TREND MICRO™

10.6 OfficeScan™ SP2

管理手冊

企業資訊安全整體防護

端點安全

防護雲端

Web 安全

文件編號：OSTM105795/121114

發行日期：2013 年 1 月

文件版本號碼：1.0

產品名稱和版本號碼：OfficeScan™ 10.6 SP2

受美國專利保護，專利編號： 5,951,698

Trend Micro OfficeScan 10.6 SP2 使用手冊的目的是介紹本軟體的主要功能，並提供適用於您生產環境的安裝說明。安裝或使用軟體之前，您應閱讀完該手冊。

如需有關如何使用軟體特定功能的詳細資訊，請參閱線上說明檔和趨勢科技網站上的「常見問題集」。

趨勢科技十分重視文件品質的提升。隨時歡迎您的指教。請至下列網站並給予您對此文件的評估意見：

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

目錄

部分 III: 管理 OfficeScan 伺服器和用戶端

第 13 章: 管理 OfficeScan 伺服器

第 14 章: 管理 OfficeScan 用戶端

部分 IV: 提供其他防護

第 15 章: 使用 Plug-In Manager

第 16 章: 使用 Policy Server for Cisco NAC

序言

序言

歡迎使用《Trend Micro™ OfficeScan ™ *管理手冊*》。本文件討論使用資訊、用戶端安裝程序及 OfficeScan 伺服器和用戶端管理。

本章內容：

OfficeScan 文件

OfficeScan 文件包含下列各項：

表 1. OfficeScan 文件

文件	說明
安裝和升級手冊	討論安裝 OfficeScan 伺服器以及升級伺服器和用戶端的需求與程序的 PDF 文件
管理手冊	討論使用資訊、用戶端安裝程序及 OfficeScan 伺服器和用戶端管理的 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。您可以從 OfficeScan 伺服器、用戶端、策略伺服器主控台和 OfficeScan 主安裝程式存取「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： http://www.trendmicro.com.tw/solutionbank/corporate/default.asp

您可以從下列位置下載最新的 PDF 文件和 Readme 檔：

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

讀者

OfficeScan 文件適用於下列使用者：

- OfficeScan 管理員：負責管理 OfficeScan，包括 OfficeScan 伺服器和 OfficeScan 用戶端的安裝與管理。這些使用者必須具備進階網路管理和伺服器管理知識。
- Cisco NAC 管理員：負責使用 Cisco NAC 伺服器與 Cisco 網路設備設計和維護安全系統。他們必須具備操作這些設備的經驗。

- 終端使用者：其電腦上已安裝 OfficeScan 用戶端的使用者。這些使用者的電腦技術程度從初學者到進階使用者都有。

文件慣例

為協助您輕鬆地尋找和解譯資訊，OfficeScan 文件會使用下列慣例：

表 2. 文件慣例

慣例	說明
全部大寫	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、選項和工作
斜體	參考其他文件或新技術元件
「用戶端電腦 > 用戶端管理」	每個程序的開頭都有一個「導覽列」，可協助使用者瀏覽至相關 Web 主控台畫面。多個導覽列表示有多種方式可以前往相同的畫面。
<文字>	表示應該以實際資料取代角括號中的文字。例如，`C:\Program Files\<檔案名稱>`，可以是 `C:\Program Files\sample.jpg`。
 注意	提供組態設定注意事項或建議
 秘訣	提供最佳實作資訊和趨勢科技的建議
 警告!	提供可能會對網路上的電腦造成傷害的活動的警告

詞彙

下表提供 OfficeScan 文件中使用的正式詞彙：

表 3. OfficeScan 詞彙

詞彙	說明
OfficeScan 用戶端	OfficeScan 用戶端程式
用戶端電腦	已安裝 OfficeScan 用戶端的電腦
用戶端使用者（或使用者）	管理用戶端電腦上 OfficeScan 用戶端的人員
伺服器	OfficeScan 伺服器程式
伺服器電腦	已安裝 OfficeScan 伺服器的電腦
管理員（或 OfficeScan 管理員）	管理 OfficeScan 伺服器的人員
主控台	用於設定和管理 OfficeScan 伺服器及用戶端設定的使用者介面 OfficeScan 伺服器程式的主控台稱為「Web 主控台」，而 OfficeScan 用戶端程式的主控台稱為「用戶端主控台」。
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 OfficeScan 伺服器期間啟動
OfficeScan 服務	透過 Microsoft 管理主控台 (MMC) 所代管的服務。例如：`ofcservice.exe`（OfficeScan 主服務）。
程式	包括 OfficeScan 用戶端、Cisco Trust Agent 和 Plug-In Manager
元件	負責針對安全威脅進行掃瞄、偵測和採取中毒處理行動

用戶端安裝資料夾	電腦上包含 OfficeScan 用戶端檔案的資料夾。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\OfficeScan Client`
	`C:\Program Files\Trend Micro (x86)\OfficeScan Client`

詞彙	說明

伺服器安裝資料夾	電腦上包含 OfficeScan 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\OfficeScan`
	`C:\Program Files\Trend Micro (x86)\OfficeScan`
	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\OfficeScan\PCCSRV\<檔案名稱>`。

雲端掃瞄用戶端	已設定為使用雲端截毒掃瞄的 OfficeScan 用戶端
標準用戶端	已設定為使用標準掃瞄的 OfficeScan 用戶端
雙堆疊	同時具有 IPv4 和 IPv6 位址的實體。例如： • 雙堆疊端點是指同時具有 IPv4 和 IPv6 位址的電腦。 • 雙堆疊用戶端是指安裝在雙堆疊端點上的用戶端。 • 雙堆疊更新代理程式會將更新分發到用戶端。 • 雙堆疊 Proxy 伺服器（如 DeleGate）可以在 IPv4 和 IPv6 位址之間進行轉換。
純 IPv4	僅具有 IPv4 位址的實體
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 OfficeScan 功能和嵌入程式

部分 I

簡介和入門

第 1 章

OfficeScan 簡介

本章介紹趨勢科技™ OfficeScan™，並提供其特性與功能的總覽。

本章內容：

關於 OfficeScan

趨勢科技™ OfficeScan™ 可保護企業網路不受惡意程式、網路病毒、Web-based 安全威脅、間諜程式和混合式安全威脅的攻擊。OfficeScan 是一種整合式的解決方案，它是由常駐於端點的 OfficeScan 用戶端程式和用於管理所有用戶端的伺服器程式所組成。OfficeScan 用戶端可保護電腦，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在每一部用戶端上，設定協調的安全策略和部署更新。

OfficeScan 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聰明的安全解決方案。獨一無二的雲端技術和輕量型用戶端可減少對於傳統病毒碼下載的依賴，以及降低因為病毒碼延遲佈署所造成的風險。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。

本版本中的新功能

趨勢科技 OfficeScan 包含下列新功能和加強功能。

Data Loss Prevention 加強功能

該版本中的 Data Loss Prevention 加強功能包括下列功能。

表 1-1. Data Loss Prevention 加強功能

功能	說明
鑑識資料隔離	OfficeScan 用戶端會建立加密的鑑識資料檔案並將其上傳至伺服器，以便公司追蹤和記錄網路上發生的特定 Data Loss Prevention 事件。OfficeScan 會為每個鑑識檔案產生一個雜湊值，以用於驗證並確保完整性。 透過與 Control Manager 整合，安全管理人員可以檢視引發每個事件的確切數位資產，並採取適當的措施。 如需詳細資訊，請參閱鑑識資料夾和 DLP 資料庫 第 3-8 頁。
多規則策略	管理員可以為單一策略建立多條規則。每條規則可包含多個範本，管理員可以根據所識別數位資產的類型或傳輸活動所經由的通道，來指定特定的處理行動。全域例外規則會套用至指定策略中的所有規則，這樣便無需複製設定。 如需詳細資訊，請參閱 Data Loss Prevention 策略 第 10-3 頁。
加強的記錄檔詳細資訊	記錄檔顯示有關各個 Data Loss Prevention 事件的更多詳細記錄。詳細資訊不僅包括觸發事件的規則，還包括識別數位資產的確切範本。 如需詳細資訊，請參閱 Data Loss Prevention 記錄檔 第 10-47 頁。

10.6 版 SP2 的新功能

趨勢科技 OfficeScan SP2 包含下列新功能和加強功能。

平台和瀏覽器支援

此版本的 OfficeScan 支援將伺服器和用戶端安裝在 Windows Server™ 2012/Server Core 2012 上。

此版本的 OfficeScan 還支援將用戶端安裝在 Windows 8™ 上。

此版本的 OfficeScan 支援 Internet Explorer™ 10。

注意

使用 Windows UI 模式運作的用戶端會得到部分支援。如需詳細資訊，請參閱 Windows 8 和 Windows Server 2012 支援 第 C-1 頁。

偵測與效能加強功能

此版本的 OfficeScan 提供下列偵測與效能加強功能。

表 1-2. 偵測與效能加強功能

加強功能	說明
MSI 安裝	即時掃瞄現在會先驗證 MSI 安裝套件的檔案簽章，然後再繼續安裝。一旦 OfficeScan 收到檔案簽章是受信任簽章的確認，即時掃瞄便會允許安裝作業繼續執行，而不會進行進一步的檔案掃瞄。

VDI 加強功能

此版本的 OfficeScan 加強了虛擬環境的雲端截毒掃瞄更新功能。當大量雲端截毒掃瞄用戶端要求病毒碼更新時，伺服器現在會將用戶端要求放在佇列中，直到伺服器可以傳送回應為止。當每一個用戶端完成更新時，伺服器會提示佇列中的下一個用戶端開始更新。

Data Loss Prevention 加強功能

此版本的 OfficeScan 可加強 Data Loss Prevention 功能，以提供：

- Windows 8、Windows Server 2012、Windows Server Core 2012 支援
  - Windows UI 上的 Windows 市集應用程式支援及桌面應用程式支援
  - 使用 Internet Explorer 10 時的 HTTPS 支援
- 使用 Chrome™ 第 19、20、21 和 22 版時的 HTTPS 支援
- 更新的 Gmail 支援

- Microsoft Office™ 2013 支援

10.6 SP1 版新功能

趨勢科技 OfficeScan SP1 包含下列新功能和加強功能。

Control Manager 提供的策略管理

Control Manager 6.0 允許管理員建立策略，並將其部署到 Control Manager 管理的 OfficeScan 伺服器。如需詳細資訊，請參閱《Control Manager 管理手冊》。

支援行為監控（64 位元）

OfficeScan 的行為監控功能現可支援下列平台的 64 位元版本：

- Windows Server 2008™
- Windows 7™
- Windows Vista™ SP1（或更新版本）

支援本機自我保護（64 位元）

「本機自我保護」現可支援下列平台的 64 位元版本：

- Windows Server 2008™
- Windows 7™
- Windows Vista™ SP1（或更新版本）

未經授權的變更防護支援周邊設備存取控管（64 位元）

OfficeScan 的「周邊設備存取控管」功能現可在「未經授權的變更防護」監控過程中支援下列平台的 64 位元版本：

- Windows 2008™
- Windows 7™
- Windows Vista™ SP1（或更新版本）

注意

「資料安全防護」的「周邊設備存取控管」可支援下列 Windows 平台的 64 位元版本：如需有關設定 64 位元權限的詳細資訊，請參閱儲存裝置的權限 第 9-3 頁。

資料安全防護加強功能

OfficeScan 10.6 SP1 的「資料安全防護」加強功能包含下列支援和升級：

- Data Loss Prevention 和「周邊設備存取控管」可支援下列 Windows 平台的 64 位元版本：
- 超過 100 種全新預先設定的 Data Loss Prevention 範本和資料識別碼

虛擬桌面基礎結構加強功能

此版本的 OfficeScan 加強了「虛擬桌面基礎結構」(VDI) 支援與功能。

- Microsoft Hyper-V™ 支援：管理員現在可以使用 Microsoft Hyper-V™ 伺服器、VMware vCenter™ 伺服器以及 Citrix XenServer™ 以管理虛擬用戶端。
- 非持續環境加強功能：OfficeScan 現在依「媒體存取控制」(MAC) 位址識別虛擬用戶端。如此可防止 OfficeScan 指定多個「全域唯一識別碼」(GUID) 給非持續環境中的相同用戶端。

如需詳細資訊，請參閱趨勢科技虛擬桌面支援 第 14-65 頁。

延伸網頁信譽評等通訊埠掃描

OfficeScan 現在可針對所有違反網頁信譽評等策略的所有連接埠掃瞄 HTTPS 流量看是否有網路安全威脅。如果管理員不想針對所有連接埠掃瞄流量，OfficeScan 會針對預設的 80、81 和 8080 HTTP 連接埠提供掃瞄流量的選項。

如需詳細資訊，請參閱設定網頁信譽評等策略 第 11-3 頁。

10.6 版的新功能

趨勢科技 OfficeScan 10.6 包含下列新功能和加強功能。

- 資料安全防護

  「資料安全防護」模組提供了 Data Loss Prevention，並擴展了「周邊設備存取控管」所監控的裝置範圍。

  Plug-in Manager 會管理資料安全防護模組的安裝與授權。如需詳細資訊，請參閱資料安全防護安裝 第 3-2 頁。

  表 1-3. OfficeScan 資料安全防護功能

資料安全防護功能	詳細資訊
Data Loss Prevention	Data Loss Prevention 可保護組織的數位資產，免遭受意外或有意的外洩。Data Loss Prevention 允許您： • 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：電子郵件和外部裝置）傳輸數位資產 • 強制遵守制定的隱私權標準 如需詳細資訊，請參閱關於 Data Loss Prevention 第 10-2 頁。

資料安全防護功能	詳細資訊
周邊設備存取控管	OfficeScan 隨附可立即使用的「周邊設備存取控管」功能，可規範對於 USN 儲存裝置、CD/DVD、軟碟機和網路磁碟機的存取。屬於「資料安全防護」模組一部分的「周邊設備存取控管」透過規範對於下列裝置的存取，擴展了裝置範圍： • 影像裝置 • 數據機 • 通訊埠（COM 和 LPT） • 紅外線裝置 • PCMCIA 卡 • 列印螢幕鍵 • IEEE 1394 介面 如需詳細資訊，請參閱周邊設備存取控管 第 9-2 頁。

- Plug-in Manager 2.0

  Plug-in Manager 2.0 會隨 OfficeScan 伺服器一起安裝。這個 Plug-in Manager 版本提供 Widget：

  Widget 提供快速視覺參考，讓您檢視對業務最為重要的 OfficeScan 功能和嵌入程式解決方案。您可以從 OfficeScan 伺服器的「摘要」管理平台（取代了先前版本 OfficeScan 中的「摘要」畫面）中使用這些 Widget。如需詳細資訊，請參閱摘要管理平台 第 2-5 頁。

- IPv6 支援

  OfficeScan 伺服器和用戶端現在可以安裝在 IPv6 電腦上。

  此外，新版本的 Control Manager 和主動式雲端截毒技術伺服器現在也支援 IPv6，可以提供與 OfficeScan 伺服器和用戶端的緊密整合。

  如需詳細資訊，請參閱適用於 OfficeScan 伺服器和用戶端的 IPv6 支援 第 A-2 頁。

- 用於掃瞄的快取記憶體檔案

OfficeScan 用戶端現在會建置快取檔案，其中包含之前已掃瞄的安全檔案及趨勢科技認為值得信任的檔案的相關資訊。快取檔案會在依要求掃瞄期間提供快速的參考，因而可減少使用系統資源。依需求掃瞄（手動掃瞄、預約掃瞄和立即掃瞄）現在執行效率更高，掃瞄速度效能提高達 40%。

如需詳細資訊，請參閱用於掃瞄的快取設定 第 7-59 頁。

- 啟動加強功能

  電腦啟動時，如果 CPU 使用率超過 20%，OfficeScan 用戶端會延後載入某些用戶端服務。當 CPU 使用率低於限制時，用戶端才會開始載入這些服務。

  這些服務包括：

  - OfficeScan NT 防火牆
  - OfficeScan 資料安全防護服務
  - 趨勢科技未經授權的變更阻止服務

- 損害清除及復原服務加強功能

  損害清除及復原服務現在可在進階清除模式下執行，以停止詐欺安全軟體（又稱為 FakeAV）所執行的活動。用戶端也會使用進階清除規則來主動偵測並停止出現 FakeAV 行為的應用程式。

  為手動掃瞄、即時掃瞄、預約掃瞄和立即掃瞄設定病毒/惡意程式中毒處理行動時，可以選擇清除模式。如需詳細資訊，請參閱損害清除及復原服務 第 7-38 頁。

- 網頁信譽評等 HTTPS 支援

  用戶端現在可掃瞄 HTTPS 流量看是否有網路安全威脅。您可以在建立網頁信譽評等策略時設定這項功能。如需詳細資訊，請參閱網頁信譽評等策略 第 11-3 頁。

重要

- HTTPS 掃瞄僅支援以桌面模式運作的 Windows 8 或 Windows 2012 平台。
- 在執行 Internet Explorer 9 或 10 的 OfficeScan 用戶端上首次啟動 HTTPS 掃瞄之後，使用者必須在瀏覽器快顯視窗中啟動 `TmIEPlugInBHO Class` 附加元件，HTTPS 掃瞄才能正常運作。

- Windows Server Core 2008 支援

  OfficeScan 用戶端現在可以安裝在 Windows Server Core 2008 上。使用者可以使用命令列介面啟動用戶端主控台，並檢查端點的防護狀態。

  如需詳細資訊，請參閱 Windows Server Core 2008/2012 支援 第 B-2 頁。

- 其他加強功能

  此版本包含下列加強功能：

  - 雲端掃瞄用戶端現在會在雲端截毒掃瞄模式下執行 Outlook 郵件掃瞄。在舊版中，雲端掃瞄用戶端會在標準掃瞄模式下執行 Outlook 郵件掃瞄。
  - 間諜程式/可能的資安威脅程式偵測的記錄檔和通知現在會顯示偵測時登入電腦的使用者名稱。
  - 在間諜程式/可能的資安威脅程式記錄檔中，如果第二層掃瞄結果是「暫不處理」，則第一層掃瞄結果現在會是「需要進一步的處理行動」，而不是「不需要處理行動」。有了這個加強功能，現在就可以採取其他措施，如清除您認為有害的間諜程式/可能的資安威脅程式。
  - 您現在可以在用戶端樹狀結構中設定「本機自我保護」這項精細設定。
  - 您現在可以將所有用戶端設定為傳送活動訊號訊息到 OfficeScan 伺服器。在先前版本中，只有無法連線的網路中的用戶端可以傳送活動訊號訊息。如需詳細資訊，請參閱無法連線到用戶端 第 14-38 頁。
  - 將用戶端樹狀結構設定匯出到 `.dat` 檔案時，現在可以匯出所有設定。在先前版本中，只能匯出掃瞄設定和用戶端權限/其他設定。如

需有關匯出設定的詳細資訊，請參閱匯入和匯出用戶端設定 第 14-47 頁。

- 現在使用 Client Mover 工具時，可以將用戶端樹狀結構子網域指定給移至新上層伺服器後將進行分組的用戶端。如需詳細資訊，請參閱Client Mover 第 14-20 頁。

主要功能和優點

OfficeScan 提供下列功能和優點：

- Plug-In Manager 和嵌入程式解決方案

  Plug-In Manager 可幫助安裝、部署及管理嵌入程式解決方案。

  管理員可以安裝兩種嵌入程式解決方案：

  - Plug-in 程式
  - 本機 OfficeScan 功能

- 集中化管理

  Web-based 管理主控台會給予管理員對網路上所有用戶端和伺服器的透明存取權。Web 主控台會協調在每部用戶端和伺服器上進行自動部署安全策略、病毒碼檔案和軟體更新。而有了「病毒爆發防範服務」，它會阻擋感染媒介並迅速部署攻擊專屬安全策略，或在病毒碼檔案推出前先預防或防堵病毒爆發。OfficeScan 還會執行即時監控、提供事件通知和傳送全面的報告。管理員可以執行遠端管理、針對個別桌面或群組設定自訂策略，以及鎖定用戶端安全設定。

- 安全威脅防護

  OfficeScan 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，OfficeScan 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。

  OfficeScan 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電腦上的大量簽章改由主動式雲端截毒伺服器來源處

理。透過這種方式，可以大幅減少不斷增加的端點系統簽章更新量對於系統和網路的影響。

如需有關雲端截毒掃瞄以及如何將其部署到用戶端的資訊，請參閱掃瞄方法 第 7-6 頁。

- 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）。為了處理特洛伊木馬程式所帶來的威脅和侵擾，「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，OfficeScan 有時會通知使用者重新啟動電腦，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電腦，免於遭受惡意和可能有害之網站的威脅。「網頁信譽評等」會中斷感染鏈並防止下載惡意程式碼。

  請將 OfficeScan 與「主動式雲端截毒技術伺服器」或「趨勢科技主動式雲端截毒技術」整合，來驗證網站和網頁的可信度。

- OfficeScan 防火牆

  OfficeScan 防火牆使用狀態檢測和高效能網路病毒掃瞄，來保護網路上的用戶端和伺服器。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。

- Data Loss Prevention

Data Loss Prevention 可保護組織的數位資產，免遭受意外或有意的外洩。Data Loss Prevention 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電腦的外部儲存裝置與網路資源的存取。周邊設備存取控管有助於防止資料遺失與外洩，並且可與檔案掃瞄搭配使用，以協助防禦安全威脅。

- 行為監控

  行為監控會不斷地監控用戶端上的作業系統或已安裝軟體是否發生了異常修改。

- 實施安全和策略

  OfficeScan 緊密整合 Cisco™ Trust Agent，能夠在 Cisco Self-Defending Network 中執行最有效的策略。OfficeScan 也包括能與 Cisco Access Control Server 自動通訊的策略伺服器。與 Trend Micro™ Network VirusWall™ 或其他 Network Admission Control (NAC) 裝置整合後，OfficeScan 可檢查嘗試進入網路的用戶端，然後補救、重新導向、限制、拒絕或允許存取。如果電腦易受攻擊或已中毒，則 OfficeScan 可以自動隔離該電腦及其網路區段，直到所有電腦更新或清除完成為止。

OfficeScan 伺服器

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

伺服器會執行兩項重要功能：

- 安裝、監控和管理 OfficeScan 用戶端

- 下載用戶端所需的大部分元件。OfficeScan 伺服器會從趨勢科技主動式更新伺服器下載元件，然後分發給用戶端。

注意

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

圖 1-1. OfficeScan 伺服器的運作方式

OfficeScan 伺服器能為伺服器和用戶端之間提供即時且雙向的通訊。從網路上幾乎任何一個位置存取 Browser-based Web 主控台，管理員可透過它來管理用戶端。伺服器與用戶端會透過「超文字傳輸通訊協定」(HTTP) 互相通訊。

OfficeScan 用戶端

在每部電腦上安裝 OfficeScan 用戶端保護 Windows 電腦不受安全威脅的侵襲。

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

與趨勢科技產品和服務整合

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

表 1-4. 與 OfficeScan 整合的產品和服務

產品/服務	說明	版本
主動式更新伺服器	提供 OfficeScan 用戶端保護用戶端免受安全威脅危害所需的所有元件	無
主動式雲端截毒技術	提供檔案信譽評等服務和網頁信譽評等服務給用戶端。 主動式雲端截毒技術是由趨勢科技所代管。	無
獨立式主動式雲端截毒技術伺服器	提供主動式雲端截毒技術所提供的相同檔案信譽評等服務和網頁信譽評等服務。 獨立式主動式雲端截毒技術伺服器主要用途是供客戶在企業網路內執行服務，以最佳化效能。 注意 整合式主動式雲端截毒技術伺服器會隨 OfficeScan 伺服器一起安裝，其功能與整合式主動式雲端截毒技術伺服器相同，只是它的容量有限。	• 2.5（建議使用） • 2.0

產品/服務	說明	版本
Control Manager	一項軟體管理解決方案，讓您能夠從一個集中位置控制防毒和內容安全程式，而不受限於程式的平台或實體位置。	• 6.0（建議使用） • 5.5 SP1 • 5.5 • 5.0

第 2 章

使用 OfficeScan

本章說明如何開始使用趨勢科技™OfficeScan™ 和初始組態設定。

本章內容：

Web 主控台

Web 主控台是監控整個企業網路中 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 Java、CGI、HTML 和 HTTP 等標準 Internet 技術。

注意

從 Web 主控台設定逾時設定。如需詳細資訊，請參閱 Web 主控台設定 第 13-40 頁。

可使用 Web 主控台執行下列工作：

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

注意

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

開啟 Web 主控台的需求

您可以從網路上具有下列資源的任何電腦開啟 Web 主控台：

- 300MHz Intel™ Pentium™ 處理器或同級處理器
- 128MB RAM

- 至少 30MB 可用磁碟空間
- 支援 1024 x 768 解析度（256 色）或以上的顯示器
- Microsoft Internet Explorer™ 7.0 或更新版本

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

表 2-1. OfficeScan Web 主控台 URL

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

注意

如果從舊版 OfficeScan 升級，Web 瀏覽器和 Proxy 伺服器的快取記憶體檔案可能會讓 OfficeScan Web 主控台無法正常載入。請清除瀏覽器和任何 Proxy 伺服器（位於 OfficeScan 伺服器與用來存取 Web 主控台的電腦之間）上的快取記憶體。

登入帳號

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

定義使用者角色並設定使用者帳號，讓其他使用者不需要使用 root 帳號就可以存取 Web 主控台。當使用者登入主控台時，可以使用您為其設定的使用者帳號。如需詳細資訊，請參閱以角色為基礎的管理 第 13-2 頁。

Web 主控台標題

Web 主控台的標題區域提供下列選項：

圖 2-1. Web 主控台標題區域

- <帳號名稱>：按一下帳號名稱（例如：root）即可修改該帳號的詳細資料（例如：密碼）。
- 登出：讓您從 Web 主控台登出
- 說明（ ）
  - 新增功能：開啟其中列出目前產品版本內含的新功能的頁面
  - 內容與索引：開啟「OfficeScan 伺服器說明」
  - 常見問題集：開啟趨勢科技常見問題集，可從中檢視常見問答集和更新的產品資訊、聯絡客服部門，以及註冊 OfficeScan
  - 安全資訊：顯示「趨勢科技安全資訊」頁面，您可於其中參閱關於最新安全威脅的資訊
  - 企業安全防護採購：顯示趨勢科技的企業安全防護採購網頁，可讓您聯絡當地的銷售人員
  - 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
  - 關於：提供產品的概觀、檢查元件版本詳細資料的指示以及智慧型支援系統的連結。如需詳細資訊，請參閱智慧型支援系統 第 18-2 頁。

摘要管理平台

當您開啟 OfficeScan Web 主控台或按一下主功能表中的「摘要」時，會顯示「摘要」畫面。

每個 Web 主控台使用者帳號都具有一個完全獨立的管理平台。對使用者帳號的主控台所做的任何變更將不會影響其他使用者帳號的主控台。

如果管理平台包含 OfficeScan 用戶端資料，顯示的資料取決於使用者帳號的用戶端網域權限。例如，如果授與某個使用者帳號管理網域 A 和 B 的權限，則該使用者帳號的管理平台將僅顯示來自屬於網域 A 和 B 的用戶端的資料。

如需有關使用者帳號的詳細資訊，請參閱以角色為基礎的管理 第 13-2 頁。

「摘要」管理平台包含以下內容：

- 「產品使用授權狀態」區段
- Widget
- 標籤

「產品使用授權狀態」區段

本區段位於管理平台頂端，它會顯示 OfficeScan 使用授權的狀態。

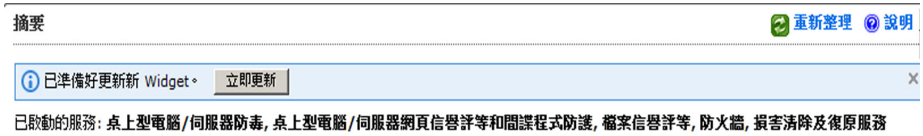


圖 2-2. 「產品使用授權狀態」區段

出現下列情況時顯示有關使用授權狀態的提醒：

- 如果您有完整版使用授權：
  - 授權到期 60 天前

  - 在產品的寬限期內。寬限期視地區而定。請向您的趨勢科技銷售人員確認寬限期。
  - 使用授權到期且經過寬限期以後。在這期間，您無法取得技術支援或執行元件更新。掃瞄引擎仍會掃瞄使用過期元件的電腦。這些過期元件可能無法保護您不受最新的安全威脅侵襲。
- 如果您有試用版使用授權：
  - 授權到期 14 天前
  - 使用授權到期時。在這期間，OfficeScan 會關閉元件更新、掃瞄和所有用戶端功能。

如果您已取得「啟動碼」，請移至「管理｜ > 產品使用授權」續約使用授權。

標籤和 Widget

Widget 是管理平台的核心元件。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：

- OfficeScan 伺服器和用戶端
- 嵌入程式解決方案及其用戶端代理程式
- 趨勢科技主動式雲端截毒技術

注意

啟動 Smart Feedback 以顯示來自主動式雲端截毒技術的資料。如需 Smart Feedback 的詳細資訊，請參閱 Smart Feedback 第 13-44 頁。

標籤為 Widget 提供了容器。「摘要」管理平台最多支援 30 個標籤。

使用標籤

請執行以下工作來管理標籤：

表 2-2. 標籤工作

工作	步驟
新增標籤	1. 按一下管理平台頂端的新增圖示。接著會顯示一個新畫面。  2. 指定下列項目： • 標題：標籤的名稱 • 配置：從可用的配置中選擇 • 自動調整：如果您選取了具有多個方塊的配置（例如「  」）且每個方塊只包含一個 Widget，請啟動自動調整。自動調整會將 Widget 調整為方塊的大小。 3. 按一下「儲存」。
修改標籤設定	1. 按一下標籤右上角的「標籤設定」。接著會顯示一個新畫面。  2. 修改標籤名稱、配置和自動調整設定。 3. 按一下「儲存」。
移動標籤	使用拖放功能變更標籤的位置。
刪除標籤	按一下標籤標題旁邊的刪除圖示。  刪除標籤會刪除標籤中的全部 Widget。

使用 Widget

請執行以下工作來管理 Widget：

表 2-3. Widget 工作

工作	步驟
新增 Widget	1. 按一下某個標籤。 2. 按一下標籤右上角的「新增 Widget」。接著會顯示一個新畫面。 3. 選取要新增的 Widget。如需可用 Widget 的清單，請參閱可用的 Widget 第 2-9 頁。 • 按一下顯示圖示 ()，該圖示位於畫面右上方，以切換詳細檢視和摘要檢視。 • 畫面的左欄為 Widget 類別。選取一個類別以縮小選取的範圍。 • 使用畫面頂端的搜尋文字方塊可搜尋特定 Widget。 4. 按一下「新增」。
移動 Widget	使用拖放功能將 Widget 移動到標籤內的不同位置。
調整 Widget 的大小	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。
編輯 Widget 標題	1. 按一下編輯圖示（  ）隨即顯示新畫面。 2. 輸入新標題。 注意 對於某些 Widget（如 OfficeScan 和 Plug-in 混搭），可以修改與 Widget 相關的項目。 3. 按一下「儲存」。
重新整理 Widget 資料	按一下重新整理圖示（  ）。
刪除 Widget	按一下刪除圖示（  ）。

預先定義的標籤和 Widget

「摘要」管理平台隨附一組預先定義的標籤和 Widget。您可以重新命名或刪除這些標籤和 Widget。

表 2-4.「摘要」管理平台中的預設標籤

標籤	說明	WIDGET
OfficeScan	此標籤包含的資訊與先前版本 OfficeScan 的「摘要」畫面中的資訊相同。在此標籤中，可以檢視 OfficeScan 網路的總體安全威脅防護。您還可以對需要立即干預的項目（例如病毒爆發或過期的元件）採取處理行動。	• 「用戶端連線能力」Widget 第 2-11 頁 • 安全威脅偵測 Widget 第 2-15 頁 • 病毒爆發 Widget 第 2-16 頁 • 用戶端更新 Widget 第 2-18 頁
OfficeScan 和 Plug-in	此標籤會顯示執行 OfficeScan 用戶端和嵌入程式解決方案的用戶端。使用此標籤可以評估用戶端的總體安全狀態。	「OfficeScan 與 Plug-ins 混搭」Widget 第 2-19 頁
主動式雲端截毒技術	此標籤包含的資訊來自趨勢科技主動式雲端截毒技術，會提供檔案信譽評等服務和網頁信譽評等服務給 OfficeScan 用戶端。	• 網頁信譽評等最常見的安全威脅來源 Widget 第 2-23 頁 • 網頁信譽評等最受威脅的使用者 Widget 第 2-24 頁 • 檔案信譽評等安全威脅分佈圖 Widget 第 2-25 頁

可用的 Widget

本發行版本提供以下 Widget：

表 2-5. 可用的 Widget

WIDGET 名稱	可用性
用戶端連線能力	開箱即用 如需詳細資訊，請參閱「用戶端連線能力」Widget 第 2-11 頁。
安全威脅偵測	開箱即用 如需詳細資訊，請參閱安全威脅偵測 Widget 第 2-15 頁。
病毒爆發	開箱即用 如需詳細資訊，請參閱病毒爆發 Widget 第 2-16 頁。
用戶端更新	開箱即用 如需詳細資訊，請參閱用戶端更新 Widget 第 2-18 頁。
OfficeScan 和 Plug-ins 混搭	開箱即用，但只會顯示 OfficeScan 用戶端中的資料 啟用以下每個嵌入程式解決方案後，即可使用這些解決方案中的資料： • Intrusion Defense Firewall • 趨勢科技虛擬桌面支援 如需詳細資訊，請參閱「OfficeScan 與 Plug-ins 混搭」Widget 第 2-19 頁。
最常見的 Data Loss Preventions 事件	啟用 OfficeScan 資料安全防護後即可使用 如需詳細資訊，請參閱「最常見的 Data Loss Prevention 事件」Widget 第 2-20 頁。
歷來 Data Loss Prevention 事件	啟用 OfficeScan 資料安全防護後即可使用 如需詳細資訊，請參閱歷來 Data Loss Prevention 事件 Widget 第 2-22 頁。
網頁信譽評等最常見的安全威脅來源	開箱即用 如需詳細資訊，請參閱網頁信譽評等最常見的安全威脅來源 Widget 第 2-23 頁。

WIDGET 名稱	可用性
網頁信譽評等最受威脅的使用者	開箱即用 如需詳細資訊，請參閱網頁信譽評等最受威脅的使用者 Widget 第 2-24 頁。
檔案信譽評等安全威脅分佈圖	開箱即用 如需詳細資訊，請參閱檔案信譽評等安全威脅分佈圖 Widget 第 2-25 頁。
IDF - 警訊狀態	啟用 Intrusion Defense Firewall 後即可使用。如需這些 Widget 的詳細資訊，請參閱 IDF 文件。
IDF - 電腦狀態	
IDF - 網路事件歷史記錄	
IDF - 系統事件歷史記錄	

「用戶端連線能力」Widget

用戶端連線能力 Widget 會顯示防毒用戶端與 OfficeScan 伺服器之間的連線狀態。資料以表格和圓形圖顯示。您可以以按一下圖示（在表格和圓形圖之間切換  ）。

圖 2-3. 顯示表格的用戶端連線能力 Widget

顯示為表格的用戶端連線能力 Widget

表格會依掃瞄方法細分用戶端。

如果特定狀態的用戶端數量大於等於 1，您可以按一下該數值來檢視用戶端樹狀結構中的用戶端。您可以在這些用戶端上啟動工作或變更其設定。

如果只要顯示使用特定掃瞄方法的用戶端，請按一下「全部」，然後選取掃瞄方法。

圖 2-4. 標準用戶端的連線狀態

圖 2-5. 雲端掃瞄用戶端的連線狀態

如果您已選取「雲端截毒掃瞄」：

- 表格會依與主動式雲端截毒技術伺服器的連線狀態細分線上雲端掃瞄用戶端。

  注意

  只有線上用戶端可以報告他們與主動式雲端截毒技術伺服器的連線狀態。

  如果用戶端與主動式雲端截毒技術伺服器之間的連線中斷，請執行主動式雲端截毒伺服器來源無法使用 第 14-35 頁中所述的步驟來恢復連線。

- 每一部主動式雲端截毒技術伺服器都是可點選的 URL，按一下即可啟動伺服器的主控台。

- 如果有多部主動式雲端截毒技術伺服器，請按一下「更多」。此時會開啟新畫面，其中顯示所有的主動式雲端截毒技術伺服器。

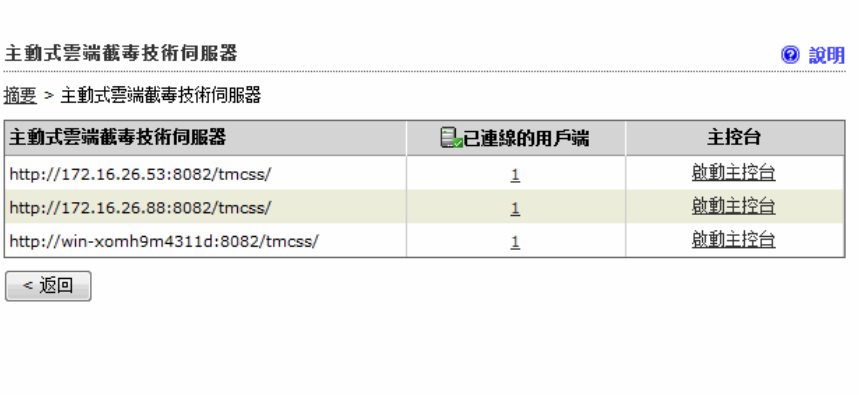


圖 2-6. 主動式雲端截毒技術伺服器清單

在此畫面中，您可以：

- 檢視用戶端所連線的所有主動式雲端截毒技術伺服器，以及連線到每部伺服器的用戶端數目。按一下數字可開啟用戶端樹狀結構，並在其中管理用戶端設定。
- 按一下伺服器的連結即可啟動伺服器的主控台。

以圓形圖顯示的用戶端連線能力 Widget

圓形圖只會顯示各個狀態的用戶端數目，但不會依掃瞄方法細分用戶端。按一下狀態，即可將其與圓形圖的剩餘部分分開，或將其重新連接到圓形圖的剩餘部分。

圖 2-7. 顯示圓形圖的用戶端連線能力 Widget

安全威脅偵測 Widget

安全威脅偵測測 Widget 會顯示安全風險和中毒電腦的數量。

圖 2-8. 安全威脅偵測 Widget

如果中毒電腦的數量大於等於 1，則可以按一下該數值檢視用戶端樹狀結構中的中毒電腦。您可以在這些電腦的用戶端上啟動工作或變更其設定。

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。

圖 2-9. 病毒爆發 Widget

在此 Widget 中，您可以：

- 按一下警訊的日期/時間連結檢視病毒爆發詳細資料。
- 重設病毒爆發警訊狀態資訊，並在 OfficeScan 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 7-94 頁。

- 按一下「檢視前 10 名安全威脅統計資料」，查看最常見的安全風險、安全風險數量最多的電腦和主要的感染來源。隨即顯示新畫面。

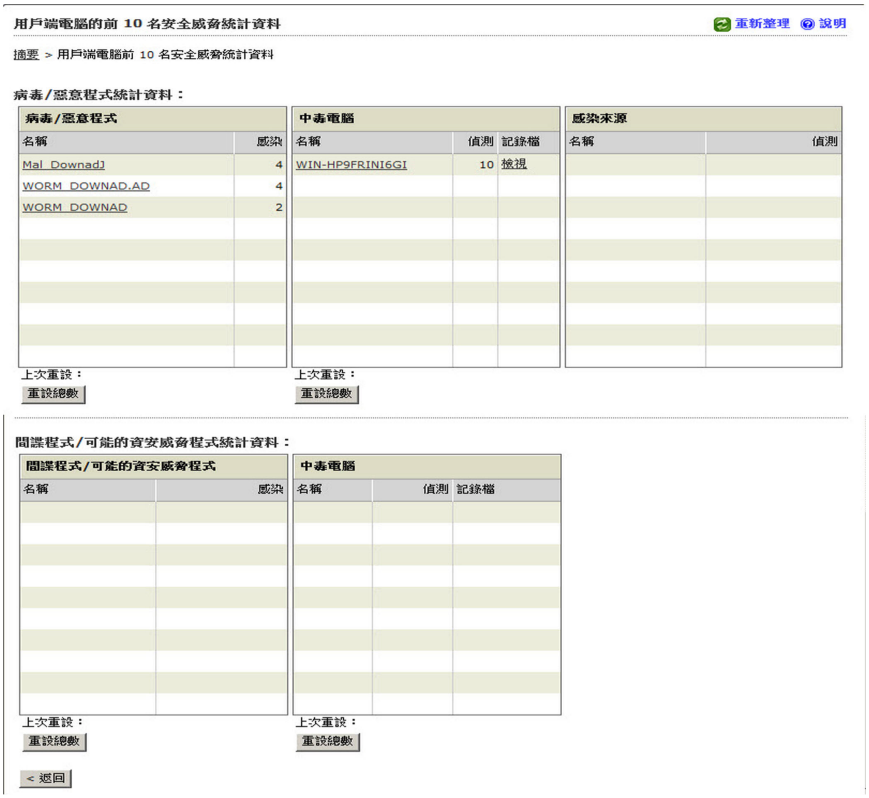


圖 2-10. 前 10 名安全威脅統計資料畫面

在「前 10 名安全威脅統計資料」畫面中，您可以：

- 按一下安全威脅名稱檢視安全威脅的詳細資訊。
- 按一下電腦名稱檢視特定電腦的整體狀態。
- 按一下與電腦名稱對應的「檢視」，檢視電腦的安全威脅記錄檔。
- 按一下「重設計數」重設各資料表內的統計資料。

用戶端更新 Widget

用戶端更新 Widget 會顯示可保護用戶端電腦免於安全威脅的元件和程式。

圖 2-11. 用戶端更新 Widget

在此 Widget 中，您可以：

- 檢視每個元件的目前版本。
- 在「已過期」欄下，檢視具有過期元件的用戶端數。如果有需要更新的用戶端，請按一下數目連結開始更新。
- 您可按一下與各程式對應的數字連結以檢視尚未升級程式的用戶端。

注意

如果要升級 Cisco Trust Agent，請移至「Cisco NAC > 代理程式部署」。

「OfficeScan 與 Plug-ins 混搭」Widget

此 OfficeScan 和 Plug-ins 混搭 Widget 會將 OfficeScan 用戶端中的資料和安裝的嵌入程式中的資料結合，然後將資料顯示在用戶端樹狀結構中。此 Widget 有助於快速評估用戶端上的保護範圍，並減少管理個別嵌入程式所需的管理費用。

圖 2-12.「OfficeScan 與 Plug-ins 混搭」Widget

此 Widget 會顯示以下嵌入程式的資料：

- Intrusion Defense Firewall
- 趨勢科技虛擬桌面支援

您必須為混搭 Widget 啟動這些嵌入程式，才能顯示資料。如果有更新版本可用，則升級嵌入程式。

在此 Widget 中，您可以：

- 選擇顯示在用戶端樹狀結構中的欄。按一下編輯圖示（ ），該圖示位於 Widget 右上角，然後在顯示的畫面中選取欄。

表 2-6. OfficeScan 和 Plug-ins 混搭欄

欄名稱	說明
電腦名稱	端點名稱 此欄始終可用，無法移除。
網域階層	OfficeScan 用戶端樹狀結構中的端點網域
連線狀態	OfficeScan 用戶端與其上層 OfficeScan 伺服器之間的連線
病毒/惡意程式	OfficeScan 用戶端偵測到的病毒和惡意程式數目
間諜程式/可能的資安威脅程式	OfficeScan 用戶端偵測到的間諜程式和可能的資安威脅程式數目
VDI 支援	指出端點是否為虛擬機器
IDF 安全資料檔	如需這些欄和欄顯示的資料的詳細資訊，請參閱 IDF 文件。
IDF 防火牆	
IDF 狀態	
IDF DPI	

- 按兩下表格中的資料。如果按兩下 OfficeScan 資料，將會顯示 OfficeScan 用戶端樹狀結構。如果按兩下嵌入程式資料（VDI 支援欄中的資料除外），會顯示嵌入程式主畫面。
- 使用搜尋功能尋找個別端點。您可以輸入完整或部分的主機名稱。

「最常見的 Data Loss Prevention 事件」Widget

只有在啟用 OfficeScan 資料安全保護後，此 Widget 才可使用。

此 Widget 會顯示數位資產的傳輸次數，而不管處理行動是封鎖還是暫不處理。

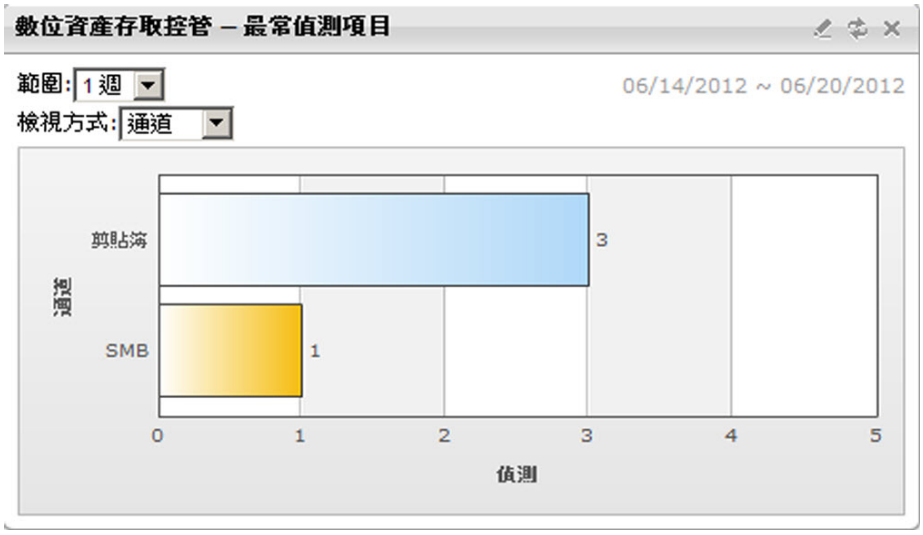


圖 2-13.「最常見的 Data Loss Prevention 事件」Widget

如果要檢視資料：

1. 選取偵測的時間範圍。從下列選項選擇：
   - 今天：過去 24 小時內（包括目前時刻）的偵測
   - 1 週：過去 7 天內（包括當日）的偵測
   - 2 週：過去 14 天內（包括當日）的偵測
   - 1 個月：過去 30 天內（包括當日）的偵測
2. 選取時間範圍後，從下列選項選擇：
   - 使用者：傳輸數位資產次數最高的使用者
   - 通道：最常用於傳輸數位資產的通道
   - 範本：觸發大多數偵測的數位資產範本
   - 電腦：傳輸數位資產次數最高的電腦

注意

此 Widget 最多顯示 10 個使用者、通道、範本或電腦。

歷來 Data Loss Prevention 事件 Widget

只有在啟用 OfficeScan 資料安全保護後，此 Widget 才可使用。

此 Widget 會繪製一段時間以來的數位資產傳輸次數。傳輸包括遭到封鎖或暫不處理（允許）的傳輸。

圖 2-14. 歷來 Data Loss Prevention 事件 Widget

如果要檢視資料，請選取偵測的時間範圍。從下列選項選擇：

- 今天：過去 24 小時內（包括目前時刻）的偵測
- 1 週：過去 7 天內（包括當日）的偵測
- 2 週：過去 14 天內（包括當日）的偵測

- 1 個月：過去 30 天內（包括當日）的偵測

網頁信譽評等最常見的安全威脅來源 Widget

此 Widget 會顯示「網頁信譽評等服務」進行的安全威脅偵測總數。這些資訊會依地理位置顯示在世界地圖中。如需使用此 Widget 的說明，請按一下 Widget 頂端的「 說明 」按鈕 ( )。

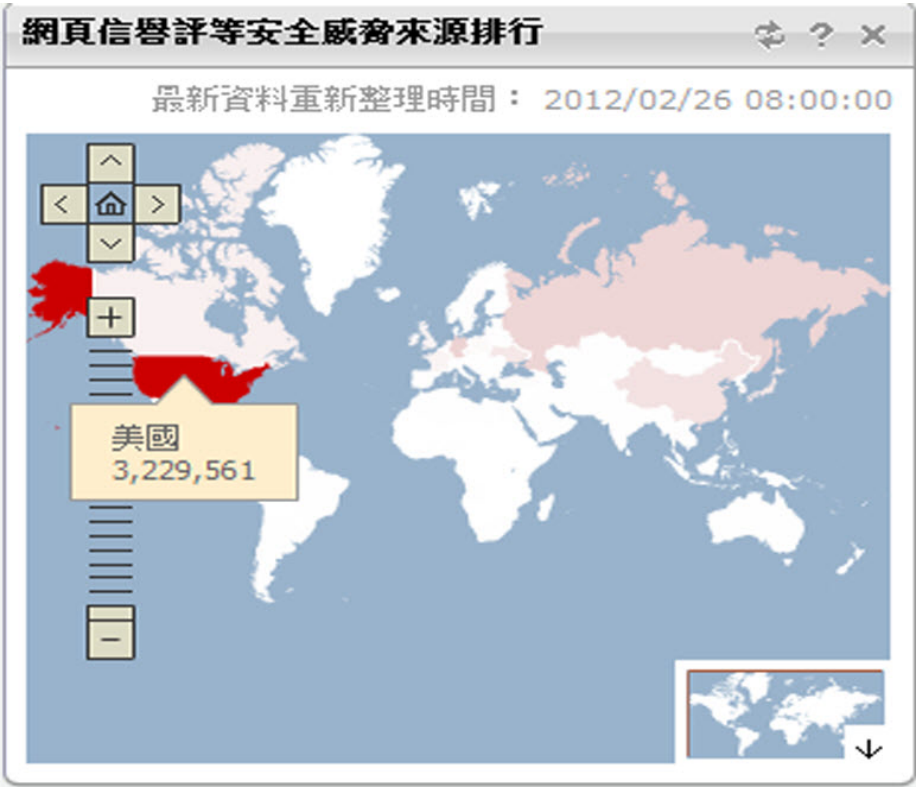


圖 2-15. 網頁信譽評等最常見的安全威脅來源 Widget

網頁信譽評等最受威脅的使用者 Widget

此 Widget 會顯示「網頁信譽評等服務」偵測到的惡意 URL 所影響的使用者數量。這些資訊會依地理位置顯示在世界地圖中。如需使用此 Widget 的說明，請按一下 Widget 頂端的「 說明 」按鈕 ( )。

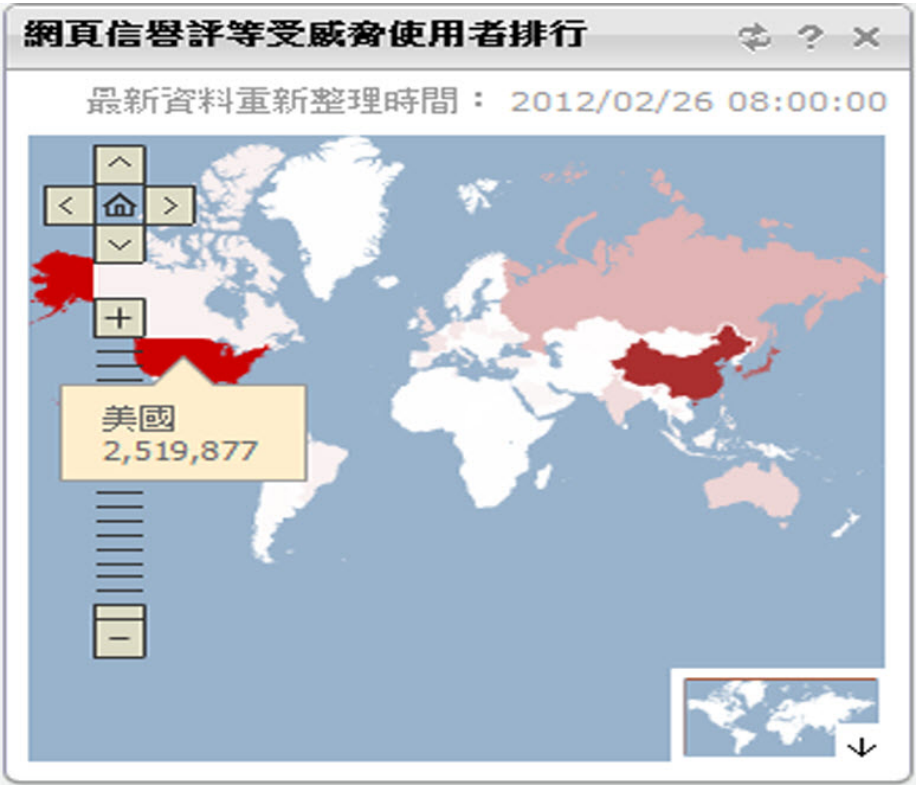


圖 2-16. 網頁信譽評等最受威脅的使用者 Widget

檔案信譽評等安全威脅分佈圖 Widget

此 Widget 會顯示「檔案信譽評等服務」進行的安全威脅偵測總數。這些資訊會依地理位置顯示在世界地圖中。如需使用此 Widget 的說明，請按一下 Widget 頂端的「 說明 」按鈕（ ）。

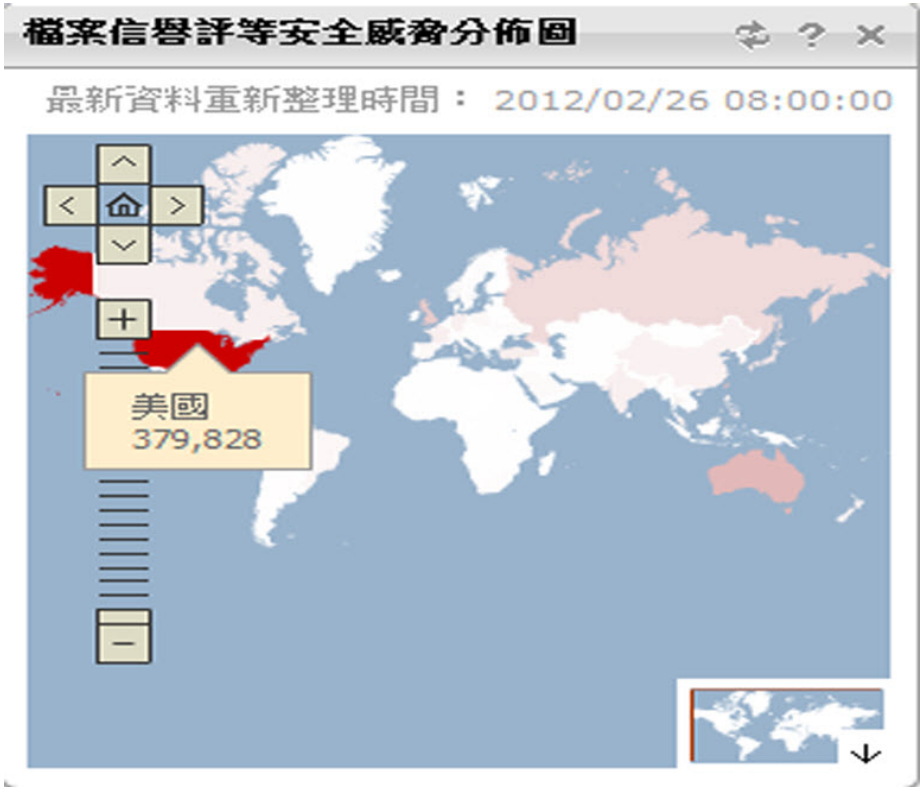


圖 2-17. 檔案信譽評等安全威脅分佈圖 Widget

Active Directory 整合

整合 OfficeScan 與您的 Microsoft™Active Directory™ 結構，讓您更有效率地管理 OfficeScan 用戶端、使用 Active Directory 帳號指派 Web 主控台權限，以及判斷哪些用戶端未安裝安全防護軟體。網路網域中所有的使用者都可以安全存取 OfficeScan 主控台。您也可以針對特定使用者（甚至是在另一個網域中的使用者）設定有限制的存取。驗證程序和加密金鑰會提供使用者認證的驗證。

Active Directory 整合可讓您充分利用下列功能：

- 以角色為基礎的管理：授與使用者使用其 Active Directory 帳號存取產品主控台的權限，將特定的管理責任指派給該使用者。如需詳細資訊，請參閱以角色為基礎的管理 第 13-2 頁。
- 自訂用戶端群組：使用 Active Directory 或 IP 位址，以手動方式將用戶端分組，然後將它們對應到 OfficeScan 用戶端樹狀結構中的網域。如需詳細資訊，請參閱自動用戶端分組 第 2-43 頁。
- 外部伺服器管理：確保位於網路中但不受 OfficeScan 伺服器管理的電腦都符合公司的安全指導方針。如需詳細資訊，請參閱適用於未受管端點的安全性符合 第 14-60 頁。

手動或定期同步處理 Active Directory 結構與 OfficeScan 伺服器，以確保資料一致性。如需詳細資訊，請參閱同步處理資料與 Active Directory 網域 第 2-28 頁。

將 Active Directory 與 OfficeScan 整合

程序

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

a. 按一下「輸入網域認證」。

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

- 網域\使用者名稱
- 使用者名稱@網域

c. 按一下「儲存」。

4. 按一下（ + ）按鈕可新增更多網域。如有必要，請指定網域認證給任何新增的網域。

5. 按一下（ - ）按鈕可刪除網域。

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

a. 移至「網域認證的加密設定」區段。

b. 請輸入不超過 128 個字元的加密金鑰。

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

警告!

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

7. 按一下下列其中一個項目：

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

8. 預約定期同步處理。如需詳細資訊，請參閱同步處理資料與 Active Directory 網域 第 2-28 頁。

同步處理資料與 Active Directory 網域

定期同步處理資料與 Active Directory 網域，可讓 OfficeScan 用戶端樹狀結構保持最新狀態以及查詢未受管理的用戶端。

手動同步處理資料與 Active Directory 網域

程序

1. 瀏覽至「管理 > Active Directory > Active Directory 整合」。
2. 確認網域認證與加密設定並未變更。
3. 按一下「存儲並同步處理」。

自動同步處理資料與 Active Directory 網域

程序

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

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

4. 按一下「儲存」。

OfficeScan 用戶端樹狀結構

OfficeScan 用戶端樹狀結構會顯示伺服器目前管理的所有用戶端（歸入 OfficeScan 網域 第 2-42 頁）。將用戶端歸入網域中，即可同時設定、管理和套用相同組態設定至所有網域成員。

當您存取主功能表中的特定功能時，用戶端樹狀結構會顯示在主框架中。

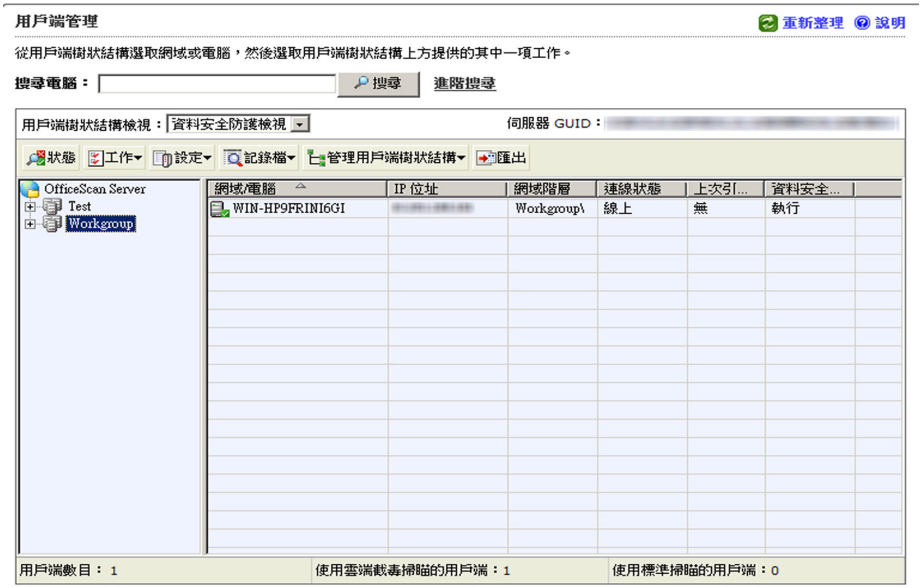


圖 2-18. OfficeScan 用戶端樹狀結構

用戶端樹狀結構圖示

OfficeScan 用戶端樹狀結構圖示提供視覺提示，指出 OfficeScan 所管理之電腦的類型和 OfficeScan 用戶端的狀態。

表 2-7. OfficeScan 用戶端樹狀結構圖示

圖示	說明
	網域
	根目錄
	更新代理程式
	雲端截毒掃瞄可用的 OfficeScan 用戶端
	雲端截毒掃瞄不可用的 OfficeScan 用戶端
	雲端截毒掃瞄可用的更新代理程式
	雲端截毒掃瞄不可用的更新代理程式

用戶端樹狀結構一般工作

下列是顯示用戶端樹狀結構時，您可以執行的一般工作：

程序

- 按一下根網域圖示 () 以選取所有網域和用戶端。選取根網域圖示並從用戶端樹狀結構上方選擇工作之後，會顯示畫面供您進行設定。在該畫面中，選擇下列一般選項：

- 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
- 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

- 如果要選取多個連續的網域或用戶端：
  - 從右邊面板中選取第一個網域，按住 SHIFT 鍵不放，然後按一下範圍中最後一個網域或用戶端。
- 如果要從右邊面板中選取某個範圍內的不連續網域或用戶端，請按住 CTRL 鍵，然後按一下您要選取的網域或用戶端。
- 請在「搜尋電腦」文字方塊中指定用戶端名稱，以搜尋要管理的用戶端。隨即顯示網域和該網域中所有用戶端的清單，並反白顯示指定的用戶端名稱。如果要移至下一個用戶端，請再按一下「搜尋」。如需更多搜尋選項，請按一下「進階搜尋」。

注意

搜尋特定用戶端時不能指定 IPv6 或 IPv4 位址。請使用「進階搜尋」依 IPv4 或 IPv6 位址進行搜尋。如需詳細資訊，請參閱進階搜尋選項 第 2-32 頁。

- 選取網域後，用戶端樹狀結構表格會展開，以顯示屬於該網域的用戶端和包含每個用戶端相關資訊的所有欄位。如果只要檢視一組相關欄位，請在用戶端樹狀結構檢視中選取一個項目。
  - 檢視全部：顯示所有欄位
  - 更新檢視：顯示所有元件和程式
  - 防毒檢視：顯示防毒元件
  - 間諜程式防護檢視：顯示間諜程式防護元件
  - 資料安全防護檢視：顯示用戶端上「資料安全防護」模組的狀態
  - 防火牆檢視：顯示防火牆元件
  - 雲端防護檢視：顯示用戶端（標準或雲端截毒掃瞄）所使用的掃瞄方法和雲端防護元件

  - 更新代理程式檢視：顯示由 OfficeScan 伺服器的所有更新代理程式的資訊
- 拖曳欄位標題到用戶端樹狀結構的不同位置即可重新安排欄位。OfficeScan 會自動儲存新的欄位位置。
- 按一下欄位名稱即可根據欄位資訊排序用戶端。
- 按一下重新整理圖示（即可重新整理用戶端樹狀結構  ）。
- 檢視用戶端樹狀結構下的用戶端統計資料，例如：用戶端總數、雲端掃瞄用戶端數目，以及標準用戶端數目。

進階搜尋選項

根據下列條件搜尋用戶端：

程序

- 基本：包含電腦的基本資訊，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 位址範圍搜尋需要部分 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電腦。例如，輸入 10.5 會傳回 IP 位址範圍從 10.5.0.0 到 10.5.255.255 的所有電腦。
  - 依 IPv6 位址範圍搜尋時，會要求字首和長度。
  - 依 MAC 位址搜尋需要以十六進位標記表示的 MAC 位址範圍，例如：000A1B123C12。
- 元件版本：選取元件名稱旁邊的核取方塊，選取「低於」或「低於（含）」並輸入版本號碼來縮小條件。根據預設會顯示目前版本號碼。
- 狀態：包含用戶端設定

指定搜尋條件之後，請按一下「搜尋」。用戶端樹狀結構中會顯示符合條件的電腦名稱清單。

用戶端樹狀結構特定工作

當您存取 Web 主控台上的特定畫面時，會顯示用戶端樹狀結構。用戶端樹狀結構上方是功能表項目，功能表項目視您存取的畫面而異。這些功能表項目可讓您執行特定工作，例如設定用戶端設定或開始用戶端工作。如果要執行這些工作，請先選取工作目標（根網域圖示（選取根目錄圖示可將設定套用到所有用戶端）、一或多個網域，或者是一或多個用戶端），然後選取功能表項目。

下列畫面顯示用戶端樹狀結構：

- 「用戶端管理」畫面 第 2-33 頁
- 「病毒爆發防範」畫面 第 2-36 頁
- 用戶端電腦的元件更新畫面 第 2-37 頁
- 「還原」畫面 第 2-38 頁
- 用戶端電腦的安全威脅記錄檔畫面 第 2-39 頁
- 「代理程式部署」畫面 第 2-41 頁

「用戶端管理」畫面

如果要查看此畫面，請瀏覽至用戶端電腦 > 用戶端管理。

在「用戶端管理」畫面中管理一般用戶端設定。

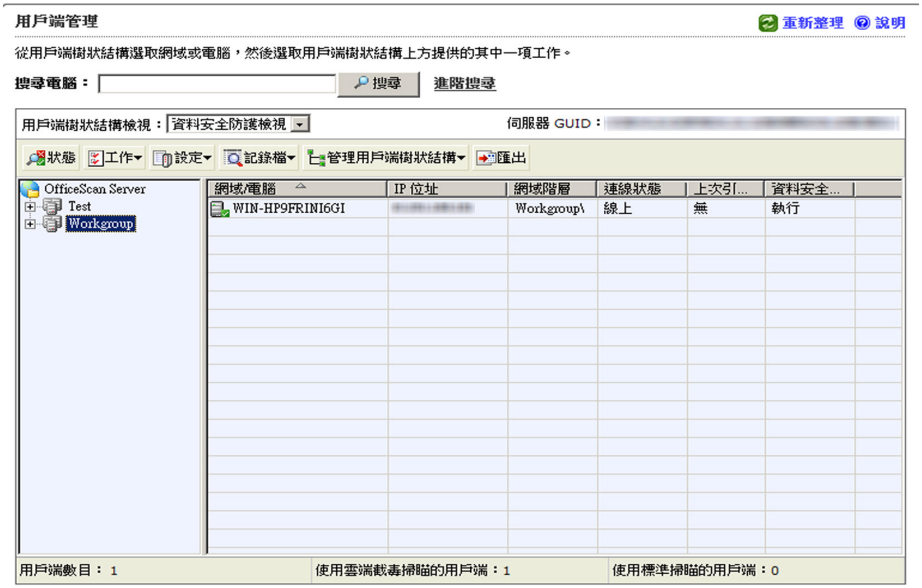


圖 2-19. 「用戶端管理」畫面

下表列出了您可以執行的工作：

表 2-8. 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 OfficeScan 用戶端資訊 第 14-46 頁。
工作	• 在用戶端電腦上執行立即掃瞄。如需詳細資訊，請參閱開始立即掃瞄 第 7-22 頁。 • 解除安裝用戶端。如需詳細資訊，請參閱從 Web 主控台解除安裝 OfficeScan 用戶端 第 5-65 頁。 • 恢復間諜程式/可能的資安威脅程式元件。如需詳細資訊，請參閱回存間諜程式/可能的資安威脅程式 第 7-46 頁。

功能表按鈕	工作

設定	• 設定掃瞄設定。如需詳細資訊，請參閱下列主題：
	  • 掃瞄方法 第 7-6 頁
	  • 手動掃瞄 第 7-16 頁
	  • 即時掃瞄 第 7-13 頁
	  • 預約掃瞄 第 7-18 頁
	  • 立即掃瞄 第 7-20 頁
	• 設定網頁信譽評等設定。如需詳細資訊，請參閱網頁信譽評等策略 第 11-3 頁。
	• 設定行為監控設定。如需詳細資訊，請參閱行為監控 第 8-2 頁。
	• 設定周邊設備存取控管設定。如需詳細資訊，請參閱周邊設備存取控管 第 9-2 頁。
	• 設定 Data Loss Prevention 策略。如需詳細資訊，請參閱 Data Loss Prevention 策略組態設定 第 10-38 頁。
	• 將用戶端指定為「更新代理程式」。如需詳細資訊，請參閱更新代理程式組態設定 第 6-47 頁。
	• 設定用戶端權限和其他設定。如需詳細資訊，請參閱設定用戶端權限及其他設定 第 14-78 頁。
	• 啟動或關閉 OfficeScan 用戶端服務。如需詳細資訊，請參閱 OfficeScan 用戶端服務 第 14-6 頁。
	• 間諜程式/可能的資安威脅程式核可清單。如需詳細資訊，請參閱間諜程式/可能的資安威脅程式核可清單 第 7-44 頁。
	• 匯入和匯出用戶端設定。如需詳細資訊，請參閱匯入和匯出用戶端設定 第 14-47 頁。

功能表按鈕	工作
記錄檔	檢視下列記錄檔： • 病毒/惡意程式記錄檔（如需詳細資訊，請參閱檢視病毒/惡意程式記錄檔 第 7-79 頁） • 間諜程式/可能的資安威脅程式記錄檔（如需詳細資訊，請參閱檢視間諜程式/可能的資安威脅程式記錄檔 第 7-85 頁） • 防火牆記錄檔（如需詳細資訊，請參閱防火牆記錄檔 第 12-26 頁） • 網頁信譽評等記錄檔（如需詳細資訊，請參閱網頁信譽評等記錄檔 第 11-10 頁） • 行為監控記錄檔（如需詳細資訊，請參閱行為監控記錄檔 第 8-10 頁） • 周邊設備存取控管記錄檔（如需詳細資訊，請參閱周邊設備存取控管記錄檔 第 9-16 頁） 刪除記錄檔。如需詳細資訊，請參閱記錄檔管理 第 13-31 頁。
管理用戶端樹狀結構	管理用戶端樹狀結構。如需詳細資訊，請參閱用戶端分組工作 第 2-48 頁。
匯出	將用戶端清單匯出到逗號分隔值 (CSV) 檔案。

「病毒爆發防範」畫面

如果要查看此畫面，請瀏覽至用戶端電腦 > 病毒爆發防範。

在「病毒爆發防範」畫面中指定並啟用病毒爆發防範設定。如需詳細資訊，請參閱設定安全威脅爆發防範 第 7-93 頁。

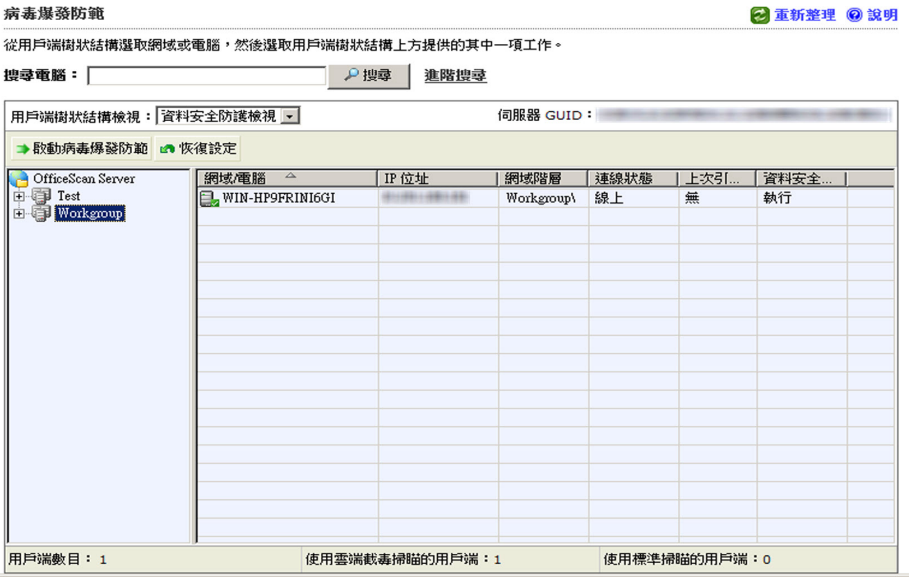


圖 2-20. 「病毒爆發防範」畫面

用戶端電腦的元件更新畫面

如果要查看此畫面，請瀏覽至更新 > 用戶端電腦 > 手動更新。選取「手動選取用戶端」，然後按一下「選取」。

在「用戶端電腦的元件更新」畫面中啟動手動更新。如需詳細資訊，請參閱 OfficeScan 用戶端手動更新 第 6-37 頁。

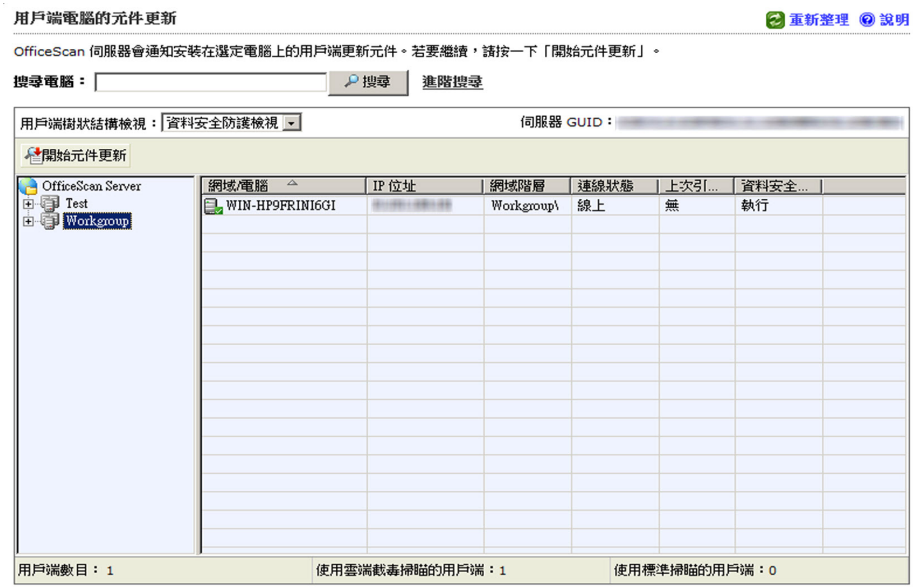


圖 2-21. 用戶端電腦的元件更新畫面

「還原」畫面

如果要查看此畫面，請瀏覽至更新 > 還原。按一下「同步處理伺服器」。

在「還原」畫面中還原用戶端元件。如需詳細資訊，請參閱 OfficeScan 用戶端的還原元件 第 6-44 頁。

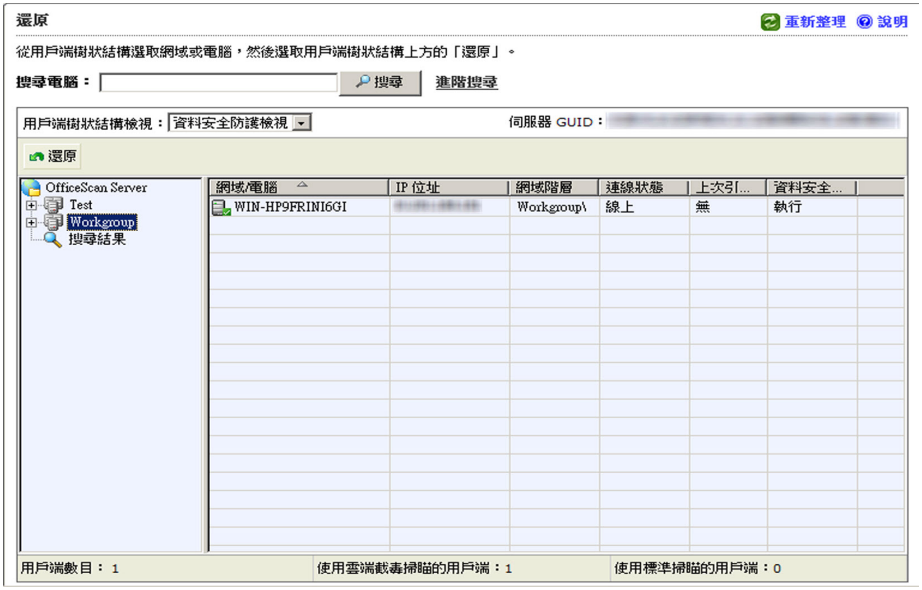


圖 2-22. 「還原」畫面

用戶端電腦的安全威脅記錄檔畫面

如果要查看此畫面，請瀏覽至記錄檔 > 用戶端電腦記錄檔 > 安全威脅。

在「用戶端電腦的安全威脅記錄檔」畫面中檢視和管理記錄檔。

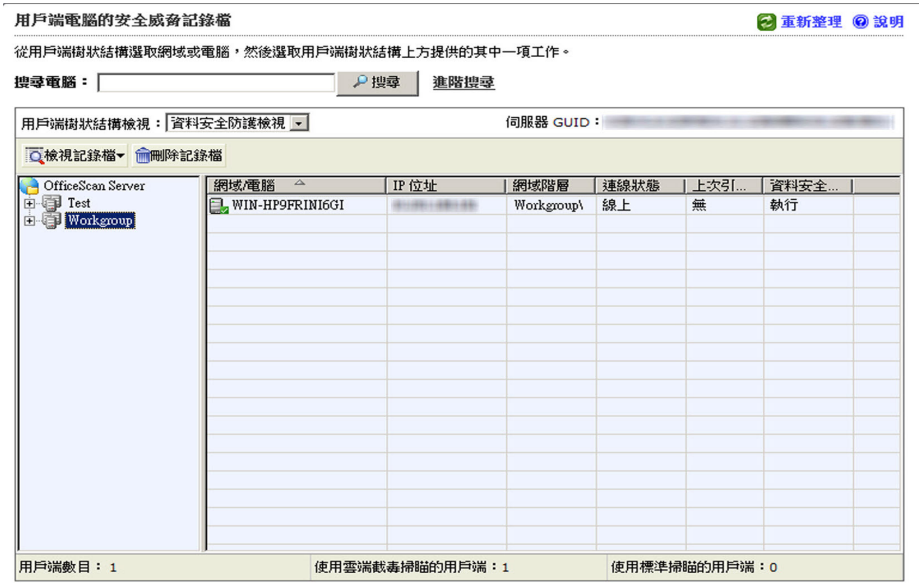


圖 2-23. 用戶端電腦的安全威脅記錄檔畫面

執行下列工作：

1. 檢視用戶端傳送至伺服器的記錄檔。如需詳細資訊，請參閱：
   - 檢視病毒/惡意程式記錄檔 第 7-79 頁
   - 檢視間諜程式/可能的資安威脅程式記錄檔 第 7-85 頁
   - 檢視防火牆記錄檔 第 12-26 頁
   - 檢視網頁信譽評等記錄檔 第 11-10 頁
   - 檢視行為監控記錄檔 第 8-11 頁
   - 檢視周邊設備存取控管記錄檔 第 9-16 頁
   - 檢視 Data Loss Prevention 記錄檔 第 10-47 頁

