

ESET Endpoint Antivirus

使用者手冊

[按一下此處顯示此文件的連線版本](#)

版權 ©2024 由 ESET, spol. s r.o. 所有

ESET Endpoint Antivirus 由 ESET, spol. s r.o. 所開發

如需詳細資訊，請造訪 <https://www.eset.com>

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

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

技術支援 <https://support.eset.com>

修訂。2024年m月12日

1 ESET Endpoint Antivirus	1
1.1 新增功能	2
1.2 系統需求	2
1.2 支援的語言	3
1.3 變更防護記錄	4
1.4 預防	4
1.5 終止支援狀態	5
1.6 說明頁面	8
2 遠端受管端點適用的文件	9
2.1 ESET PROTECT 簡介	10
2.2 ESET PROTECT Cloud 簡介	10
2.3 密碼保護的設定	11
2.4 何謂原則?	11
2.4 合併原則	12
2.5 旗標的運作方式	12
3 安裝	13
3.1 使用 ESET AV Remover 安裝	14
3.1 ESET AV Remover	14
3.1 使用 ESET AV Remover 解除安裝結束時發生錯誤	17
3.2 安裝 (.exe)	17
3.2 變更安裝資料夾 (.exe)	19
3.3 安裝 (.msi)	19
3.3 進階安裝 (.msi)	20
3.4 最小模組安裝	21
3.5 命令列安裝	21
3.6 使用 GPO 或 SCCM 進行部署	25
3.7 升級至最新版本	27
3.7 舊版產品自動升級	28
3.8 安全性和穩定性更新	28
3.9 產品啟動	28
3.9 在啟動期間輸入您的授權金鑰	29
3.9 ESET HUB 帳戶	29
3.9 如何使用舊版授權憑證來啟動 ESET 端點產品	30
3.9 啟動失敗	30
3.9 註冊	30
3.9 啟動進度	30
3.9 啟動成功	30
3.10 常見安裝問題	30
4 初學者手冊	31
4.1 系統匣圖示	31
4.2 鍵盤快捷鍵	31
4.3 設定檔	32
4.4 內容功能表	32
4.5 更新設定	33
4.6 配置網路防護	34
4.7 封鎖的雜湊	35
5 使用 ESET Endpoint Antivirus	35
5.1 防護狀態	37
5.2 電腦掃描	39
5.2 自訂掃描啟動器	41

5.2 掃描進度	42
5.2 電腦掃描防護記錄	43
5.3 更新	45
5.3 如何建立更新工作	48
5.4 設定	48
5.4 電腦	49
5.4 偵測到威脅	51
5.4 網路	53
5.4 網路存取疑難排解	54
5.4 暫時性 IP 位址黑名單	54
5.4 網路防護防護記錄	54
5.4 解決 ESET 網路防護問題	55
5.4 記錄並從防護記錄建立規則或例外	55
5.4 從防護記錄建立規則	55
5.4 網路防護進階記錄	56
5.4 使用網路流量掃描器解決問題	56
5.4 已封鎖網路威脅	57
5.4 Web 和電子郵件	57
5.4 防網路釣魚防護	58
5.4 匯入及匯出設定	59
5.5 工具	60
5.5 防護記錄檔案	61
5.5 防護記錄過濾	63
5.5 審查防護記錄	64
5.5 執行程序	65
5.5 安全性報告	66
5.5 ESET SysInspector	67
5.5 排程器	68
5.5 已排程掃描選項	70
5.5 已排程的工作概要	70
5.5 工作細節	70
5.5 工作時間	71
5.5 工作時間 - 一次	71
5.5 工作時間 - 每天	71
5.5 工作時間 - 每週	71
5.5 工作時間 - 由事件觸發	71
5.5 略過的工作	71
5.5 工作詳細資料 - 更新	72
5.5 工作詳細資料 - 執行應用程式	72
5.5 提交樣本以供分析	72
5.5 選取樣本以供分析 - 可疑檔案	73
5.5 選取樣本以供分析 - 可疑網站	73
5.5 選取樣本以供分析 - 誤判檔案	73
5.5 選取樣本以供分析 - 誤判網站	74
5.5 選取樣本以供分析 - 其他	74
5.5 隔離區	74
5.6 說明及支援	76
5.6 關於 ESET Endpoint Antivirus	76
5.6 提交系統配置資料	77
5.6 技術支援	77
6 進階設定	78

6.1 偵測引擎	79
6.1 排除	79
6.1 效能排除	80
6.1 新增或編輯效能排除	81
6.1 路徑排除格式	82
6.1 偵測排除	83
6.1 新增或編輯偵測排除	85
6.1 建立偵測排除精靈	86
6.1 偵測引擎進階選項	87
6.1 網路流量掃描器	87
6.1 雲端型防護	87
6.1 適用於雲端型防護的排除過濾器	90
6.1 惡意軟體掃描	90
6.1 掃描設定檔	91
6.1 掃描目標	91
6.1 閒置狀態掃描	92
6.1 閒置狀態偵測	92
6.1 啟動掃描	92
6.1 啟動檔案自動檢查	93
6.1 可移除的媒體	93
6.1 文件防護	94
6.1 HIPS - 主機入侵預防系統	94
6.1 HIPS 排除	96
6.1 HIPS 進階設定	97
6.1 一律允許載入驅動程式	97
6.1 HIPS 互動視窗	97
6.1 偵測到潛在的勒索軟體行為	98
6.1 HIPS 規則管理	98
6.1 HIPS 規則設定	99
6.1 新增 HIPS 的應用程式/登錄路徑	101
6.2 更新	101
6.2 更新還原	104
6.2 產品更新	106
6.2 連線選項	106
6.2 更新映像	107
6.2 適用於映像的 HTTP 伺服器和 SSL	108
6.2 從映像更新	109
6.2 疑難排解映像更新問題	110
6.3 防護	111
6.3 即時檔案系統防護	114
6.3 程序排除	116
6.3 新增或編輯程序排除	117
6.3 何時修改即時防護配置	117
6.3 檢查即時防護	117
6.3 即時防護無法運作時怎麼辦	117
6.3 網路存取防護	118
6.3 網路連線設定檔	119
6.3 新增或編輯網路連線設定檔	119
6.3 啟動項	120
6.3 IP 集	121
6.3 編輯 IP 集	122

6.3 網路攻擊防護 (IDS)	122
6.3 IDS 規則	123
6.3 蠻力攻擊防護	125
6.3 規則	125
6.3 排除	127
6.3 進階選項	128
6.3 SSL/TLS	129
6.3 應用程式掃描規則	130
6.3 憑證規則	131
6.3 加密的網路流量	132
6.3 電子郵件用戶端防護	132
6.3 郵件傳輸防護	132
6.3 排除的應用程式	133
6.3 排除的 IP	134
6.3 信箱防護	135
6.3 整合	136
6.3 Microsoft Outlook 工具列	136
6.3 確認對話方塊	136
6.3 重新掃描郵件	136
6.3 回應	137
6.3 ThreatSense	137
6.3 Web 存取防護	139
6.3 排除的應用程式	141
6.3 排除的 IP	142
6.3 URL 清單管理	143
6.3 位址清單	144
6.3 建立新的位址清單	145
6.3 如何新增 URL 遮罩	146
6.3 HTTP 流量掃描	146
6.3 ThreatSense	147
6.3 裝置控制	149
6.3 裝置控制規則編輯器	149
6.3 偵測到的裝置	150
6.3 新增裝置控制規則	151
6.3 裝置群組	153
6.3 ThreatSense	154
6.3 清除層級	156
6.3 從掃描中排除的檔案副檔名	157
6.3 其他 ThreatSense 參數	157
6.4 工具	157
6.4 時段	158
6.4 Microsoft Windows 更新	158
6.4 對話方塊視窗 - 作業系統更新	159
6.4 更新資訊	159
6.4 ESET CMD	159
6.4 遠端監視和管理	161
6.4 ERMM 命令列	162
6.4 ERMM JSON 命令清單	163
6.4 取得防護 - 狀態	164
6.4 取得應用程式 - 資訊	164
6.4 取得授權 - 資訊	167

6.4 取得防護記錄	167
6.4 取得啟動 - 狀態	168
6.4 取得掃描 - 資訊	169
6.4 取得配置	170
6.4 取得更新 - 狀態	171
6.4 開始掃描	172
6.4 開始啟動	172
6.4 開始停用	173
6.4 開始更新	174
6.4 設定配置	174
6.4 授權間隔檢查	175
6.4 防護記錄檔案	175
6.4 簡報模式	176
6.4 診斷	176
6.4 技術支援	177
6.5 連線	177
6.6 使用者介面	179
6.6 使用者介面元素	179
6.6 存取設定	180
6.6 進階設定的密碼	181
6.6 密碼	182
6.6 安全模式	182
6.7 通知	182
6.7 應用程式狀態	183
6.7 桌面通知	184
6.7 自訂通知	185
6.7 對話方塊視窗 - 桌面通知	185
6.7 互動警告	186
6.7 互動警告清單	187
6.7 確認訊息	189
6.7 進階設定衝突錯誤	189
6.7 需要重新啟動	190
6.7 建議重新啟動	190
6.7 轉送	190
6.7 將所有設定還原為預設值	192
6.7 還原目前區段中的所有設定	192
6.7 儲存配置時發生錯誤	193
6.8 指令列掃描器	193
7 常見問題	195
7.1 自動更新常見問題	196
7.2 如何更新 ESET Endpoint Antivirus	198
7.3 如何從我的 PC 移除病毒	198
7.4 如何在排程器中建立新的工作	198
7.4 如何安排每週電腦掃描	199
7.5 如何連接 ESET Endpoint Antivirus 至 ESET PROTECT	199
7.5 如何使用覆寫模式	200
7.5 如何為 ESET Endpoint Antivirus 套用建議的原則	201
7.6 如何配置映像	203
7.7 如何利用 ESET Endpoint Antivirus 升級至 Windows 10	204
7.8 如何啟動遠端監視和管理	204
7.9 如何封鎖從網際網路下載特定檔案類型	206

7.10 如何將 ESET Endpoint Antivirus 使用者介面縮至最小	207
8 使用者授權合約	208
9 隱私權原則	213

ESET Endpoint Antivirus

ESET Endpoint Antivirus 代表確實整合電腦安全性的新方法。最新版本的 ESET LiveGrid® 掃描引擎利用速度及精確度確保電腦安全。其成品就是能夠持續監控危害您電腦的攻擊及惡意軟體的智慧型系統。

ESET Endpoint Antivirus 是經由長期努力所開發的完整安全性解決方案，結合了最嚴格的防護並佔用最低的系統使用量。這種奠基於人工智慧的進階技術，能夠主動消除**病毒**、間諜程式、特洛伊木馬、蠕蟲、廣告軟體、rootkit 及其他**網際網路型攻擊**的入侵，而且不會妨礙系統效能或中斷電腦運作。

ESET Endpoint Antivirus 的設計主要用於小型企業環境中的工作站。

在[安裝](#)一節中，您可以找到分成數個章節的說明主題，以提供您訓練並幫助您熟悉本產品內容，包括[下載與安裝](#)和[啟動](#)。

在企業環境中[使用 ESET Endpoint Antivirus 與 ESET PROTECT](#) 搭配時，可讓您輕鬆管理任意數目的用戶端工作站、套用原則與規則、監視偵測，並從任何網路電腦遠端配置。

[常見問題](#)一章涵蓋一些使用者最常詢問的問題以及最常遇到的問題。

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 Endpoint Antivirus 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 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 Endpoint Antivirus 檢查執行中處理程序與檔案的聲譽。
遠端管理	ESET PROTECT 可讓您透過一個中央位置、在網路環境中的工作站、伺服器和行動裝置管理 ESET 產品。您可以使用 ESET PROTECT Web 主控台 (ESET PROTECT Web 主控台)，部署 ESET 解決方案、管理工作、執行安全性原則、監視系統狀態，並快速回應遠端電腦上的問題或威脅。
網路攻擊防護	分析網路流量內容以及防護其免於網路攻擊。將封鎖任何視為有害的流量並防止來自網路的攻擊。
Web 控制 (僅限 ESET Endpoint Security)	Web 控制可讓您封鎖可能包含潛在冒犯性資訊的網頁。此外，雇主或系統管理員可禁止存取超過 27 個預先定義的網站類別及 140 多個子類別。

新增功能

ESET Endpoint Antivirus 第 11 版中的新增功能

弱點與修補程式管理

[ESET PROTECT Cloud](#) 中提供的功能會定期掃描工作站，以偵測任何容易遭到安全性風險感染的已安裝軟體。[修補程式管理](#)會在開始下載之前檢查可用空間是否相符（預設值和最小值為 2GB）並透過自動軟體更新說明修復這些風險，使裝置更加安全。

終止支援產品狀態

ESET Endpoint Antivirus 在此版本中可以顯示各種[終止支援產品狀態](#)。您可以在[通知](#)中設定終止支援狀態。

各種錯誤修正和效能提升

系統需求

若要使 ESET Endpoint Antivirus 順暢地運作，系統應滿足下列硬體和軟體需求（預設產品設定）：

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


作業系統

Microsoft® Windows® 11

Microsoft® Windows® 10

 如需受支援 Microsoft® Windows® 10 和 Microsoft® Windows® 11 版本的詳細清單，請參閱 [Windows 作業系統支援原則](#)

 一律嘗試將作業系統維持在最新狀態。

 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](#)

ESET Endpoint Antivirus 功能需求

請參閱下表中特定 ESET Endpoint Antivirus 功能的系統需求：

功能	需求
Intel® Threat Detection Technology	參閱 支援的處理器
專用清除程式	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。

i 在 ESET PROTECT 中建立的 ESET Endpoint Antivirus 安裝程式支援 Windows 10 Enterprise for Virtual Desktops 和 Windows 10 多重工作階段模式。

其他

- 已滿足在電腦上安裝作業系統和其他軟體的系統需求
- 0.3 GB 的可用系統記憶體（請參閱附註 1）
- 1 GB 的可用硬碟空間（請參閱附註 2）
- 最小顯示器解析度 1024 x 768
- 網際網路或區域網路連線至產品更新的來源（請參閱附註 3）
- 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

雖然可能在未符合這些需求的系統上安裝並執行產品，我們建議依據效能需求先行作使用性測試。

- i** (1) 如果在嚴重受感染的電腦上使用不到記憶體，或是當資料大量清單已匯入到產品之中（例如 URL 的白名單），產品可能會使用更多記憶體。
- (2) 需要硬碟空間來下載安裝程式、安裝產品、並在程式資料中保留安裝套件的副本，同時也保留產品更新的備份以支援回復功能。在不同的設定下（例如，產品更新的備份版本增加時，保留記憶體傾印或大量的防護記錄）或是在受感染的電腦上（由於隔離區功能），產品可能會使用更多硬碟空間。我們建議保留足夠的硬碟空間，來支援作業系統和 ESET 產品的更新。
- (3) 雖然不建議這麼做，產品仍可自卸除式媒體上進行手動更新。

支援的語言

ESET Endpoint Antivirus 提供以下語言的安裝和下載。

語言	語言代碼	LCID
英文（美國）	en-US	1033
阿拉伯文（埃及）	ar-EG	3073
保加利亞文	bg-BG	1026
簡體中文	zh-CN	2052
繁體中文	zh-TW	1028
克羅埃西亞文	hr-HR	1050
捷克文	cs-CZ	1029
愛沙尼亞文	et-EE	1061
芬蘭文	fi-FI	1035
法文（法國）	fr-FR	1036
法文（加拿大）	fr-CA	3084
德文（德國）	de-DE	1031
希臘文	el-GR	1032
*希伯來文	he-IL	1037
匈牙利文	hu-HU	1038
*印尼文	id-ID	1057
義大利文	it-IT	1040
日文	ja-JP	1041
哈薩克文	kk-KZ	1087

語言	語言代碼	LCID
韓文	ko-KR	1042
*拉脫維亞文	lv-LV	1062
立陶宛文	lt-LT	1063
Nederlands	nl-NL	1043
挪威文	nb-NO	1044
波蘭文	pl-PL	1045
葡萄牙文（巴西）	pt-BR	1046
羅馬尼亞文	ro-RO	1048
俄文	ru-RU	1049
西班牙文（智利）	es-CL	13322
西班牙文（西班牙）	es-ES	3082
瑞典文（瑞典）	sv-SE	1053
斯洛伐克文	sk-SK	1051
斯洛維尼亞文	sl-SI	1060
泰文	th-TH	1054
土耳其文	tr-TR	1055
烏克蘭文（烏克蘭）	uk-UA	1058
*越南文	vi-VN	1066

* ESET Endpoint Antivirus 提供此語言，但不提供線上使用者指南（重新導向至英文版本）。

若要變更此線上使用者指南的語言，請查看語言選取方塊（在右上角）。

變更防護記錄

預防

當您使用電腦時，尤其是在瀏覽網際網路時，請記得沒有任何防毒系統可以完全消除[偵測](#)與[遠端攻擊](#)。為達到最大的保護性及方便性，您必須正確地使用防毒解決方案並遵守數項有用的規則：

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 Virus Lab 的專家每天分析這些威脅，並準備和發佈更新以持續地為使用者改進防護層級。為確保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代碼的效力。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 Microsoft Edge 等 Web 瀏覽器就是會有安全更新定期發佈的兩個範例。

備份重要資料

惡意軟體作者通常不關心使用者需求，惡意程式活動常常導致作業系統故障和重要資料遺失。定期備份您的資料至 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已知與未知的病毒、蠕蟲、特洛伊木馬程式及 Rootkit[®]。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

最有用且最有效的規則就是務必小心謹慎。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。

終止支援狀態

ESET Endpoint Antivirus 可以顯示自動通知或警告，以在主要程式視窗中的多個位置通知您即將終止支援的資訊。

閱讀更多相關資訊：

- [生命週期結束原則（商業產品）](#)
- [產品更新](#)
- [安全性和穩定性 Hotfix](#)

如需關於 ESET Endpoint Antivirus 變更的其他資訊，請參閱以下 [ESET 知識庫文章](#)^②

下表顯示產品狀態和通知的一些範例，其中包含基於類別的操作：

類別	通知或警告視窗	更新頁面	說明及支援頁面
推出新功能或服務更新	<p>i 有可用的新版本</p> <p>包含 ESET Endpoint Antivirus 所需的重要服務修正的更新現已推出。立即更新以確保提供最新防護。</p> <p>處理方法:深入瞭解</p>	<p>i ESET Endpoint Antivirus 有新的版本。</p> <p>ESET Endpoint Antivirus 有新的版本。</p> <p>處理方法:立即更新/啟用自動更新</p>	<p>i ESET Endpoint Antivirus 有新的版本。立即更新以獲得具有全新和改進功能的最新版本。</p> <p>支援的期限mm/dd/yyyy</p>
	<p>i 產品更新現已推出</p> <p>ESET Endpoint Antivirus 有新的版本。立即更新以獲得具有全新和改進功能的最新版本。</p> <p>處理方法:深入瞭解</p>	<p>i ESET Endpoint Antivirus 的服務更新現已推出</p> <p>安裝的版本號碼 支援的期限mm/dd/yyyy</p> <p>處理方法:深入瞭解</p>	<p>i 包含 ESET Endpoint Antivirus 所需的重要服務修正的更新現已推出。立即更新以確保提供最新防護。</p> <p>支援的期限mm/dd/yyyy</p>
	<p>! 建議重新啟動裝置</p> <p>包含 ESET Endpoint Antivirus 所需的重要服務修正的更新現已推出。立即更新以確保提供最新防護。</p> <p>處理方法:深入瞭解</p>		<p>支援的期限mm/dd/yyyy</p>
	<p>! 重大服務更新現已推出</p> <p>包含 ESET Endpoint Antivirus 所需的重大服務修正的更新現已推出。立即更新以確保提供最新防護。</p> <p>處理方法:深入瞭解</p>	<p>! ESET Endpoint Antivirus 的重大服務更新現已推出</p> <p>安裝的版本號碼 支援的期限mm/dd/yyyy</p> <p>處理方法:深入瞭解</p>	<p>! 包含 ESET Endpoint Antivirus 所需的重大服務修正的更新現已推出。立即更新以確保提供最新防護。</p> <p>支援的期限mm/dd/yyyy</p>
	<p>! 需要重新啟動裝置</p> <p>已下載版本號碼更新，其中包含您 ESET Endpoint Antivirus 所需的重要服務和穩定性修正。立即更新以確保提供最新防護。</p> <p>處理方法:深入瞭解</p>		<p>支援的期限mm/dd/yyyy</p>

類別	通知或警告視窗	更新頁面	說明及支援頁面
對應 用程 式的 支援 即將 到期	<p> 對於您已安裝應用程式版本的支援將於 mm/dd/yyyy 結束，您的裝置很快將會失去防護。立即更新以持續受到防護。</p> <p>處理方法: 立刻更新</p>	<p> 安裝的版本號碼/支援的期限 mm/dd/yyyy</p> <p>處理方法: 立即更新/啟用自動更新</p>	<p> 對於 ESET Endpoint Antivirus 安裝版本的支援即將結束，並且您的電腦將失去防護。立即更新以持續受到防護。</p> <p>支援的期限 mm/dd/yyyy</p>
	<p> 對於您已安裝應用程式版本的 ESET 延伸支援將於 mm/dd/yyyy 結束，您的裝置很快將會失去防護。立即更新以持續受到防護。</p> <p>處理方法: 立刻更新</p>	<p> 安裝的版本號碼/支援的期限 mm/dd/yyyy</p> <p>處理方法: 立即更新/啟用自動更新</p>	<p> 對於 ESET Endpoint Antivirus 安裝版本的 ESET 延伸支援即將結束，並且您的裝置將失去防護。立即更新以持續受到防護。</p> <p>支援的期限 mm/dd/yyyy</p>
	<p> 安裝的作業系統已過期，對於您已安裝應用程式版本的支援已於 mm/dd/yyyy 結束。升級您的作業系統以取得最新的應用程式更新並保持防護。</p> <p>處理方法: 深入瞭解</p>	<p> 安裝的版本號碼 支援的期限 mm/dd/yyyy</p> <p>處理方法: 深入瞭解</p>	<p> 對於 ESET Endpoint Antivirus 安裝版本的支援即將結束，並且您的電腦將失去防護。立即更新以持續受到防護。</p> <p>支援的期限 mm/dd/yyyy</p>
	<p> 已安裝應用程式版本的 ESET 延伸支援即將結束</p> <p>安裝的作業系統已過期，對於您已安裝應用程式版本的支援已於 mm/dd/yyyy 結束。升級您的作業系統以取得最新的應用程式更新並保持防護。</p> <p>處理方法: 深入瞭解</p>	<p> 對於 ESET Endpoint Antivirus 安裝版本的 ESET 延伸支援即將結束</p> <p>安裝的版本號碼 支援的期限 mm/dd/yyyy</p> <p>處理方法: 深入瞭解</p>	<p> 對於 ESET Endpoint Antivirus 安裝版本的 ESET 延伸支援即將結束，並且您的裝置將失去防護。立即更新以持續受到防護。</p> <p>支援的期限 mm/dd/yyyy</p>
不再 支援 應用 程式 版本	<p> 不再支援已安裝的應用程式版本</p> <p>對於您已安裝應用程式版本的支援已結束，並且您的裝置可能不受保護。立即更新以取得防護。</p> <p>處理方法: 立刻更新</p>	<p> 不再支援已安裝的 ESET Endpoint Antivirus 版本</p> <p>安裝的版本號碼/支援的期限 mm/dd/yyyy</p> <p>處理方法: 立即更新/啟用自動更新</p>	<p> 支援的期限 mm/dd/yyyy</p>
	<p> 不再支援已安裝的應用程式版本</p> <p>安裝的作業系統已過期，對於您已安裝應用程式版本的支援已結束。您的電腦未受保護。升級您的作業系統，以接收最新的應用程式更新並取得防護。</p> <p>處理方法: 深入瞭解</p>	<p> 不再支援已安裝的 ESET Endpoint Antivirus 版本</p> <p>安裝的版本號碼 支援的期限 mm/dd/yyyy</p> <p>處理方法: 深入瞭解</p>	<p> 對於 ESET Endpoint Antivirus 安裝版本的支援已結束，並且您的電腦不受保護。立即更新以取得防護。</p> <p>支援的期限 mm/dd/yyyy</p>

類別	通知或警告視窗	更新頁面	說明及支援頁面
需要作業系統更新	 安裝的作業系統已過期 安裝的作業系統已過期。升級您的作業系統以取得最新的應用程式更新並保持防護。 處理方法: 深入瞭解	 ESET Endpoint Antivirus 安裝的版本號碼	支援的期限mm/dd/yyyy

說明頁面

歡迎使用 ESET Endpoint Antivirus 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

開始使用 ESET Endpoint Antivirus 之前，請注意，可以使用 [ESET PROTECT](#) 遠端管理產品。我們也建議您先熟悉在使用電腦時可能遇到的各種[偵測類型](#)和[遠端攻擊](#)。

請參閱「[新功能](#)」以瞭解這個 ESET Endpoint Antivirus 版本所推出功能的相關資訊。我們準備了手冊，以協助您設定及自訂 ESET Endpoint Antivirus 的基本設定。


如何使用 ESET Endpoint Antivirus 說明頁面

[說明] 主題分成數個章節，以提供您訓練並幫助您熟悉本產品內容。您可以瀏覽說明頁面結構，即可找到相關的資訊。


若要瞭解有關程式中任何視窗的詳細資訊，請按下 **F1** 鍵。即會顯示與目前檢視視窗相關的說明頁面。


您可以依關鍵字或輸入字詞或片語來搜尋「說明」頁面。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，而且僅會顯示包含所搜尋單字或片語的頁面。

為了維持一致性並協助避免造成混亂，本指南中所使用的術語都是根據 ESET Endpoint Antivirus 參數名稱。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。請閱讀並了解位於警告括弧內的文字，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。
<i>斜體</i>	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。

遠端受管端點適用的文件

您可以透過一個中央位置，在網路環境的用戶端工作站、伺服器 and 行動裝置上遠端管理 ESET 商業產品與 ESET Endpoint Antivirus。管理 10 個以上用戶端工作站的系統管理員可能會考慮部署其中一個 ESET 遠端管理工具，透過一個中央位置在遠端電腦上來部署 ESET 解決方案、管理工作、強制執行[安全性原則](#)、監視系統狀態並快速回應問題或威脅。

ESET 遠端管理工具

ESET Endpoint Antivirus ESET PROTECT 或 ESET PROTECT Cloud 可以遠端管理。

- [ESET PROTECT](#) 簡介
- [ESET PROTECT Cloud](#) 簡介
- [ESET HUB](#) – 通往 ESET PROTECT 統一安全性平台的中心閘道。它為所有 ESET 平台模組提供集中身分、訂閱和使用管理。有關啟動產品的說明，請參閱 [ESET PROTECT 授權管理](#)。ESET HUB 會將 ESET Business Account 完全取代為 ESET MSP Administrator。
- [ESET Business Account](#) – ESET 商業產品的授權管理入口網站。有關啟動產品的指示，請參閱 [ESET PROTECT 授權管理](#)，或如需使用 ESET Business Account 的詳細資訊，請參閱 [ESET Business Account 線上說明](#)。如果您已經具有 ESET 發行的使用者名稱與密碼，而您想要將其轉換成授權金鑰，請參閱[轉換舊版授權憑證](#)一節。

其他安全性產品

- [ESET Inspect](#) – 完整的端點偵測與回應系統，其中包含下列功能：事件偵測、事件管理與回應、資料收集、危害偵測、異常偵測、行為偵測和原則違規的指示器。
- [ESET Endpoint Encryption](#) – 是完整的安全性應用程式，旨在保護您的待用和傳輸中的資料。使用 ESET Endpoint Encryption 您可以加密檔案、資料夾和電子郵件，或建立加密的虛擬磁碟、壓縮壓縮檔並包括用於保護檔案刪除安全的桌面碎紙機。

第三方遠端管理工具

- [遠端監視和管理 \(RMM\)](#)

最佳實務

- [將具有 ESET Endpoint Antivirus 的所有端點連接至 ESET PROTECT](#)
- 在已連線的用戶端電腦上保護[進階設定](#)來避免未經授權的修改
- 套用[建議的原則](#)來強制執行可用的安全性功能
- [最小化使用者介面](#) – 來減少或限制使用者與 ESET Endpoint Antivirus 的互動

使用說明指南

- [如何使用覆寫模式](#)
- [如何使用 GPO 或 SCCM 部署 ESET Endpoint Antivirus](#)

ESET PROTECT 簡介

ESET PROTECT 可讓您透過一個中央位置、在網路環境中的工作站、伺服器和行動裝置管理 ESET 產品。

您可以使用 ESET PROTECT Web 主控台，在遠端電腦上部署 ESET 解決方案、管理工作、強制執行[安全性原則](#)、監視系統狀態並快速回應問題或威脅。另請參閱[ESET PROTECT 架構與基礎架構元素概覽](#)、[開始使用 ESET PROTECT Web 主控台](#)，以及[支援的桌面佈建環境](#)。

ESET PROTECT 由以下元件組成：

- [ESET PROTECT 伺服器](#) – 它會處理與代理程式的通訊，以及收集應用程式資料並將其儲存在資料庫中。ESET PROTECT 伺服器可以安裝在 Windows 和 Linux 伺服器上，也可當作虛擬設備使用。
- [ESET PROTECT Web 主控台](#) - Web 主控台是可讓您在環境中管理用戶端電腦的主要介面。它會顯示您網路上用戶端的狀態概觀，並可讓您從遠端將 ESET 解決方案部署至未受管理的電腦。在安裝 ESET PROTECT 伺服器之後，您可以使用 Web 瀏覽器存取 Web 主控台。如果您選擇使 Web 伺服器可透過網際網路使用，則可以從任何具有網際網路連線的位置或裝置使用 ESET PROTECT。
- [ESET Management 代理程式](#) – 可提升 ESET PROTECT 伺服器和用戶端電腦之間的通訊。代理程式必須安裝在用戶端電腦上，才能在該電腦與 ESET PROTECT 伺服器之間建立通訊。ESET Management 代理程式位於用戶端電腦，能儲存多種安全情況，所以可以使對新威脅的反應時間大幅縮短。使用 ESET PROTECT Web 主控台，您可以將 [ESET Management 代理程式部署](#)至 Active Directory 或 ESET [RD Sensor](#) 所識別的未受管理電腦。如有必要，您也可以用戶端電腦上[手動安裝 ESET Management 代理程式](#)。
- [ESET Rogue Detection Sensor](#) – 能偵測出現在您網路上的未受管理電腦，並將這些電腦的資訊傳送至 ESET PROTECT 伺服器。這可讓您在 ESET PROTECT 中管理新用戶端電腦，而無需手動搜尋和新增它們。Rogue Detection Sensor 會記住已經發現的電腦，相同的資訊不會傳送兩次。
- [ESET Bridge](#) – 是一項服務，可搭配 ESET PROTECT 以：
 - 將更新散佈到用戶端電腦，並將安裝套件散佈到 ESET Management 代理程式。
 - 將通訊從 ESET Management 代理程式轉發到 ESET PROTECT 伺服器。
- [行動裝置連接器](#) – 是一種允許「行動裝置管理」與 ESET PROTECT 搭配的元件，可讓您管理行動裝置 (Android 和 iOS) 以及管理 ESET Endpoint Security for Android。
- [ESET PROTECT 虛擬設備](#) – 可供想在虛擬環境中執行 ESET PROTECT 的使用者使用。
- [ESET PROTECT Virtual Agent Host](#) – 是虛擬化代理程式實體，以管理無代理程式虛擬機器的 ESET PROTECT 元件。此解決方案能夠進行自動化、動態群組利用，以及與 ESET Management 代理程式在實體電腦上所執行時，相同層級的工作管理。虛擬代理程式會從虛擬機器收集資訊，並將它傳送至 ESET PROTECT 伺服器。
- [映像工具](#) – 需有映像工具才能進行離線模組更新。如果您的用戶端電腦沒有網際網路連線，您可以使用映像工具從 ESET 更新伺服器下載更新檔案並儲存在本機上。
- [ESET Remote Deployment Tool](#) – 用於部署在 <%PRODUCT%> Web 主控台中建立的全方位套件。這是一種透過網路，在電腦上發送 ESET Management 代理程式與 ESET 產品的便利方式。

 如需詳細資訊，請參閱 [ESET PROTECT 線上說明](#)。

ESET PROTECT Cloud 簡介

ESET PROTECT Cloud 可讓您從一個中央位置，管理網路環境中工作站和伺服器上的 ESET 產品，而不需具備 ESET PROTECT 或 的實體或虛擬伺服器。您可以使用 ESET PROTECT Cloud Web 主控台，部署 ESET 解決方案、管理工作、強制執行安全原則、監視系統狀態，以及快速回應遠端電腦上的問題或威脅。

ESET PROTECT Cloud 由以下元件組成：

- [ESET PROTECT Cloud 執行個體](#) – 它會處理與代理程式的通訊，以及收集應用程式資料並將其儲存在資料庫中。
- [ESET PROTECT Cloud Web 主控台](#) - Web 主控台是可讓您在環境中管理用戶端電腦的主要介面。它會顯示您網路上用戶端的狀態概觀，並可讓您從遠端將 ESET 解決方案部署至未受管理的電腦。您可以從任何具有網際網路連線的地方或裝置使用 ESET PROTECT Cloud。
- [ESET Management 代理程式](#) – 可提升 ESET PROTECT Cloud 和用戶端電腦之間的通訊。代理程式必須安裝在用戶端電腦上，才能在該電腦與 ESET PROTECT Cloud 之間建立通訊。ESET Management 代理程式位於用戶端電腦，能儲存多種安全情況，所以可以使對新威脅的反應時間大幅縮短。使用 ESET PROTECT Cloud Web 主控台，您可以將 [ESET Management 代理程式部署](#) 至未受管理電腦。如有必要，您也可以用戶端電腦上 [手動安裝 ESET Management 代理程式](#)。
- [ESET Bridge](#) – 是一項服務，可搭配 ESET PROTECT Cloud 以：
 - 將更新散佈到用戶端電腦，並將安裝套件散佈到 ESET Management 代理程式。
 - 將通訊從 ESET Management 代理程式轉送到 ESET PROTECT Cloud。
- [行動裝置管理](#) – 是一種允許「行動裝置管理」與 ESET PROTECT Cloud 搭配的元件，可讓您管理行動裝置 (Android 和 iOS) 以及管理 ESET Endpoint Security for Android。
- [弱點與修補程式管理](#) – ESET PROTECT Cloud 中提供的功能定期掃描工作站，以偵測任何可能容易遭到安全性風險感染的已安裝軟體。[修補程式管理](#) 透過自動軟體更新協助修復這些風險，使裝置更加安全。

i 如需詳細資訊，請參閱 [ESET PROTECT Cloud 線上說明](#)。

密碼保護的設定

若要為您的系統提供最高安全性，需要正確地配置 ESET Endpoint Antivirus。任何不合格的變更或設定可能導致用戶端安全性和防護層級的降低。若要限制使用者存取進階設定，管理員可用密碼保護設定。

管理員可以建立一個原則，以密碼保護已連線用戶端電腦上 ESET Endpoint Antivirus 的進階設定。若要建立新的原則，請執行下列動作：

1. 在 ESET PROTECT Web 主控台或，按一下左邊主功能表中的 **[原則]**。
2. 按一下 **[新增原則]**。
3. 命名新原則，並選擇性地給與簡短說明。按一下 **[繼續]** 按鈕。
4. 從產品清單中，選取 **[ESET Endpoint for Windows]**。
5. 按一下 **[設定]** 清單中的 **[使用者介面]**，並展開 **[存取設定]**。
6. 根據 ESET Endpoint Antivirus 的版本，按一下滑動軸以啟用 **[使用密碼保護設定]**。請注意 ESET Endpoint 第 7 版產品提供加強的防護。如果您在網路中同時具有 Endpoint 產品的第 7 版與第 6 版，建議您為每個版本建立兩個單獨的原則，並使用不同的密碼。
7. 在通知視窗中，建立新密碼、確認它，然後按一下 **[確定]**。按一下 **[繼續]**。
8. 將原則指派給用戶端。按一下 **[指派]**，並選取要以密碼保護的電腦或電腦群組。按一下 **[確定]** 以確認。
9. 檢查所有需要的用戶端電腦是否位於目標清單中，然後按一下 **[繼續]**。
10. 檢閱摘要中的原則設定，然後按一下 **[完成]** 來儲存您的新原則。

何謂原則？

管理員可以使用來自 ESET PROTECT Web 主控台的原則，將特定配置推送至用戶端電腦上執行的 ESET 產品。原則可以直接套用至個別電腦和電腦群組。您也可以將多個原則指派給一部電腦或一個群組。

使用者必須具有下列權限，才能建立新原則：**[讀取]** 權限用來讀取原則清單、**[使用]** 權限用來將原則指派給目標電腦，以及 **[寫入]** 權限用來建立、修改或編輯原則。

系統會依靜態群組的排列順序套用原則。對於動態群組，會先將原則套用至子動態群組。這可讓您套用對群組樹狀結構頂端產生更大影響的原則，並將更具體的原則套用至子群組。使用**旗標**，能夠存取樹狀結構中較高層級群組的 ESET Endpoint Antivirus 使用者，就可以覆寫較低層級群組的原則。此演算法會在 [ESET PROTECT 線上說明](#) 中加以說明。

i

我們建議您將較為一般的原則（例如，更新伺服器原則）指派給在群組樹狀結構內，位於較高層級的群組。更具體的原則（例如，裝置控制設定）應該在群組樹狀結構中的更深處指派。在合併時，較低層級的原則通常會覆寫較高層級原則的設定（除非使用**原則旗標**進行不同定義）。



合併原則

套用到用戶端的原則通常是合併成最終原則之多個原則的結果。策略被一一合併。在合併原則時，其一般規則是較新的原則會一律取代之前原則所設定的設定。若要變更此行為，您可以使用**原則旗標**（適用於每一個設定）。

建立原則時，您將注意到有些設定具有您可以配置的額外規則（取代/附加/前面加上）。

- **取代** – 整個清單可被取代、加入新值，以及移除所有先前的值。
- **附加** – 項目會新增至目前套用之清單的底端（必須是另一個原則，因為一律會覆寫本機清單）。
- **前面加上** – 項目會新增至清單的頂端（會覆寫本機清單）。

ESET Endpoint Antivirus 支援以新方式合併本機設定與遠端原則。如果設定是清單（例如，封鎖的網站清單）且遠端原則與現有的本機設定衝突，則遠端原則會覆寫現有本機設定。您可以對下列情況選取不同的合併規則，來選擇如何組合本機與遠端清單：




-  合併遠端原則的設定。
-  合併本機和遠端原則 – 本機設定與結果產生的遠端原則。

若要進一步瞭解合併原則，請遵循 [ESET PROTECT 線上使用者手冊](#) 並參閱**範例**。

旗標的運作方式

套用至用戶端電腦的原則通常是將合併成單一最終原則之多個原則的結果。合併原則時，由於套用原則的順序，您可以使用原則旗標來調整最終原則的預期行為。這些旗標定義原則將如何處理特定的設定。

對於每一個設定，您可以選取下列其中一個旗標：

 不套用	原則不會設定任何具有此旗標的設定。因為此設定不是由原則設定，所以稍後套用的其他原則可以變更它。
 套用	包含 [套用] 旗標的設定將套用至用戶端電腦。不過，當合併原則時，稍後套用的其他原則會覆寫它。當原則傳送至包含以此旗標標記之設定的用戶端電腦時，那些設定將變用戶端電腦的本機配置。因為未強制進行設定，所以稍後套用的其他原則仍可變更它。
 強制	包含 [強制] 旗標的設定具有優先權，而且稍後套用的任何原則都無法覆寫它們（即使其也具有 [強制] 旗標也一樣）。這確定稍後套用的其他原則無法在合併期間變更此設定。當原則傳送至包含以此旗標標記之設定的用戶端電腦時，那些設定將變用戶端電腦的本機配置。

案例管理員想要允許使用者 *John* 可在其家用群組中建立或編輯原則，並查看管理員建立的所有原則，包括具有 ⚡ [強制] 旗標的原則。管理員想要 *John* 能夠查看所有原則，但不能編輯管理員建立的現有原則。*John* 只能在其家用群組聖地牙哥內建立或編輯原則。

解決方案：管理員必須遵循下列步驟：

建立自訂靜態群組和權限集

1. 建立新的靜態群組，稱為聖地牙哥
2. 建立新的權限集（稱為原則 - 全部 *John*），其可以存取靜態群組全部，並具有 [原則] 的 [讀取] 權限。
3. 建立新的權限集（稱為原則 *John*），其可以存取靜態群組聖地牙哥，並具有 [群組與電腦] 及 [原則] 的功能存取 [寫入] 權限。此權限集允許 *John* 在其家用群組聖地牙哥中建立或編輯原則。
4. 建立新的使用者 *John*，並在 [權限集] 區段中，選取原則 - 全部 *John* 及原則 *John*

建立原則

5. 建立新的原則全部 - 啟用防火牆，展開 [設定] 區段、選取 [ESET Endpoint for Windows]，瀏覽至 [個人防火牆] > [基本]，然後透過 ⚡ [強制] 旗標套用所有設定。展開 [指派] 區段，並選取靜態群組全部
6. 建立新的原則 *John* 群組 - 啟用防火牆，展開 [設定] 區段、選取 [ESET Endpoint for Windows]，瀏覽至 [個人防火牆] > [基本]，然後透過 ● [套用] 旗標套用所有設定。展開 [指派] 區段，並選取靜態群組聖地牙哥

結果

首先將套用 *Administrator* 建立的原則，因為 ⚡ [強制] 旗標已套用至原則設定。套用強制旗標的設定具有優先權，而且稍後套用的原則無法覆寫它們。在管理員建立原則之後，將套用使用者 *John* 建立的原則。

若要查看最終原則順序，請瀏覽至 [其他] > [群組] > [聖地牙哥]。選取電腦並選取 [顯示詳細資料]。在 [配置] 區段中，按一下 [套用的原則]

安裝

除非您透過 [ESET PROTECT](#) 或 [ESET PROTECT Cloud](#) 在遠端將 ESET Endpoint Antivirus 佈署到用戶端工作站，否則在用戶端工作站上有數種 ESET Endpoint Antivirus 安裝方法。

i 您可以透過執行已安裝 ESET Endpoint Antivirus 的 ESET Endpoint Security 安裝程式從 ESET Endpoint Antivirus 升級到 ESET Endpoint Security。但是，您必須安裝相同或更高版本。

方法	目的	下載連結
使用 ESET AV Remover 安裝	ESET AV Remover 工具會協助您移除幾乎所有先前安裝在您系統上的防毒軟體，再繼續進行安裝。	下載 64-位元 下載 32-位元
*** 安裝 (.exe)	不使用 ESET AV Remover 的安裝程序。	下載 64-位元 下載 32-位元
安裝 (.msi)	.msi 安裝程式是商業環境中偏好的安裝套件。這主要是由使用 ESET PROTECT 等各種工具的離線和遠端佈署所致。	下載 64-位元 下載 32-位元
命令列安裝	ESET Endpoint Antivirus 您可使用命令列在本機安裝，或從 ESET PROTECT 使用用戶端工作進行遠端安裝。	N/A
使用 GPO 或 SCCM 進行部署	使用 GPO 或 SCCM 等管理工具，將 ESET Management Agent 和 ESET Endpoint Antivirus 部署到用戶端工作站。	N/A

方法	目的	下載連結
使用 RMM 工具部署	適用於遠端管理和監視 (RMM) 的 ESET DEM 外掛程式工具可讓您將 ESET Endpoint Antivirus 部署至用戶端工作站。	N/A

ESET Endpoint Antivirus [提供 30 個以上的語言](#)

使用 ESET AV Remover 安裝

在您繼續安裝程序前，請務必解除安裝電腦上任何現有的安全性應用程式。請選取 **「我要使用 ESET AV Remover 解除安裝不需要的防毒應用程式」** 旁邊的核取方塊，讓 ESET AV Remover 掃描您的系統並移除任何 [支援的安全性應用程式](#)。保持核取方塊未選取並按一下 **「繼續」** 以安裝 ESET Endpoint Antivirus 而不執行 ESET AV Remover。



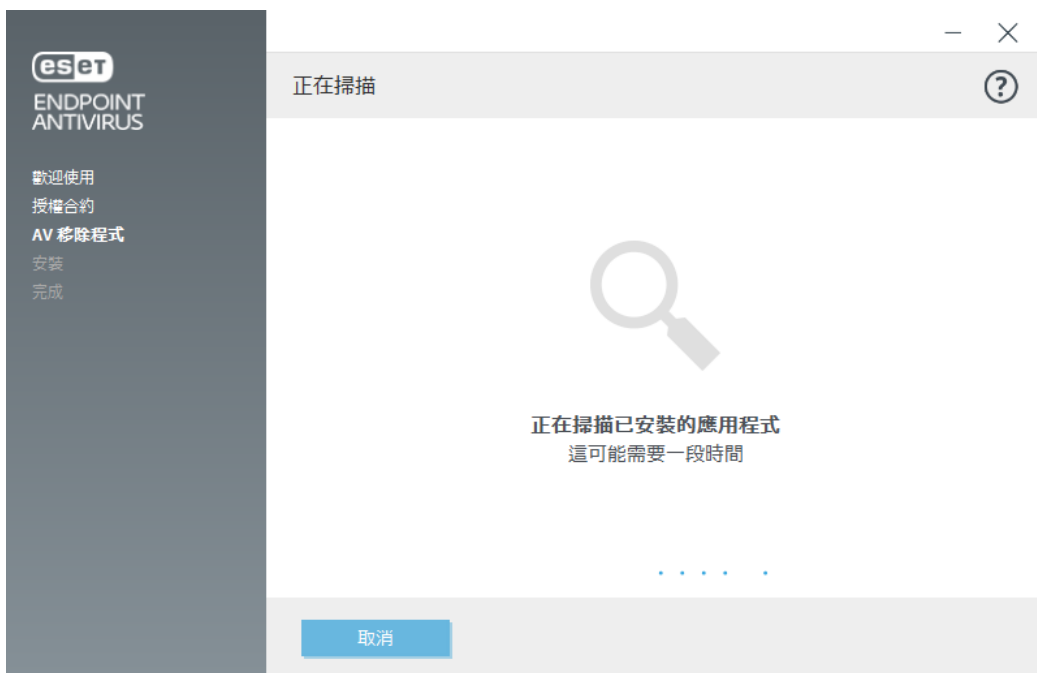
ESET AV Remover

ESET AV Remover 工具會協助您移除幾乎所有先前安裝在在您的系統上的防毒軟體。請遵循下列指示以使用 ESET AV Remover 移除現有防毒程式：

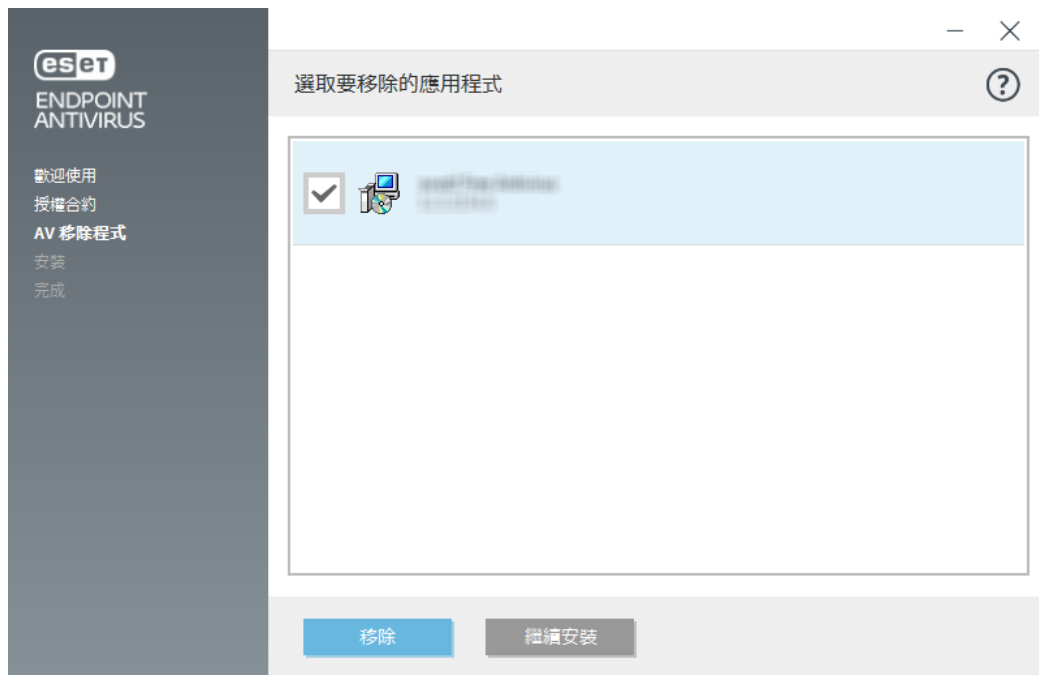
- 若要檢視 ESET AV Remover 可移除的防毒軟體清單，[請造訪 ESET 資料庫文章](#)
- 請閱讀使用者授權合約，並按一下 **「接受」** 以確認您接受此合約。按一下 **「拒絕」** 將繼續安裝 ESET Endpoint Antivirus 而不移除電腦上現有的安全性應用程式。



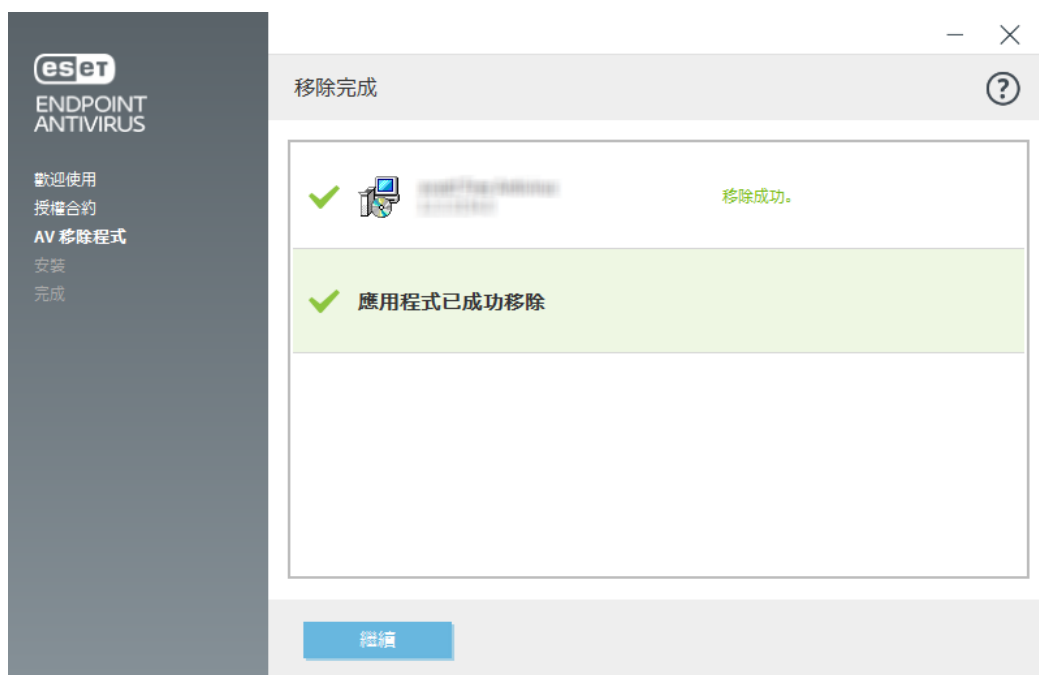
2. ESET AV Remover 將開始搜尋您系統中的防毒軟體。



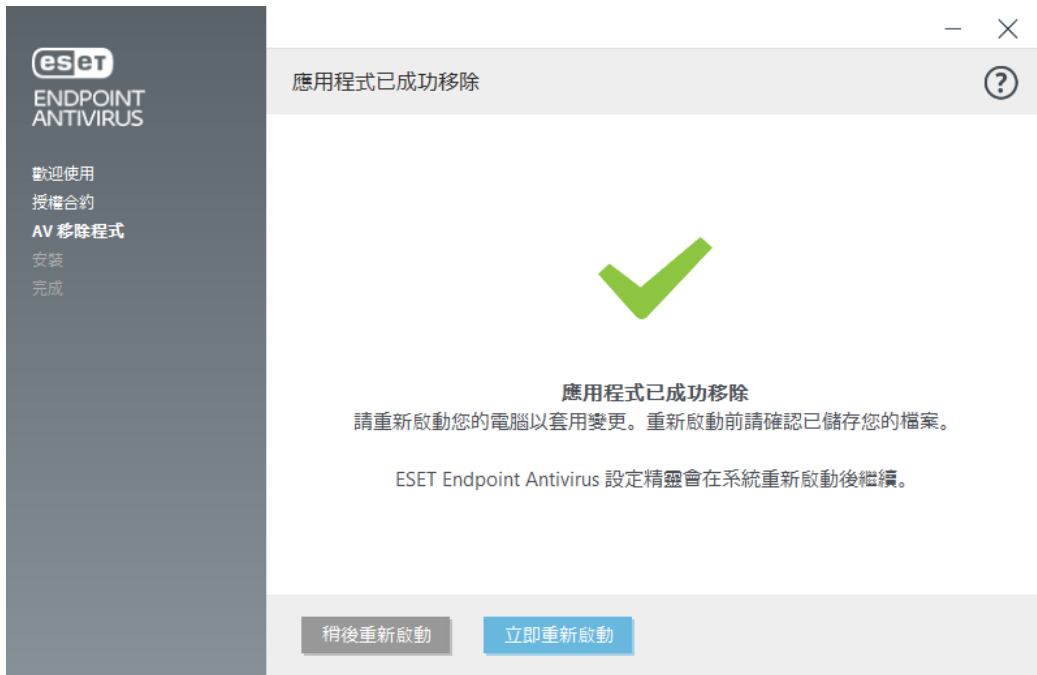
2. 選取任何列出的防毒應用程式，並按一下 [移除]。移除可能需要一段時間。



2. 移除成功後，請按一下 **[繼續]**。



6. 請重新啟動您的電腦以套用變更並繼續安裝 ESET Endpoint Antivirus。如果解除安裝不成功，請參閱這份指南中的[使用 ESET AV Remover 解除安裝結束時發生錯誤](#)一節。



