ESET File Security

使用者手冊

按一下此處顯示此文件的連線版本

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

如需詳細資訊，請造訪 https://www.eset.com

技術支援https://support.eset.com

修訂。2023年m月19日

前言

本指南目的是協助您充分利用 ESET File Security若要深入瞭解程式中的任何視窗，請將該視窗開啟並按下鍵盤上的 **F1** 鍵。與您目前檢視視窗相關的說明頁面即會顯示。

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 File Security 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
> 「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。

> 重要
> 這需要您的注意，且不建議略過它。重要告示會提供非重大但卻重要的資訊。

> 警告
> 重大資訊，您需要多加注意。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。

> 範例
> 此為協助您瞭解如何使用特定功能的使用方案或實際範例。

如果您在說明頁面的右上角看見下列元素，它代表 ESET File Security 圖形使用者介面 (GUI) 的視窗內導覽。使用這些指示前往個別說明頁面中描述的視窗。

開啟 ESET File Security
按一下［設定］>［伺服器*] > [OneDrive* 掃描設定］>［註冊］ 

格式設定慣例：

慣例	代表意義
粗體	區段標題、功能名稱或使用者介面項目，如按鈕。
斜體	是您提供資訊的版面配置區。例如，檔案名稱或路徑代表您輸入實際路徑或檔案名稱。
`Courier New`	代碼範例或指令。
超連結	提供迅速輕鬆地存取交互參照主題或外部網路位置。超連結會以藍色字顯示，且會加底線。
%ProgramFiles%	儲存 Windows 或其他安裝程式的 Windows 系統目錄。

ESET File Security 的線上說明頁面分為數個章節和子章節。您可以瀏覽說明頁面的內容找到相關資訊。或者，您也可以輸入單字或片語使用全文搜尋。

概觀

ESET File Security 是一套整合性的解決方案，專為 Microsoft Windows Server 環境而設計。ESET File Security 對於各種類型的惡意軟體攻擊提供有效且強大的防護，提供兩種類型的防護：惡意軟體防護和間諜程式防護。

主要功能

下表提供適用於 ESET File Security中可用功能的清單。ESET File Security 支援大部分的 Microsoft Windows Server 2008 R2 SP1、2012、2016 以及 2019 獨立版本和叢集環境版本。在大型網路中，您可以使用 ESET Security Management Center 遠端管理 ESET File Security。

真正的 64 位元產品核心	為產品核心元件提升效能及穩定性。
惡意軟體防護	獲獎 和創新的惡意軟體防護。這項先端技術，並使用具有雲端功能的掃描，達到更佳的偵測率，消滅各種類型的威脅，包括病毒、勒索軟體、Rootkit、蠕蟲及間諜程式。佔用較小的空間，減輕系統資源負擔而不會影響其性能。其使用分層安全模型。每個層（即階段）都有許多核心技術。執行前階段具有 *UEFI* 掃描器、網路攻擊防護、信譽與快取、產品內的沙箱、*DNA* 偵測等技術。執行階段技術為惡意探索封鎖程式、勒索軟體保護、進階記憶體掃描器和指令碼掃描程式 *(AMSI)*。而執行後階段使用殭屍網路防護、雲端惡意軟體防護系統和沙箱。此功能豐富的核心技術組合可提供無與倫比的防護。
OneDrive 掃描	這是一項新增功能，可用於掃描放置在 OneDrive 雲端儲存空間中的檔案。適用於 Office 365 企業帳戶。
Hyper-V 掃描	是一項新科技，可讓您掃描 Microsoft Hyper-V Server 上的虛擬機器 (VM) 磁碟，無須在特定 VM 上安裝任何「代理程式」。
ESET Dynamic Threat Defense (EDTD)	ESET 雲端式服務。ESET File Security 偵測到可疑程式碼或行為時，會暫時將之放入 ESET Dynamic Threat Defense 隔離區以防止進一步的威脅活動。系統會自動將可疑的樣本提交至 ESET Dynamic Threat Defense 伺服器，以讓最先進的惡意軟體偵測引擎進行分析。您的 ESET File Security 稍後會收到分析結果。系統會根據結果處理可疑檔案。
ESET 叢集	ESET 叢集允許從單一位置管理多個伺服器，與 ESET File Security 6 for Microsoft Windows Server 類似，由於可在所有叢集成員之間散佈單一配置原則，因此將工作站加入至節點會提供額外的自動化管理。叢集建立本身可使用安裝的節點，可讓其遠端安裝並啟動所有節點。ESET 伺服器產品可以彼此通訊，並交換資料，例如配置和通知，也可以將產品執行個體群組進行適當作業所必需的資料同步化。它可以為整個叢集的產品提供相同配置。ESET File Security 可支援 Windows 容錯移轉叢集」和「網路負載平衡 (NLB) 叢集」。此外，您不需要特定的 Windows 叢集就可以手動新增 ESET 叢集成員。ESET 叢集可在網域與工作群組環境中運作。
自動排除	自動偵測並排除重要的應用程式和伺服器檔案，使伺服器的運作更加順暢並提升效能。
程序排除	從惡意軟體防護存取時掃描中排除特定程序。惡意軟體防護存取時掃描在特定情況下可能會造成衝突，例如備份程序或虛擬機器即時移轉。「程序排除」有助於將這類潛在衝突的風險降至最低，並提升排除應用程式的效能，因此對整個系統的整體效能與穩定性具有正面效果。程序/應用程式的排除是其可執行檔 (*.exe*) 的排除。
eShell ESET Shell	eShell 現在可使用 是一種命令列介面，為進階的使用者和管理員提供更完整的選項來管理 ESET 伺服器產品。
ESET Security Management Center	與 ESET Security Management Center (包含排程「指定掃描」的功能）的整合度更佳。如需詳細資訊，請參閱 ESET Security Management Center 線上說明
元件式安裝	可以自訂安裝，僅包含選取的產品部分。

新增功能

ESET File Security 引進以下的新功能：

- 真正的 64 位元產品核心
- OneDrive 掃描
- ESET Dynamic Threat Defense (EDTD)
- ESET Enterprise Inspector 支援
- ESET RMM
- 機器學習偵測

防護類型

有兩種類型的防護：

- 反惡意軟體防護
- 間諜程式防護

惡意軟體及間諜程式防護是 ESET File Security 產品的其中一項基本功能。該防護可藉由控制檔案、電子郵件及網際網路通訊來防止惡意系統攻擊。如果發現威脅，偵測模組可透過封鎖，接著清除、刪除或將其移至隔離區來消滅它。

準備安裝

在準備安裝產品時，我們建議您採取幾個步驟：

- 購買 ESET File Security 之後，從 ESET 網站 下載 `.msi` 安裝套件。

- 確定您打算安裝 ESET File Security 的伺服器符合系統需求
- 使用 Administrator 帳戶登入伺服器。

注意
請注意，您必須使用「內建管理員」帳戶或網域管理員帳戶執行安裝程式（已停用本機「內建管理員」帳戶情況下）。任何其他使用者，即使是管理員群組的成員，也沒有足夠的存取權限。因此，您需要使用「內建管理員」帳戶，否則您無法在任何其他本機或網域管理員以外的使用者帳戶下成功完成安裝。

- 如果您要從 ESET File Security 的現有安裝升級，建議您使用匯出設定功能備份其目前配置。
- 若適用，從您的系統移除/解除安裝任何第三方病毒防護軟體。我們建議您使用 ESET AV Remover。如需可使用 ESET AV Remover 移除的第三方防毒軟體清單，請參閱此知識庫文章
- 如果您在 Windows Server 2016 上 ESET File Security 安裝Microsoft 建議您解除安裝 Windows Defender 功能並撤銷 Windows Defender ATP 註冊，以防止因為在機器上安裝多個防毒產品而產生的問題。

您可以在兩個安裝模式中執行 ESET File Security 安裝程式：

- 圖形使用者介面 (GUI)
這是建議的安裝類型，會以安裝精靈的形式呈現。
- 無訊息 / 自動安裝
除了安裝精靈以外，您還可以選擇透過指令行，以無訊息方式安裝 ESET File Security

重要
如果可能，強烈建議您將 ESET File Security 安裝在全新安裝及配置的作業系統上。如果您需要在現有的系統上安裝，我們建議您移除安裝之前的 ESET File Security 版本，重新啟動伺服器然後安裝新的 ESET File Security

- 升級為較新版本
如果您使用的是舊版 ESET File Security則可選擇適當的升級方式。

當您成功安裝或升級 ESET File Security 之後，進一步的活動是：

- 產品啟動
啟動視窗中可使用的特定啟動狀況會視國家及發行方法而異。
- 配置一般設定
您可以修改 ESET File Security 之每個功能的進階設定來進行微調，以符合您的需求。

系統需求

支援的作業系統：

- Microsoft Windows Server 2019 (Server Core 和桌面體驗)
- Microsoft Windows Server 2016 (Server Core 和桌面體驗)
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1 (已安裝 KB4474419 及 KB4490628)
- Server Core (Microsoft Windows Server 2008 R2 SP1, 2012, 2012 R2)

注意
如果您執行的是 Microsoft Windows Server 2008 R2 SP1，請參閱 SHA-2 必要相容性並確保您的作業系統已套用所有必要的修補程式。

儲存裝置、Small Business 及 MultiPoint 伺服器：

- Microsoft Windows Storage Server 2016
- Microsoft Windows Storage Server 2012 R2
- Microsoft Windows Storage Server 2012

- Microsoft Windows Server 2019 Essentials
- Microsoft Windows Server 2016 Essentials
- Microsoft Windows Server 2012 R2 Essentials
- Microsoft Windows Server 2012 Essentials
- Microsoft Windows Server 2012 Foundation
- Microsoft Windows Small Business Server 2011 SP1 (x64) (已安裝 KB4474419 及 KB4490628)

- Microsoft Windows MultiPoint Server 2012
- Microsoft Windows MultiPoint Server 2011
- Microsoft Windows MultiPoint Server 2010

支援的 Hyper-V 角色主機作業系統：

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1 – 虛擬機器只有在離線時才能進行掃描

硬體需求須視所用的作業系統版本而定。建議您閱讀 Microsoft Windows Server 產品文件，以瞭解硬體需求的詳細資訊。

注意
我們強烈建議您安裝 Microsoft 伺服器作業系統及伺服器應用程式最新的 Service Pack，然後再安裝 ESET 安全性產品。我們也建議您盡可能安裝最新的 Windows 更新與修正程式。

最低硬體需求：

元件	需求
處理器	Intel 或 AMD 單核心 x86 或 x64
記憶體	256 MB 的可用記憶體
硬碟	700 MB 的可用磁碟空間
螢幕解析度	800 x 600 像素或更高

SHA-2 必要相容性

Microsoft 於 2019 年初宣佈淘汰安全雜湊演算法 1 (SHA-1)並開始轉移到 SHA-2因此，所有使用 SHA-1 演算法簽名的憑證將不再受認可，並將導致安全警報。遺憾的是，隨著時間改變，有鑑於演算法中發現的弱點、處理器效能提升及雲端運算的進展SHA-1 雜湊演算法的安全性已經降低。

SHA-2 雜湊演算法（作為 SHA-1 的後繼產品）現在是保證 SSL 安全持續性的首選方法。請參閱關於雜湊及簽署演算法 的 Microsoft Docs 文件，以取得進一步的詳細資料。

> 注意
> 這項變更代表在沒有 SHA-2 支援的作業系統上，您的 ESET 安全性解決方案將無法更新其模組（包含偵測引擎），這最終會導致您的 ESET File Security 無法發揮完整功能，而且無法提供足夠的防護。

如果您執行的是 **Microsoft Windows Server 2008 R2 SP1** 或 **Microsoft Windows Small Business Server 2011 SP1**，請確保您的系統與 SHA-2 相容。根據您的特定作業系統版本套用修補程式，如下所示：

- **Microsoft Windows Server 2008 R2 SP1** – 套用 KB4474419 及 KB4490628（可能需要另外重新啟動系統）
- **Microsoft Windows Small Business Server 2011 SP1** (x64) — 套用 KB4474419 及 KB4490628（可能需要另外重新啟動系統）

> 重要
> 安裝更新並重新啟動系統之後，請開啟 ESET File Security GUI 以檢查其狀態。如果狀態顯示為橘色，請另外重新啟動系統。狀態應顯示為綠色，以表示最大防護。

> 注意
> 我們強烈建議您安裝 Microsoft 伺服器作業系統及伺服器應用程式最新的 Service Pack我們也建議您盡可能安裝最新的 Windows Update 與修正程式。

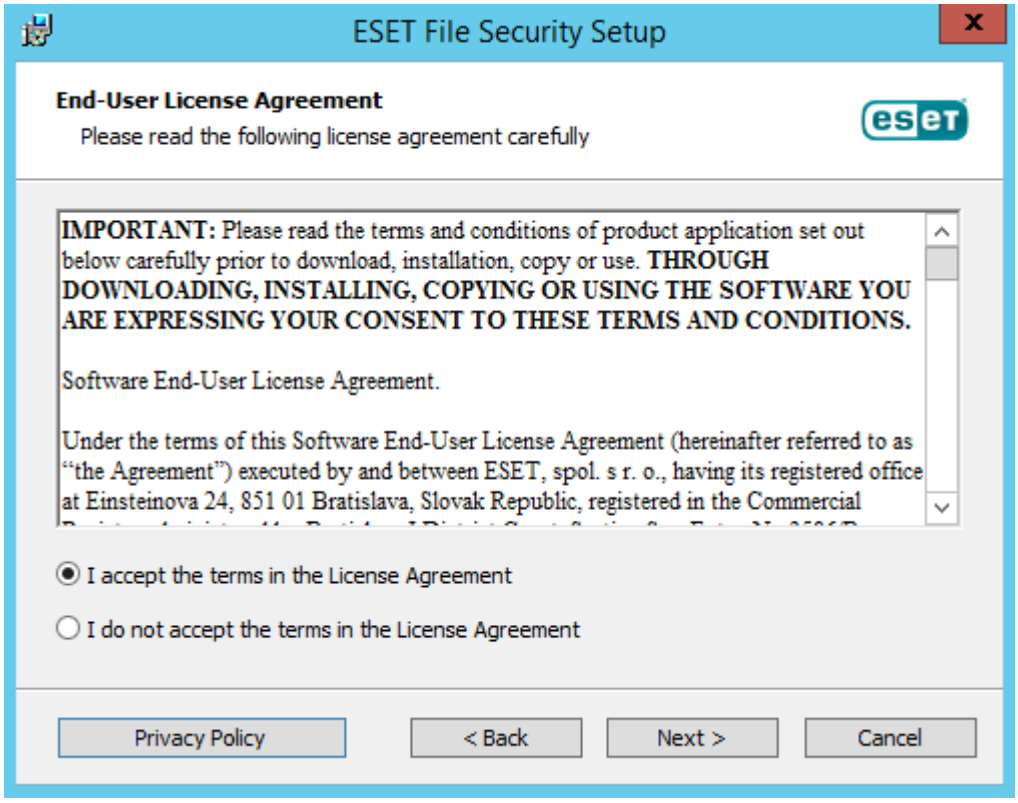
ESET File Security 安裝步驟

這是典型 GUI 安裝精靈。連按兩下 `.msi` 套件並依照步驟以安裝 ESET File Security

1.按一下 **[下一步]** 繼續，如果您要結束安裝，則按 **[取消]**

2.安裝精靈會以指定為您作業系統之 **[地區]** > **[位置]** 的 **[當前位置]**（或舊版系統中 **[地區及語言]** > **[位置]** 的 **[目前位置]** 設定）的語言執行。使用下拉式功能表以選取要安裝 ESET File Security 的 **[產品語言]**。針對 ESET File Security 選取的語言與您在安裝精靈中看到的語言無關。

3.按一下［**下一步**］即會顯示「使用者授權合約」。確認您接受［**使用者授權合約**］(EULA) 及隱私權政策之後，按一下［**下一步**］

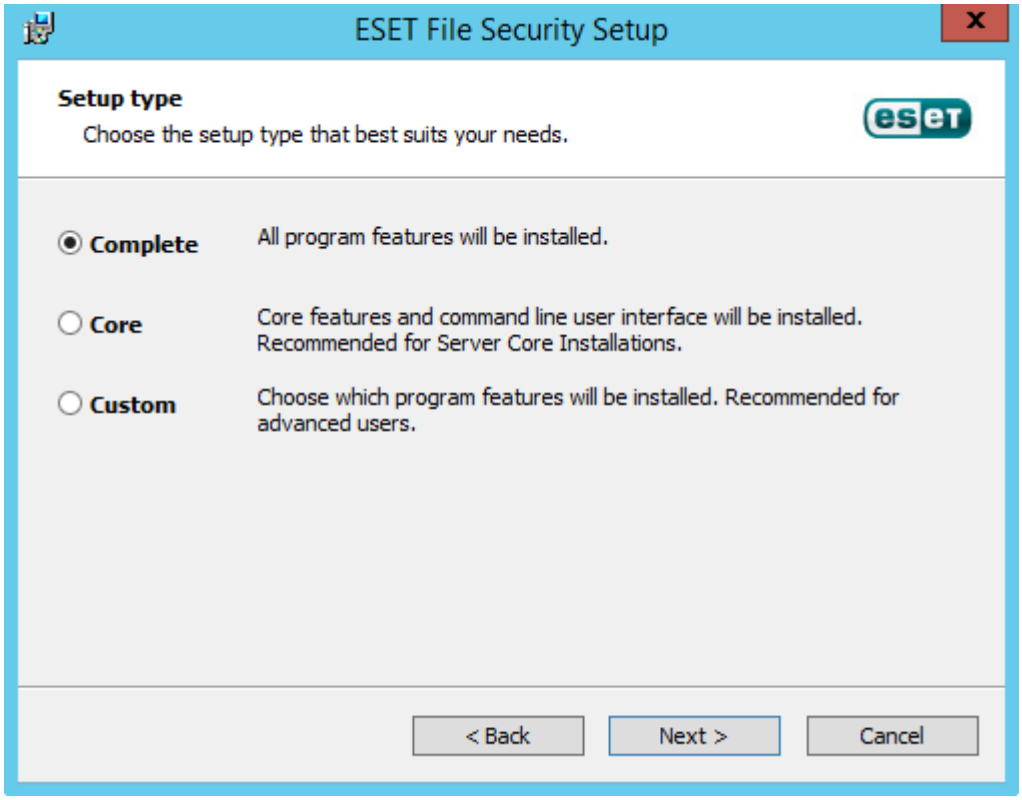


4.選取其中一個可用的安裝類型（通常視您的作業系統而定）：

完整

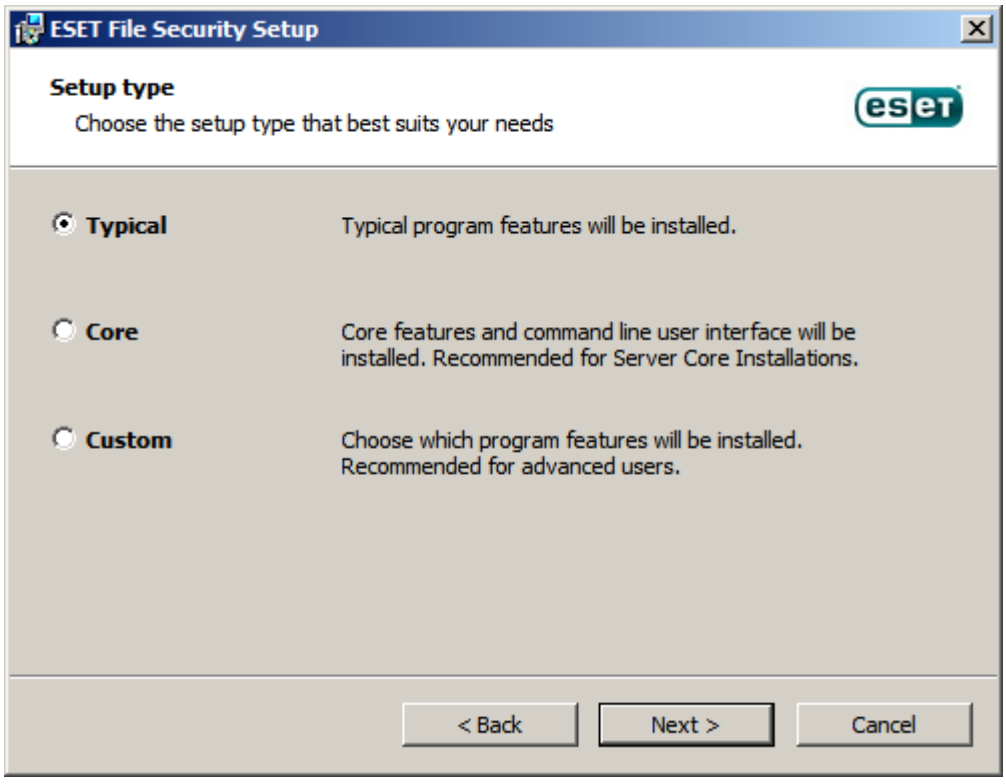
安裝所有 ESET File Security 功能。也稱為完整安裝。這是建議的安裝類型，適用於 **Windows Server 2012□2012 R2□2016□2019□Windows Server 2012 Essentials□2012 R2 Essentials□2016 Essentials 與 2019**

Essentials



[典型]

安裝推薦的 ESET File Security 功能。適用於 2008 R2 SP1 和 2011。



核心

此安裝類型適用於 Windows Server Core 版本。安裝步驟與完整安裝相同，但僅會選擇安裝核心功能和指令列使用者介面。雖然核心安裝主要使用在 Windows Server Core您仍可以安裝在標準 Windows

Server 上。使用核心安裝方法安裝的 ESET 安全性產品不會有任何 GUI這代表使用 ESET File Security 時，您僅能使用命令列使用者介面。如需更多詳細資訊以及有關其他特殊參數的資訊，請參閱「指令列安裝」區段。

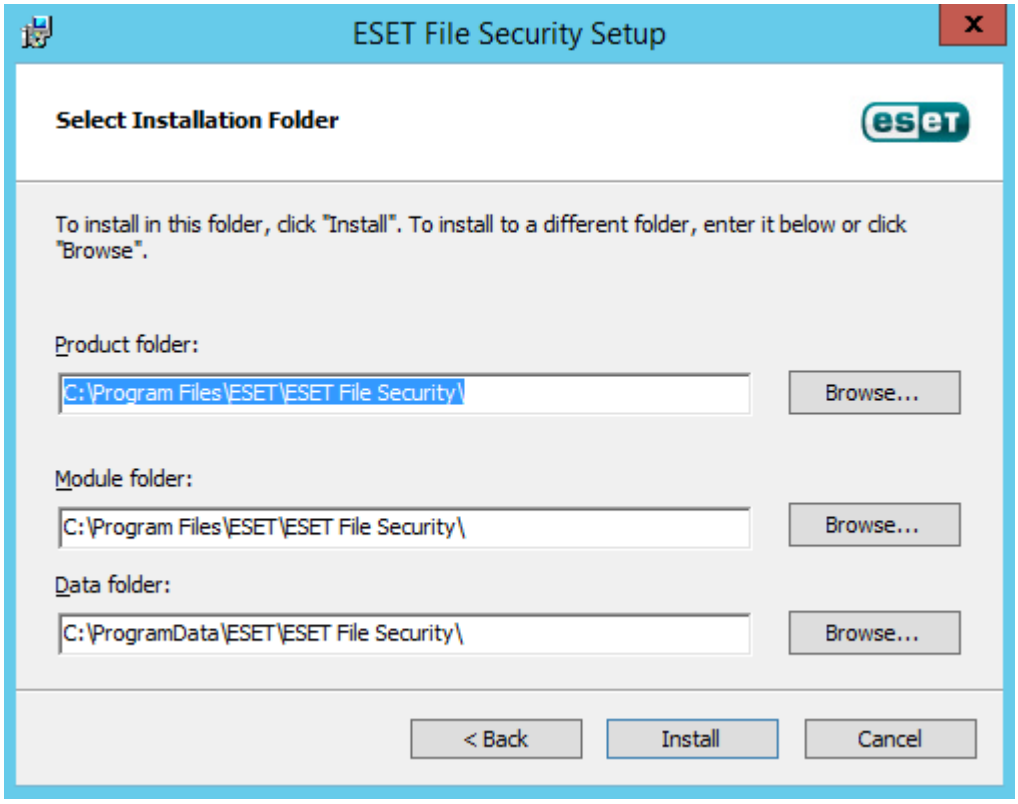
範例
如要透過指令列執行核心安裝，請使用以下範例指令：
```
msiexec /qn /i efsw_nt64.msi ADDLOCAL=_Base
```

自訂

自訂安裝可讓您選取安裝在系統上的 ESET File Security 功能。開始安裝時，產品模組和功能清單將會顯示。此模式在您僅要自訂 ESET File Security 中需要的元件時相當實用。

注意
在 Windows Server 2008 R2 SP1 上，預設會停用 **[網路防護]** 元件的安裝（**[典型]** 安裝）。如果您希望安裝此元件，請選擇 **[自訂]** 安裝類型。

5.系統將提示您選取要安裝 ESET File Security 的位置。依預設，程式會安裝在 C:*Program Files**ESET**ESET File Security*。按一下 **[瀏覽]** 變更此位置（不建議）。



6.按一下 **[安裝]** 以開始安裝。安裝完成時ESET GUI 會開始且匣圖示 會顯示在通知區域（系統匣）中。

修改現有的安裝

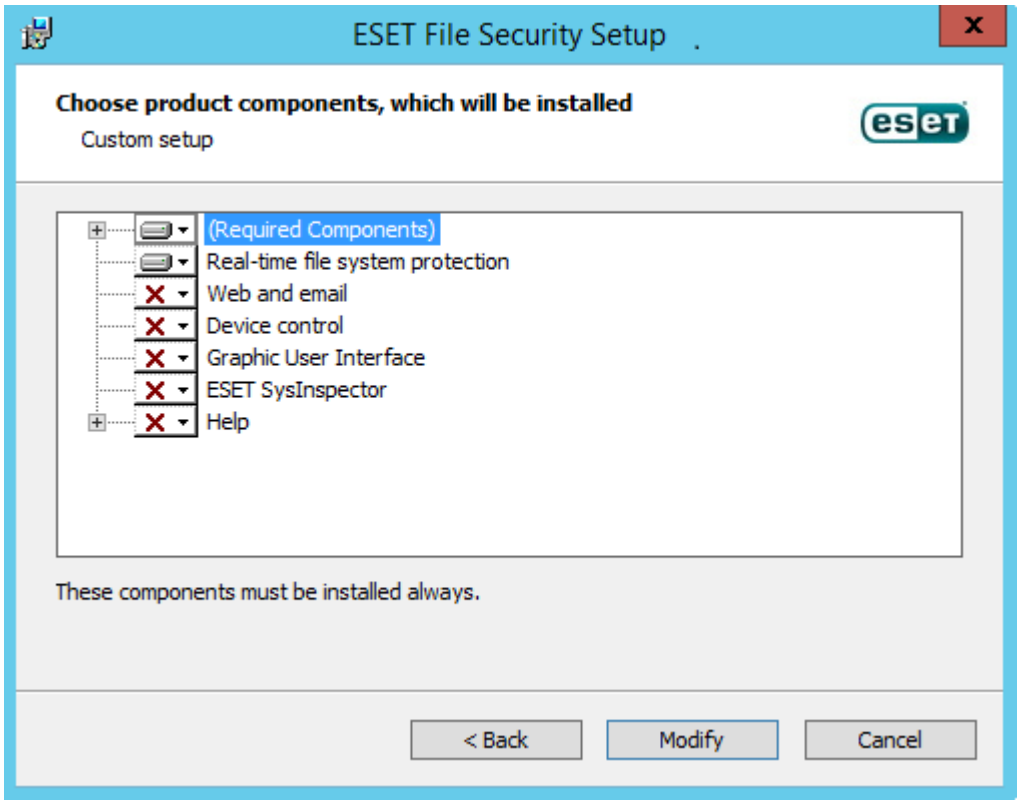
您可以在您的安裝中新增或移除元件。若要這樣做，您可以執行在初始安裝期間使用的 `.msi` 安裝程式套件，或移至 **[程式和功能]**（可從 Windows [控制台] 存取）。用滑鼠右鍵按一下 ESET File Security然後選取 **[變更]**。遵循以下步驟新增或移除元件。

在 3 種選項當中，您可以 **[修改]** 已安裝的元件、**[修復]** 您安裝的 ESET File Security 或完全地 **[移除]**

(解除安裝)。

如果您選擇［**修改**］，系統會顯示可用程式元件的清單。

選擇您想要新增或移除的元件。您可以同時新增/移除多個元件。按一下元件然後從下拉式功能表選取需要的選項：



在選取選項之後，按一下［**修改**］以執行修改。

注意
您可以透過執行安裝程式隨時修改已安裝的元件。對於大多數元件，執行變更無須重新啟動伺服器GUI 將重新啟動，而您只會看到您選擇安裝的元件。對於需要重新啟動伺服器的元件Windows Installer 會提示您重新啟動。伺服器恢復上線後，您就可以使用新元件。

無訊息 / 自動安裝

執行以下命令以透過命令列完成安裝： `msiexec /i <packagename> /qn /l*xv msi.log`

注意
在 Windows Server 2008 R2 SP1 上，將不會安裝 **[網路防護]** 功能。

若要確定順利安裝或是安裝發生任何問題，請使用 Windows 事件檢視器以檢查 **[應用程式記錄]**（從此來源查詢記錄MsiInstaller)

範例
64 位元系統上的**完整安裝**
```
msiexec /i efsw_nt64.msi /qn /l*xv msi.log ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,SysInspector,SysRescue,Rmm,eula
```

安裝完成時ESET GUI 會開始且匣圖示 會顯示在通知區域（系統匣）中。

範例
以**特定語言**安裝產品（德文）：
```
msiexec /i efsw_nt64.msi /qn ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,^
SysInspector,SysRescue,Rmm,eula PRODUCT_LANG=1031 PRODUCT_LANG_CODE=de-de
```
請參閱「命令列安裝」中的 **[語言參數]** 以取得進一步詳細資訊以及語言代碼清單。

重要
指定 `REINSTALL` 參數的值時，您必須列出尚未用於 `ADDLOCAL` 或 `REMOVE` 參數值的其餘功能。若要讓指令行安裝正確執行，則需要將所有功能列為 `REINSTALL`ADDLOCAL 和`REMOVE` 參數的值。如果您不使用 `REINSTALL` 參數，則可能無法成功新增或移除。
請參閱命令列安裝區段以取得完整的功能清單。

範例
完成從 64 位元系統移除（解除安裝）：
```
msiexec /x efsw_nt64.msi /qn /l*xv msi.log
```

注意
成功解除安裝之後，您的伺服器便會自動重新開機。

命令列安裝

以下列設定僅適用於使用者介面的**減少**基本與**無**層級。請參閱文件中有關用於適當命令列切換參數的 **msiexec** 版本說明。

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
- 例如： `efsw_nt64.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

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。
- 與 ESET `.msi` 套件搭配使用：`efsw_nt64.msi /qn ADDLOCAL=<list>`
- 如需有關 `ADDLOCAL` 屬性的詳細資訊，請參閱 https://docs.microsoft.com/en-gb/windows/desktop/Msi/addlocal
- `ADDLOCAL` 清單是以逗號分隔的清單，包含所有將要安裝的功能。
- 選取要安裝的功能時，清單必須明確包含完整路徑（所有上層功能）。

REMOVE=<list>

- 元件安裝 – 您不希望在本機安裝的上層功能。
- 與 ESET `.msi` 套件搭配使用：`efsw_nt64.msi /qn REMOVE=<list>`
- 如需有關 `REMOVE` 屬性的詳細資訊，請參閱 https://docs.microsoft.com/en-gb/windows/desktop/Msi/addlocal
- `REMOVE` 清單是將不會安裝之上層功能的逗號區隔清單（或者，若是現有安裝則會予以移除）。
- 只需要指定上層功能即已足夠。不需要明確包含該清單的所有下層功能。

ADDEXCLUDE=<list>

- `ADDEXCLUDE` 清單是不要安裝之所有功能名稱的逗號區隔清單。
- 選取不要安裝的功能時，整個路徑（例如，其所有子功能）且相關不可見的功能必須明確包含在清單中。
- 與 ESET `.msi` 套件搭配使用：`efsw_nt64.msi /qn ADDEXCLUDE=<list>`

> 注意
> `ADDEXCLUDE` 無法與 `ADDLOCAL` 一起使用。

功能的存在

- **強制** – 一律會安裝此功能。
- **選用** – 可取消選取安裝的功能。
- **不可見** – 其他功能適當運作的強制性邏輯功能。

ESET File Security 功能清單：

> 重要
> 所有功能名稱都會區分大小寫，例如 `RealtimeProtection` 不等於 `REALTIMEPROTECTION`

功能名稱	功能的存在
SERVER	強制
RealtimeProtection	必要
WMIProvider	強制
HIPS	強制
Updater	強制
eShell	強制
UpdateMirror	強制
DeviceControl	選用
DocumentProtection	選用
WebAndEmail	選用
ProtocolFiltering	隱藏
NetworkProtection	選用
IdsAndBotnetProtection	選用
Rmm	選用
WebAccessProtection	選用
EmailClientProtection	選用
MailPlugins	隱藏
Cluster	選用
_Base	必要
eula	必要
ShellExt	選用
_FeaturesCore	必要
GraphicUserInterface	選用
SysInspector	選用
SysRescue	選用
EnterpriseInspector	選用

如果您希望移除下列任一個功能，則必須指定屬於該群組的所有功能，以移除整個群組。否則系統將不會移除功能。此處有兩個群組（每條線代表一個群組）：

```
GraphicUserInterface,ShellExt

NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,ProtocolFiltering,MailPlugins,EmailClientProtection
```

> 範例
> 使用 REMOVE 參數並僅指定上層功能，以便從安裝排除 **[網路防護]** 區段（包含下層功能）：
> `msiexec /i efsw_nt64.msi /qn ADDLOCAL=ALL REMOVE=NetworkProtection`
> 或者，您可以使用 ADDEXCLUDE 參數，但您也必須指定所有下層功能：
> `msiexec /i efsw_nt64.msi /qn ADDEXCLUDE=NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,^ProtocolFiltering,MailPlugins,EmailClientProtection`

> 範例
> **核心**安裝範例：
> `msiexec /qn /i efsw_nt64.msi /l*xv msi.log ADDLOCAL=RealtimeProtection,Rmm`

如果您希望在安裝之後自動設定 ESET File Security則可在安裝指令內只定基本設定參數。

範例
安裝 ESET File Security 並停用 ESET LiveGrid®
```
msiexec /qn /i efsw_nt64.msi ADDLOCAL=RealtimeProtection,Rmm,GraphicUserInterface CFG_LIVEGRID_ENABLED=0
```

所有設定內容清單：

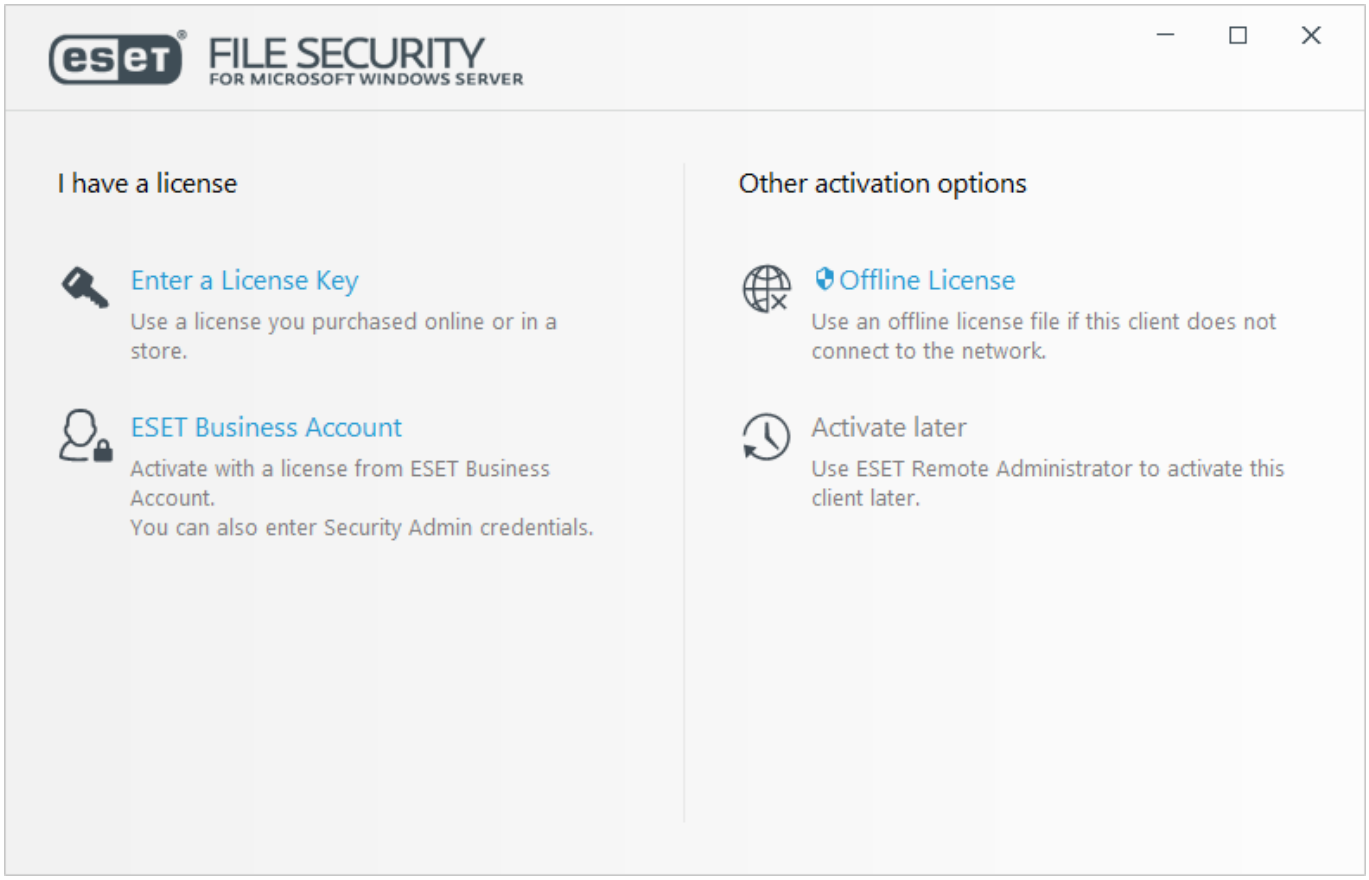
開關	值
CFG_POTENTIALLYUNWANTED_ENABLED=1/0	0 – 停用，1 – 啟用
CFG_LIVEGRID_ENABLED=1/0	0 – 停用，1 – 啟用
FIRSTSCAN_ENABLE=1/0	0 – 停用，1 – 啟用
CFG_PROXY_ENABLED=0/1	0 – 停用，1 – 啟用
CFG_PROXY_ADDRESS=<ip>	Proxy IP 位址
CFG_PROXY_PORT=<port>	Proxy 連接埠號碼
CFG_PROXY_USERNAME=<user>	驗證的使用者名稱
CFG_PROXY_PASSWORD=<pass>	驗證密碼

語言參數： 產品語言（您必須指定兩個參數）

開關	值
PRODUCT_LANG=	LCID 十進位數值（地區設定 ID)例如 1033 代表 *English - United States*，請參閱「語言代碼清單」
PRODUCT_LANG_CODE=	LCID 字串（地區文化名稱），例如 en-us 代表 *English - United States*，請參閱「語言代碼清單」

產品啟動

安裝完成時，系統將提示您啟動您的產品。



您也可以使用下列任何一種方法來啟動 ESET File Security。

輸入授權金鑰

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 Business Account

如果您已註冊且具有已匯入 ESET File Security 授權之 ESET 商業帳戶 (EBA)，請使用此選項。您也可以輸入您在 ESET License Administrator 入口網站上使用的 **[安全管理員]** 憑證。

離線授權檔案

自動產生的檔案，其將傳輸到 ESET 產品以提供授權資訊。您的離線授權檔案是從授權入口網站產生，且將用於應用程式無法連接到授權單位的環境。

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 Security Management Center 執行遠端啟動，請以 ESET Security Management Center 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。

您可以在主要程式視窗中選取 **[說明及支援]** > **[管理授權]**，以便隨時管理您的授權資訊。您將可看見用來依 ESET 識別產品公用授權 ID 以及授權識別。電腦用來註冊的使用者名稱儲存在 [關於] 區段，以滑鼠右鍵按一下系統匣圖示 就能檢視。

在成功啟動 ESET File Security 之後，主程式視窗將會開啟，並於監控頁面中顯示您目前的狀態。一開始可能必須多加留意，例如，系統可能會詢問您是否要成為 ESET LiveGrid® 的成員。

主程式視窗也會顯示與其他項目有關的通知，例如系統更新 (Windows Update) 或偵測引擎更新。當需要注意的所有項目都已解決之後，監控狀態將會變成綠色並顯示 **「您已受到保護」** 狀態。

您也可以在［說明及支援］>［啟動產品］下的主要功能表或在［防護］狀態 >［產品未啟動］中啟動您的產品。

> 注意
> ESET Security Management Center 可透過管理員提供的授權，無訊息地啟動用戶端電腦。

ESET Business Account

您可以使用 ESET Business Account 來管理多個授權。若您未擁有 ESET Business Account，請按一下［建立帳戶］，接著系統會將您重新導向到 ESET Business Account 入口網站，供您在其中註冊憑證。

> 注意
> 如需詳細資訊，請參閱 ESET Business Account (EBA) 使用者指南。

若您使用安全管理員憑證且忘記自己的密碼，請按一下［我忘記密碼］，接著系統會將您重新導向到 ESET License Administrator 入口網站。請輸入您的電子郵件地址，並按一下［提交］以確認。完成之後，您將收到一封包含重設密碼指示的郵件。

啟動成功

啟動成功，ESET File Security 現在已啟動。從現在開始，ESET File Security 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。

啟動失敗

Activation of ESET File Security 啟動失敗。請確定您已經輸入正確的［授權金鑰］或已附加［離線授權］。若您有不同的［離線授權］，請再次輸入。若要檢查您輸入的授權金鑰，請按一下［重新檢查授權金鑰］或［輸入不同的授權］。

授權

您將收到提示，要求您選取與要用於 ESET File Security 的帳戶相關授權。按一下［繼續］已繼續啟動。

升級為較新版本

新推出 ESET File Security 版本將改善或修正自動程式模組更新無法解決的問題。

升級方法：

- ［解除安裝 / 安裝］ – 請先移除舊版本，然後再安裝新版本。下載最新版的 ESET File Security。如果您想保存配置，請從您現有的 ESET File Security 匯出設定。解除安裝 ESET File Security 並重新啟動伺服器。使用您已下載的安裝程式執行初次安裝。匯入設定以載入您的配置。如果您有正在執行 ESET File Security 的單一伺服器，我們建議您執行此程序。
- ［保留原位］ – 不移除現有版本，並在該版本上安裝新 ESET File Security 的升級方法。

重要
因為 Windows Update 或其他原因，在您的伺服器上必須**沒有擱置的 Windows Update**，以及**沒有擱置的重新啟動**。如果您嘗試使用擱置中的 Windows Update 或重新啟動來執行保留原位升級，可能無法正確移除現有版本的 ESET File Security。如果您之後決定手動刪除 ESET File Security 的舊版本，也會遇到問題。

注意
ESET File Security 升級期間系統將需要重新啟動伺服器。

- 遠端 – 在大型網路環境中使用，由 ESET Security Management Center 管理。這基本上是一種清除升級方法，不過是遠端執行。如果您擁有多台執行 ESET File Security 的伺服器，則此方法相當實用。

- ESET 叢集精靈 – 也可用作一種升級方法。我們建議這種方法適用於具有 ESET File Security 的 2 部以上伺服器。這基本上是一種就地升級方法，不過是透過 ESET 叢集進行。一旦升級完成時，您可以持續使用 ESET 叢集並利用其功能。

注意
將 ESET File Security 升級後，建議您完成所有設定，以確定配置正確並符合您的需求。

透過 ESMC 升級

ESET Security Management Center 可讓您升級執行舊版本 ESET File Security 的多部伺服器。此方法的優勢在於升級大量伺服器的同時，也能確保每個 ESET File Security 的配置完全相同（若有需求）。

此流程包含下列階段：

- 手動**升級第一部伺服器**，即安裝最新版本的 ESET File Security 來覆蓋現有版本，以便保留包含規則、多個白名單和黑名單在內的所有配置。此階段會於正在執行 ESET File Security 的伺服器本機上執行。

- 此為新升級至版本 7.x 的 ESET File Security **要求配置**，以及在 ESET Security Management Center 中**轉換為原則**。該原則將稍後套用至所有升級的伺服器。此階段以及下列階段會使用 ESMC 來遠端執行。

- 在執行舊版本 ESET File Security 的所有伺服器上**執行軟體解除安裝**工作。

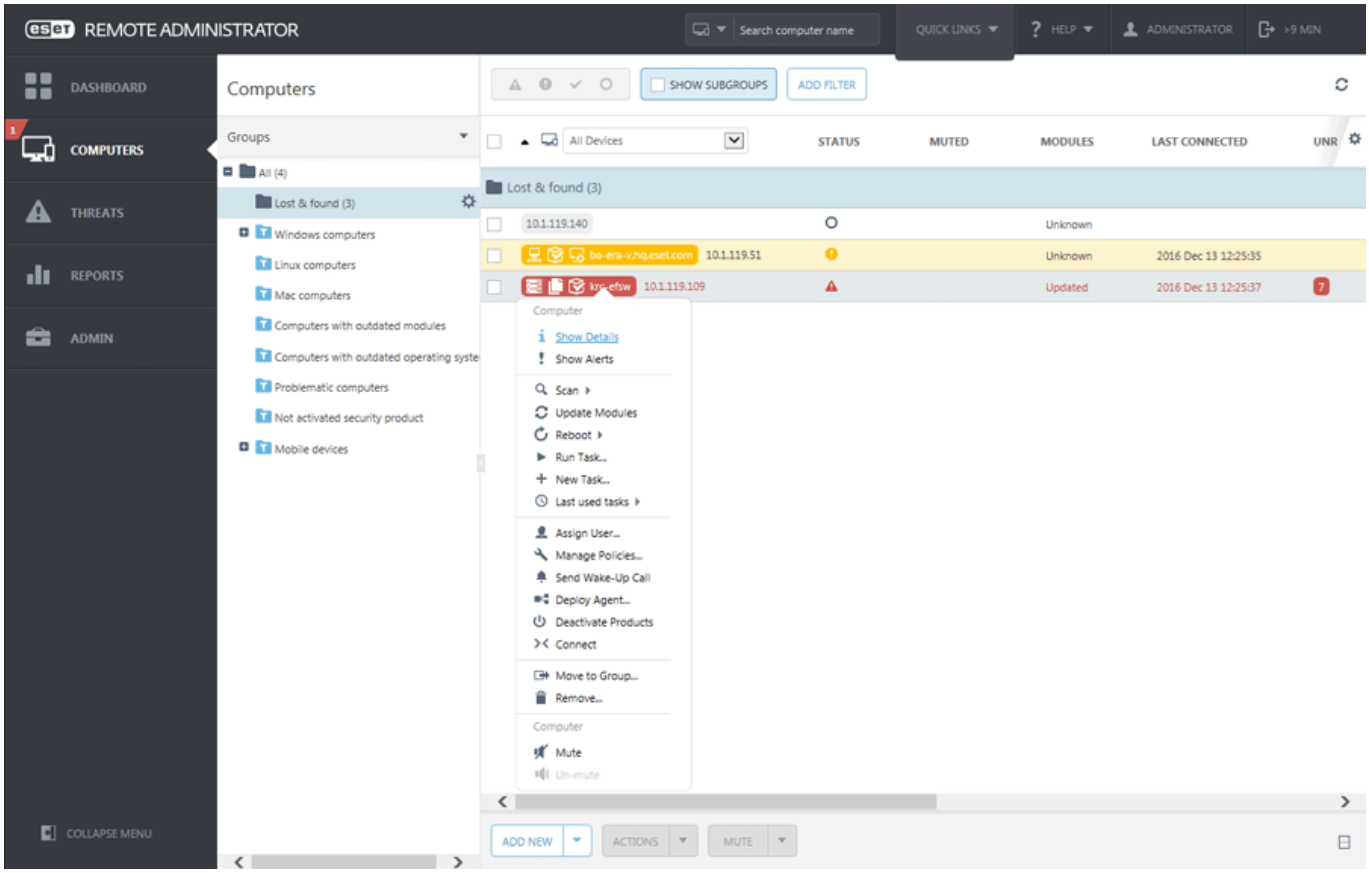
- 在您想要執行最新版本 ESET File Security 的所有伺服器上**執行軟體解除安裝**工作。

- 針對執行最新版本 ESET File Security 的所有伺服器**指派配置原則**。

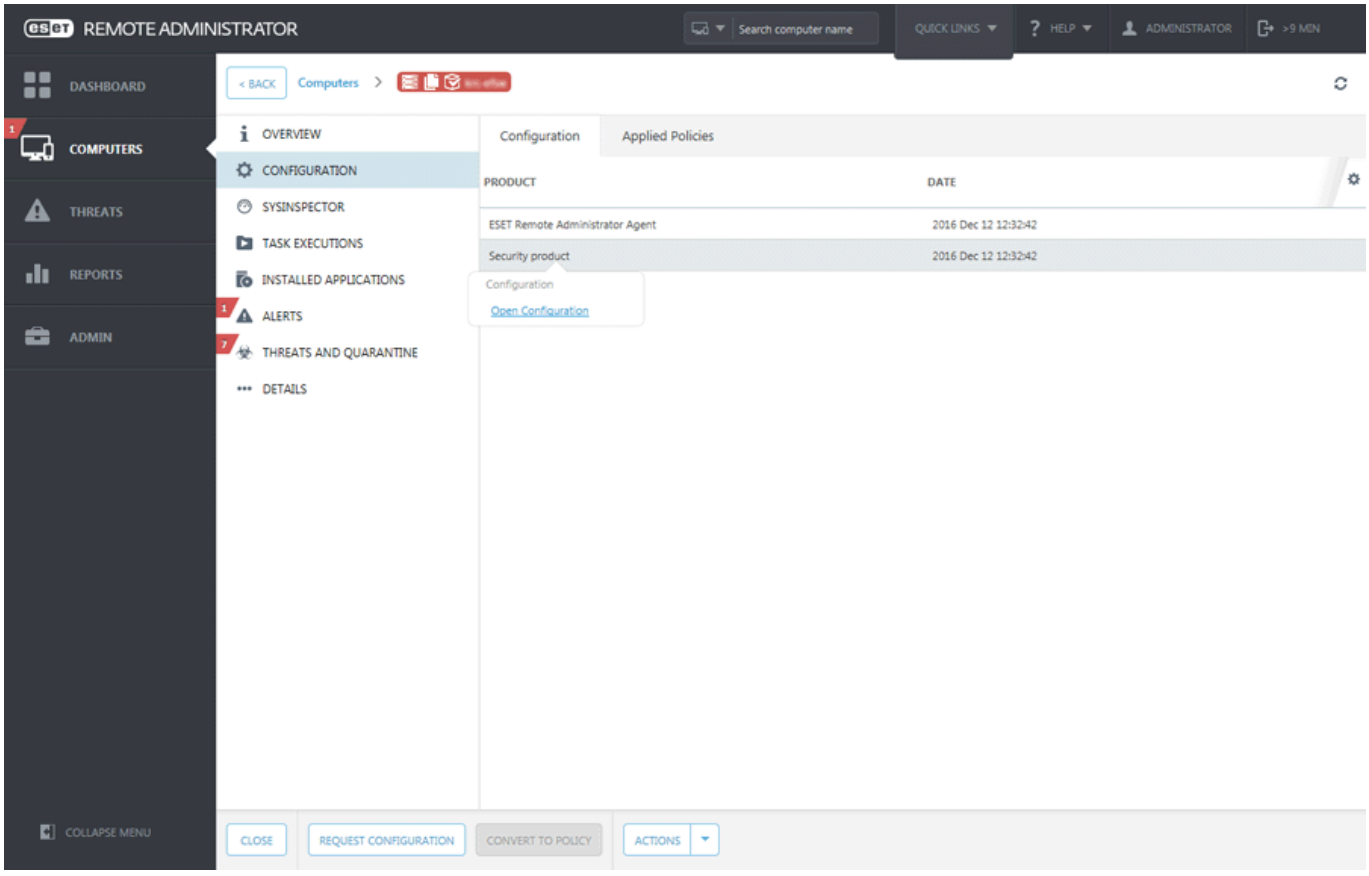
逐步安裝流程：

1.登入至執行 ESET File Security 的其中一部伺服器，並透過降級並安裝最新版本來覆蓋現有版本的方式來進行升級。遵循標準安裝的步驟。系統將於安裝期間保留您舊版本 ESET File Security 的所有原始配置。

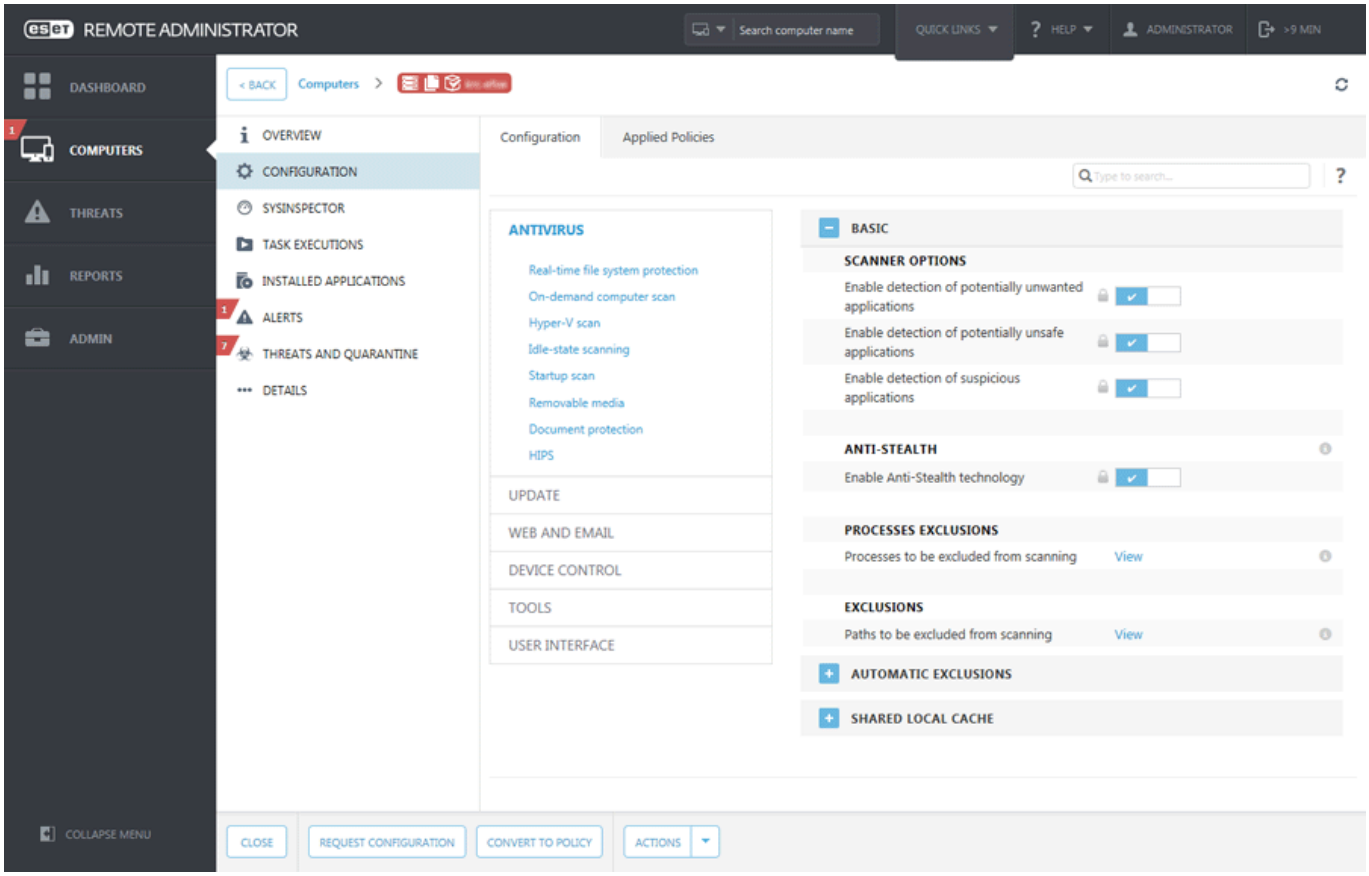
2.開啟 **[ESET Security Management Center Web Console]**，從「靜態」或「動態」群組內選取用戶端電腦，然後按一下 **[顯示] [詳細資訊]**。



3.瀏覽至 [配置] 索引標籤，然後按一下 **[要求配置]** 按鈕來收集所有受管理產品的配置。取得配置將需要花費一些時間。一旦最新配置顯示在清單中，按一下 **[指定產品]** 並選擇 **[開啟配置]**



4.透過按一下 **[轉換為原則]** 按鈕來建立配置原則。輸入新原則的 **[名稱]**，然後按一下 **[完成]**



5.瀏覽至 **[用戶端工作]**，然後選擇 [軟體解除安裝] 工作。建立解除安裝工作時，我們建議您先透過選取核取方塊 **[必要時自動重新開機]** 來解除安裝，然後再重新啟動伺服器。一旦工作建立之後，新增所有需要的目標電腦以進行解除安裝。

6.確保已從所有目標解除安裝 ESET File Security。

7.建立 [軟體安裝] 工作，以便將最新版本的 ESET File Security 安裝至所有需要的目標。

8.針對執行 ESET File Security 的所有伺服器**指派配置原則**，最好是指派至群組。

透過 ESET 叢集升級

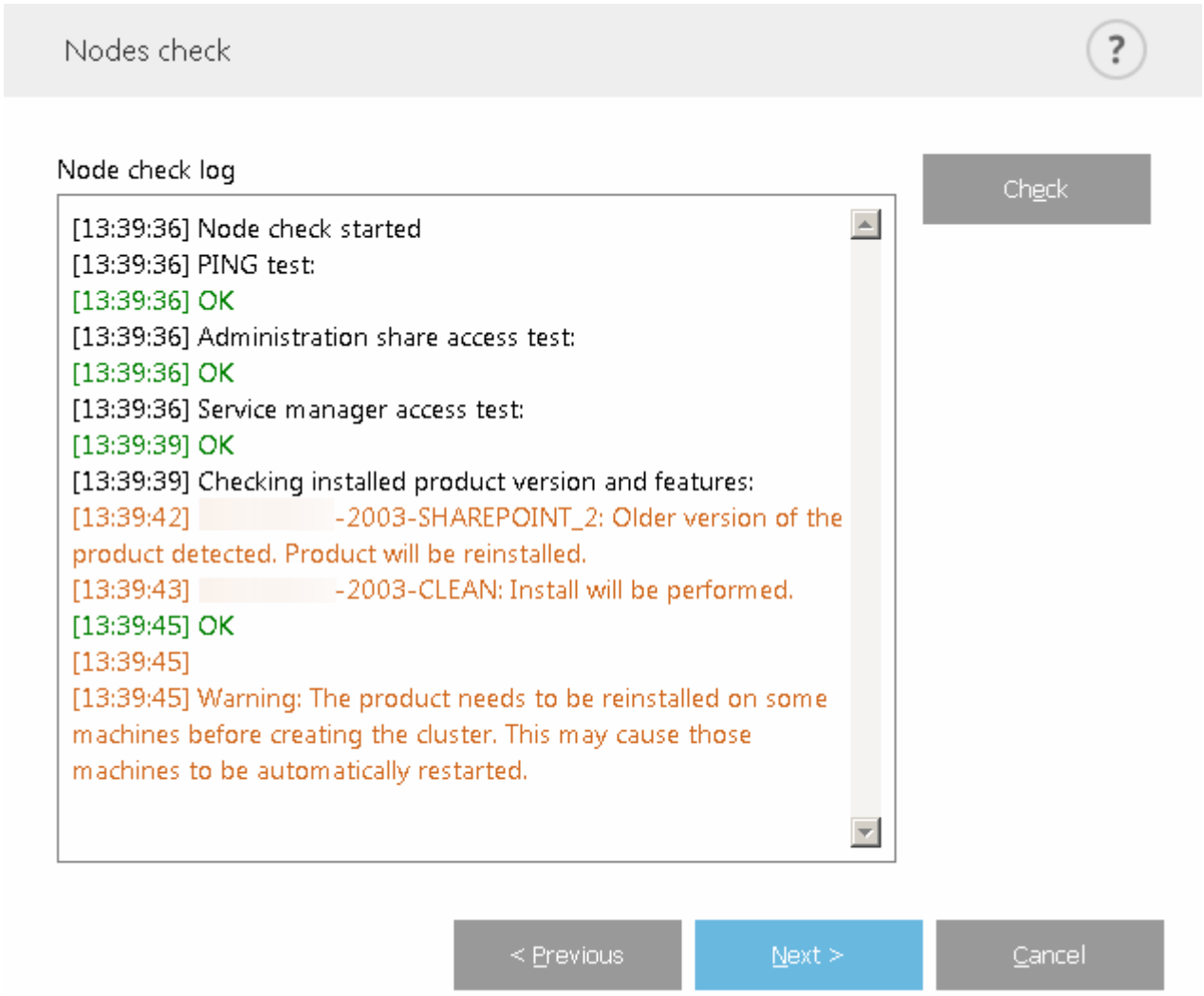
建立 ESET 叢集可讓您升級具有舊版本 ESET File Security 的多部伺服器。它是 ESMC 升級的替代選擇。如果您在環境中擁有包含 ESET File Security 的 2 部以上伺服器，則我們建議使用 ESET 叢集方法。此升級方法的其他好處在於您可以繼續使用 ESET 叢集，以便在所有成員節點上同步化 ESET File Security 配置。

遵循以下步驟以使用此方法升級：

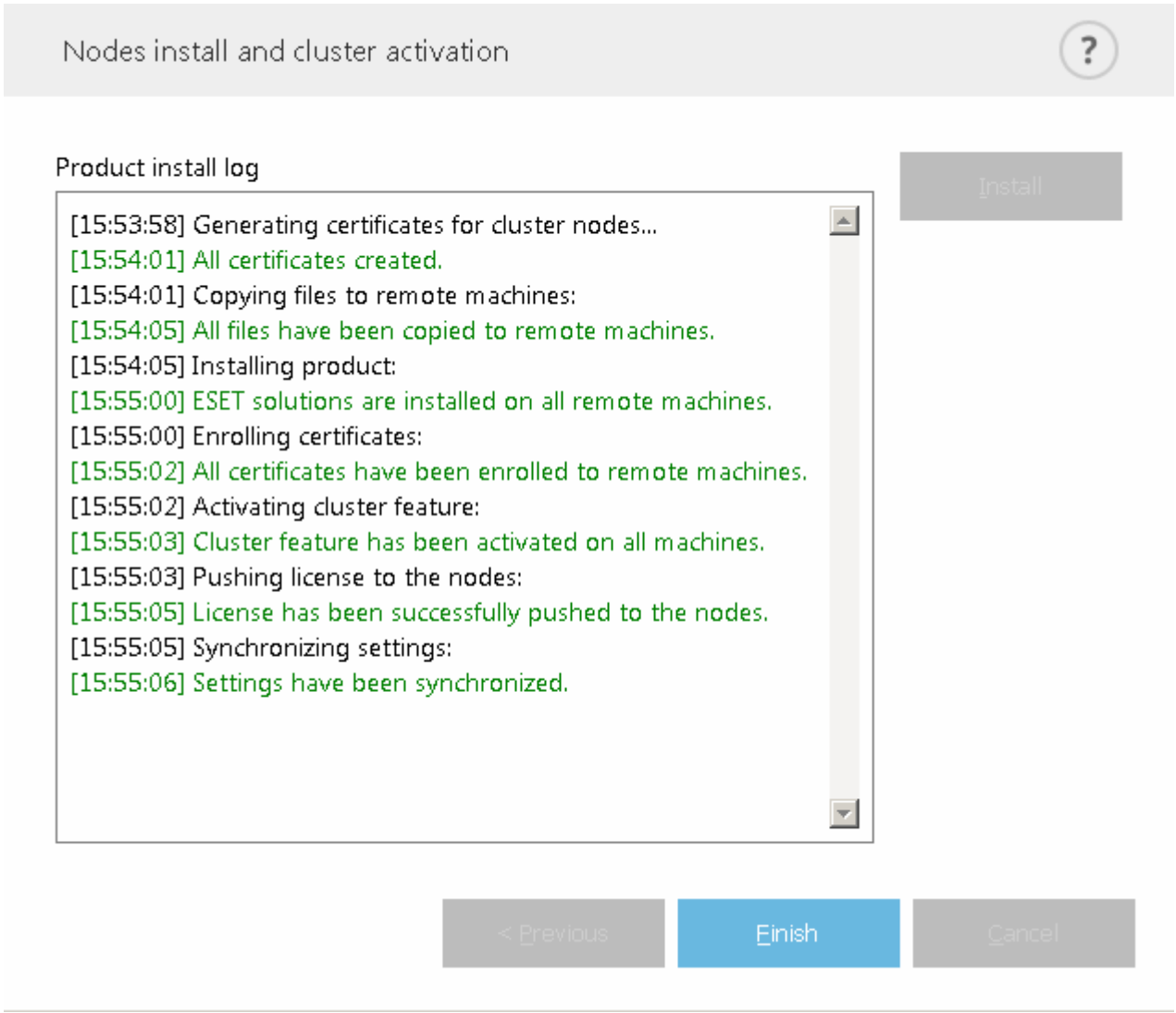
1.登入至執行 ESET File Security 的其中一部伺服器，並透過下載並安裝最新版本來覆蓋現有版本的方式來進行升級。遵循標準安裝的步驟。系統將於安裝期間保留您舊版本 ESET File Security 的所有原始配置。

