人防火牆的完整保護。

通訊類型 - 針對各種類型的通訊選取特定的規則建立參數。共有四種通訊類型：

- **來自「信任區域」的外來流量** - 來自信任區域的對內連線範例，就是來自信任區域內的遠端電腦正在嘗試與電腦上執行中的本機應用程式建立通訊。
- **至「信任區域」的對外流量** - 正在嘗試與區域網路內，或信任區域中網路內另一台電腦建立連線的本機應用程式。
- **外來網際網路連線** - 正在嘗試與電腦上執行中應用程式進行通訊的遠端電腦。
- **對外網際網路連線** - 正在嘗試與另一台電腦建立連線的本機應用程式。

每個區段可讓您定義要加入新建立之規則的參數：

新增本機連接埠 - 納入網路通訊的本機連接埠號碼。對於對外通訊來說，通常會隨機產生號碼。因此，我們建議您只針對對內通訊啟用此選項。

新增應用程式 - 納入本機應用程式的名稱。此選項適用於日後建立應用程式層級的規則 (定義整個應用程式之通訊的規則)。例如，您可以只啟用 Web 瀏覽器或電子郵件用戶端的通訊。

新增遠端連接埠 - 納入網路通訊的遠端連接埠號碼。例如，您可以允許或拒絕與標準連接埠號碼 (HTTP - 80、POP3 - 110 等) 相關的特定服務。

新增遠端 IP 位址/信任區域 - 對於定義所有本機系統與指定遠端位址/區域間網路連線的新規則來說，遠端 IP 位址或區域可用為這些規則的參數。此選項適用於當您想定義特定電腦或網路電腦群組的處理方法時。

應用程式的相異規則數目上限 - 如果應用程式透過不同連接埠與多個 IP 位址通訊，則學習模式中的防火牆可建立適當數量的應用程式規則。此選項允許您限制可針對一個應用程式建立的規則數量。

4.3.2 防火牆設定檔

設定檔可用於控制 ESET Smart Security 個人防火牆的行為。建立或編輯個人防火牆規則時，可以將它指派給特定設定檔或套用至每個設定檔。當設定檔在網路介面上作用中時，只會套用全域規則 (未指定設定檔的規則) 與已經指派給該設定檔的規則。您可以建立多個不同規則的設定檔，並將其指派給網路介面卡或網路，輕鬆改變個人防火牆行為。

按一下 **[設定檔清單]** 旁的 **[編輯]** 以開啟 **[防火牆設定檔]** 視窗，您可以在此編輯設定檔。

當網路介面卡連線至特定網路時，可設定為使用針對該網路所配置的設定檔。您也可以在 **[進階設定]** (F5) > **[個人防火牆]** > **[已知網路]** 中，將特定的設定檔指派為用於指定網路。從 **[已知網路]** 清單中選取網路，並按一下 **[編輯]** 以從 **[防火牆設定檔]** 下拉式功能表將防火牆設定檔指派給特定網路。若無指派給該網路的設定檔，則會使用介面卡的預設設定檔。若該介面卡已設定為不使用網路的設定檔，則會使用介面卡的預設設定檔，無論其連線至哪個網路。如果沒有用於網路或介面卡配置的設定檔，則會使用全域預設設定檔。若您想將設定檔指派給網路介面卡，請選取網路介面卡，按一下 **[指派給網路介面卡的設定檔]** 旁的 **[編輯]**，從 **[預設防火牆設定檔]** 下拉式功能表選取設定檔，然後按一下 **[儲存]**。

當個人防火牆切換至其他設定檔時，右下角 (系統時鐘附近) 會出現通知。

4.3.2.1 指派給網路介面卡的設定檔

經由切換設定檔，您可快速進行多個防火牆行為變更。您可以設定自訂規則以套用在特定的設定檔中。電腦上所有介面卡上的網路介面卡項目已自動新增至 **[網路介面卡]** 清單。

直欄

名稱 - 網路介面卡的名稱。

預設防火牆設定檔 - 如果您連線的網路沒有已配置的設定檔，或網路介面卡已設定為不使用網路設定檔，則會使用預設的設定檔。

偏好網路設定檔 - 當**偏好連線網路的防火牆設定檔** 啟用時，網路介面卡將盡量使用指派給已連線網路的防火牆設定檔。

控制項元素

新增 - 新增新的網路介面卡。

編輯 - 允許您編輯現有網路介面卡。

移除 - 如果您想將某個網路介面卡從清單中移除，請選取網路介面卡並按一下 **[移除]**。

確定/取消 - 若您想儲存變更，請按一下 **[確定]**，或按一下 **[取消]** 離開而不進行任何變更。

4.3.3 配置及使用規則

規則代表一組條件，可用來依目的測試所有網路連線，及所有指派給這些條件的處理方法。您可以使用個人防火牆規則定義在建立不同網路連線時所要採取的動作。若要存取規則過濾設定，請瀏覽至 **[進階設定]** (F5) > **[個人防火牆]** > **[基本]**。有些預先定義的規則受來自 **[允許的服務]** (IDS 與進階選項) 的核取方塊限制且無法直接關閉，須透過相關的核取方塊才能關閉。

不同於舊版的 ESET Smart Security，規則會依照最上到最下的形式來評估。第一個相符規則的處理方法會用於評估中的每個網路連線。與舊版本相比，此為一個重要的行為改變，讓規則的優先順序能自動形成，且較為特定的規則比起較為一般的規則擁有更高的優先順序。

連線可劃分為對內及對外連線。對內連線由遠端電腦啟動，嘗試建立與本機系統的連線。對外連線則相反，由本機系統連絡遠端電腦。

如果偵測到新的不明通訊，則您必須仔細考量是允許還是拒絕它。來路不明、不安全或不明的連線對系統造成安全風險。如果建立此類連線，我們建議您特別注意嘗試連接您電腦的遠端電腦及應用程式。許多入侵嘗試取得及傳送私人資料，或將其他惡意應用程式下載到主機工作站。個人防火牆允許您偵測及終止此類連線。

4.3.3.1 防火牆規則

在 **[基本]** 索引標籤區段中，按一下 **[規則]** 旁邊的 **[編輯]** 以顯示 **[防火牆規則]** 視窗，其中會顯示所有規則的清單。**[新增]**? **[編輯]** 和 **[移除]** 讓您新增、配置或刪除規則。您可以選取規則並按一下 **[頂端/向上/向下/底端]**，以調整規則的優先順序層級。

提示: 您可以使用 **[搜尋]** 欄位，透過名稱、通訊協定或連接埠來尋找規則。

直欄

名稱 - 規則的名稱。

已啟用 - 顯示規則為已啟用或已停用，必須選取對應的核取方塊才能啟動規則。

通訊協定 - 此規則能有效運作的通訊協定。

設定檔 - 顯示此規則能有效運作的防火牆設定檔。

處理方法 - 顯示通訊的狀態 (封鎖/允許/詢問)。

方向 - 通訊的方向 (對內/對外/兩者)。

本機 - 本機電腦的 IP 位址和連接埠。

遠端 - 遠端電腦的 IP 位址和連接埠。

應用程式 - 套用規則的應用程式。

控制項元素

新增 - 建立新規則。

編輯 - 讓您編輯現有規則。

移除 - 移除現有規則。

顯示內建 (預先定義的) 規則 - 由 ESET Smart Security 所預先定義用來允許或拒絕特定通訊的規則。您可以停用這些規則，但您無法刪除預先定義的規則。

頂端/向上/向下/底端 - 可讓您調整規則的優先順序層級 (規則會依照最上到最下的形式來評估)。

4.3.3.2 使用規則

每當受監視的參數變更時，都需要修改。若完成的變更導致規則無法滿足條件，且無法套用指定的處理方法，則指定的連線會遭拒絕。這可能會使受該規則影響的應用程式作業發生問題。遠端網路位址或連接埠號碼的變更就是一個範例。

視窗的上部分包含三個索引標籤：

- **一般** - 指定規則名稱、連線方向、處理方法 (**允許**？ **拒絕**？ **詢問**)、通訊協定以及套用規則的設定檔。
- **本機** - 顯示本機的連線資訊，包括本機連接埠編號或連接埠範圍，以及通訊應用程式名稱。您也可以按一下 **[新增]** 透過各種 IP 位址在這裡新增預先定義或建立的區域。
- **遠端** - 此索引標籤包含遠端連接埠 (連接埠範圍) 的相關資訊。它還允許您定義特定規則的遠端 IP 位址或區域的清單。您也可以按一下 **[新增]** 透過各種 IP 位址在這裡新增預先定義或建立的區域。

建立新規則時，必須在 **[名稱]** 欄位中輸入規則的名稱。從 **[方向]** 下拉式功能表中選取規則套用的方向，並從 **[處理方法]** 下拉式功能表中選取通訊符合規則時要執行的處理方法。

通訊協定 代表用於規則的傳送通訊協定。從下拉式功能表中選取針對指定規則使用的通訊協定。

ICMP 類型/代碼 代表已透過數字識別的 ICMP 訊息 (例如，0 代表「回應回覆」)。

所有規則依預設已啟用 **[任何設定檔]** 設定檔。或者，使用 **[設定檔]** 下拉式功能表選取自訂防火牆設定檔。

如果您啟用 **[防護記錄]**，與規則連接的活動將記錄在防護記錄中。**[通知使用者]** 則會在套用規則時顯示通知。

提示: 下面是建立新規則的範例，可讓 Web 瀏覽器應用程式能存取網路。您必須設定下列內容：

- 在 **[一般]** 索引標籤上，啟用透過 TCP 及 UDP 通訊協定對外通訊。
- 在 **[本機]** 索引標籤中新增瀏覽器應用程式 (iexplore.exe 代表 Internet Explorer)。
- 在 **[遠端]** 索引標籤上，若您要允許標準的網際網路瀏覽，則啟用連接埠號碼 80。

附註: 請注意，預先定義的規則之修改方式有限。

4.3.4 配置區域

區域代表建立 IP 位址邏輯群組的網路位址集合，當您需要在多個規則中重複使用相同位址集時，這相當實用。特定群組中的每個位址皆會接受相似規則的指派，這些規則是針對整個群組而集中定義的。此類群組的一個範例為 **[信任區域]**。「信任區域」代表網路位址群組，絕對不會被個人防火牆封鎖。按一下 **[區域]** 旁的 **[編輯]** 按鈕，就可以在 **[進階設定]** > **[個人防火牆]** > **[基本]** 中配置這些區域。若要新增區域，請按一下 **[新增]**，並輸入區域的 **[名稱]**？ **[描述]**，並在 **[遠端電腦位址 (IPv4/IPv6、範圍、遮罩)]** 欄位中新增遠端 IP 位址。

您可以在 **[防火牆區域]** 設定視窗中指定區域名稱、描述、網路位址清單 (另請參閱「已知網路編輯器」)。

4.3.5 已知網路

當您使用的電腦經常連線至公用網路或您一般工作網路以外的網路時，建議您驗證所連線新網路的網路可靠性。定義網路後，ESET Smart Security 可使用 **[網路識別]** 中所配置的各種網路參數來識別信任的 (家用/工作) 網路。電腦通常會以類似信任網路的 IP 位址進入網路。在這種情況下，ESET Smart Security 可能會將未知網路視為信任的 (家用/工作) 網路。建議您使用 **[網路驗證]** 以避免此類型的情況。

當網路介面卡已連線至網路或其網路設定已重新配置時，ESET Smart Security 將搜尋已知網路清單以取得符合新網路的記錄。若 **[網路識別]** 與 **[網路驗證]** (選用) 相符，則此介面中的網路將標記為已連線。若找不到已知網路，系統會使用網路識別配置來建立新的網路，以便在您下次連線時識別該網路。依預設，新網路連線將使用 **[公用]** 防護類型。**[偵測到新網路連線]** 對話方塊視窗將提示您選擇 **[公用]** 或 **[家用/工作]** 防護類型。若網路介面卡已連線至已知網路，且該網路已標記為 **[家用/工作]** 網路，則介面卡的本機子網路將新增至「信任區域」。

附註: 當您選取「**不要求新網路的防護類型。自動將新網路標記為公開**」時，**[偵測到新網路連線]** 對話方塊將不會出現，且連線的網路將自動標記為公開。此將造成特定功能 (例如檔案共用與遠端桌面) 無法從新網路存取。

已知網路可於已知網路編輯器視窗中手動配置。

4.3.5.1 已知網路編輯器

您可以按一下 **[編輯]** 以在 **[進階設定]** > **[個人防火牆]** > **[已知網路]** 中手動配置已知網路。

直欄

名稱 - 已知網路的名稱。

防護類型 - 顯示網路是否已設定為**家用**/**工作**或**公用**。

防火牆設定檔 - 從 **[顯示用於設定檔的規則]** 下拉式功能表選取設定檔，以顯示設定檔的規則過濾器。

控制項元素

新增 - 建立新的已知網路。

編輯 - 按一下以編輯現有已知網路。

移除 - 選取並按一下 **[移除]** 以將其從已知網路清單中移除。

頂端/向上/向下/底端 - 可讓您調整已知網路的優先順序層級 (已知網路會依照最上到最下的形式來評估)。

網路配置設定將細分為下列索引標籤：

網路

您可以在這裡定義網路名稱並選取網路的防護類型 (**[公用]** 或 **[家用/工作]**)。使用 **[防火牆設定檔]** 下拉式功能表以選取該網路的設定檔。如果網路使用的是 **[家用/工作]** 防護類型，則系統會將網路中所有直接連線的子網路視為信任的網路。例如，若網路介面卡使用 IP 位址 192.168.1.5 和子網路遮罩 255.255.255.0 連線至某網路，則其子網路 192.168.1.0/24 會新增至該介面卡的信任區域。若介面卡有更多位址/子網路，也將會新增至信任區域，無論已知網路的 **[網路識別]** 配置為何。

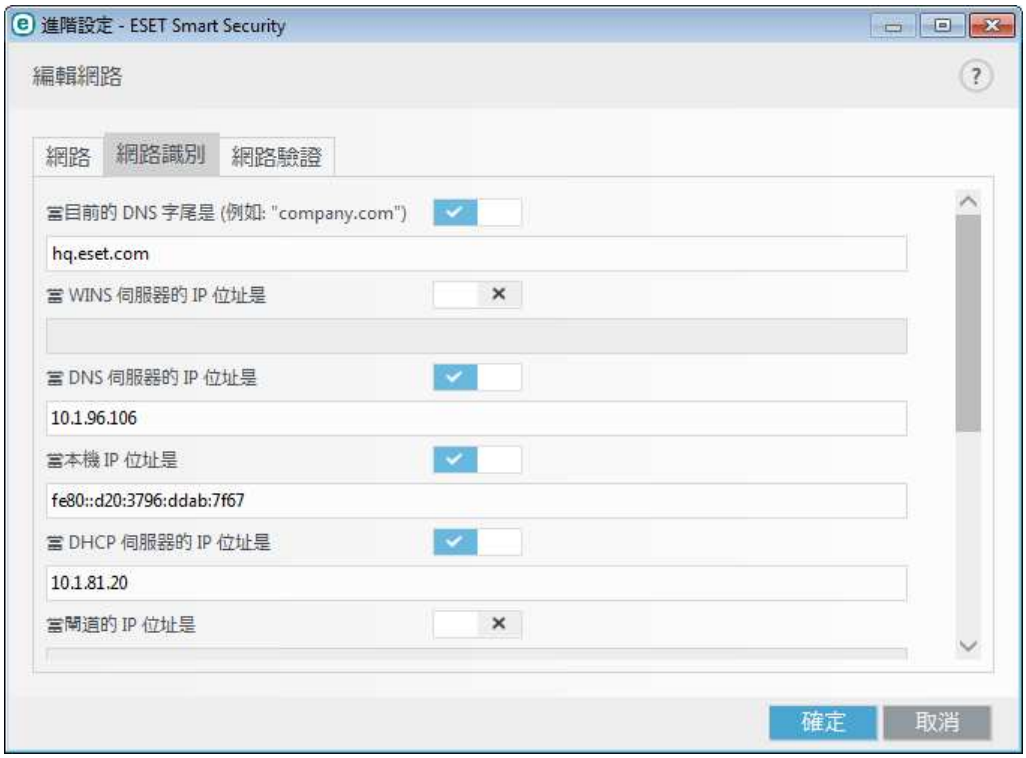
此外，新增於 **[其他信任的位址]** 之下的位址將一律新增至連線到此網路的介面卡的信任區域 (無論該網路的防護類型為何)。

網路必須符合下列條件才會在已連線網路清單中標記為「已連線」：

- 網路識別 - 所有填入的參數必須與作用中的連線參數相符。
- 網路驗證 - 如果已選取驗證伺服器，則必須使用 ESET 驗證伺服器成功執行驗證。
- 網路限制 (僅限於 Windows XP) - 必須滿足所有選取的全域限制。

網路識別

網路識別會根據本機網路介面卡參數來執行。所有選取的參數都會與作用中網路連線的實際參數相比較。允許 IPv4 及 IPv6 位址。

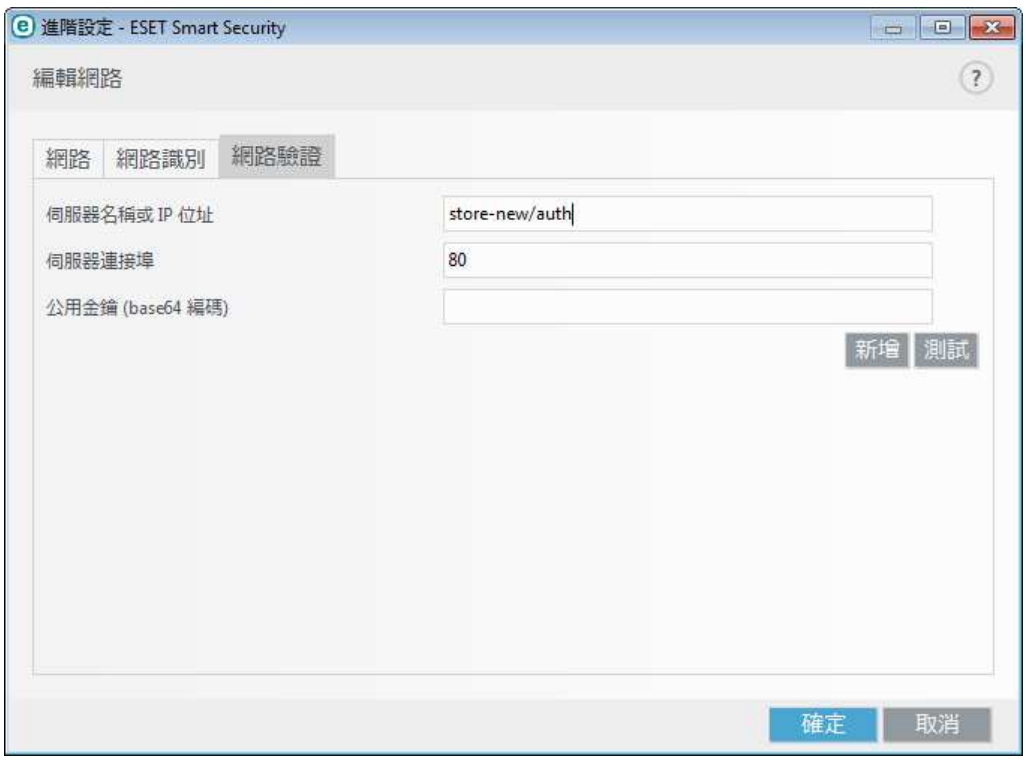


網路驗證

「網路驗證」會搜尋網路中的特定伺服器，並使用非對稱式加密 (RSA) 來驗證伺服器。驗證中的網路名稱必須符合驗證伺服器設定中所設定的區域名稱。名稱有區分大小寫。指定伺服器名稱、伺服器監聽連接埠以及對應私密伺服器金鑰的公用金鑰 (請參閱網路驗證 - 伺服器配置)。伺服器名稱可以 IP 位址、DNS 或 NetBios 名稱的形式輸入，且後面可以跟著路徑，以指定伺服器上的金鑰位置 (例如 server_name_/directory1/directory2/authentication)。您可以透過附加至路徑的方式指定使用的替代伺服器，並以分號分隔。

公用金鑰可以用下列任一種檔案類型匯入：

- PEM 加密公用金鑰 (.pem)，此金鑰可使用 ESET 驗證伺服器產生 (請參閱網路驗證 - 伺服器配置)。
- 加密公用金鑰
- 公用金鑰憑證 (.crt)



按一下 **[測試]** 以測試您的設定。如果驗證成功，就會顯示「*伺服器驗證成功*」。如果未正確配置驗證，則會顯示以下其中一

個錯誤訊息：

伺服器驗證失敗。簽章無效或不相符。
伺服器簽章與輸入的公用金鑰不相符。

伺服器驗證失敗。網路名稱不相符。
已配置的網路名稱無法對應驗證伺服器區域名稱。檢閱這兩個名稱，並確認其名稱相同。

伺服器驗證失敗。無效或伺服器無回應。
若伺服器並未執行或無法存取，則無法接收回應。若其他的 HTTP 伺服器於指定位址執行，則可能會接收到無效的回應。

輸入的公用金鑰無效。
驗證您輸入的公用金鑰檔案並未損毀。

網路限制 (僅限 Windows XP)

於最新的 Windows 作業系統上 (Windows Vista 和更新版)，每個網路介面卡皆有自己的信任區域及作用中的防火牆設定檔。很遺憾，Windows XP 不支援此配置，因此所有網路介面卡將一律共用相同的信任區域及作用中的防火牆設定檔。當電腦同時連線至多個網路時，便會發生潛在性安全風險。在這種情況下，可能會使用為其他已連線網路所配置的信任區域與防火牆設定檔，以評估來自不信任網路的流量。為減輕安全性風險，您可以在連線其他 (潛在不信任的) 網路時使用下列限制以避免全域套用網路配置。

於 Windows XP 上，已連線網路設定 (信任區域及防火牆設定檔) 將全域套用，除非以下限制至少有一項已啟用或未滿足：

a. 只有一個作用中的連線
b. 未建立無線連線
c. 未建立不安全的無線網路

4.3.5.2 網路驗證 - 伺服器配置

驗證程序可由連接到要驗證之網路的任一部電腦/伺服器執行。只要是用戶端嘗試連接到網路時會存取以進行驗證的電腦/伺服器，就必須安裝 ESET 驗證伺服器應用程式。ESET 驗證伺服器應用程式的安裝檔案可從 ESET 網站下載。

安裝 ESET 驗證伺服器應用程式之後，就會出現對話方塊視窗 (您可以隨時按一下 **[開始]** > **[程式集]** > **[ESET]** > **[ESET驗證伺服器]** 存取該應用程式)。

若要配置驗證伺服器，請輸入驗證區域名稱、伺服器監聽連接埠 (預設值為 80)，以及儲存公用金鑰與私密金鑰配對的位置。然後產生將用於驗證程序的公用金鑰與私密金鑰。在防火牆設定中設定區域時，私密金鑰將保留在伺服器上，而公用金鑰則必須匯入「區域」驗證區段中的用戶端。

如需詳細資訊，請閱讀以下 ESET 知識庫文章。

4.3.6 記錄

ESET Smart Security 個人防火牆會將所有重大事件儲存在防護記錄檔案中，您可以從主要功能表直接檢視該檔案。按一下 **[工具]** > **更多工具** > **[防護記錄檔案]**，然後從 **[防護記錄]** 下拉式功能表中選取 **[個人防火牆]**。

防護記錄檔案可用於偵測錯誤，並揭露系統的入侵事件。ESET 個人防火牆防護記錄包含下列資料：

- 事件的日期及時間
- 事件的名稱
- 來源
- 目標網路位址
- 網路通訊協定
- 套用的規則或蠕蟲名稱 (如果已識別)
- 涉及的應用程式
- 使用者

此資料的全面分析可協助偵測影響系統安全的嘗試。許多其他因素可指出潛在的安全風險，並允許您將其影響降至最小：經常與不明位置連線、多次嘗試建立連線、不明應用程式通訊或不常使用的連接埠號碼。

4.3.7 建立連線 - 偵測

個人防火牆會偵測到每個新建立的網路連線。作用中的防火牆模式可決定要針對新規則執行的處理方法。若 **[自動模式]** 或 **[原則型模式]** 已啟動，則個人防火牆會執行預先定義的處理方法，而無需使用者互動。

互動模式會顯示資訊視窗，報告偵測到新網路連線，並附有連線的詳細資訊。您可以選擇允許或拒絕 (封鎖) 連線。如果您在對話方塊視窗中重複允許同一連線，則建議您針對該連線建立新的規則。若要執行此處理方法，請選取 **[建立規則並永久記住規則]**，並將處理方法儲存為個人防火牆的新規則。如果防火牆將來會識別同一連線，則不需要使用者介入便會套用現有規則。

建立新規則時請小心，並且僅允許已知為安全的連線。如果允許所有連線，則個人防火牆無法達到其目的。重要的連線參數如下所示：

- **遠端** - 僅允許連線到受信任的已知位址。
- **本機應用程式** - 不建議允許不明應用程式及處理程序的連線。
- **[連接埠號碼]** - 在正常情況下，應該允許一般連接埠上的通訊 (如 web 流量 - 連接埠號碼 80)。

為求擴散，電腦入侵通常會使用網際網路及隱藏的連線來協助它們感染遠端系統。如果正確地配置規則，則個人防火牆會成為抵禦多種惡意代碼攻擊的有用工具。

4.3.8 使用 ESET 個人防火牆解決問題

若您在使用已安裝的 ESET Smart Security 時遇到連線問題，則可使用幾種方法來判別是否因 ESET 個人防火牆所導致。此外，ESET 個人防火牆還能協助您建立新規則或例外來解決連線問題。

請參閱下列有關協助解決 ESET 個人防火牆相關問題的主題：

- 疑難排解精靈
- 記錄並從防護記錄建立規則或例外
- 從防火牆通知建立例外
- 進階 PCAP 記錄
- 解決通訊協定過濾的相關問題

4.3.8.1 疑難排解精靈

疑難排解精靈會默默地監控所有封鎖的連線，並且將引導您完成疑難排解程序，以便使用特定應用程式或裝置來修正防火牆問題。接下來，精靈會建議您可在核准後進行套用的新規則集。在 **[設定]** > **[網路防護]** 下的主要功能表中可找到 **[疑難排解精靈]**。

4.3.8.2 記錄並從防護記錄建立規則或例外

依預設，ESET 個人防火牆不會記錄所有已封鎖的連線。若您想查看由個人防火牆封鎖的內容，請在 **[進階設定]** 的 **[工具]** > **[診斷]** > **[啟用個人防火牆進階記錄]** 下啟用記錄。若您在防護記錄中發現不希望個人防火牆封鎖的項目，您可以對該項目按一下滑鼠右鍵，並選取 **[日後不再封鎖類似的事件]**，為其建立規則或 IDS 例外。請注意，所有遭封鎖連線的防護記錄可能包含幾千筆項目，因此可能很難在此防護記錄中找到特定的連線。您可以在解決問題之後關閉記錄功能。

如需防護記錄的詳細資訊，請參閱「防護記錄檔案」。

附註: 使用記錄查看個人防火牆封鎖特定連線的順序。此外，從防護記錄建立規則可讓您建立確實需要的規則。

4.3.8.2.1 從防護記錄建立規則

新版的 ESET Smart Security 可讓您從防護記錄建立規則。從主要功能表中按一下 **[工具]** > **[更多工具]** > **[防護記錄檔案]**。從下拉式功能表中選擇 **[個人防火牆]**，在需要的防護記錄項目上按一下滑鼠右鍵，再從內容功能表選擇 **[日後不再封鎖類似的事件]**。這時會出現顯示新規則的通知視窗。

若要允許從防護記錄建立新規則，ESET Smart Security 必須配置為下列設定：

- 在 **[進階設定]** (F5) > **[工具]** > **[防護記錄檔案]** 中，將記錄最簡化設定為 **[診斷]**
- 啟用 **[進階設定]** (F5) > **[個人防火牆]** > **[IDS 與進階選項]** > **[入侵偵測]** 中的 **[也顯示針對安全漏洞傳入攻擊的通知]**。

4.3.8.3 從個人防火牆通知建立例外

當 ESET 個人防火牆偵測到惡意的網路活動時，這時會顯示說明該事件的通知視窗。這項通知包含的連結可讓您瞭解關於事件，以及設定該事件例外 (若您需要) 的更多資訊。

附註: 如果網路應用程式或裝置未正確實作網路標準，可能會觸發重複的防火牆 IDS 通知。您可以直接從通知中建立例外，使 ESET 個人防火牆持續避免偵測此應用程式或裝置。

4.3.8.4 進階 PCAP 記錄

這個功能是用來針對 ESET 客戶支援提供更複雜的防護記錄檔案。僅在 ESET 客戶支援要求時才使用這個功能，因為其可能會產生大量的防護記錄檔案而降低您的電腦速度。

1. 瀏覽至 **[進階設定]** > **[工具]** > **[診斷]** 並啟用 **[啟用個人防火牆進階記錄]**。

2. 嘗試重現您所遇到的問題。

3. 停用進階 PCAP 記錄。

4. 您可以在系統產生診斷記憶體傾印的相同目錄中找到 PCAP 防護記錄檔案：

- Microsoft Windows Vista 或更新版本

  C:\ProgramData\ESET\ESET Smart Security\Diagnostics

- Microsoft Windows XP

  C:\Documents and Settings\All Users\...

