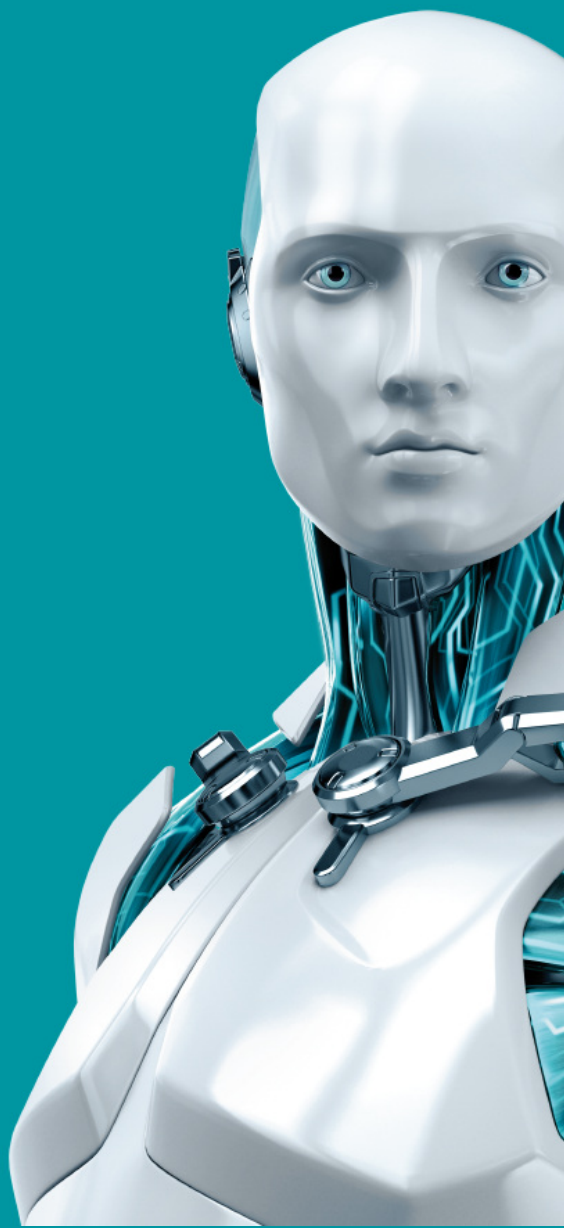
CYBER SECURITY PRO

使用者手冊

(僅適用於 6.5 或更高版本)

按一下這裡以下載此文件的最新版本。



ENJOY SAFER TECHNOLOGY™

ESET Cyber Security Pro 是由 ESET, spol. s r.o. 開發的產品
如需相關資料，請造訪 www.eset.com。

客戶關懷：www.eset.com/support。

REV. 2017/10/13

內容

1. ESET Cyber Security Pro 5
1.1 第 6 版最新功能 5
1.2 系統需求 6
2. 安裝 6
2.1 一般安裝 7
2.2 自訂安裝 7
3. 產品啟動 8
4. 解除安裝 9
5. 基本概觀 10
5.1 鍵盤快捷鍵 10
5.2 檢查防護狀態 11
5.3 如果程式運作不正常怎麼辦 11
6. 電腦防護 12
6.1 病毒及間諜程式防護 12
6.1.1 一般 12
6.1.1.1 排除 12
6.1.2 啟動防護 12
6.1.3 即時檔案系統防護 13
6.1.3.1 進階選項 13
6.1.3.2 何時修改即時防護配置 13
6.1.3.3 檢查即時防護 13
6.1.3.4 即時防護無法運作時怎麼辦 13
6.1.4 指定電腦掃描 14
6.1.4.1 掃描類型 14
6.1.4.1.1 智慧型掃描 14
6.1.4.1.2 自訂掃描 15
6.1.4.2 掃描目標 15
6.1.4.3 掃描設定檔 15
6.1.5 ThreatSense 引擎參數設定 16
6.1.5.1 物件 16
6.1.5.2 選項 16
6.1.5.3 清除 16
6.1.5.4 排除 17
6.1.5.5 限制 17
6.1.5.6 其他 17
6.1.6 偵測到入侵 17
6.2 可移除的媒體掃描和封鎖 18
7. 網路釣魚防護 19
8. 防火牆 20
8.1 過濾模式 20
8.2 防火牆規則 20
8.2.1 建立新規則 21
8.3 防火牆區域 21
8.4 防火牆設定檔 21
8.5 防火牆防護記錄 21
9. Web 和電子郵件防護 22
9.1 Web 防護 22
9.1.1 連接埠 22
9.1.2 URL 清單 22
9.2 電子郵件防護 22
9.2.1 POP3 通訊協定檢查 23
9.2.2 IMAP 通訊協定檢查 23
10. 家長控制 24
11. 更新 25
11.1 更新設定 25
11.1.1 進階選項 25
11.2 如何建立更新工作 25
11.3 將 ESET Cyber Security Pro 升級為新版本 25
11.4 系統更新 26
12. 工具 27
12.1 防護記錄檔案 27
12.1.1 防護記錄維護 27
12.1.2 防護記錄過濾 27
12.2 排程器 28
12.2.1 建立新工作 28
12.2.2 建立使用者定義的工作 29
12.3 隔離區 29
12.3.1 隔離檔案 29
12.3.2 從隔離區還原 29
12.3.3 從隔離區提交檔案 30
12.4 執行中的處理程序 30
12.5 Live Grid 30
12.5.1 Live Grid 設定 31
13. 使用者介面 32
13.1 警告及通知 32
13.1.1 顯示警告 32
13.1.2 防護狀態 32
13.2 權限 33
13.3 內容功能表 33
14. 其他選項 34
14.1 匯入及匯出設定 34
14.2 Proxy 伺服器設定 34
15. 字彙 35
15.1 入侵類型 35
15.1.1 病毒 35
15.1.2 蠕蟲 35
15.1.3 特洛伊木馬程式 35

15.1.4 Rootkit 36
15.1.5 廣告程式 36
15.1.6 間諜程式 36
15.1.7 潛在不安全的應用程式 36
15.1.8 潛在不需要應用程式 36
15.2 **遠端攻擊類型** 37
15.2.1 DoS 攻擊 37
15.2.2 DNS Poisoning 37
15.2.3 連接埠掃描 37
15.2.4 TCP 去同步化 37
15.2.5 SMB Relay 37
15.2.6 ICMP 攻擊 38
15.3 **電子郵件** 38
15.3.1 廣告 38
15.3.2 惡作劇 38
15.3.3 網路釣魚 39
15.3.4 識別垃圾郵件詐騙 39

1. ESET Cyber Security Pro

ESET Cyber Security Pro 提供一種真正整合電腦安全性的新方法。最新版本的 ThreatSense® 掃描引擎結合了電子郵件用戶端防護、防火牆與家長控制，充分運用速度與精準度來保護電腦安全。所造就出的智慧型系統會持續警戒，保護您的電腦免遭攻擊和惡意軟體入侵。

ESET Cyber Security Pro 是經由長期努力所開發的完整安全性解決方案，結合了最嚴格的防護並佔用最低的系統使用量。這些包含 ESET Cyber Security Pro 的進階技術是以人工智慧為基礎，可主動清除病毒、蠕蟲、特洛伊木馬程式、間諜程式、廣告程式、Rootkit 和其他經網際網路的攻擊等入侵，且不會妨礙系統效能。

1.1 第 6 版最新功能

ESET Cyber Security Pro 第 6 版引進下列更新與改善：

- **網路釣魚防護** - 防止偽造的網站偽裝成受信任的網站以竊取您的個人資訊
- **系統更新** - ESET Cyber Security Pro 第 6 版功能包含多種修正與改善，包括作業系統更新的通知。若要深入瞭解此功能，請參閱系統更新 26 一節。
- **防護狀態** - 隱藏來自防護狀態畫面的通知 (例如 *電子郵件防護已停用* 或 *需要重新啟動電腦*)
- **待掃描媒體** - 可以將特定類型的媒體從即時掃描器中排除 (本機磁碟機、可移除的媒體、網路媒體)

1.2 系統需求

若要使 ESET Cyber Security Pro 發揮最佳效能，您的系統應滿足或超過下列硬體和軟體需求：

	系統需求
處理器架構	Intel 32 位元、64 位元
作業系統	macOS 10.6 或更新版本
記憶體	300 MB
可使用的磁碟空間	200 MB

2. 安裝

開始安裝程序之前，請關閉電腦中所有開啟的程式。ESET Cyber Security Pro 包含的元件可能與您電腦上已經安裝的其他防毒程式發生衝突。ESET 強烈建議移除其他任何防毒程式，以避免潛在的問題。

若要啟動安裝精靈，請執行下列任一個步驟：

- 如果您從安裝 CD/DVD 進行安裝，請將 CD/DVD 插入電腦，從桌面或 **[Finder]** 視窗予以開啟，然後按兩下 **[安裝]** 圖示。
- 如果您使用從 ESET 網站下載的檔案進行安裝，請開啟您下載的檔案，然後按兩下 **[安裝]** 圖示。

安裝精靈將引導您進行基本設定。在安裝的初始階段期間，安裝程式會自動線上檢查最新的產品版本。如果找到新的版本，您可在繼續安裝程序前選擇下載最新版本。

同意「使用者授權合約」後，您可以從下列選擇一種安裝模式：

- 一般安裝 6
- 自訂安裝 7

2.1 一般安裝

一般安裝模式包括適用於大多數使用者的配置選項。這些設定值結合優良的系統效能提供最大安全性。一般安裝是預設選項，如果您沒有特定設定的特殊需求，建議使用此選項。

ESET Live Grid
Live Grid 預早警告系統可協助您確保 ESET 可立即且持續收到新入侵情況的通知，以迅速保護我們的客戶。系統可將新威脅提交至 ESET 威脅實驗室，以在此分析並處理這些威脅。**[啟用 ESET Live Grid (建議)]** 預設為已選取。按一下 **[設定]**，以修改提交可疑檔案的詳細設定。如需更多資訊，請參閱 Live Grid 30。

潛在不需要應用程式
安裝程序的最後一個步驟是配置 **[潛在不需要應用程式]** 偵測。這些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。這些應用程式通常隨附於其他程式，且可能在安裝程序期間很難注意到。雖然這些應用程式通常會在安裝期間顯示通知，但亦可未經您的同意輕易安裝。

安裝 ESET Cyber Security Pro 後，應該執行電腦掃描以偵測是否有惡意程式碼。從主要功能表視窗中，按一下 **[電腦掃描]**，然後按一下 **[智慧型掃描]**。如需有關「指定」電腦掃描的更多資訊，請參閱指定電腦掃描 14 一節。

2.2 自訂安裝

自訂安裝模式是針對想要在安裝程序期間修改進階設定的進階使用者設計。

Proxy 伺服器
如果您使用的是 Proxy 伺服器，您現在可選取 **[我使用 Proxy 伺服器]** 來定義其參數。在下一個視窗中，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。如果您未使用 Proxy 伺服器，請選取 **[我不使用 Proxy 伺服器]**。如果您不確定是否有使用 Proxy 伺服器，可以藉由選取 **[使用系統設定 (建議)]**。

權限
在下一步中，您會定義能夠編輯程式配置的有權限使用者或群組。從左側的使用者清單中，選取使用者並將其 **[新增]** 到 **[有權限的使用者]** 清單中。若要顯示所有系統使用者，請選取 **[顯示所有使用者]**。如果您將 [有權限的使用者] 保留空白，則系統會視所有使用者都具有權限。

ESET Live Grid
Live Grid 預早警告系統可協助您確保 ESET 可立即且持續收到新入侵情況的通知，以迅速保護我們的客戶。系統可將新威脅提交至 ESET 威脅實驗室，以在此分析並處理這些威脅。**[啟用 ESET Live Grid (建議)]** 預設為已選取。按一下 **[設定 ..]** 以修改可疑檔案提交的詳細設定。如需更多資訊，請參閱 Live Grid 30。

潛在不需要應用程式
安裝程序的下一步是配置 **[潛在不需要應用程式]** 偵測。這些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。這些應用程式通常隨附於其他程式，且可能在安裝程序期間很難注意到。雖然這些應用程式通常會在安裝期間顯示通知，但亦可未經您的同意輕易安裝。

防火牆
在最後一個步驟中，您可選取防火牆過濾模式。如需更多詳細資訊，請參閱過濾模式 20。

安裝 ESET Cyber Security Pro 後，應該執行電腦掃描以偵測是否有惡意程式碼。從主要功能表視窗中，按一下 **[電腦掃描]**，然後按一下 **[智慧型掃描]**。如需有關「指定」電腦掃描的更多資訊，請參閱指定電腦掃描 14一節。

3. 產品啟動

安裝完成後，[產品啟動] 視窗會自動顯示。若要隨時存取產品啟動對話方塊，請按一下位於 macOS 功能表列 (畫面頂端) 中的 ESET Cyber Security Pro 圖示 ⓔ，然後再按一下 **[產品啟動 ..]**。

- **授權金鑰** - 格式為 XXXX-XXXX-XXXX-XXXX-XXXX 或 XXXX-XXXXXXXX 的唯一字串，用於識別授權擁有者和啟動授權。如果您購買的是零售盒裝產品，請使用授權金鑰啟動您的產品。授權金鑰通常位於產品包裝內或背部。
- **使用者名稱與密碼** - 如果您有使用者名稱與密碼，但不知道如何啟動 ESET Cyber Security Pro，請按一下 **[我有使用者名稱與密碼，該怎麼做？]**。系統會將您重新導向至 my.eset.com，在此您可以將您的憑證轉換至授權金鑰。
- **免費 BETA 測試** - 如果您在購買前想要先試用 ESET Cyber Security Pro，請選取此選項。請填入您的電子郵件地址以啟動有使用時間限制的 ESET Cyber Security Pro。您將可透過電子郵件收到試用版授權。每位客戶只能啟動一次不同產品的試用版授權。
- **購買授權** - 如果您沒有授權但想要購買授權，請按一下 [購買授權]。此選項會將您重新引導至當地的 ESET 經銷商網站。
- **稍後啟動** - 如果您這次不想啟動，請按一下此選項。

4. 解除安裝

若要解除安裝 ESET Cyber Security Pro，請執行下列任一個步驟：

- 將 ESET Cyber Security Pro 安裝 CD/DVD 插入電腦，從桌面或 **Finder** 視窗予以開啟，然後按兩下 **[解除安裝]**
- 開啟 ESET Cyber Security Pro 安裝檔案 (*.dmg*)，然後按兩下 **[解除安裝]**
- 啟動 **[Finder]**，開啟硬碟上的 **[應用程式]** 資料夾，按下 Ctrl 並按一下 **ESET Cyber Security Pro** 圖示，然後選取 **[顯示套件內容]**。開啟 **Contents** > **Helpers** 資料夾，然後按兩下 **Uninstaller** 圖示。

5. 基本概觀

ESET Cyber Security Pro 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。

從主要功能表可存取以下區段：

- **首頁** –提供關於您電腦防護狀態、防火牆、Web 和電子郵件防護與家長控制的資訊。
- **電腦掃描** –此區段可讓您配置及啟動指定電腦掃描 14。
- **[更新]** –顯示有關偵測模組更新的資訊。
- **設定** –選取此區段以調整您電腦的安全等級。
- **工具** –可存取防護記錄檔案 27、排程器 28、隔離區 29、執行中的處理程序 30和其他程式功能。
- **說明** –顯示說明檔案、網際網路知識庫、支援要求表單和其他程式資訊的存取方式。

5.1 鍵盤快捷鍵

執行 ESET Cyber Security Pro 時可使用的鍵盤快捷鍵包括：

- *cmd+,* - 顯示 ESET Cyber Security Pro 偏好設定，
- *cmd+O* - 調整 ESET Cyber Security Pro 主要 GUI 視窗大小為預設大小並將其移動至畫面中央，
- *cmd+Q* - 隱藏 ESET Cyber Security Pro 主要 GUI 視窗。您可以按一下 macOS 功能表列 (畫面頂端) 中的 ESET Cyber Security Pro 圖示 ⓔ，便可開啟該視窗，
- *cmd+W* - 關閉 ESET Cyber Security Pro 主要 GUI 視窗。

下列鍵盤快速鍵只有在 **[使用標準功能表]** 啟用時才能運作，位於 **[設定]** > **[進入應用程式喜好設定 ..]** > **[介面]**：

- *cmd+alt+L* - 開啟 **[防護記錄檔案]** 區段，
- *cmd+alt+S* - 開啟 **[排程器]** 區段，
- *cmd+alt+Q* - 開啟 **[隔離區]** 區段。

5.2 檢查防護狀態

若要檢視防護狀態，請按一下主要功能表中的 **[首頁]**。ESET Cyber Security Pro 模組作業的狀態摘要顯示在主要視窗。

5.3 如果程式運作不正常怎麼辦

模組若正常運作，會顯示綠色的圖示。模組若未正常運作，會顯示紅色驚嘆號或橙色通知圖示。同時會顯示模組的其他相關資訊，以及修正模組的建議解決方案。若要變更個別模組的狀態，請按一下每個通知訊息下方的藍色連結。

如果您無法使用建議的解決方案解決問題，您可以在 ESET 知識庫中搜尋解決方案，或連絡 ESET 客戶關懷。客戶關懷會快速回覆您的問題，並協助使用 ESET Cyber Security Pro 解決任何問題。

6. 電腦防護

您可以在 **[設定]** > **[電腦]** 中找到電腦配置。其中會顯示 **[即時檔案系統防護]** 和 **[可移除的媒體封鎖]** 的狀態。若要關閉個別模組，請將相關的模組按鈕切換至 **[已停用]**。請注意，這可能會降低電腦的防護能力。若要存取每個模組的詳細設定，請按一下 **[設定 ..]**。

6.1 病毒及間諜程式防護

病毒防護透過修改造成潛在威脅的檔案來防止惡意系統攻擊。如果偵測到含有惡意程式碼的威脅，「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威脅。

6.1.1 一般

在 **[一般]** 區段中 (**[設定]** > **[進入應用程式喜好設定 ..]**> **[一般]**)，您可以啟用下列應用程式類型的偵測：

- **潛在不需要應用程式** - 這些應用程式不一定是惡意的，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。如果它們存在於您的電腦上，系統的行為會有所不同 (相較於安裝應用程式前的行為)。最明顯的變更包括：不需要的快顯視窗、啟動及執行隱藏的程序、增加系統資源的使用、搜尋結果中的變更，以及與遠端伺服器通訊的應用程式。
- **潛在不安全的應用程式** - 這些應用程式是某些商業軟體和合法軟體，在未經使用者同意的情況下安裝這些軟體時，攻擊者便能取得濫用的機會。此類別包括如遠端存取工具等程式，因此預設停用此選項。
- **[可疑應用程式]** - 這些應用程式包括附帶 Packer 或 Protector 的壓縮程式。惡意軟體的作者通常會利用這些 Protector 類型的弱點以躲避偵測。Packer 是一種會將多種惡意軟體彙總為單一封裝的 Runtime 自我解壓縮可執行檔。最常見的 Packer 是 UPX、PE_Compact、PKLite 及 ASPack。使用不同的 Packer 壓縮時，偵測相同惡意軟體的結果可能會有所不同。Packer 也有不斷變動「病毒碼」的能力，使惡意程式更難以偵測或移除。

若要設定 檔案系統或 Web 和電子郵件排除 12，請按一下 **[設定 ..]** 按鈕。

6.1.1.1 排除

在 **[排除]** 區段中，您可以從掃描中排除特定檔案 資料夾、應用程式或 IP/IPv6 位址。

所有掃描器將排除列於 **[檔案系統]** 索引標籤中的檔案和資料夾：啟動、即時、指定 (電腦掃描)。

- **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，則代表該檔案只針對該威脅排除，但不是完全排除。如果該檔案在稍後被其他惡意軟體感染，則防毒模組仍會偵測到該檔案。
- + –建立新的排除。輸入到物件的路徑 (您也可以使用萬用字元 *和 ?) 或從樹狀結構中選取資料夾或檔案。
- − –移除已選取的項目
- **預設** –取消所有的排除

您可以在 **[Web 和電子郵件]** 索引標籤中排除特定 **[應用程式]** 或 **[IP/IPv6 位址]**，使其不必進行通訊協定掃描。

6.1.2 啟動防護

啟動檔案檢查會在系統啟動時自動掃描檔案。依預設，此掃描會在使用者登入或偵測模組更新之後定期執行為已排程工作。若要修改 ThreatSense 引擎參數設定以便進行啟動掃描，請按一下 **[設定]** 按鈕。您可參閱此章節 16以深入瞭解 ThreatSense 引擎設定。

6.1.3 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，並且根據各種事件觸發掃描。使用 ThreatSense 技術 (如 ThreatSense 引擎參數設定 16 所述) 時，針對新建立檔案及現有檔案，即時檔案系統防護可能有所不同。可更精確控制新建立的檔案。

依預設，在**[檔案開啟]**、**[檔案建立]** 或 **[檔案執行]** 時，所有檔案都會執行掃描。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。即時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 (如與其他即時掃描器發生衝突時)，可以按一下功能表列 (畫面頂端) 中的 ESET Cyber Security Pro 圖示 ⓔ，然後選取 **[停用即時檔案系統防護]**，終止即時防護。您也可以從主要程式視窗停用即時檔案系統防護 (按一下 **[設定]** > **[電腦]** 並將 **[即時檔案系統防護]** 切換至 **[已停用]**)。

下列媒體類型可以從 Real-time 掃描器排除：
- **[本機磁碟]** - 系統硬碟
- **[可移除的媒體]** - CD、DVD、USB 媒體、藍芽裝置等
- **[網路媒體]** - 所有對應的磁碟機

我們建議您使用預設值設定，只有在特殊情況下才修改掃描排除，例如掃描某些媒體而明顯減慢資料傳送速度時。

若要修改即時檔案系統防護的進階設定，請移至 **[設定]** > **[進入應用程式喜好設定 ..]**(或按下 *cmd+,*) > **[即時防護]**，然後按一下 **[進階選項]** 旁的 **[設定 ..]** (如進階掃描選項 13 所述)。

6.1.3.1 進階選項

在此視窗中，您可以定義由 ThreatSense 引擎掃描的物件類型。若要瞭解有關 **[自我解壓檔]**、**[運行時間壓縮器]** 和 **[進階啟發式]** 的更多資訊，請參閱 ThreatSense 引擎參數設定 16。