使用 ESET AV Remover 解除安裝結束時發生錯誤

若您無法使用 ESET AV Remover 移除防毒程式，您將收到通知，顯示 ESET AV Remover 可能不支援您嘗試移除的應用程式。請造訪 ESET 知識庫上的[支援的產品清單](#)或[一般 Windows 防毒軟體的解除安裝程式](#)，了解此特定程式是否可移除。

若解除安裝安全性產品不成功，或某些元件僅部分解除安裝，系統將提示您 **[重新啟動並重新掃描]**。請在啟動後確認 UAC 並繼續掃描及解除安裝程序。

必要時請連絡 [ESET 技術支援](#) 以開啟支援要求，並提供 **AppRemover.log** 檔案以協助 ESET 技術人員。**AppRemover.log** 檔案位於 **eset** 資料夾。瀏覽至 Windows 檔案總管中的 **%TEMP%** 以存取此資料夾。ESET 技術支援將盡快回覆以協助解決您的問題。

安裝 (.exe)

一旦啟動 .exe 安裝程式，安裝精靈將引導您進行安裝程序。



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



1. 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](#)
- [潛在不需要應用程式偵測](#)

i 按一下 [繼續] 或 [全部允許並繼續]，即表示您接受使用者授權合約，並瞭解隱私權政策。您可以按一下[變更安裝資料夾](#)來將 ESET Endpoint Antivirus 安裝到指定的資料夾。



2. 完成之後，系統將提示您[啟動 ESET Endpoint Antivirus](#)

變更安裝資料夾 (.exe)

您可以在安裝期間 [變更安裝資料夾]。為 ESET Endpoint Antivirus 安裝選取一個位置。依預設，程式會安裝至以下目錄：

`C:\Program Files\ESET\ESET Security\`

您可以指定程式模組和資料的位置。依預設，這些內容會分別安裝至以下目錄：

`C:\Program Files\ESET\ESET Security\Modules\`

`C:\ProgramData\ESET\ESET Security\`

按一下 [瀏覽] 即可變更這些位置（不建議）。

按一下 [上一步]，然後繼續進行安裝程序。

安裝 (.msi)

一旦啟動 .msi 安裝程式，安裝精靈將引導您進行安裝程序。

✓ .msi 安裝程式是商業環境中偏好的安裝套件。這主要是由使用 ESET PROTECT 等各種工具的離線和遠端佈署所致。

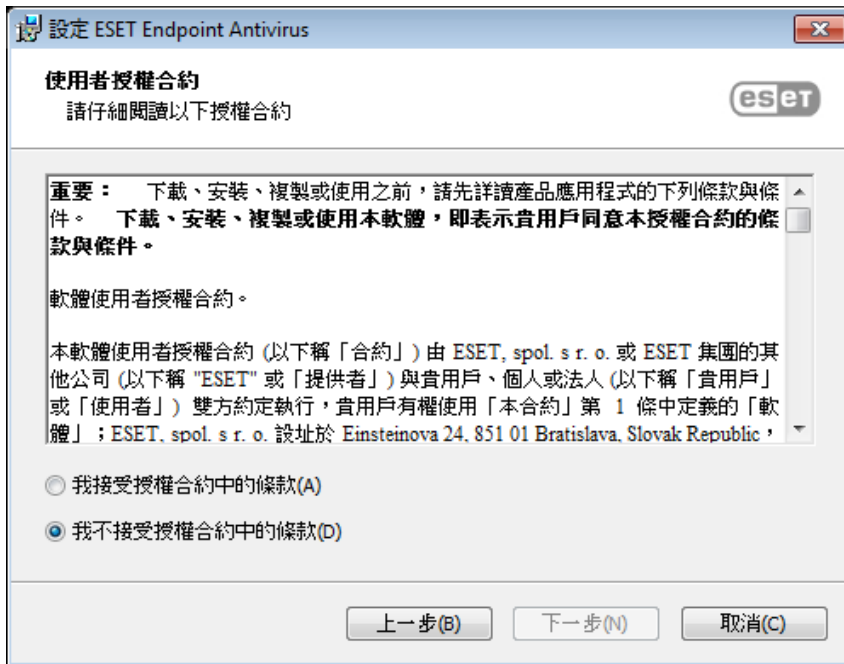
⚠ 請確定電腦上未安裝任何其他防毒程式。如果在單一電腦上安裝兩個或兩個以上的防毒解決方案，會造成彼此衝突。我們建議您解除安裝系統上的任何其他防毒程式。請參閱[知識庫文章](#)以取得一般防毒軟體的解除安裝程式工具清單（提供英文與其他語言版本）。

i 在 ESET PROTECT 中建立的 ESET Endpoint Antivirus 安裝程式支援 Windows 10 Enterprise for Virtual Desktops 和 Windows 10 多重工作階段模式。

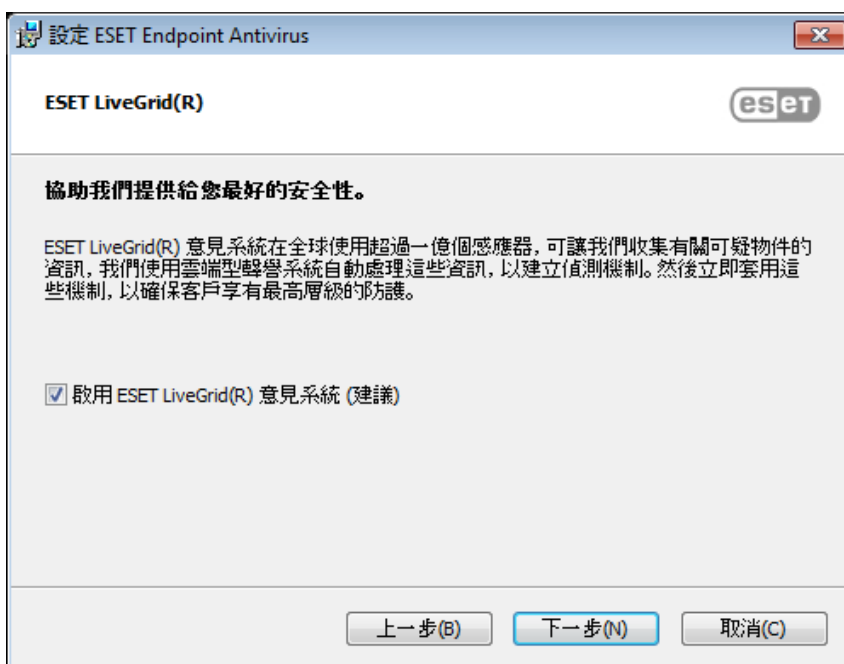
1. 選取想要的語言，並按一下 [下一步]。



2. 閱讀「使用者授權合約」，並按一下 [我接受授權合約中的條款] 以認知您已接受使用者授權合約。在接受條款後按 [下一步]，便能繼續安裝程序。



3. 選取您偏好的 [ESET LiveGrid® 意見系統](#)。ESET LiveGrid® 可協助確保 ESET 立即並持續地接收新入侵的相關資訊通知，讓我們為客戶提供更強大的保護。此系統允許您將新威脅提交到 ESET 病毒實驗室，並對其進行分析、處理及新增到偵測引擎。按一下 **[進階設定]** 以 [配置其他安裝參數](#)。



4. 最後一步是按一下 **[安裝]** 來確認安裝。完成之後，系統將提示您 [啟動 ESET Endpoint Antivirus](#)。

進階安裝 (.msi)

進階安裝可讓您自訂在執行一般安裝時無法使用的安裝參數。

1. 您可以在安裝期間 **[變更安裝資料夾]**。為 ESET Endpoint Antivirus 安裝選取一個位置。依預設，程式會安裝至以下目錄：

`C:\Program Files\ESET\ESET Security\`

您可以指定程式模組和資料的位置。依預設，這些內容會分別安裝至以下目錄：

C:\Program Files\ESET\ESET Security\Modules\
C:\ProgramData\ESET\ESET Security\

按一下 **[瀏覽]** 即可變更這些位置（不建議）。

2. 選擇要安裝哪一個產品元件。您可以選取 [電腦掃描](#) 和所有可用 [防護](#) 的喜好設定。[更新映像](#) 元件可讓您用來更新網路上的其他電腦。[遠端監視和管理 \(RMM\)](#) 是監督和控制軟體系統的程序，其使用管理服務提供者可以存取的本機安裝代理程式來運作。
3. 按一下 **[安裝]** 以啟動安裝程序。

最小模組安裝

若為減少與安裝程式大小相關的網路流量並節省資源，ESET 隨附最小模組安裝程式。安裝程式僅包含基本模組，所有其他模組將在產品啟用之後的初始模組更新期間下載。主要優點是安裝程式明顯更小，並且在您使用授權金鑰啟動產品時，ESET Endpoint Antivirus 僅會下載最新的應用程式模組。

最小模組安裝程式仍包含下列模組：

- 載入器
- Direct Cloud 通訊
- 轉譯支援
- 配置
- SSL

產品啟用之後，您將看到 **正在初始化防護** 狀態，它將通知您功能初始化的相關資訊。



如果模組下載出現問題（例如 Proxy 設定、無網路等），則會顯示 **需要注意** 警告應用程式狀態。在主要程式視窗中，按一下 **[更新]** > **[檢查更新]**，再次開始程序。



在幾次嘗試不成功之後，會顯示 **防護設定失敗** 紅色應用程式狀態。按一下 **[重試]** 以再次啟動防護設定。如果初始化過程失敗，並且一樣無法下載模組，請在此處 [下載完整 MSI 安裝程式](#)。



如果您的用戶端電腦沒有網際網路連線或離線工作，並且需要更新，請使用下列方法從 ESET 更新伺服器下載更新檔案：

- [從映像更新](#)
- [使用映像工具](#)

命令列安裝

您可以在本機使用命令列來安裝 ESET Endpoint Antivirus 或遠端使用 ESET PROTECT 中的用戶端工作來進行安裝。

受支援的參數

APPDIR=<path>

- 路徑 – 有效的目錄路徑
- 應用程式安裝目錄。

APPDATADIR=<path>

- 路徑 - 有效的目錄路徑
- 應用程式資料安裝目錄。

MODULEDIR=<path>

- 路徑 - 有效的目錄路徑
- 模組安裝目錄。

ADDLOCAL=<list>

- 元件安裝 - 待安裝在本機上的非必要功能清單。
- 使用 ESET .msi 套件: `ees_nt64_ENU.msi /qn ADDLOCAL=<list>`
- 如需有關 **ADDLOCAL** 屬性的詳細資訊，請參閱 <http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx>

ADDEXCLUDE=<list>

- ADDEXCLUDE 是以逗號分隔的清單，列出所有沒有要安裝的功能名稱，作為過時 REMOVE 的取代。
- 選取沒有要安裝的功能時，必須在清單中明確包含整個路徑（例如，所有其子功能）和相關的隱藏功能。
- 使用 ESET .msi 套件: `ees_nt64_enu.msi /qn ADDEXCLUDE=Firewall,Network`

i 您無法將 **ADDEXCLUDE** 與 **ADDLOCAL** 搭配使用。

請參閱[文件](#)來了解用於適當命令列切換的 **msiexec** 版本。

規則

- **ADDLOCAL** 清單是以逗號分隔的清單，列出所有要安裝的功能名稱。
- 選擇要安裝的功能時，清單上必須明確包含整個路徑（所有上層功能）。
- 請參閱其他規則，以便正確使用此功能。

元件和功能

i 使用 ADDLOCAL/ADDEXCLUDE 參數的元件安裝不適用於 ESET Endpoint Antivirus[®]

這些功能分成 4 種類別：

- **必要** - 一律會安裝這類功能。
- **選用** - 可以取消選取這類功能，因此不會進行安裝。
- **隱藏** - 其他功能正常運作所必須的邏輯功能
- **版面配置區** - 對產品沒有影響的功能，但必須列為子功能

ESET Endpoint Antivirus 的功能集如下：

說明	功能名稱	家長功能	存在
基本程式元件	Computer		版面配置區
偵側引擎	Antivirus	Computer	必要

說明	功能名稱	家長功能	存在
偵測引擎/惡意軟體掃描	Scan	Computer	必要
偵測引擎/即時檔案系統防護	RealtimeProtection	Computer	必要
偵測引擎/惡意軟體掃描/文件防護	DocumentProtection	Antivirus	選用
裝置控制	DeviceControl	Computer	選用
網路防護	Network		版面配置區
網路防護/防火牆	Firewall	Network	選用
網路防護/網路攻擊防護/...	IdsAndBotnetProtection	Network	選用
安全的瀏覽器	OnlinePaymentProtection	WebAndEmail	選用
Web 和電子郵件	WebAndEmail		版面配置區
Web 和電子郵件/通訊協定篩選	ProtocolFiltering	WebAndEmail	隱藏
Web 和電子郵件/Web 存取防護	WebAccessProtection	WebAndEmail	選用
Web 和電子郵件/電子郵件用戶端防護	EmailClientProtection	WebAndEmail	選用
Web 和電子郵件/電子郵件用戶端防護/電子郵件用戶端	MailPlugins	EmailClientProtection	隱藏
Web 和電子郵件/電子郵件用戶端防護/電子郵件用戶端反垃圾郵件	Antispam	EmailClientProtection	選用
Web 和電子郵件/Web 控制	WebControl	WebAndEmail	選用
工具/ESET RMM	Rmm		選用
更新/設定檔/更新映像	UpdateMirror		選用
ESET Inspect 外掛程式	EnterpriseInspector		隱藏

群組功能集：

說明	功能名稱	功能的存在
所有必要功能	_Base	隱藏
所有可用功能	ALL	隱藏

其他規則

- 如果選取任何 **WebAndEmail** 功能來進行安裝，必須將隱藏 **ProtocolFiltering** 功能包含在清單中。
- 所有功能的名稱都區分大小寫，例如 `UpdateMirror` 不等於 `UPDATEMIRROR`

配置屬性的清單

屬性	值	功能
CFG_POTENTIALLYUNWANTED_ENABLED=	0 – 已停用 1 – 已啟用	PUA 偵測
CFG_LIVEGRID_ENABLED=	如下所示	請參閱 以下 LiveGrid 屬性
FIRSTSCAN_ENABLE=	0 – 已停用 1 – 已啟用	安排安裝後的 電腦掃描時間並加以執行

屬性	值	功能
CFG_PROXY_ENABLED=	0 - 已停用 1 - 已啟用	Proxy 伺服器設定
CFG_PROXY_ADDRESS=	<ip>	Proxy 伺服器 IP 地址
CFG_PROXY_PORT=	<port>	Proxy 伺服器連接埠號碼
CFG_PROXY_USERNAME=	<username>	驗證的使用者名稱
CFG_PROXY_PASSWORD=	<password>	驗證的密碼
ACTIVATION_DATA=	如下所示	產品啟用、授權金鑰或離線授權檔案
ACTIVATION_DLG_SUPPRESS=	0 - 已停用 1 - 已啟用	設為「1」時，在第一次啟動後沒有顯示產品啟用對話方塊
ADMINCFG=	<path>	已匯出 XML 配置 的路徑 (預設值 <i>cfg.xml</i>)

LiveGrid® 屬性

利用 CFG_LIVEGRID_ENABLED 安裝 ESET Endpoint Antivirus 時，安裝後的產品行為會是：

功能	CFG_LIVEGRID_ENABLED=0	CFG_LIVEGRID_ENABLED=1
ESET LiveGrid® 聲譽系統	開啟	開啟
ESET LiveGrid® 意見系統	關閉	開啟
提交匿名統計	關閉	開啟

ACTIVATION_DATA 屬性

格式	方法
ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE	使用 ESET 授權金鑰來啟動 (應啟動網際網路連線)
ACTIVATION_DATA=offline:C:\ProgramData\ESET\ESET Security\license.lf	使用離線授權檔案來啟動

語言屬性

ESET Endpoint Antivirus 語言 (您必須指定兩種屬性)。

屬性	值
PRODUCT_LANG=	LCID 小數 (地區設定 ID) 例如，英文 (美國) 是 1033。請參閱 語言代碼清單
PRODUCT_LANG_CODE=	小寫 LCID 字串 (語言文化名稱)，例如，英文 - 美國是 en-us 請參閱 語言代碼清單

重新啟動屬性

指定以下參數以在安裝後重新啟動電腦：

屬性	值	功能
REBOOT_WHEN_NEEDED=	0 - 已停用 1 - 已啟用	如果啟用，電腦將在安裝後重新啟動。

屬性	值	功能
REBOOT_CANCELABLE=	0 - 已停用 1 - 已啟用	如果啟用，使用者可以取消電腦重新啟動。
REBOOT_POSTPONE=	值（以秒為單位）	使用者延後電腦重新啟動的最長時間（秒）。

i REBOOT_CANCELABLE 和 REBOOT_POSTPONE 僅在啟用 REBOOT_WHEN_NEEDED 時可用。

命令列安裝範例

! 確保您閱讀[使用者授權合約](#)並在執行安裝前具備管理權限。

✓ 將 **NetworkProtection** 區段從此安裝中排除（您也必須指定所有子功能）：
`msiexec /qn /i ees_nt64.msi ADDEXCLUDE=Network,Firewall,IdsAndBotnetProtection`

如果您想要在安裝後自動配置 ESET Endpoint Antivirus[®]，您可以在安裝命令中指定基本配置參數。
 ✓ 在 ESET LiveGrid[®] 啟用的情形下安裝 ESET Endpoint Antivirus[®]
`msiexec /qn /i ees_nt64.msi CFG_LIVEGRID_ENABLED=1`

✓ 安裝至非預設值的不同應用程式安裝目錄。
`msiexec /qn /i ees_nt64_enu.msi APPDIR=C:\ESET\`

✓ 使用 ESET 授權金鑰安裝和啟動 ESET Endpoint Antivirus[®]
`msiexec /qn /i ees_nt64_enu.msi ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE`

✓ 使用詳細記錄（可用於疑難排解）以及僅使用包含必要元件的 RMM 來進行無訊息安裝：
`msiexec /qn /i ees_nt64.msi /l*xv msi.log ADDLOCAL=_Base,Rmm`

✓ 使用[指定語言](#)強制執行無訊息完整安裝。
`msiexec /qn /i ees_nt64.msi ADDLOCAL=ALL PRODUCT_LANG=1033 PRODUCT_LANG_CODE=en-us`

安裝後命令列選項

- [ESET CMD](#) - 匯入 .xml 配置檔或開啟/關閉安全性功能
- [命令列掃描器](#) - 透過命令列執行電腦掃描

使用 GPO 或 SCCM 進行部署

除了在[用戶端工作站直接安裝 ESET Endpoint Antivirus](#)，您也可以使用群組原則物件 (GPO)[®]Software Center Configuration Manager (SCCM)[®]Symantec Altiris 或 Puppet 之類的管理工具來進行安裝。

受管理（建議）

對於受管理的電腦，我們會先安裝 ESET Management 代理程式，然後透過 ESET PROTECT 部署 ESET Endpoint Antivirus[®]必須將 ESET PROTECT 安裝在您的網路中。

1. 下載 ESET Management 代理程式的[獨立安裝程式](#)[®]
2. [準備 GPO/SCCM 遠端部署指令碼](#)[®]
3. 使用 GPO 或 SCCM 部署 ESET Management 代理程式。
4. 確保已將[用戶端電腦](#)新增至 ESET PROTECT[®]
5. 將 [ESET Endpoint Antivirus](#) 部署至您的用戶端電腦並加以啟動[®]

下列 ESET 知識庫文章可能僅以英文提供：

- [透過 SCCM 或 GPO 部署 ESET Management Agent](#)
- [使用群組原則物件 \(GPO\) 部署 ESET Management Agent](#)

未受管理的

對於未受管理的電腦，您可以將 ESET Endpoint Antivirus 直接部署到用戶端工作站。我們不建議這麼做，因為您將無法在工作站上為所有 ESET 端點產品監視和強制實施原則。

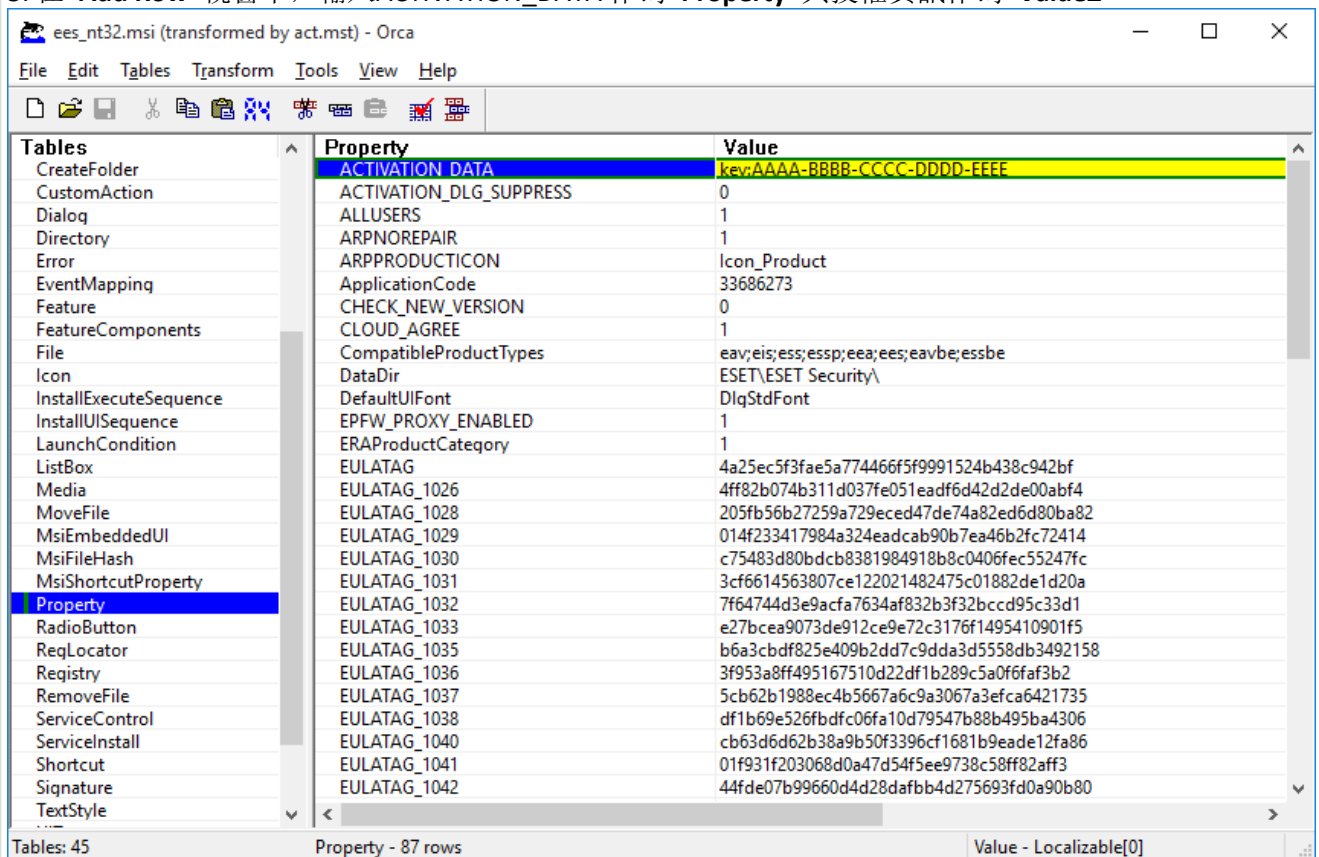
依預設，安裝後不會啟動 ESET Endpoint Antivirus，因此此產品不會運作。

選項 1（軟體安裝）

1. [下載 ESET Endpoint Antivirus 的 .msi 安裝程式](#)
2. 透過 .msi 檔案（例如，藉由使用 Orca .msi 編輯器）建立 .mst 轉換套件來包含產品啟用屬性（請參閱 [命令列安裝](#) 中的 ACTIVATION_DATA）

 [顯示在 Orca 中建立 .mst 的步驟](#)

1. 開啟 Orca
2. 透過按一下 **File > Open** 來載入 .msi 安裝程式。
3. 按一下 **Transform > New Transform**
4. 在 **Tables** 區段中按一下 **Property**，然後在功能表中按一下 **Tables > Add row**
5. 在 **Add Row** 視窗中，輸入 ACTIVATION_DATA 作為 **Property** 與授權資訊作為 **Value**



The screenshot shows the Orca .msi editor window titled "ees_nt32.msi (transformed by act.mst) - Orca". The "Tables" pane on the left has "Property" selected. The main table has two columns: "Property" and "Value". The first row is highlighted in yellow.

Property	Value
ACTIVATION_DATA	key:AAAA-BBBB-CCCC-DDDD-EEEE
ACTIVATION_DLG_SUPPRESS	0
ALLUSERS	1
ARPNOREPAIR	1
ARPPRODUCTICON	Icon_Product
ApplicationCode	33686273
CHECK_NEW_VERSION	0
CLOUD_AGREE	1
CompatibleProductTypes	eav;eis;ess;essp;eea;ees;eavbe;essbe
DataDir	ESET\ESET Security\
DefaultUIFont	DlgStdFont
EPFW_PROXY_ENABLED	1
ERAPProductCategory	1
EULATAG	4a25ec5f3fae5a774466f5f9991524b438c942bf
EULATAG_1026	4ff82b074b311d037fe051eadf6d42d2de00abf4
EULATAG_1028	205fb56b27259a729eced47de74a82ed6d80ba82
EULATAG_1029	014f233417984a324eadcab90b7ea46b2fc72414
EULATAG_1030	c75483d80bdc8381984918b8c0406fec55247fc
EULATAG_1031	3cf6614563807ce122021482475c01882de1d20a
EULATAG_1032	7f64744d3e9acfa7634af832b3f32bccd95c33d1
EULATAG_1033	e27bcea9073de912ce9e72c3176f1495410901f5
EULATAG_1035	b6a3cbdf825e409b2dd7c9dda3d5558db3492158
EULATAG_1036	3f953a8ff495167510d22df1b289c5a0f6faf3b2
EULATAG_1037	5cb62b1988ec4b5667a6c9a3067a3efca6421735
EULATAG_1038	df1b69e526fbd0c06fa10d79547b88b495ba4306
EULATAG_1040	cb63d6d62b38a9b50f3396cf1681b9eade12fa86
EULATAG_1041	01f931f203068d0a47d54f5ee9738c58ff82aff3
EULATAG_1042	44fde07b99660d4d28dafbb4d275693fd0a90b80

At the bottom, it says "Tables: 45" and "Property - 87 rows". The status bar shows "Value - Localizable[0]".

6. 按一下 **[轉換] > [產生轉換]** 來儲存 .mst 檔案。

1. 選用：若要匯入自訂的 ESET Endpoint Antivirus .xml 配置檔（例如，若要啟用 RMM 或配置 Proxy 伺服器設定），請將 cfg.xml 檔案放在與 .msi 安裝程式相同的位置。

2. 遠端使用 GPO (透過軟體安裝) 或 SCCM - 搭配 .mst 檔案來部署 .msi 安裝程式。

選項 2 (使用已排程的工作)

1. [下載 ESET Endpoint Antivirus 的 .msi 安裝程式](#)
2. 準備[命令列安裝](#)指令碼來包含產品啟用屬性 (請參閱 ACTIVATION_DATA)
3. 讓 .msi 安裝程式 .cmd 程式碼可在網路中供所有工作站使用。
4. 選用: 若要[匯入](#)自訂的 ESET Endpoint Antivirus .xml 配置檔 (例如, 若要啟用 RMM 或配置 Proxy 伺服器設定), 請將 cfg.xml 檔案放在與 .msi 安裝程式相同的位置。
5. 使用 GPO 或 SCCM 來套用準備好的命令列安裝指令碼。
 - 若是 GPO 使用 [群組原則喜好設定] > [群組原則已排程的工作] > [立即工作]



如果您不想要使用 ESET PROTECT 來遠端管理 ESET 端點產品, ESET Endpoint Antivirus 包含的 RMM ESET 外掛程式可讓您使用在本機安裝的代理程式來監督和控制軟體系統, 而管理服務提供者可存取在本機安裝的代理程式。[尋找更多資訊](#)

升級至最新版本

新推出的 ESET Endpoint Antivirus 版本已改善或修正自動程式模組更新無法解決的問題。

透過以下幾種方式即可升級為最新版本:

1. 使用 ESET PROTECT, 或 ESET PROTECT Cloud 自動升級。
2. 自動[使用 GPO 或 SCCM](#)
3. 自動地使用程式更新。

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, 以確保所有可能的系統配置的功能。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。

請確定您已經啟用 [進階設定] > [更新] > [設定檔] > [產品更新] 中的 [更新模式]
4. 透過下載並[安裝較新版本](#)覆蓋舊版的方式手動升級。

建議升級情況

我遠端管理, 或是希望遠端管理我的 ESET 產品

如果您管理超過 10 個 ESET Endpoint 產品, 可考慮使用 ESET PROTECT 或 ESET PROTECT Cloud 處理升級。請參閱以下文件:

- [ESET PROTECT | 透過用戶端工作升級 ESET 軟體](#)
- [ESET PROTECT | 適用於最多管理 250 個 Windows ESET 端點產品的中小型企業指南](#)
- [ESET PROTECT Cloud 簡介](#)

在用戶端工作站上手動升級

若要在個別用戶端工作站上手動升級 ESET Endpoint Antivirus

1. 驗證[您目前安裝的版本是否受到支援](#)
2. 確認您的作業系統[受支援](#)
2. 下載[最新版本並](#)以覆蓋舊版的方式進行安裝。

對於具有「終止支援」支援層級的版本，無法保證可對舊版本成功安裝為最新版本。參閱[終止支援原則](#)以檢閱 ESET Endpoint Antivirus 支援層級。

若要從不受支援的版本升級，請先解除安裝您的 ESET Endpoint Antivirus®。如需在用戶端工作stations升級 ESET Endpoint Antivirus 相關的其他資訊，請閱讀下列 [ESET 知識庫文章](#)。

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

i 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 產品有效授權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](#)，或者如果您不想參加，請按一下 **[繼續]**。
3. 使用授權金鑰啟動新的 ESET 產品後，將顯示首頁。如果未找到授權資訊，您將繼續使用新試用授權。如果先前產品使用的授權無效，請[啟動您的 ESET 產品](#)。
4. 需要重新啟動裝置才能完成安裝。

安全性和穩定性更新

更新 ESET Endpoint Antivirus 是保持全面防範惡意程式碼的重要環節。每個 ESET Endpoint Antivirus 新版本都有諸多功能改善和錯誤修復。我們強烈建議定期更新 ESET Endpoint Antivirus®以防止出現安全性弱點和威脅。ESET Endpoint Antivirus 如同其他 ESET 產品，適用於產品生命週期的特定階段。

閱讀更多相關資訊：

[生命週期結束原則（商業產品）](#)

i [產品更新](#)

[安全性和穩定性 Hotfix](#)

如需 ESET Endpoint Antivirus 變更的其他資訊，請閱讀下列 [ESET 知識庫文章](#)。

! 自動更新將確保您的產品具有最大的安全性和穩定性。您無法停用安全性和穩定性更新。

產品啟動

安裝完成之後，系統將提示您啟動您的產品。

有數個方法可啟動您的產品。啟動視窗中可使用的特定啟動狀況會視國家及發行方法（ESET 網頁、安裝程式類型 .msi 或 .exe 等）而異。

您可以在 [\[主程式視窗\]](#) > [\[說明及支援\]](#) > [\[啟動產品\]](#) 或 [\[防護狀態\]](#) > [\[啟動產品\]](#) 中啟動 ESET Endpoint Antivirus®。


您也可以使用下列任何一種方法來啟動 ESET Endpoint Antivirus®。

- **使用購買的授權金鑰** - 採用格式 XXXX-XXXX-XXXX-XXXX-XXXX 的唯一字串，可供您用來識別授權擁有者和授權的啟動。
- **ESET HUB** - 您必須建立的 [ESET HUB 帳戶](#)。ESET HUB 是至 ESET PROTECT 統一安全性平台的中心閘道。它為所有 ESET 平台模組提供集中身分、訂閱和使用者管理。您也可以使用此選項，使用較舊的授權管理工具：[ESET Business Account](#) 或 [ESET MSP Administrator](#) 啟動 ESET Endpoint Antivirus。
- **離線授權** - 自動產生的檔案，其將傳輸到 ESET 產品以提供授權資訊。如果授權允許您下載離線授權檔案 (.If) 則該檔案可用來執行離線啟動。離線授權的數量將會從可用授權的總數中減去。如需產生離線檔案的相關詳細資料，請參閱 [ESET Business Account 使用者指南](#)。

如果您的電腦是受管理網路的成員，而且您的管理員將透過 ESET PROTECT 執行遠端啟動，請按一下 **[稍後啟動]**。如果您想要稍後再啟動此用戶端，也可以使用此選項。

如果您有用於啟動舊版 ESET 產品的使用者名稱與密碼，[請將您的舊版憑證轉換為授權金鑰](#)。

您可以隨時在 [主程式視窗](#) > **[說明及支援]** > **[變更授權]** 中變更您的產品授權。您將會看到用於識別您 ESET 支援授權的公用授權 ID。

 ESET PROTECT 可透過管理員提供的授權，默默地啟動用戶端電腦。有關說明，請參閱 [ESET PROTECT 線上說明](#)。

 [產品啟用失敗？](#)

在啟動期間輸入您的授權金鑰

自動更新對您的安全性而言相當重要。只有在使用您的**授權金鑰**啟動 ESET Endpoint Antivirus 後，才能收到更新。

如果在安裝完成後仍未輸入您的授權金鑰，您的產品將不會啟動。您可以在主要程式視窗中變更您的授權。若要這樣做，請按一下 **[說明及支援]** > **[啟動授權]**，然後將您所收到的隨附於 ESET 安全性產品之授權資料輸入到 **[產品啟動]** 視窗中。

當您輸入**授權金鑰**時，請務必照實輸入：

- 您的授權金鑰是採用格式 XXXX-XXXX-XXXX-XXXX-XXXX 的唯一字串，可供您用來識別授權擁有者和授權的啟動。

我們建議您從您的註冊電子郵件中複製並貼上授權金鑰以確保正確無誤。

ESET HUB 帳戶

ESET HUB 是至 ESET PROTECT 統一安全性平台的中心閘道。它為所有 ESET 平台模組提供集中身分、訂閱和使用者管理。使用 ESET HUB 您可以：

- 取得安全性訂閱概觀
- 檢查已訂閱服務的使用方式和狀態
- 配置和控制對各個 ESET 平台的細微存取
- 所有連結和可存取 ESET 平台的單一登入

您也可以使用此啟動選項，使用較舊的授權管理工具：[ESET Business Account](#) 或 [ESET MSP Administrator](#) 啟動 ESET Endpoint Antivirus。

您可以[建立 ESET HUB 帳戶](#)並使用您的 [電子郵件位址] 和 [密碼] 登入。

若您忘記自己的密碼，請按一下 [我忘記密碼]，然後系統會將您重新導向到 ESET HUB。請輸入您的電子郵件地址，並按一下 [登入] 以確認。接下來，您將收到一封指示如何重設密碼的郵件。

如何使用舊版授權憑證來啟動 ESET 端點產品

如果您已經有 [使用者名稱] 和 [密碼] 並且想要接收 [授權金鑰]，請造訪 [ESET Business Account 入口網站](#)，您可以在其中轉換憑證至新的授權金鑰。

啟動失敗

如果啟動 ESET Endpoint Antivirus 不成功，最常見的情況為：

- 授權金鑰已在使用中
- 您已輸入無效的授權金鑰。
- 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

確定您已輸入正確的 [授權金鑰] 或已附加 [離線授權]，並嘗試再次啟動。

如果您無法啟動，我們的歡迎使用套件會帶您逐步了解啟動和授權的常見問題、錯誤與問題（提供英文與其他語言）。

- [開始 ESET 產品啟用疑難排解](#)

註冊

請填妥註冊表格中的包含欄位，並按一下 [繼續] 來註冊您的授權。用括號標示必要的是必填欄位。此資訊僅用於與您 ESET 授權相關的事宜。

啟動進度

ESET Endpoint Antivirus 現在正在啟動，這可能需要一段時間。

啟動成功

啟動成功。ESET Endpoint Antivirus 現在已啟動。從現在開始，ESET Endpoint Antivirus 會收到定期更新以識別最新的威脅，並確保電腦受到防護。按一下 [完成] 以完成產品啟動。

常見安裝問題

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。

初學者手冊

本章提供 ESET Endpoint Antivirus 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。

i 若要存取系統匣 (Windows 通知區域) 圖示功能表，請確保[使用者介面元素](#)的啟動模式設定為「完整」。

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 和電子郵件通訊防止攻擊。**[時間間隔]** 下拉式功能表允許您指定停用防護的時間。

[進階設定] - 開啟 ESET Endpoint Antivirus [進階設定](#)。若要從[主要程式視窗](#)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 Endpoint Antivirus - 從系統匣 (Windows 通知區域) 圖示開啟 ESET Endpoint Antivirus [主要程式視窗](#)。

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

[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 Endpoint Antivirus 每天多次自動檢查更新。

[關於](#) - 提供系統資訊、ESET Endpoint Antivirus 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 Endpoint Antivirus 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
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 授權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 Endpoint Antivirus 內的兩個區段 - 在 **[指定掃描]** 區段和 **[更新]** 區段中。

電腦掃描

ESET Endpoint Antivirus 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。

i 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 [潛在不安穩的應用程式](#)，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。

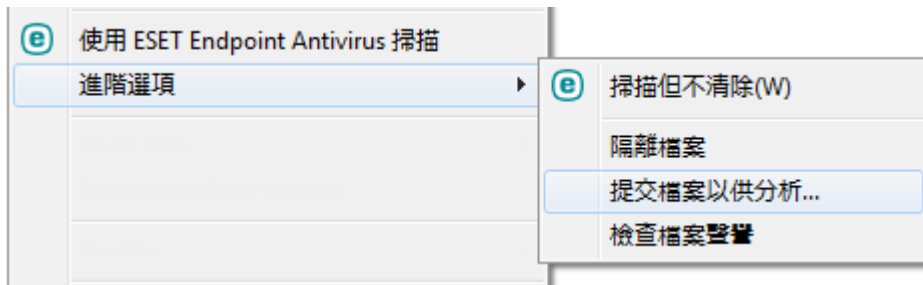
設定檔清單 - 建立新的設定檔或移除現有的更新設定檔。

內容功能表

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

您可以將 ESET Endpoint Antivirus 控制項元素整合至內容功能表。在 [\[進階設定\]](#) > [\[使用者介面\]](#) > [\[使用者介面元素\]](#) 中，可以使用此功能的設定選項。

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

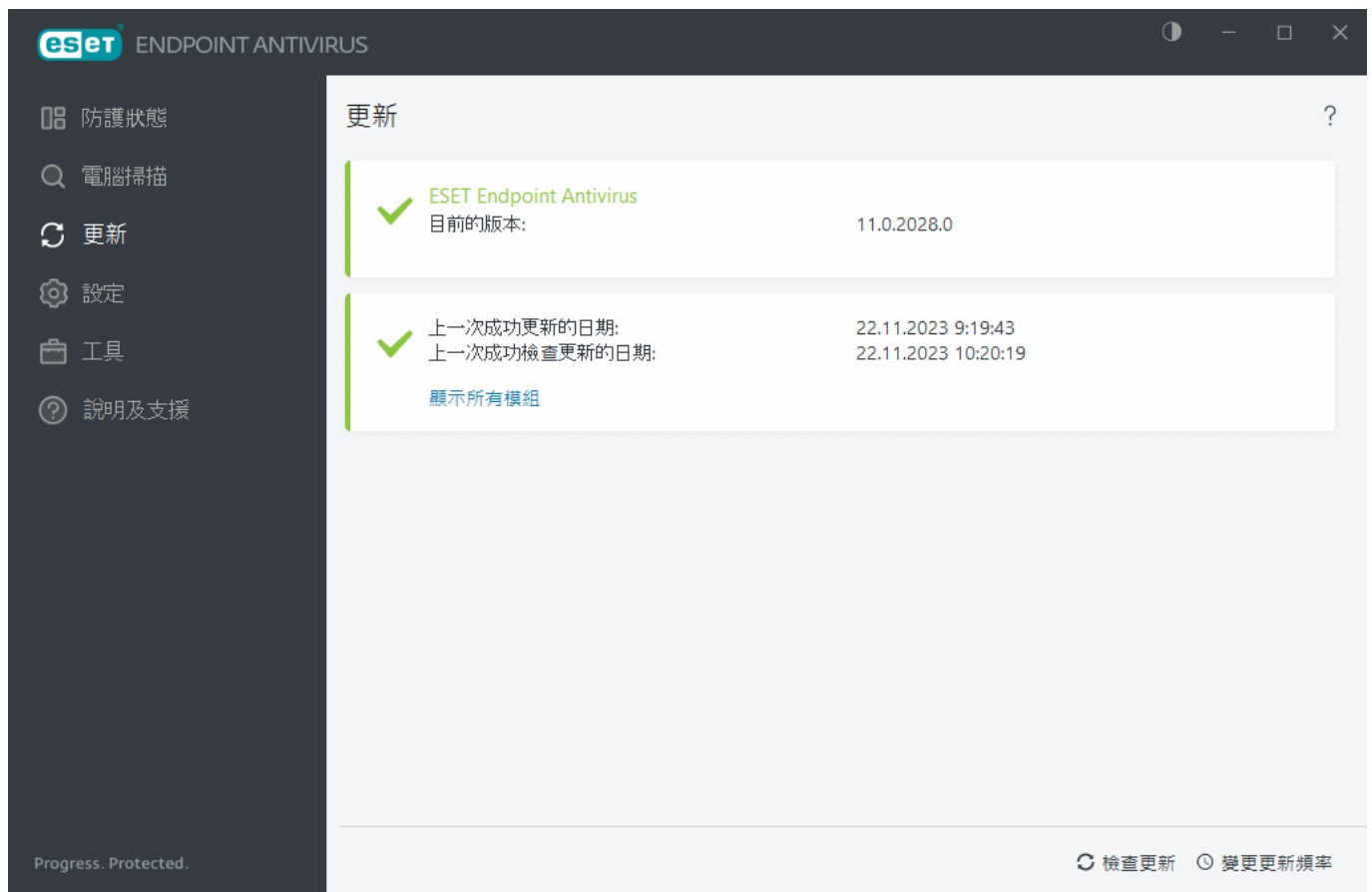


更新設定

定期更新 ESET Endpoint Antivirus 是向電腦提供最高安全性的最佳方法。更新模組確保程式模組和系統元件永遠為最新狀態。

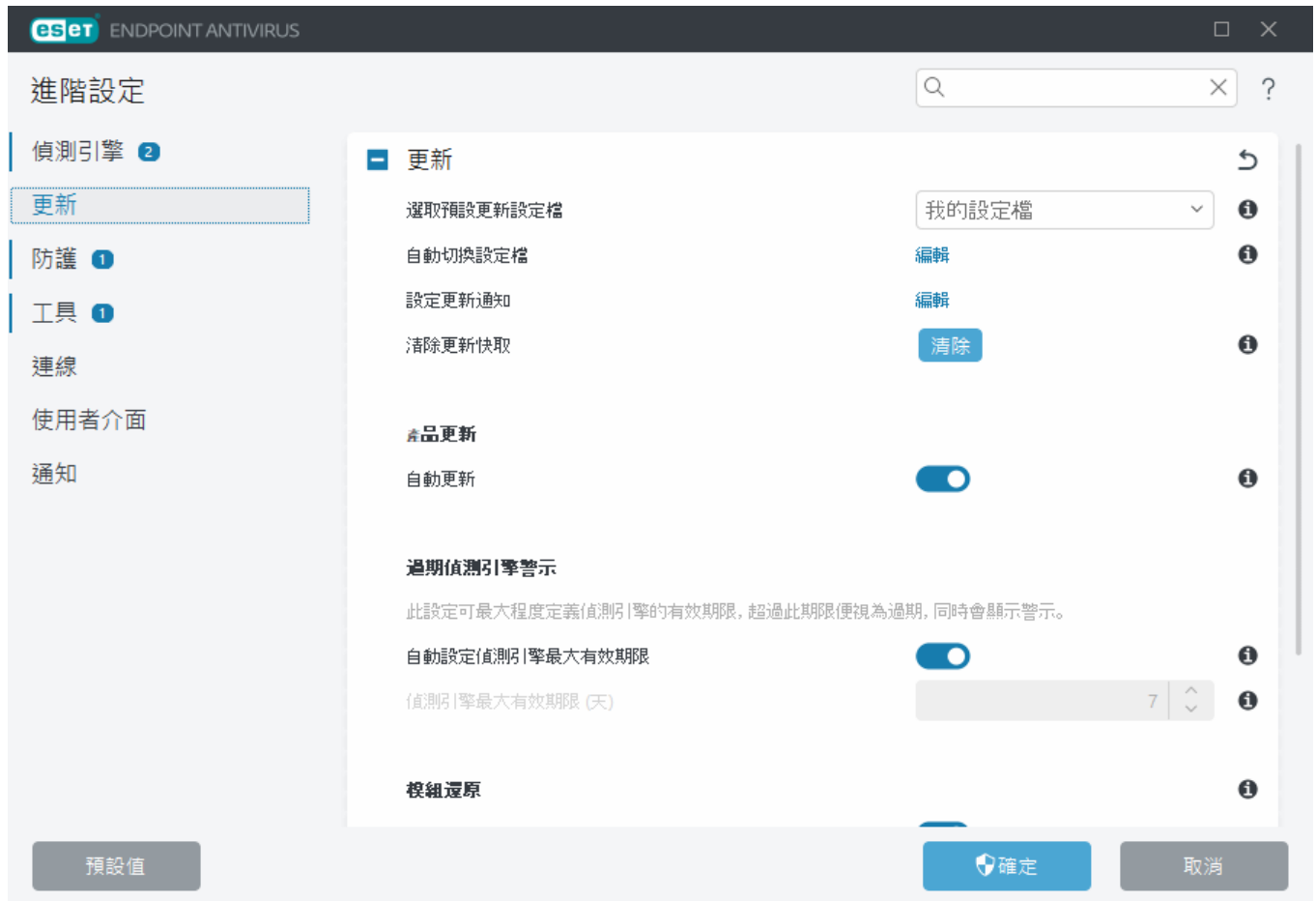
在[主要程式視窗](#)中按一下 **[更新]** 可以檢視目前更新狀態，包括最後的成功更新日期與時間，並在需要時更新。

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。

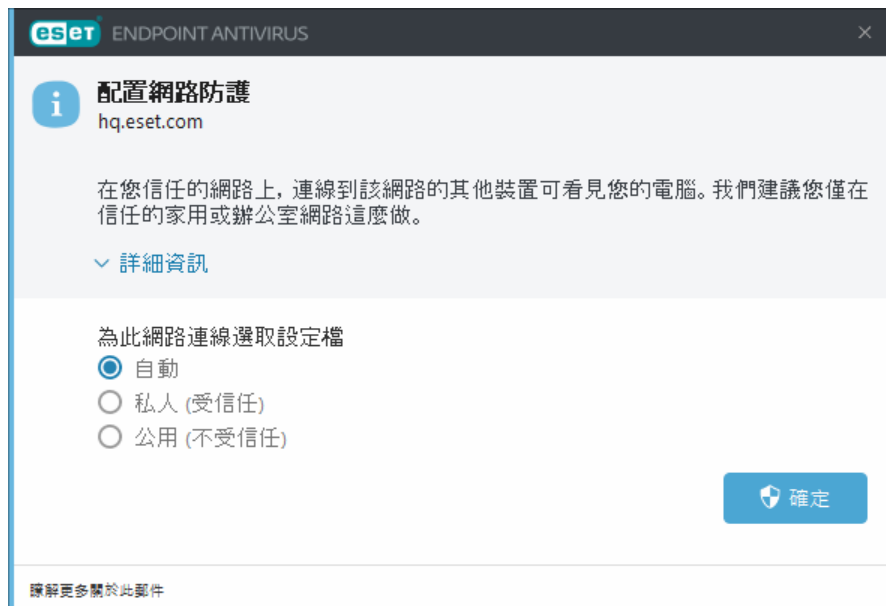


預設啟用 [\[進階設定\]](#) > [\[更新\]](#) > [\[設定檔\]](#) > [\[更新\]](#) > [\[模組更新\]](#) 中的 [\[自動選擇\]](#) 選項。使用 ESET 更新伺服器接收更新時，我們建議您讓此選項保持現狀。

若要取得最佳功能，程式必須自動更新。僅當在 [\[說明及支援\]](#) > [\[啟動產品\]](#) 中輸入正確的授權金鑰時才會自動更新。如果您並未在安裝後輸入您的授權金鑰，您可以隨時輸入。如需更多有關啟動的資訊，請參閱[如何啟動 ESET Endpoint Antivirus](#)。

配置網路防護

在預設情況下，在偵測到新網路連線時，ESET Endpoint Antivirus 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 Endpoint Antivirus 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，啟用了對內網通訊，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。

封鎖的雜湊

在您的環境中使用 ESET Inspect 可讓管理員根據其雜湊封鎖對指定可執行檔的存取。如果管理員封鎖對可執行檔的存取，而您嘗試存取它，ESET Endpoint Antivirus 會顯示此通知：

檔案存取已封鎖 - 應用程式（顯示應用程式的名稱）嘗試存取管理員不允許的檔案。

如果您是管理員並想要允許對通知中指定之應用程式的存取，請參閱 ESET Inspect 線上說明中的[已封鎖雜湊](#)。如果您是使用者並且想要變更應用程式的行為，請與您的管理員連絡。

使用 ESET Endpoint Antivirus

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

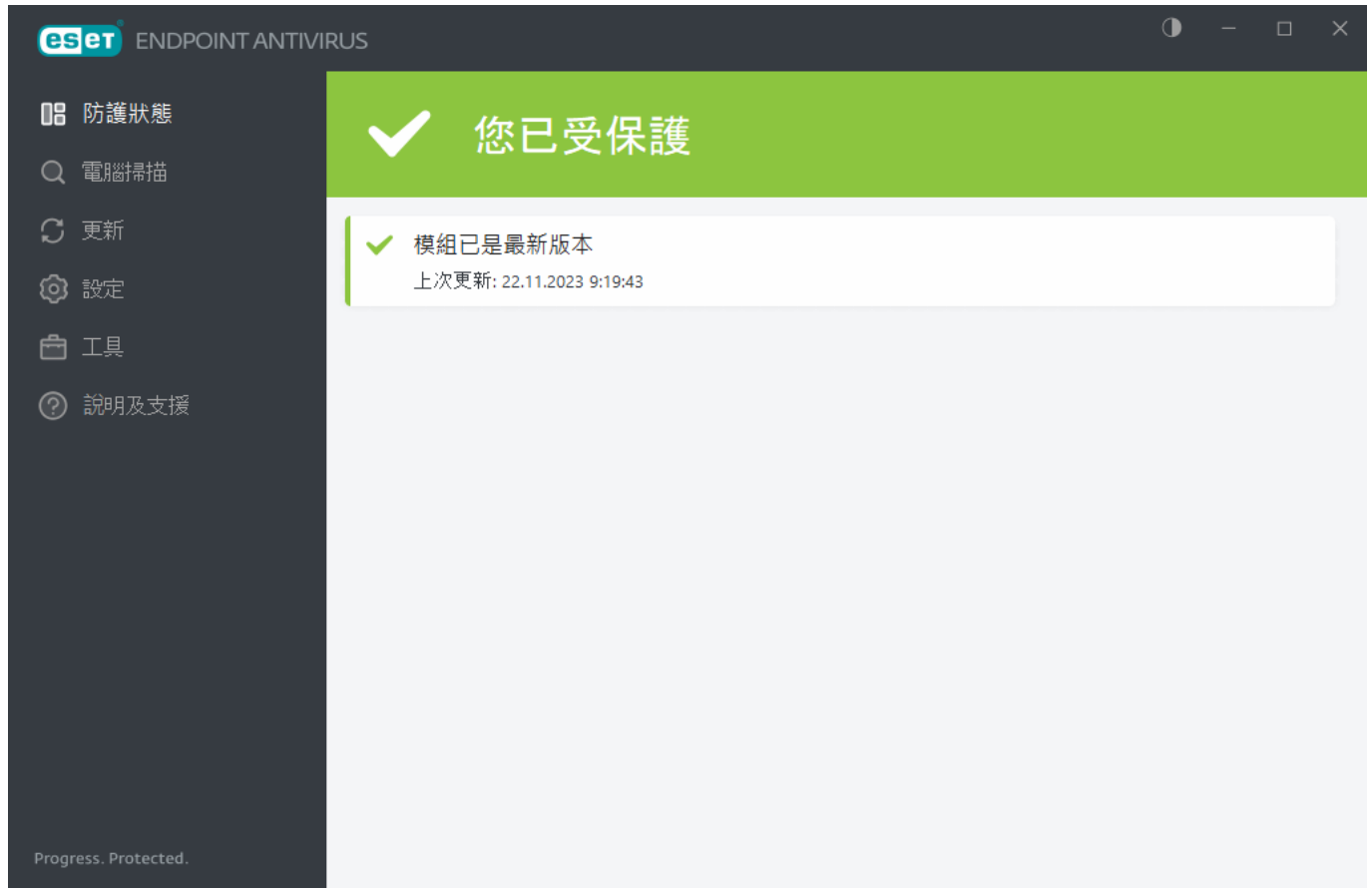


圖解指示

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 Endpoint Antivirus 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 Endpoint Antivirus 的色彩配置。
- **[深色]**—ESET Endpoint Antivirus 將具有深色配置（深色模式）。
- **[淺色]**—ESET Endpoint Antivirus 將具有標準、淺色配置。



主要功能表選項：

[防護狀態](#) - 提供與 ESET Endpoint Antivirus 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](#) - 可協助簡化程式管理，並為進階使用者提供其他選項的模組。

