ESET Internet Security

使用者手冊

按一下此處顯示此文件的連線版本

Digital Security
Progress. Protected.

ESET Internet Security 由 ESET, spol. s r.o. 所開發

如需詳細資訊，請造訪 https://www.eset.com

技術支援https://support.eset.com

修訂。2024年m月12日

1 ESET Internet Security 1
1.1 新增功能 2
1.2 我所擁有的是哪款產品? 2
1.3 系統需求 3
1.3 Microsoft Windows 的過期版本 4
1.4 預防 5
1.5 說明頁面 6
2 安裝 6
2.1 Live Installer 7
2.2 離線安裝 8
2.2 訂閱升級 10
2.2 產品升級 10
2.2 訂閱降級 11
2.2 產品降級 12
2.3 安裝疑難排解員 13
2.4 安裝完成後先掃描 13
2.5 升級至最新版本 14
2.5 舊版產品自動升級 14
2.5 將安裝 ESET Internet Security 15
2.5 變更為不同的產品線 15
2.5 註冊 15
2.5 啟動進度 15
2.5 啟動成功 15
3 開始使用 16
3.1 系統匣圖示 16
3.2 鍵盤快捷鍵 16
3.3 設定檔 17
3.4 更新 18
3.5 配置網路防護 19
3.6 啟用 防盜 20
3.7 家長控制 20
4 產品啟動 21
4.1 在啟動期間輸入啟動金鑰 22
4.2 使用 ESET HOME 帳戶 22
4.3 啟動免費試用版 23
4.4 免費 ESET 啟動金鑰 23
4.5 啟動失敗 – 一般案例 24
4.6 訂閱狀態 24
4.6 由於訂閱過度使用而啟動失敗 25
5 使用 ESET Internet Security 26
5.1 概觀 27
5.2 電腦掃描 29
5.2 自訂掃描啟動器 31
5.2 掃描進度 32
5.2 電腦掃描防護記錄 34
5.3 更新 36
5.3 對話方塊視窗 – 需要重新啟動 38
5.3 如何建立更新工作 38
5.4 工具 39
5.4 防護記錄檔案 40

5.4 防護記錄過濾 42
5.4 執行程序 44
5.4 安全性報告 45
5.4 網路連線 46
5.4 網路活動 48
5.4 ESET SysInspector 49
5.4 排程器 49
5.4 已排程掃描選項 51
5.4 已排程的工作概要 52
5.4 工作細節 52
5.4 工作時間 52
5.4 工作時間 – 一次 53
5.4 工作時間 – 每天 53
5.4 工作時間 – 每週 53
5.4 工作時間 – 由事件觸發 53
5.4 略過的工作 53
5.4 工作詳細資料 – 更新 54
5.4 工作詳細資料 – 執行應用程式 54
5.4 系統清除程式 54
5.4 網路檢查 55
5.4 網路檢查中的網路裝置 57
5.4 通知 | 網路檢查 58
5.4 隔離區 58
5.4 選取樣本以供分析 61
5.4 選取樣本以供分析 – 可疑檔案 62
5.4 選取樣本以供分析 – 可疑網站 62
5.4 選取樣本以供分析 – 誤判檔案 62
5.4 選取樣本以供分析 – 誤判網站 62
5.4 選取樣本以供分析 – 其他 63
5.5 設定 63
5.5 電腦防護 64
5.5 偵測到入侵 65
5.5 網際網路防護 68
5.5 防網路釣魚防護 69
5.5 家長控制 70
5.5 網站例外 72
5.5 從使用者複製例外 74
5.5 從帳戶複製類別 74
5.5 網路防護 74
5.5 網路連線 75
5.5 網路連線詳細資料 75
5.5 網路存取疑難排解 76
5.5 暫時性 IP 位址黑名單 77
5.5 網路防護防護記錄 77
5.5 使用防火牆解決問題 78
5.5 記錄並從防護記錄建立規則或例外 79
5.5 從防護記錄建立規則 79
5.5 從個人防火牆通知建立例外 79
5.5 網路防護進階記錄 79
5.5 使用網路流量掃描器解決問題 80
5.5 已封鎖網路威脅 81

5.5 偵測到新網路 81
5.5 建立連線 – 偵測 82
5.5 應用程式變更 83
5.5 對內的受信任通訊 83
5.5 對外的受信任通訊 85
5.5 對內通訊 86
5.5 對外通訊 87
5.5 連線視圖設定 88
5.5 安全性工具 88
5.5 安全銀行與瀏覽 89
5.5 瀏覽器內通知 89
5.5 瀏覽器隱私權與安全性 90
5.5 防盜 91
5.5 登入您的 ESET HOME 帳戶 93
5.5 設定裝置名稱 94
5.5 防盜 已啟用/已停用 94
5.5 新增裝置失敗 94
5.5 匯入及匯出設定 94
5.6 說明及支援 95
5.6 關於 ESET Internet Security 96
5.6 ESET 最新消息 96
5.6 提交系統配置資料 97
5.6 技術支援 97
5.7 ESET HOME 帳戶 98
5.7 連線到 ESET HOME 99
5.7 登入 ESET HOME 100
5.7 登入失敗 – 常見錯誤 101
5.7 在 ESET HOME 中新增裝置 102
6 進階設定 102
6.1 偵側引擎 103
6.1 排除 103
6.1 效能排除 104
6.1 新增或編輯效能排除 105
6.1 路徑排除格式 106
6.1 偵測排除 107
6.1 新增或編輯偵測排除 109
6.1 建立偵測排除精靈 110
6.1 偵測引擎進階選項 110
6.1 網路流量掃描器 110
6.1 雲端型防護 111
6.1 適用於雲端型防護的排除過濾器 113
6.1 惡意軟體掃描 113
6.1 掃描設定檔 114
6.1 掃描目標 114
6.1 閒置狀態掃描 115
6.1 閒置狀態偵測 115
6.1 啟動掃描 115
6.1 啟動檔案自動檢查 116
6.1 可移除的媒體 116
6.1 文件防護 117
6.1 主機入侵預防系統 (HIPS) 118

6.1 HIPS 排除 120
6.1 HIPS 進階設定 120
6.1 一律允許載入驅動程式 120
6.1 HIPS 互動視窗 120
6.1 學習模式已結束 121
6.1 偵測到潛在的勒索軟體行為 122
6.1 HIPS 規則管理 122
6.1 HIPS 規則設定 123
6.1 新增 HIPS 的應用程式/登錄路徑 126
6.2 更新 126
6.2 更新還原 128
6.2 回復時間間隔 129
6.2 產品更新 130
6.2 連線選項 130
6.3 防護 130
6.3 即時檔案系統防護 134
6.3 程序排除 135
6.3 新增或編輯程序排除 136
6.3 何時修改即時防護配置 136
6.3 檢查即時防護 136
6.3 即時防護無法運作時怎麼辦 137
6.3 網路存取防護 137
6.3 網路連線設定檔 138
6.3 新增或編輯網路連線設定檔 139
6.3 啟動項 140
6.3 IP 集 141
6.3 編輯 IP 集 142
6.3 網路檢查 142
6.3 防火牆 143
6.3 學習模式設定 144
6.3 防火牆規則 145
6.3 新增或編輯防火牆規則 146
6.3 應用程式修改偵測 149
6.3 從偵測中排除的應用程式清單 149
6.3 網路攻擊防護 (IDS) 149
6.3 IDS 規則 150
6.3 蠻力攻擊防護 152
6.3 規則 153
6.3 進階選項 155
6.3 SSL/TLS 156
6.3 應用程式掃描規則 158
6.3 憑證規則 159
6.3 加密的網路流量 159
6.3 電子郵件用戶端防護 160
6.3 郵件傳輸防護 160
6.3 排除的應用程式 161
6.3 排除的 IP 162
6.3 信箱防護 163
6.3 整合 164
6.3 Microsoft Outlook 工具列 165
6.3 確認對話方塊 165

6.3 重新掃描郵件 165
6.3 回應 166
6.3 地址清單管理 167
6.3 位址清單 167
6.3 新增/編輯地址 168
6.3 地址處理結果 169
6.3 ThreatSense 169
6.3 Web 存取防護 172
6.3 排除的應用程式 174
6.3 排除的 IP 175
6.3 URL 清單管理 176
6.3 位址清單 177
6.3 建立新的位址清單 178
6.3 如何新增 URL 遮罩 179
6.3 HTTP 流量掃描 179
6.3 ThreatSense 179
6.3 家長控制 182
6.3 使用者帳戶 183
6.3 使用者帳戶設定 183
6.3 類別 185
6.3 瀏覽器防護 186
6.3 安全銀行與瀏覽 186
6.3 裝置控制 187
6.3 裝置控制規則編輯器 188
6.3 偵測到的裝置 188
6.3 新增裝置控制規則 189
6.3 裝置群組 191
6.3 網路攝影機防護 192
6.3 網路攝影機防護規則編輯器 192
6.3 ThreatSense 193
6.3 清除層級 195
6.3 從掃描中排除的檔案副檔名 196
6.3 其他 ThreatSense 參數 197
6.4 工具 197
6.4 Microsoft Windows® 更新 197
6.4 對話方塊視窗 – 系統更新 198
6.4 更新資訊 198
6.4 ESET CMD 198
6.4 防護記錄檔案 199
6.4 玩家模式 200
6.4 診斷 201
6.4 技術支援 202
6.5 連線 202
6.6 使用者介面 203
6.6 使用者介面元素 203
6.6 存取設定 204
6.6 進階設定的密碼 205
6.6 螢幕助讀程式支援 205
6.7 通知 206
6.7 對話方塊視窗 – 應用程式狀態 206
6.7 桌面通知 207

6.7 桌面通知清單 ... 208
6.7 互動警告 ... 209
6.7 確認訊息 ... 210
6.7 轉送 ... 212
6.8 隱私權設定 ... 214
6.8 還原為預設值 ... 214
6.8 還原目前區段中的所有設定 ... 214
6.8 儲存配置時發生錯誤 ... 215
6.9 指令列掃描器 ... 215
7 常見問題 ... 217
7.1 如何更新 ESET Internet Security ... 218
7.2 如何從我的 PC 移除病毒 ... 218
7.3 如何允許特定應用程式的通訊 ... 219
7.4 如何啟用帳戶的家長控制 ... 219
7.5 如何在排程器中建立新的工作 ... 220
7.6 如何安排每週電腦掃描 ... 221
7.7 如何解除鎖定進階設定 ... 221
7.8 如何從 ESET HOME 解決產品停用的問題 ... 222
7.8 產品已停用，裝置已中斷連線 ... 222
7.8 產品未啟動 ... 223
8.1 客戶經驗改進計畫 ... 223
8.2 使用者授權合約 ... 224
8.3 隱私權原則 ... 232

ESET Internet Security

ESET Internet Security 代表確實整合電腦安全性的新方法。最新版的 ESET LiveGrid® 掃描引擎結合了自訂防火牆與反垃圾郵件模組，利用速度及精確度確保電腦受到防護。 其成品就是能夠持續監控可能威脅您電腦的攻擊及惡意軟體的智慧型系統。

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

功能與優點

重新設計的使用者介面	這個版本的使用者介面已根據使用性測試的結果大幅重新設計並簡化。所有 GUI 文字內容和通知均已謹慎檢閱，使用者介面現在支援由右至左書寫的語言，例如希伯來文和阿拉伯文。線上說明現已整合至 ESET Internet Security 並提供動態更新支援內容。
深色模式	一個可幫助您快速將畫面切換到深色主題的擴充功能。您可以在使用者介面元素中選擇您偏好的色彩配置。
病毒及間諜程式防護	主動偵測及清除多種已知和未知的病毒、蠕蟲、特洛伊木馬程式及 Rootkit、進階啟發式甚至可標記前所未見的惡意軟體，讓您避免不明威脅的危害，並在威脅造成任何傷害之前使其失去效力、Web 存取防護和防網路釣魚防護會監視 Web 瀏覽器與遠端伺服器（包含 SSL) 之間的通訊。電子郵件用戶端防護可控制透過 POP3(S) 和 IMAP(S) 通訊協定收到的電子郵件通訊。
定期更新	定期更新偵測引擎（先前稱為「病毒資料庫」）與程式模組是確保電腦有最高度安全性的最佳方法。
ESET LiveGrid®（具有雲端功能聲譽）	您可以直接從 ESET Internet Security 檢查執行中處理程序與檔案的聲譽。
裝置控制	自動掃描所有 USB 隨身碟、記憶卡及 CD/DVD、根據媒體類型、製造商、大小與其他特性封鎖可移除的媒體。
HIPS 功能	您可以更詳細地自訂系統的行為，並為系統登錄、作用中的處理程序與程式指定規則，也可以微調您的安全性狀態。
玩家模式	讓所有快顯視窗、更新或其他佔用大量系統資源的活動延後顯示或進行，保留系統資源供遊戲和其他全螢幕活動使用。

ESET Internet Security 中的功能

安全銀行與瀏覽	「安全銀行與瀏覽」提供安全的瀏覽器供您在存取線上銀行交易或線上付款閘道時使用，以確保所有線上交易均在受信任且安全的環境下進行。
支援網路簽章	網路簽章可讓您快速識別並封鎖進入及離開使用者裝置的惡意流量，例如 Bot 和弱點封包。此功能可視為殭屍網路防護的增強功能。
智慧型防火牆	可防止未授權使用者存取您的電腦，並利用您的個人資料。
電子郵件用戶端反垃圾郵件	垃圾郵件佔所有電子郵件通訊的 50 %。電子郵件用戶端反垃圾郵件對此問題進行防護。

防盜	防盜 當電腦遺失或遭竊能夠擴大使用者層級的安全性。當您安裝 ESET Internet Security 和 防盜 時，Web 介面將列出您的裝置，Web 介面可讓您在裝置上管理 防盜 配置及管理 防盜 功能。
家長控制	阻擋各種網站類別，讓您的家人免受潛在冒犯性網站內容的危害。

訂閱需要處於作用中狀態，ESET Internet Security 的功能才能運作。我們建議您在 ESET Internet Security 訂閱到期前數週將您的訂閱續約。

新增功能

ESET Internet Security 17.1 的新增功能

- 對網路檢查的小改善
- 安全銀行與瀏覽的小改善
- 其他小錯誤修復和改善

若要停用 **[新增功能通知]**，請執行以下操作：
1. 開啟 [進階設定] > **[通知]** > **[桌面通知]**。
2. 按一下 **[桌面通知]** 旁邊的 **[編輯]**。
3. 取消選取 **[顯示新增功能通知]** 核取方塊，然後按一下 **[確定]**。
如需關於通知的詳細資訊，請參閱通知區段。

有關 ESET Internet Security 中變更的詳細清單，請參閱 ESET Internet Security 變更防護記錄。

我所擁有的是哪款產品？

ESET 提供了多種安全性層級的全新產品，從強大且快速的防毒解決方案，到僅需佔用最低系統使用量的全方位安全性解決方案：

- **ESET NOD32 Antivirus**
- **ESET Internet Security**
- **ESET Smart Security Premium**
- **ESET Security Ultimate**

為判斷您已安裝了哪款產品，請開啟主要程式視窗，您將會在視窗頂端處看到產品名稱（請參閱知識庫文章）。

下列表格詳細記載了各個特定產品中所提供的功能。

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
偵側引擎	✔	✔	✔	✔
進階機器學習	✔	✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
惡意探索封鎖程式	✔	✔	✔	✔
指令碼型攻擊防護	✔	✔	✔	✔
網路釣魚防護	✔	✔	✔	✔
Web 存取防護	✔	✔	✔	✔
HIPS (包含勒索軟體保護)	✔	✔	✔	✔
垃圾郵件防護		✔	✔	✔
防火牆		✔	✔	✔
網路檢查		✔	✔	✔
網路攝影機防護		✔	✔	✔
網路攻擊防護		✔	✔	✔
殭屍網路防護		✔	✔	✔
安全銀行與瀏覽		✔	✔	✔
瀏覽器隱私權與安全性		✔	✔	✔
家長控制		✔	✔	✔
防盜		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

上述部分產品可能無法提供給您的語言 / 區域。

系統需求

為使 ESET Internet Security 能以最佳化的狀態執行，您的系統應符合下列軟硬體需求：

支援的處理器

Intel 或 AMD 32 位元 (x86) 處理器（含 SSE2 指令集）或 64 位元 (x64) 處理器1 GHz 或更高速度
ARM64 型處理器1GHz 或更高

受支援的作業系統

Microsoft® Windows® 11

Microsoft® Windows® 10

必須在所有 Windows 作業系統上安裝 Azure Code Signing 支援，才能安裝或升級 2023 年 7 月之後發佈的 ESET 產品。更多資訊

一律嘗試將作業系統維持在最新狀態。

ESET Internet Security 功能需求

請參閱下表中特定 ESET Internet Security 功能的系統需求：

功能	需求
Intel® Threat Detection Technology	參閱支援的處理器
安全銀行與瀏覽	查看支援的 Web 瀏覽器
透明背景	Windows 10 版本 RS4 及更新版本。
專用清除程式	非 ARM64 型處理器。
系統清除程式	非 ARM64 型處理器。
惡意探索封鎖程式	非 ARM64 型處理器。
深層行為檢查	非 ARM64 型處理器。

其他

需要有內部連線才能啟動且 ESET Internet Security 更新才能正常運作。

在同一裝置上同時執行的兩個病毒防護程式會不可避免地導致系統資源衝突，例如減慢系統運行速度使其不可操作。

Microsoft Windows 的過期版本

問題

- 您希望在使用 Windows 7、Windows 8 (8.1) 或 Windows Home Server 2011 的電腦上安裝 ESET Internet Security 的最新版本
- ESET Internet Security 會在安裝期間顯示 **舊版作業系統** 的錯誤通知

[詳細資訊]

最新版本的 ESET Internet Security 需要 Windows 10 或 Windows 11 作業系統。

解決方案

以下為可用解決方案：

升級到 Windows 10 或 Windows 11

升級程序相當容易，在許多情況下，您都可以進行升級，而不會失去任何檔案。升級到 Windows 10 之前：

1. 備份重要資料
2. 閱讀 Microsoft 升級到 Windows 10 常見問題或升級到 Windows 11 常見問題 並更新您的 Windows 作業系統。

安裝 **ESET Internet Security 版本 16.0**

若無法升級 Windows，請安裝 ESET Internet Security 版本 16.0。如需詳細資訊，請參閱 ESET Internet Security 16.0 線上說明。

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遠端攻擊。為達到最大的保護性及方便性，正確地使用防毒解決方案並遵守數項有用的規則是很重要的：

定期更新

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

下載安全修補程式

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

備份重要資料

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

定期掃描電腦中的病毒

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

遵循基本安全規則

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

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

說明頁面

歡迎使用 ESET Internet Security 使用者手冊。這裡提供的資訊將向您介紹產品，並協助您讓電腦更加安全。

開始使用

使用 ESET Internet Security 前，您可以閱讀關於您使用電腦時可能遇到的各種偵測類型和遠端攻擊。我們針對在 ESET Internet Security 中所推出的新功能編譯了清單。

從安裝 ESET Internet Security 開始。如果已安裝 ESET Internet Security，請參閱使用 ESET Internet Security。

如何使用 ESET Internet Security 說明頁面

線上說明分散在數個章節和段落中。在 ESET Internet Security 中按 **F1** 可檢視有關目前已開啟視窗的資訊。

程式可讓您使用關鍵字搜尋說明主題，或者輸入單字或片語搜尋內容。這兩種方法之間的不同之處在於：關鍵字可能與文字中不包含該特定關鍵字的說明頁面邏輯相關。依單字或片語搜尋會搜尋所有頁面的內容，而且僅會顯示實際文字中包含所搜尋單字或片語的頁面。

為了維持一致性並避免造成混亂，本指南中所使用的術語都是根據 ESET Internet Security 使用者介面。我們也使用一組統一的符號，來強調特別關注或深具意義的主題。

「注意」只是簡短的觀察。雖然您可以忽略它，但「注意」可以提供重要資訊，例如特定的功能或是一些相關主題的連結。

這需要您的注意，我們建議您不要將其略過。通常，它會提供非重大但卻重要的資訊。

這是需要您特別注意與留心的資訊。放置警告是要特別防止您犯下可能造成損害的錯誤。閱讀並了解文字，因為它是有關高度敏感的系統設定或是其他風險。

這是使用案例或實際範例，旨在協助您瞭解如何使用特定功能或特性。

慣例	代表意義
粗體	介面項目的名稱，例如方塊和選項按鈕。
斜體	是您提供資訊的版面配置區。例如，檔案名稱或路徑代表您輸入實際路徑或檔案名稱。
`Courier New`	代碼範例或指令。
超連結	提供迅速輕鬆地存取交互參照主題或外部網路位置。超連結會以藍色字顯示，且會加底線。
%ProgramFiles%	Windows 系統目錄儲存了安裝於 Windows 中的程式。

線上說明是說明內容的主要來源。當您有可用的網際網路連線時，系統會自動顯示最新版的線上說明。

安裝

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

- Live installer － 從 ESET 網站上下載或 CD/DVD。此安裝套件普遍適用於所有語言（請選擇適當的語言）。Live Installer 是一個小型的檔案；安裝 ESET Internet Security 時所需要的其他檔案都會自動下載。

- 離線安裝 – 使用 .exe 檔案比 Live Installer 更大，且不需要網際網路連線或其他檔案即可完成安裝。

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

Live Installer

下載 Live installer 安裝套件後，按兩下安裝檔案，並遵循安裝程式精靈中的逐步指示。

此安裝類型需要連接至網際網路。

1. 從下拉式功能表中選取適當的語言，並按一下 **[繼續]**。

如果您正在安裝的新版會覆蓋受到密碼保護設定的舊版，請輸入您的密碼。您可以在存取設定中配置設定密碼。

2. 選取下列功能的喜好設定，閱讀使用者授權合約與隱私權政策，並按一下 **[繼續]**，或按一下 **[全部允許並繼續]** 以啟用所有功能：

- ESET LiveGrid® 意見系統
- 潛在不需要的應用程式
- 客戶經驗改進計畫

按一下 **[繼續]** 或 **[全部允許繼續]**，即表示您接受使用者授權合約，並瞭解隱私權政策。

3. 若要使用 ESET HOME 來啟動、管理及檢視裝置的安全性，請將您的裝置與 ESET HOME 帳戶連線。按

一下［**略過登入**］繼續進行，無須連線至 ESET HOME。您稍後可以將裝置與您的 ESET HOME 帳戶連線。

4. 如果要繼續進行但不連線 ESET HOME，請選擇啟動選項。如果您以覆蓋舊版的方式安裝較新版本，系統將會自動輸入您的**啟動金鑰**。

5. 安裝精靈可根據您的訂閱來決定要安裝哪個 ESET 產品。一律會預先選取安全功能最多的版本。如果您想要安裝其他版本的 ESET 產品，請按一下［**變更產品**］。按一下［**繼續**］以開始安裝程序。可能需要幾分鐘時間。

如果過去解除安裝的 ESET 產品有任何容錯移轉（檔案或資料夾），則會提示您允許刪除它們。按一下［**安裝**］以繼續。

6. 按一下［**完成**］以結束安裝精靈。

安裝疑難排解員

在產品安裝和啟動後，模組會開始下載。正在初始化防護，除非完成下載，否則某些功能可能無法完全運作。

離線安裝

使用以下離線安裝程式 (.exe) 下載並安裝 ESET Windows 家庭版產品。選擇要下載的 ESET 家用產品版本 (32 位元、64 位元或 ARM)

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
64 位元下載 32 位元下載 ARM 下載	64 位元下載 32 位元下載 ARM 下載	64 位元下載 32 位元下載 ARM 下載	64 位元下載 32 位元下載 ARM 下載

如果您具有作用中的網際網路連線，則使用 Live Installer 安裝 ESET 產品

當您啟動離線安裝程式 (.exe) 時，安裝精靈將引導您進行設定程序。

1. 從下拉式功能表中選取適當的語言，並按一下 **[繼續]**。

如果您正在安裝的新版會覆蓋受到密碼保護設定的舊版，請輸入您的密碼。您可以在存取設定中配置設定密碼。

2. 選取下列功能的喜好設定，閱讀使用者授權合約與隱私權政策，並按一下 **[繼續]**，或按一下 **[全部允許並繼續]** 以啟用所有功能：

- ESET LiveGrid® 意見系統
- 潛在不需要的應用程式
- 客戶經驗改進計畫

按一下 **[繼續]** 或 **[全部允許繼續]**，即表示您接受使用者授權合約，並瞭解隱私權政策。

3. 按一下 **[略過登入]**。當您具有網際網路連線時，可以將您的裝置連線至 ESET HOME 帳戶。

4. 按一下 **[略過啟動]**。在安裝後必須啟動 ESET Internet Security 才能完全運作。產品啟用需要作用中的網際網路連線。

5. 安裝精靈會根據已下載的離線安裝程式來顯示要安裝哪個 ESET 產品。按一下 **[繼續]** 以開始安裝程序。可能需要幾分鐘時間。

如果過去解除安裝的 ESET 產品有任何容錯移轉（檔案或資料夾），則會提示您允許刪除它們。按一下 **[安裝]** 以繼續。

6. 按一下 **[完成]** 以結束安裝精靈。

安裝疑難排解員

訂閱升級

當用於啟動 ESET 產品的訂閱遭到變更時，此通知視窗便會顯示。您已變更的訂閱可讓您啟動具有更多安全功能的產品。如果未執行任何變更，ESET Internet Security 會顯示警示視窗一次，視窗名稱為 **[變更至包含更多功能的產品]**。

是（建議） - 可自動安裝產品，而且具有更多安全功能。

不，謝謝 - 不會進行任何變更，而且通知將永久消失。

若要稍後再變更產品，請參閱我們的 ESET 知識庫文章。有關 ESET 訂閱的詳細資訊，請參閱訂閱常見問題。

下列表格詳細記載了各個特定產品中所提供的功能。

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
偵側引擎	✔	✔	✔	✔
進階機器學習	✔	✔	✔	✔
惡意探索封鎖程式	✔	✔	✔	✔
指令碼型攻擊防護	✔	✔	✔	✔
網路釣魚防護	✔	✔	✔	✔
Web 存取防護	✔	✔	✔	✔
HIPS (包含勒索軟體保護)	✔	✔	✔	✔
垃圾郵件防護		✔	✔	✔
防火牆		✔	✔	✔
網路檢查		✔	✔	✔
網路攝影機防護		✔	✔	✔
網路攻擊防護		✔	✔	✔
殭屍網路防護		✔	✔	✔
安全銀行與瀏覽		✔	✔	✔
瀏覽器隱私權與安全性		✔	✔	✔
家長控制		✔	✔	✔
防盜		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

產品升級

您已下載預設的安裝程式並決定變更要啟動的產品，或是您希望將已安裝的產品變更為具有更多安全功能的產品。

在安裝期間變更產品

下列表格詳細記載了各個特定產品中所提供的功能。

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
偵側引擎	✔	✔	✔	✔
進階機器學習	✔	✔	✔	✔
惡意探索封鎖程式	✔	✔	✔	✔
指令碼型攻擊防護	✔	✔	✔	✔
網路釣魚防護	✔	✔	✔	✔
Web 存取防護	✔	✔	✔	✔
HIPS (包含勒索軟體保護)	✔	✔	✔	✔
垃圾郵件防護		✔	✔	✔
防火牆		✔	✔	✔
網路檢查		✔	✔	✔
網路攝影機防護		✔	✔	✔
網路攻擊防護		✔	✔	✔
殭屍網路防護		✔	✔	✔
安全銀行與瀏覽		✔	✔	✔
瀏覽器隱私權與安全性		✔	✔	✔
家長控制		✔	✔	✔
防盜		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

訂閱降級

當用於啟動 ESET 產品的訂閱遭到變更時，此對話視窗便會顯示。您變更的訂閱僅能與具有較少安全功能的不同 ESET 產品搭配使用。該產品已遭到自動變更，以防止喪失防護。

有關 ESET 訂閱的詳細資訊，請參閱訂閱常見問題

下列表格詳細記載了各個特定產品中所提供的功能。

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
偵側引擎	✔	✔	✔	✔
進階機器學習	✔	✔	✔	✔
惡意探索封鎖程式	✔	✔	✔	✔
指令碼型攻擊防護	✔	✔	✔	✔
網路釣魚防護	✔	✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Web 存取防護	✔	✔	✔	✔
HIPS (包含勒索軟體保護)	✔	✔	✔	✔
垃圾郵件防護		✔	✔	✔
防火牆		✔	✔	✔
網路檢查		✔	✔	✔
網路攝影機防護		✔	✔	✔
網路攻擊防護		✔	✔	✔
殭屍網路防護		✔	✔	✔
安全銀行與瀏覽		✔	✔	✔
瀏覽器隱私權與安全性		✔	✔	✔
家長控制		✔	✔	✔
防盜		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

產品降級

您目前安裝的產品和您即將啟動的產品相比，有更多的安全性功能。 您將會遺失防盜防護及在 ESET HOME 入口網站上對相關儲存資料的存取權。

下列表格詳細記載了各個特定產品中所提供的功能。

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
偵側引擎	✔	✔	✔	✔
進階機器學習	✔	✔	✔	✔
惡意探索封鎖程式	✔	✔	✔	✔
指令碼型攻擊防護	✔	✔	✔	✔
網路釣魚防護	✔	✔	✔	✔
Web 存取防護	✔	✔	✔	✔
HIPS (包含勒索軟體保護)	✔	✔	✔	✔
垃圾郵件防護		✔	✔	✔
防火牆		✔	✔	✔
網路檢查		✔	✔	✔
網路攝影機防護		✔	✔	✔
網路攻擊防護		✔	✔	✔
殭屍網路防護		✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
安全銀行與瀏覽		✔	✔	✔
瀏覽器隱私權與安全性		✔	✔	✔
家長控制		✔	✔	✔
防盜		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

安裝疑難排解員

如果在安裝期間發生問題，安裝精靈將提供可解決此問題的疑難排解員（如果可能）。

按一下**［執行疑難排解員］**以啟動疑難排解員。疑難排解員完成時，請按照建議的解決方案進行。

如果問題持續存在，請參閱常見安裝錯誤和解決方案的清單。

安裝完成後先掃描

在安裝 ESET Internet Security 之後，電腦掃描將在第一次成功更新之後自動啟動，以檢查惡意程式碼。

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

升級至最新版本

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

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。
確定您已經啟用 **[進階設定]** > [更新] > **[設定檔]** > **[更新]** 中的 **[應用程式功能更新]**。

2. 手動升級，請按一下主要程式視窗之 **[更新]** 區段中的 **[檢查更新]**。

3. 透過下載並安裝較新版本覆蓋舊版的方式手動升級。

如需其他資訊及圖解指示，請參閱：

- 更新 ESET 產品 – 請檢查最新的產品模組
- 不同 ESET 產品更新及版本類型為何？

舊版產品自動升級

您的 ESET 產品版本已不再受支援，產品已升級到最新版本。

常見安裝問題

每個新版本的 ESET 產品都具有許多錯誤修復和改良功能。具有 ESET 產品有效訂閱的現有客戶可以免費升級到最新版本的同一產品。

若要完成安裝：

1. 按一下［**接受並繼續**］以接受使用者授權合約並同意隱私權政策。如果您不同意使用者授權合約，請按一下［**解除安裝**］。無法恢復為先前的版本。

2. 按一下［**全部允許並繼續**］以允許 ESET LiveGrid® 意見系統和客戶經驗改進計畫，或者如果您不想參加，請按一下［**繼續**］。

3. 使用啟動金鑰啟動新的 ESET 產品後，將顯示概觀頁面。如果未找到您的訂閱資訊，請繼續免費試用版。如果先前產品使用的訂閱無效，請啟動您的 ESET 產品。

4. 需要重新啟動裝置才能完成安裝。

將安裝 ESET Internet Security

會顯示此對話方塊視窗：

- 安裝過程中 – 按一下［**繼續**］以安裝 ESET Internet Security。
- 在 ESET Internet Security 變更訂閱時—按一下［**啟動**］以變更訂閱並啟動 ESET Internet Security。

［**變更產品**］選項可讓您根據您的 ESET 訂閱在 ESET Windows 家用產品之間切換。如需詳細資訊，請參閱我所擁有的是哪款產品？

變更為不同的產品線

您可以根據您的 ESET 訂閱，在各種 ESET Windows 家用產品之間切換。如需詳細資訊，請參閱我所擁有的是哪款產品？

註冊

請填妥註冊表格中包含的欄位，並按一下［**啟動**］來註冊您的訂閱。用括號標示必要的是必填欄位。您提供的資訊僅用於與您 ESET 訂閱相關的事宜。

啟動進度

等候數秒讓啟動程序完成（所需時間會視網際網路連線速度或電腦而不同）。

啟動成功

啟動程序完成。 遵循安裝後精靈以完成式設定 ESET Internet Security。

模組更新將在數秒後開始。ESET Internet Security 的定期更新將立即開始。

初始掃描將在模組更新後的 20 分鐘內自動開始。

如果產品未與 ESET HOME 建立關聯，則啟動程序可能會中斷。登入您的 ESET HOME 帳戶或建立一個帳戶。

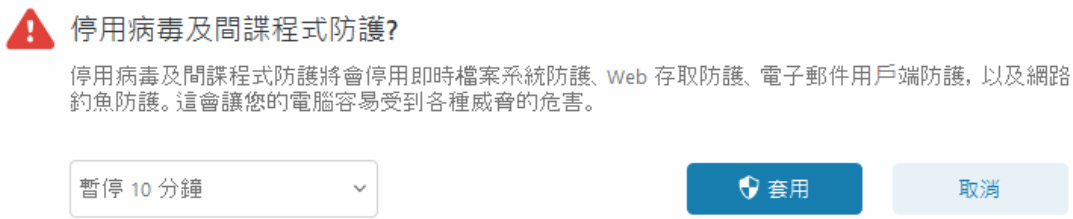
初學者手冊

本章提供 ESET Internet Security 及其基本設定的初始概觀。

系統匣圖示

以滑鼠右鍵按一下系統匣圖示，可以使用某些最重要的設定選項及功能。

暫停防護 – 顯示停用偵測引擎的確認對話方塊，此功能藉由控制檔案、Web 和電子郵件通訊來防禦惡意系統攻擊。**[時間間隔]** 下拉式功能表允許您指定停用防護的時間。



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

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

[進階設定] – 開啟 ESET Internet Security 進階設定。若要從主要產品視窗開啟 [進階設定]，按鍵盤上的 F5 或按一下 **[設定] > [進階設定]**。

防護記錄檔案 – 防護記錄檔案包含已發生的重要程式事件相關資訊，並提供偵測概觀。

[開啟 ESET Internet Security] – 開啟 ESET Internet Security 主要程式視窗。

[重設視窗配置] – 將 ESET Internet Security 的視窗重設為螢幕上的預設大小及位置。

[色彩模式]—開啟使用者介面設定，您可以在其中變更 GUI 色彩。

[檢查更新] – 啟動模組或產品更新以確保受到保護。ESET Internet Security 每天多次自動檢查更新。

關於 – 提供系統資訊、ESET Internet Security 已安裝版本的詳情、已安裝的程式模組，以及作業系統與系統資源的相關資訊。

鍵盤快捷鍵

為了更方便在 ESET Internet Security 中瀏覽，可以使用下列鍵盤快捷鍵：

鍵盤快捷鍵	處理方法
F1	開啟 [說明] 頁面

鍵盤快捷鍵	處理方法
F5	開啟進階設定
向上箭頭/向下箭頭	在下拉式功能表項目中瀏覽
TAB	移至視窗中的下一個 GUI 元素
Shift+TAB	移至視窗中的上一個 GUI 元素
ESC	關閉作用中的對話方塊視窗
Ctrl+U	顯示 ESET 訂閱和您電腦的相關資訊（技術支援詳細資料）
Ctrl+R	將產品視窗重設為預設大小及畫面上的預設位置
ALT + 左箭頭	向後瀏覽
ALT + 右箭頭	向前瀏覽
ALT+Home	瀏覽首頁

您還可以使用滑鼠按鍵後退或前進以進行瀏覽。

設定檔

設定檔管理程式用於 ESET Internet Security 內的兩個區段 – 在 **[指定掃描]** 區段和 **[更新]** 區段中。

電腦掃描

ESET Internet Security 中有 4 個預先定義的掃描設定檔：

- **[智慧型掃描]** – 這是預設的進階掃描設定檔。智慧型掃描設定檔會使用智慧型最佳化技術，此技術可排除先前掃描中發現要清除，並自從該掃描後未進行修改的檔案。這樣可在盡可能不影響系統安全性的情況下，降低掃描時間。

- **[內容功能表掃描]** – 您可以從內容功能表中，啟動任何檔案的指定掃描。內容功能表掃描設定檔可讓您定義掃描配置檔，在您透過此方法觸發掃描時使用。

- **深入掃描** – 深入掃描設定檔預設不會使用智慧型最佳化，因此不會使用此設定檔從掃描中排除任何檔案。

- **[電腦掃描]** – 這是標準電腦掃描中所使用的預設設定檔。

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] > **[偵測引擎]** > **[惡意軟體掃描]** > **[指定掃描]** > **[設定檔清單]** > **[編輯]**。**[設定檔管理員]** 視窗包括 **[已選取的設定檔]** 下拉式功能表，其中列出現有的掃描設定檔與可建立新設定檔的選項。為協助您建立掃描設定檔以符合您的需求，請參閱 ThreatSense 以取得每個掃描設定參數的說明。

> 假設您要建立您自己的掃描設定檔且有部分適用 **[掃描您的電腦]** 配置，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 **[一律修復偵測]**。請在 **[設定檔管理程式]** 視窗中輸入新設定檔的名稱並按一下 **[新增]**。從 **[已選取的設定檔]** 下拉式功能表中選取新設定檔，並調整剩餘的參數以符合您的需求，接著按一下 **[確定]** 以儲存新的設定檔。

更新

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

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

［**更新設定檔**］ - 目前使用的更新設定檔。若要變更，請從下拉式功能表選擇設定檔。

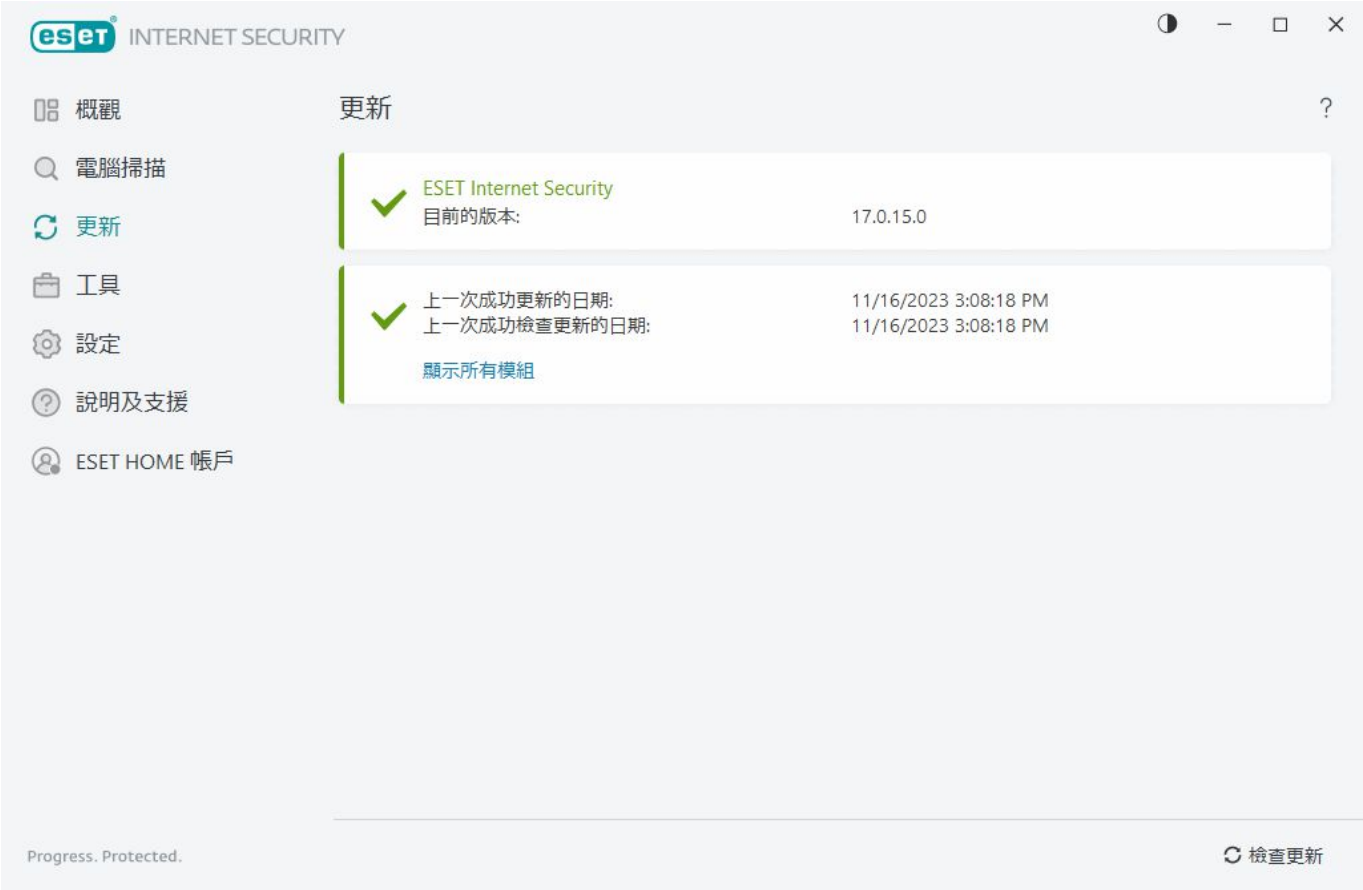
設定檔清單 - 建立新的設定檔或移除現有的更新設定檔。

更新

定期更新 ESET Internet Security 是讓電腦確保有最高安全性等級的最佳方法。更新模組確保程式模組和系統元件永遠為最新狀態。

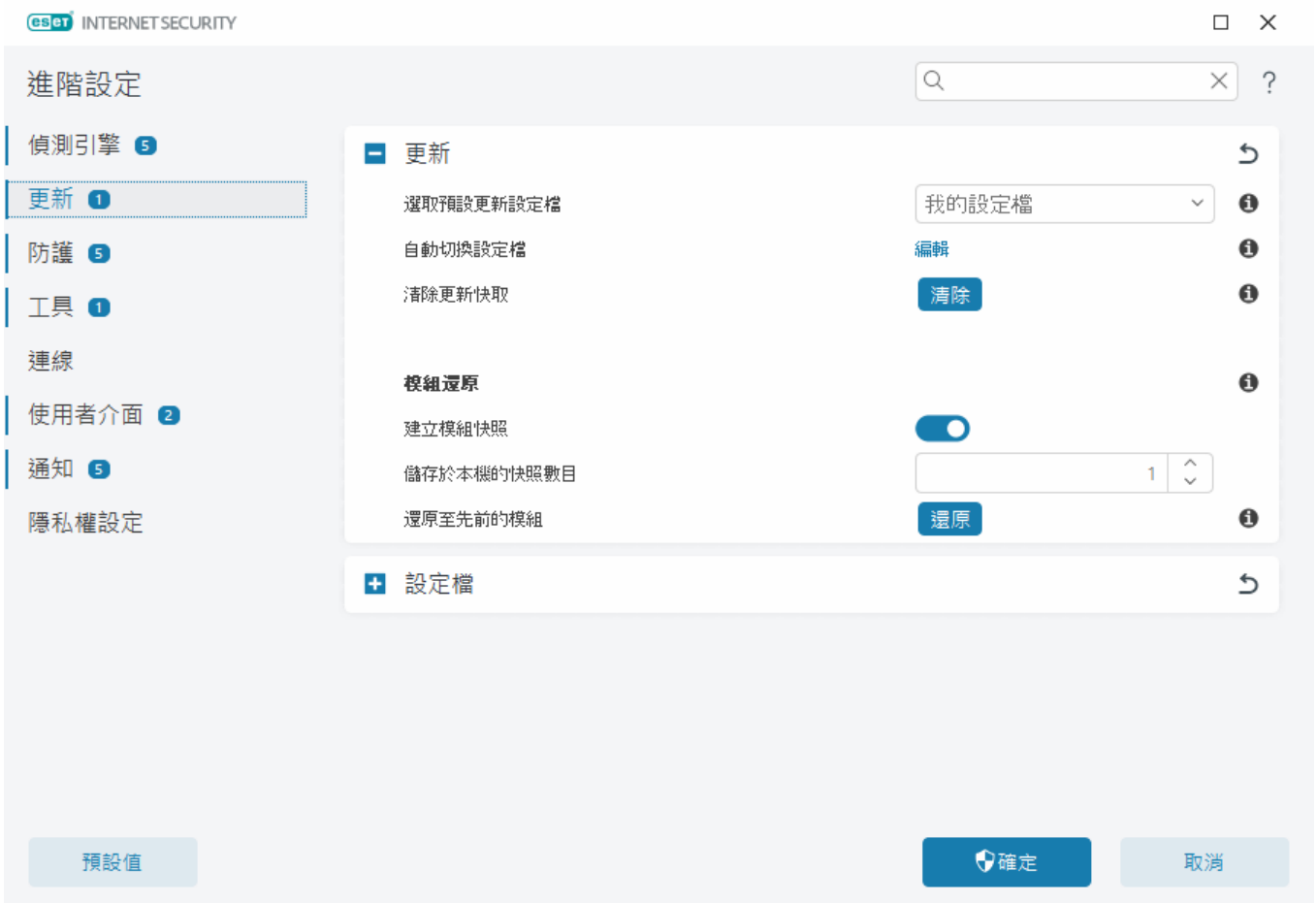
在主要程式視窗中按一下［**更新**］可以檢視目前更新狀態，包括最後的成功更新日期與時間，並在需要時更新。

除了自動更新，您還可以按一下［**檢查更新**］以觸發手動更新。



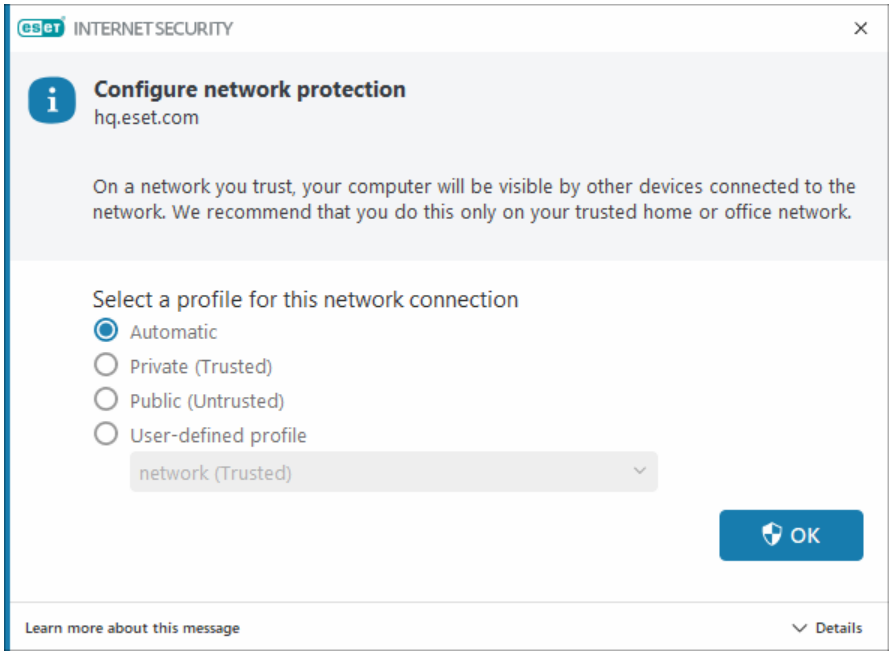
［進階設定］>［**更新**］包含其他更新選項，例如更新模式Proxy 伺服器存取和 LAN 連線。

如果更新遭遇問題，請按一下［**清除**］以清除更新快取。如果您仍無法更新程式模組，請參閱「模組更新失敗」訊息的疑難排解一節。



配置網路防護

在預設情況下，在偵測到新網路連線時ESET Internet Security 會使用 Windows 設定。若要在偵測到新網路時顯示對話方塊視窗，請將網路防護設定指派變更為 **[詢問]**。每當您的電腦連線到新網路時都會顯示網路防護配置。



您可以從以下網路連線設定檔中進行選擇：

自動 - ESET Internet Security 將根據為每個設定檔配置的啟動項自動選取設定檔。

私人 – 適用於信任的網路（家用或辦公室網路）。您的電腦和儲存在您電腦上的共用檔案可供其他網路使用者查看，且網路上其他使用者可以存取系統資源（啟用了對共用檔案和印表機的存取，啟用了對內 RPC 通訊，並且遠端桌面共用可用）。建議您在存取安全的區域網路時使用此設定。如果設定檔在 Windows 中配置為網域或私人網路，則會自動將其指派給網路連線。

公用 – 適用於不信任的網路（公用網路）。您系統上的檔案和資料夾未與網路上其他使用者共用或設為可見，系統資源分享將停用。建議您在存取無線網路時使用此設定。此設定檔將自動指派給 Windows 中未配置為網域或私人網路的任何網路連線。

使用者定義的設定檔 – 您可以從下拉式功能表中選取您建立的設定檔。僅當您建立了至少一個自訂設定檔時，此選項才可用。

不正確的網路配置可能會對電腦造成安全風險。

啟用 防盜

每日從家裏到工作或其他公共場所的過程中，個人裝置一直都存在著遺失或遭竊的風險。防盜 這項功能可在裝置遺失或遭竊時擴展使用者層級安全性。防盜 可讓您監控裝置的使用情況，並在 ESET HOME 中使用依 IP 位址定位的功能追蹤遺失的裝置，協助您取回裝置及保護個人資料。

透過地理 IP 位址查閱、網路攝影機影像擷取、使用者帳戶防護，以及裝置監控等現代科技，防盜 能協助您和執法機構找到遺失或遭竊的電腦或裝置。在 ESET HOME 中，您可以看見電腦或裝置上發生哪些活動。

若要深入瞭解 ESET HOME 中的 防盜，請參閱 ESET HOME 線上說明

由於使用者帳戶管理中的限制，防盜 可能無法在網域中的電腦上正常運作。

若要在裝置遺失或遭竊時啟用 防盜 並保護您的裝置，請選擇以下選項之一：

- 在主程序視窗 > **[概觀]** 中，按一下 **防盜** 旁邊的 **[設定]**
- 如果您在主程式視窗 > **[概觀]** 畫面中看到Anti-Theft 已可使用」訊息，請按一下 **[啟用 防盜]**
- 在主要程式視窗中，按一下 **[設定]** > **[安全性工具]**。啟用切換開關 **防盜** 並遵循螢幕上的說明進行操作。

如果裝置未連線到 ESET HOME，您必須：
1. 啟用 防盜 時登入您的 ESET HOME 帳戶
2. 設定裝置名稱

防盜 不支援 Microsoft Windows Home Server

啟用 防盜 後，您可以在 [主程式視窗] > **[設定]** > **[安全性工具]** > **[防盜]** 中，最佳化裝置的安全性

家長控制

如果您已經在 ESET Internet Security 中啟用家長控制，您也必須配置所有相關使用者帳戶的家長控制。

當家長控制處於作用中且未配置使用者帳戶時ESET Internet Security 在 **[概觀]** 畫面上會顯示「未設定家

長控制」通知。按一下 **[設定規則]** 並參閱家長控制一節以取得詳細資訊。

產品啟動

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

- 如果您購買零售版本的產品，或收到一封包含訂閱詳細資料的電子郵件，請按一下 **[使用購買的啟動金鑰]** 來啟動您的產品。您必須輸入提供的啟動金鑰，才能成功啟動產品。啟動金鑰是格式為 XXXX-XXXX-XXXX-XXXX-XXXX 或 XXXX-XXXXXXXX 的唯一字串，可供您識別訂閱擁有者和進行啟動。啟動金鑰通常位於產品包裝內部或背面。

- 選取使用 ESET HOME 帳戶後，系統會要求您登入 ESET HOME 帳戶。

- 如果您在購買之前想要評估 ESET Internet Security，請選取 [免費試用版]。請輸入您的電子郵件地址和國家，以在有限的時間內啟動 ESET Internet Security。您的免費試用版將透過電子郵件寄給您。每位客戶只能啟動免費試用版一次。

- 如果您沒有訂閱但想要購買訂閱，請按一下 **[購買訂閱]**。此選項會將您重新引導至當地的 ESET 經銷商網站。ESET Windows 家庭版產品訂閱不是免費的。

您可以隨時變更您的產品訂閱。若要這麼做，請在主要程式視窗中按一下 **[說明及支援]** > **[變更訂閱]**。您將會看到用於識別您 ESET 支援訂閱的公用授權 ID。

產品啟用失敗？

在啟動期間輸入啟動金鑰

自動更新對您的安全性而言相當重要，只有在啟動後 ESET Internet Security 才能收到更新。

當您輸入**啟動金鑰**時，請務必照實輸入。您的啟動金鑰是採用格式XXXX-XXXX-XXXX-XXXX-XXXX的唯一字串，可供您用來識別訂閱擁有者和訂閱的啟動。

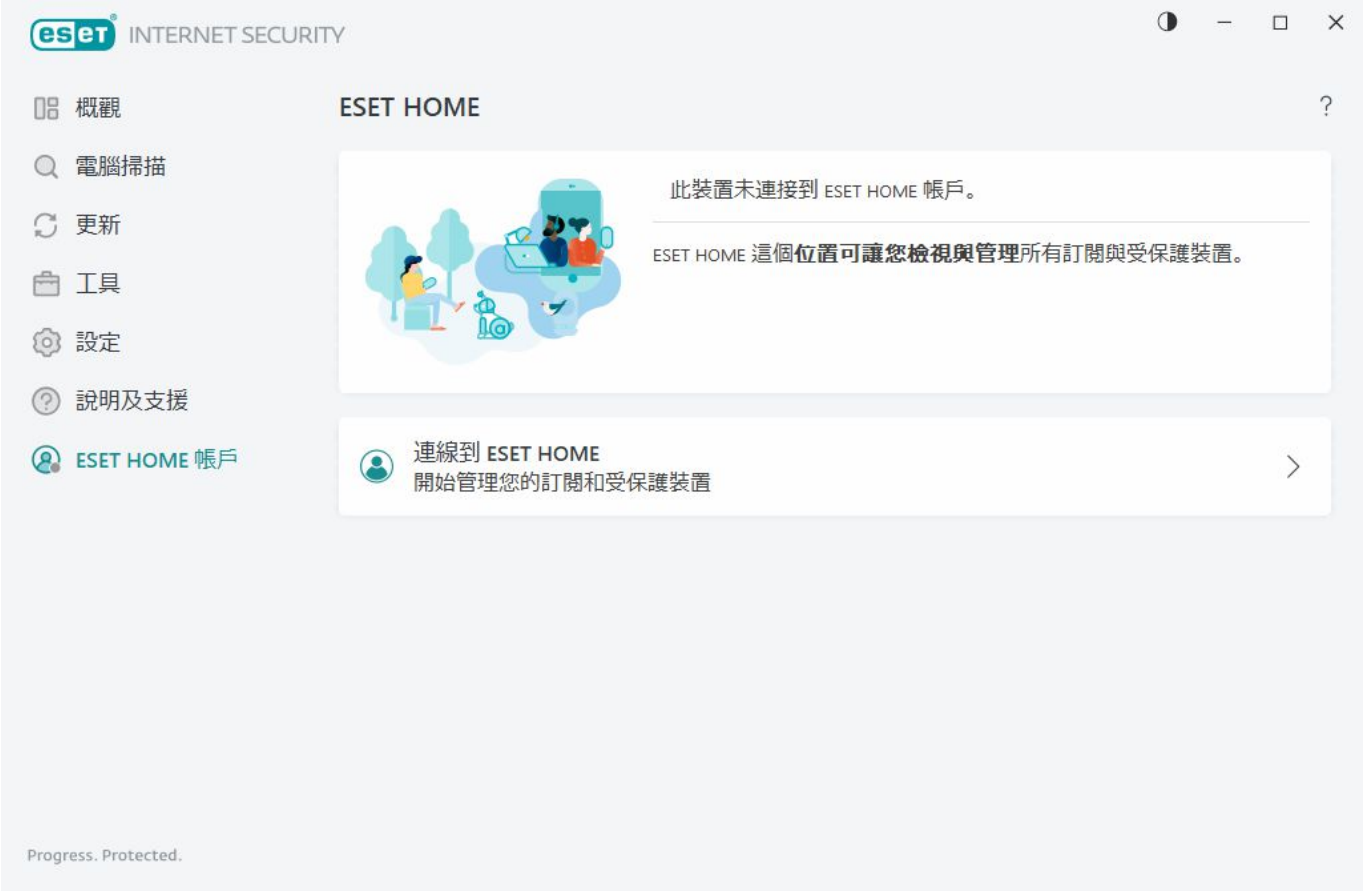
我們建議您從您的註冊電子郵件中複製並貼上啟動金鑰以確保正確無誤。

如果在安裝完成後仍未輸入您的啟動金鑰，您的產品將不會啟動。您可以在［主程式視窗］>［**說明及支援**］>［**啟動訂閱**］中啟動 ESET Internet Security。

ESET Windows 家庭版產品訂閱不是免費的。

使用 ESET HOME 帳戶

將您的裝置連線到 ESET HOME 以檢視和管理您所有啟動的 ESET 訂閱和裝置。您可以續約、升級或延長訂閱，並檢視重要的訂閱詳細資訊。在 ESET HOME 管理入口網站或行動應用程式中，您可以新增不同訂閱、下載產品至您的裝置、檢查產品安全性狀態，或透過電子郵件共用訂閱。如需詳細資訊，請造訪 ESET HOME 線上說明。



在選取［**使用 ESET HOME 帳戶**］做為啟動方法，或在安裝期間連線至 ESET HOME 帳戶時：

1. 登入您的 ESET HOME 帳戶。

如果您沒有 ESET HOME 帳戶，請按一下 **［建立帳戶］** 以註冊或查看 ESET HOME 線上說明中的指示。
若您忘記密碼，按一下 **［我忘記密碼］**，並遵循畫面上的步驟或查看 ESET HOME 線上說明中的指示。

2. 為您要在所有 ESET HOME 服務中使用的裝置設定 **［裝置名稱］**，然後按一下 **［繼續］**。

3. 選擇一個訂閱進行啟動，或新增新訂閱。按一下 **［繼續］** 以啟動 ESET Internet Security。

啟動免費試用版

若要啟動您的 ESET Internet Security 試用版本，請在 **［電子郵件地址］** 和 **［確認電子郵件地址］** 欄位中輸入有效的電子郵件地址。啟動之後，將會產生 ESET 訂閱並傳送至您的電子郵件。產品到期通知及與 ESET 的其他通訊也會使用此電子郵件地址。免費試用版只能啟動一次。

從 **［國家］** 下拉式功能表中，選取您的國家/地區，以便向將提供技術支援的本地經銷商登錄 ESET Internet Security。

免費 ESET 啟動金鑰

ESET Internet Security 訂閱不是免費的。

ESET 啟動金鑰是 ESET 所提供的唯一序列（由破折號分隔的字母及數字），以便允許合法使用 ESET Internet Security 而得以遵循使用者授權合約。依據 ESET 授予的授權數量，每個使用者都只能在其有權使用 ESET Internet Security 的範圍內使用啟動金鑰。啟動金鑰視為機密，無法共用，但您可以使用 ESET HOME 共用訂閱。

網際網路上可能有些來源可為您提供「免費」的 ESET 啟動金鑰，但請記住：

- 按一下［免費 ESET 訂閱］廣告可能會破壞您的電腦或裝置，而且可能遭到惡意軟體感染。惡意軟體可以隱藏於非官方 Web 內容（例如影片）、顯示廣告以根據您造訪次數而賺取金錢的網站等。通常，這些都是陷阱。
- ESET 能夠及確實會停用盜版訂閱。
- 擁有盜版啟動金鑰並不符合您安裝 ESET Internet Security 時必須接受的使用者授權合約之規定。
- 僅透過官方管道（例如 www.eset.com、ESET 經銷商或轉銷商）購買 ESET 訂閱；切勿從如 eBay 等非官方第三方網站購買，或向第三方購買共用訂閱。
- 下載 ESET Internet Security 是免費的，但在安裝期間啟動需要使用有效的 ESET 啟動金鑰（您可以下載和安裝啟動金鑰，但若未啟動，則無法運作）。
- 請勿在網際網路或社交媒體上共用您的訂閱（可能會被廣為傳播）。

若要識別及報告盜版 ESET 訂閱，請造訪知識庫文章以取得指示。

如果您不確定如何購買 ESET 安全性產品，您可以在決定下列事項時使用試用版本：

1. 使用免費試用版啟動 ESET Internet Security

2. 參與 ESET Beta 方案

3. 如果您使用 Android 行動裝置安裝 ESET Mobile Security，則可免費增值。

若要取得折扣/延長您的授權，請 [續約 ESET]

啟動失敗 – 一般案例

如果啟動 ESET Internet Security 不成功，最常見的情況為：

- 啟動金鑰已在使用中
- 您已輸入無效的啟動金鑰。
- 啟動表單中的資訊遺失或無效。
- 與啟動伺服器的通訊失敗。
- 沒有或已停用與 ESET 啟動伺服器的連線

確認您輸入的啟動金鑰是否正確，以及您的網際網路連線是否作用中。再次嘗試啟動 ESET Internet Security 如果您將 ESET HOME 帳戶用於啟動，請參閱 ESET HOME 訂閱與訂閱管理 – 線上說明

如果收到特定錯誤（例如，「訂閱已暫停使用」或「過度使用訂閱」），請按照訂閱狀態中的說明進行操作。

如果您仍然無法啟動 ESET Internet Security ESET 啟動疑難排解員會引導您解決常見問題、錯誤，以及與啟動和授權相關的問題（提供英語及其他數種語言）。

訂閱狀態

您的訂閱可以有不同的狀態。您可以在 ESET HOME 中找到您的訂閱狀態。若要將訂閱新增至 ESET HOME 帳戶，請參閱新增訂閱

如果您沒有 ESET HOME 帳戶，您可以建立新的 ESET HOME 帳戶

如果訂閱狀態未處於 **[作用中]**，您將在啟動期間收到錯誤訊息或在主要程式視窗中收到通知。

若要停用訂閱狀態通知，請開啟 [進階設定] > **[通知]** > **[應用程式狀態]**。按一下 **[應用程式狀態]** 旁的 **[編輯]**，展開 **授權**，然後取消選取欲停用之通知旁的核取方塊。停用通知不能解決此問題。

請參閱下表中適用於不同訂閱狀態的說明和建議的解決方案：

訂閱狀態	說明	解決方案
啟動	訂閱有效，無需您進行互動ESET Internet Security 可以啟動，您可以在主要程式視窗 > **[說明及支援]** 中找到訂閱詳情。	
過度使用	使用此訂閱的裝置數量超過其所允許的數量。您將收到啟動錯誤。	請參閱由於訂閱過度使用而啟動失敗取得更多資訊。

訂閱狀態	說明	解決方案
暫停使用	由於付款問題，您的訂閱已暫停使用。若要使用訂閱，請確定您在 ESET HOME 中的付款詳細資訊是最新的，或連絡您的訂閱轉銷商。您可以在啟動期間或在主要程式視窗中收到此錯誤。	已安裝的產品—如果您有 ESET HOME 帳戶，在主要程式視窗中顯示的通知中，按一下**［在 ESET HOME 中管理訂閱］**並檢閱您的付款詳細資訊。否則，請連絡您的訂閱轉銷商。 啟動錯誤—如果您有 ESET HOME 帳戶，在啟動錯誤視窗中，按一下**［開啟 ESET HOME］**並檢閱您的付款詳細資訊。否則，請連絡您的訂閱轉銷商。
已到期	您的訂閱已到期，並且不可使用此訂閱啟動 ESET Internet Security。您可以在啟動期間或在主要程式視窗中收到此錯誤。如果您已安裝 ESET Internet Security，您的電腦未受保護且為更新。	已安裝的產品—在主要程式視窗中顯示的通知中，按一下**［續約訂閱］**並遵循如何續約我的訂閱？中的指示，或按一下**［啟動產品］**並選擇您的啟動方法。 啟動錯誤—在啟動錯誤視窗中，按一下**［續約訂閱］**並遵循如何續約我的訂閱？中的指示，或輸入新或續約的啟動金鑰並按一下**［續約訂閱］**。
已取消	ESET 或您的訂閱轉銷商已取消您的訂閱。	如果您收到錯誤：已在主要程式視窗中或啟動期間取消訂閱，您的訂閱應該能正常運作，請連絡您的訂閱轉銷商。

由於訂閱過度使用而啟動失敗

問題

- 您的訂閱可能被過度使用或濫用
- 由於訂閱過度使用而啟動失敗

解決方案

使用此訂閱的裝置數量超過其所允許的數量。您可能是盜版軟體或仿冒品的受害者。此訂閱無法用於啟動任何其他 ESET 產品。如果您能夠管理您的 ESET HOME 帳戶的訂閱，或已從合法來源購買訂閱，即可直接解決此問題。如果您尚未擁有帳戶，請建立一個帳戶。

如果您是訂閱擁有者且系統並未提示您輸入電子郵件地址：

1. 若要管理 ESET 訂閱，請開啟 Web 瀏覽器並瀏覽至 https://home.eset.com。存取 ESET License Manager 並移除或停用席位。如需詳細資訊，請參閱過度使用訂閱時怎麼辦。

2. 若要識別及報告盜版 ESET 訂閱，請造訪我們的識別及報告盜版 ESET 訂閱文章以取得指示。

3. 如果您不確定，請按一下**［上一步］**並傳送電子郵件給 ESET 技術支援。

如果您不是訂閱擁有者，請連絡此訂閱的擁有者，提供資訊說明因為訂閱過度使用而無法啟動 ESET 產品。擁有者可以在 ESET HOME 入口網站中解決問題。

如果系統提示您確認電子郵件地址（僅限數個案例），請輸入原先用來購買或啟動 ESET Internet Security 的電子郵件地址。

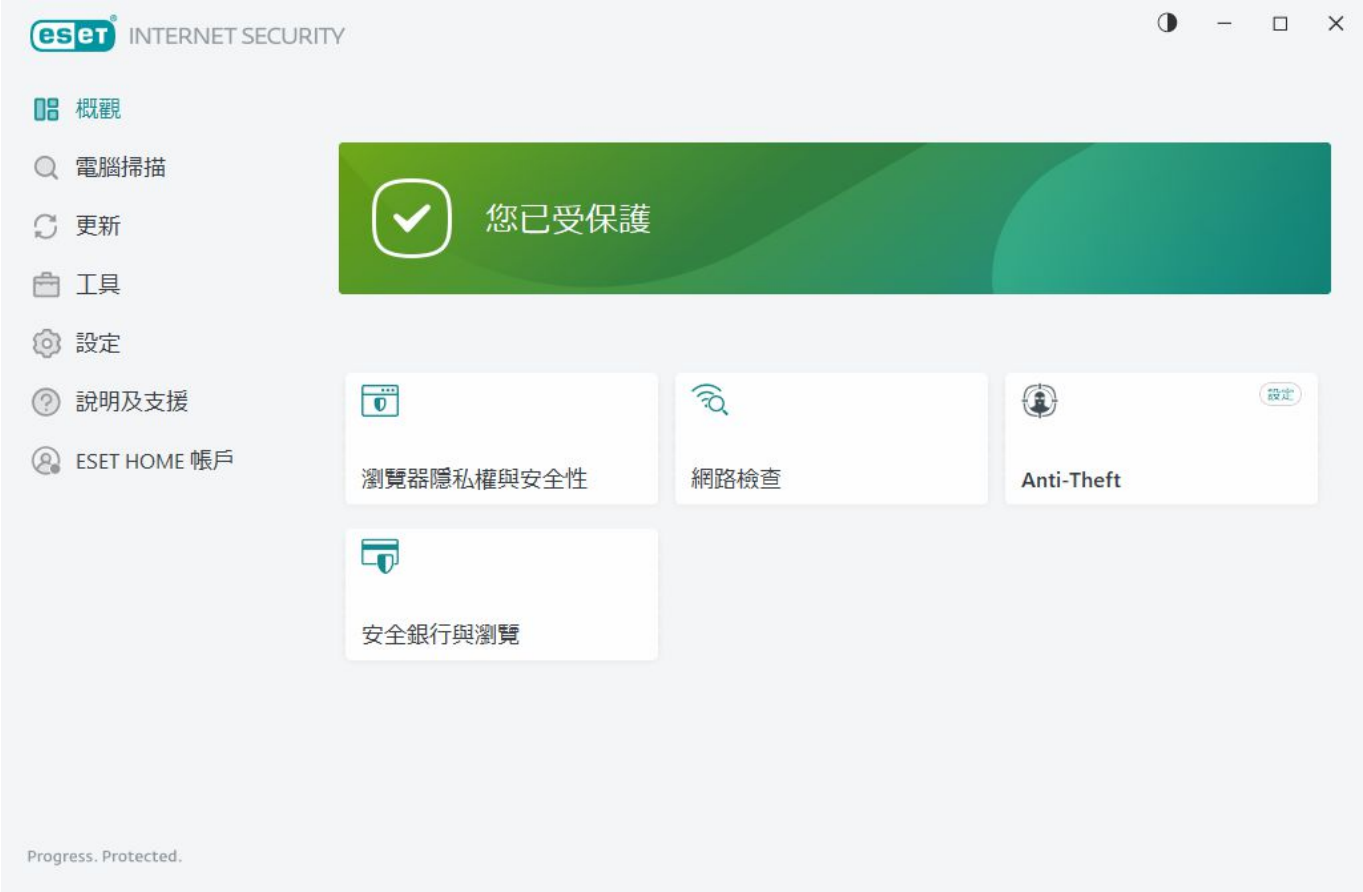
使用 ESET Internet Security

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

> **圖解指示**
> 請參閱開啟 ESET Windows 產品的主要程式視窗圖解指示（以英文和其他數種語言提供）。

您可以選擇主要程式視窗右上角的 ESET Internet Security GUI 色彩主題。按一下 **[最小化]** 圖示旁的 **[色彩主題]** 圖示（該圖示會根據當前選擇的色彩主題變更），然後從下拉式功能表選擇色彩主題：

- **[與系統色彩相同]**—根據您的作業系統設定設定 ESET Internet Security 的色彩配置。
- **[深色]**—ESET Internet Security 將具有深色配置（深色模式）。
- **[淺色]**—ESET Internet Security 將具有標準、淺色配置。



主要功能表選項：

[概觀] - 提供與 ESET Internet Security 的防護狀態有關的資訊。

[電腦掃描] - 配置並啟動電腦掃描，或建立自訂掃描。

更新 - 顯示有關模組和偵測引擎更新的資訊。

工具 - 提供對網路檢查和其他功能的存取，這些功能有助於簡化程式管理，並為進階使用者提供其他選項。

設定 – 提供 ESET Internet Security 防護功能的配置選項（電腦防護、網際網路防護、網路防護與安全性工具）以及對進階設定的存取。

說明及支援 – 顯示有關訂閱、已安裝的 ESET 產品的資訊以及指向 線上說明、ESET 知識庫和技術支援 的連結。

ESET HOME 帳戶 – 將裝置連接到 ESET HOME 或檢閱 ESET HOME 帳戶連線狀態。使用 ESET HOME 以檢視並管理您的 防盜 設定與啟動的 ESET 訂閱和裝置。

概觀

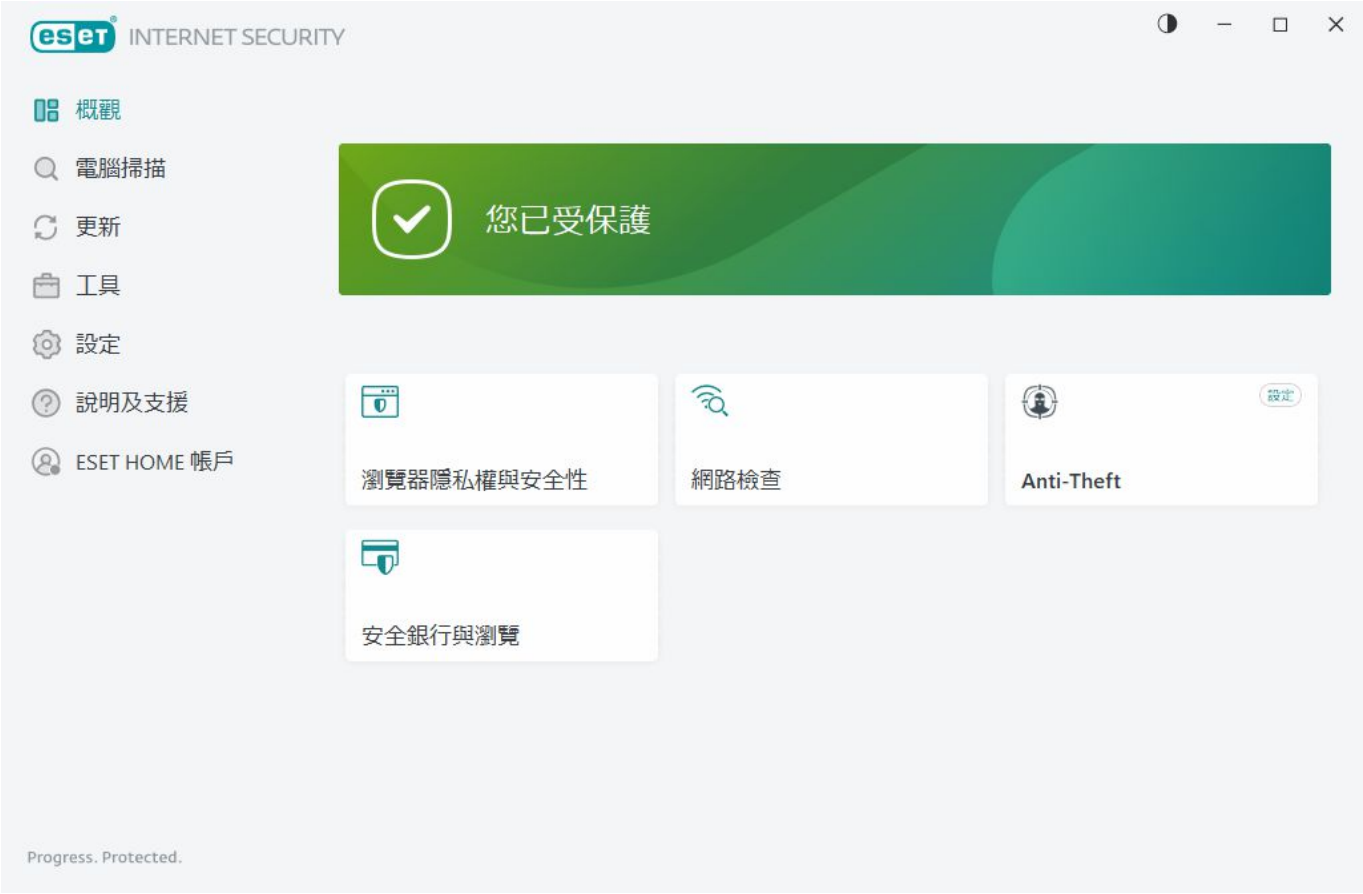
[概觀] 視窗顯示有關電腦目前防護的資訊以及指向 ESET Internet Security 中安全性功能的快速連結。

[概觀] 視窗顯示含有詳細資訊和建議解決方案的通知，以改善 ESET Internet Security 的安全性、開啟其他功能或確保盡可能的防護。如果有更多通知，按一下 **[X 更多通知]** 即可全部展開。

網路檢查 – 檢查您網路的安全性。

安全銀行與瀏覽—在安全模式下，啟動在 Windows 中設為預設值的瀏覽器。

防盜—啟動 [防盜 設定]。若已設定 防盜，請以快速連結開啟 防盜 頁面。



綠色圖示和綠色的 **[您已受保護]** 狀態表示已確保最嚴格的防護。

如果程式運作不正常怎麼辦

如果作用中的防護模組運作正常，其防護狀態圖示會顯示為綠色。紅色驚嘆號或橙色通知圖示表示不確定為最嚴格的防護。有關每個模組防護狀態的其他資訊，以及用於還原完全防護的建議解決方案，在**［概觀］**視窗中顯示為通知。若要變更個別模組的狀態，請按一下**［設定］**並選取所需的模組。

紅色圖示及紅色**安全性警告**狀態表示嚴重問題。有幾個原因會顯示此狀態，例如：

- **［產品未啟動］**或**［訂閱已到期］** – 這是由紅色的防護狀態圖示所表示。您的訂閱過期後即無法更新程式。請按照警告視窗中的指示續約您的訂閱。
- **偵測引擎已過期** – 在數次嘗試更新偵測引擎失敗之後，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。
- **即時檔案系統防護已停用** – 使用者已停用即時防護。無法保護您的電腦阻擋威脅。按一下**［啟用即時檔案系統防護］**以重新啟用此功能。
- **［病毒及間諜程式防護已停用］** – 您可以按一下**［啟用病毒及間諜程式防護］**，以重新啟用病毒及間諜程式防護。
- **［ESET 防火牆已停用］** – 此問題也會在桌面上的**［網路］**項目旁邊以安全性通知表示。您可以按一下**［啟用防火牆］**，以重新啟用網路防護。

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

- **［防盜最佳化警告］** – 裝置未針對 防盜 進行最佳化。例如，您的電腦可能未建立幽靈帳戶（當您將裝置標記為遺失時自動觸發的安全性功能）。您可使用 防盜 Web 介面中的最佳化功能建

立一個幽靈帳戶。

- **[玩家模式作用中]** – 啟用玩家模式有潛在的安全性風險。啟用此功能會停用所有通知/警告視窗並停止任何已排程的工作。
- **[您的訂閱即將到期]/[您的訂閱今日到期]** – 這是由在系統時鐘旁顯示驚嘆號的防護狀態圖示所表示。您的訂閱到期後，程式將無法更新，[防護] 狀態圖示將變成紅色。

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

電腦掃描

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

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

請參閱掃描進度，取得更多關於掃描進度的資訊。

依預設ESET Internet Security 會嘗試自動清除或刪除在電腦掃描期間中發現的偵測項目。在某些情況下，如果無法執行任何動作，您會收到互動式警示並且必須選取清理動作（例如，刪除或忽略）。若要變更清理層級並取得更多詳細資訊，請參閱清理。若要檢閱之前的掃描，請參閱防護記錄檔案

掃描您的電腦

[掃描您的電腦] 可讓您快速啟動電腦掃描並清除感染的檔案，無需使用者介入。**掃描您的電腦**的優點在於可以輕鬆執行作業，而不需要詳細的掃描配置。掃描會檢查本機磁碟機中所有的檔案，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

您也可以使用 **[拖放掃描]** 功能以手動掃描檔案或資料夾，方式是按一下檔案或資料夾，持續按住滑鼠按鈕並將滑鼠指標移動到標記的區域，並放開滑鼠。隨後應用程式即會移動到最上層。

下列是可在 **[進階掃描]** 下取得的掃描選項：

自訂掃描

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

卸除式媒體掃描

與 **[掃描您的電腦]** 類似 – 可快速啟動掃描目前與電腦連接的卸除式媒體（如 CD/DVD/USB）當您將 USB 隨身碟連接到電腦，並想要掃描其內容是否有惡意軟體或其他潛在威脅時，這功能十分有用。

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

重複上次掃描

可讓您使用先前執行時所使用的相同設定，快速啟動先前執行的掃描。

[掃描後的處理方法] 下拉式功能表可讓您設定在掃描完成後自動執行的處理方法：

- **離開** – 掃描結束後，不會執行任何處理方法。
- **關機** – 掃描結束後關閉電腦。
- **需要時重新啟動**—電腦僅在需要完全清除偵測到的威脅時才會重新啟動。
- **重新開機** – 掃描結束後關閉所有已開啟的程式，並重新啟動電腦。
- **需要時強制重新啟動**—電腦僅在需要完全清除偵測到的威脅時才會強制重新啟動。
- **[強制重新開機]** – 強制關閉所有開啟的程式，而無需等待使用者互動，並在掃描完成後重新啟動電腦。
- **睡眠** – 儲存您的工作階段，並且讓電腦處於低耗電狀態，如此您就能夠快速地繼續工作。
- **休眠** – 將您在 RAM 執行的所有作業移動至您硬碟上的特殊檔案。您的電腦會關機，但下一次啟動時又會恢復至先前狀態。

[睡眠] 或 **[休眠]** 動作是否可用取決於您電腦的電源和睡眠作業系統設定，或您電腦/膝上型電腦的功能。請記得睡眠中的電腦仍在運作。當您的電腦以電池運作時，其仍在執行基本功能並會耗電。若要維持電池壽命，例如當您在辦公室外活動時，我們建議使用 [休眠] 選項。

在完成所有執行中的掃描之後，將會開始選取的動作。當您選擇 **[關機]** 或 **[重新開機]** 時，產品確認對話方塊視窗將顯示 30 秒倒數計時（按一下 **[取消]** 可停用要求的處理方法）。

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]** 將掃描配置為排定的工作。如何安排每週電腦掃描?

