Trend Micro Apex One™

Patch 5

管理手冊

企業資訊安全整體防護

Endpoint Security

Protected Cloud

Web Security

文件編號：APTM09289/210618

發行日期：2021 年 6 月

受美國專利保護，專利編號： 5,951,698

本文件介紹了產品的主要功能，並/或提供作業環境的安裝說明。在安裝或使用產品前，請先閱讀此文件。

如需有關如何使用產品特定功能的詳細資訊，請參閱趨勢科技線上說明中心和/或趨勢科技常見問題集。

趨勢科技十分重視文件品質的提升。如果您對於本文件或其他趨勢科技文件有任何問題、意見或建議，請與我們聯絡，電子郵件信箱為 docs@trendmicro.com。

請至下列網站並給予您對此文件的評估意見：

https://www.trendmicro.com/download/documentation/rating.asp

隱私權資料和個人資料蒐集披露

趨勢科技產品中所提供的部分功能會蒐集與產品使用和偵測相關的資訊，並建議傳送回饋給趨勢科技。少數資訊在部分司法管轄權和法規下會視為個人資料。如果您不希望趨勢科技蒐集您的個人資訊，則建議您務必詳細瞭解並確認是否要關閉相關功能。

以下連結列出 Trend Micro Apex One 將蒐集的資料類型，並提供有關如何關閉特定資訊回饋功能的詳細說明。

https://success.trendmicro.com/data-collection-disclosure

趨勢科技所蒐集的資料將遵循趨勢科技隱私權注意事項中的規定：

https://www.trendmicro.com/privacy

目錄

附錄 A：Apex One 中的 IPv6 支援

附錄 B：Windows Server Core 支援

附錄 C：Apex One 還原

附錄 D：詞彙

索引

序言

序言

本文件討論使用資訊、用戶端安裝程序及 Apex One 伺服器和用戶端管理。

包含下列主題：

Apex One 文件

Apex One 文件包含下列各項：

表 1. Apex One 文件

文件	說明
安裝和升級手冊	討論安裝 Apex One 伺服器以及升級伺服器和用戶端的需求與程序的 PDF 文件 注意 次要發行版本、Service Pack 和修補程式可能不提供《安裝和升級手冊》。
系統需求	簡述安裝 Apex One 伺服器以及升級伺服器和用戶端的最低與建議系統需求的 PDF 文件
管理手冊	討論開始使用資訊、Security Agent 安裝程序及 Apex One 伺服器與用戶端管理的 PDF 文件
說明	編譯為 WebHelp 或 CHM 格式的 HTML 檔案，提供「相關指示」、使用建議和特定領域資訊。可以從 Apex One 伺服器和用戶端主控台存取「說明」，也可以從 Apex One 主安裝程式存取。
Readme 檔	包含一份已知問題和基本安裝步驟的清單。可能也包含「說明」或印刷文件中未提供的最新產品資訊
常見問題集	提供問題解決方法和疑難排解資訊的線上資料庫。此資料庫提供有關產品已知問題的最新資訊。如果要取得「常見問題集」，請至下列網站： http://www.trendmicro.com.tw/solutionbank/corporate/default.asp

您可以從下列位置下載最新的 PDF 文件和 Readme 檔：

http://docs.trendmicro.com/zh-tw/enterprise/apex-one.aspx

讀者

Apex One 文件適用於下列使用者：

- Apex One 管理員負責管理 Apex One，包括 Apex One 伺服器和 Security Agent 的安裝與管理。這些使用者必須具備進階網路管理和伺服器管理知識。
- 終端使用者：已在其端點上安裝 Security Agent 的使用者。這些使用者的端點技術程度從初學者到進階使用者都有。

文件慣例

本文件會使用下列慣例。

表 2. 文件慣例

慣例	說明
大寫	頭字語、縮寫、特定的命令名稱和鍵盤上的按鍵
粗體	功能表和功能表命令、命令按鈕、標籤和選項
斜體	參考其他文件
等寬	指令行範例、程式碼、Web URL、檔案名稱和程式輸出
瀏覽 > 路徑	可達到特定畫面的瀏覽路徑 例如，「檔案 > 儲存」代表請點選「檔案」，然後請點選介面上的「儲存」
 注意	組態設定注意事項
 秘訣	推薦或建議

慣例	說明
 重要	必要或預設組態設定和產品限制的相關資訊
 警告!	重要的處理行動和組態設定選項

詞彙

下表提供 Apex One 文件中使用的正式詞彙：

表 3. Apex One 詞彙

詞彙	說明
Security Agent	Apex One 用戶端 程式
用戶端端點	安裝 Security Agent 的端點。
用戶端使用者（或使用者）	用戶端端點上管理 Security Agent 的人員。
伺服器	Apex One 伺服器程式
伺服器電腦	安裝 Apex One 伺服器的端點。
管理員（或 Apex One 管理員）	管理 Apex One 伺服器的人員
主控台	用於設定和管理 Apex One 伺服器及用戶端設定的使用者介面 Apex One 伺服器程式的主控台稱為「Web 主控台」，而 Security Agent 程式的主控台稱為「Security Agent 主控台」。
安全威脅	病毒/惡意程式、間諜程式/可能的資安威脅程式和網路安全威脅的總稱

詞彙	說明
使用授權服務	包括「防毒」、「損害清除及復原服務」、「網頁信譽評等」和「間諜程式防護」—上述功能都會在安裝 Apex One 伺服器期間啟動
Apex One 服務	透過 Microsoft 管理主控台 (MMC) 所代管的服務。例如：`ofcservice.exe`（Apex One Master Service）。
程式	包括 Security Agent 和 Plug-in Manager
元件	負責針對安全威脅進行掃瞄、偵測和採取中毒處理行動

用戶端安裝資料夾	端點上包含 Security Agent 檔案的資料夾。如果在安裝期間接受預設設定，您可以在下列任一位置找到安裝資料夾：
	`C:\Program Files\Trend Micro\Security Agent`
	`C:\Program Files (x86)\Trend Micro\Security Agent`

伺服器安裝資料夾	端點上包含 Apex One 伺服器檔案的資料夾。如果在安裝期間接受預設設定，您可以在下列任一位置找到安裝資料夾：
	`C:\Program Files\Trend Micro\Apex One`
	`C:\Program Files (x86)\Trend Micro\Apex One`
	例如，如果在伺服器安裝資料夾的 `\PCCSRV` 下找到特定檔案，則該檔案的完整路徑是：
	`C:\Program Files\Trend Micro\Apex One\PCCSRV\<file_name>`.

雲端截毒掃瞄用戶端	已設定為使用雲端截毒掃瞄的任何 Security Agent
標準掃瞄用戶端	已設定為使用標準掃瞄的任何 Security Agent

詞彙	說明
雙堆疊	同時具有 IPv4 和 IPv6 位址的實體。 例如： • 同時具有 IPv4 和 IPv6 位址的端點 • 安裝在雙堆疊端點上的 Security Agent • 會將更新分發到用戶端的更新代理程式 • 雙堆疊 Proxy 伺服器（如 DeleGate）可以在 IPv4 和 IPv6 位址之間進行轉換
單純 IPv4	僅具有 IPv4 位址的實體
單純 IPv6	僅具有 IPv6 位址的實體
嵌入程式解決方案	透過 Plug-in Manager 提供的本機 Apex One 功能和嵌入程式

部分 I

簡介和入門

第 1 章

Apex One 簡介

本章介紹 Trend Micro Apex One™，並提供其特性與功能的總覽。

包含下列主題：

關於 Apex One

Trend Micro Apex One™ 可保護企業網路不受惡意程式、網路病毒、Web-based 安全威脅、間諜程式和混合式安全威脅的攻擊。Apex One 是一種整合式解決方案，它是由常駐於端點的 Security Agent 程式和用於管理所有用戶端的伺服器程式所組成。Security Agent 可保護端點，並向伺服器回報其安全狀態。伺服器的 Web-based 管理主控台則可讓您輕鬆地設定協調的安全策略和向每個 Security Agent 部署更新。

Apex One 應用了新一代的雲端用戶端基礎結構「趨勢科技主動雲端截毒技術™」，這種技術提供比傳統方式更具智慧的安全解決方案。獨一無二的雲端技術和輕量型用戶端可減少對於傳統病毒碼下載的依賴，以及降低通常與桌面更新相關聯的的延遲。此技術可讓企業減少網路頻寬耗用、降低處理量並節省相關成本。不論使用者在企業網路內、在家裡或在外，只要一連線就可以立即享有最新的防護。

新增功能

下表概述此版本的 Trend Micro Apex One™ 中的新功能和增強功能。

表 1-1. Apex One Patch 5

項目	說明
管理員通知增強功能	管理員通知功能支援透過選用的 SSL/TLS 加密進行 NTLM 驗證。
Security Agent 自我保護	自我保護設定會自動啟動，使用者無法設定。為了讓所有 Security Agent 隨時受到保護，已移除先前對自我保護功能的相依項目。
平台支援	對 Windows 10 May 2021 Update (21H1) 的 Security Agent 安裝支援。

表 1-2. Apex One Patch 4

項目	說明
SQL 傳輸工具	SQL 傳輸工具支援轉移 Endpoint Sensor 資料庫（前提是安裝在與 Apex One 資料庫所在的同一部伺服器上）。

項目	說明
Endpoint Sensor	Endpoint Sensor 經過增強，可將樣本提交傳送至所設定的沙盒虛擬平台。
平台支援	支援在 Windows 10 October Update (20H2) 上進行 Security Agent 安裝。

表 1-3. Apex One Patch 3

項目	說明
密碼複雜度增強功能	「卸載和解除安裝 Security Agent」功能納入經過增強的密碼複雜度要求，以確保更高的安全性。
加強的平台支援	對 Windows 10 May 2020 Update (20H1) 的 Security Agent 安裝支援。
SQL Server 支援	Apex One 支援 SQL Server 2019

主要功能和優點

Apex One 提供下列功能和優點。

表 1-4. 主要功能和優點

功能	優點
勒索軟體防護	加強的掃瞄功能可透過識別常見行為和封鎖通常與勒索軟體程式關聯的程序，來識別和封鎖針對在端點上執行的文件的勒索軟體程式。
連線的威脅防範	將 Apex One 設定為從 Apex Central 伺服器訂閱可疑物件清單。使用 Apex Central 主控台，您可以為由可疑物件清單偵測到的物件建立自訂處理行動，以針對由您環境專屬的趨勢科技產品保護的端點所識別的安全威脅提供自訂防範。 您可以將 Security Agent 設定為在發現檔案物件可能包含先前未曾識別出的安全威脅時，將檔案物件提交給沙箱做進一步分析。沙箱在評估物件之後，如果發現物件包含未知的安全威脅，就會將物件新增至沙箱可疑物件清單，然後將清單分發給整個網路中的其他 Security Agent。

功能	優點
Plug-in Manager 和嵌入程式解決方案	Plug-in Manager 可幫助安裝、部署及管理 Plug-in 解決方案。 管理員可以安裝兩種嵌入程式解決方案： • Plug-in 程式 • 本機 Apex One 功能
集中化管理	Web-based 管理主控台會給予管理員對網路上所有端點和伺服器的透明存取權。Web 主控台會協調每個端點和伺服器上安全策略、病毒碼檔案和軟體更新的自動部署。而有了「病毒爆發防範服務」，它會阻擋感染媒介並迅速部署攻擊專屬安全策略，以在病毒碼檔案推出前先預防或防堵病毒爆發。Apex One 還會執行即時監控、提供事件通知和傳送全面的報告。管理員可以執行遠端管理、針對個別桌面或群組設定自訂策略，以及鎖定端點安全設定。
防毒/安全威脅防護	Apex One 可透過掃瞄檔案，然後針對偵測到的每個安全威脅執行特定處理動作，來保護電腦免於遭受安全威脅。在短時間內偵測到大量安全威脅為病毒爆發警訊。為控制病毒爆發，Apex One 會強制執行病毒爆發防範策略並隔離中毒電腦，直到電腦不包含任何安全威脅。 Apex One 使用雲端截毒掃瞄讓掃瞄程序更有效率。此技術的運作方式是將先前儲存在本機端點上的大量簽章卸載到主動雲端截毒技術來源。透過這種方式，可以大幅減少不斷增加的端點系統簽章更新量對於系統和網路的影響。 如需有關雲端截毒掃瞄以及如何將其部署到用戶端的資訊，請參閱掃瞄方法類型 第 7-7 頁。

功能	優點
損害清除及復原服務	損害清除及復原服務™會透過全自動程序清除電腦上的 File-based 和網路病毒，以及殘存病毒和蠕蟲（特洛伊木馬程式、登錄項目、病毒檔案）。為了處理所帶來的安全威脅和侵擾，「損害清除及復原服務」會執行下列處理行動： • 偵測並移除活動的特洛伊木馬程式 • 終結特洛伊木馬程式所建立的處理程序 • 修復特洛伊木馬程式修改的系統檔案 • 刪除特洛伊木馬程式遺留的檔案和應用程式 因為「損害清除及復原服務」會在背景自動執行，所以沒有必要進行設定。使用者甚至不會知道「損害清除及復原服務」正在執行。然而，Apex One 有時會通知使用者重新啟動其端點，以便完成移除特洛伊木馬程式的程序。
網頁信譽評等	網頁信譽評等技術會主動在企業網路內外保護用戶端端點，以免於遭受惡意和可能有害之網站的威脅。「網頁信譽評等」會中斷感染鏈並防止下載惡意程式碼。 請將 Apex One 與「主動雲端截毒技術伺服器」或「趨勢科技主動雲端截毒技術」整合，來驗證網站和網頁的可信度。
Apex One 防火牆	Apex One 防火牆使用狀態檢測和高效能網路病毒掃瞄，來保護網路上的端點和伺服器。 您可以依據應用程式、IP 位址、通訊埠號碼或通訊協定來建立用於過濾連線的規則，然後將這些規則套用至不同的使用者群組。
資料外洩防護	資料外洩防護可保護組織的數位資產，免遭受意外或有意的外洩。資料外洩防護允許系統管理員： • 識別要保護的數位資產 • 建立策略，以限制或防止透過常見傳輸通道（例如：電子郵件訊息和外部裝置）傳輸數位資產 • 強制遵守制定的隱私權標準
周邊設備存取控管	「周邊設備存取控管」會規範對連線到端點的外部儲存裝置與網路資源的存取。周邊設備存取控管有助於防止資料遺失與外洩，並且可與檔案掃瞄搭配使用，以協助防禦安全威脅。

功能	優點
行為監控	行為監控會不斷地監控端點上的作業系統或已安裝軟體是否發生了異常修改。

Apex One 伺服器

Apex One 伺服器是所有用戶端組態設定、安全威脅記錄檔和更新的中央儲存庫。

伺服器會執行兩項重要功能：

- 安裝、監控和管理 Security Agent
- 下載用戶端所需的大部分元件。Apex One 伺服器會從趨勢科技主動式更新伺服器下載元件，然後分發給用戶端。

注意

某些元件是由主動式雲端截毒伺服器來源下載。如需詳細資訊，請參閱主動雲端截毒伺服器來源 第 4-5 頁。

圖 1-1. Apex One 伺服器的運作方式

Apex One 伺服器能為伺服器和 Security Agent 之間提供即時且雙向的通訊。從網路上幾乎任何一個位置存取 Browser-based Web 主控台，管理員可透過它來管理用戶端。伺服器與用戶端（以及用戶端與伺服器）會透過「超文字安全傳輸通訊協定」(HTTPS) 進行通訊。

Security Agent

在每個端點上安裝 Security Agent 來保護 Windows 端點不受安全威脅的侵襲。

Security Agent 會從它的安裝位置向上層伺服器回報。使用 Agent Mover 工具設定用戶端，讓用戶端向另一部伺服器回報。Security Agent 會即時將事件和狀態資訊傳送給該伺服器。範例事件包括病毒/惡意程式偵測、Security Agent 啟動、Security Agent 關機、掃瞄啟動以及更新完成。

與趨勢科技產品和服務整合

Apex One 會與下表中列出的趨勢科技產品和服務整合。為了達成緊密整合，請確定產品執行的是所需或建議的版本。

表 1-5. 與 Apex One 整合的產品和服務

產品/服務	說明	版本
主動式更新伺服器	提供保護端點不受安全威脅危害的 Security Agent 所需的所有元件	無
主動雲端截毒技術	提供檔案信譽評等服務和網頁信譽評等服務給用戶端。 主動雲端截毒技術是由趨勢科技所代管。	無
獨立式主動雲端截毒技術伺服器	提供主動雲端截毒技術所提供的相同檔案信譽評等服務和網頁信譽評等服務。 獨立式主動雲端截毒技術伺服器主要用途是供客戶在企業網路內執行服務，以最佳化效能。 注意 整合式主動雲端截毒技術伺服器會隨 Apex One 伺服器一起安裝，其功能與整合式主動雲端截毒技術伺服器相同，只是它的容量有限。	• 3.3
Apex Central	一項軟體管理解決方案，讓您能夠從一個集中位置控制防毒和內容安全程式，而不受限於程式的平台或實體位置。	• 任何版本
Trend Micro Control Manager		• 7.0 Patch 1
Deep Discovery Analyzer	Deep Discovery 提供網路範圍內的監控功能，這項功能由自訂沙盒和相關即時智慧驅動，可以提早偵測攻擊、啟用快速包含，並且提供自訂安全性更新，能立即改善保護能力，遏止進一步的攻擊。	5.1 和更新版本

第 2 章

使用 Apex One

本章說明如何開始使用 Trend Micro Apex One 和初始組態設定。

包含下列主題：

Web 主控台

Web 主控台是監控整個企業網路中 Apex One 的中央點。主控台內有一組預設設定和預設值，您可根據這些安全需求和規定設定這些設定和值。Web 主控台使用諸如 JavaScript、CGI、HTML 和 HTTPS 等標準 Internet 技術。

注意

從 Web 主控台設定逾時設定。

如需詳細資訊，請參閱設定 Web 主控台設定值 第 14-53 頁。

可使用 Web 主控台執行下列工作：

- 管理安裝在網路端點上的用戶端
- 將用戶端分組到邏輯網域，以同時進行設定和管理
- 在一或多部網路端點上設定掃瞄設定及開始執行手動掃瞄
- 設定關於網路上安全威脅的通知及檢視由用戶端傳送的記錄檔
- 設定病毒爆發條件和通知
- 透過設定角色和使用者帳號，將 Web 主控台管理工作委派給其他 Apex One 管理員
- 確保用戶端符合安全指導方針

注意

Web 主控台不支援以 Windows UI 模式執行的 Windows 8、8.1、10 或 Windows Server 2012。

開啟 Web 主控台的需求

您可以從網路上具有下列資源的任何端點開啟 Web 主控台：

- 300MHz Intel™ Pentium™ 處理器或同級處理器
- 128MB RAM
- 至少 30MB 可用磁碟空間
- 支援 1366 x 768 解析度（256 色）或以上的顯示器
- Web 瀏覽器支援：
  - Microsoft Internet Explorer™ 10.0 或更新版本
  - Microsoft Edge（舊版及 Chromium 版）
  - Chrome

注意

Apex One 僅支援使用 HTTPS 流量檢視 Web 主控台。

在 Web 瀏覽器上，根據 Apex One 伺服器的安裝類型在網址列輸入下列任一項目：

表 2-1. Apex One Web 主控台 URL

安裝類型	URL
在有 SSL 的預設網站上	`https://<Apex One 伺服器 FQDN 或 IP 位址>/Apex One`
在有 SSL 的虛擬網站上	`https://<Apex One 伺服器 FQDN 或 IP 位址>:<通訊埠號碼>/Apex One`

注意

如果從舊版伺服器升級，Web 瀏覽器和 Proxy 伺服器的快取檔案可能會讓 Apex One Web 主控台無法正常載入。請清除瀏覽器和任何 Proxy 伺服器（位於 Apex One 伺服器與您用來存取 Web 主控台的端點之間）上的快取記憶體。

登入帳號

安裝 Apex One 伺服器期間，安裝程式會建立 root 帳號，並提示您輸入此帳號的密碼。首次開啟 Web 主控台時，請輸入「root」做為使用者名稱，並輸入 root 帳號密碼。如果忘記密碼，請洽詢您的經銷商以協助重設密碼。

定義使用者角色並設定使用者帳號，讓其他使用者不需要使用 root 帳號就可以存取 Web 主控台。當使用者登入主控台時，可以使用您為其設定的使用者帳號。如需詳細資訊，請參閱以角色為基礎的管理 第 14-3 頁。

Web 主控台標題

Web 主控台的標題區域提供下列選項：

- <帳號名稱>：請點選帳號名稱（例如：root）即可修改該帳號的詳細資料（例如：密碼）。
- 登出：讓使用者從 Web 主控台登出

取得說明

「說明」功能表可讓您存取下列支援資訊：

- 目錄與索引：開啟線上說明
- 支援：顯示趨勢科技支援網頁，您可於其中提交問題並找到與趨勢科技產品有關的常見問題的解答
- 安全威脅百科全書：顯示「安全威脅百科全書」網站，它是趨勢科技惡意程式相關資訊的儲存庫。趨勢科技安全威脅專家會定期發佈偵測到的惡意程式、垃圾郵件、惡意 URL 和弱點。「安全威脅百科全書」也會說明備受矚目的 Web 攻擊，並提供相關資訊。
- 聯絡趨勢科技：顯示具有全球辦公室資訊的趨勢科技「與我們聯絡」網站。
- 關於：提供產品的概觀、檢查元件版本詳細資料的說明以及智慧型支援系統的連結。

如需詳細資訊，請參閱智慧型支援系統 第 18-2 頁。

資訊中心

當您開啟 Apex One Web 主控台或請點選主功能表中的「資訊中心」時，會顯示「資訊中心」畫面。

每個 Web 主控台使用者帳號都具有一個完全獨立的資訊中心。對使用者帳號的資訊中心所做的任何變更將不會影響其他使用者帳號的資訊中心。

如果資訊中心包含 Apex One 用戶端資料，顯示的資料取決於使用者帳號的用戶端網域權限。例如，如果授與某個使用者帳號管理網域 A 和 B 的權限，則該使用者帳號的資訊中心將僅顯示來自屬於網域 A 和 B 的用戶端的資料。

如需有關使用者帳號的詳細資訊，請參閱以角色為基礎的管理 第 14-3 頁。

「資訊中心」畫面包含以下內容：

- 「產品使用授權狀態」區段
- Widget
- 標籤

「產品使用授權狀態」區段

本區段位於資訊中心頂端，它會顯示 Apex One 使用授權的狀態。

出現下列情況時顯示有關使用授權狀態的提醒：

- 如果您有完整版使用授權：
  - 授權到期 60 天前
  - 在產品的寬限期內。寬限期視地區而定。請向您的趨勢科技銷售人員確認寬限期。

- 使用授權到期且經過寬限期以後。在這期間，您無法取得技術支援或執行元件更新。掃瞄引擎仍會掃瞄使用過期元件的電腦。這些過期元件可能無法保護您不受最新的安全威脅侵襲。

- 如果您有試用版使用授權：
  - 授權到期 14 天前
  - 使用授權到期時。在此期間，Apex One 會關閉元件更新、掃瞄和所有用戶端功能。

如果您已取得「啟動碼」，請移至「管理 > 設定 > 產品使用授權」續約使用授權。

產品資訊列

Apex One 會在「資訊中心」畫面的頂端顯示各種訊息，以提供額外資訊給管理員。

顯示的資訊包括：

- Apex One 可用的最新 Service Pack 或 Patch

  注意

  按一下「詳細資訊」，以從趨勢科技下載中心下載 Patch(http://downloadcenter.trendmicro.com/?regs=TW; http://www.trendmicro.com/download/zh-tw/default.asp)。

- 可用的新 Widget
- 合約接近到期日時的維護合約通知
- 評估模式通知
- 正版通知

注意

如果用於 Apex One 的使用授權並非正版，將會顯示資訊訊息。如果您未取得正版使用授權，Apex One 會顯示警告並停止執行更新。

標籤和 Widget

Widget 是資訊中心的核心元件。Widget 提供有關各種安全相關事件的特定資訊。透過某些 Widget，您可以執行特定工作，如更新過期的元件。

Widget 顯示以下出處的資訊：

- Apex One 伺服器和 用戶端
- 嵌入程式解決方案及其用戶端
- 趨勢科技主動雲端截毒技術

注意

啟動 Smart Feedback 以顯示來自主動雲端截毒技術的資料。如需 Smart Feedback 的詳細資訊，請參閱 Smart Feedback 第 14-57 頁。

標籤為 Widget 提供了容器。「資訊中心」最多支援 30 個標籤。

使用標籤

透過新增、重新命名、變更配置、刪除以及自動在標籤檢視間切換等動作來管理標籤。

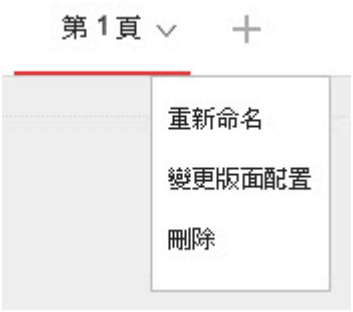
步驟

1. 移至「資訊中心」。
2. 如果要新增標籤：
   a. 請點選新增圖示。

b. 為新標籤輸入名稱。

3. 如果要重新命名標籤：

   a. 將滑鼠游標暫留在標籤名稱上，然後請點選向下箭號。



   b. 請點選「重新命名」，然後輸入新的標籤名稱。

4. 如果要變更標籤上各 Widget 的配置：

   a. 將滑鼠游標暫留在標籤名稱上，然後請點選向下箭號。

   b. 請點選「變更配置」。

   c. 在出現的畫面中選取新的配置。

   d. 請點選「儲存」。

5. 如果要刪除標籤：

   a. 將滑鼠游標暫留在標籤名稱上，然後請點選向下箭號。

   b. 請點選「刪除」並確認。

6. 如果要播放標籤投影片放映：

   a. 請點選標籤顯示右側的「設定」按鈕。

b. 啟動「標籤投影片放映」控制項。

c. 選取在切換到下一個標籤前，每個標籤顯示的時間長度。

使用 Widget

透過新增、移動、調整大小、重新命名和刪除項目等動作來管理 Widget。

步驟

1. 移至「資訊中心」。
2. 請點選某個標籤。
3. 如果要新增 Widget：
   a. 請點選標籤顯示右側的「設定」按鈕。

b. 請點選「新增 Widget」。

c. 選取要新增的 Widget。

- 在 Widget 頂端的下拉式清單，選取類別以縮小選取範圍。
- 使用畫面頂端的搜尋文字方塊可搜尋特定 Widget。

d. 請點選「新增」。

4. 如果要將 Widget 移至同一個標籤上的新位置，請將 Widget 拖放至新位置。

5. 將滑鼠游標指向 Widget 的右邊緣，然後向左或向右移動游標，即可調整多欄標籤上的 Widget 大小。

6. 如果要重新命名 Widget：

a. 點選設定圖示 (>)。

b. 輸入新標題。

> **注意**
>
> 對於某些 Widget（如 Apex One 與嵌入程式混搭技術），您可以修改與 Widget 相關的項目。

c. 請點選「儲存」。

7. 如果要刪除 Widget，請點選刪除圖示 (>)。

摘要標籤 Widget

「摘要」標籤提供您網路上所有 Security Agent 的安全狀態總覽。

注意

您無法新增、刪除或修改「摘要」標籤上顯示的 Widget。

可用的 Widget：

- 整體安全威脅偵測與策略違規 Widget 第 2-11 頁
- 端點狀態 Widget 第 2-13 頁
- 勒索軟體摘要 Widget 第 2-14 頁
- 偵測到的前幾名勒索軟體 Widget 第 2-17 頁
- 歷來的安全威脅偵測 Widget 第 2-18 頁

整體安全威脅偵測與策略違規 Widget

此 Widget 提供過去 24 小時內，在網路中偵測到的所有安全威脅與策略違規的總覽。

將滑鼠游標暫留在安全威脅或違規總數上，可檢視每個群組中特定偵測類型的明細。若要檢視特定特徵的記錄檔，請點選右側的總數。

表 2-2. 偵測類別

類別	說明
已知安全威脅	顯示所有會偵測趨勢科技已確認之安全威脅的特徵 • 病毒/惡意程式 • 間諜程式/可能的資安威脅程式 • 網頁信譽評等
未知安全威脅	顯示所有會使用進階邏輯分析、分析或特徵建模來偵測潛在安全威脅的特徵 • Machine Learning • 行為監控 • 可疑連線 • 可疑檔案物件
策略違規	顯示所有包含您企業安全標準特定策略違規的特徵 • 防火牆 • 周邊設備存取控管 • 資料外洩防護

端點狀態 Widget

此 Widget 會提供您網路上 Security Agent 的連線與更新狀態總覽，以及未向 Apex One 伺服器報告的未受管理端點的最新安全性符合總數。

將滑鼠游標暫留在總數上，可檢視不同狀態的明細。若要檢視特定狀態的記錄檔，請點選右側的總數。

表 2-3. 用戶端/端點群組

群組	說明
受管理的用戶端	顯示上次報告的您網路上 Security Agent 的連線狀態 • 線上 • 離線 • 單機
已過期的用戶端	顯示元件類別清單，以及每個類別中有元件過期的 Security Agent 總數

群組	說明
未受管理的端點	顯示 Apex One 偵測得到，但未安裝 Security Agent 程式或未向 Apex One 伺服器報告之所有端點的清單 **注意** 若要確保 Apex One 伺服器定期更新未受管理端點的總數： 1. 定義要評估的 Active Directory / IP 位址範圍。 如需詳細資訊，請參閱 Active Directory 整合 第 2-31 頁。 2. 設定預約評估。 如需詳細資訊，請參閱適用於未受管端點的安全性符合 第 15-62 頁。

勒索軟體摘要 Widget

圖 2-1. 預設檢視，其中會顯示所有勒索軟體資料，以及「勒索軟體嘗試已偵測到」長條圖的放大檢視

此 Widget 提供指定時間範圍內，所有勒索軟體攻擊嘗試的總覽。

預設檢視會以摘要的形式顯示所有偵測到的勒索軟體嘗試，並根據感染通道將各項嘗試進一步分類。

- 請點選預設檢視上的勒索軟體偵測總數，可開啟「安全威脅 - 勒索軟體」記錄檔畫面，其中會列出勒索軟體偵測詳細資料。

請點選 Widget 右側的任何一個圖表，可顯示圖表資料的放大檢視。

- 將滑鼠游標暫留在任何特定一天的節點上，可檢視所顯示偵測類別的偵測總數。請點選節點可重新導向至「安全威脅 - 勒索軟體」記錄檔畫面，其中會列出那一天的勒索軟體偵測詳細資料。

表 2-4. 勒索軟體偵測通道

通道	說明	偵測者
Web	使用網路用戶端（例如瀏覽器或 FTP 用戶端）下載的檔案	• 網頁信譽評等 • 即時掃瞄 • 行為監控
網路流量	「可疑連線」功能偵測到的勒索軟體	• 可疑連線
雲端同步	使用下列受支援的雲端儲存服務，可以將檔案同步到本機同步資料夾： • Microsoft™ OneDrive™	• 即時掃瞄 • 行為監控 • Machine Learning
電子郵件	使用 Microsoft Outlook 開啟的電子郵件附件 **注意** Apex One 會將所有使用其他電子郵件用戶端應用程式開啟的附件分類在本機或網路磁碟機通道中。	• 即時掃瞄 • 行為監控
自動執行檔案	位於卸除式存放磁碟機上並由自動執行檔案執行的程式 **注意** Apex One 會將所有其他並非由卸除式儲存裝置上的自動執行程式執行的檔案/程式，分類在本機或網路磁碟機通道中。	• 即時掃瞄 • 行為監控

通道	說明	偵測者
本機或網路磁碟機	在本機或網路磁碟機上偵測到的勒索軟體包括： • 使用 Microsoft Outlook 以外的電子郵件用戶端開啟的電子郵件附件 • 卸除式儲存裝置上並非由自動執行檔案執行的檔案	• 即時掃瞄 • 手動掃瞄 • 預約掃瞄 • 立即掃瞄 • 行為監控

安全威脅 - 勒索軟體記錄檔

安全威脅 - 勒索軟體記錄檔提供了在您網路上偵測到的所有勒索軟體安全威脅總覽，不管偵測到這些安全威脅的掃瞄類型如何。

項目	說明
日期/時間	發生偵測的時間
安全威脅	安全威脅的名稱
類別	偵測到安全威脅的掃瞄類型
檔案路徑/URL	偵測到安全威脅的位置或用於偵測惡意網站的清單
處理行動	對安全威脅採取的處理行動
感染通道	安全威脅源自的通道
端點	發生偵測的端點

偵測到的前幾名勒索軟體 Widget

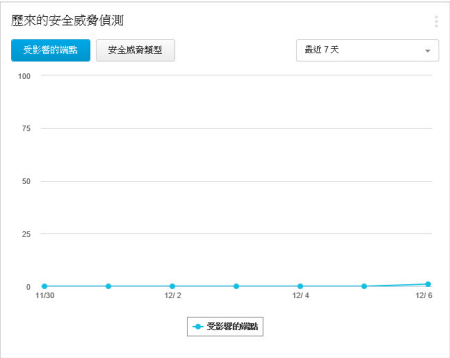
此 Widget 提供指定時間範圍內，偵測到的前幾名勒索軟體的總覽。

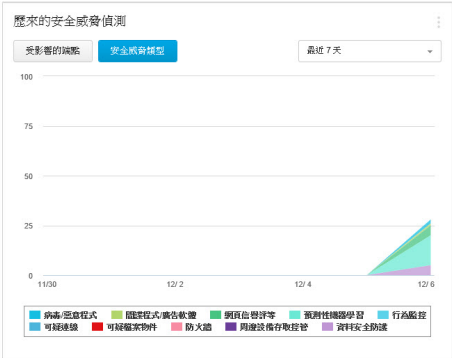
使用下拉式清單，選取要顯示的勒索軟體資料類型。

檢視	說明
端點	顯示您網路上偵測到最多勒索軟體的端點 請點選勒索軟體偵測總數，可開啟「安全威脅 - 勒索軟體」記錄檔畫面，其中會列出勒索軟體偵測詳細資料。
勒索軟體類型	顯示您網路上偵測到最多次的勒索軟體類型 如需有關特定安全威脅類型的進一步資訊，請點選「安全威脅名稱」連結，以開啟趨勢科技安全威脅百科全書。

檢視	說明
網域	顯示您網路上偵測到最多次的勒索軟體網域 如需有關特定網域的進一步資訊，請點選「安全威脅名稱」連結，以開啟趨勢科技安全威脅百科全書。

歷來的安全威脅偵測 Widget





此 Widget 提供指定時間範圍內，您網路上端點的總覽，包括偵測到的安全威脅，以及對您網路造成影響的安全威脅類型。

請點選「受影響的端點」或「安全威脅類型」按鈕，即可在不同的檢視間切換。

檢視	說明
受影響的端點	顯示指定時間範圍內，偵測到安全威脅或策略違規的端點每日趨勢

檢視	說明
安全威脅類型	顯示圖形來概述在指定時間範圍內，記錄的安全威脅與策略違規數目 • 請點選圖形底部的安全威脅類型名稱，可在圖形上顯示/隱藏偵測資訊。 • 將滑鼠游標暫留在任何特定一天的節點上，可檢視所顯示安全威脅類型的偵測總數。請點選節點，重新導向至記錄檔畫面，可查看清單中反白顯示的安全威脅類型。

秘訣

您可以新增此 Widget 多次來同時顯示這兩個檢視。

資料安全防護 Widget

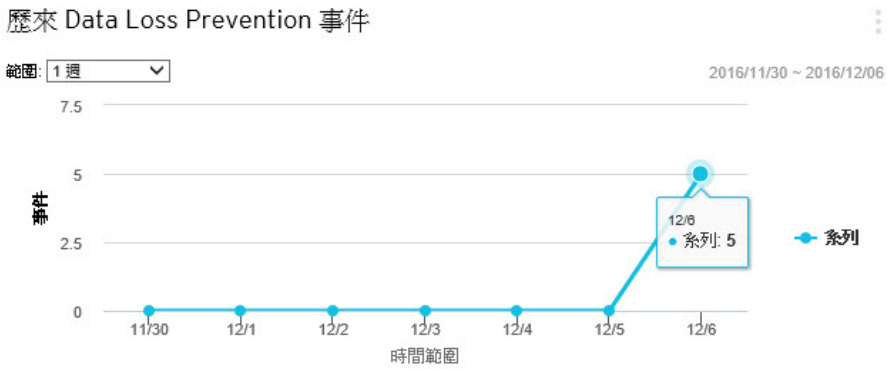
注意

啟動 Apex One 資料安全防護之後，即可使用資料安全防護 Widget。

可用的 Widget：

- 歷來資料外洩防護事件 Widget 第 2-20 頁
- 最常見的資料外洩防護事件 Widget 第 2-21 頁

歷來資料外洩防護事件 **Widget**

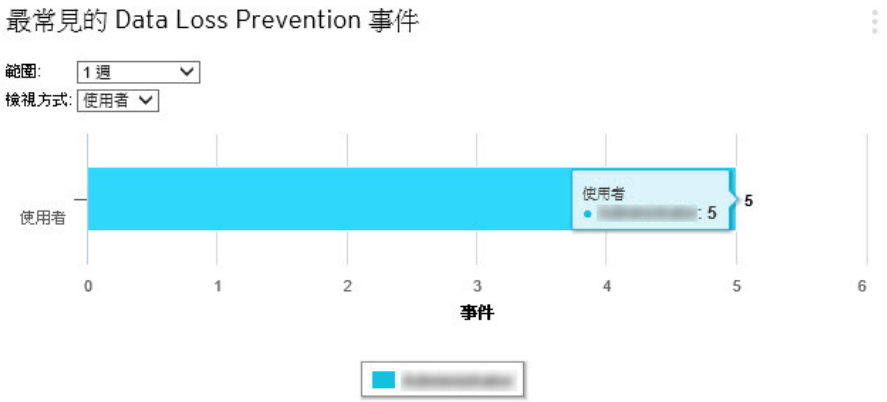


此 Widget 顯示特定時間範圍的資料外洩防護事件總數。

注意

此偵測項目包含所有資料外洩防護事件，而無論當下採取的處理行動（「封鎖」或「暫不處理」）為何。

最常見的資料外洩防護事件 **Widget**



此 Widget 顯示指定時間範圍內觸發資料外洩防護事件最多的使用者、通道、範本或端點。

注意

- 此 Widget 最多顯示 10 個使用者、通道、範本或端點。
- 此偵測項目包含所有資料外洩防護事件，而無論當下採取的處理行動（「封鎖」或「暫不處理」）為何。

使用「檢視方式」下拉式清單，選取顯示的資料外洩防護資料類型：

表 2-5. 資料外洩防護檢視

檢視	說明
使用者	傳輸數位資產數目最多的使用者 • 請點選圖形底部的使用者名稱，可在圖形上顯示/隱藏偵測資訊。 • 將滑鼠游標暫留在偵測列上，可檢視使用者名稱和該使用者的資料外洩防護事件數目。
通道	最常用於傳輸數位資產的通道 • 請點選圖形底部的通道名稱，可在圖形上顯示/隱藏偵測資訊。 • 將滑鼠游標暫留在偵測列上，可檢視通道名稱和該通道的資料外洩防護事件數目。
範本	觸發最多偵測的數位資產範本 • 請點選圖形底部的範本名稱，可在圖形上顯示/隱藏偵測資訊。 • 將滑鼠游標暫留在偵測列上，可檢視範本名稱和該範本的資料外洩防護事件數目。
端點	傳輸數位資產數目最多的端點 • 請點選圖形底部的端點名稱，可在圖形上顯示/隱藏偵測資訊。 • 將滑鼠游標暫留在偵測列上，可檢視端點名稱和該端點的資料外洩防護事件數目。

Apex One Widget

Apex One Widget 提供有關 Security Agent 安全狀態與偵測、嵌入程式資訊以及病毒爆發事件的快速參考。

可用的 Widget：

- C&C 回呼事件 Widget 第 2-23 頁

C&C 回呼事件 **Widget**

此 Widget 會顯示所有 C&C 回呼事件資訊，包括攻擊目標和來源回呼位址。

您可以選擇從特定 C&C 伺服器清單檢視 C&C 回呼資訊。如果要選取清單來源（全球資訊、沙箱），請點選編輯圖示 (>)，然後從「C&C 清單來源」下拉式清單中選取清單。

使用「檢視方式」下拉式清單，選取顯示的 C&C 回呼資料類型：

- 遭到入侵的主機：針對每個目標端點，顯示最新 C&C 資訊

  表 2-6. 遭到入侵的主機資訊

欄	說明
遭到入侵的主機	C&C 攻擊的目標端點名稱

欄	說明
回呼位址	端點嘗試聯絡的回呼位址數目
最新回呼位址	端點嘗試聯絡的最後一個回呼位址
回呼嘗試次數	目標端點嘗試聯絡回呼位址的次數 注意 請點選超連結以開啟「C&C 回呼記錄檔」畫面，並檢視更多詳細資訊。

- 回呼位址：針對每個 C&C 回呼位址，顯示最新 C&C 資訊

表 2-7. C&C 位址資訊

欄	說明
回呼位址	來自網路的 C&C 回呼位址
C&C 風險等級	由全球智慧或沙箱清單所判定的回呼位址風險等級
遭到入侵的主機	回呼位址的目標端點數目
最新遭到入侵的主機	最後一次嘗試聯絡 C&C 回呼位址的端點名稱
回呼嘗試次數	從網路對位址進行的回呼嘗試次數 注意 請點選超連結以開啟「C&C 回呼記錄檔」畫面，並檢視更多詳細資訊。

安全威脅偵測 **Widget**

此 Widget 會顯示偵測到的安全威脅數目，以及受影響的端點數目。

請點選端點總數，可開啟「用戶端管理」畫面，其中會以用戶端樹狀結構列出受影響的 Security Agent。

Apex One 與嵌入程式混搭技術 **Widget**

此 Widget 會將 Security Agent 中的資料和已安裝的嵌入程式中的資料結合，然後在用戶端樹狀結構中顯示資料。此 Widget 有助於快速評估用戶端上的防護範圍，並減少管理個別嵌入程式所需的管理費用。

此 Widget 會顯示下列嵌入程式的資料：

- 趨勢科技虛擬桌面支援

重要

您必須先啟動支援的嵌入程式，混搭 Widget 才能顯示對應的資料。如果有更新版本可用，則升級嵌入程式。

如果要選取用戶端樹狀結構中所顯示的欄，請按一下 Widget 右上角的「更多選項」按鈕，然後按一下「Widget 設定」按鈕。

請點選任何一欄下的資料，即會開啟對應的嵌入程式主控台或是 Apex One 的「用戶端管理」畫面。所顯示的畫面視您按下的資料類型而定。

防毒用戶端連線能力 **Widget**

圖 2-2. 顯示所有雲端截毒掃瞄與標準掃瞄用戶端的預設檢視，以及展開的主動雲端截毒技術伺服器之雲端截毒掃瞄用戶端檢視

此 Widget 會顯示所設定掃瞄方法（「雲端截毒掃瞄」和「標準掃瞄」）下，Security Agent 與 Apex One 伺服器之間的連線狀態。

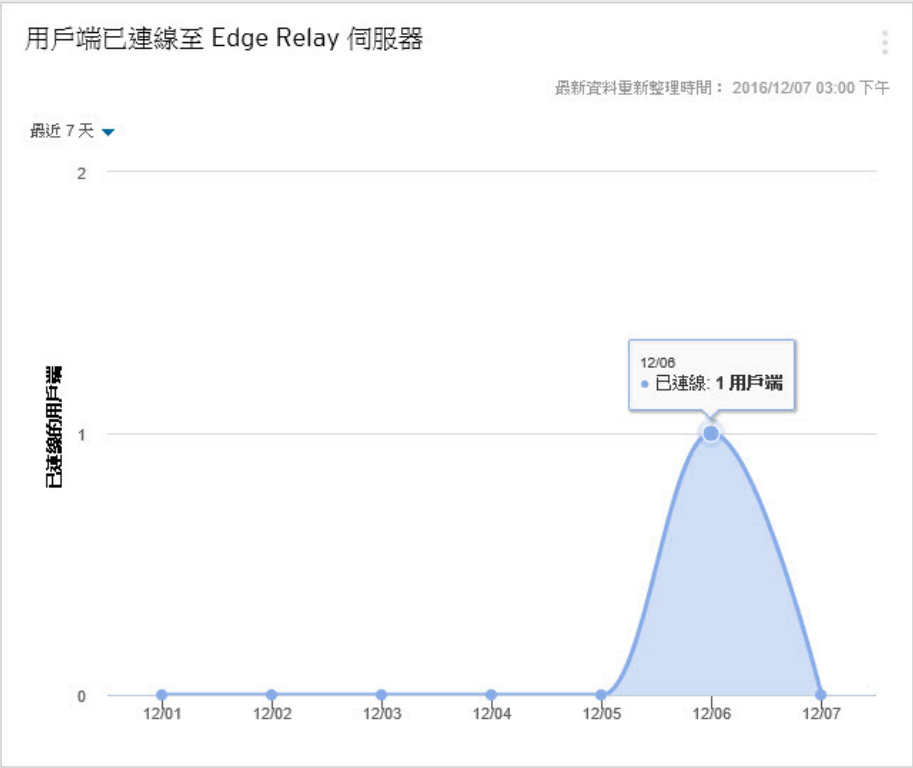
請點選顯示圖示 ( )，可選擇要以表格還是圓餅圖顯示資料。

使用表格/圖形上方的下拉式清單，可變更顯示的資料類型。請點選任何狀態的計數，可開啟「用戶端管理」畫面，其中會以用戶端樹狀結構列出相關的 Security Agent。

檢視	說明
所有	同時顯示這兩種掃瞄方法下所有 Security Agent 的連線狀態
標準掃瞄	顯示所有使用標準掃瞄方法的 Security Agent 的連線狀態

檢視	說明
雲端截毒掃瞄	顯示所有使用雲端截毒掃瞄方法的 Security Agent 的連線狀態 以表格檢視用戶端連線狀態時： • 展開「線上」用戶端資訊，可檢視用戶端與主動雲端截毒技術伺服器的連線狀態。 • 請點選 URL，可開啟主動雲端截毒技術伺服器管理主控台。 注意 只有線上用戶端（向 Apex One 伺服器報告）可以報告自己與主動雲端截毒技術伺服器的連線狀態。 若要讓離線用戶端恢復與主動雲端截毒技術伺服器的連線，請參閱 Security Agent 圖示所指示問題的解決方案 第 15-34 頁。

用戶端已連線至 Edge Relay 伺服器 Widget



此 Widget 會顯示特定時間範圍內連線到 Apex One Edge Relay 伺服器的 Security Agent 數目。

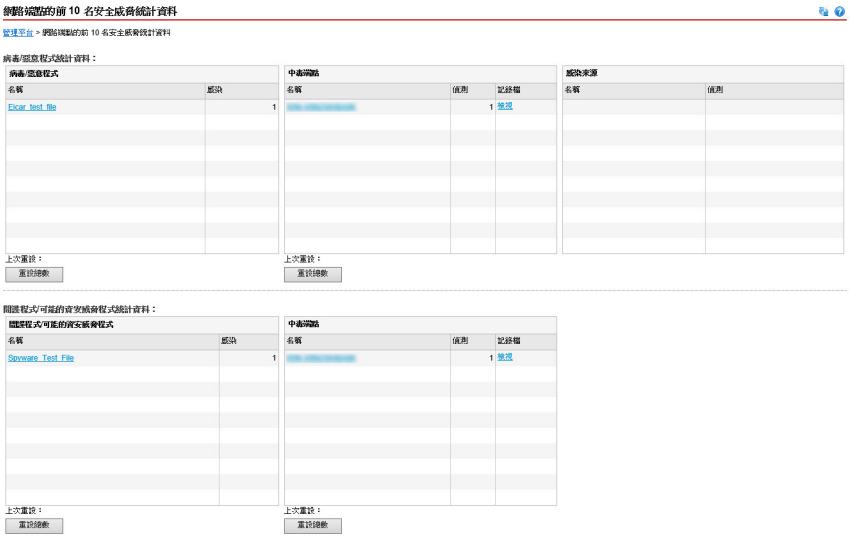
病毒爆發 Widget

病毒爆發 Widget 提供任何最新安全威脅病毒爆發的狀態和上次病毒爆發警訊。

- 請點選警訊的日期/時間連結，可檢視更多有關病毒爆發的詳細資料。
- 重設病毒爆發警訊狀態資訊，並在 Apex One 偵測到病毒爆發時立即採取病毒爆發防範措施。

  如需實施病毒爆發防範措施的詳細資訊，請參閱病毒爆發防範策略 第 7-97 頁。

- 請點選「檢視前 10 名安全威脅統計資料」，可檢視最常見的安全威脅、安全威脅數量最多的端點和主要的感染來源。



在「前 10 名安全威脅統計資料」畫面中，您可以：

- 請點選安全威脅名稱檢視安全威脅的詳細資訊。
- 請點選端點名稱檢視特定端點的整體狀態。
- 請點選與端點名稱對應的「檢視」，檢視端點的安全威脅記錄檔。
- 請點選「重設計數」重設各資料表內的統計資料。

用戶端更新 **Widget**

此 Widget 會顯示可保護 Security Agent 免於安全威脅的元件和程式。

請點選「已過期」計數，則會開啟「用戶端管理」畫面，其中會以用戶端樹狀結構列出需要更新的 Security Agent。

管理 Widget

管理 Widget 會顯示 Security Agent 與 Apex One 伺服器之間的連線狀態。

可用的 Widget：

- 用戶端與伺服器之間的連線能力 Widget 第 2-31 頁

用戶端與伺服器之間的連線能力 Widget

此 Widget 會顯示所有用戶端與 Apex One 伺服器之間的連線狀態。

您可以以請點選圖示（在表格和圓形圖之間切換）。

請點選任何狀態的計數，可開啟「用戶端管理」畫面，其中會以用戶端樹狀結構列出相關的 Security Agent。

Active Directory 整合

整合 Apex One 與您的 Microsoft™ Active Directory™ 結構，讓您更有效率地管理 Security Agent、使用 Active Directory 帳號指派 Web 主控台權限，以及

確定哪些用戶端未安裝安全防護軟體。網路網域中所有的使用者都可以安全存取 Apex One 主控台。您也可以針對特定使用者（甚至是在另一個網域中的使用者）設定有限制的存取。驗證程序和加密金鑰會提供使用者認證的驗證。

Active Directory 整合可讓您充分利用下列功能：

- 自訂用戶端群組：使用 Active Directory 或 IP 位址，以手動方式將用戶端分組，然後將它們對應到 Apex One 用戶端樹狀結構中的網域。

  如需詳細資訊，請參閱自動用戶端分組 第 2-50 頁。

- 未受管理的端點：確保位於網路中但不受 Apex One 伺服器管理的端點都符合公司的安全指導方針。

  如需詳細資訊，請參閱適用於未受管端點的安全性符合 第 15-62 頁。

手動或定期同步處理 Active Directory 結構與 Apex One 伺服器，以確保資料一致性。

如需詳細資訊，請參閱同步處理資料與 Active Directory 網域 第 2-34 頁。

將 Active Directory 與 Apex One 整合

步驟

1. 移至「管理 > Active Directory > Active Directory 整合」。
2. 在「Active Directory 網域」下指定 Active Directory 網域名稱。
3. 指定同步處理資料與指定的 Active Directory 網域時，Apex One 伺服器將使用的認證。如果伺服器不屬於網域，將需要使用認證。否則，該認證為選用項目。請確認這些認證並未過期，否則伺服器將無法同步處理資料。

   a. 請點選「指定網域認證」。

   b. 在開啟的快顯視窗中，輸入使用者名稱和密碼。您可以使用下列任一種格式指定使用者名稱：

      - 網域\使用者名稱

- 使用者名稱@網域

c. 請點選「儲存」。

4. 請點選 (+) 按鈕新增更多網域。如有必要，請指定網域認證給任何新增的網域。

5. 請點選 (-) 按鈕刪除網域。

6. 如果您指定了網域認證，請指定加密設定。基於安全性考量，Apex One 會先加密您指定的網域認證，再將其儲存到資料庫。當 Apex One 同步處理資料與任何指定的網域時，它會使用加密金鑰來解密網域認證。

   a. 移至「網域認證的加密設定」區段。

   b. 請輸入不超過 128 個字元的加密金鑰。

   c. 指定用於儲存加密金鑰的檔案。您可以選擇使用常見的檔案格式，例如 `.txt`。輸入檔案的完整路徑和名稱（例如：`C:\AD_Encryption\EncryptionKey.txt`）。

警告!

如果檔案已移除或路徑已變更，Apex One 將無法同步處理資料與所有指定的網域。

7. 請點選下列其中一個項目：

   - 儲存：僅儲存設定。由於同步處理資料會使用大量的網路資源，您可以選擇僅儲存設定並於稍後（例如，非忙碌的上班時間）進行同步處理。

   - 存儲和同步處理：儲存設定並同步處理資料與 Active Directory 網域。

8. 預約定期同步處理。如需詳細資訊，請參閱同步處理資料與 Active Directory 網域 第 2-34 頁。

同步處理資料與 Active Directory 網域

定期與 Active Directory 網域同步處理資料，可讓 Apex One 用戶端樹狀結構保持最新狀態並查詢未受管理的用戶端。

手動同步處理資料與 Active Directory 網域

步驟

1. 移至「管理 > Active Directory > Active Directory 整合」。
2. 確認網域認證與加密設定並未變更。
3. 請點選「存儲並同步處理」。

自動同步處理資料與 Active Directory 網域

步驟

1. 移至「管理 > Active Directory > 預約同步處理」。
2. 選取「啟動預約 Active Directory 同步處理」。
3. 指定同步處理預約時程。

   注意

   如果是每日、每週和每月同步處理，則期間是指 Apex One 同步處理 Apex One 伺服器與 Active Directory 的時數。

4. 請點選「儲存」。

Apex One 用戶端樹狀結構

Apex One 用戶端樹狀結構會顯示分組到伺服器目前管理之網域的所有用戶端。將用戶端分組到網域中，您就可以同時設定、管理和套用相同組態設定至所有網域成員。

用戶端連線狀態

Security Agent 連線狀態視 Apex One 伺服器與 Security Agent 通訊的方式而定。下表簡述 Security Agent 可能存在的不同連線狀態。

表 2-8. Office 用戶端連線狀態

狀態	說明
線上	Security Agent 可以針對下列項目，與 Apex One 伺服器連線來進行雙向通訊： • 策略設定 • 更新 • 掃瞄命令 • 可疑物件清單同步處理 • 樣本提交 • 記錄檔提交
離線	Security Agent 與 Apex One 伺服器或 Edge Relay 伺服器之間沒有正常運作的連線。

狀態	說明
單機	Security Agent 可以與伺服器連線，但通訊受限。在單機模式下： • Security Agent 不會從伺服器接受策略設定 • Security Agent 不會從伺服器開始掃瞄命令 • Security Agent 不會傳送記錄檔給伺服器 您可以為「單機」用戶端設定權限，使其能夠在與 Apex One 伺服器之間有正常運作的連線時，允許或封鎖元件更新。 使用者可以在單機模式下的用戶端上，手動開始掃瞄和更新。
外部部署	Security Agent 位於企業網路外，無法直接與 Apex One 伺服器連線。不過，Security Agent 可以針對下列項目，與 Edge Relay 伺服器連線： • 可疑物件清單同步處理 • 樣本提交 • 記錄檔提交 注意 外部部署用戶端的連線狀態在用戶端樹狀結構中顯示為「離線」，“”因為 Apex One 伺服器未與 Security Agent 直接連線。

用戶端樹狀結構圖示

Apex One 用戶端樹狀結構圖示提供視覺提示，指出 Apex One 所管理之端點的類型和 Security Agent 的狀態。

表 2-9. Apex One 用戶端樹狀結構圖示

圖示	說明
	網域

圖示	說明
	根目錄
	更新代理程式
	標準掃瞄用戶端
	雲端截毒掃瞄可用的 Security Agent
	雲端截毒掃瞄不可用的 Security Agent
	雲端截毒掃瞄可用的更新代理程式
	雲端截毒掃瞄不可用的更新代理程式

搜尋用戶端樹狀結構

使用用戶端樹狀結構（用戶端 > 用戶端管理）上方的搜尋和檢視功能，可以尋找受 Apex One　管理的特定端點。

步驟

- 請在「搜尋端點」文字方塊中指定用戶端名稱，以搜尋要管理的任何用戶端。

  結果清單會顯示在用戶端樹狀結構中。如需更多搜尋選項，請點選「進階搜尋」。

注意

您必須利用「進階搜尋」功能來尋找使用 IPv4 或 IPv6 位址的端點。

如需詳細資訊，請參閱進階搜尋選項 第 2-38 頁。

- 選取網域後，用戶端樹狀結構表格會展開，以顯示屬於該網域的用戶端和包含每個用戶端相關資訊的所有欄位。如果只要檢視一組相關欄位，請在用戶端樹狀結構檢視中選取一個項目。
  - 檢視全部：顯示所有欄位
  - 更新檢視：顯示所有元件和程式
  - 防毒檢視：顯示防毒元件
  - 間諜程式防護檢視：顯示間諜程式防護元件
  - 資料安全防護檢視：顯示用戶端上「資料安全防護」模組的狀態
  - 防火牆檢視：顯示防火牆元件
  - 主動雲端截毒技術檢視：顯示用戶端（標準或雲端截毒掃瞄）所使用的掃瞄方法和雲端防護元件
  - 更新代理程式檢視：顯示受 Apex One 伺服器管理的所有更新代理程式的資訊
  - 外部部署用戶端檢視：顯示向 Edge Relay 伺服器報告的所有用戶端的資訊

進階搜尋選項

根據下列條件搜尋用戶端：

區段	說明
基本條件	包含端點的基本資訊，例如，IP 位址、作業系統、網域、MAC 位址、掃瞄方法和網頁信譽評等狀態 • 依 IPv4 網段搜尋需要部分 IP 位址（開頭為首個八位元組）。搜尋會傳回 IP 位址中包含該項目的所有端點。例如，輸入 10.5 會傳回 IP 位址範圍從 10.5.0.0 到 10.5.255.255 的所有電腦。 • 依 IPv6 位址範圍搜尋時，會要求字首和長度。 • 依 MAC 位址搜尋需要以十六進位標記表示的 MAC 位址範圍，例如：000A1B123C12。
元件版本	選取元件名稱旁邊的核取方塊，選取「低於」或「低於（含）」並輸入版本號碼來縮小條件。根據預設會顯示目前版本號碼。
狀態	包含用戶端設定

指定搜尋條件之後，請點選「搜尋」。用戶端樹狀結構中會顯示符合條件的端點名稱清單。

用戶端樹狀結構特定工作

當您存取 Web 主控台上的特定畫面時，會顯示用戶端樹狀結構。用戶端樹狀結構上方是功能表項目，功能表項目視您存取的畫面而異。這些功能表項目可讓您執行特定工作，例如設定用戶端設定或開始用戶端工作。如果要執行其中任何工作，請選取工作目標，再選取功能表項目。

下列畫面顯示用戶端樹狀結構：

- 用戶端管理畫面 第 2-40 頁
- 病毒爆發防範 畫面 第 2-44 頁
- 用戶端選項畫面 第 2-44 頁
- 還原畫面 第 2-45 頁
- 安全威脅記錄檔 畫面 第 2-46 頁

用戶端管理畫面

如果要檢視此畫面，請移至「用戶端 > 用戶端管理」。

在「用戶端管理」畫面上，管理一般用戶端設定並檢視有關特定用戶端的狀態資訊（例如，「登入使用者」、「IP 位址」和「連線狀態」。

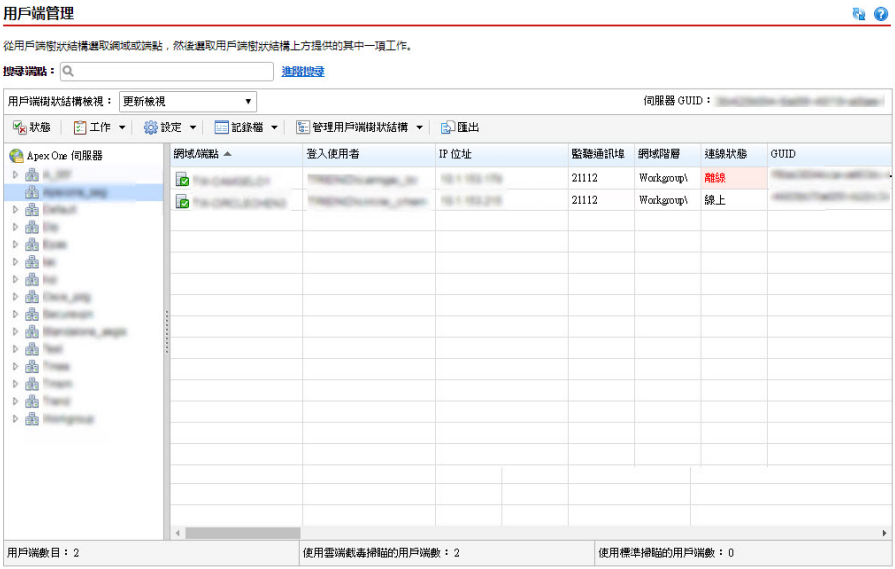


圖 2-3. 用戶端管理畫面

下表列出了您可以執行的工作：

表 2-10. 用戶端管理工作

功能表按鈕	工作
狀態	檢視詳細的用戶端資訊。如需詳細資訊，請參閱檢視 Security Agent 資訊 第 15-48 頁。

功能表按鈕	工作
工作	• 在用戶端端點上執行「立即掃瞄」。如需詳細資訊，請參閱開始立即掃瞄 第 7-21 頁。 • 解除安裝用戶端。如需詳細資訊，請參閱從 Web 主控台解除安裝 Security Agent 第 5-56 頁。 • 恢復偵測到的可疑檔案。如需詳細資訊，請參閱恢復隔離的檔案 第 7-38 頁。 • 恢復間諜程式/可能的資安威脅程式元件。如需詳細資訊，請參閱回存間諜程式/可能的資安威脅程式 第 7-46 頁。

功能表按鈕	工作

設定	• 設定掃瞄設定。如需詳細資訊，請參閱下列主題：
	  • 掃瞄方法類型 第 7-7 頁
	  • 手動掃瞄 第 7-15 頁
	  • 即時掃瞄 第 7-12 頁
	  • 預約掃瞄 第 7-17 頁
	  • 立即掃瞄 第 7-19 頁
	• 設定網頁信譽評等設定。如需詳細資訊，請參閱網頁信譽評等策略 第 12-4 頁。
	• 設定 Machine Learning 設定。如需詳細資訊，請參閱設定 Machine Learning 設定 第 8-3 頁。
	• 設定可疑連線設定。如需詳細資訊，請參閱設定可疑連線設定 第 8-7 頁。
	• 設定行為監控設定。如需詳細資訊，請參閱行為監控 第 9-2 頁。
	• 設定周邊設備存取控管設定。如需詳細資訊，請參閱周邊設備存取控管 第 10-2 頁。
	• 設定資料外洩防護策略。如需詳細資訊，請參閱資料外洩防護策略組態設定 第 11-43 頁。
	• 設定樣本提交設定。如需詳細資訊，請參閱設定樣本提交 第 8-9 頁。
	• 將用戶端指定為「更新代理程式」。如需詳細資訊，請參閱更新代理程式組態設定 第 6-49 頁。
	• 設定用戶端權限和其他設定。如需詳細資訊，請參閱設定用戶端權限及其他設定 第 15-84 頁。
	• 啟動或關閉 Security Agent 服務。如需詳細資訊，請參閱 Security Agent 服務 第 15-6 頁。
	• 間諜程式/可能的資安威脅程式核可清單。如需詳細資訊，請參閱間諜程式/可能的資安威脅程式核可清單 第 7-44 頁。
	• 設定信任的程式清單。如需詳細資訊，請參閱設定信任的程式清單 第 7-48 頁。
	• 匯入和匯出用戶端設定。如需詳細資訊，請參閱匯入和匯出用戶端設定 第 15-48 頁。

功能表按鈕	工作
記錄檔	檢視下列記錄檔： • 病毒/惡意程式記錄檔（如需詳細資訊，請參閱檢視病毒/惡意程式記錄檔 第 7-79 頁） • 間諜程式/可能的資安威脅程式記錄檔（如需詳細資訊，請參閱檢視間諜程式/可能的資安威脅程式記錄檔 第 7-86 頁） • 防火牆記錄檔（如需詳細資訊，請參閱防火牆記錄檔 第 13-25 頁） • 網頁信譽評等記錄檔（如需詳細資訊，請參閱網路安全威脅記錄檔 第 12-18 頁） • 可疑連線記錄檔（如需詳細資訊，請參閱檢視可疑連線記錄檔 第 8-13 頁） • 可疑檔案記錄檔（如需詳細資訊，請參閱檢視可疑檔案記錄檔 第 7-90 頁） • C&C 回呼記錄檔（如需詳細資訊，請參閱檢視 C&C 回呼記錄檔 第 12-20 頁。） • 行為監控記錄檔（如需詳細資訊，請參閱行為監控記錄檔 第 9-19 頁） • Machine Learning 記錄檔（如需詳細資訊，請參閱檢視 Machine Learning 記錄檔 第 8-10 頁） • 周邊設備存取控管記錄檔（如需詳細資訊，請參閱周邊設備存取控管記錄檔 第 10-17 頁） • DLP 記錄檔（如需詳細資訊，請參閱資料外洩防護記錄檔 第 11-52 頁） • 掃瞄作業記錄檔（如需詳細資訊，請參閱檢視掃瞄作業記錄檔 第 7-91 頁） 刪除記錄檔。如需詳細資訊，請參閱記錄檔管理 第 14-39 頁。
管理用戶端樹狀結構	管理用戶端樹狀結構。如需詳細資訊，請參閱用戶端分組工作 第 2-54 頁。
匯出	將用戶端清單匯出到逗號分隔值 (.csv) 檔案。

病毒爆發防範 畫面

如果要檢視此畫面，請移至「用戶端 > 病毒爆發防範」。

在「病毒爆發防範」畫面中指定並啟動病毒爆發防範設定。如需詳細資訊，請參閱設定安全威脅爆發防範 第 7-96 頁。

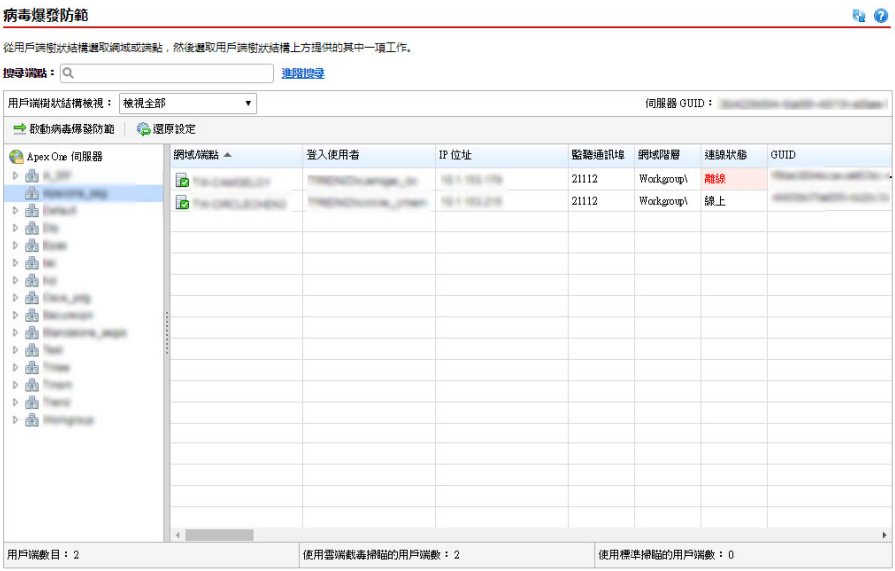


圖 2-4. 病毒爆發防範 畫面

用戶端選項畫面

如果要檢視此畫面，請移至「更新 > 用戶端 > 手動更新」。選取「手動選取用戶端」，然後請點選「選取」。

在「用戶端選項」畫面中，開始手動更新。如需詳細資訊，請參閱 Security Agent 手動更新 第 6-40 頁。

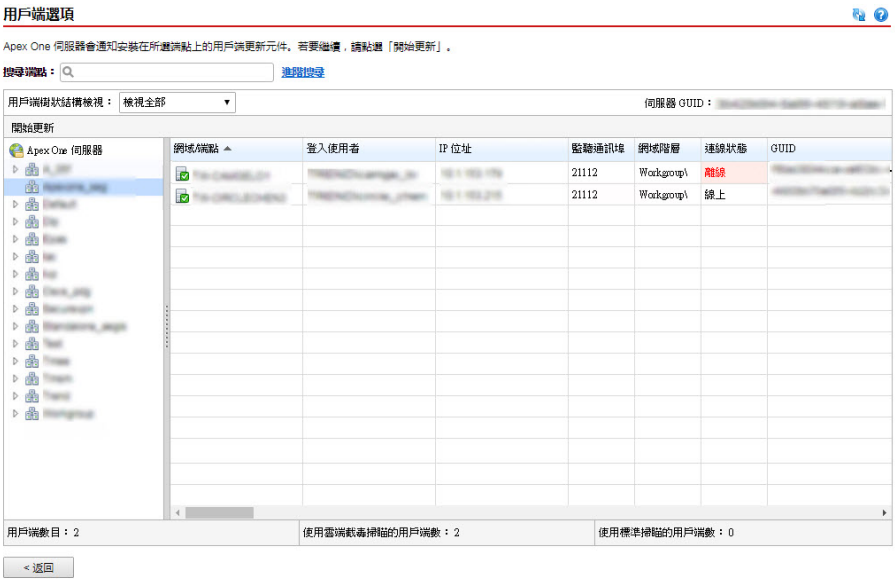


圖 2-5. 用戶端選項畫面

還原畫面

如果要檢視此畫面，請移至「更新 > 還原」。請點選「同步處理伺服器」。

在「還原」畫面中還原用戶端元件。如需詳細資訊，請參閱還原 Security Agent 的元件 第 6-47 頁。

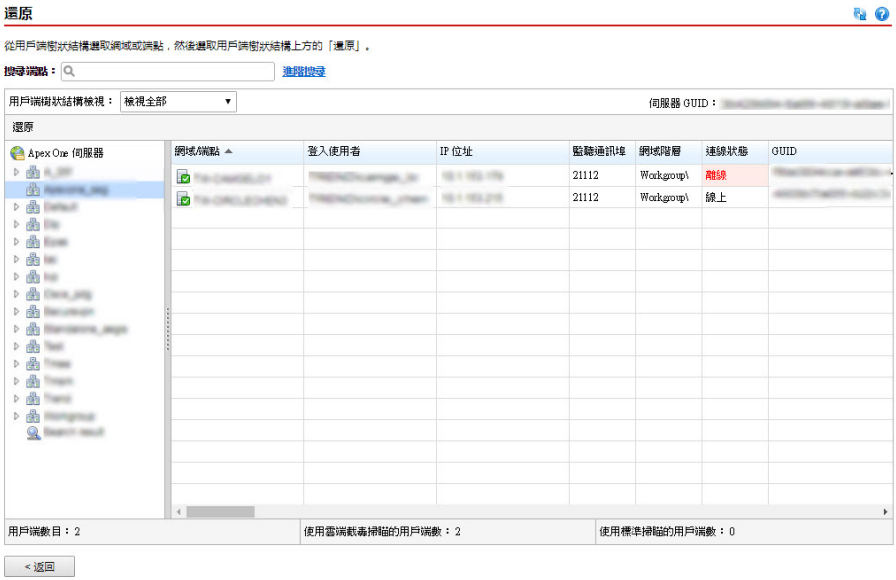


圖 2-6. 還原畫面

安全威脅記錄檔 畫面

如果要檢視此畫面，請移至「記錄檔 > 用戶端 > 安全威脅」。

在「安全威脅記錄檔」畫面中檢視和管理記錄檔。

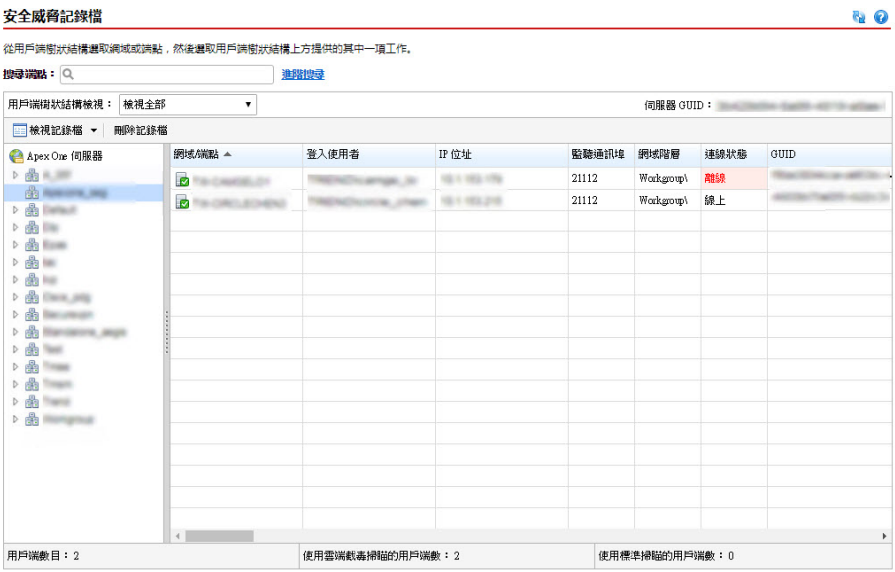


圖 2-7. 安全威脅記錄檔 畫面

執行下列工作：

1. 檢視用戶端傳送至伺服器的記錄檔。如需詳細資訊，請參閱：
   - 檢視病毒/惡意程式記錄檔 第 7-79 頁
   - 檢視間諜程式/可能的資安威脅程式記錄檔 第 7-86 頁
   - 檢視防火牆記錄檔 第 13-26 頁
   - 檢視網頁信譽評等記錄檔 第 12-19 頁
   - 檢視可疑連線記錄檔 第 8-13 頁
   - 檢視可疑檔案記錄檔 第 7-90 頁
   - 檢視 C&C 回呼記錄檔 第 12-20 頁

- 檢視行為監控記錄檔 第 9-19 頁
- 檢視 Machine Learning 記錄檔 第 8-10 頁
- 檢視周邊設備存取控管記錄檔 第 10-17 頁
- 檢視資料外洩防護記錄檔 第 11-52 頁
- 檢視掃瞄作業記錄檔 第 7-91 頁

2. 刪除記錄檔。如需詳細資訊，請參閱記錄檔管理 第 14-39 頁。

Apex One 網域

Apex One 中的網域是一組擁有相同組態設定並執行相同工作的用戶端。透過將用戶端分組到網域中，您可以設定、管理和套用相同組態設定至所有網域成員。

如需有關用戶端分組的詳細資訊，請參閱用戶端分組 第 2-48 頁。

用戶端分組

使用「用戶端分組」，以手動或自動方式建立及管理 Apex One 用戶端樹狀結構中的網域。

有兩種方法可將 Security Agent 歸入網域中。

表 2-11. 用戶端分組方法

方法	用戶端分組	說明
手動	• NetBIOS 網域 • Active Directory 網域 • DNS 網域	手動用戶端分組會定義新安裝的用戶端應屬於哪一個網域。當該用戶端顯示在用戶端樹狀結構中時，您可以將其移至其他網域或其他 Apex One 伺服器。 透過手動用戶端分組，還可以在用戶端樹狀結構中建立、管理和移除網域。 如需詳細資訊，請參閱手動用戶端分組 第 2-49 頁。

方法	用戶端分組	說明
自動	自訂用戶端群組	自動用戶端分組會使用規則來排序用戶端樹狀結構中的用戶端。定義規則之後，您可以存取用戶端樹狀結構來手動排序用戶端，或允許 Apex One 在發生特定事件時自動排序用戶端。 如需詳細資訊，請參閱自動用戶端分組 第 2-50 頁。

手動用戶端分組

Apex One 只有在全新的用戶端安裝期間才會使用此設定。安裝程式會檢查目標端點所屬的網路網域。如果網域名稱已存在於用戶端樹狀結構中，則 Apex One 會將目標端點上的用戶端分組到該網域下，而且會套用針對該網域所設定的設定。如果該網域名稱不存在，Apex One 會將該網域新增到用戶端樹狀結構，將該用戶端分組在該網域下，然後將根設定套用至該網域和用戶端。

設定手動用戶端分組

步驟

1. 移至「用戶端 > 用戶端分組」。
2. 指定用戶端分組方法：
   - NetBIOS 網域
   - Active Directory 網域
   - DNS 網域
3. 請點選「儲存」。

接下來需執行的動作

執行以下工作來管理網域以及分組在這些網域下的用戶端：

- 新增網域

- 刪除網域或用戶端
- 重新命名網域
- 將單一用戶端移至另一個網域

如需詳細資訊，請參閱用戶端分組工作 第 2-54 頁。

自動用戶端分組

自動用戶端分組使用由 IP 位址或 Active Directory 網域定義的規則。如果某個規則定義了 IP 位址或 IP 位址範圍，則 Apex One 伺服器會將具有相符 IP 位址的用戶端分組到用戶端樹狀結構中的特定網域。同樣地，如果某個規則定義了一或多個 Active Directory 網域，則 Apex One 伺服器會將屬於特定 Active Directory 網域的用戶端分組到用戶端樹狀結構中的特定網域。

用戶端一次僅套用一個規則。設定規則的優先順序，以便任何用戶端在符合多個規則時套用最高優先順序的規則。

設定自動用戶端分組

步驟

1. 移至「用戶端 > 用戶端分組」
2. 移至「用戶端分組」區段，然後選取「針對現有 Security Agent 建立自訂用戶端群組」。
3. 移至「自動用戶端分組」區段。
4. 如果要開始建立規則，請點選「新增」，然後選取「Active Directory」或「IP 位址」。
   - 如果選取「Active Directory」，請參閱依據 Active Directory 網域定義用戶端分組規則 第 2-52 頁中的組態設定指示。
   - 如果選取「IP 位址」，請參閱依據 IP 位址定義用戶端分組規則 第 2-53 頁中的組態設定指示。

5. 如果建立了多個規則，請執行以下步驟來設定規則的優先順序：

   a. 選取某個規則。

   b. 請點選「群組優先順序」欄下的箭頭，在清單中上移或下移該規則。規則的 ID 號碼則會變更以反映新位置。

6. 如果要在用戶端排序期間使用規則：

   a. 選取要使用的規則的核取方塊。

   b. 將「狀態」控制項切換到「開啟」，以啟動規則。

   注意

   如果未選取某個規則的核取方塊或是關閉某個規則，則在用戶端樹狀結構中對用戶端進行排序時將不會使用該規則。例如，如果該規則指定任何用戶端應移至新網域，則該用戶端將不會移動並且會保留在其目前的網域中。

7. 在「預約網域建立」區段指定排序預約。

   a. 選取「啟動預約網域建立」。

   b. 在「預約網域建立」下指定預約。

8. 請從下列選項選擇：

   - 儲存並立即建立網域：如果您在依據 IP 位址定義用戶端分組規則 第 2-53 頁的步驟 7 或依據 Active Directory 網域定義用戶端分組規則 第 2-52 頁的步驟 7 中指定了新網域，則選擇此選項。
   - 儲存：如果您尚未指定新網域或只有在用戶端排序執行時才要建立新網域，則選擇此選項：

   注意

   完成此步驟後，不會啟動用戶端排序。

依據 Active Directory 網域定義用戶端分組規則

在執行以下程序中的步驟之前，請確定已設定 Active Directory 整合設定。如需詳細資訊，請參閱 Active Directory 整合 第 2-31 頁。

步驟

1. 移至「用戶端 > 用戶端分組」。
2. 移至「用戶端分組」區段，然後選取「針對現有 Security Agent 建立自訂用戶端群組」。
3. 移至「自動用戶端分組」區段。
4. 請點選「新增」，然後選取「Active Directory」。

   隨即顯示新畫面。
5. 選取「啟動分組」。
6. 指定此規則的名稱。
7. 在「Active Directory 來源」下，選取 Active Directory 網域或子網域。
8. 在「用戶端樹狀結構」下，選取 Active Directory 網域對應的現有 Apex One 網域。如果所需的 Apex One 網域不存在，則執行以下步驟：

   a. 將滑鼠游標移至特定 Apex One 網域上並請點選「新增網域」圖示 (➕)。

   b. 在出現的文字方塊中輸入網域名稱。

   c. 請點選文字方塊旁邊的選取記號。隨即新增並自動選取新網域。
9. （選用）選取「將 Active Directory 結構複製到用戶端樹狀結構」。此選項會將所選取 Active Directory 網域的階層複製到選取的 Apex One 網域。
10. 請點選「儲存」。

依據 IP 位址定義用戶端分組規則

使用網路 IP 位址建立自訂的用戶端群組，以對 Apex One 用戶端樹狀結構中的用戶端進行分類。此功能可協助管理員在用戶端向 Apex One 伺服器註冊之前，先行排列 Apex One 用戶端樹狀結構。

步驟

1. 移至「用戶端 > 用戶端分組」。
2. 移至「用戶端分組」區段，然後選取「針對現有 Security Agent 建立自訂用戶端群組」。
3. 移至「自動用戶端分組」區段。
4. 請點選「新增」，然後選取「IP 位址」。

   隨即顯示新畫面。
5. 選取「啟動分組」。
6. 請指定此分組的名稱。
7. 指定下列其中一個項目：
   - 單一 IPv4 或 IPv6 位址
   - IPv4 位址範圍
   - IPv6 字首和長度

   注意

   如果雙堆疊用戶端的 IPv4 和 IPv6 位址屬於兩個單獨的用戶端群組，則這個用戶端會分組在 IPv6 群組下。如果在用戶端的主機上關閉了 IPv6，則用戶端會移至 IPv4 群組。
8. 選取 IP 位址或 IP 位址範圍對應的 Apex One 網域。如果網域不存在，請執行下列動作：
   a. 將滑鼠游標移至用戶端樹狀結構上的任意位置，然後請點選新增網域圖示。

圖 2-8. 新增網域圖示

b. 在出現的文字方塊中輸入網域。

c. 請點選文字方塊旁邊的選取記號。隨即新增並自動選取新網域。

9. 請點選「儲存」。

用戶端分組工作

在對網域中的用戶端進行分組時，您可以執行下列工作：

- 新增網域。如需詳細資訊，請參閱新增網域 第 2-54 頁。
- 刪除網域或用戶端。如需詳細資訊，請參閱刪除網域或用戶端 第 2-55 頁。
- 重新命名網域。如需詳細資訊，請參閱重新命名網域 第 2-56 頁。
- 將單一用戶端移至其他網域或其他 Apex One 伺服器。如需詳細資訊，請參閱將 Security Agent 移至其他網域或伺服器 第 2-56 頁。

新增網域

步驟

1. 瀏覽到「用戶端 > 用戶端管理」。

2. 請點選「管理用戶端樹狀結構 > 新增網域」。
3. 輸入您想新增的網域名稱。
4. 請點選「新增」。

   新網域會出現在用戶端樹狀結構中。
5. （選用）建立子網域。
   a. 選取上一層網域。
   b. 請點選「管理用戶端樹狀結構 > 新增網域」。
   c. 輸入子網域名稱。

刪除網域或用戶端

步驟

1. 瀏覽到「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，選取：
   - 一個或多個網域
   - 屬於某個網域的一個、多個或所有用戶端
3. 請點選「管理用戶端樹狀結構 > 移除網域/用戶端」。
4. 如果要刪除某個空白的網域，只要請點選「移除網域/用戶端」即可。如果該網域具有用戶端，當您請點選「移除網域/用戶端」，Apex One 伺服器會重新建立網域，並在下次用戶端連線到 Apex One 伺服器時將所有用戶端分組到該網域之下。在刪除該網域之前，您可以執行下列工作：
   a. 將用戶端移至其他網域。如果要將用戶端移至其他網域，請將用戶端拖放到目標網域。
   b. 刪除全部用戶端。
5. 如果要刪除單一用戶端，請點選「移除網域/用戶端」。

注意

從 用戶端樹狀結構中刪除用戶端不會從用戶端端點中移除 Security Agent。Security Agent 仍然可以執行與伺服器無關的工作，例如更新元件。不過，由於伺服器偵測不到用戶端的存在，因此不會部署組態設定，也不會傳送通知到用戶端。

重新命名網域

步驟

1. 瀏覽到「用戶端 > 用戶端管理」。
2. 從用戶端樹狀結構中選取一個網域。
3. 請點選「管理用戶端樹狀結構 > 重新命名網域」。
4. 輸入網域的新名稱。
5. 請點選「重新命名」。

   新網域名稱會出現在用戶端樹狀結構中。

將 Security Agent 移至其他網域或伺服器

步驟

1. 瀏覽至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，選取一個、多個或所有用戶端。
3. 請點選「管理用戶端樹狀結構 > 移動用戶端」。
4. 如果要將用戶端移至其他網域，請執行下列步驟：
   - 選取「將選取的用戶端移動到其他網域」。
   - 選取網域。

- （選用）將新網域的設定套用到用戶端。

秘訣

您也可以將用戶端拖放到用戶端樹狀結構中的其他網域。

5. 如果要將用戶端移至其他伺服器，請執行下列步驟：
   - 選取「將選取的用戶端移動到其他伺服器」。
   - 輸入伺服器名稱或 IPv4/IPv6 位址，以及 HTTP 或 SSL (443) 通訊埠號碼。

注意

如果您要將 Security Agent 移至 Apex One as a Service，可以存取 Apex Central 主控台來取得 Apex One as a Service 伺服器資訊。移至「目錄 > 產品伺服器」，然後在「伺服器類型」下拉式清單中選取「Apex One」。

6. 請點選「移動」。

第 3 章

使用資料安全防護

本章討論如何安裝和啟動「資料安全防護」模組。

包含下列主題：

資料安全防護安裝

「資料安全防護」模組包含下列功能：

- 資料外洩防護 (DLP)：防止未經授權的數位資產傳輸
- 周邊設備存取控管：規範對於外部裝置的存取

注意

Apex One 內建「周邊設備存取控管」功能，可規範對於常用裝置（例如：USB 儲存裝置）的存取。「周邊設備存取控管」（「資料安全防護」模組的一部分）可擴大監控的裝置範圍。如需受監控的裝置清單，請參閱周邊設備存取控管 第 10-2 頁。

「資料外洩防護」和「周邊設備存取控管」是 Apex One 內建的功能，但您必須另行為其取得使用授權。安裝 Apex One 伺服器之後，這些功能就會可用，但是無法運作，而且您無法將它們部署到 Security Agent。安裝「資料安全防護」表示您必須從主動式更新伺服器或自訂更新來源（如果已設定自訂更新來源）下載檔案。當該檔案整合至 Apex One 伺服器之後，您就可以註冊「資料安全防護」使用授權，以啟動其完整功能。您必須從 Plug-in Manager 執行安裝和註冊。

安裝資料安全防護

步驟

1. 開啟 Apex One Web 主控台，然後按一下主功能表中的「嵌入程式」。
2. 在 Plug-in Manager 畫面上，移至「Apex One 資料安全防護」區段，然後按一下「下載」。

   要下載的檔案大小會顯示在「下載」按鈕旁。

   Plug-In Manager 會將下載的檔案儲存到 <伺服器安裝資料夾>\PCCSRV\Download\Product。

注意

如果 Plug-in Manager 無法下載該檔案，它會在 24 小時後自動重新下載。如果要手動讓 Plug-in Manager 下載該檔案，請從 Microsoft 管理主控台重新啟動 Apex OnePlug-in Manager 服務。

3. 監控下載進度。

   下載期間您可以瀏覽其他畫面。

   如果在下載該檔案時遇到問題，請檢查 Apex One Web 主控台上的伺服器更新記錄檔。在主功能表上，按一下「記錄檔 > 伺服器更新」。

   當 Plug-in Manager 下載該檔案之後，「Apex One 資料安全防護」會顯示在新畫面中。

注意

如果未顯示「Apex One 資料安全防護」，請參閱 Plug-in Manager 疑難排解 第 17-11 頁，以查知原因和解決方案。

4. 如果要立即安裝「Apex One 資料安全防護」，請點選「立即安裝」，或者如果要稍後安裝，請執行下列步驟：

   a. 請點選「稍後安裝」。

   b. 開啟「Plug-in Manager」畫面。

   c. 移至「Apex One 資料安全防護」區段，然後按一下「安裝」。

5. 閱讀授權合約，然後請點選「同意」表示您接受其中的條款。

   安裝便會開始。

6. 監控安裝進度。安裝之後，會顯示「Apex One 資料安全防護」版本。

資料安全防護使用授權

您可以從 Plug-in Manager 檢視、註冊和續約「資料安全防護」使用授權。

請從趨勢科技取得啟動碼，然後用它來註冊使用授權。

啟動嵌入程式授權

步驟

1. 開啟 Apex One Web 主控台，然後請點選主功能表中的「嵌入程式」。
2. 在 Plug-in Manager 畫面中，移至嵌入程式區段，然後請點選「管理程式」。

   會出現「產品使用授權新啟動碼」畫面。
3. 在文字欄位輸入或複製並貼上啟動碼。
4. 請點選「儲存」。

   會出現嵌入程式主控台。

檢視和更新使用授權資訊

步驟

1. 開啟 Apex One Web 主控台，然後請點選主功能表中的「嵌入程式」。
2. 在 Plug-in Manager 畫面中，移至嵌入程式區段，然後請點選「管理程式」。
3. 請點選「檢視使用授權資訊」，在趨勢科技網站上檢視目前使用授權的相關資訊。
4. 在開啟的畫面中檢視下列使用授權詳細資訊。

選項	說明
狀態	顯示「已啟動」、「未啟動」或「已到期」

選項	說明
版本	顯示「完整版」或「試用版」 注意 同時啟動完整版和試用版時顯示的版本是「完整版」。
授權數目	顯示嵌入程式可管理的端點數量
使用授權逾期期限	如果嵌入程式有多個使用授權，會顯示最新的到期日。 例如，如果使用授權到期日為 2011 年 12 月 31 日和 2011 年 6 月 30 日，則會顯示 2011 年 12 月 31 日。
啟動碼	顯示啟動碼
提醒	視您目前的使用授權版本而定，嵌入程式會在寬限期（僅完整版）或使用授權到期時，顯示使用授權到期日提醒

注意

寬限期視地區而定。請向您的趨勢科技銷售人員確認嵌入程式的寬限期。

5. 如果要更新畫面以顯示最新的使用授權資訊，請點選「更新資訊」。
6. 請點選「新啟動碼」，開啟「產品使用授權新啟動碼」畫面。

   如需詳細資訊，請參閱啟動嵌入程式授權 第 3-4 頁。

將資料安全防護部署到 Security Agent

啟動「資料安全防護」模組的使用授權之後，您就可以將它部署到 Security Agent。部署之後，Security Agent 會開始使用「資料外洩防護」和「周邊設備存取控管」。

重要

- 依預設，Windows Server 平台會關閉此模組，以避免主機電腦的效能受到影響。如果要啟動此模組，請持續監控系統效能，並在發現效能變差時採取必要的處理行動。

  您可以從 Web 主控台啟動或關閉此模組。如需詳細資訊，請參閱 Security Agent 服務 第 15-6 頁。

- 如果 Trend Micro Data Loss Prevention 軟體已存在於端點上，Apex One 不會使用「資料安全防護」模組來取代它。
- 線上用戶端會立即安裝「資料安全防護」模組。離線與單機用戶端會在重新連線至 Apex One 伺服器後安裝此模組。
- 使用者必須重新啟動電腦，才能完成資料外洩防護驅動程式的安裝。重新啟動之前請先通知使用者。
- 趨勢科技建議您啟動偵錯記錄功能，以協助您解決部署問題。如需詳細資訊，請參閱啟動資料安全防護模組的偵錯記錄功能 第 11-57 頁。

將資料安全防護模組部署到 Security Agent

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，您可以：
   - 請點選根網域圖示 ( )，以將該模組部署到所有現有和未來的用戶端。
   - 選取特定網域，以將該模組部署到該網域下的所有現有和未來的用戶端。
   - 選取特定用戶端，只將該模組部署到該用戶端。
3. 以兩種方式進行部署：
   - 請點選「設定 > DLP 設定」。

- 請點選「設定 > 周邊設備存取控管設定」。

注意

如果您從「設定 > DLP 設定」部署，然後成功部署資料安全防護模組，系統將會安裝資料外洩防護驅動程式。如果驅動程式安裝成功，就會顯示訊息，通知使用者重新啟動端點以完成驅動程式的完裝。

如果未顯示訊息，表示安裝驅動程式時可能發生問題。如果已啟動偵錯記錄功能，請檢查偵錯記錄檔，以尋找與驅動程式安裝問題有關的詳細資訊。

4. 會顯示一則訊息，指出尚未安裝該模組的用戶端數目。請點選「是」以開始部署。

注意

如果您請點選「否」（或如果模組因故無法部署至一個或多個用戶端），則當您再請點選「設定 > DLP 設定」或「設定 > 周邊設備存取控管設定」時會顯示相同的訊息。

Security Agent 會開始從伺服器下載該模組。

5. 檢查該模組是否已部署至用戶端。

   a. 在用戶端樹狀結構中，選取網域。

   b. 在用戶端樹狀結構檢視中，選取「資料安全防護檢視」或「檢視全部」。

   c. 檢查「資料安全防護狀態」欄。部署狀態可以是下列任一種：

      - 執行中：模組已經部署成功，而且其功能已經啟動。
      - 需要重新啟動：由於使用者尚未重新啟動電腦，因此系統仍未將資料外洩防護驅動程式安裝完成。如果未安裝驅動程式，資料外洩防護將無法運作。
      - 已停止：模組的服務尚未啟動或目標端點已正常關機。如果要啟動資料安全防護服務，請移至「用戶端 > 用戶端管理 > 設定 > 其他服務設定」，然後啟動資料安全防護服務。

- 無法安裝：將模組部署到用戶端時發生問題。您將需要從用戶端樹狀結構重新部署該模組。
- 無法安裝（資料外洩防護已存在）：Trend Micro Data Loss Prevention 軟體已存在於端點上。Apex One 不會使用「資料安全防護」模組來取代它。
- 未安裝：該模組尚未部署至用戶端。如果您選擇不將該模組部署至用戶端，或在部署期間用戶端處於「離線」或「單機」模式，則會顯示此狀態。

鑑識資料夾和 DLP 資料庫

發生資料外洩防護事件之後，Apex One 會在專用的鑑識資料庫中記錄該事件的詳細資料。Apex One 也會建立一個加密檔案，其中包含觸發事件的敏感資料副本，並針對驗證目的產生一個雜湊值，以確保敏感資料的完整性。Apex One 會在用戶端機器上建立加密的鑑識檔案，然後將檔案上傳到伺服器上的指定位置。

重要

- 經過加密的鑑識檔案包含高度敏感的資料，管理員在授與這些檔案的存取權時，應格外謹慎小心。
- Apex One 整合了 Apex Central，可將 DLP 事件檢閱者或 DLP 符合性主管的角色提供給 Apex Central 使用者，使其能夠存取加密檔案中的資料。如需 Apex Central 中的 DLP 角色和鑑識檔案存取權的詳細資訊，請參閱《Control Manager 管理手冊》或《Apex Central 管理手冊》。

修改鑑識資料夾和資料庫設定

管理員可透過修改 Apex One 的 INI 檔案來變更鑑識資料夾的位置並刪除排程，以及用戶端上傳的最大檔案大小。

警告!

在記錄資料外洩防護事件之後變更鑑識資料夾的位置，會導致資料庫資料與現有鑑識檔案之間的連線中斷。趨勢科技建議在修改鑑識資料夾位置後，手動將任何現有的鑑識檔案移轉至新的鑑識資料夾。

下表列出位於 Apex One 伺服器的 <伺服器安裝資料夾>\PCCSRV\Private\ofcserver.ini 檔案中可用的伺服器設定。

表 3-1. PCCSRV\Private\ofcserver.ini 中的鑑識資料夾伺服器設定

目的	INI 設定	值
啟動使用者定義的鑑識資料夾位置	[INI_IDLP_SECTION] EnableUserDefinedUploadFolder	0：關閉（預設值） 1：啟動
設定使用者定義的鑑識資料夾位置	[INI_IDLP_SECTION] UserDefinedUploadFolder 注意 • 管理員必須先啟動 EnableUserDefinedUploadFolder 設定，資料外洩防護才能套用此設定。 • 鑑識資料夾的預設位置為： <伺服器安裝資料夾>\PCCSRV\Private\DLPForensicData • 使用者定義的鑑識資料夾位置必須是伺服器電腦上的（內部或外部）實體磁碟機。Apex One 不支援對應網路磁碟機位置。	預設值：<請以客戶定義的資料夾路徑取代此值。例如：C:\VolumeData\OfficeScanDlpForensicData> 使用者定義的值：必須是伺服器電腦上磁碟機的實體位置
啟動清除鑑識資料檔案	[INI_IDLP_SECTION] ForensicDataPurgeEnable	0：關閉 1：啟動（預設值）

目的	INI 設定	值
設定鑑識資料檔案清除檢查的時間頻率	[INI_IDLP_SECTION] `ForensicDataPurgeCheckFrequency` 注意 • 管理員必須先啟動 `ForensicDataPurgeEnable` 設定，Apex One 才能套用此設定。 • Apex One 只會刪除超過 `ForensicDataExpiredPeriodInDays` 設定中指定之到期日的資料檔案。	1：每月，每月第一天的 00:00 2：每週（預設值），每個星期日的 00:00 3：每天，每天的 00:00 4：每小時，每小時 HH:00
設定伺服器上保存鑑識資料檔案的時間長度	[INI_IDLP_SECTION] `ForensicDataExpiredPeriodInDays`	預設值（天）：180 最小值：1 最大值：3650
設定鑑識資料檔案磁碟空間檢查的時間頻率	[INI_SERVER_DISK_THRESHOLD] `MonitorFrequencyInSecond` 注意 如果鑑識資料資料夾的可用磁碟空間低於 `InformUploadOnDiskFreeSpaceInGb` 設定所設的值，Apex One 將會在 Web 主控台上記錄事件記錄檔。	預設值（秒）：5
設定鑑識資料檔案磁碟空間檢查的上傳頻率	[INI_SERVER_DISK_THRESHOLD] `IsapiCheckCountInRequest` 注意 如果鑑識資料資料夾的可用磁碟空間低於 `InformUploadOnDiskFreeSpaceInGb` 設定所設的值，Apex One 將會在 Web 主控台上記錄事件記錄檔。	預設值（檔案數）：200

目的	INI 設定	值
設定觸發有限磁碟空間通知的最小磁碟空間值	[INI_SERVER_DISK_THRESHOLD] `InformUploadOnDiskFreeSpaceInGb` **注意** 如果鑑識資料資料夾的可用磁碟空間低於所設定的值，Apex One 將會在 Web 主控台上記錄事件記錄檔。	預設值 (GB)：10
設定從用戶端上傳鑑識資料檔案的最小可用空間	[INI_SERVER_DISK_THRESHOLD] `RejectUploadOnDiskFreeSpaceInGb` **注意** 如果鑑識資料資料夾的可用磁碟空間低於所設定的值，則用戶端不會上傳鑑識資料檔案至伺服器，Apex One 將會在 Web 主控台上記錄事件記錄檔。	預設值 (GB)：1

下表列出位於 Apex One 伺服器的 <伺服器安裝資料夾>\PCCSRV\ofcscan.ini 檔案中可用的 Security Agent 設定。

表 3-2. PCCSRV\ofcscan.ini 中的鑑識檔案用戶端設定

目的	INI 設定	值
啟動上傳鑑識資料檔案到伺服器	`UploadForensicDataEnable`	0：關閉 1：啟動（預設值）
設定 Security Agent 上傳到伺服器的檔案大小上限	`UploadForensicDataSizeLimitInMb` **注意** Security Agent 只會將低於此大小的檔案傳送到伺服器。	預設值 (MB)：10 最小值：1 最大值：20

目的	INI 設定	值
設定 Security Agent 上儲存鑑識資料檔案的時間長度	`ForensicDataKeepDays` **注意** Security Agent 會根據前一天的清除時間，每天刪除一次已超過指定到期日的鑑識資料檔案。	預設值（天）：180 最小值：1 最大值：3650
設定 Security Agent 檢查伺服器連線的頻率	`ForensicDataDelayUploadFrequenceInMinutes` **注意** Security Agent 無法上傳鑑識檔案到伺服器時，會自動嘗試使用指定的時間間隔重新傳送檔案。	預設值（分鐘）：5 最小值：5 最大值：60

建立鑑識資料的備份

根據公司的安全策略，保存鑑識資料資訊所需的時間長度可能有很大的差異。為了釋出伺服器上的磁碟空間，趨勢科技建議手動備份鑑識資料夾資料和鑑識資料庫。

步驟

1. 移至伺服器上的鑑識資料資料夾位置。
   - 預設位置：<伺服器安裝資料夾>\PCCSRV\Private\DLPForensicData
   - 如果要找到自訂的鑑識資料夾位置，請參閱設定使用者定義的鑑識資料夾位置 第 3-9 頁。
2. 將資料夾複製到新位置。
3. 如果要手動備份鑑識資料資料庫，請瀏覽至 <伺服器安裝資料夾>\PCCSRV\Private。

4. 將 DLPForensicDataTracker.db 檔案複製到新位置。

解除安裝資料安全防護

如果從 Plug-in Manager 解除安裝資料安全防護模組：

- 系統會從 Apex One 伺服器移除所有資料外洩防護組態、設定和記錄檔。
- 系統會從伺服器移除資料安全防護模組所提供的所有「周邊設備存取控管」組態和設定。
- 系統會從用戶端移除資料安全防護模組。必須重新啟動用戶端端點，才能完成移除資料安全防護。
- 用戶端上不會再實施資料外洩防護策略。
- 「周邊設備存取控管」不會再監控對下列裝置的存取：
  - Bluetooth 介面卡
  - COM 和 LPT 通訊埠
  - IEEE 1394 介面
  - 影像裝置
  - 紅外線裝置
  - 數據機
  - PCMCIA 卡
  - 列印螢幕鍵
  - 無線 NIC

隨時重新安裝「資料安全防護」模組。重新安裝之後，請使用有效的啟動碼來註冊使用授權。

從 Plug-in Manager 解除安裝資料安全防護

步驟

1. 開啟 Apex One Web 主控台，然後按一下主功能表中的「嵌入程式」。
2. 在 Plug-in Manager 畫面上，移至「Apex One 資料安全防護」區段，然後按一下「解除安裝」。
3. 監控解除安裝進度。解除安裝期間您可以瀏覽其他畫面。
4. 解除安裝之後，請重新整理 Plug-in Manager 畫面。您可以再次安裝「Apex One 資料安全防護」。

部分 II

保護 Security Agent

第 4 章

使用趨勢科技主動雲端截毒技術

本章討論趨勢科技主動雲端截毒技術解決方案，並說明如何設定使用該解決方案所需的環境。

包含下列主題：

關於趨勢科技主動雲端截毒技術

趨勢科技™主動雲端截毒技術是新一代的雲端用戶端內容安全基礎結構，旨在保護客戶不受安全威脅和網路安全威脅的侵襲。該技術支援本機和代管解決方案，不論使用者是位於網路上、在家中還是在路上，都可受到保護，方法是使用輕量型 用戶端 來存取電子郵件、網頁和檔案信譽評等技術以及安全威脅資料庫的獨一無二的雲端關聯性。隨著存取這個網路的產品、服務和使用者越來越多，等於為其使用者建立了一個即時的守望相助系統，因此客戶受到的保護會自動更新和強化。

藉由併入雲端信譽評等、掃瞄和相互關聯技術，趨勢科技主動雲端截毒技術解決方案可減少對於傳統病毒碼檔案下載的依賴，以及消除通常與桌上型電腦關聯的延遲。

新解決方案的必要性

在目前的檔案型威脅處理方法中，保護端點所需的病毒碼（或定義）大多是經由預約方式傳遞。病毒碼是從趨勢科技分批傳遞至用戶端。用戶端上的病毒/惡意程式防護軟體在收到更新後，即會將這批針對新病毒/惡意程式威脅的病毒碼定義重新載入記憶體中。如果有新的病毒/惡意程式威脅出現，則需要對此病毒碼再進行部分或全部更新，並重新載入到用戶端上，以確保持續防護。

隨著時間的推移，各式各樣的新型安全威脅的數量快速激增。預計在未來幾年內，安全威脅的數量將繼續以接近指數的速率飛增。按照這樣的增長率，以後的安全威脅數量將遠遠超越目前已知的安全威脅數量。此外，這麼多的安全威脅數量意味著新型態的安全威脅。安全威脅的數量會影響伺服器和工作站效能、網路頻寬用量，以及提供高品質防護的總用時（即「防護前置時間」）。

趨勢科技已創造一套應付大量安全威脅的新方法，旨在讓趨勢科技客戶免於受到激增的病毒/惡意程式的襲擊。這項創舉中所使用的技術和架構，利用了將病毒/惡意程式防護簽章和病毒碼改為儲存在雲端中的技術。藉由將這些病毒/惡意程式簽章改為儲存到雲端，趨勢科技得以為客戶提供更好的防護，以抵禦未來新興的大量安全威脅。

主動雲端截毒技術服務

主動雲端截毒技術包括提供儲存在雲端的惡意程式防護簽章、網頁信譽評等和安全威脅資料庫等服務。

主動雲端截毒技術服務包括：

- 檔案信譽評等服務：檔案信譽評等服務會將先前儲存在用戶端電腦上的大量惡意程式防護簽章改由主動雲端截毒伺服器來源處理。

  如需詳細資訊，請參閱檔案信譽評等服務 第 4-3 頁。

- 網頁信譽評等服務：網頁信譽評等服務讓本機主動雲端截毒伺服器來源可以代管先前只由趨勢科技獨力代管的 URL 信譽評等資料。這兩項技術可確保在更新病毒碼或檢查 URL 的有效性時耗用較少的頻寬。

  如需詳細資訊，請參閱網頁信譽評等服務 第 4-4 頁。

- Smart Feedback：趨勢科技會繼續收集從世界各地的趨勢科技產品匿名傳送的資訊，以便主動判斷每個新的安全威脅。

  如需詳細資訊，請參閱 Smart Feedback 第 4-4 頁。

檔案信譽評等服務

檔案信譽評等服務會對照龐大的雲端資料庫檢查每個檔案的信譽。惡意程式資訊由於是儲存於雲端，因此可立即供所有使用者使用。高效能的網路內容傳送網路和本機快取伺服器可確保將檢查程序期間的延遲降至最低。雲端用戶端架構可提供更即時的防護、消除部署病毒碼的麻煩，同時大幅減少整體用戶端佔用空間。

用戶端必須處於雲端截毒掃瞄模式才能使用檔案信譽評等服務。在本文件中，這些用戶端稱為雲端截毒掃瞄用戶端。用戶端未處於雲端截毒掃瞄模式下時，不會使用檔案信譽評等服務，這些用戶端稱為標準掃瞄用戶端。Apex One 管理員可以將全部或多個用戶端設定為使用雲端截毒掃瞄模式。

網頁信譽評等服務

透過全世界其中一個最大的網域信譽評等資料庫，趨勢科技網頁信譽評等技術會依據諸如網站的存在時間長短、位置變更記錄，以及透過惡意程式行為分析所發現的可疑活動指標等因素來指定信譽評等，以追蹤 Web 網域的可信度。然後網頁信譽評等服務會繼續掃瞄網站，並阻止使用者存取中毒的網站。網頁信譽評等功能有助於確認使用者存取的是安全網頁，且不含任何網路安全威脅，例如惡意程式、間諜程式，以及專門誘騙使用者提供個人資訊的網路釣魚詐騙手法。為了提高準確度並減少誤判的情形，趨勢科技網頁信譽評等技術會為網站內的特定網頁或連結指定信譽評分，而不是將整個網站進行分類或封鎖，因為通常合法網站只有部分受到駭客入侵，而信譽評等會隨著時間動態變更。

受網頁信譽評等策略約束的 Security Agent 會使用網頁信譽評等服務。Apex One 管理員可以使全部或多個用戶端受網頁信譽評等策略的約束。

Smart Feedback

趨勢科技 Smart Feedback 提供趨勢科技產品之間不間斷的通訊，以及該公司每天 24 小時、一週 7 天的安全威脅研究中心和技術。若是每個單一客戶在執行例行信譽檢查時發現任何新的安全威脅，就會自動更新所有趨勢科技的安全威脅資料庫，以避免任何後續客戶受到該安全威脅的攻擊。

趨勢科技藉由持續處理透過廣大全球客戶和合作夥伴網路收集的安全威脅資訊，提供自動的即時防護以抵禦最新的安全威脅侵襲，同時提供更佳的協同安全防護，就像是自動化的守望相助系統，動員整個社群來保護其中的每個人。因為所收集的安全威脅資訊基於通訊來源的信譽評等而非特定通訊內容，所以客戶個人或商業資訊的隱私一律會受到保護。

舉例來說，會傳送給趨勢科技的資訊包括：

- 檔案總和檢查碼
- 已存取的網站
- 檔案資訊，包括大小與路徑
- 執行檔名稱

您可以隨時從 Web 主控台終止參加此計畫。

秘訣

您即使不參與 Smart Feedback，您的端點也會受到保護。您可以選擇是否參與，而且可以隨時選擇退出。趨勢科技建議您參與 Smart Feedback，以協助為所有的趨勢科技客戶提供更全面的防護。

如需主動雲端截毒技術的詳細資訊，請造訪：

http://www.trendmicro.com.tw/SPN.htm

主動雲端截毒伺服器來源

趨勢科技會提供「檔案信譽評等服務」和「網頁信譽評等服務」給 Apex One 和主動雲端截毒伺服器來源。

主動雲端截毒伺服器來源會透過裝載大多數病毒/惡意程式病毒碼定義來提供「檔案信譽評等服務」。Security Agent 則裝載其餘的定義。如果用戶端自身的病毒碼定義無法判斷檔案的風險，會將掃瞄查詢傳送至主動雲端截毒伺服器來源。主動雲端截毒伺服器來源會使用識別資訊來判斷風險。

主動雲端截毒伺服器來源會裝載網頁信譽評等資料（以前僅由趨勢科技裝載的伺服器提供）以提供「網頁信譽評等服務」。用戶端會將網頁信譽評等查詢傳送至主動雲端截毒伺服器來源，以檢查使用者嘗試存取之網站的信譽。用戶端會將網站的信譽與端點上實施的特定網頁信譽評等策略關聯，以判斷要允許還是封鎖存取該網站。

用戶端所連線的主動雲端截毒技術來源取決於用戶端的位置。用戶端可連線至趨勢科技主動雲端截毒技術或主動雲端截毒技術伺服器。

趨勢科技™主動雲端截毒技術™

趨勢科技™主動雲端截毒技術™是新一代的雲端用戶端內容安全基礎結構，旨在保護客戶不受安全威脅和網路安全威脅的侵襲。我們提供內部部署及趨勢科技託管兩種解決方案，可以保護使用者在家或隨身使用網路的安全。主動雲端

截毒技術讓輕量型用戶端能使用電子郵件、網頁和檔案信譽評等技術以及安全威脅資料庫的獨特雲端相互關聯性。隨著存取這個網路的產品、服務和使用者越來越多，等於為其使用者建立了一個即時的守望相助系統，因此客戶受到的保護會自動更新和強化。

如需主動雲端截毒技術的詳細資訊，請造訪：

http://www.trendmicro.com.tw/SPN.htm

主動雲端截毒技術伺服器

主動雲端截毒技術伺服器可供存取其企業區域網路的使用者使用。本機伺服器供客戶在企業網路內執行雲端防護服務，以最佳化效能。

主動雲端截毒技術伺服器的類型有兩種：

- 整合式主動雲端截毒技術伺服器：Apex One 安裝程式中包含與 Apex One 伺服器安裝在同一端點上的整合式主動雲端截毒技術伺服器。安裝之後，可透過 Apex One Web 主控台管理此伺服器的設定。整合式伺服器適用於小規模的 Apex One 部署。如果是較大的部署，則需要獨立式主動雲端截毒技術伺服器。
- 獨立式主動雲端截毒技術伺服器：獨立式主動雲端截毒技術伺服器安裝於 VMware 或 Hyper-V 伺服器上。獨立式伺服器具有個別的管理主控台，不受 Apex One Web 主控台管理。

主動雲端截毒伺服器來源比較

下表重點說明主動雲端截毒技術與主動雲端截毒技術伺服器之間的差別。

表 4-1. 主動雲端截毒伺服器來源比較

比較基準	主動雲端截毒技術伺服器	趨勢科技主動雲端截毒技術
可用性	可供內部用戶端使用，內部用戶端是指符合在 Apex One Web 主控台指定的位置條件的用戶端	主要供外部用戶端使用，外部用戶端是指不符合在 Apex One Web 主控台指定的位置條件的用戶端

比較基準	主動雲端截毒技術伺服器	趨勢科技主動雲端截毒技術
用途	設計目標和主要用途是供客戶在企業網路內執行主動雲端截毒技術服務，以最佳化效能	具備全球規模的 Internet-based 基礎架構，可將主動雲端截毒技術服務提供給無法直接存取其企業網路的用戶端
管理	Apex One 管理員會安裝和管理這些主動雲端截毒伺服器來源	趨勢科技維護此來源
病毒碼更新來源	趨勢科技主動式更新伺服器	趨勢科技主動式更新伺服器
用戶端連線通訊協定	HTTP 和 HTTPS	HTTPS

主動雲端截毒技術病毒碼檔案

主動雲端截毒技術病毒碼檔案用於檔案信譽評等服務和網頁信譽評等服務。趨勢科技會通過趨勢科技主動式更新伺服器發佈這些病毒碼檔案。

本機雲端病毒碼

本機雲端病毒碼每天更新一次，並由 Apex One 用戶端的更新來源（Apex One 伺服器或自訂更新來源）下載。然後，更新來源會將病毒碼部署到雲端截毒掃瞄用戶端。

注意

雲端截毒掃瞄用戶端是管理員已設定為使用檔案信譽評等服務的 Security Agent。不使用檔案信譽評等服務的用戶端稱為標準掃瞄用戶端。

在掃瞄安全威脅時，雲端截毒掃瞄用戶端會使用本機雲端病毒碼。如果該病毒碼無法確定檔案的風險，這時會利用稱為雲端病毒碼的另一個病毒碼。

雲端病毒碼

雲端病毒碼每小時更新一次，從主動雲端截毒伺服器來源下載。雲端截毒掃瞄用戶端不會下載雲端病毒碼。用戶端會將掃瞄查詢傳送至主動雲端截毒伺服器來源，並與病毒碼比對來確認潛在的安全威脅。

網頁封鎖清單

網頁封鎖清單是由主動雲端截毒伺服器來源下載。受網頁信譽評等策略約束的 Security Agent 不會下載網頁封鎖清單。

注意

管理員可以使全部或多個用戶端受網頁信譽評等策略的約束。

受網頁信譽評等服務策略約束的用戶端會傳送網頁信譽評等查詢至主動雲端截毒技術來源，並比對網頁封鎖清單來確認網站的信譽。該用戶端會將接收自主動雲端截毒技術來源的信譽資料與端點上執行的網頁信譽評等策略關聯。根據該策略，用戶端將允許或封鎖對網站的存取。

