System Center

Endpoint Protection 適用於 Mac

安裝手冊與使用手冊

Microsoft

內容

System Center Endpoint Protection

由於 Unix 作業系統越來越普及，因此惡意軟體的作者不斷開發更多的威脅來攻擊 Mac 使用者。System Center Endpoint Protection 可提供強大而有效的防護措施來抵禦新出現的威脅。System Center Endpoint Protection 含有使 Windows 威脅轉向的功能，可保護與 Windows 使用者互動的 Mac 使用者，反之亦然。雖然 Windows 使用者不會對 Mac 造成直接威脅，但停用已感染 Mac 電腦的惡意軟體會防止其透過區域網路或網際網路散播至 Windows 電腦。

系統需求

若要使 System Center Endpoint Protection 發揮最佳效能，您的系統應滿足下列硬體和軟體需求：

System Center Endpoint Protection:

	系統需求
處理器架構	32 位元、64 位元 Intel R
作業系統	Mac OS X 10.6 以及更新版本
記憶體	512 MB
可使用的磁碟空間	100 MB

安裝

開始安裝程序之前，請關閉電腦中所有開啟的程式。System Center Endpoint Protection 包含的元件可能與您電腦上已經安裝的其他防毒程式發生衝突。強烈建議移除其他任何防毒程式，以避免潛在的問題。您可以從安裝 CD/DVD 或從 ESET 網站下載的檔案安裝 System Center Endpoint Protection。

若要啟動安裝精靈，請執行下列任一個步驟：

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

啟動安裝程式而安裝精靈將引導您進行基本設定。同意「軟體授權合約」並閱讀「隱私權聲明」後，您可以選擇下列安裝類型：

- 一般 4
- 自訂 4

一般安裝

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

選取 **[一般]** 安裝模式後，請配置 **[潛在不需要應用程式偵測]**。潛在不需要應用程式不一定是惡意的，但是可能會經常對作業系統的行為造成負面影響。這些應用程式通常隨附於其他程式，且可能在安裝程序期間很難注意到。雖然這些應用程式通常會在安裝期間顯示通知，但亦可未經您的同意輕易安裝。

安裝 System Center Endpoint Protection 後，應該執行電腦掃描以偵測是否有惡意程式碼。從主要程式視窗中，按一下 **[電腦掃描]**，然後按一下 **[智慧型掃描]**。如需有關「指定」電腦掃描的更多資訊，請參閱指定電腦掃描 10一節。

自訂安裝

自訂安裝模式是針對想要在安裝程序期間修改進階設定的進階使用者設計。

選取 **[自訂]** 安裝模式後，系統會提示您配置 **[Proxy 伺服器]** 設定。如果您使用的是 Proxy 伺服器，則可以選取 **[我使用 Proxy 伺服器]** 選項來定義其參數。將 Proxy 伺服器的 IP 位址或 URL 輸入到 **[位址]** 欄位中。在連接埠欄位中，指定 Proxy 伺服器接受連線所在的連接埠 (依預設為 3128)。如果 Proxy 伺服器需要驗證，則必須輸入有效的 **[使用者名稱]** 及 **[密碼]**，授與 Proxy 伺服器的存取權限。如果您確定不使用任何 Proxy 伺服器，請選擇 **[我不使用 Proxy 伺服器]** 選項。如果您不確定，可以藉由選取 **[使用系統設定 (建議)]** 來使用目前的系統設定。

在下一步中，您可以 **[定義有權限的使用者]** 編輯程式配置。從左側的使用者清單中，選取使用者並將其 **[新增]** 到 **[有權限的使用者]** 清單中。若要顯示所有系統使用者，請選取 **[顯示所有使用者]** 選項。

安裝程序的下一步是配置 **[潛在不需要應用程式偵測]**。潛在不需要應用程式不一定是惡意的，但是可能會經常對作業系統的行為造成負面影響。這些應用程式通常隨附於其他程式，且可能在安裝程序期間很難注意到。雖然這些應用程式通常會在安裝期間顯示通知，但亦可未經您的同意輕易安裝。

安裝 System Center Endpoint Protection 後，應該執行電腦掃描以偵測是否有惡意程式碼。從主要程式視窗中，按一下 **[電腦掃描]**，然後按一下 **[智慧型掃描]**。如需有關「指定」電腦掃描的更多資訊，請參閱指定電腦掃描 10 一節。

解除安裝

如果您想要從電腦解除安裝 System Center Endpoint Protection，請執行下列任一個步驟：

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

初學者手冊

本章提供 System Center Endpoint Protection 及其基本設定的初始概觀。

使用者介面

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

以下為主要功能表中選項的說明：

- **防護狀態** - 提供與 System Center Endpoint Protection 的防護狀態有關的資訊。如果啟用 **[進階模式]**，則會顯示 **[統計]** 子功能表。
- **電腦掃描** - 此選項可讓您配置及啟動指定電腦掃描。
- **更新** - 顯示有關病毒資料庫更新的資訊。
- **設定** - 選取此選項以調整您電腦的安全等級。如果啟用 **[進階模式]**，則會顯示 **[病毒及間諜程式防護]** 子功能表。
- **工具** - 可存取 **[防護記錄檔案]**? **[隔離區]** 和 **[排程器]**。此選項僅在 **[進階模式]** 中顯示。
- **說明** - 提供程式資訊和存取說明檔案。

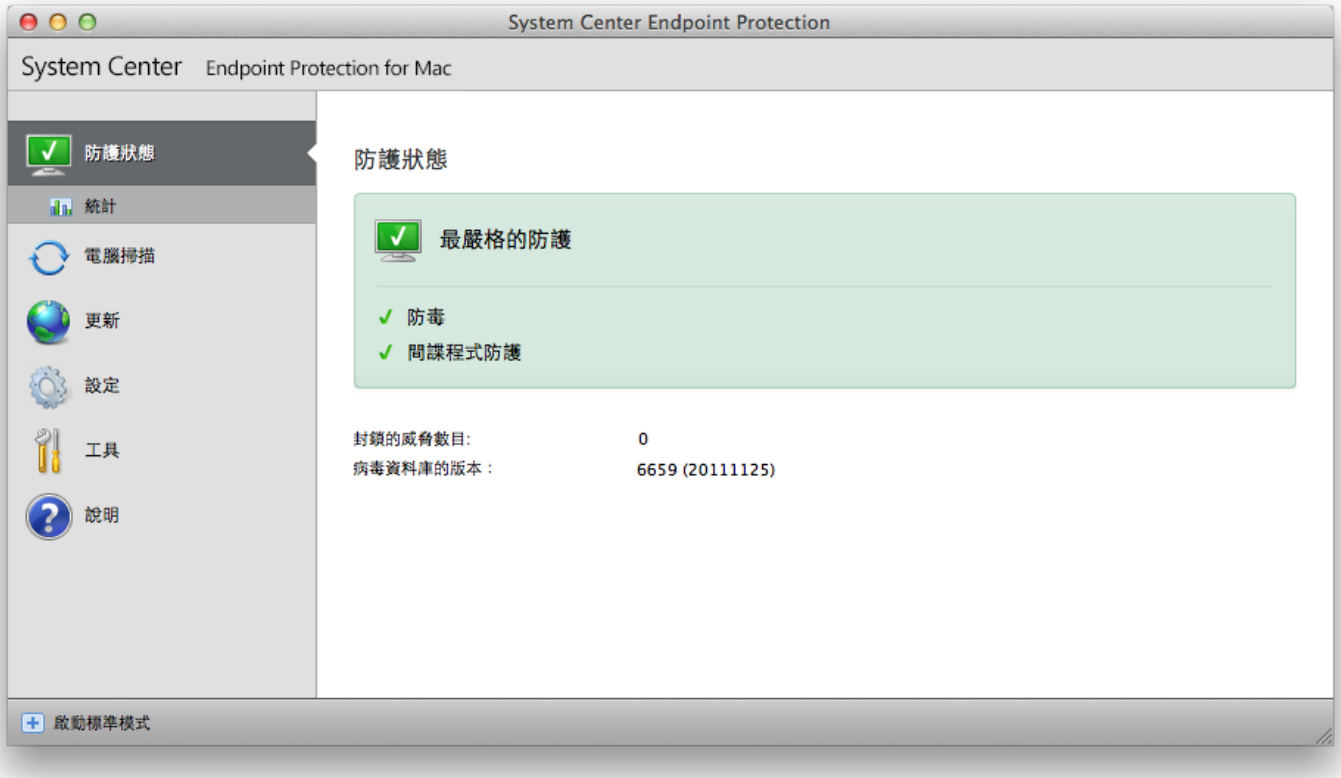
System Center Endpoint Protection 使用者介面可讓使用者切換「標準」和「進階」模式。標準模式可存取一般作業所需的功能。不顯示任何進階選項。若要切換模式，請按一下主要程式視窗左下角 **[啟動進階模式]**/**[啟動標準模式]** 旁的加號 (+) 圖示，或按下 cmd+M。