2. 刪除記錄檔。如需詳細資訊，請參閱記錄檔管理 第 13-31 頁。

「代理程式部署」畫面

如果要查看此畫面，請瀏覽至「Cisco NAC > 代理程式部署。

如果已設定策略伺服器 for Cisco NAC，請在「代理程式部署」畫面中，將 Cisco Trust Agent (CTA) 部署到用戶端。如需詳細資訊，請參閱 Cisco Trust Agent 部署 第 16-25 頁。

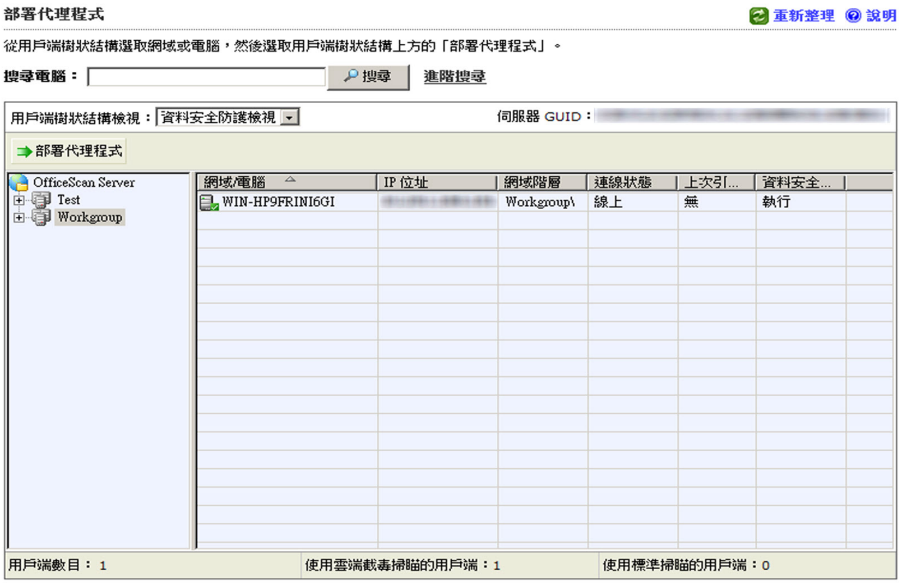


圖 2-24. 「代理程式部署」畫面

OfficeScan 網域

OfficeScan 中的網域是一組擁有相同設定並執行相同工作的用戶端。只要將用戶端歸入網域中，即可設定、管理和套用相同組態設定至所有網域成員。如需有關用戶端分組的詳細資訊，請參閱用戶端分組 第 2-42 頁。

用戶端分組

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

有兩種方法可將用戶端歸入網域中。

表 2-9. 用戶端分組方法

方法	用戶端分組	說明
手動	• NetBIOS 網域 • Active Directory 網域 • DNS 網域	手動用戶端分組會定義新安裝的用戶端應屬於哪一個網域。當該用戶端顯示在用戶端樹狀結構中時，您可以將其移至其他網域或其他的 OfficeScan 伺服器。 透過手動用戶端分組，還可以在用戶端樹狀結構中建立、管理和移除網域。 如需詳細資訊，請參閱手動用戶端分組 第 2-42 頁。
自動	自訂用戶端群組	自動用戶端分組會使用規則來排序用戶端樹狀結構中的用戶端。定義規則之後，您可以在發生特定事件時或以預約的時間間隔，存取用戶端樹狀結構以手動排序用戶端，或允許 OfficeScan 自動排序用戶端。 如需詳細資訊，請參閱自動用戶端分組 第 2-43 頁。

手動用戶端分組

OfficeScan 只有在全新的用戶端安裝時才會使用此設定。安裝程式會檢查目標電腦所屬的網路網域。如果網域名稱已存在於用戶端樹狀結構，則 OfficeScan 會將目標電腦上的用戶端分組到該網域下，而且會套用針對該網域所設定的設

定。如果該網域名稱不存在，OfficeScan 會將該網域新增到用戶端樹狀結構、將該用戶端分組在該網域下，然後套用根目錄設定至該網域和用戶端。

設定手動用戶端分組

程序

1. 瀏覽至「用戶端電腦 > 用戶端分組」。
2. 指定用戶端分組法：
   - NetBIOS 網域
   - Active Directory 網域
   - DNS 網域
3. 按一下「儲存」。

接下來需執行的動作

請執行以下工作來管理網域以及分組在這些網域下的用戶端：

- 新增網域
- 刪除網域或用戶端
- 重新命名網域
- 將用戶端移至另一個網域

如需詳細資訊，請參閱用戶端分組工作 第 2-48 頁。

自動用戶端分組

自動用戶端分組會使用由 IP 位址或 Active Directory 網域定義的規則。如果某個規則定義了 IP 位址或 IP 位址範圍，則 OfficeScan 伺服器會將 IP 位址相符的用戶端分組到用戶端樹狀結構中的特定網域。同樣地，如果某個規則定義了一個或多個 Active Directory 網域，則 OfficeScan 伺服器會將屬於特定 Active Directory 網域的用戶端分組到用戶端樹狀結構中的特定網域。

用戶端一次只會套用一個規則。設定規則的優先順序，以便用戶端在符合多個規則時，只套用最高優先順序的規則。

設定自動用戶端分組

程序

1. 瀏覽至「用戶端電腦 > 用戶端分組」。
2. 移至「用戶端分組」區段，然後選取「自訂用戶端群組」。
3. 移至「自動用戶端分組」區段。
4. 如果要開始建立規則，請按一下「新增」，然後選取「Active Directory」或「IP 位址」。
   - 如果選取「Active Directory」，請參閱依 Active Directory 網域定義用戶端分組規則 第 2-45 頁中的組態設定指示。
   - 如果選取「IP 位址」，請參閱依 IP 位址定義用戶端分組規則 第 2-47 頁中的組態設定指示。
5. 如果建立了多個規則，請執行以下步驟來設定規則的優先順序：
   a. 選取某個規則。
   b. 按一下「分組優先順序」欄下的箭頭，在清單中上移或下移該規則。規則的 ID 號碼則會變更以反映新位置。
6. 如果要在用戶端排序期間使用規則：
   a. 選取要使用的規則的核取方塊。
   b. 請確定已啟動這些規則。在「狀態」欄下，綠色核取記號圖示 ( )。如果出現紅色「x」記號圖示 ( )，按一下該圖示即啟動該規則，並且會將該圖示變更為綠色。

注意

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

7. 在「預約網域建立」區段指定排序預約。
   a. 選取「啟動預約網域建立」。
   b. 在「基於預約的網域建立」下指定預約。
8. 請從下列選項選擇：
   - 儲存並立即建立網域：如果您在步驟 7 的依 IP 位址定義用戶端分組規則 第 2-47 頁或步驟 7 的依 Active Directory 網域定義用戶端分組規則 第 2-45 頁中指定了新網域，則選擇此選項：
   - 儲存：如果您尚未指定新網域或只有在用戶端排序執行時才要建立新網域，則選擇此選項：

   注意
   完成此步驟後，不會啟動用戶端排序。
9. 如果要立即排序用戶端，請移至用戶端樹狀結構，然後排序用戶端。如需詳細資訊，請參閱排序用戶端 第 2-51 頁。如果在步驟 6 中設定了排序預約，則會在指定的日期和時間啟動排序。當發生以下事件時，OfficeScan 也會執行排序工作：
   - 安裝用戶端。
   - 用戶端重新載入。
   - 用戶端的 IP 位址發生變更。
   - 用戶端使用者啟動或關閉行動模式。

依 Active Directory 網域定義用戶端分組規則

在執行以下程序中的步驟之前，請確定已設定 Active Directory 整合設定。如需詳細資訊，請參閱Active Directory 整合 第 2-26 頁。

程序

1. 瀏覽至「用戶端電腦 > 用戶端分組」。

2. 移至「用戶端分組」區段，然後選取「自訂用戶端群組」。
3. 移至「自動用戶端分組」區段。
4. 按一下「新增」，然後選取「Active Directory」。

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

   a. 將滑鼠游標移至特定 OfficeScan 網域上並按一下「新增網域」圖示。在以下的範例中，新網域會新增至 OfficeScan 根網域底下。

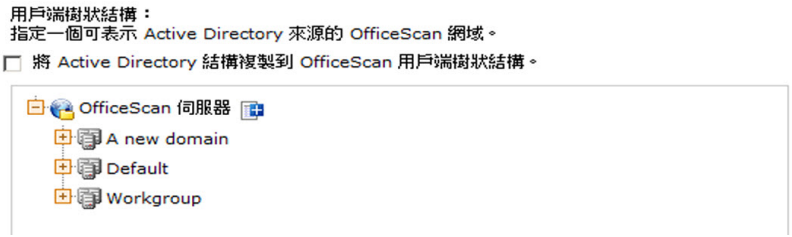


圖 2-25. 新增網域圖示

   b. 在出現的文字方塊中輸入網域名稱。

   c. 按一下文字方塊旁邊的選取記號。隨即新增並自動選取新網域。
9. （選用）選取「將 Active Directory 結構複製到 OfficeScan 用戶端樹狀結構」。此選項會將所選取 Active Directory 網域的階層複製到選取的 OfficeScan 網域。
10. 按一下「儲存」。

依 IP 位址定義用戶端分組規則

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

程序

1. 瀏覽至「用戶端電腦 > 用戶端分組」。
2. 移至「用戶端分組」區段，然後選取「自訂用戶端群組」。
3. 移至「自動用戶端分組」區段。
4. 按一下「新增」，然後選取「IP 位址」。

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

   注意

   如果雙堆疊用戶端的 IPv4 和 IPv6 位址屬於兩個單獨的用戶端群組，則這個用戶端會被分組在 IPv6 群組下。如果在用戶端的主機上關閉了 IPv6，則用戶端會移至 IPv4 群組。
8. 選取 IP 位址或 IP 位址範圍對應的 OfficeScan 網域。如果網域不存在，請執行下列動作：
   a. 將滑鼠游標移至用戶端樹狀結構上任意一處，然後按一下新增網域圖示。

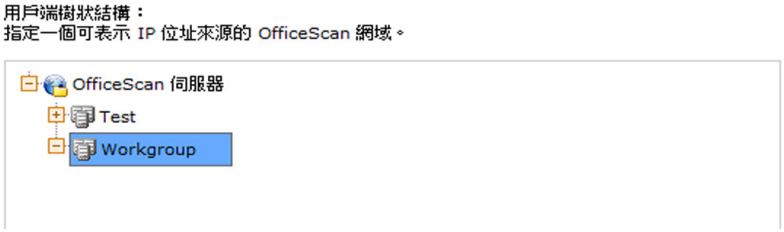


圖 2-26. 新增網域圖示

b. 在出現的文字方塊中輸入網域。

c. 按一下文字方塊旁邊的選取記號。隨即新增並自動選取新網域。

9. 按一下「儲存」。

用戶端分組工作

在對網域中的用戶端進行分組時，您可以執行下列工作：

如果是手動用戶端分組：

- 新增網域。如需詳細資訊，請參閱新增網域 第 2-49 頁。
- 刪除網域或用戶端。如需詳細資訊，請參閱刪除網域或用戶端 第 2-49 頁。
- 重新命名網域。如需詳細資訊，請參閱重新命名網域 第 2-50 頁。
- 將用戶端移至其他網域或其他 OfficeScan 伺服器。如需詳細資訊，請參閱將 OfficeScan 用戶端移至其他網域或 OfficeScan 伺服器 第 2-50 頁。

如果是自動用戶端分組：

- 排序用戶端。如需詳細資訊，請參閱排序用戶端 第 2-51 頁。
- 刪除網域或用戶端。如需詳細資訊，請參閱刪除網域或用戶端 第 2-49 頁。

新增網域

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 按一下「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. 按一下「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. 按一下「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

程序

1. 瀏覽至「用戶端電腦 > 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、多個或所有的用戶端
3. 按一下「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，只要按一下「移除網域/用戶端」即可。如果該網域具有用戶端，當您按一下「移除域/用戶端」，OfficeScan 伺服器會重新建立網域並在下次用戶端連線到 OfficeScan 伺服器時將所有的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. 刪除所有用戶端。

5. 如果要刪除用戶端，請按一下「移除網域/用戶端」。

注意

從用戶端樹狀結構中刪除用戶端並不會從用戶端電腦中移除 OfficeScan 用戶端。OfficeScan 用戶端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，也不會傳送通知到用戶端。

重新命名網域

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 從用戶端樹狀結構中選取一個網域。
3. 按一下「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. 按一下「重新命名」。

   新網域名稱會出現在用戶端樹狀結構中。

將 OfficeScan 用戶端移至其他網域或 OfficeScan 伺服器

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，開啟某個網域，然後選取一個、多個或所有的用戶端。

3. 按一下「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：
   - 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 OfficeScan 伺服器：
   - 選取「將選取的用戶端移動到其他 OfficeScan 伺服器」。
   - 輸入伺服器名稱或 IPv4/IPv6 位址，以及 HTTP 通訊埠號碼。
6. 按一下「移動」。

排序用戶端

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，執行以下任何操作：
   - 如果要排序所有的用戶端，請按一下 OfficeScan 根網域圖示（  ）。
   - 如果只要排序屬於特定網域的用戶端，請選取這些網域。
   - 如果要排序屬於特定網域的多個或所有用戶端，請開啟該網域，然後選取用戶端。
3. 按一下「管理用戶端樹狀結構 > 排序用戶端」。
4. 按一下「開始」。

5. 完成排序時，按一下「關閉」。已排序的用戶端現在應該屬於其指定的網域。

第 3 章

使用資料安全防護

本章討論如何安裝及啟動資料安全防護模組。

本章內容：

資料安全防護安裝

「資料安全防護」模組包含下列功能：

- Data Loss Prevention (DLP)：防止未經授權傳輸數位資產
- 周邊設備存取控管：規範對於外部裝置的存取

注意

OfficeScan 內建「周邊設備存取控管」功能，可規範對於常用裝置（例如：USB 儲存裝置）的存取。「周邊設備存取控管」（「資料安全防護」模組的一部分）可擴大監控的裝置範圍。如需受監控的裝置清單，請參閱周邊設備存取控管 第 9-2 頁。

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

重要

- 如果端點已安裝單機版 Trend Micro Data Loss Prevention 軟體並正在執行該軟體，您就不需要安裝「資料安全防護」模組。
- 「資料安全防護」模組可以安裝在純 IPv6 Plug-In Manager 上。但是，只有「周邊設備存取控管」功能可以部署到純 IPv6 用戶端。「Data Loss Prevention」無法在純 IPv6 用戶端上運作。

安裝資料安全防護

程序

1. 開啟 OfficeScan Web 主控台，然後按一下主功能表中的「Plug-in Manager」。

2. 在 Plug-in Manager 畫面上，移至「OfficeScan 資料安全防護」區段，然後按一下「下載」。

   要下載的檔案大小會顯示在「下載」按鈕旁。

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

   注意

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

3. 監控下載進度。

   下載期間您可以瀏覽其他畫面。

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

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

   注意

   如果未顯示「OfficeScan 資料安全防護」，請參閱 Plug-In Manager 疑難排解 第 15-9 頁，以查知原因和解決方案。

4. 如果要立即安裝「OfficeScan 資料安全防護」，請按一下「立即安裝」，或者如果要稍後安裝，請執行下列步驟：

   a. 按一下「稍後安裝」。

b. 開啟「Plug-in Manager」畫面。

c. 移至「OfficeScan 資料安全防護」區段，然後按一下「安裝」。

5. 閱讀授權合約，然後按一下「同意」表示您接受其中的條款。

   安裝便會開始。

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

資料安全防護使用授權

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

請從趨勢科技取得啟動碼，然後用它來註冊使用授權。

啟動或續約資料安全防護使用授權

程序

1. 開啟 OfficeScan Web 主控台，然後按一下主功能表中的「Plug-in Manager」。
2. 在 Plug-in Manager 畫面上，移至「OfficeScan 資料安全防護」區段，然後按一下「管理程式」。
3. 按一下「新啟動碼」
4. 輸入啟動碼。

   您也可以複製啟動碼，然後將它貼到任一文字方塊中。
5. 按一下「儲存」。

檢視資料安全防護使用授權資訊

程序

1. 開啟 OfficeScan Web 主控台，然後按一下主功能表中的「Plug-in Manager」。
2. 在 Plug-in Manager 畫面上，移至「OfficeScan 資料安全防護」區段，然後按一下「管理程式」。
3. 按一下「檢視使用授權資訊」。
4. 在開啟的畫面中檢視下列使用授權詳細資訊。
   - 狀態：顯示「已啟動」、「未啟動」或「已到期」。
   - 版本：顯示「完整版」或「試用版」。同時啟動完整版和試用版時顯示的版本是「完整版」。
   - 授權數目：顯示可安裝「資料安全防護」模組的 OfficeScan 用戶端數量
   - 使用授權逾期期限：如果「資料安全防護」有多個使用授權，會顯示最新的到期日。例如，如果使用授權到期日為 2011/12/31 和 2011/6/30，則會顯示 2011/12/31。
   - 啟動碼：顯示啟動碼
   - 提醒：視您目前的使用授權版本而定，資料安全防護會在寬限期（僅完整版）或使用授權到期時，顯示使用授權到期日提醒。

   
   注意

   寬限期視地區而定。請向您的趨勢科技銷售人員確認寬限期。

   如果沒有續約使用授權，「Data Loss Prevention」和「周邊設備存取控管」仍可運作，但您將無法再取得技術支援。
5. 按一下「線上檢視詳細的使用授權」，在趨勢科技網站上檢視您的使用授權相關資訊。

6. 如果要更新畫面以顯示最新的使用授權資訊，請按一下「更新資訊」。

將「資料安全防護」部署到用戶端

註冊「資料安全防護」模組的使用授權之後，您就可以將它部署到 OfficeScan 用戶端。部署之後，OfficeScan 用戶端會開始使用「Data Loss Prevention」和「周邊設備存取控管」。

重要

- 依預設，Windows Server 2003、Windows Server 2008 和 Windows Server 2012 會關閉此模組，以避免主機的效能受到影響。如果要啟動此模組，請持續監控系統效能，並在發現效能變差時採取必要的處理行動。

  注意

  您可以從 Web 主控台啟動或關閉此模組。如需詳細資訊，請參閱 OfficeScan 用戶端服務 第 14-6 頁。

- 如果 Trend Micro Data Loss Prevention 軟體已存在於端點上，OfficeScan 不會使用「資料安全防護」模組來取代它。
- 只有「周邊設備存取控管」能部署到純 IPv6 用戶端。「Data Loss Prevention」無法在純 IPv6 用戶端上運作。
- 線上用戶端會立即安裝「資料安全防護」模組。離線和行動用戶端會在成為線上狀態時安裝此模組。
- 使用者必須重新啟動電腦，才能完成 Data Loss Prevention 驅動程式的安裝。重新啟動之前請先通知使用者。
- 趨勢科技建議您啟動偵錯記錄功能，以協助您解決部署問題。如需詳細資訊，請參閱資料安全防護偵錯記錄檔 第 10-52 頁。

將「資料安全防護」模組部署到用戶端

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，您可以：
   - 按一下根網域圖示 ()，以將該模組部署到所有現有和未來的用戶端。
   - 選取特定網域，以將該模組部署到該網域下的所有現有和未來的用戶端。
   - 選取特定用戶端，只將該模組部署到該用戶端。
3. 以兩種方式進行部署：
   - 按一下「設定 > DLP 設定」。
   - 按一下「設定 > 周邊設備存取控管設定」。

   注意

   如果您從「設定 > DLP 設定」部署，然後成功部署資料安全防護模組，系統將會安裝 Data Loss Prevention 驅動程式。如果驅動程式安裝成功，就會顯示訊息，通知使用者重新啟動其電腦以完成驅動程式的完裝。

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

4. 會顯示一則訊息，指出尚未安裝該模組的用戶端數目。按一下「是」以開始部署。

   注意

   如果您按一下「否」（或如果模組因故無法部署至一或多個用戶端），則當您再按一下「設定 > DLP 設定」或「設定 > 周邊設備存取控管設定」時會顯示相同的訊息。

用戶端會開始從伺服器下載該模組。

5. 檢查該模組是否已部署至用戶端。

   a. 在用戶端樹狀結構中，選取網域。

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

   c. 檢查「資料安全防護狀態」欄。部署狀態可以是下列任一種：

      - 執行中：模組已經部署成功，而且其功能已經啟動。
      - 需要重新啟動：由於使用者尚未重新啟動電腦，因此系統仍未將 Data Loss Prevention 驅動程式安裝完成。如果未安裝驅動程式，Data Loss Prevention 將無法運作。
      - 已停止：模組的服務尚未啟動或目標電腦已正常關機。若要啟動資料安全防護服務，請瀏覽至「用戶端電腦 > 用戶端管理 > 設定 > 其他服務設定」，然後啟動資料安全防護服務。
      - 無法安裝：將模組部署到用戶端時發生問題。您將需要從用戶端樹狀結構重新部署該模組。
      - 無法安裝（Data Loss Prevention 已存在）：Trend Micro Data Loss Prevention 軟體已經存在於端點上。OfficeScan 不會使用「資料安全防護」模組來取代它。
      - 未安裝：該模組尚未部署至用戶端。如果您選擇不要將該模組部署至用戶端，或用戶端的狀態在部署時是離線或行動用戶端，會顯示此狀態。

鑑識資料夾和 DLP 資料庫

發生 Data Loss Prevention 事件後，OfficeScan 會在專用的鑑識資料庫中記錄事件詳細資訊。OfficeScan 還會建立一個加密檔案，檔案中包含觸發事件之敏感資料的副本，同時產生雜湊值，以用於驗證並確保敏感資料的完整性。OfficeScan 會在用戶端電腦上建立加密的鑑識檔案，然後將該檔案上傳至伺服器上的指定位置。

重要

- 加密的鑑識檔案包含高度敏感資料，管理員應謹慎授與這些檔案的存取權。
- OfficeScan 與 Control Manager 整合，以便具有 DLP Incident Reviewer 或 DLP Compliance Officer 角色的 Control Manager 使用者能夠存取加密檔案中的資料。如需有關 DLP 角色以及 Control Manager 中鑑識檔案資料之存取權的詳細資訊，請參閱《Control Manager 管理手冊 6.0 Patch 2》或更新版本。

修改鑑識資料夾和資料庫設定

管理員可以透過修改 OfficeScan 的 INI 檔案，來變更鑑識資料夾的位置和刪除排程，以及用戶端上傳的檔案大小上限。

警告!

如果在記錄 Data Loss Prevention 事件後變更鑑識資料夾的位置，則可能導致資料庫資料與現有鑑識檔案位置之間的連線中斷。趨勢科技建議您在修改鑑識資料夾位置後，手動將任何現有鑑識檔案移轉至新的鑑識資料夾。

下表列出了 OfficeScan 伺服器上<伺服器安裝資料夾>\PCCSRV\Private\ofcserver.ini 檔案中可用的伺服器設定。

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

目標	INI 設定	值
啟動使用者定義的鑑識資料夾位置	[INI_IDLP_SECTION] EnableUserDefinedUploadFolder	0: 關閉（預設） 1: 啟動

目標	INI 設定	值
設定使用者定義的鑑識資料夾位置	[INI_IDLP_SECTION] `UserDefinedUploadFolder` 注意 • 管理員必須啟動 `EnableUserDefinedUploadFolder` 設定後，OfficeScan 才會套用此設定。 • 鑑識資料夾的預設位置為： <伺服器安裝資料夾>`\PCCSRV\Private\DLPForensicData` • 使用者定義的鑑識資料夾位置必須是伺服器電腦上的實體磁碟機（內部或外部）。OfficeScan 不支援對應網路磁碟機位置。	預設值：<請使用客戶定義的資料夾路徑來取代此值。例如：C:\VolumeData\OfficeScanDlpForensicData> 使用者定義的值：必須是伺服器電腦上的磁碟機實體位置
啟動鑑識資料檔案清除	[INI_IDLP_SECTION] `ForensicDataPurgeEnable`	0: 關閉 1: 啟動（預設）
設定鑑識資料檔案清除檢查的時間頻率	[INI_IDLP_SECTION] `ForensicDataPurgeCheckFrequency` 注意 • 管理員必須啟動 `ForensicDataPurgeEnable` 設定後，OfficeScan 才會套用此設定。 • OfficeScan 只會刪除已超過 `ForensicDataExpiredPeriodInDays` 設定中所指定到期日的資料檔案。	1: 每月一次，每月第一天的 00:00 2: 每週一次（預設），每個星期日的 00:00 3: 每日一次，每天 00:00 4: 每小時一次，每小時的 HH:00
設定在伺服器上儲存鑑識資料檔案的時長	[INI_IDLP_SECTION] `ForensicDataExpiredPeriodInDays`	預設值（天）：180 最小值：1 最大值：3650

目標	INI 設定	值
設定鑑識檔案磁碟空間檢查的時間頻率	[INI_SERVER_DISK_THRESHOLD] `MonitorFrequencyInSecond` 注意 如果鑑識資料所在資料夾中的可用磁碟空間小於 `InformUploadOnDiskFreeSpaceInGb` 設定中所設定的值，則 OfficeScan 會在 Web 主控台上記錄事件記錄檔。	預設值（秒）：5
設定鑑識檔案磁碟空間檢查的上傳頻率	[INI_SERVER_DISK_THRESHOLD] `IsapiCheckCountInRequest` 注意 如果鑑識資料所在資料夾中的可用磁碟空間小於 `InformUploadOnDiskFreeSpaceInGb` 設定中所設定的值，則 OfficeScan 會在 Web 主控台上記錄事件記錄檔。	預設值（檔案數目）：200
設定觸發有限磁碟空間通知的磁碟空間最小值	[INI_SERVER_DISK_THRESHOLD] `InformUploadOnDiskFreeSpaceInGb` 注意 如果鑑識資料所在資料夾中的可用磁碟空間小於設定的值，則 OfficeScan 會在 Web 主控台上記錄事件記錄檔。	預設值 (GB)：10

目標	INI 設定	值
設定從用戶端上傳鑑識資料檔案所需的最低可用空間	[INI_SERVER_DISK_THRESHOLD] `RejectUploadOnDiskFreeSpaceInGb` **注意** 如果鑑識資料所在資料夾中的可用磁碟空間小於設定的值，則 OfficeScan 用戶端不會將鑑識資料檔案上傳至伺服器，且 OfficeScan 會在 Web 主控台上記錄事件記錄檔。	預設值 (GB)： 1

下表列出了 OfficeScan 伺服器上<伺服器安裝資料夾>`\PCCSRV\ofcscan.ini` 檔案中可用的 OfficeScan 用戶端設定。

表 3-2. `PCCSRV\ofcscan.ini` 中的鑑識檔案 OfficeScan 用戶端設定

目標	INI 設定	值
啟動將鑑識資料檔案上傳至伺服器	`UploadForensicDataEnable`	0: 關閉 1: 啟動（預設）
設定 OfficeScan 用戶端上傳至伺服器的檔案大小上限	`UploadForensicDataSizeLimitInMb` **注意** OfficeScan 用戶端只會將低於這一上限的檔案傳送至伺服器。	預設值 (MB)：10 最小值：1 最大值： 2048
設定在 OfficeScan 用戶端上儲存鑑識資料檔案的時長	`ForensicDataKeepDays` **注意** OfficeScan 用戶端會在每天上午 11:00 刪除已超過指定到期日的鑑識資料檔案。	預設值（天）：180 最小值：1 最大值： 3650

目標	INI 設定	值
設定 OfficeScan 用戶端檢查伺服器連線情況的頻率	`ForensicDataDelayUploadFrequenceInMinutes` 注意 無法將鑑識檔案上傳至伺服器的 OfficeScan 用戶端，會自動嘗試在指定的時間間隔重新傳送檔案。	預設值（分）：5 最小值：5 最大值： 60

建立鑑識資料的備份

視公司的安全策略而定，儲存鑑識資料資訊所需的時長可能大有不同。趨勢科技建議您手動備份鑑識資料夾中的資料以及鑑識資料庫，以釋放伺服器上的磁碟空間。

程序

1. 瀏覽至伺服器上鑑識資料所在的資料夾位置。
   - 預設位置：<伺服器安裝資料夾>`\PCCSRV\Private\DLPForensicData`
   - 若要尋找自訂的鑑識資料夾位置，請參閱設定使用者定義的鑑識資料夾位置 第 3-10 頁。
2. 將資料夾複製到新位置。
3. 若要手動備份鑑識資料的資料庫，請瀏覽至<伺服器安裝資料夾>`\PCCSRV\Private`。
4. 將 `DLPForensicDataTracker.db` 檔案複製到新位置。

解除安裝資料安全防護

如果從 Plug-In Manager 解除安裝「資料安全防護」模組：

- 系統會從 OfficeScan 伺服器移除所有 Data Loss Prevention 組態、設定和記錄檔。
- 系統會從伺服器移除「資料安全防護」模組所提供的所有「周邊設備存取控管」組態和設定。
- 系統會從用戶端移除「資料安全防護」模組。必須重新啟動用戶端電腦，才能完成移除「資料安全防護」。
- 系統不會再於用戶端上實施 Data Loss Prevention 策略。
- 「周邊設備存取控管」不會再監控對下列裝置的存取：
  - COM 和 LPT 通訊埠
  - IEEE 1394 介面
  - 影像裝置
  - 紅外線裝置
  - 數據機
  - PCMCIA 卡
  - 列印螢幕鍵

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

從 Plug-In Manager 解除安裝「資料安全防護」

程序

1. 開啟 OfficeScan Web 主控台，然後按一下主功能表中的「Plug-in Manager」。

2. 在 Plug-in Manager 畫面上，移至「OfficeScan 資料安全防護」區段，然後按一下「解除安裝」。
3. 監控解除安裝進度。解除安裝期間您可以瀏覽其他畫面。
4. 解除安裝之後，請重新整理 Plug-in Manager 畫面。您可以再次安裝「OfficeScan 資料安全防護」。

部分 II

保護用戶端電腦

第 4 章

使用趨勢科技主動式雲端截毒技術

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

本章內容：

關於趨勢科技主動式雲端截毒技術

趨勢科技™主動式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。此解決方案同時提供本機並裝載解決方案，不論使用者是位於網路上、在家中或路上都可提供保護，方法是使用輕量型用戶端來存取電子郵件、網頁和檔案信譽評等技術以及安全威脅資料庫的獨一無二雲端相互關聯性。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。

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

新解決方案的必要性

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

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

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

雲端防護服務

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

主動式雲端截毒技術服務包括：

- 檔案信譽評等服務：「檔案信譽評等服務」會將先前儲存在用戶端電腦上的大量惡意程式防護簽章改由主動式雲端截毒技術伺服器來源處理。如需詳細資訊，請參閱檔案信譽評等服務 第 4-3 頁。
- 網頁信譽評等服務：「網頁信譽評等服務」讓本機主動式雲端截毒技術伺服器來源可以控管先前只由趨勢科技獨力控管的 URL 信譽評等資料。這兩項技術可確保在更新病毒碼或檢查 URL 的有效性時耗用較少的頻寬。如需詳細資訊，請參閱網頁信譽評等服務 第 4-3 頁。
- Smart Feedback：趨勢科技還會繼續收集從世界各地的趨勢科技產品匿名傳送的資訊，以便主動判斷每個新的安全威脅。如需詳細資訊，請參閱Smart Feedback 第 4-4 頁。

檔案信譽評等服務

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

用戶端必須處於雲端截毒掃瞄模式時才能使用檔案信譽評等服務。在本文件中，這些用戶端稱為雲端掃瞄用戶端。用戶端不在雲端截毒掃瞄模式下時，就不會使用檔案信譽評等服務，這些用戶端稱為標準用戶端。OfficeScan 管理員可以將全部或多個用戶端設定為使用雲端截毒掃瞄模式。

網頁信譽評等服務

透過全世界其中一個最大的網域信譽評等資料庫，趨勢科技網頁信譽評等技術會依據諸如網站的存在時間長短、位置變更記錄，以及透過惡意程式行為分析

所發現的可疑活動指標等因素來指定信譽評等，以追蹤 Web 網域的可信度。網頁信譽評等會繼續掃瞄網站，並阻擋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，以及專門在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 OfficeScan 用戶端會使用「網頁信譽評等服務」。OfficeScan 管理員可以使全部或數個用戶端受網頁信譽評等策略的約束。

Smart Feedback

Trend Micro 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 Checksum
- 已存取的網站
- 檔案資訊，包括大小與路徑
- 可執行檔案的名稱

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，您的電腦也會受到保護。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。

如需有關主動式雲端截毒技術的詳細資訊，請造訪：

http://www.trendmicro.com.tw/spn/index.asp

主動式雲端截毒伺服器來源

趨勢科技會提供「檔案信譽評等服務」和「網頁信譽評等服務」給 OfficeScan 和主動式雲端截毒技術伺服器來源。

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

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

用戶端所連線的主動式雲端截毒伺服器來源取決於用戶端位置。用戶端可以連線到趨勢科技主動式雲端截毒技術或主動式雲端截毒技術伺服器。

趨勢科技™主動式雲端截毒技術™

趨勢科技™主動式雲端截毒技術™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。主動式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。

如需有關主動式雲端截毒技術的詳細資訊，請造訪：

www.trendmicro.com.tw/spn/index.asp

主動式雲端截毒技術伺服器

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

主動式雲端截毒技術伺服器的類型有兩種：

- 整合式主動式雲端截毒技術伺服器：OfficeScan 安裝程式中包含與 OfficeScan 伺服器安裝在同一部電腦上的整合式主動式雲端截毒技術伺服器。安裝之後，可透過 OfficeScan Web 主控台管理此伺服器的設定。整合式伺服器用於 OfficeScan 的小規模部署，其中，用戶端的數量不會超過 3,000。如果是較大的部署，則需要獨立式主動式雲端截毒技術伺服器。
- 獨立式主動式雲端截毒技術伺服器：獨立式主動式雲端截毒技術伺服器安裝於 VMware 或 Hyper-V 伺服器上。獨立式伺服器具有個別的管理主控台，不受 OfficeScan Web 主控台管理。

主動式雲端截毒技術伺服器來源比較

下表重點說明主動式雲端截毒技術與主動式雲端截毒技術伺服器之間的差別。

表 4-1. 主動式雲端截毒技術伺服器來源比較

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

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

雲端防護病毒碼檔案

雲端防護病毒碼檔案用於檔案信譽評等服務和網頁信譽評等服務。趨勢科技會過趨勢科技主動式更新伺服器發佈這些病毒碼檔案。

本機雲端病毒碼

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

注意

雲端掃瞄用戶端是管理員已將其設定為使用檔案信譽評等服務的 OfficeScan 用戶端。不使用檔案信譽評等服務的用戶端稱為標準用戶端。

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

雲端病毒碼

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

網頁封鎖清單

網頁封鎖清單是由主動式雲端截毒技術伺服器來源下載。受網頁信譽評等服務策略限制的 OfficeScan 用戶端不會下載網頁封鎖清單。

注意

管理員可以使全部或數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式雲端截毒伺服器來源，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式雲端截毒技術伺服器來源的信譽資料與電腦上執行的網頁信譽評等策略關聯。根據該策略，用戶端將允許或封鎖對網站的存取。

主動式雲端截毒技術病毒碼更新程序

源自趨勢科技主動式更新伺服器的雲端防護病毒碼。

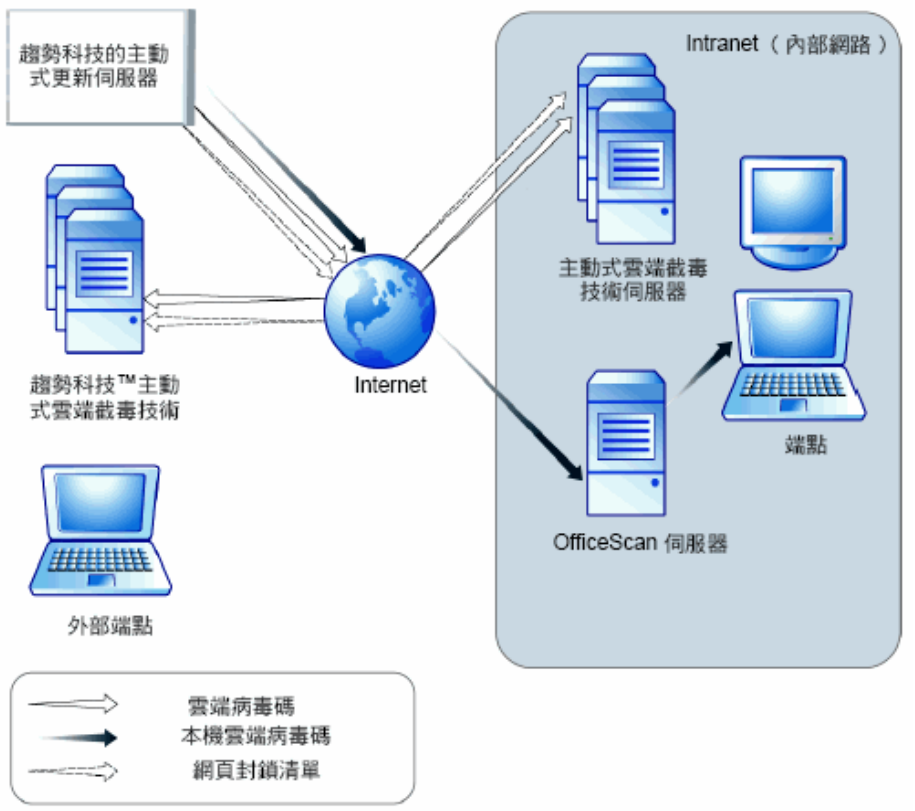


圖 4-1. 病毒碼更新程序

主動式雲端截毒技術病毒碼的使用

OfficeScan 用戶端會使用本機雲端病毒碼掃瞄安全威脅，且僅當該本機雲端病毒碼無法確定檔案的風險才會查詢雲端病毒碼。在使用者嘗試存取網站時，用

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

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

秘訣

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

目前不在內部網路的用戶端則可以連線到趨勢科技主動式雲端截毒技術來查詢。要連線到主動式雲端截毒技術，必須提供 Internet 連線。

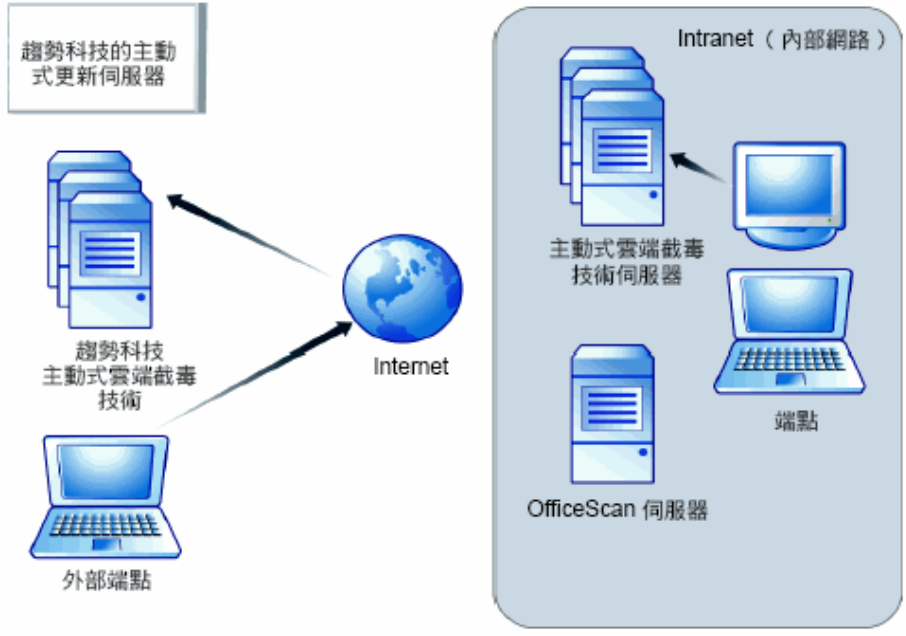


圖 4-2. 查詢程序

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

下表摘要了根據用戶端位置的防護範圍。

表 4-2. 根據位置的防護行為

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

設定主動式雲端截毒技術服務

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

- 主動式雲端截毒技術伺服器安裝 第 4-12 頁
- 整合式主動式雲端截毒技術伺服器管理 第 4-17 頁

- 主動式雲端截毒技術來源清單 第 4-21 頁
- 用戶端連線 Proxy 伺服器設定 第 4-28 頁
- 趨勢科技網路病毒牆安裝 第 4-28 頁

主動式雲端截毒技術伺服器安裝

如果用戶端數目不會超過 1,000 部，您可以安裝整合式或獨立式主動式雲端截毒技術伺服器。如果用戶端數超過 1,000，則安裝獨立式主動式雲端截毒技術伺服器。

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

由於整合式伺服器與 OfficeScan 伺服器在同一部電腦上執行，因此在這兩部伺服器的尖峰流量期間內，電腦的效能可能會大幅降低。請考慮使用獨立式主動式雲端截毒技術伺服器做為用戶端的主要主動式雲端截毒伺服器來源，並使用整合式伺服器做為備用。

獨立式主動式雲端截毒技術伺服器安裝

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

整合式主動式雲端截毒技術伺服器安裝

如果在 OfficeScan 伺服器安裝期間安裝了整合式伺服器：

- 啟動整合式伺服器並設定該伺服器的設定。如需詳細資訊，請參閱整合式主動式雲端截毒技術伺服器管理 第 4-17 頁。
- 如果整合式伺服器和 OfficeScan 用戶端位於同一台伺服器電腦上，請考慮關閉 OfficeScan 防火牆。OfficeScan 防火牆是設計給用戶端電腦使用，在伺服器電腦上啟動它可能會影響效能。如需關閉防火牆的指示，請參閱啟動或關閉 OfficeScan 防火牆 第 12-5 頁。

注意

請考量關閉防火牆的影響，並確定這樣做符合您的安全計劃。

秘訣

在使用 整合式主動式雲端截毒技術伺服器工具 第 4-13 頁 完成 OfficeScan 安裝後，再安裝整合式主動式雲端截毒技術伺服器。

整合式主動式雲端截毒技術伺服器工具

趨勢科技 OfficeScan 整合式主動式雲端截毒技術工具可協助管理員在 OfficeScan 伺服器安裝完成後，安裝或解除安裝整合式主動式雲端截毒技術伺服器。目前的 OfficeScan 版本不允許管理員在 OfficeScan 伺服器安裝完成後再安裝/移除整合式主動式雲端截毒技術伺服器。這項工具加強了舊版 OfficeScan 的安裝功能彈性。

在安裝整合式主動式雲端截毒技術伺服器之前，請匯入以下項目至您已升級的 OfficeScan 10.6 SP2 伺服器：

- 網域結構
- 以下根和網域層級設定：
  - 所有掃瞄類型的掃瞄設定 (手動、即時、預約、立即掃瞄)
  - 網頁信譽評等服務組態設定
  - 核可的 URL 清單
  - 行為監控設定
  - 周邊設備存取控管設定
  - Data Loss Prevention 設定
  - 權限和其他設定
  - 其他服務設定
  - 間諜程式/可能的資安威脅程式核可清單
- 全域用戶端設定

- 電腦位置
- 防火牆策略和資料檔
- 主動式雲端截毒伺服器來源
- 伺服器更新預約時程
- 用戶端更新來源和預約時程
- 通知
- Proxy 伺服器設定

程序

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

   表 4-3. 安裝程式選項

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

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

表 4-4. 整合式主動式雲端截毒技術伺服器的信譽評等服務之通訊埠

Web 伺服器和設定	檔案信譽評等服務的通訊埠		網頁信譽評等服務的 HTTP 通訊埠
	HTTP	HTTPS (SSL)	
Apache web server（已啟動 SSL）	8080	4343（不可設定）	8080（不可設定）
Apache web server（已關閉 SSL）	8080	4345（不可設定）	8080（不可設定）
IIS 預設網站（已啟動 SSL）	80	443（不可設定）	80（不可設定）
IIS 預設網站（已關閉 SSL）	80	443（不可設定）	80（不可設定）
IIS 虛擬網站（已啟動 SSL）	8082	4345（可設定）	5274（可設定）
IIS 虛擬網站（已關閉 SSL）	8082	4345（可設定）	5274（可設定）

3. 安裝完成後，請開啟 OfficeScan Web 主控台並驗證以下項目：

- 開啟 Microsoft 管理主控台（請在「開始」功能表輸入 `services.msc`）並確認 Trend Micro Local Web Classification Server 和趨勢科技雲端截毒掃瞄伺服器已列為「已啟動」狀態。
- 開啟「Windows 工作管理員」。在程序標籤中，確認 `iCRCService.exe` 和 `LWCSService.exe` 正在執行，
- 在 OfficeScan Web 主控台，確認功能表項目主動式雲端截毒技術 > 整合式伺服器已顯示。

主動式雲端截毒技術伺服器最佳做法

透過執行以下操作來最佳化主動式雲端截毒技術伺服器的效能：

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

為獨立式伺服器自訂 ptngrowth.ini

程序

1. 開啟 `/var/tmcss/conf/` 中的 `ptngrowth.ini` 檔案。
2. 使用以下的建議值，修改 `ptngrowth.ini` 檔案：
   - `[COOLDOWN]`
   - `ENABLE=1`
   - `MAX_UPDATE_CONNECTION=1`
   - `UPDATE_WAIT_SECOND=360`
3. 儲存 `ptngrowth.ini` 檔案。
4. 透過在命令列介面 (CLI) 中輸入以下命令，重新啟動 `lighttpd` 服務：

- `service lighttpd restart`

為整合式伺服器自訂 ptngrowth.ini

程序

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

整合式主動式雲端截毒技術伺服器管理

透過執行以下工作來管理整合式主動式雲端截毒技術伺服器：

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

啟動整合式伺服器的檔案信譽評等服務和網頁信譽評等服務

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

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

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

記錄整合式伺服器的位址

為內部用戶端設定主動式雲端截毒技術來源清單時，將需要整合式伺服器的位址。如需有關此清單的詳細資訊，請參閱主動式雲端截毒技術來源清單 第 4-21 頁。

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

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

秘訣

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

更新整合式伺服器的元件

整合式伺服器會更新以下元件：

- 雲端病毒碼：用戶端會將掃瞄查詢傳送至整合式伺服器，並與雲端病毒碼比對來確認潛在的安全威脅。

- 網頁封鎖清單：受網頁信譽評等服務策略約束的用戶端會傳送網頁信譽評等查詢至整合式伺服器，並比對網頁封鎖清單來確認網站的信譽。

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

注意

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

整合式伺服器的核可/封鎖 URL 清單設定

用戶端會維護自己的核可/封鎖的 URL 清單。請在設定網頁信譽評等服務策略時設定用戶端的清單（如需詳細資訊，請參閱網頁信譽評等策略 第 11-3 頁）。系統會自動允許或封鎖用戶端的清單中的任何 URL。

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

注意

封鎖的 URL 清單具有的優先順序高於網頁封鎖清單。

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

設定整合式主動式雲端截毒技術伺服器設定

程序

1. 瀏覽至「主動式雲端截毒技術 > 整合式伺服器」。
2. 選取「啟動檔案信譽評等服務」。

3. 選取用戶端傳送掃瞄查詢至整合式伺服器時將使用的通訊協定（HTTP 或 HTTPS）。

4. 選取「啟動網頁信譽評等服務」。

5. 記錄在「伺服器位址」欄下找到的整合式伺服器的位址。

6. 如果要更新整合式伺服器的元件：

   - 檢視雲端病毒碼和網頁封鎖清單的目前版本。如果有更新可用，請按一下「立即更新」。更新結果會顯示在畫面頂端。
   - 如果要自動更新病毒碼：

     a. 選取「啟動預約更新」。

     b. 選擇要每小時更新一次還是每 15 分鐘更新一次。

     c. 選取「檔案信譽評等服務」下的更新來源。將從此來源更新雲端病毒碼。

     d. 選取「網頁信譽評等服務」下的更新來源。將從此來源更新網頁封鎖清單。

注意

- 如果選擇主動式更新伺服器作為更新來源，請確定伺服器有 Internet 連線；如果使用 Proxy 伺服器，請測試是否可以使用 Proxy 伺服器設定建立 Internet 連線。如需詳細資訊，請參閱用於 OfficeScan 伺服器更新的 Proxy 第 6-16 頁。
- 如果選擇自訂更新來源，請為此更新來源設定適當的環境和更新資源。此外，請確定伺服器電腦與此更新來源之間的連線正常。如果需要設定更新來源的協助，請聯絡您的經銷商。

---

7. 如果要設定整合式伺服器的核可/封鎖清單：

   a. 按一下「匯入」使用預先格式化的 .csv 檔案中的 URL 填入該清單。您可以從獨立式主動式雲端截毒技術伺服器中取得 `.csv` 檔案。

   b. 如果具有現成清單，請按一下「匯出」將該清單儲存為 `.csv` 檔案。

8. 按一下「儲存」。

主動式雲端截毒技術來源清單

用戶端在掃瞄安全威脅並判定網站的信譽時，會傳送查詢至主動式雲端截毒技術來源。

主動式雲端截毒技術伺服器來源的 IPv6 支援

純 IPv6 用戶端無法將查詢直接傳送到純 IPv4 來源，例如：

- 主動式雲端截毒技術伺服器 2.0（整合式或獨立式）

  注意

  主動式雲端截毒技術伺服器自 2.5 版開始會支援 IPv6。

- 趨勢科技主動式雲端截毒技術

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

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

主動式雲端截毒技術伺服器來源和電腦位置

用戶端連線到哪個主動式雲端截毒技術來源取決於用戶端電腦所處的位置。

如需設定位置設定的詳細資訊，請參閱電腦位置 第 14-2 頁。

表 4-5. 主動式雲端截毒技術來源（依位置）

位置	主動式雲端截毒伺服器來源
外部	外部用戶端會將掃瞄和網頁信譽評等查詢傳送至趨勢科技主動式雲端截毒技術。

位置	主動式雲端截毒伺服器來源
內部	內部用戶端會將掃瞄和網頁信譽評等查詢傳送至主動式雲端截毒技術伺服器或趨勢科技主動式雲端截毒技術。 如果您已安裝主動式雲端截毒技術伺服器，請在 OfficeScan Web 主控台上設定主動式雲端截毒伺服器來源清單。內部用戶端在需要查詢時，會從此清單中挑選伺服器。如果用戶端無法連線到第一部伺服器，則會挑選清單上的另一部伺服器。 秘訣 請將獨立式主動式雲端截毒技術伺服器指定為主要掃瞄來源，而將整合式伺服器指定為備用來源。如此可降低導向至控管 OfficeScan 伺服器與整合式伺服器之電腦的流量。獨立式伺服器也可以處理更多查詢。 您可以設定主動式雲端截毒技術伺服器來源的標準清單或自訂清單。標準清單適用於所有內部用戶端。自訂清單定義 IP 位址範圍。如果內部用戶端的 IP 位址在範圍之內，用戶端即會使用自訂清單。

設定主動式雲端截毒技術來源標準清單

程序

1. 瀏覽至「主動式雲端截毒技術 > 主動式雲端截毒技術伺服器來源」。
2. 按一下「內部用戶端」標籤。
3. 選取「使用標準清單（清單將由所有內部用戶端使用）」。
4. 按一下「標準清單」連結。

   接著會開啟一個新畫面。
5. 按一下「新增」。

   接著會開啟一個新畫面。
6. 指定主動式雲端截毒技術伺服器的主機名稱或 IPv4/IPv6 位址。如果指定的是 IPv6 位址，則使用括號將該位址括起來。

注意

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

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

   a. 如果希望用戶端使用 HTTP，請輸入伺服器的 HTTP 要求監聽通訊埠。如果希望用戶端使用 HTTPS，請選取 SSL 並輸入伺服器的 HTTPS 要求監聽通訊埠。

   b. 按一下「測試連線」，以檢查是否可以建立到伺服器的連線。

秘訣

監聽通訊埠構成伺服器位址的一部分。取得伺服器位址：

若使用整合式伺服器，請開啟 OfficeScan Web 主控台並前往 主動式雲端截毒技術 > 整合式伺服器。

若使用獨立式伺服器，請開啟獨立式伺服器主控台並前往「摘要」畫面。

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

   a. 輸入伺服器的 HTTP 要求的監聽通訊埠。

   b. 按一下「測試連線」，以檢查是否可以建立到伺服器的連線。

9. 按一下「儲存」。

   畫面隨即關閉。

10. 透過重複以上步驟來新增更多伺服器。

11. 在畫面頂端，選取「順序」或「隨機」。

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

- 隨機：用戶端隨機挑選伺服器。

秘訣

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

12. 在畫面中執行其他工作。

- 如果您已從其他伺服器匯出清單，而想要將此清單匯入此畫面，請按一下「匯入」，然後尋找 .dat 檔案。此清單會載入至畫面上。
- 如果要將清單匯出為 .dat 檔案，請按一下「匯出」，再按一下「儲存」。
- 如果要重新整理伺服器的服務狀態，請按一下「重新整理」。
- 按一下伺服器名稱以執行下列其中一項作業：
  - 檢視或編輯伺服器資訊。
  - 檢視網頁信譽評等服務或檔案信譽評等服務的完整伺服器位址。
- 如果要開啟主動式主動式雲端截毒技術伺服器的主控台，請按一下「啟動主控台」。
  - 若為整合式主動式雲端截毒技術伺服器，將會顯示伺服器的組態設定畫面。
  - 若為獨立式主動式雲端截毒技術伺服器與其他 OfficeScan 伺服器的整合式主動式雲端截毒技術伺服器，則會顯示主控台登入畫面。
- 如果要刪除某個項目，請選取該伺服器的核取方塊，然後按一下「刪除」。

13. 按一下「儲存」。

畫面隨即關閉。

14. 按一下「通知所有用戶端」。

設定主動式雲端截毒技術來源自訂清單

程序

1. 瀏覽至「主動式雲端截毒技術 > 主動式雲端截毒技術伺服器來源」。
2. 按一下「內部用戶端」標籤。
3. 選取「使用以用戶端 IP 位址為基礎的自訂清單」。
4. （選用）選取「如果自訂清單中的所有伺服器均無法使用，則使用標準清單」。
5. 按一下「新增」。

   接著會開啟一個新畫面。
6. 在「IP 範圍」區段中，指定 IPv4 或 IPv6 位址範圍，或兩者都指定。

   注意

   使用 IPv4 位址的用戶端可以連接純 IPv4 或雙堆疊主動式雲端截毒技術伺服器。使用 IPv6 位址的用戶端可以連接純 IPv6 或雙堆疊主動式雲端截毒技術伺服器。同時使用 IPv4 和 IPv6 位址的用戶端可以連接任何主動式雲端截毒技術伺服器。
7. 在「Proxy 伺服器設定」區段中，指定將用於連線到主動式雲端截毒技術伺服器的 Proxy 伺服器設定用戶端。
   a. 選取「使用 Proxy 伺服器進行用戶端與主動式雲端截毒技術伺服器通訊」。
   b. 指定 Proxy 伺服器名稱或 IPv4/IPv6 位址，以及通訊埠號碼。
   c. 如果 Proxy 伺服器需要驗證，請輸入使用者名稱和密碼，然後確認密碼。
8. 在「自訂主動式雲端截毒技術伺服器清單」中，新增主動式雲端截毒技術伺服器。

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

注意

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

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

   i. 如果希望用戶端使用 HTTP，請輸入伺服器的 HTTP 要求監聽通訊埠。如果希望用戶端使用 HTTPS，請選取 SSL 並輸入伺服器的 HTTPS 要求監聽通訊埠。

   ii. 按一下「測試連線」，以檢查是否可以建立到伺服器的連線。

秘訣

監聽通訊埠構成伺服器位址的一部分。取得伺服器位址：

若使用整合式伺服器，請開啟 OfficeScan Web 主控台並前往 主動式雲端截毒技術 > 整合式伺服器。

若使用獨立式伺服器，請開啟獨立式伺服器主控台並前往「摘要」畫面。

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

   i. 輸入伺服器的 HTTP 要求的監聽通訊埠。

   ii. 按一下「測試連線」，以檢查是否可以建立到伺服器的連線。

d. 按一下「新增到清單」。

e. 透過重複以上步驟來新增更多伺服器。

f. 選取「順序」或「隨機」。

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

秘訣

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

g. 在畫面中執行其他工作。

- 如果要重新整理伺服器的服務狀態，請按一下「重新整理」。
- 如果要開啟主動式主動式雲端截毒技術伺服器的主控台，請按一下「啟動主控台」。
  - 若為整合式主動式雲端截毒技術伺服器，將會顯示伺服器的組態設定畫面。
  - 若為獨立式主動式雲端截毒技術伺服器與其他 OfficeScan 伺服器的整合式主動式雲端截毒技術伺服器，則會顯示主控台登入畫面。
- 如要刪除項目，請按一下「刪除」（ 

）。

9. 按一下「儲存」。

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

10. 重複步驟 4 到步驟 8，可新增更多自訂清單。

11. 在畫面中執行其他工作。

- 如果要修改清單，請按一下 IP 範圍連結，然後在開啟的畫面中修改設定。

- 如果要將清單匯出為 .dat 檔案，請按一下「匯出」，再按一下「儲存」。
- 如果您已從其他伺服器匯出清單，而想要將此清單匯入此畫面，請按一下「匯入」，然後尋找 .dat 檔案。此清單會載入至畫面上。

12. 按一下「通知所有用戶端」。

用戶端連線 Proxy 伺服器設定

如果在連線至主動式雲端截毒技術時必須進行 Proxy 伺服器驗證，請指定驗證憑證。如需詳細資訊，請參閱 OfficeScan 用戶端的外部 Proxy 伺服器 第 14-43 頁。

設定用戶端在連線至主動式雲端截毒技術伺服器時將會使用的內部 Proxy 伺服器設定。如需詳細資訊，請參閱 OfficeScan 用戶端的內部 Proxy 伺服器 第 14-42 頁。

電腦位置設定

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

如果要設定位置設定，請參閱電腦位置 第 14-2 頁。

趨勢科技網路病毒牆安裝

如果您已安裝趨勢科技™網路病毒牆™：

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

使用主動式雲端截毒技術服務

正確設定主動式雲端截毒技術環境後，用戶端就可以使用「檔案信譽評等服務」和「網頁信譽評等服務」。您還可以設定 Smart Feedback 設定。

注意

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

如果要獲得「檔案信譽評等服務」提供的防護，用戶端必須使用稱為雲端截毒掃瞄的掃瞄方法。如需雲端截毒掃瞄以及如何在用戶端上啟動雲端截毒掃瞄的詳細資訊，請參閱掃瞄方法 第 7-6 頁。

如果要允許 OfficeScan 用戶端使用「網頁信譽評等服務」，請設定網頁信譽評等策略。如需詳細資訊，請參閱網頁信譽評等策略 第 11-3 頁。

注意

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

如需設定 Smart Feedback 的相關指示，請參閱 Smart Feedback 第 13-44 頁。

第 5 章

安裝 OfficeScan 用戶端

本章說明趨勢科技™OfficeScan™ 系統需求和 OfficeScan 用戶端安裝程序。

如需有關升級 OfficeScan 用戶端的詳細資訊，請參閱*《OfficeScan 安裝和升級手冊》*。

本章內容：

OfficeScan 用戶端全新安裝

OfficeScan 用戶端可安裝在執行 Microsoft Windows 平台的電腦上。OfficeScan 也與各種協力廠商產品相容。

請造訪下列網站，以取得系統需求和相容協力廠商產品的完整清單：

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

安裝考量

安裝用戶端之前，請先考量下列事項：

- OfficeScan 用戶端功能：某些用戶端功能在特定 Windows 平台上無法使用。
- IPv6 支援：您可以將 OfficeScan 用戶端安裝在雙堆疊或純 IPv6 用戶端上。然而：
  - 某些可安裝 OfficeScan 用戶端的 Windows 作業系統不支援 IPv6 定址。
  - 對於某些安裝方法，需符合特殊需求才能成功地安裝 OfficeScan 用戶端。
- OfficeScan 用戶端 IP 位址：對於具有 IPv4 和 IPv6 位址的用戶端，您可以選擇當用戶端向伺服器註冊時要使用的 IP 位址。
- 例外清單：確認已正確設定下列功能的例外清單：
  - 行為監控：將重要的電腦應用程式新增到「核可的程式」清單，以防止 OfficeScan 用戶端被禁止使用這些應用程式。如需詳細資訊，請參閱行為監控例外清單 第 8-5 頁。
  - 網頁信譽評等：將您認為安全的網站新增到「核可的 URL」清單，以防止 OfficeScan 用戶端被禁止存取這些網站。如需詳細資訊，請參閱網頁信譽評等策略 第 11-3 頁。

OfficeScan 用戶端功能

電腦上可用的 OfficeScan 用戶端功能取決於電腦的作業系統。

表 5-1. 伺服器平台上的 OfficeScan 用戶端功能

功能	Windows 作業系統		
	Server 2003	Server 2008/ Server Core 2008	Server 2012/ Server Core 2012
手動掃瞄、即時掃瞄和預約掃瞄	是	是	是
元件更新（手動和預約更新）	是	是	是
更新代理程式	是	是	是
網頁信譽評等	是，但在安裝伺服器期間預設是關閉的	是，但在安裝伺服器期間預設是關閉的	是，但在安裝伺服器期間預設是關閉的，且僅部分支援 Windows UI 模式
損害清除及復原服務	是	是	是
OfficeScan 防火牆	是，但在安裝伺服器期間預設是關閉的	是，但在安裝伺服器期間預設是關閉的	是，但在安裝伺服器期間預設是關閉的，且不支援應用程式過濾
行為監控	是（32 位元），但預設是關閉的	是（32 位元），但預設是關閉的	是（64 位元），但預設是關閉的
	否（64 位元）	是（64 位元），但預設是關閉的	
下列項目的本機自我保護： • 登錄機碼 • 程序	是（32 位元），但預設是關閉的	是（32 位元），但預設是關閉的	是（64 位元），但預設是關閉的
	否（64 位元）	是（64 位元），但預設是關閉的	

功能	Windows 作業系統		
	Server 2003	Server 2008/ Server Core 2008	Server 2012/ Server Core 2012
下列項目的本機自我保護： • 服務 • 檔案保護	是	是	是
周邊設備存取控管 （未經授權的變更阻止服務）	是（32 位元），但預設是關閉的	是（32 位元），但預設是關閉的	是（64 位元），但預設是關閉的
	否（64 位元）	是（64 位元），但預設是關閉的	
資料安全防護 (包含「周邊設備存取控管」的「資料安全防護」)	是（32 位元），但預設是關閉的	是（32 位元），但預設是關閉的	是（64 位元），但預設是關閉的
	是（64 位元），但預設是關閉的	是（64 位元），但預設是關閉的	
Microsoft Outlook 郵件掃瞄	是（32 位元）	否	否
	否（64 位元）		
POP3 郵件掃瞄	是	是	是
支援 Cisco NAC	否	否	否
Client Plug-in Manager	是	是	是
行動模式	是	是 (Server) 否 (Server Core)	是
SecureClient 支援模組	是（32 位元）	否	否
	否（64 位元）		
Smart Feedback	是	是	是

表 5-2. 桌上型電腦平台上的 OfficeScan 用戶端功能

功能	Windows 作業系統			
	XP	Vista	Windows 7	Windows 8
手動掃瞄、即時掃瞄和預約掃瞄	是	是	是	是
元件更新（手動和預約更新）	是	是	是	是
更新代理程式	是	是	是	是
網頁信譽評等	是	是	是	是，但僅部分支援 Windows UI 模式
損害清除及復原服務	是	是	是	是
OfficeScan 防火牆	是	是	是	是，但不支援應用程式過濾
行為監控	是（32 位元）	是（32 位元）	是（32 位元）	是（32 位元）
	否（64 位元）	是（64 位元） 64 位元 Vista 支援需要 SP1 或 SP2	是（64 位元）	是（64 位元）
下列項目的本機自我保護： • 登錄機碼 • 程序	是（32 位元）	是（32 位元）	是（32 位元）	是（32 位元）
	否（64 位元）	是（64 位元） 64 位元 Vista 支援需要 SP1 或 SP2	是（64 位元）	是（64 位元）

功能	Windows 作業系統			
	XP	Vista	Windows 7	Windows 8
下列項目的本機自我保護： • 服務 • 檔案保護	是	是	是	是
周邊設備存取控管 （未經授權的變更阻止服務）	是（32 位元）	是（32 位元）	是（32 位元）	是（32 位元）
	否（64 位元）	是（64 位元） 64 位元 Vista 支援需要 SP1 或 SP2	是（64 位元）	是（64 位元）
資料安全防護 (包含「周邊設備存取控管」的「資料安全防護」)	是（32 位元）	是（32 位元）	是（32 位元）	是（32 位元），以桌面模式執行
	是（64 位元）	是（64 位元）	是（64 位元）	是（64 位元），以桌面模式執行
Microsoft Outlook 郵件掃瞄	是（32 位元）	否	否	否
	否（64 位元）			
POP3 郵件掃瞄	是	是	是	是
支援 Cisco NAC	是	否	否	否
Client Plug-in Manager	是	是	是	是
行動模式	是	是	是	是

功能	Windows 作業系統			
	XP	Vista	Windows 7	Windows 8
SecureClient 支援模組	是（32 位元）	否	否	否
	否（64 位元）			
Smart Feedback	是	是	是	是

OfficeScan 用戶端安裝和 IPv6 支援

此主題討論將 OfficeScan 用戶端安裝到雙堆疊或純 IPv6 用戶端時應考量的事項。

作業系統

OfficeScan 用戶端只能安裝在支援 IPv6 定址的下列作業系統上：

- Windows Vista™（所有版本）
- Windows Server 2008（所有版本）
- Windows 7（所有版本）
- Windows Server 2012（所有版本）
- Windows 8（所有版本）

請造訪下列網站，以取得系統需求的完整清單：

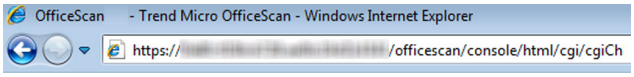
http://docs.trendmicro.com/zh-tw/enterprise/officescan.aspx

安裝方法

要將 OfficeScan 用戶端安裝在純 IPv6 或雙堆疊用戶端時，可以使用所有 OfficeScan 用戶端安裝方法。對於某些安裝方法，需符合特殊需求才能成功地安裝 OfficeScan 用戶端。

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

表 5-3. 安裝方法和 IPv6 支援

安裝方法	需求/考量
Web 安裝網頁和 Browser-based 安裝	安裝頁面的 URL 包含 OfficeScan 伺服器的主機名稱或其 IP 位址。  如果您要安裝到純 IPv6 用戶端，伺服器必須是雙堆疊或純 IPv6 用戶端，而且其主機名稱或 IPv6 位址必須是 URL 的一部分。 對於雙堆疊用戶端，安裝狀態畫面中顯示的 IPv6 位址取決於您在「偏好的 IP 位址」內的用戶端電腦 > 全域用戶端設定區段中選取的選項。
用戶端封裝程式	執行封裝程式工具時，您必須選擇是否要將「更新代理程式」權限指定給用戶端。請記住，純 IPv6 更新代理程式只能將更新檔分發到純 IPv6 或雙堆疊用戶端。
安全性符合、Vulnerability Scanner 和遠端安裝	純 IPv6 伺服器無法在純 IPv4 端點上安裝 OfficeScan 用戶端。同樣地，純 IPv4 伺服器也無法在純 IPv6 端點上安裝 OfficeScan 用戶端。

用戶端 IP 位址

安裝在支援 IPv6 定址的環境中的 OfficeScan 伺服器可以管理下列 OfficeScan 用戶端：

- 安裝在純 IPv6 主機上的 OfficeScan 伺服器可以管理純 IPv6 用戶端。

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

安裝或升級用戶端之後，用戶端會使用 IP 位址向伺服器註冊。

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

設定雙堆疊用戶端向伺服器註冊時使用的 IP 位址

只有雙堆疊 OfficeScan 伺服器可使用此設定，而且此設定只會由雙堆疊用戶端套用。

程序

1. 瀏覽至「用戶端電腦 > 全域用戶端設定」。
2. 移至「偏好的 IP 位址」區段。
3. 請從下列選項選擇：
   - 僅 IPv4：用戶端使用其 IPv4 位址。
   - 先 IPv4 再 IPv6：用戶端先使用其 IPv4 位址。如果用戶端無法使用其 IPv4 位址來註冊，它會使用其 IPv6 位址。如果無法使用這兩種位址來註冊，用戶端會使用此選項的 IP 位址優先順序來重試。
   - 先 IPv6 再 IPv4：用戶端先使用其 IPv6 位址。如果用戶端無法使用其 IPv6 位址來註冊，它會使用其 IPv4 位址。如果無法使用這兩種位址來註冊，用戶端會使用此選項的 IP 位址優先順序來重試。
4. 按一下「儲存」。

部署考量

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

如果您要安裝用戶端且要啟動 IPv6 支援，請閱讀 OfficeScan 用戶端安裝和 IPv6 支援 第 5-7 頁中的指導方針。

表 5-4. 安裝的部署考量

安裝方法/作業系統支援	部署考量					
	WAN 部署	集中管理	需要使用者的操作	需要 IT 資源	大規模部署	耗用頻寬
Web 安裝網頁 所有作業系統都支援（Windows Server Core 2008 和以 Windows UI 模式運作的 Windows 8/ Server 2012/Server Core 2012 除外）	否	否	是	否	否	高
從「開始 Browser-based 安裝」頁面 支援所有作業系統 注意 以 Windows UI 模式運作的 Windows 8 或 Windows Server 2012 不支援。	否	否	是	是	否	高（如果同時啟動多個安裝）

安裝方法/作業系統支援	部署考量					
	WAN 部署	集中管理	需要使用者的操作	需要 IT 資源	大規模部署	耗用頻寬
UNC-based 安裝 支援所有作業系統	否	否	是	是	否	高（如果同時啟動多個安裝）
從「遠端安裝」頁面 支援除下列作業系統之外的所有作業系統： • Windows Vista Home Basic 和 Home Premium Edition • Windows XP Home Edition • Windows 7 Home Basic/ Home Premium • Windows 8（Basic 版本）	否	是	否	是	否	高
Login Script Setup 支援所有作業系統	否	否	是	是	否	高（如果同時啟動多個安裝）
用戶端封裝程式 支援所有作業系統	否	否	是	是	否	低（如果已經排定）
用戶端封裝程式（透過 Microsoft SMS 部署的 MSI 套件） 支援所有作業系統	是	是	是/否	是	是	低（如果已經排定）

安裝方法/作業系統支援	部署考量					
	WAN 部署	集中管理	需要使用者的操作	需要 IT 資源	大規模部署	耗用頻寬
Client Packager（透過 Active Directory 部署 MSI 套件） 支援所有作業系統	是	是	是/否	是	是	高（如果同時啟動多個安裝）
用戶端磁碟映像 支援所有作業系統	否	否	否	是	否	低
Trend Micro Vulnerability Scanner (TMVS) 支援除下列作業系統之外的所有作業系統： • Windows Vista Home Basic 和 Home Premium Edition • Windows XP Home Edition • Windows 8（Basic 版本）	否	是	否	是	否	高

安裝方法/作業系統支援	部署考量					
	WAN 部署	集中管理	需要使用者的操作	需要 IT 資源	大規模部署	耗用頻寬
安全性符合安裝 支援除下列作業系統之外的所有作業系統： • Windows Vista Home Basic 和 Home Premium Edition • Windows XP Home Edition • Windows 7 Home Basic/ Home Premium • Windows 8（Basic 版本）	否	是	否	是	否	高

Web 安裝網頁的安裝

如果您已將 OfficeScan 伺服器安裝到執行下列平台的電腦，使用者便可以從 Web 安裝網頁安裝 OfficeScan 用戶端程式：

- Windows Server 2003（含 Internet Information Server (IIS) 6.0 或 Apache 2.0.x）
- Windows Server 2008（含 Internet Information Server (IIS) 7.0）
- Windows Server 2008 R2（含 Internet Information Server (IIS) 7.5）
- Windows Server 2012（含 Internet Information Server (IIS) 8.0）

如果要從 Web 安裝網頁安裝，您需要下列項目：

- Internet Explorer（必須將安全層級設定為允許 ActiveX™ 控制項）。所需版本如下：
  - 6.0 (Windows XP 和 Windows Server 2003)
  - 7.0 (Windows Vista 和 Windows Server 2008)
  - 8.0 (Windows 7)
  - 10.0（Windows 8 和 Windows Server 2012）
- 電腦的管理員權限

傳送下列指示給使用者，讓他們從 Web 安裝網頁安裝 OfficeScan 用戶端。如果要透過電子郵件傳送 OfficeScan 用戶端安裝通知，請參閱開始 Browser-based 安裝 第 5-16 頁。

從 Web 安裝網頁進行安裝

程序

1. 使用內建的管理員帳號登入電腦。

   注意

   若是 Windows 7 或 8 平台，您必須先啟動內建的管理員帳號。依預設，Windows 7 和 8 會關閉內建的管理員帳號。如需詳細資訊，請參閱 Microsoft 支援網站 (http://technet.microsoft.com/en-us/library/dd744293%28WS.10%29.aspx)。

2. 如果要安裝到執行 Windows XP、Vista、Server 2008、7、8 或 Server 2012 的電腦，請執行下列步驟：

   a. 啟動 Internet Explorer 並將 OfficeScan 伺服器 URL（例如：`https://<OfficeScan server name>:4343/officescan`）新增至信任的網站清單中。在 Windows XP Home 中，移至「工具 > 網際網路選項 > 安全性」標籤，選取「信任的網站」圖示並按一下「網站」，即可存取此清單。

b. 修改 Internet Explorer 安全性設定，以啟動「自動提示 ActiveX 控制項」。在 Windows XP 中，移至「工具 > 網際網路選項 > 安全性」標籤，然後按一下「自訂層級」。

3. 開啟 Internet Explorer 視窗，並輸入下列其中一項：

   - OfficeScan 伺服器（含 SSL）：

     ```
     https://<OfficeScan server name>:<port>/officescan
     ```

   - OfficeScan 伺服器（不含 SSL）：

     ```
     http://<OfficeScan server name>:<port>/officescan
     ```

4. 按一下登入頁面上的連結。

5. 在顯示的新畫面中，按一下「立即安裝」即可開始安裝 OfficeScan 用戶端。OfficeScan 用戶端安裝隨即開始。收到提示時，請允許安裝 ActiveX 控制項。安裝後，Windows 系統匣內會出現 OfficeScan 用戶端圖示。

注意

如需系統匣上顯示的圖示清單，請參閱 OfficeScan 用戶端圖示 第 14-23 頁。

Browser-based 安裝

設定電子郵件訊息，以指示網路上的使用者安裝 OfficeScan 用戶端。使用者可以按一下電子郵件中提供的 OfficeScan 用戶端安裝程式連結以開始安裝。

在您安裝 OfficeScan 用戶端之前：

- 檢查 OfficeScan 用戶端安裝需求。
- 識別網路上有哪些電腦目前沒有受到免於遭受安全威脅的防護。執行下列工作：
  - 執行 Trend Micro Vulnerability Scanner。此工具會根據您指定的 IP 位址範圍，分析電腦是否已安裝防毒軟體。如需詳細資訊，請參閱 Vulnerability Scanner 使用率 第 5-34 頁。

- 執行「安全性符合」。如需詳細資訊，請參閱適用於未受管端點的安全性符合 第 14-60 頁。

開始 Browser-based 安裝

程序

1. 瀏覽至「用戶端電腦 > 用戶端安裝 > Browser-based」。
2. 視需要修改電子郵件訊息的主旨行。
3. 按一下「建立電子郵件」。

   會開啟預設郵件程式。
4. 將電子郵件傳送給預期收件者。

執行 UNC-based 安裝

`AutoPcc.exe` 是一種能將 OfficeScan 用戶端安裝到未受保護的電腦，並更新程式檔案和元件的獨立式程式。電腦必須是網域的一部分，才能經由通用命名慣例 (UNC) 路徑使用 AutoPcc。

程序

1. 瀏覽至「用戶端電腦 > 用戶端安裝 > UNC-based」。
   - 如果要使用 `AutoPcc.exe` 將 OfficeScan 用戶端安裝到未受保護的電腦：
     a. 連接到伺服器電腦。瀏覽至 UNC 路徑：

        `\\<伺服器電腦名稱>\ofscan`

     b. 以滑鼠右鍵按一下 `AutoPcc.exe`，然後選取「以系統管理員身分執行」。
   - 使用 `AutoPcc.exe` 進行遠端桌面安裝：

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

b. 瀏覽至 `\\<伺服器電腦名稱>\ofscan` 目錄，然後執行 `AutoPcc.exe`。

從 OfficeScan Web 主控台遠端安裝

您可以從遠端將 OfficeScan 用戶端安裝到一部或多部連線到網路的電腦。您務必要有目標電腦的管理員權限，才能執行遠端安裝。遠端安裝不會在執行 OfficeScan 伺服器的電腦上安裝 OfficeScan 用戶端。

注意

此安裝方法無法用在執行 Windows XP Home、Windows Vista Home Basic 和 Home Premium Edition、Windows 7 Home Basic 和 Home Premium Edition（32 位元和 64 位元版本）以及 Windows 8（32 位元和 64 位元 Basic 版本）的電腦上。純 IPv6 伺服器無法在純 IPv4 用戶端上安裝 OfficeScan 用戶端。同樣地，純 IPv4 伺服器也無法在純 IPv6 用戶端上安裝 OfficeScan 用戶端。