4.3.8.5 解決通訊協定過濾的相關問題

若您的瀏覽器或電子郵件用戶端發生問題，這時您要做的第一步是判斷通訊協定過濾是否有回應。若要這樣做，請嘗試在進階設定中暫時停用應用程式通訊協定過濾 (請記得完成之後要重新啟動，否則瀏覽器和電子郵件用戶端不會受到保護)。若問題在過濾關閉之後消失，則可參考下列常見問題和解決方法的清單：

更新或保護通訊問題

若您的應用程式通知您無法更新或某通訊通道不安全：

- 若您已啟用 SSL 通訊協定過濾，請嘗試暫時將其關閉。若這樣有效，您可以排除有問題的通訊，以繼續使用 SSL 過濾，並使更新運作順利：
  將 SSL 通訊協定過濾模式切換成互動模式。重新執行更新。這時應該會出現對話方塊，通知您有關加密網路流量的資訊。請確認應用程式就是您要疑難排解的應用程式，而且憑證看起來是來自其更新來源伺服器。接著選擇記住此憑證的處理方法，並按一下略過。如果沒有顯示其他相關對話方塊，您可以將過濾模式切回自動模式，而問題應該獲得解決。
- 若發生問題的應用程式不是瀏覽器或電子郵件用戶端，您可以完全將其排除在通訊協定過濾之外 (這樣處理瀏覽器或電子郵件用戶端會使您暴露在風險中)。任何通訊受到過濾的應用程式都應該已經在新增例外時所提供給您的清單中，因此不需要手動新增。

存取網路上裝置時遇到的問題

若您無法在網路上使用裝置的任何功能 (可能是指開啟網路攝影機的網頁，或是在家用媒體播放器上播放視訊)，請嘗試將 IPv4 和 IPv6 位址新增到已排除位址清單中。

存取特定網站時遇到的問題

您可以使用 URL 位址管理，從通訊協定過濾中排除特定網站。例如，當您無法存取 https://www.gmail.com/intl/en/mail/help/about.html 時，可嘗試將網址 *gmail.com* 新增到排除位址的清單中。

錯誤「某些有能力匯入管理者認證的應用程式仍然在運行」

當您啟用 SSL 通訊協定過濾時，ESET Smart Security 會確認所安裝的應用程式透過將憑證匯入其憑證儲存區的方式，信任其過濾 SSL 通訊協定的方式。有些應用程式在執行期間無法這樣處理。這包括 Firefox 和 Opera。確定這類應用程式不在執行中 (完成這項操作的最好方法是開啟 [工作管理員]，確定 [處理程序] 索引標籤下面沒有 firefox.exe 或 opera.exe)，接著再點擊重試。

有關不信任的發行人或簽章無效的錯誤

這很可能是指前述的匯入作業失敗。首先，請確定任何上述的應用程式不在執行中。接著，停用 SSL 通訊協定過濾，然後重新啟用。這樣會重新執行匯入作業。

4.4 安全性工具

安全性工具 設定可讓您調整下列模組：

- 銀行和付款防護
- 家長控制
- 防盜

4.4.1 家長控制

[家長控制] 模組可讓您配置家長控制設定，以提供父母自動工具來協助保護他們的子女，並且針對裝置和服務設定限制。主要目的在於避免讓子女和年輕人存取包含不適當或有害內容的頁面。

家長控制功能可讓您封鎖可能包含潛在冒犯性資訊的網頁。此外，家長可禁止存取超過 40 個預先定義的網站類別及 140 多個子類別。

若要啟動特定使用者帳戶的家長控制，請遵循以下步驟：

1. 依預設，ESET Smart Security 中的家長控制為停用。有兩種方式可以啟用家長控制：
   - 從主要程式視窗中，按一下 **[設定]** > **[安全性工具]** > **[家長控制]** 中的  ，並將家長控制狀態變更為已啟用。
   - 按下 F5 以存取 **[進階設定]** 樹狀目錄，瀏覽至 **[Web 和電子郵件]** > **[家長控制]**，接著選取 **[整合至系統]** 旁邊的切換。
2. 按一下主要程式視窗中的 **[設定]** > **[安全性工具]** > **[家長控制]**。即使 **[啟用]** 已顯示於 **[家長控制]** 旁，您仍需按一下 **[保護此帳戶]**，為所需的帳戶建立新的家長控制角色。在帳戶設定視窗中輸入年齡以決定存取層級與適合年齡的建議網頁。現在指定帳戶的家長控制為啟用。按一下帳戶名稱下的 **[允許和禁止的內容...]**，即可在類別索引標籤中自訂您要允許或封鎖的類別。若要允許或封鎖不符合類別的自訂網頁，請按一下 [例外] 索引標籤。

若您從 ESET Smart Security 的主要產品視窗中按一下 **[設定]** > **[安全性工具]** > **[家長控制]**，您將看到主要視窗包含：

Windows 使用者帳戶

如果您已為現有帳戶建立角色，該角色會在此顯示。按一下滑桿  ，便會在帳戶的 [家長控制] 旁顯示綠色核取標記  。按一下作用中帳戶下的 [允許和禁止的內容...]，即可顯示此帳戶允許的網頁類別，以及封鎖和允許的網頁。

重要 若要建立新的帳戶 (例如子女的帳戶)，請使用以下的 Windows 7 或 Windows Vista 逐步說明：

1. 按一下 **[開始]** 按鈕 (位於桌面的左下角)、**[控制台]**，再按一下 **[使用者帳戶]**，開啟 **[使用者帳戶]**。
2. 按一下 **[管理使用者帳戶]**。如果提示您輸入管理員密碼或確認，請輸入密碼或提供資訊。
3. 按一下 **[建立新帳戶]**。
4. 輸入您想要為使用者帳戶命名的名稱，按一下帳戶類型，再按一下 **[建立帳戶]**。
5. 再按一下 ESET Smart Security 主要程式視窗的 **[設定]** > **[安全性工具]** > **[家長控制]**，即可重新開啟 [家長控制] 窗格。

視窗底端部分包含

新增網站例外... - 您可根據您針對每個家長帳戶的偏好設定，個別允許或封鎖特定網站。

顯示防護記錄 - 在此，您可以查看家長控制活動 (封鎖的頁面、頁面已封鎖的帳戶、類別等) 的詳細防護記錄。您也可以按一下  **[過濾]**，根據選擇的條件過濾此防護記錄。

家長控制

在停用家長控制之後，將會顯示 **[停用家長控制]** 視窗。在此您可以設定防護停用的時間間隔。選項接著會變更為 **[暫停]** 或 **[永久停用]**。

請務必使用密碼來保護 ESET Smart Security 中的設定。此密碼可在存取設定區段中進行設定。若未設定密碼，則會顯示下列警告 - **[使用密碼防護家長控制以防止未經授權的變更]** 將會顯示。[家長控制] 中的限制設定只影響標準的使用者帳戶。因為「管理員」可以覆寫所有的限制，所以沒有任何影響。

預設不會過濾 HTTPS (SSL) 通訊。因此，「家長控制」無法封鎖以 *https://* 開頭的網頁。若要啟用此功能，請開啟 **[Web 和電子郵件]** > **[SSL/TLS]** 下 **[進階設定]** 樹狀目錄中的 **[啟用 SSL/TLS 通訊協定過濾]** 設定。

附註： 「家長控制」需要啟用應用程式通訊協定內容過濾，HTTP 通訊協定檢查及個人防火牆才能正常運作。這些功能皆預設為已啟用。

4.4.1.1 類別

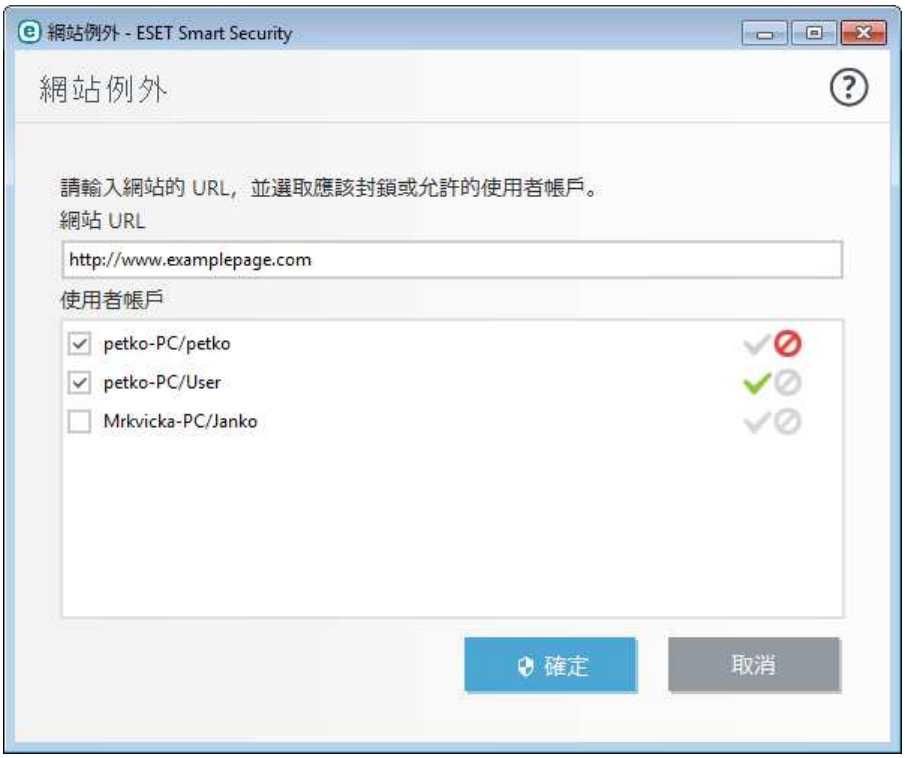
如果選取類別旁邊的核取方塊，則允許此類別。取消選取特定類別旁邊的核取方塊，可封鎖選取帳戶的該類別。

將滑鼠移動於類別上方，就會顯示屬於該類別的網頁清單。以下為使用者可能不熟悉之類別 (群組) 的範例：

- **其他選項** - 通常是私人 (本機) IP 位址，例如內部網路、127.0.0.0/8、192.168.0.0/16 等。若顯示 403 或 404 錯誤碼，則該網站也符合此類別。
- **未解決** - 此類別包含在連線至家長控制資料庫引擎時，因為發生錯誤而未解析的網頁。
- **未分類** - 尚未出現在家長控制資料庫中的不明網頁。
- **[檔案共用]** - 這些網頁包含如相片、影片或點電子書籍等的大量資料。這些網站有包含潛在攻擊性話題或成人內容的風險。

4.4.1.2 網站例外

在清單下的空白欄位中輸入 URL、選取使用者帳戶旁的核取方塊、選取 或 並按一下 **[確定]** 以將其新增至清單。若要從清單中刪除 URL 位址，請按一下 **[設定]** > **[安全性工具]** > **[家長控制]** > **[允許和禁止的內容]**。在所需的使用者帳戶下，按一下 **[例外]** 索引標籤，選取例外並按一下 **[移除]**。



在 URL 位址清單中，無法使用特殊符號 *(星號) 及 ?(問號)。例如，含有多個 TLD 的網址必須手動輸入 (*examplepage.com*? *examplepage.sk* 等)。將網域新增至清單時，將按照您選擇的 URL 處理方法，封鎖或允許此網域及所有子網域 (例如 *sub.examplepage.com*) 中所有的內容。

附註： 封鎖或允許特定網頁會比封鎖或允許網頁類別更加精確。變更這些設定和新增類別/網頁至清單時請小心。

4.5 更新程式

定期更新 ESET Smart Security 是讓電腦確保有最高安全性等級的最佳方法。「更新」模組會透過兩種方式來確保程式永遠為最新，藉由更新病毒資料庫及更新系統元件。

在主要程式視窗中按一下 **[更新]** 可以檢視目前更新狀態，包括最後的成功更新日期與時間，並在需要時更新。主要視窗內也含有病毒資料庫版本。此數字指示是連往 ESET 網站的作用中連結，而網站中會列出指定更新中新增的所有病毒碼。

除了自動更新以外，您也可以按一下 **[立即更新]** 以手動觸發更新。更新病毒資料庫及更新程式元件是維持完整防護、防止惡意代碼的一個重要部分。請注意其配置與作業。您必須使用您的授權金鑰啟動產品，才可接收更新。如果您未在安裝期間這麼做，您可以在更新以存取 ESET 更新伺服器時輸入您的授權金鑰以啟動產品。

附註: 購買 ESET Smart Security 後，ESET 會透過電子郵件提供您授權金鑰。

上一次成功更新 - 上次更新的日期。如果您看到的不是最近的日期，表示病毒資料庫不是最新的狀態。

病毒資料庫版本 - 病毒資料庫號碼，也是連結至 ESET 網站的作用中連結。按一下可檢視在指定更新內新增的所有病毒碼清單。

按一下 **[檢查更新]** 以偵測最新的可用 ESET Smart Security 版本。

更新處理程序

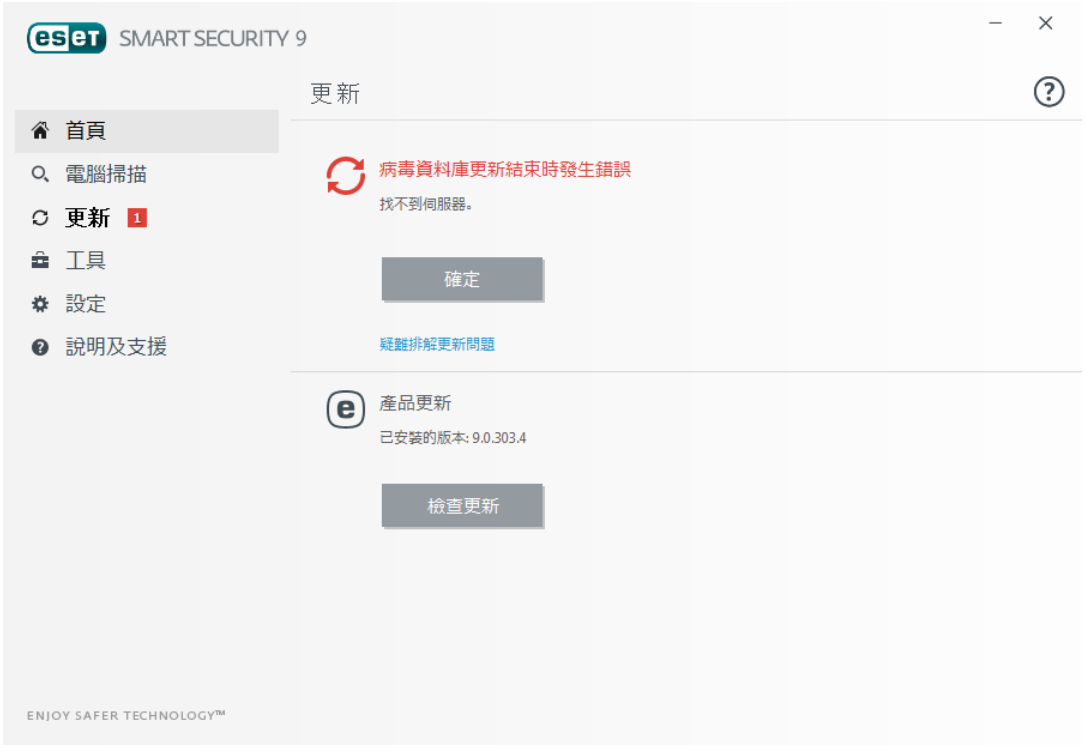
按一下 **[立即更新]** 之後，即會開始下載。畫面上會顯示下載進度列及下載剩餘時間。若要中斷更新，請按一下 **[取消更新]**。

：

重要 在正常情況下，**更新** 視窗中會出現 **[不需要更新 - 病毒資料庫是最新狀態]** 訊息。若非如此，即表示程式過期，因此更容易遭到感染。請儘快更新病毒資料庫。否則，會顯示下列其中一項訊息：

前一個通知與下列關於失敗更新的兩項 **[病毒資料庫更新結束時發生錯誤]** 訊息相關：

1. **無效的授權** - 在更新設定中已錯誤地輸入授權金鑰。建議您檢查驗證資料。[進階設定] 視窗 (從主要功能表按一下 **[設定]**，然後按一下 **[進階設定]**，或按鍵盤上的 F5) 包含其他的更新選項。從主要功能表按一下 **[說明及支援]** > **[變更授權]** 以輸入新的授權金鑰。
2. **下載更新檔案時發生錯誤** - 這可能是因不正確的網際網路連線設定所造成。建議您檢查網際網路連線 (透過在 Web 瀏覽器中開啟任何網站)。如果網站未開啟，可能是尚未建立網際網路連線，或是電腦連線有問題。請與「網際網路服務提供者 (ISP)」確認是否有可使用的網際網路連線。



附註： 如需詳細資訊，請造訪此 ESET 知識庫文章。

4.5.1 更新設定

在 **[更新]**> **[基本]** 下的 **[進階設定]** 樹狀結構 (F5) 中可使用更新設定選項。此區段可指定更新來源資訊，如正在使用的更新伺服器及這些伺服器的驗證資料。

一般

目前使用的更新設定檔顯示於 **[已選取的設定檔]** 下拉式功能表中。若要建立新設定檔，請按一下 **[設定檔清單]** 旁的 **[編輯]**，並輸入您自己的 **[設定檔名稱]**，然後按一下 **[新增]**。

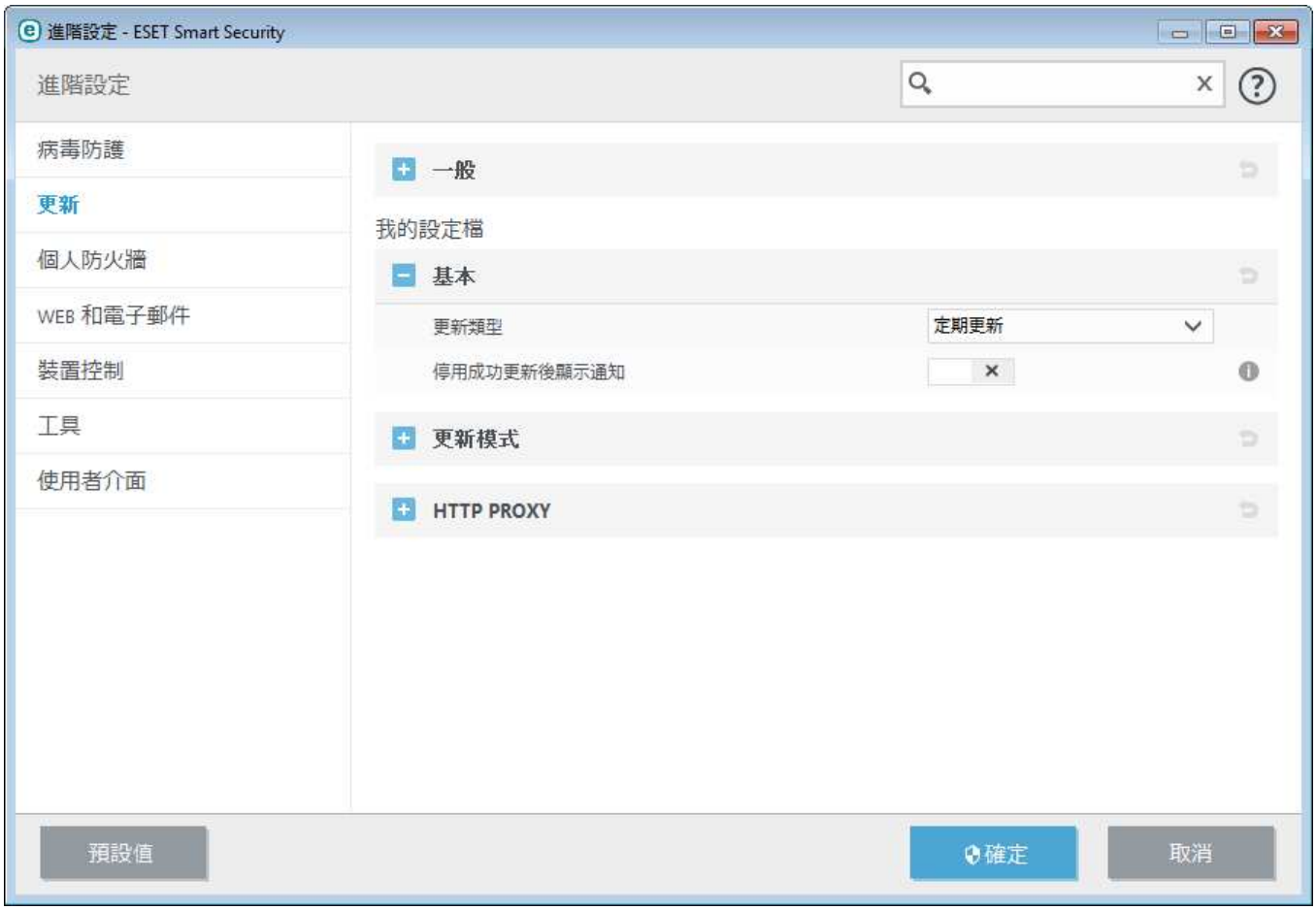
如果您在嘗試下載病毒資料庫更新時遇到困難，請按一下 **[清除]** 以清除暫時更新檔案/快取。

還原

如果您懷疑病毒資料庫和/或程式模組的新更新不穩定或損壞，您可以還原回上一版，並在一段期間內停用任何更新。如果您先前已無限期延後更新，您也可以啟用這些停用的更新。

ESET Smart Security 會記錄病毒資料庫與程式模組的快照，以搭配還原功能使用。若要建立病毒資料庫快照，請讓 **[建立更新檔案快照]** 切換選項保持在啟用狀態。**[儲存於本機的快照數目]** 欄位定義先前儲存的病毒資料庫快照數目。

如果您按一下 **[還原]** (**[進階設定]** (F5) > **[更新]** > **[一般]**)，您必須從 [暫停更新] 下拉式功能表中選取時間間隔，這代表暫停病毒資料庫與程式模組更新的時間。



若要適當地下載更新，必須正確地填入所有更新參數。如果您使用防火牆，請確定您的 ESET 程式可以與網際網路通訊 (即 HTTP 通訊)。

基本

依預設，**[更新類型]** 會設定成 **[定期更新]**，以確保更新檔案會自動從 ESET 伺服器使用最少網路流量下載。發佈前更新 (**[發佈前更新]** 選項) 就是已完成內部測試且即將廣泛提供的更新。啟用發佈前更新，可讓您存取最新的偵測方法與修復程式。不過，發佈前更新有時可能會不穩定，而「不應該」在需要最大可用性與穩定性的生產伺服器與工作站上使用。