切換至進階模式會將 **[工具]** 選項新增至主要功能表。**[工具]** 選項可讓您存取 **[防護記錄檔案]**? **[隔離區]** 和 **[排程器]** 的子功能表。

附註： 本手冊中以下的所有說明，均針對 **[進階模式]**。

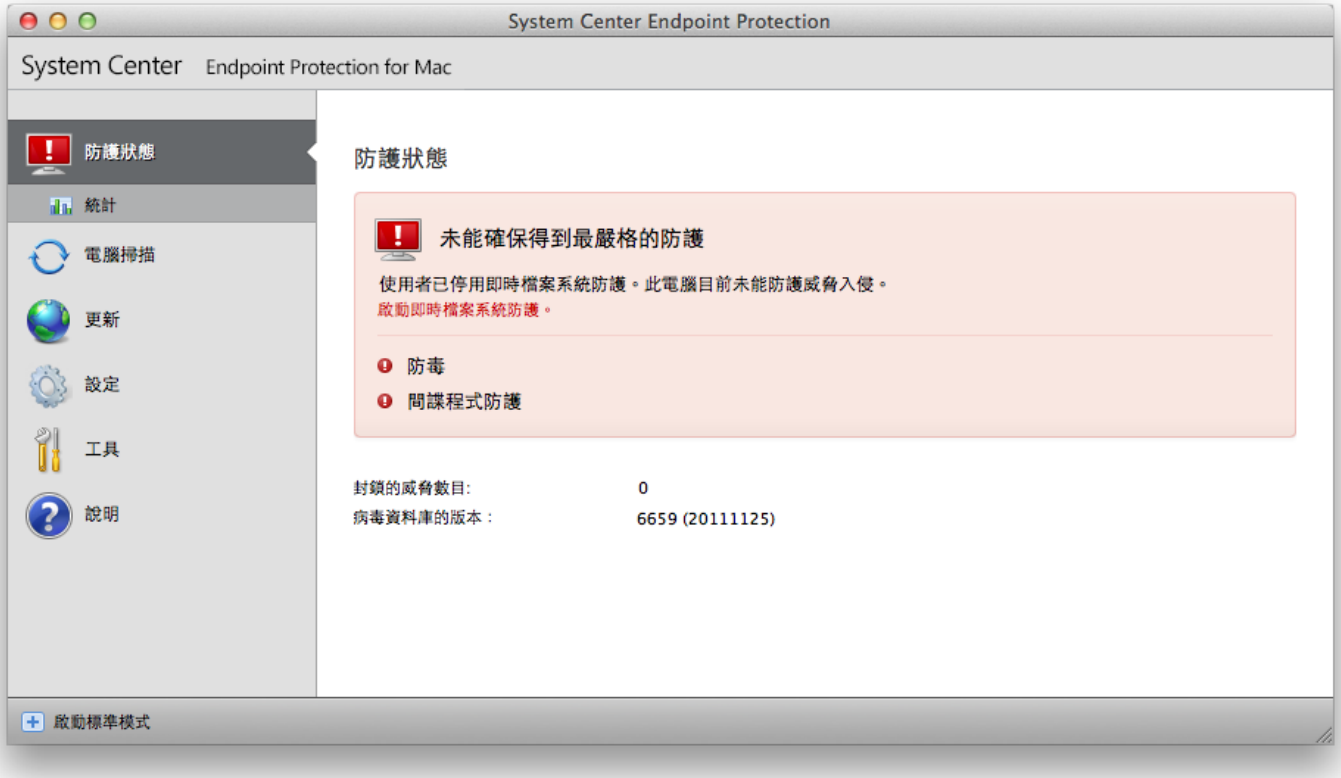
檢查系統的作業

若要檢視 **[防護狀態]**，請按一下主要功能表頂端的選項。System Center Endpoint Protection 相關作業的狀態摘要顯示在主要視窗及有 **[統計]** 的子功能表中。選取該選項以檢視更多與您的系統執行的電腦掃描有關的詳細資訊與統計。[統計] 視窗僅能在進階模式中使用。



如果程式運作不正常怎麼辦

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



使用 System Center Endpoint Protection

病毒及間諜程式防護

病毒防護透過修改造成潛在威脅的檔案來防止惡意系統攻擊。如果偵測到含有惡意程式碼的威脅，「防毒」模組可透過封鎖，接著清除、刪除或將其移至隔離區來消滅威脅。

即時檔案系統防護

即時檔案系統防護控制系統中與防毒相關的所有事件。開啟、建立或在電腦上執行所有檔案時，都會掃描這些檔案是否具有惡意程式碼。在系統啟動時會啟動即時檔案系統防護。

即時防護設定

即時檔案系統防護會檢查所有媒體類型，並且根據各種事件觸發掃描。針對新建立的檔案及現有檔案，即時檔案系統防護可能有所不同。若為新建立的檔案，則可套用較深入的控制層級。

依預設，即時防護會在系統啟動時同時啟動，並持續提供掃描。在特殊情況下 (如與其他即時掃描器發生衝突時)，可以按一下功能表列 (位於畫面頂端) 中的 System Center Endpoint Protection 圖示，然後再選取 **[停用即時檔案系統防護]** 選項，終止即時防護。您也可以從主要程式視窗終止即時防護 (**[設定]** > **[病毒及間諜程式防護]** > **[停用]**)。

若要修改即時防護的進階設定，請移至 **[設定]** > **[進入應用程式喜好設定...]**> **[防護]** > **[即時防護]**，然後按一下 **[進階選項]** 旁的 **[設定...]** 按鈕 (如標題為進階掃描選項 8 的章節所述)。