程序

1. 如果電腦執行 Windows Vista、Windows 7、Windows 8（Pro、Enterprise）或 Windows Server 2012，請執行下列步驟：

   a. 開啟一個內建的管理者帳號，並為這個帳號設定密碼。

   b. 關閉端點上的簡易檔案共用。

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

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

   e. 開啟 Microsoft 管理主控台（按一下「開始 > 執行」，再輸入 `services.msc`），然後啟動 Remote Registry 和 Remote Procedure Call 服務。安裝 OfficeScan 用戶端時，請使用內建的管理員帳號和密碼。

2. 在 Web 主控台中，移至「用戶端電腦 > 用戶端安裝 > 遠端」。

3. 選取目標電腦。

   - 「網域和電腦」清單會顯示網路上的所有 Windows 網域。如果要顯示網域下的電腦，請按兩下網域名稱。選取電腦，然後按一下「新增」。
   - 如果要使用特定電腦名稱，請在頁面頂端的欄位中輸入電腦名稱，然後按一下「搜尋」。

   OfficeScan 將提示您輸入目標電腦的使用者名稱和密碼。使用管理員帳號的使用者名稱和密碼以繼續執行。

4. 輸入使用者名稱和密碼，然後按一下「登入」。

   目標電腦會出現在「選定的電腦」表格中。

5. 重複步驟 3 和 4 以新增更多電腦。

6. 當您準備好將 OfficeScan 用戶端安裝到目標電腦時，請按一下「 安裝 」。

   確認方塊便會出現。

7. 按一下「是」確認要將 OfficeScan 用戶端安裝到目標電腦。

   當程式檔案複製到每部目標電腦時便會出現進度畫面。

在目標電腦上安裝好 OfficeScan 後，電腦名稱會在「選定的電腦」清單的「網域和電腦」清單中顯示，並顯示紅色核取記號。

當「網域和電腦」清單中的所有目標電腦都出現紅色核取記號時，表示您已完成遠端安裝。

注意

如果您安裝到多部電腦，OfficeScan 會在記錄檔中記錄所有不成功的安裝（如需詳細資訊，請參閱全新安裝記錄檔 第 18-17 頁），但不會延後其他安裝。按一下「安裝」後，您不需要監督安裝。稍後檢查記錄檔，以查看安裝結果。

使用 Login Script Setup 安裝

Login Script Setup 會在未受保護的電腦登入網路時，自動安裝 OfficeScan 用戶端到這些電腦上。Login Script Setup 會將一個名為 AutoPcc.exe 的程式新增至伺服器登入程序檔。

AutoPcc.exe 會將 OfficeScan 用戶端安裝到未受保護的電腦，並更新程式檔案和元件。電腦必須是網域的一部分，才能經由登入程式檔使用 AutoPcc。

OfficeScan 用戶端安裝

AutoPcc.exe 會在未受保護的 Windows Server 2003 電腦登入您已修改其登入程式檔的伺服器時，自動將 OfficeScan 用戶端安裝到該電腦上。不過，AutoPcc.exe 不會自動將 OfficeScan 用戶端安裝到 Windows Vista、7、8、Server 2008 和 Server 2012 的電腦上。使用者必須連線到伺服器電腦，瀏覽至 \\<伺服器電腦名稱>\ofcscan，以滑鼠右鍵按一下 AutoPcc.exe，然後選取「以系統管理員身分執行」。

使用 AutoPcc.exe 進行遠端桌面安裝：

- 電腦必須以 Mstsc.exe/主控台模式執行。如此會使 AutoPcc.exe 安裝在作業階段 0 中執行。
- 將磁碟機對應到「ofcscan」資料夾，並從該處執行 AutoPcc.exe。

程式和元件更新

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

Windows Server 2003, 2008 與 2012 程式檔

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

Login Script Setup 會在程式檔的檔尾附加下列命令：

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

說明：

- `<Server_name>` 是 OfficeScan 伺服器電腦的電腦名稱或 IP 位址。
- "`ofcscan`" 是伺服器上的 OfficeScan 共享資料夾名稱。
- "`autopcc`" 是指向安裝 OfficeScan 用戶端的 autopcc 可執行檔案的連結。

登入程式檔位置（透過網路登入共享目錄）：

- `Windows Server 2003：\\Windows 2003 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`
- `Windows Server 2008：\\Windows 2008 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`
- `Windows Server 2012：\\Windows 2012 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`

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

程序

1. 在您用來執行伺服器安裝的電腦上，從 Windows「開始」功能表按一下「程式集 > Trend Micro OfficeScan 伺服器 <伺服器名稱> > Login Script Setup」。

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

2. 找出要修改其登入程式檔的伺服器，選取該伺服器，然後按一下「選取」。確定伺服器是網域主控站，而且您已具備該伺服器的管理員存取權。

   Login Script Setup 會提示您輸入使用者名稱和密碼。

3. 輸入使用者名稱和密碼。按一下「確定」繼續。

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

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

5. 如果要修改所有使用者的登入程式檔，請按一下「全部新增」。

6. 如果要排除之前選取的使用者資料檔，請從「選定的使用者」清單選取名稱，然後按一下「刪除」。

7. 如果要重設選擇，請按一下「全部刪除」。

8. 當所有目標使用者資料檔都位於「選定的使用者」清單中時，請按一下「套用」。

   此時會出現訊息，通知您已成功修改伺服器登入程式檔。

9. 按一下「確定」。

   Login Script Setup 會返回其初始畫面。

10. 如果要修改其他伺服器的登入程式檔，請重複步驟 2 到 4。

11. 如果要關閉 Login Script Setup，請按一下「結束」。

以用戶端封裝程式安裝

「用戶端封裝程式」可建立安裝套件，而且您可以使用傳統媒體（例如：CD-ROM）將安裝套件傳送給使用者。使用者可以在用戶端電腦上執行該套件，以安裝或升級 OfficeScan 用戶端和更新元件。

要將 OfficeScan 用戶端或元件部署到低頻寬遠端辦公室的用戶端時，「用戶端封裝程式」特別實用。使用「用戶端封裝程式」安裝的 OfficeScan 用戶端會向建立該套件的伺服器回報。

「Client Packager」需要下列項目：

- 350MB 的可用磁碟空間
- Windows Installer 2.0（執行 MSI 套件）

使用用戶端封裝程式建立安裝套件

程序

1. 在 OfficeScan 伺服器電腦上，瀏覽至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\ClientPackager。
2. 按兩下 ClnPack.exe 執行此一工具。Client Packager 主控台便會開啟。
3. 選取您要建立的套件類型。

   表 5-5. 用戶端套件類型

套件類型	說明
安裝	選取「安裝」將套件建立為可執行檔案。套件會安裝 OfficeScan 用戶端程式和伺服器上目前可用的元件。如果目標電腦已安裝舊版 OfficeScan 用戶端，則執行這個可執行檔案會升級用戶端。
更新	選取「更新」可以建立包含伺服器上目前可用元件的套件。套件將會建立為可執行檔案。如果更新用戶端電腦上的元件時發生問題，請使用此套件。
MSI	選取「MSI」可以建立符合 Microsoft Installer 套件格式的套件。套件也會安裝 OfficeScan 用戶端程式和伺服器上目前可用的元件。如果目標電腦已安裝舊版 OfficeScan 用戶端，則執行 MSI 檔案會升級用戶端。

4. 進行下列設定（某些設定只有當您選取特定套件類型時才能使用）：
   - Windows 作業系統類型 第 5-24 頁
   - 掃瞄方法 第 5-24 頁
   - 自動安裝 第 5-25 頁
   - 關閉安裝前掃瞄 第 5-25 頁

- 以最新版本強制覆寫 第 5-26 頁
- 更新代理程式功能 第 5-26 頁
- Outlook 郵件掃瞄 第 5-27 頁
- Check Point SecureClient 支援 第 5-27 頁
- 元件 第 5-27 頁

5. 在「來源檔案」旁確認 `ofcscan.ini` 檔案的位置正確。如果要修改路徑，請按一下 (...) 以瀏覽 `ofcscan.ini` 檔案。依預設，這個檔案位於 OfficeScan 伺服器的 <伺服器安裝資料夾>\PCCSRV 資料夾中。

6. 在「輸出檔案」中，按一下 (...) 以指定要建立 OfficeScan 用戶端套件的位置，並輸入套件檔案名稱（例如：`ClientSetup.exe`）。

7. 按一下「建立」。

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

8. 部署套件。

套件部署指導方針

1. 將套件傳送給使用者，然後請他們按兩下 `.exe` 或 `.msi` 檔案，在電腦上執行 OfficeScan 用戶端套件。

   注意

   請僅將套件傳送給其 OfficeScan 用戶端會向建立套件的所在伺服器進行報告的使用者。

2. 如果有使用者將在執行 Windows Vista、Server 2008、7、8 或 Server 2012 的電腦上安裝 `.exe` 套件，請指示他們用滑鼠右鍵按一下 `.exe` 檔案並選取「以系統管理員身分執行」。

3. 如果您是建立 `.msi` 檔案，請執行下列工作來部署該套件：

- 使用 Active Directory 或 Microsoft SMS。如需詳細資訊，請參閱使用 Active Directory 部署 MSI 套件 第 5-28 頁或使用 Microsoft SMS 部署 MSI 套件 第 5-29 頁。

4. 啟動 MSI 套件（從命令提示字元視窗），以無訊息方式將 OfficeScan 用戶端安裝到執行 Windows XP、Vista、Server 2008、7、8 或 Server 2012 的遠端電腦。

Windows 作業系統類型

選取要針對其建立套件的作業系統。只將該套件部署到執行該類型的作業系統的電腦。如果要部署到另一種類型的作業系統，請建立另一個套件。

掃瞄方法

為套件選取掃瞄方法。如需詳細資訊，請參閱掃瞄方法 第 7-6 頁。

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

選取掃瞄方法之前，請記住下列指導方針，以便有效率地部署套件：

- 如果您將使用套件將用戶端升級到此 OfficeScan 版本，請檢查 Web 主控台上的網域等級掃瞄方法。在主控台上，移至「用戶端電腦 > 用戶端管理」，選取用戶端所屬用戶端樹狀結構網域，然後按一下「設定 > 掃瞄設定 > 掃瞄方法」。網域等級掃瞄方法應該與套件的掃瞄方法一致。
- 如果您將使用套件來執行 OfficeScan 用戶端的全新安裝，請檢查用戶端分組設定。在 Web 主控台上，移至「用戶端電腦 > 用戶端分組」。
- 如果用戶端是按照 NetBIOS、Active Directory 或 DNS 網域分組，請檢查目標電腦所屬的網域。如果網域存在，請檢查為該網域設定的掃瞄方法。如果網域不存在，請檢查根層級掃瞄方法（選取用戶端樹狀結構上的根網域圖示，然後按一下設定 > 掃瞄設定 > 掃瞄方法）。網域或根層級掃瞄方法應該與套件的掃瞄方法一致。

- 如果用戶端是按照自訂用戶端群組分組，請檢查「分組優先順序」和「來源」。

圖 5-1.「自動用戶端分組」預覽窗格

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

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

自動安裝

此選項可建立在用戶端電腦背景中安裝的套件，不但用戶端不會察覺，而且也不會顯示安裝狀態視窗。如果您規劃將套件部署到遠端目標電腦，請啟動此選項。

關閉安裝前掃瞄

此選項只適用於全新安裝。

如果目標電腦並未安裝 OfficeScan 用戶端，套件會先掃瞄電腦中是否有安全威脅，再安裝 OfficeScan 用戶端。如果您確定目標電腦沒有感染安全威脅，則可以關閉安裝前掃瞄。

如果啟動安裝前掃瞄，安裝程式會掃瞄電腦最容易遭受攻擊的區域中是否有病毒/惡意程式，這些區域如下：

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

以最新版本強制覆寫

此選項會使用伺服器上目前可用的版本覆寫用戶端的元件版本。啟動此選項可確保伺服器上的元件與用戶端上的元件同步。

更新代理程式功能

此選項會將「更新代理程式」權限指定給目標電腦上的 OfficeScan 用戶端。「更新代理程式」可協助 OfficeScan 伺服器部署元件到用戶端。如需詳細資訊，請參閱更新代理程式 第 6-46 頁。

您可以允許「更新代理程式」執行下列工作：

- 部署元件
- 部署設定
- 部署程式

如果將「更新代理程式」權限指定給 OfficeScan 用戶端：

1. 請記住，如果套件將部署至純 IPv6 用戶端，「更新代理程式」只能將更新檔分發到純 IPv6 或雙堆疊用戶端。
2. 使用「預約更新組態設定工具」來啟動並設定代理程式的預約更新。如需詳細資訊，請參閱更新代理程式的更新方式 第 6-52 頁。
3. 管理「更新代理程式」的 OfficeScan 伺服器將無法同步處理或部署下列設定到代理程式：
    - 更新代理程式權限
    - 用戶端預約更新
    - 來自趨勢科技主動式更新伺服器的更新檔

- 從其他更新來源更新

因此，請只將 OfficeScan 用戶端套件部署到不會由 OfficeScan 伺服器管理的電腦。然後，設定「更新代理程式」從 OfficeScan 伺服器以外的更新來源（例如：自訂更新來源）取得其更新檔。如果想要讓 OfficeScan 伺服器與「更新代理程式」同步處理設定，請勿使用「Client Packager」，而應該改為選擇其他 OfficeScan 用戶端安裝方法。

Outlook 郵件掃瞄

此選項會安裝「Outlook 郵件掃瞄」程式，此程式可掃瞄 Microsoft Outlook™ 信箱是否有安全威脅。如需詳細資訊，請參閱郵件掃瞄權限和其他設定 第 7-57 頁。

Check Point SecureClient 支援

此工具會新增對於 Check Point™ SecureClient™ for Windows XP 和 Windows Server 2003 的支援。SecureClient 會在允許連線到網路之前先驗證病毒碼版本。如需詳細資訊，請參閱 Check Point 架構和組態設定總覽 第 17-2 頁。

注意

SecureClient 不會驗證使用雲端截毒掃瞄的用戶端上的病毒碼版本。

元件

選取要加入套件中的元件和功能。

- 如需有關元件的詳細資訊，請參閱 OfficeScan 元件和程式 第 6-2 頁。
- 只有當您安裝並註冊「資料安全防護」之後，才能使用「資料安全防護」模組。如需有關「資料安全防護」的詳細資訊，請參閱使用 Data Loss Prevention 第 10-1 頁。

使用 Active Directory 部署 MSI 套件

利用 Active Directory 的功能，將 MSI 套件同時部署到多部用戶端電腦。如需有關建立 MSI 檔的詳細資訊，請參閱以用戶端封裝程式安裝 第 5-21 頁。

程序

1. 執行下列工作：
   - Windows Server 2003 和更早版本：
     a. 開啟 Active Directory 主控台。
     b. 以滑鼠右鍵按一下要在其中部署 MSI 套件的「組織單位」(OU)，然後按一下「內容」。
     c. 在「群組原則」標籤中，按一下「新增」。
   - Windows Server 2008 和 Windows Server 2008 R2：
     a. 開啟「群組原則管理主控台」。按一下「開始 > 控制台 > 管理工具 > 群組原則管理」。
     b. 在主控台樹狀結構中，展開樹狀結構和網域（包含您要編輯的 GPO）中的「群組原則物件」。
     c. 以滑鼠右鍵按一下您要編輯的 GPO，然後按一下「編輯」。這時會開啟「群組原則物件編輯器」。
   - Windows Server 2012：
     a. 開啟「群組原則管理主控台」。按一下「伺服器管理 > 工具 > 群組原則管理」。
     b. 在主控台樹狀結構中，展開樹狀結構和網域（包含您要編輯的 GPO）中的「群組原則物件」。
     c. 以滑鼠右鍵按一下您要編輯的 GPO，然後按一下「編輯」。這時會開啟「群組原則物件編輯器」。
2. 選擇「電腦組態設定」或「使用者組態設定」其中一項，然後開啟其下方的「軟體設定」。

秘訣

趨勢科技建議您使用「電腦組態設定」而非「使用者組態設定」，以確保不論登入電腦的使用者是誰，都能成功安裝 MSI 套件。

3. 在「軟體設定」下，以滑鼠右鍵按一下「軟體安裝」，然後選取「新增」和「套件」。
4. 找出 MSI 套件並加以選取。
5. 選取部署方法，然後按一下「確定」。
   - 已指定：MSI 套件會在使用者下次登入電腦時（如果您選取「使用者組態設定」），或是在電腦重新啟動時（如果您選取「電腦組態設定」）自動部署。這種方法完全不需要使用者的操作。
   - 已發佈：如果要執行 MSI 套件，請通知使用者移至「控制台」，開啟「新增/移除程式」畫面，然後選取在網路上新增/安裝程式的選項。OfficeScan 用戶端的 MSI 套件顯示時，使用者便可繼續安裝 OfficeScan 用戶端。

使用 Microsoft SMS 部署 MSI 套件

如果您的伺服器上已安裝 Microsoft BackOffice SMS，則可以使用 Microsoft System Management Server (SMS) 來部署 MSI 套件。如需有關建立 MSI 檔的詳細資訊，請參閱以用戶端封裝程式安裝 第 5-21 頁。

SMS 伺服器必須先從 OfficeScan 伺服器取得 MSI 檔，才能將套件部署到目標電腦。

- 本機：SMS 伺服器和 OfficeScan 伺服器位於同一部電腦上。
- 遠端：SMS 伺服器和 OfficeScan 伺服器位於不同的電腦上。

使用 Microsoft SMS 進行安裝時的已知問題：

- 「未知」出現在 SMS 主控台的「執行時間」欄位中。
- 如果安裝不成功，SMS 程式監視器上的安裝狀態可能仍會顯示安裝已完成。如需有關如何檢查安裝是否成功的詳細資訊，請參閱安裝後 第 5-61 頁。

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

在本機取得套件

程序

1. 開啟「SMS 管理員」主控台。
2. 在「樹狀結構」標籤上，按一下「套件」。
3. 在「動作」功能表上，按一下「新增｜ > 出自定義的套件」。

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

   會出現「套件定義」畫面。
5. 按一下「瀏覽」。

   會出現「開啟」畫面。
6. 瀏覽並選取由用戶端封裝程式建立的 MSI 套件，然後按一下「開啟」，

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

   會出現「來源檔案」畫面。
8. 按一下「一律由來源目錄取得檔案」，然後按「下一步」。

   會出現「來源目錄」畫面，其中顯示要建立的套件名稱和來源目錄。
9. 按一下「網站伺服器上的本機磁碟機」。
10. 按一下「瀏覽」，然後選取包含 MSI 檔案的來源目錄。
11. 按「下一步」。

精靈便會建立套件。完成程序後，套件名稱會出現在「SMS 管理員」主控台上。

從遠端取得套件

程序

1. 在 OfficeScan 伺服器上，使用用戶端封裝程式建立副檔名為 `.exe` 的安裝程式套件（您無法建立 `.msi` 套件）。如需詳細資訊，請參閱以用戶端封裝程式安裝 第 5-21 頁。
2. 在要儲存來源的電腦上建立共享資料夾。
3. 開啟「SMS 管理員」主控台。
4. 在「樹狀結構」標籤上，按一下「套件」。
5. 在「動作」功能表上，按一下「新增｜ > 出自定義的套件」。

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

   會出現「套件定義」畫面。
7. 按一下「瀏覽」。

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

   會出現「來源檔案」畫面。
10. 按一下「一律由來源目錄取得檔案」，然後按「下一步」。

    會出現「來源目錄」畫面。
11. 按一下「網路路徑（UNC 名稱）」。
12. 按一下「瀏覽」，然後選取包含 MSI 檔案的來源目錄（您建立的共享資料夾）。

13. 按「下一步」。

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

將套件分發到目標電腦

程序

1. 在「樹狀結構」標籤上，按一下「通告」。
2. 在「動作」功能表上，按一下「所有工作｜ > 分發軟體」。

   會出現「分發軟體精靈」的「歡迎使用」畫面。
3. 按「下一步」。

   會出現「套件」畫面。
4. 按一下「分發現有套件」，然後按一下您建立的安裝程式套件名稱。
5. 按「下一步」。

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

   會出現「通告程式」畫面。
7. 按一下「是」以通告 OfficeScan 用戶端安裝程式套件，然後按「下一步」。

   會出現「通告目標」畫面。
8. 按一下「瀏覽」以選取目標電腦。

   會出現「瀏覽集合」畫面。
9. 按一下「所有 Windows NT 系統」。
10. 按一下「確定」。

    會再度出現「通告目標」畫面。

11. 按「下一步」。

    會出現「通告名稱」畫面。

12. 在文字方塊中，輸入通告的名稱和備註，然後按「下一步」。

    會出現「通告至子集合」畫面。

13. 選擇是否要將套件通告至子集合。選擇只將程式通告至指定集合的成員，或是通告至子集合的成員。

14. 按「下一步」。

    會出現「通告預約時程」畫面。

15. 輸入或選取日期和時間，以指定何時要通告 OfficeScan 用戶端安裝程式套件。

    注意

    如果要讓 Microsoft SMS 在特定日期停止通告套件，請按一下「是，這項通告應到期」，然後在「到期日期和時間」清單方塊中指定日期和時間。

16. 按「下一步」。

    會出現「指定程式」畫面。

17. 按一下「是，指定程式」，然後按「下一步」。

    Microsoft SMS 會建立通告，並將其顯示在「SMS 管理員」主控台上。

18. 當 Microsoft SMS 將已通告的程式（亦即 OfficeScan 用戶端程式）分發到目標電腦時，每部目標電腦上都會顯示一個畫面。指示使用者按一下「是」，然後遵循精靈提供的指示將 OfficeScan 用戶端安裝到他們的電腦上。

使用用戶端磁碟映像安裝

磁碟映像技術可讓您使用磁碟映像軟體建立 OfficeScan 用戶端的映像，並且複製該映像至網路上的其他電腦。

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

建立 OfficeScan 用戶端的磁碟映像

程序

1. 在電腦上安裝 OfficeScan 用戶端。
2. 將 <伺服器安裝資料夾>`\PCCSRV\Admin\Utility\ImgSetup` 中的 `ImgSetup.exe` 複製到這部電腦。
3. 在這部電腦上執行 `ImgSetup.exe`。

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

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

警告!

為避免在 OfficeScan 資料庫中出現兩部相同名稱的電腦，請手動變更複製的 OfficeScan 用戶端的電腦名稱或網域名稱。

Vulnerability Scanner 使用率

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

使用 Vulnerability Scanner 時的考量

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

網路管理

表 5-6. 網路管理

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

網路拓撲和架構

表 5-7. 網路拓撲和架構

安裝	VULNERABILITY SCANNER 的有效性
單一位置	非常有效。Vulnerability Scanner 允許您掃瞄整個 IP 網段，並且輕鬆地在 LAN 上安裝 OfficeScan 用戶端。
具備高速連線的多個位置	普通有效
具備低速連線的多個位置	無效。您必須在每一個位置執行弱點掃瞄，而且必須將 OfficeScan 用戶端安裝指向一台本機 OfficeScan 伺服器。
遠端和隔離電腦	普通有效

軟體/硬體規格

表 5-8. 軟體/硬體規格

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

網域結構

表 5-9. 網域結構

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

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

網路傳輸

表 5-10. 網路傳輸

安裝	Vulnerability Scanner 的有效性
LAN 連線	非常有效
512 Kbps	普通有效
T1 連線或更高速的連線	普通有效
撥接	無效。要完成安裝 OfficeScan 用戶端可能會花費很長一段時間。

網路大小

表 5-11. 網路大小

安裝	Vulnerability Scanner 的有效性
超大型企業	非常有效。網路愈大，愈需要使用 Vulnerability Scanner 來檢查有無安裝 OfficeScan 用戶端。
中小型企業	普通有效。如果是小型網路，也可以選擇 Vulnerability Scanner 安裝 OfficeScan 用戶端。其他 OfficeScan 用戶端安裝方法可能會證明實作更為容易。

使用 Vulnerability Scanner 安裝 OfficeScan 用戶端的指導方針

在下列情況中，Vulnerability Scanner 將不會安裝 OfficeScan 用戶端：

- 目標主機上已安裝 OfficeScan 伺服器或其他安全防護軟體。
- 遠端電腦執行的是 Windows XP Home、Windows Vista Home Basic、Windows Vista Home Premium、Windows 7 Home Basic、Windows 7 Home Premium 或 Windows 8（Basic 版本）。

注意

您可以使用部署考量 第 5-10 頁中討論的其他安裝方法，將 OfficeScan 用戶端安裝到目標主機。

使用 Vulnerability Scanner 安裝 OfficeScan 用戶端之前，請先執行下列步驟：

- 如果是 Windows Vista（Business、Enterprise 或 Ultimate Edition）或 Windows 7（Professional、Enterprise 或 Ultimate Edition）、Windows 8（Pro、Enterprise）、Windows Server 2012 (Standard)：
  1. 開啟一個內建的管理者帳號，並為這個帳號設定密碼。
  2. 按一下「開始 > 程式集 > 管理工具 > 具有進階安全性的 Windows 防火牆」。
  3. 如果是「網域資料檔」、「私密資料檔」和「公開資料檔」，請將防火牆狀態設為「關閉」。
  4. 開啟 Microsoft 管理主控台（按一下「開始 > 執行」，再輸入 `services.msc`），然後啟動「遠端登錄」服務。安裝 OfficeScan 用戶端時，請使用內建的管理員帳號和密碼。
- 如果是 Windows XP Professional (32 位元或 64 位元版本)：
  1. 開啟「Windows 檔案總管」，然後按一下「工具 > 資料夾選項」。
  2. 按一下「檢視」標籤，並關閉「使用簡易檔案共用（建議使用）」。

弱點掃瞄方法

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

有許多方法可以執行弱點掃瞄。

表 5-12. 弱點掃瞄方法

方法	詳細資訊
手動弱點掃瞄	管理員可以視需要執行弱點掃瞄。
DHCP 掃瞄	管理員可以在向 DHCP 伺服器請求 IP 位址的主機上執行弱點掃瞄。 Vulnerability Scanner 會監聽第 67 號通訊埠（DHCP 要求的 DHCP 伺服器監聽通訊埠）。如果它偵測到來自主機的 DHCP 要求，則會在該主機上執行弱點掃瞄。 注意 如果您在 Windows Server 2008、Windows 7、Windows 8 或 Windows Server 2012 上啟動 Vulnerability Scanner，則它將無法偵測 DHCP 要求。
預約弱點掃瞄	系統會根據管理員設定的預約自動執行弱點掃瞄。

Vulnerability Scanner 執行之後，它會顯示目標主機上的 OfficeScan 用戶端狀態。狀態可以是下列任一種：

- 一般：OfficeScan 用戶端已啟動且正常運作中
- 異常：OfficeScan 用戶端服務未執行，或用戶端沒有即時安全防護
- 未安裝：TMListen 服務遺失或未安裝 OfficeScan 用戶端
- 無法連接：Vulnerability Scanner 無法建立與主機的連線，因此無法判斷 OfficeScan 用戶端的狀態

執行手動弱點掃瞄

程序

1. 如果要在 OfficeScan 伺服器電腦上執行弱點掃瞄，請瀏覽至<伺服器安裝資料夾>\PCCSRV\Admin\Utility\TMVS，然後按兩下 TMVS.exe。隨即顯示「Trend Micro Vulnerability Scanner」主控台。在另一部執行 Windows Server 2003、Server 2008、Vista、7、8 或 Server 2012 的電腦上執行弱點掃瞄：

   a. 在 OfficeScan 伺服器電腦上，瀏覽至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility。

   b. 將 TMVS 資料夾複製到另一部電腦。

   c. 在該電腦上，開啟 TMVS 資料夾，然後按兩下 TMVS.exe。

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

   注意

   您無法從「終端機伺服器」啟動此工具。

2. 移至「手動掃瞄」區段。

3. 輸入您要檢查的電腦 IP 位址範圍。

   a. 輸入 IPv4 位址範圍。

   注意

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

   b. 對於 IPv6 位址範圍，請輸入 IPv6 字首和長度。

   注意

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

4. 按一下「設定」。

   會出現「設定」畫面。

5. 設定下列設定：

   a. Ping 設定：弱點掃瞄可以 "ping" 您在上一個步驟中指定要檢查的 IP 位址（如果那些位址目前使用中）。如果目標主機使用 IP 位址，Vulnerability Scanner 可以判斷該主機的作業系統。如需詳細資訊，請參閱 Ping 設定 第 5-53 頁。

   b. 擷取電腦說明的方法：對於已回應 "ping" 命令的主機，Vulnerability Scanner 可以擷取該主機的其他相關資訊。如需詳細資訊，請參閱擷取電腦說明的方法 第 5-50 頁。

   c. 產品查詢：Vulnerability Scanner 可以檢查主機上是否有安全防護軟體。如需詳細資訊，請參閱產品查詢 第 5-47 頁。

   d. OfficeScan 伺服器設定：如果想要讓 Vulnerability Scanner 自動將 OfficeScan 用戶端安裝到未受保護的主機，您可以設定這些設定。這些設定可識別 OfficeScan 用戶端的上層伺服器，以及用來登入主機的系統管理認證。如需詳細資訊，請參閱 OfficeScan 伺服器設定 第 5-54 頁。

   注意

   特定情況可能會造成無法在目標主機上 OfficeScan 用戶端。如需詳細資訊，請參閱使用 Vulnerability Scanner 安裝 OfficeScan 用戶端的指導方針 第 5-38 頁。

   e. 通知：Vulnerability Scanner 可將弱點掃瞄結果傳送給 OfficeScan 管理員。它也可以在未受保護的主機上顯示通知。如需詳細資訊，請參閱通知 第 5-51 頁。

   f. 儲存結果：除了將弱點掃瞄結果傳送給管理員之外，Vulnerability Scan 也可以將結果儲存為 `.csv` 檔案。如需詳細資訊，請參閱弱點掃瞄結果 第 5-52 頁。

6. 按一下「確定」。

   會關閉「設定」畫面。

7. 按一下「開始」。

   弱點掃瞄結果會在「手動掃瞄」標籤下的「結果」表格中顯示。

   注意

   如果電腦執行的是 Windows Server 2008 或 Windows Server 2012，則「結果」表格不會顯示 MAC 位址資訊。

8. 如果要將結果儲存成逗號分隔值 (CSV) 檔案，請按一下「匯出」，找到您要儲存檔案的資料夾，然後輸入檔案名稱，再按一下「儲存」。

執行 DHCP 掃瞄

程序

1. 在位於下列資料夾的 `TMVS.ini` 檔案設定 DHCP 設定：<伺服器安裝資料夾>\PCCSRV\Admin\Utility\TMVS。

   表 5-13. `TMVS.ini` 檔案中的 DHCP 設定

設定	說明
DhcpThreadNum=x	指定 DHCP 模式的執行緒數量。最小是 3，最大是 100。預設值是 3。
DhcpDelayScan=x	這是在檢查發出要求的電腦是否已安裝防毒軟體之前，以秒為單位的延遲時間。 最小值是 0（不等待），而最大值是 600。預設值是 60。
LogReport=x	0 表示關閉記錄功能，1 表示啟動記錄功能。 Vulnerability Scanner 會將掃瞄結果傳送到 OfficeScan 伺服器。記錄檔會顯示在 Web 主控台的「系統事件記錄檔」畫面中。
OsceServer=x	這是 OfficeScan 伺服器的 IP 位址或 DNS 名稱。
OsceServerPort=x	這是 OfficeScan 伺服器上的 Web 伺服器通訊埠。

2. 如果要在 OfficeScan 伺服器電腦上執行弱點掃瞄，請瀏覽至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\TMVS，然後按兩下 TMVS.exe。隨即顯示「Trend Micro Vulnerability Scanner」主控台。

   a. 在 OfficeScan 伺服器電腦上，瀏覽至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility。

   b. 將 TMVS 資料夾複製到另一部電腦。

   c. 在該電腦上，開啟 TMVS 資料夾，然後按兩下 TMVS.exe。

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

注意

您無法從「終端機伺服器」啟動此工具。

---

3. 在「手動掃瞄」區段下，按一下「設定」。

   會出現「設定」畫面。

4. 設定下列設定：

   a. 產品查詢：Vulnerability Scanner 可以檢查主機上是否有安全防護軟體。如需詳細資訊，請參閱產品查詢 第 5-47 頁。

   b. OfficeScan 伺服器設定：如果想要讓 Vulnerability Scanner 自動將 OfficeScan 用戶端安裝到未受保護的主機，您可以設定這些設定。這些設定可識別 OfficeScan 用戶端的上層伺服器，以及用來登入主機的系統管理認證。如需詳細資訊，請參閱OfficeScan 伺服器設定 第 5-54 頁。

注意

特定情況可能會造成無法在目標主機上 OfficeScan 用戶端。如需詳細資訊，請參閱使用 Vulnerability Scanner 安裝 OfficeScan 用戶端的指導方針 第 5-38 頁。

---

   c. 通知：Vulnerability Scanner 可將弱點掃瞄結果傳送給 OfficeScan 管理員。它也可以在未受保護的主機上顯示通知。如需詳細資訊，請參閱通知 第 5-51 頁。

d. 儲存結果：除了將弱點掃瞄結果傳送給管理員之外，Vulnerability Scan 也可以將結果儲存為 .csv 檔案。如需詳細資訊，請參閱弱點掃瞄結果 第 5-52 頁。

5. 按一下「確定」。

   會關閉「設定」畫面。

6. 在「結果」表格中，按一下「DHCP 掃瞄」標籤。

   注意

   執行 Windows Server 2008、Windows 7、Windows 8 和 Windows Server 2012 的電腦上不會顯示「DHCP 掃瞄」標籤。

7. 按一下「開始」。

   Vulnerability Scanner 會開始監聽 DHCP 要求，並且在電腦登入到網路時對電腦執行弱點檢查。

8. 如果要將結果儲存成逗號分隔值 (CSV) 檔案，請按一下「匯出」，找到您要儲存檔案的資料夾，然後輸入檔案名稱，再按一下「儲存」。

設定預約弱點掃瞄

程序

1. 如果要在 OfficeScan 伺服器電腦上執行弱點掃瞄，請瀏覽至<伺服器安裝資料夾>\PCCSRV\Admin\Utility\TMVS，然後按兩下 TMVS.exe。隨即顯示「Trend Micro Vulnerability Scanner」主控台。在另一部執行 Windows Server 2003、Server 2008、Vista、7、8 或 Server 2012 的電腦上執行弱點掃瞄：

   a. 在 OfficeScan 伺服器電腦上，瀏覽至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility。

   b. 將 TMVS 資料夾複製到另一部電腦。

   c. 在該電腦上，開啟 TMVS 資料夾，然後按兩下 TMVS.exe。

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

注意

您無法從「終端機伺服器」啟動此工具。

2. 移至「預約掃瞄」區段。
3. 按一下「新增/編輯」。

   隨即出現「預約掃瞄」畫面。
4. 設定下列設定：
   a. 名稱：輸入預約弱點掃瞄的名稱。
   b. IP 位址範圍：輸入您要檢查的電腦 IP 位址範圍。
      i. 輸入 IPv4 位址範圍。

      注意

      如果在純 IPv4 或具有可用 IPv4 位址的雙堆疊主機上執行 Vulnerability Scanner，它只能查詢 IPv4 位址範圍。Vulnerability Scanner 只支援類別 B 的 IP 位址範圍，例如 168.212.1.1 到 168.212.254.254。

      ii. 對於 IPv6 位址範圍，請輸入 IPv6 字首和長度。

      注意

      如果在純 IPv6 或具有可用 IPv6 位址的雙堆疊主機上執行 Vulnerability Scanner，它只能查詢 IPv6 位址範圍。
   c. 預約：使用 24 小時制時間格式指定開始時間，然後選取預約掃瞄的執行頻率。選擇「每日一次」、「每週一次」或「每月一次」。
   d. 設定：選取要使用哪一組弱點掃瞄設定。
      - 如果已設定手動弱點掃瞄設定，且想要使用該設定，請選取「使用目前設定」。如需有關手動弱點掃瞄設定的詳細資訊，請參閱執行手動弱點掃瞄 第 5-40 頁。
      - 如果未指定手動弱點掃瞄設定，或想要使用另一組設定，請選取「修改設定」，然後按一下「設定」。會出現「設定」畫面。

您可以設定下列設定，然後按一下「確定」：

- Ping 設定：弱點掃瞄可以 "ping" 您在步驟 4b 中指定要檢查的 IP 位址（如果那些位址目前使用中）。如果目標主機使用 IP 位址，Vulnerability Scanner 可以判斷該主機的作業系統。如需詳細資訊，請參閱 Ping 設定 第 5-53 頁。
- 擷取電腦說明的方法：對於已回應 "ping" 命令的主機，Vulnerability Scanner 可以擷取該主機的其他相關資訊。如需詳細資訊，請參閱擷取電腦說明的方法 第 5-50 頁。
- 產品查詢：Vulnerability Scanner 可以檢查主機上是否有安全防護軟體。如需詳細資訊，請參閱產品查詢 第 5-47 頁。
- OfficeScan 伺服器設定：如果想要讓 Vulnerability Scanner 自動將 OfficeScan 用戶端安裝到未受保護的主機，您可以設定這些設定。這些設定可識別 OfficeScan 用戶端的上層伺服器，以及用來登入主機的系統管理認證。如需詳細資訊，請參閱 OfficeScan 伺服器設定 第 5-54 頁。

  注意

  特定情況可能會造成無法在目標主機上 OfficeScan 用戶端。如需詳細資訊，請參閱使用 Vulnerability Scanner 安裝 OfficeScan 用戶端的指導方針 第 5-38 頁。

- 通知：Vulnerability Scanner 可將弱點掃瞄結果傳送給 OfficeScan 管理員。它也可以在未受保護的主機上顯示通知。如需詳細資訊，請參閱通知 第 5-51 頁。
- 儲存結果：除了將弱點掃瞄結果傳送給管理員之外，Vulnerability Scan 也可以將結果儲存為 .csv 檔案。如需詳細資訊，請參閱弱點掃瞄結果 第 5-52 頁。

5. 按一下「確定」。

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

6. 如果要立即執行預約弱點掃瞄，請按一下「立即執行」。

弱點掃瞄結果會顯示在「預約掃瞄」標籤下的「結果」表格中。

注意

如果電腦執行的是 Windows Server 2008 或 Windows Server 2012，則「結果」表格不會顯示 MAC 位址資訊。

7. 如果要將結果儲存成逗號分隔值 (CSV) 檔案，請按一下「匯出」，找到您要儲存檔案的資料夾，然後輸入檔案名稱，再按一下「儲存」。

弱點掃瞄設定

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

注意

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

產品查詢

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

表 5-14. Vulnerability Scanner 所檢查的安全防護產品

產品	說明
ServerProtect for Windows	Vulnerability Scanner 使用 RPC 端點來檢查 `SPNTSVC.exe` 是否正在執行。它傳回的資訊包括作業系統和「病毒掃瞄引擎」、「病毒碼」和產品版本。Vulnerability Scanner 無法偵測「ServerProtect 資料伺服器」或「ServerProtect 管理主控台」。
ServerProtect for Linux	如果目標電腦並非執行 Windows，Vulnerability Scanner 會嘗試連線到第 14942 號通訊埠，檢查電腦是否已安裝 ServerProtect for Linux。

產品	說明
OfficeScan 用戶端	Vulnerability Scanner 使用 OfficeScan 用戶端通訊埠來檢查是否已安裝 OfficeScan 用戶端，也會檢查 `TmListen.exe` 程序是否正在執行。如果是從預設位置執行，它會自動擷取通訊埠號碼。 如果您是從 OfficeScan 伺服器以外的電腦啟動 Vulnerability Scanner，請檢查並使用該電腦的通訊埠。
PortalProtect™	Vulnerability Scanner 會載入 `http://localhost:port/PortalProtect/index.html` 網頁，檢查是否有安裝該產品。
ScanMail™ for Microsoft Exchange™	Vulnerability Scanner 會載入 `http://ipaddress:port/scanmail.html` 網頁，檢查是否有安裝 ScanMail。依預設，ScanMail 會使用第 16372 號通訊埠。如果 ScanMail 使用其他通訊埠號碼，請指定該通訊埠號碼。否則，Vulnerability Scanner 會偵測不到 ScanMail。
InterScan™ 系列產品	Vulnerability Scanner 會載入每個不同產品的網頁，檢查是否有安裝產品。 • InterScan Messaging Security Suite 5.x:`http://localhost:port/eManager/cgi-bin/eManager.htm` • InterScan eManager 3.x:`http://localhost:port/eManager/cgi-bin/eManager.htm` • InterScan VirusWall™ 3.x: `http://localhost:port/InterScan/cgi-bin/interscan.dll`
Trend Micro Internet Security™ (PC-cillin)	Vulnerability Scanner 使用通訊埠 40116 來檢查是否已安裝 Trend Micro Internet Security。
McAfee VirusScan ePolicy Orchestrator	Vulnerability Scanner 會將一個特別的 Token 傳送到第 8081 號 TCP 通訊埠，這是用於提供伺服器和用戶端之間連線的 ePolicy Orchestrator 預設通訊埠。具有此防毒產品的電腦會使用特別的 Token 類型回應。Vulnerability Scanner 偵測不到單機版 McAfee VirusScan。
Norton Antivirus™ Corporate Edition	Vulnerability Scanner 會將一個特別的 Token 傳送到第 2967 號 UDP 通訊埠，這是 Norton Antivirus Corporate Edition RTVScan 的預設通訊埠。具有此防毒產品的電腦會使用特別的 Token 類型回應。由於 Norton Antivirus Corporate Edition 是透過 UDP 進行通訊，因此不保證正確率。而且，網路傳輸可能會影響 UDP 等待時間。

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

- RPC：偵測 ServerProtect for NT
- UDP：偵測 Norton AntiVirus Corporate Edition 用戶端
- TCP：偵測 McAfee VirusScan ePolicy Orchestrator
- ICMP：藉由傳送 ICMP 封包偵測電腦
- HTTP：偵測 OfficeScan 用戶端
- DHCP：如果偵測到 DHCP 要求，Vulnerability Scanner 會檢查要求電腦上是否已經安裝防毒軟體。

設定產品查詢設定

產品查詢設定是弱點掃瞄設定的子集合：如需有關弱點掃瞄設定的詳細資訊，請參閱弱點掃瞄方法 第 5-39 頁。

程序

1. 如果要從 Vulnerability Scanner (`TMVS.exe`) 指定產品查詢設定：
   a. 啟動 `TMVS.exe`。
   b. 按一下「設定」。
      會出現「設定」畫面。
   c. 移至「產品查詢」區段。
   d. 選取要檢查的產品。
   e. 按一下產品名稱旁邊的「設定」，然後指定 Vulnerability Scanner 要檢查的通訊埠號碼。
   f. 按一下「確定」。
      會關閉「設定」畫面。
2. 如果要設定 Vulnerability Scanner 同時檢查有無安全防護軟體的電腦數量：
   a. 瀏覽至 <伺服器安裝資料夾>`\PCCSRV\Admin\Utility\TMVS`，然後使用文字編輯器（例如：記事本）開啟 `TMVS.ini`。

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

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

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

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

d. 儲存 `TMVS.ini`。

擷取電腦說明的方法

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

- 快速擷取：只擷取電腦名稱
- 一般擷取：擷取網域和電腦資訊

配置擷取設定

擷取設定是弱點掃瞄設定的子集合。如需有關弱點掃瞄設定的詳細資訊，請參閱弱點掃瞄方法 第 5-39 頁。

程序

1. 啟動 `TMVS.exe`。
2. 按一下「設定」。

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

6. 按一下「確定」。

   會關閉「設定」畫面。

通知

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

設定通知設定

通知設定是弱點掃瞄設定的子集合。如需有關弱點掃瞄設定的詳細資訊，請參閱弱點掃瞄方法 第 5-39 頁。

程序

1. 啟動 `TMVS.exe`。
2. 按一下「設定」。

   會出現「設定」畫面。
3. 移至「通知」區段。
4. 如果要自動將「弱點掃瞄」結果傳送給您自己或您組織中的其他管理員：
   a. 選取「將結果以電子郵件寄給系統管理員」。
   b. 按一下「設定」，指定電子郵件設定。
   c. 在「收件人」中，輸入收件人的電子郵件信箱。
   d. 在「寄件人」中，輸入寄件者的電子郵件信箱。
   e. 在「SMTP 伺服器」中，輸入 SMTP 伺服器位址。

      例如，輸入 `smtp.company.com`。SMTP 伺服器是必要資訊。
   f. 在「主旨」中，輸入訊息的新主旨或使用預設的主旨。
   g. 按一下「確定」。
5. 如果要通知使用者其電腦未安裝安全防護軟體：

a. 選取「在未受保護的電腦上顯示通知」。

b. 按一下「自訂」設定通知訊息。

c. 在「通知訊息」畫面中輸入新訊息或接受預設訊息。

d. 按一下「確定」。

6. 按一下「確定」。

會關閉「設定」畫面。

弱點掃瞄結果

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

配置掃瞄結果

弱點掃瞄結果設定是弱點掃瞄設定的子集合。如需有關弱點掃瞄設定的詳細資訊，請參閱弱點掃瞄方法 第 5-39 頁。

程序

1. 啟動 `TMVS.exe`。
2. 按一下「設定」。

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

   a. 按一下「瀏覽」。

   b. 選取電腦或網路上的目標資料夾。

   c. 按一下「確定」。
6. 按一下「確定」。

會關閉「設定」畫面。

Ping 設定

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

配置 Ping 設定

Ping 設定是弱點掃瞄設定的子集合。如需有關弱點掃瞄設定的詳細資訊，請參閱弱點掃瞄方法 第 5-39 頁。

程序

1. 如果要從 Vulnerability Scanner (`TMVS.exe`) 指定 ping 設定：
   a. 啟動 `TMVS.exe`。
   b. 按一下「設定」。
      會出現「設定」畫面。
   c. 移至「Ping 設定」區段。
   d. 選取「允許「Vulnerability Scanner」Ping 您網路中的電腦以檢查其狀態」。
   e. 在「封包大小」和「逾時」欄位中，接受或修改預設值。
   f. 選取「使用 ICMP OS 特徵鑑別偵測作業系統類型」。
      如果選取此選項，Vulnerability Scanner 會判斷主機是執行 Windows 或其他作業系統。如果主機執行 Windows，Vulnerability Scanner 可以識別其 Windows 版本。
   g. 按一下「確定」。
      會關閉「設定」畫面。
2. 如果要設定 Vulnerability Scanner 同時 Ping 的電腦數量：

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

b. 變更 EchoNum 的值。請指定介於 1 和 64 之間的值。

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

c. 儲存 TMVS.ini。

OfficeScan 伺服器設定

在下列情況中，會使用 OfficeScan 伺服器設定：

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

  注意

  特定情況可能會造成無法在目標主機上 OfficeScan 用戶端。如需詳細資訊，請參閱使用 Vulnerability Scanner 安裝 OfficeScan 用戶端的指導方針 第 5-38 頁。

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

配置 OfficeScan 伺服器設定

OfficeScan 伺服器設定是弱點掃瞄設定的子集合。如需有關弱點掃瞄設定的詳細資訊，請參閱弱點掃瞄方法 第 5-39 頁。

程序

1. 啟動 TMVS.exe。
2. 按一下「設定」。

   會出現「設定」畫面。

3. 移至「OfficeScan 伺服器設定」區段。

4. 輸入 OfficeScan 伺服器名稱和通訊埠號碼。
5. 選取「在未受保護的電腦上自動安裝 OfficeScan 用戶端」。
6. 如果要設定系統管理認證：
   a. 按一下「安裝至帳號」。
   b. 在「帳號資訊」畫面中，輸入使用者名稱和密碼。
   c. 按一下「確定」。
7. 選取「將記錄檔傳送至 OfficeScan 伺服器」。
8. 按一下「確定」。

   會關閉「設定」畫面。

以安全性符合進行安裝

將 OfficeScan 用戶端安裝到網路網域中的電腦，或使用電腦的 IP 位址將 OfficeScan 用戶端安裝到目標電腦。

在安裝 OfficeScan 用戶端之前，請注意下列事項：

程序

1. 記錄每部電腦的登入憑證。在安裝期間，OfficeScan 會提示您指定登入憑證。
2. 在下列情況中，無法在電腦上安裝 OfficeScan 用戶端：
   - 電腦上已安裝 OfficeScan 伺服器。
   - 電腦執行的是 Windows XP Home、Windows Vista Home Basic、Windows Vista Home Premium、Windows 7™ Starter、Windows 7 Home Basic、Windows 7 Home Premium 和 Windows 8（Basic 版本）。如果您的電腦執行這些平台，請選擇另一種安裝方法。如需詳細資訊，請參閱部署考量 第 5-10 頁。

3. 如果目標電腦執行的是 Windows Vista（Business、Enterprise 或 Ultimate Edition）、Windows 7（Professional、Enterprise 或 Ultimate Edition）、Windows 8（Pro、Enterprise）或 Windows Server 2012 (Standard)，請在電腦上執行下列步驟：

   a. 開啟一個內建的管理者帳號，並為這個帳號設定密碼。

   b. 關閉 Windows 防火牆。

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

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

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

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

   - `tmuninst.ptn`
   - `tmuninst_as.ptn`

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

安裝 OfficeScan 用戶端

程序

1. 瀏覽至「安全性符合 > 外部伺服器管理」。
2. 按一下用戶端樹狀結構頂端的「安裝」。

- 如果電腦上已安裝舊版 OfficeScan 用戶端，而您按一下「安裝」，將會略過安裝，而且用戶端不會升級至此版本。如果要升級用戶端，必須關閉一個設定。

  a. 移至「用戶端電腦 > 用戶端管理」。

  b. 按一下「設定 > 權限和其他設定 > 其他設定」標籤。

  c. 關閉「用戶端可更新元件，但不升級用戶端程式或部署 HotFix」選項。

3. 為每部電腦指定管理員登入帳號，然後按一下「登入」。OfficeScan 會開始在目標電腦上安裝用戶端。

4. 檢視安裝狀態。

移轉至 OfficeScan 用戶端

將目標電腦上安裝的用戶端安全防護軟體取代為 OfficeScan 用戶端。

從其他端點安全防護軟體移轉

安裝 OfficeScan 用戶端時，安裝程式會檢查目標電腦上是否已安裝趨勢科技或協力廠商端點安全防護軟體。安裝程式可以自動解除安裝該軟體，並使用 OfficeScan 用戶端來取代它。

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

- tmuninst.ptn
- tmuninst_as.ptn

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

OfficeScan 用戶端移轉問題

- 如果成功自動移轉用戶端，但使用者在安裝後立即遇到 OfficeScan 用戶端的問題，請重新啟動電腦。
- 如果 OfficeScan 安裝程式繼續安裝 OfficeScan 用戶端，但無法解除安裝其他安全防護軟體，則兩個軟體之間會發生衝突。請解除安裝這兩個軟體，然後使用部署考量 第 5-10 頁中討論的任一安裝方法來安裝 OfficeScan 用戶端。

從 ServerProtect 一般伺服器移轉

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

「ServerProtect 一般伺服器移轉工具」的硬體和軟體規格與 OfficeScan 伺服器相同。請在執行 Windows Server 2003 或 Windows Server 2008 的電腦上執行此工具。

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

安裝 OfficeScan 用戶端時，移轉工具用戶端安裝程式有時可能會逾時並通知您安裝不成功。不過，OfficeScan 用戶端可能已成功安裝。請從 OfficeScan Web 主控台驗證用戶端電腦的安裝是否成功。

在下列情況下無法成功移轉：

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

注意

「ServerProtect 一般伺服器移轉工具」不會解除安裝 ServerProtect 的 Control Manager™ 代理程式。如需如何解除安裝該代理程式的指示，請參閱 ServerProtect 和（或）Control Manager 文件。

使用 ServerProtect 一般伺服器移轉工具

程序

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

2. 按兩下 SPNSXfr.exe 以開啟此工具。

   便會開啟「Server Protect 一般伺服器移轉工具」主控台。

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

4. 選取執行「ServerProtect 一般伺服器」的電腦以在該電腦上執行移轉，其方式是按一下「目標電腦」下的任一選項：

   - Windows 網路樹狀結構：顯示網路上的網域樹狀結構。如果要使用此方法選取電腦，請按一下要在其中搜尋用戶端電腦的網域。
   - 資料伺服器名稱：依「資訊伺服器」名稱搜尋。如果要使用此方法選取電腦，請在文字方塊中輸入網路上的「資料伺服器」名稱。如果要搜尋多部「資料伺服器」，請在伺服器名稱之間插入分號（「;」）。
   - 特定的一般伺服器名稱：依「一般伺服器」名稱搜尋。如果要使用此方法選取電腦，請在文字方塊中輸入網路上的「一般伺服器」名稱。如果要搜尋多部「一般伺服器」，請在伺服器名稱之間輸入分號（「;」）。

- IP 範圍搜尋：依 IP 位址範圍搜尋。如果要使用此方法選取電腦，請在「IP 範圍」下輸入類別 B 的 IP 位址。

注意

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

5. 選取「安裝後重新啟動」，以便在移轉後自動重新啟動目標電腦。

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

6. 按一下「搜尋」。

   搜尋結果會顯示在「ServerProtect 一般伺服器」下。

7. 請按一下要執行移轉的電腦。

   a. 如果要選取所有電腦，請按一下「全選」。

   b. 如果要清除所有電腦，請按一下「取消全選」。

   c. 如果要將清單匯出為逗號分隔值 (CSV) 檔案，請按一下「匯出到 CSV」。

8. 如果登入目標電腦時需要使用者名稱和密碼，請執行下列動作：

   a. 選取「使用群組帳號/密碼」核取方塊。

   b. 按一下「設定登入帳號」。

      會出現「輸入管理員資訊」視窗。

   c. 輸入使用者名稱和密碼。

      注意

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

   d. 按一下「確定」。

e. 按一下「如果登入不成功則再詢問一次」，在移轉程序期間若無法登入，可以再次輸入使用者名稱和密碼。

9. 按一下「移轉」。

10. 如果您不選取「安裝後重新啟動」選項，請重新啟動目標電腦以完成移轉。

安裝後

完成安裝後，請驗證下列項目：

- OfficeScan 用戶端捷徑 第 5-62 頁
- 程式清單 第 5-62 頁
- OfficeScan 用戶端服務 第 5-62 頁
- OfficeScan 用戶端安裝記錄檔 第 5-63 頁

OfficeScan 用戶端捷徑

用戶端電腦的 Windows「開始」功能表上出現趨勢科技 OfficeScan 用戶端捷徑。

圖 5-2. OfficeScan 用戶端捷徑

程式清單

OfficeScan 用戶端已列於用戶端電腦「控制台」的「新增/移除程式」清單。

OfficeScan 用戶端服務

Microsoft 管理主控台已顯示下列 OfficeScan 用戶端服務：

- OfficeScan NT 監聽程式 (`TmListen.exe`)
- OfficeScan NT 即時掃瞄 (`NTRtScan.exe`)
- OfficeScan NT Proxy 服務 (`TmProxy.exe`)

注意

OfficeScan NT Proxy 服務在 Windows 8 或 Windows Server 2012 平台上不存在。

- OfficeScan NT 防火牆 (`TmPfw.exe`)；如果在安裝期間已啟動防火牆
- 趨勢科技未經授權的變更阻止服務 (`TMBMSRV.exe`)

OfficeScan 用戶端安裝記錄檔

OfficeScan 用戶端安裝記錄檔 `OFCNT.LOG` 位於下列位置：

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

建議的安裝後工作

趨勢科技建議您執行下列安裝後工作。

元件更新

更新 OfficeScan 用戶端元件，以確保用戶端擁有最新的安全威脅防護。您可以從 Web 主控台執行手動用戶端更新，或指示使用者從其電腦執行「立即更新」。

使用 EICAR 測試程式檔來測試掃瞄

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

http://www.eicar.org

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

警告!

請勿使用真的病毒測試防毒產品。

執行測試掃瞄

程序

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

秘訣

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

解除安裝 OfficeScan 用戶端

有兩種方式可以從電腦解除安裝 OfficeScan 用戶端：

- 從 Web 主控台解除安裝 OfficeScan 用戶端 第 5-65 頁
- 執行 OfficeScan 用戶端解除安裝程式 第 5-66 頁

如果 OfficeScan 用戶端也安裝了 Cisco Trust Agent (CTA)，解除安裝 OfficeScan 用戶端程式不一定會移除該代理程式。這取決於您部署該代理程式時所進行的設定。如需詳細資訊，請參閱 Cisco Trust Agent 部署 第 16-25 頁。

如果 Cisco Trust Agent 在您解除安裝 OfficeScan 用戶端之後存在，請從「新增/移除程式」畫面手動將它移除。

如果無法使用上述方法解除安裝 OfficeScan 用戶端，請手動解除安裝 OfficeScan 用戶端。如需詳細資訊，請參閱手動解除安裝 OfficeScan 用戶端 第 5-67 頁。

從 Web 主控台解除安裝 OfficeScan 用戶端

從 Web 主控台解除安裝 OfficeScan 用戶端程式。請只有在程式發生問題時才執行解除安裝，但之後要立即重新安裝，以讓電腦能夠持續防禦安全威脅。

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「工作 > 用戶端解除安裝」。
4. 在「用戶端解除安裝」畫面中，按一下「開始解除安裝」。伺服器便會傳送通知給用戶端。
5. 檢查通知狀態並檢查是否有用戶端未收到通知。
   a. 依序按下「選取未通知的電腦」和「開始解除安裝」，立即重新傳送通知給未通知的用戶端。
   b. 按一下「停止解除安裝」提示 OfficeScan 停止通知目前要通知的用戶端。已通知並執行解除安裝的用戶端將會略過這個命令。

OfficeScan 用戶端解除安裝程式

授與使用者解除安裝 OfficeScan 用戶端程式的權限，然後指示他們從其電腦上執行用戶端解除安裝程式。

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

授與 OfficeScan 用戶端解除安裝權限

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 權限和其他設定」。
4. 在「權限」標籤上，移至「解除安裝」區段。
5. 如果要允許不需密碼就可解除安裝，請選取「允許使用者解除安裝 OfficeScan 用戶端」。如果要求必須輸入密碼，請選取「使用者需要密碼才能解除安裝 OfficeScan 用戶端」，然後輸入密碼並確認。
6. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

執行 OfficeScan 用戶端解除安裝程式

程序

1. 在 Windows「開始」功能表上，按一下「程式集 > 趨勢科技 OfficeScan 用戶端 > 解除安裝 OfficeScan 用戶端」。

您也可以執行下列步驟：

a. 按一下「控制台 > 新增或移除程式」。

b. 尋找「趨勢科技 OfficeScan 用戶端」，然後按一下「變更」。

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。OfficeScan 會通知使用者解除安裝的進度以及完成結果。使用者不需重新啟動用戶端電腦就能完成解除安裝。

手動解除安裝 OfficeScan 用戶端

只有在發生下列情況時才手動執行解除安裝：從 Web 主控台解除安裝 OfficeScan 用戶端發生問題，或執行解除安裝程式後發生問題。

程序

1. 使用具有管理員權限的帳號登入用戶端電腦。
2. 以滑鼠右鍵按一下系統匣上的 OfficeScan 用戶端圖示，然後選取「卸載 OfficeScan」。如果系統提示您輸入密碼，請指定卸載密碼，然後按一下「確定」。

注意

- 對於 Windows 8 和 Windows Server 2012，請切換至桌面模式以卸載 OfficeScan 用戶端。
- 請關閉將卸載 OfficeScan 用戶端的電腦上的密碼。如需詳細資訊，請參閱設定用戶端權限及其他設定 第 14-78 頁。

3. 如果未指定卸載密碼，請從 Microsoft 管理主控台停止下列服務：
   - OfficeScan NT 監聽程式
   - OfficeScan NT 防火牆
   - OfficeScan NT 即時掃瞄

- OfficeScan NT Proxy 服務

  注意

  OfficeScan NT Proxy 服務在 Windows 8 或 Windows Server 2012 平台上不存在。

- 趨勢科技未經授權的變更阻止服務

4. 從「開始」功能表中移除 OfficeScan 用戶端捷徑。

   - 在 Windows 8 和 Windows Server 2012 上：

     a. 切換至桌面模式。

     b. 將滑鼠游標移至畫面的右下角，並從出現的功能表中按一下「開始」。

        會出現「首頁」畫面。

     c. 以滑鼠右鍵按一下「趨勢科技 OfficeScan」。

     d. 按一下「從開始功能表取消釘選」。

   - 在所有其他的 Windows 平台上：

     按一下「開始 > 程式集」，以滑鼠右鍵按一下「趨勢科技 OfficeScan 用戶端」，然後按一下「刪除」。

5. 開啟「登錄編輯程式」(`regedit.exe`)。

   警告!

   下列步驟需要您刪除登錄機碼。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」。

6. 刪除下列登錄機碼：

   - 如果電腦沒有安裝其他趨勢科技產品：

     - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro`

       適用於 64 位元電腦：

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro

- 如果電腦上已安裝其他趨勢科技產品，請您只刪除下列機碼：
  - HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC
  - HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfcWatchDog

    適用於 64 位元電腦：

    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\OfcWatchDog
  - HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp

    適用於 64 位元電腦：

    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\PC-cillinNTCorp

7. 刪除下列登錄機碼/值：
   - 適用於 32 位元系統：
     - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\OfficeScanNT
     - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 下的 OfficeScanNT 監視器 (REG_SZ)
   - 適用於 64 位元系統：
     - HKEY_LOCAL_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\OfficeScanNT
     - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run 下的 OfficeScanNT 監視器 (REG_SZ)
8. 刪除下列位置的所有下列登錄機碼實體：
   - 位置：
     - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

- `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services`
- `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services`
- `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services`

- 機碼：
  - NTRtScan
  - tmcfw
  - tmcomm
  - TmFilter
  - TmListen
  - tmpfw
  - TmPreFilter
  - TmProxy

    注意

    TmProxy 在 Windows 8 或 Windows Server 2012 平台上不存在。

  - tmtdi

    注意

    tmtdi 在 Windows 8 或 Windows Server 2012 平台上不存在。

  - VSApiNt
  - tmlwf（適用於 Windows Vista/Server 2008/7/8/Server 2012 電腦）
  - tmwfp（適用於 Windows Vista/Server 2008/7/8/Server 2012 電腦）
  - tmactmon
  - TMBMServer
  - TMebc

- tmevtmgr
- tmeevw（適用於 Windows 8/Server 2012）
- tmusa（適用於 Windows 8/Server 2012）

9. 關閉「登錄編輯程式」。
10. 按一下「開始 > 設定 > 控制台」，然後按兩下「系統」。

注意
對於 Windows 8 和 Windows Server 2012 系統，請略過此步驟。

11. 按一下「硬體」標籤，然後按一下「裝置管理員」。

注意
對於 Windows 8 和 Windows Server 2012 系統，請略過此步驟。

12. 按一下「檢視 > 顯示隱藏裝置」。

注意
對於 Windows 8 和 Windows Server 2012 系統，請略過此步驟。

13. 展開「非隨插即用驅動程式」，然後解除安裝下列裝置（適用於 Windows XP/Vista/7/Server 2003/Server 2008）：

- tmcomm
- tmactmon
- tmevtmgr
- Trend Micro Filter
- Trend Micro PreFilter
- Trend Micro TDI Driver
- Trend Micro VSAPI NT
- 趨勢科技未經授權的變更阻止服務

- Trend Micro WFP Callout Driver (適用於 Windows Vista/Server 2008/7 電腦)

14. 使用命令列編輯器，利用下列命令手動刪除趨勢科技驅動程式（僅限 Windows 8/Server 2012）：

    - `sc delete tmcomm`
    - `sc delete tmactmon`
    - `sc delete tmevtmgr`
    - `sc delete tmfilter`
    - `sc delete tmprefilter`
    - `sc delete tmwfp`
    - `sc delete vsapint`
    - `sc delete tmeevw`
    - `sc delete tmusa`
    - `sc delete tmebc`

    注意

    請使用管理員權限執行命令列編輯器（例如，以滑鼠右鍵按一下 `cmd.exe`，然後按一下「以系統管理員身分執行」），以確保命令成功執行。

15. 解除安裝「一般防火牆驅動程式」。

    a. 以滑鼠右鍵按一下「網路上的芳鄰」，然後按一下「內容」。

    b. 以滑鼠右鍵按一下「區域連線」，然後按一下「內容」。

    c. 在「一般」標籤上，選取「趨勢科技的一般防火牆驅動程式」，然後按一下「解除安裝」。

    注意

    下列步驟僅適用於 Windows Vista/Server 2008/7/8/Server 2012 作業系統。使用其他作業系統的用戶端請跳至步驟 15。

d. 以滑鼠右鍵按一下「網路」，然後按一下「內容」。

e. 按一下「管理網路連線」。

f. 以滑鼠右鍵按一下「區域連線」，然後按一下「內容」。

g. 在「網路功能」標籤上，選取「趨勢科技 NDIS 6.0 過濾器驅動程式」，然後按一下「解除安裝」。

16. 重新啟動用戶端電腦。

17. 如果電腦上沒有安裝其他趨勢科技產品，請刪除 `Trend Micro` 安裝資料夾（通常是 `C:\Program Files\Trend Micro`）。若是 64 位元電腦，您可以在 `C:\Program Files (x86)\Trend Micro` 下找到安裝資料夾。

18. 如果已安裝其他趨勢科技產品，請刪除下列資料夾：

    - <用戶端安裝資料夾>
    - 趨勢科技安裝資料夾下的 `BM` 資料夾（通常是 32 位元系統的 `C:\Program Files\Trend Micro\BM` 和 64 位元系統的 `C:\Program Files (x86)\Trend Micro\BM`）。

第 6 章

維持最新的防護

本章說明趨勢科技™OfficeScan™ 元件和更新程序。

本章內容：

OfficeScan 元件和程式

OfficeScan 使用元件和程式來保護用戶端電腦免於遭受最新的安全威脅。請透過執行手動或預約更新，將這些元件和程式維持在最新狀態。

除了元件之外，OfficeScan 用戶端還會從 OfficeScan 伺服器接收更新的組態設定檔案。用戶端需要這個組態設定檔案以套用新的設定。每一次您經由 Web 主控台修改 OfficeScan 設定時，組態設定檔案都會變更。

元件分為下列幾種類別：

防毒元件

防毒元件包含下列病毒碼、驅動程式及引擎：

病毒碼

用戶端電腦可用的病毒碼取決於用戶端使用的掃瞄方式。如需有關掃瞄方法的資訊，請參閱掃瞄方法 第 7-6 頁。

表 6-1. 病毒碼

掃瞄方法	使用中的病毒碼
標準掃瞄	病毒碼包含一些資訊，可協助 OfficeScan 識別最新的病毒/惡意程式和混合式安全威脅攻擊。趨勢科技每週會多次建立和發行新版本的「病毒碼」，並且在發現破壞力特別大的病毒/惡意程式後，隨時建立和發行病毒碼。 趨勢科技建議至少每小時預約自動更新，這是所有已交付產品的預設設定。
雲端截毒掃瞄	使用雲端截毒掃瞄模式時，OfficeScan 用戶端會使用兩個共同運作的小型病毒碼，提供與標準惡意程式防護病毒碼和間諜程式防護病毒碼相同的防護。 主動式雲端截毒技術來源會裝載雲端病毒碼」。此病毒碼每小時會更新一次，而且包含大多數病毒碼定義。雲端掃瞄用戶端不會下載此病毒碼。用戶端會將掃瞄查詢傳送至主動式雲端截毒技術伺服器來源，並與病毒碼比對來確認潛在的安全威脅。 用戶端更新來源（OfficeScan 伺服器或自訂更新來源）會裝載「本機雲端病毒碼」。此病毒碼會每日更新，而且包含「雲端病毒碼」中未包含的所有其他病毒碼定義。用戶端會使用與下載其他 OfficeScan 元件相同的方式，從更新來源下載此病毒碼。 如需雲端病毒碼和本機雲端病毒碼的詳細資訊，請參閱雲端防護病毒碼檔案 第 4-7 頁。

病毒掃瞄引擎

所有趨勢科技產品的核心都是掃瞄引擎，掃瞄引擎最早是開發來處理早期檔案型電腦病毒。現在的掃瞄引擎則非常複雜，而且可以偵測不同類型的病毒和惡意程式 第 7-2 頁。掃瞄引擎也可以偵測開發用於研究的受控制病毒。

掃瞄引擎會使用病毒碼檔案來識別下列情形，而非逐一掃瞄每個檔案中的每個位元組：

- 病毒碼的明顯特性
- 檔案中隱藏病毒的確切位置

OfficeScan 一偵測到病毒/惡意程式即加以移除，並恢復檔案的完整性。

更新掃瞄引擎

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

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

病毒掃瞄驅動程式

「病毒掃瞄驅動程式」會監控使用者操作檔案的情形。操作包括開啟或關閉檔案，以及執行應用程式。此驅動程式有兩個版本。即 `TmXPFlt.sys` 和 `TmPreFlt.sys`。`TmXPFlt.sys` 用於病毒掃瞄引擎的即時組態設定，`TmPreFlt.sys` 用於監控使用者作業。

注意

此元件不會在主控台上顯示。如果要檢查其版本，請瀏覽至 <伺服器安裝資料夾>\PCCSRV\Pccnt\Drv。以滑鼠右鍵按一下 .sys 檔案，選取「內容」，再移至「版本」標籤。

IntelliTrap 病毒碼

IntelliTrap 病毒碼 (如需詳細資訊，請參閱 IntelliTrap 第 D-6 頁)。「 病毒碼」可偵測包裝為可執行檔的即時壓縮檔。

IntelliTrap 例外病毒碼

IntelliTrap 例外病毒碼包含「許可的」壓縮檔清單。

損害清除及復原服務元件

損害清除及復原服務元件包含下列引擎和範本。

- 病毒清除引擎 第 6-5 頁
- 病毒清除範本 第 6-5 頁

病毒清除引擎

「病毒清除引擎」可掃瞄並移除特洛伊木馬程式和特洛伊木馬程式程序。此引擎支援 32 位元和 64 位元平台。

病毒清除範本

「病毒清除引擎」會使用「病毒清除範本」來識別特洛伊木馬程式檔案和程序，以便引擎可將它們清除。

間諜程式防護元件

間諜程式防護元件包含下列引擎和病毒碼：

- 間諜程式病毒碼 第 6-6 頁
- 間諜程式掃瞄引擎 第 6-6 頁
- 間諜程式主動式監控病毒碼 第 6-6 頁

間諜程式病毒碼

「間諜程式病毒碼」會識別檔案和程式、記憶體模組、Windows 登錄和 URL 捷徑中的間諜程式/可能的資安威脅程式。

間諜程式掃瞄引擎

「間諜程式掃瞄引擎」可掃瞄間諜程式/可能的資安威脅程式並執行適當的中毒處理行動。此引擎支援 32 位元和 64 位元平台。

間諜程式主動式監控病毒碼

「間諜程式主動式監控病毒碼」是用來執行即時間諜程式/可能的資安威脅程式掃瞄。只有標準用戶端會使用此病毒碼。

雲端掃瞄用戶端會使用「本機雲端病毒碼」來執行即時間諜程式/可能的資安威脅程式掃瞄。如果用戶端在掃瞄期間無法判斷掃瞄目標是否有風險，即會將掃瞄查詢傳送至主動式雲端截毒技術伺服器來源。

防火牆元件

防火牆元件包含下列驅動程式和病毒碼：

- 一般防火牆驅動程式 第 6-6 頁
- 一般防火牆病毒碼 第 6-7 頁

一般防火牆驅動程式

「一般防火牆驅動程式」是搭配「一般防火牆病毒碼」使用，可掃瞄用戶端電腦是否有網路病毒。此驅動程式支援 32 位元和 64 位元平台。

一般防火牆病毒碼

與「病毒碼」相同，「一般防火牆病毒碼」可協助 OfficeScan 識別病毒特徵，病毒特徵是指表明存在網路病毒的獨特位元和位元組病毒碼。

網頁信譽評等元件

網頁信譽評等元件為 URL 過濾引擎。

URL 過濾引擎

「URL 過濾引擎」可促進 OfficeScan 和趨勢科技「URL 過濾服務」之間的通訊。「URL 過濾服務」是一個將 URL 予以分級並提供分級資訊給 OfficeScan 的系統。

行為監控元件

行為監控元件包含下列病毒碼、驅動程式及服務：

- 行為監控偵測特徵碼 第 6-7 頁
- 行為監控驅動程式 第 6-8 頁
- 行為監控核心服務 第 6-8 頁
- 行為監控配置特徵碼 第 6-8 頁
- 數位簽章特徵碼 第 6-8 頁
- 策略實施特徵碼 第 6-8 頁

行為監控偵測特徵碼

此病毒碼包含偵測可疑安全威脅行為的規則。

行為監控驅動程式

此核心模式驅動程式可監控系統事件，並將它們傳遞到「行為監控核心服務」以便進行策略實施。

行為監控核心服務

此使用者模式服務具有下列功能：

- 提供 Rootkit 偵測
- 規範對於外部裝置的存取
- 保護檔案、登錄機碼和服務

行為監控配置特徵碼

「行為監控驅動程式」使用此特徵碼來識別正常系統事件，並將它們從策略實施排除。

數位簽章特徵碼

此特徵碼包含有效數位簽章清單，「行為監控核心服務」使用這些數位簽章來判斷負責系統事件的程式是否安全。

策略實施特徵碼

「行為監控核心服務」會根據此特徵碼中的策略檢查系統事件。

程式

OfficeScan 使用下列程式和產品更新：

- OfficeScan 用戶端程式 第 6-9 頁

- Cisco Trust Agent 第 6-9 頁
- HotFix、Patch 和 Service Pack 第 6-9 頁

OfficeScan 用戶端程式

OfficeScan 用戶端程式提供免於安全威脅的實際防護。

Cisco Trust Agent

Cisco Trust Agent 可讓用戶端和支援 Cisco NAC 的路由器彼此通訊。安裝策略伺服器 for Cisco NAC 之後，此代理程式才能運作。

HotFix、Patch 和 Service Pack

在產品正式發行之後，趨勢科技通常會開發下列項目來解決問題，以增強產品的效能或增加新功能：

- Hot Fix 第 D-5 頁
- Patch 第 D-9 頁
- 安全修補程式 第 D-10 頁
- Service Pack 第 D-11 頁

您的廠商或經銷商會在這些項目可供使用時聯絡您。如需有關新的 HotFix、Patch 和 Service Pack 發行的資訊，請造訪趨勢科技網站：

http://www.trendmicro.com/download/zh-tw/

所有發行都有 Readme 檔，其中包含安裝、部署和組態設定資訊。請詳細閱讀 Readme 檔再執行安裝。

HotFix 和 Patch 歷史記錄

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

用物流軟體（例如：Microsoft SMS、LANDesk™ 或 BigFix™）來查詢多部用戶端的此資訊。

注意

此功能不會記錄只部署到伺服器的 HotFix 和 Patch。

從 OfficeScan 8.0 Service Pack 1 Patch 3.1 開始提供此功能。

- 從 8.0 Service Pack 1 Patch 3.1 或更新版本升級的用戶端會記錄針對 8.0 及更新版本所安裝的 HotFix 和 Patch。
- 從 8.0 Service Pack 1 Patch 3.1 以前的版本升級的用戶端只會記錄針對 10.0 及更新版本所安裝的 HotFix 和 Patch。

資訊儲存在下列機碼中：

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

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

檢查下列機碼：

- 機碼：`HotFix_installed`

  類型：`REG_SZ`

  值：`<HotFix 或 Patch 名稱>`
- 機碼：`HotfixInstalledNum`

  類型：`DWORD`

  值：`<HotFix 或 Patch 號碼>`

更新總覽

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

注意

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

OfficeScan 伺服器和 OfficeScan 用戶端更新

OfficeScan 伺服器會下載用戶端所需的大部分元件。唯一不會下載的元件是雲端病毒碼，此元件會由主動式雲端截毒技術伺服器來源下載。

如果 OfficeScan 伺服器 管理大量用戶端，更新可能會耗用大量的伺服器電腦資源，進而影響伺服器的穩定性和效能。為了解決這個問題，OfficeScan 具有的「更新代理程式」功能可讓特定用戶端分擔分配更新檔到其他用戶端的工作。

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

表 6-2. 伺服器-用戶端更新選項

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

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

主動式雲端截毒技術來源更新

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

注意

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

下表說明主動式雲端截毒技術伺服器來源的更新程序。

表 6-3. 主動式雲端截毒技術來源更新程序

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

OfficeScan 伺服器更新

OfficeScan 伺服器會下載下列元件並部署到用戶端：

表 6-4. OfficeScan 伺服器所下載的元件

元件	分配	
	標準用戶端	雲端掃瞄用戶端
本機雲端病毒碼	否	是
病毒碼	是	否
病毒掃瞄引擎	是	是
病毒掃瞄驅動程式	是	是
IntelliTrap 病毒碼	是	是
IntelliTrap 例外病毒碼	是	是
病毒清除引擎	是	是
病毒清除範本	是	是

元件	分配	
	標準用戶端	雲端掃瞄用戶端
間諜程式病毒碼	是	是
間諜程式掃瞄引擎	是	是
間諜程式主動式監控病毒碼	是	否
一般防火牆驅動程式	是	是
一般防火牆病毒碼	是	是
URL 過濾引擎	是	是
行為監控驅動程式	是	是
行為監控核心服務	是	是
行為監控配置特徵碼	是	是
行為監控偵測特徵碼	是	是
數位簽章特徵碼	是	是
策略實施特徵碼	是	是