停用成功更新後顯示通知 - 關閉畫面右下角的系統匣通知。如果正在執行全螢幕應用程式或遊戲，則選取此選項很有用。請注意，簡報模式將關閉所有通知。

4.5.1.1 更新設定檔

對於各種更新配置及工作，可建立更新設定檔。建立更新設定檔對於行動使用者特別有用，對於會定期變更的網際網路連線內容，行動使用者需要這些內容的替代設定檔。

[選取的設定檔] 下拉式功能表會顯示目前選取的設定檔，預設是設定為 **[我的設定檔]**。若要建立新設定檔，請按一下 **[設定檔...]**，然後按一下 **[新增...]**，並輸入您自己的 **[設定檔名稱]**。建立新設定檔時，您可以從 **[從設定檔複製設定]** 下拉式功能表中選取現有設定檔，以複製其中的設定。

4.5.1.2 進階更新設定

若要檢視進階更新設定，請按一下 **[設定...]**。進階更新設定選項包含 **[更新模式]**? **[HTTP Proxy]** 與 **[LAN]**。

4.5.1.2.1 更新模式

[更新模式] 索引標籤包含程式元件更新相關的選項。新程式元件可以升級時，程式可讓您預先定義其行為。

程式元件更新會提供新功能，或變更舊版已存在的功能。安裝程式元件更新之後，可能需要重新啟動電腦。

應用程式更新 - 啟用之後，將會以無訊息方式自動執行每個程式元件升級，而不完整升級產品。

若 **[下載更新前詢問]** 選項已啟用，有新的更新時將顯示通知。

若更新檔案大小超過 **[詢問更新檔案是否大於 (kB)]** 欄位中指定的值，程式將顯示通知。

4.5.1.2.2 HTTP Proxy

若要存取指定更新設定檔的 Proxy 伺服器設定選項，請按一下 **[進階設定]** 樹狀目錄 (F5) 中的 **[更新]**，然後按一下 **[HTTP Proxy]**。按一下 **[Proxy 模式]** 下拉式功能表，然後選取下列三個選項之一：

- 不使用 Proxy 伺服器
- 經由 Proxy 伺服器連線
- 使用全域 Proxy 伺服器設定

選取 **[使用全域 Proxy 伺服器設定]** 選項，將使用已經在 [進階設定] 樹狀結構的 **[工具]** > **[Proxy 伺服器]** 子目錄中指定的 Proxy 伺服器配置選項。

選取 **[不使用 Proxy 伺服器]** 可明確定義不使用任何 Proxy 伺服器更新 ESET Smart Security。

如果出現下列狀況，務必選取 **[透過 Proxy 伺服器連線]** 選項：

- 應用來更新 ESET Smart Security 的 Proxy 伺服器與全域設定中所指定的 Proxy 伺服器不同 (**[工具]** > **[Proxy 伺服器]**)。若是如此，則應該在其中指定設定：**[Proxy 伺服器]** 位址、通訊**連接埠** (依預設為 3128)，以及 Proxy 伺服器的 **[使用者名稱]** 及 **[密碼]** (如果需要的話)。
- 並未全域設定 Proxy 伺服器，但是 ESET Smart Security 將連接至 Proxy 伺服器進行更新。
- 電腦透過 Proxy 伺服器連接至網際網路。系統在程式安裝期間從 Internet Explorer 取得設定，但如果它們隨後有所變更 (例如您變更 ISP)，請檢查此視窗中所列的 HTTP Proxy 設定是否正確。否則，程式將無法連接至更新伺服器。

Proxy 伺服器的預設值為 **[使用全域 Proxy 伺服器設定]**。

附註： 驗證資料 (例如 **[使用者名稱]** 及 **[密碼]**) 是用來存取 Proxy 伺服器的。只有在需要使用者名稱及密碼時，才填寫這些欄位。請注意這些欄位並不是使用 ESET Smart Security 的使用者名稱/密碼，僅當您瞭解您需要密碼以透過 Proxy 伺服器存取網際網路時才填寫。

4.5.1.2.3 連接到區域網路

從使用 Windows NT 作業系統版本的本機伺服器更新時，預設需要每個網路連線的驗證。

若要配置這類帳戶，請從 **[本機使用者類型]** 下拉式功能表選取：

- **系統帳戶(預設)**?
- **目前使用者**?
- **指定使用者**。

選取 **[系統使用者 (預設)]**，以使用系統帳戶來驗證。通常，如果主要更新設定區段中沒有提供任何驗證資料，則不會發生驗證程序。

若要確保程式授權其自己使用目前登入的使用者帳戶，請選取 **[目前使用者]**。此解決方案的缺點是如果目前沒有任何使用者登入，則程式無法連接至更新伺服器。

如果您想要程式使用特定使用者帳戶來驗證，請選取 **[指定使用者]**。當預設系統帳戶連線失敗時，會使用此方法。請記得指定的使用者帳戶必須具有本機伺服器上更新檔案目錄的存取權。否則，程式將無法建立連線並下載更新。

警告: 選取 **[目前使用者]** 或 **[指定使用者]** 選項時，如果將程式身分變更為所需使用者，則可能會發生錯誤。我們建議將區

域網路 (LAN) 驗證資料輸入主要更新設定區段。在此更新設定區段中，驗證資料輸入應該如下所示：*網域名稱\使用者* (如果是工作群組，請輸入*工作群組名稱\名稱*) 及密碼。當從本機伺服器 HTTP 版本更新時，不需要驗證。

如果即使在已下載更新之後伺服器連線仍處於作用中，請選取 **[更新後中斷伺服器連線]** 來強制中斷連線。

4.5.2 更新還原設定

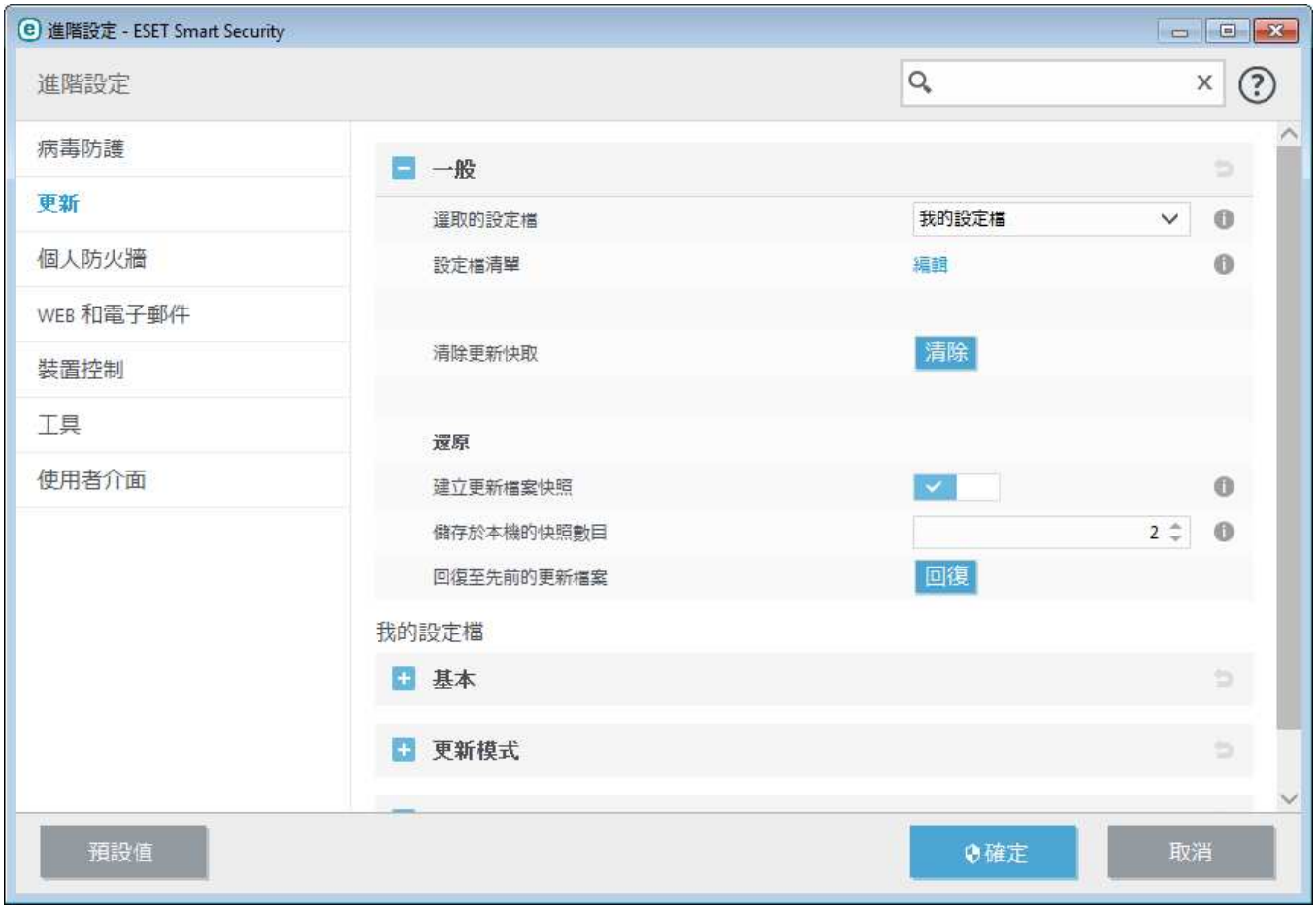
如果您懷疑病毒資料庫和/或程式模組的新更新不穩定或損壞，您可以還原回上一版，並在一段期間內停用任何更新。如果您先前已無限期延後更新，您也可以啟用這些停用的更新。

ESET Smart Security 會記錄病毒資料庫與程式模組的快照，以搭配*還原*功能使用。若要建立病毒資料庫快照，請讓 **[建立更新檔案快照]** 核取方塊保持在勾選狀態。**[儲存於本機的快照數目]** 欄位定義先前儲存的病毒資料庫快照數目。

如果您按一下 **[還原]** (**[進階設定]** (F5) > **[更新]** > **[更新還原設定]**)，您必須從 **[暫停更新]** 下拉式功能表中選取時間間隔，這代表暫停病毒資料庫與程式模組更新的時間。

選取 **[直到取消為止]** 可無限期延後定期更新，直到您手動還原更新功能為止。由於這有潛在性安全風險，因此不建議選取此選項。

如果還原已執行，則 **[還原]** 按鈕會變成 **[允許更新]**。不允許在從 **[暫停更新]** 下拉式功能表中選取的時間間隔內進行更新。病毒資料庫版本會降級到最舊的可用版本，並以快照形式儲存在本機電腦檔案系統中。



範例： 假設編號 6871 是病毒資料庫的最新版本，6870 與 6868 則儲存成病毒資料庫快照。請注意，6869 無法使用，例如，因為電腦已關機，且在 6869 下載前已進行較新的更新。如果您在 **[儲存於本機的快照數目]** 欄位中設為 2，並按一下 **[還原]**，則病毒資料庫 (包含程式模組) 將還原回編號 6868 的版本。此程序可能需要一些時間。從 ESET Smart Security 主要程式視窗的 [更新] 區段中檢查病毒資料庫版本是否已降級。

4.5.3 如何建立更新工作

您可使用下列方式手動觸發更新：按一下主要功能表中的 **[更新]** 之後，在顯示的主要視窗中按一下 **[更新病毒資料庫]**。

更新還可以執行為已排程的工作。若要設定已排程的工作，請按一下 **[工具]** > **[排程器]**。依預設，會在 ESET Smart Security 中啟動下列工作：

- **定期自動更新**
- **撥號連線後自動更新**
- **使用者登入後自動更新**

各個更新工作都可以修改，以滿足您的需求。除了預設更新工作之外，您亦可利用使用者定義的配置來建立新的更新工作。如需建立及配置更新工作的詳細資料，請參閱排程器一節。

4.6 工具

[工具] 功能表包括的模組，可協助簡化程式管理，並為進階使用者提供其他選項。

銀行和付款防護 - ESET Smart Security 可在您使用線上交易或付款網站時保護您的信用卡號和其他機密個人資料。將啟動受保護的瀏覽器以提供更安全的銀行交易。

防盜 - 可在裝置遺失或遭竊時定位並協助您尋找遺失的裝置。

按一下 ESET Smart Security 中的工具 以顯示其他工具以保護您的電腦。

4.6.1 ESET Smart Security 中的工具

該**更多工具**功能表包括的模組，可協助簡化程式管理，並為進階使用者提供其他選項。

此功能表包括下列工具：

防護記錄檔案

防護統計

即時監控

執行中的處理程序 (如果已在 ESET Smart Security 中啟用 ThreatSense)

網路連線 (如果個人防火牆在 ESET Smart Security 中已啟用)

ESET SysInspector

ESET SysRescue Live - 將您重新導向至 ESET SysRescue Live 頁面，您可以在此處下載 Microsoft Windows 作業系統的 ESET SysRescue Live 影像或 Live CD/USB Creator。

排程器

提交樣本以供分析 - 可讓您將可疑檔案提交至 ESET 研究實驗室以供分析。本節會說明按一下此選項之後顯示的對話方塊視窗。

隔離區

附註： 舊版 ESET 安全性產品中的 ESET SysRescue 可能不適用於 Windows 8。在此情況下，我們建議您升級產品或在其他的 Microsoft Windows 版本中建立 ESET SysRescue 磁碟。

4.6.1.1 防護記錄檔案

防護記錄檔案包含所有已發生之重要程式事件的相關資訊，並提供偵測到之威脅的概觀。在系統分析、威脅偵測及疑難排解方面，記錄都是一項很重要的工具。記錄作業會主動在背景中執行，不需使用者介入。系統會依據目前的防護記錄冗贅設定來記錄資訊。您可以直接從 ESET Smart Security 環境檢視文字訊息及防護記錄，以及保存防護記錄。

從主要程式視窗中按一下 **[工具]**，可存取防護記錄檔案。 > **更多工具** > **防護記錄檔案**。從 **[防護記錄]** 下拉式功能表中選取所需的防護記錄類型。以下是可用的防護記錄：

- **偵測到威脅** - 威脅防護記錄提供 ESET Smart Security 所偵測到入侵的詳細資訊。防護記錄資訊包括偵測時間、入侵的名稱、位置，以及在偵測到入侵時，所登入的使用者名稱及其執行的處理方法。按兩下任何防護記錄項目，以在個別視窗中顯示其詳細資訊。
- **事件** - ESET Smart Security 執行的所有重要處理方法都會記錄在事件防護記錄中。事件防護記錄包含程式中已發生事件及錯誤的相關資訊。此選項專供系統管理員及使用者用來解決問題。通常在這裡找到的資訊可協助您找到程式中所發生問題的解決方案。
- **電腦掃描** - 所有已完成的手動或計劃之掃描結果都會顯示在此視窗中。每一行均與單一電腦控制項對應。按兩下任何項目，以檢視各個掃描的詳情。
- **HIPS** - 包含已標記要記錄之特定 HIPS 規則的記錄。通訊協定會顯示觸發作業、結果 (是否允許或禁止規則)，及已建立規則名稱的應用程式。
- **個人防火牆** - 防火牆防護記錄可顯示個人防火牆偵測到的所有遠端攻擊。您可以在這裡找到電腦上任何攻擊的資訊。*[事件]* 直欄會列出已偵測到的攻擊。*[來源]* 直欄會告知您關於攻擊者的相關資訊。*[通訊協定]* 直欄會反映用於攻擊的通訊協定。防火牆防護記錄分析可協助即時偵測到系統入侵的企圖，以防止未經授權的系統存取。
- **已過濾的網站** -如果您想要檢視 Web 存取防護或家長控制所封鎖的網站清單，此功能很實用。 這些防護記錄會顯示建立特定網站連線的時間、URL 位址、使用者與應用程式。
- **垃圾郵件防護** - 包含關於標記為垃圾郵件之電子郵件的相關記錄。
- **家長控制** - 顯示由家長控制所封鎖或允許的網頁。*[比對類型]* 與 *[比對值]* 直欄會告訴您過濾規則的套用方式。
- **裝置控制** - 包含連接到電腦的可移除媒體或裝置記錄。僅含有個別裝置控制規則的裝置將記錄於防護記錄檔案中。如果規則不符合連接的裝置，將不會對連接的裝置建立防護記錄項目。您也可以在這裡看見詳細資訊，例如裝置類型、序號、供應商名稱及媒體大小 (如果有)。

在每個區段中，選取項目並使用鍵盤快捷鍵 **Ctrl + C**，可將顯示的資訊複製到剪貼簿。**Ctrl** 和 **Shift** 鍵可用來選取多個項目。

按一下 **[過濾]** 開啟 **[防護記錄過濾]** 視窗，您可以在其中定義過濾條件。

您可以滑鼠右鍵按一下特定記錄，來顯示內容功能表。內容功能表有以下可用選項：

- **顯示** - 顯示有關在新視窗中所選取防護記錄的詳細資訊。
- **過濾相同的記錄** - 啟動此過濾器之後，您只會看見相同類型的記錄 (診斷、警告...)。
- **過濾.../尋找...** - 按一下此選項之後，會出現 [搜尋防護記錄] 視窗，可讓您定義特定防護記錄項目的過濾條件。
- **啟用過濾** - 啟動過濾設定。
- **停用過濾** - 清除所有過濾器設定值 (如上所述)。
- **複製/全部複製** - 複製視窗中所有記錄的相關資訊。
- **刪除/全部刪除** - 刪除選取的記錄或所有顯示的記錄 - 此動作需要管理員權限才能執行。
- **匯出...** - 以 XML 格式匯出記錄相關資訊。
- **全部匯出...** - 以 XML 格式匯出所有記錄的相關資訊。
- **捲動防護記錄** - 將此選項保持在啟用狀態，以自動捲動舊的防護記錄，並且檢視 **[防護記錄檔案]** 視窗中的作用中防護記錄。

4.6.1.1.1 防護記錄檔案

ESET Smart Security 的防護記錄配置可從主要程式視窗存取。按一下 **[設定]** > **[進入進階設定...]**> **[工具]** > **[防護記錄檔案]**。防護記錄區段用於定義管理防護記錄的方式。程式會自動刪除較舊的防護記錄以節省硬碟空間。您可以指定下列用於防護記錄檔案的選項：

記錄最簡化 - S指定要記錄事件的最小冗贅層級。

- **診斷** - 要微調程式和上述的所有記錄所需的防護記錄資訊。
- **資訊性** - 記錄資訊性訊息，包含成功更新訊息及上述所有記錄。
- **警告** - 記錄嚴重錯誤及警告訊息。
- **錯誤** - 會記錄諸如「*下載檔案時發生錯誤*」類型的錯誤及嚴重錯誤。
- **嚴重** - 僅記錄嚴重錯誤 (啟動病毒防護、個人防火牆等時發生錯誤)。

將自動刪除超過 **[自動刪除超過指定 (天數) 的記錄]** 欄位中指定天數的防護記錄項目。

自動最佳化防護記錄檔案 - 如果勾選，且百分比高於 **[如果未使用的記錄數目超過 (%)]** 欄位所指定的值，則將自動重組防護記錄檔案。

按一下 **[最佳化]**，開始重組防護記錄檔案。在此程序中將移除所有空白的防護記錄項目，以提升效能及防護記錄處理速度。如果防護記錄包含大量的項目，則可明顯察覺此提升效果。

[啟用文字通訊協定] 讓除了使用防護記錄檔案以外，還可用其他檔案格式來儲存防護記錄檔案：

- **[目標目錄]** - 防護記錄檔案所儲存的目錄 (僅適用於 Text/CSV)。每個防護記錄區段皆具備已預先定義檔案名稱的檔案 (例如，若您使用純文字檔案格式以儲存防護記錄，則 *virlog.txt* 適用於防護記錄檔案的 **[偵測到威脅]** 區段)。
- **類型** - 若您選取 **[文字]** 檔案格式，則防護記錄將以文字檔格式儲存，而資料將分隔為索引標籤。相同方法也適用於以逗號分隔的 **[CSV]** 檔案格式。若您選擇 **[事件]**，防護記錄將儲存於 Windows 事件記錄檔 (可使用 [控制台] 中的 [事件檢視器] 進行檢視)，與檔案相反。

刪除所有防護記錄檔案 - 消除所有目前在 **[類型]** 下拉式功能表中所選取的已儲存防護記錄。會顯示成功刪除記錄檔案的通知。

附註: 為了協助您更快速解決問題，ESET 可能會要求您提供電腦中的防護記錄。ESET Log Collector 讓收集所需資訊變得更加容易。如需 ESET Log Collector 的詳細資訊，請造訪 ESET 知識庫文章。

4.6.1.1.2 Microsoft NAP

網路存取保護 (NAP) 是 Microsoft 所開發的技術，可根據主機的系統狀態，控制電腦主機對網路的存取。使用 NAP，組織中電腦網路的系統管理員便能定義系統狀態需求的原則。

網路存取保護 (NAP) 是設計來協助管理員維護網路上電腦的狀態，並依次協助維護網路整體的完整性。這並非設計用來保護網路免於惡意使用者的攻擊。例如， 如果電腦具備所有網路存取規則所需的軟體和配置，則會將電腦視為狀況良好或相容，並將授與對網路的適當存取權限。NAP 不會防止使用相容電腦的已授權使用者上傳惡意程式至網路或採取其他不適當的行為。

NAP 允許管理員建立並強制使用連接到企業網路電腦的狀態規則。此原則會同時管理已安裝的軟體元件和系統配置。連接到網路的電腦，例如：膝上型電腦、工作站和其他類似裝置會根據配置的狀態需求進行評估。

狀態需求包含：

• 防火牆已啟用、
• 防毒程式已安裝、
• 防毒程式是最新狀態、
• [自動 Windows Update] 已啟用等。

4.6.1.2 執行中的處理程序

執行中處理程序會顯示電腦上執行的 程式或處理程序，確保迅速持續地通知 ESET 新入侵的相關資訊。ESET Smart Security 可提供執行中處理程序的詳細資訊，以使用 ThreatSense 技術保護使用者。

處理程序 - 目前在電腦上執行的程式或處理程序的影像名稱。若要查看電腦上的所有處理程序，您也可以使用 Windows 工作管理員。您可以在工具列的空白區按下滑鼠右鍵開啟 [工作管理員]，然後按一下 **[工作管理員]**，或按下鍵盤上的 Ctrl+Shift +Esc 鍵。

風險等級 - 在大部分情況下，ESET Smart Security 和 ThreatSense 技術會使用一系列的啟發式規則 (檢查每個物件的特性，然後衡量惡意活動潛在的可能性) 來指派物件 (檔案、處理程序、登錄機碼等) 的風險等級。根據這些啟發式規則，指派從 1 - 良好 (綠色) 至 9 - 危險 (紅色) 的風險層級給物件。

附註： 標示為良好 (綠色)的已知應用程式絕對是無病毒的 (白名單)，將排除在掃瞄名單之外，如此可以改善電腦上指定電腦掃描或即時檔案系統防護的速度。

使用者數目 - 使用指定應用程式的使用者數目。此資訊是由 ThreatSense 技術收集。

發現時間 - 應用程式由 ThreatSense 技術發現以來的時間。

附註： 應用程式被標示為不明 (橙色) 安全等級時，不一定確定是惡意軟體。它通常只是新的應用程式。若您對檔案不確定，可以提交檔案以供分析至 ESET 的研究實驗室。若經證實，檔案為惡意的應用程式，則其偵測會新增到其中一個近期的更新。

應用程式名稱 - 程式或處理程序的指定名稱。

在新視窗中開啟 - 在開啟的新視窗中顯示執行中處理程序的資訊。

經由按一下最下方的指定應用程式，視窗底部會出現以下資訊：

- **檔案** - 電腦上應用程式的位置。
- **檔案大小** - 單位為 B (位元組) 的檔案大小。
- **檔案說明** - 根據作業系統說明的檔案特性。
- **公司名稱** - 供應商或應用程式處理程序的名稱。
- **檔案版本** - 來自應用程式發行者的資訊。
- **產品名稱** - 應用程式名稱和/或商業名稱。

附註： 聲譽也可在不作為執行中程式/處理程序的檔案上檢查 - 標記您要檢查的檔案，並以滑鼠右鍵按一下這些檔案，然後選取 **[進階選項]** > **[使用 ThreatSense 檢查檔案聲譽]**。

4.6.1.3 防護統計

若要檢視與 ESET Smart Security 防護模組相關的統計資料圖表，請按一下 **[工具]** > **[防護統計]**。從 **[統計]** 下拉式功能表中選取想要的防護模組，以查看對應的圖表及圖例。如果將滑鼠游標置於圖例中的項目上，則在圖表中只會顯示該項目的資料。

下列為可用的統計圖表：

- **病毒及間諜程式防護** - 顯示受感染及已清除的物件數目。
- **[檔案系統防護]** - 只顯示已讀取或寫入檔案系統的物件。
- **電子郵件用戶端防護** - 只顯示電子郵件用戶端傳送或接收的物件。
- **[Web 存取及網路釣魚防護]** - 只顯示 Web 瀏覽器下載的物件。
- **電子郵件用戶端垃圾郵件防護** - 顯示自上一次啟動以來，垃圾郵件防護統計資料的歷程。

在統計圖表下方，您可以看見已掃描物件的總數、最近掃描的物件，以及統計資料時間郵戳。按一下 **[重設]** 以清除所有的統計資訊。

4.6.1.4 即時監控

若要以圖形格式查看目前的 **[檔案系統活動]**，請按一下 **[工具]** > **更多工具** > **監控活動**。在圖形的底端，是根據選取之時間範圍即時記錄「檔案系統活動」的時間表。若要變更時間範圍，請從 **[重新整理率]** 下拉式功能表中選取。