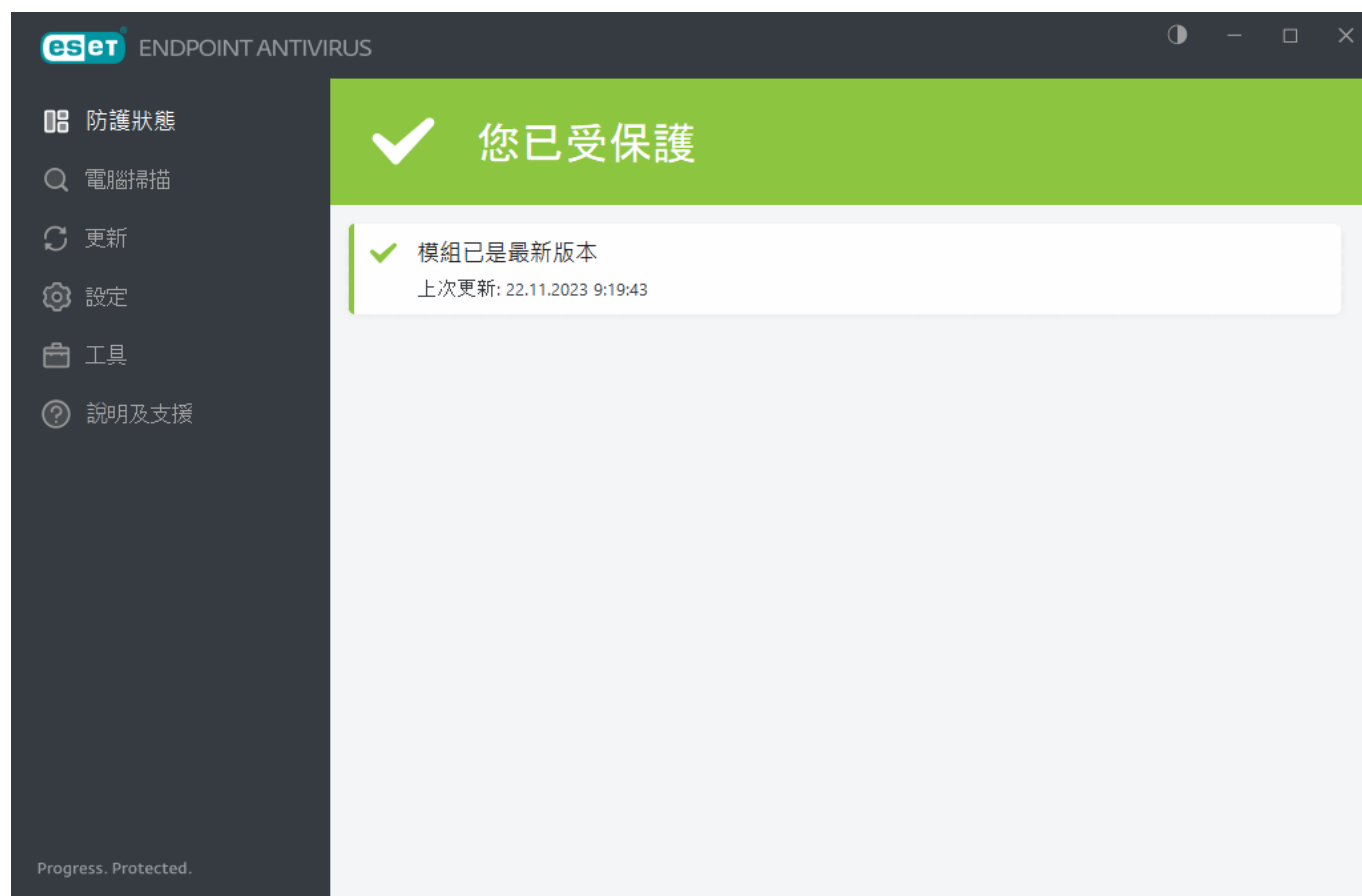
[設定](#) - 提供 ESET Endpoint Antivirus 防護功能的配置選項，以及對[進階設定](#)的存取。

[說明及支援](#) - 顯示有關授權、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。

防護狀態

防護狀態 視窗顯示有關電腦目前防護和上次更新的資訊。綠色 **「最嚴格的防護」** 狀態表示已確保最嚴格的防護。

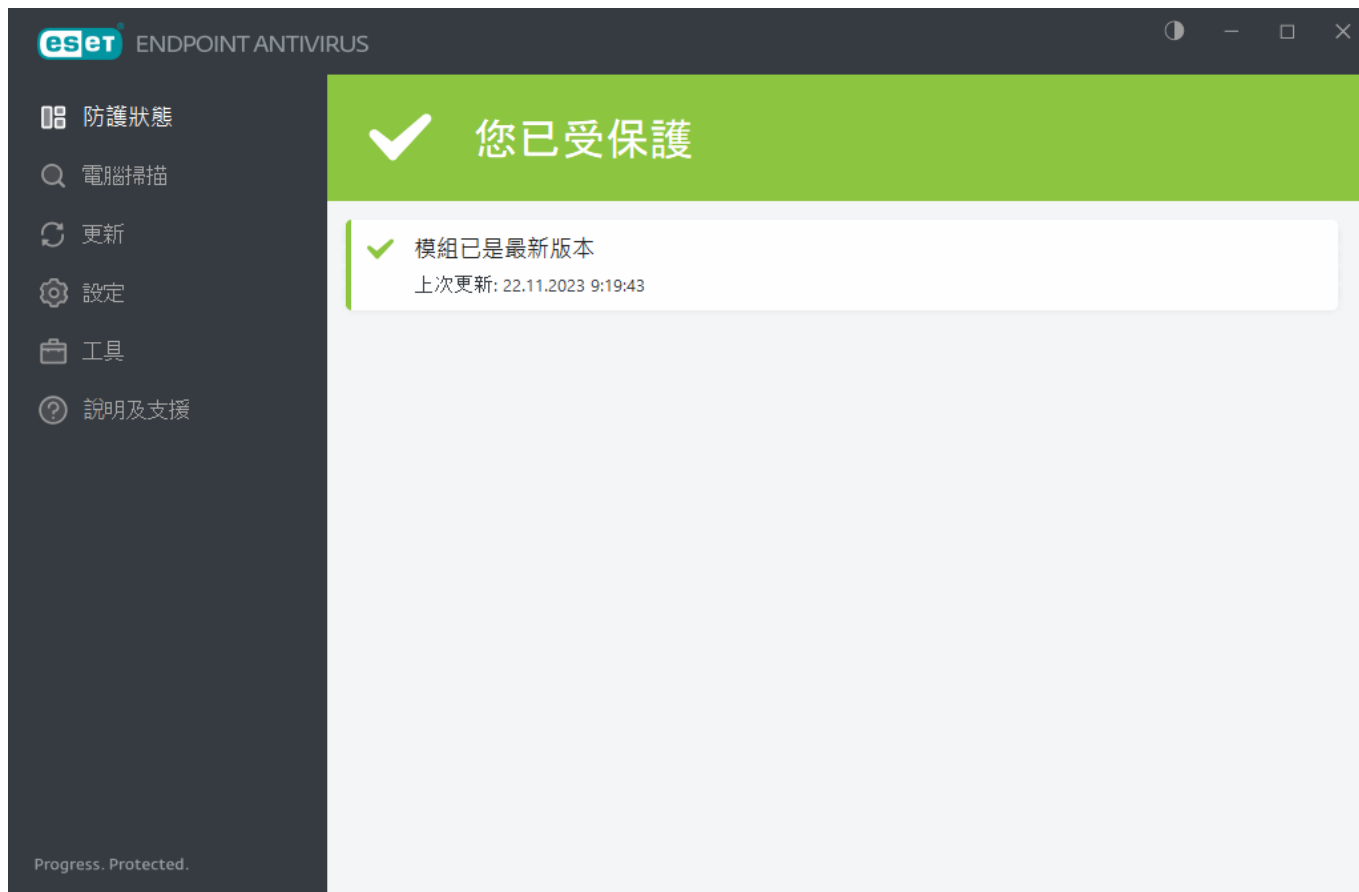
「防護狀態」 視窗顯示含有詳細資訊和建議解決方案的[通知](#)，以改善 ESET Endpoint Antivirus 的安全性、開啟其他功能或確保盡可能的防護。



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

在所有完全運作的程式模組旁邊將顯示核取標記。如果模組需要注意，則會顯示紅色驚嘆號或橘色通知圖示。視窗的上半部會顯示模組的其他相關資訊，包括如何還原完整功能的相關建議。若要變更模組的狀態，請按一下主要功能表中的 **「設定」**，然後按一下需要的模組。



紅色驚嘆號 (!) 圖示指出未確定電腦獲得最嚴格的防護。您可能在下列案例中碰到此類型的通知：

- **病毒及間諜程式防護已暫停** - 按一下 [防護狀態] 窗格中的 [啟動所有病毒及間諜程式防護模組]，或按一下主要程式視窗中 [設定] 窗格內的 [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。
- **病毒防護無法運作** - 病毒掃描器初始化失敗。大部分 ESET Endpoint Antivirus 模組將無法正常運作。
- **網路釣魚防護無法運作** - 由於其他必要的程式模組為非作用中，因此這個功能無法運作。
- **[偵測引擎已過期]** - 在數次嘗試更新偵測引擎（舊稱為病毒資料庫）失敗之後，就會出現此錯誤。我們建議您檢查更新設定。此錯誤最常見的原因是輸入的[驗證資料](#)錯誤或[連線設定](#)的配置錯誤。
- **[產品未啟動] 或 [您的授權已到期]** - 這是由紅色的防護狀態圖示所表示。您的授權過期後即無法更新程式。請按照警告視窗中的指示續約您的授權。
- **主機入侵預防系統 (HIPS) 已停用** - 停用 HIPS 時，即會指出此問題。無法保護您的電腦阻擋某些類型的威脅，因此應該按一下 [啟用 HIPS]，立即重新啟用防護。
- **沒有已排程的定期更新** - ESET Endpoint Antivirus 將不會檢查或接收重要更新，除非您排定更新工作。
- **[網路存取已封鎖]** - 當此工作站（來自 ESET PROTECT）的 [將電腦與網路隔離] 用戶端工作觸發時，即會顯示。如需詳細資訊，請連絡系統管理員。
- **即時檔案系統防護已暫停** - 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 [啟用即時防護] 以重新啟用此功能。



橙色 "i" 表示您的 ESET 產品需要注意非嚴重問題。可能的原因包含：

- **Web 存取防護已停用** - 按一下安全性通知以重新啟用 Web 存取防護，然後再按一下 [啟動 Web 存取防護]。
- **您的授權即將到期/您的授權今日到期** - 這是由顯示驚嘆號的防護狀態圖示所表示。您的授權到期後，程式將無法更新，[防護] 狀態圖示將變成紅色。
- **電子郵件用戶端反垃圾郵件已暫停** - 按一下 [啟用電子郵件用戶端反垃圾郵件] 以重新啟用此功能。

- **Web 控制已暫停** - 按一下 [**啟用 Web 控制**] 以重新啟用此功能。
- **原則覆寫作用中** - 暫時覆寫原則所設定的配置，可能直到疑難排解完成為止。只有獲授權的使用者才能覆寫原則設定。如需詳細資訊，請參閱[如何使用覆寫模式](#)。
- **裝置控制已暫停** - 按一下 [**啟用裝置控制**] 以重新啟用此功能。

若要在 ESET Endpoint Antivirus 的第一個窗格中調整產品內狀態的可視度，請參閱[應用程式狀態](#)。

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，可提交 ESET 技術支援要求。ESET 技術支援將快速回答您的問題並協助尋找解決方法。

i 如果狀態屬於 ESET PROTECT 原則所封鎖的功能，則您將無法按一下連結。

電腦掃描

指定掃描器是 ESET Endpoint Antivirus 防毒解決方案中的一個重要部分。它可用來針對電腦中的檔案及資料夾執行掃描。從安全觀點來看，不應該僅在懷疑有感染時才執行電腦掃描，出於常規安全性考量也應定期執行掃描。我們建議您定期執行（例如一個月一次）系統深入掃描以偵測未由[即時檔案系統防護](#)偵測出的病毒。當資料寫入磁碟時，即時檔案系統防護已停用、偵測引擎已過時，或是當檔案儲存至磁碟時未偵測為病毒，就可能發生上述情況。



可以使用兩種**電腦掃描**類型。[**掃描您的電腦**] 可快速掃描系統，而無需進一步配置掃描參數。[**自訂掃描**] 可讓您選取任何預先定義的掃描設定檔，以及定義特定的掃描目標。

請參閱[掃描進度](#)，取得更多關於掃描進度的資訊。

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。

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）。

i 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。

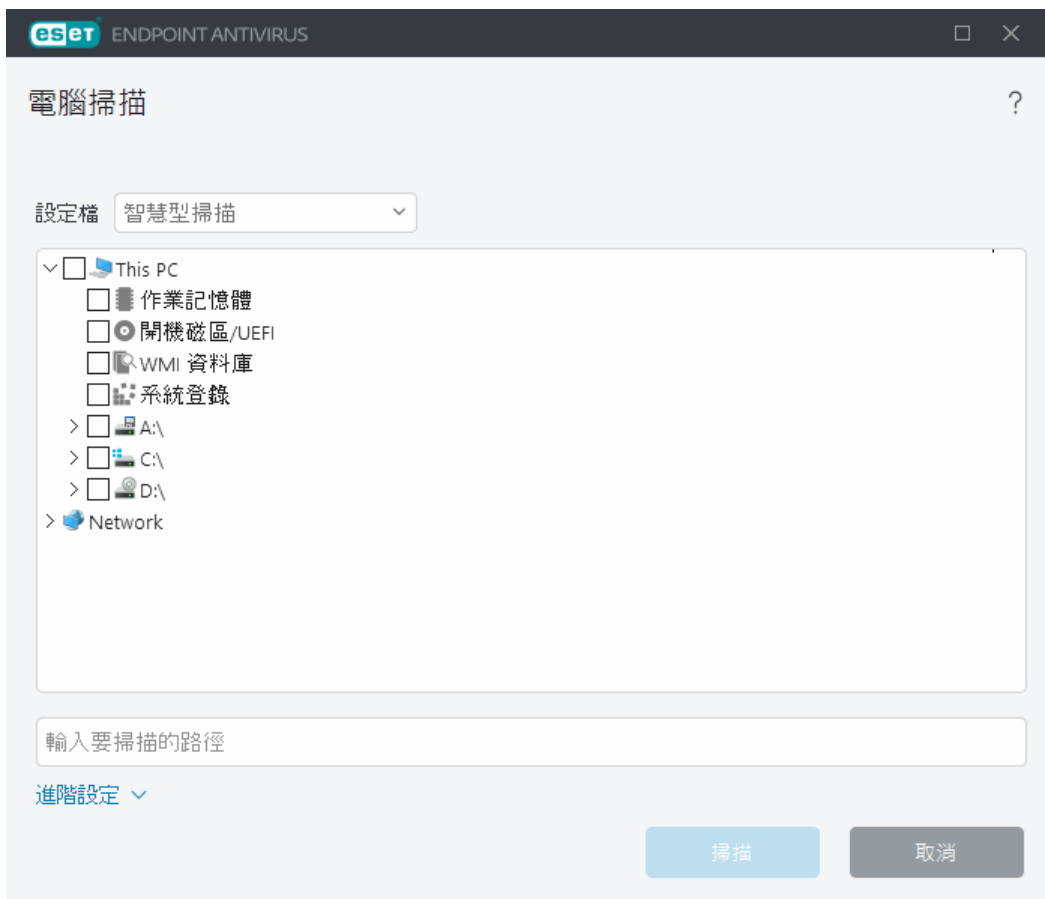
資料夾（樹狀）結構還包含特定掃描目標。

- **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。

i 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。

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

i **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。

i 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【睡眠】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

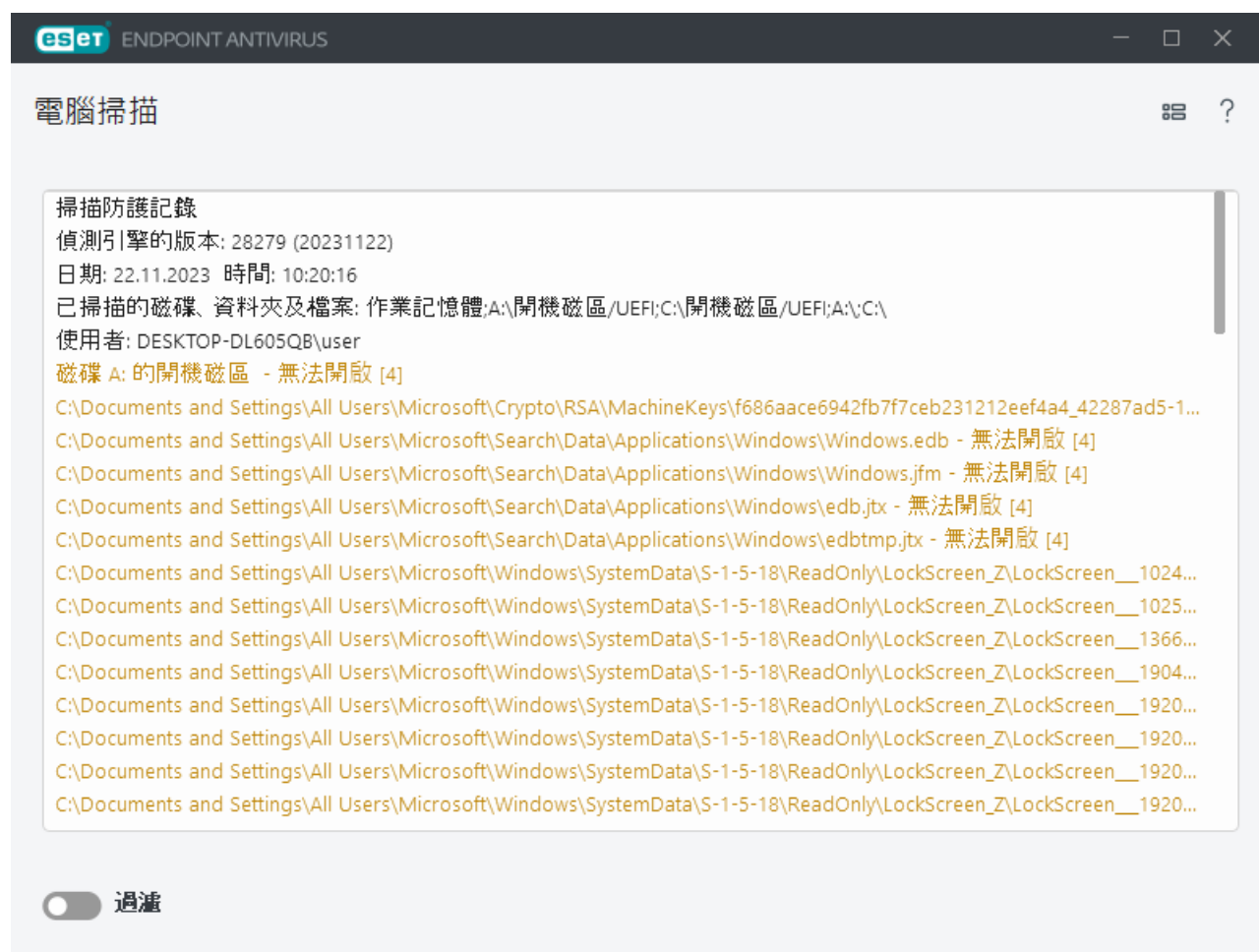
您可以在[防護記錄檔案](#)中檢視與特定掃描相關的詳細資訊。掃描防護記錄包含以下資訊：

- 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

i 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。



i 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

處理方法	使用量
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。
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。

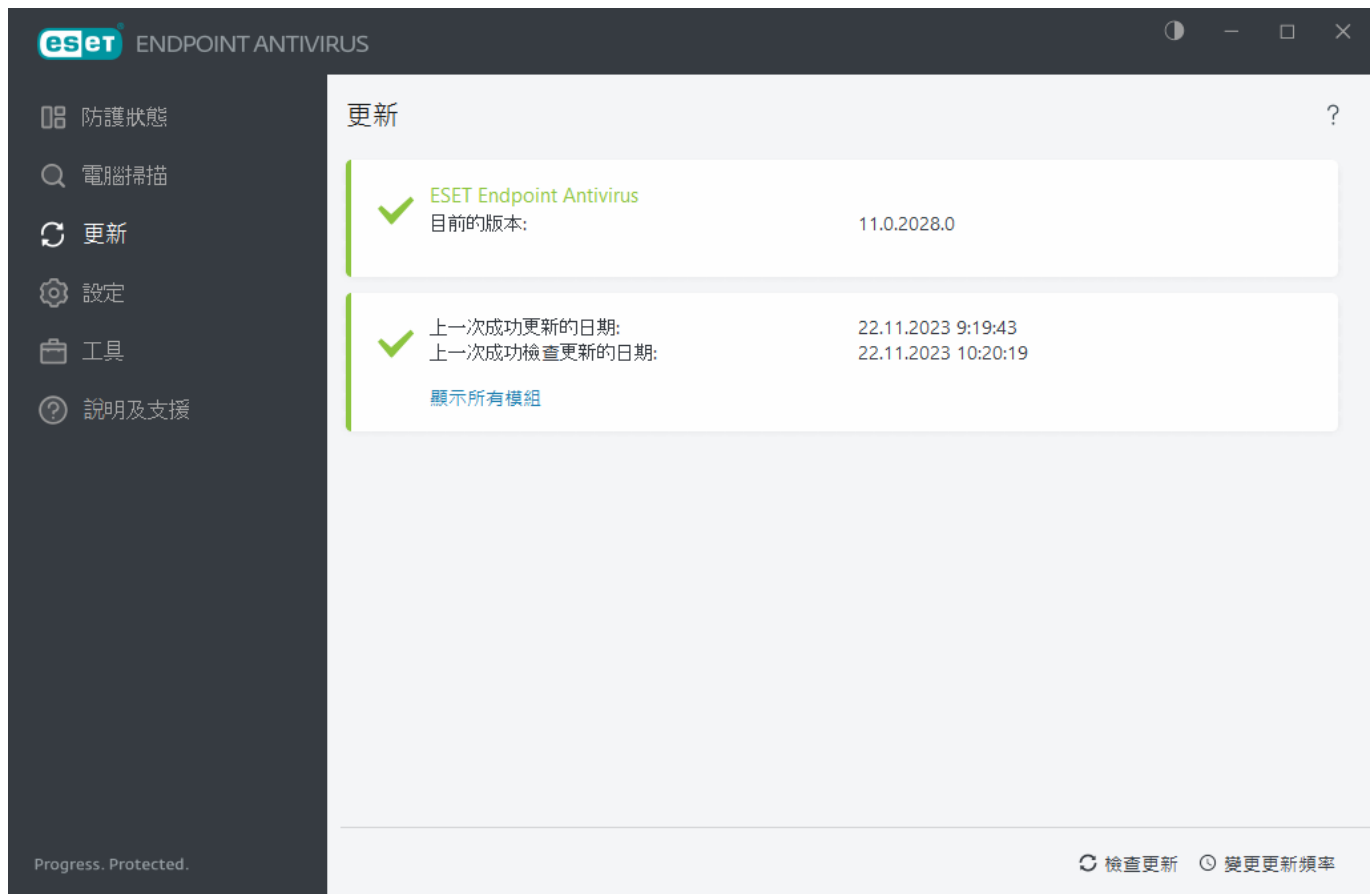
更新

定期更新 ESET Endpoint Antivirus 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。您必須使用您的授權金鑰來啟動產品，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 Endpoint Antivirus 產品](#)以存取 ESET 更新伺服器。購買 ESET Endpoint Antivirus 後，ESET 會透過電子郵件將授權金鑰傳送給您。

如果您使用沒有使用者名稱與密碼的離線授權檔案啟動 ESET Endpoint Antivirus 並嘗試更新，則會出現 **[模組更新失敗]** 紅色訊息提示您只能從映像下載更新。



目前的版本 – ESET Endpoint Antivirus 組建編號。

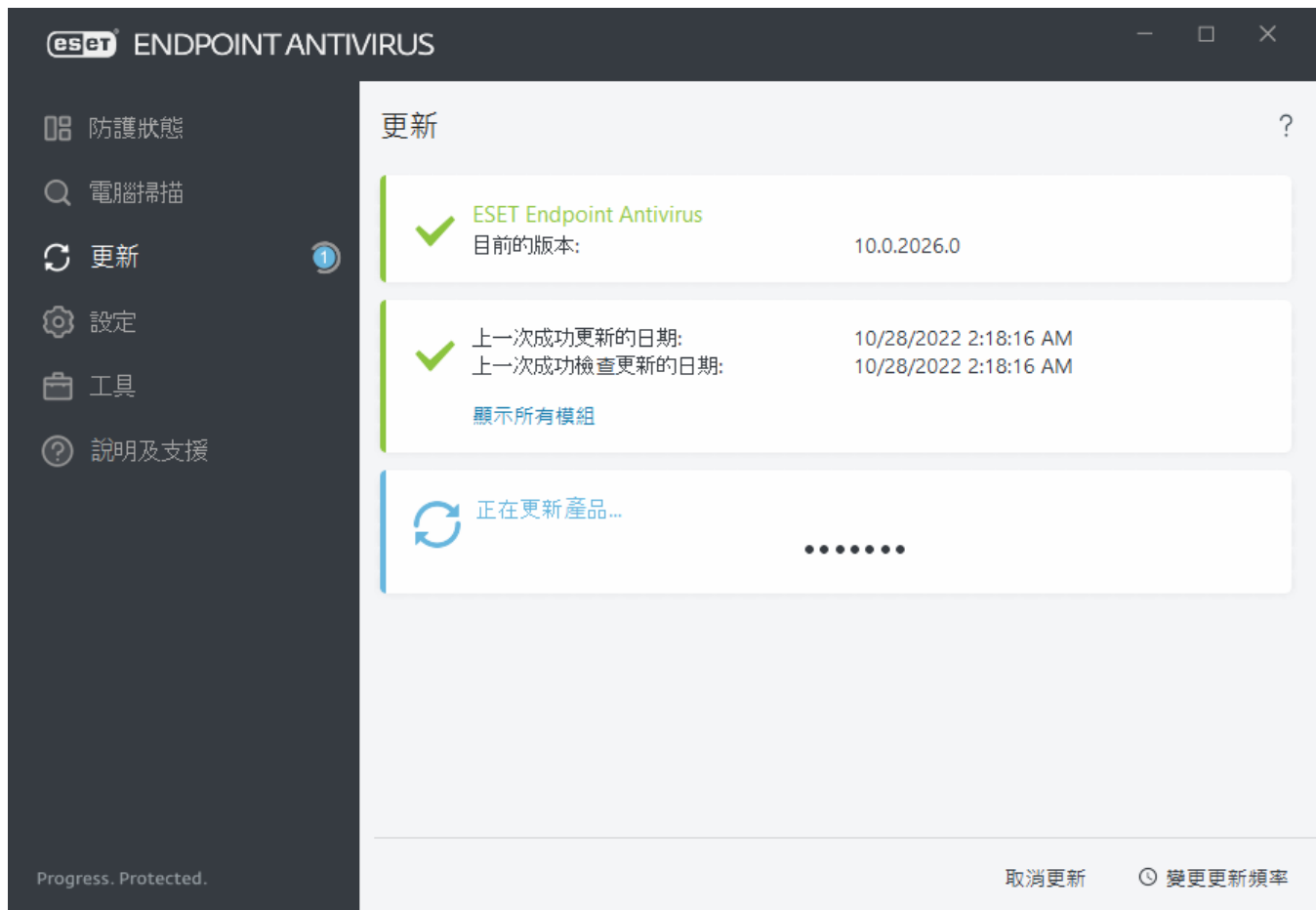
上次成功更新 – 上次成功更新的日期和時間。請確認系統是指出最近的日期，表示偵測引擎是最新的。

上次成功檢查更新 – 上次成功嘗試更新模組的日期和時間。

顯示所有模組 – 按一下連結即可開啟已安裝模組的清單，並檢查模組的版本和上次更新。

更新處理程序

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



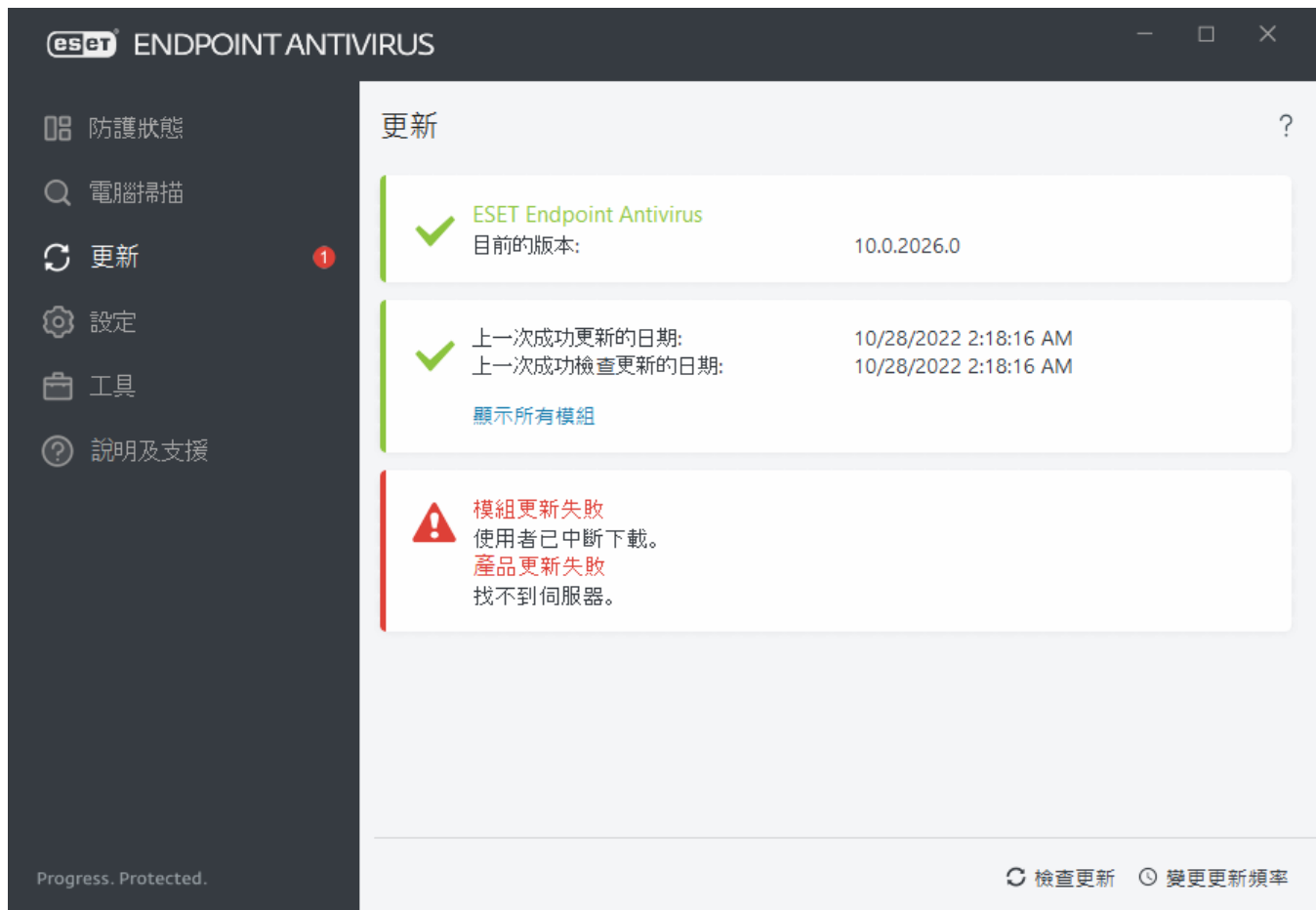
在正常情況下，您將在【更新】視窗中看見綠色核取標記，表示程式是最新狀態。如果您沒有看見綠色核取標記，即表示程式過期，因此更容易遭到感染。請儘快更新程式模組。

更新失敗

偵測引擎已過期 - 在數次嘗試更新模組失敗之後，就會出現此錯誤。我們建議您檢查更新設定。此錯誤最常見的原因是輸入的驗證資料錯誤或[連線設定](#)的配置錯誤。

前一個通知與下列關於失敗更新的兩項【**模組更新失敗**】訊息相關：

1. **無效授權** - 您的授權非作用中。建議您檢查驗證資料。從主要功能表按一下【說明及支援】>【變更授權】以輸入新的授權金鑰。
2. **下載更新檔案時發生錯誤** - 此錯誤可能是因不正確的[網際網路連線設定](#)所造成。建議您檢查網際網路連線（透過在 Web 瀏覽器中開啟任何網站）。如果網站未開啟，可能是尚未建立網際網路連線，或是電腦連線有問題。請確保您的網際網路服務提供者 (ISP) 具有可使用的網際網路連線。



i 如需詳細資訊，請參閱 [ESET 知識庫文章](#)。

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 Endpoint Antivirus 中啟動下列更新工作：

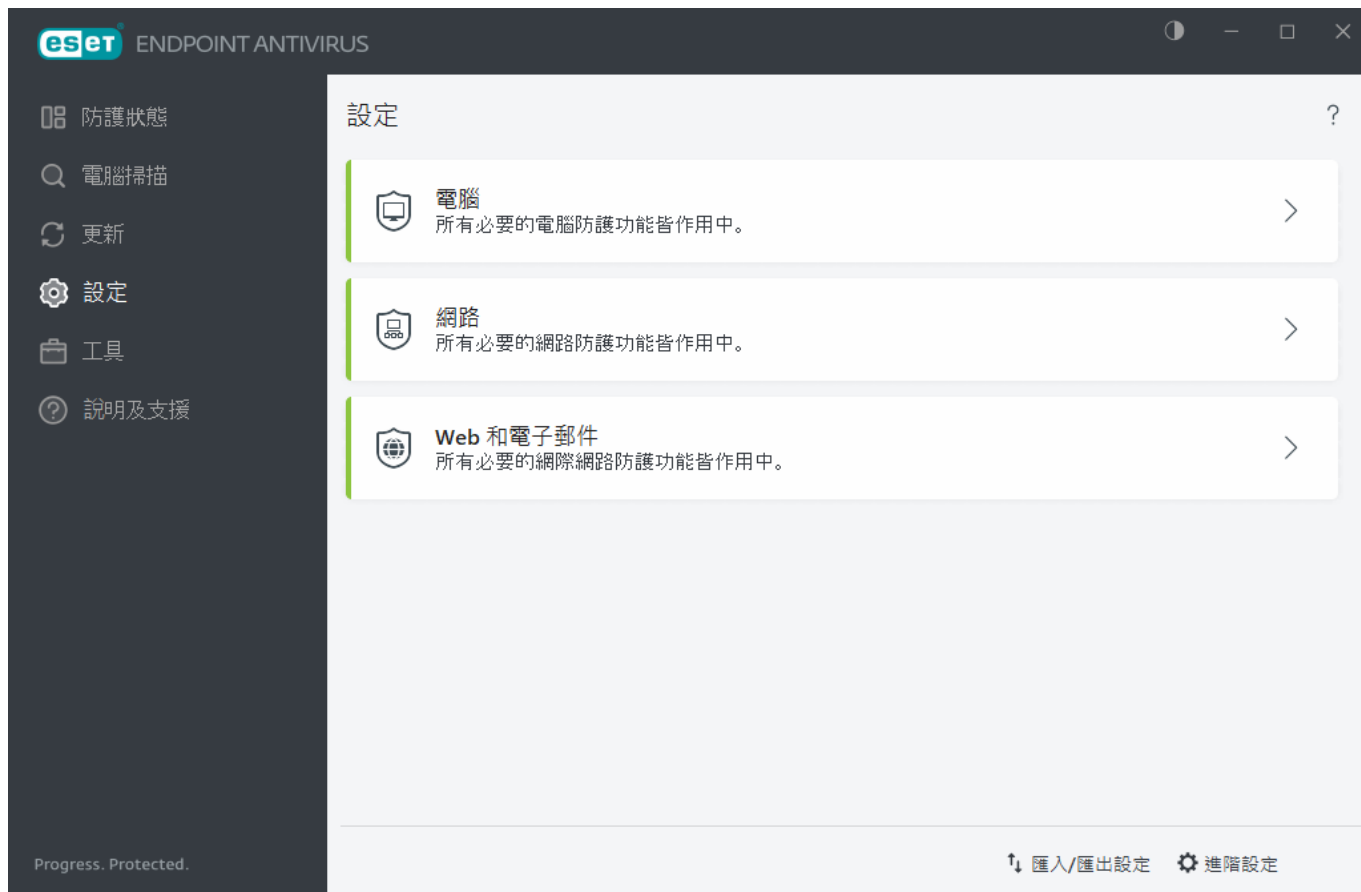
- 定期自動更新
- 使用者登入後自動更新

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。

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。

i 從 ESET PROTECT Web 主控台建立原則時，您可以為每一個設定選取旗標。含強制旗標的設定具有優先權，無法由較新的原則覆寫（即使較新的原則含有強制旗標）。這確保將不會變更此設定（例如，由使用者或在合併期間由更新的原則變更）。如需詳細資訊，請參閱 [ESET PROTECT 線上說明中的旗標](#)。




[設定] 功能表包含下列區段：

[電腦](#)

[網路](#)

[Web 和電子郵件](#)

當套用 ESET PROTECT 原則時，您將在特定元件旁看到鎖定圖示 。在登入的使用者（例如管理員）進行驗證之後，可在本機覆寫 ESET PROTECT 所套用的原則。如需詳細資訊，請參閱 [ESET PROTECT 線上說明](#)。

i 透過這種方式停用的所有防護方法都會在電腦重新啟動後重新啟用。



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


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



在 **「電腦」** 區段中，您可以啟用或停用下列元件：

- **即時檔案系統防護** - 開啟、建立或在電腦上執行所有檔案時，都會掃描這些檔案是否具有惡意程式碼。按一下 **「即時檔案系統防護」** 旁邊的齒輪圖示 ，接著按一下 **「編輯排除」** 來開啟 **排除設定視窗**，並從掃描中排除檔案與資料夾。若要開啟 **「即時檔案系統防護」** 進階設定，按一下 **「配置」**。
- **裝置控制** - 提供自動裝置 (CD/DVD/USB/...) *******。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。
- **Host Intrusion Prevention System (HIPS) - HIPS** 系統監控作業系統中所發生的事件，並根據自訂的規則集合執行反應動作。
- **「進階記憶體掃描器」** - 可與惡意探索封鎖程式一起搭配，強化對抗惡意軟體在整個利用欺騙及/或加密時對惡意軟體防護產品所啟用偵測功能的規避動作。進階記憶體掃描器依預設已啟用。請在 **字彙** 中閱讀更多有關此類型防護的資訊。
- **惡意探索封鎖程式** - 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。
- **「勒索軟體保護」** 是另一種層級的防護，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 .
- **「簡報模式」** - 一項專為要求可不間斷地使用軟體、不想受到通知打擾，而且想要將 **CPU** 使用量減到最少的使用者所設計的功能。啟用 **「簡報模式」** 之後，您將收到警告訊息（潛在的安全性風險），接著主要程式視窗會轉為橙色。

停用病毒及間諜程式防護 - 每當您要暫時停用「病毒及間諜程式防護」時，您可以使用下拉式功能表選取您所選取要停用元件的時間長度，然後按一下 **「套用」** 來停用安全性元件。若要重新啟用防護，請按一下 **「啟用病毒及間諜程式防護」** .

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。

偵測到威脅

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 Endpoint Antivirus 處理入侵的一般範例，入侵的偵測可使用：

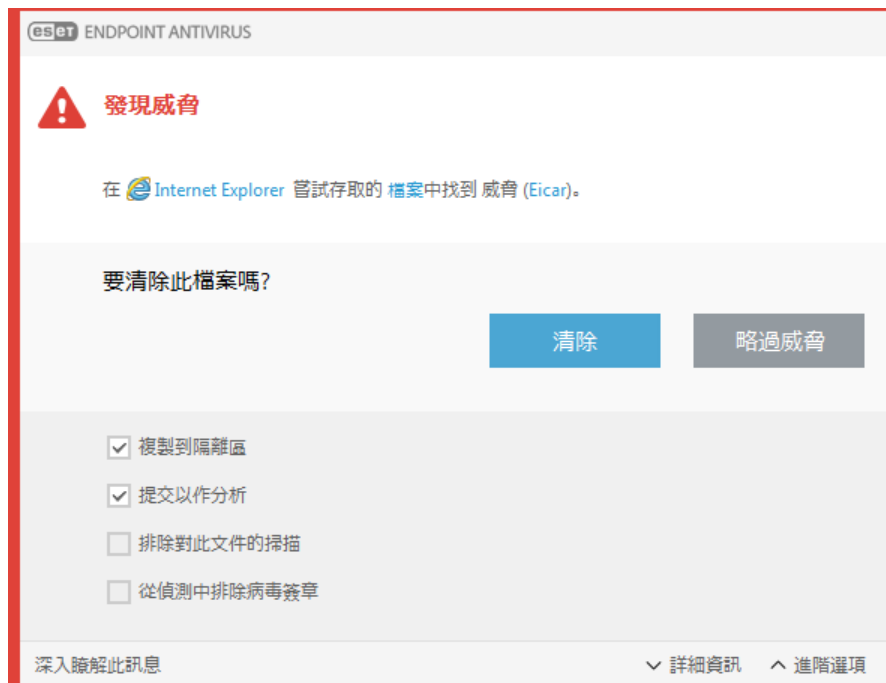
- [即時檔案系統防護](#)
- [Web 存取防護](#)
- [電子郵件用戶端防護](#)
- [指定電腦掃描](#)

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](#)。



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 Endpoint Antivirus 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。

刪除壓縮檔中的檔案

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


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

- 開啟 ESET Endpoint Antivirus然後按一下 [電腦掃描]
- 按一下 [智慧型掃描]（如需詳細資訊，請參閱電腦掃描）
- 完成掃描之後，請檢閱已掃描、受感染及已清除的防護記錄


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

網路

開啟 [\[主程式視窗\]](#) > **[設定]** > **[網路]** 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  ²

 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）以存取進階設定。

網路攻擊防護 (IDS) – 分析網路流量的內容，並防範網路攻擊。會封鎖任何被視為有害的流量²ESET Endpoint Antivirus 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 – 快速準確地識別系統中的惡意軟體。

解決封鎖的通訊 – 協助您解決 ESET 防火牆所造成的連線問題。如需更多詳細資訊，請參閱[疑難排解精靈](#)²

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](#)²



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] > [網路] 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。

 下列 ESET 知識庫文章可能僅以英文提供：

- [使用疑難排解精靈新增例外](#)

 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 Endpoint Antivirus 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] > **[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

i 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。

解決 ESET 網路防護問題

若您在使用已安裝的 ESET Endpoint Antivirus 時遇到連線問題，則可使用幾種方法來判別問題是否因 ESET 網路防護所導致。此外，ESET 網路防護還能協助您建立新規則或例外來解決連線問題。

請參閱下列有關協助解決 ESET 網路防護相關問題的主題：

- [網路存取疑難排解](#)
- [記錄並從防護記錄建立規則或例外](#)
- [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」](#)。

i 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 Endpoint Antivirus 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 Endpoint Antivirus 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
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]^②

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. 瀏覽至 [進階設定] > [工具] > [診斷] 並啟用 [啟用網路防護進階記錄]^②
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^②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 Endpoint Antivirus 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，請確保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。

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。

i 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](#)[®]。


Web 和電子郵件

網際網路連線是個人電腦中的標準功能，也是傳輸惡意程式碼的主要媒介。開啟 [\[主程式視窗\]](#) > [設定] > [Web 和電子郵件] 以配置增強網際網路防護的 ESET Endpoint Antivirus 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。

[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。

- i** 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 Endpoint Antivirus 可控制來自電子郵件用戶端的所有通訊。

防網路釣魚防護

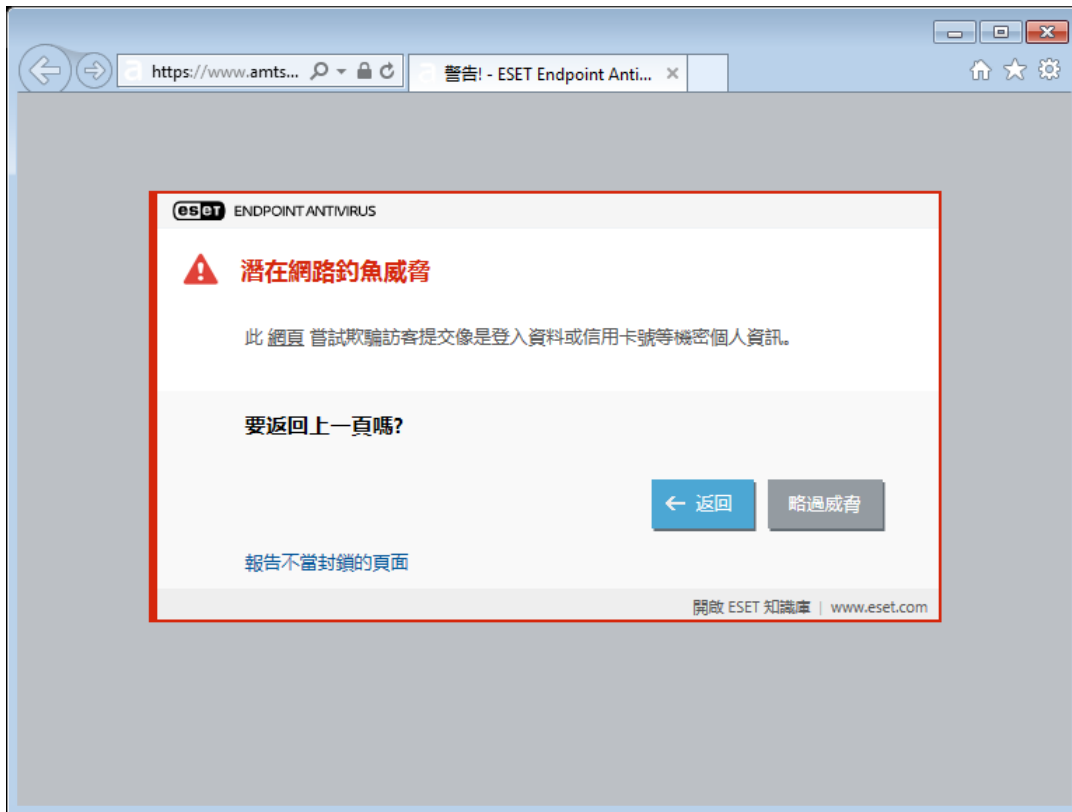
網路釣魚是一種利用社交工程（操縱使用者以取得機密資訊）的犯罪活動。網路釣魚用於存取敏感資料，例如銀行帳號、PIN 等。如需詳細資訊，請參閱[字彙](#)。ESET Endpoint Antivirus 包含防網路釣魚防護，封鎖已知會散佈這類內容的網頁。

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 Endpoint Antivirus 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）。

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 Endpoint Antivirus.xml 配置檔案。

i 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 Endpoint Antivirus 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。當您想要在各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。

i 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。



工具

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

- [防護記錄檔案](#)
- [執行中的處理程序](#)（如果已在 ESET Endpoint Antivirus 中啟用 ESET LiveGrid®）
- [安全性報告](#)（適用於未管理端點）
- [ESET SysInspector](#)
- [排程器](#)
- [提交範例以供分析](#) – 可讓您將可疑檔案提交至 ESET 研究實驗室以供分析（根據您的 ESET LiveGrid® 配置，有可能無法使用）。
- [隔離區](#)



防護記錄檔案

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

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

- **偵測** - 此防護記錄提供 ESET Endpoint Antivirus 模組所偵測到偵測與入侵的詳細資訊。此資訊包括偵測時間、偵測名稱、位置，以及在偵測到入侵時，所登入的使用者名稱及其執行的處理方法。按兩下任何防護記錄項目，以在個別視窗中顯示其詳細資料。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 Endpoint Antivirus 執行的所有重要處理方法都會記錄在事件防護記錄中。事件防護記錄包含程式中已發生事件及錯誤的相關資訊。此選項專門用來協助系統管理員及使用者解決問題。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** - 所有掃描結果都會顯示在這個視窗中。每一行均與單一電腦控制項對應。按兩下任何項目，以檢視各個掃描的詳情。
- **封鎖的檔案** - 包含在連線 ESET Enterprise Inspector 時，無法存取的封鎖檔案記錄。通訊協定顯示封鎖檔案的原因和來源模組，以及執行檔案的應用程式和使用者。如需詳細資訊，請參閱 [ESET Enterprise Inspector 線上使用者手冊](#)。
- **傳送的檔案** - 包含已傳送至 ESET LiveGrid® 或 [ESET LiveGuard](#) 以供分析的檔案記錄。
- **審查防護記錄** - 每筆防護記錄都包含執行變更時的日期和時間、變更類型、說明、來源和使用者等相關資訊。如需詳細資訊，請參閱[審查防護記錄](#)。
- **HIPS** - 包含已標記要記錄之特定規則的記錄。通訊協定會顯示呼叫該作業的應用程式、結果（是否

允許或禁止規則)，及已建立規則的名稱。

- **網路防護** - 防火牆防護記錄顯示由**網路攻擊防護**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料，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**封鎖的網站清單，此清單非常有用。這些防護記錄會顯示開啟特定網站連線的時間、URL、使用者與應用程式。
- **裝置控制** - 包含連接到電腦的可移除媒體或裝置記錄。僅含有裝置控制規則的裝置將記錄於防護記錄檔案中。如果規則不符合連接的裝置，將不會對連接的裝置建立防護記錄項目。您也可以在這裡看見詳細資訊，例如裝置類型、序號、供應商名稱及媒體大小（如果有）。



選取任何防護記錄的內容並且按 **Ctrl + C** 將其複製到剪貼簿。按住 **Ctrl + 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，您可以定義[防護記錄過濾](#)視窗的過濾條件。
- **啟用過濾** - 啟動過濾設定。
- **停用過濾** - 清除所有過濾器設定值（如上所述）。
- **複製/全部複製** - 複製視窗中所有記錄的相關資訊。
- **[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** - 以 XML 格式匯出記錄相關資訊。
- **全部匯出** - 以 XML 格式匯出所有記錄的相關資訊。

- **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。
- **[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）。

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。

審查防護記錄

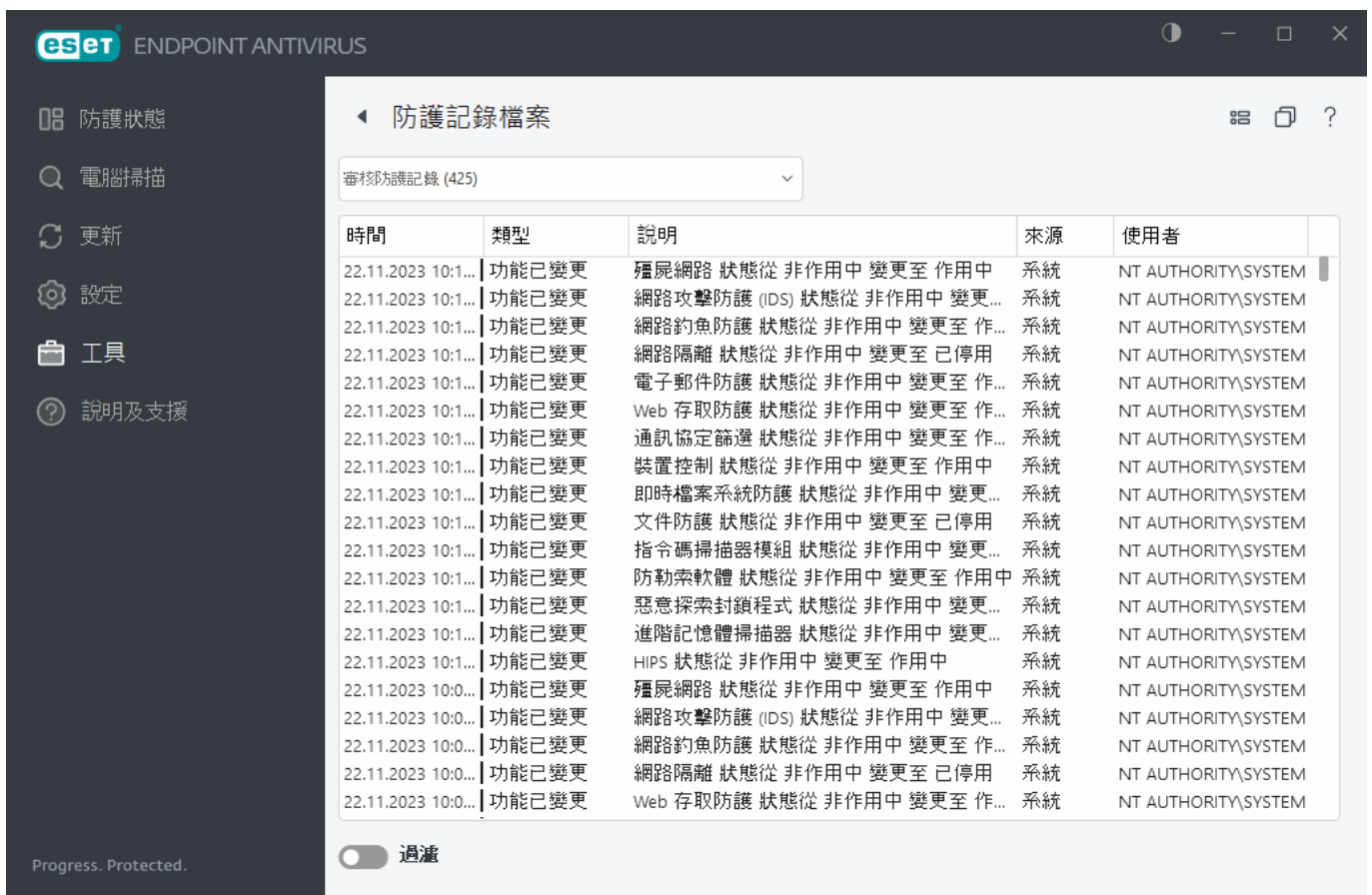
在企業環境中，通常有多位使用者具備針對配置端點而定義的存取權限。因為修改產品配置可能會大幅影響產品運作方式，所以管理員必須追蹤使用者所做的變更，協助他們快速識別、解決，以及防止未來發生相同或類似的問題。

審核防護記錄是用於找出問題起源的新記錄類型。審核防護記錄可追蹤配置和防護狀態的變更，以及記錄快照供稍後參考。

若要查看 [審查防護記錄]，請按一下主功能表中的 [工具]，然後按一下 [防護記錄檔案] 並從下拉式功能表中選取 [審查防護記錄]。

審查防護記錄包含以下相關資訊：

- 時間 – 執行變更的時間
- 類型 – 已變更的設定或功能類型
- 說明 – 確切的變更內容，以及哪部分的設定已隨著變更的設定數目一起變更
- 來源 – 變更的來源
- 使用者 – 進行變更的人員



The screenshot shows the ESET Endpoint Antivirus interface. On the left is a sidebar with navigation options: 防護狀態, 電腦掃描, 更新, 設定, 工具, and 說明及支援. The main window is titled '防護記錄檔案' (Defense Log). Below the title is a dropdown menu showing '審核防護記錄 (425)'. The main area contains a table with the following columns: 時間 (Time), 類型 (Type), 說明 (Description), 來源 (Source), and 使用者 (User). The table lists various configuration changes, such as '殭屍網路' (Botnet), '網路攻擊防護 (IDS)' (Network Attack Protection), '網路釣魚防護' (Phishing Protection), '網路隔離' (Network Isolation), '電子郵件防護' (Email Protection), 'Web 存取防護' (Web Access Protection), '通訊協定篩選' (Protocol Filtering), '裝置控制' (Device Control), '即時檔案系統防護' (Real-time File System Protection), '文件防護' (File Protection), '指令碼掃描器模組' (Script Scanner Module), '防勒索軟體' (Ransomware Protection), '惡意探索封鎖程式' (Malicious Explorer Blocking), '進階記憶體掃描器' (Advanced Memory Scanner), 'HIPS' (Host Intrusion Prevention System), and 'Web 存取防護' (Web Access Protection). At the bottom of the window, there is a '過濾' (Filter) button and the status 'Progress. Protected.'