2.執行 ESET 叢集精靈，並新增叢集節點（您想要升級 ESET File Security 的伺服器）。您可以在必要時新增其他尚未執行 ESET File Security 的伺服器（安裝將在這些伺服器上執行）。我們建議您在指定叢集名稱和安裝類型（確保已勾選 **[將授權推送到節點，但不啟動產品]**）時保留預設的設定。

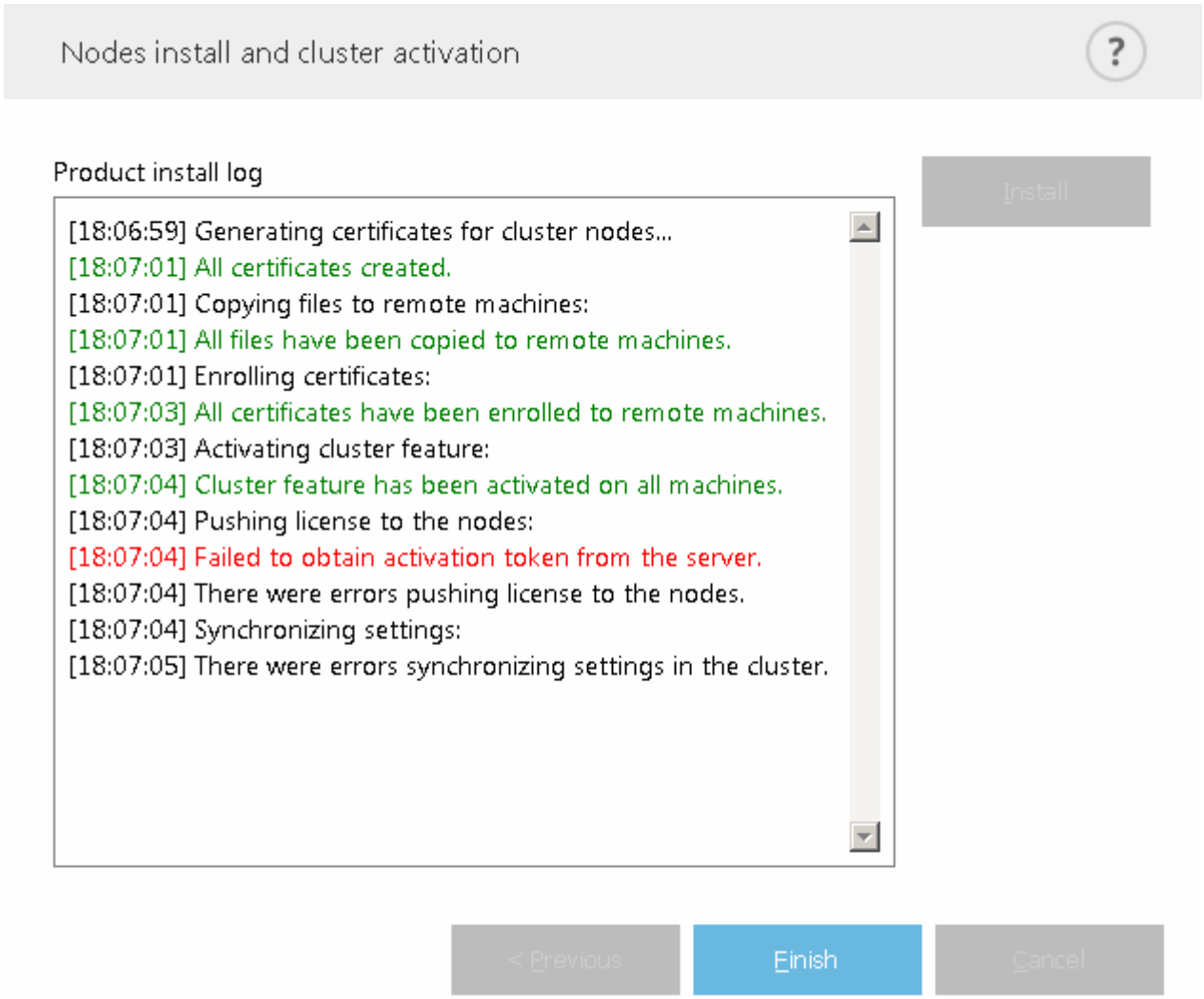
3.檢視 **[節點檢查記錄]** 畫面。它會列出包含舊版產品的伺服器，而該產品將會重新安裝ESET File Security 也將在目前尚未安裝的任何新增伺服器上安裝。



4.**[節點安裝和叢集啟動]** 畫面將顯示安裝進度。安裝成功完成時，完成結果看起來應該類似於：



若您的網路或 DNS 並未正確配置，則您可能會收到表示 **[無法從伺服器取得啟動 Token]** 的錯誤訊息。請再次嘗試執行 ESET 叢集精靈。這將會銷毀叢集並建立新叢集（不含重新安裝產品），而啟動應於此時成功完成。若問題持續存在，請檢查您的網路和 DNS 設定。



安裝在叢集環境

您可在叢集環境中部署 ESET File Security (例如容錯移轉叢集)。建議您在作用中的節點上安裝 ESET File Security之後使用 ESET File Security 的 ESET 叢集功能重新散佈安裝在被動節點上。除了安裝以外ESET 叢集會作為 ESET File Security 配置的複製，以確保叢集結點間正確作業所需的一致性。

終端機伺服器

如果您在作為終端機伺服器的 Windows Server 上安裝 ESET File Security而且想要停用 ESET File Security GUI 以避免每次使用者登入時即啟動，請參閱停用終端機伺服器的 GUI，以瞭解停用 GUI 的特定步驟。

開始使用

下列部分應該能協助您開始使用 ESET File Security

監視

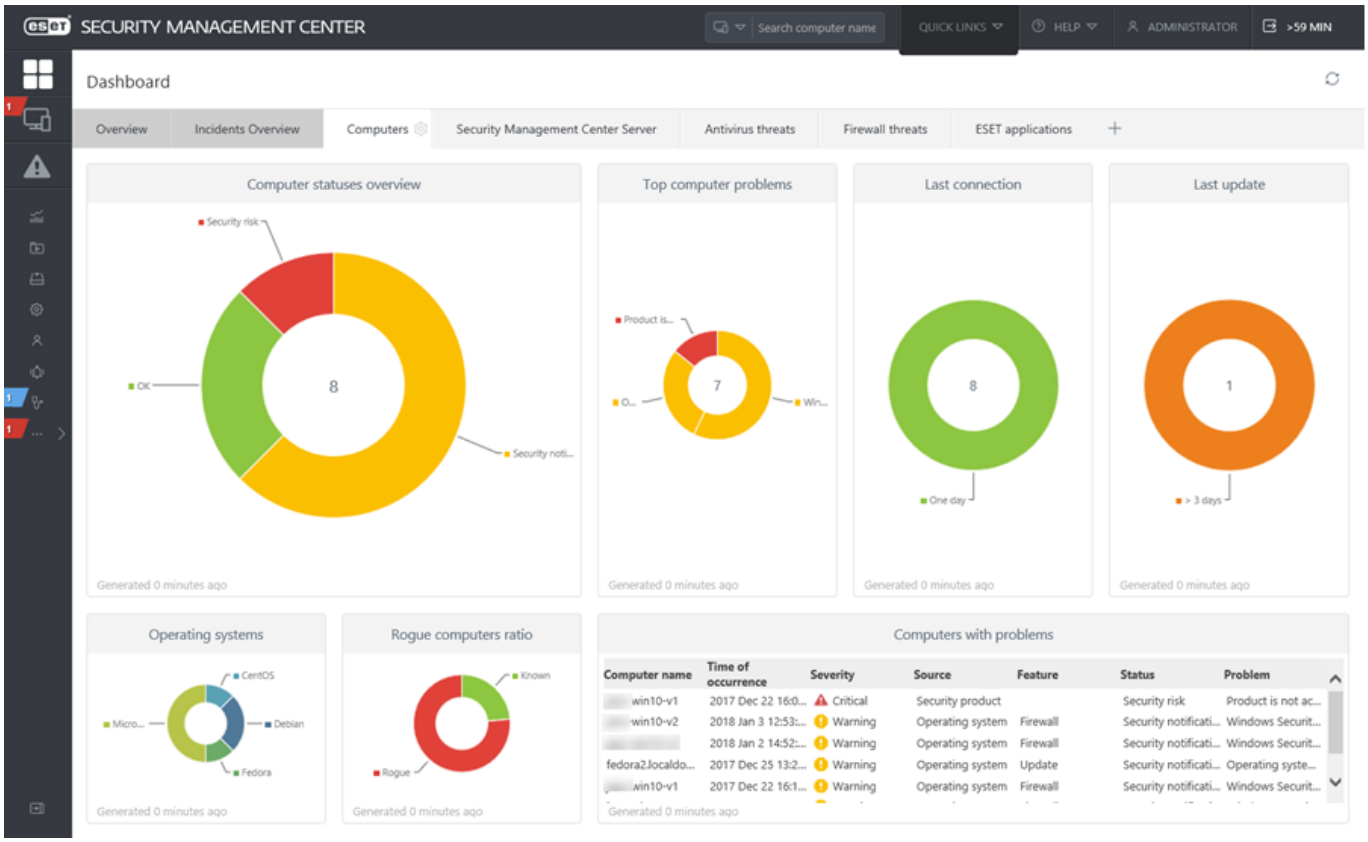
可讓您立即檢視 ESET File Security 目前狀態的概觀。乍看之下，您就能發現是否有任何問題需要您留意。

已透過 ESET Security Management Center 管理

您可以使用 ESET Security Management Center 遠端管理 ESET File Security。

已透過 ESET Security Management Center 管理

ESET Security Management Center (ESMC) 是一個應用程式，允許您在網路環境中透過一個中央位置管理 ESET 產品。ESET Security Management Center 工作管理系統允許您在遠端電腦安裝 ESET 安全性解決方案並對新問題和威脅快速作出回應。ESET Security Management Center 本身不提供保護以防範惡意程式碼，該功能由每個用戶端上安裝的 ESET 安全性解決方案所提供。ESET 安全性解決方案支援包含多種平台類型的網路。您的網路可以是由目前的 Microsoft、Linux、Mac OS X 和行動作業系統組合而成。



如需 ESMC 的詳細資訊，請參閱 [ESET Security Management Center 線上說明]。

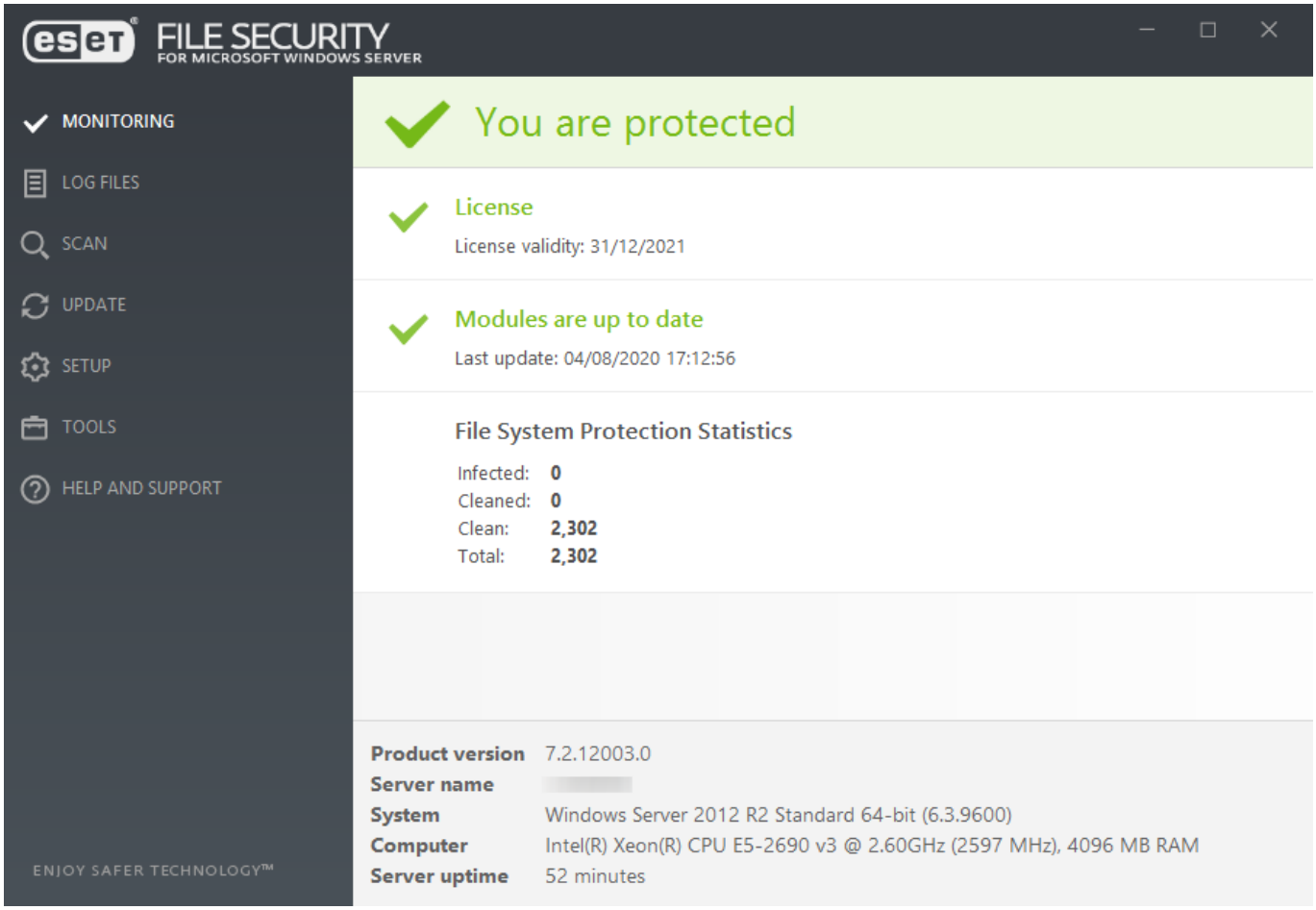
監視

顯示於**監視**區段中的防護狀態會通知您電腦目前的防護層級。ESET File Security 作業的狀態摘要顯示在主要視窗。

綠色**您已受到保護** 狀態表示已確保最嚴格的防護。

紅色圖示表示嚴重問題 – 未確保電腦獲得最嚴格的防護。如需可能防護狀態的清單，請參閱「狀態」區段。

橙色圖示表示您的 ESET 產品需要注意非嚴重問題。



正常運作的模組會標上綠色核取符號。未完全運作的模組會標上紅色驚嘆號或顯示橙色通知圖示。視窗的上半部會顯示模組的其他相關資訊。同時還會顯示修正模組的建議解決方案。若要變更個別模組的狀態，請按一下主要功能表中的［設定］，然後按一下需要的模組。

監視頁面也包含以下系統資訊：

- **產品版本** - ESET File Security 的版本號碼。
- **伺服器名稱** – 機器主機名稱或 FQDN。
- **系統** – 作業系統詳細資訊。
- **電腦** – 硬體詳細資訊。
- **伺服器執行時間** – 顯示系統啟動與執行的時間長度，基本上會與停機時間相反。

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

狀態

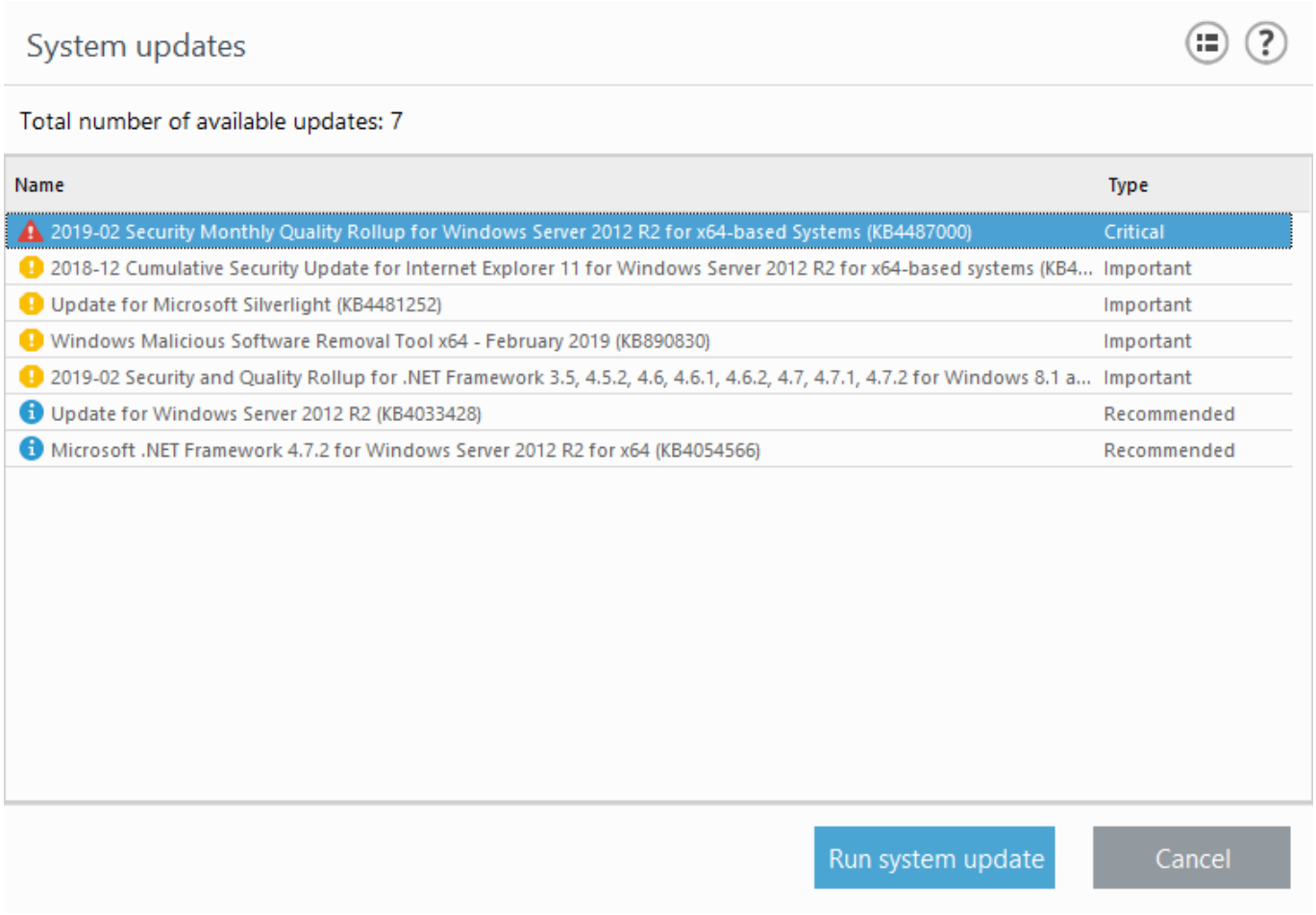
ESET File Security 的狀態摘要以及系統詳細資訊會顯示於主要視窗。在正常情況下，若所有功能運作正常且沒有發生問題，防護狀態會是 綠色。但是，防護狀態會在特定情況下變更。防護狀態會變更為 橘色或 紅色，而且如果發生下列任一情況，便會顯示警告訊息：

警告訊息	警告訊息詳細資料
尚未配置潛在不需要應用程式偵測	潛在不需要的應用程式 (PUA) 是含有廣告軟體、安裝工具列或具有其他不明企圖的程式。在某些情況下，使用者可能會認為潛在不需要的應用程式的優點大於風險。
即時檔案系統防護已暫停	按一下［監控］標籤中的**［啟用即時防護］**或重新啟用主要程式視窗中［設定］標籤中的**［即時檔案系統防護］**。
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，因此此功能無法運作。
已停用 ESET LiveGrid®	在**［進階設定］**中停用 ESET LiveGrid® 時表示此問題。
已停用通訊協定過濾	按一下［啟用通訊協定篩選］重新啟用此功能。
作業系統不是最新的	［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。
您的裝置將會失去防護	有關如何更新您的 Microsoft Windows 版本的詳細資訊，請按一下查看您的選項。如果您執行的是 **Microsoft Windows Server 2008 R2 SP1** 或 **Microsoft Windows Small Business Server 2011 SP1**，請確保您的系統與 SHA-2 相容。請根據特定作業系統版本套用修補程式。
已啟用簡報模式	所有快顯視窗均已隱藏且已排程工作已暫停。
網路攻擊防護 (IDS) 已暫停	按一下［啟用網路攻擊防護 (IDS)］重新啟用此功能。
殭屍網路防護已暫停	按一下［啟用殭屍網路防護］重新啟用此功能。
Web 存取防護已暫停	按一下［監控］中的**［啟用 Web 存取防護］**，或是在主要程式視窗的［設定］窗格重新啟用[Web 存取防護]。
裝置控制已暫停	按一下［啟用裝置控制］重新啟用此功能。
產品尚未啟動或授權已過期	這是由變成紅色的［防護］狀態圖示所表示。授權過期後即無法更新程式。請按照警告視窗中的指示更新您的授權。
原則覆蓋作用中	這會暫時覆寫原則所設定的配置，有可能會一路直到疑難排解完成為止。如果您正在使用 ESMC 管理 ESET File Security且擁有指派給它的原則，系統將會根據原則所屬功能，鎖定（呈現灰色）狀態連結。

如果您無法使用建議的解決方案解決問題，請搜尋ESET 知識庫」。如果仍然需要協助，您可以提交支援要求ESET 客戶服務」將快速回答您的問題並協助尋找解決方法。

有可用的 Windows 更新

［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。以滑鼠右鍵按一下任何更新列，然後按一下**［更多資訊］**以在快顯視窗中顯示其他資訊：



按一下［**執行系統更新**］開啟 **[Windows 更新]** 視窗並繼續進行系統更新。

網路隔離

ESET File Security 可讓您選擇是否要封鎖伺服器的網路連線，這稱為網路隔離。在某些極端情況下，您可能希望隔離網路中的伺服器作為防護措施。例如，如果您發現伺服器受到惡意軟體感染或是機器受到危害。

啟動網路隔離，即會封鎖所有網路流量，下列除外：

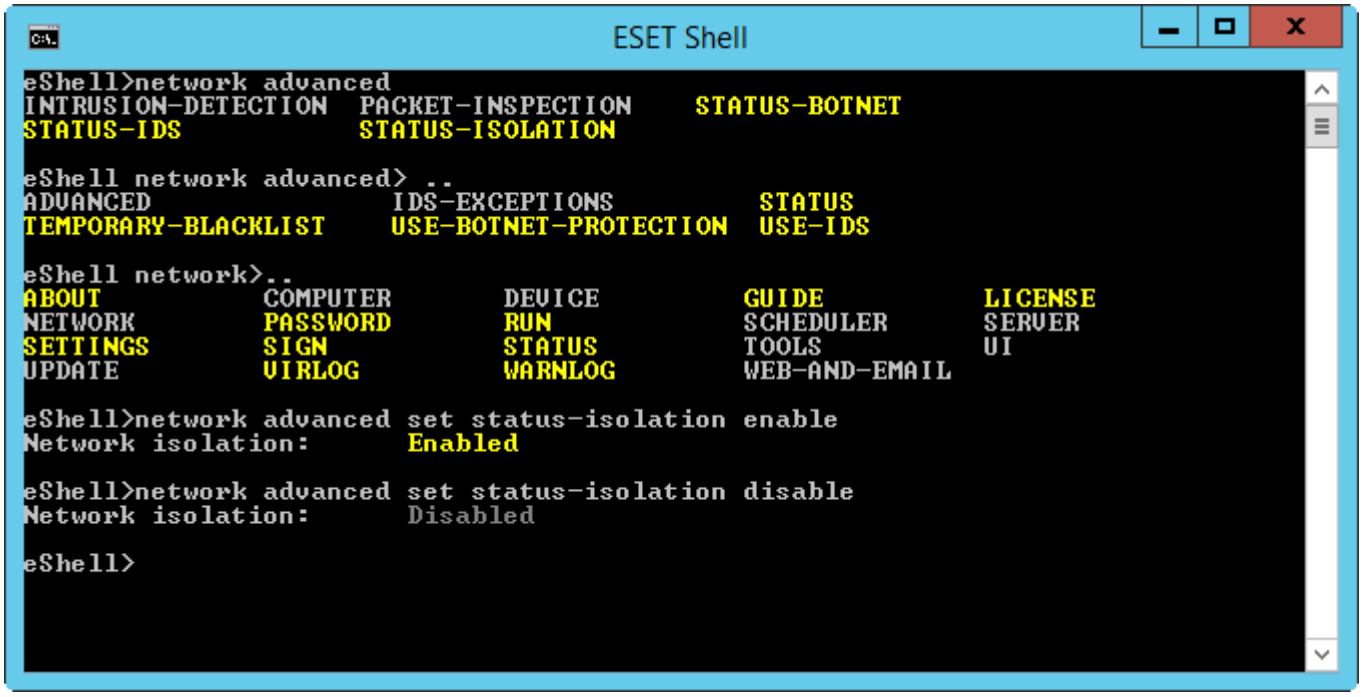
- 仍可連線至網域控制站
- ESET File Security 仍可進行通訊
- 若是如此，ESET Management Agent 及 ESET Enterprise Inspector 代理程式仍可透過網路進行通訊。

使用 eShell 命令或 ESET Security Management Center 用戶端工作來啟動和停用網路隔離。

eShell

在互動模式中：

- 啟動網路隔離：`network advanced set status-isolation enable`
- 停用網路隔離：`network advanced set status-isolation disable`



或者，您可以使用批次/指令碼模式建立並執行批次檔案。

ESET Security Management Center

- 透過用戶端工作 啟動網路隔離。
- 透過用戶端工作 停用網路隔離。

啟動網路隔離時，ESET File Security 狀態會變更為紅色，而且會顯示訊息 **[網路存取已封鎖]**。

使用 ESET File Security

此部分包含程式使用者介面的詳細說明，而且著重於說明如何使用 ESET File Security。

使用者介面可讓您快速存取常用的功能：

- 監視
- 防護記錄檔案
- 掃描
- 更新
- 設定
- 工具

掃描

指定掃描器是 ESET File Security 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。如要確保網路的安全性，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。資料寫入磁碟時，若即時檔案系統防護已停用、偵測引擎未更新，或是未在檔案初次儲存至磁碟時偵測到檔案，就可能發生威脅入侵情況。

選取適用於 ESET File Security 的指定掃描：

儲存裝置掃描

掃描所有本機伺服器上的共用資料夾。如果無法使用［儲存裝置掃描］，表示您的伺服器上沒有共用資料夾。

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。智慧型掃描的優點在於可以輕鬆執行作業，而不需要詳細的掃描配置。掃描您的電腦會檢查本機磁碟中所有的檔案，且會自動清除或刪除偵測到的入侵。清除層級會自動設為預設值。如需更多有關清除類型的資訊，請參閱清除

注意
我們建議您一個月至少執行一次電腦掃描。可以將掃描配置為已排程的工作

自訂掃描

如果您想要指定掃描參數（例如掃描目標及掃描方法），則自訂掃描是可最理想的解決方案。自訂掃描的優點是可以詳細地配置掃描參數。您可以將配置儲存為使用者定義的掃描設定檔，以利於使用相同參數重複執行掃描。

可移除的媒體掃描

與「智慧型掃描」類似 – 可快速啟動掃描與電腦連接的可移除媒體（如 CD/DVD/USB)當您將 USB 隨身碟連接到電腦，想要掃描其內容是否有潛在威脅時，此功能相當實用。也可以按一下 **［自訂掃描］**，然後從 **［掃描目標］** 下拉式功能表選取 **［卸除式媒體］** 並按一下 **［掃描］**，開始進行這類型的掃描。

Hyper-V 掃描

執行 ESET File Security 的伺服器必須已安裝 Hyper-V Manager您才會在功能表中看到此選項Hyper-V 掃描可掃描 Microsoft Hyper-V Server 上的虛擬機器 (VM) 磁碟，無須在特定 VM 上安裝任何「代理程式」。

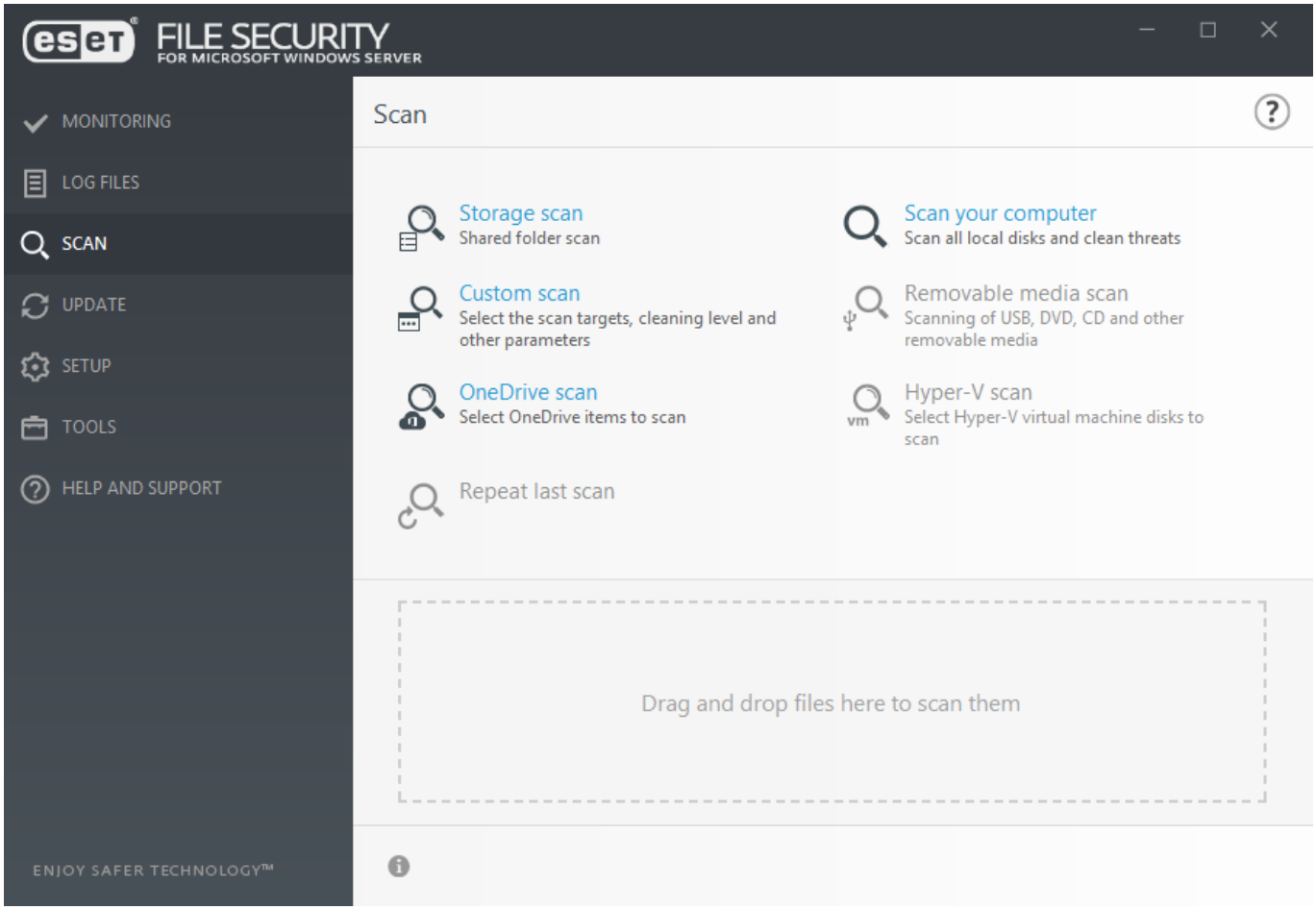
OneDrive 掃描

可讓您掃描 OneDrive 雲端儲存空間上的使用者檔案。

重複上次掃描

使用完全相同的設定重覆您的上一次掃描作業。

注意
存在指定資料庫掃描時，無法使用重複上次掃描功能。



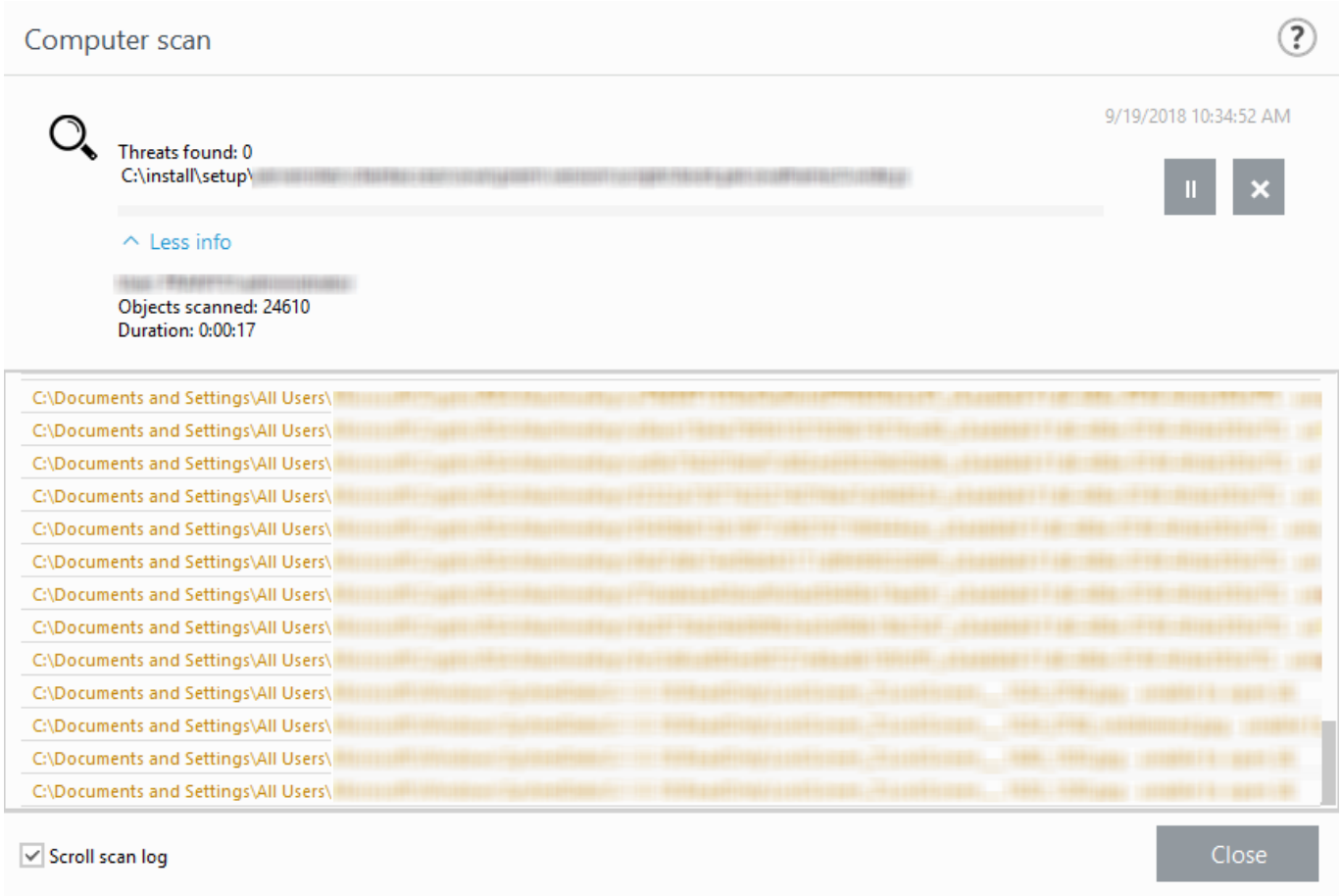
您可以使用選項並顯示掃描狀態的詳細資訊：

拖放檔案	**您也可以將檔案拖放到 ESET File Security 掃描視窗。會立即掃描這些檔案是否存有病毒。**
關閉/全部關閉	關閉指定訊息。
掃描狀態	顯示初始掃描的狀態。此掃描已完成或是由使用者中斷。
顯示防護記錄	顯示更詳細的資訊。
更多資訊	在掃描期間，查看詳細資料，例如執行掃描的 **[使用者]**、**[已掃描的物件]** 的數量以及掃描 **[持續時間]**。
開啟掃描視窗	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。

掃描視窗及掃描防護記錄

掃描視窗會顯示目前掃描的物件（包含其位置、找到的威脅數目（若有的話）、已掃描的物件數目及掃描期間）。視窗底部是掃描防護記錄，其中會顯示偵測引擎版本號碼、開始掃描的日期及時間及目標選取項目。

掃描正在進行時，如果您想要暫時中斷掃描，可按一下 **[暫停]**。暫停掃描程序時，可使用 **[繼續]** 選項。

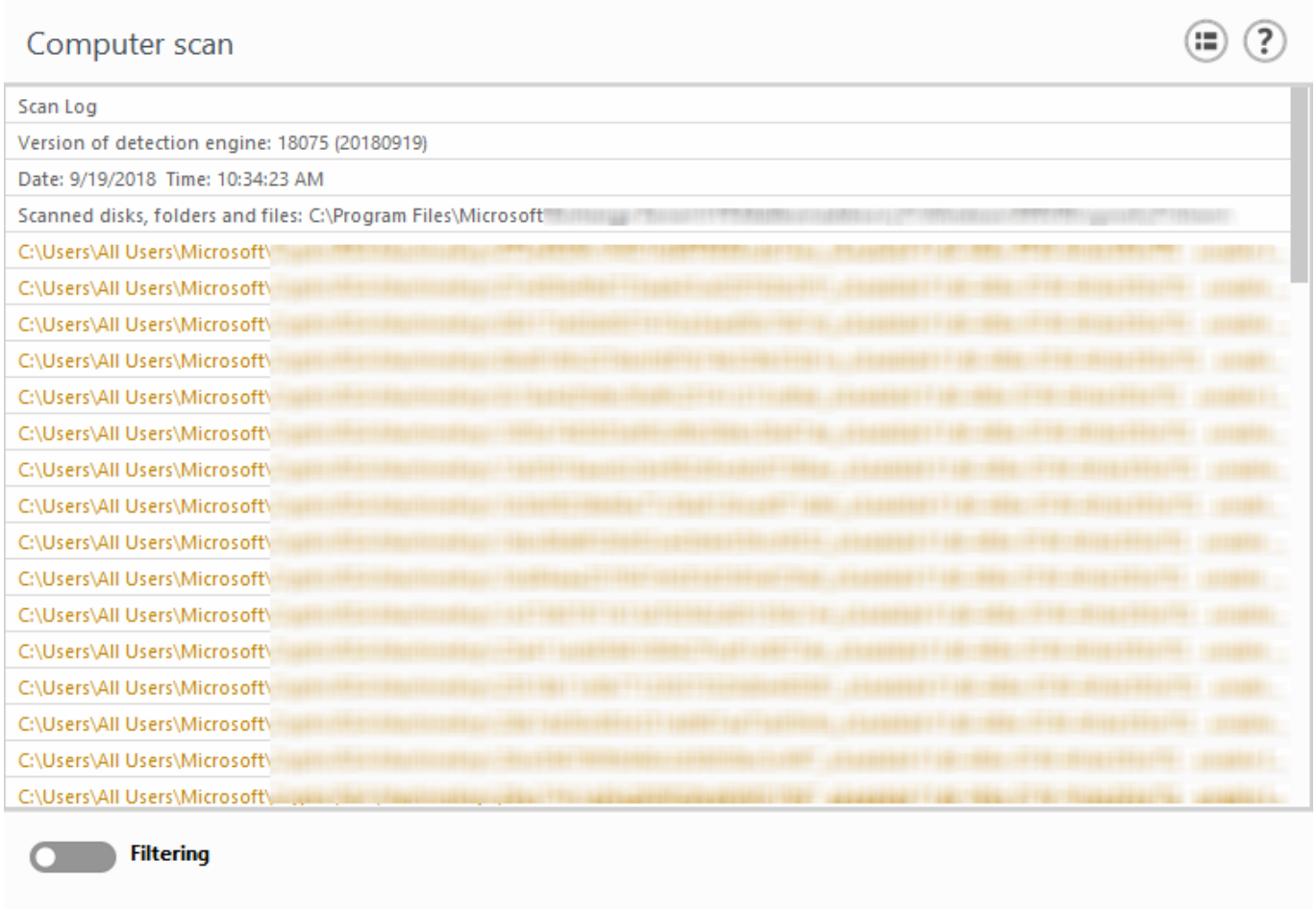


捲動掃描防護記錄

將此選項保持在啟用狀態，以自動捲動舊的防護記錄，並且檢視［防護記錄檔案］視窗中的作用中防護記錄。

> 注意
> 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）。

完成掃描之後，您會看到包含與特定掃描相關之所有相關資訊的掃描防護記錄。



按一下切換圖示 **[過濾]** 以開啟 [防護記錄篩選] 視窗，您可以在其中定義過濾或搜尋條件。若要檢視內容功能表，在特定防護記錄項目按一下滑鼠右鍵：

處理方法	使用	快捷鍵	也請參閱
過濾相同的記錄	此功能會啟動防護記錄過濾並只顯示與所選記錄相同的記錄類型。	Ctrl + Shift + F	
過濾...	按一下此選項之後，會出現 [防護記錄過濾] 視窗，可讓您定義特定防護記錄項目的過濾條件。		防護記錄過濾
啟用過濾	啟動過濾設定。第一次啟動過濾，您必須定義設定。		
停用過濾	關閉過濾（與按一下底部的切換相同）。		
複製	將選取的/強調的記錄資訊複製到剪貼簿。	Ctrl + C	
全部複製	複製視窗中所有記錄的資訊。		
匯出...	匯出選取的/強調的記錄資訊至 XML 檔案。		
全部匯出...	將視窗中的所有資訊匯出至 XML 檔案。		

防護記錄檔案

防護記錄檔案包含已發生之重要程式事件的相關資訊，並提供掃描結果、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 File Security 環境檢視文字訊息及防護記錄，或是匯出這些記錄以供檢視。

從下拉式功能表中選取適當的防護記錄類型。下列防護計畫可供使用：

偵測

偵測防護記錄提供 ESET File Security 模組所偵測到入侵的詳細資訊。資訊包括偵測時間、入侵的名稱、位置，以及在偵測到入侵時，所登入的使用者名稱及其執行的動作。按兩下防護記錄項目（偵測），以在個別視窗中顯示其詳細資訊。如果有需要，您可以建立偵測排除 – 滑鼠右鍵按一下防護記錄項目（偵測），然後按一下**[建立排除]**。這將會以預定義準則開啟排除精靈。如果在排除檔案旁有偵測名稱，表示該檔案只受到特定的偵測排除。如果該檔案之後受到其他惡意軟體感染，仍然會被偵測到。

事件

ESET File Security 執行的所有重要處理方法，都會記錄在事件防護記錄中。事件防護記錄包含在程式中發生的事件及錯誤相關資訊，專門用來協助系統管理員及使用者解決問題。針對程式中發生的問題，在這裡找到的資訊通常可協助您找到解決方案。

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

包含遭到封鎖且無法存取的檔案記錄。通訊協定會顯示封鎖該檔案之來源模組的原因，以及會執行該檔案的應用程式及使用者。

已傳送檔案

包含雲端型防護ESET 動態威脅防禦及 ESET LiveGrid® 的檔案記錄。

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

包含殭屍網路防護及 IDS (網路攻擊防護）封鎖的檔案記錄。

已過濾的網站

已由 Web 存取防護 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

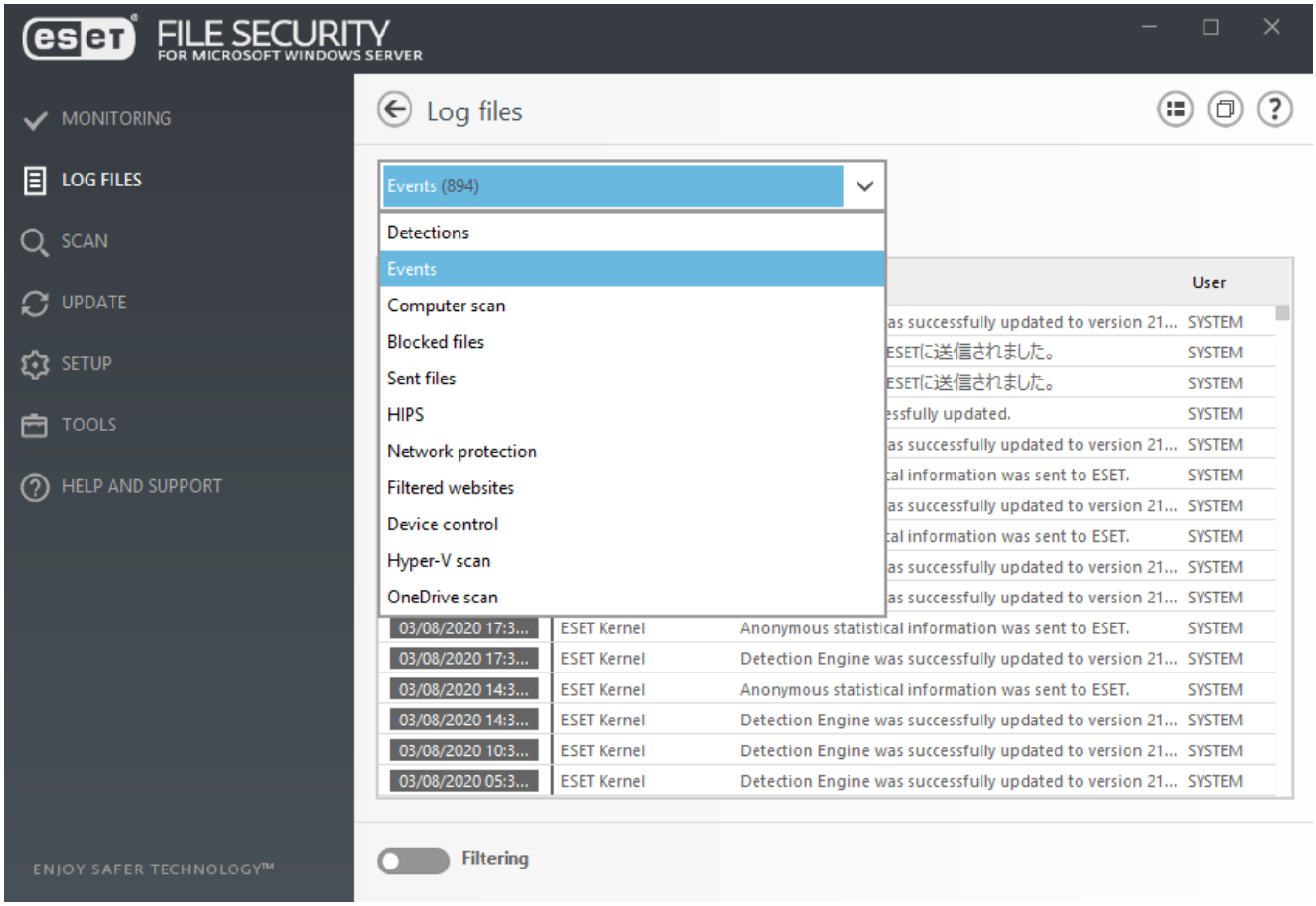
包含連接到電腦的可移除媒體或裝置記錄。僅含有裝置控制規則的裝置將記錄於防護記錄檔案中。如果規則不符合連接的裝置，將不會對連接的裝置建立防護記錄項目。您也可以在這裡看見詳細資訊，例如裝置類型、序號、供應商名稱及媒體大小（如果有）。

Hyper-V 掃描

包含 Hyper-V scan 掃描結果清單。按兩下任何項目，以檢視各個掃描的詳情。

OneDrive 掃描

包含 OneDrive 掃描結果的清單。



（以滑鼠右鍵按一下）內容功能表讓您選擇要對防護記錄採取的動作：

處理方法	使用	快捷鍵	也請參閱
顯示	顯示有關在新視窗中所選取防護記錄的詳細資訊（與按兩下相同）。		
過濾相同的記錄	此功能會啟動防護記錄過濾並只顯示與所選記錄相同的記錄類型。	Ctrl + Shift + F	

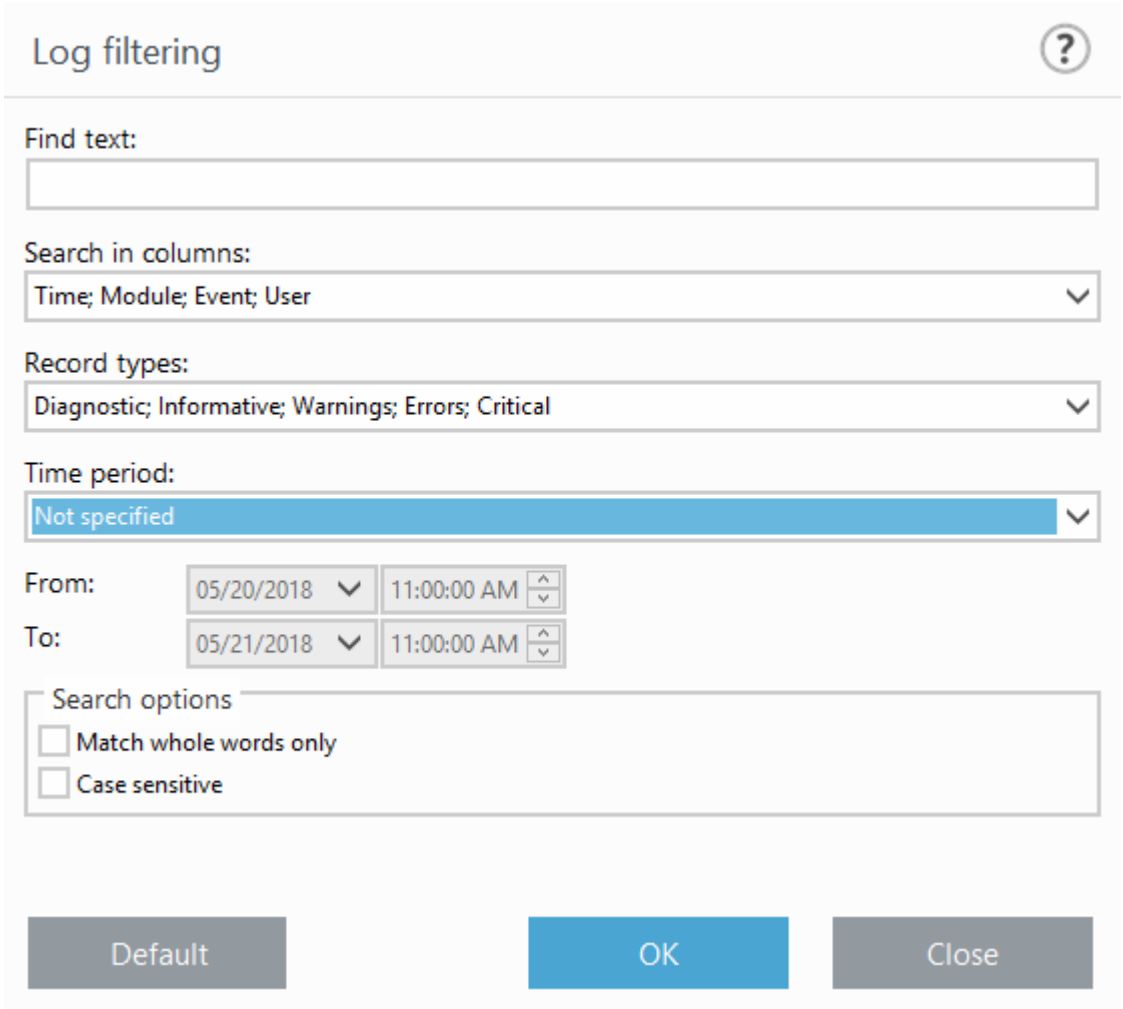
處理方法	使用	快捷鍵	也請參閱
過濾...	按一下此選項之後，會出現［防護記錄過濾］視窗，可讓您定義特定防護記錄項目的過濾條件。		防護記錄過濾
啟用過濾	啟動過濾設定。第一次啟動過濾，您必須定義設定。		
停用過濾	關閉過濾（與按一下底部的切換相同）。		
複製	將選取的/強調的記錄資訊複製到剪貼簿。	Ctrl + C	
全部複製	複製視窗中所有記錄的資訊。		
刪除	刪除選取/強調的記錄 – 此動作需要管理員權限才能執行。		
全部刪除	刪除視窗中的所有記錄 – 此動作需要管理員權限才能執行。		
匯出...	匯出選取的/強調的記錄資訊至 XML 檔案。		
全部匯出...	將視窗中的所有資訊匯出至 XML 檔案。		
尋找...	開啟［在防護記錄中尋找］視窗可讓您定義搜尋條件。即使在過濾功能開啟時，您也可以使用搜尋功能找出特定記錄。	Ctrl + F	在防護記錄中尋找
尋找下一個	使用先前定義的搜尋條件尋找下一筆項目。	F3	

處理方法	使用	快捷鍵	也請參閱
尋找上一個	尋找前一筆項目。	Shift + F3	
建立排除	若要使用偵測名稱、路徑或其雜湊從清除排除物件。		建立排除

防護記錄過濾

防護記錄過濾功能會協助您找到您正在尋找的資訊，特別是有許多記錄時。這可讓您縮小防護記錄的範圍，例如，如果您正在尋找特定類型的事件、狀態或時段。您可以指定特定搜尋選項來過濾防護記錄、記錄，而且只有相關（根據那些搜尋選項）的記錄會顯示在［防護記錄檔案］視窗中。

將您正在搜尋的關鍵字輸入**［尋找文字］**欄位中。使用**［搜尋直欄］**下拉式功能表以精簡您的搜尋。從**［防護記錄類型］**下拉式功能表選擇一或多個記錄。定義您想要顯示結果的**［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（整個單字或單字的一部分）。將僅尋找包含此字串的記錄。將忽略其他記錄。

搜尋直欄

選取搜尋時將考慮哪些直欄。您可以勾選將用於搜尋的一個或多個直欄。

記錄類型

從下拉式功能表中選擇一或多個記錄防護記錄類型：

- **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** – 僅防護記錄嚴重錯誤。

時段

定義要顯示結果的時段。

- **未指定**（預設）– 不搜尋時間內的記錄，而搜尋整個防護記錄。
- **前一天**
- **上一週**
- **上個月**
- **時段** – 您可以指定確切的時間（[開始時間:] 及 [結束時間:]，以便僅搜尋指定時段內的記錄。

所有文字須相符

若您想利用完整文字進行更精確的搜尋，請使用此核取方塊。

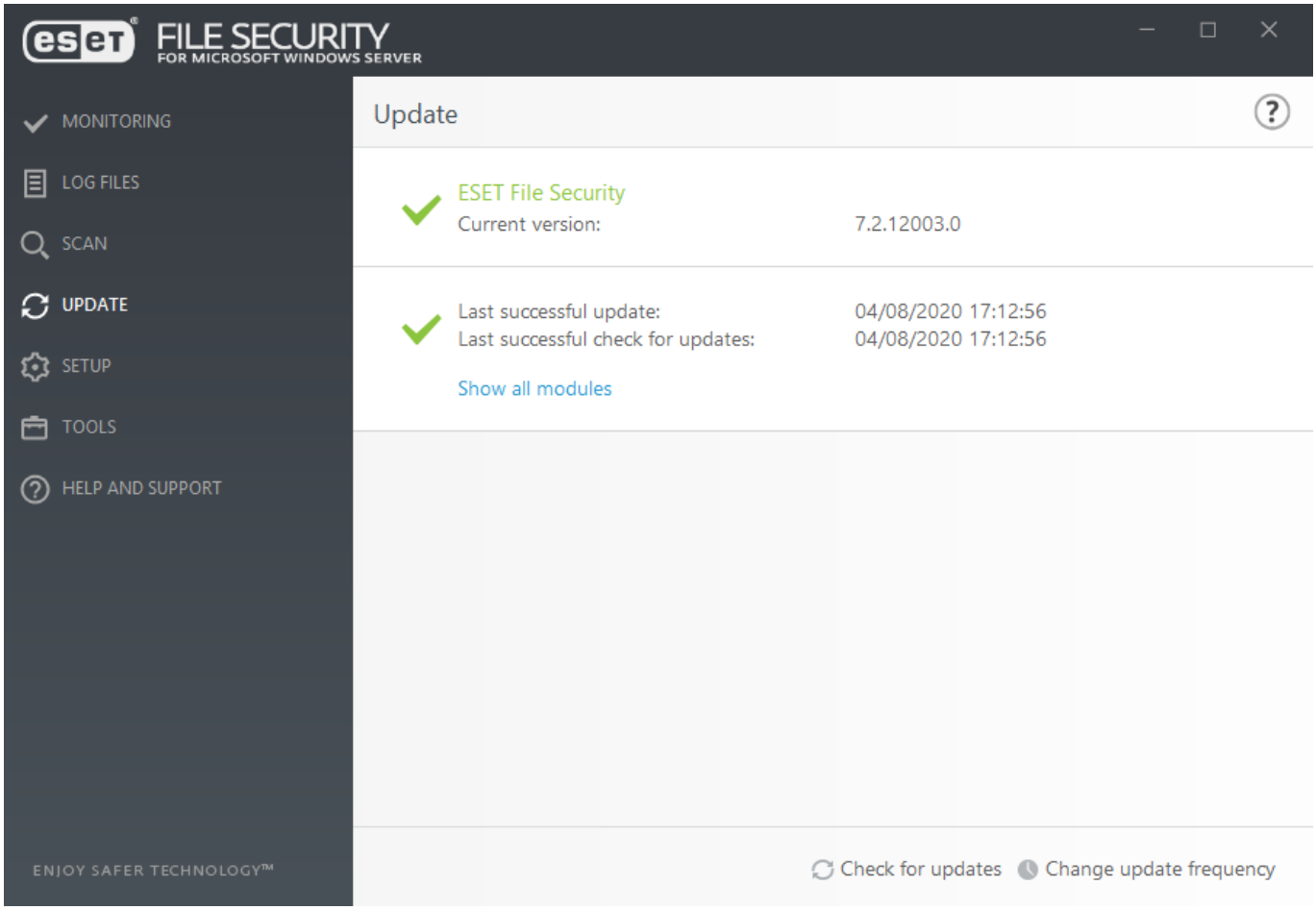
區分大小寫

如果您認為過濾時使用大小寫很重要請，請啟用此選項。配置您的過濾/搜尋選項之後，按一下 **[確定]** 以顯示過濾的防護記錄或 **[尋找]** 以開始搜尋。會從上至下搜尋防護記錄 – 從目前位置（強調顯示的記錄由上至下搜尋防護記錄檔案。找到第一個對應的記錄時，搜尋便會停止。按下 **F3** 搜尋下一個記錄或按一下滑鼠郵件並選取 **[尋找]** 以精簡您的搜尋選項。

[更新]

在 [更新] 區段中，您會看到 ESET File Security 的目前更新狀態，包含最後成功更新的日期及時間。定期更新 ESET File Security 是讓伺服器保有最高安全性等級的最佳方法。「更新」模組會透過更新病毒資料庫及更新系統元件兩種方式，確保程式永遠為最新。更新偵測引擎及程式元件是提供完整防護以抵禦惡意軟體的重要部分。

> 注意
> 如果您尚未輸入授權金鑰，您就無法接收更新，而且系統會提示您啟動產品。若要這麼做，請瀏覽至 **[說明及支援] > [啟動產品]**



目前的版本

ESET File Security 建置版本。

上一次的成功更新

上次更新的日期。請確認系統是指出最近的日期，表示模組是最新的。

上次成功檢查更新

上次嘗試更新模組的日期。

顯示所有模組

開啟已安裝模組的清單。

檢查更新

更新模組是維持完整防護、防止惡意代碼的一個重要部分。

變更更新頻率

您可以編輯排程器工作自動定期更新的工作時間。

如果您並未儘快檢查更新，會顯示下列其中一項訊息：

錯誤訊息	說明
模組更新已過期	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。

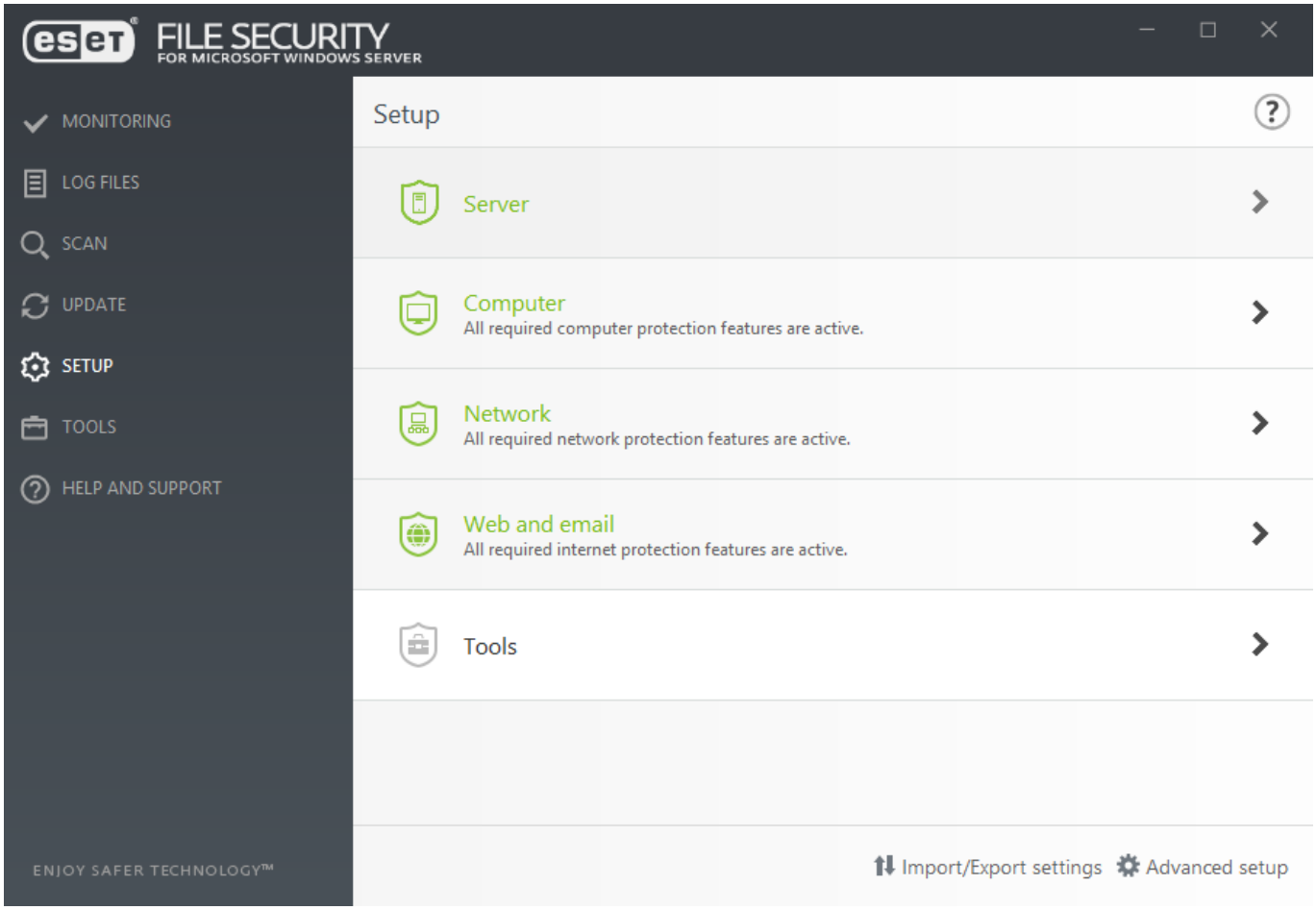
錯誤訊息	說明
模組更新失敗 – 產品未啟動	在更新設定中已錯誤地輸入授權金鑰。建議您檢查驗證資料。[**進階設定**] (**F5**) 包含其他的更新選項。從主要功能表按一下 [**說明及支援**] > [管理授權] 以輸入新的授權金鑰。
下載更新檔案時發生錯誤	這可能是因為網際網路連線設定發生問題。建議您檢查網際網路連線（透過在 Web 瀏覽器中開啟任何網站）。如果網站未開啟，可能是尚未建立網際網路連線，或是電腦連線有問題。請與「網際網路服務提供者(ISP)確認是否有可使用的網際網路連線。
模組更新失敗 錯誤 0073	按一下 [**更新**] > [**檢查更新**]，如需相關資訊，請造訪此知識庫文章

注意
各種更新設定檔的 Proxy 伺服器選項可能不同。如果是這種情況，請在 [**進階設定**] (**F5**) 中按一下 [**更新**] > [設定檔]

設定

[設定] 功能表視窗包含下列區段：

- 伺服器
- 電腦
- 網路
- Web 和電子郵件
- 工具 – 診斷記錄



若要暫時停用個別模組，請按一下適用模組旁的綠色滑桿  。這會降低電腦的防護層級。

若要將停用的安全性元件防護重新啟用，按一下適用模組旁的紅色滑桿  ，便可將元件返回啟用狀態。

若要存取特定安全元件的詳細設定，請按一下齒輪圖示 

匯入/匯出設定

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。

[進階設定]

根據自身需求配置進階設定和選項。若要從程式的任意處存取 **[進階設定]** 畫面，按下 **F5**。

伺服器

您將可看見元件清單，可使用滑桿  來啟用/停用。若要配置特定項目的設定，請按一下齒輪圖示  。

自動排除

可識別重要的伺服器應用程式及伺服器作業系統檔案，並自動將這些新增至排除清單中。此功能會將潛在衝突的風險降至最低，並提升執行威脅偵測軟體時的伺服器整體效能。

叢集

配置及啟動 ESET 叢集。

OneDrive 掃描設定

您可以從 Microsoft OneDrive 註冊或取消註冊 ESET OneDrive 掃描器應用程式。

若要暫時停用個別模組，請按一下適用模組旁的綠色滑桿  。這會降低電腦的防護層級。

若要將停用的安全性元件防護重新啟用，按一下適用模組旁的紅色滑桿  ，便可將元件返回啟用狀態。

若要存取特定安全元件的詳細設定，請按一下齒輪圖示 

匯入/匯出設定

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。

[進階設定]