執行掃描的時間 (事件觸發的掃描)

依預設，在 **[檔案開啟]**? **[檔案建立]** 或 **[檔案執行]** 所有檔案時會執行掃描。我們建議您保留預設設定，因為這些預設值會為電腦提供最高等級的即時防護。

進階掃描選項

在此視窗中，您可以定義由掃描引擎掃描的物件類型，以及啟用/停用 **[進階探索法]** 與修改壓縮檔與檔案快取的設定。

我們不建議變更 **[預設壓縮檔設定]** 區段中的預設值，除非解決特定問題所需，因為更高的巢狀壓縮檔值會妨礙系統效能。

您可以按一下各個參數區段的 **[進階探索法]** 核取方塊，以分別對已執行的檔案、已建立的檔案和已修改的檔案切換進階探索法掃描。

若要在使用即時防護時佔用最低的系統使用量，您可以定義最佳快取的大小。當您使用 **[啟用未感染檔案快取]** 選項時，此行為正作用中。如果停用此功能，則每次存取所有檔案時，都會進行掃描。檔案快取後不會重複掃描檔案 (除非檔案被修改)，視定義的快取大小而定。每次更新病毒資料庫之後，會立即重新掃描檔案。

按一下 **[啟用未感染檔案快取]** 以啟用/停用此功能。只要在 **[快取大小]** 旁的輸入欄位中輸入所需值即可設定要快取的檔案數量。

在 **[引擎設定]** 視窗中可設定其他掃描參數。您可以定義應掃描的 **[物件]** 類型、使用的 **[選項]** 與 **[清除]** 層級，以及定義要即時檔案系統防護的 **[副檔名]** 與檔案大小 **[限制]**。您可以按一下 [進階設定] 視窗中的 **[引擎]** 旁的 **[設定...]** 按鈕進入 [引擎設定] 視窗。如需更多有關引擎參數的詳細資訊，請參閱引擎參數設定 12。

從掃描中排除

本區段可讓您從掃描中排除特定檔案及資料夾。

- **路徑** - 排除檔案及資料夾的路徑
- **威脅** - 如果排除檔案旁有威脅的名稱，則代表該檔案只是因為給定威脅而排除，但不是完全排除。因此，如果該檔案在稍後被其他惡意軟體感染，則防毒模組仍會偵測到該檔案。
- **新增...** - 從偵測中排除物件。輸入到物件的路徑 (您也可以使用萬用字元 * 和 ?) 或從樹狀結構中選取資料夾或檔案。
- **編輯...** - 可讓您編輯已選取的項目
- **刪除** - 移除已選取的項目
- **預設** - 取消所有排除。

何時修改即時防護配置

即時防護是維護系統安全的最重要組成部分。修改即時防護參數時請小心。建議您僅在特定情況中修改這些參數。例如，在與特定應用程式或另一個防毒程式的即時掃描器發生衝突的情況下。

System Center Endpoint Protection 的所有設定在安裝後即已最佳化，為使用者提供最高等級的系統安全。若要還原預設設定，請按一下位於 **[即時防護]** 視窗左下方的 **[預設]** 按鈕。請依下列方式存取 [即時防護] 視窗：**[設定]** > **[進入應用程式喜好設定...]** > **[防護]** > **[即時防護]**。

檢查即時防護

若要確認即時防護是否正在運作和偵測病毒，請使用 eicar.com 測試檔案。此測試檔案是所有防毒程式都可以偵測到的特殊無害檔案。該檔案由 EICAR 協會 (European Institute for Computer Antivirus Research) 建立，目的是用來測試防毒程式的功能。

若要遠端檢查即時防護的狀態，請使用 **[終端機]** 連線至用戶端電腦並發出下列命令：

```
/Applications/.scep/Contents/MacOS/scep_daemon --status
```

即時掃描器狀態將以 `RTPStatus=Enabled` 或 `RTPStatus=Disabled` 顯示。

終端機 bash 輸出也包括下列狀態：

- 用戶端電腦中已安裝的 System Center Endpoint Protection 版本
- 病毒資料庫的日期和版本
- 更新伺服器的路徑

附註： 僅建議進階使用者使用「終端機」。

即時防護無法運作時怎麼辦

在本章中，我們說明使用即時防護時可能發生的問題情況，以及如何疑難排解這些問題。

已停用即時防護

如果使用者不小心停用即時防護，則需要重新啟動。若要重新啟動即時防護，請瀏覽至 **[設定]** > **[病毒及間諜程式防護]**，並按一下主要程式視窗的 **[啟用即時檔案系統防護]** 連結 (右側)。或者您可以選取 **[啟用即時檔案系統防護]** 選項，以在 **[防護]** > **[即時防護]** 下的 [進階設定] 視窗中啟用即時檔案系統防護。

即時防護不會偵測及清除入侵
請確定電腦上未安裝任何其他防毒程式。如果同時啟用兩個即時防護程式，則可能互相衝突。我們建議您解除可能在安裝系統上的任何其他防毒程式。

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

指定電腦掃描

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

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

您也可以從桌面或 [Finder] 視窗將選取的檔案或資料夾拖放至 System Center Endpoint Protection 主畫面、停駐圖示、功能表列圖示 (畫面頂端) 或應用程式圖示 (位於 /Applications 資料夾)。

掃描類型

有兩種可用的指定電腦掃描類型。**[智慧型掃描]** 可快速掃描系統，而無需進一步配置掃描參數。**[自訂掃描]** 可讓您選取任何預先訂義的掃描設定檔，以及選擇特定掃描目標。

智慧型掃描

智慧型掃描可讓您快速啟動電腦掃描並清除感染的檔案，無需使用者介入。它的主要優點是可以輕鬆執行作業，而不需要詳細的掃描配置。智慧型掃描會檢查所有資料夾中的所有檔案，且會自動清除或刪除偵測到的入侵。清除層級會自動設為預設值。如需更多有關清除類型的詳細資訊，請參閱清除 13。

自訂掃描

如果您要指定掃描參數 (例如掃描目標及掃描方法)，則可選用最佳的**自訂掃描**。執行「自訂」掃描的優點是可以詳細地配置參數。您可以將不同的配置儲存為使用者定義的掃描設定檔，以利於使用相同參數重複執行掃描。

若要選取掃描目標，請選取 **[電腦掃描]** > **[自訂掃描]**，然後從樹狀結構中選取特定的 **[掃描目標]**。亦可輸入您希望納入的資料夾或檔案路徑，更精確地指定掃描目標。如果您只對掃描系統有興趣，且不使用其他清除處理方式，請選取 **[掃描但不清除]** 選項。您亦可進一步使用下列方法選用三種清除層級：按一下 **[設定...]**> **[清除]**。