自訂掃描啟動器

您可以使用 [自訂掃描] 來掃描磁碟內的作業記憶體、網路或特定部分，而不是掃描整個磁碟。若要這樣做，請按一下 **[進階掃描] > [自訂掃描]**，然後從資料夾（樹狀）結構中選取特定目標。

您可以從 **[設定檔]** 下拉式功能表中選擇設定檔，在掃描特定目標時使用。預設的設定檔是 **[智慧型掃描]**。還有三個預先定義的掃描設定檔，名稱分別是 **[深入掃描]**、**[內容功能表掃描]** 與 **[電腦掃描]**。這些掃描設定檔會使用不同的 ThreatSense 參數。可用選項的說明在 [進階設定] > **[偵測引擎] > [惡意軟體掃描] > [指定掃描] >** [ThreatSense] 中。

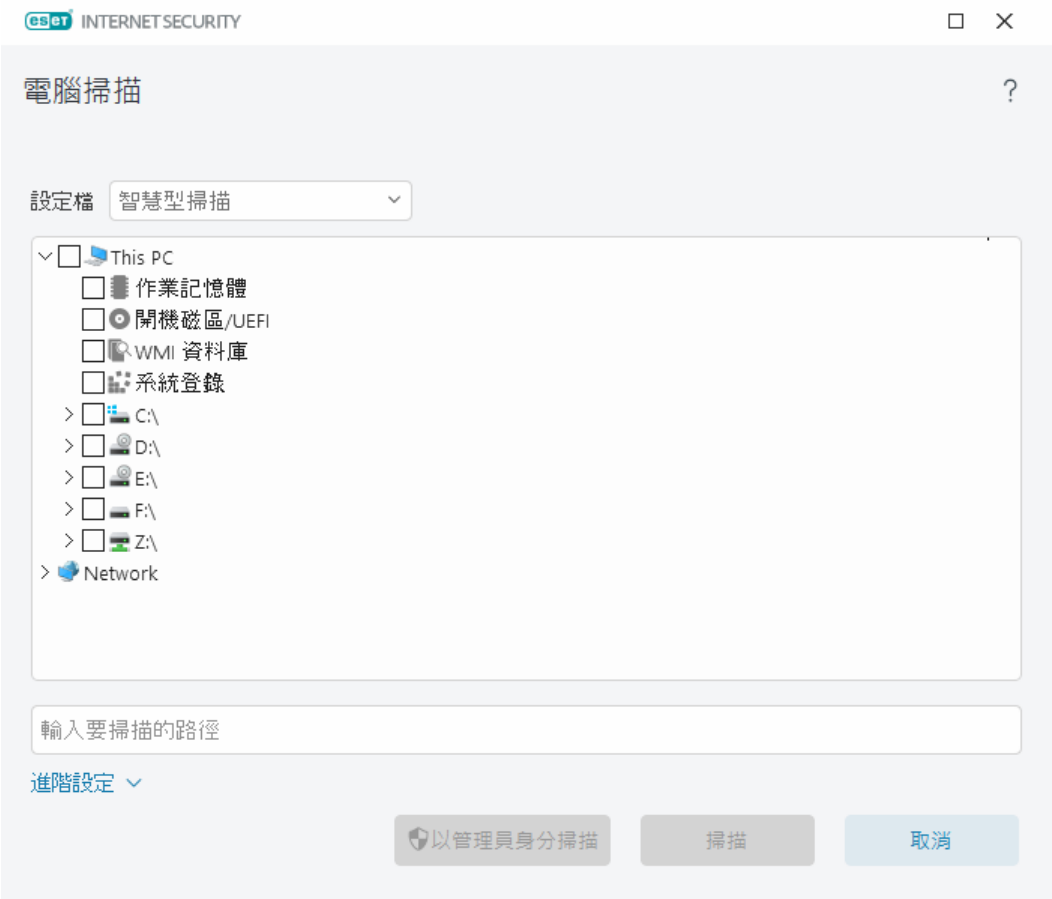
資料夾（樹狀）結構還包含特定掃描目標。

- **作業記憶體** – 掃描目前由作業記憶體使用的所有處理程序和資料。
- **開機磁區/UEFI** – 掃描開機磁區和 UEFI 中是否有惡意軟體。請在字彙中閱讀更多有關 UEFI 掃描器的資訊。
- **WMI 資料庫** – 掃描整個 Windows Management Instrumentation (WMI) 資料庫、所有命名空間、所有類型實例和所有屬性。搜尋對受感染檔案或作為資料嵌入的惡意軟體的參照。
- **系統登錄** – 掃描整個系統登錄、所有鍵和子鍵。搜尋對受感染檔案或作為資料嵌入的惡意軟體的參照。清除偵測時，該參照將保留在登錄表中，以確保不會遺失任何重要資料。

若要快速瀏覽至掃描目標（檔案或資料夾），請在樹狀結構下方的文字欄位中輸入其路徑。該路徑區分大小寫。若要在掃描中包含目標，請在樹狀結構中選取其核取方塊。

如何安排每週電腦掃描

若要安排定期工作，請閱讀如何安排每週電腦掃描



您可以在［進階設定］>［**偵測引擎**］>［**惡意軟體掃描**］>［**指定掃描**］>［**ThreatSense**］>［**清除**］中配置掃描的清除參數。若要執行不使用清除處理方式的掃描，請按一下［**進階設定**］，並選取［**掃描但不清除**］。掃描歷程會儲存在掃描防護記錄中。

當選取［**忽略例外**］時，系統將會掃描其副檔名先前遭排除的檔案，無一例外。

按一下［**掃描**］使用您已設定的自訂參數來執行掃描。

［**以管理員身分掃描**］可讓您在管理員帳戶下執行掃描。若目前的使用者權限不足，無法存取您想要掃描的檔案時，請使用此選項。如果目前的使用者無法以管理員身分呼叫 UAC 作業，則無法使用此按鈕。

當掃描完成時，您可以按一下［顯示記錄檔］來檢視電腦掃描防護記錄檔。

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。

通常無法掃瞄某些檔案，例如密碼保護的檔案或系統專用的檔案（一般是 *pagefile.sys* 及某些防護記錄檔案）。您可以在我們的知識庫文章中找到更多詳細資料。

如何安排每週電腦掃描
若要安排定期工作，請閱讀如何安排每週電腦掃描

掃描進度 – 進度列顯示正在執行的掃描之狀態。

目標 – 目前掃描的物件名稱及其位置。

[發生偵測] – 顯示掃描期間已掃描檔案、找到的威脅與已清除威脅的總數。

按一下 [詳細資訊] 以顯示以下資訊：

- **使用者** – 啟動掃描之使用者帳戶的名稱。
- **掃描的物件數** – 已掃描物件的數量。
- **持續時間** – 已用時間。

暫停圖示 – 暫停掃描。

繼續圖示 – 當掃描進度暫停時，可看見此選項。按一下圖示以繼續掃描。

停止圖示 – 終止掃描。

按一下 **[開啟掃描視窗]** 以開啟電腦掃描防護記錄，其中包含有關掃描的更多詳細資料。

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。

按一下放大鏡或箭頭以顯示目前執行掃描的詳細資訊。您可以按一下 **[掃描您的電腦]** 或 **[進階掃描] > [自訂掃描]**，以執行另一個平行掃描。

[掃描後的處理方法] 下拉式功能表可讓您設定在掃描完成後自動執行的處理方法：

- **離開** – 掃描結束後，不會執行任何處理方法。
- **關機** – 掃描結束後關閉電腦。
- **需要時重新啟動**—電腦僅在需要完全清除偵測到的威脅時才會重新啟動。

- **重新開機** – 掃描結束後關閉所有已開啟的程式，並重新啟動電腦。
- **需要時強制重新啟動**—電腦僅在需要完全清除偵測到的威脅時才會強制重新啟動。
- **[強制重新開機]** – 強制關閉所有開啟的程式，而無需等待使用者互動，並在掃描完成後重新啟動電腦。
- **睡眠** – 儲存您的工作階段，並且讓電腦處於低耗電狀態，如此您就能夠快速地繼續工作。
- **休眠** – 將您在 RAM 執行的所有作業移動至您硬碟上的特殊檔案。您的電腦會關機，但下一次啟動時又會恢復至先前狀態。

[睡眠]或**[休眠]**動作是否可用取決於您電腦的電源和睡眠作業系統設定，或您電腦/膝上型電腦的功能。請記得睡眠中的電腦仍在運作。當您的電腦以電池運作時，其仍在執行基本功能並會耗電。若要維持電池壽命，例如當您在辦公室外活動時，我們建議使用［休眠］選項。

在完成所有執行中的掃描之後，將會開始選取的動作。當您選擇**[關機]**或**[重新開機]**時，產品確認對話方塊視窗將顯示 30 秒倒數計時（按一下**[取消]**可停用要求的處理方法）。

電腦掃描防護記錄

您可以在防護記錄檔案中檢視與特定掃描相關的詳細資訊。掃描防護記錄包含以下資訊：

- 偵測引擎的版本
- 開始日期和時間
- 已掃描的磁碟、資料夾及檔案清單
- 已排程掃描名稱（僅已排程掃描)
- 啟動掃描的使用者。
- 掃描狀態
- 已掃描的物件數目
- 已發現的偵測數目
- 完成時間
- 掃描時間總計

如果之前執行的同一個已排程工作仍在執行中，則會略過已排程電腦掃描工作的新啟動。略過的已排程掃描工作將建立無已掃描物件且狀態為**[掃描未啟動，因為之前的掃描仍在執行中]**的電腦掃描防護記錄。

若要尋找先前的掃描防護記錄，請在主程式視窗中選取**[工具] > [防護記錄檔案]**。在下拉式功能表中，選取**[電腦掃描]**並且按兩下所需的記錄。

若要深入瞭解「無法開啟」、「開啟時發生錯誤」和/或「壓縮檔已損毀」記錄，請參閱我們的 ESET 知識庫文章

按一下滑動軸圖示 **[過濾]** 以開啟 [防護記錄過濾] 視窗，您可在其中定義自訂條件來縮小搜尋範圍。若要檢視內容功能表，請以滑鼠右鍵按一下特定防護記錄項目：

處理方法	使用量
過濾相同的記錄	啟動防護記錄過濾。防護記錄只會顯示與所選記錄相同類型的記錄。
過濾	此選項會開啟 [防護記錄過濾] 視窗，可讓您定義特定防護記錄項目的條件。快捷鍵：Ctrl+Shift+F
啟用過濾	啟動過濾設定。如果您第一次啟動過濾，則必須定義設定，而 [防護記錄過濾] 視窗會隨即開啟。
停用過濾	關閉過濾（如同按一下底部的切換）。
複製	將醒目提示的記錄複製到剪貼簿中。快捷鍵：Ctrl+C
全部複製	複製視窗中的所有記錄。
匯出	將醒目提示的記錄匯出至 XML 檔案。
全部匯出	此選項會將視窗中的所有記錄匯出至 XML 檔案。

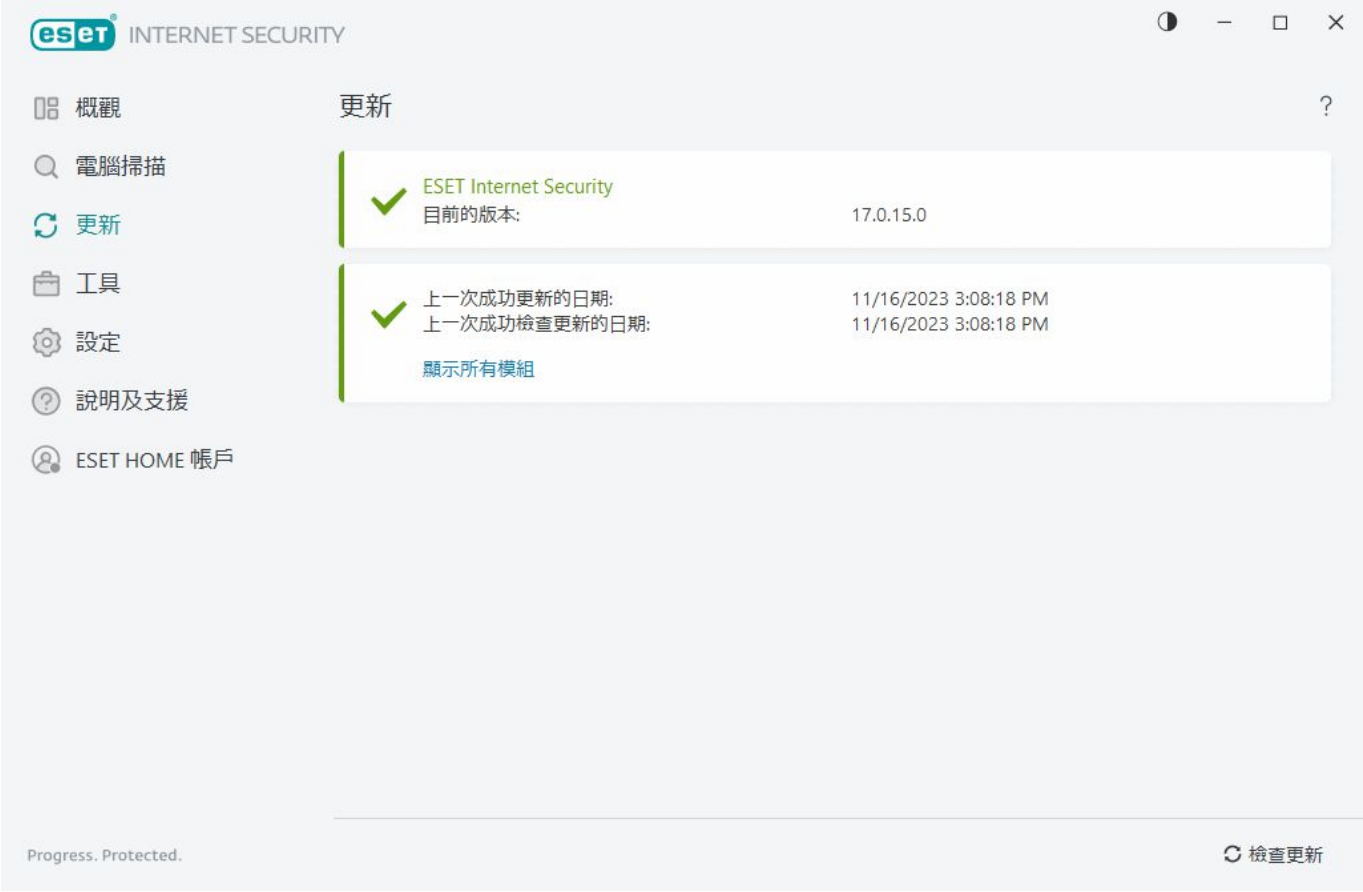
處理方法	使用量
偵測說明	開啟 ESET 威脅百科全書，其中包含有關反白顯示的入侵的危險與症狀詳細資訊。

更新

定期更新 ESET Internet Security 是讓電腦確保有最高安全性等級的最佳方法。更新模組確保程式模組和系統元件永遠為最新狀態。

在主要程式視窗中按一下［**更新**］可以檢視目前更新狀態，包括最後的成功更新日期與時間，並在需要時更新。

除了自動更新，您還可以按一下［**檢查更新**］以觸發手動更新。定期更新程式模組及元件是維持完整防護、防止惡意程式碼的重要一環。請注意產品模組的配置與作業。您必須使用您的啟動金鑰來啟動產品，才可接收更新。如果您未在安裝期間這麼做，您將需要啟動 ESET Internet Security 產品以存取 ESET 更新伺服器。購買 ESET Internet Security 之後ESET 會透過電子郵件將啟動金鑰傳送給您。



［**目前的版本**］ - 顯示您已安裝的目前產品版本的版本編號。

［**上次成功更新**］ - 顯示上次成功更新的日期。如果您看到的不是最近的日期，表示您的產品模組不是最新的狀態。

［**上一次成功檢查更新**］ - 顯示上次成功檢查更新的日期。

［**顯示所有模組**］ - 顯示已安裝的程式模組清單。

按一下［**檢查更新**］以檢查最新可用的 ESET Internet Security 版本。

更新處理程序

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

在正常情況下，您將在［**更新**］視窗中看見綠色核取標記，表示程式是最新狀態。如果您沒有看見綠色核取標記，即表示程式過期，因此更容易遭到感染。請儘快更新程式模組。

更新失敗

若您收到模組更新失敗的訊息，可能是由下列問題所造成：

1. **無效訂閱**—用於啟動的訂閱無效或已過期。在主程式視窗中，按一下［**說明及支援**］>［**變更訂閱**］，並啟動您的產品。

2. **［下載更新檔案時發生錯誤］** – 這可能是因不正確的網際網路連線設定所造成。建議您檢查網際網路連線（透過在 Web 瀏覽器中開啟任何網站）。如果網站未開啟，可能是尚未建立網際網路連線，或是電腦連線有問題。請與「網際網路服務提供者 (ISP)」確認是否有可使用的網際網路連線。

成功將 ESET Internet Security 更新至較新產品版本後，必須重新啟動電腦，以確保所有程式模組都已正確更新。您不需要在定期的模組更新後重新啟動電腦。

如需詳細資訊，請造訪「模組更新失敗」訊息的疑難排解

對話方塊視窗 – 需要重新啟動

將 ESET Internet Security 更新到新版本後，需要重新啟動電腦。新推出的 ESET Internet Security 版本已改善或修正程式模組自動更新所無法解決的問題。

可根據程式更新設定自動安裝新版 ESET Internet Security或透過下載並安裝新版以覆蓋舊版來手動安裝。

按一下 **[立即重新啟動]** 以重新啟動電腦。如果您打算稍後再重新啟動電腦，請按一下 **[稍後提醒我]**。稍後，您可以從主程式視窗中的 **[概觀]** 區段手動重新啟動您的電腦。

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 **[檢查更新]**。

更新還可以執行為已排程的工作。若要設定排程工作，請按一下 **[工具]** > **[排程器]**。預設在 ESET Internet Security 中啟動下列更新工作：

- **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，請參閱排程器一節。

工具

工具 功能表包含許多功能，提供您更高的安全性且有助於簡化 ESET Internet Security 管理。以下工具皆可使用：

 防護記錄檔案

 執行中的處理程序（如果已在 ESET Internet Security 中啟用 ESET LiveGrid®）

 安全性報告

 網路連線（如果防火牆在 ESET Internet Security 中已啟用）

 ESET SysInspector

 排程器

 系統清除程式

 網路檢查

 ［提交範例以進行分析］（可能根據 ESET LiveGrid® 配置無法使用）。

 隔離

防護記錄檔案

防護記錄檔案包含已發生之重要程式事件的相關資訊，並提供偵測到之威脅的概觀。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 Internet Security 環境檢視文字訊息及防護記錄，以及保存防護記錄。

從主要程式視窗中按一下 **[工具] > [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。

• **偵測** – 此防護記錄提供 ESET Internet Security 所偵測到偵測與入侵的詳細資訊。防護記錄資訊包括在偵測到入侵、雜湊與第一次發生時，記錄的偵測時間、掃描器類型、物件類型、物件位置、偵測名稱、採取的動作，以及使用者名稱。未清除的入侵一律會在淺紅色背景上以紅色文字標記。已清除的入侵會在白色背景上以黃色文字標記。而未清除的 PUA 或潛在不安全的應用程式會在白色背景上以黃色文字標記。

• **事件**–ESET Internet Security 執行的所有重要處理方法都會記錄在事件防護記錄中。事件防護記錄包含程式中已發生事件及錯誤的相關資訊。此選項專供系統管理員及使用者用來解決問題。通常在這裡找到的資訊可協助您找到程式中所發生問題的解決方案。

• **電腦掃描** – 所有已完成的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，以檢視所選掃描的詳細資料。

• **[HIPS]** – 包含已標記要記錄之特定 HIPS 規則的記錄。通訊協定會顯示觸發作業、結果（是否允許或禁止規則），及規則名稱的應用程式。

• **[瀏覽器防護]**—包含瀏覽器中載入的未驗證/不受信任之檔案的記錄。

• **[網路防護]** – 網路防護記錄會顯示防火牆、網路攻擊防護 (IDS) 和殭屍網路防護偵測到的所有遠端攻擊。您可以在這裡找到電腦上任何攻擊的資訊。事件直欄會列出已偵測到的攻擊。［來源］直欄會告知您關於攻擊者的相關資訊。［通訊協定］直欄會反映用於攻擊的通訊協定。網路防護記錄分析可協助即時偵測到系統入侵的企圖，以防止未經授權的系統存取。如需網路攻擊的詳細資訊，請參閱 IDS 及進階選項。

• **已過濾的網站** – 如果要檢視被 Web 存取防護或家長控制封鎖的網站清單，此清單非常有用。每個防護記錄會包含建立特定網站連線的時間、URL 位址、使用者與應用程式。

- **電子郵件用戶端反垃圾郵件** – 包含與標記為垃圾郵件之電子郵件相關的記錄。

- **[家長控制]** – 顯示由家長控制所封鎖或允許的網頁。比對類型與比對值直欄會告訴您過濾規則的套用方式。

- **裝置控制** – 包含連接到電腦的可移除媒體或裝置記錄。僅含有個別裝置控制規則的裝置將記錄於防護記錄檔案中。如果規則不符合連接的裝置，將不會對連接的裝置建立防護記錄項目。您也可以檢視詳細資訊，例如裝置類型、序號、供應商名稱及媒體大小（如果有）。

- **[網路攝影機防護]** – 包含網路攝影機防護封鎖的應用程式記錄。

選取任何防護記錄的內容並按下 **CTRL + C** 將其複製到剪貼簿。按住 **CTRL** 或 **SHIFT** 以選取多個項目。

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

以滑鼠右鍵按一下特定記錄，來開啟內容功能表。內容功能表有以下可用選項：

- **顯示** – 顯示有關在新視窗中所選取防護記錄的詳細資訊。

- **過濾相同的記錄** – 啟動此過濾器之後，您只會看見相同類型的記錄（診斷、警告...）。

- **[過濾]** – 按一下此選項之後，會出現 [防護記錄過濾] 視窗，可讓您定義特定防護記錄項目的過濾條件。

- **啟用過濾** – 啟動過濾設定。

- **停用過濾** – 清除所有過濾器設定值（如上所述）。

- **複製/全部複製** – 複製視窗中所選記錄的相關資訊。

- **[複製儲存格]**—複製按右鍵之儲存格的內容。

- **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/全部匯出** – 以 XML 格式匯出所選記錄或所有記錄的相關資訊。

- **尋找/尋找下一個/尋找上一個** – 在按一下此選項後，可以使用 [防護記錄過濾] 視窗定義過濾條件來反白顯示特定項目。

- **偵測說明** – 開啟 ESET 威脅百科全書，其中包含有關已記錄入侵的危險與症狀詳細資訊。

- **[建立排除]** – 使用精靈建立新的偵測排除（不適用於惡意軟體偵測）。

- **新增至瀏覽器防護允許清單**—開啟瀏覽器防護允許清單視窗，並將項目新增到清單中。

防護記錄過濾

按一下 **[工具] > [防護記錄檔案]** 中的 **[過濾]**，用以定義過濾標準。

防護記錄過濾功能會協助您找到您所尋找的資訊，尤其是在有許多記錄的情況下。該功能可讓您縮小防護記錄範圍，例如，若要尋找特定類型、狀態或時段的事件。您可以指定某些搜尋選項來過濾防護記錄，讓 [防護記錄檔案] 視窗只顯示相關（根據搜尋選項）的記錄。

在 **[尋找文字]** 欄位中輸入您要搜尋的關鍵字。使用 **[搜尋直欄]** 下拉式功能表來縮小搜尋範圍。從 **[記**

錄防護記錄類型］下拉式功能表中選擇一或多筆記錄。定義要顯示結果的［**時段**］。您也可以使用進一步的搜尋選項，例如［**所有文字須相符**］或［**區分大小寫**］。

尋找文字

輸入字串（字詞，部分的字詞）。只會顯示包含此字串的記錄。將會省略其他記錄。

搜尋直欄

選取在搜尋時所要納入考量的欄。您可以勾選一或多個要用於搜尋的欄。

記錄類型

從下拉式功能表中選擇一或多個防護記錄類型：

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

時段

定義要顯示結果的時段。

- **未指定**（預設） – 不會在時段內搜尋，而是搜尋整個防護記錄。
- **前一天**
- **上週**
- **上個月**
- **時段** – 您可以指定確切的時段（［自：］和［至：］），只過濾所指定時段的記錄。

所有文字須相符

若您想利用完整文字進行更精確的搜尋，請選取此核取方塊。

區分大小寫

若過濾時一定要使用大寫或小寫字母，請啟用此選項。在您配置好過濾/搜尋選項後，請按一下［**確定**］以顯示過濾後的防護記錄，或按一下［**尋找**］開始搜尋。系統會從您目前的位置（醒目提示的記錄），由上至下搜尋防護記錄檔案。搜尋會在找到第一筆對應記錄時停止。按 **[F3]** 以搜尋下一筆記錄，或按一下滑鼠右鍵並選取［**尋找**］來縮小您的搜尋範圍選項。

執行程序

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 Internet Security 可提供執行中處理程序的詳細資訊，以使用 ESET LiveGrid® 技術保護使用者。

[聲譽] - 在大部分情況下，ESET Internet Security 和 ESET LiveGrid® 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。

[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。若要開啟［工作管理員］，請於工具列的空白區按下滑鼠右鍵，然後按一下**［工作管理員］**，或按下鍵盤上的 **Ctrl+Shift+Esc** 鍵。

標記為良好（綠色）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以改善效能。

[PID] - 處理程序識別碼可在不同的功能呼叫中作為參數使用，例如：調整程序的優先順序。

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 LiveGrid® 技術收集。

發現時間 - 應用程式由 ESET LiveGrid® 技術發現以來的時間。

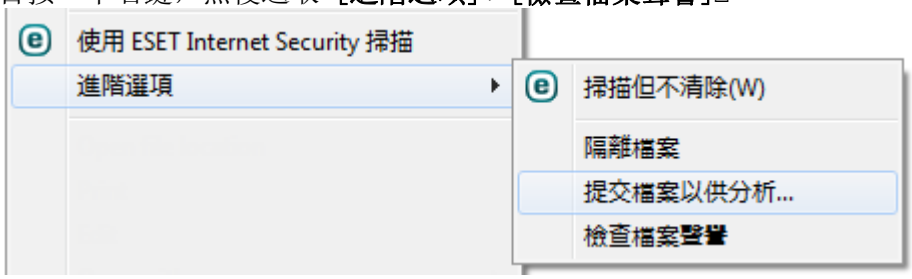
標記為未知（橙色）的應用程式並不代表一定是惡意軟體。它通常只是新的應用程式。若您對檔案不確定，可以提交檔案以供分析至 ESET 的研究實驗室。如果檔案證實為惡意的應用程式，則其偵測會新增到近期的更新中。

應用程式名稱 - 程式或處理程序的指定名稱。

對任一應用程式按一下以顯示該應用程式的下列詳細資訊：

- **路徑** – 電腦上應用程式的位置。
- **大小** – 單位為 kB 或 MB 的檔案大小。
- **說明** – 根據作業系統說明的檔案特性。
- **公司** – 供應商或應用程式處理程序的名稱。
- **版本** – 來自應用程式發行者的資訊。
- **產品** – 應用程式名稱和/或商業名稱。
- **[建立/修改日期]** – 建立（修改）的日期及時間。

您也可以針對不作為執行中程式/處理程序的檔案檢查聲譽。若要這麼做，請在檔案總管中對這些項目按一下右鍵，然後選取 **[進階選項] > [檢查檔案聲譽]**。



安全性報告

此功能提供下列類別的統計資料概觀：

- **[已封鎖網頁]** – 顯示已封鎖的網頁數目 (PUA 的黑名單 URL、網路釣魚、遭駭的路由器、IP 或憑證)。
- **[偵測到受感染的電子郵件物件]** – 顯示偵測到的受感染電子郵件物件數目。
- **[已封鎖之家長控制中的網頁]** – 在 [家長控制] 中顯示已封鎖的網頁數目。
- **偵測到 PUA** – 顯示潛在不需要的應用程式 (PUA) 數目。
- **[偵測到垃圾郵件]** – 顯示偵測到的垃圾電子郵件數目。
- **已封鎖的網路攝影機存取** – 顯示已封鎖的網路攝影機存取權數目。
- **已掃描文件數**—顯示已掃描的文件數目。
- **已掃描應用程式數** – 顯示已掃描的可執行檔物件數目。
- **已掃描其他物件數** – 顯示其他已掃描物件數目。
- **已掃描網頁物件數** – 顯示已掃描的網頁物件數目。
- **已掃描的電子郵件物件數** – 顯示已掃描的電子郵件物件數目。

這些類別的順序是根據數值從最大排序到最小。值為零的類別不會顯示。按一下 **[顯示更多]** 可展開與顯

示隱藏的類別。

安全性報告的最後一個部分可讓您啟用以下功能：

- 家長控制
- 防盜

此功能一旦啟用後，在安全性報告中便不再顯示成無法運作。

按一下右上角的齒輪 ⚙，您可以 **[啟用/停用安全性報告通知]**，或選取是否將顯示過去 30 天的資料，或自報告啟用起的資料。如果 ESET Internet Security 安裝不到 30 天，則只能選取自安裝起的天數。依預設期間設為 30 天。

[重設資料] 將清除所有統計資料，並移除安全性報告的現有資料。必須確認此動作，除非您取消選取 **[進階設定]** > [通知] > **[互動警示]** > **[確認訊息]** > **[編輯]** 中的 **[重設統計之前詢問]** 選項。

網路連線

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

按一下圖表圖示 以開啟網路活動。

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

直欄

應用程式/本機 IP – 應用程式名稱、本機 IP 位址及通訊連接埠。

遠端 IP – 特定遠端電腦的 IP 位址及連接埠號碼。

通訊協定 – 使用的傳送通訊協定。

上傳速度/下載速度 – 對外與對內資料的目前速度。

已傳送/已接收 – 連線內交換的資料數量。

顯示詳情 – 選擇此選項以顯示所選取連線的詳細資訊。

以滑鼠右鍵按一下連線可查看其他選項，包括：

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

僅顯示 TCP 連線 – 清單僅顯示屬於 TCP 通訊協定組合的連線。

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

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

重新整理速度 – 選擇重新整理作用中連線的頻率。

立即重新整理 – 重新載入**[網路連線]**視窗。

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

[暫時拒絕處理程序的通訊] – 拒絕指定應用程式的目前連線。如果已建立新連線，則防火牆會使用預先定義的規則。您可以在防火牆規則區段中找到設定的說明。

[暫時允許處理程序的通訊] – 允許指定應用程式的目前連線。如果已建立新連線，則防火牆會使用預先定義的規則。您可以在防火牆規則區段中找到設定的說明。

網路活動

若要以圖形格式查看目前的**[網路活動]**，請按一下**[工具] > [網路連線]**，然後按一下圖形圖示 。圖形的底端是根據所選時間範圍即時記錄網路活動的時間表。若要變更時間範圍，請從**[重新整理率]**下拉式功能表中選取適用的值。

可用選項如下：

- **1 秒** – 圖表每秒鐘都會重新整理，且時間表包含最近 4 分鐘。
- **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。
- **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。

圖形的垂直軸表示接收或傳送的資料數量。將滑鼠游標暫留在圖形上，即可查看特定時間的確切接收/傳送資料數量。

ESET SysInspector

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

ESET SysInspector 視窗會顯示以下的防護記錄相關資訊：

- **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：

- **顯示** – 在 ESET SysInspector 中開啟所選的防護記錄。您也可以在指定的防護記錄檔案上按一下右鍵，並從內容功能表選取 **[顯示]**。
- **建立** – 建立新的防護記錄。先等候直到產生 ESET SysInspector 為止（**[已建立]** 狀態），再嘗試存取防護記錄。防護記錄儲存在 C:\ProgramData\ESET\ESET Security\SysInspector 中。
- **刪除** – 從清單移除選取的防護記錄。

選取一個或多個防護記錄後，內容功能表中即有以下項目可供使用：

- **顯示** – 在 ESET SysInspector 中開啟所選取的防護記錄（與按兩下防護記錄的功能相同）。
- **建立** – 建立新的防護記錄。先等候直到產生 ESET SysInspector 為止（**[已建立]** 狀態），再嘗試存取防護記錄。
- **刪除** – 從清單移除選取的防護記錄。
- **全部刪除** – 刪除所有防護記錄。
- **匯出** – 將防護記錄匯出至 .xml 檔或壓縮的 .xml。

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 Internet Security 主要程式視窗存取排程器。**[排程器]** 包含已排程的工作與其配置內容（如預先定義的日期、時間及使用的掃描設定檔）的清單。

[排程器] 可用來排程下列工作： 更新模組、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**[新增工作]** 或 **[刪除]**）。您可以按一下 **[預設]**，將排程的工作清單還原成預設，並刪除所有變更。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**
- **使用者登入後自動更新**
- **啟動檔案自動檢查**（使用者登入後）
- **[啟動檔案自動檢查]**（成功更新偵測引擎後）

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]**。

新增工作

1. 按一下視窗底部的 **[新增工作]**。
2. 輸入工作的名稱。
3. 自下拉式功能表選取想要的工作：
   - **執行外部應用程式** - 排程以執行外部應用程式。
   - **防護記錄維護** - 防護記錄檔案還包括已刪除記錄的剩餘部分。此工作會定期最佳化防護記錄檔案中的記錄，以有效運作。
   - **系統啟動檔案檢查** - 檢查系統啟動或登入時允許執行的檔案。
   - **建立電腦狀態快照** - 建立 ESET SysInspector 電腦快照 - 收集關於系統元件（例如驅動程式、應

用程式）的詳細資訊，並評估各個元件的風險層級。

- **指定電腦掃描** - 針對電腦中的檔案及資料夾執行掃描。
- **[更新]** - 更新模組來排程更新工作。

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

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

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

- **於下次排程的時間**
- **儘快**
- **如果距離上次執行的時間超過（小時），則立即執行工作** - 表示自第一次略過工作執行起經過的時間。如果已超過此時間，此工作會立即執行。使用下方的微調按鈕設定時間。

若要檢閱已排程的工作，以滑鼠右鍵按一下工作，然後按一下**[顯示工作詳情]**。

已排程掃描選項

在此視窗中，您可以指定已排程電腦掃描工作的進階選項。

若要執行不使用清除處理方式的掃描，請按一下**[進階設定]**，並選取**[掃描但不清除]**。掃描歷程會儲存在掃描防護記錄中。

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

[掃描後的處理方法]下拉式功能表可讓您設定在掃描完成後自動執行的處理方法：

- **離開** - 掃描結束後，不會執行任何處理方法。
- **關機** - 掃描結束後關閉電腦。
- **需要時重新啟動**—電腦僅在需要完全清除偵測到的威脅時才會重新啟動。
- **重新開機** - 掃描結束後關閉所有已開啟的程式，並重新啟動電腦。
- **需要時強制重新啟動**—電腦僅在需要完全清除偵測到的威脅時才會強制重新啟動。
- **[強制重新開機]** - 強制關閉所有開啟的程式，而無需等待使用者互動，並在掃描完成後重新啟動

電腦。

- **睡眠** – 儲存您的工作階段，並且讓電腦處於低耗電狀態，如此您就能夠快速地繼續工作。
- **休眠** – 將您在 RAM 執行的所有作業移動至您硬碟上的特殊檔案。您的電腦會關機，但下一次啟動時又會恢復至先前狀態。

i **［睡眠］**或**［休眠］**動作是否可用取決於您電腦的電源和睡眠作業系統設定，或您電腦/膝上型電腦的功能。請記得睡眠中的電腦仍在運作。當您的電腦以電池運作時，其仍在執行基本功能並會耗電。若要維持電池壽命，例如當您在辦公室外活動時，我們建議使用［休眠］選項。

在完成所有執行中的掃描之後，將會開始選取的動作。當您選擇**［關機］**或**［重新開機］**時，產品確認對話方塊視窗將顯示 30 秒倒數計時（按一下**［取消］**可停用要求的處理方法）。

選取**［掃描無法取消］**，拒絕讓不具權限的使用者可在掃描後停止動作。

如果您要允許受限的使用者暫停電腦掃描一段指定的時間，選取**［使用者可以暫停掃描的時間（分鐘）］**此選項。

另請參閱掃描進度

已排程的工作概要

當您按兩下自訂工作，或在自訂排程器工作上按一下滑鼠右鍵，並按一下**［顯示工作詳情］**時，此對話方塊視窗會顯示關於所選取已排程工作的詳細資訊。

工作細節

在**［工作名稱］**中輸入名稱，並選取其中一個**［工作類型］**選項，接著按一下**［下一步］**

- **執行外部應用程式** – 排程以執行外部應用程式。
- **防護記錄維護** – 防護記錄檔案還包括已刪除記錄的剩餘部分。此工作會定期最佳化防護記錄檔案中的記錄，以有效運作。
- **系統啟動檔案檢查** – 檢查系統啟動或登入時允許執行的檔案。
- **建立電腦狀態快照** – 建立 ESET SysInspector 電腦快照 – 收集關於系統元件（例如驅動程式、應用程式）的詳細資訊，並評估各個元件的風險層級。
- **指定電腦掃描** – 針對電腦中的檔案及資料夾執行掃描。
- **［更新］** – 更新模組來排程更新工作。

工作時間

工作將在指定的時間間隔內重複執行。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之後執行。

使用電池執行時略過工作 – 在工作應啟動時，如果電腦使用電池執行，則不會啟動工作。以 UPS 執行的電腦也一樣。

工作時間 – 一次

執行工作 – 指定的工作僅會在指定的日期與時間執行一次。

工作時間 – 每天

工作會每天在指定的時間執行。

工作時間 – 每週

此工作將重複在每週所選的星期幾和時間執行。

工作時間 – 由事件觸發

下列任一事件將會觸發工作：

- **每次電腦啟動時**
- **每天電腦第一次啟動時**
- **撥號連線至網際網路/VPN**
- **模組成功更新時**
- **產品成功更新時**
- **使用者登入**
- **威脅偵測**

當排程由事件觸發的工作時，您可以指定兩次工作完成之間的最小間隔。例如，如果您一天登入電腦多次，則可以選擇只在當天第一次登入後的 24 小時內執行工作，接著是隔天第一次登入後的 24 小時內。

略過的工作

如果電腦使用電池執行或已關閉電源，則會略過工作。從這些選項中選取要執行已略過工作的時間，接著按一下 **[下一步]**。

- **在下次排程的時間** – 工作將在電腦於下次排程的時間開啟時執行。
- **盡快** – 工作將在電腦開啟時執行。

• **如果距離上次排程執行的時間超過（小時），則立即執行工作** – 表示自第一次略過工作執行起經過的時間。如果已超過此時間，此工作會立即執行。

如果距離上次排程執行的時間超過（小時），則立即執行工作 – 範例

範例工作設定為每小時重複執行一次。**[如果距離上次排程執行的時間超過（小時），則立即執行工作]** 選項已選取，且超過的時間設定為兩小時。工作在 13:00 執行，完成時電腦會進入睡眠狀態：

• 電腦在 15:30 喚醒。第一個略過的工作執行時間是在 14:00。從 14:00 開始僅過去 1.5 小時，因此工作將在 16:00 執行。

• 電腦在 16:30 喚醒。第一個略過的工作執行時間是在 14:00. 從 14:00 開始已過去兩個半小時，因此工作將立即執行。

工作詳細資料 – 更新

如果您想要從兩個更新伺服器更新程式，則需要建立兩個不同的更新設定檔。如果第一個設定檔無法下載更新檔案，則程式會自動切換至替代設定檔。舉例說明，此設定適用於筆記型電腦，因為擁有人通常會從本機區域網路更新伺服器進行更新，但使用其他網路卻經常連接至網際網路。所以，如果第一個設定檔失敗，則第二個會自動從 ESET 的更新伺服器下載更新檔案。

工作詳細資料 – 執行應用程式

此工作會排程外部應用程式的執行時間。

執行檔 – 從目錄樹狀結構選擇可執行檔，按一下 **[...]** 選項或手動輸入路徑。

工作資料夾 – 定義外部應用程式的工作目錄。將在此目錄中建立選取的 **[執行檔]** 暫存檔案。

參數 – 應用程式的命令列參數（選用）。

按一下 **[完成]** 以套用工作。

系統清除程式

系統清除程式是協助您清除威脅後，將電腦還原到可使用狀態的工具。惡意軟體能夠停用系統公用程式，例如登錄編輯器 、工作管理員或 Windows 更新。系統清除程式只要按一下即可還原指定系統的預設值和設定。

系統清除程式會從五個設定類別回報問題：

- **[安全性設定]**： 可能造成您電腦弱點擴大的設定中之變更，例如 Windows 更新
- **[系統設定]**： 可能變更您電腦行為的系統設定中之變更，例如檔案關聯
- **[系統外觀]**： 影響您系統顯示風格的設定，例如桌面桌布
- **[停用的功能]**： 可能已停用的重要功能和應用程式
- **[Windows 系統還原]** Windows 系統還原功能設定，可允許您將系統還原到先前的狀態

可在這些情況中要求系統清除：

- 發現威脅時

- 使用者按一下［**重設**］時

您可檢閱變更並在適當時候重設設定。

僅具有管理員權限的使用者可在系統清除程式中執行動作。

網路檢查

［網路檢查］可協助識別信任（家用或辦公室）網路弱點（例如已開啟的連接埠或弱式路由器密碼）。此功能也可提供給您已連線的裝置清單，並依照裝置類型分類（例如印表機、路由器、行動裝置等），來顯示連線到您網路的裝置（例如遊戲主機、IoT 或其他智慧型家用裝置）。

［網路檢查］可協助您在連線至網路時識別路由器的弱點，並提高防護等級。

網路檢查不會為您重新配置路由器。您需使用路由器特定的介面自行變更。家用路由器很容易受到惡意軟體的危害，進而啟動分散式拒絕服務攻擊 (DDoS)。若使用者未從預設變更路由器密碼，則駭客可輕易猜到密碼，並登入您的路由器且重新配置或危害您的網路。

我們強烈建議您建立強式密碼，要夠長且包含數字、符號或大寫字母。若要使密碼難以破解，請使用混合或不同類型的字元。

如果您連線的網路已配置為信任，則可以將網路標記為「我的網路」。按一下**［標記為「我的網路」］**以將「我的網路」標籤新增至網路。在整個 ESET Internet Security 中此標籤將顯示在網路旁邊，以提供更佳的識別與安全性概觀。按一下**［取消標記為「我的網路」］**以移除標籤。

每部連線至網路的裝置都會在清單檢視中顯示，並顯示基本資訊。按一下特定裝置，即可編輯裝置或檢視裝置的詳細資訊。

［**網路**］下拉式功能表允許您根據以下條件過濾裝置：

- 連線到特定網路的裝置
- 連線至**所有網路**的裝置
- 未分類的裝置

按一下裝置圖示以編輯裝置或檢視裝置的詳細資訊。最近連線的裝置會顯示在靠近路由器的位置，這樣您就可以輕易認出。

按一下右上角的齒輪 ⚙，選取在網路中發現新裝置時，是否要傳送通知。

按一下［**掃描您的網路**］以手動執行掃描您目前連線的網路。［**掃描網路**］僅適用於信任的網路。請參閱網路連線設定檔以檢閱或編輯網路設定。

您可以從下列掃描選項中選擇：

- 全部掃描
- 僅掃描路由器
- 僅掃描裝置

⚠ 僅在信任的網路上執行網路掃描！若您在不信任的網路上執行此動作，則會有潛在的危險。

掃描完成時，將會顯示包含連結到有關裝置基本資訊的通知；您也可以在清單或聲納檢視中連按兩下可疑裝置。按一下［**疑難排解**］以查看最近封鎖的通訊。防火牆疑難排解詳細資訊

有兩種由網路檢查模組顯示的通知：

- **[連線至網路的新裝置]** – 如果之前從未見過的裝置在使用者連線時連線至網路，即會顯示。
- **找到新的網路裝置** – 如果您重新連線至您信任的網路且出現從未見過的裝置時，即會顯示。

若有未授權的裝置正嘗試連線至您的網路，這兩種通知都會告知您。按一下 **[檢視一部裝置]** 以顯示裝置詳細資料。

網路檢查中的裝置圖示有何含義？

	黃色星形圖示表示網路上的新裝置，或是 ESET 首次檢測到的裝置。
	黃色警告圖示表示您的路由器可能包含弱點。請按一下您產品中的圖示，以獲得該問題的更多詳細資訊。
	紅色警告圖示表示您的路由器包含弱點，且可能有已遭感染的裝置。請按一下您產品中的圖示，以獲得該問題的更多詳細資訊。
	當您的 ESET 產品具有路由器的其他資訊，但不需要立即注意（因為不存在安全風險）時，可能會出現藍色圖示。請按一下您產品中的圖示，以獲得更多詳細資訊。

網路檢查中的網路裝置

可在此找到有關裝置的詳細資訊，包含下列資訊：

- 裝置名稱
- 裝置類型
- 上次連線
- 網路名稱
- IP 位址
- MAC 位址
- 作業系統

鉛筆圖示表示您可以修改裝置名稱或變更裝置類型。

[從歷程移除] – 將裝置從裝置清單中刪除。此選項僅適用於目前未與網路連線的裝置。

對於每種類型的裝置，以下是可用的處理方法：

路由器

[路由器設定] – 您可以從 Web 介面、行動應用程式，或按一下 **[開啟路由器介面]**，來存取路由器設定。如果您擁有網際網路服務提供者提供的路由器，則可能需要連絡網際網路服務提供者支援資源或路由器製造商，以解決偵測到的安全性問題。請一律遵循路由器使用者指南中指示的適當安全預防措施。
防護若要保護您的路由器和網路免於網路安全性攻擊，請遵循這些基本建議。

網路裝置

[裝置識別] - 如果您不確定裝置是否與您的網路連線，請檢查裝置名稱下方的供應商或製造商名稱。這可以幫助您確定裝置類型。您可以更改裝置名稱以供日後參考。
[正在中斷裝置的連線] - 如果您不確定連線的裝置對您的網路或裝置是否安全，請在路由器設定中管理此裝置的網路存取權或更改網路密碼。
[保護] - 若要保護您的裝置免受攻擊與惡意軟體的威脅，請在您的裝置上安裝網路安全性防護，且讓您的作業系統與已安裝的軟體一直維持在最新的狀態。若要持續受到保護，請勿連線到不安全的 Wi-Fi 網路。

此裝置

此裝置代表您在網路上的電腦。
[網路介面卡] - 顯示您的網路介面卡資訊。

通知 | 網路檢查

下方是 ESET Internet Security 在您的路由器上偵測到弱點問題時，可以顯示的數種通知。每個通知包含一則簡短說明，並提供某些解決方案或應該依序進行的步驟，用以將您路由器的弱點風險降至最低。如果您不熟悉路由器變更，我們建議您聯絡路由器製造商或網際網路提供者。

發現潛在弱點
您的路由器可能包含使它易於攻擊和入侵的已知弱點。更新您的路由器的韌體。

發現弱點
您的路由器包含使它易於攻擊和入侵的已知弱點。更新您的路由器的韌體。

發現威脅
您的路由器已遭到惡意軟體感染。重新啟動您的路由器並重複進行掃描。

弱式路由器密碼
您的路由器上的密碼太弱，可能會被其他人輕易猜到。變更您路由器中的密碼。

惡意網路重新導向
您的網際網路流量似乎被重新導向至惡意網站。這可能表示您的路由器遭到洩漏。在您的路由器中變更 DNS 伺服器設定。

開放式網路服務
您的路由器執行的網路服務可能已遭其他人入侵。這可能是因配置錯誤或洩漏的路由器所造成。檢查您路由器的配置。

敏感的開放式網路服務
您的路由器執行的敏感網路服務可能已遭其他人入侵。這可能是因配置錯誤或洩漏的路由器所造成。檢查您路由器的配置。

韌體已過時
您的路由器上的韌體過時，可能包含弱點。更新您路由器上的韌體。

惡意路由器設定
您使用的 DNS 伺服器為惡意，可能將您傳送至危險的網站。這可能表示您的路由器遭到洩漏。在您的路由器中變更 DNS 伺服器設定。

網路服務
您的路由器執行常見的網路服務。這些是網路所需且可能是安全的。檢查您路由器的配置。

隔離區

隔離區的主要功能是安全地儲存已報告的物件（例如惡意軟體、受感染的檔案或潛在不需要的應用程式）。

按一下 **[工具] > [隔離區]**，即可從 ESET Internet Security 主要程式視窗存取隔離區。

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：

- 隔離區的日期和時間、
- 檔案原始位置的路徑、
- 大小（以位元組為單位）、
- 原因（例如由使用者新增物件）、
- 以及多種偵測（例如，同一檔案的重複偵測，或者如果該檔案是包含多個滲透的壓縮檔）。

隔離檔案

ESET Internet Security 會自動隔離被刪除的檔案（如果您尚未在［警報視窗］中取消該選項）。

還應隔離符合下列條件的其他檔案：

a.無法清除、

b.若檔案不安全或建議刪除、

c.若檔案被 ESET Internet Security 錯誤地偵測到、

d.或者如果檔案行為可疑但未被防護偵測到。

若要隔離檔案，您有多個選項：

a.使用拖放掃描功能以手動隔離檔案或資料夾，其方法是按一下檔案，持續按住滑鼠按鈕並將滑鼠

指標移動到標記的區域，然後放開滑鼠。隨後應用程式即會移動到最上層。

b.以滑鼠右鍵按一下檔案 > 按一下 **[進階選項] > [隔離檔案]**。

c.從 **[隔離]** 視窗中按一下 **[移至隔離區]**。

d.也可以使用右鍵功能表達到此目的。在 **[隔離區]** 視窗中按右鍵，然後選取 **[隔離區]**。

從隔離區還原

隔離的檔案也可以還原到其原始位置：

- 對隔離區中指定的檔案按滑鼠右鍵會出現內容功能表，使用其中的 **[還原]** 功能便可達成此目的。
- 如果檔案被標記為潛在不需要的應用程式，將啟用 **[還原並從掃描中排除]** 選項。另請參閱排除。
- 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。
- 在某些情況下還原功能不可用，例如位於唯讀網路共用上的檔案。

從隔離區刪除

以滑鼠右鍵按一下指定項目，並選取 **[從隔離區中刪除]**，或選取您要刪除的項目，並按下鍵盤上的 **[刪除]**。如果要選取並刪除隔離區中的所有項目，可以在鍵盤上按下 **Ctrl + A**，然後按 **Delete**。刪除的項目會從您的裝置和隔離區永久刪除。

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，請將範例傳送至 ESET 研究實驗室。若要提交檔案，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]**。

偵測說明

以滑鼠右鍵按一下某個項目，然後按一下 **[偵測說明]** 以開啟 ESET 威脅百科全書，其中包含有關已記錄入侵的危險與症狀詳細資訊。

圖解指示

下列 ESET 知識庫文章可能僅以英文提供：

- 還原 ESET Internet Security 中隔離的檔案
- 刪除 ESET Internet Security 中隔離的檔案
- 我的 ESET 產品已向我發送偵測通知，我該做些什麼?

隔離失敗

無法將特定檔案移到隔離區的原因如下所示：

- **您沒有讀取權限** – 表示您無法檢視檔案的內容。
- **您沒有寫入權限** – 表示您無法修改檔案的內容，即新增新內容或刪除現有內容。
- **您正嘗試隔離的檔案過大** – 您需要減少檔案大小。

當您收到「隔離失敗」的錯誤訊息時，請按一下 **[更多資訊]**。隨即顯示［隔離錯誤清單］視窗，您將看到檔案的名稱以及無法隔離檔案的原因。

選取樣本以供分析

如果您在電腦上發現可疑的檔案，或在網際網路上發現可疑的網站，您可以將其提交至 ESET 研究實驗室以供分析（根據您的 ESET LiveGrid® 配置而定，有可能無法使用）。

提交檔案至 ESET 之前
請確認樣本至少符合下列一項標準，否則請勿提交：
- 完全未由您的 ESET 產品進行過偵測
- 在偵測後被誤認為威脅
- 若您提交的樣本，是希望 ESET 掃描其中是否有惡意軟體的個人檔案，恕我們無法接受；請注意 ESET 研究實驗室不為使用者執行隨選掃描）
- 請使用敘述性的主旨行，並盡可能涵蓋檔案的相關資訊（例如快照或下載的網站）。

您可以使用下列方法之一，將樣本提交（檔案或網站）傳送至 ESET 以供分析：

1. 使用產品中的樣本提交表單。表單位於 **[工具] > [提交樣本以供分析]**。提交的範例大小上限為 256 MB。

2. 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/WinZIP 來壓縮檔案、使用密碼 "infected" 來保護壓縮檔，然後將其傳送至 samples@eset.com。

3. 若要報告垃圾郵件、垃圾郵件誤判或由家長控制模組錯誤分類的網站，請參閱我們的 ESET 知識庫文章。

在 **[選取樣本以供分析]** 表單中，請從 **[提交樣本的原因]** 下拉式功能表中選取最符合您訊息目標的說明：

- 可疑檔案
- 可疑網站（受到惡意軟體感染的網站）、
- 誤判網站
- 誤判檔案（偵測為感染但實際上未受感染的檔案）、
- 其他

檔案/網站 – 要提交的檔案或網站路徑。

連絡人電子郵件 – 這個連絡人電子郵件會與可疑檔案一併傳送到 ESET 並可用於在需要進一步資訊以供分析時連絡您。輸入連絡人電子郵件為選用。選取 **[匿名提交]** 以將其保留空白。

您可能不會收到 ESET 的回應。
由於我們的伺服器每天都會接收到成千上萬個檔案，所以除非您要求更多資訊。否則我們不可能一一回覆，因此您將不會收到 ESET 的回應。
如果樣本證實為惡意的應用程式或網站，則其偵測會新增到近期的 ESET 更新中。

選取樣本以供分析 – 可疑檔案

觀察到的惡意軟體感染徵兆與信號 – 輸入在您電腦上觀察到的可疑檔案行為的說明。

[檔案來源 (URL 位址或供應商)] – 請輸入檔案來源以及您在何種狀況下發現這個檔案。

附註與其他資訊 – 您可以在這裡新增其他資訊或說明，這在處理可疑檔案時將會很有助益。

> 雖然第一個參數 – **[觀察到的惡意程式感染徵兆與信號]** – 是必要參數，但是提供其他資訊將可大幅協助實驗室識別處理程序和處理樣本。

選取樣本以供分析 – 可疑網站

請在 **[網站有什麼問題]** 下拉式功能表中選取下列其中一個選項：

- **受感染** – 網站包含病毒或透過各種方法所散佈的其他惡意軟體。
- **網路釣魚** – 通常用於存取像是銀行帳號PIN 等敏感資料。請在字彙中閱讀更多有關此類型攻擊的資訊。
- **[惡作劇]** – 騙局或詐欺網站，專門為了快速獲取利益。
- 如果上述選項不適用於您將提交的網站，請選取 **[其他]**

[附註與其他資訊] – 您可以輸入有助於分析可疑網站的其他資訊或說明。

選取樣本以供分析 – 誤判檔案

我們要求您提交偵測為感染但並未受感染的檔案，以便改善病毒及間諜程式防護引擎，並協助其他人受到防護。如果檔案樣式符合偵測引擎中所含的樣式，就會發生誤判 (FP)

應用程式名稱與版本 – 程式標題及其版本（例如編號、別名或代碼名稱）。

檔案來源 (URL 位址或供應商) – 請輸入檔案來源，並註明您在何種狀況下發現這個檔案。

應用程式目的 – 一般應用程式說明、應用程式類型（例如瀏覽器、媒體播放器...）及其功能。

附註與其他資訊 – 您可以在這裡新增其他資訊或說明，這在處理可疑檔案時將會很有助益。

> 必須有前三個參數，才能識別合法應用程式並與惡意程式碼區分。提供其他資訊將可大幅協助實驗室識別處理程序和處理樣本。

選取樣本以供分析 – 誤判網站

您必須提交偵測為感染、詐騙或網路釣魚但尚未受感染的檔案。如果檔案樣式符合偵測引擎中所含的樣式，就會發生誤判 (FP)請提供此網站以改善我們的病毒及網路釣魚防護引擎，並協助其他人受到保護。

附註與其他資訊 – 您可以在這裡新增其他資訊或說明，這在處理可疑網站時將會很有助益。

選取樣本以供分析 – 其他

如果檔案無法歸類為［**可疑檔案**］或［**誤判**］，請使用這份表單。

提交檔案的原因 – 請輸入詳細說明及傳送檔案的原因。

設定

您可以在主程式視窗 > ［**設定**］中尋找可用的防護功能群組。

［**設定**］功能表分為下列群組：

電腦防護

網際網路防護

網路防護

安全性工具

設定視窗最下方提供其他選項。按一下［進階設定］，為每個模組設定更詳細的參數。使用［匯入/匯出設定］選項可使用 .xml 配置檔案載入設定參數，或將目前的設定參數儲存至配置檔案。

電腦防護

在主程式視窗 > [設定] 中按一下 [電腦防護] 以查看所有防護模組的概觀：

- [即時檔案系統防護] - 開啟、建立或執行所有檔案時，都會掃描這些檔案是否具有惡意程式碼。
- [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。
- [玩家模式] - 啟用或停用玩家模式。啟用玩家模式之後，您將收到警告訊息（潛在的安全性風險），接著主視窗會轉為橙色。
- [網路攝影機防護] - 控制存取、您的攝影機的處理程序與應用程式。

若要暫停或停用個別防護模組，請按一下切換開關 

⚠ 關閉防護模組可能會降低您電腦的保護層級。

按一下齒輪圖示 ⚙（位於防護模組旁）以存取該模組的進階設定。

對於 [即時檔案系統防護]，按一下齒輪圖示 ⚙，並選擇以下選項：

- **配置** – 開啟即時檔案系統防護進階設定
- **編輯排除** - 開啟 [排除設定] 視窗，讓您可以排除無須掃描的檔案和資料夾。

對於 [網路攝影機防護]，按一下齒輪圖示 ⚙，並選擇以下選項：

- **配置** – 開啟網路攝影機防護進階設定
- **封鎖所有存取，直到重新啟動** - 封鎖對網路翔影機的所有存取，直到電腦重新開機。
- **永久封鎖所有存取** - 封鎖對網路攝影機的所有存取，直到此設定停用為止。
- **[停止封鎖所有存取]** - 停用對網路攝影機存取權的封鎖功能。此選項僅在封鎖網路攝影機時可供使用。

[暫停病毒及間諜程式防護] - 停用所有防毒及間諜程式防護模組。當您停用防護之後，視窗將會開啟，您可在該處使用 **[時間間隔]** 下拉式功能表來決定停用防護的時間長度。僅在您是有經驗的使用者或由 ESET 技術支援指示下使用。

偵測到入侵

入侵可以從網頁、共用資料夾等不同的進入點，透過電子郵件或從卸除式裝置 (USB、外部磁碟、CD、DVD 等) 到達系統。

標準行為

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

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

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

掃描電腦搜尋受感染的檔案

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：

1.開啟 ESET Internet Security然後按一下 **［電腦掃描］**

2.按一下 **［掃描您的電腦］**（如需詳細資訊，請參閱電腦掃描)

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。

清除及刪除

如果沒有要針對即時檔案系統防護採取的預先定義處理方法，則會提示您在警告視窗中選取一個選項。通常可以使用 **［清除］[刪除］** 及 **［離開］** 選項。不建議選取 **［離開］**，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）。

從隔離區還原

按一下 **[工具] > [隔離區]**，即可從 ESET Internet Security 主要程式視窗存取隔離區。

隔離的檔案也可以還原到其原始位置：

- 對隔離區中指定的檔案按滑鼠右鍵會出現內容功能表，使用其中的 **[還原]** 功能便可達成此目的。
- 如果檔案被標記為潛在不需要的應用程式，將啟用 **[還原並從掃描中排除]** 選項。另請參閱排除。
- 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。
- 在某些情況下還原功能不可用，例如位於唯讀網路共用上的檔案。

多種威脅

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

刪除壓縮檔中的檔案

在預設清除模式中，只有在整個壓縮檔包含受感染的檔案而不包含未感染檔案時，才會刪除它。也就是說，如果壓縮檔還包含無害的未感染檔案，則不會進行刪除。執行完全清除掃描時請小心，因為啟用完全清除後，當壓縮檔內含有至少一個受感染的檔案時，即會刪除壓縮檔，無論壓縮檔中其他檔案的狀態為何。

網際網路防護

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。開啟［主程式視窗］>［設定］>［網際網路防護］在 ESET Internet Security 中配置可增強網際網路防護的功能。

若要暫停或停用個別防護模組，請按一下切換開關

⚠ 關閉防護模組可能會降低您電腦的保護層級。

按一下齒輪圖示（位於防護模組旁）以存取該模組的進階設定。

家長控制模組會藉由封鎖網際網路上不當或有害的內容來保護您的孩子。

Web 存取防護掃描 HTTP/HTTPS 通訊以尋找惡意軟體和網路釣魚。僅應為疑難排解而關閉 Web 存取防護。

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

報告網路釣魚網站 – 向 ESET 報告網路釣魚/惡意網站以進行分析。

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

電子郵件用戶端防護可控制透過 POP3(S) 和 IMAP(S) 通訊協定收到的電子郵件通訊。使用電子郵件用戶端的外掛程式ESET Internet Security 可控制來自電子郵件用戶端的所有通訊。

電子郵件用戶端反垃圾郵件過濾來路不明的電子郵件。

對於［**電子郵件用戶端反垃圾郵件**］，按一下齒輪圖示 ，並從以下選項進行選擇：

• **配置** – 開啟電子郵件用戶端反垃圾郵件的進階設定

• **使用者的位址清單**（若已啟用） – 開啟對話方塊視窗，您可以在其中新增、編輯或刪除位址，以定義反垃圾郵件規則。此清單中的規則將套用至目前使用者。

• **全域位址清單**（若已啟用） – 開啟對話方塊視窗，您可以在其中新增、編輯或刪除位址，以定義反垃圾郵件規則。此清單中的規則將套用至所有使用者。

防網路釣魚防護

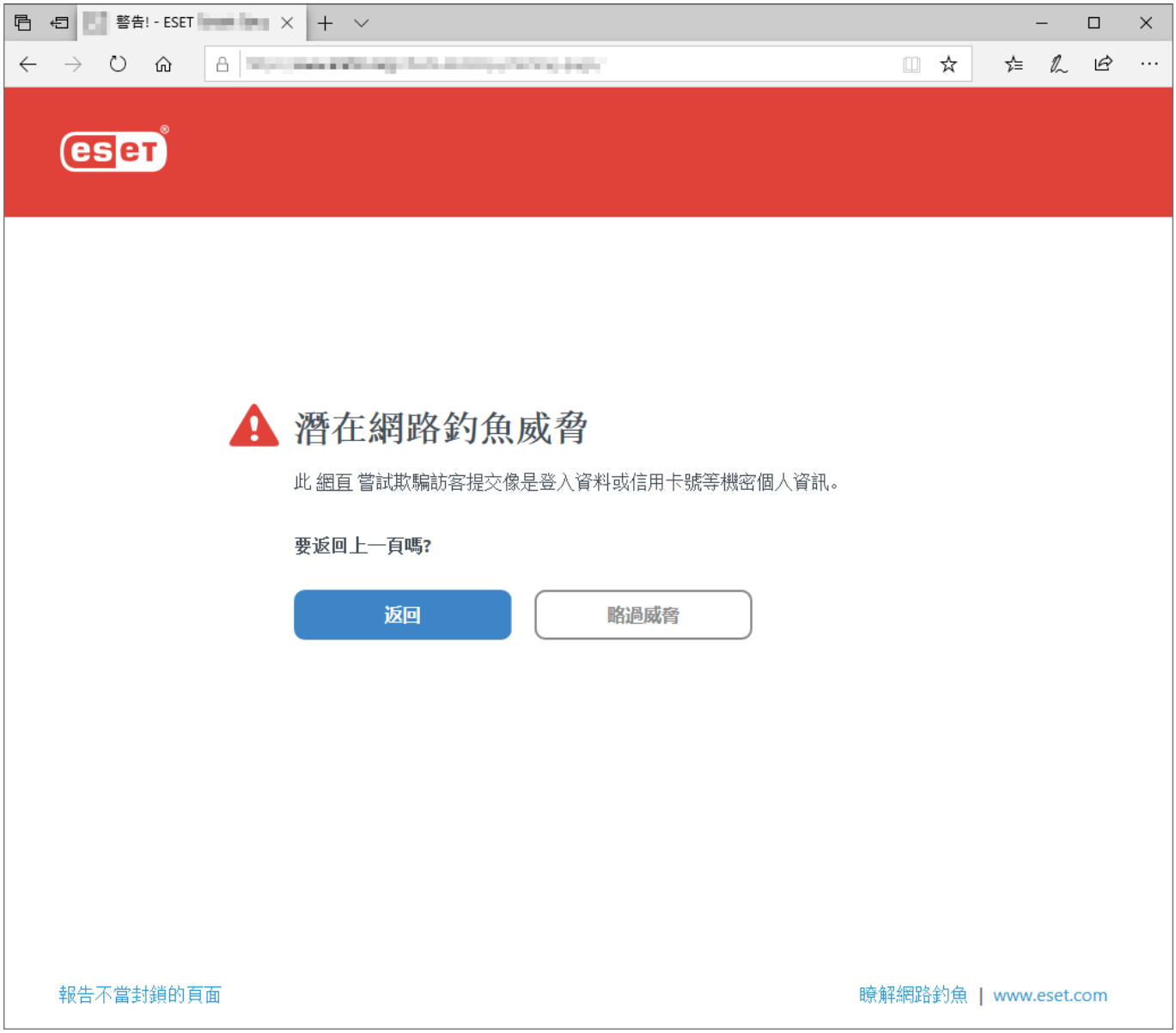
網絡釣魚是一種利用社交工程（操縱使用者以取得機密資訊）的犯罪活動。網絡釣魚用於存取敏感資料，例如銀行帳號PIN 等。如需詳細資訊，請參閱字彙ESET Internet Security 包含防網路釣魚防護，封鎖已知會散佈這類內容的網頁。

依預設，防網路釣魚防護已啟用。可在［進階設定］>［**防護**］> **[Web 存取防護**］中配置此設定。

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

存取網路釣魚網站

當您存取已辨識的釣魚網站時，您的 Web 瀏覽器將顯示以下對話方塊。如果您仍想存取網站，請按一下［**略過威脅**］（不建議）



已列入白名單的潛在網路釣魚網站會依預設在數小時後過期。若要能永久存取該網站，請使用 URL 位址管理工具。在 [進階設定] > [防護] > [Web 存取防護] > [URL 位址管理] > [位址清單] > [編輯] 中，將您要編輯的網站新增至此清單。

回報網路釣魚網站

回報不正確封鎖的頁面連結可讓您回報被錯誤偵測為威脅的網站。

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

家長控制

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

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

若要啟動特定使用者帳戶的家長控制，請遵循以下步驟：

1. 依預設ESET Internet Security 中的家長控制為停用。有兩種方式可以啟用家長控制：

   • 從主要程式視窗中，按一下 **[設定] > [網際網路防護] > [家長控制]** 中的切換開關圖示 ，並將家長控制狀態變更為已啟用。

   • 開啟 [進階設定] > **[防護] > [Web 存取防護] > [家長控制]**，然後啟用 **[啟用家長控制]** 旁邊的切換開關。

2. 按一下主要程式視窗中的 **[設定] > [網際網路防護] > [家長控制]**。即使 **[啟用]** 已顯示於 **[家長控制]** 旁，您仍需按一下箭頭符號，然後在下一個視窗中選取 **[保護兒童帳戶]** 或 **[家長帳戶]**，為所需的帳戶配置家長控制。在下一個視窗中選取出生日以決定存取層級與適合年齡的建議網頁。現在將為指定的使用者帳戶啟用家長控制。按一下帳戶名稱下的 **[封鎖的內容和設定]**，即可在類別索引標籤中自訂您要允許或封鎖的類別。若要允許或封鎖不符合類別的自訂網頁，請按一下例外索引標籤。