時間	類型	說明	來源	使用者
22.11.2023 10:1...	功能已變更	殭屍網路 狀態從 非作用中 變更至 作用中	系統	NT AUTHORITY\SYSTEM
22.11.2023 10:1...	功能已變更	網路攻擊防護 (IDS) 狀態從 非作用中 變更至 作用中	系統	NT AUTHORITY\SYSTEM
22.11.2023 10:1...	功能已變更	網路釣魚防護 狀態從 非作用中 變更至 作用中	系統	NT AUTHORITY\SYSTEM
22.11.2023 10:1...	功能已變更	網路隔離 狀態從 非作用中 變更至 已停用	系統	NT AUTHORITY\SYSTEM
22.11.2023 10:1...	功能已變更	電子郵件防護 狀態從 非作用中 變更至 作用中	系統	NT AUTHORITY\SYSTEM
22.11.2023 10:1...	功能已變更	Web 存取防護 狀態從 非作用中 變更至 作用中	系統	NT AUTHORITY\SYSTEM
22.11.2023 10:1...	功能已變更	通訊協定篩選 狀態從 非作用中 變更至 作用中	系統	NT AUTHORITY\SYSTEM
22.11.2023 10:1...	功能已變更	裝置控制 狀態從 非作用中 變更至 作用中	系統	NT AUTHORITY\SYSTEM
22.11.2023 10:1...	功能已變更	即時檔案系統防護 狀態從 非作用中 變更至 作用中	系統	NT AUTHORITY\SYSTEM
22.11.2023 10:1...	功能已變更	文件防護 狀態從 非作用中 變更至 已停用	系統	NT AUTHORITY\SYSTEM
22.11.2023 10:1...	功能已變更	指令碼掃描器模組 狀態從 非作用中 變更至 作用中	系統	NT AUTHORITY\SYSTEM
22.11.2023 10:1...	功能已變更	防勒索軟體 狀態從 非作用中 變更至 作用中	系統	NT AUTHORITY\SYSTEM
22.11.2023 10:1...	功能已變更	惡意探索封鎖程式 狀態從 非作用中 變更至 作用中	系統	NT AUTHORITY\SYSTEM
22.11.2023 10:1...	功能已變更	進階記憶體掃描器 狀態從 非作用中 變更至 作用中	系統	NT AUTHORITY\SYSTEM
22.11.2023 10:1...	功能已變更	HIPS 狀態從 非作用中 變更至 作用中	系統	NT AUTHORITY\SYSTEM
22.11.2023 10:0...	功能已變更	殭屍網路 狀態從 非作用中 變更至 作用中	系統	NT AUTHORITY\SYSTEM
22.11.2023 10:0...	功能已變更	網路攻擊防護 (IDS) 狀態從 非作用中 變更至 作用中	系統	NT AUTHORITY\SYSTEM
22.11.2023 10:0...	功能已變更	網路釣魚防護 狀態從 非作用中 變更至 作用中	系統	NT AUTHORITY\SYSTEM
22.11.2023 10:0...	功能已變更	網路隔離 狀態從 非作用中 變更至 已停用	系統	NT AUTHORITY\SYSTEM
22.11.2023 10:0...	功能已變更	Web 存取防護 狀態從 非作用中 變更至 作用中	系統	NT AUTHORITY\SYSTEM

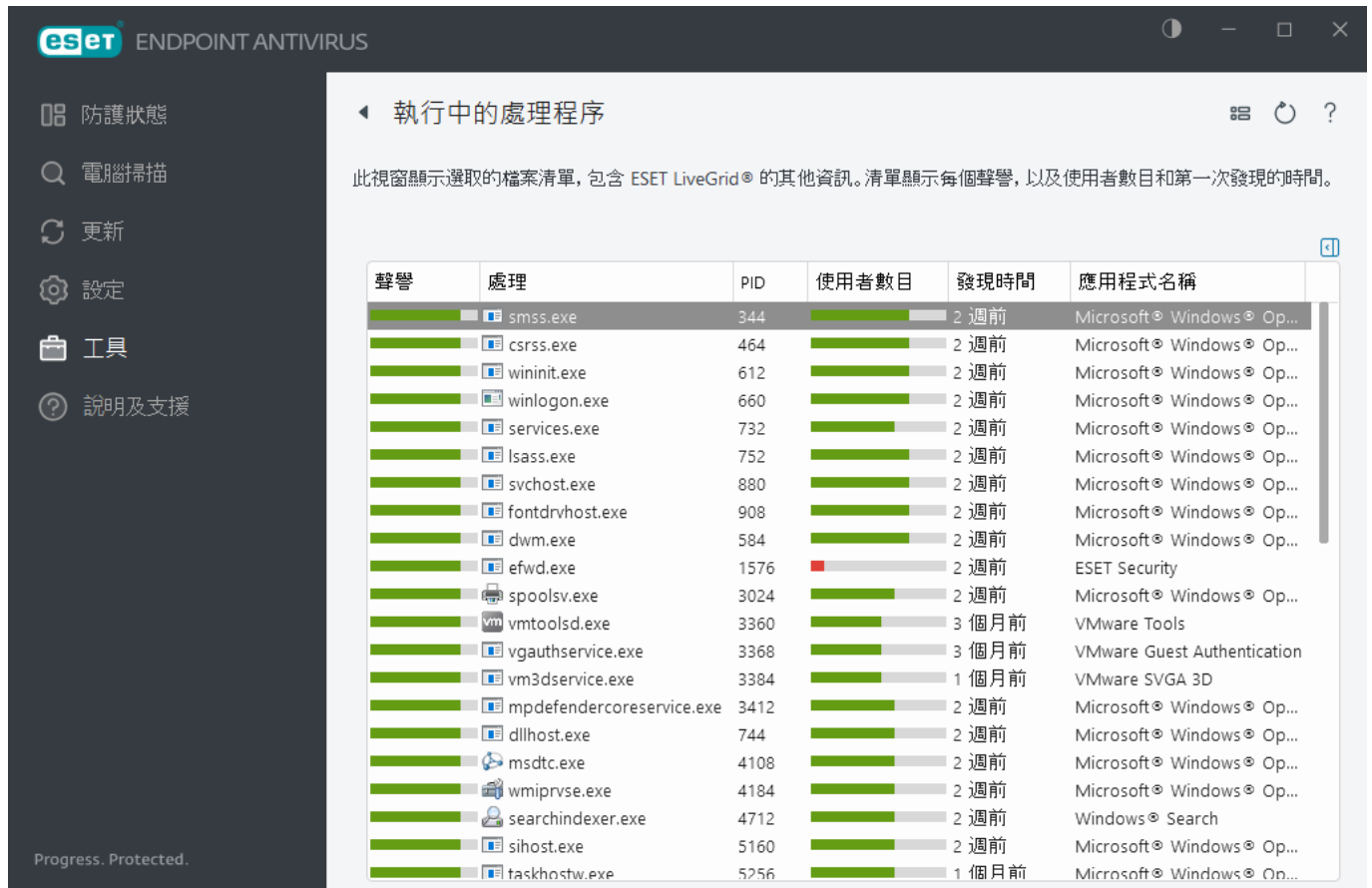
以滑鼠右鍵按一下 [防護記錄檔案] 視窗中審查防護記錄的任何 [已變更設定] 類型，然後從內容功能表選取 [顯示變更] 以顯示關於所執行變更的詳細資訊。此外，按一下內容功能表中的 [還原]（不適用於 ESET PROTECT 所管理的產品），即可還原設定變更。如果您從內容功能表選取 [全部刪除]，則會建立有關此動作詳細資訊的防護記錄。

若已在 [進階設定] > [工具] > [防護記錄檔案] 中啟用 [自動最佳化防護記錄檔案]，則審查防護記錄會如同其他防護記錄一樣自動重組。

若已在 [進階設定] > [工具] > [防護記錄檔案] 中啟用 [自動刪除超過指定（天數）的記錄]，將自動刪除超過指定天數的防護記錄項目。

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 Endpoint Antivirus 可提供執行中處理程序的詳細資訊，以啟用 ESET LiveGrid® 技術保護使用者。



聲譽	處理	PID	使用者數目	發現時間	應用程式名稱
綠色	smss.exe	344	2 週前	2 週前	Microsoft® Windows® Op...
綠色	csrss.exe	464	2 週前	2 週前	Microsoft® Windows® Op...
綠色	wininit.exe	612	2 週前	2 週前	Microsoft® Windows® Op...
綠色	winlogon.exe	660	2 週前	2 週前	Microsoft® Windows® Op...
綠色	services.exe	732	2 週前	2 週前	Microsoft® Windows® Op...
綠色	lsass.exe	752	2 週前	2 週前	Microsoft® Windows® Op...
綠色	svchost.exe	880	2 週前	2 週前	Microsoft® Windows® Op...
綠色	fontdrvhost.exe	908	2 週前	2 週前	Microsoft® Windows® Op...
綠色	dwm.exe	584	2 週前	2 週前	Microsoft® Windows® Op...
綠色	efwd.exe	1576	2 週前	2 週前	ESET Security
綠色	spoolsv.exe	3024	2 週前	2 週前	Microsoft® Windows® Op...
綠色	vmtoolsd.exe	3360	3 個月前	3 個月前	VMware Tools
綠色	vgauthservice.exe	3368	3 個月前	3 個月前	VMware Guest Authentication
綠色	vm3dservice.exe	3384	1 個月前	1 個月前	VMware SVGA 3D
綠色	mpdefendercoreservice.exe	3412	2 週前	2 週前	Microsoft® Windows® Op...
綠色	dllhost.exe	744	2 週前	2 週前	Microsoft® Windows® Op...
綠色	msdtc.exe	4108	2 週前	2 週前	Microsoft® Windows® Op...
綠色	wmiprvse.exe	4184	2 週前	2 週前	Microsoft® Windows® Op...
綠色	searchindexer.exe	4712	2 週前	2 週前	Windows® Search
綠色	sihost.exe	5160	2 週前	2 週前	Microsoft® Windows® Op...
綠色	taskhostw.exe	5256	1 個月前	1 個月前	Microsoft® Windows® Op...

聲譽 - 在大部分情況下，ESET Endpoint Antivirus 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 9 - 最佳聲譽（綠色）至 0 - 最差聲譽（紅色）的聲譽層級給物件。

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

PID - 是在 Windows 作業系統上執行程序的 ID。

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

使用者數目 - 使用指定應用程式的使用者數目。此資訊是由 ESET 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。

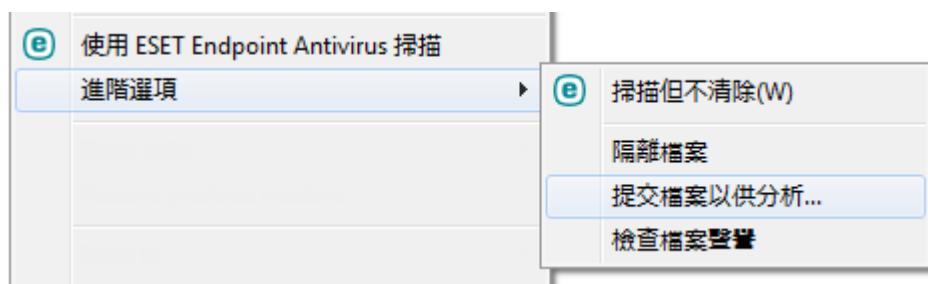
i 應用程式被標示為不明（橙色）安全等級時，不一定確定是惡意軟體。它通常只是新的應用程式。若您對檔案不確定，可以使用[提交檔案以供分析](#)功能來傳送檔案至 ESET 的病毒實驗室。若經證實，檔案為惡意的應用程式，則其偵測會新增到其中一個近期的偵測引擎更新。

應用程式名稱 - 程式或處理程序的指定名稱。

經由按一下最下方的指定應用程式，視窗底部會出現以下資訊：

- **路徑** - 電腦上應用程式的位置。
- **說明** - 根據作業系統說明的檔案特性。
- **版本** - 來自應用程式發行者的資訊。
- **公司** - 供應商或應用程式處理程序的名稱。
- **產品** - 應用程式名稱和/或商業名稱。
- **大小** - 單位為 kB 或 MB 的檔案大小。
- **建立日期** - 應用程式建立時的日期及時間。
- **修改日期** - 最近一次應用程式修改的日期及時間。

i 聲譽也可在不作為執行中程式/處理程序的檔案上檢查 - 標記您要檢查的檔案，並以滑鼠右鍵按一下這些檔案，然後從[內容功能表](#)選取 **[進階選項] > [使用 ESET LiveGrid® 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。
- **偵測到 PUA** - 顯示潛在不需要的應用程式 (PUA) 數目。
- **已掃描文件數** - 顯示已掃描的文件物件數目。
- **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。

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 Endpoint Antivirus 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](#)] > [**互動警告**] > [**確認訊息**] 中的 [**重設統計之前詢問**] 選項。

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。您也可以按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 檔。

排程器

排程器使用預先定義的配置與屬性管理及啟動已排程的工作。

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

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

依預設，下列排定工作會顯示在 **[排程器]** 中：

- 防護記錄維護
- 定期自動更新
- 撥號連線後自動更新
- 使用者登入後自動更新
- 啟動檔案自動檢查（使用者登入後）
- 啟動檔案自動檢查（模組更新成功之後）

1 在 ESET PROTECT 中，「隨機執行工作延遲」可用於在執行工作時減輕伺服器負載，尤其是在較大的網路上。此選項可讓您定義要在整個網路上執行工作的時間範圍，與同時在整個網路的所有工作站上執行工作相反。執行工作時，會隨機分割設定的時間值，以便將唯一的工作執行時間分配給網路上每個工作站。這有助於防止伺服器超載並發生相關問題（例如部分伺服器在整個網路的工作站上同時執行大量更新時，回報發生 DoS 攻擊）。

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



新增工作

- 按一下視窗底部的 **[新增工作]**。
- 輸入工作名稱。
- 從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** - 更新偵測引擎與程式模組來排程更新工作。
- 若您要啟用工作，則請開啟 **[已啟用]** 選項（您可以稍後在已排程工作清單中選取/取消選取核取方塊以完成開啟），接著按一下 **[下一步]**，並選取其中一個時間選項：
 - 一次** - 工作將在預先定義的日期及時間執行。
 - 重複** - 工作將在指定的時間間隔內執行。
 - 每日** - 工作會重複每天在指定的時間執行。
 - 每星期** - 工作將在選取的日期及時間執行。
 - 事件觸發** - 工作會在指定的事件發生時執行。
- 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）

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 [顯示工作詳細資料]²

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。

您可以使用下拉式功能表設定在掃描結束後自動執行處理方法：

- **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。
- **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。
- **需要時重新開機** - 電腦僅在需要完全清除偵測到的威脅時才重新開機。
- **[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。
- **需要時強制重新開機** - 電腦僅在需要完全清除偵測到的威脅時才重新開機。
- **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。

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](#)²

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]²

- **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。

提交樣本以供分析

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)。

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)。

樣本提交可讓您使用下列方法之一將檔案或網站傳送至 ESET 以供分析：

1. 在 [工具] > [提交樣本以供分析] 中可找到樣本提交對話方塊。
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/ZIP 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. 若要報告垃圾郵件或垃圾郵件誤判，請參閱我們的 [ESET 知識庫文章](#)

開啟 [選取樣本以供分析] 後，從 [提交樣本的原因] 下拉式功能表中選取最符合您訊息的說明：

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

檔案/網站 - 要提交的檔案或網站路徑。

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

i 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，並註明您在何種狀況下發現這個檔案。

附註與其他資訊 - 您可以在這裡輸入其他資訊或說明，這在識別可疑檔案的處理過程將會很有助益。

i 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對於樣本的識別處理程序。

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** - 通常用於騙取像是銀行帳號或 PIN 碼等敏感資料。請在[字彙](#)中閱讀更多有關此類型攻擊的資訊。
- **詐騙** - 詐騙或詐欺網站，專門為了快速獲取利益。
- 如果上述選項並不符合您要提交的網站，請選取 [其他]

附註與其他資訊 - 您可以在這裡輸入其他資訊或說明，這對於分析可疑網站將會很有助益。

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。

i 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。

隔離區

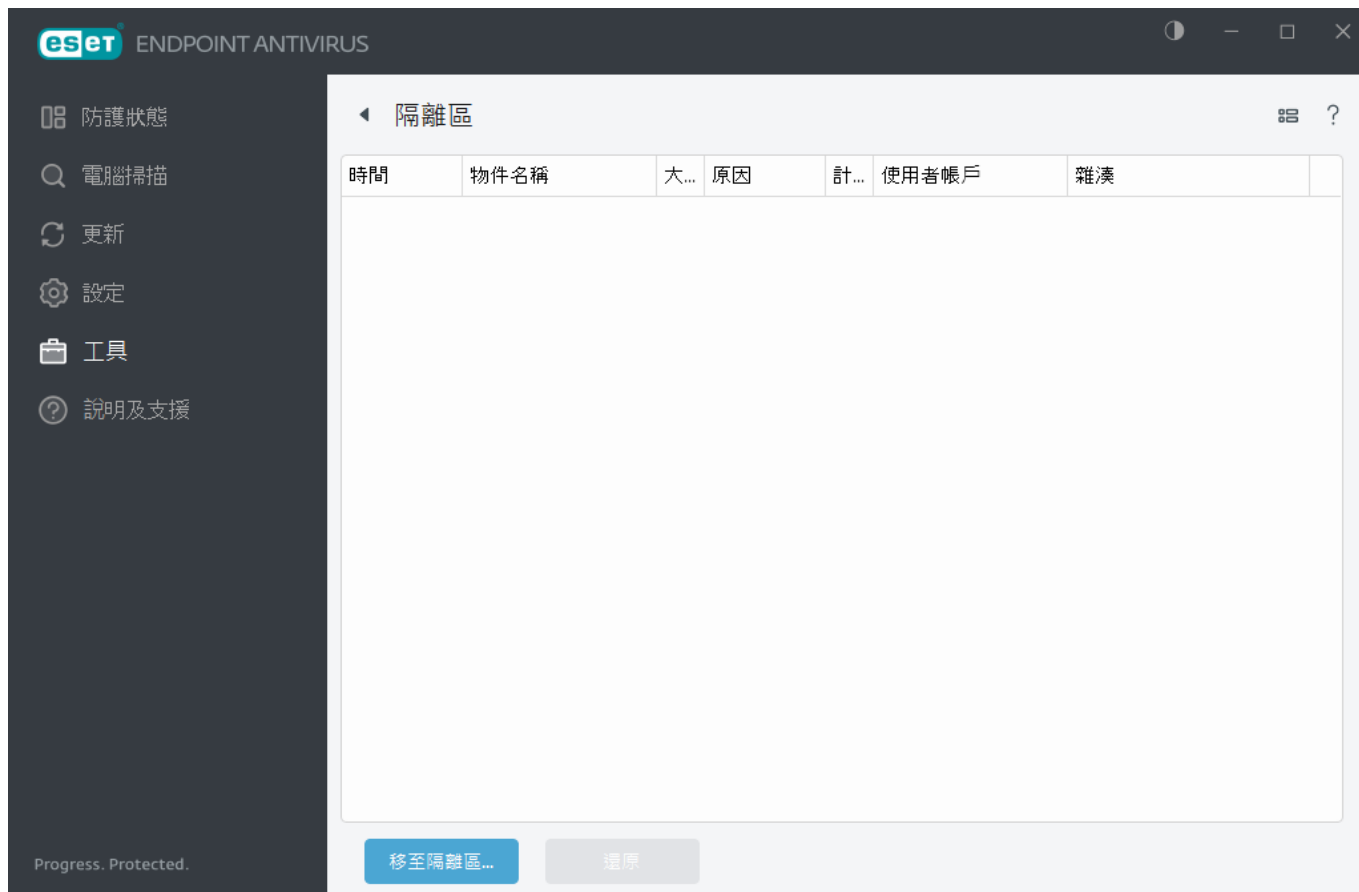
隔離區的主要功能是安全地儲存已報告的物件（例如惡意軟體、受感染的檔案或潛在不需要的應用程式）。

按一下 [工具] > [隔離區]，即可從 ESET Endpoint Antivirus 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）。

[我從遠端管理用戶端工作站上的隔離區](#)



隔離檔案

ESET Endpoint Antivirus 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：

- 無法清除、
- 若檔案不安全或建議刪除、
- 若檔案被 ESET Endpoint Antivirus 錯誤地偵測到、
- 或者如果檔案行為可疑但未被[掃描器](#)檢測到。

若要隔離檔案，您有多個選項：

- 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。
- 從主程式視窗中按一下 [\[移至隔離區\]](#)
- 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]**。您也可以選取多個項目，將其一起刪除。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]**。



下列 ESET 知識庫文章可能僅以英文提供：

- [管理 ESET PROTECT 中的隔離區](#)
- [我的 ESET 產品已向我發送偵測通知，我該做些什麼？](#)

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。



已安裝的產品

- [\[關於 ESET Endpoint Antivirus\]](#) - 顯示 ESET Endpoint Antivirus 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。
- [授權疑難排解](#) - 按一下此連結以尋找啟動或授權變更問題的解決方案。
- [變更授權](#) - 按一下以啟動 **[啟動]** 視窗，並啟動您的產品。



說明頁面 - 按一下此連結以啟動 ESET Endpoint Antivirus 說明頁面。



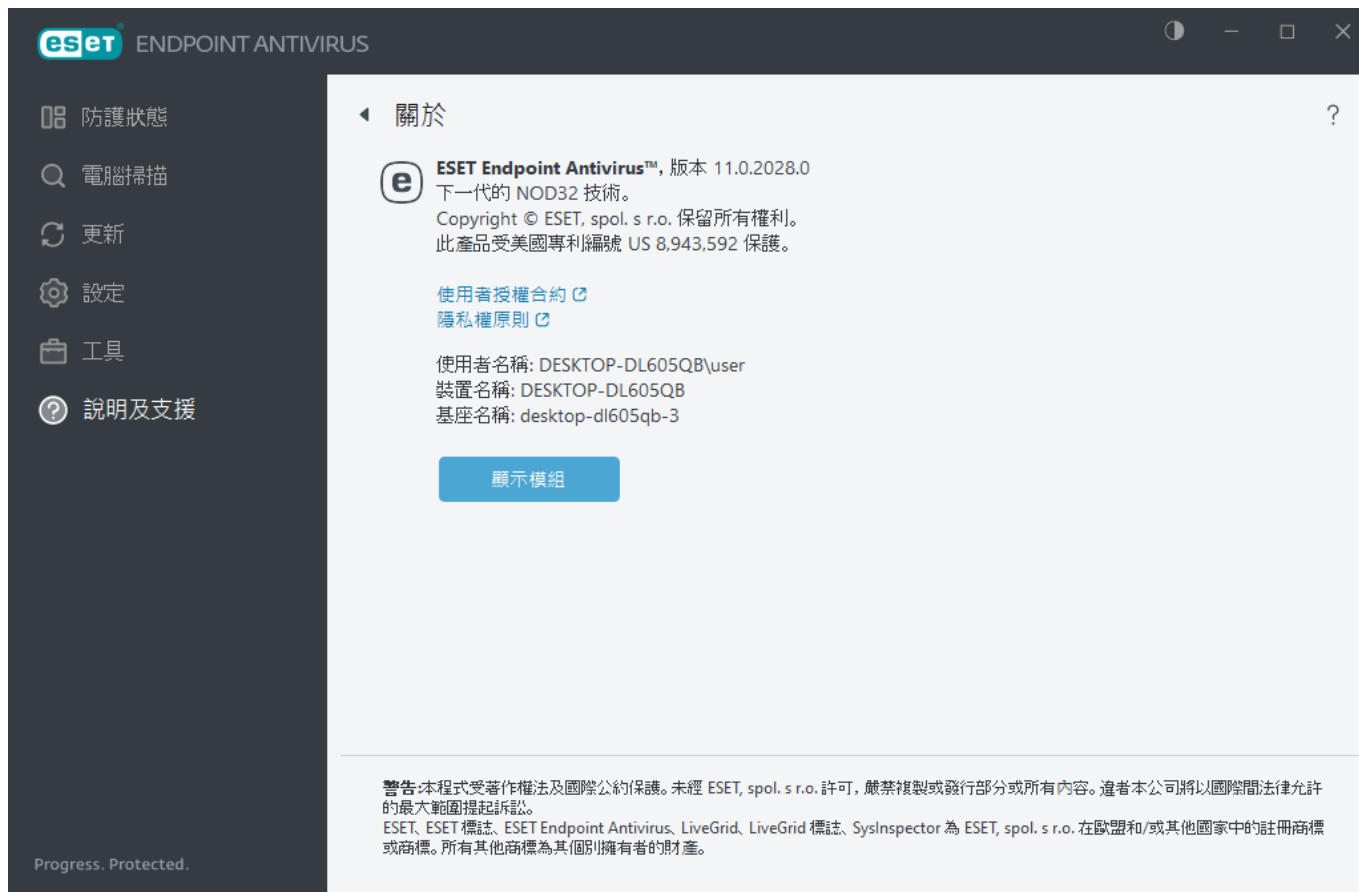
[技術支援](#)



[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 Endpoint Antivirus

此視窗會提供已安裝的 ESET Endpoint Antivirus 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。

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 Endpoint Antivirus 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（例如授權詳細資料、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。

進階設定

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

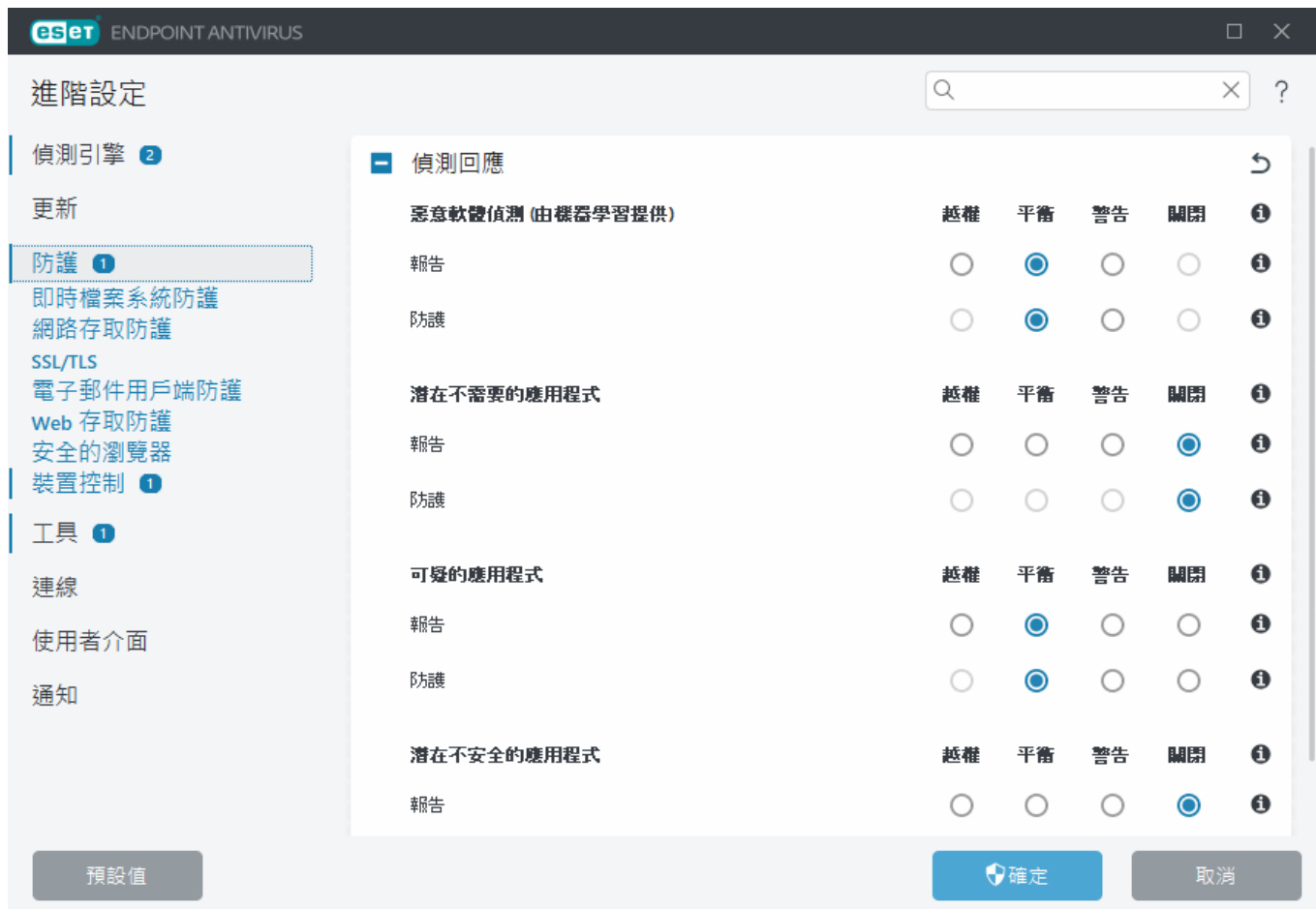
若要開啟進階設定，請開啟[主程式視窗](#)，然後按鍵盤上的 **[F5]** 鍵或按一下 **[設定] > [進階設定]**。

i 從 ESET PROTECT Web 主控台建立原則時，您可以為每一個設定選取旗標。含強制旗標的設定具有優先權，無法由較新的原則覆寫（即使較新的原則含有強制旗標）。這確保將不會變更此設定（例如，由使用者或在合併期間由更新的原則變更）。如需詳細資訊，請參閱 [ESET PROTECT 線上說明中的旗標](#)。

i 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](#)



偵測引擎

[[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](#)] 可讓您從偵測引擎中排除物件。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，從清除中排除物件。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](#)

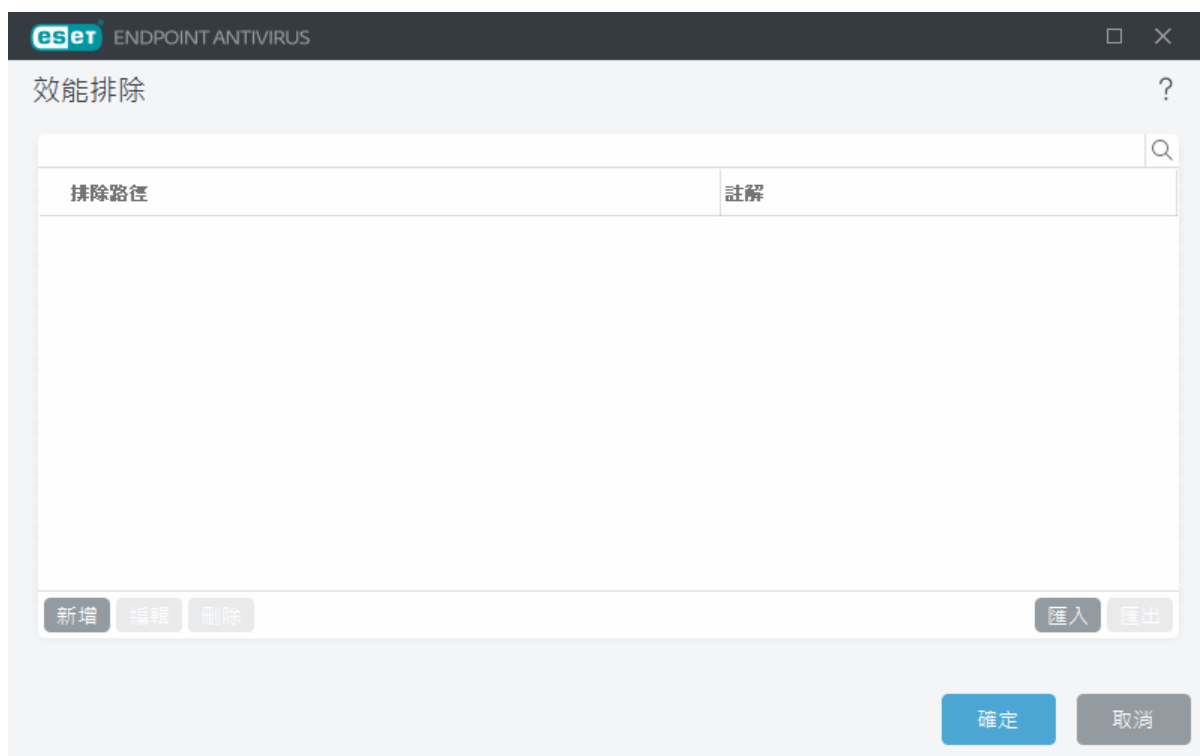
效能排除

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。

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。



i 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]** - 新增要從掃描中排除物件的項目。
- **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)。
- **[匯入]/[匯出]** - 如果您需要備份目前的排除以供日後使用，則匯入與匯出效能排除十分有用。匯出設定選項對未受管理的環境中想要在各個系統上使用慣用配置的使用者也很方便，他們可以輕鬆匯入 .txt 檔案以傳送這些設定。

[^ 顯示匯入/匯出檔案格式的範例](#)

```
# {"product":"endpoint","version":"10.0.2034","path":"Settings.ExclusionsManagement.PerformanceExclusions","columns":["Path","Description"]}
```

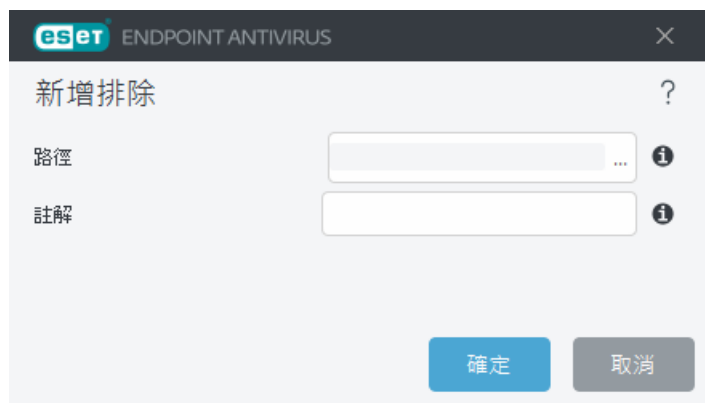
```
C:\Backup\*,custom comment
```

```
C:\pagefile.sys
```

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）。

i 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。

- 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???.exe）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。

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%`）

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。

- ! 如需詳細資訊，請參閱下列[知識庫文章](#)。
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。
- ✓ 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。

- 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。

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%`

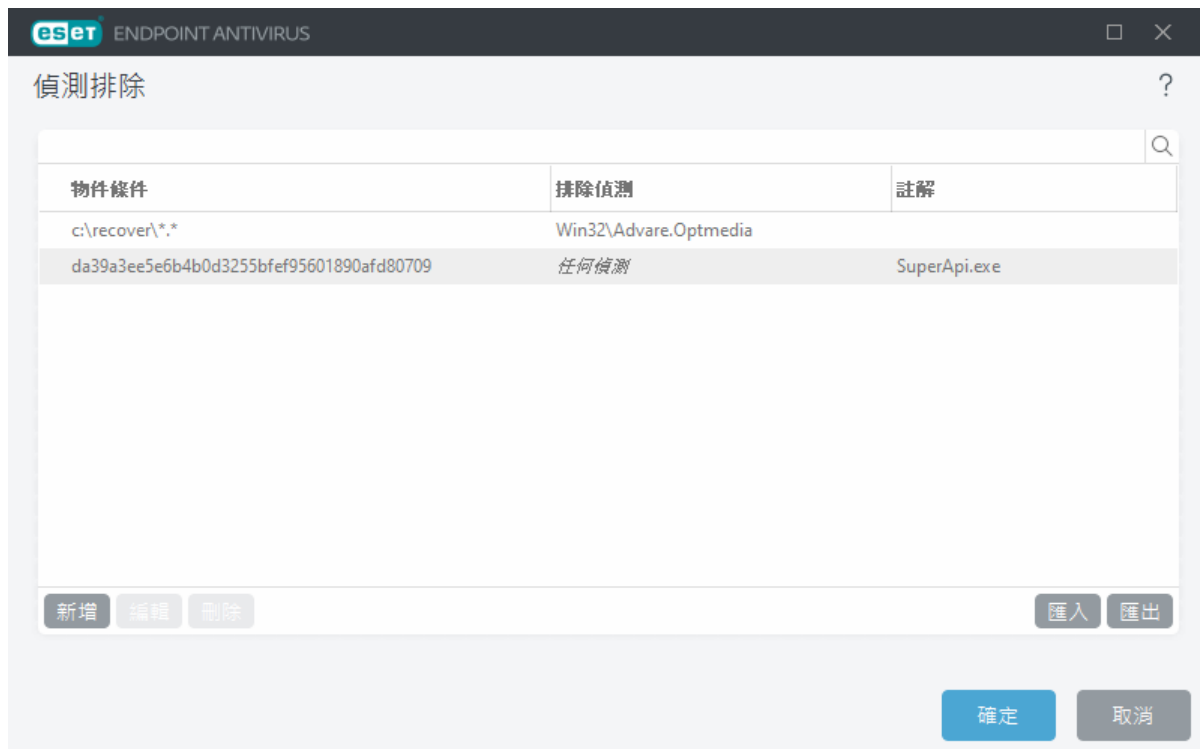
不支援使用者特有的系統變數（如 `%TEMP%` 或 `%USERPROFILE%`）或環境變數（如 `%PATH%`）。

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，從清除中排除物件。

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。

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]²

若要從清除中[排除物件 \(依其偵測名稱或雜湊\)](#)，請按一下 [\[新增\]](#)²

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 [\[排除對此文件的掃描\]](#)）²
- 從 [防護記錄檔案] 內容功能表來使用[建立偵測排除精靈](#)²
- 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 [\[還原並從掃描中排除\]](#)²

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。

控制項元素

- **[新增]** - 新增要從清除中排除物件的項目。
- **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)。
- **[匯入]/[匯出]** - 如果您需要備份目前的排除以供日後使用，則匯入與匯出偵測排除十分有用。匯出設定選項對未受管理的環境中想要多個系統上使用慣用配置的使用者也很方便，他們可以輕鬆匯入 .txt 檔案以傳送這些設定。

 [顯示匯入/匯出檔案格式的範例](#)

```
# {"product":"endpoint","version":"10.0.2034","path":"Settings.ExclusionsManagement.DetectionExclusions","columns":["Id","Path","ThreatName","Description","File Hash"]}
```

```
4c59cd02-357c-4b20-a0ac-ca8400000001,,,SuperApi.exe,00117F70C86ADB0F979021391A8AEAA497C2C8DF
```

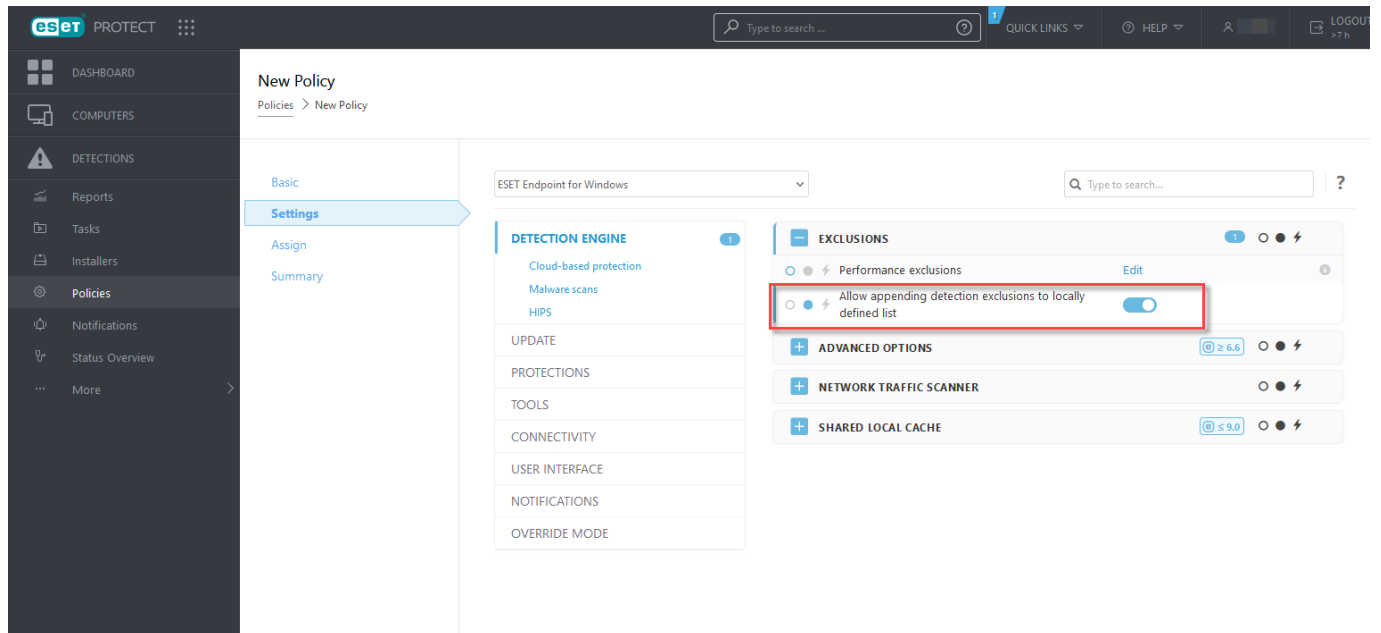
```
2c362ac8-a630-496e-9665-c76d00000001,C:\Recovery\*.*,Win32/Adware.Optmedia,
```

ESET PROTECT 中的偵測排除設定

ESET PROTECT [偵測排除管理精靈](#) - 建立偵測排除並將其套用至其他電腦/群組。

來自 ESET PROTECT 的可能偵測排除覆寫

若目前有偵測排除本機清單，管理員必須套用一個原則，[\[允許將偵測排除附加到本機定義的清單\]](#)。此後，從 ESET PROTECT 附加偵測排除將如預期運作。

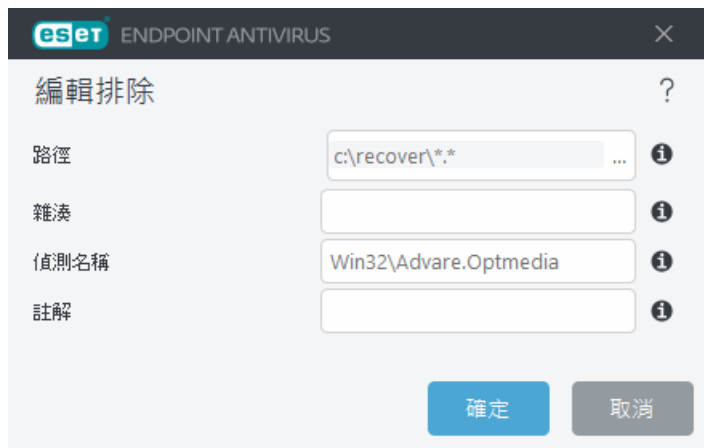


新增或編輯偵測排除

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 Endpoint Antivirus 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。



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 Endpoint Antivirus 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) 和 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) 和 POP3(S) 和 IMAP(S) 通訊協定。請注意，以下 ESET Endpoint Antivirus 功能需要啟用網路流量掃描器：

- [Web 存取防護](#)
- [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。透過全球提供可疑樣本和中繼資料的方式，ESET LiveGrid® 可讓我們立即回應客戶需求，並讓 ESET 隨時掌握最新威脅情報。

可用選項如下：

選項1：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。

選項2：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、日期與時間、威脅出現在電腦上的程序，以及電腦作業系統的相關資訊。

依預設，ESET Endpoint Antivirus 配置為將可疑檔案提交至 ESET 病毒實驗室以供詳細分析。某些副檔名的檔案，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。

選項3：您可以選擇不要啟用 ESET LiveGrid®

您不會失去軟體的任何功能，但在有些情況下，當 ESET LiveGrid® 啟用時，ESET Endpoint Antivirus 可能會比偵測引擎更新更快回應新威脅。

請在[字彙](#)中閱讀更多有關 ESET LiveGrid® 的資訊。

i 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 Endpoint Antivirus 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。

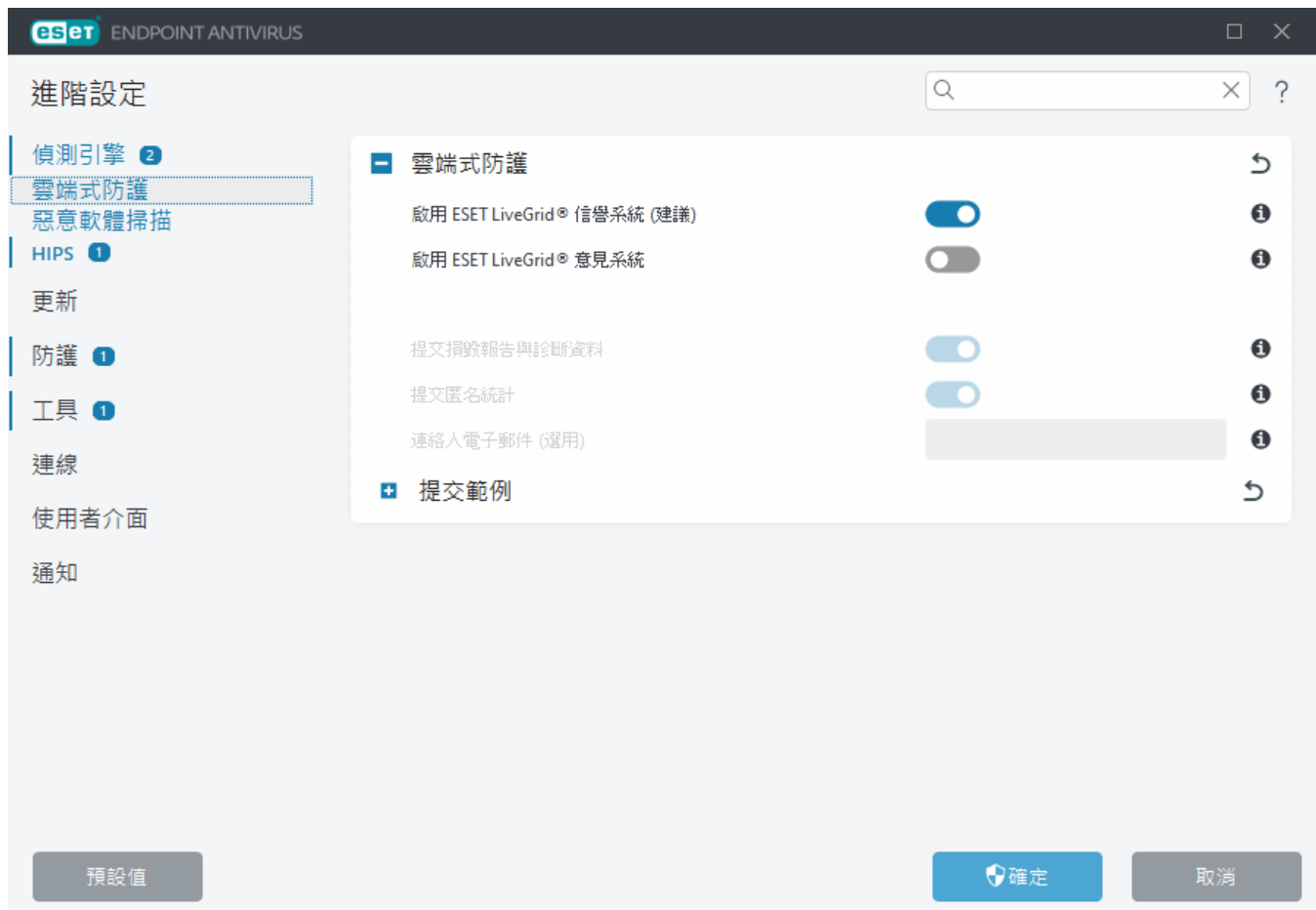
[啟用 ESET LiveGrid® 意見系統] – 將相關的提交資料（如以下 [\[提交樣本\]](#) 區段所述）連同當機報告及統計資料傳送至 ESET 研究實驗室，以進行進一步的分析。

啟用 ESET LiveGuard ([ESET LiveGuard](#) 是 ESET 銷售的附加功能，預設無法使用) – ESET LiveGuard 是 ESET 提供的付費服務。其目的在於新增專門設計的保護層，以緩解目前失控的新威脅。可疑的檔案會自動提交給 ESET 雲端。在雲端中，我們的[進階惡意軟體偵測引擎](#)會分析它們。提供範例的使用者將收到行為報告，其中提供所觀察到之範例行為的摘要。

[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。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 Endpoint Antivirus [防護模組](#)將這些範例視為可疑或有不明企圖的行為。

- **[可執行檔]** - 包括檔案如 .exe, .dll, .sys
- **[壓縮檔]** - 包括檔案類型如 .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab
- **[指令碼]** - 包括檔案類型如 .bat, .cmd, .hta, .js, .vbs, .ps1
- **[其他]** - 包括檔案類型如 .jar, .reg, .msi, .sfw, .lnk
- **[可能的垃圾郵件]** - 這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 [\[進階設定\]](#) > [\[雲端型防護\]](#) > [\[提交樣本\]](#) > [\[排除\]](#)，然後新增排除 *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)

ESET LiveGuard

若要在用戶端機器上使用 ESET LiveGuard Web 主控台啟用 ESET PROTECT，請參閱 [ESET Endpoint Antivirus 的 ESET LiveGuard 配置](#)

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。

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。

i 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](#)

[指定掃描 & 偵測回應] – 您可以為每個掃描設定檔設定報告和防護等級。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 Endpoint Antivirus 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。

i 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穩的應用程式](#)，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 Endpoint Antivirus 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 Endpoint Antivirus 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。
- **強制裝置掃描** – 已插入的卸除式媒體裝置將會執行電腦掃描，且無法取消。
- **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。

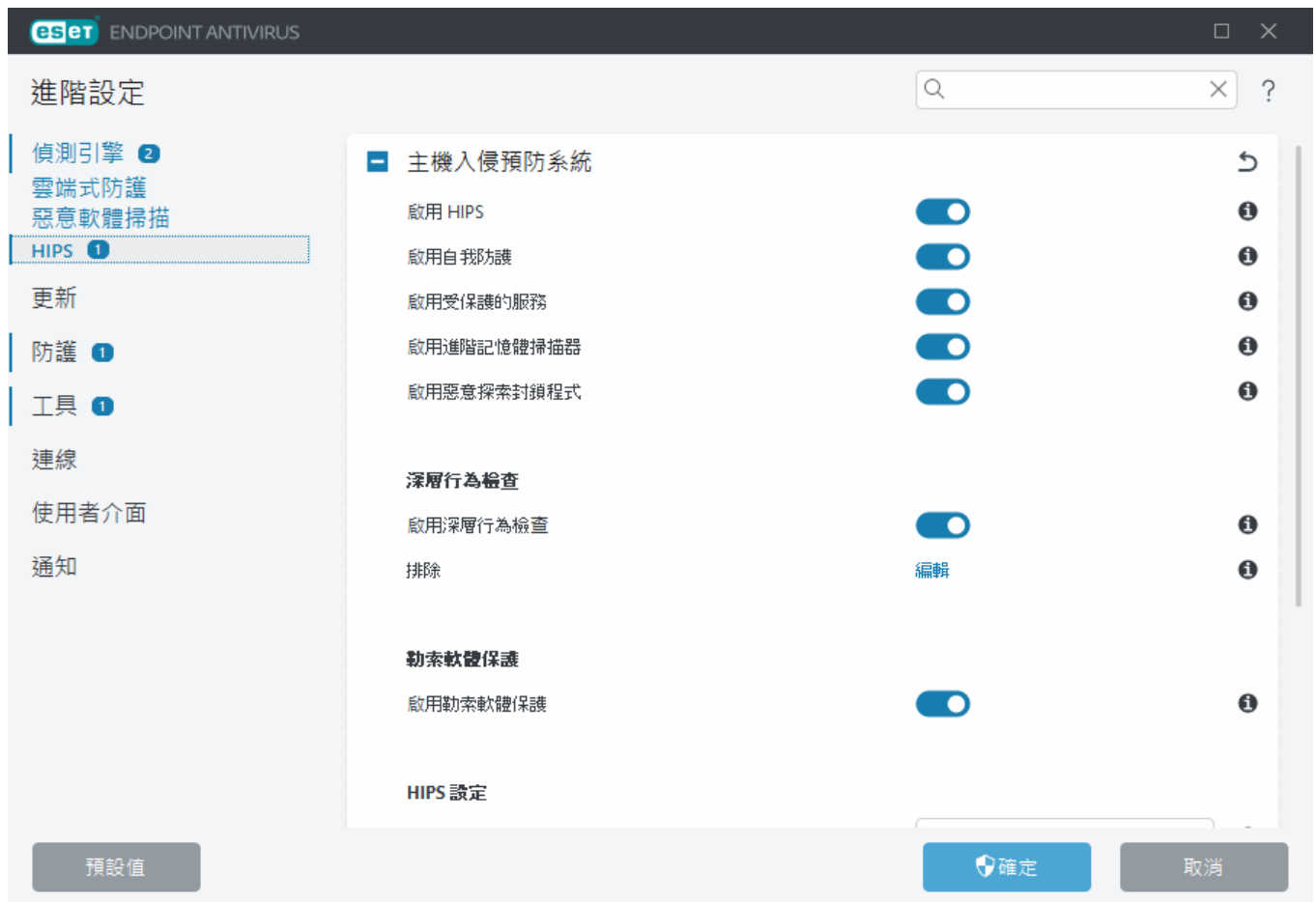
 使用 Microsoft Antivirus API 的應用程式 (例如 Microsoft Office 2000 與更新版本，或 Microsoft Internet Explorer 5.0 與更新版本) 可啟動此功能。