更新提醒和秘訣：

- 如果要允許伺服器將更新的元件部署到用戶端，請啟動自動用戶端更新。如需詳細資訊，請參閱 OfficeScan 用戶端自動更新 第 6-32 頁。如果關閉自動用戶端更新，則伺服器會下載更新檔，但不會將更新檔部署到用戶端。
- 純 IPv6 OfficeScan 伺服器無法直接將更新分發到純 IPv4 用戶端。同樣地，純 IPv4 OfficeScan 伺服器無法直接將更新分發到純 IPv6 用戶端。如果要允許 OfficeScan 伺服器將更新分發到用戶端，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。
- 趨勢科技會定期發行病毒碼檔案，讓您將用戶端防護保持在最新狀態。由於會定期提供病毒碼檔案更新，因此 OfficeScan 使用稱為「元件複製」的機制，讓您能夠更快下載病毒碼檔案。如需詳細資訊，請參閱 OfficeScan 伺服器元件複製 第 6-17 頁。

- 如果您使用 Proxy 伺服器連線到 Internet，必須使用正確的 Proxy 伺服器設定才能成功下載更新檔。
- 在 Web 主控台的「摘要」中，新增「用戶端更新」Widget 以檢視元件的目前版本，並確定具有更新元件和過期元件的用戶端數。

OfficeScan 伺服器更新來源

設定 OfficeScan 伺服器從趨勢科技主動式更新伺服器或其他來源下載元件。如果 OfficeScan 伺服器無法直接連線至主動式更新伺服器，您可以指定其他來源。如需狀況範例，請參閱隔離的 OfficeScan 伺服器更新 第 6-20 頁。

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

注意

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

對 OfficeScan 伺服器更新的 IPv6 支援

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

- 趨勢科技主動式更新伺服器
- Control Manager 5.5
- Control Manager 5.0

  注意

  Control Manager 自 5.5 SP1 版起才開始支援 IPv6。

- 任何純 IPv4 自訂更新來源

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

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

用於 OfficeScan 伺服器更新的 Proxy

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

設定 Proxy 設定

程序

1. 瀏覽到「管理 > Proxy 伺服器設定」。
2. 按一下「外部 Proxy 伺服器」標籤。
3. 移至「OfficeScan 伺服器電腦更新」區段。
4. 選取「使用 Proxy 伺服器進行病毒碼、引擎和使用授權更新」。
5. 指定 Proxy 伺服器通訊協定、伺服器名稱或 IPv4/IPv6 位址，以及通訊埠號碼。
6. 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。
7. 按一下「儲存」。

設定伺服器更新來源

程序

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

如果選擇主動式更新伺服器，請確定伺服器有 Internet 連線；如果使用 Proxy 伺服器，請測試是否可以使用 Proxy 伺服器設定建立 Internet 連線。如需詳細資訊，請參閱用於 OfficeScan 伺服器更新的 Proxy 第 6-16 頁。

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

注意

OfficeScan 伺服器在從更新來源下載元件時會使用元件複製。如需詳細資訊，請參閱OfficeScan 伺服器元件複製 第 6-17 頁。

3. 按一下「儲存」。

OfficeScan 伺服器元件複製

當趨勢科技主動式更新伺服器上有最新的完整病毒碼檔案可供下載時，也會同時提供 14 個「漸增式病毒碼」。漸增式病毒碼為完整病毒碼檔案的小型版本，僅提供最新版和之前完整病毒碼檔案版本之間的差異。例如，如果最新版為 175，則漸增式病毒碼 v_173.175 會包含 175 版中擁有，但舊版病毒碼 173 版中找不到的簽章（173 版是之前的完整病毒碼版本，病毒碼號碼是以 2 為遞增單位發行的。）漸增式病毒碼 v_171.175 則包含 175 版中擁有，但 171 中找不到的簽章。

為了減少下載最新病毒碼時產生的網路傳輸，OfficeScan 會執行元件複製，使用這種元件更新方式時，OfficeScan 伺服器或「更新代理程式」只會下載漸增式病毒碼。如需有關「更新代理程式」如何執行元件複製的資訊，請參閱更新代理程式元件複製 第 6-52 頁。

元件複製適用於下列元件：

- 病毒碼
- 本機雲端病毒碼
- 病毒清除範本
- IntelliTrap 例外病毒碼

- 間諜程式病毒碼
- 間諜程式主動式監控病毒碼

元件複製狀況

如果要瞭解伺服器的元件複製說明，請參閱下列狀況：

表 6-5. 伺服器元件複製狀況

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

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

   注意

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

   範例說明：

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

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

範例說明：

- 在伺服器上，OfficeScan 會合併 171 版與漸增式病毒碼 171.175，以產生 175 版。
- 伺服器有 1 個漸增式病毒碼 (171.175) 和最新的完整病毒碼（175 版）。

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

   範例說明：

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

     169.175, 167.175, 165.175, 163.175, 161.175, 159.175

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

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

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

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

   範例說明：

   - 主動式更新伺服器中有 14 個漸增式病毒碼：

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

   - OfficeScan 伺服器中有 7 個漸增式病毒碼：

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

   - OfficeScan 伺服器會下載額外 7 個漸增式病毒碼：

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

- 目前伺服器已擁有主動式更新伺服器上提供的所有漸增式病毒碼。

5. 最新的完整病毒碼和 14 個漸增式病毒碼都會提供給用戶端。

隔離的 OfficeScan 伺服器更新

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

本主題說明更新隔離的 OfficeScan 伺服器時所需執行的工作。

更新隔離的 OfficeScan 伺服器

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

程序

1. 識別更新來源，例如： Trend Micro Control Manager 或隨機主機。此更新來源必須有：

   - 可靠的 Internet 連線，以便可以從趨勢科技主動式更新伺服器下載最新元件。如果無法連接到 Internet，則更新來源只能自行從趨勢科技取得元件，再將元件複製到更新來源中。
   - 與 OfficeScan 伺服器之間的有效連線。如果 Proxy 伺服器介於 OfficeScan 伺服器和更新來源之間，請設定 Proxy 伺服器設定。如需詳細資訊，請參閱用於 OfficeScan 伺服器更新的 Proxy 第 6-16 頁。
   - 足夠的磁碟空間可用於儲存下載的元件

2. 使 OfficeScan 伺服器指向新的更新來源。如需詳細資訊，請參閱 OfficeScan 伺服器更新來源 第 6-15 頁。

3. 識別伺服器部署到用戶端的元件。如需可部署元件的清單，請參閱 OfficeScan 用戶端更新 第 6-24 頁。

秘訣

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

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

5. 在更新來源：

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

   b. 下載以下項目：

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

   c. 將下載的項目儲存到更新來源的某個目錄中。

6. 執行 OfficeScan 伺服器的手動更新。如需詳細資訊，請參閱手動更新 OfficeScan 伺服器 第 6-22 頁。

7. 每次需要更新元件時，請重複步驟 5 至步驟 6。

OfficeScan 伺服器更新方法

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

如果要允許伺服器將更新的元件部署到用戶端，請啟動自動用戶端更新。如需詳細資訊，請參閱 OfficeScan 用戶端自動更新 第 6-32 頁。如果關閉自動用戶端更新，則伺服器會下載更新檔，但不會將更新檔部署到用戶端。

更新方法包括：

- 手動伺服器更新：當更新很重要時，請執行手動更新，讓伺服器可以立即取得更新檔。如需詳細資訊，請參閱手動更新 OfficeScan 伺服器 第 6-22 頁。

- 預約伺服器更新：OfficeScan 伺服器會在預約日期和時間連線到更新來源，以取得最新元件。如需詳細資訊，請參閱 OfficeScan 伺服器的預約更新 第 6-22 頁。

手動更新 OfficeScan 伺服器

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

程序

1. 執行手動更新：
   - 瀏覽至「更新 > 伺服器 > 手動更新」。
   - 按一下「立即更新伺服器」 Web 主控台的主功能表。
2. 選取要更新的元件。
3. 按一下「更新」。

   伺服器會下載經過更新的元件。

OfficeScan 伺服器的預約更新

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

程序

1. 瀏覽至「更新 > 伺服器 > 預約更新」。
2. 選取「啟動 OfficeScan 伺服器 的預約更新」。
3. 選取要更新的元件。
4. 指定更新預約時程。

如果是每日、每週和每月更新，則期間是指 OfficeScan 會執行更新的時數。OfficeScan 會在此期間內的任何特定時間更新。

5. 按一下「儲存」。

OfficeScan 伺服器更新記錄檔

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

如果要避免記錄檔佔去過多硬碟空間，請手動刪除記錄檔或設定記錄檔刪除預約時程。如需有關管理記錄檔的詳細資訊，請參閱記錄檔管理 第 13-31 頁。

檢視更新記錄檔

程序

1. 瀏覽至「記錄檔 > 伺服器更新記錄檔」。
2. 檢查「結果」欄位，查看是否有未更新的元件。
3. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請按一下「匯出到 CSV」。開啟檔案或將其儲存至特定位置。

整合式主動式雲端截毒技術伺服器更新

整合式主動式雲端截毒技術伺服器會下載兩個元件，即雲端病毒碼和網頁封鎖清單。如需有關這些元件及如何更新它們的詳細資訊，請參閱整合式主動式雲端截毒技術伺服器管理 第 4-17 頁。

OfficeScan 用戶端更新

為確保用戶端免受最新安全威脅，請定期更新用戶端元件。

更新用戶端之前，請檢查其更新來源（OfficeScan 伺服器或自訂更新來源）是否具有最新的元件。如需有關如何更新 OfficeScan 伺服器的詳細資訊，請參閱OfficeScan 伺服器更新 第 6-13 頁。

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

表 6-6. 部署到用戶端的 OfficeScan 元件

元件	分配	
	標準用戶端	雲端掃瞄用戶端
本機雲端病毒碼	否	是
病毒碼	是	否
病毒掃瞄引擎	是	是
病毒掃瞄驅動程式	是	是
IntelliTrap 病毒碼	是	是
IntelliTrap 例外病毒碼	是	是
病毒清除引擎	是	是
病毒清除範本	是	是
間諜程式病毒碼	是	是
間諜程式掃瞄引擎	是	是
間諜程式主動式監控病毒碼	是	否
一般防火牆驅動程式	是	是
一般防火牆病毒碼	是	是
URL 過濾引擎	是	是

元件	分配	
	標準用戶端	雲端掃瞄用戶端
行為監控驅動程式	是	是
行為監控核心服務	是	是
行為監控配置特徵碼	是	是
行為監控偵測特徵碼	是	是
數位簽章特徵碼	是	是
策略實施特徵碼	是	是

OfficeScan 用戶端更新來源

用戶端可以從標準更新來源（OfficeScan 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OfficeScan 用戶端的標準更新來源 第 6-26 頁和OfficeScan 用戶端的自訂更新來源 第 6-27 頁。

對 OfficeScan 用戶端更新的 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 OfficeScan 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 OfficeScan 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）。

OfficeScan 用戶端的標準更新來源

OfficeScan 伺服器是用戶端的標準更新來源。

如果無法存取 OfficeScan 伺服器，用戶端就沒有備份來源，並因而會過期。如果要更新無法存取 OfficeScan 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）會決定是否可以與 OfficeScan 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 OfficeScan 用戶端更新的 IPv6 支援 第 6-25 頁。

配置 OfficeScan 用戶端的標準更新來源

程序

1. 瀏覽至「更新 > 用戶端電腦 > 更新來源」。
2. 選取「標準更新來源（從 OfficeScan 伺服器更新）」。
3. 按一下「通知所有用戶端」。

OfficeScan 用戶端更新程序

注意

本主題討論 OfficeScan 用戶端的更新程序。更新代理程式的更新程序將在OfficeScan 用戶端的標準更新來源 第 6-26 頁中討論。

如果設定 OfficeScan 用戶端直接從 OfficeScan 伺服器更新，則更新程序的執行方式如下：

1. OfficeScan 用戶端會從 OfficeScan 伺服器取得更新檔。
2. 無法從 OfficeScan 伺服器更新時，如果在「用戶端電腦 > 用戶端管理」中啟動了「用戶端從趨勢科技主動式更新伺服器下載更新程式」選項，請按一下「設定 > 權限和其他設定 > 其他設定 > 更新設定」，OfficeScan 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

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 OfficeScan 伺服器或更新代理程式下載。您可以設定 OfficeScan 用戶端僅從主動式更新伺服器下載病毒碼檔案以加速更新程序。如需詳細資訊，請參閱作為 OfficeScan 用戶端更新來源的主動式更新伺服器 第 6-30 頁。

OfficeScan 用戶端的自訂更新來源

OfficeScan 用戶端除了從 OfficeScan 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 OfficeScan 伺服器的 OfficeScan 用戶端更新傳輸，並允許無法連線至 OfficeScan 伺服器的 OfficeScan 用戶端取得即時更新。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 OfficeScan 用戶端做為更新代理程式，然後將它們新增到此清單。

配置 OfficeScan 用戶端的自訂更新來源

程序

1. 瀏覽至「更新 > 用戶端電腦 > 更新來源」。
2. 選取「自訂更新來源」，然後按一下「新增」。

3. 在顯示的畫面中，指定用戶端的 IP 位址。您可以輸入 IPv4 範圍和/或 IPv6 字首和長度。

4. 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。

注意

請確定 OfficeScan 用戶端可使用其 IP 位址連線到更新來源。例如，如果指定 IPv4 位址範圍，則更新來源必須具有 IPv4 位址。如果指定 IPv6 字首和長度，則更新來源必須具有 IPv6 位址。如需有關用戶端更新的 IPv6 支援的詳細資訊，請參閱 OfficeScan 用戶端更新來源 第 6-25 頁。

---

5. 按一下「儲存」。

6. 在畫面中執行其他工作。

   a. 選取以下任何設定。如需有關這些設定如何運作的詳細資訊，請參閱 OfficeScan 用戶端更新程序 第 6-26 頁。

      - 「更新代理程式」只會從 OfficeScan 伺服器更新元件、網域設定，以及用戶端程式與 HotFix
      - 所有自訂來源都無法使用或找不到時，會從 OfficeScan 伺服器更新元件
      - 所有自訂來源都無法使用或找不到時，會從 OfficeScan 伺服器更新網域設定
      - 所有自訂來源都無法使用或找不到時，會從 OfficeScan 伺服器更新用戶端程式和 HotFix

   b. 如果至少指定了一個更新代理程式作為來源，請按一下「更新代理程式分析報告」產生一份報告，反白顯示用戶端的更新狀態。如需有關此報告的詳細資訊，請參閱更新代理程式分析報告 第 6-53 頁。

   c. 按一下 IP 範圍連結編輯更新來源。在顯示的畫面中修改設定，然後按一下「儲存」。

   d. 選取核取方塊並按一下「刪除」，以移除清單中的更新來源。

   e. 如果要移動更新來源，請按一下向上或向下箭號。您一次只能移動一個來源。

7. 按一下「通知所有用戶端」。

OfficeScan 用戶端更新程序

注意

本主題討論 OfficeScan 用戶端的更新程序。更新代理程式的更新程序將在更新代理程式的自訂更新來源 第 6-49 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. OfficeScan 用戶端會從清單上的第一個來源更新。
2. 如果 OfficeScan 用戶端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 OfficeScan 用戶端將檢查「更新來源」畫面上的以下設定：

表 6-7. 自訂更新來源的其他設定

設定	說明
「更新代理程式」只會從 OfficeScan 伺服器更新元件、網域設定，以及用戶端程式與 HotFix	如果已啟動設定，會直接從 OfficeScan 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一般用戶端所設定的自訂更新來源設定。

設定	說明
所有自訂來源都無法使用或找不到時，用戶端會從 OfficeScan 伺服器更新下列項目: 元件	如果啟動該設定，則用戶端會從 OfficeScan 伺服器更新元件。 如果已關閉此選項，而且下列任一條件成立，則用戶端會嘗試直接連線到趨勢科技主動式更新伺服器： • 在「用戶端電腦 > 用戶端管理」中，按一下「設定 > 權限和其他設定 > 其他設定 > 更新設定，「用戶端從趨勢科技主動式更新伺服器下載更新程式」選項即會啟動。 • 主動式更新伺服器不包含在「自訂更新來源清單」中。 注意 只能從主動式更新伺服器更新元件。網域設定、程式和 HotFix 只能從該 OfficeScan 伺服器或更新代理程式下載。你可以設定用戶端僅從主動式更新伺服器下載病毒碼檔案以加速更新程序。如需詳細資訊，請參閱作為 OfficeScan 用戶端更新來源的主動式更新伺服器 第 6-30 頁。
所有自訂來源都無法使用或找不到時，用戶端會從 OfficeScan 伺服器更新下列項目: 網域設定	如果啟動該設定，則用戶端會從 OfficeScan 伺服器網域層級的設定。
所有自訂來源都無法使用或找不到時，用戶端會從 OfficeScan 伺服器更新下列項目: 用戶端程式和 HotFix	如果啟動該設定，則用戶端會從 OfficeScan 伺服器更新程式和 Hotfix。

4. 如果無法從所有可能的來源更新，則用戶端會結束更新程序。

作為 OfficeScan 用戶端更新來源的主動式更新伺服器

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

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

您無法直接從趨勢科技主動式更新伺服器更新純 IPv6 用戶端。如果要使雲端截毒掃瞄用戶端連線到來源，需要允許 OfficeScan 用戶端連線至主動式更新伺服器。

限制從主動式更新伺服器下載

程序

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

OfficeScan 用戶端更新方法

從 OfficeScan 伺服器或自訂更新來源更新元件的 OfficeScan 用戶端可以使用下列更新方法：

- 自動用戶端更新：當發生特定事件或到了預約的時間時，用戶端更新會自動執行。如需詳細資訊，請參閱 OfficeScan 用戶端自動更新 第 6-32 頁。
- 手動用戶端更新：當更新很重要時，請使用手動更新，以立即通知用戶端執行元件更新。如需詳細資訊，請參閱 OfficeScan 用戶端手動更新 第 6-37 頁。
- Privilege-based 更新：具有更新權限的使用者對於其電腦上的 OfficeScan 用戶端取得更新的方式有更大的掌控能力。如需詳細資訊，請參閱 OfficeScan 用戶端的更新權限和其他設定 第 6-39 頁。

OfficeScan 用戶端自動更新

自動更新可減輕通知所有用戶端進行更新的負擔，並消除用戶端電腦未擁有最新元件的風險。

除了元件之外，OfficeScan 用戶端也會在自動更新時，接收經過更新的組態設定檔案。用戶端需要這個組態設定檔案以套用新的設定。每一次您經由 Web 主控台修改 OfficeScan 設定時，組態設定檔案都會變更。如果要指定套用組態設定檔至用戶端的頻率，請參閱步驟 3 自動更新 OfficeScan 用戶端元件 第 6-34 頁。

注意

您可以設定讓用戶端在自動更新期間使用 Proxy 伺服器設定。如需詳細資訊，請參閱用於 OfficeScan 用戶端元件更新的 Proxy 第 6-42 頁。

自動更新有兩種類型：

- 事件觸發更新 第 6-32 頁
- 預約更新 第 6-33 頁

事件觸發更新

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

表 6-8. 事件觸發更新選項

選項	說明
在 OfficeScan 伺服器下載新元件之後，立即在用戶端開始元件更新	伺服器會在完成更新時立即通知用戶端執行更新。經常更新的用戶端只需要下載漸增式病毒碼，因此可縮短完成更新所需的時間（如需有關漸增式病毒碼的詳細資訊，請參閱 OfficeScan 伺服器元件複製 第 6-17 頁）。但是，經常更新可能會對伺服器效能造成負面影響，特別是當大量用戶端同時更新時。 如果有用戶端以行動模式執行，而且您也想要讓這些用戶端更新，請選取「包括行動和離線用戶端」。如需有關行動模式的詳細資訊，請參閱 OfficeScan 用戶端行動權限 第 14-18 頁。
當用戶端重新啟動並連線到 OfficeScan 伺服器時，讓用戶端開始元件更新（不包括行動用戶端）。	錯過更新的用戶端可在建立與伺服器之間的連線之後立即下載元件。如果用戶端離線或用戶端安裝所在電腦未開機並執行，用戶端可能會錯過更新。
更新後執行「立即掃瞄」（不包括行動用戶端）	伺服器會在事件觸發更新後通知用戶端執行掃瞄。如果特定更新是用於回應已在網路之間散播的安全威脅，請考慮啟動此選項。

注意

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

預約更新

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

注意

如果要搭配「網路位址轉譯」(Network Address Translation) 使用預約更新，請參閱使用 NAT 設定 OfficeScan 用戶端預約更新 第 6-35 頁。

自動更新 OfficeScan 用戶端元件

程序

1. 瀏覽至「更新 > 用戶端電腦 > 自動更新」。
2. 選取會觸發元件更新的事件。
   - 在 OfficeScan 伺服器下載新元件之後，立即在用戶端開始元件更新
   - 當用戶端重新啟動並連線到 OfficeScan 伺服器時，讓用戶端開始元件更新（不包括行動用戶端）。
   - 更新後執行「立即掃瞄」（不包括行動用戶端）
3. 選取擁有預約更新權限的用戶端執行預約更新的頻率。
   - 如果已授與用戶端預約更新權限，請繼續下一個步驟。
   - 如果尚未授與用戶端預約更新權限，請先執行下列步驟：

   a. 移至「用戶端電腦 > 用戶端管理」。

   b. 在用戶端樹狀結構中，選取希望具有該權限的用戶端。

   c. 按一下「設定 > 權限和其他設定」。
      - 選項 1：在「權限」標籤上，移至「元件更新權限」區段。您將會看到「啟動預約更新」選項。
      - 選項 2：在「其他設定」標籤上，移至「更新設定」區段。您將會看到另一個「啟動預約更新」選項。

注意

如果要授與用戶端使用者在 OfficeScan 用戶端主控台啟動或關閉預約更新的能力，請啟動選項 1 和選項 2。儲存設定之後，用戶端電腦將會依照預約時程執行更新。只有當用戶端使用者以滑鼠右鍵按一下系統匣上的 OfficeScan 用戶端圖示並選取「關閉預約更新」時，才會停止執行預約更新。

如果一律要執行預約更新並防止用戶端使用者關閉預約更新，請關閉選項 1 並啟動選項 2。

d. 儲存設定。

4. 設定預約時程。

a. 如果您選取「分鐘」或「小時」，可以選擇「每日僅更新一次用戶端組態設定」。如果您未選取這個選項，OfficeScan 用戶端會每隔一段指定時間就接收伺服器上提供的更新元件和任何經過更新的組態設定檔案。如果您選取這個選項，OfficeScan 每隔一段指定時間只會更新元件，而且一天更新組態設定檔案一次。

秘訣

趨勢科技經常更新元件，不過 OfficeScan 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 OfficeScan 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 OfficeScan 用戶端組態設定。

b. 如果您選取「每日一次」或「每週一次」，請指定更新時間和 OfficeScan 通知用戶端更新元件的時段。例如，如果開始時間為中午十二點且時段為兩小時，OfficeScan 會在中午十二點到下午二點之間隨機通知所有線上用戶端更新元件。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。

5. 按一下「儲存」。

離線用戶端將不通知。如果您選取「事件觸發更新」下的「當用戶端重新啟動並連線到 OfficeScan 伺服器時（不包括行動用戶端），讓用戶端開始元件更新」，時段過期後才上線的離線用戶端仍然可以更新元件。否則，這些用戶端會在下一次預約時程或您開始手動更新時更新元件。

使用 NAT 設定 OfficeScan 用戶端預約更新

如果區域網路使用 NAT，可能會發生下列問題：

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

如同以下所述，這些問題的暫行解決方法是使用預約更新方式將更新的元件和組態設定檔從伺服器部署至 OfficeScan 用戶端。

程序

- 在用戶端電腦上安裝 OfficeScan 用戶端之前：
  a. 在更新 > 用戶端電腦 > 自動更新的「預約更新」區段中設定用戶端預約更新。
  b. 在「用戶端電腦 > 用戶端管理」中，按一下「設定 > 權限和其他設定 > 權限（標籤） > 元件更新權限」，以授與用戶端啟動預約更新的權限。
- 如果 OfficeScan 用戶端已存在用戶端電腦上：
  a. 在「用戶端電腦 > 用戶端管理」中，按一下「設定 > 權限和其他設定 > 權限（標籤） > 元件更新權限」，以授與用戶端執行「立即更新」的權限。
  b. 指示使用者手動更新用戶端電腦上的元件（以滑鼠右鍵按一下系統匣中的 OfficeScan 用戶端圖示，然後按一下「立即更新」），以取得更新的組態設定。

OfficeScan 用戶端更新時，將會同時接收更新的元件和組態設定檔。

使用網域更新預約工具

在自動用戶端更新中已設定的更新預約時程僅適用於具有預約更新權限的用戶端。對於其他用戶端，可以設定單獨的更新預約時程。如果要執行此操作，您需要依照用戶端樹狀結構網域設定預約時程。屬於網域的全部用戶端都會套用此時程。

注意

無法為特定用戶端或特定子網域設定更新預約時程。全部子網域都會套用為其上層網域所設定的預約時程。

程序

1. 記錄用戶端樹狀結構網域名稱和更新預約時程。
2. 瀏覽到<伺服器安裝資料夾 第 xiii 頁 > `\PCCSRV\Admin\Utility\DomainScheduledUpdate`。
3. 將下列檔案複製到<伺服器安裝資料夾>`\PCCSRV`：
   - `DomainSetting.ini`
   - `dsu_convert.exe`
4. 使用文字編輯器（如記事本）開啟 `DomainSetting.ini`。
5. 指定用戶端樹狀結構網域，然後設定網域的更新預約時程。重複此步驟可新增更多網域。

   注意

   該 `ini` 檔案提供了詳細的組態設定指示。
6. 儲存 `DomainSetting.ini`。
7. 開啟命令提示字元，然後變更為 `PCCSRV` 資料夾的目錄。
8. 輸入以下命令並按 `Enter`。

   ```
   dsuconvert.exe DomainSetting.ini
   ```
9. 在 Web 主控台上，瀏覽至「用戶端電腦 > 全域用戶端設定」。
10. 按一下「儲存」。

OfficeScan 用戶端手動更新

在 OfficeScan 用戶端元件嚴重過期和病毒爆發時，手動更新 OfficeScan 用戶端元件。當 OfficeScan 用戶端長期無法從更新來源更新元件時，OfficeScan 用戶端元件便會嚴重過期。

除了元件之外，OfficeScan 用戶端也會在手動更新時，自動接收經過更新的組態設定檔案。OfficeScan 用戶端需要這個組態設定檔案以套用新的設定。每一次您經由 Web 主控台修改 OfficeScan 設定時，組態設定檔案都會變更。

注意

除了起始手動更新外，您還可以授與使用者執行手動更新（在 OfficeScan 用戶端電腦上也稱為「立即更新」）的權限。如需詳細資訊，請參閱 OfficeScan 用戶端的更新權限和其他設定 第 6-39 頁。

手動更新 OfficeScan 用戶端

程序

1. 瀏覽至「更新 > 用戶端電腦 > 手動更新」。
2. 畫面頂端會顯示 OfficeScan 伺服器上目前可用的元件，以及上次更新這些元件的日期。通知用戶端更新之前，請先確定元件是最新的。

   注意

   手動更新伺服器上的過期元件。如需詳細資訊，請參閱 OfficeScan 用戶端手動更新 第 6-37 頁。

3. 如果只要更新具有過期元件的用戶端：
   a. 按一下「選取具有過期元件的用戶端」。
   b. （選用）選取「包括行動和離線用戶端」：
      - 更新與伺服器之間具有有效連線的行動用戶端。
      - 更新變為線上狀態時的離線用戶端。
   c. 按一下「開始更新」。

   注意

   伺服器會搜尋元件版本比伺服器上的元件版本舊的用戶端，並通知這些用戶端更新。如果要檢查通知狀態，請移至 更新 > 摘要 畫面。

4. 如果要更新選擇的用戶端：

   a. 選取「手動選取用戶端」。

   b. 按一下「選取」。

   c. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。

   d. 按一下「開始元件更新」。

   注意

   伺服器會開始通知每一個用戶端下載經過更新的元件。如果要檢查通知狀態，請移至 更新 > 摘要 畫面。

OfficeScan 用戶端的更新權限和其他設定

授與用戶端使用者特定權限，例如：執行「立即更新」和啟動預約更新。

執行「立即更新」

具有此權限的使用者可以視需要以滑鼠右鍵按一下系統匣的 OfficeScan 用戶端圖示並選取「立即更新」來更新元件。您可以允許用戶端使用者在「立即更新」期間使用 Proxy 伺服器設定。如需詳細資訊，請參閱用戶端的 Proxy 伺服器設定權限 第 14-44 頁。

警告!

如果使用者設定的 Proxy 伺服器設定不正確，會導致發生更新問題。允許使用者設定自己的 Proxy 伺服器設定時請特別小心。

啟動預約更新

此權限允許用戶端啟動/關閉預約更新。雖然使用者具有啟動/關閉預約更新的權限，但他們無法設定實際預約時程。您必須在更新 > 用戶端電腦 > 自動更新的「預約更新」區段中指定時程。

用戶端從趨勢科技主動式更新伺服器下載更新程式

開始更新時，OfficeScan 用戶端會先從「更新 > 用戶端電腦 > 更新來源」畫面中指定的更新來源取得更新程式。如果更新不成功，用戶端便會嘗試從 OfficeScan 伺服器更新。選取這個選項可讓用戶端在無法從 OfficeScan 伺服器更新時，嘗試從趨勢科技主動式更新伺服器進行更新。

您無法直接從趨勢科技主動式更新伺服器更新純 IPv6 用戶端。如果要使雲端截毒掃瞄用戶端連線到來源，需要允許用戶端連線至主動式更新伺服器。

用戶端可更新元件，但不升級用戶端程式或部署 HotFix

此選項允許繼續更新元件，但卻會讓 HotFix 部署和 OfficeScan 用戶端升級無法執行。

如果您未選取這個選項，則所有用戶端會同步連線至伺服器以進行升級或安裝 HotFix。這樣會在擁有大量用戶端時，大幅影響伺服器效能。如果您選取這個選項，請規劃如何將伺服器上的 OfficeScan 用戶端升級或 HotFix 部署的影響降至最低，然後執行您的規劃。

授與更新權限給 OfficeScan 用戶端

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 權限和其他設定」。
4. 在「權限」標籤上，移至「元件更新權限」區段。

5. 選取下列選項：
   - 執行「立即更新」
   - 啟動預約更新
6. 按一下「其他設定」標籤，然後移至「更新設定」區段。
7. 選取下列選項：
   - 用戶端從趨勢科技主動式更新伺服器下載更新程式
   - 啟動預約更新
   - 用戶端可更新元件，但不升級用戶端程式或部署 HotFix
8. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

為 OfficeScan 用戶端更新設定保留磁碟空間

OfficeScan 可以配置特定數目的用戶端磁碟空間，以供 HotFix、病毒碼檔案、掃瞄引擎和程式更新檔使用。依預設，OfficeScan 會保留 60MB 的磁碟空間。

程序

1. 瀏覽至「用戶端電腦 > 全域用戶端設定」。
2. 移至「保留磁碟空間」區段。
3. 選取「保留 __ MB 磁碟空間以備更新」。
4. 選取磁碟空間量。

5. 按一下「儲存」。

用於 OfficeScan 用戶端元件更新的 Proxy

OfficeScan 用戶端可以在自動更新期間使用 Proxy 伺服器設定，或如果用戶端有執行「立即更新」的權限也可以使用 Proxy 伺服器設定。

表 6-9. OfficeScan 用戶端元件更新期間使用的 Proxy 伺服器設定

更新方式	使用的 Proxy 伺服器設定	使用方式
自動用戶端更新	• 自動 Proxy 伺服器設定。如需詳細資訊，請參閱適用於 OfficeScan 用戶端的自動 Proxy 伺服器設定 第 14-45 頁。 • 內部 Proxy 伺服器設定。如需詳細資訊，請參閱 OfficeScan 用戶端的內部 Proxy 伺服器 第 14-42 頁。	1. OfficeScan 用戶端會先使用自動 Proxy 伺服器設定更新元件。 2. 如果自動 Proxy 伺服器設定未啟動，則會使用內部 Proxy 伺服器設定。 3. 如果兩者都為關閉狀態，則用戶端不會使用任何 Proxy 伺服器設定。
立即更新	• 自動 Proxy 伺服器設定。如需詳細資訊，請參閱適用於 OfficeScan 用戶端的自動 Proxy 伺服器設定 第 14-45 頁。 • 使用者設定的 Proxy 伺服器設定。您可以授與用戶端使用者設定 Proxy 伺服器設定的權限。如需詳細資訊，請參閱用戶端的 Proxy 伺服器設定權限 第 14-44 頁。	1. OfficeScan 用戶端會先使用自動 Proxy 伺服器設定更新元件。 2. 如果自動 Proxy 伺服器設定尚未啟動，則會使用使用者設定的 Proxy 伺服器設定。 3. 如果兩者都為關閉狀態，或是自動 Proxy 伺服器設定為關閉狀態且用戶端使用者未具備所需權限，則用戶端更新元件時便不會使用任何 Proxy。

配置 OfficeScan 用戶端更新通知

發生更新相關事件時，OfficeScan 會通知用戶端使用者。

程序

1. 瀏覽至「用戶端電腦 > 全域用戶端設定」。
2. 移至「警訊設定」區段。
3. 選取下列選項：
   - 如果病毒碼檔案在 __ 天後仍未更新，則會在 windows 工作列上顯示警訊圖示：在 Windows 工作列上顯示警訊圖示，提醒使用者更新在指定天數內未更新的病毒碼。如果要更新病毒碼，請使用 OfficeScan 用戶端更新方法 第 6-31 頁中所述的任何一種更新方法。

     由伺服器管理的所有用戶端都會套用此設定。
   - 如果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：在安裝 HotFix 或包含新版核心模式驅動程式的升級套件之後，前一版的驅動程式可能仍然存留在電腦上。唯一能夠卸載前一版和載入新版的方式是重新啟動電腦。重新啟動電腦之後，新版驅動程式便會自動安裝，且不需再次重新啟動。

     當用戶端電腦安裝 HotFix 或升級套件之後，會立即顯示通知訊息。
4. 按一下「儲存」。

檢視 OfficeScan 用戶端更新記錄檔

檢查用戶端更新記錄檔，判斷更新用戶端上的「病毒碼」時是否發生問題。

注意

在此產品版本中，只能從 Web 主控台查詢「病毒碼」更新的記錄檔。

如果要避免記錄檔佔去過多硬碟空間，請手動刪除記錄檔或設定記錄檔刪除預約時程。如需有關管理記錄檔的詳細資訊，請參閱記錄檔管理 第 13-31 頁。

程序

1. 瀏覽至「記錄檔 > 用戶端電腦記錄檔 > 元件更新」。
2. 如果要檢視用戶端更新數量，請按一下「進度」欄位下的「檢視」。在顯示的「元件更新進度」畫面中，檢視每隔十五分鐘更新的用戶端數量和已更新的用戶端總數。
3. 如果要檢視已更新「病毒碼」的用戶端，請按一下「詳細資料」欄位下的「檢視」。
4. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請按一下「匯出到 CSV」。開啟檔案或將其儲存至特定位置。

實施 OfficeScan 用戶端更新

使用「安全性符合」確保用戶端有最新的元件。安全性符合會判斷 OfficeScan 伺服器和用戶端之間元件不一致的情況。不一致的情況通常發生在用戶端無法連線到伺服器以更新元件時。如果用戶端是從其他來源取得更新（例如主動式更新伺服器），用戶端中的元件就可能比伺服器中的元件還要新。

如需詳細資訊，請參閱適用於受管用戶端的安全性符合 第 14-49 頁。

OfficeScan 用戶端的還原元件

「還原」的意思是恢復到舊版「病毒碼」、「本機雲端病毒碼」和「病毒掃瞄引擎」。如果這些元件無法正常運作，請將它們還原成之前版本。OfficeScan 會保留目前和之前版本的「病毒掃瞄引擎」，以及最新五個版本的「病毒碼」和「本機雲端病毒碼」。

注意

只能還原上述元件。

OfficeScan 會針對執行 32 位元和 64 位元平台的用戶端使用不同的掃瞄引擎。您必須個別還原這些掃瞄引擎。所有掃瞄引擎類型的還原程序都相同。

程序

1. 瀏覽至「更新 > 還原」
2. 在適當的區段下按一下「同步處理伺服器」。
   a. 在顯示的用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
   b. 按一下「還原」。
   c. 按一下「檢視更新記錄檔」檢查結果，或按「上一步」回到「還原」畫面。
3. 如果伺服器上存在較早版本的病毒碼檔案，請按一下「還原伺服器和用戶端版本」同時恢復 OfficeScan 用戶端和伺服器的病毒碼檔案。

執行用於 OfficeScan 用戶端 Hotfix 的 Touch Tool

「Touch Tool」可以將某一檔案的時間戳記與其他檔案的時間戳記同步化，或與電腦的系統時間同步化。如果無法在 OfficeScan 伺服器上部署 HotFix，請使用 Touch Tool 變更 HotFix 的時間戳記。這會讓 OfficeScan 將這個 HotFix 解譯為新的 HotFix，使伺服器自動再次嘗試部署這個 HotFix。

程序

1. 在 OfficeScan 伺服器上，移至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\Touch。
2. 將 TMTouch.exe 複製到包含要變更的檔案的資料夾。如果要將兩個不同檔案的時間戳記同步化，請將這兩個檔案和 Touch Tool 放到相同的位置。
3. 開啟命令提示字元視窗，切換至 Touch Tool 所在的位置。

4. 輸入下列命令：

   `TmTouch.exe <目標檔案名稱> <來源檔案名稱>`

   說明：

   - `<目標檔案名稱>` 是您要變更其時間戳記的 HotFix 檔案名稱
   - `<來源檔案名稱>` 是要複製其時間戳記的檔案名稱

   注意

   如果您沒有指定來源檔案名稱，這個工具會將目標檔案時間戳記設為電腦系統時間。您可以將萬用字元 (*) 用於目標檔案，但不能用於來源檔案名稱。

5. 如果要檢查時間戳記是否已經變更，請在命令提示字元中輸入 `dir`，或在「Windows 檔案總管」中檢查檔案內容。

更新代理程式

如果要將元件、網域設定或是用戶端程式和 HotFix 部署到 OfficeScan 用戶端的工作散佈到其他用戶端，請將某些 OfficeScan 用戶端指定為「更新代理程式」或其他用戶端的更新來源。這樣能協助您確保用戶端準時收到更新，而不會將大量網路傳輸導向 OfficeScan 伺服器。

如果網路依位置區分為不同網段，而且各網段之間的網路連結出現高傳輸負載，請在每個位置至少指定一個「更新代理程式」。

更新代理程式系統需求

請造訪下列網站，以取得系統需求的完整清單：

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

更新代理程式組態設定

設定更新代理程式組態設定的程序包括兩個步驟：

1. 指定 OfficeScan 用戶端做為特定元件的更新代理程式。
2. 指定將從此「更新代理程式」更新的用戶端。

注意

單一「更新代理程式」能夠處理的同時用戶端連線數目，端視電腦的硬體規格而定。

指定 OfficeScan 用戶端做為「更新代理程式」

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，選取要指定為「更新代理程式」的用戶端。

注意

無法選取根網域圖示，因為這會將所有用戶端全指定為「更新代理程式」。純 IPv6 更新代理程式無法直接將更新分發到純 IPv4 用戶端。同樣地，純 IPv4 更新代理程式無法直接將更新分發到純 IPv6 用戶端。如果要允許「更新代理程式」將更新分發到用戶端，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。

3. 按一下「設定 > 更新代理程式設定」。
4. 選取「更新代理程式」可以共用的項目。
   - 元件更新
   - 網域設定
   - 用戶端程式和 HotFix

5. 按一下「儲存」。

指定從「更新代理程式」更新的 OfficeScan 用戶端

程序

1. 瀏覽至「更新 > 用戶端電腦 > 更新來源」。
2. 在「自訂更新來源清單」下，按一下「新增」。
3. 在顯示的畫面中，指定用戶端的 IP 位址。您可以輸入 IPv4 範圍和/或 IPv6 字首和長度。
4. 在「更新代理程式」欄位中，選取您要指定給用戶端的「更新代理程式」。

   注意

   請確定用戶端可使用其 IP 位址連線到「更新代理程式」。例如，如果指定 IPv4 位址範圍，則「更新代理程式」必須具有 IPv4 位址。如果指定 IPv6 字首和長度，則「更新代理程式」必須具有 IPv6 位址。

5. 按一下「儲存」。

更新代理程式的更新來源

「更新代理程式」可以從各種來源取得更新檔，例如 OfficeScan 伺服器或自訂的更新來源。您可以從 Web 主控台的「更新來源」畫面設定更新來源。

對更新代理程式的 IPv6 支援

純 IPv6 更新代理程式無法直接從純 IPv4 更新來源更新，例如：

- 純 IPv4 OfficeScan 伺服器

- 任何純 IPv4 自訂更新來源
- 趨勢科技主動式更新伺服器

同樣地，純 IPv4 更新代理程式無法直接從純 IPv6 更新來源（例如純 IPv6 OfficeScan 伺服器）更新。

如果要允許「更新代理程式」連線到更新來源，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。

更新代理程式的標準更新來源

OfficeScan 伺服器是「更新代理程式」的標準更新來源。如果設定代理程式直接從 OfficeScan 伺服器更新，則更新程序的執行方式如下：

1. 「更新代理程式」從 OfficeScan 伺服器取得更新檔。
2. 如果代理程式無法從 OfficeScan 伺服器更新，而且下列任一條件成立，則代理程式會嘗試直接連線到趨勢科技主動式更新伺服器：
   - 在用戶端電腦 > 用戶端管理，按一下設定 > 權限和其他設定 > 其他設定 > 更新設定，此選項用戶端從趨勢科技主動式更新伺服器下載更新程式已啟動。
   - 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 OfficeScan 伺服器更新時發生問題，請將主動式更新伺服器放在該清單頂端。當「更新代理程式」直接從主動式更新伺服器更新時，網路和 Internet 之間會耗用大量頻寬。
3. 如果無法從所有可能的來源更新，則「更新代理程式」會結束更新程序。

更新代理程式的自訂更新來源

除了從 OfficeScan 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 OfficeScan 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 OfficeScan 用戶端的自訂更新來源 第 6-27 頁。

注意

確定「僅從 OfficeScan 伺服器更新代理程式更新元件、網域設定、用戶端程式 以及 HotFix」此選項已關閉

，其位於更新來源（用戶端電腦）畫面上（更新 > 用戶端電腦 > 更新來源），如此「更新代理程式」才能連線上自訂更新來源。

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. 如果代理程式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. 如果代理程式無法從所有項目更新，即會檢查下列選項：
   - 所有自訂更新來源都無法使用或找不到時，會從 OfficeScan 伺服器更新元件：如果已啟動此選項，則代理程式會從 OfficeScan 伺服器更新。

     如果已關閉此選項，而且下列任一條件成立，則代理程式會嘗試直接連線到趨勢科技主動式更新伺服器：

     注意

     您只能從主動式更新伺服器更新元件。網域設定、程式和 HotFix 只能從該伺服器或更新代理程式下載。

     - 在 用戶端電腦 > 用戶端管理中，按一下「設定 > 權限和其他設定 > 其他設定 > 更新設定」，「用戶端從趨勢科技主動式更新伺服器下載更新程式」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。
   - 所有自訂來源都無法使用或找不到時，會從 OfficeScan 伺服器更新網域設定：如果已啟動此選項，則代理程式會從 OfficeScan 伺服器更新。

- 所有自訂來源都無法使用或找不到時，會從 OfficeScan 伺服器更新用戶端程式和 HotFix：如果已啟動此選項，則代理程式會從 OfficeScan 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。

如果更新代理程式：永遠從標準更新來源 (OfficeScan 伺服器) 更新」選項已啟動，且 OfficeScan 伺服器通知代理程式更新元件，則更新程序會不一樣。程序如下：

1. 代理程式會直接從 OfficeScan 伺服器更新，並略過更新來源清單。
2. 如果代理程式無法從伺服器更新，而且下列任一條件成立，則代理程式會嘗試直接連線到趨勢科技主動式更新伺服器：
   - 在 用戶端電腦 > 用戶端管理中，按一下「設定 > 權限和其他設定 > 其他設定 > 更新設定」，「用戶端從趨勢科技主動式更新伺服器下載更新程式」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 OfficeScan 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 OfficeScan 用戶端直接從主動式更新伺服器更新時，網路和 Internet 之間會耗用大量頻寬。

3. 如果無法從所有可能的來源更新，則「更新代理程式」會結束更新程序。

設定更新代理程式的更新來源

程序

1. 瀏覽至「更新 > 用戶端電腦 > 更新來源」。
2. 選取要從更新代理程式的標準更新來源 (OfficeScan 伺服器) 還是從更新代理程式的自訂更新來源進行更新。
3. 按一下「通知所有用戶端」。

更新代理程式元件複製

如同 OfficeScan 伺服器，「更新代理程式」也會在下載元件時使用元件複製。如需有關伺服器如何執行元件複製的詳細資訊，請參閱 OfficeScan 伺服器元件複製 第 6-17 頁。

「更新代理程式」的元件複製程序如下：

1. 「更新代理程式」會比較其目前完整病毒碼版本與更新來源上的最新版本。如果兩個版本之間的差異數為 14 或以下，「更新代理程式」只會下載包含兩個版本之間差異的漸增式病毒碼。

   注意

   如果差異數為 14 以上，則「更新代理程式」會自動下載完整病毒碼檔案版本。

2. 「更新代理程式」會合併其下載的漸增式病毒碼與其目前的完整病毒碼，以產生最新的完整病毒碼。
3. 「更新代理程式」會下載更新來源上剩餘的所有漸增式病毒碼。
4. 最新的完整病毒碼和所有漸增式病毒碼都會提供給用戶端。

更新代理程式的更新方式

「更新代理程式」使用標準用戶端可用的相同更新方式。如需詳細資訊，請參閱 OfficeScan 用戶端更新方法 第 6-31 頁。

您也可以使用「預約更新組態設定」工具來啟動和設定「更新代理程式」（使用 Client Packager 所安裝）的預約更新。

注意

如果「更新代理程式」是使用其他安裝方式安裝，則無法使用此工具。如需詳細資訊，請參閱部署考量 第 5-10 頁。

使用預約更新組態設定工具

程序

1. 在「更新代理程式」電腦上，瀏覽至 <用戶端安裝資料夾>。
2. 按兩下 `SUCTool.exe` 執行此工具。「預約更新組態設定工具」主控台隨即開啟。
3. 選取「啟動預約更新」。
4. 指定更新頻率和時間。
5. 按一下「套用」。

更新代理程式分析報告

產生「更新代理程式分析報告」，以分析更新基礎架構，並判斷哪些用戶端會從 OfficeScan 伺服器、更新代理程式或主動式更新伺服器進行下載。您也可以使用此報告，檢查向更新來源要求更新的用戶端數目是否超過可用資源，並將網路流量重新導向至適當來源。

注意

此報告包括所有「更新代理程式」。如果您已將管理一或多個網域的工作委派給其他管理員，則他們還會看到不屬於其管理之網域的「更新代理程式」。

OfficeScan 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：

- OfficeScan 用戶端電腦
- 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
  - OfficeScan 用戶端程式和 HotFix

如需產生報告的詳細資訊，請參閱 OfficeScan 用戶端的自訂更新來源 第 6-27 頁。

元件更新摘要

Web 主控台提供「更新摘要」畫面（瀏覽至「更新 > 摘要」），此畫面會通知您元件整體更新狀態並可讓您更新過期元件。如果已啟動伺服器預約更新，此畫面也會顯示下一個更新預約時程。

請定期重新整理此畫面，以檢視最新的元件更新狀態。

注意

如果要檢視整合式主動式雲端截毒技術伺服器上的元件更新，請移至「主動式雲端截毒技術 > 整合式伺服器」。

OfficeScan 用戶端更新狀態

如果您開始用戶端的元件更新，可在本區段檢視下列資訊：

- 收到元件更新通知的用戶端數目。
- 尚未收到通知但已在通知佇列中的用戶端數目。如果要取消這些用戶端的通知，請按一下「取消通知」。

元件

在「更新狀態」表格中，檢視 OfficeScan 伺服器下載並散佈的每個元件的更新狀態。

您可以檢視每個元件的目前版本和最近一次的更新日期。按一下數字連結，以檢視內含過期元件的用戶端。手動更新內含過期元件的用戶端。

第 7 章

掃瞄是否有安全威脅

本章說明如何使用 File-based 掃瞄來保護電腦免於受到安全威脅的侵襲。

本章內容：

關於安全威脅

安全威脅是病毒/惡意程式與間諜程式/可能的資安威脅程式的統稱。OfficeScan 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。OfficeScan 透過強制執行病毒爆發警訊防範策略並隔離中毒電腦來協助控制病毒爆發警訊，直到電腦不包含任何安全威脅。通知與記錄檔可協助您追蹤安全威脅，並且在您需要採取立即處理行動時對您提出警訊。

病毒和惡意程式

現存病毒/惡意程式的數目成千上萬，數量每天都在增加。雖然電腦病毒一度在 DOS 或 Windows 中最常見，但是現今卻能利用企業網路、電子郵件系統及網站的弱點造成嚴重損害。

- 惡作劇程式：類似病毒的程式，往往會在電腦螢幕上作怪。
- 可能的病毒/惡意程式：具有某些病毒/惡意程式特徵的可疑檔案。如需詳細資訊，請參閱趨勢科技病毒百科全書：

  http://www.trendmicro.com/vinfo/zh-tw/virusencyclo/default.asp

- Rootkit：在使用者未同意或未知曉的情況下就在系統上安裝並執行程式碼的程式（或程式集合）。它會在電腦上使用隱形方式持續存在，且偵測不到。Rootkit 不會感染電腦，卻會在無法偵測到的情況下執行惡意程式碼。在惡意程式執行時或僅在瀏覽惡意網站時，Rootkit 就會透過社交工程安裝在系統上。安裝完成後，攻擊者在系統上幾乎可以執行任何功能，包括遠端存取、竊聽，以及隱藏程序、檔案、登錄機碼和通訊通道。
- 特洛伊木馬程式：此類型的威脅經常使用通訊埠來取得電腦或可執行程式的存取權。特洛伊木馬程式不會進行複製，但會常駐在系統上執行惡意動作，例如開放通訊埠讓駭客進入。傳統的防毒解決方案可以偵測並移除的是病毒，不是特洛伊木馬程式，特別是已經在系統上執行的那些特洛伊木馬程式。
- 病毒：會進行複製的程式。為了進行複製，病毒必須將自己附加到其他的程式檔，然後在主程式執行時執行，包括

- ActiveX 惡意程式碼：常駐在執行 ActiveX™ 控制項之網頁中的程式碼。
- 開機磁區型病毒：會感染分割區或磁碟的開機磁區的病毒。
- COM 和 EXE 檔案感染型病毒：副檔名為 .com 或 .exe 的可執行程式。
- Java 惡意程式碼：以 Java™ 撰寫或內嵌於其中的非依附作業系統型病毒碼
- 巨集型病毒：編碼為應用程式巨集，且往往隨附於文件中的病毒。
- 網路病毒：嚴格說來，透過網路傳播的病毒，並不算是網路病毒。只有蠕蟲之類的某些病毒/惡意程式類型，才有資格稱為網路病毒。具體來說，網路病毒使用網路通訊協定（例如：TCP、FTP、UDP、HTTP）和電子郵件通訊協定來自行複製，而且往往不會改變系統檔案或修改硬碟的開機磁區。網路病毒反而會感染用戶端電腦的記憶體，強迫這些電腦以流量淹沒網路，這可能會造成速度下降，甚至造成網路完全故障。因為網路病毒會留在記憶體中，所以傳統的檔案 I/O 型掃瞄方法往往偵測不到它們。

  OfficeScan 防火牆會搭配「一般防火牆病毒碼」使用，以辨識並封鎖網路病毒。如需詳細資訊，請參閱關於 OfficeScan 防火牆 第 12-2 頁。
- 封裝程式：經過壓縮和（或）加密的 Windows 或 Linux™ 可執行程式，通常是特洛伊木馬程式。壓縮可執行檔會使防毒產品更難偵測封裝程式。
- 測試病毒：行為類似真正病毒的內隱檔案，可以由病毒掃瞄軟體偵測出來。使用測試病毒 (例如：EICAR 測試程式檔)，確認您安裝的防毒程式掃瞄正常。
- VBScript、JavaScript 或 HTML 病毒：常駐在網頁中且透過瀏覽器下載的病毒。
- 電腦蠕蟲：一種自我包裝的程式（或程式集），可以將具有功能性的本體複製檔或其片段散佈到其他電腦系統，途徑往往是透過電子郵件。

- 其他：未分類到其他任何病毒/惡意程式類型下的病毒/惡意程式。

間諜程式和可能的資安威脅程式

用戶端電腦會受到潛在安全威脅而非病毒/惡意程式的侵襲。間諜程式/可能的資安威脅程式是指未歸類為病毒或特洛伊木馬程式的應用程式或檔案，但還是可能對您網路上的電腦效能有負面的影響，以及對您的組織形成重大的安全、機密和法律風險。間諜程式/可能的資安威脅程式往往會執行各種不受歡迎和具威脅的行動，例如用快顯視窗騷擾使用者，記錄使用者的按鍵動作以及暴露電腦弱點使其易受攻擊。

如果您找到 OfficeScan 無法偵測出是否為可能的資安威脅程式的應用程式或檔案，但是您認為它是一種可能的資安威脅程式，請傳送到趨勢科技進行分析：

http://subwiz.trendmicro.com/SubWiz

間諜程式/可能的資安威脅程式類型

- 間諜程式：蒐集資料（如帳號使用者名稱和密碼），並將資料傳輸至第三方。
- 廣告軟體：顯示廣告並蒐集資料（如使用者的 web 瀏覽偏好），以便透過 Web 瀏覽器讓使用者成為廣告的目標。
- 惡意撥號程式：變更電腦的 Internet 設定，而且可能會強制電腦透過數據機撥出預先設定的電話號碼。而這些號碼通常是付費電話或國際電話號碼，可能會使您公司的電話費暴增。
- 惡作劇程式：造成電腦行為異常（例如：關閉和開啟 CD-ROM 托盤），以及顯示大量訊息方塊。
- 駭客工具：幫助駭客進入電腦。
- 遠端存取工具：幫助駭客從遠端存取和控制電腦。
- 密碼破解程式：幫助駭客破解帳號使用者名稱和密碼。
- 其他：其他潛在惡意程式類型。

間諜程式/可能的資安威脅程式如何進入網路

「間諜程式/可能的資安威脅程式」經常會在使用者下載安裝套件中包含可能的資安威脅程式的合法軟體時進入企業網路。大部分軟體程式都包括「使用者授權合約」(EULA)，使用者必須接受該合約才能下載。EULA 經常包含有關應用程式及其因專門用途而收集個人資料的資訊；然而，使用者常會忽略這項資訊，或不瞭解法律用語。

潛在風險和威脅

網路上存在的間諜程式和其他類型可能的資安威脅程式，可能會導致下列各種情況：

- 電腦效能降低：為了執行工作，間諜程式/可能的資安威脅程式常需要大量的 CPU 和系統記憶體資源。
- 因 Web 瀏覽器引起的當機事件增多：廣告軟體等特定類型的可能資安威脅程式，通常會在瀏覽器框架或視窗中顯示資訊。視這些應用程式中的程式碼與系統處理程序之間的互動方式而定，可能的資安威脅程式有時可能會造成瀏覽器損毀或凍結，甚至可能需要重新啟動電腦。
- 使用者效率降低：由於需要關閉經常出現的快顯廣告以及處理惡作劇程式造成的負面影響，使用者無法專心進行主要工作。
- 網路頻寬降級：間諜程式/可能的資安威脅程式通常會定期將收集到的資料，傳輸給在網路上（或網路之外）執行的其他應用程式。
- 損失個人和公司資訊：間諜程式/可能的資安威脅程式並非只收集網站使用者瀏覽清單這類無害的資料。間諜程式/可能的資安威脅程式也會收集使用者憑證，例如用於存取線上銀行帳號和企業網路的憑證。
- 承擔法律責任的風險提高：如果您網路上的電腦資源遭綁架，駭客可能會利用您的用戶端電腦對網路之外的電腦發動攻擊或安裝間諜程式/可能的資安威脅程式。如果您的網路資源牽涉到這類活動，則可能導致您的組織必須對其他人所造成的損害負起法律責任。

間諜程式/可能的資安威脅程式和其他安全威脅的防護

您可以採取許多步驟，避免間諜程式/可能的資安威脅程式安裝到您的電腦上。趨勢科技建議您執行下列行動：

- 將所有類型的掃瞄（「手動掃瞄」、「即時掃瞄」、「預約掃瞄」和「立即掃瞄」）設為掃瞄並移除間諜程式/可能的資安威脅程式檔案和應用程式。如需詳細資訊，請參閱掃瞄類型 第 7-12 頁。
- 教導您的用戶端使用者進行下列各項：
  - 詳閱下載並安裝至電腦的應用程式「使用者授權合約」(EULA) 和隨附文件。
  - 出現任何要求授權的訊息時，按一下「否」，以下載和安裝軟體，除非用戶端使用者確定軟體建立者及檢視的網站都值得信任。
  - 略過來路不明的商業電子郵件（垃圾郵件），特別是要求使用者按一下按鈕或超連結的垃圾郵件。
- 設定可確保高安全層級的 Web 瀏覽器設定。趨勢科技建議您要求 Web 瀏覽器在安裝 ActiveX 控制項之前，先對使用者顯示提示。
- 如果使用 Microsoft Outlook，請設定安全設定，讓 Outlook 不會自動下載 HTML 項目。例如：垃圾郵件中傳送的圖片。
- 請勿允許使用對等式檔案共享服務。間諜程式和其他可能的資安威脅程式可能會喬裝為使用者想要下載的其他類型檔案，例如：MP3 音樂檔。
- 定期檢查代理程式電腦上安裝的軟體，並尋找可能為間諜程式或其他可能的資安威脅程式應用程式。
- 使用 Microsoft 提供的最新修補程式，讓您的 Windows 作業系統保持最新狀態。請參閱 Microsoft 網站以瞭解詳細資訊。

掃瞄方法

OfficeScan 用戶端可以使用兩種掃瞄方法中的任意一種，來掃瞄是否有安全威脅。掃瞄方法包括雲端截毒掃瞄和標準掃瞄。

- 雲端截毒掃瞄

  使用雲端截毒掃瞄的用戶端在本文件中稱為雲端掃瞄用戶端。雲端掃瞄用戶端將受益於「檔案信譽評等服務」提供的本機掃瞄和雲端查詢。

- 標準掃瞄

  不使用雲端截毒掃瞄的用戶端稱為標準用戶端。標準用戶端會將所有 OfficeScan 元件儲存在用戶端電腦上，並在本機掃瞄所有檔案。

預設掃瞄方法

在這個 OfficeScan 版本中，全新安裝的預設掃瞄方法是雲端截毒掃瞄。這表示如果您執行 OfficeScan 伺服器全新安裝，但未在 Web 主控台上變更掃瞄方法，則伺服器管理的所有用戶端都會使用雲端截毒掃瞄。

如果您從舊版的 OfficeScan 伺服器升級，並且啟動了用戶端自動升級，則該伺服器管理的所有用戶端仍將會使用升級前設定的掃瞄方法。例如，從僅支援標準掃瞄的 OfficeScan 8.x 進行升級，表示所有用戶端在升級後仍將使用標準掃瞄。如果從支援雲端截毒掃瞄和標準掃瞄的 OfficeScan 10 進行升級，則使用雲端截毒掃瞄的所有用戶端在升級後將繼續使用雲端截毒掃瞄，且使用標準掃瞄的所有用戶端在升級後將繼續使用標準掃瞄。

掃瞄方法比較

下表提供這兩種掃瞄方法的比較：

表 7-1. 標準掃瞄和雲端截毒掃瞄的比較

比較基準	標準掃瞄	雲端截毒掃瞄
可用性	可在此 OfficeScan 版本與所有舊版 OfficeScan 版本中使用	從 OfficeScan 10 開始提供

比較基準	標準掃瞄	雲端截毒掃瞄
掃瞄行為	標準用戶端會在本機電腦執行掃瞄。	• 雲端掃瞄用戶端會在本機電腦執行掃瞄。 • 如果用戶端無法在掃瞄期間判斷檔案的風險，則用戶端會將掃瞄查詢傳送到主動式雲端截毒伺服器來源以檢查該風險。 • 用戶端會「快取」掃瞄查詢結果以改善掃瞄效能。
元件使用中且已更新	所有元件（「本機雲端病毒碼」除外）在更新來源都可用	所有元件（「病毒碼」和「間諜程式主動式監控病毒碼」除外）在更新來源都可用
傳統更新來源	OfficeScan 伺服器	OfficeScan 伺服器

變更掃瞄方法

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 掃瞄設定 > 掃瞄方法」。
4. 選取標準掃瞄」或「雲端截毒掃瞄」。
5. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。

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

從雲端截毒掃瞄切換至標準掃瞄

將用戶端切換到標準掃瞄時，請考量下列事項：

1. 要切換的用戶端數目

   一次切換少量的用戶端，可確保有效利用 OfficeScan 伺服器與主動式雲端截毒技術伺服器的資源。當用戶端變更其掃瞄方法時，這些伺服器可以執行其他重要工作。

2. 時機

   切換回標準掃瞄時，用戶端可能會從 OfficeScan 伺服器下載完整版的病毒碼與間諜程式主動式監控病毒碼。這些病毒碼檔案僅適用於標準用戶端。

   建議您在離峰時段進行切換，以確保下載程序可在短時間內完成。同時建議您在沒有用戶端預約要從伺服器進行更新時，執行切換作業。此外，請暫時關閉用戶端上的「立即更新」，等到用戶端已切換至雲端截毒掃瞄後，再予以重新啟動。

3. 用戶端樹狀結構設定

   掃瞄方法是一項可在根、網域或個別用戶端層級上進行設定的精細設定。切換至標準掃瞄時，您可以：

   - 建立新的用戶端樹狀結構網域，並將標準掃瞄指定為其掃瞄方法。任何移至此網域的用戶端，都會使用標準掃瞄。當您移動用戶端時，請啟動「將新網域的設定套用至選取的用戶端」設定。
   - 選取網域並加以設定，使其使用標準掃瞄。屬於該網域的雲端掃瞄用戶端將會切換至標準掃瞄。
   - 從網域中選取一或多個雲端掃瞄用戶端，然後將其切換至標準掃瞄。

注意

如果網域的掃瞄方法有任何變更，都將覆寫您為個別用戶端指定的掃瞄方法。

從標準掃瞄切換至雲端截毒掃瞄

如果將用戶端從標準掃瞄切換到雲端截毒掃瞄，請確定已設定「主動式雲端截毒技術服務」。如需詳細資訊，請參閱設定主動式雲端截毒技術服務 第 4-11 頁。

下表提供了切換到雲端截毒掃瞄時的其他注意事項：

表 7-2. 切換到雲端截毒掃瞄時的注意事項

注意事項	詳細資訊
無法使用的特性和功能	雲端掃瞄用戶端無法向策略伺服器報告雲端病毒碼和本機雲端病毒碼資訊。
產品使用授權	如果要使用雲端截毒掃瞄，請確認您已啟動下列服務的使用授權，且這些使用授權尚未到期： • 防毒 • 網頁信譽評等和間諜程式防護
OfficeScan 伺服器	確定用戶端可連線到 OfficeScan 伺服器。只有線上用戶端會收到切換至雲端截毒掃瞄的通知。離線用戶端在上線後，才會接獲通知。行動用戶端會在上線後接獲通知，或是用戶端若有預約更新權限，則會在執行預約更新時接獲通知。 此外，請驗證 OfficeScan 伺服器是否具有最新的元件，因為雲端掃瞄用戶端必須由此伺服器下載本機雲端病毒碼。如果要更新元件，請參閱 OfficeScan 伺服器更新 第 6-13 頁。
要切換的用戶端數目	一次切換少量的用戶端，可確保有效利用 OfficeScan 伺服器資源。當用戶端變更其掃瞄方法時，OfficeScan 伺服器可以執行其他重要工作。

注意事項	詳細資訊
時機	首次切換至雲端截毒掃瞄時，用戶端必須從 OfficeScan 伺服器下載完整版的本機雲端病毒碼。雲端病毒碼僅適用於雲端掃瞄用戶端。 建議您在離峰時段進行切換，以確保下載程序可在短時間內完成。同時建議您在沒有用戶端預約要從伺服器進行更新時，執行切換作業。此外，請暫時關閉用戶端上的「立即更新」，等到用戶端已切換至雲端截毒掃瞄後，再予以重新啟動。
用戶端樹狀結構設定	掃瞄方法是一項可在根、網域或個別用戶端層級上進行設定的精細設定。切換至雲端截毒掃瞄時，您可以： • 建立新的用戶端樹狀結構網域，並將雲端截毒掃瞄指定為其掃瞄方法。任何移至此網域的用戶端，都會使用雲端截毒掃瞄。當您移動用戶端時，請啟動「將新網域的設定套用至選取的用戶端」設定。 • 選取網域並加以設定，使其使用雲端截毒掃瞄。屬於該網域的標準用戶端將會切換至雲端截毒掃瞄。 • 從網域中選取一或多個標準用戶端，然後將其切換至雲端截毒掃瞄。 注意 如果網域的掃瞄方法有任何變更，都將覆寫您為個別用戶端指定的掃瞄方法。

注意事項	詳細資訊
IPv6 支援	雲端掃瞄用戶端會將掃瞄查詢傳送至主動式雲端截毒技術伺服器來源。 純 IPv6 雲端掃瞄用戶端無法將查詢直接傳送到純 IPv4 來源，例如： • 主動式雲端截毒技術伺服器 2.0（整合式或獨立式） 注意 主動式雲端截毒技術伺服器自 2.5 版開始會支援 IPv6。 • 趨勢科技主動式雲端截毒技術 同樣，純 IPv4 雲端掃瞄用戶端無法將查詢傳送至純 IPv6 主動式雲端截毒技術伺服器。 如果要使雲端掃瞄用戶端連線到來源，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。

掃瞄類型

OfficeScan 提供下列掃瞄類型，以保護 OfficeScan 用戶端電腦不受安全威脅侵害：

表 7-3. 掃瞄類型

掃瞄類型	說明
即時掃瞄	每當接收、開啟、下載、複製或修改檔案時，自動掃瞄電腦上的檔案 如需詳細資訊，請參閱即時掃瞄 第 7-13 頁。
手動掃瞄	由使用者開始執行的掃瞄，會掃瞄使用者所要求的一或多個檔案 如需詳細資訊，請參閱手動掃瞄 第 7-16 頁。
預約掃瞄	根據管理員或終端使用者所設定的預約時程，自動掃瞄電腦上的檔案 如需詳細資訊，請參閱預約掃瞄 第 7-18 頁。

掃瞄類型	說明
立即掃瞄	由管理員開始的掃瞄，掃瞄一或多部目標電腦上的檔案 如需詳細資訊，請參閱立即掃瞄 第 7-20 頁。
密集掃瞄	一種自動起始的掃瞄，提供更高層級的掃瞄作業，在判定為高風險的電腦上尋找可能的惡意程式 如需詳細資訊，請參閱密集掃瞄 第 7-23 頁。

即時掃瞄

「即時掃瞄」會一直持續進行。每當接收、開啟、下載、複製或修改檔案時，「即時掃瞄」即會掃瞄檔案是否存在安全威脅。如果 OfficeScan 未偵測到任何安全威脅，檔案會保留在其位置，供使用者繼續存取。如果 OfficeScan 偵測到安全威脅或可能的病毒/惡意程式，則會顯示一則通知訊息，指出中毒檔案的名稱和具體的安全威脅。

注意

如果要修改通知訊息，請開啟 Web 主控台，然後移至「通知 > 用戶端使用者通知」。

請設定「即時掃瞄」設定，並將其套用至一或多個用戶端與網域，或套用至伺服器管理的所有用戶端。

設定即時掃瞄設定

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 掃瞄設定 > 即時掃瞄設定」。

4. 在「目標」標籤上，設定下列選項：
   - 啟動病毒/惡意程式掃瞄
   - 啟動間諜程式/可能的資安威脅程式掃瞄

   注意

   如果您關閉病毒/惡意程式掃瞄，間諜程式/可能的資安威脅程式掃瞄也會隨之關閉。在病毒爆發期間，「即時掃瞄」將無法關閉（如果原本關閉，將會自動啟動），以防止病毒修改或刪除用戶端電腦上的檔案與資料夾。

5. 設定下列掃瞄條件：
   - 使用者對檔案執行的活動 第 7-25 頁
   - 要掃瞄的檔案 第 7-25 頁
   - 掃瞄設定 第 7-26 頁
   - 掃瞄例外 第 7-28 頁
6. 按一下「動作」標籤，然後設定下列項目：

表 7-4. 即時掃瞄中毒處理行動

處理行動	關係
病毒/惡意程式處理行動	主要處理行動（選取一個）： • 使用主動式處理行動 第 7-35 頁 • 對所有的病毒/惡意程式類型使用相同的處理行動 第 7-36 頁 • 對每個病毒/惡意程式類型使用特定的處理行動 第 7-36 頁 注意 如需有關不同處理行動的詳細資訊，請參閱病毒/惡意程式中毒處理行動 第 7-33 頁。 其他病毒/惡意程式處理行動： • 隔離目錄 第 7-37 頁 • 清除前先備份檔案 第 7-38 頁 • 損害清除及復原服務 第 7-38 頁 • 偵測到病毒/惡意程式時顯示通知訊息 第 7-39 頁 • 偵測到可能的病毒/惡意程式時顯示通知訊息 第 7-40 頁
間諜程式/可能的資安威脅程式處理行動	主要處理行動： • 間諜程式/可能的資安威脅程式中毒處理行動 第 7-43 頁 其他間諜程式/可能的資安威脅程式處理行動： • 偵測到間諜程式/可能的資安威脅程式時顯示通知訊息 第 7-44 頁

7. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

- 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
- 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

手動掃瞄

「手動掃瞄」是依要求執行的掃瞄，會在使用者於 OfficeScan 用戶端主控台上執行掃瞄後立即啟動。完成掃瞄所需的時間，視要掃瞄的檔案數目和 OfficeScan 用戶端電腦的硬體資源而定。

請設定「手動掃瞄」設定，並將其套用至一或多個用戶端與網域，或套用至伺服器管理的所有用戶端。

設定手動掃瞄

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 掃瞄設定 > 手動掃瞄設定」。
4. 在「目標」標籤上，設定下列項目：
   - 要掃瞄的檔案 第 7-25 頁
   - 掃瞄設定 第 7-26 頁
   - CPU 使用率 第 7-27 頁
   - 掃瞄例外 第 7-28 頁
5. 按一下「動作」標籤，然後設定下列項目：

表 7-5. 手動掃瞄處理行動

處理行動	關係
病毒/惡意程式處理行動	主要處理行動（選取一個）： • 使用主動式處理行動 第 7-35 頁 • 對所有的病毒/惡意程式類型使用相同的處理行動 第 7-36 頁 • 對每個病毒/惡意程式類型使用特定的處理行動 第 7-36 頁 注意 如需有關不同處理行動的詳細資訊，請參閱病毒/惡意程式中毒處理行動 第 7-33 頁。 其他病毒/惡意程式處理行動： • 隔離目錄 第 7-37 頁 • 清除前先備份檔案 第 7-38 頁 • 損害清除及復原服務 第 7-38 頁
間諜程式/可能的資安威脅程式處理行動	主要處理行動： • 間諜程式/可能的資安威脅程式中毒處理行動 第 7-43 頁

6. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

預約掃瞄

「預約掃瞄」會在指定的日期與時間自動執行。使用「預約掃瞄」即可針對用戶端自動進行例行掃瞄，並增進掃瞄管理效率。

請設定「預約掃瞄」設定，並將其套用至一或多個用戶端與網域，或套用至伺服器管理的所有用戶端。

設定預約掃瞄

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 掃瞄設定 > 預約掃瞄設定」。
4. 在「目標」標籤上，設定下列選項：
   - 啟動病毒/惡意程式掃瞄
   - 啟動間諜程式/可能的資安威脅程式掃瞄

   注意

   如果您關閉病毒/惡意程式掃瞄，間諜程式/可能的資安威脅程式掃瞄也會隨之關閉。
5. 設定下列掃瞄條件：
   - 預約 第 7-28 頁
   - 要掃瞄的檔案 第 7-25 頁
   - 掃瞄設定 第 7-26 頁
   - CPU 使用率 第 7-27 頁
   - 掃瞄例外 第 7-28 頁

6. 按一下「動作」標籤，然後設定下列項目：

表 7-6. 預約掃瞄中毒處理行動

處理行動	關係
病毒/惡意程式處理行動	主要處理行動（選取一個）： • 使用主動式處理行動 第 7-35 頁 • 對所有的病毒/惡意程式類型使用相同的處理行動 第 7-36 頁 • 對每個病毒/惡意程式類型使用特定的處理行動 第 7-36 頁 注意 如需有關不同處理行動的詳細資訊，請參閱病毒/惡意程式中毒處理行動 第 7-33 頁。 其他病毒/惡意程式處理行動： • 隔離目錄 第 7-37 頁 • 清除前先備份檔案 第 7-38 頁 • 損害清除及復原服務 第 7-38 頁 • 偵測到病毒/惡意程式時顯示通知訊息 第 7-39 頁 • 偵測到可能的病毒/惡意程式時顯示通知訊息 第 7-40 頁
間諜程式/可能的資安威脅程式處理行動	主要處理行動： • 間諜程式/可能的資安威脅程式中毒處理行動 第 7-43 頁 其他間諜程式/可能的資安威脅程式處理行動： • 偵測到間諜程式/可能的資安威脅程式時顯示通知訊息 第 7-44 頁

7. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

- 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
- 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

立即掃瞄

「立即掃瞄」是由 OfficeScan 管理員透過 Web 主控台從遠端開始，可以一或多部用戶端電腦為目標。

請設定「立即掃瞄」設定，並將其套用至一或多個用戶端與網域，或套用至伺服器管理的所有用戶端。

進行立即掃瞄設定

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 掃瞄設定 > 立即掃瞄設定」。
4. 在「目標」標籤上，設定下列選項：
   - 啟動病毒/惡意程式掃瞄
   - 啟動間諜程式/可能的資安威脅程式掃瞄

注意

如果您關閉病毒/惡意程式掃瞄，間諜程式/可能的資安威脅程式掃瞄也會隨之關閉。

5. 設定下列掃瞄條件：
   - 要掃瞄的檔案 第 7-25 頁
   - 掃瞄設定 第 7-26 頁
   - CPU 使用率 第 7-27 頁
   - 掃瞄例外 第 7-28 頁
6. 按一下「動作」標籤，然後設定下列項目：

表 7-7. 立即掃瞄處理行動

處理行動	關係
病毒/惡意程式處理行動	主要處理行動（選取一個）： • 使用主動式處理行動 第 7-35 頁 • 對所有的病毒/惡意程式類型使用相同的處理行動 第 7-36 頁 • 對每個病毒/惡意程式類型使用特定的處理行動 第 7-36 頁 注意 如需有關不同處理行動的詳細資訊，請參閱病毒/惡意程式中毒處理行動 第 7-33 頁。 其他病毒/惡意程式處理行動： • 隔離目錄 第 7-37 頁 • 清除前先備份檔案 第 7-38 頁 • 損害清除及復原服務 第 7-38 頁
間諜程式/可能的資安威脅程式處理行動	主要處理行動： • 間諜程式/可能的資安威脅程式中毒處理行動 第 7-43 頁

7. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

- 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
- 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

開始立即掃瞄

對您懷疑遭到感染的電腦開始「立即掃瞄」。

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「工作 > 立即掃瞄」。
4. 如果要在開始掃瞄前先變更預先設定的「立即掃瞄」設定，請按一下「設定」。

   「立即掃瞄設定」畫面隨即開啟。如需詳細資訊，請參閱立即掃瞄 第 7-20 頁。
5. 在用戶端樹狀結構中，選取要執行掃瞄的用戶端，然後按一下「開始立即掃瞄」。

   注意

   如果您未選取任何用戶端，OfficeScan 會自動通知用戶端樹狀結構中的所有用戶端。

   伺服器便會傳送通知給用戶端。
6. 檢查通知狀態並確認是否有用戶端未收到通知。

7. 依序按一下「選取未通知的電腦」和「開始立即掃瞄」，以立即重新傳送通知給未接獲通知的用戶端。

   例如：用戶端總數：50

   表 7-8. 未通知的用戶端案例

用戶端樹狀結構選項	已通知的用戶端（按一下「開始立即掃瞄」之後）	未通知的用戶端
無（會自動選取所有的 50 部用戶端）	50 部用戶端的其中 35 部	15 部用戶端
手動選取（選取 50 部用戶端中的 45 部）	45 部用戶端的其中 40 部	5 部用戶端 + 手動選取未包含的另外 5 部用戶端

8. 按一下「停止通知」，以提示 OfficeScan 停止通知正在接收通知的用戶端。已經收到通知的用戶端以及正在執行掃瞄的用戶端將會忽略此命令。

9. 對於正在執行掃瞄的用戶端，請按一下「停止立即掃瞄」通知它們停止掃瞄。

密集掃瞄

執行手動掃瞄時，如果 OfficeScan 在用戶端電腦上偵測到指定數目的惡意程式威脅，OfficeScan 會自動開始密集掃瞄。OfficeScan 用戶端會使用提高的威脅偵測層級，重新啟動端點的掃瞄作業。密集掃瞄偵測的可能惡意程式數目多於依需求掃瞄。

注意

密集掃瞄需要的系統資源多於一般的依需求掃瞄。

密集掃瞄的預設處理行動如下：

- 第一個處理行動：隔離
- 第二個處理行動：刪除

注意

管理員無法修改密集掃瞄的處理行動。

使用 ofcscan.ini 設定密集掃瞄

當 OfficeScan 用戶端電腦偵測到感染門檻值時，OfficeScan 會觸發密集掃瞄。管理員可以透過修改 `ofcscan.ini` 檔案，設定觸發密集掃瞄所需的惡意程式偵測數目。

程序

1. 存取 <伺服器安裝資料夾>\PCCSRV。
2. 使用記事本等文字編輯器開啟 `ofcscan.ini` 檔案。
3. 搜尋字串「`IntensiveScanThreshold`」，然後在其旁邊輸入新值。