若您從 ESET Internet Security 的主要產品視窗中按一下 **[設定] > [網際網路防護] > [家長控制]**，您將看到主要視窗包含：

Windows 使用者帳戶

如果您已為現有帳戶建立角色，該角色會在此顯示。按一下滑桿 ，便會在帳戶的［家長控制］旁顯示綠色核取標記 。在作用中的帳戶下，按一下封鎖內容和設定 ，即可顯示此帳戶允許的網頁類別清單，以及封鎖和允許的網頁。

視窗底端部分包含

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

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

家長控制

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

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

家長控制需要啟用網路流量掃描器、HTTP(S) 流量掃描和防火牆才能正常運作。這些功能皆預設為已啟用。

網站例外

若要新增網站例外，請按一下 **［設定］** > **［網際網路防護］** > **［家長控制］** 然後按一下 **［新增網站例外］**。

在 **［網站 URL］** 欄位中輸入 URL 選取 （已允許）或 （已封鎖）項目，適用於個別的特定使用者帳戶，接著按一下 **［確定］** 以將該項目新增至清單。

若要從清單中刪除 URL 位址，請按一下 **[設定] > [網際網路防護] > [家長控制]**，在所需的使用者帳戶下按一下 **[封鎖內容和設定]**，按一下 **[例外]** 索引標籤，選取例外並按一下 **[移除]**。

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

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

從使用者複製例外

從下拉式功能表選取您要從其位置複製已建立例外的使用者。

從帳戶複製類別

讓您從現有的已修改帳戶複製遭封鎖或允許的類別清單。

網路防護

開啟 [主程式視窗] > [設定] > [網路防護] 配置基本網路防護設定或對網路通訊進行疑難排解。

若要暫停或停用個別防護模組，請按一下切換開關

關閉防護模組可能會降低您電腦的保護層級。

按一下齒輪圖示 （位於防護模組旁）以存取該模組的進階設定。

防火牆 – 根據 ESET Internet Security 配置過濾所有網路通訊。

配置 – 開啟防火牆進階設定視窗，您可在其中定義防火牆處理網路通訊的方式。

暫停防火牆（允許所有流量） – 關閉所有防火牆過濾選項，允許所有對內及對外連線。當網路流量過濾處於此模式時，按一下 **[啟用防火牆]** 以重新啟用防火牆。

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

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

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

網路攻擊防護 (IDS) – 分析網路流量的內容，並防範網路攻擊。將封鎖任何視為有害的流量。ESET Internet Security 會在您連線至未受保護的無線網路或防護不足的網路時通知您。

[殭屍網路防護] – 快速及準確地發現系統裡的惡意程式。

網路連線 – 顯示網路介面卡連線到的網路以及詳細資訊。

解決封鎖的通訊 – 協助您解決 ESET 防火牆所造成的連線問題。如需詳細資訊，請參閱「疑難排解精靈」。

解決暫時封鎖的 IP 位址 – 檢視已偵測為攻擊來源的 IP 位址清單，並新增至黑名單中以封鎖特定期間的連線

顯示防護記錄 – 開啟網路防護防護記錄檔案。

網路連線

顯示網路介面卡要連線的網路。若要查看網路連線，請開啟 [主程式視窗] > **[設定]** > **[網路防護]** > **[網路連線]**。

按兩下清單中的連線以顯示其詳細資料和網路介面卡詳細資料。

將滑鼠暫留在特定網路連線上，然後按一下 **[信任]** 欄中的功能表圖示 ⋮，以選擇以下選項之一：

- **編輯** – 開啟配置網路防護視窗，您可以在其中將網路防護設定檔指派給特定網路
- **忘記** – 將網路連線配置重設為預設值
- **使用網路檢查掃描網路** – 開啟網路檢查以執行網路掃描。
- **標記爲「我的網路」** – 在網路中新增「我的網路」標籤；此標籤將在整個 ESET Internet Security 中顯示在網路旁邊，以便提供更好的識別和安全性概觀
- **取消標記為「我的網路」** – 移除「我的網路」標籤；僅當網路已被標記時才可用

網路連線詳細資料

按兩下網路連線清單中的連線，以顯示其詳細資料以及網路介面卡詳細資料。網路連線和介面卡詳細資料可協助您識別嘗試在網路存取防護中配置的網路。

網路連線詳細資料：

- 網路連線的狀態

- 首次網路偵測的日期和時間
- 上次網路處於作用中狀態的時間
- 連線到此網路所耗總時間
- 網路連線設定檔
- 在 Windows 中定義的網路連線設定檔
- 網路防護配置（網路是否受信任）

網路介面卡詳細資料：

- 連線類型（有線、虛擬等）
- 網路介面卡名稱
- 介面卡說明
- 包含 MAC 位址的 IP 位址
- 具有子網路的網絡之 IPv4 和 IPv6 位址
- DNS 尾碼
- DNS 伺服器 IP
- DHCP 伺服器 IP
- 預設閘道 IP 和 MAC 位址
- 介面卡 MAC 位址

網路存取疑難排解

疑難排解精靈能幫助您解決防火牆所造成的連線問題。可以在主程式視窗 > **[設定]** > **[網路防護]** > **[解決封鎖的通訊]** 中找到 **[網路存取疑難排解]**。

選取是要顯示 **[本機應用程式]** 封鎖的通訊還是自 **[遠端裝置]** 封鎖的通訊。

從下拉式功能表中，選取要封鎖通訊的時段。最近封鎖的通訊可讓您概覽應用程式或裝置類型和該時段中封鎖的應用程式和裝置總數及聲譽。如需有關封鎖通訊的詳細資料，請按一下 **[詳細資料]**。下個步驟是解除封鎖您發生連線問題的應用程式或裝置。

當您按一下 **[解除封鎖]** 時，將會允許先前封鎖的通訊。若應用程式持續發生問題，或者您的裝置未如預期運作，請按一下 **[建立其他規則]**，先前針對該裝置封鎖的所有通訊現在將會允許。若問題持續存在，請重新啟動電腦。

按一下 **[開啟防火牆規則]** 以查看精靈建立的規則。此外，您也可看到精靈在 [進階設定] > **[防護]** > **[網路存取防護]** > **[防火牆]** > **[規則]** > **[編輯]** 中建立的規則。

如果無法建立規則，您將收到錯誤訊息。按一下 **[再試一次]** 並重複處理程序以取消封鎖的通訊，或從封鎖的通訊清單中建立其他規則。

暫時性 IP 位址黑名單

若要檢視已偵測為攻擊來源且已新增至黑名單中（以在特定時間段內封鎖連線）的 IP 位址，請開啟 [主程式視窗] > [設定] > [網路防護] > [解決暫時封鎖的 IP 位址]。暫時性封鎖的 IP 會封鎖 1 小時。

直欄

[IP 位址] – 顯示已封鎖的 IP 位址。

[封鎖原因] – 顯示已從位址避免的攻擊類型（例如 TCP 連接埠掃描攻擊）。

[逾時] – 顯示黑名單中位址將到期的時間和日期。

控制項元素

[移除] – 按一下位址以在其到期之前從黑名單中移除。

[全部移除] – 按一下以立即從黑名單中移除所有位址。

[新增例外] – 按一下以將防火牆例外新增至 IDS 過濾。

網路防護防護記錄

ESET Internet Security 網路防護將所有重要事件儲存在防護記錄檔案中。若要檢視防護記錄檔案，請開啟 [主程式視窗] > [設定] > [網路防護] > [顯示防護記錄]。

防護記錄檔案可用於偵測錯誤，並揭露系統的入侵事件。網路防護記錄檔案包含下列資料：

- 事件的日期及時間
- 事件名稱
- 來源
- 目標網路位址
- 網路通訊協定
- 套用的規則，或蠕蟲名稱（若已識別）
- 應用程式路徑和名稱
- 雜湊
- 使用者
- 應用程式的簽章者（發行者）
- 套件名稱
- 服務名稱

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

> **安全性弱點利用**
> 即使已經對特定弱點進行了修補，系統也會記錄利用安全性弱點的訊息，因為在網路層級偵測並封鎖利用嘗試，才能避免實際利用的情形。

使用防火牆解決問題

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

請參閱下列有關協助解決防火牆相關問題的主題：

- 網路存取疑難排解
- 記錄並從防護記錄建立規則或例外
- 從防火牆通知建立例外
- 網路防護進階記錄
- 使用網路流量掃描器解決問題

記錄並從防護記錄建立規則或例外

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

如需防護記錄的詳細資訊，請參閱「防護記錄檔案

使用記錄查看網路防護封鎖特定連線的順序。此外，從防護記錄建立規則可讓您建立確實需要的規則。

從防護記錄建立規則

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

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

1. 在 [進階設定] > [工具] > [防護記錄檔案] 中，將記錄最簡化設定為 [診斷]

2. 在 [進階設定] > [防護] > [網路存取防護] > [網路攻擊防護] > [進階選項] > [入侵偵測] 中啟用 [通知針對安全性漏洞的對內攻擊]

從防火牆通知建立例外

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

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

網路防護進階記錄

這個功能是用來針對 ESET 技術支援提供更複雜的防護記錄檔案。僅在 ESET 技術支援要求時才使用這個功能，因為其可能會產生大量的防護記錄檔案，而讓您的電腦速度變慢。

1. 開啟 [進階設定] > [工具] > [診斷] > [進階記錄] 並啟用 [啟用網路防護進階記錄]

2. 嘗試重現您所遇到的問題。

3. 停用網路防護進階記錄。

4. 您可以在系統產生診斷記憶體傾印的相同目錄中，找到由網路防護進階記錄所建立的 PCAP 防護記錄檔案： *C:\ProgramData\ESET\ESET Security\Diagnostics*

使用網路流量掃描器解決問題

若您的瀏覽器或電子郵件用戶端發生問題，第一步是判斷網路流量掃描器是否有回應。若要那麼做，在[進階設定] > [**偵測引擎**] > [**網路流量掃描器**] 嘗試暫時停用網路瀏覽掃描器（完成後請記住將其重新開啟，否則，您的瀏覽器和電子郵件用戶端將保持未受防護）。若問題在過濾關閉之後消失，則可參考下列常見問題和解決方法的清單：

更新或保護通訊問題

若您的應用程式通知您無法更新或某通訊通道不安全：

- 若您已啟用 SSL/TLS，請嘗試暫時將其關閉。若有效，您可以排除有問題的通訊，以繼續使用 SSL/TLS 並使更新運作順利：
停用 SSL/TLS重新執行更新。這時應該會出現對話方塊，通知您有關加密網路流量的資訊。請確認應用程式就是您要疑難排解的應用程式，而且憑證看起來是來自其更新來源伺服器。接著選擇記住此憑證的處理方法，並按一下略過。如果沒有顯示其他相關對話方塊，您可以將過濾模式切回自動模式，而問題應該獲得解決。

- 若發生問題的應用程式不是瀏覽器或電子郵件用戶端，您可以完全將其排除在 Web 存取防護之外（這樣處理瀏覽器或電子郵件用戶端會使您暴露在風險中）。任何通訊受到過濾的應用程式都應該已經在新增例外時所提供給您的清單中，因此不需要手動新增。

存取網路上裝置時遇到的問題

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

存取特定網站時遇到的問題

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

錯誤「某些有能力匯入管理者認證的應用程式仍然在運行」

當您啟用 SSL/TLS 時，ESET Internet Security 會確認所安裝的應用程式透過將憑證匯入其憑證儲存區的方式，信任其過濾 SSL 通訊協定的方式。某些應用程式可能會要求重新啟動以匯入憑證。這包括 Firefox 和 Opera 確定這類應用程式不在執行中（完成這項操作的最好方法是開啟［工作管理員］，確定［處理程序］索引標籤下面沒有 firefox.exe 或 opera.exe)接著再點擊重試。

有關不信任的發行人或簽章無效的錯誤

這很可能是指前述的匯入作業失敗。首先，請確定任何上述的應用程式不在執行中。然後停用 SSL/TLS 並重新啟用它。這樣會重新執行匯入作業。

請參閱知識庫文章，以了解如何在 ESET Windows 家用產品中管理網路流量掃描器

已封鎖網路威脅

當您電腦上的某些應用程式正嘗試傳送惡意流量至網路上另一台裝置、濫用安全漏洞，甚至系統偵測到有人試圖掃描連接埠，此情況可能會發生。

您可以在通知中尋找威脅類型和相關裝置 IP 位址。按一下［**變更此威脅的處理方式**］以顯示以下選項：

［**繼續封鎖**］ - 封鎖偵測到的威脅。若您不想再從特定遠端位址接收此類威脅的通知，請選擇［**不通知**］旁的按鈕，然後按一下［**繼續封鎖**］。這會建立具有以下配置的 入侵偵測服務 (IDS) 規則**封鎖** - 預設值，**通知** - 否，**防護記錄** - 否。

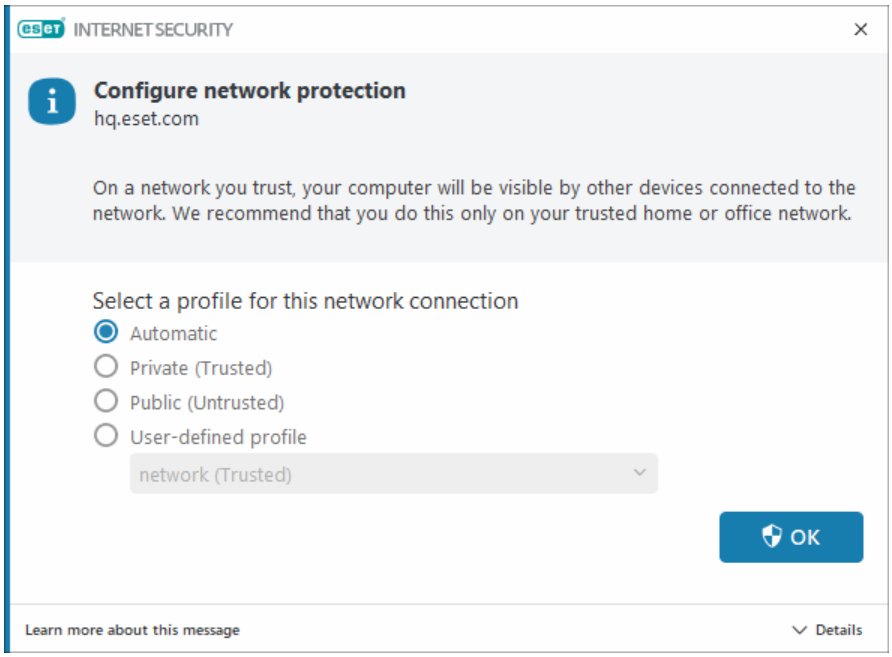
允許—建立 入侵偵測服務 (IDS) 規則 以允許偵測到的威脅。在按下［**允許**］以指定規則設定之前，請從以下選項擇一：

- **僅在此威脅遭封鎖時通知**—規則配置：**封鎖** - 否，**通知** - 否，**防護記錄** - 否。
- **每當此威脅發生時通知**—規則配置：**封鎖** - 否，**通知** - 預設值，**防護記錄** - 預設值。
- **不通知**—規則配置：**封鎖** - 否，**通知** - 否，**防護記錄** - 否。

此通知視窗中顯示的資訊可能會視偵測到的威脅類型而不同。
如需威脅和其他相關詞彙的詳細資訊，請參閱遠端攻擊的類型或入侵類型
若要解決［**重複的網路 IP 位址**］事件，請參閱我們的 ESET 知識庫文章

偵測到新網路

在預設情況下，在偵測到新網路連線時ESET Internet Security 會使用 Windows 設定。若要在偵測到新網路時顯示對話方塊視窗，請將網路防護設定指派變更為［**詢問**］。每當您的電腦連線到新網路時都會顯示網路防護配置。



您可以從以下網路連線設定檔中進行選取：

自動 - ESET Internet Security 將根據為每個設定檔配置的啟動項自動選取設定檔。

私人 – 適用於信任的網路（家用或辦公室網路）。您的電腦和儲存在您電腦上的共用檔案可供其他網路使用者查看，且網路上其他使用者可以存取系統資源（啟用了對共用檔案和印表機的存取，啟用了對內 RPC 通訊，並且遠端桌面共用可用）。建議您在存取安全的區域網路時使用此設定。如果設定檔在 Windows 中配置為網域或私人網路，則會自動將其指派給網路連線。

公用 – 適用於不信任的網路（公用網路）。您系統上的檔案和資料夾未與網路上其他使用者共用或設為可見，系統資源分享將停用。建議您在存取無線網路時使用此設定。此設定檔將自動指派給 Windows 中未配置為網域或私人網路的任何網路連線。

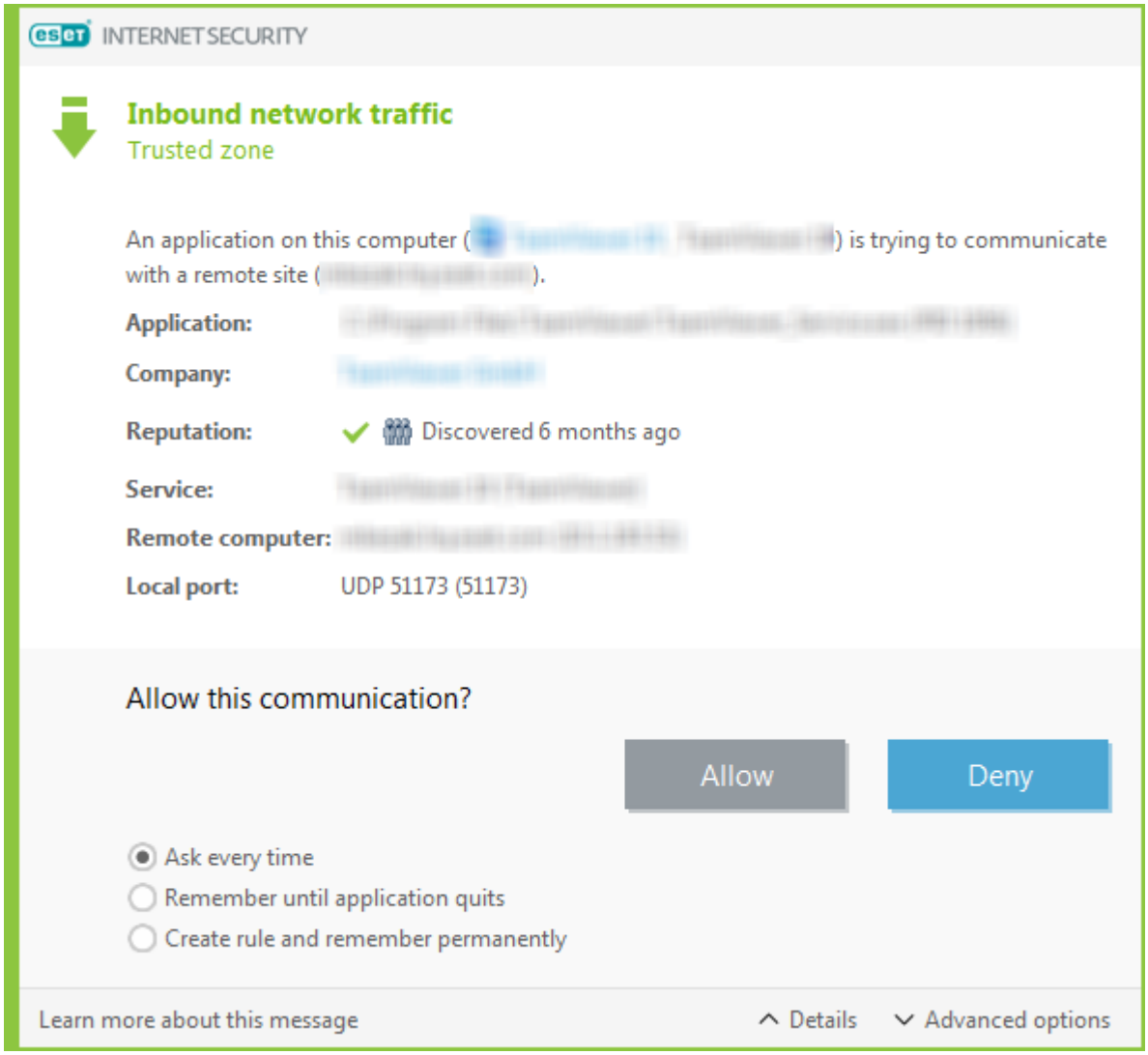
使用者定義的設定檔 – 您可以從下拉式功能表中選取您建立的設定檔之一。僅當您至少建立了一個自訂設定檔時，此選項才可用。

⚠ 不正確的網路配置可能會對電腦造成安全風險。

建立連線 – 偵測

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

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



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

應用程式 – 可執行檔的位置和處理程序識別碼。不允許與不明應用程式和處理程序連線。

簽章者 – 應用程式的發行者名稱。按一下文字以顯示公司的安全性憑證。

聲譽 – 連線的風險層級。為連線指派風險層級：良好（綠色）、未知（橙色）或危險（紅色），其透過使用一系列啟發式規則來檢查每個連線的特性、使用者數目及探索時間。此資訊是由 ESET LiveGrid® 技術收集。

服務 – 如果應用程式是 Windows 服務，則為服務的名稱。

遠端電腦 – 遠端裝置的位址。僅允許連線到受信任的已知位址。

遠端連接埠 – 通訊連接埠。在正常情況下，可允許一般連接埠上的通訊（如 Web 流量 – 連接埠號碼 80, 443）。

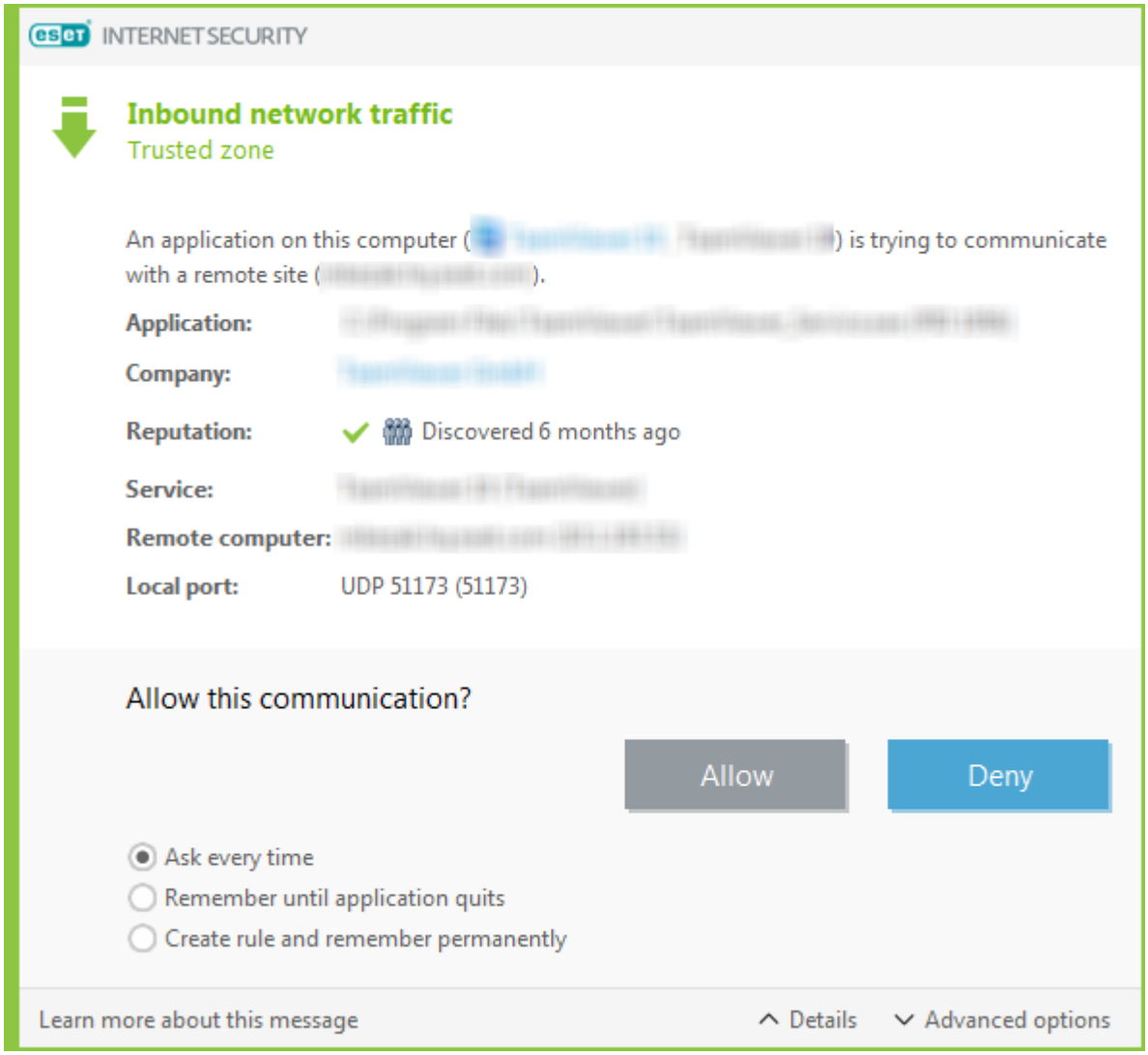
電腦入侵通常會使用網際網路及隱藏的連線來協助它們感染遠端系統。如果正確地配置規則，則防火牆會成為防護多種惡意程式碼攻擊的有用工具。

應用程式變更

防火牆已偵測到用於從電腦建立對外連線的應用程式中的修改。應用程式有可能只是已更新到新版本。另一方面，惡意的應用程式可能導致修改。如果您不清楚任何合法修改，我們建議您拒絕連線並使用最新的病毒資料庫掃描您的電腦。

對內的受信任通訊

信任區域內對內連線的範例：
來自信任區域內的遠端電腦正在嘗試與電腦上執行中的本機應用程式建立通訊。



應用程式 – 由遠端裝置連絡的應用程式。

應用程式路徑 – 應用程式的位置。

Microsoft store 應用程式 - Microsoft store 中應用程式的名稱。

簽章者 – 應用程式的發行者名稱。按一下文字以顯示公司的安全性憑證。

聲譽 – ESET LiveGrid® 技術所取得的應用程式聲譽。

[服務] – 目前正在您電腦上執行的服務名稱。

遠端電腦 – 正在嘗試與電腦上應用程式建立通訊的遠端電腦。

遠端連接埠 – 用於通訊的連接埠。

[每次都詢問] – 若規則的預設處理方法已設定為 **[詢問]**，每次觸發規則時都會出現對話方塊視窗。

[直到結束應用程式之前都會記住] – ESET Internet Security 將記住所選的處理方法，直到下次重新啟動為止。

[建立規則並永久記住規則] – 如果在允許或拒絕通訊之前選取此選項，則 ESET Internet Security 會記憶該處理方法，並在遠端電腦重新連絡應用程式時使用該處理方法。

允許 – 允許對內通訊。

拒絕 – 拒絕對內通訊。

編輯規則 – 可讓您使用防火牆規則編輯器自訂規則屬性。

對外的受信任通訊

信任區域內對外連線的範例：
正在嘗試與區域網路內，或信任區域中網路內另一台電腦建立連線的本機應用程式。

應用程式 – 由遠端裝置連絡的應用程式。

應用程式路徑 – 應用程式的位置。

Microsoft store 應用程式 - Microsoft store 中應用程式的名稱。

簽章者 – 應用程式的發行者名稱。按一下文字以顯示公司的安全性憑證。

聲譽 – ESET LiveGrid® 技術所取得的應用程式聲譽。

[服務] – 目前正在您電腦上執行的服務名稱。

遠端電腦 – 正在嘗試與電腦上應用程式建立通訊的遠端電腦。

遠端連接埠 – 用於通訊的連接埠。

[每次都詢問] – 若規則的預設處理方法已設定為 **[詢問]**，每次觸發規則時都會出現對話方塊視窗。

[直到結束應用程式之前都會記住] – ESET Internet Security 將記住所選的處理方法，直到下次重新啟動為止。

[建立規則並永久記住規則] – 如果在允許或拒絕通訊之前選取此選項，則 ESET Internet Security 會記憶該處理方法，並在遠端電腦重新連絡應用程式時使用該處理方法。

允許 – 允許對內通訊。

拒絕 – 拒絕對內通訊。

編輯規則 – 可讓您使用防火牆規則編輯器自訂規則屬性。

對內通訊

對內網際網路連線的範例：
正在嘗試與電腦上執行中應用程式進行通訊的遠端電腦。

應用程式 – 由遠端裝置連絡的應用程式。

應用程式路徑 – 應用程式的位置。

Microsoft store 應用程式 - Microsoft store 中應用程式的名稱。

簽章者 – 應用程式的發行者名稱。按一下文字以顯示公司的安全性憑證。

聲譽 – ESET LiveGrid® 技術所取得的應用程式聲譽。

[服務] – 目前正在您電腦上執行的服務名稱。

遠端電腦 – 正在嘗試與電腦上應用程式建立通訊的遠端電腦。

遠端連接埠 – 用於通訊的連接埠。

[每次都詢問] – 若規則的預設處理方法已設定為 **[詢問]**，每次觸發規則時都會出現對話方塊視窗。

[直到結束應用程式之前都會記住] – ESET Internet Security 將記住所選的處理方法，直到下次重新啟動為止。

[建立規則並永久記住規則] – 如果在允許或拒絕通訊之前選取此選項，則 ESET Internet Security 會記憶該處理方法，並在遠端電腦重新連絡應用程式時使用該處理方法。

允許 – 允許對內通訊。

拒絕 – 拒絕對內通訊。

編輯規則 – 可讓您使用防火牆規則編輯器自訂規則屬性。

對外通訊

對外網際網路連線的範例：
正在嘗試建立網際網路連線的本機應用程式。

應用程式 – 由遠端裝置連絡的應用程式。

應用程式路徑 – 應用程式的位置。

Microsoft store 應用程式 - Microsoft store 中應用程式的名稱。

簽章者 – 應用程式的發行者名稱。按一下文字以顯示公司的安全性憑證。

聲譽 – ESET LiveGrid® 技術所取得的應用程式聲譽。

[服務] – 目前正在您電腦上執行的服務名稱。

遠端電腦 – 正在嘗試與電腦上應用程式建立通訊的遠端電腦。

遠端連接埠 – 用於通訊的連接埠。

[每次都詢問] – 若規則的預設處理方法已設定為 **[詢問]**，每次觸發規則時都會出現對話方塊視窗。

[直到結束應用程式之前都會記住] – ESET Internet Security 將記住所選的處理方法，直到下次重新啟動為止。

[建立規則並永久記住規則] – 如果在允許或拒絕通訊之前選取此選項，則 ESET Internet Security 會記憶該處理方法，並在遠端電腦重新連絡應用程式時使用該處理方法。

允許 – 允許對內通訊。

拒絕 – 拒絕對內通訊。

編輯規則 – 可讓您使用防火牆規則編輯器自訂規則屬性。

連線視圖設定

以滑鼠右鍵按一下連線可查看其他選項，包括：

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

僅顯示 TCP 連線 – 清單僅顯示屬於 TCP 通訊協定組合的連線。

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

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

重新整理速度 – 選擇重新整理作用中連線的頻率。

立即重新整理 – 重新載入 **[網路連線]** 視窗。

安全性工具

開啟 [主程式視窗] > **[設定]** > **[安全性工具]** 以調整以下模組：

安全銀行與瀏覽 – 新增一層額外的保護，專為保護您線上交易期間的金融資料而設計。啟用安全銀行與瀏覽進階設定中的 **[保護所有瀏覽器]**，以在安全模式中啟動所有支援的 Web 瀏覽器。

瀏覽器隱私權與安全性—在不留下數位足跡的情況下，保持您線上活動的私密和安全。

Anti-Theft – 讓 防盜 在電腦遺失或遭竊時保護電腦。

安全銀行與瀏覽

安全銀行與瀏覽是一層額外的保護，專為保護您線上交易中的金融資料而設。

依預設，所有支援的Web瀏覽器都會從安全模式啟動。這可讓您自動在一個安全的瀏覽器中瀏覽網際網路、存取網際網路銀行，以及進行線上購買和交易。

必須啟用 ESET LiveGrid® 信譽系統（依預設啟用），才能確保「安全銀行與瀏覽」正常運作。

若要配置安全的瀏覽器行為，請參閱安全銀行與瀏覽進階設定。如果停用 **[保護所有瀏覽器]**，則可以在主要程序視窗 > **[概觀]** > **[安全銀行與瀏覽]** 中或按一下 **[安全銀行與瀏覽]** 桌面圖示，來存取安全的瀏覽器。在 Windows 中設為預設的瀏覽器會在安全模式中啟動。

執行受保護的瀏覽必須使用 HTTPS 加密通訊。以下瀏覽器支援「安全銀行與瀏覽」：

- Internet Explorer 8.0.0.0+
- Microsoft Edge 83.0.0.0+
- Google Chrome 64.0.0.0+
- Firefox 24.0.0.0+

僅支援搭載 ARM 處理器裝置上的 Firefox 和 Microsoft Edge

如需關於「安全銀行與瀏覽」功能的詳細資訊，請閱讀以下 ESET 知識庫文章（提供英文和數種其他語言版本）：

- 如何使用 ESET 安全銀行與瀏覽？
- 暫停或停用 ESET Windows 家用產品中的安全銀行與瀏覽
- ESET 安全銀行與瀏覽—常見錯誤
- ESET 詞彙表 | 安全銀行與瀏覽

瀏覽器內通知

安全的瀏覽器透過瀏覽器內通知和瀏覽器框架顏色，來告知其目前狀態。

瀏覽器內通知會顯示在右側的索引標籤中。

若要展開瀏覽器內通知，請按一下 ESET 圖示。若要將通知最小化，請按一下通知文字。若要隱藏通知和綠色瀏覽器框架，請按一下關閉圖示。

僅能隱藏資訊通知和綠色瀏覽器框架。

瀏覽器內通知

通知類型	狀態
資訊性通知與綠色瀏覽器框架	已確定有最大防護力，並預設將瀏覽器內通知最小化。展開瀏覽器內通知，然後按一下**[設定]**以開啟安全性工具設定。
警告和橙色瀏覽器框架	安全的瀏覽器需要您注意非嚴重問題。如需問題或解決方案的更多資訊，請遵循瀏覽器內通知中的指示。
安全性警告和紅色瀏覽器框架	此瀏覽器不受ESET 安全銀行與瀏覽」的保護。請重新啟動瀏覽器，以確保防護功能為作用中。若要解決與瀏覽器中載入之檔案的衝突，請開啟 [防護記錄檔案] > **[安全銀行與瀏覽]**，並確保下次啟動瀏覽器時不會載入已記錄的檔案。如果問題持續存在，請遵循我們知識庫文章中的指示，與 ESET 技術支援 連絡。

瀏覽器隱私權與安全性

您可以透過支援瀏覽器（僅限 Google ChromeMozilla Firefox 和 Microsoft Edge）上可用的自訂延伸模組，來啟用「瀏覽器隱私權與安全性」功能。

若要安裝並啟用延伸模組，請執行以下操作：

1. 確定您使用的是最新版 ESET Internet Security並在更新後成功重新啟動電腦。
2. 開啟您的瀏覽器。
3. 該延伸模組安裝在您的瀏覽器中。
4. 啟用延伸模組，畫面上會顯示帶有延伸模組詳細頁面的瀏覽器。

「瀏覽器隱私權與安全性」延伸模組的主要功能表分為以下幾個部分：

概觀

安全搜尋

按一下**[掃描搜尋結果]**旁邊的切換圖示 以啟用該功能，並查看可以安全地按一下哪些結果。安全搜尋會評估列出的連結位址，但不一定代表網站不包含惡意軟體。我們的偵測引擎接著會偵測網站上的惡意軟體。

瀏覽器清除

刪除瀏覽資料或設定定期清理。您可以新增您想要接受 Cookie 並在執行瀏覽器清除之後仍維持登入狀態的網站，方法是**將網站新增至清單**

• **一次性清除**—從下拉式功能表中選取時間範圍，以及要刪除的資料類型。您可以從選項中選擇所有資料、私有和自訂選擇。

• **定期清除**—按一下**[定期清除]旁邊的切換開關圖示** 可啟用該功能。 從下拉功能表中選取時間範圍，以及您要定期刪除的資料類型。您可以從選項中選擇所有資料、私有和自訂選擇。

[自訂資料]選項包含以下類別：

- 瀏覽歷程
- 下載歷程

- Cookie 和網站資料
- 快取的映像和檔案
- 密碼和登入資料
- 表單自動填滿資料

網站設定檢閱

輕鬆地存取和管理網站權限，以控制網站可以使用的資訊內容。

- **通知**—檢閱您想要［**允許/阻止**］通知的網站，或者您是否希望瀏覽器延伸模組每次都［**詢問**］您。

進階設定

瀏覽器清除

進階 Cookie 設定

您想要接受 Cookie 並在執行瀏覽器清除之後仍維持登入狀態的網站清單。在文字欄位中輸入 URL 位址，然後按一下［**新增**］。您可以隨時按下一下特定網站旁邊的減號圖示  ，將其從清單中移除。

頁面底部是瀏覽器中目前開啟的建議網域清單。如果您看不到特定網站，請按一下［**重新整理清單**］，然後按一下加號圖示  ，將其新增到已接受 Cookie 清單中。

網站設定檢閱

輕鬆地存取和管理網站權限，以控制網站可以使用的資訊內容。

- **通知**—檢閱您想要［**允許/阻止**］通知的網站，或者您是否希望瀏覽器延伸模組每次都［**詢問**］您。

外觀

自訂介面的色彩配置以配合您的喜好。您可以透過選取［**淺色**］或［**深色**］核取方塊，來選擇偏好的色彩配置。

防盜

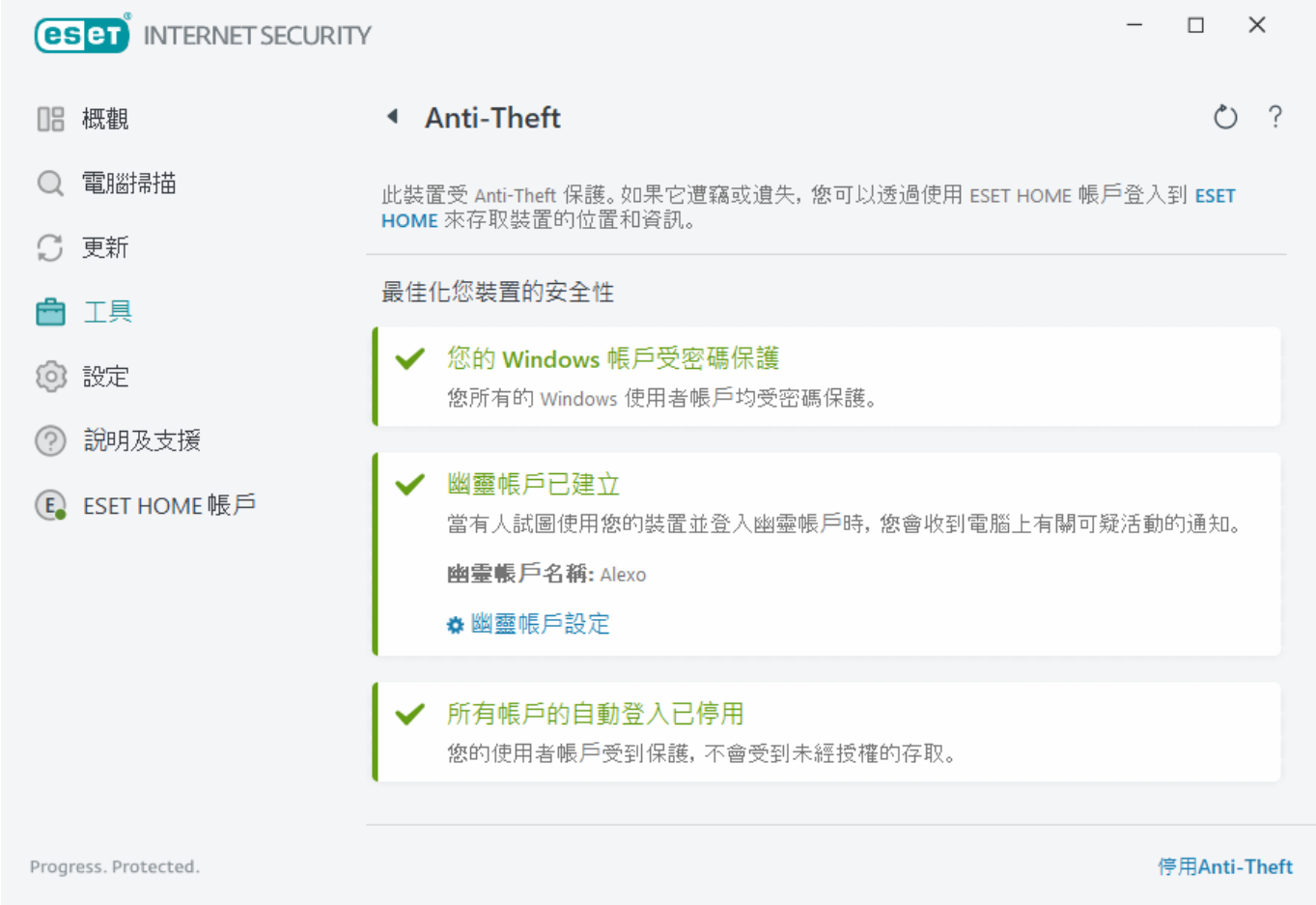
每日從家裏到工作或其他公共場所的過程中，個人裝置一直都存在著遺失或遭竊的風險。防盜 這項功能可在裝置遺失或遭竊時擴展使用者層級安全性。防盜 可讓您監控裝置的使用情況，並在 ESET HOME 中使用依 IP 位址定位的功能追蹤遺失的裝置，協助您取回裝置及保護個人資料。

透過地理 IP 位址查閱、網路攝影機影像擷取、使用者帳戶防護，以及裝置監控等現代科技，防盜 能協助您和執法機構找到遺失或遭竊的電腦或裝置。在 ESET HOME 中，您可以看見電腦或裝置上發生哪些活動。

若要深入瞭解 ESET HOME 中的 防盜，請參閱 ESET HOME 線上說明

由於使用者帳戶管理中的限制，防盜 可能無法在網域中的電腦上正常運作。

啟用 防盜 後，您可以在［主程式視窗］> [**設定**] > [**安全性工具**] > [**防盜**］中，最佳化裝置的安全性。



最佳化選項

幽靈帳戶未建立

建立「幽靈帳戶」可增加定位遺失或被遭竊裝置的機會。如果您將裝置標記為遺失，則 防盜 將封鎖存取您的作用中使用者帳戶，以保護您的敏感資料。任何嘗試使用該裝置的人將僅允許使用幽靈帳戶。幽靈帳戶是一種權限有限的來賓帳戶。它將作為預設系統帳戶，直到您的裝置標記為復原為止 – 防止任何人登入其他使用者帳戶或存取使用者的資料。

當您的電腦在正常狀態時，只要有人登入幽靈帳戶，系統就會以電子郵件通知您，並提供電腦上可疑活動的相關資訊。收到電子郵件通知後，您可以決定是否要將電腦標記為遺失。

若要建立幽靈帳戶，請按一下 **[建立幽靈帳戶]**，在文字欄位中輸入 **[幽靈帳戶名稱]**，然後按一下 **[建立]**。

建立幽靈帳戶後，按一下 **[幽靈帳戶設定]** 可將帳戶重新命名或刪除。

Windows 帳戶密碼防護

您的使用者帳戶未受密碼保護。如果至少一個使用者帳戶未受到密碼保護，您將收到此最佳化警告。為電腦上的所有使用者（**[幽靈]** 帳戶除外）建立密碼可解決此問題。

若要為使用者帳戶建立密碼，請按一下 **[管理 Windows 帳戶]**，然後變更密碼或依照下方指示進行：

1. 按下鍵盤上的 CTRL+Alt+Delete。
2. 按一下 **[變更密碼]**。

3. 將［**舊密碼**］欄位保留空白。

4. 在［**新密碼**］和［**確認密碼**］欄位中輸入密碼，然後按下 **Enter**。

Windows 帳戶的自動登入

您的使用者帳戶已啟用自動登入；因此，無法保護您的帳戶免遭未經授權的存取。如果至少一個使用者帳戶已啟用自動登入，您將收到此最佳化警告。按一下［**停用自動登入**］以解決此最佳化問題。

幽靈帳戶的自動登入

已啟用您裝置上**幽靈帳戶**的自動登入。當裝置在正常狀態時，不建議您使用自動登入，因為可能會在您存取真正使用者帳戶時造成問題，或傳送有關電腦遺失狀態的錯誤警示。按一下［**停用自動登入**］以解決此最佳化問題。

登入您的 ESET HOME 帳戶

若要在 ESET HOME 中啟用/停用 防盜 及存取裝置位置與資訊，請登入您的 ESET HOME 帳戶。

有幾種方法可用來登入您的 ESET HOME 帳戶：

- ［**使用您的 ESET HOME 電子郵件地址和密碼**］ – 輸入您用來建立 ESET HOME 帳戶的［**電子郵件地址**］和［**密碼**］，然後按一下［**登入**］。

- ［**使用您的 Google 帳戶/AppleID**］ – 按一下［**繼續使用 Google**］或［**繼續使用 Apple**］以登入適當帳戶。成功登入後，系統會將您重新導向至 ESET HOME 確認網頁。若要繼續，請切換回 ESET 產品視窗。如需關於 Google 帳戶/AppleID 登入的詳細資訊，請參閱 ESET HOME 線上說明中的指示。

- ［**掃描 QR 代碼**］ – 按一下［**掃描 QR 代碼**］以顯示 QR 代碼。開啟您的 ESET HOME 行動應用程式並

掃描 QR 代碼，或將您的裝置相機指向 QR 代碼。如需詳細資訊，請參閱 ESET HOME 線上說明中的指示。

登入失敗 – 常見錯誤

如果您沒有 ESET HOME 帳戶，請按一下 **[建立帳戶]** 以註冊或查看 ESET HOME 線上說明中的指示。若您忘記密碼，按一下 **[我忘記密碼]**，並遵循畫面上的步驟或查看 ESET HOME 線上說明中的指示。

防盜 不支援 Microsoft Windows Home Server

設定裝置名稱

[裝置名稱] 欄位代表電腦（裝置）的名稱，此名稱將在所有 ESET HOME 服務中作為識別碼顯示。預設是使用您電腦的電腦名稱。輸入裝置名稱或使用預設名稱，然後按一下 **[繼續]**。

防盜 已啟用/已停用

當您啟用/停用 防盜 時，此視窗包含確認訊息：

- 已啟用 – 您的裝置現在受到 防盜 的保護，您可以使用您的帳戶在 ESET HOME 入口網站上遠端管理其安全性。
- 已停用 – 此裝置上的 防盜 已停用，且與此裝置的 <%ESET_ANTTHEFT%> 相關的所有資料皆會從 ESET HOME 入口網站中移除。

新增裝置失敗

啟動 防盜 時發生錯誤。

最常見的情況為：

- 登入 ESET HOME 時發生錯誤
- 無網際網路連線（或網際網路目前無法運作）

如果無法解決此問題，請連絡 ESET 技術支援。

匯入及匯出設定

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

圖解指示
請參閱使用 .xml 檔案匯入或匯出 ESET 配置設定圖解指示（以英文和其他數種語言提供）。

如果您必須備份 ESET Internet Security 的目前配置以供日後使用，匯入與匯出配置檔案功能則十分有用。當您想要在多個系統上使用慣用配置時，匯出設定選項也很方便。您可以匯入 .xml 檔案以傳輸這些設定。

若要匯入配置，請在主要程式視窗中，按一下 **[設定]** > **[匯入/匯出設定]**，然後選取 **[匯入設定]**。輸入配置檔案名稱，或按一下 **[...]** 按鈕以瀏覽您要匯入的配置檔案。

若要匯出配置，請在主要程式視窗中，按一下 **[設定] > [匯入/匯出設定]**。選取 **[匯出設定]**，然後輸入包含名稱的完整檔案路徑。按一下 **...** 以瀏覽至您電腦上儲存配置檔案的位置。

如果您沒有足夠的權限將匯出檔案寫入指定目錄，則可能會在匯出設定時遭遇錯誤。

說明及支援

按一下主程式視窗中的 **[說明及支援]** 以顯示支援資訊和疑難排解工具，它們可協助您解決可能遇到的問題。

訂閱

- 訂閱疑難排解—按一下此連結以尋找啟動或訂閱變更問題的解決方案。
- 變更訂閱 – 按一下以啟動 [啟動] 視窗，並啟動您的產品。如果您的裝置連線至 ESET HOME，請從您的 ESET HOME 帳戶選擇訂閱，或新增一個新授權。

已安裝的產品

- [新增功能] – 按一下此處以開啟關於全新及增強功能的資訊視窗。
- [關於 ESET Internet Security] – 顯示 ESET Internet Security 副本的相關資訊。
- 產品疑難排解 – 按一下此連結以尋找大多數常見問題的解決方案。
- **變更產品** – 按一下這裡以查看是否能以目前訂閱，將 ESET Internet Security 變更為不同的產品系列

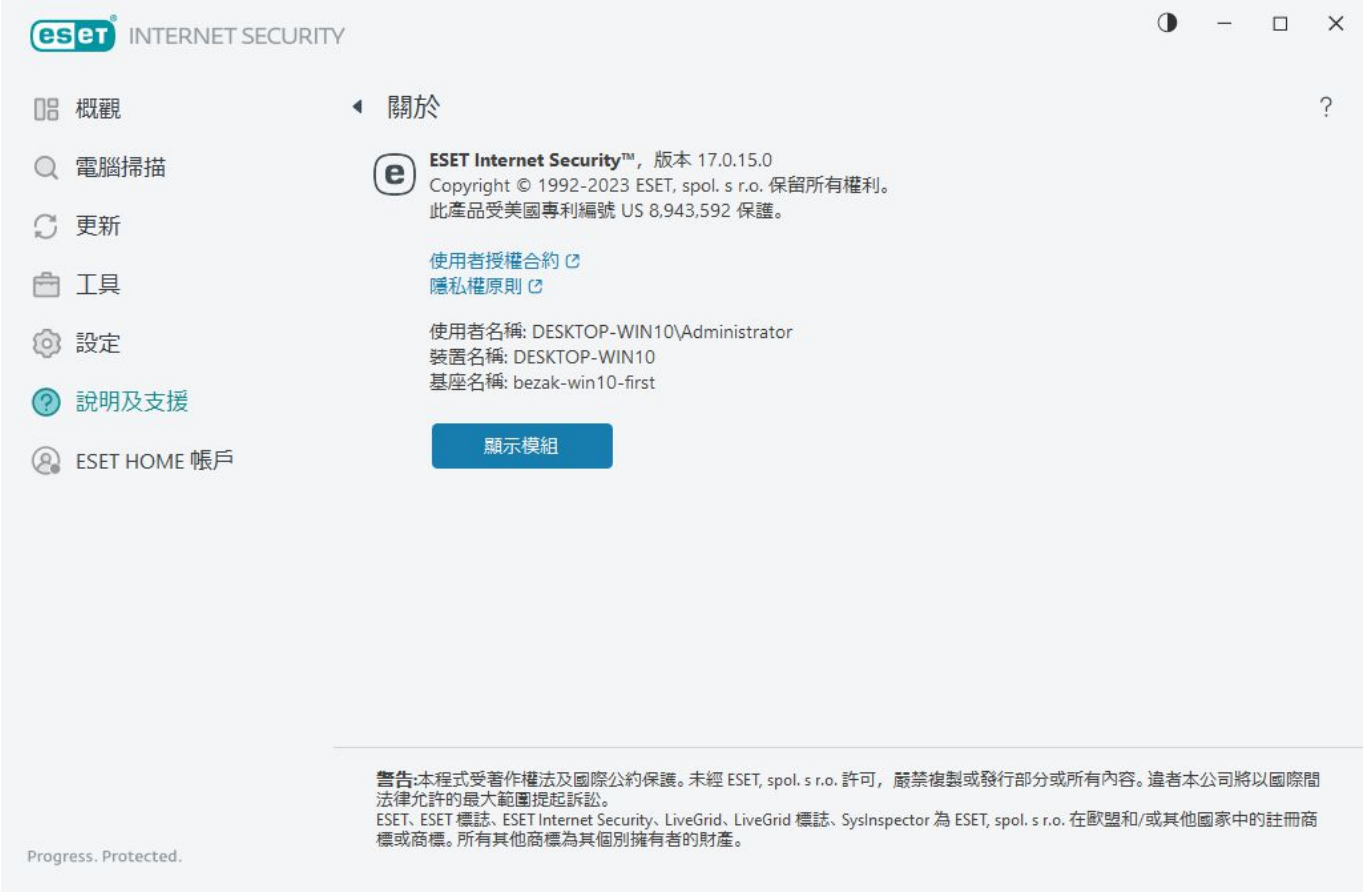
說明頁面 – 按一下此連結以啟動 ESET Internet Security 說明頁面。

技術支援

[**知識庫**] – ESET 知識庫包含常見問題的解答，以及各種問題的建議解決方案。ESET 技術專家會定期更新知識庫，使其成為解決各種問題的最強工具。

關於 ESET Internet Security

此視窗會提供已安裝的 ESET Internet Security 版本和電腦相關的詳細資料。



按一下［**顯示模組**］以查看已載入程式模組清單的相關資訊。

- 按一下［**複製**］便能將模組相關資訊複製到剪貼簿。這在疑難排解或聯繫技術支援時可能有用。
- 按一下［模組］視窗中的［**偵測引擎**］，以開啟 ESET 病毒雷達，該雷達包含每一版 ESET 偵測引擎的相關資訊。

ESET 最新消息

在此視窗中，ESET Internet Security 會定期通知您 ESET 最新消息。

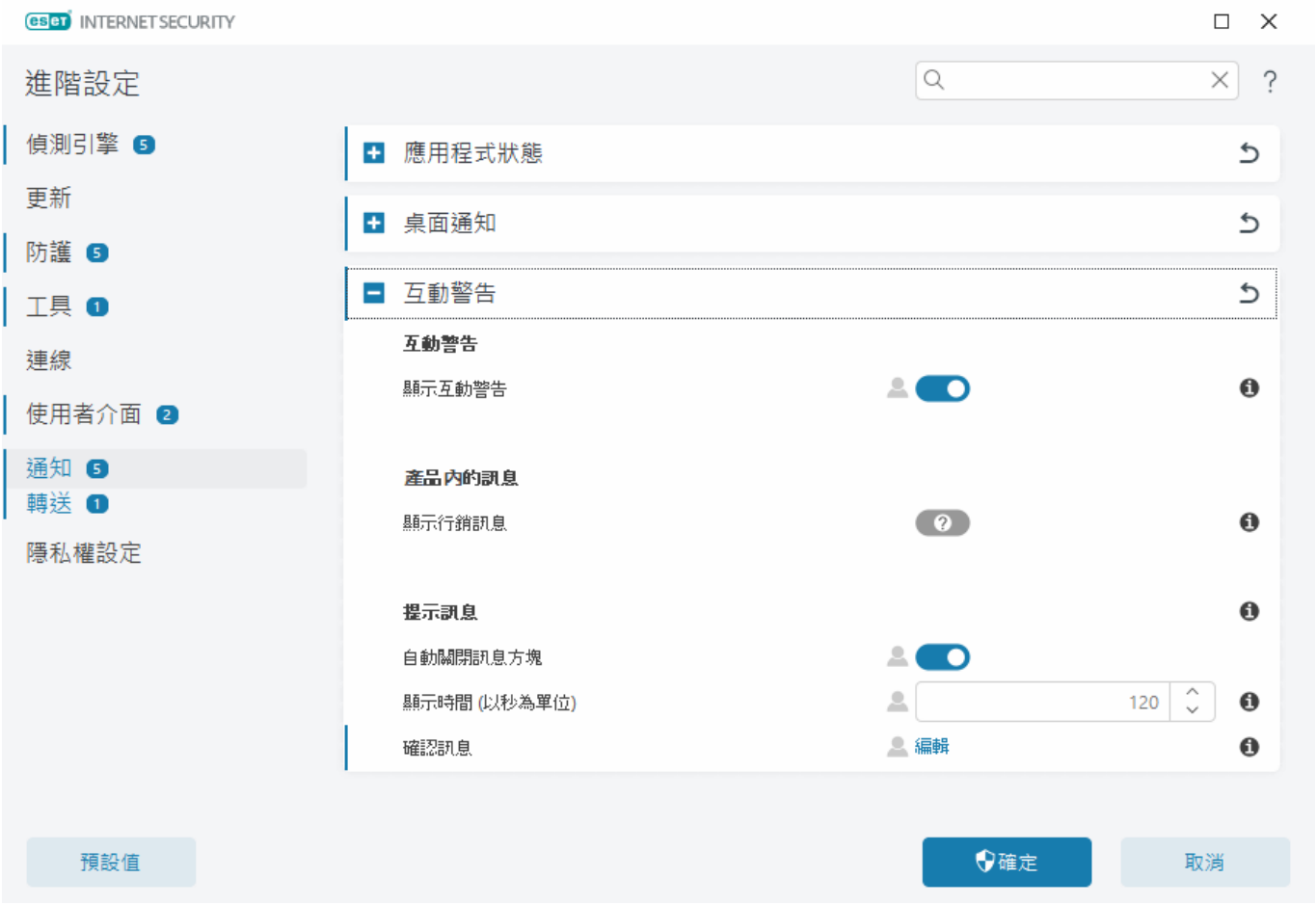
產品內訊息的設計是為了通知使用者ESET的最新消息與其他通訊。傳送行銷訊息需取得使用者同意。因此，行銷訊息預設不會傳送給使用者（顯示為問號）。啟用此選項代表您同意收到 ESET 行銷訊息。如果您不想收到 ESET 行銷資料，請停用［**顯示行銷訊息**］選項。

若要啟用或停用透過通知視窗接收行銷訊息，請遵循以下指示進行。

1. 開啟進階設定。

2. 按一下 **[通知] > [互動式警示]**。

3. 修改 **[顯示行銷訊息]** 選項。



提交系統配置資料

為盡可能快速準確的提供協助，ESET 需要 ESET Internet Security 配置相關的資訊、系統和處理程序的詳細資訊（ESET SysInspector 防護記錄檔案）和登錄資料。ESET 將僅使用這些資料向客戶提供技術協助。

提交 Web 表單後，您的系統配置資料會傳送至 ESET。如果您要記住此處理程序的此動作，請選取 **[永遠提交此資訊]**。若要提交 Web 表單，而不傳送任何資料，請按一下 **[不提交資料]** 並繼續。

您可以在 [進階設定] > **[工具]** > **[診斷]** > [技術支援] 中配置系統配置資料的提交。

> 如果您已決定提交系統配置資料，則必須填寫並提交 Web 表單。否則，將不會建立您的票證，並且您的系統配置資料將遺失。如果無法提交系統配置資料，請填寫 Web 表單並等待來自技術支援的說明。

技術支援

在主程式視窗中，按一下 **[說明及支援] > [技術支援]**。

連絡技術支援

請求支援 – 如果您找不到問題的答案，可以使用位於 ESET 網站上的這個表單，快速地連絡 ESET 技術支援部門。根據您的設定，在填寫此網頁表單之前會顯示提交您的系統配置資料視窗。

取得技術支援的相關資訊

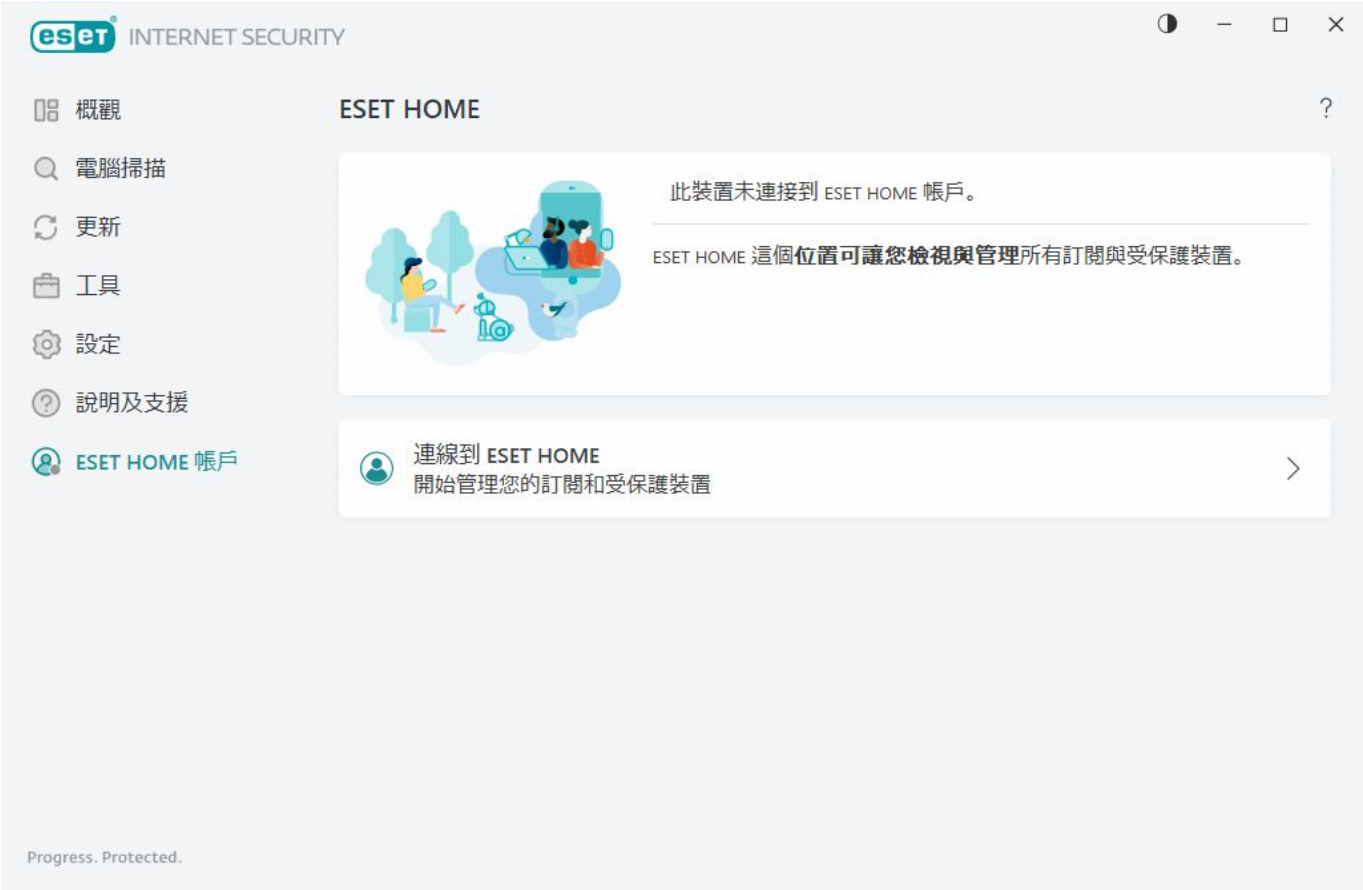
技術支援詳細資料 – 看到提示時，您可以複製資訊並傳送至 ESET 技術支援（例如訂閱詳細資料、產品名稱、產品版本、作業系統和電腦資訊）。

ESET Log Collector – 可連結至 ESET 知識庫文章，讓您在其中下載可自動收集電腦的資訊和防護記錄的 ESET Log Collector 應用程式，以便協助更快速解決問題。如需詳細資訊，請參閱 ESET Log Collector 線上使用者手冊。

啟用［進階防護記錄］以針對所有可用功能建立進階防護記錄，協助開發人員診斷並解決問題。記錄最簡化設定為［**診斷**］層級。進階記錄會在兩小時後自動停用，除非您按下［**停止進階記錄**］提早予以停止。所有防護記錄皆已建立時，系統會顯示通知視窗，提供您直接存取內含已建立防護記錄的診斷資料夾。

ESET HOME 帳戶

您可以在主要程式視窗 > **[ESET HOME 帳戶]** 中檢閱 ESET HOME 帳戶連線狀態。



此裝置未連接到 ESET HOME 帳戶

按一下連接到 ESET HOME 以將裝置連接到 ESET HOME 並管理您的訂閱和受保護的裝置。您可以續約、升級或延長訂閱，並檢視重要的詳細資訊。在 ESET HOME 管理入口網站或行動應用程式中，您可以新增不同

訂閱、下載產品至您的裝置、檢查產品安全性狀態，或透過電子郵件共用訂閱。如需詳細資訊，請造訪 ESET HOME 線上說明

此裝置已連接到 ESET HOME 帳戶

您可以使用 ESET HOME 入口網站或行動應用程式遠端管理裝置的安全性。按一下 **App Store** 或 **Google Play** 以顯示可以使用行動手機掃描的 QR 代碼，以從 App Store 或 Google Play 下載 ESET HOME 行動應用程式。

[ESET HOME 帳戶]—您的 ESET HOME 帳戶名稱。

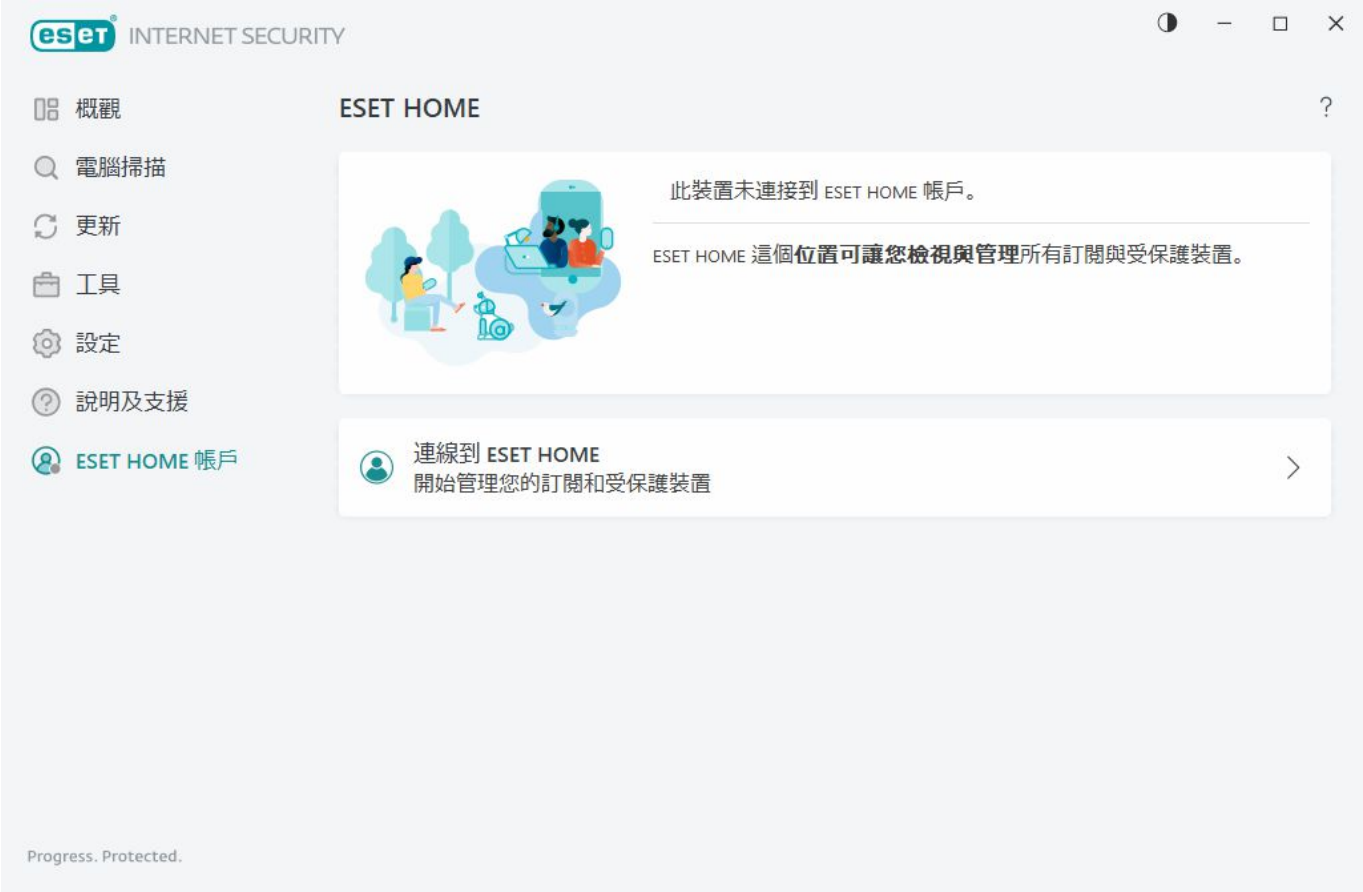
[裝置名稱]—在 ESET HOME 帳戶中顯示此裝置的名稱。

[開啟 ESET HOME]—開啟 ESET HOME 管理入口網站。

若要將裝置與 ESET HOME 帳戶斷開連接，按一下 **[從 ESET HOME 中斷連線] > [中斷連線]**。用於啟動的訂閱仍處於作用中，並且您的裝置將受到保護。

連線到 ESET HOME

將您的裝置連線到 ESET HOME 以檢視和管理您所有啟動的 ESET 訂閱和裝置。您可以續約、升級或延長訂閱，並檢視重要的訂閱詳細資訊。在 ESET HOME 管理入口網站或行動應用程式中，您可以新增不同訂閱、下載產品至您的裝置、檢查產品安全性狀態，或透過電子郵件共用訂閱。如需詳細資訊，請造訪 ESET HOME 線上說明



將您的裝置連線至 ESET HOME:

如果您在安裝期間或選取［**使用 ESET HOME 帳戶**］為啟動方法時，連線至 ESET HOME，請依照使用 ESET HOME 帳戶主題中的指示進行。
如果您已安裝 ESET Internet Security 並使用您 ESET HOME 帳戶中新增的訂閱加以啟動，您可以使用 ESET HOME 入口網站將裝置連線到 ESET HOME，請遵循 ESET HOME 線上說明指南中的指示並允許 ESET Internet Security 中的連線。

1. 在主要程式視窗中，按一下［**ESET HOME 帳戶**］>［**連線到 ESET HOME**］，或在［**將此裝置連線到 ESET HOME** 帳戶］通知中，按一下［**連線到 ESET HOME**］。

2. 登入您的 ESET HOME 帳戶。

如果您沒有 ESET HOME 帳戶，請按一下［**建立帳戶**］以註冊或查看 ESET HOME 線上說明中的指示。
若您忘記密碼，按一下［**我忘記密碼**］，並遵循畫面上的步驟或查看 ESET HOME 線上說明中的指示。

3. 設定［**裝置名稱**］，然後按一下［**繼續**］。

4. 連線成功後，隨即顯示詳細資訊視窗。按一下［**完成**］。

登入 ESET HOME

有幾種方法可用來登入您的 ESET HOME 帳戶：

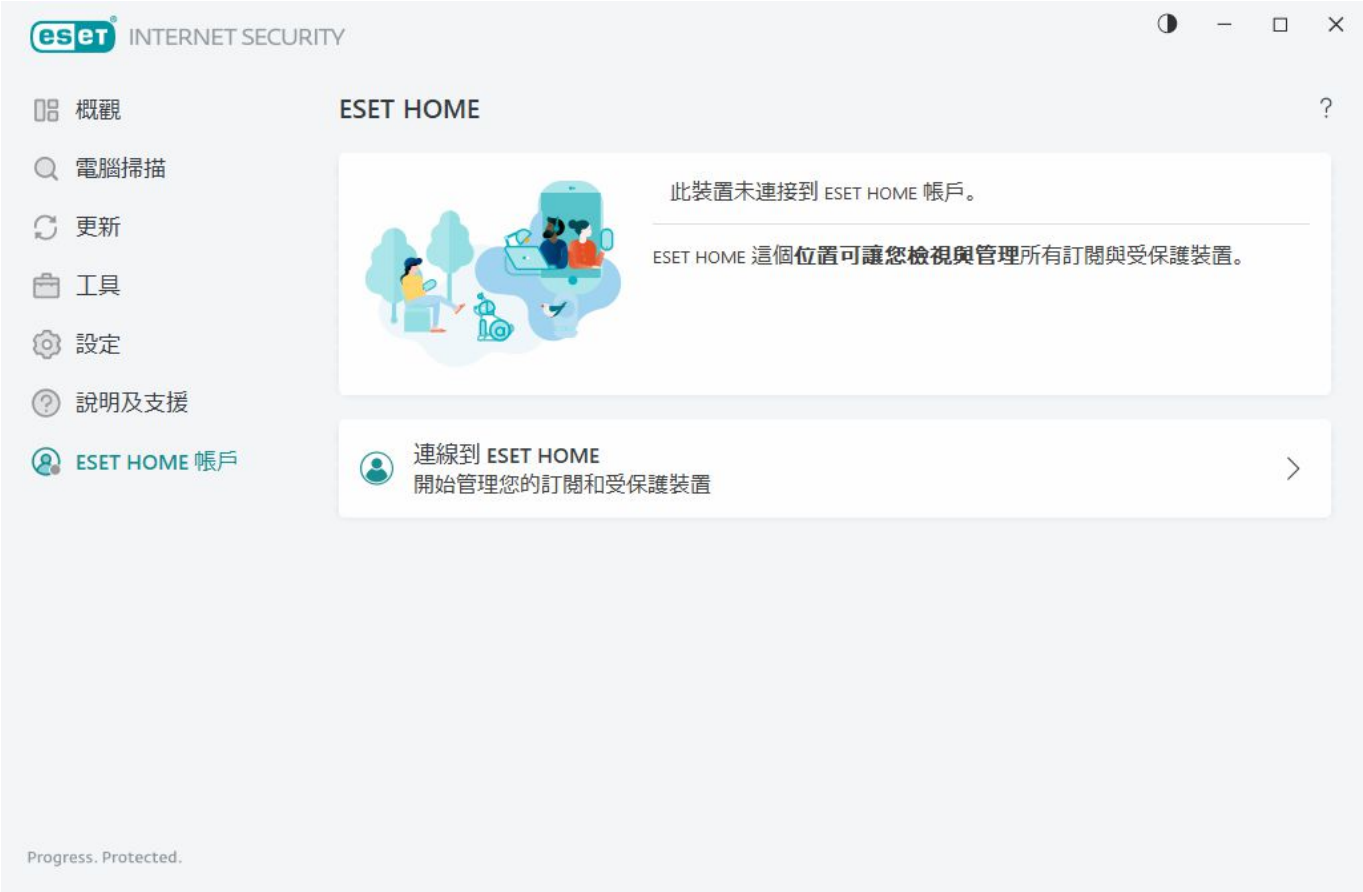
- ［**使用您的 ESET HOME 電子郵件地址和密碼**］ – 輸入您用來建立 ESET HOME 帳戶的［**電子郵件地址**］和［**密碼**］，然後按一下［**登入**］。