可用選項如下：

- **跳過：1 秒** - 圖表每秒鐘都會重新整理，且時間表包含最近 10 分鐘。
- **跳過：1 分鐘 (最近 24 小時)** - 圖表每分鐘都會重新整理，且時間表包含最近 24 小時。
- **跳過：1 小時 (最近一個月)** - 圖表每小時都會重新整理，且時間表包含最近一個月。
- **跳過：1 小時 (選取的月份)** - 圖表每小時都會重新整理，且時間表包含選取的最近 X 個月。

[檔案系統活動圖形] 中的縱軸表示已讀取資料量 (藍色) 及已寫入資料量 (紅色)。兩個值都以 KB/MB/GB 為單位。如果將滑鼠游標置於圖表下方圖例中已讀取資料或已寫入資料上，則圖表將只會顯示該活動類型的資料。

從 **[活動]** 下拉式功能表中，您也可以選取 **[網路活動]**。**[檔案系統活動]** 及 **[網路活動]** 的圖表顯示及選項相同，但是後者顯示已接收資料量 (紅色) 及已傳送資料量 (藍色)。

4.6.1.5 網路連線

在 [網路連線] 區段中，您可以看到作用中及擱置連線的清單。這可協助您控制建立對外連線的所有應用程式。

第一行顯示應用程式的名稱及資料傳送速度。若要查看由應用程式建立之連線的清單 (及其他詳細資訊)，請按一下 **[+]**。

直欄

應用程式/本機 IP - 應用程式名稱、本機 IP 位址及通訊連接埠。

遠端 IP - 特定遠端電腦的 IP 位址及連接埠號碼。

通訊協定 - 使用的傳送通訊協定。

上傳速度/下載速度 - 對外與對內資料的目前速度。

已傳送/已接收 - 連線內交換的資料數量。

顯示詳情 - 選擇此選項以顯示所選取連線的詳細資訊。

網路連線畫面中的 **[配置連線視圖...]** 選項可讓您進入此區段的進階設定結構，讓您修改連線視圖選項：

解析主機名稱 - 可能的話，所有網路位址都會以 DNS 格式顯示，而非數字 IP 位址格式。

僅顯示 TCP 連線 - 清單僅顯示屬於 TCP 通訊協定組合的連線。

顯示等待中的連線 - 選取此選項以僅顯示目前尚未建立任何通訊，但系統已開啟連接埠且正在等待連線的連線。

顯示電腦內部的連線 - 選取此選項以僅顯示遠端為本機系統的連線 (即 *localhost* 連線)。

以滑鼠右鍵按一下連線可查看其他選項，包括：

拒絕連線的通訊 - 終止已建立的通訊。只有在按一下作用中連線之後，才能使用此選項。

重新整理速度 - 選擇重新整理作用中連線的頻率。

立即重新整理 - 重新載入 [網路連線] 視窗。

只有在按一下應用程式或處理程式，而非作用中連線之後，才能使用下列這兩種選項：

暫時拒絕處理程序的通訊 - 拒絕指定應用程式的目前連線。如果已建立新連線，則防火牆會使用預先定義的規則。您可以在配置及使用規則一節中找到設定的說明。

暫時允許處理程序的通訊 - 允許指定應用程式的目前連線。如果已建立新連線，則防火牆會使用預先定義的規則。您可以在配置及使用規則一節中找到設定的說明。

4.6.1.6 ESET SysInspector

ESET SysInspector 是全面檢查電腦、收集系統元件 (例如驅動程式和應用程式、網路連線，或重要的登錄項目) 的詳細資訊並評估各個元件風險層級的應用程式。此資訊可協助判定可疑系統行為是肇因於軟體或硬體不相符，還是惡意軟體感染。

SysInspector 視窗會顯示建立的防護記錄相關的下列資訊：

- **時間** - 防護記錄建立的時間。
- **註解** - 簡短註解。
- **使用者** - 建立防護記錄的使用者名稱。
- **狀態** - 防護記錄建立的狀態。

以下是可用的處理方法：

- **開啟**- 開啟已建立的防護記錄。您也可以在指定的防護記錄檔案上按一下右鍵，並從內容功能表選取 **[顯示]**。
- **比較** - 比較兩份現有防護記錄。
- **建立...** - 建立新的防護記錄。請等候直到 ESET SysInspector 完成 (防護記錄狀態會顯示為 [已建立])，再嘗試存取防護記錄。
- **刪除** - 從清單移除選取的防護記錄。

選取一個或多個防護記錄後，內容功能表中即有以下項目可供使用：

- **顯示** - 在 ESET SysInspector 中開啟所選取的防護記錄 (與按兩下防護記錄的功能相同)。
- **比較** - 比較兩份現有防護記錄。
- **建立...** - 建立新的防護記錄。請等候直到 ESET SysInspector 完成 (防護記錄狀態會顯示為 [已建立])，再嘗試存取防護記錄。
- **全部刪除** - 刪除所有防護記錄。
- **匯出...** - 將防護記錄匯出至 *.xml* 檔或壓縮的 *.xml*。

4.6.1.7 排程器

排程器使用預先定義的配置與屬性管理及啟動已排程的工作。

按一下 **[工具]** > **[排程器]**，即可從 ESET Smart Security 主要程式視窗存取「排程器」。**[排程器]** 包含已排程的工作與其配置內容 (如預先定義的日期、時間及使用的掃描設定檔) 的清單。

[排程器] 可用來排程下列工作：病毒資料庫更新、掃描工作、系統啟動檔案檢查及防護記錄維護。您可以直接在主 [排程器] 視窗中新增或刪除工作 (按一下底端的**[新增...]** 或 **[刪除]**)。在 [排程器] 視窗中的任何位置按一下滑鼠右鍵，以執行下列處理方法：顯示詳細資訊、立即執行工作、新增工作及刪除現有工作。使用每個項目前端的核取方塊來啟動/停用工作。

依預設，下列排定工作會顯示在 **[排程器]** 中：

- **防護記錄維護**
- **定期自動更新**
- **撥號連線後自動更新**
- **使用者登入後自動更新**
- **定期檢查最新產品版本** (參閱更新模式)
- **自動啟動檔案檢查** (使用者登入後)
- **啟動檔案自動檢查** (成功更新病毒資料庫後)
- **自動先掃描**

若要編輯 (預設及使用者定義的) 現有排定工作的配置，請在工作上按一下滑鼠右鍵並按一下 **[編輯...]**，或選取要修改的工作，再按一下 **[編輯...]**。

新增工作

1. 按一下視窗底部的 **[新增工作]**。

2. 輸入工作的名稱。

3. 自下拉式功能表選取想要的工作：

- **執行外部應用程式** - 排程以執行外部應用程式。
- **防護記錄維護** - 防護記錄檔案還包括已刪除記錄的剩餘部分。此工作會定期最佳化防護記錄檔案中的記錄，以有效運作。
- **系統啟動檔案檢查** - 檢查系統啟動或登入時允許執行的檔案。
- **建立電腦掃描** - 建立 ESET SysInspector 電腦快照 - 收集關於系統元件 (例如驅動程式、應用程式) 的詳細資訊，並評估各個元件的風險層級。
- **指定電腦掃描** - 針對電腦中的檔案及資料夾執行掃描。
- **先掃描** - 依預設，在安裝後 20 分鐘或電腦重新開機時，將以低優先順序工作級別執行電腦掃描。
- **更新** - 更新病毒資料庫與程式模組來排程更新工作。

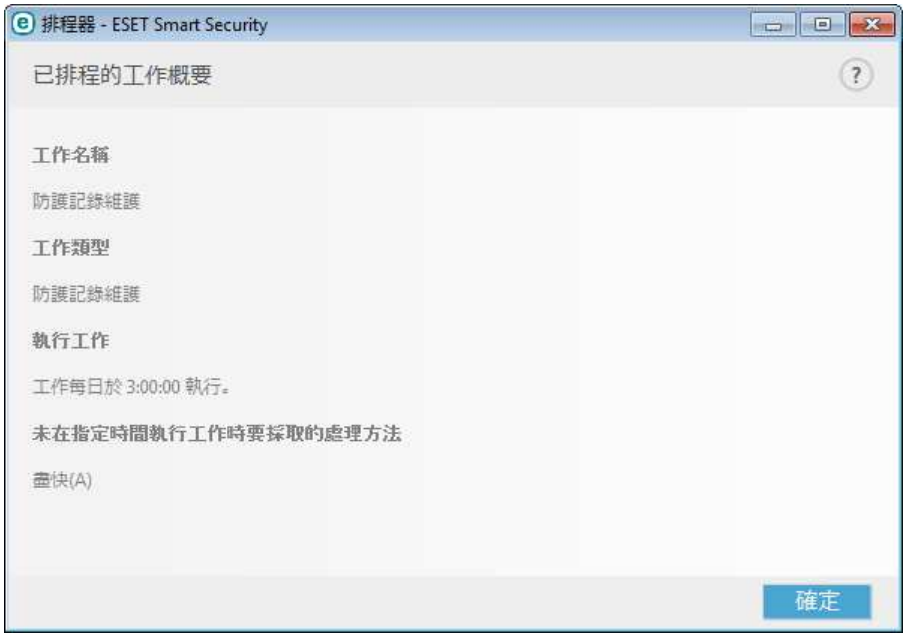
4. 若您要啟用工作，則請開啟 **[已啟用]** 選項 (您可以稍後在已排程工作清單中選取/取消選取核取方塊以完成開啟)，接著按一下 **[下一步]**，並選取其中一個時間選項：

- **一次** - 工作將在預先定義的日期及時間執行。
- **重複** - 工作將在指定的時間間隔內執行。
- **每日** - 工作會重複每天在指定的時間執行。
- **每星期** - 工作將在選取的日期及時間執行。
- **事件觸發** - 工作會在指定的事件發生時執行。

5. 選取 **[使用電池執行時略過工作]** 以在膝上型電腦使用電池執行時，將系統資源消耗降到最低。工作會在 **[工作執行]** 欄位中的指定日期和時間執行。如果工作無法在預先定義的時間執行，您可以指定工作的再次執行時間：

- **於下次排程的時間**
- **盡快(A)**
- **如果距離上次執行的時間超過指定值，則立即執行工作** (可以使用 **[自上次執行後經過的時間]** 捲動方塊定義間隔)

您可以按一下滑鼠右鍵並按一下 **[顯示工作詳情]** 以檢閱已排程的工作。



4.6.1.8 ESET SysRescue

ESET SysRescue 是一套公用程式，可讓您建立包含 ESET Security 解決方案其中之一的開機磁碟 - 可能是 ESET NOD32 Antivirus、ESET Smart Security 或某些伺服器導向的產品。ESET SysRescue 的主要優點是 ESET Security 解決方案獨立於主機作業系統之外執行，且同時可以直接存取磁碟及檔案系統。因此它能夠移除一般無法刪除的入侵，例如在作業系統執行時，進行刪除動作等。

4.6.1.9 ESET LiveGrid®

ESET LiveGrid® (以先進的 ESET ThreatSense.Net 進階預早警告系統為基礎) 會應用全球各地 ESET 使用者提交、並傳送到 ESET 研究實驗室的資料。透過全球提供可疑樣本和中繼資料的方式，ESET LiveGrid® 可讓我們立即回應客戶需求，並讓 ESET 隨時掌握最新威脅情報。請在字彙中閱讀更多有關 ESET LiveGrid® 的資訊。

使用者可直接從程式的介面或關聯式功能表，查看執行中的處理程序與檔案的聲譽，以及可從 ESET LiveGrid® 取得的其他資訊。有兩個選項：

1. 您可以選擇不啟用 ESET LiveGrid®。您不會失去軟體的任何功能，但在有些情況下，當 ESET Live Grid 啟用時，ESET Smart Security 可能會比病毒資料庫更新更快回應新威脅。
2. 您可以配置 ESET LiveGrid®，以提交新威脅與包含新威脅代碼位置的匿名資訊。此檔案可傳送至 ESET，以供詳細分析。研究這些威脅會協助 ESET 更新其威脅偵測能力。

ESET LiveGrid® 會收集與新偵測到之威脅相關的電腦資訊。此資訊可能包括出現威脅的檔案範例或副本、檔案路徑、檔案名稱、日期與時間、威脅出現在電腦上程序，以及電腦作業系統的相關資訊。

依預設，ESET Smart Security 配置為將可疑檔案提交至 ESET 病毒實驗室以供詳細分析。例如 *.doc* 或 *.xls* 等某些副檔名的檔案一律排除。如果有您或您的組織要避免傳送的特殊檔案，您也可以新增其他副檔名。

ESET LiveGrid® 設定功能表提供數個用於啟用/停用 ESET LiveGrid® 的選項，可將可疑檔案及匿名統計資訊提交至 ESET 實驗室。按一下 **[工具]** > **[ESET LiveGrid®]**，即可從 [進階設定] 樹狀目錄中存取該設定。

啟用 ESET LiveGrid® 聲譽系統 (建議) - ESET LiveGrid® 聲譽系統可將掃描的檔案與雲端中的白名單和黑名單項目比較，以改善 ESET 惡意軟體防護解決方案的效益。

提交匿名統計 - 允許 ESET 收集新偵測到威脅的相關資訊，例如威脅名稱、偵測的日期與時間、偵測方法與關聯的中繼資料、產品版本與配置 (包括您系統的相關資訊)。

提交檔案 - 類似威脅的檔案，和/或有異常特性或行為的檔案，可提交至 ESET 進行分析。

選取 **[啟用記錄]** 可建立事件防護記錄，以記錄檔案及統計資訊提交。當傳送檔案或統計資訊時，此選項允許記錄在事件防護記錄中。

連絡人電子郵件 (選用) - 傳送任何可疑的檔案時會連同您的連絡人電子郵件一併傳送。在分析時若需要您提供進一步的資訊，便可利用這個電子郵件連絡您。請注意，除非需要更多資訊，否則您將不會收到 ESET 的任何回應。

[排除] - 排除過濾可讓您排除某些不提交的檔案/資料夾 (例如，您可使用此選項，排除可能包含機密資訊的檔案，例如文件或試算表)。絕對不會將列出的檔案傳送至 ESET 實驗室以供分析，即使其包含可疑代碼。依預設，最常見的檔案類型 (.doc 等) 均會被排除在外。如果需要，您可以新增到排除檔案清單中。

如果您使用過 ESET LiveGrid® 但現已停用，則可能還有待傳送的資料套件。即使已停用，此類套件仍會傳送到 ESET。一旦已傳送所有目前資訊，便不會繼續建立套件。

4.6.1.9.1 可疑檔案

ESET LiveGrid® 進階設定的 **[檔案]** 索引標籤可讓您配置將威脅提交至 ESET 研究實驗室進行分析的方法。

如果您找到可疑檔案，您可以提交給我們的 ESET 研究實驗室以供分析。若檔案為惡意的應用程式，則其偵測會新增到下一個病毒資料庫更新。

排除過濾 - [排除過濾] 可讓您排除某些不提交的檔案/資料夾。我們絕對不會將列出的檔案傳送至 ESET 研究實驗室以供分析，即使其包含可疑代碼。例如，您可使用此選項，排除可能包含機密資訊的檔案，例如文件或試算表。依預設，最常見的檔案類型 (.doc 等) 均會被排除在外。如果需要，您可以新增到排除檔案清單中。

連絡人電子郵件 (選用) - 傳送任何可疑的檔案時會連同您的連絡人電子郵件一併傳送。在分析時若需要您提供進一步的資訊，便可利用這個電子郵件連絡您。請注意，除非需要更多資訊，否則您將不會收到 ESET 的任何回應。

選取 **[啟用記錄]** 可建立事件防護記錄，以記錄檔案及統計資訊提交。當傳送檔案或統計資訊時，此選項允許記錄在事件防護記錄中。

4.6.1.10 隔離區

隔離區的主要功能是安全地儲存受感染檔案。對於無法清除、無法安全刪除或不建議刪除的檔案，或者 ESET Smart Security 錯誤偵測到的檔案，應該予以隔離。

您可以選擇隔離任何檔案。如果檔案行為可疑，但防毒掃描器沒有偵測到，則建議進行隔離。您可將隔離的檔案提交至 ESET 研究實驗室進行分析。

您可以在表格中檢視隔離資料夾中儲存的檔案，其中顯示隔離的日期與事件、受感染檔案原始位置的路徑、大小 (以位元組為單位)、原因 (例如，由使用者新增...)，以及威脅數量 (例如，包含多個入侵的壓縮檔)。

隔離檔案

ESET Smart Security 會自動隔離刪除的檔案 (如果您尚未在警告視窗中取消此選項)。如果需要，您可以按一下 **[隔離...]**，手動隔離任何可疑檔案。如果是這種情況的，不會從原始位置移除原始檔案。內容功能表也可用於此目的 - 以滑鼠右鍵按一下 **[隔離區]** 視窗，並選取 **[隔離...]**。

從隔離區還原

隔離的檔案還可還原至其原始位置。使用 **[還原]** 功能可達到此目的，此功能可從內容功能表取得，方法是以滑鼠右鍵按一下 [隔離區] 視窗中的特定檔案。如果檔案標記為 [潛在不需要應用程式]，則 **[還原並從掃描中排除]** 選項已啟用。請在字彙中閱讀更多有關此類型應用程式的資訊。內容功能表還提供 **[還原到...]** 選項，可讓您將檔案還原到其原始刪除位置外的其他位置。

附註: 如果程式不小心隔離了無惡意檔案，請在還原後從掃描中排除檔案，並將該檔案傳送至 ESET 客戶服務。

從隔離區提交檔案

如果您已隔離程式未偵測到的可疑檔案，或錯誤地將檔案判定為受感染 (例如以代碼的啟發式分析) 且因此隔離，請將檔案傳送至 ESET 病毒實驗室。若要從隔離提交檔案，請在檔案上按一下滑鼠右鍵，並從內容功能表選取 **[提交檔案以供分析]**。

4.6.1.11 Proxy 伺服器

在大型 LAN 網路中，Proxy 伺服器可用來調節電腦與網際網路的通訊。使用此配置則需要定義下列設定。否則，程式將無法自動進行更新。在 ESET Smart Security 中，Proxy 伺服器設定位於 [進階設定] 樹狀目錄的兩個不同區段中。

首先，Proxy 伺服器設定可在 **[工具]** > **[Proxy伺服器]** 下的 **[進階設定]** 中配置。在這個等級指定 Proxy 伺服器，會定義所有 ESET Smart Security 的全域 Proxy 伺服器設定。需連線到網際網路的所有模組，都會使用這裡的參數。

若要指定此層級的 Proxy 伺服器設定，請選取 **[使用 Proxy 伺服器]**，然後將 Proxy 伺服器的位址和 **[連接埠]** 號碼輸入 **[Proxy 伺服器]** 欄位中。

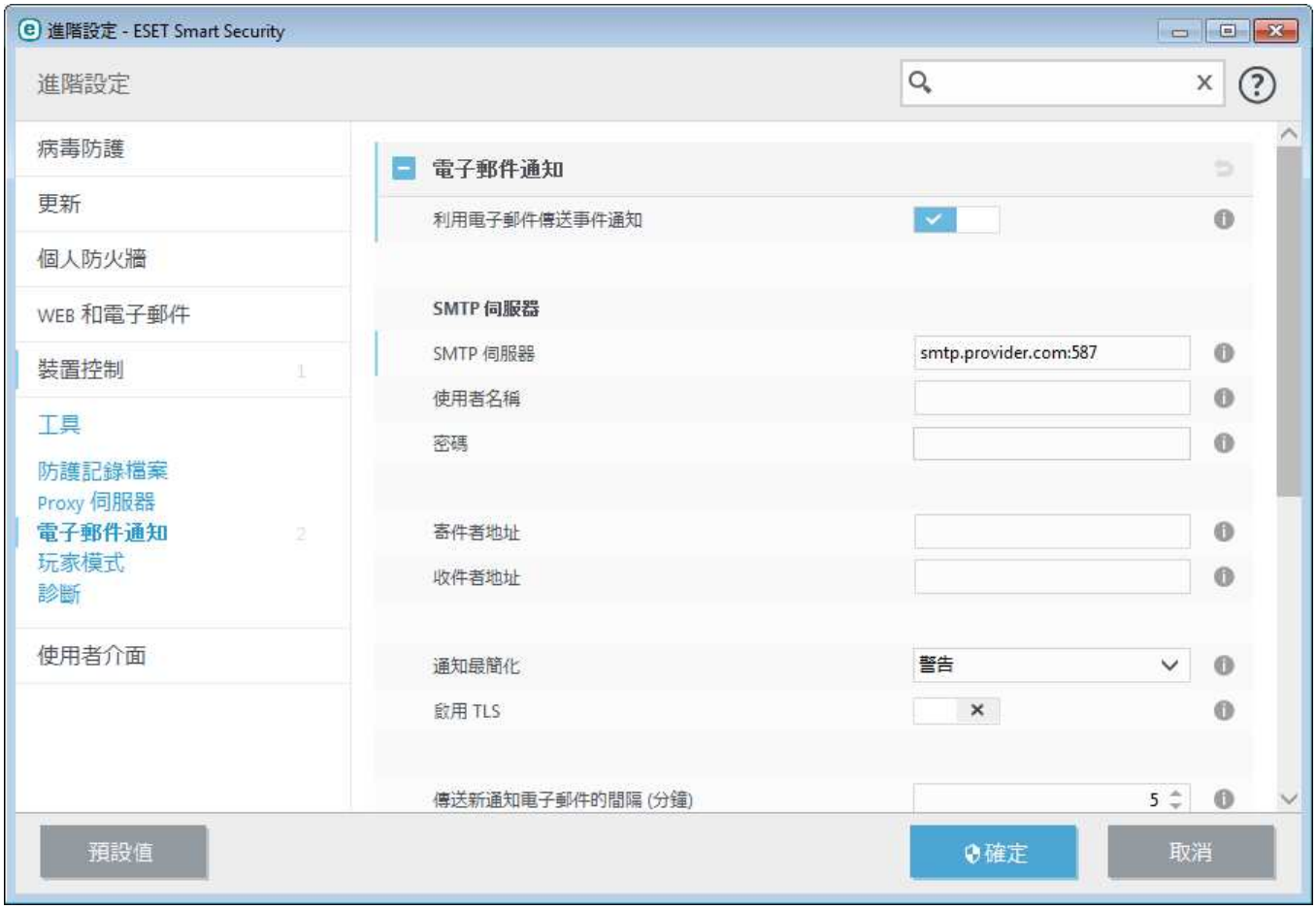
如果與 Proxy 伺服器之間的通訊需要驗證，請選取 **[Proxy 伺服器需要驗證]**，並將有效的 **[使用者名稱]** 及 **[密碼]** 輸入各自的欄位中。按一下 **[偵測]**，以自動偵測和填入 Proxy 伺服器設定。將複製 Internet Explorer 中指定的參數。

附註： 您必須在 **[Proxy 伺服器]** 設定中手動輸入使用者名稱和密碼。

Proxy 伺服器設定也可以在 [進階] 更新設定中建立 (從 **[Proxy 模式]** 下拉式功能表選取 **[透過 Proxy 伺服器連線]** 中的 **[進階設定]** > **[更新]** > **[HTTP Proxy]**)。此設定適用於指定更新設定檔且建議用於筆記型電腦；筆記型電腦通常會從遠端位置接收病毒碼更新。如需此設定的詳細資訊，請參閱進階更新設定。

4.6.1.12 電子郵件通知

如果發生與所選簡化層級相關的事件，則 ESET Smart Security 可以自動傳送電子郵件通知。啟用 **[利用電子郵件傳送事件通知]** 以啟動電子郵件通知。



SMTP 伺服器

SMTP 伺服器 - 用於傳送通知的 SMTP 伺服器 (例如 *smtp.provider.com:587*，預先定義的連接埠為 25)。

附註： ESET Smart Security 支援具備 TLS 加密功能的 SMTP 伺服器。

使用者名稱及密碼 - 如果 SMTP 伺服器需要驗證，則應該在這些欄位中填寫有效的使用者名稱及密碼，以存取 SMTP 伺服器。

寄件者地址 - 此欄位指定將在通知電子郵件檔頭顯示的寄件者地址。

收件者地址 - 此欄位指定將在通知電子郵件檔頭顯示的收件者地址。

從 **[通知最簡化]** 下拉式功能表中，您可以選取將傳送通知的起始嚴重性層級。

- **診斷** - 要微調程式和上述的所有記錄所需的防護記錄資訊。
- **資訊** - 記錄例如非標準網路事件的資訊性訊息，包含成功更新訊息及上述所有記錄。
- **警告** - 記錄嚴重錯誤及警告訊息 (反隱藏技術未正確執行或更新失敗)。
- **錯誤** - 會記錄錯誤 (例如文件防護未啟用) 及嚴重錯誤。
- **嚴重** - 僅記錄嚴重錯誤，例如啟動病毒防護或除受感染的系統。

啟用 TLS - 啟用 TLS 加密支援的傳送警告及通知訊息。

傳送新通知電子郵件的間隔 (分鐘) - 以電子郵件傳送新通知的間隔 (分鐘)。如果您將該值設為 0，則會立即傳送通知。

以不同的電子郵件傳送每個通知 - 啟用後，收件者會收到各個通知的新電子郵件。這可能會造成短時間內收到大量的電子郵件。

訊息格式

事件訊息格式 - 在遠端電腦顯示的事件訊息格式。

威脅警告訊息格式 - 威脅警告及通知訊息具有預先定義的預設格式。我們建議您不要變更此格式。然而，在某些情況下 (例如，如果您具有自動電子郵件處理系統)，您可能需要變更訊息格式。

使用本機字母字元 - 以 Windows Regional 設定的編碼將電子郵件訊息轉換為 ANSI 字元 (例如，windows-1250)。如果您將此選項保持為空白，則訊息會以 ACSII 7 位元轉換並編碼 (例如 "á" 會變更為 "a"，未知符號會變更為 "?")。