建議具有使用防毒程式經驗的進階使用者使用「自訂掃描」執行電腦掃描。

掃描目標

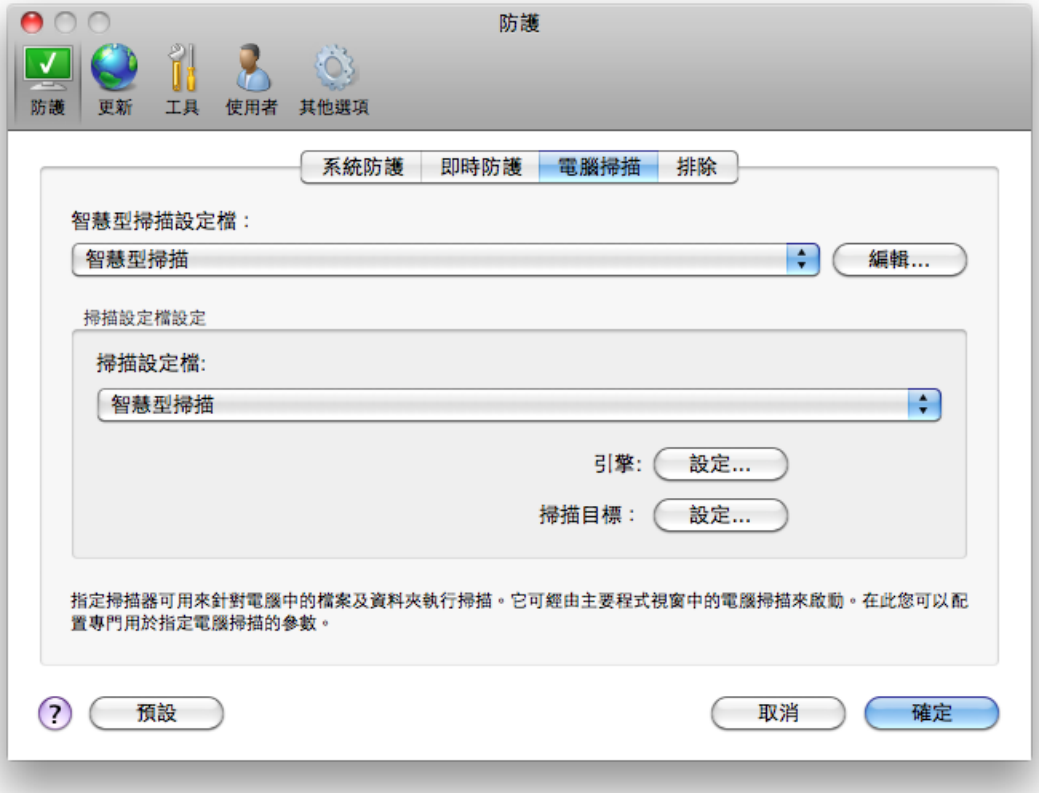
掃描目標樹狀結構可讓您選取要進行病毒掃描的檔案與資料夾。您也可以根據設定檔的設定來選取資料夾。

輸入您希望納入掃描的資料夾或檔案路徑，以更精確地定義掃描目標。從列出電腦上所有可用資料夾的樹狀結構中選取目標。

掃描設定檔

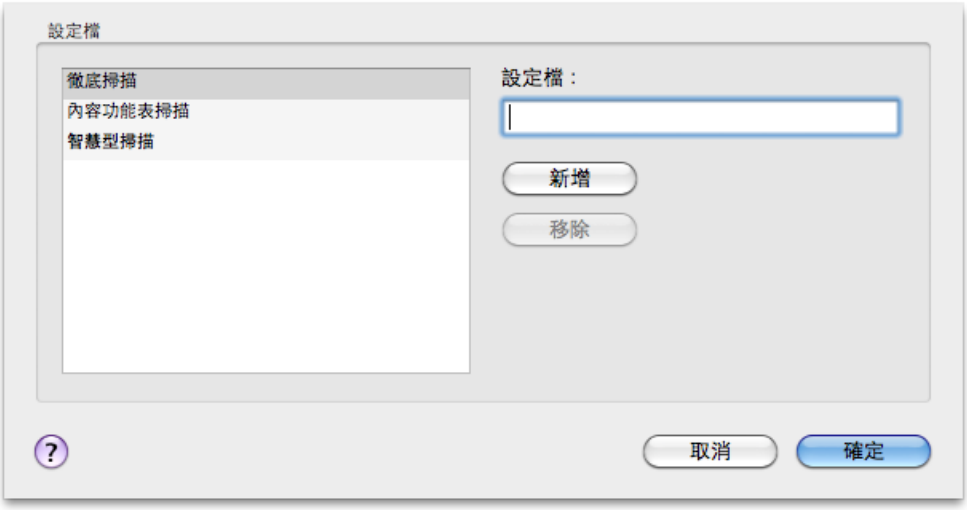
您偏好的掃描設定可儲存供未來掃描時使用。我們建議您盡量為定期進行的掃描建立不同設定檔 (含有各種掃描目標、掃描方法及其他參數)。

若要建立新的設定檔，請移至 **[設定]** > **[進入應用程式喜好設定...]**> **[防護]** > **[電腦掃描]**，然後再按一下目前設定檔清單旁的 **[編輯...]**。



若要協助您建立掃描設定檔以符合您的需求，請參閱引擎參數設定 12 一節以取得每個掃描設定參數的說明。

範例：假設您要建立您自己的掃描設定檔且「智慧型掃描」配置有部份適用，但不要掃描 Runtime Packer 或潛在不安全的應用程式，並且要套用「完全清除」。在 **[指定掃描器設定檔清單]** 視窗中，輸入設定檔名稱，按一下 **[新增]** 按鈕後按一下 **[確定]** 確認。然後設定 **[引擎]** 和 **[掃描目標]** 來調整參數以符合您的需求。



引擎參數設定

System Center Endpoint Protection 中使用的掃描技術是主動式的，也就是說它也可在新威脅擴散的前幾個小時期間提供保護。其使用多種方法組合 (代碼分析、代碼模擬、一般資料庫、病毒資料庫)，共同合作以大幅增強系統安全性。掃描引擎可以同時控制數個資料串流，以最大化效能及偵測率。這種技術還可以成功防範 Rootkit。

引擎技術設定選項允許您指定數個掃描參數：

- 要掃描的檔案類型及副檔名
- 各種偵測方法的組合
- 清除的等級等

若要進入設定視窗，請按一下 **[設定]** > **[病毒及間諜程式防護]** > **[進階病毒及間諜程式防護設定]**，然後按一下位於 **[系統防護]**? **[即時防護]** 及 **[電腦掃描]** 萬用字元中的 **[設定...]** 按鈕。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，分別進行引擎參數配置：

- **[系統防護]** > [自動啟動檔案檢查]
- **[即時防護]** > [即時檔案系統防護]
- **[電腦掃描]** > [指定電腦掃描]

每個模組的引擎參數都已特別最佳化，其修改對系統作業有很大影響。例如，變更設定一定會掃描 Runtime Packer，或啟用即時檔案系統防護模組中的進階探索法可能會造成系統速度變慢。因此，除了「電腦」掃描之外，我們建議您不要變更任何模組的預設引擎參數。

物件

[物件] 區段可讓您定義要掃描是否有入侵的電腦檔案。

- **檔案** - 掃描所有一般檔案類型 (程式、圖片、音訊檔、視訊檔、資料庫檔案等)。
- **捷徑** - (僅限指定掃描器) 掃描包含文字字串的特殊檔案類型，該文字字串由作業系統解譯並接著作為到另一個檔案或目錄的路徑。
- **電子郵件檔案** - (無法在即時防護中使用) 掃描包含電子郵件訊息的特殊檔案。
- **信箱** - (無法在即時防護中使用) 掃描系統中的使用者信箱。使用此選項的方法錯誤可能導致與您的電子郵件用戶端產生衝突。
- **壓縮檔** - (無法在即時防護中使用) 掃描壓縮在壓縮檔 (.rar、.zip、.arj、.tar 等) 中的檔案。
- **自我解壓縮檔** - (無法在即時防護中使用) 掃描包含在自我解壓縮檔中的檔案。
- Runtime Packer - 除了 UPX、yoda、ASPack、FGS 等標準靜態壓縮器之外，Runtime Packer (不同於標準壓縮檔類型) 會在記憶體中解壓縮。