- ［**使用您的 Google 帳戶/AppleID**］ – 按一下［**繼續使用 Google**］或［**繼續使用 Apple**］以登入適當帳戶。成功登入後，系統會將您重新導向至 ESET HOME 確認網頁。若要繼續，請切換回 ESET 產品視窗。如需關於 Google 帳戶/AppleID 登入的詳細資訊，請參閱 ESET HOME 線上說明中的指示。

- ［**掃描 QR 代碼**］ – 按一下［**掃描 QR 代碼**］以顯示 QR 代碼。開啟您的 ESET HOME 行動應用程式並掃描 QR 代碼，或將您的裝置相機指向 QR 代碼。如需詳細資訊，請參閱 ESET HOME 線上說明中的指示。

如果您沒有 ESET HOME 帳戶，請按一下［**建立帳戶**］以註冊或查看 ESET HOME 線上說明中的指示。
若您忘記密碼，按一下［**我忘記密碼**］，並遵循畫面上的步驟或查看 ESET HOME 線上說明中的指示。

登入失敗 – 常見錯誤



登入失敗 – 常見錯誤

我們找不到與輸入的電子郵件地址相符的帳戶

您輸入的電子郵件地址不符合任何 ESET HOME 帳戶。按一下 **[返回]**，然後輸入正確的電子郵件地址和密碼。

如需登入，您必須建立 ESET HOME 帳戶。如果您沒有 ESET HOME 帳戶，請按一下 **[上一步] > [建立帳戶]** 或查看建立新的 ESET HOME 帳戶

使用者名稱和密碼不相符

輸入的密碼不符合輸入的電子郵件地址。按一下 **[返回]**，輸入正確的密碼並驗證輸入的電子郵件地址是否正確。若您仍無法登入，請按一下 **[上一步] > [我忘記密碼]** 來重設您的密碼，並遵循畫面上的步驟或查看我忘記 ESET HOME 密碼

選取的登入選項不符合您的帳戶

您的帳戶已連結至社交媒體帳戶。若要登入 ESET HOME請按一下 **[繼續使用 Google]** 或 **[繼續使用 Apple]** 以登入正確的帳戶。成功登入後，系統會將您重新導向至 ESET HOME 確認網頁。您可以在 ESET HOME 入口網站上，將您的社交媒體帳戶與 ESET HOME 帳戶中斷連線。

密碼不正確

若您的 ESET Internet Security 已經連線到 ESET HOME且您所做的變更要求您登入（例如，停用 Anti-Theft）而您輸入的密碼不符合您的帳戶，就會發生此錯誤。按一下 **[返回]** 並輸入正確的密碼。若您仍無法登入，

請按一下［**上一步**］>［**我忘記密碼**］來重設您的密碼，並遵循畫面上的步驟或查看我忘記 ESET HOME 密碼。

在 ESET HOME 中新增裝置

如果您已安裝 ESET Internet Security 並使用您 ESET HOME 帳戶中新增的訂閱加以啟動，您可以使用 ESET HOME 入口網站將裝置連線到 ESET HOME。

1. 向您的裝置傳送連線要求。

2. ESET Internet Security 會顯示［**將此裝置連線到 ESET HOME 帳戶**］對話方塊視窗，並包含 ESET HOME 帳戶名稱。按一下［**允許**］將裝置連線到先前提過的 ESET HOME 帳戶。

如果沒有互動，將在大約 30 分鐘後自動取消連線要求。

進階設定

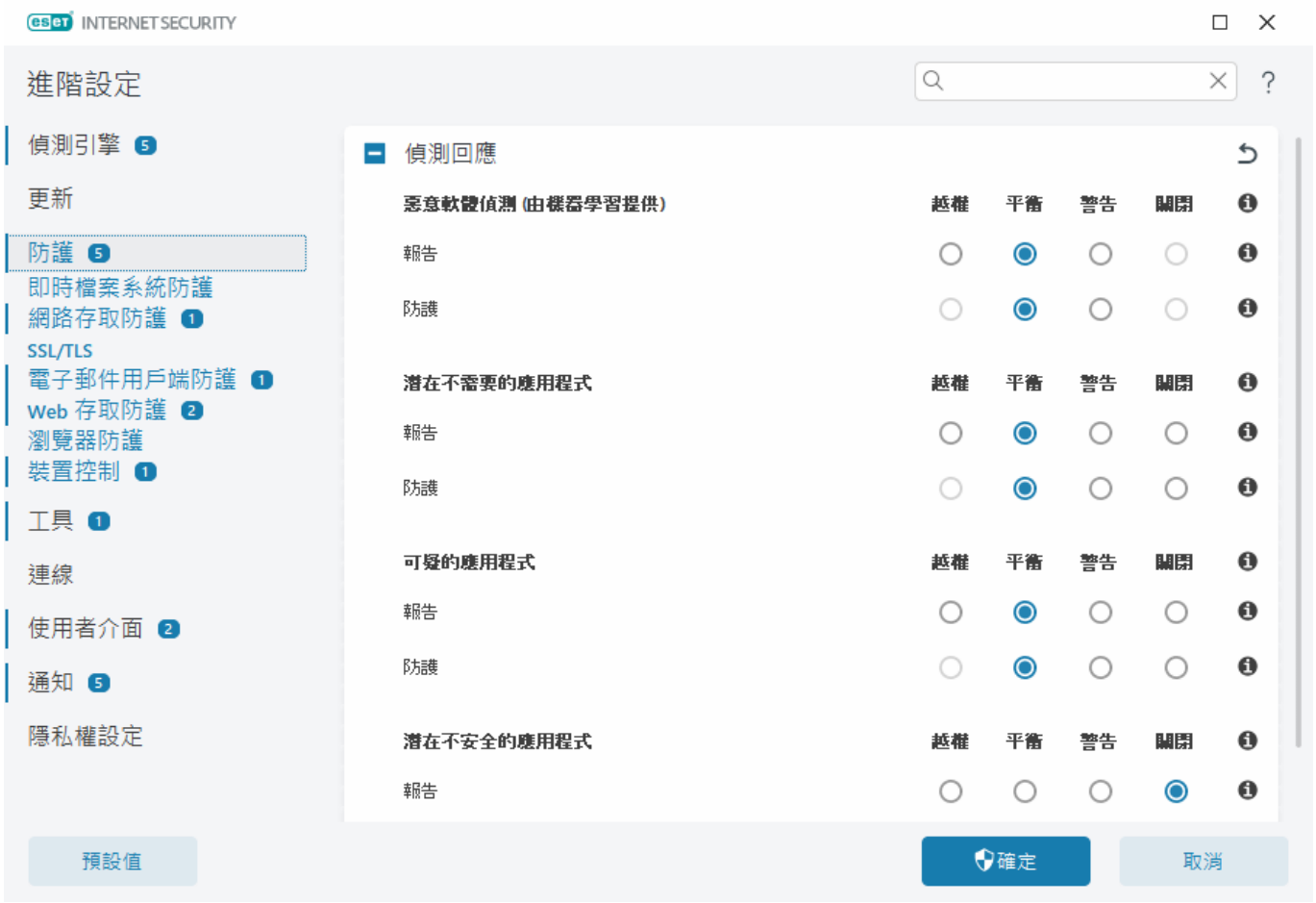
進階設定可讓您配置詳細 ESET Internet Security 設定以滿足您的需求。

若要開啟進階設定，請開啟主程式視窗，然後按鍵盤上的 **[F5]** 鍵或按一下［**設定**］>［**進階設定**］。

根據您的存取設定，系統可能會提示您鍵入密碼以開啟進階設定。

在進階設定中，您可以配置以下設定：

- 偵側引擎
- 更新
- 防護
- 工具
- 連線
- 使用者介面
- 通知
- 隱私權設定



偵側引擎

[進階設定] > **[偵測引擎]** 使您能夠配置以下選項：

- 排除
- 進階選項
- 網路流量掃描器

排除

[排除] 可讓您從偵測擎中排除物件。為確保所有物件進行掃描，我們建議您只有在絕對必要時建立排除。在可能需要排除物件的情況下，可能包括掃描大型資料庫項目，這會在掃描期間降低電腦速度的物件，或包括與掃描發生衝突的軟體。

效能排除 – 從掃描中排除檔案和資料夾。效能排除有助於排除遊戲應用程式的檔案層級掃描，或在導致系統行為異常或效能提升時有所幫助。

偵測排除可讓您使用偵測名稱、路徑或其雜湊，從偵測中排除物件。與效能排除相同，偵測排除不會從掃描中排除檔案和資料夾。只在偵測引擎偵測到物件，而且排除清單中有適當的規則時，偵測排除才會排除這些物件。

不要與其他排除類型混淆：

- 程序排除 – 所有歸因於排除的應用程式程序的檔案作業會從掃描中排除（可能需要改善備份速度

和服務可用性)。

- 排除的副檔名
- HIPS 排除
- 適用於雲端型防護的排除過濾器

效能排除

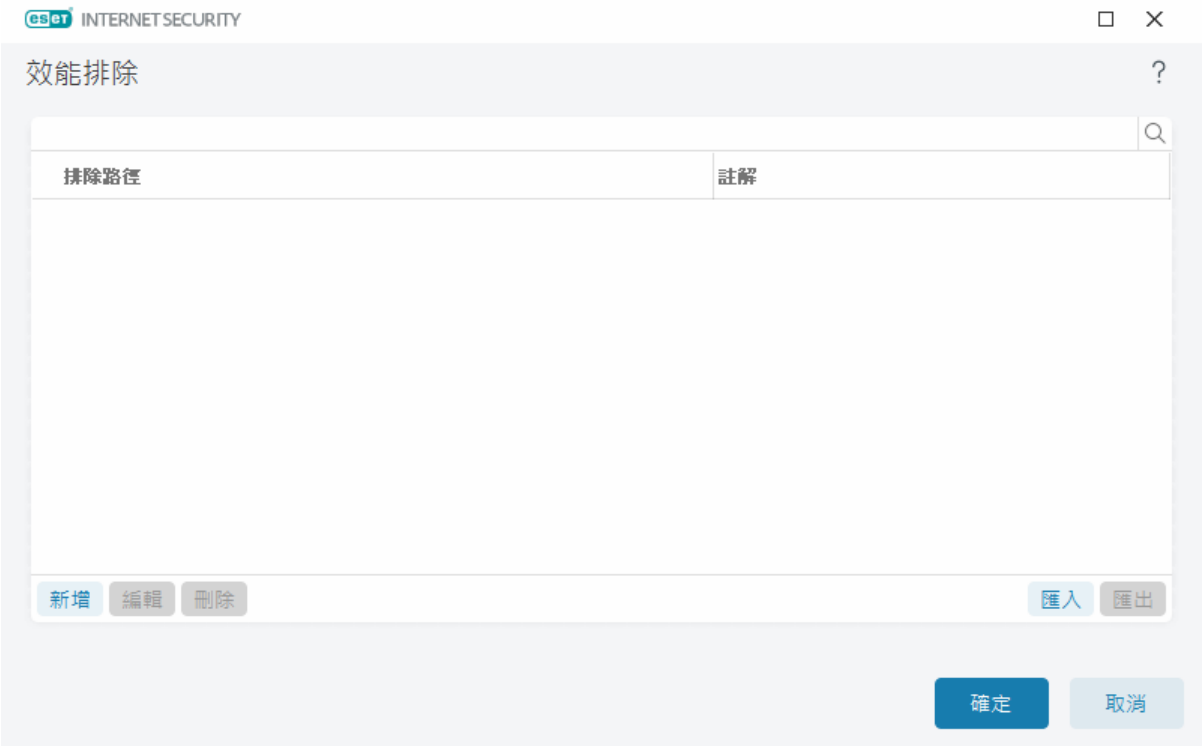
效能排除允許您從掃描中排除檔案和資料夾。

若要確保掃描所有物件是否存在威脅，建議您只有在絕對必要時建立效能排除。然而在某些情況下，您可能需要排除物件，例如排除在掃描期間可能會使電腦速度變慢的大型資料庫項目，或排除與掃描衝突的軟體。

您可以透過 [進階設定] > **[偵測引擎]** > **[排除]** > **[效能排除]** > **[編輯]**，將要從掃描中排除的檔案和資料夾新增到排除清單中。

請勿與偵測排除排除的副檔名HIPS 排除或程序排除混淆。

若要從掃描中排除物件（路徑、檔案或資料夾），請按一下 **[新增]** 並輸入適當的路徑或在樹狀結構中進行選取。



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

控制項元素

- **新增** – 從偵測中排除物件。

- **編輯** – 可讓您編輯已選取的項目。
- **刪除** – 移除已選取的項目 (CTRL + 按一下以選取多個項目)。

新增或編輯效能排除

此對話方塊視窗會排除此電腦的特定路徑（檔案或目錄）。

選擇路徑或手動輸入
若要選擇適當路徑，請按一下［**路徑**］欄位中的 **...**
手動輸入時，請參閱以下更多的排除格式範例

您可以使用萬用字元來排除一組檔案。問號（*?*）代表一個字元，而星號（***）代表含有零或多個字元的字串。

排除格式
- 如果您想要排除資料夾中的所有檔案和子資料夾，請輸入資料夾的路徑並使用遮罩 ***
- 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），但您只確定第一個字元（例如D)請使用下列格式：
D????.exe（問號取代遺失/不明的字元）

範例：
- *C:\Tools** – 路徑必須以反斜線 (\) 和星號 (*) 結尾，以指出它是資料夾以及所有將排除的子資料夾內容（檔案和子資料夾）。
- *C:\Tools*.** – 與 *C:\Tools** 相同的行為
- 將不會排除 *C:\Tools – Tools* 資料夾。從掃描器觀點來看，*Tools* 也可以是檔案名稱。
- *C:\Tools*.dat* – 這將排除 *Tools* 資料夾中的 .dat 檔案。
- *C:\Tools\sg.dat* – 這將排除這個位於確切路徑的特定檔案。

排除中的系統變數

您可以使用系統變數（如 %PROGRAMFILES%) 來定義掃描排除。

- 若要使用此系統變數排除 Program Files 資料夾，請在新增至排除時使用路徑 *%PROGRAMFILES%** （請記得在路徑結尾加上反斜線和星號）。
- 若要排除 *%PROGRAMFILES%* 子目錄中的所有檔案及資料夾，請使用路徑 *%PROGRAMFILES%\Excluded_Directory**

展開支援的系統變數清單

下列變數可以路徑排除格式使用：

- *%ALLUSERSPROFILE%*
- *%COMMONPROGRAMFILES%*
- *%COMMONPROGRAMFILES(X86)%*
- *%COMSPEC%*
- *%PROGRAMFILES%*
- *%PROGRAMFILES(X86)%*
- *%SystemDrive%*
- *%SystemRoot%*
- *%WINDIR%*
- *%PUBLIC%*

不支援使用者特有的系統變數（如 *%TEMP%* 或 *%USERPROFILE%*）或環境變數（如 *%PATH%*）。

不支援路徑中間的萬用字元

使用路徑中間的萬用字元（例如 *C:\Tools*\Data\file.dat*）可能可以運作，但未正式支援性能排除。使用偵測排除時，在路徑中間使用萬用字元不受限制。

排除順序

- 沒有使用頂端/底端按鈕調整排除優先順序的選項（就從上到下執行規則的防火牆規則而言）。
- 當掃描器符合第一個適用規則時，將不會評估第二個適用規則。
- 規則越少，掃描效能越好。
- 避免建立並行規則。

路徑排除格式

您可以使用萬用字元來排除一組檔案。問號（*?*）代表一個字元，而星號（***）代表含有零或多個字元的字串。

排除格式

- 如果您想要排除資料夾中的所有檔案和子資料夾，請輸入資料夾的路徑並使用遮罩 ***
- 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），但您只確定第一個字元（例如「D」）請使用下列格式：

D????.exe（問號取代遺失/不明的字元）

範例：

- *C:\Tools** – 路徑必須以反斜線（\）和星號（*）結尾，以指出它是資料夾以及所有將排除的子資料夾內容（檔案和子資料夾）。
- *C:\Tools*.** – 與 *C:\Tools** 相同的行為
- 將不會排除 *C:\Tools – Tools* 資料夾。從掃描器觀點來看，*Tools* 也可以是檔案名稱。
- *C:\Tools*.dat* – 這將排除 *Tools* 資料夾中的 .dat 檔案。
- *C:\Tools\sg.dat* – 這將排除這個位於確切路徑的特定檔案。

排除中的系統變數

您可以使用系統變數（如 %PROGRAMFILES%) 來定義掃描排除。

• 若要使用此系統變數排除 Program Files 資料夾，請在新增至排除時使用路徑 *%PROGRAMFILES%** （請記得在路徑結尾加上反斜線和星號）。

• 若要排除 *%PROGRAMFILES%* 子目錄中的所有檔案及資料夾，請使用路徑 *%PROGRAMFILES%\Excluded_Directory**

展開支援的系統變數清單

下列變數可以路徑排除格式使用：

- *%ALLUSERSPROFILE%*
- *%COMMONPROGRAMFILES%*
- *%COMMONPROGRAMFILES(X86)%*
- *%COMSPEC%*
- *%PROGRAMFILES%*
- *%PROGRAMFILES(X86)%*
- *%SystemDrive%*
- *%SystemRoot%*
- *%WINDIR%*
- *%PUBLIC%*

不支援使用者特有的系統變數（如 *%TEMP%* 或 *%USERPROFILE%*）或環境變數（如 *%PATH%*）

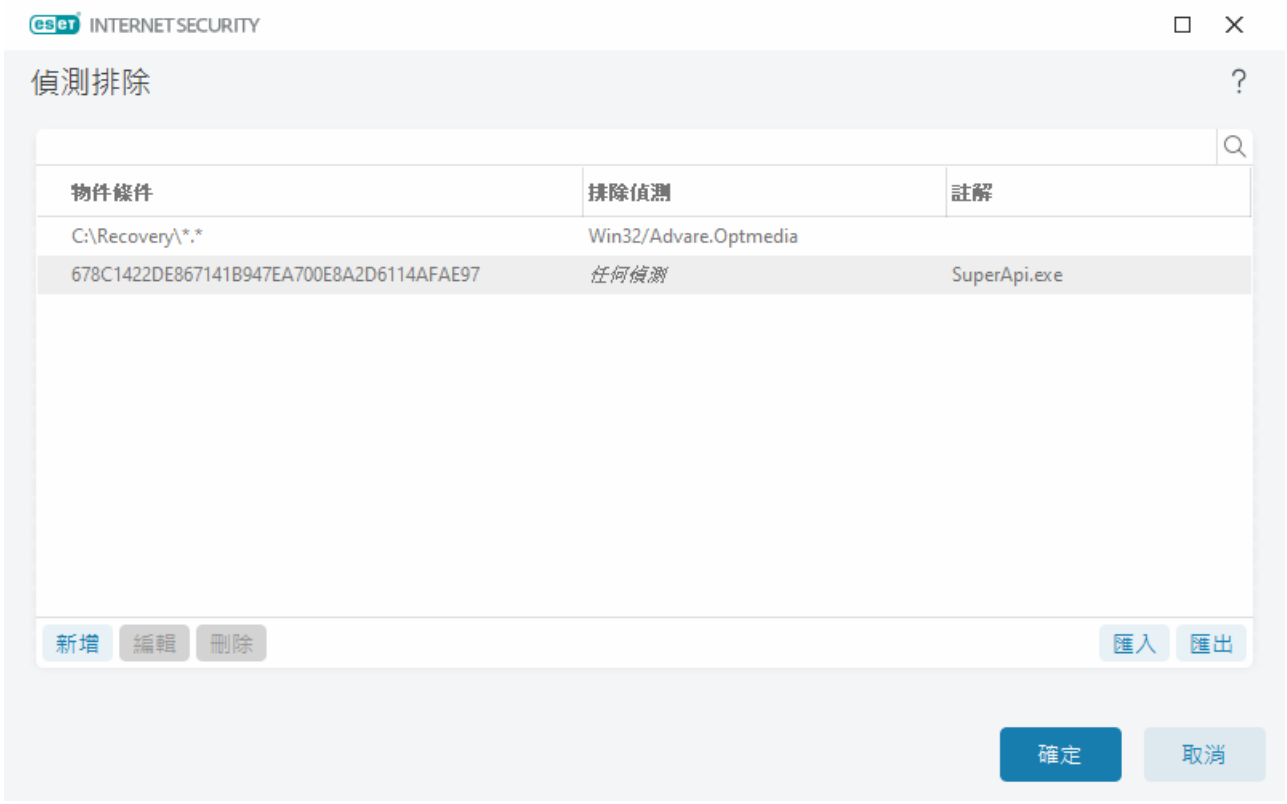
偵測排除

偵測排除可讓您藉由過濾偵測名稱、物件路徑或其雜湊，從偵測中排除物件。

偵測排除的運作方式

與效能排除相同，偵測排除不會從掃描中排除檔案和資料夾。只在偵測引擎偵測到物件，而且排除清單中有適當的規則時，偵測排除才會排除這些物件。

例如（請參閱下圖的第一列），當物件偵測為 Win32/Adware.Optmedia 且偵測到的檔案為 *C:\Recovery\file.exe*。在第二列上，儘管是偵測名稱，但會一律排除每一個具有適當 SHA-1 雜湊的檔案。



若要確保偵測所有威脅，建議您只有在絕對必要時建立偵測排除。

若要將檔案與資料夾新增至排除清單，請按一下［進階設定］> **[偵測引擎]** > **[排除]** > **[偵測排除]** > **[編輯]**。

請勿與效能排除、排除的副檔名、HIPS 排除或程序排除混淆。

若要從偵測引擎中排除物件（依其偵測名稱或雜湊），請按一下 **[新增]**。

對於潛在不需要的應用程式和潛在不安全的應用程式，還可以按偵測名稱建立排除：

- 在報告偵測的警示視窗中（按一下 **[顯示進階選項]**，然後選取 **[排除對此文件的掃描]**）。
- 從［防護記錄檔案］內容功能表來使用建立偵測排除精靈。
- 按一下 **[工具]** > **[隔離區]**，然後用滑鼠右鍵按一下隔離檔案，並選取內容功能表中的 **[還原並從掃描中排除]**。

偵測排除物件條件

- **[路徑]** – 限制指定路徑（或任何路徑）的偵測排除。
- **偵測名稱** – 如果排除檔案旁有偵測的名稱，則代表該檔案只針對該次偵測排除，但不是完全排除。如果該檔案在稍後被其他惡意軟體感染，則仍會偵測到該檔案。
- **雜湊** – 不論檔案類型、位置、名稱或其副檔名為何，請根據指定的雜湊 SHA-1 排除檔案。

新增或編輯偵測排除

排除偵測

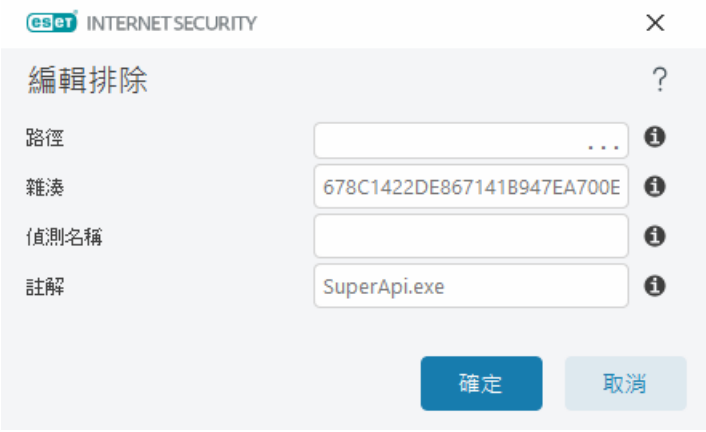
應提供有效的 ESET 偵測名稱。如需有效的偵測名稱，請參閱防護記錄檔案，然後從［防護記錄檔案］下拉式功能表中選取［**偵測**］。在 ESET Internet Security 中偵測到誤判範例時，這很實用。排除真實入侵非常危險，請考慮按一下［**路徑**］欄位中的 **[...]**，只排除受影響的檔案/目錄，和/或只排除暫時一段時間。排除也適用於潛在不需要的應用程式、潛在不安全的應用程式和可疑的應用程式。

另請參閱路徑排除格式

請參閱下面的偵測排除範例

排除雜湊

不論檔案類型、位置、名稱或其副檔名為何，請根據指定的雜湊 SHA-1 排除檔案。



依偵測名稱排除

若要依偵測名稱排除特定的偵測，請輸入有效的偵測名稱：
Win32/Adware.Optmedia
從 ESET Internet Security 警告視窗排除偵測時，您也可以使用下列格式：
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

控制項元素

- **新增** – 從偵測中排除物件。
- **編輯** – 可讓您編輯已選取的項目。
- **刪除** – 移除已選取的項目 (CTRL + 按一下以選取多個項目)。

建立偵測排除精靈

也可以從防護記錄檔案內容功能表建立偵測排除（不適用於惡意軟體偵測）：

1. 在主程式視窗中，按一下 **[工具] > [防護記錄檔案]**。
2. 以滑鼠右鍵按一下 **[偵測防護記錄]** 中的偵測。
3. 按一下 **[建立排除]**。

若要根據 **[排除標準]** 排除一個或多個偵測，請按一下 **[變更標準]**。

- **[相符檔案]** – 依據其 SHA-1 雜湊來排除每個檔案。
- **[偵測]** – 依據其偵測名稱來排除每個檔案。
- **[路徑 + 偵測]** – 依據偵測名稱和路徑來排除每個檔案，包括檔案名稱（例如，*file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*）。

建議選項是根據偵測類型預先選取。

或者，在按一下 **[建立排除]** 之前，您可以新增 **[註解]**。

偵測引擎進階選項

[透過 AMSI 啟用進階掃描] 是 Microsoft 反惡意軟體掃描介面工具，允許掃描 PowerShell 指令碼，其指令碼由 Windows Script Host 執行以及使用 AMSI SDK 掃描的資料。

網路流量掃描器

網路流量掃描器為應用程式通訊協定提供惡意軟體防護，該通訊協定整合了多種進階惡意軟體掃描技術。網路流量掃描器自動掃描 HTTP(S)、POP3(S) 和 IMAP(S) 通訊協定，無論網際網路瀏覽器或電子郵件用戶端如何。您可以在 [進階設定] > **[偵測引擎] > [網路流量掃描器]** 中啟用/停用網路流量掃描器。

啟用網路流量掃描器 – 如果停用此選項，則不會掃描 HTTP(S)、POP3(S) 和 IMAP(S) 通訊協定。請注意，以下 ESET Internet Security 功能需要啟用網路流量掃描器：

- Web 存取防護
- 家長控制
- 瀏覽器隱私權與安全性
- 安全銀行與瀏覽

- SSL/TLS
- 防網路釣魚防護
- 電子郵件用戶端防護

雲端型防護

ESET LiveGrid® (以先進的 ESET ThreatSense.Net 進階預早警告系統為基礎）會應用全球各地 ESET 使用者提交、並傳送到 ESET 研究實驗室的資料。透過提供可疑範例和中繼資料，ESET LiveGrid® 可讓我們立即回應客戶需求，並讓 ESET 隨時掌握最新威脅情報。

可用選項如下：

啟用 ESET LiveGrid® 聲譽系統

ESET LiveGrid® 聲譽系統提供雲端型白名單和黑名單。

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

啟用 ESET LiveGrid® 意見系統

除了 ESET LiveGrid® 聲譽系統以外，ESET LiveGrid® 意見系統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
- 日期和時間
- 威脅出現在電腦上的程序
- 電腦作業系統的相關資訊

依預設，ESET Internet Security 配置為將可疑檔案提交至 ESET 病毒實驗室以供詳細分析。特定副檔名的檔案，例如 *.doc* 或 *.xls* 等則會一律排除。如果有您或貴組織要避免傳送的特殊檔案，您也可以新增其他副檔名。

請在隱私權政策中閱讀更多有關傳送相關資料的資訊。

您可以選擇不要啟用 ESET LiveGrid®

您不會遺失軟體中的任何功能，但在某些情況下，當 ESET LiveGrid® 啟用時，ESET Internet Security 可能會更快回應新威脅。如果您使用過 ESET LiveGrid® 但現已停用，則可能還有待傳送的資料套件。即使已停用，此類套件仍會傳送到 ESET。一旦已傳送所有目前資訊，便不會繼續建立套件。

請在字彙中閱讀更多有關 ESET LiveGrid® 的資訊。
請參閱我們的圖解指示（以英文和其他數種語言提供），了解如何在 ESET Internet Security 中啟用或停用 ESET LiveGrid®

進階設定中的雲端型防護配置

如需存取 ESET LiveGrid® 的設定，請開啟 [進階設定] > **[偵測引擎]** > **[雲端型防護]**

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

- **[啟用 ESET LiveGrid® 意見系統]** – 將相關的提交資料（如以下 **[提交樣本]** 區段所述）連同當機報告及統計資料傳送至 ESET 研究實驗室，以進行進一步的分析。

- **[提交損毀報告與診斷資料]** – 提交 ESET LiveGrid® 相關診斷資料，例如損毀報告和模組記憶體傾印。我們建議將此保持啟用狀態，以協助 ESET 診斷問題、改善產品及確保更完善的使用者防護。

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

- **[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。除非需要更多資訊，否則您將不會收到 ESET 的任何回應。

提交樣本

手動提交範例 – 可選擇從內容功能表、隔離區或工具，將範例手動提交到 ESET 進行分析。

自動提交偵測的範例

選取會將何種類型的範例提交給 ESET以供分析並改善未來的偵測（預設範例大小上限為 64 MB)可用選項如下：

- **所有偵測的範例** – 偵測引擎所偵測到的所有物件（包括在掃描器設定中啟用時潛在不需要的應用程式）。

- **文件以外的所有範例** – **文件**以外所有偵測到的物件（如下所示）。

- **不提交** – 不會將偵測到的物件傳送給 ESET

自動提交可疑樣本

如果偵測引擎未偵測到這些範例，也會將其傳送給 ESET例如，幾乎錯過偵測的範例，或其中一個 ESET Internet Security 防護模組將這些範例視為可疑或有不明企圖的行為（預設範例大小上限為 64 MB)

- **可執行檔** – 包括 .exe, .dll, .sys 之類的可執行檔案。

- **壓縮檔** – 包括 .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab 之類的壓縮檔檔案類型。

- **指令碼** – 包括 .bat, .cmd, .hta, .js, .vbs, .ps1 之類的指令碼檔案類型。

- **[其他]** – 包括檔案類型如 .jar, .reg, .msi, .sfw, .lnk

• **[可能的垃圾郵件]** – 可將含附件的疑似垃圾郵件一部分或者整封郵件傳送至 ESET以供進一步分析。啟用此選項可提升垃圾郵件全域偵測的效果，包含為您提升未來垃圾郵件偵測的成效。

• **文件** – 包括 Microsoft Office 或 PDF 文件（不論是否包含作用中內容）。

展開以查看所有內含文件檔案類型的清單

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

排除

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

若要排除從 download.domain.com 下載的檔案，請按一下 [進階設定] > **[偵測引擎]** > **[雲端型防護]** > **[提交樣本]**，然後按一下 **[排除]** 旁邊的 **[編輯]**。新增排除 .download.domain.com

範例大小上限 (MB) – 定義自動上傳的範例大小上限 (1-64 MB)

適用於雲端型防護的排除過濾器

[排除過濾] 可讓您在提交範例時排除某些檔案或資料夾。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。常見的檔案類型（如 .doc 等）依預設排除在外。

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。

若要排除從 download.domain.com 下載的檔案，請開啟 [進階設定] > **[偵測引擎]** > **[雲端型防護]** > **[提交範例]** > **[排除]**，然後新增排除 *download.domain.com*

惡意軟體掃描

[惡意軟體掃描] 區段可從 [進階設定] > **[偵測引擎]** > **[惡意軟體掃描]** 中存取，並允許您為掃描設定檔配置掃描參數。

指定掃描

[選取的設定檔] – 一組專門由指定掃描器使用的參數。若要建立新設定檔，請按一下 **[設定檔清單]** 旁的 **[編輯]**。如需詳細資料，請參閱掃描設定檔

選取掃描設定檔後，可以配置以下選項：

掃描目標 – 如果您要掃描特定的目標或目標群組，請按一下 **[掃描目標]** 旁的 **[編輯]**，然後從資料夾（樹狀目錄）結構中選取選項。如需詳細資料，請參閱掃描目標

指定與機器學習防護 – 您可以為每個掃描設定檔配置報告和防護層級。根據預設，掃描設定檔使用與即時檔案系統防護中定義的相同設定。停用 **[使用即時防護設定]** 旁邊的切換開關，以配置自訂報告和防護層級。有關報告和防護層級的詳細說明，請參閱防護

ThreatSense – 進階設定選項，例如您要控制的檔案副檔名和使用的偵測方法。如需詳細資訊，請參閱 ThreatSense

掃描設定檔

ESET Internet Security 中有 4 個預先定義的掃描設定檔：

- **[智慧型掃描]** – 這是預設的進階掃描設定檔。智慧型掃描設定檔會使用智慧型最佳化技術，此技術可排除先前掃描中發現要清除，並自從該掃描後未進行修改的檔案。這樣可在盡可能不影響系統安全性的情況下，降低掃描時間。

- **[內容功能表掃描]** – 您可以從內容功能表中，啟動任何檔案的指定掃描。內容功能表掃描設定檔可讓您定義掃描配置檔，在您透過此方法觸發掃描時使用。

- **深入掃描** – 深入掃描設定檔預設不會使用智慧型最佳化，因此不會使用此設定檔從掃描中排除任何檔案。

- **[電腦掃描]** – 這是標準電腦掃描中所使用的預設設定檔。

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] > **[偵測引擎]** > **[惡意軟體掃描]** > **[指定掃描]** > **[設定檔清單]** > **[編輯]**。**[設定檔管理員]** 視窗包括 **[已選取的設定檔]** 下拉式功能表，其中列出現有的掃描設定檔與可建立新設定檔的選項。為協助您建立掃描設定檔以符合您的需求，請參閱 ThreatSense 以取得每個掃描設定參數的說明。

> 假設您要建立您自己的掃描設定檔且有部分適用 **[掃描您的電腦]** 配置，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 **[一律修復偵測]**。請在 **[設定檔管理程式]** 視窗中輸入新設定檔的名稱並按一下 **[新增]**。從 **[已選取的設定檔]** 下拉式功能表中選取新設定檔，並調整剩餘的參數以符合您的需求，接著按一下 **[確定]** 以儲存新的設定檔。

掃描目標

[掃描目標] 下拉式功能表可讓您選取預先定義的掃描目標。

- **[使用設定檔設定]** – 選取所選掃描設定檔指定的目標。
- **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。

- **自訂選擇** – 取消所有先前的選擇。

資料夾（樹狀）結構還包含特定掃描目標。

- **作業記憶體** – 掃描目前由作業記憶體使用的所有處理程序和資料。

- **開機磁區/UEFI** – 掃描開機磁區和 UEFI 中是否有惡意軟體。請在字彙中閱讀更多有關 UEFI 掃描器的資訊。

• **WMI 資料庫** – 掃描整個 Windows Management Instrumentation (WMI) 資料庫、所有命名空間、所有類型實例和所有屬性。搜尋對受感染檔案或作為資料嵌入的惡意軟體的參照。

• **系統登錄** – 掃描整個系統登錄、所有鍵和子鍵。搜尋對受感染檔案或作為資料嵌入的惡意軟體的參照。清除偵測時，該參照將保留在登錄表中，以確保不會遺失任何重要資料。

若要快速瀏覽至掃描目標（檔案或資料夾），請在樹狀結構下方的文字欄位中輸入其路徑。該路徑區分大小寫。若要在掃描中包含目標，請在樹狀結構中選取其核取方塊。

閒置狀態掃描

您可以在［進階設定］>［**偵測引擎**］>［**惡意軟體掃描**］>［**閒置狀態掃描**］中啟用閒置狀態掃描器。

閒置狀態掃描

啟用［**啟用閒置狀態掃描**］旁的切換開關以啟用此功能。電腦在閒置狀態時，會在所有本機磁碟機上執行無訊息電腦掃描。

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

在［進階］設定中開啟［**啟用記錄**］，即可在防護記錄檔案區段中記錄電腦掃描輸出（在主要程式視窗中按一下［**工具**］>［**防護記錄檔案**］，並從［**防護記錄**］下拉式功能表中選擇［**電腦掃描**］）。

閒置狀態偵測

請參閱閒置狀態偵測觸發，以取得要觸發閒置狀態掃描器所必須符合的完整條件清單。

ThreatSense – 進階設定選項，例如您要控制的檔案副檔名和使用的偵測方法。如需詳細資訊，請參閱 ThreatSense。

閒置狀態偵測

閒置狀態偵測設定可在［進階設定］>［**偵測引擎**］>［**惡意軟體掃描**］>［**閒置狀態掃描**］>［**閒置狀態偵測**］中配置。這些設定可指定在以下狀況下觸發閒置狀態掃描。

- **已關閉螢幕或螢幕保護程式**
- **電腦鎖定**
- **使用者登出**

使用各種狀態的切換以啟用或停用不同閒置狀態偵測觸發。

啟動掃描

依預設，在系統啟動和偵測引擎更新時，將執行啟動檔案自動檢查。這項掃描取決於排程器配置及工作。

啟動掃描選項是［**系統啟動檔案檢查**］排程器工作的一部分。若要變更其設定，請前往［**工具**］>［**排程器**］，按一下［**自動啟動檔案檢查**］，接著［**編輯**］。在最後一步中，自動啟動檔案檢查視窗將出現。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。

ThreatSense – 進階設定選項，例如您要控制的檔案副檔名和使用的偵測方法。如需詳細資訊，請參閱 ThreatSense

啟動檔案自動檢查

建立「系統啟動檔案檢查」排程工作時，有數個選項可供您調整下列參數：

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

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

此外也包含兩個特定的群組：

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

已針對上方每個群組修正了要掃描的檔案清單。如果您針對要在系統啟動時執行的檔案，選擇降低掃描深度，則會在開啟或執行時，對不掃描的檔案進行掃描。

掃描優先順序 – 用於決定何時開始掃描的優先順序層級：

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

可移除的媒體

插入電腦時ESET Internet Security 提供自動卸除式媒體 (CD/DVD/USB/...) 掃描。插入電腦時提供自動卸除式媒體掃描。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。

若已插入卸除式媒體，且 **[顯示掃描選項]** 已在 [進階設定] > **[偵測引擎]** > **[惡意軟體掃描]** > **[卸除式媒體]** 中設定，則會顯示下方對話方塊：

此對話方塊的選項：

- **立即掃描** – 將會觸發掃描可移除的媒體。
- **不掃描** – 將不會掃描卸除式媒體。
- **設定** – 開啟［進階設定］。
- **永遠使用選取的選項** – 選取後，在其他時間插入可移除媒體後會執行相同的處理方法。

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

若要存取卸除式媒體掃描的設定，請開啟［進階設定］>［**偵測引擎**］>［**惡意軟體掃描**］>［**卸除式媒體**］。

插入可移除媒體之後要採取的處理方法 – 選取預設處理方法，在將可移除媒體裝置插入電腦之後執行 (CD/DVD/USB)。將卸除式媒體插入電腦時，請選擇所需的動作：

- **不掃描** – 不執行任何處理方法，且不會開啟**偵測到新裝置**視窗。
- **自動裝置掃描** – 已插入的卸除式媒體裝置將會執行電腦掃描。
- **顯示掃描選項** – 開啟［**卸除式媒體**］區段。

文件防護

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

若要啟動文件防護，請開啟［進階設定］>［**偵測引擎**］>［**惡意軟體掃描**］>［**文件防護**］，然後按一下［**啟用文件防護**］旁的滑動軸。

ThreatSense – 進階設定選項，例如您要控制的檔案副檔名和使用的偵測方法。請參閱 ThreatSense 以取得更多資訊。

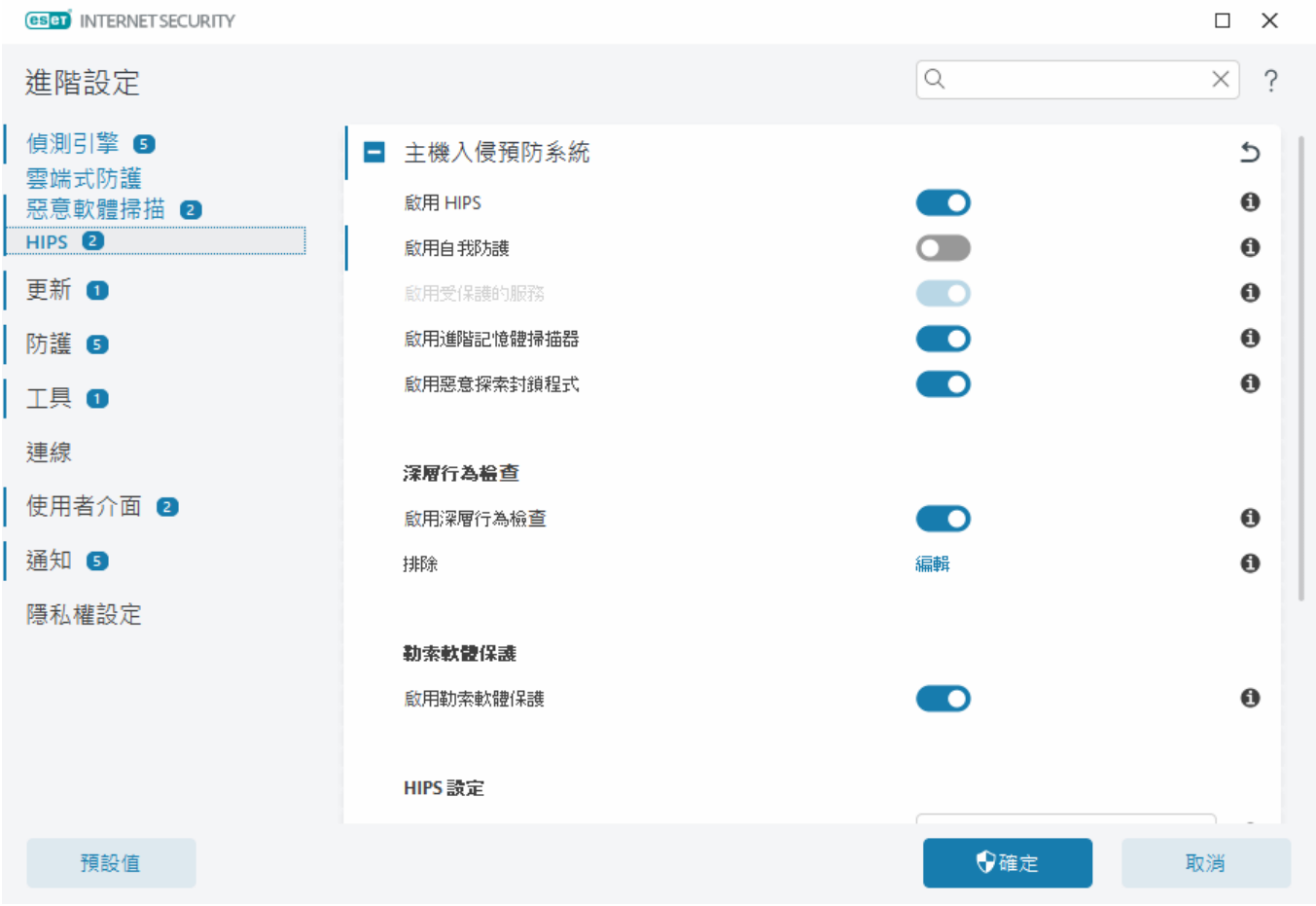
> 使用 Microsoft Antivirus API 的應用程式（例如 Microsoft Office 2000 與更新版本，或 Microsoft Internet Explorer 5.0 與更新版本）可啟動此功能。

主機入侵預防系統 (HIPS)

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

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

您可以在 [進階設定] > **[偵測引擎] > [HIPS] > [主機入侵預防系統]** 中配置 HIPS 設定。HIPS 狀態（已啟用/已停用）顯示在 ESET Internet Security 主程式視窗 > **[設定] > [電腦防護]** 中。



主機入侵預防系統

啟用 HIPS – 依預設會在 ESET Internet Security 中啟用 HIPS。關閉 HIPS 會停用其餘的 HIPS 功能，像是惡意探索封鎖程式。

啟用自我防護 – ESET Internet Security 使用內建的 **[自我防護]** 技術作為 HIPS 一部分，可防止惡意軟體損毀或停用您的防毒及間諜程式防護。自我防護可保護重要系統和 ESET 的程序、登錄機碼和檔案不受竄改。

啟用受保護的服務 – 為 ESET 服務 (ekrn.exe) 啟用防護。啟用防護時，會以受保護的 Windows 處理程序啟動此服務來防禦來自惡意軟體的攻擊。

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

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

深層行為檢查

啟用深層行為檢查 – 另一種層級的防護，可作為 HIPS 功能的一部分運作。此 HIPS 延伸模組會分析電腦上所有執行中程式的行為，並警告您處理程序的行為是否為惡意。

深層行為檢查中的 HIPS 排除可讓您從分析中排除處理程序。為確保所有處理程序是否已掃描可能的威脅，我們建議您只有在絕對必要時建立排除。

勒索軟體保護

啟用勒索軟體防護 – 另一種層級的防護，可作為 HIPS 功能的一部分運作。您必須啟用 ESET LiveGrid® 聲譽系統以便讓勒索軟體防護正常運作。請閱讀更多有關此類型防護的資訊

啟用 Intel® Threat Detection Technology – 利用唯一的Intel CPU 遙測，幫助偵測勒索軟體攻擊，提高偵測效率、減少誤判警報，以及擴展可見度以捕獲進階逃避技術。參閱支援的處理器

HIPS 設定

[過濾模式] 可在下列四種模式之一中執行：

過濾模式	說明
自動模式	系統會啟用作業，但受到保護系統的預先定義規則封鎖的作業除外。
智慧型模式	僅會通知使用者關於非常可疑的事件。
互動模式	系統將提示使用者確認作業。
原則型模式	封鎖特定規則未定義但允許的所有操作。
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 **[HIPS 規則]** 編輯器中檢視，但與手動建立的規則或自動模式下建立的規則相較之下，其優先順序較低。當您從 **[過濾模式]** 下拉式功能表選取 **[學習模式]**，即可使用 **[學習模式將在下列情況結束]** 設定。選取您要啟用學習模式的時間範圍，最長持續時間為 14 天。過了指定的持續時間之後，會提示您在學習模式中編輯 HIPS 建立的規則。您可以選擇不同的過濾模式，或者延後決定並持續使用學習模式。

學習模式到期後的模式設定 – 選取將在學習模式到期後使用的過濾模式。到期之後，**詢問使用者**選項需具備管理權限，才能對 HIPS 過濾模式執行變更。

HIPS 系統監控作業系統中的事件，並根據類似防火牆規則的規則執行反應動作。按一下 **[規則]** 旁邊的 **[編輯]** 以開啟 **[HIPS 規則]** 編輯器。在 HIPS 規則視窗中，您可以選取、新增、編輯或移除規則。在編輯 HIPS 規則中可找到更多關於規則建立與 HIPS 作業的詳細資料。

HIPS 排除

排除可讓您從 HIPS 深層行為檢查中排除程序。

若要編輯 HIPS 排除，請開啟［進階設定］> **[偵測引擎] > [HIPS] >** ［**主機入侵預防系統**］> ［**排除**］> ［**編輯**］

請勿將排除的副檔名偵測排除效能排除或程序排除混淆。

若要排除物件，請按一下［**新增**］並輸入物件的路徑或在樹狀結構中進行選取。您也可以［編輯］或［刪除］所選的項目。

HIPS 進階設定

以下選項可用於除錯及分析應用程式的行為：

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

［**記錄所有封鎖的作業**］– 所有封鎖的作業將寫入 HIPS 防護記錄中。只有在疑難排解時或在ESET 技術支援」要求下才能使用這個功能，因為這可能會產生大量的防護記錄檔案，而使電腦速度變慢。

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

一律允許載入驅動程式

除非使用者規則明確封鎖，否則無論 HIPS 過濾模式為何，一律允許載入此清單上顯示的驅動程式。

新增 – 新增新的驅動程式。

編輯 – 編輯已選取的驅動程式。

［**移除**］– 從清單移除驅動程式。

重設 – 重新載入一組系統驅動程式。

如果您不想要包含已經手動新增的驅動程式，請按一下［**重設**］。如果您已經新增數個驅動程式且您無法手動從清單上刪除這些驅動程式，這可能很有用。

安裝後，驅動程式清單為空白ESET Internet Security 會在一段時間後自動填寫該清單。

HIPS 互動視窗

HIPS 通知視窗可讓您根據 HIPS 偵測的新處理方法來建立規則，然後定義允許或拒絕該處理方法所依據的條件。

系統認定從通知視窗建立的規則等於手動建立的規則。從通知視窗建立的規則無需像觸發該對話視窗的規則那般明確。這表示，在對話方塊中建立規則後，同樣的作業可以觸發相同的視窗。如需詳細資訊，請參閱 HIPS 規則的優先順序

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

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

［**建立規則並永久記住規則**］選項會建立新的 HIPS 規則，稍後可以在 HIPS 規則管理一節中加以變更（需要系統管理權限）。

按一下底部的［**詳細資料**］，查看觸發此作業的應用程式為何、檔案的聲譽為何，或要求您允許或拒絕的作業種類。

按一下［**進階選項**］，可以存取更多詳細規則參數的設定。如果您選擇［**建立規則並永久記住規則**］，即可使用以下選項：

- **僅建立對此應用程式有效的規則** – 如果您取消選取此核取方塊，則會針對所有來源應用程式建立規則。
- **僅適用於作業** – 選擇規則檔案/應用程式/登錄作業。請參數所有 HIPS 作業的說明
- **僅適用於目標** – 選擇規則檔案/應用程式/登錄目標。

無窮盡的 HIPS 通知？
若要停止顯示通知，請在［**進階設定**］> ［偵側引擎］> **[HIPS]** > ［**主機入侵預防系統**］中將過濾模式變更為［**自動**］

學習模式已結束

學習模式會自動建立並保存規則。您可以在 HIPS 規則設定中檢查所有已建立的規則。此模式最適合用於 HIPS 的初始配置，但只能保持短時間。因為 ESET Internet Security 會根據預先定義的參數來儲存規則，所

以不需要與使用者互動。已為作業系統中執行的必要程序建立所有規則後，切換到［**互動**］或［**原則型模式**］，以避免發生安全性風險。

如果您不想變更設定，可以推遲此決定。

偵測到潛在的勒索軟體行為

在偵測到潛在的勒索軟體行為時，此互動視窗將會出現。您可以選擇［**拒絕**］或［**允許**］作業。

按一下［**詳細資料**］以檢視特定偵測參數。此對話視窗可讓您［**提交檔案以供分析**］或［**從偵測中排除**］。

ESET LiveGrid® 必須啟用以確保勒索軟體防護可正常運作。

HIPS 規則管理

來自 HIPS 系統的使用者定義和自動新增的規則清單。更多關於規則建立與 HIPS 作業的詳細資料可在 HIPS 規則設定中取得。另請參閱 HIPS 的一般原則。

直欄

規則 - 使用者定義或自動選擇的規則名稱。

已啟用 - 如果您想要將規則保留在清單中，但不想使用它，請停用滑動軸。

處理方法 - 規則指定在條件正確時應執行的處理方法 - ［**允許**］。［**封鎖**］或［**詢問**］。

來源 - 只有當事件是由此應用程式觸發時，才會使用此規則。

目標 - 只有當作業與特定檔案、應用程式或登錄項目相關時，才會使用此規則。

［**防護記錄嚴重性**］ - 如果您啟動此選項，有關此規則的資訊將寫入 HIPS 防護記錄。

通知—若觸發事件，右下角將出現一個小的通知。

控制項元素

新增 – 建立新規則。

編輯 – 可讓您編輯已選取的項目。

[刪除] – 移除已選取的項目。

HIPS 規則的優先順序

沒有使用頂端/底端按鈕調整 HIPS 規則優先順序的選項（就從上到下執行規則的防火牆規則而言）。

- 您建立的所有規則都具有相同的優先順序
- 規則越明確，優先順序越高（例如，特定應用程式適用規則的優先順序高於所有應用程式適用的規則）
- HIPS 內部包含您無法存取的較高優先順序規則（例如，您無法覆寫自我防護定義的規則）
- 若您建立的規則可能凍結您的作業系統，將不會套用該規則（其優先順序最低）

編輯 HIPS 規則

請先參閱 HIPS 規則管理

規則名稱 – 使用者定義或自動選擇的規則名稱。

處理方法 – 指定在符合條件時應執行的處理方法 – **[允許]****[封鎖]** 或 **[詢問]**

影響到的作業 – 您必須選取要套用規則的作業類型。規則只會使用於此類作業以及選取的 [目標]。

已啟用 – 如果您想要將規則保留在清單中，但不想套用它，請停用切換開關。

[防護記錄嚴重性] – 如果您啟動此選項，有關此規則的資訊將寫入 HIPS 防護記錄

通知使用者 – 若觸發事件，右下角將出現一個小的通知。

規則包含三個部分，說明觸發此規則的條件：

來源應用程式 – 只有當事件是由此應用程式觸發時，才會使用此規則。從下拉式功能表中選取 **[特定應用程式]**，並按一下 **[新增]** 以新增新的檔案，或者您可以從下拉式功能表中選取 **[所有應用程式]** 以新增所有應用程式。

目標檔案 – 只有當作業與此目標相關時，才會使用此規則。從下拉式功能表中選取 **[特定檔案]**，並按一下 **[新增]** 以新增新的檔案或資料夾，或者您可以從下拉式功能表中選取 **[所有檔案]** 以新增所有應用程式。

應用程式 – 只有當作業與此目標相關時，才會使用此規則。從下拉式功能表中選取 **[特定應用程式]**，並按一下 **[新增]** 以新增新的檔案或資料夾，或者您可以從下拉式功能表中選取 **[所有應用程式]** 以新增所有應用程式。

登錄項目 – 只有當作業與此目標相關時，才會使用此規則。從下拉式功能表選取 **[特定項目]**，並按一

下［**新增**］以手動輸入，或按一下［**開啟登錄編輯器**］以從登錄中選取機碼。您也可以從下拉式功能表選取［**所有項目**］以新增所有應用程式。

根據預設，不能封鎖且必須允許由 HIPS 預先定義之特定規則的某些作業。此外，並非所有的系統作業皆由 HIPS 監視。HIPS 監視系統視為不安全的作業。

重要作業的說明：

檔案作業

- **刪除檔案** – 應用程式正在要求權限，以刪除目標檔案。
- **寫入檔案** – 應用程式正在要求權限，以寫入目標檔案。
- **［直接存取磁碟］** – 應用程式正嘗試以非標準程序從磁碟讀取或寫入磁碟，此動作將規避一般的 Windows 程序。這會導致在沒有對應規則之應用程式的情況下，修改檔案。此作業可能是因為惡意軟體嘗試規避偵測、備份軟體嘗試複製完整的磁碟副本，或是分割區管理程式嘗試重新組織磁碟區所造成。
- **［安裝全域攔截］** – 表示呼叫 MSDN 程式庫中的 SetWindowsHookEx 函式。
- **載入驅動程式** – 將驅動程式安裝於系統中並載入。

應用程式作業

- **對另一個應用程式進行除錯** – 附加除錯工具至處理程序。執行應用程式除錯作業時，您可以檢視並修改其行為的多種詳細資料，並且存取其資料。
- **攔截另一個應用程式的事件** – 來源應用程式嘗試獲取特定應用程式鎖定的事件（例如 Keylogger 嘗試擷取瀏覽器事件）。
- **終止/暫停另一個應用程式** – 暫停、恢復或終止處理程序（可從 Process Explorer 或［處理程序］窗格直接存取）。
- **開始新應用程式** – 開始新的應用程式或處理程序。
- **修改另一個應用程式的狀態** – 來源應用程式嘗試寫入目標應用程式的記憶體或代表自身執行程式碼。透過在封鎖使用此作業的規則中，將重要的應用程式配置為目標應用程式來進行保護，這樣做很有助益。

登錄作業

- **［修改啟動設定］** – 設定中的任何變更，這些設定是定義哪些應用程式將在 Windows 啟動時執行。例如，您可以透過搜尋 Windows 登錄中的 Run 機碼，找到這些設定。
- **從登錄刪除** – 刪除登錄機碼或其值。
- **重新命名登錄機碼** – 重新命名登錄機碼。
- **修改登錄** – 建立登錄機碼的新值、變更現有的值、在資料庫樹狀結構中移動資料，或設定登錄機碼的使用者或群組權限。

輸入目標時，您可以在某些限制下使用萬用字元。登錄路徑中不使用特定機碼，而是使用 *（星號）符號。例如，*HKEY_USERS*\software* 可能是指 *HKEY_USER\.default\software*，而非*HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*。*HKEY_LOCAL_MACHINE\system\ControlSet** 不是有效的登錄機碼路徑。登錄機碼路徑若包含 *，表示「此路徑，或該符號之後的所有層級的所有路徑」。這是針對檔案目標使用萬用字元的唯一方法。首先，會先評估確實路徑，然後評估萬用字元符號（*）之後的路徑。

⚠ 如果您建立了過於廣泛的規則，則會顯示此種規則類型的相關警告。

在下列範例中，我們將示範如何限制特定應用程式發生不想要的行為：

1. 替規則命名並選取［**處理方法**］下拉式功能表中的［**封鎖**］（如果您偏好稍後選擇，則選取［**詢問**］）。

2. 啟用［**通知使用者**］旁邊的滑動軸，以在每次套用規則時顯示通知。

3. 在將套用規則的［**影響的作業**］區段中，選取［至少一個作業］。

4. 按［**下一步**］。

5. 在［**來源應用程式**］視窗中，從下拉式功能表選取［**特定應用程式**］，將您的新規則套用至所有嘗試在您指定的應用程式上執行任何已選取應用程式作業的應用程式。

6. 按一下［**新增**］，再按一下［**...**］以選擇特定應用程式的路徑，然後按［**確定**］。如果您想要，可以新增其他應用程式。
例如： *C:\Program Files (x86)\Untrusted application\application.exe*

7. 選取［**寫入檔案**］作業。

8. 從下拉式功能表中選取［**所有**］。這會阻止前一個步驟中所選的應用程式嘗試寫入任何檔案。

9. 按一下［**完成**］以儲存您的新規則。

新增 HIPS 的應用程式/登錄路徑

按一下 **...** 選項，選取檔案應用程式路徑。選取資料夾時，將包括位於此位置的所有應用程式。

［開啟登錄編輯器］選項將啟動 Windows 登錄編輯器 (regedit)。新增登錄路徑時，請在 **［值］**欄位中輸入正確的位置。

以下為檔案或登錄路徑範例：

- *C:\Program Files\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

更新

更新設定選項在［進階設定］> **［更新］**中可用。此區段可指定更新來源資訊，如正在使用的更新伺服器及這些伺服器的驗證資料。

更新

目前使用的更新設定檔已顯示在 **［選取預設更新設定檔］**下拉式功能表中。

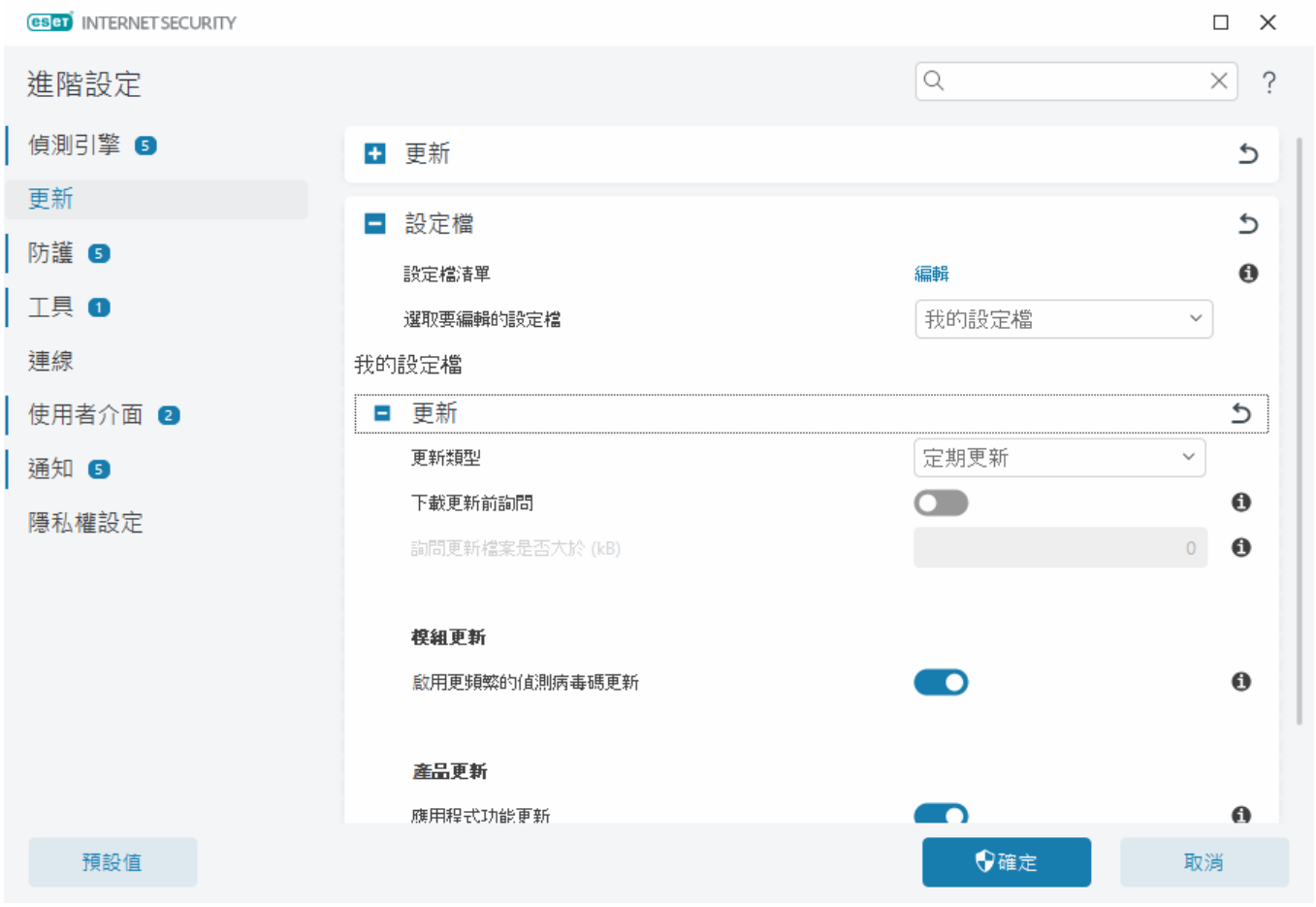
若要建立新設定檔，請參閱更新設定檔一節。

自動設定檔切換 – 可讓您將更新設定檔指派給特定的網路連線設定檔。

如果您在嘗試下載偵測引擎或模組更新時遇到困難，請按一下 **［清除更新快取］**旁的 **［清除］**以清除暫時更新檔案/快取。

模組還原

如果您懷疑偵測引擎和/或程式模組的新更新不穩定或損壞，您可以還原回上一版，並在一段期間內停用任何更新。



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

設定檔

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

[選取要編輯的設定檔] 下拉式功能表會顯示目前選取的設定檔，依預設會設定為 **[我的設定檔]**。若要建立新設定檔，請按一下 **[設定檔清單]** 旁的 **[編輯]**，輸入您自己的 **[設定檔名稱]**，然後按一下 **[新增]**。

更新

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

[下載更新前詢問] – 程式會顯示通知，讓您可以選擇確認或拒絕更新檔案下載。

[若更新檔案大於 (kB) 則詢問] – 如果更新檔案大於指定值，程式會顯示確認對話方塊。若更新檔案大小設為 0 kB，則程式將一律顯示確認對話方塊。

模組更新

[啟用更頻繁的偵測簽章更新] – 偵測簽章會在更短的間隔內更新。停用此設定可能會對偵測速率造成負面影響。

產品更新

應用程式功能更新 – 自動安裝新版的 ESET Internet Security。

連線選項

若要使用代理伺服器來下載更新，請參閱連線選項區段。

更新還原

如果您懷疑新的偵測引擎更新或程式模組不穩定或損壞，您可以還原回上一版，並暫時停用任何更新。如果您先前已無限期延後更新，您也可以啟用這些停用的更新。

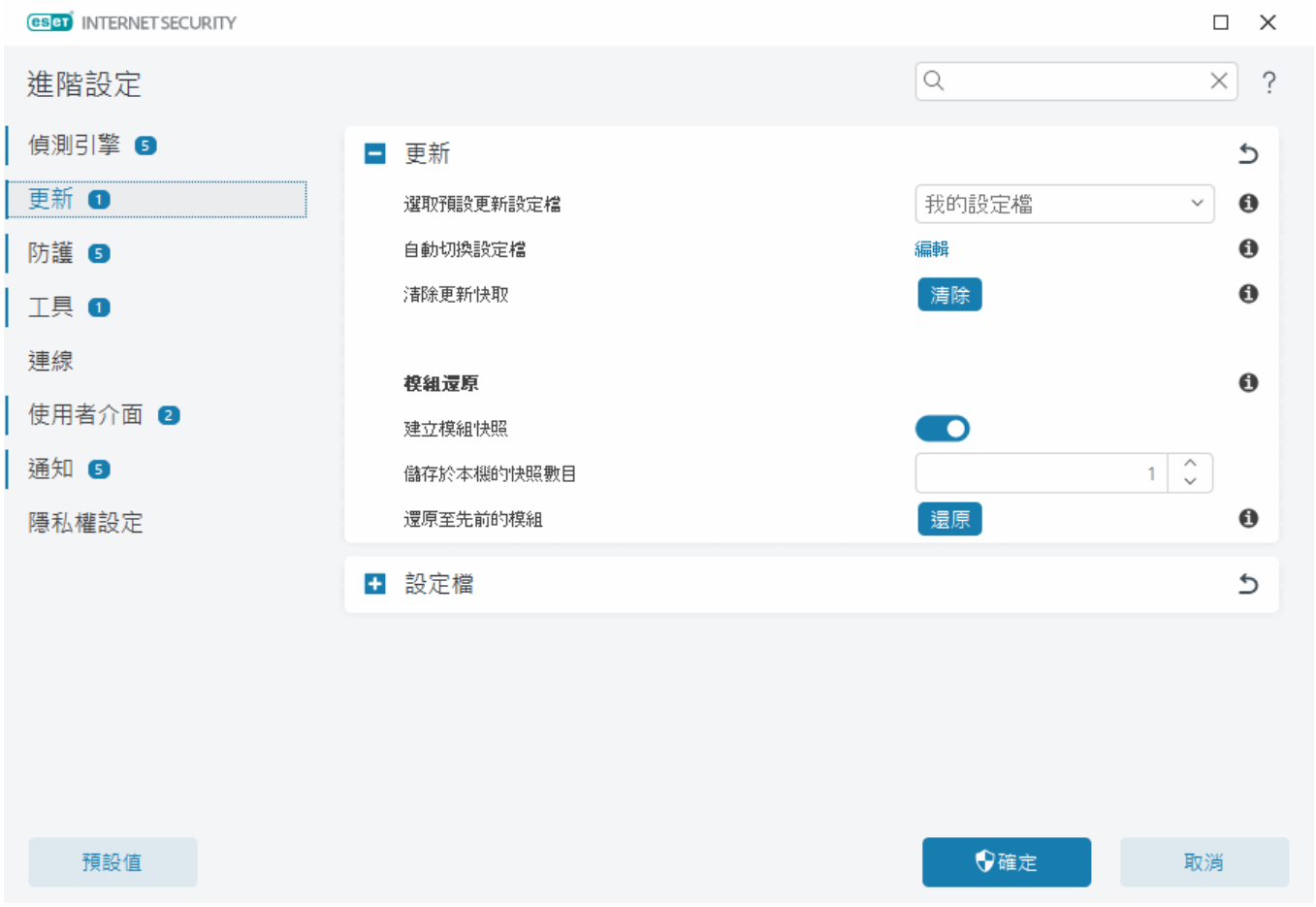
ESET Internet Security 會記錄偵測引擎與程式模組的快照，以搭配 還原功能使用。若要建立病毒資料庫快照，請將 **[建立模組快照]** 核取方塊保持在啟用狀態。啟用 **[建立模組快照]** 後，在第一次更新期間會建立第一個快照。下一個則在 48 小時後建立。**[儲存於本機的快照數目]** 欄位會定義已儲存的偵測引擎快照數量。

當達到最大快照量（例如三個）時，最舊的快照將每 48 小時替換為一個新的快照。ESET Internet Security 會將偵側引擎程式模組更新版本還原至最舊的快照。

如果您按一下 [進階設定] > **[更新]** > **[基本]** 中的 **[回復]**），您必須從 **[持續時間]** 下拉式功能表中選取時間間隔，代表暫停偵測引擎與程式模組更新的時間。

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

如果還原已執行，則 **[還原]** 按鈕會變成 **[允許更新]**。不允許在從 **[暫停更新]** 下拉式功能表中選取的時間間隔內進行更新。偵測引擎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。



假設編號 22700 是偵測引擎的最新版本，且 22698 和 22696 會儲存為偵測引擎的快照。請注意，22697 無法使用。在此案例中，因為電腦已在 22697 更新中關機，且在 22697 下載前已進行較新的更新。如果您在 **[儲存於本機的快照數目]** 欄位中設為 2，並按一下 **[還原]**，則偵測引擎（包含程式模組）將還原回編號 22696 的版本。此程序可能需要一些時間。從主要程式視窗的 [更新] 區段中檢查偵測引擎版本是否已降級。

回復時間間隔

如果您按一下 [進階設定] > **[更新]** > **[基本]** 中的 **[回復]**），您必須從 **[持續時間]** 下拉式功能表中選取時間間隔，代表暫停偵測引擎與程式模組更新的時間。

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

因此 ESET 不建議選取此選項。

產品更新

[產品更新] 區段可讓您在新的功能更新可用時自動安裝該更新。

應用程式功能更新會引入新功能，或變更舊版中已存在的功能。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。在已安裝應用程式功能更新後，可能需要重新啟動電腦。

應用程式功能更新 – 啟用後，將自動執行應用程式功能更新。

連線選項

若要存取特定更新設定檔的 Proxy 伺服器設定選項，請開啟 [進階設定] > **[更新]** > **[設定檔]** > **[更新]** > **[連線選項]**。按一下 **[Proxy 模式]** 下拉式功能表，然後選取下列三個選項之一：

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

選取 **[使用全域 Proxy 伺服器設定]** 以使用已在 [進階設定] > **[連線]** > **[Proxy 伺服器]** 中指定的 Proxy 伺服器配置

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

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

- 已使用與 [進階設定] > **[連線]** 中定義不同的 Proxy 伺服器來更新 ESET Internet Security在此配置中，應該在 **Proxy 伺服器**位址和通訊**連接埠**（預設為 3128）下指定新 Proxy 的資訊，並在有需要時指定 Proxy 伺服器的**使用者名稱**以及**密碼**
- 並未全域設定 Proxy 伺服器，但是 ESET Internet Security 將連接至 Proxy 伺服器進行更新。
- 電腦透過 Proxy 伺服器連接至網際網路。系統在程式安裝期間從 Internet Explorer 取得設定，但如果它們隨後有所變更（例如您變更 ISP)請檢查此視窗中的 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]**

[如果 Proxy 無法使用，請使用直接連線] – 如果 Proxy 無法存取，便會在更新期間略過 Proxy

> 此區段中的 **[使用者名稱]** 和 **[密碼]** 欄位專屬於該 Proxy 伺服器。只有在需要使用者名稱及密碼來存取 Proxy 伺服器時，才填寫這些欄位。僅當您瞭解您需要密碼以透過 Proxy 伺服器存取網際網路時才填寫這些欄位。