主動雲端截毒技術病毒碼更新程序

源自趨勢科技主動式更新伺服器的雲端防護病毒碼。

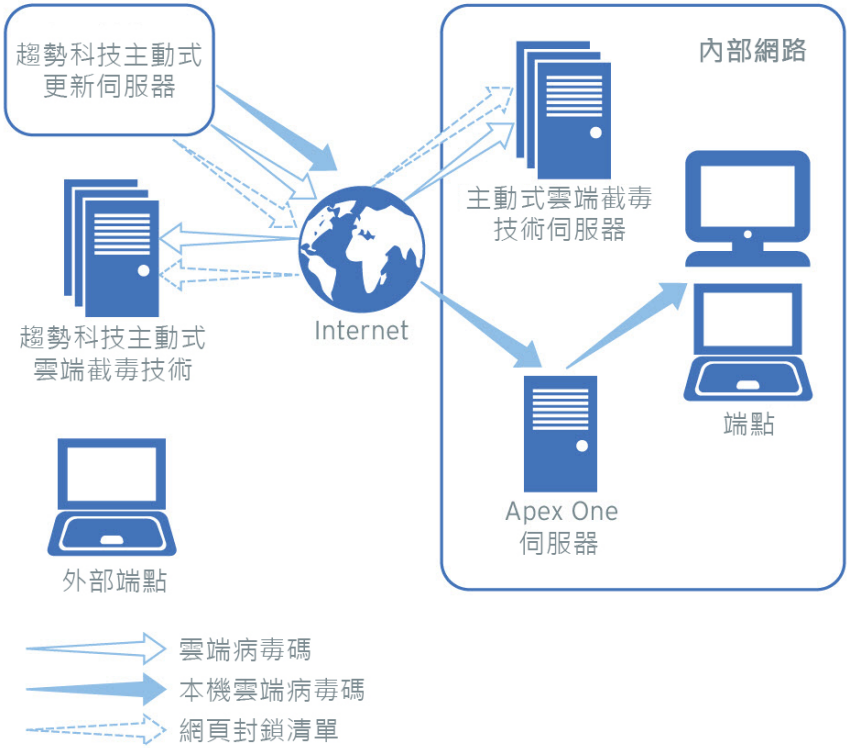


圖 4-1. 病毒碼更新程序

主動雲端截毒技術病毒碼的使用

Security Agent 會使用本機雲端病毒碼掃瞄安全威脅，且僅當本機雲端病毒碼無法確定檔案的風險才會查詢雲端截毒掃瞄病毒碼。在使用者嘗試存取網站

時，用戶端會查詢網頁封鎖清單。進階過濾技術可讓用戶端「快取」查詢結果。這樣便不需要多次傳送相同的查詢。

目前在 Intranet 中的用戶端可以連線到主動雲端截毒技術伺服器，以查詢雲端截毒掃瞄病毒碼或網頁封鎖清單。必須有網路連線，才能連線到主動雲端截毒技術伺服器。如果已設定多部主動雲端截毒技術伺服器，管理員可以決定連線優先順序。

秘訣

請安裝多個主動雲端截毒技術伺服器，以防萬一與某個主動雲端截毒技術伺服器的連線無法使用時，還是能夠繼續提供防護。

目前不在 Intranet 中的用戶端則可以連線到趨勢科技主動雲端截毒技術來查詢。要連線到主動雲端截毒技術，必須提供 Internet 連線。

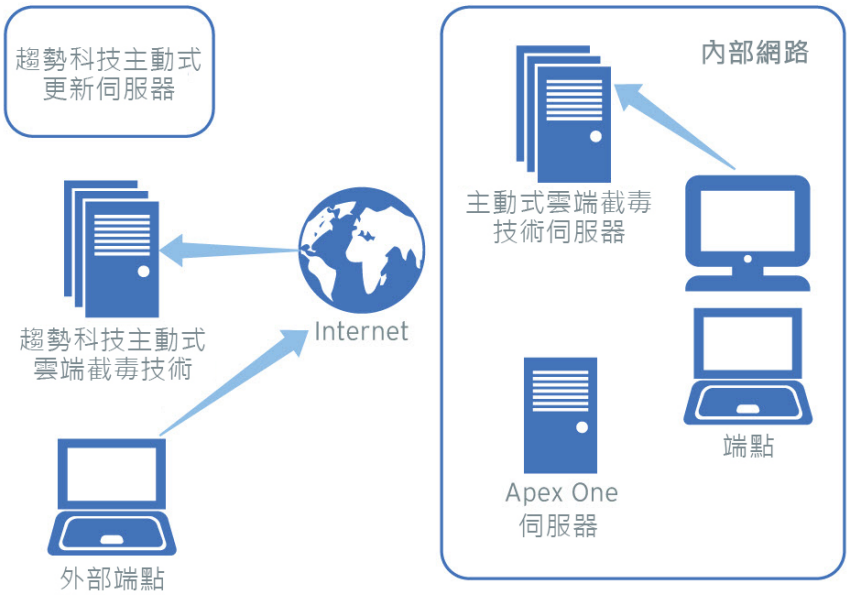


圖 4-2. 查詢程序

無法存取網路或 Internet 的用戶端仍能享有由本機雲端病毒碼和包含先前查詢結果的快取所提供的防護。僅當需要執行新查詢且用戶端在重複嘗試後仍無法連接主動雲端截毒技術來源時，防護才會降低。在這種情況下，用戶端會將檔案標記為需進行驗證並暫時允許存取該檔案。當與主動式雲端截毒伺服器來源之間的連線恢復時，便會重新掃瞄所有已標示的檔案。接著，會對已確認為威脅的檔案執行適當的處理行動。

下表根據用戶端位置概述了防護範圍。

表 4-2. 根據位置的防護行為

位置	病毒碼檔案和查詢行為
存取內部網路	• 病毒碼檔案：用戶端會從 Apex One 伺服器或自訂更新來源下載本機雲端病毒碼檔案。 • 檔案和網頁信譽評等查詢：用戶端連線到主動雲端截毒技術伺服器進行查詢。
無法使用 Intranet 但可連線到主動雲端截毒技術	• 病毒碼檔案：除非用戶端可以連線到 Apex One 伺服器或自訂更新來源，否則無法下載最新的本機雲端病毒碼檔案。 • 檔案和網頁信譽評等查詢：用戶端連線到主動雲端截毒技術網路進行查詢。
無法使用內部網路且無法連線到主動雲端截毒技術	• 病毒碼檔案：除非用戶端可以連線到 Apex One 伺服器或自訂更新來源，否則無法下載最新的本機雲端病毒碼檔案。 • 檔案和網頁信譽評等查詢：用戶端不會接收查詢結果，必須仰賴本機雲端病毒碼和包含先前查詢結果的快取。

設定主動雲端截毒技術服務

請確定已正確設定主動雲端截毒技術環境，用戶端才能利用檔案信譽評等服務和網頁信譽評等服務。請檢查下列項目：

- 主動雲端截毒技術伺服器安裝 第 4-12 頁
- 整合式主動雲端截毒技術伺服器管理 第 4-16 頁

主動雲端截毒技術伺服器安裝

如果用戶端數目不超過 1,000，您可以安裝整合式或獨立式主動雲端截毒技術伺服器。如果用戶端數目超過 1,000，請安裝獨立式主動雲端截毒技術伺服器。

趨勢科技建議您安裝多部主動雲端截毒技術伺服器，以供容錯移轉之用。無法連線到特定伺服器的用戶端，會嘗試連線到您所設定的其他伺服器。

由於整合式伺服器與 Apex One 伺服器在同一個端點上執行，因此在這兩部伺服器的尖峰流量期間內，端點的效能可能會大幅降低。請考慮使用獨立式主動雲端截毒技術伺服器做為用戶端的主要主動雲端截毒技術來源，並使用整合式伺服器做為備用。

獨立式主動雲端截毒技術伺服器安裝

如需有關安裝和管理獨立式主動雲端截毒技術伺服器的指示，請參閱《主動雲端截毒技術伺服器安裝和升級手冊》。

整合式主動雲端截毒技術伺服器安裝

如果在 Apex One 伺服器安裝期間安裝了整合式伺服器：

- 啟動整合式伺服器並設定該伺服器的設定。如需詳細資訊，請參閱整合式主動雲端截毒技術伺服器管理 第 4-16 頁。
- 如果整合式伺服器和 Security Agent 位於同一台伺服器電腦上，請考慮關閉 Apex One 防火牆。Apex One 防火牆是設計給用戶端端點使用，在伺服

器上啟動它可能會影響效能。如需關閉防火牆的指示，請參閱啟動或關閉 Apex One 防火牆 第 13-5 頁。

注意

請考量關閉防火牆的影響，並確定這樣做符合您的安全計劃。

秘訣

在使用整合式主動雲端截毒技術伺服器工具 第 4-13 頁完成 Apex One 安裝後，再安裝整合式主動雲端截毒技術伺服器。

整合式主動雲端截毒技術伺服器工具

趨勢科技整合式主動雲端截毒技術工具可協助管理員在 Apex One 伺服器安裝完成後，安裝或解除安裝整合式主動雲端截毒技術伺服器。Apex One Web 主控台不允許管理員在 Apex One 伺服器安裝完成後再安裝/移除整合式主動雲端截毒技術伺服器。

步驟

1. 開啟命令提示並移至 `ISPSInstaller.exe` 所在的 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\ISPSInstaller 目錄。
2. 使用下列命令之一執行 `ISPSInstaller.exe`：

表 4-3. 安裝程式選項

命令	說明
`ISPSInstaller.exe /i`	使用預設通訊埠設定安裝整合式主動雲端截毒技術伺服器。 如需有關預設通訊埠設定的詳細資訊，請參閱下表。

命令	說明
`ISPSInstaller.exe /i /f:[通訊埠號碼] /s:[通訊埠號碼] /w:[通訊埠號碼]`	使用指定的通訊埠安裝整合式主動雲端截毒技術伺服器： **注意** 使用 Apache Web 伺服器時，您僅能設定主機。 說明： • `/f:[通訊埠號碼]` 代表 HTTP 檔案信譽評等通訊埠 • `/s:[通訊埠號碼]` 代表 HTTPS 檔案信譽評等通訊埠 • `/w:[通訊埠號碼]` 代表網頁信譽評等通訊埠 **注意** 會為未指定的通訊埠自動指派預設值。
`ISPSInstaller.exe /u`	解除安裝整合式主動雲端截毒技術伺服器

表 4-4. 整合式主動雲端截毒技術伺服器的信譽評等服務之通訊埠

Web 伺服器和設定	檔案信譽評等服務的通訊埠		網頁信譽評等服務的 HTTP 通訊埠
	HTTP	HTTPS (SSL)	
IIS 預設網站（已啟動 SSL）	80	443（不可設定）	80（不可設定）
IIS 預設網站（已關閉 SSL）	80	443（不可設定）	80（不可設定）
IIS 虛擬網站（已啟動 SSL）	8080	4343（可設定）	8080（可設定）
IIS 虛擬網站（已關閉 SSL）	8080	4343（可設定）	8080（可設定）

3. 安裝完成後，請開啟 Apex One Web 主控台並驗證以下項目：
   - 開啟 Microsoft 管理主控台（請在「開始」功能表輸入 `services.msc`）並確認 Trend Micro Local Web Classification Server 和 Trend Micro Smart Scan Server 已列為「已啟動」狀態。
   - 開啟「Windows 工作管理員」。在程序標籤中，確認 `iCRCService.exe` 和 `LWCSService.exe` 正在執行，
   - 在 Apex One Web 主控台上，確認功能表項目「管理 > 主動式雲端截毒技術 > 整合式伺服器」已顯示。

主動雲端截毒技術伺服器最佳做法

透過執行以下操作來最佳化主動雲端截毒技術伺服器的效能：

- 避免同時執行手動掃瞄和預約掃瞄。以群組方式交錯進行掃瞄。
- 避免將所有用戶端都設為同時執行「立即掃瞄」。
- 透過變更 `ptngrowth.ini` 檔案，自訂主動雲端截毒技術伺服器以進行較慢的網路連線（約 512Kbps）。

為獨立式伺服器自訂 ptngrowth.ini

步驟

1. 開啟 `/var/tmcss/conf/` 中的 `ptngrowth.ini` 檔案。
2. 使用以下的建議值，修改 `ptngrowth.ini` 檔案：
   - `[COOLDOWN]`
   - `ENABLE=1`
   - `MAX_UPDATE_CONNECTION=1`
   - `UPDATE_WAIT_SECOND=360`

3. 儲存 ptngrowth.ini 檔案。
4. 透過在命令列介面 (CLI) 中輸入以下命令，重新啟動 lighttpd 服務：
   - `service lighttpd restart`

為整合式伺服器自訂 ptngrowth.ini

步驟

1. 開啟 <伺服器安裝資料夾>\PCCSRV\WSS\ 中的 ptngrowth.ini 檔案。
2. 使用以下的建議值，修改 ptngrowth.ini 檔案：
   - `[COOLDOWN]`
   - `ENABLE=1`
   - `MAX_UPDATE_CONNECTION=1`
   - `UPDATE_WAIT_SECOND=360`
3. 儲存 ptngrowth.ini 檔案。
4. 重新啟動 趨勢科技主動雲端截毒技術伺服器 服務。

整合式主動雲端截毒技術伺服器管理

透過執行以下工作來管理整合式主動雲端截毒技術伺服器：

- 啟動整合式伺服器的檔案信譽評等服務和網頁信譽評等服務
- 記錄整合式伺服器的位址
- 更新整合式伺服器的元件
- 設定整合式伺服器的核可/封鎖的 URL 清單

如需詳細資訊，請參閱設定整合式主動雲端截毒技術伺服器設定 第 4-19 頁。

啟動整合式伺服器的檔案信譽評等服務和網頁信譽評等服務

如果要讓用戶端傳送掃瞄和網頁信譽評等查詢至整合式伺服器，必須啟動檔案信譽評等服務和網頁信譽評等服務。透過啟動這些服務，整合式伺服器還可以從主動式更新伺服器更新元件。

如果您在 Apex One 伺服器安裝期間選擇安裝整合式伺服器，則會自動啟動這些服務。

如果您關閉這些服務，請務必安裝獨立式主動雲端截毒技術伺服器，以便用戶端可以向其傳送查詢。

如需詳細資訊，請參閱設定整合式主動雲端截毒技術伺服器設定 第 4-19 頁。

記錄整合式伺服器的位址

為內部用戶端設定主動雲端截毒技術來源清單時，將需要整合式伺服器的位址。如需有關此清單的詳細資訊，請參閱主動雲端截毒技術來源清單 第 4-20 頁。

在用戶端傳送掃瞄查詢至整合式伺服器時，會透過兩個檔案信譽評等服務位址（HTTP 或 HTTPS 位址）中的一個來識別伺服器。透過 HTTPS 位址的連線更安全，而 HTTP 連線使用的頻寬較少。

在用戶端傳送網頁信譽評等查詢時，會透過整合式伺服器的網頁信譽評等服務位址來識別該伺服器。

秘訣

由其他 Apex One 伺服器管理的用戶端也可以連線到這部整合式伺服器。在其他 Apex One 伺服器的 Web 主控台上，將整合式伺服器的位址新增到主動雲端截毒技術伺服器來源清單。

如需詳細資訊，請參閱設定整合式主動雲端截毒技術伺服器設定 第 4-19 頁。

更新整合式伺服器的元件

整合式伺服器會更新以下元件：

- 雲端病毒碼：Security Agent 會將掃瞄查詢傳送至整合式伺服器，並與雲端病毒碼比對來確認潛在的安全威脅。
- 網頁封鎖清單：受網頁信譽評等策略約束的 Security Agent 會傳送網頁信譽評等查詢至整合式伺服器，並比對網頁封鎖清單來確認網站的信譽。

您可以手動更新這些元件或設定更新預約時程。整合式伺服器會從主動式更新伺服器下載元件。

注意

您無法直接從趨勢科技主動式更新伺服器更新純 IPv6 整合式伺服器。如果要允許整合式伺服器連線到主動式更新伺服器，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。

如需詳細資訊，請參閱設定整合式主動雲端截毒技術伺服器設定 第 4-19 頁。

整合式伺服器的核可/封鎖 URL 清單設定

用戶端會維護自己的核可/封鎖的 URL 清單。請在設定網頁信譽評等策略時設定用戶端的清單（如需詳細資訊，請參閱網頁信譽評等策略 第 12-4 頁）。系統會自動允許或封鎖用戶端的清單中的任何 URL。

整合式伺服器具有自己的核可/封鎖的 URL 清單。如果 URL 不在用戶端的清單中，用戶端會傳送網頁信譽評等查詢至整合式伺服器（如果該整合式伺服器已被指定為主動雲端截毒技術來源）。如果在整合式伺服器的核可/封鎖的 URL 清單中找到該 URL，整合式伺服器會通知用戶端允許或封鎖該 URL。

注意

封鎖的 URL 清單具有的優先順序高於網頁封鎖清單。

如果要將 URL 新增到整合式伺服器的核可/封鎖的清單，請從獨立式主動雲端截毒技術伺服器中匯入清單。您無法手動新增 URL。

如需詳細資訊，請參閱設定整合式主動雲端截毒技術伺服器設定 第 4-19 頁。

設定整合式主動雲端截毒技術伺服器設定

步驟

1. 移至「管理 > 主動式雲端截毒技術 > 整合式伺服器」。
2. 選取「啟動檔案信譽評等服務」。
3. 選取用戶端傳送掃瞄查詢至整合式伺服器時將使用的通訊協定（HTTP 或 HTTPS）。
4. 選取「啟動網頁信譽評等服務」。
5. 記錄在「伺服器位址」欄下找到的整合式伺服器的位址。
6. 如果要更新整合式伺服器的元件：
   - 檢視雲端病毒碼和網頁封鎖清單的目前版本。如果有更新可用，請點選「立即更新」。更新結果會顯示在畫面頂端。
   - 如果要自動更新病毒碼：
     a. 選取「啟動預約更新」。
     b. 選擇要每小時更新一次還是每 15 分鐘更新一次。
     c. 選取「檔案信譽評等服務」下的更新來源。將從此來源更新雲端病毒碼。
     d. 選取「網頁信譽評等服務」下的更新來源。將從此來源更新網頁封鎖清單。

注意

- 如果選擇主動式更新伺服器作為更新來源，請確定伺服器有 Internet 連線；如果使用 Proxy 伺服器，請測試是否可以使用 Proxy 設定建立 Internet 連線。如需詳細資訊，請參閱用於 Apex One 伺服器更新的 Proxy 第 6-17 頁。
- 如果選擇自訂更新來源，請為此更新來源設定適當的環境和更新資源。此外，請確定伺服器電腦與此更新來源之間的連線正常。如果需要設定更新來源的協助，請聯絡您的經銷商。

7. 如果要設定整合式伺服器的核可/封鎖清單：
   a. 請點選「匯入」使用預先格式化的 .csv 檔案中的 URL 填入該清單。您可以從獨立式主動雲端截毒技術伺服器中取得 .csv 檔案。
   b. 如果具有現成清單，請點選「匯出」將該清單儲存為 .csv 檔案。
8. 請點選「儲存」。

主動雲端截毒技術來源清單

用戶端在掃瞄安全威脅並判定網站的信譽時，會傳送查詢至主動雲端截毒伺服器來源。

主動雲端截毒伺服器來源的 IPv6 支援

純 IPv6 用戶端無法將查詢直接傳送到純 IPv4 來源，例如：

- 趨勢科技主動雲端截毒技術

同樣，純 IPv4 用戶端無法將查詢傳送至純 IPv6 主動雲端截毒技術伺服器。

如果要使用用戶端連線到來源，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。

主動雲端截毒伺服器來源和端點位置

用戶端所連線的主動雲端截毒技術來源取決於用戶端端點的位置。

如需設定位置設定的詳細資訊，請參閱端點位置 第 15-2 頁。

表 4-5. 主動雲端截毒伺服器來源（依位置）

位置	主動雲端截毒伺服器來源
外部	外部用戶端會將掃瞄和網頁信譽評等查詢傳送至趨勢科技主動雲端截毒技術。
內部	內部用戶端會將掃瞄和網頁信譽評等查詢傳送至主動雲端截毒技術伺服器或趨勢科技主動雲端截毒技術。 如果您已安裝主動雲端截毒技術伺服器，請在 Apex One Web 主控台上設定主動雲端截毒技術來源清單。內部用戶端在需要進行查詢時，會從此清單中挑選伺服器。如果用戶端無法連線到第一部伺服器，則會挑選清單上的另一部伺服器。 秘訣 請將獨立式主動雲端截毒技術伺服器指定為主要掃瞄來源，而將整合式伺服器指定為備用來源。如此可降低導向至代管 Apex One 伺服器與整合式伺服器之端點的傳輸。獨立式伺服器也可以處理更多查詢。 您可以設定主動雲端截毒伺服器來源的標準清單或自訂清單。標準清單供所有內部用戶端使用。自訂清單定義 IP 位址範圍。如果某個內部用戶端的 IP 位址在範圍之內，則該用戶端會使用自訂清單。

設定主動雲端截毒伺服器來源標準清單

步驟

1. 移至「管理 > 主動式雲端截毒技術 > 主動式雲端截毒技術來源」。
2. 請點選「內部用戶端」標籤。
3. 選取「使用標準清單 (適用於所有內部用戶端)」。

4. 請點選「標準清單」連結。

   接著會開啟一個新畫面。

5. 請點選「新增」。

   接著會開啟一個新畫面。

6. 指定主動雲端截毒技術伺服器的主機名稱或 IPv4/IPv6 位址。如果指定的是 IPv6 位址，則使用括號將該位址括起來。

   注意

   如果有 IPv4 和 IPv6 用戶端連線到主動雲端截毒技術伺服器，請指定主機名稱。

7. 選取「檔案信譽評等服務」。用戶端會使用 HTTP 或 HTTPS 通訊協定傳送掃瞄查詢。HTTPS 可進行較為安全的連線，而 HTTP 則使用較少的頻寬。

   a. 如果希望用戶端使用 HTTP，請輸入伺服器用來監聽 HTTP 要求的通訊埠。如果希望用戶端使用 HTTPS，請選取 SSL 並輸入伺服器用來監聽 HTTPS 要求的通訊埠。

   b. 請點選「測試連線」，以檢查是否可以建立到伺服器的連線。

   秘訣

   監聽通訊埠構成伺服器位址的一部分。取得伺服器位址：

   若使用整合式伺服器，請開啟 Apex One Web 主控台並移至「管理 > 主動式雲端截毒技術 > 整合式伺服器」。

   若使用獨立式伺服器，請開啟獨立式伺服器主控台並前往「摘要」畫面。

8. 選取「網頁信譽評等服務」。用戶端會使用 HTTP 通訊協定傳送網頁信譽評等查詢。不支援 HTTPS。

   a. 輸入伺服器用來監聽 HTTP 要求的通訊埠。

   b. 請點選「測試連線」，以檢查是否可以建立到伺服器的連線。

9. 請點選「儲存」。

   畫面隨即關閉。

10. 透過重複以上步驟來新增更多伺服器。

11. 在畫面頂端，選取「順序」或「隨機」。

    - 順序：用戶端會依伺服器出現在清單中的順序來挑選伺服器。如果您選取「順序」，請使用「順序」欄下的箭頭，在清單中上下移動伺服器。
    - 隨機：用戶端隨機挑選伺服器。

    秘訣

    由於整合式主動雲端截毒技術伺服器與 Apex One 伺服器在同一個端點上執行，因此在這兩部伺服器的尖峰流量期間內，端點的效能可能會大幅降低。為了減少導向 Apex One 伺服器電腦的流量，請將獨立式主動雲端截毒技術伺服器指定為主要主動雲端截毒伺服器來源，而將整合式伺服器指定為備份來源。

12. 在畫面中執行其他工作。

    - 如果您已從其他伺服器匯出清單，而想要將此清單匯入此畫面，請點選「匯入」，然後尋找 .dat 檔案。此清單會載入至畫面上。
    - 如果要將清單匯出為 .dat 檔案，請點選「匯出」，再請點選「儲存」。
    - 如果要重新整理伺服器的服務狀態，請點選「重新整理」。
    - 請點選伺服器名稱以執行下列其中一項作業：
        - 檢視或編輯伺服器資訊。
        - 檢視網頁信譽評等服務或檔案信譽評等服務的完整伺服器位址。
    - 如果要開啟主動雲端截毒技術伺服器的主控台，請點選「啟動主控台」。
        - 若為整合式主動雲端截毒技術伺服器，將會顯示伺服器的組態設定畫面。

- 若為獨立式主動雲端截毒技術伺服器與其他 Apex One 伺服器的整合式主動雲端截毒技術伺服器，則會顯示主控台登入畫面。

- 如果要刪除某個項目，請選取該伺服器的核取方塊，然後請點選「刪除」。

13. 請點選「儲存」。

    畫面隨即關閉。

14. 請點選「通知所有用戶端」。

設定主動雲端截毒伺服器來源自訂清單

步驟

1. 移至「管理 > 主動式雲端截毒技術 > 主動式雲端截毒技術來源」。
2. 請點選「內部用戶端」標籤。
3. 選取「使用以用戶端 IP 位址為基礎的自訂清單」。
4. （選用）選取「如果自訂清單中的所有伺服器均無法使用，則使用標準清單」。

   秘訣

   趨勢科技建議啟動此功能，確保萬一自訂來源變得無法使用，用戶端可以連線到主動雲端截毒技術來源。

5. 請點選「新增」。

   接著會開啟一個新畫面。

6. 在「IP 範圍」區段中，指定 IPv4 或 IPv6 位址範圍，或兩者都指定。

注意

使用 IPv4 位址的用戶端可以連接純 IPv4 或雙堆疊主動雲端截毒技術伺服器。使用 IPv6 位址的用戶端可以連接純 IPv6 或雙堆疊主動雲端截毒技術伺服器。同時使用 IPv4 和 IPv6 位址的用戶端可以連接任何主動雲端截毒技術伺服器。

7. 在「Proxy 設定」區段中，指定將用於連線到主動雲端截毒技術伺服器的 Proxy 設定用戶端。

   a. 選取「使用 Proxy 伺服器進行用戶端與主動雲端截毒技術伺服器通訊」。

   b. 指定 Proxy 伺服器名稱或 IPv4/IPv6 位址，以及通訊埠號碼。

   c. 如果 Proxy 伺服器需要驗證，請輸入使用者名稱和密碼。

8. 在「自訂主動雲端截毒技術伺服器清單」中，新增主動雲端截毒技術伺服器。

   a. 指定主動雲端截毒技術伺服器的主機名稱或 IPv4/IPv6 位址。如果指定的是 IPv6 位址，則使用括號將該位址括起來。

      注意

      如果有 IPv4 和 IPv6 用戶端連線到主動雲端截毒技術伺服器，請指定主機名稱。

   b. 選取「檔案信譽評等服務」。用戶端會使用 HTTP 或 HTTPS 通訊協定傳送掃瞄查詢。HTTPS 可進行較為安全的連線，而 HTTP 則使用較少的頻寬。

      i. 如果希望用戶端使用 HTTP，請輸入伺服器用來監聽 HTTP 要求的通訊埠。如果希望用戶端使用 HTTPS，請選取「SSL」並輸入伺服器用來監聽 HTTPS 要求的通訊埠。

      ii. 請點選「測試連線」，以檢查是否可以建立到伺服器的連線。

秘訣

監聽通訊埠構成伺服器位址的一部分。取得伺服器位址：

若使用整合式伺服器，請開啟 Apex One Web 主控台並移至「管理 > 主動式雲端截毒技術 > 整合式伺服器」。

若使用獨立式伺服器，請開啟獨立式伺服器主控台並前往「摘要」畫面。

c. 選取「網頁信譽評等服務」。用戶端會使用 HTTP 通訊協定傳送網頁信譽評等查詢。不支援 HTTPS。

   i. 輸入伺服器用來監聽 HTTP 要求的通訊埠。

   ii. 請點選「測試連線」，以檢查是否可以建立到伺服器的連線。

d. 請點選「新增到清單」。

e. 透過重複以上步驟來新增更多伺服器。

f. 選取「順序」或「隨機」。

   - 順序：用戶端會依伺服器出現在清單中的順序來挑選伺服器。如果您選取「順序」，請使用「順序」欄下的箭頭，在清單中上下移動伺服器。
   - 隨機：用戶端隨機挑選伺服器。

秘訣

由於整合式主動雲端截毒技術伺服器與 Apex One 伺服器是在同一部電腦上執行，因此在這兩部伺服器的尖峰流量期間，電腦的效能可能會大幅降低。為了減少導向 Apex One 伺服器電腦的流量，請將獨立式主動雲端截毒技術伺服器指定為主要主動雲端截毒伺服器來源，而將整合式伺服器指定為備份來源。

g. 在畫面中執行其他工作。

   - 如果要重新整理伺服器的服務狀態，請點選「重新整理」。
   - 如果要開啟主動雲端截毒技術伺服器的主控台，請點選「啟動主控台」。

- 若為整合式主動雲端截毒技術伺服器，將會顯示伺服器的組態設定畫面。
- 若為獨立式主動雲端截毒技術伺服器與其他 Apex One 伺服器的整合式主動雲端截毒技術伺服器，則會顯示主控台登入畫面。

- 如要刪除項目，請點選「刪除」()。

9. 請點選「儲存」。

   畫面隨即關閉。剛才新增的清單會顯示為「IP 範圍」表格下的 IP 範圍連結。

10. 重複步驟 4 到步驟 8，可新增更多自訂清單。

11. 在畫面中執行其他工作。

    - 如果要修改清單，請點選 IP 範圍連結，然後在開啟的畫面中修改設定。
    - 如果要將清單匯出為 .dat 檔案，請點選「匯出」，再請點選「儲存」。
    - 如果您已從其他伺服器匯出清單，而想要將此清單匯入此畫面，請點選「匯入」，然後尋找 .dat 檔案。此清單會載入至畫面上。

12. 請點選「通知所有用戶端」。

用戶端連線 Proxy 設定

如果在連線至主動雲端截毒技術時必須進行 Proxy 驗證，請指定驗證憑證。

設定用戶端在連線至主動雲端截毒技術伺服器時會使用的內部 Proxy 設定。

如需詳細資訊，請參閱 Security Agent Proxy 設定 第 15-42 頁。

端點位置設定

Apex One 具有位置偵測功能，可識別用戶端電腦的位置，並判定用戶端是連線到主動雲端截毒技術還是主動雲端截毒技術伺服器。如此可確保用戶端無論位於何處，都可受到保護。

如果要設定位置設定，請參閱端點位置 第 15-2 頁。

趨勢科技網路病毒牆安裝

如果您已安裝趨勢科技™網路病毒牆™：

- 安裝 Hotfix（對於網路病毒牆 2500，請安裝 Build 1047，而對於網路病毒牆 1200，則安裝 Build 1013）。
- 將 OPSWAT 引擎更新至 2.5.1017 版，讓產品能夠偵測用戶端的掃瞄方法。

使用主動雲端截毒技術服務

正確設定主動雲端截毒技術環境後，用戶端便可以使用檔案信譽評等服務和網頁信譽評等服務。您還可以設定 Smart Feedback 設定。

注意

如需設定主動雲端截毒技術環境的相關指示，請參閱設定主動雲端截毒技術服務 第 4-11 頁。

如果要獲得檔案信譽評等服務提供的防護，用戶端必須使用稱為雲端截毒掃瞄的掃瞄方法。如需雲端截毒掃瞄以及如何在用戶端上啟動雲端截毒掃瞄的詳細資訊，請參閱掃瞄方法類型 第 7-7 頁。

如果要允許 Security Agent 使用網頁信譽評等服務，請設定網頁信譽評等策略。如需詳細資訊，請參閱網頁信譽評等策略 第 12-4 頁。

注意

掃瞄方法和網頁信譽評等策略的設定很精細。您可以根據自己的需求，設定將套用至所有用戶端的設定，也可以為個別用戶端 或用戶端群組設定單獨的設定。

如需設定 Smart Feedback 的相關指示，請參閱 Smart Feedback 第 14-57 頁。

第 5 章

安裝 Security Agent

本章說明 Trend Micro Apex One 系統需求和 Security Agent 安裝程序。

如需有關升級 Security Agent 的詳細資訊，請參閱《Apex One 安裝和升級手冊》。

包含下列主題：

Security Agent 全新安裝

Security Agent 可安裝在執行 Microsoft Windows 平台的電腦上。Apex One 還與各種協力廠商產品相容。

請造訪下列網站，以取得系統需求和相容協力廠商產品的完整清單：

http://docs.trendmicro.com/zh-tw/enterprise/apex-one.aspx

安裝考量

安裝 Security Agent 之前，請先考量下列事項：

表 5-1. Security Agent 安裝考量

注意事項	說明
Windows 功能支援	某些 Security Agent 功能在特定 Windows 平台上無法使用。
IPv6 支援	您可以將 Security Agent 安裝在雙堆疊或純 IPv6 端點上。然而： • 某些可安裝 Security Agent 的 Windows 作業系統不支援 IPv6 定址。 • 對於某些安裝方法，需符合特殊需求才能成功安裝 Security Agent。
Security Agent IP 位址	對於具有 IPv4 和 IPv6 位址的 Security Agent，您可以選擇當 Security Agent 註冊伺服器時要使用的 IP 位址。
例外清單	確認已正確設定下列功能的例外清單： • 行為監控：將重要的端點應用程式新增到「核可的程式」清單，以防止 Security Agent 封鎖這些應用程式。 如需詳細資訊，請參閱行為監控例外清單 第 9-7 頁。 • 網頁信譽評等：將您認為安全的網站新增到「核可的 URL」清單，以防止 Security Agent 封鎖對這些網站的存取。 如需詳細資訊，請參閱網頁信譽評等策略 第 12-4 頁。

Security Agent 功能

端點上可用的 Security Agent 功能取決於作業系統。

表 5-2. 伺服器平台上的 Security Agent 功能

功能	Windows 作業系統			
	Server 2008 R2/Server Core 2008 R2	Server 2012/ Server Core 2012	Server 2016/ Server Core 2016	Server 2019/ Server Core 2019
手動掃瞄、即時掃瞄和預約掃瞄	是	是	是	是
元件更新（手動和預約更新）	是	是	是	是
更新代理程式	是	是	是	是
網頁信譽評等	是，但在安裝伺服器期間預設是關閉的	是，但在安裝伺服器期間預設是關閉的	是，但在安裝伺服器期間預設是關閉的	是，但在安裝伺服器期間預設是關閉的
損害清除及復原服務	是	是	是	是
Apex One 防火牆	是，但在安裝伺服器期間預設是關閉的	是，但在安裝伺服器期間預設是關閉的	是，但在安裝伺服器期間預設是關閉的	是，但在安裝伺服器期間預設是關閉的
行為監控	是（64 位元），但預設是關閉的	是（64 位元），但預設是關閉的	是（64 位元），但預設是關閉的	是（64 位元），但預設是關閉的
下列項目的用戶端自我保護： • 登錄機碼 • 程序 • 服務 • 檔案保護	是	是	是	是

功能	Windows 作業系統			
	Server 2008 R2/Server Core 2008 R2	Server 2012/ Server Core 2012	Server 2016/ Server Core 2016	Server 2019/ Server Core 2019
周邊設備存取控管 （未經授權的變更阻止服務）	是（64 位元），但預設是關閉的	是（64 位元），但預設是關閉的	是（64 位元），但預設是關閉的	是（64 位元），但預設是關閉的
資料安全防護 (包含「周邊設備存取控管」的「資料安全防護」)	是（64 位元），但預設是關閉的	是（64 位元），但預設是關閉的	是（64 位元），但預設是關閉的	是（64 位元），但預設是關閉的
可疑連線設定	是	是	是	是
樣本提交	是	是	是	是
POP3 郵件掃瞄	是	是	是	是
Machine Learning	是	是	是	是
用戶端 Plug-in Manager	是	是	是	是
單機模式	是 (Server) 否 (Server Core)	是	是	是
Smart Feedback	是	是	是	是

表 5-3. 桌面平台上的 Security Agent 功能

功能	Windows 作業系統		
	Windows 7	Windows 8.1	Windows 10
手動掃瞄、即時掃瞄和預約掃瞄	是	是	是
元件更新（手動和預約更新）	是	是	是

功能	Windows 作業系統		
	Windows 7	Windows 8.1	Windows 10
更新代理程式	是	是	是
網頁信譽評等	是	是，但僅部分支援 Windows UI 模式	是
損害清除及復原服務	是	是	是
Apex One 防火牆	是	是	是
行為監控	是（32 位元）	是（32 位元）	是（32 位元）
	是（64 位元）	是（64 位元）	是（64 位元）
下列項目的用戶端自我保護： • 登錄機碼 • 程序 • 服務 • 檔案保護	是	是	是
周邊設備存取控管	是（32 位元）	是（32 位元）	是（32 位元）
（未經授權的變更阻止服務）	是（64 位元）	是（64 位元）	是（64 位元）
資料安全防護	是（32 位元）	是（32 位元）	是（32 位元）
(包含「周邊設備存取控管」的「資料安全防護」)	是（64 位元）	是（64 位元），以桌面模式執行	是（64 位元）
可疑連線設定	是	是	是
樣本提交	是	是	是
POP3 郵件掃瞄	是	是	是
Machine Learning	是	是	是
用戶端 Plug-in Manager	是	是	是

功能	Windows 作業系統		
	Windows 7	Windows 8.1	Windows 10
單機模式	是	是	是
Smart Feedback	是	是	是

Security Agent 安裝和 IPv6 支援

此主題討論將 Security Agent 安裝到雙堆疊或純 IPv6 端點時應考量的事項。

安裝方法

要將 Security Agent 安裝在純 IPv6 或雙堆疊 Security Agent 上，可以使用所有 Security Agent 安裝方法。對於某些安裝方法，需符合特殊需求才能成功地安裝 Security Agent。

您無法使用「ServerProtect 一般伺服器移轉工具」將 ServerProtect™ 移轉到 Security Agent，因為該工具不支援 IPv6 定址。

表 5-4. 安裝方法和 IPv6 支援

安裝方法	需求/考量
Web 安裝網頁和 Browser-based 安裝	安裝頁面的 URL 包含 Apex One 伺服器的主機名稱或其 IP 位址。 如果您要安裝到純 IPv6 Security Agent，伺服器必須是雙堆疊或純 IPv6，而且其主機名稱或 IPv6 位址必須是 URL 的一部分。 對於雙堆疊 Security Agent，安裝狀態畫面中顯示的 IPv6 位址取決於您在「網路」標籤上「用戶端 > 全域用戶端設定」的「偏好的 IP 位址」區段中選取的選項。
用戶端封裝程式	執行封裝程式工具時，您必須選擇是否要將「更新代理程式」權限指定給 Security Agent。請記住，純 IPv6 更新代理程式只能將更新分發到純 IPv6 或雙堆疊 Security Agent。

安裝方法	需求/考量
安全性符合、Vulnerability Scanner 和遠端安裝	純 IPv6 伺服器無法在純 IPv4 端點上安裝 Security Agent。同樣地，純 IPv4 伺服器也無法在純 IPv6 端點上安裝 Security Agent。

用戶端 IP 位址

安裝在支援 IPv6 定址的環境中的 Apex One 伺服器可以管理下列 Security Agent：

- 安裝在純 IPv6 主機上的 Apex One 伺服器可以管理純 IPv6 用戶端。
- 安裝在雙堆疊主機上且已指定 IPv4 和 IPv6 位址的 Apex One 伺服器可以管理純 IPv6、雙堆疊和純 IPv4 用戶端。

安裝或升級用戶端之後，用戶端會使用 IP 位址向伺服器註冊。

- 純 IPv6 用戶端會使用其 IPv6 位址來註冊。
- 純 IPv4 用戶端會使用其 IPv4 位址來註冊。
- 雙堆疊用戶端會使用其 IPv4 或 IPv6 位址來註冊。您可以選擇這些用戶端將使用的 IP 位址。

設定雙堆疊用戶端向伺服器註冊時使用的 IP 位址

只有雙堆疊 Apex One 伺服器可使用此設定，而且此設定僅由雙堆疊用戶端套用。

步驟

1. 移至「用戶端 > 全域用戶端設定」。
2. 請點選「網路」標籤。
3. 移至「偏好的 IP 位址」區段。
4. 請從下列選項選擇：

- 僅 IPv4：用戶端使用其 IPv4 位址。
- 先 IPv4 再 IPv6：用戶端先使用其 IPv4 位址。如果用戶端無法使用其 IPv4 位址來註冊，則會使用其 IPv6 位址。如果使用這兩種 IP 位址進行註冊都不成功，用戶端會使用此選項的 IP 位址優先順序來重試。
- 先 IPv6 再 IPv4：用戶端先使用其 IPv6 位址。如果用戶端無法使用其 IPv6 位址來註冊，則會使用其 IPv4 位址。如果使用這兩種 IP 位址進行註冊都不成功，用戶端會使用此選項的 IP 位址優先順序來重試。

5. 請點選「儲存」。

部署考量

本節提供執行 Security Agent 的全新安裝時可使用的不同 Security Agent 安裝方法的摘要。所有安裝方法都需要目標電腦上的本機管理員權限。

如果您要安裝用戶端且要啟動 IPv6 支援，請閱讀 Security Agent 安裝和 IPv6 支援 第 5-6 頁中的指導方針。

表 5-5. 安裝的部署考量

安裝方法/作業系統支援	部署考量					
	WAN 部署	集中管理	需要使用者的操作	需要 IT 資源	大規模部署	耗用頻寬
Web 安裝網頁 在 Windows Server Core 平台上不支援	否	否	是	否	否	高
電子郵件連結安裝 在 Windows Server Core 平台上不支援	否	否	是	是	否	高（如果同時啟動多個安裝）

安裝方法/作業系統支援	部署考量					
	WAN 部署	集中管理	需要使用者的操作	需要 IT 資源	大規模部署	耗用頻寬
UNC-based 安裝 支援所有作業系統	否	否	是	是	否	高（如果同時啟動多個安裝）
遠端安裝 支援除下列作業系統之外的所有作業系統： • Windows 7 Home Basic/ Home Premium • Windows 8.1（基本版本） • Windows 10 Home Edition	否	是	否	是	否	高
Login Script Setup 支援所有作業系統	否	否	是	是	否	高（如果同時啟動多個安裝）
用戶端封裝程式 支援所有作業系統	否	否	是	是	否	低（如果已經排定）
用戶端封裝程式（透過 Microsoft SMS 部署的 MSI 套件） 支援所有作業系統	是	是	是/否	是	是	低（如果已經排定）
用戶端封裝程式（透過 Active Directory 部署的 MSI 套件） 支援所有作業系統	是	是	是/否	是	是	高（如果同時啟動多個安裝）

安裝方法/作業系統支援	部署考量					
	WAN 部署	集中管理	需要使用者的操作	需要 IT 資源	大規模部署	耗用頻寬
用戶端磁碟映像 支援所有作業系統	否	否	否	是	否	低
Trend Micro Vulnerability Scanner (TMVS) 支援除下列作業系統之外的所有作業系統： • Windows 8.1（基本版本） • Windows 10 Home Edition	否	是	否	是	否	高
安全性符合安裝 支援除下列作業系統之外的所有作業系統： • Windows 7 Home Basic/ Home Premium • Windows 8.1（基本版本） • Windows 10 Home Edition	否	是	否	是	否	高

從 Web 安裝網頁進行安裝

步驟

1. 開啟支援的 Web 瀏覽器視窗，並輸入下列內容：

   `https://<Apex One 伺服器名稱>:<通訊埠>/officescan`

2. 點選登入頁面上的「安裝程式」連結，下載 32 位元或 64 位元 MSI 套件（視您的作業系統而定）。

3. 安裝完成後，Security Agent 圖示會出現在 Windows 系統匣中。

注意

如需系統匣上顯示的圖示清單，請參閱 Security Agent 圖示 第 15-24 頁。

電子郵件連結安裝

設定電子郵件訊息，以指示網路上的使用者安裝 Security Agent。使用者可以請點選電子郵件中提供的 Security Agent 安裝程式連結來開始安裝。

在安裝 Security Agent 之前：

- 檢查 Security Agent 安裝需求。
- 識別網路上有哪些電腦目前沒有受到免於遭受安全威脅的防護。執行下列工作：
  - 執行 Trend Micro Vulnerability Scanner。此工具會根據您指定的 IP 位址範圍，分析端點是否已安裝防毒軟體。

    如需詳細資訊，請參閱 Vulnerability Scanner 使用率 第 5-29 頁。

  - 執行「安全性符合」。

    如需詳細資訊，請參閱適用於未受管端點的安全性符合 第 15-62 頁。

傳送電子郵件連結

如果您要安裝到純 IPv6 用戶端，伺服器必須是雙堆疊或純 IPv6，而且其主機名稱或 IPv6 位址必須是 URL 的一部分。

對於雙堆疊用戶端，安裝狀態畫面中顯示的 IPv6 位址取決於您在「網路」標籤上「OSCE 用戶端設定」用戶端 > 全域用戶端設定的「偏好的 IP 位址」區段中選取的選項。

如需詳細資訊，請參閱用戶端 IP 位址 第 5-7 頁。

步驟

1. 移至「用戶端 > 用戶端安裝 > 電子郵件連結」。
2. 視需要修改電子郵件訊息的主旨行。
3. 請點選「建立電子郵件」。

   會開啟預設郵件程式。
4. 將電子郵件傳送給預期收件者。

執行 UNC-based 安裝

`AutoPcc.exe` 是一個獨立式程式，它能將 Security Agent 安裝到未受保護的端點，並更新程式檔案和元件。端點必須是網域的一部分，才能經由通用命名慣例 (UNC) 路徑使用 AutoPcc。

步驟

1. 移至「用戶端 > 用戶端安裝 > UNC-based」。
   - 如果要使用 `AutoPcc.exe` 將 Security Agent 安裝到未受保護的端點：
     a. 連接到伺服器電腦。移至 UNC 路徑：

        `\\<伺服器電腦名稱>\ofcscan`

b. 以滑鼠右鍵請點選 AutoPcc.exe，然後選取「以系統管理員身分執行」。

- 使用 AutoPcc.exe 進行遠端桌面安裝：

  a. 在主控台模式下開啟遠端桌面連線 (Mstsc.exe)。如此會使 AutoPcc.exe 安裝在作業階段 0 中執行。

  b. 移至 \\<伺服器電腦名稱>\ofcscan 目錄，然後執行 AutoPcc.exe。

從 Apex One Web 主控台遠端安裝

將 Security Agent 遠端安裝到一部或多部連線到網路的端點。您務必要有目標端點的管理員權限，才能執行遠端安裝。遠端安裝不會在已在執行 Apex One 伺服器的端點上安裝 Security Agent。

注意

此安裝方法不可用於執行 Windows 7 Home Basic 與 Home Premium Edition（32 位元和 64 位元版本）、Windows 8.1（32 位元和 64 位元 Basic 版本）或 Windows 10 Home Edition 的端點。純 IPv6 伺服器無法在純 IPv4 用戶端上安裝 Security Agent。同樣地，純 IPv4 伺服器也無法在純 IPv6 用戶端上安裝 Security Agent。

步驟

1. 執行下列安裝前工作。

   a. 開啟一個內建的網域管理者帳號，並為這個帳號設定密碼。

   b. 移至「開始 > 程式集 > 系統管理工具 > 具有進階安全性的 Windows 防火牆」。

   c. 根據您的網路環境，針對「網域」、「私密」和/或「公開」啟動「檔案及印表機共用」規則。

d. 開啟 Microsoft Management Console（按一下「開始 > 執行」，再輸入 `services.msc`），然後啟動「遠端登錄」和「遠端程序呼叫」服務。安裝 Security Agent 時，請使用內建的管理員帳號和密碼。

2. 在 Web 主控台上，移至「用戶端 > 用戶端安裝 > 遠端」。

3. 選取目標端點。

   - 「網域和端點」清單會顯示網路上的所有 Windows 網域。如果要顯示網域下的端點，請按兩下網域名稱。選取任意端點，然後請點選「新增」。
   - 如果您想好特定的端點名稱，請在頁面頂部的「搜尋端點」欄位中輸入該端點名稱，然後按 Enter。

   Apex One 將提示您輸入目標端點使用者名稱和密碼。使用管理員帳號的使用者名稱和密碼以繼續執行。

4. 輸入使用者名稱和密碼，然後請點選「登入」。

   目標端點會出現在「選定的端點」表格中。

5. 重複步驟 3 和 4 以新增更多端點。

6. 當您準備好將 Security Agent 安裝到目標端點時，請點選「安裝」。

   確認方塊便會出現。

7. 請點選「是」確認要將 Security Agent 安裝到目標端點。

   當程式檔案複製到每個目標端點時便會出現進度畫面。

在目標端點上安裝好 Apex One 後，端點名稱會從「選定的端點」清單中消失，並在「網域和端點」清單中以帶有紅色核取記號的形式顯示。

當「網域和端點」清單中的所有目標端點都顯示紅色核取記號時，表示您已完成遠端安裝。

注意

如果您安裝到多個端點，Apex One 會在記錄檔中記錄所有不成功的安裝（如需詳細資訊，請參閱全新安裝記錄檔 第 18-14 頁），但不會延後其他安裝。請點選「安裝」後，您不需要監督安裝。稍後檢查記錄檔，以查看安裝結果。

使用 Login Script Setup 安裝

Login Script Setup 會在未受保護的端點登入網路時，自動將 Security Agent 安裝到這些端點上。Login Script Setup 會將一個名為 `AutoPcc.exe` 的程式新增至伺服器登入程序檔。

`AutoPcc.exe` 會將 Security Agent 安裝到未受管理的端點，並更新程式檔案和元件。端點必須是網域的一部分，才能經由登入程式檔使用 AutoPcc。

Security Agent 安裝

`AutoPcc.exe` 不會自動將 Security Agent 安裝到端點。使用者必須連線到伺服器電腦，移至 `\\<伺服器電腦名稱>\ofcscan`，以滑鼠右鍵請點選 `AutoPcc.exe`，然後選取「以系統管理員身分執行」。

使用 `AutoPcc.exe` 進行遠端桌面安裝：

- 端點必須在 `Mstsc.exe /console mode` 上執行。如此會使 `AutoPcc.exe` 安裝在作業階段 0 中執行。
- 將磁碟機對應到「ofcscan」資料夾，並從該處執行 `AutoPcc.exe`。

程式和元件更新

`AutoPcc.exe` 會更新程式檔案以及防毒、間諜程式防護和「損害清除及復原服務」元件。

Windows Server 程式檔

如果您已經有現有的登入程式檔，Login Script Setup 會附加執行 `AutoPcc.exe` 的指令。否則，Apex One 會建立名稱為 `ofcscan.bat` 的批次檔案，其中包含執行 `AutoPcc.exe` 的命令。

Login Script Setup 會在程式檔的檔尾附加下列命令：

```
\\<Server_name>\ofcscan\autopcc
```

說明：

- `<Server_name>` 是 Apex One 伺服器電腦的端點名稱或 IP 位址。
- "`ofcscan`" 是伺服器上的 Apex One 共享資料夾名稱。
- "`autopcc`" 是指向安裝 Security Agent 的 autopcc 可執行檔案的連結。

登入程式檔位置（透過網路登入共享目錄）：

- `Windows Server 2012:\\Windows 2012 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`
- `Windows Server 2016:\\Windows 2016 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`
- `Windows Server 2019 \\Windows 2019 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`

使用 Login Script Setup 將 autopcc.exe 加入登入程式檔

步驟

1. 在您用來執行伺服器安裝的端點上，從 Windows「開始」功能表中按一下「程式集 > Trend Micro Apex One 伺服器<伺服器名稱> > Login Script Setup」。

   隨即載入 Login Script Setup 公用程式。主控台會顯示樹狀結構，顯示網路上的所有網域。

2. 找出要修改其登入程式檔的伺服器，選取該伺服器，然後請點選「選取」。確定伺服器是網域主控站，而且您已具備該伺服器的管理員存取權。

   Login Script Setup 會提示您輸入使用者名稱和密碼。

3. 輸入使用者名稱和密碼。請點選「確定」繼續。

   會出現「使用者選項」畫面。「使用者」清單會顯示登入該伺服器的使用者資料檔。「選定的使用者」清單會顯示要修改其登入程式檔的使用者資料檔。

4. 如果要修改使用者資料檔的登入程式檔，請從「使用者」清單選取使用者資料檔，然後按一下「新增」。

5. 如果要修改所有使用者的登入程式檔，請點選「全部新增」。

6. 如果要排除之前選取的使用者資料檔，請從「選定的使用者」清單選取名稱，然後請點選「刪除」。

7. 如果要重設選擇，請點選「全部刪除」。

8. 當所有目標使用者資料檔都位於「選定的使用者」清單中時，請點選「套用」。

   此時會出現訊息，通知您已成功修改伺服器登入程式檔。

9. 請點選「確定」。

   Login Script Setup 會返回其初始畫面。

10. 如果要修改其他伺服器的登入程式檔，請重複步驟 2 到 4。

11. 如果要關閉 Login Script Setup，請點選「結束」。

以用戶端封裝程式安裝

「用戶端封裝程式」可建立安裝套件，而且您可以使用傳統媒體（例如 CD-ROM）將安裝套件傳送給使用者。使用者可以在代理程式端點上執行該套件，以安裝或升級 Security Agent 和更新元件。

部署 Security Agent 或元件到低頻寬遠端辦公室的端點時，用戶端封裝程式特別有用。使用用戶端封裝程式安裝的 Security Agent 會向建立該套件的伺服器進行回報。

「用戶端封裝程式」需要下列項目：

- 800MB 的可用磁碟空間
- Windows Installer 2.0（執行 MSI 套件）

套件部署指導方針

將套件傳送給使用者，然後讓他們在其端點上執行 Security Agent 套件。

注意

請僅將套件傳送給其 Security Agent 會向建立套件的所在伺服器回報的使用者。

- 對於 EXE 套件，請以滑鼠右鍵按一下安裝程式檔案，然後按一下「以系統管理員身分執行」。
- 對於 MSI 套件，請執行下列作業：
  1. 執行下列工作以部署套件
     - 使用 Active Directory 部署 MSI 套件 第 5-22 頁
     - 使用 Microsoft SMS 部署 MSI 套件 第 5-23 頁。
  2. 從命令提示字元視窗啟動 MSI 套件，以無訊息方式將 Security Agent 安裝到遠端端點。

用戶端套件的掃瞄方法指導方針

為套件選取掃瞄方法。如需詳細資訊，請參閱掃瞄方法類型 第 7-7 頁。

套件中包含的元件取決於您選取的掃瞄方法。如需每種掃瞄方法可用的元件的詳細資訊，請參閱 Security Agent 更新 第 6-24 頁。

選取掃瞄方法之前，請記住下列指導方針，以便有效率地部署套件：

- 如果您要使用套件將用戶端升級到此 Apex One 版本，請在 Web 主控台上檢查網域等級掃瞄方法。在主控台上，移至「用戶端 > 用戶端管理」，選取用戶端所屬的用戶端樹狀結構網域，然後請點選「設定 > 掃瞄設定 > 掃瞄方法」。網域等級掃瞄方法應該與套件的掃瞄方法一致。
- 如果您要使用套件來執行 Security Agent 的全新安裝，請檢查用戶端分組設定。在 Web 主控台上，移至「用戶端 > 用戶端分組」。
- 如果用戶端是按照 NetBIOS、Active Directory 或 DNS 網域分組，請檢查目標端點所屬的網域。如果網域存在，請檢查為該網域設定的掃瞄方法。如果網域不存在，請檢查根等級掃瞄方法（選取用戶端樹狀結構中的根網域圖示 ( )，然後請點選「設定 > 掃瞄設定 > 掃瞄方法」）。網域或根層級掃瞄方法應該與套件的掃瞄方法一致。
- 如果用戶端是按照自訂用戶端群組分組，請檢查「分組優先順序」和「來源」。

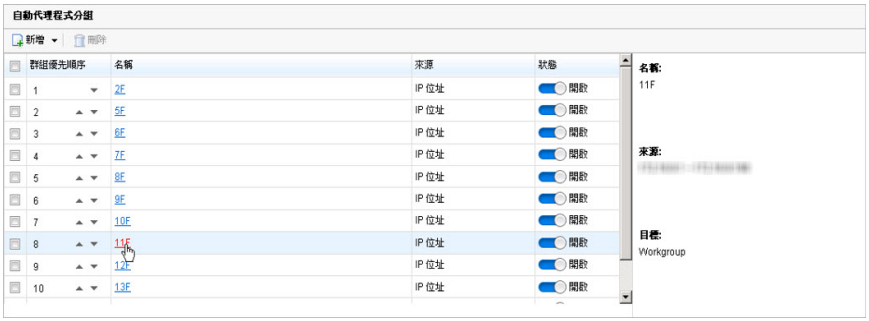


圖 5-1. 「自動用戶端分組」預覽窗格

如果目標端點屬於特定來源，請檢查對應的「目標」。目標是出現在用戶端樹狀結構中的網域名稱。用戶端將在安裝後套用該網域的掃瞄方法。

- 如果您要使用套件來更新使用此 Apex One 版本的用戶端上的元件，請檢查為該用戶端所屬的用戶端樹狀結構網域設定的掃瞄方法。網域等級掃瞄方法應該與套件的掃瞄方法一致。

使用用戶端封裝程式建立安裝套件

步驟

1. 在 Apex One 伺服器電腦上，瀏覽至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\ClientPackager。
2. 按兩下 ClnPack.exe 執行此一工具。

   此時會開啟「用戶端封裝程式」主控台。
3. 選取您要建立的套件類型。

   表 5-6. 用戶端套件類型

套件類型	說明
安裝	選取「安裝」將套件建立為可執行檔案。套件會安裝 Security Agent 程式及伺服器上目前可用的元件。如果目標端點已安裝舊版的用戶端，則執行可執行檔案會升級用戶端。
更新	選取「更新」可以建立包含伺服器上目前可用元件的套件。套件將會建立為可執行檔案。如果更新任何用戶端端點上的元件時發生問題，請使用此套件。
MSI	選取「MSI」可以建立符合 Microsoft Installer 套件格式的套件。套件也會安裝 Security Agent 程式及伺服器上目前可用的元件。如果目標端點已安裝舊版的用戶端，則執行這個 MSI 檔案會升級用戶端。

4. 選取要針對其建立套件的作業系統。僅將套件部署到執行該作業系統類型的端點。如果要部署到其他作業系統類型，請建立其他套件。
5. 選取用戶端套件部署的掃瞄方法。

   如需如何選取掃瞄方法的相關指導方針，請參閱用戶端套件的掃瞄方法指導方針 第 5-18 頁。
6. 在「網域」下，選取下列其中一項：
   - 允許用戶端自動報告其網域：安裝 Security Agent 後，用戶端 會查詢 Apex One 伺服器資料庫並向伺服器回報其網域設定。

- 清單中的任何網域：用戶端封裝程式會與 Apex One 伺服器進行同步，並列出用戶端樹狀結構中目前使用的網域。

7. 在「選項」下，從下列項目中選取：

選項	說明
自動安裝	此選項可建立在背景中安裝在用戶端端點上的套件，不但用戶端不會察覺，而且也不會顯示安裝狀態視窗。如果您規劃將套件遠端部署到目標端點，請啟動此選項。
以最新版本強制覆寫	此選項會使用伺服器上目前可用的元件版本覆寫用戶端上的版本。啟動此選項可確保伺服器上的元件與用戶端上的元件保持同步。
關閉安裝前掃瞄（僅限全新安裝）	如果目標端點未安裝 Security Agent，套件會先掃瞄端點上是否有安全威脅，再安裝 Security Agent。如果您確定目標端點沒有感染安全威脅，則可以關閉安裝前掃瞄。 如果啟動安裝前掃瞄，安裝程式會掃瞄端點最容易遭受攻擊的區域中是否有病毒/惡意程式，這些區域如下： • 開機區和開機目錄（針對開機型病毒） • Windows 資料夾 • Program files 資料夾

8. 在「更新代理程式功能」下，選取更新代理程式可部署的功能。
9. 在「元件」下，選取要加入套件中的元件和功能。
   - 如需有關元件的詳細資訊，請參閱 Apex One 元件和程式 第 6-2 頁。
   - 資料安全防護模組僅在安裝並啟動了資料安全防護後可用。如需有關資料安全防護的詳細資料，請參閱使用資料安全防護 第 3-1 頁。
10. 在「來源檔案」旁確認 `ofcscan.ini` 檔案的位置正確。如果要修改路徑，請點選 (...)，以瀏覽 `ofcscan.ini` 檔案。

    依預設，這個檔案位於 Apex One 伺服器的 <伺服器安裝資料夾>\PCCSRV 資料夾中。
11. 在「輸出檔案」中，請點選(...)，指定要建立 Security Agent 套件的位置，並輸入套件檔案名稱（例如 `AgentSetup.exe`）。

12. 請點選「建立」。

    當「用戶端封裝程式」建立套件之後，會出現「套件建立成功」訊息。在您於上一個步驟指定的目錄中尋找套件。

13. 部署套件。

使用 Active Directory 部署 MSI 套件

利用 Active Directory 的功能，將 MSI 套件同時部署到多個 Security Agent 端點。

如需有關建立 MSI 檔案的指示，請參閱以用戶端封裝程式安裝 第 5-17 頁。

步驟

1. 執行下列工作：

   - Windows Server 2008 R2：

     a. 開啟「群組原則管理主控台」。按一下「開始 > 控制台 > 系統管理工具 > 群組原則管理」。

     b. 在主控台樹狀結構中，展開樹狀結構和網域（包含您要編輯的 GPO）中的「群組原則物件」。

     c. 以滑鼠右鍵請點選您要編輯的 GPO，然後請點選「編輯」。這時會開啟「群組原則物件編輯器」。

   - Windows Server 2012 或更新版本：

     a. 開啟「群組原則管理主控台」。按一下「伺服器管理 > 工具 > 群組原則管理」。

     b. 在主控台樹狀結構中，展開樹狀結構和網域（包含您要編輯的 GPO）中的「群組原則物件」。

     c. 以滑鼠右鍵請點選您要編輯的 GPO，然後請點選「編輯」。這時會開啟「群組原則物件編輯器」。

2. 選擇「電腦設定」或「使用者設定其中一項，然後開啟其下方的「軟體設定」」。

秘訣

趨勢科技建議您使用「電腦設定」而非「使用者設定」，以確保不論登入端點的使用者是誰，都能成功安裝 MSI 套件。

3. 在「軟體設定」下，以滑鼠右鍵請點選「軟體安裝」，然後選取「新增」和「套件」。
4. 找出 MSI 套件並加以選取。
5. 選取部署方法，然後請點選「確定」。
   - 已指定：MSI 套件會在使用者下次登入端點時（如果您已選取「使用者設定」），或是在端點重新啟動時（如果您已選取「電腦設定」）自動部署。這種方法完全不需要使用者的操作。
   - 已發佈：如果要執行 MSI 套件，請通知使用者移至「控制台」，開啟「新增/移除程式」畫面，然後選取在網路上新增/安裝程式的選項。Security Agent 的 MSI 套件顯示時，使用者便可繼續安裝 Security Agent。

使用 Microsoft SMS 部署 MSI 套件

如果您的伺服器上已安裝 Microsoft BackOffice SMS，則可以使用 Microsoft System Management Server (SMS) 來部署 MSI 套件。

如需有關建立 MSI 檔案的指示，請參閱以用戶端封裝程式安裝 第 5-17 頁。

SMS 伺服器必須先從 Apex One 伺服器取得 MSI 檔，才能將套件部署到目標端點。

- 本機：SMS 伺服器和 Apex One 伺服器位於同一個端點上。
- 遠端：SMS 伺服器和 Apex One 伺服器位於不同的端點上。

使用 Microsoft SMS 進行安裝時的已知問題：

- 「未知」出現在 SMS 主控台的「執行時間」欄位中。
- 如果安裝不成功，SMS 程式監視器上的安裝狀態可能仍會顯示安裝已完成。

  如需有關如何檢查安裝是否成功的指示，請參閱安裝後 第 5-53 頁。

如果您使用 Microsoft SMS 2.0 和 2003，則適用下列指示。

在本機取得套件

步驟

1. 開啟「SMS 管理員」主控台。
2. 在「樹狀結構」標籤上，請點選「套件」。
3. 在「動作」功能表上，請點選「新增 > 出自定義的套件」。

   會出現「從定義精靈建立套件」的「歡迎使用」畫面。
4. 按「下一步」。

   會出現「套件定義」畫面。
5. 請點選「瀏覽」。

   會出現「開啟」畫面。
6. 瀏覽並選取由用戶端封裝程式建立的 MSI 套件檔案，然後請點選「開啟」。

   MSI 套件名稱會出現在「套件定義」畫面上。套件會顯示「Security Agent」和程式版本。
7. 按「下一步」。

   會出現「來源檔案」畫面。
8. 請點選「一律由來源目錄取得檔案」，然後按「下一步」。

   會出現「來源目錄」畫面，其中顯示要建立的套件名稱和來源目錄。

9. 請點選「網站伺服器上的本機磁碟機」。
10. 請點選「瀏覽」，然後選取包含 MSI 檔案的來源目錄。
11. 按「下一步」。

    精靈便會建立套件。完成程序後，套件名稱會出現在「SMS 管理員」主控台上。

從遠端取得套件

步驟

1. 在 Apex One 伺服器上，使用用戶端封裝程式建立副檔名為 EXE 的安裝程式套件（您無法建立 MSI 套件）。如需詳細資訊，請參閱以用戶端封裝程式安裝 第 5-17 頁。
2. 在要儲存來源的端點上建立共享資料夾。
3. 開啟「SMS 管理員」主控台。
4. 在「樹狀結構」標籤上，請點選「套件」。
5. 在「動作」功能表上，請點選「新增 > 出自定義的套件」。

   會出現「從定義精靈建立套件」的「歡迎使用」畫面。
6. 按「下一步」。

   會出現「套件定義」畫面。
7. 請點選「瀏覽」。

   會出現「開啟」畫面。
8. 瀏覽 MSI 套件檔案，該檔案位於您建立的共享資料夾內。
9. 按「下一步」。

   會出現「來源檔案」畫面。
10. 請點選「一律由來源目錄取得檔案」，然後按「下一步」。

會出現「來源目錄」畫面。

11. 請點選「網路路徑（UNC 名稱）」。
12. 請點選「瀏覽」，然後選取包含 MSI 檔案的來源目錄（您建立的共享資料夾）。
13. 按「下一步」。

    精靈便會建立套件。完成程序後，套件名稱會出現在「SMS 管理員」主控台上。

將套件分發到目標端點

步驟

1. 在「樹狀結構」標籤上，請點選「通告」。
2. 在「動作」功能表上，請點選「所有工作 > 分發軟體」。

   會出現「分發軟體精靈」的「歡迎使用」畫面。
3. 按「下一步」。

   會出現「套件」畫面。
4. 請點選「分發現有套件」，然後請點選您建立的安裝程式套件名稱。
5. 按「下一步」。

   會出現「散佈點」畫面。
6. 選取您要複製套件的散佈點，然後按「下一步」，

   會出現「通告程式」畫面。
7. 請點選「是」以通告 Security Agent 安裝程式套件，然後按「下一步」。

   會出現「通告目標」畫面。
8. 請點選「瀏覽」以選取目標端點。

   會出現「瀏覽集合」畫面。

9. 請點選「所有 Windows NT 系統」。
10. 請點選「確定」。

    會再度出現「通告目標」畫面。
11. 按「下一步」。

    會出現「通告名稱」畫面。
12. 在文字方塊中，輸入通告的名稱和備註，然後按「下一步」。

    會出現「通告至子集合」畫面。
13. 選擇是否要將套件通告至子集合。選擇只將程式通告至指定集合的成員，或是通告至子集合的成員。
14. 按「下一步」。

    會出現「通告預約時程」畫面。
15. 輸入或選取日期和時間，以指定何時要通告 Security Agent 安裝程式套件。

    注意

    如果要讓 Microsoft SMS 在特定日期停止通告套件，請點選「是，這項通告應到期」，然後在「到期日期和時間」清單方塊中指定日期和時間。
16. 按「下一步」。

    會出現「指定程式」畫面。
17. 請點選「是，指定程式」，然後按「下一步」。

    Microsoft SMS 會建立通告，並將其顯示在「SMS 管理員」主控台上。
18. 當 Microsoft SMS 將已通告的程式（即 Security Agent 程式）分發到目標端點時，每個目標端點上都會顯示一個畫面。指示使用者請點選「是」，然後遵循精靈提供的指示將 Security Agent 安裝到他們的端點上。

使用用戶端磁碟映像的安裝

磁碟映像技術可讓您使用磁碟映像軟體建立 Security Agent 的映像，並且將該映像複製到網路上的其他電腦。

每個 Security Agent 安裝都需要「全域唯一識別碼」(GUID)，如此伺服器才能個別識別用戶端。請使用名為 `imgSetup.exe` 的 Apex One 程式為每個複製的映像建立不同的 GUID。

建立 Security Agent 的磁碟映像

步驟

1. 在端點上安裝 Security Agent。
2. 將 `ImgSetup.exe` 從 <伺服器安裝資料夾>`\PCCSRV\Admin\Utility\ImgSetup` 複製到此端點。
3. 在此端點上執行 `ImgSetup.exe`。

   如此便會在 `HKEY_LOCAL_MACHINE` 下建立 `RUN` 登錄機碼。
4. 使用磁碟映像軟體建立 Security Agent 的磁碟映像。
5. 重新啟動複製。

   `ImgSetup.exe` 將會自動啟動並建立一個新的 GUID 值。Security Agent 會向伺服器回報這個新的 GUID，而伺服器將為新的 Security Agent 建立新記錄。

警告!

為避免在 Apex One 資料庫中出現兩部相同名稱的電腦，請手動變更複製的 Security Agent 的端點名稱或網域名稱。

Vulnerability Scanner 使用率

使用 Vulnerability Scanner 偵測已安裝的防毒解決方案、搜尋網路上未受保護的電腦，並將 Security Agent 安裝到這些電腦上。

使用 Vulnerability Scanner 時的考量

為協助您判斷是否使用 Vulnerability Scanner，請考慮下列事項：

- 網路管理 第 5-29 頁
- 網路拓撲和架構 第 5-30 頁
- 軟體/硬體規格 第 5-30 頁
- 網域結構 第 5-30 頁
- 網路傳輸 第 5-31 頁
- 網路大小 第 5-31 頁

網路管理

表 5-7. 網路管理

安裝	VULNERABILITY SCANNER 的有效性
使用嚴格安全策略進行管理	非常有效。不論所有電腦是否都已安裝防毒軟體，Vulnerability Scanner 都會報告。
分散在不同網站的管理責任	普通有效
集中化管理	普通有效
外包服務	普通有效
使用者管理自己的電腦	無效。因為 Vulnerability Scanner 會掃瞄網路是否有安裝防毒程式，所以讓使用者掃瞄自己的電腦是不可行的。

網路拓撲和架構

表 5-8. 網路拓撲和架構

安裝	VULNERABILITY SCANNER 的有效性
單一位置	非常有效。Vulnerability Scanner 允許您掃瞄整個 IP 網段，並輕鬆地在 LAN 上安裝 Security Agent。
具備高速連線的多個位置	普通有效
具備低速連線的多個位置	無效。您需要在每一個位置執行 Vulnerability Scanner，而且 Security Agent 安裝必須指向本機 Apex One 伺服器。
遠端和隔離電腦	普通有效

軟體/硬體規格

表 5-9. 軟體/硬體規格

安裝	VULNERABILITY SCANNER 的有效性
Windows NT 作業系統	非常有效。Vulnerability Scanner 可以輕鬆地將 Security Agent 遠端安裝到執行 NT 作業系統的電腦。
混合式作業系統	普通有效。Vulnerability Scanner 只能安裝到執行 Windows NT 作業系統的電腦。
桌面管理軟體	無效。Vulnerability Scanner 無法與桌面管理軟體一起使用。不過，它可以協助追蹤 Security Agent 的安裝進度。

網域結構

表 5-10. 網域結構

安裝	VULNERABILITY SCANNER 的有效性
Microsoft Active Directory	非常有效。在 Vulnerability Scanner 中指定網域管理員帳號，允許遠端安裝 Security Agent。

安裝	VULNERABILITY SCANNER 的有效性
工作群組	無效。Vulnerability Scanner 無法安裝到使用不同管理帳號和密碼的電腦。
Novell™ Directory Service	無效。Vulnerability Scanner 需要 Windows 網域帳號才能安裝 Security Agent。
對等式檔案共享	無效。Vulnerability Scanner 無法安裝到使用不同管理帳號和密碼的電腦。

網路傳輸

表 5-11. 網路傳輸

安裝	VULNERABILITY SCANNER 的有效性
LAN 連線	非常有效
512 Kbps	普通有效
T1 連線或更高速的連線	普通有效
撥接	無效。完成 Security Agent 安裝可能會花費很長時間。

網路大小

表 5-12. 網路大小

安裝	VULNERABILITY SCANNER 的有效性
超大型企業	非常有效。網路愈大，愈需要使用 Vulnerability Scanner 來檢查是否安裝 Security Agent。
中小型企業	普通有效。如果是小型網路，也可以選擇 Vulnerability Scanner 來安裝 Security Agent。其他 Security Agent 安裝方法可能實作起來更為容易。

使用 Vulnerability Scanner 安裝 Security Agent 時的指導方針

在下列情況下，Vulnerability Scanner 將不會安裝 Security Agent：

- 目標主機上已安裝 Apex One 伺服器或其他安全防護軟體。
- 遠端端點執行的是 Windows 7 SP1 Home Basic、Windows 7 SP1 Home Premium、Windows 8.1（Basic 版本）或 Windows 10 Home。

注意

您可以使用部署考量 第 5-8 頁中討論的其他安裝方法，將 Security Agent 安裝到目標主機。

使用 Vulnerability Scanner 安裝 Security Agent 之前，請先執行下列步驟：

- 如果是 Windows 7 SP1（Professional、Enterprise、Ultimate Edition）、Windows 8.1（Pro、Enterprise）、Windows 10（Pro、Education、Enterprise）或任何支援的 Windows Server（所有版本）：
  1. 開啟一個內建的管理者帳號，並為這個帳號設定密碼。
  2. 按一下「開始 > 程式集 > 系統管理工具 > 具有進階安全性的 Windows 防火牆」。
  3. 如果是「網域資料檔」、「私密資料檔」和「公開資料檔」，請將防火牆狀態設為「關閉」。
  4. 開啟 Microsoft 管理主控台（請點選「開始」>「執行」，再輸入 `services.msc`），然後啟動「遠端登錄」服務。安裝 Security Agent 時，請使用內建的管理員帳號和密碼。

弱點掃瞄方法

弱點掃瞄可檢查主機上是否有安全防護軟體，並將 Security Agent 安裝到未受保護的主機。

方法	詳細資訊
手動弱點掃瞄	管理員可以視需要執行弱點掃瞄。
預約弱點掃瞄	系統會根據管理員設定的預約自動執行弱點掃瞄。

Vulnerability Scanner 執行之後，它會在目標主機上顯示 Security Agent 狀態。狀態可以是下列任一種：

- 一般：Security Agent 已啟動且正常運作中
- 異常：Security Agent 服務未執行，或 Security Agent 沒有即時防護
- 未安裝：TMListen 服務遺失或未安裝 Security Agent
- 無法連接：Vulnerability Scanner 無法與主機建立連線，因此無法判斷 Security Agent 的狀態

執行手動弱點掃瞄

步驟

1. 如果要在 Apex One 伺服器電腦上執行弱點掃瞄，請瀏覽至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\TMVS，然後按兩下 TMVS.exe。隨即顯示「Trend Micro Vulnerability Scanner」主控台。如果要在其他端點上執行弱點掃瞄，請執行下列作業：

   a. 在 Apex One 伺服器電腦上，移至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility。

   b. 將 TMVS 資料夾複製到另一個端點。

   c. 在該端點上，開啟 TMVS 資料夾，然後按兩下 TMVS.exe。

      隨即顯示「Trend Micro Vulnerability Scanner」主控台。

   注意

   您無法從「終端機伺服器」啟動此工具。

2. 移至「手動掃瞄」區段。
3. 輸入您要檢查的端點 IP 位址範圍。
   a. 輸入 IPv4 位址範圍。

      注意

      如果在純 IPv4 或雙堆疊主機上執行 Vulnerability Scanner，它只能查詢 IPv4 位址範圍。Vulnerability Scanner 僅支援類別 B 的 IP 位址範圍，例如 `168.212.1.1` 到 `168.212.254.254`。

   b. 對於 IPv6 位址範圍，請輸入 IPv6 字首和長度。

      注意

      如果在純 IPv6 或雙堆疊主機上執行 Vulnerability Scanner，它只能查詢 IPv6 位址範圍。

4. 請點選「設定」。

   會出現「設定」畫面。

5. 設定下列設定：

選項	說明
Ping 設定	弱點掃瞄可以 ping 您在上一步中指定的 IP 位址，以檢查這些位址目前是否在使用中。如果目標主機使用 IP 位址，Vulnerability Scanner 可以判斷該主機的作業系統。 如需詳細資訊，請參閱 Ping 設定 第 5-44 頁。
擷取電腦說明的方法	對於已回應 "ping" 命令的主機，Vulnerability Scanner 可以擷取該主機的其他相關資訊。 如需詳細資訊，請參閱擷取端點說明的方法 第 5-41 頁。
產品查詢	Vulnerability Scanner 可以檢查主機上是否有安全防護軟體。 如需詳細資訊，請參閱產品查詢 第 5-38 頁。

選項	說明
Apex One 伺服器設定	如果想要讓 Vulnerability Scanner 自動將 Security Agent 安裝到未受保護的主機，您可以設定這些設定。這些設定可識別上層伺服器，以及 Security Agent 用來登入主機的系統管理認證。 如需詳細資訊，請參閱 Apex One 伺服器設定 第 5-45 頁。 注意 特定情況可能會造成無法在目標主機上安裝 Security Agent。 如需詳細資訊，請參閱使用 Vulnerability Scanner 安裝 Security Agent 時的指導方針 第 5-32 頁。
通知	Vulnerability Scanner 可將弱點掃瞄結果傳送給 Apex One 管理員。它也可以在未受保護的主機上顯示通知。 如需詳細資訊，請參閱通知 第 5-42 頁。
儲存結果	除了將弱點掃瞄結果傳送給管理員之外，Vulnerability Scan 也可以將結果儲存為 `.csv` 檔案。 如需詳細資訊，請參閱弱點掃瞄結果 第 5-43 頁。

6. 請點選「確定」。
7. 請點選「開始」。

   弱點掃瞄結果會在「手動掃瞄」標籤下的「結果」表格中顯示。
8. 如果要將結果儲存成逗號分隔值 (CSV) 檔案，請點選「匯出」，找到您要儲存檔案的資料夾，然後輸入檔案名稱，再請點選「儲存」。

設定預約弱點掃瞄

步驟

1. 如果要在 Apex One 伺服器電腦上執行弱點掃瞄，請瀏覽至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\TMVS，然後按兩下 `TMVS.exe`。隨即顯示「Trend Micro Vulnerability Scanner」主控台。如果要在其他端點上執行弱點掃瞄，請執行下列作業：

a. 在 Apex One 伺服器電腦上，移至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility。

b. 將 TMVS 資料夾複製到另一個端點。

c. 在該端點上，開啟 TMVS 資料夾，然後按兩下 TMVS.exe。

隨即顯示「Trend Micro Vulnerability Scanner」主控台。

注意

您無法從「終端機伺服器」啟動此工具。

2. 移至「預約掃瞄」區段。
3. 請點選「新增/編輯」。

隨即出現「預約掃瞄」畫面。

4. 輸入預約弱點掃瞄的名稱。
5. 輸入您要檢查的端點 IP 位址範圍。

a. 輸入 IPv4 位址範圍。

注意

如果在純 IPv4 或雙堆疊主機上執行 Vulnerability Scanner，它只能查詢 IPv4 位址範圍。Vulnerability Scanner 僅支援類別 B 的 IP 位址範圍，例如 168.212.1.1 到 168.212.254.254。

b. 對於 IPv6 位址範圍，請輸入 IPv6 字首和長度。

注意

如果在純 IPv6 或雙堆疊主機上執行 Vulnerability Scanner，它只能查詢 IPv6 位址範圍。

6. 使用 24 小時制時間格式指定預約時程的開始時間，然後選取掃瞄的執行頻率。選擇「每日一次」、「每週一次」或「每月一次」。
7. 選取要使用哪一組弱點掃瞄設定。

a. 如果已設定手動弱點掃瞄設定，且想要使用該設定，請選取「使用目前設定」。

   如需有關手動弱點掃瞄設定的詳細資訊，請參閱執行手動弱點掃瞄 第 5-33 頁。

b. 如果未指定手動弱點掃瞄設定，或想要使用另一組設定，請選取「修改設定」，然後請點選「設定」。

   會出現「設定」畫面。

c. 設定下列設定：

Ping 設定	弱點掃瞄可以 ping 您在上一步中指定的 IP 位址，以檢查這些位址目前是否在使用中。如果目標主機使用 IP 位址，Vulnerability Scanner 可以判斷該主機的作業系統。 如需詳細資訊，請參閱 Ping 設定 第 5-44 頁。
擷取電腦說明的方法	對於已回應 "ping" 命令的主機，Vulnerability Scanner 可以擷取該主機的其他相關資訊。 如需詳細資訊，請參閱擷取端點說明的方法 第 5-41 頁。
產品查詢	Vulnerability Scanner 可以檢查主機上是否有安全防護軟體。 如需詳細資訊，請參閱產品查詢 第 5-38 頁。
Apex One 伺服器設定	如果想要讓 Vulnerability Scanner 自動將 Security Agent 安裝到未受保護的主機，您可以設定這些設定。這些設定可識別上層伺服器，以及 Security Agent 用來登入主機的系統管理認證。 如需詳細資訊，請參閱 Apex One 伺服器設定 第 5-45 頁。  注意 特定情況可能會造成無法在目標主機上安裝 Security Agent。 如需詳細資訊，請參閱使用 Vulnerability Scanner 安裝 Security Agent 時的指導方針 第 5-32 頁。

通知	Vulnerability Scanner 可將弱點掃瞄結果傳送給 Apex One 管理員。它也可以在未受保護的主機上顯示通知。 如需詳細資訊，請參閱通知 第 5-42 頁。
儲存結果	除了將弱點掃瞄結果傳送給管理員之外，Vulnerability Scan 也可以將結果儲存為 .csv 檔案。 如需詳細資訊，請參閱弱點掃瞄結果 第 5-43 頁。

8. 請點選「確定」。

   隨即關閉「預約掃瞄」畫面。您建立的預約弱點掃瞄會顯示在「預約掃瞄」區段下。如果已啟動通知，Vulnerability Scanner 會將預約弱點掃瞄結果傳送給您。

9. 如果要立即執行預約弱點掃瞄，請點選「立即執行」。

   弱點掃瞄結果會顯示在「預約掃瞄」標籤下的「結果」表格中。

10. 如果要將結果儲存成逗號分隔值 (CSV) 檔案，請點選「匯出」，找到您要儲存檔案的資料夾，然後輸入檔案名稱，再請點選「儲存」。

弱點掃瞄設定

弱點掃瞄設定是從 Trend Micro Vulnerability Scanner (TMVS.exe) 或 TMVS.ini 檔案設定。

注意

如需有關如何收集 Vulnerability Scanner 偵錯記錄的詳細資訊，請參閱使用 LogServer.exe 的伺服器偵錯記錄檔 第 18-3 頁。

產品查詢

Vulnerability Scanner 可以檢查用戶端上是否有安全防護軟體。下表討論 Vulnerability Scanner 檢查安全防護產品的方法：

表 5-13. Vulnerability Scanner 所檢查的安全防護產品

產品	說明
ServerProtect for Windows	Vulnerability Scanner 使用 RPC 端點來檢查 `SPNTSVC.exe` 是否正在執行。它傳回的資訊包括作業系統和「病毒掃瞄引擎」、「病毒碼」和產品版本。Vulnerability Scanner 無法偵測「ServerProtect 資料伺服器」或「ServerProtect 管理主控台」。
ServerProtect for Linux	如果目標端點未執行 Windows，Vulnerability Scanner 會嘗試連線到通訊埠 14942，檢查電腦是否已安裝 ServerProtect for Linux。
Security Agent	Vulnerability Scanner 使用 Security Agent 通訊埠來檢查是否已安裝 Security Agent。也會檢查 `TmListen.exe` 程序是否正在執行。如果是從預設位置執行，它會自動擷取通訊埠號碼。 如果您是從 Apex One 伺服器以外的任何端點啟動 Vulnerability Scanner，請檢查然後使用該端點的通訊埠。
PortalProtect™	Vulnerability Scanner 會載入 `http://localhost:port/PortalProtect/index.html` 網頁，檢查是否有安裝該產品。
ScanMail™ for Microsoft Exchange™	Vulnerability Scanner 會載入 `http://ipaddress:port/scanmail.html` 網頁，檢查是否有安裝 ScanMail。依預設，ScanMail 會使用第 16372 號通訊埠。如果 ScanMail 使用其他通訊埠號碼，請指定該通訊埠號碼。否則，Vulnerability Scanner 會偵測不到 ScanMail。
InterScan™ 系列產品	Vulnerability Scanner 會載入每個不同產品的網頁，檢查是否有安裝產品。 • InterScan Messaging Security Suite 5.x: `http://localhost:port/eManager/cgi-bin/eManager.htm` • InterScan eManager 3.x: `http://localhost:port/eManager/cgi-bin/eManager.htm` • InterScan VirusWall™ 3.x: `http://localhost:port/InterScan/cgi-bin/interscan.dll`
Trend Micro Internet Security™ (PC-cillin)	Vulnerability Scanner 使用通訊埠 40116 來檢查是否已安裝 Trend Micro Internet Security。

產品	說明
McAfee VirusScan ePolicy Orchestrator	Vulnerability Scanner 會將一個特別的 Token 傳送到 TCP 通訊埠 8081，這是在伺服器與用戶端之間提供連線的 ePolicy Orchestrator 預設通訊埠。具有此防毒產品的端點會使用特別的 Token 類型回應。Vulnerability Scanner 偵測不到單機版 McAfee VirusScan。
Norton Antivirus™ Corporate Edition	Vulnerability Scanner 會將一個特別的 Token 傳送到第 2967 號 UDP 通訊埠，這是 Norton Antivirus Corporate Edition RTVScan 的預設通訊埠。具有此防毒產品的端點會使用特別的 Token 類型回應。由於 Norton Antivirus Corporate Edition 是透過 UDP 進行通訊，因此不保證正確率。而且，網路傳輸可能會影響 UDP 等待時間。

Vulnerability Scanner 使用下列通訊協定來偵測產品和電腦：

- RPC：偵測 ServerProtect for NT
- UDP：偵測 Norton AntiVirus Corporate Edition 用戶端
- TCP：偵測 McAfee VirusScan ePolicy Orchestrator
- ICMP：藉由傳送 ICMP 封包偵測電腦
- HTTP：偵測 Security Agent
- DHCP：如果偵測到 DHCP 要求，Vulnerability Scanner 會檢查發出要求的端點上是否已經安裝防毒軟體。

設定產品查詢設定

產品查詢設定是弱點掃瞄設定的子集合：如需有關弱點掃瞄設定的詳細資訊，請參閱弱點掃瞄方法 第 5-32 頁。

步驟

1. 如果要從 Vulnerability Scanner (`TMVS.exe`) 指定產品查詢設定：
   a. 啟動 `TMVS.exe`。
   b. 請點選「設定」。

      會出現「設定」畫面。

c. 移至「產品查詢」區段。

d. 選取要檢查的產品。

e. 請點選產品名稱旁邊的「設定」，然後指定 Vulnerability Scanner 要檢查的通訊埠號碼。

f. 請點選「確定」。

會關閉「設定」畫面。

2. 如果要設定 Vulnerability Scanner 同時檢查有無安全防護軟體的電腦數量：

a. 移至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\TMVS，然後使用文字編輯器（如記事本）開啟 TMVS.ini。

b. 如果要設定執行手動弱點掃瞄期間要檢查的電腦數量，請變更 ThreadNumManual 的值。請指定介於 8 和 64 之間的值。

例如，如果要讓 Vulnerability Scanner 在同一時間檢查 60 部電腦，請輸入 `ThreadNumManual=60`。

c. 如果要設定執行預約弱點掃瞄期間要檢查的電腦數量，請變更 ThreadNumSchedule 的值。請指定介於 8 和 64 之間的值。

例如，如果要讓 Vulnerability Scanner 在同一時間檢查 50 部電腦，請輸入 `ThreadNumSchedule=50`。

d. 儲存 TMVS.ini。

擷取端點說明的方法

當 Vulnerability Scanner 可以 "ping" 主機時，它可以擷取主機的其他相關資訊。擷取資訊的方法有兩種：

- 快速擷取：僅擷取端點名稱
- 一般擷取：擷取網域和端點資訊

配置擷取設定

擷取設定是弱點掃瞄設定的子集合。如需有關弱點掃瞄設定的詳細資訊，請參閱弱點掃瞄方法 第 5-32 頁。

步驟

1. 啟動 `TMVS.exe`。
2. 請點選「設定」。

   會出現「設定」畫面。
3. 移至「擷取電腦說明的方法」區段。
4. 選取「一般」或「快速」。
5. 如果已選取「一般」，請選取「擷取可用的電腦說明」。
6. 請點選「確定」。

   會關閉「設定」畫面。

通知

Vulnerability Scanner 可將弱點掃瞄結果傳送給 Apex One 管理員。它也可以在未受保護的主機上顯示通知。

設定通知設定

通知設定是弱點掃瞄設定的子集合。如需有關弱點掃瞄設定的詳細資訊，請參閱弱點掃瞄方法 第 5-32 頁。

步驟

1. 啟動 `TMVS.exe`。
2. 請點選「設定」。

   會出現「設定」畫面。

3. 移至「通知」區段。
4. 如果要自動將「弱點掃瞄」結果傳送給您自己或您組織中的其他管理員：
   a. 選取「將結果以電子郵件寄給系統管理員」。
   b. 請點選「設定」，指定電子郵件設定。
   c. 在「收件人」中，輸入收件人的電子郵件信箱。
   d. 在「寄件人」中，輸入寄件者的電子郵件信箱。
   e. 在「SMTP 伺服器」中，輸入 SMTP 伺服器位址。

      例如，輸入 `smtp.company.com`。SMTP 伺服器是必要資訊。
   f. 在「主旨」中，輸入訊息的新主旨或使用預設的主旨。
   g. 請點選「確定」。
5. 如果要通知使用者其電腦未安裝安全防護軟體：
   a. 選取「在未受保護的電腦上顯示通知」。
   b. 請點選「自訂」設定通知訊息。
   c. 在「通知訊息」畫面中輸入新訊息或接受預設訊息。
   d. 請點選「確定」。
6. 請點選「確定」。

   會關閉「設定」畫面。

弱點掃瞄結果

您可以設定 Vulnerability Scanner，以將弱點掃瞄結果儲存為逗號分隔值 (CSV) 檔案。

配置掃瞄結果

弱點掃瞄結果設定是弱點掃瞄設定的子集合。如需有關弱點掃瞄設定的詳細資訊，請參閱弱點掃瞄方法 第 5-32 頁。

步驟

1. 啟動 TMVS.exe。
2. 請點選「設定」。

   會出現「設定」畫面。
3. 移至「儲存結果」區段。
4. 選取「自動將結果儲存到 CSV 檔案」。
5. 如果要變更用來儲存 CSV 檔案的預設資料夾：

   a. 請點選「瀏覽」。

   b. 選取端點或網路上的目標資料夾。

   c. 請點選「確定」。
6. 請點選「確定」。

   會關閉「設定」畫面。

Ping 設定

使用 "ping" 設定來驗證目標電腦是否存在並判斷其作業系統。如果這些設定已關閉，Vulnerability Scanner 會掃瞄所指定 IP 位址範圍中的所有 IP 位址（包含主機未使用的位址），因此掃瞄時間會比預期久。

配置 Ping 設定

Ping 設定是弱點掃瞄設定的子集合。如需有關弱點掃瞄設定的詳細資訊，請參閱弱點掃瞄方法 第 5-32 頁。

步驟

1. 如果要從 Vulnerability Scanner (TMVS.exe) 指定 ping 設定：

   a. 啟動 TMVS.exe。

b. 請點選「設定」。

會出現「設定」畫面。

c. 移至「Ping 設定」區段。

d. 選取「允許「Vulnerability Scanner」Ping 您網路中的電腦以檢查其狀態」。

e. 在「封包大小」和「逾時」欄位中，接受或修改預設值。

f. 選取「使用 ICMP OS 特徵鑑別偵測作業系統類型」。

如果選取此選項，Vulnerability Scanner 會判斷主機是執行 Windows 或其他作業系統。如果主機執行 Windows，Vulnerability Scanner 可以識別其 Windows 版本。

g. 請點選「確定」。

會關閉「設定」畫面。

2. 如果要設定 Vulnerability Scanner 同時 Ping 的電腦數量：

a. 移至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\TMVS，然後使用文字編輯器（如記事本）開啟 TMVS.ini。

b. 變更 EchoNum 的值。請指定介於 1 和 64 之間的值。

例如，如果要 Vulnerability Scanner 在同一時間 ping 60 部電腦，則輸入 `EchoNum=60`。

c. 儲存 TMVS.ini。

Apex One 伺服器設定

在下列情況中，會使用 Apex One 伺服器設定：

- Vulnerability Scanner 將 Security Agent 安裝到未受保護的目標電腦。伺服器設定可讓 Vulnerability Scanner 識別 Security Agent 的上層伺服器，以及登入目標電腦時要使用的系統管理認證。

注意

特定情況可能會造成無法在目標主機上安裝 Security Agent。

如需詳細資訊，請參閱使用 Vulnerability Scanner 安裝 Security Agent 時的指導方針 第 5-32 頁。

- Vulnerability Scanner 會將用戶端安裝記錄檔傳送到 Apex One 伺服器。

配置 Apex One 伺服器設定

Apex One 伺服器設定是弱點掃瞄設定的子集合。如需有關弱點掃瞄設定的詳細資訊，請參閱弱點掃瞄方法 第 5-32 頁。

步驟

1. 啟動 `TMVS.exe`。
2. 請點選「設定」。

   會出現「設定」畫面。
3. 移至「Apex One 伺服器設定」區段。
4. 輸入 Apex One 伺服器名稱和通訊埠號碼。
5. 選取「在未受保護的電腦上自動安裝 Security Agent」。
6. 如果要設定系統管理認證：
   a. 請點選「安裝至帳號」。
   b. 在「帳號資訊」畫面中，輸入使用者名稱和密碼。
   c. 請點選「確定」。
7. 選取「將記錄檔傳送至 Apex One 伺服器」。
8. 請點選「確定」。

   會關閉「設定」畫面。

以安全性符合進行安裝

將 Security Agent 安裝到網路網域中的電腦，或使用目標端點的 IP 位址將 Security Agent 安裝到端點上。

安裝 Security Agent 之前，請注意下列事項：

步驟

1. 記錄每個端點的登入憑證。在安裝期間，Apex One 會提示您指定登入憑證。

2. 在下列情況中，無法在端點上安裝 Security Agent：

   - 端點上已安裝 Apex One 伺服器。
   - 端點執行的是 Windows 7™ Starter、Windows 7 Home Basic、Windows 7 Home Premium、Windows 8.1（基本版本）和 Windows 10 Home。如果您的端點執行這些平台，請選擇另一種安裝方法。如需詳細資訊，請參閱部署考量 第 5-8 頁。

3. 如果目標端點執行的是 Windows 7（Professional、Enterprise 或 Ultimate Edition）、Windows 8.1（Pro、Enterprise）、Windows 10（Pro、Education、Enterprise）、Windows Server 2012 (Standard)、Windows Server 2016（所有版本）或 Windows Server 2019（所有版本），請在端點上執行下列步驟：

   a. 開啟一個內建的管理者帳號，並為這個帳號設定密碼。

   b. 關閉 Windows 防火牆。

   c. 按一下「開始 > 程式集 > 管理工具 > 具有進階安全性的 Windows 防火牆」。

   d. 如果是「網域資料檔」、「私密資料檔」和「公開資料檔」，請將防火牆狀態設為「關閉」。

   e. 開啟 Microsoft 管理主控台（按一下「開始 > 執行」，再輸入 `services.msc`），然後啟動「遠端登錄」服務。安裝 Security Agent 時，請使用內建的管理員帳號和密碼。

4. 如果端點上已安裝趨勢科技或協力廠商端點安全防護程式，請檢查 Apex One 是否可以自動解除安裝該軟體並以 Security Agent 取代。如需 Apex One 會自動解除安裝的用戶端安全防護軟體清單，請開啟位於 <伺服器安裝資料夾>\PCCSRV\Admin 中的下列檔案。您可以使用文字編輯器（例如：記事本）開啟這些檔案。

   - tmuninst.ptn
   - tmuninst_as.ptn

   如果目標端點上的軟體不在此清單中，請先手動解除安裝該軟體。視軟體的解除安裝程序而定，端點不一定要在解除安裝後重新啟動。

安裝 Security Agent

步驟

1. 移至「評估 > 未受管理的端點」。
2. 請點選用戶端樹狀結構頂端的「安裝」。
   - 如果端點上已安裝舊版 Security Agent，當您點選「安裝」時，Apex One 會略過安裝，而且不會將端點升級至此版本。如果要升級端點，請務必設定下列設定。
     a. 移至「用戶端 > 用戶端管理」。
     b. 請點選「設定 > 權限和其他設定 > 其他設定」標籤。
     c. 移至「更新設定」區段。
     d. 在「Security Agent 僅會更新下列元件」下拉式清單中，選取「所有元件（包括 Hotfix 和用戶端程式）」。
     e. 請點選「套用至所有用戶端」。
3. 為每個端點指定管理員登入帳號，然後點選「登入」。Apex One 會開始在目標端點上安裝用戶端。

4. 檢視安裝狀態。

移轉至 Security Agent

將目標端點上安裝的用戶端安全防護軟體取代為 Security Agent。

從其他端點安全防護軟體移轉

安裝 Security Agent 時，安裝程式會檢查目標端點上是否已安裝任何趨勢科技或協力廠商端點安全防護軟體。安裝程式可以自動解除安裝該軟體，並將其取代為 Security Agent。

如需 Apex One 會自動解除安裝的端點安全防護軟體清單，請開啟位於 <伺服器安裝資料夾>\PCCSRV\Admin 中的下列檔案。請使用文字編輯器（例如：記事本）開啟這些檔案。

- tmuninst.ptn
- tmuninst_as.ptn

如果目標端點上的軟體不在此清單中，請先手動解除安裝該軟體。視軟體的解除安裝程序而定，端點不一定要在解除安裝後重新啟動。

Security Agent 移轉問題

- 如果成功自動移轉用戶端，但使用者在安裝後立即遇到 Security Agent 的問題，請重新啟動端點。
- 如果 Apex One 安裝程式繼續安裝 Security Agent，但無法解除安裝其他安全防護軟體，則兩個軟體之間會發生衝突。請解除安裝這兩個軟體，然後使用部署考量 第 5-8 頁中討論的任一安裝方法來安裝 Security Agent。

從 ServerProtect 一般伺服器移轉

「ServerProtect™ 一般伺服器移轉工具」可協助將執行「Trend Micro ServerProtect 一般伺服器」的電腦移轉到 Security Agent。

「ServerProtect 一般伺服器移轉工具」的硬體和軟體規格與 Apex One 伺服器相同。請在執行 Windows Server 平台的電腦上執行此工具。

當成功解除安裝「ServerProtect 一般伺服器」時，此工具便會安裝 Security Agent。它也會將掃瞄例外清單設定（適用於所有掃瞄類型）移轉至 Security Agent。

安裝 Security Agent 時，移轉工具用戶端安裝程式有時可能會逾時並通知您安裝不成功。不過，Security Agent 可能已成功安裝。請從 Apex One Web 主控台驗證在 Security Agent 端點的安裝作業是否成功。

在下列情況下無法成功移轉：

- 遠端用戶端只有一個 IPv6 位址。移轉工具不支援 IPv6 定址。
- 遠端用戶端無法使用 NetBIOS 通訊協定。
- 通訊埠 455、337 和 339 已被封鎖。
- 遠端用戶端無法使用 RPC 通訊協定。
- 遠端登錄服務已停止。

注意

「ServerProtect 一般伺服器移轉工具」不會解除安裝 ServerProtect 的 Trend Micro Apex Central™ 用戶端。如需如何解除安裝該用戶端的指示，請參閱 ServerProtect 和（或）Apex Central 文件。

使用 ServerProtect 一般伺服器移轉工具

步驟

1. 在 Apex One 伺服器電腦上，開啟 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\SPNSXfr，並將檔案 SPNSXfr.exe 和 SPNSX.ini 複製到 <伺服器安裝資料夾>\PCCSRV\Admin。

2. 按兩下 SPNSXfr.exe 以開啟此工具。

   便會開啟「Server Protect 一般伺服器移轉工具」主控台。

3. 選取 Apex One 伺服器。Apex One 伺服器的路徑會出現在「Apex One 伺服器路徑」下。如果路徑不正確，請按一下「瀏覽」，然後在您安裝 Apex One 的目錄中選取 PCCSRV 資料夾。如果要在您下次開啟此工具時讓它再自動尋找 Apex One 伺服器，請選取「自動搜尋伺服器路徑」核取方塊（預設為選取）。

4. 選取執行「ServerProtect 一般伺服器」的電腦以在該電腦上執行移轉，方法是請點選「目標端點」下的任一選項：

   - Windows 網路樹狀結構：顯示網路上的網域樹狀結構。如果要使用此方法選取電腦，請點選要在其中搜尋用戶端電腦的網域。
   - 資料伺服器名稱：依資訊伺服器名稱搜尋。如果要使用此方法選取電腦，請在文字方塊中輸入網路上的「資料伺服器」名稱。如果要搜尋多部「資料伺服器」，請在伺服器名稱之間插入分號（「;」）。
   - 特定的一般伺服器名稱：依一般伺服器名稱搜尋。如果要使用此方法選取電腦，請在文字方塊中輸入網路上的「一般伺服器」名稱。如果要搜尋多部「一般伺服器」，請在伺服器名稱之間輸入分號（「;」）。
   - IP 範圍搜尋：依 IP 位址範圍搜尋。如果要使用此方法選取電腦，請在「IP 範圍」下輸入類別 B 的 IP 位址。

   注意

   如果網路上的 DNS 伺服器在搜尋用戶端時沒有回應，搜尋會停止回應。請等候搜尋逾時。

5. 選取「安裝後重新啟動」，以便在移轉後自動重新啟動目標電腦。

   必須重新啟動才能成功完成移轉。如果您不選取這個選項，請在移轉後手動重新啟動電腦。

6. 請點選「搜尋」。

   搜尋結果會顯示在「ServerProtect 一般伺服器」下。

7. 請點選要執行移轉的電腦。

   a. 如果要選取所有電腦，請點選「全選」。

   b. 如果要清除所有電腦，請點選「取消全選」。

   c. 如果要將清單匯出為逗號分隔值 (CSV) 檔案，請點選「匯出到 CSV」。

8. 如果登入目標電腦時需要使用者名稱和密碼，請執行下列動作：

   a. 選取「使用群組帳號/密碼」核取方塊。

   b. 請點選「設定登入帳號」。

      會出現「輸入管理員資訊」視窗。

   c. 輸入使用者名稱和密碼。

      注意

      請使用本機/網域管理員帳號登入目標端點。如果用來登入目標電腦的權限不足（例如「Guest」或「Normal user」），將無法執行安裝。

   d. 請點選「確定」。

   e. 請點選「如果登入不成功則再詢問一次」，在移轉程序期間若無法登入，可以再次輸入使用者名稱和密碼。

9. 請點選「移轉」。

10. 如果您不選取「安裝後重新啟動」選項，請重新啟動目標電腦以完成移轉。

安裝後

完成安裝後，請驗證下列項目：

- 程式清單 第 5-53 頁
- Security Agent 服務 第 5-53 頁
- Security Agent 安裝記錄檔 第 5-54 頁

程式清單

「Trend Micro Apex One Security Agent」會列在用戶端端點「控制台」的「新增/移除程式」清單中。

Security Agent 服務

「Microsoft 管理主控台」上顯示下列 Security Agent 服務：

表 5-14. 預設處理程序

處理程序	說明	位置
TmListen.exe	接收來自 Apex One 伺服器的指令與通知，並促進 Security Agent 與伺服器之間的通訊	<用戶端安裝資料夾>\tmlisten.exe
NTRtScan.exe	在 Security Agent 上執行即時、預約與手動掃瞄	<用戶端安裝資料夾>\ntrtscan.exe
TmPfw.exe	提供封包層級防火牆、網路病毒掃瞄和入侵偵測功能	<用戶端安裝資料夾>\TmPfw.exe

處理程序	說明	位置
TMBMSRV.exe	規範對於外部儲存裝置的存取，並防止未經授權變更登錄機碼和程序 注意 如果啟動此選項，Security Agent 可能會使得您無法在端點上成功地安裝協力廠商產品。如果遇到此問題，您可以先暫時關閉此選項，然後在安裝完協力廠商產品之後重新啟動此選項。	<%Program Files (x86) 資料夾%>\Trend Micro\BM\TMBMSRV.exe
TmCCSF.exe	執行瀏覽器弱點攻擊防護和記憶體掃瞄	<用戶端安裝資料夾>\CCSF\TmCCSF.exe
TmWSCSvc.exe	將 Apex One Security Agent 的安全狀態回報給安全中心	<用戶端安裝資料夾>\TmWSCSvc.exe

Security Agent 安裝記錄檔

Security Agent 安裝記錄檔 OFCNT.LOG 位於下列位置：

- %windir%（適用於除 MSI 套件安裝方法以外的所有安裝方法）
- %temp%（適用於 MSI 套件安裝方法）

建議的安裝後工作

趨勢科技建議您執行下列安裝後工作。

元件更新

更新 Security Agent 元件，以確保用戶端擁有最新的安全威脅防護。您可以從 Web 主控台手動執行用戶端更新，或指示使用者從其端點執行「立即更新」。

使用 EICAR 測試程式檔來測試掃瞄

「歐洲電腦防毒研究協會」(EICAR) 已開發出 EICAR 測試程式檔，這是一種確認已正確安裝和設定防毒軟體的安全方式。如需詳細資訊，請造訪 EICAR 網站：

http://www.eicar.org

EICAR 測試程式檔是副檔名為 .com 的內隱文字檔。它並不是病毒，也不包含病毒碼的任何片段，但大多數防毒軟體會將其當作病毒而有反應。請使用此檔案模擬病毒事件，並確認電子郵件通知和病毒記錄都能正常運作。

警告!

請勿使用真的病毒測試防毒產品。

執行測試掃瞄

步驟

1. 啟動用戶端上的「即時掃瞄」。
2. 複製下列字串並貼到「記事本」或任何純文字編輯器中：`X5O!P %@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE! $H+H*`
3. 將檔案儲存到暫存目錄中，並命名為 `EICAR.com`。Apex One 會立即偵測到該檔案。
4. 如果要測試網路上的其他電腦，請將 EICAR.com 檔案附加到電子郵件訊息，然後傳送給其中一部電腦。

秘訣

趨勢科技建議您使用壓縮軟體（例如：WinZip）來壓縮 EICAR 檔案，然後執行另一次測試掃瞄。

Security Agent 解除安裝

有兩種方式可以從端點解除安裝 Security Agent：

- 從 Web 主控台解除安裝 Security Agent 第 5-56 頁
- 執行 Security Agent 解除安裝程式 第 5-58 頁

從 Web 主控台解除安裝 Security Agent

從 Web 主控台解除安裝 Security Agent。請僅在程式發生問題時執行解除安裝，但之後應立即重新安裝，讓端點能夠持續防禦安全威脅。

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「工作 > 用戶端解除安裝」。
4. 在「用戶端解除安裝」畫面中，請點選「開始解除安裝」。
5. 檢查通知狀態並檢查是否有用戶端未收到通知。
   a. 依序請點選「選取未通知的端點」和「開始解除安裝」，立即重新傳送通知給未收到通知的用戶端。
   b. 請點選「停止解除安裝」以提示 Apex One 停止通知目前要通知的用戶端。已接獲通知並執行解除安裝的用戶端將會忽略此命令。

Security Agent 解除安裝程式

Security Agent 解除安裝權限允許使用者在本機端點上解除安裝 Security Agent 程式。

視您的組態而定，您可能必須在解除安裝時輸入密碼。如果需要密碼，請確定您只將該密碼提供給需要執行解除安裝程式的使用者；如果該密碼已洩漏給其他使用者，請立即變更密碼。

授與 Security Agent 解除安裝權限

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 權限和其他設定」。
4. 在「權限」標籤上，移至「解除安裝」區段。
5. 設定密碼需求。
   - 不需要密碼
   - 需要密碼：輸入要求的密碼和確認密碼

    注意

   密碼必須符合下列複雜度要求：
   - 長度為 8 到 32 字元
   - 以下每項包含至少一個：大寫字母 (A-Z)、小寫字母 (a-z)、數字 (0-9) 和特殊字元
   - 不可包含非可列印 ASCII 字元
6. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。

- 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

執行 Security Agent 解除安裝程式

步驟

1. 在 Windows「開始」功能表上，按一下「程式集 > Trend Micro Apex One Security Agent > 解除安裝 Security Agent」。

   您也可以執行下列步驟：

   a. 按一下「控制台 > 解除安裝程式」。

   b. 找出「Trend Micro Apex One Security Agent」，然後按一下「解除安裝」。

   c. 請遵循畫面上的說明。

2. 如果看到提示，請輸入解除安裝密碼。Apex One 會通知使用者解除安裝的進度以及完成結果。

   注意

   如果您在用戶端上安裝了「資料安全防護」，則必須重新啟動端點才能完成解除安裝程序。

第 6 章

維持最新的防護

本章說明 Trend Micro Apex One 元件和更新程序。

包含下列主題：

Apex One 元件和程式

Apex One 使用元件和程式來保護用戶端端點免遭最新的安全威脅。請透過執行手動或預約更新，將這些元件和程式維持在最新狀態。

除了元件之外，Apex One 用戶端還會從 Apex One 伺服器接收更新過的組態設定檔。Security Agent 需要有這些組態設定檔來套用新設定。每一次您經由 Web 主控台修改 Apex One 設定時，組態設定檔案都會變更。

元件分為下列幾種類別：

防毒元件

元件	說明
病毒掃瞄引擎（32/64 位元）	所有趨勢科技產品的核心都是掃瞄引擎，其最初的開發目的是偵測早期的檔案型病毒。現在的掃瞄引擎則非常成熟，而且可以偵測不同類型的病毒和惡意程式。掃瞄引擎也可以偵測開發用於研究目的的受控制病毒。 引擎和病毒碼檔案不會掃瞄每個檔案的每個位元組，而會一起合作來辨識下列項目： • 病毒程式碼的獨有特徵 • 檔案內病毒所在的確切位置
病毒碼	「病毒碼」所含的資訊，可協助 Security Agent 識別最新的病毒/惡意程式和混合式安全威脅攻擊。趨勢科技會每週建立數次新版的「病毒碼」並發行，而在發現特別具有破壞力的病毒/惡意程式時會立即建立並發行。
病毒掃瞄驅動程式	「病毒掃瞄驅動程式」會監控使用者操作檔案的情形。操作包括開啟或關閉檔案，以及執行應用程式。此驅動程式有兩個版本。即 `TmXPFlt.sys` 和 `TmPreFlt.sys`。`TmXPFlt.sys` 用於病毒掃瞄引擎的即時組態設定，`TmPreFlt.sys` 用於監控使用者作業。 **注意** 此元件不會在主控台上顯示。若要檢查其版本，請移至 <伺服器安裝資料夾>\PCCSRV\Pccnt\Drv。以滑鼠右鍵請點選 .sys 檔案，選取「內容」，然後移至「版本」標籤。
雲端截毒掃瞄病毒碼 本機雲端病毒碼	使用雲端截毒掃瞄模式時，Security Agent 會使用兩個共同運作的小型病毒碼，提供與標準惡意程式防護病毒碼和間諜程式防護病毒碼相同的防護。 雲端截毒掃瞄病毒碼包含大多數病毒碼定義。本機雲端病毒碼包含雲端截毒掃瞄病毒碼中未包含的所有其他病毒碼定義。 Security Agent 使用本機雲端病毒碼掃瞄安全威脅。如果 Security Agent 在掃瞄期間無法判斷檔案的風險，就會傳送掃瞄查詢到掃瞄伺服器（由 Apex One 伺服器 代管的服務），以確認風險。掃瞄伺服器會使用雲端截毒掃瞄病毒碼驗證該風險。Security Agent 會「快取」由掃瞄伺服器提供的掃瞄查詢結果，以提升掃瞄效能。

元件	說明
IntelliTrap 病毒碼	IntelliTrap 病毒碼用於偵測包裝成為可執行檔的即時壓縮檔的檔案。 如需詳細資訊，請參閱 IntelliTrap 第 D-6 頁。
IntelliTrap 例外病毒碼	IntelliTrap 例外病毒碼包含「許可的」壓縮檔清單。
記憶體檢測病毒碼	「即時掃瞄」會使用「記憶體檢測病毒碼」來評估「行為監控」識別的可執行壓縮檔。「即時掃瞄」會對可執行壓縮檔執行以下動作： 1. 確認處理程序映像路徑後在記憶體中建立對應檔案。 注意 「掃瞄例外」清單會覆寫檔案掃瞄。 2. 向「進階防護服務」傳送處理程序 ID，然後該服務會： a. 使用「病毒掃瞄引擎」執行記憶體掃瞄。 b. 使用全域核可清單過濾該處理程序，以搜尋 Windows 系統檔案、來自可信來源的數位簽署檔案以及趨勢科技測試的檔案。確認檔案安全後，Apex One 不會對檔案執行任何處理行動。 3. 處理記憶體掃瞄後，「進階防護服務」將結果傳送到「即時掃瞄」。 4. 然後，「即時掃瞄」隔離所有偵測到的惡意程式威脅並終止該處理程序。
關聯式智慧引擎（32/64 位元）	關聯式智慧引擎會監控不常見的檔案所執行的程序、擷取其中的行為特徵，由關聯式智慧查詢處理程式傳送給 Machine Learning 引擎進行分析。
關聯式智慧型病毒碼	關聯式智慧型病毒碼包含「核可的」行為清單，其中所列行為與任何已知的安全威脅無關。
關聯式智慧查詢處理程式（32/64 位元）	關聯式智慧查詢處理程式會處理關聯式智慧引擎所識別的行為，然後將報告傳送給 Machine Learning 引擎。

元件	說明
進階威脅掃描引擎（32/64 位元）	進階威脅掃描引擎會從不常見的檔案中擷取檔案特徵，然後將該資訊傳送給 Machine Learning 引擎。
進階安全威脅關聯病毒碼	進階安全威脅關聯病毒碼包含一份檔案特徵清單，其中所列檔案特徵與任何已知的安全威脅無關。

更新掃瞄引擎

透過將最容易隨時間變化的病毒/惡意程式資訊儲存在病毒碼中，趨勢科技可將掃瞄引擎更新的次數降到最低，同時保持最新的防護。不過，趨勢科技還是會定期提供新版的掃瞄引擎。趨勢科技會在下列情況發行新的引擎：

- 將新的掃瞄和偵測技術納入軟體中
- 發現掃瞄引擎無法處理的新潛在有害病毒/惡意程式
- 強化掃瞄效能
- 新增檔案格式、指令碼語言、編碼和（或）壓縮格式

間諜程式防護元件

元件	說明
間諜程式/可能的資安威脅程式病毒碼	間諜程式/可能的資安威脅程式病毒碼可識別檔案和程式中的間諜程式/可能的資安威脅程式、記憶體中的模組、Windows 登錄和 URL 捷徑。
間諜程式/可能的資安威脅程式掃瞄引擎（32/64 位元）	間諜程式/可能的資安威脅程式掃瞄引擎會掃瞄間諜程式/可能的資安威脅程式，並對其執行適當的中毒處理行動。

元件	說明
間諜程式主動式監控病毒碼	間諜程式主動式監控病毒碼用於進行即時間諜程式/可能的資安威脅程式掃瞄。只有標準掃瞄用戶端會使用此病毒碼。 雲端截毒掃瞄 用戶端 會使用「本機雲端病毒碼」來執行即時間諜程式/可能的資安威脅程式掃瞄。如果 用戶端 在掃瞄期間無法判斷掃瞄目標是否有風險，則會將掃瞄查詢傳送至主動雲端截毒技術來源。

損害清除及復原服務元件

元件	說明
損害清除及復原引擎（32/64 位元）	「損害清除及復原引擎」可掃瞄並移除特洛伊木馬程式和特洛伊木馬程式處理程序。
損害清除及復原範本	「損害清除及復原範本」由損害清除及復原引擎用於辨識特洛伊木馬程式檔案和處理程序，以便引擎可將它們清除。
Early Boot Cleanup 驅動程式（32/64 位元）	趨勢科技 Early Boot Cleanup 驅動程式會在作業系統驅動程式載入之前載入，以偵測和封鎖開機型 Rootkit。載入 Security Agent 之後，Early Boot Cleanup 驅動程式會調用「損害清除及復原服務」來清除 Rootkit。

防火牆元件

元件	說明
一般防火牆驅動程式（32/64 位元）	「一般防火牆驅動程式」搭配「一般防火牆病毒碼」使用，可掃瞄用戶端端點是否有網路病毒。此驅動程式支援 32 位元和 64 位元平台。
一般防火牆病毒碼	與病毒碼相同，一般防火牆病毒碼可協助用戶端識別病毒特徵（表明存在網路病毒的獨特位元和位元組病毒碼）。

行為監控元件

元件	說明
行為監控偵測病毒碼（32/64 位元）	此病毒碼包含用於偵測可疑安全威脅行為的規則。
行為監控核心驅動程式（32/64 位元）	此核心模式驅動程式可監控系統事件，並將它們傳遞到「行為監控核心服務」以便進行策略實施。
行為監控核心服務（32/64 位元）	此使用者模式服務具有下列功能： • 提供 Rootkit 偵測 • 規範對於外部裝置的存取 • 保護檔案、登錄機碼和服務
行為監控配置特徵碼	「行為監控驅動程式」使用此特徵碼來識別正常系統事件，並將它們從策略實施排除。
數位簽章特徵碼	此特徵碼包含有效數位簽章清單，「行為監控核心服務」使用這些數位簽章來判斷負責系統事件的程式是否安全。
策略實施特徵碼	「行為監控核心服務」會根據此病毒碼中的策略來檢查系統事件。
記憶體掃瞄觸發病毒碼（32/64 位元）	偵測到以下作業後，「行為監控」會使用「記憶體掃瞄觸發病毒碼」來識別可能的威脅： • 檔案寫入處理行動 • 登錄寫入處理行動 • 建立新處理程序 識別其中一項作業後，「行為監控」會呼叫「即時掃瞄」的「記憶體檢測病毒碼」來檢查是否存在安全威脅。 如需有關「即時掃瞄」作業的詳細資訊，請參閱記憶體檢測病毒碼 第 6-4 頁。
損害還原病毒碼	損害還原病毒碼包含用來監控可疑安全威脅行為的策略。
程式檢測監控病毒碼	程式檢測監控病毒碼會監控和儲存用來行為監控的檢測點。

可疑連線元件

元件	說明
全域 C&C IP 清單	全域 C&C IP 清單是搭配網路內容檢測引擎 (NCIE) 使用，可偵測與已知 C&C 伺服器的連線。NCIE 會偵測任何網路通道中的 C&C 伺服器連線。 Apex One 會記錄所有連線資訊到全域 C&C IP 清單中的伺服器，以進行評估。
相關性規則病毒碼	可疑連線服務使用相關性規則病毒碼偵測網路封包標頭中的唯一惡意程式系列特徵。

瀏覽器弱點攻擊解決方案

元件	說明
瀏覽器弱點攻擊防護特徵碼	此病毒碼可識別最新網頁瀏覽器攻擊，並防止攻擊者利用這些攻擊對網頁瀏覽器造成危害。
程式檔分析器統一病毒碼	此病毒碼分析網頁中的程式檔並識別惡意程式檔。

程式

元件	說明
Security Agent	Security Agent 程式提供免於安全威脅的實際防護。

元件	說明
Basecamp	為了最佳化安全性並提供更佳的支援，趨勢科技建議您允許 Basecamp 定期蒐集基本端點資訊。 **重要** 在您同意資料蒐集後，Basecamp 才會開始將任何資料傳送至趨勢科技。 由於 Basecamp 需要使用 Internet 連線，您可能必須另外設定防火牆設定。 • 檔案名稱：`EndpointBasecamp.exe` • 安裝路徑：`C:\Program Files\Trend Micro\Endpoint Basecamp`
HotFix、Patch 和 Service Pack	在產品正式發行之後，趨勢科技通常會開發下列項目來解決問題，以增強產品的效能或增加新功能： • Hot Fix 第 D-5 頁 • 修補程式 第 D-9 頁 • 安全修補程式 第 D-10 頁 • Service Pack 第 D-11 頁 您的廠商或支援提供者會在這些項目可供使用時聯絡您。如需有關新的 Hot Fix、修補程式和 Service Pack 發行的資訊，請造訪趨勢科技網站： http://downloadcenter.trendmicro.com/?regs=TW; http://www.trendmicro.com/download/zh-tw/default.asp 所有發行都有 Readme 檔，其中包含安裝、部署和組態設定資訊。請詳細閱讀 Readme 檔再執行安裝。

HotFix 和 Patch 歷史記錄

當 Apex One 伺服器將 HotFix 或 Patch 檔案部署到 Security Agent 時，用戶端程式會在「登錄編輯程式」中記錄關於該 HotFix 或 Patch 的資訊。您可以使

用物流軟體（例如：Microsoft SMS、LANDesk™ 或 BigFix™）來查詢多個用戶端的這項資訊。

注意

此功能不會記錄只部署到伺服器的 HotFix 和 Patch。

資訊儲存在下列機碼中：

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\HotfixHistory\<Product version>`
- 對於執行 x64 類型平台的電腦：

  `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\ PC-cillinNTCorp\CurrentVersion\HotfixHistory\<Product version>`

檢查下列機碼：

- 機碼：`HotFix_installed`

  類型：`REG_SZ`

  值：`<Hot fix or patch name>`
- 機碼：`HotfixInstalledNum`

  類型：`DWORD`

  值：`<Hot fix or patch number>`

網頁信譽評等元件

元件	說明
URL 過濾引擎	URL 過濾引擎可促進 Apex One 和趨勢科技 URL 過濾服務之間的通訊。URL 過濾服務是一個對 URL 進行分級並向 Apex One 提供分級資訊的系統。

更新總覽

源自趨勢科技主動式更新伺服器的所有元件更新。如果有可用的更新，Apex One 伺服器和主動雲端截毒伺服器來源（主動雲端截毒技術伺服器或主動雲端截毒技術）會下載更新的元件。Apex One 伺服器和主動雲端截毒伺服器來源之間並沒有元件下載重疊的情形，因為每部伺服器都只會下載特定的元件組。

注意

您可以同時將 Apex One 伺服器和主動雲端截毒技術伺服器設定為從趨勢科技主動式更新伺服器以外的來源更新。如果要這麼做，您必須設定自訂更新來源。如果需要設定此更新來源的協助，請聯絡您的經銷商。

Apex One 伺服器和 Security Agent 更新

Apex One 伺服器會下載用戶端所需的大部分元件。唯一不會下載的元件是雲端截毒掃瞄病毒碼，此元件會由主動式雲端截毒伺服器來源下載。

如果 Apex One 伺服器管理大量用戶端，更新可能會耗用大量的伺服器電腦資源，進而影響伺服器的穩定性和效能。為了解決這個問題，Apex One 的更新代理程式功能可讓特定用戶端分擔分發更新到其他用戶端的工作。

下表說明 Apex One 伺服器和用戶端的不同元件更新選項，以及使用各選項的建議時機：

表 6-1. 伺服器-用戶端更新選項

更新選項	說明	建議
主動式更新伺服器 > 伺服器 > 用戶端	Apex One 伺服器會從趨勢科技主動式更新伺服器（或其他更新來源）接收更新的元件，並在用戶端上開始元件更新。	如果 Apex One 伺服器和用戶端之間沒有低頻寬的區段，請使用這個方法。

更新選項	說明	建議
主動式更新伺服器 > 伺服器 > 更新代理程式 > 用戶端	Apex One 伺服器會從主動式更新伺服器（或其他更新來源）接收更新的元件，並在用戶端上開始元件更新。接著充當更新代理程式的用戶端會通知用戶端更新元件。	如果 Apex One 伺服器和用戶端之間有低頻寬的區段，請使用這個方法來平衡網路上的傳輸負載。
主動式更新伺服器 > 更新代理程式 > 用戶端	更新代理程式會直接從主動式更新伺服器（或其他更新來源）接收更新的元件，並通知用戶端更新元件。	只有在從 Apex One 伺服器或其他「更新代理程式」更新「更新代理程式」發生問題時，才使用這個方法。 大部分情況下，「更新代理程式」從 Apex One 伺服器或其他「更新代理程式」接收更新的速度， 會比從外部更新來源接收來得快。
主動式更新伺服器 > 用戶端	Apex One 用戶端會直接從主動式更新伺服器（或其他更新來源）接收更新的元件。	只有在您從 Apex One 伺服器或更新代理程式更新用戶端發生問題時，才使用這個方法。 大部分情況下，用戶端從 Apex One 伺服器或更新代理程式接收更新的速度，會比從外部更新來源接收來得快。

主動雲端截毒技術來源更新

主動雲端截毒技術來源（主動雲端截毒技術伺服器或主動雲端截毒技術）會下載雲端截毒掃瞄病毒碼。雲端截毒掃瞄用戶端不會下載此病毒碼。用戶端會將掃瞄查詢傳送至主動雲端截毒技術來源，並與病毒碼比對來確認潛在的安全威脅。

注意

如需主動雲端截毒伺服器來源的詳細資訊，請參閱主動雲端截毒伺服器來源 第 4-5 頁。

下表說明主動雲端截毒伺服器來源的更新程序。

表 6-2. 主動雲端截毒技術來源更新程序

更新程序	說明
主動式更新伺服器 > 主動雲端截毒技術	趨勢科技主動雲端截毒技術會從趨勢科技主動式更新伺服器接收更新。未連線至企業網路的雲端截毒掃瞄用戶端會將查詢傳送到趨勢科技主動雲端截毒技術。
主動式更新伺服器 > 主動雲端截毒技術伺服器	主動雲端截毒技術伺服器（整合式或獨立式）會從趨勢科技主動式更新伺服器接收更新。未連線至企業網路的主動雲端截毒技術用戶端會將查詢傳送到主動雲端截毒技術伺服器。
主動雲端截毒技術 > 主動雲端截毒技術伺服器	主動雲端截毒技術伺服器（整合式或獨立式）會從趨勢科技主動雲端截毒技術接收更新。未連線至企業網路的主動雲端截毒技術用戶端會將查詢傳送到主動雲端截毒技術伺服器。

Apex One 伺服器更新

Apex One 伺服器會下載下列元件並將其部署到用戶端：

表 6-3. Apex One 伺服器所下載的元件

元件	分配	
	標準掃瞄用戶端	雲端截毒掃瞄用戶端
防毒		
本機雲端病毒碼	否	是
病毒碼	是	否
IntelliTrap 病毒碼	是	是
IntelliTrap 例外病毒碼	是	是
病毒掃瞄引擎（32/64 位元）	是	是
記憶體檢測病毒碼	是	是
開機初期啟動的惡意程式防護特徵碼（32/64 位元）	是	是

元件	分配	
	標準掃瞄用戶端	雲端截毒掃瞄用戶端
關聯式智慧引擎（32/64 位元）	是	是
關聯式智慧型病毒碼	是	是
關聯式智慧查詢處理程式（32/64 位元）	是	是
進階威脅掃描引擎（32/64 位元）	是	是
進階安全威脅關聯病毒碼	是	是
間諜程式防護		
間諜程式/可能的資安威脅程式病毒碼	是	是
間諜程式主動式監控病毒碼	是	否
間諜程式/可能的資安威脅程式掃瞄引擎（32/64 位元）	是	是
損害清除及復原服務		
損害清除及復原範本	是	是
損害清除及復原引擎（32/64 位元）	是	是
Early Boot Cleanup 驅動程式（32/64 位元）	是	是
防火牆		
一般防火牆病毒碼	是	是
行為監控元件		
行為監控偵測病毒碼（32/64 位元）	是	是
行為監控核心驅動程式（32/64 位元）	是	是
行為監控核心服務（32/64 位元）	是	是
行為監控配置特徵碼	是	是

元件	分配	
	標準掃瞄用戶端	雲端截毒掃瞄用戶端
策略實施特徵碼	是	是
數位簽章特徵碼	是	是
記憶體掃瞄觸發病毒碼（32/64 位元）	是	是
程式檢測監控病毒碼	是	是
損害還原病毒碼	是	是
可疑連線		
全域 C&C IP 清單	是	是
相關性規則病毒碼	是	是
瀏覽器弱點攻擊解決方案		
瀏覽器弱點攻擊防護特徵碼	是	是
程式檔分析器統一病毒碼	是	是

更新提醒和秘訣：

- 如果要允許伺服器將更新的元件部署到用戶端，請啟動自動用戶端更新。如需詳細資訊，請參閱 Security Agent 自動更新 第 6-34 頁。如果關閉自動用戶端更新，則伺服器會下載更新檔，但不會將更新檔部署到用戶端。
- 純 IPv6 Apex One 伺服器無法直接將更新分發給純 IPv4 用戶端。同樣地，純 IPv4 Apex One 伺服器無法直接將更新分發給純 IPv6 用戶端。如果要讓 Apex One 伺服器能夠將更新分發給用戶端，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。
- 趨勢科技會定期發行病毒碼檔案，讓您將用戶端防護保持在最新狀態。由於會定期提供病毒碼檔案更新，因此 Apex One 使用稱為「元件複製」的機制，讓您能夠更快下載病毒碼檔案。如需詳細資訊，請參閱 Apex One 伺服器元件複製 第 6-18 頁。
- 如果您使用 Proxy 伺服器連線到 Internet，必須使用正確的 Proxy 設定才能成功下載更新檔。

- 在 Web 主控台的「資訊中心」中，新增「用戶端更新」Widget 以檢視元件的目前版本，並判斷具有更新元件和過期元件的用戶端數目。

Apex One 伺服器更新來源

設定 Apex One 伺服器從趨勢科技主動式更新伺服器或其他來源下載元件。如果 Apex One 伺服器無法直接連線至主動式更新伺服器，您可以指定其他來源。如需狀況範例，請參閱隔離的 Apex One 伺服器更新 第 6-21 頁。

伺服器下載可用的更新之後，會根據您在「更新 > 用戶端 > 自動更新」中指定的設定，自動通知用戶端更新其元件。如果元件更新為重要更新，請轉至「更新 > 用戶端 > 手動更新」，讓伺服器立即通知用戶端。

注意

如果您未在「更新 > 用戶端 > 自動更新」中指定部署預約時程或事件觸發更新設定，伺服器仍會下載更新，但是不會通知用戶端進行更新。

對 Apex One 伺服器更新的 IPv6 支援

純 IPv6 Apex One 伺服器無法直接從純 IPv4 更新來源更新，例如：

- 趨勢科技主動式更新伺服器
- 任何純 IPv4 自訂更新來源

同樣地，純 IPv4 Apex One 伺服器無法直接從純 IPv6 自訂更新來源更新。

如果要允許伺服器連線到更新來源，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。

用於 Apex One 伺服器更新的 Proxy

設定伺服器電腦上裝載的伺服器程式，以在從趨勢科技主動式更新伺服器下載更新檔時使用 Proxy 設定。伺服器程式包括 Apex One 伺服器和整合式主動雲端截毒技術伺服器。

設定伺服器 Proxy 設定

步驟

1. 移至「管理 > 設定 > Proxy 伺服器」。
2. 請點選「伺服器」標籤。
3. 選取「在連線到雲端上的趨勢科技伺服器來更新病毒碼、引擎與使用授權時，使用 Proxy 伺服器」。
4. 指定 Proxy 通訊協定、伺服器名稱或 IPv4/IPv6 位址，以及通訊埠號碼。
5. 如果 Proxy 伺服器需要驗證，請輸入使用者名稱和密碼。
6. 請點選「儲存」。

設定伺服器更新來源

步驟

1. 移至「更新 > 伺服器 > 更新來源」。
2. 選取要下載元件更新的來源位置。

   如果選擇主動式更新伺服器，請確定伺服器有 Internet 連線；如果使用 Proxy 伺服器，請測試是否可以使用 Proxy 設定建立 Internet 連線。如需詳細資訊，請參閱用於 Apex One 伺服器更新的 Proxy 第 6-17 頁。

如果選擇自訂更新來源，請為此更新來源設定適當的環境和更新資源。此外，請確定伺服器電腦與此更新來源之間的連線正常。如果需要設定更新來源的協助，請聯絡您的經銷商。

注意

Apex One 伺服器在從更新來源下載元件時會使用元件複製。如需詳細資訊，請參閱 Apex One 伺服器元件複製 第 6-18 頁。

3. 請點選「儲存」。

Apex One 伺服器元件複製

當趨勢科技主動式更新伺服器上有最新的完整病毒碼檔案可供下載時，也會同時提供 14 個「漸增式病毒碼」。漸增式病毒碼為完整病毒碼檔案的小型版本，僅提供最新版和之前完整病毒碼檔案版本之間的差異。例如，如果最新版為 175，則漸增式病毒碼 v_173.175 會包含 175 版中擁有，但舊版病毒碼 173 版中找不到的簽章（173 版是之前的完整病毒碼版本，病毒碼號碼是以 2 為遞增單位發行的）。

為了減少下載最新病毒碼時產生的網路傳輸，Apex One 會執行元件複製，使用這種元件更新方式時，Apex One 伺服器或「更新代理程式」只會下載漸增式病毒碼。如需有關「更新代理程式」如何執行元件複製的資訊，請參閱更新代理程式元件複製 第 6-54 頁。

元件複製適用於下列元件：

- 病毒碼
- 本機雲端病毒碼
- 損害清除及復原範本
- IntelliTrap 例外病毒碼
- 間諜程式/可能的資安威脅程式病毒碼
- 間諜程式主動式監控病毒碼

元件複製狀況

如果要瞭解伺服器的元件複製說明，請參閱下列狀況：

表 6-4. 伺服器元件複製狀況

Apex One 伺服器上的完整病毒碼	目前的版本：171 其他可用版本： 169	167	165	161	159	
主動式更新伺服器上的最新版本	173.175	171.175	169.175	167.175	165.175	163.175
	161.175	159.175	157.175	155.175	153.175	151.175
	149.175	147.175				

1. Apex One 伺服器會比較其目前完整病毒碼版本與主動式更新伺服器上的最新版本。如果兩個版本之間的差異數為 14 或以下，伺服器只會下載包含兩個版本之間差異的漸增式病毒碼。

   注意

   如果差異數為 14 以上，則伺服器會自動下載完整病毒碼檔案版本以及 14 個漸增式病毒碼。

   範例說明：

   - 171 版和 175 版之間的差異數為 2。也就是說，伺服器上沒有 173 版和 175 版。
   - 伺服器會下載漸增式病毒碼 171.175。這個漸增式病毒碼含括了 171 和 175 兩個版本之間的差異。

2. 伺服器會合併漸增式病毒碼與其目前的完整病毒碼，以產生最新的完整病毒碼。

   範例說明：

   - 在伺服器上，Apex One 會合併 171 版與漸增式病毒碼 171.175，以產生 175 版。

- 伺服器有 1 個漸增式病毒碼 (171.175) 和最新的完整病毒碼（175 版）。

3. 伺服器會根據伺服器上提供的其他完整病毒碼，產生漸增式病毒碼。如果伺服器未產生這些遞增病毒碼，未下載舊版漸增式病毒碼的用戶端將會自動下載完整的病毒碼檔案，進而產生更多網路傳輸。

   範例說明：

   - 由於伺服器有 169、167、165、163、161、159 等病毒碼版本，因此可以產生下列漸增式病毒碼：

     169.175, 167.175, 165.175, 163.175, 161.175, 159.175

   - 伺服器不需要使用 171 版，因為它已經擁有漸增式病毒碼 171.175。
   - 目前伺服器有 7 個漸增式病毒碼：

     171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175

   - 伺服器會保留最後 7 個完整病毒碼版本（版本 175、171、169、167、165、163、161），並移除任何更早之前的版本（159 版）。

4. 伺服器會比較其目前的漸增式病毒碼與主動式更新伺服器上提供的漸增式病毒碼。伺服器會下載其所沒有的漸增式病毒碼。

   範例說明：

   - 主動式更新伺服器中有 14 個漸增式病毒碼：

     173.175, 171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175, 157.175, 155.175, 153.175, 151.175, 149.175, 147.175

   - Apex One 伺服器中有 7 個漸增式病毒碼：

     171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175

   - Apex One 伺服器會下載額外 7 個漸增式病毒碼：

     173.175, 157.175, 155.175, 153.175, 151.175, 149.175, 147.175

   - 目前伺服器已擁有主動式更新伺服器上提供的所有漸增式病毒碼。

5. 最新的完整病毒碼和 14 個遞增病毒碼都可提供給用戶端。

隔離的 Apex One 伺服器更新

如果 Apex One 伺服器屬於一個與所有外部來源完全隔離的網路，則可透過從包含最新元件的內部來源進行更新，使伺服器元件保持最新。

本主題說明更新隔離的 Apex One 伺服器時所需執行的工作。

更新隔離的 Apex One 伺服器

本此程序僅供參考。如果可以完成此程序中的所有工作，請洽詢經銷商有關各項工作的詳細步驟。

步驟

1. 識別更新來源，例如：Trend Micro Apex Central 或隨機主機。此更新來源必須有：
   - 可靠的 Internet 連線，以便可以從趨勢科技主動式更新伺服器下載最新元件。如果無法連接到 Internet，則更新來源只能自行從趨勢科技取得元件，再將元件複製到更新來源中。
   - 與 Apex One 伺服器之間的有效連線。如果 Proxy 伺服器介於 Apex One 伺服器和更新來源之間，請設定 Proxy 設定。如需詳細資訊，請參閱用於 Apex One 伺服器更新的 Proxy 第 6-17 頁。
   - 足夠的磁碟空間可用於儲存下載的元件
2. 使 Apex One 伺服器指向新的更新來源。如需詳細資訊，請參閱 Apex One 伺服器更新來源 第 6-16 頁。
3. 識別伺服器部署到用戶端的元件。如需可部署元件的清單，請參閱 Security Agent 更新 第 6-24 頁。

秘訣

確定元件是否要部署到用戶端的方法之一是，移至 Web 主控台上的「更新摘要」畫面（「更新 > 摘要」）。在此畫面中，將要部署的元件的更新率一定大於 0%。

4. 確定下載元件的頻率。病毒碼檔案會頻繁（有些是每天更新）更新，因此最好定期進行更新。至於引擎和驅動程式，您可以要求經銷商通知您重要的更新。

5. 在更新來源：

   a. 連線到主動式更新伺服器。伺服器的 URL 取決於 Apex One 的版本。

   b. 下載以下項目：

      - `server.ini` 檔案。此檔案包含有關最新元件的資訊。
      - 在步驟 3 中確定的元件。

   c. 將下載的項目儲存到更新來源的某個目錄中。

6. 執行 Apex One 伺服器的手動更新。如需詳細資訊，請參閱手動更新 Apex One 伺服器 第 6-23 頁。

7. 每次需要更新元件時，請重複步驟 5 至步驟 6。

Apex One 伺服器更新方法

您可以手動更新 Apex One 伺服器元件，或透過設定更新預約時程來更新。

如果要允許伺服器將更新的元件部署到用戶端，請啟動自動用戶端更新。如需詳細資訊，請參閱 Security Agent 自動更新 第 6-34 頁。如果關閉自動用戶端更新，則伺服器會下載更新，但不會將更新部署到用戶端。

更新方法包括：

- 手動伺服器更新：如果更新很重要，請執行手動更新，讓伺服器可以立即取得更新。如需詳細資訊，請參閱手動更新 Apex One 伺服器 第 6-23 頁。
- 預約伺服器更新：Apex One 伺服器會在預約的日期和時間連線到更新來源，取得最新元件。如需詳細資訊，請參閱 Apex One 伺服器的預約更新 第 6-23 頁。

手動更新 Apex One 伺服器

安裝或升級 Apex One 伺服器之後，以及在病毒爆發時，需要手動更新 Apex One 伺服器元件。

步驟

1. 移至「更新 > 伺服器 > 手動更新」。
2. 選取要更新的元件。
3. 請點選「更新」。

   伺服器會下載經過更新的元件。

Apex One 伺服器的預約更新

設定 Apex One 伺服器定期檢查其更新來源並自動下載任何可用的更新。使用預約更新是確保您永遠擁有最新安全威脅防護的簡單有效方式，因為用戶端一般會從伺服器取得更新。

步驟

1. 移至「更新 > 伺服器 > 預約更新」。
2. 選取「啟動 Apex One 伺服器的預約更新」。
3. 選取要更新的元件。
4. 指定更新預約時程。

   如果是每日、每週和每月更新，則時間範圍是指 Apex One 會執行更新的時數。Apex One 會在此時間範圍內的任何特定時間進行更新。
5. 請點選「儲存」。

Apex One 伺服器更新記錄檔

檢查伺服器更新記錄檔，判斷更新特定元件時是否發生問題。記錄檔包含 Apex One 伺服器的元件更新。

如果要避免記錄檔佔去過多硬碟空間，請手動刪除記錄檔或設定記錄檔刪除預約時程。如需有關管理記錄檔的詳細資訊，請參閱記錄檔管理 第 14-39 頁。

檢視更新記錄檔

步驟

1. 移至「記錄檔 > 伺服器更新」。
2. 檢查「結果」欄位，查看是否有未更新的元件。
3. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請點選「匯出到 CSV」。開啟檔案或將其儲存至特定位置。

整合式主動雲端截毒技術伺服器更新

整合式主動雲端截毒技術伺服器會下載兩個元件，即雲端病毒碼和網頁封鎖清單。如需有關這些元件及如何更新它們的詳細資訊，請參閱整合式主動雲端截毒技術伺服器管理 第 4-16 頁。

Security Agent 更新

為確保用戶端免受最新安全威脅，請定期更新代理程式元件。

更新代理程式之前，請檢查其更新來源（Apex One 伺服器或自訂更新來源）是否具有最新元件。如需有關如何更新 Apex One 伺服器的詳細資訊，請參閱Apex One 伺服器更新 第 6-13 頁。

下表列出了更新來源部署到用戶端的全部元件，以及使用特定掃瞄方法時所使用的元件。

表 6-5. 部署到用戶端的 Apex One 元件

元件	分配	
	標準掃瞄用戶端	雲端截毒掃瞄用戶端
防毒		
本機雲端病毒碼	否	是
病毒碼	是	否
IntelliTrap 病毒碼	是	是
IntelliTrap 例外病毒碼	是	是
病毒掃瞄引擎（32/64 位元）	是	是
記憶體檢測病毒碼	是	是
開機初期啟動的惡意程式防護特徵碼（32/64 位元）	是	是
關聯式智慧引擎（32/64 位元）	是	是
關聯式智慧型病毒碼	是	是
關聯式智慧查詢處理程式（32/64 位元）	是	是
進階威脅掃描引擎（32/64 位元）	是	是
進階安全威脅關聯病毒碼	是	是
間諜程式防護		
間諜程式/可能的資安威脅程式病毒碼	是	是
間諜程式主動式監控病毒碼	是	否
間諜程式/可能的資安威脅程式掃瞄引擎（32/64 位元）	是	是
損害清除及復原服務		

元件	分配	
	標準掃瞄用戶端	雲端截毒掃瞄用戶端
損害清除及復原範本	是	是
損害清除及復原引擎（32/64 位元）	是	是
Early Boot Cleanup 驅動程式（32/64 位元）	是	是
網頁信譽評等服務		
URL 過濾引擎	是	是
防火牆		
一般防火牆病毒碼	是	是
一般防火牆驅動程式（32/64 位元）	是	是
行為監控元件		
行為監控偵測病毒碼（32/64 位元）	是	是
行為監控核心驅動程式（32/64 位元）	是	是
行為監控核心服務（32/64 位元）	是	是
行為監控配置特徵碼	是	是
策略實施特徵碼	是	是
數位簽章特徵碼	是	是
記憶體掃瞄觸發病毒碼（32/64 位元）	是	是
程式檢測監控病毒碼	是	是
損害還原病毒碼	是	是
可疑連線		
全域 C&C IP 清單	是	是
相關性規則病毒碼	是	是

元件	分配	
	標準掃瞄用戶端	雲端截毒掃瞄用戶端
瀏覽器弱點攻擊解決方案		
瀏覽器弱點攻擊防護特徵碼	是	是
程式檔分析器統一病毒碼	是	是

Security Agent 更新來源

用戶端可以從標準更新來源（Apex One 伺服器）取得更新，或從自訂更新來源（如趨勢科技主動式更新伺服器）取得特定元件。如需詳細資訊，請參閱Security Agent 的標準更新來源 第 6-27 頁和Security Agent 的自訂更新來源 第 6-29 頁。

對 Security Agent 更新的 IPv6 支援

純 IPv6 用戶端無法直接從純 IPv4 更新來源更新，例如：

- 純 IPv4 Apex One 伺服器
- 純 IPv4 更新代理程式
- 任何純 IPv4 自訂更新來源
- 趨勢科技主動式更新伺服器

同樣地，純 IPv4 用戶端無法直接從純 IPv6 更新來源（例如純 IPv6 Apex One 伺服器或更新代理程式）更新。

如果要允許用戶端連線到更新來源，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。

Security Agent 的標準更新來源

Apex One 伺服器是用戶端的標準更新來源。

如果無法存取 Apex One 伺服器，用戶端將沒有備份來源，因此會一直是過時的。如果要更新無法存取 Apex One 伺服器的用戶端，趨勢科技建議使用「用戶端封裝程式」。使用此工具可建立一個含有伺服器上可用最新元件的套件，然後再於用戶端上執行該套件。

注意

用戶端的 IP 位址（IPv4 或 IPv6）會確定是否可以與 Apex One 伺服器建立連線。如需有關用戶端更新的 IPv6 支援的詳細資訊，請參閱對 Security Agent 更新的 IPv6 支援 第 6-27 頁。

設定 Security Agent 的標準更新來源

步驟

1. 移至「更新 > 用戶端 > 更新來源」。
2. 選取「標準更新來源（從 Apex One 伺服器更新）」。
3. 請點選「通知所有用戶端」。

Security Agent 更新程序

注意

本主題討論 Security Agent 的更新程序。更新代理程式的更新程序將在 Security Agent 的標準更新來源 第 6-27 頁中討論。

如果將 Security Agent 設定為直接從 Apex One 更新，則更新程序的執行方式如下：

1. Security Agent 從 Apex One 伺服器取得更新。
2. 無法從 Apex One 伺服器更新時，如果在「用戶端 > 用戶端管理」中啟動了「Security Agent 會從趨勢科技主動式更新伺服器下載更新」選項，請按一下「設定 > 權限和其他設定 > 其他設定（標籤） > 更新設定」，Security Agent 便會嘗試直接連線到趨勢科技主動式更新伺服器。

注意

只能從主動式更新伺服器更新元件。網域設定、程式和 HotFix 只能從該 Apex One 伺服器或更新代理程式下載。您可以將 Security Agent 設定為僅從主動式更新伺服器下載病毒碼檔案，以加速更新程序。如需詳細資訊，請參閱作為 Security Agent 更新來源的主動式更新伺服器 第 6-33 頁。

Security Agent 的自訂更新來源

Security Agent 除了從 Apex One 伺服器更新之外，還可以從自訂更新來源更新。自訂更新來源可協助減少導向至 Apex One 伺服器的 Security Agent 更新傳輸，並允許無法連線至 Apex One 伺服器的 Security Agent 取得即時更新。在「自訂更新來源清單」上指定自訂更新來源，您最多可以指定 1024 個更新來源。

秘訣

趨勢科技建議您指定一些 Security Agent 做為更新代理程式，然後將它們新增到此清單。

設定 Security Agent 的自訂更新來源

重要

OfficeScan XG Service Pack 1（或更新版本）支援在更新代理程式與設定為從更新代理程式接收更新的 Security Agent 之間使用 HTTPS 作為通訊協定。在將通訊協定變更為 HTTPS 之前，必須先將更新代理程式及向更新代理程式報告的所有 Security Agent 升級為 OfficeScan XG Service Pack 1（或更新版本）。

步驟

1. 移至「更新 > 用戶端 > 更新來源」。
2. 選取「自訂更新來源」。
3. 選取更新代理程式和 Security Agent 接收更新的方式。

- 更新代理程式只會從 Apex One 伺服器更新元件、網域設定，以及代理程式與 HotFix
- 所有自訂來源都無法使用或找不到時，Security Agent 會從 Apex One 伺服器更新下列項目：
  - 元件
  - 網域設定
  - Security Agent 和 HotFix

如需詳細資訊，請參閱 Security Agent 更新程序 第 6-28 頁。

4. 如果至少指定了一個更新代理程式作為更新來源，請點選「更新代理程式分析報告」產生一份報告，反白顯示端點的更新狀態。

   如需有關此報告的詳細資訊，請參閱更新代理程式分析報告 第 6-55 頁。

5. 新增或編輯「自訂更新來源清單」。
   - 點選「新增」以指定新更新來源。
   - 點選「IP 範圍」欄中的值以編輯現有更新來源。

   注意

   編輯現有更新來源以將現有 OfficeScan XG SP1（或更新版本）更新代理程式的通訊協定變更為 HTTPS。

   「新增/編輯 IP 範圍和更新來源」畫面隨即顯示。

6. 設定從更新來源接收更新之端點的 IP 地址。
   - IPv4：指定使用更新來源之端點的 IPv4 地址範圍
   - IPv6：指定使用更新來源之端點的 IPv6 字首和長度

注意

請確定 Security Agent 可使用其 IP 位址連線到更新來源。例如，如果指定 IPv4 位址範圍，則更新來源必須具有 IPv4 位址。如果指定 IPv6 字首和長度，則更新來源必須具有 IPv6 位址。

如需有關端點更新的 IPv6 支援的詳細資訊，請參閱 Security Agent 更新來源 第 6-27 頁。

7. 指定更新來源。您可以選取「更新代理程式」（如果已指定），或輸入特定來源的 URL。

   - URL：指定更新來源的 URL

     注意

     若要將已存在的更新代理程式通訊協定從 HTTP 變更為 HTTPS，請修改 URL 值。

   - 更新代理程式：從下拉式功能表中選取預先設定的更新代理程式，然後選擇 Security Agent 連線到更新代理程式的方式

     - 使用更新代理程式 IP 位址來連線
     - 使用更新代理程式主機名稱來連線

     注意

     如果更新代理程式已更新為 OfficeScan XG SP1 或更新版本，Apex One 會自動設定外部來源 URL 以使用 HTTPS 通訊協定。

8. 請點選「儲存」。
9. 管理「自訂更新來源清單」。
   a. 選取核取方塊並請點選「刪除」，以移除清單中的更新來源。
   b. 如果要移動更新來源，請點選向上或向下箭號。您一次只能移動一個來源。
10. 請點選「通知所有用戶端」。

Security Agent 更新程序

注意

本主題討論 Security Agent 的更新程序。更新代理程式的更新程序將在更新代理程式的自訂更新來源 第 6-52 頁中討論。

設定並儲存此自訂更新來源清單之後，更新程序會以下列方式繼續執行：

1. Security Agent 會從清單上的第一個來源進行更新。
2. 如果 Security Agent 無法從第一個來源更新，則會從第二個來源更新，依此類推。
3. 如果無法從全部來源更新，則 Security Agent 將檢查「更新來源」畫面上的以下設定：

表 6-6. 自訂更新來源的其他設定

設定	說明
「更新代理程式」只會從 Apex One 伺服器更新元件、網域設定，以及用戶端與 HotFix	如果已啟動設定，會直接從 Apex One 伺服器更新更新代理程式，並略過「自訂更新來源清單」。 如果已關閉，更新代理程式會套用為一般用戶端所設定的自訂更新來源設定。
所有自訂來源都無法使用或找不到時，Security Agent 會從 Apex One 伺服器更新下列項目：	

設定	說明
元件	如果啟動此設定，則用戶端會從 Apex One 伺服器更新元件。 如果已關閉此選項，而且下列任一條件成立，則用戶端會嘗試直接連線到趨勢科技主動式更新伺服器： • 在「用戶端 > 用戶端管理」中，請點選「設定 > 權限和其他設定 > 其他設定（標籤） > 更新設定」，「Security Agent 從趨勢科技主動式更新伺服器下載更新」選項即會啟動。 • 主動式更新伺服器不包含在「自訂更新來源清單」中。  注意 只能從主動式更新伺服器更新元件。網域設定、程式和 HotFix 只能從該 Apex One 伺服器或更新代理程式下載。您可以將用戶端設定為僅從主動式更新伺服器下載病毒碼檔案，以加速更新程序。如需詳細資訊，請參閱作為 Security Agent 更新來源的主動式更新伺服器 第 6-33 頁。
網域設定	如果啟動此設定，則用戶端會從 Apex One 伺服器更新網域層級的設定。
Security Agent 和 HotFix	如果啟動此設定，則用戶端會從 Apex One 伺服器更新程式和 Hotfix。

4. 如果無法從所有可能的來源更新，則用戶端會結束更新程序。

作為 Security Agent 更新來源的主動式更新伺服器

當 Security Agent 直接從趨勢科技主動式更新伺服器下載更新時，您可以將下載限制為只下載病毒碼檔案，以減少更新期間耗用的頻寬並加速更新程序。

掃瞄引擎和其他元件的更新不像病毒碼檔案的更新那樣頻繁，這是將下載限制為只下載病毒碼檔案的另一個原因。

您無法直接從趨勢科技主動式更新伺服器更新純 IPv6 用戶端。如果要允許 Security Agent 連線到主動式更新伺服器，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。

限制從主動式更新伺服器下載

步驟

1. 移至「用戶端 > 全域用戶端設定」。
2. 請點選「系統」標籤。
3. 移至「更新」區段。
4. 選取「執行更新時只從主動式更新伺服器下載病毒碼檔案」。

Security Agent 更新方法

從 Apex One 伺服器或自訂更新來源更新元件的 Security Agent，可以使用下列更新方法：

- 自動更新：當發生特定事件或根據預約時程，用戶端更新會自動執行。如需詳細資訊，請參閱 Security Agent 自動更新 第 6-34 頁。
- 手動更新：當更新很重要時，請使用手動更新，以立即通知用戶端執行元件更新。如需詳細資訊，請參閱 Security Agent 手動更新 第 6-40 頁。
- Privilege-based 更新：具有更新權限的使用者對於其電腦上的 Security Agent 取得更新的方式有更大的掌控能力。如需詳細資訊，請參閱設定更新權限及其他設定 第 6-41 頁。

Security Agent 自動更新

「自動更新」可讓您擺脫通知所有用戶端進行更新的負擔，並消除用戶端電腦未擁有最新元件的風險。

除了元件之外，Security Agent 也會在自動更新時接收更新的組態設定檔案。用戶端需要組態設定檔案來套用新的設定。每一次您經由 Web 主控台修改 Apex One 設定時，組態設定檔案都會變更。如果要指定套用組態設定檔案至用戶端的頻率，請參閱步驟 3 設定 Security Agent 自動更新 第 6-36 頁。

注意

您可以設定用戶端以在自動更新期間使用 Proxy 設定。如需詳細資訊，請參閱用於 Security Agent 元件更新的 Proxy 第 6-44 頁。

自動更新有兩種類型：

- 事件觸發更新 第 6-35 頁
- 預約更新 第 6-36 頁

事件觸發更新

伺服器可以在下載最新元件後通知線上用戶端更新元件，也可以在離線用戶端重新開機並連線到伺服器時通知這些用戶端更新元件。請在更新之後，選擇性地在 Security Agent 端點上開始「立即掃瞄」（手動掃瞄）。

表 6-7. 事件觸發更新選項

選項	說明
在 Apex One 伺服器下載新元件之後，立即在用戶端開始元件更新	伺服器會在完成更新時立即通知用戶端執行更新。經常更新的用戶端只需要下載漸增式病毒碼，因此可縮短完成更新所需的時間（如需有關漸增式病毒碼的詳細資訊，請參閱 Apex One 伺服器元件複製 第 6-18 頁）。但是，經常更新可能會對伺服器效能造成負面影響，特別是當大量用戶端同時更新時。 如果有用戶端以單機模式執行，而且您也想要讓這些用戶端更新，請選取「包含單機與離線用戶端」。 如需有關單機模式的詳細資訊，請參閱 Security Agent 單機模式權限 第 15-17 頁。
讓用戶端在重新啟動並連線至 Apex One 伺服器後開始元件更新（不包括單機用戶端）	錯過更新的用戶端可在建立與伺服器之間的連線之後立即下載元件。如果用戶端離線或用戶端安裝所在端點未開機並執行，用戶端可能會錯過更新。

選項	說明
更新後執行「立即掃瞄」（不包括單機用戶端）	伺服器會在事件觸發更新後通知用戶端執行掃瞄。如果特定更新是用於回應已在網路之間散播的安全威脅，請考慮啟動此選項。

注意

Apex One 伺服器如果在下載元件後無法成功傳送更新通知給用戶端，則會在 15 分鐘後自動重新傳送通知。伺服器最多會持續傳送更新通知五次，直到用戶端回應為止。如果第五次嘗試失敗，伺服器會停止傳送通知。如果您選取「用戶端重新開機後連線到伺服器時更新元件」選項，元件更新仍會繼續進行。

預約更新

用戶端必須具有相應的權限才能執行預約更新。您需要先選取要授與權限的 Security Agent，這些 Security Agent 才能依照預約時程執行更新。

注意

如果要搭配「網路位址轉譯」(Network Address Translation) 使用預約更新，請參閱使用 NAT 設定 Security Agent 預約更新 第 6-38 頁。

設定 Security Agent 自動更新

步驟

1. 移至「更新 > 用戶端 > 自動更新」。
2. 選取用於「事件觸發更新」的事件：
   - 在 Apex One 伺服器下載新元件之後，立即在用戶端開始元件更新
     - 包含單機與離線用戶端
   - 讓用戶端在重新啟動並連線至 Apex One 伺服器後開始元件更新（不包括單機用戶端）

- 更新後執行「立即掃瞄」（不包括單機用戶端）

如需有關可用選項的詳細資訊，請參閱事件觸發更新 第 6-35 頁。

3. 設定「預約更新」的時程。

   - 小時

     當時程設定為每小時的更新頻率時，「每日僅更新一次用戶端組態設定」選項可用。組態設定檔案包含使用 Web 主控台設定的所有 Security Agent 設定。

     秘訣

     趨勢科技經常更新元件，不過 Apex One 組態設定可能比較不常變更。同時更新組態設定檔和元件需要更多頻寬，而且會增加 Apex One 完成更新所花費的時間。因此，趨勢科技建議每日僅更新一次 Security Agent 組態設定。

   - 「每日一次」或「每週一次」

     指定更新時間和 Apex One 伺服器通知用戶端更新元件的時間範圍。

     秘訣

     這個設定可以避免所有線上用戶端在指定開始時間同時連線到伺服器，大幅降低導向至伺服器的傳輸量。例如，如果開始時間為中午 12 點且時間範圍為 2 小時，則 Apex One 會在中午 12 點到下午 2 點之間隨機通知所有線上用戶端來更新元件。

     注意

     設定更新預約時程之後，在選取的用戶端上啟動該時程。

     如需啟動預約更新的詳細資訊，請參閱設定更新權限及其他設定 第 6-41 頁的步驟 4。

4. 請點選「儲存」。

Apex One 無法立即通知離線用戶端。選取「讓用戶端在重新啟動並連線至 Apex One 伺服器後開始元件更新（不包括單機用戶端）」，以更新時

段過期後才上線的離線用戶端。未啟動此設定的離線用戶端會在下一次預約時程或手動更新時更新元件。

使用 NAT 設定 Security Agent 預約更新

如果區域網路使用 NAT，可能會發生下列問題：

- Security Agent 在 Web 主控台上顯示為離線。
- Apex One 伺服器無法成功通知用戶端有關更新和組態設定變更的資訊。

如下所述，這些問題的暫行解決方法是使用預約更新將更新的元件和組態設定檔案從伺服器部署至 Security Agent。

步驟

- 在用戶端電腦上安裝 Security Agent 之前：
  a. 在「更新 > 用戶端 > 自動更新」的「預約更新」區段中設定用戶端預約更新。
  b. 在「用戶端 > 用戶端管理」中請點選「設定 > 權限和其他設定 > 權限（標籤） > 元件更新」，授與用戶端權限以啟動預約更新。
- 如果 Security Agent 已存在於用戶端電腦上：
  a. 在「用戶端 > 用戶端管理」中請點選「設定 > 權限和其他設定 > 權限（標籤） > 元件更新」，授與用戶端權限以執行「立即更新」。
  b. 指示使用者手動更新用戶端端點上的元件（以滑鼠右鍵請點選系統匣中的 Security Agent 圖示，然後請點選「立即更新」），以取得更新的組態設定。

Security Agent 更新時，將會同時接收更新的元件和組態設定檔案。

使用網域預約更新工具

在自動用戶端更新中設定的更新預約時程僅適用於具有預約更新權限的用戶端。對於其他用戶端，可以設定單獨的更新預約時程。如果要執行此操作，您

需要依照用戶端樹狀結構網域設定預約時程。屬於網域的全部用戶端都會套用此預約時程。

注意

無法為特定用戶端或特定子網域設定更新預約時程。全部子網域都會套用為其上層網域所設定的預約時程。

步驟

1. 記錄用戶端樹狀結構網域名稱和更新預約時程。
2. 移至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\DomainScheduledUpdate。
3. 將以下檔案複製到 <伺服器安裝資料夾>\PCCSRV：
   - DomainSetting.ini
   - dsu_convert.exe
4. 使用文字編輯器（如記事本）開啟 DomainSetting.ini。
5. 指定用戶端樹狀結構網域，然後設定網域的更新預約時程。重複此步驟可新增更多網域。

   注意

   該 ini 檔案提供了詳細的組態設定指示。
6. 儲存 DomainSetting.ini。
7. 開啟命令提示字元，然後變更為 PCCSRV 資料夾的目錄。
8. 輸入以下命令並按 Enter。

   ```
   dsuconvert.exe DomainSetting.ini
   ```
9. 在 Web 主控台上，移至「用戶端 > 全域用戶端設定」。
10. 請點選「儲存」。

Security Agent 手動更新

您可以在 Security Agent 元件嚴重過時和發生病毒爆發時，手動更新 Security Agent 元件。當 Security Agent 長期無法從更新來源更新元件時，Security Agent 元件便會嚴重過時。

除了元件之外，Security Agent 也會在手動更新時自動接收更新的組態設定檔案。Security Agent 需要組態設定檔案來套用新的設定。每一次您經由 Web 主控台修改 Apex One 設定時，組態設定檔案都會變更。

注意

除了啟動手動更新外，您還可以授與使用者執行手動更新（在 Security Agent 端點上也稱為「立即更新」）的權限。如需詳細資訊，請參閱設定更新權限及其他設定 第 6-41 頁。

手動更新 Security Agent

步驟

1. 移至「更新 > 用戶端 > 手動更新」。
2. 畫面頂端會顯示 Apex One 伺服器上目前可用的元件，以及上次更新這些元件的日期。通知用戶端更新之前，請先確定元件是最新的。

   注意

   手動更新伺服器上的過期元件。

   如需詳細資訊，請參閱 Security Agent 手動更新 第 6-40 頁。

3. 如果只要更新具有過期元件的用戶端：
   a. 請點選「選取具有過期元件的用戶端」。
   b. （選用）選取「包含單機與離線用戶端」：
      - 更新與伺服器之間具有正常運作連線的單機用戶端。

- 更新變為線上狀態時的離線用戶端。

c. 請點選「開始更新」。

注意

伺服器會搜尋元件版本比伺服器上的元件版本舊的用戶端，並通知這些用戶端更新。如果要檢查通知狀態，請移至「更新 > 摘要」畫面。

4. 如果要更新選擇的用戶端：

a. 選取「手動選取用戶端」。

b. 請點選「選取」。

c. 在用戶端樹狀結構中，請點選根網域圖示 ( ) 以包含所有的用戶端，或選取特定網域或用戶端。

d. 請點選「開始更新」。

注意

伺服器會開始通知每一個用戶端下載經過更新的元件。如果要檢查通知狀態，請移至「更新 > 摘要」畫面。

設定更新權限及其他設定

設定更新設定並授與用戶端使用者特定權限，例如：執行「立即更新」和啟動預約更新。

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 ( ) 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 權限和其他設定」。

4. 請點選「其他設定」標籤，然後設定「更新設定」區段中的下列選項：

選項	說明
Security Agent 會從趨勢科技主動式更新伺服器下載更新	開始更新時，Security Agent 會先從「更新 > 用戶端 > 更新來源」畫面中指定的更新來源取得更新。 如果更新不成功，用戶端會嘗試從 Apex One 伺服器更新。選取此選項可讓用戶端在無法從 Apex One 伺服器更新時，嘗試從趨勢科技主動式更新伺服器進行更新。 注意 您無法直接從趨勢科技主動式更新伺服器更新純 IPv6 用戶端。如果要允許用戶端連線到主動式更新伺服器，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。
啟動 Apex One 用戶端的預約更新	選取此選項會將所有 Security Agent 設定為依預設啟動預約更新。具有「啟動/關閉預約更新」權限的使用者可以覆寫此設定。 如需設定更新預約時程的詳細資訊，請參閱設定 Security Agent 自動更新 第 6-36 頁。
Security Agent 僅會更新下列元件	此選項控制執行元件更新的方式。 您可以選取下列選項： • 所有元件（包括 Hotfix 和用戶端）：Security Agent 會更新所有元件 • 病毒碼檔案、引擎、驅動程式：Security Agent 不會升級 Security Agent 程式或部署 Hotfix • 病毒碼檔案：Security Agent 不會升級 Security Agent 程式、部署 Hotfix 或更新引擎和驅動程式 注意 選取「所有元件（包括 Hotfix 和用戶端）」可能會嚴重影響伺服器效能，因為所有用戶端會同時連線到伺服器進行升級或安裝 HotFix。

5. 請點選「權限」標籤，然後設定「元件更新」區段中的下列選項：

選項	說明
執行「立即更新」	具有此權限的使用者可以視需要，以滑鼠右鍵請點選系統匣的 Security Agent 圖示並選取「立即更新」來更新元件。 注意 Security Agent 使用者可以在「立即更新」期間使用 Proxy 伺服器設定。 如需詳細資訊，請參閱授與 Proxy 設定權限 第 15-47 頁。
啟動/關閉預約更新	選取此選項可讓 Security Agent 使用者使用 Security Agent 右鍵功能表（該功能表可以覆寫「啟動預約更新」設定）啟動和關閉預約更新。 注意 管理員必須先在「其他設定」標籤上選取「啟動 Security Agent 的預約更新」設定，然後功能表項目才會顯示在 Security Agent 功能表上。

6. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

為 Security Agent 更新設定保留磁碟空間

Apex One 可以配置特定的用戶端磁碟空間量，以供 HotFix、病毒碼檔案、掃瞄引擎和程式更新檔使用。依預設，Apex One 會保留 60MB 的磁碟空間。

步驟

1. 移至「用戶端 > 全域用戶端設定」。
2. 請點選「系統」標籤。
3. 移至「更新」區段。
4. 選取「保留 __ MB 磁碟空間以備更新」。
5. 選取磁碟空間量。
6. 請點選「儲存」。

用於 Security Agent 元件更新的 Proxy

Security Agent 可以在自動更新期間使用 Proxy 設定，或者如果用戶端有執行「立即更新」的權限，也可以使用 Proxy 設定。

表 6-8. Security Agent 元件更新期間使用的 Proxy 設定

更新方式	使用的 Proxy 設定	使用方式
自動更新	• 內部 Proxy 設定。 如需詳細資訊，請參閱 設定內部用戶端 Proxy 設定 第 15-44 頁。	1. 用戶端會優先套用內部 Proxy 設定。 2. 如果您沒有設定內部 Proxy 設定，用戶端將不會使用任何 Proxy 設定。

更新方式	使用的 Proxy 設定	使用方式
立即更新	• 內部 Proxy 設定。 如需詳細資訊，請參閱 設定內部用戶端 Proxy 設定 第 15-44 頁。 • 使用者設定的 Proxy 設定。您可以授與用戶端使用者設定 Proxy 設定的權限。 如需詳細資訊，請參閱 授與 Proxy 設定權限 第 15-47 頁。	1. 用戶端會優先套用內部 Proxy 設定。 2. 如果未啟動 Proxy 設定，用戶端使用者也沒有必要權限，則在更新元件時，用戶端將不會使用任何 Proxy。

設定 Security Agent 更新通知

發生更新相關事件時，Apex One 會通知用戶端使用者。

步驟

1. 移至「用戶端 > 全域用戶端設定」。
2. 請點選「用戶端控制」標籤。
3. 移至「警訊設定」區段。
4. 選取下列選項：
   - 如果病毒碼檔案在 __ 天後仍未更新，則會在 Windows 工作列上顯示警訊圖示：在 Windows 工作列上顯示警訊圖示，提醒使用者更新在指定天數內未更新的病毒碼。如果要更新病毒碼，請使用 Security Agent 更新方法 第 6-34 頁中所述的任何一種更新方法。

     由伺服器管理的所有用戶端都會套用此設定。
   - 如果端點需要重新啟動以載入核心模式驅動程式，則會顯示通知訊息：在安裝 HotFix 或包含新版核心模式驅動程式的升級套件之後，前一版的驅動程式可能仍然存留在端點上。結束前一版並載入新版的

唯一方式是重新啟動端點。重新啟動端點之後，新版驅動程式會自動安裝，不需再次重新啟動。

在用戶端端點安裝 HotFix 或升級套件之後，會立即顯示通知訊息。

5. 請點選「儲存」。

檢視 Security Agent 更新記錄檔

檢查用戶端更新記錄檔，判斷更新用戶端上的病毒碼時是否發生問題。

注意

在此產品版本中，只能從 Web 主控台查詢「病毒碼」更新的記錄檔。

如果要避免記錄檔佔去過多硬碟空間，請手動刪除記錄檔或設定記錄檔刪除預約時程。如需有關管理記錄檔的詳細資訊，請參閱記錄檔管理 第 14-39 頁。

步驟

1. 移至「記錄檔 > 用戶端 > 用戶端元件更新」。
2. 如果要檢視用戶端更新數量，請點選「進度」欄位下的「檢視」。在顯示的「元件更新進度」畫面中，檢視每隔十五分鐘更新的用戶端數量和已更新的用戶端總數。
3. 如果要檢視已更新病毒碼的用戶端，請點選「詳細資料」欄位下的「檢視」。
4. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請點選「匯出到 CSV」。開啟檔案或將其儲存至特定位置。

實施 Security Agent 更新

使用「安全性符合」確保用戶端有最新的元件。安全性符合會判斷 Apex One 伺服器和用戶端之間元件不一致的情況。不一致的情況通常發生在用戶端無法

連線到伺服器以更新元件時。如果用戶端是從其他來源（例如主動式更新伺服器）取得更新，用戶端中的元件就可能比伺服器中的元件還要新。

如需詳細資訊，請參閱適用於受管用戶端的安全性符合 第 15-50 頁。

還原 Security Agent 的元件

「還原」的意思是恢復到舊版「病毒碼」、「本機雲端病毒碼」和「病毒掃瞄引擎」。如果這些元件無法正常運作，請將它們還原到之前版本。Apex One 會保留目前和之前版本的「病毒掃瞄引擎」，以及最近五個版本的「病毒碼」和「本機雲端病毒碼」。

注意

只能還原上述元件。

Apex One 會針對執行 32 位元和 64 位元平台的用戶端使用不同的掃瞄引擎。您必須個別還原這些掃瞄引擎。所有掃瞄引擎類型的還原程序都相同。

步驟

1. 移至「更新 > 還原」。
2. 在適當的區段下請點選「同步處理伺服器」。
   a. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
   b. 請點選「還原」。
   c. 請點選「檢視更新記錄檔」檢查結果，或按「上一步」回到「還原」畫面。
3. 如果伺服器上存在較早版本的病毒碼檔案，請點選「還原伺服器和用戶端版本」同時恢復用戶端和伺服器的病毒碼檔案。

執行用於 Security Agent Hotfix 的 Touch Tool

「Touch Tool」可以將某一檔案的時間戳記與其他檔案的時間戳記同步化，或與端點的系統時間同步化。如果無法在 Apex One 伺服器上部署 HotFix，請使用 Touch Tool 變更 HotFix 的時間戳記。這會讓 Apex One 將這個 HotFix 解譯為新的 HotFix，使伺服器自動再次嘗試部署這個 HotFix。

步驟

1. 在 Apex One 伺服器上，移至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\Touch。
2. 將 TMTouch.exe 複製到包含要變更的檔案的資料夾。如果要將兩個不同檔案的時間戳記同步化，請將這兩個檔案和 Touch Tool 放到相同的位置。
3. 開啟命令提示字元視窗，切換至 Touch Tool 所在的位置。
4. 輸入下列命令：

   ```
   TmTouch.exe <目標檔案名稱> <來源檔案名稱>
   ```

   說明：

   - <目標檔案名稱> 是您要變更其時間戳記的 HotFix 檔案名稱
   - <來源檔案名稱> 是要複製其時間戳記的檔案名稱

   注意

   如果您沒有指定來源檔案名稱，該工具會將目標檔案時間戳記設為端點的系統時間。您可以將萬用字元 (*) 用於目標檔案，但不能用於來源檔案名稱。

5. 如果要檢查時間戳記是否已經變更，請在命令提示字元中輸入 dir，或在「Windows 檔案總管」中檢查檔案內容。

更新代理程式

如果要將部署元件、網域設定或用戶端程式和 HotFix 的工作分發給 Security Agent，請指派部分 Security Agent 來擔任「更新代理程式」或擔任其他用戶

端的更新來源。這樣能協助您確保 Security Agent 準時收到更新，而不會將大量網路流量導向至 Apex One 伺服器。

如果網路依位置區分為不同網段，而且各網段之間的網路連結出現高傳輸負載，請在每個位置至少指定一個「更新代理程式」。

注意

指定從某個更新代理程式更新元件的 Security Agent 僅會從該更新代理程式收到更新的元件和設定。所有 Security Agent 仍會向 Apex One 伺服器報告其狀態。

更新代理程式系統需求

請造訪下列網站，以取得系統需求的完整清單：

http://docs.trendmicro.com/zh-tw/enterprise/apex-one.aspx

更新代理程式組態設定

設定更新代理程式組態設定的程序包括兩個步驟：

1. 指定 Security Agent 做為特定元件的更新代理程式。
2. 指定將從此更新代理程式更新的用戶端。

注意

單一更新代理程式能夠處理的同時用戶端連線數目，視端點的硬體規格而定。

將 Security Agent 指定為「更新代理程式」

步驟

1. 移至「用戶端 > 用戶端管理」。

2. 在用戶端樹狀結構中，選取要指定為更新代理程式的用戶端。

   注意

   無法選取根網域圖示，因為這會將所有用戶端全部指定為更新代理程式。純 IPv6 更新代理程式無法直接將更新分發到純 IPv4 用戶端。同樣地，純 IPv4 更新代理程式無法直接將更新分發到純 IPv6 用戶端。如果要允許更新代理程式將更新分發到用戶端，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。

3. 請點選「設定 > 更新代理程式設定」。
4. 選取「更新代理程式」可以共用的項目。
   - 元件更新
   - 網域設定
   - Security Agent 和 Hotfix
5. 請點選「儲存」。

指定從更新代理程式更新的 Security Agent

步驟

1. 移至「更新 > 用戶端 > 更新來源」。
2. 在「自訂更新來源清單」下，請點選「新增」。
3. 在顯示的畫面中，指定用戶端的 IP 位址。您可以輸入 IPv4 範圍和/或 IPv6 字首和長度。
4. 在「更新代理程式」欄位中，選取您要指定給用戶端的更新代理程式。

   注意

   請確定用戶端可使用其 IP 位址連線到更新代理程式。例如，如果指定 IPv4 位址範圍，則「更新代理程式」必須具有 IPv4 位址。如果指定 IPv6 字首和長度，則「更新代理程式」必須具有 IPv6 位址。

5. 請點選「儲存」。

更新代理程式的更新來源

「更新代理程式」可以從各種來源取得更新檔，例如 Apex One 伺服器或自訂的更新來源。您可以從 Web 主控台的「更新來源」畫面設定更新來源。

對更新代理程式的 IPv6 支援

純 IPv6 更新代理程式無法直接從純 IPv4 更新來源更新，例如：

- 純 IPv4 Apex One 伺服器
- 任何純 IPv4 自訂更新來源
- 趨勢科技主動式更新伺服器

同樣地，純 IPv4 更新代理程式無法直接從純 IPv6 更新來源（例如純 IPv6 Apex One 伺服器）更新。

如果要允許「更新代理程式」連線到更新來源，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。

更新代理程式的標準更新來源

Apex One 伺服器是「更新代理程式」的標準更新來源。如果設定用戶端直接從 Apex One 伺服器更新，則更新程序的執行方式如下：

1. 「更新代理程式」從 Apex One 伺服器取得更新檔。
2. 如果用戶端無法從 Apex One 伺服器更新，而且下列任一條件成立，則用戶端會嘗試直接連線到趨勢科技主動式更新伺服器：
   - 在「用戶端 > 用戶端管理」中，按一下「設定 > 權限和其他設定 > 其他設定 > 更新設定」，「Security Agent 從趨勢科技主動式更新伺服器下載更新」選項即會啟動。

- 主動式更新伺服器是「自訂更新來源清單」中的第一個項目。

秘訣

如果從 Apex One 伺服器更新時發生問題，請將主動式更新伺服器放在該清單頂端。當「更新代理程式」直接從主動式更新伺服器更新時，網路和 Internet 之間會耗用大量頻寬。

3. 如果無法從所有可能的來源更新，則「更新代理程式」會結束更新程序。

更新代理程式的自訂更新來源

除了從 Apex One 伺服器更新之外，「更新代理程式」還可以從自訂更新來源更新。自訂更新來源可協助減少導向至 Apex One 伺服器的用戶端更新傳輸。在「自訂更新來源清單」上指定自訂更新來源，您最多可以指定 1024 個更新來源。如需有關設定清單的步驟，請參閱 Security Agent 的自訂更新來源 第 6-29 頁。

注意

確保 用戶端的更新來源 畫面（更新 > 用戶端 > 更新來源）上的「「更新代理程式」只會從 Apex One 伺服器更新元件、網域設定，以及用戶端與 HotFix」選項已關閉，如此「更新代理程式」才能連線至自訂更新來源。

設定並儲存此清單之後，更新程序會以下列方式繼續執行：

1. 「更新代理程式」會從清單上的第一個項目更新。
2. 如果用戶端無法從第一個項目更新，則會從第二個項目更新，依此類推。
3. 如果用戶端無法從所有項目更新，它會檢查「所有自訂來源都無法使用或找不到時，Security Agent 會從 Apex One 伺服器更新下列項目」標題下的下列選項：

   - 元件：如果已啟動此選項，則用戶端會從 Apex One 伺服器更新。

     如果已關閉此選項，而且下列任一條件成立，則用戶端會嘗試直接連線到趨勢科技主動式更新伺服器：

注意

您只能從主動式更新伺服器更新元件。網域設定、程式和 HotFix 只能從該伺服器或更新代理程式下載。

- 在「用戶端 > 用戶端管理」中，請點選「設定 > 權限和其他設定 > 其他設定 > 更新設定」，「用戶端從趨勢科技主動式更新伺服器下載更新」選項即會啟動。
- 主動式更新伺服器不包含在「自訂更新來源清單」中。

- 網域設定：如果已啟動此選項，則用戶端會從 Apex One 伺服器更新。
- Security Agent 和 HotFix：如果已啟動此選項，則用戶端會從 Apex One 伺服器更新。

4. 如果無法從所有可能的來源更新，則「更新代理程式」會結束更新程序。

如果「標準更新來源（從 Apex One 伺服器更新）」選項已啟動，且 Apex One 伺服器通知用戶端更新元件，則更新程序會有所不同。程序如下：

1. 用戶端會直接從 Apex One 伺服器更新，並略過更新來源清單。
2. 如果用戶端無法從伺服器更新，而且下列任一條件成立，則用戶端會嘗試直接連線到趨勢科技主動式更新伺服器：
   - 在「用戶端 > 用戶端管理」中，請點選「設定 > 權限和其他設定 > 其他設定 > 更新設定」，「Security Agent 從趨勢科技主動式更新伺服器下載更新」選項即會啟動。
   - 主動式更新伺服器是「自訂更新來源清單」中的第一個項目。

秘訣

如果從 Apex One 伺服器更新時發生問題，請將主動式更新伺服器放在該清單頂端。當 Security Agent 直接從主動式更新伺服器更新時，網路與 Internet 之間會耗用大量頻寬。

3. 如果無法從所有可能的來源更新，則「更新代理程式」會結束更新程序。

設定更新代理程式的更新來源

步驟

1. 移至「更新 > 用戶端 > 更新來源」。
2. 選取要從更新代理程式的標準更新來源 (Apex One 伺服器) 還是從更新代理程式的自訂更新來源進行更新。
3. 請點選「通知所有用戶端」。

更新代理程式元件複製

如同 Apex One 伺服器，「更新代理程式」也會在下載元件時使用元件複製。如需有關伺服器如何執行元件複製的詳細資訊，請參閱 Apex One 伺服器元件複製 第 6-18 頁。

「更新代理程式」的元件複製程序如下：

1. 「更新代理程式」會比較其目前完整病毒碼版本與更新來源上的最新版本。如果兩個版本之間的差異數為 14 或以下，「更新代理程式」只會下載包含兩個版本之間差異的漸增式病毒碼。

   注意

   如果差異數為 14 以上，則「更新代理程式」會自動下載完整病毒碼檔案版本。

2. 「更新代理程式」會合併其下載的漸增式病毒碼與其目前的完整病毒碼，以產生最新的完整病毒碼。
3. 「更新代理程式」會下載更新來源上剩餘的所有漸增式病毒碼。
4. 最新的完整病毒碼和所有漸增式病毒碼都會提供給用戶端。

更新代理程式的更新方式

更新代理程式使用一般用戶端可使用的相同更新方式。如需詳細資訊，請參閱Security Agent 更新方法 第 6-34 頁。

您也可以使用「預約更新組態設定」工具來啟動和設定「更新代理程式」（使用用戶端封裝程式所安裝）的預約更新。

注意

如果「更新代理程式」是使用其他安裝方式安裝，則無法使用此工具。如需詳細資訊，請參閱部署考量 第 5-8 頁。

使用預約更新組態設定工具

步驟

1. 在更新代理程式端點上，瀏覽至 <用戶端安裝資料夾>。
2. 按兩下 `SUCTool.exe` 執行此工具。「預約更新組態設定工具」主控台隨即開啟。
3. 選取「啟動預約更新」。
4. 指定更新頻率和時間。
5. 請點選「套用」。

更新代理程式分析報告

產生「更新代理程式分析報告」，以分析更新基礎架構，並判斷哪些用戶端會從更新代理程式和其他更新來源下載部分更新。

注意

此報告包括設定為從更新代理程式接收部分更新的所有 Security Agent。如果您已將管理一或多個網域的工作委派給其他管理員，則他們還會看到設定為從不屬於其管理之網域的更新代理程式接收部分更新的所有 Security Agent。

Apex One 會將「更新代理程式分析報告」匯出成逗號分隔值 (.csv) 檔案。

此報告包含下列資訊：

- Security Agent 端點
- IP 位址
- 用戶端樹狀結構路徑
- 更新來源
- 用戶端是否從更新代理程式下載下列項目：
  - 元件
  - 網域設定
  - Security Agent 程式和 HotFix

重要

「更新代理程式分析報告」僅會列出設定為從更新代理程式接收部分更新的 Security Agent。設定為從更新代理程式執行完整更新（包括元件、網域設定、Security Agent 程式以及 HotFix）的 Security Agent 不會顯示在報告中。

如需產生報告的詳細資訊，請參閱 Security Agent 的自訂更新來源 第 6-29 頁。

元件更新摘要

Web 主控台提供「更新摘要」畫面（移至「更新 > 摘要」），此畫面會通知您整體元件更新狀態並可讓您更新過期元件。如果已啟動伺服器預約更新，此畫面也會顯示下一個更新預約時程。

請定期重新整理此畫面，以檢視最新的元件更新狀態。

注意

如果要檢視整合式主動雲端截毒技術伺服器上的元件更新，請移至「管理 > 主動式雲端截毒技術 > 整合式伺服器」。

Security Agent 的更新狀態

如果您已開始用戶端的元件更新，可在本區段檢視下列資訊：

- 收到元件更新通知的用戶端數目。
- 尚未收到通知但已在通知佇列中的用戶端數目。如果要取消這些給用戶端的通知，請點選「取消通知」。

元件

在「更新狀態」表格中，檢視 Apex One 伺服器下載並散佈的每個元件的更新狀態。

您可以檢視每個元件的目前版本和最近一次的更新日期。請點選數字連結，以檢視內含過期元件的用戶端。手動更新內含過期元件的用戶端。

第 7 章

掃瞄是否有安全威脅

本章說明如何使用 File-based 掃瞄來保護端點免遭安全威脅的侵襲。

包含下列主題：

關於安全威脅

安全威脅是病毒/惡意程式與間諜程式/可能的資安威脅程式的統稱。Apex One 可透過掃瞄檔案，然後針對偵測到的每個安全威脅執行特定處理行動，來保護端點免於遭受安全威脅。在短時間內偵測到大量安全威脅，表示有病毒爆發。Apex One 可強制執行病毒爆發防範策略並隔離中毒端點來協助控制病毒爆發，直到這些端點不存在任何安全威脅。通知與記錄檔可協助您追蹤安全威脅，並且在您需要採取立即處理行動時對您提出警訊。

病毒和惡意程式

病毒/惡意程式種類繁多，而且每天都有新的病毒/惡意程式出現。雖然端點病毒一度在 DOS 或 Windows 中最常見，但是現今卻能利用企業網路、電子郵件系統及網站的弱點造成嚴重損害。

表 7-1. 病毒/惡意程式類型

病毒/惡意程式類型	說明
惡作劇程式	惡作劇程式是類似病毒的程式，往往會在端點監視器上作怪。
其他	「其他」包含未歸類在任何其他病毒/惡意程式類型下的病毒/惡意程式。
封裝程式	封裝程式是指經過壓縮和（或）加密的 Windows 或 Linux™ 可執行程式，通常是特洛伊木馬程式。壓縮執行檔會讓防毒產品更不容易偵測到封裝程式。
勒索軟體	勒索軟體是一種藉由加密、修改或鎖死檔案，然後試圖向使用者勒索一筆贖金來取回資料的安全威脅。如果使用者未在限期內支付贖金，有些勒索軟體安全威脅會自動刪除資料。
Rootkit	Rootkit 是指在終端使用者未同意或未知曉的情況下就在系統上安裝並執行程式碼的程式（或程式集合）。它們會在電腦上以隱形方式持續存在，且偵測不到。Rootkit 不會感染電腦，卻會在無法偵測到的情況下執行惡意程式碼。在惡意程式執行時或僅在瀏覽惡意網站時，Rootkit 就會透過社交工程安裝在系統上。安裝完成後，攻擊者在系統上幾乎可以執行任何功能，包括遠端存取、竊聽，以及隱藏程序、檔案、登錄機碼和通訊通道。

病毒/惡意程式類型	說明
測試病毒	測試病毒是指行為類似真正病毒的內隱檔案，可以由病毒掃瞄軟體偵測出來。使用測試病毒 (例如：EICAR 測試程式檔)，確認您安裝的防毒程式掃瞄正常。
特洛伊木馬程式	特洛伊木馬程式經常使用通訊埠來取得電腦或可執行程式的存取權。特洛伊木馬程式不會進行複製，但會常駐在系統上執行惡意動作，例如開放通訊埠讓駭客進入。傳統的防毒解決方案只能偵測並移除病毒，但卻無法偵測或移除特洛伊木馬程式，特別是已經在系統上執行的特洛伊木馬程式。
病毒	病毒是指會進行複製的程式。為了進行複製，病毒必須將自己附加到其他的程式檔，然後在主程式執行時執行，包括 • ActiveX 惡意程式碼：常駐在執行 ActiveX™ 控制項之網頁中的程式碼。 • 開機磁區型病毒：感染分割區或磁碟的開機磁區的病毒。 • COM 和 EXE 檔案感染型病毒：副檔名為 .com 或 .exe 的可執行程式。 • Java 惡意程式碼：以 Java™ 撰寫或內嵌於其中的非依附作業系統型病毒碼 • 巨集型病毒：編碼為應用程式巨集的病毒，通常包含在文件中。 • VBScript、JavaScript 或 HTML 病毒：常駐在網頁中且透過瀏覽器下載的病毒。 • 蠕蟲：一種自我包裝的程式（或程式集），可以將具有功能性的本體複本或其片段散佈到其他端點系統，途徑往往是透過電子郵件。
網路病毒	嚴格說來，透過網路傳播的病毒，並不算是網路病毒。只有蠕蟲之類的某些病毒/惡意程式類型，才有資格稱為網路病毒。具體來說，網路病毒使用網路通訊協定（例如：TCP、FTP、UDP、HTTP）和電子郵件通訊協定來自行複製。而且往往不會改變系統檔案或修改硬碟的開機磁區。而是會感染用戶端端點的記憶體，強制端點產生大量網路流量，以降低網路傳輸速度，甚至使網路完全無法使用。因為網路病毒會留在記憶體中，所以傳統的檔案 I/O 型掃瞄方法往往偵測不到它們。

病毒/惡意程式類型	說明
可能的病毒/惡意程式	可能的病毒/惡意程式是具有某些病毒/惡意程式特徵的可疑檔案。 如需詳細資訊，請參閱趨勢科技安全威脅百科全書： https://www.trendmicro.com/vinfo/tw/threat-encyclopedia/#malware 注意 無法對可能的病毒/惡意程式執行清除，但可以設定中毒處理行動。

間諜程式和可能的資安威脅程式

除了病毒/惡意程式，端點還會受到潛在安全威脅的侵襲。間諜程式/可能的資安威脅程式是指未歸類為病毒或特洛伊木馬程式的應用程式或檔案，但還是可能對您網路上的端點效能有負面的影響，以及對您的組織形成重大的安全、機密和法律風險。間諜程式/可能的資安威脅程式往往會執行各種不受歡迎和具威脅的行動，例如用快顯視窗騷擾使用者，記錄使用者的按鍵動作以及暴露端點弱點使其易受攻擊。

如果您發現 Trend Micro Apex One 無法偵測出是否為可能的資安威脅程式的應用程式或檔案，但是您認為它是一種可能的資安威脅程式，請將其傳送到趨勢科技進行分析：

http://esupport.trendmicro.com/solution/zh-tw/1059565.aspx

類型	說明
間諜程式	蒐集資料（如帳號使用者名稱和密碼），並將資料傳輸至第三方。
廣告軟體	顯示廣告並蒐集資料（如使用者的 web 瀏覽偏好），以便透過 Web 瀏覽器讓使用者成為廣告的目標。
惡意撥號程式	變更端點的 Internet 設定，而且可能會強制端點透過數據機撥出預先設定的電話號碼。而這些號碼通常是付費電話或國際電話號碼，可能會使您公司的電話費暴增。

類型	說明
惡作劇程式	造成端點行為異常（例如：闔上和打開 CD-ROM 托盤），以及顯示大量訊息方塊。
駭客工具	幫助駭客進入端點。
遠端存取工具	幫助駭客從遠端存取和控制端點。
密碼破解程式	幫助駭客破解帳號使用者名稱和密碼。
其他	其他潛在惡意程式類型。

間諜程式/可能的資安威脅程式如何進入網路

間諜程式/可能的資安威脅程式通常會在使用者下載安裝套件中含有可能的資安威脅應用程式的合法軟體時進入企業網路。大多數軟體程式包含使用者授權合約 (EULA)，使用者必須接受該合約才能進行下載。通常，EULA 中包含應用程式及其收集個人資料之預期用途的相關資訊；但是，使用者通常會忽略此資訊或不瞭解相關法律術語。

潛在風險和威脅

網路上存在的間諜程式和其他類型可能的資安威脅程式，可能會導致下列各種情況：

表 7-2. 潛在風險和威脅

風險或威脅	說明
端點效能降低	為了執行工作，間諜程式/可能的資安威脅程式常需要大量的 CPU 和系統記憶體資源。
因 Web 瀏覽器引起的當機事件增多	廣告軟體等特定類型的可能資安威脅程式，通常會在瀏覽器框架或視窗中顯示資訊。視這些應用程式中的程式碼與系統處理程序之間的互動方式而定，可能的資安威脅程式有時可能會造成瀏覽器損毀或凍結，甚至可能需要重新啟動端點。
使用者效率降低	由於需要關閉經常出現的快顯廣告以及處理惡作劇程式造成的負面影響，使用者無法專心進行主要工作。

風險或威脅	說明
網路頻寬降級	間諜程式/可能的資安威脅程式通常會定期將收集到的資料，傳輸給在網路上（或網路之外）執行的其他應用程式。
損失個人和公司資訊	間諜程式/可能的資安威脅程式並非只收集網站使用者瀏覽清單這類無害的資料。間諜程式/可能的資安威脅程式也會收集使用者憑證，例如用於存取線上銀行帳號和企業網路的憑證。
承擔法律責任的風險提高	如果您網路上的端點資源遭綁架，駭客可能會利用您的用戶端電腦對網路之外的電腦發動攻擊或安裝間諜程式/可能的資安威脅程式。如果您的網路資源牽涉到這類活動，則可能導致您的組織必須對其他人所造成的損害負起法律責任。

防範間諜程式/可能的資安威脅程式和其他安全威脅

您可以採取許多步驟來阻止將間諜程式/可能的資安威脅程式安裝到您的端點上。趨勢科技建議執行下列操作：

- 將所有類型的掃瞄（「手動掃瞄」、「即時掃瞄」、「預約掃瞄」和「立即掃瞄」）設為掃瞄並移除間諜程式/可能的資安威脅程式檔案和應用程式。如需詳細資訊，請參閱掃瞄類型 第 7-12 頁。
- 教導您的用戶端使用者進行下列各項：
  - 下載應用程式並在電腦上安裝之前，務必先閱讀使用者授權合約 (EULA) 和隨附的文件。
  - 出現任何要求授權的訊息時，請點選 「否」，以下載和安裝軟體，除非用戶端使用者確定軟體建立者及檢視的網站都值得信任。
  - 不要開啟來路不明的廣告郵件（垃圾郵件），特別是當垃圾郵件要求使用者按下按鈕或超連結時。
- 設定網路瀏覽器，確保使用嚴格的安全層級。趨勢科技建議要求網路瀏覽器在安裝 ActiveX 控制項之前提示使用者。
- 如果您是使用 Microsoft Outlook，請設定安全設定，讓 Outlook 不會自動下載 HTML 項目（例如：在垃圾郵件中傳送的圖片）。

- 禁止使用點對點檔案共用服務。間諜程式和可能的資安威脅應用程式可能會偽裝為您的使用者可能想要下載的其他類型的檔案（例如：MP3 音樂檔）。
- 定期檢查用戶端電腦中安裝的軟體，並找到可能為間諜程式或其他可能的資安威脅程式的應用程式。
- 為 Windows 作業系統安裝 Microsoft 提供的最新修補程式，以將其維持在最新狀態。如需詳細資訊，請瀏覽 Microsoft 網站。

掃瞄方法類型

Security Agent 可以使用兩種掃瞄方法中的其中一種來掃瞄是否有安全威脅。掃瞄方法包括雲端截毒掃瞄和標準掃瞄。

- 雲端截毒掃瞄

  使用雲端截毒掃瞄的 Security Agent 在本文件中稱為雲端截毒掃瞄用戶端。雲端截毒掃瞄用戶端將受益於檔案信譽評等服務提供的本機掃瞄和雲端查詢。

- 標準掃瞄

  不使用雲端截毒掃瞄的 用戶端稱為標準掃瞄用戶端。標準掃瞄用戶端會將所有 Security Agent 元件儲存在端點上，並在本機掃瞄所有檔案。

預設掃瞄方法

在這個 Apex One 版本中，全新安裝的預設掃瞄方法是雲端截毒掃瞄。這表示如果您執行 Apex One 伺服器全新安裝，但未在 Web 主控台上變更掃瞄方法，則伺服器管理的所有用戶端都會使用雲端截毒掃瞄。

如果您從舊版的 Apex One 伺服器升級，並且啟動了用戶端自動升級，則該伺服器管理的所有用戶端仍將會使用升級前設定的掃瞄方法。例如，如果從支援雲端截毒掃瞄和標準掃瞄的舊版 Apex One 進行升級，則使用雲端截毒掃瞄的

所有用戶端在升級後將繼續使用雲端截毒掃瞄，且使用標準掃瞄的所有用戶端在升級後將繼續使用標準掃瞄。

掃瞄方法比較

下表提供這兩種掃瞄方法的比較：

表 7-3. 標準掃瞄和雲端截毒掃瞄的比較

比較基準	標準掃瞄	雲端截毒掃瞄
掃瞄行為	標準掃瞄 Security Agent 會對本機端點執行掃瞄。	• 雲端截毒掃瞄 Security Agent 會對本機端點執行掃瞄。 • 如果 Security Agent 無法在掃瞄期間判斷檔案的風險，則 Security Agent 會將掃瞄查詢傳送到主動雲端截毒技術來源以檢查該風險。 • Security Agent 會「快取」掃瞄查詢結果以改善掃瞄效能。
元件使用中且已更新	所有元件（「本機雲端病毒碼」除外）在更新來源都可用	所有元件（「病毒碼」和「間諜程式主動式監控病毒碼」除外）在更新來源都可用
傳統更新來源	Apex One 伺服器	Apex One 伺服器

變更掃瞄方法

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 掃瞄設定 > 掃瞄方法」。

4. 選取標準掃瞄」或「雲端截毒掃瞄」。

5. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

從雲端截毒掃瞄切換至標準掃瞄

下表列出切換 Security Agent 使用的掃瞄方法前應瞭解的一些考量事項。

1. 要切換的 Security Agent 數目

   一次切換少量的 Security Agent，可確保有效利用 Apex One 伺服器與主動雲端截毒技術伺服器資源。當 Security Agent 變更掃瞄方法的同時，這些伺服器可以執行其他重要工作。

2. 時機

   切換掃瞄方法時，Security Agent 必需下載適用於新掃描方法的完整版必要病毒碼檔案。

   建議您在離峰時段進行切換，以便將對網路頻寬的影響及對使用者日常作業的干擾降到最低。趨勢科技建議您在轉換程序進行期間關閉 Security Agent 中的「立即更新」功能。

3. 用戶端樹狀結構設定

   掃瞄方法是一項可在根、網域或個別 Security Agent 層級上套用的精細設定。在切換掃瞄方法時，您可以：

   - 建立新的用戶端樹狀結構網域，並將標準掃瞄指定為其掃瞄方法。任何移至此網域的用戶端，都會使用標準掃瞄。當您移動用戶端時，請啟動「將新網域的設定套用至選取的用戶端」設定。

- 選取網域並加以設定，使其使用標準掃瞄。屬於該網域的雲端截毒掃瞄用戶端將會切換至標準掃瞄。
- 從網域中選取一或多個雲端截毒掃瞄用戶端，然後將其切換至標準掃瞄。

注意

如果網域的掃瞄方法有任何變更，都將覆寫您為個別用戶端設定的掃瞄方法。

從標準掃瞄切換至雲端截毒掃瞄

如果要將用戶端從標準掃瞄切換到雲端截毒掃瞄，請確定已設定「主動雲端截毒技術服務」。

如需詳細資訊，請參閱設定主動雲端截毒技術服務 第 4-11 頁。

下表提供切換到雲端截毒掃瞄時的其他注意事項。

表 7-4. 切換到雲端截毒掃瞄時的注意事項

注意事項	詳細資訊
產品使用授權	如果要使用雲端截毒掃瞄，請確認您已啟動下列服務的使用授權，且這些使用授權尚未到期： • 防毒 • 網頁信譽評等和間諜程式防護
Apex One 伺服器	確定用戶端可連線到 Apex One 伺服器。只有線上用戶端會收到切換至雲端截毒掃瞄的通知。離線用戶端在上線後，才會接獲通知。單機用戶端會在上線後接獲通知，或者用戶端若有預約更新權限，則會在執行預約更新時接獲通知。 此外，請驗證 Apex One 伺服器是否具有最新的元件，因為雲端截毒掃瞄用戶端必須從此伺服器下載本機雲端病毒碼。 如果要更新元件，請參閱 Apex One 伺服器更新 第 6-13 頁。

注意事項	詳細資訊
要切換的用戶端數目	一次切換少量的用戶端，可確保有效利用 Apex One 伺服器資源。當用戶端變更其掃瞄方法時，Apex One 伺服器可以執行其他重要工作。
時機	首次切換至雲端截毒掃瞄時，用戶端必須從 Apex One 伺服器下載完整版的本機雲端病毒碼。雲端截毒掃瞄病毒碼僅適用於雲端截毒掃瞄用戶端。 建議您在離峰時段進行切換，以確保下載程序可在短時間內完成。同時建議您在沒有用戶端預約要從伺服器進行更新時，執行切換作業。此外，請暫時關閉用戶端上的「立即更新」，等到用戶端已切換至雲端截毒掃瞄後，再予以重新啟動。
用戶端樹狀結構設定	掃瞄方法是一項可在根、網域或個別用戶端層級上進行設定的精細設定。切換至雲端截毒掃瞄時，您可以： • 建立新的用戶端樹狀結構網域，並將雲端截毒掃瞄指定為其掃瞄方法。任何移至此網域的用戶端，都會使用雲端截毒掃瞄。當您移動用戶端時，請啟動「將新網域的設定套用至選取的用戶端」設定。 • 選取網域並加以設定，使其使用雲端截毒掃瞄。屬於該網域的標準掃瞄用戶端將會切換至雲端截毒掃瞄。 • 從網域中選取一或多個標準掃瞄用戶端，然後將其切換至雲端截毒掃瞄。 注意 如果網域的掃瞄方法有任何變更，都將覆寫您為個別用戶端設定的掃瞄方法。
IPv6 支援	雲端截毒掃瞄用戶端會將掃瞄查詢傳送至主動雲端截毒技術來源。 純 IPv6 雲端截毒掃瞄用戶端無法將查詢直接傳送到純 IPv4 來源，例如： • 趨勢科技主動雲端截毒技術 同樣，純 IPv4 雲端截毒掃瞄用戶端無法將查詢傳送至純 IPv6 主動雲端截毒技術伺服器。 如果要使雲端截毒掃瞄用戶端連線到來源，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。

掃瞄類型

Apex One 提供下列掃瞄類型，以保護 Security Agent 電腦不受安全威脅侵害：

表 7-5. 掃瞄類型

掃瞄類型	說明
即時掃瞄	每當接收、開啟、下載、複製或修改檔案時，自動掃瞄端點上的檔案 如需詳細資訊，請參閱即時掃瞄 第 7-12 頁。
手動掃瞄	由使用者開始執行的掃瞄，會掃瞄使用者所要求的一或多個檔案 如需詳細資訊，請參閱手動掃瞄 第 7-15 頁。
預約掃瞄	根據管理員或終端使用者所設定的預約時程，自動掃瞄端點上的檔案 如需詳細資訊，請參閱預約掃瞄 第 7-17 頁。
立即掃瞄	由管理員開始的掃瞄，掃瞄一或多部目標電腦上的檔案 如需詳細資訊，請參閱立即掃瞄 第 7-19 頁。

即時掃瞄

「即時掃瞄」會一直持續進行。每當接收、開啟、下載、複製或修改檔案時，「即時掃瞄」即會掃瞄檔案是否存在安全威脅。如果 Security Agent 未偵測到安全威脅，則使用者可以繼續存取檔案。如果 Security Agent 偵測到安全威脅或可能的病毒/惡意程式，則會顯示一則通知訊息，指出中毒檔案的名稱和具體的安全威脅。

即時掃瞄會保留一個持續的掃瞄快取，每次 Security Agent 啟動時都會重新載入該掃瞄快取。Security Agent 會追蹤在結束 Security Agent 後對檔案或資料夾進行的所有變更，並將這些檔案從快取移除。

注意

如果要修改通知訊息，請開啟 Web 主控台，然後移至「管理 > 通知 > 用戶端」。

設定「即時掃瞄」設定，並將其套用至一或多個 Security Agent 與網域，或套用至伺服器管理的所有 Security Agent。

設定即時掃瞄設定

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 掃瞄設定 > 即時掃瞄設定」。
4. 選取下列選項：
   - 啟動病毒/惡意程式掃瞄
   - 啟動間諜程式/可能的資安威脅程式掃瞄

    注意

   如果您關閉病毒/惡意程式掃瞄，間諜程式/可能的資安威脅程式掃瞄也會隨之關閉。在病毒爆發期間，「即時掃瞄」將無法關閉（如果原本已關閉，將會自動啟動），以防止病毒修改或刪除用戶端電腦上的檔案與資料夾。
5. 在「目標」標籤上，設定下列項目：
   - 使用者對檔案執行的活動 第 7-22 頁
   - 要掃瞄的檔案 第 7-23 頁
   - 掃瞄設定 第 7-23 頁
6. 請點選「動作」標籤，然後設定下列項目：

表 7-6. 中毒處理行動

處理行動	關係
病毒/惡意程式處理行動	主要處理行動（選取一個）： • 使用主動式處理行動 第 7-33 頁 • 對所有的病毒/惡意程式類型使用相同的處理行動 第 7-34 頁 • 對每個病毒/惡意程式類型使用特定的處理行動 第 7-35 頁 注意 如需有關不同處理行動的詳細資訊，請參閱病毒/惡意程式中毒處理行動 第 7-32 頁。 其他病毒/惡意程式處理行動： • 隔離目錄 第 7-35 頁 • 清除前先備份檔案 第 7-36 頁 • 損害清除及復原服務 第 7-37 頁 • 偵測到病毒/惡意程式時顯示通知訊息 第 7-38 頁 • 偵測到可能的病毒/惡意程式時顯示通知訊息 第 7-38 頁
間諜程式/可能的資安威脅程式處理行動	主要處理行動： • 間諜程式/可能的資安威脅程式中毒處理行動 第 7-42 頁 其他間諜程式/可能的資安威脅程式處理行動： • 偵測到間諜程式/可能的資安威脅程式時顯示通知訊息 第 7-44 頁

7. 在「掃瞄例外」標籤上，將目錄、檔案和副檔名設定為從掃瞄中排除。

   如需詳細資訊，請參閱掃瞄例外 第 7-27 頁。

8. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

- 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
- 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

手動掃瞄

「手動掃瞄」是依需求掃瞄，會在使用者於 Security Agent 主控台上執行掃瞄後立即啟動。完成掃瞄所需的時間，視要掃瞄的檔案數目和 Security Agent 端點的硬體資源而定。

請設定「手動掃瞄」設定，並將其套用至一或多個用戶端與網域，或套用至伺服器管理的所有用戶端。

設定手動掃瞄設定

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 掃瞄設定 > 手動掃瞄設定」。
4. 在「目標」標籤上，設定下列項目：
   - 要掃瞄的檔案 第 7-23 頁
   - 掃瞄設定 第 7-23 頁
   - CPU 使用率 第 7-25 頁
5. 請點選「動作」標籤，然後設定下列項目：

表 7-7. 中毒處理行動

處理行動	關係
病毒/惡意程式處理行動	主要處理行動（選取一個）： • 使用主動式處理行動 第 7-33 頁 • 對所有的病毒/惡意程式類型使用相同的處理行動 第 7-34 頁 • 對每個病毒/惡意程式類型使用特定的處理行動 第 7-35 頁 注意 如需有關不同處理行動的詳細資訊，請參閱病毒/惡意程式中毒處理行動 第 7-32 頁。 其他病毒/惡意程式處理行動： • 隔離目錄 第 7-35 頁 • 清除前先備份檔案 第 7-36 頁 • 損害清除及復原服務 第 7-37 頁
間諜程式/可能的資安威脅程式處理行動	主要處理行動： • 間諜程式/可能的資安威脅程式中毒處理行動 第 7-42 頁

6. 在「掃瞄例外」標籤上，將目錄、檔案和副檔名設定為從掃瞄中排除。

   如需詳細資訊，請參閱掃瞄例外 第 7-27 頁。

7. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

預約掃瞄

「預約掃瞄」會在指定的日期與時間自動執行。使用「預約掃瞄」，可針對用戶端自動執行例行掃瞄，並提高掃瞄管理效率。

請設定「預約掃瞄」設定，並將其套用至一或多個用戶端與網域，或套用至伺服器管理的所有用戶端。

設定預約掃瞄設定

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 掃瞄設定 > 預約掃瞄設定」。
4. 選取下列選項：
   - 啟動病毒/惡意程式掃瞄
   - 啟動間諜程式/可能的資安威脅程式掃瞄

    注意

   必須先啟動病毒/惡意程式掃瞄，然後才能啟動間諜程式/可能的資安威脅程式掃瞄。
5. 在「目標」標籤上，設定下列項目：
   - 預約 第 7-26 頁
   - 要掃瞄的檔案 第 7-23 頁
   - 掃瞄設定 第 7-23 頁
   - CPU 使用率 第 7-25 頁

6. 請點選「動作」標籤，然後設定下列項目：

表 7-8. 中毒處理行動

處理行動	關係
病毒/惡意程式處理行動	主要處理行動（選取一個）： • 使用主動式處理行動 第 7-33 頁 • 對所有的病毒/惡意程式類型使用相同的處理行動 第 7-34 頁 • 對每個病毒/惡意程式類型使用特定的處理行動 第 7-35 頁 注意 如需有關不同處理行動的詳細資訊，請參閱病毒/惡意程式中毒處理行動 第 7-32 頁。 其他病毒/惡意程式處理行動： • 隔離目錄 第 7-35 頁 • 清除前先備份檔案 第 7-36 頁 • 損害清除及復原服務 第 7-37 頁 • 偵測到病毒/惡意程式時顯示通知訊息 第 7-38 頁 • 偵測到可能的病毒/惡意程式時顯示通知訊息 第 7-38 頁
間諜程式/可能的資安威脅程式處理行動	主要處理行動： • 間諜程式/可能的資安威脅程式中毒處理行動 第 7-42 頁 其他間諜程式/可能的資安威脅程式處理行動： • 偵測到間諜程式/可能的資安威脅程式時顯示通知訊息 第 7-44 頁

7. 在「掃瞄例外」標籤上，將目錄、檔案和副檔名設定為從掃瞄中排除。

   如需詳細資訊，請參閱掃瞄例外 第 7-27 頁。

8. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

立即掃瞄

「立即掃瞄」由管理員透過 Web 主控台從遠端開始，可以將一或多個 Security Agent 端點做為目標。

請設定「手動掃瞄」設定，並將其套用至一或多個 Security Agent 與網域，或套用至伺服器管理的所有 Security Agent。

進行立即掃瞄設定

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 掃瞄設定 > 立即掃瞄設定」。
4. 選取下列選項：
   - 啟動病毒/惡意程式掃瞄
   - 啟動間諜程式/可能的資安威脅程式掃瞄

注意

必須先啟動病毒/惡意程式掃瞄，然後才能啟動間諜程式/可能的資安威脅程式掃瞄。

5. 在「目標」標籤上，設定下列項目：
   - 要掃瞄的檔案 第 7-23 頁
   - 掃瞄設定 第 7-23 頁
   - CPU 使用率 第 7-25 頁
6. 請點選「動作」標籤，然後設定下列項目：

表 7-9. 中毒處理行動

處理行動	關係
病毒/惡意程式處理行動	主要處理行動（選取一個）： • 使用主動式處理行動 第 7-33 頁 • 對所有的病毒/惡意程式類型使用相同的處理行動 第 7-34 頁 • 對每個病毒/惡意程式類型使用特定的處理行動 第 7-35 頁 注意 如需有關不同處理行動的詳細資訊，請參閱病毒/惡意程式中毒處理行動 第 7-32 頁。 其他病毒/惡意程式處理行動： • 隔離目錄 第 7-35 頁 • 清除前先備份檔案 第 7-36 頁 • 損害清除及復原服務 第 7-37 頁
間諜程式/可能的資安威脅程式處理行動	主要處理行動： • 間諜程式/可能的資安威脅程式中毒處理行動 第 7-42 頁

7. 在「掃瞄例外」標籤上，將目錄、檔案和副檔名設定為從掃瞄中排除。

   如需詳細資訊，請參閱掃瞄例外 第 7-27 頁。

8. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

開始立即掃瞄

對您懷疑遭到感染的電腦開始「立即掃瞄」。

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「工作 > 立即掃瞄」。
4. 如果要在開始掃瞄前先變更預先設定的「立即掃瞄」設定，請點選「設定」。

   「立即掃瞄設定」畫面隨即開啟。如需詳細資訊，請參閱立即掃瞄 第 7-19 頁。

5. 在用戶端樹狀結構中，選取要執行掃瞄的用戶端，然後請點選「開始立即掃瞄」。

   伺服器便會傳送通知給用戶端。

6. 檢查通知狀態並確認是否有用戶端未收到通知。

7. 依序請點選「選取不接收通知的端點」和「開始立即掃瞄」，以立即重新傳送通知給未接獲通知的用戶端。

   例如：用戶端總數：50

   表 7-10. 未通知的用戶端案例

用戶端樹狀結構選項	已通知的用戶端（請點選「開始立即掃瞄」之後）	未通知的用戶端
無（會自動選取所有的 50 個用戶端）	50 個用戶端中的 35 個	15 用戶端
手動選取（選取 50 個用戶端中的 45 個）	45 個用戶端中的 40 個	5 個用戶端 + 手動選取未包含的另外 5 個用戶端

8. 請點選「停止通知」，以提示 Apex One 停止通知正在接收通知的用戶端。已經收到通知以及正在執行掃瞄的用戶端將會忽略此命令。
9. 對於正在執行掃瞄的用戶端，請點選「停止立即掃瞄」通知它們停止掃瞄。

所有掃瞄類型的共用設定

請為每種掃瞄類型設定三組設定：掃瞄條件、掃瞄例外和中毒處理行動。請將這些設定部署至一或多個用戶端與網域，或部署至伺服器管理的所有用戶端。

掃瞄條件

請使用檔案類型與副檔名等檔案屬性，指定特定掃瞄類型所應掃瞄的檔案。此外，請指定將會觸發掃瞄的條件。例如，您可以將「即時掃瞄」設定為在每個檔案下載至端點後加以掃瞄。

使用者對檔案執行的活動

選擇對檔案執行哪些活動時會觸發「即時掃瞄」。請選取下列選項：

- 在建立/修改檔案時掃瞄：掃瞄引入端點的新檔案（例如，在下載檔案後），或掃瞄所修改的檔案
- 在擷取檔案時掃瞄：在檔案開啟時掃瞄
- 在建立/修改和擷取檔案時掃瞄

例如，若選取第三個選項，會對下載至端點的新檔案進行掃瞄；若未偵測到安全威脅，則會保留在其目前位置上。當使用者開啟檔案，或使用者修改檔案後要進行儲存前，將會掃瞄該檔案。

要掃瞄的檔案

請選取下列選項：

- 所有可掃瞄的檔案：掃瞄所有檔案
- 智慧型掃瞄所掃瞄的檔案類型：僅掃瞄已知可能含有惡意程式碼的檔案，包括以無害副檔名偽裝的檔案。

  如需詳細資訊，請參閱智慧型掃瞄 第 D-6 頁。
- 具有下列副檔名的檔案：僅掃瞄其副檔名列入副檔名清單中的檔案。請新增副檔名，或移除任何現有的副檔名。

掃瞄設定

請選取下列一或多個選項：

- 在系統關機時掃瞄軟碟機：「即時掃瞄」會在關閉端點前掃瞄軟碟機中是否有開機型病毒。如此可防止任何病毒/惡意程式在使用者透過磁碟重新啟動端點時伺機執行。
- 掃瞄隱藏資料夾：允許 Apex One 在「手動掃瞄」期間偵測端點上的隱藏資料夾，然後加以掃瞄。
- 掃瞄網路磁碟機：在「手動掃瞄」或「即時掃瞄」期間，掃瞄對應至 Security Agent 端點的網路磁碟機或資料夾。

- 在插入 USB 儲存裝置之後掃瞄其開機磁區：在每次使用者插入 USB 儲存裝置時，僅自動掃瞄其開機磁區（即時掃瞄）。
- 在插入卸除式儲存裝置之後掃瞄其中所有檔案：在每次使用者插入 USB 儲存裝置時，自動掃瞄其所有檔案（即時掃瞄）。
- 隔離在記憶體中偵測到的惡意程式變體：「行為監控」會掃瞄系統記憶體中是否有可疑程序，而「即時掃瞄」會對應程序並掃瞄其是否有惡意程式威脅。如果存在惡意程式威脅，「即時掃瞄」會隔離程序和/或檔案。

注意

- 此功能需要管理員啟動「未經授權的變更阻止服務」和「進階防護服務」。
- 記憶體掃瞄會與行為監控中的弱點攻擊防護搭配運作，以針對無檔案型態攻擊提供增強的防護。

- 掃瞄壓縮檔：允許 Apex One 掃瞄指定數目的壓縮層，並略過超出此數目的任何壓縮層。Apex One 也會清除或刪除壓縮檔內的中毒檔案。例如，如果最大層數是兩層，而要掃瞄的壓縮檔有六層，則 Apex One 會掃瞄兩層而略過其餘四層。如果壓縮檔包含安全威脅，Apex One 會清除或刪除該檔案。

注意

Apex One 會將 Office Open XML 格式的 Microsoft Office 2007 檔案視為壓縮檔。Office Open XML 使用 ZIP 壓縮技術，是 Office 2007 應用程式的檔案格式。如果要掃瞄使用這些應用程式建立的檔案中是否有病毒/惡意程式，您必須啟動掃瞄壓縮檔。

- 掃瞄 OLE 物件：當檔案包含多個「物件連結與嵌入」(OLE) 層時，Apex One 會掃瞄指定數目的層，並略過剩餘的層。

  由伺服器管理的所有用戶端在執行「手動掃瞄」、「即時掃瞄」、「預約掃瞄」和「立即掃瞄」期間都會檢查此設定。Apex One 會掃瞄每一層是否包含病毒/惡意程式和間諜程式/可能的資安威脅程式。

  例如：

  您指定的層數是 2。檔案中嵌入的物件是 Microsoft Word 文件（第一層），該 Word 文件又嵌入 Microsoft Excel 試算表（第二層），而試算表

中又嵌入一個 .exe 檔案（第三層）。Apex One 將會掃瞄 Word 文件和 Excel 試算表，並略過 .exe 檔案。

- 在 OLE 檔案中偵測到弱點攻擊程式碼：OLE 弱點攻擊偵測會檢查 Microsoft Office 檔案中是否有弱點攻擊程式碼，主動發現惡意程式。

> **注意**
>
> 指定的層數會同時適用於「掃瞄 OLE 物件」和「偵測弱點攻擊程式碼」選項。

- 啟動 IntelliTrap：偵測並移除壓縮可執行檔中的病毒/惡意程式。此選項僅適用於即時掃瞄。

  如需詳細資訊，請參閱 IntelliTrap 第 D-6 頁。

- 對經由 Web 與電子郵件通道下載的檔案啟動 CVE 弱點攻擊掃瞄：根據常見弱點和漏洞 (CVE) 系統，封鎖會嘗試攻擊市售產品已知弱點的程序。此選項僅適用於即時掃瞄。
- 掃瞄開機區：在「手動掃瞄」、「預約掃瞄」與「立即掃瞄」期間，掃瞄硬碟的開機磁區中是否有病毒/惡意程式。

CPU 使用率

Apex One 可在掃瞄某個檔案後、掃瞄下一個檔案之前暫停。「手動掃瞄」、「預約掃瞄」與「立即掃瞄」期間均適用此設定。

請選取下列選項：

- 高：掃瞄之間不暫停
- 中：如果 CPU 耗用大於 50% 便在檔案掃瞄間暫停；如果等於或小於 50% 則不暫停
- 低：如果 CPU 耗用大於 20% 便在檔案掃瞄間暫停；如果等於或小於 20% 則不暫停

如果您選擇「中」或「低」，在掃瞄啟動後若 CPU 耗用在門檻值（50% 或 20%）以內，Apex One 將不會在掃瞄之間暫停，如此可縮短掃瞄時間。Apex

One 在此程序中會使用較多的 CPU 資源，但由於 CPU 耗用已最佳化，因此端點效能不會受到嚴重影響。當 CPU 耗用開始超過門檻值時，Apex One 即會暫停以降低 CPU 使用率，而在耗用再度回落在門檻值之內時結束暫停。

如果您選擇「高」，Apex One 將不會檢查實際的 CPU 耗用，而會持續掃瞄檔案不暫停。

預約

設定執行「預約掃瞄」的頻率（每天、每週或每月）和時間。

對於每月「預約掃瞄」，您可以選擇月份中的特定日期，或當月中的第幾個星期幾。

- 月份中的特定日期：在第 1 日到第 31 日之間進行選取。如果選取第 29 日、第 30 日或第 31 日，但該月沒有此日期，則 Apex One 會在該月最後一天執行「預約掃瞄」。因此：
  - 如果選取第 29 日，則「預約掃瞄」會在 2 月 28 日執行（閏年除外），而對於所有其他月份則在第 29 日執行。
  - 如果選取第 30 日，則「預約掃瞄」會在 2 月 28 或 29 日執行，而對於所有其他月份則在第 30 日執行。
  - 如果選取第 31 日，則「預約掃瞄」會在 2 月 28 或 29 日、4 月 30 日、6 月 30 日、9 月 30 日、11 月 30 日執行，而對於所有其他月份則在第 31 日執行。
- 當月中的第幾個星期幾：一週中的某一天每個月都會出現四或五次。例如：一個月通常有四個星期一。指定當月中的第幾個星期幾。例如：選擇在每個月的第二個星期一執行「預約掃瞄」。如果選擇第五個星期中的某一天，而這一天在特定月份中只出現四次，則掃瞄將於第四個星期中的這一天執行。

掃瞄例外

設定掃瞄例外可提高掃瞄效能，並略過會導致誤判警訊的檔案。在執行特定掃瞄類型時，Apex One 會檢查掃瞄例外清單，以判定端點上有哪些檔案將同時排除在病毒/惡意程式與間諜程式/可能的資安威脅程式掃瞄之外。

當您啟動掃瞄例外時，Apex One 將不會掃瞄處於下列情況的檔案：

- 位於特定目錄（或任何其子目錄）下的檔案。
- 檔案名稱符合例外清單中的任何名稱。
- 副檔名符合例外清單中的任何副檔名。

秘訣

如需趨勢科技建議排除在「即時掃瞄」作業之外的產品清單，請移至：

http://esupport.trendmicro.com/solution/en-US/1059770.aspx

萬用字元例外

檔案和目錄的掃瞄例外清單支援使用萬用字元。使用「?」字元取代一個字元，使用「*」取代多個字元。

請謹慎使用萬用字元。用錯字元可能會排除不適當的檔案或目錄。例如，新增 C:* 至「掃瞄例外清單 (檔案)」將不會掃瞄整個 C:\ 磁碟機。

表 7-11. 使用萬用字元的掃瞄例外

值	已排除	未排除
c:\director*\fil*.txt	c:\directory\fil\doc.txt c:\directories\fil\files\document.txt	c:\directory\file\ c:\directories\files\ c:\directory\file\doc.txt c:\directories\files\document.txt

值	已排除	未排除
`c:\director?\file\*.txt`	`c:\directory\file\doc.txt`	`c:\directories\file\document.txt`
`c:\director?\file\?.txt`	`c:\directory\file\1.txt`	`c:\directory\file\doc.txt` `c:\directories\file\document.txt`
`c:\*.txt`	`C:\` 目錄中的所有 `.txt` 檔案	`C:\` 目錄中的所有其他檔案類型
`[]`	不支援	不支援

掃瞄例外清單 (目錄)

Apex One 不會掃瞄位於電腦上特定目錄下的所有檔案。您最多可以指定 256 個目錄。

注意

Apex One 可藉由將目錄從掃瞄任務中排除，來將該目錄的所有子目錄從掃瞄任務中排除。

您也可以選擇「不掃瞄趨勢科技產品的安裝目錄」。如果您選取此選項，Apex One 就會自動將下列趨勢科技產品的目錄排除在掃瞄作業之外：

- <伺服器安裝資料夾>

  注意

  在手動掃瞄期間，Apex One 仍會掃瞄伺服器安裝資料夾。

- IM 安全性
- InterScan eManager 3.5x
- InterScan Web Security Suite
- InterScan Web Protect

- InterScan FTP VirusWall
- InterScan Web VirusWall
- InterScan NSAPI Plug-in
- InterScan E-mail VirusWall
- ScanMail eManager™ 3.11、5.1、5.11、5.12
- ScanMail for Lotus Notes™ eManager NT
- ScanMail™ for Microsoft Exchange

如果您的趨勢科技產品「不」包含在此清單中，請將該產品目錄新增到掃瞄例外清單。

此外，請移至「安全設定」標籤上「用戶端 > 全域用戶端設定」的「掃瞄設定」區段，來設定 Apex One 排除 Microsoft Exchange 2000/2003 目錄。如果您使用 Microsoft Exchange 2007 或更新版本，請手動將目錄新增至掃瞄例外清單中。如需掃瞄例外的詳細資訊，請參閱下列網站：

http://technet.microsoft.com/en-us/library/bb332342.aspx

設定檔案清單時，請從下列選項進行選擇：

- 保留目前清單（預設）：Apex One 提供此選項以避免意外覆寫用戶端的現有例外清單。若要儲存和部署對例外清單所做的變更，請選取其他任何選項。
- 覆寫：此選項會移除用戶端上的整個例外清單，並使用目前清單取而代之。請點選「套用至所有用戶端」之後，Apex One 會顯示確認警告訊息。
- 將路徑新增到：此選項會將目前清單中的項目新增至用戶端的現有例外清單。如果某個項目已存在於用戶端的例外清單中，則用戶端會略過該項目。
- 移除下列位置中的路徑：此選項會從用戶端的現有例外清單（如找到）移除您目前清單中的項目。

掃瞄例外清單支援的系統變數（目錄）

您可以使用一般 Windows 系統變數來設定目錄的「掃瞄例外清單」。下表列出 Apex One 支援的變數。

系統變數	說明
%ALLUSERSPROFILE%	是指 `%PROFILESFOLDER%\Public` 或 `%PROFILESFOLDER%\all users` 資料夾 例如： • 在 Windows 7 中，%ALLUSERSPROFILE% 的預設位置是： `C:\ProgramData`
%COMMONPROGRAMFILES(X86)%	是指 64 位元系統上的 `C:\Program Files (x86)\Common Files` 資料夾
%PROGRAMFILES%	Program Files 資料夾 典型路徑為 `C:\Program Files`
%PROGRAMFILES(X86)%	是指 64 位元系統上的 `C:\Program Files (x86)` 資料夾
%SYSTEMROOT%	是指系統磁碟機的根目錄 典型路徑為 `C:\Windows`
%WINDIR%	是指位於系統磁碟機上的 Windows 資料夾 典型路徑為 `C:\Windows`

掃瞄例外清單（檔案）

如果檔案名稱符合此例外清單中包含的任何名稱，則 Apex One 不會掃瞄該檔案。如果想要排除位於端點上特定位置下的檔案，請包含檔案路徑，如 `C:\Temp\sample.jpg`。

您最多可以指定 256 個檔案。

設定檔案清單時，請從下列選項進行選擇：

- 保留目前清單（預設）：Apex One 提供此選項以避免意外覆寫用戶端的現有例外清單。若要儲存和部署對例外清單所做的變更，請選取其他任何選項。
- 覆寫：此選項會移除用戶端上的整個例外清單，並使用目前清單取而代之。請點選「套用至所有用戶端」之後，Apex One 會顯示確認警告訊息。
- 將路徑新增到：此選項會將目前清單中的項目新增至用戶端的現有例外清單。如果某個項目已存在於用戶端的例外清單中，則用戶端會略過該項目。
- 移除下列位置中的路徑：此選項會從用戶端的現有例外清單（如找到）移除您目前清單中的項目。

掃瞄例外清單 (副檔名)

如果檔案的副檔名符合此例外清單中包含的任何副檔名，Apex One 即不會掃瞄該檔案。您最多可以指定 256 個副檔名。副檔名之前不需要加句號 (.)。

若為「手動掃瞄」、「預約掃瞄」與「立即掃瞄」，請使用問號 (?)（用於取代單一字元）或星號 (*)（用於取代多個字元）做為萬用字元。例如，如果您不要掃瞄副檔名以 D 開頭的所有檔案（例如 DOC、DOT 或 DAT），請輸入 `D*` 或 `D??`。

注意

「即時掃瞄」不支援在指定的副檔名中使用萬用字元。

套用掃瞄例外設定至所有掃瞄類型

Apex One 可讓您為特定掃瞄類型設定掃瞄例外設定，然後將相同的設定套用至所有其他的掃瞄類型。例如：

Apex One 管理員 Chris 於 1 月 1 日發現用戶端電腦上有大量的 JPG 檔案，並確認這些檔案不具任何安全威脅。Chris 將 JPG 新增至「手動掃瞄」的檔案例外清單中，然後將此設定套用至所有掃瞄類型。此時，「即時掃瞄」、「立即掃瞄」與「預約掃瞄」均已設定成略過 .jpg 檔案的掃瞄。

一週後，Chris 從「即時掃瞄」的例外清單中移除了 JPG，但並未將掃瞄例外設定套用至所有掃瞄類型。現在將會掃瞄 JPG 檔案，但僅限於「即時掃瞄」期間。

中毒處理行動

指定 Apex One 在特定掃瞄類型偵測到安全威脅時所執行的處理行動。Apex One 針對病毒/惡意程式和間諜程式/可能的資安威脅程式有一組不同的中毒處理行動。

病毒/惡意程式中毒處理行動

Apex One 執行的中毒處理行動視病毒/惡意程式種類和偵測到病毒/惡意程式的掃瞄類型而定。例如，當 Apex One 在手動掃瞄（掃瞄類型）過程中偵測到特洛伊木馬程式（病毒/惡意程式類型）時，會清除（中毒處理行動）中毒的檔案。

如需不同病毒/惡意程式類型的詳細資訊，請參閱病毒和惡意程式 第 7-2 頁。

下列是 Apex One 可針對病毒/惡意程式執行的處理行動。

表 7-12. 病毒/惡意程式中毒處理行動

處理行動	說明
刪除	Apex One 會刪除中毒的檔案。
隔離	Apex One 會重新命名並加密中毒檔案，然後將其移至用戶端端點上位於 <用戶端安裝資料夾>\Suspect 中的暫時隔離目錄。 然後，Security Agent 會將已隔離的檔案傳送到指定的隔離目錄。 如需詳細資訊，請參閱隔離目錄 第 7-35 頁。 預設隔離目錄在 Apex One 伺服器上的 <伺服器安裝資料夾>\PCCSRV\Virus 下。 如果您需要恢復任何已隔離的檔案，請使用中央隔離區恢復。 如需詳細資訊，請參閱恢復隔離的檔案 第 7-38 頁。

處理行動	說明
清除	Apex One 會先清除中毒的檔案，才允許完整存取該檔案。 如果無法清除檔案，Apex One 會執行第二個中毒處理行動，可能是下列其中一個中毒處理行動：隔離、刪除、重新命名與暫不處理。 如果要設定第二個處理行動，請移至「用戶端 > 用戶端管理」。請點選「設定 > 掃瞄設定 > {掃瞄類型} > 處理行動」標籤。 系統可對所有類型的惡意程式（但不包括可能的病毒/惡意程式）執行此處理行動。
重新命名	Apex One 會將中毒檔案的副檔名變更為「vir」。使用者一開始無法開啟重新命名的檔案，但是如果使檔案與特定的應用程式產生關聯，就可以開啟該檔案。 開啟重新命名的中毒檔案時，可能會執行病毒/惡意程式。
暫不處理	Apex One 只有在「手動掃瞄」、「預約掃瞄」和「立即掃瞄」過程中偵測到任何類型的病毒時，才可以使用此中毒處理行動。Apex One 在即時掃瞄過程中無法使用此中毒處理行動，因為在偵測到嘗試開啟或執行中毒的檔案時，若未執行任何中毒處理行動，則會允許執行病毒/惡意程式。「即時掃瞄」過程中可以使用其他所有的中毒處理行動。
拒絕存取	此中毒處理行動只能在「即時掃瞄」過程中執行。當 Apex One 偵測到嘗試開啟或執行中毒的檔案時，會立即阻止該操作。 使用者可以手動刪除中毒的檔案。

使用主動式處理行動

不同類型的病毒/惡意程式需要不同的中毒處理行動。自訂中毒處理行動需要具備病毒/惡意程式的相關知識，並且可能會是一項冗長而乏味的工作。Apex One 會使用「主動式處理行動」來解決這些問題。

「主動式處理行動」是一套預先設定的中毒處理行動，可以處理病毒/惡意程式。如果您不熟悉中毒處理行動，或是不確定何種中毒處理行動適合那一種特定的病毒/惡意程式，趨勢科技建議您使用「主動式處理行動」。

使用「主動式處理行動」具有以下優點：

- 「主動式處理行動」會使用趨勢科技建議的中毒處理行動。您不需要耗費時間來設定中毒處理行動。

- 病毒撰寫者會不斷變更病毒/惡意程式攻擊電腦的方式。更新「主動式處理行動」設定以抵禦最新威脅和最新的病毒/惡意程式攻擊方法。

注意

進行間諜程式/可能的資安威脅程式掃瞄時，無法使用主動式處理行動。

下表說明「主動式處理行動」處理每種類型病毒/惡意程式的方式：

表 7-13. 趨勢科技建議的病毒/惡意程式中毒處理行動

病毒/惡意程式類型	即時掃瞄		手動掃瞄/預約掃瞄/立即掃瞄	
	第一個中毒處理行動	第二個中毒處理行動	第一個中毒處理行動	第二個中毒處理行動
CVE 弱點攻擊	拒絕存取	無	無	無
惡作劇	隔離	無	隔離	無
特洛伊木馬程式	隔離	無	隔離	無
病毒	清除	隔離	清除	隔離
測試病毒	拒絕存取	無	暫不處理	無
封裝程式	隔離	無	隔離	無
可能的惡意程式	拒絕存取或使用者設定的處理行動	無	暫不處理或使用者設定的處理行動	無
其他惡意程式	清除	隔離	清除	隔離

對於可能的惡意程式，即時掃瞄期間的預設中毒處理行動是「拒絕存取」，而手動掃瞄、預約掃瞄和立即掃瞄期間的預設中毒處理行動是「暫不處理」。如果這些不是您的偏好處理行動，可以將其變更為「隔離」、「刪除」或「重新命名」。

對所有的病毒/惡意程式類型使用相同的處理行動

如果您要對可能的病毒/惡意程式以外的所有病毒/惡意程式類型執行相同的處理行動，請選取此選項。若您選擇「清除」做為第一個處理行動，請選取清除

不成功時 Apex One 所要執行的第二個處理行動。如果第一個處理行動不是「清除」，則無法設定第二個處理行動。

如果選擇「清除」作為第一項處理行動，則 Apex One 在偵測到可能的病毒/惡意程式時會執行第二項處理行動。

對每個病毒/惡意程式類型使用特定的處理行動

針對每一種病毒/惡意程式類型手動選取中毒處理行動。

對於可能的病毒/惡意程式以外的全部病毒/惡意程式類型，所有中毒處理行動均可用。若您選擇「清除」做為第一個處理行動，請選取清除不成功時 Apex One 所要執行的第二個處理行動。如果第一個處理行動不是「清除」，則無法設定第二個處理行動。

對於可能的病毒/惡意程式，「清除」以外的所有中毒處理行動均可用。

隔離目錄

如果針對中毒檔案的處理行動為「隔離」，則 Security Agent 會加密該檔案，並將其移至 <用戶端安裝資料夾>\SUSPECT 下的暫時隔離資料夾，然後將檔案傳送至指定的隔離目錄。

注意

您可以在日後需要存取加密的隔離檔案時加以恢復。

如需詳細資訊，請參閱恢復加密檔案 第 7-39 頁。

接受位於 Apex One 伺服器電腦上的預設隔離目錄。此目錄採用 URL 格式，並且包含伺服器的主機名稱或 IP 位址。

- 如果伺服器同時管理 IPv4 和 IPv6 用戶端，請使用主機名稱，以便所有 Security Agent 都可以將隔離檔案傳送到伺服器。
- 如果伺服器只具有 IPv4 位址，或只透過其 IPv4 位址進行識別，則只有純 IPv4 和雙堆疊 Security Agent 可以將隔離檔案傳送到伺服器。

- 如果伺服器只具有 IPv6 位址，或只透過其 IPv6 位址進行識別，則只有純 IPv6 和雙堆疊 Security Agent 可以將隔離檔案傳送到伺服器。

您也可以輸入 URL、UNC 路徑或絕對檔案路徑格式的位置來指定替代的隔離目錄。Security Agent 應該可以連線到此替代目錄。例如，如果替代目錄將接收來自雙堆疊和純 IPv6 Security Agent 的隔離檔案，此目錄應具有 IPv6 位址。趨勢科技建議指定雙堆疊替代目錄、透過其主機名稱識別目錄並在輸入目錄時使用 UNC 路徑。

如需何時應使用 URL、UNC 路徑或絕對檔案路徑的相關指引，請參閱下表：

表 7-14. 隔離目錄

隔離目錄	接受的格式	範例	注意
管理伺服器電腦上的目錄	URL	`http://<osceserver>`	這是預設的目錄。 進行此目錄的設定，如隔離資料夾的大小等。 如需詳細資訊，請參閱隔離區管理員 第 14-54 頁。
	UNC 路徑	`\\<osceserver>\ofcscan\Virus`	
其他 Apex One 伺服器電腦上的目錄（若您在網路上有其他 Apex One 伺服器）	URL	`http://<osceserver2>`	確定 Security Agent 可連線到此目錄。如果您指定不正確的目錄，Security Agent 會將隔離的檔案保留在 SUSPECT 資料夾中，直到指定正確的隔離目錄為止。在伺服器的病毒/惡意程式記錄檔中，掃瞄結果為「無法將隔離檔案傳送到指定的隔離資料夾」。 如果您使用 UNC 路徑，請確定是否可讓「Everyone」群組共享隔離目錄資料夾，並指定讀取和寫入權限給這個群組。
	UNC 路徑	`\\<osceserver2>\ofcscan\Virus`	
網路上的其他端點	UNC 路徑	`\\<computer_name>\temp`	
Security Agent 上的其他目錄	絕對路徑	`C:\temp`	

清除前先備份檔案

如果 Apex One 設定為清除中毒的檔案，它將會先備份檔案。這可讓您在日後需要檔案時加以回存。Apex One 會加密備份檔案以防止他人開啟，然後將檔案儲存在 <用戶端安裝資料夾>\Backup 資料夾中。

如果要恢復加密的備份檔案，請參閱恢復加密檔案 第 7-39 頁。

損害清除及復原服務

損害清除及復原服務會清除電腦上的 File-based 和網路病毒，以及殘存病毒和蠕蟲（特洛伊木馬程式、登錄項目、病毒檔案）。

用戶端 會在病毒/惡意程式掃瞄之前或之後觸發「損害清除及復原服務」，具體取決於掃瞄類型。

- 當「手動掃瞄」、「預約掃瞄」或「立即掃瞄」執行時，Security Agent 會先觸發「損害清除及復原服務」，然後繼續執行病毒/惡意程式掃瞄。在病毒/惡意程式掃瞄期間，如果需要進行清除，用戶端可能會再次觸發「損害清除及復原服務」。
- 在「即時掃瞄」期間，如果需要進行清除，Security Agent 會先執行病毒/惡意程式掃瞄，然後觸發「損害清除及復原服務」。

您可以選取損害清除及復原服務執行的清除類型：

- 標準清除：Security Agent 會在標準清除期間執行下列任何處理行動：
  - 偵測並移除活動的特洛伊木馬程式
  - 終結特洛伊木馬程式所建立的處理程序
  - 修復特洛伊木馬程式修改的系統檔案
  - 刪除特洛伊木馬程式遺留的檔案和應用程式
- 進階清除：除了標準清除處理行動外，Security Agent 還會遏止詐欺安全軟體（亦稱為 FakeAV）及某些 Rootkit 變體的活動。Security Agent 也會使用進階清除規則來主動偵測，並停止出現 FakeAV 和 Rootkit 行為的應用程式。

注意

提供主動式安全防護的同時，進階清除也會導致大量誤報。

損害清除及復原服務不會對可能的病毒/惡意程式執行清除，除非選取「偵測到可能的病毒/惡意程式時執行清除」選項。只有對可能的病毒/惡意程式的處理

行動不是「暫不處理」也不是「拒絕存取」時，才能選取該選項。例如，如果 Security Agent 在「即時掃瞄」期間偵測到可能的病毒/惡意程式，且處理行動為「隔離」，則 Security Agent 會先隔離中毒檔案，然後根據需要執行清除。清除類型（標準或進階）取決於您的選擇。

偵測到病毒/惡意程式時顯示通知訊息

Apex One 若在「即時掃瞄」與「預約掃瞄」期間偵測到病毒/惡意程式，它會顯示通知訊息，讓使用者得知偵測的相關資訊。

如果要修改通知訊息，請從「管理 > 通知 > 用戶端」中的「類型」下拉式清單選取「病毒/惡意程式」。

偵測到可能的病毒/惡意程式時顯示通知訊息

Apex One 若在「即時掃瞄」與「預約掃瞄」期間偵測到可能的病毒/惡意程式，它會顯示通知訊息，讓使用者得知偵測的相關資訊。

如果要修改通知訊息，請從「管理 > 通知 > 用戶端」中的「類型」下拉式清單選取「病毒/惡意程式」。

恢復隔離的檔案

如果您確信偵測不正確，您可以恢復 Apex One 隔離的檔案。「中央隔離區還原」功能可讓您搜尋隔離目錄中的檔案以及執行 SHA1 驗證檢查，以確認您要恢復的檔案沒有進行任何修改。

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，選取某個網域或選取任一用戶端。
3. 請點選「工作 > 中央隔離區還原」。

   會出現「中央隔離區還原條件」畫面。

4. 在「中毒檔案/物件」欄位中輸入要恢復之資料的名稱。
5. 視需要指定時間範圍、安全威脅名稱與資料的檔案路徑。
6. 請點選「搜尋」。

   會出現「中央隔離區還原」畫面，其中顯示搜尋結果。
7. 選取「將已恢復檔案新增到網域層級例外清單」，以確保恢復檔案之網域中的所有 Security Agent 將檔案新增到掃瞄例外清單。

   這可確保 Apex One 在日後的掃瞄期間不會將檔案偵測為安全威脅。

   重要

   Security Agent 使用 Apex Central 策略進行管理僅適用於已恢復的檔案例外，直到 Apex Central 伺服器下次更新 Security Agent 策略並覆寫例外清單。若要防止 Security Agent 重新掃瞄已恢復的檔案，請將檔案例外新增到 Apex Central Security Agent 策略。
8. 視需要輸入檔案的 SHA-1 值，以用於驗證目的。
9. 從清單中選取要恢復的檔案，然後請點選「恢復」。

   秘訣

   如果要檢視恢復檔案的個別 Security Agent，請點選「端點」欄位中的連結。
10. 請點選確認對話方塊中的「關閉」。

    如果要驗證 Apex One 是否成功恢復隔離檔案，請參閱檢視中央隔離區恢復記錄檔 第 7-85 頁。

恢復加密檔案

為了防止開啟中毒檔案，Apex One 會在下列情況下加密檔案：

- 隔離檔案前

- 在清除檔案前加以備份時

Apex One 提供了一個工具，可讓您將檔案解密，然後在您需要擷取檔案中的資訊時恢復檔案。Apex One 可以解密及恢復下列檔案：

表 7-15. Apex One 可解密及恢復的檔案

檔案	說明
用戶端端點上的隔離檔案	這些檔案位於 <用戶端安裝資料夾>\SUSPECT\Backup 資料夾中，會在 7 天後自動清除。這些檔案也會上傳至 Apex One 伺服器上的指定隔離目錄。
指定隔離目錄中的隔離檔案	依預設，此目錄位於 Apex One 伺服器電腦上。 如需詳細資訊，請參閱隔離目錄 第 7-35 頁。
備份的加密檔案	這些是 Apex One 可清除之中毒檔案的備份。這些檔案位於 <用戶端安裝資料夾>\Backup 資料夾中。如果要恢復這些檔案，使用者必須將其移至 <用戶端安裝資料夾>\SUSPECT\Backup 資料夾中。 您必須移至「用戶端 > 用戶端管理」並請點選「設定 > 掃瞄設定 > {掃瞄類型} > 處理行動」標籤，然後選取「清除前先備份檔案」，Apex One 才會在清除前先備份並加密檔案。

警告!