   預設值為 0 偵測數（關閉）。

   注意

   密集掃瞄需要的系統資源多於一般的依需求掃瞄。請確保設定的門檻值足夠高，以避免不必要的掃瞄。
4. 儲存檔案。
5. 移至「用戶端電腦 > 全域用戶端設定」。
6. 按一下「儲存」。

   OfficeScan 會將更新後的設定部署至所有 OfficeScan 用戶端。

所有掃瞄類型的共用設定

請為每種掃瞄類型設定三組設定：掃瞄條件、掃瞄例外和中毒處理行動。請將這些設定部署至一或多個用戶端與網域，或部署至伺服器管理的所有用戶端。

掃瞄條件

請使用檔案類型與副檔名等檔案屬性，指定特定掃瞄類型所應掃瞄的檔案。此外，請指定將會觸發掃瞄的條件。例如，您可以將「即時掃瞄」設定為在每個檔案下載至電腦後加以掃瞄。

使用者對檔案執行的活動

選擇對檔案執行哪些活動時會觸發「即時掃瞄」。請選取下列選項：

- 建立/修改時：掃瞄引入電腦的新檔案（例如，在下載檔案後），或掃瞄所修改的檔案
- 擷取時：在檔案開啟時掃瞄
- 在建立/修改和擷取檔案時掃瞄

例如，若選取第三個選項，便會對下載至電腦的新檔案進行掃瞄；若未偵測到安全威脅，則會保留在其原有位置上。當使用者開啟檔案，或使用者修改檔案後要進行儲存前，將會掃瞄該檔案。

要掃瞄的檔案

請選取下列選項：

- 所有可掃瞄的檔案：掃瞄所有檔案
- 智慧型掃瞄所掃瞄的檔案類型：僅掃瞄已知可能含有惡意程式碼的檔案，包括以無害副檔名偽裝的檔案。如需詳細資訊，請參閱 IntelliScan 第 D-6 頁。

- 具有特定副檔名的檔案：僅掃瞄其副檔名列入副檔名清單中的檔案。請新增副檔名，或移除任何現有的副檔名。

掃瞄設定

請選取下列一或多個選項：

- 在系統關機時掃瞄軟碟機：在關閉電腦前掃瞄軟碟機中是否有開機型病毒。如此可防止病毒/惡意程式在使用者透過磁片重新啟動電腦時伺機執行。
- 掃瞄隱藏資料夾：允許 OfficeScan 在「手動掃瞄」期間偵測電腦上的隱藏資料夾，然後加以掃瞄。
- 掃瞄網路磁碟機：在「手動掃瞄」或「即時掃瞄」期間，掃瞄對應至 OfficeScan 用戶端電腦的網路磁碟機或資料夾。
- 在插入 USB 儲存裝置之後掃瞄其開機磁區：在每次使用者插入 USB 儲存裝置時，僅自動掃瞄其開機磁區（即時掃瞄）。
- 掃瞄壓縮檔：允許 OfficeScan 掃瞄指定數目的壓縮層數，並略過超出此數目的任何壓縮層。OfficeScan 也會清除或刪除壓縮檔內的中毒檔案。例如，如果最大層數是兩層，而要掃瞄的壓縮檔有六層，則 OfficeScan 會掃瞄兩層而略過其餘四層。如果壓縮檔包含安全威脅，OfficeScan 會清除或刪除該檔案。

  注意

  OfficeScan 會將 Office Open XML 格式的 Microsoft Office 2007 檔案視為壓縮檔。Office Open XML 使用 ZIP 壓縮技術，是 Office 2007 應用程式的檔案格式。如果要掃瞄使用這些應用程式建立的檔案中是否有病毒/惡意程式，您必須啟動掃瞄壓縮檔。

- 掃瞄 OLE 物件：當檔案包含多個「物件連結與嵌入」(OLE) 層時，OfficeScan 會掃瞄指定數目的層，並略過剩餘的層。

  由伺服器管理的所有 OfficeScan 用戶端在執行「手動掃瞄」、「即時掃瞄」、「預約掃瞄」和「立即掃瞄」期間都會檢查此設定。OfficeScan 會掃瞄每一層是否包含病毒/惡意程式和間諜程式/可能的資安威脅程式。

例如：

您指定的層數是 2。檔案中嵌入的物件是 Microsoft Word 文件（第一層），該 Word 文件又嵌入 Microsoft Excel 試算表（第二層），而試算表中又嵌入 .exe 檔案（第三層）。OfficeScan 將會掃瞄該 Word 文件和 Excel 試算表，並略過該 .exe 檔案。

- 在 OLE 檔案中偵測到弱點攻擊程式碼：OLE 弱點攻擊偵測會檢查 Microsoft Office 檔案中是否有弱點攻擊程式碼，主動發現惡意程式。

  注意

  指定的層數會同時適用於「掃瞄 OLE 物件」和「偵測弱點攻擊程式碼」選項。

- 啟動 IntelliTrap：偵測並移除壓縮可執行檔中的病毒/惡意程式。此選項僅適用於即時掃瞄。如需詳細資訊，請參閱 IntelliTrap 第 D-6 頁。
- 掃瞄開機區：在「手動掃瞄」、「預約掃瞄」與「立即掃瞄」期間，掃瞄用戶端電腦硬碟的開機磁區中是否有病毒/惡意程式。

CPU 使用率

OfficeScan 可在掃瞄某個檔案後、掃瞄下一個檔案之前暫停。「手動掃瞄」、「預約掃瞄」與「立即掃瞄」期間均適用此設定。

請選取下列選項：

- 高：掃瞄之間不暫停
- 中：如果 CPU 耗用大於 50% 便在檔案掃瞄間暫停；如果小於 50% 則不暫停
- 低：如果 CPU 耗用大於 20% 便在檔案掃瞄間暫停；如果小於 20% 則不暫停

如果您選擇「中」或「低」，在掃瞄啟動後若 CPU 耗用在門檻值（50% 或 20%）內，OfficeScan 將不會在掃瞄之間暫停，如此可縮短掃瞄時間。OfficeScan 在此程序中會使用較多的 CPU 資源，但由於 CPU 耗用已最佳化，因此電腦效能不會受到嚴重影響。當 CPU 耗用開始超過門檻值時，OfficeScan 即會暫停以降低 CPU 使用率，而在耗用再度回落在門檻值之內時結束暫停。

如果您選擇「高」，OfficeScan 將不會檢查實際的 CPU 耗用，而會持續掃瞄檔案不暫停。

預約

設定執行「預約掃瞄」的頻率（每天、每週或每月）和時間。

對於每月「預約掃瞄」，您可以選擇月份中的特定日期，或當月中的第幾個星期幾。

- 月份中的特定日期：在第 1 日到第 31 日之間進行選取。如果選取第 29 日、第 30 日或第 31 日，但該月沒有此日期，則 OfficeScan 會在該月最後一天執行「預約掃瞄」。因此：
  - 如果選取第 29 日，則「預約掃瞄」會在 2 月 28 日執行（閏年除外），而對於所有其他月份則在第 29 日執行。
  - 如果選取第 30 日，則「預約掃瞄」會在 2 月 28 或 29 日執行，而對於所有其他月份則在第 30 日執行。
  - 如果選取第 31 日，則「預約掃瞄」會在 2 月 28 或 29 日、4 月 30 日、6 月 30 日、9 月 30 日、11 月 30 日執行，而對於所有其他月份則在第 31 日執行。
- 當月中的第幾個星期幾：一週中的某一天每個月都會出現四或五次。例如：一個月通常有四個星期一。指定當月中的第幾個星期幾。例如：選擇在每個月的第二個星期一執行「預約掃瞄」。如果選擇第五個星期中的某一天，而這一天在特定月份中只出現四次，則掃瞄將於第四個星期中的這一天執行。

掃瞄例外

設定掃瞄例外可提高掃瞄效能，並略過會導致誤判警訊的檔案。在執行特定掃瞄類型時，OfficeScan 會檢查掃瞄例外清單，以判定電腦上有哪些檔案將同時排除在病毒/惡意程式與間諜程式/可能的資安威脅程式掃瞄之外。

當您啟動掃瞄例外時，OfficeScan 將不會掃瞄處於下列情況的檔案：

- 位於特定目錄（或任何其子目錄）下的檔案。

- 檔案名稱符合例外清單中的任何名稱。
- 副檔名符合例外清單中的任何副檔名。

秘訣

如需趨勢科技建議排除在即時掃瞄之外的產品清單，請移至：

http://esupport.trendmicro.com/solution/en-US/1059770.aspx

萬用字元例外

檔案和目錄的掃瞄例外清單支援使用萬用字元。使用「?」字元取代一個字元，使用「*」取代多個字元。

請謹慎使用萬用字元。用錯字元可能會排除不適當的檔案或目錄。例如，C:* 將會不掃瞄整個 C:\ 磁碟機。

表 7-9. 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
c:\director?\file\?.txt	c:\directory\file\1.txt	c:\directory\file\doc.txt c:\directories\file\document.txt
c:*.txt	c:\doc.txt	c:\directory\file\doc.txt c:\directories\files\document.txt

值	已排除	未排除
`[]`	不支援	不支援
`*.*`	不支援	不支援

掃瞄例外清單（目錄）

OfficeScan 不會掃瞄位於電腦上特定目錄下的所有檔案。您最多可以指定 250 個目錄。

注意

OfficeScan 可藉由將目錄從掃瞄任務中排除，來將該目錄的所有子目錄從掃描任務中排除。

您也可以選擇「不掃瞄趨勢科技產品的安裝目錄」。如果您選取此選項，OfficeScan 就會自動將下列趨勢科技產品的目錄排除在掃瞄作業之外：

- <伺服器安裝資料夾>
- ScanMail™ for Microsoft Exchange（除了第 7 版以外的所有版本）。如果您使用的是第 7 版，請將下列資料夾新增至例外清單：
  - `\Smex\Temp`
  - `\Smex\Storage`
  - `\Smex\ShareResPool`
- ScanMail eManager™ 3.11、5.1、5.11、5.12
- ScanMail for Lotus Notes™ eManager NT
- InterScan™ Messaging Security Suite
- InterScan Web Security Suite
- InterScan Web Protect
- InterScan VirusWall 3.53

- InterScan FTP VirusWall
- InterScan Web VirusWall
- InterScan E-mail VirusWall
- InterScan NSAPI Plug-in
- InterScan eManager 3.5x

如果您的趨勢科技產品「不」包含在此清單中，請將該產品目錄新增到掃瞄例外清單。

此外，請移至用戶端電腦 > 全域用戶端設定的「掃瞄設定」區段，來設定 OfficeScan 以排除 Microsoft Exchange 2000/2003 目錄。如果您使用 Microsoft Exchange 2007 或更新版本，請手動將目錄新增至掃瞄例外清單中。如需掃瞄例外的詳細資訊，請參閱下列網站：

http://technet.microsoft.com/en-us/library/bb332342.aspx

設定檔案清單時，請從下列選項進行選擇：

- 保留用戶端電腦的例外清單：這是預設的選取項目。如果對例外清單進行了變更，並啟動了此選項，將無法儲存變更。此選項之提供，是為了防止意外覆寫用戶端的現有例外清單。如果要部署所做的變更，請選取其他任何選項。
- 覆寫用戶端電腦的例外清單：此選項會移除用戶端上的整個例外清單，並使用剛設定的清單取而代之。如果選擇此選項，OfficeScan 會顯示警告。如果要繼續，必須在訊息視窗中按一下「確定」。
- 將路徑新增至用戶端電腦的例外清單：此選項會將您剛設定的清單中項目新增至用戶端的現有例外清單。如果某個項目已存在於用戶端的例外清單中，則用戶端會略過該項目。
- 從用戶端電腦的例外清單中移除路徑：用戶端會移除其例外清單中的項目，只要該項目符合您剛設定的清單中項目。

掃瞄例外清單（檔案）

如果檔案的名稱符合此例外清單中包含的任何名稱，OfficeScan 即不會掃瞄該檔案。如果要排除位於電腦上特定位置下的檔案，請納入檔案路徑，如 `C:\Temp\sample.jpg`。

您最多可以指定 250 個檔案。

設定檔案清單時，請從下列選項進行選擇：

- 保留用戶端電腦的例外清單：這是預設的選取項目。如果對例外清單進行了變更，並啟動了此選項，將無法儲存變更。此選項之提供，是為了防止意外覆寫用戶端的現有例外清單。如果要部署所做的變更，請選取其他任何選項。
- 覆寫用戶端電腦的例外清單：此選項會移除用戶端上的整個例外清單，並使用剛設定的清單取而代之。如果選擇此選項，OfficeScan 會顯示警告。如果要繼續，必須在訊息視窗中按一下「確定」。
- 將路徑新增至用戶端電腦的例外清單：此選項會將您剛設定的清單中項目新增至用戶端的現有例外清單。如果某個項目已存在於用戶端的例外清單中，則用戶端會略過該項目。
- 從用戶端電腦的例外清單中移除路徑：用戶端會移除其例外清單中的項目，只要該項目符合您剛設定的清單中項目。

掃瞄例外清單（副檔名）

如果檔案的副檔名符合此例外清單中包含的任何副檔名，OfficeScan 即不會掃瞄該檔案。您最多可以指定 250 個副檔名。副檔名之前不需要加句號 (.)。

若為「即時掃瞄」，請在指定副檔名時使用星號 (*) 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*`。

若為「手動掃瞄」、「預約掃瞄」與「立即掃瞄」，請使用問號 (?) 或星號 (*) 做為萬用字元。

套用掃瞄例外設定至所有掃瞄類型

OfficeScan 可讓您為特定掃瞄類型設定掃瞄例外設定，然後將相同的設定套用至所有其他的掃瞄類型。例如：

OfficeScan 管理員 Chris 於 1 月 1 日發現用戶端電腦上有大量的 JPG 檔案，並確認這些檔案不具任何安全威脅。Chris 將 JPG 新增至「手動掃瞄」的檔案例外清單中，然後將此設定套用至所有掃瞄類型。此時，「即時掃瞄」、「立即掃瞄」與「預約掃瞄」均已設定成略過 .jpg 檔案的掃瞄。

一週後，Chris 從「即時掃瞄」的例外清單中移除了 JPG，但並未將掃瞄例外設定套用至所有掃瞄類型。現在將會掃瞄 JPG 檔案，但僅限於「即時掃瞄」期間。

中毒處理行動

指定 OfficeScan 在特定掃瞄類型偵測到安全威脅時所執行的處理行動。OfficeScan 針對病毒/惡意程式和間諜程式/可能的資安威脅程式有不同的中毒處理行動集。

病毒/惡意程式中毒處理行動

OfficeScan 執行的中毒處理行動視病毒/惡意程式種類和偵測到病毒/惡意程式的掃瞄類型而定。例如，當 OfficeScan 在手動掃瞄（掃瞄類型）過程中偵測到特洛伊木馬程式（病毒/惡意程式類型）時，會清除（中毒處理行動）中毒的檔案。

如需不同病毒/惡意程式類型的詳細資訊，請參閱病毒和惡意程式 第 7-2 頁。

下列是 OfficeScan 可針對病毒/惡意程式執行的處理行動：

表 7-10. 病毒/惡意程式中毒處理行動

處理行動	說明
刪除	OfficeScan 會刪除中毒的檔案。

處理行動	說明
隔離	OfficeScan 會重新命名中毒的檔案，再將這些檔案移至用戶端電腦上位於 <用戶端安裝資料夾>\Suspect 下的暫時隔離目錄。 然後，OfficeScan 用戶端會將已隔離的檔案傳送到指定的隔離目錄。如需詳細資訊，請參閱隔離目錄 第 7-37 頁。 預設隔離目錄在 OfficeScan 伺服器上的<伺服器安裝資料夾>\PCCSRV\Virus 下。OfficeScan 會加密傳送至此目錄的隔離檔案。 如果您需要恢復任何已隔離的檔案，請使用 VSEncrypt 工具。如需使用此工具的詳細資訊，請參閱 Server Tuner 第 13-41 頁。
清除	OfficeScan 會先清除中毒的檔案，才允許完整存取該檔案。 如果無法清除檔案，OfficeScan 會執行第二個中毒處理行動，可能是下列其中一個中毒處理行動：隔離、刪除、重新命名與暫不處理。如果要設定第二個中毒處理行動，請移至用戶端電腦 > 用戶端管理。按一下「 設定 > 掃瞄設定 > ｛掃瞄類型｝ > 處理行動 」標籤。 系統可對所有類型的惡意程式（但不包括可能的病毒/惡意程式）執行此處理行動。
重新命名	OfficeScan 會將中毒檔案的副檔名變更為「vir」。使用者一開始無法開啟重新命名的檔案，但是如果使檔案與特定的應用程式產生關聯，就可以開啟該檔案。 開啟重新命名的中毒檔案時，可能會執行病毒/惡意程式。
暫不處理	OfficeScan 只有在「手動掃瞄」、「預約掃瞄」和「立即掃瞄」過程中偵測到任何類型的病毒時，才可以使用此中毒處理行動。OfficeScan 在即時掃瞄過程中無法使用此中毒處理行動，因為在偵測到嘗試開啟或執行中毒的檔案時，若未執行任何中毒處理行動，則會允許執行病毒/惡意程式。「即時掃瞄」過程中可以使用其他所有的中毒處理行動。
拒絕存取	此中毒處理行動只能在「即時掃瞄」過程中執行。當 OfficeScan 偵測到嘗試開啟或執行中毒的檔案時，會立即阻止該操作。 使用者可以手動刪除中毒的檔案。

使用主動式處理行動

不同類型的病毒/惡意程式需要不同的中毒處理行動。自訂中毒處理行動需要有病毒/惡意程式的知識，並且可能會是冗長而乏味的工作。OfficeScan 會使用「主動式處理行動」來對抗這些問題。

「主動式處理行動」是一套預先設定的中毒處理行動，可以處理病毒/惡意程式。如果您不熟悉中毒處理行動，或是不確定何種中毒處理行動適合那一種特定的病毒/惡意程式，趨勢科技建議您使用「主動式處理行動」。

使用「主動式處理行動」具有以下優點：

- 「主動式處理行動」會使用趨勢科技建議的中毒處理行動。您不需要耗費時間來設定中毒處理行動。
- 病毒撰寫者會不斷變更病毒/惡意程式攻擊電腦的方式。更新「主動式處理行動」設定以抵禦最新威脅和最新的病毒/惡意程式攻擊方法。

注意

進行間諜程式/可能的資安威脅程式掃瞄時，無法使用主動式處理行動。

下表說明「主動式處理行動」處理每種類型病毒/惡意程式的方式：

表 7-11. 趨勢科技建議的病毒/惡意程式中毒處理行動

病毒/惡意程式類型	即時掃瞄		手動掃瞄/預約掃瞄/立即掃瞄	
	第一個中毒處理行動	第二個中毒處理行動	第一個中毒處理行動	第二個中毒處理行動
惡作劇程式	隔離	刪除	隔離	刪除
特洛伊木馬程式	隔離	刪除	隔離	刪除
病毒	清除	隔離	清除	隔離
測試病毒	拒絕存取	無	無	無
封裝程式	隔離	無	隔離	無
其他	清除	隔離	清除	隔離

病毒/惡意程式類型	即時掃瞄		手動掃瞄/預約掃瞄/立即掃瞄	
	第一個中毒處理行動	第二個中毒處理行動	第一個中毒處理行動	第二個中毒處理行動
可能的病毒/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

對於可能的病毒/惡意程式，即時掃瞄期間的預設處理行動是「拒絕存取」，而手動掃瞄、預約掃瞄和立即掃瞄期間的預設處理行動是「暫不處理」。如果這些不是您的偏好處理行動，可以將其變更為「隔離」、「刪除」或「重新命名」。

對所有的病毒/惡意程式類型使用相同的處理行動

如果您要對可能的病毒/惡意程式以外的所有病毒/惡意程式類型執行相同的處理行動，請選取此選項。若您選擇「清除」做為第一個處理行動，請選取清除不成功時 OfficeScan 所要執行的第二個處理行動。如果第一個處理行動不是「清除」，則無法設定第二個處理行動。

如果選擇「清除」作為第一項處理行動，則 OfficeScan 在偵測到可能的病毒/惡意程式時會執行第二項處理行動。

對每個病毒/惡意程式類型使用特定的處理行動

針對每一種病毒/惡意程式類型手動選取中毒處理行動。

對於可能的病毒/惡意程式以外的全部病毒/惡意程式類型，所有中毒處理行動均可用。若您選擇「清除」做為第一個處理行動，請選取清除不成功時 OfficeScan 所要執行的第二個處理行動。如果第一個處理行動不是「清除」，則無法設定第二個處理行動。

對於可能的病毒/惡意程式，「清除」以外的所有中毒處理行動均可用。

隔離目錄

如果中毒檔案的處理行動為「隔離」，OfficeScan 用戶端即會加密該檔案，並將其移至 <伺服器安裝資料夾>\SUSPECT 下的暫時隔離資料夾，然後將檔案傳送至指定的隔離目錄。

注意

您可以在日後需要存取加密的隔離檔案時加以恢復。如需詳細資訊，請參閱還原加密檔案 第 7-40 頁。

接受位於 OfficeScan 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，則使用主機名稱，以便全部用戶端都可以將隔離檔案傳送到該伺服器。
- 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 和雙堆疊用戶端可以將隔離檔案傳送到該伺服器。
- 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 和雙堆疊用戶端可以將隔離檔案傳送到該伺服器。

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。用戶端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用戶端和純 IPv6 用戶端的隔離檔案，此目錄應具有 IPv6 位址。趨勢科技建議指定雙堆疊替代目錄、透過其主機名稱識別目錄並在輸入目錄時使用 UNC 路徑。

如需何時應使用 URL、UNC 路徑或絕對檔案路徑的相關指引，請參閱下表：

表 7-12. 隔離目錄

隔離目錄	接受的格式	範例	注意
OfficeScan 伺服器電腦上的目錄	URL	`http://<osceserver>`	這是預設的目錄。 進行此目錄的設定，如隔離資料夾的大小等。如需詳細資訊，請參閱隔離區管理員 第 13-40 頁。
	UNC 路徑	`\\<osceserver>\ofcscan\Virus`	

隔離目錄	接受的格式	範例	注意
其他 OfficeScan 伺服器電腦上的目錄（若您在網路上有其他 OfficeScan 伺服器）	URL	`http://<osceserver2>`	確定用戶端可連線到此目錄。如果您指定不正確的目錄，OfficeScan 用戶端會將已隔離的檔案保留在 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`	
網路上的另一部電腦	UNC 路徑	`\\<computer_name>\temp`	
OfficeScan 用戶端上的其他目錄	絕對路徑	`C:\temp`	

清除前先備份檔案

如果 OfficeScan 設定為清除中毒的檔案，它將會先備份檔案。這可讓您在日後需要檔案時加以恢復。OfficeScan 會加密備份檔案以防止他人開啟，然後將檔案儲存在 <用戶端安裝資料夾>\Backup 資料夾中。

如果要恢復加密的備份檔案，請參閱還原加密檔案 第 7-40 頁。

損害清除及復原服務

損害清除及復原服務會清除電腦上的 File-based 和網路病毒，以及殘存病毒和蠕蟲（特洛伊木馬程式、登錄項目、病毒檔案）。

用戶端會在病毒/惡意程式掃瞄之前或之後觸發損害清除及復原服務，具體取決於掃瞄類型。

- 當手動掃瞄、預約掃瞄或立即掃瞄執行時，OfficeScan 用戶端會先觸發損害清除及復原服務，然後繼續執行病毒/惡意程式掃瞄。在病毒/惡意程式掃瞄期間，如果需要進行清除，用戶端可能會再次觸發損害清除及復原服務。
- 在即時掃瞄期間，如果需要進行清除，OfficeScan 用戶端會先執行病毒/惡意程式掃瞄，然後觸發損害清除及復原服務。

您可以選取損害清除及復原服務執行的清除類型：

- 標準清除：OfficeScan 用戶端會在標準清除期間執行下列任何的處理行動：
  - 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，OfficeScan 用戶端還會遏止詐欺安全軟體（亦稱為 FakeAV）的活動。OfficeScan 用戶端也會使用進階清除規則來主動偵測並停止出現 FakeAV 行為的應用程式。

注意

提供主動式安全防護的同時，進階清除也會導致大量誤報。

損害清除及復原服務不會對可能的病毒/惡意程式執行清除，除非選取「偵測到可能的病毒/惡意程式時執行清除」選項。只有對可能的病毒/惡意程式的處理行動不是「暫不處理」也不是「拒絕存取」時，才能選取該選項。例如，如果 OfficeScan 用戶端在即時掃瞄期間偵測到可能的病毒/惡意程式，且處理行動為「隔離」，則 OfficeScan 用戶端會先隔離中毒檔案，然後根據需要執行清除。清除類型（標準或進階）取決於您的選擇。

偵測到病毒/惡意程式時顯示通知訊息

OfficeScan 若在「即時掃瞄」與「預約掃瞄」期間偵測到病毒/惡意程式，它會顯示通知訊息，讓使用者得知偵測的相關資訊。

如果要修改通知訊息，請移至「 通知 > 用戶端使用者通知 」中的「 病毒/惡意程式 」標籤。

偵測到可能的病毒/惡意程式時顯示通知訊息

OfficeScan 若在「即時掃瞄」與「預約掃瞄」期間偵測到可能的病毒/惡意程式，它會顯示通知訊息，讓使用者得知偵測的相關資訊。

如果要修改通知訊息，請移至「 通知 > 用戶端使用者通知 」中的「 病毒/惡意程式 」標籤。

還原加密檔案

為了防止開啟中毒檔案，OfficeScan 會在下列情況下加密檔案：

- 隔離檔案前
- 在清除檔案前加以備份時

OfficeScan 所提供的工具可讓您將檔案解密，然後在您需要擷取檔案的資訊時恢復檔案。OfficeScan 可以解密及恢復下列檔案：

表 7-13. OfficeScan 可解密及恢復的檔案

檔案	說明
用戶端電腦上的隔離檔案	這些檔案位於<用戶端安裝資料夾>\SUSPECT\Backup 資料夾中，會在 7 天後自動清除。這些檔案也會上傳至 OfficeScan 伺服器上的指定隔離目錄。
指定隔離目錄中的隔離檔案	依預設，此目錄位於 OfficeScan 伺服器電腦上。如需詳細資訊，請參閱隔離目錄 第 7-37 頁。
備份的加密檔案	這些是 OfficeScan 可清除之中毒檔案的備份。這些檔案位於<用戶端安裝資料夾>\Backup 資料夾中。如果要恢復這些檔案，使用者必須將其移至<用戶端安裝資料夾>\SUSPECT\Backup 資料夾中。 您必須在「 用戶端電腦 > 用戶端管理>設定 > 掃瞄設定 > {掃瞄類型} > 處理行動 」標籤中選取「清除前先備份檔案」，OfficeScan 才會在清除前先備份並加密檔案。

警告!

恢復中毒檔案可能會將病毒/惡意程式散佈到其他檔案與電腦。在恢復檔案前，請先隔離中毒的電腦，並將此電腦上的重要檔案移至備份位置。

解密和恢復檔案

程序

- 如果檔案位於 OfficeScan 用戶端電腦上：
  a. 開啟命令提示字元，然後瀏覽至<用戶端安裝資料夾>。
  b. 輸入下列命令，以執行 `VSEncode.exe`：

     ```
     VSEncode.exe /u
     ```

     此參數會開啟一個畫面，其中顯示位於<用戶端安裝資料夾>\SUSPECT\Backup 下的檔案清單。
  c. 選取要恢復的檔案，然後按一下「恢復」。此工具一次只能恢復一個檔案。
  d. 在開啟的畫面中，指定要將檔案恢復到哪個資料夾。
  e. 按一下「確定」。檔案即會恢復到指定的資料夾。

     注意

     在檔案恢復後，OfficeScan 有可能重新掃瞄該檔案，並將其視為中毒檔案。為了防止該檔案遭到掃瞄，請將其新增至掃瞄例外清單中。如需詳細資訊，請參閱掃瞄例外 第 7-28 頁。
  f. 完成檔案恢復後，請按一下「關閉」。
- 如果檔案位於 OfficeScan 伺服器或自訂的隔離目錄中：
  a. 如果檔案位於 OfficeScan 伺服器電腦上，請開啟命令提示字元，然後瀏覽至<伺服器安裝資料夾>\PCCSRV\Admin\Utility\VSEncrypt。

如果檔案位於自訂的隔離目錄中，請瀏覽至<伺服器安裝資料夾>\PCCSRV\Admin\Utility，然後將 VSEncrypt 資料夾複製到自訂隔離目錄所在的電腦上。

b. 建立文字檔，然後輸入要加密或解密的檔案的完整路徑。

例如，如果要恢復 C:\My Documents\Reports 中的檔案，請在文字檔中輸入 C:\My Documents\Reports*.*。

OfficeScan 伺服器電腦上的隔離檔案位於<伺服器安裝資料夾>\PCCSRV\Virus 下。

c. 以 INI 或 TXT 副檔名儲存文字檔。例如，您可以在 C: 磁碟機上將其儲存為 ForEncryption.ini 磁碟機。

d. 開啟命令提示字元，然後瀏覽至 VSEncrypt 資料夾所在的目錄。

e. 輸入下列命令，以執行 VSEncode.exe：

```
VSEncode.exe /d /i <INI 或 TXT 檔案的位置>
```

說明：

<INI 或 TXT 檔案的位置>就是您建立的 INI 或 TXT 檔案的路徑（例如：C:\ForEncryption.ini）。

f. 使用其他參數發出各種命令。

表 7-14. 恢復參數

參數	說明
無（沒有參數）	加密檔案
/d	解密檔案
/debug	建立偵錯記錄檔，並將其儲存至電腦。在 OfficeScan 用戶端電腦上，偵錯記錄檔 VSEncrypt.log 會建立於 <用戶端安裝資料夾>。
/o	覆寫已存在的加密或解密檔案
/f <檔案名稱>	加密或解密單一檔案
/nr	不恢復原始檔名

參數	說明
/v	顯示工具的相關資訊
/u	啟動工具的使用者介面
/r <目標資料夾>	用以恢復檔案的資料夾
/s <原始檔名>	原始加密檔案的檔名

例如，輸入 `VSEncode [/d] [/debug]`，可以解密 `Suspect` 資料夾中的檔案，並建立偵錯記錄檔。當您解密或加密檔案時，OfficeScan 便會在相同資料夾中建立解密或加密檔案。在解密或加密檔案前，請確認檔案並未鎖定。

間諜程式/可能的資安威脅程式中毒處理行動

OfficeScan 執行的中毒處理行動視偵測到間諜程式/可能的資安威脅程式的掃瞄類型而定。您可以為每個病毒/惡意程式類型設定特定的處理行動，但對於所有類型的間諜程式/可能的資安威脅程式，則只能設定一個處理行動（如需不同間諜程式/可能的資安威脅程式類型的詳細資訊，請參閱間諜程式和可能的資安威脅程式 第 7-4 頁）。例如，當 OfficeScan 在「手動掃瞄」（掃瞄類型）過程中偵測到任何類型的間諜程式/可能的資安威脅程式時，會清除（中毒處理行動）受影響的系統資源。

下列是 OfficeScan 可針對間諜程式/可能的資安威脅程式執行的處理行動：

表 7-15. 間諜程式/可能的資安威脅程式中毒處理行動

處理行動	說明
清除	OfficeScan 會終止程序或刪除登錄、檔案、Cookie 和捷徑。 在清除間諜程式/可能的資安威脅程式後，OfficeScan 用戶端會備份間諜程式/可能的資安威脅程式資料，如果您認為可安全存取這些間諜程式/可能的資安威脅程式，便可恢復這些資料。如需詳細資訊，請參閱回存間諜程式/可能的資安威脅程式 第 7-46 頁。

處理行動	說明
暫不處理	OfficeScan 不會對偵測到的間諜程式/可能的資安威脅程式元件執行任何中毒處理行動，但是會在記錄檔中記錄偵測到間諜程式/可能的資安威脅程式。此處理行動只能在「手動掃瞄」、「預約掃瞄」與「立即掃瞄」期間執行。在「即時掃瞄」期間，處理行動為「拒絕存取」。 如果偵測到的間諜程式/可能的資安威脅程式包含在核可清單中，OfficeScan 將不會執行任何處理行動。如需詳細資訊，請參閱間諜程式/可能的資安威脅程式核可清單 第 7-44 頁。
拒絕存取	OfficeScan 會拒絕存取（複製、開啟）偵測到的間諜程式/可能的資安威脅程式元件。此處理行動只能在「即時掃瞄」期間執行。在「手動掃瞄」、「預約掃瞄」和「立即掃瞄」期間，處理行動為「暫不處理」。

偵測到間諜程式/可能的資安威脅程式時顯示通知訊息

OfficeScan 若在「即時掃瞄」與「預約掃瞄」期間偵測到間諜程式/可能的資安威脅程式，它會顯示通知訊息，讓使用者得知偵測的相關資訊。

如果要修改通知訊息，請移至「即時掃瞄通知 > 用戶端使用者通知」，然後按一下「間諜程式/可能的資安威脅程式」標籤。

間諜程式/可能的資安威脅程式核可清單

OfficeScan 會提供「許可的」間諜程式/可能的資安威脅程式清單，其中包含您不希望被視為間諜程式/可能的資安威脅程式的檔案或應用程式。在掃瞄期間偵測到特定的間諜程式/可能的資安威脅程式時，OfficeScan 會檢查核可清單，如果在核可清單中找到相符項目，則不會執行任何處理行動。

請將核可清單套用至一或多個用戶端與網域，或套用至伺服器管理的所有用戶端。將核可清單套用至所有的掃瞄類型，表示在「手動掃瞄」、「即時掃瞄」、「預約掃瞄」與「立即掃瞄」期間，都將使用相同的核可清單。

將已偵測到的間諜程式/可能的資安威脅程式加入核可清單

程序

1. 瀏覽至下列其中一個項目：
   - 「用戶端電腦 > 用戶端管理」
   - 記錄檔 > 用戶端電腦記錄檔 > 安全威脅
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「記錄檔 > 間諜程式/可能的資安威脅程式記錄檔」或「檢視記錄檔 > 間諜程式/可能的資安威脅程式記錄檔」。
4. 指定記錄條件，然後按一下「顯示記錄檔」。
5. 選取記錄檔，然後按一下「新增到核可清單」。
6. 只將許可的間諜程式/可能的資安威脅程式套用至選取的用戶端電腦，或是套用至特定網域。
7. 按一下「儲存」。選取的用戶端會套用該設定，OfficeScan 伺服器會將間諜程式/可能的資安威脅程式新增至「用戶端電腦 > 用戶端管理」 >「設定 > 間諜程式/可能的資安威脅程式核可清單」中找到的核可清單。

注意

OfficeScan 最多可在核可清單中容納 1024 個間諜程式/可能的資安威脅程式。

管理間諜程式/可能的資安威脅程式核可清單

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。

2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。

3. 按一下「設定 > 間諜程式/可能的資安威脅程式核可清單」。

4. 在「間諜程式/可能的資安威脅程式名稱」表格中，選取間諜程式/可能的資安威脅程式名稱。如果要選取多個名稱，請按住 Ctrl 鍵並進行選取。

   - 您也可以在「搜尋」欄位中輸入關鍵字，然後按一下「搜尋」。OfficeScan 會以符合關鍵字的名稱重新整理表格。

5. 按一下「新增」。

   名稱會移至「核可清單」表格中。

6. 如果要從核可清單移除名稱，請選取名稱並按一下「移除」。如果要選取多個名稱，請按住 Ctrl 鍵並進行選取。

7. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。

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

回存間諜程式/可能的資安威脅程式

清除間諜程式/可能的資安威脅程式後，OfficeScan 用戶端會備份間諜程式/可能的資安威脅程式資料。如果您認為資料無害，請通知線上用戶端恢復備份資料。請根據備份時間選擇要恢復的間諜程式/可能的資安威脅程式資料。

注意

OfficeScan 用戶端使用者無法開始間諜程式/可能的資安威脅程式恢復，而且不會接獲用戶端能夠恢復哪些備份資料的通知。

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，開啟某個網域，然後選取用戶端。

   注意

   每次只有一個用戶端可以執行間諜程式/可能的資安威脅程式恢復。

3. 按一下「工作 > 間諜程式/可能的資安威脅程式恢復」。
4. 如果要檢視各資料區段所要恢復的項目，請按一下「檢視」。

   接著會顯示一個新畫面。按一下「返回」可回到上一個畫面。
5. 選取您要恢復的資料區段。
6. 按一下「恢復」。

   OfficeScan 會通知您恢復狀態。請檢查間諜程式/可能的資安威脅程式的恢復記錄檔，以取得完整報告。如需詳細資訊，請參閱檢視間諜程式/可能的資安威脅程式恢復記錄檔 第 7-88 頁。

掃瞄權限和其他設定

具有掃瞄權限的使用者，比較能控制掃瞄其電腦上的檔案的方式。具有掃瞄權限的使用者或 OfficeScan 用戶端可以執行下列工作：

- 使用者可以設定「手動掃瞄」、「預約掃瞄」與「即時掃瞄」設定。如需詳細資訊，請參閱掃瞄類型權限 第 7-48 頁。
- 使用者可以延後、停止或略過預約掃瞄。如需詳細資訊，請參閱預約掃瞄權限和其他設定 第 7-51 頁。
- 使用者可啟動 Microsoft Outlook 與 POP3 電子郵件訊息的病毒/惡意程式掃瞄。如需詳細資訊，請參閱郵件掃瞄權限和其他設定 第 7-57 頁。

- OfficeScan 用戶端可以使用快取設定來提高其掃瞄效能。如需詳細資訊，請參閱用於掃瞄的快取設定 第 7-59 頁。

掃瞄類型權限

允許使用者設定自己的手動掃瞄、即時掃瞄和預約掃瞄設定。

授與掃瞄類型權限

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 權限和其他設定」。
4. 在「使用權限」標籤中，移至「掃瞄權限」區段。
5. 選取允許使用者設定的掃瞄類型。
6. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

設定 OfficeScan 用戶端電腦的掃瞄設定

程序

1. 以滑鼠右鍵按一下系統匣上的 OfficeScan 用戶端圖示，然後選取「OfficeScan 主控台」。
2. 按一下「設定 > {掃瞄類型}」。

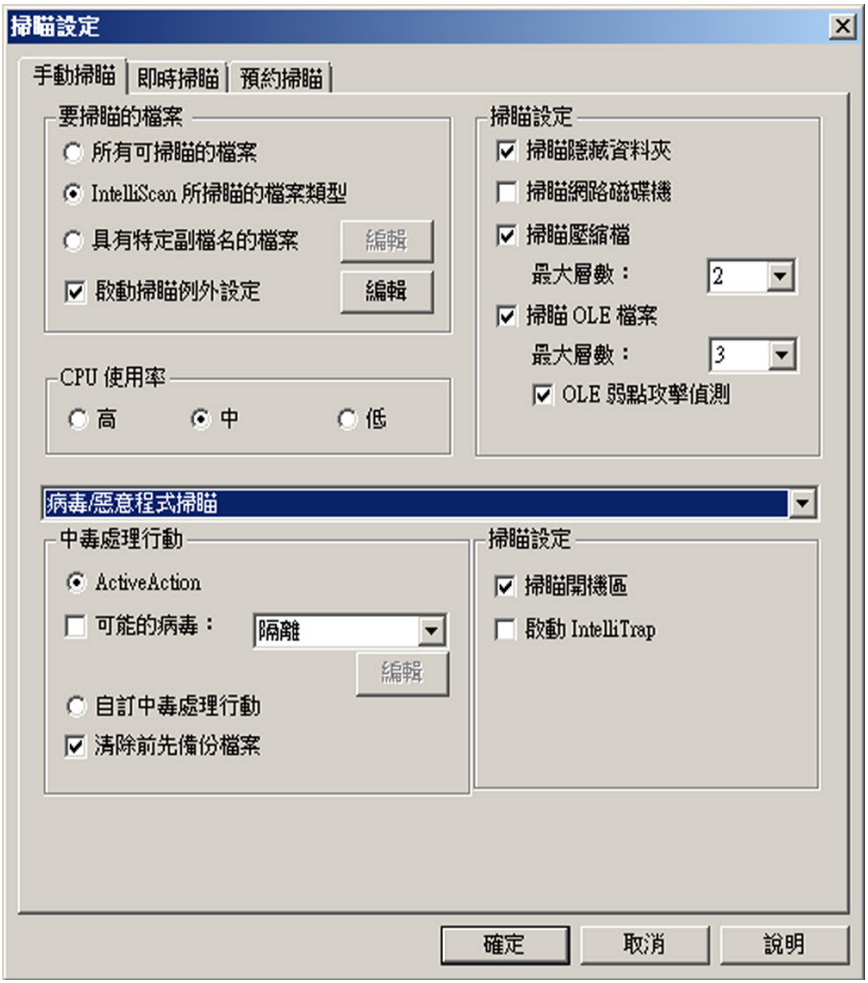


圖 7-1. OfficeScan 用戶端主控台上的掃瞄設定

3. 設定下列設定：

   - 手動掃瞄設定：要掃瞄的檔案、掃瞄設定、CPU 使用率、掃瞄例外、中毒處理行動

- 即時掃瞄設定：使用者對檔案執行的活動、要掃瞄的檔案、掃瞄設定、掃瞄例外、中毒處理行動
- 預約掃瞄設定：預約、要掃瞄的檔案、掃瞄設定、CPU 使用率、掃瞄例外、中毒處理行動

4. 按一下「確定」。

預約掃瞄權限和其他設定

如果設定在用戶端上執行預約掃瞄，使用者可以延後和略過/停止預約掃瞄。

延後預約掃瞄

具有「延後預約掃瞄」權限的使用者可以執行下列動作：

- 在預約掃瞄開始前將其延後，並指定延後時間長度。「預約掃瞄」功能只能延後一次。
- 如果「預約掃瞄」正在進行中，使用者可以停止掃瞄並稍後重新啟動。使用者可以接著指定掃瞄重新開始之前應該經過的時間長度。一旦掃瞄重新啟動，先前掃瞄過的所有檔案都會重新掃瞄一遍。「預約掃瞄」只能停止並重新啟動一次。

注意

使用者可以指定的延後時間長度與經過時間長度下限為 15 分鐘。您可前往用戶端電腦 > 全域用戶端設定以減少 12 小時又 45 分鐘的上限數。在「預約掃瞄設定」區段中，修改「延後預約掃瞄最多 __ 小時又 __ 分鐘」的設定。

略過及停止預約掃瞄

此權限允許使用者執行以下動作：

- 在預約掃瞄執行之前予以略過

- 停止進行中的預約掃瞄

預約掃瞄權限通知

如果要允許使用者使用預約掃瞄權限，請設定 OfficeScan 在執行「預約掃瞄」之前顯示通知訊息，提醒他們您授與他們的權限。

授與預約掃瞄權限並顯示權限通知

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 權限和其他設定」。
4. 在「使用權限」標籤中，移至「預約掃瞄權限」區段。
5. 選取下列選項：
   - 延後預約掃瞄
   - 略過及停止預約掃瞄
6. 按一下「其他設定」，並移至「預約掃瞄設定」區段。
7. 選取「執行預約掃瞄之前顯示通知」。

   啟動此選項時，開始執行「預約掃瞄」前數分鐘會在用戶端電腦上顯示通知訊息。這時使用者會收到有關掃瞄預約時程（日期與時間）及其「預約掃瞄」權限（例如：延後、略過，或是停止預約掃瞄）的通知。

注意

您可以設定分鐘數。如果要設定分鐘數，請移至 用戶端電腦 > 全域用戶端設定。在預約掃瞄設定區段中，修改「在預約掃瞄開始前 __ 分鐘提醒使用者」的設定。

8. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

在用戶端電腦延後/略過及停止預約掃瞄

程序

- 如果預約掃瞄尚未開始：

  a. 以滑鼠右鍵按一下系統匣上的 OfficeScan 用戶端圖示，並選取「預約掃瞄進階設定」。

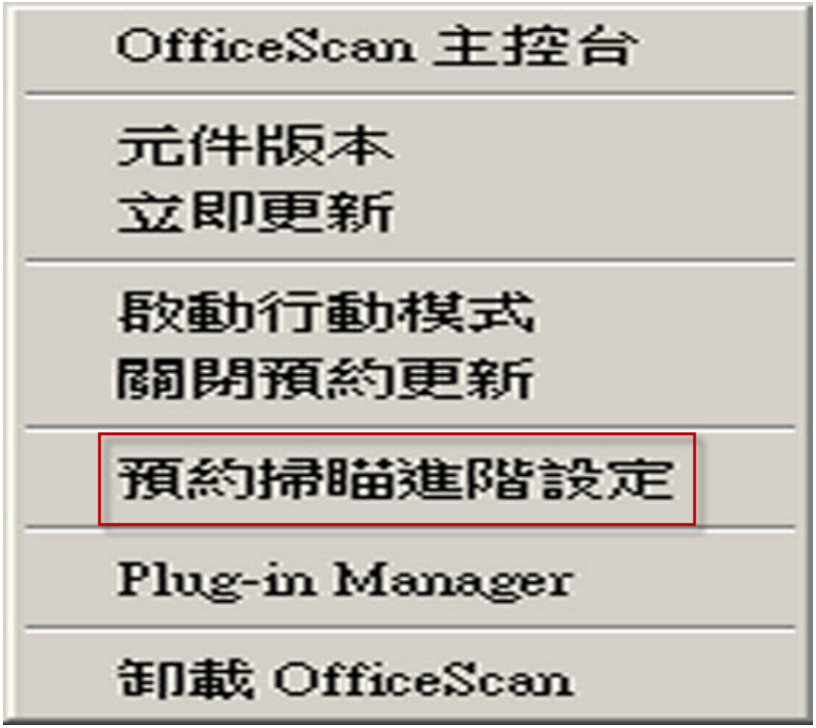


圖 7-2. 「預約掃瞄進階設定」選項

注意

如果通知訊息已啟動並設定為在開始執行「預約掃瞄」前數分鐘顯示，則使用者不需要執行此步驟。如需有關通知訊息的詳細資訊，請參閱預約掃瞄權限通知 第 7-52 頁。

b. 在顯示的通知視窗上，選取下列其中一個選項：

- 延後掃瞄 __ 小時 __ 分鐘。
- 略過此預約掃瞄。下一次預約掃瞄將在 <date> 的 <time> 執行。

圖 7-3. OfficeScan 用戶端電腦上的預約掃瞄權限

- 如果預約掃瞄正在進行：

  a. 以滑鼠右鍵按一下系統匣上的 OfficeScan 用戶端圖示，並選取「預約掃瞄進階設定」。

  b. 在顯示的通知視窗上，選取下列其中一個選項：

     - 停止掃瞄。在此時間後重新啟動掃瞄：__ 小時 __ 分鐘。
     - 停止掃瞄。下一次預約掃瞄將在 <date> 的 <time> 執行。

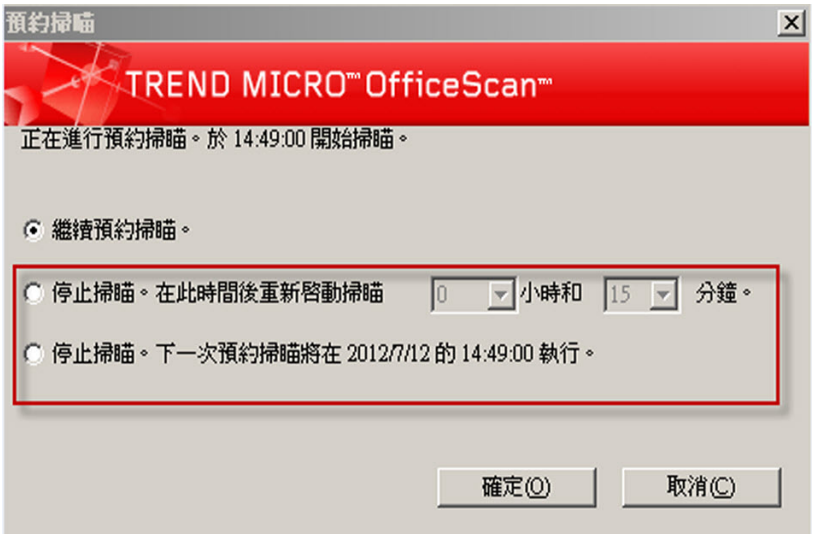


圖 7-4. OfficeScan 用戶端電腦上的預約掃瞄權限

郵件掃瞄權限和其他設定

當用戶端具有「郵件掃瞄」權限時，OfficeScan 用戶端主控台會顯示「郵件掃瞄」標籤。「郵件掃瞄」標籤會顯示兩個郵件掃瞄程式，即 Outlook 郵件掃瞄和 POP3 郵件掃瞄。

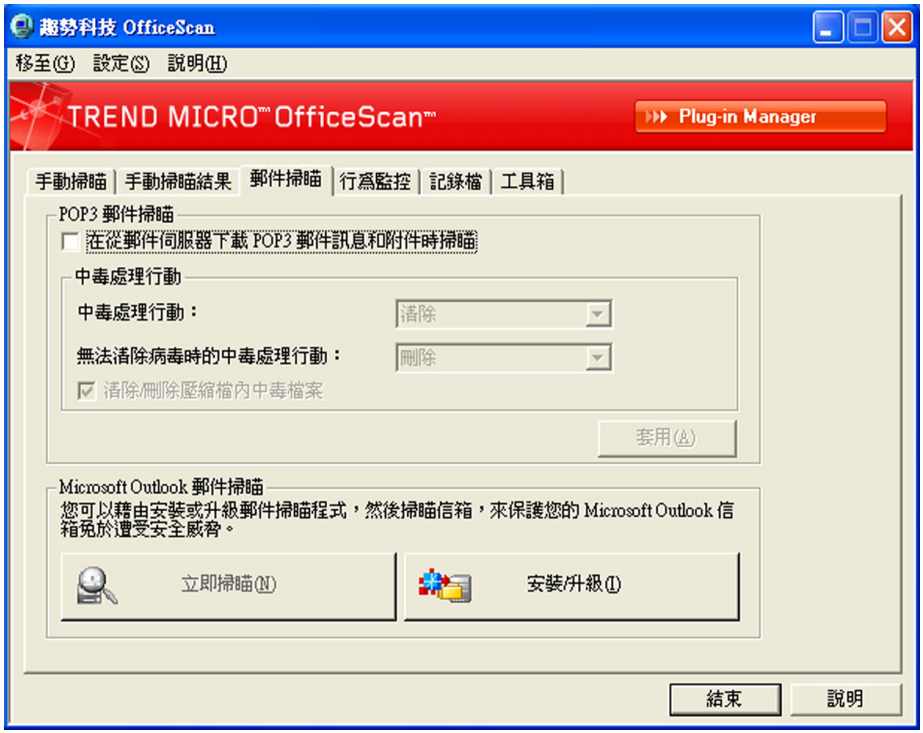


圖 7-5. OfficeScan 用戶端主控台上的「郵件掃瞄」標籤

下表說明 Outlook 郵件掃瞄和 POP3 郵件掃瞄程式。

表 7-16. 郵件掃瞄程式

詳細資訊	OUTLOOK 郵件掃瞄	POP3 郵件掃瞄
用途	掃瞄 Microsoft Outlook 電子郵件中是否存在病毒/惡意程式	掃瞄 POP3 電子郵件訊息中是否有病毒/惡意程式
先決條件	必須先由使用者從 OfficeScan 用戶端主控台進行安裝，然後才能使用該程式	• 必須先由管理員從 Web 主控台將其啟動，然後使用者才能使用該程式 注意 如果要啟動 POP3 郵件掃瞄，請參閱授與郵件掃瞄權限和啟動 POP3 郵件掃瞄 第 7-59 頁。 • 您可以從 OfficeScan 用戶端主控台設定針對病毒/惡意程式的處理行動，但無法從 Web 主控台進行設定
支援的掃瞄類型	手動掃瞄 只有在使用者按一下 OfficeScan 用戶端主控台上的「郵件掃瞄」標籤中的「立即掃瞄」時，才會執行掃瞄。	即時掃瞄 從 POP3 郵件伺服器擷取電子郵件時，便會執行掃瞄。
掃瞄結果	• 有關掃瞄完成後偵測到的安全威脅的資訊 • 未在 OfficeScan 用戶端主控台的「記錄檔」畫面中記錄的掃瞄結果 • 未傳送到伺服器的掃瞄結果	• 有關掃瞄完成後偵測到的安全威脅的資訊 • 未在 OfficeScan 用戶端主控台的「記錄檔」畫面中記錄的掃瞄結果 • 未傳送到伺服器的掃瞄結果
其他詳細資訊	無	與網頁信譽評等功能共用 OfficeScan NT Proxy 服務 (`TMProxy.exe`)

授與郵件掃瞄權限和啟動 POP3 郵件掃瞄

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 權限和其他設定」。
4. 在「權限」標籤上，移至「郵件掃瞄權限」區段。
5. 選取「顯示用戶端主控台上的「郵件掃瞄」標籤」。
6. 按一下「其他設定」，並移至「POP3 電子郵件掃瞄設定」區段。
7. 選取「掃瞄 POP3 電子郵件」。
8. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

用於掃瞄的快取設定

OfficeScan 用戶端可以建置數位簽章和依需求掃瞄快取檔案以提高其掃瞄效能。執行依需求掃瞄時，OfficeScan 用戶端會依次檢查數位簽章快取檔案和依需求掃瞄快取檔案，以選擇從掃瞄中排除的檔案。如果不掃瞄大量檔案，將會縮短掃瞄時間。

數位簽章快取

數位簽章快取檔案會在手動掃瞄、預約掃瞄和立即掃瞄期間使用。用戶端不會掃瞄快取已新增到數位簽章快取檔案的檔案。

OfficeScan 用戶端使用行為監控所用的數位簽章特徵碼，來建立數位簽章快取檔案。數位簽章特徵碼包含趨勢科技認為可信，因而可以不掃瞄的檔案清單。

注意

行為監控會在 Windows 伺服器平台上自動關閉（不支援 Windows XP 64 位元、Windows 2003 64 位元和 Windows Vista（不含 Service Pack 1）64 位元平台）。如果啟動數位簽章快取，這些平台上的 OfficeScan 用戶端會下載要在快取中使用的數位簽章特徵碼，而不會下載其他行為監控元件。

用戶端會根據預約時程構建數位簽章快取檔案，該時程可從 Web 主控台進行設定。用戶端執行此操作的目的如下：

- 為建立上一快取檔案後加入系統的新檔案新增快取
- 移除系統中已修改或已刪除檔案的快取

在快取建置過程中，用戶端會檢查以下資料夾中的可信檔案，然後將這些檔案的快取新增到數位簽章快取檔案：

- `%PROGRAMFILES%`
- `%WINDIR%`

快取建置程序不會影響電腦的效能，因為用戶端在此程序中使用的系統資源非常少。用戶端還可以繼續進行由於某種原因（例如，主機電源關閉或無線電腦的交流電轉接器未插電時）而中斷的快取建置工作。

依要求掃瞄快取

依需求掃瞄快取檔案會在手動掃瞄、預約掃瞄和立即掃瞄期間使用。OfficeScan 用戶端不會掃瞄其快取已新增到依需求掃瞄快取檔案的檔案。

每次執行掃瞄時，OfficeScan 用戶端都會檢查不存在威脅的檔案的內容。如果某個不存在威脅的檔案在一段時間（可設定該時段）內未經修改，則

OfficeScan 用戶端會將該檔案的快取新增到依需求掃瞄快取檔案。如果在下一次掃瞄時檔案的快取未到期，則不會掃瞄該檔案。

不存在威脅的檔案的快取會在一定天數（亦可設定該時段）內到期。如果在快取到期時或到期之後進行掃瞄，OfficeScan 用戶端會移除到期的快取並在檔案中掃瞄威脅。如果檔案不存在威脅且保持不變，則會將該檔案的快取新增回依需求掃瞄快取檔案。如果檔案不存在威脅但最近進行了修改，則不會新增相應的快取，並將在下次掃瞄時重新掃瞄該檔案。

不存在威脅的檔案的快取到期可防止從掃瞄中排除中毒檔案，如以下範例所示：

- 嚴重過期特徵碼檔案可能已將受感染、未修改的檔案視為不存在威脅。如果快取未到期，則中毒檔案會保存在系統中，直到該檔案修改並透過即時掃瞄偵測到。
- 如果修改了快取的檔案，且即時掃瞄在修改檔案期間不可用，則只有快取到期後，才能對修改的檔案掃瞄威脅。

新增到依需求掃瞄快取檔案的快取數取決於掃瞄類型及其掃瞄目標。例如，如果在手動掃瞄期間 OfficeScan 用戶端只掃描了電腦中 1,000 個檔案中的 200 個，則快取數可能會較少。

如果頻繁執行依需求掃瞄，則依需求掃瞄快取檔案的掃瞄時間會大大降低。在全部快取均未到期的掃瞄工作中，通常需要 12 分鐘的掃瞄可以降到 1 分鐘。降低檔案必須保持不變的天數和延長快取有效期限通常可以提高效能。由於檔案必須在相對較短的時間內保持不變，因此可以將更多的快取新增到快取檔案。快取還可能會保持較長的有效期，這意味著有更多的檔案跳過掃瞄。

如果很少執行依需求掃瞄，則可以關閉依需求掃瞄快取，因為快取會在下一次執行掃瞄時到期。

設定用於掃瞄的快取設定

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。

3. 按一下「設定 > 權限和其他設定」。
4. 按一下「其他設定」，並移至「用於掃瞄的快取設定」區段。
5. 設定數位簽章快取的設定。
   a. 選取「啟動數位簽章快取」。
   b. 在「每隔 __ 天建置快取」中指定用戶端建置快取的頻率。
6. 設定依需求掃瞄快取的設定。
   a. 選取「啟動依要求掃瞄快取」。
   b. 在「針對內容不變達下列天數的安全檔案新增快取：__ 天」中指定檔案在快取之前必須保持不變的天數。
   c. 在「每個安全檔案的快取在下列天數內到期：__ 天」中指定快取保留在快取檔案中的最大天數。

   注意

   為了防止掃瞄期間新增的全部快取在同一天到期，快取將在您指定的最大天數內隨機到期。例如，如果今天將 500 個快取新增到快取，且指定的最大天數為 10，則其中一小部分快取會在次日到期，而大部分快取將在隨後幾天到期。在第 10 天，剩餘的全部快取都將到期。

7. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

全域掃瞄設定

可透過多種方式將全域掃瞄設定套用至用戶端。

- 特定的掃瞄設定可套用至伺服器管理的所有用戶端，或者只套用至具有特定掃瞄權限的用戶端。例如，如果您設定了延後「預約掃瞄」期間，則只有具備延後「預約掃瞄」權限的用戶端才能使用此設定。
- 特定掃瞄設定可套用至所有掃瞄類型，或者只套用至特定的掃瞄類型。例如，在已安裝 OfficeScan 伺服器與 OfficeScan 用戶端的電腦上，您可以將 OfficeScan 伺服器資料庫排除在掃瞄作業之外。但是，此設定僅適用於「即時掃瞄」期間。
- 可在掃瞄病毒/惡意程式和（或）間諜程式/可能的資安威脅程式時套用特定掃瞄設定。例如，評估模式僅適用於間諜程式/可能的資安威脅程式掃瞄期間。

設定全域掃瞄設定

程序

1. 瀏覽至「用戶端電腦 > 全域用戶端設定」。
2. 設定每個可用區段中的全域掃瞄設定。
   - 掃瞄設定區段 第 7-63 頁
   - 預約掃瞄設定區段 第 7-69 頁
   - 病毒/惡意程式記錄檔頻寬設定區段 第 7-71 頁
3. 按一下「儲存」。

掃瞄設定區段

全域掃描設定的掃瞄設定區段可讓管理員設定下列項目：

- 設定大型壓縮檔的掃瞄設定 第 7-64 頁
- 將「手動掃瞄」新增至 OfficeScan 用戶端電腦的 Windows 捷徑功能表 第 7-64 頁

設定大型壓縮檔的掃瞄設定

由伺服器管理的所有 OfficeScan 用戶端在「手動掃瞄」、「即時掃瞄」、「預約掃瞄」和「立即掃瞄」期間掃瞄壓縮檔是否有病毒/惡意程式和間諜程式/可能的資安威脅程式時，會先檢查下列設定：

- 請勿掃瞄壓縮檔內檔案大小超過 __ MB 的檔案：OfficeScan 不會掃瞄任何超過該大小上限的檔案。
- 在壓縮檔中，只會掃瞄前前 __ 個檔案：OfficeScan 將壓縮檔解壓縮之後，會掃瞄指定數目的檔案，並略過任何剩餘的檔案（如果有）。

將「手動掃瞄」新增至 OfficeScan 用戶端電腦的 Windows 捷徑功能表

啟動此設定時，由伺服器管理的所有 OfficeScan 用戶端都會將使用 OfficeScan 用戶端掃瞄選項新增到「Windows 檔案總管」的右鍵功能表。當使用者以滑鼠右鍵按一下 Windows 桌面或「Windows 檔案總管」中的檔案或資料夾並選取此

選項時，OfficeScan 便會使用「手動掃瞄」來掃瞄檔案或資料夾是否包含病毒/惡意程式和間諜程式/可能的資安威脅程式。

圖 7-6. 「使用 OfficeScan 用戶端掃瞄」選項

不對 OfficeScan 伺服器資料庫的資料夾進行即時掃瞄

如果 OfficeScan 用戶端和 OfficeScan 伺服器位於同一部電腦上，OfficeScan 用戶端在「即時掃瞄」期間將不會掃瞄伺服器資料庫是否包含病毒/惡意程式和間諜程式/可能的資安威脅程式。

秘訣

啟動此設定可防止掃瞄期間可能造成的資料庫損毀。

不掃瞄 Microsoft Exchange Server 的資料夾和檔案

如果 OfficeScan 用戶端和 Microsoft Exchange 2000/2003 伺服器位於同一部電腦，OfficeScan 在「手動掃瞄」、「即時掃瞄」、「預約掃瞄」和「立即掃

瞄」期間將不會掃瞄下列 Microsoft Exchange 資料夾和檔案是否包含病毒/惡意程式和間諜程式/可能的資安威脅程式：

- 位於 `\Exchsrvr\Mailroot\vsi 1` 中的下列資料夾：`Queue`、`PickUp` 和 `BadMail`
- `.\Exchsrvr\mdbdata`，包括以下檔案：`priv1.stm`、`priv1.edb`、`pub1.stm` 和 `pub1.edb`
- `.\Exchsrvr\Storage` 群組

如果為 Microsoft Exchange 2007 或更新版本資料夾，您必須手動將資料夾新增至掃瞄例外清單中。如需有關掃瞄例外的詳細資訊，請參閱下列網站：

http://technet.microsoft.com/en-us/library/bb332342.aspx

如需設定掃瞄例外清單的步驟，請參閱掃瞄例外 第 7-28 頁。

清除/刪除壓縮檔內中毒檔案

當伺服器管理的所有用戶端在手動掃瞄、即時掃瞄、預約掃瞄和立即掃瞄期間於壓縮檔中偵測到病毒/惡意程式，而且符合下列條件時，用戶端會清除或刪除中毒檔案。

- 「清除」或「刪除」是 OfficeScan 設定要執行的中毒處理行動。移至「用戶端電腦」>「用戶端管理」>「設定」>「掃瞄設定」>｛掃瞄類型｝>「處理行動」標籤，以檢查 OfficeScan 對中毒檔案執行的處理行動。
- 啟動此設定。啟動此設定可能會增加掃瞄過程中使用的電腦資源，而且掃瞄作業會花更長的時間才能完成。這是因為 OfficeScan 需要將壓縮檔解壓縮、清除/刪除壓縮檔內的中毒檔案，然後重新壓縮檔案。
- 支援壓縮檔格式。OfficeScan 只支援特定的壓縮檔格式，包括 ZIP 和使用 ZIP 壓縮技術的 Office Open XML。Office Open XML 是 Excel、PowerPoint 和 Word 等 Microsoft Office 2007 應用程式的預設格式。

注意

如需支援之壓縮檔格式的完整清單，請聯絡您的經銷商。

例如，「即時掃瞄」已設定為刪除感染病毒的檔案。「即時掃瞄」將名為 abc.zip 的壓縮檔解壓縮並偵測到壓縮檔內有中毒檔案 123.doc 後，OfficeScan 會刪除 123.doc 並重新壓縮 abc.zip，讓您可以安全地存取此檔案。

下表說明如果未符合任一條件，會有什麼情形。

表 7-17. 壓縮檔情形和結果

「清除/刪除壓縮檔內中毒檔案」的狀態	設定 OFFICESCAN 執行的中毒處理行動	壓縮檔格式	結果
已啟動	清除或刪除	不支援 例如：def.rar 包含一個中毒檔案 123.doc。	OfficeScan 會加密 def.rar，但是並不會對 123.doc 進行清除、刪除或執行其他任何中毒處理行動。
已關閉	清除或刪除	支援/不支援 例如：abc.zip 包含一個中毒檔案 123.doc。	OfficeScan 並不會對 abc.zip 和 123.doc 進行清除、刪除或執行其他任何中毒處理行動。

「清除/刪除壓縮檔內中毒檔案」的狀態	設定 OFFICESCAN 執行的中毒處理行動	壓縮檔格式	結果
啟動/關閉	不清除或刪除（換言之，下列任一種中毒處理行動：重新命名、隔離、拒絕存取或暫不處理）	支援/不支援 例如：abc.zip 包含一個中毒檔案 123.doc。	OfficeScan 會對 abc.zip（而非 123.doc）執行設定的中毒處理行動（重新命名、隔離、拒絕存取或暫不處理）。 如果中毒處理行動為： 重新命名：OfficeScan 會將 abc.zip 重新命名為 abc.vir，但是不會重新命名 123.doc。 隔離：OfficeScan 會隔離 abc.zip（會隔離 123.doc 和所有未中毒的檔案）。 暫不處理：OfficeScan 不會對 abc.zip 和 123.doc 執行任何中毒處理行動，但是會記錄偵測到病毒。 拒絕存取：OfficeScan 會在 abc.zip 開啟時拒絕存取此檔案（無法開啟 123.doc 和所有未中毒的檔案）。

啟動評估模式

在評估模式下，所有由伺服器管理的用戶端都會在手動掃瞄、預約掃瞄、即時掃瞄與立即掃瞄期間記錄偵測到的間諜程式/可能的資安威脅程式，但是不會清除這些間諜程式/可能的資安威脅程式元件。清除會終止程序，或刪除登錄、檔案、Cookie 和捷徑。

趨勢科技提供評估模式，可讓您評估趨勢科技偵測為間諜程式/可能的資安威脅程式的項目，再根據評估採取適當的中毒處理行動。例如，可以將偵測到但不認為是安全威脅的間諜程式/可能的資安威脅程式新增至間諜程式/可能的資安威脅程式核可清單..