選項

在 **[選項]** 區段中，您可以選取在掃描系統是否有入侵時使用的方法。可用選項如下：

- **探索法** - 探索法是分析程式 (惡意) 活動的演算法。探索法偵測的主要優點是可以偵測之前不存在或不在已知病毒清單 (病毒資料庫) 中的新惡意軟體。
- **進階探索法** - 進階探索法由獨特的探索演算法組成，其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所撰寫。程式的偵測能力因進階探索法而大幅提高。
- **潛在不需要應用程式** - 這些應用程式不一定是惡意的，但是會以負面方式影響電腦的效能。這些應用程式通常需要經過同意才能安裝。如果他們存在於您的電腦上，系統的行為會有所不同 (相較於安裝應用程式前的行為)。最明顯的變更包括：不需要的快顯視窗、啟動及執行隱藏的程序、增加系統資源的使用、搜尋結果中的變更，以及與遠端伺服器通訊的應用程式。
- **潛在不安全的應用程式** - 這些應用程式指的是某些商業軟體和合法軟體，當使用者在未察覺的情況下安裝這些軟體時，攻擊者便能取得濫用的機會。此類別包括如遠端存取工具等程式，因此預設停用此選項。

清除

清除設定決定掃描器清除受感染檔案的方法。有 3 個清除層級：

- **不清除** - 不會自動清除受感染的檔案。程式會顯示警告視窗並允許您選擇處理方法。
- **標準清除** - 程式會嘗試自動清除或刪除受感染檔案。如果無法自動選取正確的處理方法，則程式會提供後續處理方法的選項。無法完成預先定義的處理方法時，也會顯示後續處理方法的選項。
- **完全清除** - 程式會清除或刪除所有受感染檔案 (包括壓縮檔)。只有系統檔案例外。如果無法清除受感染的檔案，則會在警告視窗中提供您可採取的處理方法。

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

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。參數設定的這個區段可讓您定義要從掃描排除的檔案類型。

依預設，會掃描所有檔案，無論其副檔名為何。可以將任何副檔名新增至從掃描中排除的檔案清單。使用 **[新增]** 及 **[移除]** 按鈕，您可以啟用或禁止所需副檔名的掃描。

如果掃描某些檔案類型會造成應用程式無法正常運作，有時必須排除這種檔案不予掃描。例如，建議排除 .log? .cfg 與 .tmp 副檔名。

限制

[限制] 區段可讓您指定物件的大小上限，以及要掃描的巢狀壓縮檔層級：

- **大小上限：**定義要掃描的物件大小上限。防毒模組則會掃描小於指定大小的物件。我們不建議變更預設值，因為通常沒有要修改預設值的理由。只有進階使用者基於特定的理由，才應變更此選項來排除掃描較大物件。
- **掃描時間上限：**定義分配用於掃描物件的時間上限。如果已在這裡輸入使用者定義的值，則當該時間到期，防毒模組會停止掃描物件，無論掃描是否完成。
- **巢狀層級上限：**指定壓縮檔掃描的深度層級上限。我們不建議變更預設值 10；在正常情況下，應該沒有要修改預設值的理由。如果由於巢狀壓縮檔的數目而提前結束掃描，則壓縮檔會保持未檢查狀態。
- **檔案大小上限：**此選項可讓您指定要掃描的壓縮檔中，所包含檔案的大小上限 (解壓縮時)。如果掃描由於此上限的結果而提前結束，則壓縮檔會保持未檢查狀態。

其他

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。各種保護模組都會聰明地掃描，並利用不同的掃描方式將其套用至特定的檔案類型。產品中沒有嚴格地定義「智慧型最佳化」。我們的開發小組繼續實作新的變更，然後透過定期更新來整合至 System Center Endpoint Protection。如果停用「智慧型最佳化」，則當執行掃描時，只會套用特定模組的引擎核心中使用者定義的設定。

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

偵測到入侵

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

如果您的電腦出現速度變慢、經常停止等惡意軟體感染的徵兆，我們建議下列步驟：

1. 開啟 System Center Endpoint Protection，然後按一下 **[電腦掃描]**。
2. 按一下 **[智慧型掃描]** 按鈕 (如需更多資訊，請參閱智慧型掃描 10 一節)。
3. 完成掃描之後，請檢閱已掃描、受感染及已清除的防護記錄。

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

在此為了說明 System Center Endpoint Protection 如何處理入侵，請假設使用預設清除層級的即時檔案系統監視器偵測到入侵。此時該監視器通常會嘗試清除或刪除檔案。如果沒有針對即時防護模組的預先定義處理方法，則會要求您在警告視窗中選取一個選項。通常，可以使用 **[清除]**? **[刪除]** 及 **[不進行處理]** 選項。不建議選取 **[不進行處理]**，因為此選項會以原貌保留受感染的檔案。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。

清除及刪除 - 如果檔案受到已連接惡意程式碼的病毒攻擊，則套用清除。如果是這種情況，則請先嘗試清除受感染的檔案，以將其還原為原始狀態。如果該檔案僅由惡意程式碼組成，則會刪除該檔案。

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

更新程式

維持最高等級安全性必須定期更新 System Center Endpoint Protection。「更新」模組下載最新的病毒資料庫，確保程式永遠是最新程式。

從主要功能表中按一下 **[更新]** 可以尋找目前更新狀態，包括上一次成功更新日期與時間，並在需要時更新。若要以手動方式啟動更新程序，請按一下 **[更新病毒資料庫]**。

在正常情況下，適當地下載更新之後，[更新] 視窗中會出現 *[不需要更新 - 已安裝的病毒資料庫是最新的]* 訊息。

[更新] 視窗內也含有病毒資料庫版本的相關資訊。此數字指示是連往網站的作用中連結，而網站中會列出特定更新中新增的所有病毒碼。

更新設定

若要使用測試模式 (下載發佈前更新)，請按一下 **[進階選項]** 旁的 **[設定...]** 按鈕，選取 **[啟用發佈前更新]** 核取方塊。若要停用每次成功更新後於系統匣中顯示的通知，請選取 **[不顯示成功更新的通知]** 核取方塊。

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

如何建立更新工作

您可使用下列方式手動觸發更新：按一下主要功能表中的 **[更新]** 之後，在顯示的主要視窗中按一下 **[更新病毒資料庫]**。

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

- **定期自動更新**
- **使用者登入後自動更新**

各個更新工作都可以修改，以滿足您的需求。除了預設更新工作之外，您亦可利用使用者定義的配置來建立新的更新工作。如需建立及配置更新工作的詳細資料，請參閱排程器 16 一節。

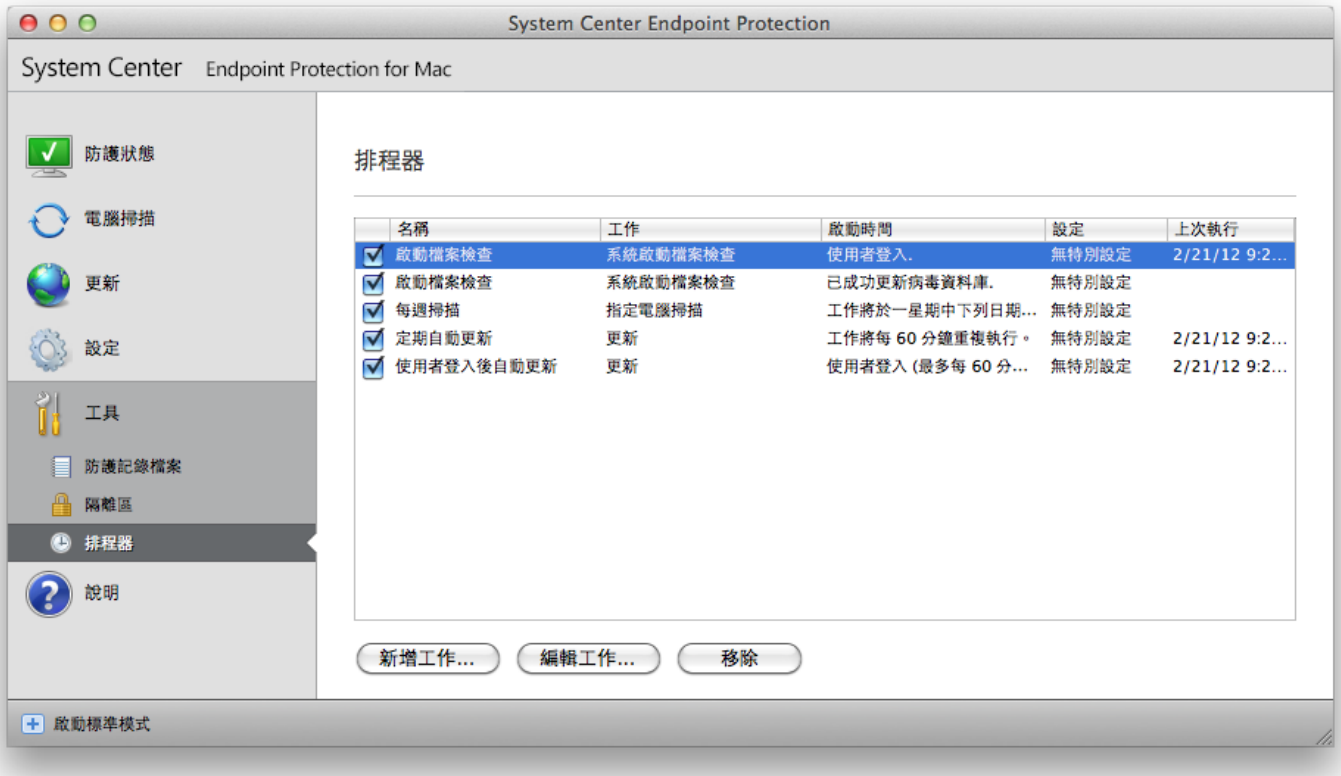
升級為新組建

若要保持最嚴格的防護，使用 System Center Endpoint Protection 的最新組建是很重要的。若要檢查是否有新版本，請按一下左側主要功能表中的 **[更新]**。當有新組建可用時，視窗底部將會顯示 *[新版產品已推出！]* 訊息。按一下 **[深入瞭解...]** 在新視窗中顯示新組建的版本號碼及變更記錄。

按一下 **[下載]** 以下載最新的組建。按一下 **[關閉]** 以關閉視窗，並稍後再下載升級程式。

排程器

如果已啟動了 System Center Endpoint Protection 的「進階」模式，則可以使用 **[排程器]**。您可在 **[工具]** 下方的 System Center Endpoint Protection 主要功能表中找到 [排程器]。**[排程器]** 包含所有已排程的工作及其配置內容 (例如預先定義的日期、時間、使用的掃描設定檔) 的清單。



依預設，下列已排程的工作會顯示在「排程器」中：

- 定期自動更新
- 使用者登入後自動更新
- 使用者登入後進行啟動檔案檢查
- 成功更新病毒資料庫後進行啟動檔案檢查
- 防護記錄維護 (啟用排程器設定中的 **[顯示系統工作]** 選項後)
- 每週掃描

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

排程工作的目的

排程器使用預先定義的配置與內容管理及啟動排程工作。配置與內容包含資訊，如日期與時間，以及工作執行期間要使用的指定設定檔。

建立新工作

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

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

由於更新是其中一個最常用的已排程工作，因此我們將說明如何新增新的更新工作。

從 **[已排程的工作]** 下拉式功能表中，選取 **[更新]**。將工作名稱輸入 **[工作名稱]** 欄位中。從 **[執行工作]** 下拉式功能表中選取工作頻率。可用選項如下：**[使用者定義]**? **[一次]**? **[重複]**? **[每日]**? **[每星期]** 與 **[事件觸發]**。系統會根據選取的頻率，提示您不同的更新參數。

如果您選取 **[使用者定義]**，則系統會提示您以 cron 格式指定日期/時間 (如需更多詳細資料，請參閱建立使用者定義的工作 17一節)。

在下一步中，定義排程期間無法執行或完成工作時要採取的處理方法。可用的三個選項如下所示：

- **等到下一個排程的時間**
- **盡快執行工作**
- **如果距離上次執行工作的時間超過指定的時間間隔，則立即執行工作** (可以使用 **[最小工作時間間隔]** 選項定義間隔)

在下一步中，則會顯示含有目前已排程工作相關資訊的摘要視窗。按一下 **[完成]** 按鈕。

新已排程的工作將新增至目前已排程的工作清單。

依預設，系統包含重要的已排程工作，以確保產品功能正常。依預設，不應改變與隱藏這些工作。若要變更此選項並顯示這些工作，請進入 **[設定]** > **[進入應用程式喜好設定...]**> **[工具]** > **[排程器]**，然後再選取 **[顯示系統工作]** 選項。

建立使用者定義的工作

[使用者定義] 工作的日期和時間必須以全年排程的 cron 格式 (由 6 個以空格分隔的欄位所組成的字串) 輸入：
`分鐘(0-59) 小時(0-23) 月中日(1-31) 月份(1-12) 年份(1970-2099) 週間日(0-7)(星期日 = 0 或 7)`

範例：
```
30 6 22 3 2012 4
```

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

不支援日期名稱 (星期一 - 星期日) 及月份名稱 (1 月 - 12 月)。

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

隔離區

隔離區的主要工作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 System Center Endpoint Protection 錯誤偵測到的檔案，應該予以隔離。

您可以選擇隔離任何檔案。如果檔案行為可疑，但防毒掃描器沒有偵測到，則建議進行隔離。

您可以在表格中檢視隔離區資料夾中儲存的檔案，其中顯示隔離的日期與事件、受感染檔案原始位置的路徑、大小 (以位元組為單位)、原因 (例如，由使用者新增...)，以及威脅數量 (例如，包含多個入侵的壓縮檔)。內有隔離檔案的隔離區資料夾 (/Library/Application Support/Microsoft/scep/cache/quarantine) 即使在解除安裝 System Center Endpoint Protection 後仍會留在系統中。隔離的檔案以安全的加密形式儲存，而且在安裝 System Center Endpoint Protection 後可以再次還原。

隔離檔案

System Center Endpoint Protection 會自動隔離刪除的檔案 (如果您尚未在警告視窗中取消此選項)。如果需要，您可以按一下 **[隔離...]** 按鈕，手動隔離任何可疑檔案。亦可使用內容功能表達到此目的 - 按下 Ctrl，按一下空白欄位，選取 **[隔離...]**，選擇您想要隔離的檔案並按一下 **[開啟]** 按鈕。

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]** 按鈕可達到此目的。[還原] 可從內容功能表取得，方法是按下 Ctrl，並且按一下 **[隔離區]** 視窗中指定的檔案，然後按一下 **[還原]**。內容功能表還提供 **[還原到...]** 選項，可讓您將檔案還原到其原始刪除位置外的其他位置。

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，並提供偵測到威脅的概觀。在系統分析、威脅偵測及疑難排解方面，防護記錄都是一項很重要的工具。防護記錄會主動在背景中執行，不需使用者互動。系統會根據目前的防護記錄冗贅設定來記錄資訊。您可以直接從 System Center Endpoint Protection 環境檢視文字訊息及防護記錄，以及保存防護記錄。

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

1. **偵測到威脅** - 使用此選項，可檢視與偵測入侵相關之事件的所有資訊。
2. **事件** - 此選項專供系統管理員及使用者用來解決問題。System Center Endpoint Protection 執行的所有重要處理方法都會記錄在「事件」防護記錄中。
3. **電腦掃描** - 所有已完成的掃描結果都會顯示在此視窗中。按兩下任何項目，以檢視各個指定電腦掃描的詳細資料。

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

防護記錄維護

System Center Endpoint Protection 的記錄配置可從主要程式視窗存取。按一下 **[設定]** > **[進入應用程式喜好設定...]**> **[工具]** > **[防護記錄檔案]**。您可以指定下列用於防護記錄檔案的選項：

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

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

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

根據 **[文字防護記錄檔案:][編輯]** 下所選的選項，您可以在儲存防護記錄時寫入下列資訊：

- 將啟動掃描器、即時防護或電腦掃描偵測到的威脅儲存至名為 threatslog.txt 的檔案。
- 將*無效的使用者名稱和密碼*? *無法更新病毒資料庫*等事件寫入 eventslog.txt 檔案。
- 將所有已完成掃描的結果以 scanlog.NUMBER.txt 格式儲存。

若要配置 **[預設電腦掃描防護記錄]** 過濾器，請按一下此選項旁的 **[編輯...]** 按鈕，並視需要選取/取消選取防護記錄類型。您可在此章節 18找到這些防護記錄類型的進一步說明。

防護記錄過濾

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

最常使用的防護記錄類型如下所示：

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

使用者介面

System Center Endpoint Protection 中的使用者介面配置選項允許您調整工作環境以符合您的需要。從 **[設定]** > **[進入應用程式喜好設定...]**> **[使用者]** > **[介面]** 可存取這些配置選項。

在此區段中，[進階模式] 選項提供使用者切換至「進階模式」的功能。「進階模式」會顯示 System Center Endpoint Protection 更多的詳細設定與其他控制項。

若要啟用啟動時顯示開機歡迎畫面，請選取 **[啟動時顯示開機歡迎畫面]** 選項。

在 **[使用標準功能表]** 區段中，您可以選取 **[在標準模式]**/**[在進階模式]** 選項 ，以啟用個別顯示模式的主要程式視窗中的標準功能表。

若要啟用工具提示，請選取 **[顯示工具提示]** 選項。**[顯示隱藏的檔案]** 選項可讓您看到並選取 **[電腦掃描]** 的 **[掃描目標]** 設定中的隱藏檔案。

警告及通知

[警告及通知] 區段可讓您配置在 System Center Endpoint Protection 中如何處理威脅警告與系統通知。

停用 **[顯示警告]** 選項會取消所有警告視窗，而且只適用在特定情況中。對於大部分使用者而言，建議保留此選項的預設值 (啟用)。

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

警告及通知進階設定

只顯示需要使用者互動的通知
使用此選項，您可以切換需要使用者互動之訊息的顯示。

只顯示在全螢幕模式中執行應用程式時需要使用者互動的通知
此選項在簡報或執行其他需要全螢幕的活動時有用。

權限

System Center Endpoint Protection 設定對您公司的安全原則可能非常重要。未獲授權的修改可能會危害您系統的穩定性及防護功能。因此，您可以選擇哪一個使用者有編輯程式配置的權限。

若要指定有權限的使用者，請進入 **[設定]** > **[進入應用程式喜好設定...]**> **[使用者]** > **[權限]**。

為了提供系統最大的安全性，請務必正確地配置程式。未獲授權的修改可能會導致重要資料遺失。若要設定有權限的使用者清單，從左側的 **[使用者]** 清單中選取使用者，然後按一下 **[新增]** 按鈕。若要移除使用者，從右側的 **[有權限的使用者]** 清單中選取使用者名稱，然後按一下 **[移除]**。

附註： 如果有權限的使用者清單空白，表示系統的所有使用者都有編輯程式設定的權限。

內容功能表

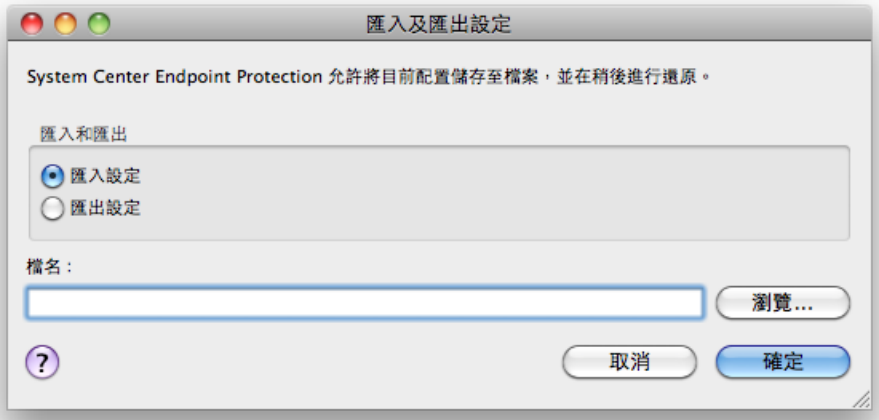
您可在 **[設定]** > **[進入應用程式喜好設定...]**> **[使用者]** > **[內容功能表]** 區段中啟用 **[整合至內容功能表]** 核取方塊，以啟用內容功能表整合。

進階使用者

匯入及匯出設定

在 **[設定]** 下的進階模式中可以匯入和匯出 System Center Endpoint Protection 的配置。

匯入和匯出都使用壓縮檔儲存設定。如果您需要備份 System Center Endpoint Protection 的目前配置以供稍後使用，匯入和匯出很有幫助。匯出設定選項對想要在多個系統上使用 System Center Endpoint Protection 慣用設定的使用者也很方便，他們可以輕鬆匯入配置檔案以傳送所需的設定。



匯入設定

匯入配置很簡單。從主要功能表中，按一下 **[設定]** > **[匯入及匯出設定...]**，然後選取 **[匯入設定]** 選項。輸入配置檔案的名稱，或按一下 **[瀏覽...]** 按鈕以瀏覽您要匯入的配置檔案。

匯出設定

匯出配置的步驟非常類似。從主要功能表中，按一下 **[設定]** > **[匯入及匯出設定...]**。選取 **[匯出設定]** 選項，並輸入配置檔案的名稱。使用瀏覽器，選取在電腦上儲存配置檔案的位置。

Proxy 伺服器設定

您可在 **[其他選項]** > **[Proxy 伺服器]** 下配置 Proxy 伺服器設定。在這個等級指定 Proxy 伺服器，會定義所有 System Center Endpoint Protection 功能的全域 Proxy 伺服器設定。需連線到網際網路的所有模組，都會使用這裡設定的參數。

若要在這個等級指定 Proxy 伺服器設定，請選取 **[使用 Proxy 伺服器]** 核取方塊，然後在 **[Proxy 伺服器]** 欄位提供您 Proxy 伺服器的 IP 位址或 URL。在連接埠欄位中，指定 Proxy 伺服器接受連線所在的連接埠 (依預設為 3128)。如果與 Proxy 伺服器之間的通訊需要驗證，請選取 **[Proxy 伺服器需要驗證]** 核取方塊，並將有效的 **[使用者名稱]** 及 **[密碼]** 輸入各自的欄位中。

可移除的媒體封鎖

可移除的媒體 (如 CD 或 USB 隨身碟) 可能包含惡意程式碼，讓您的電腦瀕於危險。若要封鎖可移除的媒體，選取 **[啟用可移除的媒體封鎖]** 旁的核取方塊。若要允許存取特定媒體類型，請取消選取欲允許之媒體類型旁的核取方塊。

如果您要將這些設定套用至 CD、DVD、FireWire 或 USB 以外的媒體類型，請選取 **[其他]** 旁的核取方塊。此設定會特別套用至任何透過 Thunderbolt 介面連接至您電腦的任何周邊設備。

字彙

入侵類型

「入侵」是嘗試進入及/或損害使用者電腦的一種惡意軟體。

病毒

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

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

電腦病毒有目的與嚴重性之分。有些病毒因為能夠故意將硬碟機中的檔案刪除，而顯得極度危險。另一方面，有些病毒並不會造成真正的損害 –這些病毒只會困擾使用者，並展現其作者的技術。

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

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

病毒的範例如下：OneHalf? Tenga 和 Yankee Doodle。

蠕蟲

電腦蠕蟲是含有惡意程式碼的程式，該程式會攻擊主機電腦，並透過網路散佈。病毒與蠕蟲的基本差異在於蠕蟲有能力自行複製及傳輸 - 蠕蟲不需仰賴主機檔案 (或開機磁區)。蠕蟲透過連絡人名單中的電子郵件地址散佈，或利用網路應用程式中的安全性弱點。

因此，蠕蟲的存活率比電腦病毒高多了。因為網際網路的普及，蠕蟲可能在發佈的數小時內，就散佈到全世界，有時甚至只需幾分鐘的時間。這種獨立又快速的複製能力，使蠕蟲比其他類型的惡意軟體更加危險。

在系統中活化的蠕蟲會造成許多不便：如刪除檔案、降低系統效能，甚至會停用程式。電腦蠕蟲的本質使其能夠成為其他入侵類型的「傳輸媒介」。

如果您的電腦感染了蠕蟲，我們建議您刪除受感染的檔案，因為其中可能包含惡意程式碼。

知名的蠕蟲範例如下：Lovsan/Blaster? Stration/Warezov? Bagle 和 Netsky。

特洛伊木馬程式

從歷史角度來看，電腦特洛伊木馬程式已被定義為一種入侵活動類別，該程式會嘗試以有用的程式呈現，矇騙使用者執行這些程式。如今特洛伊木馬程式已經不需要再偽裝自己。特洛伊木馬程式唯一的目的，就是用最容易的方法進行入侵，並達成其惡意的目標。「特洛伊木馬程式」已經變成非常普遍的詞彙，用以描述無法歸入特定類別的入侵。

由於這是非常廣泛的類別，所以通常會細分為許多子類別：

- 下載程式 - 會從網際網路下載其他入侵的一種惡意程式。
- 病毒植入程式 - 這種特洛伊木馬程式類型主要會將其他類型的惡意軟體放置在被入侵的電腦上。
- 後門程式 - 一種與遠端攻擊者通訊的應用程式，可讓攻擊者存取系統，進而控制系統。
- 鍵盤記錄木馬程式 - (按鍵側錄程式) - 此程式會記錄使用者按下的每一個按鍵，並將該資訊傳送給遠端攻擊者。
- 播號程式 - 播號程式是專門用來連線至高費率電話號碼的程式。使用者幾乎不可能查覺到有新的連線建立。Dialer 只能對使用撥接數據機的使用者造成損害，而現在已經不常使用撥接數據機了。
- 特洛伊木馬程式通常採用執行檔的形式。如果偵測到您的電腦上有某個檔案是特洛伊木馬程式，建議您將該程式刪除，因為其中極可能包含惡意程式碼。

知名的特洛伊木馬程式範例如下：NetBus？ Trojandownloader.Small.ZL？ Slapper。

廣告程式

廣告程式是廣告支援軟體的簡稱。舉凡可顯示廣告素材的程式均屬於這個種類的軟體。廣告程式應用程式會經常在網際網路瀏覽器中自動開啟包含廣告的快顯視窗，或變更瀏覽器的首頁。廣告程式通常隨附於免費軟體程式，讓免費軟體程式建立者負擔其 (通常很有用) 應用程式的開發成本。

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

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

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

間諜程式

此類別包括會在使用者未同意/不知情的情況下，傳送私人資訊的所有應用程式。間諜程式會利用追蹤功能來傳送各種統計資料，例如：造訪過的網站清單、使用者通訊錄中的電子郵件地址，或是記錄過的按鍵清單。

間諜程式的作者會宣稱這些技術的目的是為了深入瞭解使用者的需求和興趣，使宣傳目標更為精準。問題是有益的和惡意的應用程式之間沒有明顯的分界，而且沒有人可以確保所擷取的資訊不會被濫用。間諜程式應用程式取得的資料可能包含安全密碼、PIN、銀行帳號等等。免費版程式的作者通常會將間諜程式搭載於該程式，以創造收益，或是激勵您購買軟體。通常在程式安裝期間，就會讓使用者知道間諜程式的存在，以刺激其升級為沒有間諜程式的付費版本。

例如，P2P (點對點) 網路的用戶端應用程式，就是著名的搭載間諜程式的免費軟體產品。Spyfalcon 或 Spy Sheriff (以及許多其他程式) 屬於特定的間諜軟體子類別，看似間諜程式防護程式，但事實上本身就是間諜程式。

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

潛在不安全的應用程式

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

「潛在不安全的應用程式」是用於商業、合法軟體的分類。此分類包括的程式諸如遠端存取工具、密碼破解應用程式，以及 keylogger (會記錄使用者按下之每個按鍵的程式)。

如果您在電腦上發現有潛在不安全的應用程式存在並執行中 (而您沒有安裝該程式)，請洽詢您的網路系統管理員，或是移除該應用程式。

潛在不需要應用程式

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

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