防護

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。例如，如果偵測到分類為惡意軟體

的物件，將啟動修復。防護可以消除此物件，方法為將其封鎖，然後清除、刪除或將其移至隔離區。

若要詳細配置防護，請開啟 [進階設定] > **[防護]**。

⚠ 僅應由有經驗的使用者變更防護。未正確配置的設定可能導致防護層級降低。

在此區段中：

- 偵測回應
- 報告設定
- 防護設定

偵測回應

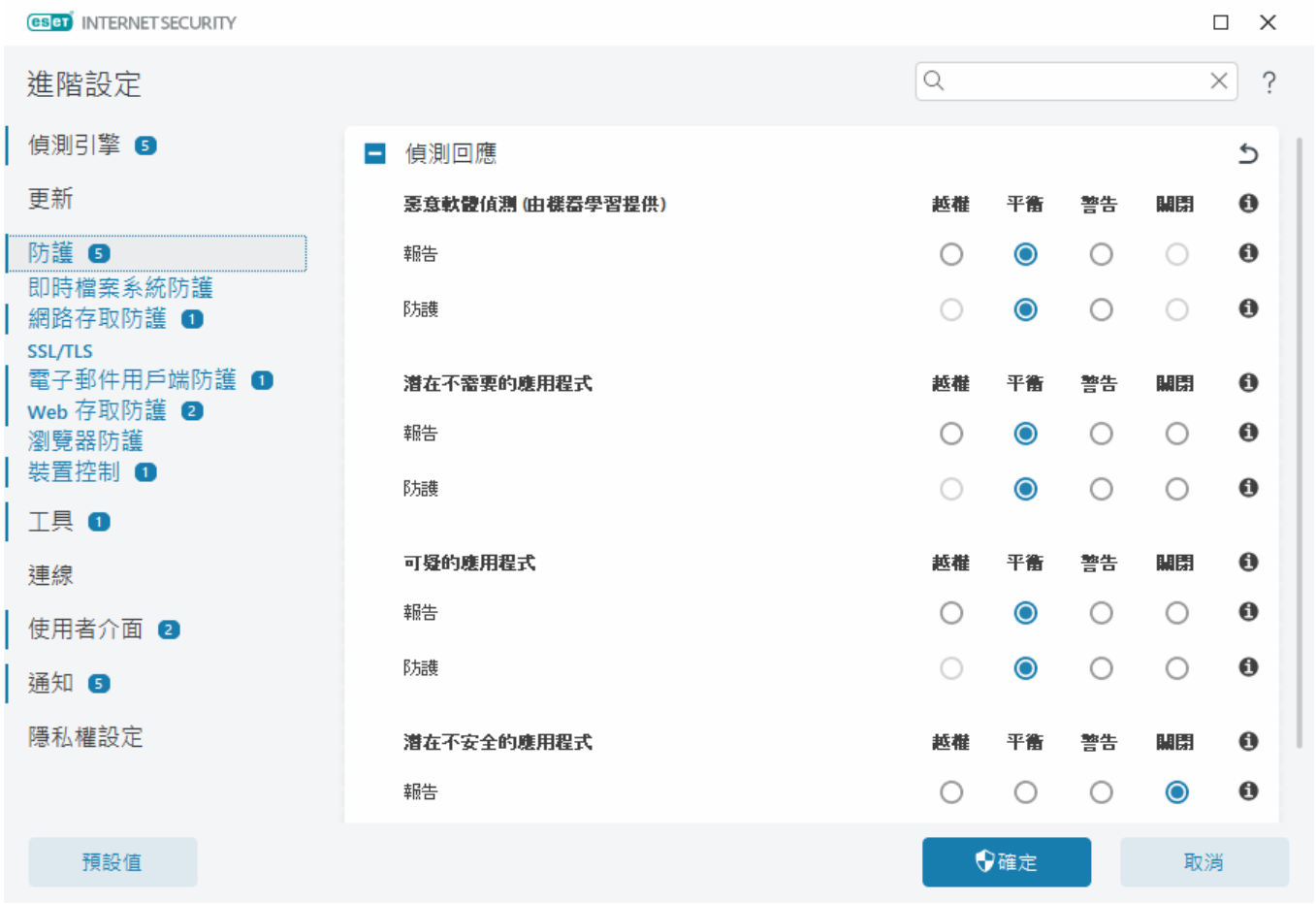
偵測回應使您能夠為以下類別配置報告和防護層級：

- **惡意軟體偵測（由機器學習提供）** – 電腦病毒是一種惡意程式碼，會預置或附加到電腦的現有檔案上。但是，「病毒」一詞常常遭到濫用。「惡意軟體」才是比較準確的用詞。惡意軟體偵測會由結合了機器學習元件的偵測引擎模組執行。在字彙中閱讀更多有關這些應用程式類型的資訊。

- **潛在不需要的應用程式** – 灰色軟體或潛在不需要的應用程式 (PUA) 是軟體的廣泛類別，其意圖明確地不帶有惡意，不像其他類型的惡意軟體（如病毒或特洛伊木馬程式）。不過，它可以安裝其他不需要的軟體、變更數位裝置的行為，或是執行使用者未認可或預期的活動。在字彙中閱讀更多有關這些應用程式類型的資訊。

- **可疑的應用程式**包括以加殼或保護工具壓縮的程式。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。

- **潛在不安全的應用程式** – 是指合法但可能不當用於惡意用途的商業軟體。例如遠端存取工具、密碼破解應用程式及鍵盤記錄程式（記錄每次使用者按鍵的程式）等，皆為潛在不安全的應用程式 (PUA)。在字彙中閱讀更多有關這些應用程式類型的資訊。



已改善的防護

進階機器學習現在是防護的一部分，做為進階的防護層，能夠根據機器學習改善偵測。請在字彙中進一步瞭解此類型的防護。

報告設定

當偵測發生（例如，找到威脅並將其分類為惡意軟體）時，資訊會記錄至偵測防護記錄，而且若在 ESET Internet Security 中配置，則會發生桌面通知

報告閾值是針對每個類別（稱為CATEGORY) 而配置：

1.惡意軟體偵測

2.潛在不需要的應用程式

3.潛在不安全

4.可疑應用程式

利用偵測引擎執行的報告，包括機器學習元件。您可設定高於目前防護閾值的報告閾值。這些報告設定不會影響封鎖、清除或刪除物件

請先閱讀下列資訊，然後再修改 CATEGORY 報告的閾值（或層級）：

閥值	說明
越權	配置為最大敏感度的 CATEGORY 報告。報告了更多偵測項目。［**越權**］設定可能將物件錯誤判斷為 CATEGORY
平衡	配置為平衡的 CATEGORY 報告。此設定已經過最佳化處理，而可平衡效能及偵測率的準確性，以及錯誤報告物件的數量。
警告	在維持足夠防護層級時，配置為盡量減少錯誤識別物件的 CATEGORY 報告。只會在可能性顯而易見且符合 CATEGORY 行為時，才會報告物件。
關閉	CATEGORY 的報告不在使用中，而且找不到、未報告或未清除此類型的偵測。因此，此設定會停用此偵測類型的防護。 關閉不適用於惡意軟體報告，而且它是潛在不安全的應用程式預設值。

ESET Internet Security 防護模組的可用性

所選取 CATEGORY 閥值之防護模組的可用性（已啟用或已停用）如下：

	越權	平衡	警告	關閉*
進階機器學習模組	✓ （越權模式）	✓ （保留模式）	X	X
偵測引擎模組	✓	✓	✓	X
其他防護模組	✓	✓	✓	X

*不建議。

決定產品版本、程式模組版本和組建日期

1. 按一下［**說明及支援**］>［**關於 ESET Internet Security**］。
2. 在［**關於**］畫面中，第一行文字顯示 ESET 產品的版本號碼。
3. 按一下［**已安裝的元件**］來存取特定模組的相關資訊。

基調

為您的環境設定適當閥值時有數個基調：

- 建議大部分設定使用［**平衡**］閥值。
- 報告閥值越高，偵測率就越高，但錯誤識別物件的機會也隨之提高。
- 從真實世界的觀點來看，無法保證 100% 偵測率，以及將已清除的物件分類為惡意軟體的機會無法保證為 0。
- 將 ESET Internet Security 及其模組保持最新，以在偵測率的效能及正確性與錯誤報告物件的數目之間達到最佳平衡。

防護設定

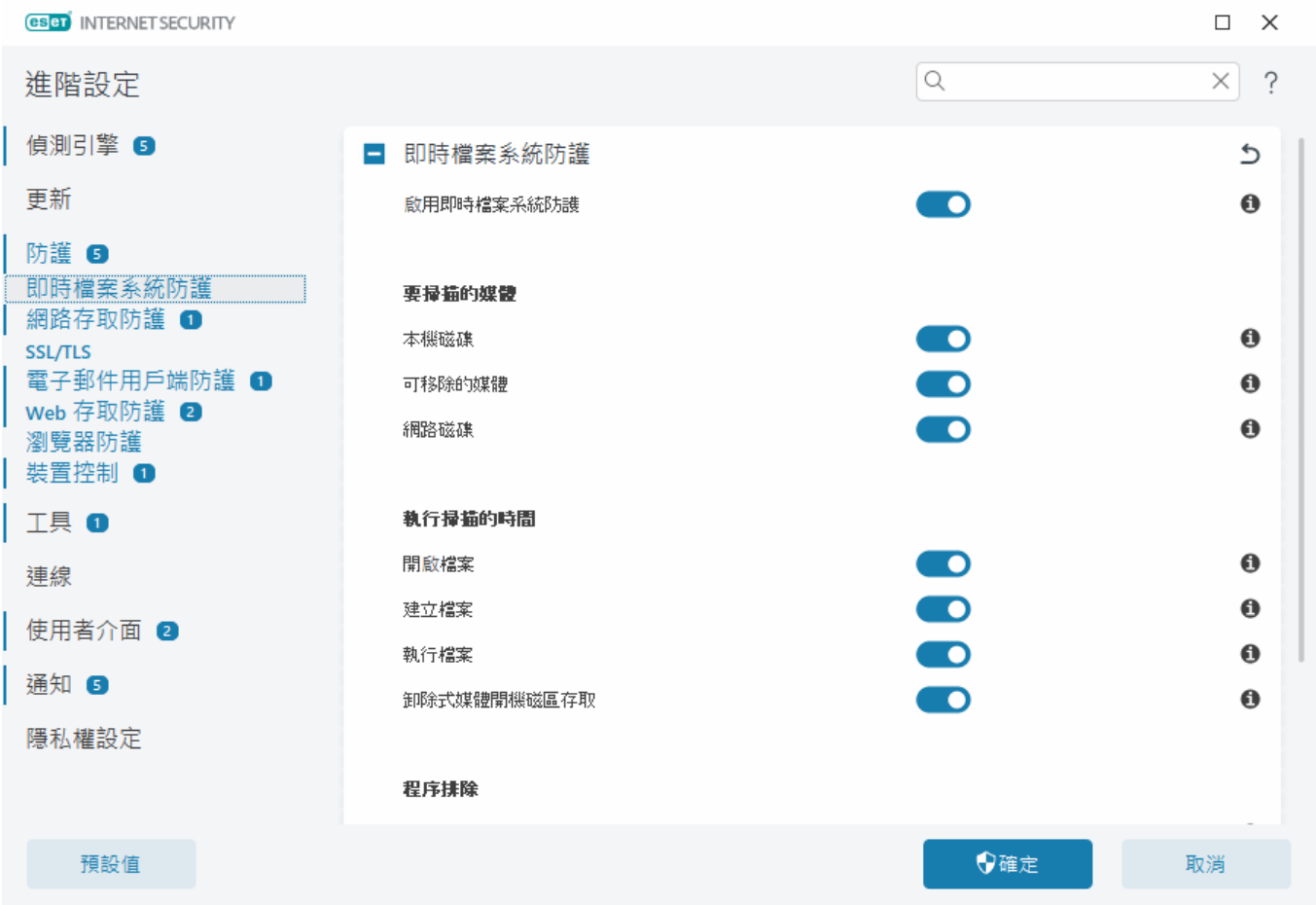
如果報告分類為 CATEGORY 的物件，則程式會封鎖此物件，然後清除、刪除或將其移至隔離區。

請先閱讀下列資訊，然後再修改 CATEGORY 防護的閥值（或層級）：

閥值	說明
越權	報告的越權（或較低）層級偵測會遭到封鎖，而且會啟動自動修復（例如，清除）。掃描所有端點是否有越權設定且已將錯誤報告物件新增至偵測排除時，建議使用此設定。
平衡	報告的平衡（或較低）層級偵測會遭到封鎖，而且會啟動自動修復（例如，清除）。
警告	報告的警告層級偵測會遭到封鎖，而且會啟動自動修復（例如，清除）。
關閉	對於識別及排除錯誤報告的物件很有幫助。 關閉不適用於惡意軟體防護，而且它是潛在不安全的應用程式預設值。

即時檔案系統防護

即時檔案系統防護可控制系統中的所有檔案，以在開啟、建立或執行檔案時找出惡意程式碼。



依預設，即時檔案系統防護會在系統啟動時同時啟動，並持續提供不中斷的掃描。我們不建議在 **[進階設定]** > [防護] > **[即時檔案系統防護]** > **[即時檔案系統防護]** 中停用 **[啟用即時檔案系統防護]**。

要掃描的媒體

依預設，會掃描所有媒體類型是否有潛在的威脅：

- **[本機磁碟機]** – 掃描所有系統和固定硬碟機（範例：*C:*、*D:*）
- **[卸除式媒體]** – 掃描 CD/DVD、USB 儲存裝置、記憶卡等

- **[網路磁碟機]** – 掃描所有對應的網路磁碟機（範例：*H:* 對應為 *\\store04*）或直接存取網路磁碟機（範例：*\\store08*）。

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

執行掃描的時間

依預設，開啟、建立和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]** – 在開啟檔案時掃描。
- **[建立檔案]** – 掃描已建立或已修改的檔案。
- **[執行檔案]** – 在執行檔案時掃描。
- **[卸除式媒體開機磁區存取]** – 當包含開機磁區的卸除式媒體插入裝置中時，系統會立即掃描開機磁區。此選項不會啟用卸除式媒體檔案掃描。卸除式媒體檔案掃描位於 **[要掃描的媒體] > [卸除式媒體]**。若要使 **[卸除式媒體開機磁區存取]** 正常運作，請在 ThreatSense 中將 **[開機磁區/UEFI]** 保持為啟用狀態。

程序排除

請參閱程序排除。

ThreatSense

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 中所述），即時檔案系統防護可配置為將新建立的檔案與現有檔案區別對待。例如，您可以配置即時檔案系統防護以更密切監視新建立的檔案。

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

即時檔案系統防護還可讓您配置其他 ThreatSense 參數。

程序排除

程序排除功能可讓您從即時檔案系統防護中排除應用程式程序。為了改善備份速度、程序完整性和服務可用性，在備份期間會使用有些已知會與檔案層級惡意軟體防護相衝突的技術。嘗試即時遷移虛擬機器時，可能會發生類似問題。透過排除特定程序（例如備份解決方案的程序），系統會略過所有可歸因於排除程序的檔案作業並將其視為安全，因而將備份程序的干擾降至最低。我們建議您在建立排除時格外小心 – 已排除的備份工具可以存取受感染的檔案，但不會觸發警告，這就是為何只允許在即時防護模組中使用擴充的權限。

請勿將排除的副檔名、HIPS 排除、偵測排除或效能排除混淆。

程序排除有助於將潛在衝突的風險降至最低，以及改善已排除應用程式的效能，這會對作業系統的整體效能和穩定性帶來正面影響。排除程序/應用程式就是排除其可執行檔（*.exe*）。

您可以在［進階設定］>［防護］>［即時檔案系統防護］>［即時檔案系統防護］>［程序排除］中將可執行檔新增至排除的程序清單中。

這項功能旨在排除備份工具。從掃描中排除備份工具的程序不僅可確保系統穩定性，而且也不會影響備份效能，因為備份在執行時不會變慢。

按一下［編輯］以開啟［程序排除］管理視窗，您可以在其中新增排除及瀏覽可執行檔（例如 *Backup-tool.exe*），該檔案將會從掃描中排除。
將 *.exe* 檔案新增至排除後，ESET Internet Security 就不會監視此程序的活動，而且不會對此程序所執行的任何檔案作業執行掃描。

如果未在選取程序可執行檔時使用瀏覽功能，則必須手動輸入可執行檔的完整路徑。否則，排除無法正常運作且 HIPS 可能會回報錯誤。

您也可以**編輯**現有的程序或將其從排除中**刪除**。

Web 存取防護不會將此排除納入考量，所以如果您排除 Web 瀏覽器的可執行檔，仍會掃描已下載的檔案。如此一來，仍可偵測到入侵。此案例只是範例而已，我們不建議您針對Web瀏覽器建立排除。

新增或編輯程序排除

此對話方塊可讓您［新增］已從偵測引擎中排除的程序。程序排除有助於將潛在衝突的風險降至最低，以及改善已排除應用程式的效能，這會對作業系統的整體效能和穩定性帶來正面影響。排除程序/應用程式就是排除其可執行檔（*.exe*）。

按一下［...］（例如 *C:\Program Files\Firefox\Firefox.exe*），選取已排除應用程式的檔案路徑。「請勿」輸入應用程式的名稱。
將 *.exe* 檔案新增至排除後，ESET Internet Security 就不會監視此程序的活動，而且不會對此程序所執行的任何檔案作業執行掃描。

如果未在選取程序可執行檔時使用瀏覽功能，則必須手動輸入可執行檔的完整路徑。否則，排除無法正常運作且 HIPS 可能會回報錯誤。

您也可以**編輯**現有的程序或將其從排除中**刪除**。

何時修改即時防護配置

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

安裝 ESET Internet Security之後，所有設定都已最佳化，為使用者提供最高層級的系統安全。若要還原預設設定，請按一下［進階設定］>［防護］>［偵測回應］旁邊的 。

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 *www.eicar.com* 的測試檔案。此測試檔案是所有防毒程式都可偵測到的無害檔案。該檔案由 EICAR (European Institute for Computer Antivirus Research) 公司建立，用來測試防毒程式的功能。

可在此處下載檔案：http://www.eicar.org/download/eicar.com

在您將此 URL 輸入至瀏覽器之後，應該會看到已移除威脅的訊息。

即時防護無法運作時怎麼辦

在本章中，我們說明使用即時防護時可能發生的問題，以及如何疑難排解這些問題。

已停用即時防護

如果使用者無意中停用即時防護，您應該重新啟動該功能。若要重新啟用即時防護，請移至主要程式視窗中的 **[設定]**，然後按一下 **[電腦防護] > [即時檔案系統防護]**。

如果在系統啟動時未啟動即時防護，通常是由於已停用 **[啟用即時檔案系統防護]**。若要確保啟用此選項，請開啟 [進階設定] > **[防護] > [即時檔案系統防護]**。

如果即時防護不會偵測及清除入侵

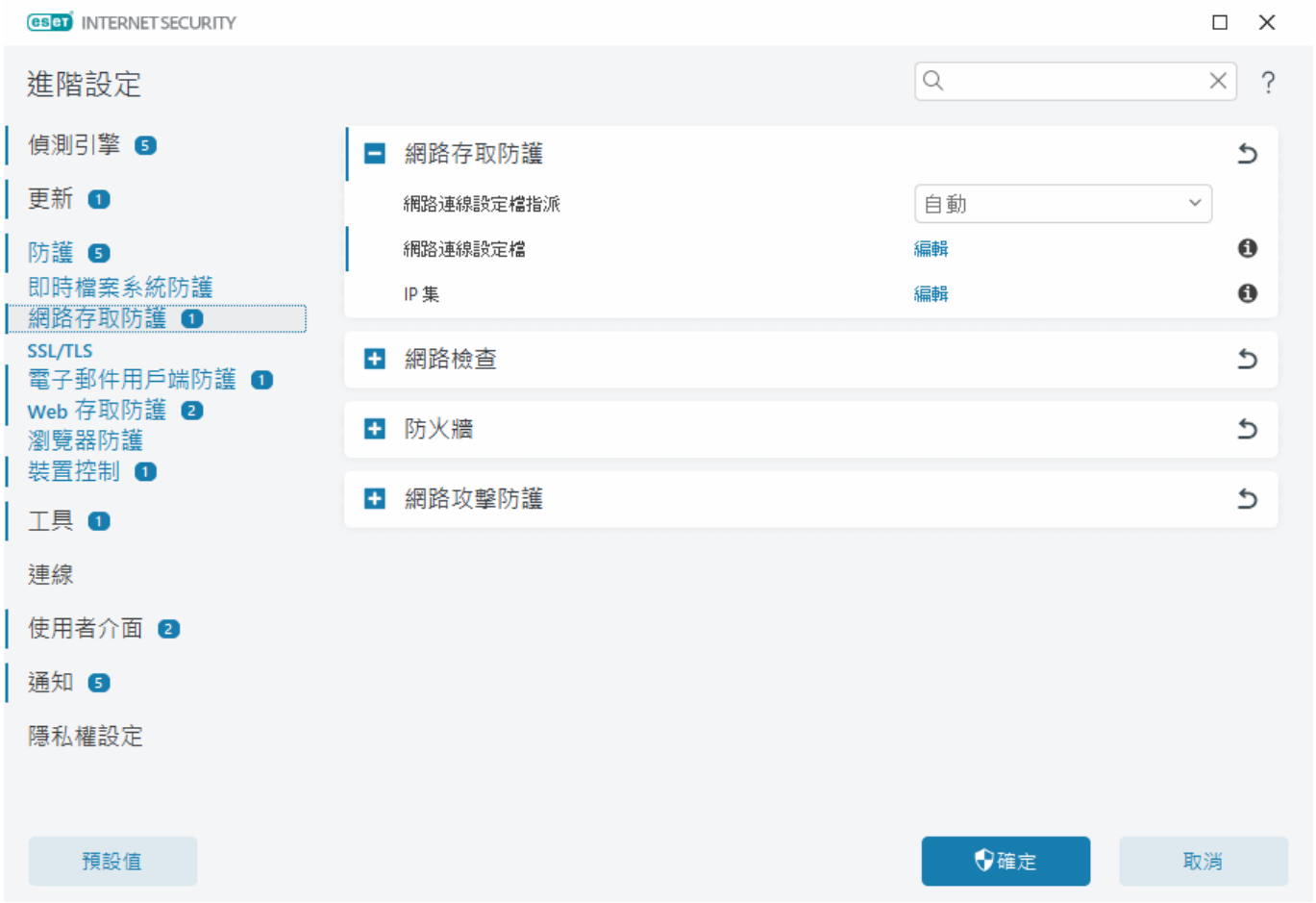
請確定電腦上未安裝任何其他防毒程式。若您同時安裝兩個防毒程式，它們可能會與彼此衝突。我們建議您先解除安裝系統上的任何其他防毒程式，再安裝 ESET。

即時防護未啟動

如果在系統啟動時未啟動即時防護（且已啟用 **[啟用即時檔案系統防護]**），則可能是由於與其他程式發生衝突。如需解決此問題，請建立 ESET SysInspector 防護記錄，並提交至 ESET 技術支援進行分析。

網路存取防護

網路存取防護使您能夠詳細配置所有網路連線。您可以根據配置允許/拒絕特定網路上對您電腦的存取，允許/拒絕從電腦存取網路裝置等等。根據預設，ESET Internet Security 具有預先配置的防火牆規則和網路存取防護，以實現最大的安全性。但是，特定環境可能需要自訂配置。應僅由有經驗的使用者變更預設設定。



您可以在 [進階設定] > **[防護]** > **[網路存取防護]**（按一下下方的連結以取得每個網路存取防護選項的詳細描述）配置以下設定：

網路存取防護

網路連線設定檔 – 您可以使用設定檔來控制特定網路連線的防火牆行為。

IP 集 – 您可以定義 IP 位址的集合，這些集合建立一個 IP 位址的邏輯群組，可以用於防火牆規則。

網路檢查

防火牆

網路攻擊防護

網路連線設定檔

設定檔可用於控制特定網路連線的 ESET Internet Security 網路防護行為。建立或編輯防火牆規則時，IDS 規則或暴力密碼破解攻擊防護規則，您可以將其指派給特定設定檔，也可以將其套用至所有設定檔。當設定檔在網路連線上作用中時，只會套用全域規則（未指定設定檔的規則）與已經指派給該設定檔的規則。您可以使用指派給網路連線的不同規則建立多個設定檔，以輕鬆變更防火牆行為。

您可以在 [進階設定] > **[防護]** > **[網路存取防護]** > **[網路存取防護]** 中配置網路連線設定檔和指派。

網路連線設定檔指派 – 可讓您選擇是否根據網路連線設定檔中配置的啟動項自動（從下拉式功能表中選取 **[自動]**）為新發現的網路連線指派預先定義或自訂設定檔，或者是否希望每次偵測到新的網路連線時都詢問您（從下拉式功能表中選取 **[詢問]**）以配置網路防護並手動指派設定檔。

您還可以在［主程式視窗］>［設定］>［網路防護］>［網路連線］中手動指派特定網路連線設定檔。將滑鼠暫留在特定網路連線上，然後按一下功能表圖示 ⋮ >［編輯］以開啟配置網路防護視窗並選取設定檔。

網路連線設定檔 – 按一下［編輯］以新增或編輯網路連線設定檔。

以下設定檔是預先定義的，無法編輯/刪除：

私人 – 適用於信任的網路（家用或辦公室網路）。您的電腦和儲存在您電腦上的共用檔案可供其他網路使用者查看，且網路上其他使用者可以存取系統資源（啟用了對共用檔案和印表機的存取，啟用了對內 RPC 通訊，並且遠端桌面共用可用）。建議您在存取安全的區域網路時使用此設定。如果設定檔在 Windows 中配置為網域或私人網路，則會自動將其指派給網路連線。

公用 – 適用於不信任的網路（公用網路）。您系統上的檔案和資料夾未與網路上其他使用者共用或設為可見，系統資源分享將停用。建議您在存取無線網路時使用此設定。此設定檔將自動指派給 Windows 中未配置為網域或私人網路的任何網路連線。

當網路連線切換至其他設定檔時，畫面右下角會出現通知。

新增或編輯網路連線設定檔

您可以在［進階設定］>［防護］>［網路存取防護］>［網路存取防護］>［網路連線設定檔］>［編輯］中新增或編輯網路連線設定檔。若要編輯設定檔，必須從［網路連線設定檔］視窗清單中選取它。

以下設定檔是先預定義的，無法編輯/刪除：

私人 – 適用於信任的網路（家用或辦公室網路）。您的電腦和儲存在您電腦上的共用檔案可供其他網路使用者查看，且網路上其他使用者可以存取系統資源（啟用了對共用檔案和印表機的存取，啟用了對內 RPC 通訊，並且遠端桌面共用可用）。建議您在存取安全的區域網路時使用此設定。如果設定檔在 Windows 中配置為網域或私人網路，則會自動將其指派給網路連線。

公用 – 適用於不信任的網路（公用網路）。您系統上的檔案和資料夾未與網路上其他使用者共用或設為可見，系統資源分享將停用。建議您在存取無線網路時使用此設定。此設定檔將自動指派給 Windows 中未配置為網域或私人網路的任何網路連線。

頂端/向上/向下/低端  – 允許您調整網路連線設定檔的優先順序層級（網路連線設定檔依其優先順序進行評估和套用。一律套用第一個相符的設定檔）。

新增或編輯設定檔

自訂網路連線設定檔使您能夠套用防火牆規則並為特定網路連線定義其他設定。您將在啟動項區段中指定自訂設定檔將指派給哪些網路連線。

若要開啟設定檔編輯器，請在［網路連線設定檔］視窗中：

- 按一下［新增］。
- 選取其中一個現有設定檔，然後按一下［編輯］。
- 選取其中一個現有設定檔，然後按一下［複製］。

名稱 – 設定檔的自訂名稱。

描述 – 設定檔的描述，可協助識別設定檔。

其他信任的位址 – 此處定義的位址將新增至已套用此設定檔的網路連線之信任區域（無論網路的防護類型爲何）。

信任連線 – 您的電腦和儲存在您電腦上的共用檔案可供其他網路使用者查看，且網路上其他使用者可以存取系統資源（啟用了對共用檔案和印表機的存取，啟用了對內 RPC 通訊，並且遠端桌面共用可用）。建議在為安全的本機網路連線建立設定檔時使用此設定。所有直接連線的網路子網路也視為受信任。例如，若網路介面卡使用 IP 位址 192.168.1.5 和子網路遮罩 255.255.255.0 連線至此網路，則子網路 192.168.1.0/24 會新增至該網路連線的信任區域。如果介面卡具有更多位址/子網路，則所有位址/子網路都將受信任。

[報告弱式 WiFi 加密] – ESET Internet Security 會在您連線至未受保護的無線網路或防護不足的網路時顯示桌面通知

啟動項 – 將此網路連線設定檔指派給網路連線必須滿足的自訂條件。有關詳細說明，請參閱啟動項

啟動項

啟動項是將網路連線設定檔指派給網路連線時必須滿足的自訂條件。如果已連線網路具有與已連線網路設定檔之啟動項中定義的相同屬性，則該設定檔將套用至網路。網路連線設定檔可以有一個或多個啟動。如果有多個啟動項，則 OR 邏輯適用（必須至少滿足一個條件）。您可以在網路連線設定檔編輯器中定義啟動項。應由有經驗的使用者建立自訂網路連線設定檔。

以下啟動項可用（如果您想知道目前網路的詳細資料，請參閱網路連線）

介面卡

介面卡類型 – 如果在所選介面卡類型上建立了網路連線，則套用設定檔。
介面卡名稱 – 如果網路介面卡名稱相符，則套用設定檔。
介面卡 IP – 如果網路介面卡的 IP 位址相符，則套用設定檔。

DNS

DNS 尾碼 – 如果網域名稱相符，則套用設定檔。
DNS IP – 如果 DNS 伺服器 IP 位址相符，則套用設定檔。

WINS

如果 Windows Internet Name Service (WINS) 對應的 IP 位址相符，則套用設定檔。

DHCP

DHCP IP – 比對 DHCP 伺服器 IP 位址。

預設閘道

IP – 如果預設閘道 IP 位址相符，則套用設定檔。
MAC 位址 – 如果預設閘道 MAC 位址相符，則套用設定檔。

Wi-Fi

SSID – 如果 SSID (Wi-Fi 的名稱) 相符，則套用設定檔。
設定檔名稱 – 如果 Wi-Fi 設定檔名稱相符，則套用設定檔。
安全性類型 – 如果安全性類型與從下拉式功能表中選取的安全性類型相符，則套用設定檔。如果要比對多個啟動項，請建立另一個啟動項。
加密類型 – 如果加密類型與從下拉式功能表中選取的加密類型相符，則套用設定檔。如果要比對多個啟動項，請建立另一個啟動項。
網路安全性 – 如果網路為 **[開放]/[安全]** 狀態，則套用設定檔。

Windows 設定檔

如果網路在 Windows 中配置為 **[網域]/[私人]/[公用]**，則套用設定檔。

驗證

「網路驗證」會搜尋網路中的特定伺服器，並使用非對稱式加密 (RSA) 來驗證伺服器。驗證的網路之名稱必須與驗證伺服器設定中設定的名稱相符。該名稱區分大小寫。伺服器名稱可以鍵入為 IP 位址、DNS 或 NetBios 名稱。
下載 ESET 驗證伺服器
公用金鑰可以用下列任一種檔案類型匯入：
• PPEM 加密公用金鑰 (.PEM)可以使用 ESET 驗證伺服器產生此金鑰
• 加密公用金鑰
• 公用金鑰憑證 (.crt)
按一下 **[測試]** 以測試您的設定。如果驗證成功，則會顯示伺服器驗證成功。如果未正確配置驗證，則會顯示以下其中一個錯誤訊息：
伺服器驗證失敗。簽章無效或不相符。
伺服器簽章與輸入的公用金鑰不相符。
伺服器驗證失敗。網路名稱不相符。
已配置的網路名稱無法對應驗證伺服器網路名稱。檢閱這兩個名稱，並確認其名稱相同。
伺服器驗證失敗。無效或伺服器無回應。
若伺服器並未執行或無法存取，則無法接收回應。若其他的 HTTP 伺服器於指定位址執行，則可能會接收到無效的回應。
輸入的公用金鑰無效。
驗證您輸入的公用金鑰檔案並未損毀。

IP 集

IP 集是建立一個 IP 位址邏輯群組的 IP 位址集合，在多個防火牆規則或暴力密碼破解攻擊防護規則中重複使用同一組位址時非常有用。ESET Internet Security 還包含套用了內部規則的預先定義 IP 集。此類群組的一個範例為 **[信任區域]**。信任區域表示網路位址群組，其中您的電腦和儲存在您電腦上的共用檔案可供其他網路使用者查看，網路上其他使用者可以存取系統資源。

若要新增 IP 集：

1. 開啟 [進階設定] > **[防護]** > **[網路存取防護]** > **[IP 集]** > **[編輯]**。

2. 按一下 **[新增]**，輸入區域的 **[名稱]** 和**[說明]**，然後在 **[遠端電腦位址 (IPv4/IPv6、範圍、遮罩)]** 中輸入遠端 IP 位址。

3. 按一下 **[確定]**。

如需詳細資訊，請參閱編輯 IP 集。

編輯 IP 集

如需 IP 集的詳細資訊，請參閱 IP 集

直欄

[名稱] – 一組遠端電腦的名稱。

[說明] – 群組的一般說明。

[IP 位址] – 屬於 IP 集的遠端 IP 位址。

控制項元素

當您 **[新增]** 或 **[編輯]** IP 集時，下列欄位可用：

[名稱] – 一組遠端電腦的名稱。

[說明] – 群組的一般說明。

[遠端電腦位址 (IPv4IPv6範圍、遮罩)] – 可讓您新增遠端位址、位址範圍或子網路。

[刪除] – 從清單移除區域。

無法移除預先定義的 IP 集。

IP 位址範例

新增 IPv4 位址：

[單一位址] – 新增個別電腦的 IP 位址（例如，*192.168.0.10*）

[位址範圍] – 輸入開始及結尾位址 IP 位址以指定數台電腦的 IP 範圍（例如，*192.168.0.1-192.168.0.99*）

[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 子網路的網路遮罩。排除 *192.168.1.0/24* 中的整個子網路類型。

新增 IPv6 位址：

[單一位址] – 新增個別電腦的 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*）

網路檢查

[網路檢查] 可協助識別信任（家用或辦公室）網路弱點（例如已開啟的連接埠或弱式路由器密碼）。此功能也可提供給您已連線的裝置清單，並依照裝置類型分類（例如印表機、路由器、行動裝置等），來顯示連線到您網路的裝置（例如遊戲主機IoT 或其他智慧型家用裝置）。您可以在 [進階設定] > **[防護]** > **[網路存取防護]** > **[網路檢查]** 中設定網路檢查。

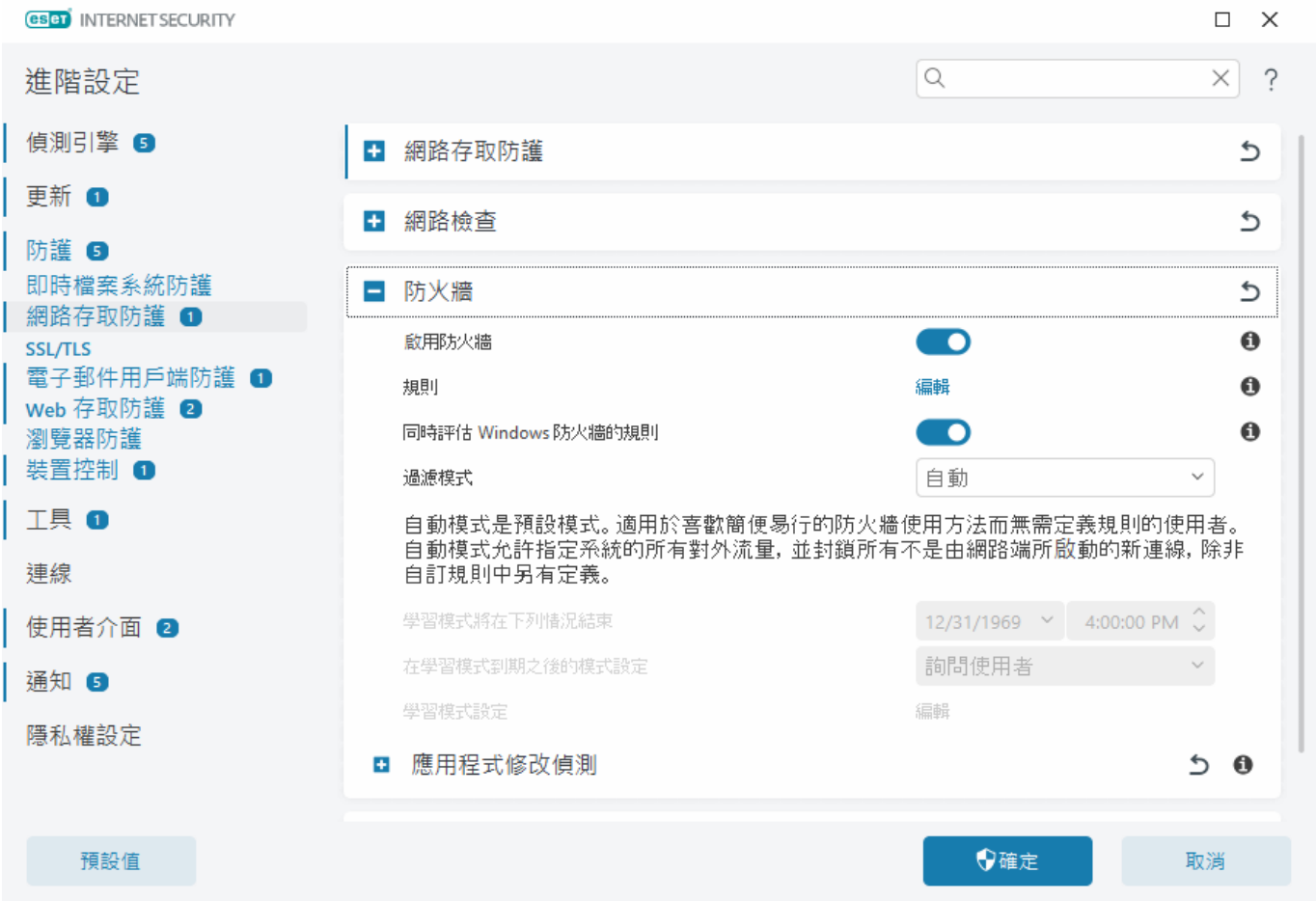
啟用「網路檢查」 – 網路檢查可幫助識別家用網路中的弱點，例如開啟的連接埠或弱式路由器密碼。另可提供按裝置類型分類的已連線裝置清單。

[針對新發現的網路裝置進行通知] – 在網路上偵測到新裝置時進行通知。

防火牆

防火牆根據內部規則和您定義的規則，控制電腦上的所有外來和對外網路流量。這是透過允許或拒絕個別網路連線來實現的。防火牆提供防護以免於遭受遠端裝置的攻擊，並封鎖有潛在威脅性的服務。

若要配置防火牆，請開啟 [進階設定] > [防護] > [網路存取防護] > [防火牆]。



防火牆

啟用防火牆

我們建議您保持啟用此功能以確保系統的安全性。啟用防火牆後，將雙向掃描網路流量。

規則

規則設定使您能夠檢視和編輯套用至受信任連線和網際網路內個別應用程式產生之流量的所有防火牆規則。

當遭到殭屍網路攻擊時，您可以為電腦建立 IDS 規則。可以在 [進階設定] > [防護] > [網路存取防護] > [網路攻擊防護] > [IDS 規則] 中按一下 [編輯] 修改規則。

同時評估 Windows 防火牆的規則

在自動過濾模式下，也允許 Windows 防火牆規則允許的傳入流量，除非 ESET 規則明確封鎖。

過濾模式

過濾模式 – 防火牆行為的變更係以過濾的模式為根據。過濾模式還影響需要使用者互動的層級。

ESET Internet Security 防火牆提供下列過濾模式：

過濾模式	說明
自動模式	預設模式。此模式適用於喜歡簡便易行的防火牆使用方法而無需定義規則的使用者。雖然可以建立自訂的使用者定義規則，不過【自動模式】並未強制使用這類規則。自動模式允許指定系統的所有對外流量，並封鎖大多數的外來流量，除了來自「信任區域」的某些流量（IDS 及進階選項/允許的服務所指定），以及最近對外通訊的回應。
互動模式	互動模式 – 讓您為防火牆建立自訂配置。當偵測到通訊但沒有適用的規則時，將會顯示一個對話方塊視窗，報告不明連線。該對話方塊視窗提供允許及拒絕通訊的選項，且允許或拒絕的決定將儲存成防火牆的新規則。如果您選擇建立新規則，則系統會根據該規則，允許或封鎖將來所有此類型的連線。
原則型模式	會封鎖所有尚未在特定規則中定義為允許的連線。此模式允許進階使用者定義僅允許所需及安全連線的規則。防火牆會封鎖所有其他未指定的連線。
學習模式	自動建立並儲存規則；此模式最適合用於防火牆的初始配置，但不應該長時間保持開啟。因為 ESET Internet Security 會根據預先定義的參數來儲存規則，所以不需要與使用者互動。在建立所需通訊的所有規則之後，您應停止使用學習模式以避免安全性風險。

學習模式的結束時間 – 設定學習模式自動結束的日期和時間。您也可以隨時手動關閉學習模式。

學習模式到期後的模式設定 – 定義 防火牆將在學習模式期間結束後還原為何種過濾模式。在上表中閱讀有關過濾模式的更多資訊。結束後，**[詢問使用者]** 選項需具備管理權限，才能對防火牆過濾模式執行變更。

學習模式設定 – 按一下 **[編輯]** 以配置用於儲存在學習模式中建立的規則之參數。

應用程式修改偵測

如果已修改的應用程式於防火牆規則存在的情況下嘗試建立連線，則應用程式修改偵測功能會顯示通知。

學習模式設定

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

此模式可能導致您的電腦暴露在風險中，建議您只用於防火牆的初始配置。

從 [進階設定] > **[防護]** > **[網路存取防護]** > **[防火牆]** > **[防火牆]** > **[過濾模式]** 中的下拉式功能表選取 **[學習]** 以啟動學習模式選項。按一下 **[學習模式設定]** 旁邊的 **[編輯]** 以配置以下選項：

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

來自受信任區域的傳入流量 – 受信任區域內的傳入連線範例是來自受信任區域的遠端裝置嘗試與您電腦上執行的本機應用程式建立通訊。

到受信任區域的傳出流量 – 本機應用程式嘗試與本機網路或受信任區域的網路中的另一個裝置建立連線。

傳入網際網路流量 – 嘗試與電腦上執行的應用程式通訊的遠端裝置。

傳出網際網路流量 – 嘗試與另一裝置建立連線的本機應用程式。

每個區段可讓您定義要加入新建立之規則的參數：

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

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

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

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

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

防火牆規則

防火牆規則代表一組條件，可用於有意義地測試所有網路連線，及所有指派給這些條件的動作。您可以使用防火牆規則定義在建立不同類型的網路連線時所要採取的動作。

規則從上到下進行評估，您可以在第一欄中看到其優先順序。第一個相符規則的處理方法會用於評估中的每個網路連線。

連線可劃分為對內及對外連線。對內連線是由嘗試與本機系統建立連線的遠端裝置所啟動。對外連線則相反，由本機系統連絡遠端裝置。

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對系統造成安全風險。如果建立此類連線，我們建議您注意嘗試連接您電腦的遠端裝置及應用程式。許多入侵嘗試取得及傳送私人資料，或將其他惡意應用程式下載到主機工作站。防火牆允許您偵測及終止此類連線。

您可以在 [進階設定] > **[防護]** > **[網路存取防護]** > **[防火牆]** > **[規則]** > **[編輯]** 中檢視和編輯防火牆規則。

如果有許多防火牆規則，則可以使用過濾器以僅顯示特定規則。若要過濾防火牆規則，請按一下防火牆規則清單上方 **[更多過濾器]**。您可以根據以下條件過濾規則：

- 來源
- 方向
- 處理方法
- 可用性

預先定義的防火牆規則預設隱藏。若要顯示所有預先定義的規則，請停用 **[隱藏內建（預先定義）規則]** 旁邊的切換開關。您可以停用這些規則，但您無法刪除預先定義的規則。

按一下右上方的搜尋圖示 以搜尋規則。

直欄

優先順序 – 規則從上到下進行評估，您可以在第一欄中看到其優先順序。

已啟用 – 顯示規則為已啟用或已停用，必須選取對應的核取方塊才能啟動規則。

應用程式 – 套用規則的應用程式。

方向 – 通訊的方向（對內/對外/兩者）。

處理方法 – 顯示通訊的狀態（封鎖/允許/詢問）。

名稱 – 規則的名稱ESET 圖示 表示預先定義的規則。

套用次數 – 套用規則的總次數。

按一下展開圖示 以顯示規則的詳細資料。

控制項元素

新增 – 建立新規則

編輯 – 編輯現有規則

刪除 – 移除現有規則。

複製 – 建立所選規則的副本。

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

新增或編輯防火牆規則

防火牆規則代表條件，可用於有意義地測試所有網路連線，及所有指派給這些條件的動作。當網路設定進行變更（例如，遠端的網路位址或連接埠號碼進行變更）時，可能需要編輯或新增防火牆規則，以確保受規則影響的應用程式的正常作業。有經驗的使用者應建立自訂防火牆規則。

圖解指示

下列 ESET 知識庫文章可能僅以英文提供：

- 使用防火牆開啟或關閉（允許或拒絕）特定連接埠
- 從 ESET Internet Security 的防護記錄檔案中建立防火牆規則

若要新增或編輯防火牆規則，請開啟 [進階設定] > [防護] > [網路存取防護] > [防火牆] > [規則] > [編輯]。在防火牆規則視窗中，按一下 [新增] 或 [編輯]。

名稱 – 鍵入規則的名稱。

已啟用 – 按一下切換開關以使規則作用中。

為防火牆規則新增處理方法和條件：

處理方法

處理方法 – 選取您是要 [允許]/[封鎖] 與此規則中定義之條件相符的通訊，還是要讓 ESET Internet Security 在每次建立通訊時 [詢問]。
防護記錄規則 – 如果套用了規則，它將記錄在防護記錄檔案中。
記錄嚴重性 – 選取此規則的防護記錄的嚴重性。
[通知使用者] – 會在套用規則時顯示通知。

應用程式

指定將套用此規則的應用程式。
應用程式路徑 – 按一下 **[...]** 並瀏覽到應用程式或鍵入應用程式的完整路徑（例如 C:\Program Files\Firefox\Firefox.exe）請勿單獨輸入應用程式的名稱。
應用程式簽章 – 您可以根據應用程式的簽章（發行者名稱）將規則套用至應用程式。請從下拉式功能表中選取是要將規則套用至具有 **[任何有效簽章]** 的應用程序或 **[由特定簽章者簽署的應用程式]**。如果選取 **[由特定簽章者簽署的應用程式]**，則必須在 **[簽章者名稱]** 欄位中定義簽章者。
Microsoft Store 應用程式 – 在下拉式功能表中選取從 Microsoft Store 安裝的應用程式。
服務 – 您可以選取系統服務而不是應用程式。開啟下拉式功能表以選取服務。
套用至子處理程序 – 某些應用程式可能會執行更多處理程序，而您只能看到一個應用程式視窗。按一下切換開關以為指定應用程式中的每個處理程序啟用規則。

方向

為此規則選取通訊 **[方向]**
- **兩者** – 對內和對外通訊
- **對內** – 僅對內通訊
- **對外** – 僅對外通訊

IP 通訊協定

如果您僅希望此規則套用至特定通訊協定，請從下拉式功能表中選取 **[通訊協定]**

本機主機

套用了此規則的本機位址、位址範圍或子網路。如果未指定位址，則規則將套用至與本機主機的所有通訊。您可以將 IP 位址、位址範圍或子網路直接新增至 **[IP]** 文字欄位中，也可以透過按一下 **[IP 集]** 旁邊的 **[編輯]** 從現有 IP 集中進行選取。

本機連接埠

本機**連接埠**號碼。如果未提供號碼，則規則將套用至任何連接埠。您可以新增單一通訊連接埠或通訊連接埠範圍。

遠端主機

套用了此規則的遠端位址、位址範圍或子網路。如果未指定位址，則規則將套用至與遠端主機的所有通訊。您可以將 IP 位址、位址範圍或子網路直接新增至 **[IP]** 文字欄位中，也可以透過按一下 **[IP 集]** 旁邊的 **[編輯]** 從現有 IP 集中進行選取。

遠端連接埠

遠端**連接埠**號碼。如果未提供號碼，則規則將套用至任何連接埠。您可以新增單一通訊連接埠或通訊連接埠範圍。

設定檔

防火牆規則可以套用至特定網路連線設定檔
任何 – 規則將套用至任何網路連線，不管使用的設定檔。
已選取 – 規則將根據所選取設定檔套用至特定網路連線。選取您想選取之設定檔旁的核取方塊。

我們會建立新規則，讓 Firefox Web 瀏覽器應用程式能存取 網際網路 / 區域網路網站。
1.在 **[處理方法]** 區段，選取 **[處理方法] > [允許]**
2.在 **[應用程式]** 區段中，指定網頁瀏覽器的 **[應用程式路徑]**（例如 C:\Program Files\Firefox\Firefox.exe）請勿單獨輸入應用程式的名稱。
3.在 **[方向]** 區段中，選取 **[方向] > [對外]**
4.在 **[IP 通訊協定]** 區段中，從 **[通訊協定]** 下拉式功能表中選取 **[TCP 與 UDP]**
5.在 **[遠端連接埠]** 區段中，新增 **[連接埠]** 號碼：*80,443* 以允許標準瀏覽。

應用程式修改偵測

如果已修改的應用程式於防火牆規則存在的情況下嘗試建立連線，則應用程式修改偵測功能會顯示通知。應用程式修改機制會暫時或永久地將原始應用程式的執行檔取代為其他應用程式執行檔（可避免濫用防火牆規則）。

請注意，通常這個功能並不是用來偵測任何應用程式的修改動作。其目的是為了避免濫用現有的防火牆規則，因此只會監控存在特定防火牆規則的應用程式。

若要編輯 **[應用程式修改偵測]**，請開啟 [進階設定] > **[防護]** > **[網路存取防護]** > **[防火牆]** > **[應用程式修改偵測]**

啟用應用程式修改偵測 – 如果選取，則程式會監視應用程式的變更（更新、感染及其他修改）。當已修改的應用程式嘗試建立連線時，防火牆會通知您。

[允許修改已簽署的（受信任）應用程式] – 若應用程式在修改前後的有效數位簽章相同，則不進行通知。

[從偵測中排除的應用程式清單] – 此視窗可讓您新增或移除允許修改不需通知的個別應用程式。

從偵測中排除的應用程式清單

ESET Internet Security 的防火牆會偵測存在規則之應用程式的變更（請參閱「應用程式修改偵測

在某些情況下，如果您不想讓防火牆檢查這些應用程式，則您可能不想針對部分應用程式使用此功能。

新增 – 系統會開啟視窗，可讓您選取應用程式來新增到已從修改偵測中排除的應用程式清單。您可以從具有開放式網路通訊正在執行應用程式的清單中，選擇防火牆規則存在的應用程式或新增特定的應用程式。

編輯 – 系統會開啟視窗，可讓您變更位於修改偵測中排除的應用程式清單上的應用程式位置。您可以從具有開放式網路通訊正在執行應用程式的清單中，選擇防火牆規則存在的應用程式，或手動變更位置。

[移除] – 在從修改偵測中排除的應用程式清單中移除項目。

網路攻擊防護 (IDS)

網路攻擊防護 (IDS) 可更適切地偵測已知弱點的利用情形。請閱讀詞彙表中關於網路攻擊防護的更多資訊。若要配置網路攻擊防護，請開啟 [進階設定] > **[防護]** > **[網路存取防護]** > **[網路攻擊防護]**

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

啟用殭屍網路防護 – 在電腦受到感染且 Bot 嘗試通訊時，根據一般模式偵測並封鎖與惡意指令及控制伺服器的通訊。請在字彙中閱讀更多有關殭屍網路防護的資訊。

IDS 規則 – 此選項可讓您配置進階過濾選項，以偵測可能會用來損害您電腦的數種類型攻擊與利用。

> **圖解指示**
> 下列 ESET 知識庫文章可能僅以英文提供：
> - 從 ESET Internet Security 中的 IDS 排除 IP 位址

網路防護偵測到的所有重要事件都儲存在防護記錄檔案中。如需詳細資訊，請參閱網路防護記錄

IDS 規則

在某些狀況中，入侵偵測服務 (IDS) 可能會將路由器或內部網路裝置之間的通訊偵測成潛在威脅。例如，您可以將已知為安全的位址新增至［自 IDS 區排除的位址］以略過 IDS

圖解指示
下列 ESET 知識庫文章可能僅以英文提供：
- 從 ESET Internet Security 中的 IDS 排除 IP 位址

管理 IDS 規則

- **［新增］** – 按一下以建立新的 IDS 規則。
- **［編輯］** – 按一下以編輯現有 IDS 規則。
- **［移除］** – 若您要從 IDS 規則清單中移除某個規則，則請選取並按一下。
- **頂端/向上/向下/底端** – 可讓您調整規則的優先順序層級（例外會依照最上到最下的形式來評估）。

規則編輯器

偵測 –偵測類型。

威脅名稱 – 您可以為某些可用的偵測指定威脅名稱。

應用程式 – 按一下［...］（例如 *C:\Program Files\Firefox\Firefox.exe*），選取已排除應用程式的檔案路徑。「請勿」輸入應用程式的名稱。

遠端 IP 位址 – 遠端 IPv4 或 IPv6 位址/範圍/子網路的清單。多個位址必須使用逗號分隔。

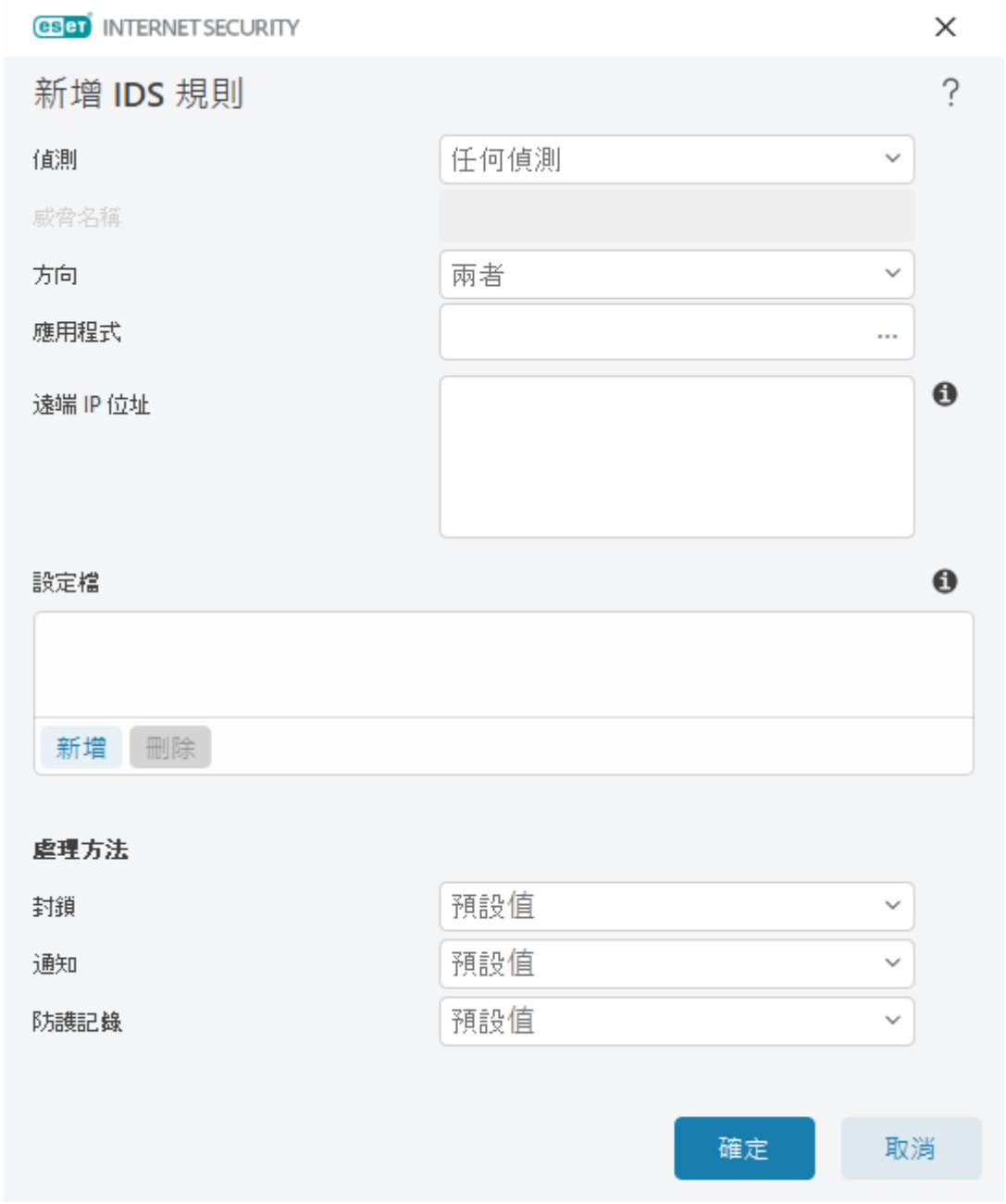
設定檔 – 您可以選擇將套用此規則的網路連線設定檔。

處理方法

封鎖 – 每個系統處理程序都有自己的預設行為和指派的處理方法（封鎖或允許）。若要覆寫 ESET Internet Security 的預設行為，您可以使用下拉式功能表來選擇封鎖或允許。

通知 – 選取［是］以在您的電腦上顯示［桌面通知］。如果您不要桌面通知，請選取［否］。可用的值為［預設值］/［是］/［否］。

防護記錄 – 選取**［是］**將事件記錄到防護記錄檔案。如果您不想要記錄事件，請選取**［否］**。可用的值為**［預設值］/［是］/［否］**。



如果您想要在每次發生事件時顯示通知及收集防護記錄：
1.按一下［**新增**］以新增 IDS 規則。
2.從［**偵測**］下拉式功能表中選取指定偵測。
3.針對您要套用此通知的項目按一下 **[...]**，以選擇應用程式路徑。
4.保留［**封鎖**］下拉式功能表中的［**預設值**］。這會繼承 ESET Internet Security 所套用的預設處理方法。
5.將［**通知**］和［**記錄**］下拉式功能表都設為［**是**］
6.按一下［**確定**］儲存此通知。

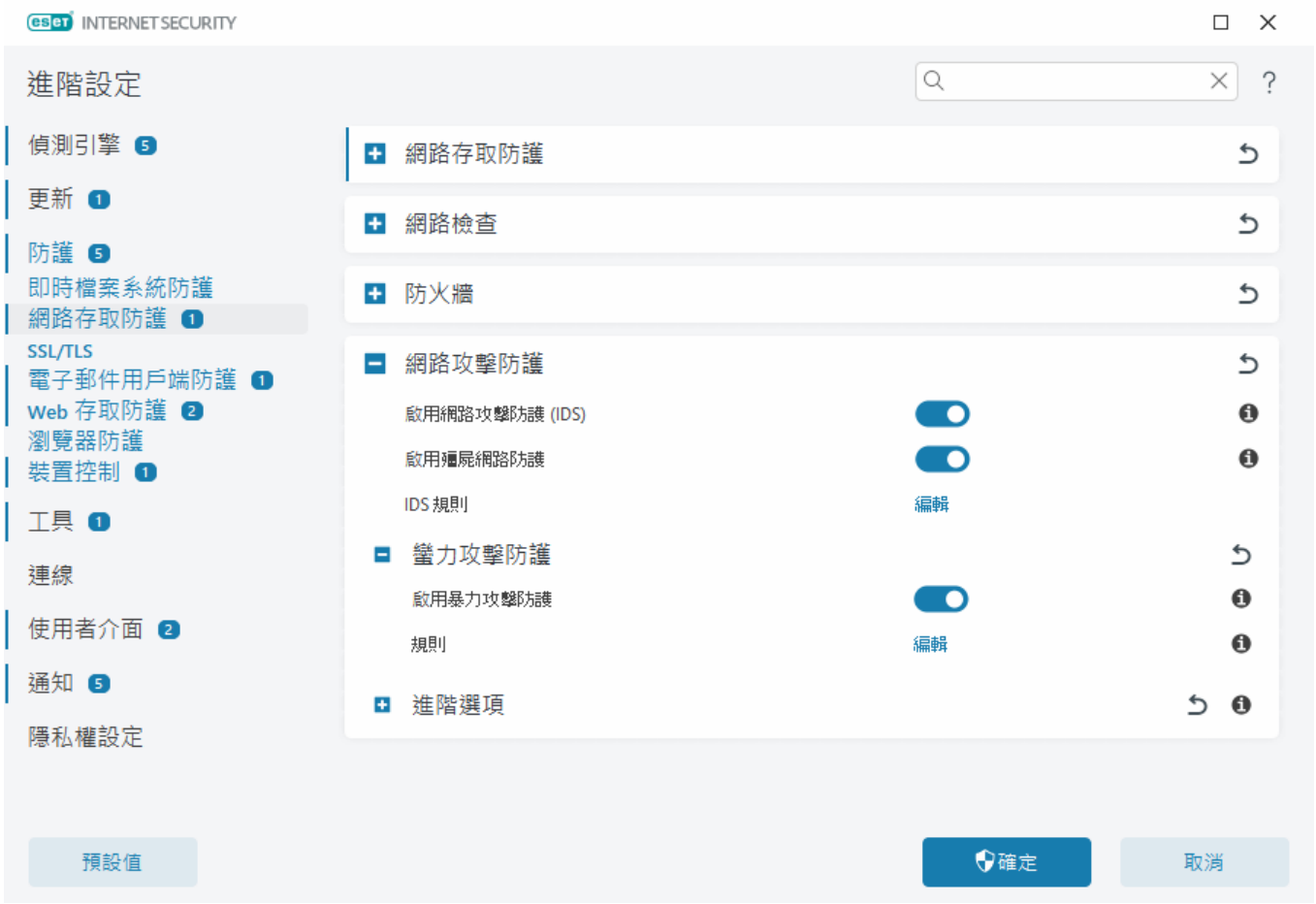
如果您想要針對並未視為特定［**偵測**］類型的威脅顯示週期性通知：
1.按一下［**新增**］以新增 IDS 規則。
2.從［**偵測**］下拉式功能表選取特定偵測，例如［**沒有安全延伸模組的 SMB 工作階段**］或［**傳輸控制通訊協定連接埠掃描攻擊**］
3.如果是來自外來通訊，則從下拉式功能表中選取［**外來**］
4.將［**通知**］下拉式功能表設為［**否**］
5.將［**記錄**］下拉式功能表設為［**是**］
6.將［**應用程式**］空白。
7.如果通訊不是來自特定 IP 位址，請將［**遠端 IP 位址**］保留空白。
8.按一下［**確定**］儲存此通知。

蠻力攻擊防護

暴力密碼破解攻擊防護可封鎖對 RDP 與 SMB 服務進行的密碼猜測攻擊。暴力密碼破解攻擊是一種透過系統性地嘗試字母、數字和符號的所有可能組合來發現目標密碼的方式。若要配置暴力密碼破解攻擊防護，請開啟［進階設定］> [**防護**] > [**網路存取防護**] > [**網路攻擊防護**] > [**暴力密碼破解攻擊防護**]

啟用暴力密碼破解攻擊防護 - ESET Internet Security 會檢查網路流量內容，並封鎖密碼猜測攻擊的嘗試。

規則 – 可讓您為傳入和傳出網路連線建立、編輯和檢視規則。如需詳細資訊，請參閱規則一章。



規則

暴力密碼破解攻擊防護規則允許您為傳入和傳出網路連線建立、編輯和檢視規則。無法編輯或刪除預先定義的規則。

管理暴力攻擊防護規則

新增 - 建立新規則。

編輯 - 編輯現有規則。

[刪除] - 將現有規則從規則清單中移除。

頂端/向上/向下/底端 - 調整規則的優先順序層級。

若要確保儘可能高的防護，當多個封鎖規則與偵測條件相符時，即使規則在規則清單中的位置較低，也會套用具有最低**最大嘗試次數**值的封鎖規則。

規則編輯器

名稱 – 規則的名稱。

已啟用 – 如果您想要將規則保留在清單中，但不想套用它，請停用切換開關。

[處理方法] – 選擇當滿足規則設定時，是要 **[拒絕]** 或 **[允許]** 連線。

[通訊協定] – 此規則將檢查的通訊協定。

設定檔 – 可以為特定設定檔設定和套用自訂規則。

最大嘗試次數 – 在封鎖 IP 位址並新增到黑名單之前，允許的攻擊重複嘗試的最大次數。

黑名單保留期（分鐘） – 設定位址在黑名單中到期的時間。

來源 IP – IP 位址/範圍/子網路清單。多個位址必須使用逗號分隔。

來源 IP 集 – 已在 IP 集中定義的 IP 位址集。

進階選項

在［進階設定］>［防護］>［網路存取防護］>［網路攻擊防護］>［進階選項］中，您可以啟用或停用偵測可能危害電腦之幾種類型的攻擊和利用。

在某些情況中，您將不會收到與通訊封鎖有關的威脅通知。請參閱「記錄並從防護記錄建立規則或例外」一節以取得關於在防火牆防護記錄中檢視所有已封鎖通訊的指示。

此視窗中可使用的特定選項會視您的 ESET 產品的類型或版本和防火牆模組，以及作業系統的版本而異。

入侵偵測

入侵偵測會監視裝置網路通訊是否存在惡意活動。

- **［通訊協定 SMB］** – 偵測並封鎖 SMB 通訊協定中的各種安全性問題
- **［通訊協定 RPC］** – 偵測並封鎖針對分散式運算環境 (DCE) 所開發遠端程序呼叫系統中的各種 CVE
- **［通訊協定 RDP］** – 偵測並封鎖 RDP 通訊協定中的各種 CVE (請參閱上述內容)。
- **[ARP Poisoning 攻擊偵測]** – 偵測「中間人(man-in-the-middle) 發動而導致的 ARP Poisoning 攻擊或偵測網路交換器上的探查。網路應用程式或裝置會使用 ARP (位址解析通訊協定) 來判斷 Ethernet 位址。
- **[TCP/UDP 連接埠掃描攻擊偵測]** – 偵測連接埠掃描軟體的攻擊 – 此應用程式可將用戶端要求傳送至特定的連接埠位址範圍以偵測已開啟連接埠的主機，其目的在於尋找作用中的連接埠並利用服務的弱點。請在字彙中閱讀更多有關此類型攻擊的資訊。
- **攻擊偵測之後封鎖不安全的位址** – 已偵測為攻擊來源的 IP 位址會新增至黑名單中以防止特定期間的連線。您可以定義**黑名單保留期**，其設定在偵測到攻擊後位址被封鎖的時長。
- **［攻擊偵測後顯示通知］** – 開啟畫面右下角的 Windows 通知區域通知。
- **也顯示針對安全漏洞傳入攻擊的通知** – 如果偵測到有針對安全漏洞的攻擊或者有威脅嘗試透過此方式進入系統，則也會警告您。

封包檢查

一種封包分析，會篩選正透過網路傳輸的資料。

- **允許外來連線連接至 SMB 通訊協定中的管理共用** – 管理共用 (admin shares) 是一種預設網路共用，可與系統資料夾（*ADMIN$*）共用系統中的硬碟分割區（*C$*、*D$*、...）。。 停用與管理共用的連線將可減輕許多安全風險。例如Conficker 蠕蟲會執行字典攻擊以連線至管理共用項目。
- **［拒絕舊（不支援）的 SMB 方言］** – 拒絕使用 IDS 不支援之舊 SMB 方言的 SMB 工作階段。新的 Windows 作業系統會因為與舊版作業系統（例如 Windows 95) 的舊版相容性而支援舊的 SMB 方言。攻擊者可在 SMB 工作階段中使用舊方言以規避流量檢查。如果您的電腦不需要與舊版 Windows 的電腦共用檔案（或使用一般的 SMB 通訊），請拒絕舊的 SMB 方言。
- **［拒絕不含延伸安全性的 SMB 工作階段］** – 您可以在 SMB 工作階段交涉期間使用延伸的安全性，以提供比 LAN Manager 挑戰/回應 (LM) 驗證更安全的驗證機制LM 配置是一種較薄弱的機制，因此不建議您使用。

• **［拒絕在 SMB 通訊協定中開啟「信任區域」外伺服器上的執行檔］** – 當您嘗試在防火牆中從不屬於信任區域的伺服器共用資料夾開啟可執行檔 (.exe、.dll) 時，連線將會中斷。請注意，從受信任的來源複製可執行檔可能是合法的。請注意，從信任來源複製執行檔是合法的，然而，此偵測可減輕因在惡意伺服器上開啟不需要的檔案而造成的風險（例如，因使用者按一下共用的惡意執行檔連結就能開啟的檔案）。

• **［拒絕] SMB 通訊協定中用於連線「信任區域」中的 NTLM 驗證］** – 使用 NTLM(兩種版本）驗證配置的通訊協定可能會受到憑證轉送攻擊（在 SMB 通訊協定的情況中亦稱為 SMB Relay 攻擊）。拒絕伺服器位於「信任區域」以外的 NTLM 驗證應可減輕「信任區域」以外之惡意伺服器轉送憑證所造成的風險。同樣地，您可以拒絕伺服器位於「信任區域」之內的 NTLM 驗證。

• **允許與「安全性帳戶管理員」服務通訊** – 如需有關此服務的詳細資訊，請參閱 [MS-SAMR]。

• **允許與「本機安全性授權」服務通訊** – 如需有關此服務的詳細資訊，請參閱[MS-LSAD] 和 [MS-LSAT]。

• **允許與「遠端登錄」服務通訊** – 如需有關此服務的詳細資訊，請參閱 [MS-RRP]。

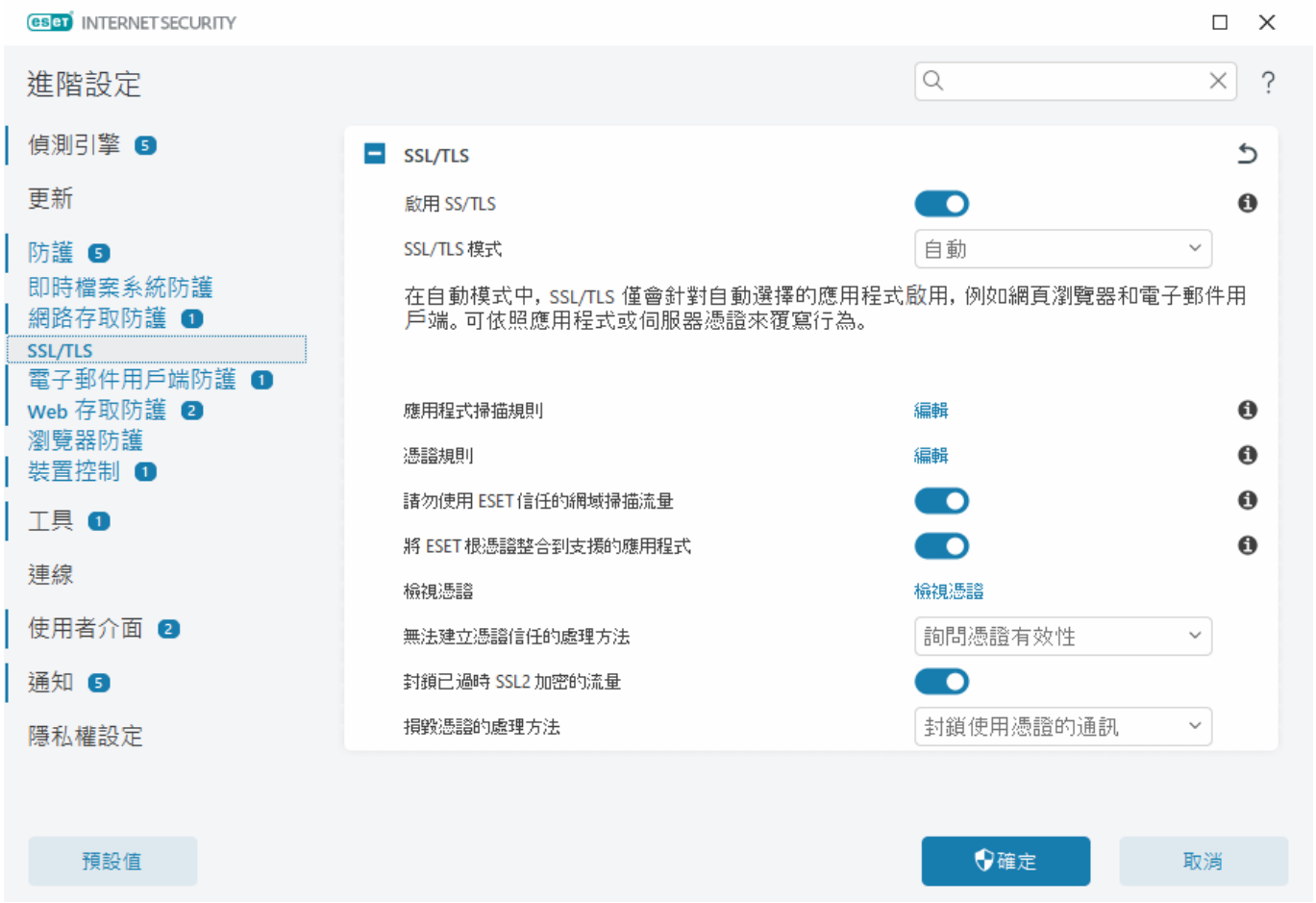
• **允許與「服務控制管理員」服務通訊** – 如需有關此服務的詳細資訊，請參閱 [MS-SCMR]。

• **允許與「伺服器」服務通訊** – 如需有關此服務的詳細資訊，請參閱 [MS-SRVS]。

• **允許與其他服務通訊** – 其他 MSRPC 服務。MSRPC 是 Microsoft 對於 DCE RPC 機制的實作。此外，MSRPC 可使用在 SMB (網路檔案共用）通訊協定中執行的具名管道進行傳輸 (ncacn_np 傳輸)。MSRPC 服務可提供遠端存取及管理 Windows 系統的介面。我們在 Windows MSRPC 系統中發現數種「逍遙法外」的安全性弱點 (Conficker 蠕蟲、Sasser 蠕蟲…）。停用一些您不需要的 MSRPC 服務通訊可減輕許多安全風險（例如遠端程式碼執行或服務失敗攻擊）。

SSL/TLS

ESET Internet Security 可以檢查使用 SSL 通訊協定的通訊威脅。對於使用信任的憑證、未知憑證或排除在 SSL 防護通訊檢查之外的憑證進行的 SSL 防護通訊，您可以運用各種篩選模式來檢查。若要編輯 SSL/TLS 設定，請開啟［進階設定］> **［防護］> [SSL/TLS]**。



啟用 SSL/TLS – 若停用ESET Internet Security 不會掃描 SSL/TLS 上的通訊。

SSL/TLS 模式提供下列選項：

過濾模式	說明
自動	預設模式僅會掃描適當的應用程式，例如網頁瀏覽器和電子郵件用戶端。您可以透過選取在其中掃描通訊的應用程式來覆寫它。
互動	如果您輸入新的 SSL 防護網站（含有未知憑證），則會顯示處理方式選取項目對話方塊。此模式可讓您建立將排除在掃描之外的 SSL 憑證/應用程式列在其中的清單。
原則型	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。使用標記為受信任的不信任憑證（其在受信任憑證清單中）存取伺服器時，允許與伺服器進行通訊，並過濾通訊通道內容。