根據自身需求配置進階設定和選項。若要從程式的任意處存取 **[進階設定]** 畫面，按下 **F5**。

電腦

ESET File Security 包含所有必要的元件，以確保與電腦相同層級的重要防護。此模組可讓您啟用/停用並配置下列元件：

即時檔案系統防護

開啟、建立或是在電腦上執行所有檔案時，會掃描檔案是否有惡意軟體。如需［即時檔案系統防護］，也可使用**［配置］**或**［編輯排除］**，這將可開啟［排除］設定視窗，讓您從掃描中排除檔案及資料夾。

裝置控制

此模組可讓您掃描、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。

主機入侵預防系統 (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
- 惡意探索封鎖程式
- 勒索軟體保護

簡報模式

一項專為要求可不間斷地使用軟體、不想受到快顯視窗打擾，而且想要將 CPU 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。

暫停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］**。

若要暫時停用個別模組，請按一下適用模組旁的綠色滑桿 。這會降低電腦的防護層級。

若要將停用的安全性元件防護重新啟用，按一下適用模組旁的紅色滑桿 ，便可將元件返回啟用狀態。

若要存取特定安全元件的詳細設定，請按一下齒輪圖示 。

匯入/匯出設定

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。

［進階設定］

根據自身需求配置進階設定和選項。若要從程式的任意處存取**［進階設定］**畫面，按下 **F5**。

網路

這可根據您的過濾規則，藉由允許或拒絕個別網路連線而完成此作業。其可抵禦遠端電腦的攻擊並封鎖一些可能的危險服務。

［網路］模組可讓您啟用/停用並配置下列元件：

網路攻擊防護 (IDS)

分析網路流量的內容並防止來自網路的攻擊。被視為有害的流量會遭到封鎖。

殭屍網路防護

偵測並封鎖殭屍網路通訊。快速且準確地識別系統中的惡意軟體。

暫時性 IP 位址黑名單（封鎖的位址）

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

疑難排解精靈（最近封鎖的應用程式或裝置）

協助您解決網路攻擊防護導致的連線問題。

若要暫時停用個別模組，請按一下適用模組旁的綠色滑桿 。這會降低電腦的防護層級。

若要將停用的安全性元件防護重新啟用，按一下適用模組旁的紅色滑桿，便可將元件返回啟用狀態。

若要存取特定安全元件的詳細設定，請按一下齒輪圖示

匯入/匯出設定

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。

[進階設定]

根據自身需求配置進階設定和選項。若要從程式的任意處存取 **[進階設定]** 畫面，按下 **F5**。

網路疑難排解精靈

疑難排解精靈會監視所有封鎖的連線，而且會引導您進行疑難排解程序以更正特定應用程式或裝置的網路攻擊防護問題。接下來，精靈會建議您一組新規則，如果您核准便會套用這些規則。

Web 和電子郵件

Web 和電子郵件可讓您啟用/停用並配置下列元件：

Web 存取防護

如果啟用，則會掃描 HTTP 或 HTTPS 所有流量以尋找惡意軟體。

電子郵件用戶端防護

可監視透過 POP3 和 IMAP 通訊協定收到的通訊。

網路釣魚防護

保護您免受攻擊者透過非法網站偽裝成合法網站來取得您的密碼、銀行資料和其他敏感資料。

若要暫時停用個別模組，請按一下適用模組旁的綠色滑桿 。這會降低電腦的防護層級。

若要將停用的安全性元件防護重新啟用，按一下適用模組旁的紅色滑桿，便可將元件返回啟用狀態。

若要存取特定安全元件的詳細設定，請按一下齒輪圖示

匯入/匯出設定

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。

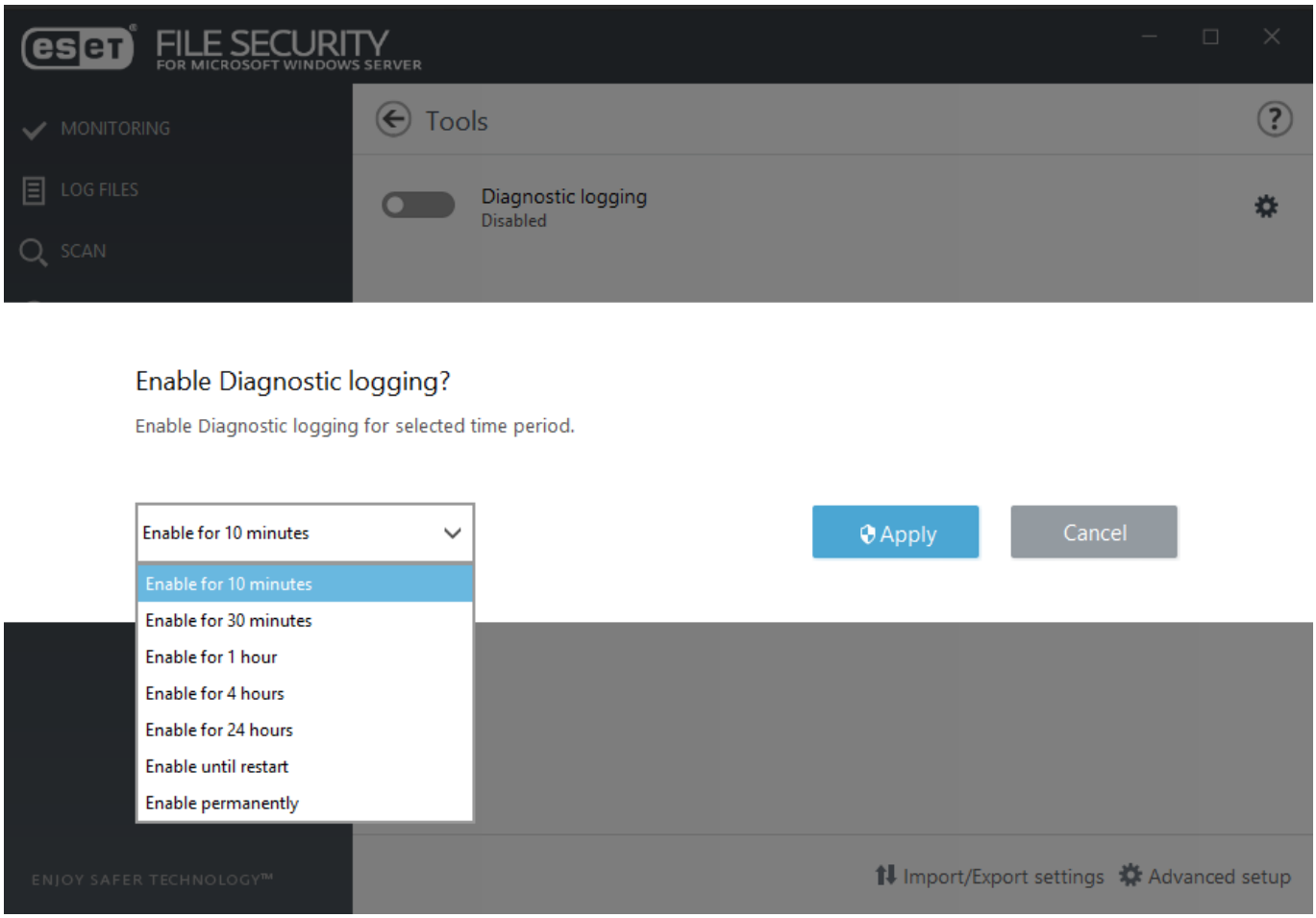
[進階設定]

根據自身需求配置進階設定和選項。若要從程式的任意處存取 **[進階設定]** 畫面，按下 **F5**

工具 – 診斷記錄

如果您需要特定 ESET File Security 功能之行為的相關詳細資訊（例如，疑難排解時），您可以啟用診斷記錄。當您按一下齒輪圖示 ，則可針對哪些功能應配置診斷記錄。

選擇啟用的時間（10 分鐘、30 分鐘、1 小時、4 小時、24 小時，直到下次伺服器重新啟動或永久）。開啟診斷記錄之後ESET File Security 將會依據啟用的功能來收集詳細的防護記錄。



若要暫時停用個別模組，請按一下適用模組旁的綠色滑桿 。這會降低電腦的防護層級。

若要將停用的安全性元件防護重新啟用，按一下適用模組旁的紅色滑桿，便可將元件返回啟用狀態。

若要存取特定安全元件的詳細設定，請按一下齒輪圖示

匯入/匯出設定

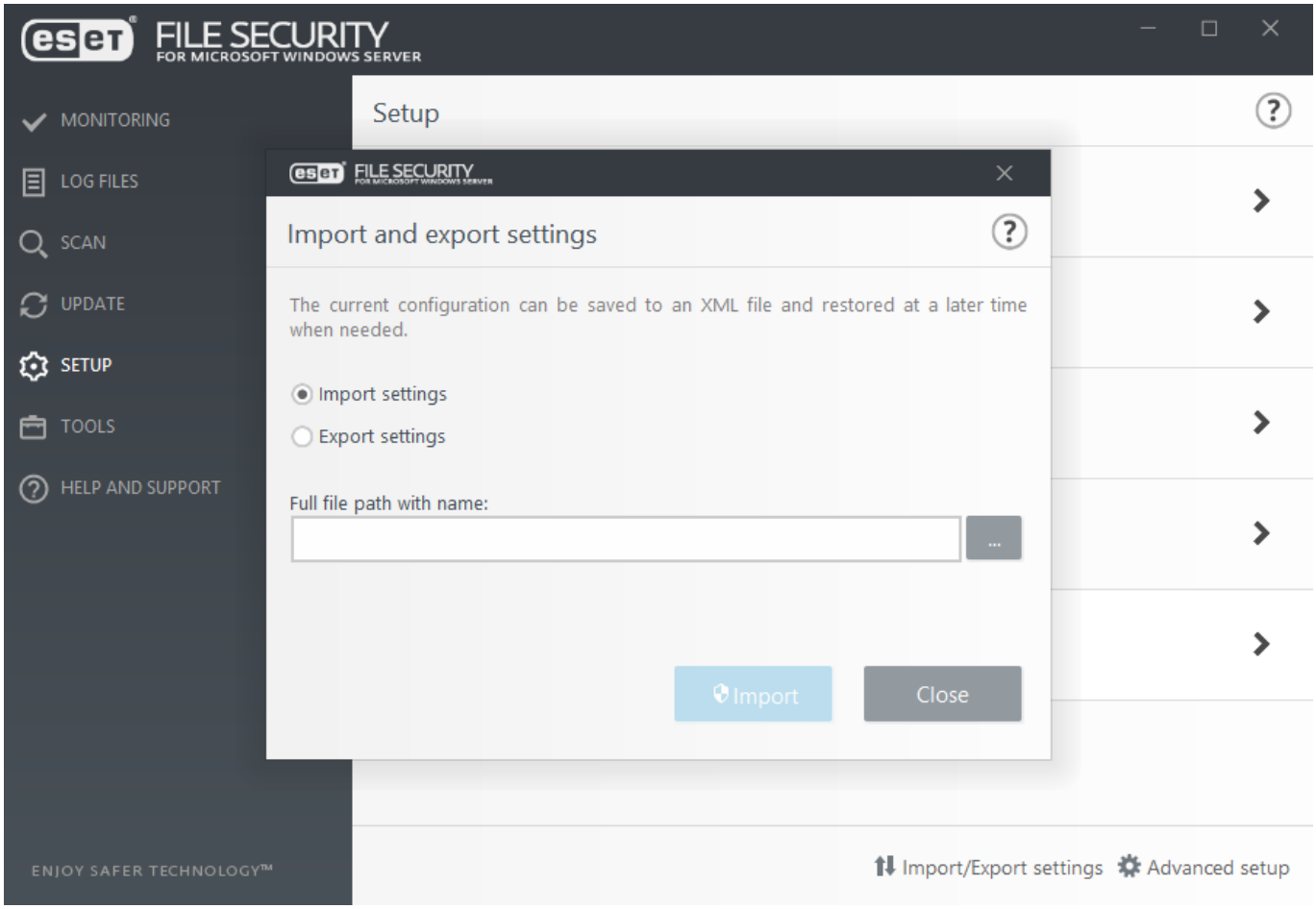
使用 *.xml* 配置檔案載入設定參數，或將目前的設定參數儲存至配置檔案。

[進階設定]

根據自身需求配置進階設定和選項。若要從程式的任意處存取 **[進階設定]** 畫面，按下 **F5**。

匯入及匯出設定

如果您需要備份 ESET File Security 的目前配置，匯入/匯出設定功能非常實用。您也可以利用 ESET File Security 使用匯入功能將相同設定分配/套用至其他伺服器。將設定匯出至 *.xml* 檔案。



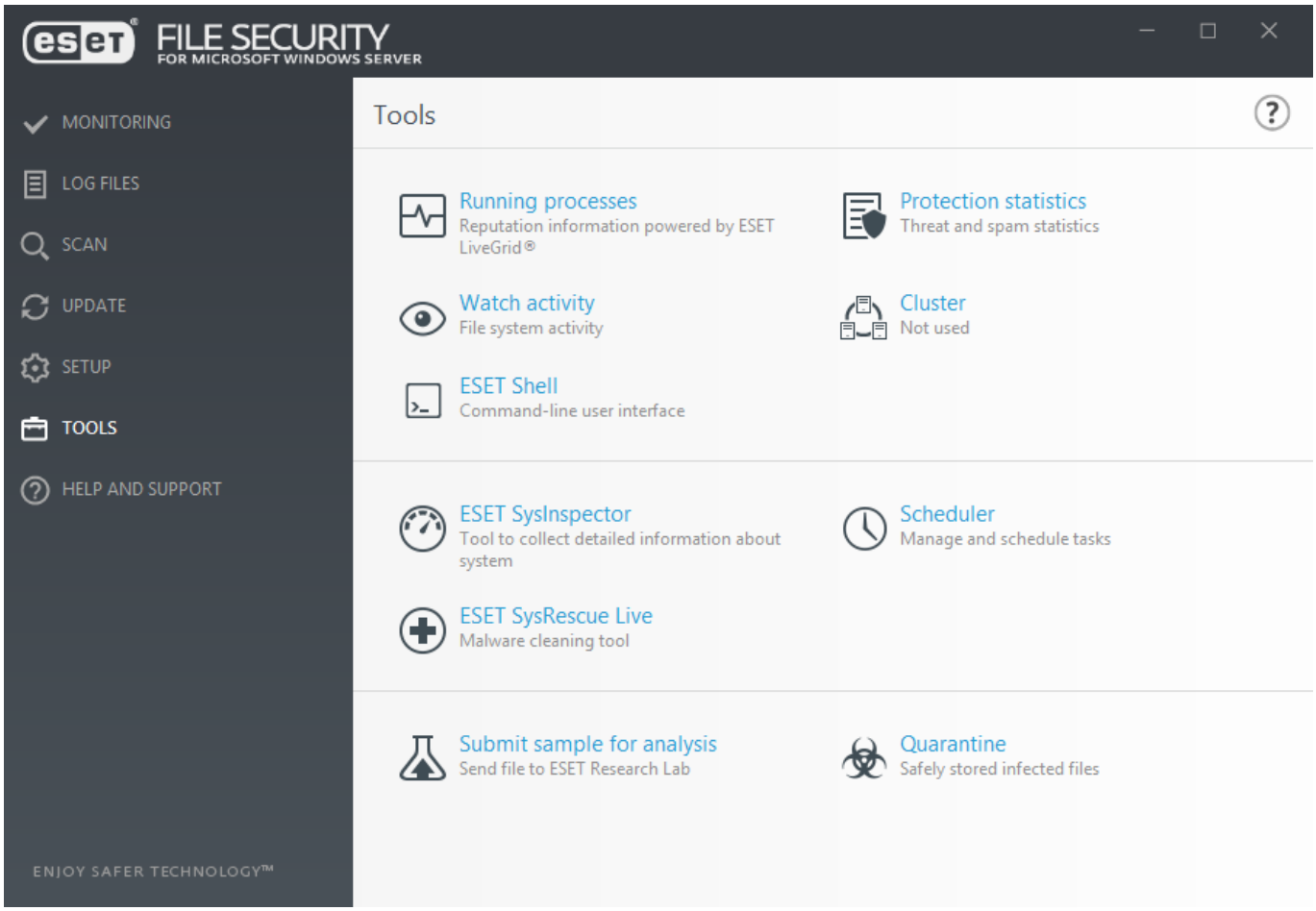
注意
如果您沒有權限將匯出檔案寫入指定目錄，則可能會在匯出設定時遭遇錯誤。

工具

下列功能適用於 ESET File Security 管理：

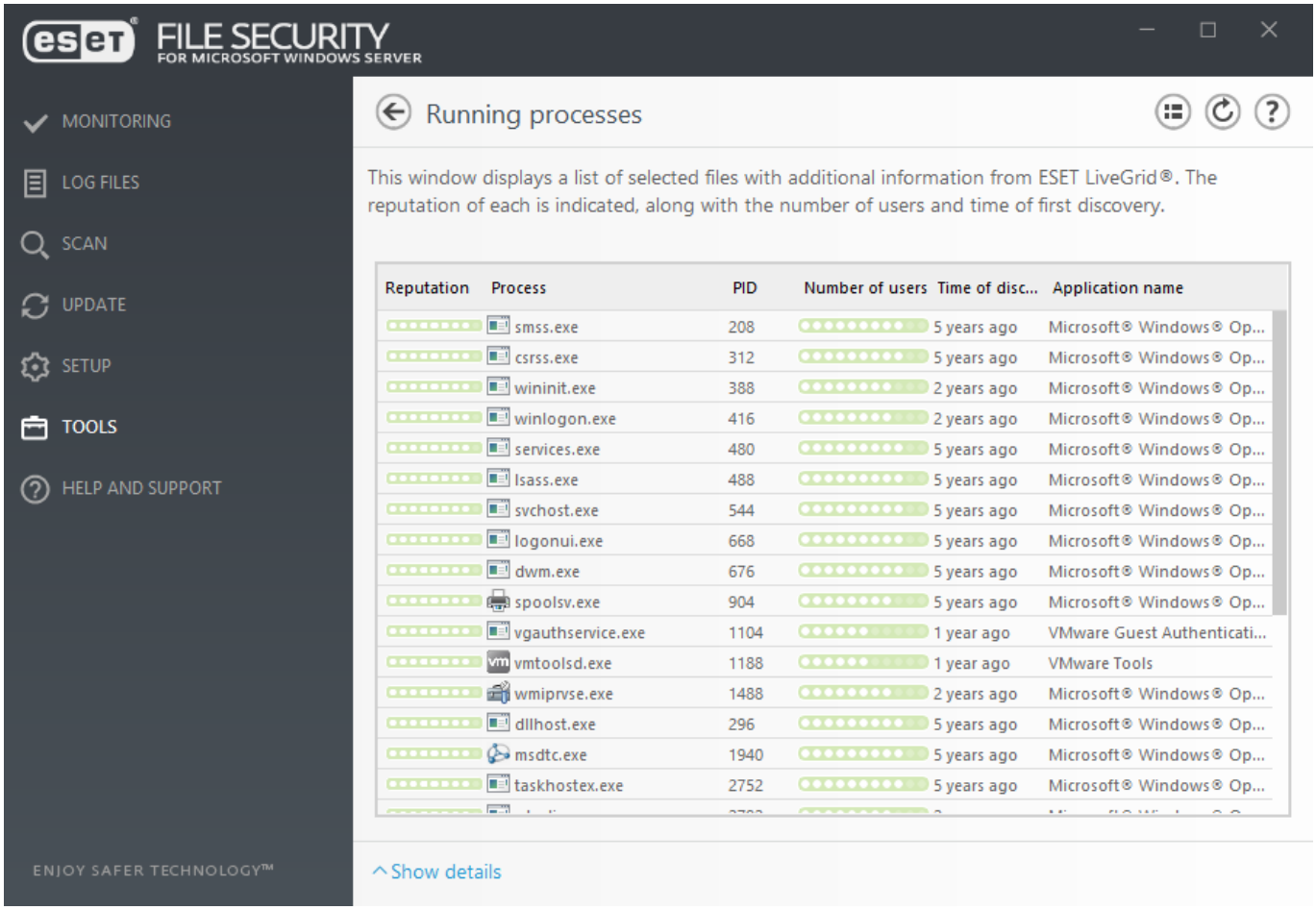
- 執行中的處理程序
- 即時監控
- 防護統計
- 叢集
- ESET Shell

- ESET Dynamic Threat Defense
- ESET SysInspector
- ESET SysRescue Live
- 排程器
- 提交樣本以供分析
- 隔離區



執行中的處理程序

執行中處理程序會顯示電腦上執行的程式或處理程序，確保迅速持續地通知 ESET 新入侵的相關資訊。ESET File Security 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。



注意
標示為最佳聲譽（綠色）的已知應用程式是無病毒的（白名單），且將排除在掃瞄名單之外，如此可以改善電腦上指定電腦掃描或即時檔案系統防護的速度。

聲譽	**在大部分情況下，ESET File Security 和 ESET LiveGrid® 技術會使用一系列的啟發式規則（檢查每個物件（檔案、處理程序、登錄機碼等）的特性，然後衡量惡意活動潛在的可能性。根據這些啟發式規則，將從 9 – 最佳聲譽（綠色）至 0 – 最差聲譽（紅色）的聲譽層級指派給物件。**
處理	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
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。
應用程式名稱	此程序所屬的程式指定名稱。

注意
應用程式被標示為不明（橙色）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，可以使用提交樣本以供分析功能來傳送檔案至 ESET 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病毒資料庫更新。

顯示詳情

視窗底部會出現以下資訊：

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

新增至程序排除

在［執行程序］視窗中的程序按一下滑鼠郵件，將之從掃描範圍中排除。其路徑將會新增至程序排除清單中。

即時監控

若要監看活動，在圖表格式中包含活動，然後在活動之後從下拉式功能表選取：

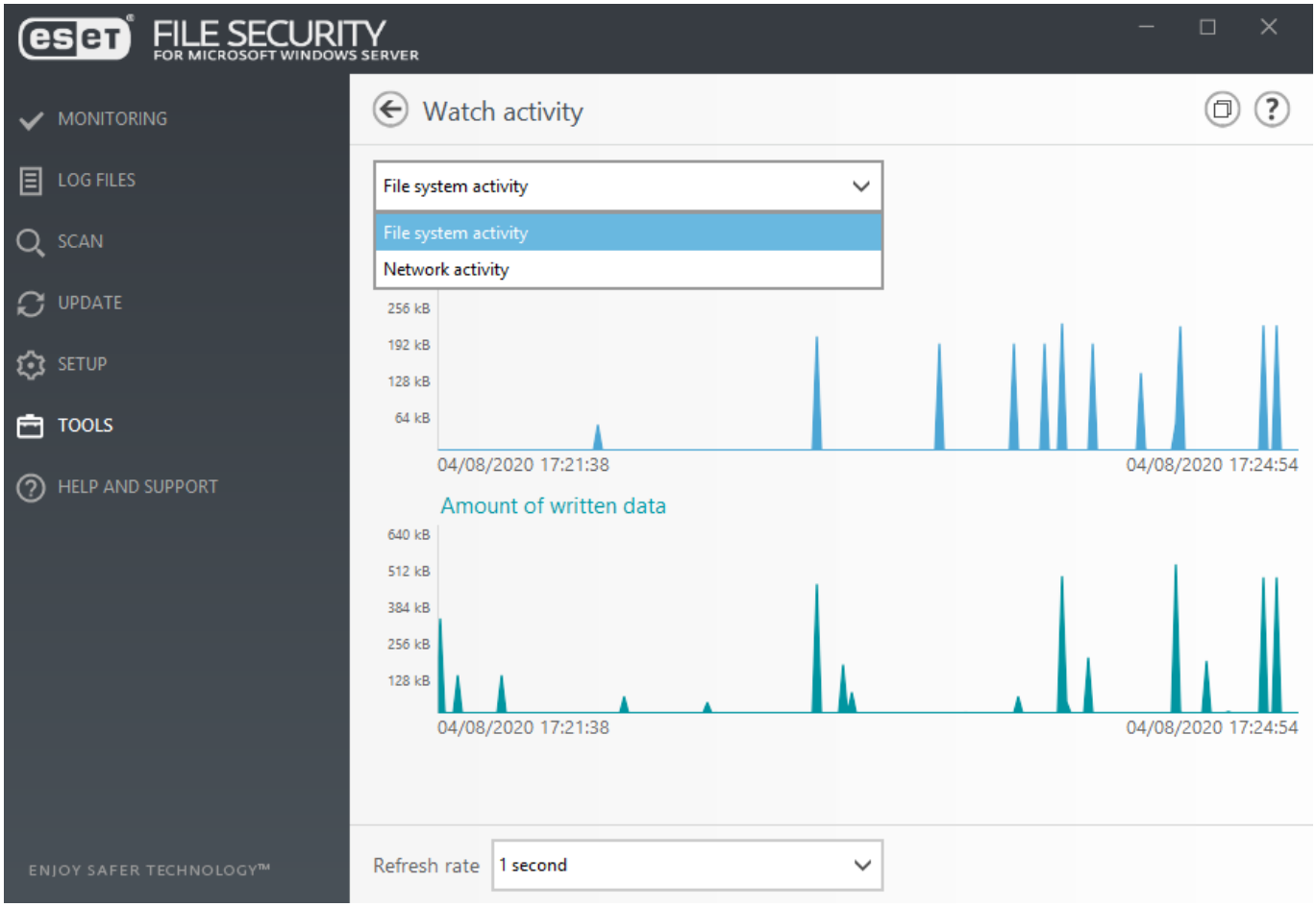
檔案系統活動

讀取或寫入的資料量。圖表的垂直軸代表讀取的資料（藍）及寫入的資料（綠）。

網路活動

接收或傳送的資料量。圖表的垂直軸代表接收的資料（藍）及傳送的資料（綠）。

在圖表的底端，是根據選取之時間範圍即時記錄「檔案系統活動」的時間表。使用**［重新整理率］**下拉式功能表以改變更新頻率。

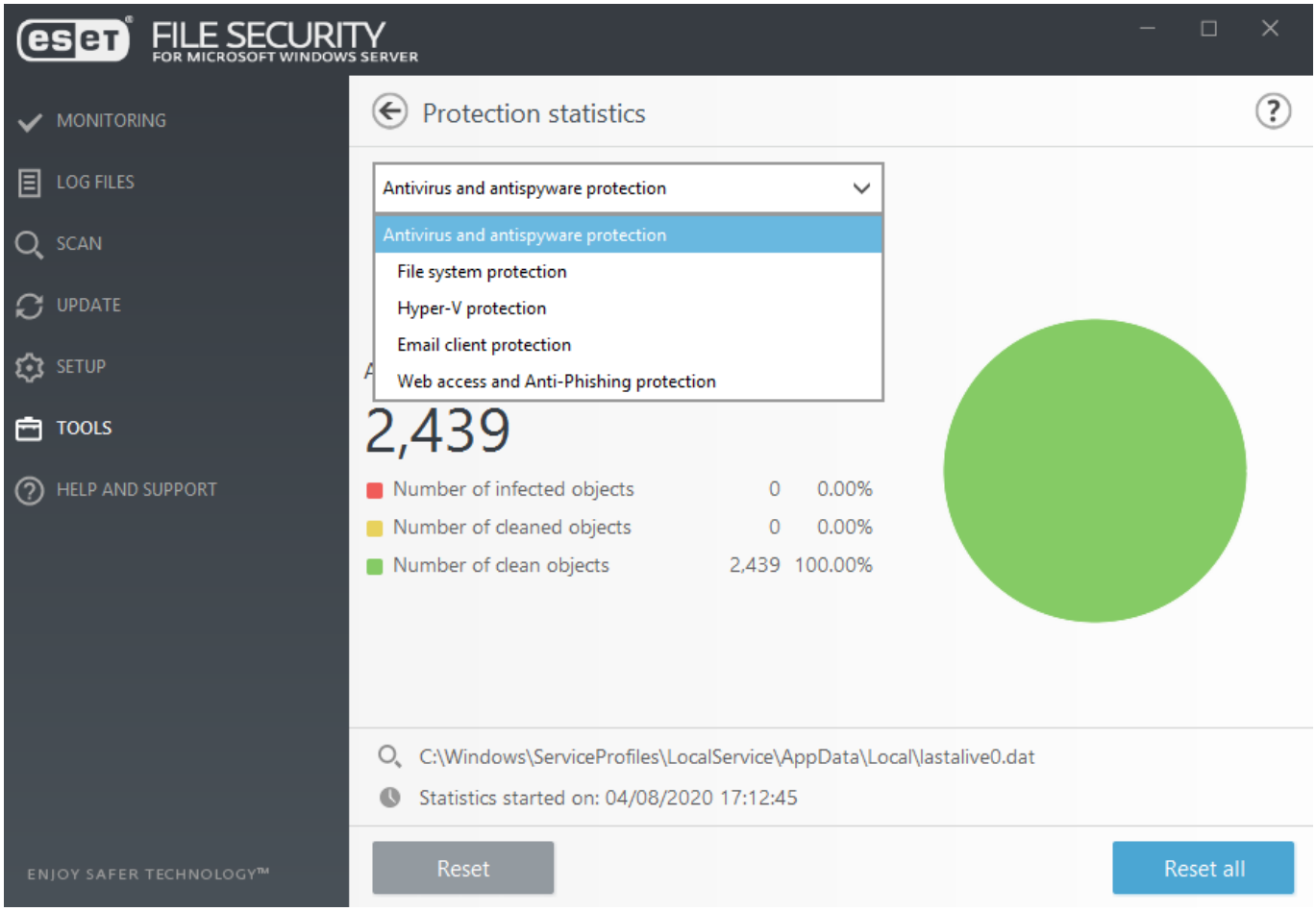


可用選項如下：

1 秒	**圖表每秒鐘都會重新整理，且時間表包含最近 10 分鐘。**
1 分鐘（最近 24 小時）	圖表每分鐘都會重新整理，且時間表包含最近 24 小時。
1 小時（最近一個月）	圖表每小時都會重新整理，且時間表包含最近一個月。
1 小時（選取的月份）	圖表每小時都會重新整理，且時間表包含選取的月份。從下拉式功能表選取月份（及年度）以檢視活動。按一下 **[變更]**。

防護統計

若要檢視與 ESET File Security 防護模組相關的統計資料，從下拉式功能表選取適用的防護模組。統計資料包含所有已掃描物件的數目、受感染的物件數目、已清除的物件數目，以及不含病毒物件的數目。將滑鼠停留在圖形旁邊，圖形中便只會顯示特定物件的資料。若要清除目前防護模組的統計資料資訊，按一下 **[重設]**。若要清除所有模組的資料，按一下 **[全部重設]**。



下列為 ESET File Security 中的可用統計圖表：

病毒及間諜程式防護

顯示受感染及已清除物件的總數。

檔案系統防護

僅顯示已讀取或寫入檔案系統的物件。

Hyper-V 防護

顯示受感染、已清除及不含病毒物件的總數（僅限於具有 Hyper-V 的系統）。

電子郵件用戶端防護

僅顯示電子郵件用戶端傳送或接收的物件。

Web 存取及網路釣魚防護

僅顯示 Web 瀏覽器下載的物件。

叢集

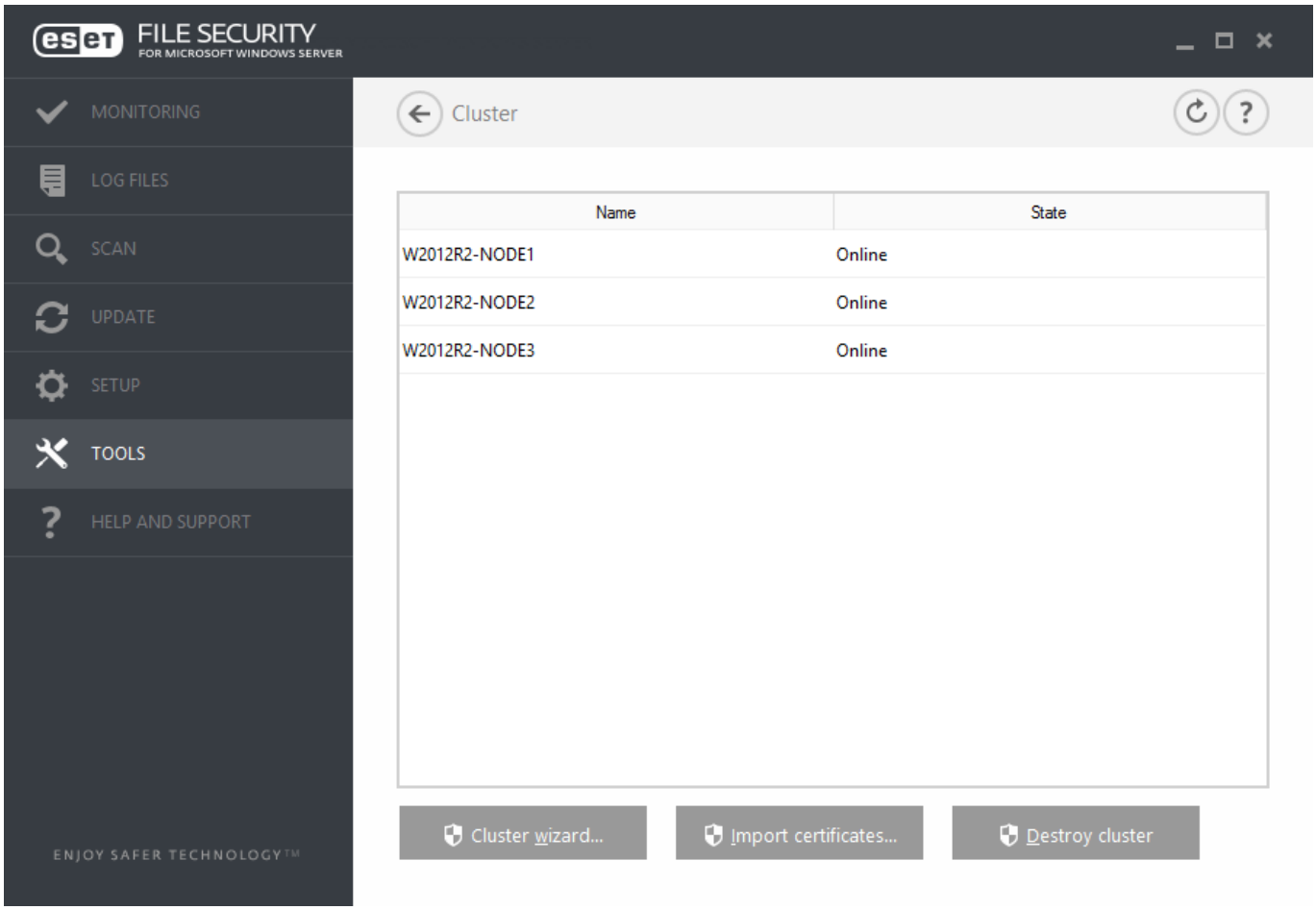
ESET 叢集 是 ESET 產品系列中適用於 Microsoft Windows Server 的 P2P 通訊基礎架構。

本基礎架構可讓 ESET 伺服器產品彼此互相通訊以及交換資料，例如配置和通知，而且可以 ，以及同步化

產品執行個體群組中正確作業所需的資料。這類群組的範例為Windows 容錯移轉叢集」或「網路負載平衡 (NLB) 叢集」中的節點群組，其包含已安裝的 ESET 產品，且整個叢集需要相同的產品配置ESET 叢集」能確保執行個體間的一致性。

注意
使用者介面設定並未在ESET 叢集」節點之間同步化。

您能夠從主要功能表內的 [工具] > [叢集] 來存取ESET 叢集」狀態頁面，正確配置後，狀態頁面應看起來像這樣：



注意
不支援在 ESET File Security 和 ESET File Security (適用於 Linux) 之間建立ESET 叢集」。

當設定ESET 叢集」時，有兩種方法可以新增節點：

自動偵測

如果您有現有的 Windows 容錯移轉叢集/NLB 叢集，自動偵測便會自動將其成員新增到 ESET 叢集。

瀏覽

您可以輸入伺服器名稱來手動新增節點（可以是相同「工作群組」或相同「網域」的成員）。

注意
伺服器不 一定要是Windows 容錯移轉叢集/NLB 叢集」的成員，才能使用 ESET 叢集功能。即使環境中沒有Windows 容錯移轉叢集/NLB 叢集」，您也可以使用ESET 叢集」。

新增節點至「ESET 叢集」後，下一個步驟是在各節點上安裝 ESET File Security。這在「ESET 叢集」設定期間將會自動完成。在其他叢集節點上遠端安裝 ESET File Security 所需要的憑證：

網域情況

網域管理員憑證。

工作群組情況

您需要確認所有節點使用相同的本機管理員帳戶憑證。

在「ESET 叢集」中，您也可以使用自動新增的節點組合作為現有「Windows 容錯移轉叢集 / NLB 叢集」的成員並手動新增節點（在相同「網域」時提供）。

> 重要
> 您無法將「網域」節點與「工作群組」節點結合。

使用「ESET 叢集」的另一個要求是必須在推送 ESET File Security 至「ESET 叢集」節點前，在「Windows 防火牆」啟用 **[檔案及印表機共用]**。

您可以執行叢集精靈隨時將節點新增至現有的「ESET 叢集」。

匯入憑證

使用 HTTPS 時，會使用憑證以提供堅實的機器對機器驗證。每個 ESET 叢集都有獨立的憑證階層。階層有一個根目錄憑證和一組由根目錄憑證簽署的節點憑證。建立所有節點憑證之後，便會銷毀根目錄憑證的私人金鑰。將新節點新增到叢集時，便會建立新的憑證階層。請瀏覽至包含憑證的資料夾（會在叢集精靈期間產生）。選取該憑證檔案並按一下 **[開啟]**。

銷毀叢集

可移除「ESET 叢集」。每個節點將會在事件防護記錄寫入關於銷毀「ESET 叢集」的記錄。完成之後，系統會從「Windows 防火牆」移除所有 ESET 防火牆規則。先前的節點會回復到原本的狀態，必要時可以在其他「ESET 叢集」再次使用。

叢集精靈 – 選取節點

設定「ESET 叢集」的第一個步驟為新增節點。您可以使用 **[自動偵測]** 選項或 **[瀏覽...]** 來新增節點。或者，您可以在文字方塊輸入伺服器名稱然後按一下 **[新增]**。

自動偵測

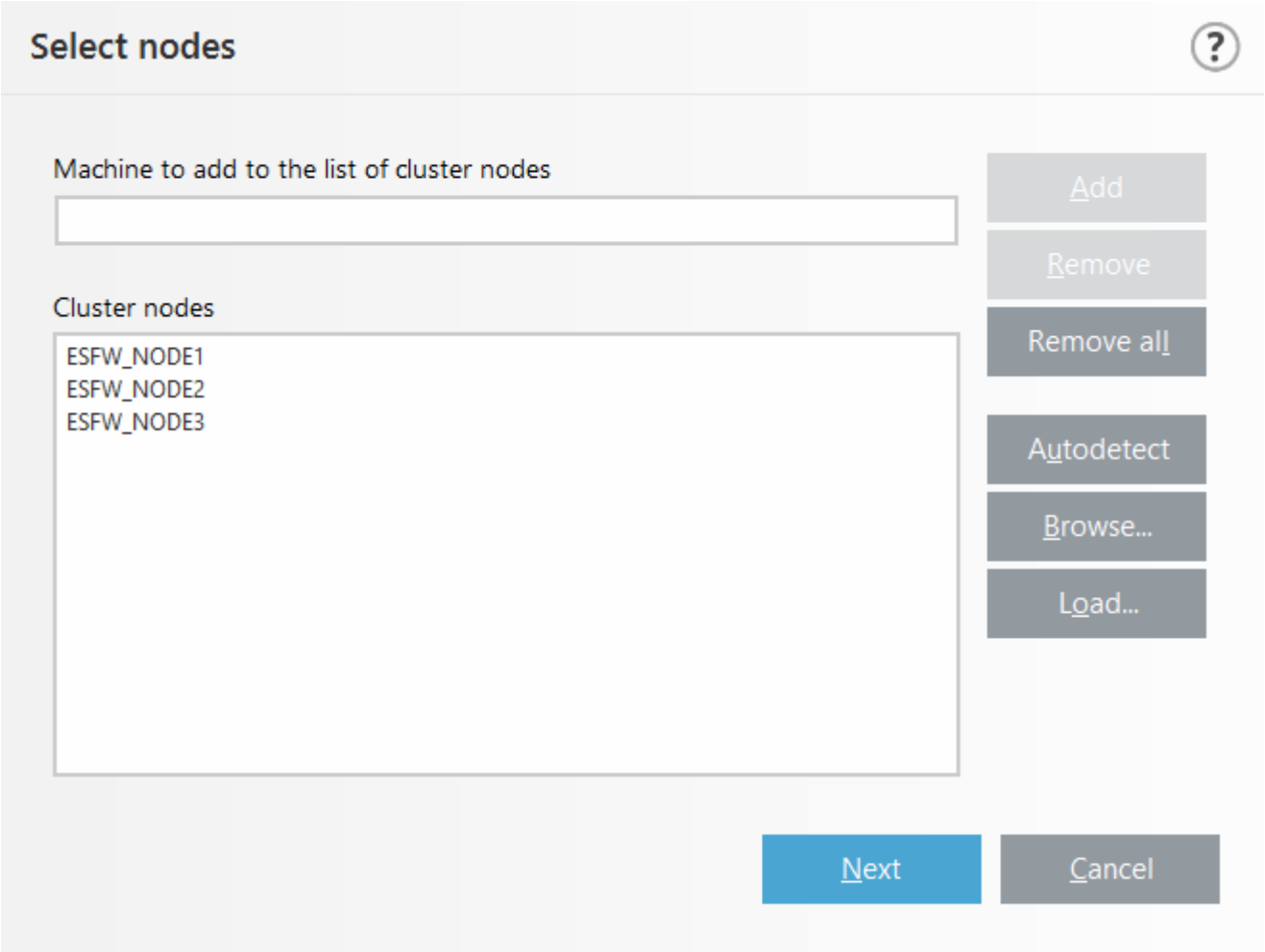
會自動從現有「Windows 容錯移轉叢集 / 網路負載平衡(NLB) 叢集」新增節點。您用來建立「ESET 叢集」的伺服器需為此「Windows 容錯移轉叢集 / NLB 叢集」的成員才能自動新增節點。「NLB 叢集」必須針對「ESET 叢集」在叢集屬性中啟用 **[允許遠端控制]** 功能才能正確偵測節點。一旦您有了新的新增節點清單，您可以移除不需要的節點。

瀏覽

可在「網域」或「工作群組」中尋找和選取電腦。此方法可手動新增節點至「ESET 叢集」。另一個新增節點的方法為輸入您所要新增伺服器的主機名稱，然後按一下 **[新增]**。

載入

從檔案匯入節點清單。



若要修改清單中的 **[叢集節點]**，請選取您想要移除的節點然後按一下 **[移除]**，或按一下**[全部移除]** 來完全清除清單。

如果您已具備現有的「ESET 叢集」，您可以隨時新增節點。步驟與上述內容相同。

> 注意
> 所有保留在清單的節點必須為上線狀態並且可以連線「Localhost 依預設已新增至「叢集」節點。

叢集精靈 – 叢集設定

定義叢集名稱及特定網路（如有需要）。

叢集名稱

輸入叢集名稱，並按一下 **[下一步]**「

監聽 連接埠 –（預設連接埠為 9777）

如果您已經在網路環境中使用連接埠 9777，請指定尚未使用的其他連接埠號。

在 Windows 防火牆中開啟連接埠

選取時會在 Windows 防火牆中建立規則。

叢集精靈 – 叢集安裝設定

定義憑證發送模式和是否要在其他節點上安裝產品。

憑證發送

- **自動** 遠端 – 將自動安裝憑證。
- **手動** – 按一下 **[產生]** 並選取要儲存憑證的適當資料夾。其中包括已建立的「系統管理員」憑證和每個節點的憑證，包括您設定「ESET 叢集」的本機。若要註冊本機上的憑證，按一下 **[是]**。

安裝至其他節點的產品

- **自動遠端** - ESET File Security 將會在每個節點上自動安裝（作業系統為相同架構時才提供）。
- **手動** – 手動安裝 ESET File Security (例如，您在某些節點上有不同的 OS 架構時)。

將授權推送到節點，但不啟動產品

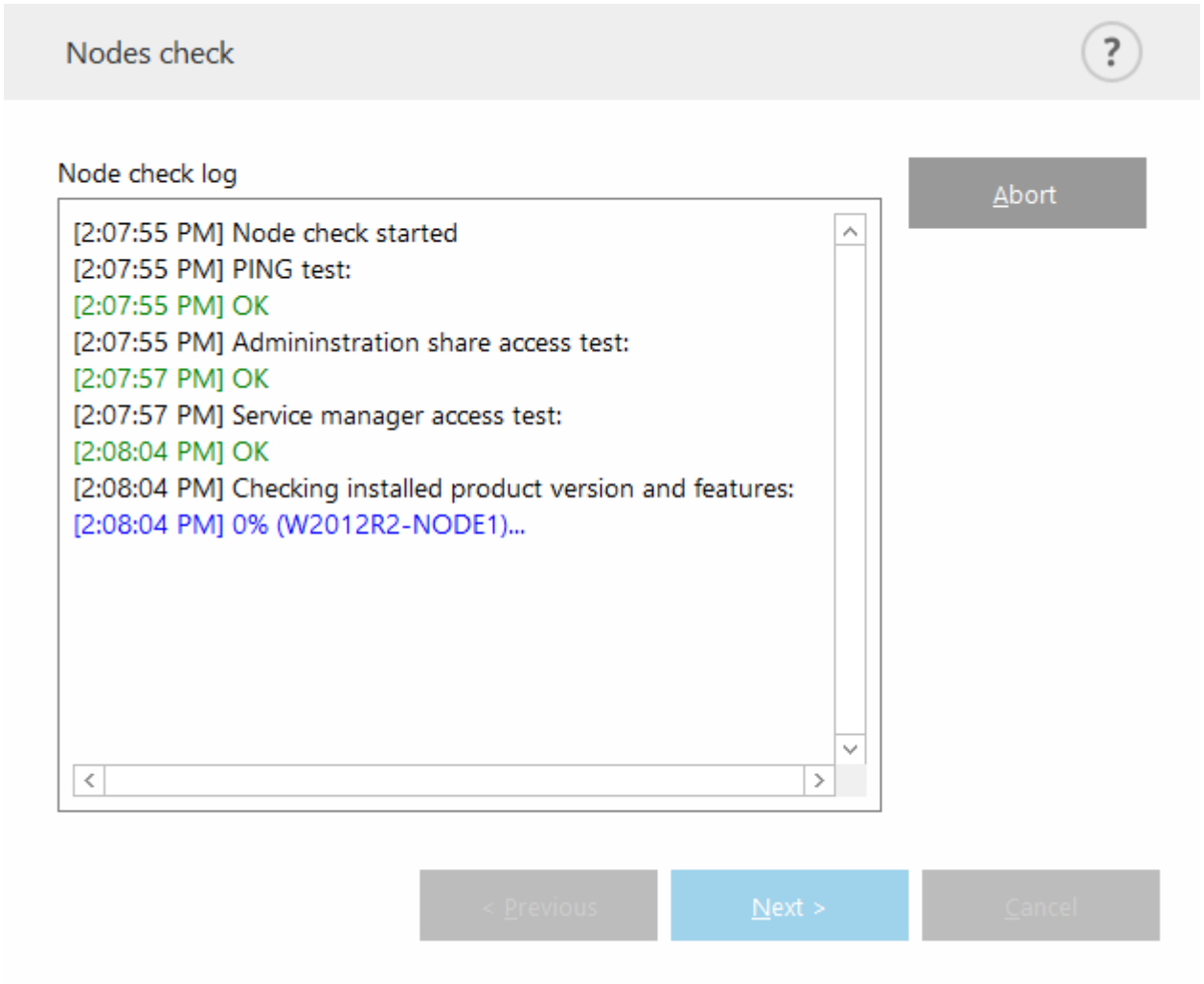
ESET Security 會自動啟動安裝在節點上的 ESET 解決方案，而不需要授權。

> 注意
> 若要使用混合的作業系統架構（32 位元和 64 位元）建立「ESET 叢集」，請手動 ESET File Security 下一個步驟時將會偵測使用中的作業系統，您將在防護記錄視窗看到此資訊。

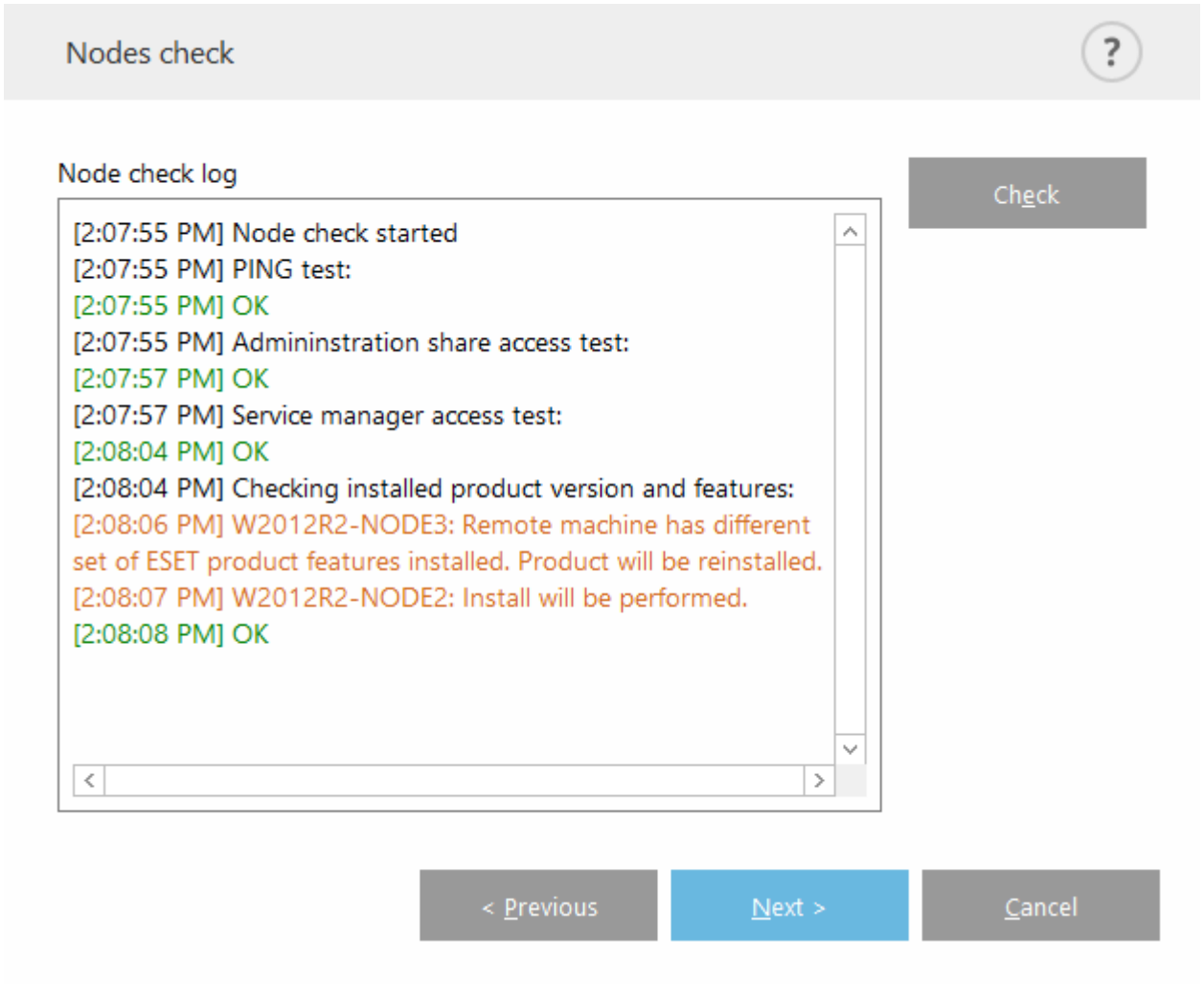
叢集精靈 – 節點檢查

指定安裝詳情後會執行節點檢查。下列資訊會顯示在 **[節點檢查記錄]**。

- 確認是否所有的現有節點皆為上線狀態
- 確認是否可存取新的節點
- 節點為上線狀態
- 可存取管理共用
- 可遠端執行
- 已安裝產品的正 確版本（或未安裝產品）
- 確認是否存在新的憑證

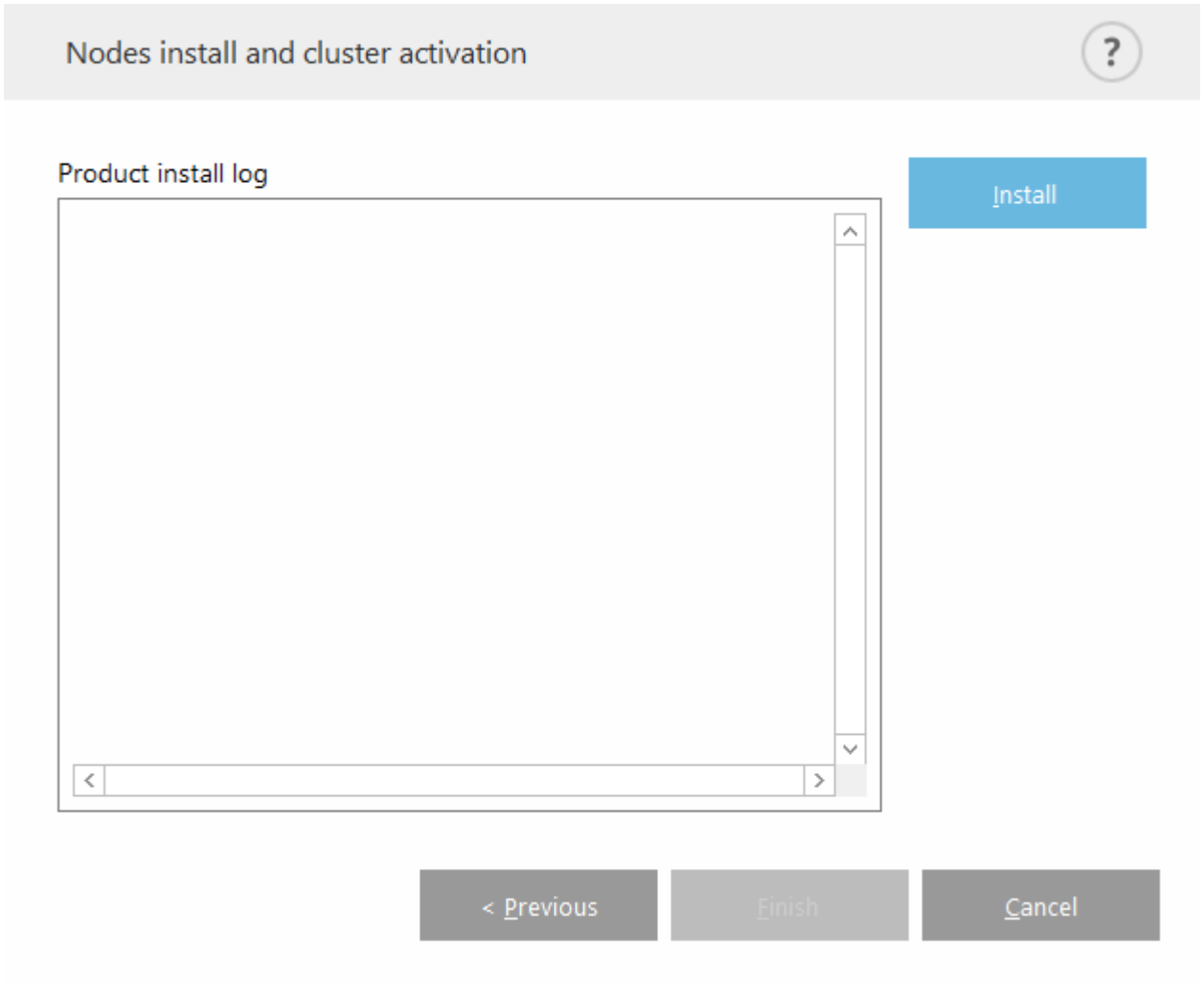


節點檢查完成後您將會看到報告：

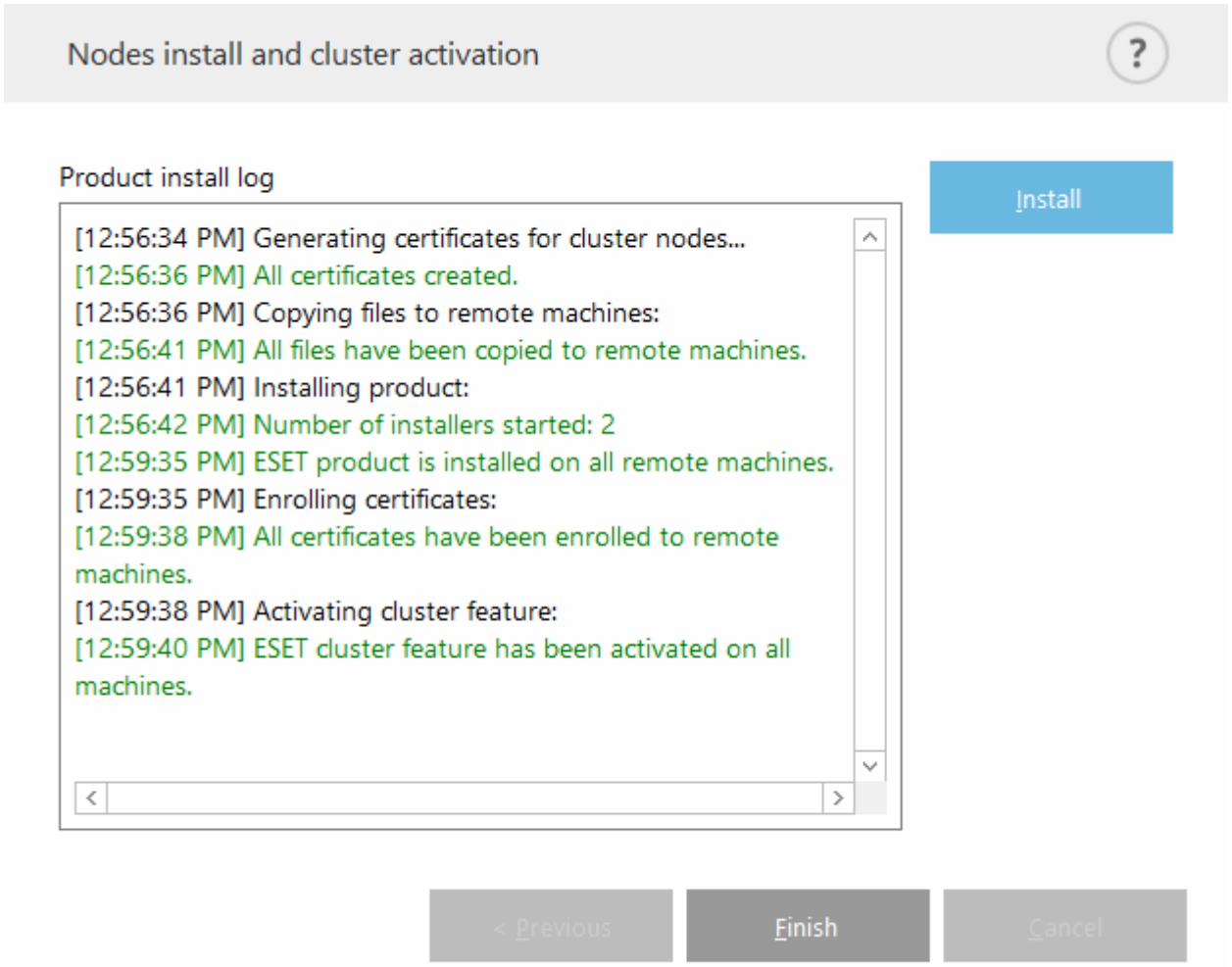


叢集精靈 – 節點安裝

當「ESET 叢集」初始化期間必須在遠端機器上安裝產品時，精靈會在目錄 *%ProgramData%\ESET\ESET Security\Installer* 中嘗試尋找安裝程式。如果找不到安裝程式套件，系統會要求您尋找安裝程式套件。

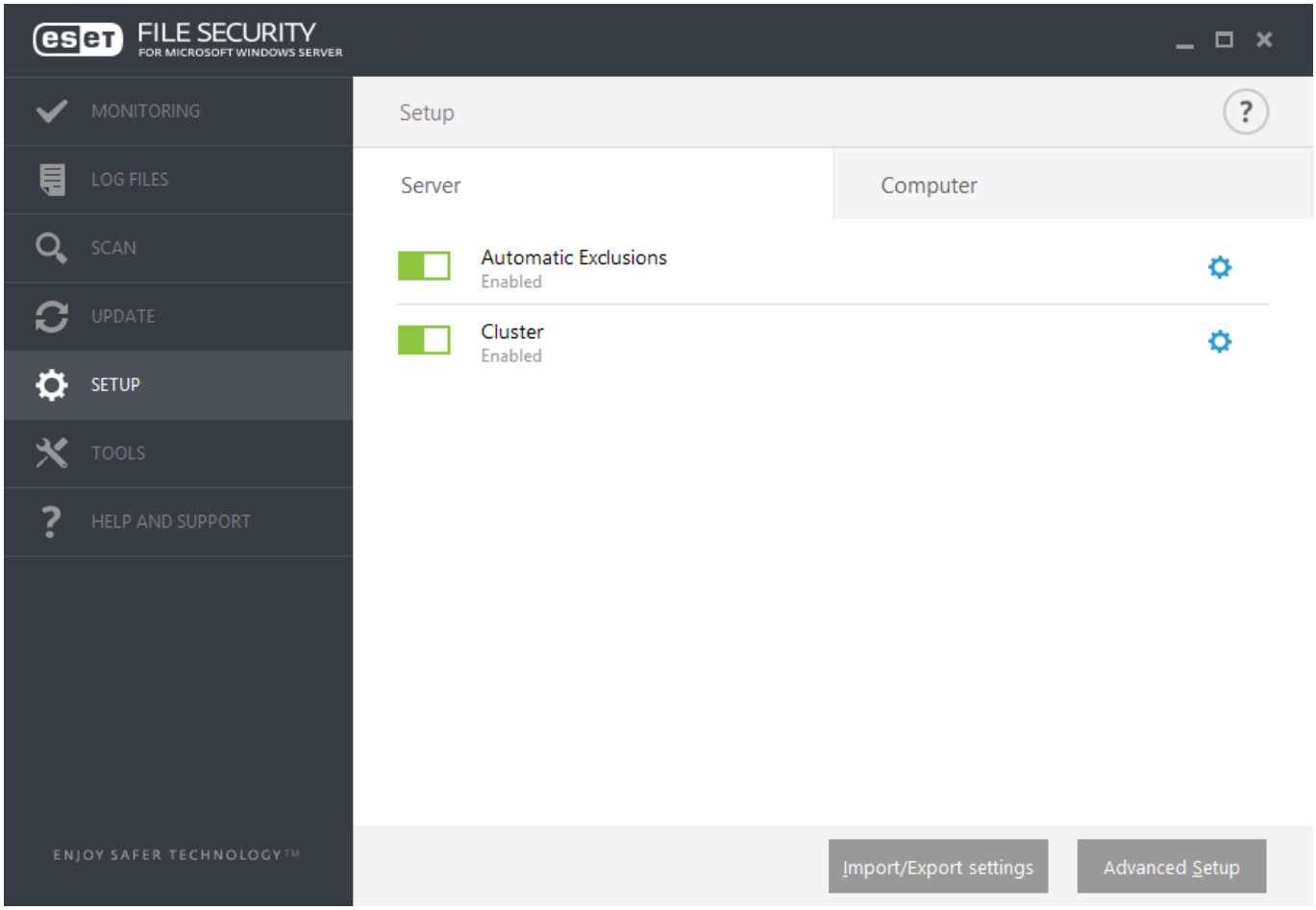


注意
使用不同的架構（32 位元與 64 位元）嘗試使用節點的自動遠端安裝時，系統會進行偵測並提示執行手動安裝。



您正確配置ESET 叢集」後ESET 叢集」將會在 **[設定] > [伺服器]** 頁面中顯示啟用。

注意
如某些節點已安裝較舊版的 ESET File Security系統會通知您需要在這些電腦上安裝最新版本。更新 ESET File Security 可能會造成自動重新啟動。



此外，您同時可以從「叢集」狀態頁面檢查其目前狀態（**[工具] > [叢集]**）。

ESET Shell

eShell (ESET Shell 的簡稱）是 ESET File Security 的命令列介面。它是圖形使用者介面 (GUI) 的替代選擇。eShell 包含 GUI 一般提供的所有功能和選項。eShell 可讓您無需使用 GUI 即可配置與管理整個程式。

除了可提供所有 GUI 的功能與特性之外，此介面也可以讓您透過執行腳本，以自動配置、修改配置或執行處理方法。此外，對於偏好使用命令列勝過 GUI 的使用者而言，eShell 也非常實用。

> 注意
> 如需取得完整功能，我們建議您使用以管理員身分執行開啟 eShell。當透過 Windows 命令提示字元 (cmd) 執行單一命令時也適用相同方法。使用 以管理員身分執行開啟提示字元。若無法以管理員身分執行命令提示字元，則會因為缺乏權限而防止您執行命令。

eShell 可在兩種模式下執行：

1. **互動模式** – 當您想要使用 eShell (不只是執行單一命令）進行工作時可使用此模式，例如變更配置、檢視防護記錄等。如果您尚未熟悉所有命令，可以使用互動模式。互動模式可協助您更輕鬆地瀏覽 eShell 的內容。它也會告訴您在特定內容中可使用的命令。

