Trend Micro Apex One™

Service Pack 1 Patch 2

安裝和升級手冊

企業資訊安全整體防護

文件編號：APTM29870/231128

發行日期：2023 年 12 月

受美國專利保護，專利編號： 5,951,698

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

如需有關如何使用產品特定功能的詳細資訊，請參閱 Trend Micro 線上說明中心和/或 Trend Micro 常見問題集。

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

請至下列網站並給予您對此文件的評估意見：

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

隱私權資料和個人資料蒐集披露

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

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

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

趨勢科技所蒐集的資料將遵循趨勢科技隱私權注意事項中的規定：

https://www.trendmicro.com/privacy

目錄

序言

第 1 章：規劃 Apex One 安裝和升級

第 2 章：安裝 Trend Micro Apex One

第 3 章：升級 Trend Micro Apex One

第 6 章：疑難排解資源

第 7 章：技術支援

附錄 A：部署範例

索引

序言

序言

歡迎使用 Trend Micro Apex One™《安裝和升級手冊》。本文件討論安裝 Apex One 伺服器以及升級伺服器和 Security Agent 的需求與程序。

本章內容：

注意

如需有關安裝 Security Agent 的資訊，請參閱《管理手冊》。

Apex One 文件

Apex One 文件包含下列各項：

表 1. Apex One 文件

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

您可以從下列位置下載最新的 PDF 文件和 Readme 檔：

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

讀者

Apex One 文件適用於下列使用者：

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

文件慣例

本文件會使用下列慣例。

表 2. 文件慣例

慣例	說明
大寫	頭字語、縮寫、特定的命令名稱和鍵盤上的按鍵
粗體	功能表和功能表命令、命令按鈕、標籤和選項
斜體	參考其他文件
等寬	指令行範例、程式碼、Web URL、檔案名稱和程式輸出
瀏覽 > 路徑	可達到特定畫面的瀏覽路徑 例如，「檔案 > 儲存」代表請點選「檔案」，然後請點選介面上的「儲存」
 注意	組態設定注意事項
 秘訣	推薦或建議
 重要	必要或預設組態設定和產品限制的相關資訊
 警告!	重要的處理行動和組態設定選項

詞彙

下表提供 Apex One 文件中使用的正式詞彙：

表 3. Apex One 詞彙

詞彙	說明
Security Agent	Apex One 用戶端 程式
用戶端端點	安裝 Security Agent 的端點。
用戶端使用者（或使用者）	用戶端端點上管理 Security Agent 的人員。
伺服器	Apex One 伺服器程式
伺服器電腦	安裝 Apex One 伺服器的端點。
管理員（或 Apex One 管理員）	管理 Apex One 伺服器的人員
主控台	用於設定和管理 Apex One 伺服器及用戶端設定的使用者介面 Apex One 伺服器程式的主控台稱為「Web 主控台」，而 Security Agent 程式的主控台稱為「Security Agent 主控台」。
安全威脅	病毒/惡意程式、間諜程式/可能的資安威脅程式和網路安全威脅的總稱
使用授權服務	包括「防毒」、「損害清除及復原服務」、「網頁信譽評等」和「間諜程式防護」—上述功能都會在安裝 Apex One 伺服器期間啟動
Apex One 服務	透過 Microsoft 管理主控台 (MMC) 所代管的服務。例如：`ofcservice.exe`（Apex One Master Service）。
程式	包括 Security Agent 和 Plug-in Manager
元件	負責針對安全威脅進行掃瞄、偵測和採取中毒處理行動

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`

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

雲端截毒掃瞄用戶端	已設定為使用雲端截毒掃瞄的任何 Security Agent
標準掃瞄用戶端	已設定為使用標準掃瞄的任何 Security Agent
雙堆疊	同時具有 IPv4 和 IPv6 位址的實體。 例如： • 同時具有 IPv4 和 IPv6 位址的端點 • 安裝在雙堆疊端點上的 Security Agent • 會將更新分發到用戶端的更新代理程式 • 雙堆疊 Proxy 伺服器（如 DeleGate）可以在 IPv4 和 IPv6 位址之間進行轉換
單純 IPv4	僅具有 IPv4 位址的實體
單純 IPv6	僅具有 IPv6 位址的實體
嵌入程式解決方案	透過 Plug-in Manager 提供的本機 Apex One 功能和嵌入程式

第 1 章

規劃 Apex One 安裝和升級

本章說明 Trend Micro Apex One™ 安裝與升級的安裝前準備資訊。

重要

- 您無法在已安裝 Apex Central 的伺服器電腦上執行 Apex One 伺服器的全新安裝。
- 如果您升級到 Apex One，Control Manager 會安裝在同一部伺服器電腦上，對 Apex One 和 Apex Central 的單一伺服器電腦支援取決於您啟動的功能。

  如需詳細資訊，請疑至 https://success.trendmicro.com/dcx/s/solution/000267022?language=en_US。

本章內容：

Apex One 伺服器需求

下列主題概述您在安裝或升級至 Apex One 伺服器前應考量的一些事項。

作業系統支援

下表概述 Apex One 伺服器的作業系統支援和移轉可用性。

秘訣

趨勢科技建議您在安裝或升級至 Apex One 伺服器之前，先在目標伺服器電腦上執行完整的 Windows Update

作業系統	Apex One	Apex One Service Pack 1
Windows Server 2012	是	是
Windows Server 2012 R2	是	是
Windows Server 2016	是	是
Windows Server 2019	是	是
Windows Server 2022	是	是

重要

Apex One 已完全不再支援 Apache 伺服器。

SQL Server 需求

Apex One 不再支援舊版 OfficeScan 所用的較舊 Codebase 資料庫模型。您可以在安裝前準備好自己的 SQL Server，或讓 Apex One 安裝程式在伺服器安裝過程中安裝 SQL Server 2016 SP2 Express。

重要

升級至 Apex One 後，Apex One Web 主控台上將不再顯示用來備份舊版 Codebase 資料庫的較舊「資料庫備份」畫面。

下表概述 Apex One 伺服器的資料庫支援和移轉可用性。

資料庫	APEX ONE	具有 ENDPOINT SENSOR 的 APEX ONE
Codebase	-	-
SQL Server 2014	是	-
SQL Server 2016	是	-
SQL Server 2016 SP2	是	是
SQL Server 2016 Express SP2	是	-
SQL Server 2017	是	是
SQL Server 2019	是	是
SQL Server 2022	是	是

注意

當安裝或升級至具有 Endpoint Sensor 功能的 Apex One 時，您必須先在版本受支援的 SQL Server 上啟動「搜尋的全文檢索和語意擷取」，然後再開始安裝程序。

如需有關 Endpoint Sensor 需求的詳細資訊，請參閱 Apex One Endpoint Sensor 第 1-9 頁。

Security Agent 支援

下表概述 Security Agent 的需求和建議的設定。

重要

當端點上同時執行大量應用程式時，可能會發生資源使用量突增情況。如果在目標端點執行時可用的記憶體或磁碟空間已不多，趨勢科技建議您先升級必要硬體元件，然後再安裝或升級 Apex One Security Agent。

趨勢科技建議您配置所列示的最低系統需求，做為 Security Agent 程式的專用資源，以確保在執行密集掃瞄作業期間仍具有充足效能。

項目	說明
支援 HTTPS	Apex One 伺服器與 Security Agent 之間需要進行 HTTPS 通訊。 重要 如果您在執行升級程序期間未選取允許 HTTPS 通訊，則無法升級至 Apex OneService Pack 1 伺服器。
伺服器-用戶端通訊	趨勢科技建議您在安裝完成後，在「全域用戶端設定」畫面上，為 Apex One 伺服器與 Security Agent 之間的通訊啟動 AES-256 加密。
作業系統支援	Apex One 僅支援執行特定 Windows 作業系統的端點。 如需 Apex One 伺服器和 Security Agent 需求的完整清單，請參閱「系統需求」文件。 在升級安裝期間，安裝程式會確認所有向伺服器報告的端點皆執行支援的作業系統。如果安裝程式偵測到不受支援的作業系統，將無法繼續升級。 在升級至 Apex One 伺服器之前，請將安裝於不支援的作業系統上的所有用戶端移至舊版 OfficeScan 伺服器，或是將用戶端程式解除安裝。

安裝驗證

下表概述如何驗證 Apex One 伺服器和 Security Agent 順利完成。

項目	說明
Apex One 伺服器	檢查下列服務是否正在執行中： • Apex One Master Service (`OfcService.exe`) • Apex One Plug-in Manager (`OfcAoSMgr.exe`) • Apex One Active Directory Service (`OSCEIntegrationService.exe`) • Apex One Log Receiver Service (`OfcLogReceiverSvc.exe`) • Apex One Deep Discovery Service (`ofcDdaSvr.exe`) • Apex One database process (`DbServer.exe`)

Security Agent	檢查下列服務是否正在執行中：
	• 桌上型電腦平台：
	  • Apex One Common Client Solution Framework Service (`TmCCSF.exe`)
	  • Apex One NT Listener (`Tmlisten.exe`)
	  • Apex One NT RealTimeScan (`Ntrtscan.exe`)
	  • Apex One NT Firewall (`Tmpfw.exe`)
	  • Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`)
	• 伺服器平台：
	  • Apex One Common Client Solution Framework Service (`TmCCSF.exe`)
	  • Apex One NT Listener (`Tmlisten.exe`)
	  • Apex One NT RealTimeScan (`Ntrtscan.exe`)

Apex Central 擴充功能的需求

如果您計劃部署透過與 Apex Central Web 主控台整合所獲得的其他安全防護功能，請確定您瞭解其他功能對 Apex One 系統需求造成的影響。下列主題概述與增強的產品功能相關的系統需求、安裝和升級資訊，以及任何其他資訊。

• Apex One Application Control 第 1-6 頁

Apex One Application Control

表 1-1. 先決條件

項目	需求
系統需求	與 Apex One 伺服器及 Security Agent 相同
使用授權	• 隨附於 Windows 版和 Mac 版 Apex One 完整功能使用授權 • 現有的 Trend Micro Endpoint Application Control 使用授權（已在 Apex Central 中啟動）
Apex Central 註冊	進行授權和 Security Agent 策略部署的必要項目
與 Trend Micro Endpoint Application Control 的相容性	• 伺服器：具有 Application Control 的 Apex One 伺服器可以與 Trend Micro Endpoint Application Control 共存在同一部伺服器上（不建議這樣做）。 重要 Trend Micro Endpoint Application Control 伺服器的設定與 Apex One Application Control 功能不相容。您必須使用 Apex Central Web 主控台手動設定所有策略。 • 用戶端：在您將 Application Control 策略部署到 Apex One Security Agent 後，Security Agent 會自動解除安裝任何現有的 Trend Micro Endpoint Application Control 用戶端，然後再套用 Apex One Application Control 設定。

表 1-2. 全新安裝資訊

類型	說明
伺服器	Apex One 安裝程式會在正常安裝 Apex One 伺服器期間自動安裝 Application Control 功能。 在確認啟動碼包含 Application Control 之後，Apex One 會在 Apex One 伺服器電腦上啟動 Trend Micro Application Control Service。
用戶端	Security Agent 程式包含 Application Control Service，但不會在正常安裝 Security Agent 期間立即安裝此服務。如果要在 Security Agent 上安裝 Apex One Application Control 功能，您必須從 Apex Central Web 主控台啟動並部署 Application Control 策略。 一旦 Security Agent 收到 Application Control 設定，Security Agent 就會安裝 Application Control 功能。

表 1-3. 升級注意事項

類型	說明
OfficeScan 伺服器	Apex One 使用授權僅包含用於全新安裝的 Application Control 啟動。如果您是從舊版 OfficeScan 伺服器升級，請務必聯絡您的銷售人員以取得新的使用授權來啟動 Application Control 功能。 Apex One 安裝程式會在正常安裝 Apex One 伺服器期間自動安裝 Apex One Application Control 功能。
Trend Micro Endpoint Application Control 伺服器	Apex One 不支援執行從獨立式 Trend Micro Endpoint Application Control 伺服器到 Apex One Application Control 功能的任何升級或設定移轉。 重要 Trend Micro Endpoint Application Control 伺服器的設定與 Apex One Application Control 功能不相容。您必須使用 Apex Central Web 主控台手動設定所有策略。

類型	說明
Trend Micro Endpoint Application Control 用戶端	Apex One 不支援將 Trend Micro Endpoint Application Control 用戶端程式升級至 Apex One Security Agent。 如果您在已安裝 Trend Micro Endpoint Application Control 用戶端的端點上安裝 Apex One Security Agent，並且從 Apex Central 主控台部署 Application Control 策略，Security Agent 會自動解除安裝 Trend Micro Endpoint Application Control 用戶端並安裝 Apex One Application Control 功能。

表 1-4. 安裝驗證

類型	說明

Apex One 伺服器	在使用功能的有效使用授權安裝 Apex One 伺服器後，您可以驗證下列項目：
	• Trend Micro Application Control Service 正在 Apex One 伺服器電腦上執行。
	• Application Control Service 資料夾存在於 Apex One 伺服器電腦中的下列位置：
	`<伺服器安裝資料夾>/iServiceSvr/iAC`
	• Application Control Service 安裝記錄檔存在於 Apex One 伺服器電腦中的下列位置：
	`%windir%/OFCMAS.LOG`

Security Agent 端點	安裝 Security Agent 並從 Apex Central 部署 Application Control 策略後，您可以驗證下列項目： • Trend Micro Application Control Service（用戶端）正在 Security Agent 端點上執行。 • Application Control Service 資料夾存在於端點中的下列位置： `<Security Agent 安裝資料夾>/iService/iAC`

表 1-5. 安裝後的設定

設定	說明
伺服器	在 Apex Central Web 主控台中，移至「管理 > 更新 > 手動更新」，然後確保下載認證安全防護軟體病毒碼。

設定	說明
Security Agent 端點	在 Apex Central Web 主控台中，移至「策略 > 策略管理」，然後視需要新增或修改 Apex One Security Agent 策略的「Application Control 設定」。

Apex One Endpoint Sensor

已購買 Apex One™: Endpoint Sensor 使用授權並且整合了 Apex Central 的客戶，可使用 Endpoint Sensor。您只能使用 Apex Central Web 主控台來進行 Endpoint Sensor 策略設定。

安裝 Apex One 伺服器之前，請確保您可存取正確版本的 SQL Server。如果想要使用 Endpoint Sensor 功能，您必須安裝並備妥特定版本的 SQL Server。

注意

如果您不安裝 Endpoint Sensor 服務，但選取了已啟動「搜尋的全文檢索和語意擷取」的受支援 SQL Server，則日後使用 Endpoint Sensor 的唯一方法是前往 Windows「控制台」的「解除安裝或變更程式」畫面。

選取 Apex One 伺服器，然後按一下「變更」。

- 先決條件 第 1-10 頁
- 全新安裝資訊 第 1-11 頁
- 升級注意事項 第 1-12 頁

表 1-6. 先決條件

項目	需求
系統需求	伺服器：作業系統需求與 Apex One 伺服器相同（SQL Server 有不同需求） 端點：系統需求與 Apex One Security Agent 相同 **重要** 只有下列平台正式支援這項功能： • Windows 8.1 • Windows 10
使用授權	• Apex One Endpoint Sensor 使用授權（已在 Apex Central 中啟動） • 現有的 Trend Micro Endpoint Sensor 使用授權（已在 Apex Central 中啟動）
Apex Central 註冊	進行授權和 Security Agent 策略部署的必要項目