應用程式掃描規則 – 允許您自訂針對特定應用程式的 ESET Internet Security 行為。

憑證清單 – 可讓您自訂針對特定 SSL 憑證的 ESET Internet Security 行為。

不掃描 ESET 信任的網域之流量 – 啟用後，將從掃描中排除與受信任網域的通訊ESET 管理的內建白名單決定了網域的可信度。

將 ESET 根憑證整合到支援的應用程式 – 為了使 SSL 通訊能在瀏覽器/電子郵件用戶端中正常運作，您需要將 ESET 的系統管理員憑證新增至已知系統管理員憑證（發行者）的清單中。啟用後ESET Internet Security 可自動將 ESET SSL Filter CA 憑證新增至已知瀏覽器中（例如 Opera)對於使用系統憑證儲存區的瀏覽器來說，憑證會自動新增。例如 Firefox 會自動配置為信任系統憑證儲存區中的根驗證。

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

無法建立憑證信任時的處理方式 – 在某些情況下，無法使用信任的根憑證授權 (TRCA) 存放區驗證網站憑

證（例如，過期的憑證、不信任的憑證、對特定網域無效的憑證或可以剖析但未正確簽署憑證的簽章）。合法網站將一律使用信任的憑證。如果它們不提供，則可能表示攻擊者正在解密您的通訊或網站發生技術問題。

如果選取了**［詢問憑證有效性］**（預設選取），系統就會在建立加密通訊時提示使用者選擇處理方式。會顯示處理方式選取項目對話方塊，您能在該處決定將憑證標示為信任或排除。如果 TRCA 清單中沒有憑證，視窗就會變成紅色。如果 TRCA 清單中有憑證，視窗就會變成綠色。

您可以選取**［封鎖使用憑證的通訊］**，一律終止與使用不信任憑證之網站的加密連線。

封鎖由過時 SSL2 加密的流量 – 將自動封鎖使用舊版 SSL 通訊協定的通訊。

針對已損毀憑證的處理方法 – 損毀的憑證表示憑證使用了 ESET Internet Security 無法識別的格式，或者收到時已損壞（例如，被隨機資料覆寫）。在這種情況下，建議保持選取**［封鎖使用憑證的通訊］**。如果選取了**［詢問憑證有效性］**，則系統將在加密通訊建立時提示使用者選擇處理方法。

> 圖解範例
> 下列 ESET 知識庫文章可能僅以英文提供：
> • ESET Windows 家用產品中的憑證通知
> • 造訪網頁時會顯示「加密的網路流量：不信任的憑證」

應用程式掃描規則

應用程式掃描規則可用於自訂針對特定應用程式的 ESET Internet Security 行為，並記住 **SSL/TLS 模式**處於**互動模式**時選擇的處理方式。可以在 ［進階設定］ > **［防護］ > [SSL/TLS] > ［應用程式掃描規則］ > ［編輯］** 中檢視和編輯清單。

［應用程式掃描規則］視窗包括：

直欄

應用程式 – 從目錄樹狀結構選擇可執行檔，按一下 **[...]** 選項或手動輸入路徑。

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

控制項元素

新增 – 新增過濾應用程式。

編輯 – 選取您想配置的應用程式並按一下 **［編輯］**

刪除 – 選取您想刪除的應用程式並按一下 **［刪除］**

匯入/匯出 – 從檔案導入應用程式或將目前的應用程式清單儲存到檔案中。

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

憑證規則

憑證規則可用於自訂針對特定 SSL 憑證的 ESET Internet Security 行為，並記住 **SSL/TLS 模式**處於**互動模式**時選擇的處理方式。可以在 ［進階設定］ > ［**防護**］ > **[SSL/TLS]** > ［**憑證規則**］ > ［**編輯**］ 中檢視和編輯清單。

［**憑證規則**］ 視窗包含：

直欄

名稱 – 憑證名稱。

憑證發行者 – 憑證建立者名稱。

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

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

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

控制項元素

［**新增**］ – 新增新憑證並調整關於存取和掃描選項的設定。

編輯 – 選取您想配置的憑證並按一下 ［**編輯**］。

刪除 – 選取您想刪除的憑證並按一下 ［**移除**］。

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

加密的網路流量

若您的系統已配置為使用 SSL/TLS 掃描，提示您選擇處理方法的對話方塊視窗將在兩種情況下顯示：

首先，當網站使用未通過驗證或無效的憑證，且 ESET Internet Security 已配置為在該情況下詢問使用者（依預設，未通過驗證者為是，無有效憑證者為否），這時會出現對話方塊詢問您要 ［**允許**］ 或 ［**封鎖**］ 該連線。如果憑證不是位於 Trusted Root Certification Authorities store (TRCA)則會被視為不受信任。

第二，如果 **SSL/TLS 模式**已設定為 ［**互動模式**］，每個網站的對話方塊會詢問是否要 ［**掃描**］ 或 ［**略過**］ 流量。某些應用程式會驗證其 SSL 流量是否未經任何使用者修改或檢查，在這種情況下ESET Internet Security 必須 ［**略過**］ 該流量以繼續讓應用程式運作。

> 圖解範例
> 下列 ESET 知識庫文章可能僅以英文提供：
> • ESET Windows 家用產品中的憑證通知
> • 造訪網頁時會顯示「加密的網路流量：不信任的憑證」

在這兩種情況下，使用者可以選擇記住選取的處理方法。已儲存的處理方法儲存在憑證規則中。

電子郵件用戶端防護

若要配置電子郵件用戶端防護，請開啟 [進階設定] > [防護] > [電子郵件用戶端防護]，然後從以下配置選項中進行選擇：

- 郵件傳輸防護
- 信箱防護
- 地址清單管理
- ThreatSense

郵件傳輸防護

在電子郵件用戶端應用程式中IMAP(S) 和 POP3(S) 通訊協定是接收電子郵件通訊使用最廣泛的通訊協定。網際網路訊息存取通訊協定 (IMAP) 是另一種用於擷取電子郵件的網際網路通訊協定IMAP 有些優點凌駕 POP3例如多重用戶端可以同時連接到相同信箱，並維持郵件狀態資訊（例如郵件是否已讀取、回覆或刪除）。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。

無論使用的電子郵件用戶端為何ESET Internet Security 均可防護這些通訊協定，而無須重新配置電子郵件用戶端。依預設，無論預設 POP3/IMAP 連接埠號碼為何，所有透過 POP3 和 IMAP 通訊協定的通訊都會經過掃描。
MAPI 通訊協定尚未掃描。不過，電子郵件用戶端中的整合模組 (Microsoft Outlook) 可以掃描與 Microsoft Exchange 伺服器的通訊。

> ESET Internet Security 也支援掃描 IMAPS (585993) 和 POP3S (995) 通訊協定，其使用加密的通道以在伺服器與用戶端間傳輸資訊ESET Internet Security 會檢查利用 SSL (安全通訊端層）與 TLS (傳輸層安全性）通訊協定的通訊。
> 預設會掃描加密的通訊。若要檢視掃描器設定，請開啟 [進階設定] > [防護] > [SSL/TLS]

若要配置郵件傳輸防護，請開啟 [進階設定] > [防護] > [電子郵件用戶端防護] > [郵件傳輸防護]

啟用郵件傳輸防護 – 啟用后，郵件傳輸通訊將由 ESET Internet Security 掃描。

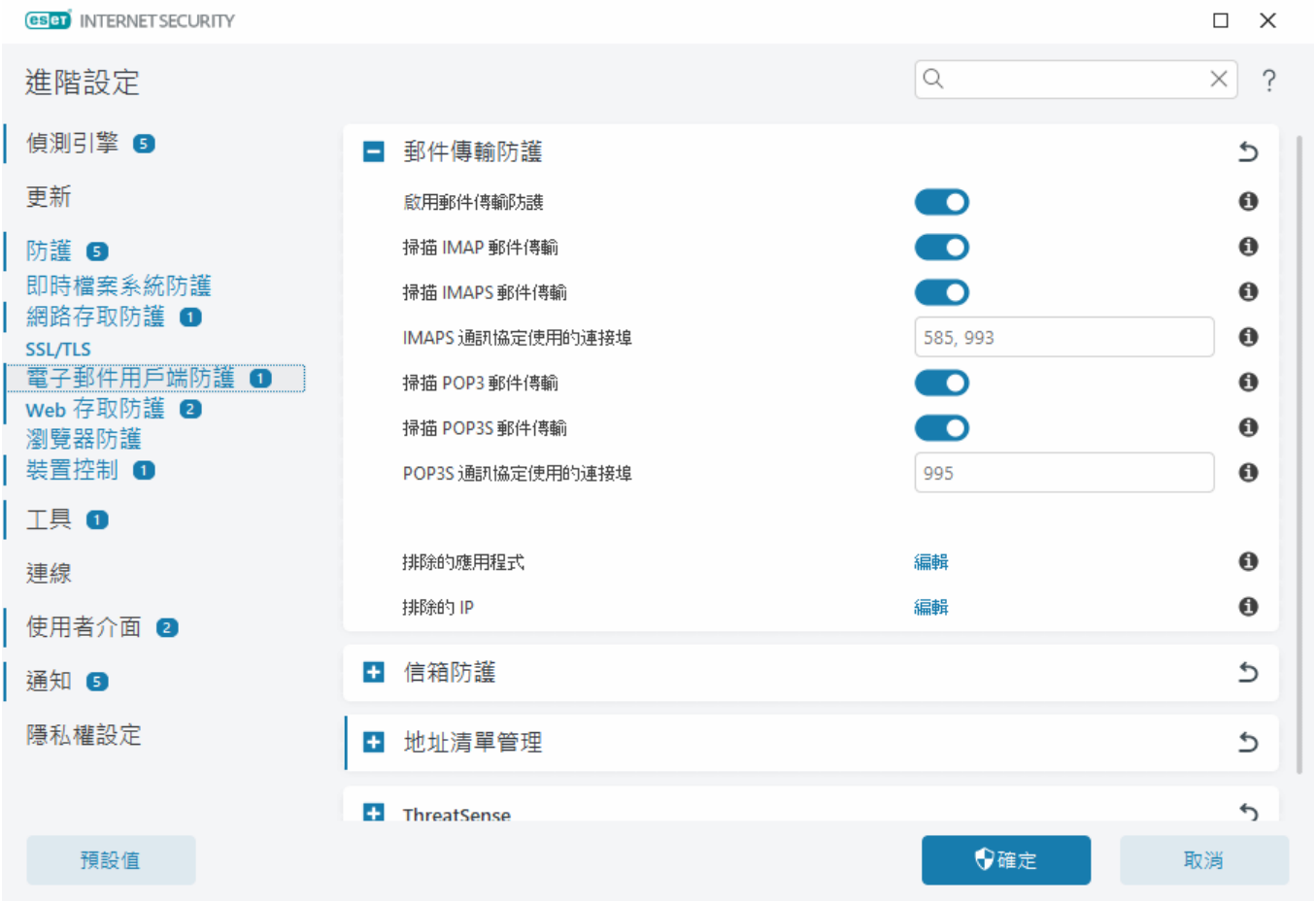
您可以透過按一下下方選項旁邊的切換開關來選擇要掃描的郵件傳輸通訊協定（預設情況下，啟用對所有通訊協定的掃描）：

- **掃描 IMAP 郵件傳輸**
- **掃描 IMAPS 郵件傳輸**
- **掃描 POP3 郵件傳輸**
- **掃描 POP3S 郵件傳輸**

預設情況下ESET Internet Security 將掃描標準連接埠上的 IMAPS 和 POP3S 通訊。若要為 IMAPS 和 POP3S 通訊協定新增自訂連接埠，請將它們新增到 **[IMAPS 通訊協定使用的連接埠]** 或 **[POP3S 通訊協定使用的連接埠]** 旁邊的文字欄位中。多個連接埠號必須以逗號分隔。

排除的應用程式 – 使您能夠透過郵件傳輸防護排除特定應用程式的掃描。當 Web 存取防護導致相容性問題時很有用。

排除的 IP – 使您能够透過郵件傳輸防護排除特定遠端位址的掃描。當 Web 存取防護導致相容性問題時很有用。



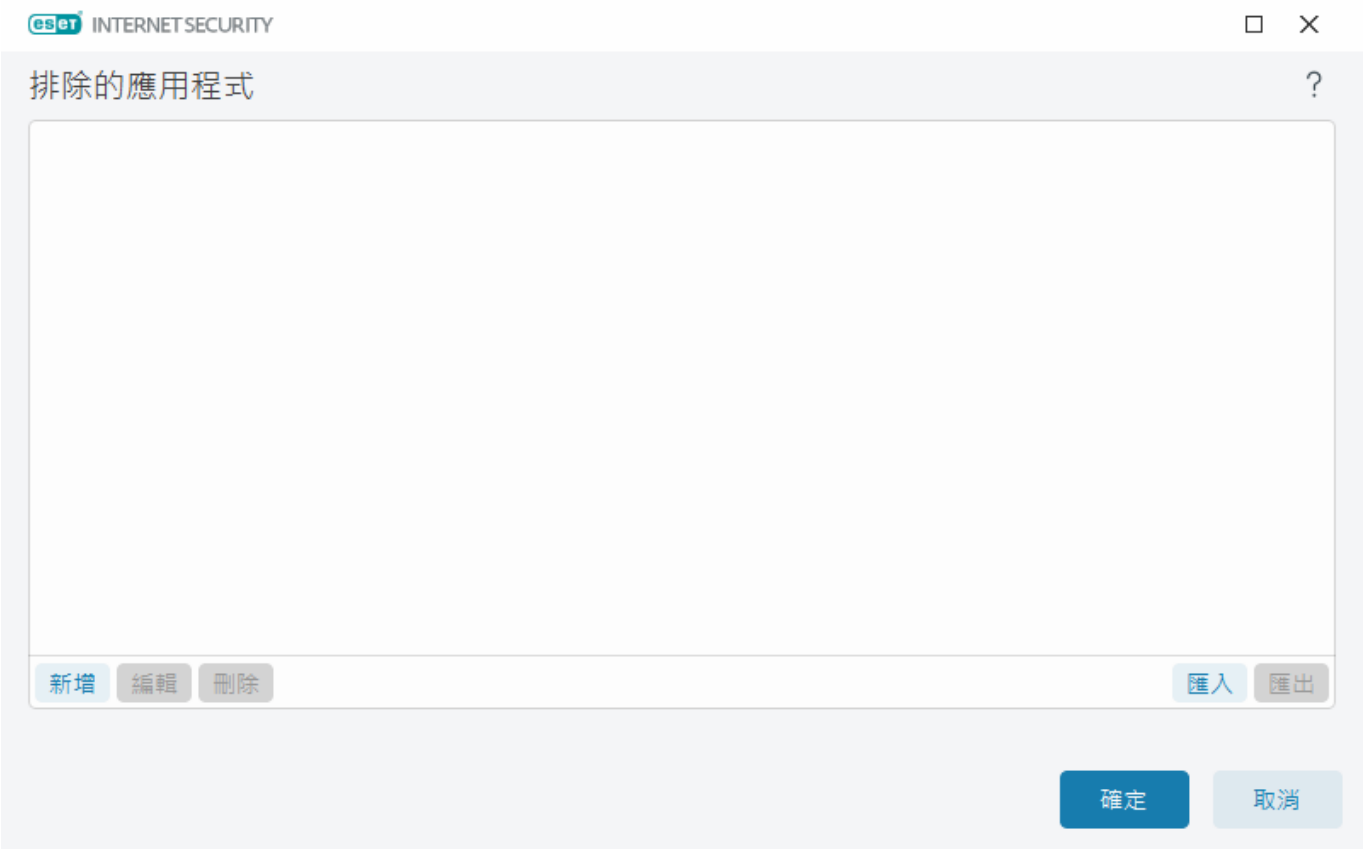
排除的應用程式

要排除掃描特定應用程式的通訊，請將它們新增至清單中。屆時將不會針對所選應用程式的 HTTP(S)/POP3(S)/IMAP(S) 通訊檢查是否存在威脅。建議僅將其用於在掃描通訊時無法正常運作的應用程式。

當您按一下 **[新增]** 時，正在執行的應用程式和服務將在此處自動可用。按一下 **[...]** 並瀏覽到應用程式以手動新增排除。

編輯 – 從清單中編輯選取的項目。

移除 – 從清單中移除選取的項目。



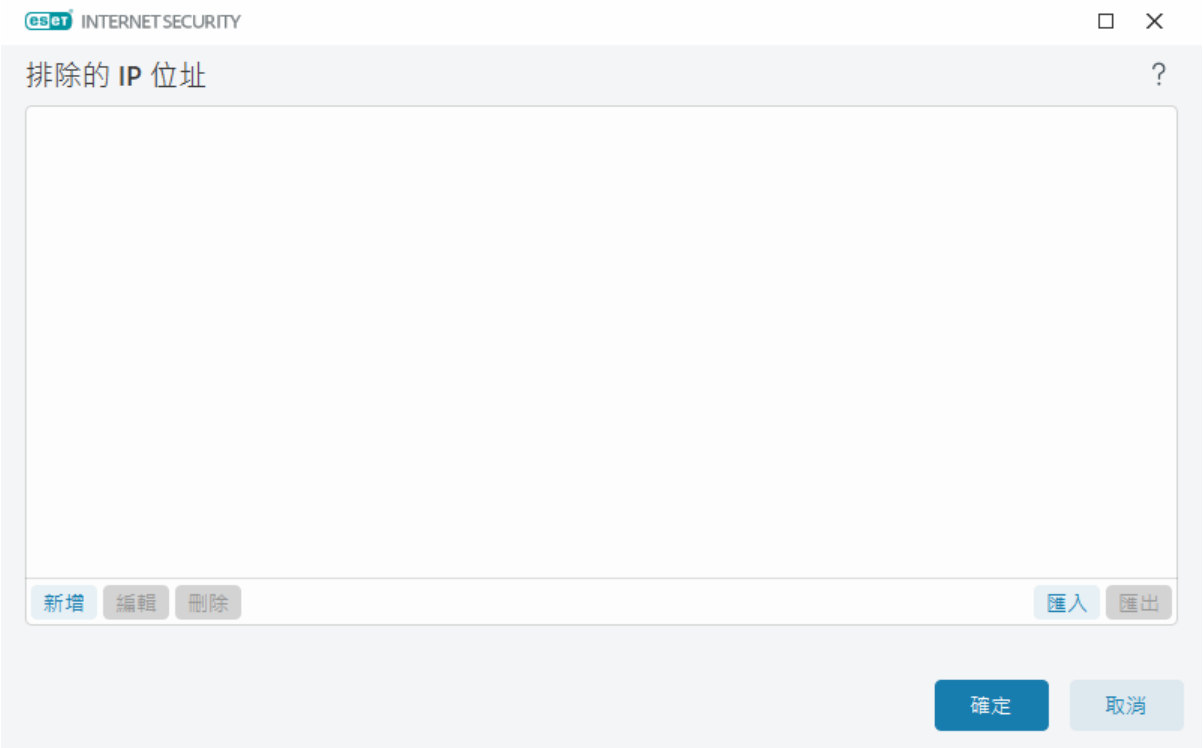
排除的 IP

清單中的項目將從掃描中排除。屆時將不會針對所選位址的 HTTP(S)/POP3(S)/IMAP(S) 往來通訊檢查是否存在威脅。我們建議只將此選項用於已知值得信賴的位址。

按一下［**新增**］以排除遠端位置的 IP 位址/位址範圍/子網路。

按一下［**編輯**］以變更選取的 IP 位址。

按一下［**刪除**］從清單中移除選取的項目。



IP 位址範例

新增 IPv4 位址：

[單一位址] - 新增個別電腦的 IP 位址（例如，*192.168.0.10*）

[位址範圍] - 輸入開始及結尾位址 IP 位址以指定數台電腦的 IP 範圍（例如，*192.168.0.1-192.168.0.99*）

[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 子網路的網路遮罩。排除 *192.168.1.0/24* 中的整個子網路類型。

新增 IPv6 位址：

[單一位址] - 新增個別電腦的 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*）

信箱防護

ESET Internet Security 與您信箱的整合可提高對電子郵件中惡意程式碼主動防護層級。

若要配置信箱防護，請開啟 [進階設定] > **[防護]** > **[電子郵件用戶端防護]** > **[信箱防護]**

啟用用戶端外掛程式的電子郵件防護 - 若停用，電子郵件用戶端外掛程式的防護就會關閉。

選取要掃描的電子郵件：

- **已接收電子郵件**
- **已傳送電子郵件**
- **已閱讀電子郵件**
- **已修改的電子郵件**

我們建議您將**啟用用戶端外掛程式的電子郵件防護**保持啟用狀態。即使整合未啟用或未運作，電子郵件通訊仍會受到郵件傳輸防護 (IMAP/IMAPS 和 POP3/POP3S) 的防護。

掃描垃圾郵件

來路不明的電子郵件（又稱為垃圾郵件）已成為最大的電子通訊問題。垃圾郵件佔所有電子郵件通訊的 30 %。電子郵件用戶端反垃圾郵件用於對此問題進行防護。電子郵件用戶端反垃圾郵件結合了數種電子郵件安全性原則，提供卓越的過濾，讓收件匣清除垃圾郵件。垃圾郵件偵測中的一個重要原則是：可以根據預先定義的信任地址（已允許）及垃圾郵件地址（已封鎖），來識別來路不明的電子郵件。

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

啟用電子郵件用戶端反垃圾郵件 – 啟用後，將掃描收到的郵件以尋找垃圾郵件。

使用進階垃圾郵件掃描器 – 將定期下載其他反垃圾郵件資料，提高反垃圾郵件功能，從而產生更好的結果。

垃圾郵件分數記錄 – ESET Internet Security 反垃圾郵件防護引擎會將垃圾郵件分數指派給各個掃描的郵件。郵件將記錄於反垃圾郵件防護防護記錄中（[主程式視窗] > [**工具**] > [**防護記錄檔案**] > [**電子郵件用戶端反垃圾郵件**])

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

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

附件處理最佳化 – 如果停用最佳化，將立即掃描所有附件。您可能會遇到電子郵件用戶端效能速度減慢。

整合 – 可讓您將信箱防護整合到電子郵件用戶端中。有關詳細資訊，請參閱整合

回應 – 可讓您自訂垃圾郵件的處理方式。有關詳細資訊，請參閱回應

整合

ESET Internet Security 與您電子郵件用戶端的整合可提高對電子郵件中惡意程式碼主動防護層級。如果您的電子郵件用戶端受支援，您可以在 ESET Internet Security 中啟用此整合。如果整合至電子郵件用戶端ESET Internet Security 工具列會直接插入電子郵件用戶端，以便更有效進行電子郵件防護。若要編輯整合設定，請開啟 [進階設定] > [**防護**] > [**電子郵件用戶端防護**] > [**信箱防護**] > [**整合**]

整合至 Microsoft Outlook – Microsoft Outlook 目前是唯一支援的電子郵件用戶端。電子郵件防護是以外掛程式的形式運作。外掛程式的主要優勢為其獨立於所使用的通訊協定。當電子郵件用戶端接收到加密的郵件，它會將其解密並傳送到病毒掃描器。如需支援的 Microsoft Outlook 版本的完整清單，請參閱此 ESET 知識庫文章

進階電子郵件用戶端處理 – 處理額外 Outlook Messaging API (MAPI) 事件：已修改物件

（fnevObjectModified）和已建立物件（fnevObjectCreated）。如果在處理電子郵件用戶端時發生系統速度減慢，請停用此選項。

Microsoft Outlook 工具列

Microsoft Outlook 防護是以外掛程式模組來運作ESET Internet Security 安裝後，此工具列包含防毒防護和電子郵件用戶端反垃圾郵件選項，已新增至 Microsoft Outlook 中：

垃圾郵件 – 將所選郵件標記為垃圾郵件。標記之後，會將郵件的「指紋」傳送至儲存垃圾郵件簽章的中央伺服器。如果伺服器從多位使用者收到更多類似的「指紋」，則將來會將該郵件分類為垃圾郵件。

非垃圾郵件 – 將所選郵件標記為非垃圾郵件。

[垃圾郵件地址]（已封鎖，垃圾郵件地址的清單） – 將新的寄件者地址新增至地址清單作為封鎖。接收到來自該名單的所有郵件都會自動分類為垃圾郵件。

⚠ 請注意詐騙 – 偽造電子郵件上的寄件者地址以誤導電子郵件收件者進行閱讀及回應。

[受信任的地址]（已允許，受信任的地址清單） – 將新的寄件者地址新增至地址清單作為允許。從允許的地址接收的所有訊息絕對不會自動分類為垃圾郵件。

ESET Internet Security – 按兩下圖示以開啟 ESET Internet Security 的主視窗。

重新掃描郵件 – 可讓您手動啟動電子郵件檢查。您可以指定要檢查的郵件，且可以啟動重新掃描已接收的電子郵件。如需詳細資訊，請參閱信箱防護

掃描器設定 – 顯示信箱防護設定選項。

反垃圾郵件設定 – 顯示信箱防護設定選項。

通訊錄 – 開啟位址清單管理視窗，您可從中存取已排除、信任及垃圾郵件地址的清單。

確認對話方塊

此通知可用於驗證使用者是否真的想要執行選取的處理方法，此舉能消除可能的錯誤。

另一方面，該對話方塊也具有停用確認的選項。

重新掃描郵件

整合至電子郵件用戶端的 ESET Internet Security 工具列可讓使用者指定多個電子郵件檢查選項。**[重新掃描郵件]** 選項提供兩種掃描模式：

位於目前資料夾中的所有郵件 – 掃描目前所顯示資料夾中的郵件。

僅限選取的郵件 – 僅掃描使用者標記的郵件。

[重新掃描已掃描的郵件] 核取方塊可供使用者選擇針對先前已掃描的郵件再次執行掃描。

回應

根據郵件掃描結果□ESET Internet Security 可以移動掃描的郵件或向主旨新增自訂文字。您可以在「進階設定」>［防護］>［電子郵件用戶端防護］>［信箱防護］>［回應］中配置這些設定。

ESET Internet Security 中的電子郵件用戶端反垃圾郵件可讓您為郵件配置以下參數：

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

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

移至自訂資料夾 – 啟用時，垃圾郵件將被移至下方指定的資料夾。

資料夾 – 指定偵測到受感染電子郵件時，要將其移到哪個自訂資料夾。

如果存在包含偵測的郵件，則根據預設□ESET Internet Security 會嘗試清除該郵件。如果無法清除郵件，您可以選擇［**無法清除時要採取的處理方式**］□

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

資料夾 – 指定偵測到受感染電子郵件時，要將其移到哪個自訂資料夾。

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

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

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電子郵件**或 **將標籤訊息附加到已傳送的電子郵件**。請注意，雖然這些情況不常發生，但是標籤訊息有可能會在有問題 HTML 訊息中省略，或訊息由惡意軟體所產生。標籤訊息可以新增至已接收及已讀取的電子郵件或已傳送的電子郵件（或兩者）。可用選項如下：

- **［絕不］** – 不會新增標籤訊息。
- **發生偵測時** – 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。

更新已接收和已讀取電子郵件的主旨 / 更新已傳送電子郵件的主旨 – 啟用此選項可將下方指定的自訂文字新增至郵件中。

要新增至已偵測到的電子郵件主旨的文字 – 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。此功能會將郵件主旨□Hello□取代成以下格式：□[detection %DETECTIONNAME%] Hello□。變數 %DETECTIONNAME% 代表偵測。

地址清單管理

ESET Internet Security 中的電子郵件用戶端反垃圾郵件功能可讓您配置位址清單的各種參數。若要配置位址清單，請開啟 [進階設定] > **[防護] > [電子郵件用戶端防護] > [地址清單管理]**。

啟用使用者的位址清單 – 啟用此選項以啟動使用者的位址清單。

使用者的位址清單 – 電子郵件地址清單，您可以在其中新增、編輯或刪除位址，以定義反垃圾郵件規則。此清單中的規則將套用至目前使用者。

啟用全域位址清單 – 啟用此選項以啟動此裝置上所有使用者共用的全域位址清單。

全域位址清單 – 電子郵件地址清單，您可以在其中新增、編輯或刪除位址，以定義反垃圾郵件規則。此清單中的規則將套用至所有使用者。

自動允許並新增到使用者的位址清單

將來自通訊錄中的地址視為受信任 – 系統會將連絡人清單中的地址視為受信任，不需新增至使用者的位址清單。

新增外寄郵件中的收件者地址 – 將已傳送郵件中的收件者地址新增至使用者的位址清單中成為允許。

新增重新分類為「非」垃圾郵件的地址 – 將重新分類為「非」垃圾郵件的郵件其寄件者地址新增至使用者位址清單中成為允許。

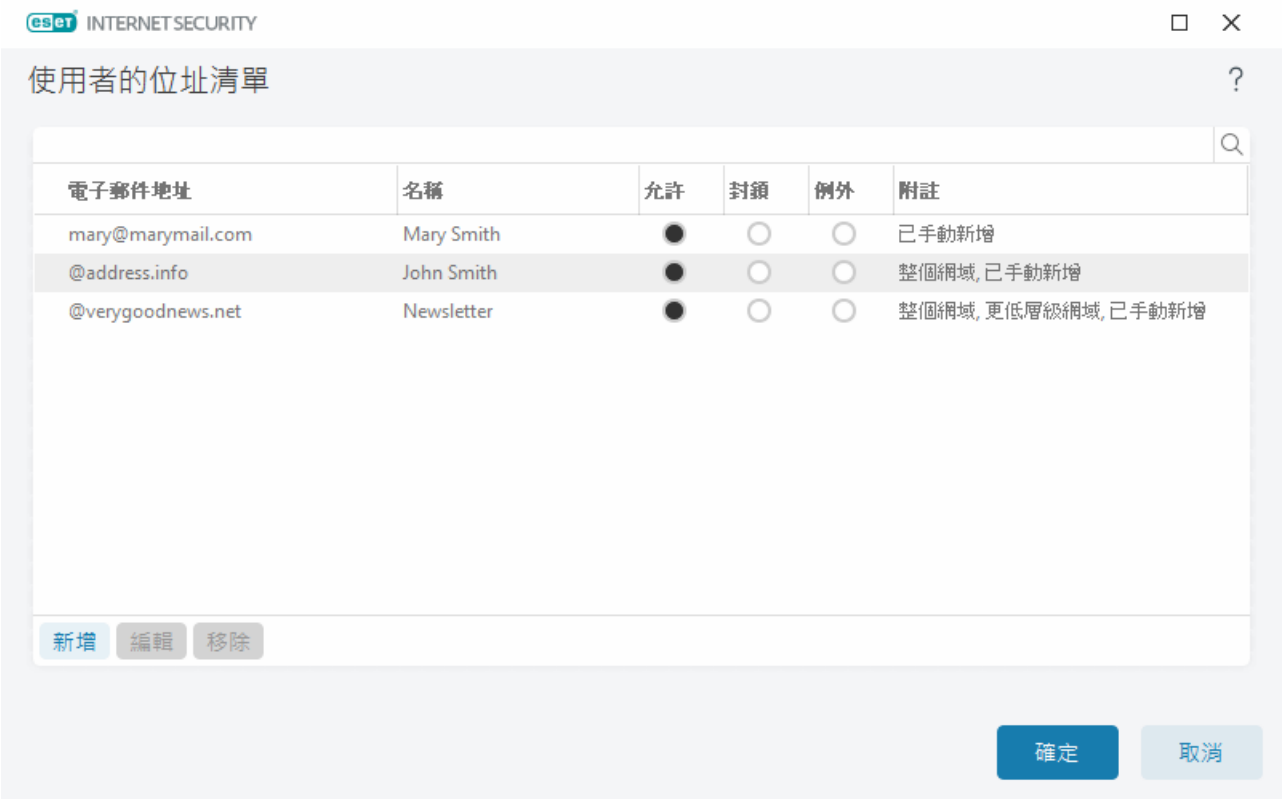
自動新增到使用者的位址清單並設為例外

新增來自自己帳戶中的地址 – 將現有電子郵件用戶端帳戶的地址新增使用者的位址清單中成為例外。

位址清單

為預防來路不明的電子郵件，ESET Internet Security 可讓您在位址清單中分類電子郵件地址。

若要編輯位址清單，請開啟 [進階設定] > **[防護] > [電子郵件用戶端防護] > [位址清單管理]**，然後按一下 **[使用者的位址清單]** 或 **[全域位址清單]** 旁邊的 **[編輯]**。



直欄

電子郵件地址 – 將套用規則的地址。不支援萬用字元。

名稱 – 自訂規則名稱。

允許/封鎖/例外 – 用於決定要為電子郵件地址採取何種處理方法的選項按鈕（按一下偏好欄中的選項按鈕可快速變更處理方法）：

- **允許** – 視為安全的地址，且您想要收到來自這些地址的郵件。
- **封鎖** – 視為不安全/垃圾郵件的地址，且您不想要收到來自這些地址的郵件。
- **例外** – 系統一律檢查是否為垃圾郵件及可能受詐騙而被用來傳送垃圾郵件的地址。

注意 – 有關如何建立規則以及規則是否套用於整個網域/較低層級網域的資訊。

管理地址

- **新增** – 按一下可新增新地址的規則。
- **編輯** – 選擇並按一下以編輯現有規則。
- **移除** – 如果您希望從位址清單中刪除規則，請選擇並按一下該規則。

新增/編輯地址

此視窗可讓您在位址清單管理中新增或編輯位址，並配置採取的處理方法：

電子郵件地址 – 將套用規則的地址。

名稱 – 自訂規則名稱。

處理方法 – 如果連絡人的電子郵件地址符合［**電子郵件地址**］欄位中指定的地址，則採取以下處理方法：

- **允許** – 視為安全的地址，且您想要收到來自這些地址的郵件。
- **封鎖** – 視為不安全/垃圾郵件的地址，且您不想要收到來自這些地址的郵件。
- **例外** – 系統一律檢查是否為垃圾郵件及可能受詐騙而被用來傳送垃圾郵件的地址。

整個網域 – 為即將套用到聯絡人整個網域的規則選取此選項（不只是［**電子郵件地址**］欄位中指定的地址，還有 *address.info* 網域的所有電子郵件地址）。

更低層級網域 – 為即將套用到聯絡人更低層級網域的規則選取此選項（*address.info* 代表網域，而 *my.address.info* 代表子網域）。

地址處理結果

新增新位址或變更為電子郵件地址採用的處理方法時，ESET Internet Security 會顯示通知訊息。根據您嘗試執行的處理方法，通知訊息的內容可能不同。

選取［**不要再詢問**］核取方塊，可自動執行處理方法且下次不顯示訊息。

ThreatSense

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

ThreatSense 引擎設定選項可讓您指定數個掃描參數：

- 要掃描的檔案類型及副檔名
- 各種偵測方法的組合
- 清除的層級等

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

- 即時檔案系統防護
- 閒置狀態掃描
- 啟動掃描
- 文件防護
- 電子郵件用戶端防護

- Web 存取防護
- 電腦掃描

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

要掃描的物件

此區段可讓您定義要掃描是否有入侵的電腦元件及檔案。

[作業記憶體] - 掃描攻擊系統作業記憶體的威脅。

開機磁區/UEFI - 掃描開機磁區的主要開機記錄中是否有惡意軟體。請在字彙中閱讀更多有關 UEFI 的資訊

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。

[自我解壓檔] - 自我解壓檔 (SFX) 是可以自行解壓縮的壓縮檔。

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

掃描選項

選取在掃描系統是否有入侵時使用的方法。可用選項如下：

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

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

清除

清除設定會決定 ESET Internet Security 在清除物件期間的行為。清除層級有 4 個：

ThreatSense 具有下列修復（即，清除）層級。

ESET Internet Security 中的修復

清除層級	說明

清除層級	說明
一律修復偵測	清除物件時嘗試修復偵測，不需要任何使用者介入。在某些少見的情況下（例如，系統檔案），如果無法修復偵測，回報的物件會保持在原始位置。
如果安全無虞則修復偵測，否則請保留	清除物件時嘗試修復偵測，不需要任何使用者介入。在某些情況下（例如，同時具有乾淨或受感染檔案的系統檔案或壓縮檔），如果無法修復偵測，回報的物件會保持在原始位置。
如果安全無虞則修復偵測，否則請詢問	清除物件時嘗試修復偵測。在某些情況下，如果無法執行任何動作，使用者會收到互動警告且必須選取修復的動作（例如，刪除或忽略）。建議對大多數情況使用此設定。
一律詢問使用者	使用者會在清除物件時收到互動視窗，而且必須選取修復動作（例如，刪除或忽略）。此層級是針對其他進階使用者而設計的，這些進階使用者瞭解偵測時需採取哪些步驟。

排除

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

其他

配置指定電腦掃描的 ThreatSense 引擎參數時，**[其他]** 區段也有以下可用選項：

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

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

[記錄所有物件] – 掃描防護記錄將顯示自我解壓檔中所有掃描的檔案，即使未受到感染的檔案也會顯示（可能產生許多掃描防護記錄資料，因而增加掃描防護記錄檔案的大小）。

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

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

限制

[限制] 區段可讓您指定物件的大小上限，以及要掃描的巢狀保存檔層級：

物件設定

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

物件的掃描時間上限（秒） – 定義掃描容器物件的時間值上限（例如 RAR/ZIP 壓縮檔或具有多個附件的電子郵件）。此設定不適用於獨立檔案。如果已輸入使用者定義的值，且已經過指定時間，則掃描將儘快停止，不論容器物件中每個檔案的掃描是否已完成。
如果壓縮檔帶有大型檔案，掃描將不會比擷取壓縮檔中的檔案更早結束（例如，當使用者定義的變數為 3 秒，而檔案擷取需要 5 秒）。該時間經過後，將不會掃描壓縮檔中的其餘檔案。
若要限制掃描時間（包括較大的壓縮檔），請在壓縮檔中使用 **[物件大小上限]** 和 **[壓縮檔中檔案的大小上限]**（不建議，因為可能存在安全風險）。
預設值：無限制

壓縮檔掃描設定

壓縮檔巢狀層級 – 指定壓縮檔掃描的深度上限。預設值：10.

壓縮檔中檔案的大小上限 – 此選項可讓您指定要掃描的壓縮保存檔中，所包含檔案的大小上限（解壓縮時）。最大值是 **3 GB**

> 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。

Web 存取防護

Web 存取防護允許您配置進階網際網路防護模組設定。以下選項在 [進階設定] > **[防護] > [Web 存取防護] > [Web 存取防護]** 中可用：

[啟用 Web 存取防護] – 停用之後，無法執行 Web 存取防護和防網路釣魚防護

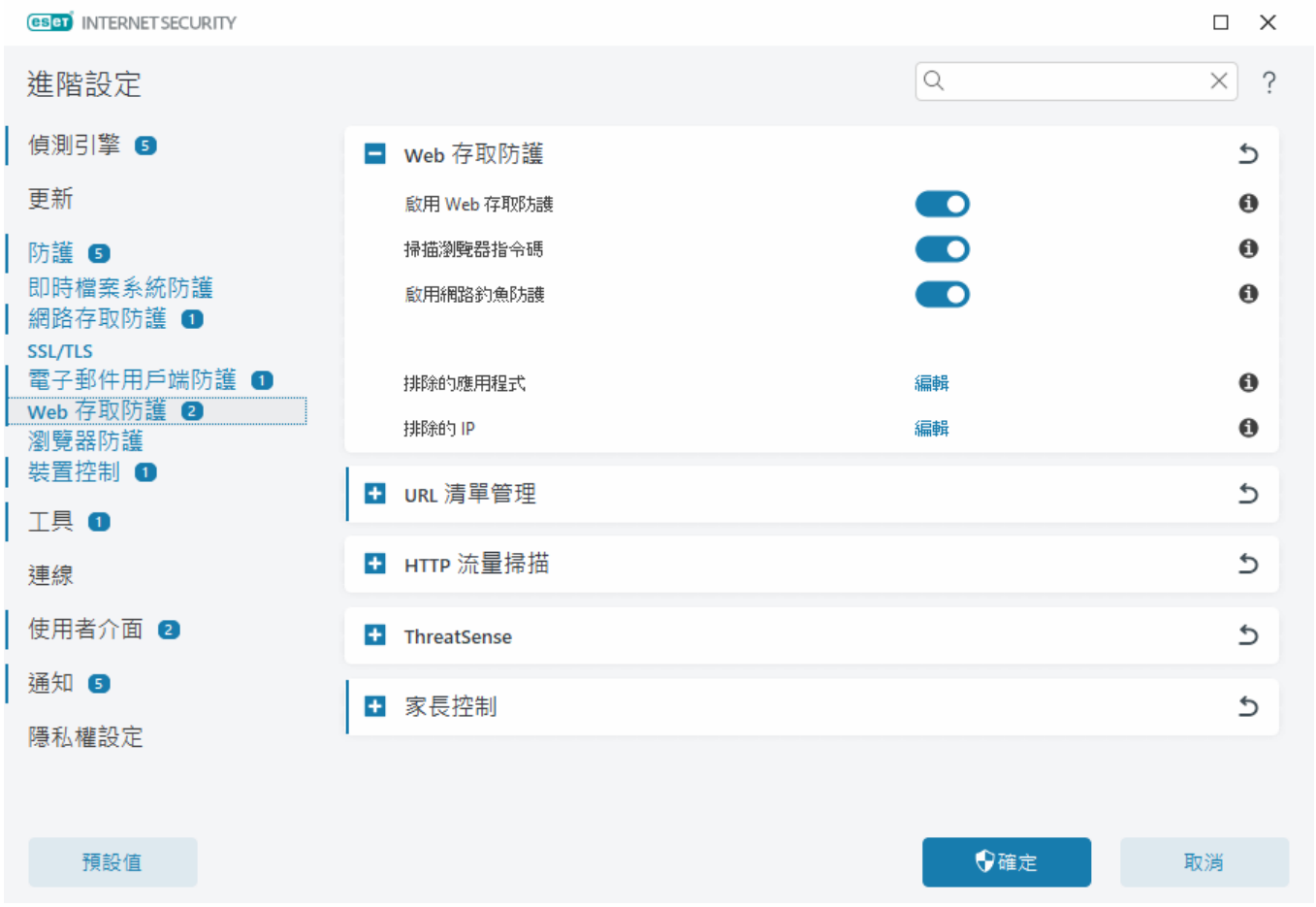
> 強烈建議您保持啟用 Web 存取防護，並不排除任何應用程式或 IP 位址（根據預設）。

掃描瀏覽器指令碼 – 啟用時，偵測引擎會檢查 web 瀏覽器執行的所有 JavaScript 程式。

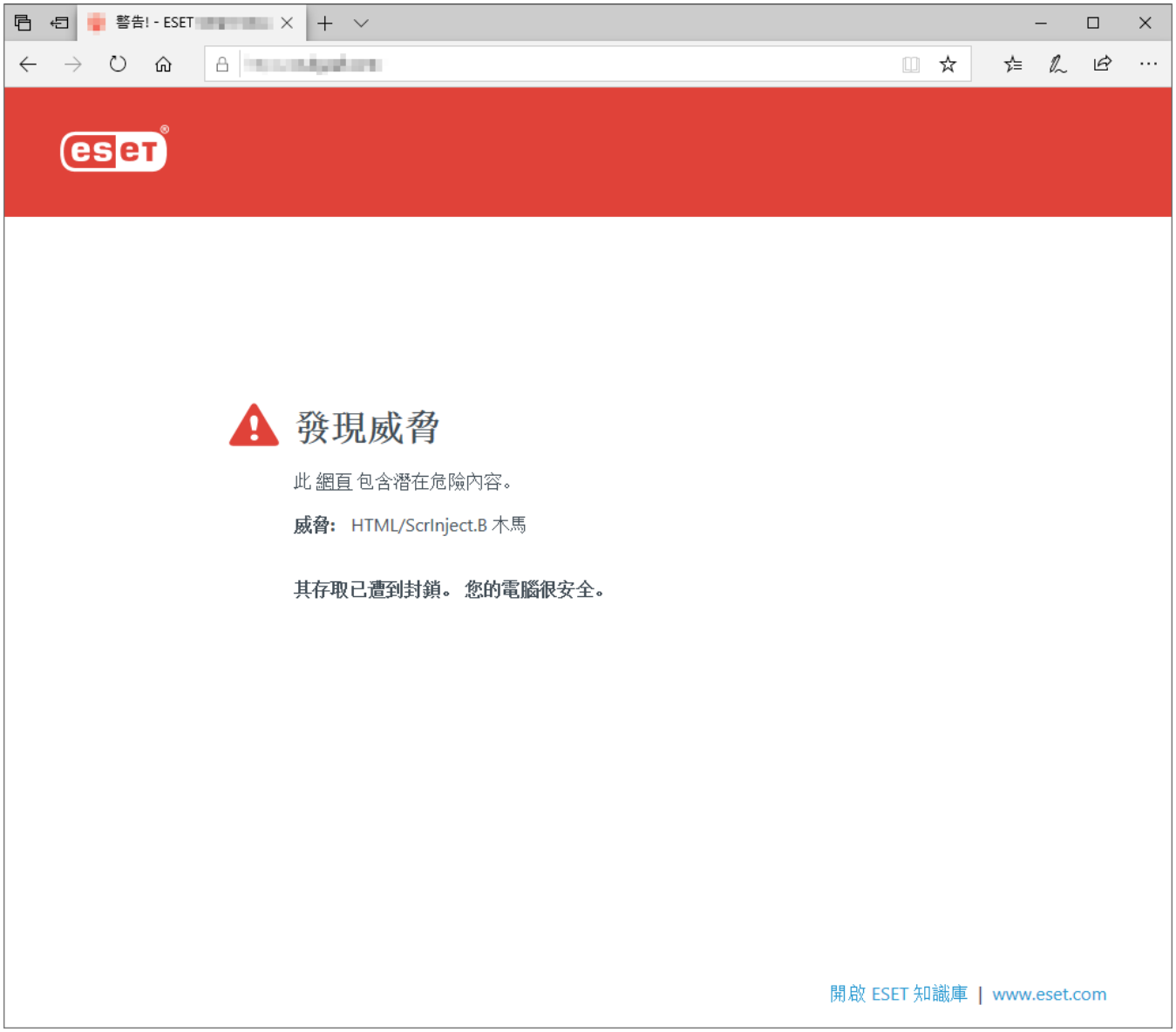
啟用防網路釣魚防護 – 啟用時，將封鎖網路釣魚網頁。請參閱「網路釣魚防護」以取得詳細資訊。

排除的應用程式 – 使您能夠將特定應用程式從 Web 存取防護掃描中排除。當 Web 存取防護導致相容性問題時很有用。

排除的 IP – 使您能夠從 Web 存取防護的掃描中排除特定遠端位址。當 Web 存取防護導致相容性問題時很有用。



當網站遭到封鎖時Web 存取防護將在您的瀏覽器中顯示下列訊息：



圖解指示

下列 ESET 知識庫文章可能僅以英文提供：

- 排除安全網站以免遭 Web 存取防護封鎖
- 使用 ESET Internet Security 封鎖網站

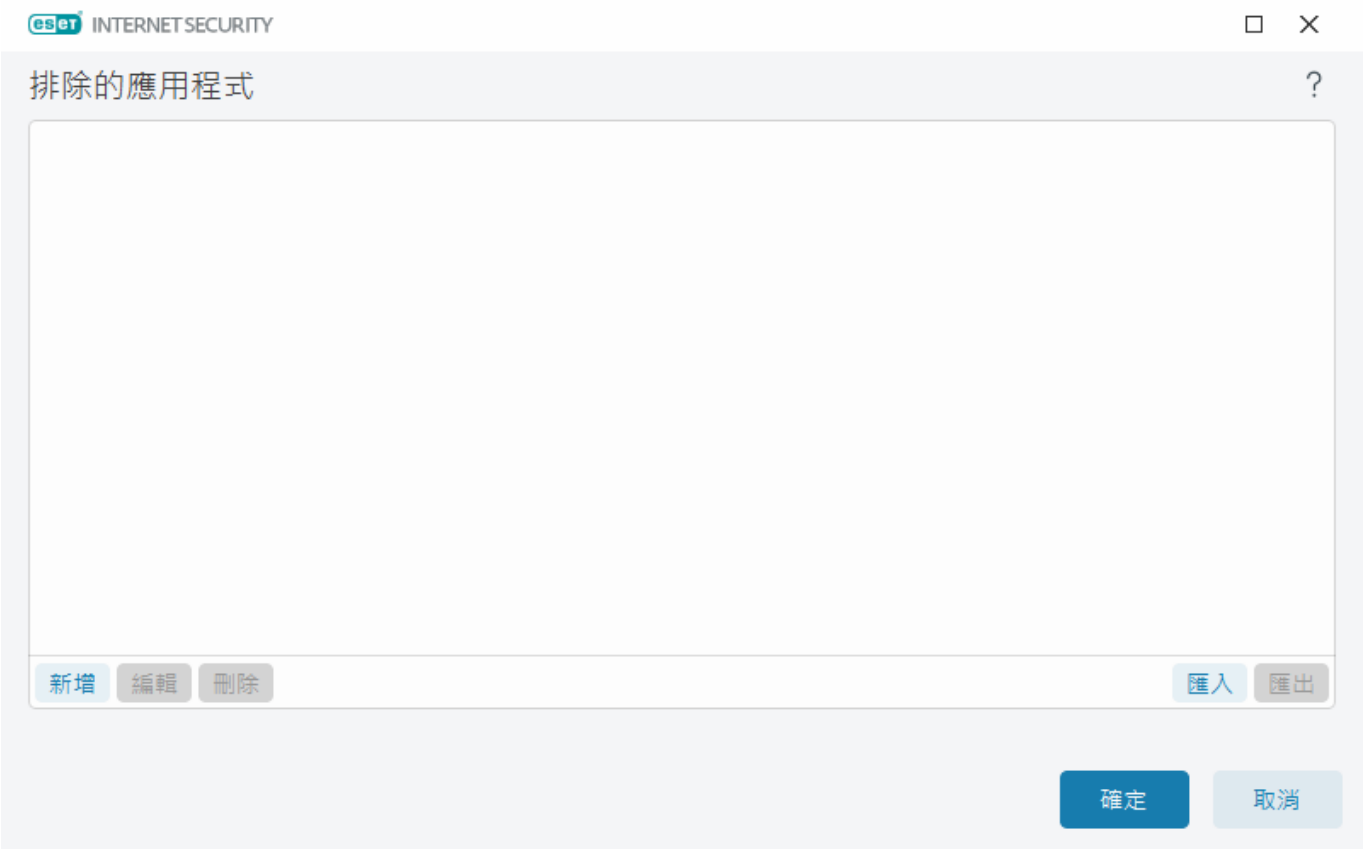
排除的應用程式

要排除掃描特定應用程式的通訊，請將它們新增至清單中。屆時將不會針對所選應用程式的 HTTP(S)/POP3(S)/IMAP(S) 通訊檢查是否存在威脅。建議僅將其用於在掃描通訊時無法正常運作的應用程式。

當您按一下［**新增**］時，正在執行的應用程式和服務將在此處自動可用。按一下 **[...]** 並瀏覽到應用程式以手動新增排除。

編輯 - 從清單中編輯選取的項目。

移除 - 從清單中移除選取的項目。



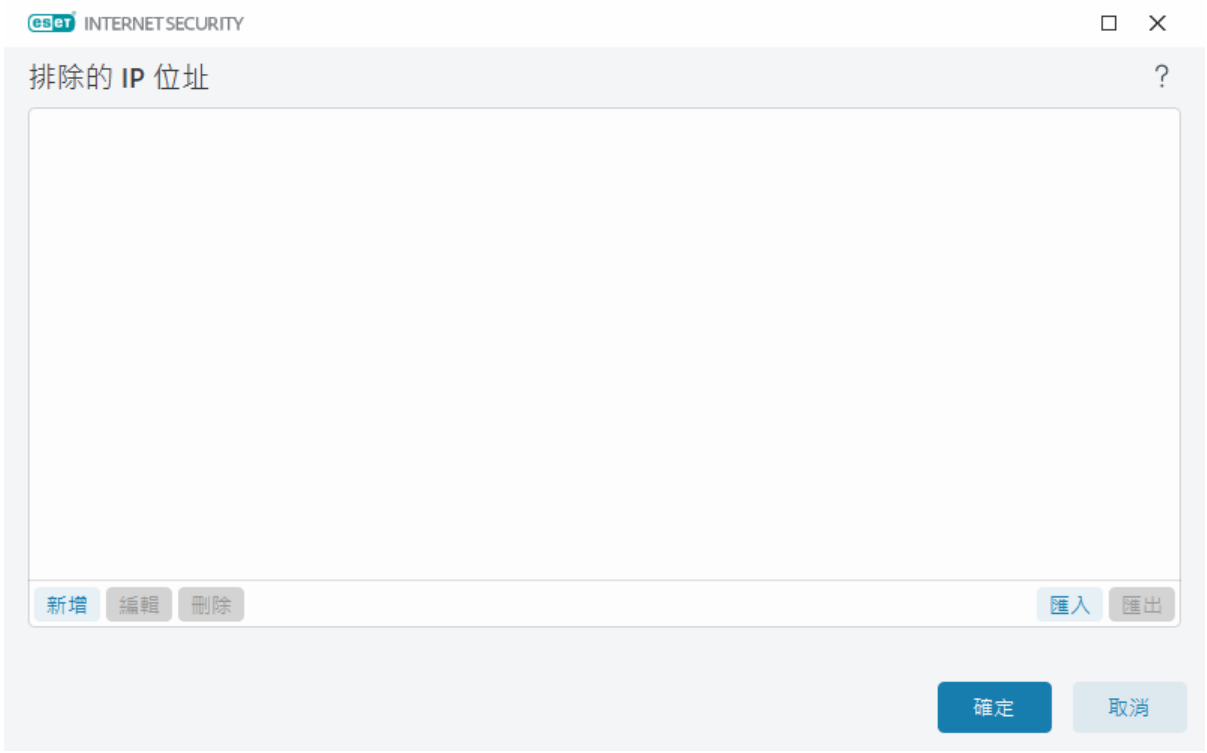
排除的 IP

清單中的項目將從掃描中排除。屆時將不會針對所選位址的 HTTP(S)/POP3(S)/IMAP(S) 往來通訊檢查是否存在威脅。我們建議只將此選項用於已知值得信賴的位址。

按一下 **［新增］**以排除遠端位置的 IP 位址/位址範圍/子網路。

按一下 **［編輯］**以變更選取的 IP 位址。

按一下 **［刪除］**從清單中移除選取的項目。



IP 位址範例

新增 IPv4 位址：

[單一位址] - 新增個別電腦的 IP 位址（例如，*192.168.0.10*）

[位址範圍] - 輸入開始及結尾位址 IP 位址以指定數台電腦的 IP 範圍（例如，*192.168.0.1-192.168.0.99*）

[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 子網路的網路遮罩。排除 *192.168.1.0/24* 中的整個子網路類型。

新增 IPv6 位址：

[單一位址] - 新增個別電腦的 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*）

URL 清單管理

[進階設定] > **[防護] > [Web 存取防護]** 中的 **[URL 清單管理]** 可讓您指定 HTTP 位址以封鎖、允許或從內容掃描中排除。

除了 HTTP 之外，如果還要過濾 HTTPS 位址，必須啟用 SSL/TLS。否則只有您已造訪 HTTPS 網站的網域將會新增，但完整 URL 則不會新增。

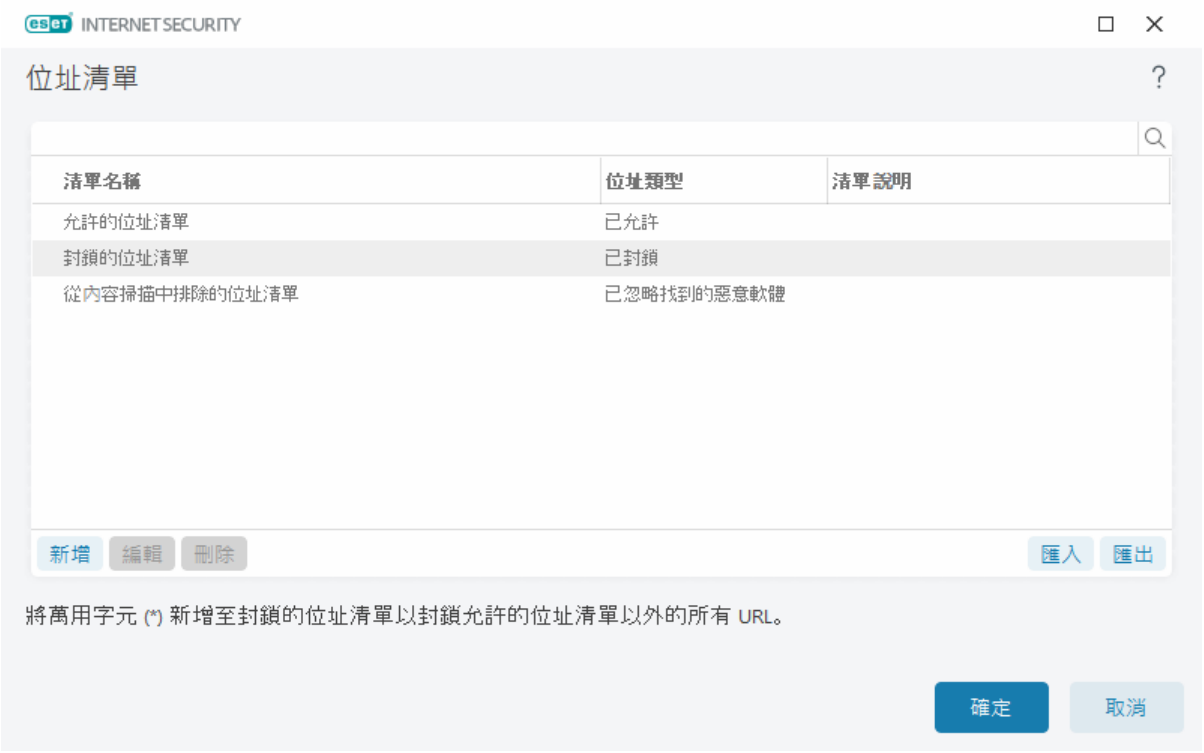
不可以存取 **[封鎖位址清單]** 中的網站，除非它們包含在 **[允許的位址清單]** 中。**[從內容掃描中排除的位址清單]** 中的網站在存取時將不檢查是否含有惡意程式碼。

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

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

ESET 信任的位址

如果啟用的［**不掃描 ESET 信任的網域之流量**］為 SSL/TLS，則由 ESET 管理的白名單上的網域將不受 URL 清單管理配置的影響。



控制項元素

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

［**編輯**］ - 修改現有清單。使用它來新增或移除位址。

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

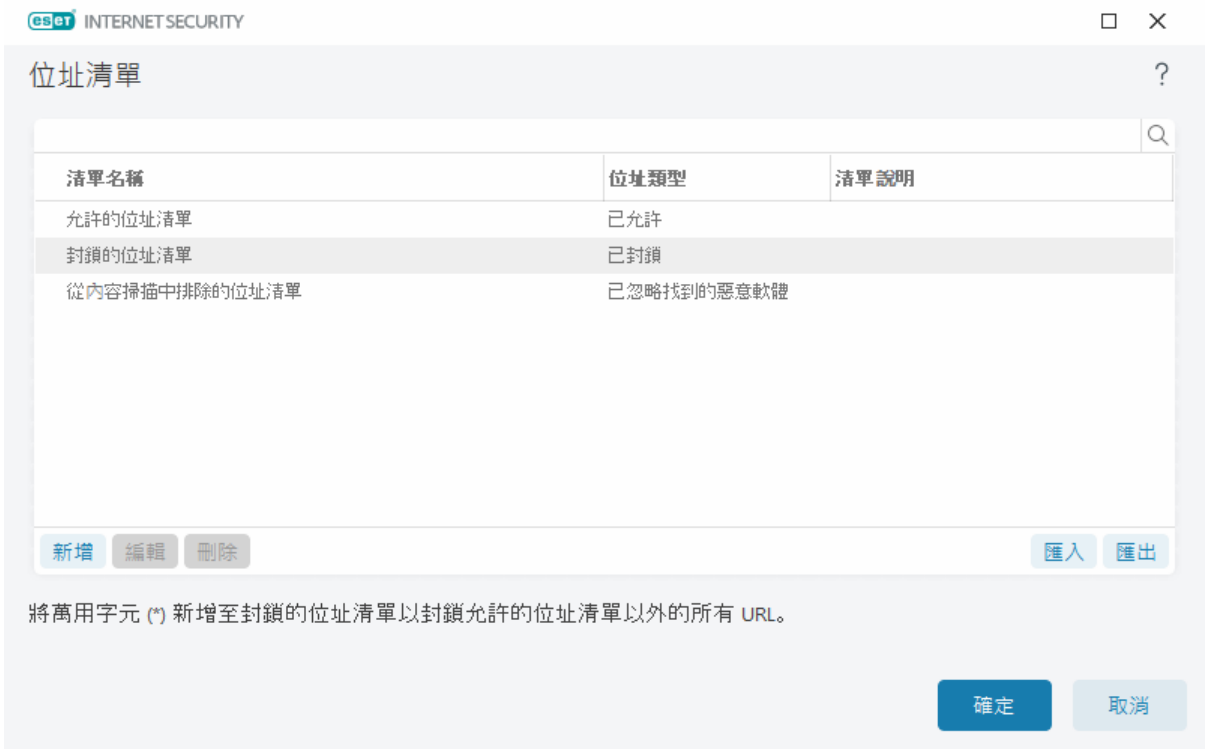
位址清單

在區段中您可以指定要封鎖、允許或從檢查中排除的 HTTP(S) 位址清單。

依預設，可使用的三種清單類型如下：

- **從內容掃描中排除的位址清單** - 不檢查任何加入此清單之位址中是否含有惡意代碼。
- **允許的位址清單** - 如果已啟用「在允許的位址清單中，只允許 HTTP 位址的存取」，而且封鎖的位址清單包含 *（所有項目皆符合），使用者只允許存取清單中的指定位址。即使包含在封鎖的位址清單上，也會允許存取此清單中的位址。
- **封鎖的位址清單** - 除非也在允許的位址清單上，否則不允許使用者存取此清單中的指定位址。

按一下［**新增**］以建立新的清單。若要刪除選取的清單，請按一下［**刪除**］。



圖解指示

下列 ESET 知識庫文章可能僅以英文提供：

- 排除安全網站以免遭 Web 存取防護封鎖
- 使用 ESET Windows 家用產品封鎖網站

如需詳細資訊，請參閱 URL 清單管理

建立新的位址清單

此對話方塊視窗讓您能夠配置一個新的 URL 位址/遮罩清單，將會封鎖、允許這些 URL 位址/遮罩或排除在檢查之外。

您可以配置下列選項：

[位址清單類型] – 可使用三種清單類型：

- **已忽略找到的惡意軟體** – 不檢查任何加入此清單之位址中是否含有惡意代碼。
- **已封鎖** – 存取此清單中指定的位址將會封鎖。
- **已允許** – 存取此清單中指定的位址將會允許。允許此清單中的位址，即使其與封鎖的位址清單相符。

清單名稱 – 可指定清單的名稱。編輯其中一個預先定義清單時，將無法使用此欄位。

[清單說明] – 可輸入簡短的清單說明（選用）。編輯其中一個預先定義清單時無法使用。

若要啟動清單，請選取該清單旁的 **[作用中清單]**。如果您希望在存取網站時使用特定清單時收到通知，選取 **[套用時通知]**。例如，當網站遭封鎖或允許時您會收到通知，因為其包含在已封鎖或已允許位址的清單中。通知會包含清單的名稱。

[記錄嚴重性] – 有關存取網站時使用之特定清單的資訊可以寫入防護記錄檔案

控制項元素

新增 – 將新 URL 位址新增到清單中（輸入用分行符號分隔的多個值）。

編輯 – 修改清單中的現有位址。僅適用於使用［**新增**］而建立的位址。

［**移除**］ – 刪除清單中的現有位址。僅適用於使用［**新增**］而建立的位址。

匯入 – 匯入包含 URL 位址的檔案（使用分行符號分隔的個別值，例如，使用 UTF-8 編碼方式的 *.txt)。

如何新增 URL 遮罩

請先參閱此對話方塊中的說明，再輸入所需的位址/網域遮罩。

ESET Internet Security 可讓使用者封鎖存取特定網站，避免網際網路瀏覽器顯示其內容。此外，其可讓使用者指定應從檢查中排除的位址。如果不知道遠端伺服器的完整名稱，或者使用者想要指定遠端伺服器的整個群組，則所謂的遮罩可以用來識別此類群組。遮罩包括 ？ 及 * 符號：

- 使用 ？ 來取代一個符號
- 使用 * 來取代一個文字字串。

例如，*.c?m 適用所有位址，最後面的部分以字母 c 開始，以字母 m 結束，它們中間包括一個未知符號 (.com、.cam 等)。

如果網域名稱中的「*.」位於開頭，則需要特別處理。首先，在此情況中 * 萬用字元將無法與分號字元 (’/’) 相符。此是為了避免規避遮罩，例如遮罩 **.domain.com* 就不會與 *http://anydomain.com/anypath#.domain.com* 相符（這類字尾可以在不影響下載的情況下附加於任何 URL 之後)。第二，「*.」於此特殊情況下仍能與空白字串相符。這是為了能允許比對整個網域，包含任何使用單一遮罩的子網域在內。例如，遮罩 **.domain.com* 也與 *http://domain.com.* 相符。使用 **domain.com* 則不正確，因為它也與 *http://anotherdomain.com* 相符。

HTTP 流量掃描

預設情況下，ESET Internet Security 配置為掃描網際網路瀏覽器和其他應用程式使用的 HTTP 和 HTTPS 流量。僅當您在使用第三方軟體時遇到問題並想知道問題是否由 ESET Internet Security 引起時，才應停用流量掃描。

啟用 HTTP 流量掃描 – 一律監視所有應用程式在所有連接埠上的 HTTP 流量。

啟用 HTTPS 流量掃描 - HTTPS 流量使用加密的通道以在伺服器與用戶端間傳輸資訊，ESET Internet Security 會檢查利用 SSL (安全通訊端層）與 TLS (傳輸層安全性）通訊協定的通訊。此程式將只掃描 **[HTTPS 通訊協定使用的連接埠]** 中定義的連接埠流量，無論其作業系統的版本為何（您可以將連接埠新增至預先定義的 443 和 0-65535)。

ThreatSense

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

除 Rootkit

ThreatSense 引擎設定選項可讓您指定數個掃描參數：

- 要掃描的檔案類型及副檔名
- 各種偵測方法的組合
- 清除的層級等

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

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

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

要掃描的物件

此區段可讓您定義要掃描是否有入侵的電腦元件及檔案。

[作業記憶體] - 掃描攻擊系統作業記憶體的威脅。

開機磁區/UEFI - 掃描開機磁區的主要開機記錄中是否有惡意軟體。請在字彙中閱讀更多有關 UEFI 的資訊

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。

[自我解壓檔] - 自我解壓檔 (SFX) 是可以自行解壓縮的壓縮檔。

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

掃描選項

選取在掃描系統是否有入侵時使用的方法。可用選項如下：

[啟發式[– 啟發式是分析程式（惡意）活動的演算法。這項技術的主要優點是可以識別不存在或先前偵測引擎不瞭解的惡意軟體。缺點是有錯誤警示的可能性（很小）。

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

清除

清除設定會決定 ESET Internet Security 在清除物件期間的行為。清除層級有 4 個：

ThreatSense 具有下列修復（即，清除）層級。

ESET Internet Security 中的修復

清除層級	說明
一律修復偵測	清除物件時嘗試修復偵測，不需要任何使用者介入。在某些少見的情況下（例如，系統檔案），如果無法修復偵測，回報的物件會保持在原始位置。
如果安全無虞則修復偵測，否則請保留	清除物件時嘗試修復偵測，不需要任何使用者介入。在某些情況下（例如，同時具有乾淨或受感染檔案的系統檔案或壓縮檔），如果無法修復偵測，回報的物件會保持在原始位置。
如果安全無虞則修復偵測，否則請詢問	清除物件時嘗試修復偵測。在某些情況下，如果無法執行任何動作，使用者會收到互動警告且必須選取修復的動作（例如，刪除或忽略）。建議對大多數情況使用此設定。
一律詢問使用者	使用者會在清除物件時收到互動視窗，而且必須選取修復動作（例如，刪除或忽略）。此層級是針對其他進階使用者而設計的，這些進階使用者瞭解偵測時需採取哪些步驟。

排除

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

其他

配置指定電腦掃描的 ThreatSense 引擎參數時，**[其他]** 區段也有以下可用選項：

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

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

[記錄所有物件] – 掃描防護記錄將顯示自我解壓檔中所有掃描的檔案，即使未受到感染的檔案也會顯示（可能產生許多掃描防護記錄資料，因而增加掃描防護記錄檔案的大小）。

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

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

限制

[限制] 區段可讓您指定物件的大小上限，以及要掃描的巢狀保存檔層級：

物件設定

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

物件的掃描時間上限（秒） – 定義掃描容器物件的時間值上限（例如 RAR/ZIP 壓縮檔或具有多個附件的電子郵件）。此設定不適用於獨立檔案。如果已輸入使用者定義的值，且已經過指定時間，則掃描將儘快停止，不論容器物件中每個檔案的掃描是否已完成。
如果壓縮檔帶有大型檔案，掃描將不會比擷取壓縮檔中的檔案更早結束（例如，當使用者定義的變數為 3 秒，而檔案擷取需要 5 秒）。該時間經過後，將不會掃描壓縮檔中的其餘檔案。
若要限制掃描時間（包括較大的壓縮檔），請在壓縮檔中使用 **[物件大小上限]** 和 **[壓縮檔中檔案的大小上限]**（不建議，因為可能存在安全風險）。
預設值：無限制

壓縮檔掃描設定

壓縮檔巢狀層級 – 指定壓縮檔掃描的深度上限。預設值：10.