我們不建議在 **[預設壓縮檔設定]** 區段中進行變更，除非解決特定問題所需，因為更高的壓縮檔巢狀值會妨礙系統效能。

[用於已執行檔案的 ThreatSense 參數] - 根據預設，執行檔案時會使用 **[進階啟發式]**。我們強烈建議您保持啟用智慧型最佳化和 ESET Live Grid 以減輕對系統效能的影響。

提升網路磁碟區的相容性 - 當透過網路存取檔案，此選項可提升效能。若您在存取網路磁碟時體驗到速度減慢，則應啟用此選項。此功能在 macOS 10.10 及更新版本上使用系統檔案協調器。請注意，並非所有應用程式都支援系統檔案協調器，例如 Microsoft Word 2011 不提供支援，但 Word 2016 提供支援。

6.1.3.2 何時修改即時防護配置

即時防護是以 ESET Cyber Security Pro 維護系統安全時最重要的組成部分。修改即時防護參數時請小心。建議您僅在特定情況中修改這些參數。例如，當某個應用程式有衝突時。

ESET Cyber Security Pro 的所有設定在安裝後即已最佳化，為使用者提供最高等級的系統安全。若要還原預設設定，請按一下 **[即時防護]** 視窗左下方的 **[預設]**。[即時防護] 視窗位於 **[設定]** > **[進入應用程式喜好設定 ..]**> **[即時防護]**)。

6.1.3.3 檢查即時防護

若要確認即時防護為運作中並在偵測病毒，請下載 eicar.com 測試檔案，然後查看 ESET Cyber Security Pro 是否將該檔案識為威脅。此測試檔案是所有防毒程式都可以偵測到的特殊無害檔案。該檔案由 EICAR 協會 (European Institute for Computer Antivirus Research) 建立，目的是用來測試防毒程式的功能。

6.1.3.4 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。若要重新啟動即時防護，請在主要功能表中按一下 **[設定]** > **[電腦]** 並將 **[即時檔案系統防護]** 切換至 **[已啟用]**。或者您可以選取 **[啟用即時檔案系統防護]**，以在 **[即時防護]** 下的應用程式喜好設定視窗中啟用即時檔案系統防護。

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防護程式，則可能互相衝突。我們建議您解除可能在安裝系統上的任何其他防毒程式。

即時防護未啟動
如果系統啟動時未啟動即時防護，可能是因為與其他程式衝突。如果是這種情況，請洽詢 ESET 客戶關懷。

6.1.4 指定電腦掃描

如果您懷疑電腦受感染 (行為異常)，請執行 **[智慧型掃描]** 以檢查電腦是否含有入侵。為了取得最完善的防護能力，基於例行安全考量應定期執行電腦掃描，而不只是在懷疑受感染時執行。定期掃描可以偵測到即時掃描器在入侵儲存至磁碟時，未偵測到的入侵。若在停用即時掃描器期間受到感染，或偵測模組不是最新的，就可能發生上述情況。

我們建議您一個月至少執行一次指定電腦掃描。您可以透過 **[工具]** > **[排程器]** 將掃描配置為已排程的工作。

我們建議您一個月至少執行一次指定電腦掃描。您可以透過 **[工具]** > **[排程器]** 將掃描配置為已排程的工作。

您也可以從桌面或 **[Finder]** 視窗將選取的檔案或資料夾拖放至 ESET Cyber Security Pro 主畫面、Dock 圖示、功能表列圖示 (畫面頂端) 或應用程式圖示 (位於 */Applications* 資料夾)。

6.1.4.1 掃描類型

有兩種可用的指定電腦掃描類型。**[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訂義的掃描設定檔，以及選擇特定掃描目標。

6.1.4.1.1 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。它的主要優點是可以輕鬆執行作業，而不需要詳細的掃描配置。智慧型掃描會檢查所有資料夾中的所有檔案，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詳細資訊，請參閱清除 16 一節。

6.1.4.1.2 自訂掃描

如果您要指定掃描參數 (例如掃描目標及掃描方法)，則可選用最佳的**自訂掃描**。執行 「自訂」掃描的優點是可以詳細地配置參數。您可以將不同的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]**，然後從樹狀結構中選取特定的 **[掃描目標]**。亦可輸入您希望納入的資料夾或檔案路徑，更精確地指定掃描目標。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]**。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]**。

附註：建議具有使用防毒程式經驗的進階使用者使用 「自訂掃描」執行電腦掃描。

6.1.4.2 掃描目標

掃描目標樹狀結構可讓您選取要進行病毒掃描的檔案與資料夾。您也可以根據設定檔的設定來選取資料夾。

輸入您希望納入掃描的資料夾或檔案路徑，以更精確地定義掃描目標。選取與指定檔案或資料夾對應的核取方塊，藉此從列出電腦上所有可用資料夾的樹狀結構中選取目標。

6.1.4.3 掃描設定檔

您偏好的掃描設定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，從主要功能表中按一下 **[設定]** > **[進入應用程式喜好設定 ..]** (或按下 *cmd+,*) > **[電腦掃描]**，然後再按一下目前設定檔清單旁的 **[編輯 ..]**。

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 16 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 Runtime Packer 或潛在不安全的應用程式，並且要套用 「完全清除」。在 **[指定掃描器設定檔清單]** 視窗中，輸入設定檔名稱，按一下 **[新增]** 按鈕後按一下 **[確定]** 確認。然後設定 **[ThreatSense 引擎]** 和 **[掃描目標]** 來調整參數以符合您的需求。

如果指定掃描完成後，您想要關閉作業系統並讓電腦關機，請使用 **[掃描後關閉電腦]** 選項。

6.1.5 ThreatSense 引擎參數設定

ThreatSense 是包含了數種複雜威脅偵測方法的 ESET 專利技術。此技術是主動式的，也就是說它也可在新威脅擴散的前幾個小時期間提供保護。該技術使用多種方法組合 (代碼分析、代碼模擬、一般資料庫等)，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。此外，ThreatSense 技術還可以成功防範 Rootkit。

ThreatSense 技術設定選項允許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
- 清除的層級等

若要開啟設定視窗，請按一下 **[設定 > 進入應用程式喜好設定]** (或按一下 *cmd+,*)，然後按一下 **[啟動防護]**、**[即時防護]** 和 **[電腦掃描]** 模組中的 ThreatSense 引擎 **[設定]** 按鈕，這些功能全部使用 ThreatSense 技術 (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：

- **[啟動防護]** - 自動啟動檔案檢查
- **即時防護** - 即時檔案系統防護
- **電腦掃描** - 指定電腦掃描
- **Web 存取防護**
- **電子郵件防護**

每個模組的 ThreatSense 參數都已特別最佳化，其修改對系統作業有很大影響。例如，變更設定一定會掃描 Runtime Packer，或啟用即時檔案系統防護模組中的進階啟發式可能會造成系統速度變慢。因此，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。

6.1.5.1 物件

[物件] 區段可讓您定義要掃描是否有入侵的檔案。

- **[捷徑]** - (僅限電腦掃描) 掃描包含文字字串的檔案，該文字字串由作業系統解譯並接著作為到另一個檔案或目錄的路徑。
- **[電子郵件檔案]** - (無法在即時防護中使用) 掃描電子郵件檔案。
- **[信箱]** - (無法在即時防護中使用) 掃描系統中的使用者信箱。使用此選項的方法錯誤可能導致與您的電子郵件用戶端產生衝突。如需瞭解更多有關此選項的優點與缺點的資訊，請閱讀下列知識庫文章。
- **[壓縮檔]** - (無法在即時防護中使用) 掃描壓縮在壓縮檔 (.rar、zip、arj、tar 等) 中的檔案。
- **[自我解壓縮檔]** - (無法在即時防護中使用) 掃描包含在自我解壓縮檔中的檔案。
- **[Runtime Packers]** - Runtime Packer (不同於標準壓縮檔類型) 會在記憶體中解壓縮。選取此選項後，也會掃描 UPX、yoda、ASPack、FGS 等標準靜態壓縮器。

6.1.5.2 選項

在 **[選項]** 區段中，您可以選取在掃描系統時使用的方法。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。啟發式偵測的主要優點是可以偵測之前不存在的新惡意軟體。
- **進階啟發式** –進階啟發式由獨特的啟發式演算法組成，由 ESET 開發，最佳化偵測以高階程式設計語言所撰寫的電腦蠕蟲及特洛伊木馬程式。程式的偵測能力因進階啟發式而大幅提高。

6.1.5.3 清除

清除設定可決定掃描器清除受感染檔案的方法。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您選擇處理方法。
- **標準清除** - 程式會嘗試自動清除或刪除受感染檔案。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，也會顯示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 (包括壓縮檔)。只有系統檔案例外。如果無法清除檔案，系統會通知您並要求您選取要採取的處理方法類型。

警告： 在「預設標準清除」模式中，只有在壓縮檔中的所有檔案都受到感染時，才會刪除整個壓縮檔。如果壓縮檔包含合法檔案與受感染的檔案，則不會刪除壓縮檔。如果在「完全清除」模式中偵測到受感染的壓縮檔，則即使未感染檔案存在，也會刪除整個壓縮檔。

6.1.5.4 排除

副檔名是檔案名稱中以句點隔開的部份。副檔名可定義檔案的類型及內容。ThreatSense 參數設定的這個區段可讓您定義要從掃描排除的檔案類型。

依預設，會掃描所有檔案，無論其副檔名為何。可以將任何副檔名新增至從掃描中排除的檔案清單。使用 + 和 − 按鈕，您可以啟用或禁止特定副檔名的掃描。

如果掃描某些檔案類型會造成應用程式無法正常運作，有時必須排除這種檔案不予掃描。例如，可能建議排除 *log*、*cfg* 和 *tmp* 檔案。輸入檔案副檔名的正確格式為：
log
cfg
tmp

6.1.5.5 限制

[限制] 區段可讓您指定物件的大小上限，以及要掃描的巢狀壓縮檔層級：

- **大小上限:**定義要掃描的物件大小上限。定義大小上限後，防毒模組則僅會掃描小於指定大小的物件。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。
- **掃描時間上限:** 定義分配用於掃描物件的時間上限。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。
- **巢狀層級上限:** 指定壓縮檔掃描的深度層級上限。我們不建議變更預設值 10；在正常情況下，應該沒有要修改預設值的理由。如果由於巢狀壓縮檔的數目而提前結束掃描，則壓縮檔會保持未檢查狀態。
- **檔案大小上限:** 此選項可讓您指定要掃描的壓縮檔中，所包含檔案的大小上限 (解壓縮時)。如果掃描由於此上限的結果而提前結束，則壓縮檔會保持未檢查狀態。

6.1.5.6 其他

啟用智慧型最佳化
啟用「智慧型最佳化」時，系統會最佳化設定以確保在不影響掃描速度的情況下達成最有效率的掃描層級。各種防護模組皆會利用不同的掃描方法進行智慧掃描。產品中沒有嚴格地定義「智慧型最佳化」。「ESET 開發小組」繼續實作新的變更，然後透過定期更新將變更整合至 ESET Cyber Security Pro。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。

[掃描替代資料串流] (僅限指定掃描器)
由檔案系統使用的替代資料串流(資源 資料分支) 由檔案系統使用，是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。

6.1.6 偵測到入侵

入侵可以從不同的進入點到達系統：網頁、共用資料夾、電子郵件，或可移除的電腦裝置 (USB、外部磁碟、CD、DVD 等)。

如果您的電腦出現速度變慢、經常停止等惡意軟體感染的徵兆，我們建議您進行下列步驟：

1. 按一下 **[電腦掃描]**。
2. 按一下 **[智慧型掃描]** 按鈕 (如需更多資訊，請參閱智慧型掃描 14 節)。
3. 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。

在此為了說明 ESET Cyber Security Pro 如何處理入侵，請假設使用預設清除層級的即時檔案系統監視器偵測到入侵。即時防護通常會嘗試清除或刪除檔案。如果沒有針對即時防護模組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]**，因為此選項會將受感染的檔案保留在受感染的狀態。但若您確定檔案無害，只是因失誤而偵測為入侵，則該情況適用此選項。

清除及刪除 - 如果檔案受到已附加惡意程式碼的病毒攻擊，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。

刪除壓縮檔中的檔案 - 在預設清除模式中，壓縮檔只有在僅包含受感染的檔案而不包含未感染檔案時，才會整個遭到刪除。也就是說，如果壓縮檔還包含無害的未感染檔案，則不會進行刪除。但執行 **[完全清除]** 掃描時請小心，因為在 「完全清除」模式中，只要壓縮檔內含有至少一個受感染的檔案時，即無論壓縮檔中其他檔案的狀態為何，都會刪除壓縮檔。

6.2 可移除的媒體掃描和封鎖

ESET Cyber Security Pro 可針對可移除的媒體裝置 (CD、DVD、USB、iOS 裝置等) 執行指定掃描。

可移除的媒體可能包含惡意程式碼，讓您的電腦瀕於危險。若要封鎖可移除的媒體，請按一下 **[媒體封鎖設定]** (參閱上圖) 或主要視窗中的 **[設定]** > **[進入應用程式喜好設定 ..]**> **[媒體]**，然後選取 **[啟用可移除的媒體封鎖]**。若要允許存取特定類型的媒體，請取消選取所需媒體磁碟區。

附註：若要允許存取透過 USB 纜線連接電腦的外部 CD-ROM 光碟機，請取消選取 **[CD-ROM]** 選項。

7. 網路釣魚防護

網路釣魚 一詞表示一種使用社會工程的犯罪活動 (操控使用者以取得機密訊)。網路釣魚通常用來取得如銀行帳戶號碼、信用卡號碼、PIN 碼或使用者名稱及密碼等敏感資料。

我們建議您將網路釣魚防護 (**[設定]** > **[進入應用程式喜好設定 ..]**> **網路釣魚防護**) 保持啟用。來自 ESET 惡意軟體資料庫列出之網站或網域的所有潛在網路釣魚攻擊將遭到封鎖，並顯示警告通知以告知攻擊的相關資訊。

8. 防火牆

防火牆會根據指定的過濾規則允許或拒絕各個網路連線，藉此控制所有出入系統的網路流量。它可針對來自遠端電腦的攻擊提供防護，並封鎖某些服務。此外，它還可針對 HTTP、POP3 和 IMAP 通訊協定提供病毒防護。

您可以在 **[設定]** > **[防火牆]** 中找到防火牆配置。它還可讓您調整過濾模式、規則和詳細設定。您也可以在此存取更詳細的程式設定。

如果您將 **[封鎖所有網路流量:中斷網路]** 切換至 **[已啟用]**，則防火牆將封鎖所有外來及對外的通訊。只有當您懷疑可能遭到嚴重安全性風險而需要中斷與網路的連線時，才可使用此選項。

8.1 過濾模式

ESET Cyber Security Pro 防火牆提供三種過濾模式。您可在 ESET Cyber Security Pro 喜好設定 (按下 *cmd+,*) > **[防火牆]** 中找到這些過濾模式設定。防火牆的行為會根據選取的模式而有所改變。篩選模式也會影響需要的使用者互動層級。

已封鎖所有流量 - 將封鎖所有外來及對外的連線。

含例外情況的自動模式 - 預設模式。此模式適合偏好簡單及方便使用的防火牆且不需要定義規則的使用者。自動模式允許特定系統的標準對外流量，並封鎖所有網路端非初始化的連線。您也可以新增自訂、使用者定義的規則。

互動模式 –可讓您針對防火牆建置自訂配置。當系統偵測到通訊且沒有要套用到該通訊的現有規則時，則會顯示一個對話視窗以報告不明的連線。該對話視窗可讓您選擇允許或拒絕通訊，以及是否要將允許或拒絕動作記憶為防火牆的新規則。如果您這時選擇建立新規則，則之後都將根據規則允許或封鎖此類型的所有連線。

若要將所有封鎖連線的相關詳細資訊記錄到防護記錄檔案中，請選取 **[記錄所有封鎖的連線]**。若要檢閱防火牆防護記錄，從主要功能表中按一下 **[工具]** > **[防護記錄]**，然後在 **[防護記錄]** 下拉式功能表選取 **[防火牆]**。

8.2 防火牆規則

規則代表一組條件，這些條件用於測試所有網路連線，以及決定已指派給這些條件的動作。如果已建立由規則定義的連線，則您可以使用防火牆規則來定義要採取的處理方法類型。

傳入連線是由嘗試與本機系統建立連線的遠端電腦所初始化。對外連線則相反，由本機系統連絡遠端電腦。

如果系統偵測到新的不明通訊，請務必謹慎考慮是否該允許或拒絕該通訊。來路不明、不安全或不明的連線會對系統造成安全性威脅。如果建立這類連線，我們建議您特別注意嘗試與您的電腦連線的遠端電腦和應用程式。許多的入侵行為都會嘗試取得並傳送私人資料，或將其他惡意應用程式下載至主機工作站。防火牆允許您偵測及終止此類連線。

依預設，由 Apple 簽署的應用程式可以自動存取網路。如果您想要停用此功能，取消選取 **[允許由 Apple 所簽署的軟體可自動存取網路]**。

8.2.1 建立新規則

[規則] 索引標籤包含所有規則的清單，這些規則皆套用於由個別應用程式所產生的流量。系統會根據使用者對新通訊的反應來自動新增規則。

1. 若要建立新規則，請按一下 **[新增 ..]**。，輸入規則名稱，然後將應用程式圖示拖放到空白欄位，或按一下 **[瀏覽 ..]** 在 */Applications* 資料夾中尋找該程式。若將規則套用至安裝在電腦上的所有應用程式，請選取 **[所有應用程式]** 選項。
2. 在下一個視窗中，指定通訊的 **[處理方法]** (允許或拒絕所選應用程式與網路之間的通訊) 和 **[方向]** (傳入、傳出或兩者)。您可以將與此規則有關的所有通訊記錄到防護記錄檔案中，若要這麼做，請選取 **[防護記錄規則]** 選項。若要檢閱防護記錄，請按一下 ESET Cyber Security Pro 主要功能表的 **[工具]** > **[防護記錄]**，然後在 **[防護記錄]** 下拉式功能表選取 **[防火牆]**。
3. 在 **[通訊協定 連接埠]** 區段中，選取應用程式通訊所使用的通訊協定與連接埠號碼 (如果已選取 TCP 或 UDP 通訊協定)。傳輸通訊協定層可提供安全且有效率的資料傳輸。
4. 最後，指定規則的 **[目的地]** 條件 (IP 位址、範圍、子網路、乙太網路或網際網路)。

8.3 防火牆區域

區域代表可建立一個邏輯群組的網路位址組合。指定群組中的每個位址都會被指派一個為整個群組集中定義的類似規則。

您可以按一下 **[新增 ..]** 來建立這些區域。輸入區域的 **[名稱]** 和 **[說明]** (選用)，選取此區域所屬設定檔，並新增 IPv4/IPv6 位址、位址範圍、子網路、Wi-Fi 網路或介面。

8.4 防火牆設定檔

[設定檔] 可讓您控制 ESET Cyber Security Pro 防火牆的行為。當您建立或編輯防火牆規則時，可將其指派至特定設定檔。當您選取設定檔時，只會套用全域規則 (未指定任何設定檔) 以及已指派至該設定檔的規則。您可以建立已指派不同規則的多個設定檔，以輕鬆地變更防火牆行為。

8.5 防火牆防護記錄

ESET Cyber Security Pro 防火牆會將所有的重要事件儲存在防護記錄檔案中。若要從主要功能表存取防火牆防護記錄，請按一下 **[工具]** > **[防護記錄]**，然後在 **[防護記錄]** 下拉式功能表選取 **[防火牆]**。

防護記錄檔案是一種相當重要的工具，可用來偵測錯誤並揭露系統遭到入侵的情況。ESET 防火牆防護記錄包含下列資料：

- 事件日期及時間
- 事件名稱
- 來源
- 目標網路位址
- 網路通訊協定
- 套用的規則
- 受影響的應用程式
- 使用者

對此資料進行完整分析可協助您偵測任何破壞系統安全性的企圖。許多其他因素可指出潛在的安全風險，並能使用防火牆加以防禦，例如：從不明位置進行連線的頻率過高、多個建立連線的嘗試、不明的應用程式通訊或連接埠號碼不尋常。

9. Web 和電子郵件防護

若要使用 Web 和電子郵件防護，請從主要功能表中，按一下 **[設定]** > **[Web 和電子郵件]**。您也可以點一下 **[設定]**，在此存取每個模組的詳細設定。

- **Web 存取防護** - 監視 Web 瀏覽器與遠端伺服器的 HTTP 通訊。
- **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。
- **網路釣魚防護** - 來自 ESET 惡意軟體資料庫列出之網站或網域的所有潛在網路釣魚攻擊將遭到封鎖。

9.1 Web 防護

Web 存取保護會監視 Web 瀏覽器與遠端伺服器之間的通訊，以遵守 HTTP (超文字傳輸通訊協定) 規則。

可藉由定義 HTTP 通訊的連接埠數量 22和 或 URL 位址 22來取得 Web 過濾。

9.1.1 連接埠

在 **[連接埠]** 索引標籤中，您可以定義用於 HTTP 通訊的連接埠號碼。依預設會預先定義連接埠號碼 80、8080 和 3128。

9.1.2 URL 清單

[URL 清單] 區段可讓您指定要在檢查中封鎖、允許或排除的 HTTP 位址。位於封鎖的位址清單中的網站將無法進行存取。位於排除的位址清單中的網站可進行存取，但系統不會掃描網站檢查是否有惡意程式碼。

若要允許僅存取 **[允許的 URL]** 清單中所列的 URL 位址，請選取 **[限制 URL 位址]** 選項。

若要啟動清單，請選取清單名稱旁的 **[已啟用]**。如果您想在進入目前清單中的位址時收到通知，請選取 **[已通知]**。

您可以在任何清單中使用特殊符號 *(星號) 和 ?(問號)。星號可代替任何字元字串，問號則可代替任何符號。在指定排除的位址時應特別注意，因為此清單只能包含受信任且安全的位址。同樣地，在此清單中，您還必須確認符號 *和 ？的使用是否正確。

9.2 電子郵件防護

電子郵件防護可控制透過 POP3 和 IMAP 通訊協定收到的電子郵件通訊。在檢查傳入的郵件時，程式會使用 ThreatSense 掃描引擎中包含的所有進階掃描方法。POP3 和 IMAP 通訊協定通訊的掃描與使用的電子郵件用戶端並沒有關聯。

ThreatSense 引擎：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]** 以顯示詳細掃描器設定視窗。

[將標籤訊息附加到電子郵件註腳] –在掃描電子郵件之後，包含掃描結果的通知會附加到郵件中。您不能完全依賴標籤訊息，因為其可能會在有問題的 HTML 郵件中遭到忽略，某些病毒也會偽造這些訊息。可用選項如下：
- **[絕不]** –不會新增任何標籤訊息
- **[僅針對受感染電子郵件]** –僅有包含惡意軟體的郵件會標記為已勾選
- **[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中包含病毒警告，請選取此核取方塊。此功能可針對受感染的電子郵件進行簡易過濾。它也可以提升收件者的信任層級，並且在偵測到入侵情況時提供與特定電子郵件或寄件者威脅層級有關的實用資訊。

[已新增到受感染電子郵件主旨的範本] –編輯此範本可修改受感染電子郵件的主旨字首格式。

您也可以在此視窗底部啟用 /停用檢查透過 POP3 和 IMAP 通訊協定收到的電子郵件通訊。若要瞭解更多相關資訊，請參閱下列主題：
- POP3 通訊協定檢查 23
- IMAP 通訊協定檢查 23

9.2.1 POP3 **通訊協定檢查**

POP3 通訊協定是最為廣泛使用的通訊協定，可用來接收電子郵件用戶端應用程式中的電子郵件通訊。無論使用的電子郵件用戶端為何，ESET Cyber Security Pro 都可針對此通訊協定提供防護。

提供此控制的防護模組會在系統啟動時自動初始化，並接著在記憶體中作用。確定該模組已啟用讓通訊協定過濾器能正確運作，且無需重新配置您的電子郵件用戶端就會自動執行 POP3 通訊協定檢查。依預設，系統會掃描連接埠 110 上的所有通訊，不過您可以視需要新增其他通訊連接埠。連接埠號碼必須以逗點分隔。

如果您已啟用 **[啟用 POP3 通訊協定檢查]** 選項，系統會監視所有 POP3 流量中是否含有任何惡意軟體。

9.2.2 IMAP **通訊協定檢查**

網際網路訊息存取通訊協定 (IMAP) 是用來擷取電子郵件的另一種網際網路通訊協定。IMAP 與 POP3 相較具有一些優勢。舉例來說，多個用戶端可同時連線至相同的信箱，並且可保留郵件狀態資訊，例如郵件是否已讀取、已回覆或已刪除。無論使用的電子郵件用戶端為何，ESET Cyber Security Pro 都可針對此通訊協定提供防護。

提供此控制的防護模組會在系統啟動時自動初始化，並接著在記憶體中作用。確定該 IMAP 通訊協定檢查已啟用讓模組能正確運作；系統已自動執行 IMAP 通訊協定控制，不需要重新配置您的電子郵件用戶端。依預設，系統會掃描連接埠 143 上的所有通訊，不過您可以視需要新增其他通訊連接埠。連接埠號碼必須以逗點分隔。

如果您已啟用 **[啟用 IMAP 通訊協定檢查]**，系統會監視通過 IMAP 的所有流量以檢查是否含有任何惡意軟體。

10. 家長控制

[家長控制] 區段可讓您配置家長控制設定，提供自動化工具以協助家長保護他們的小孩。其目的在於防止孩童及青少年存取包含不當或有害內容的網頁。您可以使用家長控制來封鎖有潛在攻擊性資料的網頁。此外，家長最多可禁止存取 27 種預先定義的網站類別。

您的使用者帳戶會列於 **[家長控制]** 視窗 (**[設定]** > **[進入應用程式喜好設定 ..]**> **[家長控制]**) 中。請選取一個供家長控制使用的帳戶。若要指定所選帳戶的防護層級，請按一下 **[設定 ..]**。若要建立新帳戶，請按一下 **[新增 ..]**。這會將您重新導向 macOS 系統帳戶視窗。

選取 **[家長控制設定]** 視窗中 **[設定設定檔]** 下拉式功能表中其中一個預先定義的設定檔或複製其他使用者帳戶中的家長設定。每個設定檔都包含已修改的允許類別清單。已勾選的類別表示已允許。將滑鼠移至類別上方會顯示屬於該類別的網頁清單。

若要修改 **[允許和封鎖的網頁]** 清單，請按一下位於視窗底部的 **[設定 ..]**，並在所需的清單中新增網域名稱。請不要輸入 *http://*。您不需要使用萬用字元 (*)。如果您只輸入網域名稱，就會包含所有的子網域。例如，如果您將 *google.com* 新增到 **[允許的網頁清單]**，則將允許所有的子網域 (*mail.google.com* 、*news.google.com* 、*maps.google.com* 等)。

附註：封鎖或允許特定網頁會比封鎖或允許整個網頁類別更為準確。

11. 更新

維持最高等級安全性必須定期更新 ESET Cyber Security Pro。「更新」模組下載最新的偵測模組，確保程式永遠是最新程式。

從主要功能表中按一下 **[更新]** 以檢視目前 ESET Cyber Security Pro 的更新狀態，包括上一次成功更新日期與時間，並在需要時更新。若要開始手動更新程序，請按一下 **[更新模組]**。

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 -已安裝的模組是最新的]** 訊息。如果無法更新模組，建議您檢查更新設定 25。此錯誤最常見的原因是輸入的驗證資料 (使用者名稱和密碼) 不正確或連線設定 34的配置錯誤。

更新視窗內也含有偵測引擎版本號碼。版本號碼會連結至 ESET 的網頁，其中列出偵測引擎更新資訊。

11.1 更新設定

若要刪除所有暫存的更新資料，請按一下 **[清除更新快取]** 旁的 **[清除]**。如果更新時遇到困難，請使用此選項。

11.1.1 進階選項

若要停用每次成功更新後顯示的通知，請選取 **[不顯示成功更新的通知]**。

啟用 **[發佈前更新]** 以下載最後測試階段中的開發模組。發佈前更新通常包含產品問題的修正。**[延遲更新]** 會在發佈後的數小時下載更新，以確保用戶端會在經確認沒有遺漏任何問題後才接收更新。

ESET Cyber Security Pro 會記錄偵測與程式模組的快照，以搭配 **[更新還原]** 功能使用。讓 **[建立更新檔案快照]** 為啟用，可使 ESET Cyber Security Pro 自動記錄這些快照。如果您懷疑偵測模組和 或程式模組的新更新可能不穩定或損壞，您可以使用還原功能來還原為上一版，並在一段期間內停用任何更新。或者，如果您先前已無限期延後更新，您也可以啟用這些停用的更新。當使用 [更新還原] 來還原為上一版時，請使用 **[設定暫停時間為]** 下拉式功能表來指定您想要暫停更新的時段。如果您選取 **[直到撤銷前]**，則一般更新在您手動還原之前不會恢復進行。設定要暫停更新的時段時請小心。

[自動設定資料庫有效期限] –允許設定時間上限 (以天計)，超過期限後，偵測模組會回報過期。預設值為 7 天。

11.2 如何建立更新工作

您可以按一下主要功能表中的 **[更新]**，再按一下 **[更新模組]**，手動觸發更新。

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

- **定期自動更新**
- **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 28一節。

11.3 將 ESET Cyber Security Pro 升級為新版本

若要保持最嚴格的防護，使用 ESET Cyber Security Pro 的最新組建是很重要的。若要檢查是否有新版本，請按一下主要功能表中的 **[首頁]**。有新組建可用時，系統將會顯示訊息。按一下 **[深入瞭解 ..]** 在新視窗中顯示新組建的版本號碼及變更記錄。

請按一下 **[是]** 以下載最新組建，或按一下 **[不是現在]** 以關閉視窗並於稍後下載升級。

如果您按一下 **[是]**，系統會將該檔案下載至您的下載資料夾 (或是您的瀏覽器預設資料夾)。檔案完成下載之後，請啟動該檔案並遵循安裝指示。您的使用者名稱和密碼將會自動地傳送至新的安裝。建議您定期檢查升級程式，尤其是透過 CD 或 DVD 安裝 ESET Cyber Security Pro 時。

11.4 系統更新

macOS 系統更新功能是專為保護使用者免於惡意軟體傷害的重要元件。為了最嚴格的安全性，我們建議在提供可用的更新後立刻安裝。ESET Cyber Security Pro 會依照您指定的層級通知遺漏的更新。您可以在 **[設定]** > **[進入應用程式喜好設定 ..]**(或按下 *cmd+,*) > **[警告及通知]** > **[設定 ..]** 中變更 **[作業系統更新]** 旁的 **[顯示條件]** 選項調整更新通知的可用性。

- **顯示所有更新** - 系統更新遺漏時將隨時顯示通知
- **僅顯示建議更新** - 只通知您建議的更新

如果您不想收到遺漏更新的通知，取消選取 **[作業系統更新]** 旁的核取方塊。

通知視窗會提供透過 macOS 原生工具 「軟體更新」所更新的 macOS 作業系統與應用程可用更新的概要。您可以從通知視窗直接安裝更新，或從 ESET Cyber Security Pro **[首頁]** 區段按一下 **[安裝遺漏的更新]**。

通知視窗包含應用程式名稱、版本、大小、屬性 (旗標) 與可用更新的其他資訊。[旗標] 欄包含下列資訊：

- **建議** - 作業系統製造商建議您安裝此更新以加強系統安全性與穩定性
- **重新啟動** - 需要重新啟動電腦才可繼續安裝
- **關閉** - 必須關閉電腦然後再重新開機才可繼續安裝

通知視窗顯示由命令列工具 「softwareupdate」所擷取的更新。此工具所擷取的更新與 「軟體更新」應用程式所顯示的更新可能不同。如果您想安裝顯示於 「遺漏系統更新」視窗中的所有可用更新，以及 「軟體更新」應用程式未顯示的更新，您必須使用 「softwareupdate」命令列工具。如需深入瞭解有關此工具的資訊，請在 [終端機] 視窗中輸入 man softwareupdate 以參閱 「softwareupdate」手冊。僅建議進階使用者使用。

12. 工具

[工具] 功能表包含的模組可簡化程式管理，並可為進階使用者提供其他選項。

12.1 防護記錄檔案

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

從 ESET Cyber Security Pro 主要功能表中按一下 **[工具]** > **[防護記錄]**，可存取防護記錄檔案。使用視窗頂端的 **[防護記錄]** 下拉式功能表選取所需的防護記錄類型。以下是可用的防護記錄：

1. **偵測到威脅** - 使用此選項，可檢視與偵測入侵相關之事件的所有資訊。
2. **事件** - 此選項專供協助系統管理員及使用者用解決問題。ESET Cyber Security Pro 執行的所有重要處理方法都會記錄在「事件」防護記錄中。
3. **電腦掃描** - 所有已完成的掃描結果都會顯示在此防護記錄中。按兩下任何項目，以檢視各個指定電腦掃描的詳細資料。
4. **家長** - 家長控制所封鎖的所有網頁清單。
5. **防火牆** - 此防護記錄包含所有網路相關事件的結果。
6. **已過濾網站** - 此清單在您要檢視 Web 存取防護所封鎖的網站清單時相當實用。這些防護記錄會顯示開啟特定網站連線的時間、URL、狀態、IP 位址、使用者與應用程式。

在每個區段中，選取項目並按一下 **[複製]** 按鈕，可將顯示的資訊直接複製到剪貼簿。

12.1.1 防護記錄維護

ESET Cyber Security Pro 的記錄配置可從主要程式視窗存取。按一下 **[設定]** > **[進入應用程式喜好設定]** (或按下 *cmd+,*) > **[防護記錄檔案]**。您可以指定下列用於防護記錄檔案的選項：

- **自動刪除舊的防護記錄** - 將自動刪除超過指定天數的防護記錄項目 (依預設為 90 天)。
- **自動最佳化防護記錄檔案** - 如果超出指定的未使用記錄百分比，則將啟用自動重組防護記錄檔案 (依預設為 25%)。

顯示在圖形使用者介面、威脅和事件訊息的所有相關資訊可使用一般人可閱讀的文字格式儲存，例如純文字或 CSV (Comma-separated values)。如果您想使用第三方工具處理這些檔案，請選取 **[啟用記錄至文字檔]** 旁的核取方塊。

若要定義儲存防護記錄檔案的目標資料夾，請按一下 **[進階選項]** 旁的 **[設定]**。

根據在 **[文字防護記錄檔案]下方選取的選項：[編輯]**，您可以在儲存防護記錄時寫入下列資訊：

- 將 *無效的使用者名稱和密碼* 、*無法更新模組* 等事件寫入 eventslog.txt 檔案
- 將啟動掃描器、即時防護或電腦掃描偵測到的威脅儲存至名為 threatslog.txt 的檔案
- 將所有已完成掃描的結果以 scanlog.NUMBER.txt 格式儲存。
- 所有與透過防火牆通訊的相關事件皆會寫入至 firewalllog.txt

若要配置 **[預設電腦掃描防護記錄]** 過濾器，請按一下 **[編輯]**，然後視需要選取 取消選取防護記錄類型。您可在防護記錄過濾 27中找到這些防護記錄類型的進一步說明。

12.1.2 防護記錄過濾

防護記錄可儲存重要系統事件的相關資訊。防護記錄過濾功能可讓您顯示和特定事件類型相關的記錄。

最常使用的防護記錄類型如下所示：

- **嚴重警告** - 嚴重系統錯誤 (例如，病毒防護無法啟動)
- **錯誤** - 例如「*下載檔案時發生錯誤* 」及嚴重錯誤等錯誤訊息
- **警告** - 警告訊息
- **資訊性記錄** - 資訊性的訊息，包括成功更新、警告等
- **診斷記錄** - 微調程式與上述所有記錄所需的資訊。

12.2 排程器

您可在 **[工具]** 下方的 ESET Cyber Security Pro 主要功能表中找到 **[排程器]**。**[排程器]** 包含所有已排程的工作及其配置內容 (例如預先定義的日期、時間、使用的掃描設定檔) 的清單。

排程器會使用預先定義的配置與內容來管理和啟動已排程的工作。配置與內容包含資訊，如日期與時間，以及工作執行期間要使用的指定設定檔。

依預設，下列已排程的工作會顯示在「排程器」中：

- 防護記錄維護 (啟用排程器設定中的 **[顯示系統工作]** 選項後)
- 使用者登入後進行啟動檔案檢查
- 成功更新偵測模組後進行啟動檔案檢查
- 定期自動更新
- 使用者登入後自動更新

若要編輯 (預設及使用者定義的) 現有已排程工作的配置，請按下 CTRL，然後按一下想要修改的工作，並且選取 **[編輯]**，或選取工作，然後按一下 **[編輯工作]**。

12.2.1 建立新工作

若要在 [排程器] 中建立新工作，請按一下 **[新增工作 ..]**，或按下 Ctrl，並且按一下空白欄位，然後從內容功能表中選取 **[新增 ..]**。可用的已排程工作有五種類型：

- **執行應用程式**
- **更新**
- **防護記錄維護**
- **指定電腦掃描**
- **系統啟動檔案檢查**

附註：您可以點選 **[執行應用程式]** 以「nobody」的系統使用者身分執行程式。透過排程器執行應用程式的權限將由 macOS 定義。

由於更新是其中一個最常用的已排程工作，因此我們將在下方範例中使用排程器新增新的更新工作：

1. 從 **[已排程的工作]** 下拉式功能表中，選取 **[更新]**。
2. 將工作名稱輸入 **[工作名稱]** 欄位中。
3. 從 **[執行工作]** 下拉式功能表中選取工作頻率。系統會根據選取的頻率，提示您指定不同的更新參數。如果您選取 **[使用者定義]**，則系統會提示您以 cron 格式指定日期 時間 (如需更多詳細資料，請參閱建立使用者定義的工作 29 一節)。
4. 在下一步中，定義排程期間無法執行或完成工作時要採取的處理方法。
5. 在最後一步中，則會顯示含有目前已排程工作相關資訊的摘要視窗。按一下 **[完成]**。新已排程的工作將新增至目前已排程的工作清單。

依預設，ESET Cyber Security Pro 包含預先定義的已排程工作，以確保產品功能正常。依預設，不應改變與隱藏這些工作。若要顯示這些工作，從主要功能表中按一下 **[設定]** > **[進入應用程式喜好設定 ..]**(或按下 *cmd+,*) > **[排程器]**，然後再選取 **[顯示系統工作]**。

12.2.2 建立使用者定義的工作

[使用者定義] 工作的日期和時間必須以全年排程的 cron 格式 (包含 6 個以空格分隔的欄位所組成的字串) 輸入：

```
分鐘(0-59) 小時(0-23) 月中日(1-31) 月份(1-12) 年份(1970-2099) 週間日(0-7)(星期日 = 0 或 7)
```

範例：

```
30 6 22 3 2012 4
```

cron 運算式支援的特殊字元：

- 星號 (*) - 運算式會符合欄位的所有值 ;例如 :星號在第 3 個欄位 (月中日) 就表示每一天
- 連字號 (-) - 定義範圍 ;例如：`3-9`
- 逗點 (,) - 分隔清單中的項目 ;例如：`1,3,7,8`
- 斜線 (/) - 定義範圍的遞增量 ;例如 :`3-28/5` 在第 3 個欄位 (月中日) 就表示每月的第 3 天起每隔 5 天。

不支援日名稱 (Monday-Sunday) 及月份名稱 (January-December)。

附註：如果您同時定義月中日及週間日，則程式只會在同時符合這兩個欄位時才執行命令。

12.3 隔離區

隔離區的主要目的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 Cyber Security Pro 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 威脅實驗室進行分析。

您可以在表格中檢視隔離區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)。內含隔離檔案的隔離資料夾 (*/Library/Application Support/Eset/esets/cache/quarantine*) 即使解除安裝 ESET Cyber Security Pro 之後仍會保留在系統中。隔離的檔案以安全的加密形式儲存，而且在安裝 ESET Cyber Security Pro 後可以再次還原。

12.3.1 隔離檔案

ESET Cyber Security Pro 會自動隔離刪除的檔案 (如果您尚未在警告視窗中取消選取此選項)。您可以按一下 **[隔離 ..]** 手動隔離任何可疑的檔案 .亦可使用內容功能表達到此目的 :按住 Ctrl 並按一下空白欄位，選取 **[隔離]**，選取您想要隔離的檔案，然後按一下 **[開啟]** 按鈕。

12.3.2 從隔離區還原

隔離的檔案也可以還原到其原始的位置，若要這麼做，請選取隔離的檔案，然後按一下 **[還原]**。也可以從內容功能表還原，做法是按下 CTRL 並按一下 [隔離] 視窗中指定的檔案，然後按一下 **[還原]**。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。

12.3.3 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，或錯誤地將檔案評估為受感染 (例如以代碼的啟發式分析) 且因此隔離，請將檔案傳送至 ESET 威脅實驗室。若要從隔離提交檔案，請下 CTRL 並按一下該檔案，然後從內容功能表選取 **[提交檔案以供分析]**。

12.4 執行中的處理程序

[執行中的處理程序] 清單會顯示電腦正在執行的處理程序。ESET Cyber Security Pro 會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** - 目前您電腦上正在執行之處理程序的名稱。若要查看所有執行中的處理程序，您也可以使用 Activity Monitor (可在 */Applications/Utilities* 中找到)。
- **風險層級** - 在大多數的情況下，ESET Cyber Security Pro 和 ESET Live Grid 技術會使用一連串的啟發式規則檢查每個物件的特性，然後評量其進行惡意活動的潛在可能，再將風險層級指派給物件 (檔案、處理程序等)。系統會根據這些啟發式規則，將風險層級指派給物件。以綠色標記的已知應用程式是絕對安全的 (列入白名單) 且將會從掃描中排除。這會同時提升指定和即時掃描的速度。當應用程式標記為未知時 (黃色)，並不代表一定是惡意軟體。該程式通常只是較新的應用程式。若您對於檔案不確定，可以將檔案提交到 ESET 威脅實驗室進行分析。若該檔案的分析結果為惡意的應用程式，系統則會將其特徵碼新增至其中一個即將進行的更新中。
- **使用者數目** - 使用指定應用程式的使用者數目。此資訊係由 ESET Live Grid 技術所收集。
- **發現時間** - 從 ESET Live Grid 技術探索到應用程式至目前的一段時間。
- **應用程式套件 ID** - 廠商或應用程式處理程序的名稱。

按一下指定處理程序，視窗底端將出現下列資訊：

- **檔案** - 應用程式在您電腦上的所在位置
- **檔案大小** - 檔案在磁碟上的實體大小
- **檔案說明** - 根據作業系統說明的檔案特性
- **應用程式套件 ID** - 廠商或應用程式處理程序的名稱
- **檔案版本** - 來自應用程式發佈者的資訊
- **產品名稱** - 應用程式名稱和 戚商用名稱

12.5 Live Grid

Live Grid 預早警告系統可讓 ESET 立即且持續收到與新入侵情況有關的通知。雙向 Live Grid 預早警告系統就只有一個目的 -提升我們為您提供的防護效能。若要確保您能在威脅入侵的第一時間掌握其行蹤，您可以 「連結」到越多的客戶越好，使他們成為我們的 「威脅偵察者」。您有兩種選擇：

1. 您可以選擇不啟用 Live Grid 預早警告系統。這不會讓您失去軟體的任何功能，並且仍可受到我們所提供的最佳防護。
2. 您可以配置 Live Grid 預早警告系統提交與新威脅有關的匿名資訊以及放置新威脅程式碼的位置。此資訊會傳送至 ESET 進行詳細分析。ESET 可研究這些威脅來更新其威脅資料庫，並提升程式的威脅偵測功能。

Live Grid 預早警告系統將收集與新偵測到威脅有關的電腦資訊。這項資訊可能包含出現威脅的檔案範例或複本、該檔案的路徑、檔案名稱、日期和時間、威脅入侵電腦的處理程序，以及與電腦作業系統有關的資訊。

雖然這項資訊可能偶爾會將您自己或電腦的相關資訊 (目錄路徑中的使用者名稱等) 洩漏給 ESET 的威脅實驗室，但我們除了利用這些資訊來對新威脅立即做出回應以外，不會將其使用於任何其他目的。

若要從主要功能表存取 Live Grid 設定檔，請按一下 **[設定]** > **[進入應用程式喜好設定 ..]**(或按下 *cmd+,*) > **[Live Grid]**。選取 **[啟用 Live Grid 預早警告系統]** 以啟動 Live Grid，然後按一下 **[進階選項]** 旁的 **[設定 ..]**。

12.5.1 Live Grid 設定

依預設，系統會配置 ESET Cyber Security Pro 為將可疑檔案提交給 ESET 的威脅實驗室以供詳細分析。若您不想自動提交這些檔案，請取消選取 **[提交檔案]**。

如果您找到可疑檔案，您可以提交給我們的威脅實驗室以供分析。如要提供檔案，請從主要程式視窗按一下 **[工具]** > **[提交樣本以供分析]**。如果它是惡意的應用程式，則其偵測將新增至近期的更新中。

提交匿名統計 –ESET Live Grid 預早警告系統會收集您電腦上相關的最新偵測威脅匿名資訊。此資訊包括入侵名稱、偵測日期及時間、ESET 安全產品版本、作業系統版本，以及位置設定。在一般情況下，每天會將這些統計資料傳遞到 ESET 伺服器一或兩次。

以下是提交的統計套件範例：

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/rdgFR1463[1].zip
```

[排除過濾器] –此選項可讓您排除特定不提交的檔案類型。例如，此選項在排除可能包含機密資訊的檔案，如文件或試算表時可能會有所幫助。依預設，最常見的檔案類型 (如 doc、rtf 等) 均會排除在外。您可以新增檔案類型到排除檔案清單中。

連絡人電子郵件 (選用) –如果我們需要進一步的資料來進行分析，將會使用您的電子郵件地址與您連絡。請注意，除非我們需要更多資訊，否則您並不會收到來自 ESET 的回應。

13. 使用者介面

使用者介面配置選項可讓您依需求調整工作環境。您可按一下 **[設定]** > **[進入應用程式喜好設定 ..]**(或按下 *cmd+,*) > **[介面]** 從主要功能表存取這些選項。

- 若要在系統啟動時顯示 ESET Cyber Security Pro 開頭顯示畫面，請選取 **[啟動時顯示開頭顯示畫面]**。
- **[在 Dock 中提供應用程式]** 可讓您在 macOS Dock 中顯示 ESET Cyber Security Pro 圖示 ⓔ，並可透過按下 *cmd-tab* 在 ESET Cyber Security Pro 與其他執行中應用程式之間切換。這些變更會在您重新啟動 ESET Cyber Security Pro 之後生效 (通常是由電腦重新啟動所觸發)。
- **[使用標準功能表]** 選項允許您使用某些鍵盤快捷鍵 (請參閱鍵盤快捷鍵 10) 和查看 macOS 功能表列 (畫面頂端) 上的標準功能表項目 (使用者介面、設定和工具)。
- 若要啟用 ESET Cyber Security Pro 某些選項的工具提示，請選取 **[顯示工具提示]**。
- **[顯示隱藏的檔案]** 選項可讓您看到並選取 **[電腦掃描]** 的 **[掃描目標]** 設定中的隱藏檔案。
- 依預設，ESET Cyber Security Pro 圖示 ⓔ 顯示在功能表列額外項目中，出現在 macOS 功能表列 (畫面頂端) 的右方。若要停用此圖示，取消選取 **[顯示功能表列額外項目的圖示]**。此變更會在您重新啟動 ESET Cyber Security Pro 之後生效 (通常是由電腦重新啟動所觸發)。

13.1 警告及通知

[警告及通知] 區段可讓您配置 ESET Cyber Security Pro 處理威脅警告與系統通知的方式。

停用 **[顯示警告]** 會停用所有警告視窗，而且只建議在特定情況中這麼做。對於大部分使用者而言，建議保留此選項的預設值 (啟用)。本章中 32 有進階選項的說明。

選取 **[於桌面顯示通知]** 將造成警告視窗不需要使用者互動就可以在桌面上顯示 (依預設在您畫面的右上角)。您可以藉由調整 **[自動關閉通知於 X 秒後]** 的值來定義顯示通知的時間 (預設為 5 秒)。

自從 ESET Cyber Security Pro 6.2 版本後，您也可以阻止特定**防護狀態**顯示於程式的主畫面中 (**[防護狀態]**視窗)。若要瞭解更多相關資訊，請參閱防護狀態 32。

13.1.1 顯示警告

ESET Cyber Security Pro 會顯示警告對話方塊視窗來通知您有新的程式版本、作業系統更新、停用某些程式元件及刪除防護記錄等。您可以選取 **[不再顯示此對話方塊]** 來個別隱藏每個通知。

[對話方塊清單] (**[設定]** > **[進入應用程式喜好設定 ..]**> **[警告及通知]** > **[設定 ..]**) 會顯示 ESET Cyber Security Pro.觸發的所有警告對話方塊清單。若要啟用或隱藏每個通知，請選取 **[對話方塊名稱]** 左側的核取方塊。此外，您也可以定義 **[顯示條件]**，其中會顯示新程式版本和作業系統更新的相關通知。

13.1.2 防護狀態

您可以變更 ESET Cyber Security Pro 目前的防護狀態，透過在 **[設定]** > **[進入應用程式喜好設定 ..]** > **[警告及通知]** > **[在防護狀態畫面中顯示:設定]** 中啟用或停用狀態。各種程式功能的狀態將會在 ESET Cyber Security Pro 主畫面中顯示或隱藏 (**[防護狀態]**視窗)。

您可以隱藏下列程式功能的防護狀態：

- 防火牆
- 網路釣魚防護
- Web 存取防護
- 電子郵件用戶端防護
- 作業系統更新
- 授權到期
- 需要重新啟動電腦

13.2 權限

ESET Cyber Security Pro 設定對您公司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。因此，您可以定義哪一個使用者擁有編輯程式配置的權限。

若要指定有權限的使用者，請按一下 **[設定]** > **[進入應用程式喜好設定 ..]**(或按下 *cmd+,*) > **[權限]**。從左側的清單選取使用者或群組，然後按一下 **[新增]**。若要顯示所有系統使用者 群組，請選取 **[顯示所有使用者 群組]**。若要移除使用者，從右側的 **[所選的使用者]** 清單中選取使用者名稱，然後按一下 **[移除]**。

附註：如果您將 [所選的使用者] 清單保留空白，則系統會視所有使用者都具有權限。

13.3 內容功能表

您可按一下 **[設定]** > **[進入應用程式喜好設定 ..]**(或按下 *cmd+,*) > **[內容功能表]** 區段，選取 **[整合至內容功能表]** 選項，以啟用內容功能表整合。您需要登出或重新啟動電腦才能使變更生效。當您按下 Ctrl，並且按一下任何檔案，即可在 **Finder** 視窗中使用內容功能表選項。

14. 其他選項

14.1 匯入及匯出設定

若要匯入現有配置或匯出您的 ESET Cyber Security Pro 配置，按一下 **[設定]** > **[匯入或匯出設定]**。

如果您需要備份 ESET Cyber Security Pro 的目前配置以供日後使用，匯入和匯出很有幫助。[匯出設定] 對想要在多個系統上使用 ESET Cyber Security Pro 慣用設定的使用者也很方便。您可以輕鬆匯入配置檔案以傳輸所需的設定。

若要匯入配置，請選取 **[匯入設定]**，然後按一下 **[瀏覽]** 以瀏覽至您要匯入的配置檔案。若要匯出，請選取 **[匯出設定]** 並使用瀏覽器選取電腦上的位置以儲存配置檔案。

14.2 Proxy 伺服器設定

您可在 **[設定]** > **[進入應用程式喜好設定 ..]**(或按下 *cmd+,*) > **[Proxy 伺服器]** 下配置 Proxy 伺服器設定。在這個等級指定 Proxy 伺服器，會定義所有 ESET Cyber Security Pro 功能的全域 Proxy 伺服器設定。需連線到網際網路的所有模組，都會使用這裡定義的參數。ESET Cyber Security Pro 支援 Basic Access 及 NTLM (NT LAN Manager) 類型的驗證。

若要指定此層級的 Proxy 伺服器設定，請選取 **[使用 Proxy 伺服器]**，然後在 **[Proxy 伺服器]** 欄位輸入您 Proxy 伺服器的 IP 位址或 URL。在 [連接埠] 欄位中，指定 Proxy 伺服器接受連線的連接埠 (依預設為 3128)。您也可以按一下 **[偵測]** 讓程式填寫這兩個欄位。

如果與 Proxy 伺服器間的通訊需要驗證，請在個別欄位中輸入有效的 **[使用者名稱]** 和 **[密碼]**。

15. 字彙

15.1 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。

15.1.1 病毒

電腦病毒是會損毀電腦上現有檔案的入侵活動。病毒這個名稱取自生物學的病毒，因為病毒會利用類似的方式，從一部電腦散播至另一部電腦。

電腦病毒通常會攻擊執行檔、腳本及文件。為進行複製，病毒會將其「內容」附加在目標檔案結尾。簡而言之，電腦病毒的運作如下：執行受感染的檔案之後，病毒會自行活化 (在原始應用程式之前)，並執行其預先定義的工作。之後才會讓原始應用程式執行。除非使用者 (有意或無意) 執行或開啟惡意程式，否則病毒無法感染電腦。

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。相反地，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。

有一點要特別注意的是，病毒 (與特洛伊木馬程式或間諜程式相較) 慢慢地愈來愈少見，因為對惡意軟體的作者而言，病毒沒有什麼商業誘因。此外，「病毒」這個詞經常被誤用來泛指所有種類的入侵活動。這種情況已逐漸減少，而改用較精確的新詞彙「malware」(惡意軟體)。

如果您的電腦感染病毒，則必須將被感染的檔案還原為原來的狀態，通常是使用防毒程式來清除病毒。

15.1.2 蠕蟲

電腦蠕蟲是含有惡意程式碼的程式，該程式會攻擊主機電腦，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複製及傳輸；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，蠕蟲可能在發佈的數小時內，就散佈到全世界，有時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。

15.1.3 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入侵活動類別，該程式會嘗試以有用的程式呈現，矇騙使用者執行這些程式。如今特洛伊木馬程式已經不需要再偽裝自己。特洛伊木馬程式唯一的目的，就是用最容易的方法進行入侵，並達成其惡意的目標。「特洛伊木馬程式」已經變成非常普遍的詞彙，用以描述無法歸入特定類別的入侵。

由於這是非常廣泛的類別，所以通常會細分為許多子類別。

- Downloader - 會從網際網路下載其他入侵的一種惡意程式
- Dropper - 這種特洛伊木馬程式類型主要會將其他類型的惡意軟體放置在被入侵的電腦上
- Backdoor - 一種與遠端攻擊者通訊的應用程式，可讓攻擊者存取系統，進而控制系統
- 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
- 播號程式 - 播號程式是專門用來連線至高費率電話號碼的程式。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。

特洛伊木馬程式通常採用執行檔的形式。如果偵測到您的電腦上有某個檔案是特洛伊木馬程式，建議您將該程式刪除，因為其中極可能包含惡意程式碼。

15.1.4 Rootkit

Rootkits 是一種惡意程式，它會將系統的無限存取權限授與網際網路攻擊者，同時隱匿他們的行蹤。在存取系統 (通常會利用系統弱點) 之後，Rootkits 會使用作業系統中的各種功能來避免遭到防毒軟體的偵測：它們會隱匿程序及檔案。也因為如此，使用一般的測試技術幾乎無法偵測到 Rootkit 的存在。

15.1.5 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，只是使用者會受到廣告的騷擾。其危險性在於廣告程式可能也會執行追蹤功能 (間諜程式也會執行此功能)。

如果您決定使用免費軟體產品，請特別注意安裝程式。安裝程式很可能會在安裝額外廣告程式程式時通知您。您通常可以取消安裝廣告程式而只安裝程式。

不安裝廣告程式便無法安裝某些程式，或者會限制程式的功能。這通常表示廣告程式會以「合法」方式存取系統，因為使用者已同意。在此情況下，保證安全總比留下遺憾好。如果電腦上有偵測為是廣告程式的檔案，建議您刪除該檔案，因為其中很可能包含惡意程式碼。

15.1.6 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，其看似反間諜程式，但事實上，其本身就是間諜程式。

如果電腦上有偵測為是間諜程式的檔案，建議您刪除該檔案，因為其中很可能包含惡意程式碼。

15.1.7 潛在不安全的應用程式

有很多合法程式的功能都可用來簡化網路電腦的系統管理作業。然而，如果落入有心人士的手中，可能就會被用來從事惡意活動。ESET Cyber Security Pro 提供偵測這類威脅的選項。

潛在不安全的應用程式一般是商業軟體和合法軟體。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)。

15.1.8 潛在不需要應用程式

潛在不需要應用程式不一定是惡意的，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 (相較於安裝前的行為)。最顯著的變更如下：

- 開啟您從未看過的新視窗
- 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

15.2 遠端攻擊類型

攻擊者可利用許多特殊技巧來入侵遠端系統。這些攻擊可區分成數種類別。

15.2.1 DoS 攻擊

DoS (或「拒絕服務」) 會讓欲使用電腦或網路的使用者無法使用。受攻擊的使用者將無法相互進行通訊，且無法繼續正常運作。受到 DoS 攻擊的電腦通常必須重新啟動才能正常運作。

在大部分的情況下，受攻擊的目標通常是 Web 伺服器，目的是使得使用者在一段特定期間內無法使用這些伺服器。

15.2.2 DNS Poisoning

駭客會利用 DNS (網域名稱伺服器) Poisoning 來混淆任何電腦的 DNS 伺服器，使其相信駭客所偽造的資料是合法且真實的。系統會將偽造的資訊存入快取一段時間，讓攻擊者重新撰寫 IP 位址的 DNS 回覆。然後，嘗試存取網站的使用者將會下載病毒或蠕蟲，而非其原始內容。

15.2.3 連接埠掃描

連接埠掃描可用來判斷哪些電腦連接埠在網路主機上為開放狀態。連接埠掃描器則是一種可搜尋這類連接埠的軟體。

電腦連接埠是一種用來處理傳入及傳出資料的虛擬點；從安全性觀點來說此一連接埠非常重要。在大型網路中，連接埠掃描器所收集的資訊可用來識別潛在弱點。這類用途是合法的。

然而，駭客通常會利用連接埠掃描來破壞安全性。他們的第一步是將封包傳送到每個連接埠。然後根據回應類型來判斷使用中的連接埠。掃描動作本身並不會造成任何問題，不過這種活動會揭露潛在弱點，使攻擊者有機會控制遠端電腦。

因此我們建議網路管理員封鎖所有未使用的連接埠，並保護使用中的連接埠不會遭到未獲授權的存取。

15.2.4 TCP 去同步化

TCP 去同步化是在 TCP 攔截攻擊中使用的技術。在觸發該技術的程序中，傳入封包中的序號與預期的序號不相同。非預期序號的封包會被移除 (位於目前通訊視窗的封包則會儲存在緩衝儲存區中)。

在去同步化程序中，兩種通訊端點都會移除收到的封包，使遠端攻擊者得以入侵並提供具有正確序號的封包。攻擊者甚至可以控制或修改通訊內容。

TCP 攔截攻擊的目的在於中斷伺服器用戶端或點對點通訊。不過您可以使用各個 TCP 區段的驗證來避免許多的攻擊。我們也建議您在網路裝置上使用推薦的配置。

15.2.5 SMB Relay

SMBRelay 和 SMBRelay2 是可對遠端電腦進行攻擊的特殊程式。這些程式會利用 NetBIOS 分層下的「伺服器訊息塊」檔案共用通訊協定。共用 LAN 中任何資料夾或目錄的使用者通常會使用此檔案共用通訊協定。

本機網路通訊內通常會交換密碼雜湊。

SMBRelay 會接收 UDP 連接埠 139 和 445 上的連線、轉送用戶端和伺服器交換的封包，然後進行修改。在進行連線和驗證之後，用戶端會中斷連線。SMBRelay 會建立新的 IP 位址。SMBRelay 會轉送交涉和驗證以外的 SMB 通訊協定通訊。只要用戶端電腦連線時，遠端攻擊者就可使用 IP 位址。

SMBRelay2 會依照與 SMBRelay 相同的原則運作，但其使用的是 NetBIOS 名稱而非 IP 位址。這兩種方式都會執行「中間人」(man-in-the-middle) 攻擊。這些攻擊可讓遠端攻擊者在無人發現的情況下讀取、插入及修改兩個通訊端點之間交換的訊息。受到這類攻擊的電腦通常會停止回應或意外地重新啟動。

若要避免受到這類攻擊，我們建議您使用驗證密碼或金鑰。

15.2.6 ICMP 攻擊

ICMP (網際網路控制訊息通訊協定) 是一種常見且廣泛使用的網際網路通訊協定。連接網路的電腦通常會使用此通訊協定來傳送各種錯誤訊息。

遠端攻擊者也會嘗試利用 ICMP 通訊協定的這些弱點。ICMP 通訊協定是專供不需要驗證的單向通訊使用。它可讓遠端攻擊者觸發 DoS (拒絕服務) 攻擊，或者讓未獲授權的個別使用者存取傳入及傳出的封包。

典型的 ICMP 攻擊為封包洪流、ICMP_ECHO 洪流和 Smurf 攻擊。當電腦受到 ICMP 攻擊時，其速度會變得非常緩慢 (影響使用網際網路的所有應用程式) 且無法正常連接網際網路。

15.3 電子郵件

電子郵件 (或 Email) 是一種具備多項優勢的現代化通訊形式。其具有高彈性、速度快與直接傳輸等特性，在 90 年代初期的網際網路盛行期間扮演相當關鍵的角色。

不過很不幸地，電子郵件和網際網路也因為其高度匿名特性使得垃圾郵件等非法活動有了發展空間。垃圾郵件包括來路不明的廣告、惡作劇與惡意軟體 (Malware) 的擴散。由於寄送垃圾郵件的成本相當低廉，且垃圾郵件的作者可利用許多工具取得新的電子郵件地址，因而為您帶來許多不便與危險。此外，垃圾郵件的龐大數量及種類也很難加以控制。您使用電子郵件地址的時間越長，被納入垃圾郵件引擎資料庫的可能性也越高。與防護相關的秘訣：

- 請盡量不要在網際網路上公開您的電子郵件地址
- 您的電子郵件地址只能提供給您所信任的對象
- 請盡量不要使用一般的別名。使用的別名越複雜，被追蹤的可能性也就越低
- 請勿回覆已進入收件匣中的垃圾郵件
- 填寫網際網路表格時請小心，尤其是注意 *[是，我要接收資訊]* 等選項
- 使用 「專用」電子郵件地址，例如其中一個地址專供公司使用，另一個則用來與好友進行連絡。
- 每隔一段時間就變更您的電子郵件地址
- 使用 「垃圾郵件防護」解決方案

15.3.1 廣告

網際網路廣告是一種成長最為快速的廣告形式。其主要的市場優勢是最低廉的成本與高層級的直接傳遞性，不僅如此，這些郵件還可即時傳遞。許多公司都會使用電子郵件行銷工具以更有效率地與目前及潛在的客戶進行聯繫。

這類廣告是合法的，因為您可能會希望收到與某些產品有關的商業資訊。但也有許多公司會大量傳送來路不明的廣告訊息。在此情況下，這些超出規範的電子郵件廣告就變成了垃圾郵件。

大批來路不明的電子郵件已逐漸造成問題，且情況沒有任何減緩的跡象。來路不明的電子郵件作者會嘗試將垃圾郵件偽裝成合法郵件。

15.3.2 惡作劇

惡作劇是一種透過網際網路所廣為流傳的錯誤資訊。惡作劇通常會透過電子郵件或 ICQ 及 Skype 等通訊工具來傳送。訊息本身的內容通常只是笑話或小道消息。

「電腦病毒」惡作劇會嘗試在收件者之間製造恐慌、不確定及懷疑等情緒，使他們相信某種 「無法偵測的病毒」會刪除檔案、擷取密碼，或在他們的系統中執行一些有害的活動。

某些惡作劇訊息會要求收件者將郵件傳送給他們的連絡人，使惡作劇訊息能繼續流傳出去。某些手機惡作劇會尋求協助，從國外匯錢給您等等，通常我們很難判斷發送者的動機為何。

如果您收到的訊息要求您將其轉寄給所有您認識的人，就可以很確定這是一則惡作劇。目前您可以在網際網路上找到許多可檢查電子郵件是否合法的網站。如果您懷疑任何訊息可能是惡作劇，請務必在轉寄之前執行網際網路搜尋。

15.3.3 **網路釣魚**

網路釣魚一詞表示一種使用社會工程的犯罪活動 (操控使用者以取得機密資訊)。其目的在於取得如銀行帳戶號碼、PIN 碼等敏感資料。

它通常會傳送偽裝成受信任之人士或公司 (例如金融機構、保險公司) 的電子郵件來存取資訊。此電子郵件乍看之下非常真實，其中包含的圖片及內容可能源自其所偽裝的對象。各種偽裝的活動 (資料驗證、金融操作) 會要求您輸入一些個人資料，例如銀行帳戶號碼或使用者名稱及密碼等等。您提交的所有資料會輕易遭到竊取及盜用。

銀行、保險公司與其他合法公司絕不會透過來路不明的電子郵件來要求您提供使用者名稱和密碼。

15.3.4 **識別垃圾郵件詐騙**

通常您可以透過一些指標來協助您識別信箱中的垃圾郵件 (來路不明的電子郵件)。如果郵件至少符合下列幾項條件，就很有可能是垃圾郵件。

- 寄件者地址不屬於連絡人清單中的任何人
- 某個人可提供您大筆的金錢，但條件是您必須先提供一小筆金錢
- 各種偽裝的活動 (資料驗證、金融操作) 會要求您輸入一些個人資料，例如銀行帳戶號碼、使用者名稱及密碼等等。
- 郵件內容以外文撰寫
- 要求您購買您不感興趣的產品。但如果您想要購買，請務必確認郵件寄件者為可信賴的廠商 (洽詢原始產品製造商)
- 故意拼錯某些單字以嘗試躲過垃圾郵件過濾器的篩選。例如 *vaigra*，而非 *viagra* 等。