與 Trend Micro Endpoint Sensor 的相容性	• 伺服器：如果您在獨立式 Trend Micro Endpoint Sensor 伺服器所在的同一部伺服器上安裝具有 Apex One Endpoint Sensor 功能的 Apex One 伺服器（不建議這樣做）：
	  • 獨立式 Trend Micro Endpoint Sensor 伺服器已關閉。
	  • 獨立式 Trend Micro Endpoint Sensor 的檔案和資料庫繼續常駐在伺服器電腦上，並且可能對效能造成影響。
	重要
	獨立式 Trend Micro Endpoint Sensor 伺服器的設定與 Apex One Endpoint Sensor 功能不相容。您必須使用 Apex Central Web 主控台手動設定所有策略。
	• 用戶端：在您將 Endpoint Sensor 策略部署到 Apex One Security Agent 後，Security Agent 會自動解除安裝任何現有的獨立式 Trend Micro Endpoint Sensor 用戶端，然後再套用 Apex One Endpoint Sensor 設定。

項目	需求
Redis 服務	Apex One 伺服器電腦不能已安裝現有的 Redis 服務。您必須解除安裝任何現有的 Redis 服務，並允許安裝程式安裝新服務。 確認 按一下「Endpoint Sensor 安裝」畫面上的「下一步」後
SQL Server 版本	• SQL Server 2022 • SQL Server 2019 • SQL Server 2017 • SQL Server 2016 SP1 注意 此功能不支援 SQL Server Express 版本。 確認 按一下「Apex One 資料庫設定」畫面上的「下一步」後
資料庫組態設定	已啟動「搜尋的全文檢索和語意擷取」 如需有關啟動「搜尋的全文檢索和語意擷取」的詳細資訊，請參閱您的 SQL Server 文件。 確認 按一下「Apex One 資料庫設定」畫面上的「下一步」後
	tempdb 資料庫的存取權（可存取資料庫維護功能） 確認 無

表 1-7. 全新安裝資訊

類型	說明
伺服器	Apex One 安裝程式提供在正常安裝 Apex One 伺服器期間安裝 Apex One Endpoint Sensor 功能的選項。

類型	說明
用戶端	Security Agent 程式包含 Endpoint Sensor 服務，但不會在正常安裝 Security Agent 期間立即安裝此服務。若要在 Security Agent 上安裝 Endpoint Sensor 服務，您必須從 Apex Central Web 主控台啟動並部署 Endpoint Sensor 策略。 一旦 Security Agent 收到 Endpoint Sensor 設定，Security Agent 就會安裝 Endpoint Sensor 服務。

表 1-8. 升級注意事項

類型	說明
OfficeScan 伺服器	Apex One 安裝程式提供在正常升級 Apex One 伺服器期間安裝 Apex One Endpoint Sensor 功能的選項。
Trend Micro Endpoint Sensor 伺服器	Apex One 不支援執行從獨立式 Trend Micro Endpoint Sensor 伺服器到 Apex One Endpoint Sensor 功能的任何升級或設定移轉。 重要 獨立式 Trend Micro Endpoint Sensor 伺服器的設定與 Apex One Endpoint Sensor 功能不相容。您必須使用 Apex Central Web 主控台手動設定所有策略。
Trend Micro Endpoint Sensor 用戶端	Apex One 不支援將 Trend Micro Endpoint Sensor 用戶端程式升級至 Apex One Security Agent。 如果您在已安裝獨立式 Trend Micro Endpoint Sensor 用戶端的端點上安裝 Apex One Security Agent，並且從 Apex Central 主控台部署 Endpoint Sensor 策略，Security Agent 會自動解除安裝 Trend Micro Endpoint Sensor 用戶端並安裝 Apex One Endpoint Sensor 功能。

Managed Detection and Response 服務

您必須已透過銷售人員購買 Endpoint Sensor 服務並已訂閱 MDR 服務，才能使用 Managed Detection and Response (MDR) 服務。除了下列額外的工作需求外，MDR 服務的系統需求、部署和升級皆與 Endpoint Sensor 服務一致。

工作	額外磁碟空間需求
評估工作	當 MDR 服務開始進行評估工作時，Apex One 伺服器需要額外的 20 GB 磁碟空間（每 100 個端點），才能處理增加的記錄檔資訊。
趨勢科技調查套件 (TMIK)	當 MDR 服務部署 TMIK 時，Apex One 伺服器需要額外的 40 GB 磁碟空間（每 100 個端點），才能處理增加的記錄檔資訊。

Apex One Vulnerability Protection

表 1-9. 先決條件

項目	需求
系統需求	與 Apex One 伺服器及 Security Agent 相同
使用授權	• 隨附於 Windows 版和 Mac 版 Apex One 完整功能使用授權 • 現有的 Trend Micro Vulnerability Protection 使用授權（已在 Apex Central 中啟動）
Apex Central 註冊	進行授權和 Security Agent 策略部署的必要項目
與 Trend Micro Vulnerability Protection 的相容性	• 伺服器：具有 Vulnerability Protection 的 Apex One 伺服器可以與 Trend Micro Vulnerability Protection 共存在同一部伺服器上（不建議這樣做）。 • 用戶端：在您將 Vulnerability Protection 策略部署到 Apex One Security Agent 後，Security Agent 會自動解除安裝任何現有的 Trend Micro Vulnerability Protection 用戶端，然後再套用 Apex One Vulnerability Protection 設定。

項目	需求
與其他趨勢科技產品的相容性	下列趨勢科技產品與 Apex One Vulnerability Protection 功能不相容： • Deep Security 用戶端 • Intrusion Defense Firewall 用戶端 您無法在安裝於已安裝不相容用戶端程式之端點的 Security Agent 上啟動 Apex One Vulnerability Protection 功能。您必須解除安裝發生衝突的程式，然後才能啟動 Apex One Vulnerability Protection 功能。

表 1-10. 全新安裝資訊

類型	說明
伺服器	Apex One 安裝程式會在正常安裝 Apex One 伺服器期間自動安裝 Apex One Vulnerability Protection 功能。 在確認啟動碼包含 Vulnerability Protection 之後，Apex One 會在 Apex One 伺服器電腦上啟動 Trend Micro Vulnerability Protection 服務。
用戶端	Security Agent 程式包含 Apex One Vulnerability Protection 功能，但不會在正常安裝 Security Agent 期間立即安裝此功能。如果要在 Security Agent 上安裝 Vulnerability Protection 功能，您必須從 Apex Central Web 主控台啟動並部署 Vulnerability Protection 策略。 一旦 Security Agent 收到 Vulnerability Protection 設定，Security Agent 就會安裝 Vulnerability Protection 功能。

表 1-11. 升級注意事項

類型	說明
OfficeScan 伺服器	Apex One 使用授權僅包含用於全新安裝的 Vulnerability Protection 啟動。如果您是從舊版 OfficeScan 伺服器升級，請務必聯絡您的銷售人員以取得新的使用授權來啟動 Vulnerability Protection 功能。 Apex One 安裝程式會在正常安裝 Apex One 伺服器期間自動安裝 Apex One Vulnerability Protection 功能。
Trend Micro Vulnerability Protection 伺服器	Apex One 不支援執行從獨立式 Trend Micro Vulnerability Protection 伺服器到 Apex One Vulnerability Protection 功能的任何升級或設定移轉。

類型	說明
Trend Micro Vulnerability Protection 用戶端	Apex One 不支援將 Trend Micro Vulnerability Protection 用戶端程式升級至 Apex One Security Agent。 如果您在已安裝 Trend Micro Vulnerability Protection 用戶端的端點上安裝 Apex One Security Agent，並且從 Apex Central 主控台部署 Vulnerability Protection 策略，Security Agent 會自動解除安裝 Trend Micro Vulnerability Protection 用戶端並安裝 Apex One Vulnerability Protection 功能。

表 1-12. 安裝驗證

類型	說明
Apex One 伺服器	在使用功能的有效使用授權安裝 Apex One 伺服器後，您可以驗證下列項目： • Trend Micro Vulnerability Protection 服務正在 Apex One 伺服器電腦上執行。 • Vulnerability Protection 服務資料夾存在於 Apex One 伺服器電腦中的下列位置： <伺服器安裝資料夾>/iServiceSvr/iVP • Vulnerability Protection 服務安裝記錄檔存在於 Apex One 伺服器電腦中的下列位置： <伺服器安裝資料夾>/iServiceSvr/iVP/install.log
Security Agent 端點	安裝 Security Agent 並從 Apex Central 部署 Vulnerability Protection 策略後，您可以驗證下列項目： • Trend Micro Vulnerability Protection 服務（用戶端）正在 Security Agent 端點上執行。 • Vulnerability Protection 服務資料夾存在於端點中的下列位置： <Security Agent 安裝資料夾>/iService/iVP

表 1-13. 安裝後的設定

設定	說明
伺服器	在 Apex Central Web 主控台中，移至「管理 > 更新 > 預約更新」，然後確保排定 Vulnerability Protection 病毒碼的自動更新時程。

設定	說明
Security Agent 端點	在 Apex Central Web 主控台中，移至「策略 > 策略管理」，然後視需要新增或修改 Apex One Security Agent 策略的「Vulnerability Protection 設定」。

安裝和升級檢查清單

安裝程式在安裝或升級 Apex One 伺服器時，會提示使用者輸入下列資訊。

表 1-14. 安裝和升級檢查清單

安裝資訊	下列期間需要的資訊	
	全新安裝	升級
Apex One 安裝路徑 預設的伺服器安裝路徑為： • `C:\Program Files\Trend Micro\Apex One` • `C:\Program Files (x86)\Trend Micro\Apex One`（適用於 x64 類型的平台） 識別安裝路徑或使用預設路徑。如果該路徑不存在，安裝程式會自動建立。	是	否
Proxy 伺服器設定 如果 Apex One 伺服器透過 Proxy 伺服器連線至 Internet，請指定下列項目： • Proxy 類型（HTTP 或 SOCKS 4） • 伺服器名稱或 IP 位址 • 通訊埠 • Proxy 驗證憑證	是	否

安裝資訊	下列期間需要的資訊	
	全新安裝	升級
Web 伺服器設定 Web 伺服器會執行 Web 主控台 CGI，並接受來自用戶端的命令。指定下列項目： • HTTP 通訊埠：預設通訊埠為 8080。如果您使用 IIS 預設網站，請檢查 HTTP 伺服器的 TCP 通訊埠。 警告! 許多透過 HTTP 傳送的駭客和病毒/惡意程式攻擊會使用通訊埠 80 和（或）8080。大多數組織都使用這些通訊埠號碼做為 HTTP 通訊的預設 TCP 通訊埠。如果預設通訊埠號碼目前正在使用中，請改用其他通訊埠號碼。 如果要啟動安全連線： • SSL 憑證有效期間 • SSL 通訊埠（預設值： 4343)	是	否

註冊
 	
註冊產品以收到「啟動碼」。下列為註冊產品的必要資訊：
• 若為舊有的使用者：
  • 線上註冊帳號（登入名稱與密碼）
• 若為尚無帳號的使用者：
  • 授權碼
	是	是

啟動 取得啟動碼	是	是

安裝資訊	下列期間需要的資訊	
	全新安裝	升級
整合式主動雲端截毒技術伺服器安裝 安裝整合式伺服器時，請指定下列項目： • SSL 憑證有效期間 • SSL 通訊埠	是	是
安裝 Security Agent	是	否
管理員帳號密碼 安裝程式會建立 Web 主控台登入的 root 帳號。指定下列項目： • Root 帳號密碼 請指定下列項目，以防止未經授權解除安裝或結束 Security Agent： • Security Agent 解除安裝/結束密碼	是	否
Security Agent 安裝路徑 指定用戶端端點上要用來安裝 Security Agent 的目錄。指定下列項目： • 安裝路徑：預設的用戶端安裝路徑為 `C:\Program Files\Trend Micro\Security Agent` 或 `C:\Program Files (x86)\Trend Micro\Security Agent`。識別安裝路徑或使用預設路徑。如果該路徑不存在，安裝程式會在用戶端安裝期間予以建立。 • Security Agent 通訊埠號碼	是	否
資料庫備份 指定伺服器電腦上要用來備份 Apex One 伺服器以供還原之用的位置。 注意 備份套件需要至少 300MB 的可用磁碟空間，而且可能需要一些時間才能完成。	否	是

安裝資訊	下列期間需要的資訊	
	全新安裝	升級
伺服器驗證憑證 Apex One 會在安裝期間嘗試偵測先前存在的驗證憑證。如果 Apex One 未偵測到憑證，請為新憑證指定備份密碼。	是	是
程式資料夾捷徑 Apex One 伺服器安裝資料夾的捷徑會在 Windows「開始」功能表中顯示。預設的捷徑名稱為 Trend Micro Apex One 伺服器-<伺服器名稱>。找出不同的名稱或使用預設名稱。	是	否

已知的相容性問題

本節說明在同一個端點上安裝 Apex One 伺服器和特定協力廠商應用程式時的相容性問題。如需詳細資訊，請參閱協力廠商應用程式的說明文件。

Microsoft Lockdown Tool 和 URLScan

使用 Microsoft IIS Lockdown Tool 或 URLScan 時，鎖定下列 Apex One 檔案可能會封鎖 Security Agent 與伺服器的通訊：

- 組態 (`.ini`) 檔案
- 資料 (`.dat`) 檔案
- 動態連結庫 (`.dll`) 檔案
- 可執行 (`.exe`) 檔案

阻止用戶端-伺服器通訊中的 URLScan 干擾

步驟

1. 停止 Trend Micro Apex One 伺服器電腦上的網際網路全球資訊網發佈服務。
2. 將 URLScan 組態檔修改為允許上述指定的檔案類型。

3. 重新啟動 World Wide Web Publishing 服務。

Microsoft Exchange Server

在伺服器安裝期間安裝 Security Agent 時，Apex One 必須能夠存取用戶端要掃瞄的所有檔案。由於 Microsoft Exchange Server 會將訊息佇列在本機目錄中，所以必須排除掃瞄這些目錄，才能讓 Exchange Server 處理電子郵件訊息。

Apex One 會自動不掃瞄所有 Microsoft Exchange 2000/2003 目錄。請在 Web 主控台上進行此設定（「安全設定」標籤上的「用戶端 > 全域用戶端設定 > 掃瞄設定」）。如需 Microsoft Exchange 2007 掃瞄例外詳細資料，請參閱：

https://technet.microsoft.com/en-us/library/bb332342(EXCHG.80).aspx

資料庫伺服器

管理員可以掃瞄資料庫伺服器；不過，這可能會降低存取資料庫的應用程式的效能。請考慮將資料庫及其備份資料夾排除在「即時掃瞄」之外。在離峰時段執行手動掃瞄可將資料庫掃瞄的影響降到最低。

第 2 章

安裝 Trend Micro Apex One

本章說明安裝 Trend Micro Apex One™ 的步驟。

本章內容：

全新安裝考量

重要

您無法在已安裝 Apex Central 的伺服器電腦上執行 Apex One 伺服器的全新安裝。

在執行 Apex One 伺服器的全新安裝時，請考慮下列項目：

- Apex One 伺服器位置 第 2-2 頁
- 伺服器效能 第 2-3 頁
- 在安裝期間部署掃瞄方法 第 2-3 頁
- 網路傳輸 第 2-4 頁
- 協力廠商安全軟體 第 2-6 頁
- Active Directory 第 2-6 頁

請造訪下列網站，以取得全新安裝需求的完整清單：

http://docs.trendmicro.com/zh-tw/home.aspx

Apex One 伺服器位置

Apex One 可適應各種網路環境。例如，您可以在 Apex One 伺服器及其用戶端之間設置防火牆，或是在單一網路防火牆後方設置伺服器和所有用戶端。如果伺服器及其用戶端之間存在防火牆，請將防火牆設定為允許用戶端和伺服器監聽通訊埠之間的傳輸。

如需相關資訊來解決在使用網路位址轉譯的網路上管理 Security Agent 時所發生的問題，請參閱《管理手冊》。

重要

基於安全考量，趨勢科技建議將 Apex One 伺服器安裝在公司內部網路內。如果需要管理離開近端內部網路的端點，趨勢科技建議在 DMZ 中安裝 Apex One Edge Relay 伺服器。

伺服器效能

企業網路需要規格高於中小型企業所需的伺服器。

秘訣

趨勢科技建議至少針對 Apex One 伺服器配備 2 GHz 雙處理器和 3 GB 以上的 RAM。

單一 Apex One 伺服器可管理的用戶端端點用戶端數目會視許多因素而定，例如可用伺服器資源和網路拓撲。如需協助判斷伺服器可管理的用戶端數目，請聯絡趨勢科技銷售人員。

專用伺服器

選取 端點 裝載 Apex One 伺服器時，請考慮下列事項：

- 端點所處理的 CPU 負載
- 端點是否執行其他功能

如果目標端點有其他用途，請選擇不執行關鍵應用程式或需要大量資源的應用程式的端點。

在安裝期間部署掃瞄方法

在這個 Apex One 版本中，您可以將用戶端設定為使用「雲端截毒掃瞄」或「標準掃瞄」。

標準掃瞄

「標準掃瞄」是所有舊版 Apex One 使用的掃瞄方法。標準掃瞄用戶端會將所有 Apex One 元件儲存在用戶端端點上，並在本機掃瞄所有檔案。

雲端截毒掃瞄

雲端截毒掃瞄會利用儲存在雲端的安全威脅特徵來進行掃瞄。在「雲端截毒掃瞄」模式下，Apex One 用戶端首先會掃瞄本機是否存在安全威脅。如果用戶

端無法在掃瞄期間判斷檔案是否存在安全威脅隱患，則用戶端會連線到主動雲端截毒技術伺服器。

雲端截毒掃瞄提供下列功能和優點：

- 提供快速、即時的雲端安全狀態查詢功能。
- 縮短爆發新安全威脅時提供防護的整體時間。
- 減少更新病毒碼期間耗用的網路頻寬。大量的病毒碼定義更新只需傳遞到雲端，不必傳遞到許多用戶端。
- 降低在公司內全面部署病毒碼所需的成本和經常性費用。
- 減少在端點上耗用的核心記憶體。記憶體耗用量會隨著時間延長稍微增加。

掃瞄方法部署

在全新安裝期間，用戶端 的預設掃瞄方法是「雲端截毒掃瞄」方法。Apex One 也允許您在安裝伺服器後，針對每個網域自訂掃瞄方法。請考慮下列項目：

- 如果您在安裝伺服器後沒有變更掃瞄方法，您安裝的所有用戶端將會使用「雲端截毒掃瞄」。
- 如果要在所有用戶端上使用「標準掃瞄」，請在安裝伺服器之後，將根層級掃瞄方法變更為「標準掃瞄」。
- 如果要同時使用「標準掃瞄」和「雲端截毒掃瞄」，趨勢科技建議您保留雲端截毒掃瞄做為根層級掃瞄方法，然後再對要套用「標準掃瞄」的網域變更掃瞄方法。

網路傳輸

規劃部署時，請考量 Apex One 所產生的網路流量。伺服器在進行下列動作時會產生傳輸：

- 連線到趨勢科技主動式更新伺服器查看是否有更新元件並加以下載
- 通知用戶端下載更新元件

- 通知用戶端有關組態設定的變更

Security Agent 在執行下列動作時會產生流量：

- 啟動
- 更新元件
- 更新設定並安裝 HotFix
- 掃瞄是否有安全威脅
- 在「單機」模式和「一般」模式之間切換
- 在標準掃瞄和雲端截毒掃瞄之間切換

元件更新期間的網路傳輸

Apex One 在更新元件時會產生大量網路流量。為了減少在元件更新期間產生的網路流量，Apex One 會執行元件複製。Apex One 不會下載經過更新的完整病毒碼檔案，只會下載「漸增式」病毒碼（完整病毒碼檔案的小型版本），然後在下載後將其與舊病毒碼檔案合併。

定期更新的 Security Agent 只會下載漸增式病毒碼。未定期更新的用戶端會下載完整的病毒碼檔案。

趨勢科技會定期發行新的病毒碼檔案。在發現具有破壞力且快速散播的病毒/惡意程式時，趨勢科技也會立即發行新的病毒碼檔案。

更新代理程式和網路傳輸

如果在用戶端和 Apex One 伺服器之間有「低頻寬」或「高流量」的網路區段，可將選取的 Apex One 用戶端指定為「更新代理程式」或其他用戶端的更新來源。如此將有助於分散將元件部署到所有用戶端的負擔。

例如，如果您的遠端辦公室有 20 個以上的端點，請將「更新代理程式」指定為從 Apex One 伺服器複製更新，並做為區域網路上其他用戶端端點的散佈點使用。如需「更新代理程式」的詳細資訊，請參閱《管理手冊》。

Apex Central 和網路傳輸

Trend Micro Apex Central™ 會在閘道、郵件伺服器、檔案伺服器和企業桌上型電腦層級管理趨勢科技產品與服務。Apex Central 的 Web-based 管理主控台提供單一監控點來監控整個網路上的產品與服務。

使用 Apex Central 即可從單一位置管理數部 Apex One 伺服器。Internet 連線快速穩定的 Apex Central 伺服器可從趨勢科技主動式更新伺服器下載元件。然後，Apex Central 會將元件部署至一或多部 Internet 連線不穩定或沒有 Internet 連線的 Apex One 伺服器。

如需詳細資訊，請參閱 Apex Central 文件。

協力廠商安全軟體

請從安裝 Apex One 伺服器的端點中移除協力廠商端點安全防護軟體。這些應用程式可能會讓 Apex One 伺服器無法成功安裝或影響其效能。請在移除協力廠商安全防護軟體之後，立即安裝 Apex One 伺服器與 Security Agent，以保護端點不受安全威脅的侵襲。

注意

Apex One 無法自動解除安裝任何協力廠商防毒產品的伺服器元件，但可以解除安裝用戶端元件。如需詳細資訊，請參閱《管理手冊》。

Active Directory

所有 Apex One 伺服器都必須納入 Active Directory 網域中，以利用以角色為基礎的管理和安全性符合功能。

無訊息安裝

如果有多部 Apex One 伺服器要使用相同的安裝設定，請以無訊息的方式安裝或升級這些伺服器。

準備無訊息安裝

步驟

1. 執行安裝程式並將安裝設定記錄至 `.iss` 檔，藉此建立回應檔。所有使用回應檔以無訊息方式安裝的伺服器都會使用這些設定。

   

   重要

   - 安裝程式只會顯示本機安裝的畫面。
   - 如需執行全新安裝，請從未安裝 Apex One 伺服器的任一端點上建立回應檔。

2. 從命令提示字元執行安裝程式，然後將安裝程式指向用於無訊息安裝的回應檔位置。

將安裝程式組態記錄到回應檔

此程序不會安裝 Apex One。只會將安裝程式組態記錄到回應檔。

步驟

1. 下載 `ApexOne.exe` 檔案，然後解壓縮其中的內容。
2. 開啟命令提示字元，然後輸入 Apex One `setup.exe` 檔的目錄。

   例如，「`CD C:\Apex One Installer\setup.exe`」。
3. 輸入下列命令：

   ```
   setup.exe -r
   ```

   `-r` 參數會觸發安裝程式啟動安裝作業，並將安裝詳細資訊記錄到回應檔。
4. 執行安裝程式中的安裝步驟。
5. 完成這些步驟後，請檢查 `%windir%` 中的回應檔 `setup.iss`。

執行無訊息安裝

步驟

1. 將安裝套件與 `setup.iss` 複製到目標端點。
2. 在目標端點中，開啟命令提示字元並輸入安裝套件的目錄。
3. 輸入下列命令：

   `setup.exe -s <-f1path>setup.iss <-f2path>setup.log`。

   例如：`C:\setup.exe -s -f1C:\setup.iss -f2C:\setup.log`

   說明：

   - `-s`：觸發安裝程式執行無訊息安裝
   - `<-f1path>setup.iss`：回應檔位置。如果路徑包含空格，請以引號 (") 括住路徑，例如，`-f1"C:\osce script\setup.iss"`。
   - `<-f2path>setup.log`：安裝程式將在安裝後建立的記錄檔位置。如果路徑包含空格，請以引號 (") 括住路徑，例如，`-f2"C:\osce log\setup.log"`。
4. 按 ENTER。

   安裝程式會以無訊息方式將伺服器安裝到端點。
5. 如果要判斷安裝是否成功：
   - 檢查目標端點上的 Apex One 程式捷徑。如果無法使用捷徑，請重新嘗試進行安裝。
   - 登入 Apex One Web 主控台。

安裝程式

當您準備好開始安裝 Apex One 伺服器時，請執行安裝程式。

在開始進行 Apex One 伺服器的全新安裝之前，請確保已正確備妥您的環境。如需有關全新安裝考量事項的詳細資訊，請參閱：

- 全新安裝考量 第 2-2 頁
- Apex Central 擴充功能的需求 第 1-5 頁

當您確定已準備好開始時，請遵循畫面上的指示來安裝 Apex One 伺服器。

授權合約

請仔細閱讀授權合約並接受授權合約條款，以繼續進行安裝。不接受授權合約條款便無法繼續進行安裝。

端點安裝前掃瞄

在 Apex One 伺服器安裝開始之前，安裝程式會掃瞄目標端點是否有病毒與惡意程式。安裝程式會掃瞄端點最容易遭受攻擊的區域，包括：

- 開機區和開機目錄（針對開機型病毒）
- Windows 資料夾
- Program Files 資料夾

對於偵測到的病毒/惡意程式和特洛伊木馬程式，安裝程式可以執行下列處理行動：

- 刪除：刪除中毒檔案
- 清除：清除可清除的檔案後才允許完整存取該檔案，或讓指定的下一個中毒處理行動處理無法清除的檔案。
- 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檔案，但如果使檔案與特定應用程式相關聯，則可以開啟。開啟重新命名的中毒檔案時，病毒/惡意程式可能就會執行。
- 暫不處理：允許完整存取中毒檔案，不對檔案執行任何動作。使用者可以複製/刪除/開啟檔案。

重要

在本機升級安裝期間，安裝程式會提示您更新勒索軟體防護設定，以便受到針對勒索軟體安全威脅最佳化的防護。

套用更新的設定只會變更已啟動「行為監控」之用戶端上的設定。

Proxy 伺服器

Apex One 伺服器使用 HTTPS 通訊協定在用戶端與伺服器之間進行通訊，並且連線到趨勢科技主動式更新伺服器來下載更新。如果 Proxy 伺服器處理網路上的 Internet 流量，則 Apex One 需要 Proxy 伺服器設定，以確保伺服器可以從主動式更新伺服器下載更新。

管理員可以在安裝期間略過指定 Proxy 伺服器設定，安裝後再從 Apex One Web 主控台指定設定。

產品啟動

指定您所收到區分大小寫的啟動碼，以啟動所有 Apex One 功能。

若要取得「啟動碼」，請點選「線上註冊」。安裝程式會開啟趨勢科技註冊網站。完成註冊表單後，趨勢科技會寄出含有「啟動碼」的電子郵件。收到代碼後，請繼續進行安裝程序。

產品版本

安裝 Apex One 完整版或試用版。兩種版本都需要不同類型的「啟動碼」。若要取得「啟動碼」，請向趨勢科技註冊產品。

表 2-1. 版本比較

版本	說明
完整版	完整版包含所有產品功能和客戶服務，並且在授權到期後提供寬限期（通常為 30 天）。寬限期到期後，便不提供技術支援和元件更新。掃瞄引擎會繼續掃瞄使用過期元件的端點。這些過期元件可能無法保護端點不受最新安全威脅的侵襲。請購買更新維護，以在授權到期前或到期後續約授權。

版本	說明
試用版	此試用版包含所有產品功能。您可以隨時將試用版升級為完整版。如果在試用期結束時沒有升級，Apex One 便會關閉元件更新、掃瞄和所有用戶端功能。

授權碼和啟動碼

在安裝期間，請指定啟動碼以啟動所有功能。

使用產品隨附的授權碼取得啟動碼（如果尚未取得）。安裝程式會自動重新導向至趨勢科技網站，進行產品註冊。

產品註冊完畢後，趨勢科技會寄送「啟動碼」。

請聯絡趨勢科技銷售人員以取得「授權碼」或「啟動碼」（如果在安裝時沒有「授權碼」或「啟動碼」）。

如需詳細資訊，請參閱聯絡趨勢科技 第 7-3 頁。

注意

如有關於註冊的問題，請參閱：

https://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326。

安裝路徑

接受預設安裝路徑或指定新路徑。

伺服器識別

指定 Security Agent 是依完整的網域名稱 (FQDN)、主機（網域）名稱還是 IP 位址來識別伺服器電腦。

伺服器電腦和 Security Agent 之間的通訊依指定的 IP 位址而定。變更 IP 位址會導致 Security Agent 無法與 Apex One 伺服器通訊。恢復通訊的唯一方法是重新部署所有 Security Agent。如果是依主機名稱識別伺服器電腦，且其主機名稱已變更，則適用於相同的情況。

在大多數網路中，伺服器電腦的 IP 位址較其主機名稱更有可能變更，因此通常會偏好依主機名稱來識別伺服器電腦。

秘訣

對於使用 IP 位址而非主機名稱的管理員，趨勢科技建議不要在安裝後變更 IP 位址（從 DHCP 伺服器取得）。管理員可以使用從 DHCP 伺服器取得的相同 IP 位址資訊，將 IP 位址組態設定設為「靜態」（在 DHCP 伺服器上），從而避免 Security Agent 後續發生通訊問題。

保留 IP 位址組態設定的另一種方法是，僅保留 Apex One 伺服器的 IP 位址。這會迫使 DHCP 伺服器為 Apex One 指定相同的 IP 位址，即便 DHCP 已啟動時也如此。

當您使用靜態 IP 位址時，將依其 IP 位址來識別伺服器。此外，如果伺服器電腦擁有多張網路介面卡 (NIC)，請考慮使用其中一個 IP 位址而非主機名稱，以確保用戶端與伺服器之間順利進行通訊。

Web 伺服器

Apex One Web 伺服器會代管 Web 主控台、讓管理員能夠執行主控台「通用閘道介面」(CGI) 及接受來自 Security Agent 的命令。Web 伺服器會將這些命令轉換為 Security Agent CGI，並將其轉送到 Apex One Master Service。

HTTP 通訊埠

Web 伺服器會在 HTTP 通訊埠監聽 Security Agent 要求，並將這些要求轉送到 Apex One Master Service。此服務會在指定的 Security Agent 通訊埠將資訊傳回給 Security Agent。

SSL 支援

為了在 Web 主控台與伺服器之間進行安全通訊，Apex One 會使用 Secure Sockets Layer (SSL)。SSL 提供額外的保護層來對抗駭客。雖然 Apex One 會先將在 Web 主控台上指定的密碼進行加密，再傳送給 Apex One 伺服器，但駭客仍然可以竊聽封包，並且不需將其解密即可「重現」密碼，取得主控台的存取權。SSL 通道會防止駭客透過網路竊聽封包。

使用的 SSL 版本視 Web 伺服器支援的版本而定。

當選取 SSL 時，安裝程式會自動建立 SSL 憑證，需要這項憑證才能進行 SSL 連線。憑證包含伺服器資訊、公開金鑰和私密金鑰。

SSL 憑證的有效期間應介於 1 到 20 年之間。管理員在憑證到期之後，仍可使用憑證。不過，每當使用相同憑證啟動 SSL 連線時，就會出現一個警告訊息。

通訊透過 SSL 的運作方式為：

1. 管理員透過 SSL 連線從 Web 主控台傳送資訊到 Web 伺服器。
2. Web 伺服器會回應具有必要憑證的 Web 主控台。
3. 瀏覽器會使用 RSA 加密執行金鑰交換。
4. Web 主控台會使用 RC4 加密傳送資料到 Web 伺服器。

雖然 RSA 加密是較安全的方法，但會使通訊流速降低。因此，它僅用於金鑰交換，而 RC4 這種速度較快的替代品則用於資料傳輸。

Web 伺服器通訊埠

下表列出 Web 伺服器的預設通訊埠號碼。

表 2-2. Apex One Web 伺服器的通訊埠號碼

Web 伺服器和設定	通訊埠	
	HTTP	HTTPS (SSL)
IIS 預設網站（已啟動 SSL）	80（不可設定）	443（不可設定）
IIS 虛擬網站（已啟動 SSL）	8080（可設定）	4343（可設定）

Endpoint Sensor 安裝

如果您整合了 Apex Central 並已購買 Endpoint Sensor 使用授權，請選取「安裝 Endpoint Sensor」以確保所有必要的 Endpoint Sensor 服務均可供 Security Agent 使用。

注意

只有下列平台正式支援這項功能：

- Windows 7 SP1
- Windows 8.1
- Windows10

下表概述安裝 Endpoint Sensor 服務所需的最低需求。

項目	需求	確認
Redis 服務	Apex One 伺服器電腦不能已安裝現有的 Redis 服務。您必須解除安裝任何現有的 Redis 服務，並允許安裝程式安裝新服務。	按一下「Endpoint Sensor 安裝」畫面上的「下一步」後
SQL Server 版本	• SQL Server 2017 • SQL Server 2016 SP1 注意 此功能不支援 SQL Server Express 版本。	按一下「Apex One 資料庫設定」畫面上的「下一步」後
資料庫組態設定	已啟動「搜尋的全文檢索和語意擷取」 如需有關啟動「搜尋的全文檢索和語意擷取」的詳細資訊，請參閱您的 SQL Server 文件。	按一下「Apex One 資料庫設定」畫面上的「下一步」後
	tempdb 資料庫的存取權（可存取資料庫維護功能）	無

注意

如果您不安裝 Endpoint Sensor 服務，但選取了已啟動「搜尋的全文檢索和語意擷取」的受支援 SQL Server，則日後使用 Endpoint Sensor 的唯一方法是前往 Windows「控制台」的「解除安裝或變更程式」畫面。

選取 Apex One 伺服器，然後按一下「變更」。

Apex One 資料庫設定

重要

如果您計劃使用 Endpoint Sensor 功能，您必須在已正確備妥且版本受支援的 SQL Server 上建立資料庫。

如需詳細資訊，請參閱 Apex One Endpoint Sensor 第 1-9 頁。

步驟

1. 選擇 Apex One 資料庫的位置：
   - 安裝/建立新的 SQL Server Express 執行個體：選擇安裝 SQL Server 2016 SP2 Express 並建立「\OFFICESCAN」資料庫執行個體

     

     重要

     如果您選擇安裝 Endpoint Sensor 功能，此選項將無法使用。

   - SQL Server：選取 Apex One 應使用的已存在的 SQL Server 安裝和資料庫執行個體。
2. 選取「資料庫驗證」方法。

   使用「Windows 帳號」登入伺服器時，Apex One 會套用目前登入之使用者的「使用者名稱」。

重要

使用者帳號必須屬於本機管理員群組或 Active Directory (AD) 內建管理員，而您必須使用 Windows「本機安全性原則」或「群組原則管理」主控台設定「使用者權限指派」中的下列原則：

- 以服務方式登入
- 以批次工作登入
- 允許本機登入

使用者帳號還必須具有下列資料庫角色：

- dbcreator

注意

僅當使用安裝程式來建立新的資料庫執行個體時，才需要此選項。

- bulkadmin
- db_owner

3. 在「資料庫名稱」區段中，指定 SQL Server 上供必要 Apex One 資料庫使用之資料庫執行個體的名稱。

注意

- 僅當您選擇安裝 Endpoint Sensor 功能時，才會顯示「Endpoint Sensor」選項。
- 如果 SQL Server 上沒有指定的資料庫，安裝程式會自動建立新的資料庫執行個體。已設定的驗證帳號必須擁有 dbcreator 權限，才能建立新的資料庫。

Apex One Security Agent 部署

有數種方法可以安裝或升級 Security Agent。此畫面列出不同的部署方法，以及大約所需的網路頻寬。

使用此畫面可估計將 Security Agent 部署到目標用戶端時，所需的伺服器空間大小以及耗用的頻寬。

注意

所有這些安裝方法都需要目標端點上的本機管理員或網域管理員權限。

安裝整合式主動雲端截毒技術伺服器

安裝程式可在目標端點上安裝整合式主動雲端截毒技術伺服器。整合式伺服器會為使用雲端截毒掃瞄的 Security Agent 提供檔案信譽評等服務，並為受網頁信譽評等策略管制的 Security Agent 提供網頁信譽評等服務。從 Apex One Web 主控台管理整合式伺服器。

重要

此版本的 Apex One 僅支援使用 HTTPS 通訊來進行檔案信譽評等查詢及網頁信譽評等查詢。

趨勢科技建議您安裝獨立式主動雲端截毒技術伺服器，它與整合式伺服器具有相同功能，但能夠為較多的 Security Agent 提供服務。獨立式伺服器是獨立安裝，並具有其自己的管理主控台。如需獨立式伺服器的相關資訊，請參閱《趨勢科技主動雲端截毒技術伺服器管理手冊》。

秘訣

由於整合式主動雲端截毒技術伺服器與 Apex One 伺服器在同一個端點上執行，因此在這兩部伺服器的尖峰流量期間，端點的效能可能會大幅降低。為了減少導向 Apex One 伺服器的流量，請將獨立式主動雲端截毒技術伺服器指定為主要主動雲端截毒技術來源，而將整合式伺服器指定為備份來源。如需為 Security Agent 設定主動雲端截毒技術來源的詳細資訊，請參閱《管理手冊》。

未安裝整合式伺服器

執行全新安裝，並且選擇不安裝整合式伺服器時：

- 標準掃瞄將成為預設掃瞄方法。
- 在獨立的安裝畫面中啟動網頁信譽評等策略時（如需詳細資訊，請參閱網頁信譽評等服務 第 2-21 頁），用戶端無法傳送網頁信譽評等查詢，因為 Apex One 會假定未安裝任何主動雲端截毒技術伺服器。

如果安裝 Apex One 之後有獨立伺服器可用，請從 Apex One Web 主控台執行下列工作：

- 將掃瞄方法變更為雲端截毒掃瞄。
- 將獨立式伺服器新增至主動雲端截毒技術來源清單，讓用戶端能夠傳送檔案信譽評等與網頁信譽評等查詢到該伺服器。

安裝 Security Agent

選擇在目標伺服器上安裝 Security Agent。

Security Agent 程式提供抵禦安全威脅的實際防護。因此，如果要保護 Apex One 伺服器電腦免受安全威脅侵襲，該伺服器也需要安裝 Security Agent 程式。選擇在伺服器安裝期間安裝 Security Agent 便於確保伺服器已自動受到保護，也可免除在安裝伺服器後安裝 Security Agent 的額外工作。

注意

安裝伺服器後，再將 Security Agent 安裝到網路上的其他端點。

如需詳細資訊，請參閱《管理手冊》。

如果伺服器電腦上目前已安裝趨勢科技或協力廠商的端點安全防護軟體，則 Apex One 不一定能夠自動解除安裝該軟體並以 Security Agent 來取代。如需 Apex One 會自動解除安裝的軟體清單，請聯絡您的支援供應商。如果無法自動解除安裝軟體，請先手動解除安裝，然後再繼續安裝 Apex One。

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

Security Agent 安裝

接受預設的 Security Agent 安裝設定，或指定其他安裝路徑。如果安裝目錄的磁碟空間不足，請變更其路徑。

秘訣

趨勢科技建議使用預設設定。

指定不同的安裝路徑時，請輸入靜態路徑或是使用變數。如果指定的路徑包含 Security Agent 上不存在的目錄，則安裝程式會在 Security Agent 安裝期間自動建立該目錄。

如果要輸入靜態 Security Agent 安裝路徑，請輸入包含磁碟機代號的磁碟機路徑。例如，`C:\Program Files\Trend Micro\Security Agent`。

注意

在 Apex One 伺服器安裝完成之後，就無法修改 Security Agent 安裝路徑。所有已安裝的 Security Agent 都使用相同的安裝路徑。

指定 Security Agent 安裝路徑的變數時，請使用下列變數：

- `$BOOTDISK`：端點開機硬碟的磁碟機代號，預設是 `C:\`
- `$WINDIR`:Windows 目錄，預設是 `C:\Windows`
- `$ProgramFiles`:在 Windows 中自動設定的 Program Files 目錄，通常用於安裝軟體，預設是 `C:\Program Files`

同樣在這個畫面上，請設定下列項目：

- 通訊埠號碼：Apex One 伺服器使用指定的通訊埠與用戶端進行溝通。請接受預設值或輸入新值。

Apex One 防火牆

Apex One 防火牆使用狀態檢測、高效能網路病毒掃瞄和消除，來保護網路上的 Security Agent 和伺服器。您可以依據 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。

視需要選擇關閉 Apex One 防火牆，並於稍後從 Apex One 伺服器 Web 主控台加以啟動。

視需要在伺服器平台上啟動 Apex One 防火牆。如果正在進行升級，且已在伺服器平台上啟動 Apex One 防火牆，請選取「啟動 Apex One 防火牆 (在伺服器平台上)」，讓 Apex One 在升級後不會關閉 Apex One 防火牆。

間諜程式防護功能

在評估模式下，所有受伺服器管理的用戶端都會將手動掃瞄、預約掃瞄、即時掃瞄與立即掃瞄期間偵測到的間諜程式/可能的資安威脅程式記錄下來，但是不

會清除這些間諜程式/可能的資安威脅程式元件。清除會終止程序，或刪除登錄、檔案、Cookie 和捷徑。

趨勢科技提供評估模式，可針對趨勢科技偵測為間諜程式/可能的資安威脅程式的項目進行評估。然後管理員可以設定適當的動作。例如，將偵測為具安全威脅的間諜程式/可能的資安威脅程式加入間諜程式/可能的資安威脅程式核可清單中。

安裝後，如需有關評估模式時建議採用的處理行動，請參閱《管理手冊》。

您可以在這個畫面中指定週數，將評估模式設為僅在某個期間生效。安裝後，可以從 Web 主控台變更評估模式設定（「用戶端 > 全域用戶端設定」的「安全設定」標籤上的「僅限間諜程式/可能的資安威脅程式掃瞄設定」區段）。

網頁信譽評等服務

網頁信譽評等策略會指定 Apex One 是封鎖還是允許對某個網站的存取。如需政策的詳細資訊，請參閱《管理手冊》。

選取「啟動網頁信譽評等服務 (在桌上型電腦平台上)」，為安裝於桌上型電腦平台上的內部和外部 用戶端 啟動策略。如果伺服器平台需要與桌上型電腦平台相同的 Web 威脅防護層級，請選取「啟動網頁信譽評等服務 (在伺服器平台上)」。

Security Agent 會使用您在 Web 主控台的「端點位置」畫面中設定的位置條件，來判斷其位置以及要套用的策略。Security Agent 會在每次位置變更時切換策略。

請在安裝後，從 Web 主控台進行網頁信譽評等策略設定。Apex One 管理員通常會針對外部用戶端設定較嚴格的策略。

網頁信譽評等策略是 Apex One 用戶端樹狀結構中的精細設定。對所有用戶端、用戶端群組或個別用戶端強制執行特定的策略。

啟動網頁信譽評等服務策略時，請務必安裝主動雲端截毒技術伺服器（整合式或獨立式），並將其新增至 Apex One Web 主控台上的主動雲端截毒技術來源清單。Security Agent 會將網頁信譽評等查詢傳送至伺服器，以驗證使用者正在存取之網站的安全性。

注意

整合式伺服器會與 Apex One 伺服器一起安裝。如需詳細資訊，請參閱安裝整合式主動雲端截毒技術伺服器 第 2-17 頁。獨立式伺服器需個別安裝。

伺服器驗證憑證

安裝程式會在安裝期間嘗試偵測先前存在的驗證憑證。如果先前存在的憑證存在，Apex One 將自動對應「伺服器驗證憑證」畫面上的檔案。如果先前存在的憑證不存在，Apex One 會預設選取「產生新的驗證憑證」選項。

Apex One 使用公開金鑰密碼編譯來驗證 Apex One 伺服器在用戶端上開始的通訊。使用公開金鑰密碼編譯時，伺服器可以保留私密金鑰並將公開金鑰部署到所有用戶端。用戶端使用公開金鑰確認輸入通訊是由伺服器開始的且有效。如果驗證成功，用戶端會發出回應。

注意

Apex One 不會驗證用戶端在伺服器上開始的通訊。

Apex One 可在安裝期間產生驗證憑證，或是管理員可從其他 Apex One 伺服器匯入先前存在的驗證憑證。

管理員帳號密碼

請指定用於存取 Web 主控台以及結束和解除安裝 Security Agent 的密碼。

存取 Web 主控台

安裝程式會在安裝期間建立 root 帳號。root 帳號具備所有 Apex One Web 主控台功能的完整存取權限。管理員也可以使用此帳戶登入，然後建立自訂的使用者帳號，供其他使用者用來登入 Web 主控台。視使用者帳號的存取權限而定，使用者可以設定或檢視 Web 主控台的一個或多個功能。

請指定只有 Apex One 管理員才知道的密碼。如需協助重設忘記的密碼，請聯絡您的支援供應商。

結束並解除安裝 Security Agent

請指定密碼，以防止未經授權解除安裝或結束 Security Agent。只有在 Security Agent 功能發生問題時，才能解除安裝或結束 Security Agent，並立即進行安裝/重新載入。

Apex One 程式捷徑

接受預設資料夾名稱、指定新名稱，或選取安裝程式要新增程式捷徑的現有資料夾。

安裝資訊

此畫面提供安裝設定的摘要。檢視安裝資訊，如果要變更任何一項設定或選項，請點選「上一步」。如果要開始安裝，請點選「安裝」。

已完成執行安裝精靈

安裝完成後，請檢視 Readme 檔中有關產品與已知問題的基本資訊。

還原您備份至下列位置的鑑識資料夾和資料庫：

```
<Apex One 伺服器安裝資料夾>\PCCSRV\Private\
```

管理員可以啟動 Web 主控台，開始進行 Apex One 設定。

第 3 章

升級 Trend Micro Apex One

本章說明升級 Trend Micro Apex One™ 的步驟。

本章內容：

升級考量

重要

如果您升級到 Apex One，Control Manager 會安裝在同一部伺服器電腦上，對 Apex One 和 Apex Central 的單一伺服器電腦支援取決於您啟動的功能。

如需詳細資訊，請疑至 https://success.trendmicro.com/dcx/s/solution/000267022?language=en_US。

此版本的 Apex OneService Pack 1 支援從 Apex One 升級。

注意

趨勢科技強烈建議先對目前的 Apex One 伺服器套用所有可用的修補程式與 HotFix，然後才執行升級。

請造訪下列網站，以取得 Apex One 系統需求的完整清單：

https://docs.trendmicro.com/en-us/home.aspx

在升級 Apex One 伺服器和 Security Agent 時，請考量下列事項：

- IPv6 支援 第 3-2 頁
- Trend Micro Apex One 設定與組態 第 3-3 頁
- 在升級期間部署掃瞄方法 第 3-4 頁

IPv6 支援

Apex One 伺服器和用戶端升級的 IPv6 需求如下：

- 伺服器必須已使用 IIS Web 伺服器。
- 指派 IPv6 位址給伺服器。此外，伺服器必須由其主機名稱識別，偏好使用其完整網域名稱 (FQDN)。如果伺服器是由其 IPv6 位址識別，則目前由該伺服器管理的所有用戶端便無法連線到伺服器。如果伺服器是由其 IPv4 位址識別，則該伺服器無法將用戶端部署到純 IPv6 端點。

- 確認可以使用諸如 ping 或 nslookup 等命令擷取主機的 IPv6 或 IPv4 位址。

Trend Micro Apex One 設定與組態

在升級 Trend Micro Apex One 伺服器之前，請先備份 Trend Micro Apex One 資料庫與重要組態設定檔。

秘訣

這個版本的 Trend Micro Apex One 提供了備份機制，以備還原之用。如果您並不打算在安裝期間使用自動化備份，請執行手動資料庫備份。

備份與恢復 Apex One 資料庫和組態設定檔

步驟

1. 從 Microsoft 管理主控台停止 Apex One Master Service。
2. 停止 Apex One Apex Central Agent 服務。
3. 停止 Apex One Plug-in Manager 服務。
4. 停止 World Wide Web 發行服務。
5. 手動備份 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\SQ 中的下列資料庫檔案：
   - libSQLDatabaseUpgrade.dll
   - oscedbt.exe
6. 手動備份位於<伺服器安裝資料夾>\PCCSRV 中的下列檔案與資料夾：

注意

備份這些檔案和資料夾，以防遇到升級問題時，可以還原 Apex One。

   - ofcscan.ini：包含全域用戶端設定

- ous.ini：包含防毒元件部署的更新來源表格
- Private 資料夾：包含防火牆和更新來源設定
- Web\tmOPP 資料夾：包含病毒爆發防範設定
- Pccnt\Common\OfcPfw*.dat：包含防火牆設定
- Download\OfcPfw*.dat：包含防火牆部署設定
- Log 資料夾：包含系統事件和連線驗證記錄檔
- Virus 資料夾：包含隔離檔案
- HTTPDB 資料夾：包含 Apex One 資料庫

7. 升級 Apex One 伺服器。

注意

如果您遇到升級問題，請將步驟 6 的備份檔案複製到目標端點上的 <伺服器安裝資料夾>\PCCSRV 資料夾，然後重新啟動下列服務：

- World Wide Web 發行服務
- Apex One Plug-in Manager 服務
- Apex One Apex Central Agent 服務
- Apex One Master 服務

在升級期間部署掃瞄方法

在此 Apex One 版本中，管理員可以將 Security Agent 設定為使用雲端截毒掃瞄或標準掃瞄。

當您從舊版升級 Apex One 時，可以根據所選擇的升級方法，保留或自訂每個網域的掃瞄方法。請考慮下列項目：

- 如果打算直接在伺服器電腦上升級 Apex One 伺服器，則不需要從 Web 主控台變更掃瞄方法，因為用戶端會在升級之後保留其掃瞄方法設定。
- 打算將 Security Agent 移到 Apex OneService Pack 1 伺服器來進行升級時：

- 在 Apex One Service Pack 1 伺服器中，選擇手動用戶端分組。這種用戶端分組方法可讓您建立新網域。

注意

當使用自動用戶端分組時，請只在所有用戶端都已升級之後再啟動，以確保在用戶端升級期間會保留所有的掃瞄方法設定。

- 將舊版 Apex One 伺服器中的網域結構和掃瞄方法設定複製到 Apex OneService Pack 1 伺服器中。如果兩部伺服器上的網域結構和掃瞄方法設定並不相同，則有些移到 Apex OneService Pack 1 伺服器的 Security Agent 可能無法套用其原始掃瞄方法設定。

升級伺服器與用戶端之前

升級 Apex One 伺服器和用戶端之前，請注意下列事項：

1. 在 Apex One 伺服器上，手動建立下列鑑識資料夾和資料庫的備份，以取得資料外洩防護：

   - `<Apex One 伺服器安裝資料夾>\PCCSRV\Private\DLPForensicData`
   - `<Apex One 伺服器安裝資料夾>\PCCSRV\Private\DLPForensicDataTracker.db`

重要

記下檔案位置。完成升級程序後，請將鑑識資料夾和資料庫還原至同一位置。

2. 此安裝套件包含防火牆驅動程式的更新。如果您在目前的伺服器版本中已啟動 Apex One 防火牆，則部署此套件時可能會導致下列用戶端端點發生中斷：

   - 當「一般防火牆驅動程式」更新開始執行，用戶端端點會暫時中斷網路。中斷連線之前不會通知使用者。

     預設為啟動的 Apex One Web 主控台選項，會將一般防火牆驅動程式更新延後至用戶端端點重新啟動時進行。為避免斷線問題，請務必啟動這個選項。

若要檢查此選項的狀態：

a. 移至「用戶端 > 全域用戶端設定」，然後按一下「安全設定」標籤。

b. 移至「防火牆設定」區段。此選項為「只在系統重新啟動後更新 Apex One 防火牆驅動程式」。

- 部署此套件之後，TDI 驅動程式的上一版仍然存在於用戶端端點上，要等到重新啟動端點之後，才會載入新版本。使用者若未立即重新啟動，Security Agent 可能會發生問題。

  如果在 Web 主控台上已啟動顯示重新啟動通知訊息的選項，會提示使用者重新啟動。不過，不會再次提示決定要延後重新啟動的使用者。如果已關閉此選項，則完全不會通知使用者。

  依預設，會啟動顯示重新啟動通知訊息的選項。若要檢查此選項的狀態：

  - a. 移至「用戶端 > 全域用戶端設定」，然後按一下「用戶端控制」標籤。

    b. 移至「警訊設定」區段。選項為「如果端點需要重新啟動以載入核心模式驅動程式，則會顯示通知訊息」。

3. 下列情況 Apex One 伺服器無法升級至此版本：

   - 在伺服器升級時，用戶端正在執行 Login Script (`AutoPcc.exe`)。在升級伺服器之前，請確定沒有用戶端正在執行 Login Script。
   - 伺服器正在執行資料庫相關工作。升級前，請先檢查伺服器資料庫 (`DbServer.exe`) 的狀態。例如，開啟「Windows 工作管理員」，並確認 `DbServer.exe` 的 CPU 使用率為 00。如果 CPU 使用率較高，請等候使用率變成 00，這表示資料庫相關工作已完成。如果您執行升級並遭遇升級問題，則可能是資料庫檔案已遭到鎖定。此時，請重新啟動伺服器電腦來解除鎖定檔案，然後再次執行升級。

請使用下列其中一種升級方法：

- 升級方法 1：關閉自動用戶端升級 第 3-7 頁
- 升級方法 2：升級更新代理程式 第 3-8 頁

升級方法 1：關閉自動用戶端升級

關閉自動用戶端升級後，可先升級伺服器，然後升級用戶端群組。當要升級大量用戶端時，可以使用此升級方法。

第 1 階段：設定 Apex One 伺服器上的更新設定

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 () 以選取所有用戶端。
3. 按一下「設定 > 權限和其他設定」，然後移至「其他設定」標籤。
4. 在「Security Agent 僅會更新下列元件」下拉式清單中，選取「病毒碼檔案」。
5. 請點選「套用至所有用戶端」。

   在複雜的網路環境上且用戶端眾多的情況下，可能需要一些時間才能將設定部署到線上用戶端。在升級之前，請預留足夠的時間，以便讓設定部署到所有用戶端。未套用設定的 Security Agent 會自動升級。

第 2 階段：升級 Apex One 伺服器

如需升級 Apex One 伺服器的詳細資訊，請參閱執行本機升級 第 3-17 頁。

在完成安裝之後，請立即使用 Web 主控台來進行 Apex One 伺服器設定，然後再升級用戶端。

如需有關如何進行 Apex One 設定的詳細指示，請參閱《管理手冊》或「伺服器線上說明」。

第 3 階段：升級 Security Agent

步驟

1. 移至「更新 > 用戶端 > 自動更新」，並確保已啟動以下選項：
   - 在 Apex One 伺服器下載新元件之後，立即在用戶端開始元件更新
   - 讓用戶端在重新啟動並連線至 Apex One 伺服器後開始元件更新（不包括單機用戶端）
2. 移至「用戶端 > 用戶端管理」。
3. 在用戶端樹狀結構中，選取您要升級的用戶端。您可以選取一個或數個網域，或一個網域內的個別/所有用戶端。
4. 按一下「設定 > 權限和其他設定」，然後移至「其他設定」標籤。
5. 在「Security Agent 僅會更新下列元件」下拉式清單中，選取「所有元件（包括 Hotfix 和用戶端程式）」。
6. 請點選「儲存」。
7. 檢查升級結果。
   - 線上用戶端 第 3-12 頁
   - 離線用戶端 第 3-13 頁
   - 單機（行動）用戶端 第 3-13 頁
8. 重新啟動用戶端端點，完成用戶端的升級。
9. 請重複步驟 2 到步驟 8 直至所有用戶端都已升級。

升級方法 2：升級更新代理程式

如果要從更新代理程式更新大量用戶端，可以使用此升級方法。這些用戶端將從各自的更新代理程式進行升級。

不是從更新代理程式更新的 Security Agent 將從 Apex One 伺服器進行升級。

第 1 階段：設定 Apex One 伺服器上的更新設定

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 () 以選取所有用戶端。
3. 按一下「設定 > 權限和其他設定」，然後移至「其他設定」標籤。
4. 在「Security Agent 僅會更新下列元件」下拉式清單中，選取「病毒碼檔案」。
5. 請點選「套用至所有用戶端」。

   在複雜的網路環境上且用戶端眾多的情況下，可能需要一些時間才能將設定部署到線上用戶端。在升級之前，請預留足夠的時間，以便讓設定部署到所有用戶端。未套用設定的 Security Agent 會自動升級。

第 2 階段：升級 Apex One 伺服器

如需升級 Apex One 伺服器的詳細資訊，請參閱執行本機升級 第 3-17 頁。

在完成安裝之後，請立即使用 Web 主控台來進行 Apex One 伺服器設定，然後再升級用戶端。

如需有關如何進行 Apex One 設定的詳細指示，請參閱《管理手冊》或「伺服器線上說明」。

第 3 階段：升級更新代理程式

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，選取要升級的更新代理程式。

秘訣

如果要更快地找出更新代理程式，請選取網域，移至用戶端樹狀結構頂端的「用戶端樹狀結構檢視」，然後選取「更新代理程式檢視」。

3. 按一下「設定 > 權限和其他設定」，然後移至「其他設定」標籤。
4. 在「Security Agent 僅會更新下列元件」下拉式清單中，選取「所有元件（包括 Hotfix 和用戶端程式）」。
5. 請點選「儲存」。
6. 移至「更新 > 用戶端 > 手動更新」。
7. 選取「手動選取用戶端」選項，然後請點選「選取」。
8. 在開啟的用戶端樹狀結構中，選擇要升級的更新代理程式。

秘訣

如果要更快地找出更新代理程式，請選取網域，移至用戶端樹狀結構頂端的「用戶端樹狀結構檢視」，然後選取「更新代理程式檢視」。

9. 請點選用戶端樹狀結構頂端的「開始更新」。
10. 檢查升級結果。
    - 在開始元件升級後，線上更新代理程式會立即進行更新。
    - 離線「更新代理程式」會在上線後開始升級。
    - 單機（先前稱為行動）更新代理程式會在上線後升級，或者「更新代理程式」若有預約更新權限，則會在執行預約更新時升級。
11. 重新啟動更新代理程式的端點，完成用戶端的升級。
12. 請重複步驟 1 到步驟 11，直到所有更新代理程式都已升級。

第 4 階段：進行更新代理程式設定

步驟

1. 移至「用戶端 > 用戶端管理」。
2. 在用戶端樹狀結構中，選取要升級的更新代理程式。

   

   秘訣

   如果要更快地找出更新代理程式，請選取網域，移至用戶端樹狀結構頂端的「用戶端樹狀結構檢視」，然後選取「更新代理程式檢視」。
3. 請確定「更新代理程式」具有最新的元件。
4. 按一下「設定 > 更新代理程式設定」。
5. 選取下列選項：
   - 元件更新
   - 網域設定
   - Security Agent 和 HotFix
6. 請點選「儲存」。

   請等候更新代理程式完成用戶端的下載，再繼續進行第 5 階段。
7. 請重複步驟 1 到步驟 6 直至所有更新代理程式都已完成必要的設定。

第 5 階段：升級 Security Agent

步驟

1. 移至「更新 > 用戶端 > 自動更新」，並確保已啟動以下選項：
   - 在 Apex One 伺服器下載新元件之後，立即在用戶端開始元件更新
   - 讓用戶端在重新啟動並連線至 Apex One 伺服器後開始元件更新（不包括單機用戶端）

2. 移至「用戶端 > 用戶端管理」。
3. 在用戶端樹狀結構中，選取您要升級的用戶端。您可以選取一個或數個網域，或一個網域內的個別/所有用戶端。
4. 按一下「設定 > 權限和其他設定」，然後移至「其他設定」標籤。
5. 在「Security Agent 僅會更新下列元件」下拉式清單中，選取「所有元件（包括 Hotfix 和用戶端程式）」。
6. 請點選「儲存」。
7. 檢查升級結果。
   - 線上用戶端 第 3-12 頁
   - 離線用戶端 第 3-13 頁
   - 單機（行動）用戶端 第 3-13 頁
8. 重新啟動用戶端端點，完成用戶端的升級。
9. 請重複步驟 2 到步驟 8 直至所有用戶端都已升級。

升級結果

線上用戶端

注意

在升級後重新啟動用戶端端點。

- 自動升級

  發生下列任何一個事件時，線上用戶端便會開始升級：

  - Apex One 伺服器下載新的元件，並通知用戶端進行更新。
  - 用戶端會重新載入。
  - 用戶端會重新啟動，然後連線至 Apex One 伺服器。

- 預約更新會在用戶端端點上執行（僅限於具有預約更新權限的用戶端）。

- 手動升級

  如果上述事件皆未發生，請執行下列任一工作立即升級用戶端：

  - 建立並部署 EXE 或 MSI Security Agent 套件。

    

    注意

    如需建立用戶端套件的指示，請參閱《管理手冊》。

  - 指示使用者在用戶端端點上執行「立即更新」。
  - 以滑鼠右鍵按一下 `AutoPcc.exe`，然後選取「以系統管理員身分執行」。
  - 開始手動用戶端更新。

  如果要開始手動更新：

  1. 瀏覽至「更新 > 用戶端 > 手動更新」。
  2. 選取「手動選取用戶端」選項，然後請點選「選取」。
  3. 在開啟的用戶端樹狀結構中，選擇要升級的用戶端。
  4. 請點選用戶端樹狀結構頂端的「開始元件更新」。

離線用戶端

離線用戶端會在上線後升級。

單機（行動）用戶端

單機用戶端（先前稱為行動用戶端）會在上線後升級，或者用戶端若有預約更新權限，則會在執行預約更新時升級。

升級方法 3：將用戶端移至 Apex One Service Pack 1 伺服器

執行 Apex One Service Pack 1 伺服器的全新安裝，然後將用戶端移至此伺服器。當您移動用戶端時，用戶端會自動升級為 Apex One Service Pack 1。

第 1 階段：執行 Apex One 伺服器的全新安裝，然後進行更新設定

步驟

1. 執行 Apex One Service Pack 1 伺服器的全新安裝。

   如需詳細資訊，請參閱安裝程式 第 2-8 頁。

2. 登入 Web 主控台。
3. 移至「更新 > 用戶端 > 自動更新」，並確保已啟動以下選項：
   - 在 Apex One 伺服器下載新元件之後，立即在用戶端開始元件更新
   - 讓用戶端在重新啟動並連線至 Apex One 伺服器後開始元件更新（不包括單機用戶端）
4. 移至「用戶端 > 用戶端管理」。
5. 在用戶端樹狀結構中，請點選根網域圖示 () 以選取所有用戶端。
6. 按一下「設定 > 權限和其他設定」，然後移至「其他設定」標籤。
7. 在「Security Agent 僅會更新下列元件」下拉式清單中，選取「所有元件（包括 Hotfix 和用戶端程式）」。
8. 請點選「套用至所有用戶端」。
9. 記錄下列 Apex OneService Pack 1 伺服器資訊。移動用戶端時，在舊版 Apex One 伺服器上指定此資訊：
   - 端點名稱或 IP 位址
   - 伺服器監聽通訊埠

如果要檢視伺服器監聽通訊埠，請瀏覽至「管理 > 設定 > 用戶端連線」。通訊埠號碼會顯示在畫面上。

第 2 階段：升級 Security Agent

步驟

1. 在舊版伺服器的 Web 主控台上，移至「更新 > 摘要」。
2. 請點選「取消通知」。此功能會清除伺服器通知佇列，以避免在將用戶端/代理程式移至 Apex One 伺服器時發生問題。

   

   警告!

   立即執行後續步驟。如果伺服器通知佇列在您移動用戶端/用戶端之前便已更新，用戶端/用戶端可能無法順利移動。

3. 移至「用戶端 > 用戶端管理」。
4. 在用戶端樹狀結構中，選取您要升級的用戶端。請僅選取線上用戶端，因為離線與行動用戶端無法移動。
5. 按如下所示移動用戶端：
   a. 請點選「管理用戶端樹狀結構 > 移動用戶端」。
   b. 在「將選取的用戶端移動到其他 Apex One 伺服器」下，指定 Apex One 伺服器電腦名稱/IP 位址與伺服器監聽通訊埠。
6. 請點選「移動」。

升級結果

- 線上用戶端會開始移動並升級。
- 管理離線與單機（之前稱為行動）用戶端的秘訣：
  - 關閉用戶端上的單機（之前稱為行動）模式以升級用戶端。
  - 如果是離線用戶端，請指示使用者要連線到網路，用戶端才能變成線上狀態。如果是長期離線的用戶端，請指示使用者從端點解除安裝用

戶端，然後使用合適的用戶端安裝方法（例如用戶端封裝程式）來安裝 Security Agent，如《管理手冊》中所述。

注意

重新啟動用戶端端點，完成用戶端的升級。

升級方法 4：啟動自動用戶端升級

將 Apex One 伺服器升級為此版本後，伺服器會立即通知它所管理的所有用戶端進行升級。

如果伺服器管理的用戶端數量不多，請考慮讓用戶端立即升級。您也可以使用先前所述的升級方法。

第 1 階段：設定 Apex One 伺服器上的更新設定

步驟

1. 移至「更新 > 用戶端 > 自動更新」，並確保已啟動以下選項：
   - 在 Apex One 伺服器下載新元件之後，立即在用戶端開始元件更新
   - 讓用戶端在重新啟動並連線到 Apex One 伺服器後開始元件更新（不包括單機用戶端）
2. 移至「用戶端 > 用戶端管理」。
3. 在用戶端樹狀結構中，請點選根網域圖示 () 以選取所有用戶端。
4. 按一下「設定 > 權限和其他設定」，然後移至「其他設定」標籤。
5. 在「Security Agent 僅會更新下列元件」下拉式清單中，選取「病毒碼檔案」。
6. 請點選「套用至所有用戶端」。

   在複雜的網路環境上且用戶端眾多的情況下，可能需要一些時間才能將設定部署到線上用戶端。在升級之前，請預留足夠的時間，以便讓設定部署到所有用戶端。未套用設定的 Security Agent 會自動升級。

第 2 階段：升級 Apex One 伺服器

如需升級 Apex One 伺服器的詳細資訊，請參閱執行本機升級 第 3-17 頁。

注意

為加快升級程序，在升級執行 Windows Server 2008 Standard（64 位元）的任何 Apex One 伺服器前，請先結束 Security Agent。

在完成安裝之後，請立即使用 Web 主控台來進行 Apex One 伺服器設定，然後再升級用戶端。

如需有關如何進行 Apex One 設定的詳細指示，請參閱《管理手冊》或「伺服器線上說明」。

升級結果

- 線上用戶端會在伺服器完成升級後立即升級。
- 離線用戶端會在上線後開始升級。
- 單機（先前稱為行動）用戶端會在上線後升級，或者用戶端若有預約更新權限，則會在執行預約更新時升級。

注意

重新啟動用戶端端點，完成用戶端的升級。

執行本機升級

在本機升級期間，Apex One 將套用舊版 Apex One 伺服器所使用的設定。有限的畫面子集合顯示，可讓您設定 Apex One Service Pack 1 所提供的新功能。

重要

升級 Apex One 伺服器之前，建立下列鑑識資料夾和資料庫的備份，以取得資料外洩防護：

- <Apex One 伺服器安裝資料夾>\PCCSRV\Private\DLPForensicData
- <Apex One 伺服器安裝資料夾>\PCCSRV\Private\DLPForensicDataTracker.db

記下檔案位置。完成升級程序後，請將鑑識資料夾和資料庫還原至同一位置。

授權合約

請仔細閱讀授權合約並接受授權合約條款，以繼續進行安裝。不接受授權合約條款便無法繼續進行安裝。

鑑識資料

在 Apex One 伺服器上，手動建立下列鑑識資料夾和資料庫的備份，以取得資料外洩防護：

- <Apex One 伺服器安裝資料夾>\PCCSRV\Private\DLPForensicData
- <Apex One 伺服器安裝資料夾>\PCCSRV\Private\DLPForensicDataTracker.db

重要

記下檔案位置。完成升級程序後，請將鑑識資料夾和資料庫還原至同一位置。

Security Agent 升級

安裝程式會評估目標端點資源。在升級期間，如果目標端點上存在舊版 Security Agent 程式，則會出現警告畫面。

啟動增強式防護

趨勢科技建議您在所有 Security Agent 上啟動勒索軟體和網路攻擊防護。

下表列出 Apex One Web 主控台針對每個設定啟動的功能。

設定	Web 主控台位置	功能
抵禦勒索軟體	「用戶端 > 用戶端管理 > 設定 > 行為監控設定 > 規則 > 惡意程式行為封鎖」區段	• 啟動惡意程式行為封鎖 • 要封鎖的安全威脅：已知和潛在安全威脅 • 保護文件以防止未經授權的加密或修改 • 啟動程式檢測，以偵測並封鎖遭到入侵的可執行檔 重要 啟動「抵禦勒索軟體」並不會自動啟動「未經授權的變更阻止服務」。如果您已關閉「未經授權的變更阻止服務」，則必須手動啟動此服務，Security Agent 才能抵禦勒索軟體攻擊。
抵禦網路攻擊	「用戶端 > 用戶端管理 > 設定 > 其他服務設定 > 可疑連線服務」區段	在「Windows 桌上型電腦」上啟動「可疑連線服務」
	「用戶端 > 用戶端管理 > 設定 > 「可疑連線設定」	• 偵測對全域 C&C IP 清單中的位址進行的網路連線：封鎖 • 使用惡意程式網路特徵鑑別來偵測連線：封鎖

資料庫備份

在升級期間，安裝程式會提供選項，讓您在升級至最新版本的 Apex One 之前先備份 Apex One 資料庫。您可以將此備份資訊用於還原目的。

注意

備份套件可能需要超過 300MB 的可用磁碟空間。

Endpoint Sensor 安裝

如果您整合了 Apex Central 並已購買 Endpoint Sensor 使用授權，請選取「安裝 Endpoint Sensor」以確保所有必要的 Endpoint Sensor 服務均可供 Security Agent 使用。

注意

只有下列平台正式支援這項功能：

- Windows 7 SP1
- Windows 8.1
- Windows10

下表概述安裝 Endpoint Sensor 服務所需的最低需求。

項目	需求	確認
Redis 服務	Apex One 伺服器電腦不能已安裝現有的 Redis 服務。您必須解除安裝任何現有的 Redis 服務，並允許安裝程式安裝新服務。	按一下「Endpoint Sensor 安裝」畫面上的「下一步」後
SQL Server 版本	• SQL Server 2017 • SQL Server 2016 SP1 注意 此功能不支援 SQL Server Express 版本。	按一下「Apex One 資料庫設定」畫面上的「下一步」後
資料庫組態設定	已啟動「搜尋的全文檢索和語意擷取」 如需有關啟動「搜尋的全文檢索和語意擷取」的詳細資訊，請參閱您的 SQL Server 文件。	按一下「Apex One 資料庫設定」畫面上的「下一步」後
	tempdb 資料庫的存取權（可存取資料庫維護功能）	無

注意

如果您不安裝 Endpoint Sensor 服務，但選取了已啟動「搜尋的全文檢索和語意擷取」的受支援 SQL Server，則日後使用 Endpoint Sensor 的唯一方法是前往 Windows「控制台」的「解除安裝或變更程式」畫面。

選取 Apex One 伺服器，然後按一下「變更」。

Apex One 資料庫設定

重要

如果您計劃使用 Endpoint Sensor 功能，您必須選取已正確備妥且版本受支援之 SQL Server 上的資料庫。

如需詳細資訊，請參閱 Apex One Endpoint Sensor 第 1-9 頁。

步驟

1. 在「SQL Server」旁邊，選取 Apex One 應使用的已存在的 SQL Server 安裝和資料庫執行個體。
2. 選取資料庫驗證方法。

   使用「Windows 帳號」登入伺服器時，Apex One 會套用目前登入之使用者的「使用者名稱」。

   domain_name\user_name 或 user_name

重要

使用者帳號必須屬於本機管理員群組或 Active Directory (AD) 內建管理員，而您必須使用 Windows「本機安全性原則」或「群組原則管理」主控台設定「使用者權限指派」中的下列原則：

- 以服務方式登入
- 以批次工作登入
- 允許本機登入

使用者帳號還必須具有下列資料庫角色：

- dbcreator
- bulkadmin
- db_owner

3. 指定 SQL Server 上 Apex One 的「資料庫名稱」。
4. 按「下一步」。

重要

如果您選擇安裝 Endpoint Sensor 服務，安裝程式會立即評估選取的 SQL Server 資料庫是否已正確設定，並且符合最低需求。如果 SQL Server 資料庫不符合需求，您必須選取其他 SQL Server 資料庫，或返回上一步並選擇不安裝 Endpoint Sensor。

Apex One Security Agent 部署

有數種方法可以安裝或升級 Security Agent。此畫面列出不同的部署方法，以及大約所需的網路頻寬。

使用此畫面可估計將 Security Agent 部署到目標用戶端時，所需的伺服器空間大小以及耗用的頻寬。

注意

所有這些安裝方法都需要目標端點上的本機管理員或網域管理員權限。

安裝資訊

此畫面提供安裝設定的摘要。檢視安裝資訊，如果要變更任何一項設定或選項，請點選「上一步」。如果要開始安裝，請點選「安裝」。

Edge Relay 伺服器更新

重要

僅當舊版 Apex One 伺服器擁有已註冊的 Edge Relay 伺服器時才會顯示。

Apex One 不支援 Edge Relay 伺服器的較舊 OfficeScan 版本。您必須安裝新的 Edge Relay 伺服器或升級現有的 Edge Relay 伺服器，才能保護外部部署 Security Agent。

安裝或升級 Edge Relay 伺服器之後，您要使用 Edge Relay 伺服器管理的所有 Security Agent 都必須直接連線至 Apex One 伺服器，才能取得最新的 Edge Relay 伺服器設定。

如需有關 Edge Relay 伺服器安裝或升級的詳細資訊，請參閱《Apex One 管理手冊》。

已完成執行安裝精靈

安裝完成後，請檢視 Readme 檔中有關產品與已知問題的基本資訊。

還原您備份至下列位置的鑑識資料夾和資料庫：

<Apex One 伺服器安裝資料夾>\PCCSRV\Private\

管理員可以啟動 Web 主控台，開始進行 Apex One 設定。

第 4 章

安裝後的工作

Apex One 伺服器安裝完成之後，請執行下列工作。

本章內容：

確認伺服器安裝或升級

完成安裝或升級後，請驗證下列項目：

表 4-1. 安裝 Apex One 後要確認的項目

要確認的項目	詳細資訊
Apex One 伺服器捷徑	趨勢科技 Apex One 伺服器捷徑會出現在伺服器電腦的 Windows「開始」功能表上。
程式清單	趨勢科技 Apex One 伺服器會列在伺服器電腦「控制台」上的「新增/移除程式」清單中。
Apex One Web 主控台	在 Internet Explorer 瀏覽器中輸入下列 URL： • HTTPS 連線：`https://<Apex One 伺服器名稱>:<通訊埠號碼>/officescan` 其中 `<Apex One 伺服器名稱>` 是 Apex One 伺服器的名稱或 IP 位址。 Web 主控台登入畫面隨即顯示。

要確認的項目	詳細資訊
Apex One 伺服器服務	Microsoft Management Console 中會顯示下列 Apex One 伺服器服務： • Apex One Active Directory Integration Service：如果 Active Directory 整合和以角色為基礎的管理功能運作正常，將會顯示此服務。 • Apex One Apex Central Agent：如果已向 Apex Central 註冊 Apex One 伺服器，則此服務的狀態應為「已啟動」。 • Apex One Deep Discovery Service：此服務的狀態應為「已啟動」。 • Apex One Master Service：此服務的狀態應為「已啟動」。 • Apex One Log Receiver Service：此服務的狀態應為「已啟動」。 • Apex One Plug-in Manager：此服務的狀態應為「已啟動」。 • Trend Micro Smart Protection Query Handler：此服務的狀態應為「已啟動」。 • Trend Micro Smart Protection Server：此服務的狀態應為「已啟動」。 • Trend Micro Local Web Classification Server:如果安裝期間已啟動網頁信譽評等服務，則此服務的狀態應為「已啟動」。
Apex One 伺服器程序	當您開啟「Windows 工作管理員」時，DBServer.exe 正在執行中：
伺服器安裝記錄檔	伺服器安裝記錄檔 (OFCMAS.LOG) 存在於 `%windir%` 中。

登錄機碼	存在下列登錄機碼：
	• 32 位元平台：
	`HKEY_LOCAL_MACHINE\Software\TrendMicro\OfficeScan`
	• 64 位元平台：
	`HKEY_LOCAL_MACHINE\Software\Wow6432Node\TrendMicro\OfficeScan`

程式資料夾	Apex One 伺服器檔案位於 <伺服器安裝資料夾> 下。

確認整合式主動雲端截毒技術伺服器安裝

Apex One 會在全新安裝期間，自動安裝整合式主動雲端截毒技術伺服器。

步驟

1. 在伺服器 Web 主控台上，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「標準清單」連結。
3. 在開啟的畫面上，請點選「整合式主動雲端截毒技術伺服器」。
4. 在顯示的畫面上，請點選「測試連線」。

   應可與整合式伺服器成功連線。

更新 Apex One 伺服器

Apex One 安裝完畢後，請更新伺服器上的元件。

注意

本節說明手動更新的執行。如需有關預約更新和更新組態的詳細資訊，請參閱「伺服器線上說明」。

步驟

1. 登入 Web 主控台。
2. 在主功能表上，按一下「更新 > 伺服器 > 手動更新」。

   會出現「手動更新」畫面，顯示最新的元件、其版本號碼以及最近更新日期。
3. 選取要更新的元件。
4. 請點選「更新」。伺服器會檢查更新伺服器是否有更新元件，電腦會顯示更新進度和狀態。

檢查預設設定

Apex One 會使用預設設定進行安裝。如果這些設定不符合您的安全需求，請在 Web 主控台修改設定。如需有關 Web 主控台可用設定的詳細資訊，請參閱「伺服器線上說明」和《管理手冊》。

掃瞄設定

Apex One 提供多種掃瞄類型，以保護端點不受安全威脅的侵襲。請移至「用戶端 > 用戶端管理」，然後請點選「設定 > {掃瞄類型}」，來從 Web 主控台修改掃瞄設定。

用戶端 設定

Apex One 提供多種設定類型，可套用到所有已向伺服器註冊的用戶端或所有具備特定權限的用戶端。在 Web 主控台中移至「用戶端 > 全域用戶端設定」來修改用戶端設定。

用戶端權限

預設的用戶端權限包括在 Security Agent 端點上顯示系統匣圖示。從 Web 主控台修改預設用戶端權限。

1. 移至用戶端 > 用戶端管理。
2. 請點選「設定 > 權限和其他設定」。

向 Apex Central 註冊 Apex One

當 Apex Central 伺服器管理新安裝的 Apex One 伺服器時，請在安裝後向 Apex Central 註冊 Apex One。

注意

Apex Central 註冊只適用於新安裝的 Apex One 伺服器。

在 Apex One Web 主控台上，移至「管理 > 設定 > Apex Central」。

如需此程序的相關資訊，請參閱 *Apex One* 伺服器說明或《*Apex One* 管理手冊》。

第 5 章

解除安裝 Apex One

本章說明解除安裝 Apex One 伺服器的步驟。

本章內容：

解除安裝考量

當使用 Apex One 發生問題時，請使用解除安裝程式安全地從 端點 移除 Apex One 伺服器。在解除安裝伺服器之前，請將它所管理的用戶端移至其他 Apex One 伺服器。

在解除安裝 Apex One 伺服器之前

使用解除安裝程式安全地移除 Apex One 伺服器。

在解除安裝伺服器之前，請將它所管理的用戶端移至相同版本的其他 Apex One 伺服器。請考慮備份伺服器資料庫與組態檔，以便稍後重新安裝該伺服器。

將用戶端移至其他伺服器

Apex One Web 主控台提供您一個選項，讓您將該伺服器所管理的用戶端移至其他伺服器。

步驟

1. 記下其他伺服器的下列資訊。移動用戶端時需要此資訊。
   - 端點名稱或 IP 位址
   - 伺服器監聽通訊埠

   如果要檢視伺服器監聽通訊埠，請移至「管理 > 設定 > 用戶端連線」。通訊埠號碼會顯示在畫面上。
2. 在您要解除安裝之伺服器的 Web 主控台中，移至「用戶端 > 用戶端管理」。
3. 在用戶端樹狀結構中，選取要移動的用戶端，然後按一下「管理用戶端樹狀結構 > 移動用戶端」。
4. 在「將選取的用戶端移動到其他 Apex One 伺服器」下，指定其他 Apex One 伺服器的伺服器電腦名稱/IP 位址與伺服器監聽通訊埠。
5. 請點選「移動」。

所有用戶端都已移動完畢，且已由其他伺服器進行管理時，可以安全地解除安裝 Apex One 伺服器。

備份與恢復 Apex One 組態設定檔

在解除安裝 Apex One 伺服器之前，請先備份重要的組態設定檔。

注意

在執行解除安裝程序期間，Apex One 會為您提供不刪除 SQL 資料庫的選項。

步驟

1. 從 Microsoft Management Console 停止 Apex One Master Service。
2. 手動備份位於 <伺服器安裝資料夾>\PCCSRV 中的下列檔案與資料夾：
   - ofcscan.ini：包含全域用戶端設定
   - ous.ini：包含防毒元件部署的更新來源表格
   - Private 資料夾：包含防火牆和更新來源設定
   - Web\tmOPP 資料夾：包含病毒爆發防範設定
   - Pccnt\Common\OfcPfw*.dat：包含防火牆設定
   - Download\OfcPfw.dat:包含防火牆部署設定
   - Log 資料夾：包含系統事件和連線驗證記錄檔
   - Virus 資料夾：包含隔離檔案
3. 解除安裝 Apex One 伺服器。

   如需詳細資訊，請參閱解除安裝 Apex One 伺服器 第 5-4 頁。
4. 執行全新安裝。

   如需詳細資訊，請參閱安裝程式 第 2-8 頁。
5. 安裝程式結束後，開啟 Microsoft Management Console (services.msc)。

6. 以滑鼠右鍵按一下「Apex One Master Service」，然後按一下「停止」。
7. 將備份檔案複製到目標端點上的 <伺服器安裝資料夾>\PCCSRV 資料夾。
8. 重新啟動 Apex One Master Service。

解除安裝 Apex One 伺服器

請使用解除安裝程式來解除安裝 Apex One 伺服器與整合式主動雲端截毒技術伺服器。

如果解除安裝程式發生問題，請手動解除安裝伺服器。

注意

如需解除安裝 Security Agent 的指示，請參閱《管理手冊》。

使用解除安裝程式來解除安裝 Apex One 伺服器

步驟

1. 執行解除安裝程式。存取解除安裝程式的方式有兩種。
   - 方法 A
     a. 在 Apex One 伺服器電腦上，按一下「開始 > 程式集 > Trend Micro Apex One 伺服器 > 解除安裝 Apex One」。會出現確認畫面。
     b. 請點選「是」。伺服器解除安裝程式會提示您輸入管理員密碼。
     c. 輸入管理員密碼，然後請點選「確定」，伺服器解除安裝程式就會開始移除伺服器檔案。接著會出現確認訊息。
     d. 請點選「確定」以關閉解除安裝程式。
   - 方法 B
     a. 按兩下 Windows「新增/移除程式」畫面上的 Apex One 伺服器程式。

b. 按一下「控制台 > 新增或移除程式」。找到並按兩下「Trend Micro Apex One 伺服器」。遵循畫面上的指示，直到系統提示您輸入管理員密碼。

c. 輸入管理員密碼，然後請點選「確定」，伺服器解除安裝程式就會開始移除伺服器檔案。接著會出現確認訊息。

d. 請點選「確定」以關閉解除安裝程式。

手動解除安裝 Apex One 伺服器

第 1 階段：解除安裝整合式主動雲端截毒技術伺服器

步驟

1. 開啟 Microsoft Management Console 並停止 Apex One Master Service。
2. 開啟命令提示字元，然後移至<伺服器安裝資料夾>\PCCSRV。
3. 執行下列命令：

   ```
   SVRSVCSETUP.EXE -uninstall
   ```

   此命令會解除安裝 Apex One 相關服務，但不會移除組態設定檔或 Apex One 資料庫。
4. 移至 <伺服器安裝資料夾>\PCCSRV\private，然後開啟 ofcserver.ini。
5. 修改下列設定：

   表 5-1. ofcserver.ini 設定

設定	指示
WSS_INSTALL=1	將 1 變更為 0
WSS_ENABLE=1	刪除此行
WSS_URL=https://<computer_name>:4345/tmcss/	刪除此行

6. 瀏覽至<伺服器安裝資料夾>\PCCSRV，然後開啟 OfUninst.ini。刪除下列各行：

```
[WSS_WEB_SERVER]

ServerPort=8082

IIS_VhostName=Smart Protection Server（整合式）

IIS_VHostIdx=5
```

注意

IIS_VHostidx 的值應與下行中指示的「isapi」值相同：

```
ROOT=/tmcss,C:\Program Files\Trend
Micro\OfficeScan\PCCSRV\WSS\isapi,,<值>
```

```
[WSS_SSL]

SSLPort=<SSL 通訊埠>
```

7. 開啟命令提示字元，然後移至<伺服器安裝資料夾>\PCCSRV。
8. 執行下列命令：

```
Svrsvcsetup -install

Svrsvcsetup -enablessl

Svrsvcsetup -setprivilege
```

9. 確認已移除下列項目：
   - Microsoft 管理主控台中的趨勢科技主動雲端截毒技術伺服器服務
   - 主動雲端截毒技術伺服器效能計數器
   - 主動雲端截毒技術伺服器（整合式）網站

第 2 階段：解除安裝 Apex One 伺服器

步驟

1. 開啟「登錄編輯程式」，並執行下列步驟：

警告!

下列步驟需要刪除登錄機碼。如果登錄變更不正確，可能會造成嚴重系統問題。請一律先製作備份副本，再進行任何登錄變更。如需詳細資訊，請參閱「登錄編輯程式說明」。

a. 移至 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\。

b. 確認已刪除 ofcservice 機碼集。

c. 移至 HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\OfficeScan\，然後刪除 OfficeScan 機碼集。

對於 64 位元端點，路徑為 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\OfficeScan\。

d. 移至 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\。刪除 OfficeScan Management Console-<伺服器名稱>資料夾。

2. 移至 <伺服器安裝資料夾>\PCCSRV 資料夾，然後取消共用 PCCSRV 資料夾。

3. 重新啟動伺服器電腦。

4. 移至 <伺服器安裝資料夾>\PCCSRV，然後刪除 PCCSRV 資料夾。

5. 從 Internet Information Services (IIS) 主控台刪除 Apex One 網站。

a. 開啟 IIS 主控台。

b. 展開 ServerName。

c. 如果您已將 Apex One 安裝在其他網站，請移至「網站」資料夾，然後刪除 Apex One。

d. 如果您已將 Apex One 虛擬目錄安裝在預設的網站下，請移至「預設的網站」，然後刪除 Apex One 虛擬目錄。

第 6 章

疑難排解資源

本章說明可用於疑難排解這個 Apex One 版本各種潛在使用問題的資源。

本章內容：

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 GUID 可確保趨勢科技可針對所收到要評估的檔案提供回應。

Case Diagnostic Tool

Trend Micro Case Diagnostic Tool (CDT) 會在問題發生時從客戶的產品中收集必要偵錯資訊，也會自動開啟產品的偵錯狀態並根據問題類別收集必要檔案。趨勢科技會使用這項資訊針對產品相關問題進行疑難排解。

如果要取得這項工具和相關文件，請聯絡您的經銷商。

趨勢科技效能調整工具

趨勢科技提供獨立式效能調整工具，來識別可能引起效能問題的應用程式。趨勢科技效能調整工具在試驗程序期間應在標準工作站映像和（或）少數目標工作站上執行，以事先獲得實際部署「行為監控」和「周邊設備存取控管」時發生的效能問題。

注意

趨勢科技效能調整工具只支援 32 位元平台。

識別佔用大量系統資源的應用程式

步驟

1. 請聯絡趨勢科技客服部門以取得「趨勢科技效能調整工具」。
2. 將 `TMPerfTool.exe` 從 `TMPerfTool.zip` 中解壓縮出來。
3. 將 `TMPerfTool.exe` 放在<用戶端安裝資料夾>或 `TMBMCLI.dll` 所在資料夾。
4. 以滑鼠右鍵請點選 `TMPerfTool.exe`，然後選取「以系統管理員身分執行」。

5. 閱讀並接受終端使用者合約，然後請點選「確定」。
6. 請點選「分析」。此工具會開始監控 CPU 使用狀況與事件負載。

   系統會以紅色反白顯示耗用大量系統資源的處理程序。

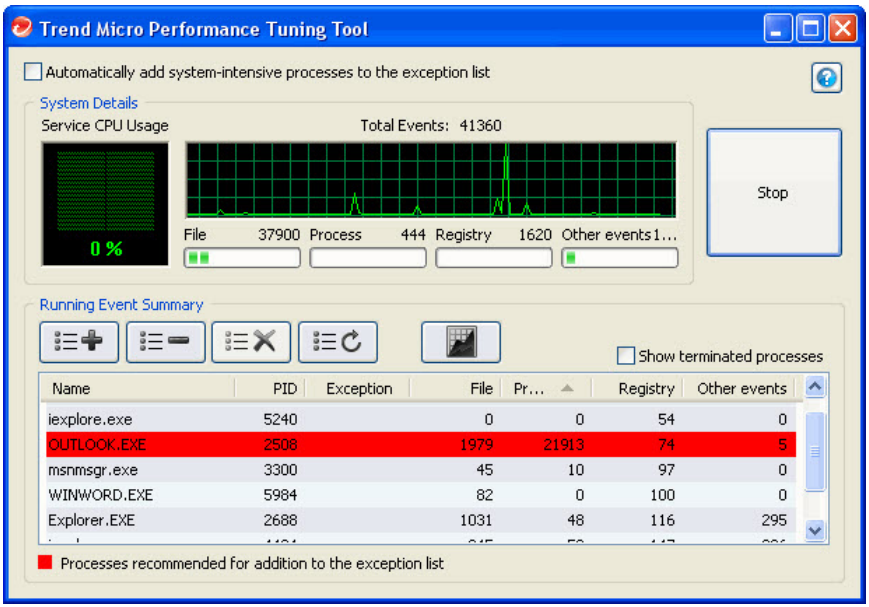

圖 6-1. 系統會反白顯示耗用大量系統資源的處理程序

7. 選取耗用大量系統資源的處理程序，然後按一下「新增至例外清單（允許）」按鈕（）。
8. 檢查系統或應用程式效能是否變好。
9. 如果效能變好，請再選取一次該處理程序，然後按一下「從例外清單移除」按鈕（）。
10. 如果效能再次變差，請執行下列步驟：
    a. 請記下應用程式的名稱。
    b. 請點選「停止」。

c. 按一下「產生報告」按鈕 ()，然後儲存 .xml 檔案。

d. 檢視系統識別為發生衝突的應用程式，然後將它們新增到「行為監控」例外清單。如需詳細資訊，請參閱《管理手冊》。

安裝記錄檔

使用 Apex One 自動產生的安裝記錄檔，即可對安裝問題進行疑難排解。

表 6-1. 安裝記錄檔

記錄檔	檔案名稱	位置
伺服器本機安裝/升級記錄檔	OFCMAS.LOG	%windir%
伺服器遠端安裝/升級記錄檔	OFCMAS.LOG（在您啟動安裝程式的端點上） OFCMAS.LOG（在目標端點上）	%windir%
Security Agent 安裝記錄檔	OFCNT.LOG	%windir%（適用於 MSI 套件以外的所有安裝方法） %temp%（適用於 MSI 套件安裝方法）

伺服器偵錯記錄檔

請先啟動偵錯記錄，再執行下列伺服器工作：

- 先解除安裝伺服器，然後再安裝一次。
- 將 Apex One 升級為新版本。
- 執行遠端安裝/升級（偵錯記錄功能會在您啟動安裝程式的端點上啟動，而不會在遠端端點上啟動）。

警告!

偵錯記錄檔可能會影響伺服器的效能，並且消耗大量的磁碟空間。務必僅在必要時啟動偵錯記錄，並且在不需要偵錯資料時立即關閉。如果記錄檔變得過大，請將其移除。

啟動 Apex One 伺服器電腦上的偵錯記錄

選項 1：

步驟

1. 登入 Web 主控台。
2. 在 Web 主控台的標題上，按一下「Apex One」中的「A」。這樣會開啟「除錯記錄檔設定」畫面。
3. 指定偵錯記錄檔設定。
4. 請點選「儲存」。
5. 檢查預設位置中的記錄檔 (ofcdebug.log)：<伺服器安裝資料夾>\PCCSRV\Log。

選項 2：

步驟

1. 將位於<伺服器安裝資料夾>>\PCCSRV\Private 中的「LogServer」資料夾複製到 C:\。
2. 建立名為 ofcdebug.ini 的檔案，其中包含下列內容：

```
[debug]

DebugLevel=9

DebugLog=C:\LogServer\ofcdebug.log

debugLevel_new=D
```

```
debugSplitSize=10485760

debugSplitPeriod=12

debugRemoveAfterSplit=1
```

3. 將 `ofcdebug.ini` 儲存到 `C:\LogServer`。
4. 執行適當工作（亦即重新安裝伺服器，升級為新的伺服器版本或執行遠端安裝/升級）。
5. 檢查 `C:\LogServer` 中的 `ofcdebug.log`。

注意

如果 Apex One 伺服器上存在 Security Agent，則該用戶端也會將它的偵錯記錄檔輸出到伺服器的偵錯記錄檔中。

用戶端 偵錯記錄檔

在安裝 Security Agent 之前啟動偵錯記錄。

警告!

偵錯記錄檔可能會影響用戶端的效能，並消耗大量的磁碟空間。務必僅在必要時啟動偵錯記錄，並且在不需要偵錯資料時立即關閉。如果記錄檔變得過大，請將其移除。

啟動 Security Agent 上的偵錯記錄

步驟

1. 建立名為 `ofcdebug.ini` 的檔案，其中包含下列內容：

```
[Debug]

Debuglog=C:\ofcdebug.log

debuglevel=9
```

```
debugLevel_new=D

debugSplitSize=10485760

debugSplitPeriod=12

debugRemoveAfterSplit=1
```

2. 傳送 `ofcdebug.ini` 給用戶端使用者，並指示他們將檔案儲存至 `C:\`。

   `LogServer.exe` 會自動在用戶端端點每次啟動時執行。

3. 如果要啟動偵錯記錄，請重新載入 Security Agent 或重新啟動端點。

   指示使用者「不要」關閉端點啟動時開啟的 `LogServer.exe` 命令視窗，因為這會提示 Apex One 停止偵錯記錄。如果使用者關閉命令視窗，可以執行位於 `\Security Agent\Temp` 的 `LogServer.exe` 以再次啟動偵錯記錄。

4. 在每個用戶端端點上，查看 `C:\` 中的 `ofcdebug.log`。

5. 如果要針對 Security Agent 關閉偵錯記錄功能，請刪除 `ofcdebug.ini`。

第 7 章

技術支援

瞭解下列主題：

疑難排解資源

聯絡技術支援之前，請考慮造訪下列趨勢科技線上資源。

使用支援入口網站

趨勢科技支援入口網站是全年無休的線上資源，包含有關常見和不常見問題的最新資訊。

步驟

1. 移至「https://success.trendmicro.com/tw/business-support」。
2. 從可用產品中進行選取，或請點選適當的按鈕來搜尋解決方案。
3. 使用「搜尋支援」方塊搜尋可用的解決方案。
4. 如果未找到解決方案，請點選「聯絡支援」，然後選取所需的支援類型。

秘訣

若要線上提交支援案例，請造訪下列 URL：

https://success.trendmicro.com/tw/sign-in

趨勢科技支援工程師會在 24 小時或更短時間內調查案例並對其進行回應。

安全威脅百科全書

現今的大多數惡意程式都包含混合安全威脅（合併了兩種或更多種技術），以略過電腦安全通訊協定。趨勢科技會使用建立自訂防範策略的產品來抵禦此複雜惡意程式。安全威脅百科全書提供了多種混合性安全威脅的名稱和癥狀的完整清單，包括已知惡意程式、垃圾郵件、惡意 URL 和已知弱點。

移至 https://www.trendmicro.com/vinfo/tw/threat-encyclopedia/malware/ 以瞭解更多資訊：

- 目前正在使用中或「擴散中」的惡意程式和惡意可攜式程式碼。
- 用於形成完整網頁攻擊過程的關聯安全威脅資訊頁面
- 有關目標攻擊和安全威脅的 Internet 安全威脅諮詢
- 網頁攻擊和線上趨勢資訊
- 每週惡意程式報告

聯絡趨勢科技

可以透過電話或電子郵件聯絡趨勢科技代表：

地址	趨勢科技股份有限公司 台北市敦化南路二段 198 號 8 樓
電話	(886) 2-23789666
網站	https://www.trendmicro.com
電子郵件信箱	企業授權用戶技術專線 Web mail：http://www.trend.com.tw/corpmail/

- 全球客戶服務據點：

  https://www.trendmicro.com/us/about-us/contact/index.html

  與台灣趨勢科技聯絡：

  http://www.trendmicro.tw/tw/about-us/contact/index.html

- 趨勢科技產品文件：

  https://docs.trendmicro.com/zh-tw/home.aspx

加速支援要求

為了提高解決問題的速度，現已提供下列資訊：

- 問題模擬的步驟
- 裝置或網路資訊

- 電腦品牌、型號以及連接的任何其他硬體或裝置
- 記憶體大小和可用硬碟空間
- 作業系統和 Service Pack 版本
- 安裝的用戶端版本
- 產品序號或啟動碼
- 安裝環境的詳細說明
- 已接收的任何錯誤訊息的確切文字

將可疑內容傳送到趨勢科技

有多個選項可供將可疑內容傳送到趨勢科技，以便進一步分析。

電子郵件信譽評等服務

查詢特定 IP 位址的信譽評等，並指定一個訊息轉移用戶端，以將其包含在全域核可清單中：

https://servicecentral.trendmicro.com/en-us/ers/

請參閱下列「常見問題集」項目，將訊息範例傳送給趨勢科技：

https://success.trendmicro.com/tw/solution/1112106

檔案信譽評等服務

收集系統資訊並將可疑檔案內容提交到趨勢科技：

https://success.trendmicro.com/tw/solution/1059565

記錄案例編號以供追蹤。

網頁信譽評等服務

查詢疑似網路釣魚網站的 URL 的安全分級和內容類型，或其他所謂「病媒」（間諜程式和惡意程式等 Internet 威脅的蓄意來源）：

https://global.sitesafety.trendmicro.com/

如果指定的分級不正確，請傳送重新分類要求到趨勢科技。

其他資源

除了解決方案和支援外，線上還提供許多其他實用資源，可讓您保持最新狀態、瞭解創新以及最新的安全趨勢。

下載專區

有時，趨勢科技可能會針對報告的已知問題發行修補程式，或是發行適用於特定產品或服務的升級。如果要瞭解是否有適用的修補程式，請移至：

https://downloadcenter.trendmicro.com/index.php?regs=tw

如果未套用修補程式（修補程式已過期），請開啟 Readme 檔以判斷其是否與您的環境相關。Readme 檔還包含安裝說明。

文件意見反應

趨勢科技始終力求改善其文件。如果您對本文件或趨勢科技的任何文件有任何疑問、意見或建議，請透過 https://docs.trendmicro.com/en-us/survey.aspx 聯絡我們。

附錄 A

部署範例

本節說明根據網路拓撲和可用網路資源來部署 Apex One 的方式。在公司中規劃部署 Apex One 時，請參考使用此方式。

基本網路

圖 1 說明 Apex One 伺服器與用戶端直接相連的基本網路。大多數企業網路都有這項組態設定，其中 LAN（和（或）WAN）存取速度為 10Mbps、100Mbps 或 1Gbps。在這種狀況下，符合 Apex One 系統需求並具備充足資源的端點，就是安裝 Apex One 伺服器的首選。

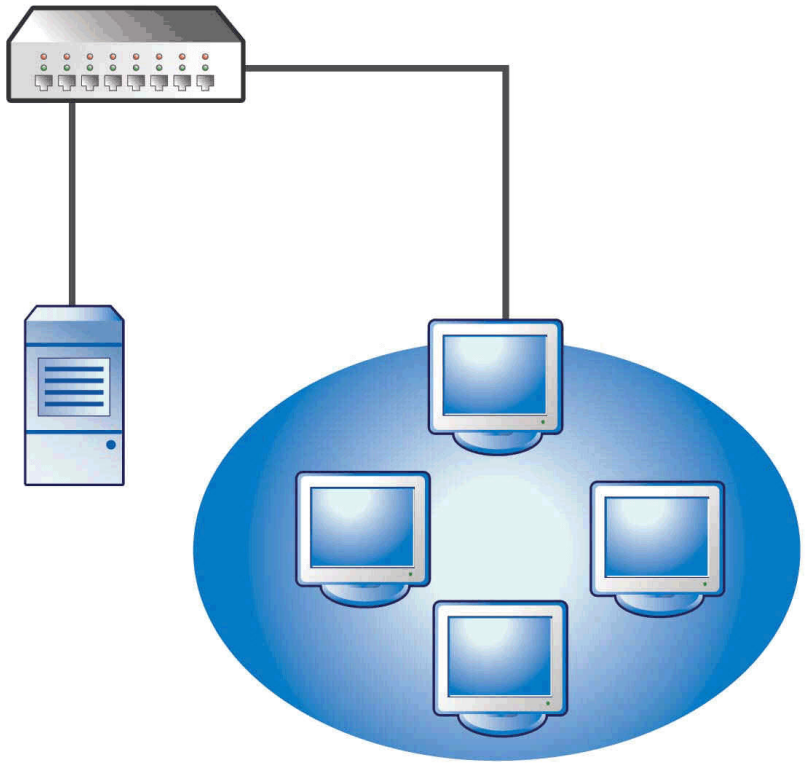

圖 A-1. 基本網路拓撲

多站台網路

如果網路具有多個無線網路存取點和多個頻寬不同的遠端站台：

- 就辦公室和網路頻寬分析合併點。
- 判斷每個辦公室目前的頻寬使用率。

如此便可更清楚地瞭解部署 Apex One 的最佳方式。圖 1 說明多站台網路拓撲。

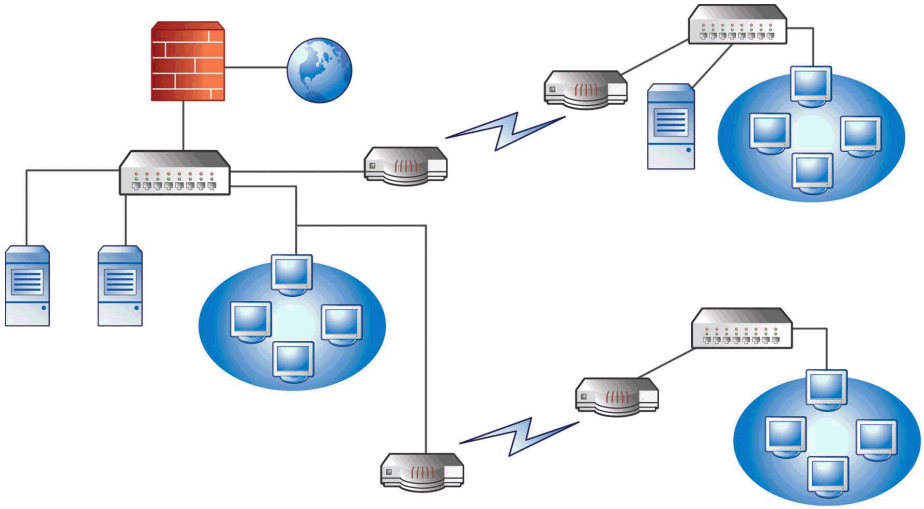

圖 A-2. 多站台網路拓撲

網路資訊：

- 遠端站台 1 在上班時間的 WAN 連結平均使用率約為 70%，而這個站台上有 35 個用戶端端點。
- 遠端站台 2 在上班時間的 WAN 連結平均使用率約為 40%，而這個站台上有 9 個用戶端端點。
- 伺服器 3 僅當成遠端站台 1 中群組的檔案與列印伺服器使用。這個端點可當成 Apex One 伺服器的候選安裝位置，但由於要多付管理費用，所以不

划算。所有伺服器都執行 Windows Server 2012。該網路使用 Active Directory，但主要用於網路驗證。

- 總公司、遠端站台 1 和遠端站台 2 中的所有用戶端端點都執行 Windows Server 2012 或 Windows 7。

準備多站台網路

步驟

1. 識別要安裝 Apex One 伺服器的端點。
2. 識別可用的用戶端安裝方法，並去除不符合需求的方法。如需有關用戶端安裝方法的詳細資訊，請參閱《管理手冊》。

   可能的安裝方法：

   - Login Script Setup

     如果因為本地傳輸無關緊要而使得原地沒有 WAN，則 Login Script Setup 的使用效果會很好。不過，如果有超過 50MB 的資料傳輸到每個端點，這個選項便不可行。

   - 從 Web 主控台進行遠端安裝

     這種方法對總公司所有連接 LAN 的端點都有效。因為這些端點都執行 Windows Server 2012，所以很容易將套件都部署到端點上。

     由於這兩個遠端站台之間的連結速度很低，所以如果是在上班時間部署 Apex One，這種部署方法可能會影響可用頻寬。在多數人已下班的非上班時間，使用整個連結容量來部署 Apex One。不過，如果使用者關閉端點，則無法成功將 Apex One 部署到這些端點。

   - Security Agent 套件部署

     如果要部署遠端站台，部署 Security Agent 套件似乎是最佳選擇。不過，遠端站台 2 沒有可適當促進用戶端套件佈署的本機伺服器。就所有選擇深入看來，這個選擇的適用範圍最能涵蓋大多數端點。

總公司部署

在總公司部署用戶端最簡單的方式，是從 Apex One Web 主控台進行遠端安裝。如需此程序的詳細資訊，請參閱《管理手冊》。

遠端站台 1 部署

如果要部署到遠端站台 1，則需要設定 Microsoft 的「分散式檔案系統」(DFS)。如需有關 DFS 的詳細資訊，請參閱 http://support.microsoft.com/?kbid=241452。設定 DFS 後，遠端站台 1 的伺服器 3 必須啟動 DFS，然後複製現有的 DFS 環境或建立新環境。

適合的部署方法是使用 Microsoft Installer (MSI) 套件格式來建立用戶端套件，並且將用戶端套件部署到 DFS。如需此程序的詳細資訊，請參閱《管理手冊》。由於套件會在下次預約更新期間複製到伺服器 3，因此部署用戶端套件對頻寬的影響會最小。

您也可以透過 Active Directory 部署用戶端套件。如需詳細資訊，請參閱《管理手冊》。

將 WAN 全面性元件更新的影響降到最低

步驟

1. 指定一個用戶端做為遠端站台 1 的「更新代理程式」。
   a. 登入 Web 主控台並瀏覽至「用戶端 > 用戶端管理」。
   b. 在用戶端樹狀結構中，選取要做為「更新代理程式」的用戶端，然後請點選「設定 > 更新代理程式設定」。
2. 選取遠端站台 1 中要從「更新代理程式」更新元件的用戶端。
   a. 瀏覽至「更新 > 伺服器 > 更新來源」。
   b. 選取「自訂更新來源」，然後請點選「新增」。
   c. 在顯示的畫面中，輸入遠端站台 1 中端點的 IP 位址範圍。

d. 選取「更新來源」，然後從下拉式清單中選取指定的「更新代理程式」。

遠端站台 2 部署

遠端站台 2 的關鍵問題在於頻寬很低。不過，雖然可用頻寬約為 154 Kbit，但在上班時間有 60% 的頻寬無人使用。

安裝 Security Agent 的最佳方式是使用遠端站台 1 中所用同一個 MSI 格式的用戶端套件。不過，由於沒有可用的伺服器，所以您無法使用「分散式檔案系統」(DFS)。

其中一個選項是使用協力廠商的管理工具，讓管理員在遠端端點上設定或建立共用目錄，而不需透過實體方式加以存取。在單一端點上建立共用目錄後，將用戶端套件複製到該目錄所需的管理費用，會比將用戶端安裝到九個端點還要少。

使用另一個 Active Directory 策略，不過請同樣不要將 DFS 共用指定為來源。

這些方法都可讓安裝傳輸保持在本端網路，將透過 WAN 的傳輸量降到最低。

如果要將透過 WAN 更新元件的影響降到最低，請將一個用戶端指定為「更新代理程式」。如需詳細資訊，請參閱遠端站台 1 部署 第 A-5 頁。

索引

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: APTM29870/231128