HIPS – 主機入侵預防系統

 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 Endpoint Antivirus [主程式視窗](#) > [\[設定\]](#) > [\[電腦\]](#) 中。



主機入侵預防系統

啟用 HIPS - 依預設會在 ESET Endpoint Antivirus 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 Endpoint Antivirus 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。ESET Management 代理程式也會在安裝後受到保護。

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。Windows 8.1 和 Windows 10 中提供此功能。

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](#)。

啟用審核模式 - 系統不會自動封鎖勒索軟體保護偵測到的項目，但會以警告嚴重性來記錄這些項目並使用「審核模式」旗標將項目傳送至管理主控台。管理員可以決定排除這類偵測來避免進一步偵測，或讓這類偵測保持作用中，這表示在審核模式結束後，這類偵測就會遭封鎖且移除。啟用/停用審核模式也會登入在 ESET Endpoint Antivirus 僅在 ESET PROTECT 原則組態編輯器中可使用此選項。

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 [\[進階設定\]](#) > [\[偵測引擎\]](#) > [\[HIPS\]](#) > [\[主機入侵預防系統\]](#) > [\[排除\]](#) > [\[編輯\]](#)。

i 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。

i 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。

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

i 一律允許載入驅動程式特定於每個裝置，無法使用 ESET PROTECT 原則進行編輯。安裝後，驅動程式清單為空白 ESET Endpoint Antivirus 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或 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：

- **建立僅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** - 選取規則檔案/應用程式/登錄作業。[請參數所有 HIPS 作業的說明](#)²
- **僅適用於目標** - 選取規則檔案/應用程式/登錄目標。



若要停止顯示通知，請在 **[進階設定]** > [\[偵側引擎\]](#) > **[HIPS]** > **[基本]** 中將過濾模式變更為 **[自動模式]**²



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]**²



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

這是 HIPS 系統中使用者定義且自動新增的規則清單。如需關於規則建立和 HIPS 作業的詳細資訊，請參閱 [HIPS 規則設定](#) 一章。另請參閱 [HIPS 的一般原則](#)²

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，請停用此選項。

處理方法 - 此規則指定在條件符合時應執行的處理方法 - **[允許]**²**[封鎖]** 或 **[詢問]**²

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](#)²

通知 - 若觸發事件，右下角會出現一個通知。

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。

- 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）

HIPS 規則設定

請先參閱 [HIPS 規則管理](#)²

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]**²**[封鎖]** 或 **[詢問]**²

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](#)²

通知 - 若觸發事件，右下角會出現一個通知。

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**

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。從下拉式功能表中選取 [特定項目]，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 [所有項目] 以新增所有應用程式。

i 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。

i 指定路徑時 `C:\example` 會影響與資料夾本身的動作，而 `C:\example*.*` 會影響資料夾中的檔案。

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。

在規則中使用萬用字元

規則中的星號只能用來取代取特定機碼，例

如“`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet*\Start`”不支援其他使用萬用字元的方式。

i 建立將 HKEY_CURRENT_USER 機碼設為目標的規則

此機碼只會連結至 SID (安全識別碼) 所識別之使用者特有的適當 HKEY_USERS 子機碼。為了只對目前使用者建立規則，而不是使用 HKEY_CURRENT_USER 的路徑，請使用指向 HKEY_USERS\%SID% 的路徑。您可以使用星號作為 SID 讓規則適用於所有使用者。

⚠ 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】** 切換選項，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。



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 HTTPS 通訊）。

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。

[配置更新通知] - 按一下 [編輯] 以選取要顯示哪些[應用程式通知](#)。您可以選擇通知為 [在桌面上顯示] 和/或 [透過電子郵件傳送]。

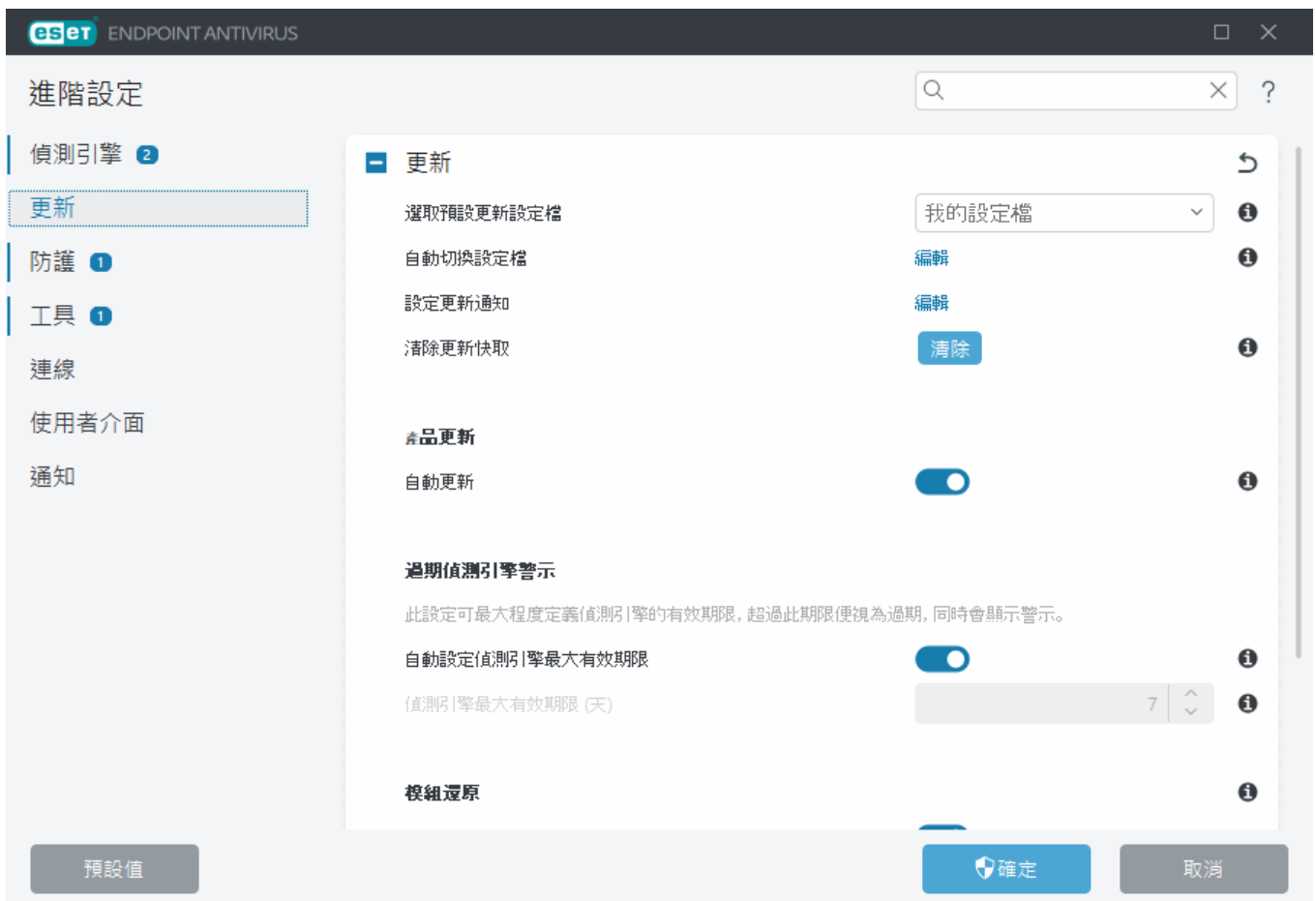
如果您在嘗試下載模組更新時遇到困難，請按一下 [清除更新快取] 旁的 [清除] 以清除暫時更新檔案/快取。

過期偵測引擎警示

自動設定偵測引擎有效期限 - 允許設定時間上限（以天計），超過期限後，偵測引擎會回報過期。[偵測引擎有效期限（天數）] 的預設值為 7。

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。



■ 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]²

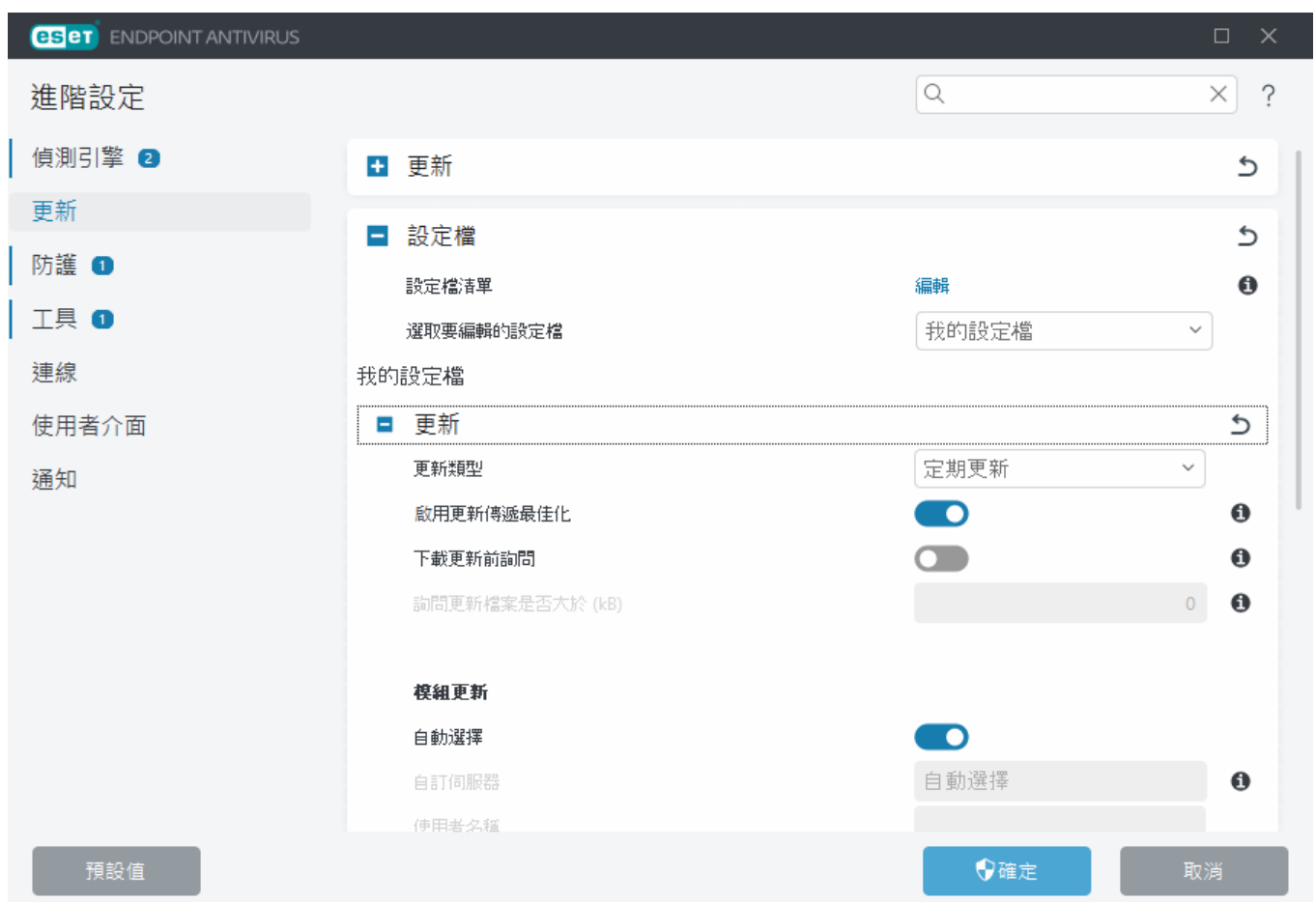
若要建立新設定檔，請按一下 [設定檔清單] 旁的 [編輯]，輸入您自己的 [設定檔名稱]，然後按一下 [新增]²

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。[延遲更新] 允許從特殊更新伺服器更新，該伺服器會延遲至少 X 小時再提供新版的病毒資料庫（亦即資料庫已在實際環境中測試，因此可視為穩定）。

[啟用更新傳遞最佳化] - 啟用之後，可以從 CDN (內容傳遞網路) 下載更新檔案。如果專用的 ESET 更新伺服器超載，停用此設定可能導致下載中斷和速度減慢。當防火牆限制為只存取 [ESET 更新伺服器 IP 位址](#)，或無法連線至 CDN 服務時，停用很有用。

[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。若更新檔案大小超過 [詢問更新檔案是否大於 (kB)] 欄位中指定的值，程式將顯示確認對話方塊。若更新檔案大小設為 0 kB²則程式將一律顯示確認對話方塊。



模組更新

依預設會啟用 **[自動選擇]** **[自訂伺服器]** 選項是儲存更新的位置。若您使用 ESET 更新伺服器，我們建議您讓預設選項保持選取狀態。

[啟用更頻繁的偵測簽章更新] - 偵測簽章會在更短的時間內更新。停用此設定可能會對偵測速率造成負面影響。

允許從卸除式媒體進行模組更新 - 可讓您透過包含建立映像的卸除式媒體進行更新。選取 **[自動]** 時，更新將在背景執行。若您想顯示更新對話，請選取 **[一律詢問]**。

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

`http://電腦名稱或其_IP_位址:2221`

當透過 SSL 使用本機 HTTP 伺服器時，更新伺服器應設定如下：

`https://電腦名稱或其_IP_位址:2221`

當使用本機共用資料夾時，更新伺服器應設定如下：

`\\電腦名稱或其_IP_位址\共用資料夾`

i 上述範例中指定的 HTTP 伺服器連接埠號碼取決於 HTTP/HTTPS 伺服器所接聽的連接埠。

產品更新

請參閱 [產品更新](#)

連線選項

請參閱 [連線選項](#)

更新映像

請參閱 [更新映像](#)

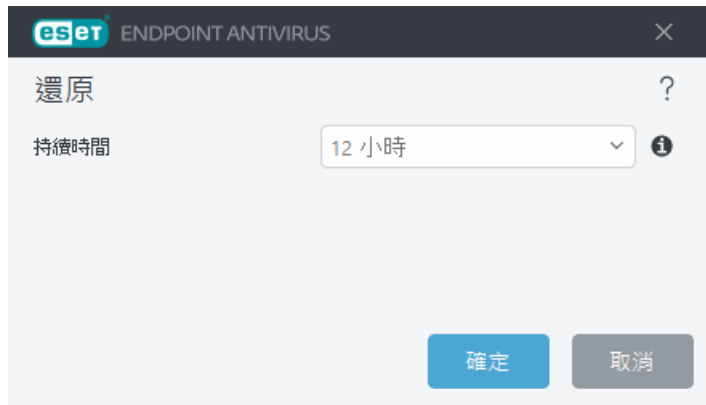
更新還原

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 Endpoint Antivirus 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。

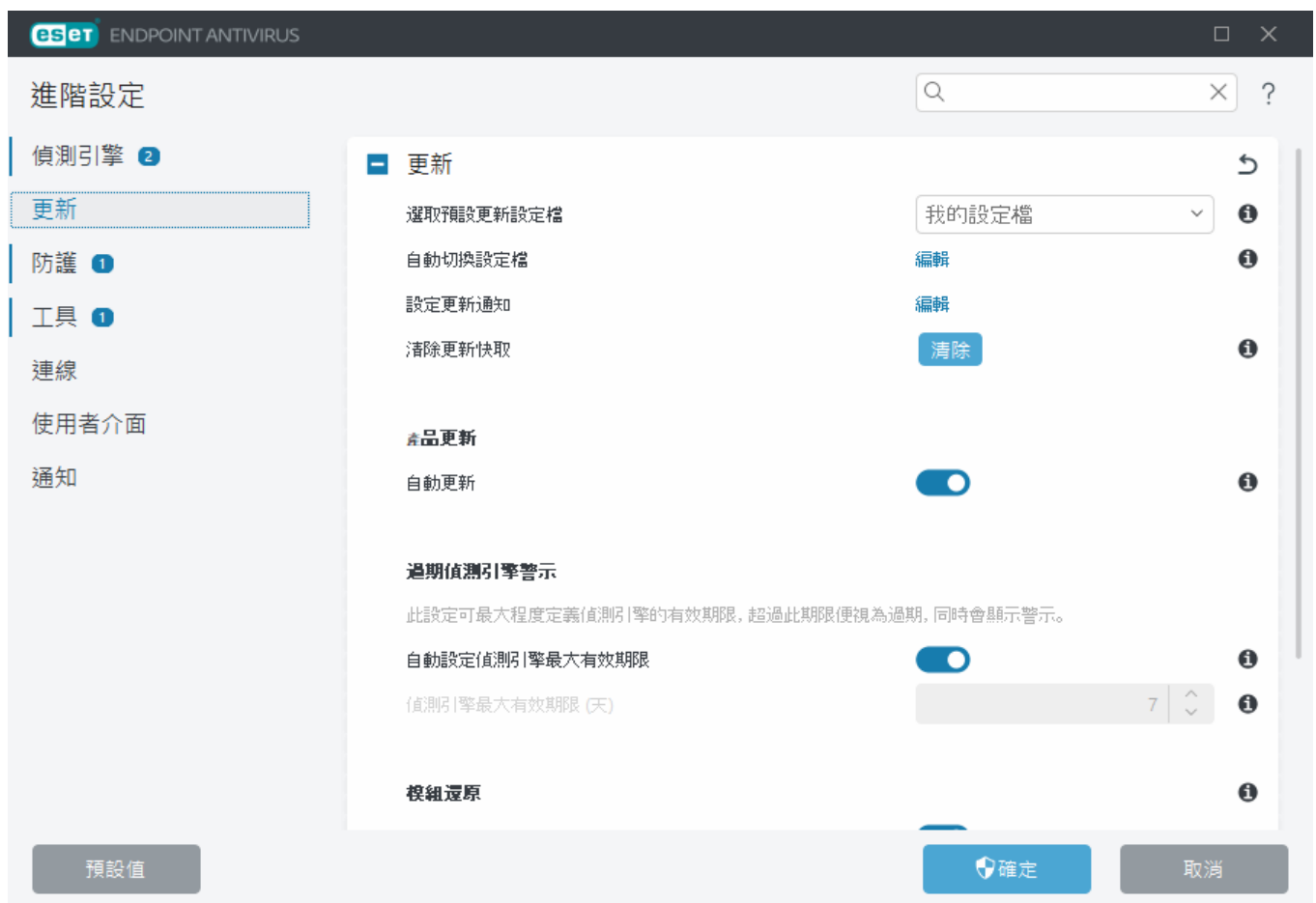
i 當達到最大快照量（例如三個）時，最舊的快照將每 48 小時替換為一個新的快照。ESET Endpoint Antivirus 會將偵測引擎程式模組更新版本還原至最舊的快照。

開啟 [\[進階設定\]](#) > **[更新]** > **[更新]** > **[模組還原]** > **[還原]** 從 **[持續時間]** 下拉式功能表中選取時間間隔。



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

如果還原已執行，則 **「還原」** 按鈕會變成 **「允許更新」**。不允許在從 **「暫停更新」** 下拉式功能表中選取的時間間隔內進行更新。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。

產品更新

[產品更新] 區段包含產品更新相關的選項。新產品更新可以升級時，程式可讓您預先定義其行為。

產品更新會提供新功能，或變更舊版已存在的功能。它可自動執行而無需使用者介入，或者您也可以選擇提前通知。安裝產品更新之後，可能需要重新啟動電腦。

自動更新 - 在使用其他網路或以計量付費連線來連線到網際網路時，暫停特定更新設定檔的自動更新會暫時停用自動產品更新。啟用此設定以持續存取最新的功能和儘可能高的防護。如需關於自動更新的詳細資訊，請參閱[自動更新常見問題](#)。

依預設，產品更新是從 ESET 存放庫伺服器下載。在大型或離線環境中，可以散佈流量來允許內部快取產品檔案。

定義程式元件更新的自訂伺服器

1. 在 **[自訂伺服器]** 欄位中定義產品更新的路徑。
該路徑可以是 HTTP(S) 連結、SMB 網路共用路徑、本機磁碟機或卸除式媒體路徑。對於網路磁碟機，使用 UNC 路徑而非對應的磁碟機代號。
2. 如非必要，請將 **[使用者名稱]** 和 **[密碼]** 空白。
如有必要，請在此定義適當的憑證，以便在自訂 Web 伺服器上進行 HTTP 驗證。
3. 確認變更，並使用標準 ESET Endpoint Antivirus 更新來測試產品更新是否存在。

i 選取最適當的選項需視將套用設定的工作站而定。請注意，工作站與伺服器之間有區別，例如，產品更新後自動重新啟動伺服器會導致公司蒙受重大損失。

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 [\[進階設定\]](#) > [\[更新\]](#) > [\[設定檔\]](#) > [\[更新\]](#) > [\[連線選項\]](#)。

Proxy 伺服器

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 Endpoint Antivirus。

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 **工具 > Proxy 伺服器** 中定義不相同的 Proxy 伺服器來更新 ESET Endpoint Antivirus。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 Endpoint Antivirus 將連接至 Proxy 伺服器進行更新。
- 電腦透過 Proxy 伺服器連接至網際網路。系統在程式安裝期間從瀏覽器取得設定，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

Windows 共用

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

若要配置這類帳戶，請從 **[以下列身分連接到區域網路]** 下拉式功能表選取：

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

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

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

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

[使用者名稱] 和 **[密碼]** 設定是選擇性的。



選取 **[目前使用者]** 或 **[指定使用者]** 選項時，如果將程式身分變更為所需使用者，則可能會發生錯誤。我們建議將區域網路 (LAN) 驗證資料輸入主要更新設定區段。在此更新設定區段中，驗證資料輸入應該如下所示：網域名稱\使用者（如果是工作群組，請輸入工作群組名稱\名稱）及密碼。當從本機伺服器 HTTP 版本更新時，不需要驗證。

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

更新映像

ESET Endpoint Antivirus 可讓您建立更新檔案的副本，可用於更新網路中的其他工作站。「映像」的功用 - LAN 環境中更新檔案的副本很方便，因為不需要由每個工作站從廠商更新伺服器重覆下載更新檔案。更新會下載至本機映像伺服器然後散佈至所有工作站，以避免網路流量超載風險。從映像更新用戶端工作站會最佳化網路負載平衡，節省網際網路連線頻寬。

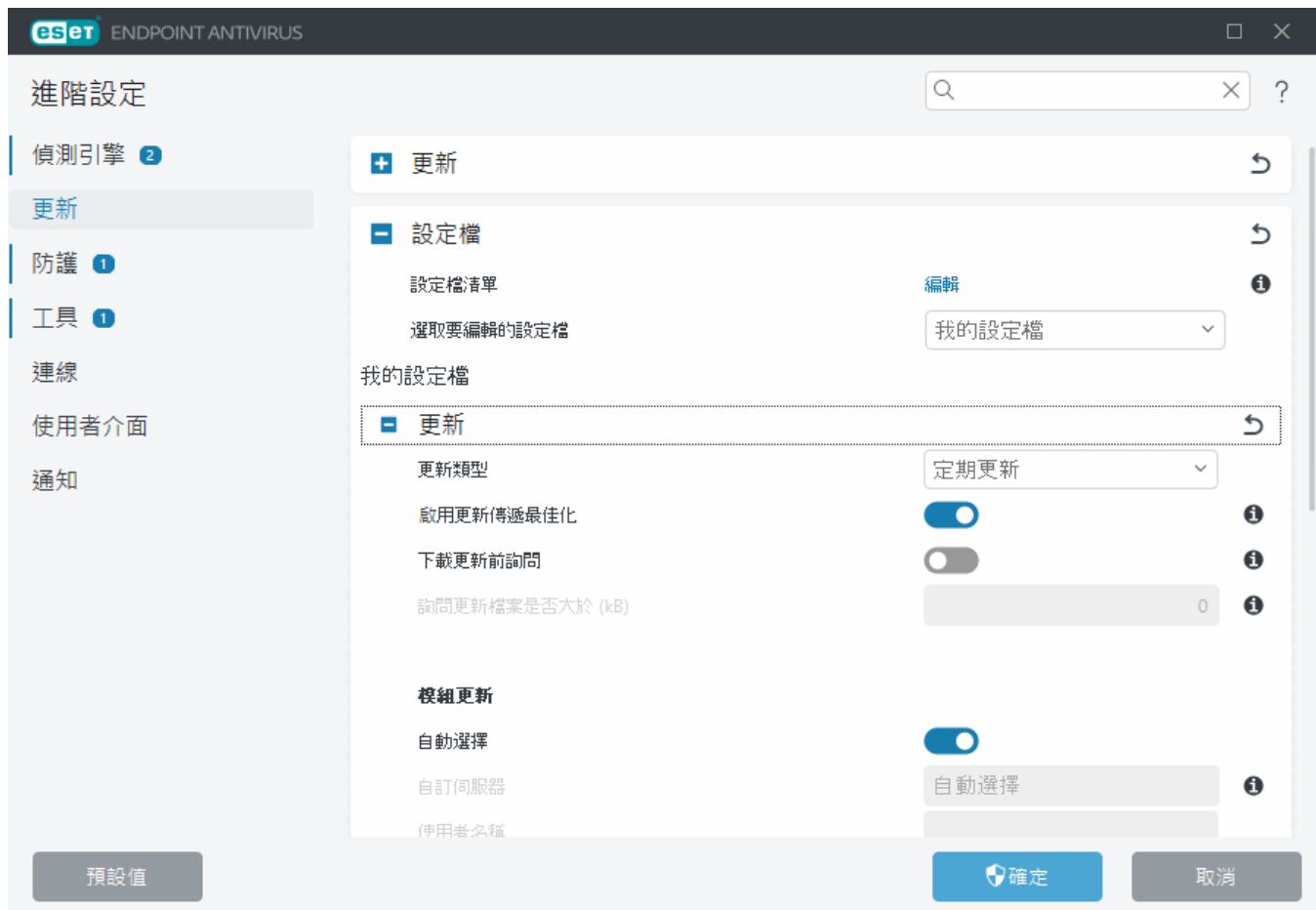


更新映像以建立更新檔案的副本，這些副本可用於更新執行相同世代的 ESET Endpoint Antivirus for Windows 的工作站。（例如 ESET Endpoint Antivirus for Windows 10.x 版僅為 ESET Endpoint Antivirus for Windows 和 ESET Endpoint Security for Windows 10.x 版建立更新檔案）



若要最大程度地減少使用 ESET PROTECT 管理大量用戶端的網際網路流量，建議您使用 ESET Bridge 而不是將用戶端配置為映像。可以使用全方位安裝程式或作為獨立元件透過 ESET PROTECT 安裝 ESET Bridge 有關 Apache HTTP Proxy 映像工具和直接連接之間的詳細資訊和區別，請參閱我們的 [ESET PROTECT 線上說明頁面](#)

本機映像伺服器的配置選項位於 **[進階設定] > [更新] > [設定檔] > [更新映像]** 中。



若要在用戶端工作站上建立映像，請啟用 **[建立更新映像]**。啟用此選項會啟動其他映像配置選項，例如存取更新檔案的方式及映像檔案的更新路徑。

存取更新檔案

[啟用 HTTP 伺服器] - 如果已啟用，則[透過 HTTP 即可存取](#)更新檔案，而且不需要憑證。

存取映像伺服器的方法在[從映像更新](#)中有詳細說明。現在有存取映像的兩個基本方法 - 含有更新檔案的資料夾可以顯示為共用網路資料夾，或用戶端可以存取 HTTP 伺服器上的映像。

專用於儲存映像更新檔案的資料夾定義於 **[儲存映像檔案的資料夾]** 下方。若要選擇不同的資料夾，請按一下 **[清除]** 以刪除預先定義的資料夾 `C:\ProgramData\ESET\ESET Endpoint Antivirus\mirror`，然後按一下 **[編輯]**，以瀏覽本機電腦上的資料夾或共用網路資料夾。如果需要指定資料夾的授權，必須在 **[使用者名稱]** 及 **[密碼]** 欄位中輸入驗證資料。如果選取的目標資料夾位於執行 Windows NT/2000/XP 作業系統的網路磁碟上，則指定的使用者名稱及密碼必須具有已選取資料夾的寫入權。使用者名稱的輸入格式應為網域/使用者或工作群組/使用者。請記得提供對應的密碼。

適用於映像的 HTTP 伺服器和 SSL

在 **[映像]** 索引標籤的 **[HTTP 伺服器]** 區段中，您可以指定 HTTP 伺服器將接聽的 **[伺服器連接埠]**，以及 HTTP 伺服器使用的 **[驗證]** 類型。依預設，伺服器連接埠設定為 **2221**。

驗證 - 定義用於存取更新檔案的驗證方法。可用選項如下：**[無]**、**[基本]** 及 **[NTLM]**。選取 **[基本]** 以使用具有基本使用者名稱及密碼驗證的 base64 編碼。**[NTLM]** 選項提供使用安全編碼方法的編碼。對於驗證，會使用共用更新檔案之工作站上建立的使用者。預設值為 **[無]**，這會授與對無需驗證之更新檔案的存取權。

i 驗證資料（例如 [使用者名稱] 及 [密碼]）僅用於存取映像 HTTP 伺服器。只有在需要使用者名稱及密碼時，才填寫這些欄位。

如果您想要執行支援 HTTPS (SSL) 的 HTTP 伺服器，請附加您的 [憑證連鎖檔案]，或產生自我簽署的憑證。以下為可用的憑證類型：ASN 和 PEM 和 PFX。為了額外的安全性，您可以使用 HTTPS 通訊協定以提供更新檔案以供下載。使用此通訊定幾乎不可能追蹤資料傳輸和登入憑證。[私密金鑰類型] 選項依預設設定為 [整合]（因此 [私密金鑰檔案] 選項會依預設停用）。這代表著私密金鑰是所選憑證連鎖檔案的一部分。

HTTPS 映像的自我簽署憑證

! 如果您使用 HTTPS 映像伺服器，則需要將其憑證匯入到所有用戶端電腦上受信任的根儲存區中。請參閱 Windows 中的 [安裝信任的系統管理員憑證](#)。

從映像更新

配置映像有兩個基本方法，映像實際上是一個存放庫，讓用戶端可以下載更新檔案。含有更新檔案的資料夾可以顯示為共用網路資料夾或 HTTP 伺服器。

! 更新映像以建立更新檔案的副本，這些副本可用於更新執行相同世代的 ESET Endpoint Antivirus for Windows 的工作站。（例如：ESET Endpoint Antivirus for Windows 10.x 版僅為 ESET Endpoint Antivirus for Windows 和 ESET Endpoint Security for Windows 10.x 版建立更新檔案）

使用內部 HTTP 伺服器存取映像

這是預先定義程式配置中指定的預設配置。若要允許使用 HTTP 伺服器存取映像，請瀏覽至 [\[進階設定\]](#) > [\[更新\]](#) > [\[設定檔\]](#) > [\[更新映像\]](#)，並選取 [\[建立更新映像\]](#)。

在 [映像] 索引標籤的 [HTTP 伺服器] 區段中，您可以指定 HTTP 伺服器將接聽的 [伺服器連接埠]，以及 HTTP 伺服器使用的 [驗證] 類型。依預設，伺服器連接埠設定為 **2221**。

驗證 - 定義用於存取更新檔案的驗證方法。可用選項如下：[無]、[基本] 及 [NTLM]。選取 [基本] 以使用具有基本使用者名稱及密碼驗證的 base64 編碼。[NTLM] 選項提供使用安全編碼方法的編碼。對於驗證，會使用共用更新檔案之工作站上建立的使用者。預設值為 [無]，這會授與對無需驗證之更新檔案的存取權。

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

i 數次從 [映像] 嘗試更新失敗之後，[無效的使用者名稱和/或密碼] 錯誤會出現在主要功能表中的 [更新] 窗格中。我們建議您瀏覽至 [\[進階設定\]](#) > [\[更新\]](#) > [\[設定檔\]](#) > [\[更新映像\]](#)，然後檢查「使用者名稱」和「密碼」。此錯誤最常見的原因是輸入的驗證資料錯誤。

配置完成您的映像伺服器之後，您必須在用戶端工作站上新增新的更新伺服器。若要執行此處理方法，請遵循以下步驟：

- 開啟 [\[進階設定\]](#)，並按一下 [\[更新\]](#) > [\[設定檔\]](#) > [\[更新\]](#) > [\[模組更新\]](#)。
- 用下列其中一種格式解除 [自動選擇] 並將新的伺服器新增至 [更新伺服器] 欄位：
`http://IP_address_of_your_server:2221`
`https://IP_address_of_your_server:2221` (如果使用 SSL 的話)

透過系統共用存取映像

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

然後，停用 [啟用 HTTP 伺服器]，配置 [進階設定] > [更新] > [設定檔] > [更新映像] 索引標籤中的映像存取權。依預設，會在程式安裝套件中啟用此選項。

如果共用資料夾位於網路中的另一台電腦，必須輸入存取其他電腦的驗證資料。若要輸入驗證資料，請開啟 [進階設定]，並按一下 [更新] > [設定檔] > [更新] > [連線選項] > [Windows 共用] > [以下列身分連接到區域網路]。此與「[以下列身分連接到區域網路](#)」一節所說明用來更新的設定相同。

若要存取映像資料夾，此動作需要在與登入電腦（建立映像的所在）所用的同一個帳戶下執行。若電腦在網域中，應該使用 "domain\user" 使用者名稱。若電腦不在網域中，應該使用 "IP_address_of_your_server\user" 或 "hostname\user"。

映像配置完成之後，在用戶端工作站上，依照下列步驟將 \\UNC\PATH 設定為更新伺服器：

1. 開啟 [進階設定]，並按一下 [更新] > [設定檔] > [更新]。
2. 解除 [模組更新] 旁的 [自動選擇]，並使用 \\UNC\PATH 格式，將新的伺服器新增至 [更新伺服器] 欄位。

i 若要更新正常運作，映像資料夾的路徑必須指定為 UNC 路徑。來自對應磁碟機的更新不會運作。

使用映像工具來建立映像

! 映像工具建立的資料夾結構與端點映像建立的資料夾結構不同。每個資料夾會為一組產品保留更新檔案。您必須在使用映像的產品更新設定中指定正確資料夾的完整路徑。
例如，若要透過映像更新 ESET PROTECT，請將 [更新伺服器](#) 設為（根據您的 HTTP 伺服器根位置）：
`http://your_server_address/mirror/eset_upd/ep10`

最後一個區段控制程式元件 (PCU) 依預設，下載的程式元件已準備好複製到本機映像。如果已啟動 [程式更新]，則不需要按一下 [更新]，因為檔案會在備妥時自動複製到本機映像。如需產品更新的詳細資訊，請參閱 [更新模式](#)。

疑難排解映像更新問題

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

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

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

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

ESET Endpoint Antivirus 下載更新檔案時報告錯誤 - 可能的原因是本機工作站下載更新所在更新伺服器（映像資料夾的網路路徑）的指定不正確。

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。

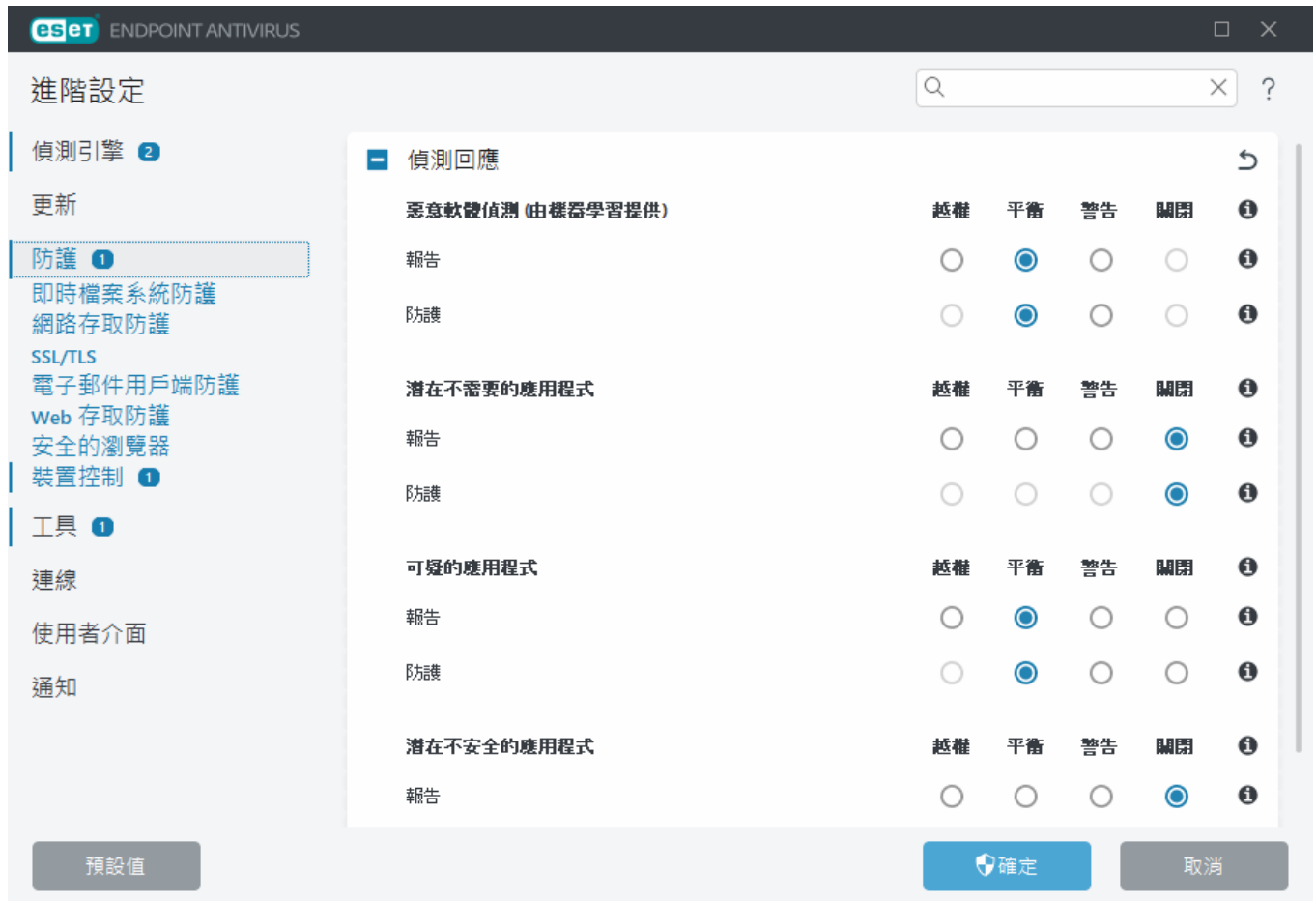
在此區段中：

- [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

報告設定

報告閾值是針對每個類別（稱為“CATEGORY”）而配置：

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。

閾值	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 2

閾值	說明
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 Endpoint Antivirus 防護模組的可用性](#)

所選取 CATEGORY 閾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](#)

- 按一下 [說明及支援] > [關於 ESET Endpoint Antivirus]
- 在 [關於] 畫面中，第一行文字顯示 ESET 產品的版本號碼。
- 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閾值時有數個基調：

- 建議大部分設定使用 [平衡] 閾值。
- 若環境優先著重於透過安全軟體將錯誤識別物件減至最少，則建議使用 [警告] 閾值。
- 報告閾值越高，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 Endpoint Antivirus 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 防護的閾值（或層級）：

閾值	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。

閾值	說明
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。

最佳實務

未受管理（個別用戶端工作站）

將預設建議值保持原狀。

受管理環境

這些設定通常透過[原則](#)套用至工作站。

1. 初始階段

此階段最多可能需要一週的時間。

- 將所有 [報告] 閾值設定為 [平衡]²
注意：如有需要，設定為 [越權]²
- 將針對惡意軟體的 [防護] 設定或保留為 [平衡]²
- 將其他「類別」的 [防護] 設定為 [警告]²
注意：不建議在此階段將 [防護] 閾值設定為 [越權]，因為將修復所有找到的偵測項目，包括錯誤識別的偵測項目。
- 從[偵測防護記錄](#)中找出錯誤識別物件，並首先將它們新增至[偵測排除](#)²

2. 轉換階段

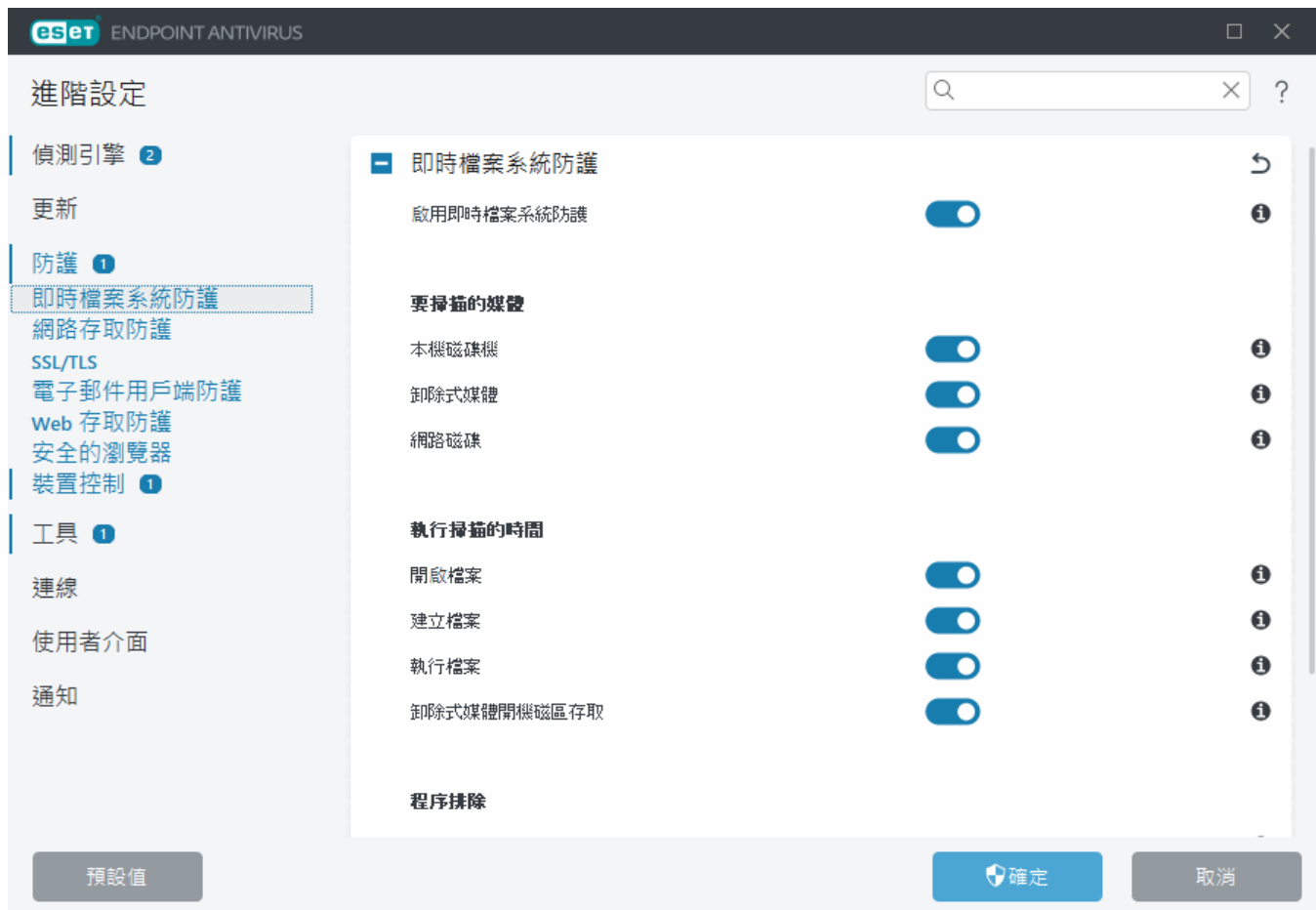
- 對部分工作站實作「生產階段」做為測試（但不對網路上的所有工作站進行此動作）。

3. 生產階段

- 將所有 [防護] 閾值設定為 [平衡]²
- 遠端管理時，請針對 ESET Endpoint Antivirus 使用適當的防毒[預先定義原則](#)²
- 如果需要最高偵測率，並接受錯誤識別物件，則可以設定 [越權] 防護閾值。
- 檢查[偵測防護記錄](#)或 ESET PROTECT 報告，找出可能遺失的偵測。

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。

i 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 Endpoint Antivirus 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。

o 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](#)

i [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 Endpoint Antivirus 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 Endpoint Antivirus 之後，所有設定都已最佳化，為使用者提供最高層級的系統安全。若要還原預設設定，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 [eicar.com](http://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，以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]** > **[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

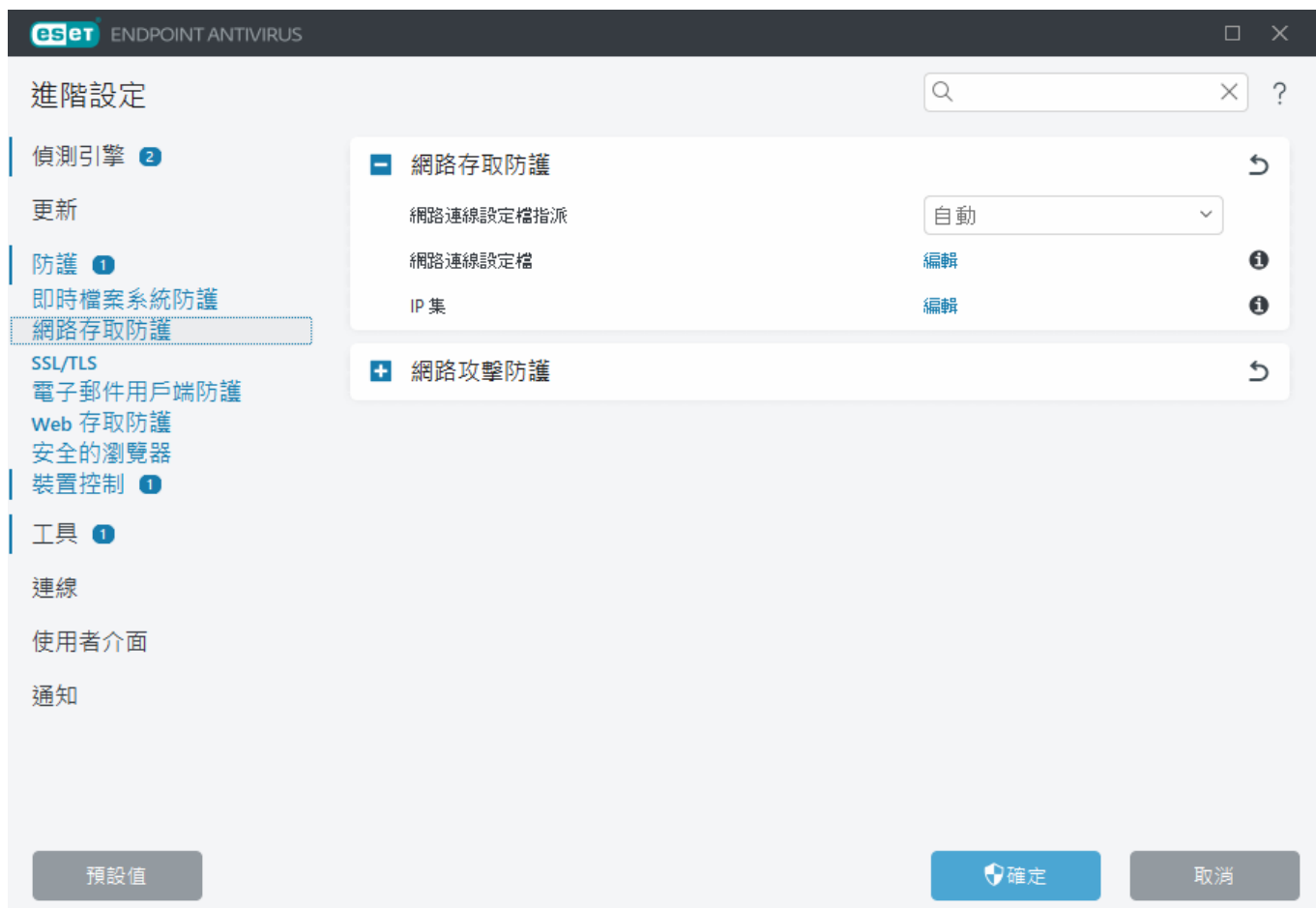
請確定電腦上未安裝任何其他防毒程式。若您同時安裝兩個防毒程式，它們可能會與彼此衝突。我們建議您先解除安裝系統上的任何其他防毒程式，再安裝 ESET。

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配置所有網路連線。根據預設，ESET Endpoint Antivirus 具有預先配置的網路存取防護，以實現最大的安全性。但是，特定環境可能需要自訂配置。僅應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 - 設定檔可用於控制特定網路連線的網路存取防護。

IP 集 - 您可以定義建立一個邏輯 IP 位址群組的 IP 位址集合，然後將其新增為信任區域或從[網路攻擊防護](#)中排除。


[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 Endpoint Antivirus 網路存取防護行為。建立或編輯[IDS 規則](#)或[暴力密碼破解攻擊](#)規則時，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 [\[主程式視窗\]](#) > [\[設定\]](#) > [\[網路\]](#) > [\[網路連線\]](#) 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，啟用了對內網 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。

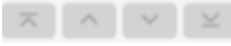
新增或編輯網路連線設定檔

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，啟用了對內網 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[暴力密碼破解攻擊防護](#)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〕**^②
- 選取其中一個現有設定檔，然後按一下 **〔編輯〕**^②
- 選取其中一個現有設定檔，然後按一下 **〔複製〕**^②

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為何）。

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 Endpoint Antivirus 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**^②

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**^②

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：

^ 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，就會顯示「伺服器驗證成功」。如果未正確配置驗證，則會顯示以下其中一個錯誤訊息：

伺服器驗證失敗。簽章無效或不相符。

伺服器簽章與輸入的公用金鑰不相符。

伺服器驗證失敗。網路名稱不相符。

已配置的網路名稱無法對應驗證伺服器網路名稱。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[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 Endpoint Antivirus 還包含套用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 (IPv4/IPv6 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。

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

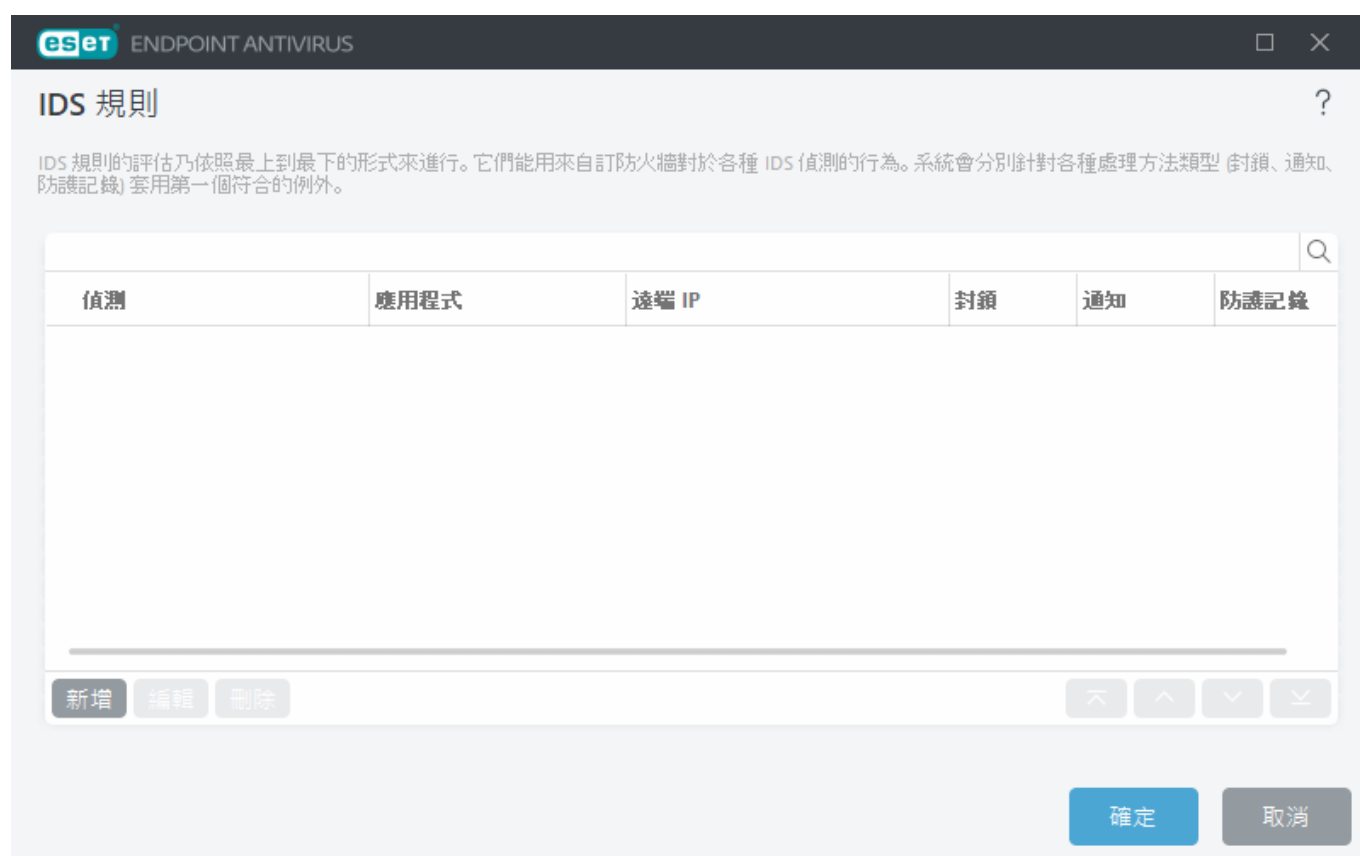
在某些狀況中，[入侵偵測服務 \(IDS\)](#) 可能會將路由器或內部網路裝置之間的通訊偵測成潛在威脅。例如，您可以將已知為安全的位址新增至 [自 IDS 區排除的位址] 以略過 IDS。

下列 ESET 知識庫文章可能僅以英文提供：

- [在 ESET Endpoint Antivirus 中的用戶端工作站上建立 IDS 規則](#)
- [在 ESET PROTECT 中為用戶端工作站建立 IDS 規則](#)

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）。



如果管理員在[ESET PROTECT Web 主控台中建立 IDS 排除](#)，將會顯示索引標籤**排除**。IDS 排除只能包含允許規則，並會在 IDS 規則之前評估。

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 Endpoint Antivirus 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[ESET Endpoint Antivirus 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]。

新增 IDS 規則

偵測: 任何偵測

威脅名稱:

方向: 兩者

應用程式:

遠端 IP 位址:

設定檔:

新增 刪除

處理方法

封鎖: 預設值

通知: 預設值

防護記錄: 預設值

確定 取消

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警告。
3. 按一下 **[...]**，然後選取您要套用通知之應用程式的檔案路徑。
4. 保留 **[封鎖]** 下拉式功能表中的 **[預設值]**。這會繼承 ESET Endpoint Antivirus 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。

您想要針對並未視為威脅的偵測類型移除週期性通知：

1. 按一下 **[新增]** 以新增 IDS 例外。
2. 從 **[警報]** 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]**。
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 Endpoint Antivirus 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**。





排除 - 由 IP 位址或應用程式路徑定義的排除偵測清單。您可以在 ESET PROTECT 中建立和編輯排除。如需詳細資訊，請參閱 **排除**。

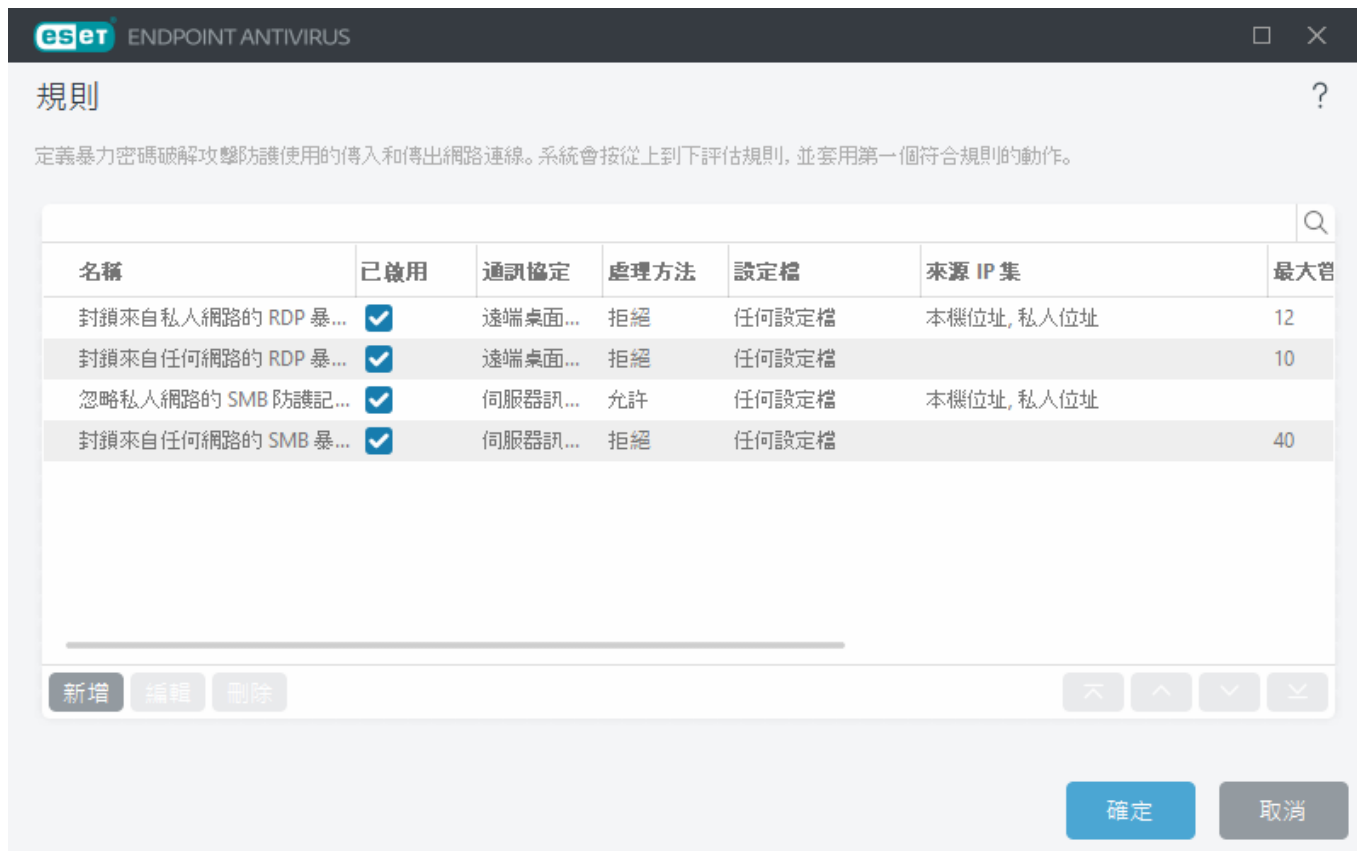
i 如需有關暴力密碼破解攻擊防護的詳細資訊，請參閱 **ESET 數位安全指南文章**。

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。無法編輯或删除預先定義的規則。

管理暴力攻擊防護規則

- **新增** - 按一下以建立新的暴力攻擊防護規則。
- **編輯** - 按一下以編輯現有暴力攻擊防護規則。
- **[移除]** - 若您要從 IDS 規則清單中移除某個例外，則請選取並按一下。
-     **頂端/向上/向下/底端** - 調整規則的優先順序層級。



i 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 - 您可以選擇將套用此規則的[網路連線設定檔](#)。

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。

eset

ENDPOINT ANTIVIRUS

×

新增規則?