2. **單一命令 / 批次模式** – 如果您只需要執行一個命令而不需要進入 eShell 互動模式，可使用此模式。請從 Windows 命令提示字元輸入 eshell 和適當的參數。

> 範例
> `eshell get status` 或 `eshell computer set real-time status disabled 1h`

有一些設定您必須先配置，才能在批次/腳本模式中執行某些命令（例如上述第二個範例）。否則，您會得到一個**已拒絕存取**訊息。這是基於安全考量。

注意
變更設定需要允許從 Windows 命令提示字元中使用 eShell 命令。如需更多有關執行批次檔案的詳細資訊，請按一下這裡

有兩種方式可以在 eShell 進入互動模式：

1.經由 **Windows開始」功能表**：［開始］>［所有程式] > [ESET] > [ESET File Security] > ESET Shell

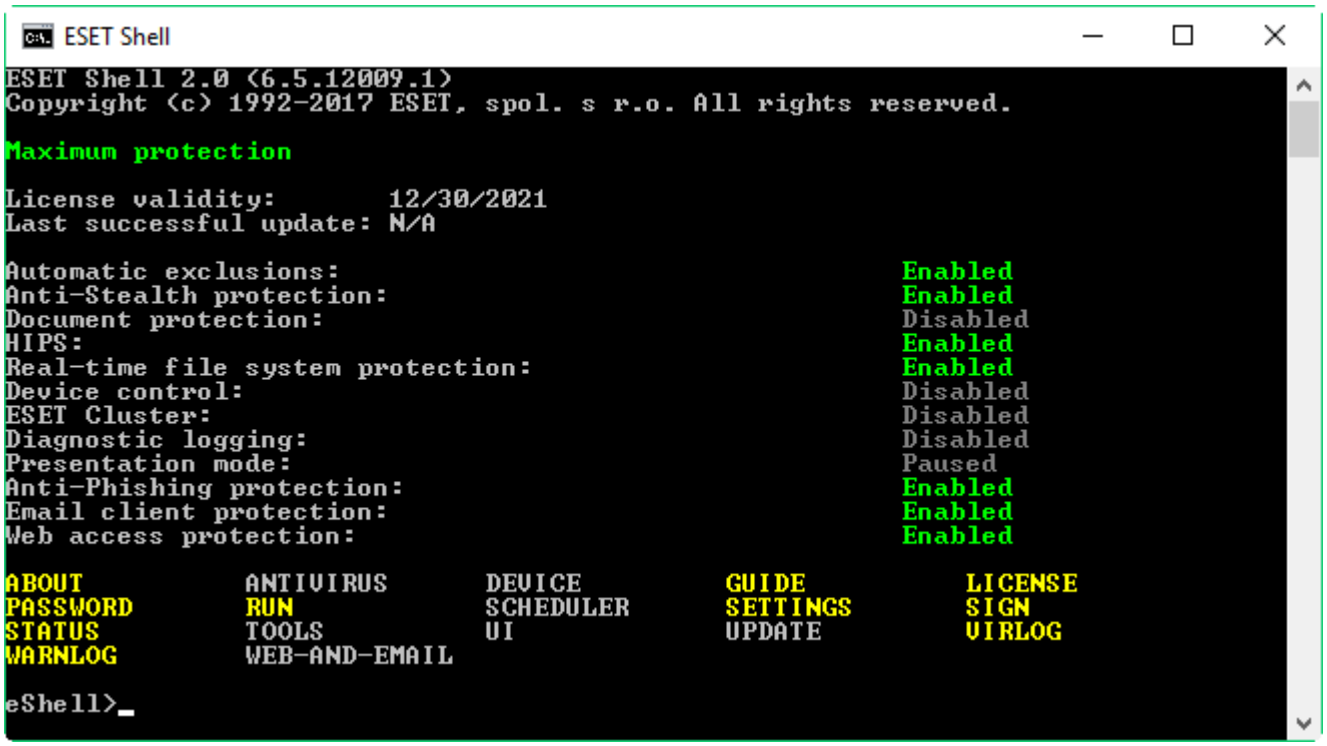
2.從 **Windows 命令提示字元**輸入 `eshell` 並按下 Enter 鍵

重要
如果您遇到錯誤 `'eshell' is not recognized as an internal or external command`，這是因為安裝 ESET File Security 之後，系統未載入新的環境變數。開啟命令提示字元，並嘗試再次啟動 eShell如果您仍遇到錯誤或有 ESET File Security 的核心安裝，請使用絕對路徑啟動 eShell例如 `"%PROGRAMFILES%\ESET\ESET File Security\eShell.exe"`（您必須使用 ″″，命令才能運作）。

當您第一次在互動模式中執行 eShell 時，將顯示初次執行（指導）畫面。

注意
如果您想在之後也顯示初次執行畫面，請輸入 `指南` 命令。此畫面會顯示一些基本範例，告訴您如何搭配語法、前置詞、命令路徑、縮寫形式、別名等方式使用 eShell

下一次您執行 eShell 時，將會看到此畫面：



注意
命令不區分大小寫。無論使用大寫或小寫，都可以執行命令。

自訂 eShell

您可以在 ui eshell 內容中自訂 eShell您可以為指令碼配置別名、顏色、語言、執行原則以隱藏命令和執行其他動作。

使用

語法

指令必須使用正確的語法格式化才能運作，並可由前置詞、內容、引數、選項等組成。這是適用於整個 eShell 的一般語法：

[<prefix>] [<command path>] <command> [<arguments>]

範例（此命令會啟動文件防護）：

```
SET COMPUTER SCANS DOCUMENT REGISTER ENABLED
```

SET – 前置詞
COMPUTER SCANS DOCUMENT – 特定命令的路徑，是此命令所隸屬的內容
REGISTER – 命令本身
ENABLED – 命令的引數

使用 ? 作為命令的引數，將會顯示該特定命令的語法。例如，STATUS ? 將會顯示 STATUS 命令的語法：

語法：

```
[get] status
```

作業：

get – 顯示所有防護模組的狀態

您會發現 [get] 位於中括弧內。這會指定前置詞 get 是 status 命令的預設值。這表示當您執行 status 且未指定任何前置詞時，命令會確實使用預設的前置詞（在此情況為 get status）。使用無前置詞的命令可節省輸入的時間。通常 get 是大部分命令的預設前置詞，但是您必須確定特定命令是使用何種預設前置詞，而且該命令確實是您想要執行的命令。

> 注意
> 命令不區分大小寫，因此無論使用大寫或小寫都可執行命令。

前置詞 / 作業

前置詞是一項作業。GET 前置詞將提供您如何配置 ESET File Security 特定功能的資訊，或顯示狀態（例如 GET COMPUTER REAL-TIME STATUS 會顯示即時模組目前的防護狀態）。SET 前置詞將配置功能或變更其狀態（SET COMPUTER REAL-TIME STATUS ENABLED 會啟動即時防護）。

這些是 eShell 讓您使用的前置詞。命令可能或無法支援所有前置詞：

GET	傳回目前的設定/狀態
SET	設定值/狀態
SELECT	選取項目

GET	傳回目前的設定/狀態
ADD	新增項目
REMOVE	移除項目
CLEAR	移除所有項目/檔案
START	啟用處理方法
STOP	停用處理方法
PAUSE	暫停處理方法
RESUME	繼續使用處理方法
RESTORE	還原預設設定/物件/檔案
SEND	傳送物件/檔案
IMPORT	從檔案匯入
EXPORT	匯出至檔案

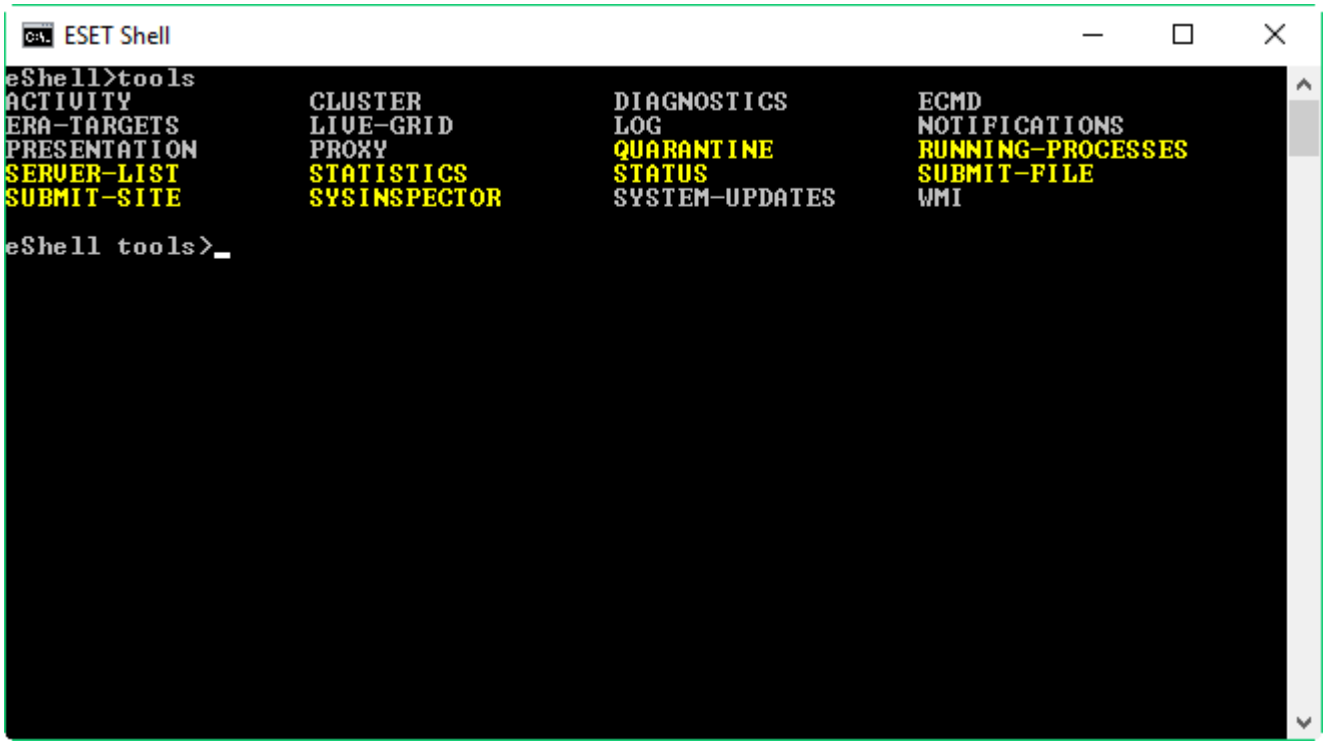
> 注意
> GET 及 SET 等前置詞可與許多命令搭配使用，但是某些命令，（例如 EXIT）並不使用前置詞。

命令路徑 / 內容

命令位於形成樹狀結構的內容中。此樹狀結構的最高層級是根。當您執行 eShell 時，您是位於根層級：

```
eShell>
```

您可以從此處執行命令，或是輸入內容名稱以在樹狀結構內瀏覽。例如，當您輸入 TOOLS 內容時，將會列出從此處可用的所有命令與子內容。



黃色項目是您可以執行的命令，而灰色項目是您可以輸入的子內容。子內容包含更多命令。

如果您需要返回更高層級，請使用 .. (兩個點)。

範例
假設您在此處：
eShell computer real-time>
輸入 .. 以移至更高一個層級到：
eShell computer>

如果您想從 eShell computer real-time> 返回根（此位置比根低兩層級），只需輸入 .. ..（兩個點加上空格，再加上兩個點）。透過執行此動作，您將移至上兩個層級，在此情況為根層級。使用反斜線 \ 可從任何層級直接回到根目錄，無論您在內容樹狀結構內的深度為何。如果您想要到上層的特定內容，只要視需要使用適當數量的 .. 指令以到達所需的層級，使用空格分隔。例如，如果您想要到達上三層，請使用 .. .. ..

路徑與目前的內容相關。如果命令包含在現有內容，請不要輸入路徑。例如，若要執行 GET COMPUTER REAL-TIME STATUS，請輸入：

GET COMPUTER STATUS - 如果您位在根內容（命令列顯示 eShell>
GET STATUS - 如果您位在內容 COMPUTER（命令列顯示 eShell computer>)
.. GET STATUS - 如果您位在內容 COMPUTER REAL-TIME（命令列顯示 eShell computer real-time>)

您可以使用單一 .（點）而不使用兩個 .. 因為單一點就是兩個點的縮寫。

範例
. GET STATUS - 如果您位在內容 COMPUTER REAL-TIME（命令列顯示 eShell computer real-time>)

引數

引數是專為特定命令所執行的處理方法。例如，命令 CLEAN-LEVEL（位於 COMPUTER REAL-TIME ENGINE）可與下列引數搭配使用：

rigorous - 一律補救偵測
safe - 若安全則補救偵測，若不安全則繼續
normal - 若安全則補救偵測，若不安全則詢問
none - 一律詢問使用者

另一個範例則是引數 ENABLED 或 DISABLED，可用來啟用或停用特定功能。

縮寫形式 / 簡短的命令

eShell 可讓您縮短內容、命令和引數（假設引數是參數或替代選項）。您無法縮短具體值的前置詞或引數（例如數字、名稱或路徑）。您可以使用數字1 和 0而不是啟用和停用的引數。

範例
computer set real-time status enabled => com set real stat 1
computer set real-time status disabled => com set real stat 0

簡短形式的範例：

範例
computer set real-time status enabled => com set real stat en
computer exclusions add detection-excludes object C:\path\file.ext => com excl add det obj C:\path\file.ext
computer exclusions remove detection-excludes 1 => com excl rem det 1

當兩個命令或內容以同樣的字母為開頭時（例如您輸入 ADVANCEDA 作為 AUTO-EXCLUSIONS 和 A 的簡短命令)，eShell 將無法決定您要執行哪一個命令。系統將會顯示錯誤訊息，並且列出以 A 為開頭的命令供您選擇：

```
eShell>a

The following command is not unique: a
```

下列為 COMPUTER 內容中可用的子內容：

```
ADVANCED

AUTO-EXCLUSIONS
```

透過新增一或多個字母（例如，AD 而非只是 A) eShell 將輸入 ADVANCED 子內容，因為其現在是唯一的。這也適用於縮寫的命令。

注意
當您想確定命令是依照您所需方式執行時，我們建議您不要縮寫命令、引數等，請使用完整形式。如此 eShell 將依照您所需方式執行，而且可避免不必要的錯誤。批次檔案 / 程式碼尤其如此。

自動完成

這個在 eShell 2.0 推出的新功能，與 Windows 命令提示字元的自動完成非常類似：Windows 命令提示字元完成檔案路徑，而 eShell 完成命令、內容與作業名稱。不支援完成引數。輸入命令時，只要按下 Tab 即可完成或在可用的變化中循環切換。按下 Shift + Tab 則會往回切換。不支援混合使用縮寫形式與自動完成。請使用其中一個。例如，當您輸入 computer real-time additional 並按下 Tab 將不會有反應。相反地，請輸入 com 然後按下 Tab 完成 computer，並繼續輸入 real + Tab 和 add + Tab：按下 Enter：輸入 on + Tab 然後按下 Tab：在所有可用的變化之間循環切換：on-execute-ah、on-execute-ah-removable、on-write-ah、on-write-archive-default 等。

別名

別名是替代名稱，可用來執行命令（假設已指派別名給命令)。有一些預設別名，如下：

```
(global) close - 結束
(global) quit - 結束
(global) bye - 結束
warnlog - 工具防護記錄事件
virlog - 工具防護記錄偵測
```

"(global)" 表示命令可用於任何位置，無論目前內容為何。一個命令可指派多個別名，例如命令 EXIT 有別名 CLOSE、QUIT 和 BYE。當您要結束 eShell 時，您可以使用 EXIT 命令本身，或任一別名。別名 VIRLOG 是命令 DETECTIONS 的別名，此命令位於 TOOLS LOG 內容中。如此，便可從 ROOT 內容使用偵測命令，也因此更易於存取（您不需要進入 TOOLS，然後 LOG 內容，而且可直接從 ROOT 執行)。

eShell 可讓您定義自己的別名。命令 ALIAS 位於 UI ESHELL 內容。

密碼保護的設定

ESET File Security 設定可受到密碼保護。您可以使用 GUI 或於 eShell 使用 set ui access lock-password 來設定密碼。之後您將必須以互動的方式為某些命令（例如變更設定或修改資料的命令）輸入此密碼。如果您計劃長時間使用 eShell 而且不想重覆輸入密碼，您可以使用 set password 命令（自 root 執行）讓 eShell 記住此密碼。此後每個需要密碼的執行命令都會自動填入您的密碼，並在您結束 eShell 前記住密碼。這表示在您開始新工作階段並希望 eShell 記住您的密碼時，將需要再次使用 set password。

手冊 / 說明

當您執行 GUIDE 或 HELP 命令時，系統會顯示「初次執行畫面」說明如何使用 eShell。此命令只能在 ROOT 內容（eShell>）中使用。

命令歷程

eShell 會保留先前已執行之命令的歷程。這只適用於目前的 eShell 互動工作階段。一旦您結束 eShell，系統將捨棄命令歷程。使用鍵盤上的方向鍵 Up 和 Down 來瀏覽歷程。在您找到尋找的命令之後，您無需自開頭輸入完整的命令便可再次執行此命令，或是進行修改。

CLS / 清除畫面

CLS 命令可用來清除畫面。這與 Windows 命令提示字元或類似的命令列介面運作方式相同。

EXIT / CLOSE / QUIT / BYE

若要關閉或結束 eShell，您可以輸入任一命令（EXIT、CLOSE、QUIT 或 BYE）。

命令

本節會列出一些基本的 eShell 命令並加以說明。

> 注意
> 命令不區分大小寫，因此無論使用大寫或小寫都可執行命令。

範例命令（包含在［根］內容內）：

關於

列出關於程式的資訊。它會顯示資訊，例如：

- 您安裝的 ESET 安全性產品名稱及其版本編號。
- 作業系統和基本的硬體詳細資訊。
- 使用者名稱（包括網域）、完整電腦名稱 (FQDN)（若您的伺服器是網域的成員）以及基座名稱。
- 您的 ESET 安全性產品已安裝的元件，包括每個元件的版本編號。

內容路徑：

```
root
```

密碼

通常，若要執行受密碼保護的命令時，系統會基於安全性理由提示您輸入密碼。此規則適用於停用惡意軟體防護及可能影響 ESET File Security 配置的命令。系統將在您每次執行這類命令時，提示您輸入密碼。然而，若要避免每次輸入密碼，您可以定義此密碼。eShell將會記住此密碼，而且在執行受密碼保護的命令時，系統會自動輸入此密碼。

> 注意
> 您的密碼只適用於目前的 eShell 互動工作階段。一旦您結束 eShell, 系統將捨棄此定義的密碼。當您再次啟動 eShell 時，您需要再次定義密碼。

定義的密碼在執行未簽署的批次檔案或腳本時也可使用。執行未簽署的批次檔案時，請確認 ESET Shell 執行原則設定為完整存取權限。這類批次檔案的範例如下：

```
eshell set password plain <yourpassword> "&" computer set real-time status disabled
```

上述連鎖的命令會定義密碼並停用防護。

> 重要
> 我們建議您盡可能使用已簽署的批次檔案。如此一來您即可避免在批次檔案中有純文字密碼（若使用上述的方法）。請參閱批次檔案 / 腳本（已簽署的批次檔案一節），以取得更多詳細資料。

內容路徑：

```
root
```

語法：

```
[get] | restore password
```

```
set password [plain <password>]
```

作業：

`get` – 顯示密碼

`set` – 設定或清除密碼

`restore` – 清除密碼

引數：

`plain` – 切換將輸入的密碼作為參數

`password` – 密碼

範例：

`set password plain <yourpassword>` – 設定將用於受密碼保護之命令的密碼

`restore password` – 清除密碼

範例：

`get password` – 使用此命令來檢視是否已配置密碼（只會顯示星號「*」，不會列出密碼本身），沒有顯示星號時表示尚未設定密碼

`set password plain <yourpassword>` – 使用此命令來設定已定義的密碼

`restore password` – 此命令會清除已定義的密碼

狀態

顯示關於 ESET File Security 目前即時防護狀態的資訊，也讓您能暫停 / 繼續保護（類似 GUI)

內容路徑：

`computer real-time`

語法：

```
[get] status
set status enabled | disabled  [ 10m | 30m | 1h | 4h | temporary ]
restore status
```

作業：

`get` – 返回目前設定/狀態

`set` – 設定值/狀態

`restore` – 還原預設設定/物件/檔案

引數：

`enabled` – 啟用防護/功能

`disabled` – 停用防護/功能

`10m` – 停用 10 分鐘

`30m` – 停用 30 分鐘

`1h` – 停用 1 小時

`4h` – 停用 4 小時

`temporary` – 停用至下次重新開機

> 注意
> 無法使用單一命令停用所有防護功能。您可以使用 `status` 命令逐一管理防護功能和模組。每個防護功能或模組都有專屬的 `status` 命令。

使用 `status` 命令的功能清單：

功能	內容和命令
自動排除	`COMPUTER AUTO-EXCLUSIONS STATUS`
主機入侵預防系統 (HIPS)	`COMPUTER HIPS STATUS`
即時檔案系統防護	`COMPUTER REAL-TIME STATUS`

功能	內容和命令
裝置控制	`DEVICE STATUS`
殭屍網路防護	`NETWORK ADVANCED STATUS-BOTNET`
網路攻擊防護 (IDS)	`NETWORK ADVANCED STATUS-IDS`
網路隔離	`NETWORK ADVANCED STATUS-ISOLATION`
ESET 叢集	`TOOLS CLUSTER STATUS`
診斷記錄	`TOOLS DIAGNOSTICS STATUS`
簡報模式	`TOOLS PRESENTATION STATUS`
網路釣魚防護	`WEB-AND-EMAIL ANTIPHISHING STATUS`
電子郵件用戶端防護	`WEB-AND-EMAIL MAIL-CLIENT STATUS`
Web 存取防護	`WEB-AND-EMAIL WEB-ACCESS STATUS`

VIRLOG

這是 `DETECTIONS` 命令的別名。當您需要檢視關於所偵測到入侵的資訊時，可使用此命令。

WARNLOG

這是 `EVENTS` 命令的別名。當您需要檢視關於各種事件的資訊時，可使用此命令。

批次檔案 / 腳本

您可以使用 eShell 作為強大的腳本工具以自動進行作業。若要搭配 eShell 使用批次檔案，請使用 eShell 建立一個批次檔案並在其中寫入命令。

> 範例
> `eshell get computer real-time status`

您也可以連鎖命令，有時這是必要的，例如您想要取得某個已排程的工作，請如下輸入：

```
eshell select scheduler task 4 "&" get scheduler action
```

項目的選取（在本例中為第 4 號工作）通常僅適用於 eShell 的目前執行中實例。如果您連續執行這兩命令，則第二個命令會失敗，錯誤為「未選取工作或所選取的工作不存在」。

基於安全性理由，執行原則會預設為**「限制的腳本」**。這可讓您使用 eShell 作為監控工具，但不會讓您變更 ESET File Security 的組態。若您嘗試針對會影響安全性的命令執行腳本，如停用防護，則會顯示**［已拒絕存取］**訊息。建議您使用已簽署的批次檔案，以執行會變更組態的命令。

如要使用在 Windows 命令提示字元中手動輸入的單一命令來變更配置，您必須授予 eShell 完整存取權（不建議）。若要授予完整存取權，請使用 eShell 自身互動模式中的 `ui eshell shell-execution-policy`，或透過 **［進階設定］(F5) > ［使用者介面］ > ESET Shell** 內的 GUI 即可。

已簽署的批次檔案

eShell 允許您使用簽章保護一般批次檔案(*.bat)以用來防護設定的相同密碼簽署指令碼。為了簽署指令碼，您必須先啟用設定防護。這可以透過 GUI 完成，或從 eShell 中使用 `set ui access lock-password` 命令。設定好設定防護密碼後，您可以啟動簽署的批次檔案。

注意
如果您變更設定防護密碼，則您必須再次簽署所有的腳本，否則腳本便無法執行以下密碼變更。簽署腳本時，輸入的密碼必須符合目標系統上的設定保護密碼。

若要簽署此批次檔案，請從 eShell 的內容執行 `sign <script.bat>`，其中 *script.bat* 是所要簽署指令碼的路徑。此密碼必須符合設定防護密碼。簽章會以註解形式放在批次檔案結尾處。如果此指令碼已經簽署，便會由新的簽署取代。

注意
當您修改先前已簽署的批次檔案時，該檔案需要再簽署一次。

若要從 Windows 命令提示字元執行已簽署的批次檔案，或以排程工作的方式執行，請使用下列命令：

```
eshell run <script.bat>
```

其中 script.bat 是批次檔案的路徑。

範例
```
eshell run d:\myeshellscript.bat
```

ESET SysInspector

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

按一下 **[建立]**，然後在 **[註解]** 中輸入說明待建立防護記錄的簡短描述。請等候直到 ESET SysInspector 防護記錄產生（狀態顯示為 [已建立]）。視硬體配置和系統資料而定，防護記錄建立可能需要一些時間。

ESET SysInspector 視窗會顯示建立的防護記錄相關的下列資訊：

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

可用動作如下所示：

- **顯示** – 開啟已建立的防護記錄。在防護記錄上按一下滑鼠右鍵並從內容功能表選取 [顯示]。
- **比較** – 比較兩份現有防護記錄。
- **建立** – 建立新的防護記錄。輸入簡單註解說明要建立的防護記錄，並按一下 [建立]。請等候直到 ESET SysInspector 防護記錄完成（狀態為已建立）。
- **刪除** – 從清單移除選取的防護記錄。

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

- **顯示** – 在 ESET SysInspector 中開啟所選取的防護記錄（與按兩下防護記錄的功能相同）。
- **比較** – 比較兩份現有防護記錄。
- **建立** – 建立新的防護記錄。輸入簡單註解說明要建立的防護記錄，並按一下 **[建立]**。請等候直到 ESET SysInspector 防護記錄完成（**狀態**為已建立）。
- **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。

ESET SysRescue Live

ESET SysRescue Live 是免費的公用程式，讓您建立可開機的救援 CD/DVD 或 USB 隨身碟。您可以從救援媒體啟動受感染的電腦，然後掃描是否存在惡意軟體，並清除受感染檔案。

ESET SysRescue Live 的主要優點是 ESET Security 解決方案獨立於主機作業系統之外執行，但可直接存取磁碟及檔案系統。因此它能夠移除一般無法刪除（例如在作業系統執行時）的威脅。

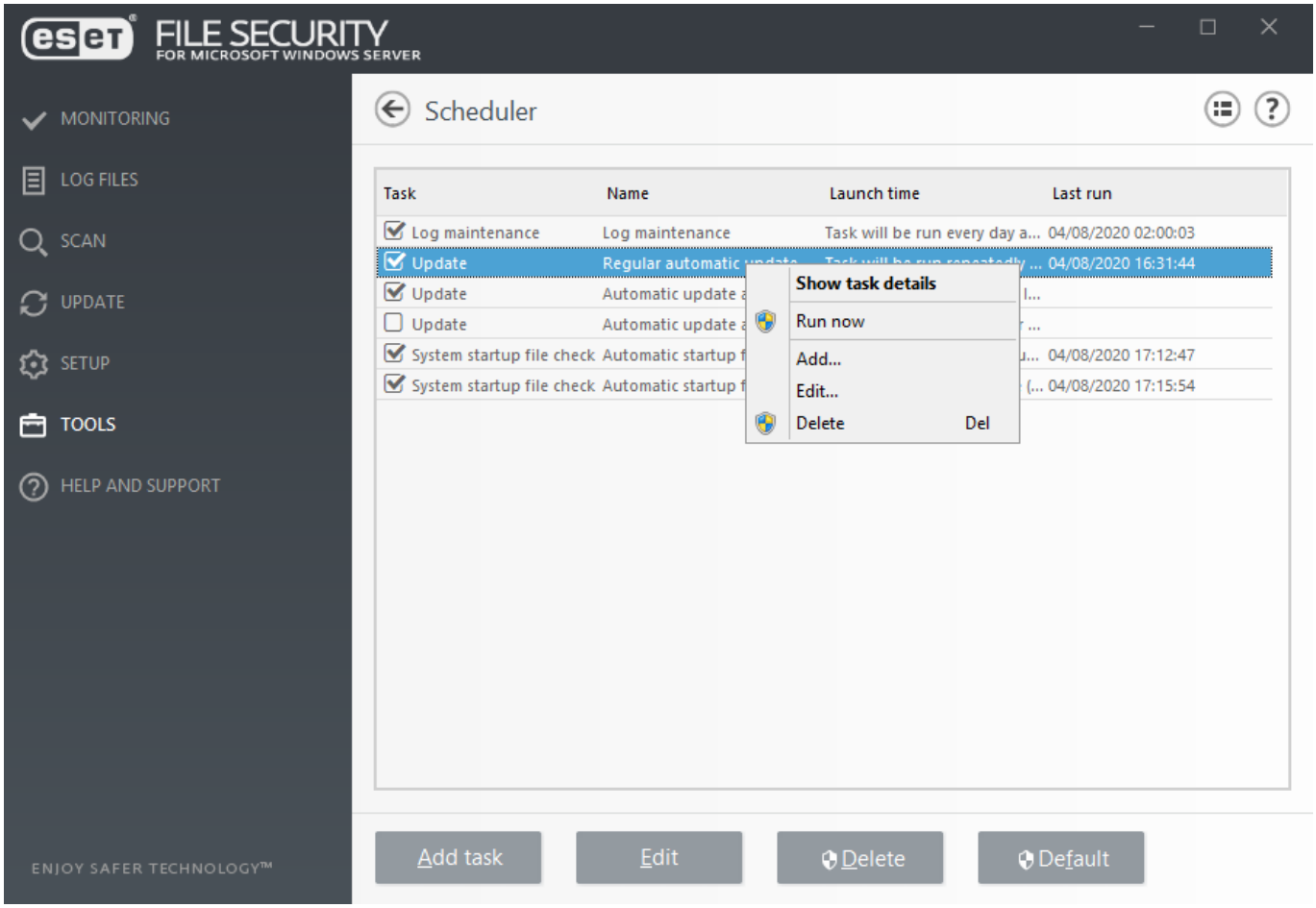
排程器

排程器會根據定義的參數來管理和啟動已排程的工作。您可以看見所有的已排程工作以表格形式列為清單，其中會顯示這些工作的參數，例如工作類型及名稱、啟動時間和上次執行時間。您也可以按一下［新增工作］建立新的已排程工作。若要編輯現有已排程工作的配置，請按一下**［編輯］**按鈕。若要將已排程的工作清單還原為預設設定，請按一下**［預設值］**，然後按一下**［還原為預設值］**，所有完成的變更都會遺失且無法恢復。

有一組預先定義的預設工作：

- 防護記錄維護
- 定期自動更新（使用此工作更新頻率)
- 撥號連線後自動更新
- 使用者登入後自動更新
- 自動啟動檔案檢查（使用者登入後）
- 自動啟動檔案檢查（成功模組更新後）

> 注意
> 核取適當的核取方塊以啟動或停用工作。



若要執行下列動作，以滑鼠右鍵按一下工作：

顯示工作詳細資訊	**按兩下，或以滑鼠右鍵按一下已排程的工作時，顯示關於已排程工作的詳細資訊。**
立即執行	執行選取的排程器工作並立即執行工作。
新增...	啟動會協助您建立新的排程器工作
編輯...	編輯（預設及使用者定義的）現有排定工作的配置。
刪除	刪除現有的工作。

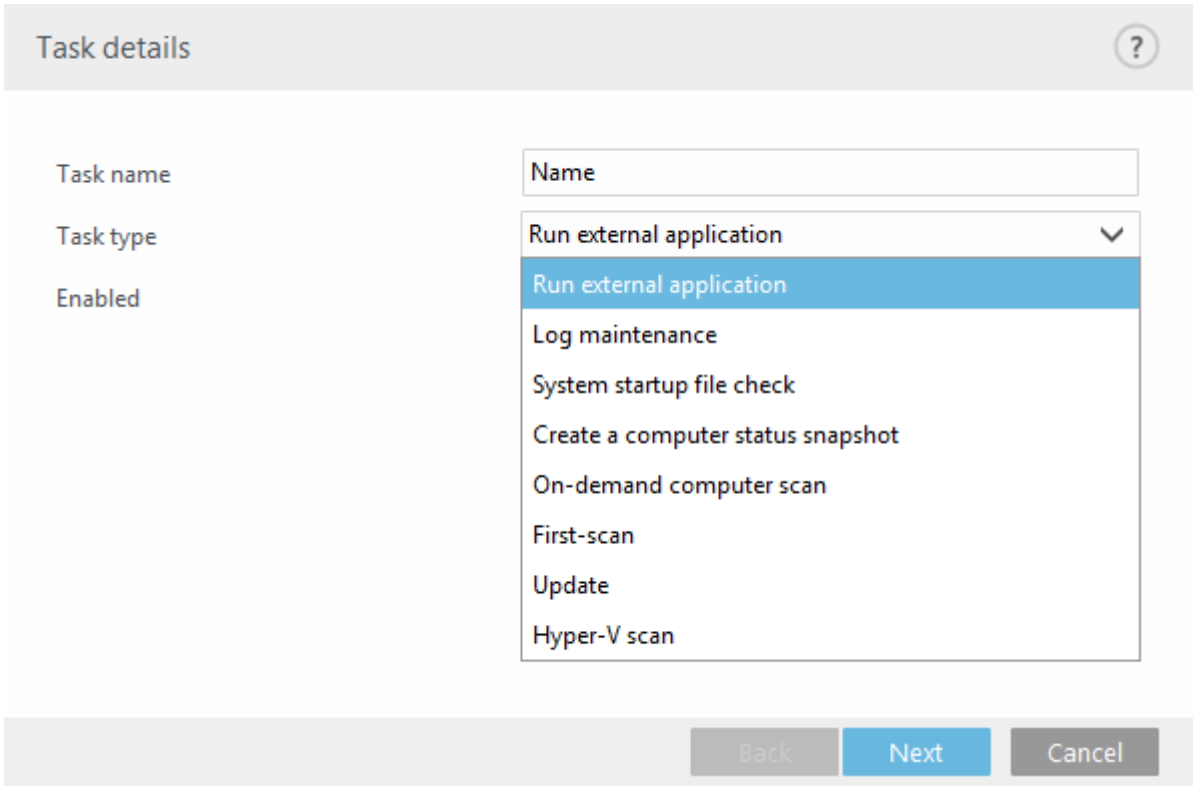
排程器 – 新增工作

若要建立新已排程的工作：

1.按一下 **[新增工作]**

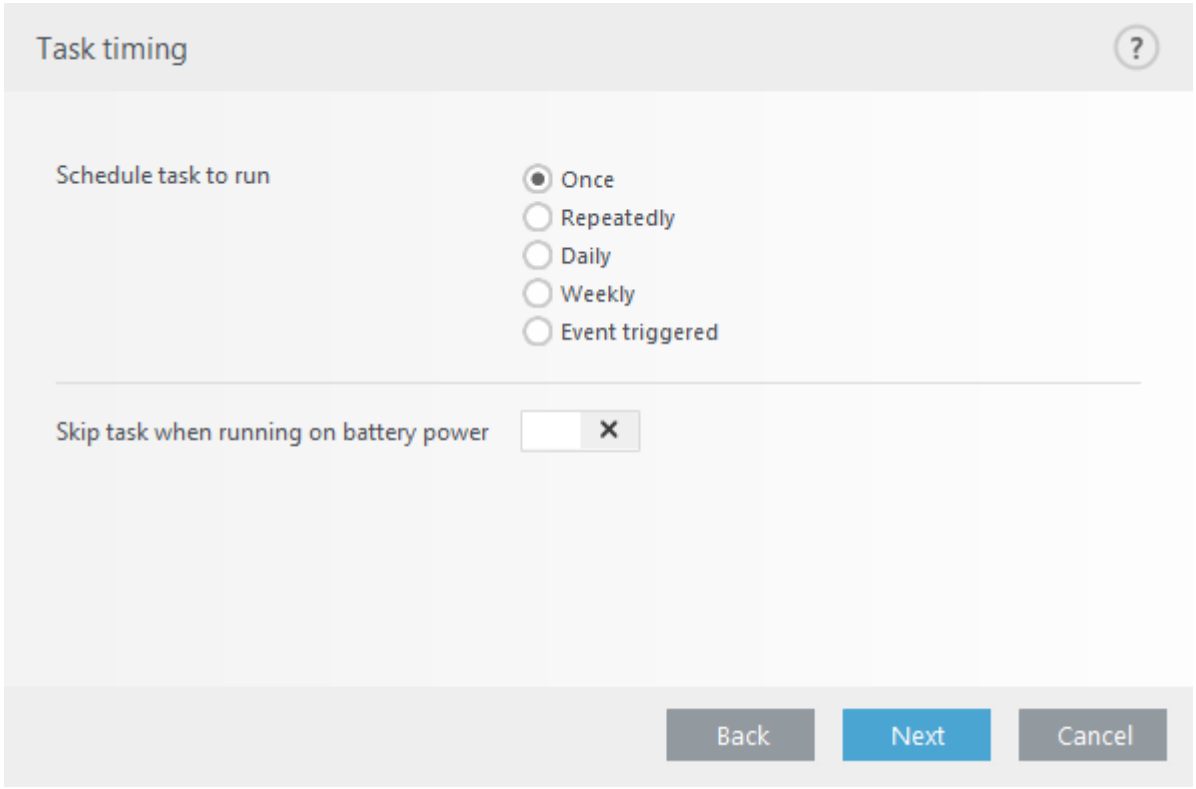
2.輸入 **[工作名稱]** 並配置您的自訂已排程工作。

3. 工作類型 – 從下拉式功能表選取適用的 **[工作類型]**

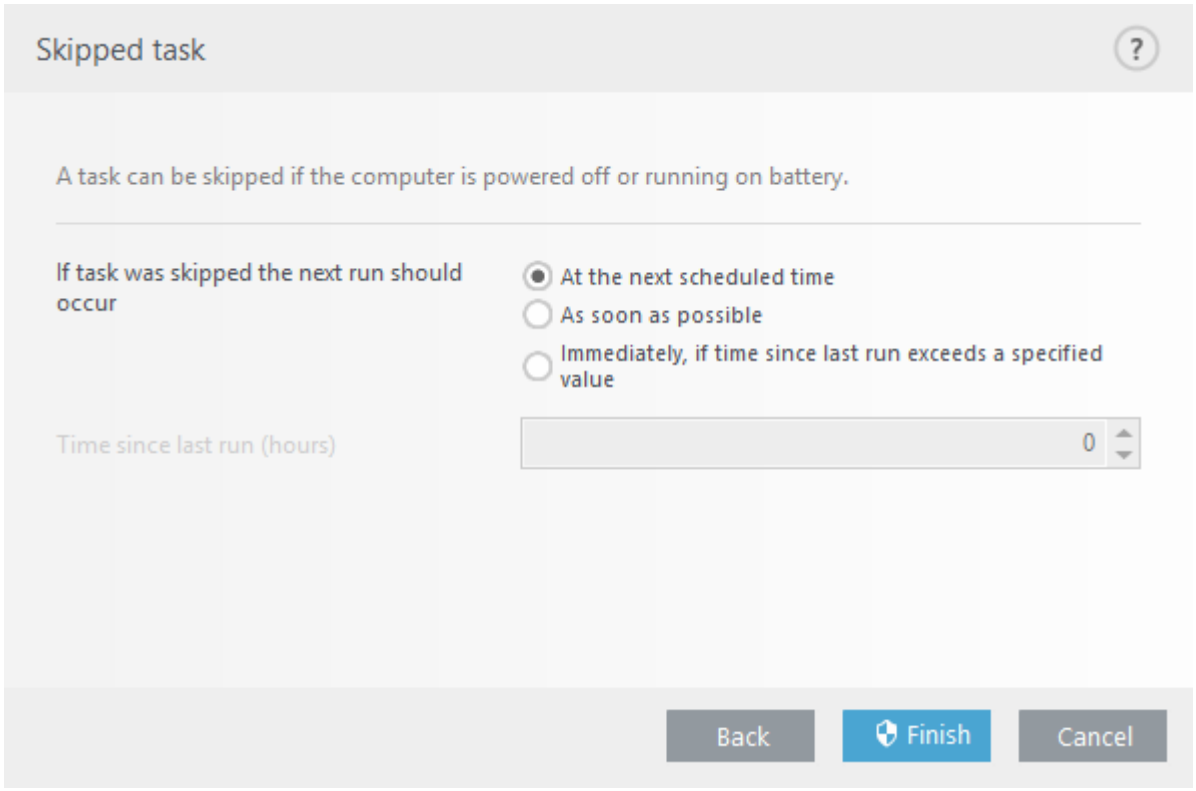


注意
若要停用工作，請按一下 **[已啟用]**旁的滑桿。若要在稍後啟動工作，使用 [排程器] 視圖中的核取方塊。

4. 工作時間 – 選取其中一個選項，以定義您要執行工作的時間。根據您的選擇，系統便會提示您選擇特定時間、日期、間隔或事件。



5. 略過的工作 – 如果工作無法在預先定義的時間執行，您可以指定工作的執行時間



6. 執行應用程式 – 如果將工作排程為執行外部應用程式，請從目錄樹狀結構選擇可執行檔。

7.如果您必須進行變更，按一下［上一步］返回前幾個步驟並修改參數。

8.按一下［完成］以建立工作或套用變更。

新的已排程工作將會出現在［排程器］視圖中。

工作類型

配置精靈與已排程工作的每個工作類型不同。輸入**工作名稱**並從下拉式功能表選取您想要的**工作類型**。

- **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。此工作會定期將防護記錄檔案中的記錄最佳化，以確保有效運作。
- **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** – 排程更新工作以執行偵測引擎和程式模組的更新。
- **Hyper-V 掃描** – 為 Hyper-V 內的虛擬磁碟排程掃描。
- **OneDrive 掃描** – 排程掃描儲存在 OneDrive 上的檔案。

若要在工作建立後停用工作，如果您要停用該工作，請按一下**已啟用**旁的切換鈕。若要在之後啟動工作，按一下排程器視圖中的核取方塊。按一下［下一步］以繼續下一步。

工作時間

選取下列其中一個時間選項：

- **一次** – 工作將只會在指定的日期和時間執行一次。在指定時間，只執行工作一次。在**［工作執行］**中指定一次的開始日期和時間。
- **重複** – 工作將在指定的時間間隔（分鐘）內執行。在**［工作執行］**指定每天要執行工作的時間。
- **每日** – 工作會在每天指定的時間重複執行。
- **每星期** – 工作每星期在選取的日期及時間執行一或多次。在一週（以指定的日期和時間開始）的特定日期重複執行工作。在工作執行時間中指定開始時間。選取應執行工作當週的天數。
- 事件觸發 - 工作會在指定的事件之後執行。

如果您啟用**使用電池執行時略過工作** 在工作應啟動時，如果系統使用電池執行，則不會啟動工作。例如，以 UPS 執行的電腦。

事件觸發

在排程由事件觸發的工作時，您可以指定距離兩項工作完成之間的最少間隔。

下列任一事件都會觸發工作：

- **每次電腦啟動時**
- **每天第一次啟動電腦時**
- **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** – 使用者登入系統時，便會部署此工作。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，接著隔天同樣選擇並執行工作。
- **威脅偵測**

執行應用程式

此工作會排程外部應用程式的執行。

- **［執行檔］** – 從目錄樹狀結構選擇可執行檔，按一下**瀏覽（...）**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）。

略過的工作

如果工作無法在預先定義的時間執行，您可以指定工作的執行時間：

- **於下次排程的時間** – 此工作將於指定時間執行（例如在 24 小時後）。
- **儘快** – 當阻止工作執行的動作不再有效時，工作將會儘快執行。
- **如果距離上次執行的時間超過指定值，則立即執行工作 – 自上次執行後經過的時間（小時）** – 選取此選項後，您的工作將會在特定時間（小時）後重覆執行。

已排程的工作概要

當您在**排程器**視圖中的工作上按兩下，或以滑鼠右鍵按一下已排程的工作並選擇**［顯示工作詳細資料］**時，此對話方塊視窗會顯示關於已排程工作的詳細資訊。

提交樣本以供分析

樣本提交對話方塊可讓您將檔案或網站傳送至 ESET 以供分析。如果您在電腦中發現行跡可疑的檔案，或在網際網路中發現可疑的網站，您可以將其提交至 ESET 病毒實驗室以供分析。如果檔案證實為惡意的應用程式或網站，則其偵測會新增到近期的更新中。

若要透過電子郵件來提交檔案，請使用 WinRAR 或 WinZip 壓縮檔案，使用密碼「*infected*」來保護壓縮檔，然後將其傳送至 samples@eset.com。請使用敘述性的主旨，並盡可能涵蓋檔案的相關資訊（例如下載的網站）。

在將樣本提交至 ESET 之前，請確定其符合下列一或兩個條件：

- 完全未偵測該檔案或網站
- 錯將該檔案或網站偵測為威脅

如果上述要求至少有一個不符合，則在提供進一步資訊之前，您將不會收到回應。

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。

聯絡人電子郵件

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

匿名提交

使用［**匿名提交**］旁邊的核取方塊以傳送可疑的檔案或網站，而不需要輸入您的電子郵件地址。

可疑檔案

觀察到的惡意程式感染徵兆與信號

輸入在您電腦上觀察到的可疑檔案行為的說明。

檔案來源 (URL 位址或供應商)

請輸入檔案來源，以及您在何種狀況下發現這個檔案。

附註與其他資訊

您可以在這裡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。

> 注意
> 雖然第一個參數 – ［**觀察到的惡意軟體感染徵兆與信號**］– 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。

可疑網站

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：

已感染

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。

垃圾郵件

詐騙或詐欺網站。

其他

如果上述選項均不適用於您要提交的網站，請使用此選項。

附註與其他資訊

您可以輸入進一步的資訊或說明，這對於分析可疑網站將有所助益。

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，以便改善偵測引擎，並協助其他人受到防護。如果檔案模式符合偵測引擎中所含的模式，就會發生誤判 (FP)

注意
該 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。

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。

誤判網站

我們建議您提交偵測為感染、詐騙或網路釣魚但尚未受感染的檔案。如果檔案模式符合偵測引擎中所含的模式，就會發生誤判 (FP)請提供此網站以改善我們的偵測引擎，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，這在處理可疑檔案時將會很有助益。

其他

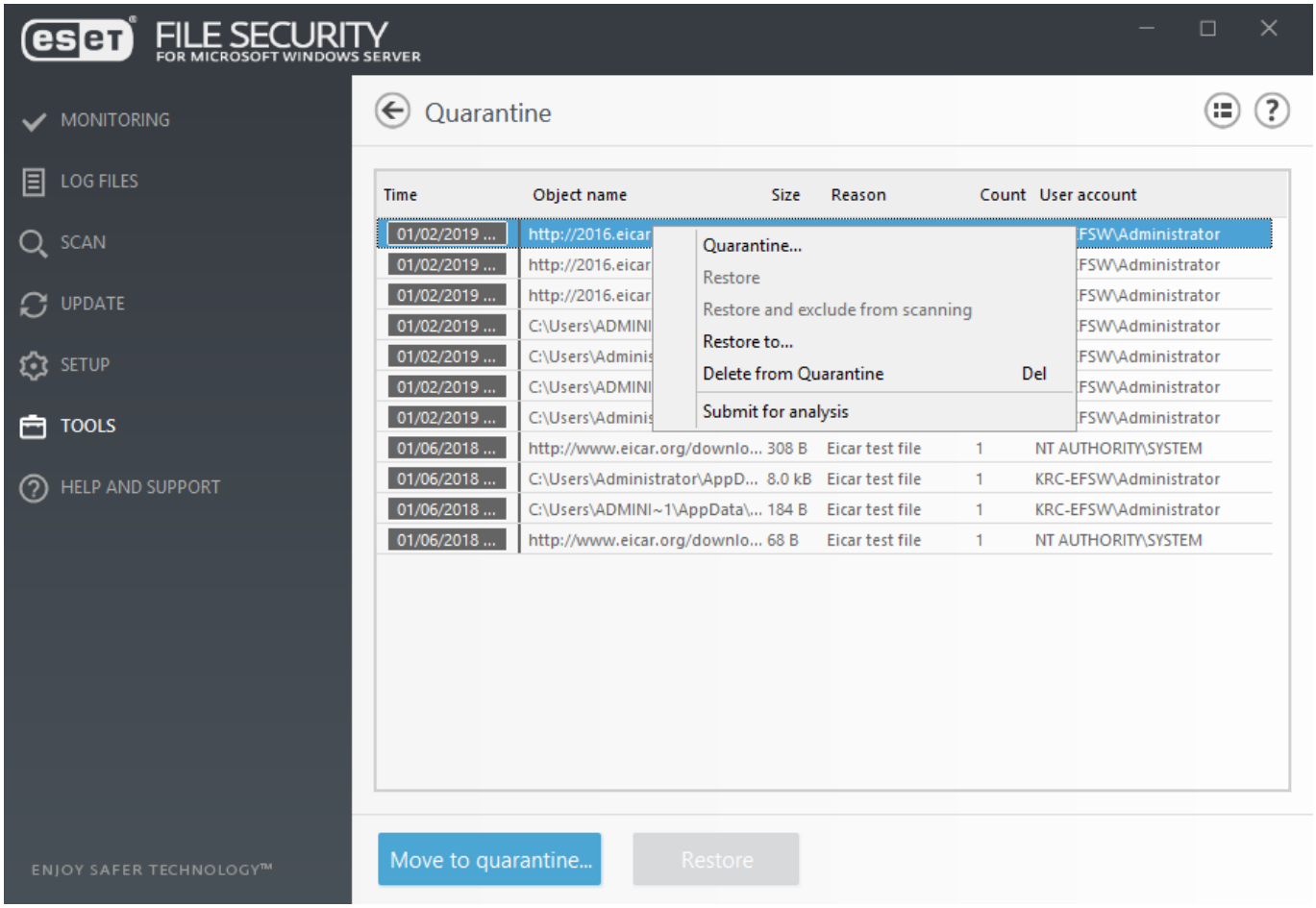
如果檔案無法歸類為**可疑檔案**或**誤判**，請使用這份表單。

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受感染檔案。對於無法清除、無法安全刪除或不建議刪除的檔案，或者 ESET File Security 錯誤偵測到的檔案，應該予以隔離。您可以選擇隔離任何檔案。如果檔案行為可疑，但惡意軟體掃描器沒有偵測到，則建議進行隔離。您可將隔離的檔案提交至 ESET 病毒實驗室進行分析。



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

如果電子郵件訊息物件被放置於檔案隔離區，則系統會以前往信箱/資料夾/檔案名稱路徑的形式顯示資訊。

隔離檔案

ESET File Security 會自動隔離刪除的檔案（如果您尚未在警告視窗中停用此選項）。若要手動隔離任何可疑檔案，按一下 **[隔離]**。手動隔離任何可疑檔案，隔離檔案將從隔離檔案原始位置移除。內容功能表也可用於此目的 – 以滑鼠右鍵按一下 **[隔離區]** 視窗，並選取 **[隔離]**。

從隔離區還原

隔離的檔案還可還原至其原始位置。使用 **[還原]** 功能可從內容功能表取得，方法是以滑鼠右鍵按一下［隔離區］視窗中的指定檔案。如果檔案標記潛在不需要的應用程式，則可以使用 **[還原並從掃描中排除]** 選項。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。

> 注意
> 如果程式錯誤地隔離了無惡意檔案，請在還原後從掃描中排除檔案，並將該檔案傳送至ESET客戶服務。

從隔離區提交檔案

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

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]**。

OneDrive 掃描設定

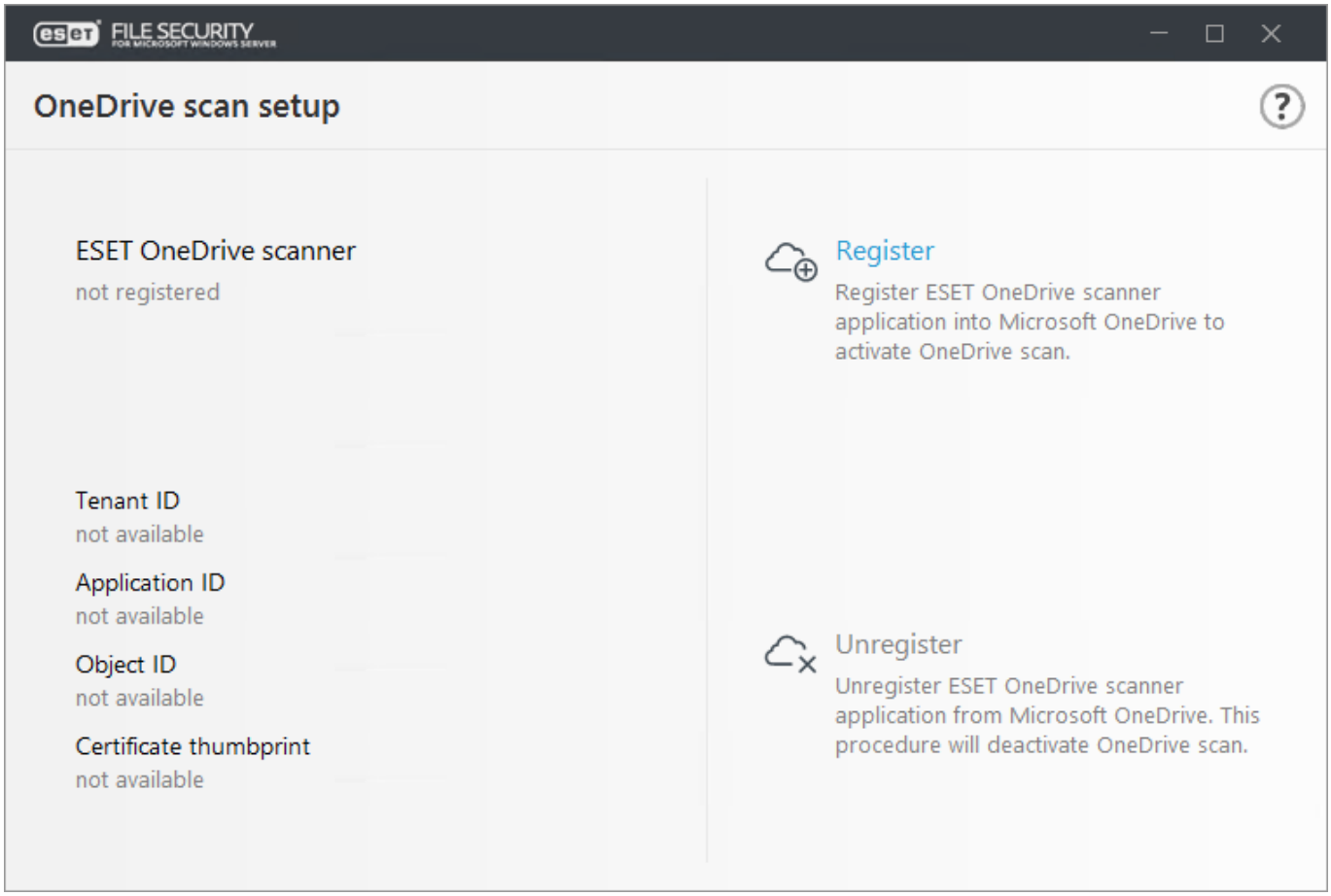
開啟 ESET File Security
按一下［設定］>［伺服器*] > [OneDrive* 掃描設定］ 

此功能可讓您掃描儲存在 Microsoft 商務用 OneDrive 雲端儲存空間中的檔案。ESET File Security OneDrive 掃描僅可為您處理檔案和資料夾，而不會掃描其他類型資料，例如電子郵件、SharePoint 檔案、連絡人或行事曆。

快速連結

註冊 ESET OneDrive 掃描器
取消註冊 ESET OneDrive 掃描器

若要開始使用 ESET File Security OneDrive 掃描，請向 Microsoft OneDrive / Microsoft Office 365 / Microsoft Azure 註冊 ESET OneDrive 掃描器應用程式。OneDrive 掃描設定頁面會顯示註冊狀態；如果已註冊，您將看到註冊詳細資料（租戶 ID、應用程式 ID、物件 ID 和憑證指紋）。您可以「註冊」或「取消註冊」ESET OneDrive 掃描器：



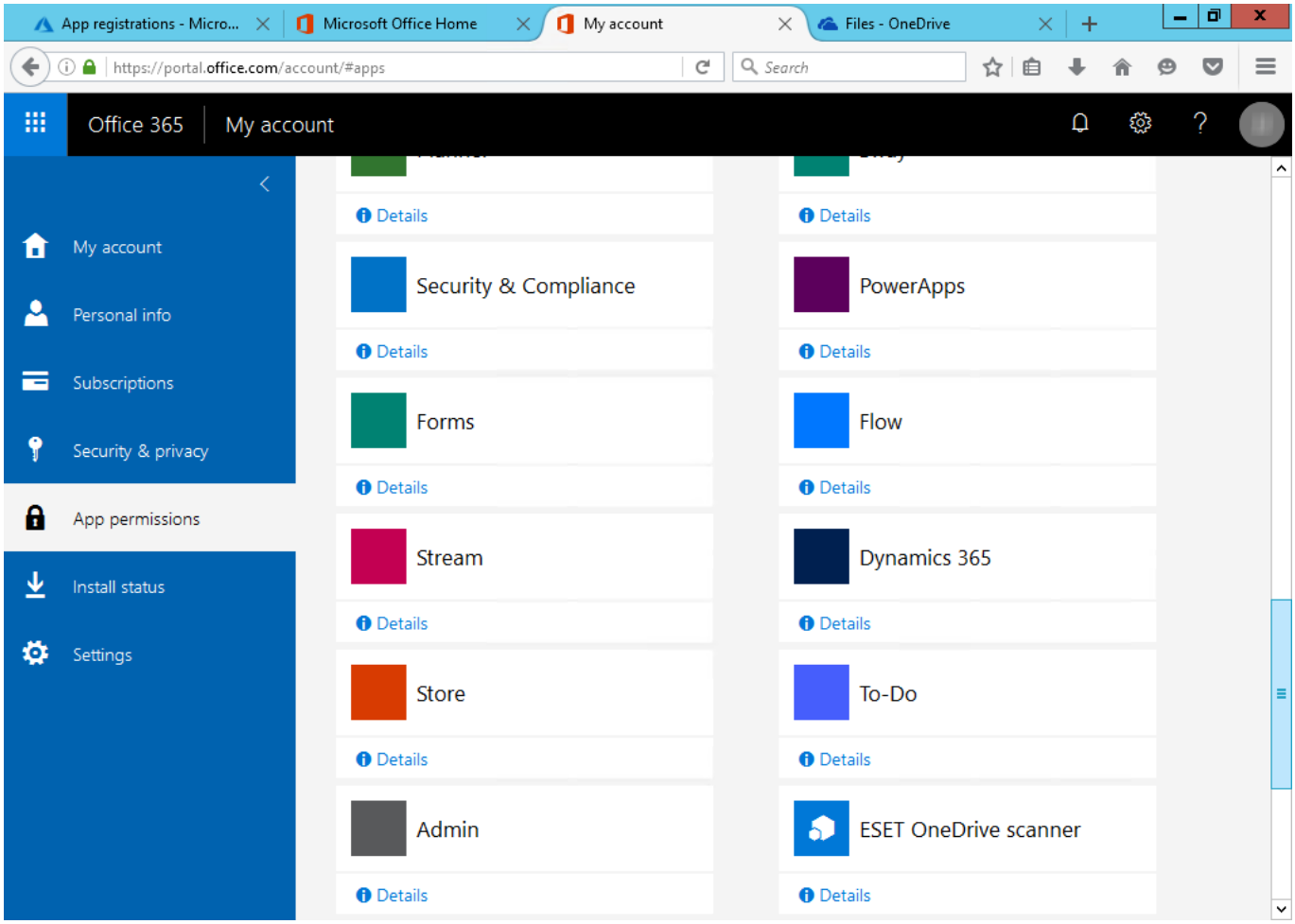
成功註冊後，OneDrive 掃描會出現在［掃描］功能表中，並會顯示使用者清單以及可供選取進行掃描的資料夾結構和檔案。ESET File Security OneDrive 掃描可掃描任何使用者儲存在商務用 OneDrive 的檔案。

注意
ESET File Security OneDrive 掃描會從商務用 OneDrive 雲端儲存裝置下載檔案並在本機執行掃描。一旦完成掃描，系統會移除已下載的檔案。從 OneDrive 下載大量資料會影響您的網路流量。

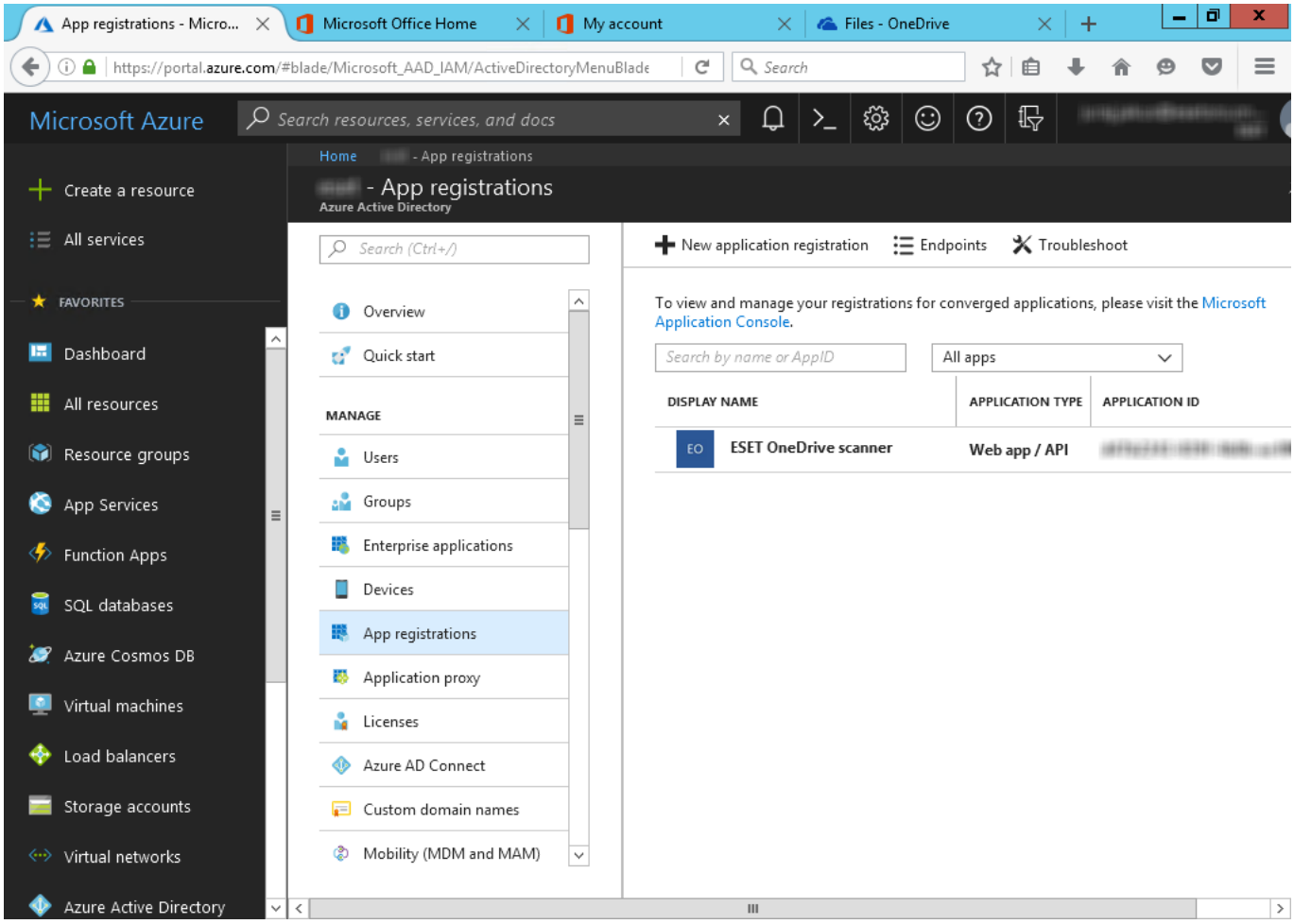
注意
使用其他帳戶重新註冊：如果您要以新的 Microsoft 商務用 OneDrive / Office 365 帳戶註冊 ESET File Security OneDrive 掃描器，您必須在您以舊有帳戶註冊的掃描器上進行取消註冊 ESET OneDrive 掃描器，並以新的 Microsoft 商務用 OneDrive / Office 365 帳戶執行註冊。

您可以在 Office 365 和 Azure 中看到 ESET OneDrive 掃描器已註冊為應用程式。

Office 365 入口網站 – 按一下［我的帳戶］頁面上的 **[應用程式權限]**，您將會看到 ESET OneDrive 掃描器應用程式已經列出。



Azure – 導覽至 **[Azure Active Directory]** > **[應用程式註冊]**，按一下**[檢視所有應用程式]**，您將會看到 ESET OneDrive 掃描器已經列出。按一下應用程式即可查看詳細資料。