使用評估模式時，OfficeScan 會執行下列中毒處理行動：

- 暫不處理：在手動掃瞄、預約掃瞄和立即掃瞄期間
- 拒絕存取：在即時掃瞄期間

注意

評估模式會覆寫任何使用者設定的中毒處理行動。例如，即使您選擇「清除」做為「手動掃瞄」期間的中毒處理行動，「暫不處理」仍會是用戶端在評估模式時採取的中毒處理行動。

掃瞄 Cookie

如果您認為 Cookie 是可能的安全威脅，請選取此選項。選取此選項時，伺服器管理的所有用戶端在「手動掃瞄」、「預約掃瞄」、「即時掃瞄」和「立即掃瞄」期間會掃瞄 Cookie 中是否包含間諜程式/可能的資安威脅程式。

預約掃瞄設定區段

只有設定為執行「預約掃瞄」的用戶端會使用下列設定。「預約掃瞄」可以掃瞄病毒/惡意程式和間諜程式/可能的資安威脅程式。

全域掃描設定的預約掃瞄設定區段可讓管理員設定下列項目：

- 執行預約掃瞄之前 __ 分鐘提醒使用者 第 7-70 頁
- 延後預約掃瞄最多 __ 小時又 __ 分鐘 第 7-70 頁
- 當掃瞄時間超過 __ 小時又 __ 分鐘時，自動停止預約掃瞄 第 7-70 頁
- 無線電腦的電池電力剩餘時間若少於 __ %，而且已拔掉 AC 電源轉接器，則略過預約掃瞄 第 7-70 頁
- 繼續未執行的預約掃瞄 第 7-71 頁

執行預約掃瞄之前 __ 分鐘提醒使用者

OfficeScan 可以在掃瞄開始前數分鐘顯示通知訊息，藉此提醒使用者掃瞄預約時程（日期與時間）以及您授與使用者的任何「預約掃瞄」權限。

您可以從「用戶端電腦 > 用戶端管理 > 設定 > 權限和其他設定 > 其他設定」的標籤 > 「預約掃瞄設定」啟動/關閉通知訊息。如果關閉通知訊息，將不會顯示提醒。

延後預約掃瞄最多 __ 小時又 __ 分鐘

只有具有「延後預約掃瞄」權限的使用者可以執行下列動作：

- 在預約掃瞄開始前將其延後，並指定延後時間長度。
- 如果「預約掃瞄」正在進行中，使用者可以停止掃瞄並稍後重新啟動。使用者可以接著指定掃瞄重新開始之前應該經過的時間長度。一旦掃瞄重新啟動，先前掃瞄過的所有檔案都會重新掃瞄一遍。

  使用者可以指定的延後時間長度/經過的時間長度上限為 12 小時又 45 分鐘，而您可以在提供的時數和（或）分鐘數欄位中進行指定以縮短上限。

當掃瞄時間超過 __ 小時又 __ 分鐘時，自動停止預約掃瞄

OfficeScan 會在超過指定的時間而掃瞄尚未完成時停止掃瞄。OfficeScan 會立即通知使用者在掃瞄期間偵測到的任何安全威脅。

無線電腦的電池電力剩餘時間若少於 __ %，而且已拔掉 AC 電源轉接器，則略過預約掃瞄

如果 OfficeScan 偵測到無線電腦的電池電力不足，且其 AC 電源轉接器並未連接至任何電源時，就會在「預約掃瞄」啟動時立即略過掃瞄。如果電池電力不足，但是 AC 電源轉接器已經連接至電源，則會繼續掃瞄。

繼續未執行的預約掃瞄

您可以指定當「預約掃瞄」因為 OfficeScan 不在執行狀態而未在預定的日期和時間啟動時，OfficeScan 將在何時繼續掃瞄：

- 隔天同一時間：如果 OfficeScan 在隔天同一時間執行，則會繼續掃瞄。
- 電腦啟動後 __ 分鐘：OfficeScan 會在使用者開啟電腦並經過指定的分鐘數後繼續掃瞄。分鐘數介於 10 到 120 之間。

注意

如果系統管理員啟動適當的權限，使用者可以延後或略過錯過的「預約掃瞄」。如需詳細資訊，請參閱預約掃瞄權限和其他設定 第 7-51 頁。

病毒/惡意程式記錄檔頻寬設定區段

全域掃描設定的病毒/惡意程式記錄檔頻寬設定區段可讓管理員設定下列項目：

啟動 OfficeScan 用戶端，為於一小時內偵測到的相同病毒/惡意程式建立單一病毒/惡意程式記錄項目 第 7-71 頁

啟動 OfficeScan 用戶端，為於一小時內偵測到的相同病毒/惡意程式建立單一病毒/惡意程式記錄項目

OfficeScan 在偵測到相同病毒/惡意程式在短時間內造成的多個感染時，會整合病毒記錄項目。OfficeScan 會多次偵測單一病毒/惡意程式，迅速填入病毒/惡意程式記錄檔，並且在 OfficeScan 用戶端傳送記錄檔資訊至伺服器時消耗網路頻寬。啟動此功能可同時減少產生的病毒/惡意程式記錄項目數，以及 OfficeScan 用戶端向伺服器報告病毒記錄資訊時消耗的網路頻寬數量。

安全威脅通知

OfficeScan 隨附一組預設通知訊息，用於通知您、其他 OfficeScan 管理員和 OfficeScan 用戶端使用者偵測到的安全威脅。

如需有關傳送給管理員的通知的詳細資訊，請參閱管理員的安全威脅通知 第 7-72 頁。

如需有關傳送給 OfficeScan 用戶端使用者的通知的詳細資訊，請參閱OfficeScan 用戶端使用者的安全威脅通知 第 7-76 頁。

管理員的安全威脅通知

將 OfficeScan 設為在下列時機，將通知傳送給您及其他的 OfficeScan 管理員：當其偵測到安全威脅，或是只有在安全威脅處理行動失敗，因而需要您介入時。

OfficeScan 隨附一組預設通知訊息，用於通知您和其他 OfficeScan 管理員偵測到的安全威脅。您可以視需要修改通知和設定其他通知設定。

注意

OfficeScan 可以透過電子郵件、呼叫器、SNMP Trap 和 Windows NT 事件記錄檔來傳送通知。設定 OfficeScan 何時透過這些通道傳送通知的設定。如需詳細資訊，請參閱管理員通知設定 第 13-28 頁。

設定管理員的安全威脅通知

程序

1. 瀏覽至「通知 > 管理員通知 > 標準通知」。
2. 在「條件」標籤中：
   a. 移至「病毒/惡意程式」和「間諜程式/可能的資安威脅程式」區段。

b. 指定是否在 OfficeScan 偵測到病毒/惡意程式和間諜程式/可能的資安威脅程式時傳送通知，或是只在對這些安全威脅採取的處理行動失敗時傳送通知。

3. 在「電子郵件」標籤中：

a. 移至「病毒/惡意程式偵測」和「間諜程式/可能的資安威脅程式偵測」區段。

b. 選取「啟動電子郵件通知」。

c. 選取「傳送通知給具有用戶端樹狀結構網域權限的使用者」。

您可以使用以角色為基礎的管理將用戶端樹狀結構網域權限授與使用者。若在屬於特定網域的 OfficeScan 用戶端上進行偵測，電子郵件將傳送給具網域權限之使用者的電子郵件信箱。如需範例，請參閱下表：

表 7-18. 用戶端樹狀結構網域和權限

用戶端樹狀結構網域	具有網域權限的角色	具有該角色的使用者帳號	使用者帳號的電子郵件信箱
網域 A	Administrator（內建）	root	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
網域 B	Administrator（內建）	root	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

如果屬於網域 A 的 OfficeScan 用戶端偵測到病毒，系統就會將電子郵件傳送至 mary@xyz.com、john@xyz.com 和 chris@xyz.com。

如果屬於網域 B 的 OfficeScan 用戶端偵測到間諜程式，系統就會將電子郵件傳送至 mary@xyz.com 和 jane@xyz.com。

注意

若您啟動此選項，具網域權限的所有使用者都必須有一個對應的電子郵件信箱。電子郵件通知不會傳送給沒有電子郵件信箱的使用者。使用者和電子郵件信箱是從「管理 > 使用者帳號」進行設定的。

d. 選取「傳送通知到下列電子郵件信箱」，然後輸入電子郵件信箱。

e. 接受或修改預設的主旨和訊息。您可以使用 Token 變數代表「主旨」和「訊息」欄位中的資料。

表 7-19. 安全威脅通知的 Token 變數

變數	說明
病毒/惡意程式偵測	
%v	病毒/惡意程式名稱
%s	具有病毒/惡意程式的電腦
%i	電腦的 IP 位址
%c	電腦的 MAC 位址
%m	電腦網域
%p	病毒/惡意程式的位置
%y	病毒/惡意程式偵測的日期和時間
%e	病毒掃瞄引擎版本
%r	病毒碼版本
%a	針對安全威脅執行的處理行動
%n	登入中毒電腦的使用者名稱
間諜程式/可能的資安威脅程式偵測	
%s	具有間諜程式/可能的資安威脅程式的電腦
%i	電腦的 IP 位址
%m	電腦網域

變數	說明
%y	間諜程式/可能的資安威脅程式偵測的日期和時間
%n	偵測時登入電腦的使用者名稱
%T	間諜程式/可能的資安威脅程式和掃瞄結果

4. 在「呼叫器」標籤中：
   a. 移至「病毒/惡意程式偵測」和「間諜程式/可能的資安威脅程式偵測」區段。
   b. 選取「啟動呼叫器通知」。
   c. 輸入訊息。
5. 在「SNMP Trap」標籤中：
   a. 移至「病毒/惡意程式偵測」和「間諜程式/可能的資安威脅程式偵測」區段。
   b. 選取「啟動 SNMP Trap 通知」。
   c. 接受或修改預設的訊息。您可以使用 Token 變數代表「訊息」欄位中的資料。如需詳細資訊，請參閱表 7-19: 安全威脅通知的 Token 變數 第 7-74 頁。
6. 在「NT 事件記錄檔」標籤中：
   a. 移至「病毒/惡意程式偵測」和「間諜程式/可能的資安威脅程式偵測」區段。
   b. 選取「啟動 NT 事件記錄檔通知」。
   c. 接受或修改預設的訊息。您可以使用 Token 變數代表「訊息」欄位中的資料。如需詳細資訊，請參閱表 7-19: 安全威脅通知的 Token 變數 第 7-74 頁。
7. 按一下「儲存」。

OfficeScan 用戶端使用者的安全威脅通知

OfficeScan 可以在以下情況下在 OfficeScan 用戶端電腦上顯示通知訊息：

- 「即時掃瞄」和「預約掃瞄」偵測病毒/惡意程式和間諜程式/可能的資安威脅程式。啟動通知訊息，並視需要修改其內容。
- 必須重新啟動用戶端電腦才能完成清除中毒檔案時。對於「即時掃瞄」，會在掃瞄到特定安全威脅之後顯示訊息。對於「手動掃瞄」、「預約掃瞄」和「立即掃瞄」，只會在 OfficeScan 完成掃瞄所有掃瞄目標的程序之後顯示一次訊息。

通知使用者有關病毒/惡意程式和間諜程式/可能的資安威脅程式偵測資訊

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 掃瞄設定 > 即時掃瞄設定」或「設定 > 掃瞄設定 > 預約掃瞄設定」。
4. 按一下「處理行動」標籤。
5. 選取下列選項：
   - 偵測到病毒/惡意程式時在用戶端電腦上顯示通知訊息
   - 偵測到可能的病毒/惡意程式時在用戶端電腦上顯示通知訊息
6. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。

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

設定病毒/惡意程式通知

程序

1. 瀏覽至「通知 > 用戶端使用者通知」。
2. 按一下「病毒/惡意程式」標籤。
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：OfficeScan 用戶端無法處理重大惡意程式
      - 中：OfficeScan 用戶端無法處理惡意程式
      - 低：OfficeScan 用戶端無法解決所有安全威脅
   b. 接受或修改預設的訊息。
4. 如果要在用戶端使用者的電腦產生病毒/惡意程式時顯示通知訊息：
   a. 選取「病毒/惡意程式感染來源」下的核取方塊。
   b. 指定傳送通知的間隔。
   c. 您可以視需要修改預設的通知訊息。

   注意

   只有在您啟動「Windows Messenger 服務」時，才會顯示此通知訊息。在「服務」畫面（「控制台 > 系統管理工具 > 服務 > Messenger」）中檢查此服務的狀態。

5. 按一下「儲存」。

設定間諜程式/可能的資安威脅程式通知

程序

1. 瀏覽至「通知 > 用戶端使用者通知」。
2. 按一下「間諜程式/可能的資安威脅程式」標籤。
3. 接受或修改預設的訊息。
4. 按一下「儲存」。

通知用戶端重新啟動以完成清除中毒檔案

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 權限和其他設定」。
4. 按一下「其他設定」標籤，然後移至「重新啟動通知」區段。
5. 選取「如果用戶端電腦需要重新啟動以完成清除中毒檔案，則會顯示通知訊息」。
6. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

安全威脅記錄檔

OfficeScan 在偵測到病毒/惡意程式或間諜程式/可能的資安威脅程式時，以及在恢復間諜程式/可能的資安威脅程式時，都會產生記錄檔。

如果要避免記錄檔佔去過多硬碟空間，請手動刪除記錄檔或設定記錄檔刪除預約時程。如需有關管理記錄檔的詳細資訊，請參閱記錄檔管理 第 13-31 頁。

檢視病毒/惡意程式記錄檔

OfficeScan 用戶端在偵測到病毒和惡意程式時會產生記錄檔，並將記錄檔傳送到伺服器。

程序

1. 瀏覽至下列其中一個項目：
   - 「記錄檔 > 用戶端電腦記錄檔 > 安全威脅」
   - 用戶端電腦 > 用戶端管理
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「記錄檔 > 病毒/惡意程式記錄檔」或「檢視記錄檔 > 病毒/惡意程式記錄檔」。
4. 指定記錄條件，然後按一下「顯示記錄檔」。
5. 檢視記錄檔。記錄檔包含下列資訊：
   - 病毒/惡意程式偵測的日期和時間
   - 中毒電腦
   - 病毒/惡意程式名稱
   - 感染來源
   - 中毒檔案

- 偵測到病毒/惡意程式的掃瞄類型
- 掃瞄結果

注意

如需有關掃瞄結果的詳細資訊，請參閱病毒/惡意程式掃瞄結果 第 7-80 頁。

- IP 位址
- MAC 位址
- 記錄檔詳細資訊（按一下「檢視」可查看詳細資訊。）

6. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請按一下「匯出到 CSV」。開啟檔案或將其儲存至特定位置。

   CSV 檔案包含以下資訊：

   - 記錄檔中的所有資訊
   - 偵測時登入電腦的使用者名稱

病毒/惡意程式掃瞄結果

下列掃瞄結果會顯示在病毒/惡意程式記錄檔中：

- 已刪除
  - 第一個中毒處理行動是「刪除」，並已刪除中毒的檔案。
  - 第一個中毒處理行動是「清除」，但是清除失敗。第二個處理行動是「刪除」，並已刪除中毒的檔案。
- 已隔離
  - 第一個中毒處理行動是「隔離」，並已隔離中毒的檔案。
  - 第一個中毒處理行動是「清除」，但是清除失敗。第二個處理行動是「隔離」，並已隔離中毒的檔案。

- 已清除

  已清除中毒的檔案。

- 已重新命名

  - 第一個中毒處理行動是「重新命名」，並已重新命名中毒的檔案。
  - 第一個中毒處理行動是「清除」，但是清除失敗。第二個處理行動是「重新命名」，並已重新命名中毒的檔案。

- 拒絕存取

  - 第一個中毒處理行動是「拒絕存取」，而在使用者嘗試開啟中毒的檔案時拒絕存取該檔案。
  - 第一個中毒處理行動是「清除」，但是清除失敗。第二個中毒處理行動是「拒絕存取」，而在使用者嘗試開啟中毒的檔案時拒絕存取該檔案。
  - 在「即時掃瞄」期間偵測到可能的病毒/惡意程式。
  - 即使中毒處理行動為「清除」（第一個處理行動）和「隔離」（第二個處理行動），「即時掃瞄」仍可能拒絕存取受到開機型病毒感染的檔案。這是因為嘗試清除開機型病毒，可能會損害中毒電腦的「主開機記錄 (MBR)」。執行「手動掃瞄」，讓 OfficeScan 能夠清除或隔離檔案。

- 暫不處理

  - 第一個中毒處理行動是「暫不處理」。OfficeScan 未對中毒的檔案執行任何中毒處理行動。
  - 第一個中毒處理行動是「清除」，但是清除失敗。第二個中毒處理行動是「暫不處理」，所以 OfficeScan 未對中毒的檔案執行任何中毒處理行動。

- 暫不處理潛在的安全威脅

  只有在 OfficeScan 於「手動掃瞄」、「預約掃瞄」與「立即掃瞄」期間偵測到「可能的病毒/惡意程式」時，才會顯示此掃瞄結果。如需有關可能的病毒/惡意程式以及如何將可疑檔案送給趨勢科技進行分析的詳細資訊，請參閱趨勢科技線上病毒百科全書的下列頁面。

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=POSSIBLE_VIRUS&VSect=Sn

- 無法清除或隔離這個檔案

  「清除」是第一個處理行動。「隔離」是第二個處理行動，而兩項行動都失敗。

  解決方案：請參閱「無法隔離檔案/無法重新命名檔案」 第 7-82 頁。

- 無法清除或刪除這個檔案

  「清除」是第一個處理行動。「刪除」是第二個處理行動，而兩項行動都失敗。

  解決方案：請參閱「無法刪除這個檔案」 第 7-82 頁。

- 無法清除或重新命名這個檔案

  「清除」是第一個處理行動。「重新命名」是第二個處理行動，而兩項行動都失敗。

  解決方案：請參閱「無法隔離檔案/無法重新命名檔案」 第 7-82 頁。

- 無法隔離檔案/無法重新命名檔案

  說明 1

  中毒檔案可能被其他應用程式鎖定或正在執行，或者可能位於 CD 上。在應用程式釋放檔案或檔案執行後，OfficeScan 會隔離/重新命名檔案。

  解決方案：

  如果中毒檔案位於 CD 上，建議不要再使用該 CD，因為病毒可能會感染網路上的其他電腦。

  說明 2

  中毒檔案位於用戶端電腦的 Temporary Internet Files 資料夾中。因為電腦在您瀏覽時下載檔案，所以 Web 瀏覽器可能鎖定了中毒檔案。當 Web 瀏覽器釋放檔案時，OfficeScan 會隔離/重新命名檔案。

  解決方案：無

- 無法刪除檔案

說明 1

中毒檔案可能包含在壓縮檔內，而且「用戶端電腦 > 全域用戶端設定」中的「清除/刪除壓縮檔內中毒檔案」設定已經關閉。

解決方案：

啟動「清除/刪除壓縮檔內中毒檔案」選項。啟動此選項時，OfficeScan 會將壓縮檔解壓縮、清除/刪除壓縮檔中的中毒檔案，然後重新壓縮檔案。

注意

啟動此設定可能會增加掃瞄過程中使用的電腦資源，而且掃瞄作業會花更長的時間才能完成。

說明 2

中毒檔案可能被其他應用程式鎖定或正在執行，或者可能位於 CD 上。在應用程式釋放檔案或檔案執行後，OfficeScan 會刪除檔案。

解決方案：

如果中毒檔案位於 CD 上，建議不要再使用該 CD，因為病毒可能會感染網路上的其他電腦。

說明 3

中毒檔案位於 OfficeScan 用戶端電腦的 Temporary Internet Files 資料夾中。因為電腦在您瀏覽時下載檔案，所以 Web 瀏覽器可能鎖定了中毒檔案。當 Web 瀏覽器釋放檔案時，OfficeScan 會刪除檔案。

解決方案：無

- 無法將隔離檔案傳送到指定的隔離資料夾

  雖然 OfficeScan 可以成功將檔案隔離在 OfficeScan 用戶端電腦的 `\Suspect` 資料夾中，但卻無法將檔案傳送到指定的隔離目錄。

  解決方案：

  請先判斷偵測出病毒/惡意程式的掃瞄類型（「手動掃瞄」、「即時掃瞄」、「預約掃瞄」或「立即掃瞄」），然後檢查在「 用戶端電腦 > 用戶端管理 > 設定 > {掃瞄類型} > 處理行動 」標籤中指定的隔離目錄。

如果隔離目錄位於 OfficeScan 伺服器電腦或其他 OfficeScan 伺服器電腦上：

1. 檢查用戶端是否能連線至伺服器。
2. 如果您使用 URL 做為隔離目錄格式：
    a. 請確認您在「http://」後面指定的電腦名稱是否正確。
    b. 請檢查中毒檔案的大小。如果中毒檔案超過「管理 > 隔離區管理員」中指定的檔案大小上限，請調整設定以容納檔案。您也可以執行其他處理行動，例如：刪除檔案。
    c. 檢查隔離目錄資料夾的大小並判斷其是否超過「管理 > 隔離區管理員」中指定的資料夾容量。調整資料夾的容量，或手動刪除隔離目錄中的檔案。
3. 如果您使用 UNC 路徑，請確定是否可讓「Everyone」群組共享隔離目錄資料夾，並指定讀取和寫入權限給這個群組。此外，也請檢查隔離目錄資料夾是否存在及 UNC 路徑是否正確。

如果隔離目錄位於網路上的其他電腦（此時您只可以使用 UNC 路徑）：

1. 檢查 OfficeScan 用戶端是否能連線至電腦。
2. 請確定是否可讓「Everyone」群組共享隔離目錄資料夾，並指定讀取和寫入權限給這個群組。
3. 檢查隔離目錄資料夾是否存在。
4. 檢查 UNC 路徑是否正確。

如果隔離目錄位於 OfficeScan 用戶端電腦的不同目錄中（此時您只可以使用絕對路徑），請檢查隔離目錄資料夾是否存在。

- 無法清除檔案

    說明 1

    中毒檔案可能包含在壓縮檔內，而且「用戶端電腦 > 全域用戶端設定」中的「清除/刪除」壓縮檔內中毒檔案設定已經關閉。

    解決方案：

啟動「清除/刪除壓縮檔內中毒檔案」選項。啟動此選項時，OfficeScan 會將壓縮檔解壓縮、清除/刪除壓縮檔中的中毒檔案，然後重新壓縮檔案。

注意

啟動此設定可能會增加掃瞄過程中使用的電腦資源，而且掃瞄作業會花更長的時間才能完成。

說明 2

中毒檔案位於 OfficeScan 用戶端電腦的 Temporary Internet Files 資料夾中。因為電腦在您瀏覽時下載檔案，所以 Web 瀏覽器可能鎖定了中毒檔案。當 Web 瀏覽器釋放檔案時，OfficeScan 會清除該檔案。

解決方案：無

說明 3

檔案無法清除。如需詳細資訊與解決方案，請參閱 Uncleanable File（無法清除的檔案） 第 D-15 頁。

檢視間諜程式/可能的資安威脅程式記錄檔

OfficeScan 用戶端在偵測到間諜程式和可能的資安威脅程式時會產生記錄檔，並將記錄檔傳送到伺服器。

程序

1. 瀏覽至下列其中一個項目：
   - 「記錄檔 > 用戶端電腦記錄檔 > 安全威脅」
   - 用戶端電腦 > 用戶端管理
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「記錄檔 > 間諜程式/可能的資安威脅程式記錄檔」或「檢視記錄檔 > 間諜程式/可能的資安威脅程式記錄檔」。

4. 指定記錄條件，然後按一下「顯示記錄檔」。
5. 檢視記錄檔。記錄檔包含下列資訊：
   - 間諜程式/可能的資安威脅程式偵測的日期和時間
   - 受影響的電腦
   - 間諜程式/可能的資安威脅程式名稱
   - 偵測到間諜程式/可能的資安威脅程式的掃瞄類型
   - 有關間諜程式/可能的資安威脅程式掃瞄結果（中毒處理行動是否執行成功）的詳細資訊。如需詳細資訊，請參閱間諜程式/可能的資安威脅程式掃瞄結果 第 7-86 頁。
   - IP 位址
   - MAC 位址
   - 記錄檔詳細資訊（按一下「檢視」可查看詳細資訊。）
6. 將您認為無害的間諜程式/可能的資安威脅程式新增到間諜程式/可能的資安威脅程式核可清單。
7. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請按一下「匯出到 CSV」。開啟檔案或將其儲存至特定位置。

   CSV 檔案包含以下資訊：
   - 記錄檔中的所有資訊
   - 偵測時登入電腦的使用者名稱

間諜程式/可能的資安威脅程式掃瞄結果

下列掃瞄結果會顯示在間諜程式/可能的資安威脅程式記錄檔中：

- 成功，不需要處理行動

  這是中毒處理行動成功時的第一層結果。第二層結果可能是下列任一種：

- 已清除：OfficeScan 已終止程序或已刪除登錄、檔案、Cookie 和捷徑。
- 拒絕存取：OfficeScan 已拒絕存取（複製、開啟）偵測到的間諜程式/可能的資安威脅程式元件。

- 需要進一步的處理行動

  這是中毒處理行動未成功時的第一層結果。第二層結果至少具有下列其中一則訊息：

  - 暫不處理：OfficeScan 不執行任何處理行動，但已記錄偵測到間諜程式/可能的資安威脅程式以進行評估。

    解決方案：將您認為安源的間諜程式/可能的資安威脅程式新增到間諜程式/可能的資安威脅程式核可清單。

  - 清除間諜程式/可能的資安威脅程式可能造成系統異常：這則訊息會顯示「間諜程式掃瞄引擎」是否嘗試清除任何單一資料夾，以及顯示是否符合下列條件：

    - 要清除的項目超過 250MB。
    - 作業系統使用資料夾中的檔案。正常系統作業可能也需要該資料夾。
    - 該資料夾為根目錄（例如 `C:`或 `F:`）

    解決方案：請與您的支援供應商聯絡，以獲得協助。

  - 已手動停止間諜程式/可能的資安威脅程式掃瞄。請執行完整掃瞄：使用者在掃瞄作業完成之前停止掃瞄。

    解決方案：執行「手動掃瞄」並等待掃瞄完成。

  - 間諜程式/可能的資安威脅程式已清除，需要重新啟動。請重新啟動電腦：OfficeScan 清除了間諜程式/可能的資安威脅程式元件，但是必須重新啟動電腦才能完成工作。

    解決方案：立即重新啟動電腦。

  - 無法清除間諜程式/可能的資安威脅程式：在 CD-ROM 或網路磁碟機上偵測到間諜程式/可能的資安威脅程式。OfficeScan 無法清除在這些位置偵測到的間諜程式/可能的資安威脅程式。

解決方案：手動移除中毒檔案。

- 無法識別間諜程式/可能的資安威脅程式掃瞄結果。請聯絡趨勢科技客服部門：新版的「間諜程式掃瞄引擎」提供新的掃瞄結果，OfficeScan 尚未設定為能夠處理這種掃瞄結果。

  解決方案：請聯絡您的支援供應商，以取得判斷新掃瞄結果的協助。

檢視間諜程式/可能的資安威脅程式恢復記錄檔

清除間諜程式/可能的資安威脅程式後，OfficeScan 用戶端會備份間諜程式/可能的資安威脅程式資料。如果您認為資料無害，請通知線上用戶端恢復備份資料。有關哪些間諜程式/可能的資安威脅程式備份資料已恢復、受影響的電腦與恢復結果的資訊，均可在記錄檔中找到。

程序

1. 瀏覽至「記錄檔 > 用戶端電腦記錄檔 > 間諜程式/可能的資安威脅程式恢復」。
2. 檢查「結果」欄，查看 OfficeScan 是否已成功恢復間諜程式/可能的資安威脅程式資料。
3. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請按一下「匯出到 CSV」。開啟檔案或將其儲存至特定位置。

掃瞄記錄檔

執行手動掃瞄、預約掃瞄或立即掃瞄時，OfficeScan 用戶端會建立包含該掃瞄相關資訊的掃瞄記錄檔。您可以存取 OfficeScan 用戶端主控台來檢視掃瞄記錄檔。用戶端不會將掃瞄記錄檔傳送至伺服器。

掃瞄記錄檔會顯示下列資訊：

- OfficeScan 開始掃瞄的日期和時間
- OfficeScan 停止掃瞄的日期和時間

- 掃瞄狀態
  - 已完成：掃瞄作業已順利完成，未發生任何問題。
  - 已停止：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：OfficeScan 的即時掃瞄服務可能意外終止，或使用者強制重新啟動用戶端。
- 掃瞄類型
- 已掃瞄的物件數目
- 中毒檔案數目
- 不成功的處理行動數目
- 成功的處理行動數目
- 病毒碼版本
- 本機雲端病毒碼版本
- 間諜程式病毒碼版本

安全威脅爆發

當特定時段偵測到的病毒/惡意程式、間諜程式/可能的資安威脅程式和共享資料夾作業階段超過某一臨界值時，即發生安全威脅爆發。有數種方式可因應及抑制病毒在網路上爆發疫情，包括：

- 啟動 OfficeScan 以監控網路上的可疑活動
- 封鎖重要的用戶端電腦通訊埠與資料夾
- 傳送病毒爆發警訊給用戶端
- 清除中毒的電腦

安全威脅爆發條件和通知

設定 OfficeScan 在發生下列事件時，傳送通知給您和其他 OfficeScan 管理員：

- 病毒/惡意程式爆發
- 間諜程式/可能的資安威脅程式爆發
- 防火牆違規事件爆發
- 共享資料夾作業階段病毒爆發

根據偵測次數和偵測期間，定義病毒爆發條件。在超過偵測期限內的偵測次數時，會觸發病毒爆發。

OfficeScan 隨附一組預設通知訊息，用於通知您和其他 OfficeScan 管理員偵測到的病毒爆發。您可以視需要修改通知和設定其他通知設定。

注意

OfficeScan 可以透過電子郵件、呼叫器、SNMP Trap 和 Windows NT 事件記錄檔傳送安全威脅爆發通知。對於共享資料夾作業階段病毒爆發，OfficeScan 會透過電子郵件傳送通知。設定 OfficeScan 何時透過這些通道傳送通知的設定。如需詳細資訊，請參閱管理員通知設定 第 13-28 頁。

配置安全威脅爆發條件和通知

程序

1. 瀏覽至「通知 > 管理員通知 > 病毒爆發通知」。
2. 在「條件」標籤中：
   a. 移至「病毒/惡意程式」和「間諜程式/可能的資安威脅程式」區段：
   b. 指定唯一偵測來源的數量。
   c. 指定每個安全威脅的偵測次數和偵測期限。

秘訣

趨勢科技建議您接受此畫面中的預設值。

OfficeScan 會在超過偵測到的數目時傳送通知訊息。例如，在「病毒/惡意程式」區段下，如果您指定了 10 個唯一來源，偵測次數為 100 並且時段為 5 小時，則 OfficeScan 會在 10 個不同的用戶端於 5 小時內回報的安全威脅總數達到 101 時傳送通知。如果 5 小時內偵測到的全部實體僅發生在一個用戶端上，OfficeScan 將不傳送通知。

3. 在「條件」標籤中：

   a. 移至「共享資料夾作業階段」區段。

   b. 選取「監控網路上的共享資料夾作業階段」。

   c. 在「記錄的共享資料夾作業階段」中，按一下數字連結，以檢視含有共享資料夾的電腦和存取共享資料夾的電腦。

   d. 指定共享資料夾作業階段數和偵測期間。

   OfficeScan 會在超過共享資料夾作業階段數時傳送通知訊息。

4. 在「電子郵件」標籤中：

   a. 移至「病毒/惡意程式爆發」、「間諜程式/可能的資安威脅程式爆發」和「共享資料夾作業階段病毒爆發」 區段。

   b. 選取「啟動電子郵件通知」。

   c. 指定電子郵件收件者。

   d. 接受或修改預設的電子郵件主旨和訊息。您可以使用 Token 變數代表「主旨」和「訊息」欄位中的資料。

   表 7-20. 安全威脅爆發通知的 Token 變數

變數	說明
病毒/惡意程式爆發	
%CV	偵測到的病毒/惡意程式總數

變數	說明
%CC	具有病毒/惡意程式的電腦總數
間諜程式/可能的資安威脅程式爆發	
%CV	偵測到的間諜程式/可能的資安威脅程式總數
%CC	具有間諜程式/可能的資安威脅程式的電腦總數
共享資料夾作業階段病毒爆發	
%S	共享資料夾作業階段數量
%T	共享資料夾作業階段累計的時段
%M	時段，以分鐘為單位

e. 選取其他要納入電子郵件中的病毒/惡意程式與間諜程式/可能的資安威脅程式資訊。您可以納入用戶端/網域名稱、安全威脅名稱、偵測的日期與時間、路徑與中毒檔案，以及掃瞄結果。

f. 接受或修改預設的通知訊息。

5. 在「呼叫器」標籤中：

   a. 移至「病毒/惡意程式爆發」和「間諜程式/可能的資安威脅程式爆發」區段。

   b. 選取「啟動呼叫器通知」。

   c. 輸入訊息。

6. 在「SNMP Trap」標籤中：

   a. 移至「病毒/惡意程式爆發」和「間諜程式/可能的資安威脅程式爆發」區段。

   b. 選取「啟動 SNMP Trap 通知」。

   c. 接受或修改預設的訊息。您可以使用 Token 變數代表「訊息」欄位中的資料。如需詳細資訊，請參閱表 7-20: 安全威脅爆發通知的 Token 變數 第 7-91 頁。

7. 在「NT 事件記錄檔」標籤中：

a. 移至「病毒/惡意程式爆發」和「間諜程式/可能的資安威脅程式爆發」區段。

b. 選取「啟動 NT 事件記錄檔通知」。

c. 接受或修改預設的訊息。您可以使用 Token 變數代表「訊息」欄位中的資料。如需詳細資訊，請參閱表 7-20: 安全威脅爆發通知的 Token 變數 第 7-91 頁。

8. 按一下「儲存」。

設定安全威脅爆發防範

病毒疫情爆發時，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。

程序

1. 瀏覽至「用戶端電腦 > 病毒爆發防範」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「啟動病毒爆發防範」。
4. 按一下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 7-95 頁
   - 封鎖易受攻擊的通訊埠 第 7-96 頁
   - 拒絕檔案和資料夾的寫入權限 第 7-97 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。如果要永久封鎖或拒絕存取特定檔案、資料夾或通訊埠，請直接修改電腦和網路設定，而不要使用 OfficeScan。

7. 接受或修改預設的用戶端通知訊息。

注意

如果要設定 OfficeScan 在病毒爆發時通知您，請移至 通知 > 管理員通知 > 病毒爆發通知。

8. 按一下「啟動病毒爆發通知」。

   您所選取的病毒爆發防範措施會顯示在新視窗中。

9. 回到用戶端樹狀結構中，核取「病毒爆發防範」欄。

   套用病毒爆發防範措施的電腦上會出現核取記號。

OfficeScan 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）
- OfficeScan 用戶端事件（啟動病毒爆發防範）

病毒爆發防範策略

病毒疫情爆發時，請實施下列任何一項策略：

- 限制/拒絕存取共享資料夾 第 7-95 頁
- 封鎖易受攻擊的通訊埠 第 7-96 頁
- 拒絕檔案和資料夾的寫入權限 第 7-97 頁

限制/拒絕存取共享資料夾

在病毒爆發期間，請限制或拒絕存取網路上的共享資料夾，以防止安全威脅透過共享資料夾散佈。

此策略生效時，使用者仍可共享資料夾，但此策略不會套用至新的共享資料夾。因此，請通知使用者不要在病毒爆發期間共享資料夾，或是重新部署策略並將其套用至新的共享資料夾。

程序

1. 瀏覽至「用戶端電腦 > 病毒爆發防範」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「啟動病毒爆發防範」。
4. 按一下「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
   - 拒絕完整存取

   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. 按一下「儲存」。

   「病毒爆發防範設定」畫面會再次顯示。
7. 按一下「啟動病毒爆發通知」。

   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 OfficeScan 用戶端電腦。

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，OfficeScan 便無法在病毒爆發期間與用戶端通訊。

程序

1. 瀏覽至「用戶端電腦 > 病毒爆發防範」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「啟動病毒爆發防範」。
4. 按一下「封鎖通訊埠」。
5. 選取是否要封鎖信任的通訊埠。
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，請按一下「新增」。在開啟的畫面中，選取要封鎖的通訊埠，然後按一下「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。
      - 一般使用的通訊埠：至少為 OfficeScan 選取一個通訊埠號碼，以便儲存通訊埠封鎖設定。
      - 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。如需詳細資訊，請參閱 Trojan Port（特洛伊木馬程式通訊埠） 第 D-13 頁。
      - 1 到 65535 之間的通訊埠號碼或範圍：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），則按一下這項。

b. 如果要編輯遭封鎖通訊埠的設定，請按一下通訊埠號碼。

c. 在開啟的畫面中修改設定，然後按一下「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，然後按一下「刪除」。

7. 按一下「儲存」。

「病毒爆發防範設定」畫面會再次顯示。

8. 按一下「啟動病毒爆發通知」。

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電腦上的檔案和資料夾。在病毒疫情爆發時，請設定 OfficeScan，讓它防止病毒/惡意程式修改或刪除 OfficeScan 用戶端電腦上的檔案和資料夾。

程序

1. 瀏覽至「用戶端電腦 > 病毒爆發防範」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「啟動病毒爆發防範」。
4. 按一下「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，請按一下「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，然後按一下「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，然後按一下「新增」。
8. 按一下「儲存」。

   「病毒爆發防範設定」畫面會再次顯示。
9. 按一下「啟動病毒爆發通知」。

   您所選取的病毒爆發防範措施會顯示在新視窗中。

關閉病毒爆發防範

當您確認已抑制病毒爆發且 OfficeScan 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。

程序

1. 瀏覽至「用戶端電腦 > 病毒爆發防範」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「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用戶端使用者」。
5. 接受或修改預設的用戶端通知訊息。
6. 按一下「恢復設定」。

注意

如果您沒有手動恢復網路設定，OfficeScan 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。

OfficeScan 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 OfficeScan 用戶端啟動病毒爆發防範）
- OfficeScan 用戶端事件（啟動病毒爆發防範）

7. 在關閉病毒爆發防範後，掃瞄用戶端電腦是否有安全威脅，以確保已抑制病毒爆發。

第 8 章

使用行為監控

本章說明如何使用行為監控功能來保護電腦免於受到安全威脅的侵襲。

本章內容：

行為監控

行為監控會不斷地監控端點上的作業系統或已安裝軟體是否發生了異常修改。行為監控透過惡意程式行為封鎖和事件監控來保護端點。這兩個功能搭配使用者已設定的例外清單和認證安全防護軟體服務更是相得益彰。

重要

行為監控不支援 Windows XP 或 Windows 2003 64 位元平台。

行為監控不支援 Windows Vista 64 位元平台搭配 SP1 或更新版本。

依預設，所有版本的 Windows Server 2003、Windows Server 2008 和 Windows Server 2012 會關閉行為監控。在這些伺服器平台上啟動行為監控之前，請先閱讀 OfficeScan 用戶端服務 第 14-6 頁中所列的指導方針和最佳做法。

惡意程式行為封鎖

惡意程式行為封鎖能夠提供多一層的必要安全威脅防護，以封鎖存在惡意行為的程式。它會觀察一段時間內的系統事件。當程式執行不同的動作組合或動作序列時，惡意程式行為封鎖會偵測已知的惡意行為並封鎖關聯程式。使用此功能可以確保提供更高等級的保護，以抵禦全新的、不明的和新興的安全威脅。

如果封鎖了某個程式且啟動了通知，OfficeScan 將在 OfficeScan 用戶端電腦上顯示通知。如需有關通知的詳細資訊，請參閱 OfficeScan 用戶端使用者的行為監控通知 第 8-9 頁。

事件監控

事件監控提供了一種更為通用的方法來抵禦未授權軟體和惡意程式攻擊。它會在系統區域中監控某些事件，允許管理員調整觸發此類事件的程式。如果您的特定系統保護需求高於惡意程式行為封鎖提供的需求，請使用事件監控。

以下表格為監控系統事件清單。

表 8-1. 監控的系統事件

事件	說明
重複的系統檔案	許多惡意程式皆有能力以 Windows 系統檔案所使用的檔案名稱，建立本身或其他惡意程式的副本。其用意通常為覆寫或取代系統檔案、規避偵測或防止使用者刪除惡意檔案。
主機檔案的修改	主機檔案會比對網域名稱與 IP 位址。許多惡意程式皆有能力修改主機檔案，而使網路瀏覽器重新導向至中毒、不存在或偽造的網站。
可疑行為	可疑行為是指合法程式不太可能會做出的某個特定或一連串處理行動。使用出現可疑行為的程式時應謹慎。
新增 Internet Explorer Plug-in	間諜程式/可能的資安威脅程式常會安裝不需要的 Internet Explorer Plug-in，包括工具列與「瀏覽器協助物件」。
Internet Explorer 設定的修改	許多病毒/惡意程式皆有能力變更 Internet Explorer 設定，包括首頁、信任的網站、Proxy 伺服器設定和功能表擴充項目等。
安全策略的修改	Windows 安全策略若遭修改，不需要的應用程式即可執行並變更系統設定。
程式庫植入	許多惡意程式皆有能力設定 Windows，而使所有應用程式自動載入程式庫 (DLL)。如此將使 DLL 中的惡意常式得以隨著應用程式啟動而執行。
Shell 的修改	許多惡意程式皆有能力修改 Windows Shell 設定，使其與特定檔案類型產生關聯。此常式將使惡意程式在使用者以 Windows 檔案總管開啟關聯的檔案時自動啟動。Windows Shell 設定變更後，也將使惡意程式得以追蹤所使用的程式，並隨著合法應用程式而啟動。
新增服務	Windows 服務是具有特殊功能的處理程序，通常會以完整的管理存取權持續在背景中執行。惡意程式有時會自行安裝為服務，並隱藏起來。
系統檔案的修改	某些 Windows 系統檔案可決定系統行為，包括啟動程式和畫面保護程式設定。許多惡意程式皆有能力修改系統檔案，進而在開機時自動啟動並控制系統行為。
防火牆策略的修改	Windows 防火牆策略可決定可存取網路的應用程式、可供通訊使用的通訊埠以及可與電腦通訊的 IP 位址。許多惡意程式皆有能力修改策略，進而存取網路和 Internet。

事件	說明
系統程序修改	許多惡意程式會在內建 Windows 程序上執行各種處理行動。這些處理行動可能包括終止或修改執行中的程序。
新的啟動程式	許多惡意程式皆有能力設定 Windows，而使所有應用程式自動載入程式庫 (DLL)。如此將使 DLL 中的惡意常式得以隨著應用程式啟動而執行。

當事件監控偵測到監控的系統事件時，它會執行針對此事件所設定的處理行動。

以下表格列出的是管理員在監控系統事件上可採取的行動。

表 8-2. 監控的系統事件的處理行動

處理行動	說明
評估	OfficeScan 一律允許與事件相關聯程式，但在記錄檔中記錄此處理行動以便評估。 這是對所有監控的系統事件的預設處理行動。 注意 這個選項不支援 64 位元系統的程式庫植入。
允許	OfficeScan 一律允許與事件相關聯程式。
需要時詢問	OfficeScan 會提示使用者允許或拒絕與事件相關聯程式，並將該程式新增到例外清單。 如果使用者在特定的時間內未回應，OfficeScan 會自動允許此程式執行。預設時間為 30 秒。如果要修改此時間長度，請參閱先修改時段再允許程式執行 第 8-6 頁。 注意 這個選項不支援 64 位元系統的程式庫植入。

處理行動	說明
拒絕	OfficeScan 一律封鎖與某個事件相關聯的程式，並在記錄檔中記錄此處理行動。 如果封鎖了某個程式且啟動了通知，OfficeScan 將在 OfficeScan 用戶端電腦上顯示通知。如需有關通知的詳細資訊，請參閱 OfficeScan 用戶端使用者的行為監控通知 第 8-9 頁。

行為監控例外清單

行為監控例外清單包含不受行為監控所監控的程式。

- 核可的程式：可以執行此清單中的程式。核可的程式仍需經過其他 OfficeScan 功能（如 File-based 掃瞄）的檢查，最後才會允許其執行。
- 封鎖的程式：始終無法啟動此清單中的程式。如果要設定此清單，必須啟動事件監控。

從 Web 主控台設定例外清單。您也可以授與使用者權限，讓他們可以從 OfficeScan 用戶端主控台設定自己的例外清單。如需詳細資訊，請參閱行為監控權限 第 8-8 頁。

設定惡意程式行為封鎖、事件監控和例外清單

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 行為監控設定」。
4. 選取「啟動惡意程式行為封鎖」。
5. 設定事件監控設定。
   a. 選取「啟動事件監控」。

b. 選擇要監控的系統事件，並針對所選取的每個件選取處理行動。如需有關監控的系統事件和處理行動的資訊，請參閱事件監控 第 8-2 頁。

6. 設定例外清單。

a. 在「輸入程式完整路徑」下，輸入要核可或封鎖的程式完整路徑。請以半形分號 (;) 來分隔多個項目。例外清單支援萬用字元和 UNC 路徑。

b. 按一下「核可的程式」或「封鎖的程式」。

c. 如果要從清單中移除封鎖的或核可的程式，請按一下垃圾桶圖示 () 在程式旁邊。

注意

OfficeScan 最多可接受 100 個核可的程式和 100 個封鎖的程式。

7. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

- 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
- 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

先修改時段再允許程式執行

只有在事件監控已啟動，且監控的系統事件的處理行動是「需要時詢問」時，這個設定才有效。此處理行動會提示使用者允許或拒絕與事件相關聯的程式。如果使用者在特定的時間內未回應，OfficeScan 會自動允許此程式執行。如需詳細資訊，請參閱事件監控 第 8-2 頁。

程序

1. 瀏覽至「用戶端電腦 > 全域用戶端設定」。

2. 移至「行為監控設定」區段。
3. 在「如果用戶端在以下時間內沒有回應，則自動允許程式：__ 秒」內指定時間長度。
4. 按一下「儲存」。

認證安全防護軟體服務

認證安全防護軟體服務會查詢趨勢科技資料中心，確認惡意程式行為封鎖或事件監控所偵測到的程式是否安全。啟動「認證安全防護軟體服務」可降低誤判的可能性。

注意

啟動認證安全防護軟體服務之前，請確定 OfficeScan 用戶端具有正確的 Proxy 伺服器設定（詳細資訊請參閱 OfficeScan 用戶端 Proxy 伺服器設定 第 14-42 頁）。Proxy 伺服器設定不正確以及網際網路連線不穩定，都可能造成趨勢科技資料中心回應接收延遲或失敗，以致監控程式顯示無回應。

此外，純 IPv6 OfficeScan 用戶端無法直接從趨勢科技資料中心進行查詢。如果要使 OfficeScan 用戶端連線到趨勢科技資料中心，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。

啟動認證安全防護軟體服務

程序

1. 瀏覽至「用戶端電腦 > 全域用戶端設定」。
2. 移至「行為監控設定」區段。
3. 選取「啟動認證安全防護軟體服務」選項。
4. 按一下「儲存」。

行為監控權限

如果用戶端具有「行為監控」權限，OfficeScan 用戶端主控台會顯示「行為監控」標籤。然後，使用者可以管理自己的例外清單。

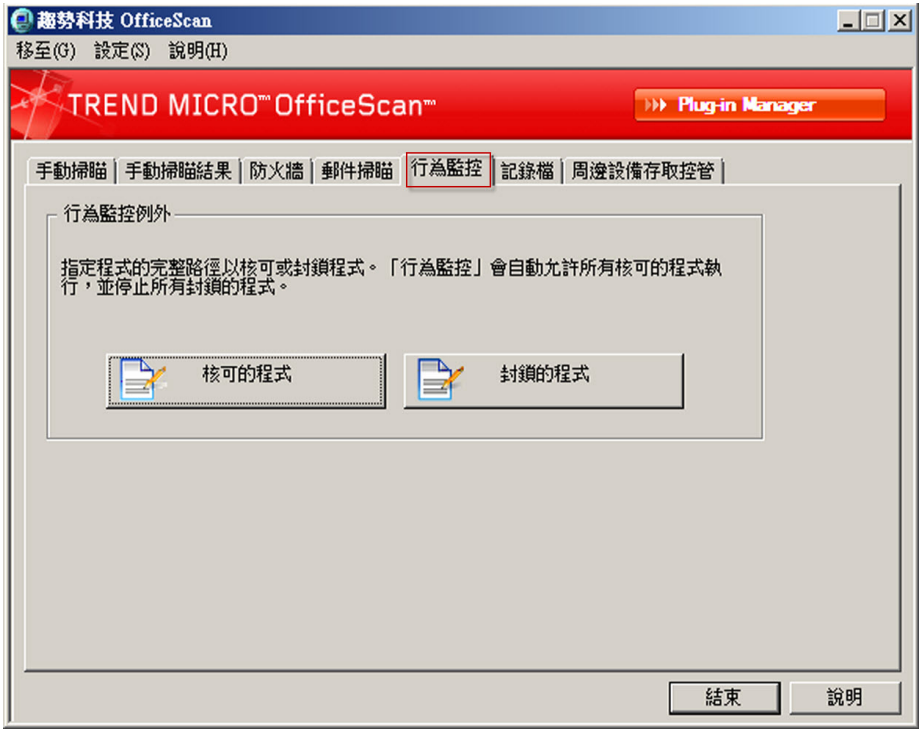


圖 8-1. OfficeScan 用戶端主控台上的「行為監控」標籤

授與行為監控權限

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。

2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 權限和其他設定」。
4. 在「權限」標籤上，移至「行為監控權限」區段。
5. 選取「顯示用戶端主控台上的「行為監控」標籤」。
6. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

OfficeScan 用戶端使用者的行為監控通知

OfficeScan 可以在行為監控封鎖某個程式後，立即在 OfficeScan 用戶端電腦上顯示通知訊息。啟動傳送通知訊息並可選擇修改訊息的內容。

啟用傳送通知訊息

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 權限和其他設定」。
4. 按一下「其他設定」，並移至「行為監控設設定」區段。

5. 選取「當程式被封鎖時顯示通知」。

6. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

修改通知訊息內容

程序

1. 瀏覽至「通知 > 用戶端使用者通知」。
2. 按一下「行為監控策略違規」標籤。
3. 在提供的文字方塊中修改預設訊息。
4. 按一下「儲存」。

行為監控記錄檔

OfficeScan 用戶端可記錄未經授權的程式存取案例，並將記錄檔傳送至伺服器。持續運作的 OfficeScan 用戶端會依指定的時間間隔（預設為每 60 分鐘）彙整一次記錄檔並進行傳送。

如果要避免記錄檔佔去過多硬碟空間，請手動刪除記錄檔或設定記錄檔刪除預約時程。如需有關管理記錄檔的詳細資訊，請參閱記錄檔管理 第 13-31 頁。

檢視行為監控記錄檔

程序

1. 瀏覽至「 記錄檔 > 用戶端電腦記錄檔 > 安全性風險」或「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「記錄檔 > 行為監控記錄檔」或「檢視記錄檔 > 行為監控記錄檔」。
4. 指定記錄條件，然後按一下「顯示記錄檔」。
5. 檢視記錄檔。記錄檔包含下列資訊：
   - 偵測到發生未經授權程序的日期/時間
   - 偵測到發生未經授權程序的電腦
   - 電腦的網域
   - 違規：即程序所違反的事件監控規則
   - 偵測到違規時執行的處理行動
   - 事件：即程式所存取的物件類型
   - 未經授權程式的風險等級
   - 程式：即未經授權的程式
   - 作業：即未經授權的程式所執行的處理行動
   - 目標：即所存取的程序
6. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請按一下「匯出到 CSV」。開啟檔案或將其儲存至特定位置。

設定行為監控記錄檔傳送預約時程

程序

1. 存取 <伺服器安裝資料夾>\PCCSRV。
2. 使用記事本等文字編輯器開啟 ofcscan.ini 檔案。
3. 搜尋字串「SendBMLogPeriod」，然後檢查旁邊的值。

   預設值為 3600 秒，而字串會顯示為 SendBMLogPeriod=3600。
4. 指定值（以秒為單位）。

   例如，如果要將記錄檔期間改成 2 小時，請將值改成 7200。
5. 儲存檔案。
6. 移至「用戶端電腦 > 全域用戶端設定」。
7. 按一下「儲存」而不變更任何設定。
8. 重新啟動用戶端。

第 9 章

使用周邊設備存取控管

本章說明如何使用周邊設備存取控管功能來保護電腦免於受到安全威脅的侵襲。

本章內容：

周邊設備存取控管

周邊設備存取控管會規範對連線到電腦的外部儲存裝置與網路資源的存取。周邊設備存取控管有助於防止資料遺失與外洩，並且可與檔案掃瞄搭配使用，以協助防禦安全威脅。

您可以為內部和外部用戶端設定「周邊設備存取控管」策略。OfficeScan 管理員通常會針對外部用戶端設定較嚴格的策略。

策略是 OfficeScan 用戶端樹狀結構中的詳細設定。您可以對用戶端群組或個別用戶端強制執行特定的策略。您也可以對所有用戶端強制執行單一策略。

部署策略之後，用戶端會使用您在「電腦位置」畫面（請參閱電腦位置 第 14-2 頁）中設定的位置條件來判斷其位置和要套用的策略。用戶端會在每次位置變更時切換策略。

重要：

- 依預設，所有版本的 Windows Server 2003、Windows Server 2008 和 Windows Server 2012 會關閉「周邊設備存取控管」。在這些伺服器平台上啟動「周邊設備存取控管」之前，請先閱讀 OfficeScan 用戶端服務 第 14-6 頁中所述的指導方針和最佳做法。
- OfficeScan 可監控的裝置類型取決於是否已註冊「資料安全防護」使用授權。您必須另行為「資料安全防護」模組取得使用授權，而且必須先啟動此模組才能使用它。如需有關「資料安全防護」使用授權的詳細資訊，請參閱資料安全防護使用授權 第 3-4 頁。

表 9-1. 裝置類型

	資料安全防護已註冊	資料安全防護未註冊
儲存裝置		
CD/DVD	已監控	已監控
軟碟	已監控	已監控
網路磁碟機	已監控	已監控
USB 儲存裝置	已監控	已監控

	資料安全防護已註冊	資料安全防護未註冊
非儲存裝置		
COM 和 LPT 通訊埠	已監控	未監控
IEEE 1394 介面	已監控	未監控
影像裝置	已監控	未監控
紅外線裝置	已監控	未監控
數據機	已監控	未監控
PCMCIA 卡	已監控	未監控
列印螢幕鍵	已監控	未監控

- 如需支援的裝置型號清單，請參閱：

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

儲存裝置的權限

當您執行下列動作時會使用儲存裝置的「周邊設備存取控管」權限：

- 允許存取 USB 儲存裝置、CD/DVD、磁片和網路磁碟機。您可以授與對這些裝置的完整存取權，或限制存取等級。
- 設定核可 USB 儲存裝置的清單。「周邊設備存取控管」可讓您封鎖對所有 USB 儲存裝置的存取，但已新增至核可裝置清單的 USB 儲存裝置除外。您可以授與對核可裝置的完整存取權，或限制存取等級。

以下表格列出了儲存裝置的權限。

表 9-2. 儲存裝置的周邊設備存取控管權限

權限	裝置上的檔案	輸入的檔案
完整存取權	允許的作業：複製、移動、開啟、儲存、刪除、執行	允許的作業：儲存、移動、複製 這表示檔案可以儲存、移動與複製到裝置上。
修改	允許的作業：複製、移動、開啟、儲存、刪除 禁止的作業：執行	允許的作業：儲存、移動、複製
讀取和執行	允許的作業：複製、開啟、執行 禁止的作業：儲存、移動、刪除	禁止的作業：儲存、移動、複製
讀取	允許的作業：複製、開啟 禁止的作業：儲存、移動、刪除、執行	禁止的作業：儲存、移動、複製
僅列出裝置內容	禁止的作業：所有作業 向使用者顯示裝置與其包含的檔案（例如，從 Windows 檔案總管）。	禁止的作業：儲存、移動、複製
封鎖 （安裝資料安全防護後即可使用）	禁止的作業：所有作業 不向使用者顯示裝置與其包含的檔案（例如，從 Windows 檔案總管）。	禁止的作業：儲存、移動、複製

OfficeScan 中的檔案型掃瞄功能可彌補裝置權限之不足，甚至加以覆寫。例如，如果權限允許開啟檔案，但 OfficeScan 偵測到檔案已感染惡意程式，則會對該檔案執行特定的中毒處理行動，以消除惡意程式。如果中毒處理行動為「清除」，檔案將會在清除後開啟。但是，如果中毒處理行動為「刪除」，則會刪除檔案。

秘訣

資料安全防護的周邊設備存取控管功能支援所有的 64 位元平台。如果要在 OfficeScan 不支援的系統上監控未經授權的變更阻止（詳細資訊請參閱 未經授權的變更防護支援周邊設備存取控管（64 位元） 第 1-5 頁），請將裝置權限設定為封鎖，以限制這些裝置的存取權。

儲存裝置的進階權限

進階權限適用於已授與有限的權限給儲存裝置的情況。權限可以是下列任一種：

- 修改
- 讀取和執行
- 讀取
- 僅列出裝置內容

您可以繼續維持受限的權限，但將進階權限授與儲存裝置和本機電腦上的某些程式。

如果要定義程式，請設定下列程式清單。

表 9-3. 程式清單

程式清單	說明	有效的輸入
對裝置具有讀取與寫入權限的程式	此清單包含的本機程式和儲存裝置上的程式，對裝置具有讀取和寫入權限。 Microsoft Word (`winword.exe`) 是本機程式的範例，它通常位於 `C:\Program Files\Microsoft Office\Office`。如果 USB 儲存裝置的權限是「僅列出裝置內容」，但在此清單中包含 `C:\Program Files\Microsoft Office\Office\winword.exe`： • 使用者將具有從 Microsoft Word 存取之 USB 儲存裝置上所有檔案的讀取和寫入權限。 • 使用者可以儲存、移動或複製 Microsoft Word 檔案到 USB 儲存裝置。	程式路徑和名稱 如需詳細資訊，請參閱指定程式路徑和名稱 第 9-7 頁。
裝置上允許執行的程式	此清單包含使用者或系統可以在儲存裝置上執行的程式。 例如，如果您要允許使用者從 CD 安裝軟體，請將安裝程式路徑和名稱（例如 `E:\Installer\Setup.exe`）新增到此單。	程式路徑和名稱或數位簽章提供者 如需詳細資訊，請參閱指定程式路徑和名稱 第 9-7 頁 或指定數位簽章提供者 第 9-7 頁。

以下是當您需要新增程式到這兩種清單時的建議。考慮使用 USB 儲存裝置的資料鎖定功能，啟動此功能後，會提示使用者輸入有效的使用者名稱和密碼才能解除鎖定裝置。資料鎖定功能使用裝置上名為 `Password.exe` 的程式，必須允許此程式執行，使用者才能成功解除鎖定裝置。`Password.exe` 也必須具有裝置的讀取和寫入權限，使用者才能變更使用者名稱或密碼。

使用者介面的每個程式清單可容納多達 100 個程式。如果您要新增更多程式到程式清單，請新增至 `ofcscan.ini` 檔案，該檔案可容納多達 1,000 個程式。如需新增程式到 `ofcscan.ini` 檔案的指示，請參閱「使用 ofcscan.ini 將程式新增到周邊設備存取控管程式清單 第 9-13 頁」。

警告!

新增到 `ofcscan.ini` 檔案的程式會部署至根網域，並且會覆寫個別網域和用戶端上的程式。

指定數位簽章提供者

指定您所信任由其發行之程式的數位簽章提供者。例如，輸入 Microsoft Corporation 或 Trend Micro, Inc.。您可以透過檢查程式的內容（例如，在程式上按一下滑鼠右鍵並選取「內容」）取得數位簽章提供者。

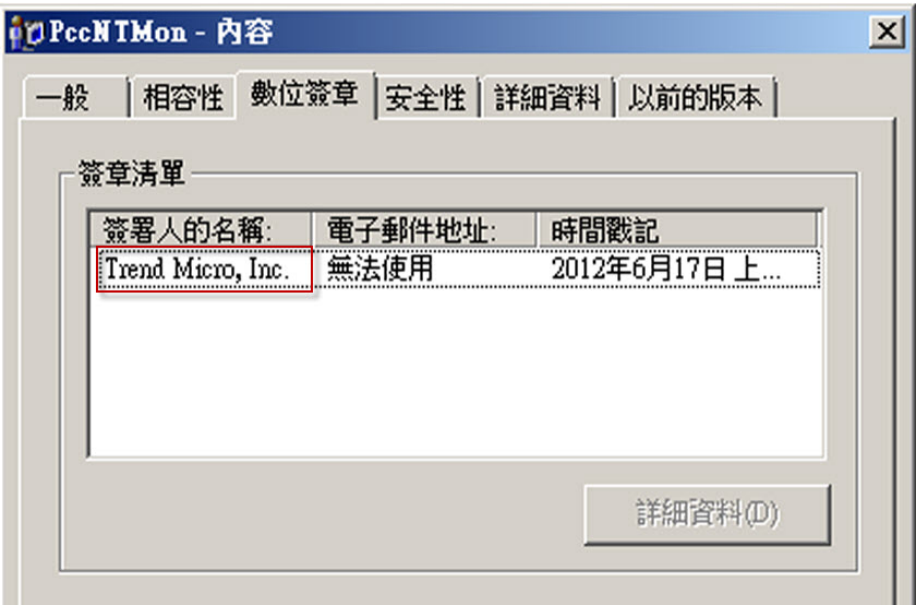


圖 9-1. OfficeScan 用戶端程式 (`PccNTMon.exe`) 的數位簽章提供者

指定程式路徑和名稱

程式路徑和名稱的長度上限為 259 個字元，並且只能包含英數字元 (A-Z、a-z、0-9)。您不能只指定程式名稱。

您可以使用萬用字元取代磁碟機代號和程式名稱。使用問號 (?) 代表單一字元資料（例如：磁碟機代號）。使用星號 (*) 代表多字元資料（例如：程式名稱）。

注意

您不能使用萬用字元代表資料夾名稱。必須指定資料夾的確實名稱。

下列是正確使用萬用字元的範例：

表 9-4. 正確的萬用字元用法

範例	符合的資料
?:\Password.exe	位於任何磁碟機正下方的「Password.exe」檔案
C:\Program Files\Microsoft *.exe	C:\Program Files 中所有具有副檔名的檔案
C:\Program Files*.*	C:\Program Files 中所有具有副檔名的檔案
C:\Program Files\a?c.exe	位於 C:\Program Files 中，具有 3 個字元且開頭為字母「a」，結尾為字母「c」的任何 .exe 檔案
C:*	位於 C:\ 磁碟機根目錄的所有檔案（含或不含副檔名）

下列是不正確使用萬用字元的範例：

表 9-5. 不正確的萬用字元用法

範例	原因
??:\Buffalo\Password.exe	?? 代表兩個字元，但磁碟機代號只能有一個字母字元。
*:\Buffalo\Password.exe	* 代表多字元資料，但磁碟機代號只能有一個字母字元。
C:*\Password.exe	您不能使用萬用字元代表資料夾名稱。必須指定資料夾的確實名稱。
C:\?\Password.exe	

非儲存裝置的權限

您可以允許或封鎖對非儲存裝置的存取。這些裝置沒有細微或進階權限。

管理外部裝置存取（已啟動資料安全防護）

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 周邊設備存取控管設定」。
4. 按一下「外部用戶端」標籤以設定外部用戶端的設定，或按一下「內部用戶端」標籤以設定內部用戶端的設定。
5. 選取「啟動周邊設備存取控管」。
6. 如下所示套用設定：
   - 如果您使用的是「外部用戶端」標籤，則可以透過選取「套用所有設定至內部用戶端」將設定套用至內部用戶端。
   - 如果您使用的是「內部用戶端」標籤，則可以透過選取「套用所有設定至外部用戶端」將設定套用至外部用戶端。
7. 選擇允許或封鎖 USB 儲存裝置的自動執行功能 (`autorun.inf`)。
8. 針對儲存裝置設定相關選項。
   a. 為每個儲存裝置選取權限。如需有關權限的詳細資訊，請參閱儲存裝置的權限 第 9-3 頁。
   b. 如果 USB 儲存裝置的權限是「封鎖」，請設定核可裝置的清單。使用者可以存取這些裝置，而您可以使用權限來控制存取等級。請參閱設定 USB 裝置核可清單 第 9-11 頁。
9. 針對每個非儲存裝置，選取「允許」或「封鎖」。

10. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

    - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
    - 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

設定進階權限

雖然您可以設定使用者介面上特定儲存裝置的進階權限與通知，但權限與通知實際上會套用至所有儲存裝置。這表示當您按一下 CD/DVD 的「進階權限與通知」時，實際上是定義所有儲存裝置的權限與通知。

注意

如需有關進階權限以及如何正確使用進階權限定義程式的詳細資訊，請參閱儲存裝置的進階權限 第 9-5 頁。

程序

1. 按一下「進階權限與通知」。

   接著會開啟一個新畫面。

2. 在「對儲存裝置具有讀取和寫入權限的程式」下方，輸入程式路徑和檔案名稱，然後按一下「新增」。

   不接受數位簽章提供者。

3. 在「儲存裝置上允許執行的程式」下方，輸入程式路徑和名稱或數位簽章提供者，然後按一下「新增」。

4. 選取「當 OfficeScan 偵測到未經授權的裝置存取時，會在用戶端電腦上顯示通知訊息」。

- 未經授權的裝置存取是指禁止的裝置作業。例如，如果裝置權限是「讀取」，使用者就無法在裝置上儲存、移動、刪除或執行檔案。如需根據權限的禁止裝置作業清單，請參閱儲存裝置的權限 第 9-3 頁。
- 您可以修改通知訊息。如需詳細資訊，請參閱修改周邊設備存取控管通知 第 9-15 頁。

5. 按一下「上一步」。

設定 USB 裝置核可清單

USB 裝置的核可清單支援使用星號 (*) 萬用字元。以星號 (*) 取代任何欄位，以包含符合其他欄位要求的所有裝置。例如，[vendor]-[model]-* 會將指定廠商和指定型號類型的所有 USB 裝置置於核可清單中，而不論序號 ID 為何。

程序

1. 按一下「核可的裝置」。
2. 輸入裝置廠商。
3. 輸入裝置型號和序號 ID。

> 秘訣
>
> 使用「裝置清單工具」查詢連接至端點的裝置。此工具可以提供每個裝置的裝置廠商、型號和序號 ID。如需詳細資訊，請參閱裝置清單工具 第 9-12 頁。

4. 為裝置選取權限。

   如需有關權限的詳細資訊，請參閱儲存裝置的權限 第 9-3 頁。

5. 如果要新增更多裝置，請按一下加號 (+) 圖示。
6. 按一下<「上一步」。

裝置清單工具

在每個本機端點上執行「裝置清單工具」可查詢連接到端點的外部裝置。此工具會掃瞄端點是否連接外部裝置，然後在瀏覽器視窗中顯示裝置資訊。接著，您可以在設定「Data Loss Prevention」和「周邊設備存取控管」的裝置設定時使用這些資訊。

如果要執行「裝置清單工具」

程序

1. 在 OfficeScan 伺服器電腦上，瀏覽到`\PCCSRV\Admin\Utility\ListDeviceInfo`。
2. 將 `listDeviceInfo.exe` 複製到目標端點。
3. 在端點上，執行 `listDeviceInfo.exe`。
4. 在顯示的瀏覽器視窗中檢視裝置資訊。「Data Loss Prevention」和「周邊設備存取控管」使用下列資訊：
   - 廠商（必要）
   - 型號（選用）
   - 序號 ID（選用）

管理外部裝置存取（已啟動資料安全防護）

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 周邊設備存取控管設定」。

4. 按一下「外部用戶端」標籤以設定外部用戶端的設定，或按一下「內部用戶端」標籤以設定內部用戶端的設定。

5. 選取「啟動周邊設備存取控管」。

6. 如下所示套用設定：

   - 如果您使用的是「外部用戶端」標籤，則可以透過選取「套用所有設定至內部用戶端」將設定套用至內部用戶端。

   - 如果您使用的是「內部用戶端」標籤，則可以透過選取「套用所有設定至外部用戶端」將設定套用至外部用戶端。

7. 選擇允許或封鎖 USB 儲存裝置的自動執行功能 (`autorun.inf`)。

8. 為每個儲存裝置選取權限。如需有關權限的詳細資訊，請參閱儲存裝置的權限 第 9-3 頁。

9. 如果儲存裝置的權限是下列任一種，請設定進階權限與通知：「修改」，「讀取和執行」，「讀取」，或「僅列出裝置內容」.請參閱設定進階權限 第 9-10 頁。

10. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

    - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。

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

使用 ofcscan.ini 新增程式到周邊設備存取控管清單

注意

如需關於程式清單以及如何正確定義可新增至清單的程式的詳細資訊，請參閱儲存裝置的進階權限 第 9-5 頁。

程序

1. 在 OfficeScan 伺服器電腦上，瀏覽至<伺服器安裝資料夾>\PCCSRV。
2. 使用文字編輯器開啟 ofcscan.ini。
3. 如果要新增對儲存裝置具有讀取和寫入權限的程式：
   a. 找到下列各行：

      ```
      [DAC_APPROVED_LIST]

      Count=x
      ```

   b. 請將「x」換成程式清單中的程式數量。
   c. 在「Count=x」下方，輸入下列命令來新增程式：

      ```
      Item<編號>=<程式路徑和名稱或數位簽章提供者>
      ```

      例如：

      ```
      [DAC_APPROVED_LIST]

      Count=3

      Item0=C:\Program Files\program.exe

      Item1=?:\password.exe

      Item2=Microsoft Corporation
      ```

4. 如果要新增儲存裝置上允許執行的程式：
   a. 找到下列各行：

      ```
      [DAC_EXECUTABLE_LIST]

      Count=x
      ```

   b. 請將「x」換成程式清單中的程式數量。
   c. 在「Count=x」下方，輸入下列命令來新增程式：

      ```
      Item<編號>=<程式路徑和名稱或數位簽章提供者>
      ```

例如：

```
[DAC_EXECUTABLE_LIST]

Count=3

Item0=?:\Installer\Setup.exe

Item1=E:\*.exe

Item2=Trend Micro, Inc.
```

5. 儲存並關閉 `ofcscan.ini` 檔案。
6. 開啟 OfficeScan Web 主控台上，並移至「用戶端電腦 > 全域用戶端設定」。
7. 按一下「儲存」，將程式清單套用至所有用戶端。

修改周邊設備存取控管通知

發生「周邊設備存取控管」違規事件時，端點上會顯示通知訊息。管理員可視需要修改預設通知訊息。

程序

1. 瀏覽至「通知 > 用戶端使用者通知」。
2. 按一下「周邊設備存取控管違規」標籤。
3. 在提供的文字方塊中修改預設訊息。
4. 按一下「儲存」。

周邊設備存取控管記錄檔

OfficeScan 用戶端可記錄未經授權的裝置存取案例，並將記錄檔傳送至伺服器。持續運作的用戶端會每 24 小時彙整記錄檔並進行傳送。重新啟動後的用戶端會檢查記錄檔上次傳送至伺服器的時間。如果經過的時間超過 24 小時，則用戶端會立即傳送記錄檔。

如果要避免記錄檔佔去過多硬碟空間，請手動刪除記錄檔或設定記錄檔刪除預約時程。如需有關管理記錄檔的詳細資訊，請參閱記錄檔管理 第 13-31 頁。

檢視周邊設備存取控管記錄檔

程序

1. 瀏覽至「 記錄檔 > 用戶端電腦記錄檔 > 安全性風險」或「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「記錄檔 > 周邊設備存取控管記錄檔」或「檢視記錄檔 > 周邊設備存取控管記錄檔」。
4. 指定記錄條件，然後按一下「顯示記錄檔」。
5. 檢視記錄檔。記錄檔包含下列資訊：
   - 偵測到發生未經授權存取的日期/時間
   - 外部裝置所連接或網路資源所對應的電腦
   - 外部裝置所連接或網路資源所對應的電腦網域
   - 存取的裝置類型或網路資源
   - 目標，即存取的裝置或網路資源上的項目
   - 存取者，可指定開始存取的位置
   - 為目標設定的權限

6. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請按一下「匯出到 CSV」。開啟檔案或將其儲存至特定位置。

第 10 章

使用 Data Loss Prevention

本章討論如何使用 Data Loss Prevention 功能。

本章內容：

關於 Data Loss Prevention

傳統的安全解決方案著重於防止外部安全威脅入侵網路。在現今的安全環境中，這麼做卻只能有一半的效果。資料遭到侵害的情況相當普遍，這會將組織的機密與敏感資料（稱為數位資產）暴露給外部未經授權的人員。資料遭到侵害可能是因為內部員工出錯或大意、資料外包、電腦設備遭竊或隨意放置、或惡意的攻擊所造成的。

資料外洩會導致：

- 品牌商譽受損
- 客戶對公司的信任度降低
- 為了進行補救措施而投入不必要的成本，以及因不遵守法規而須支付罰金
- 因智慧財產被盜，錯失商機和收益

隨著資料外洩情況越來越普遍以及因此而帶來的損害，許多公司現在都將數位資產保護視為安全措施的關鍵要素。

「Data Loss Prevention」可保護組織的機密資料，免遭受意外或有意的外洩。Data Loss Prevention 允許您：

- 使用資料識別碼識別需要保護的機密資訊
- 建立策略，以限制或防止透過常見傳輸通道（例如：電子郵件和外部裝置）傳輸數位資產
- 強制遵守制定的隱私權標準

您必須能夠回答下列問題，才能監控可能損失的機密資訊：

- 必須保護哪些資料以防止未經授權的使用者存取？
- 機密資料儲存於何處？
- 機密資料的傳輸方式為何？
- 哪些使用者具有存取或傳輸機密資料的授權？
- 發生安全違規時應採取哪些處理行動？

這項重要的監看通常涉及組織中經常接觸機密資訊的多個部門及個人。

如果您已經定義您的機密資訊與安全策略，則可以開始定義資料識別碼和公司策略。

Data Loss Prevention 策略

OfficeScan 會根據「DLP 策略」中定義的一組規則來評估檔案或資料。策略會決定必須保護以防止未經授權傳輸的檔案或資料，以及 OfficeScan 在偵測到傳輸活動時所執行的處理行動。

注意

系統不會監控 OfficeScan 伺服器和其用戶端之間的資料傳輸。

您可以為內部和外部用戶端設定策略。OfficeScan 管理員通常會針對外部用戶端設定較嚴格的策略。

您可以對用戶端群組或個別用戶端強制執行特定的策略。您也可以對所有用戶端強制執行單一策略。

部署策略之後，用戶端會使用您在「電腦位置」畫面（請參閱電腦位置 第 14-2 頁）中設定的位置條件來判斷其位置和要套用的策略。用戶端會在每次位置變更時切換策略。

策略組態設定

透過設定下列設定並將其部署至所選用戶端，來定義 DLP 策略：

表 10-1. 定義「DLP 策略」的設定

設定	說明
資料識別碼	OfficeScan 使用資料識別碼來識別機密資訊。資料識別碼包括運算式、檔案屬性，以及充當 DLP 範本之建置組塊的關鍵字。
規則	DLP 規則可由多個範本、通道和處理行動組成。每個規則都是包含的 DLP 策略的子集合。

設定	說明
範本	DLP 範本結合資料識別碼與邏輯運算子 (And、Or、Except) 以形成條件陳述式。只有滿足特定條件陳述式的檔案或資料才會受到 DLP 規則的管制。 OfficeScan 隨附一組已預先定義的範本，而且可讓您建立自訂範本。 DLP 規則可包含一個或多個範本。OfficeScan 檢查範本時會使用第一個符合的規則。這表示，如果有檔案或資料符合某個範本中的資料識別碼，OfficeScan 就不會再檢查其他範本。
通道	通道是傳輸機密資訊的實體。OfficeScan 支援常用的傳輸通道，例如，電子郵件、卸除式儲存裝置，以及即時通訊應用程式。
處理行動	當 OfficeScan 偵測到嘗試透過任一通道傳輸機密資訊的操作時，它會執行一或多個處理行動。
例外	例外用於覆寫設定的 DLP 規則。設定例外以管理不受監控的目標、受監控的目標以及壓縮檔掃瞄。

資料識別碼類型

數位資產是組織必須保護以防止未經授權傳輸的檔案和資料。您可以透過下列資料識別碼定義數位資產：

- 表示式：具有特定結構的資料。如需詳細資訊，請參閱表示式 第 10-5 頁。
- 檔案屬性：檔案類型和檔案大小等檔案內容。如需詳細資訊，請參閱檔案屬性 第 10-9 頁。
- 關鍵字：特殊字詞或字組的清單。如需詳細資訊，請參閱關鍵字 第 10-12 頁。

注意

您無法刪除目前正在「DLP 範本」中使用的資料識別碼。請先刪除範本，再刪除資料識別碼。

表示式

表示式是具有特定結構的資料。例如，信用卡號碼通常有 16 位數字，而且其格式為 "nnnn-nnnn-nnnn-nnnn"，因此很適合透過表示式來偵測。

您可以使用已預先定義的表示式或自訂表示式。如需詳細資訊，請參閱預先定義的表示式 第 10-5 頁和自訂表示式 第 10-6 頁。

預先定義的表示式

OfficeScan 隨附一組預先定義的例外。您無法修改或刪除這些表示式。

OfficeScan 會使用病毒碼比對和數學方程式來驗證這些表示式。OfficeScan 將可能的機密資料與表示式進行比對之後，可能還會對資料進行其他的驗證檢查。

如需完整的預先定義表示式清單，請參閱 http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx。

檢視預先定義的表示式設定

注意

預先定義的表示式無法修改或刪除。

程序

1. 瀏覽至「 用戶端電腦 > Data Loss Prevention > 資料識別碼 」。
2. 按一下「表示式」標籤。
3. 按一下某個表示式名稱。
4. 在開啟的畫面中檢視設定。

自訂表示式

如果預先定義的表示式不符合您的需求，您可以建立自訂表示式。

表示式是功能強大的字串比對工具。建立表示式之前，請確定您已熟悉表示式語法。設計不良的表示式會嚴重影響效能。

建立表示式時：

- 請參閱預先定義的表示式，瞭解如何定義有效的表示式。例如，如果要建立包含日期的表示式，您可以參閱以「Date」為字首的表示式。
- 請注意，OfficeScan 遵循 Perl Compatible Regular Expressions (PCRE) 中定義的表示式格式。如需 PCRE 的詳細資訊，請造訪下列網站：

  http://www.pcre.org/
- 從簡單的表示式開始。如果表示式造成誤判，請予以修改；您也可以微調表示式以提高偵測的正確性。

建立表示式時，您可以選擇數種條件。表示式必須符合您選擇的條件，OfficeScan 才能將它套用到 DLP 策略。如需有關不同條件選項的詳細資訊，請參閱自訂表示式的條件 第 10-6 頁。

自訂表示式的條件

表 10-2. 自訂表示式的條件選項

條件	規則	範例
無	無	全部 — 來自「美國戶口普查局」的姓名 表示式：[^\w]([A-Z][a-z]{1,12}(\s?,\s?|[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]

條件	規則	範例
特定字元	表示式必須包含您指定的字元。 此外，表示式中的字元數目必須介於下限到上限之間。	美國 — 美國銀行轉帳號碼 表示式：[^\d]([0123678]\d{8})[^\d] 字元： 0123456789 字元數目下限： 9 字元數目上限： 9
字尾	字尾是指表示式的最後部分。字尾必須包含您指定的字元並包含特定數目的字元。 此外，表示式中的字元數目必須介於下限到上限之間。	全部 — 住家地址 表示式：\D(\d+\s[a-z.]+\s([a-z]+\s){0,2} (lane|ln|street|st|avenue|ave|road|rd|place|pl|drive|dr|circle| cr|court|ct|boulevard|blvd)\.?[0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\ s\d{5}(-\d{4})?)[^\d-] 字尾字元： 0123456789- 字元數目： 5 表示式中的字元數目下限： 25 表示式中的字元數目上限： 80
單一字元分隔符號	表示式必須要有兩個部分並用一個字元分隔。這個字元的長度必須是 1 個位元組。 此外，分隔符號左邊的字元數目必須介於下限到上限之間。分隔符號右邊的字元數目不能超過上限。	全部 — 電子郵件信箱 表示式：[^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] 分隔符號： @ 左邊字元數目下限： 3 左邊字元數目上限： 15 右邊字元數目上限： 30

建立自訂表示式

程序

1. 瀏覽至「 用戶端電腦 > Data Loss Prevention > 資料識別碼 」。

2. 按一下「表示式」標籤。
3. 按一下「新增」。

   接著會顯示一個新畫面。
4. 輸入表示式的名稱。名稱的長度不能超過 100 個位元組，而且不能包含下列字元：

   - > < * ^ | & ? \ /
5. 請輸入長度不超過 256 個位元組的說明。
6. 輸入表示式並指定是否區分大小寫。
7. 輸入顯示的資料。

   例如，如果要建立識別碼的表示式，請輸入範例識別碼。此資料僅供參考，而且不會顯示在產品的任何地方。
8. 選擇下列其中一個條件，並為選擇的條件配置其他設定（請參閱自訂表示式的條件 第 10-6 頁）：

   - 無
   - 特定字元
   - 字尾
   - 單一字元分隔符號
9. 針對實際資料測試表示式。

   例如，如果表示式會評估國碼，請在「測試資料」文字方塊中輸入有效的識別碼，按一下「測試」，然後檢查結果。
10. 如果您對結果感到滿意，請按一下「儲存」。

注意

只在測試成功時才儲存設定。無法偵測到任何資料的表示式會浪費系統資源，而且可能會影響效能。

11. 接著會出現一則訊息，提醒您將此設定部署到用戶端。按一下「關閉」。

12. 回到「DLP 資料識別碼」畫面，按一下「 套用至所有用戶端 」。

匯入自訂表示式

如果您有包含表示式且格式正確的 .dat 檔案，請使用此選項。您可以從目前正在存取的 OfficeScan 伺服器或其他 OfficeScan 伺服器匯出表示式，來產生該檔案。

注意

由此 OfficeScan 版本產生的 .dat 表示式檔案與先前版本不相容。

程序

1. 瀏覽至「 用戶端電腦 > Data Loss Prevention > 資料識別碼 」。
2. 按一下「表示式」標籤。
3. 按一下「匯入」，然後尋找包含表示式的 .dat 檔案。
4. 按一下「開啟」。

   隨即顯示訊息，通知您是否匯入成功。如果要匯入的表示式已存在，系統將會略過該表示式。
5. 按一下「套用至所有用戶端」。

檔案屬性

檔案屬性是檔案的特定內容。定義資料識別碼時，您可以使用兩種檔案屬性，亦即檔案類型和檔案大小。例如，某個軟體開發公司可能想要限制只能與研發部門（其成員負責開發和測試該軟體）共用該公司的軟體安裝程式。在此案例中，OfficeScan 管理員可以建立一個策略，禁止將大小為 10 到 40MB 的可執行檔案傳輸到 R&D 以外的所有部門。

對於機密檔案而言，單獨使用檔案屬性不是很可靠。承上例，這樣可能也會封鎖其他部門分享的協力廠商軟體安裝程式。因此，趨勢科技建議您將檔案屬性與其他 DLP 資料識別碼結合，以便提高偵測機密檔案的正確性。

如需完整的支援檔案類型清單，請參閱 http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx。

建立檔案屬性清單

程序

1. 瀏覽至「 用戶端電腦 > Data Loss Prevention > 資料識別碼 」。
2. 按一下「檔案屬性」標籤。
3. 按一下「新增」。

   接著會顯示一個新畫面。
4. 輸入檔案屬性清單的名稱。名稱的長度不能超過 100 個位元組，而且不能包含下列字元：

   - > < * ^ | & ? \ /
5. 請輸入長度不超過 256 個位元組的說明。
6. 選取您偏好的真實檔案類型。
7. 如果您要包含的檔案類型並未列出，請選取「副檔名」，然後輸入檔案類型的副檔名。OfficeScan 會檢查具有指定副檔名的檔案，而不會檢查其真實檔案類型。指定副檔名的指導方針：

   - 每個副檔名必須以星號 (*) 為開頭，後接句點 (.)，然後是副檔名。星號是萬用字元，代表檔案的實際名稱。例如，`*.pol` 的相符項目有 `12345.pol` 和 `test.pol`。
   - 您可以在副檔名包含萬用字元。使用問號 (?) 代表單一字元，星號 (*) 代表兩個以上字元。請參閱下列範例：

     - `*.*m` 的相符項目有下列檔案：`ABC.dem`, `ABC.prm`, `ABC.sdcm`

     - `*.m*r` 的相符項目有下列檔案：`ABC.mgdr`, `ABC.mtp2r`, `ABC.mdmr`

- *.fm? 的相符項目有下列檔案：ABC.fme, ABC.fml, ABC.fmp

- 在副檔名的結尾加上星號時請務必小心，因為這可能會與部分檔案名稱及不相關的副檔名相符。例如：*.do* 的相符項目有 abc.doctor_john.jpg 和 abc.donor12.pdf。

- 請使用分號 (;) 來分隔副檔名。分號後面不用加上空格。

8. 輸入檔案大小下限和上限（以位元組為單位）。這兩個檔案大小值必須是大於零的正整數。

9. 按一下「儲存」。

10. 接著會出現一則訊息，提醒您將此設定部署到用戶端。按一下「關閉」。

11. 回到「DLP 資料識別碼」畫面，按一下「 套用至所有用戶端 」。

匯入檔案屬性清單

如果您有包含檔案屬性清單且格式正確的 .dat 檔案，請使用此選項。您可以從目前正在存取的 OfficeScan 伺服器或其他 OfficeScan 伺服器匯出檔案屬性清單，來產生該檔案。

注意

由此 OfficeScan 版本產生的 .dat 檔案屬性與先前版本不相容。

程序

1. 瀏覽至「 用戶端電腦 > Data Loss Prevention > 資料識別碼 」。

2. 按一下「檔案屬性」標籤。

3. 按一下「匯入」，然後尋找包含檔案屬性清單的 .dat 檔案。

4. 按一下「開啟」。

   隨即顯示訊息，通知您是否匯入成功。如果要匯入的檔案屬性清單已存在，系統將會略過該清單。

5. 按一下「套用至所有用戶端」。

關鍵字

關鍵字是特殊字詞或字組。您可以將相關關鍵字新增到關鍵字清單，以識別特定資料類型。例如，「診斷」、「血型」、「接種」和「醫師」是可能出現在診斷書中的關鍵字。如果要防止傳輸診斷書檔案，您可以在 DLP 策略中使用這些關鍵字，然後將 OfficeScan 配置為封鎖包含這些關鍵字的檔案。

您可以結合常用字詞以構成有意義的關鍵字。例如，您可以結合 "end"、"read"、"if" 和 "at"，以構成可在原始碼中找到的關鍵字（例如："END-IF"、"END-READ" 和 "AT END"）。

您可以使用已預先定義的關鍵字清單或自訂關鍵字清單。如需詳細資訊，請參閱預先定義的關鍵字清單 第 10-12 頁和自訂關鍵字清單 第 10-13 頁。

預先定義的關鍵字清單

OfficeScan 隨附一組預先定義的關鍵字清單。您無法修改或刪除這些關鍵字清單。每個清單都有自己的內建條件，可判斷該範本是否會觸發策略違規

如需 OfficeScan 中預先定義關鍵字清單的詳細資訊，請參閱 http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx。

關鍵字清單的運作方式

關鍵字條件的數目

每個關鍵字清單都包含要求文件中必須有特定數目的關鍵字之條件，以免該清單觸發違規。

關鍵字數目條件包含下列值：

- 所有：清單中所有關鍵字都必須出現在文件中。

- 任何：清單中任一關鍵字必須出現在文件中。
- 特定次數：文件中至少要有指定的關鍵字數目。如果文件中的關鍵字數目比指定的數目多，則會觸發違規。

距離條件

某些清單會包含「距離」條件以判定是否有違規情形。「距離」指的是某關鍵字的第一個字元和另一個關鍵的第一個字元之間的字元數。請考慮下列項目：

名字：_John_ L 姓氏：_Smith_

此表單 — 名字、姓氏清單包含「距離」條件：五十 (50)，以及常用的表單欄位：「名字」和「姓氏」。以上述的範例而言，當名字的「名」和姓氏的「姓」之間的字元數為十八 (18)，即會觸發違規。