名稱

未命名

已啟用

☒

處理方法

拒絕

▼

通訊協定

遠端桌面通訊協定 (RDP)

▼

設定檔

新增 刪除

新增 刪除

最大嘗試次數

10

i

黑名單保留期間 (分鐘)

30

i

來源 IP

i

來源 IP 集

新增 刪除

新增 刪除

確定

取消

排除

暴力排除可用於為特定條件隱藏暴力排除。這些排除是從 ESET PROTECT 暴力偵測建立而成。

直欄

- **偵測** – 偵測類型。
- **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** – 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。

管理排除

如果管理員在 [ESET PROTECT Web 主控台中建立暴力排除](#)，將會顯示排除。排除只能包含允許規則，並會在 IDS 規則之前評估。

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。

i 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

- **通訊協定 SMB** - 偵測並封鎖 SMB 通訊協定中的各種安全性問題，也就是：
 - **Rogue 伺服器挑戰攻擊驗證偵測** - 可保護您不會在驗證期間為了取得使用者驗證而受到使用 Rogue 挑戰的攻擊。
 - **具名管道開啟期間 IDS 規避偵測** - 在 SMB 通訊協定中偵測已知的開啟 MSRPC 具名管道時所使用的規避技術。
 - **CVE 偵測**（一般弱點和暴露）- 針對透過 SMB 通訊協定進行的各種攻擊、形式、安全漏洞和弱點實作的偵測方法。請參閱[位於 \[cve.mitre.org\]\(https://cve.mitre.org\) 的 CVE 網站](#)搜尋及取得與 CVE 識別碼 (CVE) 有關的詳細資訊。
- **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)。
- **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。

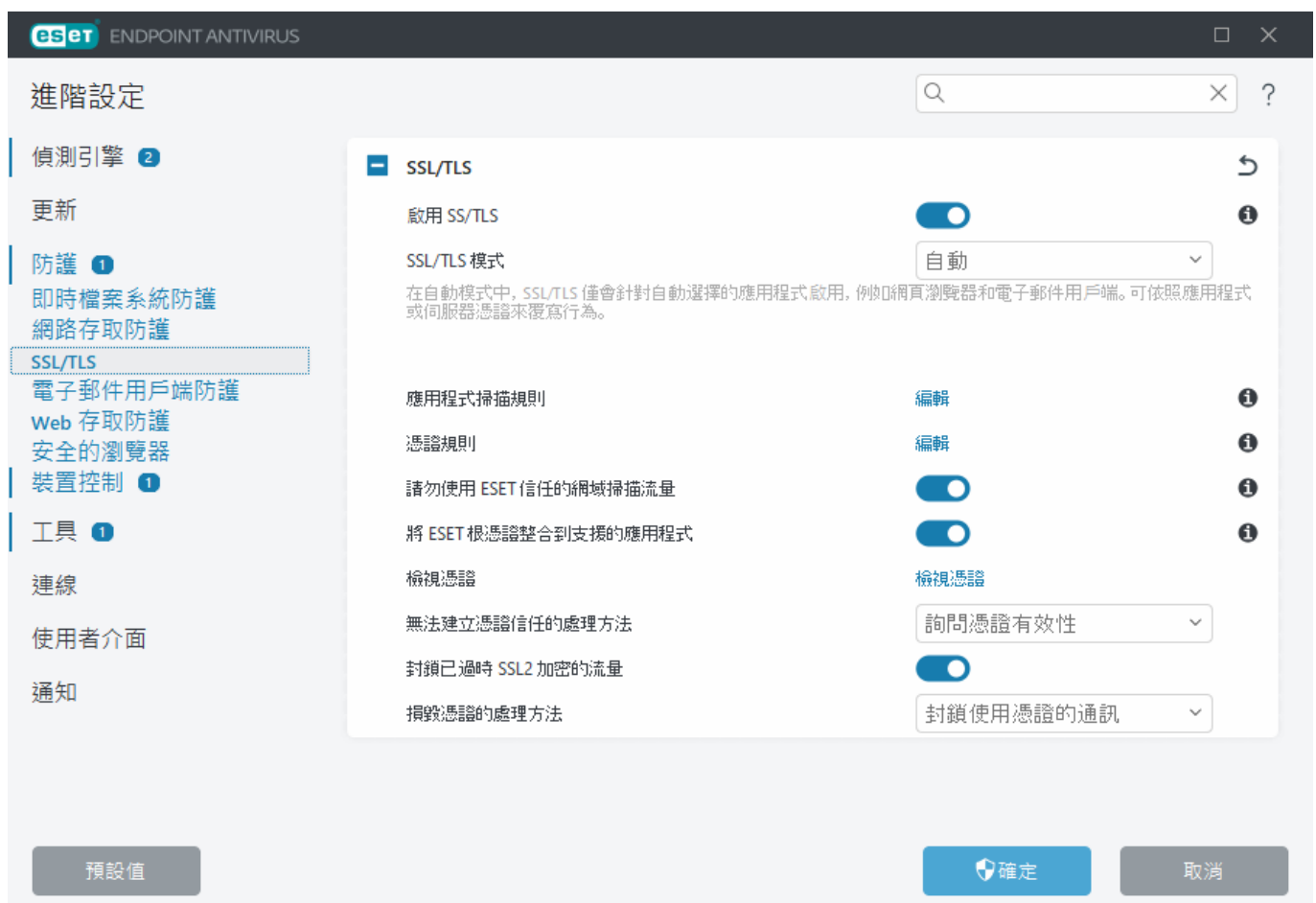
■ 封包檢查

- **允許外來連線至 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。最新的 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。

- 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 Endpoint Antivirus 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 Endpoint Antivirus 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 Endpoint Antivirus 行為。

憑證清單 – 可讓您自訂針對特定 SSL 憑證的 ESET Endpoint Antivirus 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 Endpoint Antivirus 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。

若要将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 Endpoint Antivirus 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。

下列 ESET 知識庫文章可能僅以英文提供：

- [ESET 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 Endpoint Antivirus 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]，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 Endpoint Antivirus 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，無論憑證的可信程度為何。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]，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 Endpoint Antivirus 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 Endpoint Antivirus 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 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](#)
- [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 Endpoint Antivirus 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 Endpoint Antivirus 也支援掃描 IMAPS (585-993) 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 Endpoint Antivirus 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 Endpoint Antivirus 掃描。

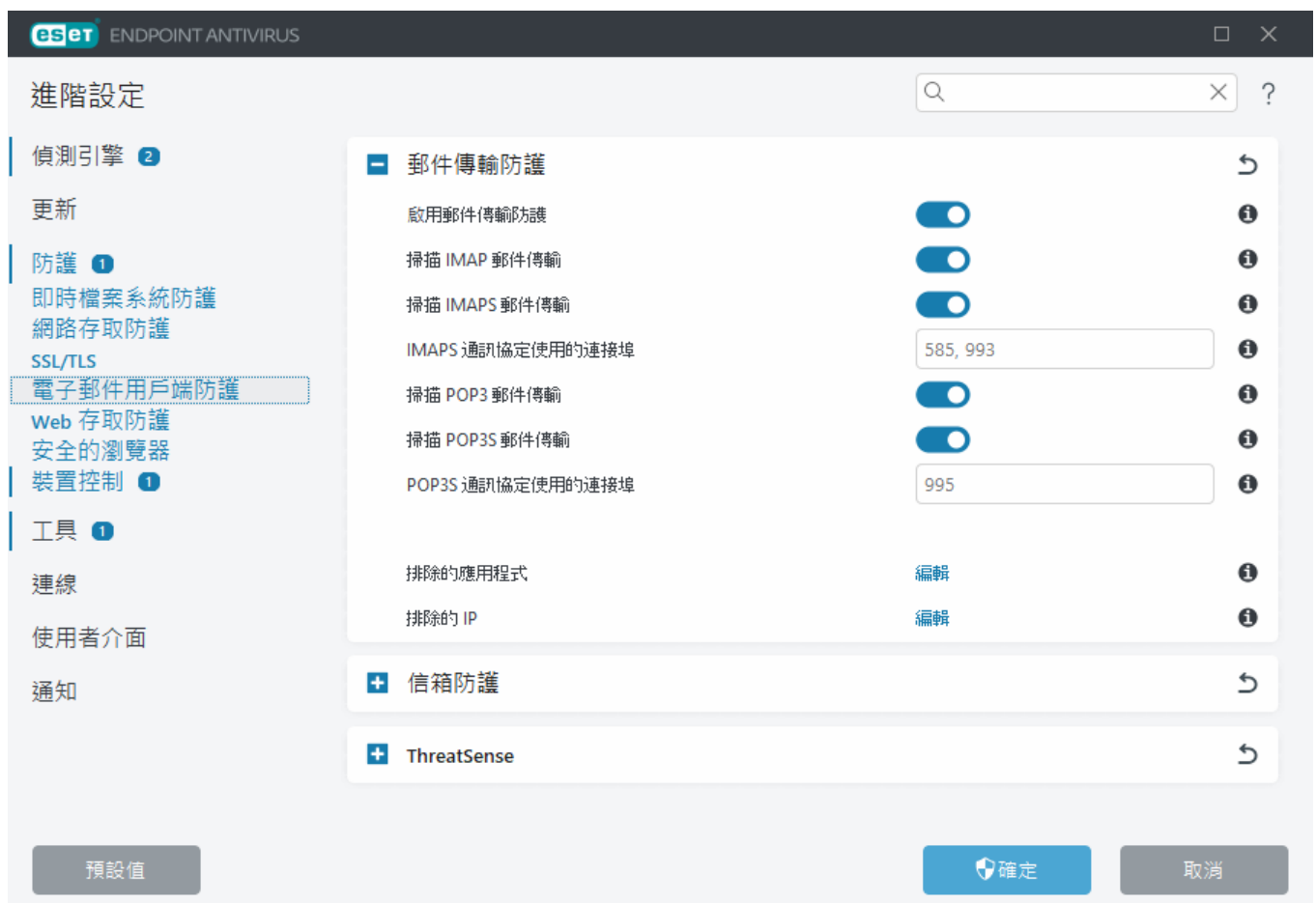
您可以透過按一下下方選項旁邊的切換開關來選擇要掃描的郵件傳輸通訊協定（預設情況下，啟用對所有通訊協定的掃描）：

- 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 Endpoint Antivirus 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 – 使您能夠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。



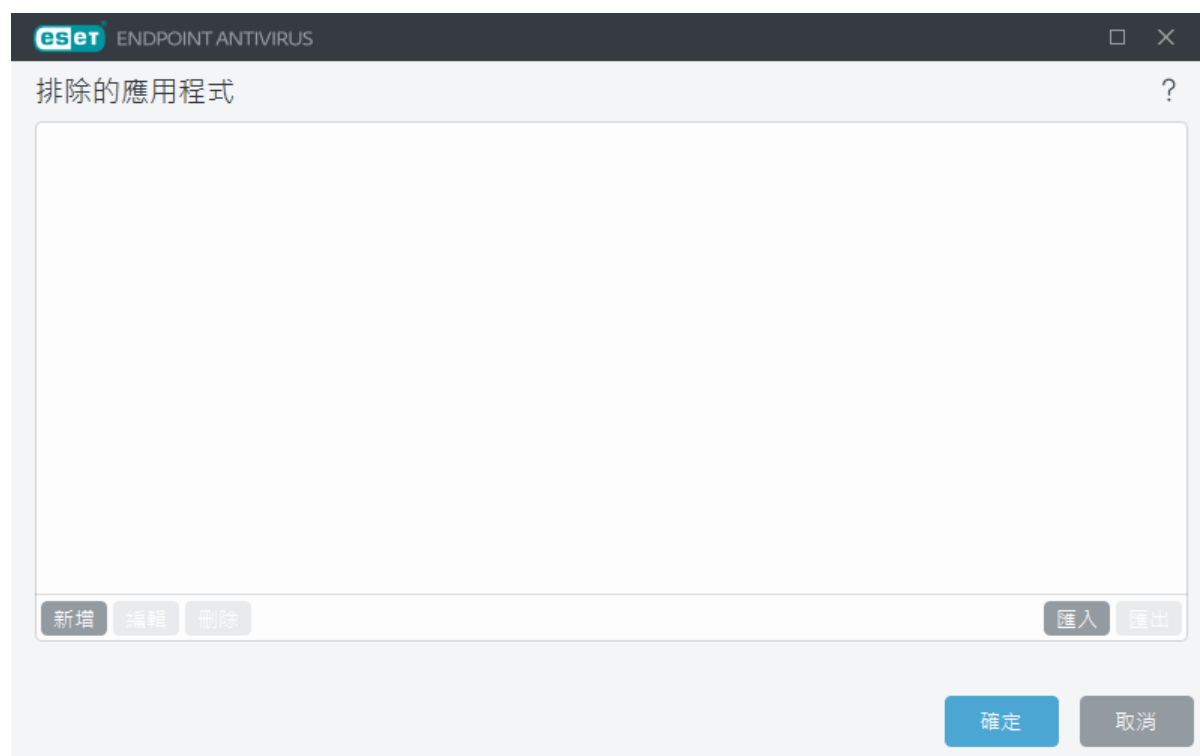
排除的應用程式

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。



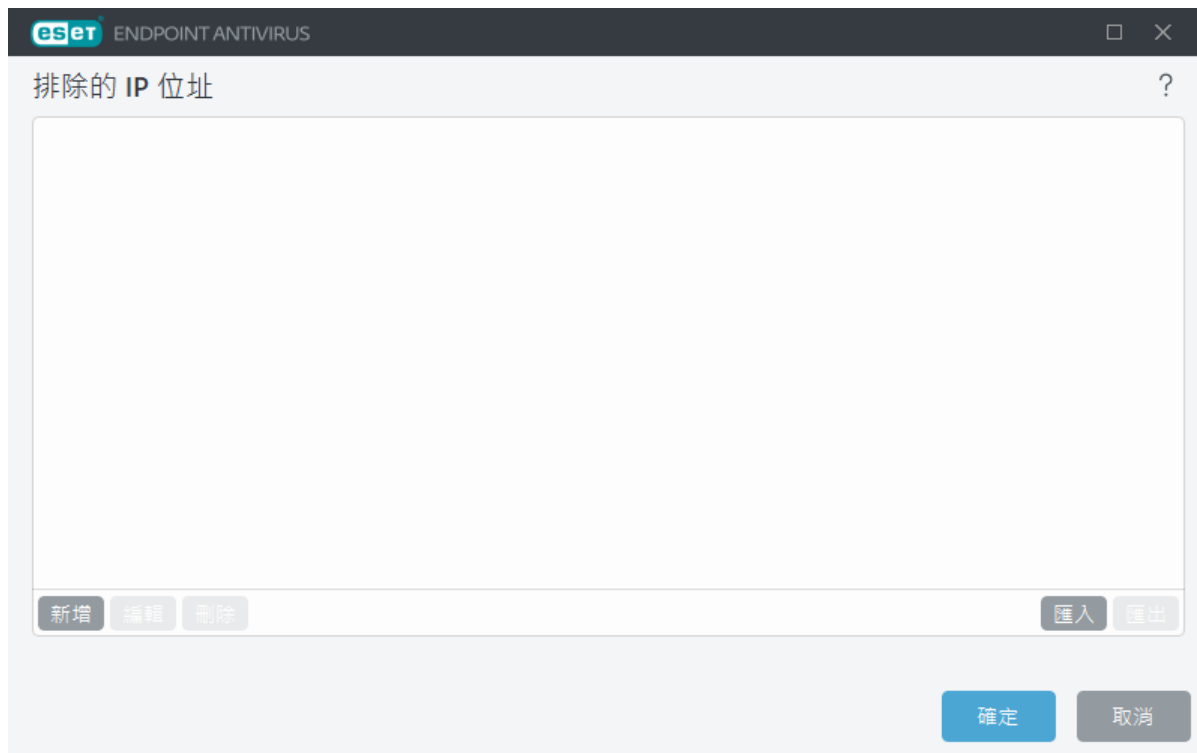
排除的 IP

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。

新增 - 按一下以新增要套用規則的遠端位置 IP 位址/位址範圍/子網路。

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。



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 Endpoint Antivirus 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。

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 Endpoint Antivirus 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 Endpoint Antivirus 中啟用此整合。如果整合至電子郵件用戶端，ESET Endpoint Antivirus 工具列會直接插入電子郵件用戶端，以便更有效進行電子郵件防護。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 Endpoint Antivirus 安裝後，此工具列包含防毒防護選項，已新增至 Microsoft Outlook 中：

ESET Endpoint Antivirus – 按兩下圖示以開啟 ESET Endpoint Antivirus 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。

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 Endpoint Antivirus 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 Endpoint Antivirus 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。

如果存在包含偵測的郵件，則根據預設 ESET Endpoint Antivirus 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。

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。

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 Endpoint Antivirus 在清除物件期間的行為。

排除

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

其他

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

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

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

[記錄所有物件] – [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²

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²

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 GB²

i 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](#)²

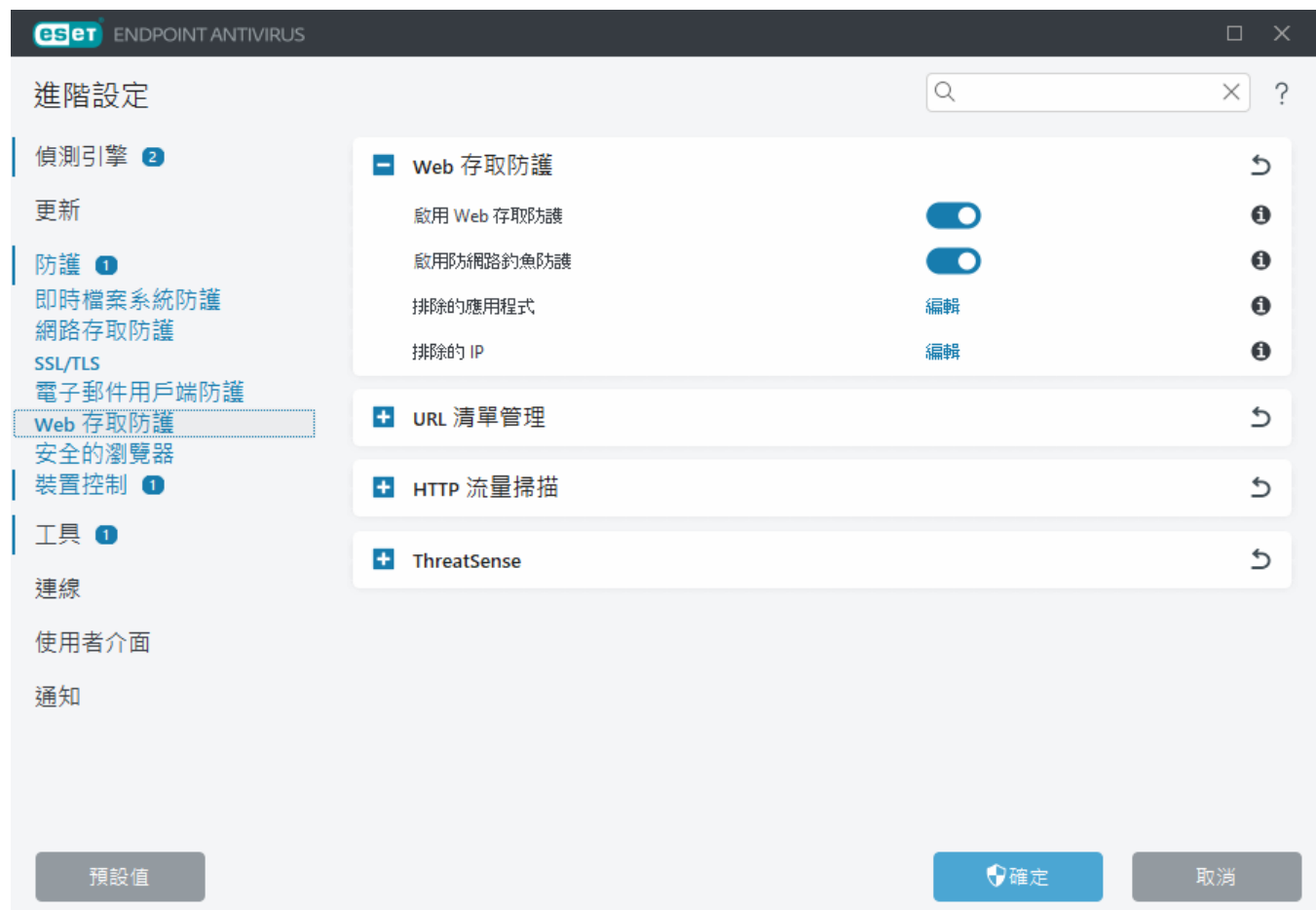
i 強烈建議您保持啟用 Web 存取防護，並不排除任何應用程式或 IP 位址（根據預設）。

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 – 使您能够將特定應用程式從 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：



下列 ESET 知識庫文章可能僅以英文提供：

- [解除鎖定 ESET Endpoint Antivirus 中個別工作站上的安全網站](#)

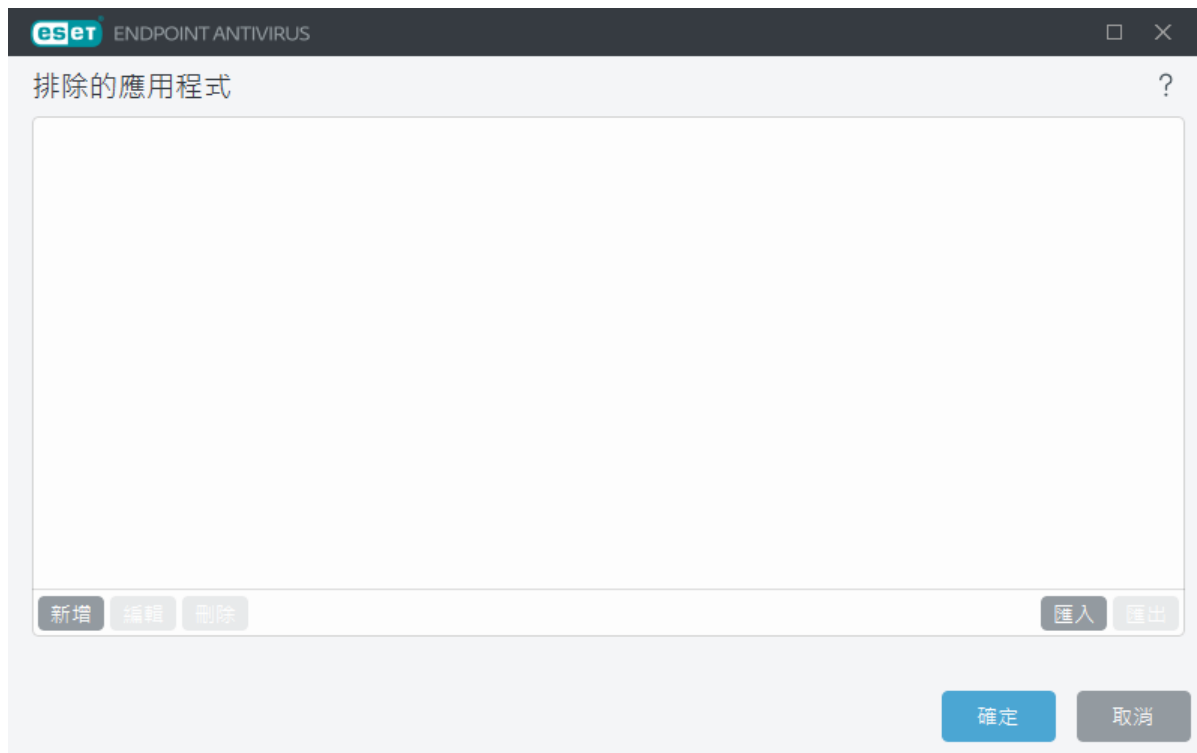
排除的應用程式

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。



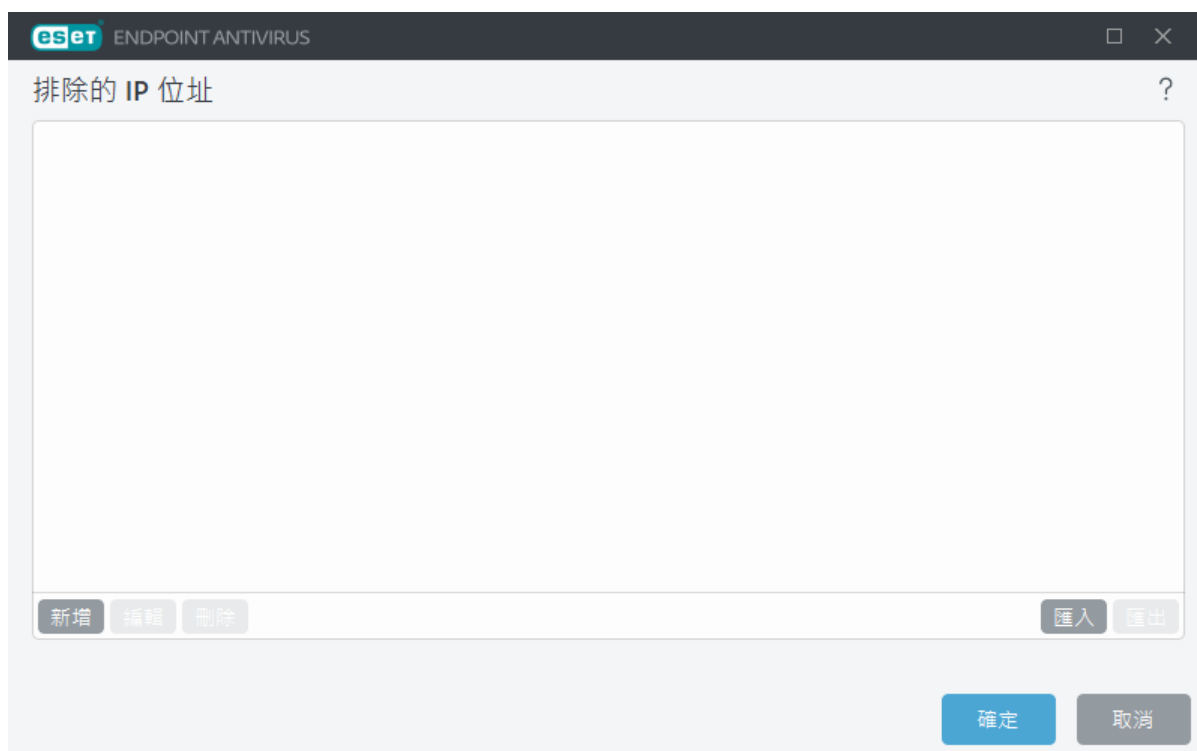
排除的 IP

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。

新增 - 按一下以新增要套用規則的遠端位置 IP 位址/位址範圍/子網路。

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。



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。

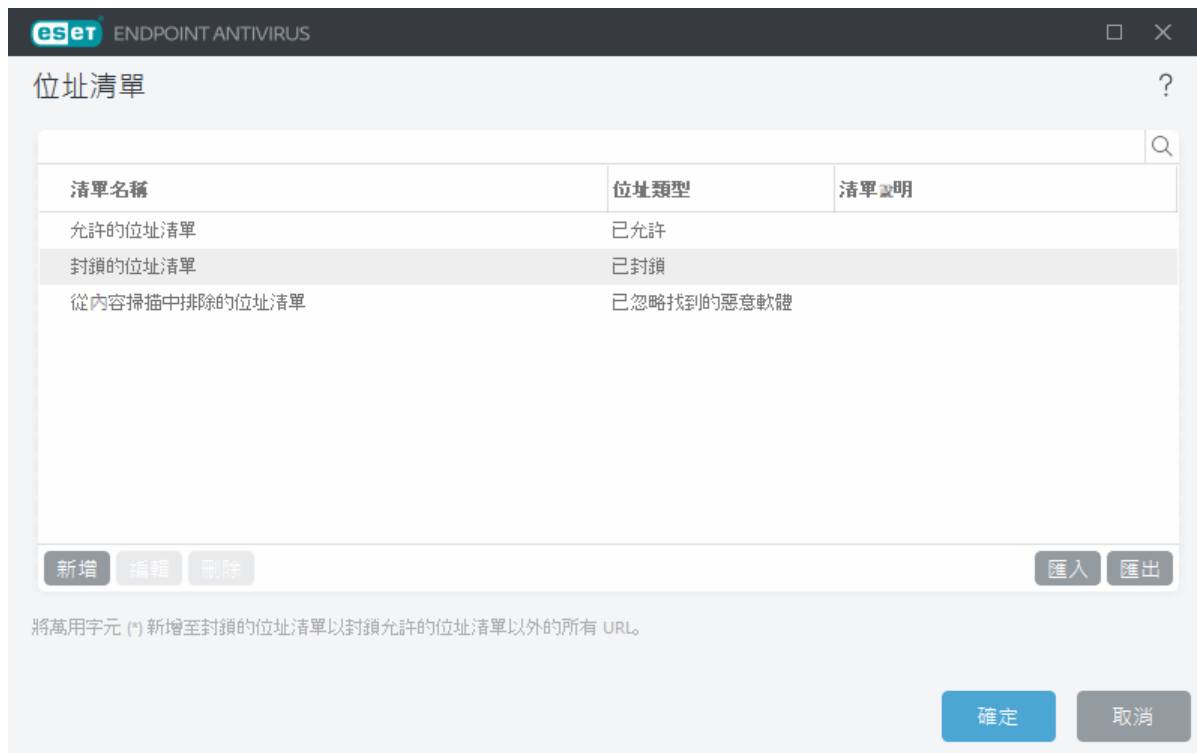
若您想封鎖所有位於作用中 [**允許的位址清單**] 以外的 HTTP 位址，請將 * 新增至作用中的 [**封鎖的位址清單**]

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元 * 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。

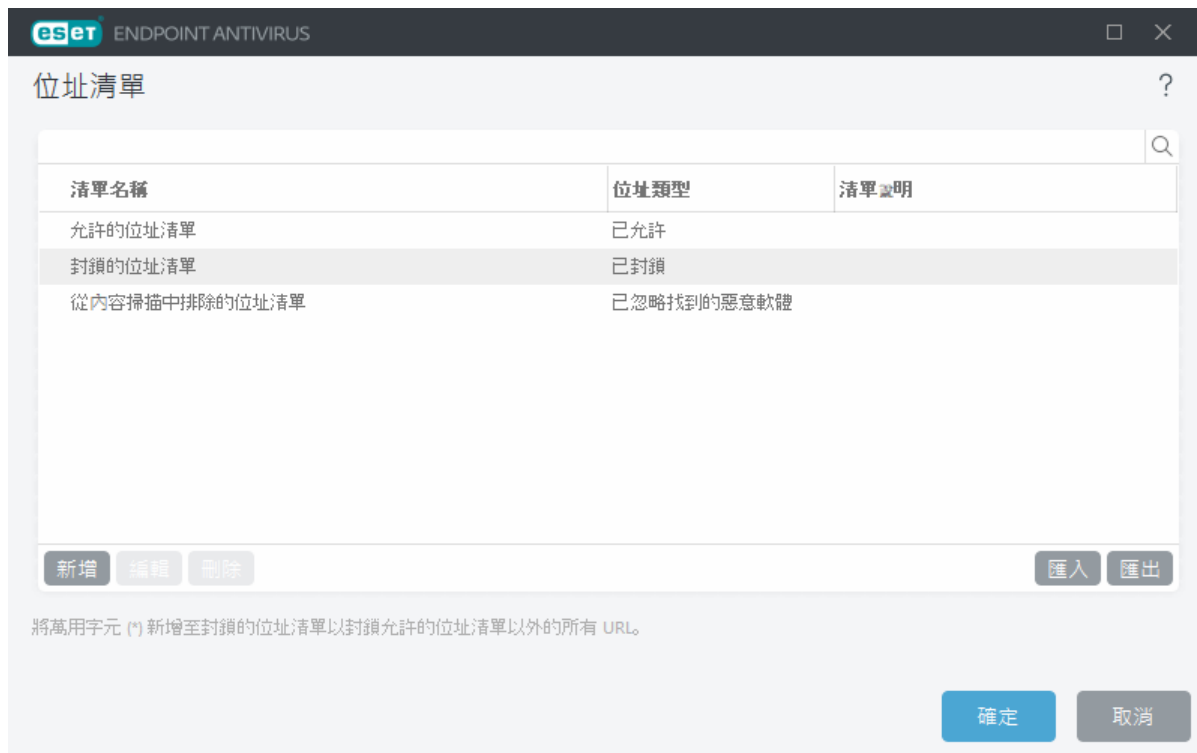
位址清單

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]**。



下列 ESET 知識庫文章可能僅以英文提供：

- [解除鎖定 ESET Endpoint Antivirus 中個別工作站上的安全網站](#)

如需詳細資訊，請參閱 [URL 位址管理](#)。

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 - 從下拉式功能表中選取記錄嚴重性 **ESET PROTECT** 或 可以收集具有 **[警告]** 詳細程度的記錄。

資訊和警告記錄詳細資訊僅適用於在網域中包含至少兩個元件（沒有萬用字元）的規則。例如：



- *.domain.com/*
- *www.domain.com/*

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）



如需詳細資訊，請參閱[如何新增 URL 遮罩](#)一章。

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 Endpoint Antivirus 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。您可以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)。

例如，遮罩 *x? 代表倒數第二個字元含有 x 的任何位址。若要符合整個網域，請以格式 *.domain.com/* 輸入。指定遮罩中的通訊協定字首 http:// 或 https:// 是選用選項，省略後遮罩會符合所有通訊協定。如果網域名稱中的「*.」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。

資訊和警告記錄詳細資訊僅適用於在網域中包含至少兩個元件（沒有萬用字元）的規則。例如：



- *.domain.com/*
- *www.domain.com/*

HTTP 流量掃描

預設情況下 ESET Endpoint Antivirus 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 Endpoint Antivirus 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 Endpoint Antivirus 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 Endpoint Antivirus 在清除物件期間的行為。

排除

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

其他

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

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

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

[記錄所有物件] – [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

i 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。

裝置控制

ESET Endpoint Antivirus 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 Endpoint Antivirus 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]**

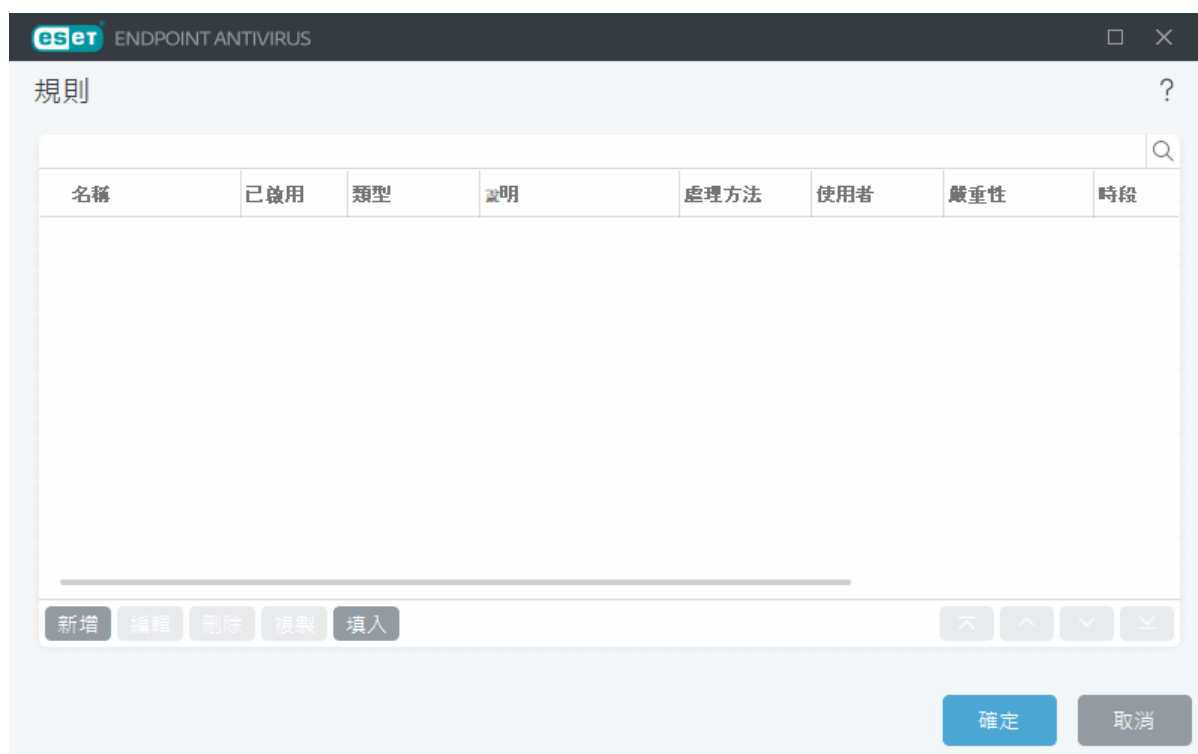
i 您可以使用排程器從 xml 檔中使用規則匯入裝置控制群組。有關詳細資訊和逐步指南，請參閱我們的 **ESET 知識庫文章**

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。亦請參閱 **新增裝置控制規則**

下列 ESET 知識庫文章可能僅以英文提供：
[使用 ESET Endpoint 產品新增和修改裝置控制規則](#)







根據使用者、使用者群組，或任何可從規則設定中指定的其他參數，即可允許或封鎖特定裝置。規則清單包含規則的數個說明，例如名稱、外部裝置類型、將外部裝置連接到電腦後要執行的動作，以及防護記錄嚴重性。

按一下 **新增** 或 **編輯** 以管理規則。取消選取規則旁的 **已啟用** 核取方塊以將其停用，直到您以後要使用時再啟用。選取一或多個規則，然後按一下 **刪除** 以永久刪除規則。

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 **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。

[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。在 **工具** > [防護記錄檔案](#) 中的 ESET Endpoint Antivirus 的主要程式視窗中，您可檢視防護記錄項目。

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）。


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。

套用期間 - 允許您在特定時間內套用建立的規則。從下拉式功能表選取建立的時段。參閱有關[時段](#)的更多資訊。

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。

i 數據機裝置類型無法使用使用者清單功能。規則將套用於所有的使用者，而目前的使用者清單將會刪除。

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，針對相同裝置進行後續連線時仍會顯示通知。


請注意，並非所有裝置類型都適用所有處理方法（權限）。如果其類型為儲存裝置，則四種處理方法都可以使用。對於非儲存裝置，只可使用三種處理方法（例如，[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

- **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，並將它們傳送至 ERA Server 
- **無** - 不記錄任何防護記錄。

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

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

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 - 取決於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**、**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）。

i 您可以使用排程器從 xml 檔中使用規則匯入裝置控制群組。有關詳細資訊和逐步指南，請參閱我們的 [ESET 知識庫文章](#)。

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。

i 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。如果您要離開 [裝置群組] 視窗而不儲存變更，請按一下 [取消]。

i 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）。

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 Endpoint Antivirus 在清除物件期間的行為。

排除

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

其他

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

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

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

[記錄所有物件] – [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

i 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 Endpoint Antivirus 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。 [一律修復偵測] 是 受管理環境 中建議使用的預設設定。
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。

i 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`）。

i 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 Endpoint Antivirus 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 Endpoint Antivirus 管理。

- [時段](#)
- [Microsoft Windows 更新](#)
- [ESET CMD](#)
- [遠端監視和管理](#)
- [授權間隔檢查](#)
- [防護記錄檔案](#)
- [簡報模式](#)
- [診斷](#)

時段

您可以建立時段，然後將其指派給 **裝置控制** 的規則。**時段** 設定可在 [進階設定](#) > **工具** 中找到。這可讓您定義常用的時段（例如工作時間、周末等），並輕鬆地重複使用它們，而不需重新定義每個規則的時段。時段適用於任何相關類型的規則，只要其支援時間型控制。

名稱	說明

若要建立時段，請完成下列動作：

1. 按一下 **編輯** > **新增**
2. 輸入時段的名稱和 **說明**，然後按一下 **新增**
3. 指定時段的日期及開始/結束時間，或選取 **全天**
4. 按一下 **確定** 以確認。

您可以使用一個或多個以日及時間為基礎的時間範圍來定義單一時段。建立時段後，它將顯示在 [裝置控制規則編輯器視窗](#) 中的 **套用期間** 下拉式功能表中。

Microsoft Windows 更新

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

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

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

對話方塊視窗 - 作業系統更新

若有某些適合您作業系統的可用更新，ESET Endpoint Antivirus 首頁視窗會顯示通知。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。您可以使用命令列 (**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 Endpoint Antivirus 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 Endpoint Antivirus 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。



進階 **ecmd** 命令只能在本機執行。僅可透過使用 ESET PROTECT 執行用戶端工作 **[執行命令]** 來執行 **ecmd** 命令。

匯出設定命令：

✓ `ecmd /getcfg c:\config\settings.xml`

匯入設定命令：

`ecmd /setcfg c:\config\settings.xml`

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>`

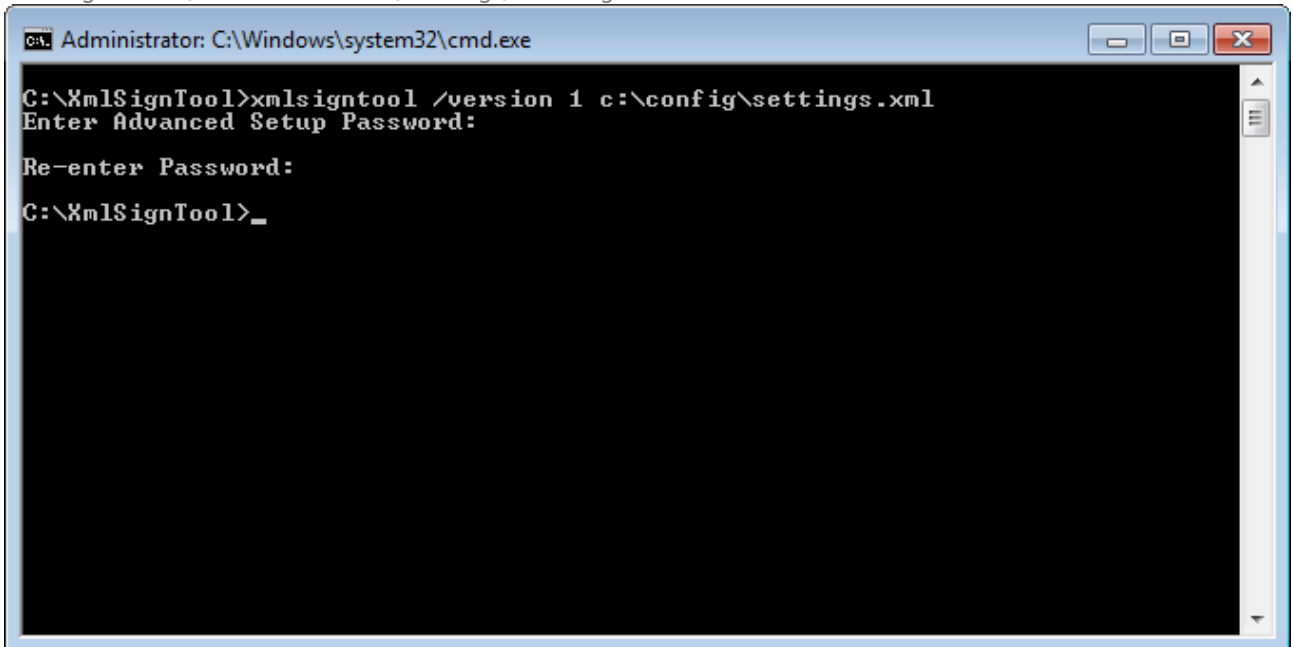


`/version` 參數的值取決於您的 ESET Endpoint Antivirus 版本。針對第 7 版和更新版本，請使用 `/version 2`

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 Endpoint Antivirus 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 Endpoint Antivirus 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。

ecmd 命令清單

透過 ESET PROTECT Client Task Run 命令可以啟用和暫時停用個別的安全性功能。這類命令不會覆寫原則設定，而在執行命令並重新啟動裝置之後，所有暫停的設定都會還原為其原始狀態。若要利用這項功能，請指定在同名的欄位中執行命令列。

檢閱以下每項安全防護功能的命令清單：

安全性功能	暫時暫停命令	啟用命令
即時檔案系統防護	ecmd /setfeature onaccess pause	ecmd /setfeature onaccess enable
文件防護	ecmd /setfeature document pause	ecmd /setfeature document enable
裝置控制	ecmd /setfeature devcontrol pause	ecmd /setfeature devcontrol enable
簡報模式	ecmd /setfeature presentation pause	ecmd /setfeature presentation enable
個人防火牆	ecmd /setfeature firewall pause	ecmd /setfeature firewall enable
網路攻擊防護 (IDS)	ecmd /setfeature ids pause	ecmd /setfeature ids enable
殭屍網路防護	ecmd /setfeature botnet pause	ecmd /setfeature botnet enable
Web 控制	ecmd /setfeature webcontrol pause	ecmd /setfeature webcontrol enable
Web 存取防護	ecmd /setfeature webaccess pause	ecmd /setfeature webaccess enable
電子郵件用戶端防護	ecmd /setfeature email pause	ecmd /setfeature email enable
電子郵件用戶端反垃圾郵件	ecmd /setfeature antispam pause	ecmd /setfeature antispam enable
防網路釣魚防護	ecmd /setfeature antiphishing pause	ecmd /setfeature antiphishing enable

遠端監視和管理

遠端監視和管理 (RMM) 是使用管理服務提供者可以存取的本機安裝代理程式來監督和控制軟體系統的程序。

ERMM - RMM 的 ESET 外掛程式

- 預設 ESET Endpoint Antivirus 安裝包含位於目錄中端點應用程式的 `ermm.exe` 檔案：
`C:\Program Files\ESET\ESET Security\ermm.exe`
- `ermm.exe` 這個命令列公用程式是為了協助端點產品的管理和與任何 RMM 外掛程式的通訊而設計。
- `ermm.exe` 會與 RMM 外掛程式交換資料，這個外掛程式會與連結到 RMM 伺服器的 RMM 代理程式通訊。依預設會停用 ESET RMM 工具。

其他資源

- [ERMM 命令列](#)
- [ERMM JSON 命令清單](#)
- [如何啟動遠端監視和管理ESET Endpoint Antivirus](#)

適用於第三方 RMM 解決方案的 ESET Direct Endpoint Management 外掛程式

RMM 伺服器會在第三方伺服器上以服務的形式執行。如需詳細資訊，請參閱以下 ESET Direct Endpoint Management 線上使用者指南：

- [ConnectWise Automate 的 ESET Direct Endpoint Management 外掛程式](#)
- [適用於 DattoRMM 的 ESET Direct Endpoint Management 外掛程式](#)
- [適用於 Solarwinds N-Central 的 ESET Direct Endpoint Management](#)
- [適用於 NinjaRMM 的 ESET Direct Endpoint Management](#)

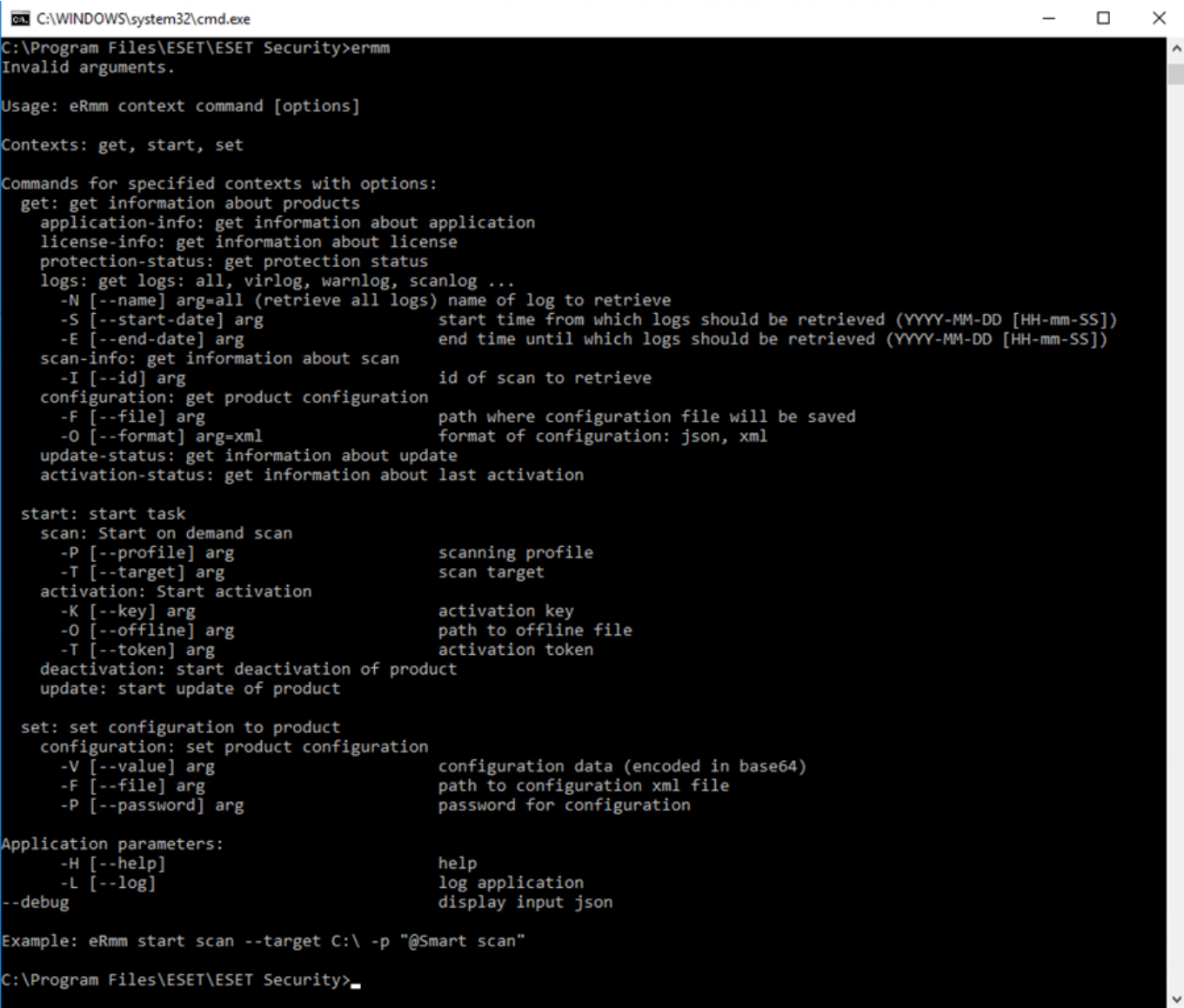
ERMM 命令列

使用命令列介面運行遠端監控管理。預設 ESET Endpoint Antivirus 安裝包含位於目錄中端點應用程式的 ermm.exe 檔案： `c:\Program Files\ESET\ESET Security`。

以管理員角色執行命令提示字元 (cmd.exe) 然後瀏覽至上述路徑（若要打開命令提示字元，請在鍵盤上按 Windows 按鈕 + R 在 [執行] 視窗中輸入 cmd，然後按下 Enter 鍵）。

命令語法為： `ermm context command [options]`

防護記錄參數區分大小寫。



[ermm.exe] 使用三種基本內容：取得、開始和設定。在下表中，您可以找到命令語法的範例。按一下 [命令] 欄中的連結，以查看進一步選項、參數和使用範例。成功執行命令後，將顯示輸出部分（結果）。若要查看輸入部分，請透過 `--debug` 命令新增參數。

內容	命令	說明
get		取得關於產品的資訊
	application-info	取得關於產品的資訊

內容	命令	說明
	license-info	取得關於授權的資訊
	protection-status	取得防護狀態
	logs	取得防護記錄
	scan-info	取得關於執行掃描的資訊
	configuration	取得產品配置
	update-status	取得關於更新的資訊
	activation-status	取得關於上次啟動的資訊
start		啟動任務
	scan	開始指定掃描
	activation	開始啟動產品
	deactivation	開始停用產品
	update	開始更新產品
set		設定產品選項
	configuration	將配置設定為產品

在每個命令的輸出結果中，顯示的第一個資訊是結果 ID。若要更充分瞭解結果資訊，請查看以下 ID 表格。

錯誤 ID	錯誤	說明
0	Success	
1	Command node not present	輸入 json 中不存在「命令」節點
2	Command not supported	不支援命令
3	General error executing the command	執行命令期間發生錯誤
4	Task already running	請求的工作已在執行中，尚未啟動
5	Invalid parameter for command	錯誤的使用者輸入
6	Command not executed because it's disabled	RMM 未在進階設定中啟用或以管理員角色啟動

ERMM JSON 命令清單

- [get protection-status](#)
- [get application-info](#)
- [get license-info](#)
- [get logs](#)
- [get activation-status](#)
- [get scan-info](#)
- [get configuration](#)
- [get update-status](#)
- [start scan](#)
- [start activation](#)
- [start deactivation](#)
- [start update](#)
- [set configuration](#)

get protection-status

Get the list of application statuses and the global application status

命令列

```
ermm.exe get protection-status
```

參數

None

範例

call

```
{
  "command": "get_protection_status",
  "id": 1,
  "version": "1"
}
```

result

```
{
  "id": 1,
  "result": {
    "statuses": [{
      "id": "EkrrnNotActivated",
      "status": 2,
      "priority": 768,
      "description": "Product not activated"
    }],
    "status": 2,
    "description": "Security alert"
  },
  "error": null
}
```

get application-info

Get information about the installed application

命令列

```
ermm.exe get application-info
```

參數

None

範例

call

```
{  
  "command": "get_application_info",  
  "id": 1,  
  "version": "1"  
}
```

result

```

{
  "id":1,
  "result":{
    "description":"ESET Endpoint Antivirus",
    "version":"6.6.2018.0",
    "product":"eea",
    "lang_id":1033,
    "modules":[{
      "id":"SCANNER32",
      "description":"Detection engine",
      "version":"15117",
      "date":"2017-03-20"
    },{
      "id":"PEGASUS32",
      "description":"Rapid Response module",
      "version":"9734",
      "date":"2017-03-20"
    },{
      "id":"LOADER32",
      "description":"Update module",
      "version":"1009",
      "date":"2016-12-05"
    },{
      "id":"PERSEUS32",
      "description":"Antivirus and antispysware scanner module",
      "version":"1513",
      "date":"2017-03-06"
    },{
      "id":"ADVHEUR32",
      "description":"Advanced heuristics module",
      "version":"1176",
      "date":"2017-01-16"
    },{
      "id":"ARCHIVER32",
      "description":"Archive support module",
      "version":"1261",
      "date":"2017-02-22"
    },{
      "id":"CLEANER32",
      "description":"Cleaner module",
      "version":"1132",
      "date":"2017-03-15"
    },{
      "id":"SYSTEMSTATUS32",
      "description":"ESET SysInspector module",
      "version":"1266",
      "date":"2016-12-22"
    },{
      "id":"TRANSLATOR32",
      "description":"Translation support module",
      "version":"1588B",
      "date":"2017-03-01"
    },{
      "id":"HIPS32",
      "description":"HIPS support module",
      "version":"1267",
      "date":"2017-02-16"
    },{
      "id":"PROTOSCAN32",
      "description":"Internet protection module",
      "version":"1300",
      "date":"2017-03-03"
    },{
      "id":"DBLITE32",
      "description":"Database module",
      "version":"1088",
      "date":"2017-01-05"
    },{
      "id":"CONFENG32",
      "description":"Configuration module (33)",
      "version":"1496B",
      "date":"2017-03-17"
    },{
      "id":"IRIS32",
      "description":"LiveGrid communication module",
      "version":"1022",
      "date":"2016-04-01"
    },{
      "id":"SAURON32",
      "description":"Rootkit detection and cleaning module",
      "version":"1006",
      "date":"2016-07-15"
    },{
      "id":"SSL32",
      "description":"Cryptographic protocol support module",
      "version":"1009",
      "date":"2016-12-02"
    }
  ],
  "error":null
}

```


get license-info

Get information about the license of the product

命令列

```
ermm.exe get license-info
```

參數

None

範例

call

```
{
  "command": "get_license_info",
  "id": 1,
  "version": "1"
}
```

result

```
{
  "id": 1,
  "result": {
    "type": "NFR",
    "expiration_date": "2020-12-31",
    "expiration_state": "ok",
    "public_id": "3XX-7ED-7XF",
    "seat_id": "6f726793-ae95-4e04-8ac3-e6a20bc620bf",
    "seat_name": "M"
  },
  "error": null
}
```

get logs

Get logs of the product

命令列

```
ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-date "2017-04-04 12-00-00"
```

參數

Name	Value
name	{ all, virlog, warnlog, scanlog, blocked, hipslog, urllog, devctrllog } : log to retrieve
start-date	start date from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
end-date	end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

範例

call

```
{
  "command": "get_logs",
  "id": 1,
  "version": "1",
  "params": {
    "name": "warnlog",
    "start_date": "2017-04-04 06-00-00",
    "end_date": "2017-04-04 12-00-00"
  }
}
```

result

```
{
  "id": 1,
  "result": {
    "warnlog": {
      "display_name": "Events",
      "logs": [
        {
          "Time": "2017-04-04 06-05-59",
          "Severity": "Info",
          "PluginId": "ESET Kernel",
          "Code": "Malware database was successfully updated to version 15198 (20170404).",
          "UserData": ""
        },
        {
          "Time": "2017-04-04 11-12-59",
          "Severity": "Info",
          "PluginId": "ESET Kernel",
          "Code": "Malware database was successfully updated to version 15199 (20170404).",
          "UserData": ""
        }
      ]
    }
  },
  "error": null
}
```

get activation-status

Get information about the last activation. Result of status can be { success, running, failure }

命令列

```
ermm.exe get activation-status
```

參數

None

範例

call

```
{
  "command": "get_activation_status",
  "id": 1,
  "version": "1"
}
```

result

```
{
  "id": 1,
  "result": {
    "status": "success"
  },
  "error": null
}
```

get scan-info

取得關於執行掃描的資訊。

命令列

```
ermm.exe get scan-info
```

參數

無

範例

來電

```
{
  "command": "get_scan_info",
  "id": 1,
  "version": "1"
}
```

結果

```
{
  "id":1,
  "result":{
    "scan-info":{
      "scans":[{
        "scan_id":65536,
        "timestamp":272,
        "state":"finished",
        "pause_scheduled_allowed":false,
        "pause_time_remain":0,
        "start_time":"2017-06-20T12:20:33Z",
        "elapsed_tickcount":328,
        "exit_code":0,
        "progress_filename":"Operating memory",
        "progress_arch_filename":"",
        "total_object_count":268,
        "infected_object_count":0,
        "cleaned_object_count":0,
        "log_timestamp":268,
        "log_count":0,
        "log_path":"C:\\ProgramData\\ESET\\ESET Security\\Logs\\eScan\\ndl31494.dat",
        "username":"test-PC\\test",
        "process_id":3616,
        "thread_id":3992,
        "task_type":2
      }],
      "pause_scheduled_active":false
    }
  },
  "error":null
}
```

get configuration

Get the product configuration. Result of status may be { success, error }

命令列

```
ermm.exe get configuration --file C:\\tmp\\conf.xml --format xml
```

參數

Name	Value
file	the path where the configuration file will be saved
format	format of configuration: json, xml. Default format is xml

範例

```
call
```

```
{
  "command": "get_configuration",
  "id": 1,
  "version": "1",
  "params": {
    "format": "xml",
    "file": "C:\\tmp\\conf.xml"
  }
}
```

result

```
{
  "id": 1,
  "result": {
    "configuration": "PD94bWwgdGVyc2lvbj0iMS4w=="
  },
  "error": null
}
```

get update-status

Get information about the update. Result of status may be { success, error }

命令列

ermm.exe get update-status

參數

None

範例

call

```
{
  "command": "get_update_status",
  "id": 1,
  "version": "1"
}
```

result

```
{
  "id": 1,
  "result": {
    "last_update_time": "2017-06-20 13-21-37",
    "last_update_result": "error",
    "last_successful_update_time": "2017-06-20 11-21-45"
  },
  "error": null
}
```

start scan

Start scan with the product

命令列

```
ermm.exe start scan --profile "profile name" --target "path"
```

參數

Name	Value
profile	Profile name of On-demand computer scan defined in product
target	Path to be scanned

範例

call

```
{
  "command": "start_scan",
  "id": 1,
  "version": "1",
  "params": {
    "profile": "Smart scan",
    "target": "c:\\\"
  }
}
```

result

```
{
  "id": 1,
  "result": {
    "task_id": 458752
  },
  "error": null
}
```

start activation

Start activation of product

命令列

```
ermm.exe start activation --key "activation key" | --offline "path to offline file"
```

參數

Name	Value
key	Activation key
offline	Path to offline file

範例

call

```
{
  "command": "start_activation"
  "id": 1,
  "version": "1",
  "params": {
    "key": "XXXX-XXXX-XXXX-XXXX-XXXX"
  }
}
```

result

```
{
  "id": 1,
  "result": {
  },
  "error": null
}
```

start deactivation

Start deactivation of the product

命令列

ermm.exe start deactivation

參數

None

範例

call

```
{
  "command": "start_deactivation",
  "id": 1,
  "version": "1"
}
```

result

```
{
  "id": 1,
  "result": {
  },
  "error": null
}
```

start update

Start update of the product. Only one update may be running in the product so in case the update is already running, "Task already running" error code is returned

命令列

ermm.exe start update

參數

None

範例

call
<pre>{ "command": "start_update", "id": 1, "version": "1" }</pre>
result
<pre>{ "id": 1, "result": { }, "error": { "id": 4, "text": "Task already running." } }</pre>

set configuration

Set configuration to the product. Result of status may be { success, error }

命令列

ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass

參數

Name	Value
file	the path where the configuration file will be saved
password	password for configuration
value	configuration data from the argument (encoded in base64)

範例

call

```
{
  "command": "set_configuration",
  "id": 1,
  "version": "1",
  "params": {
    "format": "xml",
    "file": "C:\\tmp\\conf.xml",
    "password": "pass"
  }
}
```

result

```
{
  "id": 1,
  "result": {
  },
  "error": null
}
```

授權間隔檢查

ESET Endpoint Antivirus 需要自動連線至 ESET 授權伺服器。您可以在 [\[進階設定\]](#) > [\[工具\]](#) > [\[授權\]](#) 中限制與 ESET 授權伺服器的連線數。根據預設，[\[間隔檢查\]](#) 設定為 [\[自動\]](#)，並且每小時建立幾次連線。如果網路流量增加，請將 [\[間隔檢查\]](#) 變更為 [\[有限\]](#) 以減少超載。當選取了 [\[有限\]](#) 時，ESET Endpoint Antivirus 一天只會連線到授權伺服器一次，或在電腦重新啟動時連線。



如果 [\[間隔檢查\]](#) 設定已設為 [\[有限\]](#)，則透過 ESET HUB /ESET MSP Administrator 進行的所有授權相關變更可能會花費多達一天的時間才能套用至 ESET Endpoint Antivirus 設定。

防護記錄檔案

可以在 [\[進階設定\]](#) > [\[工具\]](#) > [\[防護記錄檔案\]](#) 中存取 ESET Endpoint Antivirus 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（啟動病毒防護等錯誤）。



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] - 如果已啟用，且片段百分比高於 [\[如果未使用的記錄數目超過（%）\]](#) 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。將移除所有空白防護記錄，以改善效能並提高防護記錄的處理速度。當防護記錄包含大量項目時，便可以觀察到改善的情況。

[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]** - 選取防護記錄檔案所儲存的目錄（僅適用於 **Text/CSV**）。您可以複製路徑或按一下 **[清除]** 選取其他目錄。每個防護記錄區段皆具備已預先定義檔案名稱的檔案（例如，若您使用純文字檔案格式以儲存防護記錄，則 *virlog.txt* 適用於防護記錄檔案的 **[偵測到威脅]** 區段）。
- **[類型]** - 若您選擇 **[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。

[在審查防護記錄中啟用追蹤配置變更] - 每次配置變更時通知您。如需詳細資訊，請參閱 [審查防護記錄](#)。

i 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，請參閱 [ESET 知識庫文章](#)。

簡報模式

簡報模式是一項專為要求可不間斷地使用軟體、不想受到通知/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。簡報模式也可在簡報期間使用，在此期間中病毒活動無法干擾簡報。透過啟用此功能，所有的快顯視窗均會停用，而且排程器的活動也將完全停止。然而，系統保護功能仍會在背景執行，不需要和使用者互動。

您可以透過按一下 **[簡報模式]** 旁的 ，在 **主程式視窗** 中的 **[設定] > [電腦]** 底下啟用或停用 **[簡報模式]**。啟用簡報模式有潛在的安全性風險，所以工作列上的防護狀態圖示會變成橙色並顯示警告。您也會在 **主要程式視窗** 中看見這個警告，**[簡報模式作用中]** 則以橙色顯示。

在 **[進階設定] > [工具] > [簡報模式]** 中，啟動 **[以全螢幕執行應用程式時自動啟用簡報模式]**，在您起始全螢幕應用程式時啟動簡報模式，並在離開應用程式後停止。

啟動 **[自動停用簡報模式於]** 以定義一段時間，簡報模式會在這段時間過後自動停用。

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 Endpoint Antivirus 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。
- **[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

啟用電腦掃描器進階記錄 - 記錄透過電腦掃描或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 - 記錄產品與 Direct Cloud 伺服器之間的所有產品通訊。

[**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 - 記錄在 ESET 核心服務中發生的所有事件 (ekrn) 來允許診斷與解決問題。

[**啟用授權進階記錄**] - 記錄與 ESET 啟動和授權伺服器進行的所有產品通訊。

啟用記憶體追蹤 - 記錄所有事件，這些事件可協助開發人員診斷記憶體流失。

[**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**] - 系統將收集其他的作業系統相關資訊，例如執行中的處理程序、CPU 活動、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。

啟用推送訊息進階記錄 - 記錄在推送訊息期間發生的所有事件，以允許診斷和解決問題。

[**啟用即時檔案防護進階記錄**] - 記錄所有發生於即時檔案系統防護中的事件，以便您診斷和解決問題。

[**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。

啟用弱點與修補程式管理進階記錄 - 記錄[弱點與修補程式管理](#)中的所有事件。僅當在您的環境中啟用了弱點與修補程式管理（在 ESET PROTECT Cloud 中啟用）時，才會顯示此設定。

防護記錄檔案位於 `C:\ProgramData\ESET\ESET Security\Diagnostics\`

技術支援

當從 ESET Endpoint Antivirus 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 Endpoint Antivirus 及其模組無法自動更新在 ESET Endpoint Antivirus 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 Endpoint Antivirus 的全域 Proxy 伺服器設定。需連線到網際網路的所有模組，都會使用這裡的參數。

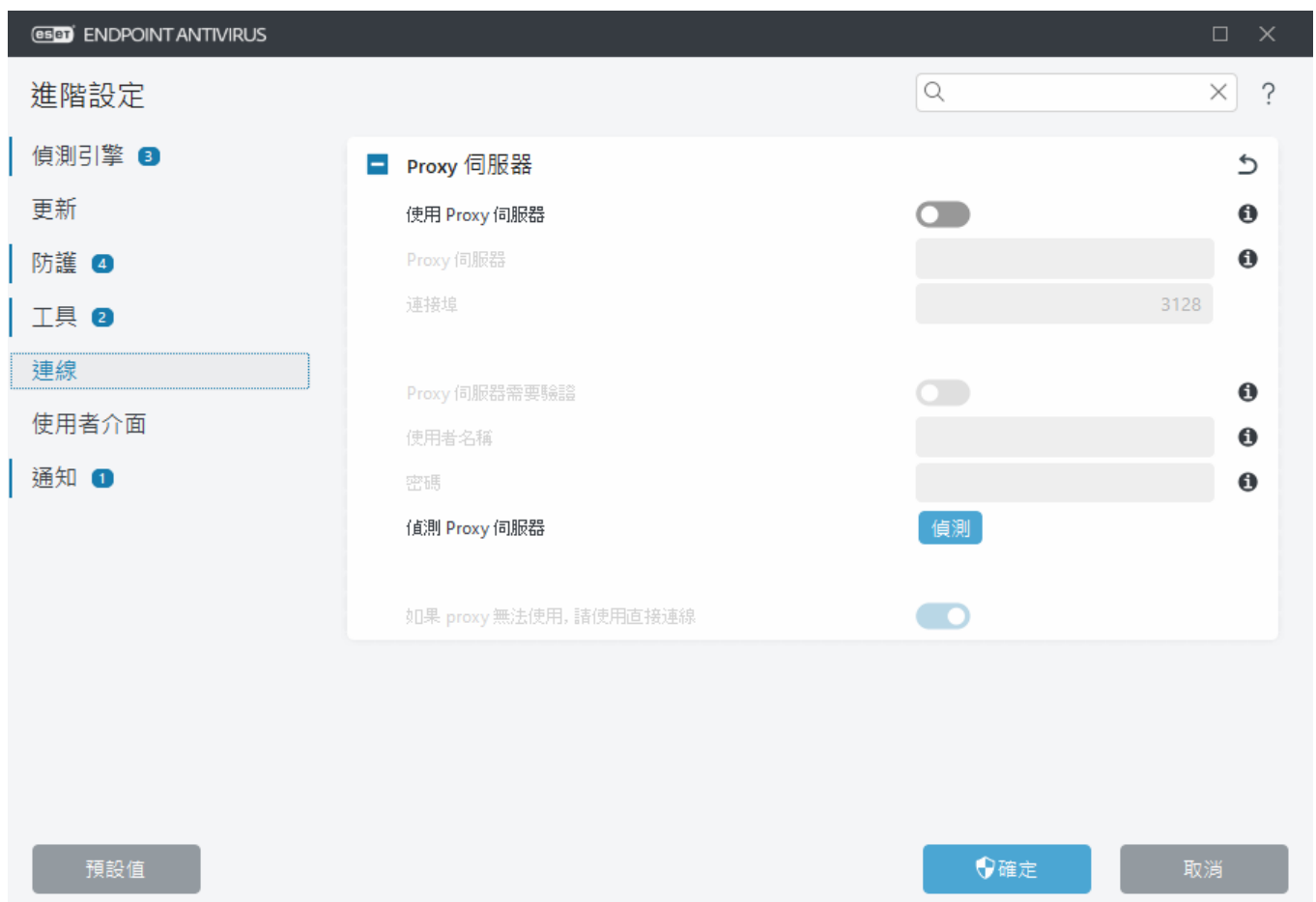
若要指定全域 Proxy 伺服器設定，請啟用 [\[使用 Proxy 伺服器\]](#)，然後鍵入 [Proxy 伺服器](#) 位址以及 Proxy 伺服器的[連接埠](#)號。

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。若要在作業系統中尋找 Proxy 設定，請按 **Windows + I** 快速鍵並按一下 [\[網路與網際網路\]](#) > [\[Proxy\]](#)。ESET Endpoint Antivirus 將複製在 Internet Explorer 或 Google Chrome 的網際網路選項中指定的參數。

i 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 Endpoint Antivirus 已配置為透過 Proxy 連線，而 Proxy 無法存取，ESET Endpoint Antivirus 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。

i 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。

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

另請參閱 [如何將 ESET Endpoint Antivirus 使用者介面縮至最小](#) (適用於受管理環境)。

使用者介面元素

ESET Endpoint Antivirus 中的使用者介面配置選項可讓您調整工作環境以符合您的需要。在 [\[進階設定\]](#) (F5) > [\[使用者介面\]](#) > [\[使用者介面元素\]](#) 中可存取這些配置選項。

您可以在 [\[使用者介面元素\]](#) 區段中調整工作環境。使用 [\[啟動模式\]](#) 下拉式功能表，從下列圖形使用者介面 (GUI) 啟動模式中選取：

完整 - 將會顯示完整的圖形使用者介面 (GUI)。

最小 - GUI 執行中僅向使用者顯示通知。

手動 - GUI 不會在登入時自動啟動。任何使用者都需要手動加以啟動。

無訊息 - 不會顯示任何通知或警告。GUI 只能由管理員啟動。在受管理環境中，或在您需要保留系統資源的情況下，這個模式很有用。

i 一旦選取 [\[最小 GUI 啟動模式\]](#) 且重新啟動電腦之後，則會顯示通知，但不會顯示圖形介面。若要還原為完整圖形使用者介面模式，請從 [\[開始\]](#) 功能表的 [\[所有程式\]](#) > [\[ESET\]](#) > ESET Endpoint Antivirus 之下，以管理員的身分執行 GUI 或者您可以透過 ESET PROTECT 使用 [原則](#) 來還原。

[\[色彩模式\]](#)—從下拉式功能表中選取 ESET Endpoint Antivirus 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 Endpoint Antivirus 的色彩配置
- [\[深色\]](#)—ESET Endpoint Antivirus 將具有深色配置 (深色模式)。
- [\[淺色\]](#)—ESET Endpoint Antivirus 將具有標準、淺色配置。

i 您也可以選擇 [主要程式視窗](#) 右上角的 ESET Endpoint Antivirus GUI 色彩主題。

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

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

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

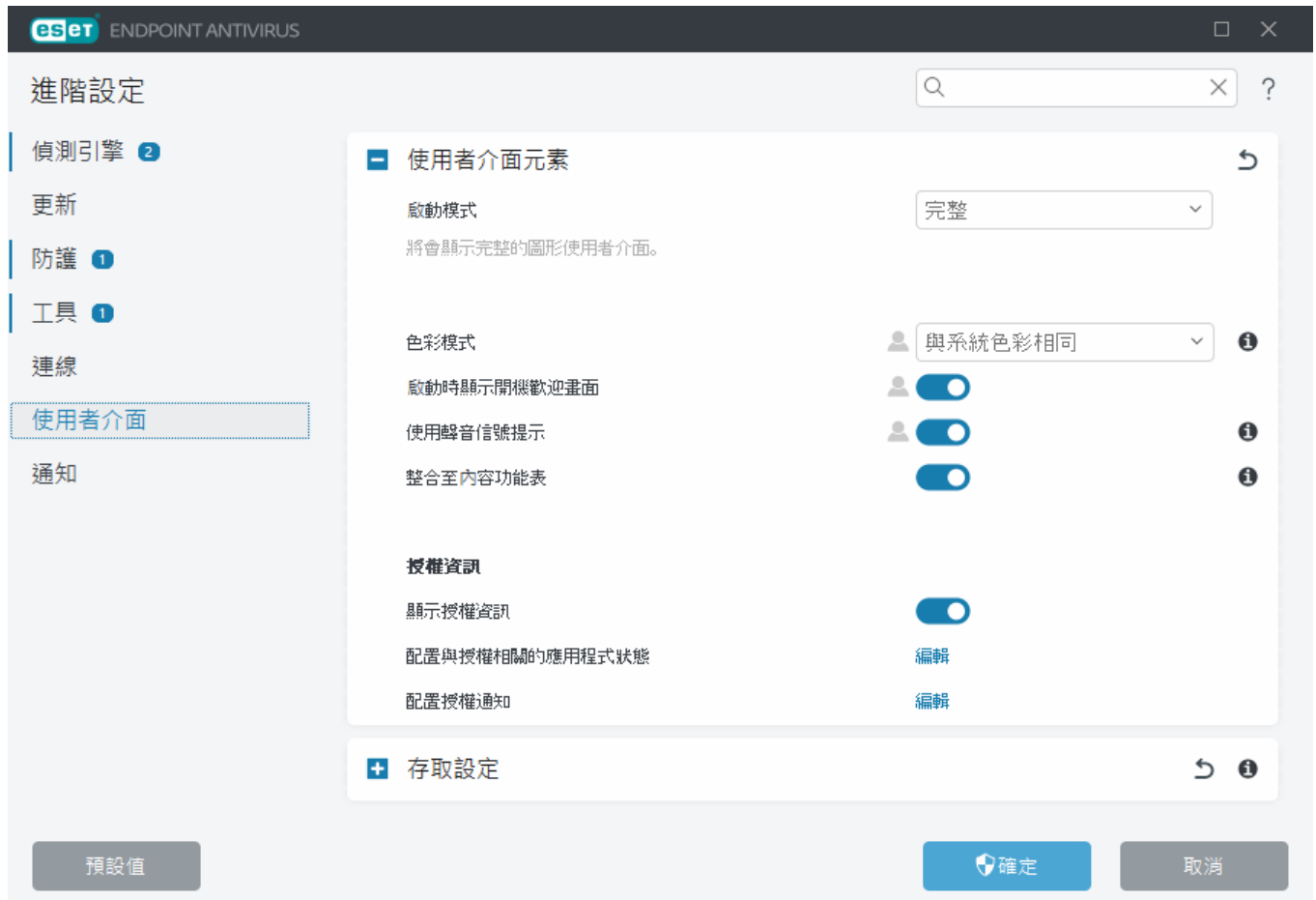
授權資訊

顯示授權資訊 - 停用時，將不會顯示 [防護狀態] 和 [說明及支援] 畫面上的授權到期日。

配置與授權相關的應用程式狀態—開啟與授權相關的[應用程式狀態](#)清單。

配置授權通知—開啟與授權相關的通知清單。

i 將套用授權資訊設定，但使用 MSP 授權啟動的 ESET Endpoint Antivirus 無法存取。



存取設定

ESET Endpoint Antivirus 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 Endpoint Antivirus 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。

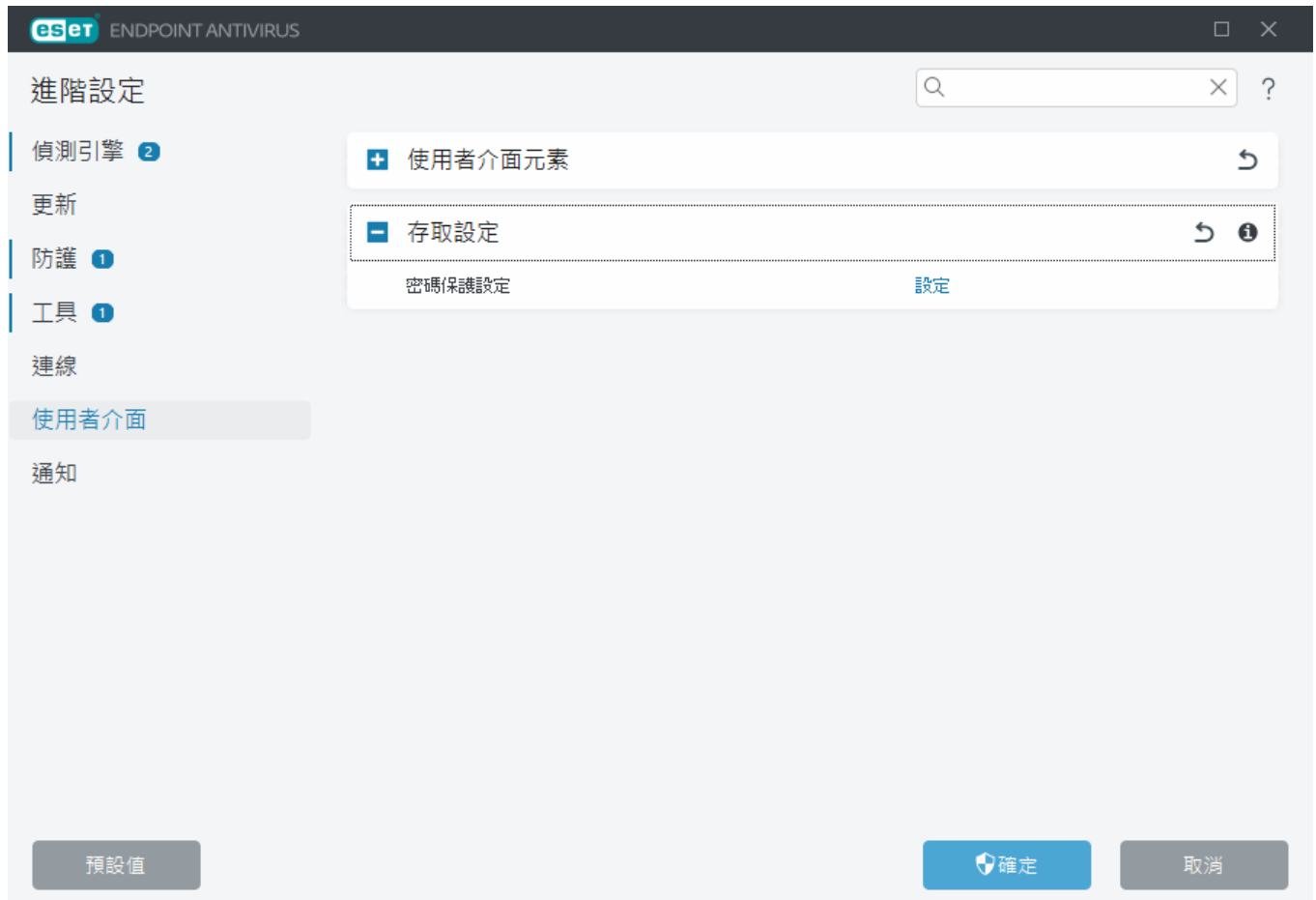
若要設定密碼以保護設定參數和解除安裝 ESET Endpoint Antivirus，請按一下 [\[密碼保護設定\]](#) 旁邊的 [\[設定\]](#)。

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 [\[移除\]](#)。

受管理的環境

管理員可以建立一個原則，以密碼保護已連線用戶端電腦上 ESET Endpoint Antivirus 的設定。若要建立新的原則，請參閱[密碼保護的設定](#)。



進階設定的密碼

若要保護 ESET Endpoint Antivirus 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】**。

受管理的環境

管理員可以建立一個原則，以密碼保護已連線用戶端電腦上 ESET Endpoint Antivirus 的設定。若要建立新的原則，請參閱[密碼保護的設定](#)。

未受管理的

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】**。

日後對 ESET Endpoint Antivirus 進行任何修改，都會需要這個密碼。

如果您忘記密碼，請參閱 [ESET Endpoint 產品中的解鎖設定密碼](#)。

若要恢復遺失的 ESET 授權金鑰、授權的到期日，或 ESET Endpoint Antivirus 的其他授權資訊，請參閱[我遺失了使用者名稱和密碼/授權金鑰](#)。

密碼

為了避免未獲授權的修改，您可以使用密碼保護 ESET Endpoint Antivirus 的設定參數。

安全模式

如果以安全模式啟動 ESET Endpoint Antivirus 的圖形介面，則畫面上會顯示對話方塊視窗，報告將以安全模式執行該應用程式。因為在安全模式中，所有的程式作業會受限，所以不可能以標準模式開啟 ESET Endpoint Antivirus 的圖形介面。

顯示的視窗將使您能夠執行電腦掃描。如果您想檢查電腦是否有惡意代碼，請選取 **[是]** 選項。

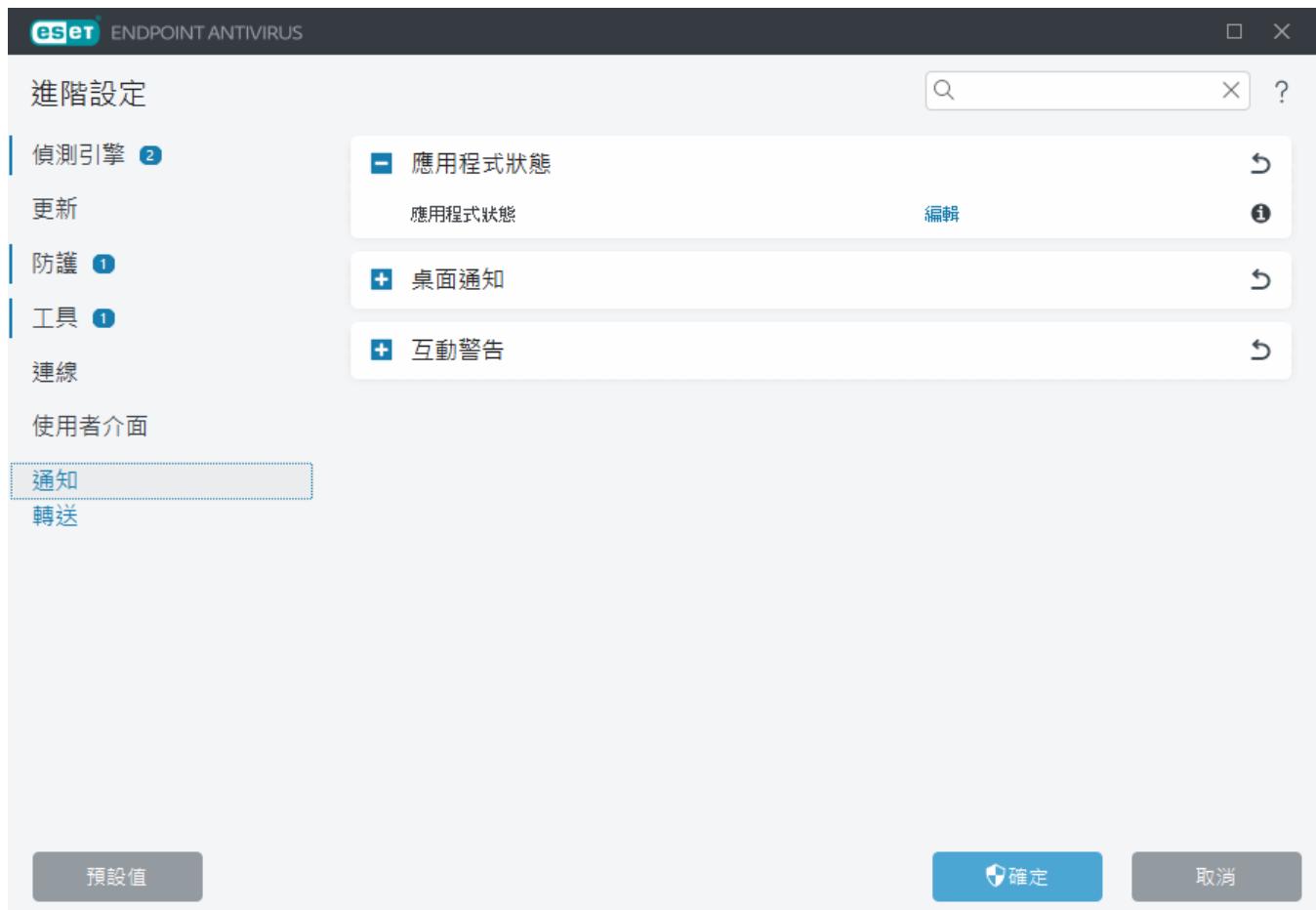
這樣做會在個別視窗中啟動掃描，使用與安裝 ESET Endpoint Antivirus 之後預設電腦掃描設定檔相同的參數。

選取 **[否]** 選項，以關閉對話方塊視窗。ESET Endpoint Antivirus 不會執行任何處理方法。

通知

若要管理 ESET Endpoint Antivirus 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](#)的 **[首頁]** 區段中顯示的通知。
- [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。
- [自訂通知](#) - 將自訂訊息新增至桌面通知（舉例來說）。



[-] 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 的 [首頁] 區段中顯示的應用程式狀態。

應用程式狀態

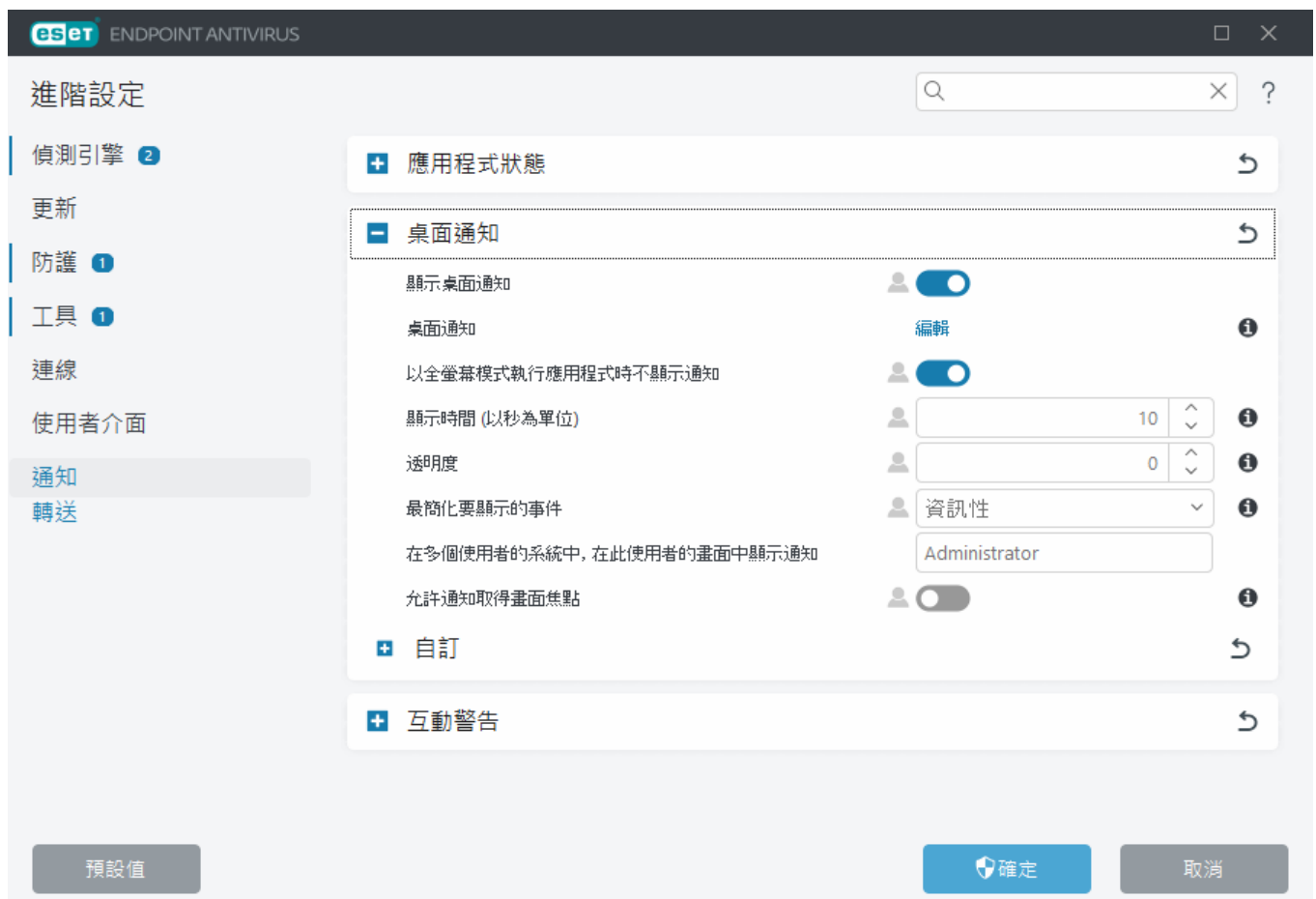
若要配置將顯示哪些應用程式狀態（例如，當您暫停防毒及間諜程式防護或啟用簡報模式時），請開啟 [\[進階設定\]](#) > [通知] 並按一下 [應用程式狀態] 旁邊的 [編輯]。

若您的產品未啟動或授權已到期，系統也會顯示應用程式狀態。此設定可以透過 [ESET PROTECT 原則](#) 來變更。



桌面通知

桌面通知是由系統工作列旁邊的小型通知表示。依預設，它會設定為顯示 10 秒，而後慢慢消失。這是 ESET Endpoint Antivirus 與使用者通訊、通知產品更新成功、已連接新裝置、病毒掃描工作完成或找到新威脅的主要方式。



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。

[逾時（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** - 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** - 僅記錄嚴重錯誤，例如啟動病毒防護或除受感染的系統。

[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 - 通知將取得畫面焦點，且可透過 **Alt+Tab** 存取。

自訂通知

在此視窗中，您可以自訂用於通知的訊息。

預設通知訊息 - 要在通知頁尾中顯示的預設訊息。

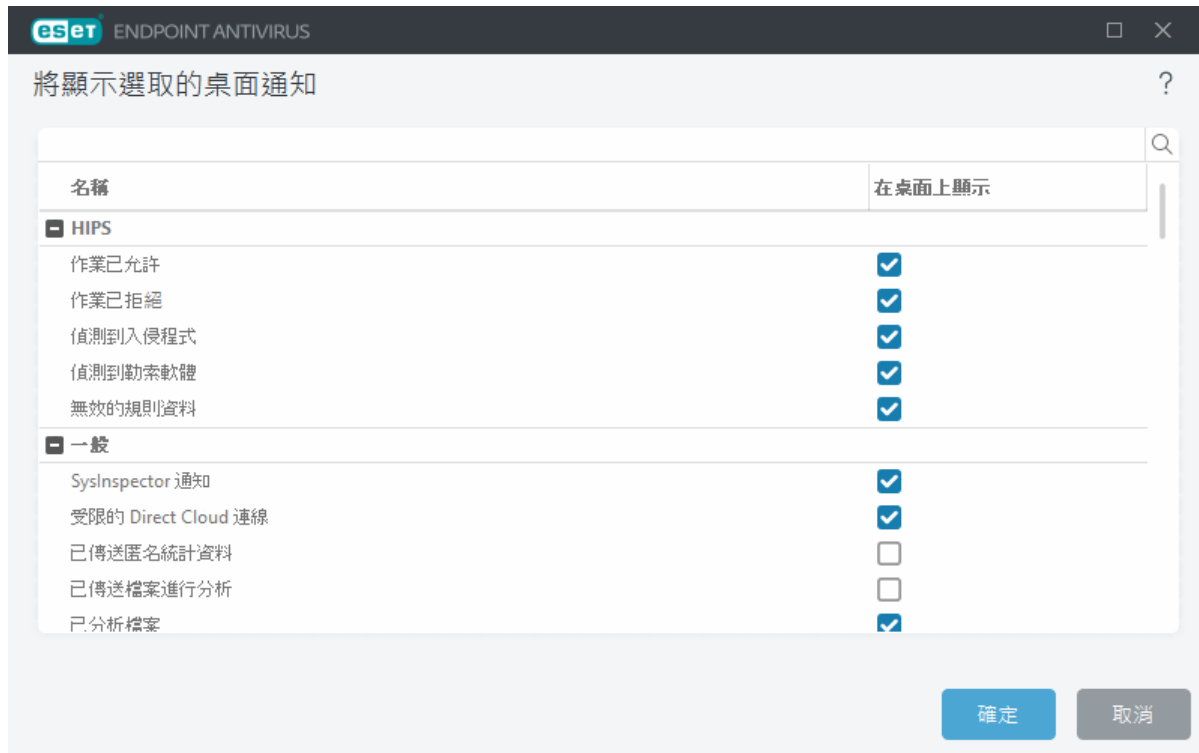
偵測

啟用 **[不自動關閉惡意軟體通知]** 讓惡意軟體通知停留在視窗中，直到手動關閉通知為止。

停用 **[使用預設訊息]** 並在 **[偵測通知訊息]** 欄位中輸入您自己的訊息，以使用自訂的通知訊息。

對話方塊視窗 - 桌面通知

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 **[在桌面上顯示]** 核取方塊。



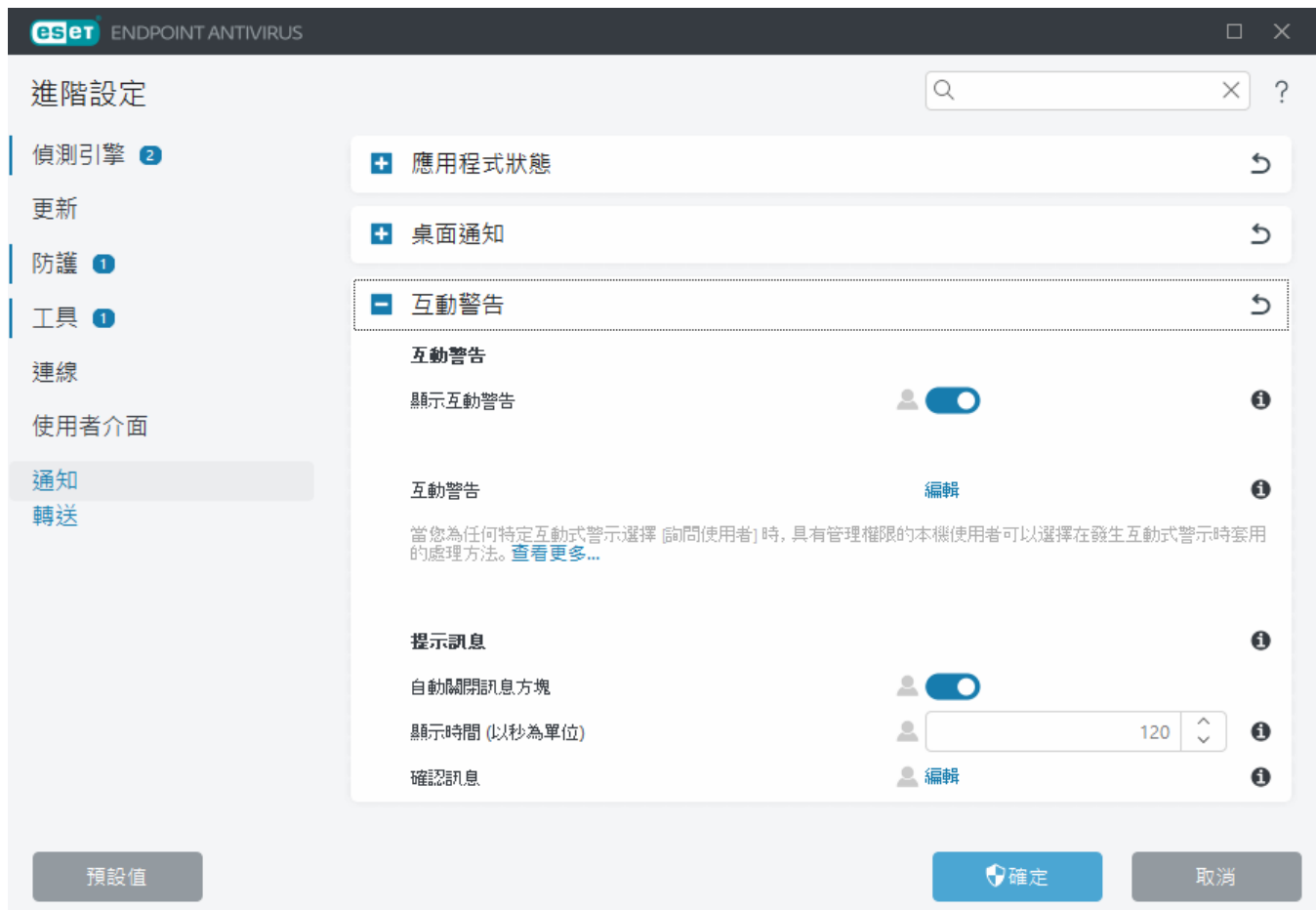
i 如果您想在使用 ESET LiveGuard 時設定 [檔案已分析] 和 [檔案未分析] 通知，則必須將[主動防護](#)設定為 [封鎖執行直到接收到分析結果]。

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](#)
- [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](#)
- [「檔案損毀」或「無法重新命名檔案」](#)
- [網站憑證已撤銷](#)
- [已封鎖網路威脅](#)
- [檔案因分析而遭到封鎖](#)

[進階設定] > [通知] 中的 [互動警示] 區段可讓您配置 ESET Endpoint Antivirus 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【顯示互動警告】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。

- 若為未受管理使用者，建議將此選項保留為預設設定（已啟用）。
- 若為受管理使用者，請將此設定保持啟用狀態，並為[互動警告清單](#)中的使用者選取預先定義的動作。

互動警告一按一下【編輯】以選取要顯示哪個[互動警告](#)。

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。

【逾時（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。

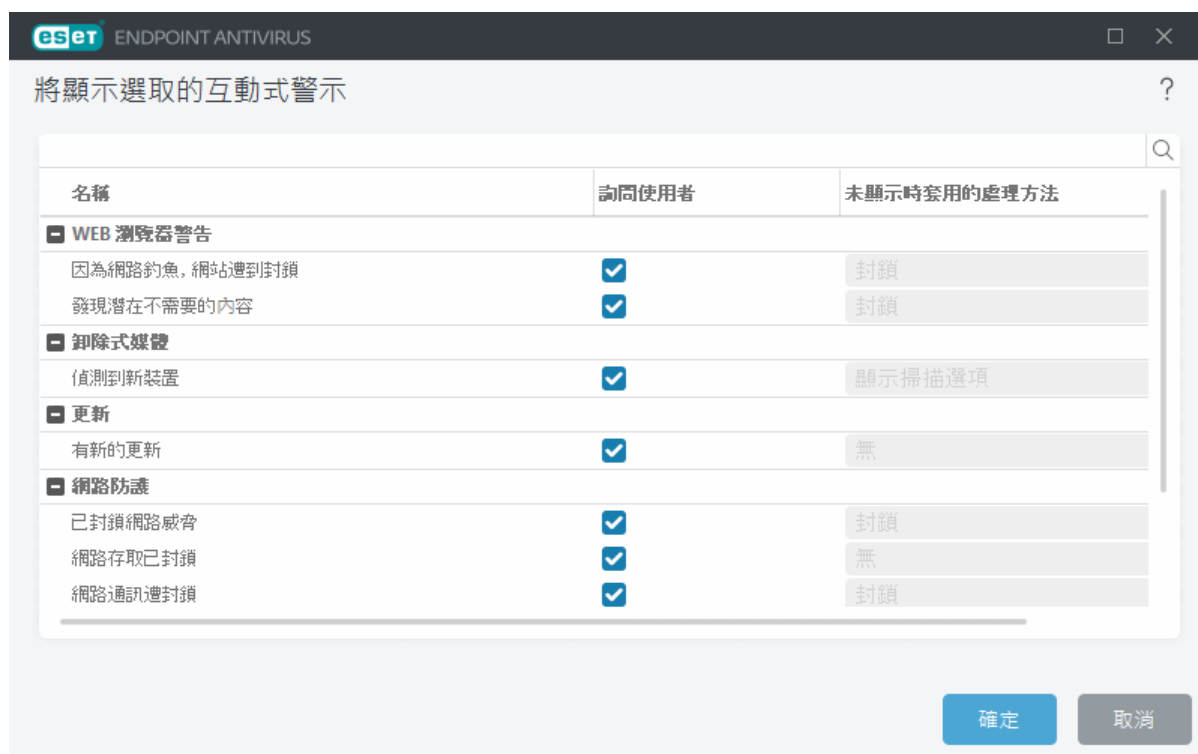
【確認訊息】－ 按一下【編輯】會顯示[確認訊息的清單](#)，並可讓您選擇是否要顯示。

互動警告清單

本節概述 ESET Endpoint Antivirus 將在執行任何動作之前顯示的數個互動警告視窗。

要調整可配置互動警告的行為，請打開 [\[進階設定\]](#) > [\[通知\]](#) > [\[互動警告\]](#)，然後按一下 [\[互動警告\]](#) 旁邊的 [\[編輯\]](#)。

i 適用於管理員可以四處取消選取 **「詢問使用者」** 的受管理環境，並選取在顯示互動警告視窗時套用的預先定義動作。



檢查其他說明區段，找出特定互動警告視窗的參考資訊：

可移除的媒體

- [偵測到新裝置](#)

