Trend Micro Apex One™ as a Service

管理手冊

企業資訊安全整體防護

文件編號：APTM09513/220328

發行日期：2022 年 4 月

受美國專利保護，專利編號： 5,951,698

本文件介紹了服務的主要功能，並/或提供作業環境的安裝說明。在安裝或使用服務前，請先閱讀此文件。

如需有關如何使用服務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

目錄

序言

序言 v

Apex One 文件 vi

讀者 vi

文件慣例 vii

詞彙 vii

部分 I：Apex One as a Service 簡介

第 1 章：Apex One as a Service 簡介

Trend Micro Apex One as a Service 1-2

功能和優點 1-2

趨勢科技主動雲端截毒技術 1-4

Web 主控台 1-7

部分 II：Security Agent 管理

第 2 章：Security Agent 安裝

Security Agent 系統需求 2-2

用戶端封裝工具 2-25

Security Agent 服務 2-25

Security Agent 解除安裝 2-30

第 3 章：用戶端樹狀結構管理

Apex One 用戶端樹狀結構 3-2

「用戶端管理」畫面 3-2
Apex One 網域 3-5

第 4 章：Security Agent 程式設定

Security Agent 的共存和完整功能比較 4-2
Security Agent 圖示 4-5
全域用戶端設定 4-15
端點位置 4-16
參考伺服器 4-17

部分 III：端點防護

第 5 章：惡意程式防護掃瞄

立即掃瞄 5-2
中毒處理行動 5-8
掃瞄例外支援 5-14
恢復隔離的檔案 5-16

第 6 章：Apex One 防火牆

Apex One 防火牆總覽 6-2
啟動或關閉端點上的 Apex One 防火牆 6-3
防火牆策略 6-3
防火牆資料檔 6-10
設定全域防火牆設定 6-13
設定 Security Agent 的防火牆通知 6-14
測試 Apex One 防火牆 6-15

第 7 章：使用病毒爆發防範

病毒爆發防範策略 7-2

設定安全威脅爆發防範 7-7

關閉病毒爆發防範 7-9

部分 IV：監控 Apex One

第 8 章：資訊中心

標籤和 Widget 8-2

摘要標籤 Widget 8-6

資料安全防護 Widget 8-11

Apex One Widget 8-13

管理 Widget 8-17

第 9 章：記錄檔

檢視掃瞄作業記錄檔 9-2

檢視中央隔離區還原記錄檔 9-3

檢視系統事件記錄檔 9-4

第 10 章：通知

Security Agent 通知 10-2

部分 V：更新和管理

第 11 章：更新

設定 Security Agent 的預約更新 11-2

Security Agent 更新來源 11-3

第 12 章：管理設定

帳號管理 12-2

主動式雲端截毒技術 12-3

通知設定 12-6

一般管理設定 12-6

部分 VI：取得說明

第 13 章：技術支援

疑難排解資源 13-2

聯絡趨勢科技 13-3

將可疑內容傳送到趨勢科技 13-4

其他資源 13-5

索引

索引 IN-1

序言

序言

本文件討論開始使用資訊、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 第 vi 頁
- 讀者 第 vi 頁
- 文件慣例 第 vii 頁
- 詞彙 第 vii 頁

Apex One 文件

Apex One 文件包含下列各項：

表 1. Apex One 文件

文件	說明
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	Web-based ASPX 或本機 HTML 檔案，提供「相關指示」、使用建議和特定領域資訊。您可以從 Apex One 伺服器和用戶端主控台存取「說明」。
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： https://esupport.trendmicro.com/zh-tw/default.aspx

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-as-a-service.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
 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
Apex One	這是可為 Apex One 伺服器提供基本架構的趨勢科技端點安全防護解決方案
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
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	包含 Security Agent
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

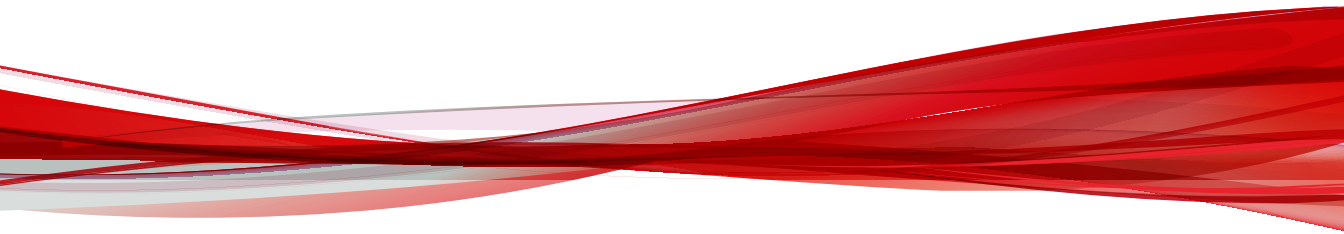
詞彙	說明

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`

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

部分 I

Apex One as a Service 簡介



第 1 章

Apex One™ as a Service 簡介

本章提供 Apex One™ as a Service 的總覽並介紹一些主要功能。

包含下列主題：

- Trend Micro™ Apex One™ as a Service 第 1-2 頁
- 功能和優點 第 1-2 頁
- 趨勢科技™主動雲端截毒技術™ 第 1-4 頁
- Web 主控台 第 1-7 頁

Trend Micro™ Apex One™ as a Service

Trend Micro Apex One as a Service 可在您目前的端點防護解決方案之上和之外提供增強的安全防護，抵禦未知、零時差和 Web-based 安全威脅。

Apex One 是一種整合式的解決方案，它是由常駐於端點的 Security Agent 程式和用於管理所有 Security Agent 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「趨勢科技主動式雲端截毒技術™」，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 Security Agent 可減少對於傳統病毒碼下載的依賴，並降低通常與桌面更新有關的延遲。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。

功能和優點

下表列出 Apex One 提供的主要功能和優點。

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
Machine Learning	「Machine Learning」引擎可透過進階檔案特徵分析與主動程序監控，保護您的網路免受新的、過去未識別或是未知安全威脅的侵襲。「Machine Learning」可判斷安全威脅存在於檔案中的可能性，以及可能的安全威脅類型，保護您免受零時差攻擊。
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。
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。 可將 Apex One 與趨勢科技主動式雲端截毒技術整合，以驗證網站和網頁的可信度

功能	優點
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。
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。
與安全解決方案無關	在「共存」模式下執行的 用戶端於任何支援的 Windows 端點上都相容，可執行任何端點安全防護軟體。
軟體即服務解決方案	由於 Apex One 伺服器是在雲端中代管及進行管理，因此您無需負擔管理本機硬體所需的經常性費用。

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

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。

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。

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

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。

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
- 在一或多個網路端點上設定掃瞄組態設定
- 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

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。

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 1-8 頁。

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。

部分 II

Security Agent 管理

第 2 章

Security Agent 安裝

本章簡述 Security Agent 程式的系統需求、安裝方法及解除安裝程序。

包含下列主題：

- Security Agent 系統需求 第 2-2 頁
- 用戶端封裝工具 第 2-25 頁
- Security Agent 服務 第 2-25 頁
- Security Agent 解除安裝 第 2-30 頁

Security Agent 系統需求

Windows 端點平台

Windows 7（32/64 位元）Service Pack 1 需求

項目	需求
版本 **重要** 需要 Service Pack 1。	• Home Basic • Home Premium • Ultimate • Professional • Enterprise • Professional for Embedded Systems • Ultimate for Embedded Systems • Thin PC
處理器	• 至少 1GHz（32 位元）/2GHz（64 位元）Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）
可用磁碟空間	• 至少 1.5GB • 建議使用 2.0GB **注意** 如果您要在 Security Agent 上啟動 Application Control、Endpoint Sensor、Vulnerability Protection 和資料安全防護，趨勢科技建議您將最低磁碟空間增加至 3.0 GB。

項目	需求
其他	• 支援 1024 x 768 解析度（256 色）或以上的顯示器 • 關閉「簡易檔案共用」 • 允許透過 Windows 防火牆（如果已啟動）進行印表機/檔案共用 • 啟動預設的本機 admin

Windows 8.1（32/64 位元）需求

項目	需求
版本（不需要有 Service Pack）	• Standard • Pro • Enterprise
處理器	• 至少 1GHz（32 位元）/2GHz（64 位元）Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）
可用磁碟空間	• 至少 1.5GB • 建議使用 2.0GB **注意** 如果您要在 Security Agent 上啟動 Application Control、Endpoint Sensor、Vulnerability Protection 和資料安全防護，趨勢科技建議您將最低磁碟空間增加至 3.0 GB。

項目	需求
其他	• 支援 1024 x 768 解析度（256 色）或以上的顯示器 • 允許透過 Windows 防火牆（如果已啟動）進行印表機/檔案共用 • 啟動預設的本機 admin 注意 不支援 Windows UI。

Windows 10（32/64 位元）需求

項目	需求
版本（不需要有 Service Pack）	• Home • Pro • Education • Enterprise
更新支援	• Windows 10 November 2021 Update (Windows 10 21H2) 和更早版本
處理器	• 至少 1GHz（32 位元）/2GHz（64 位元）Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）

項目	需求
可用磁碟空間	• 至少 1.5GB • 建議使用 2.0GB 注意 如果您要在 Security Agent 上啟動 Application Control、Endpoint Sensor、Vulnerability Protection 和資料安全防護，趨勢科技建議您將最低磁碟空間增加至 3.0 GB。
其他	• 支援 1024 x 768 解析度（256 色）或以上的顯示器 • 允許透過 Windows 防火牆（如果已啟動）進行印表機/檔案共用 • 啟動預設的本機 admin 注意 不支援 Windows UI。

Windows 11（64 位元）需求

項目	需求
版本（不需要有 Service Pack）	• Home • Pro • Education • Enterprise
處理器	• 至少 2GHz（64 位元）Intel Pentium 或同級處理器 • AMD™ 64 處理器 • Intel 64 處理器

項目	需求
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）
可用磁碟空間	• 至少 1.5GB • 建議使用 2.0GB 注意 如果您要在 Security Agent 上啟動 Application Control、Endpoint Sensor、Vulnerability Protection 和資料安全防護，趨勢科技建議您將最低磁碟空間增加至 3.0 GB。
其他	• 支援 1024 x 768 解析度（256 色）或以上的顯示器 • 允許透過 Windows 防火牆（如果已啟動）進行印表機/檔案共用 • 啟動預設的本機 admin 注意 不支援 Windows UI。

Windows Server 平台

Windows Server 2008 R2（64 位元）平台

- Windows Server 2008 R2 第 2-7 頁
- Windows Storage Server 2008 R2 第 2-8 頁
- Windows HPC Server 2008 R2 第 2-8 頁

注意

如需特定平台的處理器和 RAM 需求，請參閱該平台的 Microsoft 系統需求。

表 2-1. Windows Server 2008 R2

項目	需求
版本（Service Pack 1）	• Standard • Enterprise • Datacenter • Web • Server Core
處理器	• 至少 1.4GHz 的 Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）
可用磁碟空間	• 至少 1.5GB • 建議使用 2.0GB **注意** 如果您要在 Security Agent 上啟動 Application Control、Endpoint Sensor、Vulnerability Protection 和資料安全防護，趨勢科技建議您將最低磁碟空間增加至 3.0 GB。
其他	• 支援 1024 x 768 解析度（256 色）或以上的顯示器 • 允許透過 Windows 防火牆（如果已啟動）進行印表機/檔案共用 • 啟動預設的本機 admin

表 2-2. Windows Storage Server 2008 R2

項目	需求
版本（Service Pack 1）	• Basic • Standard • Enterprise • Workgroup
處理器	• 至少 1.4GHz 的 Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）
可用磁碟空間	• 至少 1.5GB • 建議使用 2.0GB 注意 如果您要在 Security Agent 上啟動 Application Control、Endpoint Sensor、Vulnerability Protection 和資料安全防護，趨勢科技建議您將最低磁碟空間增加至 3.0 GB。
其他	• 支援 1024 x 768 解析度（256 色）或以上的顯示器 • 允許透過 Windows 防火牆（如果已啟動）進行印表機/檔案共用 • 啟動預設的本機 admin

表 2-3. Windows HPC Server 2008 R2

項目	需求
版本（不需要有 Service Pack）	• 無

項目	需求
處理器	• 至少 1.4GHz 的 Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）
可用磁碟空間	• 至少 1.5GB • 建議使用 2.0GB 注意 如果您要在 Security Agent 上啟動 Application Control、Endpoint Sensor、Vulnerability Protection 和資料安全防護，趨勢科技建議您將最低磁碟空間增加至 3.0 GB。
其他	• 支援 1024 x 768 解析度（256 色）或以上的顯示器 • 允許透過 Windows 防火牆（如果已啟動）進行印表機/檔案共用 • 啟動預設的本機 admin

Windows MultiPoint Server 2010（64 位元）平台

注意

如需特定平台的處理器和 RAM 需求，請參閱該平台的 Microsoft 系統需求。

項目	需求
版本（無需 Service Pack）	• 無

項目	需求
處理器	• 至少 1.4GHz 的 Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）
可用磁碟空間	• 至少 1.5GB • 建議使用 2.0GB 注意 如果您要在 Security Agent 上啟動 Application Control、Endpoint Sensor、Vulnerability Protection 和資料安全防護，趨勢科技建議您將最低磁碟空間增加至 3.0 GB。
其他	• 支援 1024 x 768 解析度（256 色）或以上的顯示器 • 允許透過 Windows 防火牆（如果已啟動）進行印表機/檔案共用 • 啟動預設的本機 admin

Windows MultiPoint Server 2011（64 位元）平台

注意

如需特定平台的處理器和 RAM 需求，請參閱該平台的 Microsoft 系統需求。

項目	需求
版本（無需 Service Pack）	• Standard • Premium

項目	需求
處理器	• 至少 1.4GHz 的 Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）
可用磁碟空間	• 至少 1.5GB • 建議使用 2.0GB 注意 如果您要在 Security Agent 上啟動 Application Control、Endpoint Sensor、Vulnerability Protection 和資料安全防護，趨勢科技建議您將最低磁碟空間增加至 3.0 GB。
其他	• 支援 1024 x 768 解析度（256 色）或以上的顯示器 • 允許透過 Windows 防火牆（如果已啟動）進行印表機/檔案共用 • 啟動預設的本機 admin

Windows Server 2012（64 位元）平台

- 表 2-4：Windows Server 2012 第 2-12 頁
- 表 2-5：Windows Server 2012 R2 第 2-13 頁
- 表 2-6：Windows Storage Server 2012 第 2-14 頁
- 表 2-7：Windows Storage Server 2012 R2 第 2-15 頁
- Windows MultiPoint Server 2012 第 2-16 頁
- Windows Server 2012 容錯移轉叢集 第 2-17 頁

- Windows Server 2012 R2 容錯移轉叢集 第 2-18 頁

注意

如需特定平台的處理器和 RAM 需求，請參閱該平台的 Microsoft 系統需求。

表 2-4. Windows Server 2012

項目	需求
版本（不需要有 Service Pack）	• Standard • Datacenter • Server Core
處理器	• 至少 1.4GHz 的 Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）
可用磁碟空間	• 至少 1.5GB • 建議使用 2.0GB **注意** 如果您要在 Security Agent 上啟動 Application Control、Endpoint Sensor、Vulnerability Protection 和資料安全防護，趨勢科技建議您將最低磁碟空間增加至 3.0 GB。

項目	需求
其他	• 支援 1024 x 768 解析度（256 色）或以上的顯示器 • 允許透過 Windows 防火牆（如果已啟動）進行印表機/檔案共用 • 啟動預設的本機 admin 注意 不支援 Windows UI。

表 2-5. Windows Server 2012 R2

項目	需求
版本（不需要有 Service Pack）	• Standard • Datacenter • Server Core
處理器	• 至少 1.4GHz 的 Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）
可用磁碟空間	• 至少 1.5GB • 建議使用 2.0GB 注意 如果您要在 Security Agent 上啟動 Application Control、Endpoint Sensor、Vulnerability Protection 和資料安全防護，趨勢科技建議您將最低磁碟空間增加至 3.0 GB。

項目	需求
其他	• 支援 1024 x 768 解析度（256 色）或以上的顯示器 • 允許透過 Windows 防火牆（如果已啟動）進行印表機/檔案共用 • 啟動預設的本機 admin 注意 不支援 Windows UI。

表 2-6. Windows Storage Server 2012

項目	需求
版本（不需要有 Service Pack）	• Standard • Workgroup
處理器	• 至少 1.4GHz 的 Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）
可用磁碟空間	• 至少 1.5GB • 建議使用 2.0GB 注意 如果您要在 Security Agent 上啟動 Application Control、Endpoint Sensor、Vulnerability Protection 和資料安全防護，趨勢科技建議您將最低磁碟空間增加至 3.0 GB。

項目	需求
其他	• 支援 1024 x 768 解析度（256 色）或以上的顯示器 • 允許透過 Windows 防火牆（如果已啟動）進行印表機/檔案共用 • 啟動預設的本機 admin 注意 不支援 Windows UI。

表 2-7. Windows Storage Server 2012 R2

項目	需求
版本（不需要有 Service Pack）	• Standard • Workgroup
處理器	• 至少 1.4GHz 的 Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）
可用磁碟空間	• 至少 1.5GB • 建議使用 2.0GB 注意 如果您要在 Security Agent 上啟動 Application Control、Endpoint Sensor、Vulnerability Protection 和資料安全防護，趨勢科技建議您將最低磁碟空間增加至 3.0 GB。

項目	需求
其他	• 支援 1024 x 768 解析度（256 色）或以上的顯示器 • 允許透過 Windows 防火牆（如果已啟動）進行印表機/檔案共用 • 啟動預設的本機 admin 注意 不支援 Windows UI。

表 2-8. Windows MultiPoint Server 2012

項目	需求
版本（不需要有 Service Pack）	• Standard • Premium
處理器	• 至少 1.4GHz 的 Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）
可用磁碟空間	• 至少 1.5GB • 建議使用 2.0GB 注意 如果您要在 Security Agent 上啟動 Application Control、Endpoint Sensor、Vulnerability Protection 和資料安全防護，趨勢科技建議您將最低磁碟空間增加至 3.0 GB。

項目	需求
其他	• 支援 1024 x 768 解析度（256 色）或以上的顯示器 • 允許透過 Windows 防火牆（如果已啟動）進行印表機/檔案共用 • 啟動預設的本機 admin 注意 不支援 Windows UI。

表 2-9. Windows Server 2012 容錯移轉叢集

項目	需求
版本（不需要有 Service Pack）	• 無
處理器	• 至少 1.4GHz 的 Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）
可用磁碟空間	• 至少 1.5GB • 建議使用 2.0GB 注意 如果您要在 Security Agent 上啟動 Application Control、Endpoint Sensor、Vulnerability Protection 和資料安全防護，趨勢科技建議您將最低磁碟空間增加至 3.0 GB。

項目	需求
其他	• 支援 1024 x 768 解析度（256 色）或以上的顯示器 • 允許透過 Windows 防火牆（如果已啟動）進行印表機/檔案共用 • 啟動預設的本機 admin 注意 不支援 Windows UI。

表 2-10. Windows Server 2012 R2 容錯移轉叢集

項目	需求
版本（不需要有 Service Pack）	• 無
處理器	• 至少 1.4GHz 的 Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）
可用磁碟空間	• 至少 1.5GB • 建議使用 2.0GB 注意 如果您要在 Security Agent 上啟動 Application Control、Endpoint Sensor、Vulnerability Protection 和資料安全防護，趨勢科技建議您將最低磁碟空間增加至 3.0 GB。

項目	需求
其他	• 支援 1024 x 768 解析度（256 色）或以上的顯示器 • 允許透過 Windows 防火牆（如果已啟動）進行印表機/檔案共用 • 啟動預設的本機 admin 注意 不支援 Windows UI。

Windows Server 2016（64 位元）平台

- Windows Server 2016 第 2-19 頁
- Windows Server 2016 容錯移轉叢集 第 2-20 頁
- Windows Storage Server 2016 第 2-21 頁

注意

如需特定平台的處理器和 RAM 需求，請參閱該平台的 Microsoft 系統需求。

表 2-11. Windows Server 2016

項目	需求
版本（不需要有 Service Pack）	• Standard • Datacenter • Server Core
處理器	• 至少 1.4GHz 的 Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器