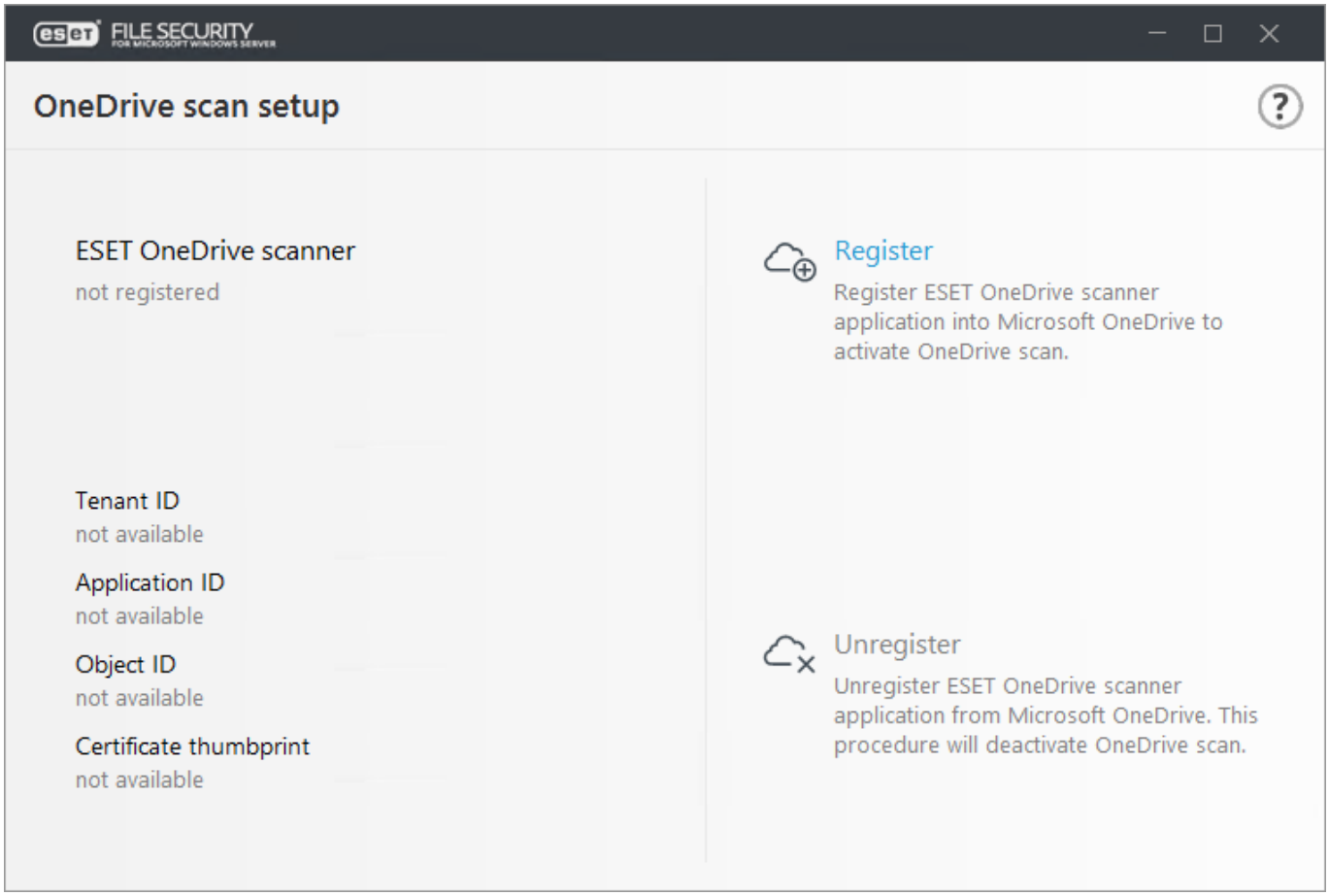


註冊 ESET OneDrive 掃描器

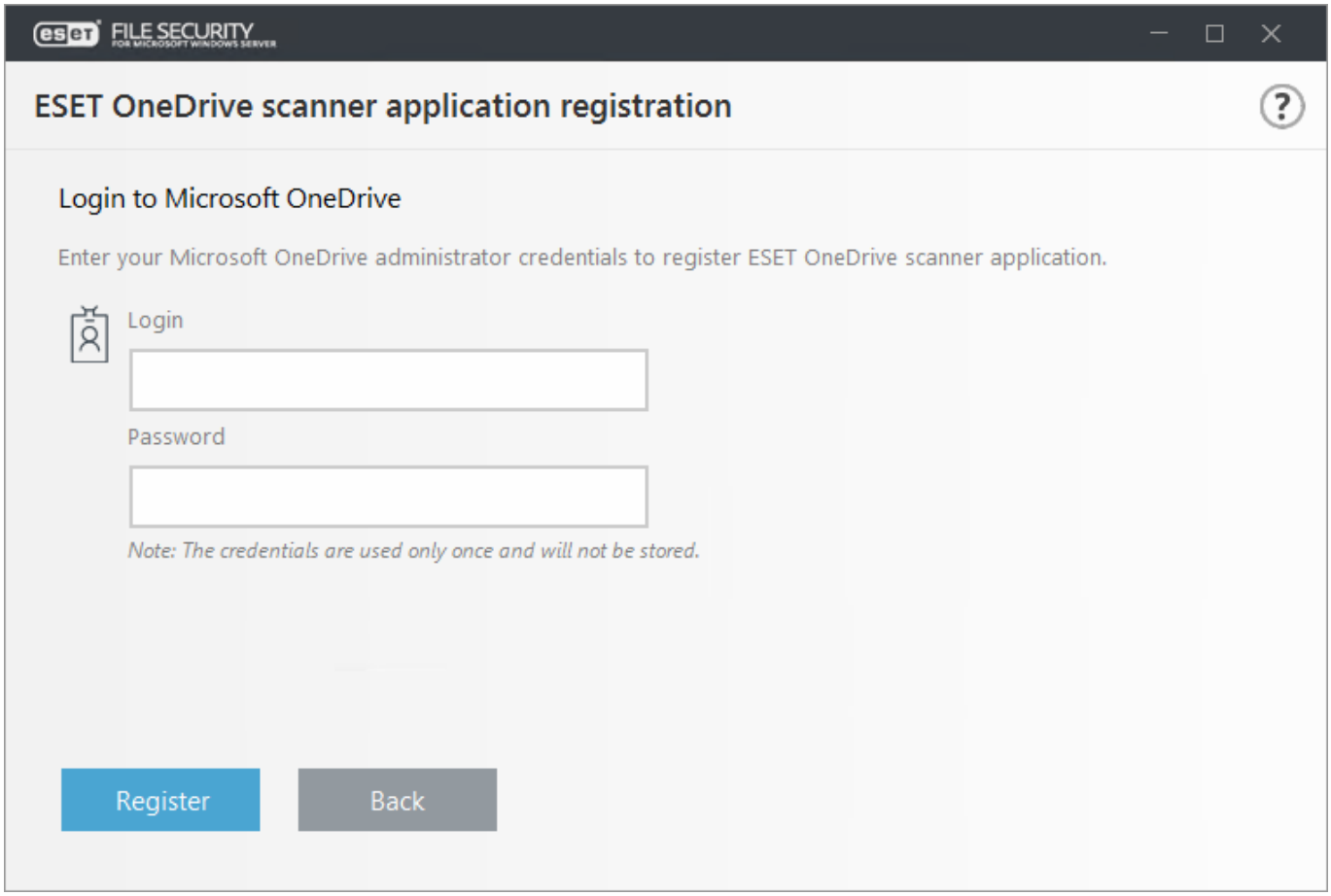
開啟 ESET File Security
按一下［設定］>［伺服器*] > [OneDrive* 掃描設定］>［註冊］ 

以下是將 ESET OneDrive 掃描器應用程式註冊到 Microsoft OneDrive / Office 365 / Azure 的程序：

- 按一下**［註冊］**以開始 ESET OneDrive 掃描器註冊，註冊精靈將會開啟。

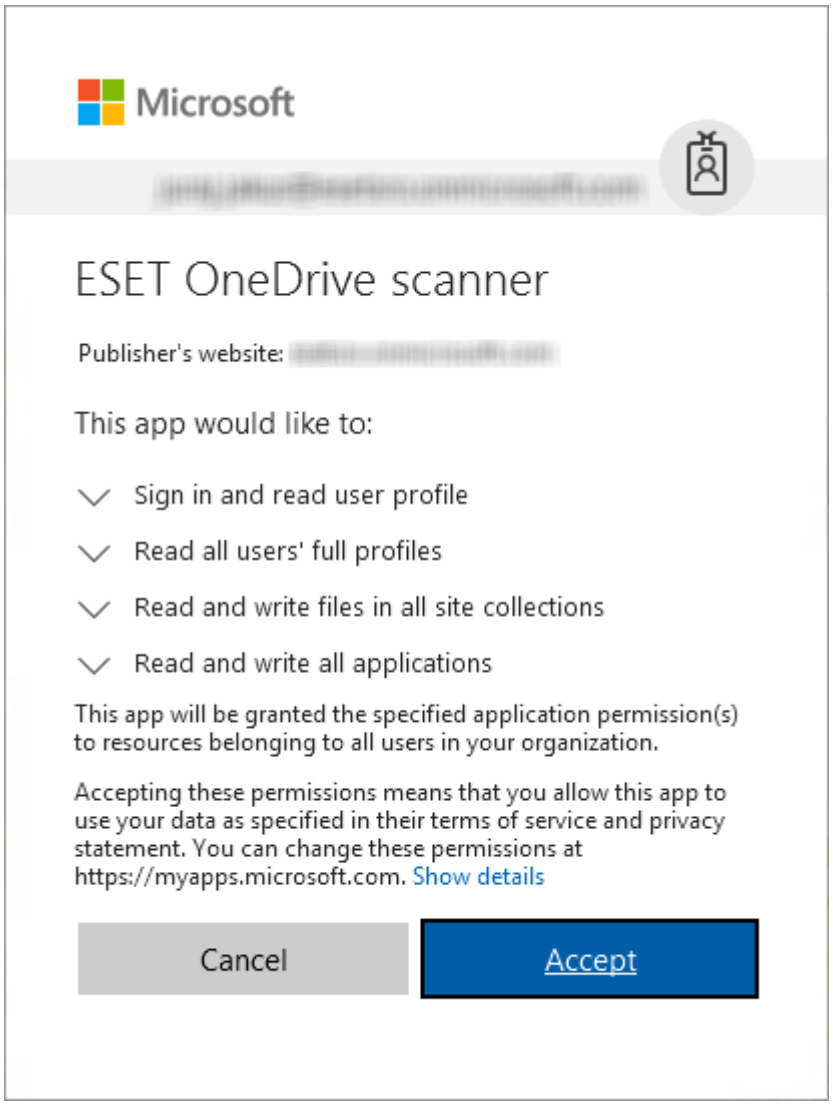


• 輸入您的 Microsoft OneDrive / Office 365 管理員帳戶認證。等待應用程式完成註冊至 Microsoft OneDrive。



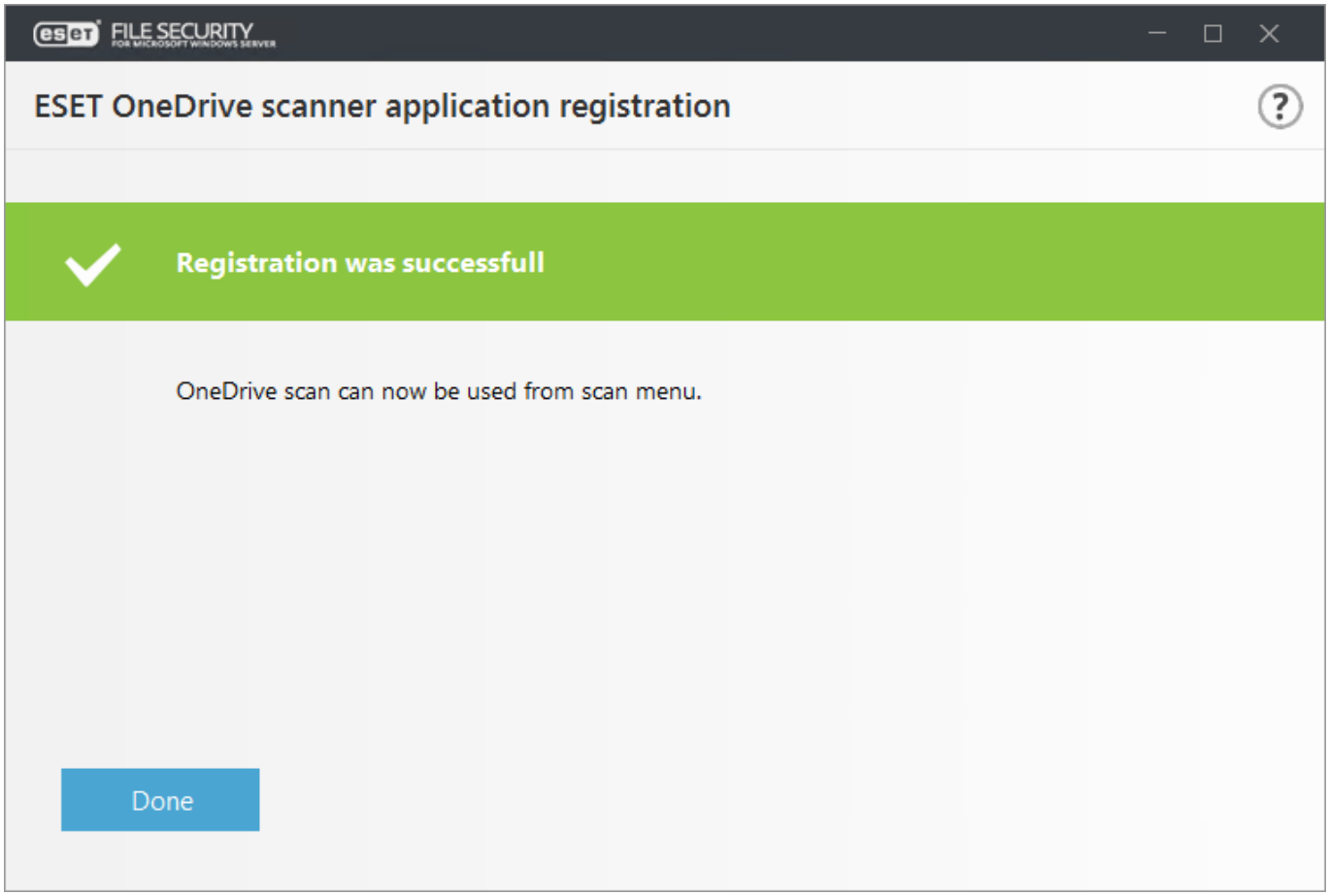
• 網頁瀏覽器即會開啟，並會顯示 Microsoft［**選取帳戶**］頁面。按一下您要使用的帳戶（如果有），或輸入您的 Microsoft OneDrive / Office 365 管理員帳戶認證，然後按一下［**登入**］。

• ESET OneDrive 掃描器應用程式需要具有在接受訊息中列出的四種權限。請按一下［**接受**］以允許 ESET File Security OneDrive 掃描器存取您 OneDrive 雲端儲存空間上的資料。



• 如果網頁瀏覽器要求您傳送此資料，請按一下［**繼續**］（資料傳送至 localhost 僅為讓 ESET File Security 知道應用程式註冊成功）。

• 一旦您關閉網頁瀏覽器，ESET OneDrive 掃描器註冊精靈會顯示「註冊成功」訊息，請按一下［**完成**］。



注意
ESET OneDrive 掃描器註冊程序可能會因情況而不同，視乎您有否使用您的管理員帳戶認證登入任何 Microsoft 入口網站 (OneDrive、Office 365、Azure 等)。請遵循註冊精靈視窗畫面上的指示和訊息。

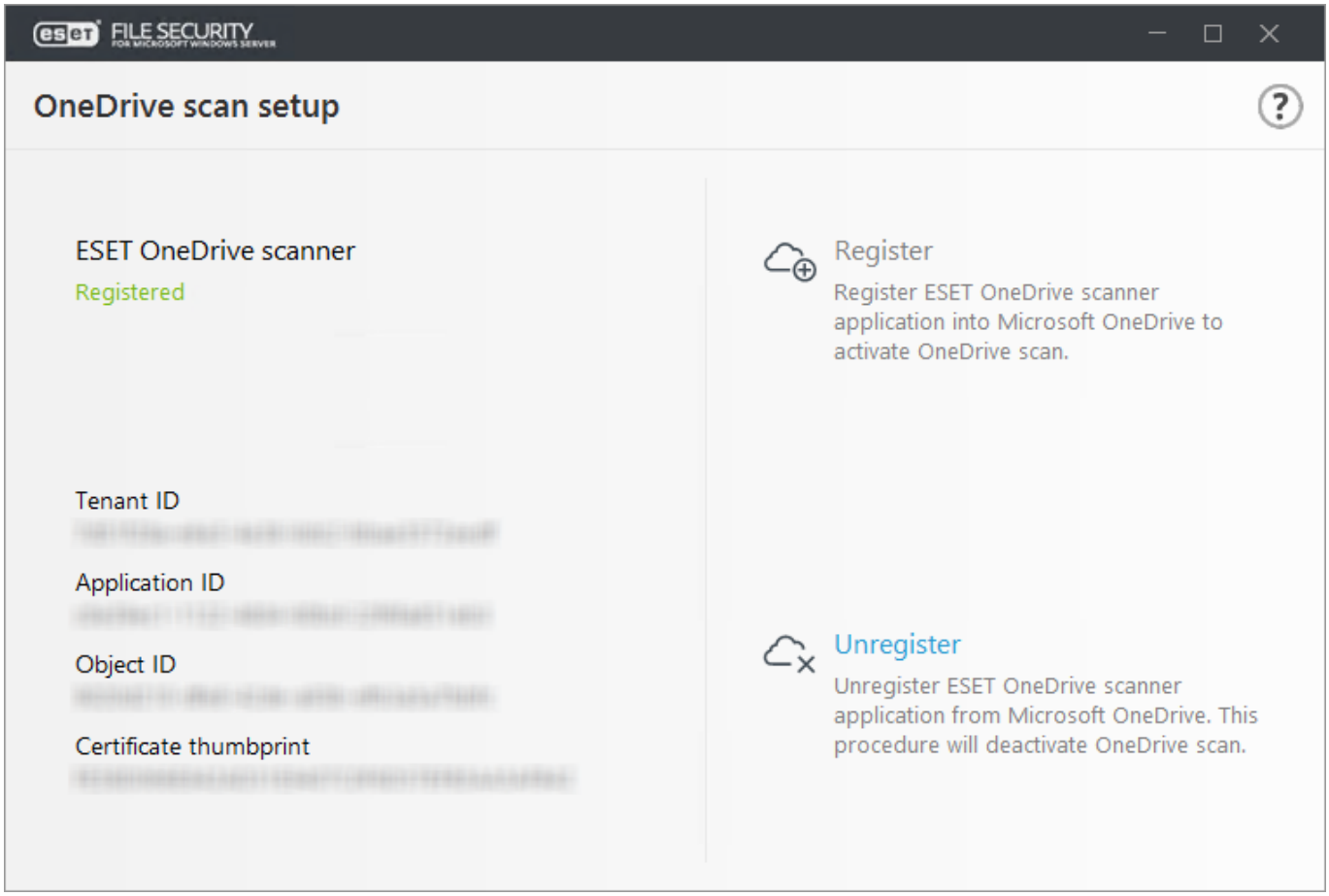
如果您在 ESET OneDrive 掃描器註冊期間遇到下列任何錯誤訊息，請查看錯誤訊息詳細資料以取得建議的解決方案：

錯誤訊息	錯誤訊息詳細資料
發生非預期錯誤。	ESET File Security 中可能發生問題。請稍後再次嘗試執行 ESET OneDrive 掃描器註冊。如果問題持續存在，請連絡 ESET 技術支援。
無法連線到 Microsoft OneDrive。	檢查您的網路/網際網路連線，然後再次執行 ESET OneDrive 掃描器註冊。
收到來自 Microsoft OneDrive 的非預期錯誤。	已傳回 HTTP 4xx 錯誤，而錯誤訊息回覆中沒有解答。如果問題持續存在，請連絡 ESET 技術支援。
收到下列來自 Microsoft OneDrive 的錯誤。	Microsoft OneDrive 伺服器傳回錯誤，並包含特定錯誤代碼/名稱，請按一下 **[顯示錯誤]**。
設定工作已逾時。	ESET OneDrive 掃描器註冊設定工作需時過長。請稍後再嘗試執行 ESET OneDrive 掃描器註冊。
已取消設定工作。	您已取消執行中的註冊工作。如果您要完成註冊，請再次執行 ESET OneDrive 掃描器註冊。
另一項設定工作已在進行中。	這是執行中的註冊工作。請等待上一個註冊程序完成。

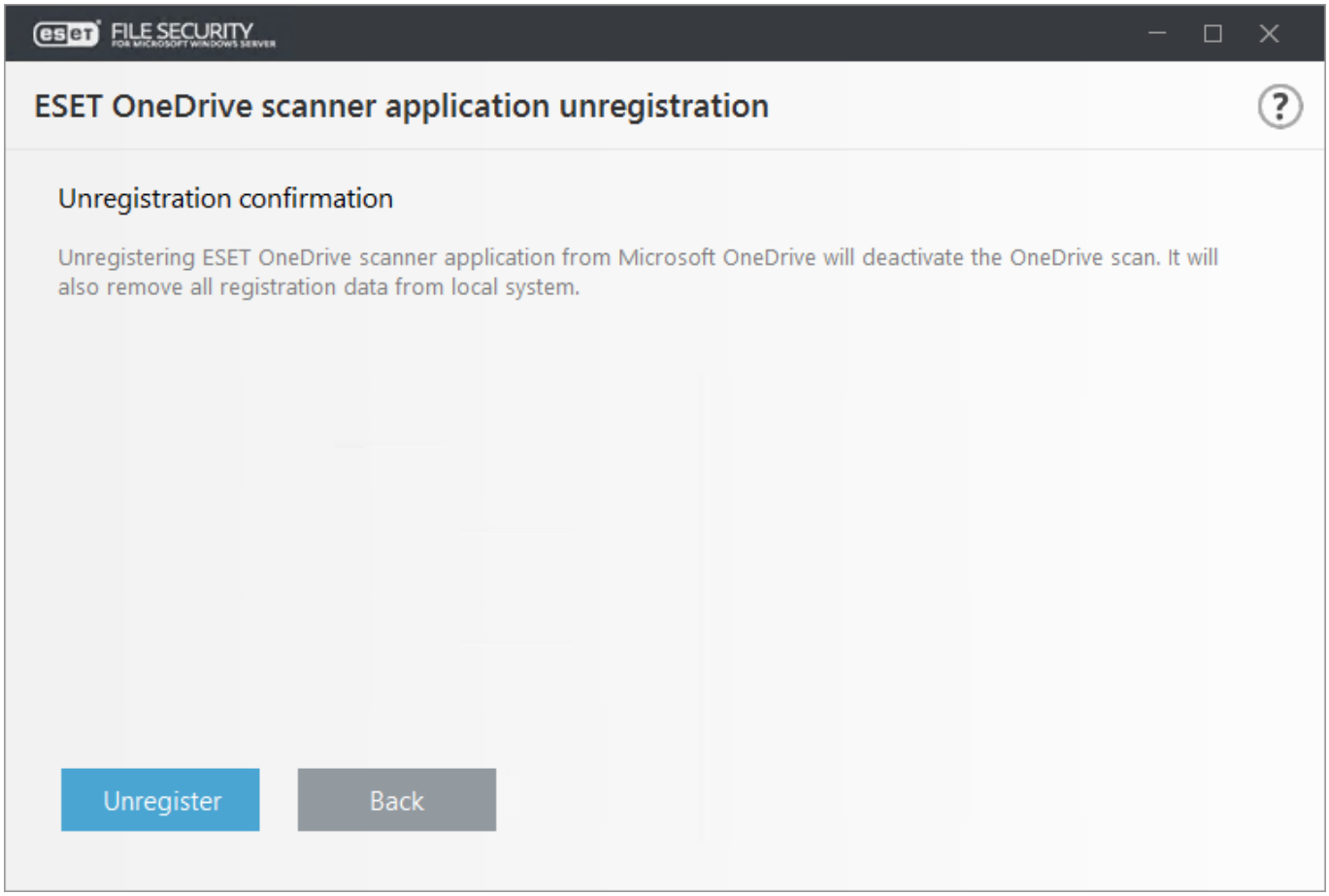
取消註冊 ESET OneDrive 掃描器

開啟 ESET File Security
按一下［設定］>［伺服器*] > [OneDrive* 掃描設定］>［取消註冊］ 
取消註冊程序可讓您從 Microsoft OneDrive / Office 365 / Azure 中移除憑證和 ESET OneDrive 掃描器應用程式。此程序也會移除本機相依性，並使「註冊」選項再次可用。

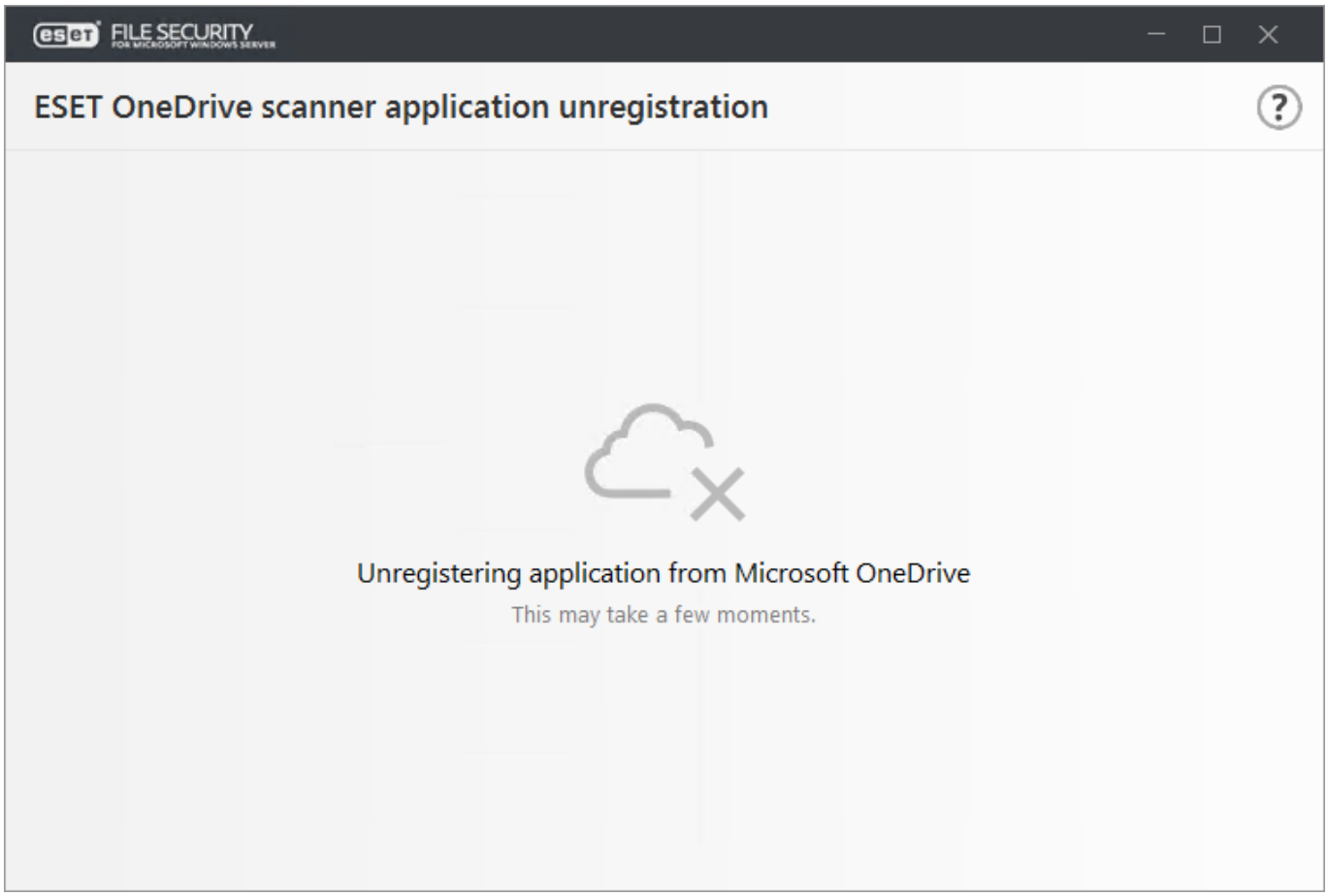
- 按一下［**取消註冊**］以開始 ESET OneDrive 掃描器取消註冊/移除程序，取消註冊精靈將會開啟。



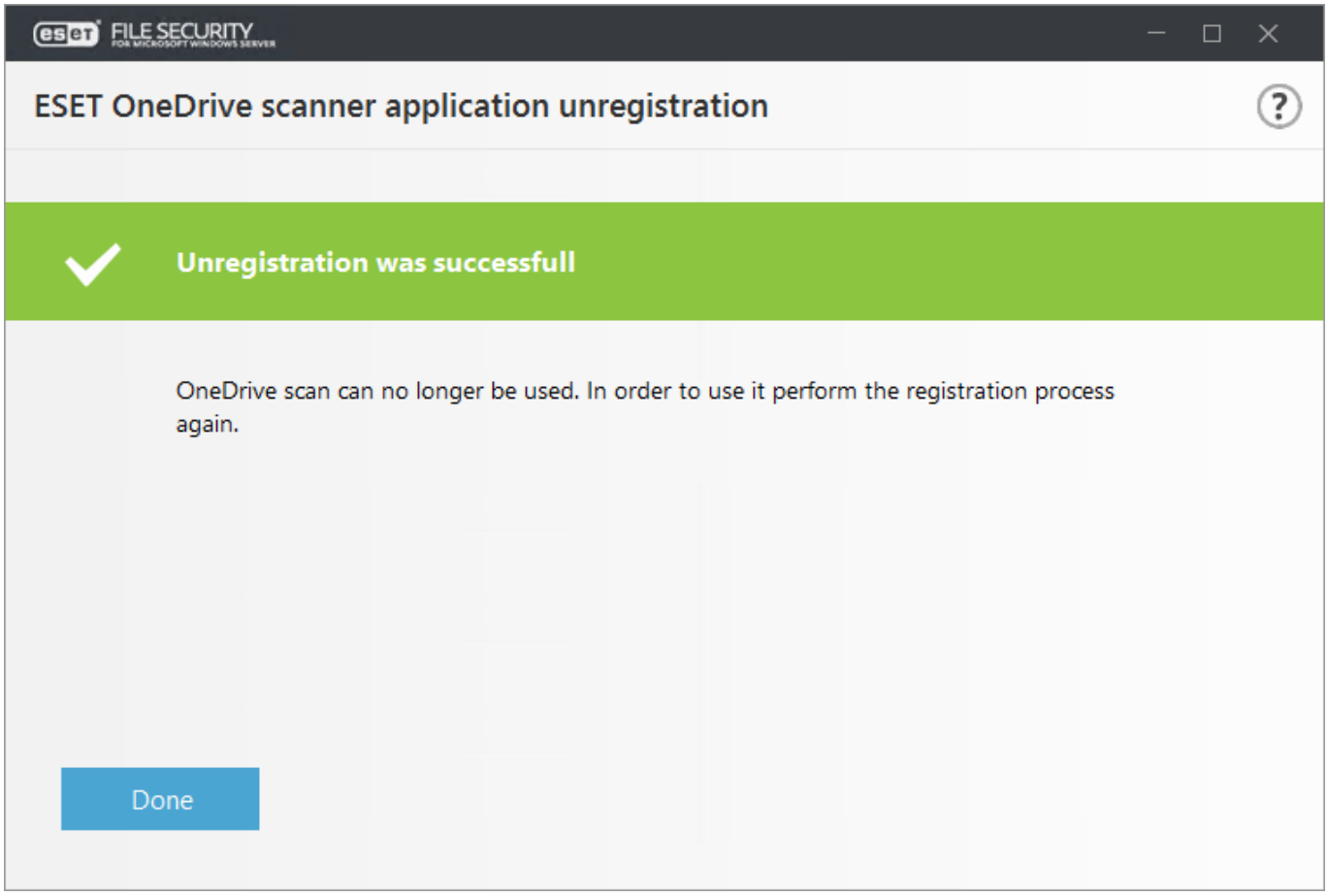
- 按一下［**取消註冊**］以確認您要移除 ESET OneDrive 掃描器。



- 等待從 Microsoft OneDrive 中取消註冊完成。



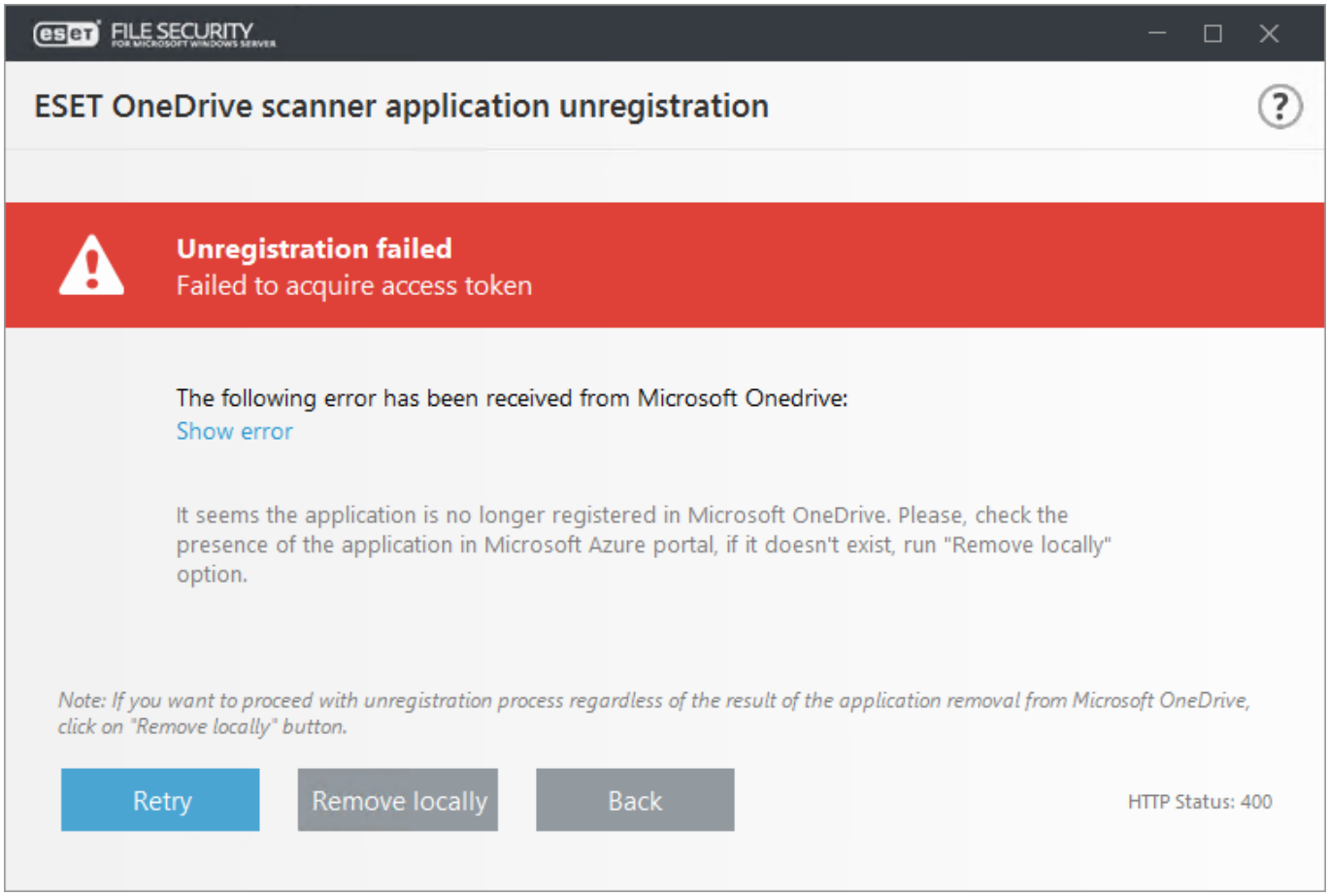
- 如果取消註冊程序成功完成，取消註冊精靈會顯示相關訊息。



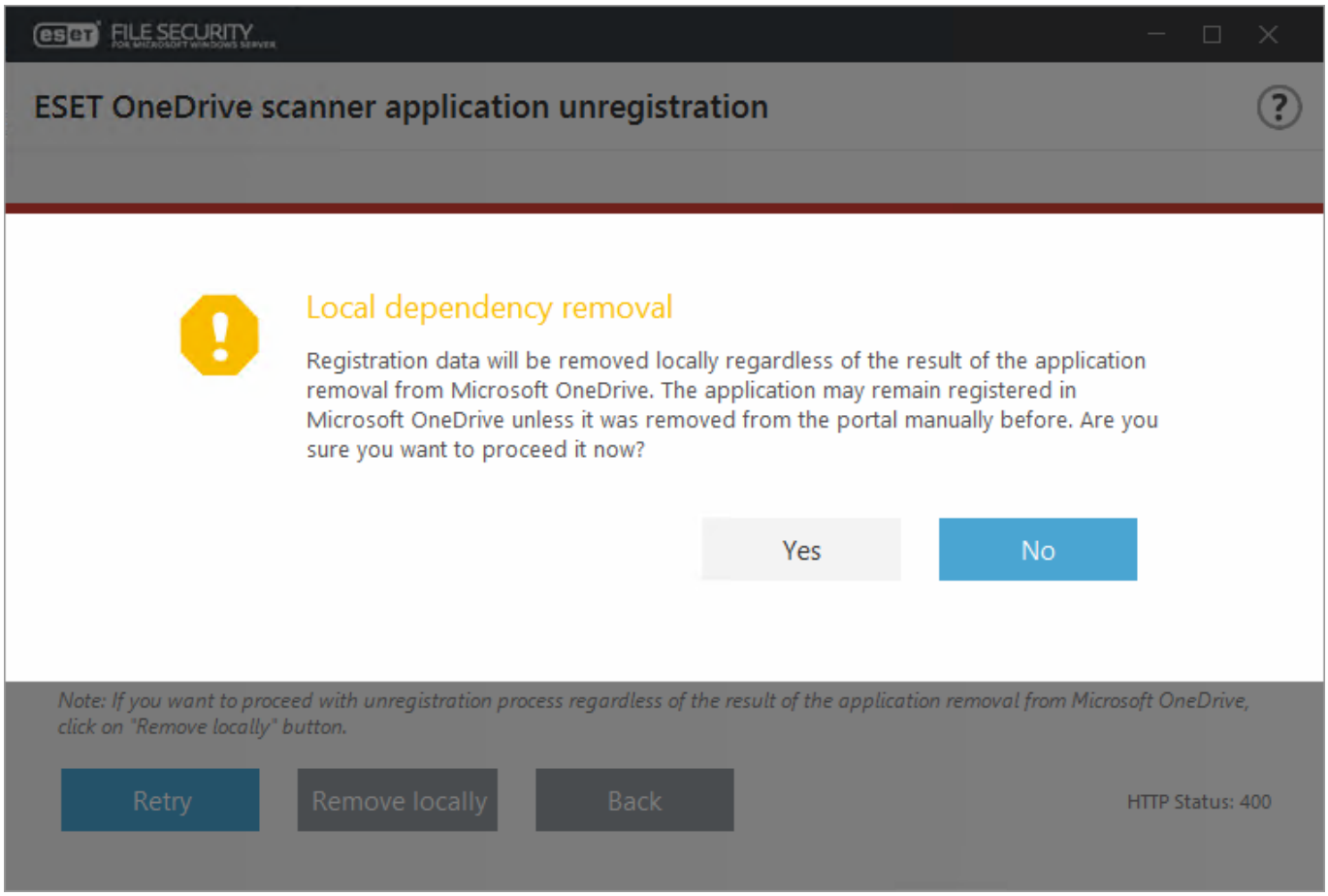
注意
如果您看到錯誤訊息（例如「取消註冊失敗」），可能是因為數個原因，例如 Microsoft OneDrive 伺服器的通用網路或網際網路連線問題，或 ESET OneDrive 掃描器應用程式不再向 Microsoft OneDrive 註冊。請參閱下表以取得錯誤訊息清單以及解決方式。

某些錯誤對話方塊可讓您選擇移除本機相依性（連線問題、Microsoft OneDrive 中不存在應用程式等）。若要於本機移除 ESET OneDrive 掃描器，請執行下列動作：

- 如果**［重試］**按鈕無法運作而問題持續存在，請按一下**［於本機移除］**以繼續執行取消註冊程序，這會移除 ESET OneDrive 掃描器本機相依性。



• 按一下［**是**］以繼續於本機移除 ESET OneDrive 掃描器ESET OneDrive 掃描將無法再使用。若要使用，您需要再次執行註冊程序。



重要
移除本機相依性不會變更 Azure 入口網站上的［應用程式註冊］，也不會變更 Office 365 入口網站上的［應用程式權限］。如果您由於 Microsoft OneDrive 伺服器的網路或連線問題而在本機移除了 ESET OneDrive 掃描器程序，則需要從 Azure 的［應用程式註冊］中手動移除 ESET OneDrive 掃描器應用程式。請參閱《OneDrive 掃描設定》「如何在 Azure 入口網站中手動尋找和刪除 ESET OneDrive 掃描器」。

如果您在 ESET OneDrive 掃描器取消註冊期間遇到任何下列錯誤訊息，請查看錯誤訊息詳細資料以取得建議的解決方案：

錯誤訊息	錯誤訊息詳細資料
無法連線至 Azure 應用程式。沒有網際網路連線。	檢查您的網路/網際網路連線，然後再次執行取消註冊。如果您想在未從 Microsoft OneDrive 移除 ESET OneDrive 掃描器應用程式的情況下繼續進行取消註冊程序，請按一下 **［於本機移除］**
無法取得存取 Token 收到來自 Microsoft OneDrive 的非預期錯誤。	ESET OneDrive 掃描器應用程式似乎不再在 Microsoft OneDrive 上註冊 ESET OneDrive 掃描器應用程式可能已在 Azure 入口網站中遭手動刪除。請檢查 Microsoft OneDrive 或 Azure 入口網站中是否存在 ESET OneDrive 掃描器應用程式。如果應用程式並未列出，請按一下 **［於本機移除］** 繼續執行取消註冊程序。
無法取得存取 Token 收到來自 Microsoft OneDrive 的伺服器錯誤。	Microsoft OneDrive 已傳回 HTTP 5xx 錯誤。目前無法完成取消註冊工作，請稍後再次嘗試執行取消註冊工作。
收到下列來自 Microsoft OneDrive 的錯誤。	Microsoft OneDrive 伺服器傳回錯誤，並包含特定錯誤代碼/名稱，請按一下 **［顯示錯誤］**
另一項設定工作已在進行中。	這是執行中的取消註冊工作。請等待上一個取消註冊程序完成。

一般設定

您可以根據自身需求來配置設定和選項。左邊的功能表包含下列類別：

偵側引擎

啟用或停用潛在不需要、不安全、可疑的應用程式偵測及反隱藏防護。指定要排除的處理程序或檔案及資料夾。配置即時檔案系統防護 ThreatSense 參數、雲端式防護 (ESET LiveGrid®) 惡意軟體掃描（指定電腦掃描及其他掃描選項) Hyper-V 掃描及 HIPS

［更新］

配置設定檔、偵測引擎年限、模組還原快照、更新類型、自訂更新伺服器、連線/Proxy 伺服器、更新鏡像、更新檔案之存取權限 HTTP 伺服器、網路連線的使用者帳戶詳細資料等更新選項。

Web 和電子郵件

可讓您設定通訊協定篩選及排除（排除的應用程式及 IP 位址) SSL/TLS 通訊協定篩選選項、電子郵件用戶端防護（整合、電子郵件通訊協定、警告及通知) Web 存取防護 (HTTP/HTTPS Web 通訊協定及 URL 位址管理）及電子郵件用戶端防網路釣魚防護。

裝置控制

啟用整合及設定裝置控制規則和群組。

工具配置

可讓您自訂工具，例如 ESET CMD、ESET RMM、WMI 提供者、ESET Security Management Center 掃描目標、Windows Update 通知、防護記錄檔案、Proxy 伺服器、電子郵件通知、診斷、叢集等。

使用者介面

設定程式的 GUI 行為、狀態、授權資訊、警告及通知、密碼防護、eShell 執行原則等。

偵側引擎

偵測引擎可藉由掃描檔案、電子郵件及網路通訊來防止惡意系統攻擊。如果偵測到分類為惡意軟體的物件，將會開始進行修復。偵測引擎可透過封鎖，接著清除、刪除或將其移至隔離區來消滅它。

即時及機器學習防護

進階機器學習現在是偵測引擎的一部分，會根據機器學習改善偵測，為您提供更進階的多一層防護。請參閱字彙 深入瞭解此防護類型。您可以配置下列類別的報告和防護層級：

惡意軟體

電腦病毒是一段惡意程式碼，其會加在您電腦上現有檔案的前面或後面。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。請在字彙中閱讀更多有關這些類型應用程式的資訊。

潛在不需要的應用程式 (PUA)

潛在不需要的應用程式是一種軟體，其意圖明確地不是惡意，但是它可能安裝其他不需要的軟體、變更數位裝置的行為、執行未經使用者認可或期待的活動或具有不明企圖的程式。
此類別包含：廣告顯示軟體、下載包裝函式、各種瀏覽器工具列、具有誤導行為的軟體、混入軟體、追蹤軟體等等。
請在字彙中閱讀更多有關這些類型應用程式的資訊。

潛在可疑的應用程式

係指附帶以加殼或保護工具壓縮的軟體，此兩者常用於使用專利壓縮和/或加密方式來防止反向工程或混淆執行檔內容（例如藏匿惡意軟體）。
此類別包含：所有以加殼或保護工具（常用於壓縮惡意軟體）壓縮的未知應用程式。

潛在不安全的應用程式

此分類適用於可能遭到惡意濫用的商業、合法軟體。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。
此分類包含：破解工具、授權金鑰產生器、駭客攻擊工具、遠端存取或控制工具、密碼破解應用程式及鍵盤記錄程式（記錄每次使用者按鍵的程式）。依預設會停用此選項。
請在字彙中閱讀更多有關這些類型應用程式的資訊。

請先閱讀下列說明，然後再修改類別報告或防護的閥值（或層級）：

報告

報告是由偵測引擎和機器學習元件所執行。您可以設定報告閥值，以便符合您的環境和需求。並沒有唯一一個正確的配置。因此我們建議您監控環境的行為，然後才決定是否不同的報告設定會更加適合您。

報告並不會和物件進行互動，而會將資訊傳給個別的防護層級，然後防護層級才會根據資訊採取動作。

越權	**報告已配置為最高敏感性。將會報告更多的偵測。儘管越權設定可能看起來最安全，但也經常太過敏感，可能導致適得其反。** 注意 越權設定可能錯誤識別物件為惡意，將會對該物件採取動作（根據防護設定）。
平衡	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，報告配置為盡量減少錯誤識別物件。只有在可能性顯而易見且符合惡意行為時，才會報告物件。
關閉	報告未啟用。找不到、已報告或已清除的偵測。 注意 無法停用惡意軟體報告；因此**［關閉］**設定不適用於惡意軟體。

如果您要將此區段中的設定還原為其預設值，請按一下區段標頭旁的「迴轉」箭頭。您在此區段完成的任何變更都會遺失。

防護

當根據上述配置和機器學習結果報告物件時，該物件會遭到封鎖，且會採取動作（已清除、已刪除或移動到隔離區）。

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）。**
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	報告未啟用。找不到、已報告或已清除的任何偵測。 注意 無法停用惡意軟體報告，因此**［關閉］**設定不適用於惡意軟體。

如果您要將此區段中的設定還原為其預設值，請按一下區段標頭旁的「迴轉」箭頭。您在此區段完成的任何變更都會遺失。

注意
依預設，上述的機器學習防護設定也會套用到隨選電腦掃描。如果有需要，您可以另外配置**［隨選與機器學習防護］**設定。按一下切換圖示以停用**［使用即時防護設定］**然後繼續進行配置。

機器學習偵測

偵測引擎可藉由掃描檔案、電子郵件及網路通訊來防止惡意系統攻擊。如果偵測到分類為惡意軟體的物件，將會開始進行修復。偵測引擎可透過封鎖，接著清除、刪除或將其移至隔離區來消滅它。

即時及機器學習防護

進階機器學習現在是偵測引擎的一部分，會根據機器學習改善偵測，為您提供更進階的多一層防護。請參閱字彙 深入瞭解此防護類型。您可以配置下列類別的報告和防護層級：

惡意軟體

電腦病毒是一段惡意程式碼，其會加在您電腦上現有檔案的前面或後面。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。請在字彙中閱讀更多有關這些類型應用程式的資訊。

潛在不需要的應用程式 (PUA)

潛在不需要的應用程式是一種軟體，其意圖明確地不是惡意，但是它可能安裝其他不需要的軟體、變更數位裝置的行為、執行未經使用者認可或期待的活動或具有不明企圖的程式。
此類別包含：廣告顯示軟體、下載包裝函式、各種瀏覽器工具列、具有誤導行為的軟體、混入軟體、追蹤軟體等等。
請在字彙中閱讀更多有關這些類型應用程式的資訊。

潛在可疑的應用程式

係指附帶以加殼或保護工具壓縮的軟體，此兩者常用於使用專利壓縮和/或加密方式來防止反向工程或混淆執行檔內容（例如藏匿惡意軟體）。
此類別包含：所有以加殼或保護工具（常用於壓縮惡意軟體）壓縮的未知應用程式。

潛在不安全的應用程式

此分類適用於可能遭到惡意濫用的商業、合法軟體。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。
此分類包含：破解工具、授權金鑰產生器、駭客攻擊工具、遠端存取或控制工具、密碼破解應用程式及鍵盤記錄程式（記錄每次使用者按鍵的程式）。依預設會停用此選項。
請在字彙中閱讀更多有關這些類型應用程式的資訊。

請先閱讀下列說明，然後再修改類別報告或防護的閥值（或層級）：

報告

報告是由偵測引擎和機器學習元件所執行。您可以設定報告閥值，以便符合您的環境和需求。並沒有唯一一個正確的配置。因此我們建議您監控環境的行為，然後才決定是否不同的報告設定會更加適合您。

報告並不會和物件進行互動，而會將資訊傳給個別的防護層級，然後防護層級才會根據資訊採取動作。

越權	**報告已配置為最高敏感性。將會報告更多的偵測。儘管越權設定可能看起來最安全，但也經常太過敏感，可能導致適得其反。** 注意 越權設定可能錯誤識別物件為惡意，將會對該物件採取動作（根據防護設定）。
平衡	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，報告配置為盡量減少錯誤識別物件。只有在可能性顯而易見且符合惡意行為時，才會報告物件。
關閉	報告未啟用。找不到、已報告或已清除的偵測。 注意 無法停用惡意軟體報告；因此［**關閉**］設定不適用於惡意軟體。

如果您要將此區段中的設定還原為其預設值，請按一下區段標頭旁的「迴轉」箭頭。您在此區段完成的任何變更都會遺失。

OneDrive 及機器學習防護

報告

由偵測引擎和機器學習元件執行。報告並不會對物件採取動作（這是由個別的防護層級進行）。

防護

配置在 OneDrive 區段中的參數會影響對報告物件採取的動作。

如果您要將此區段中的設定還原為其預設值，請按一下區段標頭旁的「迴轉」箭頭。您在此區段完成的任何變更都會遺失。

使用 eShell 配置機器學習防護。eShell 中的內容名稱為 **MLP**。請在互動模式中開啟 eShell 然後導覽至 MLP。

```
computer onedrive mlp
```

查看可疑應用程式目前的報告設定：

```
get suspicious-reporting
```

如果您希望報告不要太過嚴格，請將設定變更為警告：

```
set suspicious-reporting cautious
```

排除

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

> 警告
> 請注意不要與排除的副檔名、程序排除或排除過濾器混淆。

> 注意
> 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。

選取排除類型，再按一下 **[編輯]** 以新增項目或修改現有項目：

- [效能排除] – 可讓您從掃描排除檔案及資料夾。
- [偵測排除] – 使用特定準則從掃描排除物件 – 路徑、檔案雜湊或偵測名稱。

效能排除

此功能允許您從掃描排除檔案和資料夾。效能排除在用於排除關鍵任務應用程式的檔案層級掃描，或是當掃描造成系統行為異常/降低效能時很有幫助。

路徑

排除此電腦的特定（檔案或目錄）路徑。請勿在路徑中間使用萬用字元 – 星號（*）。請參閱下列知識庫文章取得更多資訊。

注意
若要排除資料夾內容，請別忘了在路徑（*C:\Tools**）結尾處加上星號（*）。將不會排除 *C:\Tools*，因為從掃描器的觀點看來，工具也可能是一個檔案名稱。

註解

新增選用**備註**以便在將來輕鬆辨識排除。

範例
使用星號來排除路徑：
*C:\Tools** – 路徑必須以反斜線（\）及星號（*）結尾，指出它是一個資料夾，而且會排出所有資料夾內容（檔案及子資料夾）
C:\Tools.** – 與 *C:\Tools** 相同的行為，代表會以遞迴方式進行
C:\Tools.dat* – 將會排除工具資料夾中的 *dat* 檔案
C:\Tools\sg.dat – 將會排除在確切路徑中的此檔案

範例
若要排除資料夾中的所有檔案，請輸入資料夾的路徑並使用遮罩 *.**
• 若要排除包含所有檔案與子資料夾的整個磁碟機，請使用遮罩 *D:**
• 若只要排除 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（問號取代遺漏/未知字元）

範例
使用如 *%PROGRAMFILES%* 等系統變數來定義掃描排除。
• 如要使用此系統變數來排除 Program Files 資料夾，請使用以下路徑 *%PROGRAMFILES%*（新增至排除時，請確保在路徑末端加上反斜線）
• 如果您要排除子目錄 *%HOMEDRIVE%* 中的所有檔案，請使用路徑 *%HOMEDRIVE%\Excluded_Directory*.**
以下變數可用於路徑排除格式：
%ALLUSERSPROFILE%
%COMMONPROGRAMFILES%
%COMMONPROGRAMFILES(X86)%
%COMSPEC%
%HOMEDRIVE%
%HOMEPATH%
%PROGRAMFILES%
%PROGRAMFILES(X86)%
%SystemDrive%
%SystemRoot%
%WINDIR%
%PUBLIC%
不支援使用者專用系統變數（如 *%TEMP%* 或 *%USERPROFILE%*）或環境變數（或 *%PATH%*)

偵測排除

這是另一種從掃描排除物件的方法，使用偵測名稱、路徑或其雜湊。偵測排除不會從檔案和資料夾排除檔案（例如效能排除）。只有當偵測引擎偵測到物件，並且在排除清單中有適當的規則存在時，偵測排除才會排除物件。

建立偵測型排除最簡單的方法便是從 **[防護記錄檔案]** > [偵測] 使用現有的偵測排除。滑鼠右鍵按一下防

護記錄（偵測），然後再按一下 **[建立排除]**。便會開啟含有預定義準則的排除精靈

若要手動建立偵測排除，請按一下 **[編輯]** > **[新增]**（或是當修改已存在時改用 **[編輯]**）然後指定一個或多個下列準則（可以為組合準則）：

路徑

排除此電腦的特定（檔案或目錄）路徑。您可以瀏覽尋找特定的位置/檔案，或是手動輸入字串。請勿在路徑中間使用萬用字元 – 星號（*）。請參閱下列知識庫文章取得更多資訊。

注意
若要排除資料夾內容，請別忘了在路徑（*C:\Tools**）結尾處加上星號（*）。將不會排除 *C:\Tools*，因為從掃描器的觀點看來，工具也可能是一個檔案名稱。

雜湊

根據指定的雜湊 (SHA1) 排除檔案，無論檔案類型、位置、名稱或其副檔名為何。

偵測名稱

輸入有效的偵測（威脅）名稱。如果只根據偵測名稱建立排除，可能會有安全性上的風險。我們建議您結合偵測名稱和路徑。排除準則只能用於特定類型的偵測。

註解

新增選用**備註**以便在將來輕鬆辨識排除。

ESET Security Management Center 包含偵測管理排除 以建立排除並將之套用到更多電腦/群組。

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

範例
使用星號來排除路徑：
*C:\Tools** – 路徑必須以反斜線（\）及星號（*）結尾，指出它是一個資料夾，而且會排出所有資料夾內容（檔案及子資料夾）
C:\Tools.** – 與 *C:\Tools** 相同的行為，代表會以遞迴方式進行
C:\Tools.dat* – 將會排除工具資料夾中的 *dat* 檔案
C:\Tools\sg.dat – 將會排除在確切路徑中的此檔案

範例
如果您想要排除威脅，請依下列格式輸入有效的偵測名稱：
@NAME=Win32/Adware.Optmedia
@NAME=Win32/TrojanDownloader.Delf.QQI
@NAME=Win32/Bagle.D

範例
若要排除資料夾中的所有檔案，請輸入資料夾的路徑並使用遮罩 **.**
• 若要排除包含所有檔案與子資料夾的整個磁碟機，請使用遮罩 *D:**
• 若只要排除 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（問號取代遺漏/未知字元）

範例
使用如 *%PROGRAMFILES%* 等系統變數來定義掃描排除。
• 如要使用此系統變數來排除 Program Files 資料夾，請使用以下路徑 *%PROGRAMFILES%*（新增至排除時，請確保在路徑末端加上反斜線）
• 如果您要排除子目錄 *%HOMEDRIVE%* 中的所有檔案，請使用路徑 *%HOMEDRIVE%\Excluded_Directory*.**
以下變數可用於路徑排除格式：
%ALLUSERSPROFILE%
%COMMONPROGRAMFILES%
%COMMONPROGRAMFILES(X86)%
%COMSPEC%
%HOMEDRIVE%
%HOMEPATH%
%PROGRAMFILES%
%PROGRAMFILES(X86)%
%SystemDrive%
%SystemRoot%
%WINDIR%
%PUBLIC%
不支援使用者專用系統變數（如 *%TEMP%* 或 *%USERPROFILE%*）或環境變數（或 *%PATH%*）

建立排除精靈

會依據偵測類型來預先選取建議的排除，但您可以進一步指定偵測的排除準則。請按一下 **[變更準則]**。

- **[確切檔案]** – 依其 SHA-1 雜湊排除每個檔案。
- **[偵測]** – 指定偵測名稱，然後排除每個檔案含有該偵測的檔案。
- **[路徑 + 偵測]** – 指定偵測名稱和路徑（包含檔案名稱），然後排除每個在指定位置含有偵測的檔案。

新增選用**備註**以便在將來輕鬆辨識排除。

進階選項

反隱藏技術

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

AMSI

讓 Microsoft Antimalware Scan Interface (AMSI) 掃描 Windows 指令碼主機執行的 Powershell 指令碼。

自動排除

伺服器應用程式及作業系統的開發人員建議將許多重要的工作檔案及資料夾排除在大多數產品的惡意軟體掃描之外。惡意軟體掃描對於伺服器的效能有負面影響，可能會導致衝突，甚至會使得某些應用程式無法在伺服器上執行。排除有助於將潛在衝突的風險降至最低，並提升執行惡意軟體防護軟體時的伺服器整體效能。請參閱從 ESET 伺服器產品掃描排除的完整排除檔案清單。

ESET File Security 可識別重要的伺服器應用程式及伺服器作業系統檔案，並自動將這些新增至排除清單中。所有的自動排除皆預設為已啟用。您可以使用滑動軸來停用/啟用每個伺服器應用程式，結果如下：

- 啟用後，任何重要的檔案及資料夾皆會新增到排除於掃描的檔案清單。每次伺服器重新啟動時，系統都將執行排除的自動檢查，並在系統或應用程式發生變更（例如，安裝新的伺服器應用程式）時更新該清單。此設定確保系統會一律套用建議的自動排除。
- 停用後，自動排除的檔案和資料夾將從清單中移除。任何手動輸入的使用者定義排除將不受影響。

ESET File Security 使用位於安裝資料夾中的專用應用程式 *eAutoExclusions.exe* 進行識別和產生自動排除。您不需要進行任何互動，但您可以執行 `eAutoExclusions.exe -servers`，使用命令列來列出在系統上偵測到的伺服器應用程式。若要顯示完整語法，請使用 `eAutoExclusions.exe -?`。

共用本機快取

ESET 共用本機快取會減少網路中的重複掃描，進而提高虛擬環境的效能。這樣可確保每個檔案僅會掃描一次，並存放在共用快取中。開啟 **[快取選項]** 切換，將掃描您網路中檔案與資料夾的資訊儲存到本機快取。若您執行新掃描，ESET File Security 將搜尋快取中的已掃描檔案。若檔案相符，則其將從掃描中排除。

快取伺服器包括下列設定：

- **主機名稱** – 快取所在電腦的名稱或 IP 位址。
- **連接埠** – 用於通訊的連接埠號碼（與共用本機快取中的設定相同）。
- **密碼** – 指定共用本機快取密碼（如果需要的話）。

偵測到入侵

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

標準行為

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

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

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

清除及刪除

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

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

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

多種威脅

如果在電腦掃描期間沒有清除任何受感染的檔案（或清除層級設為 **[不清除]**），則警告視窗會提示您針對顯示的那些檔案選取處理方法。針對清單中的每一項威脅個別選取動作，或者您可以使用 **[對所有列出的威脅選取處理方法]** 並選擇要對清單中所有威脅執行的動作，然後按一下 **[完成]**。

刪除壓縮檔中的檔案

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

即時檔案系統防護

即時檔案系統防護控制系統中與惡意軟體相關的所有事件。在電腦上開啟、建立或執行所有檔案時，都會掃描這些檔案是否具有惡意代碼。依預設，即時檔案系統防護會在系統啟動時同時啟動，並持續提供掃描。在特殊情況下（例如，如果與其他即時掃描器發生衝突），則可以解除 **[即時檔案系統防護] > [基本]** 下 **[進階設定] (F5)** 中的 **[自動啟動即時檔案系統防護]**，以停用即時防護。

要掃描的媒體

依預設，會掃描所有媒體類型是否有潛在的威脅：

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

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

執行掃描的時間

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

- **[開啟檔案]** – 在開啟/存取檔案時掃描。
- **[建立檔案]** – 在建立/修改檔案時掃描。
- **[執行檔案]** – 在執行檔案時掃描。
- **[卸除式媒體存取]** – 存取卸除式儲存裝置時掃描。當包含開機磁區的卸除式媒體插入裝置時，便會立即掃描開機磁區。此選項並不會啟用卸除式媒體的媒體掃描。卸除式媒體檔案掃描位於 **[待掃描媒體] > [卸除式媒體]**。為確保卸除式媒體開機磁區能正確運作，請在 ThreatSense 參數中保持 **[開機磁區/UEFI 啟用]**。

程序排除

可讓您排除特定程序。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，因此可將備份程序的干擾降到最低。

ThreatSense 參數

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。即時檔案系統防護可配置為將新建立檔案視為與現有檔案不同。例如，您可以設定即時檔案系統防護以更密切監視新建立的檔案。

為確保在使用即時防護時佔用最低的系統使用量，已掃描的檔案不予重複掃描（除非已經過修改）。每次更新偵測引擎資料庫之後，會立即重新掃描檔案。使用 **[智慧型最佳化]** 可控制此行為。如果停用 **[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，按一下 **F5** 以開啟 **[進階設定]** 並展開 **偵側引擎 > [即時檔案系統防護]**。按一下 **[ThreatSense 參數] > [其他]** 並選取或取消選取 **[啟用智慧型最佳化]**。

其他 ThreatSense 參數

您可以修改 **[用於新建立及修改檔案的其他 ThreatSense 參數]** 或 **[執行檔案的其他 ThreatSense 參數]** 的詳細選項。

ThreatSense 參數

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

> 注意
> 如需有關自動啟動檔案檢查的詳細資訊，請參閱啟動掃描。

ThreatSense 引擎設定選項可讓您指定數個掃描參數：

- **要掃描的檔案類型及副檔名**
- **各種偵測方法的組合**
- **清除層級等**

若要進入設定視窗，請按一下任何使用 ThreatSense 技術之任何模組的 **[進階設定](F5)** 視窗中的 **[ThreatSense 引擎參數設定]**（如下所示）。不同的安全情況可能需要不同的設定。瞭解這一點之後，就可針對下列防護模組，分別進行 ThreatSense 配置：

- Hyper-V 掃描
- OneDrive 掃描
- 即時檔案系統防護
- 惡意軟體掃描
- 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

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 MBR (主要開機記錄）中是否有病毒。若為 Hyper-V 虛擬機器，其磁碟 MBR 是以唯讀模式進行掃描。

電子郵件檔案

程式支援下列副檔名: DBX (Outlook Express) 和 EML

壓縮檔

程式支援下列副檔名ARJBZ2CABCHMDBXGZIPISO/BIN/NRGLHAMIMENSISRARSISTARTNEFUUEWISEZIPACE及許多其他副檔名。

自解壓縮檔

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

加殼技術虛擬機偵測

執行之後，加殼技術虛擬機偵測（不同於標準壓縮檔類型）會在記憶體中解壓縮。除了標準靜態壓縮器 (UPXyodaASPackFSG 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，在於可以識別不存在或偵測引擎先前不瞭解的惡意軟體。

進階啟發式/DNA 簽章

進階啟發式是由ESET開發的獨特啟發式演算法所組成，經過最佳化以偵測電腦蠕蟲及特洛伊木馬程式，並以高階程式設計語言撰寫。使用進階啟發式能大幅提高 ESET 產品的威脅偵測能力。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

清除設定會決定在掃描器清除受感染檔案期間的行為。有 3 個清除層級：

不清除

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

正常清除

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

完全清除

程式會清除或刪除所有受感染檔案。只有系統檔案例外。當無法清除檔案時，系統將詢問使用者要執行哪一種處理方法。

警告
如果壓縮檔包含受感染的檔案，則您可以選用兩個選項來處理壓縮檔。在預設模式的［**正常清除**］中，如果所有包含的檔案受到感染，整個壓縮檔將會刪除。在［**完全清除**］模式中，當壓縮檔內含有至少一個受感染的檔案時，即會刪除壓縮檔，無論壓縮檔中其他檔案的狀態為何。