網路防護

- 當此工作站（來自 ESET PROTECT）的 **「將電腦與網路隔離」** 用戶端工作觸發時，即會顯示 [網路存取已封鎖](#)
- [網路通訊遭封鎖](#)
- [已封鎖網路威脅](#)

Web 瀏覽器警告

- [發現潛在不需要的內容](#)
- [因為網路釣魚，網站遭到封鎖](#)

電腦

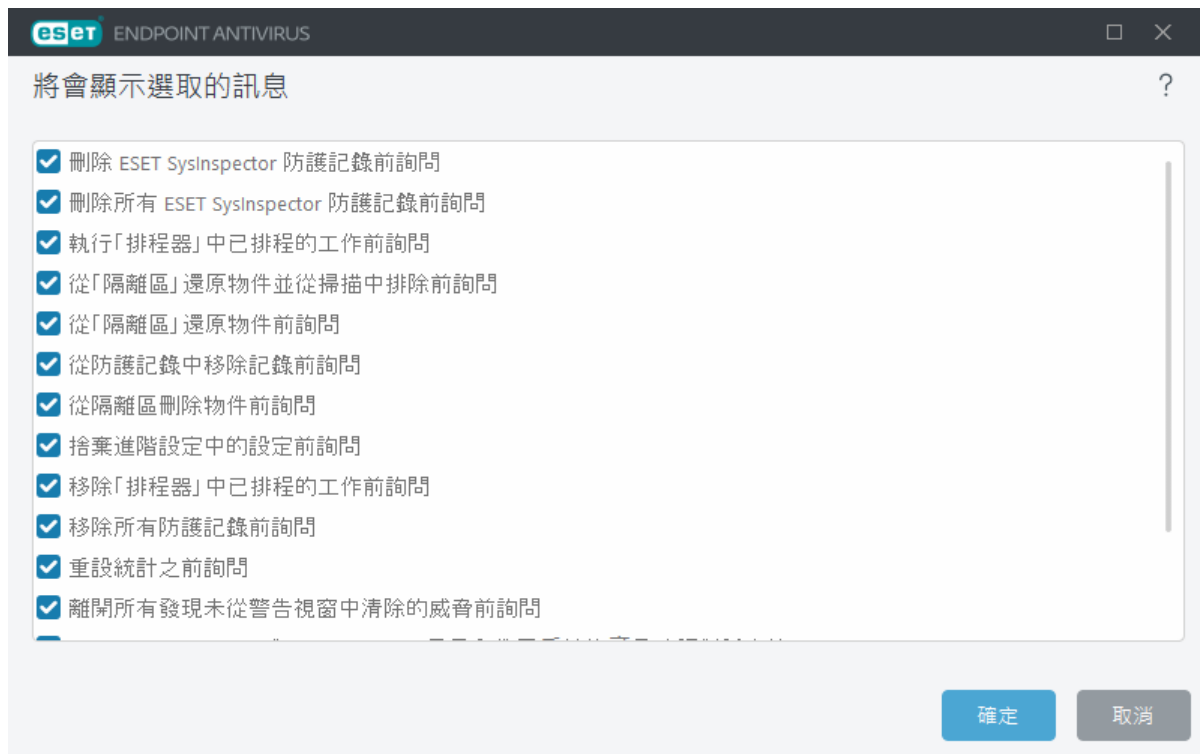
若呈現這些警告，會將使用者介面變更為下列顏色：

- [重新啟動電腦（必要）](#)
- [重新啟動電腦（建議）](#)

i 互動警告未包含偵測引擎²HIPS 或防火牆互動視窗 – 因為其行為可在特定功能中個別配置。

確認訊息

若要調整確認訊息，請瀏覽至 [\[進階設定\]](#) > [\[通知\]](#) > [\[互動警示\]](#)，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 Endpoint Antivirus 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 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](#)

進階設定衝突錯誤

如果某些元件（例如 HIPS）和使用者同時以互動或學習模式建立規則，則可能會發生此錯誤。



如果您想要建立自己的規則，我們建議將過濾模式變更為預設的 **[自動模式]**。請閱讀更多有關 **HIPS 和 HIPS 過濾模式** 的資訊。

需要重新啟動

將 ESET Endpoint Antivirus 升級到新版本或透過[弱點與修補程式管理](#)套用至應用程式後，需要重新啟動電腦。新推出的 ESET Endpoint Antivirus 版本已改善或修正程式模組自動更新所無法解決的問題。

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 **[防護狀態]** 區段手動重新啟動您的電腦。

若要停用「需要重新啟動」或「建議重新啟動」警告，請遵循以下步驟：

1. 打開 **[進階設定] (F5) > [通知] > [互動警告]**。
2. 按一下 **[互動警告]** 旁邊的 **[編輯]**。在 **[電腦]** 區段中，取消選取 **[重新啟動電腦 (必要)]** 和 **[重新啟動電腦 (建議)]** 旁邊的核取方塊。
3. 按一下 **[確定]** 以儲存您在這兩個開啟的視窗中所做的變更。
4. 端點機器上將不再出現警告。
5. (選用) 若要在 ESET Endpoint Antivirus 的主程式視窗中停用應用程式狀態，請從[應用程式狀態視窗](#)中取消選取 **[需要重新啟動電腦]** 和 **[建議重新啟動電腦]** 旁邊的核取方塊。

建議重新啟動

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

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 **[防護狀態]** 區段手動重新啟動您的電腦。

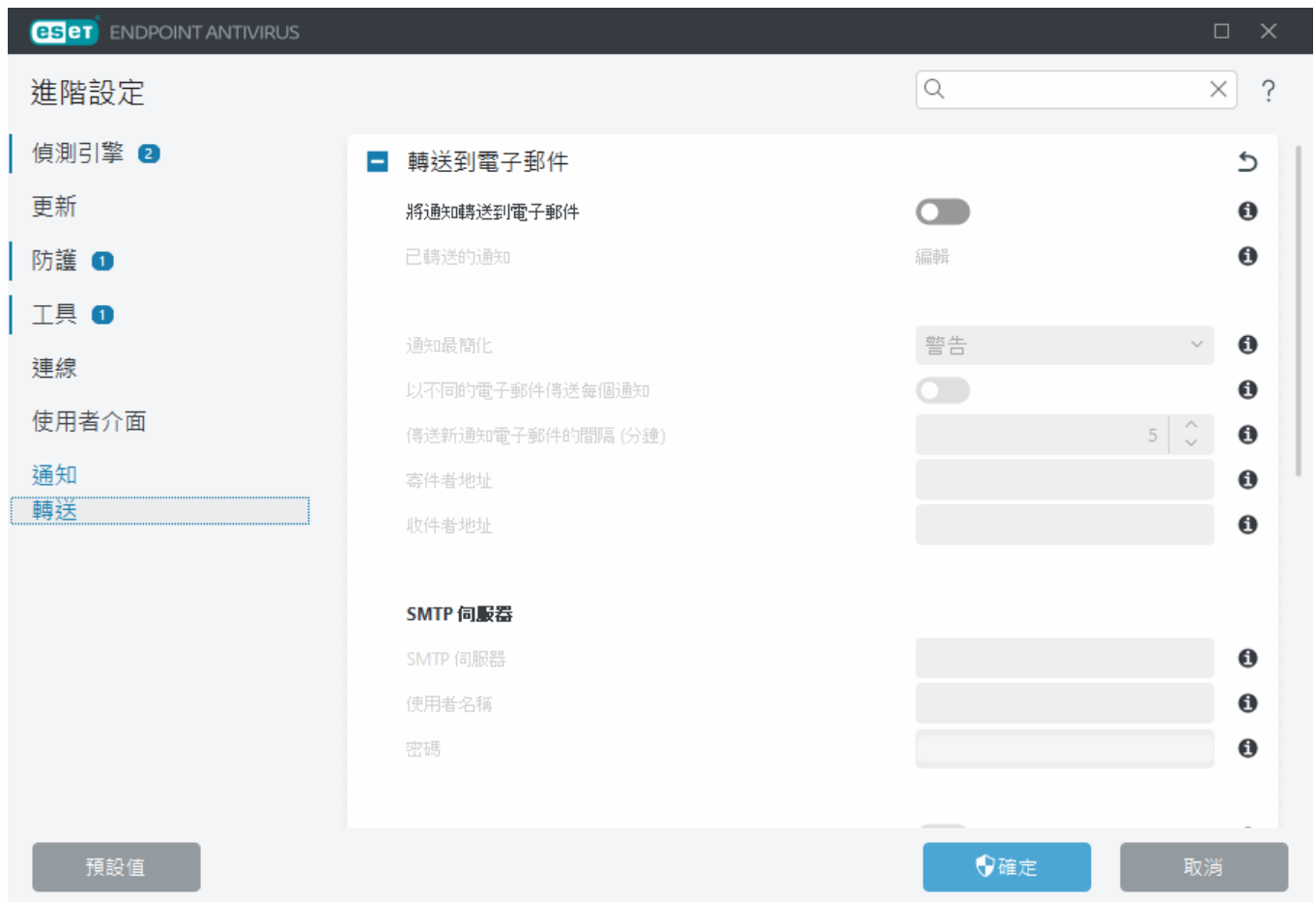
若要停用「需要重新啟動」或「建議重新啟動」警告，請遵循以下步驟：

1. 打開 **[進階設定] (F5) > [通知] > [互動警告]**。
2. 按一下 **[互動警告]** 旁邊的 **[編輯]**。在 **[電腦]** 區段中，取消選取 **[重新啟動電腦 (必要)]** 和 **[重新啟動電腦 (建議)]** 旁邊的核取方塊。
3. 按一下 **[確定]** 以儲存您在這兩個開啟的視窗中所做的變更。
4. 端點機器上將不再出現警告。
5. (選用) 若要在 ESET Endpoint Antivirus 的主程式視窗中停用應用程式狀態，請從[應用程式狀態視窗](#)中取消選取 **[需要重新啟動電腦]** 和 **[建議重新啟動電腦]** 旁邊的核取方塊。

轉送

如果發生與所選簡化層級相關的事件，則 ESET Endpoint Antivirus 可以自動傳送電子郵件通知。[\[進階設定\]](#) > **[通知] > [轉寄] > [轉寄到電子郵件]** 區段，並啟用 **[將通知轉送到電子郵件]** 以啟動電子郵件通知。

已轉送的通知 - 選取將哪些桌面通知轉送到電子郵件。



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）。

i ESET Endpoint Antivirus 支援具備 TLS 加密功能的 SMTP 伺服器。

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

寄件者地址 - 此欄位指定將在通知電子郵件檔頭顯示的寄件者地址。

收件者地址 - 此欄位指定將在通知電子郵件檔頭顯示的收件者地址。使用分號「;」分隔多個電子郵件地址。

啟用 TLS - 啟用 TLS 加密支援的傳送警告及通知訊息。

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，警告訊息及通知的預設格式是最佳的。在部分情況下，您可能需要變更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。我們建議您不要變更此格式。然而，在某些情況下（例如，如果您具有自動電子郵件處理系統），您可能需要變更訊息格式。

[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。

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

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

將所有設定還原為預設值

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 Endpoint Antivirus 的防毒模組可以透過命令列來啟動，具體方法可以是手動（使用 `ecls` 命令）或使用批次 (`bat`) 檔。

ESET 命令列掃描器使用方式：

```
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： <ul style="list-style-type: none"> • none（預設值） - 將不會進行自動清除。 • 標準 – 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 - 無論檔案為何☐ecls.exe 都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

i 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

本章涵蓋的是一些使用者最常詢問的問題以及最常遇到的問題。按一下主題標題，以瞭解如何解決您的問題：

- [如何更新 ESET Endpoint Antivirus](#)
- [如何啟動 ESET Endpoint Antivirus](#)
- [ESET Endpoint Antivirus 偵測到了威脅](#)
- [如何從我的 PC 移除病毒](#)
- [如何在排程器中建立新的工作](#)
- [如何安排每週電腦掃描](#)
- [如何管理通知和互動式警示](#)
- [如何將我的產品連接至 ESET PROTECT](#)
 - [如何使用覆寫模式](#)
 - [如何為 ESET Endpoint Antivirus 套用建議的原則](#)
- [如何配置映像](#)
- [如何利用 ESET Endpoint Antivirus 升級至 Windows 10](#)
- [如何啟動遠端監視和管理](#)

- [如何封鎖從網際網路下載特定檔案類型](#)
- [如何將 ESET Endpoint Antivirus 使用者介面縮至最小](#)

如果您的問題不在以上說明頁面清單中，請嘗試在 ESET Endpoint Antivirus [說明] 頁面搜尋可說明問題的關鍵字或片語。

如果您在 [說明] 頁面內找不到問題的解決方案，可以造訪我們提供常見問題解答的 [ESET 知識庫](#)。

- [如何解除安裝 ESET Endpoint Antivirus](#)
- [防範 Filecoder \(勒索軟體\) 惡意軟體的最佳做法](#)
- [ESET Endpoint Security 和 ESET Endpoint Antivirus 常見問題](#)
- [我應該要開啟第三方防火牆上的哪個位址和連接埠才能使用 ESET 產品的全部功能？](#)

必要的話，您可以連絡我們的線上技術支援中心，以解決您的問題。您可以在主要程式視窗中的 [說明及支援] 窗格中找到線上連絡人表單的連結。

自動更新常見問題



如需在 ESET Endpoint Antivirus 中產品更新相關的其他資訊，請閱讀下列 ESET 知識庫文章：

- [不同 ESET 產品更新及版本類型為何？](#)

電腦會自動更新嗎？重新啟動之前或之後是否會下載更新？

重新啟動之前會進行下載，同時更新的檔案也會準備完成。重新啟動之後，更新的檔案仍僅準備好以供使用，而安裝的版本提供不中斷防護。變更將在下次啟動 ESET Endpoint Antivirus 之後套用。

我擁有大約 3,000 台電腦。所有電腦都會同時下載更新嗎？能否將 Proxy 用於許多電腦的自動更新？

ESET 為大型網路提供鏡像工具和 Proxy 解決方案，因此更新僅從 Internet 下載一次，然後在本地分發。更新較小，通常為 5-10 MB。ESET 將在可用後數周內節流更新。因此，並非所有用戶端在直接連接到 ESET 伺服器時都會同時開始下載。

我可以決定自動更新多少台電腦或哪些電腦嗎？我不想每小時下載十台以上電腦，或者我僅想要現在更新十台電腦，然後過幾天再更新另一台電腦。

受管理環境具有自動更新原則，您可以在其中指定所需的最新版本。萬用字元（例如，9.0.2032.*）也受到支援。如需詳細資訊，請參閱 [ESET PROTECT](#) 或 [ESET PROTECT Cloud](#) 線上說明中的自動更新章節。很抱歉，目前沒有可用於限制自動更新的其他選項。您可以為多個群組指派多個原則。

自動更新是否僅透過原則來配置？如果不想更新 ESET 產品，能否僅停用該原則即可？

如果 ESET Endpoint 產品有「安全性和穩定性」Hotfix，即使自動更新已停用，該產品也將根據適用的使用者授權合約中設定的條款進行更新。ESET 使用「[安全性和穩定性](#)」Hotfix 來解決關鍵問題，並確保 ESET 產品的最大安全性和穩定性。

您可以將自動更新原則指派給任何端點組，而不考慮其目前的自動更新配置。在非受管理的環境中，使用

者可以在 ESET 端點產品的「進階設定」畫面中在本機配置自動更新。

如果我配置原則以使用最早的可用版本，會發生什麼事？即便如此 ESET 也會更新我的產品嗎？

Hotfix 與關鍵 Hotfix (安全性和穩定性更新) 是稍有不同的更新類別。接受使用者設定時，定期 Hotfix 會指派給具有標準優先順序的自動更新。無論使用者設定如何，都將以最高優先順序套用關鍵修補程式。

更新如何在離線情況下運作？使用者何時會使用離線存放庫？

離線存儲庫也包含 .dup 和 .fup 檔案。存放庫區段必須由映像工具下載，而非透過模組更新下載。有關其他資訊，請參閱 ESET PROTECT 線上說明中的[離線存放庫](#)主題。

ESET 產品如何知道需要更新？從存放庫？是否向伺服器傳送了資料？如果 ESET 計劃版本發佈後一個月進行更新，若這適用於全世界 ESET 伺服器能否處理全球發佈？

ESET 產品會從存放庫下載自動更新。伺服器已準備就緒，因為重大更新僅數 KB 大小 ESET 將不會節流在存放庫伺服器上的重大更新。但是，如果自動更新較大，則會有節流伺服器更新的選項。下表提供發生差異性自動更新時的 Hotfix 大小範例：

先前版本	新版本	大小
9.0.2032.2	9.0.2032.6	420 KB
8.1.2037.2	9.0.2032.2	6.5 MB
8.0.2028.0	9.0.2032.2	11.5 MB

如果差異性自動更新失敗 ESET 產品可能會開始完整更新。它仍是一種具有功能保證的自動更新，但不是 .dup 檔案，而是會下載 .fup 這是一個較大的檔案。對於版本 9.0.2032.2 的大小為 27 MB 但是，此類情形很少見。

ESET Endpoint Antivirus 是否以節流方式發佈更新？如果如此，發佈後節流更新的期程大概多久？

新版本發佈後 ESET 會在前幾周內節流更新，以減少伺服器上負載並均衡分發新版本。

自動更新將成為主要升級方法之一。具體而言它如何運作？

ESET 盡可能讓更多客戶透過自動更新進行更新。有太多更早版本難以提供支援。自動更新功能的運作方式十分簡單 - 在第一個模組更新檢查期間下載 .dup 檔案。而在更新程序期間，產品可完全正常運作，並隨時保護電腦。重新啟動之後將啟動新版本。在 ESET PROTECT (伺服器端) 中，您可以使用原則來指定要更新到的最高版本。如需詳細資訊，請參閱 [ESET PROTECT](#) 或 [ESET PROTECT Cloud](#) 線上說明中的自動更新章節。

自動更新在 1/10 時運作是否正確？我現在使用的是 ESET Endpoint Security 8.0.2028.1 如果自動更新執行，將更新至哪個版本？

由於存放庫伺服器上的節流，使用自動更新來更新產品可能會發生延遲。如果產品更新以節流方式發行，

則自動更新檢查可能不會立即收到更新。如果更新被視為安全且穩定，可能會隨後減少或完全移除節流，以便剩餘的用戶端接收更新。

節流程序在每次更新時，可能需要不同時間。具體取決於用戶端要求更新的數量、伺服器上的流量以及其他因素。此程序始終在不斷演變，且隨時會發生變更。

如果我在上午 8:45 啟動電腦並於下午 5:00 關機，那麼自動更新會何時執行？

在下次成功的排程模組更新時，最多每 24 小時更新一次。

如果電腦在執行自動更新時關機，那麼下一次更新將何時執行？

更新將在下次排程的更新時間範圍時執行。自動更新（先前稱為 uPCU）程序具有強大的故障保全機制。下載更新並重新啟動電腦之後，更新的檔案仍僅準備好以供使用，而安裝的版本提供不中斷防護。變更將在下次啟動 ESET 端點產品之後套用。

如何在不等待每隔 24 小時執行定期連線的情況下立即執行自動更新？是否還有其他方式可以按一下「檢查更新」？

您僅能在開啟主程式視窗並按一下 **[更新]** > **[檢查更新]** 時，手動啟動自動更新程序。啟動模組更新的所有其他方式皆會反映 24 小時自動更新排程器原則。目前無法遠端啟動自動更新下載。我們會在以後的更新中新增此功能。

如何更新 ESET Endpoint Antivirus

您可以手動也可以自動執行 ESET Endpoint Antivirus 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。若要變更間隔，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 **[智慧型掃描]**，開始掃描系統。
3. 完成掃描之後，請檢閱已掃描、受感染及已清除的檔案防護記錄。
4. 如果您想要僅掃描磁碟的某一部分，請按一下 **[自訂掃描]**，並選取要進行病毒掃描的目標。

如需其他資訊，請參閱我們定期更新的 [ESET 知識庫文章](#)。

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](#) > **[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 **[新增工作]**
2. 從下拉式功能表中選取 **[指定電腦掃描]**
3. 輸入工作的名稱並針對工作頻率選取 **[每星期]**
4. 設定執行工作的日期及時間。
5. 若已安排的工作因故無法執行（例如電腦已關機），請選取 **[盡快執行工作]** 以稍後執行工作。
6. 檢閱已排程工作的摘要，並按一下 **[完成]**
7. 從 **[目標]** 下拉式功能表中，選取 **[本機磁碟]**
8. 按一下 **[完成]** 以套用工作。

如何連接 ESET Endpoint Antivirus 至 ESET PROTECT

當您已在電腦上安裝 ESET Endpoint Antivirus 且您想要透過 ESET PROTECT 進行連接時，確保您也在用戶端工作站上安裝了 ESET Management 代理程式。對於與 ESET PROTECT 伺服器通訊的每個用戶端解決方案，這個代理程式是不可或缺的部分。

- [在用戶端工作站上安裝或部署 ESET Management 代理程式](#)

另請參閱：

- [遠端受管端點適用的文件](#)
- [如何使用覆寫模式](#)
- [如何為 ESET Endpoint Antivirus 套用建議的原則](#)

如何使用覆寫模式

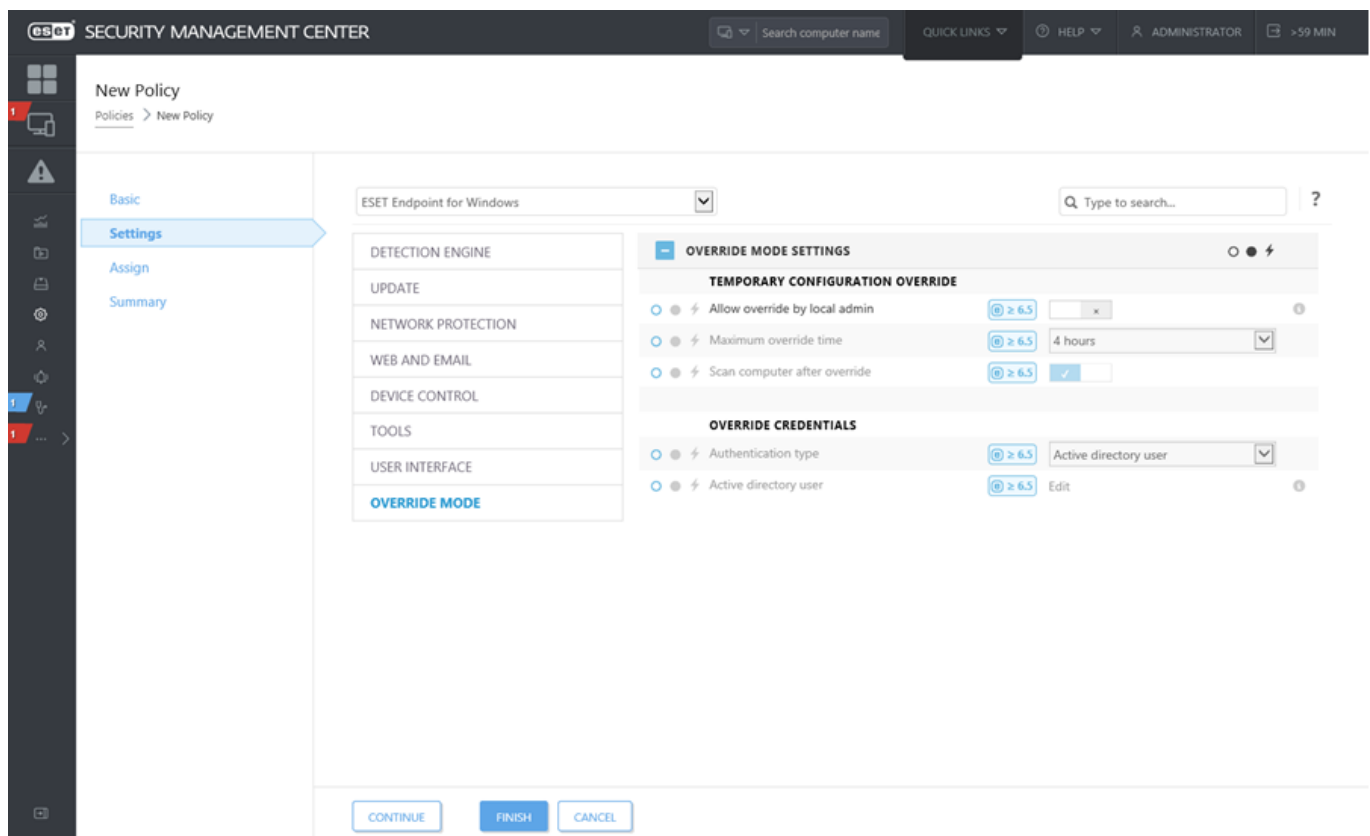
使用者若具有適用於其機器上安裝之 Windows 的 ESET 產品 (6.5 版及以上版本)，即可使用覆寫功能。覆寫模式可讓用戶端電腦層級上的使用者變更已安裝之 ESET 產品中的設定，即使已對這些設定套用原則也一樣。可對特定 AD 使用者啟用覆寫模式，或可用密碼保護此覆寫模式。啟用此功能的時間一次不得超過四小時。

啟用覆寫模式後就無法透過 ESET PROTECT Web 主控台將其停止。覆寫期間過期時就會自動停用覆寫模式。您也可在用戶端機器上關閉此模式。

- !** 使用覆寫模式的使用者也需要具有 Windows 系統管理員權限。否則，使用者無法儲存 ESET Endpoint Antivirus 設定中的變更。
支援 Active Directory 群組驗證。

若要設定 **[覆寫模式]**

1. 瀏覽至 **[原則]** > **[新增原則]**
2. 在 **[基本]** 區段中，輸入此原則的 **[名稱]** 及 **[說明]**
3. 在 **[設定]** 區段中，選取 **[ESET Endpoint for Windows]**
4. 按一下 **[覆寫模式]** 並配置覆寫模式的規則。
5. 在 **[指派]** 區段中，選取將套用此原則的電腦或電腦群組。
6. 檢閱 **[摘要]** 區段中的設定，然後按一下 **[完成]** 來套用原則。



如果 John 在使用此端點設定，封鎖其機器上的某些重要功能或 Web 存取時發生問題，則管理員可允許 John 覆寫其現有的端點設定，並在其機器上手動調整設定。之後 ESET PROTECT 可以要求這些新的設定，因此管理員可以根據它們建立新原則。

若要這麼做，請遵循以下步驟：

1. 瀏覽至 [原則] > [新增原則]
2. 完成 [名稱] 和 [說明] 欄位。在 [設定] 區段中，選取 [ESET Endpoint for Windows]
3. 按一下 [覆寫模式]、啟用覆寫模式一小時，並選取 John 作為 AD 使用者。
4. 將原則指派給 John 的電腦，然後按一下 [完成] 來儲存原則。
5. John 必須在其 ESET 端點上啟用 [覆寫模式]，並在此機器上手動變更設定。
- ✓ 6. 在 ESET PROTECT Web 主控台上，瀏覽至 [電腦]、選取 John 的電腦，然後按一下 [顯示詳細資料]
7. 在 [配置] 區段中，按一下 [要求配置] 來排定用戶端工作，從用戶端 ASAP 中取得配置。
8. 不久之後，新配置將出現。按一下產品上您要儲存的設定，然後按一下 [開啟配置]
9. 您可以檢閱設定，然後按一下 [轉換為原則]
10. 完成 [名稱] 和 [說明] 欄位。
11. 在 [設定] 區段中，您可在需要時修改設定。
12. 在 [指派] 區段中，您可以將此原則指派給 John 的電腦（或其他人的電腦）。
13. 按一下 [完成] 來儲存設定。
14. 不再需要覆寫原則時，別忘了將其移除。

如何為 ESET Endpoint Antivirus 套用建議的原則

在將 ESET Endpoint Antivirus 連接至 ESET PROTECT 後的最佳實務是套用建議的[原則](#)或套用自訂的原則。

有數個適用於 ESET Endpoint Antivirus 的內建原則：

原則	說明
防毒 - 平衡	適用於大多數設定的建議安全性配置。
防毒 - 最大安全性	利用機器學習、深度的行為檢查及 SSL 過濾。潛在不安全、不需要且可疑的應用程式偵測則會受到影響。
雲端型聲譽及意見系統	啟用 ESET LiveGrid® 雲端型聲譽及意見系統以改進最新威脅的偵測，以及協助分享惡意或未知的可能威脅，以進行日後分析。
裝置控制 - 最大安全性	已封鎖所有裝置。任何裝置需要管理員允許才能進行連線。
裝置控制 - 唯讀	所有裝置為唯讀狀態。不允許寫入。
防火牆 - 封鎖除了 ESET PROTECT 及 ESET Inspect 連線以外的所有流量	封鎖所有流量，除了與 ESET PROTECT 和 ESET Inspect 伺服器 （僅 ESET Endpoint Security）連線。
記錄 - 完整的診斷記錄	此範本將會確保系統管理員在需要時擁有所有可用的防護記錄。所有內容將以最簡化的方式記錄，包含 HIPS 和 ThreatSense 以及防火牆。防護記錄會在 90 天後自動刪除。
記錄 - 僅記錄重要事件	原則會確保記錄所有警告、錯誤和重要事件。防護記錄會在 90 天後自動刪除。
可視度 - 平衡	可視度的預設設定。已啟用狀態和通知。
可視度 - 隱藏模式	已停用通知、警告、 GUI 以及內容功能表整合。系統將不會執行 egui.exe 僅適用於來自 ESET PROTECT Cloud 的管理。
可視度 - 減少使用者互動	已停用狀態、已停用通知、已顯示 GUI

若要設定名為 **[防毒 – 最大安全性]** 的原則，而這個原則會強制執行 50 個以上、適用於在工作站上安裝的 ESET Endpoint Antivirus 的建議設定，請遵循下列步驟：

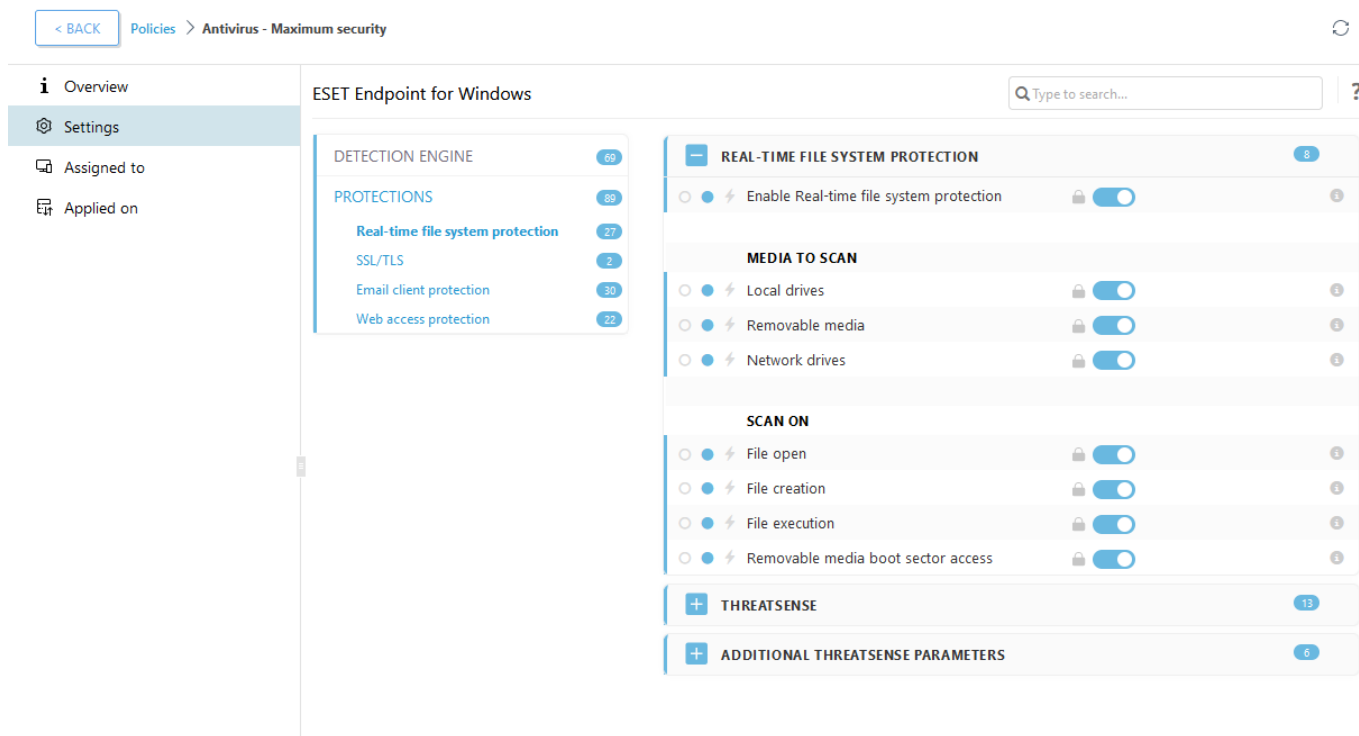
i 下列 ESET 知識庫文章可能僅以英文提供：
[使用 ESET PROTECT 套用 ESET Endpoint Antivirus 的建議或預先定義原則](#)

1. 開啟 ESET PROTECT Web 主控台。
2. 瀏覽至 **[原則]** 並展開 **[內建原則]** > **[ESET Endpoint for Windows]**
3. 按一下 **[防毒 – 最大安全性 – 建議]**
4. 在 **[指派給]** 索引標籤，按一下 **[指派用戶端]** 或 **[指派群組]** 並選取您想要套用此原則的適當電腦。

	NAME	POLI...	TAGS	DESC...	MODIFICATION TIME	LAST ...
<input type="checkbox"/>	Device control - Maximum security	ESET Eni		All de...	December 22, 2022 19:50:...	Admi...
<input type="checkbox"/>	Device control - Read only	ESET Eni		All de...	December 22, 2022 19:50:...	Admi...
<input type="checkbox"/>	Firewall - Block all traffic except ESET PR...	ESET Eni		Block ...	December 22, 2022 19:50:...	Admi...
<input type="checkbox"/>	Logging - Full diagnostic logging	ESET Eni		This t...	December 22, 2022 19:50:...	Admi...
<input type="checkbox"/>	Logging - Log important events only	ESET Eni		Policy...	December 22, 2022 19:50:...	Admi...
<input type="checkbox"/>	Antivirus - Balanced	ESET Eni		Securi...	December 22, 2022 19:50:...	Admi...
<input checked="" type="checkbox"/>	Antivirus - Maximum security	ESET Eni		Takin...	December 22, 2022 19:50:...	Admi...
<input type="checkbox"/>	Visibility - Balanced	ESET Eni		Defaul...	December 22, 2022 19:50:...	Admi...
<input type="checkbox"/>	Visibility - Invisible mode	ESET Eni		Disabl...	December 22, 2022 19:50:...	Admi...
<input type="checkbox"/>	Visibility - Reduced interaction with user	ESET Eni		Disabl...	December 22, 2022 19:50:...	Admi...
<input type="checkbox"/>	Cloud-based reputation and feedback sy...	ESET Eni		Enabl...	December 22, 2022 19:50:...	Admi...
<input type="checkbox"/>	ESET LiveGuard - Enable	ESET Eni		Enabl...	December 22, 2022 19:50:...	Admi...
<input type="checkbox"/>	ESET LiveGuard - Submit scripts and exec...	ESET Eni		Enabl...	December 22, 2022 19:50:...	Admi...
<input type="checkbox"/>	ESET LiveGuard - Optimal protection ...	ESET Eni		Docu...	June 27, 2023 10:49:29	Admi...

若要了解此原則中套用的設定，按一下 **[設定]** 索引標籤並展開進階設定樹狀目錄。

- 藍點代表此原則已變更的設定
- 藍框中的數字代表此原則已變更的設定數
- [閱讀更多關於 ESET PROTECT 原則的資訊](#)



如何配置映像

ESET Endpoint Antivirus 可配置為儲存偵測引擎更新檔案的副本並散佈更新至其他執行 ESET Endpoint Antivirus 或 ESET Endpoint Security 的工作站。

更新映像以建立更新檔案的副本，這些副本可用於更新執行相同世代的 ESET Endpoint Antivirus for Windows 的工作站。（例如 ESET Endpoint Antivirus for Windows 10.x 版僅為 ESET Endpoint Antivirus for Windows 和 ESET Endpoint Security for Windows 10.x 版建立更新檔案）

配置 ESET Endpoint Antivirus 為映像伺服器以透過內部 HTTP 伺服器提供更新

1. 按 **F5** 以存取 [進階設定] 並展開 [更新] > [設定檔] > [更新映像]
2. 展開 [更新] 並確定已啟用 [模組更新] 底下的 [自動選擇] 選項。
3. 展開 [更新映像] 並啟用 [建立更新映像] 和 [啟用 HTTP 伺服器]

如需詳細資訊，請參閱：

- [更新映像](#)
- [從映像更新](#)

配置映像伺服器以透過共用網路資料夾提供更新

1. 在本機或網路裝置上建立共用資料夾。此資料夾必須可由執行 ESET 安全解決方案的所有使用者讀取並可從本機的 SYSTEM 帳戶寫入。
2. 啟動 [進階設定] > [更新] > [設定檔] > [更新映像] 之下的 [建立更新映像]
3. 按一下 [清除] 以選擇適當的 [儲存資料夾]，然後按一下 [編輯]。瀏覽並選取已建立的共用資料夾。

如果您不想要透過內部 HTTP 伺服器提供模組更新，請停用 [啟用 HTTP 伺服器]

如何利用 ESET Endpoint Antivirus 升級至 Windows 10

! 我們強烈建議您在升級至 Windows 10 之前，將您的 ESET 產品升級至最新版本並下載最新的模組更新。這可確保您的程式設定和授權資訊在升級至 Windows 10 期間獲得完整防護及保留。

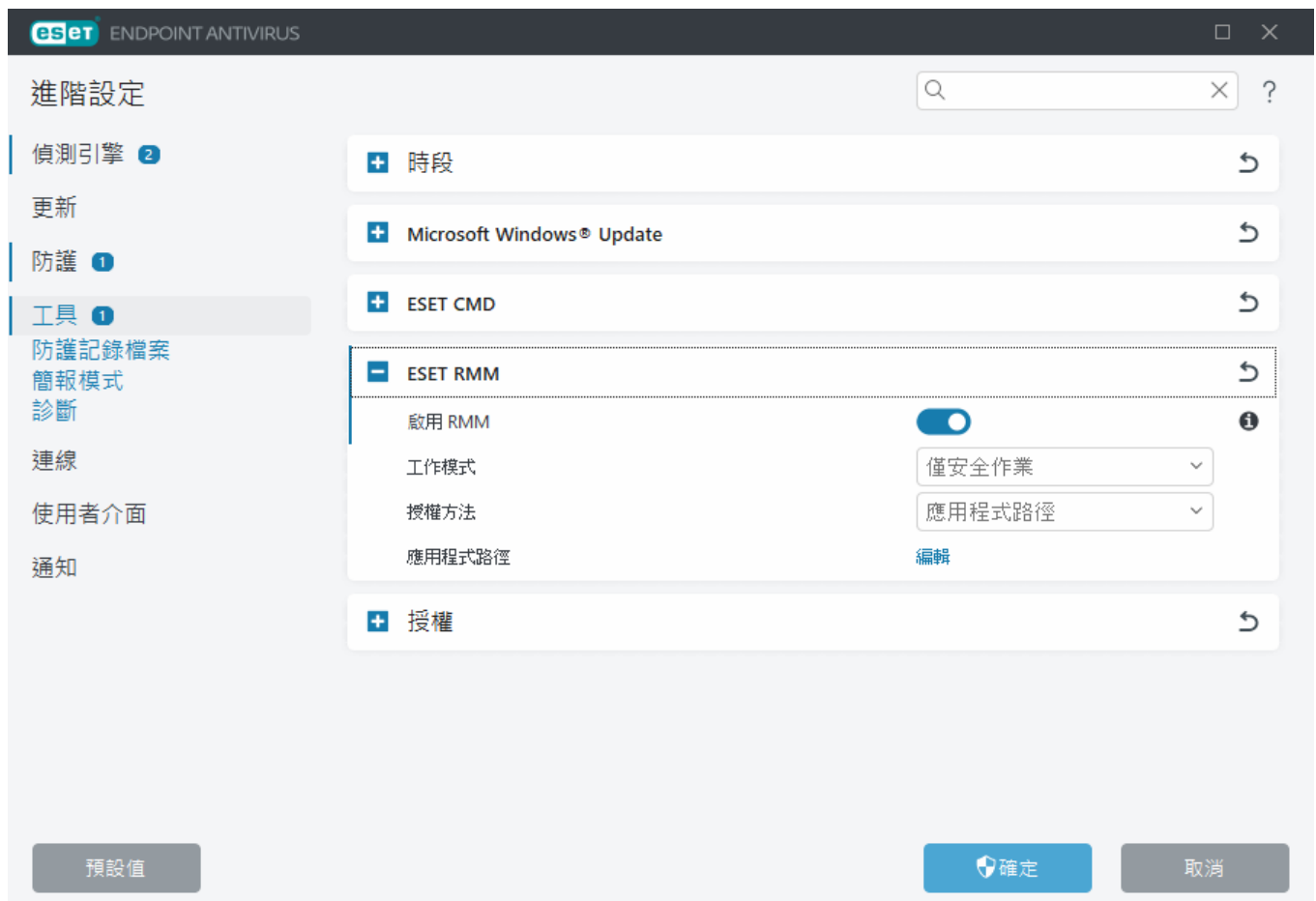
其他語言版本：

如果您正在尋找您 ESET 端點產品的其他語言版本，請造訪我們的[下載頁面](#)。

i [有關 ESET 商業產品與 Windows 10 相容性的詳細資訊](#)

如何啟動遠端監視和管理

遠端監視和管理 (RMM) 是使用管理服務提供者可以存取的本機安裝代理程式來監督和控制軟體系統（例如桌上型電腦、伺服器 and 行動裝置上的軟體系統）的程序。從 6.6.2028.0 版起 RMM 可以管理 ESET Endpoint Antivirus。



預設會停用 ESET RMM。若要啟用 ESET RMM，請開啟 [\[進階設定\]](#) > **[工具]** > **[ESET RMM]**，然後啟用 **[啟用 RMM]** 旁邊的切換開關。

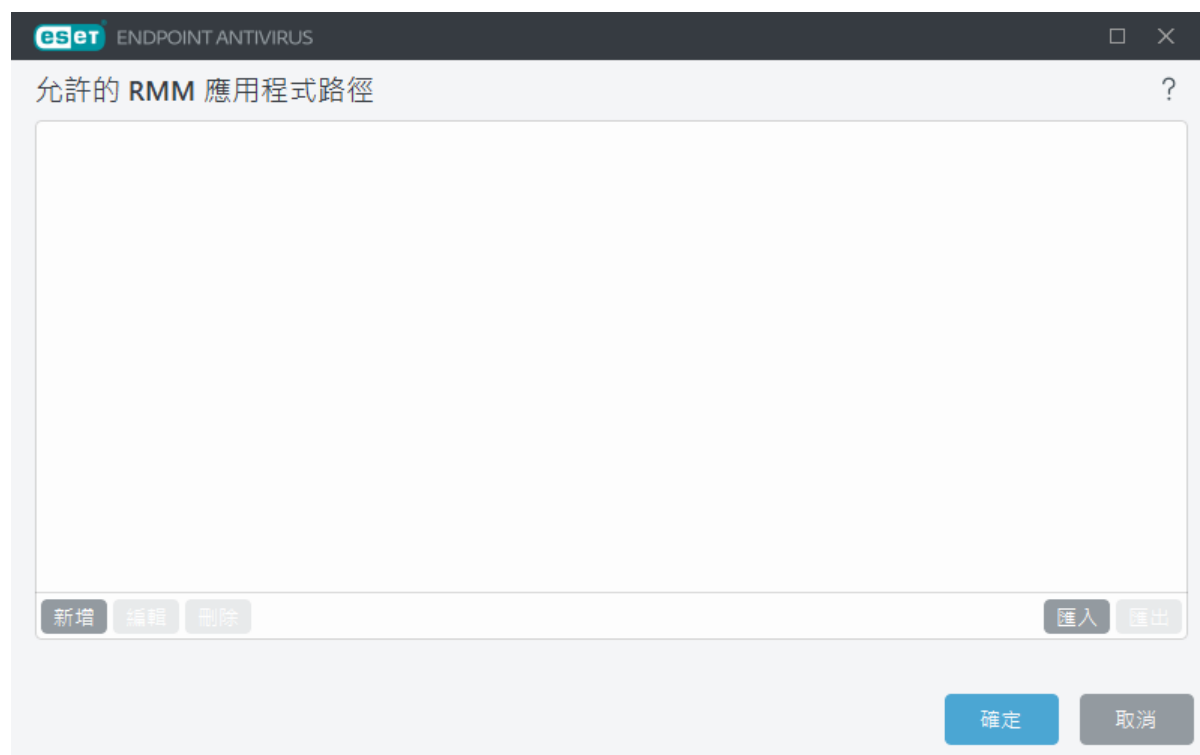
工作模式 - 如果您想讓 RMM 介面能夠進行安全和唯讀作業，請選取 **[僅安全作業]**。如果您想讓 RMM 介面能夠進行所有作業，請選取 **[所有作業]**。

操作	模式 - 僅安全作業	模式 - 所有作業
取得應用程式 - 資訊	✓	✓
取得配置	✓	✓
取得授權資訊	✓	✓
取得防護記錄	✓	✓
取得防護狀態	✓	✓
取得更新狀態	✓	✓
設定配置		✓
開始啟動		✓
開始掃描	✓	✓
開始更新	✓	✓

授權方法 - 設定 RMM 授權方法。若要使用授權，請從下拉式功能表選取 **[應用程式路徑]**，否則選取 **[無]**。

! RMM 應該一律使用授權來防止惡意軟體停用或規避 ESET 端點防護。

應用程式路徑 - 獲准執行 RMM 的特定應用程式。如果您已選取 **[應用程式路徑]** 做為授權方法，請按一下 **[編輯]** 以開啟 **[允許的 RMM 應用程式路徑]** 配置視窗。



新增 - 建立新允許的 RMM 應用程式路徑。輸入路徑或按一下 **[...]** 按鈕以選取可執行檔。

編輯 - 修改現有的允許路徑。如果可執行檔的位置已變更為其他資料夾，請使用 **[編輯]**。

刪除 - 刪除現有的允許路徑。

預設 ESET Endpoint Antivirus 安裝包含 ermm.exe 檔案，該檔案位於 Endpoint 應用程式目錄（預設路徑 **C:\Program Files\ESET\ESET Security\ermm.exe**）會與連結到 RMM 伺服器的 RMM 外掛程式（會與 RMM 代理

程式通訊) 交換資料。

- ermm.exe – ESET 所開發的命令列公用程式，能夠管理 Endpoint 產品並與任何 RMM 外掛程式通訊。
- RMM 外掛程式是在 Endpoint Windows 系統本機執行的第三方應用程式。此外掛程式設計用來與特定 RMM 代理程式 (如僅與 Kaseya) 以及與 ermm.exe 通訊。
- RMM 代理程式是在 Endpoint Windows 系統本機執行的第三方應用程式 (例如來自 Kaseya)此代理程式會與 RMM 外掛程式以及與 RMM 伺服器通訊。

如何封鎖從網際網路下載特定檔案類型

如果您不想要允許從網際網路下載特定的檔案類型 (例如 exe 或 pdf 或 zip) 請搭配使用 [URL 位址管理](#) 與萬用字元的組合。按下 F5 鍵以存取 **進階設定**。按一下 **[Web 和電子郵件] > [Web 存取防護]**，並展開 **URL 位址管理**。按一下 **位址清單** 旁邊的 **[編輯]**

在 **[位址清單]** 視窗中，選取 **[已封鎖位址清單]**，並按一下 **[編輯]** 或 **[新增]** 來建立/編輯清單。新視窗即會出現。如果您是建立新清單，請從 **[位址清單類型]** 下拉式清單中選取 **[已封鎖]**，並命名清單。如果您想要在從目前清單中存取檔案類型時收到通知，請啟用 **[在套用時通知]** 切換開關。從下拉式清單中選取 **[記錄嚴重性]** ESET PROTECT 可以收集具有 **[警告]** 冗贅的記錄。

資訊和警告記錄詳細資訊僅適用於在網域中包含至少兩個元件 (沒有萬用字元) 的規則。例如：



- *.domain.com/*
- *www.domain.com/*



按一下 **【新增】** 以輸入一個遮罩，指定您要封鎖下載的檔案類型。如果您想要封鎖從特定網站下載特定檔案的作業，請輸入完整 URL。例如，`http://example.com/file.exe`。您可以使用萬用字元來涵蓋一組檔案。問號 (?) 代表一個變數字元，而星號 (*) 代表含有零或多個字元的變數字串。例如，遮罩 `*/*.zip` 會封鎖下載所有壓縮的 zip 檔案。

請留意，您僅能夠在副檔名是此檔案 URL 的一部份時，使用此方法來封鎖特定檔案類型的下載。如果此網頁使用檔案下載 URL (例如，`www.example.com/download.php?fileid=42`)，即使位於此連結的任何檔案的副檔名已遭您封鎖，系統都會將其下載。

如何將 ESET Endpoint Antivirus 使用者介面縮至最小

遠端管理時，您可以套用 [「可視度」預先定義原則](#)。

若未停用，請手動執行下列步驟：

1. 按 **F5** 以存取進階設定，並展開 **【使用者介面】 > 【使用者介面元素】**。
2. 將 **【啟動模式】** 設定為所需的值。 [更多有關啟動模式的資訊](#)。
3. 停用 **【啟動時顯示開機歡迎畫面】** 和 **【使用聲音信號提示】**。
4. 配置 [通知](#)。

5. 配置[應用程式狀態](#)
6. 配置[確認訊息](#)
7. 配置[警告及訊息方塊](#)

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-ROM DVD 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開道功能，則「使用者」數目應等於由該開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、郵件開道或網際網路開道上使用本「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_business 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的物件，例如檔案URLIP 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、移轉或以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」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」，取代之之前與本「軟體」相關的任何聲明、討論、保證、通訊或廣告。

隱私權原則

ESET, spol. s r. o. 設址於 Einsteinova 24, 851 01 Bratislava, Slovak Republic 註冊於由 Bratislava I District Court (Section Sro, Entry No 3586/B) 管轄的 Commercial Register 公司登記號碼: 31333532, 為資料控制者 (以下稱「ESET」或「我們」), 處理客戶之個人資料及隱私力求透明。為達此目標, 「我們」茲發佈此隱私權政策, 唯一目的是就下列主題知會客戶 (以下稱「使用者」或「貴用戶」):

- 處理個人資料、
- 資料保密性、
- 資料當事人權利。

處理個人資料

ESET 提供並在我們的產品中實作的服務, 係根據軟體使用者授權合約 (以下稱「EULA」) 之條款提供, 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。針對提供服務時收集的資料, 「我們」茲對「貴用戶」提供更多詳細資訊。「我們」依據 EULA 和產品文件所述提供多項服務, 例如, 更新/升級服務「ESET LiveGrid」防止資料濫用、支援等。為使一切順利進行, 我們需要收集以下資訊:

- 更新與其他統計資料, 涵蓋安裝程序與您電腦的資訊, 包括您的產品所安裝的平台, 我方產品之操作與功能的資訊, 例如作業系統、硬體資訊、安裝 ID 授權 ID IP 位址 MAC 位址、產品組態設定。
- 與入侵相關的單向雜湊屬於 ESET LiveGrid® 聲譽系統的一部分, 可將掃描的檔案與雲端中的白名單和黑名单項目比較, 以改善惡意軟體防護解決方案的效益。
- 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
 - o 可疑病毒範例及其他惡意程式和可疑、有問題、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;
 - o 區域網路中裝置的資訊, 例如類型、供應商、型號和/或裝置名稱;
 - o 使用網路的資訊, 例如 IP 位址和地理資訊 IP 封包 URL 乙太網路框架;
 - o 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。

- 需要授權資訊 (例如, 授權 ID 及名字、姓氏、地址、電子郵件地址等個人資料) 以供計費、驗證授權真實性及提供服務。
- 您可能需要將聯絡資訊及資料納入支援請求, 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。我們可能會要求您提供給我們其他資訊, 以協助支援服務的進行。

資料機密性

ESET 公司透過交付、服務和支援網路中的附屬實體或合作夥伴, 在全球營運。為提供服務、支援或計費等

履行 EULA 之行為。ESET 處理的資訊必須移轉至關係企業實體或合作夥伴，或自後者移轉至 ESET。根據「貴用戶」選擇使用的服務及您的位置，「我們」可能需要將您的資料移轉至不具備歐盟執行委員會之適足性認定的國家。即使在此情況，每項資訊移轉皆受資料防護法規規範，且僅在必要時進行。必須建立標準個資保護契約條款 (Standard Contractual Clauses) 企業約束規則 (Binding Corporate Rules) 或其他適用的保護措施，絕無任何例外。

根據和 EULA 提供服務時，「我們」竭盡所能防止資料儲存的時間較必要時間更長。我們的保存期限會比您授權的有效期限長，讓您能夠有時間輕鬆自在地續約。可進一步處理來自 ESET LiveGrid® 的最小化及假名化統計資料及其他資料，以供統計用途。

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。我們正盡全力確保處理系統和服務時能持續保有機密性、完整性、可用性和靈活性。然而，若資料外洩導致您的權利和自由產生風險，「我們」會通知監管當局以及資料主體。身為資料當事人，您有權利向監管機構提出申訴。

資料當事人權利。

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。根據適用資料保護法律所規範的相關條款，身為資料主體，以下為您應有的權利：

- 請求存取您在 ESET 的個人資料的權利，
- 修改不正確的個人資料的權利（「貴用戶」也有將未填妥的個人資料填妥的權利），
- 請求刪除個人資料的權利，
- 請求對您的個人資料處理施加限制的權利，
- 拒絕處理的權利
- 提出投訴的權利以及
- 資料可攜性的權利。

我們相信，對於為客戶提供服務及產品的合法權益，我們處理的所有資訊對於皆為重要且必要的。

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