項目	需求
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）
可用磁碟空間	• 至少 1.5GB • 建議使用 2.0GB **注意** 如果您要在 Security Agent 上啟動 Application Control、Endpoint Sensor、Vulnerability Protection 和資料安全防護，趨勢科技建議您將最低磁碟空間增加至 3.0 GB。
其他	• 支援 1024 x 768 解析度（256 色）或以上的顯示器 • 允許透過 Windows 防火牆（如果已啟動）進行印表機/檔案共用 • 啟動預設的本機 admin **注意** 不支援 Windows UI。

表 2-12. Windows Server 2016 容錯移轉叢集

項目	需求
版本（不需要有 Service Pack）	• 無
處理器	• 至少 1.4GHz 的 Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）

項目	需求
可用磁碟空間	• 至少 1.5GB • 建議使用 2.0GB 注意 如果您要在 Security Agent 上啟動 Application Control、Endpoint Sensor、Vulnerability Protection 和資料安全防護，趨勢科技建議您將最低磁碟空間增加至 3.0 GB。
其他	• 支援 1024 x 768 解析度（256 色）或以上的顯示器 • 允許透過 Windows 防火牆（如果已啟動）進行印表機/檔案共用 • 啟動預設的本機 admin 注意 不支援 Windows UI。

表 2-13. Windows Storage Server 2016

項目	需求
版本（不需要有 Service Pack）	• Standard • Workgroup
處理器	• 至少 1.4GHz 的 Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）

項目	需求
可用磁碟空間	• 至少 1.5GB • 建議使用 2.0GB 注意 如果您要在 Security Agent 上啟動 Application Control、Endpoint Sensor、Vulnerability Protection 和資料安全防護，趨勢科技建議您將最低磁碟空間增加至 3.0 GB。
其他	• 支援 1024 x 768 解析度（256 色）或以上的顯示器 • 允許透過 Windows 防火牆（如果已啟動）進行印表機/檔案共用 • 啟動預設的本機 admin 注意 不支援 Windows UI。

Windows Server 2019（64 位元）平台

注意

如需特定平台的處理器和 RAM 需求，請參閱該平台的 Microsoft 系統需求。

表 2-14. Windows Server 2019

項目	需求
版本（不需要有 Service Pack）	• Standard • Datacenter • Server Core

項目	需求
處理器	• 至少 1.4GHz 的 Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）
可用磁碟空間	• 至少 1.5GB • 建議使用 2.0GB 注意 如果您要在 Security Agent 上啟動 Application Control、Endpoint Sensor、Vulnerability Protection 和資料安全防護，趨勢科技建議您將最低磁碟空間增加至 3.0 GB。
其他	• 支援 1024 x 768 解析度（256 色）或以上的顯示器 • 允許透過 Windows 防火牆（如果已啟動）進行印表機/檔案共用 • 啟動預設的本機 admin 注意 不支援 Windows UI。

Windows Server 2022（64 位元）平台

注意

如需特定平台的處理器和 RAM 需求，請參閱該平台的 Microsoft 系統需求。

表 2-15. Windows Server 2022

項目	需求
版本（不需要有 Service Pack）	• Standard • Datacenter • Server Core
處理器	• 至少 1.4GHz 的 Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）
可用磁碟空間	• 至少 1.5GB • 建議使用 2.0GB 注意 如果您要在 Security Agent 上啟動 Application Control、Endpoint Sensor、Vulnerability Protection 和資料安全防護，趨勢科技建議您將最低磁碟空間增加至 3.0 GB。
其他	• 支援 1024 x 768 解析度（256 色）或以上的顯示器 • 允許透過 Windows 防火牆（如果已啟動）進行印表機/檔案共用 • 啟動預設的本機 admin 注意 不支援 Windows UI。

用戶端封裝工具

使用用戶端封裝工具可更新 Apex One 伺服器傳送給端點的 Security Agent 安裝套件。當伺服器重新封裝 Security Agent 安裝程式時，Apex One 會將所有根網域設定套用至新套件，以確保新安裝擁有更新後的最新設定。

秘訣

趨勢科技建議先對根網域設定一般用戶端設定，接著重新封裝 Security Agent 程式，然後再開始在您整個網路上安裝用戶端。

注意

Apex One 會每天自動重新封裝 Security Agent 程式一次。請檢查「上次產生套件」時間，以決定是否要重新封裝 Security Agent。

步驟

1. 移至「用戶端 > 用戶端封裝工具」。
2. 請點選「立即重新封裝」。
3. 重新封裝完成後，使用 Apex Central 主控台將 Security Agent 安裝程式傳送給使用者。

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。

服務	受控制的功能
趨勢科技未經授權的變更阻止服務 (TMBMSRV.exe)	• 行為監控 • 周邊設備存取控管 • 認證安全防護軟體服務 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。
Apex One NT Firewall (TmPfw.exe)	Apex One 防火牆
Apex One Data Protection Service (dsagent.exe)	• 資料外洩防護 • 周邊設備存取控管
Apex One NT Listener (tmlisten.exe)	Security Agent 與 Apex One 伺服器間的通訊
Apex One NT RealTime Scan (ntrtscan.exe)	• 即時掃瞄 • 預約掃瞄 • 手動掃瞄/立即掃瞄
Apex One Common Client Solution Framework (TmCCSF.exe)	進階防護服務 • 瀏覽器弱點攻擊防護 • 記憶體掃瞄
趨勢科技進階安全威脅評估服務（用戶端） (ATASAgent.exe)	進階 Managed Detection and Response 工作與通訊
Trend Micro Application Control Service（用戶端） (TMiACAgentSvc.exe)	Application Control

服務	受控制的功能
• Trend Micro Endpoint Sensor 引擎封裝程式 (TMESE.exe) • Trend Micro Endpoint Sensor Service（用戶端）(TMESC.exe)	Endpoint Sensor
Trend Micro Vulnerability Protection Service（用戶端）(iVPAgent.exe)	Vulnerability Protection
Apex One NT WSC Service (TmWSCSvc.exe)	將 Apex One Security Agent 的安全狀態回報給安全中心

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。

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 2-16. 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 2-17. 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 2-18. 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

Security Agent 解除安裝

下列方法可讓您從端點解除安裝 Security Agent。

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「啟動解除安裝」。

   Security Agent 會在輪詢伺服器之後或下次預約更新期間收到命令。

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。

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 3 章

用戶端樹狀結構管理

本章說明用戶端樹狀結構、「用戶端管理」畫面，以及 Security Agent 網域和分組選項。

包含下列主題：

- Apex One 用戶端樹狀結構 第 3-2 頁
- 「用戶端管理」畫面 第 3-2 頁
- Apex One 網域 第 3-5 頁

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」。

下表列出了您可以執行的工作。

表 3-1. 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 3-5 頁。
工作	執行下列工作： • 立即掃瞄 如需詳細資訊，請參閱進行立即掃瞄設定 第 5-2 頁。 • 用戶端解除安裝 如需詳細資訊，請參閱從 Web 主控台解除安裝 Security Agent 第 2-30 頁。 • 中央隔離區還原 如需詳細資訊，請參閱恢復隔離的檔案 第 5-16 頁。
掃瞄作業記錄檔	檢視掃瞄作業記錄檔。 如需詳細資訊，請參閱檢視掃瞄作業記錄檔 第 9-2 頁。

功能表按鈕	工作
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 Apex One 網域 第 3-5 頁。
匯出	將用戶端清單匯出到逗號分隔值 (.csv) 檔案。

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 位址的端點。

- 請根據下列條件執行進階搜尋：

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 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。

區段	說明
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 Security Agent 的狀態。

表 3-2. Apex One 用戶端樹狀結構圖示

圖示	說明
	網域
	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

圖示	說明
	雲端截毒掃瞄不可用的更新代理程式

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。

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。

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

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 Apex One 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 4 章

Security Agent 程式設定

本章說明 Security Agent 如何與 Apex One 伺服器進行通訊、如何啟動及停止 Security Agent 服務，以及如何設定全域 Security Agent 設定。

包含下列主題：

- Security Agent 的共存和完整功能比較 第 4-2 頁
- Security Agent 圖示 第 4-5 頁
- 全域用戶端設定 第 4-15 頁
- 端點位置 第 4-16 頁
- 參考伺服器 第 4-17 頁

Security Agent 的共存和完整功能比較

下表比較以共存模式及完整功能集模式設定之 Security Agent 的可用功能。

重要

將設定部署至同時包含共存模式及完整功能之 Security Agent 的網域時，Security Agent 只能接收所設定模式適用的設定。如果將資料外洩防護策略部署到混合式網域，則只有處於完整功能模式的 Security Agent 可以套用這些策略。共存模式 Security Agent 會忽略資料外洩防護策略設定。

表 4-1. 全域用戶端設定

設定	完整功能模式	共存模式
安全設定		
掃瞄設定	可設定	-
預約掃瞄設定	可設定	-
防火牆設定	可設定	-
可疑連線設定	可設定	-
行為監控設定	可設定	-
系統		
認證安全防護軟體服務設定	可設定	-
服務重新啟動	可設定	-
網路		
病毒/惡意程式記錄檔頻寬設定	可設定	可設定
伺服器輪詢間隔	可設定	可設定
用戶端控制		
一般設定	可設定	-

設定	完整功能模式	共存模式
警訊設定	可設定	-
用戶端語言組態設定	可設定	可設定

注意

大部分的「全域用戶端設定」都已移至 Apex Central as a Service 主控台。若要管理 Apex One 的「全域用戶端設定」，請移至 Apex Central as a Service（「策略 > 策略管理」）。

您還是可以使用 Apex One 主控台來允許、封鎖或記錄 Security Agent 與使用者定義的 C&C IP 位址之間的所有連線，以管理「可疑連線設定」。

如需詳細資訊，請疑至 全域用戶端設定 第 4-15 頁。

表 4-2. Apex Central 中的用戶端功能/設定

設定	完整功能模式	共存模式
掃瞄設定	可設定	-
網頁信譽評等設定	可設定	可設定
Machine Learning 設定	可設定	可設定
可疑連線設定	可設定	-
行為監控設定	可設定	-
周邊設備存取控管設定	可設定	-
DLP 設定	可設定	-
樣本提交	可設定	-
更新代理程式設定	可設定	-

設定	完整功能模式	共存模式
權限和其他設定	可設定	部分可設定 權限設定： • 單機模式 • Proxy 伺服器設定 • 元件更新 • 結束並解除鎖定 • 解除安裝 其他設定： • 更新設定 • 網頁信譽評等設定 • C&C 聯絡人警訊設定 • Machine Learning 設定 • Security Agent 存取限制 • 重新啟動通知
其他服務設定	可設定	部分可設定： • 進階防護服務
間諜程式/可能的資安威脅程式核可清單	可設定	-
信任的程式清單	可設定	-
匯出設定	可設定	-
匯入設定	可設定	-

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 4-3. 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。
	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。

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。 
		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。
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： 

用戶端狀態	說明	視覺提示
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。 
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。 
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 4-4. 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

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	已啟動
	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

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
	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 4-5. 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

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	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
	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

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
	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

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	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
	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

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）	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
	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（共存）

系統匣中的 Security Agent 圖示會提供視覺提示，指出 Security Agent 程式的目前狀態，並提示使用者執行某些處理行動。

表 4-6. 共存模式用戶端圖示

圖示	說明
	• Security Agent 處於線上狀態。 • Machine Learning 已啟動且正常運作。 • Security Agent 已連線至趨勢科技主動雲端截毒技術。
	• Security Agent 正在嘗試重新連線至趨勢科技主動雲端截毒技術。 • Security Agent 處於離線狀態。 • Machine Learning 已啟動。
	• Security Agent 處於線上狀態。 • Machine Learning 已關閉。
	• Security Agent 處於離線狀態。 • Machine Learning 已關閉。 • Security Agent 無法連線至趨勢科技主動雲端截毒技術。
	• Security Agent 處於線上狀態。 • Machine Learning 未正常運作或程序無法使用。
	• Security Agent 處於離線狀態。 • Machine Learning 未正常運作或程序無法使用。 • Security Agent 無法連線至趨勢科技主動雲端截毒技術。

全域用戶端設定

大部分的「全域用戶端設定」都已移至 Apex Central as a Service 主控台。若要管理 Apex One 的「全域用戶端設定」，請移至 Apex Central as a Service（「策略 > 策略管理」）。

您還是可以使用 Apex One 主控台來允許、封鎖或記錄 Security Agent 與使用者定義的 C&C IP 位址之間的所有連線，以管理「可疑連線設定」。

若要設定「可疑連線設定」，請完成以下步驟：

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」。

   注意

   使用者定義的 IP 清單僅支援 IPv4 位址。

5. 在「核可的清單」或「封鎖清單」標籤中，新增要監控的 IP 位址。
   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。

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：

- 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。

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 Internet 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「參考伺服器」還是以「閘道 IP 與 MAC 位址」為準。

- 參考伺服器：可連線到參考伺服器的 Security Agent 是內部網路的一部分

  如需詳細資訊，請參閱參考伺服器 第 4-17 頁。

- 閘道 IP 位址：可連線到閘道的 Security Agent 是內部網路的一部分

  a. 在提供的文字方塊中輸入閘道 IPv4/IPv6 位址。

  b. （選用）輸入 MAC 位址。

  c. 請點選「新增」。

  
  注意

  如果您未輸入 MAC 位址，Apex One 會包含所有屬於指定 IP 位址的 MAC 位址。

3. 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」。

部分 III

端點防護

第 5 章

惡意程式防護掃瞄

本節說明如何在 Security Agent 中設定惡意程式防護掃瞄。

包含下列主題：

- 立即掃瞄 第 5-2 頁
- 中毒處理行動 第 5-8 頁
- 掃瞄例外支援 第 5-14 頁
- 恢復隔離的檔案 第 5-16 頁

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「工作 > 立即掃瞄」。

   會出現「立即掃瞄」畫面。
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」。
   a. 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。
   b. 設定「目標」設定。

      如需詳細資訊，請參閱立即掃瞄：「目標」標籤 第 5-3 頁。

c. 設定「處理行動」設定。

如需詳細資訊，請參閱立即掃瞄：「處理行動」標籤 第 5-5 頁。

d. 設定「掃瞄例外」設定。

如需詳細資訊，請參閱立即掃瞄：「掃瞄例外」標籤 第 5-7 頁。

e. 請點選「< 上一步」可返回「立即掃瞄」畫面。

5. 在用戶端樹狀結構中，選取要掃瞄的 Security Agent，然後點選「開始立即掃瞄」。

伺服器會傳送通知給選取的 Security Agent。

6. 依序點選「選取不接收通知的端點」和「開始立即掃瞄」，可立即重新傳送通知給未收到通知的 Security Agent。

7. 請點選「停止通知」，可取消傳送通知給 Security Agent。

已開始掃瞄的 Security Agent 會繼續正在進行中的掃瞄。

8. 對於已開始掃瞄的 Security Agent，請點選「停止立即掃瞄」即可取消作用中的掃瞄。

立即掃瞄：「目標」標籤

步驟

1. 在「要掃瞄的檔案」區段中，從下列項目中選取：

- 所有可掃瞄的檔案：包括所有可掃瞄的檔案。無法掃瞄的檔案為受密碼保護的檔案、加密檔案、或超過使用者定義的掃瞄限制範圍的檔案。

注意

此選項提供了可能的最高安全性。但是，掃瞄每個檔案是一件即費時又耗資源的事，而且在某些情況下可能會太過累贅。因此，您可以限制用戶端在掃瞄中包含的檔案數量。

- 智慧型掃瞄所掃瞄的檔案類型：根據真實檔案型態掃瞄檔案。
- 具有下列副檔名的檔案（使用逗號區隔項目）：根據副檔名手動指定要掃瞄的檔案。請使用逗號分隔多個項目。

> **注意**
>
> 設定父策略時，指定其他使用者設定子策略的方式。
>
> - 繼承自父策略：子策略必須使用在上層策略中設定的設定
> - 從父策略延伸：子策略可以將其他設定附加至從上層策略繼承的設定

2. 在「掃瞄設定」區段中，設定必要設定。

設定	說明
掃瞄壓縮檔	掃瞄封存檔中指定的壓縮層數 **注意** 掃瞄更多層有可能偵測到深藏在壓縮封存檔中的惡意程式，但這麼做可能影響系統效能。
掃瞄 OLE 物件	掃瞄檔案中指定的「物件連結與嵌入」(OLE) 層數 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，主動識別惡意程式。 **注意** 指定的層數同時適用於「掃瞄 OLE 物件」和「在 OLE 檔案中偵測到弱點攻擊程式碼」選項。
掃瞄開機區	掃瞄端點上硬碟的開機磁區是否有病毒/惡意程式

3. 在「CPU 使用率」區段中，從下列項目中選取：
   - 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

立即掃瞄：「處理行動」標籤

步驟

1. 在「病毒/惡意程式」區段中，設定必要設定。
   a. 選取 Security Agent 在偵測到安全威脅後採取的處理行動類型。
      - 使用主動式處理行動：選取此選項可使用一套預先設定的中毒處理行動，來處理病毒/惡意程式

        如需詳細資訊，請參閱主動式處理行動 第 5-8 頁。

        - 自訂可能的病毒/惡意程式的處理行動：選取並指定 Security Agent 針對可能的惡意程式安全威脅採取的處理行動
      - 對所有的病毒/惡意程式類型使用相同的處理行動：指定 Security Agent 針對所有惡意程式安全威脅採取相同的處理行動
      - 對每個病毒/惡意程式類型使用特定的處理行動：指定 Security Agent 針對特定安全威脅採取的處理行動

        如需詳細資訊，請參閱自訂中毒處理行動 第 5-10 頁。

   b. 選取「清除前先備份檔案」可在端點上的 <用戶端安裝資料夾>\Backup 資料夾中建立中毒檔案的加密複本。

      建立檔案的備份複本，可供您在需要時恢復檔案的原始版本。

   c. 指定隔離目錄的位置。
      - 隔離至 Security Agent 的管理伺服器：Security Agent 會將所有隔離檔案的加密複本傳送到管理 Apex One 伺服器
      - 隔離目錄：Security Agent 會將所有隔離檔案的加密複本傳送到指定的位置

      如需詳細資訊，請參閱隔離目錄 第 5-11 頁。

d. 在「損害清除及復原服務」區段中，設定下列項目：

- 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。
- 偵測到可能的病毒/惡意程式時執行清除：針對可能的惡意程式安全威脅執行設定的清除類型

> **注意**
>
> 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。

2. 在「間諜程式/可能的資安威脅程式」區段中，選取 Security Agent 在偵測到間諜程式或可能的資安威脅程式後採取的處理行動。

- 清除：終止所有相關的處理程序並刪除相關聯的登錄值、檔案、Cookie 和捷徑

> **注意**
>
> 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。

- 暫不處理：記錄偵測事件，但允許程式執行

立即掃瞄：「掃瞄例外」標籤

步驟

1. 選取「啟動掃瞄例外」。
2. 在「掃瞄例外清單（目錄）」區段中，設定必要設定。
   a. 選取「不掃瞄趨勢科技產品的安裝目錄」可自動排除與其他趨勢科技產品相關聯的目錄。

      如需詳細資訊，請參閱趨勢科技產品目錄例外 第 5-14 頁。

   b. 輸入不掃瞄的目錄路徑，然後點選 + 按鈕。

      Security Agent 不會掃瞄位於指定目錄（和子目錄）中的檔案。

   注意

   - 您最多可以指定 256 個不掃瞄的目錄。
   - 目錄例外支援使用萬用字元。

     如需詳細資訊，請參閱萬用字元例外 第 5-15 頁。

3. 在「掃瞄例外清單（檔案）」區段中，設定必要設定。
   a. 輸入不掃瞄的檔案名稱或加上完整目錄路徑的檔案名稱，然後點選 + 按鈕。

   注意

   - 您最多可以指定 256 個不掃瞄的檔案。
   - 檔案例外支援使用萬用字元。

     如需詳細資訊，請參閱萬用字元例外 第 5-15 頁。

4. 在「掃瞄例外清單（副檔名）」區段中，設定必要設定。
   a. 選取或輸入不掃瞄的副檔名，然後點選「新增 >」按鈕。

注意

- 您最多可以指定 256 個不掃瞄的副檔名。
- 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??`。