壓縮檔中檔案的大小上限 – 此選項可讓您指定要掃描的壓縮保存檔中，所包含檔案的大小上限（解壓縮時）。最大值是 **3 GB**

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。

家長控制

[啟用家長控制] 選項會將家長控制整合至 ESET Internet Security按一下使用者帳戶旁邊的 **[編輯]**，將由家長控制使用的 Windows 使用者帳戶與特定使用者建立關聯，來限制其存取網際網路上的不適當或有害內容。

使用者帳戶

在 [進階設定] > [防護] > [Web 存取防護] > [家長控制] > [使用者帳戶] > [編輯] 中，您可以將由家長控制使用的 Windows 使用者帳戶與特定使用者關聯，以限制其存取網際網路上的不適當或有害內容。

直欄

[Windows 帳戶] – 使用者的名稱。

[已啟用] – 啟用後，將啟動特定使用者帳戶的家長控制。

[網域] – 使用者所屬的網域名稱。

[生日] – 此帳戶所屬的使用者年齡。

控制項元素

[新增] – 使用使用者帳戶對話方塊將會顯示。

編輯—此選項可讓您編輯選取的帳戶。

[刪除] – 刪除已選取的帳戶。

[重新整理] – 若您已新增使用者帳戶，ESET Internet Security 可重新整理使用者帳戶清單，無須重新開啟此視窗。

使用者帳戶設定

視窗有三個索引標籤：

一般

啟用 **[已啟用]** 旁的切換開關，以開啟下方所選 Windows 帳戶的家長控制。

首先，**[選取]** 電腦中的 Windows 帳戶。家長控制中的限制設定只影響標準的 Windows 帳戶。管理帳戶可以覆寫限制。

若帳戶使用者為家長，請選取 **[家長帳戶]**。

設定帳戶的 **[兒童生日]**，以決定他們的存取層級並針對適合年齡的建議網頁設定存取規則。

記錄嚴重性

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

- **診斷** – 記錄微調程式時所需的資訊。
- **資訊** – 記錄資訊性訊息，包含允許和封鎖的例外，以及上述所有記錄。
- **警告** – 記錄嚴重錯誤及警告訊息。
- **無** – 不記錄任何防護記錄。

例外

建立例外可允許或拒絕使用者存取不在例外清單上的網站。若您想控制特定網站的存取權限而非使用類別，這個方式相當實用。您可複製針對某個帳戶建立的例外並將其用於其他帳戶。若您想為年齡相近的兒童建立相同規則，這相當實用。

按一下 **[新增]** 以建立新的例外。使用下拉式功能表指定 **[處理方法]**（例如，**[封鎖]**）、輸入此例外將套用的**網站 URL**，接著按一下 **[確定]**。例外將會新增至現有的例外清單，並顯示其狀態。

[新增] - 建立新例外。

[編輯] - 您可以編輯所選例外的 **[網站 URL]** 或 **[處理方法]**。

刪除 - 移除選取的例外。

[複製] - 從下拉式功能表選取您要從其位置複製已建立例外的使用者。

所定義的例外會覆寫針對選取帳戶所定義的類別。例如，如果帳戶的 **[新聞]** 類別遭到封鎖，但是您已將新聞網頁定義為允許的例外，帳戶便能存取允許的網頁。您可以在例外區段中檢視此處進行的任何變更。

類別

在 **[類別]** 索引標籤中，您可以定義要針對每個帳戶封鎖或允許的一般網站類別。選取類別旁的核取方塊以允許該類別。如果您讓核取方塊保持空白，則該帳戶將不允許使用此類別。

[複製] - 讓您從現有的已修改帳戶複製遭封鎖或允許的類別清單。

類別

勾選類別旁邊的［**已啟用**］欄中的核取方塊，以允許該類別。如果您讓核取方塊保持關閉，則該帳戶將不允許使用此類別。

以下為使用者可能不熟悉之類別（群組）的範例：

- ［**其他選項**］ - 通常是私人（本機）IP 位址，例如內部網路、127.0.0.0/8、192.168.0.0/16 等。若顯示 403 或 404 錯誤碼，則該網站也符合此類別。

- **[未解決]** – 此類別包含在連線至家長控制資料庫引擎時，因為發生錯誤而未解析的網頁。
- **[未分類]** – 尚未出現在家長控制資料庫中的不明網頁。
- **[動態]** – 會重新導向至其他網站頁面的網頁。

瀏覽器防護

瀏覽器防護是用來保護安全性和隱私的另一層防護，可保護瀏覽器記憶體免受其他程序監測、提高對鍵盤記錄程式的防範，並防止將任何被惡意軟體修改的線上支付相關資料從剪貼簿複製到安全的瀏覽器中。若要配置瀏覽器防護，請開啟 [進階設定] > **[防護]** > **[瀏覽器防護]**，然後從以下配置選項中進行選擇：

- 安全銀行與瀏覽
- 瀏覽器防護允許清單
- 瀏覽器的框架

安全銀行與瀏覽

您可以在 [進階設定] > **[保護]** > **[瀏覽器防護]** > **[安全銀行與瀏覽]** 中，配置安全銀行與瀏覽。

安全銀行與瀏覽

啟用安全銀行與瀏覽—當「安全銀行與瀏覽」啟用時，所有支援的 Web 瀏覽器預設將以安全模式啟動。

瀏覽器防護

啟用 **[保護所有瀏覽器]** 以在安全模式中啟動所有支援的 Web 瀏覽器。

延伸模組安裝模式 – 從下拉式功能表中，您可以選擇在受 ESET 保護的瀏覽器上允許安裝哪些延伸模組：

- **基本延伸模組** – 僅由特定瀏覽器製造商開發的最重要延伸模組。
- **所有延伸模組** – 特定瀏覽器支援的所有延伸模組。

> 變更延伸模組安裝模式不會影響先前安裝的瀏覽器延伸模組：

保護瀏覽器

[加密的記憶體防護] – 若已啟用，安全的瀏覽器記憶體將會受到保護，不會遭到其他處理程序監測。

鍵盤防護 – 如果啟用，透過鍵盤輸入到安全的瀏覽器資訊將會在其他應用程式中隱藏。這可增強對於鍵盤記錄程式的防護。

剪貼簿防護—若啟用ESET Internet Security 將防止將被惡意軟體修改的任何線上支付相關資料從剪貼簿貼到安全的瀏覽器中。這可確保防禦惡意軟體進行的潛在變更。

瀏覽器的框架 – 在受保護的瀏覽器中個人化瀏覽器框架的顯示設定。

瀏覽器防護允許清單 – 管理新增至瀏覽器防護允許清單的檔案。

瀏覽器隱私權與安全性

瀏覽器隱私權與安全性—若停用，則瀏覽器隱私權與安全性延伸模組將從所有 Windows 帳戶中所有支援的瀏覽器中解除安裝。

顯示「瀏覽器隱私權與安全性」通知—若啟用，ESET Internet Security 將顯示「瀏覽器隱私權與安全性」通知。

瀏覽器腳本掃描器

啟用瀏覽器指令碼進階掃描—若啟用，則防毒掃描器將檢查由網際網路瀏覽器執行的所有 JavaScript 程式。

00

裝置控制

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

支援的外部裝置：

- 磁碟儲存裝置 (HDD、USB 卸除式磁碟）
- CD/DVD
- USB 印表機
- FireWire儲存裝置
- Bluetooth 裝置
- 智慧卡讀卡機
- 影像裝置
- 數據機
- LPT/COM 連接埠
- 可攜式裝置（電池供電裝置，例如媒體播放器、智慧型手機、即插即用裝置等）
- 所有裝置類型

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

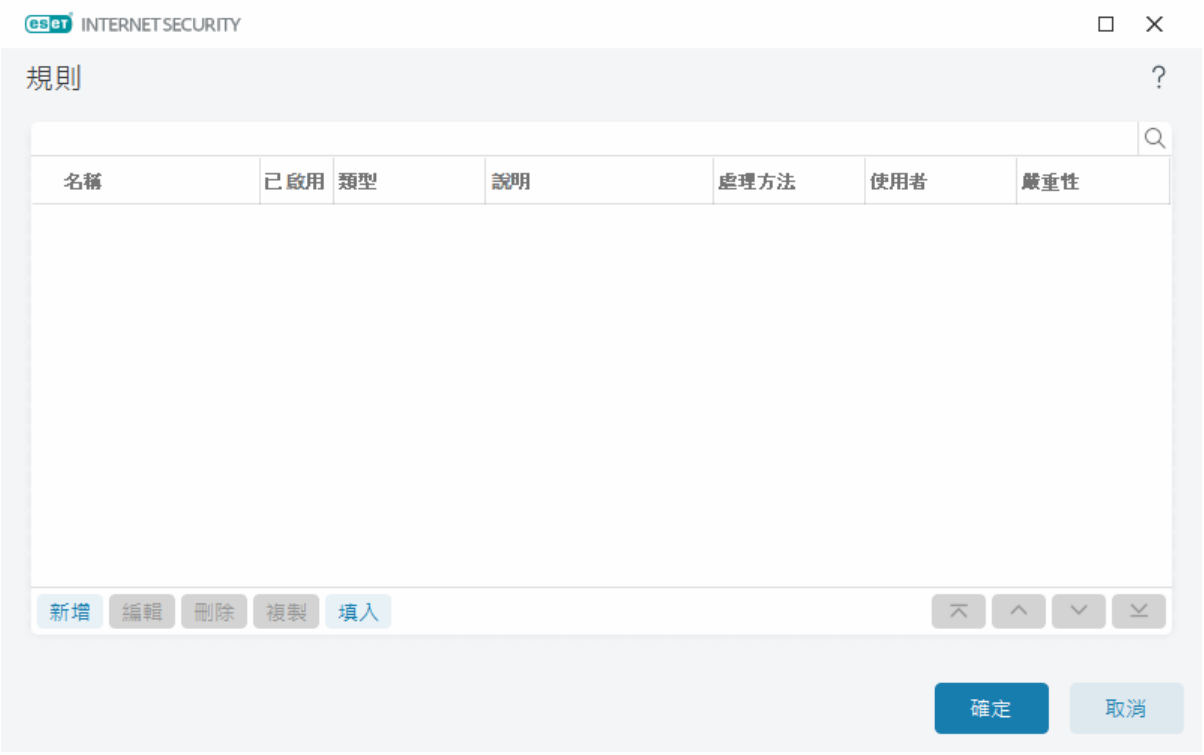
按一下 **[啟用裝置控制]** 切換開關以啟用 ESET Internet Security 中的裝置控制功能；您必須重新啟動電腦才能使此變更生效。啟用裝置控制後，您可以在規則編輯器視窗中定義 **[規則]**。

> 您可以建立不同裝置群組，並套用不同規則。您也可以只建立一個裝置群組，該群組會套用具有 **[允許]** 或 **[寫入封鎖]** 的規則。這樣可確保在無法辨識的裝置連接至您電腦時，裝置控制會將其封鎖。

如果插入的裝置遭到現有規則封鎖，將會顯示通知視窗且不授與裝置的存取權限。

裝置控制規則編輯器

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



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

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 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；如果您想保留規則，此選項很有用。

按一下 **[填入]** 可為電腦所連接的裝置自動填入可移除媒體裝置參數。

規則會依據優先順序列出，順序較高的規則會較靠近頂端。您可以按一下  **[頂端/向上/向下/底端]** 以個別或群組的方式移動規則。

您可以在主要程式視窗 > **[工具]** > [防護記錄檔案]中查看防護記錄項目。

裝置控制防護記錄會記錄所有裝置控制防護遭到觸發的事件。

偵測到的裝置

[填入] 按鈕會就所有目前已連接裝置提供下列相關資訊概觀：裝置類型、關於裝置廠商、型號和序號（若有的話）。如果要查看所有隱藏裝置，請選取 **[顯示隱藏的裝置]**

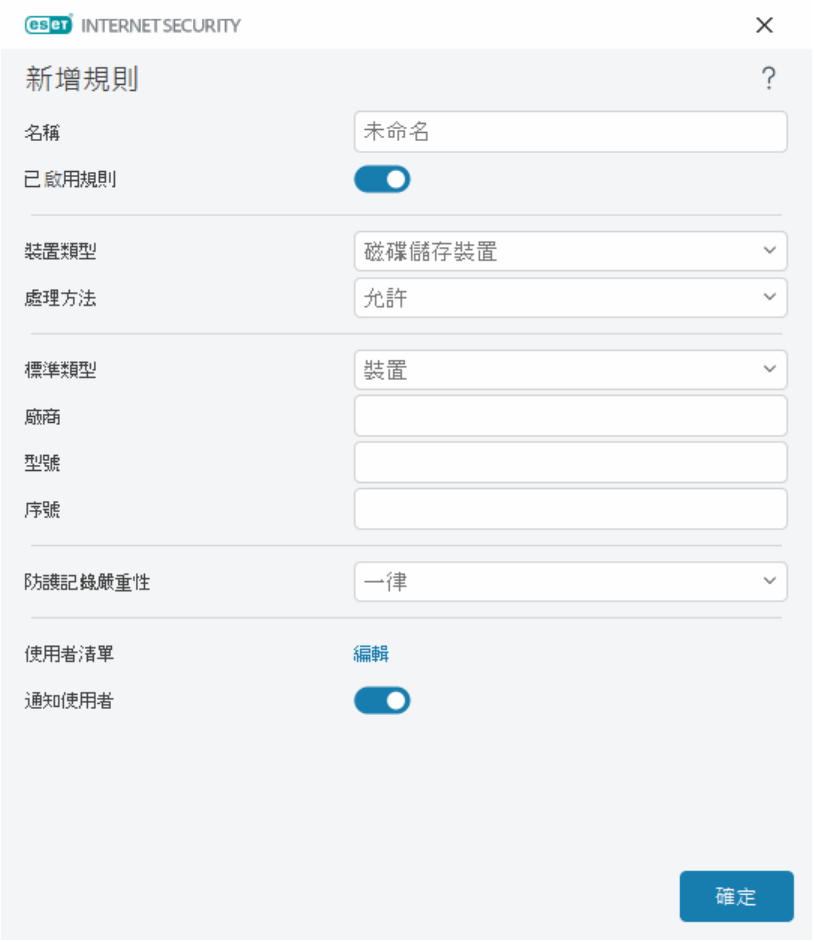
從偵測到的裝置中選取裝置，然後按一下［**確定**］來［新增裝置控制規則］以及預先定義的資訊（所有設定都可以調整）。

低電量（睡眠）模式中的裝置會以警告圖示 標記。若要啟用［**確定**］按鈕及為此裝置新增規則：

- 中斷裝置的連線
- 使用裝置（例如，在 Windows 中啟動攝影機應用程式以喚醒網路攝影機）。

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會採取的處理方法。



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

裝置類型

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

處理方法

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

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

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

標準類型

選取 **[裝置群組]** 或 **[裝置]**。

下面列出的其他參數可用於微調不同裝置的規則。所有參數均區分大小寫並支援萬用字元（*、？）：

- **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。

如果並未定義這些參數，規則在比對時就會忽略這些欄位。所有文字欄位中的篩選參數均區分大小寫並支援萬用字元（問號（?）代表一個字元，而星號（*）代表含有零或多個字元的字串）。

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

記錄嚴重性

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

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

使用者清單

按一下 **[使用者清單]** 旁邊的 **[編輯]**，將某些使用者或使用者群組新增至使用者清單後，即可將規則限制在新增的使用者或使用者群組。

- **新增** – 開啟 **[物件類型：使用者或群組]** 對話方塊視窗，可讓您選取所需的使用者。

- **[移除]** – 從過濾移除選取的使用者。

使用者清單限制
無法為具有特定裝置類型的規則定義使用者清單：
- USB 印表機
- 藍牙裝置
- 智慧卡讀卡機
- 影像裝置
- 數據機
- LPT/COM 連接埠

[通知使用者] – 如果插入的裝置遭到現有規則封鎖，系統會顯示通知視窗。

裝置群組

連接至您電腦的裝置可能會造成安全風險。

[裝置群組] 視窗分成兩部分。視窗右側包括屬於個別群組的裝置清單，視窗左側包含已建立的群組。選取要在右窗格中顯示裝置的群組。

當您開啟 [裝置群組] 視窗並選取群組時，您可以從清單新增或移除裝置。另一種將裝置新增至群組的方式為從檔案匯入。或者，您可以按一下 **[填入]** 按鈕，所有連接到您電腦的裝置便會列示於 **[偵測到的裝置]** 視窗。從已填入清單選取裝置，按一下 **[確定]** 將其新增至群組。

控制項元素

[新增] – 您可透過輸入名稱將群組或裝置新增至現有群組，取決於您按一下按鈕的視窗部分而定。

編輯 – 讓您修改已選取群組的名稱或裝置的參數（供應商、型號和序號）。

刪除 – 取決您在視窗哪個位置上按下按鈕，刪除已選取群組或裝置。

匯入 – 從文字檔匯入裝置清單。從文字檔匯入裝置需要正確的格式：

- 每個裝置都從新的行開始。
- **供應商ID型號**和**序號**必須存在於每個裝置上，並且使用逗號分隔。

以下是文字檔內容的範例：
```
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101
```

匯出 – 將裝置清單匯出到檔案。

[填入] 按鈕會就所有目前已連接裝置提供下列相關資訊概觀：裝置類型、關於裝置廠商、型號和序號（若有的話）。

新增裝置

按一下右視窗中的 **[新增]** 以將裝置新增至現有群組。下面列出的其他參數可用於微調不同裝置的規則。所有參數均區分大小寫並支援萬用字元（*、？）：

- **[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。
- **[說明]**—您對裝置的說明以便更好地進行組織。

如果並未定義這些參數，規則在比對時就會忽略這些欄位。所有文字欄位中的篩選參數均區分大小寫並支援萬用字元（問號［?］代表一個字元，而星號［*］代表含有零或多個字元的字串）。

按一下 **[確定]** 儲存變更。按一下 **[取消]**，以離開 **[裝置群組]** 視窗而不儲存變更。

建立裝置群組後，您必須為建立的裝置群組新增新的裝置控制規則並選擇要執行的處理方法。

請注意，並非所有裝置類型都適用所有處理方法（權限）。如果是儲存類型裝置，則所有四個處理方法均適用。對於非儲存裝置，只可使用三種處理方法（例如，**[寫入封鎖]** 不適用於藍牙，因此只能允許、封鎖或警告藍牙裝置）。

網路攝影機防護

[網路攝影機防護] 可通知您存取電腦網路攝影機的程序與應用程式。當應用程式嘗試存取您的網路攝影機時，系統將會顯示 **[允許]** 或 **[封鎖]** 存取的通知。警告視窗的顏色取決於應用程式聲譽。

可在 [進階設定] > **[防護]** > **[裝置控制]** > **[網路攝影機防護]** 中修改網路攝影機防護設定選項。

啟用 **[啟用網路攝影機防護]** 旁的滑動軸，便會啟動 ESET Internet Security 中的網路攝影機防護功能。

在啟用網路攝影機防護時，**[規則]** 將會變成啟用狀態，使您可以開啟規則編輯器視窗。

若要關閉規則為已修改但仍具有有效數位簽章（例如，應用程式更新）的應用程式警報，請啟用**為已修改的應用程式停用網路攝影機存取警告**旁的滑動軸。

網路攝影機防護規則編輯器

此視窗會顯示現有規則，並根據您採取的處理方法，來控制存取電腦網路攝影機的應用程式和處理程序。

以下是可用的處理方法：

- **允許存取**
- **封鎖存取**
- **詢問**（每次應用程式嘗試存取網路攝影機時詢問使用者）

取消選取 **[通知]** 欄中的核取方塊，以在應用程式存取網路攝影機時停止接收通知。

圖解指示
如何在 ESET Internet Security 中建立及編輯網路攝影機規則

ThreatSense

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

ThreatSense 引擎設定選項可讓您指定數個掃描參數：

- 要掃描的檔案類型及副檔名
- 各種偵測方法的組合
- 清除的層級等

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

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

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

要掃描的物件

此區段可讓您定義要掃描是否有入侵的電腦元件及檔案。

[作業記憶體] - 掃描攻擊系統作業記憶體的威脅。

開機磁區/UEFI - 掃描開機磁區的主要開機記錄中是否有惡意軟體。請在字彙中閱讀更多有關 UEFI 的資訊。

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。

[自我解壓檔] - 自我解壓檔 (SFX) 是可以自行解壓縮的壓縮檔。

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

掃描選項

選取在掃描系統是否有入侵時使用的方法。可用選項如下：

[啟發式[– 啟發式是分析程式（惡意）活動的演算法。這項技術的主要優點是可以識別不存在或先前偵測引擎不瞭解的惡意軟體。缺點是有錯誤警示的可能性（很小）。

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

清除

清除設定會決定 ESET Internet Security 在清除物件期間的行為。清除層級有 4 個：

ThreatSense 具有下列修復（即，清除）層級。

ESET Internet Security 中的修復

清除層級	說明
一律修復偵測	清除物件時嘗試修復偵測，不需要任何使用者介入。在某些少見的情況下（例如，系統檔案），如果無法修復偵測，回報的物件會保持在原始位置。
如果安全無虞則修復偵測，否則請保留	清除物件時嘗試修復偵測，不需要任何使用者介入。在某些情況下（例如，同時具有乾淨或受感染檔案的系統檔案或壓縮檔），如果無法修復偵測，回報的物件會保持在原始位置。
如果安全無虞則修復偵測，否則請詢問	清除物件時嘗試修復偵測。在某些情況下，如果無法執行任何動作，使用者會收到互動警告且必須選取修復的動作（例如，刪除或忽略）。建議對大多數情況使用此設定。
一律詢問使用者	使用者會在清除物件時收到互動視窗，而且必須選取修復動作（例如，刪除或忽略）。此層級是針對其他進階使用者而設計的，這些進階使用者瞭解偵測時需採取哪些步驟。

排除

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

其他

配置指定電腦掃描的 ThreatSense 引擎參數時，**[其他]** 區段也有以下可用選項：

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

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

[記錄所有物件] – 掃描防護記錄將顯示自我解壓檔中所有掃描的檔案，即使未受到感染的檔案也會顯示（可能產生許多掃描防護記錄資料，因而增加掃描防護記錄檔案的大小）。

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

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

限制

[限制] 區段可讓您指定物件的大小上限，以及要掃描的巢狀保存檔層級：

物件設定

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

物件的掃描時間上限（秒） – 定義掃描容器物件的時間值上限（例如 RAR/ZIP 壓縮檔或具有多個附件的電子郵件）。此設定不適用於獨立檔案。如果已輸入使用者定義的值，且已經過指定時間，則掃描將儘快停止，不論容器物件中每個檔案的掃描是否已完成。
如果壓縮檔帶有大型檔案，掃描將不會比擷取壓縮檔中的檔案更早結束（例如，當使用者定義的變數為 3 秒，而檔案擷取需要 5 秒）。該時間經過後，將不會掃描壓縮檔中的其餘檔案。
若要限制掃描時間（包括較大的壓縮檔），請在壓縮檔中使用 **[物件大小上限]** 和 **[壓縮檔中檔案的大小上限]**（不建議，因為可能存在安全風險）。
預設值：無限制

壓縮檔掃描設定

壓縮檔巢狀層級 – 指定壓縮檔掃描的深度上限。預設值：10.

壓縮檔中檔案的大小上限 – 此選項可讓您指定要掃描的壓縮保存檔中，所包含檔案的大小上限（解壓縮時）。最大值是 **3 GB**

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。

清除層級

若要變更所需防護模組的清除層級設定，請展開 **[ThreatSense]**（例如，**[即時檔案系統防護]**），然後從下拉式功能表中選擇 **[清除層級]**

ThreatSense 具有下列修復（即，清除）層級。

ESET Internet Security 中的修復

清除層級	說明
一律修復偵測	清除物件時嘗試修復偵測，不需要任何使用者介入。在某些少見的情況下（例如，系統檔案），如果無法修復偵測，回報的物件會保持在原始位置。
如果安全無虞則修復偵測，否則請保留	清除物件時嘗試修復偵測，不需要任何使用者介入。在某些情況下（例如，同時具有乾淨或受感染檔案的系統檔案或壓縮檔），如果無法修復偵測，回報的物件會保持在原始位置。
如果安全無虞則修復偵測，否則請詢問	清除物件時嘗試修復偵測。在某些情況下，如果無法執行任何動作，使用者會收到互動警告且必須選取修復的動作（例如，刪除或忽略）。建議對大多數情況使用此設定。
一律詢問使用者	使用者會在清除物件時收到互動視窗，而且必須選取修復動作（例如，刪除或忽略）。此層級是針對其他進階使用者而設計的，這些進階使用者瞭解偵測時需採取哪些步驟。

從掃描中排除的檔案副檔名

排除的檔案副檔名是 ThreatSense 的一部分。若要配置排除的檔案副檔名，請針對任何使用 ThreatSense 技術的模組按一下［進階設定］中的 **[ThreatSense]**。

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 設定的此區段可讓您定義要掃描的檔案類型。

> 請勿與程序排除、HIPS 排除或檔案/資料夾排除混淆。

依預設，會掃描所有檔案。可以將任何副檔名新增至從掃描中排除的檔案清單。

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

> 若要將新的副檔名新增至清單，請按一下 **［新增］**。在空白欄位輸入副檔名（例如 tmp），然後按一下 **［確定］**。當您選取 **［輸入多個值］** 時，您可新增多個以行、逗號或分號分隔的檔案副檔名（例如，從下拉式功能表中選擇 **［分號］** 作為分隔符號，然後輸入 `edb;eml;tmp`）。
> 您可以使用特殊符號 ？（問號）。問號代表任何符號（例如 `?db`）

> 若要查看 Windows 作業系統中，檔案的具體副檔名（若有），您必須從 **[Windows 檔案總管] > [檢視]**（標籤）中選取 **［檔案名稱副檔名］** 核取方塊。

其他 ThreatSense 參數

若要編輯這些設定，請開啟 [進階設定] > [防護] > [即時檔案系統防護] > [其他 ThreatSense 參數]。

用於新建立及已修改檔案的其他 ThreatSense 參數

新建立或已修改檔案感染的可能性高於現有的檔案。這正是為何程式會以額外的掃描參數檢查這些檔案的原因。ESET Internet Security 使用進階啟發式並搭配病毒碼式掃描方法，可在偵測引擎更新發行前先偵測新威脅。

除了新建立的檔案之外，也可針對 [自我解壓檔] (.sfx) 及 [執行階段惡意加殼]（內部壓縮的執行檔案）執行掃描。依預設，至多可以掃描至保存檔的第 10 層巢狀層級，並不論其實際大小都會進行檢查。若要修改壓縮檔掃描設定，請取消選取 [預設壓縮檔掃描設定]。

用於已執行檔案的其他 ThreatSense 參數

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

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

工具

您可以在 [進階設定] > [工具] 中為提供額外安全性的功能配置進階設定，並有助於簡化 ESET Internet Security 管理。

- Microsoft Windows® 更新
- ESET CMD
- 防護記錄檔案
- 玩家模式
- 診斷

Microsoft Windows® 更新

Windows Update 功能是保護使用者遠離惡意軟體的重要元件。出於這個原因，當有可用的 Microsoft Windows 更新時，立即安裝更新是很重要的。ESET Internet Security 會根據您在 [進階設定] > [工具] 中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。

對話方塊視窗 – 系統更新

如果您的作業系統有更新，ESET Internet Security 會在 主要程式視窗 > **[概觀]** 中顯示通知。按一下 **[更多資訊]** 以開啟 [系統更新] 視窗。

[系統更新] 視窗會顯示已準備好下載及安裝的可用更新清單。更新類型會顯示在更新名稱的旁邊。

在任何更新列上按兩下以顯示包含其他資訊的更新資訊視窗。

按一下 **[執行系統更新]** 以下載並安裝所有列出的作業系統更新。

更新資訊

[系統更新] 視窗會顯示已準備好下載及安裝的可用更新清單。更新優先順序層級會顯示在更新名稱的旁邊。

按一下 **[執行系統更新]**，以開始下載及安裝作業系統更新。

以滑鼠右鍵按一下任何更新列，然後按一下 **[顯示資訊]**，以在新視窗中顯示其他資訊。

ESET CMD

這是啟用進階 ecmd 命令的功能。其可讓您使用命令列 (ecmd.exe) 匯出及匯入設定。直到目前為止，僅可以使用 GUI 匯出設定，ESET Internet Security 配置可匯出到 xml.*xml* 檔案。

當您啟用 ESET CMD 時，有兩種授權方法可用：

- **[無]** – 無授權。不建議您使用此方法，因為其允許匯入任何未簽署的配置，因而造成潛在的風險。
- **[進階設定密碼]** – 從 .xml 檔案匯入配置需要密碼，這支檔案必須經過簽署（請參閱簽署 .xml 配置檔案以進一步瞭解）。必須在新的配置匯入之前，提供指定於存取設定的密碼。如果您沒有已啟用的存取設定，密碼不符或 .xml 配置檔案未經簽署，配置將不會匯入。

ESET CMD 啟用後，您可以使用指令列匯入或匯出 ESET Internet Security 配置。您可以手動執行它，或建立指令碼來自動執行它。

若要使用進階 ecmd 命令，您需要以管理員權限執行它們，或使用 **[以系統管理員身分執行]** 開啟 Windows 命令提示字元 (cmd)，否則，您將收到 **Error executing command** 訊息。此外，匯出配置時，目的地資料夾必須存在。即使在 ESET CMD 設定關閉時，匯出指令同樣會運作。

匯出設定命令：
```
ecmd /getcfg c:\config\settings.xml
```

匯入設定命令：
```
ecmd /setcfg c:\config\settings.xml
```

進階 ecmd 命令只能在本機執行。

簽署 .*xml* 配置檔案：

1. 下載 XmlSignTool 執行檔。

2. 使用 [**以管理員身分執行**] 開啟 Windows 命令提示字元 (cmd)。

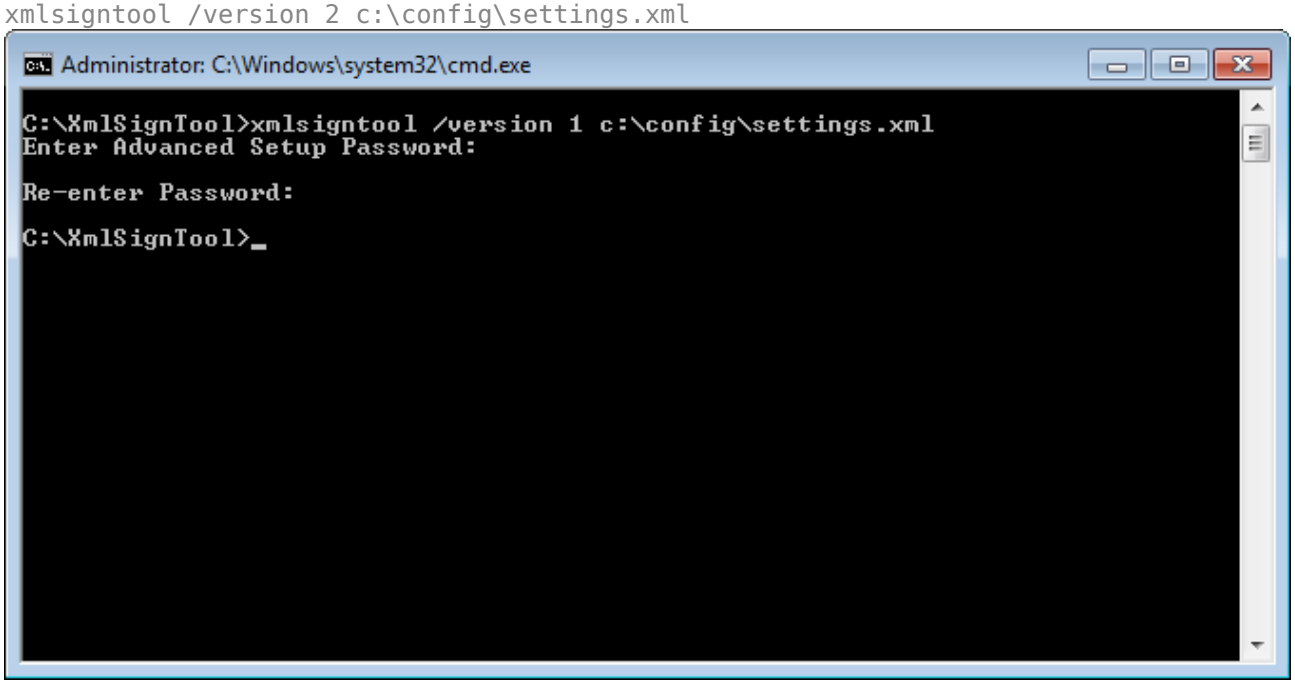
3. 請瀏覽至 `xmlsigntool.exe` 的儲存位置。

4. 執行命令來簽署 *.xml* 配置檔案，用法：`xmlsigntool /version 1|2 <xml_file_path>`

`/version` 參數的值取決於您 ESET Internet Security 的版本。針對 ESET Internet Security 早於 11.1 的舊版本，請使用 `/version 1`。針對 ESET Internet Security 目前的版本，請使用 `/version 2`。

5. 輸入並重新輸入 XmlSignTool 所提示的進階設定密碼。您的 *.xml* 配置檔案現在已完成簽署，而且可以用於匯入另一個具有 ESET CMD 的 ESET Internet Security 實例，方式為使用密碼授權方法。

簽署已匯出的配置檔案命令：
`xmlsigntool /version 2 c:\config\settings.xml`



如您的存取設定密碼已變更，而您想匯入較早以舊密碼簽署的配置，您需要使用目前的密碼再次簽署 *.xml* 配置檔案。這可讓您使用較舊的配置檔案，而不需要在匯入前先匯出配置檔案到另一台執行 ESET Internet Security 的電腦。

不建議在沒有授權的情況下啟用 ESET CMD，因為這將允許匯入任何未簽署的配置。在 [進階設定] > [**使用者介面**] > [**存取設定**] 中設定密碼，以防止使用者未經授權的修改。

防護記錄檔案

您可以在 [進階設定] > [**工具**] > [**防護記錄檔案**] 中找到 ESET Internet Security 的記錄配置。防護記錄區段用於定義管理防護記錄的方式。程式會自動刪除較舊的防護記錄以節省硬碟空間。您可以指定下列用於防護記錄檔案的選項：

記錄最簡化 – 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** – 記錄資訊性訊息，包含成功更新訊息及上述所有記錄。
- **警告** – 記錄嚴重錯誤及警告訊息。

- **錯誤** – 記錄諸如「下載檔案時發生錯誤」等類型的錯誤及嚴重錯誤。
- **[嚴重]** – 僅記錄嚴重錯誤（啟動病毒防護，防火牆，等）。

當您選取［診斷］冗贅層級時，將會記錄所有封鎖的連線。

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

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

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

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

- **[目標目錄]** – 防護記錄檔案要儲存在其中的目錄（僅適用於 Text/CSV）每個防護記錄區段皆具備已預先定義檔案名稱的檔案（例如，virlog.txt 適用於防護記錄檔案 **[偵測]** 區段）。
- **類型** – 若您選擇 **[文字]** 檔案格式，則防護記錄將以文字檔格式儲存，而資料將分隔為索引標籤。相同方法也適用於以逗號分隔的［**CSV**］檔案格式。若您選擇 **[事件]**，防護記錄將儲存於 Windows 事件記錄檔（可使用［控制台］中的［事件檢視器］進行檢視），與檔案相反。
- **[刪除所有防護記錄檔案]** – 消除所有目前在 **[類型]** 下拉式功能表中所選取的已儲存防護記錄。會顯示成功刪除記錄檔案的通知。

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

玩家模式

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

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

在［進階設定］> **[工具] > [玩家模式]** 中，啟動 **[以全螢幕執行應用程式時自動啟用玩家模式]**，在您起始全螢幕應用程式時啟動玩家模式，並在離開應用程式後停止。

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

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

診斷

診斷可提供 ESET 處理程序（例如，ekrn）的應用程式當機傾印。如果應用程式當機，就會產生傾印。這可以協助開發人員除錯和修正各種 ESET Internet Security 問題。

按一下［**傾印類型**］旁的下拉式功能表，並從三個可用選項中選取一個：

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

目標目錄 – 在當機期間產生傾印的目錄。

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

［**建立診斷傾印**］ – 按一下［**建立**］，在［**目標目錄**］中建立診斷傾印檔案。

進階記錄

在行銷訊息中啟用進階記錄 – 記錄產品內與行銷郵件有關的所有事件。

［**啟用反垃圾郵件引擎進階記錄**］ – 記錄在反垃圾郵件掃描期間發生的所有事件。這有助於開發人員診斷並修正與 ESET 反垃圾郵件引擎相關的問題。

［**啟用防盜引擎進階記錄**］ – 記錄所有發生在防盜中的事件，以進行診斷並解決問題。

啟用瀏覽器防護進階記錄—記錄「安全銀行與瀏覽」中發生的所有事件。

啟用電腦掃描器進階記錄 – 記錄透過電腦掃描來掃描檔案及資料夾時發生的所有事件。

［**啟用裝置控制進階記錄**］ – 記錄所有發生在裝置控制中的事件。這有助於開發人員診斷並修正與裝置控制相關的問題。

［**啟用 Direct Cloud 進階記錄**］ – 記錄所有發生在 ESET LiveGrid® 中的事件。這有助於開發人員診斷並修正與 ESET LiveGrid® 相關的問題。

［**啟用文件防護進階記錄**］ – 記錄所有發生於文件防護中的事件，以便您診斷和解決問題。

啟用電子郵件用戶端防護進階記錄 – 記錄在電子郵件用戶端防護和電子郵件用戶端外掛程式中發生的所有事件，以便診斷和解決問題。

啟用核心進階記錄 – 記錄所有發生於 ESET 核心 (ekrn) 中的事件。

［**啟用授權進階記錄**］ – 記錄與 ESET 啟用或 ESET License Manager 伺服器進行的所有產品通訊。

啟用記憶體追蹤 – 記錄所可協助開發人員診斷記憶體流失的事件。

［**啟用網路防護進階記錄**］ – 以 PCAP 格式記錄所有通過防火牆的網路資料，以協助開發人員診斷及修正防火牆的相關問題。

[啟用網路流量掃描器進階記錄] – 以 PCAP 格式記錄通過網路流量掃描器的所有資料，以協助開發人員診斷及修正與網路流量掃描器相關的問題。

啟用作業系統進階記錄 – 記錄其他的作業系統相關資訊，例如執行中的處理程序CPU 活動，及磁碟作業。這可幫助開發人員診斷及修正與在您作業系統上執行的 ESET 產品相關的問題。

[啟用家長控制進階記錄] – 記錄所有發生在家長控制中的事件。這有助於開發人員診斷並修正與家長控制相關的問題。

啟用推送訊息進階記錄 – 記錄在推送訊息期間發生的所有事件。

啟用即時檔案系統防護進階記錄 – 記錄透過即時檔案系統防護來掃描檔案及資料夾時發生的所有事件。

[啟用更新引擎進階記錄] – 記錄在記錄在更新程序期間發生的所有事件。這有助於開發人員診斷並修正與更新引擎相關的問題。

防護記錄檔案位於 *C:\ProgramData\ESET\ESET Security\Diagnostics*

技術支援

當從 ESET Internet Security 來連絡 ESET 技術支援時，您可以提交系統配置資料。從 **[提交系統配置資料]** 下拉式清單中選取 **[一律提交]** 以自動提交資料，或選取 **[提交之前詢問]** 以在提交資料之前先顯示提示。

連線

在特定網路中Proxy 伺服器可以調節電腦與網際網路的通訊。如果使用 Proxy 伺服器，則需要定義以下設定。否則ESET Internet Security 及其模組無法自動更新在 ESET Internet Security 中，Proxy 伺服器設定在進階設定的兩個不同區段中可用。

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

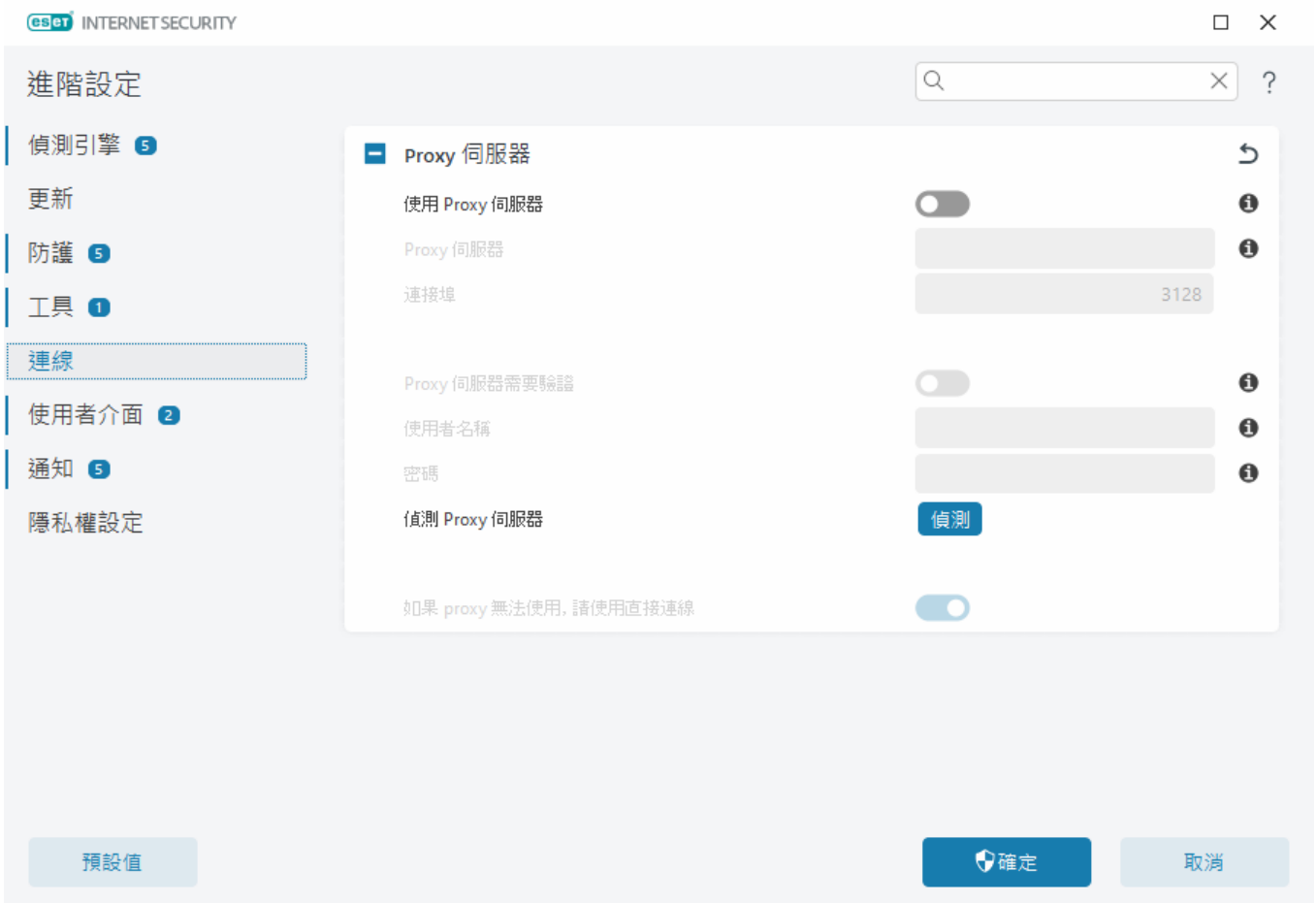
若要指定全域 Proxy 伺服器設定，請啟用 **[使用 Proxy 伺服器]**，然後鍵入 **Proxy 伺服器**位址以及 Proxy 伺服器的**連接埠**號。

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

您必須在 **[Proxy 伺服器]** 設定中手動輸入使用者名稱和密碼。

如果 Proxy 無法使用，請使用直接連線 – 如果 ESET Internet Security 已配置為透過 Proxy 連線，而 Proxy 無法存取ESET Internet Security 將避開 Proxy 並與 ESET 伺服器直接通訊。

也可以在 [進階設定] > **[更新]** > **[設定檔]** > **[更新]** > **[連線選項]** 中配置 Proxy 伺服器設定，方法是從 **[Proxy 模式]** 下拉式功能表中選取 **[透過 Proxy 伺服器連線]**。此配置僅適用於更新，建議用於從遠端位置接收模組更新的膝上型電腦。如需詳細資訊，請參考進階更新設定



使用者介面

若要配置程式的圖形使用者介面 (GUI) 行為，請開啟 [進階設定] > **[使用者介面]**。

您可以在 [使用者介面元素進階設定] 畫面中調整程式的視覺外觀與特效。

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透過密碼保護設定，來防止取消安裝或任何未經授權的變更。

若要配置系統通知、偵測警告和應用程式狀態的行為，請參閱通知一節。

使用者介面元素

您可以在 [進階設定] > **[使用者介面]** > **[使用者介面元素]** 中調整 ESET Internet Security 工作環境 (GUI) 以符合您的需要。

[色彩模式]—從下拉式功能表中選取 ESET Internet Security GUI 色彩配置：

- **[與系統色彩相同]**—根據您的作業系統設定設定 ESET Internet Security 的色彩配置。
- **[深色]**—ESET Internet Security 將具有深色配置（深色模式）。
- **[淺色]**—ESET Internet Security 將具有標準、淺色配置。

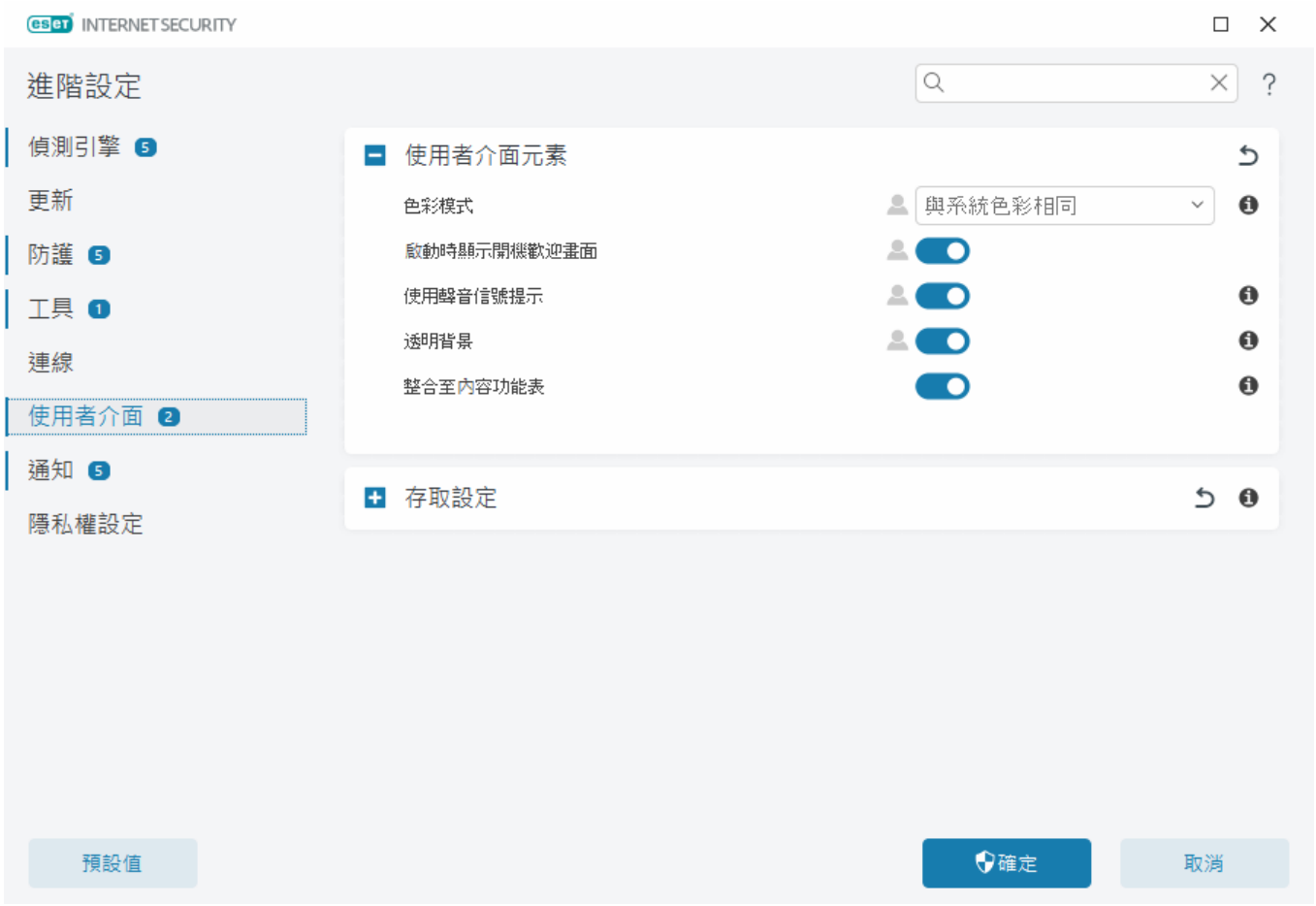
您也可以選擇主要程式視窗右上角的 ESET Internet Security GUI 色彩主題。

[啟動時顯示開機歡迎畫面] – 啟動時顯示 ESET Internet Security 開機歡迎畫面。

[使用聲音信號提示] – 會在掃描期間發生重大事件（例如當發現威脅或掃描結束）時播放音效。

[透明背景]—為主要程式視窗啟用透明背景效果。透明背景僅適用於最新 Windows 版本 (RS4 與更新版本)。

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



存取設定

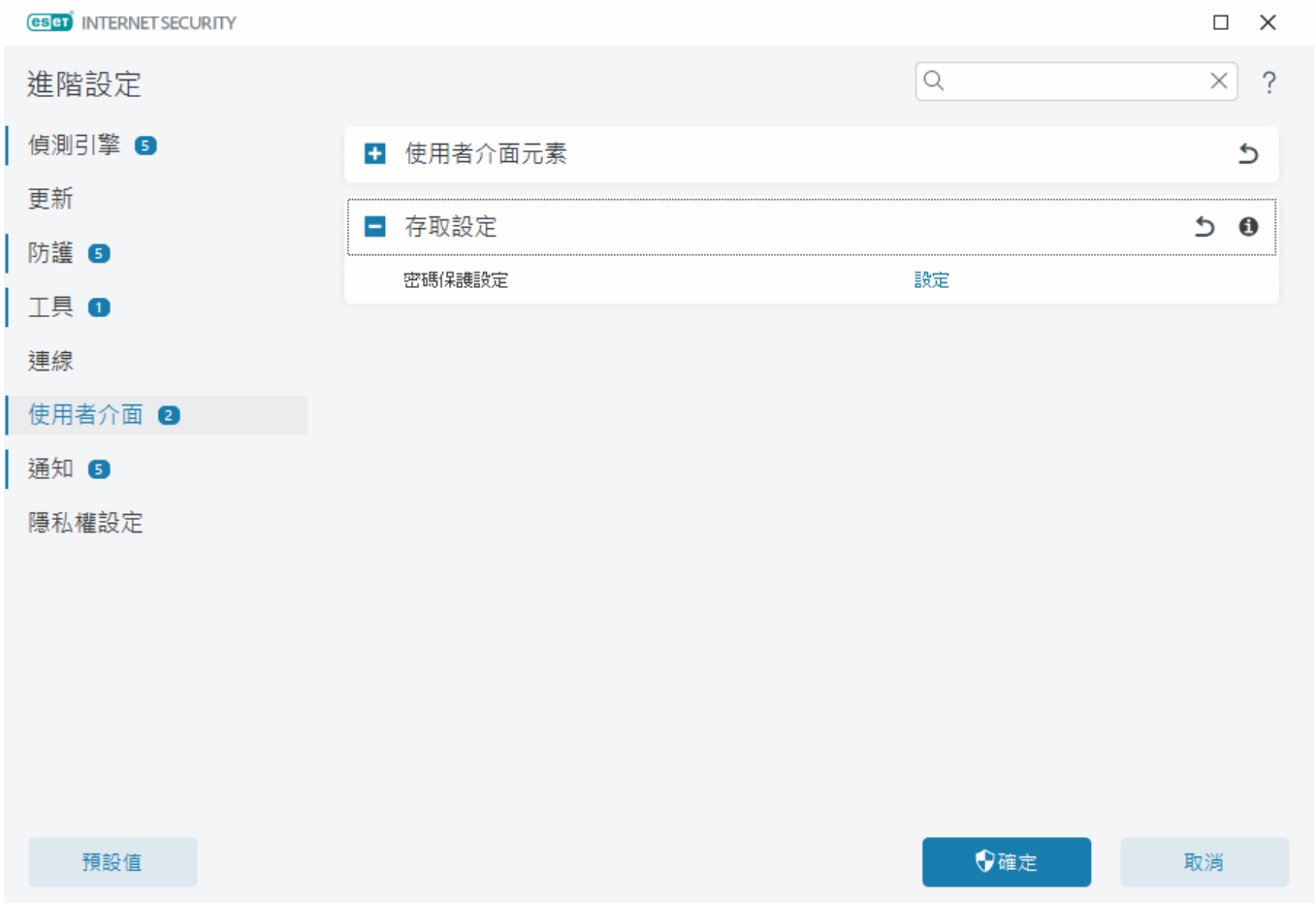
ESET Internet Security 設定是您安全原則最重要的部分。未獲授權的修改可能會危害您系統的穩定性及防護功能。為了避免未獲授權的修改，您可以使用密碼保護 ESET Internet Security 的設定參數及解除安裝。可以在 [進階設定] > **[使用者介面]** > **[存取設定]** 中配置存取設定。

若要設定密碼以保護設定參數和解除安裝 ESET Internet Security，請按一下 **[密碼保護設定]** 旁邊的 **[設定]**。

> 當您想要存取受保護的進階設定時，會顯示可供輸入密碼的視窗。如果您忘記或遺失密碼，請按一下下方的 **[還原密碼]** 選項，然後輸入您用於訂閱註冊的電子郵件地址。ESET 會將內含驗證碼和重設密碼指示的電子郵件傳送給您。
> - 如何解除鎖定進階設定

若要變更您的密碼，請按一下 **[密碼保護設定]** 旁邊的 **[變更密碼]**。

若要刪除您的密碼，請按一下 **[密碼保護設定]** 旁邊的 **[移除]**。



進階設定的密碼

若要保護 ESET Internet Security 進階設定並避免未經授權的修改，請在［**新密碼**］和［**確認密碼**］欄位中輸入您的新密碼。按一下［**確定**］。

當您想要變更現有的密碼時：

1. 請在［**舊密碼**］欄位中輸入您的舊密碼。
2. 在［**新密碼**］和［**確認密碼**］欄位中輸入您的新密碼。
3. 按一下［**確定**］。

需要此密碼才能存取進階設定。

如果忘記密碼，請參閱 ESET 家用產品中的解鎖設定密碼。

若要復原遺失的 ESET 啟動金鑰、訂閱的到期日期，或 ESET Internet Security 的其他訂閱資訊，請參閱我遺失我的啟動金鑰。

螢幕助讀程式支援

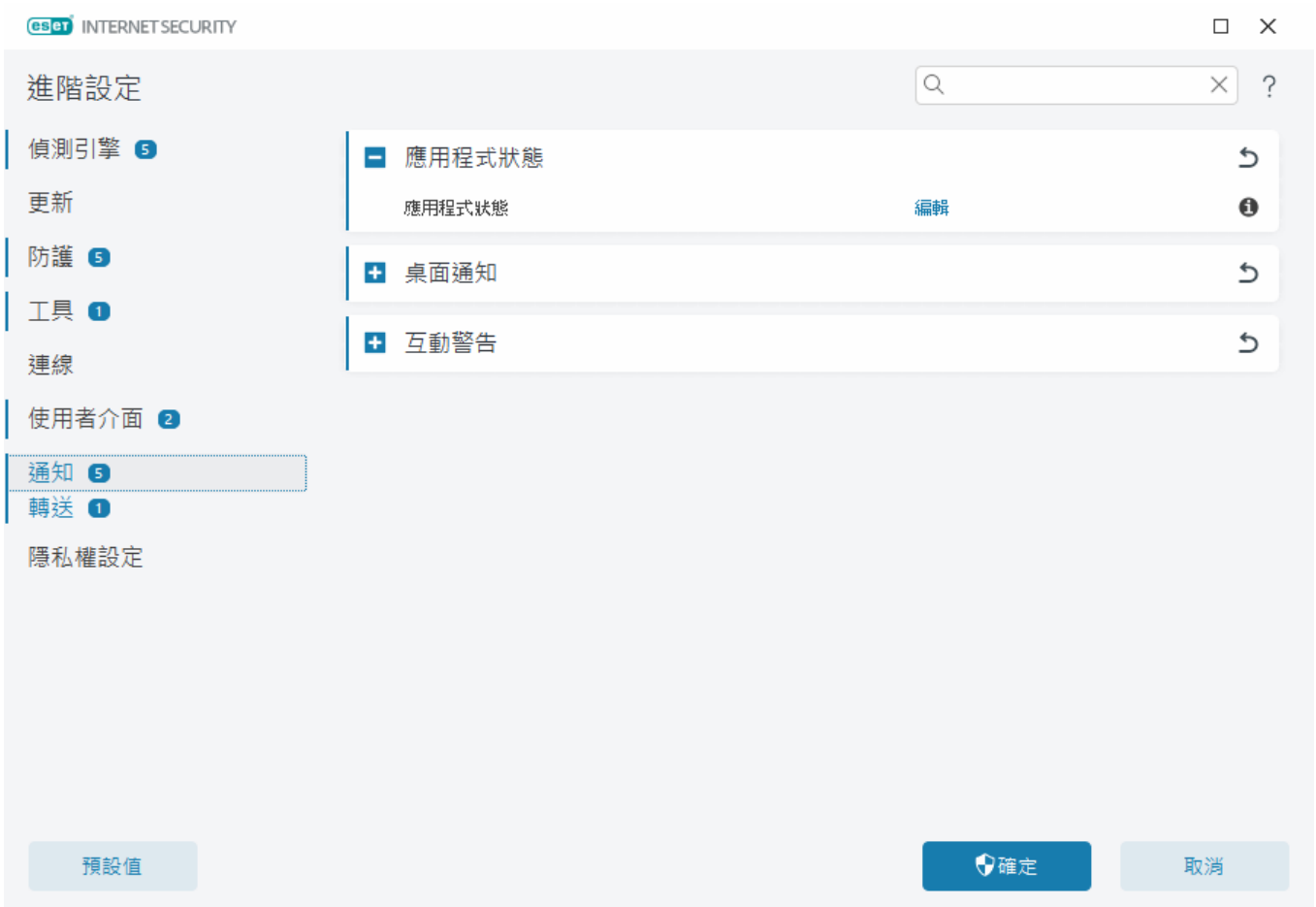
ESET Internet Security 可與螢幕助讀程式搭配使用，以便讓有視覺障礙的 ESET 使用者瀏覽產品或配置設定。(JAWS, NVDA, Narrator) 支援下列螢幕助讀程式。

若要確保螢幕助讀程式軟體可以正確存取 ESET Internet Security GUI，請遵循知識庫文章中的指示。

通知

若要管理 ESET Internet Security 通知，請開啟［進階設定］> **[通知]**。您可以配置以下類型的通知：

- 應用程式狀態 – 在主要程式視窗 > **[概觀]** 中顯示的通知。
- 桌面通知 – 系統工作列旁邊的小型通知。
- ［互動警告］ – 需要使用者互動的警示視窗與訊息方塊。
- 轉送（電子郵件通知） – 電子郵件通知會傳送到指定的電子郵件地址。



應用程式狀態

[應用程式狀態] – 按一下 **[編輯]** 以選取將在主要程式視窗 > **[概觀]** 中顯示的應用程式狀態。

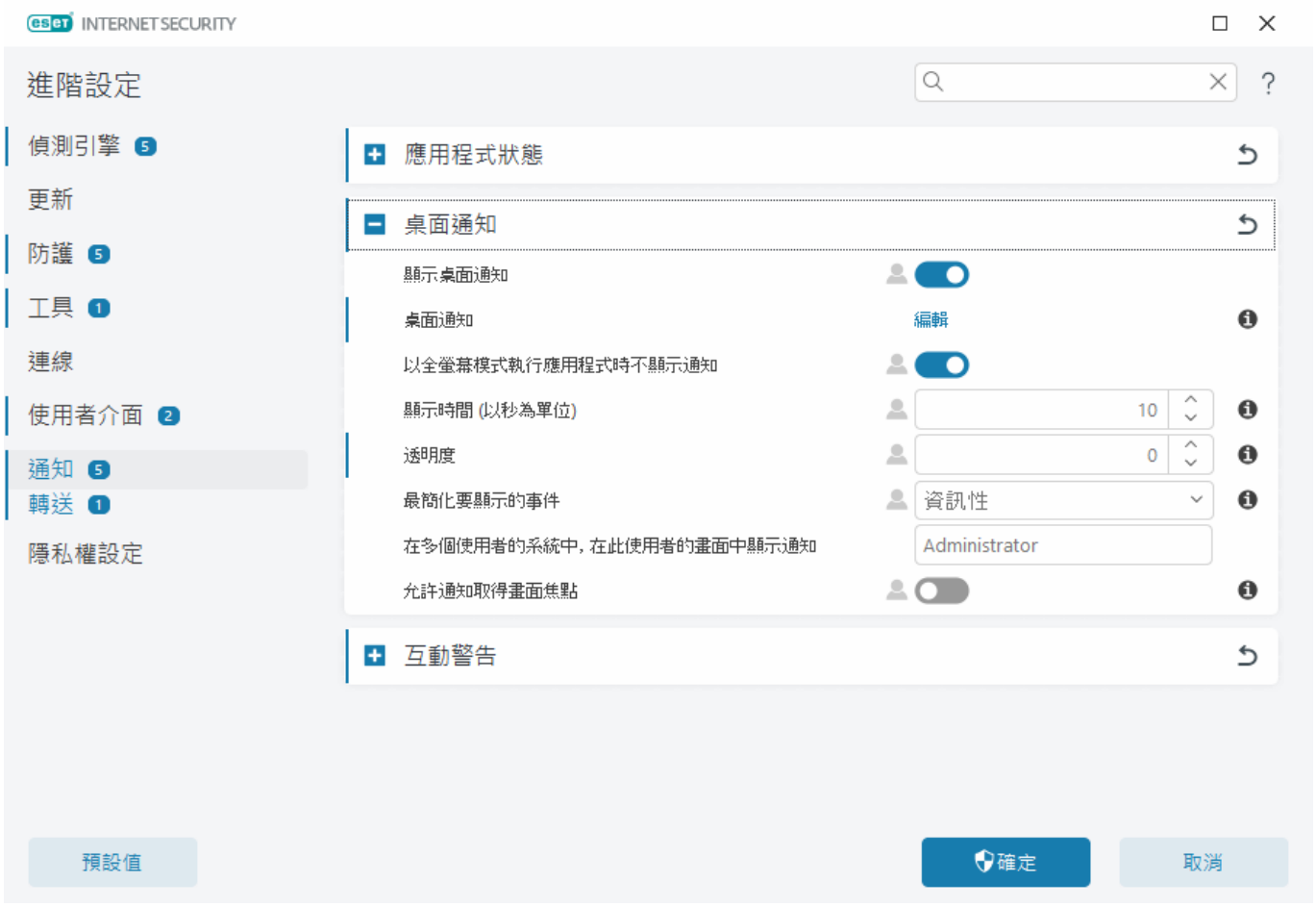
對話方塊視窗 – 應用程式狀態

在這個對話方塊視窗中，您可以選取將顯示哪些應用程式狀態。例如，當您暫停防毒及間諜程式防護或啟用［玩家］模式時。

若您的產品未啟動或訂閱已到期，系統也會顯示應用程式狀態。

桌面通知

桌面通知是由系統工作列旁邊的小型通知視窗表示。依預設，它會顯示 10 秒，而後慢慢消失。通知包括產品更新成功、已連接新裝置、病毒掃描工作完成或找到新威脅。



於桌面顯示通知 - 建議將此選項保持啟用狀態，以便產品在新事件發生時通知您。

[桌面通知] - 按一下 **[編輯]** 以啟用或停用特定桌面通知。

以全螢幕模式執行應用程式時不顯示通知 - 以全螢幕模式執行應用程式時，隱藏所有非互動式通知。

[顯示時間（以秒為單位)] - 設定通知可視度持續時間。該值必須介於 3-30 秒之間。

[透明度] - 設定通知透明度百分比。支援的範圍為 0（沒有透明度）至 80（非常高的透明度)。

[最簡化要顯示的事件] - 設定所顯示的開始通知嚴重性層級。從下拉式功能表中，選取下列其中一個選項：

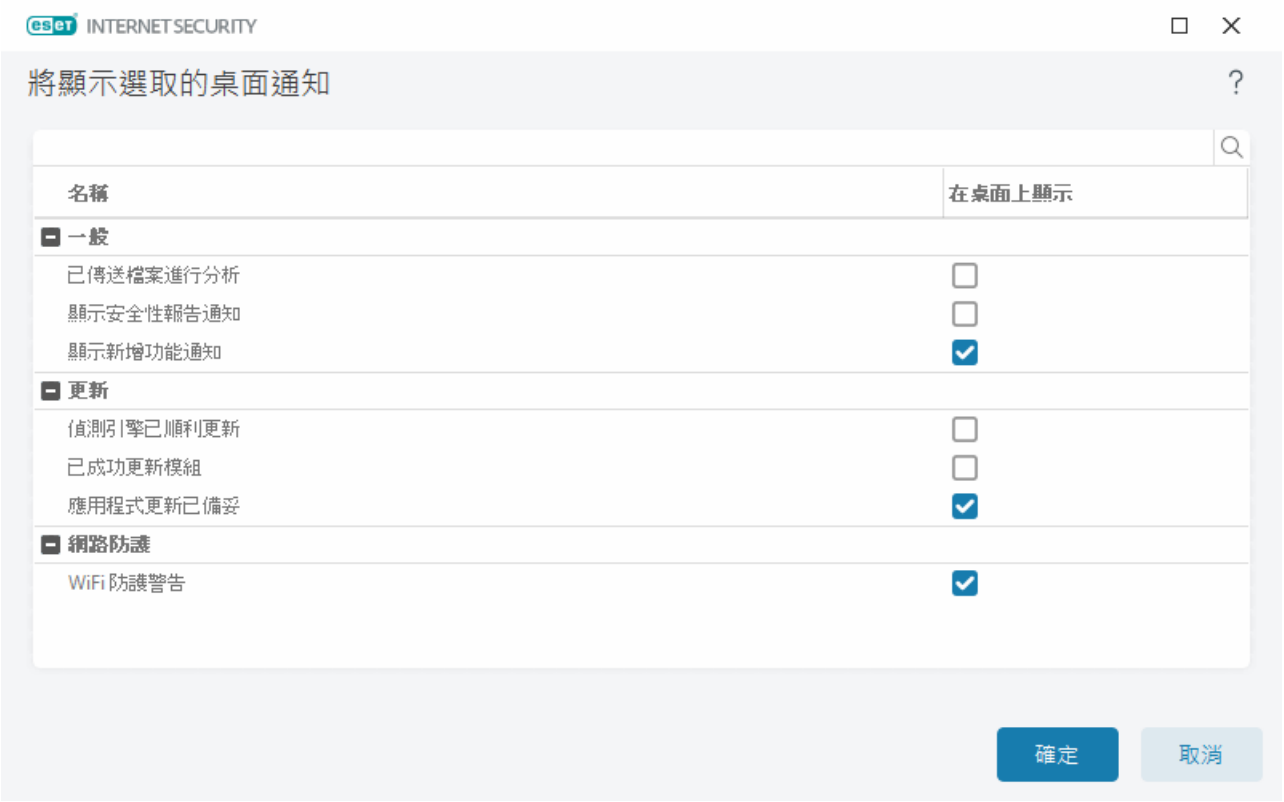
- **[診斷]** - 要微調程式和上述的所有記錄所需的防護記錄資訊。
- **資訊** - 記錄例如非標準網路事件的資訊性訊息，包含成功更新訊息及上述所有記錄。
- **警告**—顯示警告訊息、錯誤和嚴重錯誤（例如，更新失敗)。
- **[錯誤]** - 會顯示錯誤（例如文件防護未啟用）及嚴重錯誤。
- **[嚴重]** - 僅顯示嚴重錯誤（例如啟動病毒防護或受感染的系統等)。

[在多個使用者的系統中，在此使用者的畫面中顯示通知] – 允許選取的帳戶以接收桌面通知。例如，如果您不是使用管理員帳戶，請輸入完整帳戶名稱，系統將顯示指定帳戶的桌面通知。只有一個使用者帳戶才會收到桌面通知。

[允許通知取得畫面焦點] – 允許通知取得畫面焦點，並可在 **ALT + Tab** 功能表中存取。

桌面通知清單

若要調整桌面通知的可視度（顯示於畫面的右下方），請開啟 [進階設定] > **[通知]** > **[桌面通知]**。按一下 **[桌面通知]** 旁的 **[編輯]**，然後選取適當的 **[顯示]** 核取方塊。



一般

顯示安全性報告通知 – 在產生新版安全性報告時接收通知。

顯示新增功能通知 – 關於最新產品版本之所有全新與增強功能的通知。

已傳送檔案進行分析 – 每次 ESET Internet Security 傳送檔案進行分析時接收通知。

網路檢查

針對新發現的網路裝置傳送通知 —當新裝置連接到網路時接收通知。

網路防護

網路設定檔已變更—在網路設定檔發生變更時接收通知。

Wifi 防護警告 – 當您嘗試使用弱式密碼或無密碼連線至 Wi-Fi 網路時，會收到通知。

更新

應用程式更新已備妥 – 當新版本 ESET Internet Security 的更新已備妥時接收通知。

偵測引擎已順利更新 – 在產品更新偵測引擎模組時接收通知。

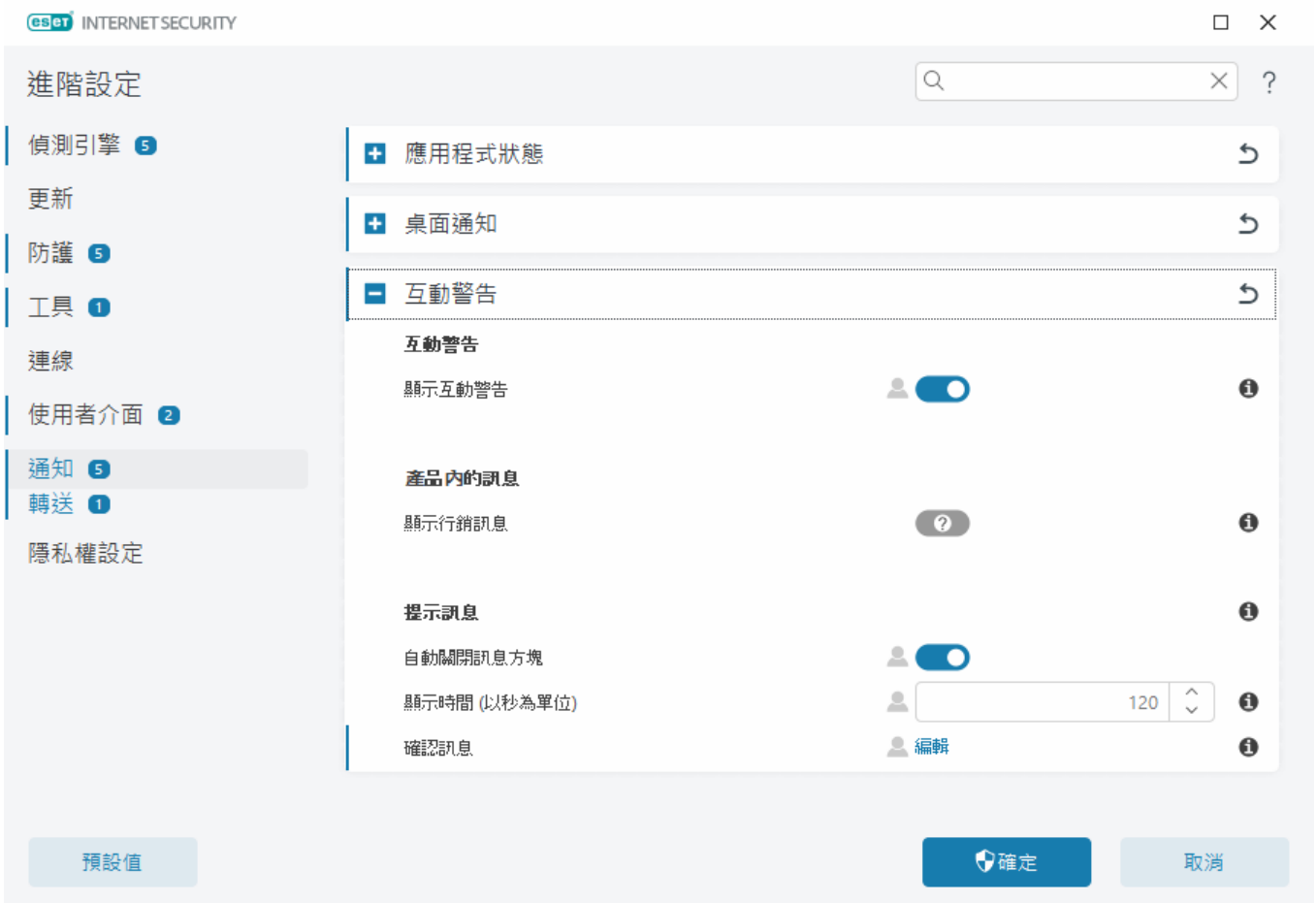
模組已順利更新 – 在產品更新程式元件時接收通知。

若要設定桌面通知的一般設定（例如，訊息顯示的時間長度或最簡化要顯示的事件），請參閱［進階設定］>［**通知**］中的桌面通知。

互動警告

尋找一般的警告及通知相關資訊？
- 發現威脅
- 位址已被封鎖
- 產品未啟動
- 變更為具有多種功能的產品
- 變更為功能較少的產品
- 有新的更新
- 更新資訊不一致
- 「模組更新失敗」訊息的疑難排解
- 解決模組更新錯誤
- 已封鎖網路威脅
- 網站憑證已撤銷

［**進階設定**］>［通知］中的［**互動警示**］區段可讓您配置 ESET Internet Security 如何處理用於偵測的訊息方塊與互動警告，其中需要使用者做出決定（例如，潛在網路釣魚網站）。



互動警告

停用 **[顯示互動警示]** 會隱藏所有警告視窗與瀏覽器內對話方塊，且僅適用於有限的指定情況中。建議您將此選項保持為啟用狀態。

產品內的訊息

產品內訊息的設計是為了通知使用者ESET的最新消息與其他通訊。傳送行銷訊息需取得使用者同意。因此，行銷訊息預設不會傳送給使用者（顯示為問號）。啟用此選項代表您同意收到 ESET 行銷訊息。如果您不想收到 ESET 行銷資料，請停用 **[顯示行銷訊息]** 選項。

訊息方塊

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

[顯示時間（以秒為單位)] – 設定警告可視度持續時間。該值必須介於 10–999 秒之間。

[確認訊息] – 按一下 **[編輯]** 會顯示確認訊息的清單，並可讓您選擇是否要顯示。

確認訊息

若要調整確認訊息，請開啟 [進階設定] > **[通知]** > **[互動警示]**，然後按一下 **[確認訊息]** 旁的 **[編輯]**。

此對話方塊視窗會顯示確認訊息，即 ESET Internet Security 會在執行任何動作之前顯示。選取或取消選取每個確認訊息旁的核取方塊以啟用或停用。

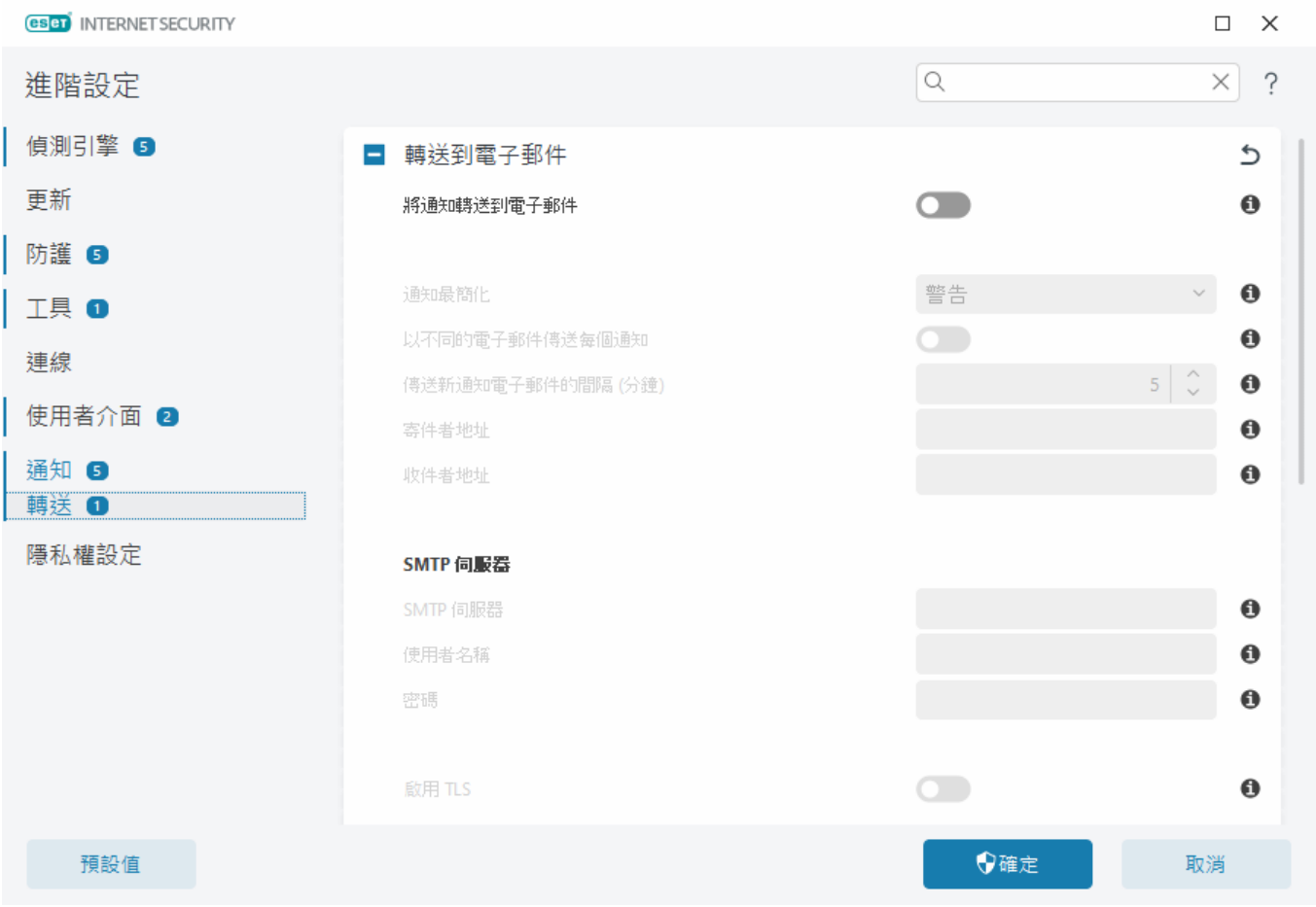
進一步瞭解與確認訊息相關的特定功能：

- 刪除 ESET SysInspector 防護記錄之前先詢問
- 刪除所有 ESET SysInspector 防護記錄前先詢問
- 從隔離區刪除物件前詢問
- 捨棄進階設定中的設定前詢問
- 離開所有發現未從警告視窗中清除的威脅前詢問
- 從防護記錄中移除記錄前詢問
- 移除「排程器」中已排程的工作前詢問
- 移除所有防護記錄前詢問
- 重設統計之前詢問
- 從「隔離區」還原物件前詢問
- 從「隔離區」還原物件並從掃描中排除前詢問
- 執行「排程器」中已排程的工作前詢問
- 顯示垃圾郵件處理結果通知

- 顯示針對電子郵件用戶端的垃圾郵件處理結果通知
- 顯示 Outlook Express 與 Windows Mail 電子郵件用戶端的產品確認對話方塊
- 顯示 Windows Live Mail 的產品確認對話方塊
- 顯示 Outlook 電子郵件用戶端的產品確認對話方塊

轉送

如果發生與所選簡化層級相關的事件，則 ESET Internet Security 可以自動傳送電子郵件通知。開啟［進階設定］>［**通知**］>［**轉寄**］，並啟用［**將通知轉送到電子郵件**］以啟動電子郵件通知。



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

- ［**診斷**］ – 要微調程式和上述的所有記錄所需的防護記錄資訊。
- **資訊** – 記錄例如非標準網路事件的資訊性訊息，包含成功更新訊息及上述所有記錄。
- **警告**—記錄嚴重錯誤及警告訊息（例如，更新失敗）。
- **錯誤** – 會記錄錯誤（例如文件防護未啟用）及嚴重錯誤。
- ［**嚴重**］ – 僅防護記錄嚴重錯誤（例如啟動病毒防護時發生錯誤，或發現威脅）。

［**以不同的電子郵件傳送每個通知**］ – 啟用後，收件者會收到各個通知的新電子郵件。這可能會造成短時間內收到許多的電子郵件。

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

[寄件者地址] - 定義將在通知電子郵件檔頭顯示的寄件者地址。

[收件者地址] - 定義會在通知電子郵件檔頭顯示的收件者地址。支援多個值。使用分號作為分隔符號。

SMTP 伺服器

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

ESET Internet Security 支援具備 TLS 加密的 SMTP 伺服器。

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

啟用 TLS - 使用 TLS 加密保護警告和通知。

測試 SMTP 連線 - 系統會將測試電子郵件傳送到收件者的電子郵件地址。需要填入 SMTP 伺服器、使用者名稱、密碼、寄件者地址和收件者地址。

訊息格式

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 傳訊服務）來完成的。在大部分情況下，對警告訊息與通知 **[使用預設訊息格式]** 是最佳的。在部分情況下，您可能需要變更事件訊息的訊息格式。

事件訊息格式 - 在遠端電腦顯示的事件訊息格式。

[威脅警告訊息格式] - 威脅警告及通知訊息具有預先定義的預設格式。建議您保留預先定義的格式。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。

[字元集] - 根據 Windows 地區設定將電子郵件訊息轉換為 ANSI 字元（例如□windows-1250□Unicode (UTF-8)□ACSII 7-bit 或日文 (ISO-2022-JP))□因此□"á" 將變更為 "a"□而未知符號將變更為 ″?″。

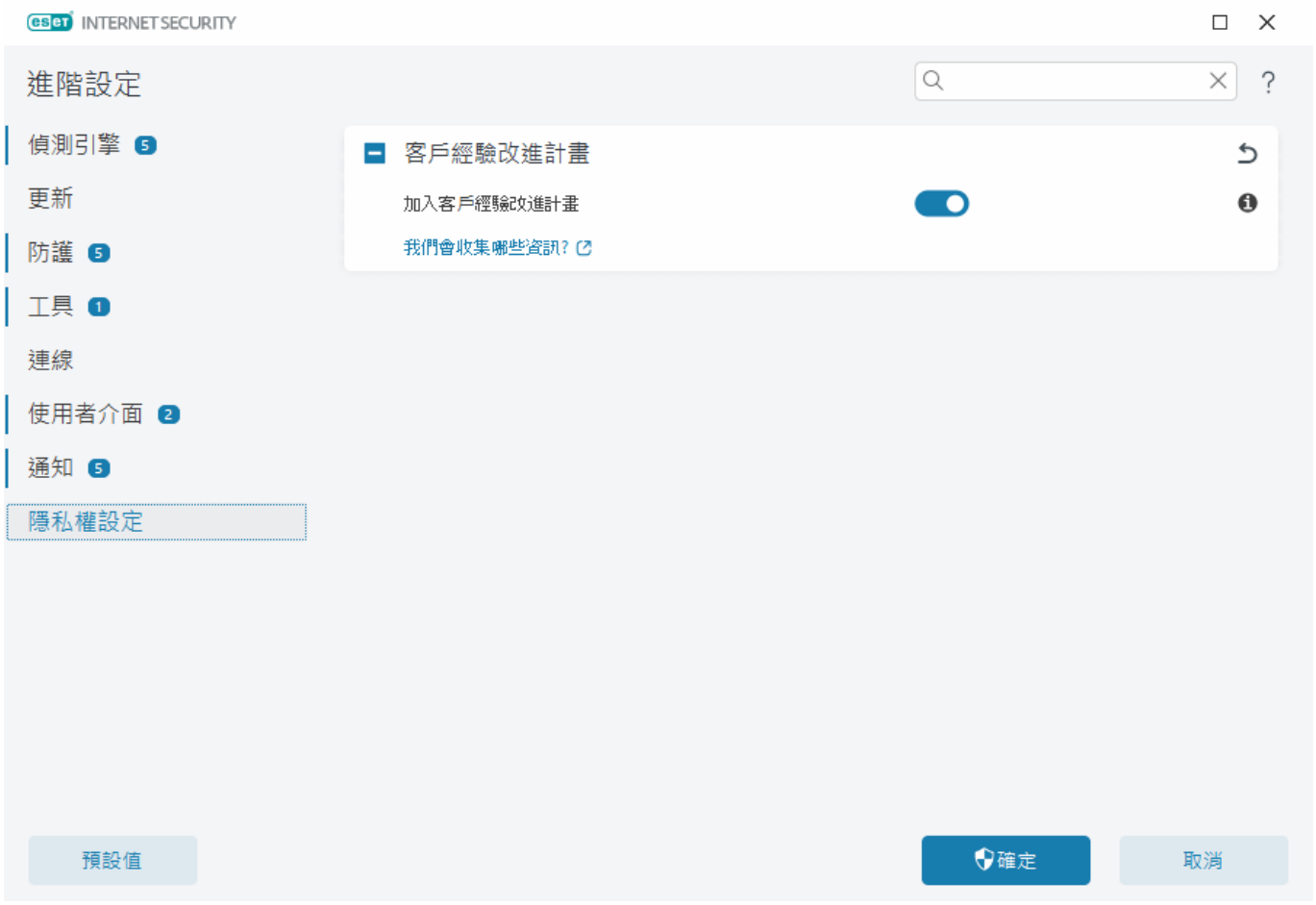
[使用可列印字元引用編碼] - 電子郵件訊息來源會編碼為可列印字元引用 (QP) 格式，此格式會使用 ASCII 字元，並正確透過電子郵件以 8 位元格式 (áéíóú) 傳輸特殊國家字元。

- **%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%** - 受感染檔案、訊息等的名稱。
- **%VirusName%** - 感染的識別碼
- **%Action%** - 對入侵採取行動
- **%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。

隱私權設定

開啟 [進階設定] > **[隱私權設定]**



客戶經驗改進計畫

啟用 **[參與客戶經驗改進計畫]** 旁的滑動軸，以加入「客戶經驗改進計畫」。藉由加入此計畫，您會將與使用 ESET 產品相關的匿名資訊提供給 ESET所收集的資料將協助我們改進您的體驗，且絕不會與第三方共用。我們會收集哪些資訊?