使用本機字元編碼 - 電子郵件訊息來源會編碼為 Quoted-printable (QP) 格式，此格式會使用 ASCII 字元，並正確透過電子郵件以 8 位元格式 (áéíóú) 傳輸特殊國家字元。

4.6.1.12.1 訊息格式

在此您可以設定在遠端電腦上顯示的事件訊息格式。

威脅警告及通知訊息具有預先定義的預設格式。我們建議您不要變更此格式。然而，在某些情況下 (例如，如果您具有自動電子郵件處理系統)，您可能需要變更訊息格式。

訊息中的關鍵字 (以 % 符號分隔的字串) 會由特定的實際資訊取代。可用關鍵字如下所示：

- **%TimeStamp%** - 事件的日期及時間
- **%Scanner%** - 模組的相關資訊
- **%ComputerName%** - 發生警告的電腦名稱
- **%ProgramName%** - 產生警告的程式
- **%InfectedObject%** - 受感染的檔案、郵件等的名稱
- **%VirusName%** - 感染的識別碼
- **%ErrorDescription%** - 非病毒事件的說明

%InfectedObject% 及 **%VirusName%** 關鍵字僅用於威脅警告訊息，而 **%ErrorDescription%** 僅用於事件訊息。

使用本機字母字元 - 根據 Windows 地區設定將電子郵件訊息轉換為 ANSI 字元編碼 (e.g. windows-1250)。如果您將此選項保持為空白，則訊息會以 ACSII 7 位元轉換並編碼 (例如 "á" 會變更為 "a"，未知符號會變更為 "?")。

使用本機字元編碼 - 電子郵件訊息來源會編碼為 Quoted-printable (QP) 格式，此格式會使用 ASCII 字元，並正確透過電子郵件以 8 位元格式 (áéíóú) 傳輸特殊國家字元。

4.6.1.13 選取樣本以供分析

[檔案提交] 對話方塊可讓您將檔案或網站傳送給 ESET 以供分析，而這個對話方塊可在 **[工具]** 中找到。 > **更多工具** > **提交樣本以供分析**。如果您在電腦中發現行跡可疑的檔案，或在網際網路中發現可疑的網站，您可以將其提交至 ESET 研究實驗室以供分析。如果檔案證實為惡意的應用程式或網站，則其偵測會新增到近期的更新中。

您也可以透過電子郵件來提交檔案。若您偏好此選項，請使用 WinRAR/ZIP 壓縮檔案，使用密碼「infected」來保護壓縮檔，然後將其傳送至 samples@eset.com。請記得使用敘述性的主旨，並盡可能涵蓋檔案的相關資訊 (例如下載的網站)。

附註：在將檔案提交至 ESET 之前，請確定其符合下列一或多個條件：
- 完全未偵測該檔案
- 錯將該檔案偵測為威脅

除非需要進一步的資訊以供分析，否則您將不會收到任何回應。

從 **[提交檔案的原因]** 下拉式功能表中選取最符合您訊息的說明：
- **可疑檔案**
- **可疑網站** (受到惡意軟體感染的網站)?
- **誤判檔案** (偵測為感染但實際上未受感染的檔案)、
- **誤判網站**
- **其他**

檔案/網站 - 要提交的檔案或網站路徑。

連絡人電子郵件 - 這個連絡人電子郵件會與可疑檔案一併傳送到 ESET，並可用於在需要進一步資訊以供分析時連絡您。輸入連絡人電子郵件是選用選項。由於我們的伺服器每天都會接收到成千上萬個檔案，所以除非需要更多資訊，否則我們不可能一一回覆，因此您將不會收到 ESET 的回應。

4.6.1.14 Microsoft Windows® 更新

Windows Update 功能是保護使用者遠離惡意軟體的重要元件。因此，當有可用的 Microsoft Windows 更新時，立即安裝更新是很重要的。ESET Smart Security 會根據指定的層級通知您遺漏的更新。以下是可用的層級：

- **無更新** - 不提供系統更新下載。
- **選用更新** - 提供下載標記為低與更高優先順序的更新。
- **建議更新** - 提供下載標記為一般與更高優先順序的更新。
- **重要更新** - 提供下載標記為重要與更高優先順序的更新。
- **重大更新** - 只提供重大更新下載。

按一下 **[確定]** 儲存變更。在與更新伺服器進行狀態驗證之後，會顯示 [系統更新] 視窗。因此，在儲存變更之後，可能不會立即出現系統更新資訊。

4.7 使用者介面

[使用者介面] 區段可讓您配置程式圖形使用者介面 (GUI) 的行為。

使用 [圖形] 工具就可以調整程式的視覺外觀與使用的特效。

配置警告及通知就可以變更已偵測到的威脅警告及系統通知的行為。這些全都可以自訂，以符合您的需求。

如果您選擇不顯示某些通知，則這些通知就會顯示於隱藏通知視窗區域中。您可以在此檢查其狀態、顯示更多詳情，或是從這個視窗中加以移除。

若要讓安全軟體的安全性達到極致，您可以使用存取設定工具。

以滑鼠右鍵按一下物件之後，會顯示內容功能表。使用此工具以將 ESET Smart Security 控制項元素整合至內容功能表。

4.7.1 使用者介面元素

ESET Smart Security 中的使用者介面配置選項可讓您調整工作環境以符合您的需要。在 ESET Smart Security [進階設定] 樹狀目錄的 **[使用者介面]** > **[使用者介面元素]** 子目錄中可存取這些配置選項。

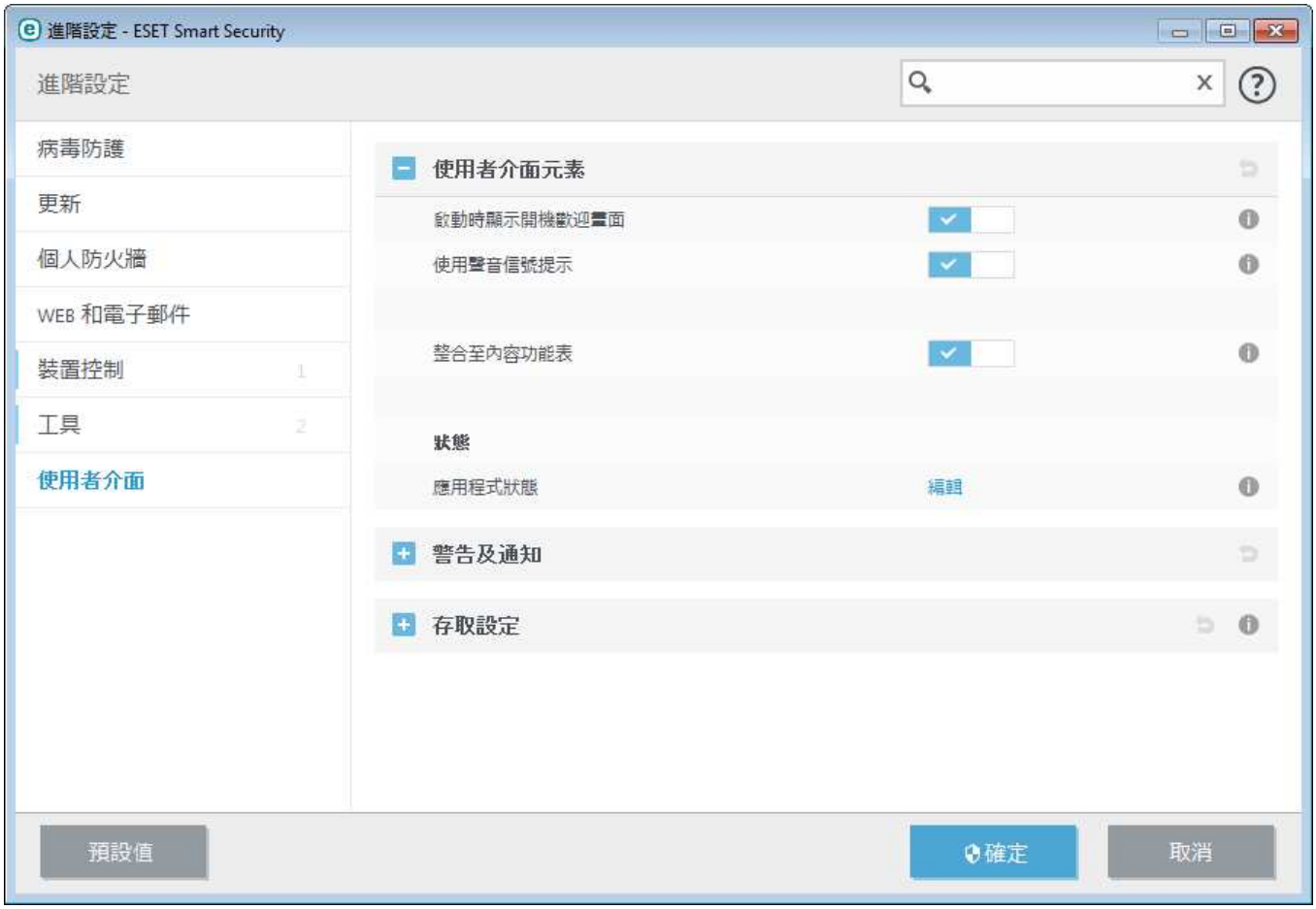
如果您要停用 ESET Smart Security 開機歡迎畫面，請取消選取 **[啟動時顯示開機歡迎畫面]**。

若要 ESET Smart Security 在掃描期間發生重大事件 (例如當發現威脅或掃描結束) 時播放音效，請選取 **[使用聲音信號提示]**。

整合至內容功能表 - 將 ESET Smart Security 控制項元素整合至內容功能表。

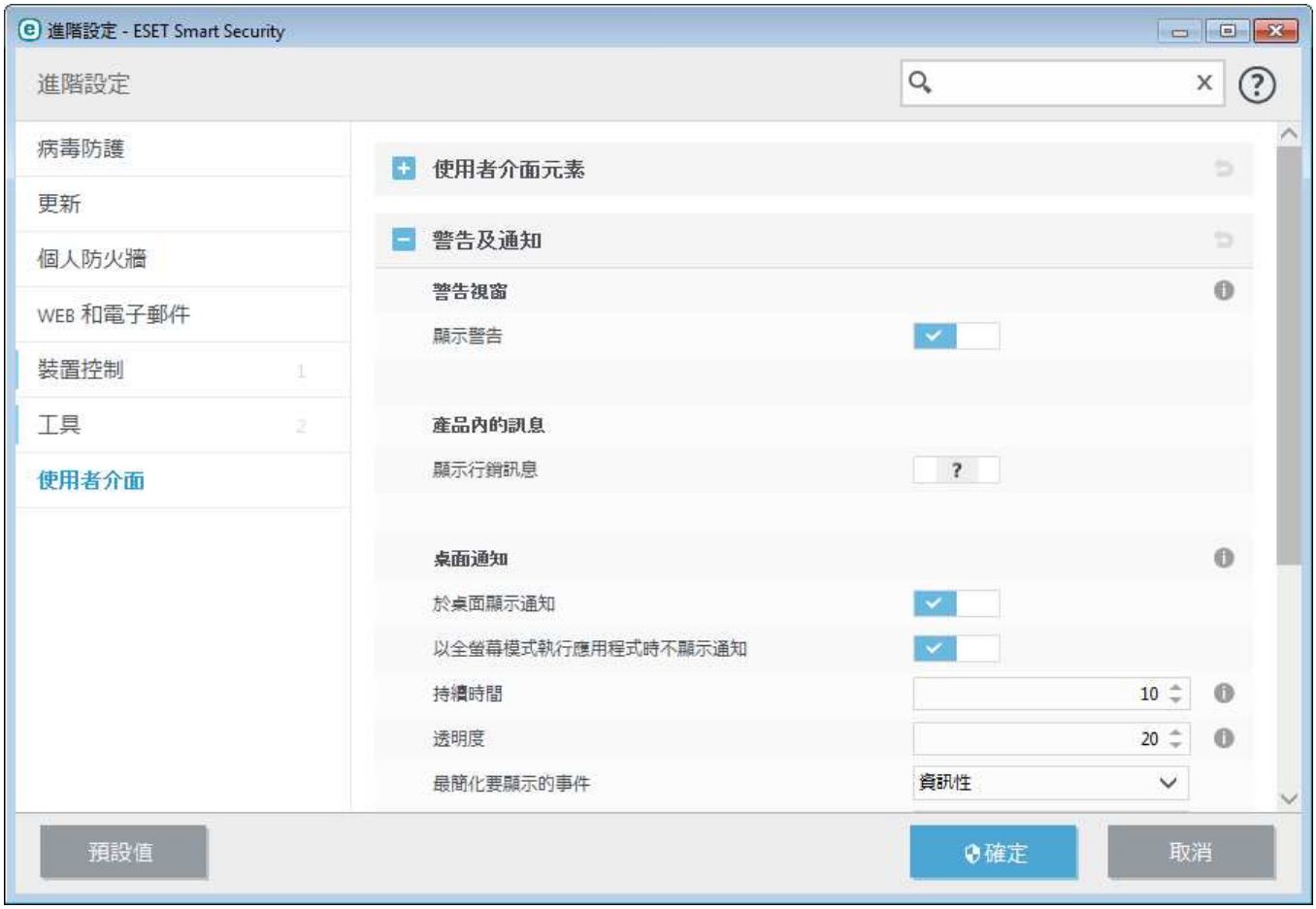
狀態

應用程式狀態 - 按一下 **[編輯]** 按鈕以管理 (停用) 顯示在主要功能表**防護狀態**窗格中顯示的狀態。



4.7.2 警告及通知

[使用者介面] 下的 **[警告及通知]** 區段可讓您配置 ESET Smart Security 如何處理威脅警告與系統通知 (例如，成功更新訊息)。您也可以設定顯示時間及系統匣通知的透明度 (這僅適用於支援系統匣通知的系統)。



警告視窗

停用 **[顯示警示]** 會取消所有警告視窗，且僅適用於有限的指定情況中。對於大部分使用者而言，我們建議保留此選項的預設值 (啟用)。

產品內的訊息

顯示行銷訊息 - 產品內訊息的設計是為了通知使用者 ESET 的最新消息與其他通訊。如果您不想要收到行銷訊息，請停用此選項。

桌面通知

桌面及球形提示上的通知僅提供資訊，不需要使用者介入。它們會顯示在畫面右下角的通知區域中。若要啟動桌面通知，請選取 **[於桌面顯示通知]**。

啟用 **[以全螢幕模式執行應用程式時不顯示通知]** 以強制不顯示所有非互動通知。可在以下修改更多詳細選項，如通知顯示時間及視窗透明度。

[最簡化要顯示的事件] 下拉式功能表中，允許您可以選取要顯示的警告及通知嚴重性層級。可用選項如下：

- **診斷** - 要微調程式和上述的所有記錄所需的防護記錄資訊。
- **資訊** - 記錄資訊性訊息，包含成功更新訊息及上述所有記錄。
- **警告** - 記錄嚴重錯誤及警告訊息。
- **錯誤** - 記錄諸如「下載檔案時發生錯誤」等類型的錯誤及嚴重錯誤。
- **嚴重** - 僅記錄嚴重錯誤 (啟動病毒防護 、內建防火牆等時發生錯誤)。

此區段的最後一個功能可讓您配置多個使用者環境的通知目的地。**[在多個使用者的系統中，在此使用者的畫面中顯示通知]** 欄位可針對允許多位使用者同時連接的系統，指定要接收系統通知與其他通知的使用者。通常為系統或網路的管理員。如果將所有系統通知都傳送給管理員，則此選項特別適用於終端機伺服器。

信箱

若要在某段時間內自動關閉快顯視窗，請選取 **[自動關閉訊息方塊]**。如果不手動關閉這些視窗，則經過指定時間後將自動關閉警告視窗。

確認訊息 - 向您顯示確認訊息的清單，並可讓您選取是否要顯示。

4.7.2.1 進階設定

從 **[最簡化要顯示的事件]** 下拉式功能表中，您可以選取將顯示警告及通知起始嚴重性層級。

- **診斷** - 要微調程式和上述的所有記錄所需的防護記錄資訊。
- **資訊性** - 記錄資訊性訊息，包含成功更新訊息及上述所有記錄。
- **警告** - 記錄嚴重錯誤及警告訊息。
- **錯誤** - 會記錄諸如「*下載檔案時發生錯誤*」類型的錯誤及嚴重錯誤。
- **嚴重** - 僅記錄嚴重錯誤 (啟動病毒防護、個人防火牆等時發生錯誤)。

此區段的最後一個功能可讓您配置多個使用者環境的通知目的地。**[在多個使用者的系統中，在此使用者的畫面中顯示通知]** 欄位可針對允許多位使用者同時連接的系統，指定要接收系統通知與其他通知的使用者。通常為系統或網路的管理員。如果將所有系統通知都傳送給管理員，則此選項特別適用於終端機伺服器。

4.7.3 隱藏通知視窗

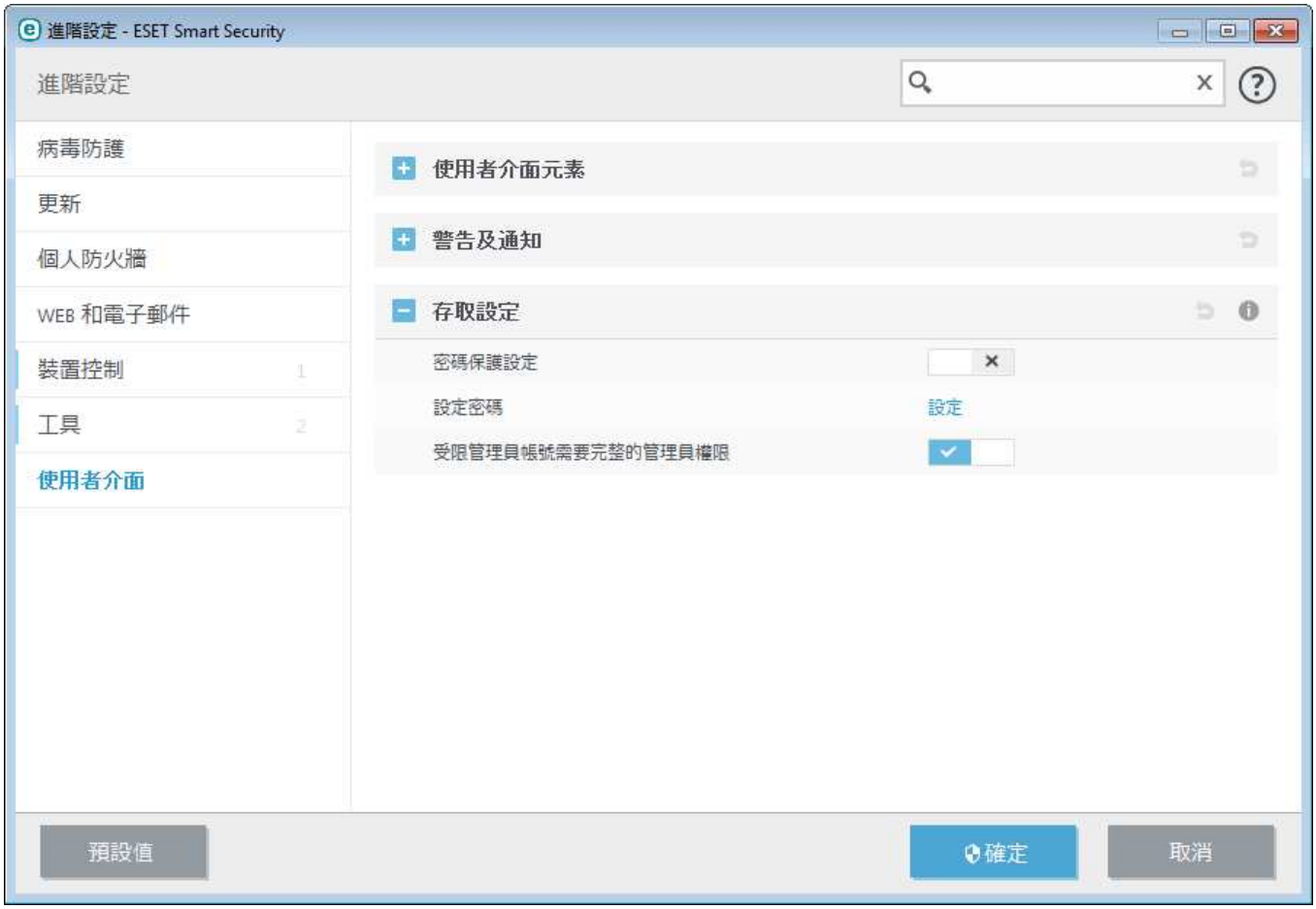
如果您曾經針對所有先前顯示的通知 (警告) 視窗選取 **[不要再顯示這則訊息]**，則這些視窗會出現在隱藏通知視窗的清單中。現在執行的處理方法會自動顯示在 **[確認]** 直欄中。

顯示 - 顯示目前未顯示，且具有已配置之自動處理方法的通知視窗預覽。

移除 - 從 **[隱藏的提示訊息]** 清單中移除項目。所有從清單中移除的通知視窗將會再次顯示。

4.7.4 存取設定

ESET Smart Security 設定是您安全原則最重要的部分。未獲授權的修改可能會危害您系統的穩定性及防護功能。為了避免未獲授權的修改，您可以使用密碼保護 ESET Smart Security 的設定參數。



密碼保護設定 - 指出密碼設定。按一下以開啟 [密碼設定] 視窗。

若要設定或變更密碼以保護設定參數，請按一下 **[設定]**。

受限管理員帳號需要完整的管理員權限 - 選取此選項以在修改特定系統參數時，提示現有使用者 (如果沒有管理員權限的話) 輸入管理員使用者名稱及密碼 (與 Windows Vista 和 Windows 7 中的「使用者帳戶控制」(UAC) 相似)。這類修改包括停用防護模組或關閉防火牆。 在未執行 UAC 的 Windows XP 系統上，使用者則可使用 **[需要管理員權限 (沒有 UAC 支援的系統)]** 選項。

僅限 Windows XP：

需要管理員權限 (沒有 UAC 支援的系統) - 啟用此選項，讓 ESET Smart Security 提示要求管理員憑證。

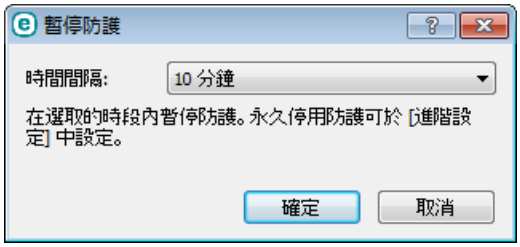
4.7.5 程式功能表

以滑鼠右鍵按一下系統匣圖示 ，可以使用某些最重要的設定選項及功能。

快速連結 - 顯示 ESET Smart Security 最常使用的部分。您可以從程式功能表快速存取這些部分。

暫停防護 - 顯示停用病毒及間諜程式防護的確認對話方塊，此功能藉由控制檔案、Web 和電子郵件通訊防止惡意系統攻擊。

[時間間隔] 下拉式功能表顯示病毒及間諜程式防護停用的期間。



暫停防火牆 (允許所有流量) - 將防火牆切換到非作用狀態。請參閱「網路」取得更多資訊。

封鎖所有網路流量 - 封鎖所有網路流量。您可按一下 **[停止封鎖所有網路流量]** 以再次啟用。

進階設定 - 選取此選項以進入 **[進階設定]** 樹狀目錄。其他開啟進階設定的方式還有按下 F5 鍵或瀏覽至 **[設定]** > **[進階設定]**。

[防護記錄檔案] - 防護記錄檔案包含已發生之重要程式事件的相關資訊，並提供偵測到之威脅的概觀。

隱藏 ESET Smart Security - 隱藏螢幕上的 ESET Smart Security 視窗。

重設視窗配置 - 將 ESET Smart Security 的視窗重設為螢幕上的預設大小及位置。

啟動產品... - 如果您尚未啟動您的 ESET 安全性產品，請選取此選項，或者在更新授權後重新輸入產品啟動頻憑證。

病毒資料庫更新 - 啟動更新病毒資料庫作業以確保您對抗惡意程式碼的防護層級。

關於 - 提供系統資訊、ESET Smart Security 已安裝版本的詳情，以及已安裝的程式模組。您還可以在這裡找到作業系統與系統資源的授權到期日期及相關資訊。

4.7.6 內容功能表

以滑鼠右鍵按一下物件之後，會顯示內容功能表。功能表會列出您可以對物件執行的所有動作。

可以將 ESET Smart Security 控制項元素整合至內容功能表。在 [進階設定] 樹狀目錄中可以使用此功能更詳細的設定選項，位於 **[使用者介面]** > **[內容功能表]** 下。

整合至內容功能表 - 將 ESET Smart Security 控制項元素整合至內容功能表。

下列選項可在 **[功能表類型]** 下拉式功能表中選用：

- **完整 (先掃描)** - 啟動所有內容功能表選項；主要功能表會顯示 **[以 ESET Smart Security 掃描，但不清除]** 為第一選項，並以 **[掃描並清除]** 做為第二層級項目。
- **掃描 (先清除)** - 啟動所有內容功能表選項；主要功能表會顯示 **[以 ESET Smart Security 掃描]** 為第一選項，並以 **[掃描但不清除]** 做為第二層級項目。

- **僅掃描** - 內容功能表只顯示 **[以 ESET Smart Security 掃描，但不清除]**。
- **僅清除** - 內容功能表只顯示 **[使用 ESET Smart Security 掃描]**。

5. 進階使用者

5.1 設定檔管理程式

設定檔管理程式是用於 ESET Smart Security 中的兩個區段 - **[指定電腦掃描]** 區段和 **[更新]** 區段。

電腦掃描

您偏好的掃描參數可儲存供未來掃描時使用。我們建議您盡量為定期進行的掃描建立不同設定檔 (含有各種掃描目標、掃描方法及其他參數)。

若要建立新的設定檔，請開啟 [進階設定] 視窗 (F5)，然後按一下 **[病毒防護]** > **[指定電腦掃描]** > **[基本]** > **[設定檔清單]**。**[設定檔管理員]** 視窗包括 **[已選取的設定檔]** 下拉式功能表，其中列出現有的掃描設定檔與可建立新設定檔的選項。若要協助您建立掃描設定檔以符合您的需求，請參閱 ThreatSense 引擎參數設定一節，以取得每個掃描設定參數的說明。