恢復中毒檔案可能會將病毒/惡意程式散佈到其他檔案與電腦。在恢復檔案前，請先隔離中毒的端點，並將此端點上的重要檔案移至備份位置。

解密和恢復檔案

步驟

- 如果檔案位於 Security Agent 端點上：
  a. 開啟命令提示字元，然後移至 <用戶端安裝資料夾>。
  b. 透過按兩下檔案或在命令提示字元中輸入下列內容來執行 VSEncode.exe：

```
VSEncode.exe /u
```

此參數會開啟一個畫面，其中顯示位於 <用戶端安裝資料夾>\SUSPECT\Backup 下的檔案清單。

c. 選取要恢復的檔案，然後請點選「恢復」。此工具一次只能恢復一個檔案。

d. 在開啟的畫面中，指定要將檔案恢復到哪個資料夾。

e. 請點選「確定」。檔案即會恢復到指定的資料夾。

注意

在檔案恢復後，Apex One 有可能重新掃瞄該檔案，並將其視為中毒檔案。為了防止該檔案遭到掃瞄，請將其新增至掃瞄例外清單中。如需詳細資訊，請參閱掃瞄例外 第 7-27 頁。

f. 完成檔案恢復後，請點選「關閉」。

- 如果檔案位於 Apex One 伺服器或自訂的隔離目錄中：

a. 如果檔案位於 Apex One 伺服器電腦上，請開啟命令提示字元，然後移至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\VSEncrypt。

如果檔案位於自訂的隔離目錄中，請瀏覽至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility，然後將 VSEncrypt 資料夾複製到自訂隔離目錄所在的端點上。

b. 建立文字檔，然後輸入要加密或解密的檔案的完整路徑。

例如，如果要恢復 C:\My Documents\Reports 中的檔案，請在文字檔中輸入 C:\My Documents\Reports*.*。

Apex One 伺服器電腦上的隔離檔案位於 <伺服器安裝資料夾>\PCCSRV\Virus 下。

c. 以 INI 或 TXT 副檔名儲存文字檔。例如，您可以在 C: 磁碟機上將其儲存為 ForEncryption.ini。

d. 開啟命令提示字元，然後移至 VSEncrypt 資料夾所在的目錄。

e. 輸入下列命令，以執行 VSEncode.exe：

```
VSEncode.exe /d /i <INI 或 TXT 檔案的位置>
```

說明：

<INI 或 TXT 檔案的位置> 就是您建立的 INI 或 TXT 檔案的路徑（例如：C:\ForEncryption.ini）。

f. 使用其他參數發出各種命令。

表 7-16. 恢復參數

參數	說明
無（沒有參數）	加密檔案
/d	解密檔案
/debug	建立偵錯記錄檔，並將其儲存至端點。在 Security Agent 端點上，偵錯記錄檔 VSEncrypt.log 會建立於 <用戶端安裝資料夾>。
/o	覆寫已存在的加密或解密檔案
/f <檔案名稱>	加密或解密單一檔案
/nr	不恢復原始檔名
/v	顯示工具的相關資訊
/u	啟動工具的使用者介面
/r <目標資料夾>	用以恢復檔案的資料夾
/s <原始檔案名稱>	原始加密檔案的檔名

例如，輸入 VSEncode [/d] [/debug]，可以解密 Suspect 資料夾中的檔案，並建立偵錯記錄檔。當您解密或加密檔案時，Apex One 便會在相同資料夾中建立解密或加密檔案。在解密或加密檔案前，請確認檔案並未鎖定。

間諜程式/可能的資安威脅程式中毒處理行動

Apex One 執行的中毒處理行動視偵測到間諜程式/可能的資安威脅程式的掃瞄類型而定。您可以為每個病毒/惡意程式類型設定特定的處理行動，但對於所有

類型的間諜程式/可能的資安威脅程式，則只能設定一個處理行動。例如，當 Apex One 在「手動掃瞄」（掃瞄類型）過程中偵測到任何類型的間諜程式/可能的資安威脅程式時，會清除（中毒處理行動）受影響的系統資源。

如需不同間諜程式/可能的資安威脅程式類型的相關資訊，請參閱間諜程式和可能的資安威脅程式 第 7-4 頁。

注意

間諜程式/可能的資安威脅程式中毒處理行動只能透過 Web 主控台設定。Security Agent 主控台不提供對這些設定的存取。

下表列出 Apex One 可針對間諜程式/可能的資安威脅程式執行的處理行動。

表 7-17. 間諜程式/可能的資安威脅程式中毒處理行動

處理行動	說明
清除	Apex One 會終止程序或刪除登錄、檔案、Cookie 和捷徑。 在清除間諜程式/可能的資安威脅程式後，Security Agent 會備份間諜程式/可能的資安威脅程式資料，如果您認為可安全存取這些間諜程式/可能的資安威脅程式，便可恢復這些資料。 如需詳細資訊，請參閱回存間諜程式/可能的資安威脅程式 第 7-46 頁。
暫不處理	Apex One 不會對偵測到的間諜程式/可能的資安威脅程式元件執行任何中毒處理行動，但是會在記錄檔中記錄偵測到間諜程式/可能的資安威脅程式。此處理行動只能在「手動掃瞄」、「預約掃瞄」與「立即掃瞄」期間執行。在「即時掃瞄」期間，處理行動為「拒絕存取」。 如果偵測到的間諜程式/可能的資安威脅程式包含在核可清單中，Apex One 將不會執行任何處理行動。 如需詳細資訊，請參閱間諜程式/可能的資安威脅程式核可清單 第 7-44 頁。
拒絕存取	Apex One 會拒絕存取（複製、開啟）偵測到的間諜程式/可能的資安威脅程式元件。此處理行動只能在「即時掃瞄」期間執行。在「手動掃瞄」、「預約掃瞄」和「立即掃瞄」期間，處理行動為「暫不處理」。

偵測到間諜程式/可能的資安威脅程式時顯示通知訊息

Apex One 若在「即時掃瞄」與「預約掃瞄」期間偵測到間諜程式/可能的資安威脅程式，它會顯示通知訊息，讓使用者得知偵測的相關資訊。

如果要修改通知訊息，請從「管理 > 通知 > 用戶端」中的「類型」下拉式清單選取「間諜程式/可能的資安威脅程式」。

間諜程式/可能的資安威脅程式核可清單

Security Agent 會提供「核可的」間諜程式/可能的資安威脅程式清單，其中包含您不希望被視為間諜程式/可能的資安威脅程式的檔案或應用程式。在掃瞄期間偵測到特定的間諜程式/可能的資安威脅程式時，Security Agent 會檢查核可清單，如果在核可清單中找到相符項目，則不會執行任何處理行動。

請將核可清單套用至一或多個 Security Agent 與網域，或套用至伺服器管理的所有 Security Agent。將核可清單套用至所有的掃瞄類型，表示在「手動掃瞄」、「即時掃瞄」、「預約掃瞄」與「立即掃瞄」期間，都將使用相同的核可清單。

將已偵測到的間諜程式/可能的資安威脅程式加入核可清單

步驟

1. 移至下列其中一個項目：
   - 用戶端 > 用戶端管理
   - 記錄檔 > 用戶端 > 安全威脅
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「記錄檔 > 間諜程式/可能的資安威脅程式記錄檔」或「檢視記錄檔 > 間諜程式/可能的資安威脅程式記錄檔」。

4. 指定記錄條件，然後請點選「顯示記錄檔」。
5. 選取記錄檔，然後請點選「新增到核可清單」。
6. 只將許可的間諜程式/可能的資安威脅程式套用至選取的用戶端電腦，或是套用至特定網域。
7. 請點選「儲存」。選取的用戶端會套用該設定，Apex One 伺服器會將間諜程式/可能的資安威脅程式新增至用戶端 > 用戶端管理>「設定」 > 「間諜程式/可能的資安威脅程式核可清單」中的核可清單。

注意

Apex One 最多可在核可清單中容納 1024 個間諜程式/可能的資安威脅程式。

管理間諜程式/可能的資安威脅程式核可清單

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 間諜程式/可能的資安威脅程式核可清單」。
4. 在「間諜程式/可能的資安威脅程式名稱」表格中，選取間諜程式/可能的資安威脅程式名稱。如果要選取多個名稱，請按住 CTRL 鍵並進行選取。
   - 您也可以在「搜尋」欄位中輸入關鍵字，然後點選「搜尋」。表格會以符合關鍵字的名稱重新整理。
5. 請點選「新增」。

   名稱會移至「核可清單」表格中。
6. 如果要從核可清單移除名稱，請選取名稱並請點選「移除」。如果要選取多個名稱，請按住 CTRL 鍵並進行選取。

7. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

回存間諜程式/可能的資安威脅程式

清除間諜程式/可能的資安威脅程式後，Security Agent 會備份間諜程式/可能的資安威脅程式資料。如果您認為資料無害，請通知線上用戶端恢復備份的資料。請根據備份時間選擇要恢復的間諜程式/可能的資安威脅程式資料。

注意

Security Agent 使用者無法開始間諜程式/可能的資安威脅程式恢復，而且不會接獲用戶端能夠恢復哪些備份資料的通知。

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，開啟某個網域，然後選取任一用戶端。

   注意

   每次只有一個用戶端可以執行間諜程式/可能的資安威脅程式恢復。

3. 請點選「工作 > 間諜程式/可能的資安威脅程式恢復」。
4. 如果要檢視各資料區段所要恢復的項目，請點選「檢視」。

   接著會顯示一個新畫面。請點選「返回」可回到上一個畫面。

5. 選取您要恢復的資料區段。

6. 請點選「恢復」。

   Apex One 會通知您恢復狀態。請檢查間諜程式/可能的資安威脅程式的恢復記錄檔，以取得完整報告。如需詳細資訊，請參閱檢視間諜程式/可能的資安威脅程式恢復記錄檔 第 7-89 頁。

信任的程式清單

您可以設定 Security Agent 在執行 Application Control、行為監控、周邊設備存取控管、Endpoint Sensor 和即時掃瞄時，略過掃瞄信任的程序。將程式新增到「信任的程式清單」後，Security Agent 不再對由該程式開始的程式或任何處理程序執行「即時掃瞄」。將信任的程式新增到「信任的程式清單」，以提升端點上的掃瞄效能。

注意

您可以將符合下列要求的檔案新增到「信任的程式」清單中：

- 檔案位於 Windows 系統目錄以外的位置。
- 檔案擁有有效的數位簽章。

將程式新增到「信任的程式清單」後，Security Agent 會自動從下列掃瞄中排除該程式：

- Application Control（只能在 Apex Central 主控台上設定）
- 行為監控
- 周邊設備存取控管
- Endpoint Sensor（只能在 Apex Central 主控台上設定）
- 即時掃瞄：檢查檔案和程序掃瞄

設定信任的程式清單

列在「信任的程式清單」中的程式以及程式所呼叫的所有子程序，都會排除在 Application Control、行為監控、周邊設備存取控管、Endpoint Sensor 和即時掃瞄之外。

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 信任的程式清單」。
4. 輸入要從清單中排除之程式的完整程式路徑。
5. 請點選「新增到信任的程式清單」。
6. 如果要從清單中移除程式，請點選「刪除」圖示。
7. 如果要匯出信任的程式清單，請點選「匯出」並為檔案選取位置。

   注意

   Apex One 會以 DAT 格式儲存清單。

8. 如果要匯入信任的程式清單，請點選「匯入」並為檔案選取位置。
   a. 請點選「瀏覽...」並選取 DAT 檔案的位置。
   b. 請點選「匯入」。
9. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。

- 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

掃瞄權限和其他設定

具有掃瞄權限的使用者，比較能控制掃瞄其電腦上的檔案的方式。具有掃瞄權限的使用者或 Security Agent 可以執行下列工作：

- 使用者可以設定「手動掃瞄」、「預約掃瞄」與「即時掃瞄」設定。如需詳細資訊，請參閱掃瞄類型權限 第 7-49 頁。
- 使用者可以延後、停止或略過預約掃瞄。如需詳細資訊，請參閱預約掃瞄權限和其他設定 第 7-51 頁。
- 使用者可啟動 POP3 電子郵件訊息的病毒/惡意程式掃瞄。如需詳細資訊，請參閱郵件掃瞄權限和其他設定 第 7-54 頁。
- Security Agent 可以使用快取設定來提高其掃瞄效能。如需詳細資訊，請參閱用於掃瞄的快取設定 第 7-56 頁。
- 使用者可以自訂個別「信任的程式清單」。如需詳細資訊，請參閱信任的程式清單權限 第 7-59 頁。

掃瞄類型權限

允許使用者設定自己的手動掃瞄、即時掃瞄和預約掃瞄設定。

授與掃瞄類型權限

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。

3. 請點選「設定 > 權限和其他設定」。
4. 在「使用權限」標籤中，移至「掃瞄」區段。
5. 選取允許使用者設定的掃瞄類型。
6. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

設定 Security Agent 的掃瞄設定

步驟

1. 以滑鼠右鍵按一下系統匣上的 Security Agent 圖示，然後選取「開啟 Security Agent 主控台」。
2. 請點選「設定 > {掃瞄類型}」。
3. 設定下列設定：
   - 即時掃瞄設定：使用者對檔案執行的活動、要掃瞄的檔案、掃瞄設定、掃瞄例外、中毒處理行動
   - 手動掃瞄設定：要掃瞄的檔案、掃瞄設定、CPU 使用率、掃瞄例外、中毒處理行動
   - 預約掃瞄設定：預約時程、要掃瞄的檔案、掃瞄設定、CPU 使用率、掃瞄例外、中毒處理行動
4. 請點選「確定」。

預約掃瞄權限和其他設定

如果設定在用戶端上執行「預約掃瞄」，使用者可以延後和略過/停止「預約掃瞄」。

延後預約掃瞄

具有「延後預約掃瞄」權限的使用者可以執行下列動作：

- 在預約掃瞄開始前將其延後，並指定延後時間長度。「預約掃瞄」功能只能延後一次。
- 如果「預約掃瞄」正在進行中，使用者可以停止掃瞄並稍後重新啟動。使用者可以接著指定掃瞄重新開始之前應該經過的時間長度。一旦掃瞄重新啟動，先前掃瞄過的所有檔案都會重新掃瞄一遍。「預約掃瞄」只能停止並重新啟動一次。

注意

使用者可以指定的延後時間長度與經過時間長度下限為 15 分鐘。上限為 12 小時 45 分鐘。

您可以移至「安全設定」標籤上的「用戶端 > 全域用戶端設定」來修改延後時間。在「預約掃瞄設定」區段中，修改「延後預約掃瞄最多 __ 小時又 __ 分鐘」設定。

略過及停止預約掃瞄

此權限允許使用者執行以下動作：

- 在預約掃瞄執行之前予以略過
- 停止進行中的預約掃瞄

注意

使用者不能多次略過或停止「預約掃瞄」。即使在系統重新啟動後，「預約掃瞄」仍會根據下次預約時間繼續掃瞄。

預約掃瞄權限通知

如果要允許使用者使用預約掃瞄權限，請設定 Apex One 在執行「預約掃瞄」之前顯示通知訊息，提醒他們您授與他們的權限。

授與預約掃瞄權限並顯示權限通知

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 權限和其他設定」。
4. 在「權限」標籤中，移至「預約掃瞄」區段。
5. 選取下列選項：
   - 延後預約掃瞄
   - 略過及停止預約掃瞄
6. 請點選「其他設定」，並移至「預約掃瞄設定」區段。
7. 選取「執行預約掃瞄之前顯示通知」。

   啟動此選項時，開始執行「預約掃瞄」前數分鐘會在用戶端端點上顯示通知訊息。這時使用者會收到有關掃瞄預約時程（日期與時間）及其「預約掃瞄」權限（例如：延後、略過，或是停止預約掃瞄）的通知。

注意

您可以設定分鐘數。如果要設定分鐘數，請移至「安全設定」標籤上的「用戶端 > 全域用戶端設定」。在「預約掃瞄設定」區段中，修改「在預約掃瞄開始前 __ 分鐘提醒使用者」的設定。

8. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

在用戶端上延後/略過及停止預約掃瞄

步驟

- 如果預約掃瞄尚未開始：

  a. 以滑鼠右鍵請點選系統匣上的 Security Agent 圖示，並選取「進階預約掃瞄設定」。

  注意

  如果通知訊息已啟動並設定為在開始執行「預約掃瞄」前數分鐘顯示，則使用者不需要執行此步驟。如需有關通知訊息的詳細資訊，請參閱預約掃瞄權限通知 第 7-52 頁。

  b. 在顯示的通知視窗上，選取下列其中一個選項：

     - 延後掃瞄 __ 小時 __ 分鐘。
     - 略過此預約掃瞄。下一次預約掃瞄將在 <日期> 的 <時間> 執行。

- 如果預約掃瞄正在進行：

a. 以滑鼠右鍵請點選系統匣上的 Security Agent 圖示，並選取「預約掃瞄進階設定」。

b. 在顯示的通知視窗上，選取下列其中一個選項：

- 停止掃瞄。在此時間後重新啟動掃瞄：__ 小時 __ 分鐘。
- 停止掃瞄。下一次預約掃瞄將在 <日期> 的 <時間> 執行。

郵件掃瞄權限和其他設定

當 Security Agent 具有郵件掃瞄權限時，Security Agent 主控台會顯示「郵件掃瞄」選項。「郵件掃瞄」選項會顯示 POP3 郵件掃瞄。

下表說明 POP3 郵件掃瞄程式。

表 7-18. 郵件掃瞄程式

詳細資訊	說明
用途	掃瞄 POP3 電子郵件訊息中是否有病毒/惡意程式
先決條件	• 必須先由管理員從 Web 主控台將其啟動，然後使用者才能使用該程式 注意 如果要啟動 POP3 郵件掃瞄，請參閱授與郵件掃瞄權限和啟動 POP3 郵件掃瞄 第 7-55 頁。 • 您可以從 Security Agent 主控台設定針對病毒/惡意程式的處理行動，但無法從 Web 主控台進行設定
支援的掃瞄類型	即時掃瞄 從 POP3 郵件伺服器擷取電子郵件時，便會執行掃瞄。

詳細資訊	說明
掃瞄結果	• 有關掃瞄完成後偵測到的安全威脅的資訊 • 未在 Security Agent 主控台的「記錄檔」畫面中記錄的掃瞄結果 • 未傳送到伺服器的掃瞄結果
其他詳細資訊	共用網頁信譽評等功能

授與郵件掃瞄權限和啟動 POP3 郵件掃瞄

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 權限和其他設定」。
4. 在「權限」標籤中，移至「郵件掃瞄」區段。
5. 選取「在 Security Agent 主控台上顯示「郵件掃瞄」設定」。
6. 請點選「其他設定」，並移至「POP3 電子郵件掃瞄設定」區段。
7. 選取「掃瞄 POP3 電子郵件」。
8. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

用於掃瞄的快取設定

Security Agent 可以建置數位簽章和依要求掃瞄快取檔案以提高其掃瞄效能。執行依要求掃瞄時，Security Agent 會依次檢查數位簽章快取檔案和依要求掃瞄快取檔案，以選擇要從掃瞄中排除的檔案。如果不掃瞄大量檔案，將會縮短掃瞄時間。

數位簽章快取

「手動掃瞄」、「預約掃瞄」與「立即掃瞄」期間均會使用數位簽章快取檔案。用戶端不會掃瞄簽章已新增到數位簽章快取檔案的檔案。

Security Agent 使用行為監控所用的數位簽章特徵碼，來建置數位簽章快取檔案。數位簽章特徵碼包含趨勢科技認為可信，因而可以不掃瞄的檔案清單。

注意

「行為監控」會在 Windows Server 平台上自動關閉。如果啟動數位簽章快取，這些平台上的 Security Agent 會下載要在快取中使用的數位簽章特徵碼，而不會下載其他行為監控元件。

用戶端會根據預約時程建置數位簽章快取檔案，該時程可從 Web 主控台進行設定。用戶端執行此操作的目的如下：

- 為建立上一快取檔案後加入系統的新檔案新增簽章
- 移除系統中已修改或已刪除檔案的簽章

在快取建置過程中，用戶端會檢查以下資料夾中的可信檔案，然後將這些檔案的簽章新增到數位簽章快取檔案：

- `%PROGRAMFILES%`
- `%WINDIR%`

快取建置程序不會影響端點的效能，因為用戶端在此程序中使用的系統資源非常少。用戶端還可以繼續進行由於某種原因（例如，主機電源關閉或無線端點的 AC 電源轉接器未插電時）而中斷的快取建置工作。

依要求掃瞄快取

在「手動掃瞄」、「預約掃瞄」和「立即掃瞄」期間使用依要求掃瞄快取檔案。Security Agent 不會掃瞄其快取已新增到依要求掃瞄快取檔案的檔案。

每次執行掃瞄時，Security Agent 都會檢查不存在安全威脅的檔案的內容。如果某個不存在安全威脅的檔案在一段時間（可設定該時間範圍）內未經修改，則 Security Agent 會將該檔案的快取新增到依要求掃瞄快取檔案。如果在下一次掃瞄時檔案的快取未到期，則不會掃瞄該檔案。

不存在威脅的檔案的快取會在一定天數（亦可設定該時段）內到期。如果在快取到期時或到期之後進行掃瞄，Security Agent 會移除已到期的快取並掃瞄檔案是否包含威脅。如果檔案不存在威脅且保持不變，則會將該檔案的快取新增回依需求掃瞄快取檔案。如果檔案不存在威脅但最近進行了修改，則不會新增相應的快取，並將在下次掃瞄時重新掃瞄該檔案。

不存在威脅的檔案的快取到期可防止從掃瞄中排除中毒檔案，如以下範例所示：

- 嚴重過期特徵碼檔案可能已將受感染、未修改的檔案視為不存在威脅。如果快取未到期，則中毒檔案會保存在系統中，直到該檔案修改並透過即時掃瞄偵測到。
- 如果修改了快取的檔案，且即時掃瞄在修改檔案期間不可用，則只有快取到期後，才能對修改的檔案掃瞄威脅。

新增到依需求掃瞄快取檔案的快取數取決於掃瞄類型及其掃瞄目標。例如，如果在「手動掃瞄」期間 Security Agent 只掃瞄了端點中 1,000 個檔案中的 200 個，則快取數可能會較少。

如果頻繁執行依需求掃瞄，則依需求掃瞄快取檔案的掃瞄時間會大大降低。在全部快取均未到期的掃瞄工作中，通常需要 12 分鐘的掃瞄可以降到 1 分鐘。降低檔案必須保持不變的天數和延長快取有效期限通常可以提高效能。由於檔案必須在相對較短的時間內保持不變，因此可以將更多的快取新增到快取檔案。快取還可能會保持較長的有效期，這意味著有更多的檔案跳過掃瞄。

如果很少執行依需求掃瞄，則可以關閉依需求掃瞄快取，因為快取會在下一次執行掃瞄時到期。

設定用於掃瞄的快取設定

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 權限和其他設定」。
4. 請點選「其他設定」，並移至「用於掃瞄的快取設定」區段。
5. 設定數位簽章快取的設定。
   a. 選取「啟動數位簽章快取」。
   b. 在「每隔 __ 天建置快取」中指定用戶端建置快取的頻率。
6. 設定依需求掃瞄快取的設定。
   a. 選取「啟動依要求掃瞄快取」。
   b. 在「針對內容不變達下列天數的安全檔案新增快取：__ 天」中指定檔案在快取之前必須保持不變的天數。
   c. 在「每個安全檔案的快取在下列天數內到期：__ 天」中指定快取保留在快取檔案中的最大天數。

   
   注意
   為了防止掃瞄期間新增的全部快取在同一天到期，快取將在您指定的最大天數內隨機到期。例如，如果今天將 500 個快取新增到快取，且指定的最大天數為 10，則其中一小部分快取會在次日到期，而大部分快取將在隨後幾天到期。在第 10 天，剩餘的全部快取都將到期。
7. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。

- 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

信任的程式清單權限

您可以授與終端使用者權限，以將 Apex One 設定為在執行 Application Control、行為監控、資料外洩防護、周邊設備存取控管、Endpoint Sensor 和即時掃瞄時略過掃瞄信任的程序。將程式新增到「信任的程式清單」後，Apex One 不再對由該程式開始的程式或任何處理程序執行「即時掃瞄」。將信任的程式新增到「信任的程式清單」，以提升端點上的掃瞄效能。

授與「信任的程式清單」設定

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 權限和其他設定」。
4. 在「權限」標籤上，移至「信任的程式清單」區段。
5. 選取「在 Security Agent 主控台上顯示信任的程式清單」。
6. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

全域掃瞄設定

可透過多種方式將全域掃瞄設定套用至用戶端。

- 特定的掃瞄設定可套用至伺服器管理的所有用戶端，或者只套用至具有特定掃瞄權限的用戶端。例如，如果您設定了延後「預約掃瞄」期間，則只有具備延後「預約掃瞄」權限的用戶端才能使用此設定。
- 特定掃瞄設定可套用至所有掃瞄類型，或者只套用至特定的掃瞄類型。例如，在已安裝 Apex One 伺服器與 Security Agent 的端點上，您可以將 Apex One 伺服器資料庫排除在掃瞄作業之外。但是，此設定僅適用於「即時掃瞄」期間。
- 可在掃瞄病毒/惡意程式和（或）間諜程式/可能的資安威脅程式時套用特定掃瞄設定。例如，評估模式僅適用於間諜程式/可能的資安威脅程式掃瞄期間。

設定全域掃瞄設定

步驟

1. 移至「用戶端 > 全域用戶端設定」。
2. 請點選「安全設定」標籤，然後在每個可用區段設定「全域掃瞄設定」。
   - 掃瞄設定區段 第 7-61 頁
   - 預約掃瞄設定區段 第 7-66 頁
3. 請點選「系統」標籤。
4. 在「認證安全防護軟體服務設定」區段，設定「啟動「認證安全防護軟體服務」以進行行為監控、防火牆和防毒掃瞄」設定。

   認證安全防護軟體服務會查詢趨勢科技資料中心，確認惡意程式行為封鎖、事件監控、防火牆或防毒掃瞄所偵測到的程式是否安全。啟動「認證安全防護軟體服務」可降低誤判的可能性。

注意

啟動認證安全防護軟體服務之前，請確定 Security Agent 具有正確的 Proxy 設定（詳細資訊請參閱 Security Agent Proxy 設定 第 15-42 頁）。Proxy 設定不正確以及網際網路連線不穩定，都可能造成趨勢科技資料中心回應接收延遲或失敗，以致監控程式顯示無回應。

此外，純 IPv6 Security Agent 無法直接從趨勢科技資料中心進行查詢。如果要使 Security Agent 連線到趨勢科技資料中心，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。

5. 請點選「網路」標籤。
6. 在「病毒/惡意程式記錄檔頻寬設定」區段，設定「啟動 Security Agent，針對一小時內偵測到的相同病毒/惡意程式建立單一病毒/惡意程式記錄項目」設定。

   Apex One 在偵測到相同病毒/惡意程式在短時間內造成的多個感染時，會整合病毒記錄項目。Apex One 會多次偵測單一病毒/惡意程式，迅速填入病毒/惡意程式記錄檔，並且在 Security Agent 傳送記錄檔資訊至伺服器時消耗網路頻寬。啟動此功能可同時減少產生的病毒/惡意程式記錄項目數，以及 Security Agent 向伺服器報告病毒記錄資訊時消耗的網路頻寬數量。
7. 請點選「用戶端控制」標籤。
8. 在「一般設定」區段，設定「將「手動掃瞄」新增到端點的 Windows 捷徑功能表」設定。

   啟動此設定時，由伺服器管理的所有 Security Agent 都會將「使用 Apex One 掃瞄」選項新增到 Windows 檔案總管的右鍵功能表。當使用者以滑鼠右鍵請點選 Windows 桌面或「Windows 檔案總管」中的檔案或資料夾並選取此選項時，Apex One 便會使用「手動掃瞄」來掃瞄檔案或資料夾是否包含病毒/惡意程式和間諜程式/可能的資安威脅程式。
9. 請點選「儲存」。

掃瞄設定區段

「全域用戶端設定」畫面「安全設定」標籤上的「掃瞄設定」區段可讓管理員設定下列項目：

不對 Apex One 伺服器資料庫的資料夾進行即時掃瞄

如果 Security Agent 和 Apex One 伺服器位於同一個端點上，則 Security Agent 在「即時掃瞄」期間將不會掃瞄伺服器資料庫是否包含病毒/惡意程式和間諜程式/可能的資安威脅程式。

秘訣

啟動此設定可防止掃瞄期間可能造成的資料庫損毀。

不掃瞄 Microsoft Exchange Server 的資料夾和檔案

如果 Security Agent 和 Microsoft Exchange 2000/2003 伺服器位於同一個端點，Apex One 在「手動掃瞄」、「即時掃瞄」、「預約掃瞄」和「立即掃瞄」期間將不會掃瞄下列 Microsoft Exchange 資料夾和檔案是否包含病毒/惡意程式和間諜程式/可能的資安威脅程式：

- 位於 `\Exchsrvr\Mailroot\vsi 1` 中的下列資料夾：`Queue`、`PickUp` 和 `BadMail`
- `.\Exchsrvr\mdbdata`，包括以下檔案：`priv1.stm`、`priv1.edb`、`pub1.stm` 和 `pub1.edb`
- `.\Exchsrvr\Storage` 群組

如果為 Microsoft Exchange 2007 或更新版本資料夾，您必須手動將資料夾新增至掃瞄例外清單中。如需有關掃瞄例外的詳細資訊，請參閱下列網站：

http://technet.microsoft.com/en-us/library/bb332342.aspx

如需設定掃瞄例外清單的步驟，請參閱掃瞄例外 第 7-27 頁。

啟動延遲掃瞄檔案作業

管理員可以設定 Apex One，使其延遲掃瞄檔案。Apex One 允許使用者複製檔案，然後在複製程序完成後再掃瞄檔案。這種延遲掃瞄的功能可改善複製和掃瞄程序的效能。

注意

延遲掃瞄要求病毒掃瞄引擎 (VSAPI) 必須是 9.713 版或更新版本。如需升級伺服器的詳細資訊，請參閱手動更新 Apex One 伺服器 第 6-23 頁。

在端點上啟動開機預先載入的惡意程式防護

Apex One 支援開機預先載入的惡意程式防護 (ELAM) 功能作為安全開機標準的一部分，以在端點上提供開機期間的防護。管理員可以啟動此功能，在端點啟動時先啟動 Apex One 用戶端，再啟動其他協力廠商軟體驅動程式。這項功能可讓 Apex One 用戶端在作業系統開機程序期間偵測惡意程式。

在掃瞄所有協力廠商軟體驅動程式之後，Apex One 用戶端會將驅動程式分類資訊回報給系統核心。管理員可以根據 Windows 群組原則中的驅動程式分類定義處理行動，並在端點上使用事件檢視器檢視掃瞄結果。

注意

僅 Windows 8.1（或更新版本）和 Windows Server 2012（或更新版本）平台支援 ELAM。

設定大型壓縮檔的掃瞄設定

由伺服器管理的所有 Security Agent 在「手動掃瞄」、「即時掃瞄」、「預約掃瞄」和「立即掃瞄」期間掃瞄壓縮檔是否有病毒/惡意程式和間諜程式/可能的資安威脅程式時，會先檢查下列設定：

- 設定大型壓縮檔的掃瞄設定：選取此選項以啟動壓縮檔處理。
- 分別對「即時掃瞄」和其他掃瞄類型（「手動掃瞄」、「預約掃瞄」和「立即掃瞄」）進行下列設定：
  - 不掃瞄壓縮檔內檔案大小超過 __ MB 的檔案：Apex One 不會掃瞄任何超過該大小上限的檔案。
  - 在壓縮檔中，僅掃瞄前 __ 個檔案：Apex One 將壓縮檔解壓縮之後，會掃瞄指定數目的檔案，並忽略任何剩餘的檔案。

清除/刪除壓縮檔內中毒檔案

當伺服器管理的所有用戶端在「手動掃瞄」、「即時掃瞄」、「預約掃瞄」和「立即掃瞄」期間於壓縮檔中偵測到病毒/惡意程式，而且符合下列條件時，用戶端會清除或刪除中毒檔案。

- 「清除」或「刪除」是 Apex One 設定要執行的中毒處理行動。移至「用戶端 > 用戶端管理> 設定 > 掃瞄設定 > {掃瞄類型} > 處理行動」標籤，以檢查 Apex One 對中毒檔案執行的處理行動。
- 啟動此設定。啟動此設定可能會增加掃瞄過程中使用的端點資源，而且掃瞄作業會花更長的時間才能完成。這是因為 Apex One 需要將壓縮檔解壓縮、清除/刪除壓縮檔內的中毒檔案，然後重新壓縮檔案。
- 支援壓縮檔格式。Apex One 只支援特定的壓縮檔格式，包括 ZIP 和使用 ZIP 壓縮技術的 Office Open XML。Office Open XML 是 Excel、PowerPoint 和 Word 等 Microsoft Office 2007 應用程式的預設格式。

> **注意**
>
> 如需支援之壓縮檔格式的完整清單，請聯絡您的經銷商。

例如，「即時掃瞄」已設定為刪除感染病毒的檔案。「即時掃瞄」將名為 `abc.zip` 的壓縮檔解壓縮並偵測到壓縮檔內有中毒檔案 `123.doc` 後，Apex One 會刪除 `123.doc` 並重新壓縮 `abc.zip`，讓您可以安全地存取此檔案。

下表說明如果未符合任一條件，會有什麼情形。

表 7-19. 壓縮檔情形和結果

「清除/刪除壓縮檔內中毒檔案」的狀態	設定 APEX ONE 執行的處理行動	壓縮檔格式	結果
已啟動	清除或刪除	不支援 例如：def.rar 包含一個中毒檔案 123.doc。	Apex One 會加密 def.rar，但是並不會對 123.doc 進行清除、刪除或執行其他任何中毒處理行動。
已關閉	清除或刪除	支援/不支援 例如：abc.zip 包含一個中毒檔案 123.doc。	Apex One 並不會對 abc.zip 和 123.doc 進行清除、刪除或執行其他任何中毒處理行動。
啟動/關閉	不清除或刪除（換言之，採取下列任一種處理行動：重新命名、隔離、拒絕存取或暫不處理）	支援/不支援 例如：abc.zip 包含一個中毒檔案 123.doc。	Apex One 會對 abc.zip（而非 123.doc）執行設定的中毒處理行動（重新命名、隔離、拒絕存取或暫不處理）。 如果中毒處理行動為： 重新命名：Apex One 會將 abc.zip 重新命名為 abc.vir，但是不會重新命名 123.doc。 隔離：Apex One 會隔離 abc.zip（會隔離 123.doc 和所有未中毒的檔案）。 暫不處理：Apex One 不會對 abc.zip 和 123.doc 執行任何處理行動，但是會記錄偵測到病毒。 拒絕存取：Apex One 會在 abc.zip 開啟時拒絕存取此檔案（無法開啟 123.doc 和所有未中毒的檔案）。

啟動評估模式

在評估模式下，所有由伺服器管理的用戶端都會在「手動掃瞄」、「預約掃瞄」、「即時掃瞄」與「立即掃瞄」期間記錄偵測到的間諜程式/可能的資安威

脅程式，但是不會清除這些間諜程式/可能的資安威脅程式元件。清除會終止程序，或刪除登錄、檔案、Cookie 和捷徑。

趨勢科技提供評估模式，可讓您評估趨勢科技偵測為間諜程式/可能的資安威脅程式的項目，再根據評估採取適當的中毒處理行動。例如，可以將偵測到但不認為是安全威脅的間諜程式/可能的資安威脅程式新增至間諜程式/可能的資安威脅程式核可清單。

使用評估模式時，Apex One 會執行下列中毒處理行動：

- 暫不處理：在手動掃瞄、預約掃瞄和立即掃瞄期間
- 拒絕存取：在即時掃瞄期間

注意

評估模式會覆寫任何使用者設定的中毒處理行動。例如，即使您選擇「清除」做為「手動掃瞄」期間的中毒處理行動，「暫不處理」仍會是用戶端在評估模式時採取的中毒處理行動。

掃瞄 Cookie

如果您認為 Cookie 是可能的安全威脅，請選取此選項。選取此選項後，伺服器管理的所有用戶端在「手動掃瞄」、「預約掃瞄」、「即時掃瞄」和「立即掃瞄」期間會掃瞄 Cookie 中是否包含間諜程式/可能的資安威脅程式。

預約掃瞄設定區段

只有設定為執行「預約掃瞄」的用戶端會使用下列設定。「預約掃瞄」可以掃瞄病毒/惡意程式和間諜程式/可能的資安威脅程式。

全域掃描設定的預約掃瞄設定區段可讓管理員設定下列項目：

- 執行預約掃瞄之前 __ 分鐘提醒使用者 第 7-67 頁
- 延後預約掃瞄最多 __ 小時 __ 分鐘 第 7-67 頁
- 當掃瞄時間超過 __ 小時又 __ 分鐘時，自動停止預約掃瞄 第 7-67 頁

- 無線端點的電池電力剩餘時間若少於 __ %，而且已拔掉 AC 電源轉接器，則略過「預約掃瞄」 第 7-67 頁
- 繼續未執行的預約掃瞄 第 7-68 頁

執行預約掃瞄之前 __ 分鐘提醒使用者

Apex One 可以在掃瞄開始前數分鐘顯示通知訊息，藉此提醒使用者掃瞄預約時程（日期與時間）以及您授與使用者的任何「預約掃瞄」權限。

您可以從「用戶端 > 用戶端管理 > 設定 > 權限和其他設定 > 其他設定 (標籤) > 預約掃瞄設定」啟動/關閉通知訊息。如果關閉通知訊息，將不會顯示提醒。

延後預約掃瞄最多 __ 小時 __ 分鐘

只有具有「延後預約掃瞄」權限的使用者可以執行下列動作：

- 在預約掃瞄開始前將其延後，並指定延後時間長度。
- 如果「預約掃瞄」正在進行中，使用者可以停止掃瞄並稍後重新啟動。使用者可以接著指定掃瞄重新開始之前應該經過的時間長度。一旦掃瞄重新啟動，先前掃瞄過的所有檔案都會重新掃瞄一遍。

  使用者可以指定的延後時間長度/經過的時間長度上限為 12 小時又 45 分鐘，而您可以在提供的時數和（或）分鐘數欄位中進行指定以縮短上限。

當掃瞄時間超過 __ 小時又 __ 分鐘時，自動停止預約掃瞄

Apex One 會在超過指定的時間而掃瞄尚未完成時停止掃瞄。Apex One 會立即通知使用者在掃瞄期間偵測到的任何安全威脅。

無線端點的電池電力剩餘時間若少於 __ %，而且已拔掉 AC 電源轉接器，則略過「預約掃瞄」

如果 Apex One 偵測到無線端點的電池電力不足，並且其 AC 電源轉接器並未連接至任何電源時，則會在「預約掃瞄」啟動時立即略過掃瞄。如果電池電力不足，但是 AC 電源轉接器已經連接至電源，則會繼續掃瞄。

繼續未執行的預約掃瞄

當「預約掃瞄」因為 Apex One 在「預約掃瞄」的日期和時間未在執行或者使用者中斷預約掃瞄（例如，在掃瞄開始後關閉端點）而未能啟動時，您可以指定 Apex One 將在何時繼續掃瞄。

指定重新啟動哪個「預約掃瞄」：

- 繼續中斷的預約掃瞄：繼續使用者透過關閉端點中斷的預約掃瞄
- 繼續未執行的預約掃瞄：繼續由於端點未執行而錯過的預約掃瞄

指定將在何時繼續掃瞄：

- 隔天同一時間：如果 Apex One 在隔天同一時間執行，則會繼續掃瞄。
- 端點啟動後 __ 分鐘：Apex One 會在使用者開啟端點指定的分鐘數後繼續掃瞄。分鐘數介於 10 到 120 之間。

注意

如果系統管理員啟動適當的權限，使用者可以延後或略過錯過的「預約掃瞄」。如需詳細資訊，請參閱預約掃瞄權限和其他設定 第 7-51 頁。

安全威脅通知

Apex One 隨附一組預設通知訊息，用於通知您、其他 Apex One 管理員和 Security Agent 使用者偵測到的安全威脅。

如需有關傳送給管理員的通知的詳細資訊，請參閱管理員的安全威脅通知 第 7-69 頁。

如需有關傳送給 Security Agent 使用者的通知的詳細資訊，請參閱給 Security Agent 使用者的安全威脅通知 第 7-75 頁。

管理員的安全威脅通知

將 Apex One 設為在下列時機，將通知傳送給您及其他的 Apex One 管理員：當其偵測到安全威脅，或是只有在安全威脅處理行動失敗，因而需要您介入時。

Apex One 隨附一組預設通知訊息，用於通知您和其他 Apex One 管理員偵測到的安全威脅。您可以視需要修改通知和設定其他通知設定。

表 7-20. 安全威脅通知的類型

類型	關係
病毒/惡意程式	設定管理員的安全威脅通知 第 7-69 頁
間諜程式/可能的資安威脅程式	設定管理員的安全威脅通知 第 7-69 頁
數位資產傳輸	設定給管理員的資料外洩防護通知 第 11-49 頁
C&C 回呼	設定給管理員的 C&C 回呼通知 第 12-12 頁

注意

Apex One 可以透過電子郵件、SNMP Trap 和 Windows NT 事件記錄檔來傳送通知。設定 Apex One 何時透過這些通道傳送通知的設定。如需詳細資訊，請參閱 管理員通知設定 第 14-35 頁。

設定管理員的安全威脅通知

步驟

1. 移至「管理 > 通知 > 管理員」。

   會出現「管理員通知」畫面。

2. 在「條件」標籤中：

   a. 移至「病毒/惡意程式」和「間諜程式/可能的資安威脅程式」區段。

b. 指定是否在 Apex One 偵測到病毒/惡意程式和間諜程式/可能的資安威脅程式時傳送通知，或是只在對這些安全威脅採取的處理行動失敗時傳送通知。

3. 在「電子郵件」標籤中：

a. 移至「病毒/惡意程式偵測」和「間諜程式/可能的資安威脅程式偵測」區段。

b. 選取「啟動電子郵件通知」。

c. 選取「傳送通知給具有用戶端樹狀結構網域權限的使用者」。

您可以使用以角色為基礎的管理將用戶端樹狀結構網域權限授與使用者。如果在屬於特定網域的任一 Security Agent 上進行偵測，電子郵件將傳送給具網域權限之使用者的電子郵件信箱。如需範例，請參閱下表：

表 7-21. 用戶端樹狀結構網域和權限

用戶端樹狀結構網域	具有網域權限的角色	具有該角色的使用者帳號	使用者帳號的電子郵件信箱
網域 A	Administrator（內建）	root	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
網域 B	Administrator（內建）	root	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

如果屬於網域 A 的任一 Security Agent 偵測到病毒，系統會將電子郵件傳送至 mary@xyz.com、john@xyz.com 和 chris@xyz.com。

如果屬於網域 B 的任一 Security Agent 偵測到間諜程式，系統會將電子郵件傳送至 mary@xyz.com 和 jane@xyz.com。

注意

若您啟動此選項，具網域權限的所有使用者都必須有一個對應的電子郵件信箱。電子郵件通知不會傳送給沒有電子郵件信箱的使用者。使用者和電子郵件信箱是從「管理 > 帳號管理 > 使用者帳號」設定的。

d. 選取「傳送通知到下列電子郵件信箱」，然後輸入電子郵件信箱。

e. 指定要在電子郵件通知中使用的「主旨」。

f. 指定「訊息」內容。

Apex One 支援在「主旨」和「訊息」欄位中使用 Token。

表 7-22. 安全威脅通知的 Token 變數

變數 TOKEN	說明
病毒/惡意程式偵測	
%v	安全威脅名稱
%s	偵測所在端點
%i	端點 IP 位址
%c	端點 MAC 位址
%m	端點網域
%p	病毒/惡意程式的位置
%y	偵測的日期和時間
%e	病毒掃瞄引擎版本
%r	病毒碼版本
%a	針對安全威脅執行的處理行動
%n	登入端點的使用者名稱
%g	Security Agent 的 GUID
%b	掃瞄類型

變數 TOKEN	說明
間諜程式/可能的資安威脅程式偵測	
%s	偵測所在端點
%i	端點 IP 位址
%m	端點網域
%y	偵測的日期和時間
%n	登入端點的使用者名稱
%T	間諜程式/可能的資安威脅程式和掃瞄結果
%d	有關間諜程式/可能的資安威脅程式偵測的詳細資訊
%g	Security Agent 的 GUID
%b	掃瞄類型

4. 在「SNMP Trap」標籤中：

   a. 移至「病毒/惡意程式偵測」和「間諜程式/可能的資安威脅程式偵測」區段。

   b. 選取「啟動 SNMP Trap 通知」。

   c. 接受或修改預設的訊息。您可以使用下表中的 Token 變數代表「訊息」欄位中的資料。

   表 7-23. 安全威脅通知的 Token 變數

變數	說明
病毒/惡意程式偵測	
%v	安全威脅名稱
%s	偵測所在端點
%i	端點 IP 位址
%c	端點 MAC 位址

變數	說明
%m	端點網域
%p	病毒/惡意程式的位置
%y	偵測的日期和時間
%e	病毒掃瞄引擎版本
%r	病毒碼版本
%a	針對安全威脅執行的處理行動
%n	登入端點的使用者名稱
%g	Security Agent 的 GUID
%b	掃瞄類型
間諜程式/可能的資安威脅程式偵測	
%s	偵測所在端點
%i	端點 IP 位址
%m	端點網域
%y	偵測的日期和時間
%n	登入端點的使用者名稱
%T	間諜程式/可能的資安威脅程式和掃瞄結果
%v	安全威脅名稱
%a	針對安全威脅執行的處理行動
%d	有關間諜程式/可能的資安威脅程式偵測的詳細資訊
%g	Security Agent 的 GUID

5. 在「NT 事件記錄檔」標籤中：

   a. 移至「病毒/惡意程式偵測」和「間諜程式/可能的資安威脅程式偵測」區段。

b. 選取「啟動 NT 事件記錄檔通知」。

c. 接受或修改預設的訊息。您可以使用下表中的 Token 變數代表「訊息」欄位中的資料。

表 7-24. 安全威脅通知的 Token 變數

變數	說明
病毒/惡意程式偵測	
%v	安全威脅名稱
%s	偵測所在端點
%i	端點 IP 位址
%c	端點 MAC 位址
%m	端點網域
%p	病毒/惡意程式的位置
%y	偵測的日期和時間
%e	病毒掃瞄引擎版本
%r	病毒碼版本
%a	針對安全威脅執行的處理行動
%n	登入端點的使用者名稱
%g	Security Agent 的 GUID
%b	掃瞄類型
間諜程式/可能的資安威脅程式偵測	
%s	偵測所在端點
%i	端點 IP 位址
%m	端點網域
%y	偵測的日期和時間

變數	說明
%n	登入端點的使用者名稱
%T	間諜程式/可能的資安威脅程式和掃瞄結果
%v	安全威脅名稱
%a	針對安全威脅執行的處理行動
%d	有關間諜程式/可能的資安威脅程式偵測的詳細資訊
%g	Security Agent 的 GUID

6. 請點選「儲存」。

給 Security Agent 使用者的安全威脅通知

Apex One 可以在以下情況下在 Security Agent 端點上顯示通知訊息：

- 「即時掃瞄」和「預約掃瞄」偵測病毒/惡意程式和間諜程式/可能的資安威脅程式。啟動通知訊息，並視需要修改其內容。
- 必須重新啟動端點才能完成清除中毒檔案。對於「即時掃瞄」，會在掃瞄到特定安全威脅之後顯示訊息。對於「手動掃瞄」、「預約掃瞄」和「立即掃瞄」，只會在 Apex One 完成掃瞄所有掃瞄目標的程序之後顯示一次訊息。

表 7-25. 安全威脅用戶端通知的類型

類型	關係
病毒/惡意程式	設定 Security Agent 的病毒/惡意程式通知 第 7-77 頁
間諜程式/可能的資安威脅程式	設定間諜程式/可能的資安威脅程式通知 第 7-77 頁
防火牆違規	修改防火牆通知訊息的內容 第 13-25 頁
網頁信譽評等違規	修改網路安全威脅通知 第 12-11 頁

類型	關係
周邊設備存取控管違規	修改周邊設備存取控管通知 第 10-16 頁
行為監控策略違規	修改通知訊息內容 第 9-18 頁
數位資產傳輸	設定給用戶端的資料外洩防護通知 第 11-52 頁
C&C 回呼	修改網路安全威脅通知 第 12-11 頁

通知使用者有關病毒/惡意程式和間諜程式/可能的資安威脅程式偵測資訊

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 掃瞄設定 > 即時掃瞄設定」或「設定 > 掃瞄設定 > 預約掃瞄設定」。
4. 請點選「處理行動」標籤。
5. 選取下列選項：
   - 偵測到病毒/惡意程式時在用戶端端點上顯示通知訊息
   - 偵測到可能的病毒/惡意程式時在用戶端端點上顯示通知訊息
6. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。

- 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

設定 Security Agent 的病毒/惡意程式通知

您可以將 Security Agent 設定為將嘗試清除或隔離病毒/惡意程式安全威脅的結果通知使用者。

步驟

1. 移至「管理 > 通知 > 用戶端」。
2. 從「類型」下拉式清單中，選取「病毒/惡意程式」。
3. 設定偵測設定。
   a. 選擇顯示所有病毒/惡意程式相關事件的通知，或依據下列嚴重性層級顯示個別通知：
      - 高：Security Agent 無法處理重大惡意程式
      - 中：Security Agent 無法處理惡意程式
      - 低：Security Agent 無法解決所有安全威脅
   b. 接受或修改預設的訊息。
4. 請點選「儲存」。

設定間諜程式/可能的資安威脅程式通知

步驟

1. 移至「管理 > 通知 > 用戶端」。
2. 從「類型」下拉式清單中，選取「間諜程式/可能的資安威脅程式」。

3. 接受或修改預設的訊息。
4. 請點選「儲存」。

通知用戶端重新啟動以完成清除中毒檔案

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 權限和其他設定」。
4. 請點選「其他設定」標籤，然後移至「重新啟動通知」區段。
5. 選取「當端點需要重新啟動以完成清除中毒檔案時顯示通知」。
6. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

安全威脅記錄檔

Apex One 在偵測到病毒/惡意程式或間諜程式/可能的資安威脅程式時，以及在恢復間諜程式/可能的資安威脅程式時，都會產生記錄檔。

如果要避免記錄檔佔去過多硬碟空間，請手動刪除記錄檔或設定記錄檔刪除預約時程。如需有關管理記錄檔的詳細資訊，請參閱記錄檔管理 第 14-39 頁。

檢視病毒/惡意程式記錄檔

Security Agent 在偵測到病毒和惡意程式時會產生記錄檔，並將記錄檔傳送到伺服器。

步驟

1. 移至下列其中一個項目：
   - 記錄檔 > 用戶端 > 安全威脅
   - 用戶端 > 用戶端管理
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請移至「病毒/惡意程式記錄檔條件」畫面：
   - 在「安全威脅記錄檔」畫面中，點選「檢視記錄檔 > 病毒/惡意程式記錄檔」。
   - 在「用戶端管理」畫面中，點選「記錄檔 > 病毒/惡意程式記錄檔」。
4. 指定記錄條件，然後請點選「顯示記錄檔」。
5. 檢視記錄檔。記錄檔包含下列資訊：

項目	說明
日期/時間	發生偵測的時間
端點	發生偵測的端點
安全威脅	安全威脅的名稱
感染通道	安全威脅源自的通道

項目	說明
中毒檔案/物件	端點上檔案/物件的位置
掃瞄類型	偵測到安全威脅的掃瞄
結果	採取處理行動的結果 注意 如需有關掃瞄結果的詳細資訊，請參閱病毒/惡意程式掃瞄結果 第 7-80 頁。
IP 位址	來源端點的 IP 位址和通訊埠號碼
MAC 位址	中毒端點的 MAC 位址
詳細資訊	顯示特定偵測詳細分析的連結

6. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請點選「全部匯出到 CSV」。開啟檔案或將其儲存至特定位置。

   CSV 檔案包含以下資訊：

   - 記錄檔中的所有資訊
   - 偵測時登入端點的使用者名稱

病毒/惡意程式掃瞄結果

下列掃瞄結果會顯示在病毒/惡意程式記錄檔中：

表 7-26. 掃瞄結果

結果	說明
已刪除	• 第一個中毒處理行動是「刪除」，並已刪除中毒的檔案。 • 第一個中毒處理行動是「清除」，但是清除失敗。第二個中毒處理行動是「刪除」，並已刪除中毒的檔案。
已隔離	• 第一個中毒處理行動是「隔離」，並已隔離中毒的檔案。

結果	說明
	• 第一個中毒處理行動是「清除」，但是清除失敗。第二個中毒處理行動是「隔離」，並已隔離中毒的檔案。
已清除	已清除中毒的檔案。
已重新命名	• 第一個中毒處理行動是「重新命名」，並已重新命名中毒的檔案。 • 第一個中毒處理行動是「清除」，但是清除失敗。第二個中毒處理行動是「重新命名」，並已重新命名中毒的檔案。
拒絕存取	• 第一個中毒處理行動是「拒絕存取」，而在使用者嘗試開啟中毒的檔案時拒絕存取該檔案。 • 第一個中毒處理行動是「清除」，但是清除失敗。第二個中毒處理行動是「拒絕存取」，而在使用者嘗試開啟中毒的檔案時拒絕存取該檔案。 • 在「即時掃瞄」期間偵測到可能的病毒/惡意程式。 • 即使中毒處理行動為「清除」（第一個中毒處理行動）和「隔離」（第二個中毒處理行動），「即時掃瞄」仍可能拒絕存取受到開機型病毒感染的檔案。這是因為嘗試清除開機型病毒，可能會損害中毒端點的「主開機記錄 (MBR)」。執行「手動掃瞄」，讓 Apex One 能夠清除或隔離檔案。
暫不處理	• 第一個中毒處理行動是「暫不處理」。“”Apex One 不會對中毒檔案執行任何中毒處理行動。 • 第一個中毒處理行動是「清除」，但是清除失敗。第二個中毒處理行動是「暫不處理」，所以 Apex One 未對中毒的檔案執行任何中毒處理行動。
暫不處理潛在的安全威脅	只有在 Apex One 於「手動掃瞄」、「預約掃瞄」與「立即掃瞄」期間偵測到「可能的病毒/惡意程式」時，才會顯示此掃瞄結果。如需有關可能的病毒/惡意程式以及如何將可疑檔案送給趨勢科技進行分析的詳細資訊，請參閱趨勢科技線上病毒百科全書的下列頁面。 https://www.trendmicro.com/vinfo/tw/threat-encyclopedia/malware/possible_virus
無法清除或隔離檔案	「清除」是第一個中毒處理行動。「隔離」是第二個中毒處理行動，而兩項行動都失敗。

結果	說明
	解決方案：請參閱「無法隔離檔案/無法重新命名檔案」 第 7-82 頁。
無法清除或刪除檔案	「清除」是第一個中毒處理行動。「刪除」是第二個中毒處理行動，而兩項行動都失敗。 解決方案：請參閱「無法刪除這個檔案」 第 7-82 頁。
無法清除或重新命名檔案	「清除」是第一個中毒處理行動。「重新命名」是第二個中毒處理行動，而兩項行動都失敗。 解決方案：請參閱「無法隔離檔案/無法重新命名檔案」 第 7-82 頁。
無法隔離檔案/無法重新命名檔案	說明 1 中毒檔案可能被其他應用程式鎖定或正在執行，或者可能位於 CD 上。在應用程式釋放檔案或檔案執行後，Apex One 會隔離/重新命名檔案。 解決方案 如果中毒檔案位於 CD 上，建議不要再使用該 CD，因為病毒可能會藉此感染網路上的其他端點。
	說明 2 中毒檔案位於用戶端端點的 Temporary Internet Files 資料夾中。因為端點在您瀏覽時下載檔案，所以 Web 瀏覽器可能鎖定了中毒檔案。當 Web 瀏覽器釋放檔案時，Apex One 會隔離/重新命名檔案。 解決方案：無
無法刪除檔案	說明 1 中毒檔案可能包含在壓縮檔內，而且「安全設定」標籤上「用戶端 > 全域用戶端設定」中的「清除/刪除壓縮檔內中毒檔案」設定已經關閉。 解決方案 啟動「清除/刪除壓縮檔內中毒檔案」選項。啟動此選項時，Apex One 會將壓縮檔解壓縮、清除/刪除壓縮檔中的中毒檔案，然後重新壓縮檔案。

結果	說明
	注意 啟動此設定可能會增加掃瞄過程中使用的端點資源，而且掃瞄作業會花更長的時間才能完成。
	說明 2 中毒檔案可能被其他應用程式鎖定或正在執行，或者可能位於 CD 上。在應用程式釋放檔案或檔案執行後，Apex One 會刪除檔案。 解決方案 如果中毒檔案位於 CD 上，建議不要再使用該 CD，因為病毒可能會藉此感染網路上的其他端點。
	說明 3 中毒檔案位於 Security Agent 端點的 Temporary Internet Files 資料夾中。因為端點在您瀏覽時下載檔案，所以 Web 瀏覽器可能鎖定了中毒檔案。當 Web 瀏覽器釋放檔案時，Apex One 會刪除檔案。 解決方案：無
無法將隔離檔案傳送到指定的隔離資料夾	雖然 Apex One 已成功將檔案隔離在 Security Agent 端點的 `\Suspect` 資料夾中，但卻無法將檔案傳送到指定的隔離目錄。 解決方案 請先判斷偵測出病毒/惡意程式的掃瞄類型（「手動掃瞄」、「即時掃瞄」、「預約掃瞄」或「立即掃瞄」），然後檢查在「用戶端 > 用戶端管理> 設定 > {掃瞄類型} > 處理行動」標籤中指定的隔離目錄。 如果隔離目錄位於 Apex One 伺服器電腦或其他 Apex One 伺服器電腦上： 1. 檢查用戶端是否能連線至伺服器。 2. 如果您使用 URL 做為隔離目錄格式： a. 請確認您在 `http://` 後面指定的端點名稱是否正確。 b. 請檢查中毒檔案的大小。如果中毒檔案超過「管理 > 設定 > 隔離區管理員」中指定的檔案大小上限，請調整設定以容納該檔案。您也可以執行其他處理行動，例如：刪除檔案。

結果	說明
	c. 檢查隔離目錄資料夾的大小，並判斷其是否超過「管理 > 設定 > 隔離區管理員」中指定的資料夾容量。調整資料夾的容量，或手動刪除隔離目錄中的檔案。 3. 如果您使用 UNC 路徑，請確定是否可讓「Everyone」群組共享隔離目錄資料夾，並指定讀取和寫入權限給這個群組。此外，也請檢查隔離目錄資料夾是否存在及 UNC 路徑是否正確。 如果隔離目錄位於網路上的其他端點（此時您只可以使用 UNC 路徑）： 1. 檢查 Security Agent 是否能連線至端點。 2. 請確定是否可讓「Everyone」 群組共享隔離目錄資料夾，並指定讀取和寫入權限給這個群組。 3. 檢查隔離目錄資料夾是否存在。 4. 檢查 UNC 路徑是否正確。 如果隔離目錄位於 Security Agent 端點上的不同目錄中（此時您只能使用絕對路徑），請檢查隔離目錄資料夾是否存在。
無法清除檔案	說明 1 中毒檔案可能包含在壓縮檔內，而且「安全設定」標籤上「用戶端 > 全域用戶端設定」中的「清除/刪除壓縮檔內中毒檔案」設定已經關閉。 解決方案 啟動「清除/刪除壓縮檔內中毒檔案」選項。啟動此選項時，Apex One 會將壓縮檔解壓縮、清除/刪除壓縮檔中的中毒檔案，然後重新壓縮檔案。 注意 啟動此設定可能會增加掃瞄過程中使用的端點資源，而且掃瞄作業會花更長的時間才能完成。
	說明 2 中毒檔案位於 Security Agent 端點的 `Temporary Internet Files` 資料夾中。因為端點在您瀏覽時下載檔案，所以 Web 瀏覽器可能鎖定了中毒檔案。當 Web 瀏覽器釋放檔案時，Apex One 會清除該檔案。

結果	說明
	解決方案：無
	說明 3 檔案無法清除。如需詳細資訊與解決方案，請參閱無法清除病毒的檔案 第 D-15 頁。
警告	Apex One 無法在沒有使用者介入的情況下對中毒檔案完成設定的處理行動。將滑鼠暫留在「警告」欄位可查看下列詳細資料。 • 「警告 - 請聯絡客服部門，以取得如何使用 Apex One 工具箱中的 Anti-Threat Tool Kit「Clean Boot」工具移除此安全威脅的詳細資料」 • 「警告 - 請聯絡客服部門，以取得如何使用 Apex One 工具箱中的 Anti-Threat Tool Kit「救援磁片」工具移除此安全威脅的詳細資料」“” • 「警告 - 請聯絡客服部門，以取得如何使用 Apex One 工具箱中的 Anti-Threat Tool Kit「Rootkit Buster」工具移除此安全威脅的詳細資料」 • 「警告 - Apex One 在中毒用戶端上偵測到安全威脅。請重新啟動端點以完成安全威脅清除程序」 • 「警告 – 需要完整系統掃瞄，才能完成從端點移除偵測到的 Rootkit 安全威脅」

檢視中央隔離區恢復記錄檔

清除惡意程式之後，Security Agent 會備份惡意程式資料。如果您認為資料無害，請通知線上用戶端恢復備份的資料。有關哪些惡意程式備份資料已恢復、受影響的端點與恢復結果的資訊，均可在記錄檔中找到。

步驟

1. 移至「記錄檔 > 用戶端 > 中央隔離區還原」。
2. 檢查「成功」、「未成功」以及「暫停中」欄位，查看 Apex One 是否已成功恢復隔離的資料。

3. 點選每欄中的計數連結，檢視有關每個受影響端點的詳細資訊。

   注意

   對於「未成功」恢復，您可以請點選「全部恢復」，在「中央隔離區還原詳細資料」畫面中嘗試再次恢復檔案。

4. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請點選「匯出到 CSV」。開啟檔案或將其儲存至特定位置。

檢視間諜程式/可能的資安威脅程式記錄檔

Security Agent 會在偵測到間諜程式和可能的資安威脅程式後產生記錄檔，並將記錄檔傳送到伺服器。

步驟

1. 移至下列其中一個項目：
   - 記錄檔 > 用戶端 > 安全威脅
   - 用戶端 > 用戶端管理
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請移至「間諜程式/可能的資安威脅程式記錄檔條件」畫面：
   - 在「安全威脅記錄檔」畫面中，點選「檢視記錄檔 > 間諜程式/可能的資安威脅程式記錄檔」。
   - 在「用戶端管理」畫面中，點選「記錄檔 > 間諜程式/可能的資安威脅程式記錄檔」。
4. 指定記錄條件，然後請點選「顯示記錄檔」。
5. 檢視記錄檔。記錄檔包含下列資訊：

項目	說明
日期/時間	發生偵測的時間
端點	發生偵測的端點
間諜程式/可能的資安威脅程式	安全威脅的名稱
掃瞄類型	偵測到安全威脅的掃瞄
結果	採取處理行動的結果 注意 如需有關掃瞄結果的詳細資訊，請參閱間諜程式/可能的資安威脅程式掃瞄結果 第 7-87 頁。
IP 位址	來源端點的 IP 位址和通訊埠號碼
MAC 位址	中毒端點的 MAC 位址
詳細資訊	顯示特定偵測詳細分析的連結

6. （選用）選取您認為無害的任何間諜程式/可能的資安威脅程式偵測事件，然後點選「新增到核可的清單」，即可將程式從後續掃瞄中排除。

7. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請點選「全部匯出到 CSV」。開啟檔案或將其儲存至特定位置。

   CSV 檔案包含以下資訊：

   - 記錄檔中的所有資訊
   - 偵測時登入端點的使用者名稱

間諜程式/可能的資安威脅程式掃瞄結果

下列掃瞄結果會顯示在間諜程式/可能的資安威脅程式記錄檔中：

表 7-27. 第一層間諜程式/可能的資安威脅程式掃瞄結果

結果	說明
成功，不需要處理行動	這是中毒處理行動成功時的第一層結果。第二層結果可能是下列任一種： • 已清除 • 拒絕存取
需要進一步的處理行動	這是中毒處理行動未成功時的第一層結果。第二層結果至少具有下列其中一則訊息： • 暫不處理 • 無法刪除受保護系統檔案中的間諜程式/可能的資安威脅程式 • 已手動停止間諜程式/可能的資安威脅程式掃瞄。請執行完整掃瞄 • 間諜程式/可能的資安威脅程式已清除，需要重新啟動。請重新啟動電腦 • 無法清除間諜程式/可能的資安威脅程式 • 無法識別間諜程式/可能的資安威脅程式掃瞄結果。請聯絡趨勢科技客服部門

表 7-28. 第二層間諜程式/可能的資安威脅程式掃瞄結果

結果	說明	解決方案
已清除	Apex One 已終止程序或已刪除登錄、檔案、Cookie 和捷徑。	無
拒絕存取	Apex One 已拒絕存取（複製、開啟）偵測到的間諜程式/可能的資安威脅程式元件。	無
暫不處理	Apex One 不執行任何處理行動，但已記錄偵測到間諜程式/可能的資安威脅程式以進行評估。	將您認為安源的間諜程式/可能的資安威脅程式新增到間諜程式/可能的資安威脅程式核可清單。

結果	說明	解決方案
無法刪除受保護系統檔案中的間諜程式/可能的資安威脅程式	如果「間諜程式掃瞄引擎」嘗試刪除任何單一資料夾，而且又符合下列條件，就會顯示此訊息： • 要清除的項目超過 250MB。 • 作業系統使用資料夾中的檔案。正常系統作業可能也需要該資料夾。 • 該資料夾為根目錄（例如 C: 或 F:）	請與您的支援供應商聯絡，以獲得協助。
已手動停止間諜程式/可能的資安威脅程式掃瞄。請執行完整掃瞄	使用者在掃瞄作業完成之前停止掃瞄。	執行「手動掃瞄」並等待掃瞄完成。
間諜程式/可能的資安威脅程式已清除，需要重新啟動。請重新啟動電腦	Apex One 已刪除間諜程式/可能的資安威脅程式元件，但是需要重新啟動端點才能完成工作。	立即重新啟動端點。
無法清除間諜程式/可能的資安威脅程式	在 CD-ROM 或網路磁碟機上偵測到間諜程式/可能的資安威脅程式。Apex One 無法刪除在這些位置偵測到的間諜程式/可能的資安威脅程式。	手動移除中毒檔案。
無法識別間諜程式/可能的資安威脅程式掃瞄結果。請聯絡趨勢科技客服部門	新版的「間諜程式掃瞄引擎」提供新的掃瞄結果，Apex One 尚未設定為能夠處理這種掃瞄結果。	請聯絡您的支援供應商，以取得判斷新掃瞄結果的協助。

檢視間諜程式/可能的資安威脅程式恢復記錄檔

清除間諜程式/可能的資安威脅程式後，Security Agent 會備份間諜程式/可能的資安威脅程式資料。如果您認為資料無害，請通知線上用戶端恢復備份的資料。有關哪些間諜程式/可能的資安威脅程式備份資料已恢復、受影響的端點與恢復結果的資訊，均可在記錄檔中找到。

步驟

1. 移至「記錄檔 > 用戶端 > 間諜程式/可能的資安威脅程式恢復」。
2. 檢查「結果」欄，查看 Apex One 是否已成功恢復間諜程式/可能的資安威脅程式資料。
3. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請點選「匯出到 CSV」。開啟檔案或將其儲存至特定位置。

檢視可疑檔案記錄檔

Security Agent 在偵測到可疑檔案清單中的檔案時會產生記錄檔，並將記錄檔傳送到伺服器。

步驟

1. 移至下列其中一個項目：
   - 記錄檔 > 用戶端 > 安全威脅
   - 用戶端 > 用戶端管理
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「記錄檔 > 可疑檔案記錄檔」或「檢視記錄檔 > 可疑檔案記錄檔」。
4. 指定記錄條件，然後請點選「顯示記錄檔」。
5. 檢視記錄檔。記錄檔包含下列資訊：
   - 可疑檔案偵測的日期和時間
   - 端點
   - 網域

- 檔案的感染來源 SHA-1 雜湊值
- 檔案路徑
- 偵測到可疑檔案的掃瞄類型
- 掃瞄結果

  注意

  如需有關掃瞄結果的詳細資訊，請參閱病毒/惡意程式掃瞄結果 第 7-80 頁。

- IP 位址

檢視掃瞄作業記錄檔

執行「手動掃瞄」、「預約掃瞄」或「立即掃瞄」時，Security Agent 會建立包含該掃瞄相關資訊的掃瞄記錄檔。您可以存取 Apex One 伺服器或 Security Agent 主控台來檢視掃瞄記錄檔。

如果要在 Apex One 伺服器上檢視掃瞄作業記錄檔，請移至下列其中一個位置：

- 記錄檔 > 用戶端 > 安全威脅，然後請點選「檢視記錄檔 > 掃瞄作業記錄檔」。
- 用戶端 > 用戶端管理，然後請點選「記錄檔 > 掃瞄作業記錄檔」。

掃瞄作業記錄檔會顯示下列資訊：

- Apex One 開始掃瞄的日期和時間
- Apex One 停止掃瞄的日期和時間
- 掃瞄狀態
  - 已完成：掃瞄正常完成。
  - 中斷：使用者在掃瞄完成前停止掃瞄。

  - 意外停止：掃瞄作業被使用者、系統或意外事件中斷。例如：Apex One 的「即時掃瞄」服務可能已意外終止，或使用者強制重新啟動端點。
- 掃瞄類型
- 已掃瞄的物件數目
- 中毒病毒/惡意程式偵測數目
- 間諜程式/可能的資安威脅程式偵測數目
- 本機雲端病毒碼版本
- 病毒碼版本
- 間諜程式/可能的資安威脅程式病毒碼版本

安全威脅爆發

當特定時段偵測到的病毒/惡意程式、間諜程式/可能的資安威脅程式和共享資料夾作業階段超過某一臨界值時，即發生安全威脅爆發。有數種方式可因應及抑制病毒在網路上爆發疫情，包括：

- 啟動 Apex One 以監控網路上的可疑活動
- 封鎖重要的用戶端端點通訊埠與資料夾
- 傳送病毒爆發警訊給用戶端
- 清除中毒端點

安全威脅爆發條件和通知

設定 Apex One 在病毒爆發時，傳送通知給您和其他 Apex One 管理員。

表 7-29. 安全威脅爆發通知類型

類型	關係
• 病毒/惡意程式爆發 • 間諜程式/可能的資安威脅程式爆發 • 共享資料夾作業階段病毒爆發	配置安全威脅爆發條件和通知 第 7-93 頁
防火牆違規事件爆發	設定防火牆違規事件爆發條件和通知 第 13-28 頁
C&C 回呼爆發	設定 C&C 回呼爆發條件和通知 第 12-16 頁

根據偵測次數和偵測期間，定義病毒爆發條件。當 Apex One 在偵測期間的偵測次數超過設定的值時，就會觸發病毒爆發警訊。

Apex One 隨附一組預設通知訊息，用於通知您和其他 Apex One 管理員偵測到的病毒爆發。您可以視需要修改通知和設定其他通知設定。

注意

Apex One 可以透過電子郵件、SNMP Trap 和 Windows NT 事件記錄檔傳送安全威脅爆發通知。對於共享資料夾作業階段病毒爆發，Apex One 會透過電子郵件傳送通知。設定 Apex One 何時透過這些通道傳送通知的設定。

如需詳細資訊，請參閱管理員通知設定 第 14-35 頁。

配置安全威脅爆發條件和通知

步驟

1. 移至「管理 > 通知 > 病毒爆發」。
2. 在「條件」標籤中：
   a. 移至「病毒/惡意程式」和「間諜程式/可能的資安威脅程式」區段：
   b. 指定唯一偵測來源的數量。

c. 指定每個安全威脅的偵測次數和偵測期限。

秘訣

趨勢科技建議您接受此畫面中的預設值。

如果 Apex One 在 24 小時內收到 101 個病毒/惡意程式偵測，就會傳送通知。

3. 在「條件」標籤中：

   a. 移至「共享資料夾作業階段」區段。

   b. 選取「監控網路上的共享資料夾作業階段」。

   c. 在「記錄的共享資料夾作業階段」中，請點選數字連結，以檢視含有共享資料夾的端點和存取共享資料夾的端點。

   d. 指定共享資料夾作業階段數和偵測期間。

   Apex One 會在超過共享資料夾作業階段數時傳送通知訊息。

4. 在「電子郵件」標籤中：

   a. 移至「病毒/惡意程式爆發」、「間諜程式/可能的資安威脅程式爆發」和「共享資料夾作業階段病毒爆發」區段。

   b. 選取「啟動電子郵件通知」。

   c. 指定電子郵件收件者。

   d. 接受或修改預設的電子郵件主旨和訊息。您可以使用 Token 變數代表「主旨」和「訊息」欄位中的資料。

   表 7-30. 安全威脅爆發通知的 Token 變數

變數	說明
病毒/惡意程式爆發	
%CV	偵測到的病毒/惡意程式總數
%CC	具有病毒/惡意程式的端點總數

變數	說明
間諜程式/可能的資安威脅程式爆發	
%CV	偵測到的間諜程式/可能的資安威脅程式總數
%CC	具有間諜程式/可能的資安威脅程式的端點總數
共享資料夾作業階段病毒爆發	
%S	共享資料夾作業階段數量
%T	共享資料夾作業階段累計的時段
%M	時段，以分鐘為單位

e. 選取其他要納入電子郵件中的病毒/惡意程式與間諜程式/可能的資安威脅程式資訊。您可以納入用戶端/網域名稱、安全威脅名稱、偵測的日期和時間、路徑與中毒檔案，以及掃瞄結果。

f. 接受或修改預設的通知訊息。

5. 在「SNMP Trap」標籤中：

a. 移至「病毒/惡意程式爆發」和「間諜程式/可能的資安威脅程式爆發」區段。

b. 選取「啟動 SNMP Trap 通知」。

c. 接受或修改預設的訊息。您可以使用 Token 變數代表「訊息」欄位中的資料。如需詳細資訊，請參閱表 7-30：安全威脅爆發通知的 Token 變數 第 7-94 頁。

6. 在「NT 事件記錄檔」標籤中：

a. 移至「病毒/惡意程式爆發」和「間諜程式/可能的資安威脅程式爆發」區段。

b. 選取「啟動 NT 事件記錄檔通知」。

c. 接受或修改預設的訊息。您可以使用 Token 變數代表「訊息」欄位中的資料。如需詳細資訊，請參閱表 7-30：安全威脅爆發通知的 Token 變數 第 7-94 頁。

7. 請點選「儲存」。

設定安全威脅爆發防範

病毒爆發時，請實施病毒爆發防範措施，以因應並抑制病毒爆發。請謹慎設定防範設定，因為不正確的設定可能會導致無法預知的網路問題。

步驟

1. 移至「用戶端 > 病毒爆發防範」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「啟動病毒爆發防範」。
4. 請點選以下任一病毒爆發防範策略，然後設定該策略的設定：
   - 限制/拒絕存取共享資料夾 第 7-97 頁
   - 封鎖易受攻擊的通訊埠 第 7-98 頁
   - 拒絕檔案和資料夾的寫入權限 第 7-100 頁
   - 拒絕存取可執行的壓縮檔 第 7-102 頁
   - 在惡意程式處理程序/檔案上建立互斥處理 第 7-101 頁
5. 選取要執行的策略。
6. 選取病毒爆發防範持續有效的小時數。預設值為 48 小時。您可以在病毒爆發防範過期之前，手動恢復網路設定。

   警告!

   不允許病毒爆發防範永久有效。如果要無限期封鎖或拒絕存取特定檔案、資料夾或通訊埠，請直接修改端點和網路設定，而不要使用 Apex One。

7. 接受或修改預設用戶端通知訊息。

注意

如果要設定 Apex One 在病毒爆發時通知您，請移至「管理 > 通知 > 病毒爆發」。

8. 請點選「啟動病毒爆發防範」。

   您所選取的病毒爆發防範措施會顯示在新視窗中。

9. 回到病毒爆發防範用戶端樹狀結構中，核取「病毒爆發防範」欄位。

   套用病毒爆發防範措施的端點上會出現核取記號。

Apex One 會在系統事件記錄檔中記錄下列事件：

- 伺服器事件（開始病毒爆發防範，並通知用戶端啟動病毒爆發防範）
- Security Agent 事件（啟動病毒爆發防範）

病毒爆發防範策略

病毒爆發時，請實施下列任何一項策略：

- 限制/拒絕存取共享資料夾 第 7-97 頁
- 封鎖易受攻擊的通訊埠 第 7-98 頁
- 拒絕檔案和資料夾的寫入權限 第 7-100 頁
- 拒絕存取可執行的壓縮檔 第 7-102 頁
- 在惡意程式處理程序/檔案上建立互斥處理 第 7-101 頁

限制/拒絕存取共享資料夾

在病毒爆發期間，請限制或拒絕存取網路上的共享資料夾，以防止安全威脅透過共享資料夾散佈。

此策略生效時，使用者仍可共享資料夾，但此策略不會套用至新的共享資料夾。因此，請通知使用者不要在病毒爆發期間共享資料夾，或是重新部署策略並將其套用至新的共享資料夾。

步驟

1. 移至「用戶端 > 病毒爆發防範」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「啟動病毒爆發防範」。
4. 請點選「限制/拒絕存取共享資料夾」。
5. 請選取下列選項：
   - 僅允許唯讀：限制存取共享資料夾
   - 拒絕存取

   注意

   唯讀設定不會套用到已設定為拒絕完整存取的共享資料夾。
6. 請點選「儲存」。

   「病毒爆發防範設定」畫面會再次顯示。
7. 請點選「啟動病毒爆發防範」。

   您所選取的病毒爆發防範措施會顯示在新視窗中。

封鎖易受攻擊的通訊埠

在病毒爆發期間，請封鎖易受攻擊的通訊埠，以防止病毒/惡意程式用以存取 Security Agent 端點。

警告!

請謹慎設定「病毒爆發防範」設定。封鎖使用中的通訊埠會使倚賴它們的網路服務無法使用。例如，如果您封鎖信任的通訊埠，Apex One 便無法在病毒爆發期間與用戶端通訊。

步驟

1. 移至「用戶端 > 病毒爆發防範」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「啟動病毒爆發防範」。
4. 請點選「封鎖通訊埠」。
5. 選取是否封鎖信任的通訊埠。
6. 在「封鎖通訊埠」欄下選取要封鎖的通訊埠。
   a. 如果表格中沒有通訊埠，請點選「新增」。在開啟的畫面中，選取要封鎖的通訊埠，然後請點選「儲存」。
      - 所有通訊埠（包括 ICMP）：封鎖所有通訊埠，但不包括信任的通訊埠。如果您要一併封鎖信任的通訊埠，請在上一個畫面中選取「封鎖信任的通訊埠」核取方塊。
      - 指定的通訊埠
        - 一般使用的通訊埠：至少為 Apex One 選取一個通訊埠號碼，以便儲存封鎖通訊埠設定。
        - 特洛伊木馬程式常用的通訊埠：封鎖特洛伊木馬程式常用的通訊埠。
        - 1 到 65535 之間的任何通訊埠或通訊埠範圍：選擇性地指定要封鎖的傳輸方向和某些備註（例如，封鎖您指定之通訊埠的原因）。
        - Ping 通訊協定（拒絕 ICMP）：如果您只要封鎖 ICMP 封包（例如：ping 要求），則請點選這項。

b. 如果要編輯遭封鎖通訊埠的設定，請點選通訊埠號碼。

c. 在開啟的畫面中修改設定，然後請點選「儲存」。

d. 如果要從清單中移除通訊埠，請選取通訊埠號碼旁的核取方塊，然後請點選「刪除」。

7. 請點選「儲存」。

   「病毒爆發防範設定」畫面會再次顯示。

8. 請點選「啟動病毒爆發防範」。

   您所選取的病毒爆發防範措施會顯示在新視窗中。

拒絕檔案和資料夾的寫入權限

病毒/惡意程式可能會修改或刪除主機端點上的檔案和資料夾。在病毒爆發時，請設定 Apex One，讓它防止病毒/惡意程式修改或刪除 Security Agent 端點上的檔案和資料夾。

警告!

Apex One 不支援拒絕寫入對應的網路磁碟機。

步驟

1. 移至「用戶端 > 病毒爆發防範」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「啟動病毒爆發防範」。
4. 請點選「拒絕檔案和資料夾的寫入權限」。
5. 輸入目錄路徑。當您輸入要防護的目錄路徑後，請點選「新增」。

注意

請輸入目錄的絕對路徑，而非虛擬路徑。

6. 在受防護的目錄中指定要防護的檔案。選取所有檔案或具有特定副檔名的檔案。如果使用副檔名，請指定不在清單中的副檔名，在文字方塊中輸入該副檔名，然後請點選「新增」。

7. 如果要保護特定檔案，請在「要防寫防護的檔案」下輸入完整檔案名稱，然後請點選「新增」。

8. 請點選「儲存」。

   「病毒爆發防範設定」畫面會再次顯示。

9. 請點選「啟動病毒爆發防範」。

   您所選取的病毒爆發防範措施會顯示在新視窗中。

在惡意程式處理程序/檔案上建立互斥處理

您可以設定病毒爆發防範來防止利用互斥處理程式的安全威脅，方法是覆寫威脅在系統中感染和散佈所需的資源。「病毒爆發防範」會在有關已知惡意程序的檔案和處理程序上建立互斥，以防止惡意程式存取這些資源。

秘訣

趨勢科技建議您在可實行惡意程式安全威脅的解決方案之前，維持使用這些例外。請聯絡客服部門以取得正確的互斥名稱來提供病毒爆發期間的防護。

注意

互斥處理需要「未經授權的變更阻止服務」，並且僅支援 32 位元平台。

步驟

1. 移至「用戶端 > 病毒爆發防範」。

2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「啟動病毒爆發防範」。
4. 請點選「在惡意程式處理程序/檔案上建立互斥處理」。
5. 在提供的文字欄位中輸入要防護的互斥名稱。

   使用 + 和 - 按鈕從清單新增或移除互斥名稱。

   注意

   病毒爆發防範最多支援對六個互斥威脅進行互斥處理。

6. 請點選「儲存」。

   「病毒爆發防範設定」畫面會再次顯示。

7. 請點選「啟動病毒爆發防範」。

   您所選取的病毒爆發防範措施會顯示在新視窗中。

拒絕存取可執行的壓縮檔

在病毒爆發期間，拒絕存取可執行的壓縮檔可防止這些檔案中可能包含的安全威脅在網路中散佈。您可以選擇允許存取由支援的可執行封裝程式建立的受信任檔案。

步驟

1. 移至「用戶端 > 病毒爆發防範」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「啟動病毒爆發防範」。
4. 請點選「拒絕存取可執行的壓縮檔」。

5. 從支援的可執行封裝程式清單中進行選取，然後請點選「新增」允許存取由這些封裝程式建立的可執行壓縮檔。

   注意

   您只能核可使用由「可執行的封裝程式」清單中的封裝程式建立的壓縮檔。病毒爆發防範拒絕存取所有其他可執行的壓縮檔格式。

6. 請點選「儲存」。

   「病毒爆發防範設定」畫面會再次顯示。

7. 請點選「啟動病毒爆發防範」。

   您所選取的病毒爆發防範措施會顯示在新視窗中。

關閉病毒爆發防範

當您確認已抑制病毒爆發且 Apex One 已清除或隔離所有中毒檔案時，請關閉「病毒爆發防範」，將網路設定恢復為正常狀態。

步驟

1. 移至「用戶端 > 病毒爆發防範」。
2. 在用戶端樹狀結構中，請點選根網域圖示 ( ) 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「恢復設定」。
4. 如果要通知使用者病毒爆發已結束，請選取「恢復原始設定後通知使用者」。
5. 接受或修改預設用戶端通知訊息。
6. 請點選「恢復設定」。

注意

如果您沒有手動恢復網路設定，Apex One 會在經過「病毒爆發防範設定」畫面的「經過 __ 小時後，自動將網路的設定恢復為正常」中指定的時數後，自動恢復這些設定。預設設定為 48 小時。

Apex One 會在系統事件記錄檔中記錄下列事件：

- 伺服器事件（開始病毒爆發防範，並通知 Security Agent 啟動病毒爆發防範）
- Security Agent 事件（啟動病毒爆發防範）

7. 在關閉病毒爆發防範後，掃瞄網路端點是否有安全威脅，以確保已抑制病毒爆發。

第 8 章

防範未知安全威脅

本章說明如何保護端點，以免未知的安全威脅嘗試入侵您的網路。

包含下列主題：

Machine Learning

趨勢科技 Machine Learning 採用進階機器學習技術來關聯安全威脅資訊，並執行深度檔案分析來偵測新興的未知安全威脅，這透過數位 DNA 指紋、API 對應和其他檔案特徵來實現。Machine Learning 還會對未知或不太普遍的處理程序執行行為分析，以確定是否有新興或未知安全威脅正企圖讓您的網路中毒。

Machine Learning 是一個功能強大的工具，可協助保護您的環境，使其免遭不明安全威脅和零時差攻擊。

偵測類型	說明
檔案	Security Agent 在偵測到未知或不常見的檔案之後，會使用進階安全威脅掃瞄引擎 (ATSE) 掃瞄該檔案，以便擷取檔案特徵，然後將報告傳送給裝載於趨勢科技主動雲端截毒技術上的 Machine Learning 引擎。透過使用惡意程式模擬，Machine Learning 將範例與惡意程式模型進行比較、指定概率分數，並確定檔案可能包含的惡意程式類型。 如果正常運作的 Internet 連線無法使用，Machine Learning 會自動切換至本機模式來提供不間斷的未知安全威脅防護，以抵禦可攜式可執行檔安全威脅。 視您對 Machine Learning 進行的設定而定，Security Agent 可能會嘗試「隔離」受影響的檔案，以防安全威脅繼續擴散到您的整個網路。

偵測類型	說明
處理程序	Security Agent 在偵測到未知或不常見的程序之後，會使用關聯式智慧型引擎監控該程序，然後將行為報告傳送給 Machine Learning 引擎。透過使用行為惡意程式塑型，Machine Learning 將處理程序行為與模型進行比較、指定概率分數，並確定處理程序可能正在執行的惡意程式類型。 程序偵測也會監控程式檔執行。如果關聯式智慧型引擎偵測到可疑程式檔執行，Machine Learning 會採取設定的處理行動。 Machine Learning 會對下列類型的程式檔執行程式檔封鎖： • cscript • jar • powershell • vbs • wscript 視您對 Machine Learning 進行的設定而定，Security Agent 可能會「終止」受影響的程序或程式檔，然後嘗試清除執行該程序或程式檔的檔案。

設定 Machine Learning 設定

注意

若要使用「Machine Learning」，您必須啟動下列服務：

- 未經授權的變更阻止
- 進階防護服務

如需詳細資訊，請參閱設定其他 Security Agent 服務 第 15-11 頁。

步驟

1. 移至「用戶端 > 用戶端管理」。

2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > Machine Learning 設定」。

   會出現「Machine Learning 設定」畫面。
4. 選取「啟動 Machine Learning」。
5. 在「偵測設定」下，選取偵測的類型以及「Machine Learning」採取的相關處理行動。

偵測類型	處理行動
檔案	• 隔離：選取此項，即會自動依「Machine Learning」分析結果，將展現惡意程式相關特徵的檔案隔離 • 僅記錄檔：選取此項，即會掃瞄未知檔案並記錄「Machine Learning」分析結果，以供內部進一步調查安全威脅
處理程序	• 終止：選取此項，即會自動依「Machine Learning」分析結果，將展現惡意程式相關行為的程序或程式檔終止 重要 「Machine Learning」會嘗試將已執行惡意程序或程式檔的檔案清除。如果清除處理行動不成功，Machine Learning 會將受影響的檔案隔離。 • 僅記錄檔：選取此項，即會掃瞄未知程序或程式檔並記錄「Machine Learning」分析結果，以供內部進一步調查安全威脅

6. 在「例外」下，設定全域的「Machine Learning」檔案例外，以防止所有用戶端將某個檔案偵測為惡意檔案。
   a. 請點選「新增檔案雜湊」。

      會出現「將檔案新增到例外清單」畫面。
   b. 指定要從掃瞄中排除的檔案 SHA-1 雜湊值。
   c. （選擇性）提供附註來解釋當成例外的原因，或是說明與雜湊值相關聯的檔案名稱。

d. 按一下「新增」。

Machine Learning 便會將檔案雜湊新增到「例外」清單。

7. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

- 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
- 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

可疑連線服務

可疑連線服務管理使用者定義的及全域 IP C&C 清單，並監控端點與潛在 C&C 伺服器之間連線的行為。

- 使用者定義的核可和封鎖 IP 清單允許進一步控制端點是否可以存取特定 IP 位址。如果要允許存取全域 C&C IP 清單封鎖的位址，或封鎖對可能具有安全威脅之位址的存取，請設定這些清單。

  如需詳細資訊，請參閱設定全域使用者定義的 IP 清單設定 第 8-6 頁。

- 全域 C&C IP 清單會與網路內容檢測引擎 (NCIE) 搭配運作，偵測與趨勢科技確認之 C&C 伺服器之間的網路連線。NCIE 會透過任何網路通道，偵測 C&C 伺服器聯絡人。可疑連線服務會記錄與全域 C&C IP 清單中的伺服器的所有連線資訊，以供評估。

  如需有關啟動全域 C&C IP 清單的詳細資訊，請參閱設定可疑連線設定 第 8-7 頁。

- 透過網路封包上的相符關聯規則病毒碼偵測到端點上的惡意程式後，可疑連線服務可以進一步調查連線行為以確定是否發生 C&C 回呼。偵測到 C&C 回呼後，可疑連線服務可以嘗試使用 GeneriClean 技術封鎖並清除連線來源。

如需有關設定可疑連線服務的詳細資訊，請參閱設定可疑連線設定 第 8-7 頁。

如需有關 GeneriClean 的詳細資訊，請參閱 GeneriClean 第 D-4 頁。

在「其他服務設定」畫面上啟動可疑連線服務，以防止用戶端受到 C&C 伺服器回呼的危害。如需詳細資訊，請參閱設定其他 Security Agent 服務 第 15-11 頁。

設定全域使用者定義的 IP 清單設定

管理員可將 Apex One 設定為允許、封鎖或記錄用戶端與使用者定義的 C&C IP 位址之間的所有連線。

注意

使用者定義的 IP 清單僅支援 IPv4 位址。

步驟

1. 移至「用戶端 > 全域用戶端設定」。
2. 請點選「安全設定」標籤。
3. 移至「可疑連線設定」區段。
4. 請點選「編輯使用者定義的 IP 清單」。
5. 在「核可的清單」或「封鎖的清單」標籤中，新增要監控的 IP 位址。

秘訣

您可以將 Apex One 設定為僅記錄檔與使用者定義的封鎖 IP 清單中的位址建立的連線。如果要僅記錄檔與使用者定義的封鎖 IP 清單中的位址建立的連線，請參閱設定可疑連線設定 第 8-7 頁。

a. 請點選「新增」。

b. 在顯示的新畫面中，輸入要讓 Apex One 監控的 IP 位址、IP 位址範圍或 IPv4 位址和子網路遮罩。

c. 請點選「儲存」。

6. 如果要從清單中移除 IP 位址，請選取位址旁的核取方塊，然後請點選「刪除」。

7. 在設定清單後，請點選「關閉」回到「全域用戶端設定」畫面。

8. 請點選「儲存」，將更新的清單部署至用戶端。

設定可疑連線設定

Security Agent 可以記錄並封鎖端點與全域 C&C IP 清單中的位址之間建立的所有連線。您還可以記錄（同時也可存取）使用者定義的封鎖 IP 清單中設定的 IP 位址。

Security Agent 也可以監控可能由僵屍網路或其他惡意程式威脅產生的連線。偵測到惡意程式威脅後，Security Agent 可嘗試清除感染。

步驟

1. 移至「用戶端 > 用戶端管理」。

2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。

3. 請點選「設定 > 可疑連線設定」。

   會出現「可疑連線設定」畫面。

4. 啟動「偵測對全域 C&C IP 清單中的位址進行的網路連線」設定，來監控對趨勢科技已確認之 C&C 伺服器進行的連線，然後選取「僅記錄」或「封鎖」連線。

   - 如果要允許用戶端連線到使用者定義的封鎖 IP 清單中的位址，請啟動「記錄並允許存取使用者定義的封鎖 IP 清單位址」設定。

注意

您必須先啟動網路連線記錄，然後 Security Agent 才能允許存取使用者定義的封鎖 IP 清單中的位址。

如需有關全域 C&C IP 清單的詳細資訊，請參閱可疑連線服務 第 8-5 頁。

5. 啟動「使用惡意程式網路特徵鑑別來偵測連線」設定，然後選取「僅記錄檔」或「封鎖」連線。

   惡意程式網路特徵鑑別會對封包標頭執行病毒碼比對。只要封包的標頭經關聯規則病毒碼比對後，符合已知惡意程式安全威脅，Security Agent 就會記錄這些封包進行的所有連線。

   - 如果要允許 Security Agent 嘗試清除與 C&C 伺服器建立的連線，請啟動「偵測到 C&C 回呼時清除可疑連線」設定。Security Agent 會使用 GeneriClean 清除惡意程式威脅，並終止與 C&C 伺服器的連線。

注意

您必須先啟動「使用惡意程式網路特徵鑑別的記錄檔連線」，Security Agent 才能嘗試清除與封包結構比對偵測到的 C&C 伺服器之間建立的連線。

6. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

樣本提交

您可以將 Security Agent 設定為在發現檔案物件可能包含先前未曾識別出的安全威脅時，將檔案物件提交給沙箱做進一步分析。沙箱在評估物件之後，如果

發現物件包含未知的安全威脅，就會將物件新增至沙箱的可疑物件清單，然後將清單分發給整個網路中的其他 Security Agent。

如需詳細資訊，請參閱可疑物件清單設定 第 14-31 頁。

使用「樣本提交」，必須符合下列條件：

- 您必須向 Control Manager 伺服器（7.0 或更新版本）或 Trend Micro Apex Central 伺服器（2019 或更新版本）註冊 Apex One 伺服器
- Control Manager 或 Trend Micro Apex Central 伺服器必須與 Trend Micro Deep Discovery Analyzer 伺服器（5.1 或更新版本）有正常運作的連線

可疑檔案包括下列任何項目：

- 未經趨勢科技判定的程式（經由支援的 Web 瀏覽器或電子郵件通道下載）
- 啟發式引擎偵測到的可疑程序（經由支援的 Web 瀏覽器或電子郵件通道下載）
- 卸除式儲存裝置中較少見的自動執行程式

Important

Security Agent 可以提交變更的樣本檔大小，視您使用的沙箱的類型而定。如果使用的是 Deep Discovery Analyzer 伺服器，樣本檔的大小可達 50 MB。如果使用的是 Deep Discovery Analyzer as a Service 附加元件，樣本檔的大小可達 60 MB。

設定樣本提交

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。

3. 請點選「設定 > 樣本提交設定」。

   會出現「樣本提交設定」畫面。

4. 選取「啟動將可疑檔案提交到沙箱」。

5. 請點選「儲存」。

未知安全威脅記錄檔

Security Agent 會記錄未知的安全威脅活動，並將記錄檔傳送給伺服器。任何持續運作的 Security Agent 會依指定的時間間隔（預設為每 60 分鐘）彙總一次記錄檔並進行傳送。

如果要避免記錄檔佔去過多硬碟空間，請手動刪除記錄檔或設定記錄檔刪除預約時程。如需有關管理記錄檔的詳細資訊，請參閱記錄檔管理 第 14-39 頁。

檢視 Machine Learning 記錄檔

步驟

1. 移至下列其中一個項目：
   - 記錄檔 > 用戶端 > 安全威脅
   - 用戶端 > 用戶端管理
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請移至「Machine Learning 記錄檔條件」畫面：
   - 在「安全威脅記錄檔」畫面中，點選「檢視記錄檔 > Machine Learning 記錄檔」。
   - 在「用戶端管理」畫面中，點選「記錄檔 > Machine Learning 記錄檔」。

4. 指定記錄條件，然後請點選「顯示記錄檔」。
5. 檢視記錄檔。記錄檔包含下列資訊：

項目	說明
日期/時間	發生偵測的時間
端點	發生偵測的端點
IP 位址	來源端點的 IP 位址和通訊埠號碼
安全威脅	Machine Learning 引擎判斷出的安全威脅名稱
結果	採取處理行動的結果
中毒檔案/物件	執行程序的檔案物件或程式名稱
類型	觸發偵測的物件類型（「檔案」或「程序」）
檔案路徑	執行程序的檔案物件路徑或程式路徑
感染通道	安全威脅源自的通道
詳細資訊	顯示特定偵測詳細分析的連結 如需詳細資訊，請參閱 Machine Learning 記錄檔詳細資料 第 8-11 頁。

6. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請點選「全部匯出到 CSV」。開啟檔案或將其儲存至特定位置。

Machine Learning 記錄檔詳細資料

您可以針對 Machine Learning 記錄檔中的每個偵測，請點選「詳細資料」欄下的「檢視」連結來檢視完整的報告。

「記錄檔詳細資料」畫面包含兩個區段：

- 頂端的標題：與記錄檔中的此特定偵測相關的特定詳細資料

- 底部的標籤控制項：與 Machine Learning 安全威脅相關的詳細資料，包括安全威脅可能性評分、檔案資訊，以及您網路中具有相同偵測項目的其他端點

下表討論頂端標題中提供的資訊。

表 8-1. 記錄檔詳細資料 - 頂端的標題

區段	說明
偵測時間/處理行動	指出記錄檔中的此特定偵測發生的時間，以及用戶端對安全威脅採取的處理行動
檔案名稱	指出在指定端點上觸發偵測的檔案名稱 秘訣 請點選「新增到例外清單」，可快速將受影響檔案的檔案雜湊值新增到全域的 Machine Learning 例外清單。在「Machine Learning 設定」畫面上，可檢視完整例外清單。 如需詳細資訊，請參閱設定 Machine Learning 設定 第 8-3 頁。 重要 此偵測所偵測到的檔案名稱可能會與其他用戶端上偵測到的檔案名稱不同。「Machine Learning」是依檔案雜湊值將偵測項目彼此關聯，而非依特定檔案名稱。檢視「受影響的端點」標籤，即可確認其他端點上的檔案名稱。
端點資訊	顯示偵測到時已登入的使用者、端點名稱，以及端點的 IP 位址
通道資訊	顯示安全威脅源自的通道，以及端點上安全威脅移轉到的資料夾位置

下表討論底部標籤上提供的資訊。

表 8-2. 記錄檔詳細資料 - 標籤資訊

標籤	說明
安全威脅指標	提供 Machine Learning 分析的結果 • 安全威脅可能性：指出檔案/程序符合惡意程式模型的程度 • 可能的安全威脅類型：指出「Machine Learning」在將分析結果與其他已知的安全威脅相比較後，所發現檔案中最可能包含的安全威脅類型 • 安全威脅識別碼：列出檔案/程序中所使用、可能指示出現了所偵測安全威脅類型的 API 函數。 重要 判斷安全威脅類型時，API 函數識別是唯一一個考量因素。「Machine Learning」會使用其他許多檔案特徵與分析方法，來計算安全威脅可能性和可能的安全威脅類型。 • 類似的已知安全威脅：列出已知會展現出與此偵測類似之檔案/程序特徵的安全威脅類型
檔案詳細資料	針對此特定偵測記錄檔，提供與檔案內容和憑證資訊相關的一般詳細資料
受影響的端點	列出您網路中其他被「Machine Learning」偵測到同一安全威脅的用戶端，並提供其他用戶端上該偵測的特定詳細資料

檢視可疑連線記錄檔

步驟

1. 移至下列其中一個項目：
   - 記錄檔 > 用戶端 > 安全威脅
   - 用戶端 > 用戶端管理
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。

3. 請移至「可疑連線記錄檔條件」畫面：
   - 在「安全威脅記錄檔」畫面中，點選「檢視記錄檔 > 可疑連線記錄檔」。
   - 在「用戶端管理」畫面中，點選「記錄檔 > 可疑連線記錄檔」。
4. 指定記錄條件，然後請點選「顯示記錄檔」。
5. 檢視記錄檔。記錄檔包含下列資訊：

項目	說明
日期/時間	發生偵測的時間
端點	發生偵測的端點
網域	發生偵測之端點的網域
處理程序	嘗試聯絡時所使用的程序 (path\application_name)
本機 IP 和通訊埠	來源端點的 IP 位址和通訊埠號碼
遠端 IP 和通訊埠	目標端點的 IP 位址和通訊埠號碼
結果	採取處理行動的結果
清單來源	辨識 C&C 伺服器的 C&C 清單來源
傳輸方向	傳輸的方向

6. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請點選「全部匯出到 CSV」。開啟檔案或將其儲存至特定位置。

檢視樣本提交記錄檔

Apex One 會在系統事件記錄檔中儲存樣本提交資料。如需樣本提交資料的更完整摘要，趨勢科技建議您使用 Apex Central 主控台來檢視記錄檔。Apex Central 會提供可疑物件檔案處理程序的詳細分析，讓您更瞭解可疑物件可能會對您的網路造成哪些影響。

步驟

1. 移至「記錄檔 > 系統事件」。
2. 在「事件」下，檢查是否有下列記錄檔類型：
   - 「已向沙盒虛擬平台提交樣本 [檔案[<file_name]，SHA1[<file_SHA1_value>]」
   - 「沙盒虛擬平台樣本分析完成 [<date_time_analysis_completed>，檔案[<file_name]，SHA1[<file_SHA1_value>]，病毒[<detection_type]，規則[<virtual_analyzer_rule_type]]」

第 9 章

使用行為監控

本章說明如何使用行為監控功能來保護電腦免於受到安全威脅的侵襲。

包含下列主題：

行為監控

行為監控會不斷地監控端點上的作業系統或已安裝軟體是否發生了異常修改。行為監控透過惡意程式行為封鎖和事件監控來保護端點。這兩個功能搭配使用者已設定的例外清單和認證安全防護軟體服務更是相得益彰。

重要

依預設，「行為監控」在所有版本的 Windows Server 平台上均是關閉的。

惡意程式行為封鎖

惡意程式行為封鎖能夠提供多一層的必要安全威脅防護，以封鎖存在惡意行為的程式。它會觀察一段時間內的系統事件。當程式執行不同的動作組合或動作序列時，惡意程式行為封鎖會偵測已知的惡意行為並封鎖關聯程式。使用此功能可確保以更高等級來抵禦全新、未知和新興的安全威脅。

「行為監控」可偵測合法 Windows 程式執行的惡意程式檔以及合法 DLL 所執行的程式檔本身真正的酬載路徑，協助端點防範隱藏在無檔案式攻擊媒介中的惡意程式。

惡意程式行為監控會提供以下威脅程度掃瞄選項：

- 「已知安全威脅」：封鎖與已知惡意程式安全威脅相關聯的行為
- 「已知和潛在威脅」：封鎖與已知威脅相關聯的行為並對可能是惡意的行為採取處理行動

在已啟動通知的情況下，封鎖某個程式後，Security Agent 會在端點上顯示通知。

如需有關通知的詳細資訊，請參閱 Security Agent 使用者的行為監控通知 第 9-17 頁。

勒索軟體防護

「勒索軟體防護」會阻止「勒索軟體」安全威脅未經授權即修改或加密用戶端上的檔案。勒索軟體是一種惡意軟體，會限制存取檔案，並要求付錢才能恢復受影響的檔案。

Apex One 提供下列方法，保護您的環境不受勒索軟體安全威脅的侵害。

注意

若要減少 Security Agent 將安全的程序偵測為惡意程式的機會，請確保用戶端具有 Internet 存取，以使用趨勢科技伺服器執行其他驗證程序。

選項	說明
保護文件以防止未經授權的加密或修改	您可以設定行為監控偵測可能代表勒索軟體攻擊的特定事件序列。在「行為監控」比對以下所有條件後，Security Agent 就會終止並嘗試隔離惡意程式： 1. 某個未被識別安全的程序嘗試在一段時間內修改、刪除或重新命名三個檔案。 2. 程序嘗試修改受保護的副檔名類型 此外，啟動「自動備份可疑程式變更的檔案」，可為端點上要加密的檔案建立副本。完成加密程序後，如果 Apex One 偵測到勒索軟體安全威脅，Apex One 會提示使用者恢復受影響的檔案，而無須承受任何資料遺失之苦。 注意 自動檔案備份需要用戶端端點上至少有 100 MB 的磁碟空間，而且僅會備份大小小於 10 MB 的檔案。 用戶端端點上的備份資料夾位置為：<用戶端安裝資料夾>\CCSF\module\DRE\data。 警告! 如果未啟動「自動備份可疑程式變更的檔案」，Apex One 無法復原受勒索軟體安全威脅影響的最初檔案。