重要
如果 Hyper-V 主機是在 Windows Server 2008 R2 SP1 上執行，則不支援［**正常清除**］和［**完全清除**］。虛擬機器磁碟的掃描是以唯讀模式執行，將不會執行清除。不論您所選取的清理層級為何，掃描一律會以唯讀模式執行。

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。此 ThreatSense 參數設定的區段可讓您定義要從掃描排除的檔案類型。

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。

以低優先級別執行背景掃描

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

記錄所有物件

如果已選取此選項，防護記錄檔案會顯示所有已掃描的檔案(即使檔案未受感染)。

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。若停用「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：

預設物件設定

- 啟用以使用預設設定（無限制)ESET File Security 將會忽略您的自訂設定。

物件大小上限

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

物件的掃描時間上限（秒）

定義掃描物件的時間值上限。如果已在這裡輸入使用者定義的值，則當該時間到期，防護模組會停止掃描物件，無論掃描是否完成。預設值：無限制

壓縮檔掃描設定

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]**

壓縮檔巢狀層級

指定壓縮檔掃描的深度上限。預設值：10。針對信箱傳輸防護偵測到的物件，實際巢狀層級為 +1，因為電子郵件中的壓縮檔附件視為第一層級。

> 範例
> 若您將巢狀層級設為 3，則只會在傳輸層達到實際層級 2 時，掃描巢狀層級 3 的壓縮檔。因此，若您想要信箱傳輸防護達到層級 3 時掃描壓縮檔，請將 **[壓縮檔巢狀層級]** 的值設為 4。

壓縮檔中檔案的大小上限

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

> 注意
> 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。

其他 ThreatSense 參數

用於新建立及修改檔案的 ThreatSense 參數

新建立或已修改檔案感染的可能性高於現有的檔案。這正是為何程式會以額外的掃描參數檢查這些檔案的原因。除了常見的病毒碼掃描方法，也會使用進階啟發式在模組更新發行前先偵測新的威脅。除了新建立的檔案之外，可針對自我解壓檔 (.sfx) 及 運行時間壓縮器（內部壓縮的執行檔案）執行掃描。依預設，至多可以掃描至保存檔的第 10 層巢狀層級，並不論其實際大小都會進行檢查。若要修改壓縮檔掃描設定，請停用 **[預設壓縮檔掃描設定]**

用於已執行檔案的其他 ThreatSense 參數

根據預設，執行檔案時會使用進階啟發式。啟用這項功能時，我們強烈建議您讓智慧型最佳化和 ESET

LiveGrid® 保持運作，以減輕對系統效能的影響。

從掃描中排除的檔案副檔名

副檔名是檔案名稱中以句點隔開的部份。副檔名定義檔案的類型及內容。正常情況下，會掃描所有檔案。不過，如果您需要執行具有特定副檔名的檔案ThreatSense 參數設定讓您可以從掃描中根據副檔名排除檔案。如果掃描特定檔案類型可防止應用程式適當執行，排除則可能很實用。

範例
若要將新的副檔名新增到清單，按一下 **[新增]**。在文字欄位中輸入副檔名（例如，`tmp`）並按一下 **[確定]**。當您選取 **[輸入多個值]**，您可以新增多個以行、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）。問號代表任何字符（例如 `?db`)

注意
若要在 Windows 作業系統內顯示所有檔案的副檔名（檔案類型），請取消選取 **[控制台] > [資料夾選項] > [檢視]** 下的 **[隱藏已知檔案類型的副檔名]**

程序排除

「程序排除」功能可讓您僅從惡意軟體防護存取掃描中排除應用程式程序。由於專用伺服器（應用程式伺服器、儲存區伺服器等）的角色非常重要，因此會強制執行定期備份以保證從任何類型的事件及時復原。為了改善備份速度、程序完整性和服務可用性，備份期間將會使用已知與檔案層級惡意軟體防護衝突的某些技術。嘗試即時遷移虛擬機器時也會發生類似問題。要避免這兩種情況發生，唯一的有效方法是停用惡意軟體防護軟體。透過排除程序（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，因此可將備份程序的干擾降到最低。我們建議您小心建立排除 – 已排除的備份工具可以存取受感染的檔案，而不會觸發警告，這便是僅在即時防護模組中允許擴充權限的原因。

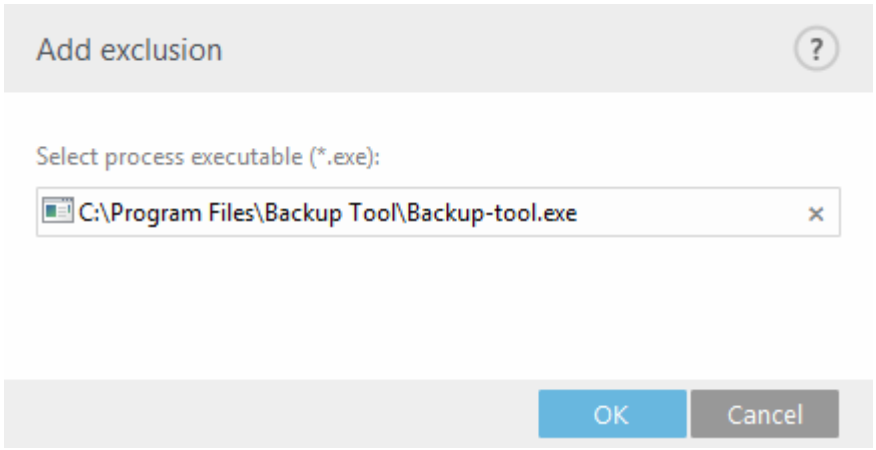
「程序排除」有助於將潛在衝突的風險降至最低，並提升排除應用程式的效能，因此對作業系統的整體效能與穩定性具有正面效果。程序/應用程式的排除是其可執行檔（*.exe*）的排除。

您可以透過 **[進階設定] (F5) > 偵側引擎 > [即時檔案系統防護] > [基礎] > [程序排除]** 或是從主要功能表 **[工具] > [執行中的處理程序]** 使用執行中的處理程序清單，然後將可執行檔新增至排除的程序。

此功能設計旨在排除備份工具。從掃描排除備份工具程序不僅可確保系統穩定性，而且不會影響備份效能，因為在備份時，備份速度並不會減緩。

範例
按一下 **[編輯]** 開啟 **[程序排除]** 管理視窗，您可以在其中 **[新增]** 排除並瀏覽可執行檔（例如，*Backup-tool.exe*），該檔案會被排除在掃描範圍外。
只要將 *.exe* 檔案新增至排除ESET File Security 不會監控排除此程序的活動，且不會針對該程序執行的任何檔案作業執行任何掃描。

重要
如果您在選取可執行的程序時並未使用瀏覽功能，您必須手動輸入可執行檔的完整路徑。或者，排除無法正確運作且 HIPS 可能會報告錯誤。



您也可以［**編輯**］現有的程序或是從排除加以［**刪除**］

注意
Web 存取防護不會考量此排除，因此如果您排除 Web 瀏覽器的執行檔，系統仍會掃描下載的檔案。如此一來，系統仍可偵測到入侵。此案例僅為範例，且我們不建議針對 Web 瀏覽器建立排除。

雲端式防護

ESET LiveGrid® 是進階的預早警告系統，結合多項雲端技術。其可根據聲譽協助偵測新出現的威脅，並透過白名單改善掃描效能。新的威脅資訊會即時串流到雲端，讓 ESET 惡意軟體研究實驗室能及時回應，並隨時提供一致的防護。使用者可直接從程式的介面或關聯式功能表，查看執行中的處理程序與檔案的聲譽，以及可從 ESET LiveGrid® 取得的其他資訊。

安裝 ESET File Security 時，請選取以下其中一個選項：

- 您可以決定不啟用 ESET LiveGrid®您的軟體不會失去任何功能，但在一些情況下ESET File Security 可能會比更新偵測引擎資料庫更慢回應新威脅。
- 您可以配置 ESET LiveGrid®以提交新威脅與偵測到新威脅代碼位置的匿名資訊。此檔案可傳送至 ESET以供詳細分析。研究這些威脅會協助 ESET 更新其威脅偵測能力。

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

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

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

資料將傳送至 ESET 研究實驗室以供進一步分析。

提交損毀報告與診斷資料

提交資料，例如損毀報告、模組或記憶體傾印。

提交匿名統計

可讓 ESET 收集有關新偵測到威脅的匿名資訊（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）、掃描的檔案（雜湊、檔案名稱、檔案來源、遙測）、已封鎖和可疑的 URL、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。請注意，除非需要更多資訊，否則您將不會收到 ESET 的任何回應。

提交樣本

自動提交受感染的樣本

這會將所有受感染的樣本傳送至 ESET 以供分析和提升未來偵測效果。

- 所有受感染的樣本
- 文件以外的所有樣本
- 不提交

自動提交可疑樣本

類似威脅的可疑範例，和/或有異常特性或行為的範例，可提交至 ESET 進行分析。

- **可執行檔** – 包含可執行檔：*.exe, .dll, .sys*
- **壓縮檔** – 包含壓縮檔檔案類型：*. zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab*
- **指令碼** – 包含指令碼檔案類型：*.bat, .cmd, .hta, .js, .vbs, .js, .ps1*
- **其他** – 包含檔案類型： *.jar, .reg, .msi, .swf, .lnk*
- **可能的垃圾電子郵件** – 改善全域的垃圾郵件偵測。
- **文件** – 包括含有啟用中內容的 Microsoft Office 文件或 PDF

排除

按一下 ESET LiveGrid® 排除旁的編輯選項可讓您配置將威脅提交至 ESET 病毒實驗室進行分析的方法。

樣本大小上限 (MB)

定義要掃描的樣本大小上限。

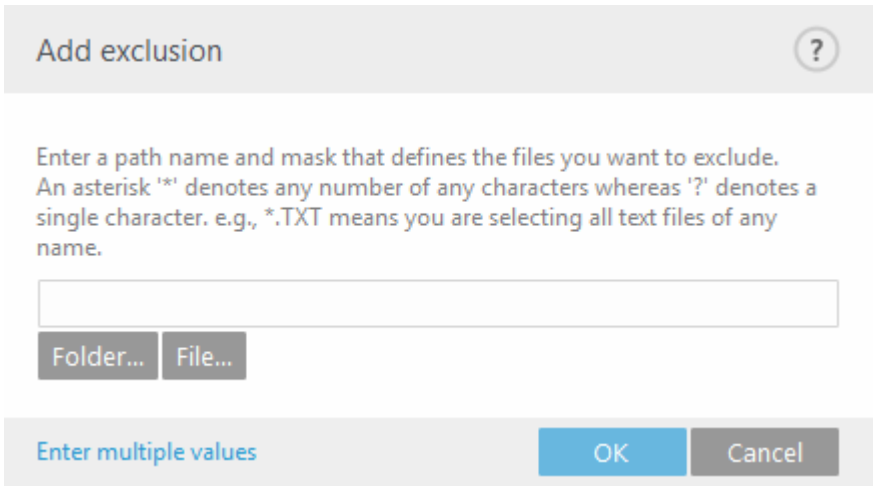
ESET Dynamic Threat Defense

在使用 ESMC Web Console 的用戶端機器上啟用 ESET Dynamic Threat Defense 服務。在 ESET Security Management Center Web 主控台中，在您希望使用 ESET Dynamic Threat Defense 的機器上建立新原則 或編輯現有原則並進行指派。

排除過濾

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

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



如果您找到可疑檔案，您可以提交給我們的威脅實驗室進行分析。若檔案為惡意的應用程式，則其偵測會新增到下一個偵測模組更新。

惡意軟體掃描

此區段提供選項以選取掃描參數。

> 注意
> 此掃描設定檔選擇器適用於［**指定掃描**］Hyper-V 掃描及 OneDrive 掃描

選取的設定檔

指定掃描器使用的一組特定參數。您可以使用其中一個預先定義的掃描設定檔或建立新設定檔。掃描設定檔會使用不同的 ThreatSense 引擎參數

設定檔清單

若要建立新參數，按一下［**編輯**］。輸入設定檔的名稱並按一下［**新增**］。新設定檔會顯示在［**選取的設定檔**］下拉式功能表中並列出現有的掃描設定檔。

掃描目標

若要掃描特定的目標，請按一下［**編輯**］並從下拉式功能表中選擇選項，或從資料夾（樹狀目錄）結構中選取特定目標。

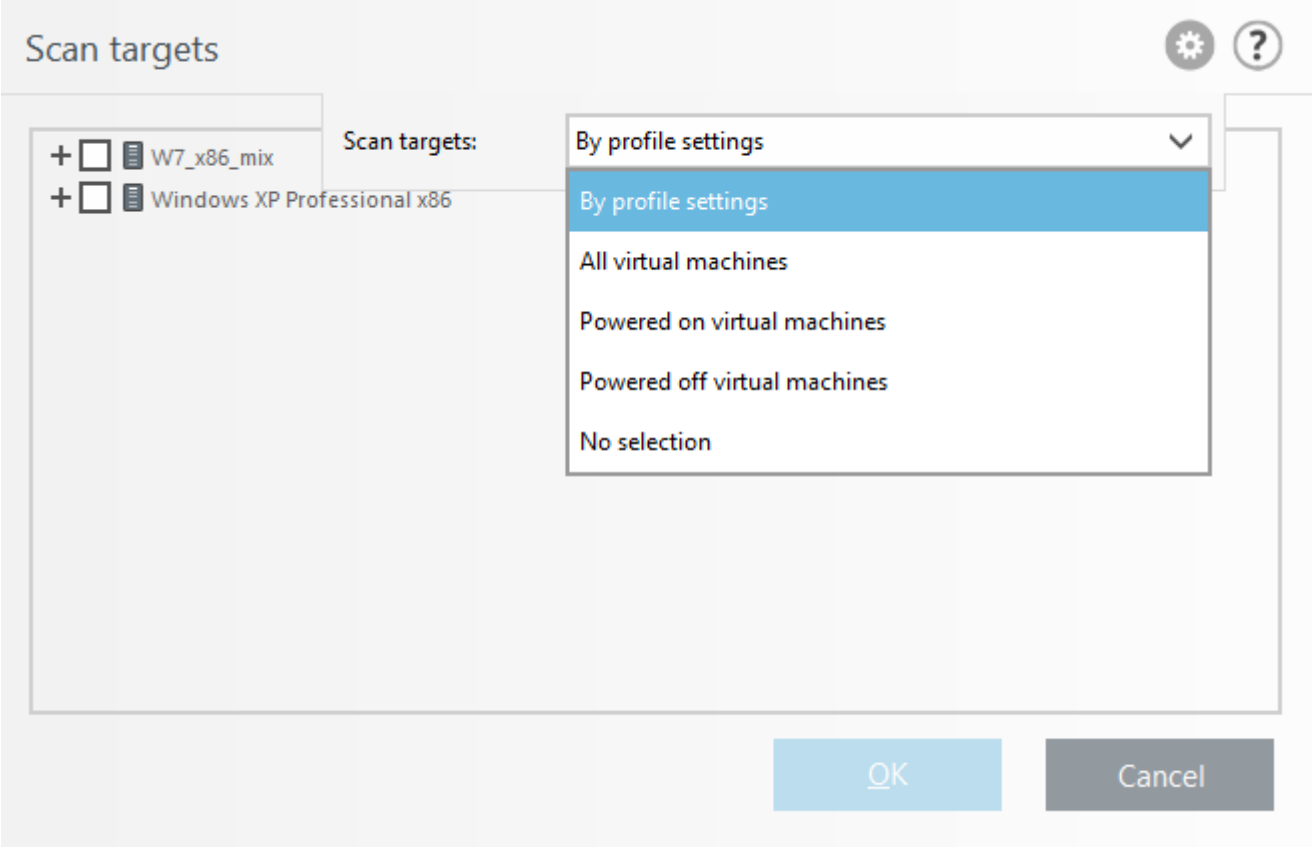
ThreatSense 參數

修改指定電腦掃描器的掃描參數。

指定及機器學習防護

報告是由偵測引擎和機器學習元件執行。

[Hyper-V 掃描］快顯視窗：



Hyper-V 下拉式功能表的［**掃描目標**］可讓您選取預先定義的掃描目標：

使用設定檔設定	選取所選掃描設定檔中設定的目標。
所有虛擬機器	選取所有虛擬機器。
開啟電源的虛擬機器	選取所有線上虛擬機器。
關閉電源的虛擬機器	選取所有離線虛擬機器。
不選擇	清除所有選擇。

按一下［**掃描**］使用您已設定的自訂參數來執行掃描。完成所有掃描之後，核取［**防護記錄檔案**］> [Hyper-V 掃描]

設定檔管理程式

［**掃描設定檔**］下拉式功能表可讓您選取預先定義的掃描設定檔。

- **智慧型掃描**
- **內容功能表掃描**
- **深入掃描**
- **我的設定檔**（套用至 Hyper-V 掃描更新設定檔 及 OneDrive 掃描)

若要協助您建立掃描設定檔以符合您的需求，請參閱 ThreatSense 引擎參數設定一節，以取得每個掃描設定參數的說明。

會在 ESET File Security 中的三個位置使用設定檔管理程式。

指定電腦掃描

您偏好的掃描參數可儲存供未來掃描時使用。我們建議您盡量為定期進行的掃描建立不同設定檔（含

有各種掃描目標、掃描方法及其他參數)。

[更新]

設定檔編輯器可讓使用者建立新的更新設定檔。只有在您的電腦使用多種方法來連接更新伺服器時，才需要建立自訂更新設定檔。

Hyper-V 掃描

建立新設定檔，選取**[設定檔清單]**旁的**[編輯]**。新設定檔會顯示在**[選取的設定檔]**下拉式功能表中並列出現有的掃描設定檔。

OneDrive 掃描

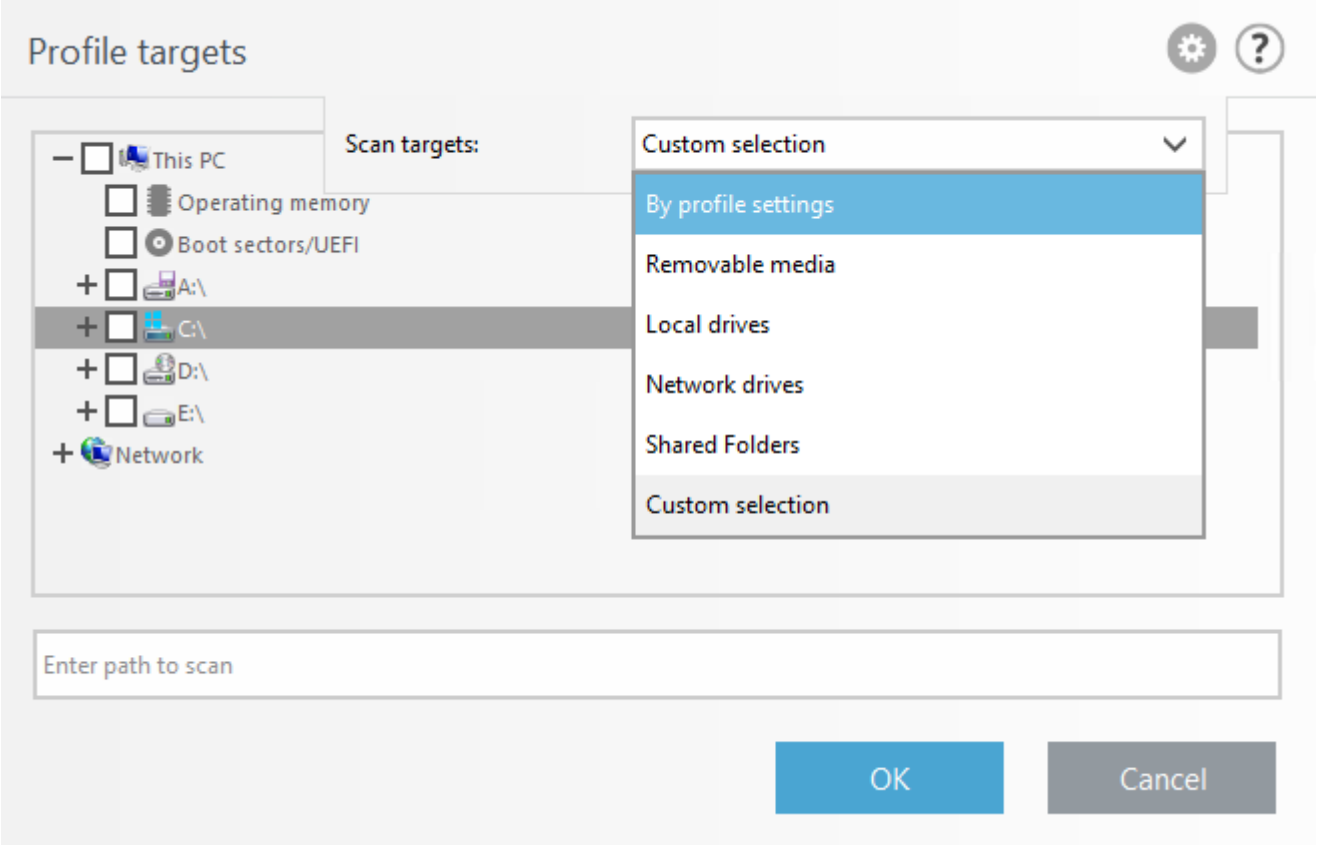
建立新設定檔，選取**[設定檔清單]**旁的**[編輯]**。新設定檔會顯示在**[選取的設定檔]**下拉式功能表中並列出現有的掃描設定檔。

描繪目標

您可以指定要掃描以進行滲入的項目。從會列出系統上所有可用目標之樹狀結構選擇物件（記憶體、開機磁區、磁碟機、檔案及資料夾或網路)。

注意
此掃描設定檔選擇器適用於**[指定掃描]**Hyper-V 掃描及 OneDrive 掃描

按一下左上方的齒輪圖示以存取**[掃描目標]**及**[掃描設定檔]**下拉式功能表。



[掃描目標]下拉式功能表可讓您選取預先定義的掃描目標：

使用設定檔設定	選取所選掃描設定檔中設定的目標。
可移除的媒體	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	選取所有對應的網路磁碟機。
共用資料夾	選取本機伺服器上共用的所有資料夾。
自訂選取項目	清除所有選取項目。清除之後，您就能自訂選取項目。

若要快速瀏覽至掃描目標（檔案或資料夾）以將之納入掃描，請在樹狀結構以下的文字欄位輸入其路徑。路徑項目會區分大小寫。

[掃描設定檔] 下拉式功能表可讓您選取預先定義的掃描設定檔：

- **智慧型掃描**
- **內容功能表掃描**
- **深入掃描**

這些掃描設定檔會使用不同的 ThreatSense 引擎參數。

顯示掃描進度

如果您只想掃描系統而不使用其他清除處理方式，請選取 **[掃描但不清除]**。當您只想要概括瞭解是否有受感染的項目或是取得有關這些感染的詳細資訊（如有），此功能可派上用場。您可以按一下 **[設定] > [ThreatSense 參數] > [清除]** 以從三種清除層級中選擇。掃描的相關資訊會儲存在掃描防護記錄中。

忽略排除

當您選取 **[忽略排除]** 時，該選項可讓您執行掃描並忽略可能適用的排除項目。

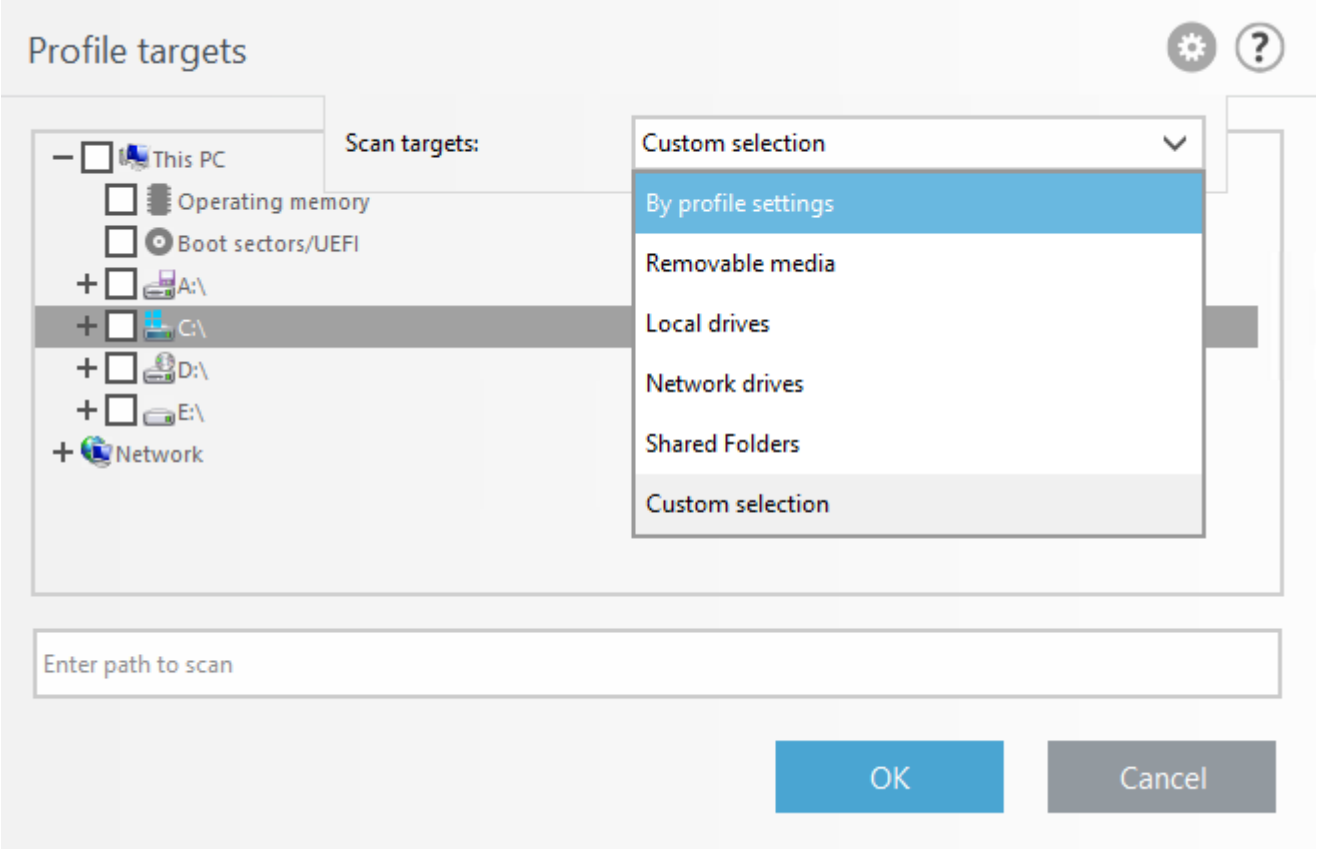
掃描目標

如果只要掃描特定的目標，您可以使用 **[自訂掃描]**，然後從 **[掃描目標]** 下拉式功能表中選擇選項，或從資料夾（樹狀目錄）結構中選取特定目標。

掃描目標設定檔選取項目適用於：

- [指定掃描]
- Hyper-V 掃描
- OneDrive 掃描

若要快速瀏覽至掃描目標，或新增新的目標檔案或資料夾，請將其輸入到資料夾清單下方的空白欄位。僅當樹狀結構中沒有選取任何目標，且**掃描目標**功能表設為**不選擇**時才可以這樣做。

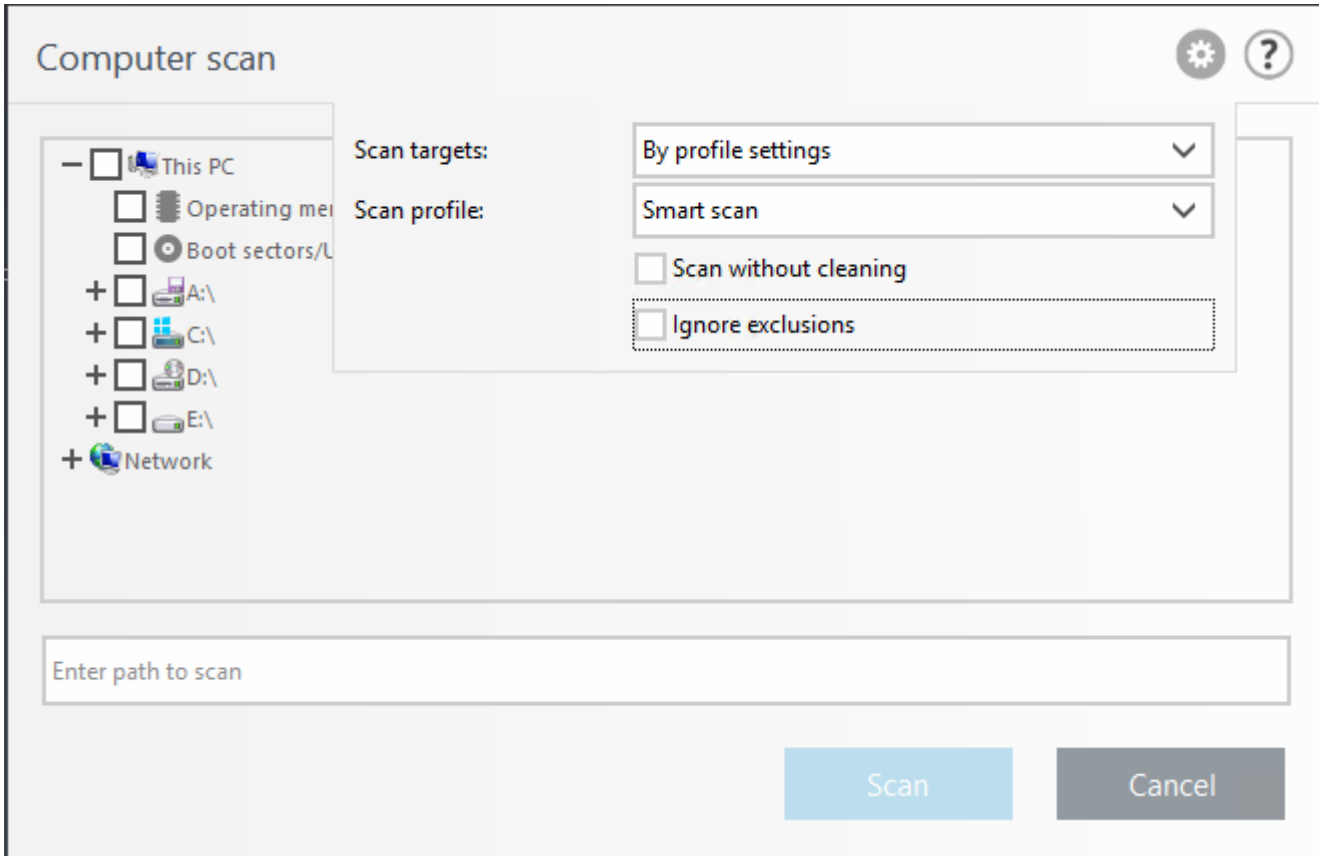


[掃描目標] 下拉式功能表可讓您選取預先定義的掃描目標。

使用設定檔設定	選取所選掃描設定檔中設定的目標。
可移除的媒體	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	選取所有對應的網路磁碟機。
共用資料夾	選取本機伺服器上共用的所有資料夾。
自訂選取項目	清除所有選取項目。清除之後，您就能自訂選取項目。

您可以從 [掃描設定檔] 下拉式功能表中選擇用於掃描所選目標的設定檔。預設的設定檔是 **[智慧型掃描]**。還有兩個預先定義的掃描設定檔，名稱分別是 **[深入掃描]** 與 **[內容功能表掃描]**。這些掃描設定檔會使用不同的 ThreatSense 引擎參數。

[自訂掃描] 快顯視窗：



顯示掃描進度

如果您只想掃描系統而不使用其他清除處理方式，請選取 **[掃描但不清除]**。當您只想要概括瞭解是否有受感染的項目或是取得有關這些感染的詳細資訊（如有），此功能可派上用場。您可以按一下 **[設定] > [ThreatSense 參數] > [清除]** 以從三種清除層級中選擇。掃描的相關資訊會儲存在掃描防護記錄中。

忽略排除

可讓您執行掃描並忽略可能適用的排除項目。

掃描

使用您已設定的自訂參數來執行掃描。

以管理員身分掃描

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

閒置時掃描

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。如果您的電腦處於下列狀態，**便會執行閒置狀態偵測**：

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

即使電腦電源來自電池仍然要執行

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。

啟用記錄

若要記錄防護記錄檔案區段內的電腦掃描輸出（在主要程式視窗中按一下［防護記錄檔案］並從下拉式功能表中選擇防護記錄類型［電腦掃描］）。

ThreatSense 參數

修改閒置狀態掃描器的參數。

啟動掃描

依預設，在系統啟動（使用者登入）和成功模組更新之後，將執行啟動檔案自動檢查。這項掃描是由排程器配置及工作所控制。

啟動掃描是**［系統啟動檔案檢查］**排程器工作的一部分。

若要修改啟動掃描設定，請瀏覽至**［工具］**> [排程器]，選取其中一個名為**［啟動檔案自動檢查］**（使用者登入或模組更新）的工作並按一下**［編輯］**。按一下精靈並在最後一個步驟中，您就能修改［啟動檔案自動檢查］的詳細選項。

自動啟動檔案檢查

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］下拉式功能表可指定系統啟動時執行的檔案掃描深度。系統會根據下列條件依遞增順序排列檔案：

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

此亦會包括兩個特定［掃描目標］群組：

使用者登入前執行的檔案

包含在使用者不用登入即可存取之位置中的檔案（包含幾乎所有的啟動位置，例如服務、瀏覽器 Helper 物件、Winlogon 通知、Windows 排程器項目、已知 DLL 等）。

使用者登入後執行的檔案

包含在只有使用者登入後才能存取之位置中的檔案（包含僅針對特定使用者執行的檔案，一般是 *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run* 中的檔案）。

每個上述群組的待掃描檔案清單是固定的。

掃描優先順序

用於決定何時開始掃描的優先順序層級：

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

可移除的媒體

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

插入可移除的媒體後要採取的處理方法

選取在將可移除媒體裝置插入電腦 (CD/DVD/USB) 時要執行的處理方法。

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

插入可移除的媒體後會顯示下列對話方塊：

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

此外，ESET File Security 具備裝置控制功能，能夠讓您定義指定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。

文件防護

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

整合至系統

此選項增強了 Microsoft Office 文件防護（在正常情況下並不需要）。

ThreatSense 參數

修改文件防護的參數。

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

Hyper-V 掃描

目前版本的 Hyper-V 掃描支援在 Hyper-V 中掃描線上或離線虛擬系統。以下顯示根據主控的 Windows Hyper-V 系統和虛擬系統的狀態所支援的掃描類型：

具有 Hyper-V 功能的虛擬系統	Windows Server 2008 R2 SP1 Hyper-V	Windows Server 2012 Hyper-V	Windows Server 2012 R2 Hyper-V	Windows Server 2016 Hyper-V	Windows Server 2019 Hyper-V
線上 VM	無掃描	唯讀	唯讀	唯讀	唯讀
離線 VM	唯讀/清理	唯讀/清理	唯讀/清理	唯讀/清理	唯讀/清理

硬體需求

伺服器應能順利執行虛擬機器。掃描活動主要是使用 CPU 資源。若要線上掃描 VM，需要可用磁碟空間。磁碟空間至少必須為檢查點/快照和虛擬磁碟使用空間的兩倍。

特定限制

- 由於動態磁碟的本質，因此不支援在 RAID 儲存裝置、合併磁碟區和動態磁碟上進行掃描。因此，如有可能，我們建議您避免在 VM 上使用動態磁碟類型。
- 掃描一律只在目前的 VM 上執行，並不影響其檢查點或快照。
- ESET File Security 目前不支援在叢集中的主機上執行 Hyper-V。
- 執行於 Windows Server 2008 R2 SP1 上之 Hyper-V 主機的虛擬機器只能以唯讀模式進行掃描（[不清除]），不論是否已在 ThreatSense 參數中選擇清除層級。

> 注意
> 雖然 ESET Security 支援掃描虛擬磁碟 MBR，但唯讀掃描是唯一支援的方法。您可以在 **[進階設定] (F5) > 偵側引擎 > [Hyper-V 掃描] >** ThreatSense 參數 **> [開機磁區]** 中變更此設定。

要掃描的虛擬機器為「離線狀態」 – 「已關閉」狀態

ESET File Security 使用 Hyper-V 管理來偵測和連線至虛擬磁碟。因此，ESET File Security 具有對虛擬磁碟內容相同的存取權，其權限就如同存取任何一般磁碟上的資料和檔案一樣。

可掃描的虛擬機器為「線上狀態」 – 執行中、暫停、 儲存狀態

ESET File Security 使用 Hyper-V 管理來偵測虛擬磁碟。無法實際連線至這些磁碟。因此，ESET File Security 會建立虛擬機器的檢查點/快照，然後連線至檢查點/快照。掃描完成後，系統便會刪除檢查點/快照。這表示可以執行唯讀掃描，因為虛擬機器不受掃描活動的影響。

允許最多一分鐘以讓 ESET File Security 在掃描時建立快照或檢查點。當您打算在大量虛擬機器上執行 Hyper-V 掃描時，應將此因素納入考量。

命名慣例

Hyper-V 掃描的模組使用下列命名慣例：

```
VirtualMachineName\DiskX\VolumeY
```

其中 X 為磁碟機編號，Y 則是磁碟區編號。例如：

```
Computer\Disk0\Volume1
```

數字字尾將依據偵測到的順序加上，且與 VM 磁碟管理員中所見的順序相同。要掃描的目標樹狀結構清單、進度列和防護記錄檔案都會使用此命名慣例。

執行掃描

- 指定掃描 – 按一下 **[Hyper-V 掃描]** 以檢視虛擬機器的清單和可供掃描的磁碟區。選取您想要掃描的虛擬機器、磁碟或磁碟區並按一下 **[掃描]**。
- 建立排程器工作。
- 透過 ESET Security Management Center 作為稱為伺服器掃描的用戶端工作。
- Hyper-V 掃描可透過 eShell 管理和啟動。

您可同時執行多個 Hyper-V 掃描。掃描完成時，您將會收到通知和防護記錄檔的連結。

可能的問題

- 在執行線上虛擬機器掃描時，必須建立特定虛擬機器的檢查點/快照，而在建立檢查點/快照期間，可能會限制或停用部分虛擬機器的一般處理方法。
- 若離線的虛擬機器正在進行掃描，它必須等到掃描結束後才可開啟。
- Hyper-V Manager 可讓您將不同的虛擬機器命名為相同名稱，當您檢閱掃描防護記錄，嘗試區分機器時會導致問題。

OneDrive 掃描

基本

您可以配置處理方法與隔離區

檔案受感染時要採取的處理方法

- **不進行處理** – 不會套用檔案中的任何變更。
- **刪除** – 移至隔離區並將檔案從 OneDrive 中刪除。但是，檔案仍在 OneDrive 資源回收桶中。

隔離受感染的檔案

當啟用時，標記為刪除的檔案將放入隔離區。請取消選取此設定以停用隔離區，讓檔案不會在累積在隔離區中。

進階

此部分包含 OneDrive 掃描註冊相關資訊（應用程式 ID、Azure 入口網站上的物件 ID、憑證指紋）。您可以配置逾時與同時下載設定。

設定檔

若要建立新設定檔，選取 **[設定檔清單]** 旁的 **[編輯]**，輸入 **[設定檔名稱]**，然後按一下 **[新增]**。新設定檔會顯示在 **[選取的設定檔]** 下拉式功能表中並列出現有的掃描設定檔。

[掃描目標] 下拉式功能表可讓您選取預先定義的掃描目標：

- **依設定檔** – 選取所選掃描設定檔中設定的目標。
- **所有使用者** – 選取所有使用者。
- **不選擇** – 清除目前的選取項目。

按一下［**掃描**］使用您已設定的自訂參數來執行掃描。完成所有掃描之後，核取［**防護記錄檔案**］> [OneDrive 掃描]

ThreatSense 參數

修改 OneDrive 掃描器的掃描參數。

OneDrive 掃描及機器學習防護

報告是由偵測引擎和機器學習元件執行。

HIPS

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

警告
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。

啟用自我防護

ESET File Security 有內建的自我防護技術，可防止惡意軟體損毀或停用您的惡意軟體防護，因此能確定系統隨時受到保護。［啟用 HIPS] 和［啟用 SD (自我防護)］設定的變更會在 Windows 作業系統重新啟動後生效。停用整個 HIPS 系統也需要重新啟動電腦。

啟用受保護的服務

Microsoft 已經引進利用 Microsoft Windows Server 2012 R2 保護服務的概念。其可抵禦服務遭到惡意攻擊。ESET File Security 的核心預設會以受保護服務的形式執行。此功能適用於 Microsoft Windows Server 2012 R2 及較新版本的伺服器作業系統。

Advanced Memory Scanner 使能

可搭配惡意探索封鎖程式，強化對抗惡意軟體，這些惡意軟體的設計目的為利用欺騙或加密來規避惡意軟體防護產品的偵測功能。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。

啟用程式漏洞防護

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。

啟用勒索軟體保護

若要使用此功能，請啟用 ESET Live Grid。請深入瞭解字彙中的勒索軟體。

過濾模式

您可以選擇下列其中一個過濾模式：

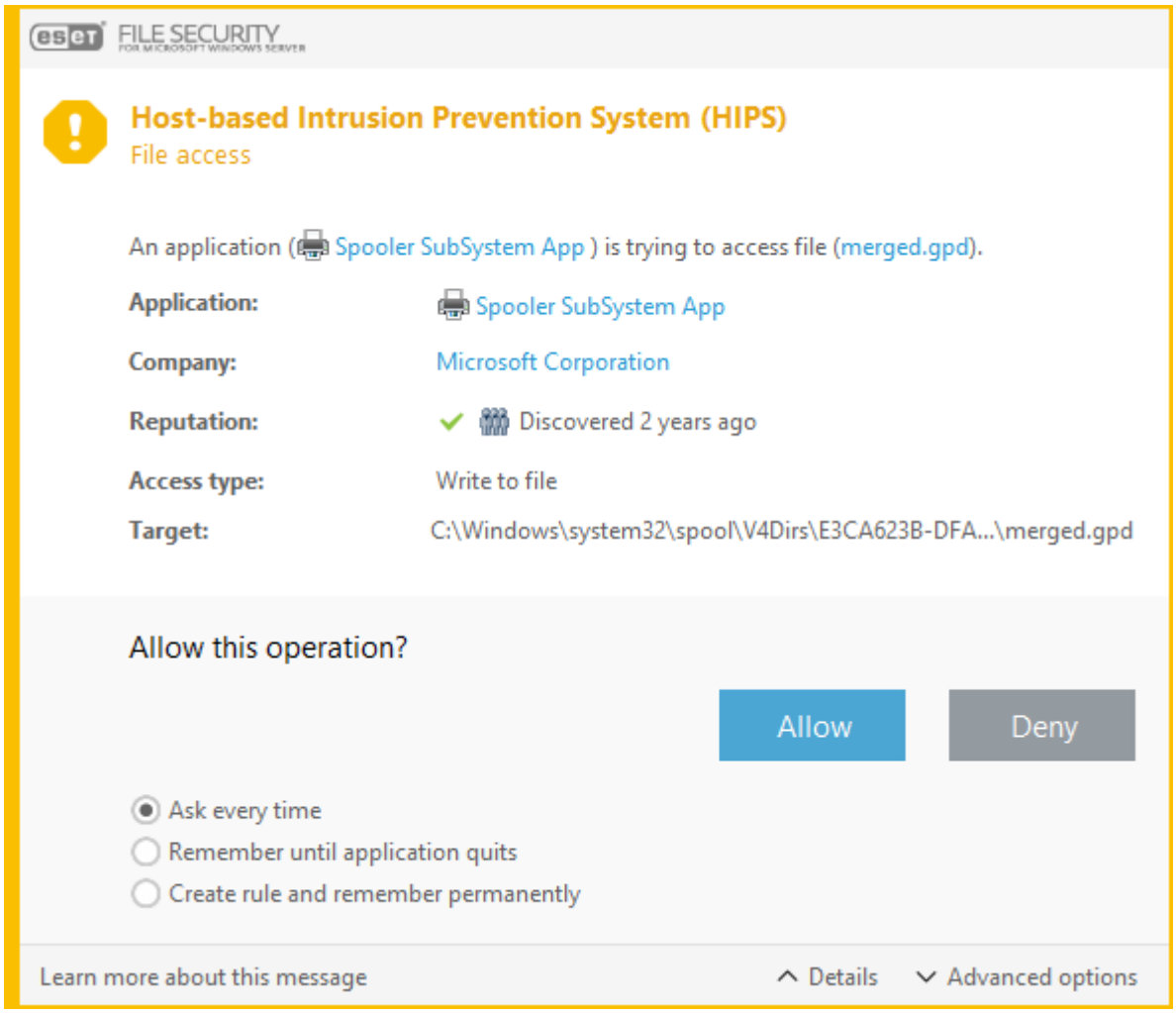
- **自動模式** – 系統會啟用作業，但受到保護系統的預先定義規則封鎖的作業除外。除了規則拒絕的處理方法以外，會允許所有處理方法。

- **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。允許/拒絕存取、建立規則、暫時記住此處理方法。
- **原則型模式** – 系統會封鎖作業。只接受使用者/預先定義的規則。
- **學習模式** – 系統會啟用作業，且每次作業後會建立規則。以此模式建立的規則可在［規則編輯器］中檢視，但與手動建立的規則或自動模式下建立的規則相較之下，其優先順序較低。當您從 [HIPS 過濾模式］下拉式功能表選取 **［學習模式］**，即可使用 **［學習模式將在下列情況結束］** 設定。選取您要啟用學習模式的持續時間（最長為 14 天）。過了指定的持續時間之後，會提示您在學習模式中編輯 HIPS 建立的規則。您可以選擇不同的過濾模式，或者延後決定並持續使用學習模式。

規則

規則會決定哪些應用程式可獲得檔案、登錄部分或其他應用程式的存取權限⍰HIPS 系統監控作業系統中的事件，並根據類似個人防火牆規則的規則執行反應動作。按一下［編輯］開啟 HIPS 規則管理視窗。若規則的預設處理方法已設定為 **［詢問］**，每次觸發規則時都會出現對話方塊視窗。您可以選擇 **［封鎖］** 或 **［允許］** 作業。如果您不在指定時間內選擇處理方法，則會根據規則選取新處理方法。

對話視窗可讓您根據 HIPS 偵測的任何新處理方法來建立規則，然後定義 **［允許］** 或 **［封鎖］** 該處理方法所依據的條件。按一下 **［詳細資料］** 以檢視進一步的資訊。系統認定使用此方法建立的規則等於手動建立的規則，因此由對話視窗建立的規則無需像觸發該對話視窗的規則那般明確。這表示，建立此類規則後，同樣的作業可以觸發相同的視窗。



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。

直到結束應用程式之前都會記住

選擇處理方法［**拒絕**］或［**允許**］會建立暫時性 HIPS 規則，在關閉有問題的應用程式之前可供使用。此外，如果您變更過濾模式、修改規則，或是在 HIPS 模組更新時，以及您重新啟動系統時，則會刪除暫時性規則。

建立規則並永久記住規則

建立新的 HIPS 規則。您可以稍後在 HIPS 規則管理區段中修改此規則。

HIPS 規則設定

此視窗為您提供現有 HIPS 規則的概觀。

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，請停用此切換選項。
處理方法	本規則指出條件正確時應執行的處理方法 – 包括［**允許**］[**封鎖**］或［**詢問**］
來源	來源 – 只有當事件是由此應用程式觸發時，才會使用此規則。
目標	只有當作業與特定檔案、應用程式或登錄項目相關時，才會使用此規則。
防護記錄嚴重性	如果您啟動此選項，有關此規則的資訊將寫入 HIPS 防護記錄
通知	若觸發事件，右下角將出現一個小的快顯視窗。

建立新規則，按一下**新增**新的 HIPS 規則或**編輯**選取的項目。

規則名稱

使用者定義或自動選擇的規則名稱。

處理方法

本規則指出條件正確時應執行的處理方法，包括［**允許**］[**封鎖**］或［**詢問**］

作業系統

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］。規則包含會說明觸發此規則之情況的部分。

來源應用程式

只有當事件是由此應用程式觸發時，才會使用此規則。從下拉式功能表中選取**特定應用程式**並按一下［**新增**］以新增檔案或資料夾；您也可以從下拉式功能表中選取［**所有應用程式**］並新增所有應用程式。

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

重要作業的說明：

檔案作業：

刪除檔案	應用程式正在要求權限，以刪除目標檔案。
寫入檔案	應用程式正在要求權限，以寫入目標檔案。

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

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。

應用程式作業：

除錯另一個應用程式	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］視窗直接存取）。
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代碼。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。

只有當作業與此目標相關時，才會使用此規則。從下拉式功能表選取［**特定應用程式**］並按一下［**新增**］以新增檔案或資料夾。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	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。

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。

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

警告
若您建立過於廣泛的規則，您將會收到通知。

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。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。您可以從清單［**新增**］驅動程式、［**編輯**］或［**刪除**］選取的驅動程式。

注意
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。

記錄所有封鎖的作業

系統會將所有遭封鎖的作業寫入 HIPS 防護記錄。

當啟動應用程式發生變更時通知

每次在系統啟動中新增或移除應用程式時，便會顯示桌面通知。

更新配置

本節會指定更新來源資訊，例如所使用的更新伺服器，以及這些伺服器的驗證資料。

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

基本

選取預設更新設定檔

選擇現有的設定檔或建立新的設定檔，預設會為該更新套用設定檔。

清除更新快取

如果更新遭遇問題，請按一下［**清除**］以清除暫時更新快取。

自動設定偵測引擎最大有效期限/偵測引擎最大有效期限（天）

可讓您設定偵測引擎期限回報過期的時間上限。預設值為 7 天。

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。或者，如果您先前已無限期延後更新，您也可以啟用這些停用的更新ESET File Security

會記錄偵測引擎與程式模組的快照，以搭配還原功能使用。若要建立偵測引擎快照，請啟用 **[建立模組快照]**。

儲存於本機的快照數目

定義先前儲存的模組快照數目。

設定檔

若要建立自訂更新設定檔，選取 **[設定檔清單]** 旁的 **[編輯]**，並輸入您自己的 **[設定檔名稱]**，然後按一下 **[新增]**。**選取設定檔以編輯**並修改**模組更新**的參數或建立**更新映像**。

更新

從下拉式功能表選取要使用的更新類型：

- **定期更新** – 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** – 是已完成內部測試且即將提供給大眾使用的更新。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，且「不應」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（例如，資料庫已在實際環境中測試，因此可視為穩定）。

下載更新前詢問

有可用的新更新時將，系統會提示您進行下載。

詢問更新檔案是否大於 (kB)

若更新檔案大小超過欄位中指定的值，便會顯示通知。

停用成功更新的相關通知

關閉畫面右下角的系統匣通知。如果正在執行全螢幕應用程式，則選取此選項很有用。請注意，簡報模式將關閉所有通知。

模組更新

模組更新下拉式功能表已預設為 **[自動選擇]**。更新伺服器是儲存更新的位置。若您使用 ESET 伺服器，我們建議您讓預設選項保持選取狀態。

當使用本機 HTTP 伺服器（也稱為「映像」）時，更新伺服器應該進行設定，如下所示： ***http://computer_name_or_its_IP_address:2221***
當透過 SSL 使用本機 HTTP 伺服器時，更新伺服器應設定如下： https://computer_name_or_its_IP_address:2221
當使用本機共用資料夾時，更新伺服器應設定如下： \\computer_name_or_its_IP_address\shared_folder

啟用更頻繁的偵測病毒碼更新

將縮短偵測引擎更新的間隔。停用此選項可能對偵測速率帶來不良影響。

允許從可移除的媒體更新模組

可讓您透過包含建立映像的可移除媒體進行更新。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**］。

程式元件更新

使用［**更新模式**］下拉式功能表，以便在有新更新可用時，選擇如何套用 ESET File Security 元件更新。元件更新通常會修改現有的功能，但也包含新功能。根據所選擇的更新模式，可自動執行元件更新，而無需中斷或確認。或者，您也可以選擇在安裝更新之前先獲得通知。在元件更新之後必須重新啟動伺服器。下列更新模式可供使用：

- ［**更新前詢問**］ – 有更新可用時，系統會提示您確認或拒絕產品更新。這是預設選項。元件更新之後，可能需要重新啟動伺服器。
- **自動更新** – 會自動下載和安裝元件更新。
- **一律不更新** – 完全不會執行元件更新。我們建議您使用此選項，因為這可讓您手動執行元件更新，然後在排程的維護時段期間重新啟動您的伺服器。

重要
自動更新模式會在元件更新完成之後，自動重新啟動您的伺服器。

連線選項

Proxy 伺服器

若要存取指定更新設定檔的 Proxy 伺服器設定選項。按一下 **[Proxy 模式]**，然後選取下列三個選項之一：

- ［**不使用 Proxy 伺服器**］ – 執行更新時 ESET File Security 不會使用 Proxy 伺服器。
- ［**使用全域 Proxy 伺服器設定**］ – 將使用已經在［**進階設定**］(**F5**) > ［**工具**］> [Proxy 伺服器］ 中指定的 Proxy 伺服器配置。
- **經由 Proxy 伺服器連線** – 如果出現下列狀況，使用此選項：

應用來更新 ESET File Security 的 Proxy 伺服器與全域設定中所指定的 Proxy 伺服器不同（［工具］> [Proxy 伺服器]）。若是如此，則應該在其中指定設定 [Proxy 伺服器］位址、通訊連接埠（依預設為 3128），以及 Proxy 伺服器的［使用者名稱］及［密碼］（如果需要的話）。

並未全域設定 Proxy 伺服器，但是 ESET File Security 將連接至 Proxy 伺服器進行更新。

電腦透過 Proxy 伺服器連接至網際網路。系統在程式安裝期間從 Internet Explorer 取得設定，但如果它們隨後有所變更（例如，您變更 ISP），請檢查此視窗中所列的 HTTP Proxy 設定是否正確。否則，程式將無法連接至更新伺服器。

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

如果 proxy 無法使用，請使用直接連線

如果產品已配置為使用 HTTP Proxy 且 Proxy 無法存取，產品將避開 Proxy 並與 ESET 伺服器直接通訊。

Windows 共用

從執行 Windows 的本機伺服器更新時，依預設需要每個網路連線的驗證。

以下列身分連接到區域網路

若要配置您的帳戶，選取下列任一選項：

- **[系統帳戶 (預設)]** – 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。
- **[目前使用者]** – 選取此選項以確保程式授權使用目前登入中的使用者帳戶。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。
- **[指定使用者]** – 選取此選項以使用特定使用者帳戶來驗證。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。如果使用者沒有存取權限，程式將無法建立連線或下載更新。

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

更新後中斷伺服器連線

在已下載更新但伺服器連線仍處於作用中時強制中斷連線。

更新映像

本機映像伺服器的配置選項位於 **[更新] > [設定檔] > [映像]** 索引標籤中的 [進階設定] **(F5)**。

更新回復

如果您按一下 **[還原]**，您必須從下拉式功能表中選取時間間隔，這代表偵測引擎資料庫與程式模組更新要暫停的時間。

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

偵測引擎資料庫版本會降級到最舊的可用版本，並以快照形式儲存在本機電腦檔案系統中。

已排程的工作 – 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。

範例
以下步驟會引導您完成工作，以編輯現有的［**定期自動更新**］
1.在主要［**排程器**］畫面中，選取名為［**定期自動更新**］的工作［**更新**］並按一下［**編輯**］，配置精靈隨即開啟。
2.設定排程器工作以執行，當您要［執行已排程的工作］時，選取下列其中一個時間選項來加以定義。
3.如果您想要在使用電池執行系統時（例如 UPS）避免執行工作，請按一下［**使用電池執行時略過工作**］旁的切換鈕。
4.選取更新設定檔以用於更新。如果已排程的工作執行由於任何原因而失敗，請選取要執行的處理方法。
5.按一下［**完成**］以套用工作。

更新映像

開啟 ESET File Security
按下 *F5* > *[*更新］> ［設定檔］> ［更新映像］ 

ESET File Security 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

建立更新映像

啟動映像配置選項。

儲存資料夾

如果您想變更定義的預設資料夾至儲存映像檔 *C:\ProgramData\ESET\ESET Security\mirror*，請按一下［清除］。按一下［**編輯**］以瀏覽本機電腦或共用網路資料夾上的資料夾。如果需要指定資料夾的授權，必須在［使用者名稱］及［密碼］欄位中輸入驗證資料。如果選取的目標資料夾位於執行 Windows NT/2000/XP 作業系統的網路磁碟上，則指定的使用者名稱及密碼必須具有已選取資料夾的寫入權。使用者名稱及密碼的輸入格式應為網域/使用者或工作群組/使用者。請記得提供對應的密碼。
應以 *Domain/User* 或 *Workgroup/User* 的格式輸入使用者名稱及密碼。請記得提供對應的密碼。

程式元件更新

檔案

配置映像時您可以指定要下載的更新的語言版本。使用者所配置的映像伺服器必須支援選取的語言。

自動更新元件

可安裝新功能和現有功能的更新。更新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。產品更新之後，可能需要重新啟動電腦。

立即更新元件

將程式元件更新到最新版本。

- HTTP 伺服器

伺服器連接埠

預設連接埠設定為 2221。如果您使用不同的連接埠，請變更此數值。

認證

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。

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

針對 HTTP 伺服器的 SSL

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：PEM、PFX 和 ASN。為了額外的安全性，您可以使用 HTTPS 通訊協定來下載更新檔案。使用此通訊協定幾乎不可能追蹤資料傳送與登入憑證。
[私密金鑰類型] 依預設設為 **[已整合]**（因此［私密金鑰檔案］選項預設為停用）。這表示私密金鑰是所選憑證連鎖檔案的一部分。

連線選項

Windows 共用

從執行 Windows 的本機伺服器更新時，依預設需要每個網路連線的驗證。

以下列身分連接到區域網路

若要配置您的帳戶，選取下列任一選項：

- **[系統帳戶 (預設)]** - 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。
- **[目前使用者]** - 選取此選項以確保程式授權使用目前登入中的使用者帳戶。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。
- **[指定使用者]** - 選取此選項以使用特定使用者帳戶來驗證。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。如果使用者沒有存取權限，程式將無法建立連線並下載更新。

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

更新後中斷伺服器連線

在已下載更新但伺服器連線仍處於作用中時強制中斷連線。

網路防護

啟用網路攻擊防護 (IDS)

可讓您從信任區域配置在電腦上執行的一些服務存取權限，以及啟用/停用可能會用來損害您電腦之數種類型攻擊與弱點的偵測。

啟用殭屍網路防護

電腦受到感染且殭屍網路嘗試通訊時，根據典型模式，以偵測及封鎖與惡意命令及控制伺服器的通訊

IDS 例外

您可以將入侵偵測系統 (IDS) 例外視為網路防護規則。請按一下 [編輯] 定義 IDS 例外。

入侵偵測：

通訊協定 SMB – 偵測和封鎖 SMB 通訊協定中的各種安全性問題
通訊協定 RPC – 偵測和封鎖針對分散式運算環境 (DCE) 而開發之遠端程序呼叫系統的各種 CVE
通訊協定 RDP – 偵測和封鎖 RDP 通訊協定（如上述）中的各種 CVE
攻擊偵測之後封鎖不安全的位址 – 將已偵測為攻擊來源的 IP 位址新增到黑名單，以封鎖特定期間的連線。
攻擊偵測後顯示通知 – 開啟畫面右下方的系統匣通知。
也顯示針對安全漏洞傳入攻擊的通知 – 如果偵測到對安全漏洞傳入攻擊，或是威脅嘗試透過此方法進入系統，便會警告您。

封包檢查：

允許外來連線至 SMB 通訊協定中的管理共用 – 管理共用是預設的網路共用，其會與系統資料夾 (ADMIN$) 共用系統中的硬碟分割區 (C$、D$、...)。停用與管理共用的連線可緩解許多安全性風險。例如，Conficker 蠕蟲會執行字典攻擊，以便連線至網路共用。
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。現代 Windows 作業系統支援舊 SMB 方言，因為其與 Windows 95 等舊作業系統向下相容。攻擊者可以在 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和使用舊版 Windows 共用檔案（或是使用一般 SMB 通訊），則可拒絕舊 SMB 方言。
拒絕不含安全性延伸模組的 SMB 安全性 – 可在 SMB 工作階段協商期間使用延伸安全性，以提供比 LAN Manager Challenge/Response (LM) 驗證更安全的驗證機制。LM 方案被視為弱式且不建議使用。
可與「安全性帳戶管理員」服務通訊 – 如需關於此服務的詳細資訊，請參閱 [MS-SAMR]
可與「本機安全性授權」服務通訊 – 如需關於此服務的詳細資訊，請參閱 [MS-LSAD] 及 [MS-LSAT]
可與「遠端登錄」服務通訊 – 如需關於此服務的詳細資訊，請參閱 [MS-RRP]
可與「服務控制管理員」服務通訊 – 如需關於此服務的詳細資訊，請參閱 [MS-SCMR]
可與「伺服器」服務通訊 – 如需關於此服務的詳細資訊，請參閱 [MS-SRVS]
可與其他服務通訊 – 其他 MSRPC 服務。

IDS 例外

基本上，入侵偵測系統 (IDS) 例外是網路防護規則。例外的評估乃依照最上到最下的形式來進行。IDS 例外編輯器可讓您在發生各種 IDS 例外時，自訂網路防護行為。系統會分別針對各種處理方法類型（封鎖、通知、防護記錄）套用第一個符合的例外。**[頂端]/[向上]/[向下]/[底端]** 可讓您調整例外的優先順序層級。若要建立新的 IDS 例外，按一下 **[新增]**。按一下 **[編輯]** 修改現有的 IDS 例外，或按 **[刪除]** 予以移除。

從下拉式清單選擇 **[警示]** 類型。指定 **[威脅名稱]** 及 **[方向]**。瀏覽您要為其建立例外的 **[應用程式]**。指定 IP 位址 (IPv4 或 IPv6) 或子網路的清單。對於多個項目，使用逗號作為分隔符號。

從下拉式功能表（**[預設值]**、**[是]**、**[否]**）選取其中一個選項，以配置 IDS 例外的 **[處理方法]**。針對每個處理方法類型（**[封鎖]**、**[通知]**、**[防護記錄]**）執行此動作。

> 範例
> 若要在發出 IDS 例外警示時顯示通知，以及記錄發生事件的時間，請讓 **[封鎖]** 處理方法類型維持 **[預設值]**，並針對其他兩個處理方法類型（**[通知]** 及 **[防護記錄]**），從下拉式功能表選擇 **[是]**。

暫時性 IP 位址黑名單

檢視已偵測為攻擊來源的 IP 位址清單，並新增至黑名單中以封鎖特定期間的連線。顯示已鎖定的 **[IP 位址]**。

封鎖原因

顯示已從位址（例如 TCP 連接埠掃描攻擊）預防的攻擊類型。

逾時

位址從黑名單到期時，會顯示時間及日期。

移除/全部移除

在選取的 IP 位址到期前，先從臨時黑名單移除該 IP 位址，或是立即從黑名單移除所有位址。

新增例外

針對選取的 IP 位址，將防火牆例外新增至 IDS 過濾。

Web 和電子郵件

您可以配置通訊協定篩選、電子郵件用戶端防護、Web 存取防護及網路釣魚防護，在進行網際網路通訊期間保護您的伺服器。

電子郵件用戶端防護

可控制所有電子郵件通訊、防範惡意程式碼，並讓您選擇偵測到感染時要採取的處理方法。

Web 存取防護

可監視 Web 瀏覽器與遠端伺服器之間的通訊，並遵循 HTTP 及 HTTPS 規則。此功能也可讓您封鎖、允

許或排除特定 URL 位址。

通訊協定過濾

提供由 ThreatSense 搜尋引擎所提供的應用程式通訊協定進階防護。無論是使用 Web 瀏覽器或電子郵件用戶端，此控制項都會自動運作。它也適合用於加密（SSL/TLS）通訊。

網路釣魚防護

可讓您封鎖已知會散播網路釣魚的網頁。

通訊協定過濾

應用程式通訊協定的惡意軟體防護由 ThreatSense 掃描引擎控制，該引擎可整合多個進階惡意程式掃描技術。無論是使用網際網路瀏覽器或電子郵件用戶端，通訊協定篩選會自動運作。如果已啟用通訊協定過濾，ESET File Security 將會檢查使用 SSL/TLS 通訊協定的通訊，請移至 **[Web 和電子郵件]** > SSL/TLS。

啟用應用程式通訊協定內容過濾

如果您停用通訊協定篩選，請注意，許多 ESET File Security 元件（**[Web 存取防護]**、**[電子郵件通訊協定防護]** 及 **[網路釣魚防護]**）必須啟用此選項才能正常運作，但並非所有功能都能使用。

排除的應用程式

若要將特定的網路識別應用程式排除在內容過濾之外，請在清單中選取這些應用程式。屆時將不會針對所選應用程式的 HTTP/POP3 通訊檢查是否存在威脅。可讓您從通訊協定篩選排除特定應用程式。按一下 **[編輯]** 及 **[新增]**，從應用程式清單選擇可執行檔，而從通訊協定篩選排除該檔案。

重要
建議僅針對在檢查通訊時無法正常運作的應用程式使用此選項。

排除的 IP 位址

可讓您從通訊協定過濾排除特定遠端位址。在清單中的 IP 位址將排除於通訊協定內容篩選之外。屆時將不會針對所選位址的 HTTP/POP3/IMAP 往來通訊檢查是否存在威脅。