中毒處理行動

您可以設定 Security Agent 根據偵測到的惡意程式類型，採用一套預先設定的中毒處理行動或自訂處理行動。

重要

某些檔案無法清除。

如需詳細資訊，請參閱：

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有病毒/惡意程式的知識，並且可能會是冗長而乏味的工作。Security Agent 使用「主動式處理行動」來因應這些問題。

「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/惡意程式攻擊端點的方式。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。

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 5-1. 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	
	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	通過	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
其他	清除	隔離	清除	隔離
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

注意

- 對於可能的病毒/惡意程式，即時掃瞄期間的預設中毒處理行動是「拒絕存取」，而手動掃瞄和預約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」。
- 有些檔案無法清除。
- 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。

自訂中毒處理行動

處理行動	說明
刪除	刪除中毒檔案。
隔離	重新命名中毒檔案，然後將其移至端點上的暫時隔離目錄。 Security Agent 會將已隔離的檔案傳送到指定的隔離目錄（預設位於管理伺服器上）。 Security Agent 會將傳送至此目錄的隔離檔案加密。 如需詳細資訊，請參閱隔離目錄 第 5-11 頁。
清除	先清除中毒檔案，才允許完整存取該檔案。 如果無法清除檔案，Security Agent 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」。 系統可對所有類型的安全威脅（但不包括可能的病毒/惡意程式）執行此中毒處理行動。 注意 某些檔案無法清除。如需詳細資訊，請參閱無法清除病毒的檔案 第 5-12 頁。
重新命名	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。
通過	不對偵測到的安全威脅執行任何處理行動，但是在記錄檔中記錄偵測到的安全威脅。
拒絕存取	當 Security Agent 偵測到嘗試開啟或執行中毒檔案時，會立即阻止該操作。 使用者可以手動刪除中毒的檔案。

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。

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 5-2. 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。
	UNC 路徑	`\\<osceserver>\ofcscan\Virus`	

隔離目錄	接受的格式	範例	注意
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`	

無法清除病毒的檔案

「病毒掃瞄引擎」無法清除下列檔案：

表 5-3. 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。

掃瞄例外支援

在將目錄和檔案名稱從惡意程式防護掃瞄中排除時，請參閱下列支援資訊：

趨勢科技產品目錄例外

如果在「掃瞄例外清單（目錄）」區段中選取了「不掃瞄趨勢科技產品的安裝目錄」，Security Agent 會自動不掃瞄下列產品目錄：

- <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

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 5-4. 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`

`c:\director?\file\*.txt`	`c:\directory\file\doc.txt`	`c:\directories\file\document.txt`

值	已排除	未排除
`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

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還原記錄檔 第 9-3 頁。

第 6 章

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：

- Apex One 防火牆總覽 第 6-2 頁
- 啟動或關閉端點上的 Apex One 防火牆 第 6-3 頁
- 防火牆策略 第 6-3 頁
- 防火牆資料檔 第 6-10 頁
- 設定全域防火牆設定 第 6-13 頁
- 設定 Security Agent 的防火牆通知 第 6-14 頁
- 測試 Apex One 防火牆 第 6-15 頁

Apex One 防火牆總覽

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。

下表說明 Apex One 防火牆提供的功能。

功能	說明
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」。
網路病毒偵測	Apex One 防火牆會檢查所有網路封包是否有網路病毒。

功能	說明
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。

啟動或關閉端點上的 Apex One 防火牆

您可以直接啟動或關閉所選端點上的 Apex One 防火牆。

步驟

- 透過 Windows 啟動或關閉 Apex One 防火牆驅動程式。
  a. 開啟「Windows 網路連線內容」。
  b. 選取或清除網路卡的「趨勢科技 NDIS 6.0 過濾驅動程式」核取方塊。
- 使用命令提示字元啟動或關閉 Apex One 防火牆驅動程式。
  a. 開啟命令提示字元並輸入 `services.msc`。
  b. 從 Microsoft Management Console (MMC) 啟動或停止「OfficeScan NT Firewall」。

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。

下表列出「防火牆策略」畫面上提供的工作。

工作	說明
新增策略	請點選「新增」以建立新策略。 如需詳細資訊，請參閱新增防火牆策略 第 6-5 頁。
複製現有的策略設定	選取現有的策略，然後點選「複製」以開啟「複製策略」畫面。視需要修改策略設定。
刪除現有的策略	選取現有的策略，然後點選下「刪除」，即可從清單中移除策略。
編輯例外範本	請點選「編輯例外範本」，可檢視目前的「例外範本」清單。 如需詳細資訊，請參閱編輯 Apex One 防火牆例外範本清單 第 6-6 頁。
修改現有的策略	請點選現有策略的「策略說明」以修改設定。

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. 選取此選項，可新增、複製或修改策略。
   - 請點選「新增」以建立新策略。
   - 選取現有的策略，然後點選「複製」以開啟「複製策略」畫面。視需要修改策略設定。
   - 請點選現有策略的「策略說明」以修改設定。
3. 在「防火牆策略」區段中，設定下列項目：
   - 名稱：指定 Apex One 防火牆策略的唯一名稱。
   - 安全層級：選取「高」、「中」或「低」，以決定 Apex One 防火牆要允許或封鎖的流量類型。

     注意

     Apex One 防火牆會自動允許或封鎖透過「例外範本」清單中指定的通訊埠所進行的連線。

     如需詳細資訊，請參閱編輯 Apex One 防火牆例外範本清單 第 6-6 頁。
4. 在「防火牆功能」區段中，設定下列項目：
   - 啟動防火牆：選取此選項可啟動此策略的 Apex One 防火牆。
   - 偵測到防火牆違規時顯示通知：選取此選項可在 Apex One 防火牆封鎖輸出封包時於 Security Agent 上顯示通知。

重要

如果您授與使用者使用 Security Agent 主控台設定 Apex One 防火牆的權限，則您無法使用 Apex One Web 主控台覆寫使用者所設定的設定。

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。

5. 在「認證安全防護軟體清單」區段中，設定下列項目：

   - 啟動本機「認證安全防護軟體清單」：選取此選項可讓趨勢科技允許使用本機病毒碼確認為安全的網路流量流向應用程式。
   - 啟動全域「認證安全防護軟體清單」(需要存取 Internet)：選取此選項可讓趨勢科技允許使用動態更新的雲端病毒碼確認為安全的網路流量流向應用程式。

     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」。

6. 在「例外」區段中，可管理僅適用於此策略的例外範本清單。

   Apex One 防火牆會自動將例外範本清單項目填入例外清單。如果您新增、修改或刪除策略「例外清單」中的任何例外，所做的變更僅會套用至目前的策略，而不會套用至「例外範本清單」。

   如需有關新增例外的詳細資訊，請參閱新增防火牆策略例外 第 6-8 頁（請遵循步驟 3 的指示操作）。

7. 請點選「儲存」。

編輯 Apex One 防火牆例外範本清單

您可以使用「編輯例外範本」畫面，以允許或封鎖 Security Agent 上的網路流量，來對網路流量進行管理。Apex One 防火牆提供預設例外，您可加以修改或刪除。

如需詳細資訊，請參閱預設防火牆策略例外規則 第 6-7 頁。

下表列出「編輯例外範本」畫面上提供的工作。

工作	說明
新增例外	請點選「新增」可建立新例外。 如需詳細資訊，請參閱新增防火牆策略例外 第 6-8 頁。 **重要** 新增例外後，您必須儲存「例外範本」清單，才能套用新的例外。如果您尚未儲存變更就從「編輯例外範本」畫面瀏覽到其他畫面，則 Apex One 防火牆不會儲存新的例外。
刪除現有的例外	選取現有的例外，然後點選「刪除」，即可從「例外範本」清單移除例外。
修改現有的例外	請點選現有範本的「名稱」，可修改例外設定。
重新排序例外的優先順序	請點選某個例外旁邊的向上或向下箭頭，可變更 Apex One 防火牆對網路流量所採取處理行動的優先順序。
儲存例外清單的變更	請點選下列其中一個按鈕，可儲存對「例外範本」清單所做的變更： • 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

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

例外名稱	處理行動	通訊協定	通訊埠	方向
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

防火牆資料檔

Apex One 防火牆資料檔定義哪些 Security Agent 會套用特定的 Apex One 防火牆策略。建立可以建立、設定或刪除特定網域資料檔的使用者角色。

下表列出「防火牆資料檔」畫面上提供的工作。

工作	說明
覆寫 Security Agent 防火牆設定	選取「覆寫用戶端安全層級/例外清單」，可以用伺服器設定取代 Security Agent 資料檔設定。 重要 只有使用內建的管理員帳號登入的使用者，或是擁有完整管理權限的使用者，可以啟動「覆寫用戶端安全層級/例外清單」選項。
新增資料檔	請點選「新增」可建立新資料檔。 如需詳細資訊，請參閱新增防火牆資料檔 第 6-11 頁。
刪除現有的資料檔	選取現有的資料檔，然後點選「刪除」，即可從清單中移除資料檔。
編輯參考伺服器清單	請點選「編輯參考伺服器清單」，可定義端點位置設定。Apex One 防火牆會使用參考伺服器清單來判斷端點位於內部網路還是外部網路。 重要 只有使用內建的管理員帳號登入的使用者，或是擁有完整管理權限的使用者，可以查看及設定參考伺服器清單。 如需詳細資訊，請參閱參考伺服器 第 4-17 頁。
修改現有的資料檔	請點選現有資料檔的「名稱」可修改設定。

工作	說明
重新排序資料檔的優先順序	請點選某個資料檔旁邊的向上或向下箭頭，可變更 Apex One 防火牆對 Security Agent 所採取處理行動的優先順序。 重要 Security Agent 端點即使符合多個資料檔定義，也只會套用優先順序最高之資料檔的資料檔設定。
將資料檔設定傳送給 Security Agent	請點選「套用資料檔到用戶端」，可將所有 Apex One 防火牆資料檔設定部署到 Security Agent。

新增防火牆資料檔

步驟

1. 移至「用戶端 > 防火牆 > 資料檔」。
2. 選取以新增或修改資料檔。
   - 請點選「新增」可建立新資料檔。
   - 請點選現有資料檔的「名稱」可修改設定。
3. 選取「啟動這個資料檔」可允許 Apex One 將資料檔部署到 Security Agent。
4. 在「資料檔設定」區段中，設定下列項目：
   - 名稱：輸入資料檔的唯一名稱。
   - 說明：（選用）輸入資料檔的說明。
   - 策略：選取要套用至資料檔的已存在的 Apex One 防火牆策略。