範例： 假設您要建立您自己的掃描設定檔且 **[掃描您的電腦]** 配置有部份適用，但不要掃描 運行時間壓縮器 或潛在不安全的應用程式，並且要套用 **[完全清除]**。在 **[設定檔管理程式]** 視窗中輸入新設定檔的名稱並按一下 **[新增]**。從 **[已選取的設定檔]** 下拉式功能表中選取新設定檔，並調整剩餘的參數以符合您的需求，接著按一下 **[確定]** 以儲存新的設定檔。

更新

[更新] 設定區段中的設定檔編輯器可讓使用者建立新的更新設定檔。請只有在您的電腦使用多種方法來連接更新伺服器時，才建立及使用您自己的自訂設定檔 (亦即，預設 **[我的設定檔]** 以外的其他設定檔)。

其中一個例子，就是膝上型電腦，它通常會連接至區域網路中的本機伺服器 (Mirror)，但是與區域網路中斷連線 (出差) 時，需要直接從 ESET 的更新伺服器下載更新，並使用兩種設定檔：第一個連接至本機伺服器，另一個連接至 ESET 的伺服器。在設定這些設定檔之後，請瀏覽至 **[工具]** > **[排程器]** 並編輯更新工作參數。指定一個設定檔為主要設定檔，另一個為次要設定檔。

已選取的設定檔 - 目前使用的更新設定檔。若要變更，請從下拉式功能表選擇設定檔。

新增... - 建立新的更新設定檔。

視窗底部會列出現有的設定檔。

5.2 鍵盤快捷鍵

為了更方便在 ESET 產品中瀏覽，可以使用下列鍵盤快捷鍵：

F1	開啟 [說明] 頁面
F5	開啟進階設定
向上/向下	在產品中瀏覽項目
-	收合 [進階設定] 樹狀結構節點
TAB 鍵	在視窗中移動游標
Esc 鍵	關閉作用中的對話方塊視窗

5.3 診斷

診斷可提供 ESET 處理程序 (例如 *ekrn*) 的應用程式當機傾印。如果應用程式當機，就會產生傾印。這可以協助開發人員除錯和修正各種 ESET Smart Security 問題。按一下 **[傾印類型]** 旁的下拉式功能表，並從三個可用選項中選取一個：

- 選取 **[停用]** (預設) 來停用這項功能。
- **最小** - 記錄最低限度的有用資訊，可用來協助識別應用程式意外當機的原因。如果空間有限，這種傾印檔案就很有助益。然而，因為資訊受限，所以分析此檔案時，可能會找不到發生問題時並非由正在執行之執行緒直接造成的錯誤。
- **完整** - 記錄系統記憶體在應用程式意外停止時的所有內容。完整記憶體傾印可能包含收集記憶體傾印時正在執行之處理程序的內容。

啟用個人防火牆進階記錄 - 以 PCAP 格式記錄所有通過個人防火牆的網路資料，以協助開發人員診斷及修正個人防火牆的相關問題。

啟用通訊協定過濾進階記錄 - 以 PCAP 格式記錄所有通過通訊協定過濾引擎的資料，以協助開發人員診斷及修正通訊協定過濾的相關問題。

您可以在以下路徑中找到防護記錄檔案：
Windows Vista 和更新版的 *C:\ProgramData\ESET\ESET Smart Security\Diagnostics* 或舊版 Windows 的 *C:\Documents and Settings\All Users\...*。

目標目錄 - 在當機期間產生傾印的目錄。

開啟診斷資料夾 - 按一下 **[開啟]**，在新的 *[Windows 檔案總管]* 視窗內開啟此目錄。

5.4 匯入及匯出設定

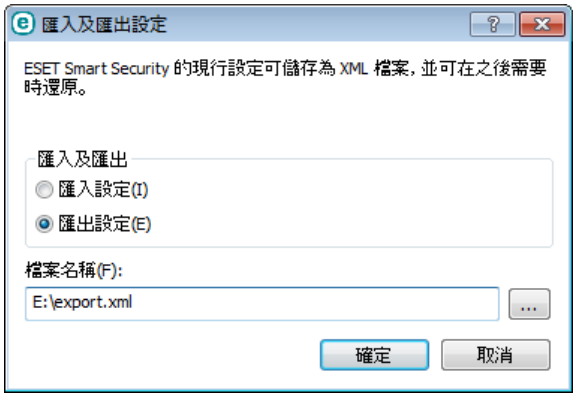
您可從 **[設定]** 功能表匯入或匯出您的自訂 ESET Smart Security .xml 配置檔案。

如果您必須備份 ESET Smart Security 的目前配置以供日後使用，匯入與匯出配置檔案功能則十分有用。匯出設定選項對想要在多個系統上使用慣用配置的使用者也很方便，他們可以輕鬆匯入 *.xml* 檔案以傳送這些設定。

匯入配置很簡單。從主要程式視窗中，按一下 **[設定]** > **[匯入及匯出設定]**，然後選取 **[匯入設定]**。輸入配置檔案的名稱，或按一下 **[...]** 按鈕以瀏覽您要匯入的配置檔案。

匯出配置的步驟非常類似。從主要程式視窗中，按一下 **[設定]** > **[匯入及匯出設定]**。選取 **[匯出設定]** 並輸入配置檔案的檔案名稱 (即 *export.xml*)。使用瀏覽器，選取在電腦上儲存配置檔案的位置。

附註： 如果您沒有足夠的權限將匯出檔案寫入指定目錄，則可能會在匯出設定時遭遇錯誤，



5.5 閒置狀態偵測

閒置狀態偵測設定可在 **[工具]** > **[閒置狀態偵測]** 下的 **[進階設定]** 中配置。這些設定可指定在以下狀況下觸發閒置狀態掃描：

- 螢幕保護程式執行中、
- 電腦已鎖住、
- 使用者已登出。

使用各種狀態的核取方塊以啟用或停用不同閒置狀態偵測觸發。

5.6 ESET SysInspector

5.6.1 ESET SysInspector 簡介

ESET SysInspector 是一款可徹底檢查電腦，並能以各種方法顯示收集之資料的應用程式。諸如安裝的驅動程式和應用程式、網路連線或重要的登錄項目等都能協助您調查可疑的系統行為，探討行為的成因究竟是來自軟體或硬體不相容，還是惡意程式感染。

有兩種方法可存取 ESET SysInspector：從 ESET Security 解決方案中整合的版本，或從 ESET 的網站免費下載獨立的版本 (SysInspector.exe)。這兩種版本在功能方面完全相同，而且有相同的程式控制項。唯一的差別在於管理輸出的方式。獨立的版本和整合的版本分別讓您將系統快照匯出為 *.xml* 檔和儲存於磁碟。不過，整合的版本可讓您將系統快照直接儲存於 **[工具]** > **ESET SysInspector** (除了 ESET Remote Administrator)。 如需更多資訊，請參閱ESET SysInspector 是 ESET Smart Security 的一部分一節。

請等候 ESET SysInspector 掃描電腦。視硬體配置、作業系統和電腦上安裝的應用程式數而定，這可能需要 10 秒到幾分鐘的時間。

5.6.1.1 啟動 ESET SysInspector

若要啟動 ESET SysInspector，只要執行從 ESET 網站下載的 *SysInspector.exe* 執行檔即可。 如果您已安裝任一款 ESET Security 解決方案，可以直接從 [開始] 功能表執行 ESET SysInspector (按一下 **[程式]** > **[ESET]** > **[ESET Smart Security]**)。

應用程式檢查系統時請稍候，這可能需花費數分鐘。

5.6.2 使用者介面和應用程式用法

為清楚起見，主要程式視窗分為四個主要區段：位於主要程式視窗頂端的「程式控制」、位於中間左側的「瀏覽」視窗、位於右側的「說明視窗」，以及位於主要程式視窗底部的「詳細資料」視窗。[防護記錄狀態] 區段列出防護記錄的基本參數 (使用的過濾器、過濾器類型、防護記錄是否為比較的結果等)。

5.6.2.1 程式控制項

本小節包含 ESET SysInspector 中提供的所有程式控制項說明。

檔案

按 **[檔案]**，您即可儲存您目前的系統狀態作為稍後調查之用，或是開啟先前儲存的防護記錄。如果您要發行防護記錄，我們建議您產生**適合傳送**的防護記錄。此形式的防護記錄將會省略機密資訊 (目前的使用者名稱、電腦名稱、網域名稱、目前的使用者權限、環境變數等)。

附註： 您可以開啟先前儲存的 ESET SysInspector 報告，只要將報告拖放至主要程式視窗即可。

樹狀結構

讓您可以展開或關閉所有節點，並且可以將選取的區段匯出成「服務」腳本。

清單

包含可以在程式內更方便瀏覽的功能，以及各式其他功能，如線上尋找資訊。

說明

包含有關應用程式及其功能的資訊。

詳情

此設定影響在主要程式視窗顯示的資訊，讓您更加輕鬆使用資訊。在「基本」模式下，您可以存取用來尋找系統常見問題的解決方案資訊。在「中階」模式下，程式會顯示不常使用的詳情。在「完整」模式下，ESET SysInspector 會顯示解決特定問題所需的所有資訊。

過濾

項目過濾最適合用來尋找系統中的可疑檔案或登錄項目。透過調整滑桿，您可以依據「風險層級」過濾項目。如果滑桿被設定至最左邊 (風險層級 1)，則所有項目都會顯示。藉由將滑桿移動至右邊，程式會濾除所有風險低於目前風險等級的項目，只出現比顯示的層級更可疑的項目。當滑桿移至最右邊，程式僅顯示已知的有害項目。

所有標示為風險範圍 6 至 9 的項目都會引起安全性風險。如果你正在使用 ESET 安全性解決方案，如果 ESET SysInspector 找到任何此類項目，我們建議您使用 ESET Online Scanner 掃描系統。ESET Online Scanner 是免費的服務。

附註： 透過比較項目的色彩和風險層級滑桿上的色彩，您可以快速判斷項目的風險層級。

比較

在比較兩筆防護記錄時，您可以選擇顯示所有項目、只顯示新增項目、只顯示移除的項目，或只顯示已取代的項目。

尋找

搜尋可以透過項目的名稱或部分名稱，快速尋找特定的項目。搜尋要求的結果會顯示在 [說明] 視窗中。

返回

按一下 [返回] 和 [下一個] 箭號，您可返回至先前 [說明視窗] 中顯示的資訊。您可以使用退格鍵和空白鍵取代按一下 [返回] 和 [下一個]。

狀態區段

顯示 [瀏覽] 視窗中目前的節點。

重要 以紅色反白顯示的項目是未知的，這就是程式將其標記為潛在危險的原因。如果項目呈現紅色，這不表示您可以理所當然地刪除該檔案。進行刪除前，請確認檔案真的有危險性或是並非必要。

5.6.2.2 在 ESET SysInspector 中瀏覽

ESET SysInspector 將各種資訊類型分成數個稱為節點的基本區段。將每個節點展開至子節點，就可以找到更多詳情 (如果有的話)。若要開啟或折疊節點，連按兩下節點名稱或者按一下節點名稱旁的 ⊞ 或 ⊟。當您在 [瀏覽] 視窗中，透過節點和子節點的樹狀結構進行瀏覽時，您會發現 [說明] 視窗中會顯示每個節點的各種詳情。如果您在 [說明] 視窗中從頭到尾瀏覽項目，則每個項目的其他詳情會顯示在 [詳情] 視窗中。

以下說明有關 [瀏覽] 視窗的主節點，以及 [說明] 視窗和 [詳情] 視窗的相關資訊。

執行程序

此節點包含有關應用程式和程序在產生防護記錄時的資訊。在 [說明] 視窗中，您會找到更多關於每個程序的詳情，如程序使用的動態程式庫及其在系統中的位置、應用程式供應商的名稱和檔案的風險等級。

[詳情] 視窗包含在 [說明] 視窗中所選取項目的其他資訊，如檔案大小或雜湊。

附註： 作業系統由數種從不間斷執行的重要核心元件構成，並提供其他使用者應用程式基本且必要的功能。在某些狀況下，這樣的程序會顯示在工具 ESET SysInspector 中，其檔案路徑以 \??\ 開始。那些符號提供程序啟動前的最佳化，這個動作對系統無害。

網路連線

[說明] 視窗包含使用 [瀏覽] 視窗中選取的通訊協定 (TCP 或 UDP)，透過網路進行通訊的程序和應用程式清單，以及應用程式要連接的遠端位址。您也可以查看 DNS 伺服器的 IP 位址。

[詳情] 視窗包含在 [說明] 視窗中所選取項目的其他資訊，如檔案大小或雜湊。

重要登錄項目

包含已選取的登錄項目清單，那些登錄項目通常與系統的各種問題有關，如指定啟動程式、瀏覽器 Helper 物件 (BHO) 等。

在 [說明] 視窗中，您可以找到與特定登錄項目相關的檔案。您可以在 [詳情] 視窗中看到其他詳情。

服務

[說明] 視窗包含登錄為 Windows 服務的檔案清單。您可以檢查服務設定啟動的方式，並在 [詳情] 視窗中檢查檔案的特定詳情。

驅動程式

安裝在系統上的驅動程式清單。

重要檔案

[說明] 視窗顯示與 Microsoft Windows 作業系統相關的重要檔案內容。

系統工作安排精靈工作

包含由 Windows 工作排程器在指定的時間 / 間隔觸發的工作清單。

系統資訊

包含硬體和軟體的詳細資訊，以及有關設定環境變數、使用者權限和系統事件防護記錄的資訊。

檔案詳情

重要系統檔案和 [Program Files] 資料夾中檔案的清單。檔案特定的其他資訊可在 [說明] 視窗和 [詳情] 視窗中找到。

關於

ESET SysInspector 版本及程式模組清單的資訊。

5.6.2.2.1 鍵盤捷徑

使用 ESET SysInspector 時可使用的鍵盤捷徑包括：

檔案

Ctrl+O	開啟現有的防護記錄
Ctrl+S	儲存已建立的防護記錄

產生

Ctrl+G	產生標準電腦狀態快照
Ctrl+H	產生可記錄敏感資料的電腦狀態快照

項目過濾

1 或 O	良好，會顯示風險層級 1-9 的項目
2	良好，會顯示風險層級 2-9 的項目
3	良好，會顯示風險層級 3-9 的項目
4 或 U	未知，會顯示風險層級 4-9 的項目
5	未知，會顯示風險層級 5-9 的項目
6	未知，會顯示風險層級 6-9 的項目
7 或 B	危險，會顯示風險層級 7-9 的項目
8	危險，會顯示風險層級 8-9 的項目
9	危險，會顯示風險層級 9 的項目
-	降低風險層級
+	提高風險層級
Ctrl+9	過濾模式，同等級或更高
Ctrl+0	過濾模式，僅同等級

檢視

Ctrl+5	依供應商，所有供應商檢視
Ctrl+6	依供應商檢視，僅 Microsoft
Ctrl+7	依供應商，所有其他供應商檢視
Ctrl+3	顯示完整詳情
Ctrl+2	顯示媒體詳情
Ctrl+1	基本顯示
退格鍵	往回移動一個步驟
空白鍵	往前移動一個步驟
Ctrl+W	展開樹狀結構
Ctrl+Q	收合樹狀結構

其他控制項

Ctrl+T	在搜尋結果中選取後，移動至項目的原始位置
Ctrl+P	顯示關於項目的基本資訊
Ctrl+A	顯示關於項目的完整資訊
Ctrl+C	複製目前項目的樹狀結構
Ctrl+X	複製項目
Ctrl+B	在網際網路尋找有關選取檔案的資訊
Ctrl+L	開啟選取檔案所在的資料夾
Ctrl+R	在登錄編輯器中開啟對應的項目
Ctrl+Z	複製檔案的路徑 (如果項目與檔案相關的話)
Ctrl+F	切換至搜尋欄位
Ctrl+D	關閉搜尋結果
Ctrl+E	執行服務腳本

比較

Ctrl+Alt+O	開啟原始/相較防護記錄

Ctrl+Alt+R	取消比較
Ctrl+Alt+1	顯示所有項目
Ctrl+Alt+2	僅顯示新增的項目，防護記錄將顯示目前防護記錄中出現的項目
Ctrl+Alt+3	僅顯示移除的項目，防護記錄將顯示先前防護記錄中出現的項目
Ctrl+Alt+4	僅顯示被取代的項目 (包括檔案)
Ctrl+Alt+5	僅顯示防護記錄間的相異之處
Ctrl+Alt+C	顯示比較
Ctrl+Alt+N	顯示目前的防護記錄
Ctrl+Alt+P	開啟先前的防護記錄

其他選項

F1	檢視說明
Alt+F4	關閉程式
Alt+Shift+F4	不詢問直接關閉程式
Ctrl+I	防護記錄統計

5.6.2.3 比較

「比較」功能可以讓使用者比較兩份現有的防護記錄。此功能的結果是兩份防護記錄之間非共同的項目組。如果您要追蹤系統的變更，此功能非常適合 - 是偵測惡意程式的實用工具。

功能啟動後，應用程式會建立新的防護記錄，該防護記錄會在新的視窗中顯示。按一下 **[檔案]** > **[儲存防護記錄]**，將防護記錄儲存至檔案。您可稍後再開啟和檢視防護記錄檔案。若要開啟現有的防護記錄，請按一下 **[檔案]** > **[開啟防護記錄]**。在主程式視窗中，ESET SysInspector 會一次顯示一份防護記錄。

比較兩份防護記錄的好處是，您可以同時檢視目前作用中的防護記錄，以及另一份儲存成檔案的記錄。若要比較防護記錄，請按一下 **[檔案]** > **[比較防護記錄]**，然後選擇 **[選取檔案]**。選取的防護記錄會與主程式視窗作用中的防護記錄進行比較。相較防護記錄僅會顯示兩份防護記錄間的相異之處。

附註： 如果您要比較兩份防護記錄檔案，請按一下 **[檔案]** > **[儲存防護記錄]**，然後儲存成 ZIP 檔案，則會儲存兩個檔案。如果您稍後開啟這個檔案，內含的防護記錄就會自動進行比較。

在顯示的項目旁，ESET SysInspector 會顯示符號來識別兩份比較防護記錄間的相異之處。

項目旁顯示的所有符號說明如下：

- + 先前防護記錄沒有的新值
- 含有新值的樹狀結構區段
- − 只存在先前防護記錄中，現已移除的值
- 含有已移除之值的樹狀結構區段
- 已變更的值 / 檔案
- 含有已修改之值 / 檔案的樹狀結構區段
- 風險層級已降低 / 先前防護記錄中的風險層級較高
- 風險等級已增加 / 先前防護記錄中的風險等級較低

左下角顯示的解釋區段描述所有的符號，也顯示正在進行比較的兩份防護記錄名稱。

任何相較防護記錄都可以儲存成檔案，並稍後再開啟。

範例

產生並儲存防護記錄 (記錄關於系統的原始資訊) 至名為 previous.xml 的檔案。系統變更生效後，開啟 ESET SysInspector 以

產生新的防護記錄。將防護記錄儲存至名為 *current.xml* 的檔案。

為追蹤這兩份防護記錄間的變更，請按一下 **[檔案]** > **[比較防護記錄]**。程式會建立相較防護記錄，顯示防護記錄間的相異之處。

如果您使用下列命令列選項，您可以保存相同的結果：

SysIsnpector.exe current.xml previous.xml

5.6.3 命令列參數

ESET SysInspector 支援使用這些參數，透過命令列產生報告：

/gen	直接從指令列產生防護記錄，而不執行 GUI
/privacy	產生忽略敏感資料的防護記錄
/zip	在 zip 壓縮檔中儲存結果防護記錄
/silent	從指令列產生防護記錄時隱藏處理視窗
/blank	- 啟動 ESET SysInspector 而不產生/載入防護記錄

範例

用法：
```
Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]
```

若要將特定防護記錄直接載入至瀏覽器，用法如下：*SysInspector.exe .\clientlog.xml*
若要從指令列產生防護記錄，用法如下：*SysInspector.exe /gen=.\mynewlog.xml*
若要以壓縮檔方式直接產生排除敏感資訊的防護記錄，用法如下：*SysInspector.exe /gen=.\mynewlog.zip /privacy /zip*
若要比較兩個防護記錄檔並瀏覽差異，用法如下：*SysInspector.exe new.xml old.xml*

附註： 如果檔案/資料夾名稱含有空格，則檔案/資料夾名稱應放在引號內。

5.6.4 服務腳本

服務腳本可以輕易從系統中移除不要的物件，是能夠對使用 ESET SysInspector 之客戶提供協助的工具。

服務腳本可以讓使用者匯出整個 ESET SysInspector 防護記錄，或是使用者選取的部份。匯出後，您可以標記不需要的部份以便進行刪除。然後，您可以執行修改過的防護記錄以刪除標記的物件。

服務腳本適用於已擁有診斷系統問題經驗的進階使用者。不合格的修改可能會導致作業系統損害。

範例

如果您懷疑電腦已感染病毒，但防毒程式沒有偵測到，請遵循以下逐步說明：

1. 執行 ESET SysInspector 以產生新的系統快照。
2. 選取左側 (樹狀結構中) 區段中的第一個項目，按下 Shift 鍵並選取最後一個項目以標記所有項目。
3. 在選取的物件上按一下滑鼠右鍵，並選取 **[將選取的區段匯出至服務腳本]**。
4. 選取的物件會匯出至新的防護記錄。
5. 這是整個程序中最重要的步驟：打開新的防護記錄，針對所有要移除的物件，將其 - 屬性變更成 +。請確認您沒有標記任何重要的作業系統檔案/物件。
6. 開啟 ESET SysInspector，並且按一下 **[檔案]** > **[執行服務腳本]**，然後輸入腳本的路徑。
7. 按一下 **[確定]** 以執行腳本。

5.6.4.1 產生服務腳本

若要產生腳本，請在 ESET SysInspector 主視窗中以滑鼠右鍵按一下功能表樹狀結構 (左側窗格) 中的任何項目。接著在內容功能表中選取 **[將所有區段匯出至服務腳本]** 或 **[將選取的區段匯出至服務腳本]**。

附註： 在比較兩份防護記錄時，無法匯出服務腳本。

5.6.4.2 服務腳本的結構

您可以在腳本檔頭的第一行發現引擎版本 (ev)、GUI 版本 (gv) 及防護記錄版本 (lv) 的相關資訊。這些資料可讓您追蹤產生腳本之 .xml 檔案中可能存在的變更，以避免在執行期間發生任何不一致的情況。請勿改動腳本的此部分。

檔案的其他部分可分為多個區段，而這些區段中的項目是可編輯的項目 (表示將由腳本處理的項目)。將項目前的 "-" 字元取代為 "+" 字元可將項目標記為要處理的項目。腳本中的各個區段是以空白的文字行做為區隔。每個區段都有各自的編號和標題。

01) 執行中的處理程序

此區段包含系統中所有執行之程序的清單。每個程序均可透過其 UNC 路徑及隨後之星號 (*) 間的 CRC16 雜湊碼加以識別。

範例：

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

在此範例中，module32.exe 程序已經過選取 (前端有 "+" 字元標記)；程序將在執行腳本後結束。

02) 載入的模組

此區段可列出目前使用的系統模組。

範例：

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

在此範例中，khbekhb.dll 模組前有 "+" 標記。執行腳本時，腳本能使用該特定的模組來辨識程序及結束程序。

03) TCP 連線

此區段含有和現有 TCP 連線相關的資訊。

範例：

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

執行腳本時，腳本能尋找已標記之 TCP 連線的通訊端擁有者，接著再停止通訊端以釋放系統資源。

04) UDP 端點

此區段含有和現有 UDP 端點相關的資訊。

範例：

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

執行腳本時，腳本能隔離已標記之 UDP 端點上的通訊端擁有者，然後再停止通訊端。

05) DNS 伺服器項目

此區段含有和目前 DNS 伺服器配置相關的資訊。

範例：

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

執行腳本時，已標記的 DNS 伺服器項目會遭到移除。

06) 重要登錄項目

此區段含有和重要登錄項目相關的資訊。

範例：

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

執行腳本時，已標記的項目將遭到刪除、減少為 0 位元值或重設其預設值。要套用至特定項目的處理方法取決於項目類別和特定登錄中的機碼值。

07) 服務

此區段可列出系統內的已登錄服務。

範例：

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

執行腳本時，已標記之服務與其相依服務均會遭到停止及解除安裝。

08) 驅動程式

此區段可列出已安裝的驅動程式。

範例：

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

當您執行腳本時，將停止選取的驅動程式。注意，某些驅動程式無法停止。

09) 重要檔案

此區段含有和作業系統正常運作所需重要之檔案相關的資訊。

範例：

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

選取的項目將遭到刪除或重設為原始的值。

10) 已排程的工作

本節包含已排程的工作相關資訊。

範例：

```
10) Scheduled tasks
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe /c
- c:\users\admin\appdata\local\google\update\googleupdate.exe /ua /installsource
- %windir%\system32\appidpolicyconverter.exe
- %windir%\system32\appidcertstorecheck.exe
- aitagent
[...]
```

5.6.4.3 執行服務腳本

標記所有需要的項目，接著再儲存及關閉腳本。選取 [檔案] 功能表中的 **[執行服務腳本]** 選項可直接從 ESET SysInspector 主視窗執行編輯過的腳本。開啟腳本時，程式會顯示下列訊息以資提示：**您確定要執行服務腳本「%Scriptname%」嗎？** 確認您選取的項目後，畫面中會出現另一則警告，通知您嘗試執行的服務腳本尚未經過簽署。按一下 **[執行]** 以啟動腳本。

畫面中隨即會出現對話方塊視窗，確認腳本已成功執行。

如果腳本只能部分執行，畫面中會出現對話方塊視窗並顯示下列訊息：**已部分執行服務腳本。您想要檢視錯誤報告嗎？** 選取 **[是]** 可檢視複雜的錯誤報告，此報告會列出未執行的作業。

如果腳本無法辨識，畫面中會出現對話方塊視窗並顯示下列訊息：**選取的服務腳本尚未經過簽署。執行未經簽署和未知的腳本會嚴重損害您的電腦資料。您確定要執行腳本及履行處理方法嗎？** 這可能是由於腳本內容不一致所引起的 (損壞的標題、損壞的區段標題、遺失區段間的空白文字行等)。您可以重新開啟腳本檔案並修正腳本內容中的錯誤，或建立新的服務腳本。

5.6.5 常見問題

ESET SysInspector 需要管理員權限才能執行嗎？

ESET SysInspector 不需要管理員權限即可執行，然而收集的部分資訊需要透過管理員帳戶才能存取。以「標準的使用者」或「限制的使用者」執行將會導致收集到較少的作業環境資訊。

ESET SysInspector 是否會建立防護記錄檔案？

ESET SysInspector 可以建立您電腦配置的防護記錄檔案。若要儲存一個防護記錄檔案，請從主要程式視窗中按一下 **[檔案]** > **[儲存防護記錄]**。防護記錄會儲存成 XML 格式。依預設，檔案會儲存至 *%USERPROFILE%\My Documents* 目錄，檔案命名的慣例是「SysInpsector-%COMPUTERNAME%-YYMMDD-HHMM.XML」。如果需要，在儲存之前，可以變更防護記錄檔案的位置和名稱。

我如何檢視 ESET SysInspector 防護記錄檔案？

若要檢視由 ESET SysInspector 建立的防護記錄檔案，請執行程式，然後按一下主要程式視窗中的 **[檔案]** > **[開啟防護記錄]**。您也可以拖放防護記錄檔案至 ESET SysInspector 應用程式。如果您必須經常檢視 ESET SysInspector 防護記錄檔案，我們建議您在桌面上建立連結至 SYSINSPECTOR.EXE 檔案的捷徑，您就可以拖放防護記錄檔案至捷徑以便進行檢視。基於安全性理由，Windows Vista/7 可能不允許在兩種不同安全性權限的視窗之間進行拖放。

防護記錄檔案格式是否有可用的規格？或是有 SDK？

目前為止，由於程式仍在開發中，所以暫不提供防護記錄檔案的規格書或是 SDK。程式上市後，視客戶的意見和需求，我們可能會提供這些服務。

ESET SysInspector 如何評估由特定物件引起的風險？

在大多數的情況下，ESET SysInspector 使用一系列的啟發式規則指派物件 (檔案、程序、登錄機碼等等) 的風險層級；規則會檢查每個物件的特性，然後衡量惡意活動的潛在性。依據這些啟發式規則，物件會被指派為「1 - 良好 (綠色)」至「9 - 危險 (紅色)」之間的風險層級。在左邊瀏覽窗格中，區段的色彩會依據內含的最高風險層級物件而改變。

風險層級「6 - 未知 (紅色)」是否意謂著物件是危險的？

ESET SysInspector 的評定不能保證物件是惡意的，測定必須由安全性專家進行。ESET SysInspector 的設計是為安全性專家提供快速評定，因此專家才能知道系統上哪個物件需要進一步檢查異常行為。

為什麼 ESET SysInspector 執行時會連線至網際網路？

就像許多應用程式一樣，ESET SysInspector 經過數位簽章「憑證」簽署，藉以協助確認軟體由 ESET 發行，未曾被改動過。為了確認憑證，作業系統會聯繫憑證授權單位，確認軟體發行者的身份。這是在 Microsoft Windows 下，所有經過數位簽章程式的一般行為。

什麼是反隱藏技術？

反隱藏技術提供有效的 Rootkit 偵測。

如果系統遭 Rootkit 方式的惡意程式攻擊，則使用者可能會暴露在資料遺失或遭竊的風險之中。如果沒有特殊的反 Rootkit 工具，幾乎不可能偵測得到 Rootkit。

為什麼有時候標記為「由 MS 簽署」的檔案同時間會有不同的「公司名稱」項目？

嘗試辨識可執行檔的數位簽章時，ESET SysInspector 會先檢查數位簽章是否內嵌在檔案內。如果找到數位簽章，檔案將以該資訊進行驗證。如果找不到數位簽章，ESI 會開始尋找對應的 CAT 檔案 (安全性目錄 - *%systemroot%\system32\catroot*)，其中包含有關可執行檔案處理的資訊。如果找到相關的 CAT 檔案，該 CAT 檔案的數位簽章將會套用到可執行檔案的驗證程序。

這就是為什麼有時候標記為「由 MS 簽署」的檔案，「公司名稱」項目不同的原因。

範例：

Windows 2000 內含 HyperTerminal 應用程式，位置是 *C:\Program Files\Windows NT*。主應用程式的可執行檔案未經數位簽署，但是 ESET SysInspector 將其標記為由 Microsoft 簽署的檔案。其中的源由是因為 *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* 中的參考指向 *C:\Program Files\Windows NT\hypertrm.exe*

(HyperTerminal 的應用程式主要可執行檔案)，而 *sp4.cat* 是由 Microsoft 進行數位簽署的。

5.6.6 ESET SysInspector 是 ESET Smart Security 的一部份

若要開啟 ESET Smart Security 中的 ESET SysInspector 區段，請按一下 **[工具]** > **ESET SysInspector**。ESET SysInspector 視窗中的管理系統和電腦掃描防護記錄或已排程工作的管理系統類似。所有包括系統快照的作業 - 建立、檢視、比較、移除和匯出 - 只需要按一次或按兩次即可存取。

ESET SysInspector 視窗包含有關已建立快照的基本資訊，如建立時間、簡短註解、建立快照的使用者名稱和快照狀態。

若要比較、建立或刪除快照，請使用 ESET SysInspector 視窗中位於快照清單下方的對應按鈕。那些選項也可在內容功能表中使用。若要檢視選取的系統快照，請選取內容功能表中的 **[顯示]**。若要將選取的快照匯出至檔案，以滑鼠右鍵按一下快照，然後選取 **[匯出...]**。

以下是可用選項的詳細說明：

- **[比較]** - 允許您比較兩份現存的防護記錄。如果您要追蹤目前防護記錄和較舊防護記錄間的變更，此功能非常適合。若要使此選項生效，您必須選取兩份要進行比較的快照。
- **[新建...]** - 可建立新記錄。建立新記錄前，您必須輸入有關記錄的簡短註解。若要瞭解 (目前產生的快照的) 快照建立的進度，請參閱 **[狀態]** 直欄。所有已完成的快照會標記為 **[已**建立] 狀態
- **[刪除 / 全部刪除]** - 從清單移除項目。
- **匯出...** - 將選取的項目儲存成 XML 檔案 (也可以是 ZIP 版本)。

5.7 命令列

ESET Smart Security 的防毒模組可以透過命令列來啟動，具體方法可以是手動 (使用「ecls」命令) 或使用批次 (「bat」) 檔。ESET 命令列掃描器用法：

```
ecls [OPTIONS..]FILES..
```

從命令列執行指定掃描器時，可以使用下列參數及切換參數：

選項

/base-dir=FOLDER	從資料夾 (FOLDER) 載入模組
/quar-dir=FOLDER	隔離資料夾 (FOLDER)
/exclude=MASK	從掃描中排除符合遮罩 (MASK) 的檔案
/subdir	掃描子資料夾 (預設值)
/no-subdir	不掃描子資料夾
/max-subdir-level=LEVEL	待掃描資料夾中的最大資料夾子層級數目
/symlink	跟循符號連結 (預設值)
/no-symlink	略過符號連結
/ads	掃描 ADS (預設值)
/no-ads	不掃描 ADS
/log-file=FILE	將輸出記錄至檔案 (FILE)
/log-rewrite	覆寫輸出檔 (預設值 - 附加)
/log-console	在主控台記錄輸出 (預設值)
/no-log-console	不在主控台記錄輸出
/log-all	也記錄清除檔案
/no-log-all	不記錄清除檔案 (預設值)
/aind	顯示活動指示器
/auto	掃描所有本機磁碟並自動清除病毒

掃描器選項

/files	掃描檔案 (預設值)
/no-files	不掃描檔案
/memory	掃描記憶體
/boots	掃描開機磁區
/no-boots	不掃描開機磁區 (預設值)
/arch	掃描壓縮檔 (預設值)

/no-arch	不掃描壓縮檔
/max-obj-size=SIZE	只掃描小於指定大小 (SIZE，單位 MB) 的檔案 (預設值 0 = 無限制)
/max-arch-level=LEVEL	待掃描壓縮檔 (巢狀壓縮檔) 內的最大壓縮檔層級
/scan-timeout=LIMIT	掃描壓縮檔的最多時間限制 (LIMIT，單位 (秒))
/max-arch-size=SIZE	僅掃描在壓縮檔中小於指定大小 (SIZE) 的檔案 (預設值 0 = 無限制)
/max-sfx-size=SIZE	只掃描在自我解壓檔中小於指定大小 (SIZE，單位 MB) 的檔案 (預設值 0 = 無限制)
/mail	掃描電子郵件檔案 (預設值)
/no-mail	不掃描電子郵件檔案
/mailbox	掃描信箱 (預設值)
/no-mailbox	不掃描信箱
/sfx	掃描自我解壓檔 (預設值)
/no-sfx	不掃描自我解壓檔
/rtp	掃描運行時間壓縮器 (預設值)
/no-rtp	不掃描運行時間壓縮器
/unsafe	掃描潛在不安全的應用程式
/no-unsafe	不掃描潛在不安全的應用程式 (預設值)
/unwanted	掃描潛在不需要應用程式
/no-unwanted	不掃描潛在不需要程式 (預設值)
/suspicious	掃描可疑的應用程式 (預設值)
/no-suspicious	不掃描可疑的應用程式
/pattern	使用簽章 (預設值)
/no-pattern	不使用簽章
/heur	啟用啟發式 (預設值)
/no-heur	停用啟發式
/adv-heur	啟用進階啟發式 (預設值)
/no-adv-heur	停用進階啟發式
/ext=EXTENSIONS	只掃描以冒號分隔的副檔名 (EXTENSIONS)
/ext-exclude=EXTENSIONS	從掃描中排除以冒號分隔的副檔名 (EXTENSIONS)
/clean-mode=MODE	針對受感染物件使用清除「模式」。 可用選項如下： • **none** - 將不會進行自動清除。 • **standard** (預設值) - ecls.exe 將嘗試自動清除或刪除受感染的檔案。 • **strict** - ecls.exe 將嘗試在沒有使用者介入的情況下，自動清除或刪除受感染的檔案 (在檔案刪除前，系統不會提醒您)。 • **rigorous** - ecls.exe 無論檔案為何，將會刪除檔案而不嘗試清除。 • **delete** - ecls.exe 將刪除檔案而不嘗試清除，但會避免刪除敏感的檔案，例如 Windows 系統檔案。
/quarantine	複製受感染檔案 (如果已清除) 到隔離區 (補充清除時執行的處理方法)
/no-quarantine	不要複製受感染檔案到隔離區

一般選項

/help	顯示說明並結束
/version	顯示版本資料並結束
/preserve-time	保存最後一次的存取時間郵戳

結束代碼

0	找不到威脅
1	找到威脅並已清除
10	無法掃描某些檔案 (可能是威脅)
50	找到威脅
100	錯誤

附註： 大於 100 的結束代碼表示未掃描檔案，檔案可能已受感染。

6. 字彙

6.1 入侵類型

「入侵」是嘗試進入及/或損害使用者電腦的一種惡意軟體。

6.1.1 病毒

電腦病毒是一種惡意程式碼，會附加到電腦的現有檔案上。病毒這個名稱取自生物學的病毒，因為病毒會利用類似的方式，從一部電腦散播至另一部電腦。「病毒」這個名詞常常被不當用於表示指任何類型的威脅。這種情況已逐漸減少，而改用較精確的詞彙「惡意軟體」(具惡意的軟體)。

電腦病毒主要會攻擊執行檔及文件。簡而言之，電腦病毒的運作如下：在執行受感染的檔案後，會先呼叫並執行惡意程式碼，再執行原始的應用程式。病毒會感染任何目前使用者有寫入權限的檔案。

電腦病毒有目的與嚴重性之分。有些病毒因為能夠故意將硬碟機中的檔案刪除，而顯得極度危險。另一方面，有些病毒並不會造成真正的損害 – 這些病毒只會困擾使用者，並展現其作者的技術。

如果您的電腦遭到病毒感染，且無法清除，請將電腦送到 ESET 研究實驗室檢查。在特定狀況下，受感染的檔案會被修改為無法清除，且必須以沒有未感染的副本取代受感染檔案的程度。

6.1.2 蠕蟲

電腦蠕蟲是含有惡意程式碼的程式，它會攻擊主機電腦，並透過網路散佈。病毒與蠕蟲的基本差異在於蠕蟲有能力自行繁殖；蠕蟲不需仰賴主機檔案 (或開機磁區)。蠕蟲透過連絡人名單中的電子郵件地址散佈，或利用網路應用程式中的安全性弱點。

因此，蠕蟲的存活率比電腦病毒高多了。因為網際網路的普及，蠕蟲可能在發佈後的數小時內，就散佈到全世界，甚至只需幾分鐘的時間。這種獨立又快速的複製能力，使蠕蟲比其他類型的惡意軟體更加危險。

在系統中活化的蠕蟲會造成許多不便：如刪除檔案、降低系統效能，甚至會停用程式。電腦蠕蟲的本質使其能夠成為其他入侵類型的「傳輸媒介」。

如果您的電腦感染了蠕蟲，我們建議您刪除受感染的檔案，因為其中可能包含惡意程式碼。

6.1.3 特洛伊木馬程式

從歷史角度來看，電腦特洛伊木馬程式已被定義為一種威脅類別，它會嘗試以有用的程式呈現，矇騙使用者執行這些程式。

由於特洛伊木馬程式是非常廣泛的類別，所以通常會細分為許多子類別：

- **Downloader** - 可從網際網路下載其他威脅的一種惡意程式。
- **Dropper** - 可將其他類型的惡意軟體放置在受危害電腦上的一種惡意程式。
- **Backdoor** - 一種與遠端攻擊者通訊、可讓攻擊者存取系統，進而控制系統的惡意程式。
- **Keylogger** - (按鍵側錄程式) – 此程式會記錄使用者按下的每一個按鍵，並將該資訊傳送給遠端攻擊者。
- **Dialer** - 一種不連線至使用者網際網路服務提供者，而連線至高費率電話號碼的惡意程式。使用者幾乎不可能查覺到有新的連線建立。Dialer 只能對使用撥接數據機的使用者造成損害，而現在已經不常使用撥接數據機了。

如果偵測到您的電腦上有某個檔案是特洛伊木馬程式，建議您將它刪除，因為它極可能僅包含惡意程式碼。

6.1.4 Rootkit

Rootkit 是惡意程式，可讓網際網路攻擊者任意存取系統，且神不知鬼不覺。Rootkit 在存取系統之後 (通常是利用系統弱點)，會使用作業系統中的功能來躲避防毒軟體的偵測：它會隱藏處理程序、檔案及 Windows 登錄資料。因此，使用一般的測試技術幾乎不可能偵測得到。

有兩種層級的偵測可預防 Rootkit：

1. 當其嘗試存取系統時：它們仍未存在，所以沒有作用。大部分的防毒系統都能夠在此層級消滅 Rootkit (假設系統真的偵測到這些檔案被感染)。
2. 當其隱藏起來以規避一般測試時：ESET Smart Security 使用者擁有「反隱藏」技術的優勢，此技術也能夠偵測並消除作用中 Rootkit。

6.1.5 廣告程式

廣告程式是廣告支援軟體的簡稱。舉凡可顯示廣告素材的程式均屬於這個種類的軟體。廣告程式應用程式會經常在網際網路瀏覽器中自動開啟包含廣告的快顯視窗，或變更瀏覽器的首頁。廣告程式通常隨附於免費軟體程式，讓免費軟體程式建立者負擔其 (通常很有用) 應用程式的開發成本。

廣告程式本身並不危險 - 使用者僅會受到廣告的騷擾。其危險性在於廣告程式可能也會執行追蹤功能 (與間諜軟體相同)。

如果您決定使用免費軟體產品，請特別注意安裝程式。安裝程式很可能會在安裝額外廣告程式程式時通知您。您通常可以取消安裝廣告程式而只安裝程式。

不安裝廣告程式便無法安裝某些程式，或者會限制程式的功能。這表示廣告程式通常以「合法」方式存取系統，因為使用者已同意。在此情況下，為了以防萬一，若電腦上偵測到廣告程式檔案，建議您刪除該檔案，因為其中很可能包含惡意程式碼。

6.1.6 間諜程式

此類別包括會在使用者未同意/不知情的情況下，傳送私人資訊的所有應用程式。間諜程式會利用追蹤功能來傳送各種統計資料，例如：造訪過的網站清單、使用者通訊錄中的電子郵件地址，或是記錄過的按鍵清單。

間諜程式的作者會宣稱這些技術的目的是為了深入瞭解使用者的需求和興趣，使宣傳目標更為精準。問題是有益的和惡意的應用程式之間沒有明顯的分界，而且沒有人可以確保所擷取的資訊不會被濫用。間諜程式應用程式取得的資料可能包含安全密碼、PIN、銀行帳號等等。免費版程式的作者通常會將間諜程式搭載於該程式，以創造收益，或是激勵您購買軟體。通常在程式安裝期間，就會讓使用者知道間諜程式的存在，以刺激其升級為沒有間諜程式的付費版本。

例如，P2P (點對點) 網路的用戶端應用程式，就是著名的搭載間諜軟體的免費軟體產品。Spyfalcon 或 Spy Sheriff (以及許多其他程式) 是屬於特定的間諜軟體子類別 - 其看似間諜程式防護程式，但事實上，其本身就是間諜程式。

如果在電腦上偵測到檔案是間諜軟體，建議您刪除該檔案，因為其中很可能包含惡意程式碼。

6.1.7 壓縮器

壓縮器是運行時間自我解壓縮的執行檔，會將數種惡意軟體封裝成單一套件。

最常見的壓縮器有 UPX、PE_Compact、PKLite 與 ASPack。同一個惡意程式若壓縮時使用不同的壓縮器，其偵測方式也會不同。壓縮器也能夠讓其「簽章」隨著時間改變，讓惡意軟體更難以偵測與移除。

6.1.8 潛在不安全的應用程式

有很多合法程式的功能都可用來簡化網路電腦的系統管理作業。然而，如果落入有心人士的手中，可能就會被用來從事惡意活動。ESET Smart Security 提供偵測這類威脅的選項。

[潛在不安全的應用程式] 是用於商業、合法軟體的分類。此分類包括的程式諸如遠端存取工具、密碼破解應用程式，以及 keylogger (會記錄使用者按下之每個按鍵的程式)。

如果您發現電腦上有潛在不安全的應用程式存在並執行中 (而您沒有安裝它)，請洽詢您的網路系統管理員，或是移除該應用程式。

6.1.9 潛在不需要應用程式

潛在不需要應用程式是含有廣告軟體、安裝工具列或具有其他不明企圖的程式。在某些情況下，使用者可能會認為潛在不需要應用程式的優點大於風險。因此，相較於其他例如特洛伊木馬或蠕蟲惡意軟體的類型，ESET 將此類應用程式指定為低風險的類別。

警告 - 發現潛在的威脅

偵測到潛在不需要應用程式時，您可以決定要採取的處理方法：

1. **清除/中斷連線**：此選項結束動作，並且防止潛在的威脅進入系統。
2. **略過**：此選項會允許潛在威脅進入您的系統。
3. 若要讓應用程式以後在電腦上不中斷地執行，請按一下 **[進階選項]**，然後選取 **[從偵測中排除]** 旁的核取方塊。

偵測到潛在不需要應用程式且無法清除時，**[位址已被封鎖]** 通知視窗會在畫面右下角顯示。如需有關此事件的詳細資訊，請從主功能表瀏覽至 **[工具]** > **更多工具** > 從主要功能表中的 **[防護記錄檔案]** > **[過濾的網站]**。

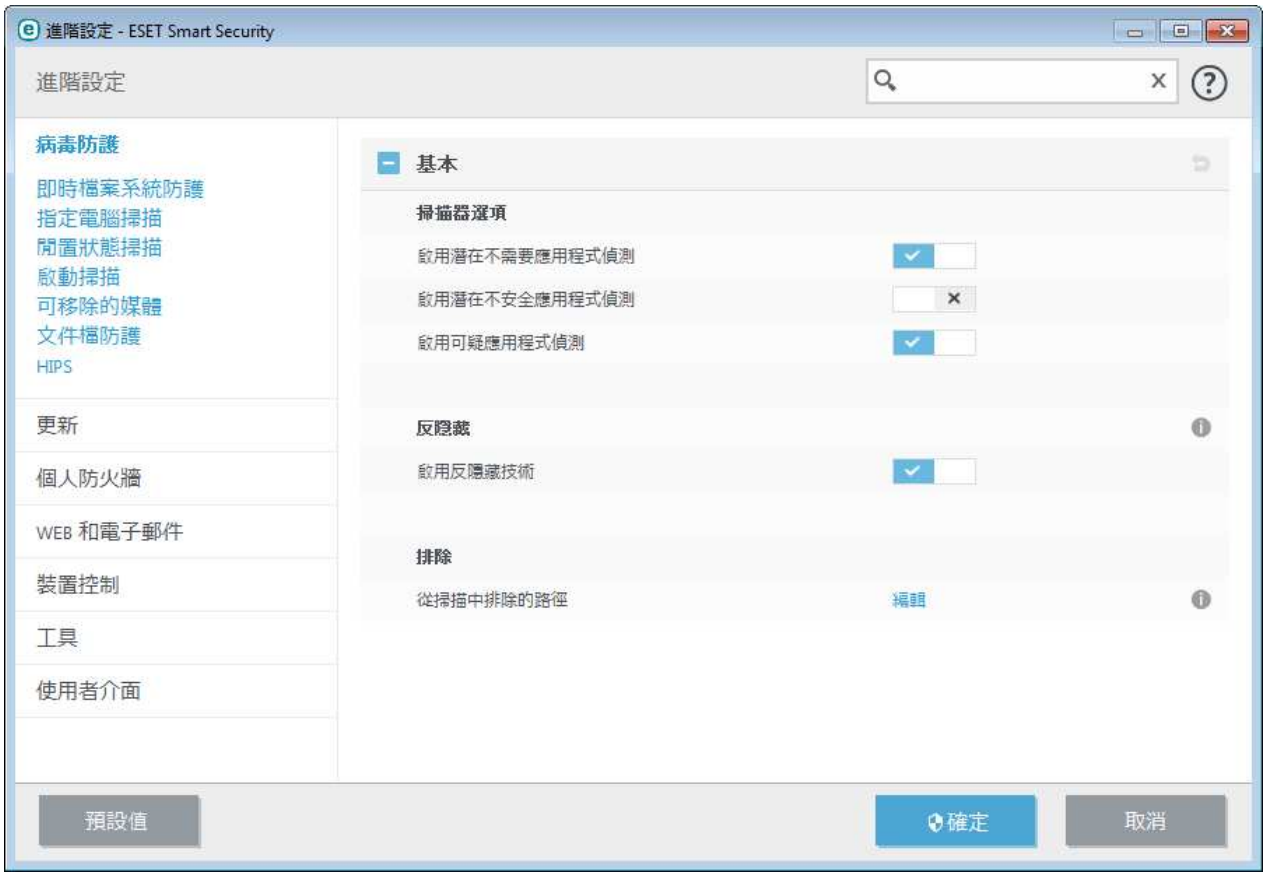
潛在不需要應用程式 - 設定

安裝您的 ESET 產品時，可以決定是否要啟用不需要應用程式的偵測，如下所示：

潛在不需要應用程式可能會安裝廣告軟體、工具列，或者具有其他不安全和不需要的程式功能。

您隨時可以在程式設定裡修改這些設定。若要啟用或停用潛在不需要、不安全或可疑應用程式的偵測，請遵循下列指示：

1. 開啟您的 ESET 產品。如何開啟我的 ESET 產品？
2. 按 **F5** 鍵以存取 **[進階設定]**。
3. 按一下 **[防毒]**，根據您的喜好啟用或停用 **[啟用潛在不需要應用程式偵測]**？**[啟用潛在不安全應用程式偵測]** 和 **[啟用可疑應用程式偵測]** 選項。按一下 **[確定]** 以確認。



潛在不需要應用程式 - 軟體包裝函式

軟體包裝函式是檔案裝載網站使用的一種特殊應用程式修改類型。其為第三方工具，會安裝您要下載的程式，但也會新增其他軟體，例如工具列或廣告軟體。這些其他軟體可能會變更您網頁瀏覽器的首頁和搜尋設定。除此之外，檔案裝載網站通常不會通知軟體廠商或接收下載的用戶其已經執行修改，且不會輕易允許取消修改。因為上述原因，ESET 將軟體包裝函式分類為一種潛在不需要應用程式，讓使用者選擇接受或不接受下載。

請參閱這份 ESET 知識庫文章以取得此說明頁面的更新版本。

6.1.10 殭屍網路

Bot (即網路機器人) 是一種自動化惡意程式，能夠掃描整個網路地址區塊，並感染防護薄弱的電腦。使駭客能夠同時掌控更多電腦，並將它們都變成 Bot (亦稱為殭屍)。駭客通常使用 Bot 感染大量的電腦，從而形成網路或殭屍網路。殭屍網路一旦進入您的電腦，駭客便能在分散式拒絕服務 (DDoS) 攻擊或 Proxy 中使用殭屍網路，也可在您不知道的情況下在網際網路上自動執行工作 (例如，傳送垃圾郵件、病毒，並竊取如銀行的授權憑證或是信用卡號碼等個人資訊)。

6.2 遠端攻擊的類型

有很多特殊的技術可讓攻擊者危害遠端系統。這些技術可分為數種類別。

6.2.1 DoS 攻擊

DoS 或「*拒絕服務*」是一種讓目標使用者無法使用電腦或網路的攻擊方式。受影響之使用者間的通訊會到受阻礙，並且無法再繼續正常運作。遭受 DoS 攻擊的電腦通常需要重新啟動，否則就無法正常運作。

在大部分的情況下，目標是 Web 伺服器，而目的是讓使用者在某段時間內無法使用它們。

6.2.2 DNS Poisoning

使用 DNS (網域名稱伺服器) Poisoning，駭客就可以欺騙所有電腦的 DNS 伺服器，讓其相信提供的假資料是合法且可信的。然後會在某段時間內快取假資訊，讓攻擊者重新寫入 IP 位址的 DNS 回應。因此，嘗試存取網際網路站台的使用者會下載電腦病毒或蠕蟲，而不會下載其原始內容。

6.2.3 蠕蟲攻擊

電腦蠕蟲是含有惡意程式碼的程式，它會攻擊主機電腦，並透過網路散佈。網路蠕蟲會利用各種應用程式中的安全性弱點。因為網際網路的可用性，它可以在其發佈的數小時內，就散佈到全世界。

使用防火牆中的預設安全性設定，或是封鎖未受保護及未使用的通訊埠，即可避免大部分的蠕蟲攻擊 (Sasser、SqlSlammer)。此外，以最新的安全修補程式來更新作業系統也很重要。

6.2.4 連接埠掃描

連接埠掃描是用來決定要在網路主機上開放的電腦連接埠。連接埠掃描器是為了尋找這類連接埠而設計的軟體。

電腦通訊埠是虛擬端點，可處理對內及對外的資料 - 就安全的觀點來看，這是很重要的。在大型網路中，連接埠掃描器所收集的資訊有助於識別潛在的弱點。這種用法是合法的。

儘管如此，連接埠掃描還是經常被駭客用來嘗試破壞安全性。第一步就是傳送封包至每一個通訊埠。依據回應類型，是可以判斷出哪些通訊埠在使用中。掃描作業本身並不會造成損害，但請注意這種活動會顯露出潛在的弱點，而讓攻擊者有機會掌控遠端電腦。

建議網路系統管理員封鎖所有未使用的通訊埠，並保護使用中的通訊埠不受未經授權的存取。

6.2.5 TCP 去同步化

TCP 去同步化是 TCP 劫持攻擊中所使用的技術。當對內封包中的序號與預期的序號不同時，就會觸發此技術。含非預期序號的封包會遭丟棄 (如果是出現在目前的通訊視窗中，則會儲存在緩衝存放區)。

在去同步化中，二邊的通訊端點都會丟棄所接收的封包，趁這個時候，遠端攻擊者就能夠入侵，並提供封包正確的序號。攻擊者甚至可以操控或修改通訊。

TCP 劫持攻擊的目的是要中斷伺服器對用戶端或點對點通訊。在每個 TCP 區段上使用驗證，可以避免許多攻擊。另外，也建議您為網路裝置使用所建議的配置。

6.2.6 SMB Relay

SMB Relay 及 SMB Relay 2 是可對遠端電腦發動攻擊的特殊程式。這二種程式會利用伺服器訊息區檔案共用通訊協定 (上至 NetBIOS 層級)。共用 LAN 中任何資料夾和目錄的使用者極可能使用此檔案共用通訊協定。

在區域網路通訊中，會交換密碼雜湊。

SMB Relay 會在 UDP 通訊埠 139 及 445 上接收連線，轉送用戶端和伺服器所交換的封包，再加以修改。連線並驗證之後，即中斷用戶端的連線。SMB Relay 會建立新的虛擬 IP 位址。使用 "net use \\192.168.1.1" 命令即可存取新位址。而任何 Windows 網路功能都可以使用該位址。SMB Relay 會轉送 SMB 通訊協定通訊，但交涉及驗證除外。用戶端電腦一經連線，遠端攻擊者即可使用該 IP 位址。

SMB Relay2 作用的原理與 SMB Relay 相同，只是它是使用 NetBIOS 名稱，而不是 IP 位址。這二種程式都會執行「中間

人」(man-in-the-middle) 攻擊。這些攻擊可讓遠端攻擊者讀取、插入及修改在二個通訊端點之間交換的郵件，而不被發現。暴露在這種攻擊下的電腦常會停止回應或突然重新啟動。

為避免這些攻擊，建議您使用驗證密碼或金鑰。

6.2.7 ICMP 攻擊

ICMP (網際網路控制訊息通訊協定) 是一種普及且廣泛使用的網際網路通訊協定。它主要由網路電腦用於傳送各種錯誤訊息。

遠端攻擊者嘗試利用 ICMP 通訊協定的弱點。ICMP 通訊協定設計用來進行不需要驗證的單向通訊。這樣可讓遠端攻擊者觸發所謂的 DoS (拒絕服務) 攻擊，或者授與未獲授權的個人對對內與對外封包的存取權。

ICMP 攻擊的典型範例是：Ping Flood、ICMP_ECHO Flood 及 Smurf 攻擊。遭受 ICMP 攻擊的電腦明顯變慢 (這適用於使用網際網路的所有應用程式)，而且連接到網際網路時會發生問題。

6.3 ESET 技術

6.3.1 惡意探索封鎖程式

惡意探索封鎖程式是設計用來強化常遭利用的應用程式類型的防護，例如 Web 瀏覽器、PDF 閱讀器、郵件用戶端和 MS Office 元件。其運作方式是監控可能是惡意探索之可疑活動的程序行為。

當惡意探索封鎖程式發現可疑程序時，就會立刻停止該程序並記錄該威脅的資料，接著將記錄傳送到 ThreatSense 雲端系統。這份資料將由 ESET 研究實驗室處理，並用來改良使所有用戶不受不明威脅和零時差威脅 (新發佈且無任何預先設定解決方法的惡意軟體) 的保護功能。

6.3.2 進階記憶體掃描器

進階記憶體掃描器可與惡意探索封鎖程式一起搭配，強化對抗惡意軟體在整個利用欺騙及/或加密時對惡意軟體防護產品所啟用偵測功能的規避動作。若在原始模擬或啟發式技術無法偵測威脅的情況下，進階記憶體掃描器可識別可疑的行動，並在威脅於系統記憶體揭露自己時進行掃描。這個解決方案甚至可以有效對抗重度欺騙的惡意軟體。

與惡意探索封鎖程式不同的是，進階記憶體掃描器是後置執行方式，意思是在其偵測到威脅時可能已有部分惡意活動已在進行；不過在其他偵測技術都已失敗的情況下，這個方法仍然算是額外的安全性層級功能。

6.3.3 弱點保護

弱點保護是一種延伸的個人防火牆，可以強化偵測網路層級的已知弱點。透過就 SMB、RPC 和 RDP 等普遍應用的通訊協定中存在的常見弱點偵測功能，這項功能打造出另一層重要保護，以便對抗到處都在但修補程式尚未發佈或部署的惡意軟體、網路主導攻擊和弱點利用。

6.3.4 ThreatSense

以 ThreatSense.Net® 進階的預早警告系統為基礎，ESET LiveGrid® 會使用全球 ESET 使用者提交的資訊，並將其傳送到 ESET 研究實驗室。透過全球提供可疑樣本和中繼資料的方式，ESET LiveGrid® 可讓我們立即回應客戶需求，並讓 ESET 隨時掌握最新威脅情報。ESET 惡意程式研究人員會使用這些資訊來建立全球威脅性質與範圍的精確快照，有利於我們鎖定正確的目標。ESET LiveGrid® 資料是我們設定自動處理優先順序時的重要關鍵。

此外還能建立聲譽系統，協助改善惡意軟體防護解決方案的整體效能。當使用者系統檢查出可執行檔或壓縮檔時，其雜湊標籤會先與白名單與黑名單項目的資料庫進行比對。若可在白名單中找到該檔案，則被檢查的檔案會判定為乾淨無毒，並且標記排除在日後掃描的清單內。如果是在黑名單中找到該檔案，則系統會根據威脅的性質採取適當的行動。如果都沒有找到該檔案，則將對該檔案徹底掃描。系統會根據這次掃描的結果，將檔案歸類為威脅或非威脅。這種方法對於掃描效能有顯著的正面影響。

這個聲譽系統能有效的偵測惡意軟體樣本，甚至在其病毒透過更新的病毒資料庫進入用戶電腦之前就偵測出來 (這種情況一天可能發生好幾次)。

6.3.5 殭屍網路防護

殭屍網路防護能透過分析其網路通訊協定而發現惡意程式。與最近幾年未變更的網路通訊協定不同，殭屍網路惡意程式經常在變更。此項新技術協助 ESET 打敗嘗試躲避偵測以及嘗試將您的電腦連結至殭屍網路的惡意程式。

6.3.6 Java 惡意探索封鎖程式

Java 惡意探索封鎖程式是現有惡意探索封鎖程式防護的延伸。其監視 Java 並且尋找類似利用的行為。可以報告封鎖的範例給惡意程式分析師，以便他們建立簽章，從而在不同的層級封鎖惡意程式。

6.3.7 銀行和付款防護

銀行和付款防護代表針對線上交易提供額外一層防護，因為您未受保護的瀏覽器可能會在交易期間受到危害。

ESET Smart Security 包含內建的預先定義網站清單，觸發時將開啟受保護瀏覽器。您可在產品配置中新增網站或編輯網站清單。

執行受保護的瀏覽必須使用 HTTPS 加密通訊。為使用安全瀏覽，您的網際網路瀏覽器應符合下列最低需求。我們建議您在結束線上交易或付款後關閉受保護的瀏覽器。

您必須使用下方顯示的瀏覽器版本號或更新版本才可使用受保護瀏覽：

- Mozilla Firefox 24
- Internet Explorer 8
- Google Chrome 30

6.4 電子郵件

電子郵件是一種具有很多優點的現代通訊形式。電子郵件使用靈活、快速且直接，在 1990 年代初期對於網際網路的擴展扮演關鍵角色。

很遺憾，由於具有高度的匿名性，電子郵件及網際網路也為垃圾郵件之類的非法活動有機可趁。垃圾郵件包括來路不明的廣告、惡作劇以及擴散具惡意的軟體 (即惡意軟體)。傳送垃圾郵件幾乎無需成本的事實會增加您的不便及危險，且垃圾郵件作者擁有許多工具及來源取得新的電子郵件地址。此外，垃圾郵件的數量及多樣性也造成管理上的困難。您使用電子郵件地址的時間越長，其最後變成垃圾郵件引擎資料庫的可能性就越高。預防的某些提示：

- 可能的話，請勿在網際網路上發佈您的電子郵件地址
- 僅將您的電子郵件地址提供給信任的個人
- 可能的話，請勿使用一般別名，因為別名越複雜，追蹤的可能性越低
- 請勿回覆已到達收件匣中的垃圾郵件
- 填寫網際網路表單時請小心，並特別注意「是，我想要接收資訊」之類的選項。
- 請使用「專門的」電子郵件地址，例如，一個地址用於工作，另一個地址用於與您的朋友通訊等等。
- 時常變更您的電子郵件地址
- 使用垃圾郵件防護解決方案

6.4.1 廣告

網際網路廣告是增長最為迅速的廣告形式之一。其主要的行銷優勢在於幾乎不需成本和高直接性；而且，訊息幾乎是立即傳遞的。許多公司都使用電子郵件行銷工具來與目前及未來的客戶進行有效的溝通。

由於使用者可能願意接收某些產品的商業資訊，所以這類廣告是合法的。不過，許多公司會傳送來路不明的大量商業訊息。在這種情況下，電子郵件廣告就會變成垃圾郵件。

大量來路不明的電子郵件已成為問題，因為其並無減緩的跡象。來路不明電子郵件的作者會嘗試將垃圾郵件偽裝成合法郵件。

6.4.2 惡作劇

惡作劇是透過網際網路擴散的一種錯誤資訊。惡作劇通常會透過電子郵件或諸如 ICQ 和 Skype 等通訊工具傳送。通常訊息本身是惡作劇或「街頭傳奇」。

「電腦病毒」惡作劇會嘗試在收件者中產生恐懼、不確定及懷疑 (FUD)，讓他們相信存在「無法偵測的病毒」正在刪除檔案並擷取密碼，或者在其電腦上執行部分其他有害活動。

某些惡作劇在運作時會要求收件者將郵件轉寄給連絡人，這會使惡作劇循環不息。包括行動電話惡作劇、尋求協助、有人從海外向您提供金錢等。通常無法判斷建立者的意圖。

若您看到一則訊息提示傳遞給您認識的每個人，則此訊息很可能是惡作劇。網際網路上有許多網站可驗證電子郵件是否合法。轉寄之前，請對您懷疑是惡作劇的訊息執行網際網路搜尋。

6.4.3 網路釣魚

網路釣魚這個詞彙是用來定義利用社交工程技巧 (操縱使用者以取得機密資訊) 的犯罪活動。其目的是要存取像是銀行帳號、PIN 碼等敏感資料。

攻擊者通常會假冒成值得信賴的個人或企業 (金融機構、保險公司) 來傳送電子郵件，以進行存取。該電子郵件看起來非常逼真，而且會包含源自其模仿對象的圖片及內容。它會以各種藉口 (資料驗證、金融作業) 要求您輸入您的個人資料，即銀行帳號或使用者名稱及密碼。這類資料一經提交，就很容易被竊取及濫用。

銀行、保險公司及其他合法公司絕不會以來路不明的電子郵件，主動要求使用者名稱和密碼。

6.4.4 識別垃圾郵件詐騙

一般而言，有幾個指標可協助您識別信箱中的垃圾郵件 (來路不明的電子郵件)。如果郵件至少滿足下列某些條件，則它極可能是垃圾郵件。

- 寄件者地址不屬於連絡人清單中的某人。
- 向您提供一大筆金錢，但是您必須先提供少數金額。
- 以各種藉口 (資料驗證、金融作業) 要求您輸入某些個人資料：銀行帳戶號碼、使用者名稱及密碼等。
- 以外文撰寫。
- 要求您購買不感興趣的產品。如果您仍然決定購買，請驗證郵件寄件者是可靠的廠商 (洽詢原始產品製造商)。
- 拼錯某些單字，以嘗試欺騙您的垃圾郵件過濾器。例如 vaigra 而不是 viagra 等。

6.4.4.1 規則

在垃圾郵件防護解決方案及電子郵件用戶端的內容中，規則是用來操作電子郵件功能的工具。其分為二個邏輯部分：

1. 條件 (例如，從特定地址對內的郵件)
2. 處理方法 (例如，刪除郵件、將郵件移至指定的資料夾)

規則的數量及組合會依垃圾郵件防護解決方案而有所不同。這些規則是做為對付垃圾郵件 (來路不明的電子郵件) 的措施。典型範例：

- 1. 條件：對內的電子郵件中包含通常會在垃圾郵件中看到的某些字眼
  2. 處理方法：刪除郵件
- 1. 條件：對內的電子郵件中包含副檔名為 .exe 的附件
  2. 處理方法：刪除附件，並傳送郵件至信箱
- 1. 條件：傳入的電子郵件是來自您的雇主
  2. 處理方法：將郵件移至 [工作] 資料夾

建議您使用反垃圾郵件程式中的規則組合，以方便系統管理，並提升過濾垃圾郵件 (來路不明的電子郵件) 的效率。

6.4.4.2 白名單

一般而言，白名單是被接受或被授與權限的項目或人員清單。「電子郵件白名單」這個詞是定義使用者想要接受之郵件寄件者的清單。這種白名單的依據是在電子郵件地址、網域名稱或 IP 位址中搜尋到的關鍵字。

如果白名單是以「排外模式」執行，則不會接收來自任何其他地址、網域或 IP 位址的郵件。如果白名單並非排外模式，則不會刪除這類郵件，但會以其他方式進行過濾。

白名單所依據的原則與黑名單相反。與黑名單相較，白名單相對較容易維護。建議您並用「白名單」與「黑名單」，以提升過濾垃圾郵件的效率。

6.4.4.3 黑名單

通常，黑名單是無法接受或遭到禁止之項目或人員的清單。在虛擬世界中，該技術可讓使用者接受所有來自此清單外之使用者的郵件。

有兩種類型的黑名單：由使用者透過垃圾郵件防護應用程式建立的黑名單，以及由特定的專門機構建立，可在網際網路上找到的定期更新黑名單。

您必須使用黑名單才能順利封鎖垃圾郵件，但由於每天都有要封鎖的新項目出現，因此難以進行維護。建議您同時使用白名單與黑名單，以發揮最大垃圾郵件過濾效率。

6.4.4.4 例外清單

例外清單通常包含可能受詐騙而被用來傳送垃圾郵件的電子郵件地址。針對例外清單中寄件者地址發出的電子郵件訊息，系統會一律掃描看是否為垃圾郵件。 依預設，例外清單預設包含所有現有電子郵件用戶端帳戶中的電子郵件地址。

6.4.4.5 伺服器端控制

伺服器端控制是一種可利用已接收的郵件數目及使用者反應為基礎，來識別大量垃圾郵件的技術。根據郵件的內容，每封郵件都會留下唯一的數位「蹤跡」。唯一的 ID 編號並不會透露電子郵件的內容為何。兩封完全相同的郵件將會有完全相同的蹤跡，而不同的郵件會有不同的蹤跡。

如果將郵件標記為垃圾郵件，則其蹤跡會傳送至伺服器。如果伺服器接收到更多相同的蹤跡 (對應於某個垃圾郵件)，該蹤跡會儲存在垃圾郵件蹤跡資料庫中。掃描對內的郵件時，程式會將郵件的蹤跡傳送至伺服器。對於經使用者標記為垃圾郵件的郵件，伺服器會傳回與其對應的蹤跡相關的資訊。

7. 常見問題

本章涵蓋的是一些使用者最常詢問的問題以及最常遇到的問題。按一下主題標題，以瞭解如何解決您的問題：

如何更新 ESET Smart Security
如何從我的 PC 移除病毒
如何允許特定應用程式的通訊
如何啟用帳戶的家長控制
如何在排程器中建立新的工作
如何排程掃描工作 (每隔 24 小時)

如果您的問題不在以上說明頁面清單中，請嘗試搜尋 ESET Smart Security 說明頁面。

如果您在「說明頁面」內找不到問題的解決辦法，可以造訪我們定期更新的線上 ESET 知識庫。以下最常用的知識庫文章連結可協助您解決一些常見問題：

我在安裝 ESET 產品時收到啟動錯誤訊息。這代表什麼意思？
如何在 ESET Smart Security/ESET NOD32 Antivirus 中輸入我的使用者名稱和密碼？
我收到 ESET 安裝已提前結束的訊息
在更新授權之後我還需要做些什麼？(家用使用者)
如果我變更電子郵件地址時該怎麼辦？
如何以安全模式或包含網路功能的安全模式啟動 Windows

必要時，您可以將您的問題告知我們的客戶服務。您可以在 ESET Smart Security **[說明及支援]** 索引標籤中找到連絡人表單。

7.1 如何更新 ESET Smart Security

您可以手動也可以自動執行 ESET Smart Security 更新。若要觸發更新，請按一下 **[更新]** 區段中的 **[立即更新]**。

預設安裝設定會建立每小時執行的自動更新工作。如果需要變更間隔，請瀏覽至 **[工具]** > **[排程器]** (如需「排程器」的相關資訊，請按一下這裡)。

7.2 如何從我的 PC 移除病毒

如果您的電腦正在顯示惡意程式感染的信號 (例如，速度更慢、頻繁凍結)，我們建議您執行下列各項：

1. 在主要程式視窗中，按一下 **[電腦掃描]**。
2. 按一下 **[掃描您的電腦]**，開始掃描系統。
3. 完成掃描之後，請檢閱已掃描、受感染及已清除的檔案防護記錄。
4. 如果您想要僅掃描磁碟的某一部分，請按一下 **[自訂掃描]**，並選取要進行病毒掃描的目標。

如需其他資訊，請參閱我們定期更新的ESET 知識庫文章。

7.3 如何允許特定應用程式的通訊

如果互動模式中偵測到新連線，且沒有相符規則，則會提示您允許或拒絕連線。如果您要 ESET Smart Security 每次應用程式嘗試建立連線時都執行相同的處理方法，請選取 **[儲存處理方法 (建立規則)]** 核取方塊。

您可以在 **[網路]** > **[個人防火牆]** > **[規則及區域]** > **[設定]** 的 [個人防火牆設定] 視窗中，為應用程式建立新的個人防火牆規則，ESET Smart Security 才會偵測這些規則。若要在 **[規則及區域設定]** 中使用 **[規則]** 索引標籤，個人防火牆過濾模式必須設為互動模式。

在 **[一般]** 索引標籤中輸入規則的名稱、方向及通訊協定。視窗可讓您定義規則適用時要採取的處理方法。

在 **[本機]** 索引標籤中輸入應用程式可執行檔的路徑及本機通訊連接埠。按一下 **[遠端]** 索引標籤，以輸入遠端位置及連接埠 (如果適用的話)。一旦應用程式再次嘗試通訊，就會套用新建立的規則。

7.4 如何啟用帳戶的家長控制

若要啟動特定使用者帳戶的家長控制，請遵循以下步驟：

1. 依預設，ESET Smart Security 中的家長控制為停用。有兩種方式可以啟用家長控制：
   - 從主要程式視窗中，按一下 **[設定]** > **[安全性工具]** > **[家長控制]** 中的  ，並將家長控制狀態變更為已啟用。
   - 按下 F5 以存取 **[進階設定]** 樹狀目錄，瀏覽至 **[Web 和電子郵件]** > **[家長控制]**，接著選取 **[整合至系統]** 旁邊的切換。
2. 按一下主要程式視窗中的 **[設定]** > **[安全性工具]** > **[家長控制]**。即使 **[啟用]** 已顯示於 **[家長控制]** 旁，您仍需按一下 **[保護此帳戶]**，為所需的帳戶建立新的家長控制角色。在帳戶設定視窗中輸入年齡以決定存取層級與適合年齡的建議網頁。現在指定帳戶的家長控制為啟用。按一下帳戶名稱下的 **[允許和禁止的內容...]**，即可在類別索引標籤中自訂您要允許或封鎖的類別。若要允許或封鎖不符合類別的自訂網頁，請按一下 [例外] 索引標籤。

7.5 如何在排程器中建立新的工作

若要在 **[工具]** > **[排程器]** 中建立新工作，請按一下 **[新增]**，或按一下滑鼠右鍵並從內容功能表中選取 **[新增...]**。有五種類型的排程工作可用：

- **執行外部應用程式** - 排程以執行外部應用程式。
- **防護記錄維護** - 防護記錄檔案還包括已刪除記錄的剩餘部分。此工作會定期最佳化防護記錄檔案中的記錄，以有效運作。
- **系統啟動檔案檢查** - 檢查系統啟動或登入時允許執行的檔案。
- **建立電腦狀態快照** - 建立 ESET SysInspector 電腦快照 - 收集關於系統元件 (例如驅動程式、應用程式) 的詳細資訊，並評估各個元件的風險層級。
- **指定電腦掃描** - 針對電腦中的檔案及資料夾執行掃描。
- **先掃描** - 依預設，在安裝後 20 分鐘或電腦重新開機時將執行掃描以進行低優先順序工作。
- **更新** - 更新病毒資料庫與程式模組來排程更新工作。

由於 **[更新]** 是其中一個最常用的排程工作，因此我們將在下面解釋如何新增更新工作：

從 **[已排程的工作]** 下拉式功能表中，選取 **[更新]**。在 **[工作名稱]** 欄位中輸入工作的名稱，接著按一下 **[下一步]**。選取工作的頻率。可用選項如下：**[一次]**？**[重複]**？**[每日]**？**[每星期]** 與 **[事件觸發]**。選取 **[使用電池執行時略過工作]** 以在膝上型電腦使用電池執行時，將系統資源消耗降到最低。工作會在 **[工作執行]** 欄位中的指定日期和時間執行。接著，若排程期間無法執行或完成工作時，請定義要採取的處理方法。可用選項如下：

- **於下次排程的時間**
- **盡快(A)**
- **如果距離上次執行的時間超過指定值，則立即執行工作** (可以使用**[自上次執行後經過的時間]** 捲動方塊定義間隔)

在下一步中，會顯示目前已排程工作資訊的摘要視窗。完成變更之後，按一下 **[完成]**。

隨即顯示對話方塊視窗，可讓您選取用於排程工作的設定檔。在這裡，您可以設定主要設定檔及替代設定檔。如果使用主要設定檔無法完成工作時將會使用替代設定檔。按一下 **[完成]** 進行確認，即可將排程工作新增至目前排程工作清單。

7.6 如何安排每週電腦掃描

若要排程定期工作，請開啟主要程式視窗並按一下 **[工具]** > **[排程器]**。以下是關於如何排程工作的簡短手冊，而此工作將會每隔 24 小時掃描一次本機磁碟。如需詳細指示，請參閱我們的知識庫文章。

若要排程掃描工作：

1. 在主要的 [排程器] 畫面中按一下 **[新增]**。
2. 從下拉式功能表中選取 **[指定電腦掃描]**。
3. 輸入工作的名稱並針對工作頻率選取 **[每星期]**。
4. 設定執行工作的日期及時間。
5. 若已安排的工作因故無法執行 (例如電腦已關機)，請選取 **[盡快執行工作]** 以稍後執行工作。
6. 檢閱已排程工作的摘要，並按一下 **[完成]**。
7. 從 **[目標]** 下拉式功能表中，選取 **[本機磁碟]**。
8. 按一下 **[完成]** 以套用工作。