重要
我們建議只將此選項用於已知值得信賴的位址。

按一下 **[編輯]** 及 **[新增]** 以指定 IP 位址、位址範圍或是要套用排除的子網路。當您選取 **[輸入多個值]**，您可新增多個以行、逗號或分號分隔的 IP 位址。當您啟用多個選項時，位址將於已排除 IP 位址清單中顯示。

注意
排除對於通訊協定過濾導致相容性問題時很有幫助。

Web 和電子郵件用戶端

由於在網際網路周圍散佈著大量的惡意代碼，因此能安全地瀏覽網際網路是電腦防護非常重要的面向。網路瀏覽器的弱點和詐騙連結會幫助惡意代碼在不被察覺的情況下進入系統，這也就是 ESET File Security 著重在網路瀏覽器安全性的原因之一。每一個存取網路的應用程式均可被標記為網路瀏覽器。您能夠在 Web

和電子郵件用戶端的清單中，新增已使用通訊協定進行通訊的應用程式，或是來自已選取路徑的應用程式。

SSL/TLS

ESET File Security 可檢查使用安全通訊端層 (SSL) / 傳輸層安全性 (TLS) 通訊協定的通訊中是否存有威脅。

對於使用信任的憑證、未知憑證或排除在 SSL 防護通訊檢查之外的憑證進行的 SSL 防護通訊，您可以運用各種掃描模式來檢查。

啟用 SSL/TLS 通訊協定過濾

若停用通訊協定過濾，程式將不會掃描使用 SSL/TLS 的通訊。安全通訊端層 (SSL) / 傳輸層安全性 (TLS) 通訊協定過濾模式適用於下列選項：

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

SSL/TLS 過濾應用程式清單

新增過濾的應用程式和設定其中一個掃描處理方法SSL/TLS 過濾應用程式的清單可用於自訂特定應用程式的 ESET File Security 行為，以及記住選擇的處理方法，如果已在 **[SSL/TLS 通訊協定過濾模式]** 中選取 **[互動模式]**

已知的憑證清單

可讓您為特定的 SSL 憑證自訂 ESET File Security 行為。透過按一下 [已知的憑證清單] 旁的 **[編輯]** 可檢視和管理清單。

排除使用信任網域的通訊

將使用延伸驗證憑證的通訊排除在通訊協定檢查（網路銀行業務）。

封鎖利用過時通訊協定 SSL 第 2 版的加密通訊

自動封鎖使用此舊版 SSL 通訊協定的通訊。

系統管理員憑證

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

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

憑證有效性

如果使用 TRCA 憑證商店無法驗證憑證

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

如果憑證無效或損毀

這表示憑證已到期或簽署方式不正確。在此情況下，我們建議維持選取［**封鎖使用憑證的通訊**］。

已知的憑證清單

若要自訂特定 Secure Sockets Layer (SSL) / Transport Layer Security (TLS) 憑證的 ESET File Security 行為，以及記得在 SSL/TLS 通訊協定過濾模式中選取［**互動模式**］時選擇的動作。您可以配置選取的憑證或是從 URL 或檔案［**新增**］憑證。當您在［新增憑證］視窗時，按一下 [URL] 或［檔案］並指定憑證 URL 或瀏覽憑證檔案。將使用憑證的資料自動填寫下列欄位：

- **憑證名稱** – 憑證的名稱。
- **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。

存取處理方法

- **自動** – 允許信任的憑證並詢問不信任的憑證。
- **［允許］或［封鎖］** – 允許/封鎖此憑證保護的通訊，無論憑證的可信任度為何。
- **詢問** – 遇到特定憑證時收到提示。

掃描處理方法

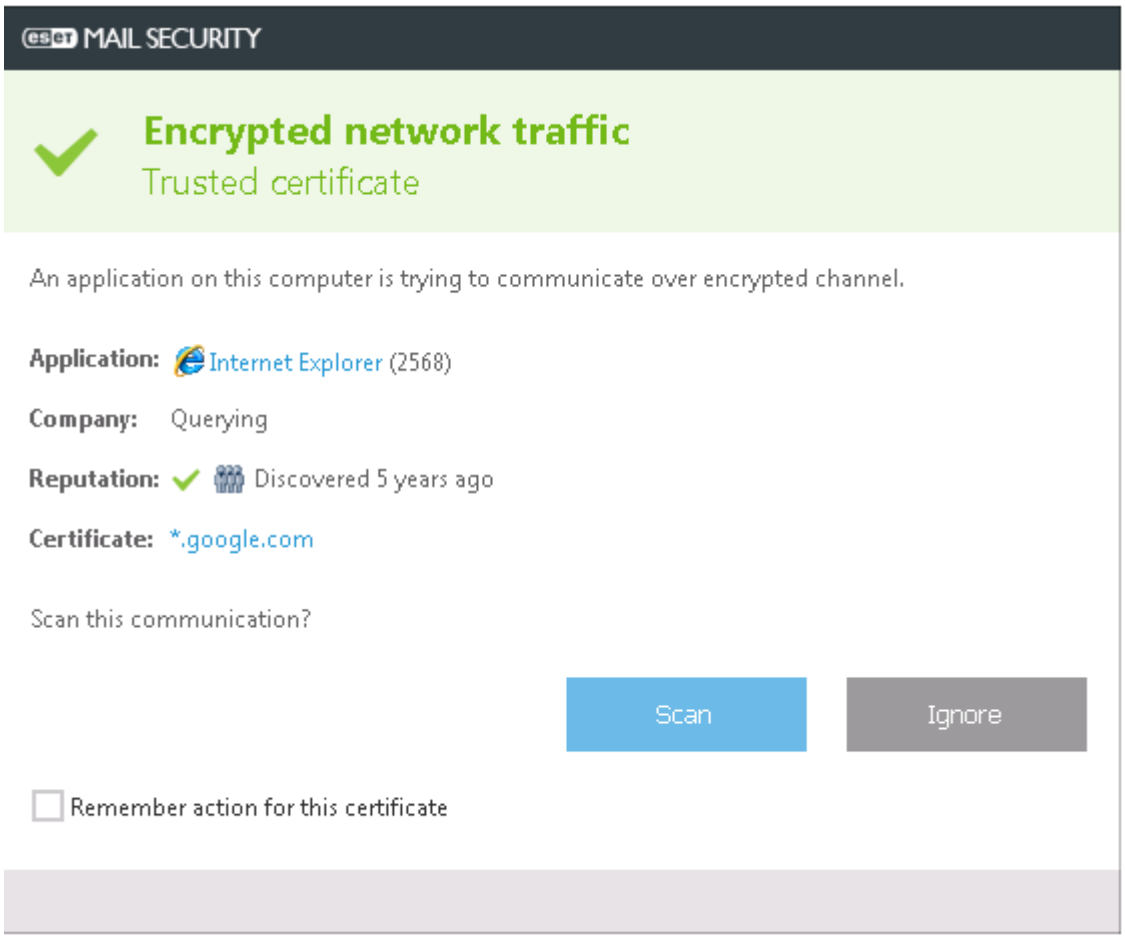
- **自動** – 在自動模式中掃描並在互動模式中詢問。
- **掃描或略過** – 掃描或略過此憑證保護的通訊。
- **詢問** – 遇到特定憑證時收到提示。

加密的 SSL 通訊

若您的系統已配置使用 SSL 通訊協定掃描，用來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 File Security 已配置為在該情況下詢問使用者（依預設，未通過驗證者為是，無有效憑證者為否），這時會出現對話方塊詢問您要［**允許**］或［**封鎖**］該連線。

並且，如果［**SSL 通訊協定過濾模式**］已設定成［**互動模式**］，這時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 File Security 必須［**略過**］該流量以繼續讓應用程式運作。



在這兩種情況下，使用者可以選擇記住選取的處理方法。儲存的處理方法會存放在已知的憑證清單。

電子郵件用戶端防護

ESET File Security 與電子郵件用戶端的整合會針對電子郵件訊息中的惡意代碼，增加作用中的防護層級。如果您的電子郵件用戶端受支援，即可在 ESET File Security 中啟動此整合。如果啟用整合，ESET File Security 工具列會直接插入電子郵件用戶端（不插入較新版的 Windows Live Mail 工具列），以便更有效進行電子郵件防護。

電子郵件用戶端整合

目前支援的電子郵件用戶端包括 Microsoft Outlook、Outlook Express、Windows Mail 和 Windows Live Mail。電子郵件防護是以外掛程式的形式在這些程式中運作。外掛程式的主要優勢為其獨立於所使用的通訊協定。當電子郵件用戶端接收到加密的郵件，它會將其解密並傳送到病毒掃描器。即使未啟用整合，電子郵件通訊仍會受到電子郵件用戶端防護 (POP3、IMAP) 的保護。如需支援的電子郵件用戶端及其版本清單，請參閱以下知識庫文章。

停用收件匣內容變更檢查

如果在處理電子郵件用戶端（僅限 MS Outlook) 時發生系統速度減慢，例如，從 Kerio Outlook Connector Store 擷取電子郵件時會發生這種狀況。

啟用客戶端外掛程式的電子郵件防護

可讓您停用電子郵件用戶端防護，而無需將整合移除至電子郵件用戶端中。您可以立即停用所有外掛程式，或是選擇性地停用下列項目：

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

針對受感染電子郵件執行的處理方法

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

更新後重複掃描

可切換為在偵測引擎更新後重新掃描。

接受其他組件的掃描結果

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

電子郵件通訊協定

啟用通訊協定過濾的電子郵件防護

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

ESET File Security 也支援掃描 IMAPS 和 POP3S 通訊協定，其使用加密的通道以在伺服器與用戶端間傳輸資訊。ESET File Security 會檢查利用 SSL (安全通訊端層）與 TLS (傳輸層安全性）通訊協定的通訊。此程式將只掃描 **IMAPS/POP3S 通訊協定**所使用從［連接埠］中定義連接埠的流量，無論其作業系統的版本為何。

IMAPS / POP3S 掃描器設定

當使用預設值時，則不掃描加密通訊。若要啟用加密通訊的掃描，請瀏覽至 SSL/TLS 通訊協定檢查。

連接埠號碼可識別它是何種類型的連接埠。以下是預設的電子郵件連接埠：

連接埠名稱	連接埠號碼	說明
POP3	110	預設的 POP3 非加密連接埠。
IMAP	143	預設的 IMAP 非加密連接埠。
安全 IMAP (IMAP4-SSL)	585	啟用 SSL/TLS 通訊協定過濾。多個連接埠號必須以逗號分隔。
IMAP4 over SSL (IMAPS)	993	啟用 SSL/TLS 通訊協定過濾。多個連接埠號必須以逗號分隔。
安全 POP3 (SSL-POP)	995	啟用 SSL/TLS 通訊協定過濾。多個連接埠號必須以逗號分隔。

警告及通知

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

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

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

將附註附加到已傳送之受感染電子郵件的主旨

如果您不想讓電子郵件防護在受感染電子郵件的主旨中包含病毒警告，請停用這項功能。此功能允許對受感染電子郵件進行以主旨為基礎的簡單過濾（若電子郵件程式支援）。它也可為收件者提升可靠性，如果偵測到入侵，則會提供有關指定電子郵件或寄件者的重要資訊。

新增到受感染電子郵件主旨的範本

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

MS Outlook 工具列

Microsoft Outlook 防護是以外掛程式模組來運作。安裝 ESET File Security 之後，此包含惡意軟體防護選項的工具列會新增至 Microsoft Outlook

ESET File Security

按一下**圖示**會開啟 ESET File Security 的主要程式視窗。

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，請參閱電子郵件用戶端防護

掃描器設定

顯示電子郵件用戶端防護設定選項。

Outlook Express 及 Windows Mail 工具列

Outlook Express 及 Windows Mail 防護是以外掛程式模組來運作。安裝 ESET File Security 之後，此包含惡意軟體防護選項的工具列會新增至 Outlook Express 或 Windows Mail

ESET File Security

按一下**圖示**會開啟 ESET File Security 的主要程式視窗。

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，請參閱電子郵件用戶端防護

掃描器設定

顯示電子郵件用戶端防護設定選項。

自訂外觀

可以修改電子郵件用戶端的工具列外觀。取消選取該選項以自訂與電子郵件程式參數無關的外觀。

- **[顯示文字]** – 顯示圖示的說明。
- **[文字靠右]** – 選項說明會從圖示的底端移至右側。
- **[大圖示]** – 顯示功能表選項的大圖示。

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。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 File Security 工具列可讓使用者指定多個電子郵件檢查選項。**[重新掃描郵件]** 選項提供兩種掃描模式：

- **位於目前資料夾中的所有郵件** – 掃描目前所顯示資料夾中的郵件。
- **僅限選取的郵件** – 僅掃描使用者標記的郵件。
- **重新掃描已掃描的郵件** – 可供使用者選擇針對先前已掃描的郵件再次執行掃描。

Web 存取防護

Web 存取的運作方式是監視 Web 瀏覽器與遠端伺服器之間的通訊，以保護您免於網路上的威脅，並遵循 HTTP (超文字傳輸通訊協定) 及 HTTPS (加密的通訊) 規則。

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

基本

強烈建議您啟用 **Web 存取防護**功能。此選項也可從 ESET File Security 的主要程式視窗存取，瀏覽至 **[設定] > [Web 和電子郵件] > [Web 存取防護]**。

啟用瀏覽器腳本進階掃描

依預設，Web 瀏覽器執行的所有 JavaScript 程序都會由偵測引擎進行檢查。

Web 通訊協定

可讓您配置監控大多數網際網路瀏覽器使用的這類標準通訊協定。依預設，會將 ESET File Security 配置為監控大多數網際網路瀏覽器使用的 HTTP 通訊協定。

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

當使用預設值時，則不掃描加密通訊。若要啟用加密通訊的掃描，請瀏覽至 **［進階設定］(F5) > [Web 和電子郵件］>** [SSL/TLS]。

ThreatSense 參數

配置此類掃描類型（電子郵件、壓縮檔、排除、限制等），以及 Web 存取防護的偵測方法等設定。

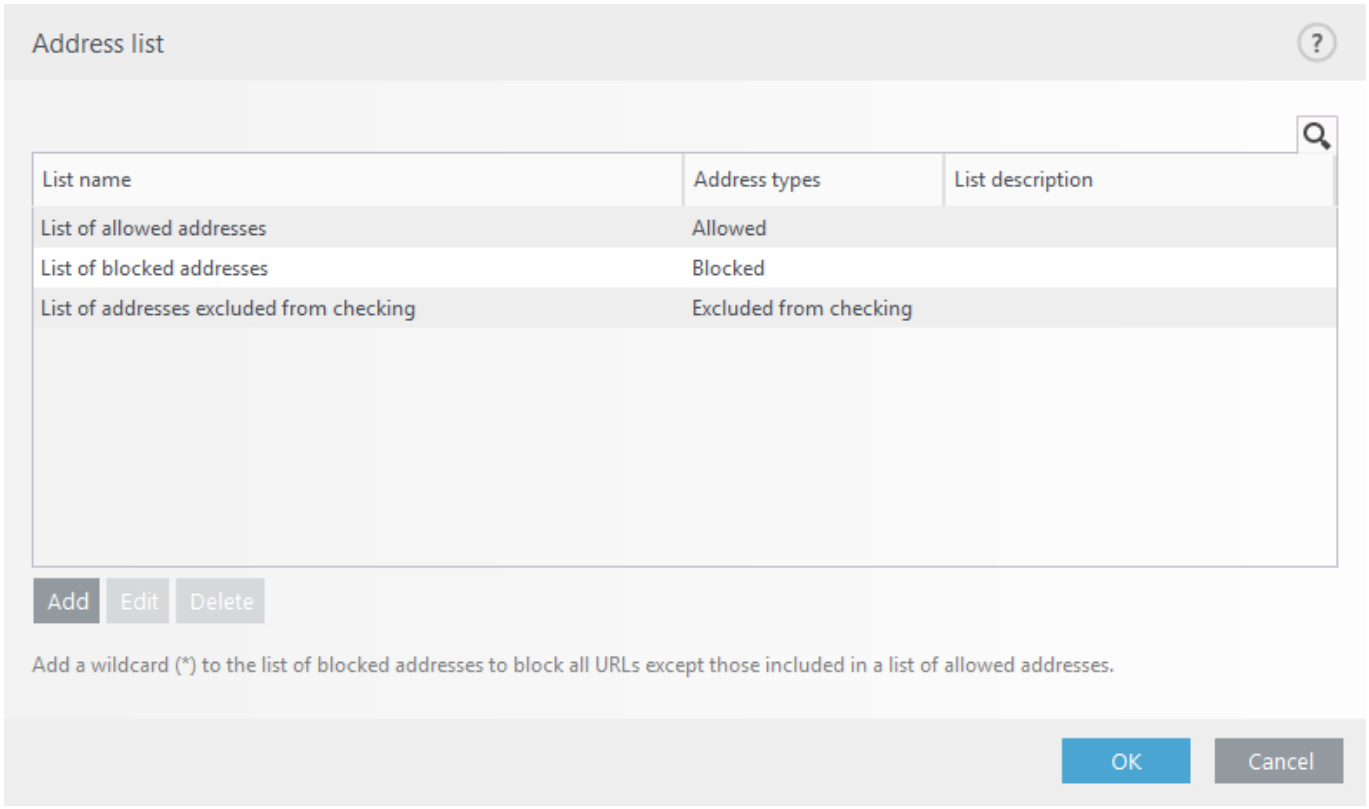
URL 位址管理

URL 位址管理可讓您指定要封鎖、允許或是從檢查排除的 HTTP 位址。除非將封鎖位址清單中的網站納入允許位址清單，否則這些位址將無法存取。存取這些位址時，將不會掃描排除檢查位址清單中的網站是否存有惡意軟體。若除了 HTTP 網頁之外，您也想過濾 HTTPS 位址，則必須啟用SSL/TLS 通訊協定過濾。否則只有您已造訪 HTTPS 網站的網域將會新增，但完整 URL 則不會新增。

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。

按一下**［編輯］**及**［新增］**以建立預先定義清單之外的新位址清單。若您想有邏輯地分隔不同的位址群組，這樣做很有幫助。依預設，下列三個清單可供使用：

- **從檢查中排除的位址清單** – 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。



您可以將新 URL 位址［**新增**］至清單中。您也可以輸入以分行符號分隔的多個值。按一下［**編輯**］以修改清單中的現有位址，或是［**刪除**］予以刪除。僅能刪除使用［**新增**］建立的位址，而無法刪除匯入的位址。

在所有清單中都可以使用特殊符號 *（星號）及 ?(問號)。星號代表任何數字或字元，而問號代表任何單一字元。指定已排除的位址時應該特別小心，因為清單應僅包含受信任及安全位址。同樣地，必須確定在此清單中正確使用字符 * 及 ?。

> 注意
> 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］。

建立新清單

清單會包括想要封鎖、允許或從檢查中排除的 URL 位址/網域遮罩。建立新清單時，請指定以下項目：

- **位址清單類型** – 從下拉式清單中選擇類型（從檢查中排除、封鎖 或 允許）。
- **清單名稱** – 可指定清單的名稱。這個欄位在編輯三個預先定義清單中的一個時會呈現灰色。
- **清單說明** – 可輸入簡短的清單說明（選用）。當編輯三個預先定義清單中的一個時會呈現灰色。
- **作用中的清單** – 使用切換以停用清單。您可以在稍後需要時啟用它。
- **套用時通知** – 若您要在使用特定清單來評估您所造訪的 HTTP 網站時收到通知。當網站遭封鎖或允許時會發出通知，因為其包含在已封鎖或已允許位址的清單中。通知會包含具有指定網站的清單名稱。
- **防護記錄嚴重性** – 從下拉式清單選擇防護記錄嚴重性（無、診斷、資訊或警告）。具有［**警告**］詳細資料的記錄可由 ESET Security Management Center 收集。

ESET File Security 可讓使用者封鎖存取特定網站，避免網際網路瀏覽器顯示其內容。此外，其可讓使用者指

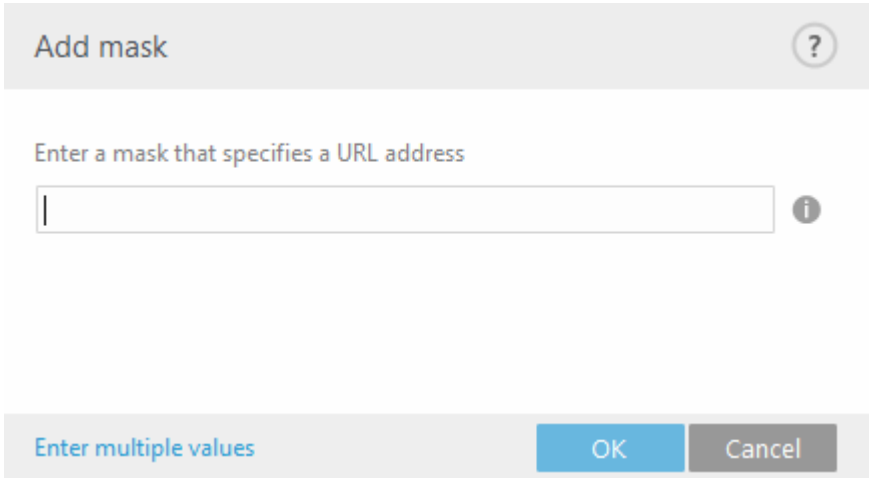
定應從檢查中排除的位址。如果不知道遠端伺服器的完整名稱，或者使用者想要指定遠端伺服器的整個群組，則所謂的遮罩可以用來識別此類群組。

遮罩包括 ？ 及 * 符號：

- 使用 ？ 來取代一個符號
- 使用 * 來取代一個文字字串

> 範例
> *.c?m* 適用於所有位址，其中最後的部分以字母 c 開始，以字母 m 結尾，兩個字母中間包含一個未知的符號（*.com*、*.cam* 等）。

如果網域名稱中的「*.」位於開頭，則需要特別處理。首先，在此情況中 * 萬用字元將無法代表斜線字元（'/'）。這是為了避免規避遮罩，例如遮罩 **.domain.com* 就不會與 *https://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。這是為了能夠比對整個網域，包含任何使用單一遮罩的子網域在內。例如，遮罩 **.domain.com* 也與 *https://domain.com* 相符。使用 **domain.com* 則不正確，因為它也與 *https://anotherdomain.com* 相符。

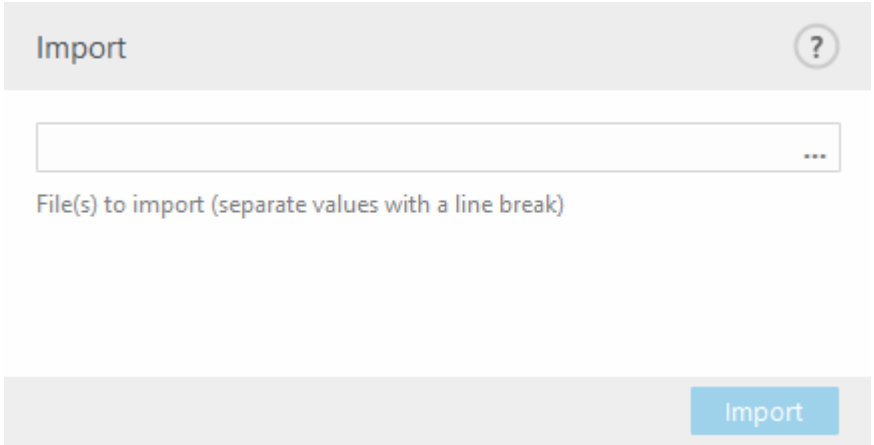


輸入多個值

新增多個 URL 位址，並透過換行、使用逗號或分號來分隔這些位址。當您啟用多個選項時，位址將於清單中顯示。

匯入

匯入包含 URL 位址的文字檔案（使用分行符號分隔的值，例如，使用編碼 UTF-8 的 `*.txt`）

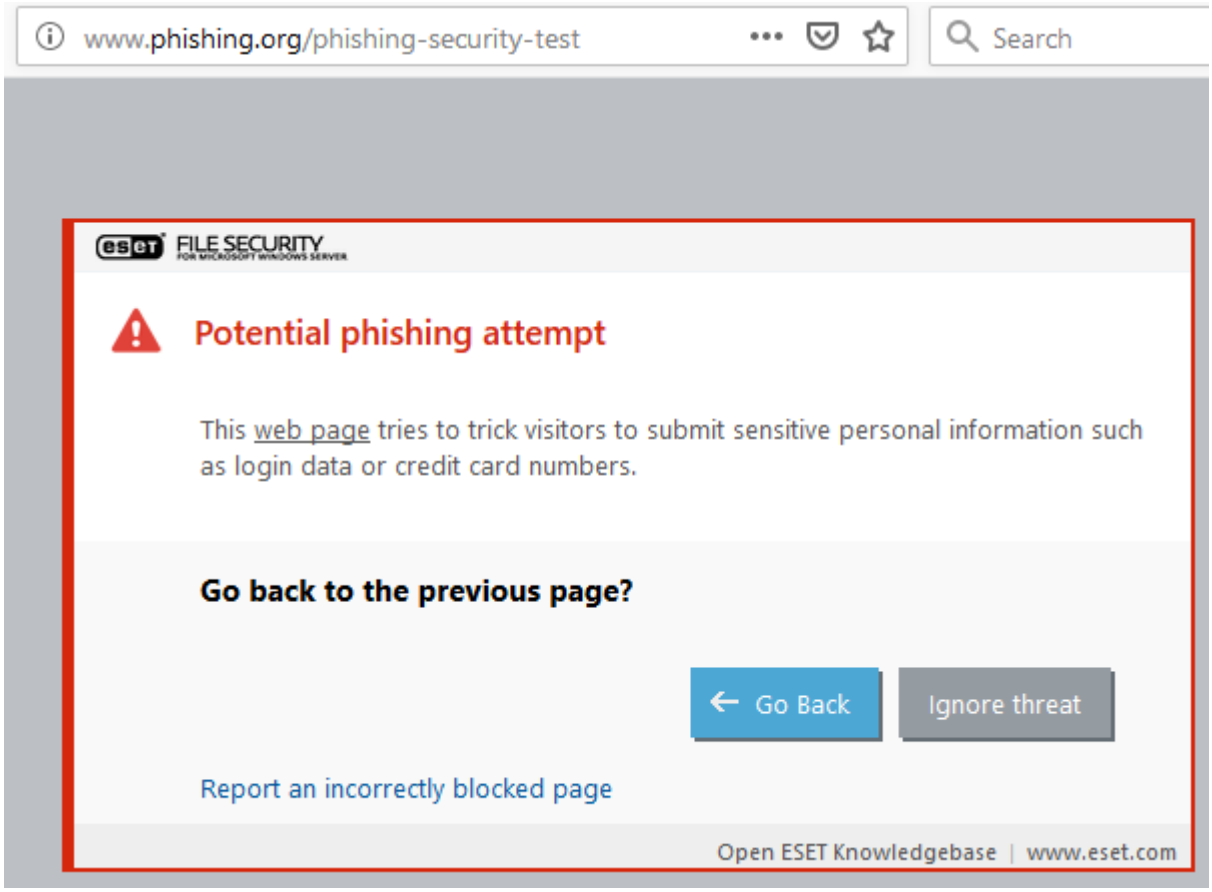


Web 網路釣魚防護

網路釣魚這個詞彙是用來定義利用社交工程（操縱使用者以取得機密資訊）的犯罪活動。網路釣魚通常用於存取像是銀行帳號、PIN 碼等敏感資料。

ESET File Security 包含網路釣魚防護，其會封鎖已知會散播此類型內容的網頁。強烈建議您在 ESET File Security 中啟用防網路釣魚。造訪我們的知識庫文章 以取得 ESET File Security 中網路釣魚防護的詳細資訊。

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



注意
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。

回報網路釣魚網站

如果您在看似會進行網路釣魚或含有惡意的可疑網站上執行，則可向 ESET 回報此事以供分析。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。在此情況下，您可以回報誤判網路釣魚網站

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）。

裝置控制

ESET File Security 包含自動裝置 (CD/DVD/USB/) 控制項。此模組可讓您掃描、封鎖或調整擴充的過濾/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不需要內容的裝置，此功能便非常實用。

> 注意
> 使用［**整合至系統**］開關時，便會啟動 ESET File Security 的裝置控制功能。但是需要重新啟動系統，此項變更才能生效。

裝置控制會變成作用中，可讓您編輯其設定。如果偵測到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。

規則

裝置控制規則會定義符合規則條件的裝置連接到電腦時將採取的處理方法。

群組

按一下［編輯］時，您可以管理裝置群組。建立新的裝置群組或選取現有群組，以便從清單新增或移除裝置。

> 注意
> 您可以檢視防護記錄檔案中的裝置控制防護記錄項目。

裝置規則

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。規則清單中包含數個規則說明，例如名稱、外部裝置類型，以及當偵測到裝置後所執行的處理方法和防護記錄嚴重性。

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

套用期間

您可以使用時段限制規則。先建立時段，該時段便會顯示在下拉式功能表中。

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/...）裝置的類型是從作業系統繼承，而且，如果裝置連接到電腦，可在系統裝置管理程式中看見裝置的類型。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，這些裝置不會提供與使用者有關的資訊，而是僅與動作有關的資訊。這表示影像裝置只能以全域方式封鎖。

處理方法

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

- **讀取/寫入** – 將允許裝置的完整存取權限。
- **封鎖** – 將封鎖裝置的存取權限。
- **唯讀** – 僅允許讀取裝置的存取權限。

- **警告** – 每次連線到一個裝置就會通知使用者是否允許存取該裝置或是要封鎖，並會建立一筆記錄項目。不會記取裝置，針對相同裝置進行後續連線時仍會顯示通知。

> 注意
> 請注意，並非所有裝置類型都適用所有權限（處理方法）。如果裝置有儲存空間，則可使用所有四種處理方法。對於非儲存裝置，只可使用兩種處理方法（例如，**[唯讀]** 不適用於藍牙，因此只能允許或封鎖藍牙裝置）。

下面列出可用來微調規則並針對裝置進行調整的其他參數。所有參數均區分大小寫：

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

> 注意
> 如果這三個描述元全為空白，比對時規則將會忽略這些欄位。所有文字欄位中的過濾參數均不區分大小寫，且不支援萬用字元 (*, ?)。

為了查明裝置的參數，可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。

從下拉式功能表選擇 **[防護記錄嚴重性]**

- **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。
- **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。按一下 **[編輯]** 管理使用者清單。

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

> 注意
> 所有裝置都會受到使用者規則過濾（例如影像裝置不會提供與使用者有關的資訊，而是僅與呼叫的動作有關）。

以下是可用的功能：

編輯

可讓您修改包含在內（供應商、型號、序號）的裝置的選取規則名稱或參數。

複製

會根據選取規則的參數建立新的規則。

刪除

可讓您刪除選取的規則。或者，您可以使用特定規則旁的核取方塊以將其停用。如果您不想要永久刪除規則，以便日後使用，此選項很有用。

填入

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、裝置廠商、型號和序號（若有的話）。當您選取裝置（從「偵測到的裝置」清單）並按一下 **[確定]**，這時規則編輯器視窗會出現並顯示預先定義的資訊（所有設定都能調整）。

規則會依據優先順序列出，順序較高的規則會在頂端。您可以選取多個規則並套用動作，例如按一下［**頂端/向上/向下/底端**］（箭頭按鈕），就能將規則刪除或在清單中向上或向下移動。

裝置群組

［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，視窗左側包含現有群組的清單。選取群組，其中包含您要顯示在右窗格中的裝置。

您可以建立不同裝置群組，並套用不同規則。您也可以建立裝置的單一群組，並設定為 **[讀取/寫入]** 或 **[唯讀]**。這樣可確保在無法辨識的裝置連接至您電腦時，裝置控制會將其封鎖。

> 警告
> 連接至您電腦的外部裝置可能會造成安全性風險。

以下是可用的功能：

新增

會透過輸入裝置群組名稱或新增裝置至現有的群組，並根據您在視窗內按下按鈕的地方，建立新的裝置群組（或者，您可以指定詳細資料，例如供應商名稱、型號和序號）。

編輯

可讓您修改包含在內（供應商、型號、序號）的裝置的選取群組名稱或參數。

刪除

根據您按一下的視窗，刪除所選取的群組或裝置。或者，您可以使用特定規則旁的核取方塊以將其停用。如果您不想要永久刪除規則，以便日後使用，此選項很有用。

匯入

會從檔案匯入裝置的序號清單。

填入

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、裝置廠商、型號和序號（若有的話）。當您選取裝置（從「偵測到的裝置」清單）並按一下 **[確定]**，這時規則編輯器視窗會出現並顯示預先定義的資訊（所有設定都能調整）。

當您完成自訂時，請按一下 **[確定]**。按一下 **[取消]** 以離開 **[裝置群組]** 視窗而不儲存您的變更。

> 注意
> 請注意，並非所有裝置類型都適用所有權限（處理方法）。如果裝置有儲存空間，則可使用所有四種處理方法。對於非儲存裝置，只可使用兩種處理方法（例如，［唯讀］不適用於藍牙，因此只能允許或封鎖藍牙裝置）。

工具配置

您可以為下列項目自訂進階設定：

- 時段
- ERA/ESMC 掃描目標
- 覆寫模式
- ESET CMD
- ESET RMM
- 授權
- WMI 提供者
- 防護記錄檔案
- Proxy 伺服器
- 電子郵件通知
- 簡報模式
- 診斷
- 叢集

時段

在裝置控制規則內使用時段，因此可在套用時限制規則。建立時段並在新增或修改現有規則時選取該時段（**[套用期間]** 參數）。這可讓您定義常用的時段（工作時間、週末等）並輕鬆地重複使用時段，而不需要針對每個規則重新定義時間範圍。時段應該適用於可支援以時間為基礎之控制的規則的任何相關類型。

Microsoft Windows 更新

Windows 更新可針對具有潛在危險性的弱點提供重要的修復程式，並提升電腦的一般安全等級。因此，當有可用的 Microsoft Windows 更新時，立即安裝更新是很重要的。ESET File Security 會根據指定的層級通知您遺漏的更新。以下是可用的層級：

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

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

ESET CMD

此為啟用進階 ecmd 命令的功能。其可讓您使用命令列 (ecmd.exe) 匯出及匯入設定。直到目前為止，僅可以使用 GUI 匯出設定。ESET File Security 配置可匯出到 *.xml* 檔案。

當您已啟用 ESET CMD，有兩個授權方法可以使用：

- **［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 File Security 配置。您可以手動操作或建立指令碼以進行自動化。

重要
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，您會得到 **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。

範例
匯出設定命令：
```
ecmd /getcfg c:\config\settings.xml
```

匯入設定命令：
```
ecmd /setcfg c:\config\settings.xml
```

注意
進階 ecmd 命令只可以在本機執行。使用 ESET Security Management Center 的執行用戶端工作 **［執行命令］** 不會運作。

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)

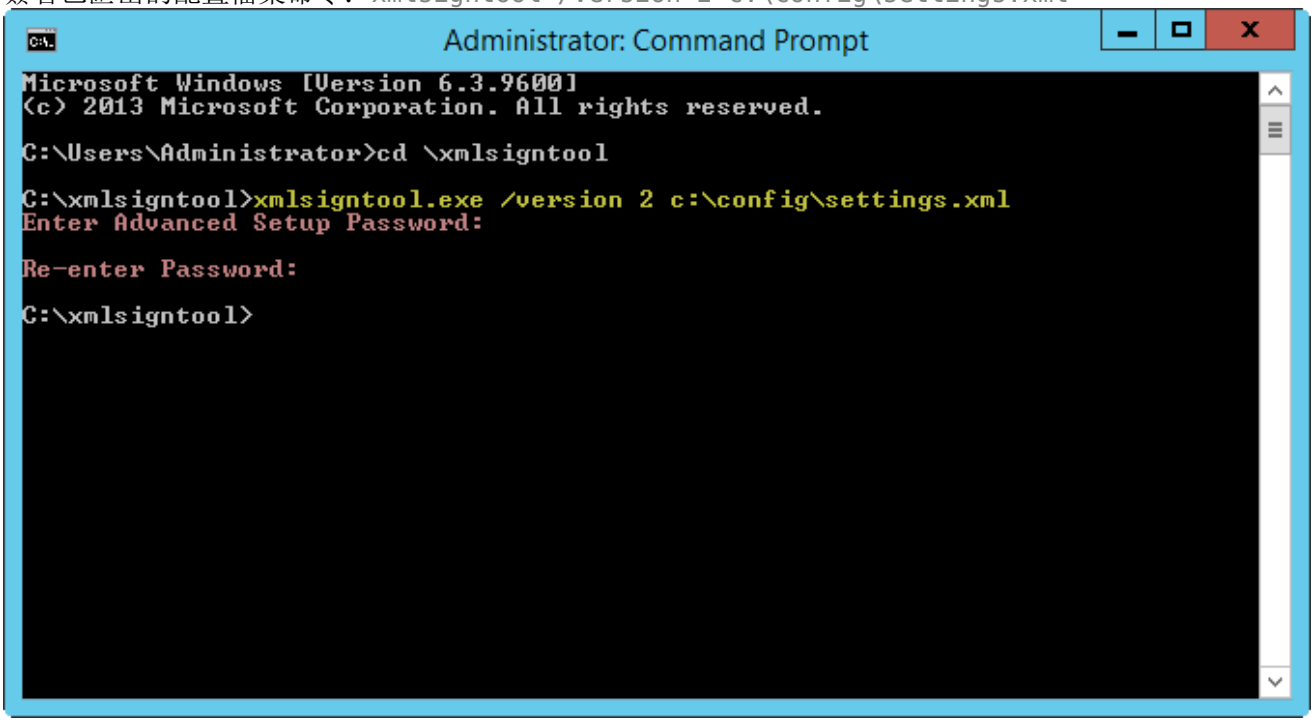
3.瀏覽至 `xmlsigntool.exe` 的位置

4.執行命令以簽署 *.xml* 配置檔案，使用：`xmlsigntool /version 1|2 <xml_file_path>`

重要
`/version` 參數值取決於您的 ESET File Security 版本。針對 ESET File Security 7 及更新版本使用 `/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 File Security 實例，方式為使用密碼授權方法。

範例
簽署已匯出的配置檔案命令：`xmlsigntool /version 2 c:\config\settings.xml`



注意
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，您可以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 File Security 的電腦。

ESET RMM

遠端監視及管理 (RMM) 是監督和控制軟體系統（例如桌面、伺服器和行動裝置上的系統）的程序，會透過本機安裝且可由管理服務提供者存取的代理程式加以進行。

啟用 RMM

可啟用遠端監視及管理命令。您必須有管理員權限才能使用 RMM 公用程式。

工作模式

從下拉式功能表選取 RMM 的工作模式：

- **僅安全隔離** – 如果您希望只對安全和唯讀的作業啟用 RMM 介面
- **所有作業** – 如果您希望對所有作業啟用 RMM 介面

授權方法

從下拉式功能表設定 RMM 授權方法：

- **無** –不會執行應用程式路徑檢查，您可以從任何應用程式執行 *ermm.exe*
- **應用程式路徑** – 指定可執行 *ermm.exe* 的應用程式

預設的 ESET Endpoint Security 安裝包含位於 ESET File Security (預設路徑 *c:\Program Files\ESET\ESET File Security*) 之檔案 *ermm.exe* 的安裝。*ermm.exe* 會和已連結至 RMM 伺服器且會與 RMM 代理程式通訊的

RMM 外掛程式交換資料。

- *ermm.exe* - ESET 命令列開發的命令列公用程式，可管理 Endpoint 產品以及與任何 RMM 外掛程式的通訊。
- RMM 外掛程式 – 在 Endpoint Windows 系統上本機執行的第三方應用程式。外掛程式設計旨在與特定 RMM 外掛程式（例如，僅限 Kaseya 發行的程式）及 *ermm.exe* 通訊。
- RMM 代理程式 – 在 Endpoint Windows 系統上本機執行的第三方應用程式（例如Kaseya 發行的應用程式）。代理程式會與 RMM 外掛程式及 RMM 伺服器通訊。
- RMM 伺服器 – 在第三方伺服器上以服務的形式執行。受支援的 RMM 系統是由 KaseyaLabtechAutotaskMax Focus 及 Solarwinds N-able 所發行。

造訪我們的知識庫文章 以在 ESET File Security 中取得關於 ESET RMM 的詳細資訊。

協力廠商 RMM 解決方案的 ESET 直接端點管理外掛程式

RMM 伺服器正在協力廠商的伺服器上執行服務。如果需要更多資訊，請參閱下列的 ESET 直接端點管理線上使用者指南：

- ConnectWise Automate 的 ESET 直接端點管理外掛程式
- DattoRMM 的 ESET 直接端點管理外掛程式
- Solarwinds N-Central 的 ESET 直接端點管理外掛程式
- NinjaRMM 的 ESET 直接端點管理外掛程式

授權

ESET File Security 會每小時數次連線到 ESET 授權伺服器以執行檢查。**間隔檢查**參數預設值為 **[自動]**。如果您希望降低授權檢查造成的網路流量，請將間隔檢查變更為 **[受限]** 然後重新啟動伺服器，授權檢查的頻率便會降低到每天一次。

當間隔檢查設為 **[受限]**，所有透過 ESET Business Account 和 ESET MSP 管理員對您的 ESET File Security 做出的相關授權變更，都可能會花上一天的時間才能套用。

WMI 提供者

Windows Management Instrumentation (WMI) 是 Microsoft 對於 Web-Based Enterprise Management (WBEM) 的實作，此一業界計畫的目的是為了開發能在企業環境中存取管理資訊的標準技術。

如需有關 WMI 的詳細資訊，請參閱 http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642(v=vs.85).aspx

ESET WMI 提供者

ESET WMI 提供者的目的是為了在企業環境中遠端監控 ESET 產品而不需要使用任何 ESET 特定軟體或工具。在透過 WMI 揭露基本產品、狀態和統計資訊之後，我們將能大幅提升企業系統管理員監控 ESET 產品的效能。管理員可利用 WMI 提供的幾種存取方法（命令列、指令碼和第三方企業監控工具）來監控 ESET 產品的狀態。

目前的實作可讓您以唯讀方式存取基本產品資訊、已安裝的功能與其保護狀態、個別掃描器的統計和產品防護記錄檔案。

WMI 提供者能使用標準 Windows WMI 基礎結構和工具來讀取產品狀態和產品記錄。

提供的資料

所有與 ESET 產品有關的 WMI 類別皆位於root\ESET命名空間。目前已實作下列詳細描述的類別：

一般

- **ESET_Product**
- **ESET_Features**
- **ESET_Statistics**

防護記錄

- **ESET_ThreatLog**
- **ESET_EventLog**
- **ESET_ODFileScanLogs**
- **ESET_ODFileScanLogRecords**
- **ESET_ODServerScanLogs**
- **ESET_ODServerScanLogRecords**
- **ESET_HIPSLog**
- **ESET_URLLog**
- **ESET_DevCtrlLog**
- **ESET_GreylistLog**
- **ESET_MailServeg**
- **ESET_HyperVScanLogs**
- **ESET_HyperVScanLogRecords**

ESET_Product 類別

ESET_Product 類別的執行個體只能有一個。此類別的屬性會參考與已安裝的 ESET 產品有關的基本資訊：

- **ID** – 產品類型識別碼，例如emsl
- **名稱** – 產品名稱，例如ESET Mail Security
- **完整名稱** – 產品名稱，例如IBM Domino 適用的 ESET Mail Security
- **版本** – 產品版本，例如「6.5.14003.0」
- **VirusDBVersion** – 病毒資料庫修訂，例如「14533 (20161201)」
- **VirusDBLastUpdate** – 病毒資料庫上次更新的時間郵戳。以 WMI 日期時間格式包含時間郵戳的字串。例如「20161201095245.000000+060」
- **LicenseExpiration** – 授權到期時間。以 WMI 日期時間格式包含時間郵戳的字串
- **KernelRunning** – 表示 ekrn 服務是否在機器上執行的布林值，例如 “TRUE”
- **StatusCode** – 表示產品防護狀態的數字：0 – 綠色 (正常)，1 – 黃色 (警告)，2 – 紅色 (錯誤)
- **StatusText** – 表示非零狀態碼原因的訊息，否則為 null

ESET_Features 類別

ESET_Features 類別有多個執行個體，視產品功能的數目而定。每個執行個體均包含：

- **Name** – 功能的名稱 (名稱清單如下所述)
- **Status** – 功能的狀態：0 – 作用中，1 – 已停用，2 – 已啟用

表示目前已識別的產品功能的字串清單：

- **CLIENT_FILE_AV** – 即時檔案系統病毒防護
- **CLIENT_WEB_AV** – 用戶端 Web 病毒防護
- **CLIENT_DOC_AV** – 用戶端文件病毒防護
- **CLIENT_NET_FW** – 用戶端個人防火牆
- **CLIENT_EMAIL_AV** – 用戶端電子郵件病毒防護
- **CLIENT_EMAIL_AS** – 用戶端垃圾電子郵件防護
- **SERVER_FILE_AV** – 受保護檔案伺服器產品上的即時檔案病毒防護，例如 ESET File Security 中，SharePoint 內容資料庫的檔案
- **SERVER_EMAIL_AV** – 受保護伺服器產品的電子郵件病毒防護，例如 MS Exchange 或 IBM Domino 中的電子郵件
- **SERVER_EMAIL_AS** – 受保護伺服器產品的垃圾電子郵件防護，例如 MS Exchange 或 IBM Domino 中的電子郵件
- **SERVER_GATEWAY_AV** – 閘道上受保護網路通訊協定的病毒防護
- **SERVER_GATEWAY_AS** – 閘道上受保護網路通訊協定的垃圾郵件防護

ESET_Statistics 類別

ESET_Statistics 類別有多個執行個體，視產品中的掃描器數目而定。每個執行個體均包含：

- **Scanner** – 特殊掃描器的字串碼，例如CLIENT_FILE
- **Total** – 掃描的檔案總數
- **Infected** – 已發現受感染的檔案數目
- **Cleaned** – 已清除的檔案數目
- **Timestamp** – 上次變更此統計資料的時間郵戳。以 WMI 日期時間格式表示，例如「20130118115511.000000+060」
- **ResetTime** – 上次重設統計資料計數器的時間郵戳。以 WMI 日期時間格式表示，例如「20130118115511.000000+060」

表示目前已識別之掃描器的字串清單：

- **CLIENT_FILE**
- **CLIENT_EMAIL**
- **CLIENT_WEB**
- **SERVER_FILE**
- **SERVER_EMAIL**
- **SERVER_WEB**

ESET_ThreatLog 類別

ESET_ThreatLog 類別有多個執行個體，每個都代表一筆Detected threats的防護記錄。每個執行個體均包含：

- **ID** – 此掃描防護記錄的唯一 ID
- **Timestamp** – 建立防護記錄的時間郵戳（使用 WMI 日期/時間格式）
- **LogLevel** – 以數字［0-8］表示的防護記錄嚴重性層級。對應下列具名層級的值Debug Info-Footnote Info Info-Important Warning Error SecurityWarning Error-Critical SecurityWarning-Critical
- **Scanner** – 建立此防護記錄事件的掃描器名稱
- **ObjectType** – 產生此防護記錄事件的物件類型
- **ObjectName** – 產生此防護記錄事件的物件名稱

- **Threat** – 在 ObjectName 和 ObjectType 屬性所描述的物件中發現的威脅名稱
- **Action** – 在識別威脅之後執行的處理方法
- **User** – 導致此防護記錄事件產生的使用者帳戶
- **Information** – 事件的其他說明
- **Hash** – 產生此防護記錄事件的物件雜湊

ESET_EventLog

ESET_EventLog 類別有多個執行個體，每個都代表一筆「Events」的防護記錄。每個執行個體均包含：

- **ID** – 此掃描防護記錄的唯一 ID
- **Timestamp** – 建立防護記錄的時間郵戳（使用 WMI 日期/時間格式）
- **LogLevel** – 以數字 [0–8] 間隔表示的防護記錄嚴重性層級。對應下列具名層級的值「Debug」「Info-Footnote」「Info」「Info-Important」「Warning」「Error」「SecurityWarning」「Error-Critical」「SecurityWarning-Critical」
- **Module** – 建立此防護記錄事件的模組名稱
- **Event** – 事件的說明。
- **User** – 導致此防護記錄事件產生的使用者帳戶

ESET_ODFileScanLogs

ESET_ODFileScanLogs 類別有多個執行個體，每個都代表一筆指定檔案掃描的記錄。這等同於防護記錄的 GUI「指定電腦掃描」清單。每個執行個體均包含：

- **ID** – 此掃描防護記錄的唯一 ID
- **Timestamp** – 建立防護記錄的時間郵戳（使用 WMI 日期/時間格式）
- **Targets** – 掃描的目標資料夾/物件
- **TotalScanned** – 掃描的物件總數
- **Infected** – 發現的受感染物件數目
- **Cleaned** – 已清除的物件數目
- **Status** – 掃描程序的狀態

ESET_ODFileScanLogRecords

ESET_ODFileScanLogRecords 類別有多個執行個體，每個都代表一筆防護記錄，這些記錄都位於 ESET_ODFileScanLogs 類別執行個體所表示的其中一個掃描防護記錄中。此類別的執行個體提供所有指定掃描/記錄的防護記錄。如果只要求特殊掃描防護記錄的執行個體，則必須由 LogID 屬性過濾。每個類別執行個體均包含：

- **LogID** – 此記錄所屬的掃描防護記錄 ID (ESET_ODFileScanLogs 類別的其中一個執行個體的 ID)
- **ID** – 此掃描防護記錄的唯一 ID
- **Timestamp** – 建立防護記錄的時間郵戳（使用 WMI 日期/時間格式）
- **LogLevel** – 以數字 [0–8] 表示的防護記錄嚴重性層級。對應下列具名層級的值「Debug」「Info-Footnote」「Info」「Info-Important」「Warning」「Error」「SecurityWarning」「Error-Critical」「SecurityWarning-Critical」
- **Log** – 實際的防護記錄訊息

ESET_ODServerScanLogs

ESET_ODServerScanLogs類別有多個執行個體，每個都代表執行一次指定伺服器掃描。每個執行個體均包含：

- **ID** – 此掃描防護記錄的唯一 ID
- **Timestamp** – 建立防護記錄的時間郵戳（使用 WMI 日期/時間格式）
- **Targets** – 掃描的目標資料夾/物件

- **TotalScanned** – 掃描的物件總數
- **Infected** – 發現的受感染物件數目
- **Cleaned** – 已清除的物件數目
- **RuleHits** – 規則命中總數
- **Status** – 掃描程序的狀態

ESET_ODServerScanLogRecords

ESET_ODServerScanLogRecords 類別有多個執行個體，每個都代表一筆防護記錄，這些記錄都位於 ESET_ODServerScanLog 類別執行個體所表示的其中一個掃描防護記錄中。此類別的執行個體提供所有指定掃描/記錄的防護記錄。如果只要求特殊掃描防護記錄的執行個體，則必須由 LogID 屬性過濾。每個類別執行個體均包含：

- **LogID** – 此記錄所屬的掃描防護記錄 ID (ESET_ ODServerScanLogs 類別的其中一個執行個體的 ID)
- **ID** – 此掃描防護記錄的唯一 ID
- **Timestamp** – 建立防護記錄的時間郵戳（使用 WMI 日期/時間格式）
- **LogLevel** – 以數字［0–8］間隔表示的防護記錄嚴重性層級。對應下列具名層級的值Debug Info-Footnote Info Info-Important Warning Error SecurityWarning Error-Critical SecurityWarning-Critical
- **Log** – 實際的防護記錄訊息

ESET_SmtpProtectionLog

ESET_SmtpProtectionLog 類別有多個執行個體，每個都代表一筆Smtp 防護」的防護記錄。每個執行個體均包含：

- **ID** – 此掃描防護記錄的唯一 ID
- **Timestamp** – 建立防護記錄的時間郵戳（使用 WMI 日期/時間格式）
- **LogLevel** – 以數字［0–8］表示的防護記錄嚴重性層級。對應下列具名層級的值Debug Info-Footnote Info Info-Important Warning Error SecurityWarning Error-Critical SecurityWarning-Critical
- **HELODomain** - HELO 網域的名稱
- **IP** – 來源 IP 位址
- **Sender** – 電子郵件寄件者
- **Recipient** – 電子郵件收件者
- **ProtectionType** – 所使用的防護類型
- **Action** – 執行的處理方法
- **原因** – 處理方法的原因
- **TimeToAccept** – 開始接受電子郵件之前的分鐘數

ESET_HIPSLog

ESET_HIPSLog 類別有多個執行個體，每個都代表一筆HIPS的防護記錄。每個執行個體均包含：

- **ID** – 此防護記錄的唯一 ID
- **Timestamp** – 建立防護記錄的時間郵戳（使用 WMI 日期/時間格式）
- **LogLevel** – 以數字［0–8］間隔表示的防護記錄嚴重性層級。對應下列具名層級的值Debug Info-Footnote Info Info-Important Warning Error SecurityWarning Error-Critical SecurityWarning-Critical
- **Application** – 來源應用程式
- **Target** – 作業類型
- **Action** - HIPS 採取的處理方法，例如，允許、拒絕等。
- **Rule** – 負責該處理方法的規則名稱
- **AdditionalInfo**

ESET_URLLog

ESET_URLLog 類別有多個執行個體，每個都代表一筆「過濾的網站」的防護記錄。每個執行個體均包含：

- **ID** – 此防護記錄的唯一 ID
- **Timestamp** – 建立防護記錄的時間郵戳（使用 WMI 日期/時間格式）
- **LogLevel** – 以數字 [0–8] 表示的防護記錄嚴重性層級。對應下列具名層級的值Debug、Info-Footnote、Info、Info-Important、Warning、Error、SecurityWarning、Error-Critical、SecurityWarning-Critical
- **URL** - URL
- **Status** - URL 發生什麼情況，例如「由 Web 控制封鎖」
- **Application** – 嘗試存取該 URL 的應用程式
- **User** – 應用程式在其中執行的使用者帳戶

ESET_DevCtrlLog

ESET_DevCtrlLog 類別有多個執行個體，每個都代表一筆「裝置控制」的防護記錄。每個執行個體均包含：

- **ID** – 此防護記錄的唯一 ID
- **Timestamp** – 建立防護記錄的時間郵戳（使用 WMI 日期/時間格式）
- **LogLevel** – 以數字 [0–8] 表示的防護記錄嚴重性層級。對應下列具名層級的值Debug、Info-Footnote、Info、Info-Important、Warning、Error、SecurityWarning、Error-Critical、SecurityWarning-Critical
- **Device** – 裝置名稱
- **User** – 使用者帳戶名稱
- **UserSID** – 使用者帳戶 SID
- **Group** – 使用者群組名稱
- **GroupSID** – 使用者群組 SID
- **Status** – 裝置發生什麼情況，例如「寫入遭到封鎖」
- **DeviceDetails** – 關於此裝置的其他資訊
- **EventDetails** – 關於此事件的其他資訊

ESET_MailServerLog

ESET_MailServerLog 類別有多個執行個體，每個都代表一筆「郵件伺服器」的防護記錄。每個執行個體均包含：

- **ID** – 此防護記錄的唯一 ID
- **Timestamp** – 建立防護記錄的時間郵戳（使用 WMI 日期/時間格式）
- **LogLevel** – 以數字 [0–8] 表示的防護記錄嚴重性層級。對應下列具名層級的值Debug、Info-Footnote、Info、Info-Important、Warning、Error、SecurityWarning、Error-Critical、SecurityWarning-Critical
- **IPAddr** – 來源 IP 位址
- **HELODomain** - HELO 網域的名稱
- **Sender** – 電子郵件寄件者
- **Recipient** – 電子郵件收件者
- **主旨** –電子郵件主旨
- **ProtectionType** – 執行目前防護記錄（例如，惡意軟體防護、垃圾郵件防護或規則）所述處理方法的防護類型。
- **Action** – 執行的處理方法
- **Reason** – 指定防護類型要在物件上執行處理方法的原因。

ESET_HyperVScanLogs

ESET_HyperVScanLogs 類別有多個執行個體，每個都代表一筆 Hyper-V 檔案掃描的記錄。這等同於防護記錄的 GUI「Hyper-V 掃描」清單。每個執行個體均包含：

- **ID** – 此防護記錄的唯一 ID
- **Timestamp** – 建立防護記錄的時間郵戳（使用 WMI 日期/時間格式）
- **Targets** – 掃描的目標機器/磁碟/磁碟區
- **TotalScanned** – 掃描的物件總數
- **Infected** – 發現的受感染物件數目
- **Cleaned** – 已清除的物件數目
- **Status** – 掃描程序的狀態

ESET_HyperVScanLogRecords

ESET_HyperVScanLogRecords 類別有多個執行個體，每個都代表一筆防護記錄，這些記錄都位於 ESET_HyperVScanLogs 類別執行個體所表示的其中一個掃描防護記錄中。此類別的執行個體提供所有 Hyper-V 掃描/記錄的防護記錄。如果只要求特殊掃描防護記錄的執行個體，則必須由 LogID 屬性過濾。每個類別執行個體均包含：

- **LogID** – 此記錄所屬的掃描防護記錄 ID (ESET_HyperVScanLogs 類別的其中一個執行個體的 ID)
- **ID** – 此防護記錄的唯一 ID
- **Timestamp** – 建立防護記錄的時間郵戳（使用 WMI 日期/時間格式）
- **LogLevel** – 以數字［0–8］表示的防護記錄嚴重性層級。對應下列具名層級的值：Debug、Info-Footnote、Info、Info-Important、Warning、Error、SecurityWarning、Error-Critical、SecurityWarning-Critical
- **Log** – 實際的防護記錄訊息

ESET_NetworkProtectionLog

ESET_NetworkProtectionLog 類別有多個執行個體，每個都代表一筆「網路防護」的防護記錄。每個執行個體均包含：

- **ID** – 此防護記錄的唯一 ID
- **Timestamp** – 建立防護記錄的時間郵戳（使用 WMI 日期/時間格式）
- **LogLevel** – 以數字［0–8］表示的防護記錄嚴重性層級。對應下列具名層級的值：Debug、Info-Footnote、Info、Info-Important、Warning、Error、SecurityWarning、Error-Critical、SecurityWarning-Critical
- **事件** – 觸發網路防護處理方法的事件
- **處理方法** – 網路防護執行的處理方法
- **來源** – 網路裝置的來源位址
- **目標** – 網路裝置的目標位址
- **通訊協定** – 用於網路通訊的通訊協定
- **RuleOrWormName** – 與事件相關的規則或蠕蟲名稱
- **應用程式** – 啟動網路通訊的應用程式
- **User** – 導致此防護記錄事件產生的使用者帳戶

ESET_SentFilesLog

ESET_SentFilesLog 類別有多個執行個體，每個都代表一筆「已傳送檔案」的防護記錄。每個執行個體均包含：

- **ID** – 此防護記錄的唯一 ID
- **Timestamp** – 建立防護記錄的時間郵戳（使用 WMI 日期/時間格式）
- **LogLevel** – 以數字［0–8］表示的防護記錄嚴重性層級。對應下列具名層級的值：Debug、Info-Footnote、Info、Info-Important、Warning、Error、SecurityWarning、Error-Critical、SecurityWarning-Critical

- **Sha1** – 已傳送檔案的 Sha-1 雜湊
- **檔案** – 已傳送的檔案
- **大小** – 已傳送檔案的大小
- **類別** – 已傳送檔案的類別
- **原因** – 傳送檔案的原因
- **SentTo** – 要將檔案傳送至哪一個 ESET 部門
- **User** – 導致此防護記錄事件產生的使用者帳戶

ESET_OneDriveScanLogs

ESET_OneDriveScanLogs 類別有多個執行個體，每個都代表 OneDrive 掃描執行。這等同於防護記錄的 GUI 「OneDrive 掃描」清單。每個執行個體均包含：

- **ID** – 此 OneDrive 防護記錄的唯一 ID
- **Timestamp** – 建立防護記錄的時間郵戳（使用 WMI 日期/時間格式）
- **Targets** – 掃描的目標資料夾/物件
- **TotalScanned** – 掃描的物件總數
- **Infected** – 發現的受感染物件數目
- **Cleaned** – 已清除的物件數目
- **Status** – 掃描程序的狀態

ESET_OneDriveScanLogRecords

ESET_OneDriveScanLogRecords 類別有多個執行個體，每個都代表一筆防護記錄，這些記錄都位於 ESET_OneDriveScanLogs 類別執行個體所表示的其中一個掃描防護記錄中。此類別的執行個體提供所有 OneDrive 掃描/防護記錄的防護記錄。如果只要求特殊掃描防護記錄的執行個體，則必須由 LogID 屬性過濾。每個執行個體均包含：

- **LogID** – 此記錄所屬的掃描防護記錄 ID (ESET_OneDriveScanLogs 類別的其中一個執行個體的 ID)
- **ID** – 此 OneDrive 防護記錄的唯一 ID
- **Timestamp** – 建立防護記錄的時間郵戳（使用 WMI 日期/時間格式）
- **LogLevel** – 以數字［0–8］表示的防護記錄嚴重性層級。對應下列具名層級的值：Debug、Info-Footnote、Info、Info-Important、Warning、Error、SecurityWarning、Error-Critical、SecurityWarning-Critical
- **Log** – 實際的防護記錄訊息

存取提供的資料

以下是一些如何從 Windows 命令列和 PowerShell 存取 ESET WMI 資料的範例，並可適用於任何目前的 Windows 作業系統。不過仍有其他許多方法可存取其他指令碼語言和工具。

不含指令碼的命令列

`wmic` 命令列工具可用來存取各種預先定義或任何自訂的 WMI 類別。

若要顯示與本機產品有關的完整資訊：

```
wmic /namespace:\\root\ESET Path ESET_Product
```

若只要顯示本機產品的產品版本號碼：

```
wmic /namespace:\\root\ESET Path ESET_Product Get Version
```

若要顯示與遠端機器 (IP 10.1.118.180) 產品有關的完整資訊：

```
wmic /namespace:\\root\ESET /node:10.1.118.180 /user:Administrator Path ESET_Product
```

PowerShell

取得及顯示與本機產品有關的完整資訊：

```
Get-WmiObject ESET_Product -namespace 'root\ESET'
```

取得及顯示與遠端機器 (IP 10.1.118.180) 產品有關的完整資訊：

```
$cred = Get-Credential # 提示使用者的憑證並以變數儲存
Get-WmiObject ESET_Product -namespace 'root\ESET' -computername '10.1.118.180' -cred
$cred
```

ERA/ESMC 掃描目標

此功能可讓 ESET Security Management Center 在具有 ESET File Security 的伺服器上執行**伺服器掃描**用戶端工作時，及為 Hyper-V 掃描使用掃描目標（指定信箱資料庫掃描）。只有在您已安裝 ESET Management Agent 時，ERA/ESMC 掃描目標設定才可供使用，否則會呈現灰色（停用）狀態。

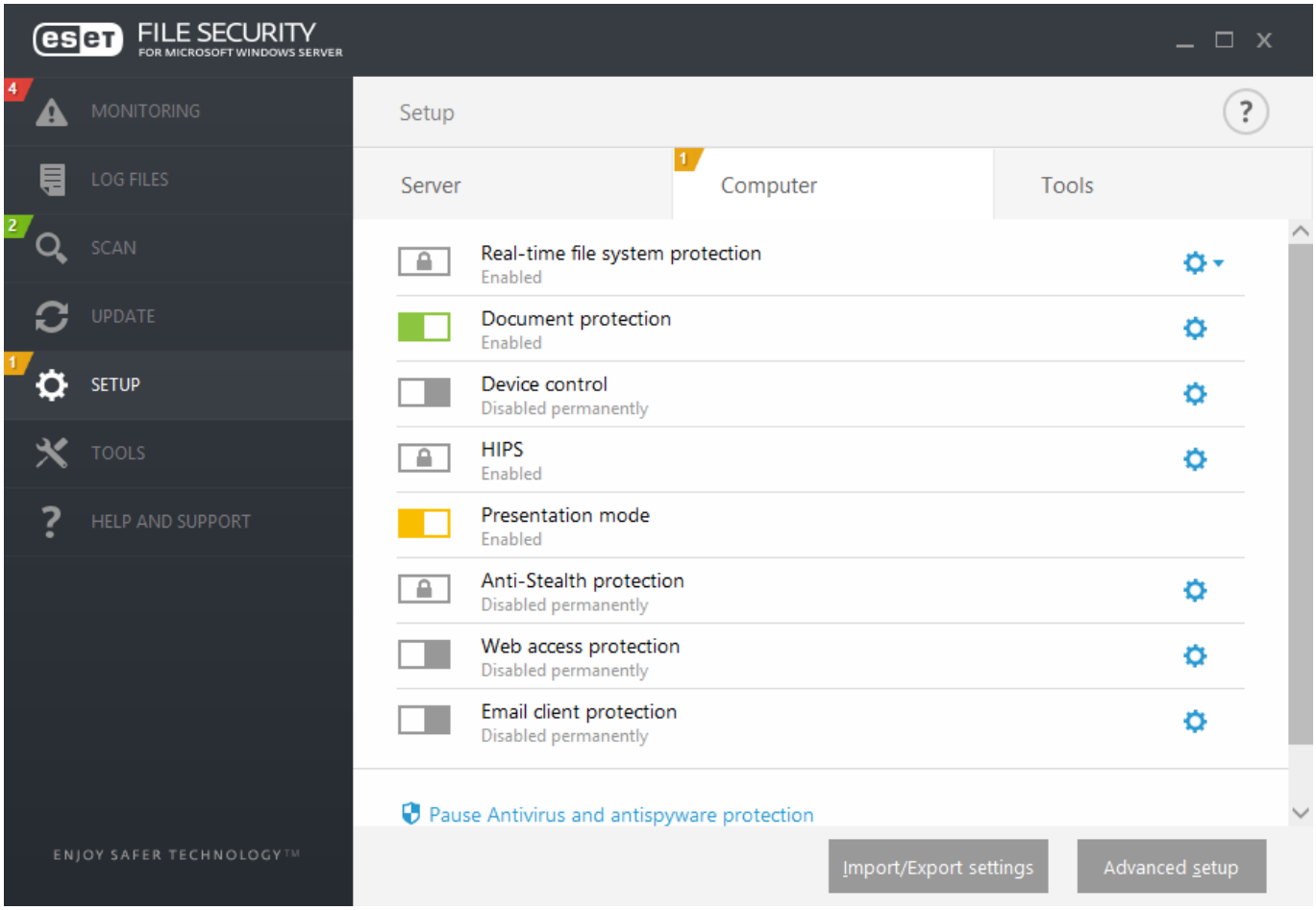
當您啟用［**產生目標清單**］時，ESET File Security 會建立可用的掃描目標清單。此清單會根據您的［**更新期間**］定期產生。

> 注意
> 第一次啟用［**產生目標清單**］時，ESET Security Management Center 約需指定［**更新期間**］的一半時間來作業。假設［**更新期間**］設為 60 分鐘，ESMC 約需 30 分鐘接收掃描目標清單。若您需要 ESET Security Management Center 更快收集清單，請將更新期間設為較小的數值。您可以稍後再增加數值。

當 ESET Security Management Center 要執行［**伺服器掃描**］用戶端工作時，會收集清單並要求您選取要在該特定伺服器上進行 Hyper-V 掃描的掃描目標。

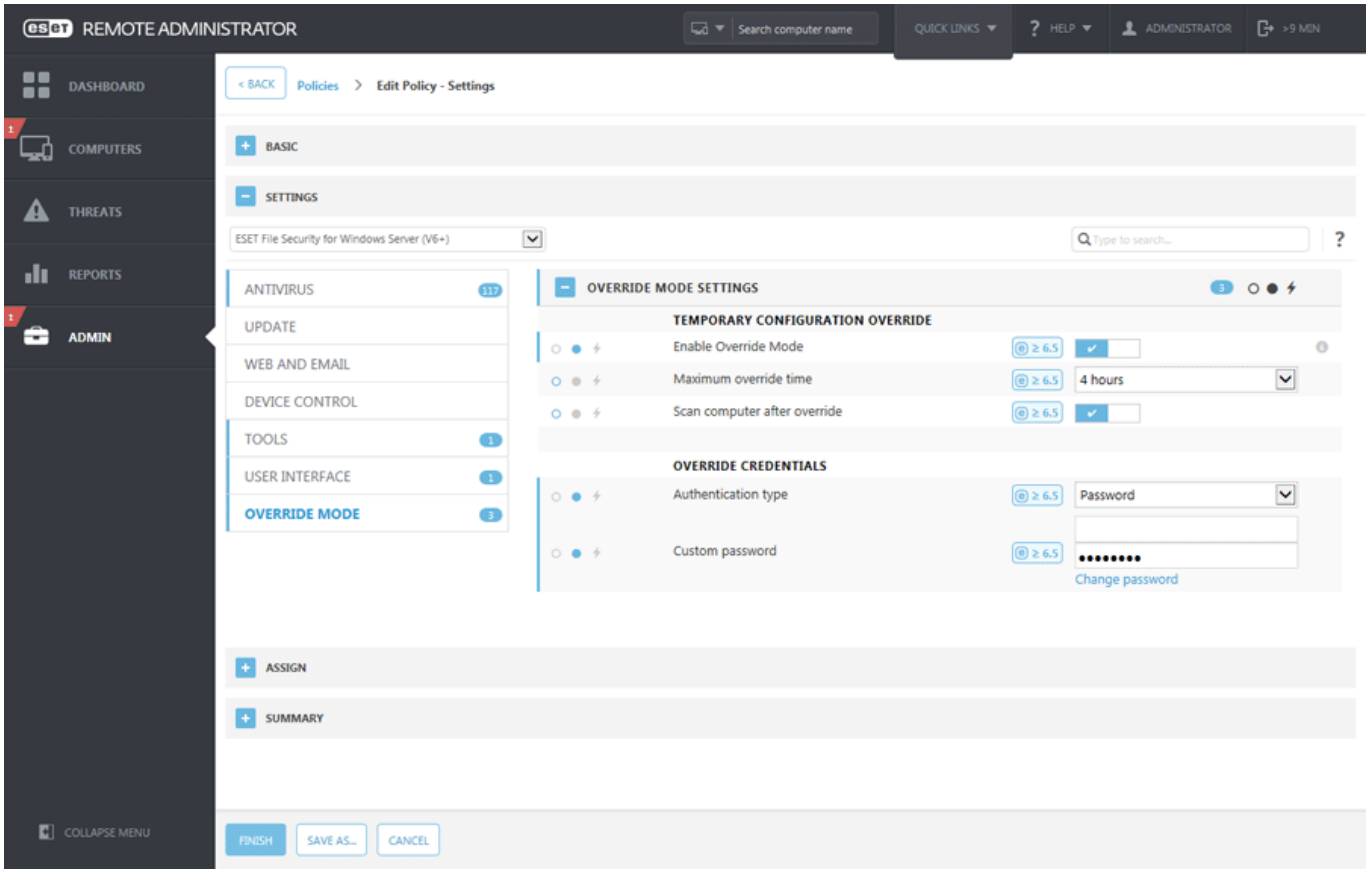
覆寫模式

如果您將 ESET Security Management Center 原則套用至 ESET File Security，您將會看到鎖定圖示  ，而不是在設定頁面上看到啟用/停用開關，也不是［**進階設定**］視窗中鎖定圖示旁邊的開關。

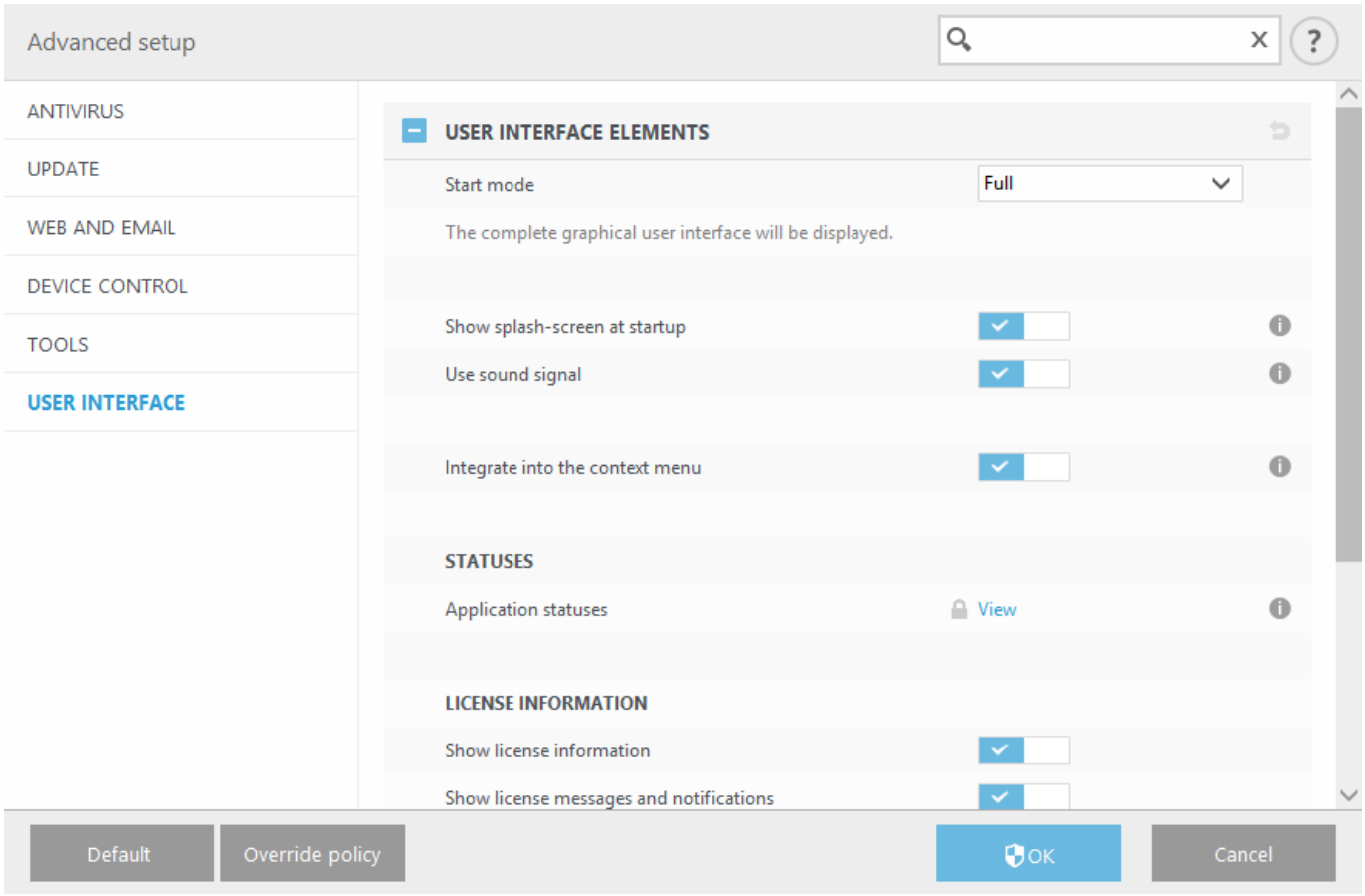


通常，無法修改透過 ESET Security Management Center 原則配置的設定。覆寫模式可讓您暫時解除鎖定這些設定。然而，您必須使用 ESET Security Management Center 原則啟用 **[覆寫模式]**。

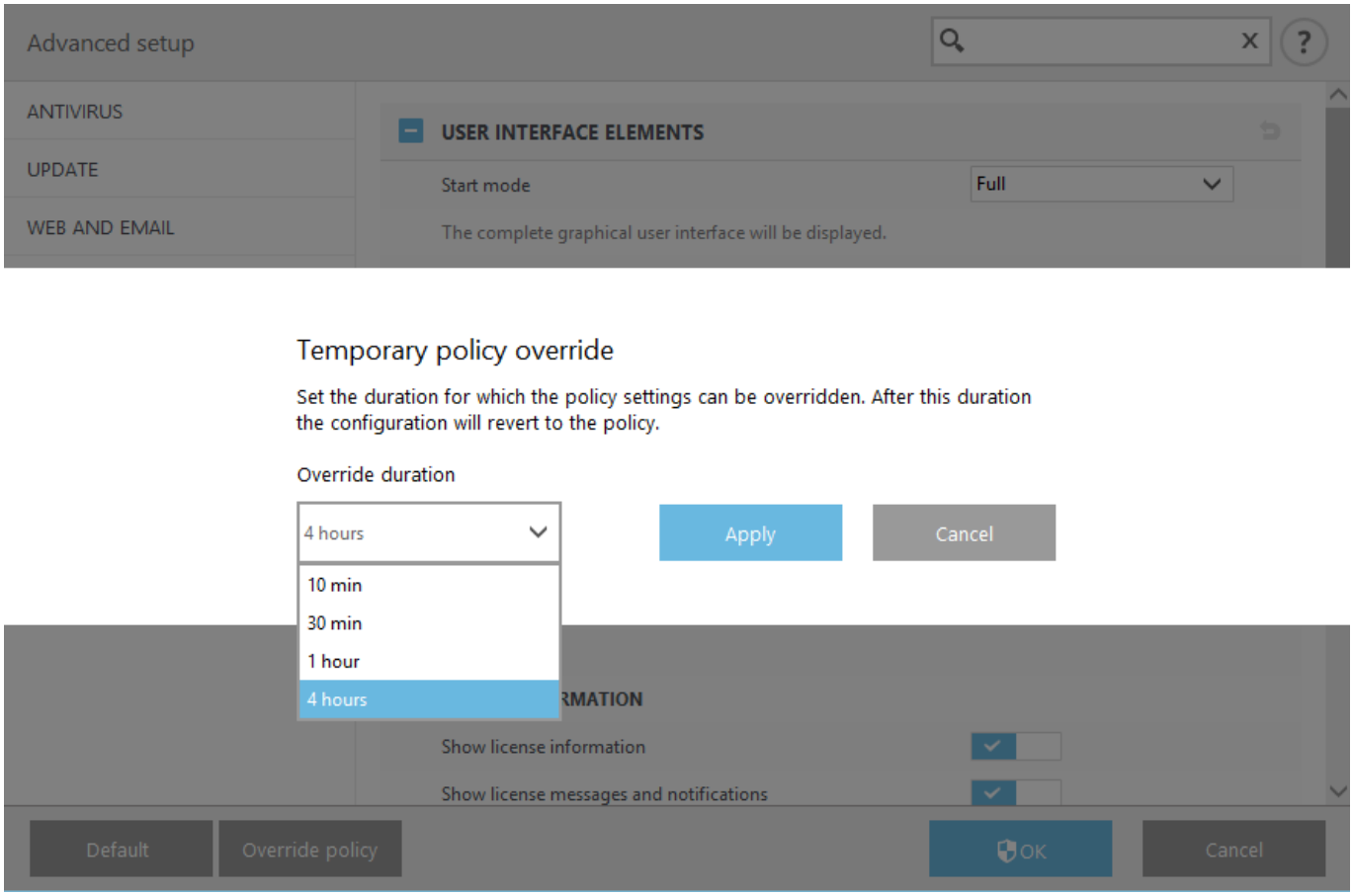
登入至 ESMC Web Console，瀏覽至 **[原則]**，選取並編輯套用至 ESET File Security 的現有原則，或建立一個新原則。在 **[設定]** 中，按一下 **[覆寫模式]**，將其啟用並配置剩餘的設定，包含驗證類型（**[Active directory 使用者]** 或 **[密碼]**）。



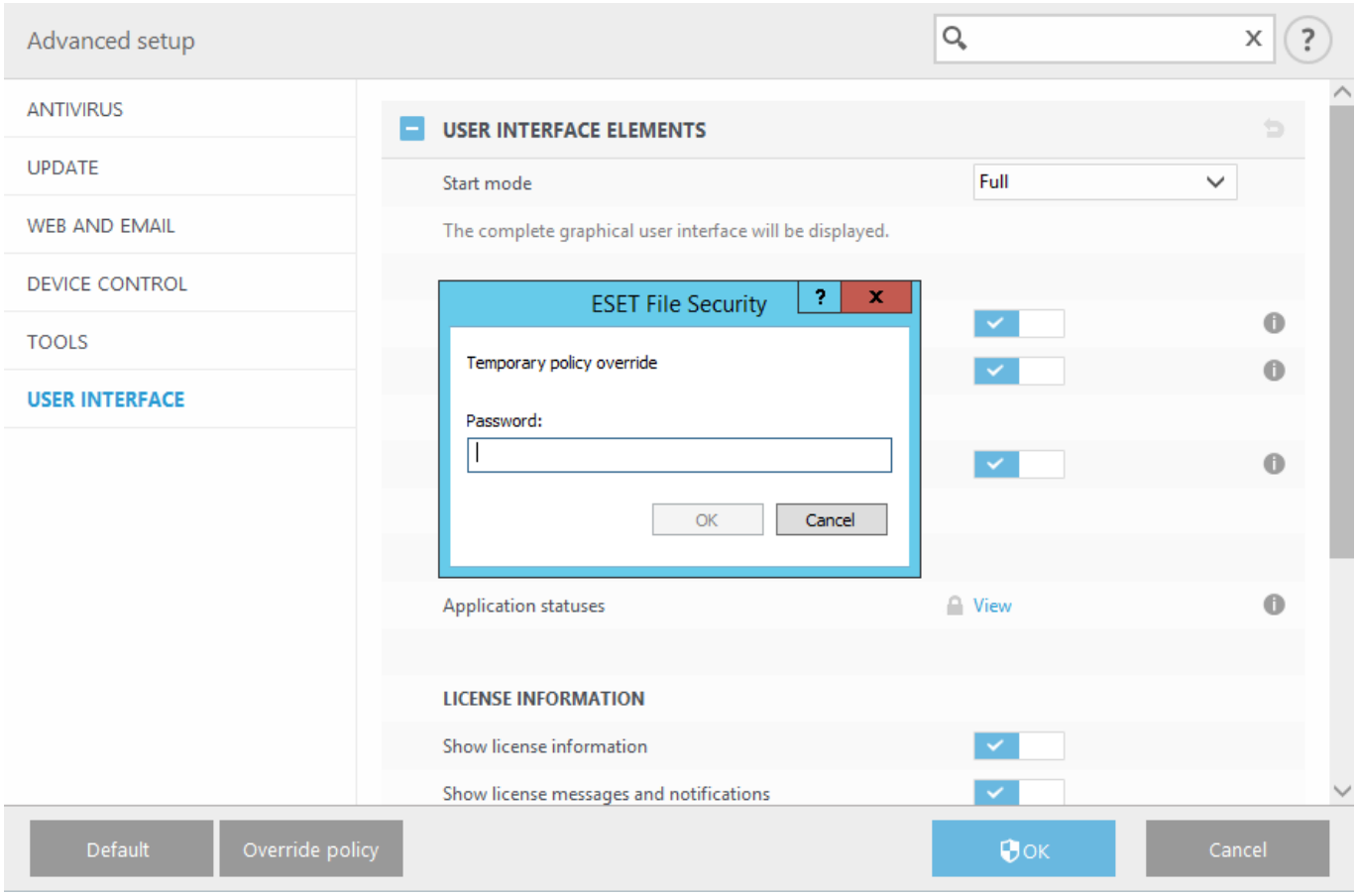
一旦修改原則，或新原則已套用至 ESET File Security，[覆寫原則］按鈕將會顯示在［進階設定］視窗中。



按一下 **［覆寫原則］**按鈕，設定持續時間並按一下 **［套用］**。



若您已選取［**密碼**］為驗證類型，請輸入原則來覆寫密碼。



一旦覆寫模式到期，您的任何配置變更將會還原至原始 ESET Security Management Center 原則設定。您會在覆寫到期前看到通知。

您可以在覆寫模式於監視頁面或在［**進階設定**］視窗中到期前，隨時**結束覆寫**模式。

防護記錄檔案

本區段可讓您修改 ESET File Security 記錄的設定。

防護記錄過濾器

因為預設會啟用所有記錄選項，所以會產生大量資料。我們建議您選擇性地停用不實用或是與問題無關的元件記錄。

> 注意
> 若要實際啟動記錄，您需要在主要功能表中的產品層級上打開一般**診斷記錄**，按［**設定**］>［工具］。一旦防護記錄本身開啟，ESET File Security 會根據在此區段啟用了什麼功能來收集詳細防護記錄。

使用切換來啟用或停用特定的功能。此選項也可以併用，取決於 ESET File Security 中各元件的可用性。

- ［**叢集診斷記錄**］– 叢集記錄會包含在一般診斷記錄中。

防護記錄檔案

定義管理防護記錄的方式。避免用完磁碟空間是非常重要的一件事。預設設定會允許自動刪除較舊的防護記錄以節省硬碟空間。

自動刪除超過指定（天數）的記錄

將刪除超過指定天數的防護記錄項目。

如果防護記錄大小超過，則自動刪除舊記錄

防護記錄檔案大小超過［**防護記錄大小上限 [MB]**］時，將刪除舊的防護記錄，直到達到［**減少後的防護記錄大小 [MB]**］為止。

備份自動刪除的記錄

將自動刪除的防護記錄與檔案備份到指定的目錄，並可選擇性壓縮成 ZIP 檔。

備份診斷防護記錄

將備份自動刪除的診斷防護記錄。未啟用則不會備份診斷防護記錄。

備份資料夾

將儲存防護記錄備份的資料夾。您可以啟用［使用 ZIP 壓縮防護記錄備份］。

自動最佳化防護記錄檔案

啟用時，如果重組百分比高於［**如果未使用的記錄數目超過（%）**］欄位中指定的數值，便會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。將會移除所有空白的防護記錄項目以提升效能及防護記錄處理速度。如果防護記錄包含大量的項目，則可明顯察覺此提升效果。

啟用文字通訊協定

啟用除了防護記錄檔案以外，還可用其他檔案格式來儲存防護記錄檔案：

- **[目標目錄]** – 防護記錄檔案所儲存的目錄（僅適用於 **Text/CSV**）。每個防護記錄區段皆具備已預先定義檔案名稱的檔案（例如，若您使用純文字檔案格式以儲存防護記錄，則 *virlog.txt* 適用於防護記錄檔案的［偵測到威脅］區段）。
- **[類型]** – 若您選擇 **[文字]** 檔案格式，則防護記錄將以文字檔格式儲存；而資料將以索引標籤分隔。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]** – 會消除所有目前在 **[類型]** 下拉式功能表中所選取的已儲存防護記錄。

> 注意
> 為了協助您更快速解決問題，ESET 技術支援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，請參閱我們的資料庫文章

Proxy 伺服器

在大型 LAN 網路中，Proxy 伺服器可用來調節電腦與網際網路的連線。如果是這種情況，則需要定義下列設定。如果您並未定義設定，程式將無法自動進行更新。在 ESET File Security 中，Proxy 伺服器設定位於 **[進階設定]** 視窗（**F5**）的兩個不同區段中。

1. **[進階設定] (F5) > [更新] > [設定檔] > [更新] > [連線選項] > [HTTP Proxy]**
   此設定適用於指定更新設定檔，且建議用於通常會從不同位置接收模組的筆記型電腦。

2. **[進階設定] (F5) > [工具] > [Proxy 伺服器]**
   在這個層級指定 Proxy 伺服器，會定義所有 ESET File Security 的全域 Proxy 伺服器設定。連線到網際網路的所有模組，都會使用這裡的參數。

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

Proxy 伺服器需要驗證

如果透過 Proxy 伺服器進行的網路通訊需要驗證，請啟用此選項並指定 **[使用者名稱]** 及 **[密碼]**。

偵測 Proxy 伺服器

按一下 **[偵測]**，以自動偵測和填入 Proxy 伺服器設定。將複製 Internet Explorer 中指定的參數。

> 注意
> 此功能不會擷取驗證資料（使用者名稱及密碼），且必須由您提供。

如果 proxy 無法使用，請使用直接連線

如果產品已配置為使用 HTTP Proxy，且 Proxy 無法存取，產品將避開 Proxy 並與 ESET 伺服器直接通訊。

通知

桌面及球形提示上的通知僅提供資訊，不需要使用者介入。它們會顯示在畫面右下角的通知區域中。可在以下修改更多詳細選項，如通知顯示時間及視窗透明度。開啟［**以全螢幕模式執行應用程式時不顯示通知**］以強制不顯示所有非互動通知。

顯示成功更新的相關通知

更新成功時，系統將顯示快顯通知。

利用電子郵件傳送事件通知

可啟用電子郵件通知。

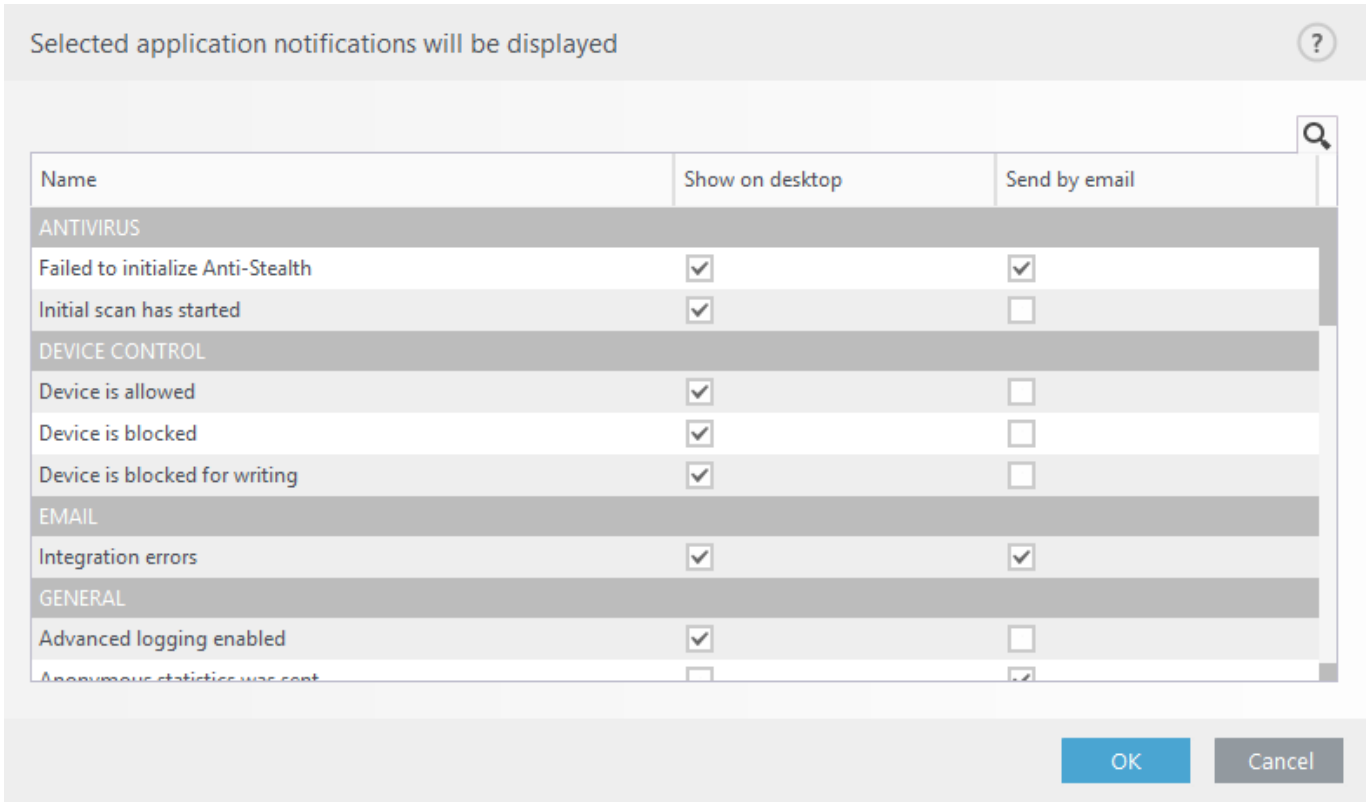
應用程式通知

按一下［編輯］以啟用或停用顯示應用程式通知。

應用程式通知

您可以將 ESET File Security 通知配置為在桌面上顯示及/或透過電子郵件傳送。

> 注意
> 如需電子郵件通知，請務必啟用［**基本**］區段中的［**利用電子郵件傳送事件通知**］，然後配置 SMTP 伺服器並視需要提供其他詳細資料。



桌面通知

您可以配置 ESET File Security 如何處理警示及系統通知威脅警告與系統通知（例如，成功更新訊息）。您也可以設定顯示時間**期間**及系統匣通知的**透明度**（這僅適用於支援系統匣通知的系統）。

[最簡化要顯示的事件] 下拉式功能表中，可讓您選取警示及通知嚴重性層級。可用選項如下：

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

[在多個使用者的系統中，在此使用者的畫面中顯示通知] 欄位可針對允許多位使用者同時連接的系統，指定要接收系統通知與其他通知的使用者。通常為系統或網路的管理員。如果將所有系統通知都傳送給管理員，則此選項特別適用於終端機伺服器。

電子郵件通知

如果發生與所選簡化層級相關的事件，則 ESET File Security 可以自動傳送電子郵件通知。

> 注意
> ESET File Security 支援具備 TLS 加密功能的 SMTP 伺服器。

SMTP 伺服器

用於傳送警告和通知的 SMTP 伺服器名稱。通常即是您的 Microsoft Exchange Server 名稱。

使用者名稱和密碼

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

輸入將在通知電子郵件檔頭顯示的寄件者地址。收件者會在 **[寄件者]** 欄位中看見這些資訊。

收件者地址

指定收件者的電子郵件地址**收件者**，通知將會傳遞給該收件者。

啟用 TLS

啟用 TLS 加密支援的警告及通知訊息。

電子郵件設定

通知最簡化

指定要傳送通知的最小冗贅層級。

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）。如果您要立即傳送這些通知，請將該值設為 0。

以不同的電子郵件傳送每個通知

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

訊息格式

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 messenger 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。另請參閱編輯格式。

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

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

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

字元集

您可以從下拉式功能表選擇編碼。電子郵件訊息會根據選取的字元編碼進行轉換。

使用可列印字元引用編碼

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

自訂

此郵件將顯示在所有選取通知的頁尾。

預設的通知訊息

通知頁尾中將顯示的預設訊息。

威脅

不自動關閉惡意軟體通知

可讓惡意軟體通知停留在畫面上，直到您手動關閉為止。

使用預設郵件

您可以關閉預設訊息並指定自訂的［**威脅通知訊息**］，該訊息會在封鎖威脅時顯示。

威脅通知郵件

輸入在威脅封鎖時顯示的自訂郵件。

簡報模式

如果使用者希望軟體使用不會中斷、不想受到快顯視窗打擾，而且想要將 CPU 用量減到最少，簡報模式是為這些使用者設計的功能。簡報模式也可在簡報期間使用，在此期間不會受到 ESET File Security 的活動干擾。啟用此功能時，將會停用所有快顯視窗，也不會執行已排程的工作。然而，系統保護功能仍會在背景執行，不需要和使用者互動。

以全螢幕模式執行應用程式時自動啟用簡報模式

當您執行全螢幕應用程式時，便會自動啟動簡報模式。使用簡報模式時，您就無法查看通知或 ESET File Security 的狀態變更

自動停用簡報模式於

若要定義一段時間（分鐘），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 File Security 問題。

按一下［**傾印類型**］旁的下拉式功能表，並從三個可用選項中選取一個：

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

目標目錄

在當機期間產生傾印的目錄。

開啟診斷資料夾

按一下［**開啟**］，在新的［*Windows* 檔案總管］視窗內開啟此目錄。

建立診斷傾印

按一下［**建立**］，在目標目錄中建立診斷傾印檔案。

進階記錄

啟用裝置控制進階記錄

記錄所有發生於裝置控制中的事件，可診斷和解決問題。

啟用核心進階記錄

記錄所有發生於 ESET 核心服務（ekrn）中的事件，可允許您診斷和解決問題。

啟用授權進階記錄

記錄與授權伺服器通訊的所有產品。

啟用網路防護進階記錄

記錄所有以 PCAP 格式通過網路防護的網路資料。這可以協助開發人員診斷和修正與個人網路防護相關的問題。

啟用作業系統進階記錄

系統將收集作業系統的其他相關資訊，例如執行中的處理程序□CPU 活動、磁碟作業。

啟用通訊協定過濾進階記錄

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

啟用更新引擎進階記錄

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。

技術支援

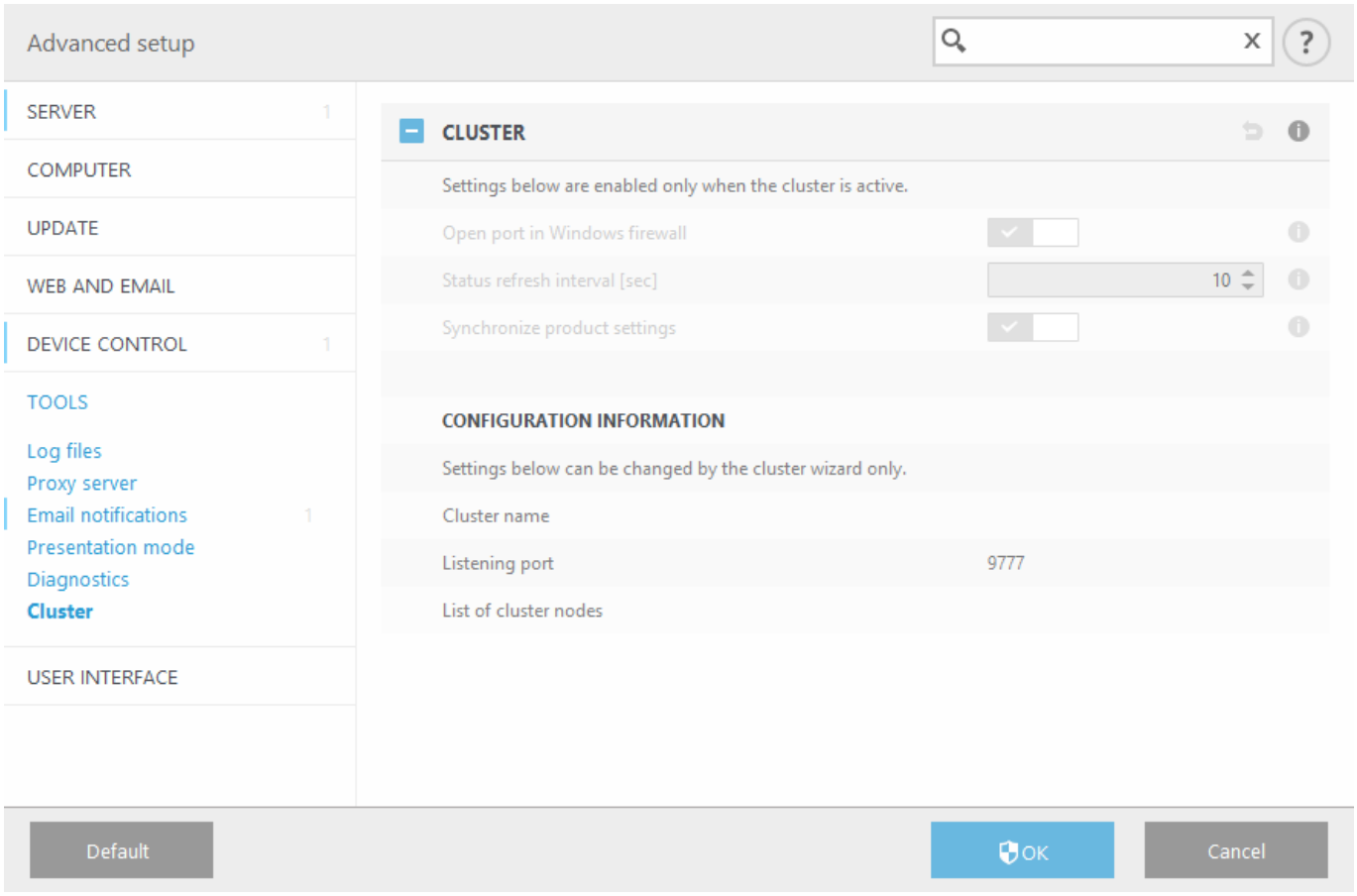
提交系統配置資料

選取［**一律提交**］即不會在向客戶服務提交 ESET File Security 配置資料之前收到提示，或是使用［**提交之前詢問**］□

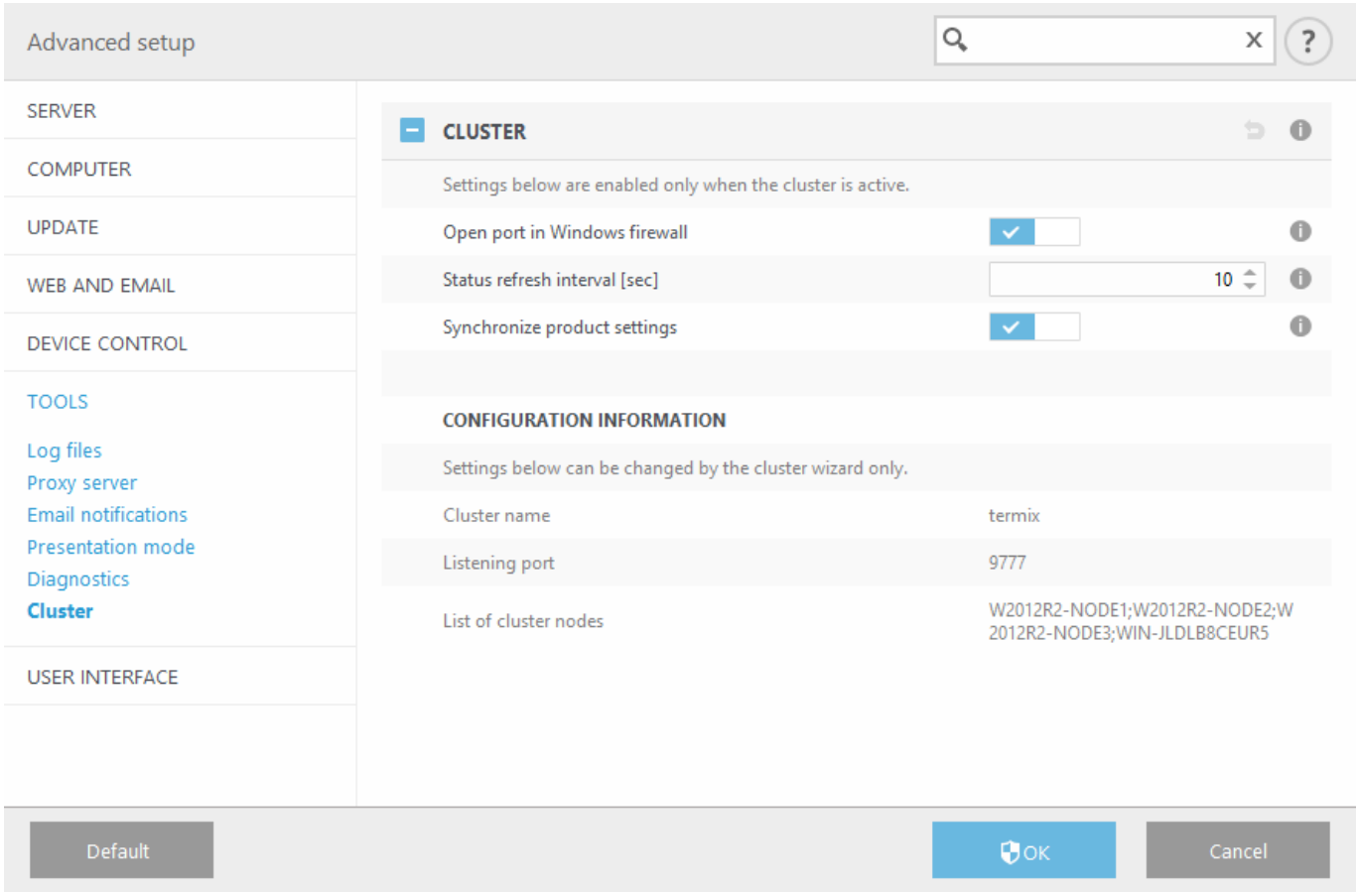
叢集

配置□ESET 叢集」後會自動啟用［啟用叢集］。您可以在［**進階設定**］(**F5**）視窗中按一下切換圖示來手動停用叢集（例如，您需要變更配置時使用，且不會影響其他□ESET 叢集」中的節點）。此選項僅會啟用或停用□ESET 叢集」功能。若要正常設定或銷毀叢集，請使用叢集精靈或位於主要程式視窗中［**工具**］>［**叢集**］區段的［**銷毀**］叢集。

□ESET 叢集」未配置且已停用：



使用「ESET 叢集」的詳情和選項進行正確配置：



使用者介面

配置 ESET File Security 的圖形使用者介面 (GUI) 行為。您可以調整程式的視覺外觀與使用的特效。

使用者介面元素

使用 [GUI 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)。
- **終端機** – 不會顯示任何通知或警告。GUI 只能由管理員啟動。如果圖形元素會減慢電腦執行的效能或導致其他問題，則使用者介面應該要設定成 [終端機]。您可能也想要關閉終端機伺服器的 GUI。如需有關安裝於終端機伺服器上之 ESET File Security 的詳細資訊，請參閱停用終端機伺服器的 GUI 主題。

啟動時顯示開機歡迎畫面

如果您不想在 ESET File Security 的 GUI 開始時（例如，登入系統時）顯示啟動畫面，則停用此選項。

使用聲音信號提示

ESET File Security 在掃描期間發生重大事件（例如當發現威脅或掃描結束）時播放音效。

整合至內容功能表

啟用時，ESET File Security 控制元素會整合至內容功能表。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。

應用程式狀態

按一下 [編輯] 以選取顯示在 [監控] 視窗中的狀態。或者，可以使用 ESET Security Management Center 原則以配置您的應用程式狀態。如果您的產品並未啟動或是授權已到期，也會顯示應用程式狀態。

授權資訊/顯示授權資訊

啟用時會顯示關於授權的訊息和通知。

警告及訊息方塊

配置 [警告及通知] 就可以變更已偵測到的威脅警告及系統通知的行為。這些全都可以自訂，以符合您的需求。如果您選擇不顯示某些通知，則這些通知就會顯示於停用訊息和狀態區域中。您可以在此檢查其狀態、顯示更多詳情，或是從這個視窗中加以移除。

存取設定

您可以使用 [存取設定] 工具確保安全性維持高設定，藉以防止任何未經授權的變更。

ESET Shell

您可以變更 ESET Shell 執行原則以配置透過 eShell 存取產品設定、功能與資料的存取權。

系統匣圖示

還原此區段中的所有設定

警告及訊息方塊

您可以配置 ESET File Security 如何處理警示及系統通知威脅警告與系統通知（例如，成功更新訊息）。您也可以設定顯示時間**期間**及系統匣通知的**透明度**（這僅適用於支援系統匣通知的系統）。

顯示互動警告

如果您想要防止 ESET File Security 在 Windows 通知區域中顯示警示，請停用此功能。

互動警告清單

對自動化非常有用。針對您想要自動執行的項目，取消選取**［詢問使用者］**，然後選取要採取的操作，而不是要等待互動的警示視窗。

「提示訊息」可用來顯示簡短的文字訊息或問題。

自動關閉訊息方塊

在某段時間內自動關閉快顯視窗，如果不手動關閉這些視窗，則經過指定時間後將自動關閉警告視窗。

確認訊息

按一下**［編輯］**時，快顯示窗會開啟且出現 ESET File Security 顯示的確認訊息清單，之後才會執行動作。使用核取方塊以自訂確認訊息的偏好設定。

存取設定

為了充分保護系統的安全性，務必正確設定 ESET File Security任何不合格的修改都可能造成問題，甚至遺失重要資料。若要避免不合格的修改，您可以使用密碼保護 ESET File Security 配置。

> 重要
> 如果您在使用存取設定密碼防護時解除安裝 ESET File Security系統會提示您輸入密碼。否則您就無法解除安裝 ESET File Security

密碼保護設定

鎖定/解除鎖定程式的設定參數。按一下以開啟**［密碼設定］**視窗。

設定密碼

若要設定或變更密碼以防護設定參數，按一下**［設定］**。若要保護 ESET File Security 的設定參數以避免未獲授權的修改，您需要設定新的密碼。當您想要變更現有的密碼時，請在**［舊密碼］**欄位中輸入您的舊密碼，並在**［新密碼］**和**［確認密碼］**欄位中輸入您的新密碼，然後按一下**［確定］**。日後對 ESET File Security 進行任何修改，都將會需要這個密碼。

受限管理員帳號需要完整的管理員權限

選取此選項以在修改特定參數時，提示現有使用者（如果沒有管理員權限的話）輸入管理員帳戶憑證（例如，停用防護模組）。

注意
如果進階設定密碼已變更，而您想使用 ESET CMD 命令列匯入現有的 *xml* 配置檔案（已在密碼變更前簽署），請確保使用目前的密碼再次簽署。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 File Security 的電腦。

ESET Shell

您可以變更 **[ESET Shell 執行原則]** 以配置透過 eShell 存取產品設定、功能與資料的存取權。預設設定為 **[限制的腳本]**，但您可以視需要將其變更為 [已停用]、[唯讀] 或 [完整存取權限]。

已停用

完全無法使用 eShell只允許 eShell 本身的配置 – 在 `ui eshell` 內容中。您可以自訂 eShell 的外觀，但無法存取產品設定或資料。

唯讀

eShell 可作為監控工具。您可以在互動與批次模式中檢視所有的設定，但您無法修改任何設定、功能或修改任何資料。

限制的腳本

在互動模式中，您可以檢視與修改所有的設定、功能與資料。在批次模式中eShell 的運作方式會與您處於唯讀模式時相同，但如果您使用已簽署的批次檔案，則可以編輯設定和修改資料。

完整存取權限

在互動與批次模式中無限制地存取所有設定（在執行批次檔案時）。您可以檢視與修改任何設定。您必須使用管理員帳戶才能以完整存取權限執行 eShell如果已啟用 UAC也需要提高權限。

停用終端機伺服器的 GUI

本章說明如何針對使用者工作階段期間在 Windows 終端機伺服器上執行的 ESET File Security 停用其 GUI

一般而言，遠端使用者登入伺服器並建立終端機工作階段時ESET File Security GUI 都會啟動。這對於終端機伺服器通常是不必要的。如果您想要關閉終端機工作階段的 GUI則可以執行 `set ui ui gui-start-mode none` 命令，透過 eShell 達成此目的。這會讓 GUI 處於終端機模式。下列為兩個可用的 GUI 啟動模式：

```
set ui ui gui-start-mode full
set ui ui gui-start-mode none
```

如果您想要瞭解目前使用的是哪個模式，請執行 `get ui ui gui-start-mode` 命令。

注意
如果您已在 Citrix 伺服器上安裝 ESET File Security我們建議您使用知識庫文章中所述的設定。

已停用訊息和狀態

確認訊息

向您顯示確認訊息的清單，並可讓您選取是否要顯示。

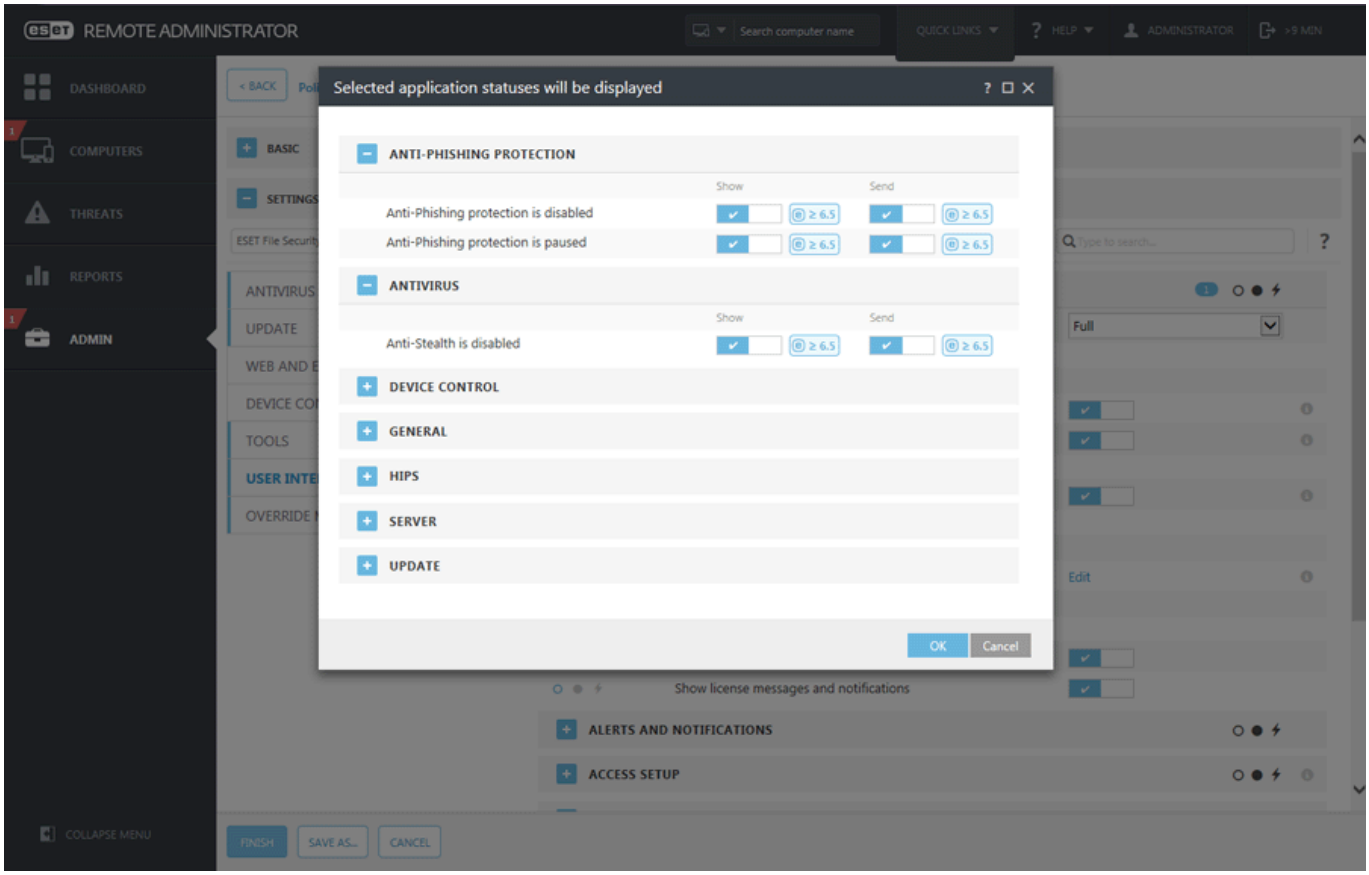
應用程式狀態設定

允許您在主要功能表的［監視］頁面中啟用或停用顯示狀態。

應用程式狀態設定

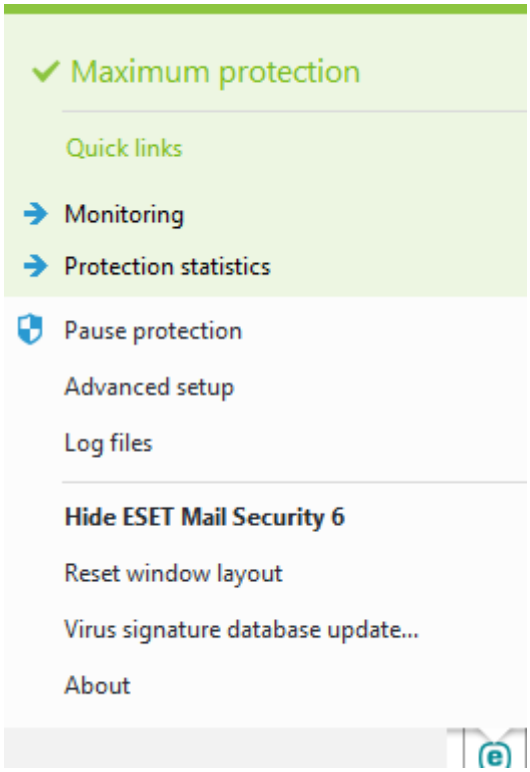
在這個對話方塊中，可讓您選取或取消選取顯示或不顯示應用程式狀態。例如，當您暫停病毒及間諜程式防護時，這將會造成防護狀態變更，並顯示在監視頁面中。若您的產品未啟用或授權已過期，系統也會顯示應用程式狀態。

應用程式狀態可以透過 ESET Security Management Center 原則來管理。類別和狀態會顯示在擁有兩個選項［**顯示**］和［**傳送**］狀態的清單。傳送應用程式狀態的欄位僅會在 ESET Security Management Center 原則配置中顯示ESET File Security 會顯示鎖定圖示的設定。您可以使用覆寫模式以暫時變更應用程式狀態。



系統匣圖示

可快速存取 ESET File Security 的常用項目和功能。以滑鼠右鍵按一下系統匣圖示 來使用這些項目和功能。



更多資訊

開啟監視頁面以顯示目前的防護狀態及訊息。

暫停防護

顯示會停用防毒及間諜程式防護的確認對話方塊，其會藉由控制檔案、Web 及電子郵件通訊來抵禦攻擊。當您暫停「病毒及間諜程式防護」時，就會出現系統匣圖示 和 **[暫停防護]** 對話方塊。這將會在選取的時段內停用惡意軟體相關防護（若要永久停用防護，您必須使用 **[進階設定]**）。請小心，停用防護會將您的系統暴露於威脅中。

[進階設定]

使用此選項以輸入 **[進階設定]**。

防護記錄檔案

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

隱藏 ESET File Security

隱藏螢幕上的 ESET File Security 視窗。

重設視窗配置

將 ESET File Security 的視窗重設為螢幕上的預設大小及位置。

檢查更新

啟動更新模組以確保您對抗惡意程式碼的防護層級。

關於

提供系統資訊ESET File Security 已安裝版本的詳情，以及已安裝的程式模組和您的授權到期日期。您可以在頁面底部找到作業系統和系統資源的相關資訊。

還原為預設值

您可以在［**進階設定**］中將設定還原為其預設值。有兩個選項。您可以將所有內容還原為預設值，或是僅針對特定區段還原設定（其他區段中的設定會維持不變）。

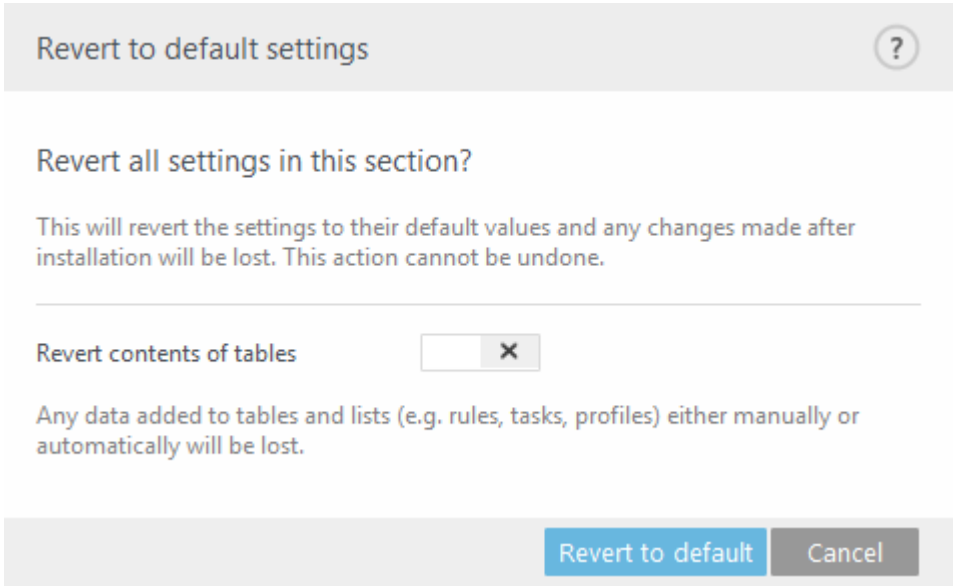
要還原所有設定嗎

進階設定之所有區段中的所有設定，都會還原至您安裝 ESET File Security 之後的狀態。您可以將之視為還原原廠預設值

> 注意
> 按一下［**還原為預設值**］之後，所有完成的變更都會遺失。此動作無法恢復。

還原此區段中的所有設定

將所選區段中的模組設定還原為數值。您在此區段完成的任何變更都會遺失。



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。

說明及支援

ESET File Security 包含疑難排解工具及支援資訊，可幫助您解決可能遇到的問題。

說明

搜尋 ESET 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，使其成為解決各種類型問題的最強工具。

開啟說明

啟動 ESET File Security 的線上說明頁面。

尋找快速解決方案

選取此選項，以尋找常見問題的解決方案。建議您在連絡技術支援之前，先閱讀此部分。

技術支援

提交支援要求

若您找不到問題的解答，您也可以使用這份位於 ESET 網站上的表單來快速連絡我們的「技術支援」部門。

技術支援詳細資訊

顯示技術支援的詳細資訊（產品名稱、產品版本等）。

支援工具

威脅百科全書

ESET 威脅百科全書的連結，其中包含有關危險以及不同入侵類型徵兆的相關資訊。

ESET Log Collector

連至 ESET Log Collector 下載頁面 的連結。Log Collector 是可自動收集伺服器配置和防護記錄等資訊的應用程式，能協助您快速解決問題。

偵側引擎歷程

可連結至 ESET 病毒雷達，其中包含 ESET 偵測模組版本的相關資訊。

ESET Specialized Cleaner

ESET 專用清除程式是一般惡意軟體感染（例如 Conficker、Sirefef 或 Necurs）的移除工具。

產品和授權資訊

啟動產品 / 變更授權

按一下以啟動［產品啟動］視窗。選取其中一種可用方法來啟動 ESET File Security。

關於 ESET File Security

顯示 ESET File Security 副本的相關資訊。

提交支援要求

為要盡可能快速準確的提供協助，ESET 需要 ESET File Security 配置相關的資訊、系統、執行中處理程序的詳細資訊（ESET SysInspector 防護記錄檔案）和登錄資料。ESET 只會將此資料用於提供客戶技術協助。也可以從 **［進階設定］(F5) > ［工具］> ［診斷］> ［技術支援］** 配置此設定。

注意
如果您選擇要提交系統資料，您必須填寫並提交 Web 表單，否則不會建立您的票證，而且您的系統資料會遺失。

提交 Web 表單時，您的系統配置資料會傳送至 ESET。如果要記住此處理程序的此處理方法，請選取 **[永遠提交此資訊]**。

請勿提交資料

如果您不想要提交檔案，請使用此選項。系統會將您重新導向至 ESET 技術支援網頁。

關於 ESET File Security

此視窗會提供已安裝的 ESET File Security 版本。視窗頂端則包含作業系統及系統資源的相關資訊、目前使用者和完整電腦名稱。

已安裝的元件

包含模組資訊，以檢視已安裝元件的清單和其詳細資料。按一下 **[複製]** 以複製清單至您的剪貼簿。當您進行疑難排解和連絡「技術支援」部門時，這樣做很有助益。

字彙

請造訪字彙 頁面以取得更多有關技術詞彙、威脅與網際網路安全性的資訊。

使用者授權合約

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**隱私權政策。

使用者授權合約

本使用者授權合約（以下稱「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）（以下稱ESET或「提供者」）與貴用戶、個人或法人（以下稱「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。若貴用戶不同意本「合約」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」或您購買本「軟體」之經銷商。

貴用戶同意使用本「軟體」即表示貴用戶已閱讀本「合約」、理解「合約」內容，並受「合約」條款與條件的約束。

1.**軟體。**本「合約」中的「軟體」一詞係指(i) 本「合約」所隨附之電腦程式及其包含的所有元件(ii) 在磁碟CD-ROMDVD電子郵件及所有附件，或其他隨附本「合約」之媒體中的所有內容，包括以資料傳送體提供、透過電子郵件傳送或透過網際網路下載的本「軟體」物件碼; (iii) 任何相關書面說明資料以及與本「軟體」相關的任何其他可能文件，尤其是本「軟體」任何說明、其規格、本「軟體」屬性或作業的任何說明、使用本「軟體」之作業環境的任何說明、本「軟體」的使用安裝指示，或如何使用軟體的任何說明(以下稱「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，並遵循所有規定的條款與條件，則「提供者」會授與貴用戶以下權限（以下稱「授權」）：

a) **安裝與使用。**貴用戶擁有非專屬、不可轉讓之權限，可將本「軟體」安裝於電腦硬碟或其他儲存資料的永久媒體上、將本「軟體」安裝並儲存於電腦系統的記憶體上，以及實作、儲存及顯示本「軟體」。

b) **授權數目規定。**本「軟體」的使用權限受「使用者」數目的限制。「一位使用者」係指(i) 本「軟體」於一個電腦系統上的安裝；或 (ii) 若授權的範圍受信箱數目的限制，則「一位使用者」係指透過 Mail User Agent (MUA) 接收電子郵件的電腦使用者。若 MUA 接受電子郵件並於稍後將郵件自動散佈給多位使用者，則「使用者」數目即根據接收所散佈之電子郵件的實際使用者數目而定。若郵件伺服器執行郵件閘道功能，則「使用者」數目應等於由該閘道提供服務之郵件伺服器使用者數目。若將任何數量之電子郵件地址引導至一位使用者（例如透過別名），且該使用者接受這些地址，而且用戶端未自動將郵件散佈給大量的使用者，則需要一台電腦的「授權」。貴用戶不得同時在多台電腦上使用同一個「授權」。使用者僅在根據「提供者」授予的授權數目造成的限制下，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) **企業版。**若要在郵件伺服器、郵件中繼站、郵件閘道或網際網路閘道上使用本「軟體」，則必須取得本「軟體」的企業版。

d) **授權期限。**本「軟體」的使用權限有時間限制。

e) **OEM 軟體。**OEM 軟體」受限於您取得該軟體的電腦OEM 軟體」無法傳輸到其他電腦。

f) **NFRTRIAL 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」更新程式（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」。針對佈建更新的目的，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。

b) **將入侵及資訊轉遞給「提供者」。**本「軟體」包含會收集電腦病毒與其他惡意電腦程式及可疑、問題、潛在不需要或潛在不安全的物件（例如檔案□URL□IP 封包及乙太網路框架（以下統稱「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/或平台的資訊和/或有關本「軟體」運作和功能的資訊，以及本機網路上裝置如類型、廠商、型號和/或裝置名稱的相關資訊（以下統稱「資訊」）。「資訊」和「入侵」可能包含有關使用者或本「軟體」安裝所在之電腦使用者的資料，包括隨機或或意外取得的個人資料 ，以及因相關聯中繼資料入侵而受影響的檔案。

「資訊」與「入侵」可由下列「軟體」功能收集：

i.LiveGrid 聲譽系統功能包括收集和傳送「入侵」相關的單向雜湊給「提供者」。此功能將在本「軟體」標準設定下啟用。

ii.LiveGrid 意見系統功能包括收集和傳送「入侵」連同關聯的中繼資料，以及「資訊」給「提供者」。此功能可由「使用者」在安裝本「軟體」期間啟動。

「提供者」僅應將收到的「資訊」與「入侵」供分析研究「入侵」、改進「軟體」與驗證「授權」真確性之用，並採取適當的措施確保「入侵」及「資訊」保持機密。貴用戶啟用本「軟體」的這項功能，表示貴用戶准許「提供者」依照隱私權政策與相關法律規定收集和處理「入侵」與「資訊」。貴用戶可隨時停用此功能。

針對本「合約」之目的，有必要收集、處理和儲存資料，使「提供者」能夠根據隱私權政策識別您的身份。貴用戶瞭解，「提供者」會使用自己的方式檢查您是否按照本協議的規定使用本「軟體」。貴用戶瞭解，針對本「合約」之目的，您的資料必須在本「軟體」與「提供者」或其商業夥伴（作為「提供者」經銷和支援網路一部分）的電腦系統之間進行通訊時傳送，以確保本「軟體」功能和使用本「軟體」的授權，以保護「提供者」的權利。

依據本「合約」結論，「提供者」或其任何作為「提供者」經銷和支援網路一部分的商業夥伴，有權利傳輸、處理與儲存可識別貴用戶的必要資料，以供計費、實行本「合約」之用，並在電腦上傳輸通知。貴用戶同意接收產品相關通知與訊息，包括但不限於行銷資訊。

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」。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。提供技術支援前，需要「使用者」先備份所有現有資料、軟體與程式設備。對於因提供技術支援所導致任何資料、財產、軟體或硬體的損壞或遺失，或利潤的損失：ESET 及/或 ESET 委任的第三方概不負責：ESET 及/或 ESET 委任的第三方保留決定解決問題是否超過技術支援範圍的權利：ESET 保留酌情拒絕、暫停或終止提供技術支援的權

利。依照隱私權政策，可能需要授權資訊、「資訊」和其他資料，以便用於技術支援佈建。

16.**授權轉讓**。本「軟體」可在電腦系統間傳輸，除非違反本「合約」條款。本「軟體」可在電腦系統間傳輸，除非違反本「合約」條款。如果未違反本「合約」條款，「使用者」是唯一具有權利的實體可在「提供者」同意下，將因本「合約」產生的「授權」與所有權利永久轉讓給另一位「使用者」，但轉讓條件為：(i) 原始「使用者」未保留本「軟體」的任何副本；(ii) 權利的轉讓必須是直接，亦即從原始「使用者」轉讓給新「使用者」；(iii) 新「使用者」必須承擔原始「使用者」依本「合約」條款所承擔的所有權利與義務；(iv) 依照第 17 條規定，原始「使用者」必須提供給新「使用者」可驗證本「軟體」真實性的文件。

17.**驗證軟體真實性。**「使用者」可使用下列其中一種方式證明使用本「軟體」的資格：(i)透過「提供者」或「提供者」所委任第三方核發的授權憑證；(ii) 透過書面授權合約（若已訂立此類合約)；(iii) 透過提交「提供者」傳送的電子郵件，其中包含授權詳細資料（使用者名稱與密碼)。依照隱私權政策，可能需要授權資訊和使用者識別資料，以便用於本「軟體」真實性驗證。

18.**美國公家機關與政府單位的授權**。根據本「合約」所述的授權權利與限制，本「軟體」可提供給公家機關，包括美國政府

19.**貿易管制法規遵循**：

a)您將不得直接或間接以出口、再出口、移轉或其他方式將本軟體提供給任何人，或以任何方式進行使用，或涉及任何可能導致 ESET 或其所有公司、其附屬機構、任何其所有公司的附屬機構，以及其所有公司所掌控之實體（下稱「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（下稱「出口管制法律」）；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（下稱「制裁法律」）。

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.

21.**準據法**。本「合約」由斯洛伐克共和國法律管理與解釋。「使用者」及「提供者」同意準據法與《聯合國際商品買賣契約公約》相抵觸的條款將不適用。貴用戶明確同意任何因本「合約」所導致與「提供者」相關的糾紛與索賠，或任何與使用本「軟體」相關的糾紛與索賠，均由 Bratislava I District Court 調解，貴用戶亦明確同意該法院行使管轄權。

22.**一般條款**。若本「合約」有任何條款無效力或不能執行，均不影響「合約」其他條款的效力。根據本「合約」規定之條件，其他條款仍保有效力並可執行。若本協議的各個語言版本之間出現差異，則優先適用英文版本。本「合約」只能以書面形式進行修改，該書面應由「提供者」的授權代表或依委託書條款明確授權行使此能力之人士簽署。

本「合約」為貴用戶和「提供者」之間與本「軟體」相關的完整「合約」，取代之前與本「軟體」相關的任何聲明、討論、保證、通訊或廣告。

EULA ID: BUS-STANDARD-20-01

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 Cour (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單項目比較，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、潛在不需要或潛在不安全物件（例如，可執行檔、您回報為垃圾郵件或是由產品標記為垃圾郵件的電子郵件）此類入侵行為；
  - 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。

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