選項	說明
封鎖通常與勒索軟體相關的程序	勒索軟體通常會先將可執行檔分發到端點上的特定位置，然後再嘗試綁架檔案。封鎖從這些位置啟動的程序，有助於讓勒索軟體無法綁架檔案。
啟動程式檢測，以偵測並封鎖遭到入侵的可執行檔	程式檢測會監控程序並執行 API 攔截，藉以判斷某個程式是否存在非預期的行為。雖然此程序可提高對遭到入侵的可執行檔的整體偵測率，卻可能會導致系統效能降低。 秘訣 如果您在「要封鎖的安全威脅」下拉式清單中選取「已知和潛在安全威脅」，程式檢測會提供增強的安全性。

弱點攻擊防護

弱點攻擊防護會與程式檢測搭配運作，藉以監控程式的行為，並偵測可能代表攻擊者已攻擊程式弱點的異常行為。偵測到異常行為後，「行為監控」就會終止程式程序。

重要

若要使用「弱點攻擊防護」，您必須選取「啟動程式檢測，以偵測並封鎖遭到入侵的可執行檔」。

新發現的程式防護

「行為監控」與「網頁信譽評等服務」和「即時掃瞄」搭配使用時，可驗證經由 Web 通道、電子郵件應用程式或 Microsoft Office 巨集指令碼下載的檔案的普遍程度。偵測到「新發現」的檔案後，管理員可選擇在執行檔案之前提示使用者。趨勢科技會根據偵測到檔案的次數或是檔案存在的時間長度（由主動雲端截毒技術判定），決定是否將程式分類為新發現的程式。

「行為監控」會掃瞄每個通道的下列檔案類型：

- Web (HTTP/HTTPS)：掃瞄 `.exe` 檔案。

- 電子郵件應用程式：掃瞄 .exe 檔案以及未加密的 .zip 和 .rar 檔案中的壓縮 .exe 檔案。

注意

- 管理員必須啟動用戶端上的「網頁信譽評等服務」以允許 Security Agent 掃瞄 HTTP 或 HTTPS 流量，然後才能顯示此提示。
- Security Agent 會在執行程序期間比對透過電子郵件應用程式下載的檔案名稱。如果檔案名稱已變更，使用者就不會收到提示。

事件監控

事件監控提供了一種更為通用的方法來抵禦未授權軟體和惡意程式攻擊。它會在系統區域中監控某些事件，允許管理員調整觸發此類事件的程式。如果您的特定系統保護需求高於惡意程式行為封鎖提供的需求，請使用事件監控。

以下表格為監控系統事件清單。

表 9-1. 監控的系統事件

事件	說明
重複的系統檔案	許多惡意程式會使用 Windows 系統檔案所使用的檔案名稱，來建立本身或其他惡意程式的副本。這樣做通常是為了覆寫或取代系統檔案、規避偵測，或讓使用者不敢隨意刪除惡意檔案。
Hosts 檔案修改	Hosts 檔案可將網域名稱對應到 IP 位址。許多惡意程式皆有能力修改主機檔案，而使網路瀏覽器重新導向至中毒、不存在或偽造的網站。
可疑行為	可疑行為是合法程式很少執行的特定動作或一系列動作。使用有可疑行為的程式時應小心謹慎。
新 Internet Explorer 嵌入程式	間諜程式/可能的資安威脅程式通常會安裝不必要的 Internet Explorer 嵌入程式，包括工具列和瀏覽器協助物件。
Internet Explorer 設定的修改	惡意程式可能會變更 Internet Explorer 設定，包括首頁、信任的網站、Proxy 伺服器設定和功能表擴充項目等。

事件	說明
安全策略修改	修改「Windows 安全策略」可允許不必要的應用程式執行及變更系統設定。
程式庫插入	許多惡意程式都會設定 Windows，以讓所有應用程式自動載入程式庫 (DLL)。這樣可讓 DLL 中的惡意常式在每次應用程式啟動時執行。
Shell 的修改	許多惡意程式都會修改 Windows Shell 設定，以將本身與特定檔案類型關聯。此常式可讓惡意程式在使用者於「Windows 檔案總管」中開啟關聯的檔案時自動啟動。變更 Windows Shell 設定也可以讓惡意程式追蹤所使用的程式，以及隨著合法應用程式啟動。
新服務	Windows 服務是具有特殊功能的處理程序，通常以完整的系統管理權限在背景連續執行。惡意程式有時會將本身安裝為服務，以維持隱藏狀態。
系統檔案修改	特定 Windows 系統檔案決定系統行為，包括啟動程式和螢幕保護裝置設定。許多惡意程式都會修改系統檔案，以在系統啟動時自動啟動並控制系統行為。
防火牆策略的修改	「Windows 防火牆策略」決定可存取網路的應用程式、開放用於通訊的通訊埠，以及可與電腦通訊的 IP 位址。許多惡意程式都會修改策略，以允許本身存取網路和 Internet。
系統程序的修改	許多惡意程式會在內建 Windows 處理程序中執行各種動作。這些動作可能包含終止或修改執行中的處理程序。
新啟動程式	惡意應用程式通常會在 Windows 登錄中新增或修改自動啟動項目，以在每次電腦啟動時自動啟動。

當事件監控偵測到監控的系統事件時，它會執行針對此事件所設定的處理行動。

以下表格列出的是管理員在監控系統事件上可採取的行動。

表 9-2. 監控的系統事件的處理行動

處理行動	說明
評估	Security Agent 一律允許與事件相關聯的程式執行，並且會記錄事件以供評估。 這是對所有監控的系統事件的預設處理行動。 注意 這個選項不支援 64 位元系統的程式庫植入（DLL 植入）事件。
允許	Security Agent 一律允許與事件相關聯的程式執行。
需要時詢問	Security Agent 會提示使用者允許或拒絕與事件相關聯的程式執行，並將該程式新增到例外清單。 如果使用者在特定的時間內未回應，Security Agent 會自動允許此程式執行。預設時間為 30 秒。 如果要修改此時間範圍，請參閱配置全域行為監控設定 第 9-14 頁。 注意 這個選項不支援 64 位元系統的程式庫植入（DLL 植入）事件。
拒絕	Security Agent 一律封鎖與事件相關聯的程式執行，並且會記錄事件。 在已啟動通知的情況下，封鎖某個程式後，Security Agent 會在端點上顯示通知。 如需有關通知的詳細資訊，請參閱 Security Agent 使用者的行為監控通知 第 9-17 頁。

行為監控例外清單

行為監控例外清單包含 Security Agent 未使用行為監控加以監控的程式。

- 核可的程式：Security Agent 會讓「核可的程式」清單中的所有程式通過行為監控掃瞄。

  注意

  雖然行為監控不會對已新增至「核可的程式」清單的程式採取處理行動，但其他掃瞄功能（例如，檔案型掃瞄）仍會先掃瞄程式再允許程式程行。

- 封鎖的程式：Security Agent 會封鎖「封鎖的程式」清單中的所有程式。若要設定「封鎖的程式」清單，請啟動「事件監控」。

從 Web 主控台設定例外清單。您也可以授與使用者權限，讓他們可以從 Security Agent 主控台設定自己的例外清單。

如需詳細資訊，請參閱行為監控權限 第 9-16 頁。

例外清單萬用字元支援

在定義檔案路徑、檔案名稱和副檔名等例外類型時，行為監控核可清單支援使用萬用字元。請使用下表來正確格式化例外清單，以確保 Apex One 不掃瞄正確的檔案和資料夾。

支援的萬用字元：

- 星號 (*)：代表任意字元或一串字元
- 問號 (?)：代表單一字元

重要

行為監控核可清單不支援使用萬用字元來取代系統磁碟機代號或 UNC 位址。

例外類型	萬用字元用法	相符	不相符
目錄	`C:\*` 排除指定磁碟機中的所有檔案和資料夾	• `C:\sample.exe` • `C:\folder\test.doc`	• `D:\sample.exe` • `E:\folder\test.doc`

例外類型	萬用字元用法	相符	不相符
特定資料夾層下的特定檔案	`C:\*\Sample.exe` 僅在 Sample.exe 檔案位於 C:\ 目錄下的任何子資料夾內時才排除此檔案	• C:\files\Sample.exe • C:\temp\files\Sample.exe	• C:\sample.exe
UNC 路徑	`\\<UNC path>\*\Sample.exe` 僅在 Sample.exe 檔案位於指定 UNC 路徑下的任何子資料夾內時才排除此檔案	• \\<UNC path>\files\Sample.exe • \\<UNC path>\temp\files\Sample.exe	• R:\files\Sample.exe 原因：不支援對應磁碟機。 • \\<UNC path>\Sample.exe 原因：檔案並未存在於 UNC 路徑下的子資料夾內。
檔案名稱和副檔名	`C:\*.*` 排除 C:\ 目錄下所有資料夾和子資料夾內具有副檔名的所有檔案	• C:\Sample.exe • C:\temp\Sample.exe • C:\test.doc	• D:\sample.exe • C:\Sample **注意** C:\Sample 沒有副檔名，因此會被排除而不掃瞄。

例外類型	萬用字元用法	相符	不相符
檔案名稱	`C:\*.exe` 排除 C:\ 目錄下所有資料夾和子資料夾內副檔名為 .exe 的所有檔案	• C:\Sample.exe • C:\temp\test.exe	• C:\Sample.doc • C:\temp\test.bat • C:\Sample **注意** C:\Sample 沒有副檔名，因此會被排除而不掃瞄。
副檔名	`C:\Sample.*` 排除 C:\ 目錄下名稱為 Sample（副檔名不限）的檔案。	• C:\Sample.exe	• C:\Sample1.doc • C:\temp\Sample.bat • C:\Sample **注意** C:\Sample 沒有副檔名，因此會被排除而不掃瞄。
特定目錄結構中的檔案	`C:\*\*\Sample.exe` 排除位於 C:\ 目錄下第二層子資料夾或任何更下層子資料夾內所有檔案名稱和副檔名為 Sample.exe 的檔案	• C:\files\temp\Sample.exe • C:\files\temp\test\Sample.exe	• C:\Sample.exe • C:\temp\Sample.exe • C:\files\temp\Sample.doc

例外類型	萬用字元用法	相符	不相符
複雜的路徑或檔案名稱	`C:\Sam*e??.exe` 排除其名稱滿足下列條件的所有檔案： • 以字元 "Sam" 為開頭 • 檔案名稱的倒數第三個字元必須是 "e" • 檔案名稱開頭的 "Sam" 字串與結尾的 "e??" 字串之間必須至少有 1 個字元 • 副檔名之前與檔案名稱中的 "e" 之後必須有正好 2 個字元 • 副檔名是 `.exe` 如果檔案符合所有要求的條件且位於 `C:\` 目錄中，「行為監控」就會排除這些檔案而不掃瞄。	• `C:\Sample12.exe` • `C:\SamSamSample12.exe`	• `C:\SaSmple12.exe` 原因：不是以 "Sam" 為開頭 • `C:\SamSamSam12.exe` 原因：倒數第三個字元不是 "e" • `C:\Same12.exe` 原因：開頭的 "Sam" 字串與倒數第三個字元 "e" 之間未包含任何其他字元 • `C:\Sample1.exe` 原因：副檔名之前與 "e" 之後未包含 2 個字元 • `C:\Sample12.doc` 原因：副檔名不正確

例外清單環境變數支援

下表列出了在新增檔案或資料夾路徑至清單時，您可以使用的環境變數。

環境變數	範例	對等路徑
$allappdata$	$allappdata$\test\sample.exe	C:\ProgramData\test\sample.exe
$allprograms$	$allprograms$\test\sample.exe	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\test\sample.exe

環境變數	範例	對等路徑
$programdir$	$programdir$\test\sample.exe	C:\Program Files\test\sample.exe
$programdirx86$	$programdirx86$\test\sample.exe	C:\Program Files (x86)\test\sample.exe
$rootdir$	$rootdir$\test\sample.exe	C:\test\sample.exe
$systemdir$	$systemdir$\test\sample.exe	C:\Windows\System32\test\sample.exe
$systemdirx86$	$systemdirx86$\test\sample.exe	C:\Windows\SysWOW64\test\sample.exe
$tempdir$	$tempdir$\test\sample.exe	C:\Windows\Temp\test\sample.exe
$userprofile$	$userprofile$\test\sample.exe	C:\user\{current_user_account}\test\sample.exe
$windir$	$windir$\test\sample.exe	C:\Windows\test\sample.exe

設定惡意程式行為封鎖、事件監控和例外清單

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 行為監控設定」。
4. 請點選「規則」標籤。
5. 在「惡意程式行為封鎖」區段中：
   a. 選取「啟動惡意程式行為封鎖」，然後指定要封鎖的安全威脅類型：
      - 已知安全威脅：封鎖與已知惡意程式安全威脅相關聯的行為
      - 已知和潛在安全威脅：封鎖與已知威脅相關聯的行為，並對可能是惡意的行為採取處理行動

b. 選取您要啟用以抵禦勒索軟體安全威脅的勒索軟體防護功能。

- 保護文件以防止未經授權的加密或修改：阻止潛在的勒索軟體安全威脅加密或修改文件內容
  - 自動備份與恢復遭可疑程式變更的檔案：在偵測到勒索軟體安全威脅時，為端點上要加密的檔案建立備份複本，以防任何資料遺失

注意

自動檔案備份需要用戶端端點上至少有 100 MB 的磁碟空間，而且僅會備份大小小於 10 MB 的檔案。

- 封鎖通常與勒索軟體相關的程序：在加密和修改文件之前，封鎖與已知勒索軟體安全威脅相關的處理程序
- 啟動程式檢測，以偵測並封鎖遭到入侵的可執行檔：程式檢測可監控處理程序並執行 API 攔截，以判斷程式是否表現出非預期的行為。雖然此程序可提高對遭到入侵的可執行檔的整體偵測率，卻可能會導致系統效能降低。

秘訣

如果您在「要封鎖的安全威脅」下拉式清單中選取「已知和潛在安全威脅」，程式檢測會提供增強的安全性。

如需詳細資訊，請參閱勒索軟體防護 第 9-3 頁。

c. 在「弱點攻擊防護」下，啟動「如果程式展現出與弱點攻擊有關的異常行為，請將其終止」，以防範可能遭到攻擊的程式。

注意

若要使用「弱點攻擊防護」，您必須選取「啟動程式檢測，以偵測並封鎖遭到入侵的可執行檔」。

如需詳細資訊，請參閱弱點攻擊防護 第 9-4 頁。

6. 在「新發現的程式」區段中，啟動「監控經由 Web 或電子郵件應用程式通道下載之新發現的程式」，然後選取要在執行所下載的程式之前先「提示使用者」，還是讓 Apex One 僅記錄檔偵測。

7. 在「事件監控」區段中：

   a. 選取「啟動事件監控」。

   b. 選擇要監控的系統事件，並針對所選取的每個件選取處理行動。

      如需有關監控的系統事件和處理行動的資訊，請參閱事件監控 第 9-5 頁。

8. 請點選「例外」標籤以設定例外清單。

   a. 在「輸入完整的程式路徑」下，輸入要核可或封鎖的程式完整路徑。

   b. 請點選「新增到例外清單」或「新增到封鎖清單」。

   c. 如果要從清單中移除封鎖的或核可的程式，請點選程式旁的垃圾桶圖示 ( )。

      注意

      Apex One 最多可接受合併總計 1024 個核可的程式和封鎖的程式。

9. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

配置全域行為監控設定

Apex One 會將全域用戶端設定套用到所有用戶端，或者僅套用到具有特定權限的用戶端。

步驟

1. 移至「用戶端 > 全域用戶端設定」。
2. 請點選「安全設定」標籤。
3. 移至「行為監控設定」區段。
4. 視需要對「如果使用者在以下時間內沒有回應，則自動採取處理行動：__ 秒」設定進行設定。

   只有在事件監控已啟動，且監控的系統事件的處理行動是「需要時詢問」時，這個設定才有效。此處理行動會提示使用者允許或拒絕與事件相關聯的程式。如果使用者在特定的時間內未回應，Apex One 會自動允許此程式執行。

   如需詳細資訊，請參閱事件監控 第 9-5 頁。
5. 請點選「系統」標籤。
6. 移至「認證安全防護軟體服務設定」區段，並視需要啟動認證安全防護軟體服務。

   認證安全防護軟體服務會查詢趨勢科技資料中心，確認惡意程式行為封鎖、事件監控、防火牆或防毒掃瞄所偵測到的程式是否安全。啟動「認證安全防護軟體服務」可降低誤判的可能性。

   注意

   啟動認證安全防護軟體服務之前，請確定 Security Agent 具有正確的 Proxy 設定（詳細資訊請參閱 Security Agent Proxy 設定 第 15-42 頁）。Proxy 設定不正確以及網際網路連線不穩定，都可能造成趨勢科技資料中心回應接收延遲或失敗，以致監控程式顯示無回應。

   此外，純 IPv6 Security Agent 無法直接從趨勢科技資料中心進行查詢。如果要使 Security Agent 連線到趨勢科技資料中心，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。
7. 請點選「儲存」。

行為監控權限

如果用戶端具有「行為監控」權限，「行為監控」選項會顯示在 Security Agent 主控台的「設定」畫面中。然後，使用者可以管理自己的例外清單。

圖 9-1. Security Agent 主控台上的「行為監控」選項

授與行為監控權限

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 權限和其他設定」。
4. 在「權限」標籤上，移至「行為監控權限」區段。
5. 選取「在 Security Agent 主控台上顯示「行為監控」設定」。
6. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

Security Agent 使用者的行為監控通知

Apex One 可以在行為監控封鎖某個程式後，立即在 Security Agent 電腦上顯示通知訊息。啟動傳送通知訊息並可選擇修改訊息的內容。

啟用傳送通知訊息

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 權限和其他設定」。
4. 請點選「其他設定」，並移至「行為監控設定」區段。
5. 選取「當程式被封鎖時顯示通知」。
6. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

修改通知訊息內容

步驟

1. 移至「管理 > 通知 > 用戶端」。
2. 從「類型」下拉式清單中，選取「行為監控策略違規」。
3. 在提供的文字方塊中修改預設訊息。
   - 行為監控策略違規：指定當「惡意程式行為封鎖」偵測到策略違規時，使用者收到的訊息。

- 新發現的程式：指定當「行為封鎖」偵測到從 Web 或電子郵件應用程式通道下載了無法辨識的程式時，使用者收到的訊息。

4. 請點選「儲存」。

行為監控記錄檔

Security Agent 可記錄未經授權的程式存取實例，並將記錄檔傳送至伺服器。任何持續運作的 Security Agent 會依指定的時間間隔（預設為每 60 分鐘）彙總一次記錄檔並進行傳送。

如果要避免記錄檔佔去過多硬碟空間，請手動刪除記錄檔或設定記錄檔刪除預約時程。如需有關管理記錄檔的詳細資訊，請參閱記錄檔管理 第 14-39 頁。

檢視行為監控記錄檔

步驟

1. 移至「記錄檔 > 用戶端 > 安全威脅」或「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「記錄檔 > 行為監控記錄檔」或「檢視記錄檔 > 行為監控記錄檔」。
4. 指定記錄條件，然後請點選「顯示記錄檔」。
5. 檢視記錄檔。記錄檔包含下列資訊：
   - 偵測到發生未經授權程序的日期/時間
   - 偵測到發生未經授權程序的端點
   - 端點網域

- 違規：即程序所違反的事件監控規則
- 偵測到違規時執行的處理行動
- 事件：即程式所存取的物件類型
- 未經授權程式的風險等級
- 程式：即未經授權的程式
- 作業：即未經授權的程式所執行的處理行動
- 目標：即所存取的程序
- 安全威脅源自的感染通道

6. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請點選「匯出到 CSV」。開啟檔案或將其儲存至特定位置。

設定行為監控記錄檔傳送預約時程

步驟

1. 存取 <伺服器安裝資料夾>\PCCSRV。
2. 使用記事本等文字編輯器開啟 ofcscan.ini 檔案。
3. 搜尋字串「SendBMLogPeriod」，然後檢查旁邊的值。

   預設值為 3600 秒，而字串會顯示為 SendBMLogPeriod=3600。
4. 指定值（以秒為單位）。

   例如，如果要將記錄檔期間改成 2 小時，請將值改成 7200。
5. 儲存檔案。
6. 移至「用戶端 > 全域用戶端設定」。
7. 請點選「儲存」而不變更任何設定。

8. 重新啟動 用戶端。

第 10 章

使用周邊設備存取控管

本章說明如何使用周邊設備存取控管功能來保護電腦免於受到安全威脅的侵襲。

包含下列主題：

周邊設備存取控管

周邊設備存取控管會規範對連線到電腦的外部儲存裝置與網路資源的存取。周邊設備存取控管有助於防止資料遺失與外洩，並且可與檔案掃瞄搭配使用，以協助防禦安全威脅。

您可以設定內部和外部用戶端的周邊設備存取控管策略。管理員通常會針對外部用戶端設定較嚴格的策略。

策略是 Apex One 用戶端樹狀結構中的精細設定。您可以對用戶端群組或個別用戶端強制執行特定的策略。您也可以對所有用戶端強制執行單一策略。

部署策略之後，用戶端會使用您在「端點位置」畫面（請參閱端點位置 第 15-2 頁）中設定的位置條件來判斷其位置和要套用的策略。用戶端會在每次位置變更時切換策略。

重要

- 依預設，「周邊設備存取控管」在所有版本的 Windows Server 上均是關閉的。在這些伺服器平台上啟動「周邊設備存取控管」之前，請先閱讀 Security Agent 服務 第 15-6 頁中所述的指導方針和最佳做法。
- 如需支援的裝置型號清單，請參閱「資料安全防護清單」文件，網址為：

  http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

---

Apex One 可監控的裝置類型取決於是否已註冊「資料安全防護」使用授權。您必須另行為「資料安全防護」模組取得使用授權，而且必須先啟動此模組才能使用它。如需有關「資料安全防護」使用授權的詳細資訊，請參閱資料安全防護使用授權 第 3-3 頁。

表 10-1. 由未經授權的變更阻止服務監控的裝置

裝置類型	裝置說明
儲存裝置	CD/DVD **重要** 「周邊設備存取控管」只能限制對使用 Live File System 格式的 CD/DVD 錄製裝置的存取。即使啟動「周邊設備存取控管」，使用主圖形格式的部分協力廠商應用程式仍可以執行讀取/寫入作業。請使用資料外洩防護限制對使用任何格式類型的 CD/DVD 錄製裝置的存取。 如需詳細資訊，請參閱封鎖對資料錄製器 (CD/DVD) 的存取 第 11-31 頁。
	軟碟
	網路磁碟機
	USB 儲存裝置

表 10-2. 資料外洩防護監控的裝置

裝置類型	裝置說明
行動裝置	行動裝置
儲存裝置	CD/DVD
	軟碟
	網路磁碟機
	USB 儲存裝置

裝置類型	裝置說明
非儲存裝置	Bluetooth 介面卡
	COM 和 LPT 通訊埠
	IEEE 1394 介面
	影像裝置
	紅外線裝置
	數據機
	PCMCIA 卡
	列印螢幕鍵
	無線 NIC

儲存裝置的權限

當您執行下列動作時會使用儲存裝置的「周邊設備存取控管」權限：

- 允許存取 USB 儲存裝置、CD/DVD、磁片和網路磁碟機。您可以授與對這些裝置的完整存取權，或限制存取等級。
- 設定核可 USB 儲存裝置的清單。「周邊設備存取控管」可讓您封鎖對所有 USB 儲存裝置的存取，但已新增至核可裝置清單的 USB 儲存裝置除外。您可以授與對核可裝置的完整存取權，或限制存取等級。

以下表格列出了儲存裝置的權限。

表 10-3. 儲存裝置的周邊設備存取控管權限

權限	裝置上的檔案	輸入的檔案
完整存取權	允許的作業：複製、移動、開啟、儲存、刪除、執行	允許的作業：儲存、移動、複製 這表示檔案可以儲存、移動與複製到裝置上。

權限	裝置上的檔案	輸入的檔案
修改	允許的作業：複製、移動、開啟、儲存、刪除 禁止的作業：執行	允許的作業：儲存、移動、複製
讀取和執行	允許的作業：複製、開啟、執行 允許的作業：儲存、移動、刪除	禁止的作業：儲存、移動、複製
讀取	允許的作業：複製、開啟 禁止的作業：儲存、移動、刪除、執行	禁止的作業：儲存、移動、複製
僅列出裝置內容	禁止的作業：所有作業 向使用者顯示裝置與其包含的檔案（例如，從 Windows 檔案總管）。	禁止的作業：儲存、移動、複製
封鎖 （安裝資料安全防護後即可使用）	禁止的作業：所有作業 不向使用者顯示裝置與其包含的檔案（例如，從 Windows 檔案總管）。	禁止的作業：儲存、移動、複製

檔案型掃瞄可彌補裝置權限之不足，甚至加以覆寫。例如，如果權限允許開啟檔案，但 Security Agent 偵測到檔案已感染惡意程式，則會對該檔案執行特定的中毒處理行動，以消除惡意程式。如果中毒處理行動為「清除」，檔案將會在清除後開啟。但是，如果中毒處理行動為「刪除」，則會刪除檔案。

秘訣

資料安全防護的周邊設備存取控管功能支援所有的 64 位元平台。如果要在 Security Agent 不支援的系統上監控未經授權的變更阻止，請將裝置權限設定為「封鎖」，以限制這些裝置的存取權。

儲存裝置的進階權限

進階權限適用於已授與有限的權限給大部分儲存裝置的情況。權限可以是下列任一種：

- 修改
- 讀取和執行
- 讀取
- 僅列出裝置內容

您可以繼續維持受限的權限，但將進階權限授與儲存裝置和本機端點上的某些程式。

如果要定義程式，請設定下列程式清單。

表 10-4. 程式清單

程式清單	說明	有效的輸入
對裝置具有讀取與寫入權限的程式	此清單包含的本機程式和儲存裝置上的程式，對裝置具有讀取和寫入權限。 Microsoft Word (`winword.exe`) 是本機程式的範例，它通常位於 `C:\Program Files\Microsoft Office\Office`。如果 USB 儲存裝置的權限是「僅列出裝置內容」，但在此清單中包含 `C:\Program Files\Microsoft Office\Office\winword.exe`： • 使用者將具有從 Microsoft Word 存取之 USB 儲存裝置上所有檔案的讀取和寫入權限。 • 使用者可以儲存、移動或複製 Microsoft Word 檔案到 USB 儲存裝置。	程式路徑和名稱 如需詳細資訊，請參閱周邊設備存取控管允許的程式清單的萬用字元支援 第 10-8 頁。
裝置上允許執行的程式	此清單包含使用者或系統可以在儲存裝置上執行的程式。 例如，如果您要允許使用者從 CD 安裝軟體，請將安裝程式路徑和名稱（例如 `E:\Installer\Setup.exe`）新增到此單。	程式路徑和名稱或數位簽章提供者 如需詳細資訊，請參閱周邊設備存取控管允許的程式清單的萬用字元支援 第 10-8 頁或指定數位簽章提供者 第 10-8 頁。

以下是當您需要新增程式到這兩種清單時的建議。考慮使用 USB 儲存裝置的資料鎖定功能，啟動此功能後，會提示使用者輸入有效的使用者名稱和密碼才能

解除鎖定裝置。資料鎖定功能使用裝置上名為 Password.exe 的程式，必須允許此程式執行，使用者才能成功解除鎖定裝置。"Password.exe 也必須具有裝置的讀取和寫入權限，使用者才能變更使用者名稱或密碼。

使用者介面的每個程式清單可容納多達 100 個程式。

如果您要新增更多程式到程式清單，請新增至 ofcscan.ini 檔案，該檔案可容納多達 1,000 個程式。如需新增程式到 ofcscan.ini 檔案的指示，請參閱「使用 ofcscan.ini 將程式新增到周邊設備存取控管程式清單 第 10-15 頁」。

警告!

新增到 ofcscan.ini 檔案的程式會部署至根網域，並且會覆寫個別網域和用戶端上的程式。

指定數位簽章提供者

指定您所信任由其發行之程式的數位簽章提供者。例如，輸入 Microsoft Corporation 或 趨勢科技, Inc.。您可以透過檢查程式的內容（例如，在程式上請點選滑鼠右鍵並選取「內容」）來取得數位簽章提供者。

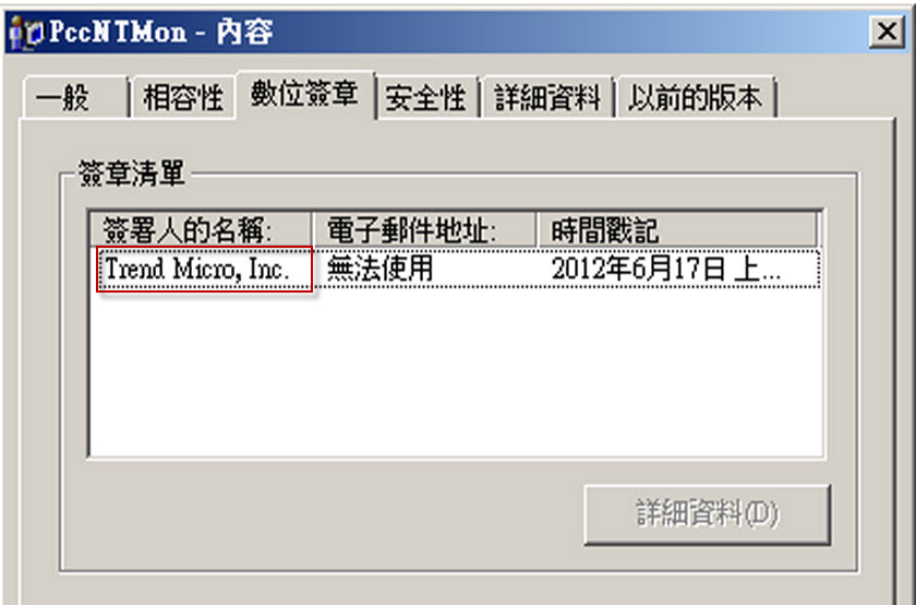


圖 10-1. Security Agent 程式 (PccNTMon.exe) 的數位簽章提供者

周邊設備存取控管允許的程式清單的萬用字元支援

程式路徑和名稱的長度上限為 259 個字元，並且只能包含英數字元 (A-Z、a-z、0-9)。您不能只指定程式名稱。

您可以使用萬用字元取代磁碟機代號和程式名稱。使用問號 (?) 代表單一字元資料（例如：磁碟機代號）。使用星號 (*) 代表多字元資料（例如：程式名稱）。

注意

您不能使用萬用字元代表資料夾名稱。必須指定資料夾的確實名稱。

下列是正確使用萬用字元的範例：

表 10-5. 正確的萬用字元用法

範例	符合的資料
?:\Password.exe	位於任何磁碟機正下方的「Password.exe」檔案
C:\Program Files\Microsoft*.exe	C:\Program Files 中所有具有副檔名的檔案
C:\Program Files*.*	C:\Program Files 中所有具有副檔名的檔案
C:\Program Files\a?c.exe	位於 C:\Program Files 中，具有 3 個字元且開頭為字母「a」，結尾為字母「c」的任何 .exe 檔案
C:*	位於 C:\ 磁碟機根目錄的所有檔案（含或不含副檔名）

下列是不正確使用萬用字元的範例：

表 10-6. 不正確的萬用字元用法

範例	原因
??:\Buffalo\Password.exe	?? 代表兩個字元，但磁碟機代號只能有一個字母字元。
*:\Buffalo\Password.exe	* 代表多字元資料，但磁碟機代號只能有一個字母字元。
C:*\Password.exe	您不能使用萬用字元代表資料夾名稱。必須指定資料夾的確實名稱。
C:\?\Password.exe	

非儲存裝置的權限

您可以允許或封鎖對非儲存裝置的存取。這些裝置沒有細微或進階權限。

管理對外部裝置的存取（已啟動資料安全防護）

步驟

1. 瀏覽至 用戶端 > 用戶端管理。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 周邊設備存取控管設定」。
4. 請點選「外部用戶端」標籤以設定外部用戶端的設定，或請點選「內部用戶端」標籤以設定內部用戶端的設定。
5. 選取「啟動周邊設備存取控管」。
6. 如下所示套用設定：
   - 如果您使用的是「外部用戶端」標籤，則可以透過選取「套用所有設定至內部用戶端」將設定套用至內部用戶端。
   - 如果您使用的是「內部用戶端」標籤，則可以透過選取「套用所有設定至外部用戶端」將設定套用至外部用戶端。

   接著會出現確認訊息。等待部署命令傳播到所有用戶端。
7. 選擇允許或封鎖 USB 儲存裝置的自動執行功能 (`autorun.inf`)。
8. 針對儲存裝置設定相關選項。
   a. 為每個儲存裝置選取權限。

      如需有關權限的詳細資訊，請參閱儲存裝置的權限 第 10-4 頁。

   b. 如果 USB 儲存裝置的權限是「封鎖」，請設定核可裝置的清單。使用者可以存取這些裝置，而您可以使用權限來控制存取等級。

      請參閱設定 USB 裝置核可清單 第 10-12 頁。
9. 針對每個非儲存裝置，選取「允許」或「封鎖」。

10. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

    - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
    - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

設定進階權限

雖然您可以設定使用者介面上特定儲存裝置的進階權限與通知，但權限與通知實際上會套用至所有儲存裝置。這表示當您請點選 CD/DVD 的「進階權限與通知」時，實際上是定義所有儲存裝置的權限與通知。

注意

如需有關進階權限以及如何正確使用進階權限定義程式的詳細資訊，請參閱儲存裝置的進階權限 第 10-5 頁。

步驟

1. 請點選「進階權限與通知」。

   接著會開啟一個新畫面。

2. 在「對儲存裝置具有讀取和寫入權限的程式」下方，輸入程式路徑和檔案名稱，然後請點選「新增」。

   不接受數位簽章提供者。

3. 在「儲存裝置上允許執行的程式」下方，輸入程式路徑和名稱或數位簽章提供者，然後請點選「新增」。

4. 選取當 Apex One 偵測到未經授權的裝置存取時，會在端點上顯示通知訊息。

- 未經授權的裝置存取是指禁止的裝置作業。例如，如果裝置權限是「讀取」，使用者就無法在裝置上儲存、移動、刪除或執行檔案。
- 您可以修改通知訊息。如需詳細資訊，請參閱修改周邊設備存取控管通知 第 10-16 頁。

5. 請點選返回。

設定 USB 裝置核可清單

USB 裝置的核可清單支援使用星號 (*) 萬用字元。以星號 (*) 取代任何欄位，以包含符合其他欄位要求的所有裝置。例如，[vendor]-[model]-* 會將指定廠商和指定型號類型的所有 USB 裝置置於核可清單中，而不論序號 ID 為何。

步驟

1. 請點選「核可的裝置」。
2. 輸入裝置廠商。
3. 輸入裝置型號和序號 ID。

> **秘訣**
>
> 使用「裝置清單工具」查詢連接至端點的裝置。此工具可以提供每個裝置的裝置廠商、型號和序號 ID。

4. 為裝置選取權限。

   如需有關權限的詳細資訊，請參閱儲存裝置的權限 第 10-4 頁。

5. 如果要新增更多裝置，請點選加號 (+) 圖示。
6. 請點選 < 返回。

裝置清單工具

在每個本機端點上執行「裝置清單工具」可查詢連接到端點的外部裝置。此工具會掃瞄端點是否連接外部裝置，然後在瀏覽器視窗中顯示裝置資訊。接著，您可以在設定「資料外洩防護」 和「周邊設備存取控管」的裝置設定時使用這些資訊。

如果要執行「裝置清單工具」

步驟

1. 找到「裝置清單工具」。
   - 在 Apex One 伺服器電腦上，移至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\ListDeviceInfo。
   - 在已安裝 Security Agent 的目標端點上，移至 C:\Windows\System32\dgagent\listDeviceInfo.exe。
   - 從支援入口網站取得 listDeviceInfo.zip，並在目標端點上解壓縮此套件。

     https://success.trendmicro.com/solution/1120385
2. 將 listDeviceInfo.exe 複製到目標端點。
3. 在端點上，執行 listDeviceInfo.exe。
4. 在顯示的瀏覽器視窗中檢視裝置資訊。「資料外洩防護」和「周邊設備存取控管」使用下列資訊：
   - 廠商（必要）
   - 型號（選用）
   - 序號 ID（選用）

管理對外部裝置的存取（未啟動資料安全防護）

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 周邊設備存取控管設定」。
4. 請點選「外部用戶端」標籤以設定外部用戶端的設定，或請點選「內部用戶端」標籤以設定內部用戶端的設定。
5. 選取「啟動周邊設備存取控管」。
6. 如下所示套用設定：
   - 如果您使用的是「外部用戶端」標籤，則可以透過選取「套用所有設定至內部用戶端」將設定套用至內部用戶端。
   - 如果您使用的是「內部用戶端」標籤，則可以透過選取「套用所有設定至外部用戶端」將設定套用至外部用戶端。

   接著會出現確認訊息。等待部署命令傳播到所有用戶端。
7. 選擇允許或封鎖 USB 儲存裝置的自動執行功能 (`autorun.inf`)。
8. 為每個儲存裝置選取權限。
9. 如果儲存裝置的權限是下列任一種，請設定進階權限與通知：「修改」、「讀取和執行」、「讀取」或「僅列出裝置內容」。

   請參閱設定進階權限 第 10-11 頁。
10. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
    - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。

- 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

使用 ofcscan.ini 新增程式到周邊設備存取控管清單

注意

如需關於程式清單以及如何正確定義可新增至清單的程式的詳細資訊，請參閱儲存裝置的進階權限 第 10-5 頁。

步驟

1. 在 Apex One 伺服器電腦上，移至 <伺服器安裝資料夾>\PCCSRV。
2. 使用文字編輯器開啟 ofcscan.ini。
3. 如果要新增對儲存裝置具有讀取和寫入權限的程式：
   a. 找到下列各行：

      ```
      [DAC_APPROVED_LIST]
      Count=x
      ```

   b. 請將「x」換成程式清單中的程式數量。
   c. 在「Count=x」下方，輸入下列命令來新增程式：

      ```
      Item<號碼>=<程式路徑和名稱或數位簽章提供者>
      ```

      例如：

      ```
      [DAC_APPROVED_LIST]
      Count=3
      Item0=C:\Program Files\program.exe
      Item1=?:\password.exe
      Item2=Microsoft Corporation
      ```

4. 如果要新增儲存裝置上允許執行的程式：
   a. 找到下列各行：

      ```
      [DAC_EXECUTABLE_LIST]
      Count=x
      ```

   b. 請將「x」換成程式清單中的程式數量。
   c. 在「Count=x」下方，輸入下列命令來新增程式：

      ```
      Item<號碼>=<程式路徑和名稱或數位簽章提供者>
      ```

      例如：

      ```
      [DAC_EXECUTABLE_LIST]
      Count=3
      Item0=?:\Installer\Setup.exe
      Item1=E:\*.exe
      Item2=Trend Micro, Inc.
      ```

5. 儲存並關閉 `ofcscan.ini` 檔案。
6. 開啟 Apex One Web 主控台，並移至用戶端 > 全域用戶端設定。
7. 請點選「儲存」，將程式清單部署至所有用戶端。

修改周邊設備存取控管通知

發生「周邊設備存取控管」違規事件時，端點上會顯示通知訊息。管理員可視需要修改預設通知訊息。

步驟

1. 移至「管理 > 通知 > 用戶端」。

2. 從「類型」下拉式清單中，選取「周邊設備存取控管違規」。
3. 在提供的文字方塊中修改預設訊息。
4. 請點選「儲存」。

周邊設備存取控管記錄檔

Security Agent 可記錄未經授權的裝置存取案例，並將記錄檔傳送至伺服器。持續運作的用戶端會每 1 小時彙整記錄檔並進行傳送。重新啟動後的用戶端會檢查記錄檔上次傳送至伺服器的時間。如果經過的時間超過 1 小時，則用戶端會立即傳送記錄檔。

如果要避免記錄檔佔去過多硬碟空間，請手動刪除記錄檔或設定記錄檔刪除預約時程。如需有關管理記錄檔的詳細資訊，請參閱記錄檔管理 第 14-39 頁。

檢視周邊設備存取控管記錄檔

注意

只有嘗試存取「儲存裝置」會產生記錄檔資料。Security Agent 會按照設定封鎖或允許存取「非儲存裝置」，但不會記錄處理行動。

步驟

1. 移至「記錄檔 > 用戶端 > 安全威脅」或「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「記錄檔 > 周邊設備存取控管記錄檔」或「檢視記錄檔 > 周邊設備存取控管記錄檔」。
4. 指定記錄條件，然後請點選「顯示記錄檔」。

5. 檢視記錄檔。記錄檔包含下列資訊：
   - 偵測到發生未經授權存取的日期/時間
   - 外部裝置所連線或網路資源所對應的端點
   - 外部裝置所連線或網路資源所對應的端點
   - 存取的裝置類型或網路資源
   - 目標，即存取的裝置或網路資源上的項目
   - 存取者，可指定開始存取的位置
   - 為目標設定的權限
6. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請點選「匯出到 CSV」。開啟檔案或將其儲存至特定位置。

第 11 章

使用資料外洩防護

本章討論如何使用資料外洩防護功能。

包含下列主題：

資料外洩防護 (DLP)

傳統的安全解決方案著重於防止外部安全威脅入侵網路。在現今的安全環境中，這麼做卻只能有一半的效果。資料遭到侵害的情況相當普遍，這會將組織的機密與敏感資料（稱為數位資產）暴露給外部未經授權的人員。資料遭到侵害可能是因為內部員工出錯或大意、資料外包、電腦設備遭竊或隨意放置、或惡意的攻擊所造成的。

資料外洩會導致：

- 品牌商譽受損
- 客戶對公司的信任度降低
- 為了進行補救措施而投入不必要的成本，以及因不遵守法規而須支付罰金
- 因智慧財產被盜，錯失商機和收益

隨著資料外洩情況越來越普遍以及因此而帶來的損害，許多公司現在都將數位資產保護視為安全措施的關鍵要素。

「資料外洩防護」可保護組織的機密資料，免遭受意外或有意的外洩。資料外洩防護允許您：

- 使用資料識別碼識別需要保護的機密資訊
- 建立策略，以限制或防止透過常見傳輸通道（例如：電子郵件和外部裝置）傳輸數位資產
- 強制遵守制定的隱私權標準

您必須能夠回答下列問題，才能監控可能損失的機密資訊：

- 必須保護哪些資料以防止未經授權的使用者存取？
- 機密資料儲存於何處？
- 機密資料的傳輸方式為何？
- 哪些使用者具有存取或傳輸機密資料的授權？
- 發生安全違規時應採取哪些處理行動？

這項重要的監看通常涉及組織中經常接觸機密資訊的多個部門及個人。

如果您已經定義您的機密資訊與安全策略，則可以開始定義資料識別碼和公司策略。

資料外洩防護策略

Apex One 會根據「DLP 策略」中定義的一組規則來評估檔案或資料。策略會決定需要保護以防止未經授權傳輸的檔案或資料，以及 Apex One 在偵測到傳輸活動後所執行的處理行動。

注意

Apex One 不會監控伺服器和 Security Agent 之間的資料傳輸。

Apex One 可讓管理員設定內部和外部 Security Agent 的策略。管理員通常會針對外部用戶端設定較嚴格的策略。

管理員可以對用戶端群組或個別用戶端強制執行特定的策略。

部署策略後，用戶端會使用「端點位置」畫面中設定的位置條件（請參閱端點位置 第 15-2 頁）來確定正確的位置設定和要套用的策略。用戶端會在每次位置發生變更時切換策略。

策略組態設定

透過進行下列設定並將設定部署到所選取的用戶端，來定義 DLP 策略：

表 11-1. 定義「DLP 策略」的設定

設定	說明
規則	一個 DLP 規則可包含多個範本、通道和處理行動。每一項規則都是上層 DLP 策略的子集。 注意 資料外洩防護會按優先順序處理規則和範本。如果規則設定為「"暫不處理"」，資料外洩防護會處理清單中的下一個規則。如果規則設定為「封鎖」或「使用者理由」，資料外洩防護會封鎖或接受使用者處理行動，不會進一步處理該規則/範本。
範本	DLP 範本結合資料識別碼和邏輯運算子（And、Or、Except）構成條件陳述式。只有滿足特定條件陳述式的檔案或資料才受到 DLP 規則的規範。 資料外洩防護隨附一組已預先定義的範本，而且可讓管理員建立自訂範本。 DLP 規則可包含一個或數個範本。資料外洩防護檢查範本時會使用最先符合 (First-match) 規則。這表示，如果檔案或資料符合某一個範本中的資料識別碼，資料外洩防護就不會再繼續檢查其他範本。
通道	通道是傳輸敏感資訊的實體。資料外洩防護支援常見的傳輸通道，像是電子郵件、卸除式儲存裝置，以及即時通訊應用程式。
處理行動	當資料外洩防護偵測到嘗試透過任一通道傳輸機密資訊的動作時，它會執行一或多個處理行動。
例外	例外用於覆寫所配置的 DLP 規則。設定例外可管理不受監控的目標、受監控的目標以及壓縮檔案的掃瞄。
資料識別碼	資料外洩防護使用資料識別碼來識別機密資訊。資料識別碼包括運算式、檔案屬性和關鍵字，這些會用作建立 DLP 範本的基礎。

資料識別碼類型

數位資產是組織必須保護以防止未經授權傳輸的檔案和資料。管理員可以透過下列資料識別碼定義數位資產：

- 表示式：具有特定結構的資料。

  如需詳細資訊，請參閱表示式 第 11-5 頁。

- 檔案屬性：檔案類型和檔案大小等檔案內容。

  如需詳細資訊，請參閱檔案屬性 第 11-10 頁。

- 關鍵字清單：特殊字詞或字組的清單。

  如需詳細資訊，請參閱關鍵字 第 11-12 頁。

注意

管理員無法刪除 DLP 範本正在使用的資料識別碼。請先刪除範本，再刪除資料識別碼。

表示式

表示式是具有特定結構的資料。例如，信用卡號碼通常有 16 位數字，而且其格式為 "nnnn-nnnn-nnnn-nnnn"，因此很適合透過表示式來偵測。

管理員可以使用已預先定義的表示式和自訂表示式。

如需詳細資訊，請參閱預先定義的表示式 第 11-5 頁和自訂表示式 第 11-6 頁。

預先定義的表示式

資料外洩防護隨附一組預先定義的表示式。您無法修改或刪除這些表示式。

資料外洩防護會使用病毒碼比對和數學方程式來驗證這些表示式。資料外洩防護將可能的機密資料與表示式進行比對之後，可能還會對資料進行其他的驗證檢查。

如需完整的預先定義表示式清單，請參閱「資料安全防護清單」文件，網址為：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx。

檢視預先定義的表示式設定

注意

預先定義的表示式無法修改或刪除。

步驟

1. 移至「用戶端 > 資料外洩防護 > 資料識別碼」。
2. 請點選「表示式」標籤。
3. 請點選某個表示式名稱。
4. 在開啟的畫面中檢視設定。

自訂表示式

如果預先定義的表示式均不符合公司的需求，您可以建立自訂表示式。

表示式是功能強大的字串比對工具。建立表示式之前，請熟悉表示式語法。設計不良的表示式會嚴重影響效能。

建立表示式時：

- 請參閱預先定義的表示式，瞭解如何定義有效的表示式。例如，如果要建立包含日期的表示式，請參閱以「Date」為字首的表示式。
- 請注意，資料外洩防護遵循 Perl Compatible Regular Expressions (PCRE) 中定義的表示式格式。如需 PCRE 的詳細資訊，請造訪下列網站：

  http://www.pcre.org/
- 從簡單的表示式開始。如果表示式造成誤判，請予以修改；您也可以微調表示式以提高偵測的正確性。

建立表示式時，管理員有數種條件可供選擇。表示式必須符合選擇的條件，資料外洩防護才能將它套用到 DLP 策略。如需有關不同條件選項的詳細資訊，請參閱自訂表示式的條件 第 11-7 頁。

自訂表示式的條件

表 11-2. 自訂表示式的條件選項

條件	規則	範例
無	無	全部 — 來自「美國戶口普查局」的姓名 • 表示式：[^\w]([A-Z][a-z]{1,12}(\s?,\s?|[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]
特定字元	表示式必須包含您指定的字元。 此外，表示式中的字元數目必須介於下限到上限之間。	美國 — 美國銀行轉帳號碼 • 表示式：[^\d]([0123678]\d{8})[^\d] • 字元：0123456789 • 字元數目下限：9 • 字元數目上限：9
字尾	字尾是指表示式的最後部分。字尾必須包含您指定的字元並包含特定數目的字元。 此外，表示式中的字元數目必須介於下限到上限之間。	全部 — 住家地址 • 表示式：\D(\d+\s[a-z.]+\s([a-z]+\s){0,2} (lane|ln|street|st|avenue|ave|road|rd|place|pl|drive|dr|circle| cr|court|ct|boulevard|blvd)\.?[0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\ s\d{5}(-\d{4})?)[^\d-] • 字尾字元：0123456789- • 字元數目：5 • 表示式中的字元數目下限：25 • 表示式中的字元數目上限：80

條件	規則	範例
單一字元分隔符號	表示式必須要有兩個部分並用一個字元分隔。這個字元的長度必須是 1 個位元組。 此外，分隔符號左邊的字元數目必須介於下限到上限之間。分隔符號右邊的字元數目不能超過上限。	全部 — 電子郵件信箱 • 表示式：[^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] • 分隔符號：@ • 左邊字元數目下限：3 • 左邊字元數目上限：15 • 右邊字元數目上限：30

建立自訂表示式

步驟

1. 移至「用戶端 > 資料外洩防護 > 資料識別碼」。
2. 請點選「表示式」標籤。
3. 請點選「新增」。

   接著會顯示一個新畫面。
4. 輸入表示式的名稱。名稱的長度不能超過 100 個位元組，而且不能包含下列字元：

   • > < * ^ | & ? \ /
5. 請輸入長度不超過 256 個位元組的說明。
6. 輸入顯示的資料。

   例如，如果要建立識別碼的表示式，請輸入範例識別碼。此資料僅供參考，而且不會顯示在產品的任何地方。
7. 選擇下列其中一個條件，並為選擇的條件配置其他設定（請參閱自訂表示式的條件 第 11-7 頁）：

- 無
- 特定字元
- 字尾
- 單一字元分隔符號

8. 針對實際資料測試表示式。

   例如，如果表示式會評估國碼，請在「測試資料」文字方塊中輸入有效的識別碼，請點選「測試」，然後檢查結果。

9. 如果您對結果感到滿意，請點選「儲存」。

注意

只在測試成功時才儲存設定。無法偵測到任何資料的表示式會浪費系統資源，而且可能會影響效能。

10. 接著會出現一則訊息，提醒您將此設定部署到用戶端。請點選「關閉」。
11. 返回「DLP 資料識別碼」畫面，並請點選「套用至所有用戶端」。

匯入自訂表示式

如果您有包含表示式且格式正確的 .dat 檔案，請使用此選項。您可以從目前正在存取的伺服器或其他伺服器匯出表示式，來產生該檔案。

步驟

1. 移至「用戶端 > 資料外洩防護 > 資料識別碼」。
2. 請點選「表示式」標籤。
3. 請點選「匯入」，然後尋找包含表示式的 .dat 檔案。
4. 請點選「開啟」。

   隨即顯示訊息，通知您是否匯入成功。如果要匯入的表示式已存在，系統將會略過該表示式。

5. 請點選「套用至所有用戶端」。

檔案屬性

檔案屬性是檔案的特定內容。定義資料識別碼時，您可以使用兩種檔案屬性，亦即檔案類型和檔案大小。例如，某個軟體開發公司可能想要限制只能與研發部門（其成員負責開發和測試該軟體）共用該公司的軟體安裝程式。在此案例中，Apex One 管理員可以建立一個策略，禁止將大小為 10 到 40 MB 的可執行檔案傳輸到 RD 以外的所有部門。

對於機密檔案而言，單獨使用檔案屬性不是很可靠。承上例，這樣可能也會封鎖其他部門共用的協力廠商軟體安裝程式。因此，趨勢科技建議您將檔案屬性與其他 DLP 資料識別碼結合，以便提高偵測機密檔案的正確性。

如需完整的支援檔案類型清單，請參閱「資料安全防護清單」文件，網址為：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx。

預先定義的檔案屬性清單

資料外洩防護隨附一個預先定義的檔案屬性清單。您無法修改或刪除此清單。此清單有自己的內建條件，可判斷該範本是否會觸發策略違規。

可使用預先定義的檔案屬性清單限制對資料錄製器 (CD/DVD) 的存取。

如需詳細資訊，請參閱封鎖對資料錄製器 (CD/DVD) 的存取 第 11-31 頁。

建立檔案屬性清單

步驟

1. 移至「用戶端 > 資料外洩防護 > 資料識別碼」。
2. 請點選「檔案屬性」標籤。

3. 請點選「新增」。

   接著會顯示一個新畫面。

4. 輸入檔案屬性清單的名稱。名稱的長度不能超過 100 個位元組，而且不能包含下列字元：

   - > < * ^ | & ? \ /

5. 請輸入長度不超過 256 個位元組的說明。

6. 選取您偏好的真實檔案類型。

7. 如果您要包含的檔案類型並未列出，請選取「副檔名」，然後輸入檔案類型的副檔名。資料外洩防護會檢查具有指定副檔名的檔案，而不會檢查其真實檔案類型。指定副檔名的指導方針：

   - 每個副檔名必須以星號 (*) 為開頭，後接句點 (.)，然後是副檔名。星號是萬用字元，代表檔案的實際名稱。例如，`*.pol` 的相符項目有 `12345.pol` 和 `test.pol`。
   - 您可以在副檔名包含萬用字元。使用問號 (?) 代表單一字元，星號 (*) 代表兩個以上字元。請參閱下列範例：

     - `*.*m` 的相符項目有下列檔案：`ABC.dem`、`ABC.prm`、`ABC.sdcm`

     - `*.m*r` 的相符項目有下列檔案：`ABC.mgdr`、`ABC.mtp2r`、`ABC.mdmr`

     - `*.fm?` 的相符項目有下列檔案：`ABC.fme`、`ABC.fml`、`ABC.fmp`

   - 在副檔名的結尾加上星號時請務必小心，因為這可能會與部分檔案名稱及不相關的副檔名相符。例如：`*.do*` 的相符項目有 `abc.doctor_john.jpg` 和 `abc.donor12.pdf`。
   - 請使用分號 (;) 來分隔副檔名。分號後面不用加上空格。

8. 輸入檔案大小下限和上限（以位元組為單位）。這兩個檔案大小值必須是大於零的正整數。

9. 請點選「儲存」。

10. 接著會出現一則訊息，提醒您將此設定部署到用戶端。請點選「關閉」。

11. 返回「DLP 資料識別碼」畫面，並請點選「套用至所有用戶端」。

匯入檔案屬性清單

如果您有包含檔案屬性清單且格式正確的 .dat 檔案，請使用此選項。您可以從目前正在存取的伺服器或其他伺服器匯出檔案屬性清單，來產生該檔案。

步驟

1. 移至「用戶端 > 資料外洩防護 > 資料識別碼」。
2. 請點選「檔案屬性」標籤。
3. 請點選「匯入」，然後尋找包含檔案屬性清單的 .dat 檔案。
4. 請點選「開啟」。

   隨即顯示訊息，通知您是否匯入成功。如果要匯入的檔案屬性清單已存在，系統將會略過該清單。
5. 請點選「套用至所有用戶端」。

關鍵字

關鍵字是特殊字詞或字組。您可以將相關關鍵字新增到關鍵字清單，以識別特定資料類型。例如，「診斷」、「血型」、「接種」和「醫師」是可能出現在診斷書中的關鍵字。如果要防止傳輸診斷書檔案，您可以在 DLP 策略中使用這些關鍵字，然後將資料外洩防護設定為封鎖包含這些關鍵字的檔案。

您可以結合常用字詞以構成有意義的關鍵字。例如，您可以結合 "end"、"read"、"if" 和 "at"，以構成可在原始碼中找到的關鍵字（例如："END-IF"、"END-READ" 和 "AT END"）。

您可以使用已預先定義的關鍵字清單或自訂關鍵字清單。如需詳細資訊，請參閱預先定義的關鍵字清單 第 11-13 頁和自訂關鍵字清單 第 11-14 頁。

預先定義的關鍵字清單

資料外洩防護隨附一組預先定義的關鍵字清單。您無法修改或刪除這些關鍵字清單。每個清單都有自己的內建條件，可判斷該範本是否會觸發策略違規。

如需資料外洩防護中預先定義關鍵字清單的詳細資訊，請參閱「資料安全防護清單」文件，網址為：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

關鍵字清單的運作方式

關鍵字條件的數目

每個關鍵字清單都包含一個條件，要求文件中必須有特定數目的關鍵字，清單才可觸發違規。

關鍵字數目條件包含下列值：

- 所有：清單中的關鍵字都必須出現在文件中。
- 任何：清單中的任一關鍵字必須出現在文件中。
- 特定數目：文件中至少要有指定數目的關鍵字。如果文件中的關鍵字數目比指定的數目多，則資料外洩防護會觸發違規。

距離條件

某些清單會包含「距離」條件以判定是否有違規情形。「距離」指的是某關鍵字的第一個字元和另一個關鍵的第一個字元之間的字元數。請考慮下列項目：

First Name:_John_ Last Name:_Smith_

此表單 — 名字、姓氏清單包含「距離」條件：五十 (50)，以及常用的表單欄位：「名字」和「姓氏」。以上述的範例而言，當「First Name」的「F」和「Last Name」的「L」之間的字元數為十八 (18) 時，資料外洩防護即會觸發違規。

對於不會觸發違規的項目範例，請考慮以下幾點：

The first name of our new employee from Switzerland is John. His last name is Smith.

在此範例中，「first name」的「f」和「last name」的「l」之間的字元數為六十一 (61)。已超過距離的門檻值，所以不會觸發違規。

自訂關鍵字清單

如果預先定義的關鍵字清單不符合您的需求，您可以建立自訂關鍵字清單。

設定關鍵字清單時，您可以選擇數種條件。關鍵字清單必須符合您選擇的條件，資料外洩防護才能將它套用到策略。為每個關鍵字清單選擇下列其中一個條件：

- 任何關鍵字
- 所有關鍵字
- 在 <x> 個字元內的所有關鍵字
- 關鍵字的結合評分超過門檻值

如需有關條件規則的詳細資訊，請參閱自訂關鍵字清單條件 第 11-14 頁。

自訂關鍵字清單條件

表 11-3. 關鍵字清單的條件

條件	規則
任何關鍵字	檔案至少必須包含關鍵字清單中的一個關鍵字。
所有關鍵字	檔案必須包含關鍵字清單中的所有關鍵字。

條件	規則
在 <x> 個字元內的所有關鍵字	檔案必須包含關鍵字清單中的所有關鍵字。此外，每個關鍵字組都必須在各自的 <x> 個字元內。 例如，您的 3 個關鍵字是 WEB、DISK 和 USB，而您指定的字元數是 20。 如果資料外洩防護依 DISK、WEB 和 USB 的順序偵測到所有這些關鍵字，則從「D」（在 DISK 中）到「W」（在 WEB 中）還有從「W」到「U」（在 USB 中），都最多只能相隔 20 個字元。 下列資料符合此條件：DISK####WEB############USB 下列資料不符合此條件：DISK******************WEB****USB（從「D」到「W」相隔 23 個字元） 決定字元數時請記住，此數字越小（例如 10）通常掃瞄時間就越短，但涵蓋的區域也相對較小。這可能會使得偵測到敏感資料的可能性降低，特別是對於大型檔案。此數字越大，涵蓋的區域也越大，但是掃瞄時間可能會比較長。
關鍵字的結合評分超過門檻值	檔案必須包含關鍵字清單中的一或多個關鍵字。如果只偵測到一個關鍵字，其評分必須高於門檻值。如果有多個關鍵字，其結合評分必須高於門檻值。 請為每個關鍵字指定介於 1 到 10 之間的評分。您應該為機密性較高的的字組或詞組（例如：對於人力資源部門的「調薪」）指定較高的評分。對於本身沒有太高權重的字組或詞組，則可以指定較低的評分。 設定門檻值時，請考慮您為關鍵字指定的評分。例如，如果您有五個關鍵字，而其中有三個關鍵字具有高優先順序，則門檻值可以等於或小於那三個高優先順序關鍵字的結合評分。這表示偵測到這三個關鍵字時就可以將該檔案視為機密檔案。

建立關鍵字清單

步驟

1. 移至「用戶端 > 資料外洩防護 > 資料識別碼」。
2. 請點選「關鍵字」標籤。
3. 請點選「新增」。

   接著會顯示一個新畫面。

4. 輸入關鍵字清單的名稱。名稱的長度不能超過 100 個位元組，而且不能包含下列字元：

   - > < * ^ | & ? \ /

5. 請輸入長度不超過 256 個位元組的說明。

6. 選擇下列其中一個條件，並為選擇的條件設定其他設定：

   - 任何關鍵字
   - 所有關鍵字
   - 在 <x> 個字元內的所有關鍵字
   - 關鍵字的結合評分超過門檻值

7. 手動將關鍵字新增到清單中：

   a. 輸入長度介於 3 到 40 個位元組之間的關鍵字，並指定是否區分大小寫。

   b. 請點選「新增」。

8. 如果要使用「匯入」選項來新增關鍵字：

   注意

   如果您有包含關鍵字且格式正確的 .csv 檔案，請使用此選項。您可以從目前正在存取的伺服器或其他伺服器匯出關鍵字，來產生該檔案。

   a. 請點選「匯入」，然後尋找包含關鍵字的 .csv 檔案。

   b. 請點選「開啟」。

      隨即顯示訊息，通知您是否匯入成功。如果要匯入的關鍵字已存在於該清單中，系統將會略過該關鍵字。

9. 如果要刪除某個關鍵字，請選取該關鍵字，然後請點選「刪除」。

10. 如果要匯出關鍵字：

注意

使用「匯出」功能來備份關鍵字或將它們匯入到另一台伺服器。將匯出關鍵字清單中的所有關鍵字。您無法匯出個別關鍵字。

a. 請點選「匯出」。

b. 將產生的 .csv 檔案儲存到想要的位置。

11. 請點選「儲存」。

12. 接著會出現一則訊息，提醒您將此設定部署到用戶端。請點選「關閉」。

13. 返回「DLP 資料識別碼」畫面，並請點選「套用至所有用戶端」。

匯入關鍵字清單

如果您有包含關鍵字清單且格式正確的 .dat 檔案，請使用此選項。您可以從目前正在存取的伺服器或其他伺服器匯出關鍵字清單，來產生該檔案。

步驟

1. 移至「用戶端 > 資料外洩防護 > 資料識別碼」。

2. 請點選「關鍵字」標籤。

3. 請點選「匯入」，然後尋找包含關鍵字清單的 .dat 檔案。

4. 請點選「開啟」。

   隨即顯示訊息，通知您是否匯入成功。如果要匯入的關鍵字清單已存在，系統將會略過該清單。

5. 請點選「套用至所有用戶端」。

資料外洩防護範本

DLP 範本結合 DLP 資料識別碼與邏輯運算子 (And、Or、Except) 以形成條件陳述式。只有滿足特定條件陳述式的檔案或資料會受到 DLP 策略的管制。

例如，檔案必須是 Microsoft Word 檔案（檔案屬性）AND （且）必須包含特定法律詞彙（關鍵字）AND（且）必須包含 ID 號碼（表示式），才能受到「聘用合約」策略管制。此策略允許人力資源部門的員工透過列印方式傳輸檔案，以便將列印複本交由員工簽署。但禁止透過其他可能的通道（例如：電子郵件）傳輸。

如果您已經設定 DLP 資料識別碼，您也可以建立自己的範本。您也可以使用已預先定義的範本。如需詳細資訊，請參閱自訂的 DLP 範本 第 11-19 頁和預先定義的 DLP 範本 第 11-18 頁。

注意

您無法刪除目前正在「DLP 策略」中使用的範本。刪除範本之前，請先從策略移除範本。

預先定義的 DLP 範本

資料外洩防護隨附以下一組已預先定義的範本，供您視各種法規標準需求使用。您無法修改或刪除這些範本。

- GLBA:Gramm-Leach-Billey Act
- HIPAA：健康保險流通與責任法案
- PCI-DSS：支付卡產業資料安全標準
- SB-1386：美國參議院法案 1386
- US PII：美國的個人識別資訊

如需所有預先定義範本的用途，以及受保護的資料範本的詳細清單，請參閱「資料安全防護清單」文件，網址為：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

自訂的 DLP 範本

如果您已經設定資料識別碼，請建立自己的範本。範本結合資料識別碼與邏輯運算子 (And、Or、Except) 以形成條件陳述式。

如需有關條件陳述式和邏輯運算子如何運作的詳細資訊和範例，請參閱條件陳述式和邏輯運算子 第 11-19 頁。

條件陳述式和邏輯運算子

資料外洩防護會從左到右評估條件陳述式。設定條件陳述式時，請小心使用邏輯運算子。使用不當會造成條件陳述式錯誤，而且有可能產生意想不到的後果。

請參閱下表中的範例。

表 11-4. 條件陳述式範例

條件陳述式	解譯和範例
[資料識別碼 1] 和 [資料識別碼 2] Except [資料識別碼 3]	檔案必須滿足 [資料識別碼 1] 和 [資料識別碼 2] 但不用滿足 [資料識別碼 3]。 例如： 檔案必須是 [Adobe PDF 文件] 而且必須包含 [電子郵件信箱]，但是不應該包含 [關鍵字清單中的所有關鍵字]。
[資料識別碼 1] 或 [資料識別碼 2]	檔案必須滿足 [資料識別碼 1] 或 [資料識別碼 2]。 例如： 檔案必須是 [Adobe PDF 文件] 或 [Microsoft Word 文件]。

條件陳述式	解譯和範例
Except [資料識別碼 1]	檔案必須不滿足 [資料識別碼 1]。 例如： 檔案不能是 [多媒體檔案]。

如表格中最後一個範例所示，如果檔案必須不能滿足陳述式中的所有資料識別碼，則條件陳述式中的第一個資料識別碼可以有「Except」運算子。不過，在大部分的情況下，第一個資料識別碼沒有運算子。

建立範本

步驟

1. 移至「用戶端 > 資料外洩防護 > DLP 範本」。
2. 請點選「新增」。

   接著會顯示一個新畫面。
3. 輸入範本的名稱。名稱的長度不能超過 100 個位元組，而且不能包含下列字元：

   - > < * ^ | & ? \ /
4. 請輸入長度不超過 256 個位元組的說明。
5. 選取資料識別碼，然後請點選「新增」圖示。

   選取定義時：

   - 按住 CTRL 鍵，然後選取資料識別碼，就可以選取多個項目。
   - 如果想要使用特定定義，可以使用搜尋功能。您可以輸入完整或部分的資料識別碼名稱。
   - 每個範本最多可以包含 30 個資料識別碼。
6. 如果要建立新的表示式，請點選「表示式」，再請點選「新增表示式」。在顯示的畫面中，設定該表示式的設定。

7. 如果要建立新的檔案屬性清單，請點選「檔案屬性」，再請點選「新增檔案屬性」。在顯示的畫面中，設定該檔案屬性清單的設定。
8. 如果要建立新的關鍵字清單，請點選 「關鍵字」，再請點選 「新增關鍵字」。在顯示的畫面中，設定該關鍵字清單的設定。
9. 如果您選取表示式，請輸入出現次數，這是指資料外洩防護將表示式套用至策略之前，表示式必須出現的次數。
10. 為每個定義選擇邏輯運算子。

注意

設定條件陳述式時，請小心使用邏輯運算子。使用不當會造成條件陳述式錯誤，而且有可能產生意想不到的後果。如需正確用法範例，請參閱條件陳述式和邏輯運算子 第 11-19 頁。

11. 如果要從選取的識別碼清單中移除資料識別碼，請點選資源回收筒圖示。
12. 在「預覽」下方，檢查條件陳述式並視需要修改不適用的陳述式。
13. 請點選「儲存」。
14. 接著會出現一則訊息，提醒您將此設定部署到用戶端。請點選「關閉」。
15. 返回「DLP 範本」畫面，請點選「套用至所有用戶端」。

匯入範本

如果您有包含範本且格式正確的 .dat 檔案，請使用此選項。您可以從目前正在存取的伺服器或其他伺服器匯出範本，來產生該檔案。

步驟

1. 移至「用戶端 > 資料外洩防護 > DLP 範本」。
2. 請點選「匯入」，然後尋找包含範本的 .dat 檔案。
3. 請點選「開啟」。

隨即顯示訊息，通知您是否匯入成功。如果要匯入的範本已存在，系統將會略過該範本。

4. 請點選「套用至所有用戶端」。

DLP 通道

使用者可以透過各種通道傳輸機密資訊。Apex One 可以監控下列通道：

- 網路通道：機密資訊是藉由網路通訊協定（例如 HTTP 和 FTP）進行傳輸。
- 系統和應用程式通道：機密資訊是藉由端點的本機應用程式和周邊進行傳輸。

網路通道

資料外洩防護可以監控透過下列網路通道傳輸的資料：

- 電子郵件用戶端
- FTP
- HTTP 和 HTTPS
- IM 應用程式
- SMB 通訊協定
- 網路郵件

為了決定要監控哪些資料傳輸，資料外洩防護會檢查您必須設定的傳輸範圍。根據您選取的範圍，資料外洩防護 會監控所有資料傳輸或只監控區域網路 (LAN) 外部的傳輸。

如需有關傳輸範圍的詳細資訊，請參閱網路通道的傳輸範圍和目標 第 11-26 頁。

電子郵件用戶端

資料外洩防護會監控透過各種電子郵件用戶端傳輸的電子郵件。資料外洩防護會檢查電子郵件的主旨、內文和附件是否包含資料識別碼。如需支援的電子郵件用戶端清單，請參閱「資料安全防護清單」文件，網址為：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

當使用者嘗試傳送電子郵件時，就會予以監控。如果電子郵件包含資料識別碼，資料外洩防護會允許或封鎖該電子郵件。

您可以定義不受監控的內部電子郵件網域和受監控的子網域。

- 不受監控的電子郵件網域：資料外洩防護會立即允許傳送到不受監控網域的電子郵件傳輸。

  注意

  資料傳輸至不受監控的電子郵件網域及受監控的電子郵件子網域（中毒處理行動是「監控」）與允許傳輸的是類似的。唯一不同之處是資料外洩防護不會記錄不受監控的電子郵件網域的傳輸，但永遠會記錄受監控的電子郵件子網域的傳輸。

- 受監控的電子郵件子網域：當資料外洩防護偵測到傳輸至受監控子網域的電子郵件時，它會檢查策略的處理行動。然後根據處理行動決定允許或封鎖傳輸。

  注意

  如果您選取電子郵件用戶端作為監控的通道，則電子郵件必須符合其受監控的策略。相反，傳送到受監控電子郵件子網域的電子郵件會自動受到監控，無論其是否符合策略。

使用下列任一格式指定網域，並以逗號分隔多個網域：

- X400 格式，例如 /O=Trend/OU=USA, /O=Trend/OU=China
- 電子郵件網域，例如 `example.com`

對於透過 SMTP 通訊協定傳送的電子郵件，資料外洩防護會檢查目標 SMTP 伺服器是否在下列清單中：

1. 受監控的目標
2. 不受監控的目標

> **注意**
>
> 如需有關受監控與不受監控的目標的詳細資訊，請參閱定義不受監控和受監控的目標 第 11-37 頁。

3. 不受監控的電子郵件網域
4. 受監控的電子郵件子網域

這表示如果電子郵件是傳送到受監控目標清單中的 SMTP 伺服器，則電子郵件會受到監控。如果 SMTP 伺服器不在受監控目標清單中，則資料外洩防護會檢查其他的清單。

對於透過其他通訊協定傳送的電子郵件，資料外洩防護只會檢查下列清單：

1. 不受監控的電子郵件網域
2. 受監控的電子郵件子網域

FTP

當 Apex One 偵測到 FTP 用戶端嘗試將檔案上傳到 FTP 伺服器時，它會檢查檔案中是否包含資料識別碼。此時尚未上傳任何檔案。視 DLP 策略而定，Apex One 會允許或封鎖上傳。

當您設定會封鎖檔案上傳的策略時，請記住下列幾點：

- 當 Apex One 封鎖上傳時，某些 FTP 用戶端會嘗試重新上傳檔案。在此情況下，Apex One 會終止該 FTP 用戶端，以禁止重新上傳。FTP 用戶端終止後，使用者不會收到通知。當您實作 DLP 策略時，請將此情況告知使用者。
- 如果要上傳的檔案會覆寫 FTP 伺服器上的檔案，可能會刪除 FTP 伺服器上的檔案。

如需支援的 FTP 用戶端清單，請參閱「資料安全防護清單」文件，網址為：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

HTTP 和 HTTPS

Apex One 會監控要透過 HTTP 和 HTTPS 傳輸的資料。對於 HTTPS，資料在加密及傳輸之前，Apex One 會先進行檢查。

如需支援的 Web 瀏覽器和應用程式清單，請參閱「資料安全防護清單」文件，網址為：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

IM 應用程式

Apex One 會監控使用者透過即時通訊（IM）應用程式傳送的訊息和檔案，但不會監控使用者接收的訊息和檔案。

如需支援的 IM 應用程式清單，請參閱「資料安全防護清單」文件，網址為：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

當 Apex One 封鎖透過 AOL Instant Messenger、MSN、Windows Messenger 或 Windows Live Messenger 傳送的訊息或檔案時，它也會終止應用程式。如果 Apex One 不這樣做，應用程式就會變成沒有回應，而且使用者仍會被迫終止應用程式。應用程式終止之後，使用者不會收到通知。當您實作 DLP 策略時，請將此情況告知使用者。

SMB 通訊協定

Apex One 會監控透過「伺服器訊息區」(SMB) 通訊協定傳輸的資料，這種通訊協定是用於共享檔案存取。當另一位使用者嘗試複製或讀取使用者共用的檔案時，Apex One 會檢查檔案是否為資料識別碼或包含資料識別碼，然後允許或封鎖該作業。

注意

周邊設備存取控管處理行動的優先順序比 DLP 處理行動還高。例如，如果「周邊設備存取控管」不允許移動對應網路磁碟機上的檔案，則即使 DLP 允許，也無法傳輸機密資料。

如需有關「周邊設備存取控管」處理行動的詳細資訊，請參閱儲存裝置的權限 第 10-4 頁。

如需 Apex One 監控是否有共用檔案存取的應用程式清單，請參閱「資料安全防護清單」文件，網址為：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

網路郵件

Web 電子郵件服務會透過 HTTP 傳輸資料。如果 Apex One 偵測到支援的服務對外傳送資料，它會檢查資料中是否包含資料識別碼。

如需支援的 Web 電子郵件服務清單，請參閱「資料安全防護清單」文件，網址為：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

網路通道的傳輸範圍和目標

傳輸範圍和目標會定義資料外洩防護必須監控之網路通道上的資料傳輸。對於應監控的傳輸，資料外洩防護會檢查其中是否有資料識別碼，以決定允許或封鎖該傳輸。對於不應監控的傳輸，資料外洩防護不會檢查其中是否有資料識別碼，且會立即允許該傳輸。

傳輸範圍：所有傳輸

資料外洩防護會監控主機電腦外部傳輸的資料。

注意

趨勢科技建議您為外部用戶端選擇此範圍。

如果您不想要監控傳輸到主機電腦外部某些目標的資料，請定義下列項目：

- 不受監控的目標：資料外洩防護不會監控傳輸到這些目標的資料。

  注意

  資料傳輸至不受監控的目標及受監控的目標（中毒處理行動是「監控」）與允許傳輸的是類似的。唯一不同之處是資料外洩防護不會記錄不受監控的目標的傳輸，但永遠會記錄受監控的目標的傳輸。

- 受監控的目標：這些是不受監控的目標之中應監控的特定目標。受監控的目標是：
  - 選用的，如果您已定義不受監控的目標。
  - 不可設定的，如果您沒有定義不受監控的目標。

例如：

下列 IP 位址已指定給貴公司的法律部門：

- 10.201.168.1 到 10.201.168.25

您正在建立策略，用於監控傳送「就業證明」給除了法律部門全職員工以外所有員工的傳輸。如果要這麼做，您可以選取「所有傳輸」作為傳輸範圍，接著：

選項	步驟
選項 1	1. 將 10.201.168.1-10.201.168.25 新增到不受監控的目標。 2. 將法律部門兼職員工的 IP 位址新增到受監控的目標。假設有 3 個 IP 位址 — 10.201.168.21-10.201.168.23。
選項 2	將法律部門全職員工的 IP 位址新增到非受監控的目標： • 10.201.168.1-10.201.168.20 • 10.201.168.24-10.201.168.25

如需有關定義受監控與不受監控的目標的指導方針，請參閱定義不受監控和受監控的目標 第 11-37 頁。

傳輸範圍：僅限區域網路外部的傳輸

資料外洩防護會監控傳輸到區域網路 (LAN) 外部任何目標的資料。

注意

趨勢科技建議您為內部用戶端選擇此範圍。

「網路」是指公司或區域網路。這包括目前網路（端點和網路遮罩的 IP 位址）及下列標準私人 IP 位址：

- 類別 A：`10.0.0.0` 到 `10.255.255.255`
- 類別 B：`172.16.0.0` 到 `172.31.255.255`
- 類別 C：`192.168.0.0` 到 `192.168.255.255`

如果您選取此傳輸範圍，則可以定義下列項目：

- 不受監控的目標：定義位於 LAN 外部且您認為安全因而不應監控的目標。

  注意

  資料傳輸至不受監控的目標及受監控的目標（中毒處理行動是「監控」）與允許傳輸的是類似的。唯一不同之處是資料外洩防護不會記錄不受監控的目標的傳輸，但永遠會記錄受監控的目標的傳輸。

- 受監控的目標：定義位於 LAN 內部的您想要監控的目標。

如需有關定義受監控與不受監控的目標的指導方針，請參閱定義不受監控和受監控的目標 第 11-37 頁。

解決衝突

如果傳輸範圍、受監控目標以及不受監控目標等設定發生衝突，Apex One 會遵循下列優先順序（以最高到最低的順序）：

- 受監控的目標
- 不受監控的目標
- 傳輸範圍

系統和應用程式通道

資料外洩防護可以監控下列系統和應用程式通道：

- 雲端儲存服務
- 資料錄製器 (CD/DVD)
- 對等式應用程式
- PGP 加密
- 印表機
- 卸除式儲存
- 同步處理軟體 (ActiveSync)
- Windows 剪貼簿

雲端儲存服務

Apex One 會監控使用者使用雲端儲存服務存取的檔案。如需支援的雲端儲存服務清單，請參閱「資料安全防護清單」文件，網址為：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

注意

當 Endpoint Encryption 安裝在用戶端端點上時，資料外洩防護在雲端儲存服務上支援加密。

資料錄製器 (CD/DVD)

Apex One 會監控錄製到 CD 或 DVD 的資料。如需支援的資料錄製裝置和軟體清單，請參閱「資料安全防護清單」文件，網址為：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

當 Apex One 在任何支援裝置或軟體上偵測到發出的「燒錄」命令，且處理行動是「暫不處理」時，資料錄製程序會繼續。如果處理行動是「封鎖」，Apex One 會檢查要錄製的檔案是否為資料識別碼或包含資料識別碼。如果 Apex One 偵測到至少一個資料識別碼，則不會錄製所有檔案（包含不屬於資料識別碼和未包含資料識別碼的檔案）。Apex One 可能也會防止 CD 或 DVD 退出。如果發生此問題，請指示使用者重新啟動軟體處理程序或重設裝置。

Apex One 會實作其他 CD/DVD 錄製規則：

- 為了減少誤判的情況，Apex One 不會監控下列檔案：

```
.bud      .dll      .gif      .gpd      .htm      .ico      .ini
.jpg      .lnk      .sys      .ttf      .url      .xml
```

- 為提高效能，系統不會監控 Roxio 資料錄製器使用的兩種檔案類型（`*.png` 和 `*.skn`）。
- Apex One 不會監控下列目錄中的檔案：

```
*:\autoexec.bat                    *:\Windows
..\Application Data                ..\Cookies
..\Local Settings                  ..\ProgramData
..\Program Files                   ..\Users\*\AppData
```

```
..\WINNT
```

- 系統不會監控裝置和軟體建立的 ISO 映像檔。

封鎖對資料錄製器 (CD/DVD) 的存取

「周邊設備存取控管」只能限制對使用 Live File System 格式的 CD/DVD 錄製裝置的存取。即使啟動「周邊設備存取控管」，使用主圖形格式的部分協力廠商應用程式仍可以執行讀取/寫入作業。請使用資料外洩防護限制對使用任何格式類型的 CD/DVD 錄製裝置的存取。

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > DLP 設定」。
4. 請點選「外部用戶端」標籤以設定外部用戶端的策略，或請點選「內部用戶端」標籤以設定內部用戶端的策略。

   注意

   如果您尚未設定 用戶端 位置設定，請進行設定。用戶端會使用這些位置設定來確定要套用的正確資料外洩防護策略。如需詳細資訊，請參閱端點位置 第 15-2 頁。

5. 選擇下列其中一個項目：
   - 如果您使用的是「外部用戶端」標籤，則可以透過選取「套用所有設定至內部用戶端」將所有資料外洩防護設定套用至內部用戶端。
   - 如果您使用的是「內部用戶端」標籤，則可以透過選取「套用所有設定至外部用戶端」將所有資料外洩防護設定套用至外部用戶端。
6. 在「規則」標籤上，，請點選「新增」。
7. 選取啟動這項規則。

8. 指定此規則的名稱。
9. 請點選「範本」標籤。
10. 從清單中選取「所有副檔名」範本，然後請點選「新增」。
11. 請點選「通道」標籤。
12. 在「系統和應用程式通道」區段中，選取「資料錄製器 (CD/DVD)」。
13. 請點選「處理行動」標籤。
14. 選取「封鎖」處理行動。
15. 請點選「儲存」。
16. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
    - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
    - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

對等式應用程式

Apex One 會監控使用者透過對等式應用程式分享的檔案。

如需支援的對等式應用程式清單，請參閱「資料安全防護清單」文件，網址為：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

PGP 加密

Apex One 會監控要由 PGP 加密軟體加密的資料。在加密之前，Apex One 會先檢查資料。

如需支援的 PGP 加密軟體清單，請參閱「資料安全防護清單」文件，網址為：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

印表機

Apex One 會監控各種應用程式起始的印表機作業。

Apex One 不會監控尚未儲存的新檔案的印表機作業，因為列印資訊此時只儲存在記憶體中。

如需支援的可起始印表機作業之應用程式清單，請參閱「資料安全防護清單」文件，網址為：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

卸除式儲存

Apex One 會監控傳輸到卸除式儲存裝置的資料或在卸除式儲存裝置中傳輸的資料。與資料傳輸有關的活動包括：

- 在裝置中建立檔案
- 將檔案從主機複製到裝置
- 關閉裝置中已修改的檔案
- 修改裝置中的檔案資訊（例如：檔案的副檔名）

當要傳輸的檔案包含資料識別碼時，Apex One 會封鎖或允許傳輸。

注意

- 周邊設備存取控管處理行動的優先順序比 DLP 處理行動還高。例如，如果「周邊設備存取控管」不允許將檔案複製到卸除式儲存裝置，則即使 DLP 允許，仍不會傳輸機密資訊。
- 當用戶端端點上安裝了 Endpoint Encryption 時，資料外洩防護支援在卸除式儲存裝置上進行加密。

如需有助於資料傳輸活動的支援卸除式儲存裝置和應用程式清單，請參閱「資料安全防護清單」文件，網址為：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

檔案傳輸至卸除式儲存裝置的處理，是一種直接的過程。例如，在 Microsoft Word 建立檔案的使用者可能想要將檔案儲存至 SD 卡（與使用者儲存的檔案類型無關）。如果檔案包含不應該傳輸的資料識別碼，Apex One 會禁止儲存檔案。

對於裝置中的檔案傳輸，Apex One 會先將檔案（如果檔案大小未超過 75MB）備份到 `%WINDIR%\system32\dgagent\temp`，然後再進行處理。如果 Apex One 允許傳輸檔案，它就會移除備份檔案。如果 Apex One 封鎖傳輸，檔案有可能會在這個過程中被刪除。在此情況下，Apex One 會將備份檔案複製到包含原始檔案的資料夾。

Apex One 可讓您定義例外。Apex One 永遠允許傳輸資料到這些裝置或在這些裝置內傳輸資料。透過裝置的廠商及選擇性提供的裝置型號和序號 ID 來識別裝置。

秘訣

使用「裝置清單工具」查詢連接至端點的裝置。此工具可以提供每個裝置的裝置廠商、型號和序號 ID。如需詳細資訊，請參閱裝置清單工具 第 10-13 頁。

同步處理軟體 (ActiveSync)

Apex One 會監控透過同步處理軟體傳輸到行動裝置的資料。

如需支援的同步處理軟體清單，請參閱「資料安全防護清單」文件，網址為：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

如果資料的來源 IP 位址是 127.0.0.1 而且是透過通訊埠 990 或 5678（用於同步處理的連接埠）傳送，Apex One 會檢查資料是否為資料識別碼，然後允許或封鎖其傳輸。

當 Apex One 封鎖通訊埠 990 上的檔案傳輸時，行動裝置的目的地資料夾可能仍會建立名稱相同，但是字元格式有誤的檔案。這是因為 Apex One 封鎖傳輸之前，檔案的某些部分已經複製到裝置上。

Windows 剪貼簿

Apex One 會監控要傳輸到 Windows 剪貼簿的資料，再允許或封鎖傳輸。

Apex One 也可以監控主機和 VMWare 或遠端桌面之間的剪貼簿活動。會在具有 Security Agent 的實體上進行監控。例如，VMware 虛擬機器上的 Security Agent 會禁止虛擬機器上的剪貼簿資料傳輸到主機。同樣地，具有 Security Agent 的主機可能不會將剪貼簿資料複製到透過遠端桌面存取的端點。

資料外洩防護處理行動

當資料外洩防護偵測到資料識別碼的傳輸時，它會針對偵測到的資料識別碼檢查「DLP 策略」，並執行為該策略設定的處理行動。

下表列出資料外洩防護處理行動。

表 11-5. 資料外洩防護處理行動

處理行動	說明
處理行動	
暫不處理	資料外洩防護允許傳輸並會記錄傳輸。
封鎖	資料外洩防護封鎖傳輸並會記錄傳輸。
其他處理行動	

處理行動	說明
通知用戶端使用者	資料外洩防護會顯示通知訊息告知傳輸資料的使用者，並告知資料已傳送或已封鎖。
記錄資料	無論主要處理行動為何，資料外洩防護都會將機密資訊記錄至 <Security Agent 安裝資料夾>\DLPLite\Forensic。選取此處理行動以評估由資料外洩防護標示的機密資訊。 已記錄的機密資訊可能會消耗太多的硬碟空間。因此，趨勢科技強烈建議您只針對高度機密資訊選擇此選項。
使用指定的金鑰/密碼加密支援的通道 (只有在安裝「端點加密」的情況下才能使用) 注意 此選項僅適用於「卸除式儲存」和「雲端儲存」服務通道且只有在選取「暫不處理」處理行動的情況下才能使用。	如果 Trend Micro Endpoint Encryption 隨 Security Agent 一起安裝，則資料外洩防護可自動加密檔案，然後允許使用者將這些檔案傳送到其他位置。如果未安裝「端點加密」，資料外洩防護會對檔案執行「封鎖」處理行動。 選擇以下其中一個加密金鑰或固定式密碼： • 使用者金鑰：亦稱為「本機金鑰」，該金鑰對每個使用者是唯一的，會限制建立加密檔案的使用者存取該檔案。 • 共用金鑰：該金鑰指的是「群組金鑰」或「企業金鑰」，端點加密管理員會使用 PolicyServer MMC 設定該類型。 • 固定式密碼：使用者會使用畫面上的提示字元手動提供固定式密碼。「端點加密」會建立一個自動解壓縮套件，使用者可在提供解密密碼後存取任一端點。

處理行動	說明
	重要 • 目標端點必須安裝了「端點加密」且使用者必須登入「端點加密」才能加密資料。 • 位於 USB 裝置上的加密檔案，會在使用者嘗試解密檔案時接受資料外洩防護掃瞄。解密 USB 裝置上含有機密資料的檔案時，會觸發 USB 加密通訊協定，使系統要求對機密資料加密 (再次)。如果要防止資料外洩防護嘗試「重新加密」資料，請將已加密的檔案移至本機磁碟機，然後再嘗試存取資料。 • 資料外洩防護會在使用網頁用戶端時阻止將檔案上傳到雲端儲存的嘗試。手動加密檔案，然後使用網頁用戶端上傳檔案。
使用者理由 注意 僅在選取「封鎖」處理行動之後，才可以使用該選項。	資料外洩防護會在執行「封鎖」處理行動之前提示使用者。透過提供敏感資料安全通過的原因，使用者可選取覆寫「封鎖」處理行動。可用的理由有： • 這是已建立的商業程序的一部分。 • 我的管理員已核可資料傳輸。 • 該檔案中的資料不是保密的。 • 其他：使用者在提供的文字欄位中提供了替代說明。

資料外洩防護例外

DLP 例外會套用到整個策略，包括策略內定義的所有規則。資料外洩防護會在掃瞄數位資產之前，先將例外設定套用到所有傳輸。如果傳輸符合其中一項例外規則，資料外洩防護會根據例外類型立即允許或掃瞄傳輸。

定義不受監控和受監控的目標

根據「通道」標籤上設定的傳輸範圍，定義不受監控的和受監控的目標。如需如何定義所有傳輸的不受監控的和受監控的目標詳細資訊，請參閱傳輸範圍：

所有傳輸 第 11-26 頁。如需如何定義僅限區域網路外部的傳輸的不受監控的和受監控的目標詳細資訊，請參閱傳輸範圍：僅限區域網路外部的傳輸 第 11-28 頁。

請遵循以下指導方針來定義受監控和不受監控的目標：

1. 根據以下項目定義每個目標：
   - IP 位址
   - 主機名稱
   - FQDN
   - 網路位址與子網路遮罩，例如，10.1.1.1/32

   注意

   對於子網路遮罩，資料外洩防護僅支援無類別網域間路由 (CIDR) 類型的通訊埠。這表示您只能輸入 32 之類的數字，而不能輸入 255.255.255.0。

2. 如果要以特定通道作為目標，請包含這些通道的預設或公司定義的通訊埠號碼。例如，通訊埠 21 通常用於 FTP 傳輸、通訊埠 80 用於 HTTP、通訊埠 443 用於 HTTPS。使用分號分隔目標與通訊埠號碼。
3. 您也可以包含通訊埠範圍。如果要包含所有通訊埠，請忽略通訊埠範圍。

   具有通訊埠號碼和通訊埠範圍的目標範例：
   - 10.1.1.1:80
   - host:5-20
   - host.domain.com:20
   - 10.1.1.1/32:20
4. 使用逗點分隔多個目標。

解壓縮規則

可以掃瞄壓縮檔中包含的檔案是否有數位資產。為了確定要掃瞄的檔案，資料外洩防護會使壓縮檔遵循下列規則：

- 解壓縮檔大小超過：__ MB (1-10240 MB)
- 壓縮層的數目超過：__ (1-20)
- 要掃瞄的檔案數超過：__ (1-2000)

規則 1：解壓縮檔大小上限

壓縮檔解壓縮後的大小必須符合指定的限制。

例如：您將限制設定為 20MB。

狀況 1：如果 `archive.zip` 解壓縮後的大小為 30MB，將不會掃瞄 `archive.zip` 中包含的任何檔案。也不會繼續檢查其他兩個規則。

狀況 2：如果 `my_archive.zip` 解壓縮後的大小為 10MB：

- 如果 `my_archive.zip` 未包含壓縮檔，則 Apex One 會略過「規則 2」並繼續進行「規則 3」。
- 如果 `my_archive.zip` 包含壓縮檔，則所有壓縮檔的大小必須在限制範圍內。例如，如果 `my_archive.zip` 包含 `AAA.rar`、`BBB.zip` 和 `EEE.zip`，且 `EEE.zip` 包含 `222.zip`：

```
my_archive.zip                    = 10MB（解壓縮後）

        \AAA.rar                  = 25MB（解壓縮後）

        \BBB.zip                  = 3MB（解壓縮後）

        \EEE.zip                  = 1MB（解壓縮後）

                \222.zip          = 2MB（解壓縮後）
```

將依據「規則 2」檢查 my_archive.zip、BBB.zip、EEE.zip 和 222.zip，因為這些檔案的合併大小低於 20MB 限制。將略過 AAA.rar。

規則 2：壓縮層數上限

指定層數內的檔案將標示為進行掃瞄。

例如：

```
my_archive.zip
                    \BBB.zip            \CCC.xls
                    \DDD.txt
                    \EEE.zip            \111.pdf
                                        \222.zip            \333.txt
```

如果您將限制設定為兩層：

- Apex One 將忽略 333.txt，因為它位於第三層。
- Apex One will 將標示下列檔案進行掃瞄，然後檢查「規則 3」：
  - DDD.txt（位於第一層）
  - CCC.xls（位於第二層）
  - 111.pdf（位於第二層）

規則 3：要掃瞄的檔案數目上限

Apex One 會掃瞄所指定數目上限的檔案。Apex One 會依據先數字後字母的順序掃瞄檔案和資料夾。

繼續以「規則 2」的範例為例，Apex One 會標示反白顯示的檔案進行掃瞄：

```
my_archive.zip
```

```
                    \BBB.zip            \CCC.xls
                    \DDD.txt
                    \EEE.zip            \111.pdf
                                        \222.zip            \333.txt
```

此外，my_archive.zip 包含名為 7Folder 的資料夾（不會根據「規則 2」進行檢查）。此資料夾包含 FFF.doc 和 GGG.ppt。這會使要掃瞄的檔案總數為 5 個，反白顯示如下：

```
my_archive.zip
                    \7Folder            \FFF.doc
                    \7Folder            \GGG.ppt
                    \BBB.zip            \CCC.xls
                    \DDD.txt
                    \EEE.zip            \111.pdf
                                        \222.zip            \333.txt
```

如果您將限制設為 4 個檔案，將掃瞄下列檔案：

- FFF.doc
- GGG.ppt
- CCC.xls
- DDD.txt

注意

對於包含內嵌檔案的檔案，Apex One 會解壓縮內嵌檔案的內容。

如果解壓縮的內容是文字，則主控檔案（例如 `123.doc`）和內嵌檔案（例如 `abc.txt` 和 `xyz.xls`）會計為一個檔案。

如果解壓縮的內容不是文字，則主控檔案（例如 `123.doc`）和內嵌檔案（例如 `abc.exe`）會分開計算。

觸發解壓縮規則的事件

下列事件會觸發解壓縮規則：

表 11-6. 觸發解壓縮規則的事件

要傳輸的壓縮檔符合策略且壓縮檔的毒處理行動為「暫不處理」（傳輸檔案）。	例如，如果要監控使用者正在傳輸的 .ZIP 檔案，您可以定義檔案屬性 (.ZIP)、將該屬性新增至範本、在策略中使用該範本，然後將處理行動設為「暫不處理」。 **注意** 如果處理行動是「封鎖」，則不會傳輸整個壓縮檔，因此無需掃瞄其所包含的檔案。
要傳輸的壓縮檔不符合策略。	在此情況下，Apex One 仍會使壓縮檔遵循解壓縮規則，以判斷其包含的哪些檔案應掃瞄是否有數位資產，以及是否傳輸整個壓縮檔。

這兩種事件具有相同的結果。當 Apex One 遇到壓縮檔時：

- 如果未滿足「規則 1」，Apex One 會允許傳輸整個壓縮檔。
- 如果滿足「規則 1」，將繼續檢查其他兩個規則。如果出現下列情況，Apex One 將允許傳輸整個壓縮檔：
  - 所有已掃瞄的檔案皆不符合策略。

- 所有已掃瞄的檔案皆符合策略且處理行動為「暫不處理」。

  如果至少一個已掃瞄的檔案符合策略且處理行動為「封鎖」，則會禁止傳輸整個壓縮檔。

資料外洩防護策略組態設定

設定資料識別碼並將它們分門別類放到各個範本之後，您就可以開始建立資料外洩防護策略。

除了資料識別碼與範本之外，建立策略的時候，還需要設定通道和處理行動。如需有關策略的詳細資訊，請參閱資料外洩防護策略 第 11-3 頁。

建立資料外洩防護策略

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > DLP 設定」。
4. 請點選「外部用戶端」標籤以設定外部用戶端的策略，或請點選「內部用戶端」標籤以設定內部用戶端的策略。

   注意

   如果您尚未設定 用戶端 位置設定，請進行設定。用戶端會使用這些位置設定來確定要套用的正確資料外洩防護策略。如需詳細資訊，請參閱端點位置 第 15-2 頁。

5. 選取「啟動資料外洩防護」。
6. 選擇下列其中一個項目：

- 如果您使用的是「外部用戶端」標籤，則可以透過選取「套用所有設定至內部用戶端」將所有資料外洩防護設定套用至內部用戶端。
- 如果您使用的是「內部用戶端」標籤，則可以透過選取「套用所有設定至外部用戶端」將所有資料外洩防護設定套用至外部用戶端。

7. 在「規則」標籤上，，請點選「新增」。

   一個策略最多可包含 40 個規則。

8. 配置下列規則設定。

   如需建立 DLP 規則的詳細資訊，請參閱建立資料外洩防護規則 第 11-44 頁。

9. 請點選「例外」標籤，然後配置任何必要的例外設定。

   如需可用例外設定的詳細資訊，請參閱資料外洩防護例外 第 11-37 頁。

10. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

    - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
    - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

建立資料外洩防護規則

注意

資料外洩防護會按優先順序處理規則和範本。如果規則設定為「暫不處理」，資料外洩防護會處理清單中的下一個規則。如果規則設定為「封鎖」或「使用者理由」，資料外洩防護會封鎖或接受使用者處理行動，不會進一步處理該規則/範本。

步驟

1. 選取啟動這項規則。
2. 指定此規則的名稱。

   配置下列範本設定：

3. 請點選「範本」標籤。
4. 從「可用的範本」清單中選取範本，然後請點選「新增」。

   選取範本時：

   - 請點選範本名稱來反白顯示名稱，藉此選取多個項目。
   - 如果想要使用特定範本，可以使用搜尋功能。您可以輸入完整或部分的範本名稱。

   注意

   每個規則最多可以包含 200 個範本。

5. 如果「可用的範本」清單中沒有您偏好的範本，請執行下列操作：

   a. 請點選「新增範本」。

      「資料外洩防護範本」畫面即會顯示。

      如需有關在「資料外洩防護範本」畫面中新增範本的指示，請參閱資料外洩防護範本 第 11-18 頁。

   b. 建立範本之後，請選取它，然後請點選「新增」。

   注意

   Apex One 檢查範本時會使用第一個符合的規則。這表示如果有檔案或資料符合某個範本的定義，Apex One 就不會再檢查其他的範本。優先順序取決於清單中範本的順序。

   配置下列通道設定：

6. 請點選「通道」標籤。

7. 選取規則的通道。

   如需有關通道的詳細資訊，請參閱網路通道 第 11-22 頁和系統和應用程式通道 第 11-29 頁。

8. 如果您已選取任何一種網路通道，請選取傳輸範圍：

   - 所有傳輸
   - 僅限區域網路外部的傳輸

   如需傳輸範圍、目標如何根據傳輸範圍運作，以及如何正確定義目標的詳細資訊，請參閱網路通道的傳輸範圍和目標 第 11-26 頁。

9. 如果您已選取「電子郵件用戶端」，請執行下列操作：

   a. 請點選「例外」。

   b. 指定受監控和不受監控的內部電子郵件網域。

      如需有關受監控與不受監控的電子郵件網域的詳細資訊，請參閱電子郵件用戶端 第 11-23 頁。

10. 如果您已選取「卸除式儲存」，請執行下列操作：

    a. 請點選「例外」。

    b. 新增按照廠商識別的不受監控卸除式儲存裝置。裝置型號和序號 ID 是選用的。

       USB 裝置的核可清單支援使用星號 (*) 萬用字元。以星號 (*) 取代任何欄位，以包含符合其他欄位要求的所有裝置。

       例如，[vendor]-[model]-* 會將指定廠商和指定型號類型的所有 USB 裝置置於核可清單中，而不論序號 ID 為何。

    c. 如果要新增更多裝置，請點選加號 (+) 圖示。

秘訣

使用「裝置清單工具」查詢連接至端點的裝置。此工具可以提供每個裝置的裝置廠商、型號和序號 ID。如需詳細資訊，請參閱裝置清單工具 第 10-13 頁。

配置下列處理行動設定：

11. 請點選「處理行動」標籤。
12. 選取主要處理行動和任何其他處理行動。

    如需有關處理行動的詳細資訊，請參閱資料外洩防護處理行動 第 11-35 頁。

注意

資料外洩防護僅支援在卸除式裝置和雲端儲存服務上加密機密資料。資料外洩防護將執行「暫不處理」處理行動，而非在不支援加密的所有通道上執行加密。目標端點必須安裝了 Endpoint Encryption 且使用者必須登入 Endpoint Encryption 才能加密資料。

13. 配置「範本」、「通道」和「處理行動」設定之後，請點選「儲存」。

匯入、匯出和複製 DLP 規則

管理員可以匯入先前定義的規則（包含在正確格式化的 .dat 檔案中）或匯出配置的 DLP 規則清單。複製 DLP 規則可以讓管理員修改先前定義規則的內容，藉此節省時間。

下表說明每項功能的運作方式。

表 11-7. 匯入、匯出和複製 DLP 規則的功能

功能	說明
匯入	匯入規則清單會將不存在的規則附加至現有的 DLP 規則清單中。資料外洩防護會略過目標清單中已存在的規則。資料外洩防護會維護每項規則的所有預先設定的設定，包括已啟動或已關閉狀態。

功能	說明
匯出	匯出規則清單會將整份清單匯出至 .dat 檔案，讓管理員接著匯入並部署到其他網域或用戶端。資料外洩防護會根據目前的組態設定，儲存所有規則設定。 注意 • 管理員必須先儲存或套用任何新的或修改過的規則，然後才能匯出清單。 • 資料外洩防護不會匯出為策略設定的任何例外，只會匯出為每個規則設定的設定。
複製	複製規則會建立與規則之目前組態設定完全相同的複本。管理員必須輸入規則的新名稱，才能對新規則進行任何必要的組態設定修改。

資料外洩防護通知

Apex One 隨附一組預設的通知訊息，用於向 Apex One 管理員和用戶端使用者通知有關數位資產傳輸的情形。

如需有關傳送給管理員的通知的詳細資訊，請參閱管理員的資料外洩防護通知 第 11-48 頁。

如需有關傳送給用戶端使用者的通知的詳細資訊，請參閱用戶端使用者的資料外洩防護通知 第 11-51 頁。

管理員的資料外洩防護通知

您可以設定 Apex One，讓它在偵測到數位資產傳輸或封鎖傳輸時通知管理員。

Apex One 具有一組預設的通知訊息，可在偵測到數位資產傳輸時通知管理員。您可以視公司需要修改通知和設定其他通知設定。

注意

Apex One 可以透過電子郵件、SNMP Trap 和 Windows NT 事件記錄檔來傳送通知。設定 Apex One 何時透過這些通道傳送通知的設定。如需詳細資訊，請參閱管理員通知設定 第 14-35 頁。

設定給管理員的資料外洩防護通知

步驟

1. 移至「管理 > 通知 > 管理員」。
2. 在「條件」標籤上：
   a. 移至「數位資產傳輸」區段。
   b. 指定要在偵測到數位資產傳輸（可封鎖或允許該動作）時傳送通知，或只在封鎖傳輸時傳送通知。
3. 在「電子郵件」標籤上：
   a. 移至「數位資產傳輸」區段。
   b. 選取「啟動電子郵件通知」。
   c. 選取「傳送通知給具有用戶端樹狀結構網域權限的使用者」。

      使用以角色為基礎的管理，將用戶端樹狀結構網域權限授與使用者。如果在屬於特定網域的用戶端上進行傳輸，系統會將電子郵件傳送給具網域權限之使用者的電子郵件信箱。如需範例，請參閱下表：

表 11-8. 用戶端樹狀結構網域和權限

用戶端樹狀結構網域	具有網域權限的角色	具有該角色的使用者帳號	使用者帳號的電子郵件信箱
網域 A	Administrator（內建）	root	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
網域 B	Administrator（內建）	root	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

如果屬於網域 A 的任何 Security Agent 偵測到數位資產傳輸，電子郵件會傳送給 mary@xyz.com、john@xyz.com 和 chris@xyz.com。

如果屬於網域 B 的任何 Security Agent 偵測到傳輸，電子郵件會傳送給 mary@xyz.com 和 jane@xyz.com。

注意

啟動此選項時，具網域權限的所有使用者都必須有一個對應的電子郵件信箱。電子郵件通知不會傳送給沒有電子郵件信箱的使用者。使用者和電子郵件信箱是從「管理 > 帳號管理 > 使用者帳號」設定的。

d. 選取「傳送通知到下列電子郵件信箱」，然後輸入電子郵件信箱。

e. 接受或修改預設的主旨和訊息。使用 Token 變數代表「主旨」和「訊息」欄位中的資料。

表 11-9. 資料外洩防護通知的 Token 變數

變數	說明
%USER%	偵測到傳輸時已登入端點的使用者
%COMPUTER%	偵測到傳輸的端點
%DOMAIN%	端點的網域

變數	說明
%DATETIME%	偵測到傳輸的日期和時間
%CHANNEL%	偵測到傳輸的通道
%TEMPLATE%	觸發偵測的數位資產範本
%RULE%	觸發偵測的規則名稱 注意 若要在訊息中顯示規則名稱，請在「訊息」欄位中新增此變數。

4. 在「SNMP Trap」標籤中：
   a. 移至「數位資產傳輸」區段。
   b. 選取「啟動 SNMP Trap 通知」。
   c. 接受或修改預設的訊息。使用 Token 變數代表「訊息」欄位中的資料。如需詳細資訊，請參閱表 11-9：資料外洩防護通知的 Token 變數 第 11-50 頁。
5. 在「NT 事件記錄檔」標籤中：
   a. 移至「數位資產傳輸」區段。
   b. 選取「啟動 NT 事件記錄檔通知」。
   c. 接受或修改預設的訊息。您可以使用 Token 變數代表「訊息」欄位中的資料。如需詳細資訊，請參閱表 11-9：資料外洩防護通知的 Token 變數 第 11-50 頁。
6. 請點選「儲存」。

用戶端使用者的資料外洩防護通知

Apex One 可以在允許或封鎖數位資產傳輸之後，立即在用戶端電腦上顯示通知訊息。

如果要在封鎖或允許數位資產傳輸時通知使用者，請在建立資料外洩防護策略時選取「通知用戶端使用者」選項。如需有關建立策略的指示，請參閱資料外洩防護策略組態設定 第 11-43 頁。

設定給用戶端的資料外洩防護通知

步驟

1. 移至「管理 > 通知 > 用戶端」。
2. 在「類型」下拉式清單中，選取「數位資產傳輸」。
3. 接受或修改預設的訊息。
4. 請點選「儲存」。

資料外洩防護記錄檔

用戶端會記錄數位資產傳輸（已封鎖和已允許的傳輸），並立即將記錄檔傳送給伺服器。如果用戶端無法傳送記錄檔，它會在 5 分鐘後重試。

如果要避免記錄檔佔去過多硬碟空間，請手動刪除記錄檔或設定記錄檔刪除預約時程。如需有關管理記錄檔的詳細資訊，請參閱記錄檔管理 第 14-39 頁。

檢視資料外洩防護記錄檔

步驟

1. 移至「用戶端 > 用戶端管理」或「記錄檔 > 用戶端 > 安全威脅」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。

3. 請點選「記錄檔 > 資料外洩防護記錄檔」或「檢視記錄檔 > DLP 記錄檔」。
4. 指定記錄條件，然後請點選「顯示記錄檔」。
5. 檢視記錄檔。

   記錄檔包含下列資訊：

表 11-10. 資料外洩防護記錄檔資訊

欄	說明
日期/時間	資料外洩防護記錄事件的日期和時間
使用者名稱	登入端點的使用者名稱
端點	資料外洩防護偵測到傳輸的端點的名稱
網域	端點的網域
IP 位址	端點的 IP 位址
規則名稱	觸發事件的規則名稱 注意 使用舊版 OfficeScan 建立的策略會顯示 LEGACY_DLP_Policy 的預設名稱。
通道	傳輸發生所經由的通道
處理程序	促進傳輸數位資產的程序（程序視通道而定） 如需詳細資訊，請參閱依通道的處理程序 第 11-54 頁。
來源	包含數位資產的檔案來源或通道（如果沒有來源可用的話）
目標	包含數位資產的檔案所指的目標，或通道（如果沒有可用來源的話）
處理行動	對傳輸採取的處理行動。
檔案/資料大小	偵測到的物件大小

欄	說明
詳細資訊	連結，其包括傳輸的其他詳細資訊 如需詳細資訊，請參閱資料外洩防護記錄檔詳細資料 第 11-56 頁。

6. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請點選「匯出到 CSV」。開啟檔案或將其儲存至特定位置。

依通道的處理程序

下表列出資料外洩防護記錄檔的「處理程序」欄位下顯示的處理程序。

表 11-11. 依通道的處理程序

通道	處理程序
同步處理軟體 (ActiveSync)	同步處理軟體的完整路徑和處理程序名稱 例如： `C:\Windows\system32\WUDFHost.exe`
資料錄製器 (CD/DVD)	資料錄製器的完整路徑與程序名稱 例如： `C:\Windows\Explorer.exe`
Windows 剪貼簿	無
電子郵件用戶端 - Lotus Notes	Lotus Notes 的完整路徑與程序名稱 例如： `C:\Program Files\IBM\Lotus\Notes\nlnotes.exe`
電子郵件用戶端 - Microsoft Outlook	Microsoft Outlook 的完整路徑與程序名稱 例如： `C:\Program Files\Microsoft Office\Office12\OUTLOOK.EXE`

通道	處理程序
電子郵件用戶端 - 所有使用 SMTP 通訊協定的用戶端	電子郵件用戶端的完整路徑與程序名稱 例如： C:\Program Files\Mozilla Thunderbird\thunderbird.exe
卸除式儲存	傳輸資料至儲存裝置或在儲存裝置內部傳輸資料的應用程式程序名稱 例如： explorer.exe
FTP	FTP 用戶端的完整路徑與程序名稱 例如： D:\Program Files\FileZilla FTP Client\filezilla.exe
HTTP	「HTTP 應用程式」
HTTPS	瀏覽器或應用程式的完整路徑與程序名稱 例如： C:\Program Files\Internet Explorer\iexplore.exe
IM 應用程式	IM 應用程式的完整路徑與程序名稱 例如： C:\Program Files\Skype\Phone\Skype.exe
IM 應用程式 - MSN	• MSN 的完整路徑與程序名稱 例如： C:\Program Files\Windows Live\Messenger\msnmsgr.exe • 如果是從聊天視窗傳輸資料，則為「HTTP 應用程式」。
對等式應用程式	對等式應用程式的完整路徑與程序名稱 例如： D:\Program Files\BitTorrent\bittorrent.exe

通道	處理程序
PGP 加密	PGP 加密軟體的完整路徑與程序名稱 例如： `C:\Program Files\PGP Corporation\PGP Desktop\ PGPmnApp.exe`
印表機	開始印表機作業之應用程式的完整路徑與程序名稱 例如： `C:\Program Files\Microsoft Office\Office12\ WINWORD.EXE`
SMB 通訊協定	從中執行共享檔案存取（複製或建立新檔案）之應用程式的完整路徑與程序名稱 例如： `C:\Windows\Explorer.exe`
網路郵件（HTTP 模式）	「HTTP 應用程式」
網路郵件（HTTPS 模式）	瀏覽器或應用程式的完整路徑與程序名稱 例如： `C:\Program Files\Mozilla Firefox\firefox.exe`

資料外洩防護記錄檔詳細資料

「資料外洩防護記錄檔詳細資料」畫面顯示有關數位資產傳輸的其他詳細資料。傳輸的詳細資料會根據 Apex One 偵測事件所使用的通道和程序而有不同。

下表列出顯示的詳細資訊。

表 11-12. 資料外洩防護記錄檔詳細資料

詳細資料	說明
日期/時間	資料外洩防護記錄事件的日期和時間

詳細資料	說明
違規 ID	事件的唯一 ID
使用者	登入端點的使用者名稱
端點	資料外洩防護偵測到傳輸的端點的名稱
網域	端點的網域
IP	端點的 IP 位址
通道	傳輸發生所經由的通道
處理程序	促進傳輸數位資產的程序（程序視通道而定） 如需詳細資訊，請參閱依通道的處理程序 第 11-54 頁。
來源	包含數位資產的檔案來源或通道（如果沒有來源可用的話）
電子郵件寄件者	產生傳輸的電子郵件信箱
電子郵件主旨	包含數位資產的電子郵件訊息主旨行
電子郵件收件者	電子郵件訊息的目的電子郵件信箱
URL	網站或網頁的 URL
FTP 使用者	用來登入 FTP 伺服器的使用者名稱
檔案類別	資料外洩防護偵測到其中包含數位資產的檔案類型
規則/範本	觸發偵測的確切規則名稱和範本清單
處理行動	對傳輸採取的處理行動。
使用者理由	使用者為繼續傳輸敏感資料所提供的理由

啟動資料安全防護模組的偵錯記錄功能

步驟

1. 從支援供應商處取得 `logger.cfg` 檔案。

2. 將下列資料新增至 HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\DlpLite（32 位元系統）或 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\DlpLite（64 位元系統）：
   - 類型：字串
   - 名稱：debugcfg
   - 值：C:\Log\logger.cfg
3. 在 C:\ directory 目錄中建立名為「Log」的資料夾。“”
4. 將 logger.cfg 複製到 “Log” 資料夾。
5. 從 Web 主控台部署「資料外洩防護」和「周邊設備存取控管」設定，以開始收集記錄檔。

注意

透過刪除登錄機碼中的 debugcfg，然後重新啟動端點，以關閉資料安全防護模組的偵錯記錄功能。

第 12 章

使用網頁信譽評等

本章說明各種 Web-based 安全威脅，以及如何使用 Apex One 來保護網路和電腦不受 Web-based 安全威脅的侵襲。

包含下列主題：

關於網路安全威脅

網路安全威脅包含各式各樣源自 Internet 的威脅。網路安全威脅的方法十分巧妙，且結合運用多種檔案和技術，而非只有單一檔案或方式。例如，網路威脅創造者會持續變更所使用的版本或變體。因為網路安全威脅是位於固定的網站位置上而不是在中毒的 端點 上，所以網路安全威脅的製造者會持續修改其程式碼以躲避偵測。

近年來，被稱為駭客、病毒撰寫者、垃圾郵件寄件人和間諜程式設計者的個人統稱為網路罪犯。這些網路犯罪者利用網路安全威脅來遂行兩個目的之一。第一個目的是竊取資訊進行販賣。這樣會造成例如個人身分等機密資訊曝光。中毒 端點 可能也會成為網路釣魚攻擊或其他資訊竊取活動的媒介。在各種影響中，這種安全威脅可能會傷害網路商業活動的互信基礎，讓大家不能放心地進行 Internet 交易。第二個目的是綁架使用者電腦的 CPU 處理能力，做為從事獲利活動的工具。此處所謂獲利活動包括傳送垃圾郵件，利用分散式拒絕服務勒索受害者，或是利用受害者電腦點擊收費服務網頁。

Command & Control 聯絡人警訊服務

趨勢科技 Command & Control (C&C) 聯絡人警訊服務可提供加強的偵測和警訊功能，以減少進階持續性安全威脅及目標攻擊所造成的損害。C&C 聯絡人警訊服務與網頁信譽評等服務整合，後者可根據網頁信譽評等安全層級決定在偵測到回呼位址時採取的處理行動。

C&C IP 清單則使用網路內容檢測引擎進一步加強 C&C 回呼偵測，以識別透過任何網路通道的 C&C 聯絡人。

如需設定網頁信譽評等服務安全層級的詳細資訊，請參閱設定網頁信譽評等策略 第 12-5 頁。

表 12-1. C&C 聯絡人警訊服務功能

功能	說明
全球智慧清單	趨勢科技主動雲端截毒技術從全世界的各種來源編譯全球資訊清單，並測試和評估每個 C&C 回呼位址的風險等級。「網頁信譽評等服務」會將全球智慧清單搭配信譽評分用於惡意網站，以提供加強的安全性，遏止進階安全威脅。網頁信譽評等安全層級會根據指定的風險等級，決定對惡意網站或 C&C 伺服器採取的處理行動。
沙盒虛擬平台清單	主動雲端截毒技術伺服器可與沙盒虛擬平台整合，以取得沙盒虛擬平台 C&C 伺服器清單。沙盒虛擬平台可對安全環境中的潛在風險進行評估，並透過使用進階邏輯分析和行為測試方法來指定所分析安全威脅的風險等級。沙盒虛擬平台會在沙盒虛擬平台清單中填入嘗試連線到可能的 C&C 伺服器的任何安全威脅。沙盒虛擬平台清單高度特定於公司，可針對目標攻擊提供更自訂的防範。 Apex One 從沙盒虛擬平台擷取該清單，並可依據全球資訊和本地沙盒虛擬平台清單，評估所有可能的 C&C 安全威脅。 如需連線沙盒虛擬平台可疑物件清單的詳細資訊，請參閱設定可疑物件清單設定 第 14-32 頁。
可疑連線服務	可疑連線服務管理使用者定義的及全域 IP C&C 清單，並監控端點與潛在 C&C 伺服器之間連線的行為。 如需詳細資訊，請參閱可疑連線服務 第 8-5 頁。
管理員通知	管理員可以選擇在偵測到 C&C 回呼後接收詳細且可自訂的通知。 如需詳細資訊，請參閱設定給管理員的 C&C 回呼通知 第 12-12 頁。
用戶端通知	管理員可選擇在端點上偵測到 C&C 回呼後，將詳細且可自訂的通知傳送給終端使用者。 如需詳細資訊，請參閱用戶端使用者的 C&C 聯絡人警訊通知 第 12-15 頁。
病毒爆發通知	管理員可以自訂 C&C 回呼事件專用的病毒爆發通知，並指定病毒爆發是發生在單一端點上還是整個網路中。 如需詳細資訊，請參閱 C&C 回呼爆發 第 12-16 頁。
C&C 回呼記錄檔	記錄檔提供有關所有 C&C 回呼事件的詳細資訊。 如需詳細資訊，請參閱檢視 C&C 回呼記錄檔 第 12-20 頁。

網頁信譽評等

網頁信譽評等技術會依據諸如網站的存在時間長短、位置變更記錄，以及透過惡意程式行為分析所發現的可疑活動指標等因素來指定信譽評等評分，以追蹤 Web 網域的可信度。趨勢科技會持續分析網站並更新網頁信譽評等評分，以防止使用者存取潛在的惡意內容。

當使用者嘗試存取某個網站時，Security Agent 會查詢主動雲端截毒技術來源，以判斷網站內容的風險等級。Security Agent 中設定好的「網頁信譽評等」策略會決定是否允許使用者存取網站。

注意

如需有關主動雲端截毒伺服器來源的詳細資訊，請參閱主動雲端截毒技術來源清單 第 4-20 頁。

「網頁信譽評等」允許您將您認為安全或危險的網站新增到核可清單或封鎖清單。對於已新增到這些清單中的網站，Security Agent 不會查詢其網頁信譽評等評分，而是自動允許或封鎖存取。

網頁信譽評等策略

網頁信譽評等策略會指定 Apex One 是否要封鎖或允許對網站的存取。

您可以為內部和外部用戶端設定策略。Apex One 管理員通常會針對外部用戶端設定較嚴格的策略。

策略是 Apex One 用戶端樹狀結構中的詳細設定。您可以對用戶端群組或個別用戶端強制執行特定的策略。您也可以對所有用戶端強制執行單一策略。

部署策略之後，用戶端會使用您在「端點位置」畫面（請參閱端點位置 第 15-2 頁）中設定的位置條件來判斷其位置和要套用的策略。用戶端會在每次位置變更時切換策略。

設定網頁信譽評等策略

如果您已經設定 Proxy 伺服器來處理組織中的 HTTP 通訊，而且必須經過驗證才能存取 Web，請指定 Proxy 伺服器驗證憑證。

如需詳細資訊，請參閱設定外部用戶端 Proxy 設定 第 15-45 頁。

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中選取目標。
3. 請點選「設定 > 網頁信譽評等設定」。
4. 請點選「外部用戶端」標籤以設定外部用戶端的策略，或請點選「內部用戶端」標籤以設定內部用戶端的策略。

   秘訣

   設定用戶端位置設定（如果您尚未這樣做）。用戶端將使用這些設定判定自己的位置，然後套用正確的網頁信譽評等策略。如需詳細資訊，請參閱端點位置 第 15-2 頁。

5. 在「請在下列作業系統啟動網頁信譽評等」下方，選取要保護的 Windows 平台類型（「Windows 桌上型電腦平台」和「Windows Server 平台」）。

   秘訣

   如果您已經使用含有網頁信譽評等功能的趨勢科技產品（例如 InterScan Web Security Virtual Appliance），趨勢科技建議您對內部用戶端關閉網頁信譽評等。

   啟動網頁信譽評等策略時：

   - 您只能將內部的內部部署 Security Agent 設定為將網頁信譽評等查詢傳送至本機的主動雲端截毒技術伺服器。

- 內部用戶端會傳送網頁信譽評等查詢至：
  - 主動雲端截毒技術伺服器，如果啟動了「傳送查詢至主動雲端截毒技術伺服器」選項。
  - 主動雲端截毒技術，如果關閉了「傳送查詢至主動雲端截毒技術伺服器」選項。

6. 選取「啟動評估模式」。

注意

處於評估模式時，Security Agent 會允許存取所有網站。如果存取的任何網站違反所設定的「安全層級」設定，Security Agent 會記錄此事件。評估模式可讓您監控網站存取，以便在主動封鎖使用者存取之前評估網站的安全性。在您評估存取記錄檔之後，您可以將信任的網站新增到「核可的 URL 清單」中，然後再關閉評估模式。

---

7. 選取「檢查 HTTPS URL」。

重要

HTTPS URL 掃瞄也支援 HTTP/2 通訊協定。您必須針對不同的瀏覽器設定某些必要設定，網頁信譽評等才能檢查 HTTPS 或 HTTP/2 URL。

如需詳細資訊，請參閱 HTTPS URL 掃瞄支援 第 12-9 頁。

---

8. 請針對內部 Security Agent 選取「傳送查詢至主動雲端截毒技術伺服器」（如果您希望 Security Agent 將網頁信譽評等查詢傳送至主動雲端截毒技術伺服器）。
   - 如果您啟動此選項：
     - 用戶端會參考主動雲端截毒技術伺服器來源清單，判斷應該將查詢傳送至哪些主動雲端截毒技術伺服器。

       如需有關主動雲端截毒技術來源的詳細資訊，請參閱主動雲端截毒技術來源清單 第 4-20 頁。
     - 請確定主動雲端截毒技術伺服器呈運行狀態。如果主動雲端截毒技術伺服器全都無法使用，用戶端便不會將查詢傳送至主動雲端截毒技術。其餘的用戶端網頁信譽評等資料來源為核可和封鎖的 URL 清單。

- 如果您希望 用戶端 透過 Proxy 伺服器來連線主動雲端截毒技術伺服器，請在「管理 > 設定 > Proxy 伺服器 > 用戶端」標籤上的「內部 Proxy 伺服器」區段中指定 Proxy 伺服器設定。
- 請確定定期更新主動雲端截毒技術伺服器，以確保防護保持在最新狀態。
- 用戶端不會封鎖未測試的網站。主動雲端截毒技術伺服器不會儲存這些網站的網頁信譽評等資料。

- 如果您關閉此選項：
  - 用戶端會將網頁信譽評等查詢傳送至主動雲端截毒技術。端點必須連線至 Internet 才能成功傳送查詢。
  - 如果與主動雲端截毒技術的連線需要 Proxy 伺服器驗證，請在「管理 > 設定 > Proxy 伺服器> 用戶端（標籤） > 外部 Proxy 伺服器」中指定驗證認證。
  - 如果您選取「封鎖尚未經由趨勢科技測試的網頁」選項，用戶端會封鎖未測試網站。

9. 選取可用的網頁信譽評等安全層級：「高」、「中」或「低」

   注意

   安全層級決定網頁信譽評等會允許還是封鎖對 URL 的存取。例如，如果您將安全層級設定為「低」，網頁信譽評等只會封鎖已知為網路安全威脅的 URL。設定較高的安全層級可提高網路安全威脅偵測率，但誤判的可能性也會提高。

10. 如果您關閉了「傳送查詢至主動雲端截毒技術伺服器」選項，您可以選取「封鎖尚未經由趨勢科技測試的網頁」。

    注意

    雖然趨勢科技會主動測試網頁以確保安全，但使用者仍可能會在造訪新的或較不熱門的網站時遇到未測試的網頁。封鎖對於未測試網頁的存取，可以提高安全，但也會讓人無法存取某些安全的網頁。

11. 選取「封鎖包含惡意程式檔的網頁」以識別網路瀏覽器弱點攻擊和惡意程式檔，並避免使用這些威脅入侵網路瀏覽器。

網頁信譽評等同時利用瀏覽器弱點攻擊防護特徵碼和程式檔分析器病毒碼，在系統受到入侵之前識別並封鎖網頁。

重要

- 瀏覽器弱點攻擊防護功能支援 Internet Explorer、Microsoft Edge Legacy、Microsoft Edge Chromium、Mozilla Firefox 及 Chrome 等瀏覽器。
- 瀏覽器弱點攻擊防護功能需要您啟動「進階防護服務」。

重要

瀏覽器弱點攻擊防護功能需要您啟動「進階防護服務」。

如果要啟動進階防護服務，請移至「用戶端 > 用戶端管理」，然後點選「設定 > 其他服務設定」。

在 Security Agent 上首次啟動瀏覽器弱點攻擊防護之後，使用者必須在瀏覽器中啟動必要的附加元件，瀏覽器弱點攻擊防護才能正常運作。針對執行 Internet Explorer 9、10 或 11 的 Security Agent，使用者必須在瀏覽器快顯視窗中啟動 `Trend Micro IE Protection` 附加元件。

12. 設定核可和封鎖的清單。

注意

核可清單優先於封鎖的清單。當 URL 與核可清單中的項目相符時，用戶端會一律允許存取該 URL，即使該 URL 列在封鎖清單中也一樣。

a. 選取「啟動核可/封鎖清單」。

b. 輸入 URL。

   您可在 URL 中的任何位置加入萬用字元 (*)。

   例如：

   - 輸入 `www.trendmicro.com/*` 表示網頁信譽評等核可趨勢科技網站中的所有網頁。
   - 輸入 `*.trendmicro.com/*` 表示網頁信譽評等核可 `trendmicro.com` 的任何子網域中的所有網頁。

您可以輸入包含 IP 位址的 URL。如果 URL 包含 IPv6 位址，請使用括號將位址括起來。

c. 請點選「新增到核可清單」或「新增到封鎖清單」。

d. 如果要將清單匯出為 .dat 檔案，請點選「匯出」，再請點選「儲存」。

e. 如果您已從其他伺服器匯出清單，而想要將此清單匯入此畫面，請點選「匯入」，然後尋找 .dat 檔案。此清單會載入至畫面上。

重要

網頁信譽評等不會對核可及封鎖清單中的位址執行任何掃瞄。

13. 如果要送出網頁信譽評等的意見反應，請點選「重新評估 URL」下提供的 URL。系統會在瀏覽器視窗中開啟趨勢科技網頁信譽評等查詢系統。

14. 選取是否允許 Security Agent 將網頁信譽評等記錄檔傳送至伺服器。如果您想分析網頁信譽評等封鎖的 URL，並針對您認為可以安全存取的 URL 採取合適的處理行動，請允許用戶端傳送記錄檔。

15. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

- 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
- 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

HTTPS URL 掃瞄支援

HTTPS 通訊使用憑證來識別 Web 伺服器。它會將資料加密以防止盜取及竊聽。雖然使用 HTTPS 存取網站的安全性較高，但仍存在風險。即使網站具有有效的憑證，一旦遭到入侵，便會裝載惡意程式並竊取個人資訊。此外，由於憑證相當容易取得，很輕易就能架設使用 HTTPS 的惡意 Web 伺服器。

重要

Internet Explorer 的 HTTPS 掃瞄僅支援以桌面模式運作的 Windows 8.1（或更新版本）和 Windows Server 2012（或更新版本）平台。

啟動 HTTPS URL 檢查，以減少接觸雖使用 HTTPS 卻已遭到入侵或惡意的網站。網頁信譽評等可以監控下列瀏覽器上的 HTTPS 流量：

表 12-2. 支援 HTTPS 流量的瀏覽器

瀏覽器	版本	先決條件
Microsoft Internet Explorer	8.x	最新版本
	9.x	使用者必須在瀏覽器快顯視窗中啟動 `Trend Micro Osprey Plugin Class` 附加元件。
	10.x	
	11.x	
Mozilla Firefox	3.5 或更新版本	無
Chrome	最新版本	
Microsoft Edge	• 舊版 • Chromium	

如需有關針對網頁信譽評等設定 Internet Explorer 設定的詳細資訊，請參閱下列常見問題集文章：

- https://success.trendmicro.com/tw/solution/1060643
- https://success.trendmicro.com/tw/solution/1095350

給用戶端使用者的網路安全威脅通知

Apex One 封鎖違反網頁信譽評等策略的 URL 之後，會立即在 Security Agent 端點上顯示通知訊息。您可以啟動通知訊息，並視需要修改通知訊息的內容。

啟動網路安全威脅通知訊息

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 權限和其他設定」。
4. 請點選「其他設定」標籤。
5. 在「網頁信譽評等設定」區段下，選取「當網站被封鎖時顯示通知」。
6. 在「C&C 回呼設定」區段中，選取「偵測到 C&C 回呼時顯示通知」。
7. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

修改網路安全威脅通知

步驟

1. 移至「管理 > 通知 > 用戶端」。
2. 從「類型」下拉式清單中，選取要修改的網路安全威脅通知：
   - 網頁信譽評等違規
   - C&C 回呼

3. 在提供的文字方塊中修改預設訊息。

4. 請點選「儲存」。

給管理員的 C&C 回呼通知

Apex One 隨附一組預設通知訊息，用於向您和其他 Apex One 管理員通知 C&C 回呼偵測情況。您可以視需要修改通知和設定其他通知設定。

設定給管理員的 C&C 回呼通知

步驟

1. 移至「管理 > 通知 > 管理員」。

2. 在「條件」標籤上：

   a. 移至「C&C 回呼」區段。

   b. 指定是在 Apex One 偵測到 C&C 回呼（處理行動可以是封鎖或記錄）時傳送通知，還是僅當回呼位址的風險等級為「高」時才傳送通知。

3. 在「電子郵件」標籤上：

   a. 移至「C&C 回呼」區段。

   b. 選取「啟動電子郵件通知」。

   c. 選取「傳送通知給具有用戶端樹狀結構網域權限的使用者」。

      使用以角色為基礎的管理，將用戶端樹狀結構網域權限授與使用者。如果在屬於特定網域的用戶端上進行傳輸，系統會將電子郵件傳送給具網域權限之使用者的電子郵件信箱。如需範例，請參閱下表：

表 12-3. 用戶端樹狀結構網域和權限

用戶端樹狀結構網域	具有網域權限的角色	具有該角色的使用者帳號	使用者帳號的電子郵件信箱
網域 A	Administrator（內建）	root	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
網域 B	Administrator（內建）	root	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

如果屬於網域 A 的任何 Security Agent 偵測到 C&C 回呼，系統便會向 mary@xyz.com、john@xyz.com 和 chris@xyz.com 傳送電子郵件。

如果屬於網域 B 的任何 Security Agent 偵測到 C&C 回呼，系統便會向 mary@xyz.com 和 jane@xyz.com 傳送電子郵件。

注意

啟動此選項時，具網域權限的所有使用者都必須有一個對應的電子郵件信箱。電子郵件通知不會傳送給沒有電子郵件信箱的使用者。使用者和電子郵件信箱是從「管理 > 帳號管理 > 使用者帳號」設定的。

d. 選取「傳送通知到下列電子郵件信箱」，然後輸入電子郵件信箱。

e. 接受或修改預設的主旨和訊息。使用 Token 變數代表「主旨」和「訊息」欄位中的資料。

表 12-4. C&C 回呼通知的 Token 變數

變數	說明
%CLIENTCOMPUTER%	傳送回呼的目標端點
%IP%	目標端點 IP 位址

變數	說明
%DOMAIN%	端點網域
%DATETIME%	偵測到傳輸的日期和時間
%CALLBACKADDRESS%	C&C 伺服器的回呼位址
%CNCRISKLEVEL%	C&C 伺服器的風險等級
%CNCLISTSOURCE%	代表 C&C 來源清單
%ACTION%	已執行的中毒處理行動

4. 在「SNMP Trap」標籤中：
   a. 移至「C&C 回呼」區段。
   b. 選取「啟動 SNMP Trap 通知」。
   c. 接受或修改預設的訊息。使用 Token 變數代表「訊息」欄位中的資料。如需詳細資訊，請參閱表 12-4：C&C 回呼通知的 Token 變數 第 12-13 頁。
5. 在「NT 事件記錄檔」標籤中：
   a. 移至「C&C 回呼」區段。
   b. 選取「啟動 NT 事件記錄檔通知」。
   c. 接受或修改預設的訊息。您可以使用 Token 變數代表「訊息」欄位中的資料。如需詳細資訊，請參閱表 12-4：C&C 回呼通知的 Token 變數 第 12-13 頁。
6. 請點選「儲存」。

用戶端使用者的 C&C 聯絡人警訊通知

Apex One 可以在封鎖某個 C&C 伺服器 URL 後，立即在 Security Agent 電腦上顯示通知訊息。您需要啟動通知訊息，並可選擇性地修改通知訊息的內容

啟動 C&C 回呼通知訊息

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 權限和其他設定」。
4. 請點選「其他設定」標籤。
5. 在「C&C 聯絡人警訊設定」區段中，選取「偵測到 C&C 回呼時顯示通知」。
6. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

修改 C&C 回呼通知

步驟

1. 移至「管理 > 通知 > 用戶端」。
2. 從「類型」下拉式清單中，選取「C&C 回呼」。
3. 在提供的文字方塊中修改預設訊息。
4. 請點選「儲存」。

C&C 回呼爆發

依回呼數目、來源和風險等級定義 C&C 回呼爆發。

Apex One 具有預設通知訊息，可在偵測到爆發時，通知您和其他 Apex One 管理員。您可以視需要修改通知訊息。

注意

Apex One 可以透過電子郵件傳送 C&C 回呼病毒爆發通知。設定電子郵件設定，讓 Apex One 可以成功地傳送電子郵件。如需詳細資訊，請參閱管理員通知設定 第 14-35 頁。

設定 C&C 回呼爆發條件和通知

步驟

1. 移至「管理 > 通知 > 病毒爆發」。

   會出現「病毒爆發通知」畫面。

2. 在「條件」標籤上的「C&C 回呼」區段中，設定下列項目：

選項	說明
同一部遭到入侵的主機	選取以根據每個端點的回呼偵測定義病毒爆發
C&C 風險等級	指定要針對所有 C&C 回呼，還是僅針對高風險來源觸發病毒爆發
處理行動	指定 Apex One 計數哪些處理行動來判斷病毒爆發狀況
偵測	指定必須超過多少偵測次數，Apex One 才會觸發病毒爆發狀況
時間範圍	指定監控期間

3. 在「電子郵件」標籤上：

   a. 在「C&C 回呼」區段中，選取「啟動電子郵件通知」。

   b. 在「收件人」欄位旁指定電子郵件收件者。

   c. 指定要在電子郵件通知中使用的「主旨」。

   d. 指定「訊息」內容。

      Apex One 支援在「主旨」和「訊息」欄位中使用 Token。

      表 12-5. C&C 回呼病毒爆發通知的 Token 變數

變數 Token	說明
%C	C&C 回呼記錄檔的數目
%T	C&C 回呼記錄檔累計的時間範圍

   e. 指定您要包含在通知中的任何其他記錄檔資料（採用表列方式）。

「記錄檔」欄	說明
日期/時間	偵測的日期和時間
遭到入侵的主機	偵測所在端點
IP 位址	遭到入侵的主機 IP 位址

「記錄檔」欄	說明
網域	發生偵測之端點的網域
回呼位址	觸發偵測的 URL
C&C 風險等級	回呼位址的風險等級
C&C 清單來源	辨識 C&C 伺服器的 C&C 清單來源
處理行動	針對安全威脅執行的處理行動

4. 在「SNMP Trap」標籤中：
   a. 移至「C&C 回呼」區段。
   b. 選取「啟動 SNMP Trap 通知」。
   c. 接受或修改預設的訊息。您可以使用 Token 變數代表「訊息」欄位中的資料。如需詳細資訊，請參閱表 12-5：C&C 回呼病毒爆發通知的 Token 變數 第 12-17 頁。
5. 在「NT 事件記錄檔」標籤中：
   a. 移至「C&C 回呼」區段。
   b. 選取「啟動 NT 事件記錄檔通知」。
   c. 接受或修改預設的訊息。您可以使用 Token 變數代表「訊息」欄位中的資料。如需詳細資訊，請參閱表 12-5：C&C 回呼病毒爆發通知的 Token 變數 第 12-17 頁。
6. 請點選「儲存」。

網路安全威脅記錄檔

設定內部和外部用戶端以同時傳送網頁信譽評等記錄檔到伺服器。如果您要分析 Apex One 所封鎖的 URL，並對您認為可安全存取的 URL 採取適當的處理行動，便可以這麼做。

如果要避免記錄檔佔去過多硬碟空間，請手動刪除記錄檔或設定記錄檔刪除預約時程。如需有關管理記錄檔的詳細資訊，請參閱記錄檔管理 第 14-39 頁。

檢視網頁信譽評等記錄檔

步驟

1. 移至下列其中一個項目：
   - 記錄檔 > 用戶端 > 安全威脅
   - 用戶端 > 用戶端管理
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請移至「網頁信譽評等記錄檔條件」畫面：
   - 在「安全威脅記錄檔」畫面中，點選「檢視記錄檔 > 網頁信譽評等記錄檔」。
   - 在「用戶端管理」畫面中，點選「記錄檔 > 網頁信譽評等記錄檔」。
4. 指定記錄條件，然後請點選「顯示記錄檔」。
5. 檢視記錄檔。記錄檔包含下列資訊：

項目	說明
日期/時間	發生偵測的時間
端點	發生偵測的端點
網域	發生偵測之端點的網域
URL	網頁信譽評等服務封鎖的 URL
風險等級	URL 的風險等級
說明	安全威脅的說明

項目	說明
處理程序	嘗試聯絡時所使用的程序 (path\application_name)
處理行動	偵測時採取的處理行動

6. 請點選「新增到核可的清單」，將您不想封鎖的 URL 新增到「核可的 URL」清單中。
7. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請點選「全部匯出到 CSV」。開啟檔案或將其儲存至特定位置。

檢視 C&C 回呼記錄檔

步驟

1. 移至下列其中一個項目：
   - 記錄檔 > 用戶端 > 安全威脅
   - 用戶端 > 用戶端管理
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 移至「C&C 回呼記錄檔條件」畫面：
   - 在「安全威脅記錄檔」畫面中，點選「檢視記錄檔 > C&C 回呼記錄檔」。
   - 在「用戶端管理」畫面中，點選「記錄檔 > C&C 回呼記錄檔」。
4. 指定記錄條件，然後請點選「顯示記錄檔」。
5. 檢視記錄檔。記錄檔包含下列資訊：

項目	說明
日期/時間	發生偵測的時間

項目	說明
使用者	偵測時已登入的使用者
遭到入侵的主機	產生回呼的端點
IP 位址	遭到入侵的主機的 IP 位址
網域	發生偵測之端點的網域
回呼位址	端點將回呼傳送到的位址
C&C 清單來源	辨識 C&C 伺服器的 C&C 清單來源
C&C 風險等級	C&C 伺服器的風險等級
通訊協定	用於傳輸的 Internet 通訊協定
處理程序	開始傳輸的處理程序 (path\application_name)
處理行動	偵測時採取的處理行動

6. 如果網頁信譽評等封鎖了您不想封鎖的 URL，請點選「新增到網頁信譽評等核可清單」按鈕，將該位址新增到網頁信譽評等核可清單。

注意

Apex One 只能將 URL 新增到網頁信譽評等核可清單。對於由全域 C&C IP 清單或沙盒虛擬平台 (IP) C&C 清單進行的偵測，請手動將這些 IP 位址新增到使用者定義的核可 C&C IP 清單。

如需詳細資訊，請參閱設定全域使用者定義的 IP 清單設定 第 8-6 頁。

7. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請點選「全部匯出到 CSV」。開啟檔案或將其儲存至特定位置。

第 13 章

使用 Apex One 防火牆

本章說明 Apex One 防火牆功能和組態設定。

包含下列主題：

關於 Apex One 防火牆

Apex One 防火牆使用狀態檢測和高效能網路病毒掃瞄，來保護網路上的 Security Agent 和伺服器。透過中央管理主控台，您就可以建立規則，依據應用程式、IP 位址、通訊埠號碼或通訊協定過濾連線，然後將規則套用至不同的使用者群組。

Apex One 防火牆包含下列主要功能和優點：

傳輸過濾

Apex One 防火牆會過濾所有輸入和輸出，提供根據下列條件封鎖特定傳輸類型的能力：

- 方向（輸入/輸出）
- 通訊協定 (TCP/UDP/ICMP/ICMPv6)
- 目標通訊埠
- 來源和目標端點

應用程式過濾

Apex One 防火牆會過濾防火牆例外清單中指定之應用程式的輸入和輸出，允許這些應用程式存取網路。網路連線的可用性視管理員設定的策略而定。

認證安全防護軟體清單

本機「認證安全防護軟體清單」列出可略過防火牆策略安全層級的應用程式清單。Apex One 防火牆會自動允許「認證安全防護軟體清單」中的程式執行及存取網路。

您也可以允許 Security Agent 查詢動態更新的全域「認證安全防護軟體清單」（保存在趨勢科技伺服器上）。

重要

必須同時啟動「未經授權的變更阻止服務」和「認證安全防護軟體服務」，才能查詢全域「認證安全防護軟體清單」。

掃瞄網路病毒

Apex One 防火牆也會檢查每個封包是否有網路病毒。如需詳細資訊，請參閱病毒和惡意程式 第 7-2 頁。

可自訂的資料檔和策略

Apex One 防火牆可讓您將策略設為封鎖或允許指定的網路傳輸類型。您可以指定策略到一或多個資料檔，然後將資料檔部署到指定的 Security Agent。這是一種高度自訂的組織和設定用戶端防火牆設定的方法。

狀態檢測

Apex One 防火牆會使用狀態檢測來監控所有與 Security Agent 的連線，並記憶所有連線狀態。Apex One 防火牆可識別任何連線的特定狀況、預測應該採用的處理行動，並偵測一般連線的中斷情況。因此，有效地使用防火牆不僅需要建立資料檔和策略，還需要分析連線和過濾通過防火牆的封包。

入侵偵測系統

入侵偵測系統 (IDS) 有助於在指出端點上可能遭到攻擊的網路封包中識別病毒碼。

入侵偵測系統 (IDS) 有助於防止下列眾所周知的入侵行為：

入侵	說明
Too Big Fragment	一種「拒絕服務」攻擊，其中駭客會將過大的 TCP/UDP 封包導向目標端點。這會造成緩衝區溢位而凍結或重新啟動端點。
Ping of Death	一種「拒絕服務」攻擊，其中駭客會將過大的 ICMP/ICMPv6 封包導向目標端點。這會造成緩衝區溢位而凍結或重新啟動端點。
Conflicted ARP	一種攻擊類型，其中駭客會傳送具有相同來源和目標 IP 位址的「位址解析通訊協定」(ARP) 要求給目標端點。目標端點持續將 ARP 回應（其 MAC 位址）傳送給自己，使端點凍結或當機。
SYN Flood	一種「拒絕服務」攻擊，其中程式會將多個 TCP 同步化 (SYN) 封包傳送到端點，造成端點持續傳送同步化確認 (SYN/ACK) 回應。這樣會耗盡端點記憶體，最後造成端點當機。
Overlapping Fragment	類似於 Teardrop 攻擊，這種「拒絕服務」攻擊會將重疊的 TCP 片段傳送到端點。這會覆寫第一個 TCP 片段中的標題資訊，且有可能通過防火牆。防火牆可能接著會允許包含惡意程式碼的後續片段通過而到達目標端點。
Teardrop	類似於重疊片段攻擊，這種「拒絕服務」攻擊與 IP 片段有關。位於第二或其後 IP 片段的混淆偏移值可能會造成接收端點上的作業系統在嘗試重組片段時當機。

入侵	說明
Tiny Fragment Attack	一種攻擊類型，其中小型 TCP 片段會迫使第一項 TCP 封包標題資訊到下一個片段中。這樣會造成負責過濾流量的路由器忽略後續片段，而其中可能含有惡意資料。
Fragmented IGMP	一種「拒絕服務」攻擊，會將片段式 IGMP 封包傳送到目標端點，而此電腦無法正確處理 IGMP 封包。這樣會凍結或拖慢端點速度。
LAND Attack	一種攻擊類型，會將具有相同來源和目標位址的 IP 同步化 (SYN) 封包傳送給端點，造成端點將同步化確認 (SYN/ACK) 回應傳送給自己。這樣會凍結或拖慢端點速度。

防火牆違規病毒爆發監控

當防火牆違規事件超過特定門檻值時，Apex One 防火牆會傳送自訂通知訊息給指定收件者，發出攻擊通知。

Security Agent 防火牆權限

授與 Security Agent 使用者在 Security Agent 主控台上檢視其防火牆設定的權限。也可以授與使用者啟動或關閉防火牆、入侵偵測系統和防火牆違規通知訊息的權限。

啟動或關閉 Apex One 防火牆

在安裝 Apex One 伺服器期間，系統會提示您啟動或關閉 Apex One 防火牆。

如果已在安裝期間啟動防火牆，並發現效能受到影響（特別是在 Windows Server 平台上），請考慮關閉防火牆。

如果已在安裝期間關閉防火牆，但現在想要啟動防火牆以保護用戶端免於遭受入侵，請先閱讀 Security Agent 服務 第 15-6 頁中的指導方針和指示。

您可以在所有或選取的 Security Agent 端點上啟動或關閉防火牆。

使用下列方法之一在 Web 主控台上啟動或關閉防火牆。

方法	程序
啟動/關閉所有 Security Agent 上的 Apex One 防火牆	使用「全域用戶端設定」設定所有 Security Agent 上的 Apex One 防火牆服務。 如需詳細資訊，請參閱設定全域防火牆設定 第 13-22 頁。 **注意** 關閉 Apex One 防火牆時，會自動關閉所有 Security Agent 上的全部防火牆策略。
從 Web 主控台啟動/關閉防火牆服務	使用「其他服務設定」設定所選 Security Agent 上的 Apex One 防火牆服務。 如需詳細資訊，請參閱 Security Agent 服務 第 15-6 頁。 **注意** 關閉防火牆服務會自動關閉所選用戶端上的所有防火牆政策。
建立新策略並將它套用到 Security Agent	1. 建立可啟動/關閉防火牆的新策略。 如需建立新策略的步驟，請參閱新增防火牆策略 第 13-9 頁。 2. 將該策略套用到 Security Agent。

防火牆策略和資料檔

Apex One 防火牆使用策略和資料檔來組織和自訂防護網路端點的方法。

透過 Active Directory 整合和以角色為基礎的管理，每個使用者角色（視其權限而定）都可以建立、設定或刪除特定網域的策略和資料檔。

秘訣

在同一端點上安裝多個防火牆可能會產生無法預期的結果。請考慮在部署和啟動 Apex One 防火牆之前，先解除安裝 Security Agent 上的其他軟體型防火牆應用程式。

下列為成功使用 Apex One 防火牆的必要步驟：

1. 建立策略。策略可讓您選取安全層級以封鎖或允許在網路端點之間的傳輸，以及啟動防火牆功能。
2. 新增例外至策略。例外可讓 Security Agent 脫離策略的限制。有了例外規則，您便可指定用戶端並允許或封鎖某些傳輸類型，而不受策略中安全層級設定的限制。例如，可以針對策略中的一組用戶端封鎖其所有流量，但建立允許 HTTP 流量的例外，如此用戶端便可存取 Web 伺服器。
3. 建立和指定資料檔給 Security Agent。防火牆資料檔包含一組用戶端屬性並與策略關聯。當任何用戶端符合資料檔中指定的屬性時，就會觸發相關聯的策略。

防火牆策略

Apex One 防火牆策略可讓您封鎖或允許未在策略例外中指定的特定網路傳輸類型。策略也會定義啟動或關閉哪些 Apex One 防火牆功能。將策略指定給一或多個防火牆資料檔。

透過 Active Directory 整合和以角色為基礎的管理，每個使用者角色（視其權限而定）都可以建立、設定或刪除特定網域的策略。

下表簡述設定防火牆策略時可用的設定。

設定	說明
安全層級	用於封鎖或允許 Security Agent 上所有輸入和（或）輸出流量的一般設定 端點

設定	說明
防火牆功能	指定要啟動還是關閉 Apex One 防火牆、入侵偵測系統 (IDS) 和防火牆違規事件通知訊息。 如需詳細資訊，請參閱入侵偵測系統 第 13-4 頁。
認證安全防護軟體清單	指定是否允許認證安全的應用程式連線到網路。 如需詳細資訊，請參閱認證安全防護軟體清單 第 13-3 頁。
策略例外清單	封鎖或允許不同網路傳輸類型的可設定例外清單

注意

您也可以在建立防火牆資料檔時授與使用者權限，讓他們可以修改安全層級與策略例外清單。

如需詳細資訊，請參閱新增防火牆資料檔 第 13-18 頁。

預設防火牆策略

Apex One 隨附一組預設策略，您可以視需要進行修改或刪除。

策略名稱	安全層級	用戶端設定	例外	建議用法
「全部存取」策略	低	啟動防火牆	無	用於允許用戶端對網路有不受限制的存取權
Trend Micro Apex Central 通訊埠	低	啟動防火牆	允許通過通訊埠 80 和 10319 的所有輸入和輸出 TCP/UDP 傳輸	用於當用戶端有安裝 MCP 用戶端時
ScanMail for Microsoft Exchange 主控台	低	啟動防火牆	允許通過通訊埠 16372 的所有輸入和輸出 TCP 傳輸	用於當用戶端需要存取 ScanMail 主控台時
InterScan Messaging Security Suite 主控台	低	啟動防火牆	允許通過通訊埠 80 的所有輸入和輸出 TCP 傳輸	用於當用戶端需要存取 IMSS 主控台時

新增防火牆策略

步驟

1. 移至用戶端 > 防火牆 > 策略。
2. 如果要新增策略，請點選「新增」。

   如果您要建立的新策略與現有策略具有類似的設定，請選取現有的策略，並請點選「複製」。
3. 輸入策略名稱。
4. 選取安全層級。

   選定的安全層級不套用於例外清單中的通訊埠。
5. 選取要用於策略的防火牆功能。
   - 當防火牆封鎖輸出封包時，會顯示防火牆違規通知訊息。如果要修改該訊息，請參閱修改防火牆通知訊息的內容 第 13-25 頁。
   - 如果管理員啟動所有防火牆功能，並授與 Security Agent 使用者進行防火牆設定的權限，則使用者可在 Security Agent 主控台中啟動/關閉這些功能及修改防火牆設定。

     警告!

     您無法使用 Apex One Web 主控台覆寫使用者所設定的 Security Agent 主控台設定。
   - 如果您並未啟動防火牆功能，則從 Apex One Web 主控台設定的防火牆設定會顯示在 Security Agent 主控台的「網路卡清單」下。
   - Security Agent 主控台「防火牆」標籤上「設定」下的資訊一律會反映從 Security Agent 主控台（而不是伺服器 Web 主控台）所設定的設定。
6. 啟動本機或全域的「認證安全防護軟體清單」。

注意

請務必在啟動此服務之前，先啟動「未經授權的變更阻止服務」和「認證安全防護軟體服務」。

7. 從「例外」下選取防火牆策略例外。此處所含的策略例外是以防火牆例外範本為基礎。如需詳細資訊，請參閱編輯防火牆例外範本 第 13-11 頁。

   - 可以請點選策略例外名稱，然後在開啟的頁面中變更其設定，以修改現有策略例外。

     注意

     已修改的策略例外只會套用到要建立的策略。如果您希望策略例外修改永久有效，就必須對防火牆例外範本中的策略例外進行相同的修改。

   - 請點選「新增」以建立新策略例外。在開啟的頁面中指定其設定。

     注意

     策略例外只會套用到要建立的策略。如果要套用此策略例外到其他策略，您就必須先將其新增到防火牆例外範本中的策略例外清單內。

8. 請點選「儲存」。

修改現有的防火牆策略

步驟

1. 移至用戶端 > 防火牆 > 策略。
2. 請點選某個策略。
3. 修改下列項目：
   - 策略名稱
   - 安全層級

- 要用於策略的防火牆功能
- 認證安全防護軟體服務清單狀態
- 要加入策略中的防火牆策略例外
  - 編輯現有策略例外（請點選策略例外名稱，並在開啟的頁面中變更設定）
  - 請點選「新增」以建立新策略例外。在開啟的頁面中指定其設定。

4. 請點選「儲存」將修改套用到現有策略。

編輯防火牆例外範本

防火牆例外範本包含策略例外，您可以設定這些例外，以根據 Security Agent 端點的通訊埠號碼和 IP 位址來允許或封鎖各種網路傳輸。建立策略例外之後，請編輯要套用策略例外的策略。

決定您要使用哪一類型的策略例外。策略例外分為下列兩種類型：

- 限制的

  只會封鎖特定類型的網路傳輸，並套用至允許所有網路傳輸的策略。限制策略例外的用途範例為封鎖容易受到攻擊的 Security Agent 通訊埠（例如：特洛伊木馬程式經常使用的通訊埠）。

- 允許的

  只會允許特定類型的網路傳輸，並套用至封鎖所有網路傳輸的策略。例如，您可能只想允許 Security Agent 存取 Apex One 伺服器和 Web 伺服器。如果要這樣做，請允許信任的通訊埠（用於與 Apex One 伺服器通訊的通訊埠）和 Security Agent 於 HTTP 通訊所用通訊埠的傳輸。

  Security Agent 監聽通訊埠：用戶端 > 用戶端管理 > 狀態。通訊埠號碼會列在「基本資訊」下。

  伺服器監聽通訊埠：管理 > 設定 > 用戶端連線。通訊埠號碼會列在「用戶端連線設定」下。

Apex One 隨附一組預設防火牆策略例外，您可以視需要進行修改或刪除。

表 13-1. 預設防火牆策略例外規則

例外名稱	處理行動	通訊協定	通訊埠	方向
DNS	允許	TCP/UDP	53	輸入和輸出
NetBIOS	允許	TCP/UDP	137, 138, 139, 445	輸入和輸出
HTTPS	允許	TCP	443	輸入和輸出
HTTP	允許	TCP	80	輸入和輸出
Telnet	允許	TCP	23	輸入和輸出
SMTP	允許	TCP	25	輸入和輸出
FTP	允許	TCP	21	輸入和輸出
POP3	允許	TCP	110	輸入和輸出
LDAP	允許	TCP/UDP	389	輸入和輸出

注意

預設例外會套用至所有用戶端。如果要讓預設例外只套用到特定用戶端，請編輯該例外，並指定用戶端的 IP 位址。

如果您是從舊版 Apex One 升級，則無法使用 LDAP 例外。如果在例外清單中並未看到此例外項目，請手動將其新增。

新增防火牆策略例外

新增例外時，請確保未封鎖用於在 Apex One 伺服器與 Security Agent 之間通訊的通訊埠。

您可以使用以下方法來找到 Apex One 伺服器與 Security Agent 所用的監聽通訊埠：

- 伺服器監聽通訊埠：請移至「OSCE 用戶端連線設定」管理 > 設定 > 用戶端連線。通訊埠號碼會列在「用戶端連線設定」下。
- Security Agent 監聽通訊埠：請移至「OSCE 用戶端樹狀結構」用戶端 > 用戶端管理>「狀態」。通訊埠號碼會列在「基本資訊」下。

步驟

1. 移至「用戶端 > 防火牆 > 策略」。
2. 請點選「編輯例外範本」。
3. 請點選「新增」。
4. 輸入策略例外的名稱。
5. 選取應用程式的類型。您可以選取所有應用程式，或者指定應用程式路徑或登錄機碼。

   注意

   檢查所輸入的名稱和完整路徑。應用程式例外不支援萬用字元。

6. 選取 Apex One 對網路傳輸執行的處理行動（封鎖或允許符合例外條件的傳輸）和傳輸方向（Security Agent 端點上的輸入或輸出網路傳輸）。
7. 選取網路通訊協定的類型：TCP、UDP、ICMP 或 ICMPv6。
8. 指定要對 Security Agent 端點上的哪些通訊埠執行處理行動。
9. 選取要加入例外的 Security Agent 端點 IP 位址。

   例如，如果您選擇拒絕所有網路傳輸（輸入和輸出）並輸入網路上某個單一端點的 IP 位址，則策略中具有此項例外的任何 Security Agent 將無法傳送資料到此 IP 位址或接收來自此 IP 位址的資料。

   - 全部 IP 位址：包括全部 IP 位址
   - 單一 IP 位址：輸入 IPv4 或 IPv6 ，或主機名稱。
   - 範圍（適用於 IPv4 或 IPv6）：輸入 IPv4 或 IPv6 位址範圍。

- 範圍（適用於 IPv6）：輸入 IPv6 位址字首和長度。
- 子網路遮罩：輸入 IPv4 位址和其子網路遮罩。

10. 請點選「儲存」。

    會出現「編輯例外範本」畫面，其中顯示新增的新例外。

11. 請點選下列其中一個按鈕，將新的例外套用到清單：
    - 儲存範本變更：儲存目前的例外範本清單設定，但不將設定套用到現有的策略
    - 儲存並且套用到現有策略：儲存目前的例外範本清單設定，並立即將設定套用到現有的所有策略

修改防火牆策略例外

步驟

1. 移至用戶端 > 防火牆 > 策略。
2. 請點選「編輯例外範本」。
3. 請點選某個策略例外。
4. 修改下列項目：
    - 策略例外名稱
    - 應用程式類型、名稱或路徑
    - Apex One 要對網路傳輸執行的處理行動和傳輸方向
    - 網路通訊協定類型
    - 策略例外的通訊埠號碼
    - Security Agent 端點 IP 位址
5. 請點選「儲存」。

儲存策略例外清單設定

步驟

1. 移至用戶端 > 防火牆 > 策略。
2. 請點選「編輯例外範本」。
3. 請點選下列其中一個儲存選項：
   - 儲存範本變更：儲存例外範本及目前的策略例外和設定。此選項只會將範本套用到日後建立的策略，不會套用到現有策略。
   - 儲存並且套用到現有策略：儲存例外範本及目前的策略例外和設定。此選項會將範本套用到現有和日後建立的策略。

防火牆資料檔

防火牆資料檔提供彈性，方法是讓您選擇單一用戶端或用戶端群組在套用策略之前所必須要有的屬性。建立可以建立、設定或刪除特定網域資料檔的使用者角色。

使用內建的管理員帳號或擁有完整管理權限的使用者還可以啟動「覆寫用戶端安全層級/例外清單」選項，以伺服器設定取代 Security Agent 資料檔設定。

資料檔包含下列項目：

- 關聯策略：每個資料檔使用單一的策略
- 用戶端屬性：擁有下列一個或多個屬性的 Security Agent 會套用關聯的策略：
  - IP 位址：擁有特定 IP 位址、在某個 IP 位址範圍內的 IP 位址，或是屬於指定之子網路的 IP 位址的任何 Security Agent
  - 網域：屬於某個 Apex One 網域的任何 Security Agent
  - 端點：具有特定端點名稱的 Security Agent

- 平台：執行特定平台類型的任何 Security Agent
- 登入名稱：指定的使用者登入的 Security Agent 端點
- NIC 說明：具有相符 NIC 說明的任何 Security Agent 端點
- 用戶端位置：Security Agent 處於線上或離線狀態

注意

如果 Security Agent 可連線到 Apex One 伺服器或任何一部參考伺服器，則該用戶端為「線上」；如果用戶端無法連線到任何伺服器，則該用戶端為「離線」。

Apex One 隨附名為「所有用戶端資料檔」的預設資料檔，此資料檔使用「所有存取」策略。您可以修改或刪除此預設資料檔。您也可以建立新的資料檔。所有預設防火牆資料檔和使用者建立的防火牆資料檔（包括與每個資料檔關聯的策略和目前的資料檔狀態）都會顯示在 Web 主控台的防火牆資料檔清單中。管理資料檔清單並部署所有資料檔到 Security Agent。Security Agent 會將所有防火牆資料檔儲存到用戶端端點。

設定防火牆資料檔清單

步驟

1. 移至用戶端 > 防火牆 > 資料檔。
2. 若是使用內建的管理員帳號或擁有完整管理權限的使用者，可以視需要啟動「覆寫用戶端安全層級/例外清單」選項，以伺服器設定取代 Security Agent 資料檔設定。
3. 如果要新增資料檔，請點選「新增」。如果要編輯現有資料檔，請選取資料檔名稱。

   隨即出現資料檔組態設定畫面。如需詳細資訊，請參閱新增並編輯防火牆資料檔 第 13-18 頁。
4. 如果要刪除現有資料檔，請選取策略旁邊的核取方塊，然後請點選「刪除」。

5. 如果要變更資料檔在清單中的順序，請選取要移動的資料檔旁的核取方塊，然後請點選「上移」或「下移」。

   Apex One 會以防火牆資料檔出現在資料檔清單中的順序將它們依序套用到 Security Agent。例如，如果用戶端符合第一個資料檔，Apex One 會將針對該資料檔設定的處理行動套用到用戶端。Apex One 會忽略針對該用戶端設定的其他資料檔。

   秘訣

   策略的專屬性越高，其理想位置就應在清單中越靠頂端。例如，將您針對單一用戶端建立的策略移至頂端，接著依次是針對某範圍用戶端、網路網域和所有用戶端建立的策略。

6. 如果要管理參考伺服器，請點選「編輯參考伺服器清單」。參考伺服器是套用防火牆資料檔時，用來替代 Apex One 伺服器的端點。參考伺服器可以是網路上的任何端點（如需詳細資訊，請參閱參考伺服器 第 14-33 頁）。Apex One 會在您啟動參考伺服器時做出下列假設：

   - 連線至參考伺服器的 Security Agent 會處於線上狀態，即使這些用戶端無法與 Apex One 伺服器通訊也是一樣。
   - 套用至線上 Security Agent 的防火牆資料檔也會套用至連線到參考伺服器的 Security Agent。

   注意

   只有使用內建的管理員帳號或擁有完整管理權限的使用者能查看和設定參考伺服器清單。

7. 如果要儲存目前的設定並指定資料檔給 Security Agent：

   a. 選取是否要「覆寫用戶端安全層級/例外清單」。此選項會覆寫使用者設定的所有防火牆設定。

   b. 請點選「指定資料檔給用戶端」。Apex One 會將資料檔清單中的所有資料檔指定給所有 Security Agent。

8. 如果要確認是否已成功指定資料檔給 Security Agent：

   a. 移至「用戶端 > 用戶端管理」。在用戶端樹狀結構檢視下拉式方塊中，選取「防火牆檢視」。

b. 確認用戶端樹狀結構中的「防火牆」欄位下方有綠色的核取記號。如果與資料檔相關的策略啟動了「入侵偵測系統」，「IDS」欄位下方也會有綠色的核取記號。

c. 驗證用戶端是否已套用正確的防火牆策略。用戶端樹狀結構的「防火牆策略」欄位下方會顯示策略。

新增並編輯防火牆資料檔

Security Agent 端點可能需要不同層級的防護。防火牆資料檔可讓您指定相關聯策略套用到的用戶端端點。一般而言，每個使用中的策略都需要一個資料檔。

新增防火牆資料檔

步驟

1. 移至「用戶端 > 防火牆 > 資料檔」。
2. 請點選「新增」。
3. 請點選「啟動這個資料檔」允許 Apex One 將資料檔部署到 Security Agent。
4. 請輸入一個用於識別資料檔的名稱和說明（選用）。
5. 選取此資料檔的策略。
6. 指定 Apex One 要套用策略的用戶端端點。根據下列條件選取端點：
   - IP 位址
   - 網域：請點選按鈕開啟用戶端樹狀結構，然後從中選取網域。

注意

只有擁有完整網域權限的使用者能夠選取網域。

- 端點名稱：請點選按鈕開啟用戶端樹狀結構，然後從中選取 Security Agent 端點。
- 平台
- 登入名稱
- NIC 說明：輸入不含萬用字元的完整或部分說明。

秘訣

趨勢科技建議您輸入 NIC 製造商，因為 NIC 說明的開頭通常是製造商的名稱。例如：如果輸入 "Intel"，則 Intel 製造的所有 NIC 都將符合條件。如果輸入特定 NIC 型號，例如："Intel(R) Pro/100"，則 NIC 說明中開頭為 "Intel(R) Pro/100" 的 NIC 才符合條件。

- 用戶端位置：從下列項目中選取：
  - 內部 — Security Agent 可以連線到所設定的參考伺服器

注意

點選「編輯參考伺服器清單」以設定位置設定。

如需詳細資訊，請參閱參考伺服器 第 14-33 頁。

  - 外部 — Security Agent 無法連線到所設定的參考伺服器

7. 選取是否授與使用者權限，讓他們可以變更防火牆安全層級，或者編輯可設定的例外清單來允許所指定類型的流量。

   如需詳細資訊，請參閱防火牆策略 第 13-7 頁。

8. 請點選「儲存」。

修改防火牆資料檔

步驟

1. 移至用戶端 > 防火牆 > 資料檔。

2. 請點選某個資料檔。
3. 請點選「啟動這個資料檔」允許 Apex One 將此資料檔部署到 Security Agent。修改下列項目：
   - 資料檔名稱和說明
   - 指定給資料檔的策略
   - Security Agent 端點，根據下列條件：
     - IP 位址
     - 網域：請點選按鈕開啟用戶端樹狀結構，然後從中選取網域。
     - 端點名稱：請點選按鈕開啟用戶端樹狀結構，然後從中選取用戶端端點。
     - 平台
     - 登入名稱
     - NIC 說明：輸入不含萬用字元的完整或部分說明。

       秘訣

       趨勢科技建議您輸入 NIC 製造商，因為 NIC 說明的開頭通常是製造商的名稱。例如：如果輸入 "Intel"，則 Intel 製造的所有 NIC 都將符合條件。如果輸入特定 NIC 型號，例如："Intel(R) Pro/100"，則 NIC 說明中開頭為 "Intel(R) Pro/100" 的 NIC 才符合條件。
     - 用戶端連線狀態
4. 請點選「儲存」。

防火牆權限

允許使用者設定自己的防火牆設定。Apex One 伺服器部署的設定無法覆寫使用者設定的任何設定。例如，如果使用者關閉「入侵偵測系統」(IDS)，而您啟

動 Apex One 伺服器上的 IDS，則 Security Agent 端點上的 IDS 仍會維持關閉狀態。

啟動下列設定讓使用者設定防火牆。

表 13-2. 防火牆權限

權限	說明
在 Security Agent 主控台上顯示防火牆設定	「防火牆」選項可在 Security Agent 上顯示所有防火牆設定。
允許使用者啟動/關閉防火牆、入侵偵測系統和防火牆違規通知訊息	Apex One 防火牆使用狀態檢測、高效能網路病毒掃瞄和消除病毒，來保護網路上的用戶端和伺服器。如果您授與使用者啟動或關閉防火牆和其功能的權限，請警告他們不要長時間關閉防火牆，以避免端點遭受入侵和駭客攻擊。 如果您並未授與使用者這些權限，則從 Apex One 伺服器 Web 主控台設定的防火牆設定會顯示在 Security Agent 主控台的「網路卡清單」下。
允許用戶端將防火牆記錄檔傳送到 Apex One 伺服器	選取此選項可分析 Apex One 防火牆所封鎖和允許的傳輸。 如需有關防火牆記錄檔的詳細資訊，請參閱防火牆記錄檔 第 13-25 頁。 如果您選取此選項，請在「安全設定」標籤上的「用戶端 > 全域用戶端設定」中設定記錄檔傳送預約時程。移至「防火牆設定」區段。此預約時程只會套用到具備防火牆記錄檔傳送權限的用戶端。如需指示，請參閱全域防火牆設定 第 13-22 頁。

授與防火牆權限

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 權限和其他設定」。

4. 在「權限」標籤上，移至「防火牆權限」區段。
5. 選取下列選項：
   - 在 Security Agent 主控台上顯示防火牆設定 第 13-21 頁
   - 允許使用者啟動/關閉防火牆、入侵偵測系統和防火牆違規通知訊息 第 13-21 頁
   - 允許用戶端將防火牆記錄檔傳送到 Apex One 伺服器 第 13-21 頁
6. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

全域防火牆設定

可透過多種方式將全域防火牆設定套用至 Security Agent。

- 可將特定防火牆設定套用至伺服器所管理的所有用戶端。
- 可將設定只套用至具有特定防火牆權限的 Security Agent。例如，您可以只將防火牆記錄檔傳送排程套用至具有將記錄檔傳送到伺服器的權限的 Security Agent。

設定全域防火牆設定

步驟

1. 移至「用戶端 > 全域用戶端設定」。

2. 在「安全設定」標籤上，移至「防火牆設定」區段並設定下列：

設定	說明
啟動 Apex One 防火牆	在套用策略和資料檔之前，必須先在所有 Security Agent 上啟動 Apex One 防火牆。
將防火牆記錄檔傳送到伺服器	您可以授與特定 Security Agent 將防火牆記錄檔傳送到 Apex One 伺服器的權限。在這個區段中設定記錄檔傳送預約時程。只有具備傳送防火牆記錄檔權限的用戶端才會使用預約。 如需可供所選用戶端使用的防火牆權限的資訊，請參閱防火牆權限 第 13-20 頁。
只在系統重新啟動後更新 Apex One 防火牆驅動程式	可讓 Security Agent 只在 Security Agent 端點重新啟動後才更新一般防火牆驅動程式。啟動此選項，可避免用戶端端點在用戶端升級期間，由於進行一般防火牆驅動程式更新而可能出現的中斷（例如暫時中斷網路連線）。
每小時傳送防火牆記錄檔資訊至 Apex One 伺服器一次，以確定是否有可能發生防火牆病毒爆發	啟動此選項時，Security Agent 會每小時向 Apex One 伺服器傳送一次防火牆記錄檔數。 如需有關防火牆記錄檔的詳細資訊，請參閱防火牆記錄檔 第 13-25 頁。 Apex One 會使用記錄檔數和防火牆違規事件爆發條件判斷防火牆違規事件爆發的可能性。發生爆發情況時，Apex One 會傳送電子郵件通知給 Apex One 管理員。

3. 在「系統」標籤上移至「認證安全防護軟體設定」區段，然後選取「啟動「認證安全防護軟體服務」以進行行為監控、防火牆和防毒掃瞄」。

   認證安全防護軟體服務會查詢趨勢科技資料中心，確認惡意程式行為封鎖、事件監控、防火牆或防毒掃瞄所偵測到的程式是否安全。啟動「認證安全防護軟體服務」可降低誤判的可能性。

注意

啟動認證安全防護軟體服務之前，請確定 Security Agent 具有正確的 Proxy 設定（詳細資訊請參閱 Security Agent Proxy 設定 第 15-42 頁）。Proxy 設定不正確以及網際網路連線不穩定，都可能造成趨勢科技資料中心回應接收延遲或失敗，以致監控程式顯示無回應。

此外，純 IPv6 Security Agent 無法直接從趨勢科技資料中心進行查詢。如果要使 Security Agent 連線到趨勢科技資料中心，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。

4. 請點選「儲存」。

Security Agent 使用者的防火牆違規通知

Apex One 防火牆封鎖違反防火牆策略的輸出流量之後，Apex One 可以立即在端點上顯示通知訊息。授與使用者啟動/關閉通知訊息的權限。

注意

設定特定防火牆策略時，您也可以啟動通知。如果要設定防火牆策略，請參閱新增防火牆策略 第 13-9 頁。

授與使用者啟動/關閉通知訊息的權限

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 權限和其他設定」。
4. 在「權限」標籤上，移至「防火牆權限」區段。

5. 選取「允許使用者啟動/關閉防火牆、入侵偵測系統和防火牆違規通知訊息」。
6. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

修改防火牆通知訊息的內容

步驟

1. 移至「管理 > 通知 > 用戶端」。
2. 在「類型」下拉式清單中，選取「防火牆違規」。
3. 在提供的文字方塊中修改預設訊息。
4. 請點選「儲存」。

防火牆記錄檔

伺服器上可用的防火牆記錄檔是由具有傳送防火牆記錄檔權限的 Security Agent 進行傳送。授與特定用戶端此權限，以監控並分析端點上由 Apex One 防火牆封鎖的傳輸。

如需有關防火牆權限的資訊，請參閱防火牆權限 第 13-20 頁。

如果要避免記錄檔佔去過多硬碟空間，請手動刪除記錄檔或設定記錄檔刪除預約時程。如需有關管理記錄檔的詳細資訊，請參閱記錄檔管理 第 14-39 頁。

檢視防火牆記錄檔

Security Agent 會在偵測到防火牆違規後產生記錄檔，並將記錄檔傳送到伺服器。

步驟

1. 移至下列其中一個項目：
   - 記錄檔 > 用戶端 > 安全威脅
   - 用戶端 > 用戶端管理
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請移至「防火牆記錄檔條件」畫面：
   - 在「安全威脅記錄檔」畫面中，點選「檢視記錄檔 > 防火牆記錄檔」。
   - 在「用戶端管理」畫面中，點選「記錄檔 > 防火牆記錄檔」。
4. 為確保可以使用最新的記錄檔，請點選「通知用戶端」。請預留一些時間給用戶端來傳送防火牆記錄檔，再繼續執行下一個步驟。
5. 指定記錄條件，然後請點選「顯示記錄檔」。
6. 檢視記錄檔。記錄檔包含下列資訊：

項目	說明
日期/時間	發生偵測的時間
端點	發生偵測的端點
網域	發生偵測的網域
遠端主機	遠端主機的 IP 位址
本機主機	本機主機的 IP 位址

項目	說明
通訊協定	使用的通訊協定
通訊埠	通訊埠號碼
方向	• 接收：表示流量為輸入 • 傳送：表示流量為輸出
處理程序	在端點上執行而觸發防火牆違規事件的可執行程式或服務
說明	指定實際的安全威脅（例如：網路病毒或 IDS 攻擊）或防火牆策略違規

7. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請點選「全部匯出到 CSV」。開啟檔案或將其儲存至特定位置。

防火牆違規事件爆發

依防火牆違規事件數目和偵測期間定義防火牆違規事件爆發。

Apex One 具有預設通知訊息，可在偵測到爆發時，通知您和其他 Apex One 管理員。您可以視需要修改通知訊息。

注意

Apex One 可以透過電子郵件傳送防火牆爆發通知。設定電子郵件設定，讓 Apex One 可以成功地傳送電子郵件。如需詳細資訊，請參閱管理員通知設定 第 14-35 頁。

設定防火牆違規事件爆發條件和通知

步驟

1. 移至「管理 > 通知 > 病毒爆發」。
2. 在「條件」標籤中：
   a. 移至「防火牆違規事件」區段。
   b. 選取「在 Security Agent 上監控防火牆違規」。
   c. 指定 IDS 記錄檔、防火牆記錄檔和網路病毒記錄檔的數量。
   d. 指定偵測期間。

   秘訣
   趨勢科技建議您接受此畫面中的預設值。

   Apex One 會在記錄檔數量超過指定值時傳送通知訊息。例如，如果您指定 100 個 IDS 記錄檔、100 個防火牆記錄檔和 100 個網路病毒記錄檔，並指定 3 小時的期間，當伺服器在 3 個小時內收到 301 個記錄檔時，Apex One 會傳送通知。
3. 在「電子郵件」標籤中：
   a. 移至「防火牆違規事件爆發」區段。
   b. 選取「啟動電子郵件通知」。
   c. 指定電子郵件收件者。
   d. 接受或修改預設的電子郵件主旨和訊息。您可以使用 Token 變數代表「主旨」和「訊息」欄位中的資料。

   表 13-3. 防火牆違規病毒爆發通知的 Token 變數

變數	說明
%A	記錄檔超出

變數	說明
%C	防火牆違規記錄檔數量
%T	防火牆違規記錄檔累計的時段

4. 請點選「儲存」。

測試 Apex One 防火牆

為確保 Apex One 防火牆能正常運作，請在單一 Security Agent 或 Security Agent 群組執行測試。

警告!

請僅在受控制的環境中測試 Security Agent 程式設定。請勿在連線至網路或 Internet 的端點執行測試。這樣做可能會讓 Security Agent 端點暴露於病毒、駭客攻擊和其他風險之中。

步驟

1. 建立並儲存測試策略。將其設定成封鎖您要測試的傳輸類型。例如，如果要禁止 Security Agent 存取 Internet，請執行下列工作：
   a. 將安全層級設定為「低」（允許所有輸入/輸出流量）。
   b. 選取「啟動防火牆」和「發生防火牆違規事件時通知使用者」。
   c. 建立封鎖 HTTP（或 HTTPS）傳輸的例外。
2. 建立並儲存測試資料檔，接著選取要對其測試防火牆功能的用戶端。使測試策略與測試資料檔相關聯。
3. 請點選「指定資料檔給用戶端」。
4. 驗證部署。
   a. 請點選「用戶端 > 用戶端管理」。

b. 選取用戶端所屬的網域。

c. 從用戶端樹狀結構檢視中選取「防火牆檢視」。

d. 檢查用戶端樹狀結構的「防火牆」欄位下方是否有綠色的核取記號。如果您已為該用戶端啟動「入侵偵測系統」，請確認「IDS」欄下也顯示綠色的核取記號。

e. 驗證用戶端是否已套用正確的防火牆策略。策略會顯示在用戶端樹狀結構的「防火牆策略」欄位下方。

5. 嘗試傳送或接收您在策略中設定的傳輸類型，以在用戶端端點上測試防火牆。

6. 如果要測試設定為防止用戶端存取 Internet 的策略，請在用戶端端點上開啟 Web 瀏覽器。如果您已設定 Apex One 在發生防火牆違規事件時顯示通知訊息，則會在發生輸出傳輸違規時在用戶端端點上顯示訊息。

部分 III

管理 Apex One 伺服器和用戶端

第 14 章

管理 Apex One 伺服器

本章說明 Apex One 伺服器管理和組態設定。

包含下列主題：

以角色為基礎的管理

使用「以角色為基礎的管理」授與和控制存取 Apex One Web 主控台的權限。如果貴組織中有多位 Apex One 管理員，可以使用此功能將特定的 Web 主控台權限分配給各個管理員，並提供只在執行特定工作所需的工具和權限給管理員。透過指定一或多個要管理的網域給管理員，還可以控制對用戶端樹狀結構的存取。此外，您可以將 Web 主控台的「僅檢視」存取權授與非管理員。

每位使用者（管理員或非管理員）都會有指定的特定角色。角色定義了對 Web 主控台的存取層級。使用者使用自訂使用者帳號或 Active Directory 帳號登入 Web 主控台。

以角色為基礎的管理包含下列工作：

1. 定義使用者角色。如需詳細資訊，請參閱使用者角色 第 14-11 頁。
2. 設定使用者帳號並指定特定角色給每個使用者帳號。如需詳細資訊，請參閱使用者帳號 第 14-3 頁。

從系統事件記錄檔檢視所有使用者的 Web 主控台活動。記錄的活動如下：

- 登入主控台
- 密碼修改
- 登出主控台
- 作業階段逾時（系統自動將使用者登出）

使用者帳號

設定手動使用者帳號或使用 Active Directory 帳號來指定權限，以檢視或設定用戶端樹狀結構中可用的精細用戶端設定、工作和資料。您必須指定特定角色給每個使用者，以決定使用者可以檢視或設定的 Web 主控台功能表項目。您可以使用 Apex One 使用者帳號來執行「單一登入」至 Apex One（從 Trend Micro Apex Central 主控台）。

安裝 Apex One 伺服器期間，安裝程式會自動建立名為「root」的內建帳號。使用 root 帳號登入的使用者可以存取所有功能表項目。您無法刪除 root 帳

號，但可修改該帳號的詳細資料（例如：密碼和帳號說明）。如果忘記 root 帳號的密碼，請聯絡經銷商取得重設密碼的協助。

注意

升級 Apex One 伺服器後，您必須編輯自訂帳號並在「步驟 3 定義用戶端樹狀結構功能表」畫面上為之前新增的自訂帳號手動啟動所有新功能。

如需有關權限的詳細資訊，請參閱定義網域權限 第 14-9 頁。

下表列出「使用者帳號」畫面上提供的工作。

工作	說明
新增帳號	請點選「新增」以建立新使用者帳號。 如需詳細資訊，請參閱新增使用者帳號 第 14-6 頁。
刪除現有的帳號	選取已存在的使用者帳號，然後點選「刪除」。
編輯現有的帳號	請點選已存在的使用者帳號的名稱，以檢視或修改目前的帳號設定。

用戶端管理功能表項目

下表列出可用用戶端管理功能表項目。

注意

只有在啟動各自的嵌入程式之後才會顯示功能表項目。例如，如果資料外洩防護模組未啟動，則清單中不會顯示任何資料外洩防護功能表項目。

表 14-1. 用戶端管理功能表項目

主功能表項目	子功能表
狀態	無

主功能表項目	子功能表
工作	• 立即掃瞄 • 用戶端解除安裝 • 中央隔離區恢復 • 間諜程式/可能的資安威脅程式恢復

設定	• 掃瞄設定
	  • 掃瞄方法
	  • 手動掃瞄設定
	  • 即時掃瞄設定
	  • 預約掃瞄設定
	  • 立即掃瞄設定
	• 網頁信譽評等設定
	• 可疑連線設定
	• 行為監控設定
	• 周邊設備存取控管設定
	• DLP 設定
	• 樣本提交
	• 更新代理程式設定
	• 權限和其他設定
	• 其他服務設定
	• 間諜程式/可能的資安威脅程式核可清單
	• 信任的程式清單
	• Machine Learning 設定
	• 匯出設定
	• 匯入設定

主功能表項目	子功能表
記錄檔	• 病毒/惡意程式記錄檔 • 間諜程式/可能的資安威脅程式記錄檔 • 防火牆記錄檔 • 網頁信譽評等記錄檔 • 可疑連線記錄檔 • 可疑檔案記錄檔 • C&C 回呼記錄檔 • 行為監控記錄檔 • Machine Learning 記錄檔 • 周邊設備存取控管記錄檔 • 資料外洩防護記錄檔 • 掃瞄作業記錄檔 • 刪除記錄檔
管理用戶端樹狀結構	• 新增網域 • 重新命名網域 • 移動用戶端 • 移除網域/用戶端
匯出	無

新增使用者帳號

設定手動使用者帳號或使用 Active Directory 帳號來指定權限，以檢視或設定用戶端樹狀結構中可用的精細用戶端設定、工作和資料。

步驟

1. 移至管理 > 帳號管理 > 使用者帳號。

2. 請點選「新增」。

   會出現「步驟 1 使用者資訊」畫面。

3. 選取「啟動此帳號」。

4. 在「選取角色」下拉式清單中，選擇先前設定的角色。

   如需詳細資訊，請參閱新增自訂角色 第 14-14 頁。

5. 在「使用者資訊」區段中，設定下列項目：

   - 自訂帳號：選取此選項以建立手動使用者帳號並指定必要資訊
     - 使用者名稱：輸入帳號的唯一使用者名稱
     - 說明：輸入帳號的說明
     - 密碼：輸入並確認帳號用於登入 Apex One Web 主控台的密碼

       重要

       密碼必須符合下列複雜度要求：

       - 長度為 8 到 32 字元
       - 以下每項包含至少一個：大寫字母 (A-Z)、小寫字母 (a-z)、數字 (0-9) 和特殊字元
       - 不可包含使用者名稱
       - 不可包含非可列印 ASCII 字元

     - 電子郵件信箱：輸入與使用者帳號相關聯的電子郵件信箱

       注意

       Apex One 會將通知傳送至此電子郵件地址。這些通知會通知收件者安全威脅偵測和數位資產傳輸。

       如需有關通知的詳細資訊，請參閱管理員的安全威脅通知 第 7-69 頁。

   - Active Directory 使用者或群組：如果想要使用現有的 Active Directory 帳號或群組來登入 Apex One Web 主控台，請選取此選項

重要

為了管理使用者帳號，必須將 Apex One 伺服器加入 Active Directory 網域。

a. 在「使用者名稱或群組」欄位中，輸入您要使用的 Active Directory 帳號。

b. 在「網域」欄位中，輸入「使用者名稱或群組」所屬的 Active Directory 網域。

c. 請點選「搜尋」。

d. 在「使用者和群組」清單中，從搜尋結果中選取帳號並點選 >，將該帳號新增到「選取的使用者和群組」清單中。

6. 按「下一步」。

   會出現「步驟 2 用戶端網域控制項」畫面。

7. 選取要授與的 root 帳號，以允許該帳號檢視所有 Apex One 網域，或選取使用者帳號可以在用戶端樹狀結構中存取的特定 Apex One 網域。

重要

當使用者帳號存取用戶端樹狀結構時，Apex One 只會顯示所選取的網域。如果未選取網域，Apex One 會在用戶端樹狀結構中隱藏網域。

8. 按「下一步」。

   會出現「步驟 3 定義用戶端樹狀結構功能表」畫面。

9. 請點選「可用的功能表項目」控制項，然後指定每個可用功能表項目的權限。如需有關可用功能表項目的清單，請參閱 用戶端管理功能表項目 第 14-4 頁。

   在步驟 8 中設定的 用戶端 樹狀結構範圍，會確定功能表項目的權限等級，並定義權限的目標。用戶端 樹狀結構範圍可以是根網域（全部 用戶端），也可以是特定 用戶端 樹狀結構網域。

表 14-2. 用戶端 管理功能表項目和 用戶端 樹狀結構範圍

條件	用戶端 樹狀結構範圍	
	根網域	特定網域
功能表項目權限	設定、檢視或無存取權	設定、檢視或無存取權
目標	根網域（全部 用戶端）或特定網域 例如，可以授與某個角色對 用戶端 樹狀結構中「工作」功能表項目的「設定」權限。如果目標為根網域，使用者可在全部 用戶端 上啟動工作。如果目標為網域 A 和 B，則僅可在網域 A 和 B 中的 用戶端 上啟動工作。	僅選定網域 例如，可以授與某個角色對 用戶端 樹狀結構中「設定」功能表項目的「設定」權限。這意味著使用者僅可將設定部署到選定網域中的 用戶端。
	僅當「伺服器/用戶端適用的功能表項目」中對用戶端管理」的權限為「檢視」時，才會顯示 用戶端 樹狀結構。	

- 如果選取「設定」下的核取方塊，則會自動選取「檢視」下的核取方塊。
- 如果未選取任何核取方塊，則權限為「無存取權」。
- 如果為特定網域設定權限，可透過請點選「將所選網域的設定複製到其他網域」，將權限複製到其他網域。

10. 請點選「完成」。
11. 將帳號詳細資訊傳送給使用者。

定義網域權限

在定義網域權限時，Apex One 會自動將上層網域的權限套用至其所管理的所有子網域。子網域所擁有的權限不得少於其上層網域。例如，如果系統管理員擁有檢視和設定 Apex One 所管理的所有 Security Agent 的權限（「Apex One 伺服器」網域），則子網域的權限必須能夠讓系統管理員存取這些設定功能。移除子網域上的權限可能表示，系統管理員將不擁有所有 Security Agent 的完整設定權限。

針對下列程序，網域樹狀結構如下：

例如，如果要向子網域「員工」授與使用者帳號「Chris」權限以檢視和設定特定的功能表項目，但僅在上層網域「管理員」中授與檢視記錄檔的權限，請執行下列程序。

表 14-3. 使用者帳號「Chris」的權限

網域	所需權限
Apex One 伺服器	無特殊權限
管理員	檢視「記錄檔」
員工	檢視及設定「工作」 檢視及設定「記錄檔」 檢視「設定」
企業安全防護採購指南	無特殊權限

步驟

1. 移至「使用者帳號：步驟 3 定義用戶端樹狀結構功能表」畫面。
2. 按一下「Apex One 伺服器」網域。
3. 清除所有「檢視」和「設定」核取方塊。

注意

僅當您在「使用者帳號：步驟 2 用戶端網域控制項」畫面上選取了「Apex One 伺服器」網域的所有子網域時，才能對該網域進行設定。

4. 請點選「企業安全防護採購指南」網域。
5. 清除所有「檢視」和「設定」核取方塊。

> **注意**
>
> 僅當在「使用者帳號：步驟 2 用戶端網域控制項」畫面中選取了「企業安全防護採購指南」網域時才會顯示該網域。

6. 請點選「管理員」網域。
7. 選取「檢視記錄檔」，並清除所有其他「檢視」和「設定」核取方塊。
8. 請點選「員工」網域。
9. 針對 Chris 選取下列功能表項目：
   - 工作：檢視及設定
   - 記錄檔：檢視及設定
   - 設定：檢視

   現在，Chris 可以針對「員工」網域檢視和設定所選功能表項目，但針對「管理員」網域，只能檢視「記錄檔」。

如果 Chris 擁有檢視和設定「管理員」網域的權限，則 Apex One 會自動授與「員工」子網域相同的權限。發生此情況的原因是，「管理員」網域管理其所有子網域。

使用者角色

定義及指定使用者角色，以限制特定使用者帳號可以在特定 Web 主控台畫面上具有的存取權。您可以將使用者角色定義為完全隱藏 W eb 主控台畫面、將存取權限於「“唯讀”」，或是授與完整的組態設定權限。

下表列出「使用者角色」畫面上提供的工作。

工作	說明
新增自訂角色	請點選「新增」以建立新自訂角色。 如需詳細資訊，請參閱新增自訂角色 第 14-14 頁。 **重要** 只有 “root” 帳號或具有內建管理員角色的使用者，可以建立自訂使用者角色並指定給使用者帳號。
從現有的自訂角色複製設定	選取已存在的自訂角色，然後點選「複製」。會出現「複製角色」畫面，您可在其中根據原始設定來建立新自訂角色。
刪除現有的自訂角色	選取已存在的自訂角色，然後點選「刪除」。 **重要** 您無法刪除目前已指定給使用者帳號的角色。
匯出自訂角色	選取已存在的自訂角色，再點選「匯出」按鈕，然後選取下列其中一個選項： • 匯出到 DAT：將選取的角色匯出到 DAT 檔案，稍後您可將該檔案匯入到其他 Apex One 伺服器 • 匯出到 CSV：將選取的角色匯出到 CSV 檔案，稍後您可使用該檔案來檢視角色設定 **重要** 您無法將產生的 CSV 檔案匯入到 Apex One 伺服器。
匯入自訂角色	請點選「匯入」以從先前匯出的使用者角色 DAT 檔案匯入使用者角色設定。 如需詳細資訊，請參閱匯入或匯出自訂角色 第 14-19 頁。

工作	說明
編輯現有的自訂角色	請點選已存在的使用者角色的名稱，以檢視或修改目前的角色設定。 注意 您無法修改任何預先定義之使用者角色的內容。 如需詳細資訊，請參閱內建使用者角色 第 14-13 頁。

內建使用者角色

Apex One 隨附一組內建的使用者角色，但您無法視需要修改或刪除。內建角色包括：

表 14-4. 內建使用者角色

角色名稱	說明
Administrator（系統管理員）	將此角色委派給其他 Apex One 管理員或對 Apex One 有相當程度瞭解的使用者。 具有此角色的使用者擁有對所有功能表項目的「設定」權限。 注意 只有指定「Administrator（內建）」角色的使用者才可存取嵌入程式功能表項目。

Guest User（訪客使用者）	將此角色委派給想要檢視 Web 主控台用於參考用途的使用者。
	• 具有此角色的使用者沒有下列功能表項目的存取權：
	  • 嵌入程式
	  • 管理 > 帳號管理 > 使用者角色
	  • 管理 > 帳號管理 > 使用者帳號
	• 使用者具有所有其他功能表項目的「檢視」權限。

新增自訂角色

如果可用的內建角色不符合需求，您可以新增自訂使用者角色。

如需詳細資訊，請參閱內建使用者角色 第 14-13 頁。

步驟

1. 移至管理 > 帳號管理 > 使用者角色。
2. 請點選「新增」。

   會出現「新增角色」畫面。
3. 在「角色資訊」區段中，指定下列項目：
   - 名稱：輸入角色的唯一名稱
   - 說明：（選用）
4. 在「角色權限」區段中：
   a. 選取指派了此角色之使用者帳號可以存取的功能表項目。
      - 伺服器/用戶端適用的功能表項目：包含全域 Security Agent 及 Apex One 伺服器設定、工作和資料

        如需詳細資訊，請參閱伺服器和用戶端適用的功能表項目 第 14-15 頁。
      - 受管理網域適用的功能表項目：包含在用戶端樹狀結構外可用的精細 Security Agent 設定、工作和資料

        如需詳細資訊，請參閱受管理網域適用的功能表項目 第 14-17 頁。

   b. 針對選取的功能表項目，選取使用者帳號指派給角色的存取權限
      - 設定：允許完整存取功能表項目

        使用者可以設定全部設定，執行全部工作並檢視功能表項目中的資料。

- 檢視：只允許使用者檢視功能表項目中的設定、工作和資料

注意

同時清除「設定」和「檢視」核取方塊，會完全隱藏功能表項目，無法檢視。指派給此角色的使用者帳號將看不到功能表項目。

5. 請點選「儲存」。

   新角色會顯示在「使用者角色」畫面上。

伺服器和用戶端適用的功能表項目

下表列出伺服器/用戶端可用的功能表項目。

注意

只有在啟動各自的嵌入程式之後才會顯示功能表項目。例如，如果資料外洩防護模組未啟動，則清單中不會顯示任何資料外洩防護功能表項目。任何額外的嵌入程式都顯示在嵌入程式功能表項目下。

只有指定「Administrator（內建）」角色的使用者才可存取嵌入程式功能表項目。

表 14-5. 用戶端功能表項目

頂層功能表項目	功能表項目
用戶端	• 用戶端管理 • 用戶端分組 • 全域用戶端設定 • 端點位置 • 資料外洩防護 • 連線驗證 • 病毒爆發防範

表 14-6. 記錄檔功能表項目

頂層功能表項目	功能表項目

記錄檔	• 用戶端
	  • 安全威脅
	  • 用戶端元件更新
	• 伺服器更新
	• 系統事件
	• 記錄檔維護

表 14-7. 更新功能表項目

頂層功能表項目	功能表項目	子功能表項目
更新	伺服器	• 預約更新 • 手動更新 • 更新來源
	用戶端	• 自動更新 • 更新來源
	還原	無

表 14-8. 管理功能表項目

頂層功能表項目	功能表項目	子功能表項目
管理	帳號管理	• 使用者帳號 • 使用者角色 注意 只有使用內建管理員帳號的使用者可以存取使用者帳號和使用者角色。

頂層功能表項目	功能表項目	子功能表項目
	主動式雲端截毒技術	• 主動式雲端截毒技術來源 • 整合式伺服器 • Smart Feedback
	Active Directory	• Active Directory 整合 • 預約同步處理
	通知	• 一般設定 • 病毒爆發 • 用戶端
	設定	• Proxy • 用戶端連線 • 離線用戶端 • 隔離區管理員 • 產品使用授權 • Apex Central • Web 主控台 • 資料庫備份 • 可疑物件清單 • Edge Relay • 伺服器移轉

受管理網域適用的功能表項目

下表列出受管理網域的可用功能表項目。

表 14-9. 資訊中心功能表項目

主功能表項目	功能表項目
資訊中心 注意 任何使用者不論其權限為何，都能存取此頁面。	無

表 14-10. 評估功能表項目

頂層功能表項目	功能表項目	子功能表項目
評估	安全性符合	• 手動報告 • 預約報告
	未受管理的端點	無

表 14-11. 用戶端功能表項目

頂層功能表項目	功能表項目	子功能表項目
用戶端	防火牆	• 策略 • 資料檔
	用戶端安裝	• Browser-based • 遠端

表 14-12. 記錄檔功能表項目

頂層功能表項目	功能表項目	子功能表項目
記錄檔	用戶端	• 連線驗證 • 中央隔離區還原 • 間諜程式/可能的資安威脅程式恢復

表 14-13. 更新功能表項目

頂層功能表項目	功能表項目	子功能表項目
更新	摘要	無
	用戶端	手動更新

表 14-14. 管理功能表項目

頂層功能表項目	功能表項目	子功能表項目
管理	通知	Administrator（系統管理員）

匯入或匯出自訂角色

步驟

1. 移至管理 > 帳號管理 > 使用者角色。
2. 如果要將自訂角色匯出到 .dat 檔案（可以將這個檔案重新匯入到其他的 Apex One 伺服器），請執行下列步驟：
   a. 選取角色，然後點選「匯出」 > 「匯出到 DAT」。
   b. 儲存 .dat 檔案。如果要管理另一部 Apex One 伺服器，可以使用該 .dat 檔案將自訂角色匯入至該伺服器。

   注意
   匯出角色操作只能在相同版本的伺服器之間完成。
3. 如果要將自訂角色匯出到 .csv 檔案：
   a. 選取角色，然後點選「匯出」 > 「匯出到 CSV」。
   b. 儲存 .csv 檔案。使用此檔案可以檢查所選角色的資訊和權限。

4. 如果您儲存了不同 Apex One 伺服器的自訂角色，而且想要將這些角色匯入到目前的 Apex One 伺服器，請點選「匯入」並尋找包含自訂角色的 `.dat` 檔案。

   - 如果您匯入相同名稱的角色，則「使用者角色」畫面上的角色會遭到覆寫。
   - 匯入角色操作只能在相同版本的伺服器之間完成。
   - 從其他 Apex One 伺服器匯入的角色：
     - 保留伺服器/用戶端功能表項目以及受管理網域功能表項目的權限。
     - 套用用戶端管理功能表項目的預設權限。在另一部伺服器上，記錄角色對用戶端管理功能表項目的權限，然後將這些權限重新套用到匯入的角色。

Trend Micro Apex Central

Trend Micro Apex Central™ 是一個中央管理主控台，可在閘道、郵件伺服器、檔案伺服器和企業桌面層級上管理趨勢科技產品和服務。Apex Central 的 Web-based 管理主控台提供單一監控點，可供網路上受管理的產品和服務使用。

Apex Central 可讓系統管理員監控並針對中毒、安全違規或病毒進入點等活動進行報告。系統管理員可以在整個網路中下載並部署元件，這有助於確保防護保持一致且最新。Apex Central 可讓使用者執行手動更新和預約更新，並將產品視為群組或個體來設定和管理，以提升彈性。

此版本 Apex One 與 Apex Central 的整合

此 Apex One 版本包含下列功能（從 Apex Central 管理 Apex One 伺服器時）：

- 建立、管理和部署 Trend Micro Apex One 防毒、資料外洩防護及周邊設備存取控管的策略，並直接從 Apex Central 主控台指定權限給 Security Agent。

  下表列出 Apex Central（任何版本）中可用的策略組態設定。

  表 14-15. Apex Central 中的 Apex One 策略管理類型

策略類型	功能
Apex One 防毒和用戶端設定	• 其他服務設定 • Application Control 設定 • 行為監控設定 • 周邊設備存取控管設定 • Endpoint Sensor 設定 • 手動掃瞄設定 • Machine Learning 設定 • 權限和其他設定 • 即時掃瞄設定 • 樣本提交 • 掃瞄方法 • 立即掃瞄設定 • 預約掃瞄設定 • 間諜程式/可能的資安威脅程式核可清單 • 可疑連線設定 • 信任的程式清單 • 更新代理程式設定 • Vulnerability Protection 設定 • 網頁信譽評等設定

策略類型	功能
資料安全防護	資料外洩防護策略設定 注意 在 Security Agent 策略中管理「資料安全防護」的「周邊設備存取控管」權限。

如需有關將 Security Agent 策略設定移轉到 Apex Central 伺服器的詳細資訊，請參閱 Apex One 設定匯出工具 第 14-27 頁。

- 從 Apex Central 主控台將下列設定從一部 Trend Micro Apex One 伺服器複製到另一部 Apex One 伺服器：
  - 資料識別碼類型 第 11-4 頁
  - 資料外洩防護範本 第 11-18 頁

注意

如果將這些設定複製到尚未啟動資料安全防護使用授權的 Trend Micro Apex One 伺服器，只有當啟動使用授權後，設定才會生效。

透過 Apex Central 進行增強的產品整合

Apex Central Web 主控台提供 Apex One Web 主控台並未提供的進階 Security Agent 策略組態設定。藉由正確授權，您可以將下列增強的安全策略傳送至整個網路中的 Security Agent。

功能	說明
Application Control	藉由與 Application Control 整合，可為 Apex One 使用者提供進階的應用程式封鎖和端點鎖定功能。您可以執行應用程式清查，還可建立策略規則以僅允許特定應用程式在您的端點上執行。您也可以根據應用程式類別、供應商或版本來建立 Application Control 規則。

功能	說明
Endpoint Sensor	藉由與 Endpoint Sensor 整合，可讓您對 Apex One 端點進行監控、記錄以及執行目前與歷史安全調查。使用 Apex Central 主控台，可先執行初步調查來找出有風險的端點，然後才執行深入根本原因分析來識別攻擊媒介。
Vulnerability Protection	藉由與 Vulnerability Protection 整合，可透過在官方修補程式正式發佈之前自動執行虛擬修補程式的應用程式，來保護 Apex One 使用者。趨勢科技會根據您的網路效能和安全優先順序，來為受保護的端點提供建議的入侵防護規則。

如需有關增強的產品整合的詳細資訊，請參閱《Apex Central 管理手冊》。

支援的 Apex Central 版本

此 Apex One 版本支援下列 Apex Central/Control Manager 版本：

- Apex Central（任何版本）
- Control Manager 7.0 或更新版本

如需有關 Apex One 伺服器和 Security Agent 回報給 Apex Central 的 IP 位址的詳細資訊，請參閱顯示 IP 位址的畫面 第 A-5 頁。

套用這些 Apex Central 版本的最新 Patch 和重要的 HotFix，讓 Apex Central 能夠管理 Apex One。如果要取得最新的 Patch 和 HotFix，請聯絡您的經銷商或瀏覽趨勢科技下載專區：

http://downloadcenter.trendmicro.com/?regs=TW; http://www.trendmicro.com/download/zh-tw/default.asp

安裝 Apex One 之後，請將它註冊到 Apex Central，然後在 Apex Central 管理主控台上設定 Apex One。如需有關管理 Apex One 伺服器的資訊，請參閱 *Apex Central* 文件。

向 Apex Central 註冊 Apex One

步驟

1. 移至「管理 > 設定 > Apex Central」。

2. 指定項目顯示名稱，這是將在 Apex Central 中顯示的 Apex One 伺服器名稱。

   依預設，項目顯示名稱會包含伺服器電腦的主機名稱和此產品的名稱（例如，Server01_OSCE）。

   注意

   在 Apex Central 中，Apex Central 所管理的 Apex One 伺服器和其他產品稱為「項目」。

3. 指定 Apex Central 伺服器的 FQDN 或 IP 位址，以及用來連線至此伺服器的通訊埠號碼。也可以選擇使用 HTTPS 以增加連線安全。

   - 對於雙堆疊 Apex One 伺服器，請輸入 Apex Central FQDN 或 IP 位址（IPv4 或 IPv6，如果可用）。
   - 對於純 IPv4 Apex One 伺服器，請輸入 Apex Central FQDN 或 IPv4 位址。
   - 對於純 IPv6 Apex One 伺服器，請輸入 Apex Central FQDN 或 IPv6 位址。

4. 按一下「Apex Central 憑證」旁邊的「瀏覽...」，然後選取從目標 Apex Central 伺服器下載的憑證檔案。

   如果要取得 Apex Central 憑證檔案，請移至 Apex Central 伺服器，然後將下列位置中的憑證檔案複製到 Apex One 伺服器：

   ```
   <Apex Central 安裝資料夾>\Certificate\CA\TMCM_CA_Cert.pem
   ```

   重要

   如果您的公司在 Apex Central 伺服器上使用自訂憑證，您必須在 Apex Central 註冊期間上傳根 CA 憑證。

   如需詳細資訊，請參閱 Apex Central 憑證授權 第 14-26 頁。

5. 如果 Apex Central 的 IIS Web 伺服器需要驗證，請輸入使用者名稱和密碼。
6. 如果要使用 Proxy 伺服器連線至 Apex Central 伺服器，請指定下列 Proxy 伺服器設定：
   - Proxy 通訊協定
   - 伺服器 FQDN 或 IPv4/IPv6 位址和通訊埠
   - Proxy 伺服器驗證的使用者 ID 和密碼
7. 決定要使用單向通訊還是雙向通訊通訊埠轉送，然後指定 IPv4/IPv6 位址和通訊埠。
8. 如果要檢查 Apex One 是否能根據您指定的設定連線至 Apex Central 伺服器，請點選「測試連線」。

   如果已成功建立連線，請點選「註冊」。
9. 如果 Control Manager 伺服器為 6.0 SP1 或更新版本，或您使用的是 Apex Central 伺服器，便會出現訊息，提示您使用 Apex Central 伺服器做為 Apex One 整合式主動雲端截毒技術伺服器的更新來源。按一下「確定」以使用 Apex Central 伺服器做為整合式主動雲端截毒技術伺服器的更新來源，或按一下「取消」以繼續使用目前的更新來源（依預設，為主動式更新伺服器）。
10. 如果您在註冊後變更此畫面中的任何設定，請在變更設定後請點選「更新設定」，將變更通知 Apex Central 伺服器。

注意

如果 Apex Central 伺服器連線到沙盒虛擬平台，自動訂閱程序便會在註冊完成後開始。如需詳細資訊，請參閱可疑物件清單設定 第 14-31 頁。

11. 如果不想再讓 Apex Central 伺服器管理 Apex One，請點選「取消註冊」。

Apex Central 憑證授權

在向 Apex Central 伺服器註冊 Apex One 之前，您必須先從 Apex Central 伺服器的下列位置取得 Apex Central 憑證檔案：

```
<Apex Central 安裝資料夾>\Certificate\CA\TMCM_CA_Cert.pem
```

Apex One 和 Apex Central 會使用憑證和公開金鑰加密，來確保伺服器間僅進行授權的註冊與策略管理通訊。如果任一伺服器偵測到未經授權的通訊，該伺服器就會拒絕收到的任何註冊或策略設定。

重要

如果您的公司在 Apex Central 伺服器上使用自訂憑證，您必須在 Apex Central 註冊期間上傳根 CA 憑證。

在 Apex Central 管理主控台上檢查 Apex One 的狀態

步驟

1. 開啟 Apex Central 管理主控台。

   如果要開啟 Apex Central 主控台，請在網路上的任何一個端點上，開啟 Web 瀏覽器並輸入：

   ```
   https://<Apex Central 伺服器名稱>/Webapp/login.aspx
   ```

   其中 `<Apex Central 伺服器名稱>` 是 Apex Central 伺服器的 IP 位址或主機名稱

2. 在主功能表上，按一下「目錄 > 產品」。
3. 在顯示的樹狀結構中，移至「[Apex Central 伺服器] > 本機資料夾 > 新實體」資料夾。
4. 檢查 Apex One 伺服器圖示是否顯示。

Apex One 設定匯出工具

Apex One 提供 Apex One 設定匯出工具，可讓管理員將舊版 OfficeScan 中的 Apex One 設定複製到目前使用的版本。Apex One 設定匯出工具可用於移轉下列設定：

<table>
<tr><th>功能</th><th>移轉的設定</th></tr>
<tr><td>用戶端管理

注意
Apex One 設定匯出工具可將適當的用戶端管理設定移轉到 <code>ApexOne_Agent_DLP_Policies.zip</code> 和 <code>ApexOne_Agent_Policies.zip</code> 套件，以在匯入到 Apex Central 伺服器時使用。</td><td>• 手動掃瞄
• 預約掃瞄
• 即時掃瞄
• 立即掃瞄
• 掃瞄方法
• 網頁信譽評等
• 行為監控
• 周邊設備存取控管
• 資料外洩防護
• 權限和其他設定
• 其他服務設定
• 間諜程式/可能的資安威脅程式核可清單
• Machine Learning
• 可疑連線
• 信任的程式清單

注意
• 伺服器移轉工具不會移轉「手動掃瞄」、「預約掃瞄」、「即時掃瞄」和「立即掃瞄」的備份目錄。
• 設定會同時保留根和網域層級的設定。</td></tr>
<tr><td>用戶端分組</td><td>所有設定

注意
在首次與 Active Directory 同步處理後，將顯示 Active Directory 網域結構。</td></tr>
<tr><td>全域用戶端設定</td><td>所有設定</td></tr>
<tr><td>端點位置</td><td>• 位置偵測設定
• 閘道 IP 位址和 MAC 清單</td></tr>
</table>

功能	移轉的設定
資料外洩防護	• 資料識別碼 • 範本
防火牆	• 策略 • 資料檔
記錄檔維護	所有設定
用戶端更新來源	• 用戶端更新來源 • 自訂更新來源清單
主動雲端截毒伺服器來源	自訂主動雲端截毒技術來源清單
通知	• 一般通知設定 • 管理員通知設定 • 病毒爆發通知設定 • 用戶端通知設定
Proxy	所有設定
離線用戶端	所有設定
隔離區管理員	所有設定
Web 主控台	所有設定
`ofcscan.ini` 設定	• [INI_CLIENT_INSTALLPATH_SECTION] WinNT_InstallPath • [INI_REESTABLISH_COMMUNICATION_SECTION]：所有設定
`ofcserver.ini` 設定	[INI_SERVER_DISK_THRESHOLD]：所有設定

注意

- 此工具不會備份 OfficeScan 伺服器的 Security Agent 清單，而僅備份網域結構。
- 此工具只會移轉舊版 OfficeScan 伺服器上可用的功能。對於那些無法在舊版伺服器上使用的功能，此工具會套用預設設定。

使用 Apex One 設定匯出工具

注意

此版本的 Apex One 支援下列移轉：

- 內部部署 Apex One 伺服器：從 OfficeScan 11.0 版和更新版本
- Apex One as a Service 伺服器：從 OfficeScan XG Service Pack 1 版

如需 Apex One 設定匯出工具移轉之設定的完整清單，請參閱 Apex One 設定匯出工具 第 14-27 頁。

較舊的 OfficeScan 版本可能不包含可在 Apex One 最新版本中使用的所有設定。對於無法從舊版 OfficeScan 伺服器中移轉的任何功能，Apex One 會自動套用預設設定。

步驟

1. 找到「伺服器移轉工具」套件。
   - 在 Apex One Web 主控台中，移至「管理 > 設定 > 伺服器移轉」，然後點選「下載 Apex One 設定匯出工具」連結。
   - 在 Apex One 伺服器電腦上，瀏覽至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\PolicyExportTool。
2. 將 Apex One 設定匯出工具複製到來源 OfficeScan 伺服器電腦。

重要

您必須在來源 OfficeScan 伺服器版本使用 Apex One 設定匯出工具，以確保新目標伺服器所有資料的格式都正確。Apex One 與舊版的伺服器移轉工具不相容。

3. 使用管理權限開啟命令提示字元，切換到工具所在位置，然後執行 `ApexOneSettingsExportTool.exe`。

   Apex One 設定匯出工具隨即執行。

注意

匯出套件的預設名稱是：

- `ApexOne_Agent_DLP_Policies.zip`（用於將 DLP 策略設定匯入 Apex Central）
- `ApexOne_Agent_Policies.zip`（用於將所有其他 Security Agent 策略設定匯入 Apex Central）
- `Server_Settings_Migration.zip`（用於將所有 Security Agent 策略設定和 OfficeScan 伺服器設定匯入其他 Apex One 伺服器）

4. 將匯出套件複製到目的 Apex One 或 Apex Central 伺服器可以存取的位置。
5. 如果要將設定匯入目的 Apex One 伺服器：
   a. 在 Apex One Web 主控台中，移至「管理 > 設定 > 伺服器移轉」，然後點選「匯入設定...」按鈕。
   b. 找到 `Server_Settings_Migration.zip` 套件，然後點選「開啟」。
   c. 確認伺服器是否包含所有舊版的 OfficeScan 設定。
6. 如果要將 Security Agent 策略設定匯入目的 Apex Central 主控台：
   a. 在 Apex Central Web 主控台中，移至「策略 > 策略管理」。 >
   b. 在「產品」下拉式功能表中，選取「Apex One Security Agent」。
   c. 點選「匯入設定」。

d. 找到 `ApexOne_Agent_Policies.zip` 套件，然後點選「開啟」。

7. 如果要將 Security Agent DLP 策略設定匯入目的 Apex Central 主控台：

   a. 在 Apex Central Web 主控台中，移至「策略 > 策略管理」。>

   b. 在「產品」下拉式功能表中，選取「Apex One 資料外洩防護」。

   c. 點選「匯入設定」。

   d. 找到 `ApexOne_Agent_DLP_Policies.zip` 套件，然後點選「開啟」。

8. 將舊版 Security Agent 移到新 Apex One 伺服器。

   如需有關移動 Security Agent 的詳細資訊，請參閱將 Security Agent 移至其他網域或伺服器 第 2-56 頁或Agent Mover 第 15-21 頁。

可疑物件清單設定

可疑物件是 Trend Micro Deep Discovery 系列產品或其他來源做完分析後所產生的數位成品。Apex One 可以將 Control Manager 7.0 （或更新版本）或 Apex Central 2019（或更新版本）內部部署伺服器（與 Deep Discovery 連線）當成來源，來同步處理可疑物件，並擷取要對這些物件採取的處理行動。

訂閱 Control Manager 或 Apex Central 之後，請選取可疑物件的類型，以監控 C&C 回呼或用戶端在網路上識別的可能目標攻擊。可疑物件包括：

- 可疑 URL 清單
- 可疑 IP 清單
- 可疑檔案清單
- 可疑網域清單

注意

如果 Apex One 訂閱了 Deep Discovery Analyzer，則只能使用可疑 URL 清單。將 Apex One 取消訂閱 Deep Discovery Analyzer 之後，就無法重新訂閱。Apex One 必須訂閱與 Deep Discovery 有所關聯的 Apex Central，才能同步處理可疑物件。

如需有關 Apex Central 如何管理可疑物件的詳細資訊，請參閱《Apex Central 管理手冊》。

設定可疑物件清單設定

Apex One 向內部部署 Apex Central 註冊期間，Apex Central 會將 API 金鑰部署到 Apex One，以開始訂閱程序。若要啟動此自動訂閱程序，請洽詢 Apex Central 管理員以確保 Apex Central 已連線到沙箱，或已手動填入可疑物件清單。

如需向 Apex Central 伺服器註冊的詳細資訊，請參閱向 Apex Central 註冊 Apex One 第 14-23 頁。

步驟

1. 移至「管理 > 設定 > 可疑物件清單」。
2. 選取要在用戶端上啟動的清單。
   - 可疑 URL 清單
   - 可疑 IP 清單（僅在訂閱註冊的 Apex Central 或 Control Manager 伺服器時適用）
   - 可疑檔案清單（僅在訂閱註冊的 Apex Central 或 Control Manager 伺服器時適用）
   - 可疑網域清單（僅在訂閱註冊的 Apex Central 或 Control Manager 伺服器時適用）

   管理員可以隨時請點選「立即同步處理」按鈕，手動同步處理可疑物件清單。

3. 在「更新 Security Agent 上的可疑物件清單」下，指定用戶端更新可疑物件清單的時機。
   - 根據 Security Agent 元件更新預約時程：Security Agent 依照目前的更新預約時程更新可疑物件清單。
   - 自動在更新伺服器上的「可疑物件」清單後執行：在 Apex One 伺服器接收更新清單後，Security Agent 會自動更新可疑物件清單。

   注意

   Security Agent 未設定為從更新代理程式接收更新，其會在同步處理期間對所訂閱的可疑物件清單執行漸增式更新。

4. 請點選「儲存」。

參考伺服器

Security Agent 決定使用哪個策略或資料檔的一種方式是，檢查與 Apex One 伺服器的連線狀態。如果某個內部 Security Agent（或企業網路內的任何用戶端）無法連線到伺服器，則用戶端狀態會變成「離線」。用戶端接著會套用適用於外部用戶端的策略或資料檔。參考伺服器會解決這個問題。

與 Apex One 伺服器中斷連線的任何 Security Agent 會嘗試連線至參考伺服器。如果用戶端成功與參考伺服器建立連線，則會套用適用於內部用戶端的策略或資料檔。

策略或資料檔由參考伺服器管理，包括：

- 防火牆資料檔
- 網頁信譽評等策略
- 資料安全防護策略
- 周邊設備存取控管策略

請記住下列事項：

- 指定具有伺服器功能的電腦（例如：Web 伺服器、SQL 伺服器或 FTP 伺服器）做為參考伺服器。您最多可以指定 320 部參考伺服器。
- Security Agent 會連線至參考伺服器清單上的第一部參考伺服器。如果無法建立連線，用戶端會嘗試連線至清單上的下一部伺服器。
- Security Agent 會在判斷要使用的防毒軟體（行為監控、周邊設備存取控管、防火牆資料檔、網頁信譽評等策略）或資料安全防護設定時使用參考伺服器。參考伺服器不會管理用戶端或部署更新與用戶端設定。Apex One 伺服器會執行這些工作。
- Security Agent 無法將記錄檔傳送至參考伺服器或使用參考伺服器做為更新來源。

管理參考伺服器清單

步驟

1. 移至「用戶端 > 防火牆 > 資料檔」或「用戶端 > 端點位置」。
2. 請根據顯示的畫面執行下列動作：
   - 如果您在 用戶端的防火牆資料檔畫面上，請點選「編輯參考伺服器清單」。
   - 如果您在 端點位置畫面上，請點選「參考伺服器清單」。
3. 選取「啟動參考伺服器清單」。
   - 排除使用 VPN 或 PPP 撥號連線的用戶端：選取此選項可將使用 VPN 或 PPP（點對點通訊協定）撥接連線來連到參考伺服器的端點定義為「外部用戶端」
4. 如果要新增任何端點至清單，請點選「新增」。
   a. 指定端點的 IPv4/IPv6 位址、名稱或完整網域名稱 (FQDN)，例如：
      - `computer.networkname`
      - `12.10.10.10`

- `mycomputer.domain.com`

b. 輸入用戶端用來與此端點通訊的通訊埠。您可以指定參考伺服器上的任何開放聯絡通訊埠（例如：通訊埠 20、23 或 80）。

> **注意**
>
> 如果要為相同的參考伺服器指定其他通訊埠號碼，請重複步驟 2a 和 2b。Security Agent 會使用清單上的第一個通訊埠號碼，如果無法建立連線，會使用下一個通訊埠號碼。

c. 請點選「儲存」。

5. 如果要編輯清單上任何端點的設定，請點選端點名稱。修改端點名稱或通訊埠，然後請點選「儲存」。
6. 如果要從清單中移除任何端點，請選取端點名稱並請點選「刪除」。
7. 如果要讓端點做為參考伺服器，請點選「指定給用戶端」。

管理員通知設定

設定管理員通知設定，讓 Apex One 能夠透過電子郵件與 SNMP Trap 順利傳送通知。Apex One 還可以透過 Windows NT 事件記錄檔傳送通知，但沒有為此通知通道設定任何設定。

偵測到以下情況時，Apex One 會傳送通知給您和其他 Apex One 管理員：

表 14-16. 觸發管理員通知的偵測

偵測	通知管道		
	電子郵件	SNMP Trap	Windows NT 事件記錄檔
病毒和惡意程式	是	是	是
間諜程式和可能的資安威脅程式	是	是	是

偵測	通知管道		
	電子郵件	SNMP TRAP	WINDOWS NT 事件記錄檔
數位資產傳輸	是	是	是
C&C 回呼	是	是	是
病毒和惡意程式爆發	是	是	是
間諜程式和可能的資安威脅程式爆發	是	是	是
防火牆違規事件爆發	是	否	否
共享資料夾作業階段病毒爆發	是	否	否
C&C 回呼爆發	是	是	是

設定一般通知設定

步驟

1. 移至「管理 > 通知 > 一般設定」。
2. 設定電子郵件通知設定。
   a. 在「SMTP 伺服器」欄位中，指定 SMTP 伺服器的端點名稱或 IPv4/IPv6 位址。
   b. 指定 SMTP 伺服器所用的通訊埠。

      有效通訊埠號碼為 1 到 65535。
   c. 在「寄件人」欄位中，指定顯示為通知寄件人的電子郵件信箱。

      如果要在下一個步驟中啟動 ESMTP，請指定有效的電子郵件信箱。
   d. 您可以視需要啟動 ESMTP。

e. 為您在「寄件人」欄位中指定的電子郵件信箱指定使用者名稱和密碼。

f. 選擇向伺服器驗證用戶端的方式：

- 登入：登入是舊版的郵件使用者用戶端。伺服器和用戶端都使用 BASE64 來驗證使用者名稱和密碼。
- 純文字：純文字是最容易使用的方式，但這種方式不安全，因為使用者名稱和密碼是以一個使用 BASE64 編碼的字串透過 Internet 傳送。
- CRAM-MD5:CRAM-MD5 使用挑戰-回應組合的驗證機制和密碼編譯訊息摘要 5 演算法來交換及驗證資訊。
- NTLM：NTLM 驗證使用挑戰/回應機制來確保使用者提供給伺服器的密碼對使用者帳號來說是正確的。

  啟動「使用 SSL/TLS 加密」可進一步加密 NTLM 驗證。

3. 設定 SNMP Trap 通知設定。

   a. 在「伺服器 IP 位址」欄位中指定 IPv4/IPv6 位址或端點名稱。

   b. 指定不容易猜中的社群名稱。

   注意

   基於安全考量，社群名稱會顯示為使用星號 (*) 字元的遮罩值。預設指派的值為：“public”.

4. 請點選「儲存」。

系統事件記錄檔

Apex One 會記錄與關機和啟動等伺服器程式相關的事件。使用這些記錄檔確認 Apex One 伺服器和服務運作正常。

如果要避免記錄檔佔去過多硬碟空間，請手動刪除記錄檔或設定記錄檔刪除預約時程。如需有關管理記錄檔的詳細資訊，請參閱記錄檔管理 第 14-39 頁。

檢視系統事件記錄檔

步驟

1. 移至「記錄檔 > 系統事件」。
2. 在「事件」下方，檢查是否有需要採取進一步處理行動的記錄。Apex One 會記錄下列事件：

表 14-17. 系統事件記錄檔

記錄類型	事件
Apex One Master Service 和資料庫伺服器	• 已啟動主服務 • 已成功停止主服務 • 停止主服務不成功
病毒爆發防範	• 已啟動「病毒爆發防範」 • 已關閉「病毒爆發防範」 • 過去 <分鐘數> 內的共享資料夾作業階段數量
資料庫備份	• 資料庫備份成功 • 資料庫備份不成功
以角色為基礎的 Web 主控台存取	• 登入主控台 • 密碼修改 • 登出主控台 • 作業階段逾時（使用者自動登出）
伺服器驗證	• Security Agent 從伺服器接收到無效命令 • 驗證憑證無效或已過期

記錄類型	事件
沙箱	• 已提交樣本進行分析 • 樣本分析已完成 • 沙箱報告先前有另一台連線的 Apex One 伺服器提交了重複的樣本

3. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請點選「匯出到 CSV」。開啟檔案或將其儲存至特定位置。

記錄檔管理

Apex One 會製作有關安全威脅偵測、事件和更新的完整記錄檔。使用這些記錄檔，您可以存取組織的防護策略，並識別較有可能中毒或受到攻擊的 Security Agent。您也可以使用這些記錄檔檢查用戶端和伺服器間的連線，並驗證元件更新是否成功。

Apex One 還會使用中央時間驗證機制，確保 Apex One 伺服器和用戶端之間的時間一致。這會防止因時區、日光節約時間和時差所造成的記錄檔不一致情形，該情形會令人在分析記錄檔時產生混淆。

注意

Apex One 會針對除伺服器更新與系統事件記錄檔外的所有記錄檔執行時間驗證。

Apex One 伺服器從 Security Agent 接收以下記錄檔：

- 檢視病毒/惡意程式記錄檔 第 7-79 頁
- 檢視間諜程式/可能的資安威脅程式記錄檔 第 7-86 頁
- 檢視間諜程式/可能的資安威脅程式恢復記錄檔 第 7-89 頁
- 檢視防火牆記錄檔 第 13-26 頁

- 檢視網頁信譽評等記錄檔 第 12-19 頁
- 檢視可疑連線記錄檔 第 8-13 頁
- 檢視可疑檔案記錄檔 第 7-90 頁
- 檢視 C&C 回呼記錄檔 第 12-20 頁
- 檢視行為監控記錄檔 第 9-19 頁
- 檢視 Machine Learning 記錄檔 第 8-10 頁
- 檢視周邊設備存取控管記錄檔 第 10-17 頁
- 檢視掃瞄作業記錄檔 第 7-91 頁
- 檢視資料外洩防護記錄檔 第 11-52 頁
- 檢視 Security Agent 更新記錄檔 第 6-46 頁
- 檢視連線驗證記錄檔 第 15-38 頁

Apex One 伺服器會產生下列記錄檔：

- Apex One 伺服器更新記錄檔 第 6-24 頁
- 系統事件記錄檔 第 14-37 頁

在 Apex One 伺服器和 Security Agent 上還有以下記錄檔：

- Windows 事件記錄檔 第 18-22 頁
- Apex One 伺服器記錄檔 第 18-3 頁
- Security Agent 記錄檔 第 18-13 頁

記錄檔維護

如果要避免記錄檔佔去過多硬碟空間，請從 Web 主控台手動刪除記錄檔或設定記錄檔刪除預約時程。

根據預約時程刪除記錄檔

步驟

1. 移至「記錄檔 > 記錄檔維護」。
2. 選取「啟動記錄檔的預約刪除」。
3. 選取要刪除的記錄檔類型。根據預約時程刪除除偵錯記錄檔外的全部 Apex One 產生的記錄檔。對於偵錯記錄檔，請關閉偵錯記錄以停止收集記錄檔。

   注意

   對於病毒/惡意程式記錄檔，可以刪除某些掃瞄類型和損害清除及復原服務產生的記錄檔。對於間諜程式/可能的資安威脅程式記錄檔，可以刪除某些掃瞄類型產生的記錄檔。如需有關掃瞄類型的詳細資訊，請參閱掃瞄類型 第 7-12 頁。

4. 選取是刪除所有選定記錄檔類型的記錄檔，還是只刪除超過特定天數的記錄檔。
5. 指定記錄檔刪除頻率和時間。
6. 請點選「儲存」。

手動刪除記錄檔

步驟

1. 移至「記錄檔 > 用戶端 > 安全威脅」或「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請執行下列其中一個步驟：
   - 如果要存取「安全威脅記錄檔」畫面，請點選「刪除記錄檔」。

- 如果要存取「用戶端管理」畫面，請點選「記錄檔 > 刪除記錄檔」。

4. 在「要刪除的記錄檔類型」下方，選取要移除的記錄檔資料類型：
   - 行為監控記錄檔
   - C&C 回呼記錄檔
   - 資料外洩防護記錄檔
   - 周邊設備存取控管記錄檔
   - 防火牆記錄檔
   - Machine Learning 記錄檔
   - 間諜程式/可能的資安威脅程式記錄檔
   - 掃瞄作業記錄檔
   - 可疑連線記錄檔
   - 可疑檔案記錄檔
   - 病毒/惡意程式記錄檔
   - 網頁信譽評等記錄檔

   注意

   對於病毒/惡意程式記錄檔，可以刪除某些掃瞄類型和損害清除及復原服務產生的記錄檔。對於間諜程式/可能的資安威脅程式記錄檔，可以刪除某些掃瞄類型產生的記錄檔。

   如需有關掃瞄類型的詳細資訊，請參閱掃瞄類型 第 7-12 頁。

5. 在「要刪除的記錄檔」下方，選取下列其中一項：
   - 選定記錄檔類型的所有記錄檔：刪除所選記錄檔類型的所有記錄檔資料
   - 超過 XX 天的記錄檔：刪除超過為所選記錄檔類型指定之天數的所有記錄檔資料

6. 請點選「刪除」。

授權

在 Web 主控台檢視、啟動和續約 Apex One 使用授權。

注意

某些本機 Apex One 功能（例如資料安全防護和虛擬桌面支援）具有自己的使用授權。這些功能的使用授權會從 Plug-in Manager 進行啟動和管理。如需有關這些功能使用授權的詳細資訊，請參閱資料安全防護使用授權 第 3-3 頁和虛擬桌面支援使用授權 第 15-71 頁。

純 IPv6 Apex One 伺服器無法連線到趨勢科技線上註冊伺服器來啟動/續約該使用授權。如果要允許 Apex One 伺服器連線到註冊伺服器，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。

管理使用授權資訊

您可在「使用授權資訊」畫面中檢視您現有產品使用授權的詳細資訊，以及進行續約。

步驟

1. 移至「管理 > 設定 > 產品使用授權」。
2. 檢視使用授權資訊。

項目	說明
產品	產品使用授權的名稱
狀態	目前的使用授權狀態
類型	表示「完整版」或「試用版」產品授權

項目	說明
授權數目	獲授權向伺服器回報的 Security Agent 數目
到期日	使用授權到期日
啟動碼	目前已向 趨勢科技註冊的啟動碼
上次更新時間	上次從 趨勢科技伺服器擷取已更新的使用授權資訊的時間

3. 續約已到期或即將到期的使用授權。
   a. 按一下「指定啟動碼」。

      會出現「新啟動碼」畫面。
   b. 貼上或輸入新的啟動碼。
   c. 請點選「儲存」。

      會出現「使用授權資訊」畫面，其中顯示已更新的使用授權資訊。

SQL Server 資料庫連線設定

使用 SQL Server 資料庫組態設定工具，您可將 Apex One 伺服器連線到現有的其他 Apex One SQL 資料庫，並且變更用來連線到您現有資料庫的登入認證。

使用 SQL Server 資料庫組態設定工具可執行下列作業：

- 切換到其他已存在的 Apex One SQL Server 資料庫實體
- 更新現有 SQL Server 資料庫的登入認證
- 設定當 SQL Server 資料庫無法使用時的警訊設定

設定 SQL Server 資料庫連線

使用 SQL Server 資料庫組態設定工具，您可將 Apex One 伺服器連線到現有的其他 Apex One SQL 資料庫，並且變更用來連線到您現有資料庫的登入認證。

步驟

1. 在 Apex One 伺服器電腦上，瀏覽至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\SQL。
2. 按兩下 SQLTxfr.exe 執行此工具。

   「Apex One SQL Server 資料庫組態設定」主控台會隨即開啟。
3. 按照如下格式指定「伺服器名稱」：<SQL Server 的主機名稱或 IP 位址>,<通訊埠號碼>\<實體名稱>

   重要

   安裝 SQL Server 時，Apex One 會自動建立 Apex One 資料庫實體。移轉至現有 SQL Server 或資料庫時，請在 SQL Server 上輸入 Apex One 實體的先前存在的實體名稱。
4. 提供 SQL Server 資料庫的驗證憑證。
   - 使用「Windows 帳號」登入伺服器時，Apex One 會套用目前登入之使用者的「使用者名稱」。

     重要

     使用者帳號必須屬於本機管理員群組或 Active Directory (AD) 內建管理員，而您必須使用 Windows「本機安全性原則」或「群組原則管理」主控台設定「使用者權限指派」中的下列原則：
     - 以服務方式登入
     - 以批次工作登入
     - 允許本機登入

     使用者帳號還必須具有下列資料庫角色：
     - dbcreator
     - bulkadmin
     - db_owner
5. 在「資料庫名稱」區段中，指定 SQL Server 上的 Apex One 資料庫名稱。

6. 如果您在安裝期間設定了 Endpoint Sensor 資料庫，請指定 Endpoint Sensor 資料庫名稱。

   注意

   如果您的 Endpoint Sensor 資料庫位於與 Apex One 資料庫不同的 SQL 執行個體中，請參閱下列常見問題集文章，以瞭解如何管理資料庫。

   https://success.trendmicro.com/solution/1122929

7. 或者，執行下列工作：

   - 請點選「Apex One 資料庫無法使用警訊...」，設定 Apex One SQL 資料庫通知設定。

     如需詳細資訊，請參閱設定 Apex One 資料庫無法使用警訊 第 14-46 頁。

   - 請點選「測試連線」，確認現有 SQL Server 或資料庫的驗證憑證。

8. 請點選「開始」，套用組態變更。

設定 Apex One 資料庫無法使用警訊

每當 SQL 資料庫無法使用時，Apex One 會自動傳送此警訊。

警告!

當資料庫變得不可用時，Apex One 會自動停止所有服務。當資料庫不可用時，Apex One 無法記錄用戶端或事件資訊、執行更新或設定用戶端。

「資料庫無法使用」警訊僅適用於 Apex One 伺服器資料庫，不適用於 Endpoint Sensor 資料庫。

步驟

1. 在 Apex One 伺服器電腦上，瀏覽至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\SQL。

2. 按兩下 `SQLTxfr.exe` 執行此工具。

   「Apex One SQL Server 資料庫組態設定」主控台會隨即開啟。

3. 請點選「Apex One 資料庫無法使用警訊...」。

   「Apex One 資料庫無法使用警訊」畫面隨即開啟。

4. 輸入警訊收件者的電子郵件信箱。

   請使用半形分號 (;) 來分隔多個項目。

5. 視需要修改「主旨」和「訊息」。

   Apex One 提供下列 Token 變數：

   表 14-18. Apex One 資料庫無法使用警訊 Token

變數	說明
%x	Apex One SQL Server 實體的名稱
%s	受影響的 Apex One 伺服器的名稱

6. 請點選「確定」。

Apex One Web 伺服器/用戶端連線設定

在 Apex One 伺服器安裝期間，安裝程式會自動設定 Web 伺服器，讓用戶端電腦連線至 Apex One 伺服器。設定網路端點用戶端要連線的 Web 伺服器。

如果從外部修改了 Web 伺服器設定（例如，從 IIS 管理主控台），則請複製 Apex One 中的變更。例如，如果您手動變更用戶端電腦的伺服器 IP 位址，或是為伺服器指定動態 IP 位址，則需重新設定 Apex One 的伺服器設定。

警告!

變更連線設定可能導致永久中斷伺服器和用戶端之間的連線，且可能需要重新部署 Security Agent。

設定連線設定

步驟

1. 移至「管理 > 設定 > 用戶端連線」。
2. 輸入 Web 伺服器的網域名稱或 IPv4/IPv6 位址和通訊埠號碼。

   注意

   通訊埠號碼是 Apex One 伺服器與 Security Agent 通訊時所使用的信任的通訊埠。

3. 請點選「儲存」。

伺服器-用戶端通訊

您可以設定 Apex One，確保伺服器與用戶端之間的所有通訊都有效。Apex One 提供公開金鑰密碼編譯和加強加密功能，以保護伺服器與用戶端之間的所有通訊。

如需有關通訊保護功能的詳細資訊，請參閱下列內容：

- 伺服器開始之通訊的驗證 第 14-48 頁
- 加強的伺服器-用戶端通訊加密 第 14-52 頁

伺服器開始之通訊的驗證

Apex One 使用公開金鑰密碼編譯來驗證 Apex One 伺服器在用戶端上開始的通訊。使用公開金鑰密碼編譯時，伺服器可以保留私密金鑰並將公開金鑰部署到所有用戶端。用戶端使用公開金鑰確認輸入通訊是由伺服器開始的且有效。如果驗證成功，用戶端會發出回應。

注意

Apex One 不會驗證用戶端在伺服器上開始的通訊。

公開金鑰和私密金鑰均與趨勢科技憑證相關聯。在 Apex One 伺服器安裝期間，安裝程式將憑證儲存在主機的憑證儲存區中。使用「驗證憑證管理員」工具來管理趨勢科技憑證和金鑰。

決定是否對所有 Apex One 伺服器使用單一驗證金鑰時，請注意下列事項：

- 執行單一憑證金鑰是標準安全層級的常見做法。這種方式可平衡組織的安全層級，並降低維護多個金鑰相關的費用。
- 在 Apex One 伺服器之間執行多個憑證金鑰可提供最高的安全層級。這種方式會增加憑證金鑰到期及需要在伺服器之間重新分發時所需的維護。

重要

重新安裝 Apex One 伺服器之前，請確保您已備份現有憑證。新安裝完成之後，匯入備份的憑證以讓 Apex One 伺服器和 Security Agent 之間的通訊驗證不中斷。如果您在伺服器安裝期間建立了新憑證，則 Security Agent 無法驗證伺服器通訊，因為它們仍然使用舊憑證（已不再存在）。

如需有關備份、還原、匯出和匯入憑證的詳細資訊，請參閱使用驗證憑證管理員 第 14-49 頁。

使用驗證憑證管理員

Apex One 伺服器維護具有過期公開金鑰之 Security Agent 的過期憑證。例如，長期未連線至伺服器的 Security Agent 擁有過期的公開金鑰。Security Agent 重新連線時，它們會將過期公開金鑰與過期憑證關聯，以讓它們識別伺服器開始的通訊。然後，伺服器會將最新公開金鑰部署至 Security Agent。

設定憑證時，請注意下列事項：

- 針對憑證路徑，可接受對應磁碟機和 UNC 路徑。
- 選擇強式密碼，然後將其記錄下來以供日後參考。

重要

使用驗證憑證管理員工具時，請注意下列需求：

- 使用者必須具有管理員權限
- 此工具僅可管理位於本機端點的憑證

步驟

1. 在 Apex One 伺服器上，開啟命令提示字元，並將目錄變更為 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\CertificateManager。
2. 發出下列任何命令：

命令	範例	說明
`CertificateManager.exe -c [Backup_Password]`	`CertificateManager.exe -c strongpassword`	產生新的趨勢科技憑證，並取代現有憑證 如果現有憑證已過期或已洩漏給未經授權的人員，請執行此作業。
`CertificateManager.exe -r [Password] [Certificate path]` **注意** 憑證採用 ZIP 格式。	`CertificateManager.exe -r strongpassword D:\Test\TrendMicro.zip`	恢復伺服器上的所有趨勢科技憑證，並將憑證內容設定為可匯出 執行此作業可在重新安裝的 Apex One 伺服器上恢復憑證。

命令	範例	說明
`CertificateManager.exe -re [Password] [Certificate path]` **注意** 憑證採用 ZIP 格式。	`CertificateManager.exe -re strongpassword D:\Test\TrendMicro.zip`	恢復伺服器上的所有趨勢科技憑證，並將憑證內容設定為不可匯出 執行此作業可在重新安裝的 Apex One 伺服器上恢復憑證。
`CertificateManager.exe -e [Certificate path]`	`CertificateManager.exe -e <Agent_installation_folder>\OfcNTCer.dat`	匯出與目前使用之憑證關聯的 Security Agent 公開金鑰 如果端點使用的公開金鑰損毀，則執行此作業。將 `.dat` 檔案複製到端點的根資料夾，覆蓋現有檔案。 **重要** Security Agent 上憑證的檔案路徑必須是： `<Agent_installation_folder>\OfcNTCer.dat`

`CertificateManager.exe -ine [Password] [Certificate path]`
 	
注意
預設憑證檔案名稱是：
 	
`OfcNTCer.pfx`
	`CertificateManager.exe -ine strongpassword D:\Test\OfcNTCer.pfx`	將趨勢科技憑證匯出到憑證儲存區

命令	範例	說明
`CertificateManager.exe -l [CSV Path]`	`CertificateManager.exe -l D:\Test\MismatchedAgentList.csv`	列出目前正在使用不相符憑證的端點（採用 CSV 格式）

加強的伺服器-用戶端通訊加密

Apex One 使用進階加密標準 (AES) 256，為伺服器與用戶端通訊提供加強版加密，以符合政府安全性標準。

重要

Apex One 僅在執行 OfficeScan 11.0 SP1（或更新版本）及 Plug-in Manager 2.2（或更新版本）的伺服器和用戶端上支援 AES-256 加密。

警告!

確保在啟動 AES-256 加密前將伺服器管理的所有用戶端升級為 11.0 SP1 版。舊版用戶端可能無法解密 AES-256 加密的通訊。在舊版用戶端上啟動 AES-256 加密可能會導致在使用 Proxy 伺服器時與 Apex One 伺服器的通訊完全中斷。

步驟

1. 移至「用戶端 > 全域用戶端設定」。
2. 請點選「網路」標籤。
3. 移至「伺服器-用戶端通訊」區段。
4. 按一下「用於 Apex One 伺服器與 Security Agent 之間通訊的 AES-256 加密」旁邊的「變更」按鈕。

   接著會出現訊息。
5. 按一下「確認版本」，確認已將所有用戶端更新為 OfficeScan 11.0 SP1 或更新版本。

6. 請點選「確定」。

Web 主控台密碼

只有當伺服器電腦沒有使用以角色為基礎的管理所需的資源時，才能存取用於管理 Web 主控台密碼（或是安裝 Apex One 伺服器時建立的 root 帳號密碼）的畫面。如果有足夠的資源，就不會顯示此畫面，而且可以透過「使用者帳號」畫面修改 root 帳號來管理密碼。

如果 Apex One 未向 Apex Central 註冊，請聯絡您的經銷商，以獲得如何取得 Web 主控台存取權的指示。

設定 Web 主控台設定值

請設定 Apex One Web 主控台設定，以決定使用者存取 Web 主控台的方式，以及畫面重新整理的頻率。

步驟

1. 移至「管理 > 設定 > Web 主控台」。
2. 設定必要的設定。

區段	設定
自動重新整理設定	選取「自動重新整理 Web 主控台」，可使 Apex One 伺服器依照指定的時間間隔重新整理畫面資料 • 重新整理間隔：選取 Web 主控台重新整理畫面資料的頻率（以秒為單位）

區段	設定
逾時設定	選取「自動將閒置過久的使用者登出」，可使 Apex One 伺服器依照指定的時間間隔將使用者登出 • 閒置間隔：選取 Web 主控台在使用者閒置多長時間（以分鐘為單位）後自動將其登出

3. 請點選「儲存」。

隔離區管理員

Security Agent 只要偵測到安全威脅且中毒處理行動為隔離時，便會加密中毒檔案，再將其移至 <用戶端安裝資料夾>\SUSPECT 中的本機隔離資料夾。

將檔案移到本機隔離目錄之後，Security Agent 會將它傳送到指定的隔離目錄。此目錄是在「用戶端 > 用戶端管理 > 設定 > {掃瞄類型} 設定 > 處理行動」標籤中指定。用戶端會加密指定隔離目錄中的檔案，避免感染其他檔案。如需詳細資訊，請參閱隔離目錄 第 7-35 頁。

如果指定的隔離目錄位於 Apex One 伺服器電腦上，請從 Web 主控台修改伺服器的隔離目錄設定。伺服器會將隔離的檔案儲存在 <伺服器安裝資料夾>\PCCSRV\Virus 中。

注意

如果 Security Agent 因任何原因（例如：網路連線問題）而無法將加密的檔案傳送至 Apex One 伺服器，則加密的檔案會留在 Security Agent 隔離資料夾中。Security Agent 將在連線到 Apex One 伺服器時嘗試再次傳送檔案。

設定隔離目錄的設定

步驟

1. 移至「管理 > 設定 > 隔離區管理員」。

2. 接受或修改隔離資料夾的預設容量，以及 Apex One 能夠在隔離資料夾中儲存的中毒檔案大小上限。

   預設值會顯示在畫面中。

3. 請點選「儲存隔離設定」。

4. 如果要移除隔離資料夾中所有現有的檔案，請點選「刪除所有隔離檔案」。

Server Tuner

使用 Server Tuner 即可將參數用於下列伺服器相關效能問題，以將 Apex One 伺服器的效能最佳化：

- 下載

  當向 Apex One 伺服器要求更新的 Security Agent 數目（包括更新代理程式）超出伺服器的可用資源時，伺服器便會將用戶端更新要求移到佇列中，並在資源可用時處理要求。用戶端成功從 Apex One 伺服器更新元件後，會通知伺服器已完成更新。請設定 Apex One 伺服器從用戶端接收更新通知之前等待的分鐘數上限。也請設定伺服器嘗試通知用戶端執行更新並套用新組態設定的次數上限。伺服器如果沒有收到用戶端通知，就會一直嘗試。

- 網路傳輸

  網路傳輸量在一天之中會有所不同。如果要控制到 Apex One 伺服器和其他更新來源的網路傳輸流量，請指定在一天之中的特定時間可以同時更新的 Security Agent 數目。

Server Tuner 需要下列檔案：`SvrTune.exe`

執行 Server Tuner

步驟

1. 在 Apex One 伺服器電腦上，移至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\SvrTune。
2. 按兩下 SvrTune.exe 啟動 Server Tuner。

   隨即開啟 Server Tuner 主控台。
3. 修改「下載」下方的下列設定：
   - 用戶端逾時：輸入 Apex One 伺服器從 Security Agent 接收更新回應之前等待的分鐘數上限。如果用戶端未能在此時間內回應，Apex One 伺服器會認為 Security Agent 沒有最新的元件。如果收到通知的 Security Agent 逾時，則會開放位置給等待通知的其他用戶端。
   - 更新代理程式逾時：輸入 Apex One 伺服器從「更新代理程式」接收更新回應之前等待的分鐘數上限。如果收到通知的 Security Agent 逾時，則會開放位置給等待通知的其他用戶端。
   - 重試總數：輸入 Apex One 伺服器嘗試通知 Security Agent 執行更新或套用新組態設定的次數上限。
   - 重試間隔：輸入 Apex One 伺服器在通知嘗試間等待的分鐘數。
4. 修改「網路傳輸」下的下列設定：
   - 一般時間：請點選代表一天之中您認為網路傳輸正常的時間的圓形按鈕。
   - 離峰時間：請點選代表一天之中您認為網路傳輸最低的時間的圓形按鈕。
   - 尖峰時間：請點選代表一天之中您認為網路傳輸最高的時間的圓形按鈕。
   - 用戶端連線上限：輸入可從「其他更新來源」和 Apex One 伺服器同時更新元件的用戶端數目上限。請為各個時段輸入用戶端數目上限。當達到連線數目上限時，Security Agent 必須等到目前的 Security Agent 連線關閉（因為更新完成或是用戶端回應達到您在「用戶端逾

時」或「更新代理程式逾時」欄位中指定的逾時值）後才能更新元件。

5. 請點選「確定」。隨即出現提示，詢問您是否要重新啟動「Apex One Master Service」。

注意

會重新啟動服務，但不會重新啟動電腦。

6. 請選取下列重新啟動選項：

   - 請點選「是」儲存 Server Tuner 設定並重新啟動服務。設定會在重新啟動之後立即生效。
   - 請點選「否」則會儲存 Server Tuner 設定，但不會重新啟動服務。請重新啟動「Apex One Master Service」或重新啟動 Apex One 伺服器電腦，以讓設定生效。

Smart Feedback

趨勢科技 Smart Feedback 會以匿名方式將安全威脅資訊與主動雲端截毒技術共享，讓趨勢科技可以迅速識別和處理新的安全威脅。您可以隨時透過這個主控台關閉 Smart Feedback 系統。

參與 Smart Feedback 系統程式

步驟

1. 移至「管理 > 主動式雲端截毒技術」。
2. 請點選 「啟動趨勢科技 Smart Feedback」。
3. 如果要協助趨勢科技瞭解您的組織，請選取「產業」類型。

4. 如果要傳送關於您 Security Agent 上檔案中潛在安全威脅的資訊，請選取「啟動對可疑程式檔案的意見反應」核取方塊。

   注意

   傳送給 Smart Feedback 的檔案未含任何使用者資料，僅提交做威脅分析之用。

5. 如果要設定傳送意見反應的條件，請針對特定時間長度選取要觸發意見反應時需達到的偵測次數。

6. 指定 Apex One 在傳送意見反應時可使用的最大頻寬，以將網路中斷造成的影響降至最低。

7. 請點選「儲存」。

第 15 章

管理 Security Agent

本章說明 Security Agent 管理和組態設定。

包含下列主題：

端點位置

Apex One 提供位置偵測功能，可判斷 Security Agent 位於內部還是外部網路。下列 Apex One 功能和服務使用位置偵測：

表 15-1. 使用位置偵測的功能和服務

功能/服務	說明
檔案信譽評等服務	對於雲端截毒掃瞄用戶端，Security Agent 位置會決定主動雲端截毒伺服器來源（Security Agent 的掃瞄查詢傳送目標）。 外部 Security Agent 會將掃瞄查詢傳送到主動雲端截毒技術，而內部 Security Agent 會將掃瞄查詢傳送到主動雲端截毒伺服器來源清單中定義的來源。 如需詳細資訊，請參閱主動雲端截毒伺服器來源 第 4-5 頁。
網頁信譽評等 資料外洩防護 周邊設備存取控管	Security Agent 位置會決定 Security Agent 是套用內部還是外部策略設定。管理員通常會針對外部 Security Agent 實施較嚴格的策略。 如需詳細資訊，請參閱： • 網頁信譽評等策略 第 12-4 頁. • 資料外洩防護策略 第 11-3 頁 • 周邊設備存取控管 第 10-2 頁

位置條件

指定位置是以 Security Agent 端點的閘道 IP 位址為準，還是以 Security Agent 與 Apex One 伺服器或任何參考伺服器的連線狀態為準。

- 用戶端連線狀態：如果 Security Agent 可以連線至 Apex One 伺服器或 Intranet 上任何指定的參考伺服器，端點位置就是內部的。此外，如果企業網路外部的任何端點可以與 Apex One 伺服器/參考伺服器建立連線，則該端點的位置也是內部的。如果上述條件都不符合，端點的位置就是外部的。

- 閘道 IP 和 MAC 位址：如果 Security Agent 端點的閘道 IP 位址符合您在端點位置 畫面上指定的任一閘道 IP 位址，則該端點的位置是內部的。否則，端點的位置就是外部的。

設定位置設定

步驟

1. 移至「用戶端 > 端點位置」。
2. 選擇位置是以「用戶端連線狀態」還是以「閘道 IP 與 MAC 位址」為準。
3. 如果選擇「用戶端連線狀態」，請決定是否要使用參考伺服器。

   如需詳細資訊，請參閱參考伺服器 第 14-33 頁。

   a. 如果您沒有指定參考伺服器，當發生下列事件時，Security Agent 會檢查 Apex One 伺服器的連線狀態：

      - Security Agent 從單機模式切換到一般（線上/離線）模式。
      - Security Agent 從一種掃瞄方法切換到另一種掃瞄方法。

        如需詳細資訊，請參閱掃瞄方法類型 第 7-7 頁。
      - Security Agent 偵測到端點發生 IP 位址變更。
      - Security Agent 重新啟動。
      - 伺服器開始連線驗證。

        如需詳細資訊，請參閱 Security Agent 圖示 第 15-24 頁。
      - 網頁信譽評等位置條件在套用全域設定時變更。
      - 病毒爆發防範策略已經不再執行，而且已經恢復病毒爆發前的設定。

   b. 如果您已經指定參考伺服器，則 Security Agent 會先檢查與 Apex One 伺服器的連線狀態，如果無法連線至 Apex One 伺服器，再檢查與參考伺服器的連線狀態。Security Agent 會在每個小時以及發生上述事件時檢查連線狀態。

4. 如果選擇「閘道 IP 與 MAC 位址」：

   a. 在提供的文字方塊中輸入閘道 IPv4/IPv6 位址。

   b. 輸入 MAC 位址。

   c. 請點選「新增」。

      如果您不是輸入 MAC 位址，Apex One 會包含所有屬於特定 IP 位址的 MAC 位址。

   d. 重覆步驟 a 到步驟 c，直到完成所有要新增的閘道 IP 位址。

   e. 使用「閘道設定匯入程式」工具匯入閘道設定清單。

      如需詳細資訊，請參閱閘道設定匯入程式 第 15-4 頁。

5. 請點選「儲存」。

閘道設定匯入程式

Apex One 會檢查端點的位置以決定要使用的網頁信譽評等策略，以及要連線的主動雲端截毒伺服器來源。Apex One 識別位置的其中一個方式，就是檢查端點的閘道 IP 位址與 MAC 位址。

您可以在「端點位置」畫面設定閘道設定，或使用「閘道設定匯入程式」工具將閘道設定清單匯入至「端點位置」畫面。

使用閘道設定匯入程式

步驟

1. 準備含有閘道設定清單的文字檔 (`.txt`)。在每一行中輸入 IPv4 或 IPv6 位址並選擇性地輸入 MAC 位址。

   請以逗號分隔 IP 位址與 MAC 位址。項目的最大數值為 4096。

   例如：

```
10.1.111.222,00:17:31:06:e6:e7

2001:0db7:85a3:0000:0000:8a2e:0370:7334

10.1.111.224,00:17:31:06:e6:e7
```

2. 在伺服器電腦上，移至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\GatewaySettingsImporter。
3. 以滑鼠右鍵請點選 GSImporter.exe，然後選取「以系統管理員身分執行」。

注意

您無法從「終端機服務」執行「閘道設定匯入程式」工具。

---

4. 在「閘道設定匯入程式」畫面上，瀏覽至步驟 1 中所建立的檔案，然後請點選「匯入」。
5. 請點選「確定」。

   閘道設定會顯示在「端點位置」畫面上，而且 Apex One 伺服器會將這些設定部署至 Security Agent。
6. 如果要刪除所有項目，請點選「全部清除」。

   如果只需要刪除特定項目，請將其從「端點位置」畫面移除。
7. 如果要將設定匯出至檔案，請點選「全部匯出」，然後指定檔案名稱與類型。

Security Agent 程式管理

下列主題討論管理和保護 Security Agent 程式的方式：

- Security Agent 服務 第 15-6 頁
- 重新啟動 Security Agent 服務 第 15-14 頁

Security Agent 服務

Security Agent 會執行下列表格中所列的服務。您可以從 Microsoft 管理主控台檢視這些服務的狀態。

表 15-2. 預設處理程序

處理程序	說明	位置
TmListen.exe	接收來自 Apex One 伺服器的指令與通知，並促進 Security Agent 與伺服器之間的通訊	<用戶端安裝資料夾>\tmlisten.exe
NTRtScan.exe	在 Security Agent 上執行即時、預約與手動掃瞄	<用戶端安裝資料夾>\ntrtscan.exe
TmPfw.exe	提供封包層級防火牆、網路病毒掃瞄和入侵偵測功能	<用戶端安裝資料夾>\TmPfw.exe
TMBMSRV.exe	規範對於外部儲存裝置的存取，並防止未經授權變更登錄機碼和程序 注意 如果啟動此選項，Security Agent 可能會使得您無法在端點上成功地安裝協力廠商產品。如果遇到此問題，您可以先暫時關閉此選項，然後在安裝完協力廠商產品之後重新啟動此選項。	<%Program Files (x86) 資料夾%>\Trend Micro\BM\TMBMSRV.exe

處理程序	說明	位置
TmCCSF.exe	執行瀏覽器弱點攻擊防護和記憶體掃瞄	<用戶端安裝資料夾>\CCSF \TmCCSF.exe
TmWSCSvc.exe	將 Apex One Security Agent 的安全狀態回報給安全中心	<用戶端安裝資料夾> \TmWSCSvc.exe

表 15-3. 擴充功能處理程序

處理程序	說明	位置
DSAgent.exe	監控機密資料的傳輸並控制對裝置的存取權	<%Windows 目錄%> \system32\dgagent \DSAGENT.exe
ATASAgent.exe	進階 Managed Detection and Response 工作與通訊	<%Program Files (x86) 資料夾%> \Trend Micro \iService\iATAS \ATASAgent.exe
TMiACAgentSvc.exe	Trend Micro Application Control Service（用戶端）	<%Program Files (x86) 資料夾%> \Trend Micro \iService\iAC \ac_bin \TMiACAgentSvc.exe
ESEServiceShell.exe	Trend Micro Endpoint Sensor 引擎封裝程式	<%Program Files (x86) 資料夾%> \Trend Micro \iService\iES \ESE \ESEServiceShell.exe

處理程序	說明	位置
ESClient.exe	Trend Micro Endpoint Sensor Service（用戶端）	C:\Program Files (x86)\Trend Micro\iService \iES\ESE \ESClient.exe
iVPAgent.exe	Trend Micro Vulnerability Protection Service（用戶端）	<%Program Files (x86) 資料夾%> \Trend Micro \iService\iVP \iVPAgent.exe

下列服務提供強固的安全防護，但其監控機制會使用系統資源，特別是在執行特別需要系統資源的應用程式的伺服器上：

- 趨勢科技未經授權的變更阻止服務 (TMBMSRV.exe)
- Apex One NT Firewall (TmPfw.exe)
- Apex One Data Protection Service (dsagent.exe)

因此，Windows Server 平台預設會關閉這些服務。如果要啟動這些服務：

- 持續監控系統效能，並在發現效能變差時採取必要的處理行動。
- 對於 TMBMSRV.exe，如果您將耗用大量系統資源的應用程式從「行為監控」策略排除，則可以啟動該服務。您可以使用效能調整工具來識別耗用大量系統資源的應用程式。

  如需詳細資訊，請參閱使用趨勢科技效能調整工具 第 15-13 頁。

對於桌上型電腦平台，只有在發現效能嚴重變差時才需要關閉那些服務。

排除協力廠商應用程式中的 Security Agent 服務及程序

下表列出您可能需要從協力廠商應用程式中排除的 Security Agent 程序的程序名稱及完整檔案位置。

表 15-4. 預設處理程序

處理程序	說明	位置
TmListen.exe	接收來自 Apex One 伺服器的指令與通知，並促進 Security Agent 與伺服器之間的通訊	<用戶端安裝資料夾>\tmlisten.exe
NTRtScan.exe	在 Security Agent 上執行即時、預約與手動掃瞄	<用戶端安裝資料夾>\ntrtscan.exe
TmPfw.exe	提供封包層級防火牆、網路病毒掃瞄和入侵偵測功能	<用戶端安裝資料夾>\TmPfw.exe
TMBMSRV.exe	規範對於外部儲存裝置的存取，並防止未經授權變更登錄機碼和程序 注意 如果啟動此選項，Security Agent 可能會使得您無法在端點上成功地安裝協力廠商產品。如果遇到此問題，您可以先暫時關閉此選項，然後在安裝完協力廠商產品之後重新啟動此選項。	<%Program Files (x86) 資料夾%>\Trend Micro\BM\TMBMSRV.exe
TmCCSF.exe	執行瀏覽器弱點攻擊防護和記憶體掃瞄	<用戶端安裝資料夾>\CCSF\TmCCSF.exe
TmWSCSvc.exe	將 Apex One Security Agent 的安全狀態回報給安全中心	<用戶端安裝資料夾>\TmWSCSvc.exe

表 15-5. 擴充功能處理程序

處理程序	說明	位置
DSAgent.exe	監控機密資料的傳輸並控制對裝置的存取權	<%Windows 目錄%>\system32\dgagent\DSAGENT.exe

處理程序	說明	位置
ATASAgent.exe	進階 Managed Detection and Response 工作與通訊	<%Program Files (x86) 資料夾%>\Trend Micro\iService\iATAS\ATASAgent.exe
TMiACAgentSvc.exe	Trend Micro Application Control Service（用戶端）	<%Program Files (x86) 資料夾%>\Trend Micro\iService\iAC\ac_bin\TMiACAgentSvc.exe
ESEServiceShell.exe	Trend Micro Endpoint Sensor 引擎封裝程式	<%Program Files (x86) 資料夾%>\Trend Micro\iService\iES\ESE\ESEServiceShell.exe
ESClient.exe	Trend Micro Endpoint Sensor Service（用戶端）	C:\Program Files (x86)\Trend Micro\iService\iES\ESE\ESClient.exe
iVPAgent.exe	Trend Micro Vulnerability Protection Service（用戶端）	<%Program Files (x86) 資料夾%>\Trend Micro\iService\iVP\iVPAgent.exe

表 15-6. 其他受保護的處理程序

處理程序	位置
ShowMsg.exe	<%Windows 目錄%>\System32\ShowMsg.exe
TmSSClient.exe	<用戶端安裝資料夾>\TmSSClient.exe

處理程序	位置
LogServer.exe	<用戶端安裝資料夾>\Temp\LogServer\LogServer.exe
TmsaInstance64.exe	<用戶端安裝資料夾>\CCSF\module\BES\TmsaInstance64.exe
CNTAoSMgr.exe	<用戶端安裝資料夾>\CNTAoSMgr.exe
ESEFrameworkHost.exe	<%Program Files (x86) 資料夾%>\Trend Micro\iService\iES\ESE\ESEFrameworkHost.exe

設定其他 Security Agent 服務

重要

啟動 Windows Server 平台上的其他服務可能會影響伺服器的效能。啟動 Windows Server 平台上的服務後，趨勢科技建議您監控伺服器一段時間，以確保效能未受影響。

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 ( ) 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請按一下「設定 > 其他服務設定」。
4. 在下列區段中選取選項，以啟動「Windows 桌上型電腦」或「Windows Server 平台」上的必要服務：
   - 未經授權的變更阻止服務

     對於 Windows Server 平台，選取要啟動的保護層級。

     - 完整模式：啟動所有服務並允許完整存取全部功能
     - 效能模式：啟動服務的輕量版本，僅允許啟動以下功能，並忽略「完整模式」下可用的所有其他設定：

- 「行為監控 > 啟動惡意程式行為封鎖 > 保護文件以防止未經授權的加密或修改」

重要

效能模式不會自動啟動任何設定。啟動某個特定功能後，「未經授權的變更阻止服務」只會啟動支援的功能並忽略所有不受支援的設定。

- 防火牆服務

重要

啟動或關閉服務會暫時中斷端點與網路的連線。請務必在非繁忙時段變更設定，以將連線中斷造成的影響降至最低。

- 可疑連線服務
- 資料安全防護服務

重要

啟動或關閉服務會暫時中斷端點與網路的連線。請務必在非繁忙時段變更設定，以將連線中斷造成的影響降至最低。

- 進階防護服務

5. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

使用趨勢科技效能調整工具

步驟

1. 從下列位置下載「趨勢科技效能調整工具」：

   http://esupport.trendmicro.com/solution/zh-tw/1074941.aspx

2. 將 `TMPerfTool.exe` 從 `TMPerfTool.zip` 中解壓縮出來。

3. 將 `TMPerfTool.exe` 放在 <用戶端安裝資料夾> 中或 `TMBMCLI.dll` 所在的同一資料夾中。

4. 以滑鼠右鍵請點選 `TMPerfTool.exe`，然後選取「以系統管理員身分執行」。

5. 閱讀並接受終端使用者合約，然後請點選「確定」。

6. 請點選「分析」。

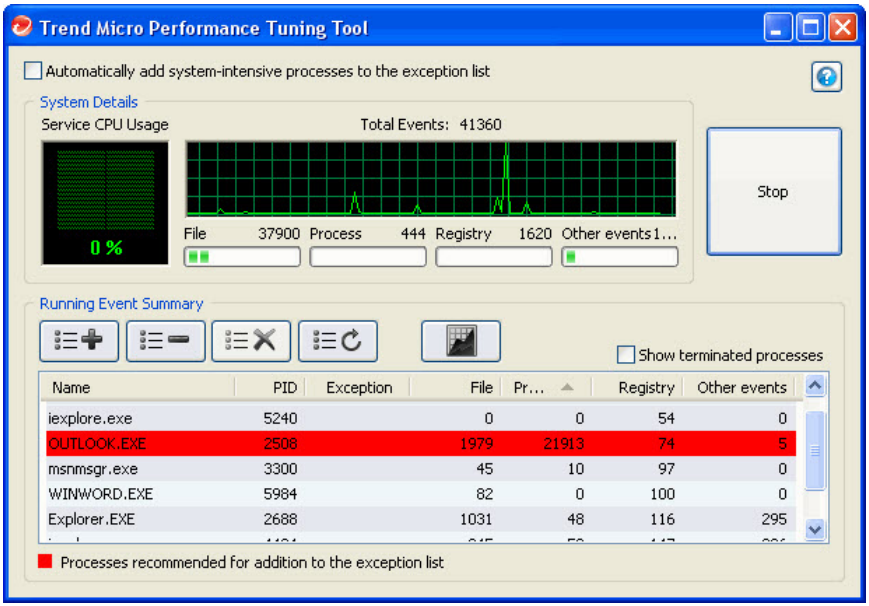


圖 15-1. 系統會反白顯示耗用大量系統資源的處理程序

此工具會開始監控 CPU 使用狀況與事件負載。系統會以紅色反白顯示耗用大量系統資源的處理程序。

7. 選取耗用大量系統資源的處理程序，然後請點選「新增至例外清單（允許）」按鈕（  ）。

8. 檢查系統或應用程式效能是否變好。

9. 如果效能變好，請再選取一次該處理程序，然後請點選「從例外清單移除」按鈕（  ）。

10. 如果效能再次變差，請執行下列步驟：

    a. 請記下應用程式的名稱。

    b. 請點選「停止」。

    c. 請點選「產生報告」按鈕（  ）然後儲存 `.xml` 檔案。

    d. 檢視系統識別為發生衝突的應用程式，然後將它們新增到「行為監控」例外清單。

       如需詳細資訊，請參閱行為監控例外清單 第 9-7 頁。

重新啟動 Security Agent 服務

Apex One 會重新啟動意外停止回應的 Security Agent 服務，以及不是由正常系統處理程序停止的用戶端服務。如需有關用戶端服務的詳細資訊，請參閱Security Agent 服務 第 15-6 頁。

設定讓 Security Agent 服務重新啟動的必要設定。

設定服務重新啟動設定

步驟

1. 移至「用戶端 > 全域用戶端設定」。

2. 請點選「系統」標籤。
3. 移至「服務重新啟動」區段。
4. 選取「如果任何 Security Agent 服務意外終止，則自動重新啟動該服務」。
5. 設定下列項目：
   - 在 __ 分鐘之後重新啟動服務：指定 Apex One 重新啟動服務之前的等候時間（以分鐘為單位）。
   - 如果第一次嘗試重新啟動服務未成功，請重試 __ 次：指定嘗試重新啟動服務的重試次數上限。如果經過指定的重試次數上限之後服務仍為停止狀態，請手動重新啟動服務。
   - 在 _ 小時之後重設重新啟動失敗計數：如果嘗試重試的次數達到上限後服務仍為停止狀態，Apex One 會等候特定的小時數，然後重設失敗計數。如果服務在經過指定的時數之後仍為停止狀態，則 Apex One 會重新啟動服務。

Security Agent 主控台存取限制

此設定可關閉從系統匣或 Windows「開始」功能表存取 Security Agent 主控台的功能。使用者存取 Security Agent 主控台的唯一方式是按兩下 <用戶端安裝資料夾> 中的 `PccNTMon.exe`。進行此設定後，請重新載入 Security Agent 以讓設定生效。

此設定不會關閉 Security Agent。Security Agent 會在背景中執行並持續提供安全威脅防護。

限制對 Security Agent 主控台的存取

步驟

1. 移至「用戶端 > 用戶端管理」。

2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 權限和其他設定」。
4. 按一下「其他設定」標籤，然後移至「Security Agent 存取限制」區段。
5. 選取「不允許使用者從系統匣或 Windows「開始」功能表存取 Security Agent 主控台」。
6. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

Security Agent 結束與解除鎖定

Security Agent 結束與解除鎖定權限可讓使用者暫時停止 Security Agent，或者不論是否擁有密碼都能取得進階 Web 主控台功能的存取權。

授與用戶端卸載與解除鎖定權限

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 權限和其他設定」。
4. 在「權限」標籤中，移至「結束並解除鎖定」區段。

5. 設定密碼需求。
   - 不需要密碼
   - 需要密碼：輸入要求的密碼和確認密碼

   注意

   密碼必須符合下列複雜度要求：
   - 長度為 8 到 32 字元
   - 以下每項包含至少一個：大寫字母 (A-Z)、小寫字母 (a-z)、數字 (0-9) 和特殊字元
   - 不可包含非可列印 ASCII 字元

6. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

Security Agent 單機模式權限

如果用戶端與伺服器之間的事件會干擾使用者的工作，您可以將 Security Agent 單機模式權限授與特定使用者。例如，經常做簡報的使用者可以在開始簡報之前先啟動單機模式，以防止 Apex One 伺服器在該 Security Agent 上部署 Security Agent 設定並開始掃瞄。

當 Security Agent 處於單機模式時：

- Security Agent 不會傳送記錄檔到 Apex One 伺服器，即使伺服器與用戶端間有正常運作的連線也一樣。
- Apex One 伺服器不會在用戶端上開始工作，也不會將 Security Agent 設定部署到用戶端，即使伺服器與用戶端間有正常運作的連線也一樣。

- 如果 Security Agent 可以連線到其任何更新來源，則會更新元件。來源包含 Apex One 伺服器、更新代理程式或自訂更新來源。

  下列事件會在單機用戶端上觸發更新動作：

  - 使用者執行手動更新時。
  - 自動用戶端更新執行時。您可以關閉單機用戶端上的自動用戶端更新。

    如需詳細資訊，請參閱在單機用戶端上關閉自動用戶端更新 第 15-19 頁。
  - 預約更新執行時。只有具有必要權限的用戶端可以執行預約更新。您可以隨時撤銷此權限。

    如需詳細資訊，請參閱在單機用戶端上撤銷預約更新權限 第 15-19 頁。

授與用戶端單機模式權限

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 權限和其他設定」。
4. 在「權限」標籤中，移至「單機模式」區段。
5. 選取「啟動單機模式」。
6. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。

- 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

在單機用戶端上關閉自動用戶端更新

步驟

1. 移至「更新 > 用戶端 > 自動更新」。
2. 移至「事件觸發更新」區段。
3. 關閉「包含單機與離線用戶端」。

> 注意
>
> 如果關閉「在 Apex One 伺服器下載新元件之後，立即在用戶端上開始元件更新」，系統會自動關閉此選項。

在單機用戶端上撤銷預約更新權限

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 或選取特定的網域或用戶端。
3. 請點選「設定 > 權限和其他設定」。
4. 在「權限」標籤上，移至「元件更新」區段。
5. 清除「啟動/關閉預約更新」選項。
6. 請點選「儲存」。

Security Agent 語言組態設定

您可以將所有 Security Agent 設定為使用 Apex One 伺服器語言設定或本機登入使用者語言設定顯示。在安裝或升級 Security Agent 程式後，用戶端會套用在「全域設定」畫面上設定的語言設定。

依預設，如果 Security Agent 不支援登入使用者的語言設定，語言設定預設為 Apex One 伺服器語言，然後是英語。

設定 Security Agent 語言設定

步驟

1. 移至「用戶端 > 全域用戶端設定」。
2. 請點選「用戶端控制」標籤。
3. 移至「用戶端語言組態設定」區段。
4. 指定 Security Agent 套用語言設定的方式：
   - 端點上的本機語言設定：Security Agent 會使用已登入使用者的語言設定來顯示。

     注意

     如果 Security Agent 不支援登入使用者語言設定，用戶端會套用 Apex One 伺服器語言。如果端點不支援 Apex One 伺服器語言，則顯示英文。

   - Apex One 伺服器語言：Security Agent 會使用 Apex One 伺服器語言來顯示。

     注意

     如果端點不支援 Apex One 伺服器語言，則顯示英文。

5. 請點選「儲存」。

Agent Mover

如果網路上有多部 Apex One 伺服器，您可以使用 Agent Mover 工具將 Security Agent 從某一部 Apex One 伺服器轉移到另一部。將新的 Apex One 伺服器新增至網路之後，當您要將現有的 Security Agent 轉移至新的伺服器時，這個工具會特別有用。

注意

兩部伺服器必須為相同語言的版本。如果您使用 Agent Mover 將執行舊版的任何 Security Agent 移到最新版本的伺服器，則 Security Agent 會自動升級。

使用此工具之前，請先確定您使用的帳號具有管理員權限。

執行 Agent Mover

步驟

1. 在 Apex One 伺服器上，移至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\IpXfer。
2. 將 IpXfer.exe 複製到 Security Agent 端點。如果 Security Agent 端點執行的是 x64 類型平台，請改為複製 IpXfer_x64.exe。
3. 在 Security Agent 端點上，開啟命令提示字元，然後移至放置複製的可執行檔案的資料夾。
4. 使用下列語法執行 Agent Mover：

   <可執行檔案名稱> -s <伺服器名稱> -p <伺服器監聽通訊埠> -c <用戶端監聽通訊埠> -d <網域或網域階層> -e <憑證位置和檔案名稱> -pwd <用戶端結束與解除鎖定權限密碼>

   表 15-7. Agent Mover 參數

參數	說明
<可執行檔案名稱>	IpXfer.exe 或 IpXfer_x64.exe

參數	說明
-s <伺服器名稱>	目標 Apex One 伺服器（Security Agent 將轉移到的伺服器）的名稱
-p <伺服器監聽通訊埠>	目標 Apex One 伺服器的監聽通訊埠（或信任的通訊埠）（僅限本機伺服器） 如果要在 Apex One Web 主控台上檢視監聽通訊埠，請按一下主功能表中的「管理 > 設定 > 用戶端連線」。
-sp <伺服器 HTTPS 監聽通訊埠>	目標 Apex One 伺服器用於 HTTPS 通訊的監聽通訊埠（或信任的通訊埠）
-c <用戶端監聽通訊埠>	Security Agent 端點用來與伺服器通訊的通訊埠號碼
-d <網域或網域階層>	用戶端將在其中分組的用戶端樹狀結構網域或子網域 網域階層應該指出子網域。
-e <憑證位置和檔案名稱>	在移動程序期間，為 Security Agent 匯入新的驗證憑證 如果此參數未使用，則 Security Agent 會自動從其新的管理伺服器擷取目前的驗證憑證。 **注意** 憑證在 Apex One 伺服器上的預設位置為： <伺服器安裝資料夾>\PCCSRV\Pccnt\Common\OfcNTCer.dat。 從 Apex One 以外的來源使用憑證時，請確定該憑證使用唯一編碼規則 (DER) 的格式。
-pwd <用戶端結束與解除鎖定權限密碼>	「權限和其他設定」中設定的結束與解除鎖定權限密碼 **注意** 如果需要結束與解除鎖定密碼，而您未提供該密碼，Agent Mover 則會先提示您輸入密碼，然後才嘗試移動用戶端。
-dbg	啟動連線偵錯記錄

範例：

- 使用 HTTP 通訊的 Apex One 伺服器：

  ```
  ipXfer.exe -s Server01 -p 8080 -c 21112 -d Workgroup -
  pwd unlock
  ```

  ```
  ipXfer_x64.exe -s Server02 -p 8080 -c 21112 -d Workgroup
  \Group01 -pwd unlock
  ```

- 使用 HTTPS 通訊的 Apex One 伺服器：

  ```
  ipXfer.exe -s Server01 -sp 443 -p 8080 -c 21112 -d
  Workgroup -pwd unlock -dbg 1
  ```

5. 如果要確認 Security Agent 現在是否會向其他伺服器回報，請執行下列操作：

   a. 在 Security Agent 端點上，以滑鼠右鍵請點選系統匣中的 Security Agent 程式圖示。

   b. 選取「元件版本」。

   c. 在「伺服器名稱/通訊埠」欄位中，檢查 Security Agent 要向其回報的 Apex One 伺服器。

   注意

   如果 Security Agent 未出現在管理它的新 Apex One 伺服器的用戶端樹狀結構中，請重新啟動新伺服器的主服務 (`ofservice.exe`)。

離線 Security Agent

當您使用 Security Agent 解除安裝程式移除端點中的 Security Agent 時，程式會自動通知伺服器。當伺服器收到此通知時，便會移除用戶端樹狀結構中的 Security Agent 圖示，表示該用戶端已不存在。

不過，如果您使用其他方法移除 Security Agent（例如：重新格式化端點硬碟或手動刪除 Security Agent 檔案），Apex One 就無法得知 Security Agent 已被移除，而會將其顯示為離線。如果使用者長期結束或關閉 Security Agent，伺服器也會將該 Security Agent 顯示為離線。

如果要讓用戶端樹狀結構只顯示連線的用戶端，請設定讓 Apex One 自動從用戶端樹狀結構中移除離線用戶端。

自動移除離線用戶端

步驟

1. 移至管理 > 設定 > 離線用戶端。
2. 選取「啟動自動移除離線用戶端」。
3. 選取應在離線多少天後，Apex One 才認為 Security Agent 離線。
4. 請點選「儲存」。

用戶端和伺服器間的連線

Security Agent 必須持續維持與其上層伺服器之間的連線，才能及時更新元件、接收通知，以及套用組態設定變更。下列主題討論如何檢查 Security Agent 的連線狀態和解決連線問題：

- 用戶端 IP 位址 第 5-7 頁
- Security Agent 圖示 第 15-24 頁
- 用戶端和伺服器間的連線驗證 第 15-37 頁
- 連線驗證記錄檔 第 15-38 頁
- 無法連接的用戶端 第 15-38 頁

Security Agent 圖示

系統匣中的 Security Agent 圖示會提供視覺提示，指出 Security Agent 目前的狀態，並提示使用者執行某些動作。該圖示在任何給定的時間會顯示下列視覺提示的組合。

表 15-8. Security Agent 圖示中指出的 Security Agent 狀態

用戶端狀態	說明	視覺提示
用戶端與 Apex One 伺服器之間的連線	線上用戶端已連線到 Apex One 伺服器。伺服器可以開始工作並將設定部署到這些用戶端	圖示包含一個類似活動訊號的符號。  背景顏色是藍色或紅色的陰影，視即時掃瞄服務的狀態而定。
	離線用戶端已中斷與 Apex One 伺服器的連線。伺服器無法管理這些用戶端。	圖示包含一個類似中斷活動訊號的符號。  背景顏色是藍色或紅色的陰影，視即時掃瞄服務的狀態而定。 即使用戶端連線到網路，可能為離線狀態。如需此問題的詳細資訊，請參閱：Security Agent 圖示所指示問題的解決方案 第 15-34 頁。
	單機用戶端有的可以與 Apex One 伺服器通訊，有的則不行。	圖示包含桌面與訊號符號。  背景顏色是藍色或紅色的陰影，視即時掃瞄服務的狀態而定。 如需有關單機模式用戶端的詳細資訊，請參閱 Security Agent 單機模式權限 第 15-17 頁。

用戶端狀態	說明	視覺提示
主動雲端截毒伺服器來源的可用性	主動雲端截毒伺服器來源包括主動雲端截毒技術伺服器和趨勢科技主動雲端截毒技術。 標準掃瞄用戶端會連線到主動雲端截毒技術來源進行網頁信譽評等查詢。 雲端截毒掃瞄用戶端會連線到主動雲端截毒技術來源進行掃瞄與網頁信譽評等查詢。	如果主動雲端截毒伺服器來源可以使用，則圖示會包含一個核取記號 。 
		如果沒有可使用的主動雲端截毒技術來源，而用戶端嘗試與伺服器來源建立連線，則圖示會包含一個進度列。  如需此問題的詳細資訊，請參閱：Security Agent 圖示所指示問題的解決方案 第 15-34 頁。
		若為標準掃瞄用戶端，當關閉用戶端上的網頁信譽評等時，將不會顯示核取記號或進度列。

用戶端狀態	說明	視覺提示
即時掃瞄服務狀態	Apex One 不只會將「即時掃瞄服務」用於「即時掃瞄」，還會用於「手動掃瞄」和「預約掃瞄」。 服務必須正常運作，否則用戶端會變得容易遭受安全威脅的攻擊。	如果即時掃瞄服務在正常運作，整個圖示會有藍色陰影覆蓋。兩個藍色陰影用來表示用戶端。 • 若為標準掃瞄：  • 若為雲端截毒掃瞄： 
		如果即時掃瞄服務已關閉或未正常運作，整個圖示會有紅色陰影覆蓋。 兩個紅色陰影用來表示用戶端的掃瞄方法。 • 若為標準掃瞄：  • 若為雲端截毒掃瞄：  如需此問題的詳細資訊，請參閱：Security Agent 圖示所指示問題的解決方案 第 15-34 頁。
即時掃瞄狀態	即時掃瞄透過在建立、修改或擷取檔案時掃瞄看是否有安全威脅，以提供主動式安全防護。	如果啟動即時掃瞄，則不會有視覺提示。
		如果關閉即時掃瞄，整個圖示會圍繞著紅色圈圈並包含紅色的對角線。  如需此問題的詳細資訊，請參閱：Security Agent 圖示所指示問題的解決方案 第 15-34 頁。

用戶端狀態	說明	視覺提示
病毒碼更新狀態	用戶端必須定期更新病毒碼，以保護用戶端不受最新的安全威脅攻擊。	如果病毒碼是最新狀態或僅稍微過期，則不會有視覺提示。
		如果病毒碼嚴重過期，則圖示會包含一個驚嘆號 。這表示病毒碼已有一段時間未更新。  如需有關如何更新代理程式的詳細資訊，請參閱 Security Agent 更新 第 6-24 頁。
Apex One 伺服器試用版使用授權狀態	線上用戶端連線到使用過期試用版使用授權的 Apex One 伺服器。	此圖示表示 Apex One 伺服器上的試用版使用授權已過期。 

雲端截毒掃瞄圖示

當 Security Agent 使用雲端截毒掃瞄時，會顯示下列任一圖示。

表 15-9. 雲端截毒掃瞄圖示

圖示	和 Apex One 伺服器之間的連線	主動雲端截毒伺服器來源的可用性	即時掃瞄服務	即時掃瞄
	線上	可用	正常運作	已啟動
	線上	可用	正常運作	已關閉
	線上	可用	已關閉或未正常運作	已關閉或未正常運作
	線上	無法使用, 重新連線至來源	正常運作	已啟動

圖示	和 Apex One 伺服器之間的連線	主動雲端截毒伺服器來源的可用性	即時掃瞄服務	即時掃瞄
	線上	無法使用, 重新連線至來源	正常運作	已關閉
	線上	無法使用, 重新連線至來源	已關閉或未正常運作	已關閉或未正常運作
	離線	可用	正常運作	已啟動
	離線	可用	正常運作	已關閉
	離線	可用	已關閉或未正常運作	已關閉或未正常運作
	離線	無法使用, 重新連線至來源	正常運作	已啟動
	離線	無法使用, 重新連線至來源	正常運作	已關閉
	離線	無法使用, 重新連線至來源	已關閉或未正常運作	已關閉或未正常運作
	單機	可用	正常運作	已啟動
	單機	可用	正常運作	已關閉
	單機	可用	已關閉或未正常運作	已關閉或未正常運作
	單機	無法使用, 重新連線至來源	正常運作	已啟動
	單機	無法使用, 重新連線至來源	正常運作	已關閉
	單機	無法使用, 重新連線至來源	已關閉或未正常運作	已關閉或未正常運作

標準掃瞄圖示

當 Security Agent 使用標準掃瞄時，會顯示下列任一圖示。

表 15-10. 標準掃瞄圖示

圖示	和 Apex One 伺服器之間的連線	由主動雲端截毒伺服器來源所提供的網頁信譽評等服務	即時掃瞄服務	即時掃瞄	病毒碼
	線上	可用	正常運作	已啟動	最新狀態或稍微過期
	線上	無法使用，重新連線至來源	正常運作	已啟動	最新狀態或稍微過期
	線上	可用	正常運作	已啟動	嚴重過期
	線上	無法使用，重新連線至來源	正常運作	已啟動	嚴重過期
	線上	可用	正常運作	已關閉	最新狀態或稍微過期
	線上	無法使用，重新連線至來源	正常運作	已關閉	最新狀態或稍微過期
	線上	可用	正常運作	已關閉	嚴重過期
	線上	無法使用，重新連線至來源	正常運作	已關閉	嚴重過期
	線上	可用	已關閉或未正常運作	已關閉或未正常運作	最新狀態或稍微過期
	線上	無法使用，重新連線至來源	已關閉或未正常運作	已關閉或未正常運作	最新狀態或稍微過期
	線上	可用	已關閉或未正常運作	已關閉或未正常運作	嚴重過期

圖示	和 Apex One 伺服器之間的連線	由主動雲端截毒伺服器來源所提供的網頁信譽評等服務	即時掃瞄服務	即時掃瞄	病毒碼
	線上	無法使用，重新連線至來源	已關閉或未正常運作	已關閉或未正常運作	嚴重過期
	離線	可用	正常運作	已啟動	最新狀態或稍微過期
	離線	無法使用，重新連線至來源	正常運作	已啟動	最新狀態或稍微過期
	離線	可用	正常運作	已啟動	嚴重過期
	離線	無法使用，重新連線至來源	正常運作	已啟動	嚴重過期
	離線	可用	正常運作	已關閉	最新狀態或稍微過期
	離線	無法使用，重新連線至來源	正常運作	已關閉	最新狀態或稍微過期
	離線	可用	正常運作	已關閉	嚴重過期
	離線	無法使用，重新連線至來源	正常運作	已關閉	嚴重過期
	離線	可用	已關閉或未正常運作	已關閉或未正常運作	最新狀態或稍微過期
	離線	無法使用，重新連線至來源	已關閉或未正常運作	已關閉或未正常運作	最新狀態或稍微過期
	離線	可用	已關閉或未正常運作	已關閉或未正常運作	嚴重過期
	離線	無法使用，重新連線至來源	已關閉或未正常運作	已關閉或未正常運作	嚴重過期

圖示	和 Apex One 伺服器之間的連線	由主動雲端截毒伺服器來源所提供的網頁信譽評等服務	即時掃瞄服務	即時掃瞄	病毒碼
	單機	可用	正常運作	已啟動	最新狀態或稍微過期
	單機	無法使用，重新連線至來源	正常運作	已啟動	最新狀態或稍微過期
	單機	可用	正常運作	已啟動	嚴重過期
	單機	無法使用，重新連線至來源	正常運作	已啟動	嚴重過期
	單機	可用	正常運作	已關閉	最新狀態或稍微過期
	單機	無法使用，重新連線至來源	正常運作	已關閉	最新狀態或稍微過期
	單機	可用	正常運作	已關閉	嚴重過期
	單機	無法使用，重新連線至來源	正常運作	已關閉	嚴重過期
	單機	可用	已關閉或未正常運作	已關閉或未正常運作	最新狀態或稍微過期
	單機	無法使用，重新連線至來源	已關閉或未正常運作	已關閉或未正常運作	最新狀態或稍微過期
	單機	可用	已關閉或未正常運作	已關閉或未正常運作	嚴重過期
	單機	無法使用，重新連線至來源	已關閉或未正常運作	已關閉或未正常運作	嚴重過期
	線上	無（已關閉用戶端上的網頁信譽評等功能）	正常運作	已啟動	最新狀態或稍微過期

圖示	和 Apex One 伺服器之間的連線	由主動雲端截毒伺服器來源所提供的網頁信譽評等服務	即時掃瞄服務	即時掃瞄	病毒碼
	線上	無（已關閉用戶端上的網頁信譽評等功能）	正常運作	已啟動	嚴重過期
	線上	無（已關閉用戶端上的網頁信譽評等功能）	正常運作	已關閉	最新狀態或稍微過期
	線上	無（已關閉用戶端上的網頁信譽評等功能）	正常運作	已關閉	嚴重過期
	線上	無（已關閉用戶端上的網頁信譽評等功能）	已關閉或未正常運作	已關閉或未正常運作	最新狀態或稍微過期
	線上	無（已關閉用戶端上的網頁信譽評等功能）	已關閉或未正常運作	已關閉或未正常運作	嚴重過期
	離線	無（已關閉用戶端上的網頁信譽評等功能）	正常運作	已啟動	最新狀態或稍微過期
	離線	無（已關閉用戶端上的網頁信譽評等功能）	正常運作	已啟動	嚴重過期
	離線	無（已關閉用戶端上的網頁信譽評等功能）	正常運作	已關閉	最新狀態或稍微過期
	離線	無（已關閉用戶端上的網頁信譽評等功能）	正常運作	已關閉	嚴重過期
	離線	無（已關閉用戶端上的網頁信譽評等功能）	已關閉或未正常運作	已關閉或未正常運作	最新狀態或稍微過期

圖示	和 Apex One 伺服器之間的連線	由主動雲端截毒伺服器來源所提供的網頁信譽評等服務	即時掃瞄服務	即時掃瞄	病毒碼
	離線	無（已關閉用戶端上的網頁信譽評等功能）	已關閉或未正常運作	已關閉或未正常運作	嚴重過期
	單機	無（已關閉用戶端上的網頁信譽評等功能）	正常運作	已啟動	最新狀態或稍微過期
	單機	無（已關閉用戶端上的網頁信譽評等功能）	正常運作	已啟動	嚴重過期
	單機	無（已關閉用戶端上的網頁信譽評等功能）	正常運作	已關閉	最新狀態或稍微過期
	單機	無（已關閉用戶端上的網頁信譽評等功能）	正常運作	已關閉	嚴重過期
	單機	無（已關閉用戶端上的網頁信譽評等功能）	已關閉或未正常運作	已關閉或未正常運作	最新狀態或稍微過期
	單機	無（已關閉用戶端上的網頁信譽評等功能）	已關閉或未正常運作	已關閉或未正常運作	嚴重過期

Security Agent 圖示所指示問題的解決方案

如果 Security Agent 圖示指示存在下列任何一種狀況，請執行必要的處理行動：

狀況	說明
病毒碼檔案已有一段時間未更新	Security Agent 使用者需要更新元件。從 Web 主控台的「更新 > 用戶端 > 自動更新」中進行元件更新設定，或授與使用者在「用戶端

狀況	說明
	> 用戶端管理 > 設定 > 權限和其他設定 > 權限（標籤） > 元件更新」中進行更新的權限。
即時掃瞄服務已關閉或未正常運作	如果「即時掃瞄服務」(Apex One NT RealTime Scan) 已關閉或未正常運作，使用者必須從 Microsoft 管理主控台手動啟動該服務。
「即時掃瞄」已關閉	從 Web 主控台啟動「即時掃瞄」（用戶端 > 用戶端管理> 設定 > 掃瞄設定 > 即時掃瞄設定）。
「即時掃瞄」已關閉，且 Security Agent 正以單機模式執行	使用者必須先關閉單機模式。關閉單機模式之後，從 Web 主控台啟動「即時掃瞄」。
Security Agent 已連線到網路但顯示為離線	從 Web 主控台驗證連線（「用戶端 > 連線驗證」），然後檢查連線驗證記錄檔（「記錄檔 > 用戶端 > 連線驗證記錄檔」）。 如果驗證之後 Security Agent 仍為離線狀態： 1. 如果伺服器和 Security Agent 上的連線狀態都是離線，請檢查網路連線。 2. 如果 Security Agent 上的連線狀態為離線，但在伺服器上顯示為線上，表示伺服器的網域名稱可能已變更，而 Security Agent 仍使用原網域名稱連線到伺服器（如果您在伺服器安裝期間選取了網域名稱）。請向 DNS 或 WINS 伺服器註冊 Apex One 伺服器的網域名稱，或是將網域名稱和 IP 資訊新增至用戶端端點上位於下列資料夾的「hosts」檔案。<Windows 資料夾>\system32\drivers\etc 3. 如果 Security Agent 上的連線狀態為線上，但在伺服器上顯示為離線，請檢查 Apex One 防火牆設定。防火牆可能會封鎖伺服器到用戶端的通訊，但是允許用戶端到伺服器的通訊。 4. 如果 Security Agent 上的連線狀態為線上，但在伺服器上顯示為離線，表示 Security Agent 的 IP 位址可能已變更，但其狀態並未反映在伺服器上（例如：重新載入用戶端時）。請嘗試重新部署 Security Agent。
主動式雲端截毒伺服器來源無法使用	如果用戶端和主動雲端截毒技術來源間的連線中斷，請執行這些工作： 1. 在 Web 主控台上，移至「端點位置」畫面（「用戶端 > 端點位置」），然後檢查下列 端點 位置設定是否已正確設定： • 參考伺服器和通訊埠號碼

狀況	說明
	• 閘道 IP 位址 2. 在 Web 主控台上，移至「主動雲端截毒技術來源」畫面（「管理 > 主動式雲端截毒技術 > 主動式雲端截毒技術來源」），然後執行下列工作： a. 檢查標準或自訂來源清單上的「主動雲端截毒技術伺服器」設定是否正確。 b. 測試是否可以和伺服器建立連線。 c. 設定來源清單之後，請點選「通知所有用戶端」。 3. 檢查主動雲端截毒技術伺服器和 Security Agent 上的下列組態設定檔案是否同步： • `sscfg.ini` • `ssnotify.ini` 4. 開啟「登錄編輯程式」，然後檢查用戶端是否已連線到企業網路。 機碼： `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\iCRC Scan\Scan Server` • 如果 `LocationProfile=1`，表示 Security Agent 已連線到網路，因此應該可以連線到主動雲端截毒技術伺服器。 • 如果 `LocationProfile=2`，表示 Security Agent 未連線到網路，而且應該連線到主動雲端截毒技術。從 Internet Explorer 檢查 Security Agent 端點是否可以瀏覽 Internet 網頁。 5. 檢查用以連線到主動雲端截毒技術和主動雲端截毒技術伺服器的內部和外部 Proxy 設定。 如需詳細資訊，請參閱設定內部用戶端 Proxy 設定 第 15-44 頁和設定外部用戶端 Proxy 設定 第 15-45 頁。 6. 針對執行 Windows 7、Server 2012 及更新版本的標準掃瞄用戶端，請確認 tmusa 驅動程式正在執行中。如果此驅動程式已停止，用戶端將無法連線到主動雲端截毒技術來源來取得網頁信譽評等。

用戶端和伺服器間的連線驗證

Security Agent 與 Apex One 伺服器間的連線狀態會顯示在 Apex One 用戶端樹狀結構中。

圖 15-2. 顯示 Security Agent 與 Apex One 伺服器間連線狀態的用戶端樹狀結構

某些情況可能使用戶端樹狀結構無法顯示正確的 Security Agent 連線狀態。例如，如果您不小心拔除 Security Agent 端點的網路纜線，Security Agent 將無法通知伺服器其現為離線狀態。這個 Security Agent 仍會在用戶端樹狀結構中顯示為線上。

手動驗證 Security Agent 與伺服器間的連線，或讓 Apex One 執行預約驗證。您無法選取特定網域或 Security Agent，然後驗證其連線狀態。Apex One 會驗證其所有已註冊 Security Agent 的連線狀態。

驗證用戶端與伺服器間的連線

步驟

1. 移至「用戶端 > 連線驗證」。
2. 如果要手動驗證用戶端與伺服器間的連線，請移至「手動驗證」標籤，然後請點選「立即驗證」。
3. 如果要自動驗證用戶端與伺服器間的連線，請移至「預約驗證」標籤。

a. 選取「啟動預約驗證」。

b. 選取驗證頻率和開始時間。

c. 請點選「儲存」以儲存驗證預約時程。

4. 檢查用戶端樹狀結構，以驗證狀態或檢視連線驗證記錄檔。

連線驗證記錄檔

Apex One 會保留連線驗證記錄檔，讓您能夠判定 Apex One 伺服器是否可與所有其註冊用戶端通訊。每當您從 Web 主控台驗證用戶端與伺服器間的連線時，Apex One 都會建立一個記錄項目。

如果要避免記錄檔佔去過多硬碟空間，請手動刪除記錄檔或設定記錄檔刪除預約時程。如需有關管理記錄檔的詳細資訊，請參閱記錄檔管理 第 14-39 頁。

檢視連線驗證記錄檔

步驟

1. 移至「記錄檔 > 用戶端 > 連線驗證記錄檔」。
2. 檢查「狀態」欄位以檢視連線驗證結果。
3. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請點選「匯出到 CSV」。開啟檔案或將其儲存至特定位置。

無法連接的用戶端

位於無法連接的網路（例如：NAT 閘道後方的網路區段）上的 Security Agent 通常始終處於離線狀態，因為伺服器無法與這些用戶端建立直接連線。因此，伺服器無法通知這些用戶端執行下列動作：

- 下載最新的元件。
- 套用從 Web 主控台設定的用戶端設定。例如：當您從 Web 主控台變更「預約掃瞄」頻率時，伺服器將立即通知用戶端套用新設定。

因此，無法連接的用戶端無法及時執行這些工作。它們只能在起始與伺服器的連線時才能執行工作，例如下列情況：

- 用戶端在安裝後向伺服器註冊。
- 用戶端重新啟動或重新載入。此事件不會經常發生，而且通常需要使用者介入。
- 手動或預約更新是在用戶端上觸發。此事件也不會經常發生。

只有在用戶端註冊、重新啟動或重新載入時，伺服器才會「得知」用戶端連線並將其視為線上狀態。不過，因為伺服器仍無法建立與用戶端的連線，因此伺服器會立即將狀態變更為離線。

Apex One 提供「活動訊號」和伺服器輪詢功能，以解決無法連接的用戶端的問題。使用這些功能時，伺服器會停止通知用戶端有關元件更新和設定變更的資訊。伺服器反而會變成被動角色，隨時等候用戶端傳送活動訊號或起始輪詢。當伺服器偵測到其中任何一種事件時，便會將用戶端視為線上狀態。

注意

與活動訊號和伺服器輪詢無關的事件（例如：用戶端開始的手動用戶端更新和記錄檔傳送）不會觸發伺服器更新無法連接的用戶端的狀態。

活動訊號

Security Agent 會傳送活動訊號訊息，以通知伺服器用戶端的連線仍正常運作。當伺服器收到活動訊號訊息時，便會將該用戶端視為處於線上狀態。在用戶端樹狀結構中，用戶端的狀態可以是下列其中一個值：

- 線上：表示一般線上用戶端
- 無法連接/線上：表示位在無法連接的網路中的線上用戶端

注意

當 Security Agent 在傳送活動訊號訊息時，它不會更新元件或套用新設定。標準用戶端會在定期更新期間執行這些工作（請參閱 Security Agent 更新 第 6-24 頁）。位在無法連接的網路中的用戶端會在伺服器輪詢期間執行這些工作。

活動訊號功能可解決位在無法連接的網路中的 Security Agent 總是看起來像是離線的問題（即使用戶端可連線到伺服器）。

Web 主控台中有一個設定，可控制用戶端傳送活動訊號訊息的頻率。如果伺服器未收到活動訊號，它不會立即將用戶端視為處於離線狀態。另一個設定可控制沒有活動訊號多長時間之後，再將用戶端的狀態變更為：

- 離線：表示一般離線 Security Agent
- 無法連接/離線：表示位在無法連接的網路中的離線 Security Agent

選擇活動訊號設定時，務必在顯示最新用戶端狀態資訊的需求和管理系統資源的需求之間取得平衡。預設設定能夠滿足大部分情況的需求。不過，當您自訂活動訊號設定時，請務必考慮下列幾點：

表 15-11. 活動訊號建議

活動訊號頻率	建議
長時間間隔活動訊號（60 分鐘以上）	活動訊號之間的時間間隔越長，伺服器在 Web 主控台上反映用戶端狀態之前可能發生的事件數目就越多。
短時間間隔活動訊號（60 分鐘以下）	短時間間隔可讓伺服器提供更即時的用戶端狀態，但會耗用較多頻寬。

伺服器輪詢

伺服器輪詢功能可解決無法連線的 Security Agent 未及時接收元件更新和 用戶端設定變更的通知的問題。此功能獨立於活動訊號功能。

使用伺服器輪詢功能時：

- Security Agent 會定期自動開始與 Apex One 伺服器的連線。當伺服器偵測到發生輪詢時，會將用戶端視為「無法連接/線上」。

- Security Agent 會連線到一或多個更新來源，以下載任何更新的元件並套用新的用戶端設定。如果 Apex One 伺服器或更新代理程式是主要更新來源，用戶端會同時取得元件和新設定。如果來源不是 Apex One 伺服器或更新代理程式，用戶端只會取得更新的元件，然後連線到 Apex One 伺服器或更新代理程式以取得新設定。

設定活動訊號和伺服器輪詢功能

步驟

1. 移至「用戶端 > 全域用戶端設定」。
2. 請點選「網路」標籤。
3. 移至「無法連線的網路」區段。
4. 設定伺服器輪詢設定。

   如需有關伺服器輪詢的詳細資訊，請參閱伺服器輪詢 第 15-40 頁。

   a. 如果 Apex One 伺服器同時具有 IPv4 和 IPv6 位址，您可以輸入 IPv4 位址範圍和 IPv6 字首和長度。

      如果伺服器是純 IPv4，請輸入 IPv4 位址；如果伺服器是純 IPv6，請輸入 IPv6 字首和長度。

      當任何用戶端的 IP 位址符合範圍中的某個 IP 位址時，用戶端會套用活動訊號和伺服器輪詢設定，而伺服器會將用戶端視為屬於無法連接的網路。

      注意

      具有 IPv4 位址的用戶端可連線到純 IPv4 或雙堆疊 Apex One 伺服器。

      具有 IPv6 位址的用戶端可連線到純 IPv6 或雙堆疊 Apex One 伺服器。

      雙堆疊用戶端可連線到雙堆疊、純 IPv4 或純 IPv6 Apex One 伺服器。

   b. 在「用戶端每隔 __ 分鐘輪詢伺服器中是否有更新的元件與設定」中，指定伺服器輪詢頻率。請輸入介於 1 到 129600 分鐘之間的值。

秘訣

趨勢科技建議至少將伺服器輪詢頻率設定為活動訊號傳送頻率的三倍。

5. 設定活動訊號設定。

   如需有關活動訊號功能的詳細資訊，請參閱活動訊號 第 15-39 頁。

   a. 選取「允許用戶端將活動訊號傳送到伺服器」。

   b. 選取「所有用戶端」或「僅限無法連接的網路中的用戶端」。

   c. 在「用戶端傳送活動訊號的間隔：__ 分鐘」中，指定用戶端傳送活動訊號的頻率。請輸入介於 1 到 129600 分鐘之間的值。

   d. 在「如果超過以下時間未收到用戶端傳送的活動訊號，則將它視為離線：__ 分鐘」中，指定 Apex One 伺服器在多久時間內未收到活動訊號會將用戶端視為離線。請輸入介於 1 到 129600 分鐘之間的值。

6. 請點選「儲存」。

Security Agent Proxy 設定

下表列出可用於連線到內部和外部伺服器的 Security Agent Proxy 設定。

Proxy 組態設定	說明
內部用戶端	設定用於連線到下列伺服器的內部用戶端 Proxy 設定。 • Apex One 伺服器：裝載了 Apex One 伺服器和整合式主動雲端截毒技術伺服器的伺服器電腦。Security Agent 會連線到 Apex One 伺服器來更新元件、取得組態設定，以及傳送記錄檔。Security Agent 會連線到整合式主動雲端截毒技術伺服器以傳送掃瞄查詢。 • 主動雲端截毒技術伺服器：主動雲端截毒技術伺服器包括所有獨立式主動雲端截毒技術伺服器和整合式主動雲端截毒技術伺服器，以及其他 Apex One 伺服器。Security Agent 會連線到這些伺服器以傳送掃瞄與網頁信譽評等查詢。 如需詳細資訊，請參閱設定內部用戶端 Proxy 設定 第 15-44 頁。
外部用戶端	外部 Security Agent 可以使用在 Internet Explorer 中設定的 Proxy 設定，連線到趨勢科技主動雲端截毒技術。 如需詳細資訊，請參閱設定外部用戶端 Proxy 設定 第 15-45 頁。
全球主動雲端截毒技術服務	Security Agent 針對下列功能向主動雲端截毒技術來源進行查詢時，會使用所設定的主動雲端截毒技術服務 Proxy 設定： • Machine Learning • 行為監控 **注意** 如果執行查詢時，整合式主動雲端截毒技術伺服器無法使用，則 Security Agent 會連線到趨勢科技主動雲端截毒技術。 如需詳細資訊，請參閱設定全球主動雲端截毒技術服務 Proxy 設定 第 15-46 頁。

Proxy 組態設定	說明
用戶端使用者 Proxy 權限	您可以授與用戶端使用者設定 Proxy 設定的權限。Security Agent 僅會在下列情況中使用使用者設定的 Proxy 設定： • 當 Security Agent 執行「立即更新」時。 • 當使用者關閉（或 Security Agent 無法偵測）自動 Proxy 設定時。 警告! 如果使用者設定的 Proxy 設定不正確，會導致發生更新問題。允許使用者設定自己的 Proxy 設定時請特別小心。 如需詳細資訊，請參閱授與 Proxy 設定權限 第 15-47 頁。

設定內部用戶端 Proxy 設定

步驟

1. 移至「管理 > 設定 > Proxy 伺服器」。
2. 請點選「用戶端」標籤。
3. 移至「內部 Proxy」區段。
4. 選取內部 Security Agent 在連線到 Apex One 伺服器或主動雲端截毒技術伺服器時使用的 Proxy 伺服器類型設定。
   - 無 Proxy：內部 Security Agent 不需要使用 Proxy 伺服器來連線到 Apex One 伺服器或主動雲端截毒技術伺服器
   - 使用 Windows Proxy 設定：內部用戶端將使用在 Windows「網際網路選項」中設定的 Proxy 伺服器設定，來連線到 Apex One 伺服器或主動雲端截毒技術伺服器

     注意
     請視需要指定 Proxy 驗證認證。

- 使用多個 Proxy 伺服器：內部用戶端將使用不同的 Proxy 伺服器來連線到 Apex One 伺服器或主動雲端截毒技術伺服器

  對於 Apex One 伺服器連線：

  a. 選取「連線到內部 Apex One 伺服器時使用的 Security Agent Proxy」。

  b. 指定 Proxy 伺服器名稱或 IPv4/IPv6 位址，以及通訊埠號碼。

  c. 請視需要指定 Proxy 驗證認證。

  對於獨立式主動雲端截毒技術伺服器連線：

  a. 選取「連線到獨立式主動雲端截毒技術伺服器時使用的 Security Agent Proxy」。

  b. 指定 Proxy 伺服器名稱或 IPv4/IPv6 位址，以及通訊埠號碼。

  c. 請視需要指定 Proxy 驗證認證。

- 使用自動 Proxy 組態設定（包括 PAC）：選取此選項以使用管理員設定的 Proxy 設定（使用 DHCP、DNS 或自動組態設定程式檔）
  - 自動偵測網路 Proxy 設定：內部用戶端將依照 DHCP 或 DNS 偵測管理員設定的 Proxy 設定
  - 使用指定的 Proxy 自動組態設定 (PAC) 程式檔：內部用戶端將使用網路管理員設定的 Proxy 自動組態設定 (PAC) 程式檔來偵測適當的 Proxy 伺服器

    注意

    輸入 PAC 程式檔的 URL 位址。

5. 請點選「儲存」。

設定外部用戶端 Proxy 設定

外部用戶端只能使用在 Windows「網際網路選項」中設定的 Proxy 伺服器設定來連線到 Apex One 伺服器或主動雲端截毒技術伺服器。

步驟

1. 移至「管理 > 設定 > Proxy 伺服器」。
2. 請點選「用戶端」標籤。
3. 移至「外部 Proxy」區段。
4. 請視需要指定 Proxy 驗證認證。
5. 請點選「儲存」。

設定全球主動雲端截毒技術服務 Proxy 設定

Security Agent 針對下列功能向主動雲端截毒技術來源進行查詢時，會使用所設定的主動雲端截毒技術服務 Proxy 設定：

- Machine Learning
- 行為監控

注意

如果執行查詢時，整合式主動雲端截毒技術伺服器無法使用，則 Security Agent 會連線到趨勢科技主動雲端截毒技術。

步驟

1. 移至「用戶端 > 全域用戶端設定」。
2. 請點選「系統」標籤。
3. 移至「主動雲端截毒技術服務 Proxy 」區段。
4. 啟動「使用所設定的主動雲端截毒伺服器來源來處理服務查詢」。

重要

主動雲端截毒技術服務 Proxy 僅支援使用 HTTPS 通訊協定進行檔案信譽評等查詢。您必須確保所有已設定會提供檔案信譽評等服務的主動雲端截毒技術伺服器，均會使用 HTTPS 通訊協定。

依預設，整合式主動雲端截毒技術伺服器並不會使用 HTTPS 通訊。若要變更通訊方法，請參閱設定整合式主動雲端截毒技術伺服器設定 第 4-19 頁.

若要確認獨立式主動雲端截毒技術伺服器所使用的通訊方法，請參閱設定主動雲端截毒伺服器來源自訂清單 第 4-24 頁。

5. 請點選「儲存」。

授與 Proxy 設定權限

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 權限和其他設定」。
4. 在「權限」標籤上，移至「Proxy 設定」區段。
5. 選取「允許使用者設定 Proxy 設定」。
6. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

檢視 Security Agent 資訊

「檢視狀態」畫面顯示有關 Security Agent 的重要資訊，包括權限、端點軟體詳細資料及系統事件。

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「狀態」。
4. 展開用戶端端點名稱以檢視狀態資訊。如果您選取了多個用戶端，請點選「全部展開」以檢視所有選定用戶端的狀態資訊。
5. （選用）使用「重設」按鈕將安全威脅數量重設為零。

匯入和匯出用戶端設定

Apex One 可讓您將用戶端樹狀結構設定（由特定 Security Agent 或網域所套用）匯出到檔案。接著，您可以匯入該檔案以將設定套用到其他用戶端和網域，或套用到具有相同版本的其他 Apex One 伺服器。

系統將匯出所有用戶端樹狀結構設定，「更新代理程式」設定除外。

匯出用戶端設定

步驟

1. 移至「用戶端 > 用戶端管理」。

2. 在用戶端樹狀結構中，請點選根網域圖示 ( ) 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 匯出設定」。
4. 請點選任何連結，以檢視您所選取 Security Agent 或網域的設定。
5. 請點選「匯出」以儲存設定。

   設定會存到 .dat 檔案中。
6. 請點選「儲存」，然後指定要儲存 .dat 檔案的位置。
7. 請點選「儲存」。

匯入用戶端設定

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 ( ) 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定｜匯入設定」。
4. 請點選「瀏覽」，在端點上尋找 .dat 檔案，然後請點選「匯入」。

   「匯入設定」畫面就會出現，並顯示設定的摘要。
5. 請點選任何連結，以檢視要匯入的掃瞄設定或權限的詳細資訊。
6. 匯入設定。
   - 如果您是請點選根網域圖示，請選取「套用至所有網域」，然後請點選「套用到目標」。
   - 如果您是選取網域，請選取「套用至屬於選取之網域的所有電腦」，然後請點選「套用到目標」。

- 如果您是選取多個用戶端，請點選「套用到目標」。

安全性符合

使用「安全性符合」來判斷缺點、部署解決方案及維護安全基礎架構。這項功能有助於減少保護網路環境安全所需的時間，並讓組織在安全性和功能的需求之間取得平衡點。

實施適用於兩種端點類型的安全性符合：

- 受管理：Security Agent 受 Apex One 伺服器所管理的端點。如需詳細資訊，請參閱適用於受管用戶端的安全性符合 第 15-50 頁。
- 未受管理：包括下列各項：
  - Security Agent 不受 Apex One 伺服器所管理
  - 未安裝 Security Agent 的端點
  - Apex One 伺服器無法與其連線的端點
  - 無法驗證其安全狀態的端點

    如需詳細資訊，請參閱適用於未受管端點的安全性符合 第 15-62 頁。

適用於受管用戶端的安全性符合

「安全性符合」可產生「符合性報告」，以協助您評估 Apex One 伺服器所管理的 Security Agent 的安全狀態。「安全性符合」可視需要或根據預約產生報告。

注意

Apex One 只會顯示以完整功能集運作之 Security Agent 的符合性報告。報告中不會顯示共存用戶端。

「手動評估」畫面會顯示下列標籤：

- 服務：使用此標籤來檢查用戶端服務是否正常運作。

  如需詳細資訊，請參閱服務 第 15-52 頁。

- 元件：使用此標籤來檢查 Security Agent 是否有最新元件。

  如需詳細資訊，請參閱元件 第 15-53 頁。

- 掃瞄符合性：使用此標籤來檢查 Security Agent 是否定期執行掃瞄。

  如需詳細資訊，請參閱掃瞄符合性 第 15-55 頁。

- 設定：使用此標籤來檢查用戶端設定是否與伺服器設定一致。

  如需詳細資訊，請參閱設定 第 15-57 頁。

注意

「元件」標籤可顯示執行最新和舊版產品的 Security Agent。其他標籤只會顯示執行最新版本之 Security Agent 的資料。

重要

- 「安全性符合」會在產生「符合性報告」之前先查詢 Security Agent 的連線狀態。它會在報告中包含線上和離線用戶端，但不會包含單機模式的用戶端。
- 對於以角色為基礎的使用者帳號：
  - 每個 Web 主控台使用者帳號都有一組完全獨立的「符合性報告」設定。變更使用者帳號的「符合性報告」設定不會影響其他使用者帳號的設定。
  - 報告的範圍取決於使用者帳號的用戶端網域權限。例如，如果您將管理網域 A 和 B 的權限授與某個使用者帳號，該使用者帳號的報告只會顯示來自屬於網域 A 和 B 的用戶端的資料。

    如需有關使用者帳號的詳細資訊，請參閱以角色為基礎的管理 第 14-3 頁。

服務

「安全性符合」會檢查下列 Security Agent 服務是否正常運作：

- 防毒
- 間諜程式防護
- 防火牆
- 網頁信譽評等
- 行為監控/周邊設備存取控管（亦稱為「趨勢科技未經授權的變更阻止服務」）
- 資料安全防護
- 可疑連線

不相容的用戶端在「符合性報告」中至少會計算兩次。

圖 15-3. 符合報告的「服務」標籤

- 在「具有非相容服務的端點」類別中
- 在 Security Agent 不相容的類別中。例如，如果 Security Agent 的防毒服務未正常運作，用戶端會在「防毒」類別中計算一次。如果多個服務未正常運作，用戶端會在每個不符合的類別中都計算一次。

請從 Web 主控台或 Security Agent 重新啟動未運作的服務。如果重新啟動服務之後服務可以正常運作，下次評估時用戶端就不會再顯示為不符合。

元件

「安全性符合」會判斷 Apex One 伺服器與 Security Agent 之間的元件版本是否一致。不一致的情況通常發生在用戶端無法連線到伺服器以更新元件時。如果用戶端是從其他來源（例如：趨勢科技主動式更新伺服器）取得更新，該用戶端的元件版本就可能比伺服器上的元件版本還要新。

「安全性符合」會檢查下列元件：

- 本機雲端病毒碼
- 病毒碼
- IntelliTrap 病毒碼
- IntelliTrap 例外病毒碼
- 病毒掃瞄引擎（32/64 位元）
- 間諜程式/可能的資安威脅程式病毒碼
- 間諜程式主動式監控病毒碼
- 間諜程式/可能的資安威脅程式掃瞄引擎（32/64 位元）
- 損害清除及復原範本
- 損害清除及復原引擎（32/64 位元）
- 一般防火牆病毒碼
- 一般防火牆驅動程式（32/64 位元）
- 行為監控核心驅動程式（32/64 位元）
- 行為監控核心服務（32/64 位元）
- 行為監控配置特徵碼
- 數位簽章特徵碼
- 策略實施特徵碼
- 行為監控偵測病毒碼（32/64 位元）
- 全域 C&C IP 清單
- 相關性規則病毒碼
- Early Boot Cleanup 驅動程式（32/64 位元）
- 記憶體掃瞄觸發病毒碼（32/64 位元）
- 記憶體檢測病毒碼
- 瀏覽器弱點攻擊防護特徵碼
- 程式檔分析器統一病毒碼
- 程式檢測監控病毒碼
- 損害還原病毒碼
- 開機初期啟動的惡意程式防護特徵碼（32/64 位元）
- 關聯式智慧引擎（32/64 位元）
- 關聯式智慧型病毒碼
- 關聯式智慧查詢處理程式（32/64 位元）
- 進階威脅掃描引擎（32/64 位元）
- 進階安全威脅關聯病毒碼
- 程式版本

不相容的用戶端在「符合性報告」中至少會計算兩次。

圖 15-4. 符合報告的「元件」標籤

- 在「具有不一致元件版本的端點」類別中
- 在用戶端不相容的類別中。例如，如果用戶端的「本機雲端病毒碼」版本與伺服器上的版本不一致，該用戶端會在「本機雲端病毒碼」類別中計算一次。如果多個元件版本不一致，該用戶端會在每個不相容的類別中都計算一次。

如果要解決元件版本不一致的問題，請更新代理程式或伺服器上的已過期元件。

掃瞄符合性

「安全性符合」會檢查「立即掃瞄」或「預約掃瞄」是否定期執行，以及這些掃瞄是否在合理的時間內完成。

注意

只有已在用戶端上啟動「預約掃瞄」時，「安全性符合」才會回報「預約掃瞄」狀態。

「安全性符合」會使用下列掃瞄符合性條件：

- 未執行「立即掃瞄」或「預約掃瞄」(x) 天：如果 Security Agent 在指定天數內未執行過「立即掃瞄」或「預約掃瞄」，則會被判定為不符合。
- 「立即掃瞄」或「預約掃瞄」已超過 (x) 小時：如果 Security Agent 上次執行「立即掃瞄」或「預約掃瞄」的持續時間已超過指定的小時數，則會被判定為不符合。

不相容的用戶端在「符合性報告」中至少會計算兩次。

圖 15-5. 符合報告的「掃瞄符合性」標籤

- 在「具有過期掃瞄的端點」類別中
- 在用戶端不相容的類別中。例如，如果上次執行「預約掃瞄」的時間超過指定的小時數，用戶端會在「「立即掃瞄」或「預約掃瞄」已超過 <x> 小

時」類別中計算一次。如果用戶端符合多個掃瞄符合性條件，它會在每個不符合的類別中都計算一次。

在尚未執行掃瞄工作或無法完成掃瞄的用戶端上，執行「立即掃瞄」或「預約掃瞄」。

設定

「安全性符合」會判斷用戶端是否與用戶端樹狀結構中的上層網域具有相同的設定。如果您將任何用戶端移到另一個套用不同組設定的網域中，或如果任何具有特定權限的用戶端使用者在 Security Agent 主控台上手動進行設定，則設定可能會不一致。

Apex One 會驗證下列設定：

- 掃瞄方法
- 手動掃瞄設定
- 即時掃瞄設定
- 預約掃瞄設定
- 立即掃瞄設定
- 權限和其他設定
- 其他服務設定
- 網頁信譽評等
- 行為監控
- 周邊設備存取控管
- 間諜程式/可能的資安威脅程式核可清單
- 資料外洩防護設定
- 可疑連線
- 信任的程式清單
- 樣本提交
- Machine Learning

不相容的用戶端在「符合性報告」中至少會計算兩次。

圖 15-6. 符合報告的「設定」標籤

- 在「具有不一致組態設定的端點」類別中
- 在用戶端不相容的類別中。例如，如果用戶端中的掃瞄方法設定與其上層網域不一致，該用戶端會在「掃瞄方法」類別中計算一次。如果多個設定不一致，該用戶端會在每個不相容的類別中都計算一次。

如果要解決設定不一致的問題，請將網域設定套用到用戶端。

依要求執行的符合性報告

您可以視需要使用「安全性符合」來產生「符合報告」。報告可協助您評估 Apex One 伺服器所管理的 Security Agent 的安全狀態。

如需有關符合性報告的詳細資訊，請參閱適用於受管用戶端的安全性符合 第 15-50 頁。

產生視需要「符合性報告」

步驟

1. 移至「評估 > 安全性符合 > 手動報告」。
2. 移至「用戶端樹狀結構範圍」區段。
3. 選取根網域或網域，然後請點選「評估」。
4. 檢視用戶端服務的「符合性報告」。

   如需有關用戶端服務的詳細資訊，請參閱服務 第 15-52 頁。

   a. 請點選「服務」標籤。

   b. 在「具有非相容服務的端點」下，檢查具有非相容服務的用戶端數量。

   c. 請點選數字連結，以顯示用戶端樹狀結構中所有受影響的用戶端。

   d. 從查詢結果中選取用戶端。

   e. 按一下「重新啟動 Security Agent」以重新啟動服務。

   > **注意**
   >
   > 若重新執行評估後，用戶端仍顯示為不相容，請手動重新啟動用戶端端點上的服務。

   f. 如果要將用戶端清單儲存到檔案，請點選「匯出」。

5. 檢視用戶端元件的「符合性報告」。

   如需有關用戶端元件的詳細資訊，請參閱元件 第 15-53 頁。

   a. 請點選「元件」標籤。

   b. 在「具有不一致元件版本的端點」下，檢查元件版本與伺服器上的版本不一致的用戶端數量。

   c. 請點選數字連結，以顯示用戶端樹狀結構中所有受影響的用戶端。

注意

如果至少有一個用戶端擁有比 Apex One 伺服器新的元件，請手動更新 Apex One 伺服器。

d. 從查詢結果中選取用戶端。

e. 請點選「立即更新」以強制用戶端下載元件。

注意

- 若要確保用戶端可以升級用戶端程式，請執行下列步驟：
  i. 移至「用戶端 > 用戶端管理」。
  ii. 按一下「設定 > 權限和其他設定 > 其他設定」標籤。
  iii. 移至「更新設定」區段。
  iv. 在「Security Agent 僅會更新下列元件」下拉式清單中，選取「所有元件（包括 Hotfix 和用戶端程式）」。
  v. 請點選「套用至所有用戶端」。
- 重新啟動端點（而不是點選「立即更新」），可更新一般防火牆驅動程式。

f. 如果要將用戶端清單儲存到檔案，請點選「匯出」。

6. 檢視掃瞄的「符合報告」。

如需有關掃瞄的詳細資訊，請參閱掃瞄符合性 第 15-55 頁。

a. 請點選「掃瞄符合性」標籤。

b. 在「具有過期掃瞄的端點」下，設定下列選項：

- 用戶端未執行「立即掃瞄」或「預約掃瞄」的天數
- 「立即掃瞄」或「預約掃瞄」的執行時數

注意

如果超過該天數或時數，則將用戶端視為不符合。

c. 請點選「用戶端樹狀結構範圍」旁的「評估」。

d. 在「具有過期掃瞄的端點」下，檢查符合掃瞄條件的用戶端數量。

e. 請點選數字連結，以顯示用戶端樹狀結構中所有受影響的用戶端。

f. 從查詢結果中選取用戶端。

g. 請點選「立即掃瞄」以在用戶端上起始「立即掃瞄」。

> **注意**
>
> 為避免重複掃瞄，如果「立即掃瞄」的執行時間超過指定時數，將關閉「立即掃瞄」選項。

h. 如果要將用戶端清單儲存到檔案，請點選「匯出」。

7. 檢視設定的「符合報告」。

   如需有關設定的詳細資訊，請參閱設定 第 15-57 頁。

   a. 請點選設定標籤。

   b. 在「具有不一致組態設定的電腦」下，檢查設定與用戶端樹狀結構網域設定不一致的用戶端數量。

   c. 請點選數字連結，以顯示用戶端樹狀結構中所有受影響的用戶端。

   d. 從查詢結果中選取用戶端。

   e. 請點選「套用網域設定」。

   f. 如果要將用戶端清單儲存到檔案，請點選「匯出」。

預約符合性報告

「安全性符合」可依預約產生「符合報告」。報告可協助您評估 Apex One 伺服器所管理的 Security Agent 的安全狀態。

如需有關符合性報告的詳細資訊，請參閱適用於受管用戶端的安全性符合 第 15-50 頁。

設定預約「符合性報告」的設定

步驟

1. 移至「評估 > 安全性符合 > 預約報告」。
2. 選取「啟動預約報告」。
3. 指定報告的標題。
4. 選取下列其中一項或全部：
   - 服務 第 15-52 頁
   - 元件 第 15-53 頁
   - 掃瞄符合性 第 15-55 頁
   - 設定 第 15-57 頁
5. 指定將接收預約「符合性報告」相關通知的電子郵件信箱。

   注意

   設定電子郵件通知設定，以確保可成功地傳送電子郵件通知。如需詳細資訊，請參閱管理員通知設定 第 14-35 頁。

6. 指定預約時程。
7. 請點選「儲存」。

適用於未受管端點的安全性符合

「安全性符合」可查詢 Apex One 伺服器所屬網路中的未受管理端點。使用 Active Directory 和 IP 位址來查詢端點。

未受管理端點的安全狀態可以是下列任一種：

表 15-12. 未受管理端點的安全狀態

狀態	說明
受其他 Apex One 伺服器管理	電腦上安裝的 Security Agent 由另一部 Apex One 伺服器管理。Security Agent 已連線，並執行此版本 Apex One 或更舊的版本。
未安裝 Security Agent	端點上已安裝 Security Agent。
無法連接	Apex One 伺服器無法連線至該端點並判斷其安全狀態。
無法解析的 Active Directory 評估	該端點屬於 Active Directory 網域，但 Apex One 伺服器無法判斷其安全狀態。 注意 Apex One 伺服器資料庫包含伺服器所管理的用戶端清單。伺服器會在 Active Directory 中查詢電腦的 GUID，然後與儲存在資料庫中的 GUID 做比較。如果 GUID 不在資料庫中，便會將端點歸類在「無法解析的 Active Directory 評估」類別下。

如果要執行安全性評估，請執行下列工作：

1. 定義查詢範圍。如需詳細資訊，請參閱定義 Active Directory/IP 位址範圍和查詢 第 15-63 頁。
2. 檢查查詢結果中未受保護的電腦。如需詳細資訊，請參閱檢視查詢結果 第 15-66 頁。
3. 安裝 Security Agent。如需詳細資訊，請參閱以安全性符合進行安裝 第 5-47 頁。
4. 設定預約查詢。如需詳細資訊，請參閱設定預約查詢評估 第 15-67 頁。

定義 Active Directory/IP 位址範圍和查詢

首次查詢時，請定義 Active Directory/IP 位址範圍，此範圍包含 Apex One 伺服器將依要求或定期查詢的 Active Directory 物件和 IP 位址。定義範圍之後，請啟動查詢程序。

注意

為定義 Active Directory 範圍，Apex One 必須先與 Active Directory 整合。如需有關整合的詳細資訊，請參閱 Active Directory 整合 第 2-31 頁。

步驟

1. 移至「評估 > 未受管理的端點」。
2. 在「Active Directory/IP 位址範圍」區段中，請點選「定義範圍」。

   接著會開啟一個新畫面。
3. 如果要定義 Active Directory 範圍：
   a. 移至「Active Directory 範圍」區段。
   b. 選取「使用依要求執行的評估」，執行即時查詢以獲得更準確的結果。關閉此選項會使得 Apex One 查詢資料庫，而非查詢每個 Security Agent。只查詢資料庫的速度比較快，但查詢結果比較不準確。
   c. 選取要查詢的物件。如果是首次查詢，請選取包含少於 1,000 個帳號的物件，然後記錄完成查詢所花的時間。使用此資料做為效能基準。
4. 如果要定義 IP 位址範圍：
   a. 移至「IP 位址範圍」區段。
   b. 選取「啟動 IP 位址範圍」。
   c. 指定 IP 位址範圍。請點選加號或減號按鈕以新增或刪除 IP 位址範圍。
   - 對於純 IPv4 Apex One 伺服器，請輸入 IPv4 位址範圍。
   - 對於純 IPv6 Apex One 伺服器，請輸入 IPv6 字首和長度。
   - 對於雙堆疊 Apex One 伺服器，請輸入 IPv4 位址範圍和（或）IPv6 字首和長度。

     IPv6 位址範圍的限制是 16 個位元，這與 IPv4 位址範圍的限制相同。因此，字首長度應該介於 112 到 128 之間。

表 15-13. IPv6 位址的字首長度和號碼

長度	IPv6 位址的號碼
128	2
124	16
120	256
116	4,096
112	65,536

5. 在「進階設定」下，指定 Apex One 伺服器用來與用戶端通訊的通訊埠。

   如果要檢視 Apex One 伺服器所使用的通訊埠，請移至「用戶端 > 用戶端管理」，然後選取網域。通訊埠會顯示在「IP 位址」欄旁邊。趨勢科技建議您記下通訊埠號碼以備參考。

   a. 請點選「指定通訊埠」。

   b. 輸入通訊埠號碼，然後請點選「新增」。重複此步驟，直到新增所需的所有通訊埠號碼。

   c. 請點選「儲存」。

6. 如果要使用特定通訊埠號碼檢查端點的連線能力，請選取「宣告無法與端點連線，方法是檢查通訊埠 <x>」。如果無法建立連線，Apex One 會立即將該端點視為無法連接。預設通訊埠號碼是 135。

   啟動此設定可加快查詢。無法建立與端點的連線時，Apex One 伺服器不需要再執行所有其他連線驗證工作，就會將這些端點視為無法連接。

7. 如果要儲存範圍並啟動查詢，請點選「儲存並重新評估」。如果只要儲存設定，請點選「僅儲存」。

   「外部伺服器管理」畫面會顯示查詢的結果。

注意

查詢可能需要較長的時間才能完成，在查詢範圍較大時更是如此。請等到「外部伺服器管理」畫面顯示結果後，再執行另一次查詢。否則，目前的查詢作業階段會終止，而且查詢程序會重新啟動。

檢視查詢結果

查詢結果會出現在「安全狀態」區段下。未受管理的端點將具有下列其中一種狀態：

- 受其他 Apex One 伺服器管理
- 未安裝 Security Agent
- 無法連接
- 無法解析的 Active Directory 評估

步驟

1. 在「安全狀態」區段中，請點選數字連結以顯示所有受影響的電腦。
2. 使用搜尋和進階搜尋功能，搜尋並僅顯示符合搜尋條件的電腦。

   如果您使用進階搜尋功能，請指定下列項目：

   - IPv4 位址範圍
   - IPv6 字首和長度（字首應該介於 112 到 128 之間）
   - 端點名稱
   - Apex One 伺服器名稱
   - Active Directory 樹狀結構
   - 安全狀態

   如果名稱不完整，Apex One 將不會傳回結果。如果不確定完整名稱，請使用萬用字元 (*)。

3. 如果要將電腦清單儲存到檔案，請點選「匯出」。
4. 對於由另一部 Apex One 伺服器管理的 Security Agent，請使用 Agent Mover 工具將這些 Security Agent 變更為由目前的 Apex One 伺服器管理。如需有關此工具的詳細資訊，請參閱 Agent Mover 第 15-21 頁。

設定預約查詢評估

設定 Apex One 伺服器定期查詢 Active Directory 和 IP 位址，以確保安全指導方針獲得實行。

步驟

1. 移至「評估 > 未受管理的端點」。
2. 請點選用戶端樹狀結構頂端的「定義預約時程」。
3. 啟動預約查詢。
4. 指定預約時程。
5. 請點選「儲存」。

趨勢科技虛擬桌面支援

使用「趨勢科技虛擬桌面支援」最佳化虛擬桌面防護。此功能會調節位於單一虛擬伺服器上的 Security Agent 工作。

在單一伺服器上執行多個桌面，以及依需求執行掃瞄或執行元件更新會耗用大量的系統資源。使用此功能可禁止用戶端同時執行掃瞄或更新元件。

例如，如果 VMware vCenter 伺服器有三個執行 Security Agent 的虛擬桌面，Apex One 可以開始「立即掃瞄」並將更新同時部署到所有三個用戶端。「虛擬桌面支援」會辨識用戶端是否位於同一個實體伺服器。「虛擬桌面支援」允許先在第一個用戶端上執行工作，延後其他兩個用戶端上執行相同工作，直到第一個用戶端完成該工作為止。

您可以在下列平台上使用「虛擬桌面支援」：

- VMware vCenter™ (VMware View™)
- Citrix™ XenServer™ (Citrix XenDesktop™)
- Microsoft Hyper-V™ 伺服器

對於使用其他虛擬化應用程式的管理員，Apex One 伺服器也可以做為模擬 Hypervisor 來管理虛擬用戶端。

使用「Apex One VDI 安裝前掃瞄範本產生工具」可最佳化依需求掃瞄或從基礎映像或模板映像中移除 GUID。

虛擬桌面支援系統需求

下表列出了「虛擬桌面支援」所支援的虛擬平台。

虛擬化供應商	支援的平台
VMware	• VMware vCenter：5.x、6.x、7.x • VMware View：4.x、5.x、6.x • VMware Horizon View：6.x、7.x、8.x
Citrix	• Citrix XenServer：6.x、7.x

虛擬化供應商	支援的平台
HyperV	Hyper-V Server： • Microsoft Hyper-V Server 2008/2008 R2（64 位元） • Microsoft Hyper-V Server 2012/2012 R2（64 位元） • Microsoft Hyper-V Server 2016（64 位元） • Microsoft Hyper-V Server 2019（64 位元） Windows Server Hyper-V： • Windows Server 2008/2008 R2（64 位元）Hyper-V • Windows Server 2012/2012 R2（64 位元）Hyper-V • Windows Server 2016（64 位元）Hyper-V • Windows Server 2019（64 位元）Hyper-V Windows Hyper-V： • Windows 8/8.1 Pro/Enterprise（64 位元）Hyper-V • Windows 10 Pro/Pro for Workstation/Enterprise （64 位元）Hyper-V

虛擬桌面支援安裝

「虛擬桌面支援」是 Apex One 內建的功能，但您必須另行為此功能取得使用授權。安裝 Apex One 伺服器之後，此功能就可用，但此功能無法運作。安裝此功能表示您必須從主動式更新伺服器（或自訂更新來源，如果已設定自訂更新來源）下載檔案。該檔案併入 Apex One 伺服器之後，您就可以註冊「虛擬桌面支援」以啟動其完整功能。您必須從 Plug-in Manager 執行安裝和註冊。

注意

純 IPv6 環境未完全支援「虛擬桌面支援」。如需詳細資訊，請參閱單純 IPv6 伺服器的限制 第 A-2 頁。

安裝虛擬桌面支援

步驟

1. 開啟 Apex One Web 主控台，然後請點選主功能表中的嵌入程式。
2. 在「Plug-in Manager」畫面中，移至「趨勢科技虛擬桌面支援」區段，然後請點選「下載」。

   套件的大小會顯示在「下載」按鈕旁。

   Plug-in Manager 會將下載的套件儲存到 <伺服器安裝資料夾>\PCCSRV\Download\Product。

   注意

   如果 Plug-in Manager 無法下載該檔案，它會在 24 小時後自動重新下載。如果要手動讓 Plug-in Manager 下載該套件，請從 Microsoft Management Console 重新啟動 Apex One Plug-in Manager 服務。
3. 監控下載進度。下載期間您可以瀏覽其他畫面。

   如果在下載套件時遇到問題，請檢查 Apex One 產品主控台中的伺服器更新記錄檔。在主功能表上，請點選「記錄檔 > 伺服器更新」。

   當 Plug-in Manager 下載該檔案之後，「虛擬桌面支援」會顯示在新畫面中。

   注意

   如果未顯示「虛擬桌面支援」，請參閱 Plug-in Manager 疑難排解 第 17-11 頁，以查知原因和解決方案。
4. 如果要立即安裝「虛擬桌面支援」，請點選「立即安裝」。如果要稍後安裝：

   a. 請點選「稍後安裝」。

   b. 開啟「Plug-in Manager」畫面。

   c. 移至「趨勢科技虛擬桌面支援」區段，然後請點選「安裝」。

5. 閱讀授權合約，然後請點選「同意」表示您接受其中的條款。

   安裝便會開始。

6. 監控安裝進度。安裝之後，會顯示「虛擬桌面支援」的版本。

虛擬桌面支援使用授權

您可以從 Plug-in Manager 檢視、註冊和續約「虛擬桌面支援」使用授權。

請從趨勢科技取得啟動碼，然後用它來啟動「虛擬桌面支援」的完整功能。

註冊或續約「虛擬桌面支援」

步驟

1. 開啟 Apex One Web 主控台，然後請點選主功能表中的嵌入程式。
2. 在 Plug-in Manager 畫面中，移至「趨勢科技虛擬桌面支援」區段，然後請點選「管理程式」。
3. 請點選「檢視使用授權資訊」。
4. 在開啟的「產品使用授權詳細資料」畫面中，請點選「新啟動碼」。
5. 在開啟的畫面中輸入「啟動碼」，然後請點選「儲存」。
6. 返回「產品使用授權詳細資料」畫面，請點選「更新資訊」重新整理該畫面，以便顯示新使用授權詳細資料和功能狀態。這個畫面也提供趨勢科技網站連結，請點選此連結即可檢視關於您的使用授權的詳細資訊。

檢視「虛擬桌面支援」的使用授權資訊

步驟

1. 開啟 Apex One Web 主控台，然後請點選主功能表中的嵌入程式 > [趨勢科技虛擬桌面支援] 管理程式。
2. 請點選「檢視使用授權資訊」。
3. 在開啟的畫面中檢視使用授權詳細資訊。

   「虛擬桌面支援使用授權詳細資料」區段提供下列資訊：

   - 狀態：顯示「已啟動」、「未啟動」或「已到期」。
   - 版本：顯示「完整版」或「試用版」。如果您同時擁有完整版和試用版，則會顯示的版本是「完整版」。
   - 到期日：如果「虛擬桌面支援」有多個使用授權，會顯示最新的到期日。例如，如果使用授權到期日為 2010 年 12 月 31 日和 2010 年 6 月 30 日，則會顯示 2010 年 12 月 31 日。
   - 授權數目：顯示可使用「虛擬桌面支援」的 Security Agent 數量
   - 啟動碼：顯示啟動碼

   出現下列情況時顯示有關使用授權的提醒：

   如果您有完整版使用授權：

   - 在功能的寬限期內。寬限期視地區而定。請向您的趨勢科技銷售人員確認寬限期。
   - 使用授權到期且經過寬限期以後。在這期間，您無法取得技術支援。

   如果您有試用版使用授權

   - 使用授權到期時。在這期間，您無法取得技術支援。
4. 請點選「線上檢視詳細的使用授權」，在趨勢科技網站上檢視您的使用授權相關資訊。

5. 如果要更新畫面以顯示最新的使用授權資訊，請點選「更新資訊」。

虛擬伺服器連線

透過新增 VMware vCenter 4 (VMware View 4)、Citrix XenServer 5.5 (Citrix XenDesktop 4) 或 Microsoft Hyper-V Server，可最佳化依需求掃瞄或元件更新。Apex One 伺服器會與指定的虛擬伺服器進行通訊，以判斷 Security Agent 是否位於同一個實體伺服器。

對於其他 VDI 伺服器，Apex One 伺服器提供了模擬虛擬 Hypervisor 來管理其他平台上的虛擬用戶端。Apex One Hypervisor 按照伺服器接收要求的順序處理虛擬用戶端要求。Apex One 伺服器每次處理一個要求，並將其他要求放在佇列中。

新增伺服器連線

步驟

1. 開啟 Apex One Web 主控台，然後請點選主功能表中的嵌入程式 > [趨勢科技虛擬桌面支援] 管理程式。
2. 選取「VMware vCenter 伺服器」、「Citrix XenServer」、「Microsoft Hyper-V」或「其他虛擬應用程式」。

   注意

   選取「其他虛擬應用程式」時，不需要任何其他資訊。Apex One 伺服器按照伺服器接收要求的順序回應虛擬用戶端要求。
3. 啟動與伺服器之間的連線。
4. 指定下列資訊：
   - 針對 VMware vCenter 和 Citrix XenServer 伺服器：
     - IP 位址

- 通訊埠
- 連線通訊協定（HTTP 或 HTTPS）
- 使用者名稱
- 密碼

- 針對 Microsoft Hyper-V 伺服器：
  - 主機名稱或 IP 位址
  - 網域\使用者名稱

  注意
  登入帳號必須為管理員群組中的網域帳號

  - 密碼

5. 您可以視需要啟動 VMware vCenter 或 Citrix XenServer Proxy 連線。
   a. 指定 Proxy 伺服器名稱或 IP 位址，以及通訊埠。
   b. 如果 Proxy 伺服器需要驗證，請指定使用者名稱和密碼。
6. 請點選「測試連線」以驗證 Apex One 伺服器是否可成功連線至伺服器。

   注意
   如需疑難排解 Microsoft Hyper-V 連線的詳細資訊，請參閱疑難排解 Microsoft Hyper-V 連線 第 15-76 頁。
7. 請點選「儲存」。

新增其他伺服器連線

步驟

1. 開啟 Apex One Web 主控台，然後請點選主功能表中的嵌入程式 > [趨勢科技虛擬桌面支援] 管理程式。

2. 請點選「新增 vCenter 連線」、「新增 XenServer 連線」或「新增 Hyper-V 連線」。
3. 重複以上步驟來提供適當的伺服器資訊。
4. 請點選「儲存」。

刪除連線設定

步驟

1. 開啟 Apex One Web 主控台，然後移至主功能表中的「嵌入程式 > [趨勢科技虛擬桌面支援] 管理程式」。
2. 請點選「刪除此連線」。
3. 請點選「確定」以確認刪除此設定。
4. 請點選「儲存」。

變更 VDI 掃瞄容量

管理員可以藉由修改 `vdi.ini` 檔案，增加執行同時掃瞄的 VDI 端點數目。趨勢科技 建議嚴密監控變更 VDI 容量所造成的影響，以確保系統資源能夠處理任何增加的掃瞄工作量。

步驟

1. 在 Apex One 伺服器電腦上，移至 <伺服器安裝資料夾>`PCCSRV\Private\vdi.ini`。
2. 找出 `[TaskController]` 設定。

   預設 TaskController 設定如下：

   - `[TaskController]`

```
Controller_02_MaxConcurrentGuests=1

Controller_03_MaxConcurrentGuests=3
```

說明：

- `Controller_02_MaxConcurrentGuests=1` 等於可以同時執行掃瞄的用戶端數目上限。
- `Controller_03_MaxConcurrentGuests=3` 等於可以同時執行更新的用戶端數目上限。

3. 視需要增加或減少每個控制器中的計數。

   所有設定的最小值為 1。

   所有設定的最大值為 65536。

4. 儲存並關閉 `vdi.ini` 檔案。
5. 重新啟動 Apex One Master Service。
6. 監控 VDI 端點的 CPU、記憶體和磁碟使用率資源。重複步驟 1 至 5，進一步修改控制器設定，以配合 VDI 環境增加/減少同時掃瞄的數目。

疑難排解 Microsoft Hyper-V 連線

Microsoft Hyper-V 連線會針對用戶端和伺服器間的通訊使用 Windows Management Instrumentation (WMI) 和 DCOM。防火牆策略可能會封鎖此通訊，而導致連線至 Hyper-V 伺服器失敗。

Hyper-V 伺服器監聽通訊埠會預設為通訊埠 135，然後會選擇一個隨機設定的通訊埠作為日後通訊之用。如果防火牆封鎖 WMI 傳輸或這兩個通訊埠的其中之一，則與伺服器的連線就會失敗。管理員可以修改防火牆策略，使與 Hyper-V 伺服器的通訊可以成功進行。

在進行下列防火牆修改前確認 IP 位址、網域\使用者名稱和密碼等所有連線設定皆正確。

允許透過 Windows 防火牆進行 WMI 通訊

步驟

1. 在 Hyper-V 伺服器上，開啟「Windows 防火牆允許的程式」畫面。

   在 Windows 2008 R2 系統上，移至「控制面板 > 系統和安全 > Windows 防火牆 > 允許程式或功能透過 Windows 防火牆」。

2. 選取「Windows Management Instrumentation (WMI)」。

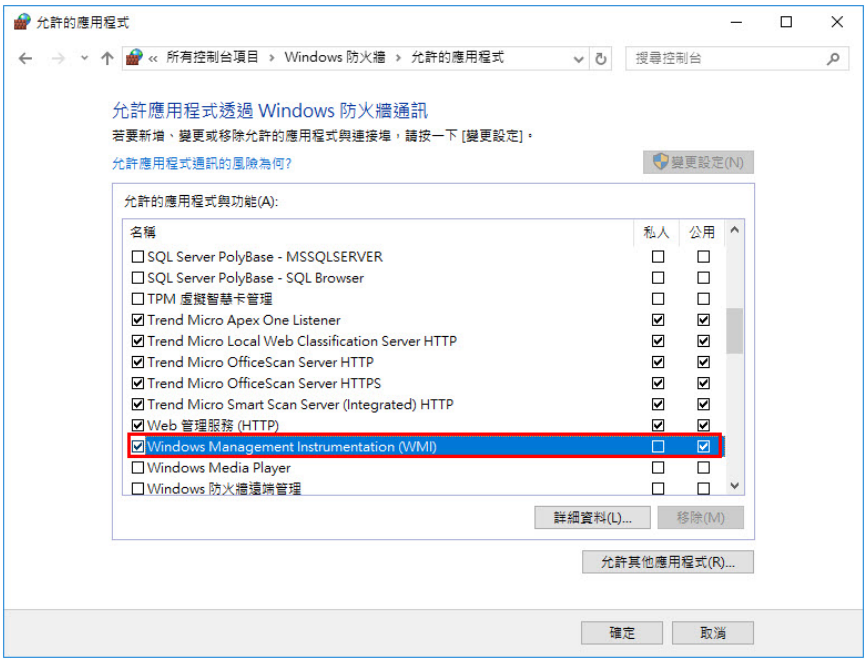


圖 15-7. 「Windows 防火牆允許的程式」畫面

3. 請點選「儲存」。

4. 重新測試 Hyper-V 連線。

允許透過 Windows 防火牆或第三方防火牆開啟通訊埠通訊

步驟

1. 在 Hyper-V 伺服器上確認防火牆允許透過通訊埠 135 進行通訊，並重新測試 Hyper-V 連線。

   如需開啟通訊埠的詳細資訊，請參閱您的防火牆文件。

2. 如果連線至 Hyper-V 伺服器失敗，則請設定 WMI 使用固定的通訊埠。

   如需「為 *WMI* 設定固定通訊埠」，請參閱：

   https://docs.microsoft.com/en-us/windows/desktop/WmiSdk/setting-up-a-fixed-port-for-wmi

3. 開啟通訊埠 135 和新建立的固定通訊埠 (24158) 以透過防火牆進行通訊。

4. 重新測試 Hyper-V 連線。

VDI 安裝前掃瞄範本產生工具

使用「Apex One VDI 安裝前掃瞄範本產生工具」可最佳化依需求掃瞄或從基礎映像或模板映像中移除 GUID。此工具會掃瞄基礎或模板映像並認證該映像。掃瞄此映像的重複項時，Apex One 只會檢查發生變更的部分。這可確保縮短掃瞄時間。

秘訣

趨勢科技建議您在套用 Windows 更新或安裝新的應用程式後產生預先掃瞄範本。

使用工具建立安裝前掃瞄範本

步驟

1. 在 Apex One 伺服器電腦上，瀏覽至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\TCacheGen。
2. 選擇 VDI 安裝前掃瞄範本產生工具的版本。下列是可以使用的版本：

   表 15-14. VDI 安裝前掃瞄範本產生工具版本

檔案名稱	指示
TCacheGen.exe	如果您要直接在 32 位元平台上執行此工具，請選擇這個檔案。
TCacheGen_x64.exe	如果您要直接在 64 位元平台上執行此工具，請選擇這個檔案。

3. 將工具複製到目標 VM 範本上的任意目錄下。

   重要

   TCacheGen.exe 不能透過網路共用來執行，必須本機複製到 VM 範本上。請務必根據 VM 範本架構（64 位元或 32 位元）複製正確的工具。

4. 按兩下 TCacheGen.exe 或 TCacheGen_x64.exe。
5. 選取「產生安裝前掃瞄範本並移除 GUID」，然後按一下「下一步」。
6. 提供 Security Agent 卸載密碼（視情況是否需要）。

   該工具會在產生安裝前掃瞄範本和移除 GUID 之前，先掃瞄映像是否有安全威脅。

   產生安裝前掃瞄範本後，工具會自動卸載 Security Agent 並刪除 TCacheGen.exe 或 TCacheGen_x64.exe 程式。

   請勿重新載入 Security Agent。如果重新載入 Security Agent，則您需要再次建立安裝前掃瞄範本。

使用 CLI 建立安裝前掃瞄範本

步驟

1. 在 Apex One 伺服器電腦上，瀏覽至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\TCacheGen。
2. 選擇 VDI 安裝前掃瞄範本產生工具的版本。下列是可以使用的版本：

   表 15-15. VDI 安裝前掃瞄範本產生工具版本

檔案名稱	指示
TCacheGen.exe TCacheGenCli.exe	如果您要從 32 位元平台的命令列介面執行此工具，請同時選擇 TCacheGenCli.exe 檔案和 TCacheGen.exe。
TCacheGen_x64.exe TCacheGenCli_x64.exe	如果您要從 64 位元平台的命令列介面執行此工具，請同時選擇 TCacheGenCli_x64.exe 和 TCacheGen_x64.exe。

3. 卸載目標 VM 範本上的 Security Agent。
4. 將上一步中選擇的工具版本複製到目標 VM 範本中的 <用戶端安裝資料夾>。

   重要

   TCacheGen.exe 不能透過網路共用來執行，必須本機複製到 VM 範本上。請務必根據 VM 範本架構（64 位元或 32 位元）複製正確的工具。

5. 重新啟動 Security Agent 程式以確保可以執行安裝前掃瞄。
6. 開啟命令提示字元，然後將目錄切換至 <用戶端安裝資料夾>。
7. 使用下列命令之一來執行工具：
   - 32 位元系統：`TCacheGenCli Generate_Template`
   - 64 位元系統：`TcacheGenCli_x64 Generate_Template`

注意

該工具會在產生安裝前掃瞄範本和移除 GUID 之前，先掃瞄映像是否有安全威脅。

產生安裝前掃瞄範本後，工具會自動卸載 Security Agent 並刪除 `TCacheGen.exe` 或 `TCacheGen_x64.exe` 程式。您必須視需要手動刪除關聯的 `TCacheGenCli.exe` 或 `TCacheGenCli_x64.exe`。

請勿重新載入 Security Agent。如果重新載入 Security Agent，則您需要再次建立安裝前掃瞄範本。

移除範本中的 GUID

步驟

1. 在 Apex One 伺服器電腦上，瀏覽至 <伺服器安裝資料夾>`\PCCSRV\Admin\Utility\TCacheGen`。
2. 選擇 VDI 安裝前掃瞄範本產生工具的版本。下列是可以使用的版本：

   表 15-16. VDI 安裝前掃瞄範本產生工具版本

檔案名稱	指示
TCacheGen.exe	如果您要直接在 32 位元平台上執行此工具，請選擇這個檔案。
TCacheGen_x64.exe	如果您要直接在 64 位元平台上執行此工具，請選擇這個檔案。
TCacheGenCli.exe	如果您要從 32 位元平台的命令列介面執行此工具，請同時選擇 `TCacheGenCli.exe` 檔案和 `TCacheGen.exe`。
TCacheGenCli_x64.exe	如果您要從 64 位元平台的命令列介面執行此工具，請同時選擇 `TCacheGenCli_x64.exe` 和 `TCacheGen_x64.exe`。

3. 將上一步中選擇的工具版本複製到目標 VM 範本中的 <用戶端安裝資料夾>。
4. 執行此工具。
   - 如果要直接執行工具：

a. 按兩下 TCacheGen.exe 或 TCacheGen_x64.exe。

b. 選取「移除範本中的 GUID」並按「下一步」。

- 如果要從命令列介面執行工具：

a. 開啟命令提示字元，然後將目錄變更為 <用戶端安裝資料夾>。

b. 輸入下列命令：

```
TCacheGenCli Remove GUID
```

或者

```
TcacheGenCli_x64 Remove GUID
```

全域用戶端設定

Apex One 會將全域用戶端設定套用到所有用戶端，或者僅套用到具有特定權限的用戶端。

步驟

1. 移至「用戶端 > 全域用戶端設定」。
2. 設定下列設定：

表 15-17. 全域用戶端設定

標籤	設定	關係
安全設定	掃瞄設定	掃瞄設定區段 第 7-61 頁
	預約掃瞄設定	預約掃瞄設定區段 第 7-66 頁
	防火牆設定	全域防火牆設定 第 13-22 頁
	可疑連線設定	設定全域使用者定義的 IP 清單設定 第 8-6 頁
	行為監控設定	配置全域行為監控設定 第 9-14 頁
系統	認證安全防護軟體服務設定	設定全域掃瞄設定 第 7-60 頁
	主動雲端截毒技術服務 Proxy	設定全球主動雲端截毒技術服務 Proxy 設定 第 15-46 頁
	更新	• 作為 Security Agent 更新來源的主動式更新伺服器 第 6-33 頁 • 為 Security Agent 更新設定保留磁碟空間 第 6-43 頁
	服務重新啟動	重新啟動 Security Agent 服務 第 15-14 頁
網路	偏好的 IP 位址	用戶端 IP 位址 第 5-7 頁
	伺服器-用戶端通訊	加強的伺服器-用戶端通訊加密 第 14-52 頁
	病毒/惡意程式記錄檔頻寬設定	設定全域掃瞄設定 第 7-60 頁
	無法連接的網路	無法連接的用戶端 第 15-38 頁
用戶端控制	一般設定	設定全域掃瞄設定 第 7-60 頁
	警訊設定	設定 Security Agent 更新通知 第 6-45 頁
	用戶端語言組態設定	Security Agent 語言組態設定 第 15-20 頁

3. 請點選「儲存」。

設定用戶端權限及其他設定

授與使用者修改特定設定並在 Security Agent 上執行高等級工作的權限。

注意

防毒設定僅會在啟動 Apex One 防毒功能之後才會顯示。

秘訣

如果要在整個組織中執行統一的設定和策略，請僅授與使用者有限的權限。

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，請點選根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請點選「設定 > 權限和其他設定」。
4. 在「權限」標籤上，設定下列使用者權限：

表 15-18. 用戶端權限

用戶端權限	關係
單機模式權限	Security Agent 單機模式權限 第 15-17 頁
掃瞄權限	掃瞄類型權限 第 7-49 頁
預約掃瞄權限	預約掃瞄權限和其他設定 第 7-51 頁
防火牆權限	防火牆權限 第 13-20 頁
行為監控權限	行為監控權限 第 9-16 頁

用戶端權限	關係
信任的程式清單	信任的程式清單權限 第 7-59 頁
郵件掃瞄權限	郵件掃瞄權限和其他設定 第 7-54 頁
Proxy 設定權限	授與 Proxy 設定權限 第 15-47 頁
元件更新權限	設定更新權限及其他設定 第 6-41 頁
結束並解除鎖定	授與用戶端卸載與解除鎖定權限 第 15-16 頁
解除安裝	授與 Security Agent 解除安裝權限 第 5-57 頁

5. 請點選「其他設定」標籤並設定下列設定：

表 15-19. 其他用戶端設定

設定	關係
更新設定	設定更新權限及其他設定 第 6-41 頁
網頁信譽評等設定	給用戶端使用者的網路安全威脅通知 第 12-10 頁
行為監控設定	行為監控權限 第 9-16 頁
C&C 聯絡人警訊設定	用戶端使用者的 C&C 聯絡人警訊通知 第 12-15 頁
中央隔離區恢復警訊設定	恢復隔離檔案後，在端點上顯示通知訊息
Machine Learning 設定	偵測到未知安全威脅後，在端點上顯示通知訊息
預約掃瞄設定	授與預約掃瞄權限並顯示權限通知 第 7-52 頁
用於掃瞄的快取設定	用於掃瞄的快取設定 第 7-56 頁
POP3 電子郵件掃瞄設定	授與郵件掃瞄權限和啟動 POP3 郵件掃瞄 第 7-55 頁
Security Agent 存取限制	Security Agent 主控台存取限制 第 15-15 頁

設定	關係
重新啟動通知	給 Security Agent 使用者的安全威脅通知 第 7-75 頁

6. 如果在用戶端樹狀結構中選取網域或用戶端，請點選「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用至未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

部分 IV

提供其他防護

第 16 章

保護外部部署用戶端

本章說明要保護離開企業內部網路的 Security Agent，必須執行的 Edge Relay 伺服器安裝與組態設定步驟。

包含下列主題：

Edge Relay 伺服器

Apex OneEdge Relay 伺服器能夠針對被使用者帶出公司內部網路的端點，讓管理員能瞭解該類端點上發生的狀況並提供增強的保護。在對外網路 (DMZ) 安裝 Edge Relay 伺服器後，外部部署 Security Agent 即使無法直接與 Apex One 伺服器連線，仍能輪詢伺服器來接收更新的策略設定。

設定 Edge Relay 伺服器之後，Security Agent 即會接收設定，並且會在 Apex One 伺服器連線無法使用時，自動開始連線到 Edge Relay 伺服器。

Edge Relay 伺服器、Apex One 伺服器與 Security Agent 之間的通訊會採用憑證驗證加密。

如需詳細資訊，請參閱管理 Edge Relay 伺服器憑證 第 16-17 頁。

Edge Relay 伺服器系統需求

安裝 Edge Relay 伺服器前，請確保目標伺服器電腦符合最低系統需求。

資源	需求
處理器	2 GHz 雙核心
記憶體	1 GB（專門用於 Edge Relay 伺服器）
磁碟空間	60 GB
作業系統	• Windows Server 2016 • Windows Server 2012 R2

網路卡	• 2 張網路卡
	  • 一張用於與 Apex One 伺服器的內部網路連線
	  • 一張用於與外部部署 Security Agent 的外部連線
	• 1 張網路卡，設定為針對內部網路與 Internet 連線使用不同的通訊埠

安裝 Edge Relay 伺服器

安裝 Edge Relay 伺服器前，請確保目標伺服器電腦符合最低系統需求。

如需詳細資訊，請參閱 Edge Relay 伺服器系統需求 第 16-2 頁。

步驟

1. 在 Apex One 伺服器電腦上找到 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\EdgeServer 資料夾，然後將該資料夾複製到目標 Edge Relay 伺服器電腦上。
2. 在目標 Edge Relay 伺服器上，開啟 EdgeServer 資料夾，然後執行 setup.exe 檔案以啟動安裝程序。

   安裝套件會檢查伺服器是否具備所需的元件。
3. 如果伺服器上不存在下列任一元件，請在執行 Edge Relay 伺服器安裝程序期間請點選「安裝」，允許安裝程式安裝缺失的元件。
   - Microsoft Visual C++ 2017 Update 3 可轉散發套件 (x86)
   - Microsoft Visual C++ 2017 Update 3 可轉散發套件 (x64)
   - Microsoft .NET Framework 4.6.1
   - Microsoft URL Rewrite Module 2.0 for IIS (x64)
   - Microsoft 應用程式要求路由 3.0 (x64)

   會出現「歡迎使用」畫面。
4. 按「下一步」。

會出現「安裝路徑」畫面。

5. 接受預設的安裝目錄，或請點選「變更...」以選取其他位置。

6. 按「下一步」>。

   會出現「Edge Relay 伺服器 — Security Agent 連線」畫面。

7. 指定外部部署 Security Agent 連線至 Edge Relay 伺服器時使用的下列設定：

   - Edge Relay 伺服器 FQDN：輸入 Edge Relay 伺服器的 FQDN
   - 憑證：為 Edge Relay 伺服器選取 Webhost 憑證，或按一下「下一步 >」讓系統建立自我簽署憑證。

   注意

   如果您沒有立即可用的自訂憑證，可以在安裝完成後使用 Edge Relay 伺服器註冊工具來變更自我簽署憑證。

   如需詳細資訊，請參閱將客戶特定憑證與 Edge Relay 伺服器繫結 第 16-15 頁。

- IP 位址：選取伺服器的 IP 位址
- 通訊埠：接受預設通訊埠，或指定通訊埠

重要

您必須將防火牆與閘道設定為允許：

- 將 Security Agent 通訊從 Internet 重新導向至 Edge Relay 伺服器
- 透過指定的通訊埠進行的通訊

8. 按「下一步」>。

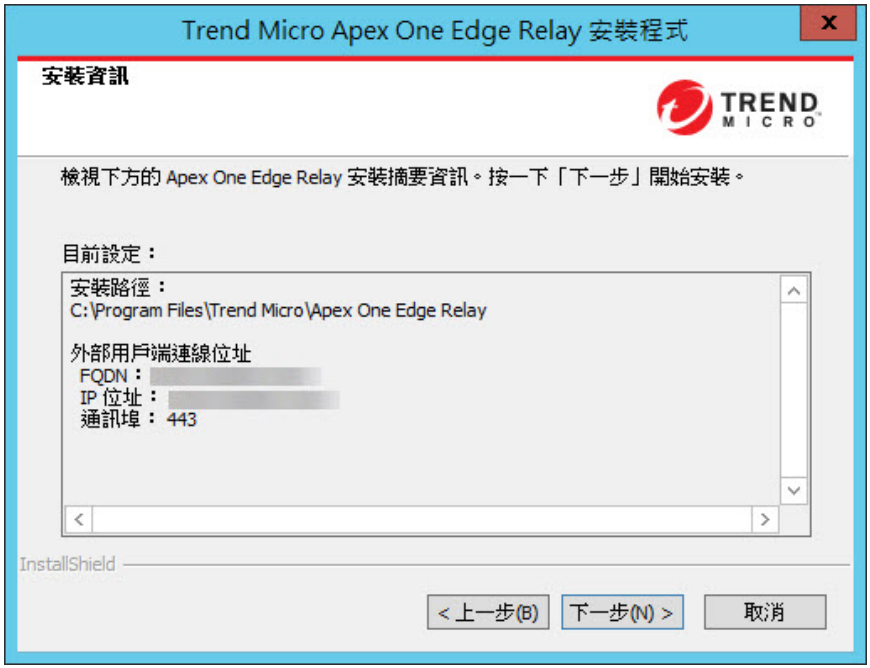
   會出現「SSL 憑證」畫面。

9. 指定並確認用於 Edge Relay 伺服器憑證（OsceOPA 憑證）的密碼。

10. 按「下一步」>。

    會出現「安裝資訊」畫面。

11. 請點選「下一步 >」開始進行安裝。



安裝完成時，會出現「已完成安裝精靈」畫面。

12. 請點選「完成」。

Edge Relay 伺服器已可供使用。您可以設定 Edge Relay 伺服器支援哪些 Apex One 伺服器。

如需詳細資訊，請參閱 Edge Relay 伺服器註冊工具 第 16-11 頁。

升級 Edge Relay 伺服器

Apex One Edge Relay 伺服器支援從舊版 Edge Relay 伺服器進行升級。在升級過程中，安裝程式會自動套用舊版使用的相同伺服器設定並移轉所有憑證。

重要

此版本的 Edge Relay 伺服器不支援舊版的用戶端程式。如果您想要管理外部部署端點，請務必將所有用戶端升級到 Apex One Security Agent，並將 Security Agent 連線到 Apex One 伺服器來取得已升級的 Edge Relay 設定。

升級 Edge Relay 伺服器前，請確保目標伺服器電腦符合最低系統需求。

如需詳細資訊，請參閱 Edge Relay 伺服器系統需求 第 16-2 頁。

步驟

1. 在 Apex One 伺服器電腦上找到 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\EdgeServer 資料夾，然後將該資料夾複製到目標 Edge Relay 伺服器電腦上。
2. 在目標 Edge Relay 伺服器上，開啟 EdgeServer 資料夾，然後執行 setup.exe 檔案以啟動升級程序。

   會出現「歡迎使用」畫面。
3. 按一下「下一步 >」

   安裝程式會自動從舊版 Edge Relay 伺服器擷取必要的設定，並顯示「安裝資訊」畫面。
4. 按一下「下一步 >」以開始進行升級。
5. 在升級完成後，您必須使用 Edge Relay 伺服器註冊工具，將升級後的 Edge Relay 伺服器向 Apex One 伺服器註冊。
   a. 在 Edge Relay 伺服器電腦上的下列位置找到 Edge Relay 伺服器註冊工具：

      <Apex One Edge Relay 安裝目錄>\OfcEdgeSvc\ofcedgecfg.exe
   b. 以管理員權限開啟命令列編輯器。

      以滑鼠右鍵按一下 cmd.exe，然後按一下「以系統管理員身分執行」。
   c. 將目錄切換到 ofcedgecfg.exe 檔案的位置。

d. 執行下列命令：

```
ofcedgecfg.exe --cmd reg --server <Apex One 伺服器位址>
--port <Apex One 伺服器通訊埠> --pwd <Apex One 'root' 帳號
的密碼>
```

在 Apex One Web 主控台（「管理 > 設定 > Edge Relay」）中確認已成功註冊升級後的 Edge Relay 伺服器。

6. 請確保您想要使用 Edge Relay 伺服器進行管理的所有 Security Agent 皆可直接連線到 Apex One 伺服器，來取得最新的 Edge Relay 伺服器設定。

Edge Relay 伺服器註冊工具

安裝 Edge Relay 伺服器後，您必須使用 Edge Relay 伺服器註冊工具，將 Edge Relay 伺服器向 Apex One（外部部署 Security Agent 向其回報）伺服器註冊。Security Agent（向 Apex One 伺服器回報）會接收已註冊的連線設定，並且可在離開企業內部網路後自動使用 Edge Relay 伺服器來輪詢 Apex One 伺服器。

Edge Relay 伺服器註冊工具讓您可以使用命令列編輯器執行下列工作：

- 向 Apex One 伺服器註冊 第 16-12 頁
- 從 Apex One 伺服器取消註冊 第 16-13 頁
- 續約自我簽署憑證（包括 OsceEdgeRoot CA、Webhost 和 OsceOPA） 第 16-13 頁
- 將客戶特定憑證與 Webhost 及 OsceOPA 憑證繫結 第 16-14 頁
- 刪除所有 IIS 規則（從所有 Apex One 伺服器取消註冊後） 第 16-15 頁

使用 Edge Relay 伺服器註冊工具

Edge Relay 伺服器註冊工具讓您可以使用命令列編輯器執行下列工作：

- 向 Apex One 伺服器註冊 第 16-12 頁

- 從 Apex One 伺服器取消註冊 第 16-13 頁
- 續約自我簽署憑證（包括 OsceEdgeRoot CA、Webhost 和 OsceOPA） 第 16-13 頁
- 將客戶特定憑證與 Webhost 及 OsceOPA 憑證繫結 第 16-14 頁
- 刪除所有 IIS 規則（從所有 Apex One 伺服器取消註冊後） 第 16-15 頁

注意

您可以將 Edge Relay 伺服器向多部 Apex One 伺服器註冊。對每個需要的 Apex One 連線執行單獨的註冊命令。

步驟

1. 在 Edge Relay 伺服器電腦上的下列位置找到 Edge Relay 伺服器註冊工具：

   `<Apex One Edge Relay 安裝目錄>\OfcEdgeSvc\ofcedgecfg.exe`

2. 以管理員權限開啟命令列編輯器。

   以滑鼠右鍵按一下 `cmd.exe`，然後按一下「以系統管理員身分執行」。

3. 將目錄切換到 `ofcedgecfg.exe` 檔案的位置。

4. 執行所需的工作。

向 Apex One 伺服器註冊

命令	`--cmd reg`	
參數	`--server <值>`	Apex One 伺服器 IP 位址
	`--port <值>`	Apex One 伺服器通訊埠號碼
	`--pwd <值>`	Apex One 伺服器 'root' 帳號的密碼

範例	`ofcedgecfg.exe --cmd reg --server <伺服器位址> --port <通訊埠> --pwd <root 密碼>`

從 Apex One 伺服器取消註冊

命令	`--cmd unreg`	
參數	`--server <值>`	Apex One 伺服器 IP 位址
	`--port <值>`	Apex One 伺服器通訊埠號碼
	`--pwd <值>`	Apex One 伺服器 'root' 帳號的密碼
範例	`ofcedgecfg.exe --cmd unreg --server <伺服器位址> --port <通訊埠> --pwd <root 密碼>`	

續約自我簽署憑證（包括 OsceEdgeRoot CA、Webhost 和 OsceOPA）

警告!

如果您使用 Edge Relay 安裝程式所建立的憑證，請僅使用 `renewcert` 命令。如果您在使用客戶特定憑證的 Edge Relay 伺服器上執行 `renewcert` 命令，該命令會刪除客戶特定憑證並取代為自我簽署憑證。

命令	`--cmd renewcert`	
參數	`--opacertpwd <值>`	OsceOPA 憑證密碼
	`--keeprootca`	續約憑證後保留根 CA（選用）
範例	`ofcedgecfg.exe --cmd renewcert --opacertpwd <OsceOPA 憑證密碼> [--keeprootca]`	

後續必要命令	續約憑證後，必須將 Edge Relay 伺服器重新註冊到 Apex One 伺服器。 如需詳細資訊，請參閱向 Apex One 伺服器註冊 第 16-12 頁。 **重要** 向 Apex One 伺服器重新註冊後，必須確保所有外部部署 Security Agent 重新連線到 Apex One 伺服器以取得更新的憑證。任何未收到最新憑證的外部部署 Security Agent，皆無法連線至 Edge Relay 伺服器。

將客戶特定憑證與 Webhost 及 OsceOPA 憑證繫結

重要

您必須備妥並正確設定 Webhost 和 OsceOPA 憑證，才能將客戶特定憑證與 Edge Relay 伺服器繫結。

如需有關準備及繫結客戶特定憑證的詳細資訊和詳細指示，請參閱將客戶特定憑證與 Edge Relay 伺服器繫結 第 16-15 頁。

命令	`--cmd bindwebsite`	
參數	`--certsubject <值>`	Webhost 憑證主體
	`--certstore <值>`	Webhost 憑證儲存區名稱：`My | webhosting`
	`--certissuer <值>`	Webhost 憑證核發者
	`--opacertpwd <值>`	OsceOPA 憑證密碼
範例	`ofcedgecfg.exe --cmd bindwebsite --certsubject <憑證主體名稱> --certstore <憑證儲存區名稱> --certissuer <憑證核發者> --opacertpwd <OsceOPA 憑證密碼>`	

後續必要命令	繫結客戶特定憑證後，必須將 Edge Relay 伺服器重新註冊到 Apex One 伺服器。 如需詳細資訊，請參閱向 Apex One 伺服器註冊 第 16-12 頁。 **重要** 向 Apex One 伺服器重新註冊後，必須確保所有外部部署 Security Agent 重新連線到 Apex One 伺服器以取得更新的憑證。任何未收到最新憑證的外部部署 Security Agent，皆無法連線至 Edge Relay 伺服器。

刪除所有 IIS 規則（從所有 Apex One 伺服器取消註冊後）

命令	`--cmd delrule`
參數	無
範例	`ofcedgecfg.exe --cmd delrule`

將客戶特定憑證與 Edge Relay 伺服器繫結

您可以建立並繫結客戶特定憑證，以驗證 Apex One 伺服器及 Security Agent 與 Edge Relay 伺服器之間的通訊。

重要

使用客戶特定憑證時，該憑證必須同時包含公開金鑰和私密金鑰，以便簽核其他憑證。

出於公開金鑰和私密金鑰的規定限制，您可能無法使用市面上大多數的第三方 CA。

步驟

1. 請備妥自訂的 Webhost 憑證：
   - 必須由信任的儲存區中所含的 CA 核發
   - 儲存在「網站代管」憑證儲存區中：「My」或「webhosting」
   - 記下下列在繫結期間需要用到的資訊：
     - 憑證主體
     - 憑證核發者

   重要

   使用客戶特定憑證時，該憑證必須同時包含公開金鑰和私密金鑰，以便簽核其他憑證。

   出於公開金鑰和私密金鑰的規定限制，您可能無法使用市面上大多數的第三方 CA。

2. 請備妥取代自我簽署 OsceOPA 憑證的有效憑證。
   - 必須由信任的儲存區中所含的 CA 核發
   - 需要的憑證主體：`OsceOPA`

     重要

     憑證主體區分大小寫。

   - 儲存在「OfcEdge」憑證儲存區中，並從儲存區中移除任何其他憑證
3. 在 Edge Relay 伺服器電腦上的下列位置找到 Edge Relay 伺服器註冊工具：

   ```
   <Apex One Edge Relay 安裝目錄>\OfcEdgeSvc\ofcedgecfg.exe
   ```

4. 以管理員權限開啟命令列編輯器。

   以滑鼠右鍵按一下 `cmd.exe`，然後按一下「以系統管理員身分執行」。

5. 將目錄切換到 ofcedgecfg.exe 檔案的位置。
6. 執行下列命令：

   ```
   ofcedgecfg.exe --cmd bindwebsite --certsubject <Webhost 憑證主體名稱> --certstore <My | webhosting> --certissuer <Webhost 憑證核發者> --opacertpwd <OsceOPA 憑證密碼>
   ```

7. 執行下列命令，以將 Edge Relay 伺服器重新註冊到 Apex One 伺服器：

   ```
   ofcedgecfg.exe --cmd reg --server <伺服器位址> --port <通訊埠> --pwd <root 密碼>
   ```

8. 指示所有外部部署使用者直接連線到近端內部網路，以便讓 Security Agent 接收更新的憑證並重新連線至 Edge Relay 伺服器。

在 Apex One 中檢視 Edge Relay 伺服器連線

與 Edge Relay 伺服器連線後，向 Apex One 伺服器報告的 Security Agent 即會接收連線設定，而且可以在離開企業內部網路後，自動與 Edge Relay 伺服器通訊。然後，您便可以從「Edge Relay 設定」畫面監控 Edge Relay 伺服器連線狀態。

步驟

1. 在 Apex One Web 主控台上，移至「管理 > 設定 > Edge Relay」。

   會出現「Edge Relay 設定」畫面。

2. 檢視目前已向 Apex One 伺服器註冊的 Edge Relay 伺服器。

管理 Edge Relay 伺服器憑證

Apex One 提供命令列工具，可讓您建立或續訂用戶端用於通訊的 Edge Relay 伺服器憑證。建立新憑證之後，Edge Relay 伺服器會將新憑證傳送給 Apex

One 伺服器，而 Apex One 伺服器會在下次用戶端與之連線時，將該憑證部署到用戶端上。

重要

外部部署 Security Agent 必須與 Apex One 伺服器連線，才能取得新的 Edge Relay 伺服器憑證。沒有收到更新版憑證的任何外部部署用戶端，除非與 Apex One 伺服器建立連線，否則無法再繼續與 Edge Relay 伺服器通訊。

步驟

1. 在 Edge Relay 伺服器上，開啟命令列編輯器，然後移至下列目錄：

   ```
   C:\Program Files\Trend Micro\Apex One Edge Relay\OfcEdgeSvc
   \
   ```

2. 執行下列命令來執行憑證工具：

   ```
   ofcedgecfg.exe --cmd renewcert --opacertpwd <OsceOPA 憑證密碼
   > [--keeprootca]
   ```

   說明：

   - `--renewcert`:建立新憑證
   - `--opacertpwd <密碼>`：指定憑證套件的密碼

   Edge Relay 伺服器便會建立新的憑證套件，並自動將憑證傳送給 Apex One 伺服器。下次 Security Agent 向 Apex One 伺服器報告時，Apex One 伺服器就會將新憑證部署到 Security Agent 上。

第 17 章

使用 Plug-in Manager

本章討論如何設定 Plug-in Manager，並提供透過 Plug-in Manager 提供之嵌入程式解決方案的總覽。

包含下列主題：

關於 Plug-in Manager

Apex One 包括一個名為 Plug-in Manager 的架構，可以將新的解決方案整合到既有的 Apex One 環境。為有效簡化這些解決方案的管理，Plug-in Manager 以 Widget 的形式提供解決方案的概覽資料。

注意

當前沒有任何嵌入解決方案支援 IPv6。伺服器可下載這些解決方案，但無法將其部署到純 IPv6 Security Agent 或純 IPv6 主機。

Plug-in Manager 提供下列優點：

- 本機產品功能

  有些本機 Apex One 功能會單獨授權，並透過 Plug-In Manager 啟動。在本版本中，有兩種功能屬於此類別，分別是「趨勢科技虛擬桌面支援」和「Apex One 資料安全防護」。

- 嵌入程式

  嵌入程式不屬於 Apex One 程式。嵌入程式擁有單獨的使用授權和管理主控台。從 Apex One Web 主控台存取管理主控台。嵌入程式的範例為「Trend Micro Apex One 工具箱」和「Trend Micro Apex One (Mac)」。

- 資訊中心標籤和 Widget

  Apex One 的「資訊中心」畫面需要有 Plug-in Manager，才能顯示用來監控 Apex One 伺服器與用戶端安全防護狀態的標籤與 Widget。

本文件提供了嵌入程式安裝和管理的一般概述，並討論了 Widget 中可用的 Plug-in 資料。如需設定和管理程式的詳細資訊，請參閱特定嵌入程式的文件。

端點上的嵌入程式用戶端

一些嵌入程式（如 Apex One (Mac)）具有安裝在端點 Windows 作業系統中的用戶端。在處理程序名稱 CNTAoSMgr.exe 下執行的 Security Agent Plug-in Manager 管理這些用戶端。

Apex One 隨 Security Agent 一起安裝 CNTAoSMgr.exe。對 CNTAoSMgr.exe 的唯一其他系統需求是 Microsoft XML Parser (MSXML) 3.0 版或更新版本。

注意

其他嵌入程式的用戶端未安裝在 Windows 作業系統上，這些用戶端不從 Security Agent Plug-in Manager 進行管理。Apex One (Mac) Security Agent 是這些用戶端的範例之一。

Widget

使用 Widget 可檢視已部署的嵌入程式解決方案的概覽資料。Apex One 伺服器的「資訊中心」畫面上提供了 Widget。一個名為「Apex One 與嵌入程式混搭技術」的特殊 Widget 會將 Security Agent 和嵌入程式解決方案中的資料結合，然後將資料顯示在用戶端樹狀結構中。

本管理手冊概述了 Widget 以及支援 Widget 的解決方案。

Plug-in Manager 安裝

在先前的 Plug-in Manager 版本中，Plug-in Manager 安裝套件是從趨勢科技主動式更新伺服器下載而來，然後安裝在裝載 Apex One 伺服器的電腦上。在此版本中，安裝套件已包含在下列位置的 Apex One 伺服器安裝套件中：

<伺服器安裝資料夾>\PCCSRV\Admin\Utility\PLM\PLMSetup.exe

執行 PLMSetup.exe 檔案以安裝 Plug-in Manager。

剛接觸 Apex One 的新使用者在完成 Apex One 安裝之後，會同時安裝 Apex One 伺服器和 Plug-in Manager。升級至此 Apex One 版本且之前已使用 Plug-

in Manager 的使用者需要先停止 Plug-in Manager 服務，然後再執行安裝套件。

執行安裝後的工作

在安裝 Plug-in Manager 之後請執行以下操作：

步驟

1. 開啟 Apex One Web 主控台，然後請點選主功能表中的「嵌入程式」。
2. 管理嵌入程式解決方案。
3. 存取 Apex One Web 主控台上的「資訊中心」，以管理用於嵌入程式解決方案的 Widget。

本機 Apex One 功能管理

本機 Apex One 功能會隨 Apex One 一起安裝，並且管理員會從 Plug-in Manager 啟動每個功能。有些功能（如趨勢科技虛擬桌面支援）是從 Plug-in Manager 進行管理，而有些功能（如 Apex One 資料安全防護）則是從 Apex One Web 主控台進行管理。

管理嵌入程式

Apex One 的嵌入程式獨立安裝和啟動。每個嵌入程式都獨立的主控台來進行產品管理。可以從 Apex One Web 主控台存取管理主控台。

嵌入程式安裝

嵌入程式會顯示在 Plug-in Manager 主控台上。可以使用主控台下載、安裝及管理該程式。Plug-in Manager 從趨勢科技主動式更新伺服器或自訂更新來源

（如果已正確設定）下載嵌入程式的安裝套件。必須有 Internet 連線，才能從主動式更新伺服器下載套件。

當 Plug-in Manager 下載安裝套件或開始安裝時，Plug-in Manager 會暫時關閉其他的嵌入程式功能，例如下載、安裝和升級。

Plug-in Manager 不支援從 Trend Micro Apex Central 的單一登入功能進行嵌入程式安裝或管理。

安裝嵌入程式

步驟

1. 開啟 Apex One Web 主控台，然後請點選主功能表中的「嵌入程式」。
2. 在 Plug-in Manager 畫面中，移至嵌入程式區段，然後請點選「下載」。

   嵌入程式套件的大小會顯示在「下載」按鈕旁邊。 Plug-in Manager 會將下載的套件儲存到 <伺服器安裝資料夾>\PCCSRV\Download\Product。

   Plug-in Manager 會將下載的套件儲存到 <伺服器安裝資料夾>\PCCSRV\Download\Product

   下載期間您可以監控進度或瀏覽其他畫面。

   注意

   如果 Apex One 在下載或安裝套件時遇到問題，請檢查 Apex One Web 主控台中的伺服器更新記錄檔。在主功能表上，請點選「記錄檔 > 伺服器更新」。
3. 請點選「立即安裝」或「稍後安裝」。
   - 請點選「立即安裝」後，開始安裝且出現安裝進度畫面。
   - 請點選「稍後安裝」後，會出現「Plug-in Manager」畫面。

     透過請點選「Plug-in Manager」畫面的嵌入程式區段中的「安裝」按鈕，來安裝嵌入程式。

   會出現「趨勢科技使用者授權合約」畫面。

注意

並非所有嵌入程式都需要此畫面。如果未顯示此畫面，表示已開始安裝嵌入程式。

4. 請點選「同意」安裝嵌入程式。

   安裝期間您可以監控進度或瀏覽其他畫面。

注意

如果 Apex One 在下載或安裝套件時遇到問題，請檢查 Apex One Web 主控台中的伺服器更新記錄檔。在主功能表上，請點選「記錄檔 > 伺服器更新」。

安裝後，目前嵌入程式版本會顯示在「Plug-in Manager」畫面上。

啟動嵌入程式授權

步驟

1. 開啟 Apex One Web 主控台，然後請點選主功能表中的「嵌入程式」。
2. 在 Plug-in Manager 畫面中，移至嵌入程式區段，然後請點選「管理程式」。

   會出現「產品使用授權新啟動碼」畫面。
3. 在文字欄位輸入或複製並貼上啟動碼。
4. 請點選「儲存」。

   會出現嵌入程式主控台。

檢視和更新使用授權資訊

步驟

1. 開啟 Apex One Web 主控台，然後請點選主功能表中的「嵌入程式」。
2. 在 Plug-in Manager 畫面中，移至嵌入程式區段，然後請點選「管理程式」。
3. 瀏覽嵌入程式主控台到「檢視使用授權資訊」超連結。

   並非所有嵌入程式都會在同一位置顯示「檢視使用授權資訊」超連結。如需詳細資訊，請參閱嵌入程式的使用者文件。
4. 在開啟的畫面中檢視下列使用授權詳細資訊。

選項	說明
狀態	顯示「已啟動」、「未啟動」或「已到期」
版本	顯示「完整版」或「試用版」 注意 同時啟動完整版和試用版時顯示的版本是「完整版」。
授權數目	顯示嵌入程式可管理的端點數量
使用授權逾期期限	如果嵌入程式有多個使用授權，會顯示最新的到期日。 例如，如果使用授權到期日為 2011 年 12 月 31 日和 2011 年 6 月 30 日，則會顯示 2011 年 12 月 31 日。
啟動碼	顯示啟動碼
提醒	視您目前的使用授權版本而定，嵌入程式會在寬限期（僅完整版）或使用授權到期時，顯示使用授權到期日提醒

注意

寬限期視地區而定。請向您的趨勢科技銷售人員確認嵌入程式的寬限期。

嵌入程式使用授權到期後，嵌入程式繼續起作用，但是更新和支援不再可用。

5. 請點選「線上檢視詳細的使用授權」，在趨勢科技網站上檢視目前使用授權的相關資訊。
6. 如果要更新畫面以顯示最新的使用授權資訊，請點選「更新資訊」。
7. 請點選「新啟動碼」，開啟「產品使用授權新啟動碼」畫面。

   如需詳細資訊，請參閱啟動嵌入程式授權 第 3-4 頁。

嵌入程式管理

從嵌入程式的管理主控台（可透過 Apex One Web 主控台存取）進行設定並執行與程式相關的工作。工作包括啟動程式，還可能包括將嵌入程式用戶端部署到端點。如需設定和管理程式的詳細資訊，請參閱特定嵌入程式的文件。

管理嵌入程式

步驟

1. 開啟 Apex One Web 主控台，然後請點選主功能表中的「嵌入程式」。
2. 在 Plug-in Manager 畫面中，移至嵌入程式區段，然後請點選「管理程式」。

   首次管理嵌入程式時，嵌入程式可能需要啟動。如需詳細資訊，請參閱啟動嵌入程式授權 第 3-4 頁。

嵌入程式升級

安裝的新版本嵌入程式會顯示在 Plug-in Manager 主控台上。在主控台上下載套件並升級嵌入程式。Plug-in Manager 會從趨勢科技主動式更新伺服器或自訂更新來源（如果已正確設定）下載套件。必須有 Internet 連線，才能從主動式更新伺服器下載套件。

當 Plug-in Manager 下載安裝套件或開始升級時，Plug-in Manager 會暫時關閉其他的嵌入程式功能，例如下載、安裝和升級。

Plug-in Manager 不支援使用 Trend Micro Apex Central 的單一登入功能進行嵌入程式升級。

升級嵌入程式

步驟

1. 開啟 Apex One Web 主控台，然後請點選主功能表中的「嵌入程式」。
2. 在 Plug-in Manager 畫面中，移至嵌入程式區段，然後請點選「下載」。

   升級套件的大小會顯示在「下載」按鈕旁。

   下載期間您可以監控進度或瀏覽其他畫面。

   注意

   如果 Apex One 在下載或安裝套件時遇到問題，請檢查 Apex One Web 主控台中的伺服器更新記錄檔。在主功能表上，請點選「記錄檔 > 伺服器更新」。
3. Plug-in Manager 下載套件後，會顯示一個新畫面。
4. 請點選「立即升級」或「稍後升級」。
   - 請點選「立即升級」後，開始升級且出現升級進度畫面。
   - 請點選「稍後升級」後，會出現「Plug-in Manager」畫面。

     透過請點選「Plug-in Manager」畫面的嵌入程式區段中的「升級」按鈕，來升級嵌入程式。

升級後，Plug-in Manager 服務可能需要重新啟動，這會導致「Plug-in Manager」畫面暫時不可用。該畫面可用時，將顯示目前嵌入程式版本。

嵌入程式解除安裝

以下列方式解除安裝嵌入程式：

- 從 Plug-in Manager 主控台解除安裝嵌入程式。
- 解除安裝 Apex One 伺服器同時也會解除安裝 Plug-in Manager 和所有安裝的嵌入程式。如需解除安裝 Apex One 伺服器的說明，請參閱 *Apex One 安裝和升級手冊*。

對於端點上具有用戶端的嵌入程式：

- 請參閱嵌入程式的文件，以查看解除安裝嵌入程式是否也將解除安裝嵌入程式用戶端。
- 對於與 Security Agent 安裝在同一端點上的嵌入程式用戶端，解除安裝 Security Agent 也將解除安裝嵌入程式用戶端和 Security Agent Plug-in Manager (`CNTAoSMgr.exe`)。

從 Plug-in Manager 主控台解除安裝嵌入程式

步驟

1. 開啟 Apex One Web 主控台，然後請點選主功能表中的「嵌入程式」。
2. 在「Plug-in Manager」畫面中，移至嵌入程式區段，然後請點選「解除安裝」。
3. 解除安裝期間您可以監控解除安裝進度或瀏覽其他畫面。
4. 解除安裝之後，請重新整理「Plug-in Manager」畫面。

   Plug-in 程式再次可供安裝。

解除安裝 Plug-in Manager

解除安裝 Apex One 伺服器同時也會解除安裝 Plug-in Manager 和所有伺服器嵌入程式。如需解除安裝 Apex One 伺服器的說明，請參閱 *Apex One* 安裝和升級手冊。

Plug-in Manager 疑難排解

檢查 Apex One 伺服器和 Plug-in Manager 的 Security Agent 偵錯記錄，以及嵌入程式偵錯資訊。

Plug-in 程式不顯示在 Plug-in Manager 主控台上

可供下載和安裝的任何嵌入程式可能會因以下原因而無法顯示在 Plug-in Manager 主控台上：

步驟

1. Plug-in Manager 仍在下載嵌入程式。如果程式的套件大小較大，可能要花些時間。請時時檢查畫面，以查看 Plug-in 程式是否有顯示。

   注意

   如果 Plug-in Manager 無法下載該嵌入程式，它會在 24 小時後自動重新下載。如果要手動觸發 Plug-in Manager 以下載嵌入程式，請重新啟動 Apex One Plug-in Manager 服務。

2. 伺服器電腦無法連線到 Internet。如果伺服器是透過 Proxy 伺服器連線到 Internet，請確定是否能夠使用 Proxy 設定建立 Internet 連線。

3. Apex One 更新來源不是主動式更新伺服器。在 Apex One Web 主控台上，移至「更新 > 伺服器 > 更新來源」，然後檢查更新來源。如果更新來源不是主動式更新伺服器，您會有下列選擇：

- 選取主動式更新伺服器做為更新來源。
- 如果選取「其他更新來源」，請先在「其他」更新來源清單中選取第一個項目做為更新來源，並且確認它可以成功連線到主動式更新伺服器。Plug-in Manager 僅支援清單中的第一個項目。
- 如果選取「包含目前檔案副本的 Intranet 位置」，請確定 Intranet 中的端點也能連線到主動式更新伺服器。

端點上的嵌入程式用戶端安裝和顯示問題

由於以下原因，在端點上安裝嵌入程式的用戶端可能會失敗，或用戶端可能無法顯示在 Security Agent 主控台上：

步驟

1. 端點上的 Plug-in Manager (`CNTAosMgr.exe`) 未執行。在 Security Agent 端點上，開啟 Windows 工作管理員並執行 `CNTAosMgr.exe` 處理程序。
2. 未將嵌入程式用戶端的安裝套件下載至 `<用戶端安裝資料夾>\AU_Data\AU_Temp\{xxx}AU_Down\Product` 中的 Security Agent 端點資料夾。請檢查位於 `\AU_Data\AU_Log\` 中的 `Tmudump.txt` 以瞭解下載失敗原因。

   注意

   如果成功安裝用戶端，則 `<用戶端安裝資料夾>\AOSSvcInfo.xml` 中的用戶端資訊可用。

3. 用戶端安裝失敗或需要進一步動作。可從嵌入程式的管理主控台檢查安裝狀態，並執行作業，如在安裝後重新啟動 Security Agent 端點或在安裝前安裝必需的作業系統 Patch。

如果 Internet Explorer 上的「自動組態設定程式檔設定」重新導向到 Proxy 伺服器，則端點上的用戶端無法啟動

由於用戶端啟動命令重新導向到 Proxy 伺服器，因此 Security Agent Plug-in Manager (`CNTAosMgr.exe`) 無法啟動端點上的用戶端。這個問題只有在 Proxy 設定將使用者的 HTTP 傳輸重新導向至 127.0.0.1 時才會發生。

如果要解決該問題，請使用定義明確的 Proxy 伺服器策略。例如，勿將 HTTP 傳輸重新導向至 127.0.0.1。

如果您需要使用控制 127.0.0.1 HTTP 要求的 Proxy 組態設定，請執行下列工作。

步驟

1. 在 Apex One Web 主控台上設定 Apex One 防火牆設定值。

   注意

   只有在 Security Agent 啟動 Apex One 防火牆時，才執行這個步驟。

   a. 在 Web 主控台上，移至用戶端 > 防火牆 > 策略，然後請點選「編輯例外範本」。

   b. 在「編輯例外範本」畫面，請點選「新增」。

   c. 使用下列資訊：

      - 名稱：您偏好的名稱
      - 處理行動：允許網路傳輸
      - 方向：輸入
      - 通訊協定：TCP
      - 通訊埠：介於 5000 和 49151 之間的通訊埠號碼

d. IP 位址：選取「單一 IP 位址」並指定您的 Proxy 伺服器 IP 位址（建議選項）或選取「所有 IP 位址」。

e. 請點選「儲存」。

f. 返回「編輯例外範本」畫面，請點選「儲存並且套用到現有策略」。

g. 移至用戶端 > 防火牆 > 資料檔，然後請點選「指定資料檔給用戶端」。

如果沒有防火牆資料檔，請點選「新增」即可建立。使用下列設定：

- 名稱：您偏好的名稱
- 說明：您偏好的說明
- 策略：所有存取策略

儲存新的資料檔之後，請點選「指定資料檔給用戶端」。

2. 修改 `ofcscan.ini` 檔案。

a. 使用文字編輯器開啟 <伺服器安裝資料夾> 中的 `ofcscan.ini` 檔案。

b. 搜尋 `[Global Setting]`，然後將 `FWPortNum=21212` 新增到下一行。將「21212」變更為您在上述步驟 c 中指定的通訊埠號碼。

例如：

```
[Global Setting]

FWPortNum=5000
```

c. 儲存檔案。

3. 在 Web 主控台上，移至用戶端 > 全域用戶端設定，然後請點選「儲存」。

系統、更新模組或 Plug-in Manager 程式中發生錯誤，且錯誤訊息提供特定錯誤碼

Plug-in Manager 將在錯誤訊息中顯示以下任何錯誤碼。如果您在參考下表中提供的解決方案後無法解決問題，請聯絡您的經銷商。

表 17-1. Plug-in Manager 錯誤碼

錯誤碼	訊息、原因和解決方案
001	Plug-in Manager 程式中發生錯誤。 查詢更新工作進度時，Plug-in Manager 更新模組無回應。模組或命令處理常式可能尚未初始化。 重新啟動 Apex One Plug-in Manager 服務，然後重新執行此工作。
002	發生系統錯誤。 Plug-in Manager 更新模組無法開啟登錄機碼 `SOFTWARE\TrendMicro\OfficeScan\service\AoS`，因為該機碼已被刪除。 執行下列步驟： 1. 開啟登錄編輯程式，然後移至 `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service\AoS\OSCE_Addon_Service_CompList_Version`。將值重設為 1.0.1000。 2. 重新啟動 Apex One Plug-in Manager 服務。 3. 下載/解除安裝嵌入程式。

錯誤碼	訊息、原因和解決方案
028	發生更新錯誤。 可能原因： • Plug-in Manager 更新模組無法下載嵌入程式。確認網路連線正常，然後再試一次。 • 由於 AU Patch 用戶端傳回錯誤，因此 Plug-in Manager 更新模組無法安裝嵌入程式。AU Patch 用戶端是一種程式，可以啟動新嵌入程式的安裝作業。如需錯誤的確切原因，請檢查 \PCCSRV\Web\Service\AU_Data\AU_Log 中的主動式更新模組偵錯記錄檔 TmuDump.txt。 執行下列步驟： 1. 開啟登錄編輯程式，然後瀏覽到 HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service\AoS\OSCE_Addon_Service_CompList_Version。將值重設為 1.0.1000。 2. 刪除此嵌入程式登錄機碼 HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_ADDON_xxxx。 3. 重新啟動 Apex One Plug-in Manager 服務。 4. 下載並安裝嵌入程式。
170	發生系統錯誤。 Plug-in Manager 更新模組目前正在處理另一項作業，因此無法處理輸入作業。 請稍後執行此工作。
202	Plug-in Manager 程式中發生錯誤。 Plug-in Manager 程式無法處理正在 Web 主控台上執行的工作。 如果有升級程式可用，請重新整理 Web 主控台或升級 Plug-in Manager。
203	Plug-in Manager 程式中發生錯誤。 嘗試與 Plug-in Manager 後端服務通訊時，Plug-in Manager 程式發生處理程序間通訊 (IPC) 錯誤。 重新啟動 Apex One Plug-in Manager 服務，然後重新執行此工作。

錯誤碼	訊息、原因和解決方案
其他錯誤碼	發生系統錯誤。 下載新的嵌入程式時，Plug-in Manager 會檢查主動式更新伺服器中的嵌入程式清單。Plug-in Manager 無法取得此清單。 執行下列步驟： 1. 開啟登錄編輯程式，然後瀏覽到 `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service\AoS\OSCE_Addon_Service_CompList_Version`。將值重設為 `1.0.1000`。 2. 重新啟動 Apex One Plug-in Manager 服務。 3. 下載並安裝嵌入程式。

第 18 章

疑難排解資源

本章提供一份資源清單，可讓您用來對 Apex One 伺服器和 Security Agent 問題進行疑難排解。

包含下列主題：

智慧型支援系統

「智慧型支援系統」是一個方便您傳送檔案給趨勢科技進行分析的頁面。此系統會判斷 Apex One 伺服器 GUID，然後將這項資訊與您傳送的檔案一起傳送。提供 Apex One 伺服器 GUID，可確保趨勢科技可針對所收到的供評估的檔案提供回應。

案例診斷工具

Trend Micro Case Diagnostic Tool (CDT) 會在問題發生時從客戶的產品中收集必要偵錯資訊，也會自動開啟產品的偵錯狀態並根據問題類別收集必要檔案。趨勢科技會使用這項資訊針對產品相關問題進行疑難排解。

在 Apex One 支援的所有平台上執行此工具。如果要取得這項工具和相關文件，請聯絡您的經銷商。

趨勢科技效能調整工具

趨勢科技提供獨立式效能調整工具，來識別可能引起效能問題的應用程式。趨勢科技效能調整工具（可參閱趨勢科技常見問題集）在試驗程序期間應在標準工作站映像和（或）少數目標工作站上執行，以事先獲得實際部署「行為監控」和「周邊設備存取控管」時發生的效能問題。

注意

效能問題通常起因於更複雜的問題。如果您無法確定效能下降的根本原因，請聯絡您的支援供應商。

Apex One 伺服器記錄檔

除了 Web 主控台上提供的記錄檔之外，您還可以使用其他類型的記錄檔（例如：偵錯記錄檔）來解決產品問題。

警告!

偵錯記錄檔可能會影響伺服器的效能，並且消耗大量的磁碟空間。務必僅在必要時啟動偵錯記錄，並且在不需要偵錯資料時立即關閉。如果您需要節省磁碟空間，請移除記錄檔。

使用 LogServer.exe 的伺服器偵錯記錄檔

使用 `LogServer.exe` 來收集下列項目的偵錯記錄檔：

- Apex One 伺服器基本記錄檔
- Trend Micro Vulnerability Scanner
- Active Directory 整合記錄檔
- 用戶端分組記錄檔
- 安全性符合記錄檔
- 以角色為基礎的管理
- 雲端截毒掃瞄

偵錯記錄

Apex One 會自動收集與「錯誤」事件相關的偵錯記錄檔。如果嘗試關閉偵錯記錄檔的收集，Apex One 會自動重新啟動「錯誤」記錄檔的收集。

步驟

1. 登入 Web 主控台。
2. 在 Web 主控台的標題中，按一下 "Trend Micro Apex One" 中的 "T"。
3. 選取「啟動偵錯記錄檔」。

   注意

   如果嘗試關閉偵錯記錄檔的收集，Apex One 會自動重新啟動「錯誤」記錄檔的收集。

4. 指定偵錯記錄檔設定。

   注意

   Apex One 會自動收集與「錯誤」事件相關的偵錯記錄檔。如果嘗試關閉偵錯記錄檔的收集，Apex One 會自動重新啟動「錯誤」記錄檔的收集。

5. 請點選「儲存」。
6. 檢查預設位置中的記錄檔 (`ofcdebug.log`)：<伺服器安裝資料夾>`\PCCSRV\Log`。

正在啟動伺服器安裝和升級的偵錯記錄

請先啟動偵錯記錄，再執行下列工作：

- 先解除安裝伺服器，然後再安裝一次。
- 將 Apex One 升級為新版本。
- 執行遠端安裝/升級（除錯記錄功能會在您啟動安裝程式的端點上啟動，而不會在遠端端點上啟動）。

步驟

1. 將位於 <伺服器安裝資料夾>`\PCCSRV\Private` 中的 `LogServer` 資料夾複製到 `C:\`。

2. 建立名為 cdebug.ini 的檔案，其中包含下列內容：

   ```
   [debug]

   debuglevel=9

   debuglog=c:\LogServer\ofcdebug.log

   debugLevel_new=D

   debugSplitSize=10485760

   debugSplitPeriod=12

   debugRemoveAfterSplit=1
   ```

3. 將 ofcdebug.ini 儲存到 C:\LogServer。
4. 執行適當工作（亦即解除安裝/重新安裝伺服器，升級為新的伺服器版本或執行遠端安裝/升級）。
5. 檢查 C:\LogServer 中的 ofcdebug.log。

安裝記錄檔

- 本機安裝/升級記錄檔

  檔案名稱：OFCMAS.LOG

  位置：%windir%

Active Directory 記錄檔

- 檔案名稱：ofcdebug.log
- 檔案名稱：ofcserver.ini

  位置：<伺服器安裝資料夾>\PCCSRV\Private\

以角色為基礎的管理記錄檔

如果要取得詳細的以角色為基礎的管理資訊，請執行下列其中一項作業：

- 執行 Trend Micro Case Diagnostics Tool。如需相關資訊，請參閱案例診斷工具 第 18-2 頁。
- 收集下列記錄檔：
  - 在 <伺服器安裝資料夾>\PCCSRV\Private\AuthorStore 資料夾中的所有檔案。
  - Apex One 伺服器記錄檔 第 18-3 頁

Security Agent 分組記錄檔

- 檔案名稱：ofcdebug.log
- 檔案名稱：ofcserver.ini

  位置：<伺服器安裝資料夾>\PCCSRV\Private\
- 檔案名稱：SortingRule.xml

  位置：<伺服器安裝資料夾>\PCCSRV\Private\SortingRuleStore\

元件更新記錄檔

檔案名稱：TmuDump.txt

位置：<伺服器安裝資料夾>\PCCSRV\Web\Service\AU_Data\AU_Log

正在取得詳細的伺服器更新資訊

步驟

1. 建立名為 aucfg.ini 的檔案，其中包含下列內容：

   ```
   [Debug]

   level=-1

   [Downloader]

   ProxyCache=0
   ```

2. 將檔案儲存到 <伺服器安裝資料夾>\PCCSRV\Web\Service。
3. 重新啟動「Apex One Master Service」。

正在停止收集詳細的伺服器更新資訊

步驟

1. 刪除 aucfg.ini。
2. 重新啟動 Apex One Master Service。

用戶端封裝程式記錄檔

啟動建立用戶端封裝程式的記錄

步驟

1. 按照下列方式修改位於 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\ClientPackager 中的 ClnExtor.ini：

```
[Common]

DebugMode=1
```

2. 檢查 C:\ 中的 ClnPack.log。

關閉建立用戶端封裝程式的記錄

步驟

1. 開啟 ClnExtor.ini。
2. 將「DebugMode」值從 1 變更為 0。

安全符合性報告記錄檔

如果要取得詳細的「安全性符合」資訊，請收集下列檔案：

- 檔案名稱：RBAUserProfile.ini

  位置：<伺服器安裝資料夾>\PCCSRV\Private\AuthorStore\

- 在 <伺服器安裝資料夾>\PCCSRV\Log\Security Compliance Report 資料夾中的所有檔案。
- Apex One 伺服器記錄檔 第 18-3 頁

外部伺服器管理記錄檔

- 檔案名稱：ofcdebug.log
- 檔案名稱：ofcserver.ini

  位置：<伺服器安裝資料夾>\PCCSRV\Private\

- 在 <伺服器安裝資料夾>\PCCSRV\Log\Outside Server Management Report\ 資料夾中的所有檔案。

周邊設備存取控管例外記錄檔

如果要取得詳細的「周邊設備存取控管例外」資訊，請收集下列檔案：

- 檔案名稱：ofcscan.ini

  位置：<伺服器安裝資料夾>\

- 來自 Apex One Web 主控台的「周邊設備存取控管例外」清單。

整合式主動雲端截毒技術伺服器網頁信譽評等記錄檔

檔案名稱：diagnostic.log

位置：<伺服器安裝資料夾>\PCCSRV\LWCS\

ServerProtect 一般伺服器移轉工具記錄檔

如果要啟動「ServerProtect 一般伺服器移轉工具」的偵錯記錄：

步驟

1. 建立名為 ofcdebug.ini 的檔案，其中包含下列內容：

   ```
   [Debug]

   DebugLog=C:\ofcdebug.log

   DebugLevel=9
   ```

2. 將檔案儲存到 C:\。

3. 檢查 C:\ 中的 ofcdebug.log。

注意

若要關閉偵錯記錄，請刪除 ofcdebug.ini 檔案。

VSEncrypt 記錄檔

Apex One 會自動在使用者帳號的暫存資料夾中建立偵錯記錄檔 (VSEncrypt.log)。例如，C:\Documents and Settings\<使用者名稱>\Local Settings\Temp。

Apex Central MCP 用戶端記錄檔

對 <伺服器安裝資料夾>\PCCSRV\CMAgent 資料夾中的檔案進行偵錯

- Agent.ini
- Product.ini
- 「Apex Central 設定」網頁擷取畫面
- ProductUI.zip

正在啟動 MCP 用戶端的偵錯記錄

步驟

1. 按照下列方式修改位於 <伺服器安裝資料夾>\PCCSRV\CmAgent 中的 product.ini：

```
[Debug]
debugmode = 3
debuglevel= 3
```

```
debugtype = 0

debugsize = 10000

debuglog = C:\CMAgent_debug.log
```

2. 從 Microsoft 管理主控台重新啟動 Apex One Apex Central Agent 服務。
3. 檢查 C:\ 中的 CMAgent_debug.log。

正在關閉 MCP 用戶端的偵錯記錄

步驟

1. 開啟 product.ini 並刪除下列內容：

```
debugmode = 3

debuglevel= 3

debugtype = 0

debugsize = 10000

debuglog = C:\CMAgent_debug.log
```

2. 重新啟動 Apex One Apex Central Agent 服務。

病毒爆發記錄檔

記錄類型	檔案
目前的防火牆違規病毒爆發記錄檔	檔案名稱：Cfw_Outbreak_Current.log 位置：<伺服器安裝資料夾>\PCCSRV\Log\

記錄類型	檔案
上次防火牆違規病毒爆發記錄檔	檔案名稱：Cfw_Outbreak_Last.log 位置：<伺服器安裝資料夾>\PCCSRV\Log\
目前的病毒/惡意程式爆發記錄檔	檔案名稱：Outbreak_Current.log 位置：<伺服器安裝資料夾>\PCCSRV\Log\
上次病毒/惡意程式爆發記錄檔	檔案名稱：Outbreak_Last.log 位置：<伺服器安裝資料夾>\PCCSRV\Log\
目前的間諜程式/可能的資安威脅程式爆發記錄檔	檔案名稱：Spyware_Outbreak_Current.log 位置：<伺服器安裝資料夾>\PCCSRV\Log\
上次間諜程式/可能的資安威脅程式爆發記錄檔	檔案名稱：Spyware_Outbreak_Last.log 位置：<伺服器安裝資料夾>\PCCSRV\Log\

虛擬桌面支援記錄檔

- 檔案名稱：vdi_list.ini

  位置：<伺服器安裝資料夾>\PCCSRV\TEMP\

- 檔案名稱：vdi.ini

  位置：<伺服器安裝資料夾>\PCCSRV\Private\

- 檔案名稱：ofcdebug.txt

  位置：<伺服器安裝資料夾>\PCCSRV\Log\

如果要產生 ofcdebug.txt，請啟動偵錯記錄。如需啟動偵錯記錄的指示，請參閱偵錯記錄 第 18-3 頁。

Security Agent 記錄檔

可以使用 Security Agent 記錄檔（例如：偵錯記錄檔）對 Security Agent 問題進行疑難排解。

警告!

偵錯記錄檔可能會影響用戶端的效能，並消耗大量的磁碟空間。務必僅在必要時啟動偵錯記錄，並且在不需要偵錯資料時立即關閉。如果記錄檔變得過大，請將其移除。

使用 LogServer.exe 的 Security Agent 偵錯記錄檔

如果要啟動 Security Agent 的偵錯記錄：

步驟

1. 將 `LogServer` 資料夾的內容 (`Log` 子資料夾除外) 複製到目標端點上的新位置。

   找到 `LogServer` 資料夾如下：

   - 新的 Security Agent：`C:\Program Files (x86)\Trend Micro\Security Agent\Temp\LogServer\`
   - 升級的 Security Agent：`C:\Program Files (x86)\Trend Micro\OfficeScan Client\Temp\LogServer\`
   - Apex One 伺服器：`\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Private\LogServer`

2. 修改 `LogServer\ofcdebug.ini` 檔案的內容如下：

   ```
   Debuglog=C:\ofcdebug.log

   debugLevel_new=D

   ForceStopOtherLogserver=1
   ```

視需要，透過更改以下項目從預設的 10MB 增加最大分割大小：
`debugSplitSize=10485760`

視需要，透過更改以下項目來修改最大記錄檔數目：`DebugMaxSplit=100`

3. 儲存檔案。
4. 在目標端點上，使用「以系統管理員身分執行」執行 `LogServer.exe`。

   此工具將建立 `ofcdebug.log` 檔案。
5. 重現問題。
6. 關閉 `LogServer.exe` 視窗以停止偵錯記錄收集。
7. 收集偵錯記錄期間所收集的全部 `.log` 和 `.7z` 記錄檔，並將檔案移到新位置。
8. 刪除步驟 1 中複製的所有檔案。

全新安裝記錄檔

若為 MSI 套件安裝：

- 檔案名稱：`OFCNT.LOG`
- 位置：在系統暫存檔中，例如在 Windows 7 中的位置：

  ```
  C:\Users\Administrator\AppData\Local\Trend Micro\Security Agent\OFCNT.LOG
  ```

若為 Web 安裝：

- 檔案名稱：`WebInstall.log`
- 位置：`C:\`

若為遠端安裝：

- 檔案名稱：`RemoteInstall.LOG`

- 位置：C:\

若為 Autopcc 和 EXE 套件安裝：

- 檔案名稱：OFCNT.LOG
- 位置：%windir%\

升級/HotFix 記錄檔

檔案名稱：upgrade_yyyymmddhhmmss.log

位置：<用戶端安裝資料夾>\Temp

損害清除及復原服務記錄檔

正在啟動「損害清除及復原服務」的偵錯記錄

步驟

1. 開啟 <用戶端安裝資料夾> 中的 TSC.ini。
2. 修改下列這行的內容：

   DebugInfoLevel=5

3. 檢查 <用戶端安裝資料夾>\debug 中的 TSCDebug.log。

正在關閉「損害清除及復原服務」的偵錯記錄

開啟 TSC.ini 並將「DebugInfoLevel」值從 5 變更為 0。

清除記錄檔

檔案名稱：yyyymmdd.log

位置：<用戶端安裝資料夾>\report\

郵件掃瞄記錄檔

檔案名稱：SmolDbg.txt

位置：<用戶端安裝資料夾>

Security Agent 連線記錄檔

檔案名稱：Conn_YYYYMMDD.log

位置：<用戶端安裝資料夾>\ConnLog

Security Agent 更新記錄檔

檔案名稱：Tmudump.txt

位置：<用戶端安裝資料夾>\AU_Data\AU_Log

取得詳細的 Security Agent 更新資訊

步驟

1. 建立名為 aucfg.ini 的檔案，其中包含下列內容：

   ```
   [Debug]
   level=-1
   ```

```
[Downloader]

ProxyCache=0
```

2. 將檔案儲存到 <用戶端安裝資料夾>。
3. 重新載入 Security Agent。

注意

刪除 aucfg.ini 檔案並且重新載入 Security Agent 以停止收集詳細的用戶端更新資訊。

病毒掃瞄引擎記錄檔

如果要啟動「病毒掃瞄引擎」的偵錯記錄：

步驟

1. 開啟「登錄編輯程式」(regedit.exe)。
2. 移至 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMFilter\Parameters。
3. 將「DebugLogFlags」的值變更為「00003eff」。
4. 執行引導您掃瞄所遭遇問題的步驟。
5. 檢查 %windir% 中的 TMFilter.log。

注意

將「DebugLogFlags」的值恢復為「00000000」以關閉偵錯記錄

病毒爆發防範記錄檔

檔案名稱：OPPLogs.log

位置：<用戶端安裝資料夾>\OppLog

病毒爆發防護恢復記錄檔

檔案名稱：

- TmOPP.ini
- TmOPPRestore.ini

位置：<用戶端安裝資料夾>\

行為監控偵錯記錄檔

若要針對「行為監控」啟動偵錯記錄：

步驟

1. 開啟「登錄編輯程式」(regedit.exe)。
2. 移至 HKLM\SOFTWARE\TrendMicro\Aegis。
3. 將機碼 「DebugLogFlags」 新增為「dword:00000032」 。
4. 執行造成您遇到所發生問題的步驟。
5. 檢查 C:\Program Files (x86)\Trend Micro\BM\log\ 資料夾中的下列記錄檔：
   - TmCommengyyyymmdd_nn.log
   - TMPEMyyyymmdd_nn.log

Apex One 防火牆記錄檔

啟動一般防火牆驅動程式的偵錯記錄（所有作業系統）

步驟

1. 修改下列登錄值：

登錄機碼	值
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmwfp\Parameters	類型：DWORD 值 (REG_DWORD) 名稱：DebugCtrl 值：0x00001111
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmlwf\Parameters	類型：DWORD 值 (REG_DWORD) 名稱：DebugCtrl 值：0x00001111

2. 重新啟動端點。
3. 檢查 C:\ 中的 wfp_log.txt 和 lwf_log.txt。

正在關閉一般防火牆驅動程式的偵錯記錄（所有作業系統）

步驟

1. 刪除登錄機碼中的 DebugCtrl。
2. 重新啟動 端點。

啟動 Apex One NT Firewall 服務的偵錯記錄

步驟

1. 按照下列方式編輯位於 <用戶端安裝資料夾> 中的 `TmPfw.ini`：

   ```
   [ServiceSession]

   Enable=1
   ```

2. 重新載入 Security Agent。
3. 檢查 `C:\temp` 中的 `ddmmyyyy_NSC_TmPfw.log`。

正在關閉 Apex One NT Firewall 服務的偵錯記錄

步驟

1. 開啟 `TmPfw.ini`，並將「`Enable`」值從 1 變更為 0。
2. 重新載入 Security Agent。

網頁信譽評等和 POP3 郵件掃瞄記錄檔

正在啟動網頁信譽評等服務和 POP3 郵件掃瞄功能的除錯記錄

步驟

1. 按照下列方式編輯位於 <用戶端安裝資料夾> 中的 `TmOsprey.ini`：

   ```
   [InteractiveSession]

   Enable=1
   ```

```
LogFolder=C:\temp

[ServiceSession]

Enable=1

LogFolder=C:\temp
```

2. 重新載入 Security Agent。
3. 檢查 `C:\temp` 中的 `yyyy-mm-dd_hh-mm-ss_EE_TmOsprey1.etl`。

正在關閉網頁信譽評等服務和 POP3 郵件掃瞄功能的除錯記錄

步驟

1. 按照下列方式編輯位於 <用戶端安裝資料夾> 中的 `TmOsprey.ini`：

```
[InteractiveSession]

Enable=0

LogFolder=C:\temp

[ServiceSession]

Enable=0

LogFolder=C:\temp
```

2. 重新載入 Security Agent。

周邊設備存取控管例外清單記錄檔

檔案名稱：`DAC_ELIST`

位置：<用戶端安裝資料夾>\

注意

如果要存取加密的記錄檔資料，請洽詢您的支援人員。

資料安全防護偵錯記錄檔

啟動資料安全防護偵錯記錄檔：

步驟

1. 從支援供應商處取得 `logger.cfg` 檔案。
2. 將下列資料新增至 `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\DlpLite`：
   - 類型：字串
   - 名稱：`debugcfg`
   - 值：`C:\Log\logger.cfg`
3. 在 `C:\ directory` 目錄中建立名為「Log」的資料夾。
4. 將 `logger.cfg` 複製到 `Log` 資料夾。
5. 從 Web 主控台部署「資料外洩防護」和「周邊設備存取控管」設定，以開始收集記錄檔。

注意

透過刪除登錄機碼中的 `debugcfg`，然後重新啟動端點，以關閉資料安全防護模組的偵錯記錄功能。

Windows 事件記錄檔

Windows 事件檢視器會記錄成功發生的應用程式事件，例如登入或變更帳號設定。

步驟

1. 執行下列其中一項作業：
   - 請點選「開始 > 控制台 > 效能與維護 > 系統管理工具 > 電腦管理」。
   - 開啟包含事件檢視器嵌入式管理單元的 MMC。
2. 請點選「事件檢視器」。

傳輸驅動程式介面 (TDI) 記錄檔

啟動傳輸驅動程式介面 (TDI) 記錄檔：

步驟

1. 將下列資料新增至 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\tmtdi\Parameters`：

參數	值
機碼 1	類型：`DWORD` 值 (`REG_DWORD`) 名稱：`Debug` 值：`1111` (十六進位)
機碼 2	類型：字串值 (`REG_SZ`) 名稱：`LogFile` 值：`C:\tmtdi.log`

2. 重新啟動 端點。
3. 檢查 `C:\` 中的 `tmtdi.log`。

注意

在登錄機碼中刪除 `Debug` 和 `LogFile` 然後重新啟動端點，以關閉 TDI 的偵錯記錄。

第 19 章

技術支援

瞭解下列主題：

疑難排解資源

聯絡技術支援之前，請考慮造訪下列趨勢科技線上資源。

使用支援入口網站

趨勢科技支援入口網站是全年無休的線上資源，包含有關常見和不常見問題的最新資訊。

步驟

1. 移至「https://success.trendmicro.com/tw/business-support」。
2. 從可用產品中進行選取，或請點選適當的按鈕來搜尋解決方案。
3. 使用「搜尋支援」方塊搜尋可用的解決方案。
4. 如果未找到解決方案，請點選「聯絡支援」，然後選取所需的支援類型。

   秘訣

   若要線上提交支援案例，請造訪下列 URL：

   https://success.trendmicro.com/tw/sign-in

   趨勢科技支援工程師會在 24 小時或更短時間內調查案例並對其進行回應。

安全威脅百科全書

現今的大多數惡意程式都包含混合安全威脅（合併了兩種或更多種技術），以略過電腦安全通訊協定。趨勢科技會使用建立自訂防範策略的產品來抵禦此複雜惡意程式。安全威脅百科全書提供了多種混合性安全威脅的名稱和癥狀的完整清單，包括已知惡意程式、垃圾郵件、惡意 URL 和已知弱點。

移至 https://www.trendmicro.com/vinfo/tw/threat-encyclopedia/malware/ 以瞭解更多資訊：

- 目前正在使用中或「擴散中」的惡意程式和惡意可攜式程式碼。
- 用於形成完整網頁攻擊過程的關聯安全威脅資訊頁面
- 有關目標攻擊和安全威脅的 Internet 安全威脅諮詢
- 網頁攻擊和線上趨勢資訊
- 每週惡意程式報告

聯絡趨勢科技

可以透過電話或電子郵件聯絡趨勢科技代表：

地址	趨勢科技股份有限公司 台北市敦化南路二段 198 號 8 樓
電話	(886) 2-23789666
網站	https://www.trendmicro.com
電子郵件信箱	企業授權用戶技術專線 Web mail：http://www.trend.com.tw/corpmail/

- 全球客戶服務據點：

  https://www.trendmicro.com/us/about-us/contact/index.html
- 與台灣趨勢科技聯絡：

  http://www.trendmicro.tw/tw/about-us/contact/index.html
- 趨勢科技產品文件：

  https://docs.trendmicro.com/zh-tw/home.aspx

加速支援要求

為了提高解決問題的速度，現已提供下列資訊：

- 問題模擬的步驟
- 裝置或網路資訊
- 電腦品牌、型號以及連接的任何其他硬體或裝置
- 記憶體大小和可用硬碟空間
- 作業系統和 Service Pack 版本
- 安裝的用戶端版本
- 產品序號或啟動碼
- 安裝環境的詳細說明
- 已接收的任何錯誤訊息的確切文字

將可疑內容傳送到趨勢科技

有多個選項可供將可疑內容傳送到趨勢科技，以便進一步分析。

電子郵件信譽評等服務

查詢特定 IP 位址的信譽評等，並指定一個訊息轉移用戶端，以將其包含在全域核可清單中：

https://ers.trendmicro.com/

請參閱下列「常見問題集」項目，將訊息範例傳送給趨勢科技：

https://success.trendmicro.com/tw/solution/1112106

檔案信譽評等服務

收集系統資訊並將可疑檔案內容提交到趨勢科技：

https://success.trendmicro.com/tw/solution/1059565

記錄案例編號以供追蹤。

網頁信譽評等服務

查詢疑似網路釣魚網站的 URL 的安全分級和內容類型，或其他所謂「病媒」（間諜程式和惡意程式等 Internet 威脅的蓄意來源）：

https://global.sitesafety.trendmicro.com/

如果指定的分級不正確，請傳送重新分類要求到趨勢科技。

其他資源

除了解決方案和支援外，線上還提供許多其他實用資源，可讓您保持最新狀態、瞭解創新以及最新的安全趨勢。

下載專區

有時，趨勢科技可能會針對報告的已知問題發行修補程式，或是發行適用於特定產品或服務的升級。如果要瞭解是否有適用的修補程式，請移至：

https://downloadcenter.trendmicro.com/index.php?regs=tw

如果未套用修補程式（修補程式已過期），請開啟 Readme 檔以判斷其是否與您的環境相關。Readme 檔還包含安裝說明。

文件意見反應

趨勢科技始終力求改善其文件。如果您對本文件或趨勢科技的任何文件有任何疑問、意見或建議，請透過 https://docs.trendmicro.com/en-us/survey.aspx 聯絡我們。

附錄

附錄

附錄 A

Apex One 中的 IPv6 支援

本附錄的適用對象是打算在支援 IPv6 定址的環境中部署 Apex One 的使用者。本附錄包含有關 Apex One 中 IPv6 支援範圍的資訊。

趨勢科技假設讀者熟悉 IPv6 概念及設定支援 IPv6 定址之網路的相關工作。

適用於 Apex One 伺服器和用戶端的 IPv6 支援

安裝或升級符合 IPv6 需求的 Apex One 伺服器和 Security Agent 之後，會自動啟動 IPv6 支援。

Apex One 伺服器需求

Apex One 伺服器的 IPv6 需求如下：

- 如果伺服器將管理 IPv4 和 IPv6 Security Agent，則必須同時具有 IPv4 和 IPv6 位址，且必須由其主機名稱加以識別。如果伺服器是由其 IPv4 位址所識別，則 IPv6 Security Agent 無法連線到伺服器。如果純 IPv4 用戶端連線到由其 IPv6 位址所識別的伺服器，則會發生相同的問題。
- 如果伺服器將只會管理 IPv6 用戶端，則最低需求為一個 IPv6 位址。伺服器可由其主機名稱或 IPv6 位址加以識別。當伺服器由其主機名稱所識別時，會偏好使用其「完整合格的網域名稱 (FQDN)」。這是因為在純 IPv6 環境中，WINS 伺服器無法將主機名稱轉換為其對應的 IPv6 位址。

注意

只有在執行伺服器的本機安裝時，才能指定 FQDN。遠端安裝不支援這項作業。

單純 IPv6 伺服器的限制

下表列出 Apex One 伺服器僅具有 IPv6 位址時所存在的限制。

表 A-1. 單純 IPv6 伺服器的限制

項目	限制
用戶端管理	純 IPv6 伺服器無法執行以下操作： • 將 Security Agent 部署到純 IPv4 端點。 • 管理純 IPv4 Security Agent。
更新和集中式管理	純 IPv6 伺服器無法從純 IPv4 更新來源更新，例如： • 趨勢科技主動式更新伺服器 • 任何純 IPv4 自訂更新來源
產品註冊、啟動和續約	純 IPv6 伺服器無法連線到趨勢科技線上註冊伺服器註冊產品、取得使用授權和啟動/續約使用授權。
Proxy 連線	純 IPv6 伺服器無法透過純 IPv4 Proxy 伺服器進行連線。
嵌入程式解決方案	純 IPv6 伺服器會包含 Plug-in Manager，但無法將任何嵌入程式解決方案部署到： • 純 IPv4 Security Agent 或純 IPv4 主機（因為無法直接連線） • 純 IPv6 Security Agent 或純 IPv6 主機（因為嵌入程式解決方案都不支援 IPv6）。

透過設定可在 IPv4 和 IPv6 位址之間進行轉換的雙堆疊 Proxy 伺服器（例如 DeleGate），可以克服上述大部分的限制。將 Proxy 伺服器置於 Apex One 伺服器以及它所連線或服務的實體之間。

純 IPv6 Security Agent 限制

下表列出 Security Agent 僅具有 IPv6 位址時所存在的限制。

表 A-2. 純 IPv6 Security Agent 的限制

項目	限制
上層 Apex One 伺服器	純 IPv4 Apex One 伺服器無法管理純 IPv6 Security Agent。

項目	限制
更新	純 IPv6 Security Agent 無法從純 IPv4 更新來源更新，例如： • 趨勢科技主動式更新伺服器 • 純 IPv4 Apex One 伺服器 • 純 IPv4 更新代理程式 • 任何純 IPv4 自訂更新來源
掃瞄查詢、網頁信譽評等查詢以及 Smart Feedback	純 IPv6 Security Agent 無法傳送查詢到主動雲端截毒技術來源，例如： • 趨勢科技主動雲端截毒技術（也用於 Smart Feedback）
軟體安全	純 IPv6 Security Agent 無法連線到趨勢科技裝載的認證安全防護軟體服務。
嵌入程式解決方案	純 IPv6 Security Agent 無法安裝嵌入程式解決方案，因為所有嵌入程式解決方案都不支援 IPv6。
Proxy 連線	純 IPv6 Security Agent 無法透過純 IPv4 Proxy 伺服器進行連線。

透過設定可在 IPv4 和 IPv6 位址之間進行轉換的雙堆疊 Proxy 伺服器（例如 DeleGate），可以克服上述大部分的限制。將 Proxy 伺服器置於 Security Agent 與它們連線的實體之間。

設定 IPv6 位址

透過 Web 主控台可設定 IPv6 位址或 IPv6 位址範圍。下面是一些組態設定準則。

- Apex One 接受標準的 IPv6 位址表示法。

  例如：

  ```
  2001:0db7:85a3:0000:0000:8a2e:0370:7334
  ```

  ```
  2001:db7:85a3:0:0:8a2e:370:7334
  ```

  ```
  2001:db7:85a3::8a2e:370:7334
  ```

```
::ffff:192.0.2.128
```

- Apex One 也接受連結-本機 IPv6 位址，例如：

```
fe80::210:5aff:feaa:20a2
```

> **警告!**
> 指定連結-本機 IPv6 位址時應謹慎小心，因為即使 Apex One 可以接受這類位址，但它可能在某些情況下無法如預期般運作。例如，如果更新來源位於其他網路區段且可由其連結-本機 IPv6 位址所辨識，Security Agent 就無法從該來源進行更新。

- IPv6 位址是 URL 的一部分時，請使用方括號 ([]) 將位址括起來。
- 對於 IPv6 位址範圍，通常需要輸入字首和字首長度。對於需要伺服器查詢 IP 位址的組態，會套用字首長度限制，以防止伺服器查詢大量 IP 位址時可能出現效能問題。例如，對於外部伺服器管理功能，字首長度只能介於 112（65,536 個 IP 位址）和 128（2 個 IP 位址）之間。
- 涉及 IPv6 位址或位址範圍的某些設定會部署到 Security Agent，但是 Security Agent 會暫不處理這些設定。例如，如果設定了主動雲端截毒技術來源清單，其中包括可由其 IPv6 位址辨識的主動雲端截毒技術伺服器，則純 IPv4 Security Agent 會略過該伺服器並連線到其他主動雲端截毒技術來源。

顯示 IP 位址的畫面

本主題將列舉 Web 主控台中顯示 IP 位址的位置。

位置	說明
用戶端樹狀結構	無論何時顯示用戶端樹狀結構，純 IPv6 Security Agent 的 IPv6 位址都會顯示在「IP 位址」欄下方。對於雙堆疊 Security Agent，如果它們是使用 IPv6 位址向伺服器註冊，則會顯示它們的 IPv6 位址。 **注意** 雙堆疊 Security Agent 向伺服器註冊時使用的 IP 位址，可透過「用戶端 > 全域用戶端設定 > 網路 > 偏好的 IP 位址」進行控制。 將用戶端樹狀結構設定匯出至檔案時，IPv6 位址也會顯示在匯出檔案中。
用戶端狀態	移至「用戶端 > 用戶端管理> 狀態」時，可取得詳細的用戶端資訊。在這個畫面中，會看到純 IPv6 Security Agent 的 IPv6 位址以及使用 IPv6 位址向伺服器註冊的雙堆疊 Security Agent 的 IPv6 位址。
記錄檔	雙堆疊和純 IPv6 Security Agent 的 IPv6 位址會顯示在以下記錄檔中： • 病毒/惡意程式記錄檔 • 間諜程式/可能的資安威脅程式記錄檔 • 防火牆記錄檔 • 連線驗證記錄檔
Apex Central 主控台	下面列出哪些 Apex One 伺服器和 Security Agent 的 IP 位址會顯示在 Apex Central 主控台上。 • 雙堆疊伺服器：IPv4 和 IPv6 • 純 IPv4 伺服器：IPv4 • 純 IPv6 伺服器：IPv6 • 雙堆疊 Security Agent：Security Agent 向 Apex One 伺服器註冊時使用的 IP 位址 • 純 IPv4 Security Agent：IPv4 • 純 IPv6 Security Agent：IPv6

附錄 B

Windows Server Core 支援

本附錄討論 Apex One 對 Windows Server Core 的支援。

Windows Server Core 支援

Windows Server Core 是 Windows Server 版本的「最小」安裝。在 Server Core 中：

- 許多 Windows Server 選項和功能都已移除。
- 伺服器是執行極精簡的核心作業系統。
- 工作大部分都必須從命令列介面執行。
- 作業系統只執行少數服務，而且在啟動期間只需要少量資源。

Apex One 可支援下列 Windows Server Core 版本上安裝的 Security Agent：

- Windows Server Core 2008 R2
- Windows Server Core 2012
- Windows Server Core 2012 R2
- Windows Server Core 2016
- Windows Server Core 2019

Security Agent 支援 Server Core。本節包含有關 Server Core 支援的資訊。

Apex One 伺服器不支援 Server Core。

Windows Server Core 安裝方法

不支援下列安裝方法或只支援部分安裝方法：

- Web 安裝網頁：因為 Server Core 不支援 Web 瀏覽器，所以不支援這種方法。
- Trend Micro Vulnerability Scanner：Vulnerability Scanner 工具無法在 Server Core 本機上執行。請從 Apex One 伺服器或另一個端點執行此工具。

下列是支援的安裝方法：

- 遠端安裝。如需詳細資訊，請參閱從 Apex One Web 主控台遠端安裝 第 5-13 頁。
- Login Script Setup
- 用戶端封裝程式

使用 Login Script Setup 安裝 Security Agent

步驟

1. 在目標端點上，開啟命令提示字元。
2. 輸入下列命令，以對應 Apex One 伺服器上 `AutoPcc.exe` 檔案的位置：

   ```
   net use <對應的磁碟機代號> \\<Apex One 伺服器主機名稱或 IP 位址>\ofcscan
   ```

   例如：

   ```
   net use P:\\10.1.1.1\ofcscan
   ```

3. 提供目標伺服器上的使用者名稱與密碼。

   隨即顯示訊息，通知您 `AutoPcc.exe` 的位置是否對應成功。

4. 輸入對應的磁碟機代號及冒號，以切換至 `AutoPcc.exe` 的位置。例如：

   ```
   P:
   ```

5. 輸入下列命令以啟動安裝：

   ```
   AutoPcc.exe
   ```

   安裝完成後，會出現新的命令提示字元。

使用 Security Agent 套件安裝 Security Agent

步驟

1. 建立套件。

   如需詳細資訊，請參閱以用戶端封裝程式安裝 第 5-17 頁。

2. 開啟命令提示字元。

3. 輸入下列命令以對應 Security Agent 套件的位置：

   ```
   net use <對應的磁碟機代號> \\<用戶端套件的位置>
   ```

   例如：

   ```
   net use P: \\10.1.1.1\Package
   ```

   隨即顯示訊息，通知您 Security Agent 套件的位置是否對應成功。

4. 輸入對應的磁碟機代號及冒號，以切換至 Security Agent 套件的位置。例如：

   ```
   P:
   ```

5. 輸入下列命令，將 Security Agent 套件複製到 Server Core 端點上的本機目錄：

   ```
   copy <套件檔案名稱> <您要將套件複製到的 Server Core 端點上的目錄>
   ```

   例如：

   ```
   複製 securityagent.msi C:\Agent Package
   ```

   隨即顯示訊息，通知您 Security Agent 套件是否複製成功。

6. 切換至本機目錄。例如：

   ```
   C:
   ```

   ```
   cd C:\Agent Package
   ```

7. 輸入套件檔案名稱以啟動安裝。例如：

`securityagent.msi`

下列內容顯示範例中命令提示字元的命令和結果。

```
C:\WINDOWS>net use P: \\10.1.1.1\Package
C:\Windows>P:
P:\>copy securityagent.msi C:\Agent Package
        1 file(s) copied.
P:\>C:
C:\WINDOWS>cd C:\Agent Package
C:\Agent Package>securityagent.msi
```

Windows Server Core 上的 Security Agent 功能

在受支援的 Windows Server 版本上可用的大部分 Security Agent 功能在 Server Core 上都可用。唯一不支援的功能是「單機模式」。

如需 Windows Server 上可用功能的清單，請參閱 Security Agent 功能 第 5-3 頁。

您只能從命令列介面存取 Security Agent 主控台。

注意

有些 Security Agent 主控台畫面會包括「說明」按鈕，只要請點選這個按鈕，即可開啟以 HTML 為架構的即時線上說明。由於 Windows Server Core 沒有瀏覽器，因此這個說明無法供使用者使用。如果要查看「說明」，使用者必須安裝瀏覽器。

Windows Server Core 命令

從命令列介面發出命令來執行 Security Agent 工作。

如果要執行命令，請移至 PccNTMon.exe 所在位置。此處理程序負責啟動 Security Agent 主控台。此程序位於 <用戶端安裝資料夾> 下。

下表列出可用命令。

表 B-1. Windows Server Core 命令

命令	處理行動
pccnt <磁碟機或資料夾路徑>	掃瞄指定的磁碟機或資料夾是否有安全威脅 指導方針： • 如果資料夾路徑包含空格，請以引號括住整個路徑。 • 不支援掃瞄個別檔案。 正確的命令： • pccnt C:\ • pccnt D:\Files • pccnt "C:\Documents and Settings" 不正確的命令： • pccnt C:\Documents and Settings • pccnt D:\Files\example.doc
pccntmon -r	開啟「即時監控」
pccntmon -v	列出用戶端元件及其版本
pccntmon -u	更新 Security Agent 元件
pccntmon -n <unload_password>	結束 Security Agent 如果要重新載入 Security Agent，請輸入下列命令： pccntmon
pccntmon -m <uninstall_password>	解除安裝 Security Agent

命令	處理行動

pccntmon -c	在命令列中顯示下列資訊：
	• 掃瞄方法
	  • 雲端截毒掃瞄
	  • 標準掃瞄
	• 病毒碼狀態
	  • 已更新
	  • 已過期
	• 即時掃瞄服務
	  • 正常運作
	  • 已關閉或未正常運作
	• 用戶端連線狀態
	  • 線上
	  • 單機
	  • 離線
	• 網頁信譽評等服務
	  • 可用
	  • 正在重新連線
	• 檔案信譽評等服務
	  • 可用
	  • 正在重新連線

pccntmon -h	顯示所有可用的命令

附錄 C

Apex One 還原

本附錄討論 Apex One 伺服器和用戶端還原支援。

使用伺服器備份套件還原 Apex One 伺服器和 Security Agent

Apex One 還原程序需要先還原 Security Agent，然後再還原 Apex One 伺服器。

重要

- 管理員必須已於安裝程序期間選擇備份伺服器，才能使用下列程序還原 Apex One 伺服器和用戶端。如果沒有伺服器備份檔案可供使用，請參閱先前安裝的 OfficeScan 版本之《安裝和升級手冊》，瞭解手動還原程序。
- 此版本的 Apex One 僅支援還原到下列 OfficeScan 版本：
  - OfficeScan XG Service Pack 1
  - OfficeScan XG
  - OfficeScan 11.0 Service Pack 1（含重要修補程式）
  - OfficeScan 11.0 Service Pack 1
  - OfficeScan 11.0

還原 Security Agent

Apex One 僅可將 Security Agent 還原成與所恢復伺服器相同的版本。您無法將 Security Agent 還原成比伺服器更舊的版本。

重要

請務必先還原 Security Agent，再還原 Apex One 伺服器。

步驟

1. 確定 Security Agent 無法升級用戶端。

a. 在 Apex One Web 主控台上，移至「用戶端 > 用戶端管理」。

b. 選取要還原的 Security Agent。

c. 按一下「設定 > 權限和其他設定 > 其他設定」標籤。

d. 在「Security Agent 僅會更新下列元件」下拉式清單中，選取「病毒碼檔案、引擎、驅動程式」。

2. 在 Apex One Web 主控台上，移至「更新 > 用戶端 > 更新來源」。

3. 選取「自訂更新來源」。

4. 在「自訂更新來源清單」上，請點選「新增」。

   接著會開啟一個新畫面。

5. 輸入將要還原之 Security Agent 的 IP 位址。

6. 輸入更新來源 URL。

   例如，輸入：

   ```
   http://<Apex One 伺服器的 IP 位址>:<通訊埠>/officescan/download/Rollback
   ```

7. 請點選「儲存」。

8. 請點選「通知所有用戶端」。

   當要還原的 Security Agent 從更新來源進行更新時，會先解除安裝 Security Agent，然後再安裝舊版的 Security Agent。

秘訣

管理員可以在 Security Agent 上開始手動更新，來加速還原程序。如需詳細資訊，請參閱手動更新 Security Agent 第 6-40 頁。

9. 安裝舊版 Security Agent 之後，請通知使用者重新啟動端點。

   還原程序完成後，Security Agent 會繼續向同一部 Apex One 伺服器回報。

注意

還原 Security Agent 後，包括「病毒碼」在內的所有元件也會一併還原為舊版。如果管理員不還原 Apex One 伺服器，已還原的 Security Agent 將無法更新元件。管理員必須將已還原 Security Agent 的更新來源變更為標準更新來源，才能接收進一步的元件更新。

還原舊版 OfficeScan 伺服器

Apex One 或 OfficeScan 伺服器的還原程序需要管理員解除安裝最新的 Apex One 伺服器、重新安裝舊版伺服器、手動停止 Windows 服務、更新系統登錄，然後取代 Apex One 安裝目錄中的 Apex One 伺服器檔案。

重要

在還原 OfficeScan 伺服器之前，務必先還原 Security Agent。

步驟

1. 解除安裝 Apex One 伺服器。
2. 移除以下登錄機碼：

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows
   \CurrentVersion\Uninstall\InstallShield Uninstall
   Information\OfficeScan Management Console-<伺服器主機名稱或 IP
   位址>
   ```

3. 安裝舊版 OfficeScan 伺服器。

秘訣

趨勢科技建議不要在恢復伺服器時變更主機名稱或 IP 位址。

如果要確認舊版伺服器，請移至 <伺服器安裝資料夾>，然後檢視在 Apex One 伺服器安裝期間所建立的還原資料夾。資料夾名稱（稱為 <Restore_folder_version>）可能為下列其中一個：

- OSCEXG_SP1：OfficeScan XG Service Pack 1
- OSCEXG：OfficeScan XG
- OSCE11_SP1:OfficeScan 11.0 Service Pack 1
- OSCE11:OfficeScan 11.0

4. 在 OfficeScan 伺服器電腦上，停止下列服務：
   - Intrusion Defense Firewall（若有安裝）
   - Trend Micro Local Web Classification Server
   - Trend Micro Smart Scan Server
   - OfficeScan Active Directory Integration Service
   - OfficeScan Control Manager Agent
   - OfficeScan Plug-in Manager
   - OfficeScan Master Service
   - World Wide Web Publishing 服務
5. 將 `<Server_installation_folder>\<Restore_folder_version>\` 目錄中的所有檔案和目錄複製到 `<Server_installation_folder>\PCCSRV\` 目錄中來取代其中的檔案與目錄。
6. 恢復 OfficeScan 登錄。
   a. 開啟「登錄編輯程式」(`regedit.exe`)。
   b. 在左瀏覽窗格中，選取下列其中一個登錄機碼：
      - 32 位元系統：`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service`

- 64 位元系統：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\Officescan\service

c. 移至「檔案 > 匯入...」。

d. 選取位於 <Server_installation_folder>\<Restore_folder_version>\ 目錄中的一般 OfficeScan 伺服器 .reg 檔案。

登錄檔名稱必須遵循以下格式：

RegBak_<Restore_folder_version>.reg

e. 按一下「是」，還原所有舊版 OfficeScan 機碼。

7. 視需要還原預約資料庫備份。

a. 開啟「登錄編輯程式」(regedit.exe)。

b. 在左瀏覽窗格中，選取下列其中一個登錄機碼：

- 32 位元系統：HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Database Backup
- 64 位元系統：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\Database Backup

c. 移至「檔案 > 匯入...」。

d. 選取位於 <Server_installation_folder>\<Restore_folder_version>\ 目錄中的資料庫 .reg 檔案。

登錄檔名稱必須遵循以下格式：

RegBak_DBBak_<Restore_folder_version>.reg

e. 按一下「是」，還原所有舊版 OfficeScan 機碼。

8. 開啟命令列編輯器 (cmd.exe)，然後輸入下列命令來重設本地網頁分類伺服器效能計數器：

```
cd <伺服器安裝資料夾>\PCCSRV\LWCS

regsvr32.exe /u /s perfLWCSPerfMonMgr.dll
```

```
regsvr32.exe /s perfLWCSPerfMonMgr.dll
```

9. 重新啟動下列服務：
   - Intrusion Defense Firewall（若有安裝）
   - Trend Micro Local Web Classification Server
   - Trend Micro Smart Scan Server
   - OfficeScan Active Directory Integration Service
   - OfficeScan Control Manager Agent
   - OfficeScan Plug-in Manager
   - OfficeScan Master Service
   - Apache 2（如果使用 Apache Web 伺服器）
   - World Wide Web Publishing 服務（如果使用 IIS Web 伺服器）
10. 手動清除 Internet Explorer 快取並移除 ActiveX 控制項。如需在 Internet Explorer 9 中移除 ActiveX 控制項的詳細資訊，請參閱 http://windows.microsoft.com/en-us/internet-explorer/manage-add-ons#ie=ie-9。

    已恢復舊版 OfficeScan 伺服器設定。

    秘訣

    管理員可以在「關於」畫面（「說明 > 關於」）上檢查 OfficeScan 版本號碼，來確認是否成功還原。

11. 視需要使用 Web 主控台向 Apex Central/Control Manager 伺服器註冊 OfficeScan 伺服器。
12. 確認 OfficeScan 成功還原後，刪除 `<Server_installation_folder>\<Restore_folder_version>\` 目錄中的所有檔案。

附錄 D

詞彙

本詞彙所含術語提供關於一般參考用端點用詞以及趨勢科技產品和技術的進一步資訊。

主動式更新

「主動式更新」是許多趨勢科技產品的通用功能。只要連線到趨勢科技更新網站，您就能透過 Internet 使用「主動式更新」下載最新的病毒碼檔案、掃瞄引擎、程式和其他趨勢科技元件檔案。

Compressed File（壓縮檔）

單一的檔案，其中包含一或多個個別檔案和資訊，可由適當的程式進行解壓縮（例如：WinZip）。

Cookie

這是一種用於儲存 Internet 使用者相關資訊（例如：名稱、偏好設定和喜好）的機制，Web 瀏覽器會儲存 Cookie 供後續使用。當您下次存取您的瀏覽器擁有其 Cookie 的網站時，瀏覽器會將 Cookie 傳送至 Web 伺服器，Web 伺服器便會使用 Cookie 中的資訊為您呈現自訂的網頁。例如，當您進入網站時，歡迎頁面上可能會顯示您的名稱。

Denial of Service Attack（拒絕服務攻擊）

「拒絕服務」(DoS) 攻擊是指對端點或網路發動可導致「服務」（即網路連線）中斷的攻擊。DoS 攻擊通常會佔用大量網路頻寬，或是使系統資源（如端點的記憶體）超載。

DHCP

「動態主機控制通訊協定」(DHCP) 是一種可將動態 IP 位址指定給網路裝置的通訊協定。透過動態定址，裝置每次連線到網路時都會有不同的 IP 位址。在

某些系統中，裝置的 IP 位址甚至可以在連線狀態下變更。DHCP 也支援混合使用靜態與動態 IP 位址。

DNS

「網域名稱系統」(DNS) 是一種通用的資料查詢服務，主要用於將 Internet 中的主機名稱轉譯為 IP 位址。

DNS 用戶端向 DNS 伺服器要求主機名稱與位址資料的程序，稱之為解析。使用基本 DNS 設定時，伺服器會執行預設解析。例如，假設有遠端伺服器向其他伺服器查詢目前區域中某部機器的資料。遠端伺服器中的用戶端軟體會查詢解析程式，而解析程式會透過其資料庫檔案回覆要求。

網域名稱

系統完整名稱包含本機主機名稱和網域名稱，例如：`tellsitall.com`。網域名稱必須足以判斷 Internet 上任何主機的唯一 Internet 位址。此程序（稱為「名稱解析」）使用「網域名稱系統」(DNS)。

Dynamic IP Address（動態 IP 位址）

動態 IP 位址是指 DHCP 伺服器指定的 IP 位址。端點的 MAC 位址將維持不變，不過 DHCP 伺服器會根據可用性指定新的 IP 位址給端點。

ESMTP

「加強版簡易郵件傳輸通訊協定」(ESMTP) 包含安全性、驗證與其他裝置，可節省頻寬並保護伺服器。

End User License Agreement（使用者授權合約）

「使用者授權合約」也稱為 EULA，是軟體發行者和軟體使用者之間的合法契約。通常會簡述對使用者的限制，如果使用者要拒絕合約，安裝時不要按「我接受」。當然，請點選「我不接受」將會結束軟體產品的安裝。

許多使用者會在安裝某些免費軟體時顯示的 EULA 上請點選「我接受」，而不小心就同意在其電腦上安裝間諜軟體和其他類型的可能的資安威脅程式。

False Positive（誤判）

安全軟體若將某個檔案錯誤偵測為中毒，就是誤判。

FTP

「檔案傳輸通訊協定」(FTP) 是一種標準通訊協定，用於透過 Internet 將檔案從伺服器傳輸到用戶端。如需詳細資訊，請參閱「網路工作群組 RFC 959」。

GeneriClean

GeneriClean（也就是所謂的參考清除）是一種即使沒有病毒清除元件也能夠清除病毒/惡意程式的新技術。GeneriClean 可使用偵測到的檔案為基礎，來確定偵測到的檔案是否在記憶體中有對應的程序/服務和登錄項目，然後一併刪除它們。

Hot Fix

Hotfix 是針對單一客戶回報的問題的因應措施或解決方案。HotFix 是針對特定問題，所以不會對所有客戶發行。Windows HotFix 包括安裝程式，而非 Windows HotFix 則不包括（通常您需要停止程式精靈、複製檔案以覆寫安裝中的對應檔案，然後重新啟動精靈）。

依預設，Security Agent 可安裝 HotFix。如果不想 Security Agent 安裝 HotFix，可移至「用戶端 > 用戶端管理」，然後請點選「設定 > 權限和其他設定 > 其他設定」標籤，在 Web 主控台中變更用戶端更新設定。

如果無法在 Apex One 伺服器上部署 HotFix，請使用 Touch Tool 變更 HotFix 的時間戳記。這會讓 Apex One 將這個 HotFix 解譯為新的 HotFix，使伺服器自動再次嘗試部署這個 HotFix。如需此工具的詳細資訊，請參閱執行用於 Security Agent Hotfix 的 Touch Tool 第 6-48 頁。

HTTP

「超文字傳輸通訊協定」(HTTP) 是標準的通訊協定，用於透過 Internet 將網頁（包括圖片和多媒體內容）從伺服器傳輸至用戶端。

HTTPS

使用安全套接字層 (SSL) 的超文件傳輸通訊協定。HTTPS 是由 HTTP 演變而來的安全版 HTTP，用於處理安全交易。

ICMP

有時候，閘道或目的主機會使用「Internet 控制訊息通訊協定」(ICMP) 與來源主機進行通訊（例如，為了回報處理資料包時發生的錯誤）。ICMP 會使用基本的 IP 支援做為較高階的通訊協定，不過 ICMP 實際上是整合的 IP 通訊埠，

並且由每個 IP 模組實作。ICMP 訊息會在數種情況下傳送：例如，資料包無法到達目的地時、閘道沒有轉送資料包的緩衝容量時，以及閘道可以指示主機以較短的路由進行傳輸時。「網際網路通訊協定」的設計並非絕對可靠。這些控制訊息的目的在於提供通訊環境中相關問題的意見反應，而非讓 IP 變得可靠。

智慧型掃瞄

「智慧型掃瞄」是識別要掃瞄之檔案的方法。對於執行檔（例如：.exe），真實的檔案類型取決於檔案內容。針對非執行檔（例如 .txt），則根據檔案標頭判斷真實檔案型態。

使用「智慧型掃瞄」具有以下優點：

- 效能最佳化：由於智慧型掃瞄使用最少的系統資源，所以不會影響用戶端上的應用程式。
- 縮短掃瞄時間：由於「智慧型掃瞄」採用真實檔案型態辨識，只掃瞄容易受到感染的檔案，因此會比掃瞄所有檔案所花的掃瞄時間少很多。

IntelliTrap

病毒撰寫者通常會使用即時壓縮演算法騙過病毒過濾機制。IntelliTrap 透過封鎖即時壓縮可執行檔並將其與其他惡意程式特徵比對，以降低這類病毒進入網路的風險。由於 IntelliTrap 會將這類檔案識別為安全威脅，而且可能會錯誤地封鎖安全的檔案，因此建議您在啟動 IntelliTrap 後隔離（不刪除或清除）檔案。如果使用者定期交換即時壓縮可執行檔，請關閉 IntelliTrap。

IntelliTrap 使用下列元件：

- 病毒掃瞄引擎
- IntelliTrap 病毒碼
- IntelliTrap 例外病毒碼

IP

「網際網路通訊協定 (IP) 可將資料區塊（稱為資料包）從來源傳輸至目的地，而來源和目的地都是以固定長度位址來識別的主機。」(RFC 791)

Java File（Java 檔案）

Java 是由 Sun Microsystems 所開發的通用程式設計語言。Java 檔案中包含 Java 程式碼。Java 提供適用於多種平台的 Java Applet 格式，支援 Internet 的程式設計。Applet 是一種以 Java 程式設計語言撰寫的程式，可納入 HTML 頁面中。當您使用支援 Java 技術的瀏覽器來檢視包含 Applet 的頁面時，Applet 會將其程式碼轉移至您的端點，讓瀏覽器的 Java 虛擬機器執行 Applet。

LDAP

「輕量型目錄存取通訊協定」(LDAP) 是一種應用程式通訊協定，用於查詢及修改透過 TCP/IP 執行的目錄服務。

Listening Port（監聽通訊埠）

監聽通訊埠可用於處理用戶端連線要求，以便進行資料交換。

MCP Agent（MCP 用戶端）

趨勢科技「管理通訊協定」(MCP) 是趨勢科技推出的新一代受管理產品的用戶端。MCP 取代了 Trend Micro Management Infrastructure (TMI)，成為 Apex Central 與 Apex One 進行通訊的方式。MCP 擁有數項新功能：

- 減少網路負載和套件大小
- 支援 NAT 和防火牆穿透
- 支援 HTTPS
- 單向和雙向通訊支援
- 支援單一登入 (SSO)
- 叢集節點支援

Mixed Threat Attack（混合式安全威脅攻擊）

混合式安全威脅攻擊會利用企業網路中的多個進入點與弱點，如「Nimda」或「Code Red」安全威脅。

NAT

「網路位址轉譯」(Network Address Translation) 是將安全 IP 位址從位址集區轉譯至暫時、外部、已登錄 IP 位址的標準。這會讓具有私人指定之 IP 位址的信任網路取得 Internet 的存取權。這也表示您無須針對網路中的每部機器取得已登錄的 IP 位址。

NetBIOS

「網路基本輸入輸出系統」(NetBIOS) 是一種應用程式介面 (API)，可將網路功能之類的功能新增至磁碟作業系統 (DOS) 的基本輸入/輸出系統 (BIOS)。

One-way Communication（單向通訊）

NAT 穿透在現實網路環境中成為越來越嚴重的問題。為了解決這個問題，MCP 使用單向通訊。單向通訊讓 MCP 用戶端可開始與伺服器的連線，且可從伺服器輪詢命令。每個要求都是 CGI 類命令查詢或記錄檔傳輸。為了減少對網路的影響，MCP 用戶端會盡量將連線保持在可用和開啟狀態。後續要求則會使用現有開啟中的連線。如果連線中斷，所有與相同主機間的 SSL 連線就能從作業階段 ID 快取記憶體中獲益，因為此快取記憶體可大幅縮短重新連線的時間。

修補程式

修補程式是一組 Hot Fix 和安全修補程式，可解決多種程式問題。趨勢科技會定期提供修補程式。Windows Patch 包括安裝程式，而非 Windows Patch 一般則有安裝程式檔。

Phish Attack（網路釣魚攻擊）

網路釣魚是一種快速發展的欺詐形式，藉由模仿合法網站來詐騙網路使用者洩漏私人資訊。

通常，未起疑心的使用者會收到乍似緊急 (且看似真實) 的電子郵件，告訴他們帳號有問題，必須立即修正才能避免帳號停用。電子郵件中會包括某個網站的 URL，看起來就和真的一模一樣（要複製合法電子郵件和合法網站很簡單），然後會變更所謂的後端，也就是指已收集資料的接收者。

電子郵件會告訴使用者要登入該網站，並且確認某些帳號資訊。駭客會收到使用者提供的資料（例如：登入名稱、密碼、信用卡號或身分證字號）。

網路釣魚的欺詐方式速度快、廉價，而且易於久存。對於施展這種方式的罪犯而言，同樣也十分有利可圖。網路釣魚就連電腦高手也很難偵測，而且執法單位也難以追蹤。更糟的是，幾乎不可能判刑。

如果您發現任何疑似釣魚網站的網站，請回報給趨勢科技。

Ping

Ping 是一種將 ICMP Echo 要求傳送至 IP 位址並等候回應的公用程式。Ping 公用程式可以判斷使用指定 IP 位址的端點是否為線上狀態。

POP3

「郵件通訊協定 3」(POP3) 是一種標準通訊協定，用於儲存電子郵件訊息以及將其從伺服器傳輸至用戶端電子郵件應用程式。

Proxy 伺服器

Proxy 伺服器是一種可接受具有特殊字首之 URL 的 World Wide Web 伺服器，用來從本機快取或遠端伺服器提取文件，然後將 URL 傳回給要求端。

RPC

「遠端程序呼叫」(RPC) 是一種網路通訊協定，可讓執行於某部主機上的程式在另一部主機上執行程式碼。

安全修補程式

安全修補程式著重於安全問題，適合對所有客戶進行部署。Windows 安全修補程式包括安裝程式，而非 Windows Patch 一般則有安裝程式檔。

Service Pack

Service Pack 是重要到足以成為產品升級的 HotFix、Patch 和功能加強的合併整合。Windows 和非 Windows Service Pack 都包括安裝程式和安裝程序檔。

SMTP

「簡易郵件傳輸通訊協定」(SMTP) 是一種標準通訊協定，用於透過 Internet 在不同的伺服器之間傳送電子郵件訊息，或是將電子郵件訊息從用戶端傳送至伺服器。

SNMP

「簡易網路管理通訊協定」(SNMP) 是一種通訊協定，可支援監控連接到網路的裝置上應得到管理注意的狀況。

SNMP Trap

SNMP Trap 是一種將通知傳送給使用管理主控台（支援這種通訊協定）的網路管理員的方式。

Apex One 可以將通知儲存在 Management Information Bases (MIB) 中。您可以使用 MIB 瀏覽器來檢視 SNMP Trap 通知。

SSL

Secure Socket Layer (SSL) 由 Netscape 所設計的通訊協定，可提供應用程式通訊協定（如 HTTP、Telnet 或 FTP）與 TCP/IP 之間的分層資料安全性。此安

全通訊協定可為 TCP/IP 連線提供資料加密、伺服器驗證、訊息完整性與選用的用戶端驗證。

SSL Certificate（SSL 憑證）

此數位憑證可建立安全的 HTTPS 通訊。

TCP

「傳輸控制通訊協定」(TCP) 是一種連線導向、端對端的可靠通訊協定，用於配合支援多個網路應用程式的分層通訊協定階層架構。TCP 會依賴 IP 資料包來完成位址解析。如需詳細資訊，請參閱 DARPA Internet Program RFC 793。

Telnet

Telnet 是藉由建立「網路虛擬終端機」，而在 TCP 上聯繫終端機裝置的標準方法。如需詳細資訊，請參閱「網路工作群組 RFC 854」。

Trojan Port（特洛伊木馬程式通訊埠）

特洛伊木馬程式通訊埠通常是特洛伊木馬程式連線到端點所使用的通訊埠。在病毒爆發期間，Apex One 會封鎖下列可能遭特洛伊木馬程式利用的通訊埠號碼。

表 D-1. 特洛伊木馬程式通訊埠

通訊埠號碼	特洛伊木馬程式	通訊埠號碼	特洛伊木馬程式
23432	Asylum	31338	Net Spy

通訊埠號碼	特洛伊木馬程式	通訊埠號碼	特洛伊木馬程式
31337	Back Orifice	31339	Net Spy
18006	Back Orifice 2000	139	Nuker
12349	Bionet	44444	Prosiak
6667	Bionet	8012	Ptakks
80	Codered	7597	Qaz
21	DarkFTP	4000	RA
3150	Deep Throat	666	Ripper
2140	Deep Throat	1026	RSM
10048	Delf	64666	RSM
23	EliteWrap	22222	Rux
6969	GateCrash	11000	Senna Spy
7626	Gdoor	113	Shiver
10100	Gift	1001	Silencer
21544	Girl Friend	3131	SubSari
7777	GodMsg	1243	Sub Seven
6267	GW Girl	6711	Sub Seven
25	Jesrto	6776	Sub Seven
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	Net Bus	12345	Valvo line
7300	Net Spy	1234	Valvo line

Trusted Port（信任的通訊埠）

伺服器和 Security Agent 使用信任的通訊埠與彼此通訊。

如果您在病毒爆發後封鎖信任的通訊埠，然後將網路設定恢復正常，Security Agent 將不會立即繼續與伺服器通訊。只有在到達您在「病毒爆發防範設定」畫面中指定的小時數後，才會恢復用戶端與伺服器之間的通訊。

Apex One 會使用 HTTP 通訊埠（預設為 8080）做為伺服器上信任的通訊埠。在安裝期間，您可以輸入其他通訊埠號碼。如果要封鎖這個信任的通訊埠和 Security Agent 上信任的通訊埠，請選取「封鎖通訊埠」畫面上的「封鎖信任的通訊埠」核取方塊。

主安裝程式會在安裝期間隨機產生 Security Agent 信任的通訊埠。

判斷信任的通訊埠

步驟

1. 存取 <伺服器安裝資料夾>\PCCSRV。
2. 使用記事本等文字編輯器開啟 ofcscan.ini 檔案。
3. 如果是伺服器信任的通訊埠，請搜尋字串 "Master_DomainPort"，然後查看其值。

   例如，如果字串顯示為 Master_DomainPort=80，這表示伺服器上信任的通訊埠為第 80 號通訊埠。
4. 如果是用戶端信任的通訊埠，請搜尋字串 "Client_LocalServer_Port"，然後查看其值。

   例如，如果字串顯示為 Client_LocalServer_Port=41375，這表示用戶端上信任的通訊埠為第 41375 號通訊埠。

Two-way Communication（雙向通訊）

雙向通訊是單向通訊的替代方案。雙向通訊是以單向通訊為基礎，但還多了接收伺服器通知的 HTTP-based 通道，可改善 MCP 用戶端即時傳遞和處理來自伺服器的命令。

UDP

「使用者資料包通訊協定」(UDP) 是搭配 IP 使用的無連線通訊協定，可讓應用程式傳送訊息至其他程式。如需詳細資訊，請參閱 DARPA Internet Program RFC 768。

無法清除病毒的檔案

「病毒掃瞄引擎」無法清除下列檔案：

表 D-2. 無法清除的檔案解決方案

無法清除的檔案	說明和解決方案
感染特洛伊木馬程式的檔案	特洛伊木馬程式是一種會執行無法預期或未經授權（惡意）動作的程式，例如：顯示訊息、刪除檔案、或將磁碟格式化。特洛伊木馬程式不會感染檔案，因此不需要清除。 解決方案：「損害清除及復原引擎」和「損害清除及復原範本」會移除特洛伊木馬程式。
感染蠕蟲的檔案	蠕蟲是一種自含程式（或一組程式集），可將本身的功能或程式碼的一部分散佈到其他端點系統。這種病毒通常透過網路連線或電子郵件的附件散播。由於蠕蟲是自含程式，因此無法清除。 解決方案：趨勢科技建議您刪除蠕蟲。
防寫的中毒檔案	解決方案：移除防寫，以允許清除檔案。
密碼保護的檔案	受密碼保護的檔案，包括受密碼保護的壓縮檔或受密碼保護的 Microsoft Office 檔案。

無法清除的檔案	說明和解決方案
	解決方案：移除密碼保護，以允許清除檔案。
備份檔案	副檔名為 RB0~RB9 的檔案是中毒檔案的備份副本。清除程序會建立中毒檔案的備份，以防病毒/惡意程式在清除期間損害檔案。 解決方案：如果成功清除中毒檔案，您便不需要保留其備份複本。如果端點運作正常，就可以將備份檔案刪除。
資源回收筒內的中毒檔案	因為系統正在執行，所以系統可能不允許移除「資源回收筒」內的中毒檔案。
	1. 以管理員權限登入端點。 2. 關閉所有執行中的應用程式，防止應用程式鎖定檔案而使 Windows 無法刪除該檔案。 3. 開啟命令提示字元。 4. 輸入下列指令以刪除檔案： `del /s \$Recycle.Bin\*` 5. 檢查檔案是否已移除。
Windows Temp 資料夾或 Internet Explorer 暫存資料夾內的中毒檔案	因為端點會使用 Windows Temp 資料夾或 Internet Explorer 暫存資料夾中的中毒檔案，所以系統不允許清除這些檔案。要清除的檔案可能是 Windows 作業所需的暫存檔。
	1. 以管理員權限登入端點。 2. 關閉所有執行中的應用程式，防止應用程式鎖定檔案而使 Windows 無法刪除該檔案。 3. 如果中毒檔案位於 Windows Temp 資料夾中： a. 開啟命令提示字元。 b. 輸入下列指令以刪除檔案： `del /s \Windows\Temp\*` c. 在標準模式下重新啟動端點。 4. 如果中毒檔案位於 Internet Explorer 暫存資料夾中： a. 開啟命令提示字元並移至 Internet Explorer Temp 資料夾。

無法清除的檔案	說明和解決方案
	• Windows 7：`%LocalAppData%\Microsoft\Windows\Temporary Internet Files` • Windows 8/8.1：`%LocalAppData%\Microsoft\Windows\INetCache` • Windows 10：`%LocalAppData%\Microsoft\Windows\INetCache\IE` b. 輸入下列指令以刪除檔案： `del /s .\*` 最後一個指令會刪除 Internet Explorer 暫存資料夾中所有的檔案。 c. 在標準模式下重新啟動端點。
使用不支援的壓縮格式壓縮的檔案。	解決方案：解壓縮檔案。
鎖住的檔案，或是目前正在執行的檔案。	解決方案：解除鎖定檔案或等候檔案執行完畢。
毀損的檔案。	解決方案：刪除檔案。

感染特洛伊木馬程式的檔案

特洛伊木馬程式是一種會執行無法預期或未經授權（通常為惡意性質）動作（例如：顯示訊息、刪除檔案、或將磁碟格式化）的程式。特洛伊木馬程式不會感染檔案，因此沒有必要清除。

解決方案：Security Agent 會使用「損害清除及復原引擎」和「損害清除及復原範本」移除特洛伊木馬程式。

感染蠕蟲的檔案

蠕蟲是一種自含程式（或程式集），可以將本身具有功能性的複製體或其片段散佈到其他端點系統。這種病毒通常透過網路連線或電子郵件的附件散播。因為檔案屬於自含程式，所以無法清除蠕蟲。

解決方案：趨勢科技建議刪除蠕蟲。

防寫的中毒檔案

解決方案：移除防寫，讓 Security Agent 清除檔案。

受密碼保護的檔案

包括受密碼保護的壓縮檔或受密碼保護的 Microsoft Office 檔案。

解決方案：移除密碼安全防護，以允許 Security Agent 清除這些檔案。

備份檔案

副檔名為 RB0~RB9 的檔案是中毒檔案的備份副本。Security Agent 會建立中毒檔案的備份，以防病毒/惡意程式在清除期間損害檔案。

解決方案：如果 Security Agent 成功清除中毒檔案，您便不需要保留備份複本。如果端點運作正常，就可以將備份檔案刪除。

索引

八畫

趨勢科技股份有限公司
台北市敦化南路二段 198 號 8 樓
電話：(886) 2-23789666　傳真：(886) 2-23780993
Web mail: http://www.trend.com.tw/corpmail/

www.trendmicro.com
Item Code: APTM09289/210618