     如需詳細資訊，請參閱防火牆策略 第 6-3 頁。
   - 選取 Apex One 防火牆用於定義要套用資料檔之 Security Agent 的條件。

條件	說明
端點	選取此選項，可將資料檔套用至從用戶端樹狀結構中選取的 Security Agent。 請點選「從用戶端樹狀結構選取端點」以開啟「防火牆資料檔設定」畫面。選取所需的 Security Agent，然後點選「選取」。
平台	選取此選項，可將資料檔套用至特定的作業系統類型。 • 支援的 Windows Server 平台 • 支援的 Windows 桌上型電腦平台 如需支援的作業系統清單，請參閱《系統需求》文件。
登入名稱	選取此選項，可將資料檔套用至已登入端點的特定使用者。 指定特定使用者的登入名稱。Apex One 防火牆會套用指定使用者所登入的 Security Agent 上的資料檔。
NIC 說明	選取此選項，可將資料檔套用至使用特定網路介面卡 (NIC) 的端點。 請輸入完整或部分 NIC 說明。 秘訣 趨勢科技建議您輸入 NIC 卡製造商，因為 NIC 說明的開頭通常是製造商名稱。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	選取此選項，可根據 Security Agent 連線狀態來套用資料檔。 • 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 4-17 頁。 • 外部 － Security Agent 無法連線到所設定的參考伺服器

5. 在「使用者權限」區段中，設定下列項目：
   - 允許使用者變更安全層級：選取此選項可允許使用者使用 Security Agent 主控台定義 Apex One 防火牆安全層級
   - 允許使用者編輯策略例外：選取此選項可允許使用者使用 Security Agent 主控台定義自訂的 Apex One 防火牆策略例外

   重要

   僅具有「在 Security Agent 主控台上顯示防火牆設定」權限的 Security Agent 可在 Security Agent 主控台上顯示防火牆設定。

6. 請點選「儲存」。

   資料檔會顯示在「防火牆資料檔」清單中。

7. 請點選「套用資料檔到用戶端」，以將更新後的資料檔傳送給 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. 請點選「安全設定」標籤。
   a. 移至「防火牆設定」區段。
   b. 請視需要進行設定。
      - 將防火牆記錄檔傳送到伺服器，間隔為每：設定具有「允許 Security Agent 將防火牆記錄檔傳送到 Apex One server」權限的 Security Agent 將防火牆記錄檔傳送到伺服器的頻率

注意

您可以在「權限和其他設定」畫面上的「權限」標籤中授與「允許 Security Agent 將防火牆記錄檔傳送到 Apex One 伺服器」權限。

- 只在系統重新啟動後更新 Apex One 防火牆驅動程式：防止 Security Agent 在正常作業期間嘗試更新一般防火牆驅動程式
- 每小時傳送防火牆記錄檔計數資訊至 Apex One server 一次，以確定是否有可能發生防火牆病毒爆發：讓 Security Agent 每小時傳送一次防火牆偵測計數給 Apex One

3. 請點選「系統」標籤。
   a. 移至「認證安全防護軟體服務設定」區段。
   b. 請視需要進行設定。
      - 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：向趨勢科技資料中心進行查詢，以確認惡意程式行為封鎖、事件監控、防火牆或防毒掃瞄偵測到的程式確實安全，以降低誤判的可能性
4. 請點選「儲存」。

設定 Security Agent 的防火牆通知

您可以將 Security Agent 設定為 Apex One 防火牆封鎖違反防火牆策略的輸出流量後通知使用者。

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. 接受或修改預設的訊息。

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。

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。

第 7 章

使用病毒爆發防範

本節說明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用資料夾作業階段超過某一門檻值時所發生的安全威脅爆發。

包含下列主題：

- 病毒爆發防範策略 第 7-2 頁
- 設定安全威脅爆發防範 第 7-7 頁
- 關閉病毒爆發防範 第 7-9 頁

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

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。

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。

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。

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，以因應並抑制病毒疫情爆發。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 7-2 頁
   - 封鎖易受攻擊的通訊埠 第 7-3 頁
   - 拒絕檔案和資料夾的寫入權限 第 7-4 頁
   - 拒絕存取可執行的壓縮檔 第 7-5 頁
   - 在惡意程式處理程序/檔案上建立互斥處理 第 7-6 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. 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。

8. 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）

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。

部分 IV

监控 Apex One

第 8 章

資訊中心

本章介紹 Apex One 資訊中心和可用的 Widget。使用資訊中心可快速檢視網路的安全狀態。

包含下列主題：

- 標籤和 Widget 第 8-2 頁
- 摘要標籤 Widget 第 8-6 頁
- 資料安全防護 Widget 第 8-11 頁
- Apex One Widget 第 8-13 頁
- 管理 Widget 第 8-17 頁

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 12-5 頁。

標籤為 Widget 提供了容器。「資訊中心」最多支援 30 個標籤。

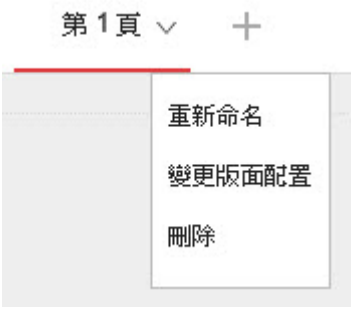
使用標籤

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

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 8-1. 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

類別	說明
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 提供您網路上 Security Agent 的連線和更新狀態的總覽。

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 8-2. 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
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

勒索軟體摘要 Widget

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 8-3. 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

通道	說明	偵測者
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
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。
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 將滑鼠游標暫留在節點上，可檢視該特定日期的受影響端點總數。

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。

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

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 8-4. 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 提供快速參考 Security Agent 安全狀態與偵測、嵌入程式資訊以及病毒爆發事件之處。

可用的 Widget：

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 8-5. 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
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 8-6. 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**

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。

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 7-2 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

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。

第 9 章

記錄檔

本章說明如何使用 Web 主控台存取系統事件和安全偵測記錄檔。

包含下列主題：

- 檢視掃瞄作業記錄檔 第 9-2 頁
- 檢視中央隔離區還原記錄檔 第 9-3 頁
- 檢視系統事件記錄檔 第 9-4 頁

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。

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「掃瞄作業記錄檔」。

   會出現「掃瞄作業記錄檔條件」畫面。
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
開始時間	掃瞄啟動時間
結束時間	掃瞄停止時間
端點	發生掃瞄的端點
狀態	掃瞄的完成狀態 • 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	執行的掃瞄類型（手動掃瞄、立即掃瞄、預約掃瞄）
已掃瞄	已掃瞄的物件數目

項目	說明
病毒/惡意程式	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	間諜程式/可能的資安威脅程式偵測數目
本機雲端病毒碼	本機雲端病毒碼版本
病毒碼	病毒碼版本
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版本

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。

檢視中央隔離區還原記錄檔

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。

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 9-1. 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
以角色為基礎的 Web 主控台存取	• 登入主控台 • 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

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。

第 10 章

通知

本章說明如何設定 Apex One 在偵測到安全威脅後通知使用者。

包含下列主題：

- Security Agent 通知 第 10-2 頁

Security Agent 通知

Apex One 可以在以下情況下在 Security Agent 端點上顯示通知訊息：

- 每當一偵測到安全威脅。啟動通知訊息，並視需要修改其內容。
- 每當一偵測到 Web-based 安全威脅。啟動通知訊息，並視需要修改其內容。

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 Security Agent 的間諜程式/可能的資安威脅程式通知

您可以將 Security Agent 設定為將嘗試清除或隔離間諜程式/可能的資安威脅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「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」。

設定 Security Agent 的防火牆通知

您可以將 Security Agent 設定為 Apex One 防火牆封鎖違反防火牆策略的輸出流量後通知使用者。

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. 接受或修改預設的訊息。
4. 請點選「儲存」。

設定 Security Agent 的網頁信譽評等通知

您可以將 Security Agent 設定為每當偵測到嘗試存取惡意網站時通知使用者。

步驟

1. 移至「管理 > 通知 > 用戶端」。
2. 從「類型」下拉式清單中，選取「網頁信譽評等違規」。
3. 接受或修改預設的訊息。
4. 請點選「儲存」。

設定 Security Agent 的周邊設備存取控管通知

您可以將 Security Agent 設定為封鎖存取未經授權的裝置後通知使用者。

步驟

1. 移至「管理 > 通知 > 用戶端」。
2. 從「類型」下拉式清單中，選取「周邊設備存取控管違規」。
3. 接受或修改預設的訊息。
4. 請點選「儲存」。

設定 Security Agent 的行為監控通知

您可以將 Security Agent 設定為封鎖存取某個應用程式或程序，或是偵測到新發現的程式後通知使用者。

步驟

1. 移至「管理 > 通知 > 用戶端」。
2. 從「類型」下拉式清單中，選取「行為監控策略違規」。
3. 接受或修改預設的訊息。

4. 請點選「儲存」。

設定 Security Agent 的 C&C 回呼通知

您可以將 Security Agent 設定為每當端點嘗試連線到已知 C&C 伺服器時通知使用者。

步驟

1. 移至「管理 > 通知 > 用戶端」。
2. 從「類型」下拉式清單中，選取「C&C 回呼」。
3. 接受或修改預設的訊息。
4. 請點選「儲存」。

設定 Security Agent 的 Machine Learning 通知

您可以將 Security Agent 設定為每當偵測到未知安全威脅時通知使用者。

步驟

1. 移至「管理 > 通知 > 用戶端」。
2. 從「類型」下拉式清單中，選取「Machine Learning 違規」。
3. 接受或修改預設的訊息。
4. 請點選「儲存」。

部分 V

更新和管理

第 11 章

更新

本章討論如何設定 Security Agent 更新，並說明用戶端上更新的元件。

包含下列主題：

- 設定 Security Agent 的預約更新 第 11-2 頁
- Security Agent 更新來源 第 11-3 頁

設定 Security Agent 的預約更新

設定 Apex One 以設定的預約時程自動更新所有 Security Agent。隨時更新元件，可確保您獲得能夠抵禦最新安全威脅的最佳防護。

步驟

1. 移至「更新 > 用戶端 > 自動更新」。
2. 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。
3. 請點選「儲存」。

