Apex One™
Apex Central™
標準安裝手冊(SOP)

企業資訊安全整體防護

端點安全

防護雲端

Web 安全

TREND MICRO SMART PROTECTION NETWORK™

目錄

第一章、 Apex One 全新安裝（建議作法） 4

1. 系統需求 4

2. 安裝 Apex One 伺服器 6

3. 安裝後檢查項目 19

第二章、 OfficeScan 伺服器『原機升級』Apex One 20

1. 可支援升級 OfficeScan 版本 20

2. 不支援升級的舊版作業系統用戶端建議作法 20

3. 升級前的檢查與考量事項 21

4. 升級至 Apex One 前的重要資料備份 24

5. 原機升級 Apex One 伺服器 29

第三章、 Apex Central 全新安裝步驟 36

1. 系統需求 36

2. 全新安裝步驟 37

第四章、 建議設定 44

1. 將 Apex One 註冊至 Apex Central 44

2. 啟用 iES 功能 49

3. 啟用 iVP 功能 54

4. 啟用 iAC 功能 59

第五章、 舊版 OfficeScan 用戶端升級 64

1. 方法一：自動升級 Security Agent 64

2. 方法二：透過更新代理程式升級 Security Agent 64

3. 方法三：將用戶端移轉至 Apex One 伺服器升級 67

第一章、 Apex One 全新安裝（建議作法）

1. 系統需求

A. 若欲啟用安裝 Endpoint Sensor (iES) 服務，資料庫需符合以下需求：

- 版本：SQL Server 2016 SP1 (或更新版本)，但不支援 SQL Server Express
- 先決條件設定：啟動「搜尋的全文檢索和語意擷取」 (Full-Text Search and Semantic Search Stored Procedures) 功能。
- SQL 定序(Collation) 必須使用預設值：「不區分大小寫(Case Insensitive)」。若要直接使用現有資料庫且定序(Collation)已經為:「區分大小寫(Case Sensitive)」將導致安裝中斷，因為 Apex 系列產品及 Endpoint Sensor 不支援該設定，請指向另一台 SQL 主機進行安裝。

B. Apex One 伺服器和 Security Agent 用戶端之間連線使用 SSL 加密通訊協定。

請務必確保 Apex One Server 與 Client 用戶端，都必須支援 TLS 1.2 安全通訊協定。

(微軟文章：檢查 TSL 1.2 是否啟用)

C. Windows 2012 R2 需先安裝 KB2919442 與 KB2919355 更新。

Windows 2016 (version 1607, build 14393)建議安裝 KB4093120 更新。

D. 不支援 SQL Server AlwaysOn

E. 不建議將 Apex One 和 Apex Central 安裝在同一主機。

Apex One 管理伺服器系統需求：

<table>
<tr><th>作業系統</th><th>處理器</th><th>記憶體</th><th>可用磁碟空間</th></tr>
<tr><td rowspan="3">• Windows Server 2012
• Windows Server 2012 R2
• Windows Server 2016
• Windows Server 2019</td><td>至少 1.86 GHz Intel™ Core™2 Duo
AMD™ 64 位元處理器
Intel 64 位元處理器</td><td>• 3 GB 以上 (不包含 iES)
• 8 GB 以上 (包含 iES)</td><td>• 7 GB 以上 (不包含 iES)
• 8 GB 以上 (包含 iES)</td></tr>
<tr><td colspan="3">IIS 設定需求</td></tr>
<tr><td colspan="3">• 一般 HTTP 功能
○ 靜態內容
○ 預設文件
○ 瀏覽目錄
○ HTTP 錯誤
• 安全性
○ Windows 驗證
○ 要求篩選
• 狀況及診斷
○ HTTP 紀錄
○ 要求監視器
• 效能
○ 靜態內容壓縮
• 應用程式開發
○ .NET 擴充性 3.x/4.x
○ ASP.NET 3.x/4.x
○ ASP
○ CGI
○ ISAPI 篩選器
○ ISAPI 擴充程式
• 管理工具
○ IIS 管理主控台
○ IIS 6 管理相容性
○ IIS 6 Metabase 相容性
○ IIS 6 WMI 相容性
○ IIS 6 指令碼工具
○ IIS 6 管理主控台</td></tr>
</table>

Apex One Security Agent 系統需求：

作業系統	處理器	記憶體	可用磁碟空間
• Windows 7 SP1 (x86/x64) • Windows 8.1 (x86/x64) • Windows 10 (x86/x64) • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019	32 位元：至少 1 GHz Intel™ Pentium 或同級 64 位元：至少 2 GHz Intel™ Pentium 或同級 AMD™ 64 位元處理器 Intel 64 位元處理器	• 2 GB 以上 (不包含 iES) • 2 GB 以上 (包含 iES)	• 1.5 GB 以上 (不包含 iES) • 2.0 GB 以上 (包含 iES)

請造訪下列網站，以取得系統需求和相容協力廠商產品的完整清單：

https://docs.trendmicro.com/all/ent/apex-one/2019/zh-tw/apexOne_2019_req.pdf

2. 安裝 Apex One 伺服器

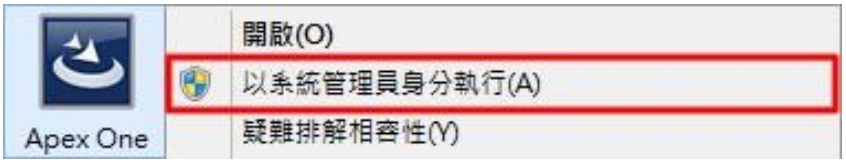
安裝前，請先妥善規劃以下設定，以備安裝過程使用（不建議安裝後異動或加入/移出網域）：

項目	預設值	設定需求
Apex One 啟動碼	無	OS-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
Apex One Server 名稱（server name）	主機名稱	讓用戶端找伺服器的目標位置，若名稱解析會有問題，請指定 IP 安裝。
Apex One Server 通訊埠（server port）	HTTP: 8080 HTTPS: 4343	供 Apex One 用戶端向 Server 溝通
用戶端通訊埠（agent port）	21112	供 Apex One server 通知用戶端
SQL 資料庫密碼	無	長度至少 8 碼，需要複雜度
Apex One 憑證備份密碼	無	長度至少 8 碼，需要複雜度
Apex One 網頁主控台密碼	無	供管理者登入使用
Apex One 用戶端卸載/移除密碼	無	Patch3 之後，需要複雜度

Apex One 伺服安裝程式下載位址：

https://www.trend.com.tw/support/downloads/Apex%20One/2019/TC/GM/apexone_2019_win_tc_gm_b1555.exe

(1) 執行安裝程式(右鍵以系統管理員身分執行)



(2) 歡迎畫面

(3) 授權合約 - 請仔細閱讀此合約

(4) 端點安裝前掃瞄 - 是否於安裝前掃瞄主機

(5) Proxy 伺服器 - 若伺服器主機存取 Internet 需透過 Proxy 請指定設定

(6) 產品啟動 - 輸入 Apex One 的啟動碼

(啟動碼格式：OS-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx)