不會觸發違規的項目範例，請考慮以下幾點：

來自瑞士的一名新進員工名字叫做 John，姓氏是 Smith。

在此範例中，名字的「名」和姓氏的「姓」之間的字元數為六十一 (61)。已超過距離的門檻值，所以不會觸發違規。

自訂關鍵字清單

如果預先定義的關鍵字清單不符合您的需求，您可以建立自訂關鍵字清單。

設定關鍵字清單時，您可以選擇數種條件。關鍵字清單必須符合您選擇的條件，OfficeScan 才能將它套用到 DLP 策略。為每個關鍵字清單選擇下列其中一個條件：

- 任何關鍵字
- 所有關鍵字
- 在 <x> 個字元內的所有關鍵字
- 關鍵字的結合評分超過門檻值

如需有關條件規則的詳細資訊，請參閱自訂關鍵字清單條件 第 10-14 頁。

自訂關鍵字清單條件

表 10-3. 關鍵字清單的條件

條件	規則
任何關鍵字	檔案至少必須包含關鍵字清單中的一個關鍵字。
所有關鍵字	檔案必須包含關鍵字清單中的所有關鍵字。
在 <x> 個字元內的所有關鍵字	檔案必須包含關鍵字清單中的所有關鍵字。此外，每個關鍵字組都必須在各自的 <x> 個字元內。 例如，您的 3 個關鍵字是 WEB、DISK 和 USB，而您指定的字元數是 20。 如果 OfficeScan 偵測到以 DISK、WEB 和 USB 順序出現的全部關鍵字，從 DISK 的「D」到 WEB 的「W」，以及從 WEB 的「W」到 USB 的「U」的關鍵字最多只能有 20 個字元。 下列資料符合該條件：DISK####WEB############USB 下列資料不符合該條件：DISK******************WEB****USB（「D」和「W」之間有 23 個字元） 決定字元數時請記住，小數字（例如：10）的掃瞄時間通常比較快，但只會包含相對小的區域。這可能會使得偵測機密資料的機率降低，特別是對於大型檔案。當該數字增加時，涵蓋的區域也會增加，但是掃瞄時間會比較慢。
關鍵字的結合評分超過門檻值	檔案必須包含關鍵字清單中的一或多個關鍵字。如果只偵測到一個關鍵字，其評分必須高於門檻值。如果有多個關鍵字，其結合評分必須高於門檻值。 請為每個關鍵字指定介於 1 到 10 之間的評分。您應該為機密性較高的的字組或詞組（例如：對於人力資源部門的「調薪」）指定較高的評分。對於本身沒有太高權重的字組或詞組，則可以指定較低的評分。 設定門檻值時，請考慮您為關鍵字指定的評分。例如，如果您有五個關鍵字，而其中有三個關鍵字具有高優先順序，則門檻值可以等於或或低於那三個高優先順序關鍵字的結合評分。這表示偵測到這三個關鍵字時就可以將該檔案視為機密檔案。

建立關鍵字清單

程序

1. 瀏覽至「 用戶端電腦 > Data Loss Prevention > 資料識別碼 」。
2. 按一下「關鍵字」標籤。
3. 按一下「新增」。

   接著會顯示一個新畫面。
4. 輸入關鍵字清單的名稱。名稱的長度不能超過 100 個位元組，而且不能包含下列字元：

   - > < * ^ | & ? \ /
5. 請輸入長度不超過 256 個位元組的說明。
6. 選擇下列其中一個條件，並為選擇的條件設定其他設定：

   - 任何關鍵字
   - 所有關鍵字
   - 在 <x> 個字元內的所有關鍵字
   - 關鍵字的結合評分超過門檻值
7. 手動將關鍵字新增到清單中：

   a. 輸入長度介於 3 到 40 個位元組之間的關鍵字，並指定是否區分大小寫。

   b. 按一下「新增」。
8. 如果要使用「匯入」選項來新增關鍵字：

注意

如果您有包含關鍵字且格式正確的 .csv 檔案，請使用此選項。您可以從目前正在存取的 OfficeScan 伺服器或其他 OfficeScan 伺服器匯出關鍵字，來產生該檔案。

a. 按一下「匯入」，然後尋找包含關鍵字的 .csv 檔案。

b. 按一下「開啟」。

隨即顯示訊息，通知您是否匯入成功。如果要匯入的關鍵字已存在於該清單中，系統將會略過該關鍵字。

9. 如果要刪除某個關鍵字，請選取該關鍵字，然後按一下「刪除」。

10. 如果要匯出關鍵字：

注意

使用「匯出」功能來備份關鍵字或將它們匯入到另一台 OfficeScan 伺服器。將匯出關鍵字清單中的所有關鍵字。您無法匯出個別關鍵字。

a. 按一下「匯出」。

b. 將產生的 .csv 檔案儲存到想要的位置。

11. 按一下「儲存」。

12. 接著會出現一則訊息，提醒您將此設定部署到用戶端。按一下「關閉」。

13. 回到「DLP 資料識別碼」畫面，按一下「 套用至所有用戶端 」。

匯入關鍵字清單

如果您有包含關鍵字清單且格式正確的 .dat 檔案，請使用此選項。您可以從目前正在存取的 OfficeScan 伺服器或其他 OfficeScan 伺服器匯出關鍵字清單，來產生該檔案。

注意

由此 OfficeScan 版本產生的 .dat 關鍵字清單檔案與先前版本不相容。

程序

1. 瀏覽至「 用戶端電腦 > Data Loss Prevention > 資料識別碼 」。

2. 按一下「關鍵字」標籤。
3. 按一下「匯入」，然後尋找包含關鍵字清單的 .dat 檔案。
4. 按一下「開啟」。

   隨即顯示訊息，通知您是否匯入成功。如果要匯入的關鍵字清單已存在，系統將會略過該清單。
5. 按一下「套用至所有用戶端」。

Data Loss Prevention 範本

DLP 範本結合 DLP 資料識別碼與邏輯運算子 (And、Or、Except) 以形成條件陳述式。只有滿足特定條件陳述式的檔案或資料會受到 DLP 策略的管制。

例如，檔案必須是 Microsoft Word 檔案（檔案屬性）AND （且）必須包含特定法律詞彙（關鍵字）AND（且）必須包含 ID 號碼（表示式），才能受到「聘用合約」策略管制。此策略允許人力資源部門的員工透過列印方式傳輸檔案，以便將列印複本交由員工簽署。但禁止透過其他可能的通道（例如：電子郵件）傳輸。

如果您已經設定 DLP 資料識別碼，您也可以建立自己的範本。您也可以使用已預先定義的範本。如需詳細資訊，請參閱自訂的 DLP 範本 第 10-18 頁和預先定義的 DLP 範本 第 10-17 頁。

注意

您無法刪除目前正在「DLP 策略」中使用的範本。刪除範本之前，請先從策略移除範本。

預先定義的 DLP 範本

OfficeScan 隨附以下一組已預先定義的範本，供您視各種法規標準需求使用。您無法修改或刪除這些範本。

- GLBA：Gramm-Leach-Billey Act
- HIPAA：《健康保險流通與責任法案》
- PCI-DSS：《支付卡產業資料安全標準》
- SB-1386:美國參議院法案 1386
- US PII：美國的個人識別資訊

如需所有預先定義範本的目的，以及受保護的資料範本的詳細清單，請參閱 http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx。

自訂的 DLP 範本

如果您已經設定資料識別碼，請建立自己的範本。範本結合資料識別碼與邏輯運算子 (And、Or、Except) 以形成條件陳述式。

如需有關條件陳述式和邏輯運算子如何運作的詳細資訊和範例，請參閱 條件陳述式和邏輯運算子 第 10-18 頁。

條件陳述式和邏輯運算子

OfficeScan 會從左到右評估條件陳述式。設定條件陳述式時，請小心使用邏輯運算子。使用不當會造成條件陳述式錯誤，而且有可能產生意想不到的後果。

請參閱下表中的範例。

表 10-4. 條件陳述式範例

條件陳述式	解譯和範例
[資料識別碼 1] And [資料識別碼 2] Except [資料識別碼 3]	檔案必須滿足 [資料識別碼 1] 和 [資料識別碼 2] 但不用滿足 [資料識別碼 3]。 例如： 檔案必須是 [Adobe PDF 文件] 而且必須包含 [電子郵件信箱]，但是不應該包含 [關鍵字清單中的所有關鍵字]。

條件陳述式	解譯和範例
[資料識別碼 1] Or [資料識別碼 2]	檔案必須滿足 [資料識別碼 1] 或 [資料識別碼 2]。 例如： 檔案必須是 [Adobe PDF 文件] 或 [Microsoft Word 文件]。
Except [資料識別碼 1]	檔案必須不滿足 [資料識別碼 1]。 例如： 檔案不能是 [多媒體檔案]。

如表格中最後一個範例所示，如果檔案必須不能滿足陳述式中的所有資料識別碼，則條件陳述式中的第一個資料識別碼可以有「Except」運算子。不過，在大部分的情況下，第一個資料識別碼沒有運算子。

建立範本

程序

1. 瀏覽至「 用戶端電腦 > Data Loss Prevention > 範本 」。
2. 按一下「新增」。

   接著會顯示一個新畫面。
3. 輸入範本的名稱。名稱的長度不能超過 100 個位元組，而且不能包含下列字元：

   - > < * ^ | & ? \ /
4. 請輸入長度不超過 256 個位元組的說明。
5. 選取資料識別碼，然後按一下「新增」圖示。

   選取定義時：

   - 按住 CTRL 鍵，然後選取資料識別碼，就可以選取多個項目。
   - 如果想要使用特定定義，可以使用搜尋功能。您可以輸入完整或部分的資料識別碼名稱。

- 每個範本最多可以包含 30 個資料識別碼。

6. 如果要建立新的表示式，請按一下「表示式」，再按一下「新增表示式」。在顯示的畫面中，設定該表示式的設定。
7. 如果要建立新的檔案屬性清單，請按一下「檔案屬性」，再按一下「新增檔案屬性」。在顯示的畫面中，設定該檔案屬性清單的設定。
8. 如果要建立新的關鍵字清單，請按一下「關鍵字」，再按一下「新增關鍵字」。在顯示的畫面中，設定該關鍵字清單的設定。
9. 如果您選取表示式，請輸入出現次數，這是指 OfficeScan 將表示式套用至 DLP 策略之前，表示式必須出現的次數。
10. 為每個定義選擇邏輯運算子。

注意

設定條件陳述式時，請小心使用邏輯運算子。使用不當會造成條件陳述式錯誤，而且有可能產生意想不到的後果。如需正確用法範例，請參閱條件陳述式和邏輯運算子 第 10-18 頁。

---

11. 如果要從選取的識別碼清單中移除資料識別碼，請按一下資源回收筒圖示。
12. 在「預覽」下方，檢查條件陳述式並視需要修改不適用的陳述式。
13. 按一下「儲存」。
14. 接著會出現一則訊息，提醒您將此設定部署到用戶端。按一下「關閉」。
15. 返回「DLP 範本」畫面，按一下「套用至所有用戶端」。

匯入範本

如果您有包含範本且格式正確的 `.dat` 檔案，請使用此選項。您可以從目前正在存取的 OfficeScan 伺服器或其他 OfficeScan 伺服器匯出範本，來產生該檔案。

注意

如果要從 OfficeScan 10.6 版匯入 DLP 範本，請先匯入相關的資料識別碼（先前稱為「定義」）。OfficeScan 無法匯入缺少相關資料識別碼的範本。

程序

1. 瀏覽至「 用戶端電腦 > Data Loss Prevention > 範本 」。
2. 按一下「匯入」，然後尋找包含範本的 .dat 檔案。
3. 按一下「開啟」。

   隨即顯示訊息，通知您是否匯入成功。如果要匯入的範本已存在，系統將會略過該範本。
4. 按一下「套用至所有用戶端」。

DLP 通道

使用者可以透過各種通道傳輸機密資訊。OfficeScan 可以監控下列通道：

- 網路通道：機密資訊是藉由網路通訊協定 (例如 HTTP 和 FTP) 進行傳輸。
- 系統和應用程式通道：機密資訊是藉由本機電腦的應用程式和周邊進行傳輸。

網路通道

OfficeScan 可以監控透過下列網路通道傳輸的資料：

- 電子郵件用戶端
- FTP
- HTTP 和 HTTPS

- IM 應用程式
- SMB 通訊協定
- 網路郵件

為了決定要監控哪些資料傳輸，OfficeScan 會檢查您必須設定的傳輸範圍。根據您選取的範圍，OfficeScan 會監控所有資料傳輸或只監控區域網路 (LAN) 外部的傳輸。如需有關傳輸範圍的詳細資訊，請參閱網路通道的傳輸範圍和目標 第 10-25 頁。

電子郵件用戶端

OfficeScan 會監控透過各種電子郵件用戶端傳輸的電子郵件。OfficeScan 會檢查電子郵件的主旨、內文和附件是否包含資料識別碼。如需支援的電子郵件用戶端清單，請參閱：

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

當使用者嘗試傳送電子郵件時，就會予以監控。如果電子郵件包含資料識別碼，OfficeScan 會允許或封鎖該電子郵件。

您可以定義受監控和不受監控的內部電子郵件網域。

- 受監控的電子郵件網域：當 OfficeScan 偵測到傳輸至受監控網域的電子郵件時，它會檢查策略的處理行動。然後根據處理行動決定允許或封鎖傳輸。

  注意

  如果您選取電子郵件用戶端作為監控的通道，則電子郵件必須符合其受監控的策略。相反的，傳送到受監控電子郵件網域的電子郵件會自動受到監控，無論其是否符合策略。

- 不受監控的電子郵件網域：OfficeScan 會立即允許傳送到不受監控網域的電子郵件傳輸。

注意

資料傳輸至不受監控的電子郵件網域及受監控的電子郵件網域（中毒處理行動是「監控」）與允許傳輸的是類似的。唯一不同之處是 OfficeScan 不會記錄不受監控的電子郵件網域的傳輸，但一定會記錄受監控電子郵件網域的傳輸。

使用下列任一格式指定網域，並以逗號分隔多個網域：

- X400 格式，例如 /O=Trend/OU=USA, /O=Trend/OU=China
- 電子郵件網域，例如 example.com

對於透過 SMTP 通訊協定傳送的電子郵件，OfficeScan 會檢查目標 SMTP 伺服器是否在下列清單中：

1. 受監控的目標
2. 不受監控的目標

注意

如需有關受監控與不受監控的目標的詳細資訊，請參閱定義不受監控和受監控的目標 第 10-33 頁。

3. 受監控的電子郵件網域
4. 不受監控的電子郵件網域

這表示如果電子郵件是傳送到受監控目標清單中的 SMTP 伺服器，則電子郵件會受到監控。如果 SMTP 伺服器不在受監控目標清單中，則 OfficeScan 會檢查其他的清單。

對於透過其他通訊協定傳送的電子郵件，OfficeScan 只會檢查下列清單：

1. 受監控的電子郵件網域
2. 不受監控的電子郵件網域

FTP

當 OfficeScan 偵測到 FTP 用戶端嘗試將檔案上傳到 FTP 伺服器時，它會檢查檔案中是否包含資料識別碼。此時尚未上傳任何檔案。視 DLP 策略而定，OfficeScan 會允許或封鎖上傳。

當您設定會封鎖檔案上傳的策略時，請記住下列幾點：

- 當 OfficeScan 封鎖上傳時，某些 FTP 用戶端會嘗試重新上傳檔案。在此情況下，OfficeScan 會終止該 FTP 用戶端，以禁止重新上傳。FTP 用戶端終止後，使用者不會收到通知。當您實作 DLP 策略時，請將此情況告知使用者。
- 如果要上傳的檔案會覆寫 FTP 伺服器上的檔案，可能會刪除 FTP 伺服器上的檔案。

如需支援的 FTP 用戶端清單，請參閱：

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

HTTP 和 HTTPS

OfficeScan 會監控要透過 HTTP 和 HTTPS 傳輸的資料。對於 HTTPS，資料在加密及傳輸之前，OfficeScan 會先進行檢查。

如需支援的 Web 瀏覽器和應用程式清單，請參閱：

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

IM 應用程式

OfficeScan 會監控使用者透過即時通訊（IM）應用程式傳送的訊息和檔案，但不會監控使用者接收的訊息和檔案。

如需支援的 IM 應用程式清單，請參閱：

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

當 OfficeScan 封鎖透過 AOL Instant Messenger、MSN、Windows Messenger 或 Windows Live Messenger 傳送的訊息或檔案時，它也會終止應用程式。如果

OfficeScan 不這樣做，應用程式就會變成沒有回應，而且使用者仍會被迫終止應用程式。應用程式終止之後，使用者不會收到通知。當您實作 DLP 策略時，請將此情況告知使用者。

SMB 通訊協定

OfficeScan 會監控透過「伺服器訊息區」(SMB) 通訊協定傳輸的資料，這種通訊協定是用於共享檔案存取。當另一位使用者嘗試複製或讀取使用者共用的檔案時，OfficeScan 會檢查檔案是否為資料識別碼或包含資料識別碼，然後允許或封鎖該作業。

注意

周邊設備存取控管處理行動的優先順序比 DLP 處理行動還高。例如，如果「周邊設備存取控管」不允許移動對應網路磁碟機上的檔案，則即使 DLP 允許，也無法傳輸機密資料。如需有關「周邊設備存取控管」處理行動的詳細資訊，請參閱儲存裝置的權限 第 9-3 頁。

如需 OfficeScan 監控是否有共用檔案存取的應用程式清單，請參閱：

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

網路郵件

Web 電子郵件服務會透過 HTTP 傳輸資料。如果 OfficeScan 偵測到支援的服務對外傳送資料，它會檢查資料中是否包含資料識別碼。

如需支援的 Web-based 電子郵件服務清單，請參閱：

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

網路通道的傳輸範圍和目標

傳輸範圍和目標會定義 OfficeScan 必須監控之網路通道上的資料傳輸。對於應監控的傳輸，OfficeScan 會檢查其中是否有資料識別碼，以決定允許或封鎖該

傳輸。對於不應監控的傳輸，OfficeScan 不會檢查其中是否有資料識別碼，且會立即允許該傳輸。

傳輸範圍：所有傳輸

OfficeScan 會監控主機電腦外部的資料傳輸。

注意

趨勢科技建議您為外部用戶端選擇此範圍。

如果您不想要監控傳輸到主機電腦外部某些目標的資料，請定義下列項目：

- 不受監控的目標：OfficeScan 不會監控傳輸到這些目標的資料。

  注意

  資料傳輸至不受監控的目標及受監控的目標（中毒處理行動是「監控」）與允許傳輸的是類似的。唯一不同之處是 OfficeScan 不會記錄不受監控的目標的傳輸，但一定會記錄受監控目標的傳輸。

- 受監控的目標：這些是不受監控目標之中應監控的特定目標。受監控的目標是：
  - 選用的，如果您已定義不受監控的目標。
  - 不可設定的，如果您沒有定義不受監控的目標。

例如：

下列 IP 位址已指定給貴公司的法律部門：

- 10.201.168.1 到 10.201.168.25

您正在建立策略，用於監控傳送「就業證明」給除了法律部門全職員工以外所有員工的傳輸。如果要這麼做，您可以選取「所有傳輸」作為傳輸範圍，接著：

選項 1：

1. 將 10.201.168.1-10.201.168.25 新增到不受監控的目標。

2. 將法律部門兼職員工的 IP 位址新增到受監控的目標。假設有 3 個 IP 位址 — 10.201.168.21-10.201.168.23。

選項 2：

將法律部門全職員工的 IP 位址新增到非受監控的目標：

- 10.201.168.1-10.201.168.20
- 10.201.168.24-10.201.168.25

如需有關定義受監控與不受監控的目標的指導方針，請參閱定義不受監控和受監控的目標 第 10-33 頁。

傳輸範圍：僅限區域網路外部的傳輸

OfficeScan 會監控傳輸到區域網路 (LAN) 外部任何目標的資料。

注意

趨勢科技建議您為內部用戶端選擇此範圍。

「網路」是指公司或區域網路。這包括目前網路（端點和網路遮罩的 IP 位址）及下列標準私人 IP 位址：

- 類別 A：10.0.0.0 到 10.255.255.255
- 類別 B：172.16.0.0 到 172.31.255.255
- 類別 C：192.168.0.0 到 192.168.255.255

如果您選取此傳輸範圍，則可以定義下列項目：

- 不受監控的目標:定義位於 LAN 外部您認為安全而應監控的目標。

注意

資料傳輸至不受監控的目標及受監控的目標（中毒處理行動是「監控」）與允許傳輸的是類似的。唯一不同之處是 OfficeScan 不會記錄不受監控的目標的傳輸，但一定會記錄受監控目標的傳輸。

- 受監控的目標：定義位於 LAN 內部您想要監控的目標。

如需有關定義受監控與不受監控的目標的指導方針，請參閱定義不受監控和受監控的目標 第 10-33 頁。

解決衝突

如果傳輸範圍、受監控目標以及不受監控目標等設定發生衝突，OfficeScan 會遵循下列優先順序（以最高到最低的順序）：

- 受監控的目標
- 不受監控的目標
- 傳輸範圍

系統和應用程式通道

OfficeScan 可以監控下列系統和應用程式通道：

- 資料錄製器 (CD/DVD)
- 對等式應用程式
- PGP 加密
- 印表機
- 卸除式儲存
- 同步處理軟體 (ActiveSync)
- Windows 剪貼簿

資料錄製器 (CD/DVD)

OfficeScan 會監控錄製到 CD 或 DVD 的資料。如需支援的資料錄製裝置和軟體清單，請參閱：

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

當 OfficeScan 在任何支援裝置或軟體上偵測到發出的「燒錄」命令，且處理行動是「暫不處理」時，資料錄製程序會繼續。如果處理行動是「封鎖」，OfficeScan 會檢查要錄製的檔案是否為資料識別碼或包含資料識別碼。如果 OfficeScan 偵測到至少一個資料識別碼，則不會錄製所有檔案（包含不屬於資料識別碼和未包含資料識別碼的檔案）。OfficeScan 可能也會防止 CD 或 DVD 退出。如果發生此問題，請指示使用者重新啟動軟體處理程序或重設裝置。

OfficeScan 會實作其他 CD/DVD 錄製規則：

- 為了減少誤判的情況，OfficeScan 不會監控下列檔案：

```
.bud      .dll      .gif      .gpd      .htm      .ico      .ini

.jpg      .lnk      .sys      .ttf      .url      .xml
```

- 為提高效能，系統不會監控 Roxio 資料錄製器使用的兩種檔案類型（`*.png` 和 `*.skn`）。
- OfficeScan 不會監控下列目錄中的檔案：

```
*:\autoexec.bat                    *:\Windows

..\Application Data                ..\Cookies

..\Local Settings                  ..\ProgramData

..\Program Files                   ..\Users\*\AppData

..\WINNT
```

- 系統不會監控裝置和軟體建立的 ISO 映像檔。

對等式應用程式

OfficeScan 會監控使用者透過對等式應用程式分享的檔案。

如需支援的對等式應用程式清單，請參閱：

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

PGP 加密

OfficeScan 會監控將由 PGP 加密軟體加密的資料。資料加密之前，OfficeScan 會先檢查。

如需支援的 PGP 加密軟體清單，請參閱：

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

印表機

OfficeScan 會監控各種應用程式起始的印表機作業。

OfficeScan 不會監控尚未儲存的新檔案的印表機作業，因為列印資訊此時只儲存在記憶體中。

如需支援的可起始印表機作業之應用程式清單，請參閱：

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

卸除式儲存

OfficeScan 會監控傳輸到卸除式儲存裝置的資料或在卸除式儲存裝置中傳輸的資料。與資料傳輸有關的活動包括：

- 在裝置中建立檔案
- 將檔案從主機複製到裝置
- 關閉裝置中已修改的檔案
- 修改裝置中的檔案資訊（例如：檔案的副檔名）

當要傳輸的檔案包含資料識別碼時，OfficeScan 會封鎖或允許傳輸。

注意

周邊設備存取控管處理行動的優先順序比 DLP 處理行動還高。例如，如果「周邊設備存取控管」不允許將檔案複製到卸除式儲存裝置，則即使 DLP 允許，仍不會傳輸機密資訊。如需有關「周邊設備存取控管」處理行動的詳細資訊，請參閱儲存裝置的權限 第 9-3 頁。

如需支援的用於資料傳輸活動之卸除式儲存裝置和應用程式清單，請參閱：

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

檔案傳輸至卸除式儲存裝置的處理，是一種直接的過程。例如，在 Microsoft Word 建立檔案的使用者可能想要將檔案儲存至 SD 卡（與使用者儲存的檔案類型無關）。如果檔案包含不應該傳輸的資料識別碼，OfficeScan 會禁止儲存檔案。

對於裝置中的檔案傳輸，OfficeScan 會先將檔案（如果檔案大小未超過 75MB）備份到 `%WINDIR%\system32\dgagent\temp`，然後再進行處理。如果 OfficeScan 允許傳輸檔案，它就會移除備份檔案。如果 OfficeScan 封鎖傳輸，檔案有可能會在這個過程中被刪除。在此情況下，OfficeScan 會將備份檔案複製到包含原始檔案的資料夾。

OfficeScan 允許您定義不受監控的裝置。OfficeScan 永遠允許傳輸資料到這些裝置或在這些裝置內傳輸資料。透過裝置的廠商及選擇性提供的裝置型號和序號 ID 來識別裝置。

秘訣

使用「裝置清單工具」查詢連接至端點的裝置。此工具可以提供每個裝置的裝置廠商、型號和序號 ID。如需詳細資訊，請參閱裝置清單工具 第 9-12 頁。

同步處理軟體 (ActiveSync)

OfficeScan 會監控透過同步處理軟體傳輸到行動裝置的資料。

如需支援的同步處理軟體清單，請參閱：

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

如果資料的來源 IP 位址是 127.0.0.1 而且是透過通訊埠 990 或 5678（用於同步處理的連接埠）傳送，OfficeScan 會檢查資料是否為資料識別碼，然後允許或封鎖其傳輸。

當 OfficeScan 封鎖通訊埠 990 上的檔案傳輸時，行動裝置的目的地資料夾可能仍會建立名稱相同，但是字元格式有誤的檔案。這是因為 OfficeScan 封鎖傳輸之前，檔案的某些部分已經複製到裝置上。

Windows 剪貼簿

OfficeScan 會監控要傳輸到 Windows 剪貼簿的資料，再允許或封鎖傳輸。

OfficeScan 也可以監控主機和 VMWare 或遠端桌面之間的剪貼簿活動。會在含 OfficeScan 用戶端的實體進行監控。例如，VMware 虛擬機器上的 OfficeScan 用戶端會禁止虛擬機器上的剪貼簿資料傳輸到主機。同樣地，含 OfficeScan 用戶端的主機無法將剪貼簿資料複製到透過遠端桌面存取的端點。

Data Loss Prevention 處理行動

當 OfficeScan 偵測到資料識別碼的傳輸時，它會針對偵測到的資料識別碼檢查「DLP 策略」，並執行為該策略設定的處理行動。

下表列出 Data Loss Prevention 處理行動。

表 10-5. Data Loss Prevention 處理行動

處理行動	說明
處理行動	
暫不處理	OfficeScan 允許並記錄傳輸
封鎖	OfficeScan 封鎖並記錄傳輸
其他處理行動	
通知用戶端使用者	OfficeScan 會顯示通知訊息告知傳輸資料的使用者，並告知資料已傳送或已封鎖。

處理行動	說明
記錄資料	無論主要處理行動為何，OfficeScan 都會將機密資訊記錄至<用戶端安裝資料夾>\DLPLite\Forensic。選取此處理行動以評估由 Data Loss Prevention 標示的機密資訊。 已記錄的機密資訊可能會消耗太多的硬碟空間。因此，趨勢科技強烈建議您只針對高度機密資訊選擇此選項。

Data Loss Prevention 例外

DLP 例外會套用至整個策略，包括策略中定義的所有規則。在掃瞄是否有數位資產之前，OfficeScan 會將例外設定套用至所有傳輸。如果某個傳輸符合其中一個例外規則，OfficeScan 會立即允許或掃瞄傳輸，具體取決於例外類型。

定義不受監控和受監控的目標

根據「通道」標籤中設定的傳輸範圍，定義不受監控和受監控的目標。如需有關如何為「所有傳輸」定義不受監控和受監控目標的詳細資料，請參閱 傳輸範圍：所有傳輸 第 10-26 頁。如需有關如何為「僅限區域網路外部的傳輸」定義不受監控和受監控目標的詳細資料，請參閱 傳輸範圍：僅限區域網路外部的傳輸 第 10-27 頁。

請遵循以下指導方針來定義受監控和不受監控的目標：

1. 根據以下項目定義每個目標：
    - IP 位址
    - 主機名稱
    - FQDN
    - 網路位址與子網路遮罩，例如，10.1.1.1/32

注意

對於子網路遮罩，OfficeScan 僅支援無類別網域間路由 (CIDR) 類型的通訊埠。這表示您只能輸入 32 之類的數字，而不能輸入 255.255.255.0。

2. 如果要以特定通道作為目標，請包含這些通道的預設或公司定義的通訊埠號碼。例如，通訊埠 21 通常用於 FTP 傳輸、通訊埠 80 用於 HTTP、通訊埠 443 用於 HTTPS。使用分號分隔目標與通訊埠號碼。
3. 您也可以包含通訊埠範圍。如果要包含所有通訊埠，請忽略通訊埠範圍。

   下面是一些具有通訊埠號碼和通訊埠範圍的目標範例：

   - 10.1.1.1:80
   - host:5-20
   - host.domain.com:20
   - 10.1.1.1/32:20
4. 使用逗點分隔多個目標。

解壓縮規則

可以掃瞄壓縮檔中包含的檔案是否有數位資產。為了確定要掃瞄的檔案，OfficeScan 會使壓縮檔遵循下列規則：

- 解壓縮檔大小超過：__ MB (1-512MB)
- 壓縮層數超過：__ (1-20)
- 要掃瞄的檔案數目超過：__ (1-2000)

規則 1：解壓縮檔大小上限

壓縮檔解壓縮後的大小必須符合指定的限制。

例如：您將限制設定為 20MB。

狀況 1：如果 archive.zip 解壓縮後的大小為 30MB，將不會掃瞄 archive.zip 中包含的任何檔案。也不會繼續檢查其他兩個規則。

狀況 2：如果 my_archive.zip 解壓縮後的大小為 10MB：

- 如果 my_archive.zip 未包含壓縮檔，則 OfficeScan 會略過「規則 2」並繼續進行「規則 3」。
- 如果 my_archive.zip 包含壓縮檔，則所有壓縮檔的大小必須在限制範圍內。例如，如果 my_archive.zip 包含 AAA.rar、BBB.zip 和 EEE.zip，且 EEE.zip 包含 222.zip：

my_archive.zip	= 10MB（解壓縮後）
\AAA.rar	= 25MB（解壓縮後）
\BBB.zip	= 3MB（解壓縮後）
\EEE.zip	= 1MB（解壓縮後）
\222.zip	= 2MB（解壓縮後）

將依據「規則 2」檢查 my_archive.zip、BBB.zip、EEE.zip 和 222.zip，因為這些檔案的合併大小低於 20MB 限制。將略過 AAA.rar。

規則 2：壓縮層數上限

指定層數內的檔案將標示為進行掃瞄。

例如：

my_archive.zip		
\BBB.zip	\CCC.xls	
\DDD.txt		
\EEE.zip	\111.pdf	
	\222.zip	\333.txt

如果您將限制設定為兩層：

- OfficeScan 將忽略 `333.txt`，因為它位於第三層。
- OfficeScan will 將標示下列檔案進行掃瞄，然後檢查「規則 3」：
  - `DDD.txt`（位於第一層）
  - `CCC.xls`（位於第二層）
  - `111.pdf`（位於第二層）

規則 3：要掃瞄的檔案數目上限

OfficeScan 會掃瞄所指定數目上限的檔案。OfficeScan 會依據先數字後字母的順序掃瞄檔案和資料夾。

繼續以「規則 2」的範例為例，OfficeScan 會標示反白顯示的檔案進行掃瞄：

```
my_archive.zip
                    \BBB.zip            \CCC.xls
                    \DDD.txt
                    \EEE.zip            \111.pdf
                                        \222.zip            \333.txt
```

此外，`my_archive.zip` 包含名為 `7Folder` 的資料夾（不會根據「規則 2」進行檢查）。此資料夾包含 `FFF.doc` 和 `GGG.ppt`。這會使要掃瞄的檔案總數為 5 個，反白顯示如下：

```
my_archive.zip
                    \7Folder            \FFF.doc
                    \7Folder            \GGG.ppt
                    \BBB.zip            \CCC.xls
                    \DDD.txt
```

```
                \EEE.zip          \111.pdf

                                  \222.zip          \333.txt
```

如果您將限制設為 4 個檔案，將掃瞄下列檔案：

- FFF.doc
- GGG.ppt
- CCC.xls
- DDD.txt

注意

對於包含內嵌檔案的檔案，OfficeScan 會解壓縮內嵌檔案的內容。

如果解壓縮的內容是文字，則主控檔案（例如 123.doc）和內嵌檔案（例如 abc.txt 和 xyz.xls）會計為一個檔案。

如果解壓縮的內容不是文字，則主控檔案（例如 123.doc）和內嵌檔案（例如 abc.exe）會分開計算。

觸發解壓縮規則的事件

下列事件會觸發解壓縮規則：

- 事件 1：

  要傳輸的壓縮檔符合策略且壓縮檔的毒處理行動為「暫不處理」（傳輸檔案）。

  例如，如果要監控使用者正在傳輸的 .ZIP 檔案，您可以定義檔案屬性 (.ZIP)、將該屬性新增至範本、在策略中使用該範本，然後將處理行動設為「暫不處理」。

  注意

  如果處理行動是「封鎖」，則不會傳輸整個壓縮檔，因此無需掃瞄其所包含的檔案。

- 事件 2：

  要傳輸的壓縮檔不符合策略。

  在此情況下，OfficeScan 仍會使壓縮檔遵循解壓縮規則，以判斷其包含的哪些檔案應掃瞄是否有數位資產，以及是否傳輸整個壓縮檔。

- 結果：

  「事件 1」與「事件 2」具有相同結果。當 OfficeScan 遇到壓縮檔時：

  - 如果未滿足「規則 1」，OfficeScan 會允許傳輸整個壓縮檔。
  - 如果滿足「規則 1」，將繼續檢查其他兩個規則。如果出現下列情況，OfficeScan 將允許傳輸整個壓縮檔：
    - 所有已掃瞄的檔案皆不符合策略。
    - 所有已掃瞄的檔案皆符合策略且處理行動為「暫不處理」。

      如果至少一個已掃瞄的檔案符合策略且處理行動為「封鎖」，則會禁止傳輸整個壓縮檔。

Data Loss Prevention 策略組態設定

設定資料識別碼並將它們分門別類放到各個範本之後，您就可以開始建立 Data Loss Prevention 策略。

除了資料識別碼與範本之外，建立策略的時候，還需要設定通道和處理行動。如需有關策略的詳細資訊，請參閱 Data Loss Prevention 策略 第 10-3 頁。

建立 Data Loss Prevention 策略

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。

2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。

3. 按一下「設定 > DLP 設定」。

4. 按一下「外部用戶端」標籤以設定外部用戶端的策略，或按一下「內部用戶端」標籤以設定內部用戶端的策略。

    注意

   設定用戶端位置設定（如果您尚未這樣做）。用戶端將使用這些設定判定自己的位置，然後套用正確的 Data Loss Prevention 策略。如需詳細資訊，請參閱電腦位置 第 14-2 頁。

5. 選取「啟動 Data Loss Prevention」。

6. 選擇下列其中一個項目：

   - 如果您使用的是「外部用戶端」標籤，則可以透過選取「套用所有設定至內部用戶端」將所有 Data Loss Prevention 設定套用至內部用戶端。
   - 如果您使用的是「內部用戶端」標籤，則可以透過選取「套用所有設定至外部用戶端」將所有 Data Loss Prevention 設定套用至外部用戶端。

7. 在「規則」標籤上，按一下「新增」。

   一個策略最多可包含 40 個規則。

8. 設定規則設定。

   如需有關建立 DLP 規則的詳細資料，請參閱建立 Data Loss Prevention 規則 第 10-40 頁。

9. 按一下「例外」標籤，然後設定任何必要的例外設定。

   如需有關可用例外設定的詳細資料，請參閱Data Loss Prevention 例外 第 10-33 頁。

10. 如果您在用戶端樹狀結構中選取了網域或用戶端，請按一下「儲存設定並套用至用戶端」。如果按下了根網域圖示，則從下列選項進行選擇：

- 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
- 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

建立 Data Loss Prevention 規則

程序

1. 選取啟動這項規則。
2. 指定此規則的名稱。

   設定範本設定：
3. 按一下「範本」標籤。
4. 從「可用的範本」清單中選取範本，然後按一下「新增」。

   選取範本時：

   - 透過按一下範本名稱（這會反白顯示該名稱）來選取多個項目。
   - 如果想要使用特定範本，可以使用搜尋功能。您可以輸入完整或部分的範本名稱。

   注意

   每個規則最多可包含 200 個範本。
5. 如果「可用的範本」清單中沒有您偏好的範本，請執行下列操作：

   a. 按一下「新增範本」。

      「Data Loss Prevention 範本」畫面即會顯示。

      如需有關在「Data Loss Prevention 範本」畫面中新增範本的指示，請參閱 Data Loss Prevention 範本 第 10-17 頁。

b. 建立範本之後，請選取它，然後按一下「新增」。

注意

OfficeScan 檢查範本時會使用第一個符合的規則。這表示如果有檔案或資料符合某個範本的定義，OfficeScan 就不會再檢查其他的範本。優先順序取決於清單中範本的順序。

設定通道設定：

6. 按一下「通道」標籤。
7. 選取規則所用通道。

   如需有關通道的詳細資訊，請參閱網路通道 第 10-21 頁和系統和應用程式通道 第 10-28 頁。

8. 如果您已選取任何一種網路通道，請選取傳輸範圍：
   - 所有傳輸
   - 僅限區域網路外部的傳輸

   如需傳輸範圍、目標如何根據傳輸範圍運作，以及如何正確定義目標的詳細資訊，請參閱網路通道的傳輸範圍和目標 第 10-25 頁。

9. 如果您已選取「電子郵件用戶端」，請執行下列操作：
   a. 按一下「例外」。
   b. 指定受監控和不受監控的內部電子郵件網域。如需有關受監控與不受監控的電子郵件網域的詳細資訊，請參閱電子郵件用戶端 第 10-22 頁。

10. 如果您已選取「卸除式儲存」，請執行下列操作：
    a. 按一下「例外」。
    b. 新增按照廠商識別的不受監控卸除式儲存裝置。裝置型號和序號 ID 是選用的。

       USB 裝置的核可清單支援使用星號 (*) 萬用字元。以星號 (*) 取代任何欄位，以包含符合其他欄位要求的所有裝置。

例如，[vendor]-[model]-* 會將指定廠商和指定型號類型的所有 USB 裝置置於核可清單中，而不論序號 ID 為何。

c. 如果要新增更多裝置，請按一下加號 (+) 圖示。

秘訣

使用「裝置清單工具」查詢連接至端點的裝置。此工具可以提供每個裝置的裝置廠商、型號和序號 ID。如需詳細資訊，請參閱裝置清單工具 第 9-12 頁。

設定處理行動設定：

11. 按一下「處理行動」標籤。
12. 選取主要處理行動和任何其他處理行動。如需有關處理行動的詳細資訊，請參閱 Data Loss Prevention 處理行動 第 10-32 頁。
13. 設定「範本」、「通道」和「處理行動」設定後，按一下「儲存」。

匯入、匯出和複製 DLP 規則

管理員可以匯入之前定義的規則（包含在格式正確的 `.dat` 檔案中），或匯出已設定的 DLP 規則清單。透過複製 DLP 規則，管理員可以修改之前已定義規則的內容，以節省時間。

下表說明每個功能的運作方式。

表 10-6. 匯入、匯出和複製 DLP 規則的功能

功能	說明
匯入	匯入規則清單會將不存在的規則附加到現有的 DLP 規則清單中。OfficeScan 會略過目標清單中已存在的規則。OfficeScan 會為每個規則維護所有預先設定的設定（包括已啟動或已關閉狀態）。

功能	說明
匯出	匯出規則清單會將整個清單匯出為 .dat 檔案，然後管理員可以匯入該檔案並將其部署至其他網域或用戶端。OfficeScan 會根據目前的設定儲存所有規則設定。 注意 • 管理員必須儲存或套用任何新增或修改的規則，然後才可匯出清單。 • OfficeScan 不會匯出為策略設定的任何例外，只會匯出為每個規則設定的設定。
複製	複製規則會建立規則目前設定的準確複本。管理員必須為規則輸入新名稱，並且可以視需要修改新規則的任何設定。

Data Loss Prevention 通知

OfficeScan 具有一組預設的通知訊息，用於向 OfficeScan 管理員和用戶端使用者通知有關數位資產傳輸的情形。

如需有關傳送給管理員的通知的詳細資訊，請參閱管理員的 Data Loss Prevention 通知 第 10-43 頁。

如需有關傳送給用戶端使用者的通知的詳細資訊，請參閱用戶端使用者的 Data Loss Prevention 通知 第 10-46 頁。

管理員的 Data Loss Prevention 通知

您可以設定 OfficeScan，讓它在偵測到數位資產傳輸或封鎖傳輸時通知管理員。

OfficeScan 具有一組預設的通知訊息，可在偵測到數位資產傳輸時通知管理員。您可以視公司需要修改通知和設定其他通知設定。

注意

OfficeScan 可以透過電子郵件、呼叫器、SNMP Trap 和 Windows NT 事件記錄檔來傳送通知。設定 OfficeScan 何時透過這些通道傳送通知的設定。如需詳細資訊，請參閱管理員通知設定 第 13-28 頁。

設定給管理員的 Data Loss Prevention 通知

程序

1. 瀏覽至「通知 > 管理員通知 > 標準通知」。
2. 在「條件」標籤上：
   a. 移至「數位資產傳輸」區段。
   b. 指定要在偵測到數位資產傳輸（可封鎖或允許該動作）時傳送通知，或只在封鎖傳輸時傳送通知。
3. 在「電子郵件」標籤上：
   a. 移至「數位資產傳輸」區段。
   b. 選取「啟動電子郵件通知」。
   c. 選取「傳送通知給具有用戶端樹狀結構網域權限的使用者」。

      您可以使用以角色為基礎的管理將用戶端樹狀結構網域權限授與使用者。如果在屬於特定網域的用戶端上偵測到傳輸，電子郵件將傳送給具網域權限的使用者的電子郵件信箱。如需範例，請參閱下表：

表 10-7. 用戶端樹狀結構網域和權限

用戶端樹狀結構網域	具有網域權限的角色	具有該角色的使用者帳號	使用者帳號的電子郵件信箱
網域 A	Administrator（內建）	root	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
網域 B	Administrator（內建）	root	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

如果屬於網域 A 的 OfficeScan 用戶端偵測到數位資產傳輸，電子郵件會傳送給 mary@xyz.com、john@xyz.com 和 chris@xyz.com。

如果屬於網域 B 的用戶端偵測到傳輸，電子郵件將會傳送給 mary@xyz.com 和 jane@xyz.com。

注意

啟動此選項時，具網域權限的所有使用者都必須有一個對應的電子郵件信箱。電子郵件通知不會傳送給沒有電子郵件信箱的使用者。使用者和電子郵件信箱是從「管理 > 使用者帳號」進行設定的。

d. 選取「傳送通知到下列電子郵件信箱」，然後輸入電子郵件信箱。

e. 接受或修改預設的主旨和訊息。使用 Token 變數代表「主旨」和「訊息」欄位中的資料。

表 10-8. Data Loss Prevention 通知 的 Token 變數

變數	說明
%USER%	偵測到傳輸時已登入電腦的使用者。
%COMPUTER%	偵測到傳輸的電腦
%DOMAIN%	電腦網域

變數	說明
%DATETIME%	偵測到傳輸的日期和時間
%CHANNEL%	偵測到傳輸的通道
%TEMPLATE%	觸發偵測的數位資產範本

4. 在「呼叫器」標籤上：
   a. 移至「數位資產傳輸」區段。
   b. 選取「啟動呼叫器通知」。
   c. 輸入訊息。
5. 在「SNMP Trap」標籤中：
   a. 移至「數位資產傳輸」區段。
   b. 選取「啟動 SNMP Trap 通知」。
   c. 接受或修改預設的訊息。使用 Token 變數代表「訊息」欄位中的資料。如需詳細資訊，請參閱表 10-8: Data Loss Prevention 通知 的 Token 變數 第 10-45 頁。
6. 在「NT 事件記錄檔」標籤中：
   a. 移至「數位資產傳輸」區段。
   b. 選取「啟動 NT 事件記錄檔通知」。
   c. 接受或修改預設的訊息。您可以使用 Token 變數代表「訊息」欄位中的資料。如需詳細資訊，請參閱表 10-8: Data Loss Prevention 通知 的 Token 變數 第 10-45 頁。
7. 按一下「儲存」。

用戶端使用者的 Data Loss Prevention 通知

OfficeScan 可以在允許或封鎖數位資產傳輸之後，立即在用戶端電腦上顯示通知訊息。

如果要在封鎖或允許數位資產傳輸時通知使用者，請在建立 Data Loss Prevention 策略時選取「 通知用戶端使用者 」。如需有關建立策略的指示，請參閱 Data Loss Prevention 策略組態設定 第 10-38 頁。

設定給用戶端的 Data Loss Prevention 通知

程序

1. 瀏覽至「通知 > 用戶端使用者通知」。
2. 按一下「數位資產傳輸」標籤。
3. 接受或修改預設的訊息。
4. 按一下「儲存」。

Data Loss Prevention 記錄檔

用戶端會記錄數位資產傳輸（已封鎖和已允許的傳輸），並立即將記錄檔傳送給伺服器。如果用戶端無法傳送記錄檔，它會在 5 分鐘後重試。

如果要避免記錄檔佔去過多硬碟空間，請手動刪除記錄檔或設定記錄檔刪除預約時程。如需有關管理記錄檔的詳細資訊，請參閱記錄檔管理 第 13-31 頁。

檢視 Data Loss Prevention 記錄檔

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」或「記錄檔 > 用戶端電腦記錄檔 > 安全威脅」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。

3. 按一下「記錄檔 > Data Loss Prevention 記錄檔」或「檢視記錄檔 > DLP 記錄檔」。
4. 指定記錄條件，然後按一下「顯示記錄檔」。
5. 檢視記錄檔。

   記錄檔包含下列資訊：

   表 10-9. Data Loss Prevention 記錄檔資訊

欄	說明
日期/時間	OfficeScan 記錄事件的日期和時間
使用者名稱	登入電腦的使用者名稱
電腦	OfficeScan 偵測到傳輸的電腦名稱
網域	電腦網域
IP	電腦的 IP 位址
規則名稱	觸發事件的規則名稱 注意 使用舊版 OfficeScan 建立的策略會顯示預設名稱 LEGACY_DLP_Policy。
通道	傳輸活動所經由的通道
處理程序	促進傳輸數位資產的程序（程序視通道而有所不同） 如需詳細資訊，請參閱依通道的處理程序 第 10-49 頁。
來源	包含數位資產之檔案的來源，或通道（如果沒有可用的來源）
處理行動	對傳輸採取的處理行動
詳細資訊	連結，其包含有關傳輸的其他詳細資料 如需詳細資訊，請參閱 Data Loss Prevention 記錄檔詳細資料 第 10-51 頁。

6. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請按一下「匯出到 CSV」。開啟檔案或將其儲存至特定位置。

依通道的處理程序

下表列出「 Data Loss Prevention 」記錄檔的「處理程序」欄下顯示的處理程序。

表 10-10. 依通道的處理程序

通道	處理程序
同步處理軟體 (ActiveSync)	同步處理軟體的完整路徑和處理程序名稱 例如： C:\Windows\system32\WUDFHost.exe
資料錄製器 (CD/DVD)	資料錄製器的完整路徑與程序名稱 例如： C:\Windows\Explorer.exe
Windows 剪貼簿	無
電子郵件用戶端 - Lotus Notes	Lotus Notes 的完整路徑與程序名稱 例如： C:\Program Files\IBM\Lotus\Notes\nlnotes.exe
電子郵件用戶端 - Microsoft Outlook	Microsoft Outlook 的完整路徑與程序名稱 例如： C:\Program Files\Microsoft Office\Office12\ OUTLOOK.EXE
電子郵件用戶端 - 所有使用 SMTP 通訊協定的用戶端	電子郵件用戶端的完整路徑與程序名稱 例如： C:\Program Files\Mozilla Thunderbird\thunderbird.exe

通道	處理程序
卸除式儲存	傳輸資料至儲存裝置或在儲存裝置內部傳輸資料的應用程式程序名稱 例如： `explorer.exe`
FTP	FTP 用戶端的完整路徑與程序名稱 例如： `D:\Program Files\FileZilla FTP Client\filezilla.exe`
HTTP	「HTTP 應用程式」
HTTPS	瀏覽器或應用程式的完整路徑與程序名稱 例如： `C:\Program Files\Internet Explorer\iexplore.exe`
IM 應用程式	IM 應用程式的完整路徑與程序名稱 例如： `C:\Program Files\Skype\Phone\Skype.exe`
IM 應用程式 - MSN	• MSN 的完整路徑與程序名稱 例如： `C:\Program Files\Windows Live\Messenger\msnmsgr.exe` • 如果是從聊天視窗傳輸資料，則為「HTTP 應用程式」。
對等式應用程式	對等式應用程式的完整路徑與程序名稱 例如： `D:\Program Files\BitTorrent\bittorrent.exe`
PGP 加密	PGP 加密軟體的完整路徑與程序名稱 例如： `C:\Program Files\PGP Corporation\PGP Desktop\PGPmnApp.exe`

通道	處理程序
印表機	開始印表機作業之應用程式的完整路徑與程序名稱 例如： `C:\Program Files\Microsoft Office\Office12\ WINWORD.EXE`
SMB 通訊協定	從中執行共享檔案存取（複製或建立新檔案）之應用程式的完整路徑與程序名稱 例如： `C:\Windows\Explorer.exe`
網路郵件（HTTP 模式）	「HTTP 應用程式」
網路郵件（HTTPS 模式）	瀏覽器或應用程式的完整路徑與程序名稱 例如： `C:\Program Files\Mozilla Firefox\firefox.exe`

Data Loss Prevention 記錄檔詳細資料

「Data Loss Prevention 記錄檔詳細資料」畫面顯示有關數位資產傳輸的其他詳細資料。傳輸詳細資料因 OfficeScan 偵測到事件所採用的通道和程序而不同。

下表列出顯示的詳細資訊。

表 10-11. 數位資產傳輸詳細資料

詳細資料	說明
日期/時間	OfficeScan 記錄事件的日期和時間
違規 ID	事件的唯一 ID
使用者名稱	登入電腦的使用者名稱
電腦	OfficeScan 偵測到傳輸的電腦名稱
網域	電腦網域

詳細資料	說明
IP	電腦的 IP 位址
通道	傳輸活動所經由的通道
處理程序	促進傳輸數位資產的程序（程序視通道而有所不同） 如需詳細資訊，請參閱依通道的處理程序 第 10-49 頁。
來源	包含數位資產之檔案的來源，或通道（如果沒有可用的來源）
電子郵件寄件者	發起傳輸的電子郵件信箱
電子郵件主旨	包含數位資產之電子郵件的主旨行
電子郵件收件者	電子郵件的目的地電子郵件信箱
URL	網站或網頁的 URL
FTP 使用者	用來登入 FTP 伺服器的使用者名稱
檔案類別	OfficeScan 偵測到包含數位資產之檔案的類型
規則/範本	觸發偵測的確切規則名稱和範本清單 **注意** 每個規則可包含觸發事件的多個範本。多個範本名稱之間以逗號分隔。
處理行動	對傳輸採取的處理行動

資料安全防護偵錯記錄檔

啟動資料安全防護模組的偵錯記錄功能

程序

1. 從支援供應商處取得 `logger.cfg` 檔案。

2. 將下列資料新增至 `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\DlpLite`：
   - 類型：字串
   - 名稱：`debugcfg`
   - 值：`C:\Log\logger.cfg`
3. 在 `C:\ directory` 目錄中建立名為「Log」的資料夾。
4. 將 `logger.cfg` 複製到 “Log” 資料夾。
5. 從 Web 主控台部署「Data Loss Prevention」和「周邊設備存取控管」設定，以開始收集記錄檔。

注意

透過刪除登錄機碼中的 `debugcfg`，然後重新啟動電腦，以關閉資料安全防護模組的偵錯記錄功能。

第 11 章

保護電腦免於受到 Web-based 安全威脅

本章說明各種 Web-based 安全威脅，以及如何使用 OfficeScan 來保護網路和電腦不受 Web-based 安全威脅的侵襲。

本章內容：

關於網路安全威脅

網路安全威脅包含各式各樣源自 Internet 的威脅。網路安全威脅的方法十分巧妙，且結合運用多種檔案和技術，而非只有單一檔案或方式。例如，網路威脅創造者會持續變更所使用的版本或變體。因為網路安全威脅是位於固定的網站位置上而不是在中毒的電腦上，所以網路安全威脅的製造者會持續修改其程式碼以躲避偵測。

近年來，被稱為駭客、病毒撰寫者、垃圾郵件寄件人和間諜程式設計者的個人統稱為網路罪犯。這些網路犯罪者利用網路安全威脅來遂行兩個目的之一。第一個目的是竊取資訊進行販賣。這樣會造成例如個人身分等機密資訊曝光。中毒電腦可能也會成為網路釣魚攻擊或其他資訊竊取活動的媒介。在各種影響中，這種安全威脅可能會傷害網路商業活動的互信基礎，讓大家不能放心地進行 Internet 交易。第二個目的是綁架使用者電腦的 CPU 處理能力，做為從事獲利活動的工具。此處所謂獲利活動包括傳送垃圾郵件，利用分散式拒絕服務勒索受害者，或是利用受害者電腦點擊收費服務網頁。

網頁信譽評等

網頁信譽評等技術會依據諸如網站的存在時間長短、位置變更記錄，以及透過惡意程式行為分析所發現的可疑活動指標等因素來指定信譽評等，以追蹤 Web 網域的可信度。然後它就會繼續掃瞄網站，並阻擋使用者存取中毒的網站。

OfficeScan 用戶端會將查詢傳送至主動式雲端截毒技術伺服器來源，以確定使用者正在嘗試存取之網站的信譽。網站的信譽和電腦上實施的特定網頁信譽評等策略有關。根據使用中的策略而定，OfficeScan 用戶端會封鎖或允許對網站的存取。

注意

如需有關主動式雲端截毒伺服器來源的詳細資訊，請參閱主動式雲端截毒技術來源清單 第 4-21 頁。

將您認為安全或危險的網站新增到核可清單或封鎖清單。OfficeScan 用戶端在偵測到存取任何這些網站時，會自動允許或封鎖存取，且不再傳送查詢至主動式雲端截毒技術伺服器來源。

網頁信譽評等策略

網頁信譽評等策略會指定 OfficeScan 是否要封鎖或允許對網站的存取。

您可以為內部和外部用戶端設定策略。OfficeScan 管理員通常會針對外部用戶端設定較嚴格的策略。

策略是 OfficeScan 用戶端樹狀結構中的詳細設定。您可以對用戶端群組或個別用戶端強制執行特定的策略。您也可以對所有用戶端強制執行單一策略。

部署策略之後，用戶端會使用您在「電腦位置」畫面（請參閱電腦位置 第 14-2 頁）中設定的位置條件來判斷其位置和要套用的策略。用戶端會在每次位置變更時切換策略。

設定網頁信譽評等策略

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中選取目標。
   - 如果要為執行 Windows XP、Vista、7 或 8 的用戶端設定策略，請選取根網域圖示（  ）、特定網域或用戶端。

注意

當您選取根網域或特定網域時，設定只會套用到執行 Windows XP、Vista、7 或 8 的用戶端。設定不會套用到執行 Windows Server 2003、Windows Server 2008 或 Windows Server 2012 的用戶端（即使它們是網域的一部分）。

- 如果要為執行 Windows Server 2003、Windows Server 2008 或 Windows Server 2012 的用戶端設定策略，請選取特定用戶端。

3. 按一下「設定 > 網頁信譽評等設定」。

4. 按一下「外部用戶端」標籤以設定外部用戶端的策略，或按一下「內部用戶端」標籤以設定內部用戶端的策略。

秘訣

設定用戶端位置設定（如果您尚未這樣做）。用戶端將使用這些設定判定自己的位置，然後套用正確的網頁信譽評等策略。如需詳細資訊，請參閱電腦位置 第 14-2 頁。

---

5. 選取「在下列作業系統啟動網頁信譽評等策略」。畫面中列出的作業系統取決於您在步驟 1 中所選取的目標。

秘訣

如果您已經使用含有網頁信譽評等功能的趨勢科技產品（例如：InterScan Web Security Virtual Appliance），趨勢科技建議您關閉內部用戶端的網頁信譽評等。

啟動網頁信譽評等策略時：

- 外部用戶端會將網頁信譽評等查詢傳送至主動式雲端截毒技術。
- 內部用戶端會傳送網頁信譽評等查詢至：
  - 主動式雲端截毒技術伺服器，如果啟動了「傳送查詢至主動式雲端截毒技術伺服器」選項。如需此選項的詳細資訊，請參閱步驟 7。
  - 主動式雲端截毒技術，如果啟動了「傳送查詢至主動式雲端截毒技術伺服器」選項。

6. 選取「啟動評估」。

注意

在評估模式下，用戶端將允許存取全部網站，但會記錄關閉評估時應封鎖的網站存取。趨勢科技提供評估模式，可讓您先評估網站，再依據評估採取適當的處理行動。例如，您可以將自己認為安全的網站新增到核可清單。

7. 選取「檢查 HTTPS URL」。

HTTPS 通訊使用憑證來識別 Web 伺服器。它會將資料加密以防止盜取及竊聽。雖然使用 HTTPS 存取網站的安全性較高，但仍存在風險。即使網站具有有效的憑證，一旦遭到入侵，便會裝載惡意程式並竊取個人資訊。此外，由於憑證相當容易取得，很輕易就能架設使用 HTTPS 的惡意 Web 伺服器。

啟動 HTTPS URL 檢查可減少接觸使用 HTTPS 的惡意網站，進而降低遭到入侵的風險。OfficeScan 可以在以下瀏覽器中監控 HTTPS 流量：

表 11-1. 支援 HTTPS 流量的瀏覽器

瀏覽器	版本
Microsoft Internet Explorer	• 6（含 SP2）或更高版本 • 7.x • 8.x • 9.x • 10.x
Mozilla Firefox	3.5 到 16.0

重要

- HTTPS 掃瞄僅支援以桌面模式運作的 Windows 8 或 Windows 2012 平台。
- 在執行 Internet Explorer 9 或 10 的 OfficeScan 用戶端上首次啟動 HTTPS 掃瞄之後，使用者必須在瀏覽器快顯視窗中啟動 `TmIEPlugInBHO Class` 附加元件，HTTPS 掃瞄才能正常運作。

  如需有關針對網頁信譽評等設定 Internet Explorer 設定的詳細資訊，請參閱下列的常見問題集文章：

  - http://esupport.trendmicro.com/solution/en-us/1060643.aspx
  - http://esupport.trendmicro.com/solution/en-us/1060644.aspx

8. 選取「 只掃瞄通用 HTTP 通訊埠 」以限制通過通訊埠 80、81 和 8080 傳輸的網頁信譽評等掃瞄。依預設，OfficeScan 會掃描所有通過通訊埠的傳輸。

9. 如果希望內部用戶端將網頁信譽評等查詢傳送至主動式雲端截毒技術伺服器，請選取「傳送查詢至主動式雲端截毒技術伺服器」。

   - 如果您啟動此選項：
     - 用戶端會參考主動式雲端截毒技術伺服器來源清單，判斷應該將查詢傳送至哪些主動式雲端截毒技術伺服器。如需有關主動式雲端截毒技術來源的詳細資訊，請參閱 主動式雲端截毒技術來源清單 第 4-21 頁。
     - 請確定主動式雲端截毒技術伺服器呈運行狀態。如果主動式雲端截毒技術伺服器全都無法使用，用戶端不會將查詢傳送至主動式雲端截毒技術。其餘的用戶端網頁信譽評等資料來源為核可和封鎖的 URL 清單 (在步驟 10 中設定)。
     - 如果您希望用戶端透過 Proxy 伺服器來連結主動式雲端截毒技術伺服器，請在「管理 > Proxy 伺服器設定」>「內部代理伺服器」標籤中指定 Proxy 伺服器設定。
     - 請確定定期更新主動式雲端截毒技術伺服器，以確保防護保持在最新狀態。
     - 用戶端將不會封鎖未測試網站。主動式雲端截毒技術伺服器不會儲存這些網站的網頁信譽評等。

- 如果您關閉此選項：
  - 用戶端會將網頁信譽評等查詢傳送至主動式雲端截毒技術。用戶端電腦必須連接 Internet 才能成功傳送查詢。
  - 如果與主動式雲端截毒技術的連線需要 Proxy 伺服器驗證，請指定驗證憑證，方法是前往「管理 > Proxy 伺服器設定」>「外部 Proxy 伺服器 (標籤) > 與趨勢科技伺服器的用戶端連線」。
  - 如果您在步驟 9 中選擇了「封鎖尚未經由趨勢科技測試的網頁」，用戶端會封鎖未測試網站。

10. 選取可用的網頁信譽評等安全層級：「高」、「中」或「低」

注意

安全層級決定 OfficeScan 會允許或封鎖對 URL 的存取。例如，如果您將安全層級設定為「低」，OfficeScan 只會封鎖已知為網路安全威脅的 URL。設定較高的安全層級可提高網路安全威脅偵測率，但誤判的可能性也會提高。

---

11. 如果您關閉步驟 7 中的傳送查詢至主動式雲端截毒技術伺服器選項，您可以選擇「封鎖尚未經由趨勢科技測試的網頁」。

注意

雖然趨勢科技會主動測試網頁以確保安全，但使用者仍可能會在造訪新的或較不熱門的網站時遇到未測試的網頁。封鎖對於未測試網頁的存取，可以提高安全，但也會讓人無法存取某些安全的網頁。

---

12. 設定核可和封鎖的清單。

注意

核可清單優先於封鎖的清單。當 URL 與核可清單中的項目相符時，用戶端一律允許存取 URL，即使該 URL 位於封鎖的清單中。

---

a. 選取「啟動核可/封鎖清單」。

b. 輸入 URL。

   您可在 URL 中的任何位置加入萬用字元 (*)。

例如：

- 輸入 `www.trendmicro.com/*` 表示將核可趨勢科技網站中的所有網頁。
- 輸入 `*.trendmicro.com/*` 表示將核可 trendmicro.com 的任何子網域中的所有網頁。

您可以輸入包含 IP 位址的 URL。如果 URL 包含 IPv6 位址，請使用括號將位址括起來。

c. 按一下「新增到核可清單」或「新增到封鎖清單」。

d. 如果要將清單匯出為 `.dat` 檔案，請按一下「匯出」，再按一下「儲存」。

e. 如果您已從其他伺服器匯出清單，而想要將此清單匯入此畫面，請按一下「匯入」，然後尋找 `.dat` 檔案。此清單會載入至畫面上。

13. 如果要送出網頁信譽評等的意見反應，請按一下「重新評估 URL」下提供的 URL。系統會在瀏覽器視窗中開啟趨勢科技網頁信譽評等查詢系統。

14. 選取是否允許 OfficeScan 用戶端將網頁信譽評等記錄檔傳送給伺服器。如果您想分析 OfficeScan 封鎖的 URL，並且針對您認為可以安全存取的 URL 採取合適的處理行動，請允許用戶端傳送記錄檔。

15. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

- 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
- 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

用於網頁信譽評等的 Proxy

如果您已經設定 Proxy 伺服器來處理組織中的 HTTP 通訊，而且必須經過驗證才能存取 Web，請指定 Proxy 伺服器驗證憑證。當 OfficeScan 連線到主動式雲

端截毒伺服器來源以判斷使用者嘗試存取的網站是否安全時，會使用這些憑證。

本 OfficeScan 版本只支援一組驗證憑證。

如需設定 Proxy 伺服器設定的相關指示，請參閱 OfficeScan 用戶端的外部 Proxy 伺服器 第 14-43 頁。

用戶端使用者的網路安全威脅通知

OfficeScan 封鎖違反網頁信譽評等策略的 URL 之後，會立即在 OfficeScan 用戶端電腦顯示通知訊息。您可以啟動通知訊息，並視需要修改通知訊息的內容。

啟動網路安全威脅通知訊息

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 權限和其他設定」。
4. 按一下「其他設定」標籤，然後移至「網頁信譽評等設定」區段。
5. 選取「當網站被封鎖時顯示通知」。
6. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。

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

修改網路安全威脅通知訊息

程序

1. 瀏覽至「通知 > 用戶端使用者通知」。
2. 按一下「網頁信譽評等違規」標籤。
3. 在提供的文字方塊中修改預設訊息。
4. 按一下「儲存」。

網頁信譽評等記錄檔

設定內部和外部用戶端同時傳送網頁信譽評等記錄檔到伺服器。如果您要分析 OfficeScan 所封鎖的 URL，並對您認為可安全存取的 URL 採取適當的處理行動，便可以這麼做。

如果要避免記錄檔佔去過多硬碟空間，請手動刪除記錄檔或設定記錄檔刪除預約時程。如需有關管理記錄檔的詳細資訊，請參閱記錄檔管理 第 13-31 頁。

檢視網頁信譽評等記錄檔

程序

1. 瀏覽至「記錄檔 > 用戶端電腦記錄檔 > 安全威脅」或「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示（  ）以包含所有的用戶端，或選取特定網域或用戶端。

3. 按一下「檢視記錄檔 > 網頁信譽評等記錄檔」或「記錄檔 > 網頁信譽評等記錄檔」。
4. 指定記錄條件，然後按一下「顯示記錄檔」。
5. 檢視記錄檔。記錄檔包含下列資訊：
   - OfficeScan 封鎖 URL 的日期/時間
   - 使用者用於存取 URL 的電腦
   - 使用者用於存取 URL 的電腦網域
   - 已封鎖的 URL
   - URL 的風險等級
   - 導向至「趨勢科技網頁信譽評等查詢系統」的連結，其中會提供所封鎖之 URL 的詳細資訊
6. 如果有不應封鎖的 URL，請按一下「新增到核可清單」按鈕，將該網站新增到核可/封鎖的 URL 清單。
7. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請按一下「匯出到 CSV」。開啟檔案或將其儲存至特定位置。

第 12 章

使用 OfficeScan 防火牆

本章說明 OfficeScan 防火牆功能和組態設定。

本章內容：

關於 OfficeScan 防火牆

OfficeScan 防火牆使用狀態檢測和高效能網路病毒掃瞄，來保護網路上的用戶端和伺服器。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。

注意

您可以在 Windows XP 電腦（已啟動 Windows 防火牆）上啟動、設定和使用 OfficeScan 防火牆。不過，必須謹慎管理您的策略，以避免建立相衝突的防火牆策略，而產生無法預期的結果。如需有關「Windows 防火牆」的詳細資訊，請參閱 Microsoft 文件。

OfficeScan 防火牆包含下列主要功能和優點：

傳輸過濾

OfficeScan 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
- 來源和目標電腦

應用程式過濾

OfficeScan 防火牆會在允許特定應用程式存取網路的同時過濾這些應用程式的入站和出站流量。但是，網路連線要視管理員設定的策略而定。

注意

OfficeScan 不支援 Windows 8 和 Windows Server 2012 平台上的特定應用程式例外。OfficeScan 會允許或拒絕具有這些平台之電腦上的所有應用程式流量。

認證安全防護軟體清單

「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。如果安全層級設定為「中」或「高」，OfficeScan 仍會允許應用程式執行和存取網路。

針對提供更多完整清單的全域「認證安全防護軟體清單」啟動查詢。這是一份由趨勢科技動態更新的清單。

注意

這項功能可配合行為監控使用。請務必在啟動全域的「認證安全防護軟體清單」之前，先啟動「未經授權的變更阻止服務」和「認證安全防護軟體服務」。

掃瞄網路病毒

OfficeScan 防火牆也會檢查每個封包是否有網路病毒。如需詳細資訊，請參閱網路病毒 第 7-3 頁。

可自訂的資料檔和策略

OfficeScan 防火牆可讓您將策略設為封鎖或允許指定的網路傳輸類型。您可以指派策略到一或多個資料檔，然後將資料檔部署到指定的 OfficeScan 用戶端。這是一種組織和設定用戶端防火牆設定的高度自訂方法。

狀態檢測

OfficeScan 防火牆是一種狀態檢測防火牆，會監控所有與 OfficeScan 用戶端間的連線，且會記憶所有連線狀態。它可識別任何連線的特定狀況、預測應該採用的處理行動，並偵測一般連線的中斷情況。因此，有效地使用防火牆不僅需要建立資料檔和策略，還需要分析連線和過濾通過防火牆的封包。

入侵偵測系統

OfficeScan 防火牆也包括「入侵偵測系統」(IDS)。IDS 系統啟動後，可以協助識別出網路封包中可能指出 OfficeScan 用戶端遭到攻擊的病毒碼。OfficeScan 防火牆有助於防止下列知名的入侵行為：

- Too Big Fragment：一種「拒絕服務」攻擊，其中駭客會將過大的 TCP/UDP 封包導向目標電腦。這會造成電腦的緩衝器溢位而凍結或重新啟動電腦。
- Ping of Death：一種「拒絕服務」攻擊，駭客會將過大的 ICMP/ICMPv6 封包導向目標電腦。這會造成電腦的緩衝器溢位而凍結或重新啟動電腦。
- Conflicted ARP：一種攻擊類型，其中駭客會傳送具有相同來源和目標 IP 位址的「位址解析通訊協定」(ARP) 要求給電腦。目標電腦持續將 ARP 回應（其 MAC 位址）傳送給自己，使其凍結或當機。
- SYN Flood： 一種「拒絕服務」攻擊，其中程式會將多個 TCP 同步化 (SYN) 封包傳送到電腦，造成電腦持續傳送同步化確認 (SYN/ACK) 回應。這會耗盡電腦記憶體且最終使電腦當機。
- Overlapping Fragment：類似於 Teardrop 攻擊，這種「拒絕服務」攻擊會將重疊的 TCP 片段傳送到電腦。這會覆寫第一個 TCP 片段中的標題資訊，

且有可能通過防火牆。防火牆可能接著會允許具有惡意程式碼的後續片段通過而到達目標電腦。

- Teardrop：類似於重疊片段攻擊，這種「拒絕服務」攻擊與 IP 片段有關。位於第二或其後 IP 片段的混淆偏移值可能會造成接收端電腦作業系統在嘗試重組片段時當機。
- Tiny Fragment Attack：一種攻擊類型，其中小型 TCP 片段會迫使第一項 TCP 封包標題資訊到下一個片段中。這會造成過濾傳輸的路由器忽略後續片段，而這些片段可能包含惡意資料。
- Fragmented IGMP：一種「拒絕服務」攻擊，會將片段式 IGMP 封包傳送到目標電腦，而此電腦無法正確處理 IGMP 封包。這可能會使電腦凍結或速度減慢。
- LAND Attack：一種攻擊類型，會將具有相同來源和目標位址的 IP 同步化 (SYN) 封包傳送給電腦，使電腦將同步化確認 (SYN/ACK) 回應傳送給自己。這可能會使電腦凍結或速度減慢。

防火牆違規疫情爆發監控

當防火牆違規事件超過特定門檻值時，OfficeScan 防火牆會傳送自訂通知訊息給指定收件者，發出攻擊通知。

OfficeScan 用戶端防火牆權限

授與 OfficeScan 用戶端使用者在 OfficeScan 用戶端主控台上檢視其防火牆設定的權限。也可以授與使用者啟動或關閉防火牆、入侵偵測系統和防火牆違規通知訊息的權限。

啟動或關閉 OfficeScan 防火牆

在安裝 OfficeScan 伺服器期間，系統會提示您啟動或關閉 OfficeScan 防火牆。

如果已在安裝期間啟動防火牆，並發現效能受到影響（特別是在 Windows Server 2003、Windows Server 2008 和 Windows Server 2012 等伺服器平台上），請考慮關閉防火牆。

如果已在安裝期間關閉防火牆，但現在想要啟動防火牆以保護用戶端免於遭受入侵，請先閱讀 OfficeScan 用戶端服務 第 14-6 頁中的指導方針和指示。

您可以在所有用戶端電腦或選取的 OfficeScan 用戶端電腦上啟動或關閉防火牆。

啟動或關閉所選電腦上的 OfficeScan 防火牆

方法 A：建立新策略並將它套用到 OfficeScan 用戶端。

程序

1. 建立可啟動/關閉防火牆的新策略。如需建立新策略的步驟，請參閱新增或修改防火牆策略 第 12-10 頁。
2. 將該策略套用到 OfficeScan 用戶端。

方法 B：啟動/關閉防火牆驅動程式和服務。

程序

1. 啟動/關閉防火牆驅動程式。
   a. 開啟「Windows 網路連線內容」。
   b. 選取或清除網路卡的「趨勢科技一般防火牆驅動程式」核取方塊。
2. 啟動/關閉防火牆服務。
   a. 開啟命令提示字元並輸入 `services.msc`。

b. 從 Microsoft 管理主控台 (MMC) 啟動或停止「OfficeScan NT 防火牆」。

方法 C：從 Web 主控台啟動/關閉防火牆服務

如需詳細步驟，請參閱 OfficeScan 用戶端服務 第 14-6 頁。

啟動或關閉所有電腦上的 OfficeScan 防火牆

程序

1. 瀏覽至「管理 > 產品使用授權」。
2. 移至「其他服務」區段。
3. 在「 其他服務 」區段中的「用戶端電腦防火牆」列旁，按一下「 啟動 」或「 關閉 」。

防火牆策略和資料檔

OfficeScan 防火牆使用策略和資料檔來組織和自訂防護用戶端電腦的方法。

透過 Active Directory 整合和以角色為基礎的管理，每個使用者角色（視其權限而定）都可以建立、設定或刪除特定網域的策略和資料檔。

秘訣

在同一電腦上安裝多個防火牆可能會產生無法預期的結果。請考慮在部署和啟動 OfficeScan 防火牆之前，先解除安裝 OfficeScan 用戶端上的其他軟體型防火牆應用程式。

下列為成功使用 OfficeScan 防火牆的必要步驟：

1. 建立策略。策略可讓您選取安全層級以封鎖或允許在用戶端電腦之間的傳輸，以及啟動防火牆功能。

2. 新增例外至策略。例外可讓 OfficeScan 用戶端脫離策略的限制。有了例外規則，您便可指定用戶端並允許或封鎖某些傳輸類型，而不受策略中安全層級設定的限制。例如，可以針對策略中的一組用戶端封鎖其所有流量，但建立允許 HTTP 流量的例外，如此用戶端便可存取 Web 伺服器。

3. 建立和指定資料檔給 OfficeScan 用戶端。防火牆資料檔包含一組用戶端屬性並與策略關聯。當用戶端符合資料檔中指定的屬性時，就會觸發相關聯的策略。

防火牆策略

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。策略也會定義要啟動或關閉的防火牆功能。將策略指定給一或多個防火牆資料檔。

OfficeScan 隨附一組預設策略，您可以視需要進行修改或刪除。

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。

下表會列出預設防火牆策略。

表 12-1. 預設防火牆策略

策略名稱	安全層級	用戶端設定	例外	建議用法
全部存取	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
Cisco Trust Agent for Cisco NAC	低	啟動防火牆	允許通過通訊埠 21862 的輸入和輸出 UDP 傳輸	用於當用戶端有安裝 Cisco Trust Agent (CTA) 時
Trend Micro Control Manager 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 代理程式時

策略名稱	安全層級	用戶端設定	例外	建議用法
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

如果預設的策略不敷使用，您也可以自行建立新策略。

所有預設防火牆策略和使用者建立的防火牆策略都會顯示在 Web 主控台的防火牆策略清單中。

設定防火牆策略清單

程序

1. 瀏覽至「用戶端電腦 > 防火牆 > 策略」。
2. 如果要新增策略，請按一下「新增」。

   如果您要建立的新策略與現有策略具有類似的設定，請選取現有的策略，並按一下「複製」。如果要編輯現有策略，請按一下策略名稱，

   會出現策略組態設定畫面。如需詳細資訊，請參閱新增或修改防火牆策略 第 12-10 頁。
3. 如果要刪除現有策略，請選取策略旁邊的核取方塊，然後按一下「刪除」。
4. 如果要編輯防火牆例外範本，請按一下「編輯例外範本」。

   如需詳細資訊，請參閱編輯防火牆例外範本 第 12-12 頁。

   則會出現「例外範本編輯器」。

新增或修改防火牆策略

為每個策略設定下列項目：

- 安全層級：封鎖或允許 OfficeScan 用戶端電腦上所有輸入和（或）輸出的一般設定
- 防火牆功能：指定要啟動或關閉 OfficeScan 防火牆、入侵偵測系統 (IDS) 和防火牆違規通知訊息。如需有關 IDS 的詳細資訊，請參閱入侵偵測系統 第 12-4 頁。
- 認證安全防護軟體清單：指定是否允許認證安全的應用程式連線到網路。如需有關認證安全防護軟體清單的詳細資訊，請參閱認證安全防護軟體清單 第 12-3 頁。
- 策略例外清單：封鎖或允許不同網路傳輸類型的可設定例外清單

新增防火牆策略

程序

1. 瀏覽至「用戶端電腦 > 防火牆 > 策略」。
2. 如果要新增策略，請按一下「新增」。

   如果您要建立的新策略與現有策略具有類似的設定，請選取現有的策略，並按一下「複製」。
3. 輸入策略名稱。
4. 選取安全層級。

   選定的安全層級不套用於例外清單中的通訊埠。
5. 選取要用於策略的防火牆功能。
   - 當防火牆封鎖輸出封包時，會顯示防火牆違規通知訊息。如果要修改該訊息，請參閱修改防火牆通知訊息的內容 第 12-26 頁。
   - 啟動所有防火牆功能會授與 OfficeScan 用戶端使用者在 OfficeScan 用戶端主控台中啟動/關閉功能及修改防火牆設定的權限。

警告!