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 11-3 頁和 Security Agent 的自訂更新來源 第 11-5 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 11-3 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更新代理程式的自訂更新來源 第 11-8 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 11-1. 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：	
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： • 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。

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「自訂的更新來源」。
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 11-4 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 11-9 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。

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」。

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 11-5 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 Apex Central 中，於指派的 Security Agent 策略中移至「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 Apex Central 中，於指派的 Security Agent 策略中移至「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。

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 11-5 頁。

第 12 章

管理設定

本章說明 Apex One 伺服器和 Security Agent 可用的管理設定。

包含下列主題：

- 帳號管理 第 12-2 頁
- 主動式雲端截毒技術 第 12-3 頁
- 通知設定 第 12-6 頁
- 一般管理設定 第 12-6 頁

帳號管理

重要

只有在特定網路環境中才需要建立使用者帳號。如果您擁有受支援的內部部署 Apex Central 或 Control Manager 伺服器，且想要用其管理 Apex One (Mac) as a Service 和 Apex One as a Service 主控台，則您必須建立使用者帳號，才能透過 Apex Central 或 Control Manager 促進 Apex One (Mac) as a Service 與 Apex One as a Service 主控台之間的通訊。

如需向內部部署 Apex Central 或 Control Manager 伺服器註冊的詳細資訊，請參閱設定 Apex Central (Control Manager) 註冊設定 第 12-7 頁。

如需使用內部部署 Apex Central 或 Control Manager 伺服器註冊 Apex One (Mac) as a Service 和 Apex One as a Service 主控台的詳細資訊，請參閱 https://success.trendmicro.com/solution/1118614#step3。

步驟

1. 移至「管理 > 帳號管理 > 使用者帳號」。

   會出現「使用者帳號」畫面。

2. 請點選「新增」。
3. 確認選取了「啟動此帳號」核取方塊。
4. 指定帳號的「使用者名稱」。
5. 指定帳號的「說明」。
6. 指定「密碼」並確認密碼。

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
- 不可包含使用者名稱
- 不可包含非可列印 ASCII 字元

7. （選用）指定帳號的「電子郵件信箱」。
8. 請點選「下一步」。

   會出現「步驟 2 用戶端網域控制項」畫面。

重要

畫面上的設定不會影響通訊設定。您不需要修改任何設定。

9. 請點選「下一步」。

   會出現「步驟 3 定義用戶端樹狀結構功能表」畫面。

重要

畫面上的設定不會影響通訊設定。您不需要修改任何設定。

10. 請點選「完成」。

    帳號隨即出現「使用者帳號」畫面上的表格中。

主動式雲端截毒技術

- 內部用戶端的主動式雲端截毒技術來源 第 12-4 頁
- Smart Feedback 第 12-5 頁

內部用戶端的主動式雲端截毒技術來源

如果 Security Agent 的閘道 IP 位址與「端點位置」畫面上指定的任何閘道 IP 位址相符，或者如果用戶端可以連線至任何參考伺服器，則 Security Agent 的位置是在內部。設定 Security Agent IP 位址的範圍，並為每個 Security Agent 指派自訂的主動雲端截毒技術伺服器清單。

如需詳細資訊，請參閱端點位置 第 4-16 頁。

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. 請點選「新增」。
4. 在「IP 範圍」區段中，指定 IPv4 位址範圍。
5. 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 位址。
   b. 啟動「檔案信譽評等服務」。
   c. 如果您的公司使用 HTTPS 通訊協定，請啟動「SSL」。
   d. 指定主動雲端截毒技術伺服器用於監聽要求的通訊埠。
   e. 啟動「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。
   f. 指定主動雲端截毒技術伺服器用於監聽要求的通訊埠。
   g. 請點選「新增到清單」。
   h. 透過重複以上步驟來新增更多伺服器。
   i. 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。

6. 請點選「儲存」。

   會出現「主動式雲端截毒技術來源」畫面，並在表格中顯示所設定的 Security Agent IP 範圍。

7. 按一下「儲存並通知用戶端」。

Smart Feedback

趨勢科技 Smart Feedback 會將受保護的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」。

通知設定

Apex One 允許您設定用戶端通知，將對特定端點上執行的偵測通知使用者。

如需有關不同類型的 Security Agent 通知設定資訊，請參閱下列章節：通知 第 10-1 頁。

一般管理設定

- 設定用於用戶端連線的 Proxy 伺服器設定 第 12-6 頁
- 設定離線用戶端移除設定 第 12-7 頁
- 設定 Apex Central (Control Manager) 註冊設定 第 12-7 頁
- 設定 Web 主控台設定值 第 12-10 頁
- 設定可疑物件清單設定 第 12-10 頁
- 從內部部署 OfficeScan 伺服器移轉至 Apex One as a Service 第 12-12 頁

設定用於用戶端連線的 Proxy 伺服器設定

用戶端連線到 Apex One 伺服器和趨勢科技主動式雲端截毒技術時，會使用 Windows「網際網路選項」中的 Proxy 伺服器設定。

步驟

1. 移至「管理 > 設定 > Proxy」。
2. 如果 Proxy 伺服器需要驗證，請輸入使用者名稱和密碼，然後確認密碼。
3. 請點選「儲存」。

設定離線用戶端移除設定

您可以設定 Apex One 何時將 Security Agent 的狀態變更為「離線」。Apex One 可以將用戶端定義為「離線」，前提是 Security Agent 出於以下任一原因而未向伺服器回報：

- 已手動將 Security Agent 程式從端點移除
- 使用者已將 Security Agent 程式關閉或結束很長一段時間

您可以將 Apex One 設定為自動從用戶端樹狀結構移除離線的 Security Agent。

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」。

設定 Apex Central (Control Manager) 註冊設定

在執行 Apex One 佈建程序期間，依預設會自動設定向 Apex Central as a Service 進行註冊的作業。如有必要（例如，您要從內部部署 Apex Central 或 Control Manager 伺服器訂閱可疑物件清單），您可向其他內部部署 Apex Central 或 Control Manager 伺服器註冊。

重要

- Apex One 僅支援向內部部署 Apex Central 或 Control Manager 7.0（或更新版本）伺服器重新註冊。
- 如果您要向內部部署 Apex Central 或 Control Manager 7.0（或更新版本）伺服器註冊，則必須先在 DMZ 中的某個端點上執行 Apex One as a Service 遠端連線工具，以促進雲端型 Apex One 主控台與本機 Apex Central 或 Control Manager 伺服器之間的通訊。

步驟

1. 移至「管理 > 設定 > Apex Central」。
2. 請點選「向不同的 Apex Central 伺服器註冊」。
3. 指定新 Apex Central（或 Control Manager）伺服器的「伺服器 FQDN 或 IP 位址」。

   重要

   - 您必須指定 Apex One 目前所註冊之伺服器以外的其他內部部署 Apex Central 或 Control Manager 伺服器。
   - 如果您已設定某個端點來建立連到內部部署 Apex Central 或 Control Manager 伺服器的遠端連線，請指定反向 Proxy 端點的「伺服器 FQDN 或 IP 位址」。

4. 指定 Apex Central 或 Control Manager 伺服器的「通訊埠 (HTTPS)」。

   重要

   如果您已設定某個端點來建立連到內部部署 Apex Central 或 Control Manager 伺服器的遠端連線，請指定反向 Proxy 端點的「通訊埠 (HTTPS)」。

5. 點選「Apex Central 憑證」旁邊的「瀏覽...」，然後選取從目標 Apex Central 或 Control Manager 伺服器下載的憑證檔案。

   如果要取得 Apex Central 或 Control Manager 憑證檔案，請移至內部部署 Apex Central 或 Control Manager 伺服器，然後將下列位置中的憑證檔案複製到 Apex One 伺服器：

```
<Control Manager 安裝資料夾>\Certificate\CA\TMCM_CA_Cert.pem
```

重要

如果您的公司在 Apex Central 或 Control Manager 伺服器上使用自訂憑證，您必須在 Apex Central 或 Control Manager 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 12-9 頁。

6. 如果內部部署 Apex Central 或 Control Manager 伺服器的 IIS Web 伺服器需要驗證，請輸入使用者名稱和密碼。

7. 指定可在 Apex Central 或 Control Manager 主控台上識別 Apex One 伺服器的「項目顯示名稱」。

   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）。

8. 請點選「連線」。

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。

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）
3. 請點選「儲存」。

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。

如需向內部部署 Apex Central 或 Control Manager 伺服器註冊的詳細資訊，請參閱設定 Apex Central (Control Manager) 註冊設定 第 12-7 頁。

重要

如果您將 Apex One as a Service 與 Apex One Sandbox as a Service 附加元件搭配使用，則您不需要進行「可疑物件清單訂閱」設定。

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」。

從內部部署 OfficeScan 伺服器移轉至 Apex One as a Service

Apex One 支援從執行版本 XG SP1（或更新版本）的內部部署 OfficeScan 伺服器移轉伺服器及 Security Agent 設定。在嘗試執行移轉程序之前，請務必先升級所有想要移轉至 Apex One 伺服器的 Security Agent。

注意

如果您的 Security Agent 是在虛擬機器中執行或使用 VPN，請確保您的環境符合先決條件。

虛擬桌面和 VPN 用戶端的移轉先決條件 第 12-13 頁

移轉程序需要您執行下列工作：

1. 使用伺服器移轉工具將來源 OfficeScan 或 Apex One 伺服器設定匯入到 Apex One 主控台。

   如需詳細資訊，請參閱使用 Apex One 設定匯出工具 第 12-14 頁。

2. 將來源 OfficeScan 或 Apex One 伺服器策略設定移轉至 Apex Central as a Service 主控台。

   如需詳細資訊，請參閱將內部部署 OfficeScan 策略設定移轉至 Apex Central 主控台 第 12-18 頁。

3. 將 Security Agent 從來源伺服器移至 Apex One

   重要

   將 Security Agent 移至 Apex One 伺服器之前，請務必先在內部部署伺服器主控台中將 Security Agent 的 Proxy 伺服器設定變更為「使用 Windows Proxy 伺服器設定」，以允許 Security Agent 連線至 Apex One 主控台。