(7) 安裝路徑 - 指定 Apex One (伺服器)的安裝路徑

(8) 伺服器識別 - 如果 DNS 無法解析 Apex One 伺服器名稱或是 Apex One 伺服器有多張網卡，

請設定 IP 位址來識別伺服器

(9) Web 伺服器 - 設定 Apex One IIS Web 伺服器設定

Apex One Server 一律使用 SSL 加密通訊協定與用戶端進行連線

(10) Endpoint Sensor 安裝 - 若有購買 Endpoint Sensor 授權且符合資料庫需求，可勾選安裝

(11) Apex One 資料庫設定 - 設定 Apex One 資料庫的名稱位置與驗證或是點選「瀏覽」找尋已安裝的 SQL Server（若是自定資料庫帳號，須確認該帳號具有 dbcreator、bulkadmin、db_owner 等資料庫角色）

(12) 設定完成後可利用「測試連線」按鈕確認與 SQL Server 連線狀況

(13) Apex One Security Agent 部署

(14) 安裝整合式主動雲端截毒技術伺服器 - 是否於主機安裝整合式伺服器

(15) 安裝 Security Agent - 選擇是否在主機上安裝 Apex One Security Agent

(16) Smart Feedback - 是否以匿名方式共享偵測資訊 (建議開啟)

(17) 安裝 Security Agent - 指定 Apex One Security Agent 的安裝路徑與通訊埠

Apex OneSecurity Agent 監聽通訊埠號碼預設為 21112，可自行指定。

(18) Apex One 防火牆 - 是否啟動 Apex One 防火牆 (伺服器預設不開啟)

(19) 間諜程式防護功能 - 是否開啟評估模式

評估模式是為了釐清自行開發程式是否會被偵測為間諜程式，因此設定間諜程式防護功能的評估時間。若沒有上述需求，卻開啟評估模式，將導致偵測到間諜程式，不會隔離(刪除)，出現持續偵測的狀況。

(20) 網頁信譽評等 - 啟動 Apex One 網頁信譽評等 (伺服器預設不開啟)

(21) 伺服器驗證憑證 - 設定 Apex OneSecurity Agent 與伺服器間的連線驗證憑證

(22) 管理員帳號密碼 - 指定 Web 主控台與 Security Agent 卸載/解除安裝的密碼

(23) Apex One 程式捷徑 - 設定程式於「開始」功能表的顯示名稱

(24) 安裝資訊 - 安裝前可檢視此次安裝的相關設定摘要

(25) 安裝成功訊息

3. 安裝後檢查項目

完成安裝後，請驗證下列項目：

要確認的項目	詳細資訊
Apex One Web 主控台	在瀏覽器(Edge 或 Chrome)中輸入下列 URL： https://< Apex One 伺服器名稱>:<通訊埠號碼>/officescan 例如： https://apexone.example.com:4343/officescan/ 或是 https://192.168.1.1:4343/officescan/

第二章、 OfficeScan 伺服器『原機升級』Apex One

1. 可支援升級 OfficeScan 版本

Apex One 伺服器支援從下列版本進行升級：

- OfficeScan XG SP1 Build 5684
- OfficeScan XG GM Critical Patch 1988
- OfficeScan 11.0 SP1 Build 6675

2. 不支援升級的舊版作業系統用戶端建議作法

註：OfficeScan XG（含 SP1）已經於 2021/3/31 終止技術支援

Apex One 不再支援 Windows 95、98、Me、Vista、XP、8、NT、2000、2003、2008 或 Itanium 架構平台。Windows 7 只支援 SP1 以上版本，2008 只支援 2008 R2 版本。請保留舊版的OfficeScan 伺服器來管理舊版作業系統用戶端。

3. 升級前的檢查與考量事項

(1) 確認欲升級 Apex One 的伺服器符合系統需求。

(2) 如果用戶端不能上網，且環境內只有整合式雲端伺服器，在原機升級的期間，用戶端將無法使用網頁信譽評等(WRS)及檔案信譽評等(FRS)。對使用者的影響是存取網站可能需要等 30 秒或是網站停止回應，掃描檔案僅有有限的病毒碼可以比對。

(3) 為避免更新後立即部署到全部用戶端，建議更新前先**停用用戶端自動更新 Hotfix**，再針對網域群組分批部署：

※分批部署的用意除了逐步觀察新版本對環境的影響之外，也是避免升級用戶端佔用頻寬影響日常維運。以下為參考傳輸量：

32 位元平台：

沒有啟動 iES 的用戶端：229.5MB

有啟動 iES 的用戶端：271.1MB

64 位元平台：

沒有啟動 iES 的用戶端：286.2MB

有啟動 iES 的用戶端：335.8MB

※在複雜的網路環境，且用戶端眾多(包含未開機)的情況下，可能需要一些時間才能將設定完全部署到所有用戶端。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。未套用到設定的 OfficeScan 用戶端會自動升級。

A. 在用戶端 > 用戶端管理 > 設定 > 權限和其他設定

B. 其他設定 > 將「OfficeScan 用戶端僅會更新下列元件」修改為「病毒碼檔案」 > 套用至所有用戶端

注意：如果您的網路環境非常複雜，而且包含大量的用戶端，可能需要一些時間才能將設定部署到所有用戶端。 在升級之前，請預留 2~7 天以便讓設定部署到所有用戶端。未套用設定的用戶端將會自動升級。

(4) 如果目前的 OfficeScan 已啟動 OfficeScan 防火牆，部署此次升級可能會導致用戶端發生網路中斷情況：

A. 為避免斷線問題，請確定啟動這個選項。如果要檢查這個選項的狀態，請移至「用戶端 | 全域用戶端設定」，然後移至「防火牆設定」區段。選項為「只在系統重新啟動後更新 OfficeScan 防火牆驅動程式」。

B. 部署此套件之後，OfficeScan 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，OfficeScan 用戶端可能會發生問題。

依預設，會啟動顯示重新啟動通知訊息的選項。如果要檢查這個選項的狀態，請移至「用戶端 | 全域用戶端設定」，然後移至「警訊設定」區段。選項為「如果用戶端

電腦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」。

(4) 請確認其語言版本，中英文版本不可相互升級

4. 升級至 Apex One 前的重要資料備份

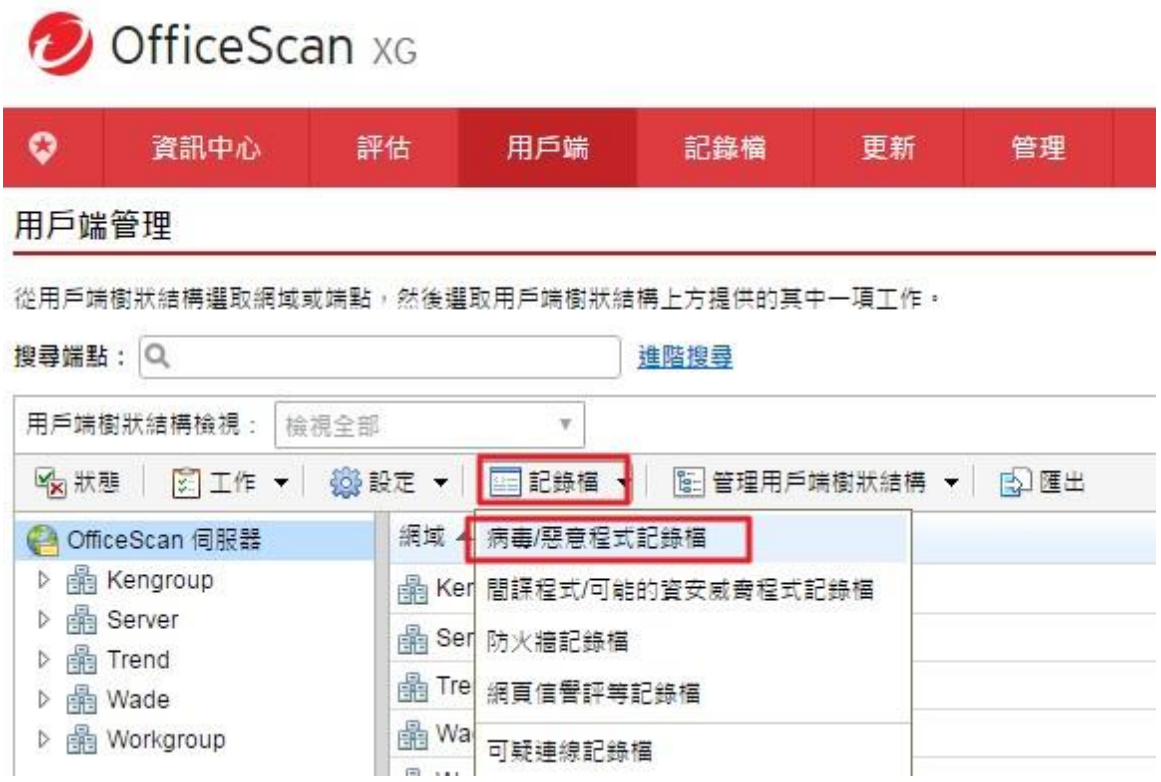
在升級 OfficeScan 伺服器之前，請先備份 OfficeScan 伺服器資料庫與重要的組態檔案。

備註：備份的目的主要是未來有需要重新安裝舊版時，還原舊設定使用。

(1) 備份及清除相關紀錄檔

A. 開啟瀏覽器登入 OfficeScan Web 管理主控台。

B. 移至「Security Agent | Security Agent 管理 | 點選 OfficeScan Server 群組 | 紀錄檔 | 病毒/惡意程式紀錄檔」。



C. 選取以下搜尋條件：

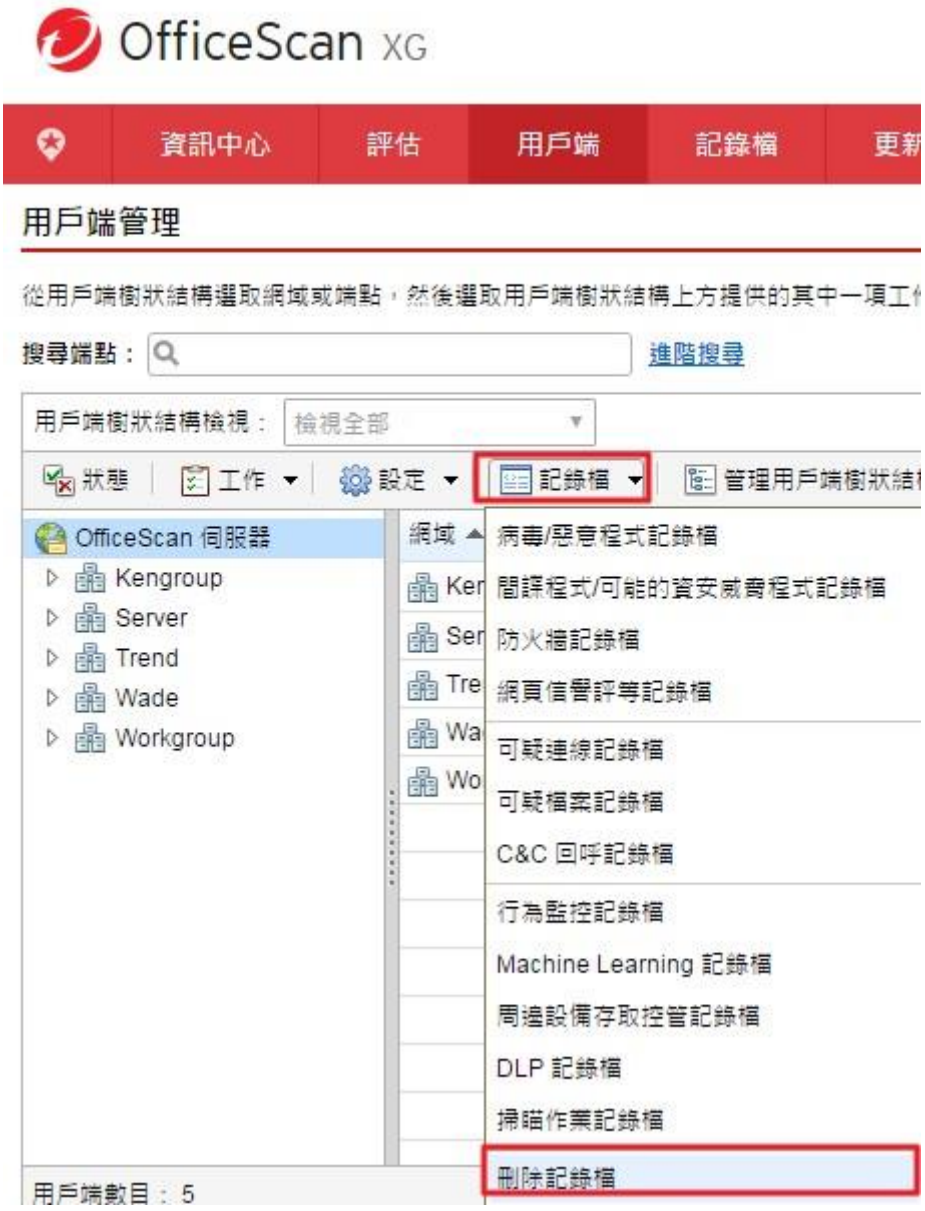
□ 時間範圍

□ 掃描類型

點選"顯示紀錄檔"。

D. 於病毒/惡意程式紀錄檔頁面中，點選"全部匯出到 CSV"，以完成紀錄檔之備份。

E. 移至「用戶端 | 用戶端管理 | 點選 OfficeScan 伺服器群組 | 紀錄檔 | 刪除紀錄檔」。



F. 於紀錄檔條件頁面中，設定以下項目：

- 在"要刪除的紀錄檔類型"，勾選"所有用戶端紀錄檔"。
- 在"要刪除的紀錄檔"，勾選"選定紀錄檔類型的所有紀錄檔"。

完成後點選"刪除"。

(2) 備份 OfficeScan 伺服器的設定與組態

A. 停止 OfficeScan 主服務：

開啟 Windows 命令提示字元，輸入"services.msc"，啟動"服務"，在 OfficeScan Master Service 項目中按右鍵點選"停止"。

B. 待服務完全停止後，手動備份"<伺服器安裝資料夾> \PCCSRV\"資料夾內的下列檔案和資料夾：

項次	檔案/資料夾	說明
1	ofcscan.ini	包含全域 Security Agent 設定
2	ous.ini	包含防毒元件部署的更新來源表格
3	Private 資料夾	包含防火牆和更新來源設定
4	Web\tmOPP 資料夾	包含病毒爆發防範設定
5	Pccnt\Common\OfcPfw*.dat	包含防火牆設定
6	Download\OfcPfw*.dat	包含防火牆部署設定
7	Log 資料夾	包含系統事件和連線驗證記錄檔
8	Virus 資料夾	包含隔離檔案
9	HTTPDB 資料夾	包含 OfficeScan 資料庫

C. 重新啟動 OfficeScan Master Service：

開啟 Windows 命令提示字元，輸入"services.msc"，啟動"服務"，在 OfficeScan Master Service 項目中按右鍵點選"啟動"。

5. 原機升級 Apex One 伺服器

A. 若欲啟用安裝 Endpoint Sensor (iES) 服務，資料庫需符合以下需求：

- 版本：SQL Server 2016 SP1 (或更新版本)，但不支援 SQL Server Express
- 先決條件設定：啟動「搜尋的全文檢索和語意擷取」(Full-Text Search and Semantic Search Stored Procedures) 功能。
- SQL 定序(Collation) 必須使用預設值：「不區分大小寫(Case Insensitive)」。若要直接使用現有資料庫且定序(Collation)已經為:「區分大小寫(Case Sensitive)」將導致安裝中斷，因為 Apex 系列產品及 Endpoint Sensor 不支援該設定，請指向另一台 SQL 主機進行安裝。

B. Apex One 伺服器和 Security Agent 用戶端之間連線使用 SSL 加密通訊協定。

請務必確保 Apex One Server 與 Client 用戶端，都必須支援 TLS 1.2 安全通訊協定。

(Microsoft 檢查 TSL 1.2 是否啟用)

C. 若 OfficeScan 11.0 SP1 [伺服器通訊埠] 使用 4343，規劃使用 [移動用戶端] 做用戶端移轉升級，並且 Apex One[伺服器通訊埠] 改採 443 的客戶。 請務必先將用戶端升級至 Hotfix b6633，避免升級後造成通訊埠不正確問題。

D. Windows 2012 R2 需先安裝 KB2919442 與 KB2919355 更新。

Windows 2016 (version 1607, build 14393)建議安裝 KB4093120 更新。

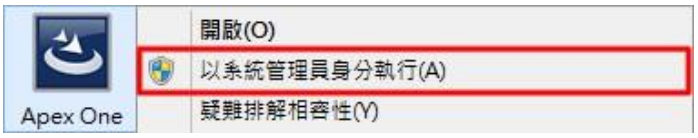
E. 不支援 SQL Server AlwaysOn

F. 升級前，請確認以下狀況，避免無法升級或升級中斷：

- 確定沒有用戶端執行 Login Script(AutoPcc.exe)
- 確定沒有執行資料庫相關工作
- 從工作管理員確認沒有 mmc.exe 和 LogServer.exe 程序。

(1) 下載並執行 Apex One 安裝程式。
https://www.trend.com.tw/support/downloads/Apex%20One/2019/TC/GM/apexone_2019_win_tc_gm_b1555.exe

(2) 以系統管理員身份執行 Apex One 主程式。執行安裝程式(右鍵以系統管理員身分執行)



(3) 執行安裝程式，出現歡迎使用的畫面，請點選「下一步」。

(4) 在授權合約畫面中，請點選「我接受授權合約的條款」和「下一步」。

(5) Security Agent 升級資訊，請點選「下一步」。

(6) 啟動增強式防護、預設選擇「抵禦勒索軟體」和「抵禦網路攻擊」項目，請點選「下一步」。

(7) 資料庫備份、可以自訂備份的位置，請點選「下一步」。

(8) 若有購買 Endpoint Sensor 服務且符合資料庫需求，可勾選安裝

(9) 選擇本機安裝 SQL Server Express 或連線到 SQL Server（若是自定資料庫帳號，須確認該帳號具有 dbcreator、bulkadmin、db_owner 等資料庫角色）

(10) Apex One Security Agent 部署「標準掃瞄」和「雲端截毒」掃瞄方法所需的更新流量，請點選「下一步」。

(11) Smart Feedback，請點選「下一步」。

(12) 確認安裝資訊，請點選「安裝」。

(13) 安裝成功畫面，請點選「完成」。

第三章、 Apex Central 全新安裝步驟

1. 系統需求

Apex Central 是 32 位元程式，在 64 位元電腦安裝時，請修改 IIS 以使用 32 位元模式。

註：請避免與 Apex One server 安裝在同一主機。

Windows 2012 需要有 KB2999226、KB2975331 更新。

Windows 2012 R2 需要有 KB2919355、KB2919442、KB3000850 更新

Apex Central 系統需求：

<table>
<tr><th>作業系統</th><th>處理器</th><th>記憶體</th><th>可用磁碟空間</th></tr>
<tr><td rowspan="4">• Windows Server 2012
• Windows Server 2012 R2
• Windows Server 2016
• Windows Server 2019</td><td>至少 2.3 GHz Intel™ Core™ i5 或相容的 CPU
AMD™ 64 processor
Intel 64 processor</td><td>• 8 GB 以上</td><td>• 至少 10 GB
• 建議 80 GB 或以上 (SAS)</td></tr>
<tr><td colspan="3">IIS 設定需求</td></tr>
<tr><td colspan="3">• Microsoft IIS 8.0/8.5/10.0
• Microsoft IIS 6.0 管理相容性
• Microsoft IIS Windows 驗證
• Microsoft IIS ASP
• Microsoft IIS ASP.NET 4.5/4.6/4.7
• Microsoft IIS ASP.NET Extensibility 4.5/4.6/4.7
• Microsoft IIS CGI
• Microsoft Message Queuing Service (MSMQ)</td></tr>
<tr><td colspan="3">資料庫伺服器</td></tr>
<tr><td></td><td colspan="3">• SQL 2008 以上的版本 *需安裝支援 TLS 1.2 的 Windows Hotfix。</td></tr>
</table>

請造訪下列網站，以取得系統需求和相容協力廠商產品的完整清單：
https://docs.trendmicro.com/all/ent/apex-cen/2019/zh-tw/apexCen_2019_req.pdf

2. 全新安裝步驟

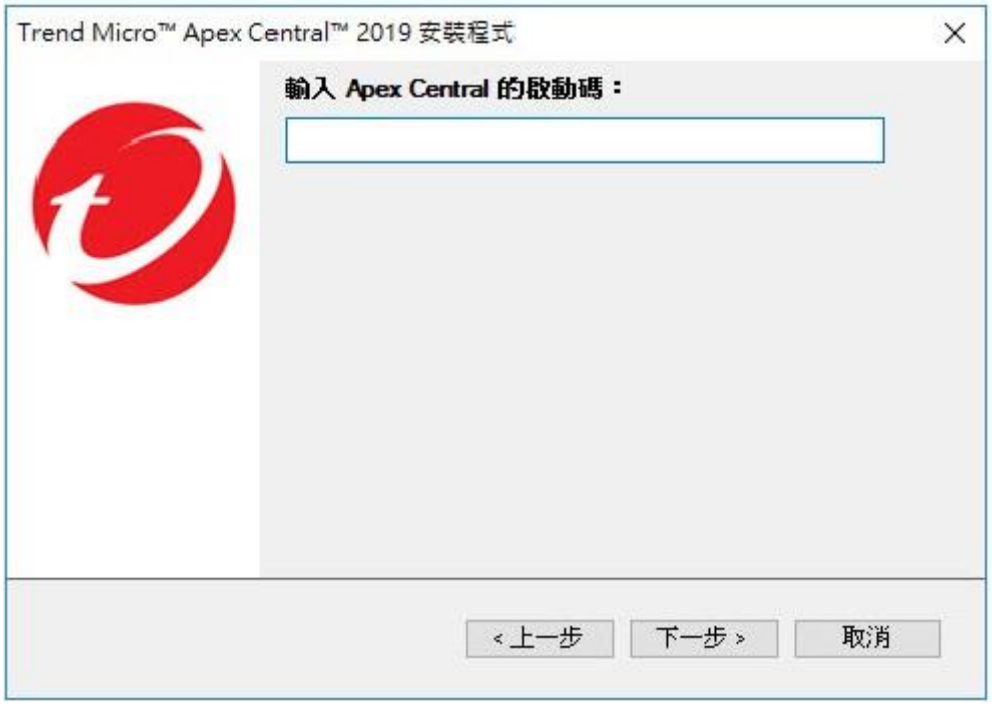
(1) 執行安裝程式，出現歡迎使用的畫面，請點選「下一步」。

(2) 在授權合約畫面中，需點選「是」，才能繼續安裝。

(3) 顯示目前安裝系統摘要，請點選「下一步」。

(4) 選擇 Apex Central 的安裝路徑。確認後請點選「下一步」。

(5) 輸入啟動碼，輸入完成後請點選「下一步」。

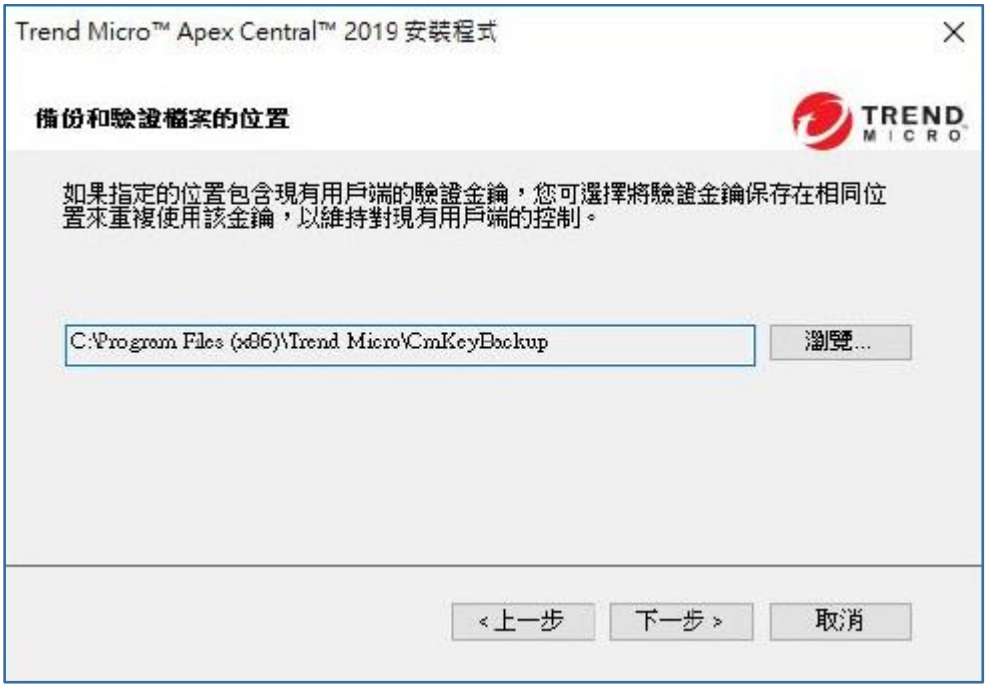


(6) 設定 Web 服務的安全通訊層級與 Apex Central 如何辨識您的伺服器，設定完成後接著點選「下一步」。

註：Web access security level：

- High - HTTPS only：所有 Apex Central 通訊都使用 HTTPS 連線。確保 Apex Central 與其它產品之間通訊的安全性。
- Medium - HTTPS primary：所有 Apex Central 通訊都使用 HTTPS 連線，如果 HTTPS 無法使用，則使用 HTTP 連線。這是 Apex Central 的預設設定。
- Low - HTTP based：所有 Apex Central 通訊都使用 HTTP 連線，這是 Apex Central 與其它產品之間最不安全的連線方式。

(7) 選擇 Apex Central 備份與身份驗證檔案的位置，確認後請點選「下一步」。



(8) 建立 Apex Central 的 root 帳號資訊，確認後請點選「下一步」。

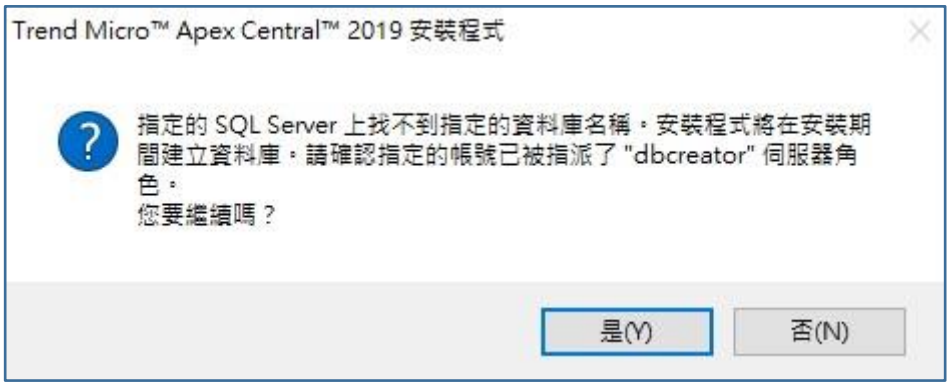
(9) 選擇 Apex Central 使用的資料庫，確認後請點選「下一步」。

- 如果未安裝 SQL Server，則安裝程式會自動選擇 Install Microsoft SQL Express。

- 如已有 SQL Server，請輸入 SQL 位址與驗證方式。

  註：登錄 SQL Server 帳號需包含 “dbcreator” 和 “db_owner” 角色。

(10) 如果指定的資料庫名稱是新的，在安裝過程會建立。並會出現下列提示請確認指定帳號具有 “dbcreator” 角色，沒有問題的話，請點選「是」。



(11) 開始安裝 Apex Central

(12) 安裝完成。

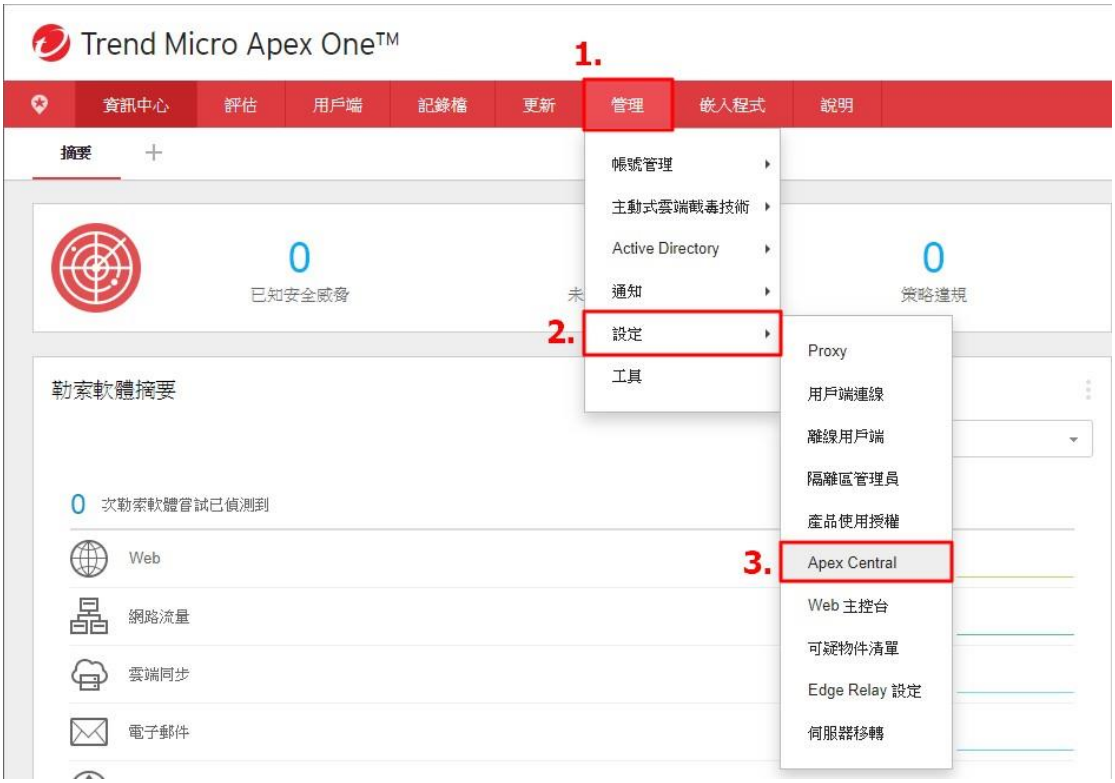
Trend Micro™ Apex Central™ 2019 安裝程式
安裝完成
已成功安裝 Trend Micro Apex Central。請先清除瀏覽器快取，然後再登入 Apex Central Web 主控台。
線上檢視 Readme 檔
啟動 Apex Central Web 主控台
完成

第四章、 建議設定

1. 將 Apex One 註冊至 Apex Central

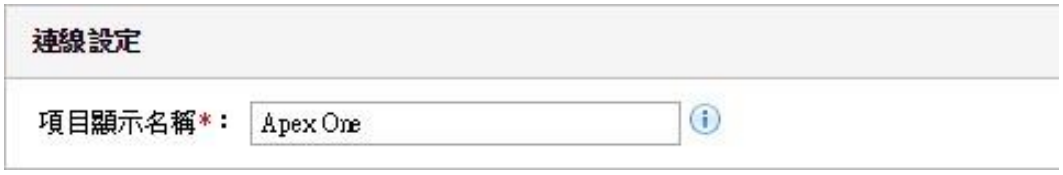
(1) 登入 Apex One Web 主控台

(2) 於上方選單移至「管理」→「設定」→「Apex Central」



(3) 設定頁面

(4) 連線設定 - 設定此 Apex One 於 Apex Central 上顯示的名稱



(5) Apex Central 伺服器設定 - 指定 Apex Central 主機 (網域名稱或 IP)

(6) Apex Central 伺服器設定 - 指定 Apex Central 主機通訊埠

(7) Apex Central 伺服器設定 - 指定 Apex Central 驗證憑證 (選擇性)

為避免兩者存在中間人攻擊(MitM)的可能，建議完成此操作。憑證檔案路徑：

[Apex Central 安裝資料夾]\Control Manager\Certificate\CA\TMCM_CA_Cert.pem

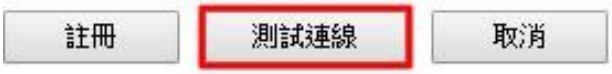
(8) Apex Central 伺服器設定 - 指定 IIS Web 伺服器驗證 (選擇性) 若 Apex Central 開啟 IIS 驗證或關閉匿名驗證才需設定此選項。

(9) 管理通訊協定 Proxy 設定 (選擇性) 若 Apex One 存取 Apex Central 主機需透過 Proxy 才需設定。

(10) 雙向通訊埠轉送 (選擇性)

Apex One 連向 Apex Central 之間有 NAT 防火牆或其他閘道才需設定。

(11) 測試連線



(12) 若測試連線成功會出現以下訊息

若測試連線失敗會出現以下訊息

(13) 註冊

註冊成功後會顯示以下畫面

(14) 登入 Apex Central 確認產品

新註冊產品需在「目錄管理」將產品移出「新增實體」資料夾，才能使後續設定的策略正確生效。

2. 啟用 iES 功能

此功能策略僅能透過 Apex Central 設定，無法透過 Apex One 設定。

(1) 設定之前：

務必確認 Apex Central 已經正確部署授權。

□ 在管理 > 使用授權管理 > 受管理的產品

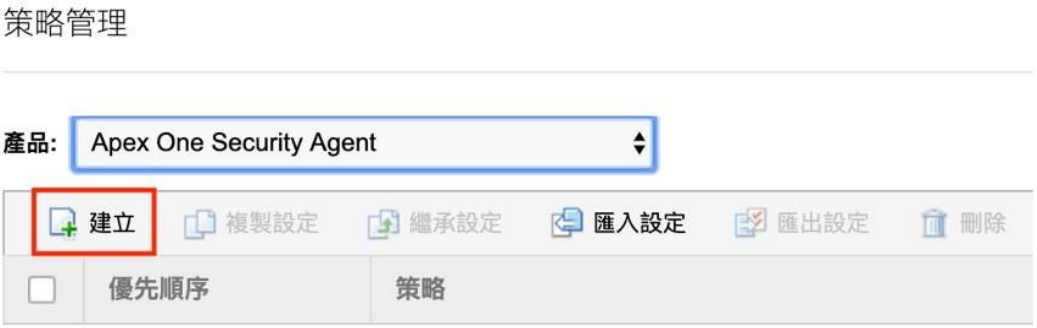
□ 應該有類似以下的授權資訊：

(2) 功能啟用步驟：

A. 切換頁面到 策略 > 策略管理

B. 在「產品」的下拉選單選擇「Apex One Security Agent」

C. 再點選「新增」建立規則。若您想對曾經設定的 Security Agent 開啟 iES，可直接選擇您原先設定的規則。



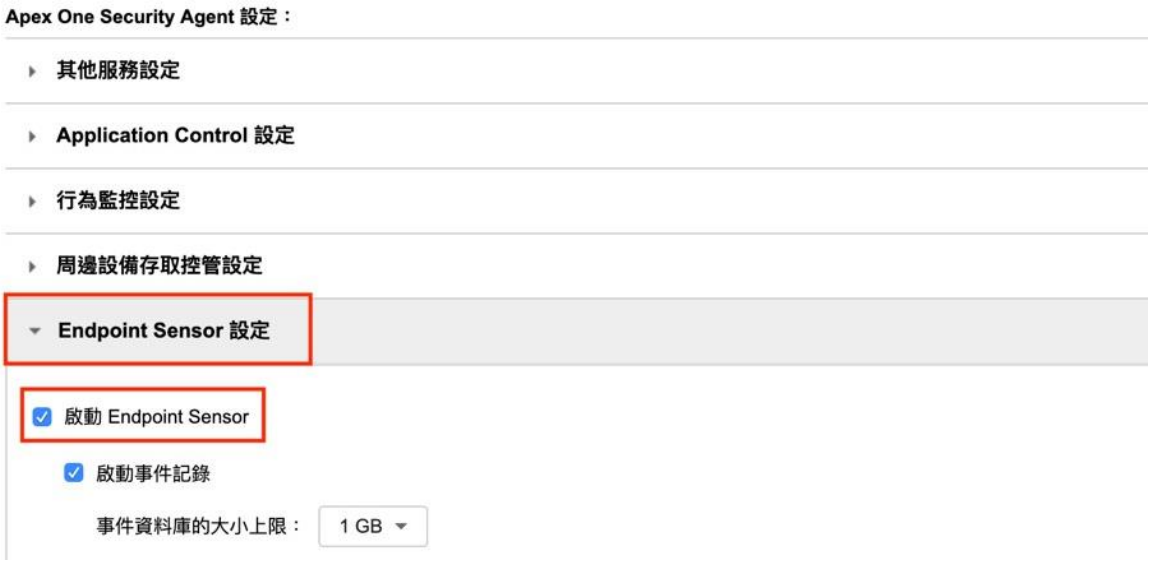
D. 在「策略名稱」輸入您方便區別規則的名稱。若是對原規則增加 iES 功能，則跳過此步驟。

E. 在「目標」選擇規則要套用的目標，可以使用「依條件過濾」過濾目標主機，或是使用「指定目標」直接指定要套用的目標。(在此例，使用的是指定目標)

F. 在產品目錄找到 Apex One 主機或是選擇旗下的群組，再點選「新增選取的資料夾中的所有項目」，或是單獨選擇一個端點，再點選「新增選取的目標」。(在此例，是選擇 Tmcc 整個群組中的主機)

G. 選擇目標後，可看到將會套用規則的主機數量及套用總數。(如下圖右下角紅框標示處)

H. 在設定項目中找到「Endpoint Sensor 設定」，並勾選「啟動 Endpoint Sensor」，並移動到畫面最下方，點選「部署」即可開始部署這次設定。



I. 在策略清單中會出現剛才設定的規則，並先在「等待中」欄位顯示這次部署的目標端點數量。

(3) 驗證項目：

A. 當規則部署完成後，會在「已部署」欄位下，看到套用規則的目標數量，這也是代表套用成功的數量。

B. 在 Security Agent 主控台上也可以看到 Endpoint Sensor 的狀態是綠燈。

3. 啟用 iVP 功能

此功能策略僅能透過 Apex Central 設定，無法透過 Apex One 設定。

(1) 設定之前：

務必確認 Apex Central 已經正確部署授權。

- 在管理 > 使用授權管理 > 受管理的產品

- 應該有類似以下的授權資訊：

(2) 功能啟用步驟：

A. 切換頁面到 策略 > 策略管理

B. 先在「產品」的下拉選單選擇「Apex One Security Agent」，再點選「新增」建立規則。若您想對曾經設定的 Security Agent 開啟 iES，則直接選擇您原先設定的規則。

C. 在「策略名稱」輸入您方便區別規則的名稱。若是對原規則增加 iVP 功能，則跳過此步驟。

D. 在「目標」選擇規則要套用的目標，可以使用「依條件過濾」過濾目標主機，或是使用「指定目標」直接指定要套用的目標。(在此例，使用的是直接指定)

E. 在產品目錄找到 Apex One 主機或是選擇旗下的群組，再點選「新增選取的資料夾中的所有項目」，或是單獨選擇一個端點，再點選「新增選取的目標」。(在此例，是選擇 Workgroup 整個群組中的主機)

F. 選擇目標後，可看到將會套用規則的主機數量及套用總數。(如下圖右下角紅框標示處)

G. 在設定項目中找到「Vulnerability Protection 設定」，並勾選「啟動 Vulnerability Protection 」，並移動到畫面最下方，點選 儲存 即可儲存這次設定。

H. 儲存規則後，則可在規則清單中看到您剛才設定的規則。且會先在等待中狀態顯示這次套用此規則的目標主機數量。

(3) 驗證項目：

A. 當規則部署完成後，會在 已部署 欄位下，看到套用規則的目標數量，這也是代表

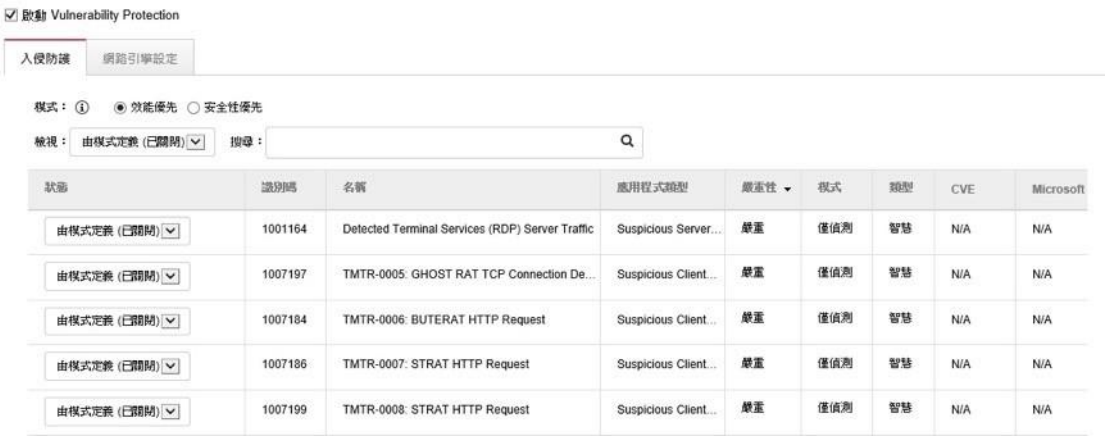
套用成功的數量。

B. 在 Security Agent console 上也可以看到 Vulnerability Protection 的狀態是綠燈。

(4) 建議策略：

入侵防護提供兩種模式

- 效能優先 - 確保防禦已知的弱點問題 (建議啟用此模式)
- 安全性優先 - 防禦已知的弱點問題，並提供增強式可疑網路活動防禦



4. 啟用 iAC 功能

此功能策略僅能透過 Apex Central 設定，無法透過 Apex One 設定。

(1) 設定之前：

務必確認 Apex Central 已經正確部署授權。

- 在管理 > 使用授權管理 > 受管理的產品

- 應該有類似以下的授權資訊：

(2) 功能啟用步驟：

A. 切換頁面到策略 > 策略管理

B. 先在「產品」的下拉選單選擇「Apex One Security Agent」，再點選「建立」建立規則。若您想對曾經設定的 Security Agent 開啟 iAC，則直接選擇您原先設定的規則。

C. 在「策略」名稱輸入您方便區別規則的名稱。若是對原規則增加 iAC 功能，則跳過此步驟。

D. 在「目標」選擇規則要套用的目標，可以使用「依條件過濾」過濾目標主機，或是使用「指定目標」直接指定要套用的目標。(在此例，使用的是直接指定)

E. 在產品目錄找到 Apex One 主機或是選擇旗下的群組，再點選「新增選取的資料夾中的所有項目」，或是單獨選擇一個端點，再點選「新增選取的目標」。(在此例，是選擇 Workgroup 整個群組中的主機)

F. 選擇目標後，可看到將會套用規則的主機數量及套用總數。

G. 在設定項目中找到「Application Control 設定」，並勾選「啟動 Application Control」，並移動到畫面最下方，點選 Save 即可儲存這次設定。

H. 儲存規則後，則可在規則清單中看到您剛才設定的規則。且會先在「等待中」狀態顯示這次套用此規則的目標主機數量。

(3) 驗證項目：

A. 當規則部署完成後，會在「已部署」欄位下，看到套用規則的目標數量，這也是代表套用成功的數量。

B. 在 Security Agent 主控台上也可以看到 Application Control 的狀態是綠燈。

第五章、 舊版 OfficeScan 用戶端升級

1. 方法一：自動升級 Security Agent

(1) 建議先小規模升級測試後再大量升級，建議觀察時間至少一周。

(2) 選定測試範圍，至「用戶端 > 用戶端管理」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。

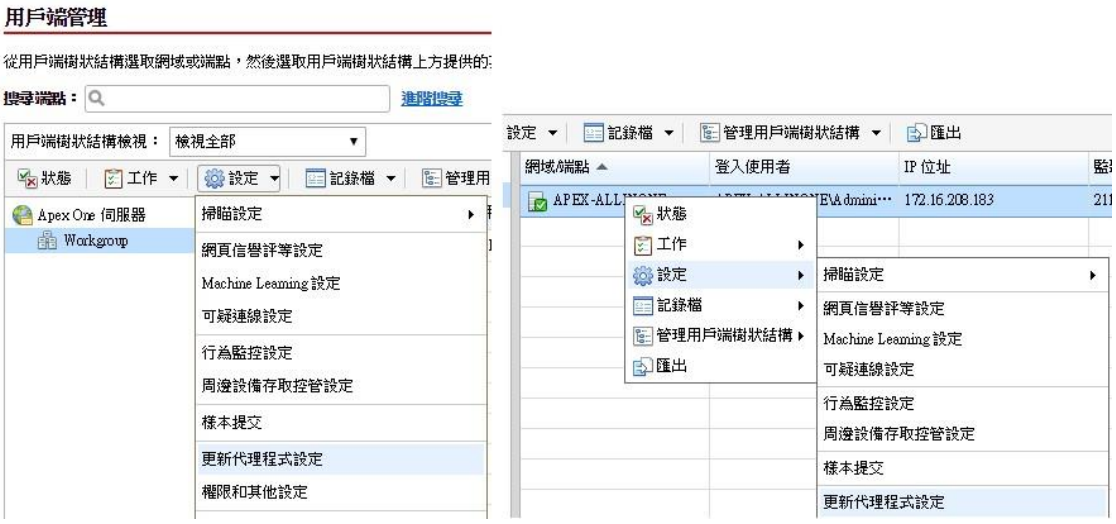
(3) 按一下「設定 > 權限和其他設定」，然後移至「其他設定」標籤。在「Security Agent 僅會更新下列元件」下拉式清單中，選取「所有元件（包括 Hotfix 和用戶端程式）」。

(4) 請點選「儲存」，並檢查升級結果。並請安排重新啟動電腦，完成用戶端的升級。

(5) 請重複步驟 (2) 到步驟 (4) 直至所有用戶端都已升級。

2. 方法二：透過更新代理程式升級 Security Agent

(1) 至「用戶端 > 用戶端管理」，在用戶端樹狀結構中，選取並指定更新代理程式。可選擇單一網域作為設定，也可指定單一或是複數用戶端為更新代理。



(2) 檢查設定，至設定>更新代理程式設定，確認勾選全部項目並儲存。

(3) 移至「更新 > 用戶端 > 手動更新」，選取「手動選取用戶端」選項，然後請點選「選取」。

(4) 在開啟的用戶端樹狀結構中，選擇要升級的更新代理程式後滑鼠點選右鍵或是點選用戶端樹狀結構頂端的「開始更新」。

小秘訣 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」。

(5) 至「用戶端 > 用戶端管理」在用戶端樹狀結構中，選取您要升級的用戶端

(6) 按一下「設定 > 權限和其他設定」，然後移至「其他設定」標籤。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)」。

(7) 點選「儲存」，檢查升級結果。

(8) 請重複步驟 (5) 到步驟 (7) 直至所有用戶端都已升級。

3. 方法三：將用戶端移轉至 Apex One 伺服器升級

(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/用戶端移至 Apex One 伺服器時發生問題。

(3) 移至「用戶端 > 用戶端管理」。

(4) 在用戶端樹狀結構中，選取要升級的用戶端。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「將選取的線上用戶端移動到其他 OfficeScan 伺服器」下，指定 Apex One 伺服器的 IP 位址與伺服器監聽通訊埠（安裝時設定的通訊埠，預設為 HTTP (8080) & SSL (4343)通訊埠號碼）。

C. 請點選「移動」。

(6) 線上用戶端會開始移動並升級，可登入主控台確認移動與升級結果。

□ 關於離線與單機（之前稱為行動）用戶端的轉移：

□ 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 。

若有其餘部署考量或是欲第三方工具派送升級，相關方法可參考管理者手冊 P.140~P.180。

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　info@trendmicro.com
www.trendmicro.com