還原為預設值

按一下**進階設定** 中的 [預設值]，來還原所有模組的所有程式設定。這將會重設為在新安裝之後將具有的狀態。

另請參閱匯入及匯出設定

還原目前區段中的所有設定

按一下彎曲箭頭 ，將目前區段中的所有設定還原為 ESET 所定義的預設設定。

請注意，所有完成的任何變更都會在您按一下［**還原為預設**］之後遺失。

還原資料表內容 – 啟用之後，手動或自動新增的規則、工作或設定檔都將遺失。

另請參閱匯入及匯出設定

儲存配置時發生錯誤

此錯誤訊息指出由於發生錯誤，沒有正確地儲存設定。

這通常表示已嘗試修改程式參數的使用者：

- 沒有足夠的存取權限或沒有必要的作業系統權限來修改配置檔和系統登錄。
  › 若要執行所需的修改，系統管理員必須登入。

- 最近已在 HIPS 或防火牆中啟用學習模式，並已嘗試對進階設定進行變更。
  › 若要儲存配置並避免發生配置衝突，請關閉進階設定而不儲存，並嘗試重新進行所需的變更。

第二個常見的原因可能是程式不再正常運作、損毀，因此需要重新安裝。

指令列掃描器

ESET Internet Security 的防毒模組可以透過命令列來啟動，具體方法可以是手動（使用ecls命令）或使用批次 (bat) 檔。

ESET 命令列掃描器使用方式：

```
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=資料夾」	從資料夾 (FOLDER) 載入模組
/quar-dir=資料夾」	隔離資料夾 (FOLDER)
/exclude=遮罩	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=層級」	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=檔案」	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=□檔案大小」	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=□層級」	待掃描壓縮檔（巢狀壓縮檔）內的最大壓縮檔層級
/scan-timeout=□時間限制」	掃描壓縮檔的最多時間限制 (LIMIT□單位（秒）)
/max-arch-size=□檔案大小」	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=□檔案大小」	只掃描在自我解壓檔中小於指定大小 (SIZE□單位 MB) 的檔案（預設值 0 = 無限制）
/mail	掃描電子郵件檔案（預設值）
/no-mail	不掃描電子郵件檔案
/mailbox	掃描信箱（預設值）
/no-mailbox	不掃描信箱
/sfx	掃描自我解壓檔（預設值）
/no-sfx	不掃描自我解壓檔
/rtp	掃描運行時間壓縮器（預設值）
/no-rtp	不掃描運行時間壓縮器
/unsafe	掃描潛在不安全的應用程式
/no-unsafe	不掃描潛在不安全的應用程式（預設值）
/unwanted	掃描潛在不需要應用程式
/no-unwanted	不掃描潛在不需要程式（預設值）
/suspicious	掃描可疑的應用程式（預設值）
/no-suspicious	不掃描可疑的應用程式
/pattern	使用簽章（預設值）
/no-pattern	不使用簽章
/heur	啟用啟發式（預設值）
/no-heur	停用啟發式

/adv-heur	啟用進階啟發式（預設值）
/no-adv-heur	停用進階啟發式
/ext-exclude=⍰副檔名」	從掃描中排除以冒號分隔的檔案副檔名 (EXTENSIONS)
/clean-mode=⍰模式」	針對受感染物件使用清除模式 可用選項如下： • none（預設值） - 將不會進行自動清除。 • standard – ecls.exe 將嘗試自動清除或刪除受感染的檔案。 • 嚴格 – ecls.exe 將嘗試在沒有使用者介入的情況下，自動清除或刪除受感染的檔案（在檔案刪除前，系統不會提醒您）。 • 嚴密 – ecls.exe 無論檔案為何，將會刪除檔案而不嘗試清除。 • 刪除 – ecls.exe 將刪除檔案而不嘗試清除，但會避免刪除敏感的檔案，例如 Windows 系統檔案。
/quarantine	複製受感染檔案（如果已清除）到隔離區 （補充清除時執行的處理方法）
/no-quarantine	不要複製受感染檔案到隔離區

一般選項

/help	顯示說明並結束
/version	顯示版本資料並結束
/preserve-time	保存最後一次的存取時間郵戳

結束代碼

0	找不到威脅
1	找到威脅並已清除
10	無法掃描某些檔案（可能是威脅）
50	找到威脅
100	錯誤

大於 100 的結束代碼表示未掃描檔案，檔案可能已受感染。

常見問題

您可以在下方找到一些使用者最常詢問的問題以及最常遇到的問題。按一下主題標題，以瞭解如何解決您的問題：

- 如何更新 ESET Internet Security
- ESET Internet Security 偵測到了威脅
- 如何從我的 PC 移除病毒
- 如何允許特定應用程式的通訊
- 如何啟用帳戶的家長控制

- 如何在排程器中建立新的工作
- 如何排程掃描工作（每週）
- 如何解除鎖定進階設定
- 如何從 ESET HOME 解決產品停用的問題

如果您的問題不在上述清單中，請嘗試搜尋 [ESET Internet Security 線上說明]。

如果您在 [ESET Internet Security 線上說明] 內找不到問題的解決辦法，可以造訪我們定期更新的線上 ESET 知識庫。以下是最常熱門的知識庫文章連結：

- 如何續約我的訂閱？
- 我在安裝 ESET 產品時收到啟動錯誤訊息。這代表什麼意思？
- 使用啟動金鑰啟動我的 ESET Windows 家用產品
- 解除安裝或重新安裝我的 ESET 家用產品
- 我收到 ESET 安裝已提前結束的訊息
- 在續約訂閱之後我還需要做些什麼？（家用使用者）
- 如果我變更電子郵件地址時該怎麼辦？
- 將我的 ESET 產品傳送到新電腦或裝置
- 如何以安全模式或包含網路功能的安全模式啟動 Windows
- 排除安全網站以免遭到封鎖
- 允許存取 ESET GUI 的螢幕助讀程式軟體

必要的話，您可以連絡我們的技術支援，以解決您的問題。

如何更新 ESET Internet Security

您可以手動也可以自動執行 ESET Internet Security 更新。若要觸發更新，請按一下主程式視窗中的 **[更新]**，然後按一下 **[檢查更新]**。

預設安裝設定會建立每小時執行的自動更新工作。如果需要變更間隔，請瀏覽至 **[工具]** > [排程器]。

如何從我的 PC 移除病毒

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

1. 在主要程式視窗中，按一下 **[電腦掃描]**。
2. 按一下 **[掃描您的電腦]**，開始掃描系統。

3. 完成掃描之後，請檢閱已掃描、受感染及已清除的檔案防護記錄。

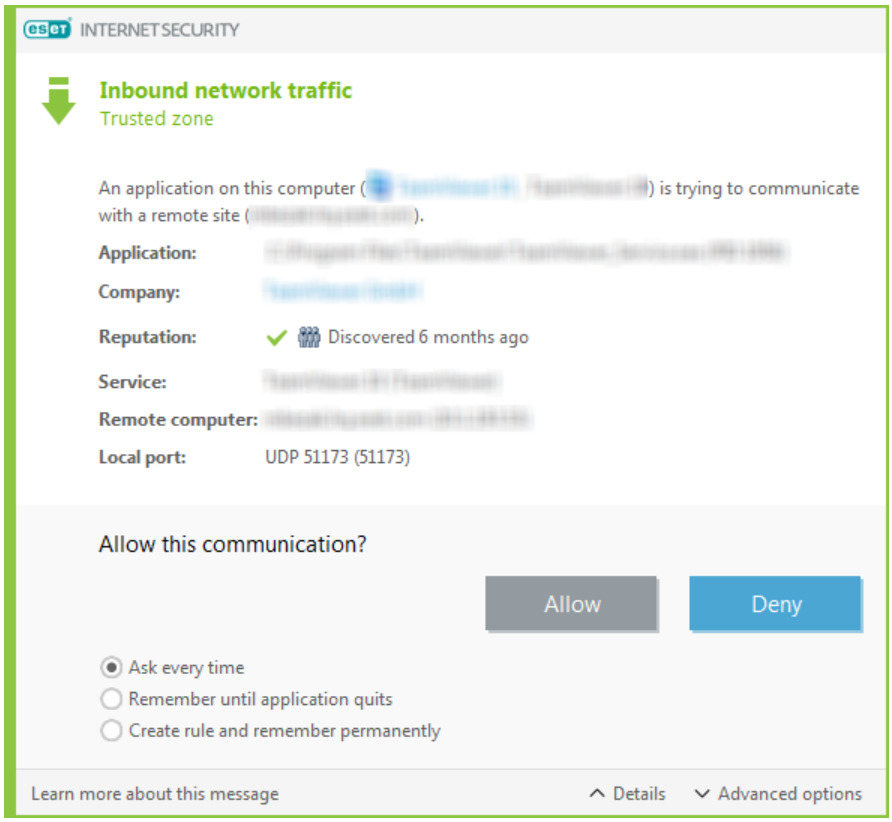
4. 如果您想要掃描僅磁碟選取的部分，請按一下 **[自訂掃描]**，並選取要進行病毒掃描的目標。

針對其他資訊，請參閱：

- ESET 知識庫文章
- 隔離區

如何允許特定應用程式的通訊

如果互動模式中偵測到新連線，且沒有相符規則，則會提示您**允許**或**拒絕**連線。如果您要 ESET Internet Security 在每次應用程式嘗試建立連線時都執行相同的處理方法，請選取 **[建立規則並永久記住規則]** 核取方塊。



在防火牆設定中，您可以在應用程式由 ESET Internet Security 偵測到之前為其建立新的防火牆規則。開啟主要程式視窗 > **[設定]** > **[網路防護]** > 按一下 **[防火牆]** 旁的 > **[配置]** > **[進階]** > **[規則]** > **[編輯]**。

按一下 **[新增]** 按鈕，在 **[一般]** 索引標籤中輸入規則的名稱、方向及通訊協定。視窗可讓您定義規則適用時要採取的處理方法。

在 **[本機]** 索引標籤中輸入應用程式可執行檔的路徑及本機通訊連接埠。按一下 **[遠端]** 索引標籤，以輸入遠端位置及連接埠（如果適用的話）。一旦應用程式再次嘗試通訊，就會套用新建立的規則。

如何啟用帳戶的家長控制

若要啟動特定使用者帳戶的家長控制，請遵循以下步驟：

1. 依預設ESET Internet Security 中的家長控制為停用。有兩種方式可以啟用家長控制：

• 從主要程式視窗中，按一下 **[設定] > [網際網路防護] > [家長控制]** 中的切換開關圖示，並將家長控制狀態變更為已啟用。

• 開啟 [進階設定] > **[防護] > [Web 存取防護] > [家長控制]**，然後啟用 **[啟用家長控制]** 旁邊的切換開關。

2. 按一下主要程式視窗中的 **[設定] > [網際網路防護] > [家長控制]**。即使 **[啟用]** 已顯示於 **[家長控制]** 旁，您仍需按一下箭頭符號，然後在下一個視窗中選取 **[保護兒童帳戶]** 或 **[家長帳戶]**，為所需的帳戶配置家長控制。在下一個視窗中選取出生日以決定存取層級與適合年齡的建議網頁。現在將為指定的使用者帳戶啟用家長控制。按一下帳戶名稱下的 **[封鎖的內容和設定]**，即可在類別索引標籤中自訂您要允許或封鎖的類別。若要允許或封鎖不符合類別的自訂網頁，請按一下例外索引標籤。

如何在排程器中建立新的工作

若要在 **[工具] > [排程器]** 中建立新工作，請按一下 **[新增工作]**，或按一下滑鼠右鍵並從內容功能表中選取 **[新增]**。有五種類型的排程工作可用：

• **執行外部應用程式** - 排程以執行外部應用程式。

• **[防護記錄維護]** - 防護記錄檔案還包括已刪除記錄的剩餘部分。此工作會定期最佳化防護記錄檔案中的記錄，以有效運作。

• **系統啟動檔案檢查** - 檢查系統啟動或登入時允許執行的檔案。

• **建立電腦狀態快照** - 建立 ESET SysInspector 電腦快照 - 收集關於系統元件（例如驅動程式、應用程式）的詳細資訊，並評估各個元件的風險層級。

- **指定電腦掃描** - 針對電腦中的檔案及資料夾執行掃描。
- **[更新]** - 更新模組來排程更新工作。

由於 **[更新]** 是其中一個最常用的排程工作，因此我們將在下面解釋如何新增更新工作：

從 **[已排程的工作]** 下拉式功能表中，選取 **[更新]**。在 **[工作名稱]** 欄位中輸入工作的名稱，接著按一下 **[下一步]**。選取工作的頻率。可用選項如下：**[一次]**、**[重複]**、**[每日]**、**[每星期]** 與 **[事件觸發]**。選取 **[使用電池執行時略過工作]** 以在膝上型電腦使用電池執行時，將系統資源消耗降到最低。工作會在 **[工作執行]** 欄位中的指定日期和時間執行。接著，定義排程期間無法執行或完成工作時要採取的處理方法。可用選項如下：

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

在下一步中，會顯示目前已排程工作資訊的摘要視窗。完成變更之後，按一下 **[完成]**。

隨即顯示對話方塊視窗，可讓您選取用於排程工作的設定檔。在這裡，您可以設定主要設定檔及替代設定檔。如果使用主要設定檔無法完成工作時將會使用替代設定檔。按一下 **[完成]** 進行確認，即可將排程工作新增至目前排程工作清單。

如何安排每週電腦掃描

若要排程定期工作，請開啟主要程式視窗並按一下 **[工具] > [排程器]**。以下是關於如何排程工作的簡短指南，而此工作將會每週掃描一次本機磁碟機。如需詳細指示，請參閱我們的知識庫文章。

若要排程掃描工作：

1. 在主要的 [排程器] 畫面中按一下 **[新增]**。
2. 輸入工作的名稱並從 **[工作類型]** 下拉式功能表選取 **[指定電腦掃描]**。
3. 選取 **[每星期]** 作為工作頻率。
4. 設定執行工作的日期及時間。
5. 若已安排的工作因故無法執行（例如電腦已關機），請選取 **[盡快執行工作]** 以稍後執行工作。
6. 檢閱已排程工作的摘要，並按一下 **[完成]**。
7. 從 **[目標]** 下拉式功能表中，選取 **[本機磁碟]**。
8. 按一下 **[完成]** 以套用工作。

如何解除鎖定密碼保護的進階設定

當您想要存取受保護的進階設定時，會顯示可供輸入密碼的視窗。如果您忘記或遺失密碼，請按一下 **[還原密碼]**，然後輸入您用於訂閱註冊的電子郵件地址。ESET 會將內含驗證碼的電子郵件傳送給您。請輸入驗證碼，然後寫入並確認新密碼。驗證碼在七天內有效。

[透過您的 ESET HOME 帳戶還原密碼] – 如果用於啟動的訂閱與您的 ESET HOME 帳戶相關聯，請使用此選項。輸入您用於登入 ESET HOME 帳戶的電子郵件地址。

如果您不記得您的電子郵件地址或還原密碼有困難，請按一下 **[連絡技術支援]**。系統便會將您重新導向至 ESET 網站，讓您可以與我們的技術支援部門取得聯絡。

[產生技術支援代碼] – 此選項將產生技術支援的代碼。請複製技術支援提供的代碼，然後按一下 **[我擁有驗證碼]**。輸入驗證碼，然後寫入並確認新密碼。驗證碼在七天內有效。

如需更多資訊，請參閱在 ESET Windows 家用產品中將設定密碼解除鎖定

如何從 ESET HOME 解決產品停用的問題

產品未啟動

當訂閱擁有者從 ESET HOME 入口網站停用您的 ESET Internet Security或與您的 ESET HOME 帳戶共用的訂閱不再共用時，會顯示此錯誤訊息。若要解決此問題：

- 按一下 **[啟動]**，然後使用其中一種啟動方法啟動 ESET Internet Security
- 連絡訂閱擁有者，並表示您的 ESET Internet Security 已由訂閱擁有者停用，或訂閱已不再與您共用。擁有者可以在 ESET HOME 解決問題。

產品已停用，裝置已中斷連線

將裝置從 ESET HOME 管理入口網站移除之後，會顯示此錯誤訊息。若要解決此問題：

- 按一下 **[啟動]**，然後使用其中一種啟動方法啟動 ESET Internet Security
- 連絡訂閱擁有者，並提供您的 ESET Internet Security 已停用且該裝置已與 ESET HOME 中斷連線的相關資訊。
- 如果您是訂閱擁有者且未注意到這些變更，請檢閱您的 ESET HOME 活動摘要。如果您發現任何可疑活動，請變更您的 ESET HOME 帳戶密碼，並連絡 ESET 技術支援

產品已停用，裝置已中斷連線

將裝置從 ESET HOME 管理入口網站移除之後，會顯示此錯誤訊息。若要解決此問題：

- 按一下 **[啟動]**，然後使用其中一種啟動方法啟動 ESET Internet Security
- 連絡訂閱擁有者，並提供您的 ESET Internet Security 已停用且該裝置已與 ESET HOME 中斷連線的相關資訊。
- 如果您是訂閱擁有者且未注意到這些變更，請檢閱您的 ESET HOME 活動摘要。如果您發現任何可疑活動，請變更您的 ESET HOME 帳戶密碼，並連絡 ESET 技術支援

產品未啟動

當訂閱擁有者從 ESET HOME 入口網站停用您的 ESET Internet Security或與您的 ESET HOME 帳戶共用的訂閱不再共用時，會顯示此錯誤訊息。若要解決此問題：

- 按一下 **[啟動]**，然後使用其中一種啟動方法啟動 ESET Internet Security
- 連絡訂閱擁有者，並表示您的 ESET Internet Security 已由訂閱擁有者停用，或訂閱已不再與您共用。擁有者可以在 ESET HOME 解決問題。

0

客戶經驗改進計畫

藉由參加「客戶經驗改進計畫」，您使用 ESET 產品的相關資訊就會匿名提供給我們。我們的隱私權政策提供資料處理的詳細資訊。

您的同意

參與此計畫是自願性質且基於您的同意。您在加入計畫後是被動參與，亦即您不需要採取進一步行動。您隨時可以變更產品設定來撤銷同意，如此會阻止我們進一步處理您的匿名資料。

您隨時可以變更產品設定來撤銷同意：

- 變更 ESET Windows 家用產品中的客戶經驗改進計畫設定

我們會收集哪些類型的資訊？

產品互動相關資料

此資訊讓我們瞭解產品的使用情況。例如，我們能藉此瞭解客戶經常使用的功能、使用者會修改的設定，或使用者使用產品所花費的時間。

裝置相關資料

我們收集此資訊，以便瞭解我們的產品使用在何處以及何種裝置上。典型的範例為裝置型號、國家、版本和作業系統名稱。

錯誤診斷資料

我們也會收集有關錯誤和毀損狀況的資訊。例如，發生了什麼錯誤，以及會造成錯誤的動作是什麼。

為什麼我們要收集此資訊？

此匿名資料讓我們能為您（我們的使用者）改善產品。這有助我們讓產品盡可能變得最相關、容易使用且完美無缺。

誰控制此資訊？

對於計畫中收集的資料ESET, spol. s r.o. 是唯一的控制者。此資訊不會與第三方共用。

使用者授權合約

自 2021 年 10 月 19 日 起生效。

重要:下載、安裝、複製或使用之前，請先詳讀產品應用程式的下列條款與條件。**下載、安裝、複製或使用本軟體，即表示貴用戶同意本授權合約的條款與條件，並瞭解**隱私權政策

使用者授權合約

本使用者授權合約（「本合約」）由 ESET, spol. s r. o. (設址於 Einsteinova 24, 85101 Bratislava, Slovak Republic註冊於 Bratislava 第一地方法院 (Section Sro, Entry No 3586/B) 所管轄的商業登記處，公司登記號碼 31333532) (ESET或「提供者」）與貴用戶、個人或法人（「貴用戶」或「使用者」）雙方約定執行，貴用戶有權使用「本合約」中第 1 條所定義的「軟體」。本「合約」中第 1 條所定義的「軟體」可儲存於資料傳送體、透過電子郵件傳送、從網際網路下載、從「提供者」伺服器下載，或從以下條款與條件中所指定的其他來源取得。

「提供者」持續擁有本「軟體」副本、商業套件中的實體媒體，以及根據本「合約」中授權「使用者」產生的任何其他副本。「提供者」持續擁有本「軟體」副本、商業套件中的實體媒體，以及根據本「合約」中授權「使用者」產生的任何其他副本。

安裝、下載、複製或使用本「軟體」期間按一下［我接受］或［我接受…］選項，即表示貴用戶同意本「合約」的條款與條件並認可「隱私權政策」。若貴用戶不同意本「合約」和/或「隱私權政策」的條款與條件，請立即按一下［取消］選項，取消安裝或取消下載，或銷毀本「軟體」，或者將本「軟體」、安裝媒體、隨附之文件及購買發票退還給「提供者」或貴用戶購買本「軟體」之經銷商。

貴用戶同意使用本「軟體」即表示貴用戶已閱讀本「合約」、理解「合約」內容，並受「合約」條款與條件的約束。

1.**軟體。**本「合約」中的「軟體」一詞係指(i) 本「合約」所隨附之電腦程式及其包含的所有元件 (ii) 在磁碟CD-ROMDVD電子郵件及所有附件，或其他隨附本「合約」之媒體中的所有內容，包括以資料傳送體提供、透過電子郵件傳送或透過網際網路下載的本「軟體」物件碼; (iii) 任何相關書面說明資料以及與本「軟體」相關的任何其他可能文件，尤其是本「軟體」任何說明、其規格、本「軟體」屬性或作業的任何說明、使用本「軟體」之作業環境的任何說明、本「軟體」的使用安裝指示，或如何使用軟體的任何說明（「文件); (iv) 由「提供者」根據本「合約」第 3 條授權給「貴用戶」的本「軟體」複本、「軟體」可能錯誤的修補程式、「軟體」新增、「軟體」擴充功能、「軟體」修改後的版本和「軟體」元件的更新（若有）。本「軟體」得完全以可執行目的碼形式提供。本「軟體」僅以可執行物件碼形式提供。

2.**安裝、電腦與授權金鑰。**本「軟體」無論是由資料傳送體提供、透過電子郵件傳送、從網際網路下載、從「提供者」伺服器下載，或從其他來源取得，皆需要安裝。安裝方法如「文件」中所述。 安裝本「軟體」的電腦上，不得安裝任何對本「軟體」有不利影響的電腦程式或硬體。「電腦」係指用於安裝和/或使用本「軟體」的硬體，包括但不限於個人電腦、筆記型電腦、工作站、掌上型電腦、智慧型手機、手持電子裝置或其他電子裝置。安裝本「軟體」的電腦上，不得安裝任何對本「軟體」有不利影響的電腦程式或硬體。「電腦」係指用於安裝和/或使用本「軟體」的硬體，包括但不限於個人電腦、筆記型電腦、工作站、掌上型電腦、智慧型手機、手持電子裝置或其他電子裝置。「授權金鑰」係指提供給使用者的唯一序列，包括符號、字母、號碼或特殊標識的序列，讓使用者可以合法使用本「軟體」，其特定版本或授權期限延續符合本「合約」。

3.**授權**。若貴用戶同意本「合約」條款、在期限內繳付「授權費」，並遵循所有規定的條款與條件，則「提供者」會授與貴用戶以下權限（以下稱「授權」）:

a) **安裝與使用。**貴用戶擁有非專屬、不可轉讓之權限，可將本「軟體」安裝於電腦硬碟或其他儲存資料的永久媒體上、將本「軟體」安裝並儲存於電腦系統的記憶體上，以及實作、儲存及顯示本「軟體」。

b) **授權數目規定。**本「軟體」的使用權限受「使用者」數目的限制。「一位使用者」係指 (i) 本「軟體」

於一個電腦系統上的安裝；或 (ii) 若授權的範圍受信箱數目的限制，則「一位使用者」係指透過 Mail User Agent (MUA) 接收電子郵件的電腦使用者。若 MUA 接受電子郵件並於稍後將郵件自動散佈給多位使用者，則「使用者」數目即根據接收所散佈之電子郵件的實際使用者數目而定。若郵件伺服器執行郵件閘道功能，則「使用者」數目應等於由該閘道提供服務之郵件伺服器使用者數目。若將任何數量之電子郵件地址引導至一位使用者（例如透過別名），且該使用者接受這些地址，而且用戶端未自動將郵件散佈給大量的使用者，則需要一台電腦的「授權」。貴用戶不得同時在多台電腦上使用同一個「授權」。使用者僅在根據「提供者」授予的授權數目造成的限制下，使用者有權使用本「軟體」時，才有權利輸入授權金鑰。授權金鑰視為機密，貴用戶不得與第三方分享或允許第三方使用授權金鑰，除非獲得本「合約」或「提供者」許可。如果貴用戶的授權金鑰遭盜用，請立即通知「提供者」。

c) **家用/企業版。**本「軟體」的家用版應僅供私人專用和/或家庭與家人於非商業環境中使用。若要在郵件伺服器、郵件中繼站、郵件閘道或網際網路閘道上使用本「軟體」，則必須取得本「軟體」的企業版才能用於商業環境。

d) **授權期限。**本「軟體」的使用權限有時間限制。

e) **OEM 軟體。**分類為□OEM□的「軟體」應受限於貴用戶用來取得該軟體的電腦□□OEM 軟體」無法傳輸到其他電腦。

f) **NFR□TRIAL 軟體。**歸類為「禁止轉售□(NFR) 或試用 (TRIAL) 的軟體不得付費轉讓，且必須僅供示範或測試本「軟體」功能之用。

g) **終止授權。**授權期結束時，本「授權」會自動終止。如果貴用戶無法遵循本「合約」中的任何規定，「提供者」有權利在不危害「提供者」任何權利或法律救濟的情況下撤銷本「合約」。本「授權」取消時，貴用戶必須立即將本「軟體」及其所有備份刪除、銷毀，或自費退回給ESET或您購買本「軟體」之經銷商。「使用者」須連線至「提供者」之伺服器或第三方伺服器，方能行使對軟體功能之使用權；授權終止時，「提供者」有權取消該使用權。

4.**資料收集功能和網際網路連線需求。**依據隱私權政策，本「軟體」必須連線到網際網路，且必須定期連線到「提供者」伺服器或第三方伺服器以及適用的資料收集，才能正確作業。本「軟體」的以下功能需要連線到網際網路以及適用的資料收集：

a) **更新「軟體」。**「提供者」有不時發行本「軟體」的更新或升級（以下稱「更新」）之權利，但無提供「更新」之義務。除非「使用者」停用自動安裝「更新」功能，否則在本「軟體」的標準設定下，會啟用這項功能而自動安裝「更新」。為了佈建更新，需要驗證「授權」，包括安裝本「軟體」的電腦和/或平台相關資訊，以符合隱私權政策。

任何更新的條款都可能需要遵守生命週期結束政策（以下稱□EOL 政策」），該政策在 https://go.eset.com/eol_home 上提供。在本「軟體」或任何其功能達到 EOL 政策中定義的生命週期結束日期後，即不再提供任何更新。

b) **將入侵及資訊轉遞給「提供者」。**本「軟體」包含會收集電腦病毒與其他惡意電腦程式及可疑、問題、潛在不需要或潛在不安全的物件，例如檔案□URL□IP 封包及乙太網路框架（「入侵」）範例的功能，然後將這些範例傳送給「提供者」，包括但不限於有關安裝程序、軟體安裝所在「電腦」和/或平台的資訊，以及有關本「軟體」運作和功能的資訊（「資訊」）。「資訊」和「入侵」可能包含有關使用者或本「軟體」安裝所在之電腦使用者的資料，包括隨機或或意外取得的個人資料 ，以及因相關聯中繼資料入侵而受影響的檔案。

「資訊」與「入侵」可由下列「軟體」功能收集：

i.LiveGrid 聲譽系統功能包括收集和傳送「入侵」相關的單向雜湊給「提供者」。此功能將在本「軟體」標準設定下啟用。

ii.LiveGrid 意見系統功能包括收集和傳送「入侵」連同關聯的中繼資料，以及「資訊」給「提供者」。此功能可由「使用者」在安裝本「軟體」期間啟動。

「提供者」僅應將收到的「資訊」與「入侵」供分析研究「入侵」、改進「軟體」與驗證「授權」真確性之用，並採取適當的措施確保「入侵」及「資訊」保持機密。貴用戶啟用本「軟體」的這項功能，表示貴用戶准許「提供者」依照隱私權政策與相關法律規定收集和處理「入侵」與「資訊」。貴用戶可隨時停用此功能。

針對本「合約」之目的，有必要收集、處理和儲存資料，使「提供者」能夠根據隱私權政策識別您的身份。貴用戶瞭解，「提供者」會使用自己的方式檢查您是否按照本協議的規定使用本「軟體」。貴用戶瞭解，針對本「合約」之目的，您的資料必須在本「軟體」與「提供者」或其商業夥伴（作為「提供者」經銷和支援網路一部分）的電腦系統之間進行通訊時傳送，以確保本「軟體」功能和使用本「軟體」的授權，以保護「提供者」的權利。

依據本「合約」結論，「提供者」或其任何作為「提供者」經銷和支援網路一部分的商業夥伴，有權利傳輸、處理與儲存可識別貴用戶的必要資料，以供計費、實行本「合約」之用，並在電腦上傳輸通知。

有關隱私權、個人資料保護和貴用戶身為資料當事人權限的詳細資料，可以在「提供者」網站上的隱私權政策中找到，並可以直接在安裝過程中取得。貴用戶也可以造訪本「軟體」的「說明」區段。

5.**行使「使用者」權利**。貴用戶必須由本人或員工行使「使用者」權利。貴用戶僅有權使用本「軟體」來保護電腦作業以及取得「授權」的電腦或電腦系統。

6.**限制權利。**貴用戶不得將本「軟體」複製、散佈、提取其元件或建立其衍生版本。使用本「軟體」時，您必須遵循下列限制：

a) 貴用戶可將本「軟體」的副本儲存於永久資料媒體上做為封存備份副本，但貴用戶的封存備份副本不得在任何電腦上安裝或使用。建立本「軟體」的任何其他副本皆違反本「合約」。

b) 貴用戶不得以非本「合約」提供之方式使用、修改、翻譯或重製本「軟體」，或轉讓本「軟體」或其副本的使用權。

c) 貴用戶不得出售、轉授權、出租或借用本「軟體」，或使用本「軟體」提供商業服務。

d) 貴用戶不得對本「軟體」進行反向工程、反向組譯或解譯，或嘗試取得本「軟體」的來源程式碼，除非相關法律明文禁止上述限制。

e) 貴用戶同意僅以符合本「軟體」使用管轄區中適用法律之方式使用本「軟體」，包括但不限於與著作權法及其他智慧財產權相關的適用限制。

f) 貴用戶同意僅以不限制其他「使用者」存取這些功能的方式使用本「軟體」和其功能。「提供者」保留限制為個別「使用者」提供服務之範圍的權利，以盡可能讓最多「使用者」可以使用服務。限制服務範圍亦表示完全終止使用任何本「軟體」的功能，並刪除任何與本「軟體」特定功能相關的「提供者」伺服器或第三方伺服器上之「資料」和資訊。

g) 貴用戶同意，若任何活動牽涉到使用授權金鑰、違反本「合約」條款或者致使授權金鑰提供給任何不具使用本「軟體」權利的人員，例如以任何形式轉移授權金鑰，以及未經授權而擅自複製或散佈重複或產生的授權金鑰，或是從其他非「提供者」處獲得授權金鑰來使用本「軟體」，貴用戶將不會進行該活動。

7.**版權**。本「軟體」及其所有權利（包括但不限於專利權及智慧財產權）皆為 ESET 和/或其授權提供者所有，並受國際條約之條款及「軟體」使用所在國家所有適用法律之保護。本「軟體」之結構、組織及程式碼是 ESET 及/或其授權者的重要商業秘密及機密資訊。貴用戶不得複製本「軟體」，唯第 6 (a) 條中指定之例外情況除外。任何依據本「合約」允許貴用戶產生之副本，必須包含與本「軟體」相同的著作權或其他所有權聲明。若貴用戶違反本「合約」條款，對本「軟體」進行反向工程、反向組譯、解譯，或嘗試發現本「軟體」的來源程式碼，則貴用戶同意從這類資訊產生的時刻起，所取得的任何資訊會自動傳送至「提供者」並由其完全擁有，無法撤回，儘管「提供者」的權利違反本「合約」。

8.**保留權利**。「提供者」保留本「軟體」的所有權利，唯本「合約」明確授予貴用戶身為本「軟體」之「使用者」的權利除外。

9.**數種語言版本、雙媒體軟體、多個副本**。若本「軟體」支援數個平台或語言，或貴用戶取得本「軟體」多個副本，則只有貴用戶所取得「授權」數目的電腦系統與版本能使用本「軟體」。貴用戶不得銷售、出租、轉授權、出借或移轉貴用戶未使用本「軟體」之任何版本或副本。

10.**「合約」開始與終止。**本「合約」於貴用戶同意本「合約」條款之日起開始生效。貴用戶永久解除安裝、銷毀並自費退回本「軟體」、所有備份副本，以及「提供者」或其商業夥伴所提供任何相關資料，即為終止本「合約」。貴用戶對於使用本「軟體」及其任何功能的權利受到 EOL 政策所規範。在本「軟體」或任何其功能達到 EOL 政策中定義的生命週期結束日期後，貴用戶對於本「軟體」的使用權利將會終止。無論終止本「合約」的方式為何，第 7、8、11、13、19 與 21 條條款規定仍繼續適用，適用時間無限。

11.**使用者聲明**。貴用戶身為「使用者」，瞭解本「軟體」係依「現狀」提供，在相關法律所允許之最大範圍內無任何類型的擔保，無論明示或默示。「提供者」、其授權提供者、分公司或版權擁有者皆不提供任何明示或默示聲明或保證，包括但不限於適售性或特定用途之適用性，亦不保證本「軟體」不侵害第三方之專利、版權、商標或其他權利。「提供者」及任何其他人不保證本「軟體」功能符合貴用戶之需求，亦不保證本「軟體」作業不會中斷或無錯誤。對於選擇使用本「軟體」是否獲得預期結果，以及對「軟體」的安裝、使用與結果，皆由貴用戶承擔所有責任與風險。

12.**無其他義務**。除本「合約」特別列出的義務之外，本「合約」對「提供者」及其授權提供者無任何其他義務要求。

13.**責任限制**。在相關法律所允許之最大範圍內，在任何情況下，對於因安裝、使用或無法使用本「軟體」所導致的收入利潤損失、銷售額損失、資料遺失、採購備用商品或服務之額外費用、財產損失、人身傷害、業務中止、商業資訊遺失，或任何特殊、直接、間接、意外、經濟、遮掩、犯罪、特殊或衍生之損害，無論其導致方式為何以及是否因合約、過失、疏忽或其他責任理論所引起，「提供者」、其員工或授權提供者概不負責，即使已告知「提供者」、其授權提供者或分公司可能會發生此類損失。因為部分國家或管轄區不允許免除責任，但允許限制責任，所以「提供者」、其員工、授權提供者或分公司受限於貴用戶已付「授權」費用之總額。

14. 本「合約」的任何條款若與任何一方身為消費者的合法權利相反，皆不損害該合法權利。

15.**技術支援**：ESET 或 ESET 委託的第三方會酌情提供技術支援，不提供任何保證或聲明。在本「軟體」或任何其功能達到EOL政策中定義的生命週期結束日期後，即不再提供任何技術支援。提供技術支援前，需要「使用者」先備份所有現有資料、軟體與程式設備。對於因提供技術支援所導致任何資料、財產、軟體或硬體的損壞或遺失，或利潤的損失，ESET 及/或 ESET 委任的第三方概不負責。ESET 及/或 ESET 委任的第三方保留決定解決問題是否超過技術支援範圍的權利。ESET 保留酌情拒絕、暫停或終止提供技術支援的權利。依照隱私權政策，可能需要授權資訊、「資訊」和其他資料，以便用於技術支援佈建。

16.**授權轉讓**。本「軟體」可在電腦系統間傳輸，除非違反本「合約」條款。本「軟體」可在電腦系統間傳輸，除非違反本「合約」條款。如果未違反本「合約」條款，「使用者」是唯一具有權利的實體可在「提供者」同意下，將因本「合約」產生的「授權」與所有權利永久轉讓給另一位「使用者」，但轉讓條件為：(i) 原始「使用者」未保留本「軟體」的任何副本；(ii) 權利的轉讓必須是直接，亦即從原始「使用者」轉讓給新「使用者」；(iii) 新「使用者」必須承擔原始「使用者」依本「合約」條款所承擔的所有權利與義務；(iv) 依照第 17 條規定，原始「使用者」必須提供給新「使用者」可驗證本「軟體」真實性的文件。

17.**驗證軟體真實性。**「使用者」可使用下列其中一種方式證明使用本「軟體」的資格：(i)透過「提供者」或「提供者」所委任第三方核發的授權憑證；(ii) 透過書面授權合約（若已訂立此類合約)；(iii) 透過提交「提供者」傳送的電子郵件，其中包含授權詳細資料（使用者名稱與密碼)。依照隱私權政策，可能需要授權資訊和使用者識別資料，以便用於本「軟體」真實性驗證。

18.**美國公家機關與政府單位的授權**。根據本「合約」所述的授權權利與限制，本「軟體」可提供給公家機關，包括美國政府

19.**貿易管制法規遵循**：

a)您將不得直接或間接以出口、再出口、移轉或其他方式將本軟體提供給任何人，或以任何方式進行使用，

或涉及任何可能導致 ESET 或其所有公司、其附屬機構、任何其所有公司的附屬機構，以及其所有公司所掌控之實體（「附屬機構」）違反以下貿易管制法律，或受到不利益結果的行為；這些法律包含

i. 由任何政府、美國各州或主管機關、新加坡、英國、歐盟或任何其會員國，或必須履行本協議中義務之任何國家/地區，或 ESET 或任何其附屬機構所組成或營運所在區域針對出口、再出口、移轉商品、軟體、技術或服務所發佈或採用予以管制、限制或強制授權要求的任何法律；以及

ii. 由任何政府、美國各州或主管機關、新加坡、英國、歐盟或任何其會員國，或必須履行本協議中義務之任何國家/地區，或 ESET 或任何其附屬機構所組成或營運所在區域強制實施的任何經濟、金融、貿易或其他、制裁、限制、禁運、進口或出口管制、禁止移轉資金或資產或執行服務或同等措施。

（上述第 i 和 ii. 點中提及的合法行為悉依「貿易管制法律」的規定）。

b) ESET 在下列情況中應有權暫停或終止其基於這些條款的義務且立即生效：

i.ESET 基於其合理意見的判斷，認為使用者違反或可能違反本協議的第 19 a) 條；或

ii. 使用者和/或軟體變得受到貿易管制法律所約束，而導致 ESET 基於其合理意見的判斷，認為繼續履行其基於本協議的義務可能會造成 ESET 或其附屬機構違反貿易管制法律，或受到不利益的結果。

c) 本協議中的任何內容並非意指，同時不應解釋或闡釋為誘使或要求任意方以任何適用之貿易管制法律所不允許、予以處罰或禁止的任何方式作為或不作為（或同意作為或不作為）。

20.**通知**。所有的通知與退回的「軟體」及「文件」必須遞送至 ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic 不得損害 ESET 通知貴用戶關於本「合約」、「隱私權政策 EOL 政策」以及「文件」中任何變更的權利。依本「合約」的第 22 條 ESET 可能會向貴用戶傳送電子郵件、透過本「軟體」的應用程式內通知，或在我們的網站上張貼通訊。貴用戶同意以電子形式接收來自 ESET 的法律通訊，包括有關本條款、特殊條款或隱私權政策變更的任何通訊、用於處理或通知的任何合約提出/接受或邀請或其他法律通訊。此類電子通訊應視為書面接收，除非適用法律特別要求採用不同形式的通訊。

21.**準據法**。本「合約」由斯洛伐克共和國法律管理與解釋。「使用者」及「提供者」同意準據法與《聯合國際商品買賣契約公約》相抵觸的條款將不適用。貴用戶明確同意任何因本「合約」所導致與「提供者」相關的糾紛與索賠，或任何與使用本「軟體」相關的糾紛與索賠，均由 Bratislava I District Court 調解，貴用戶亦明確同意該法院行使管轄權。

22.**一般條款**。若本「合約」有任何條款無效力或不能執行，均不影響「合約」其他條款的效力。根據本「合約」規定之條件，其他條款仍保有效力並可執行。本「合約」已使用英文簽署並生效。若本「合約」的任何翻譯準備供便利之用或任何其他目的，或者若本「合約」的各個語言版本之間出現差異，則優先適用英文版本。

ESET 透過更新相關文件以 (i) 反映對本「軟體」或 ESET 執行業務方式的變更 (ii) 基於法律、法規或安全性原因，或 (iii) 為防止濫用或造成傷害，保留隨時變更本「軟體」以及修改本「合約」、其附件、附錄、隱私權政策 EOL 政策以及文件，或其中任何部分的權利。針對本「合約」的任何相關修訂，我們會透過電子郵件、應用程式內通知或其他電子方式來通知貴用戶。若貴用戶不同意對本「合約」的變更，則可以按照第 10 條，在收到更改通知後的 30 天內予以終止。除非貴用戶在此時間限制內終止本「合約」，否則自收到變更通知的日期起，已提出的變更將視為接受並對貴用戶產生約束力。

本「合約」為貴用戶和「提供者」之間與本「軟體」相關的完整「合約」，取代之前與本「軟體」相關的任何聲明、討論、保證、通訊或廣告。

協定附錄

網路連線裝置安全性評估。適用於網路連線裝置安全性評估的其他條款如下所述：

本「軟體」包含檢查使用者區域網路的安全性和區域網路中裝置安全性的功能，該功能需要區域網路名稱

和區域網路中裝置的相關資訊，例如區域網路中與授權資訊相關的裝置狀態、類型、名稱IP 位址和 MAC 位址。該資訊還包括路由器裝置的無線安全性類型和無線加密類型。該功能還可以提供關於安全性軟體解決方案的可用性資訊，以保護區域網路中的裝置。

防止資料濫用。適用於防止資料濫用的其他條款如下所述：

本「軟體」擁有可防止遺失或濫用直接連線至電腦竊取之重要資料的功能。此功能在本「軟體」預設值下為關閉。貴用戶必須建立ESET HOME 帳戶」以啟動此功能，如果電腦遭竊，此功能可藉此啟動資料收集。如果貴用戶選擇啟動本「軟體」的這項功能，即表示您同意有關遭竊電腦的資料會收集並傳送給「提供者」，其中包含有關電腦的網路位置、電腦螢幕顯示的內容、電腦的設定和/或連接至電腦的攝影機所記錄的資料（以下稱「資料」）。「資料」僅為修正電腦遭竊導致的不利狀態而以此功能和 ESET HOME 帳戶取得，「使用者」有權使用「資料」。針對此功能的唯一目的，「提供者」僅能處理隱私權政策所指定與相關法律所規定的「資料」。「提供者」允許「使用者」在所需期間存取「資料」，以達到所取得資料的目的，但不得超過隱私權政策中的保存期限。「防止資料濫用」僅可使用於「使用者」合法存取的電腦和帳戶。系統會將任何非法使用報告給主管機關。當發生資料濫用時，「提供者」會遵循相關法律，並協助執法機關。貴用戶同意且瞭解「貴用戶負責保護存取 ESET HOME 帳戶的密碼」，並同意「貴用戶不可洩露密碼給任何第三方」。不論授權與否，「使用者」負責使用「防止資料濫用」功能和 ESET HOME 帳戶進行的任何活動。如果 ESET HOME 帳戶遭盜用，請立即通知「提供者」。防止資料濫用的其他條款僅適用於 ESET Internet Security 與 ESET Smart Security Premium 使用者。

ESET Secure Data適用於 ESET Secure Data 的其他條款如下所述：

1. 定義。這些 ESET Secure Data 的其他條款中，下列字詞具相應意義：

a)資訊」使用軟體所加密或解密的任何資訊；

b)產品ESET Secure Data軟體和文件；

c)ESET Secure Data用於加密和解密電子資料的軟體；

所有複數參照應包括單數，且所有陽性參照應包括陰性及中性，反之亦然。沒有明確定義的文字應按照本「合約」規定的定義使用。

2. 其他使用者聲明。貴用戶瞭解並接受：

a) 貴用戶應負責保護、維護和備份「資訊」；

b) 在安裝 ESET Secure Data 之前，貴用戶應完整備份電腦上的所有資訊和資料（包括但不限於任何重要資訊和資料）；

c) 貴用戶必須妥善保管用於設定及使用 ESET Secure Data 的任何密碼或其他資訊，貴用戶也必須在個別儲存媒體上備份所有加密金鑰、授權代碼、金鑰檔案以及其他所產生的資料；

d) 貴用戶對於產品的使用應自行負責。針對未經授權或錯誤加密或解密的資訊或其他資料（包括但不限於資訊）所導致的任何損失、索賠或損害，無論資訊或資料的儲存位置和儲存方式為何，「提供者」概不負責；

e) 縱使「提供者」已採取所有合理步驟來確保 ESET Secure Data 的完整性和安全性，產品（或任一產品）均不可用於任何依賴故障保全安全性層級的區域，或有潛在有害或危險的區域，包括但不限於核子設施、飛機導航、控制或通訊系統、武器和防禦系統以及維生系統或生命監視系統；

f) 使用者應負責確保產品提供的安全性和加密層級符合貴用戶的需求；

g) 貴用戶對於產品（或任何一項產品）的使用應自行負責，包括但不限於確保使用情況遵循斯洛伐克共和國或在當地使用產品的其他國家、地區或州的所有適用法律和法規。在使用產品之前，貴用戶必須確保使

用不違反任何政府（斯洛伐克共和國或其他國家）的禁運法令；

h) ESET Secure Data 可隨時連絡「提供者」伺服器，以檢查授權資訊、可用的修補程式、服務套件和可改善、維護、修正或增強 ESET Secure Data 操作的其他更新，並可能會依據隱私權政策傳送與 ESET Secure Data 運作相關的一般系統資訊。

i) 針對密碼、設定資訊、加密金鑰、授權啟動代碼以及使用軟體期間所產生或儲存的其他資料，若發生遺失、遭竊、濫用、損毀、損壞或毀損，「提供者」對其所導致的任何損失、損害或索賠概不負責。增補第一條僅適用於ESET Smart Security Premium 使用者」。

ESET Secure Data 的其他條款應僅適用於 ESET Smart Security Premium 使用者。

Password Manager軟體. 適用於 Password Manager 軟體的其他條款如下所述：

1. 其他使用者聲明。貴用戶瞭解並接受貴用戶不得：

a) 使用 Password Manager 軟體來操作任何可能對生命或財產造成危險的業務關鍵應用程式。貴用戶瞭解 Password Manager 軟體並非針對此類目的而設計，且對於其在此類情況下故障可能導致死亡、人身傷害或嚴重的財物或環境損害，「提供者」則概不負責。

PASSWORD MANAGER 軟體的設計、目的或授權並非用於需要故障保安控制的有害環境，包括但不限於設計、建設、維護或操作核子設施、飛機導航或通訊系統、飛航控制和維生或武器系統。「提供者」明確聲明對於此類目的的適用性並不提供明示或默示保證。

b) 以違反本合約或斯洛伐克共和國或貴用戶司法管轄區法律的方式來使用 Password Manager 軟體。明確來說，貴用戶不得使用 Password Manager 軟體進行或提倡任何非法活動，包括上傳有害內容或可用來進行非法活動的內容、或以任何形式違反法律或第三方權利的內容（包括任何智慧財產權），包括但不限於嘗試取得「儲存裝置」中帳戶的存取權（針對這些 Password Manager 軟體的其他條款之目的，「儲存裝置」代表由「提供者」或「提供者」以外之第三方，針對啟用同步化和備份使用者資料所管理的資料儲存空間），或其他 Password Manager 軟體或「儲存裝置」使用者的任何帳戶和資料。若貴用戶違反任一條款，「提供者」有權立即終止此合約並向貴用戶收取任何必要救濟的費用，以及採取任何必要步驟防止貴用戶繼續使用 Password Manager 軟體，且不予退款。

2. 責任限制PASSWORD MANAGER 軟體係依「現狀」提供。並不提供任何類型的明示或默示擔保。貴用戶使用軟體時應自負風險。生產者對於資料遺失、損壞、服務可用性限制（包括任何由 PASSWORD MANAGER 軟體為進行資料同步化和備份而傳送至外部儲存裝置的資料）概不負責。使用 PASSWORD MANAGER 軟體加密資料並不暗示「提供者」對該資料安全性負有任何責任。貴用戶明確同意使用 PASSWORD MANAGER 軟體收集、使用、加密、儲存、同步化或傳送的資料亦可儲存於第三方伺服器（僅適用於使用已啟用同步化及備份服務的 PASSWORD MANAGER 軟體）。若「提供者」自行選擇使用第三方「儲存裝置」、網站、入口網頁、伺服器或服務，則「提供者」對此類第三方服務的品質、安全性或可用性概不負責，且「提供者」亦不須就違反任何契約或法律義務對貴用戶負責，亦不須就貴用戶使用本軟體時的損害、利益損失、財務或非財務損害或任何形式的損失對貴用戶負責。「提供者」對使用 PASSWORD MANAGER 軟體或在「儲存裝置」中取得、使用、加密、儲存、同步化或傳送的任何資料內容概不負責。貴用戶瞭解提供者無權存取所儲存資料的內容，亦無法監視或移除有違法律的內容。

提供者擁有改善、升級和修正（以下稱為「改善) Password MANAGER 軟體的一切權利，即使此類改善是根據貴用戶以任何形式提供的回饋意見、想法和建議而產生。貴用戶無權獲得任何補償，包括任何與此類改善相關的權利金。

針對貴用戶或第三方使用 PASSWORD MANAGER 軟體所導致、使用或非使用任何經紀商或經銷商，或銷售或購買任何保證所導致的任何索賠和責任，無論此類索賠和責任以任何法律或衡平法理論為基礎，提供者實體和授權者概不負責。

針對因任何第三方軟體、透過 PASSWORD MANAGER 軟體存取的任何資料、因貴用戶使用或無法使用或存取 PASSWORD MANAGER 軟體，或者透過 PASSWORD MANAGER 軟體提供的任何資料所導致的任何直接、

附帶、特殊、間接或衍生性損害，無論此類損害索賠係根據任何法律理論或衡平法理論所提出，「提供者」實體和授權者概不負責。本條款排除的損害包括但不限於商業利益損失、人身傷害或財產損失、業務中斷、業務或個人資訊損失。部分司法管轄區不允許限制附帶或衍生性損害，因此貴用戶可能不適用於此限制。在此情況下，「提供者」責任的範圍將為適用法律所允許的最低限度。

對於透過 PASSWORD MANAGER 軟體提供的資訊，包括股票報價、分析、市場資訊、新聞和財務資料可能發生延遲、不精確或包含錯誤或闕漏，「提供者」實體和授權者對此概不負責。「提供者」得隨時變更或終止 PASSWORD MANAGER 軟體中的任何部分或功能，或 PASSWORD MANAGER 軟體中任何功能或技術的使用權利而不事先通知貴用戶。

若本文章有任何條款因任何原因無效，或「提供者」須根據適用法律為損失或損害等負責，雙方同意「提供者」對貴用戶的賠償責任限制於貴用戶已支付的授權費用總額。

貴用戶同意進行補償、為之抗辯並使提供者和其員工、子公司、分公司、品牌重塑和其他合作夥伴免於任何及所有第三方的（包括裝置擁有者，或其權利受 PASSWORD MANAGER 軟體或「儲存裝置」所使用資料影響的對象）索賠、責任、損害、損失、支出以及這些對象可能因貴用戶使用 PASSWORD MANAGER 軟體而收取的費用。

3.Password Manager 軟體中的資料。除非貴用戶明確選取，否則所有貴用戶輸入且儲存於 Password Manager 軟體資料庫的資料均會以加密格式儲存於貴用戶的電腦，或其他貴用戶定義的儲存裝置。貴用戶瞭解刪除、損壞任何 Password Manager 軟體資料庫或其他檔案時，其中包含的所有資料均會永久遺失，且貴用戶瞭解並接受這些遺失風險。事實上，貴用戶的個人資料以加密格式儲存於電腦並不代表資訊無遭竊風險，或遭到發現主要密碼或取得客戶定義啟動裝置存取權以開啟資料庫之人員濫用的風險。貴用戶應負責維護所有存取方式安全無虞。

4. 傳輸個人資料至提供者或儲存裝置。若貴用戶選擇這麼做，且目的僅為確保即時同步化和備份資料，則 Password Manager 軟體可透過網際網路，從 Password Manager 軟體資料庫傳輸或傳送個人資料（亦即密碼、登入資訊、帳戶和身分）至「儲存裝置」。資料僅會以加密格式傳輸。透過 Password Manager 軟體填寫含密碼、登入或其他資料的線上表單需要將資訊透過網際網路傳送至貴用戶指定的網站。Password Manager 軟體不會啟動資料傳輸，因此對於此類與多個供應商支援的任何網站之間的互動，提供者概不負責。無論是否配合 Password Manager 軟體，任何在網際網路上的交易都由貴用戶自行處理並承受風險，且貴用戶應全權負責音下載和/或使用這類材料或服務而對貴用戶電腦系統造成的任何損害或資料遺失。為盡可能降低遺失重要資料的風險，「提供者」建議客戶定期將資料庫或其他敏感檔案備份至外部磁碟機。提供者無法協助貴用戶恢復遺失或受損的資料。若「提供者」針對使用者電腦檔案受損或遭刪除之情況提供使用者資料庫檔案備份服務，此類備份服務不包含任何保證且不暗示「提供者」對貴用戶負有任何責任。

使用 Password Manager 軟體即代表貴用戶同意軟體可隨時連絡「提供者」伺服器，以檢查授權資訊、可用的修補程式、服務套件和可改善、維護、修正或增強 Password Manager 軟體操作的其他更新。符合隱私權政策下，軟體可能會傳送與 Password Manager 軟體運作相關的一般系統資訊。

5. 解除安裝資訊和指示。在解除安裝 Password Manager 軟體之前，貴用戶必須先匯出想從資料庫保留的任何資訊。

Password Manager 軟體的其他條款應僅適用於 ESET Smart Security Premium 使用者。

ESET LiveGuard. 適用於 ESET LiveGuard 的其他條款如下所述：

本軟體包含對使用者所提交檔案進行其他分析的功能。提供者應僅根據隱私權政策和相關法規，使用由使用者提交的檔案與分析結果。

ESET LiveGuard 的其他條款應僅適用於 ESET Smart Security Premium 使用者。

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

隱私權原則

我們特別重視個人資料防護□ESET, spol. s r. o. 設址於 Einsteinova 24, 851 01 Bratislava, Slovak Republic□註冊於由 Bratislava I District Cour (Section Sro, Entry No 3586/B) 管轄的 Commercial Register□公司登記號碼：31333532 身為資料控制方（以下稱□ESET□或「我們」）。我們想要遵循 EU 一般資料防護條例（以下稱□GDPR□) 中合法標準化的透明度要求。為達此目標，「我們」茲發佈此隱私權政策，唯一目的是就下列個人資料防護主題知會身為資料主體的客戶（以下稱「使用者」或「貴用戶」）：

- 個人資料處理的法律依據、
- 資料共用和機密性、
- 資料安全性、
- 貴用戶身為資料主體的權利、
- 處理貴用戶的個人資料
- 連絡人資訊。

個人資料處理的法律依據

根據與保護個人資料相關的適用法律架構，我們針對資料處理僅會使用幾項法律依據□ESET 處理個人資料主要為履行與使用者之間 使用者授權合約（以下稱□EULA□) 與使用者 (GDPR 第 6 (1) (b) 條)，適用於 ESET 產品或服務的提供，除非另有明確聲明，例如：

- 合法利益的法律依據 (GDPR 第 6 (1) (f) 條)，這使我們可以處理有關客戶如何使用我們的服務及其滿意度的資料，以便為使用者提供最佳的防護、支援和體驗。適用法律承認的對等行銷是一種正當利益，因此與我們客戶進行行銷通訊時，我們通常會依賴此概念。
- 當我們將此法律依據視為最適合的法律依據，或者如果法律要求時，我們可能會在特定情況下向貴用戶要求同意 (GDPR 第 6 (1) (a) 條)。
- 遵守法律義務 (GDPR 第 6 (1) (c) 條)，例如電子通訊、保留用於開票或計費文件的明訂要求。

資料共用和機密性

我們不會與第三方共用貴用戶的資料。但是□ESET 公司的全球營運透過銷售、服務和支援網路中的附屬公司或合作夥伴來進行□ESET 處理的授權、計費與技術支援資訊得傳輸至/自附屬機構或合作夥伴以履行提供服務或支援等 EULA 的目的。

ESET 偏好在歐盟 (EU) 境內處理其資料。但是，根據貴用戶的位置（使用我們產品和/或 EU 以外的服務）和/或貴用戶選擇的服務，可能需要將貴用戶的資料傳輸至 EU 以外的國家/地區。例如，我們會使用與雲端運算相關的第三方服務。在這種情況下，我們會仔細選擇服務提供者，並透過合約以及技術和組織措施以確保適當的資料防護層級。一般而言，我們同意 EU 標準合約條款，以及必要時的補充合約規範。

針對 EU 以外的部分國家/地區，例如英國與瑞士□EU 已決定相應的資料防護層級。基於相應的資料防護層級，向這些國家/地區傳輸資料時不需要任何特殊授權或協議。

資料安全性

ESET 運用適當的技術和組織措施確保與潛在風險相當的安全性層級。「我們」盡力確保處理系統和服務持

續具備保密性、完整性、可用性和韌性。然而，若資料外洩導致貴用戶的權利和自由產生風險，「我們」會通知相關監管當局以及作為資料主體的受影響使用者。

資料當事人權利。

我們重視每位使用者的權利，故在此通知貴用戶，所有使用者（來自任何 EU 或任何非 EU 國家/地區）在 ESET 中皆享有下列權利。若要行使資料主體的權利，貴用戶可以透過支援表格或電子郵件 dpo@eset.sk 聯繫我們。基於身分識別目的，我們會要求貴用戶提供下列資訊：姓名、電子郵件地址與授權金鑰或客戶號碼以及公司機構（若適用）。請避免向我們傳送任何其他個人資料，例如出生日期。請注意，為了能夠處理貴用戶的要求，以及基於身分識別目的，我們將會處理貴用戶的個人資料。

撤回同意的權利。撤回同意的權利僅適用於基於同意的處理行為。如果我們基於貴用戶的同意而處理個人資料，則貴用戶有權不附帶理由隨時撤回同意。貴用戶撤回同意僅對將來有效，而不會影響撤回之前已處理資料的合法性。

拒絕的權利。拒絕處理的權利僅適用於基於 ESET 或第三方合法利益的處理行為。如果我們處理個人資料以保護合法利益，則貴用戶身為資料主體有權隨時反對我們主張的合法權益以及對貴用戶個人資料的處理。貴用戶的拒絕僅對將來有效，而不會影響拒絕之前已處理資料的合法性。如果我們基於直接行銷目的而處理貴用戶的個人資料，則不必提供貴用戶的拒絕理由。此規定也適用於特徵分析，因為它與此類直接行銷相關。在所有其他情況下，我們要求貴用戶簡短地告訴我們針對 ESET 處理貴用戶個人資料的合法利益提出申訴。

請注意，在某些情況下，儘管貴用戶同意已撤回，我們仍有權基於其他法律依據（例如合約履行）進一步處理貴用戶的個人資料。

存取的權利。身為資料主體，貴用戶有權隨時免費取得 ESET 所儲存貴用戶資料的相關資訊。

修正的權利。如果我們無意中處理了關於貴用戶不正確的個人資料，則貴用戶有權修正此資料。

清除的權利與限制處理的權利。身為資料主體，貴用戶有權要求刪除或限制處理貴用戶的個人資料。如果我們處理貴用戶的個人資料，例如在貴用戶同意的情況下，貴用戶撤回同意而無其他法律依據（例如合約）時，我們會立即刪除貴用戶的個人資料。針對我們保留期結束時所規定用途而不再需要的個人資料會立即刪除。

如果我們將貴用戶的個人資料用於直接行銷的唯一目的，且貴用戶已撤回同意或反對ESET的基本合法利益，則在我們於內部黑名單中納入貴用戶連絡人資料的範圍內，我們將限制處理貴用戶的個人資料，以避免來路不明的連絡人。否則，我們將會刪除貴用戶的個人資料。

請注意，我們可能需要儲存貴用戶的資料，直到立法機關或監管機構發出的保留義務與期間到期為止。保留義務和期間可能也來自斯洛伐克法律。此後，我們將定期刪除相應資料。

資料可攜性的權利。我們很樂意替身為資料主體的貴用戶提供由 ESET 以 xls 格式處理的個人資料。

提出申訴的權利。身為資料主體，貴用戶有權隨時向監管機構提出申訴ESET 受斯洛伐克法規規範，「我們」身為歐盟一份子，也受資料保護法規規範。相關的資料監管機構即為斯洛伐克共和國個人資料防護辦公室，位於 Hraničná 12, 82007 Bratislava 27, Slovak Republic

處理貴用戶的個人資料

ESET 所提供並在我們的產品中實作的服務，係根據 使用者授權合約的條款提供，但貴用戶需特別注意其中幾項規定。我們想要將更多與我們所佈建服務連接的資料集合相關詳細資料提供給您。我們提供 EULA 與產品中所述的各種服務 文件. 為使一切順利進行，我們需要收集以下資訊：

授權與計費資料。ESET 會收集和處理姓名、電子郵件地址、授權金鑰以及（若適用）地址、公司機構與付款資料，以便協助處理啟動授權、授權金鑰傳遞、過期提醒、支援要求、授權真實性驗證、提供我們的服

務與其他通知，包含按照適用法規或貴用戶同意的行銷訊息ESET 依法有義務保留計費資訊 10 年，但授權資訊將在授權到期後的 12 個月內匿名處理。

更新與其他統計資料。處理的資訊包含安裝程序與貴用戶電腦的資訊，包含我們產品所安裝的平台，以及我們產品之操作與功能的資訊，例如作業系統、硬體資訊、安裝 IDD授權 IDDIP 位址DMAC 位址、產品配置設定，處理目的包含提供服務的更新與升級，以及符合維護、安全性與改進我們後端基礎結構的需求。

保留此資訊的目的不同於授權和計費目的所需的身分識別資訊，因為它不需要識別使用者的身分。保留期間最長 4 年。

ESET LiveGrid® 聲譽系統。與入侵相關的單向雜湊處理目的係基於 ESET LiveGrid® 聲譽系統，可將掃描的檔案與雲端中的白名單和黑名單項目比較，以改善我們的反惡意軟體解決方案的效率。此程序期間不會識別使用者的身分。

ESET LiveGrid® 意見系統。來自全球的可疑範例及中繼資料屬於 ESET LiveGrid® 意見系統的一部分，可讓 ESET 針對使用者立即採取行動並讓我們隨時掌握最新的威脅。我們仰賴您傳送

- 可疑病毒範例及其他惡意程式和可疑、有問題、潛在不需要或潛在不安全物件（例如，可執行檔、您回報為垃圾郵件或是由產品標記為垃圾郵件的電子郵件）此類入侵行為；
- 使用網路的資訊，例如 IP 位址和地理資訊DIP 封包DURLD乙太網路框架；
- 當機傾印檔案及所包含的資訊。

「我們」無意在此範圍外收集您的資料，但有時無法避免。意外收集的資料可能包含在惡意軟體本身（在您不知情或未核准的情況下所收集）或是檔案名稱或 URL 的一部分，「我們」無意使其構成我們系統的一部分，或以本隱私權政策所宣告的目的處理之。

透過 ESET LiveGrid® 意見系統取得和處理的所有資訊應在不需要識別使用者身份的情況下進行。

網路連線裝置安全性評估。為了提供安全性評估功能，我們會處理區域網路名稱和區域網路中裝置的相關資訊，例如區域網路中與授權資訊相關的裝置狀態、類型、名稱DIP 位址和 MAC 位址。該資訊還包括路由器裝置的無線安全性類型和無線加密類型。識別使用者的授權資訊將在授權到期後的 12 個月內匿名處理。

技術支援。貴用戶可能需要將連絡人與授權資訊及資料納入支援要求中以獲得支援服務。您可能需要在支援請求內納入聯絡資訊及資料，以獲得支援服務。依「貴用戶」聯絡我們的通道而定，「我們」可能會收集您的電子郵件地址、電話號碼、授權資訊、產品詳情和您支援案例的說明。為協助支援服務，我們可能要求「貴用戶」提供其他資訊。針對技術支援目的處理的資料會儲存 4 年。

防止資料濫用。如果 https://home.eset.com 上的 ESET HOME 帳戶已建立，且該功能由使用者啟動，但與電腦遭竊相關，則我們將收集和處理下列資訊：位置資料、螢幕擷取畫面、電腦配置，以及電腦相機所記錄的資料。收集的資料會儲存在我們的伺服器或服務提供者的伺服器上並保留 3 個月。

Password ManagerD若貴用戶選擇啟動 Password Manager 的功能，則與貴用戶登入詳細資料相關的資料僅會以加密形式儲存在貴用戶的電腦或其他指定的裝置中。如果您啟動同步化服務，便會將加密的資料儲存在伺服器或服務提供者的伺服器上，以確保此類服務的安全DESET 或服務提供者均無法存取加密的資料。只有您有金鑰而可解密該資料。停用該功能時將會刪除資料。

ESET LiveGuard. 若貴用戶選擇啟動 ESET LiveGuard 功能，則需要提交範例，例如使用者預先定義和選取的檔案。貴用戶針對遠端分析所選擇的範例將上傳至 ESET 服務，而分析結果將傳送回貴用戶的電腦。任何可疑範例將按照 ESET LiveGrid® 意見系統收集的資訊進行處理。

客戶經驗改進計畫。如果您選擇啟動 客戶經驗改進計畫 ，在您同意的情況下，將會收集和使用與使用我們產品相關的匿名遙測資訊。

請注意，使用我們產品與服務的使用者並非已購買產品或服務並與我們簽訂 EULA 的使用者（例如使用者的員工、家庭成員，或使用者有權根據 EULA 使用產品或服務的人員），根據 GDPR 第 6 (1) (f) 條規定，對資料的處理應基於 ESET 的合法利益，以允許使用者授權的使用者根據 EULA 使用我們所提供的產品與服務。

連絡人資訊

如果您想要行使您身為資料當事人的權利，或您有任何疑問或疑慮，請將訊息傳送給我們：

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk