

# ESET ENDPOINT ANTIVIRUS

## 使用者手冊

Microsoft R Windows R 8 / 7 / Vista / XP / 2000 / Home Server / NT4 (SP6)

[按一下這裡以下載此文件的最新版本。](#)



## ESET ENDPOINT ANTIVIRUS

**Copyright c2013 by ESET, spol. s r. o.**

ESET Endpoint Antivirus 是由 ESET, spol. s r. o. 開發的產品

如需相關資料，請造訪 [www.eset.com](http://www.eset.com)。

保留所有權利。本文件的任何部分在未獲得作者的書面同意下，不得以任何形式或利用任何方式進行重製、儲存在可擷取的系統或進行傳輸，包括電子、機械、影印、錄音或掃描等方式。

ESET, spol. s r. o. 保留變更所述應用程式軟體的權利，恕不另行通知。

全球客戶支援：[www.eset.com/support](http://www.eset.com/support)

修訂：20. 2. 2013

# 內容

<b>1. ESET Endpoint Antivirus</b>	<b>5</b>
1.1 系統需求	5
1.2 預防	5
<b>2. 安裝</b>	<b>7</b>
2.1 一般安裝	8
2.2 自訂安裝	10
2.3 輸入使用者名稱和密碼	13
2.4 升級至最新版本	13
2.5 電腦掃描	14
<b>3. 初學者手冊</b>	<b>15</b>
3.1 介紹使用者介面設計	15
3.2 如果程式運作不正常怎麼辦	16
3.3 更新設定	17
3.4 Proxy 伺服器設定	18
3.5 設定防護	19
<b>4. 使用 ESET Endpoint Antivirus</b>	<b>20</b>
4.1 電腦	21
4.1.1 病毒及間諜程式防護	22
4.1.1.1 即時檔案系統防護	22
4.1.1.1.1 要掃描的媒體	22
4.1.1.1.2 執行掃描的時機 (事件觸發的掃描)	23
4.1.1.1.3 進階掃描選項	23
4.1.1.1.4 清除層級	23
4.1.1.1.5 何時修改即時防護配置	24
4.1.1.1.6 檢查即時防護	24
4.1.1.1.7 即時防護無法運作時怎麼辦	24
4.1.1.2 文件防護	25
4.1.1.3 電腦掃描	25
4.1.1.3.1 掃描類型	26
4.1.1.3.1.1 智慧型掃描	26
4.1.1.3.1.2 自訂掃描	26
4.1.1.3.2 掃描目標	26
4.1.1.3.3 掃描設定檔	27
4.1.1.3.4 掃描進度	27
4.1.1.4 啟動掃描	28
4.1.1.4.1 自動啟動檔案檢查	28
4.1.1.5 依路徑排除	29
4.1.1.6 ThreatSense 引擎參數設定	30
4.1.1.6.1 物件	30
4.1.1.6.2 選項	30
4.1.1.6.3 清除	31
4.1.1.6.4 副檔名	31
4.1.1.6.5 限制	32
4.1.1.6.6 其他	32
4.1.1.7 偵測到入侵	32
4.1.2 可移除的媒體	34
4.1.3 裝置控制	34
4.1.3.1 裝置控制規則	35
4.1.3.2 新增裝置控制規則	36
4.1.4 主機入侵預防系統 (HIPS)	37
4.2 Web 和電子郵件	39
4.2.1 Web 存取防護	40
4.2.1.1 HTTP、HTTPS	40
4.2.1.1.1 Web 瀏覽器的主動模式	41
4.2.1.2 URL 位址管理	41
4.2.2 電子郵件用戶端防護	42
4.2.2.1 POP3、POP3S 過濾器	43
4.2.2.2 IMAP、IMAPS 通訊協定控制項	43
4.2.2.3 與電子郵件用戶端整合	44
4.2.2.3.1 電子郵件用戶端防護配置	45
4.2.2.4 移除入侵	45
4.2.3 通訊協定過濾	45
4.2.3.1 Web 和電子郵件用戶端	45
4.2.3.2 排除的應用程式	46
4.2.3.3 排除的 IP 位址	46
4.2.3.3.1 新增 IPv4 位址	47
4.2.3.3.2 新增 IPv6 位址	47
4.2.3.4 SSL 通訊協定檢查	47
4.2.3.4.1 憑證	47
4.2.3.4.1.1 信任的憑證	48
4.2.3.4.1.2 排除的憑證	48
4.2.3.4.1.3 加密的 SSL 通訊	48
4.3 更新程式	49
4.3.1 更新設定	51
4.3.1.1 更新設定檔	52
4.3.1.2 進階更新設定	52
4.3.1.2.1 更新模式	52
4.3.1.2.2 Proxy 伺服器	53
4.3.1.2.3 連線至區域網路 (LAN)	53
4.3.1.2.4 建立更新副本 - 映像	54
4.3.1.2.4.1 從映像更新	55
4.3.1.2.4.2 疑難排解映像更新問題	56
4.3.1.3 更新還原	56
4.3.2 如何建立更新工作	57
4.4 工具	58
4.4.1 防護記錄檔案	59
4.4.1.1 防護記錄維護	60
4.4.2 排程器	61
4.4.2.1 建立新工作	63
4.4.3 防護統計	64
4.4.4 即時監控	65
4.4.5 ESET SysInspector	65
4.4.6 ESET Live Grid	66
4.4.6.1 可疑檔案	66
4.4.7 執行中的處理程序	67
4.4.8 隔離區	68
4.4.9 提交檔案以供分析	69
4.4.10 警告及通知	70
4.4.10.1 訊息格式	71
4.4.11 系統更新	71
4.4.12 診斷	71
4.4.13 授權	72
4.4.14 遠端管理	73
4.5 使用者介面	74
4.5.1 圖形	74
4.5.2 警告及通知	75
4.5.2.1 進階設定	75
4.5.3 隱藏通知視窗	76
4.5.4 存取設定	76
4.5.5 程式功能表	77
4.5.6 內容功能表	78
4.5.7 簡報模式	78
<b>5. 進階使用者</b>	<b>79</b>

<b>5.1</b>	<b>Proxy 伺服器設定</b>	<b>79</b>
<b>5.2</b>	<b>匯入及匯出設定</b>	<b>79</b>
<b>5.3</b>	<b>鍵盤快捷鍵</b>	<b>80</b>
<b>5.4</b>	<b>命令列</b>	<b>80</b>
<b>5.5</b>	<b>ESET SysInspector</b>	<b>82</b>
5.5.1	ESET SysInspector 簡介	82
5.5.1.1	啟動 ESET SysInspector	82
5.5.2	使用者介面和應用程式使用	82
5.5.2.1	程式控制項	83
5.5.2.2	在 ESET SysInspector 中瀏覽	84
5.5.2.2.1	鍵盤快捷鍵	85
5.5.2.3	比較	86
5.5.3	命令列參數	87
5.5.4	服務腳本	88
5.5.4.1	產生服務腳本	88
5.5.4.2	服務腳本的結構	88
5.5.4.3	執行服務腳本	90
5.5.5	常見問題	91
5.5.6	ESET SysInspector 是 ESET Endpoint Antivirus 的一部份	92
<b>5.6</b>	<b>ESET SysRescue</b>	<b>92</b>
5.6.1	最低需求	92
5.6.2	如何建立救援 CD	93
5.6.3	目標選擇	93
5.6.4	設定	93
5.6.4.1	資料夾	93
5.6.4.2	ESET Antivirus	94
5.6.4.3	進階設定	94
5.6.4.4	網際網路通訊協定	94
5.6.4.5	開機 USB 裝置	94
5.6.4.6	燒錄	95
5.6.5	使用 ESET SysRescue	95
5.6.5.1	使用 ESET SysRescue	95
<b>6.</b>	<b>字彙</b>	<b>96</b>
<b>6.1</b>	<b>入侵類型</b>	<b>96</b>
6.1.1	病毒	96
6.1.2	蠕蟲	96
6.1.3	特洛伊木馬程式	96
6.1.4	Rootkit	97
6.1.5	廣告程式	97
6.1.6	間諜程式	97
6.1.7	潛在不安全的應用程式	97
6.1.8	潛在不需要應用程式	98
<b>6.2</b>	<b>電子郵件</b>	<b>98</b>
6.2.1	廣告	98
6.2.2	惡作劇	98
6.2.3	網路釣魚	99
6.2.4	識別垃圾郵件詐騙	99

# 1. ESET Endpoint Antivirus

ESET Endpoint Antivirus 代表確實整合電腦安全性的新方法。最新版的 ThreatSense R 掃描引擎增進了速度及精確度，藉以維護您電腦的安全。其成品就是能夠持續監控危害您電腦的攻擊及惡意軟體的智慧型系統。

ESET Endpoint Antivirus 是完整的安全性解決方案，可視為我們長期以來結合最大防護與最低系統使用量的成果。這種奠基於人工智慧的進階技術，能夠主動消除病毒、間諜軟體、特洛伊木馬、蠕蟲、廣告軟體、rootkit 及其他網際網路型攻擊的入侵，而且不會妨礙系統效能或中斷電腦運作。

ESET Endpoint Antivirus 主要設計用於小型企業環境的工作站上。這可用於 ESET Remote Administrator 連線，讓您輕鬆管理任意數目的用戶端工作站、套用原則與規則、監視偵測，並從任何網路電腦遠端配置。

## 1.1 系統需求

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

Microsoft® Windows® 2000, XP, NT4 (SP6)

400 MHz 32 位元 (x86) / 64 位元 (x64)

128MB 的系統記憶體 (RAM)

320 MB 的可用空間

Super VGA (800 x 600)

Microsoft® Windows® 8, 7, Vista, Home Server

1 GHz 32 位元 (x86) / 64 位元 (x64)

512MB 的系統記憶體 (RAM)

320 MB 的可用空間

Super VGA (800 x 600)

## 1.2 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，正確地使用防毒系統並遵守數項有用的規則是很重要的。

### 定期更新

根據 ESET Live Grid 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 病毒實驗室的專家每天都會分析那些威脅，準備並發佈更新，以不斷提高防毒程式使用者的防護層級。設定錯誤的更新會降低程式的效力。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

惡意軟體的作者特別喜歡利用各種系統弱點來增加散播惡意程式碼的效力。這就是為什麼軟體公司會密切注意其應用程式是否出現新的弱點，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。這類應用程式的範例包括視窗作業系統，或是廣泛使用的網際網路瀏覽器 Internet Explorer。

### 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，以及重要資料嚴重損毀。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，這些預防措施可讓您更容易且更快復原資料。

### 定期掃描電腦中的病毒

透過適當的設定來定期自動掃描電腦，可移除因為舊病毒碼更新而遺漏的入侵活動。

## 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電腦上的入侵活動。某些有用的規則如下：

- 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

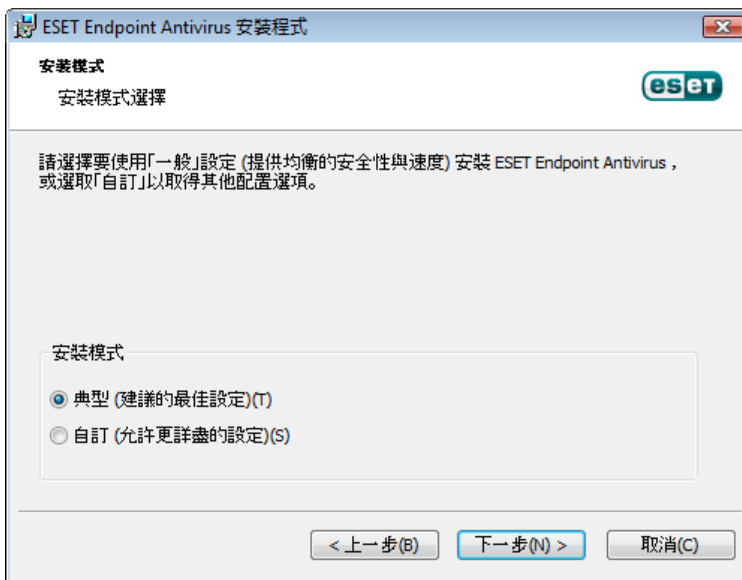
一旦啟動安裝程式，安裝精靈將引導您進行設定程序。

**重要：** 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[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)。

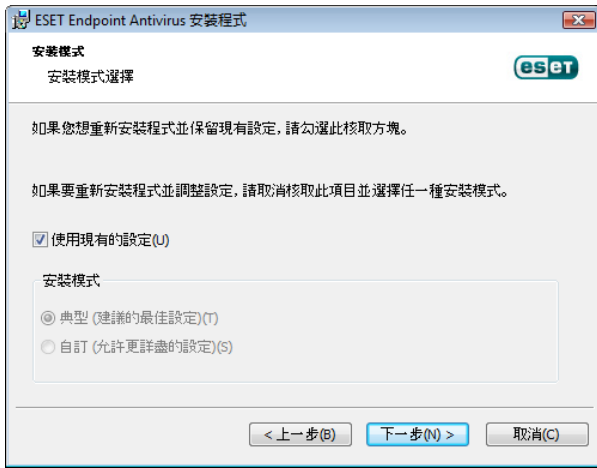


首先，程式會檢查是否有 ESET Endpoint Antivirus 的新版本可使用。如果找到更新版本，則會在安裝程序的第一個步驟通知您。如果您選取 [下載並安裝新版本] 選項，則系統會下載新版本，並且繼續安裝。下一個步驟便會顯示「使用者授權合約」。請閱讀並按一下 [接受] 以認知您已接受使用者授權合約。接受後，系統將以下列兩種可能情況繼續安裝：

1. 如果您首次在電腦上安裝 ESET Endpoint Antivirus，在您接受 [最終用戶許可協議] 後，將會看到下列視窗。您在這裡可以選擇要執行 [一般安裝](#) 還是 [自訂安裝](#)，並且根據您的選擇繼續安裝。



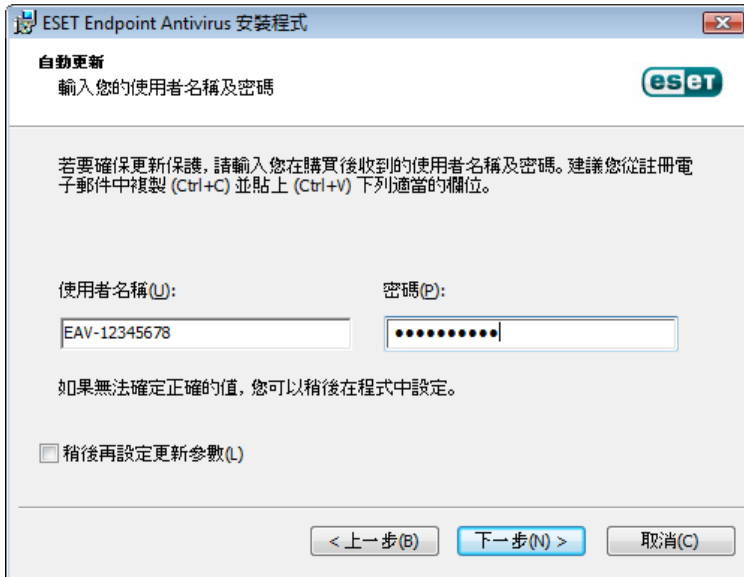
2. 如果您正透過此軟體的舊版本安裝 ESET Endpoint Antivirus，則下列視窗可讓您選擇為新安裝使用現有的程式設定，如果取消選取 [使用現有的設定] 選項，則從上述兩種安裝模式擇一使用。



## 2.1 一般安裝

一般安裝模式提供適用於大多數使用者的配置選項。這些設定提供絕佳的安全性、輕鬆的設定以及高系統效能。一般安裝模式是預設選項，如果您沒有特定設定的特殊需求，建議使用此選項。

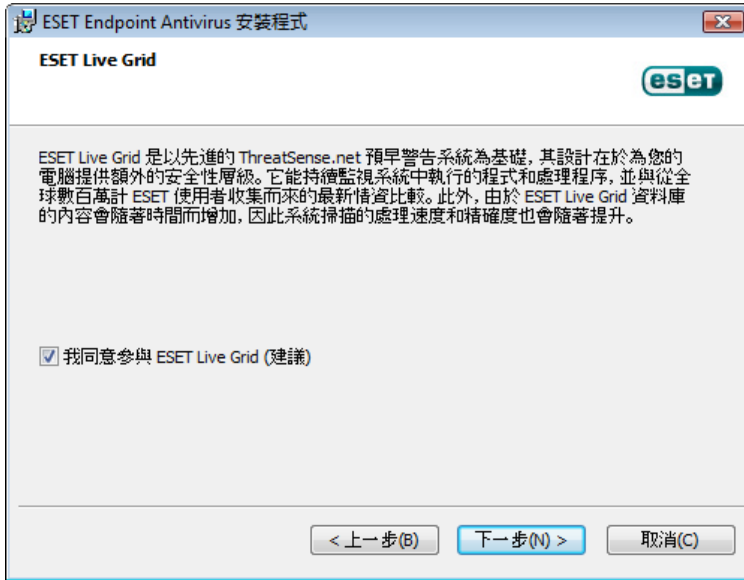
選取安裝模式並且按一下【下一步】後，程式將提示您輸入使用者名稱和密碼，以自動更新程式。這樣可為系統提供持續防護，是非常重要的步驟。



將【使用者名稱】及【密碼】(如購買或註冊產品後收到的驗證資料) 輸入到對應的欄位中。如果您目前沒有可用的使用者名稱與密碼，請按一下【稍後再設定更新參數】核取方塊。稍後程式會自行輸入您的使用者名稱與密碼。

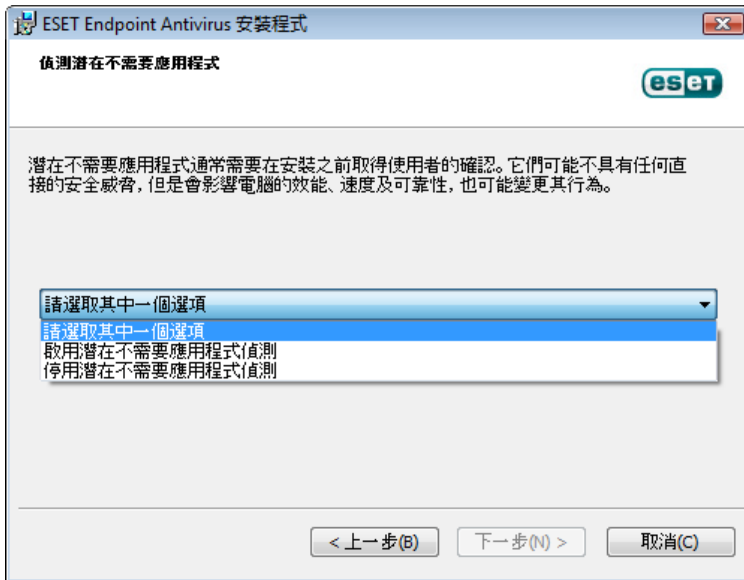
下一步是配置 ESET Live Grid。ESET Live Grid 有助於確保迅速持續通知 ESET 新入侵的相關資訊，以保護其客戶。此系統允許您將新威脅提交到 ESET 病毒實驗室，並對其進行分析、處理及新增到病毒資料庫。



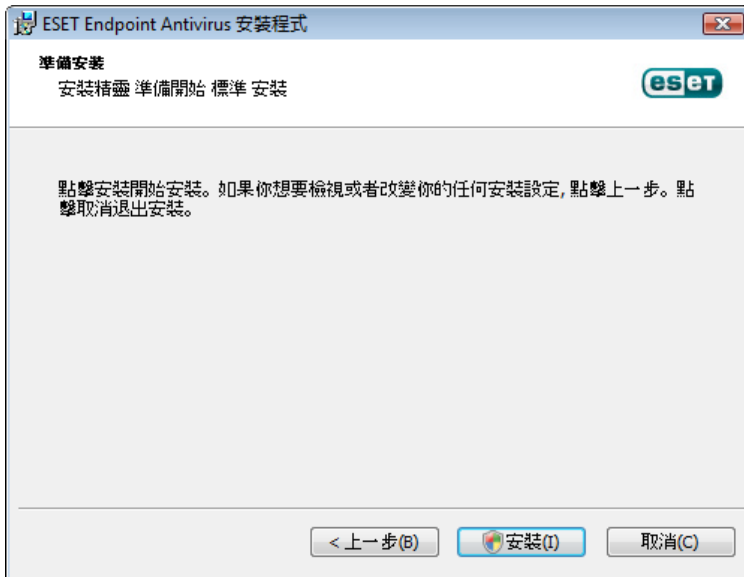


依預設，[我同意參與 ESET Live Grid] 選項會選取，這將啟動此功能。

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，但是可能會經常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。



一般安裝模式中的最後一個步驟是按一下 [安裝] 按鈕以確認安裝。



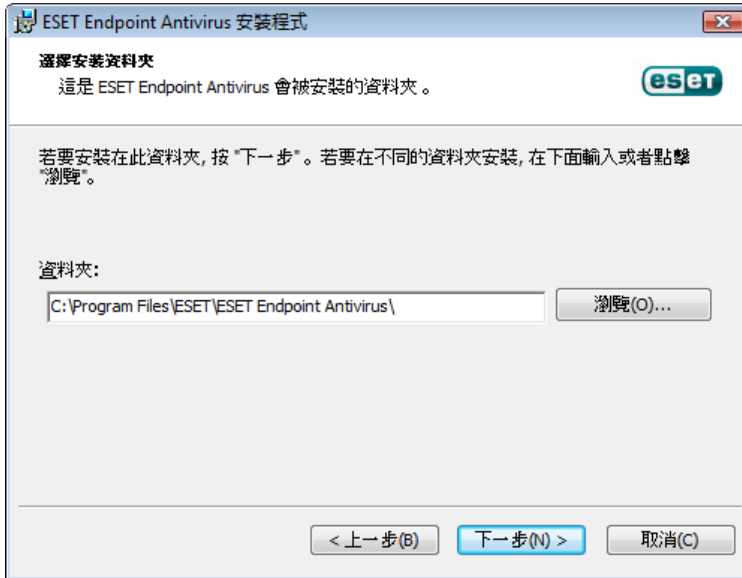
## 2.2 自訂安裝

自訂安裝模式是為具有精確調整經驗及想要在安裝期間修改進階設定的使用者而設計。

選取此安裝模式並且按 [下一步] 後，程式將提示您選取安裝的目標位置。依預設，程式會安裝至以下目錄：

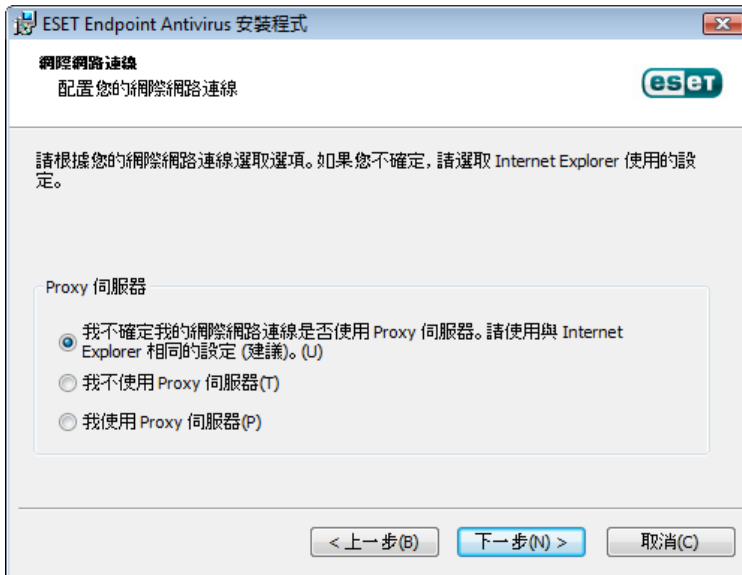
C:\Program Files\ESET\ESET Endpoint Antivirus\

按一下 [瀏覽...] 變更此位置 (不建議)。

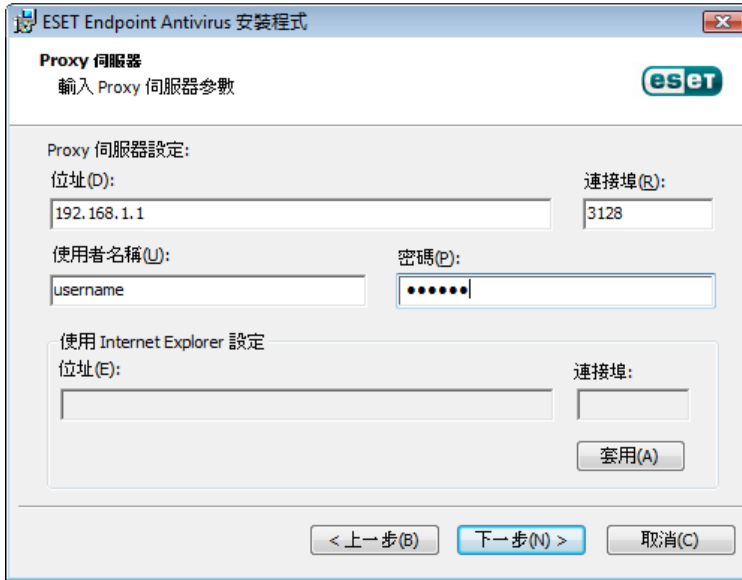


然後輸入您的 [使用者名稱] 及 [密碼]。此步驟與一般安裝相同 (請參閱「[一般安裝](#)」)。

按一下 [下一步] 並繼續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。如果您不知道您是否使用 Proxy 伺服器連接至網際網路，請選取 [我不確定我的網際網路連線是否使用 Proxy 伺服器]。請使用與 Internet Explorer 相同的設定 (建議) 並且按一下 [下一步]。如果您未使用 Proxy 伺服器，請選取 [我不使用 Proxy 伺服器] 選項。



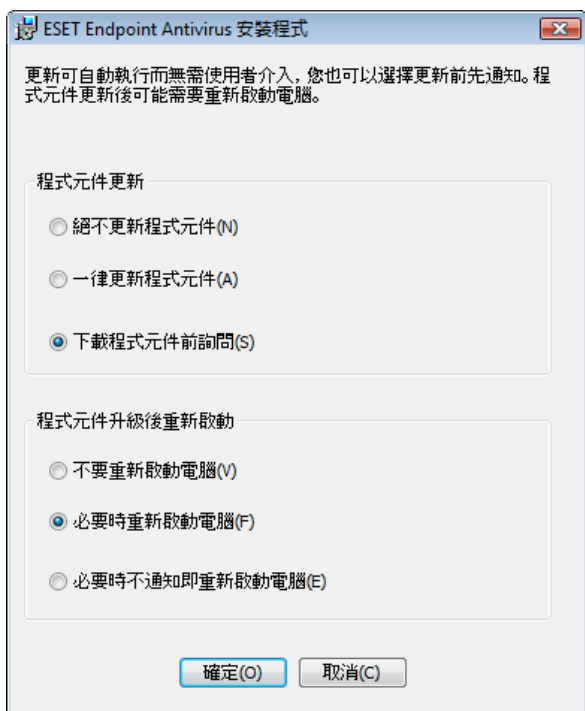
若要配置 Proxy 伺服器設定，請選取 [我使用 Proxy 伺服器]，然後按一下 [下一步]。將 Proxy 伺服器的 IP 位址或 URL 輸入到 [位址] 欄位中。在 [連接埠] 欄位中，指定 Proxy 伺服器接受連線所在的連接埠 (依預設為 3128)。如果 Proxy 伺服器需要驗證，則必須輸入有效的 [使用者名稱] 及 [密碼]，授與 Proxy 伺服器的存取權限。如果需要，也可以從 Internet Explorer 複製 Proxy 伺服器設定。若要這樣做，請按一下 [套用] 並確認選項。



此安裝步驟可讓您指定如何在系統上處理自動程式更新。按一下 [更新...] 以存取進階設定。

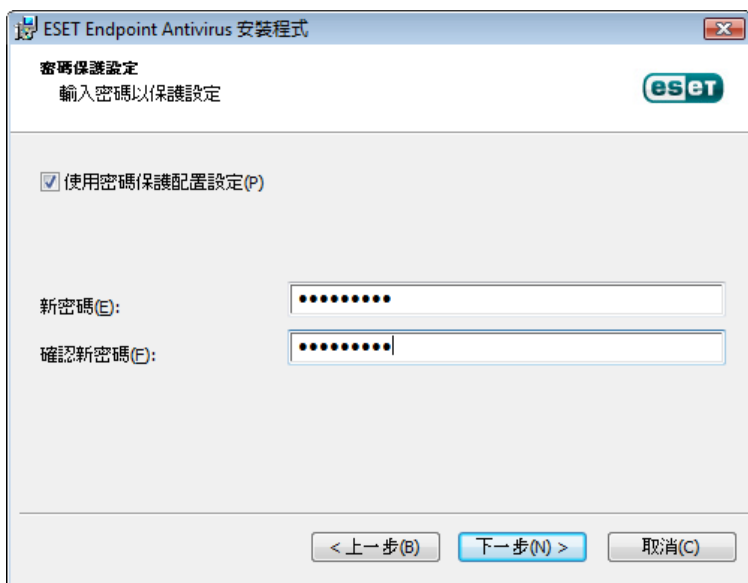


如果您不想要更新程式元件，請選取 [絕不更新程式元件] 選項。選取 [下載程式元件前詢問] 選項，以便在每次系統嘗試下載程式元件時顯示確認視窗。若要自動下載程式元件升級，請選取 [一律更新程式元件] 選項。



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] 選項。

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] 選項，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 Endpoint Antivirus 的設定。兩個密碼欄位相符時，按一下 [下一步] 以繼續進行。



接下來的安裝步驟：[自動更新]、[ESET Live Grid] 與 [偵測潛在不需要應用程式] 與一般安裝模式步驟相同 (請參閱 [「一般安裝」](#))。

按一下 [準備安裝] 視窗中的 [安裝] 完成安裝。完成安裝之後，系統將提示您啟動您的產品。如需更多有關產品啟動的資訊，請參閱 [一般安裝](#)。

## 2.3 輸入使用者名稱和密碼

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] 中輸入正確的使用者名稱和密碼，才能達到此目的。

如果安裝期間沒有輸入您的使用者名稱及密碼，您現在可以輸入。按下 CTRL+U 並將接收隨到附於 ESET 安全性產品的授權資料輸入到 [授權詳情] 視窗中。

輸入您的 [使用者名稱] 和 [密碼] 時，準確地照實輸入資訊是很重要的：

- 使用者名稱和密碼必須區分大小寫，而且必須輸入使用者名稱中的連字號。
- 密碼長度為十個字元，而且全部是小寫。
- 我們不在密碼中使用字母 l (請使用數字一 (1) 取代)。
- 大的 0 是數字零 (0)，小的 o 是小寫的字母 o。

建議從註冊電子郵件複製資料並貼上，以確保正確無誤。

## 2.4 升級至最新版本

新推出的 ESET Endpoint Antivirus 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. 透過下載新版本並安裝覆蓋舊版的方式手動升級。

開始安裝時，您可選取 [使用現有的設定] 核取方塊，以選擇保留目前的程式設定。

### 3. 透過 ESET Remote Administrator 在網路環境中以自動部署進行手動升級。

## 2.5 電腦掃描

安裝 ESET Endpoint Antivirus 後，您應該執行電腦掃描，檢查是否有惡意代碼。在主要功能表視窗中，按一下 [電腦掃描]，然後按一下 [智慧型掃描]。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 Endpoint Antivirus 及其基本設定的初始概觀。

#### 3.1 介紹使用者介面設計

ESET Endpoint Antivirus 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：

**防護狀態** - 提供與 ESET Endpoint Antivirus 的防護狀態有關的資訊。

**電腦掃描** - 此選項可讓您配置及啟動「智慧型掃描」或「自訂掃描」。

**更新** - 顯示有關病毒資料庫更新的資訊。

**設定** - 選取此選項以調整您電腦、Web 和電子郵件。

**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、排程器、隔離區、ESET SysInspector 及 ESET SysRescue。

**說明及支援** - 提供存取說明檔案、[ESET 知識庫](#)、ESET 網站和連結，以開啟「客戶服務」支援要求。



**防護狀態** 畫面可告知您電腦的安全性及目前的防護層級。綠色 [最嚴格的防護] 狀態表示已確保最嚴格的防護。

此狀態視窗也會顯示經常使用的 ESET Endpoint Antivirus 功能。您也可以在這裡找到有關程式到期日的資訊。

## 3.2 如果程式運作不正常怎麼辦

如果啟用的模組正常運作，則會標上綠色核取符號。如果不正常，則會顯示紅色驚嘆號或橙色通知圖示。視窗的上半部會顯示模組的其他相關資訊。同時還會顯示修正模組的建議解決方案。若要變更個別模組的狀態，請按一下主要功能表中的 [設定]，並按一下需要的模組。



紅色圖示表示嚴重問題 - 未確保電腦獲得最嚴格的防護。可能的原因如下：

- 即時檔案系統防護已停用
- 過期的病毒資料庫
- 產品未啟動
- 產品授權已過期

橘色圖示表示已停用 Web 存取或電子郵件用戶端防護、程式更新發生問題 (無法更新過期的病毒資料庫) 或授權接近到期日期。

病毒及間諜程式防護已停用 - 此問題會以紅色圖示表示，且 [電腦] 項目旁邊會顯示安全性通知。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。

Web 存取防護已停用 - 此問題會以橘色「i」圖示來表示，且狀態為 [安全性通知]。您可以重新啟用 Web 存取防護，方法是按一下安全性通知，然後按一下 [啟用 Web 存取防護]。

您的授權即將到期 - 這是由顯示驚嘆號的防護狀態圖示所表示。授權到期後，程式將無法更新，[防護] 狀態圖示將變成紅色。

授權已過期 - 這是由變成紅色的 [防護] 狀態圖示所表示。授權過期後即無法更新程式。建議按照警告視窗中的指示更新您的授權。

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，可以提交「ESET 客戶服務」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。



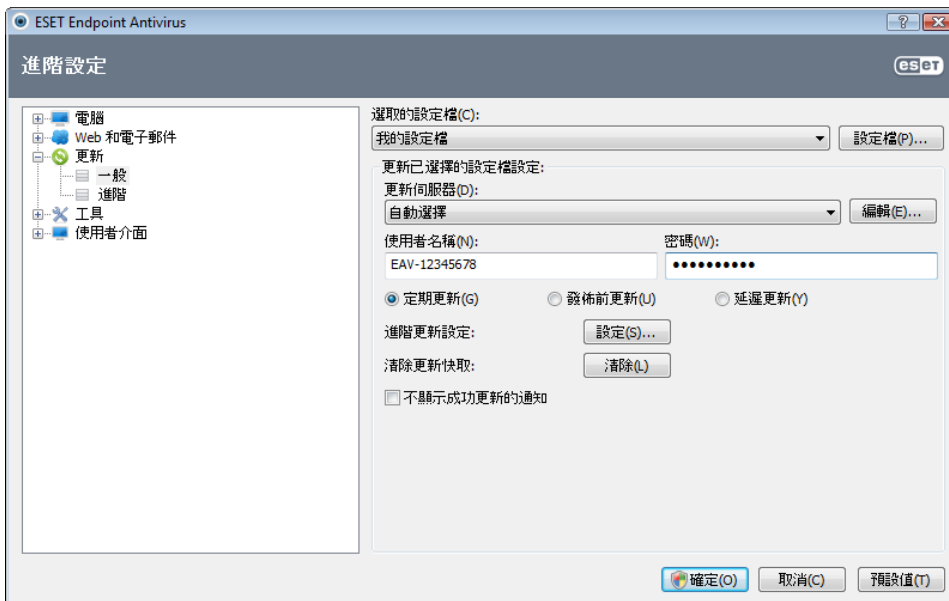
### 3.3 更新設定

更新病毒資料庫及更新程式元件是提供完整防護、防止惡意代碼的一個重要部分。請特別注意其配置與作業。從主要功能表中，選取 [更新]，然後按一下 [更新病毒資料庫]，檢查是否有較新的資料庫更新。

如果在 ESET Endpoint Antivirus 程序的安裝 期間未輸入使用者名稱與密碼，則會在此時提示您輸入。



[進階設定] 視窗 (從主要功能表按一下 [設定]，然後按一下 [進入進階設定...]，或按鍵盤上的 F5) 包含其他的更新選項。從左側的 [進階設定] 樹狀目錄中，按一下 [更新]。[更新伺服器] 下拉式功能表預設為 [自動選擇]。若要配置例如更新模式、Proxy 伺服器存取、LAN 連線，以及建立病毒碼副本之類的進階更新選項，請按一下 [設定...] 按鈕。



### 3.4 Proxy 伺服器設定

如果您在使用 ESET Endpoint Antivirus 的系統上使用 Proxy 伺服器來控制網際網路連線，則必須在 [進階設定] 中指定。若要存取 [Proxy 伺服器] 配置視窗，請按 F5 以開啟 [進階設定] 視窗，然後從 [進階設定] 樹狀目錄中按一下 [工具] > [Proxy 伺服器]。選取 [使用 Proxy 伺服器] 選項，然後填寫 [Proxy 伺服器] (IP 位址) 及 [連接埠] 欄位。必要時，可選取 [Proxy 伺服器需要驗證] 選項，然後輸入 [使用者名稱] 及 [密碼]。

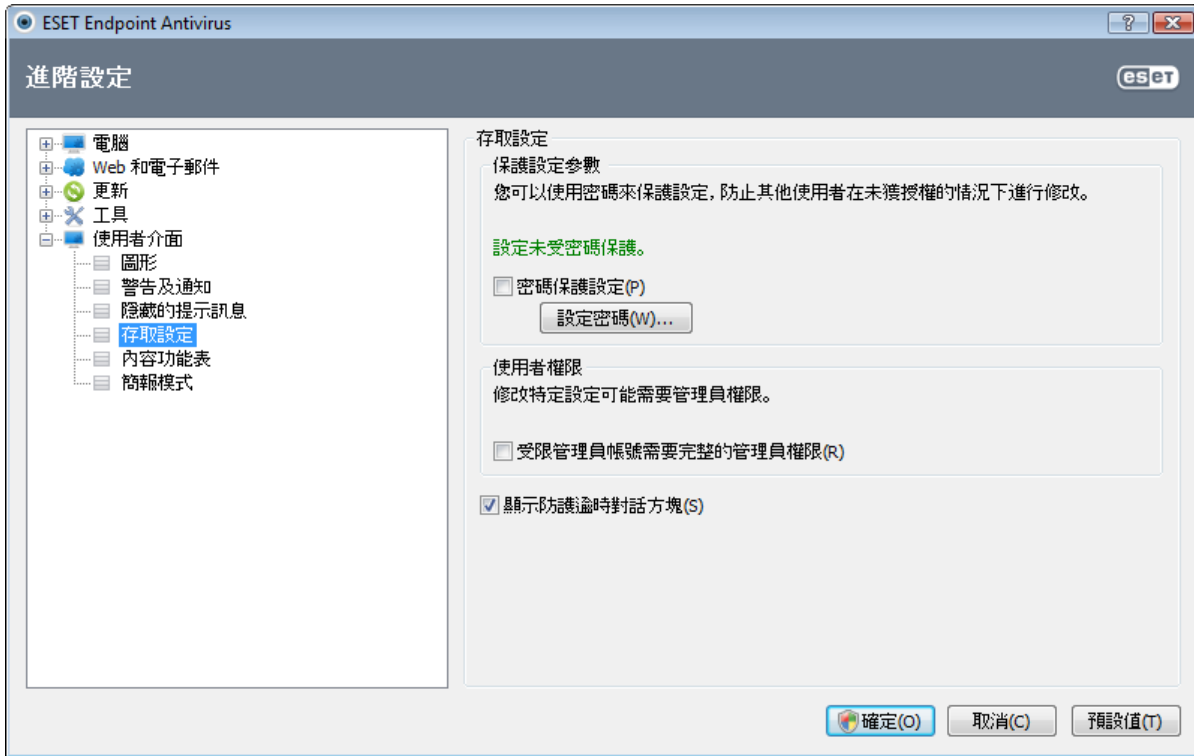


如果沒有這項資訊，您可以按一下 [偵測 Proxy 伺服器] 按鈕，嘗試自動偵測 Proxy 伺服器設定。

附註：各種更新設定檔的 Proxy 伺服器選項可能不同。如果是這種情況，請從 [進階設定] 樹狀目錄按一下 [更新]。

### 3.5 設定防護

ESET Endpoint Antivirus 設定對您的安全原則可能非常重要。未獲授權的修改可能會危害您系統的穩定性及防護功能。若要以密碼保護設定參數，請從主要功能表中，按一下 [設定] > [進入進階設定...] > [使用者介面] > [存取設定]，選取 [密碼保護設定] 選項並按一下 [設定密碼...] 按鈕。



在 [新密碼] 及 [確認新密碼] 欄位中輸入密碼，然後按一下 [確定]。日後對 ESET Endpoint Antivirus 設定進行任何修改，都將會需要這個密碼。

## 4. 使用 ESET Endpoint Antivirus

ESET Endpoint Antivirus 設定選項可讓您調整電腦的防護層級。



[設定] 功能表包含下列選項：

- 電腦
- Web 和電子郵件

按一下任何元件，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。
- 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)。
- 裝置控制 - 此模組可讓您掃描、封鎖或調整擴充的過濾器/權限，以及選取使用者存取和使用指定裝置 (CD/DVD/USB...) 的方式。
- 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。
- 簡報模式 - 啟用或停用 [簡報模式](#) 啟用以下模式之後，您將收到警告訊息 (潛在的安全性風險)，接著主視窗會轉為橘色：簡報模式。
- 反隱藏防護 - 可偵測例如 [Rootkit](#) 等危險程式，該危險程式可在作業系統中隱藏自己。這就意味著使用一般測試技術無法偵測到它們。

[Web 和電子郵件] 防護設定可讓您啟用或停用下列元件：

- Web 存取防護 - 如果啟用，則會掃描通過 HTTP 或 HTTPS 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。

附註：啟用 [進入進階設定...](F5) > [電腦] > [病毒及間諜程式防護] > [文件防護] > [整合至系統] 中的選項後，將顯示文件防護。

按一下 [停用] 之後，將顯示 [暫時停用防護] 對話方塊。按一下 [確定] 停用選取的安全性元件。[時間間隔] 下拉式功能表顯示選取元件將停用的期間。



若要將停用的安全性元件重新啟用，按一下 [停用]。

附註：使用此方法停用防護時，防護的所有停用部分將在電腦重新啟動後啟用。

設定視窗最下方有其他選項。若要使用 .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，請使用 [匯入及匯出設定...] 選項。

## 4.1 電腦

按一下 [電腦] 標題，您便可以在 [設定] 窗格中找到 [電腦] 模組。此視窗顯示所有防護模組的概觀。若要暫時關閉個別模組，請按一下所需模組下方的 [停用]。請注意，這會降低電腦的防護。若要存取每個模組的詳細設定，請按一下 [配置...]。

按一下 [編輯排除...]，以開啟 [排除] 設定視窗，可讓您從掃描排除檔案及資料夾。



暫時停用病毒及間諜程式防護 - 停用所有病毒及間諜程式防護模組。含有 [時間間隔] 下拉式功能表的 [暫時停用防護] 對話方塊將會顯示。[時間間隔] 下拉式功能表顯示防護功能將停用的期間。按一下 [確定] 以確認。

電腦掃描設定... - 按一下以調整指定掃描器的參數 (手動執行的掃描)。

#### 4.1.1 病毒及間諜程式防護

病毒及間諜程式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。

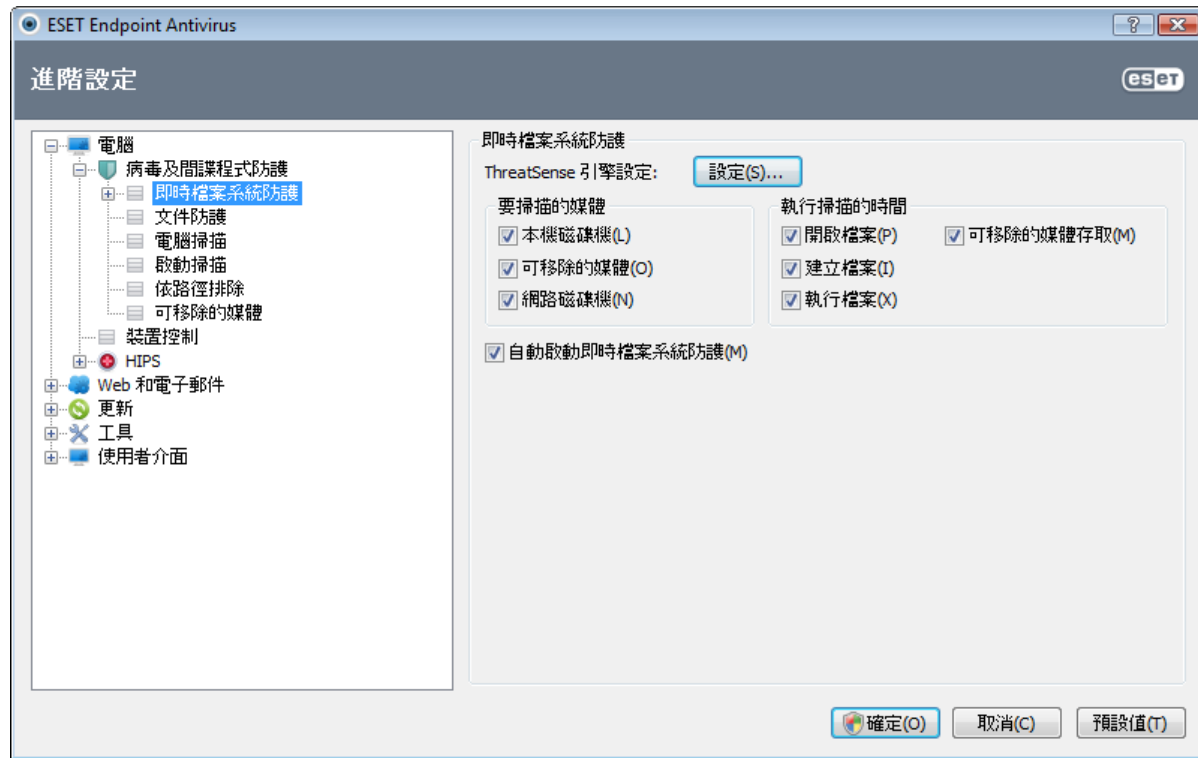
##### 4.1.1.1 即時檔案系統防護

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，會掃描它們是否具有惡意代碼。在系統啟動時會啟動即時檔案系統防護。

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)，針對新建立的檔案及現有檔案，即時檔案系統防護可能有所不同。若為新建立的檔案，則可套用較深入的控制層級。

為了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] 可配置此行為。如果停用此功能，則每次存取所有檔案時，都會進行掃描。若要修改此選項，請按 F5 開啟 [進階設定] 視窗，然後在 [進階設定] 樹狀結目錄中，按一下 [電腦] > [病毒及間諜程式防護] > [即時檔案系統防護]。然後按一下 [ThreatSense 引擎參數設定] 旁邊的 [設定...] 按鈕，接著按一下 [其他]，並且選取或取消選取 [啟用智慧型最佳化] 選項。

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)，則可以取消選取 [自動啟動即時檔案系統防護] 選項，以終止即時防護。



##### 4.1.1.1.1 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** - 磁碟片、CD/DVD、USB 儲存裝置等。

**網路磁碟** - 掃描所有對應的磁碟機。

我們建議保留預設設定，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。

#### 4.1.1.1.2 執行掃描的時機 (事件觸發的掃描)

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/停用對已開啟檔案的掃描。

建立檔案 - 啟用/停用新建立或修改檔案的掃描。

執行檔案 - 啟用/停用對已執行檔案的掃描。

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。

#### 4.1.1.1.3 進階掃描選項

在 [電腦] > [病毒及間諜程式防護] > [即時系統防護] > [進階設定] 下，可找到更詳細的設定選項。

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。除了常見的簽章掃描方法，使用進階啟發式可大幅提升偵測率，原因是啟發式會在病毒資料庫更新發行前先偵測新的威脅。除了新建立的檔案之外，也可針對自我解壓縮 (.sfx) 及 運行時間壓縮器 (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] 選項。

用於已執行檔案的其他 ThreatSense 參數 - 根據預設，執行檔案時不使用進階啟發式。然而，在某些情況下，您可能想要啟用此選項 (按一下 [執行檔案時的進階啟發式] 選項)。請注意，進階啟發式可能會由於增加系統需求的緣故，而減慢某些程式的執行速度。啟用 [從外部裝置執行檔案時的進階啟發式] 選項時，如果不想讓進階啟發式在執行檔案時掃描某些可移除媒體 (USB) 連接埠，請按一下 [例外...]，以開啟可移除媒體磁碟排除視窗。您可以在這裡選取或取消選取代表每個連接埠的核取方塊來自訂設定。

#### 4.1.1.1.4 清除層級

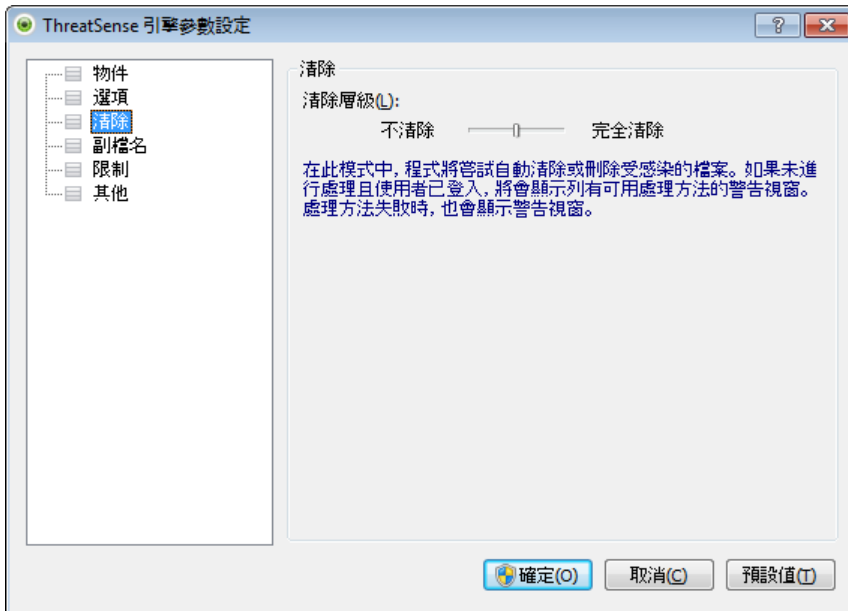
即時防護具有三個清除層級 (若要存取，請按一下 [即時檔案系統防護] 區段中的 [設定...] 按鈕，然後按一下 [清除] 子目錄)。

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。位於畫面右下角的資訊訊息會通知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，則程式會提供後續處理方法的選項。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。



#### 4.1.1.1.5 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。例如，在與特定應用程式或另一個防毒程式的即時掃描器發生衝突的情況下。

安裝 ESET Endpoint Antivirus 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，請按一下位於 [即時檔案系統防護] 視窗 ([進階設定] > [電腦] > [病毒及間諜程式防護] > [即時檔案系統防護]) 右下方的 [預設] 按鈕。

#### 4.1.1.1.6 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特殊無害的檔案。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。檔案 eicar.com 的下載連結為 <http://www.eicar.org/download/eicar.com>

#### 4.1.1.1.7 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情況，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 [即時檔案系統防護]。

如果在系統啟動時未啟動即時保護，則通常是由於已取消選取 [自動啟動即時檔案系統防護] 選項的緣故。若要啟用此選項，請瀏覽至 [進階設定] (F5)，並按一下 [進階設定] 樹狀目錄中的 [電腦] > [病毒及間諜程式防護] > [即時檔案系統防護]。在視窗底部的 [進階設定] 區段中，確定已選取 [自動啟動即時檔案系統防護] 核取方塊。

##### 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。如果同時啟用兩個即時保護程式，則它們可能互相衝突。我們建議您解除安裝系統上的任何其他防毒程式。

##### 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] 選項)，則可能是由於與其他程式發生衝突。如果是這種情況，請連絡 ESET 客戶服務。



#### 4.1.1.2 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)。[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] 樹狀目錄中，按一下 [電腦] > [病毒及間諜程式防護] > [文件防護]。啟動文件防護時，可在 ESET Endpoint Antivirus 主要視窗的 [設定] > [電腦] 區段中檢視。

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。

#### 4.1.1.3 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。從安全觀點來看，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。我們建議您定期執行完整的系統掃描以偵測病毒，這些病毒可能在寫入磁碟時，未遭 [即時檔案系統防護] 攔截。當資料寫入磁碟時，即時檔案系統防護已停用、病毒資料庫已過時，或是當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。[智慧型掃描] 可快速掃描系統，而無需進一步配置掃描參數。[自訂掃描] 可讓您選取任何預先定義的掃描設定檔，以及選擇特定掃描目標。

請參閱[掃描進度](#)一章，取得更多關於掃描進度的資訊。

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] > [排程器] 將掃描配置為已排程的工作。

#### 4.1.1.3.1 掃描類型

##### 4.1.1.3.1.1 智慧型掃描

智慧型掃描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。智慧型掃描的優點在於可以輕鬆執行作業，而不需要詳細的掃描配置。智慧型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](#)一節。

##### 4.1.1.3.1.2 自訂掃描

如果您想要指定掃描參數 (例如掃描目標及掃描方法)，則自訂掃描是可最理想的解決方案。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。

若要選取掃描目標，請選取 [電腦掃描] > [自訂掃描]，然後從 [掃描目標] 下拉式功能表中選取選項，或從樹狀結構中選取特定目標。亦可輸入您希望納入的資料夾或檔案路徑，指定掃描目標。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] 選項。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]。

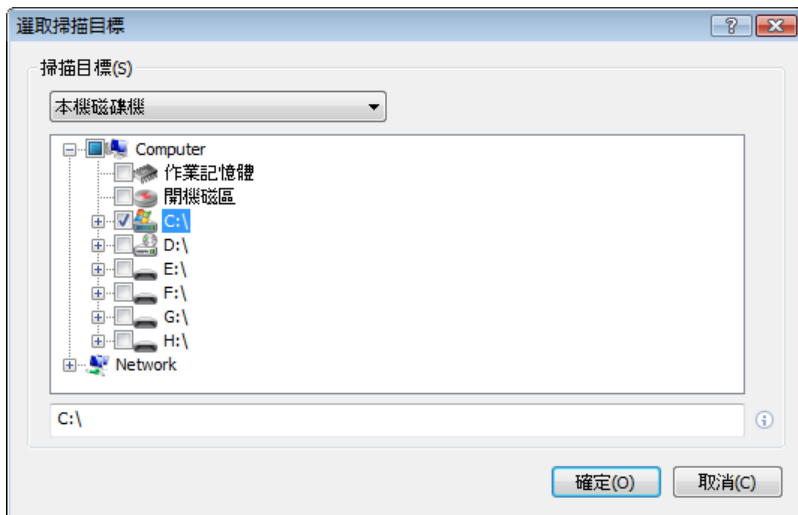
具有使用防毒程式經驗的進階使用者適合使用「自訂掃描」執行電腦掃描。

#### 4.1.1.3.2 掃描目標

[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)。[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。

輸入您希望納入掃描的資料夾或檔案路徑，也可指定掃描目標。從列出電腦上所有可用裝置的樹狀結構中選取目標。



若要快速瀏覽至掃描目標，或直接新增想要的目標，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。

#### 4.1.1.3.3 掃描設定檔

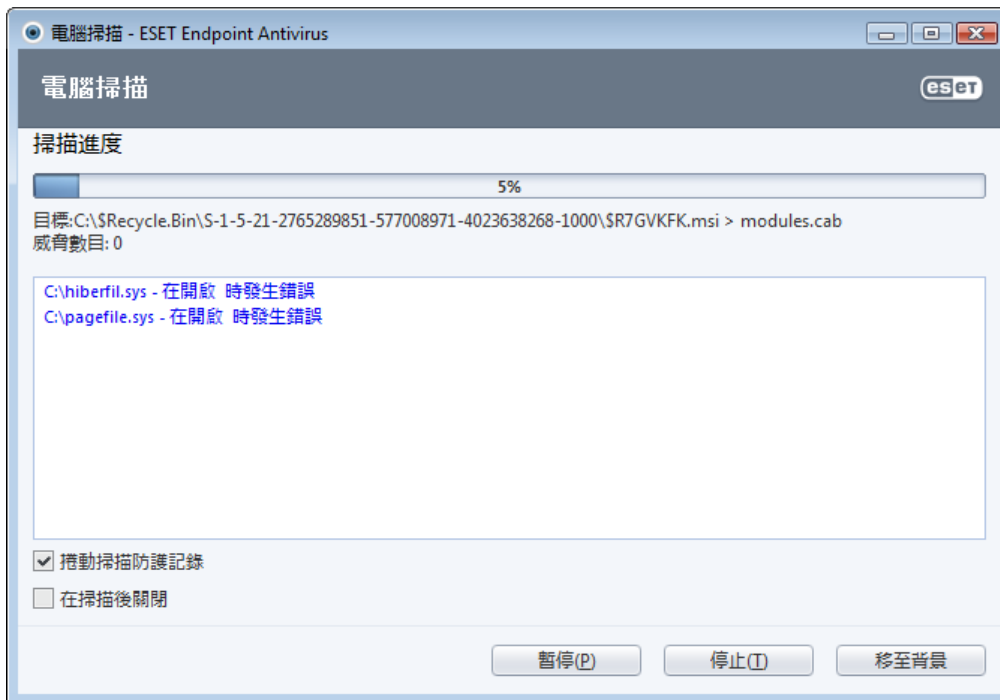
您偏好的掃描參數可儲存供未來掃描時使用。我們建議您盡量為定期進行的掃描建立不同設定檔 (含有各種掃描目標、掃描方法及其他參數)。

若要建立新的設定檔，請開啟 [進階設定] 視窗 (F5)，然後按一下 [電腦] > [病毒及間諜程式防護] > [電腦掃描] > [設定檔...]。[配置設定檔] 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「智慧型掃描」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 [配置設定檔] 視窗中，按一下 [新增...] 按鈕。在 [設定檔名稱] 欄位中輸入新設定檔的名稱，然後從 [從設定檔複製設定] 中選取 [智慧型掃描]。然後，調整剩餘的參數以符合您的需求。

#### 4.1.1.3.4 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：通常無法掃描某些檔案，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百分比。此值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。

威脅數目 - 顯示掃描期間找到的威脅總數。

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。

移至背景 - 您可以執行另一個平行掃描。此執行中的掃描將最小化並融入背景。



按一下 [移至最上層] 以將掃描移至最上層並返回掃描進度。

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。

啟用在掃描後關閉 - 當指定電腦掃描完成時，啟用已排程的關閉作業。關閉確認對話方塊視窗將開啟並於 60 秒後逾時。如果您要停用要求的關機作業，請按一下 [取消]。

#### 4.1.1.4 啟動掃描

在系統啟動或病毒資料庫更新時，將執行自動啟動檔案檢查。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] > [排程器]，並且按一下 [自動啟動檔案檢查] 及 [編輯...] 按鈕。在最後一個步驟中，[\[自動啟動檔案檢查\]](#) 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](#)。

##### 4.1.1.4.1 自動啟動檔案檢查

[掃描層級] 下拉式功能表可指定系統啟動時執行的檔案掃描深度。系統會依要掃描檔案的編號遞增排序檔案：

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

此外也包含兩個特定的 [掃描層級] 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執行檔案的位置中的檔案 (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執行檔案的位置中的檔案 (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)

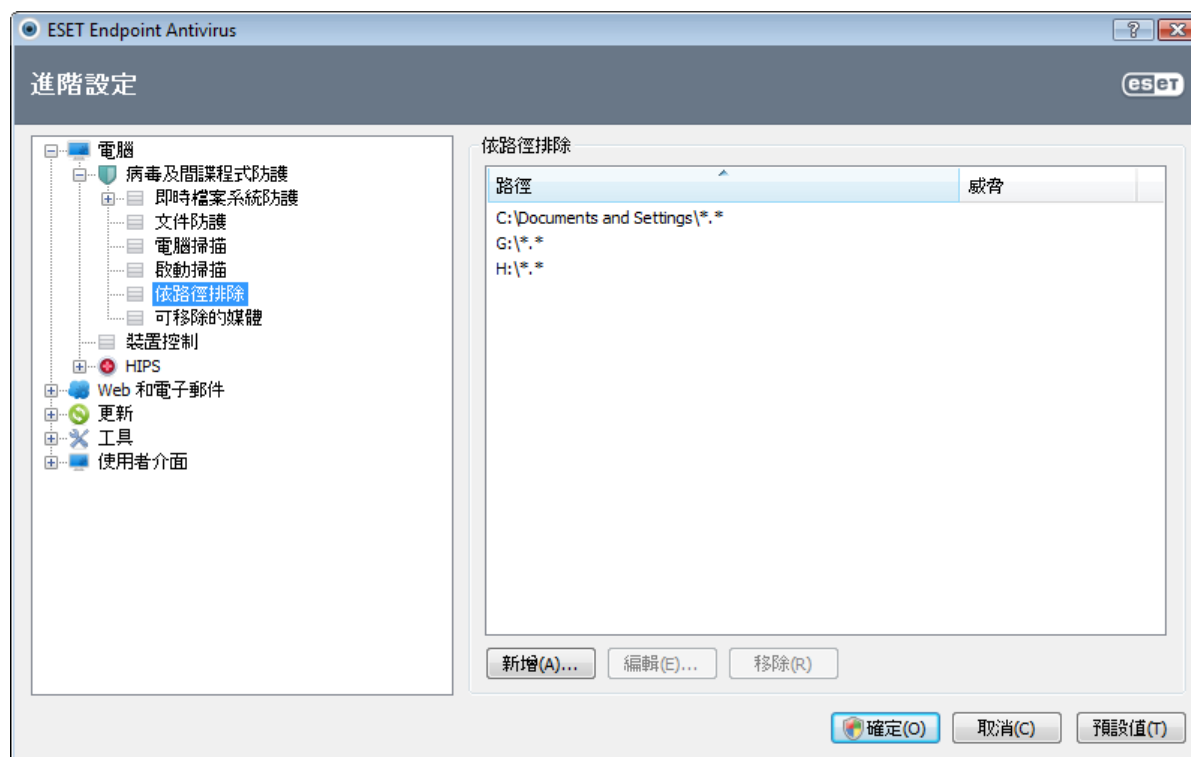
每個群組的待掃描檔案清單是固定的。

掃描優先順序 - 用於啟動掃描的優先順序層級：

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

#### 4.1.1.5 依路徑排除

[排除] 可讓您從掃描中排除檔案及資料夾。我們建議您不要改變這些選項，以確保可以掃描所有物件中的威脅。然而，在某些情況下，您可能需要排除物件。例如，大型資料庫項目可能會在掃描期間降低電腦速度，或是軟體可能與掃描衝突。



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。因此，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]) 中建立，或在 [設定] > [隔離區] 中建立 (在隔離檔案上使用內容功能表選項 [還原並從偵測中排除])。

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。

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。

#### 4.1.1.6 ThreatSense 引擎參數設定

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的前幾個小時期間提供防護。其使用多種方法組合 (代碼分析、代碼模擬、一般資料庫、病毒資料庫)，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 技術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 技術之模組設定視窗中的 [設定...] 按鈕 (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、
- 文件防護、
- 電子郵件用戶端防護、
- Web 存取防護、
- 及電腦掃描。

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。

##### 4.1.1.6.1 物件

[物件] 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。

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

運行時間壓縮器 - 執行之後，運行時間壓縮器 (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)，掃描器還支援 (由於模擬代碼) 更多類型的壓縮器。

##### 4.1.1.6.2 選項

使用 [選項] 區段，就可以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。主要的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。由於進階啟發式，程式的偵測能力大大地提高了。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 (或其略微修改的版本)。

潛在不需應用程式 (PUA) 不一定是惡意的，但是對電腦效能可能會造成負面影響。這些應用程式通常需要經過同意才能安裝。如果他們存在於您的電腦上，系統的行為會有所不同 (相較於安裝前的狀態)。最顯著的變更如下：

- 您從未看過的新視窗 (快顯視窗、廣告)、
- 啟動並執行隱藏的處理程序、
- 系統資源的用量增加、
- 搜尋結果變更、
- 應用程式會與遠端伺服器通訊。

潛在不安全的應用程式 - [潛在不安全的應用程式](#) 是用於合法商業軟體的類別。其中包括諸如遠端存取工具、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) 等程式。依預設會停用此選項。

ESET Live Grid - 透過 ESET 的聲譽技術，已針對來自雲端型 [ESET Live Grid](#) 傳來的資料，驗證有關掃描檔案的資訊，來改善偵測與掃描速度。

#### 4.1.1.6.3 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：

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。

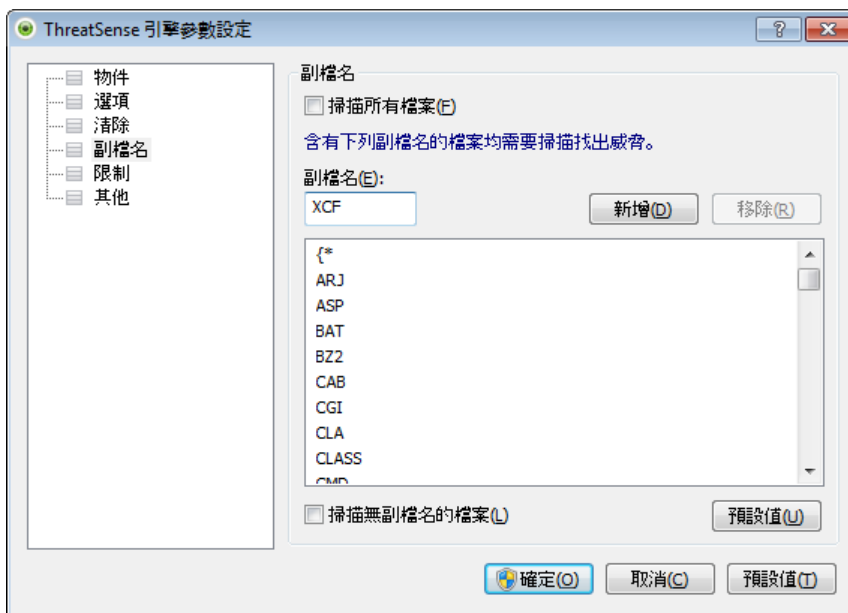
標準清除 - 程式會根據預先定義的處理方法 (視入侵的類型而定) 嘗試自動清除或刪除受感染檔案。位於畫面右下角的資訊訊息會通知受感染檔案的偵測及刪除。如果無法自動選取正確的處理方法，則程式會提供後續處理方法的選項。無法完成預先定義的處理方法時，程式也會提供後續處理方法的選項。

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。

#### 4.1.1.6.4 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。如果取消勾選 [掃描所有檔案] 選項，則清單會變更為顯示所有目前已掃描檔案的副檔名。

若要啟用沒有副檔名的檔案掃描，請選取 [掃描無副檔名的檔案] 選項。啟用 [掃描所有檔案] 選項時，才能使用 [不掃描無副檔名的檔案] 選項。

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。輸入 [副檔名] 可啟動 [新增] 按鈕，可將新副檔名新增至清單。選取清單中的副檔名，然後按一下 [移除] 按鈕，以從清單中刪除副檔名。

可以使用特殊符號 \* (星號) 及 ? (問號)。星號替代任何字元字串，而問號替代任何字符。指定已排除的位址時應該特別小心，因為清單應僅包含受信任及安全位址。同樣地，必須確定在此清單中正確使用字符 \* 及 ?。

若要僅掃描預設副檔名集，請按一下 [預設值] 按鈕，當提示確認時請按一下 [是]。

#### 4.1.1.6.5 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*。

如果由於這些原因而提前結束壓縮檔的掃描，則壓縮檔核取方塊會保持未勾選狀態。

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。

#### 4.1.1.6.6 其他

您可以在 [其他] 區段配置下列選項：

**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。

配置 [電腦掃描] 的 ThreatSense 引擎參數設定時，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。

**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)。

**捲動掃描防護記錄** - 此選項可讓您啟用/停用防護記錄捲動。如果選取此選項，資訊會在顯示視窗中向上捲動。

#### 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 Endpoint Antivirus 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或
- 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，則會要求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)。

## 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，如果保存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，因為執行完全清除，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 Endpoint Antivirus，然後按一下 [電腦掃描]，
- 按一下 [智慧型掃描] (如需詳細資訊，請參閱[智慧型掃描](#))。
- 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。

#### 4.1.2 可移除的媒體

ESET Endpoint Antivirus 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。

連接外部裝置後採取的動作 - 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]** 選項，則會顯示通知，讓您選擇想要的處理方法：

- **立即掃描** - 將針對已插入的可移除媒體裝置執行指定電腦掃描。
- **稍後掃描** - 不執行任何處理方法，且會關閉 **[偵測到新裝置]** 視窗。
- **設定...** - 開啟 **[可移除的媒體設定]** 區段。



此外，ESET Endpoint Antivirus 具備裝置控制功能，能夠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 Endpoint Antivirus 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，以及選取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

- CD/DVD/Blu-ray
- USB 儲存裝置
- FireWire 裝置
- 影像裝置
- USB 印表機
- 藍牙
- 讀卡機
- 數據機
- LPT/COM 連接埠

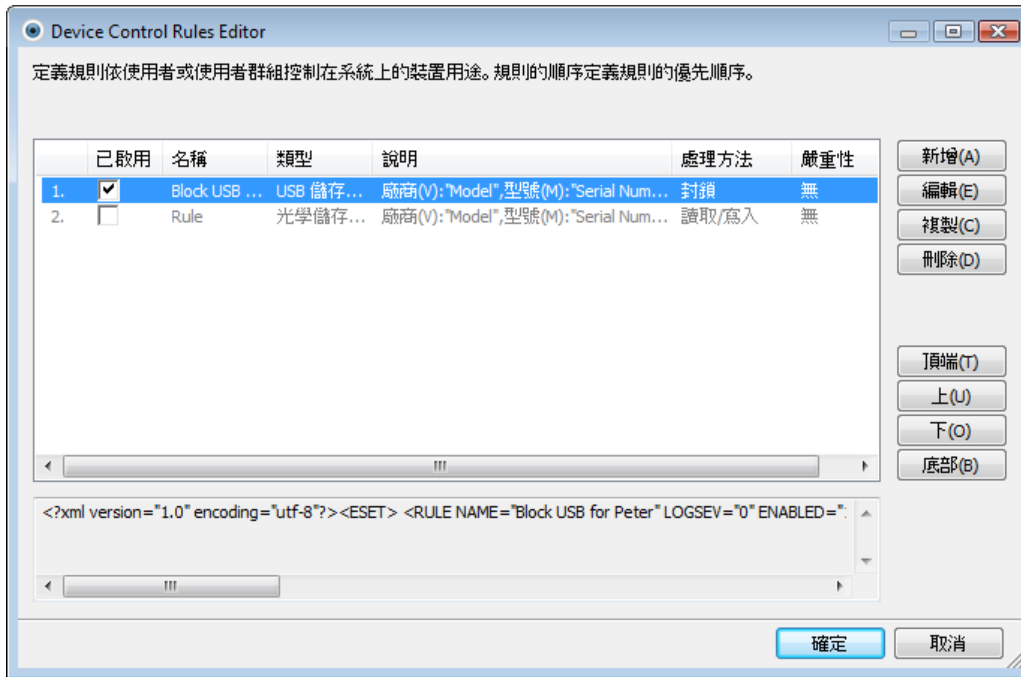
選取 **[進階設定]** (F5) > **[裝置控制]**，即可修改裝置控制設定選項。

選取 **[整合至系統]** 旁的核取方塊，可啟用 ESET Endpoint Antivirus 中的裝置控制功能；您必須重新啟動電腦才能讓變更生效。啟用裝置控制後，**[配置規則...]** 將變成作用中，可讓您開啟 **[裝置控制規則編輯器]** 視窗。

如果插入的外部裝置所套用的現有規則可執行 **[阻擋]** 動作，則會在右下角顯示快顯視窗，且不授與裝置的存取權限。

#### 4.1.3.1 裝置控制規則

[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。

在規則上按一下滑鼠右鍵即可顯示內容功能表。您可以在這裡設定規則的防護記錄項目簡化 (嚴重性)。在 ESET Endpoint Antivirus 的主要視窗中選取 [工具] > [防護記錄檔案]，即可檢視防護記錄項目。

### 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。選取 **[已啟用]** 旁的核取方塊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 (USB/藍牙/FireWire/...)。裝置的類型是從作業系統繼承，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。下拉式功能表中的 **[光學儲存裝置]** 裝置類型是指在光學可讀媒體 (例如 CD、DVD) 上儲存資料。儲存裝置涵蓋透過 USB 或 FireWire 連接的外部磁碟或常見的讀卡機。掃描器或相機都是影像裝置。智慧卡讀卡機是內嵌積體電路的智慧卡適用的讀卡機，SIM 卡或驗證卡都是智慧卡。

#### 權限

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：

- 封鎖 - 將封鎖裝置的存取權限。
- 唯讀 - 僅允許從裝置讀取。
- 讀取/寫入 - 將允許裝置的完整存取權限。

請注意，並非所有裝置類型都適用所有權限 (處理方法)。如果裝置有儲存空間，則可使用所有三種處理方法。對於非儲存裝置，只可使用兩種處理方法 (**[唯讀]** 處理方法不適用於藍牙，因此只能允許或封鎖裝置)。

可用來微調規則並針對特定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：如果這三個描述元全為空白，則當比對時規則會忽略這些欄位。

提示：為了查明裝置的參數，可建立適當裝置類型的允許規則，並且將裝置連接到電腦，然後查看 [裝置控制防護記錄](#) 中的裝置詳細資訊。

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。
- 刪除 - 從過濾器移除選取的使用者。

#### 4.1.4 主機入侵預防系統 (HIPS)

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需要活動。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分開，不是防火牆，只監控在作業系統內執行的處理程序。

按一下 [電腦] > [HIPS]，即可在 [進階設定] (F5) 中找到 HIPS。HIPS 狀態 (啟用/停用) 顯示在 [電腦] 區段右側 [設定] 窗格的 ESET Endpoint Antivirus 主視窗中。

HIPS 設定位在 [進階設定] (F5) 中。若要存取 [進階設定] 樹狀目錄中的 HIPS，請按一下 [電腦] > HIPS。HIPS 狀態 (已啟用/已停用) 顯示在 ESET Endpoint Antivirus 主視窗中 [電腦] 區段右側的 [設定] 窗格中。

**警告：** HIPS 設定若要變更，僅能由有經驗的使用者執行。

ESET Endpoint Antivirus 有內建的[自我防護]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。[啟用 HIPS] 和 [啟用自我防護] 設定的變更會在 Windows 作業系統重新啟動後生效。停用整個 HIPS 系統也需要重新啟動電腦。

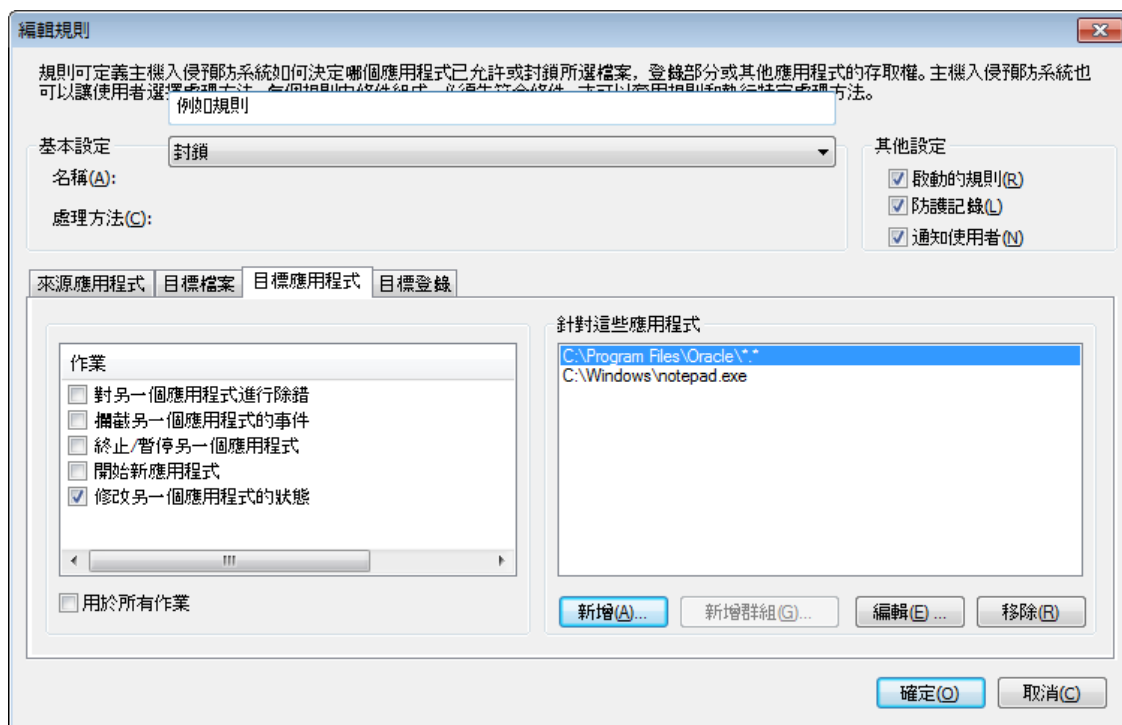
過濾可使用以下四種模式之一執行：

- [使用規則的自動模式] - 系統會啟用作業，但保護系統的預先定義規則除外。
- [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。選取 [學習模式] 之後，[學習模式在到期前 X 天通知] 選項會變成作用中。在該期間過後，將再次停用學習模式。期間最長為 14 天。此期間結束後，快顯視窗會開啟，您可以在其中編輯規則並選取不同的過濾模式。

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 [配置規則...] 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. 開啟 [目標應用程式] 索引標籤。將 [來源應用程式] 索引標籤保留空白，可將新規則套用到所有嘗試執行 [針對這些應用程式] 清單中應用程式上 [作業] 清單中所有已勾選作業的應用程式。
3. 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，在視窗中按下 F1 鍵即可顯示，如下圖所示)。
4. 將您要的一或多個應用程式新增至專案。
5. 啟用 [通知使用者] 選項後，只要套用規則就會顯示使用者通知。
6. 按一下 [確定] 以儲存新規則。



如果 [詢問] 為預設處理方法，則每一次都會出現對話視窗。使用者可由此選擇 [拒絕] 或 [允許] 作業。如果使用者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。



對話方塊視窗可讓您根據 HIPS 偵測到的任何新處理方法建立規則，再定義允許或拒絕該處理方法的狀況。按一下 [顯示選項] 之後，即可設定確實的參數。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。

[暫時記住此處理程序的此處理方法] 選項會造成使用處理方法 ([允許]/ [拒絕])，直到變更規則或篩選模式、HIPS 模式更新或系統重新啟動。在完成上述三個處理方法之一後，將刪除暫存規則。

## 4.2 Web 和電子郵件

按一下 [Web 和電子郵件] 標題，您便可以在 [設定] 窗格中找到 Web 和電子郵件配置。您可以在這裡存取程式的詳細設定。



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。因為如此，您必須審慎考量您的 **Web 存取防護**。

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 Endpoint Antivirus 可控制來自電子郵件用戶端的所有通訊 (POP3、MAPI、IMAP、HTTP)。

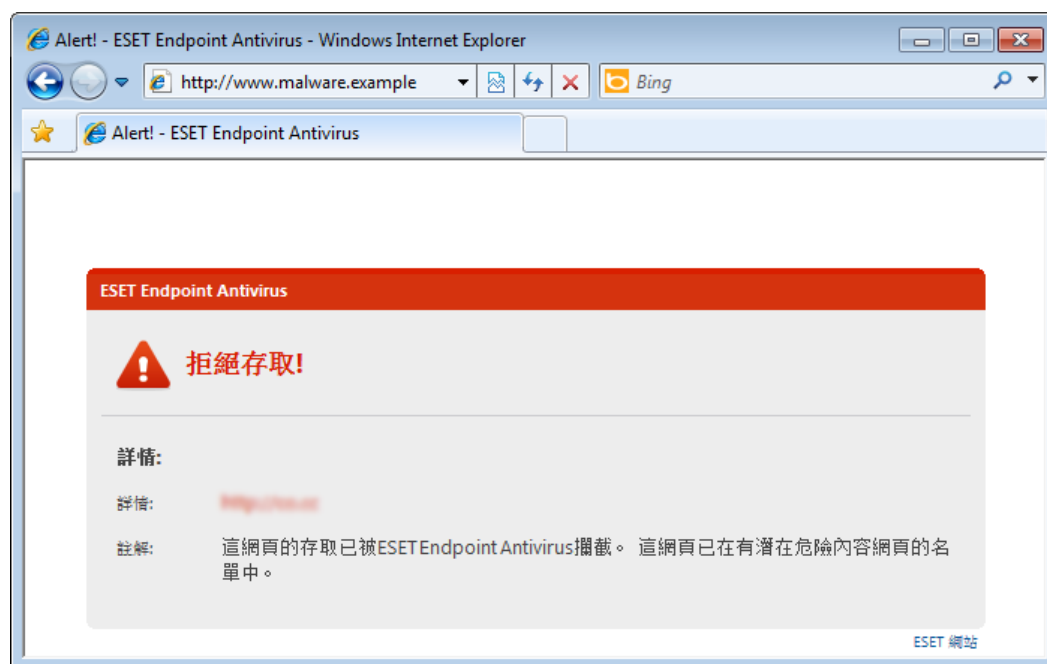
停用 - 停用電子郵件用戶端的 web/電子郵件 防護。

配置 ... - 開啟 web/電子郵件 防護進階設定。

## 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 存取防護 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。

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。請在 [字彙](#) 中閱讀更多有關此活動的資訊。ESET Endpoint Antivirus 支援網路釣魚防護，一律封鎖已知含這類內容的網頁。



我們強烈建議 Web 存取防護 為啟用。此選項可從 ESET Endpoint Antivirus 的主要視窗存取 (瀏覽至 [設定] > [Web 和電子郵件] > [Web 存取防護])。

### 4.2.1.1 HTTP、HTTPS

依預設，ESET Endpoint Antivirus 已配置為使用大多數網際網路瀏覽器的標準。不過，您可以在 [進階設定] (F5) > [Web 和電子郵件] > [Web 存取防護] > [HTTP? HTTPS] 中修改 HTTP 掃描器設定選項。在主要的 [HTTP 過濾器] 視窗中，您可以選取或取消選取 [啟用 HTTP 檢查] 選項。您也可以定義用於 HTTP 通訊的連接埠號碼。依預設，預先定義為連接埠 80 (HTTP)、8080 及 3128 (Proxy 伺服器)。

ESET Endpoint Antivirus 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 Endpoint Antivirus 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。HTTPS 檢查可以在下列模式中執行：

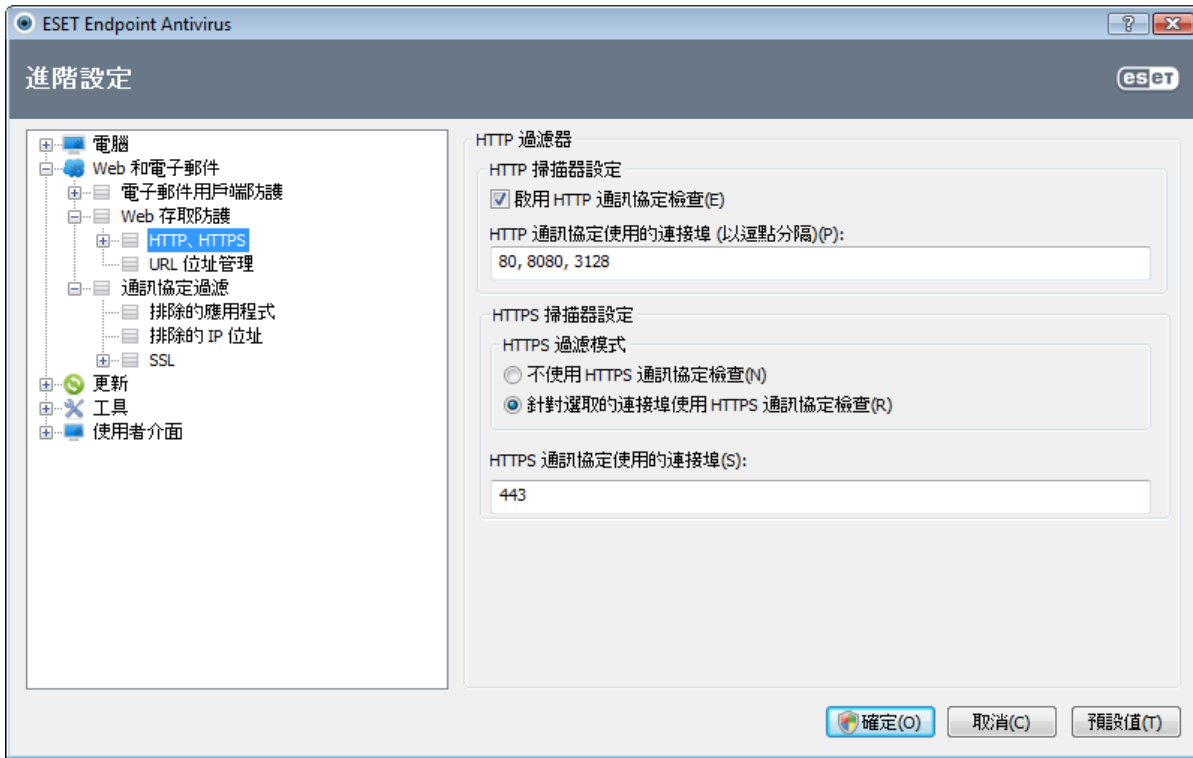
不使用 HTTPS 通訊協定檢查 - 不會檢查加密的通訊。

針對選取的連接埠使用 HTTPS 通訊協定檢查 - HTTPS 檢查只用於在 [HTTPS 通訊協定使用的連接埠] 中定義的連接埠。

針對選取的連接埠使用 HTTPS 通訊協定檢查 - 程式只會檢查在 [瀏覽器](#) 區段中指定的應用程式，以及使用在 [HTTP 通訊協定使用的連接埠] 中定義之連接埠的應用程式。預設為連接埠 443。

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 通訊協定檢查](#)，按一下 [Web 和電子郵件] > [通訊協定過濾] > [SSL]，並啟用 [一律掃描 SSL 通訊協定] 選項。





#### 4.2.1.1.1 Web 瀏覽器的主動模式

ESET Endpoint Antivirus 還包含定義網際網路瀏覽器之檢查模式的子功能表 [主動模式]。

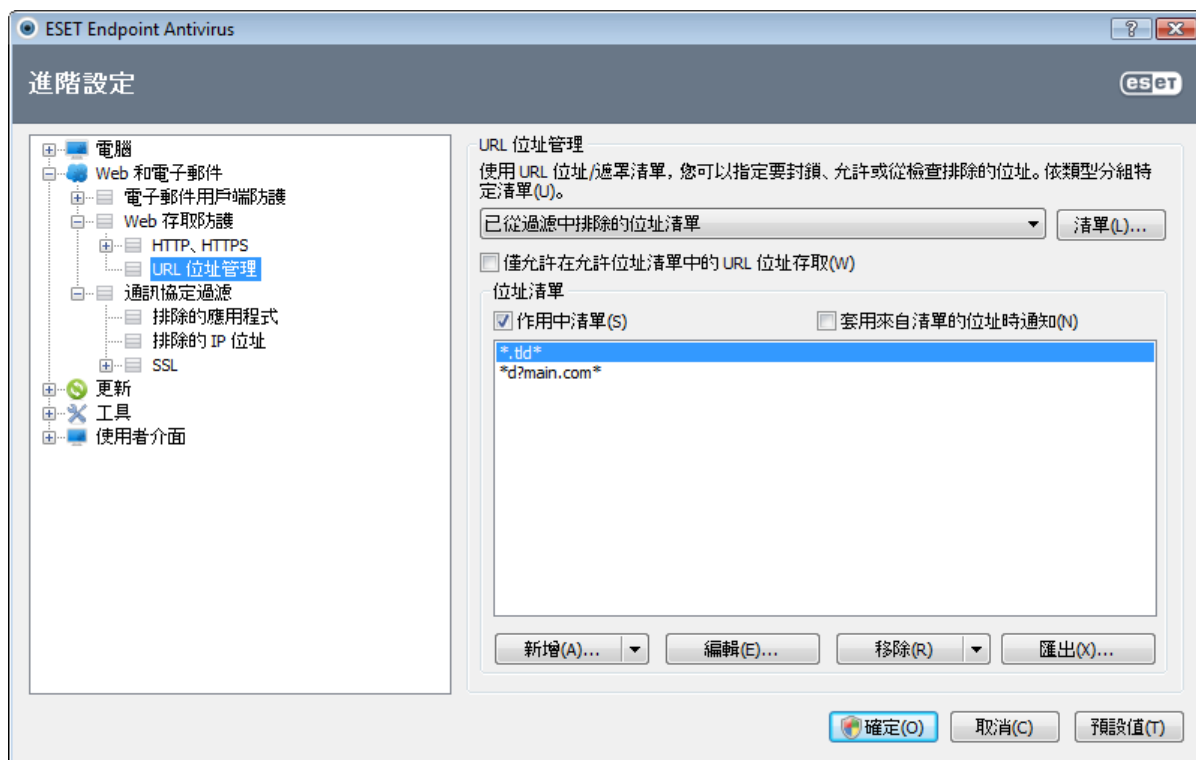
[主動模式] 很有幫助，因為它會整體檢查從存取網際網路之應用程式所傳輸的資料，無論這些應用程式是否標示為 Web 瀏覽器 (如需更多資訊，請參閱 [Web 和電子郵件用戶端](#))。如果主動模式停用，則會以批次方式逐步監視應用程式的通訊。這樣會降低資料驗證程序的效率，但是也會針對列出的應用程式提供更高的相容性。如果在使用時未發生任何問題，我們建議您選取所需應用程式旁邊的核取方塊，以啟用主動模式。以下為主動模式的運作方式：當受控制的應用程式下載資料時，會先將資料儲存到由 ESET Endpoint Antivirus 所建立的暫存檔案中。此時指定應用程式無法使用資料。下載完成之後，會檢查資料是否具有惡意代碼。如果未發現入侵，則會將資料傳送至原始應用程式。此處理程序可完全控制受控制應用程式的通訊。如果啟動被動模式，則會將資料一點一點傳送至原始應用程式，以避免逾時。

#### 4.2.1.2 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。[新增]、[編輯]、[移除] 及 [匯出] 按鈕可用來管理位址清單。不可以存取封鎖位址清單中的網站。可以存取已排除位址清單中的網站，而無需掃描惡意程式碼。如果選取 [僅允許在允許位址清單中的 URL 位址存取] 選項，則只能存取允許位址清單中的位址，而封鎖所有其他 HTTP 位址。

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。按一下 [清單...] 按鈕，就會出現 [HTTP 位址/遮罩清單] 視窗，讓您 [新增] 或 [移除] 位址清單。[一律掃描 [SSL 通訊協定](#)] 選項必須為作用中，才能將 HTTPS URL 位址新增至清單。

在所有清單中都可以使用特殊符號 \* (星號) 及 ? (問號)。星號替代任何字元字串，而問號替代任何字符。指定已排除的位址時應該特別小心，因為清單應僅包含受信任及安全位址。同樣地，必須確定在此清單中正確使用字符 \* 及 ?。若要啟動清單，請選取 [作用中的清單] 選項。如果您想要在進入目前清單中的位址時收到通知，請選取 [套用來自清單的位址時通知]。



**新增.../從檔案** - 允許您手動 ([新增]) 或從簡單文字檔 ([從檔案]) 將位址新增至清單。[從檔案] 選項可讓您新增儲存在文字檔中的多個 URL 位址/遮罩。

**編輯...** - 手動編輯位址，如加入遮罩 ("\*" 與 "?")。

**[移除/全部移除]** - 按一下 [移除] 以從清單中刪除選取的位址。若要刪除所有位址，請選取 [全部移除]。

**匯出...** - 將目前清單中的位址儲存為簡單文字檔。

#### 4.2.2 電子郵件用戶端防護

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 Endpoint Antivirus 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 ThreatSense 掃描引擎提供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。

透過 [進階設定] > [Web 和電子郵件] > [電子郵件用戶端防護] 可找到此功能的選項。

**ThreatSense 引擎參數設定** - 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 [設定...]，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] 及 [將標籤訊息附加到已傳送的郵件]。不可完全信任標籤訊息，因為它們可能會在有問題 HTML 訊息中省略，或可能由某些病毒所產生。標籤訊息可以新增至已接收及已讀取的電子郵件，或新增至已傳送的電子郵件 (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。

**將附註附加到已接收、已閱讀且受感染電子郵件的主旨** - 如果您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，請啟用此核取方塊。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。

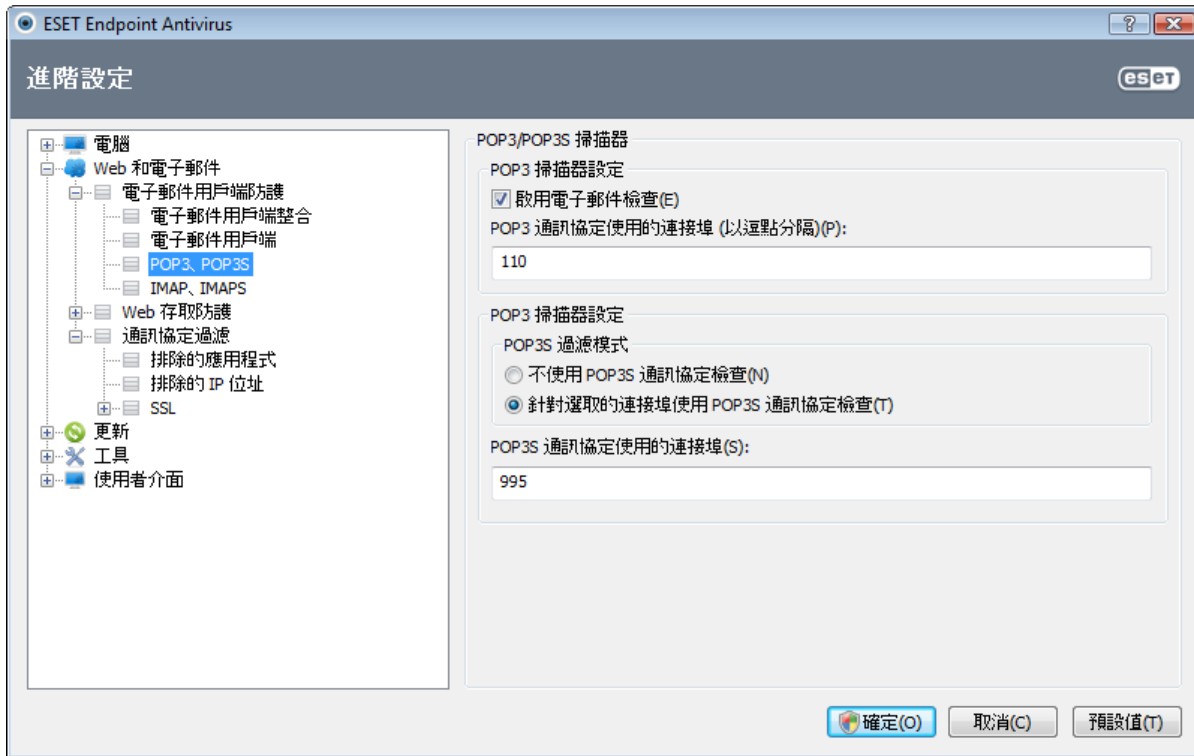
**新增到受感染電子郵件主旨的範本** - 如果您想修改受感染電子郵件的主旨字首格式，請編輯此範本。此功能會將字首值為 "[virus]" 的郵件主旨 "Hello" 取代成下列格式："[virus] Hello"。變數 %VIRUSNAME% 代表偵測到的威脅。

#### 4.2.2.1 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 Endpoint Antivirus 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 通訊協定檢查](#)，按一下 [Web 和電子郵件] > [通訊協定過濾] > [SSL]，並啟用 [一律掃描 SSL 通訊協定] 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 Endpoint Antivirus 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 Endpoint Antivirus 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。

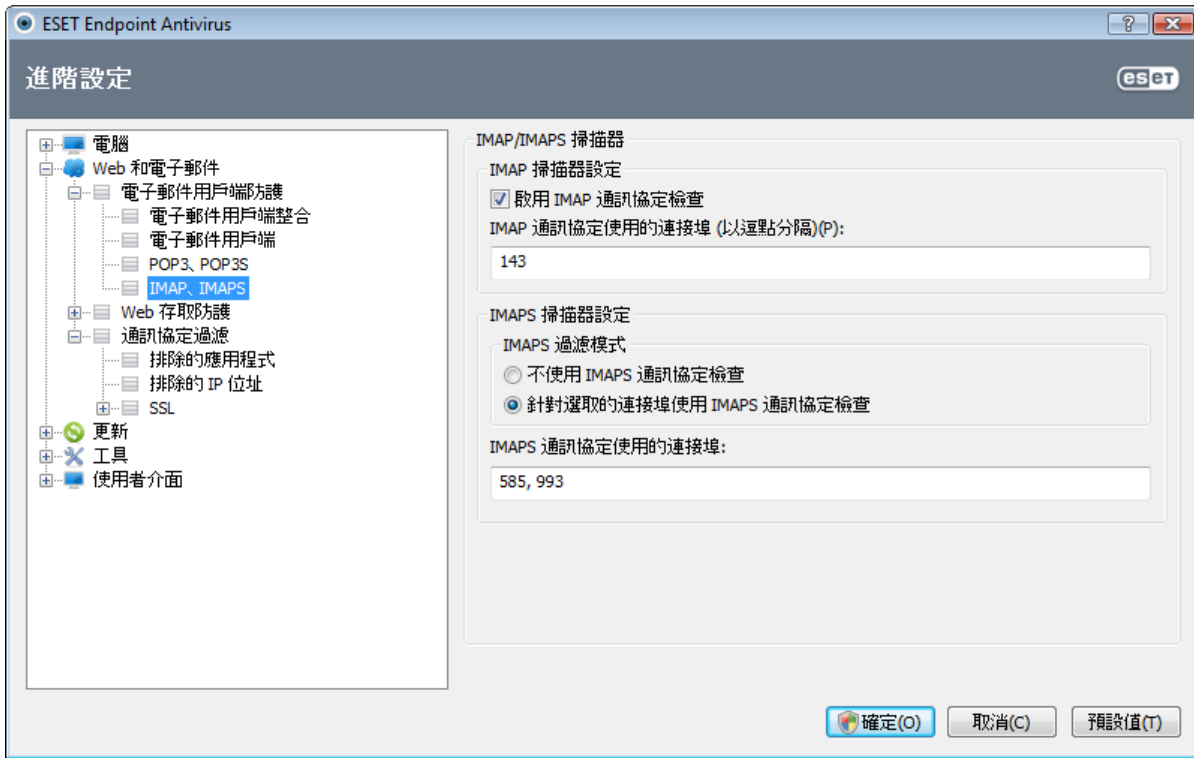
**POP3S 通訊協定使用的連接埠** - 要檢查的 POP3S 連接埠清單 (預設為 995)。

#### 4.2.2.2 IMAP、IMAPS 通訊協定控制項

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 Endpoint Antivirus 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 IMAP 通訊協定控制項，而無需重新配置電子郵件用戶端。依預設，通訊埠 143 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 通訊協定檢查](#)，按一下 [Web 和電子郵件] > [通訊協定過濾] > [SSL]，並啟用 [一律掃描 SSL 通訊協定] 選項。

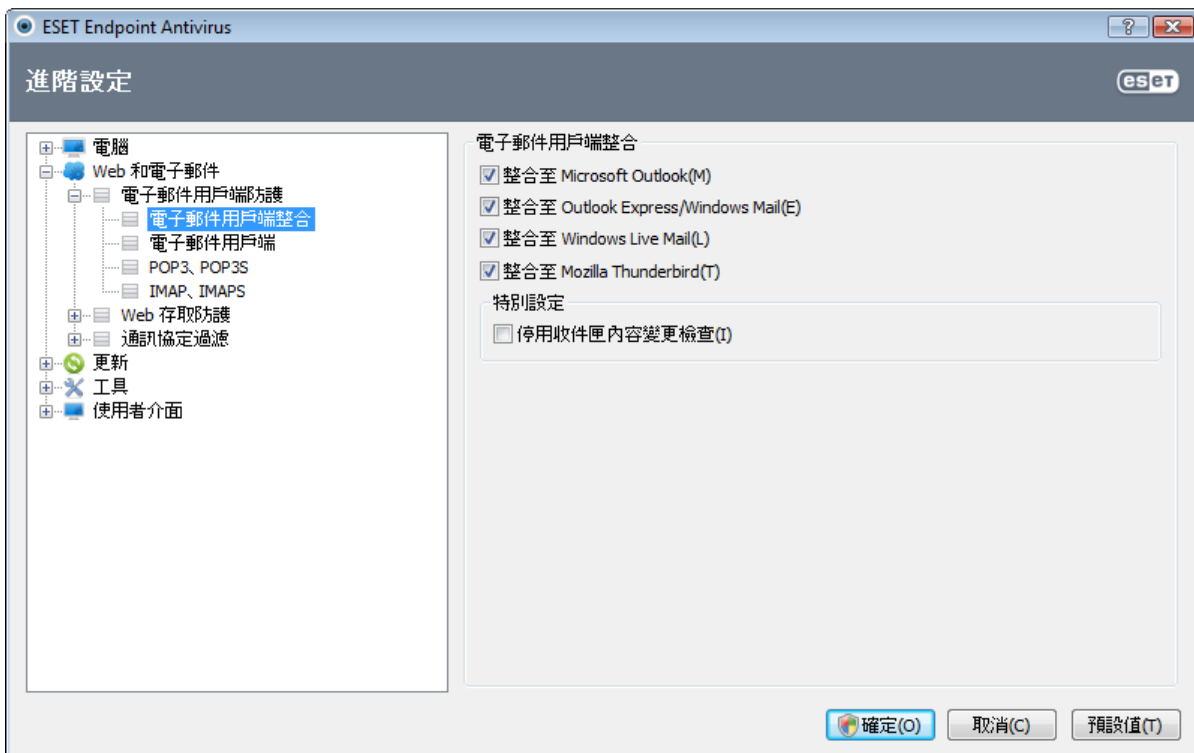


#### 4.2.2.3 與電子郵件用戶端整合

ESET Endpoint Antivirus 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 Endpoint Antivirus 中啟用此整合。如果啟用整合，ESET Endpoint Antivirus 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。可以在 [設定] > [進入進階設定...] > [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 及 Mozilla Thunderbird。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發生系統速度減慢，請選取 [停用收件匣內容變更檢查] 旁的核取方塊。從 Kerio Outlook Connector Store 下載電子郵件時可能會發生此類情況。



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。

#### 4.2.2.3.1 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。外掛程式控制項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。

##### 要掃描的電子郵件

- 已接收電子郵件 - 可切換接收郵件的檢查。
- 已傳送電子郵件 - 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。
- 將電子郵件移到資料夾 - 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。

##### 其他

- 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的掃描結果。

#### 4.2.2.4 移除入侵

如果收到受感染的電子郵件訊息，則將顯示警告視窗。警告視窗顯示寄件者名稱、電子郵件，以及入侵的名稱。在視窗下半部，有可用於已偵測到物件的 [清除]、[刪除] 或 [保留] 選項。在大多數情況下，我們建議您選取 [清除] 或 [刪除]。在某些情況下，如果您想要接收受感染的檔案，請選取 [保留]。如果已啟用 [完全清除]，則會顯示沒有可用於受感染物件之選項的資訊視窗。

#### 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，該控制都會自動運作。對於 SSL 加密通訊請檢閱 [通訊協定過濾] > [SSL]。

整合至系統 - 啟用 ESET Endpoint Antivirus 通訊協定過濾功能的驅動程式。

啟用應用程式通訊協定內容過濾 - 如果啟用，則防毒掃描器將檢查所有 HTTP(S)、POP3(S) 及 IMAP(S) 流量。

附註：從 Windows Vista Service Pack 1 與 Windows 7 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，因此無法使用下列選項：

- **HTTP 及 POP3 連接埠** - 將流量路由傳送給內部 Proxy 伺服器限制於 HTTP 及 POP3 連接埠。
- 已標記為 **Web 瀏覽器** 與電子郵件用戶端的應用程式 - 將流量路由傳送給內部 Proxy 伺服器限制於標記為瀏覽器及電子郵件用戶端的應用程式 ([Web 和電子郵件] > [通訊協定過濾] > [Web 和電子郵件用戶端])。
- 已標記為 **Web 瀏覽器** 或電子郵件用戶端的應用程式和連接埠 - 針對 HTTP 及 POP3 連接埠，以及標記為瀏覽器與電子郵件用戶端的應用程式所有通訊啟用路由傳送，傳送到內部 Proxy 伺服器。

#### 4.2.3.1 Web 和電子郵件用戶端

附註：從 Windows Vista Service Pack 1 與 Windows 7 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。

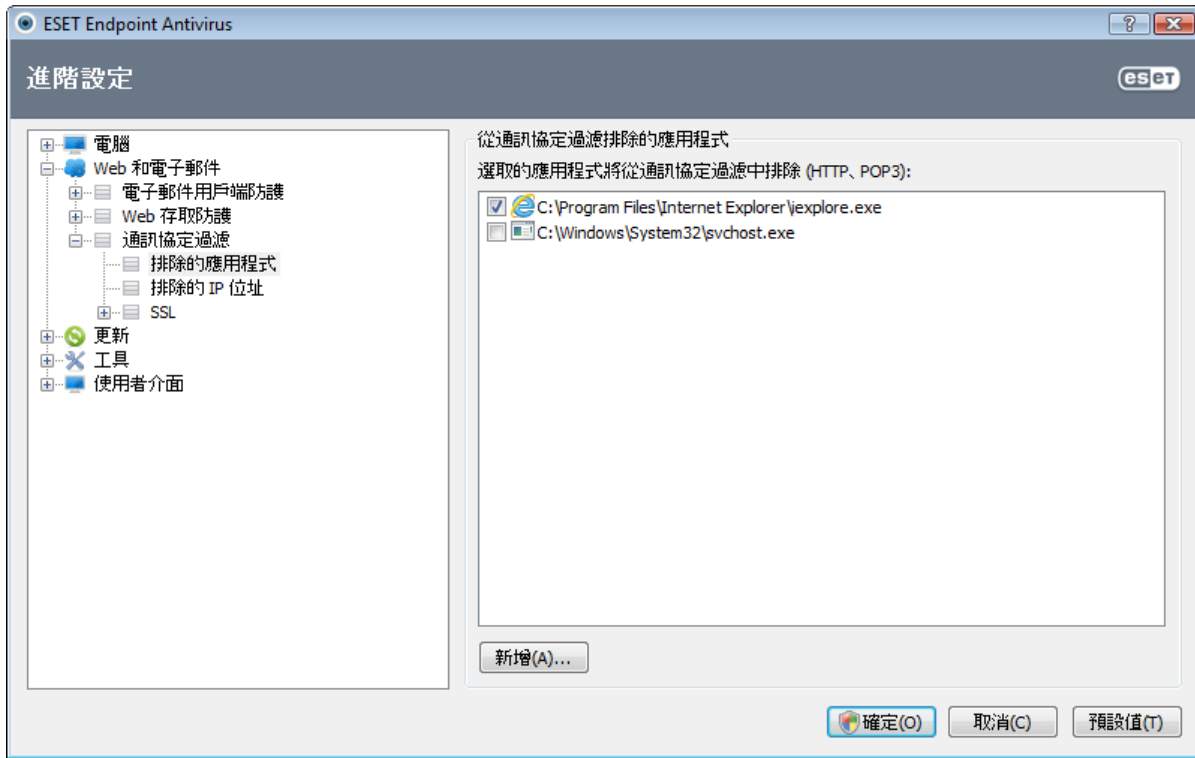
由於在網際網路周圍散佈著大量的惡意代碼，因此能安全地瀏覽網際網路是電腦防護非常重要的面向。網路瀏覽器的弱點和詐騙連結會幫助惡意代碼在不被察覺的情況下進入系統，這也就是 ESET Endpoint Antivirus 著重在網路瀏覽器安全性的原因之一。每個存取網路的應用程式都可以標記為網際網路瀏覽器。核取方塊有兩種狀態：

- **未點選** - 只過濾使用指定連接埠的應用程式通訊。
- **點選** - 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...] 按鈕，手動選取未顯示於通訊協定過濾清單上的應用程式。

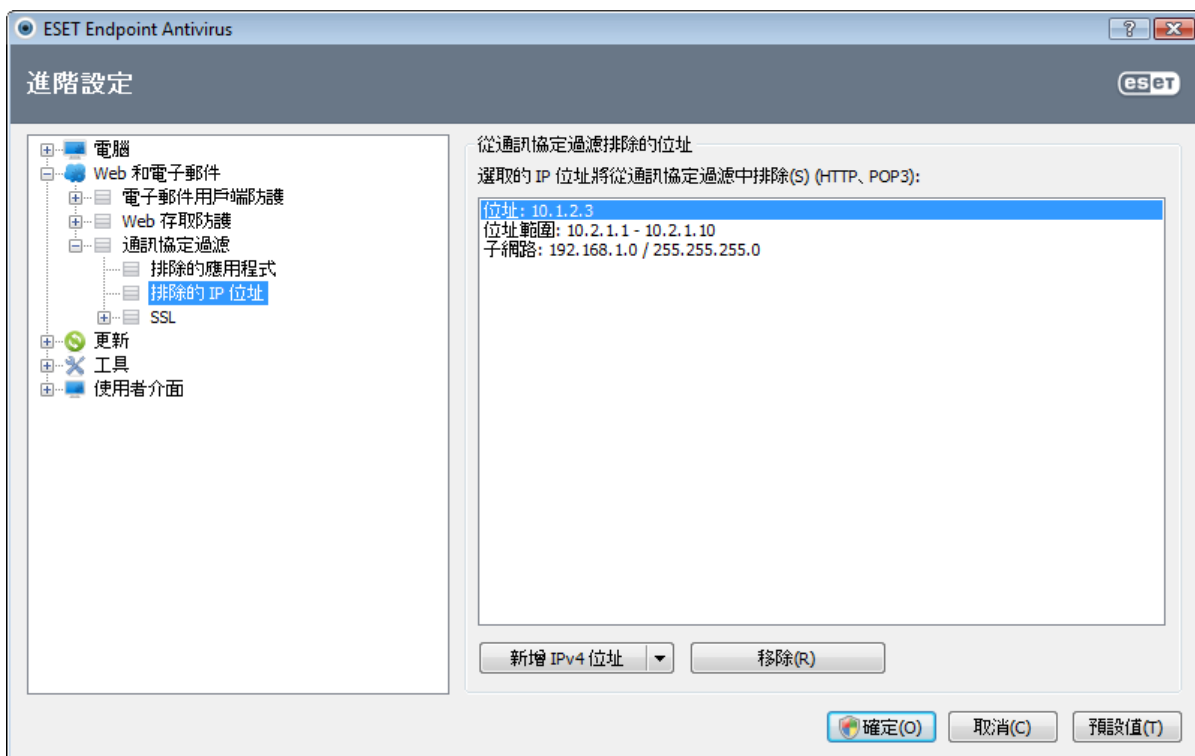


#### 4.2.3.3 排除的 IP 位址

在位址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值得信賴的位址。

**新增 IPv4/IPv6 位址** - 此選項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。

**移除** - 從清單中移除選取的項目。



#### 4.2.3.3.1 新增 IPv4 位址

此選項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。

**單一地址** - 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

此選項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。

**單一地址** - 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 通訊協定檢查

ESET Endpoint Antivirus 能夠讓您檢查 SSL 通訊協定中封裝的通訊協定。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。

**一律掃描 SSL 通訊協定** - 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。存取含有您標記為信任的不信任憑證 (新增至信任憑證清單) 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。

**詢問未造訪的網站 (可以設定排除)** - 如果您輸入新的 SSL 防護網站 (含有未知憑證)，則會顯示動作選取項目對話方塊。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。

**不掃描 SSL 通訊協定** - 如果選取，程式將不會掃描透過 SSL 的通訊。

**套用根據憑證建立的例外** - 啟用排除及受信任憑證中指定的排除來掃描 SSL 通訊。如果您選取 [**一律掃描 SSL 通訊協定**]，便可使用此選項。

**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。

#### 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, spol. s r.o. 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。因此，應該啟用 [**將系統管理員的憑證新增至已知瀏覽器**] 選項。選取此選項可自動將 ESET 根憑證新增至已知瀏覽器中 (如 Opera、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。如果選取 [**詢問憑證有效性**] 選項 (預設)，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，讓你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**] 選項，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。

#### 4.2.3.4.1.1 信任的憑證

除了 ESET Endpoint Antivirus 用來儲存信任憑證的整合「信任的根憑證授權」儲存區之外，您也可以建立將信任的憑證列出的自訂清單，而此清單可在 [進階設定] (F5) > [Web 和電子郵件] > [通訊協定過濾] > [SSL] > [憑證] > [信任的憑證] 中檢視。ESET Endpoint Antivirus 會檢查利用此清單中之憑證的加密通訊內容。

若要從清單中刪除選取的項目，請按一下 [移除] 按鈕。按一下 [顯示] 選項 (或按兩下憑證)，以顯示所選憑證的相關資訊。

#### 4.2.3.4.1.2 排除的憑證

[排除的憑證] 區段含有被視為安全的憑證。利用清單中的憑證進行加密通訊的內容將不會被掃描是否有威脅。我們建議您只排除保證安全的網站憑證，以及使用這些憑證的通訊不需要接受檢查。若要從清單中刪除選取的項目，請按一下 [移除] 按鈕。按一下 [顯示] 選項 (或按兩下憑證)，以顯示所選憑證的相關資訊。

#### 4.2.3.4.1.3 加密的 SSL 通訊

如果配置電腦進行 SSL 通訊協定掃描，則當嘗試建立加密通訊 (使用未知憑證) 時會開啟對話方塊視窗，提示您選擇處理方法。對話方塊視窗包含下列資訊：啟動通訊的應用程式名稱及使用憑證的名稱。



如果憑證不在「信任的根憑證授權」儲存區中，則會視為不信任的憑證。



下列處理方法可用於憑證：

是 - 暫時針對目前工作階段將憑證標記為信任憑證 - 在下次嘗試使用憑證時，不會顯示警告視窗。

一律為是 - 將憑證標記為信任憑證，並將其新增至信任憑證清單 - 不會針對信任憑證顯示警告視窗。

否 - 針對目前工作階段將憑證標記為不信任憑證 - 在下次嘗試使用憑證時，會顯示警告視窗。

排除 - 將憑證新增至排除憑證的清單 - 透過指定加密通道傳輸的資料將完全不受檢查。



### 4.3 更新程式

定期更新 ESET Endpoint Antivirus 是讓電腦維持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] 可以尋找目前更新狀態，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。

此外，其中有手動啟動更新程序的選項 [更新病毒資料庫] 可供使用。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。如果安裝期間沒有輸入授權詳情 (使用者名稱與密碼)，您可以在更新時輸入使用者名稱和密碼，以存取 ESET 更新伺服器。

附註: 購買 ESET Endpoint Antivirus 後，ESET 會提供您的使用者名稱和密碼。



上一次成功更新 - 上次更新的日期。請確認系統是指出最近的日期，表示病毒資料庫是最新的。

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。

## 更新處理程序

按一下 [更新病毒資料庫] 之後，即開始下載處理程序。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 [中止]。



**重要：** 在正常情況下，適當地下載更新之後，[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：

**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。

前一個通知與下列關於失敗更新的兩項 [病毒資料庫更新失敗] 訊息相關：

1. **無效的使用者名稱和/或密碼** - 在更新設定中，已錯誤地輸入使用者名稱及密碼。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 [進入進階設定...]，或按鍵盤上的 F5) 包含其他的更新選項。在 [進階設定] 樹狀目錄中按一下 [更新] > [一般]，以輸入新的使用者名稱及密碼。



2. 下載更新檔案時發生錯誤 - 此錯誤可能是因不正確的[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。



#### 4.3.1 更新設定

可從 [進階設定] 樹狀目錄 (F5 鍵) 中取得更新設定選項, 做法是按一下 [更新] > [一般]. 此定區段指定更新來源資訊, 如更新伺服器及這些伺服器的驗證資料。依預設, [更新伺服器] 下拉式功能表設定為 [自動選擇], 確保自動從 ESET 以最小網路流量自動下載更新檔案。

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



目前使用的更新設定檔顯示在 [已選取的設定檔] 下拉式功能表中。按一下 [設定檔...] 以建立新設定檔。

透過 [更新伺服器] 下拉式功能表即可存取可用更新伺服器的清單。更新伺服器是儲存更新的位置。如果您使用 ESET 伺服

器，請保持選取預設選項 [自動選擇]。若要新增更新伺服器，請按一下 [更新已選設定檔的設定] 區段中的 [編輯...]，然後按一下 [新增] 按鈕。

當使用本機 HTTP 伺服器 (也稱為「映像」) 時，更新伺服器應該進行設定，如下所示：

http://computer\_name\_or\_its\_IP\_address:2221

當透過 SSL 使用本機 HTTP 伺服器時，更新伺服器應設定如下：

https://computer\_name\_or\_its\_IP\_address:2221

更新伺服器的驗證是根據在購買後產生並傳送給您的 [使用者名稱] 與 [密碼]。當使用本機「映像」伺服器時，驗證視其配置而定。依預設，不需要任何驗證，即 [使用者名稱] 與 [密碼] 欄位為空。

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。在 [說明及支援] > [關於] ESET Endpoint Antivirus 中可找到目前模組清單。建議初級使用者將 [定期更新] 選項保留為預設的選取狀態。商務使用者可選取 [延遲更新] 選項從特殊更新伺服器更新，該伺服器會延遲至少 X 小時再提供新版的病毒資料庫，亦即資料庫已在實際環境中測試，因此可視為穩定。

按一下 [進階更新設定] 旁邊的 [設定] 按鈕，即可顯示含有進階更新選項的視窗。

如果更新遭遇問題，請按一下 [清除...] 按鈕，清除含有暫時更新檔案的資料夾。

不顯示成功更新的通知 - 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。

#### 4.3.1.1 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，行動使用者可以為定期變更的網際網路連線內容建立替代設定檔。

[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...] 按鈕，然後按一下 [新增...] 按鈕，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。

在設定檔設定視窗中，您可以從可用伺服器清單指定更新伺服器，也可以新增伺服器。[更新伺服器] 下拉式功能表中列出現有的更新伺服器清單。若要新增更新伺服器，請按一下 [更新已選設定檔的設定] 區段中的 [編輯...]，然後按一下 [新增] 按鈕。

#### 4.3.1.2 進階更新設定

若要檢視進階更新設定，請按一下 [設定...] 按鈕。進階更新設定選項包含 [更新模式]、[HTTP Proxy]、[LAN 和映像]。

##### 4.3.1.2.1 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。它可自動執行而無需使用者介入，或者您也可以選擇提前通知。安裝程式元件更新之後，可能需要重新啟動電腦。[程式元件更新] 區段中，可用的三個選項如下：

- 絕不更新程式元件 - 絕不會執行程式元件更新。此選項適用於伺服器安裝，因為伺服器通常只有在維護時才會重新啟動。
- 一律更新程式元件 - 自動下載並安裝程式元件更新。請記得系統可能要求重新啟動電腦。
- 下載程式元件前詢問 - 預設選項。將提示您確認或拒絕提供使用的程式元件更新。

程式元件更新之後，可能需要重新啟動電腦，以提供所有模組的完整功能。[程式元件升級後重新啟動] 可讓您選取下列選項之一：

- 不要重新啟動電腦 - 即使需要，系統也不會要求您重新啟動。請注意，不建議您這樣做，因為電腦可能直到下一次重新啟動時才會正常運作。
- 必要時重新啟動電腦 - 預設選項。在程式元件更新之後，對話方塊視窗中會提示您重新啟動電腦。
- 必要時不通知即重新啟動電腦 - 程式元件升級後，必須重新啟動電腦 (如果需要的話)。

附註：選取最適當的選項需視將套用設定的工作站而定。請注意，工作站與伺服器之間有區別，例如，程式升級後自動重新啟動伺服器會導致嚴重損毀。

若 [下載更新前詢問] 選項已勾選，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] 欄位中指定的值，程式將顯示通知。

#### 4.3.1.2.2 Proxy 伺服器

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 [進階更新設定] 右邊的 [設定...] 按鈕。按一下 [HTTP Proxy] 索引標籤，然後選取下列三個選項之一：

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

選取 [使用全域 Proxy 伺服器設定] 選項，將使用已經在 [進階設定] 樹狀目錄的 [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] 選項可明確定義不使用任何 Proxy 伺服器更新 ESET Endpoint Antivirus。

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 Endpoint Antivirus 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]，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 Endpoint Antivirus 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 Endpoint Antivirus 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提供。

#### 4.3.1.2.3 連線至區域網路 (LAN)

從使用 NT 型作業系統的本機伺服器更新時，預設需要每個網路連線的驗證。大多數情況下，本機系統帳戶不具有存取映像資料夾 (映像資料夾包含更新檔案的副本) 足夠的存取權限。如果是這種情況，請在更新設定區段中輸入使用者名稱及密碼，或者指定程式將存取更新伺服器 (映像) 的現有帳戶。

若要配置這類帳戶，請按一下 [區域網路 (LAN)] 索引標籤。[以下列身分連線至 LAN] 區段提供 [系統使用者 (預設值)]、[目前使用者] 及 [指定使用者] 選項。

選取 [系統使用者 (預設)] 選項，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] 選項。

#### 4.3.1.2.4 建立更新副本 - 映像

ESET Endpoint Antivirus 可讓您建立更新檔案的副本，可用於更新網路中的其他工作站。您可以很方便地建立「映像」，即 LAN 環境中更新檔案的副本，因為不需要由每個工作站從廠商更新伺服器重覆下載更新檔案。它們會集中下載至本機映像伺服器然後散佈至所有工作站，因此會避免潛在的網路流量超載的風險。從映像更新用戶端工作站會最佳化網路負載平衡，節省網際網路連線頻寬。

本機映像伺服器的配置選項可從 [進階更新設定] 區段存取 (在 ESET Endpoint Antivirus [進階設定] 區段中的[授權管理程式](#)新增有效的授權金鑰後)。若要存取此區段，請按 F5 並且按一下 [進階設定] 樹狀目錄中的 [更新]，然後按一下 [進階更新設定] 旁的 [設定...] 按鈕，並選取 [映像] 索引標籤)。



配置映像的第一個步驟是選取 [建立更新映像] 選項。選取此選項會啟動其他映像配置選項，例如存取更新檔案的方式及映像檔案的更新路徑。

透過內部 HTTP 伺服器提供更新檔案 - 如果已啟用，則透過 HTTP 即可存取更新檔案，而且不需要提供使用者名稱及密碼。按一下[進階設定...](#) 以配置延伸的映像選項。

附註：Windows XP 上的 HTTP 伺服器需要 SP2 與更新版本。

映像啟動的方法在[從映像更新](#)一節中有詳細說明。請注意，現在有存取映像的兩個基本方法 - 含有更新檔案的資料夾可以顯示為共用網路資料夾或由 HTTP 伺服器顯示。

專用於儲存映像更新檔案的資料夾定義於 [儲存映像檔案的資料夾] 區段。按一下 [資料夾...] 以瀏覽本機電腦或共用網路資料夾上的資料夾。如果需要指定資料夾的授權，必須在 [使用者名稱] 及 [密碼] 欄位中輸入驗證資料。如果選取的目標資料夾位於執行 Windows NT/2000/XP 作業系統的網路磁碟上，則指定的「使用者名稱」及「密碼」必須具有已選取資料夾的寫入權。使用者名稱及密碼的輸入格式應為 *網域/使用者* 或 *工作群組/使用者*。請記得提供對應的密碼。

配置映像時，您也可以要在要下載使用者所配置的映像伺服器中，指定目前所支援更新副本的語言版本。語言版本設定可從 [可用版本] 清單存取。

#### 4.3.1.2.4.1 從映像更新

現在有配置映像的兩個基本方法 - 含有更新檔案的資料夾可以顯示為共用網路資料夾或 HTTP 伺服器。

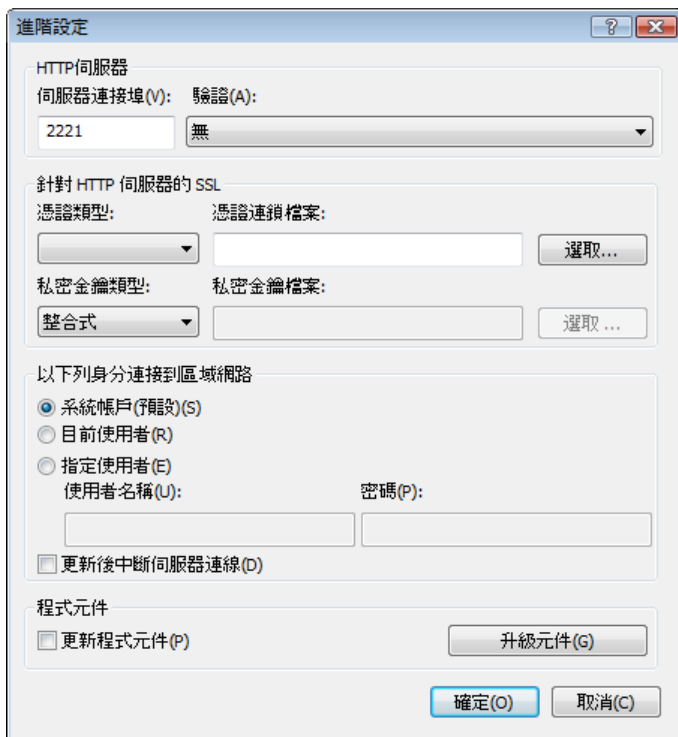
##### 使用內部 HTTP 伺服器存取映像

此組態是預先定義程式配置中指定的預設值。若要允許使用 HTTP 伺服器存取映像，請瀏覽至 [進階更新設定] (按一下 [映像] 索引標籤)，並選取 [建立更新映像] 選項。

在 [映像] 索引標籤的 [進階設定] 區段中，您可以指定 HTTP 伺服器將接聽的 [伺服器連接埠]，以及 HTTP 伺服器使用的 [驗證] 類型。依預設，伺服器連接埠設定為 2221。[驗證] 選項定義用於存取更新檔案的驗證方法。可用選項如下：[無]、[基本] 及 [NTLM]。選取 [基本] 以使用具有基本使用者名稱及密碼驗證的 base64 編碼。[NTLM] 選項提供使用安全編碼方法的編碼。對於驗證，會使用共用更新檔案之工作站上建立的使用者。預設值為 [無]，這會授與對無需驗證之更新檔案的存取權。

**警告：** 如果您想要允許透過 HTTP 伺服器的更新檔案存取，則映像資料夾必須位於 ESET Endpoint Antivirus 實例建立它時所在的電腦。

如果您想要執行支援 HTTPS (SSL) 的 HTTP 伺服器，請附加您的 [憑證連鎖檔案]，或產生自我簽署的憑證。以下為可用的類型：ASN、PEM 與 PFX。可透過 HTTPS 通訊協定下載更新檔案，此通訊協定安全性較高。使用此通訊協定幾乎不可能追蹤資料傳送與登入憑證。[私密金鑰類型] 選項預設為 [已整合] (因此 [私密金鑰檔案] 選項預設為停用)，這表示私密金鑰是所選憑證連鎖檔案的一部分。



配置映像完成之後，請移至工作站並新增更新伺服器。若要執行此處理方法，請遵循以下步驟：

- 開啟 [ESET Endpoint Antivirus 進階設定]，並按一下 [更新] > [一般]。
- 按一下 [更新伺服器] 下拉式功能表右側的 [編輯]，以使用以下其中一個格式新增伺服器：  
http://IP\_address\_of\_your\_server:2221  
https://IP\_address\_of\_your\_server:2221 (如果使用 SSL 的話)
- 從更新伺服器清單中選取新增的伺服器。

##### 透過系統共用存取映像

首先，應該在本機或網路裝置上建立共用資料夾。建立映像資料夾時，必須為將更新檔案儲存到資料夾的使用者提供「寫入」存取權，並且為將從映像資料夾更新 ESET Endpoint Antivirus 的所有使用者提供「讀取」存取權。

然後，停用 [經由內部 HTTP 伺服器提供更新檔案] 選項，配置 [映像] 索引標籤的 [進階更新設定] 區段之中的映像存取權。依預設，會在程式安裝套件中啟用此選項。

如果共用資料夾位於網路中的另一台電腦，必須輸入存取其他電腦的驗證資料。若要輸入驗證資料，請開啟 ESET Endpoint

Antivirus [進階設定] (F5)，並按一下 [更新] > [一般]。按一下 [設定...] 按鈕，然後按一下 [區域網路 (LAN)] 索引標籤。此設定與[連線至區域網路 \(LAN\)](#) 一節所說明的更新相同。

映像配置完成之後，繼續到工作站，將 \\UNC\PATH 設定為更新伺服器。使用以下步驟即可完成此作業：

- 開啟 [ESET Endpoint Antivirus 進階設定]，並按一下 [更新] > [一般]。
- 按一下 更新伺服器旁的 [編輯...]，並使用 \\UNC\PATH 格式新增伺服器。
- 從更新伺服器清單中選取新增的伺服器。

附註：若要正常發揮功能，映像資料夾的路徑必須指定為 UNC 路徑。來自對應磁碟機的更新不會運作。

最後一個區段控制程式元件 (PCU)。依預設，下載的程式元件已準備好複製到本機映像。如果已選取 [更新程式元件] 旁邊的核取方塊，則不需要按一下 [升級元件]，因為檔案會在備妥時自動複製到本機映像。如需程式元件更新的詳細資訊，請參閱[更新模式](#)。

#### 4.3.1.2.4.2 疑難排解映像更新問題

大部分情況下，導致從映像伺服器更新期間發生問題的一個或多個原因如下：[映像] 資料夾選項的不正確指定、對 [映像] 資料夾資料的不正確驗證、對嘗試從映像下載更新檔案之本機工作站的不正確配置，或以上原因的組合。以下提供從映像更新期間經常可能發生之問題的概觀：

連接至映像伺服器時，ESET Endpoint Antivirus 報告錯誤 - 可能的原因是本機工作站下載更新所在更新伺服器 (映像資料夾的網路路徑) 的指定不正確。若要驗證資料夾，請按一下 Windows [開始]，並按一下 [執行]，然後輸入資料夾名稱，並按一下 [確定]。畫面上應該會顯示資料夾內容。

ESET Endpoint Antivirus 需要使用者名稱及密碼 - 可能由於更新區段中不正確的驗證資料 (使用者名稱及密碼) 所致。使用者名稱及密碼用於授與更新伺服器 (程式更新位置) 的存取權。請確定驗證資料正確，且以正確的格式輸入。例如，*網域/使用者名稱或工作群組/使用者名稱*，以及對應的「密碼」。如果「每個人」都可以存取映像伺服器，請注意這並不表示授與所有人存取權。「每個人」不表示所有未授權的使用者，僅表示每個網域使用者都可以存取資料夾。因此，如果「每個人」都可以存取資料夾，則更新設定區段中仍需要輸入網域使用者名稱及密碼。

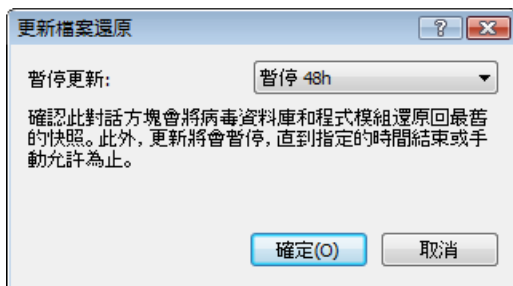
連接至映像伺服器時，ESET Endpoint Antivirus 報告錯誤 - 封鎖定義用於存取 HTTP 版本映像之連接埠的通訊。

#### 4.3.1.3 更新還原

如果您懷疑病毒資料庫的新更新不穩定或損壞，您可以還原回上一版，並停用所選期間的任何更新。或者，您可以啟用先前停用的更新。

ESET Endpoint Antivirus 提供病毒資料庫的模組備份與還原功能 (所謂的還原)。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] 欄位可定義儲存在本機電腦檔案系統中先前病毒資料庫快照的數目。

如果您按一下 [還原] ([進階設定] (F5) > [更新] > [進階])，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。



如果您想要手動允許定期更新，請選取 [直到取消為止]。由於這有潛在性安全風險，因此不建議選取此選項。

如果還原已啟用，則 [還原] 按鈕會變成 [允許更新]。不允許在從 [時間間隔] 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，因為電腦長時間關機。如果您在 [儲存於本機的快照數目] 欄位中輸入二 (2)，並按一下 [還原]，則病毒資料庫將還原回編號 6868 的版本。此程序可能需要一些時間。從 ESET Endpoint Antivirus 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。



本機映像伺服器的配置選項可從 [ESET Endpoint Antivirus 進階更新設定] 區段存取 (在[授權管理程式](#)新增有效的授權金鑰後)。如果您使用工作站作為映像，則更新副本必須已接受最新的「最終用戶許可協議」(EULA)，才能建立更新副本作為副本更新檔案，以用於更新網路中其他的工作站。如果更新時有最新版的 EULA，則會顯示對話視窗 60 秒以進行確認。若要手動確認，請按一下本視窗 [PCU 授權] 區段中的 [設定...]。



#### 4.3.2 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 Endpoint Antivirus 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。

## 4.4 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。



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](#)
- [排程器](#)
- [隔離區](#)
- [ESET SysInspector](#)

[提交檔案以供分析](#) - 可讓您將可疑檔案提交至 ESET 病毒實驗室以供分析。按一下此選項之後所顯示的對話方塊視窗，在[提交檔案以供分析](#)一節中會加以說明。

ESET SysRescue - 啟動 ESET SysRescue 建立精靈。

#### 4.4.1 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 Endpoint Antivirus 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] > [防護記錄檔案]，可存取防護記錄。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 Endpoint Antivirus 模組所偵測到入侵的詳細資訊。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 Endpoint Antivirus 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規則的記錄。通訊協定會顯示稱為作業、結果 (是否允許或禁止規則)，及已建立規則名稱的應用程式。
- **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，選取項目並按一下 [複製]，可將顯示的資訊直接複製到剪貼簿 (鍵盤快捷鍵 Ctrl + C)。若要選取多個項目，可使用 CTRL 和 SHIFT 鍵。

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：

- 過濾相同類型的記錄 - 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 [防護記錄過濾] 視窗，您可以在其中定義過濾條件。
- 停用過濾 - 清除所有過濾器設定值 (如上所述)。
- 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。
- 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，並且監控 [防護記錄檔案] 視窗中的作用中防護記錄。

#### 4.4.1.1 防護記錄維護

ESET Endpoint Antivirus 的防護記錄檔案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]。防護記錄檔案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：

**自動刪除超過指定 (天數) 的記錄** - 將自動刪除超過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 [立即最佳化]，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，以提升處理防護記錄的效能及速度。如果防護記錄包含大量的項目，則可明顯察覺此提升效果。

**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 (啟動病毒防護等時發生錯誤)。

按一下 [啟用文字通訊協定] 以另一種檔案格式儲存防護記錄，並儲存在 [防護記錄檔案](#) 之外：

- 類型 - 如果您選擇 [一般] 檔案格式，則會將防護記錄將儲存成文字檔，並以 Tab 分隔資料。這也同樣適用於以逗號分隔的 [CSV] 檔案格式。如果您選擇 [事件]，相對於檔案，防護記錄將儲存在 Windows 事件防護記錄中 (可使用控制台中的事件檢視器來檢視)。
- 目標目錄 - 儲存檔案的位置 (僅適用於 [一般]/[CSV])。每個防護記錄區段都有自己已預先定義檔名的檔案 (例如，如果您使用純文字檔案格式儲存防護記錄，則防護記錄檔中 [偵測到威脅] 區段的檔名為 virlog.txt)。

[刪除防護記錄] 按鈕會清除目前在 [類型] 下拉式功能表中選取的所有已儲存防護記錄。

#### 4.4.2 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 Endpoint Antivirus 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。



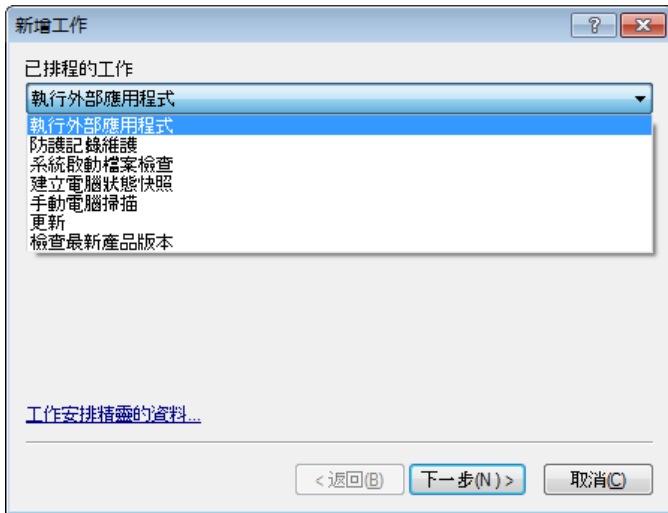
依預設，下列排定工作會顯示在 [排程器] 中：

- 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
- 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)

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...] 按鈕。

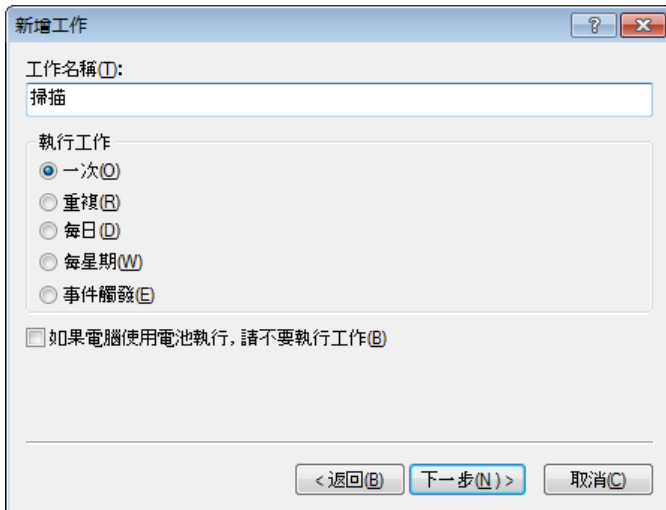
#### 新增工作

1. 按一下視窗底部的 [新增 ]。
2. 自下拉式功能表選取想要的工作。



3. 輸入工作名稱並選取任一個時間選項：

- 一次 - 工作僅會在預先定義的日期及時間執行一次。
- 重複 - 工作將在指定的時間間隔內執行 (以小時為單位)。
- 每日 - 工作會每天在指定的時間執行。
- 每星期 - 工作每星期在選取的日期及時間執行一或多次。
- 事件觸發 - 工作會在指定的事件發生時執行。



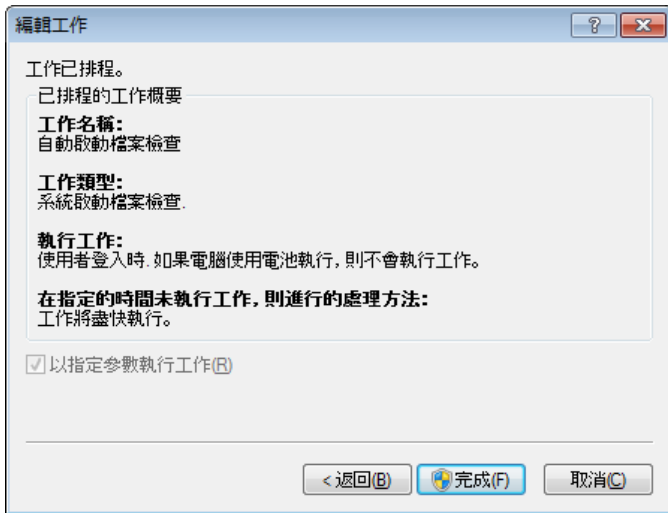
4. 視先前步驟中選擇的時間設定選項而定，將顯示以下其中一個對話方塊視窗：

- 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。

5. 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：

- 等到下一個已排程的時間
- 盡快執行工作
- 如果距離上次執行工作的時間超過指定的小時數，則立即執行工作

6. 在前一步驟中，您可以檢閱要排程的工作。按一下 [完成] 以套用工作。



#### 4.4.2.1 建立新工作

若要在 [排程器] 中建立新工作，請按一下 [新增...] 按鈕，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。
- 電腦掃描 - 針對電腦中的檔案及資料夾執行電腦掃描。
- 更新 - 更新病毒資料庫及更新系統元件來排程更新工作。

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]。按一下 [下一步]，並且在 [工作名稱] 欄位中輸入工作的名稱。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]。使用 [如果電腦使用電池執行，請不要執行工作] 選項，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。系統會根據選取的頻率，提示您不同的更新參數。接著，定義排程期間無法執行或完成工作時要採取的處理方法。可用的三個選項如下所示：

- 等到下一個已排程的時間
- 盡快執行工作
- 如果距離上次執行工作的時間超過指定的時間間隔，則立即執行工作 (可以使用 [工作間隔] 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，應會自動啟用 [以指定參數執行工作] 選項。按一下 [完成] 按鈕。

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，您可以指定主要設定檔及替代設定檔 (用於使用主要設定檔無法完成工作的情況中)。按一下 [更新設定檔] 視窗中的 [確定] 來確認。新排程工作將新增至目前排程工作清單。

#### 4.4.3 防護統計

若要檢視與 ESET Endpoint Antivirus 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：

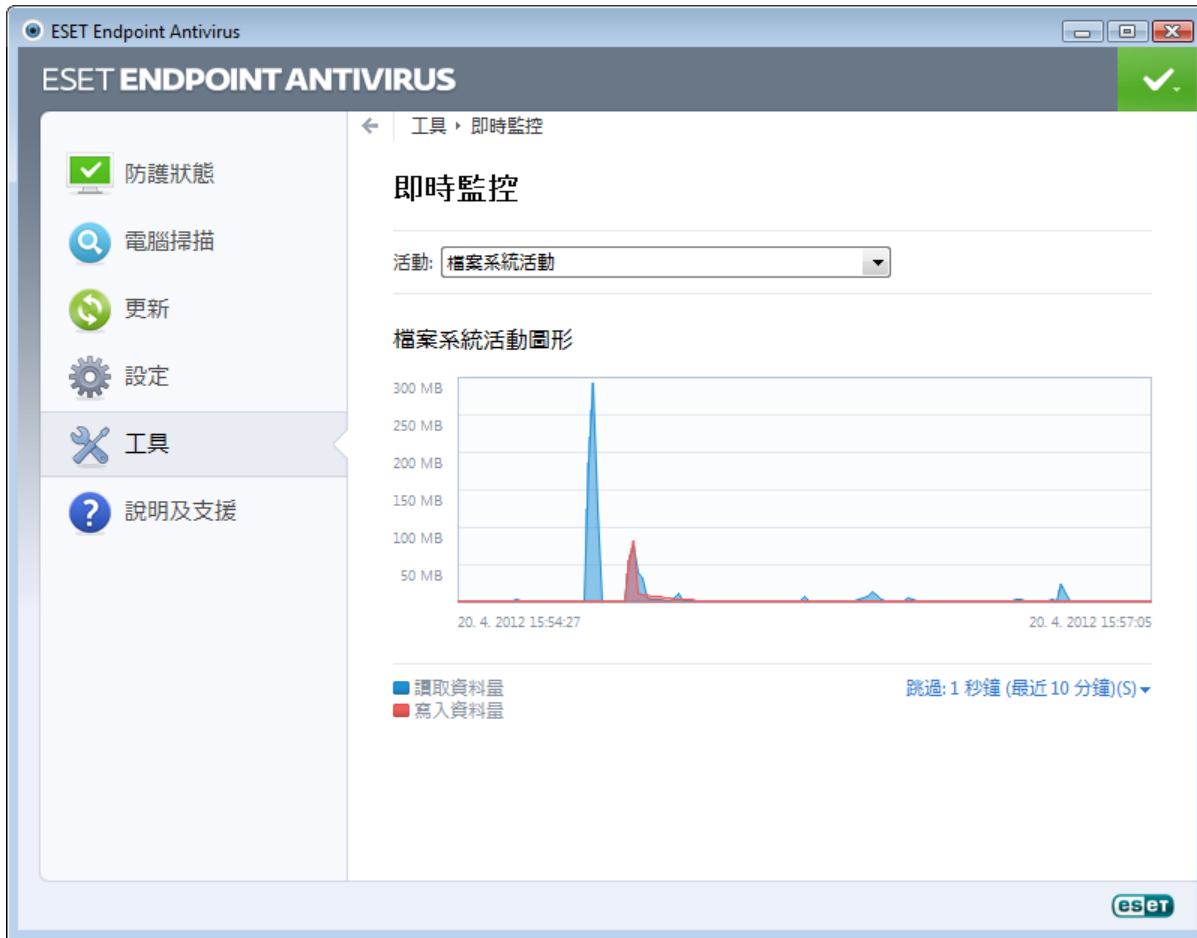
- 病毒及間諜程式防護 - 顯示受感染及已清除的物件數目。
- 檔案系統防護 - 只顯示已讀取或寫入檔案系統的物件。
- 電子郵件用戶端防護 - 只顯示電子郵件用戶端傳送或接收的物件。
- **Web** 存取防護 - 只顯示 Web 瀏覽器下載的物件。

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，以及統計資料時間戳。按一下 [重設] 以清除所有的統計資訊。



#### 4.4.4 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] > [即時監控]。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，請按一下位於視窗右下方的 [跳過 1...] 選項。



可用選項如下：

- 跳過：1 秒鐘 (最近 10 分鐘) - 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 (藍色) 及已寫入資料 (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。

#### 4.4.5 ESET SysInspector

[ESET SysInspector](#) 是全面檢查電腦、收集系統元件 (例如已安裝的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：

- 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 防護記錄完成 ([狀態] 顯示為已建立)。
- 刪除 - 從清單移除選取的防護記錄。

以滑鼠右鍵按一下一個或多個選取的防護紀錄後，內容功能表中即有以下選項可供使用：

- 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)。
- 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。

#### 4.4.6 ESET Live Grid

ESET Live Grid (下一代的 ESET ThreatSense.Net) 是一個進階的警告系統，它會根據聲譽抵抗接踵而來的新威脅。利用從「雲端」功能所提供的威脅相關資訊的即時串流，ESET 病毒實驗室力求將防護功能維持在最新狀態，以持續提供防護服務。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 Live Grid 取得的其他資訊。有兩個選項：

1. 您可以決定不啟用 ESET Live Grid。您不會失去軟體的任何功能，而且仍會收到我們提供的最佳防護。
2. 您可以配置 ESET Live Grid，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 Live Grid 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 Endpoint Antivirus 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 Live Grid 設定功能表提供數個用於啟用/停用 ESET Live Grid 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 Live Grid]，即可從 [進階設定] 樹狀目錄中存取該設定。

參與 **ESET Live Grid** - 啟用/停用 ESET Live Grid，該系統可用來將可疑檔案及匿名統計資訊提交至 ESET 實驗室。

不提交統計 - 如果不想從 ESET Live Grid 提交有關您電腦的匿名資訊，請選取此選項。這項資訊與新偵測到的威脅有關，其中可能包括入侵名稱、偵測到威脅的日期與時間的相關資訊、ESET Endpoint Antivirus 版本、電腦作業系統版本與「位置」設定的相關資訊。在一般情況下，每天會將統計傳遞到 ESET 伺服器一或兩次。

不提交檔案 - 在內容或行為上類似於入侵的可疑檔案不可透過 ESET Live Grid 技術提交至 ESET 以進行分析。

進階設定... - 開啟視窗以進一步執行 ESET Live Grid 設定。

如果您使用過 ESET Live Grid 但現已停用，則可能還有待傳送的資料套件。即使已停用，此類套件仍會在下個時段傳送到 ESET。之後，便不會繼續建立套件。

##### 4.4.6.1 可疑檔案

ESET Live Grid 進階設定的 [檔案] 索引標籤可讓您配置將威脅提交至 ESET 病毒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威脅實驗室進行分析。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。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。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。

在此區段中，您也可以選擇檔案與統計資訊是透過 ESET Remote Administrator 提交或直接提交至 ESET。如果您要確定可疑檔案與統計資訊會傳遞至 ESET，請選取 [透過 Remote Administrator 或直接提交至 ESET] 選項。在此狀況下，會透過所有可用的方法提交檔案與統計資訊。透過 Remote Administrator 提交可疑檔案時，會將檔案與統計資訊提交到遠端管理伺服器，這可確保這些檔案與資訊之後會提交至 ESET 病毒實驗室。如果選取 [直接提交至 ESET] 選項，則會將所有可疑檔案與統計資訊直接從程式傳送至 ESET 病毒實驗室。

選取 [啟用記錄] 選項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。

#### 4.4.7 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 Endpoint Antivirus 可提供執行中處理程序的詳細資訊，以使用 [ESET Live Grid](#) 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 Endpoint Antivirus 和 ESET Live Grid 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)，將排除在掃描名單之外，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 ESET Live Grid 技術收集。

**發現時間** - 應用程式由 ESET Live Grid 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 的病毒實驗室。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。

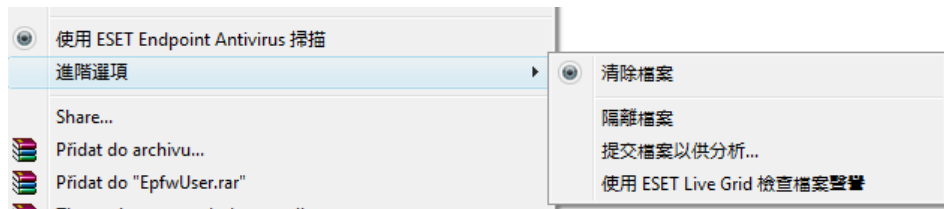
**應用程式名稱** - 程式或處理程序的指定名稱。

**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 kB 或 MB 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。

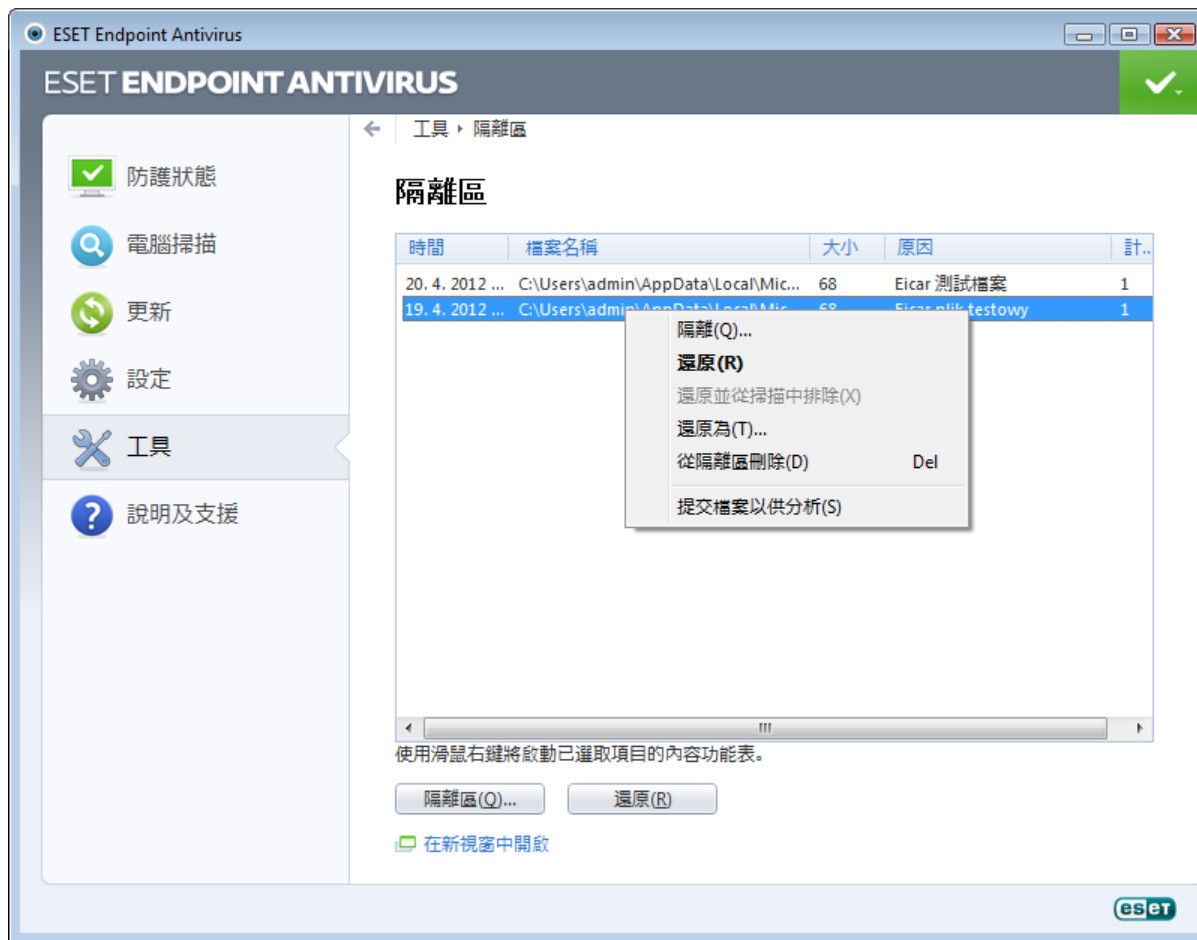
附註：聲譽也可在不作為執行中程式/處理程序的檔案上檢查 - 標記您要檢查的檔案，並以滑鼠右鍵按一下這些檔案，然後從 [內容功能表](#) 選取 [進階選項] > [使用 ESET Live Grid 檢查檔案聲譽]。



#### 4.4.8 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 Endpoint Antivirus 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 病毒實驗室進行分析。



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 Endpoint Antivirus 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]。

#### 4.4.9 提交檔案以供分析

[檔案提交] 對話方塊可讓您將檔案傳送給 ESET 以供分析，而這個對話方塊可在 [工具] > [提交檔案以供分析] 中找到。如果您在電腦中發現行跡可疑的檔案，您可以將其提交至 ESET 的病毒實驗室以供分析。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。

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](mailto: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：

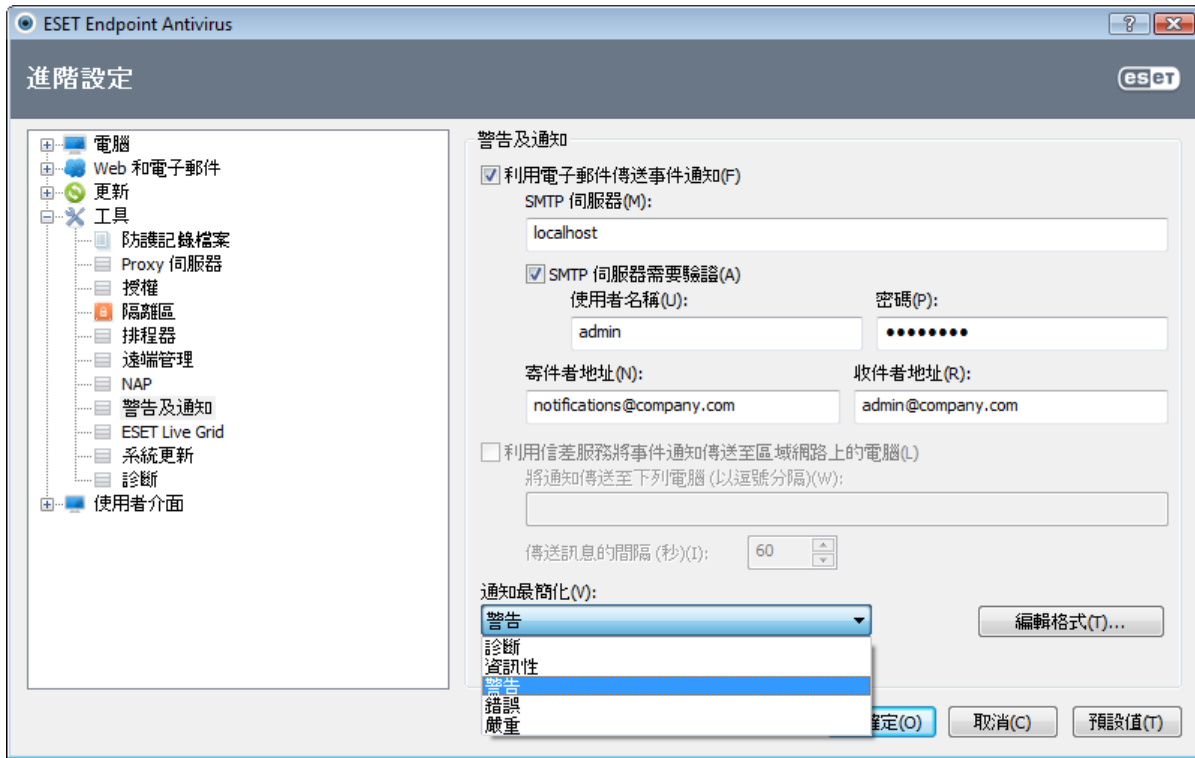
- 可疑檔案、
- 誤判 (偵測為感染但實際上未受感染的檔案)、
- 和其他。

檔案 - 要提交的檔案路徑。

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。

#### 4.4.10 警告及通知

如果發生與所選簡化層級相關的事件，則 ESET Endpoint Antivirus 支援傳送電子郵件。按一下 [利用電子郵件傳送事件通知] 核取方塊，以啟用此功能並啟動電子郵件通知。



**SMTP 伺服器** - 用於傳送通知的 SMTP 伺服器。

附註：ESET Endpoint Antivirus 不支援具備 SSL/TLS 加密功能的 SMTP 伺服器。

**SMTP 伺服器需要驗證** - 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，以授與 SMTP 伺服器的存取權限。

**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。

**利用信差服務將事件通知傳送至區域網路上的電腦** - 選取此核取方塊，透過 Windows R 傳訊服務將訊息傳送至區域網路上的電腦。

**將通知傳送至下列電腦 (以逗點分隔)** - 輸入將透過 Windows R 傳訊服務接收通知的電腦名稱。

**傳送訊息的間隔 (秒)** - 若要變更透過 LAN 傳送之通知間的間隔長度，請輸入想要的時間間隔 (以秒為單位)。

**通知最簡化** - 指定要傳送通知的最小冗贅層級。

**編輯格式...** - 程式與遠端使用者或系統管理員之間的通訊是透過電子郵件或區域網路訊息 (使用 Windows R 傳訊服務) 來完成的。在大部分情況下，警告訊息及通知的預設格式是最佳的。在部分情況下，您可能需要變更訊息格式 - 按一下 [\[編輯格式...\]](#)。

#### 4.4.10.1 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不勾選，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 (ae bu) 傳輸特殊國家字元。

#### 4.4.11 系統更新

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 Endpoint Antivirus 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。

#### 4.4.12 診斷

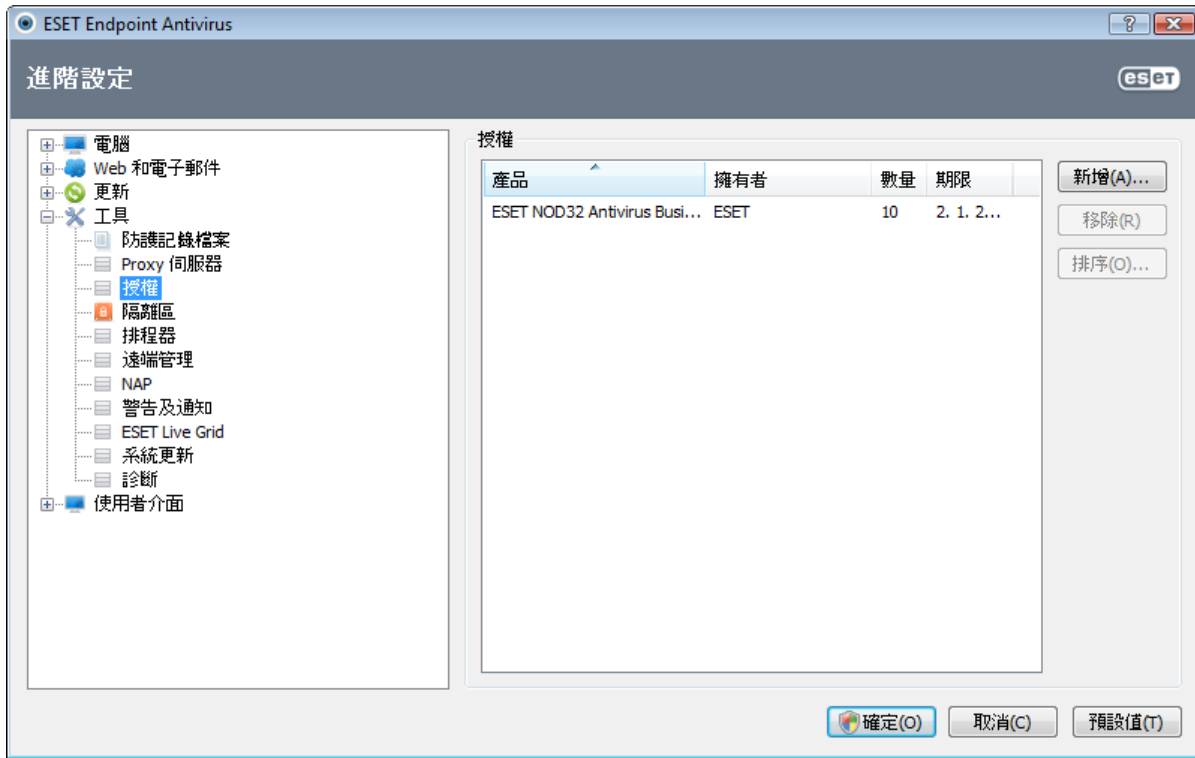
診斷可提供 ESET 處理程序 (例如 ekrm) 的應用程式當機傾印。如果應用程式當機，就會產生傾印。這可以協助開發人員除錯和修正各種 ESET Endpoint Antivirus 問題。有兩種傾印類型可以使用：

- 完整記憶體傾印 - 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。
- 最小傾印 - 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。
- 選取 **[不產生記憶體傾印]** (預設值) 以停用此功能。

目標目錄 - 在當機期間產生傾印的目錄。按一下 **[開啟資料夾...]**，在新的 **[Windows 檔案總管]** 視窗內開啟此目錄。

#### 4.4.13 授權

**[授權]** 子目錄可讓您管理 ESET Endpoint Antivirus 及其他 ESET 產品，例如 ESET Remote Administrator 的授權金鑰。購買之後，授權金鑰會與您的使用者名稱及密碼一起傳送。若要 **[新增/移除]** 授權金鑰，請按一下授權管理程式 (**[授權]**) 視窗中的相應按鈕。按一下 **[工具]** > **[授權]**，則可從 **[進階設定]** 樹狀目錄存取授權管理程式。



授權金鑰是包含所購買產品相關資訊的文字檔案：其擁有者、授權數量及到期日。

授權管理程式視窗可讓您上傳及檢視授權金鑰的內容，使用 **[新增...]** 按鈕，包含的資訊會顯示在管理程式中。若要從清單刪除授權檔案，請選取該檔案，再按一下 **[移除]**。

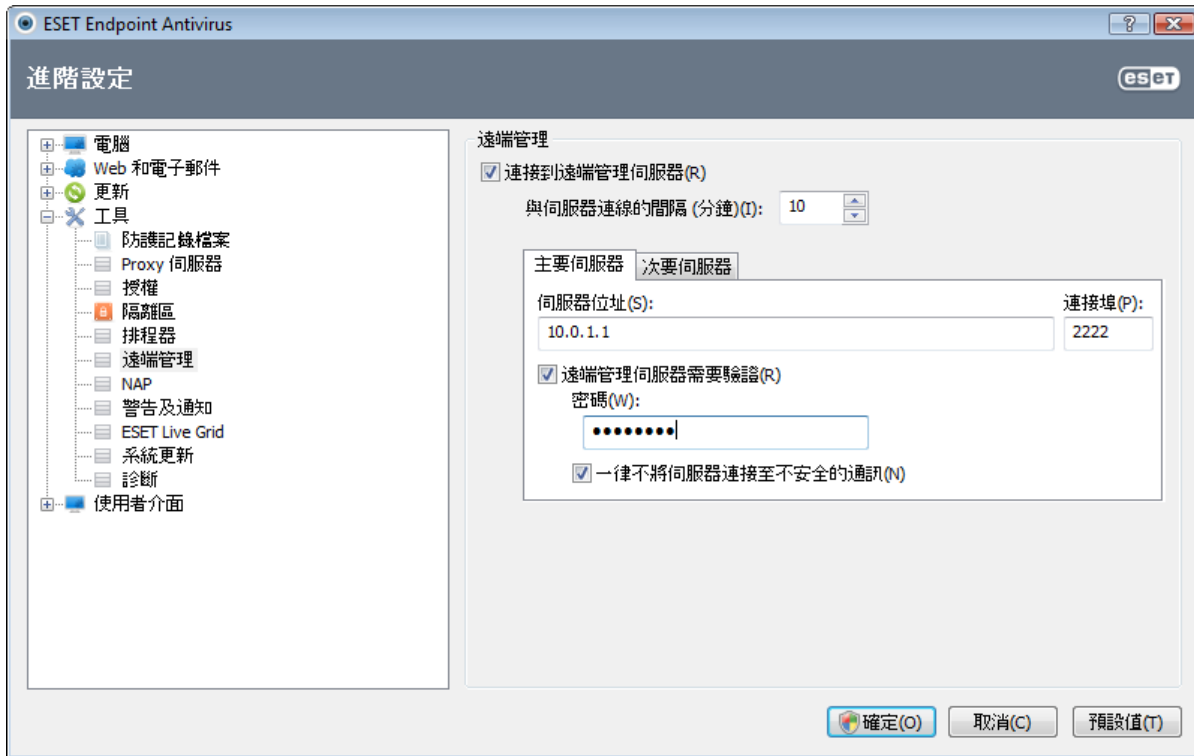
如果授權金鑰已到期且您想要續訂，請按一下 **[訂購...]** 按鈕，您會被重新導向至我們的線上商店。



#### 4.4.14 遠端管理

ESET Remote Administrator (ERA) 是一種管理安全原則及取得網路內整體安全概觀的強大工具。尤其適用於較大型網路。ERA 不僅可提高安全等級，而且也在用戶端工作站管理 ESET Endpoint Antivirus 時易於使用。您可以安裝、配置、檢視防護記錄、排程更新工作、掃描工作等。ESET Remote Administrator (ERAS) 與 ESET 安全產品之間的通訊需要在兩個端點上都具有正確的配置。

您可從主要 ESET Endpoint Antivirus 程式視窗中使用遠端管理設定選項。按一下 [設定] > [進入進階設定...] > [工具] > [遠端管理]。



選取 [連接到遠端管理伺服器] 選項以啟動遠端管理。您可以存取下面說明的其他選項：

**與伺服器連線的間隔 (分鐘)** - 這會說明 ESET 安全產品將連接 ERAS 以傳送資料的頻率。

**主要伺服器、次要伺服器** - 通常只需要配置「主要伺服器」。如果在網路上執行多個 ERA 伺服器，則可以選擇新增另一個「次要 ERA 伺服器」連線，用來當作備用解決方案。所以，如果無法存取「主要伺服器」，則 ESET 安全解決方案會自動聯絡「次要 ERA 伺服器」。同時，它會嘗試重新建立「主要伺服器」的連線。當此連線重新作用後，ESET 安全解決方案會切換回到「主要伺服器」。透過用戶端從區域網路及網路外進行連線的行動用戶端，最適合使用兩個遠端管理伺服器設定檔的配置。

**伺服器位址** - 指定執行 ERAS 之伺服器的 IP 位址或 DNS 名稱。

**連接埠** - 此欄位包含預先定義用於連線的伺服器連接埠。建議您保留預設的連接埠設定 2222。

**與伺服器連線的間隔 (分鐘)** - 此選項可指定 ESET Endpoint Antivirus 連線到 ERA Server 的頻率。如果設定為 0，則提交資訊的間隔為 5 秒。

**Remote Administrator 伺服器需要驗證** - 可讓您輸入連接至 ERA Server 的密碼 (如果需要的話)。

**一律不將伺服器連接至不安全的通訊** - 對於連往啟用未驗證存取之 ERA 伺服器的連線，選取此選項可停用連線 (請參閱 [ERA Console] > [伺服器選項] > [安全性] > [啟用用戶端的未驗證存取])。

按一下 [確定]，以確認變更並套用設定。ESET Endpoint Antivirus 將使用這些設定連接至 ERA Server。

## 4.5 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。

以滑鼠右鍵按一下選取的物件之後，會顯示[內容功能表](#)。使用此工具以將 ESET Endpoint Antivirus 控制項元素整合至內容功能表。

[簡報模式](#) 可協助使用者不會被快顯視窗、已排程工作及可能增加處理器與 RAM 負擔的任何元件中斷作業。

### 4.5.1 圖形

ESET Endpoint Antivirus 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 Endpoint Antivirus [進階設定] 樹狀目錄的 [使用者介面] > [圖形] 子目錄中可存取這些配置選項。

如果圖形元素減慢電腦執行的效能或導致其他問題，則應該在 [使用者介面元素] 區段中停用 [圖形使用者介面] 選項。在視覺障礙者使用時也可能需要停用圖形介面，因為它可能與用於閱讀畫面上所顯示文字的特殊應用程式相衝突。

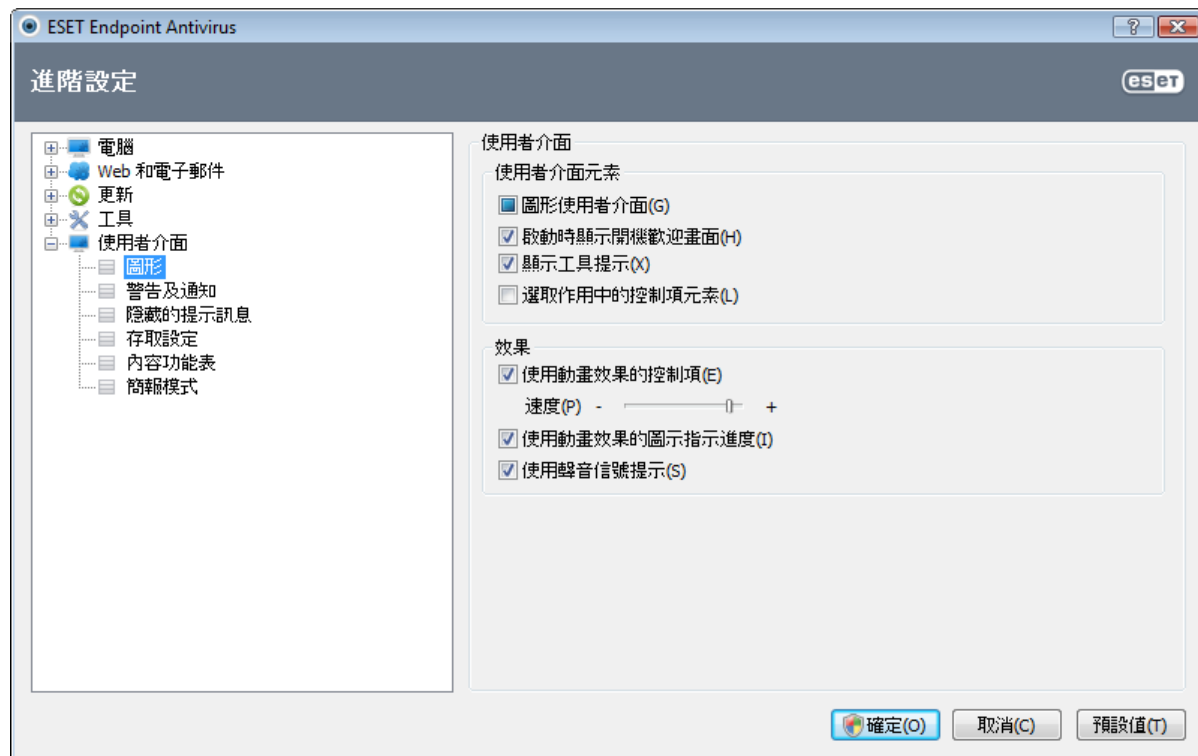
如果您要停用 ESET Endpoint Antivirus 開機歡迎畫面，請取消選取 [啟動時顯示開機歡迎畫面] 選項。

如果啟用了 [顯示工具提示] 選項，則將游標放到任何選項上時會顯示選項的簡短說明。[選取作用中的控制項元素] 選項會造成系統強調顯示目前在滑鼠游標作用中區域下的任何元素。按一下滑鼠即可啟動強調顯示的元素。

若要降低或提高動畫效果的速度，請選取 [使用動畫效果的控制項] 選項，然後左右移動 [速度] 滑動橫槓。

若要啟用動畫效果的圖示顯示各種作業的進度，請選取 [使用動畫效果的圖示指示進度] 選項。

如果您想要程式在發生重大事件時播放音效，請選取 [使用聲音信號]。請注意，只有在電腦掃描正在執行或完成時，才會播放音效。



## 4.5.2 警告及通知

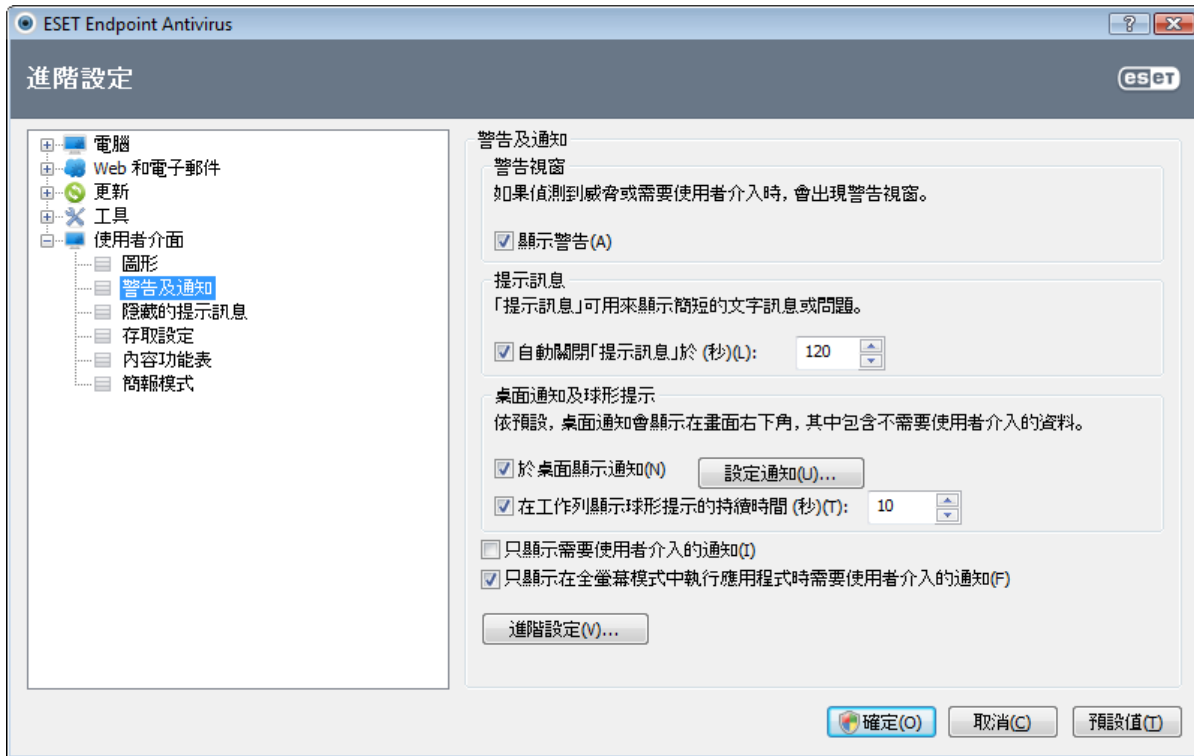
[使用者介面] 下的 [警告及通知設定] 設定可讓您配置 ESET Endpoint Antivirus 如何處理威脅警告與系統通知 (例如, 成功更新訊息)。您也可以設定顯示時間及系統匣通知的透明度層級 (僅適用於支援系統匣通知的系統)。

第一個項目是 [顯示警告]。停用此選項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, 建議保留此選項的預設值 (啟用)。

若要在某段時間內自動關閉快顯視窗, 請選取 [自動關閉提示訊息 (秒)] 選項。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。

桌面及球形提示上的通知僅提供資訊, 不需要或不提供使用者介入。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, 請啟用 [於桌面顯示通知] 選項。按一下 [配置通知...] 按鈕可以修改更多詳細選項, 如通知顯示時間及視窗透明度。若要預覽通知行為, 請按一下 [預覽] 按鈕。

若要配置球形提示顯示的持續時間, 請選取 [在工作列顯示球形提示的持續時間 (秒)] 選項, 並在相鄰欄位中輸入所需的間隔。



[只顯示需要使用者介入的通知] 選項可讓您切換不需要使用者介入之警告及通知。選取 [只顯示在全螢幕模式中執行應用程式時需要使用者介入的通知] 強制不顯示所有非互動通知。

按一下 [進階設定...], 以輸入其他 [警告及通知] 設定選項。

### 4.5.2.1 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。

### 4.5.3 隱藏通知視窗

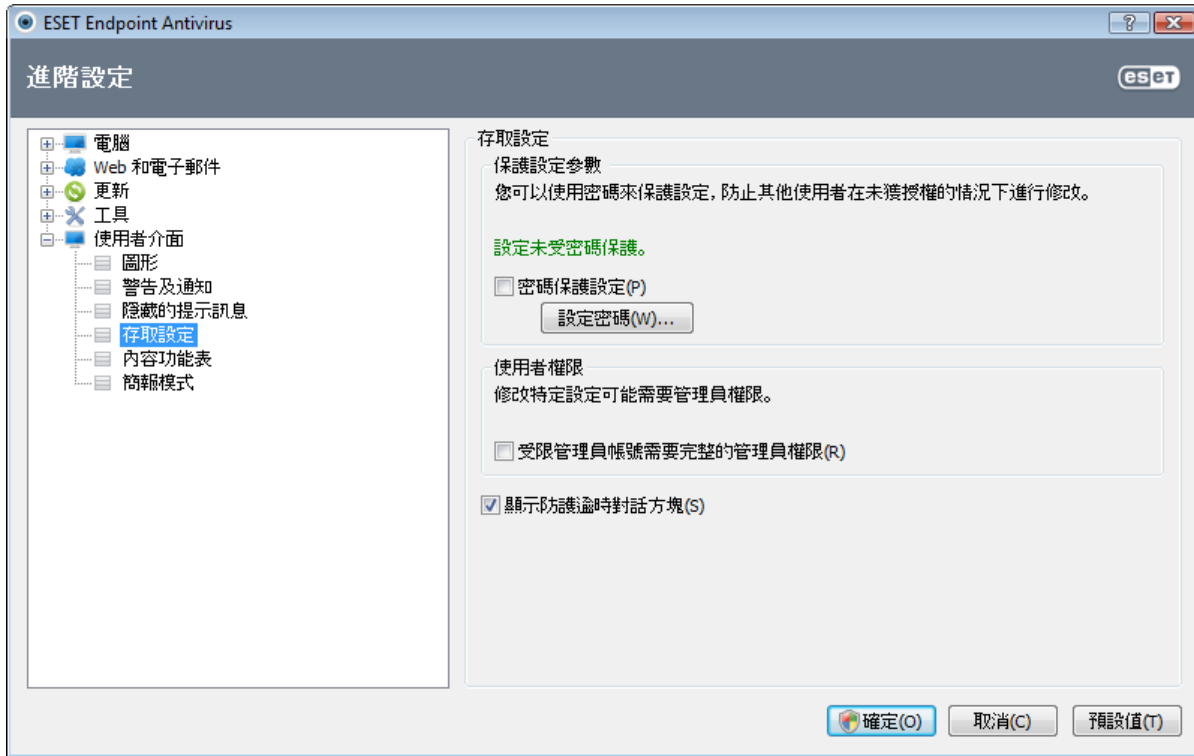
如果您曾經針對所有先前顯示的通知 (警告) 視窗選取 [不要再顯示這則訊息] 選項，則這些視窗會出現在隱藏通知視窗的清單中。現在執行的處理方法會自動顯示在標題為 [確認] 的直欄中。

**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。

### 4.5.4 存取設定

為了對系統提供最大的安全，需要正確配置 ESET Endpoint Antivirus。任何不合格的變更都會導致重要資料遺失。此選項位於 [進階設定] 樹狀目錄中 [使用者介面] 下的 [存取設定] 子功能表中。為了避免未獲授權的修改，您可以使用密碼保護 ESET Endpoint Antivirus 的設定參數。



**密碼保護設定** - 鎖定/解除鎖定程式的設定參數。勾選或取消勾選該核取方塊，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 [設定密碼...]

**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 中的 UAC 相似)。這些修改包括停用防護模組。

**顯示防護逾時對話方塊** - 如果選取此選項，且從程式功能表或透過 [ESET Endpoint Antivirus] > [設定] 區段暫時停用防護，您就會收到提示。[暫時停用防護] 視窗中的 [時間間隔] 下拉式功能表顯示所有已選取的防護部分將停用的期間。

#### 4.5.5 程式功能表

在主程式功能表中，可以使用某些最重要的設定選項及功能。



**經常使用** - 顯示 ESET Endpoint Antivirus 最常使用的部分。您可以從程式功能表快速存取這些部分。

**暫時停用防護** - 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的系統攻擊。選取 **[不要再詢問]** 核取方塊以避免將來再次收到訊息。



**[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。



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

**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。

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

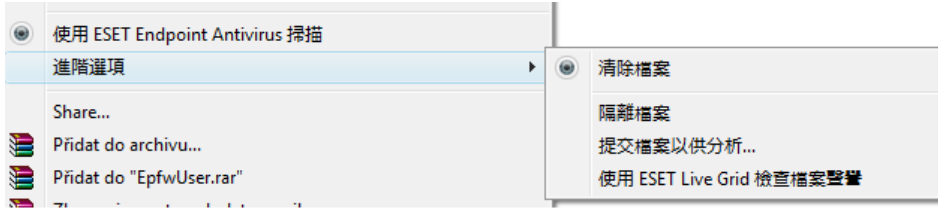
**關於** - 提供系統資訊、ESET Endpoint Antivirus 已安裝版本的詳情，以及已安裝的程式模組。您還可以在這裡找到授權到期日期。您可以在底部找到作業系統及系統資源的相關資訊。

#### 4.5.6 內容功能表

以滑鼠右鍵按一下選取的物件之後，會顯示內容功能表。功能表會列出可以在物件上執行的所有選項。

可以將 ESET Endpoint Antivirus 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 Endpoint Antivirus 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 [使用 ESET Endpoint Antivirus 掃描] 選項。
- 完整 (先清除) - 啟動所有內容功能表選項；主要功能表會顯示 [使用 ESET Endpoint Antivirus 清除] 選項。
- 僅掃描 - 內容功能表只顯示 [使用 ESET Endpoint Antivirus 掃描] 選項。
- 僅清除 - 內容功能表只顯示 [使用 ESET Endpoint Antivirus 清除] 選項。

#### 4.5.7 簡報模式

簡報模式 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 CPU 使用量降至最低的使用者所設計的功能。簡報模式 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中啟用或停用簡報模式，方法為按一下 [設定] > [電腦]，再按一下 簡報模式 下的 [啟用] [玩家] 模式，方法為展開 [使用者介面]、按一下 [簡報模式]，並勾選 [啟用玩家模式] 旁的核取方塊。啟用簡報模式 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橘色並顯示警告。您在主要程式視窗中也可看見此警告，在此您將看見已啟用簡報模式 為橘色。

選取 [以全螢幕模式執行應用程式時自動啟用 簡報模式] 核取方塊，簡報模式 就會在您啟動全螢幕應用程式之後啟動，並在您結束應用程式之後自動停止。這樣特別有助於在啟動遊戲、開啟全螢幕應用程式或開始簡報之後，直接啟動 簡報模式。

您也可以選取 [自動停用 簡報模式 於 X 分鐘後] 核取方塊以定義時間量 (預設值為 1 分鐘)。如果您只需要簡報模式 在特定時段啟動之後就自動停用，則可以使用此選項。

## 5. 進階使用者

### 5.1 Proxy 伺服器設定

在大型區域網路網路中，Proxy 伺服器可用來調節電腦與網際網路的連線。如果是這種情況，則需要定義下列設定。否則，程式將無法自動進行更新。在 ESET Endpoint Antivirus 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 Endpoint Antivirus 的全域 Proxy 伺服器設定。需連線到網際網路的所有模組，都會使用這裡設定的參數。

若要指定此層級的 Proxy 伺服器設定，請選取 [使用 Proxy 伺服器] 核取方塊，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] 核取方塊，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 Proxy 伺服器] 按鈕，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：此功能不會擷取驗證資料 (使用者名稱及密碼)，而必須由您提供。

Proxy 伺服器設定也可以在 [進階更新設定] ([進階設定] 樹狀目錄的 [更新] 子目錄) 內建立。此設定適用於指定更新設定檔且建議用於膝上型電腦；膝上型電腦通常會從不同位置接收病毒碼更新。如需更多有關此設定的資訊，請參閱 [進階更新設定](#) 一節。

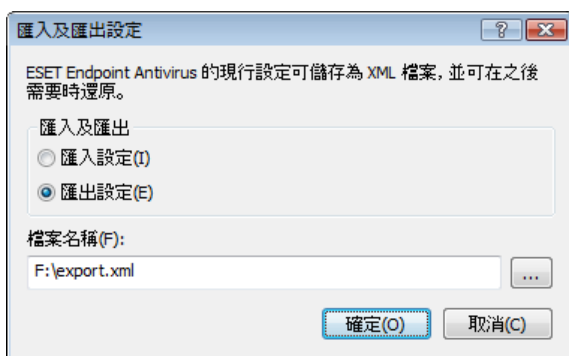
### 5.2 匯入及匯出設定

在 [設定] 下可以匯入和匯出 ESET Endpoint Antivirus 的配置。

匯入或匯出皆使用 .xml 檔案類型。如果您需要備份 ESET Endpoint Antivirus 的目前設定以供稍後使用，匯入和匯出很有幫助。匯出設定選項對想要在多個系統上使用 ESET Endpoint Antivirus 慣用配置的使用者也很方便，他們可以輕鬆匯入 .xml 檔案以傳送所需的設定。

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] 選項。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] 選項並輸入配置檔案的 [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。



## 5.3 鍵盤快捷鍵

使用 ESET Endpoint Antivirus 時可使用的鍵盤快捷鍵包括：

Ctrl+G	在產品中停用 GUI
Ctrl+I	開啟 ESET SysInspector 頁面
Ctrl+L	開啟防護記錄檔案頁面
Ctrl+S	開啟排程器頁面
Ctrl+Q	開啟隔離區頁面
Ctrl+U	開啟可設定使用者名稱及密碼的對話方塊視窗
Ctrl+R	將視窗重設為螢幕上的預設大小及位置

為了更方便在 ESET 安全性產品中瀏覽，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
*	展開 [進階設定] 樹狀目錄節點
-	收合 [進階設定] 樹狀目錄節點
TAB 鍵	在視窗中移動游標
Esc 鍵	關閉作用中的對話方塊視窗

## 5.4 命令列

ESET Endpoint Antivirus 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
/adware	掃描廣告程式/間諜程式/高風險程式 (預設值)
/no-adware	不掃描廣告程式/間諜程式/高風險程式
/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)
/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 (MODE)。 可用選項：none、standard (預設值)、strict、rigorous、delete
/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	保存最後一次存取的時間郵戳

#### 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。

## 5.5 ESET SysInspector

### 5.5.1 ESET SysInspector 簡介

ESET SysInspector 是會徹底檢查電腦，並完整地顯示所收集資料的應用程式。諸如已安裝驅動程式及應用程式、網路連線或重要登錄項目等資訊，可協助您調查可疑系統行為是肇因於軟體或硬體不相容，還是惡意軟體感染。

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，整合的版本還可讓您將系統快照直接儲存於 [工具] > [ESET SysInspector] (ESET Remote Administrator 除外)。

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目而定，這可能需要 10 秒到幾分鐘的時間。

#### 5.5.1.1 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。

請稍候等待應用程式檢查您的系統，根據收集的硬體和資料，檢查可能需要數分鐘的時間。

### 5.5.2 使用者介面和應用程式使用

為清楚起見，「主要視窗」分為四個主要區段：位於「主要視窗」頂端的「程式控制」、位於中間左側的「瀏覽視窗」、位於中間右側的「說明視窗」，以及位於「主要視窗」底部右側的「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)。

處理	路徑	PID	使用者名稱
執行中的處理程序			
System Idle Process		0	
System		4	
smss.exe		464	
csrss.exe		536	
wininit.exe		596	
csrss.exe		608	
services.exe		640	
lsass.exe		652	
lsm.exe		664	
winlogon.exe		736	
svchost.exe		848	
nvsvc.exe		892	

SHA1	348F0EDF9BA670E3713223113ECC9C6C37A67DCC
最近寫入時間	2009/04/10 23:28
建立時間	2010/06/21 17:30
檔案大小	64000
檔案說明	Windows Session Manager
公司名稱	Microsoft Corporation

### 5.5.2.1 程式控制項

本小節包含 ESET SysInspector 中所有可用程式控制的說明。

#### 檔案

只要按一下 [檔案]，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。在此格式中，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

包含可在程式內更輕鬆瀏覽的功能，以及各類其他功能，例如尋找線上資訊。

#### 說明

包含應用程式及其功能的相關資訊。

#### 詳情

此設定影響在主要視窗顯示的資訊，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「中等」模式中，程式會顯示不常使用的詳情。在「完整」模式中，ESET SysInspector 會顯示解決專門問題的所有必要資訊。

#### 項目過濾

項目過濾最適用於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：透過比較項目的顏色與「風險層級」滑桿上的顏色，可快速判定項目的「風險層級」。

#### 搜尋

搜尋可用來根據特定項目的名稱或部分名稱快速尋找該項目。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。即使項目是紅色的，也不表示您可以刪除該檔案。刪除之前，請確定檔案確實是危險或不必要的。

### 5.5.2.2 在 ESET SysInspector 中瀏覽

ESET SysInspector 會將各類型的資訊分為數個基本區段，稱為節點。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。

#### 執行中的處理程序

此節點包含產生防護記錄時執行之應用程式及處理程序的相關資訊。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、檔案的風險等級等等。

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

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。在特定情況下，此類處理程序會顯示於工具 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 [說明視窗] 中所選取項目的其他資訊，例如檔案大小或雜湊。

#### 重要登錄項目

包含所選取登錄項目的清單，通常與各種系統問題相關，例如指定啟動程式、瀏覽器 Helper 物件 (BHO) 等等。

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

系統上所安裝的驅動程式清單。

#### 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。

#### 系統排程任務

包含 Windows 工作排程器在指定時間/間隔觸發的工作清單。

#### 系統資訊

包含硬體及軟體的詳情，以及設定環境變數、使用者權限及系統事件防護記錄的相關資訊。

#### 檔案詳情

重要系統檔案及 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 版本與程式模組清單的相關資訊。

### 5.5.2.2.1 鍵盤快捷鍵

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? 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、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、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  
+ 增加風險層級  
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 依供應商檢視，所有供應商  
Ctrl+6 依供應商檢視，僅 Microsoft  
Ctrl+7 依供應商檢視，所有其他供應商  
Ctrl+3 顯示完整詳情  
Ctrl+2 顯示中等詳情  
Ctrl+1 基本顯示  
退格鍵 向前移動一步  
空格鍵 向後移動一步  
Ctrl+W 展開樹狀結構  
Ctrl+Q 收合樹狀結構

#### 其他控制項

Ctrl+T 在搜尋結果中選取之後，移至項目的原始位置  
Ctrl+P 顯示項目的基本資訊  
Ctrl+A 顯示項目的完整資訊  
Ctrl+C 複製目前項目的樹狀結構  
Ctrl+X 複製項目  
Ctrl+B 尋找網際網路上所選取檔案的相關資訊  
Ctrl+L 開啟選取之檔案所在的資料夾  
Ctrl+R 開啟登錄編輯器中的對應項目  
Ctrl+Z 複製檔案的路徑 (如果項目與檔案相關)  
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/比較防護記錄
Ctrl+Alt+R	取消比較
Ctrl+Alt+1	顯示所有項目
Ctrl+Alt+2	只顯示新增的項目，防護記錄會顯示目前防護記錄中存在的項目
Ctrl+Alt+3	只顯示移除的項目，防護記錄會顯示前一個防護記錄中存在的項目
Ctrl+Alt+4	只顯示已取代的項目 (包括檔案)
Ctrl+Alt+5	只顯示防護記錄之間的差異
Ctrl+Alt+C	顯示比較
Ctrl+Alt+N	顯示目前防護記錄
Ctrl+Alt+P	開啟前一個防護記錄

## 其他選項

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

### 5.5.2.3 比較

「比較」功能可以讓使用者比較兩份現有的防護記錄。此功能的比較結果是不通用於兩個防護記錄的一組項目。如果您要追蹤系統的變更，此功能非常適合 - 是偵測惡意程式活動狀態的實用工具。

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。瀏覽到 [檔案] > [儲存防護記錄]，將防護記錄儲存至檔案。防護記錄檔案可在稍後開啟並檢視。若要開啟現有的防護記錄，請使用 [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。







比較此兩筆防護記錄的好處是，您可以檢視目前作用中的防護記錄以及儲存於檔案中的防護記錄。若要比較防護記錄，請使用 [檔案] > [比較防護記錄] 選項，然後選擇 [選取檔案]。選取的防護記錄會與主要程式視窗中的作用中防護記錄進行比較。該相較防護記錄將只顯示兩筆防護記錄之間的差異。

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

在所顯示項目的旁邊，ESET SysInspector 會顯示識別所比較防護記錄之間差異的符號。

標記為 - 的項目只能在作用中防護記錄中找到，且不存在於開啟的比較防護記錄。由 + 標記的項目只出現在開啟的防護記錄中，而不會在作用中的防護記錄找到。

可在項目旁邊顯示之所有符號的說明：

- + 新值，不存在於前一個防護記錄中
-  樹狀結構區段包含新值
- - 移除的值，只存在於前一份防護記錄中
-  樹狀結構區段包含移除的值
-  值/檔案已變更
-  樹狀結構區段包含修改的值/檔案
-  已降低風險層級/它在前一個防護記錄中較高
-  已增加風險層級/它在前一個防護記錄中較低

在左下角顯示的說明區段會說明所有符號，並顯示要比較之防護記錄的名稱。

防護記錄狀態	
目前防護記錄:	[已產生]
前一個防護記錄:	SysInspector-LOG-110725-1042.xml [已載入...]
比較:	[比較結果]
比較圖示圖例	
+ 已新增項目	◻ 子目錄中的已新增項目
- 已移除項目	◻ 子目錄中的已移除項目
◻ 已取代的檔案	◻ 子目錄中的已新增或已移除項目
➤ 狀態已降低	◻ 子目錄中已取代的檔案
➤ 狀態已提昇	

任何比較防護記錄都可以儲存至檔案，並在稍後開啟。

### 範例

產生記錄系統原始資訊的防護記錄，並將其儲存至名為 previous.xml 的檔案。在變更系統之後，開啟 ESET SysInspector 並讓其產生新的防護記錄。將其儲存至名為 current.xml 的檔案。

為追蹤這兩份防護記錄間的變更，請瀏覽至 [檔案] > [比較防護記錄]。程式會建立比較防護記錄，顯示防護記錄之間的差異。

如果使用下列命令列選項，也可達到相同的結果：

```
SysInspector.exe current.xml previous.xml
```

### 5.5.3 命令列參數

ESET SysInspector 支援透過使用這些參數的命令列產生報告：

/gen	直接由命令列產生防護記錄，而不執行 GUI
/privacy	產生排除敏感資訊的防護記錄
/zip	以壓縮檔方式將結果防護記錄直接儲存至磁碟
/silent	強制不顯示防護記錄的產生進度列
/help, /?	顯示有關命令列參數的資訊

### 範例

若要將特定防護記錄直接載入至瀏覽器，用法如下：SysInspector.exe "c:\clientlog.xml"

若要在目前的位置產生防護記錄，用法如下：SysInspector.exe /gen

若要在特定的資料夾中產生防護記錄，用法如下：SysInspector.exe /gen="c:\folder\"

若要將防護記錄產生於特定的檔案/位置中，用法如下：SysInspector.exe /gen="c:\folder\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="c:\mynewlog.zip" /privacy /zip

若要比較兩份防護記錄，用法如下：SysInspector.exe "current.xml" "original.xml"

附註：如果檔案/資料夾的名稱包含空白，則應將其放在引號中。

## 5.5.4 服務腳本

服務腳本是專為使用 ESET SysInspector 的客戶所提供協助的工具，可輕鬆移除系統中不需要的物件。

服務腳本可讓使用者匯出整個 ESET SysInspector 防護記錄，或所選取的部分。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。

服務腳本適用於之前具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毀。

### 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：

- 執行 ESET SysInspector 以產生新的系統快照。
- 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。
- 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]** 內容功能表選項。
- 選取的物件會匯出至新的防護記錄。
- 下列是整個程序的最重要步驟：開啟新的防護記錄，並將您想要移除的所有物件 - 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。
- 開啟 ESET SysInspector，按一下 **[檔案] > [執行服務腳本]**，然後輸入腳本的路徑。
- 按一下 **[確定]** 以執行腳本。

### 5.5.4.1 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]** 選項或 **[將選取的區段匯出至服務腳本]** 選項。

附註：在比較兩份防護記錄時，無法匯出服務腳本。

### 5.5.4.2 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\khibehb.dll
- c:\windows\system32\advapi32.dll
[...]
```

在此範例中，khibehb.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
[...]
```

您執行腳本時，選取的驅動程式將停止。請注意，部分驅動程式不允許自己停止。

## 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。

### 5.5.4.3 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。執行未簽署和未知的腳本可能會嚴重損害您的電腦資料。您確定要執行腳本並執行處理方法嗎？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。

## 5.5.5 常見問題

### ESET SysInspector 是否需要管理員權限才能執行？

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「標準使用者」或「受限使用者」身分執行它，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，請從主要功能表中選取 [檔案] > [儲存防護記錄]。防護記錄會以 XML 格式儲存。依預設，檔案會儲存至 %USERPROFILE%\My Documents\ 目錄，檔案命名慣例為 "SysInspector-%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，然後選取主功能表的 [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。如果您需要經常檢視 ESET SysInspector 防護記錄檔案，建議您在桌面上建立 SYSINSPECTOR.EXE 檔案的捷徑，接著您就可以將防護記錄檔案拖放至該捷徑來進行檢視。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，因為程式仍在開發中，尚未有防護記錄檔案的規格或 SDK。在程式發佈之後，我們會根據客戶意見及需求提供這些規格。

### ESET SysInspector 如何評估特定物件所造成的風險？

在大部分情況下，ESET SysInspector 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、登錄機碼等等) 的風險層級。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。在左側的瀏覽窗格中，區段會根據其中所含物件的最高風險層級來設定顏色。

### 風險層級「6 - 未知 (紅色)」是否表示物件是危險的？

ESET SysInspector 的評量不保證物件是惡意的，應由安全專家判定。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。

### 為何 ESET SysInspector 在執行時要連接至網際網路？

如同許多應用程式，ESET SysInspector 使用數位簽章「憑證」來簽署，以協助確保軟體是由 ESET 發佈，且未遭到變更。為了驗證憑證，作業系統會聯絡憑證管理中心以驗證軟體發佈者的身分。此行為對所有 Microsoft Windows 的數位簽章程式來說是正常的。

### 何謂反隱藏技術？

反隱藏技術提供有效的隱藏程序 (Rootkit) 偵測。

如果系統遭 Rootkit 方式的惡意程式攻擊，則使用者暴露在資料遺失或遭竊的風險中。若沒有特殊的反 Rootkit 工具，要偵測到 Rootkit 幾乎是不可能。

### 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 會先檢查內嵌在檔案內的數位簽章。如果找到數位簽章，則會使用該資訊驗證檔案。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。其中的源是由因為 C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat 中的參考指向 C:\Program Files\Windows NT\hypertm.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。

### 5.5.6 ESET SysInspector 是 ESET Endpoint Antivirus 的一部份

若要開啟 ESET Endpoint Antivirus 中的 ESET SysInspector 區段，請按一下 **[工具] > [ESET SysInspector]**。[ESET SysInspector] 視窗中的管理系統與電腦掃描防護記錄或已排程工作的管理系統相似。所有使用系統快照的作業 (建立、檢視、比較、移除及匯出) 按一或兩下即可存取。

[ESET SysInspector] 視窗包含所建立快照的基本資訊，例如建立時間、簡短註解，建立快照的使用者名稱及快照狀態。

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。那些選項也可從內容功能表中取得。若要檢視選取的系統快照，請使用 **[顯示]** 內容功能表選項。若要將選取的快照匯出至檔案，請在該快照上按一下滑鼠右鍵，並選取 **[匯出...]**。

下列是可用選項的詳細說明：

- **比較** - 可讓您比較兩份現有防護記錄。如果您想要追蹤目前防護記錄與較舊防護記錄之間的變更，即適用此選項。若要使此選項生效，您必須選取兩份要進行比較的快照。
- **建立...** - 建立新的記錄。在此之前，您必須輸入關於記錄的簡短註解。若要找到 (目前已產生快照的) 快照建立進度百分比，請參閱 **[狀態]** 直欄。所有已完成快照都會標記為 **[已建立]** 狀態。
- **刪除/全部刪除** - 從清單移除項目。
- **匯出...** - 將選取的項目儲存至 XML 檔案 (同時儲存為壓縮版本)。

## 5.6 ESET SysRescue

ESET SysRescue 是一個公用程式，可讓您建立包含其中一個 ESET Security 解決方案的開機磁碟，可以是 ESET NOD32 Antivirus、ESET Smart Security，甚至是部份伺服器導向的產品。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整個檔案系統。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。

### 5.6.1 最低需求

ESET SysRescue 在以 Windows Vista 為基礎的 Microsoft Windows 預先安裝環境 (Windows PE) 2.x 版中運作。

Windows PE 是免費套件 Windows Automated Installation Kit (Windows AIK) 的一部份，因此必須先安裝 Windows AIK 才能建立 ESET SysRescue (<http://go.eset.eu/AIK>)。由於支援 32 位元版本 Windows PE 的緣故，因此在 64 位元系統上建立 ESET SysRescue 時，必須使用 32 位元的 ESET Security 解決方案安裝套件。ESET SysRescue 支援 Windows AIK 1.1 和更新版本。

附註：由於 Windows AIK 大小超過 1 GB，因此需要高速網際網路連線才能順利下載。

ESET Security 解決方案 4.0 及更新版本可使用 ESET SysRescue。

#### 支援的作業系統

- Windows 7
- Windows Vista
- Windows Vista Service Pack 1
- Windows Vista Service Pack 2
- Windows Server 2008
- Windows Server 2003 Service Pack 1 (含 KB926044)
- Windows Server 2003 Service Pack 2
- Windows XP Service Pack 2 (含 KB926044)
- Windows XP Service Pack 3

## 5.6.2 如何建立救援 CD

若要啟動 ESET SysRescue 精靈，請按一下 **[開始] > [程式集] > [ESET] > [ESET Endpoint Antivirus] > [ESET SysRescue]**。

首先，精靈會檢查系統是否存在 Windows AIK，以及建立開機媒體的適當裝置。如果電腦上沒有安裝 Windows AIK (或已損毀或安裝不正確)，精靈會提供您安裝或輸入 Windows AIK 資料夾路徑 (<http://go.eset.eu/AIK>) 的選項。

附註：由於 Windows AIK 大小超過 1 GB，因此需要高速網際網路連線才能順利下載。

在[下一個步驟](#)中，選取 ESET SysRescue 所在的目標媒體。

## 5.6.3 目標選擇

除了 CD/DVD/USB 之外，您也可以選擇將 ESET SysRescue 儲存在 ISO 檔案中。稍後，您可以將 ISO 映像燒錄在 CD/DVD 中，或以其他方式使用 (例如，在 VmWare 或 Virtualbox 等虛擬環境中)。

如果您選取 USB 作為目標媒體，開機功能可能無法在特定電腦上運作。部分 BIOS 版本可能會報告 BIOS - 開機管理程式通訊 (例如，在 Windows Vista 上) 發生問題，且開機會結束並顯示下列錯誤訊息：

```
檔案 \boot\bcd  
狀態 :0xc000000e  
資訊 :嘗試讀取開機配置資料時發生錯誤
```

如果收到此訊息，建議您選取 CD 而非 USB 媒體。

## 5.6.4 設定

起始建立 ESET SysRescue 之前，安裝精靈會在 ESET SysRescue 精靈的最後一個步驟中顯示編譯參數。您可以按一下 **[變更...]** 按鈕來修改這些參數。可用的選項包括：

- [資料夾](#)
- [ESET Antivirus](#)
- [進階](#)
- [網際網路通訊協定](#)
- [開機 USB 裝置](#) (當目標 USB 裝置已選取時)
- [燒錄](#) (當目標 CD/DVD 磁碟機已選取時)

如果沒有指定 MSI 安裝套件，或沒有在電腦上安裝 ESET Security 解決方案，則 **[建立]** 按鈕為非作用中。若要選取安裝套件，請按一下 **[變更]** 按鈕，並移至 [ESET Antivirus] 索引標籤。此外，如果您未填寫使用者名稱和密碼 (**[變更]** > [ESET Antivirus])，**[建立]** 按鈕會呈現灰色狀態。

### 5.6.4.1 資料夾

暫存資料夾 是編譯 ESET SysRescue 期間必要檔案的工作目錄。

ISO 資料夾是編譯完成後，儲存結果 ISO 檔案的資料夾。

此索引標籤上的清單顯示所有本機及對應的網路磁碟，以及可用空間。如果這裡的部分資料夾位於可用空間不足的磁碟機上，建議您選取其他具有更多可用空間的磁碟機。否則，編譯可能會因可用磁碟空間不足而提前結束。

外部應用程式 - 可讓您指定從 ESET SysRescue 媒體開機後將執行或安裝的其他程式。

併入外部應用程式 - 可讓您將外部程式新增至 ESET SysRescue 編譯。

選取的資料夾 - 將新增至 ESET SysRescue 磁碟的程式所在的資料夾。

#### 5.6.4.2 ESET Antivirus

若要建立 ESET SysRescue CD，您可以選取兩個 ESET 檔案來源以供編譯器使用。

**ESS/EAV 資料夾** - 已安裝 ESET Security 解決方案的電腦上，已包含於資料夾中的檔案。

**MSI 檔案** - 使用的 MSI 安裝程式中包含的檔案。

接著，您可以選擇更新 (nup) 檔案的位置。通常，系統設定的預設選項是 **ESS/EAV 資料夾/MSI 檔案**。在某些情況下，可選擇自訂的 **[更新資料夾]**，例如使用較舊或較新的病毒資料庫版本。

您可以在下列使用者名稱和密碼的兩個來源之中擇一使用：

**已安裝的 ESS/EAV** - 從目前已安裝的 ESET Security 解決方案複製使用者名稱和密碼。

**來源使用者** - 使用在對應文字方塊中輸入的使用者名稱和密碼。

附註：ESET SysRescue CD 中具有的 ESET Security 解決方案會從網際網路更新，或從執行 ESET SysRescue CD 之電腦上所安裝的 ESET Security 解決方案更新。

#### 5.6.4.3 進階設定

**[進階]** 索引標籤可讓您根據電腦中的記憶體數量最佳化 ESET SysRescue CD。選取 **[576 MB 以上]** 以將 CD 的內容寫入作業記憶體 (RAM)。如果您選取 **[少於 576 MB]**，則執行 WinPE 時會永久存取復原 CD。

在 **[外部磁碟機]** 區段中，您可以針對特定硬體 (通常為網路介面卡) 插入驅動程式。雖然 WinPE 是以支援多種硬體的 Windows Vista SP1 為依據，但有時候也會出現硬體無法辨識的情形，這時候就需要您手動新增驅動程式。將驅動程式引進 ESET SysRescue 編譯的方式有兩種 - 手動 (**[新增]** 按鈕) 和自動 (**[自動搜尋]** 按鈕)。若是手動引進，您必須選取對應的 .inf 檔案路徑 (適用的 \*.sys 檔案亦必須存在此資料夾內)。在自動引進的情況下，則會在指定電腦的作業系統中自動找到驅動程式。我們建議您，只有在使用 ESET SysRescue 的電腦與建立 ESET SysRescue CD 的電腦網路介面卡相同時，才使用自動引進。在建立期間，ESET SysRescue 驅動程式會引進至編譯，因此您不必稍後再尋找驅動程式。

#### 5.6.4.4 網際網路通訊協定

此區段可讓您依據 ESET SysRescue 配置基本的網路資訊與設定預先定義的連線。

選取 **[自動私人 IP 定址]** 以自動從 DHCP (動態主機設定通訊協定) 伺服器取得 IP 位址。

或者，此網路連線可以使用手動指定的 IP 位址 (也稱為靜態 IP 位址)。選取 **[自訂]** 以配置適當的 IP 設定。如果您選取此選項，您必須指定 **[IP 位址]**，此外，針對 LAN 和高速網際網路連線，指定一個 **[子網路遮罩]**。在 **[慣用 DNS 伺服器]** 和 **[替代 DNS 伺服器]** 中，輸入主要和次要 DNS 伺服器位址。

#### 5.6.4.5 開機 USB 裝置

如果您已選取 USB 裝置作為目標媒體，則可以在 **[開機 USB 裝置]** 索引標籤上選取其中一個可用 USB 媒體 (如果有多個 USB 裝置的話)。

選取適當的目標 **[裝置]**，其中將安裝 ESET SysRescue。

**警告：**選取的 USB 裝置將在 ESET SysRescue 建立期間格式化。將刪除裝置上所有的資料。

如果您選擇 **[快速格式化]** 選項，格式化作業將從分割區移除所有的檔案，但是不會掃描磁碟檢查已損壞磁區。如果您的 USB 裝置先前已經格式化，而且您確定此裝置沒有損壞，則請使用此選項。

#### 5.6.4.6 燒錄

如果您已選取 CD/DVD 作為目標媒體，則可以在 [燒錄] 索引標籤上指定其他燒錄參數。

**刪除 ISO 檔案** - 勾選此選項，可在建立 ESET SysRescue CD 之後刪除暫存的 ISO 檔案。

**已啟用刪除** - 可讓您選取快速消除及完全消除。

**燒錄裝置** - 選取要用來燒錄的磁碟機。

**警告：** 這是預設選項。如果使用的是可重新寫入 CD/DVD，則會消除該 CD/DVD 中所有資料。

[媒體] 區段包含有關 CD/DVD 裝置中的媒體資訊。

**燒錄速度** - 從下拉式功能表中選取想要的速度。選取燒錄速度時，應考量燒錄裝置的能力及使用的 CD/DVD 類型。

#### 5.6.5 使用 ESET SysRescue

若要使 CD/DVD/USB 有效運作，您必須從 ESET SysRescue 開機媒體啟動電腦。開機優先順序可以在 BIOS 中修改。或者，您可以在電腦啟動期間使用開機功能表 - 通常使用 F9 - F12 鍵的其中一個，需視主機板/BIOS 的版本而定。

從開機媒體開機之後，便會啟動 ESET Security 解決方案。因為 ESET SysRescue 只能在特定情況下使用，所以不需要使用在 ESET Security 解決方案標準版本中的部分防護模組及程式功能；其清單縮小為 [電腦掃描]、[更新] 及 [設定] 中的部分區段。更新病毒資料庫的功能是 ESET SysRescue 最重要的功能，建議您在開始電腦掃描前先更新程式。

##### 5.6.5.1 使用 ESET SysRescue

假設網路中的電腦已感染可修改執行檔 (.exe) 的病毒。ESET Security 解決方案能夠清除所有受感染的檔案，但 explorer.exe 除外，即使在「安全模式」中也不能清除該檔案。這是因為 explorer.exe 是 Windows 的基本處理程序之一，也會在安全模式中啟動。ESET Security 解決方案將無法針對該檔案執行任何處理方法，而且該檔案將持續受感染。

在這種情況下，您可以使用 ESET SysRescue 解決問題。ESET SysRescue 不需要主機作業系統中的任何元件，因此它能夠處理 (清除、刪除) 磁碟中的任何檔案。

## 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疾病，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 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 Rootkit 躲過一般測試時。ESET Endpoint Antivirus 使用者擁有「反隱藏」技術的優勢，亦可偵測及消滅作用中的 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 潛在不安全的應用程式

有很多合法律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 Endpoint Antivirus 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。

### 6.1.8 潛在不需要應用程式

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。這些應用程式通常需要經過同意才能安裝。如果他們存在於您的電腦上，系統的行為會有所不同 (相較於安裝前的狀態)。最顯著的變更如下：

- 您從未看過的新視窗 (快顯視窗、廣告)、
- 啟動並執行隱藏的處理程序、
- 系統資源的用量增加、
- 搜尋結果變更、
- 應用程式會與遠端伺服器通訊。

## 6.2 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

### 6.2.1 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。

### 6.2.2 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。

### 6.2.3 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。

### 6.2.4 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。