   如需詳細資訊，請參閱《OfficeScan 管理手冊》中的「設定內部用戶端 Proxy 伺服器設定」主題。

如需詳細資訊，請參閱將 Security Agent 移至其他網域或伺服器 第 3-7 頁。

虛擬桌面和 VPN 用戶端的移轉先決條件

移轉在虛擬機器中執行或使用 VPN 的內部部署 Security Agent 前，請確保內部部署 OfficeScan XG Service Pack 1（或更新版本）或 Apex One 伺服器上 <伺服器安裝目錄>\PCCSRV\Private\ofcserver.ini 檔案中的下列設定正確：

- 對於非持續性虛擬桌面支援環境：
  1. 在 <伺服器安裝目錄>\PCCSRV\Private\ofcserver.ini 檔案中，找到 [INI_SERVER_SECTION]。
  2. 確認存在下列值：

     ```
     EnableCheckClientMacAddress=1
     ```

  3. 儲存檔案。
  4. 在內部部署 Web 主控台中，移至「用戶端 > 全域用戶端設定」。
  5. 點選「儲存」，將設定部署至所有 Security Agent。
- 對於 VPN 用戶端（例如 Cisco Anyconnect）：
  1. 在 <伺服器安裝目錄>\PCCSRV\Private\ofcserver.ini 檔案中，找到 [INI_SERVER_SECTION]。
  2. 確認存在下列值：

     ```
     SP_DisableTmLwfRegistryKeyProtection=1
     ```

  3. 儲存檔案。
  4. 在內部部署 Web 主控台中，移至「用戶端 > 全域用戶端設定」。
  5. 點選「儲存」，將設定部署至所有 Security Agent。

使用 Apex One 設定匯出工具

重要

本版的 Apex One 僅支援從 OfficeScan 版本 XG SP1 和更新版本進行移轉。在嘗試移轉設定前，請務必先將來源 OfficeScan 伺服器和所有移轉的 Security Agent 升級至 XG SP1 或更新版本。

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 12-16 頁。

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。
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。

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：

功能	移轉的設定
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 `ApexOne_Agent_DLP_Policies.zip` 和 `ApexOne_Agent_Policies.zip` 套件，以在匯入到 Apex Central 伺服器時使用。	• 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。
用戶端分組	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。
全域用戶端設定	所有設定

功能	移轉的設定
端點位置	• 位置偵測設定 • 閘道 IP 位址和 MAC 清單
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。

將內部部署 OfficeScan 策略設定移轉至 Apex Central 主控台

OfficeScan XG SP1（或更新版本）提供策略匯出工具，可讓您用於將內部部署 OfficeScan 伺服器策略移轉至 Apex Central 主控台，以確保您不用重新設定所有目前的策略設定，即可維持當前的安全層級。

注意

策略匯出工具只能匯出網域層級的策略設定。如果您已經使用自訂設定來設定個別 Security Agent，則必須手動重新建立個別策略。

步驟

1. 移至來源 OfficeScan XG SP1 伺服器電腦。
2. 使用命令列編輯器，並指向下列目錄：

   ```
   <伺服器安裝目錄>\PCCSRV\Admin\Utility\PolicyExportTool
   ```

3. 執行下列命令：

   ```
   PolicyExportTool.exe -cmconsole
   ```

   策略匯出工具會將策略設定儲存在下列位置：

   ```
   <伺服器安裝目錄>\PCCSRV\Admin\Utility\PolicyExportTool
   \PolicyClient_CMConsole.zip
   ```

4. 登入 Apex Central Web 主控台，然後移至「策略 > 策略管理」。
5. 在「產品」下拉式功能表中，選取「Apex One Security Agent」。

6. 點選「匯入設定」。

7. 選取 <伺服器安裝目錄>\PCCSRV\Admin\Utility\PolicyExportTool\PolicyClient_CMConsole.zip 檔案並加以匯入。

   移轉後的策略設定會顯示在 Apex One Security Agent 策略管理清單中。Apex Central 會將原始 OfficeScan 網域名稱附加在每個策略名稱的結尾。

部分 VI

取得說明

第 13 章

技術支援

瞭解下列主題：

- 疑難排解資源 第 13-2 頁
- 聯絡趨勢科技 第 13-3 頁
- 將可疑內容傳送到趨勢科技 第 13-4 頁
- 其他資源 第 13-5 頁

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。

索引

A

Apex One
- Web 主控台, 1-7
- 元件, 8-17
- 文件, vi
- 程式, 8-17

C

C&C 回呼
- Widget, 8-13

M

MAC 位址, 4-16

S

Security Agent, 2-3
- Windows 10, 2-4
- Windows 11, 2-5
- Windows 7, 2-2
- Windows 8.1, 2-3
- Windows HPC Server 2008 R2, 2-8
- Windows MultiPoint Server 2010, 2-9
- Windows MultiPoint Server 2011, 2-10
- Windows MultiPoint Server 2012, 2-16
- Windows Server 2008 R2, 2-7
- Windows Server 2012, 2-12
- Windows Server 2012 R2, 2-13
- Windows Server 2012 容錯移轉叢集, 2-17, 2-18
- Windows Server 2016, 2-19
- Windows Server 2016 容錯移轉叢集, 2-20
- Windows Server 2019, 2-22
- Windows Server 2022, 2-24
- Windows Storage Server 2008 R2, 2-8
- Windows Storage Server 2012, 2-14
- Windows Storage Server 2012 R2, 2-15
- Windows Storage Server 2016, 2-21
- 和 Apex One 伺服器之間的連線, 4-5
- 連線, 4-14
- 解除安裝, 2-30
- 詳細的用戶端資訊, 3-5
- 圖示, 4-14
- 離線用戶端, 12-7

W

Web 主控台, 1-7
- 關於, 1-7

Widget, 8-2, 8-11, 8-13–8-17
- Apex One 與嵌入程式混搭技術, 8-14
- C&C 回呼事件, 8-13
- 用戶端更新, 8-17
- 用戶端與伺服器之間的連線能力, 8-17
- 安全威脅偵測, 8-14
- 防毒用戶端連線能力, 8-15
- 病毒爆發, 8-16
- 資料外洩防護 - 最常偵測項目, 8-11
- 資料外洩防護 - 歷來偵測項目, 8-11

Windows 10, 2-4
Windows 11, 2-5
Windows 7, 2-2
Windows 8.1, 2-3

Windows HPC Server 2008 R2, 2-8
Windows MultiPoint Server 2010, 2-9
Windows MultiPoint Server 2011, 2-10
Windows MultiPoint Server 2012, 2-16
Windows Server 2008 R2, 2-7
Windows Server 2012, 2-12
Windows Server 2012 R2, 2-13
Windows Server 2012 容錯移轉叢集, 2-17, 2-18
Windows Server 2016, 2-19
Windows Server 2016 容錯移轉叢集, 2-20
Windows Server 2019, 2-22
Windows Server 2022, 2-24
Windows Storage Server 2008 R2, 2-8
Windows Storage Server 2012, 2-14
Windows Storage Server 2012 R2, 2-15
Windows Storage Server 2016, 2-21

四畫

元件, 8-17
支援
    更快地解決問題, 13-4
文件, vi
文件意見反應, 13-6

五畫

主動式處理行動, 5-8
主動雲端截毒技術, 1-4, 1-5
    主動雲端截毒技術, 1-4
    病毒碼檔案, 1-5
        網頁封鎖清單, 1-5
    網頁信譽評等服務, 1-5
用戶端, 3-6, 3-7
    刪除, 3-6
    移動, 3-7
用戶端分組, 3-5–3-7
    工作, 3-5
    刪除網域或用戶端, 3-6
    重新命名網域, 3-7
    移動用戶端, 3-7
    新增網域, 3-6
用戶端更新
    自訂來源, 11-5
    標準來源, 11-3
用戶端解除安裝, 2-30
用戶端樹狀結構, 3-2, 3-3
    一般工作, 3-3
    特定工作, 3-2
        用戶端管理, 3-2
    進階搜尋, 3-3
    關於, 3-2
立即掃瞄, 5-2

六畫

安全威脅
    防護, 1-3

七畫

位置偵測, 4-16
更新代理程式
    分析報告, 11-9
更新來源
    用戶端, 11-3
防火牆, 6-2
    測試, 6-15
    策略, 6-3
    資料檔, 6-10
    預設策略例外, 6-7, 6-8

八畫

其他服務設定, 2-25
周邊設備存取控管, 1-4

十畫
特洛伊木馬程式, 1-3
病毒碼檔案
　　網頁封鎖清單, 1-5
病毒爆發防範, 8-16
　　策略, 7-2
　　關閉, 7-9
病毒爆發防範策略
　　互斥, 7-6
　　互斥處理, 7-6
　　可執行壓縮檔, 7-5
　　拒絕寫入權限, 7-4
　　拒絕壓縮檔存取, 7-5
　　封鎖通訊埠, 7-3
　　限制/拒絕存取共享資料夾, 7-2
記錄檔
　　中央隔離區還原記錄檔, 9-3
　　系統事件記錄檔, 9-4
　　掃瞄記錄檔, 9-2

十一畫
參考伺服器, 4-17
掃瞄例外, 5-15
通知
　　用戶端使用者, 10-2
通訊埠封鎖, 7-3

十二畫
智慧型支援系統, 1-7, 1-8
程式, 8-17
策略
　　防火牆, 6-3
詞彙, vii

十三畫
損害清除及復原服務, 1-3
解除安裝, 2-30
　　使用解除安裝程式, 2-31
　　從 Web 主控台, 2-30
資料外洩防護
　　Widget, 8-11
資訊中心
　　摘要, 8-2
閘道 IP 位址, 4-16
隔離目錄, 5-11

十四畫
摘要
　　資訊中心, 8-2
摘要資訊中心, 8-2
　　Widget, 8-2
　　元件和程式, 8-17
　　標籤, 8-2
網頁信譽評等, 1-3
網頁信譽評等服務, 1-5
網頁封鎖清單, 1-5
網域, 3-5–3-7
　　刪除, 3-6
　　重新命名, 3-7
　　新增, 3-6
網路端點的前 10 名安全威脅統計資料, 8-16
認證安全防護軟體清單, 6-2

十五畫
標籤, 8-2

十九畫
離線用戶端, 12-7

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: APTM09513/220328