您無法使用 OfficeScan 伺服器 Web 主控台覆寫使用者所設定的 OfficeScan 用戶端主控台設定。

- 如果您並未啟動功能，則從 OfficeScan 伺服器 Web 主控台設定的防火牆設定會顯示在 OfficeScan 用戶端主控台的「網路卡清單」下。
- OfficeScan 用戶端主控台「防火牆」標籤上「設定」下的資訊一律會反映從 OfficeScan 用戶端主控台（而不是伺服器 Web 主控台）所設定的設定。

6. 啟動本機或全域的「認證安全防護軟體清單」。

注意

請務必在啟動此服務之前，先啟動「未經授權的變更阻止服務」和「認證安全防護軟體服務」。

7. 從「例外」下選取防火牆策略例外。此處所含的策略例外是以防火牆例外範本為基礎。如需詳細資訊，請參閱編輯防火牆例外範本 第 12-12 頁。

- 可以按一下策略例外名稱，然後在開啟的頁面中變更其設定，以修改現有策略例外。

注意

已修改的策略例外只會套用到要建立的策略。如果您希望策略例外修改永久有效，就必須對防火牆例外範本中的策略例外進行相同的修改。

- 按一下「新增」以建立新策略例外。在開啟的頁面中指定其設定。

注意

策略例外只會套用到要建立的策略。如果要套用此策略例外到其他策略，您就必須先將其新增到防火牆例外範本中的策略例外清單內。

8. 按一下「儲存」。

修改現有的防火牆策略

程序

1. 瀏覽至「用戶端電腦 > 防火牆 > 策略」。
2. 按一下某個策略。
3. 修改下列項目：
   - 策略名稱
   - 安全層級
   - 要用於策略的防火牆功能
   - 認證安全防護軟體服務清單狀態
   - 要加入策略中的防火牆策略例外
     - 編輯現有策略例外（按一下策略例外名稱，並在開啟的頁面中變更設定）
     - 按一下「新增」以建立新策略例外。在開啟的頁面中指定其設定。
4. 按一下「儲存」將修改套用到現有策略。

編輯防火牆例外範本

防火牆例外範本包含策略例外，您可以設定這些例外，以根據 OfficeScan 用戶端電腦的通訊埠號碼和 IP 位址來允許或封鎖各種網路傳輸。建立策略例外之後，請編輯要套用策略例外的策略。

決定您要使用哪一類型的策略例外。策略例外分為下列兩種類型：

- 限制的

  只會封鎖特定類型的網路傳輸，並套用至允許所有網路傳輸的策略。限制策略例外的用途範例為封鎖容易受到攻擊的 OfficeScan 用戶端通訊埠（例如：特洛伊木馬程式經常使用的通訊埠）。

- 允許的

  只會允許特定類型的網路傳輸，並套用至封鎖所有網路傳輸的策略。例如，您可能只想允許 OfficeScan 用戶端存取 OfficeScan 伺服器和 Web 伺服器。如果要這樣做，請允許信任的通訊埠（用於與 OfficeScan 伺服器通訊的通訊埠）和 OfficeScan 用戶端於 HTTP 通訊所用通訊埠的傳輸。

  OfficeScan 用戶端監聽通訊埠：「用戶端電腦 > 用戶端管理 > 狀態」。通訊埠號碼會列在「基本資訊」下。

  伺服器監聽通訊埠：管理 > 連線設定。通訊埠號碼會列在「用戶端電腦的連線設定」下。

  OfficeScan 隨附一組預設防火牆策略例外，您可以視需要進行修改或刪除。

表 12-2. 預設防火牆策略例外規則

例外名稱	處理行動	通訊協定	通訊埠	方向
DNS	允許	TCP/UDP	53	輸入和輸出
NetBIOS	允許	TCP/UDP	137, 138, 139, 445	輸入和輸出
HTTPS	允許	TCP	443	輸入和輸出
HTTP	允許	TCP	80	輸入和輸出
Telnet	允許	TCP	23	輸入和輸出
SMTP	允許	TCP	25	輸入和輸出
FTP	允許	TCP	21	輸入和輸出
POP3	允許	TCP	110	輸入和輸出
LDAP	允許	TCP/UDP	389	輸入和輸出

注意

預設例外會套用至所有用戶端。如果要讓預設例外只套用到特定用戶端，請編輯該例外，並指定用戶端的 IP 位址。

如果您是從舊版 OfficeScan 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

程序

1. 瀏覽至「用戶端電腦 > 防火牆 > 策略」。
2. 按一下「編輯例外範本」。
3. 按一下「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 OfficeScan 將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（ OfficeScan 用戶端電腦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 OfficeScan 用戶端電腦上的哪些通訊埠執行處理行動。
9. 選取要加入例外的 OfficeScan 用戶端電腦 IP 位址。例如，如果您選擇拒絕所有網路流量（輸入和輸出）並輸入網路上某部電腦的 IP 位址，則策略中具有此項例外的 OfficeScan 用戶端將無法傳送資料到此 IP 位址或接收來自此 IP 位址的資料。

   - 所有 IP 位址：包含所有 IP 位址

- 單一 IP 位址：輸入 IPv4 或 IPv6 位址，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. 按一下「儲存」。

修改防火牆策略例外

程序

1. 瀏覽至「用戶端電腦 > 防火牆 > 策略」。
2. 按一下「編輯例外範本」。
3. 按一下某個策略例外。
4. 修改下列項目：
   - 策略例外名稱
   - 應用程式類型、名稱或路徑
   - OfficeScan 要對網路傳輸執行的處理行動和傳輸方向
   - 網路通訊協定類型
   - 策略例外的通訊埠號碼
   - OfficeScan 用戶端電腦 IP 位址
5. 按一下「儲存」。

儲存策略例外清單設定

程序

1. 瀏覽至「用戶端電腦 > 防火牆 > 策略」。

2. 按一下「編輯例外範本」。
3. 按一下下列其中一個儲存選項：
    - 儲存範本變更：儲存例外範本及目前的策略例外和設定。此選項只會將範本套用到日後建立的策略，不會套用到現有策略。
    - 儲存並且套用到現有策略：儲存例外範本及目前的策略例外和設定。此選項會將範本套用到現有和日後建立的策略。

防火牆資料檔

防火牆資料檔提供彈性，方法是讓您選擇用戶端或用戶端群組在套用策略之前所必須要有的屬性。建立可以建立、設定或刪除特定網域資料檔的使用者角色。

使用內建的管理員帳號或擁有完整管理權限的使用者還可以啟動「覆寫用戶端安全層級例外清單」選項，以伺服器設定取代 OfficeScan 用戶端資料檔設定。

資料檔包含下列項目：

- 關聯策略：每個資料檔使用單一的策略
- 用戶端屬性：擁有下列一個或多個屬性的 OfficeScan 用戶端會套用關聯的策略：
    - IP 位址：擁有特定 IP 位址、在某個 IP 位址範圍內的 IP 位址，或是屬於指定之子網路的 IP 位址的 OfficeScan 用戶端
    - 網域：屬於某個 OfficeScan 網域的 OfficeScan 用戶端
    - 電腦：具有特定電腦名稱的 OfficeScan 用戶端
    - 平台：執行特定平台的 OfficeScan 用戶端
    - 登入名稱：指定的使用者登入的 OfficeScan 用戶端電腦
    - NIC 說明：具有相符 NIC 說明的 OfficeScan 用戶端電腦
    - 用戶端連線狀態：OfficeScan 用戶端為線上或離線

注意

如果 OfficeScan 用戶端可連線到 OfficeScan 伺服器或任何一部參考伺服器，則該用戶端為「線上」；如果用戶端無法連線到任何伺服器，則該用戶端為「離線」。

- 使用者權限：允許或防止 OfficeScan 用戶端使用者執行下列動作：
  - 變更策略中指定的安全層級
  - 編輯與策略相關聯的例外清單

注意

這些權限只會套用到符合資料檔中指定之屬性的用戶端。您可以將其他防火牆權限指定給選取的用戶端使用者。如需詳細資訊，請參閱防火牆權限 第 12-21 頁。

OfficeScan 隨附名為「所有用戶端資料檔」的預設資料檔，此資料檔使用「所有存取」策略。您可以修改或刪除此預設資料檔。您也可以建立新的資料檔。所有預設防火牆資料檔和使用者建立的防火牆資料檔（包括與每個資料檔關聯的策略和目前的資料檔狀態）都會顯示在 Web 主控台的防火牆資料檔清單中。管理資料檔清單並部署所有資料檔到 OfficeScan 用戶端。OfficeScan 用戶端會將所有防火牆資料檔儲存到用戶端電腦。

設定防火牆資料檔清單

程序

1. 瀏覽至「用戶端電腦 > 防火牆 > 資料檔」。
2. 若是使用內建的管理員帳號或擁有完整管理權限的使用者，可以視需要啟動「覆寫用戶端安全層級例外清單」選項，以伺服器設定取代 OfficeScan 用戶端資料檔設定。
3. 如果要新增資料檔，請按一下「新增」。如果要編輯現有資料檔，請選取資料檔名稱。

   隨即出現資料檔組態設定畫面。詳細資訊請參閱 新增並編輯防火牆資料檔 第 12-19 頁。

4. 如果要刪除現有策略，請選取策略旁邊的核取方塊，然後按一下「刪除」。

5. 如果要變更資料檔在清單中的順序，請選取要移動的資料檔旁的核取方塊，然後按一下「上移」或「下移」。

   OfficeScan 會以防火牆資料檔出現在資料檔清單中的順序將它們依序套用到 OfficeScan 用戶端。例如，如果用戶端符合第一個資料檔，OfficeScan 便會將針對這個資料檔設定的行動套用到該用戶端，OfficeScan 會忽略針對該用戶端設定的其他資料檔。

   秘訣

   策略的專屬性越高，其理想位置就應在清單中越靠頂端。例如，將您針對單一用戶端建立的策略移至頂端，接著依次是針對某範圍用戶端、網路網域和所有用戶端建立的策略。

6. 如果要管理參考伺服器，請按一下「編輯參考伺服器清單」。參考伺服器是套用防火牆資料檔時，用來替代 OfficeScan 伺服器的電腦。參考伺服器可以是網路上的任何電腦（詳細資訊請參閱 參考伺服器 第 13-26 頁）。OfficeScan 會在您啟動參考伺服器時進行下列假設：

   - 即使 OfficeScan 用戶端無法與 OfficeScan 伺服器通訊，連線至參考伺服器的 OfficeScan 用戶端仍為連線狀態。
   - 套用至線上 OfficeScan 用戶端的防火牆資料檔也會套用至連線到參考伺服器的 OfficeScan 用戶端。

   注意

   只有使用內建的管理員帳號或擁有完整管理權限的使用者能查看和設定參考伺服器清單。

7. 如果要儲存目前的設定並指定資料檔給 OfficeScan 用戶端：

   a. 選取是否要「覆寫用戶端安全層級/例外清單」。此選項會覆寫使用者設定的所有防火牆設定。

   b. 按一下「指定資料檔給用戶端」。OfficeScan 會將資料檔清單中的所有資料檔指定給所有 OfficeScan 用戶端。

8. 如果要確認是否成功指定資料檔給 OfficeScan 用戶端：

a. 移至 用戶端電腦 > 用戶端管理。在用戶端樹狀結構檢視下拉式方塊中，選取「防火牆檢視」。

b. 確認用戶端樹狀結構中的「防火牆」欄位下方有綠色的核取記號。如果與資料檔相關的策略啟動了「入侵偵測系統」，「IDS」欄位下方也會有綠色的核取記號。

c. 驗證用戶端是否已套用正確的防火牆策略。用戶端樹狀結構的「防火牆策略」欄位下方會顯示策略。

新增並編輯防火牆資料檔

OfficeScan 用戶端電腦可能需要不同層級的防護。防火牆資料檔可讓您指定要套用相關策略到哪些用戶端電腦，並授與用戶端使用者修改防火牆設定的權限。一般而言，每個使用中的策略都需要一個資料檔。

新增防火牆資料檔

程序

1. 瀏覽至「用戶端電腦 > 防火牆 > 資料檔」。
2. 按一下「新增」。
3. 按一下「啟動這個資料檔」允許 OfficeScan 將資料檔部署到 OfficeScan 用戶端。
4. 請輸入一個用於識別資料檔的名稱和說明（選用）。
5. 選取此資料檔的策略。
6. 指定 OfficeScan 要套用策略的用戶端電腦。根據下列條件選取電腦：
   - IP 位址
   - 網域：按一下按鈕開啟用戶端樹狀結構，然後從中選取網域。

注意

只有擁有完整網域權限的使用者能夠選取網域。

- 電腦名稱：按一下按鈕開啟用戶端樹狀結構，然後從中選取 OfficeScan 用戶端電腦。
- 平台
- 登入名稱
- NIC 說明：輸入不含萬用字元的完整或部分說明。

秘訣

趨勢科技建議您輸入 NIC 製造商，因為 NIC 說明的開頭通常是製造商的名稱。例如：如果輸入 "Intel"，則 Intel 製造的所有 NIC 都將符合條件。如果輸入特定 NIC 型號，例如："Intel(R) Pro/100"，則 NIC 說明中開頭為 "Intel(R) Pro/100" 的 NIC 才符合條件。

- 用戶端狀態

7. 選取是否要授與使用者權限變更防火牆安全層級，或編輯可設定的例外清單以允許指定的傳輸類型。

   如需有關這些選項的詳細資訊，請參閱新增或修改防火牆策略 第 12-10 頁。

8. 按一下「儲存」。

修改防火牆資料檔

程序

1. 瀏覽至「用戶端電腦 > 防火牆 > 資料檔」。
2. 按一下某個資料檔。
3. 按一下「啟動這個資料檔」允許 OfficeScan 將此資料檔部署到 OfficeScan 用戶端。修改下列項目：

- 資料檔名稱和說明
- 指定給資料檔的策略
- OfficeScan 用戶端電腦，根據下列條件：
  - IP 位址
  - 網域：按一下按鈕開啟用戶端樹狀結構，然後從中選取網域。
  - 電腦名稱：按一下按鈕開啟用戶端樹狀結構，然後從中選取用戶端電腦。
  - 平台
  - 登入名稱
  - NIC 說明：輸入不含萬用字元的完整或部分說明。

    秘訣

    趨勢科技建議您輸入 NIC 製造商，因為 NIC 說明的開頭通常是製造商的名稱。例如：如果輸入 "Intel"，則 Intel 製造的所有 NIC 都將符合條件。如果輸入特定 NIC 型號，例如："Intel(R) Pro/100"，則 NIC 說明中開頭為 "Intel(R) Pro/100" 的 NIC 才符合條件。
  - 用戶端狀態
- 權限：選取是否要授與使用者權限變更防火牆安全層級，或編輯可設定的例外清單以允許指定的傳輸類型。如需有關這些選項的詳細資訊，請參閱新增或修改防火牆策略 第 12-10 頁。

4. 按一下「儲存」。

防火牆權限

允許使用者設定自己的防火牆設定。OfficeScan 伺服器部署的設定無法覆寫使用者設定的任何設定。例如，如果使用者關閉「入侵偵測系統」(IDS)，而您啟動 OfficeScan 伺服器上的 IDS，則 OfficeScan 用戶端電腦上的 IDS 仍會維持關閉狀態。

啟動下列設定讓使用者設定防火牆：

- 顯示用戶端主控台上的「防火牆」標籤

  「防火牆」標籤會顯示 OfficeScan 用戶端上的所有防火牆設定，並允許具有防火牆權限的使用者設定自己的設定。

- 允許使用者啟動/關閉防火牆、入侵偵測系統和防火牆違規通知訊息

  OfficeScan 防火牆使用狀態檢測、高效能網路病毒掃瞄和消除病毒，來保護網路上的用戶端和伺服器。如果您授與使用者啟動或關閉防火牆和其功能的權限，請警告他們不要長時間關閉防火牆，以避免電腦遭受入侵和駭客攻擊。

  如果您並未授與使用者這些權限，則從 OfficeScan 伺服器 Web 主控台設定的防火牆設定會顯示在 OfficeScan 用戶端主控台的「網路卡清單」下。

- 允許用戶端將防火牆記錄檔傳送到 OfficeScan 伺服器

  選取此選項可分析 OfficeScan 防火牆所封鎖和允許的傳輸。如需有關防火牆記錄檔的詳細資訊，請參閱防火牆記錄檔 第 12-26 頁。

  如果您選取此選項，請到「網路上的電腦 > 全域用戶端設定」中設定記錄檔傳送預約。移至「防火牆設定」區段。此預約時程只會套用到具備防火牆記錄檔傳送權限的用戶端。如需指示，請參閱全域防火牆設定 第 12-23 頁。

授與防火牆權限

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 權限和其他設定」。
4. 在「權限」標籤上，移至「防火牆權限」區段。
5. 選取下列選項：

- 顯示用戶端主控台上的「防火牆」標籤 第 12-22 頁
- 允許使用者啟動/關閉防火牆、入侵偵測系統和防火牆違規通知訊息 第 12-22 頁
- 允許用戶端將防火牆記錄檔傳送到 OfficeScan 伺服器 第 12-22 頁

6. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

全域防火牆設定

可透過多種方式將全域防火牆設定套用至 OfficeScan 用戶端。

- 可將特定防火牆設定套用至伺服器所管理的所有用戶端。
- 可將設定只套用至具有特定防火牆權限的 OfficeScan 用戶端。例如，您可以只將防火牆記錄檔傳送排程套用至具有將記錄檔傳送到伺服器的權限的 OfficeScan 用戶端。

視需要啟動下列全域設定：

- 將防火牆記錄檔傳送到伺服器

  您可以授與特定 OfficeScan 用戶端將防火牆記錄檔傳送到 OfficeScan 伺服器的權限。在這個區段中設定記錄檔傳送預約時程。只有具備傳送防火牆記錄檔權限的用戶端才會使用預約。

  如需選取用戶端可用的防火牆權限的資訊，請參閱防火牆權限 第 12-21 頁。

- 只在系統重新啟動後更新 OfficeScan 防火牆驅動程式

可讓 OfficeScan 用戶端只在 OfficeScan 用戶端電腦重新啟動後才更新一般防火牆驅動程式。啟動此選項，可避免用戶端電腦在用戶端升級期間，由於進行一般防火牆驅動程式更新而可能出現的中斷（例如暫時中斷網路連線）。

注意

此功能只支援從 OfficeScan 8.0 SP1 和更新版本升級的用戶端。

- 每小時傳送防火牆記錄檔資訊至 OfficeScan 伺服器一次，以確定是否有可能發生防火牆病毒爆發

  啟動此選項時，OfficeScan 用戶端會每小時向 OfficeScan 伺服器傳送一次防火牆記錄檔數。如需有關防火牆記錄檔的詳細資訊，請參閱防火牆記錄檔 第 12-26 頁。

  OfficeScan 會使用記錄檔數和防火牆違規事件爆發條件判斷防火牆違規事件爆發的可能性。發生爆發情況時，OfficeScan 會傳送電子郵件通知給 OfficeScan 管理員。

設定全域防火牆設定

程序

1. 瀏覽至「用戶端電腦 > 全域用戶端設定」。
2. 移至下列區段並進行設定：

表 12-3. 全域防火牆設定

區段	設定
防火牆設定	• 將防火牆記錄檔傳送到伺服器 第 12-23 頁 • 只在系統重新啟動後更新 OfficeScan 防火牆驅動程式 第 12-23 頁
防火牆記錄檔數	每小時傳送防火牆記錄檔資訊至 OfficeScan 伺服器一次，以確定是否有可能發生防火牆病毒爆發 第 12-24 頁

3. 按一下「儲存」。

OfficeScan 用戶端使用者的防火牆違規通知

OfficeScan 防火牆封鎖違反防火牆策略的輸出傳輸之後，OfficeScan 可以立即在用戶端電腦上顯示通知訊息。授與使用者啟動/關閉通知訊息的權限。

注意

設定特定防火牆策略時，您也可以啟動通知。如果要設定防火牆策略，請參閱新增或修改防火牆策略 第 12-10 頁。

授與使用者啟動/關閉通知訊息的權限

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 權限和其他設定」。
4. 在「權限」標籤上，移至「防火牆權限」區段。
5. 選取「允許使用者啟動/關閉防火牆、入侵偵測系統和防火牆違規通知訊息」。
6. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。

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

修改防火牆通知訊息的內容

程序

1. 瀏覽至「通知 > 用戶端使用者通知」。
2. 按一下「防火牆違規」標籤。
3. 在提供的文字方塊中修改預設訊息。
4. 按一下「儲存」。

防火牆記錄檔

伺服器上可用的防火牆記錄檔是由具有傳送防火牆記錄檔權限的 OfficeScan 用戶端所傳送。授與特定用戶端此權限，以監控並分析用戶端電腦上由 OfficeScan 防火牆封鎖的傳輸。

如需有關防火牆權限的資訊，請參閱防火牆權限 第 12-21 頁。

如果要避免記錄檔佔去過多硬碟空間，請手動刪除記錄檔或設定記錄檔刪除預約時程。如需有關管理記錄檔的詳細資訊，請參閱記錄檔管理 第 13-31 頁。

檢視防火牆記錄檔

程序

1. 瀏覽至「 記錄檔 > 用戶端電腦記錄檔 > 安全性風險」或「用戶端電腦 > 用戶端管理」。

2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「記錄檔 > 防火牆記錄檔」或「檢視記錄檔 > 防火牆記錄檔」。
4. 為確保您可以使用最新的記錄檔，請按一下「通知用戶端」。預留一些時間給用戶端傳送防火牆記錄檔，再繼續執行下一個步驟。
5. 指定記錄條件，然後按一下「顯示記錄檔」。
6. 檢視記錄檔。記錄檔包含下列資訊：
   - 偵測防火牆違規的日期和時間
   - 發生防火牆違規的電腦
   - 發生防火牆違規的電腦網域
   - 遠端主機 IP 位址
   - 本機主機 IP 位址
   - 通訊協定
   - 通訊埠號碼
   - 方向：如果輸入（接收）或輸出（送出）傳輸違反防火牆策略
   - 程序：在電腦上執行，導致發生防火牆違規的可執行程式或服務
   - 說明：指定實際的安全威脅（例如：網路病毒或 IDS 攻擊）或防火牆策略違規
7. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請按一下「匯出到 CSV」。開啟檔案或將其儲存至特定位置。

防火牆違規事件爆發

依防火牆違規事件數目和偵測期間定義防火牆違規事件爆發。

OfficeScan 具有預設通知訊息，可在偵測到爆發時，通知您和其他 OfficeScan 管理員。您可以視需要修改通知訊息。

注意

OfficeScan 可以透過電子郵件傳送防火牆爆發通知。設定電子郵件設定，讓 OfficeScan 可以成功地傳送電子郵件。如需詳細資訊，請參閱管理員通知設定 第 13-28 頁。

設定防火牆違規事件爆發條件和通知

程序

1. 瀏覽至「通知 > 管理員通知 > 病毒爆發通知」。
2. 在「條件」標籤中：
   a. 移至「防火牆違規事件」區段。
   b. 選取「監控用戶端電腦的防火牆違規事件」。
   c. 指定 IDS 記錄檔、防火牆記錄檔和網路病毒記錄檔的數量。
   d. 指定偵測期間。

   秘訣

   趨勢科技建議您接受此畫面中的預設值。

   OfficeScan 會在記錄檔數量超過指定值時傳送通知訊息。例如，如果您指定 100 個 IDS 記錄檔、100 個防火牆記錄檔和 100 個網路病毒記錄檔，並指定 3 小時的期間，當伺服器在 3 個小時內收到 301 個記錄檔時，OfficeScan 會傳送通知。
3. 在「電子郵件」標籤中：
   a. 移至「防火牆違規事件爆發」區段。
   b. 選取「啟動電子郵件通知」。

c. 指定電子郵件收件者。

d. 接受或修改預設的電子郵件主旨和訊息。您可以使用 Token 變數代表「主旨」和「訊息」欄位中的資料。

表 12-4. 防火牆違規病毒爆發通知的 Token 變數

變數	說明
%A	記錄檔超出
%C	防火牆違規記錄檔數量
%T	防火牆違規記錄檔累計的時段

4. 按一下「儲存」。

測試 OfficeScan 防火牆

為確保 OfficeScan 防火牆能正常運作，請在 OfficeScan 用戶端或 OfficeScan 用戶端群組執行測試。

警告!

只能在受控制的環境中測試 OfficeScan 用戶端程式設定。請勿在連線至網路或 Internet 的用戶端電腦執行測試。這樣做可能會讓 OfficeScan 用戶端電腦暴露於病毒、駭客攻擊和其他風險之中。

程序

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 OfficeScan 用戶端存取 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. 按一下「指定資料檔給用戶端」。
4. 驗證部署。
   a. 按一下「用戶端電腦 > 用戶端管理」。
   b. 選取用戶端所屬的網域。
   c. 從用戶端樹狀結構檢視中選取「防火牆檢視」。
   d. 檢查用戶端樹狀結構的「防火牆」欄位下方是否有綠色的核取記號。如果您已為該用戶端啟動「入侵偵測系統」，請確認「IDS」欄下也顯示了綠色的核取記號。
   e. 驗證用戶端是否已套用正確的防火牆策略。用戶端樹狀結構的「防火牆策略」欄位下方會顯示策略。
5. 嘗試傳送或接收您在策略中設定的傳輸類型，以在用戶端電腦上測試防火牆。
6. 如果要測試設定為防止用戶端存取 Internet 的策略，請在用戶端電腦上開啟 Web 瀏覽器。如果您已設定 OfficeScan 在發生防火牆違規事件時顯示通知訊息，就會在發生輸出傳輸違規時在用戶端電腦上顯示訊息。

部分 III

管理 OfficeScan 伺服器和用戶端

第 13 章

管理 OfficeScan 伺服器

本章說明 OfficeScan 伺服器管理和組態設定。

本章內容：

以角色為基礎的管理

使用「以角色為基礎的管理」授與和控制存取 OfficeScan Web 主控台的權限。如果貴組織中有多位 OfficeScan 管理員，可以使用此功能將特定的 Web 主控台權限分配給各個管理員，並提供只在執行特定工作所需的工具和權限給管理員。透過指定一個或多個要管理的網域給管理員，還可以控制對用戶端樹狀結構的存取權限。此外，您可以將 Web 主控台的「僅檢視」存取權授與非管理員。

每位使用者（管理員或非管理員）都會有指定的特定角色。角色定義了對 Web 主控台的存取層級。使用者使用自訂使用者帳號或 Active Directory 帳號登入 Web 主控台。

以角色為基礎的管理包含下列工作：

1. 定義使用者角色。如需詳細資訊，請參閱使用者角色 第 13-2 頁。
2. 設定使用者帳號並指定特定角色給每個使用者帳號。如需詳細資訊，請參閱使用者帳號 第 13-16 頁。

從系統事件記錄檔檢視所有使用者的 Web 主控台活動。記錄的活動如下：

- 登入主控台
- 密碼修改
- 登出主控台
- 作業階段逾時（系統自動將使用者登出）

使用者角色

使用者角色決定使用者可存取的 Web 主控台功能表項目。角色指定有每個功能表項目的權限。

指定下列項目的權限：

- 功能表項目權限 第 13-3 頁
- 功能表項目類型 第 13-3 頁

功能表項目權限

權限決定每個功能表項目的存取層級。功能表項目權限可以是：

- 設定：允許完整存取功能表項目。使用者可以設定全部設定，執行全部工作並檢視功能表項目中的資料。
- 檢視：只允許使用者檢視功能表項目中的設定、工作和資料。
- 無存取權：隱藏功能表項目，無法檢視。

功能表項目類型

OfficeScan 有 3 種功能表項目類型。

表 13-1. 功能表項目類型

類型	範圍
伺服器/用戶端適用的功能表項目	• 伺服器設定、工作和資料 • 全域用戶端設定、工作和資料 如需有關可用功能表項目的完整清單，請參閱伺服器和用戶端適用的功能表項目 第 13-4 頁。
受管理網域適用的功能表項目	在用戶端樹狀結構外可用的精細用戶端設定、工作和資料 如需有關可用功能表項目的完整清單，請參閱受管理網域適用的功能表項目 第 13-7 頁。
用戶端管理功能表項目	在用戶端樹狀結構內可用的精細用戶端設定、工作和資料 如需有關可用功能表項目的完整清單，請參閱用戶端管理功能表項目 第 13-8 頁。

伺服器和用戶端適用的功能表項目

下表列出伺服器/用戶端的功能表項目：

表 13-2. 伺服器/用戶端適用的功能表項目

主功能表項目	子功能表
立即掃瞄所有網域 注意 只有使用內建的管理員角色的使用者可以存取此功能。	無

用戶端電腦	• 用戶端管理
	• 用戶端分組
	• 全域用戶端設定
	• 電腦位置
	• Data Loss Prevention
	  • 資料識別碼
	  • 範本
	• 連線驗證
	• 病毒爆發防範

主動式雲端截毒技術	• 主動式雲端截毒伺服器來源 • 整合式伺服器 • Smart Feedback

主功能表項目	子功能表

更新	• 伺服器
	  • 預約更新
	  • 手動更新
	  • 更新來源
	• 用戶端電腦
	  • 自動更新
	  • 更新來源
	• 還原

記錄檔	• 用戶端電腦記錄檔
	  • 安全威脅
	  • 元件更新
	• 伺服器更新記錄檔
	• 系統事件記錄檔
	• 記錄檔維護

Cisco NAC	• 策略伺服器 • 代理程式管理 • 代理程式部署 • 用戶端憑證

通知	• 管理員通知
	  • 一般設定
	  • 病毒爆發通知
	• 用戶端使用者通知

主功能表項目	子功能表

管理	• 使用者帳號
	• 使用者角色
	
	注意
	只有使用內建管理員帳號的使用者可以存取使用者帳號和角色。
	
	• Active Directory
	  • Active Directory 整合
	  • 預約同步處理
	• Proxy 伺服器設定
	• 連線設定
	• 離線用戶端
	• 隔離區管理員
	• 產品使用授權
	• Control Manager 設定
	• Web 主控台設定
	• 資料庫備份

工具	• 管理工具 • 用戶端工具
Plug-in Manager 注意 只有使用內建管理員帳號的使用者可以存取此功能。	無

受管理網域適用的功能表項目

下表列出受管理網域的功能表項目：

表 13-3. 受管理網域適用的功能表項目

主功能表項目	子功能表
摘要 注意 任何使用者不論其權限為何，都能存取此頁面。	無

安全性符合	• 符合性評估
	  • 符合性報告
	  • 預約符合性報告
	• 外部伺服器管理

用戶端電腦	• 防火牆
	  • 策略
	  • 資料檔
	• 用戶端安裝
	  • Browser-based
	  • 遠端

更新	• 摘要 • 用戶端電腦 • 手動更新

記錄檔	• 用戶端電腦記錄檔
	  • 連線驗證
	  • 間諜程式/可能的資安威脅程式恢復

主功能表項目	子功能表
通知	• 管理員通知 • 標準通知

用戶端管理功能表項目

下表列出用戶端管理功能表項目：

表 13-4. 用戶端管理功能表項目

主功能表項目	子功能表
狀態	無
工作	• 立即掃瞄 • 用戶端解除安裝 • 間諜程式/可能的資安威脅程式恢復

主功能表項目	子功能表

設定	• 掃瞄設定
	  • 掃瞄方法
	  • 手動掃瞄設定
	  • 即時掃瞄設定
	  • 預約掃瞄設定
	  • 立即掃瞄設定
	• 網頁信譽評等設定
	• 行為監控設定
	• 周邊設備存取控管設定
	• Data Loss Prevention 設定
	• 更新代理程式設定
	• 權限和其他設定
	• 其他服務設定
	• 間諜程式/可能的資安威脅程式核可清單
	• 匯出設定
	• 匯入設定

記錄檔	• 病毒/惡意程式記錄檔 • 間諜程式/可能的資安威脅程式記錄檔 • 防火牆記錄檔 • 網頁信譽評等記錄檔 • 行為監控記錄檔 • 周邊設備存取控管記錄檔 • Data Loss Prevention 記錄檔 • 刪除記錄檔

主功能表項目	子功能表
管理用戶端樹狀結構	• 新增網域 • 重新命名網域 • 移動用戶端 • 排序用戶端 • 移除網域/用戶端
匯出	無

內建使用者角色

OfficeScan 隨附一組內建的使用者角色，但您無法視需要修改或刪除。內建角色包括：

表 13-5. 內建使用者角色

角色名稱	說明
Administrator（系統管理員）	將此角色委派給其他 OfficeScan 管理員或對 OfficeScan 有相當程度瞭解的使用者。 具有此角色的使用者擁有對所有功能表項目的「設定」權限。

Guest User（訪客使用者）	將此角色委派給想要檢視 Web 主控台用於參考用途的使用者。
	• 具有此角色的使用者沒有下列功能表項目的存取權：
	  • 立即掃瞄所有網域
	  • Plug-in Manager
	  • 「管理 > 使用者角色」
	  • 「管理 > 使用者帳號」
	• 使用者具有所有其他功能表項目的「檢視」權限。

角色名稱	說明
Trend Power User	此角色僅在從 OfficeScan 10 升級時可用。 此角色會繼承 OfficeScan 10 中「Power User（進階使用者）」角色的權限。擁有此角色的使用者具有所有用戶端樹狀結構網域的「設定」權限，但是無法存取此版本中的新功能。

自訂角色

如果沒有任何一個內建角色符合您的需求，您可以建立自訂角色。

只有具有內建管理員角色和使用在安裝 OfficeScan 期間建立的 root 帳號的使用者，才可以建立自訂使用者角色和指定這些角色給使用者帳號。

新增自訂角色

程序

1. 瀏覽至「 管理 > 使用者角色 」。
2. 按一下「新增」。如果您要建立的新角色與現有角色具有類似的設定，請選取現有的角色，並按一下「複製」。隨即顯示新畫面。
3. 輸入角色名稱，並視需要提供說明。
4. 定義用戶端樹狀結構範圍。
   a. 按一下「定義用戶端樹狀結構範圍」。接著會開啟一個新畫面。
   b. 選取根網域圖示 ()，或用戶端樹狀結構中的一個或多個網域。
   c. 按一下「儲存」。

注意

如果未定義用戶端樹狀結構範圍，將無法儲存自訂角色。

此時僅定義了網域。對選定網域的存取層級將在步驟 6 和步驟 7 中定義。

5. 按一下「全域功能表項目」標籤。

6. 按一下「伺服器/用戶端適用的功能表項目」並指定每個可用功能表項目的權限。如需有關可用功能表項目的清單，請參閱伺服器和用戶端適用的功能表項目 第 13-4 頁。

   在步驟 3 中已設定的用戶端樹狀結構範圍，會決定功能表項目的權限等級，並定義權限的目標。用戶端樹狀結構範圍可以是根網域（全部用戶端）或特定用戶端樹狀結構網域。

   表 13-6. 伺服器/用戶端適用的功能表項目和用戶端樹狀結構範圍

條件	用戶端樹狀結構範圍	
	根網域	特定網域
功能表項目權限	設定、檢視或無存取權	檢視或無存取權
目標	OfficeScan 伺服器和全部用戶端 例如，如果授與某個角色對全部伺服器/用戶端功能表項目的「設定」權限，則使用者可以： • 管理伺服器設定、工作和資料 • 部署全域用戶端設定 • 啟動全域用戶端工作 • 管理全域用戶端資料	OfficeScan 伺服器和全部用戶端 例如，如果授與某個角色對全部伺服器/用戶端功能表項目的「設定」權限，則使用者可以： • 檢視伺服器設定、工作和資料 • 檢視全域用戶端設定、工作和資料

   - 某些功能表項目不適用於自訂角色。例如，Plug-in Manager、「使用者角色」和「使用者帳號」僅適用於具有內建管理員角色的使用者。
   - 如果選取「設定」下的核取方塊，則會自動選取「檢視」下的核取方塊。
   - 如果未選取任何核取方塊，則權限為「無存取權」。

7. 按一下「受管理網域適用的功能表項目」，並指定每個可用功能表項目的權限。如需有關可用功能表項目的清單，請參閱。

在步驟 3 中已設定的用戶端樹狀結構範圍，會決定功能表項目的權限等級，並定義權限的目標。用戶端樹狀結構範圍可以是根網域（全部用戶端）或特定用戶端樹狀結構網域。

表 13-7. 受管理網域適用的功能表項目和用戶端樹狀結構範圍

條件	用戶端樹狀結構範圍	
	根網域	特定網域
功能表項目權限	設定、檢視或無存取權	設定、檢視或無存取權
目標	全部用戶端或特定用戶端 範例： • 如果使用者部署了防火牆策略，則這些策略將部署到全部用戶端。 • 使用者可以在全部用戶端或特定用戶端上啟動手動用戶端更新。 • 符合性報告可以包含全部用戶端或特定用戶端。	選定網域中的用戶端 範例： • 如果使用者部署了防火牆策略，則這些策略將僅部署到選定網域中的用戶端。 • 使用者僅可以在選定網域中的用戶端上啟動手動用戶端更新。 • 符合性報告僅包含選定網域中的用戶端。

- 如果選取「設定」下的核取方塊，則會自動選取「檢視」下的核取方塊。
- 如果未選取任何核取方塊，則權限為「無存取權」。

8. 按一下「用戶端管理功能表項目」標籤，並指定每個可用功能表項目的權限。如需有關可用功能表項目的清單，請參閱。

   在步驟 3 中已設定的用戶端樹狀結構範圍，會決定功能表項目的權限等級，並定義權限的目標。用戶端樹狀結構範圍可以是根網域（全部用戶端）或特定用戶端樹狀結構網域。

表 13-8. 用戶端管理功能表項目和用戶端樹狀結構範圍

條件	用戶端樹狀結構範圍	
	根網域	特定網域
功能表項目權限	設定、檢視或無存取權	設定、檢視或無存取權
目標	根網域（全部用戶端）或特定網域 例如，可以授與某個角色具有對用戶端樹狀結構中的「工作」功能表項目的「設定」權限。如果目標為根網域，使用者可在全部用戶端上啟動工作。如果目標為網域 A 和 B，僅可在網域 A 和 B 中的用戶端上啟動工作。	僅選定網域 例如，可以授與某個角色具有對用戶端樹狀結構中的「設定」功能表項目的「設定」權限。這意味著使用者僅可部署設定到選定網域中的用戶端。
	僅當「伺服器/用戶端適用的功能表項目」中「用戶端管理」功能表項目的權限為「檢視」時，才會顯示用戶端樹狀結構。	

- 如果選取「設定」下的核取方塊，則會自動選取「檢視」下的核取方塊。
- 如果未選取任何核取方塊，則權限為「無存取權」。
- 如果為特定網域設定權限，可透過按一下「將所選網域的設定複製到其他網域」，將權限複製到其他網域。

9. 按一下「儲存」。新角色會顯示在「使用者角色」清單上。

修改自訂角色

程序

1. 瀏覽至「 管理 > 使用者角色 」。
2. 按一下角色名稱。隨即顯示新畫面。
3. 修改下列任一項：

- 說明
- 用戶端樹狀結構範圍
- 角色權限
  - 伺服器/用戶端適用的功能表項目
  - 受管理網域適用的功能表項目
  - 用戶端管理功能表項目

4. 按一下「儲存」。

刪除自訂角色

程序

1. 瀏覽至「 管理 > 使用者角色 」。
2. 選取角色旁的核取方塊。
3. 按一下「刪除」。

注意

如果角色至少指定給一個使用者帳號，則無法刪除該角色。

匯入或匯出自訂角色

程序

1. 瀏覽至「 管理 > 使用者角色 」。
2. 如果要將自訂角色匯出到 `.dat` 檔案：
   a. 選取角色，然後按一下「匯出」。

b. 儲存 .dat 檔案。如果要管理另一部 OfficeScan 伺服器，可以使用該 .dat 檔案將自訂角色匯入至該伺服器。

注意

匯出角色操作只能在相同版本的伺服器之間完成。

3. 如果要將自訂角色匯出到 .csv 檔案：

   a. 選取角色，然後按一下「匯出角色設定」。

   b. 儲存 .csv 檔案。使用此檔案可以檢查所選角色的資訊和權限。

4. 如果您儲存了不同 OfficeScan 伺服器的自訂角色，而且想要將這些角色匯入到目前的 OfficeScan 伺服器，請按一下「匯入」並尋找包含自訂角色的 .dat 檔案。

   - 如果您匯入相同名稱的角色，則「使用者角色」畫面上的角色會遭到覆寫。
   - 匯入角色操作只能在相同版本的伺服器之間完成。
   - 從其他 OfficeScan 伺服器匯入的角色：
     - 保留伺服器/用戶端功能表項目以及受管理網域功能表項目的權限。
     - 套用用戶端管理功能表項目的預設權限。在另一台伺服器上，記錄角色對用戶端管理功能表項目的權限，然後將這些權限重新套用到匯入的角色。

使用者帳號

設定使用者帳號並指定特定角色給每個使用者。使用者角色決定使用者可檢視或設定的 Web 主控台功能表項目。

安裝 OfficeScan 伺服器期間，安裝程式會自動建立名為「root」的內建帳號。使用 root 帳號登入的使用者可以存取所有功能表項目。您無法刪除 root 帳號，但可修改該帳號的詳細資料（例如：密碼和完整名稱，或是帳號說明）。如果忘記 root 帳號的密碼，請聯絡經銷商取得重設密碼的協助。

新增自訂帳號或 Active Directory 帳號。所有顯示在「使用者帳號」清單中的使用者帳號都會列在 Web 主控台。

您可以使用 OfficeScan 使用者帳號來執行「單一登入」。單一登入允許使用者從 Trend Micro Control Manager 主控台存取 OfficeScan Web 主控台。如需詳細資訊，請參閱下面的程序。

新增自訂帳號

程序

1. 瀏覽至「 管理 > 使用者帳號 」。
2. 按一下「新增」。
3. 選取「自訂帳號」。
4. 輸入使用者名稱、全名和密碼，並確認密碼。
5. 輸入帳號的電子郵件信箱。

   注意

   OfficeScan 會將通知傳送至此電子郵件地址。這些通知會通知收件者安全威脅偵測和數位資產傳輸。如需有關通知的詳細資訊，請參閱管理員的安全威脅通知 第 7-72 頁和管理員的 Data Loss Prevention 通知 第 10-43 頁。

6. 選取帳號的角色。
7. 按一下「儲存」。
8. 將帳號詳細資訊傳送給使用者。

修改自訂帳號

程序

1. 瀏覽至「 管理 > 使用者帳號 」。

2. 按一下使用者帳號。
3. 使用提供的核取方塊啟動或關閉帳號。
4. 修改下列項目：
   - 完整名稱
   - 密碼
   - 電子郵件信箱
   - 角色
5. 按一下「儲存」。
6. 將新帳號詳細資訊傳送給使用者。

新增 Active Directory 帳號或群組

程序

1. 瀏覽至「 管理 > 使用者帳號 」。
2. 按一下「新增」。
3. 選取「Active Directory 使用者或群組」。
4. 指定帳號名稱（使用者名稱或群組）和帳號所屬的網域。

   請包含完整帳號和網域名稱。如果使用預設群組「網域使用者」，則 OfficeScan 不會傳回不完整帳號和網域名稱的結果。

   屬於某群組的所有成員會取得相同的角色。如果特定帳號屬於至少兩個群組，而且針對這兩個群組的角色不同：

   - 會合併兩個角色的權限。如果使用者設定特定設定，而該設定中有權限衝突的情況，則會套用較高的權限。
   - 所有使用者角色都會顯示在「系統事件」記錄檔中。例如，「使用者 John Doe 以下列角色登入：Administrator（管理員）、Guest User（訪客使用者）」。

5. 選取帳號的角色。
6. 按一下「儲存」。
7. 通知使用者使用其網域帳號和密碼登入 Web 主控台。

新增多個 Active Directory 帳號或群組

程序

1. 瀏覽至「 管理 > 使用者帳號 」。
2. 按一下「從 Active Directory 新增」。
3. 指定使用者名稱和帳號所屬網域，以搜尋帳號（使用者名稱或群組）。

   注意

   您可以使用 * 字元來搜尋多個帳號。如果不想指定萬用字元，請包含完整的帳號名稱。如果使用預設群組「網域使用者」，則 OfficeScan 不會傳回不完整帳號名稱的結果。

4. 當 OfficeScan 找到有效的帳號時，它會在「使用者和群組」下顯示帳號名稱。按下一步圖示 (>) 即可在「選取的使用者和群組」下移動帳戶。

   如果指定 Active Directory 群組，屬於該群組的所有成員會取得相同角色。如果特定帳號屬於至少兩個群組，而且針對這兩個群組的角色不同：

   - 會合併兩個角色的權限。如果使用者設定特定設定，而該設定中有權限衝突的情況，則會套用較高的權限。
   - 所有使用者角色都會顯示在「系統事件」記錄檔中。例如，「使用者 John Doe 以下列角色登入：系統管理員、進階使用者」。

5. 新增更多帳號或群組。
6. 選取帳號或群組的角色。
7. 按一下「儲存」。

8. 通知使用者使用其網域名稱和密碼登入 Web 主控台。

變更自訂或 Active Directory 帳號的角色

程序

1. 瀏覽至「 管理 > 使用者帳號 」。
2. 選取一個或多個自訂帳號或 Active Directory 帳號。
3. 按一下「變更角色」。
4. 在顯示的畫面上，選取新角色並按一下「儲存」。

啟動或關閉自訂或 Active Directory 帳號

程序

1. 瀏覽至「 管理 > 使用者帳號 」。
2. 按一下「啟動」下的圖示。

> 注意
> 無法關閉 root 帳號。

在 Control Manager 中使用 OfficeScan 使用者帳號

如需詳細步驟，請參閱 Control Manager 文件。

程序

1. 在 Control Manager 中建立新使用者帳號。指定使用者名稱時，請輸入 OfficeScan Web 主控台上顯示的帳號名稱。

2. 為新帳號指定對於 OfficeScan 伺服器的「存取」和「設定」權限。

注意

如果 Control Manager 使用者具有 OfficeScan 的「存取」和「設定」權限，但沒有 OfficeScan 帳號，則該使用者無法存取 OfficeScan。使用者會看到一個含有連結的訊息，按一下該連結即可開啟 OfficeScan Web 主控台的登入畫面。

Trend Micro Control Manager

Trend Micro Control Manager™ 是一個中央管理主控台，會在閘道、郵件伺服器、檔案伺服器和企業桌上型電腦層級上，管理趨勢科技產品和服務。Control Manager 的 Web-based 管理主控台提供單一監控點，可供網路上受管理的產品和服務使用。

Control Manager 可讓系統管理員監控並針對中毒、安全違規或病毒進入點等活動進行報告。系統管理員可以在整個網路上下載並部署元件，這有助於確保防護處於一致且最新的狀態。Control Manager 可讓使用者執行手動和預約更新，並將產品視為群組或個體來設定和管理，以提升彈性。

此版本 OfficeScan 與 Control Manager 的整合

此 OfficeScan 版本包含下列功能（從 Control Manager 管理 OfficeScan 伺服器時）：

- 建立、管理和部署 OfficeScan 防毒、Data Loss Prevention 及周邊設備存取控管的策略，並直接從 Control Manager 主控台指定權限給 OfficeScan 用戶端。

  下表列出 Control Manager 6.0 中可用的策略組態設定。

表 13-9. Control Manager 中的 OfficeScan 策略管理類型

策略類型	功能
OfficeScan 防毒和用戶端設定	• 其他服務設定 • 行為監控設定 • 周邊設備存取控管設定 • 手動掃瞄設定 • 權限和其他設定 • 即時掃瞄設定 • 間諜程式/可能的資安威脅程式核可清單 • 掃瞄方法 • 立即掃瞄設定 • 預約掃瞄設定 • 更新代理程式設定 • 網頁信譽評等設定
資料安全防護	Data Loss Prevention 策略設定 注意 在 OfficeScan 用戶端策略中管理「資料安全防護」的「周邊設備存取控管」權限

- 從 Control Manager 主控台將下列設定從一部 OfficeScan 伺服器複製到另一部 OfficeScan 伺服器：
  - 資料識別碼類型 第 10-4 頁
  - Data Loss Prevention 範本 第 10-17 頁

注意

如果將這些設定複製到尚未啟動資料安全防護使用授權的 OfficeScan 伺服器，只有當啟動使用授權後，設定才會生效。

支援的 Control Manager 版本

此 OfficeScan 版本支援 Control Manager 6.0、5.5 SP1、5.5 和 5.0。

表 13-10. 支援的 Control Manager 版本

OfficeScan 伺服器	Control Manager 版本			
	6.0	5.5 SP1	5.5	5.0
雙堆疊	是	是	是	是
純 IPv4	是	是	是	是
純 IPv6	是	否	否	否

注意

IPv6 僅支援 Control Manager 5.5 Service Pack 1 以上的版本。

如需有關 OfficeScan 伺服器和 OfficeScan 用戶端回報給 Control Manager 的 IP 位址詳細資訊，請參閱 顯示 IP 位址的畫面 第 A-6 頁。

套用這些 Control Manager 版本的最新 Patch 和重要的 HotFix，讓 Control Manager 能夠管理 OfficeScan。如果要取得最新的 Patch 和 HotFix，請聯絡您的經銷商或瀏覽趨勢科技下載專區：

http://www.trendmicro.com/download/zh-tw/

安裝 OfficeScan 之後，請將它註冊到 Control Manager，然後在 Control Manager 管理主控台上設定 OfficeScan。如需有關管理 OfficeScan 伺服器的資訊，請參閱 *Control Manager 文件*。

向 Control Manager 註冊 OfficeScan

程序

1. 瀏覽至「管理 > Control Manager 設定」。
2. 指定項目顯示名稱，這是將在 Control Manager 中顯示的 OfficeScan 伺服器名稱。

   依預設，項目顯示名稱包含伺服器電腦的主機名稱和此產品的名稱（例如：Server01_OSCE）。

   注意

   在 Control Manager 中，Control Manager 所管理的 OfficeScan 伺服器和其他產品稱為「項目」。
3. 指定 Control Manager 伺服器的 FQDN 或 IP 位址，以及用來連線至此伺服器的通訊埠號碼。也可以選擇使用 HTTPS 以增加連線安全。
   - 對於雙堆疊 OfficeScan 伺服器，請輸入 Control Manager FQDN 或 IP 位址（IPv4 或 IPv6，如果可用）。
   - 對於純 IPv4 OfficeScan 伺服器，請輸入 Control Manager FQDN 或 IPv4 位址。
   - 對於純 IPv6 OfficeScan 伺服器，請輸入 Control Manager FQDN 或 IPv6 位址。

   注意

   只有 Control Manager 5.5 SP1 和更新版本支援 IPv6。
4. 如果 Control Manager 的 IIS Web 伺服器需要驗證，請輸入使用者名稱和密碼。
5. 如果要使用 Proxy 伺服器連線至 Control Manager 伺服器，請指定下列 Proxy 伺服器設定：
   - Proxy 通訊協定

- 伺服器 FQDN 或 IPv4/IPv6 位址和通訊埠
- Proxy 伺服器驗證的使用者 ID 和密碼

6. 決定要使用單向通訊還是雙向通訊通訊埠轉送，然後指定 IPv4/IPv6 位址和通訊埠。
7. 如果要檢查 OfficeScan 是否能根據您指定的設定連線至 Control Manager 伺服器，請按一下「測試連線」。

   如果已成功建立連線，請按一下「註冊」。
8. 如果您在註冊後變更此畫面中的任何設定，請在變更設定後按一下「更新設定」，將變更通知 Control Manager 伺服器。
9. 如果不想再讓 Control Manager 伺服器管理 OfficeScan，請按一下「取消註冊」。

在 Control Manager 管理主控台上檢查 OfficeScan 的狀態

程序

1. 開啟 Control Manager 管理主控台。

   如果要開啟 Control Manager 主控台，請在網路上的任何一部電腦上，開啟 Web 瀏覽器並輸入：

   ```
   https://<Control Manager 伺服器名稱>/Webapp/login.aspx
   ```

   其中 `<Control Manager 伺服器名稱>` 是 Control Manager 伺服器的 IP 位址或主機名稱
2. 在「主功能表」上，按一下「產品」。
3. 檢查 OfficeScan 伺服器圖示是否顯示。

參考伺服器

OfficeScan 用戶端決定使用哪個策略或資料檔的其中一個方式是檢查與 OfficeScan 伺服器的連線狀態。如果內部 OfficeScan 用戶端（或企業網路內的用戶端）無法連線到伺服器，則用戶端狀態會成為「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。

中斷與 OfficeScan 伺服器連線的 OfficeScan 用戶端會嘗試連線至參考伺服器。如果用戶端成功建立與參考伺服器的連線，就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 32 部參考伺服器。
- OfficeScan 用戶端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。
- OfficeScan 用戶端會在判斷防毒軟體（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。OfficeScan 伺服器會執行這些工作。
- OfficeScan 用戶端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

程序

1. 瀏覽到「 用戶端電腦 > 防火牆 > 資料檔 」或「用戶端電腦 > 電腦位置」。
2. 請根據顯示的畫面執行下列動作：
   - 如果位於「用戶端電腦的防火牆資料檔」畫面中，請按一下「編輯參考伺服器清單」。
   - 如果位於「電腦位置」畫面中，請按一下「參考伺服器清單」。
3. 選取「啟動參考伺服器清單」。
4. 如果要新增電腦至清單，請按一下「新增」。
   a. 指定電腦的 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電腦通訊的通訊埠。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。OfficeScan 用戶端會使用清單上的第一個通訊埠號碼，當無法建立連線時，就會使用下一個通訊埠號碼。

   c. 按一下「儲存」。
5. 如果要編輯清單上電腦的設定，請按一下電腦名稱。修改電腦名稱或通訊埠，然後按一下「儲存」。
6. 如果要從清單中移除電腦，請選取電腦名稱並按一下「刪除」。

7. 如果要讓電腦做為參考伺服器，請按一下「指定給用戶端」。

管理員通知設定

請設定管理員通知設定，讓 OfficeScan 能夠透過電子郵件、呼叫器與 SNMP Trap 順利傳送通知。OfficeSca 還可以透過 Windows NT 事件記錄檔傳送通知，但沒有為此通知管道設定任何設定。

偵測到以下情況時，OfficeScan 會傳送通知給您和其他 OfficeScan 管理員：

表 13-11. 觸發管理員通知的偵測

偵測	通知管道			
	電子郵件	呼叫器	SNMP TRAP	WINDOWS NT 事件記錄檔
病毒和惡意程式	是	是	是	是
間諜程式和可能的資安威脅程式	是	是	是	是
數位資產傳輸	是	是	是	是
病毒和惡意程式爆發	是	是	是	是
間諜程式和可能的資安威脅程式爆發	是	是	是	是
防火牆違規事件爆發	是	否	否	否
共享資料夾作業階段病毒爆發	是	否	否	否

設定管理員通知設定

程序

1. 瀏覽至「通知 > 管理員通知 > 一般設定」。

2. 設定電子郵件通知設定。
   a. 在「SMTP 伺服器」欄位中指定 IPv4/IPv6 位址或電腦名稱。
   b. 請指定 1 和 65535 之間的通訊埠號碼。
   c. 指定名稱或電子郵件信箱。

      如果要在下一個步驟中啟動 ESMTP，請指定有效的電子郵件信箱。
   d. 您可以視需要啟動 ESMTP。
   e. 為您在「寄件人」欄位中指定的電子郵件信箱指定使用者名稱和密碼。
   f. 選擇向伺服器驗證用戶端的方式：
      - 登入：登入是舊版的郵件使用者代理程式。伺服器和用戶端都使用 BASE64 來驗證使用者名稱和密碼。
      - 純文字：純文字是最容易使用的方式，但這種方式不安全，因為使用者名稱和密碼是以一個使用 BASE64 編碼的字串透過 Internet 傳送。
      - CRAM-MD5:CRAM-MD5 使用挑戰-回應組合的驗證機制和密碼編譯訊息摘要 5 演算法來交換及驗證資訊。
3. 設定呼叫器通知設定。
   a. 針對「呼叫器號碼」欄位，可使用下列字元：
      - 0 到 9
      - #
      - *
      - ,
   b. 指定 1 到 16 之間的 COM 通訊埠。
4. 設定 SNMP Trap 通知設定。
   a. 在「伺服器 IP 位址」欄位中指定 IPv4/IPv6 位址或電腦名稱。
   b. 指定不容易猜中的社群名稱。

5. 按一下「儲存」。

系統事件記錄檔

OfficeScan 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 OfficeScan 伺服器和服務運作正常。

如果要避免記錄檔佔去過多硬碟空間，請手動刪除記錄檔或設定記錄檔刪除預約時程。如需有關管理記錄檔的詳細資訊，請參閱記錄檔管理 第 13-31 頁。

檢視系統事件記錄檔

程序

1. 瀏覽至「記錄檔 > 系統事件記錄檔」。
2. 在「事件說明」下，檢查是否有需採取進一步處理行動的記錄。OfficeScan 會記錄下列事件：

表 13-12. 系統事件記錄檔

記錄類型	事件
OfficeScan 主服務和資料庫伺服器	• 已啟動主服務 • 已成功停止主服務 • 停止主服務不成功
病毒爆發防範	• 已啟動「病毒爆發防範」 • 已關閉「病毒爆發防範」 • 在過去 <分鐘數> 的共享資料夾作業階段數量
資料庫備份	• 資料庫備份成功 • 資料庫備份不成功

記錄類型	事件
以角色為基礎的 Web 主控台存取	• 登入主控台 • 密碼修改 • 登出主控台 • 作業階段逾時（系統自動將使用者登出）

3. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請按一下「匯出到 CSV」。開啟檔案或將其儲存至特定位置。

記錄檔管理

OfficeScan 會製作有關安全威脅偵測、事件和更新的完整記錄檔。使用這些記錄檔，您就可以存取組織的防護策略，並可識別較有可能中毒或受到攻擊的 OfficeScan 用戶端。您也可以使用這些記錄檔檢查用戶端和伺服器間的連線，並驗證元件更新是否成功。

OfficeScan 還會使用中央時間驗證機制，確保 OfficeScan 伺服器和用戶端之間的時間一致。這會防止因時區、日光節約時間和時差所造成的記錄檔不一致情形，該情形會令人在分析記錄檔時產生混淆。

注意

OfficeScan 會針對除伺服器更新與系統事件記錄檔外的所有記錄檔執行時間驗證。

OfficeScan 伺服器從 OfficeScan 用戶端接收以下記錄檔：

- 檢視病毒/惡意程式記錄檔 第 7-79 頁
- 檢視間諜程式/可能的資安威脅程式記錄檔 第 7-85 頁
- 檢視間諜程式/可能的資安威脅程式恢復記錄檔 第 7-88 頁
- 檢視防火牆記錄檔 第 12-26 頁
- 檢視網頁信譽評等記錄檔 第 11-10 頁

- 檢視行為監控記錄檔 第 8-11 頁
- 檢視周邊設備存取控管記錄檔 第 9-16 頁
- 檢視 Data Loss Prevention 記錄檔 第 10-47 頁
- 檢視 OfficeScan 用戶端更新記錄檔 第 6-43 頁
- 檢視連線驗證記錄檔 第 14-38 頁

OfficeScan 伺服器會產生下列記錄檔：

- OfficeScan 伺服器更新記錄檔 第 6-23 頁
- 系統事件記錄檔 第 13-30 頁

在 OfficeScan 伺服器和 OfficeScan 用戶端上還有以下記錄檔：

- Windows 事件記錄檔 第 18-23 頁
- OfficeScan 伺服器記錄檔 第 18-3 頁
- OfficeScan 用戶端記錄檔 第 18-15 頁

記錄檔維護

如果要避免記錄檔佔去過多硬碟空間，請從 Web 主控台手動刪除記錄檔或設定記錄檔刪除預約時程。

根據預約時程刪除記錄檔

程序

1. 瀏覽至「記錄檔 > 記錄檔維護」。
2. 選取「啟動記錄檔的預約刪除」。
3. 選取要刪除的記錄檔類型。根據預約時程刪除除偵錯記錄檔外的全部 OfficeScan 產生的記錄檔。對於偵錯記錄檔，請關閉偵錯記錄以停止收集記錄檔。

注意

對於病毒/惡意程式記錄檔，可以刪除某些掃瞄類型和損害清除及復原服務產生的記錄檔。對於間諜程式/可能的資安威脅程式記錄檔，可以刪除某些掃瞄類型產生的記錄檔。如需有關掃瞄類型的詳細資訊，請參閱掃瞄類型 第 7-12 頁。

4. 選取是刪除所有選定記錄檔類型的記錄檔，還是只刪除超過特定天數的記錄檔。
5. 指定記錄檔刪除頻率和時間。
6. 按一下「儲存」。

手動刪除記錄檔

程序

1. 瀏覽到「 記錄檔 > 用戶端電腦記錄檔 > 安全威脅」或「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 請執行下列其中一個步驟：
   - 如果要存取「用戶端電腦的安全威脅記錄檔」畫面，請按一下「刪除記錄檔」或「檢視記錄檔 > 刪除記錄檔」。
   - 如果要存取「用戶端管理」畫面，請按一下「記錄檔 > 刪除記錄檔」。
4. 選取要刪除的記錄檔類型。只能手動刪除以下記錄檔：
   - 病毒/惡意程式記錄檔
   - 間諜程式/可能的資安威脅程式記錄檔
   - 防火牆記錄檔
   - 網頁信譽評等記錄檔

- 周邊設備存取控管記錄檔
- 行為監控記錄檔
- Data Loss Prevention 記錄檔

注意

對於病毒/惡意程式記錄檔，可以刪除某些掃瞄類型和損害清除及復原服務產生的記錄檔。對於間諜程式/可能的資安威脅程式記錄檔，可以刪除某些掃瞄類型產生的記錄檔。如需有關掃瞄類型的詳細資訊，請參閱掃瞄類型 第 7-12 頁。

5. 選取是刪除所有選定記錄檔類型的記錄檔，還是只刪除超過特定天數的記錄檔。
6. 按一下「刪除」。

授權

在 Web 主控台檢視、啟動和續約 OfficeScan 使用授權服務，以及啟動/關閉 OfficeScan 防火牆。OfficeScan 防火牆是「防毒」服務的一部分，這項服務也包含對 Cisco NAC 和病毒爆發防範的支援。

注意

某些本機 OfficeScan 功能（例如資料安全防護和虛擬桌面支援）具有自己的使用授權。這些功能的使用授權會從 Plug-in Manager 進行啟動和管理。如需有關這些功能使用授權的詳細資訊，請參閱 資料安全防護使用授權 第 3-4 頁 和 虛擬桌面支援使用授權 第 14-67 頁。

純 IPv6 OfficeScan 伺服器無法連線到趨勢科技線上註冊伺服器來啟動/續約該使用授權。如果要允許 OfficeScan 伺服器連線到註冊伺服器，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。

在下列情況中，請先登出 Web 主控台，然後再重新登入：

- 啟動下列使用授權服務的使用授權之後：

- 防毒
- 網頁信譽評等和間諜程式防護

注意

必須重新登入，才能啟動服務的完整功能。

- 在啟動或關閉 OfficeScan 防火牆之後。如果關閉防火牆，OfficeScan 會隱藏伺服器和用戶端上的所有防火牆功能。

檢視產品使用授權資訊

程序

1. 瀏覽至「管理 > 產品使用授權」。
2. 檢視出現在畫面頂端的使用授權狀態摘要。出現下列情況時顯示有關使用授權的提醒：

   表 13-13. 授權提醒

授權類型	提醒
完整版	在產品的寬限期內。寬限期視地區而定。請向您的趨勢科技銷售人員確認寬限期。 使用授權到期且經過寬限期以後。在這期間，您無法取得技術支援或執行元件更新。掃瞄引擎仍會掃瞄電腦，但是會使用過期的元件。這些過期元件可能無法保護您不受最新的安全威脅侵襲。
試用版	使用授權到期時。在這期間，OfficeScan 會關閉元件更新、掃瞄和所有用戶端功能。

3. 檢視使用授權資訊。「授權資訊」區段提供您下列資訊：
   - 服務：包含所有 OfficeScan 使用授權服務
   - 狀態：顯示「已啟動」、「未啟動」或「已到期」。如果某個服務具有多個使用授權，而至少有一個使用授權仍為作用中，則會顯示的狀態為「已啟動」。

- 版本：顯示「完整版」或「試用版」。如果您同時擁有完整版和試用版，則會顯示的版本是「完整版」。
- 到期日：如果某個服務有多個授權，則會顯示最新的到期日。例如，如果使用授權到期日為 2007/12/31 和 2008/6/30，則會顯示 2008/6/30。

注意

未啟動的使用授權服務的版本和到期日會顯示為「無」。

4. OfficeScan 可讓您為一個使用授權服務啟動多個授權。請按一下服務名稱，以檢視該服務的所有授權（包含作用中和到期的授權）。

啟動或續約使用授權

程序

1. 瀏覽至「管理 > 產品使用授權」。
2. 按一下使用授權服務名稱。
3. 在開啟的「產品使用授權詳細資料」畫面中，按一下「新啟動碼」。
4. 在開啟的畫面中輸入「啟動碼」，然後按一下「儲存」。

注意

啟動服務之前請先將它註冊。如需有關「授權碼」和「啟動碼」的詳細資訊，請聯絡您的趨勢科技銷售人員。

5. 返回「產品使用授權詳細資料」畫面，按一下「更新資訊」重新整理該畫面，以便顯示新使用授權詳細資料和服務狀態。這個畫面也提供趨勢科技網站連結，按一下此連結即可檢視關於您的使用授權的詳細資訊。

OfficeScan 資料庫備份

OfficeScan 伺服器資料庫包含所有 OfficeScan 設定，包括掃瞄設定和權限。如果您有備份，就可以在伺服器資料庫損毀時恢復。您可以隨時手動備份資料庫，或設定備份預約時程。

備份資料庫時，OfficeScan 會自動協助重組資料庫並修復任何可能的索引檔損毀。

檢查系統事件記錄檔以判斷備份狀態。如需詳細資訊，請參閱系統事件記錄檔 第 13-30 頁。

秘訣

趨勢科技建議您設定自動備份預約時程。在非尖峰時刻伺服器傳輸量低時備份資料庫。

警告!

請勿使用任何其他工具或軟體執行備份。務必僅從 OfficeScan Web 主控台設定資料庫備份。

備份 OfficeScan 資料庫

程序

1. 瀏覽至「管理 > 資料庫備份」。
2. 輸入您要儲存資料庫的位置。如果資料夾尚不存在，請選取「如果沒有資料夾，請建立資料夾」。包括磁碟機和完整目錄路徑（例如：`C:\OfficeScan\DatabaseBackup`）。

   依預設，OfficeScan 會將備份儲存在下列目錄中：<伺服器安裝資料夾>`\DBBackup`

注意

OfficeScan 會在備份路徑下建立子資料夾。資料夾名稱表示備份的時間，且其格式如下：YYYYMMDD_HHMMSS。OfficeScan 會保留最新的 7 個備份資料夾，並且自動刪除較舊的資料夾。

3. 如果備份路徑位於遠端電腦上（使用 UNC 路徑），請輸入適當的帳號名稱和對應的密碼。確定帳號擁有電腦的寫入權限。
4. 如果要設定預約備份：
   a. 選取「啟動預約的資料庫備份」。
   b. 指定備份頻率和時間。
   c. 如果要備份資料庫並儲存您所做的變更，請按一下「立即備份」。如果只要儲存而不要備份資料庫，請按一下「儲存」。

恢復資料庫備份檔案

程序

1. 停止「OfficeScan 主服務」。
2. 使用備份檔案覆寫 <伺服器安裝資料夾>\PCCSRV\HTTPDB 中的資料庫檔案。
3. 重新啟動「OfficeScan 主服務」。

OfficeScan Web 伺服器資訊

在 OfficeScan 伺服器安裝期間，安裝程式會自動設定 Web 伺服器（IIS 或 Apache Web Server），讓用戶端電腦連線至 OfficeScan 伺服器。設定用戶端電腦用戶端要連線的 Web 伺服器。

如果從外部修改了 Web 伺服器設定（例如，從 IIS 管理主控台），則請複製 OfficeScan 中的變更。例如，如果您手動變更用戶端電腦的伺服器 IP 位址，或是為伺服器指定動態 IP 位址，則需重新設定 OfficeScan 的伺服器設定。

警告!

變更連線設定可能導致永久中斷伺服器和用戶端之間的連線，且可能需要重新部署 OfficeScan 用戶端。

設定連線設定

程序

1. 瀏覽至「管理 > 連線設定」。
2. 輸入 Web 伺服器的網域名稱或 IPv4/IPv6 位址和通訊埠號碼。

   注意

   通訊埠號碼是信任的通訊埠，為 OfficeScan 伺服器與 OfficeScan 用戶端通訊時所使用。

3. 按一下「儲存」。

Web 主控台密碼

只有當伺服器電腦沒有使用以角色為基礎的管理所需的資源時，才能存取用於管理 Web 主控台密碼（或是安裝 OfficeScan 伺服器時建立的 root 帳號密碼）的畫面。例如，如果伺服器電腦執行 Windows 2003，而且未安裝「授權管理員運行庫」(Authorization Manager Runtime)，則可以存取此畫面。如果有足夠的資源，就不會顯示此畫面，而且可以透過「使用者帳號」畫面修改 root 帳號來管理密碼。

如果 OfficeScan 未向 Control Manager 註冊，請聯絡您的經銷商，以獲得如何取得 Web 主控台存取權的指示。

Web 主控台設定

使用「Web 主控台設定」畫面來執行下列工作：

- 設定 OfficeScan 伺服器定期重新整理「摘要」管理平台。依預設，伺服器會每隔 30 秒重新整理管理平台。秒數可以是 10 到 300 的值。
- 指定 Web 主控台逾時設定。依預設，使用者會在 30 分鐘未執行任何活動之後，自動登出 Web 主控台。分鐘數可以是 10 到 60 的值。

設定 Web 主控台設定值

程序

1. 瀏覽至「管理 > Web 主控台設定」。
2. 選取「啟動自動重新整理」，然後選取重新整理間隔。
3. 選取「啟動自動登出 Web 主控台」，然後選取逾時間隔。
4. 按一下「儲存」。

隔離區管理員

每當 OfficeScan 用戶端偵測到安全威脅且中毒處理行動為隔離時，便會加密中毒檔案，再將其移至 <用戶端安裝資料夾>\SUSPECT 中的本機隔離資料夾。

將檔案移到本機隔離目錄之後，OfficeScan 用戶端會將它傳送到指定的隔離目錄。在「用戶端電腦 > 用戶端管理 > 設定 > {掃瞄類型} 設定 > 處理行動」標籤指定此目錄。用戶端會加密指定隔離目錄中的檔案，避免感染其他檔案。如需詳細資訊，請參閱隔離目錄 第 7-37 頁。

如果指定的隔離目錄位於 OfficeScan 伺服器電腦上，請從 Web 主控台修改伺服器的隔離目錄設定。伺服器會將隔離的檔案儲存在 <伺服器安裝資料夾>\PCCSRV\Virus 中。

注意

如果 OfficeScan 用戶端因任何原因（例如：網路連線問題）而無法將加密的檔案傳送至 OfficeScan 伺服器，則加密的檔案會留在 OfficeScan 用戶端隔離資料夾中。OfficeScan 用戶端將在連線到 OfficeScan 伺服器時嘗試再次傳送檔案。

設定隔離目錄的設定

程序

1. 瀏覽至「管理 > 隔離區管理員」。
2. 接受或修改隔離資料夾的預設容量，以及 OfficeScan 能夠在隔離資料夾中儲存的中毒檔案大小上限。

   預設值會顯示在畫面中。
3. 按一下「儲存隔離設定」。
4. 如果要移除隔離資料夾中所有現有的檔案，請按一下「刪除所有隔離檔案」。

Server Tuner

使用 Server Tuner 即可將參數用於下列伺服器相關效能問題，以將 OfficeScan 伺服器的效能最佳化：

- 下載

  當向 OfficeScan 伺服器要求更新的 OfficeScan 用戶端數目（包括更新代理程式）超出伺服器的可用資源時，伺服器便會將用戶端更新要求移到佇列中，並在資源可用時處理要求。用戶端成功從 OfficeScan 伺服器更新元件

後，便會通知伺服器已完成更新。設定 OfficeScan 伺服器從用戶端接收更新通知之前等待的分鐘數上限。也請設定伺服器嘗試通知用戶端執行更新並套用新組態設定的次數上限。伺服器如果沒有收到用戶端通知就會繼續嘗試。

- Buffer

  當 OfficeScan 收到來自 OfficeScan 用戶端的多個要求（例如：執行更新的要求）時，伺服器就會盡量處理要求，並將剩餘要求放入緩衝區中。接著，伺服器會在有資源可用時逐一處理儲存在緩衝區中的要求。請指定事件（例如：用戶端更新要求和用戶端記錄檔報告要求）的緩衝區大小。

- 網路傳輸

  網路傳輸量在一天之中會有所不同。如果要控制到 OfficeScan 伺服器和其他更新來源的網路傳輸流量，請指定在一天之中的特定時間可以同時更新的 OfficeScan 用戶端數目。

Server Tuner 需要下列檔案：`SvrTune.exe`

執行 Server Tuner

程序

1. 在 OfficeScan 伺服器電腦上，瀏覽至 <伺服器安裝資料夾>`\PCCSRV\Admin\Utility\SvrTune`。
2. 按兩下 `SvrTune.exe` 啟動 Server Tuner。

   隨即開啟 Server Tuner 主控台。
3. 修改「下載」下方的下列設定：

   - 用戶端逾時：輸入 OfficeScan 伺服器從用戶端接收更新回應之前等待的分鐘數上限。如果用戶端未能在此時間內回應，OfficeScan 伺服器就會認為用戶端沒有最新的元件。當收到通知的用戶端逾時，就會開放位置給等待通知的其他用戶端。

- 更新代理程式逾時：輸入 OfficeScan 伺服器從「更新代理程式」接收更新回應之前等待的分鐘數上限。當收到通知的用戶端逾時，就會開放位置給等待通知的其他用戶端。
- 重試總數：輸入 OfficeScan 伺服器嘗試通知用戶端執行更新或套用新組態設定的次數上限。
- 重試間隔：輸入 OfficeScan 在通知嘗試間等待的分鐘數。

4. 修改「緩衝區」下方的下列設定：
   - 事件緩衝區：輸入 OfficeScan 在緩衝區中持有，而且要回報給伺服器的用戶端事件（例如：更新元件）數目上限。當用戶端要求在緩衝區中等候時，與用戶端的連線便會中斷。當 OfficeScan 處理用戶端報告並將其從緩衝區中移除時，便會建立與用戶端的連線。
   - 記錄檔緩衝區：輸入 OfficeScan 在緩衝區中持有，而且要回報給伺服器的用戶端記錄檔資訊數目上限。當用戶端要求在緩衝區中等候時，與用戶端的連線便會中斷。當 OfficeScan 處理用戶端報告並將其從緩衝區中移除時，便會建立與用戶端的連線。

   注意

   如果向伺服器回報的用戶端數目過多，請增加緩衝區的大小。不過，緩衝區大小越大，也表示會利用更多的伺服器記憶體。

5. 修改「網路傳輸」下的下列設定：
   - 一般時間：按一下代表一天之中您認為網路傳輸正常的時間的圓形按鈕。
   - 離峰時間：按一下代表一天之中您認為網路傳輸最低的時間的圓形按鈕。
   - 尖峰時間：按一下代表一天之中您認為網路傳輸最高的時間的圓形按鈕。
   - 用戶端連線上限：輸入可從「其他更新來源」和 OfficeScan 伺服器同時更新元件的用戶端數目上限。請為各個時段輸入用戶端數目上限。當達到連線數目上限時，用戶端必須等到目前的用戶端連線關閉（因為更新完成或是用戶端回應達到您在「用戶端逾時」或「更新代理程式逾時」欄位中指定的逾時值）後才能更新元件。

6. 按一下「確定」。隨即出現提示詢問您是否要重新啟動「OfficeScan 主服務」。

注意

會重新啟動服務，但不會重新啟動電腦。

7. 請選取下列重新啟動選項：

   - 按一下「是」儲存 Server Tuner 設定並重新啟動服務。設定會在重新啟動之後立即生效。
   - 按一下「否」則會儲存 Server Tuner 設定，但不會重新啟動服務。請重新啟動「OfficeScan 主服務」或重新啟動 OfficeScan 伺服器電腦，以讓設定生效。

Smart Feedback

Trend Micro Smart Feedback 會以匿名方式將安全威脅資訊與主動式雲端截毒技術共享，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

程序

1. 瀏覽至「主動式雲端截毒技術 > Smart Feedbac」。
2. 按一下「啟動 Trend Micro 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. 如果要傳送關於您用戶端電腦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 OfficeScan 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. 按一下「儲存」。

第 14 章

管理 OfficeScan 用戶端

本章說明 OfficeScan 用戶端管理和組態設定。

本章內容：

電腦位置

OfficeScan 提供位置偵測功能，可判斷 OfficeScan 用戶端位置是內部或外部。下列 OfficeScan 功能和服務使用位置偵測：

表 14-1. 使用位置偵測的功能和服務

功能/服務	說明
網頁信譽評等服務	OfficeScan 用戶端的位置決定 OfficeScan 用戶端將套用的網頁信譽評等策略。管理員通常會針對外部用戶端實施較嚴格的策略。 如需有關網頁信譽評等策略的詳細資訊，請參閱網頁信譽評等策略 第 11-3 頁。
檔案信譽評等服務	對於使用雲端截毒掃瞄的用戶端，OfficeScan 用戶端位置會決定用戶端傳送掃瞄查詢的主動式雲端截毒伺服器來源。 外部用戶端會將掃瞄查詢傳送到「主動式雲端截毒技術」，而內部用戶端會將查詢傳送到主動式雲端截毒伺服器來源清單中定義的來源。 如需有關主動式雲端截毒伺服器來源的詳細資訊，請參閱主動式雲端截毒伺服器來源 第 4-5 頁。
Data Loss Prevention	OfficeScan 用戶端的位置決定用戶端將套用的 Data Loss Prevention 策略。管理員通常會針對外部用戶端實施較嚴格的策略。 如需有關 Data Loss Prevention 策略的詳細資訊，請參閱 Data Loss Prevention 策略 第 10-3 頁.
周邊設備存取控管	OfficeScan 用戶端的位置決定用戶端將套用的「周邊設備存取控管」策略。管理員通常會針對外部用戶端實施較嚴格的策略。 如需有關「周邊設備存取控管」策略的詳細資訊，請參閱周邊設備存取控管 第 9-2 頁。

位置條件

指定位置是以 OfficeScan 用戶端電腦的閘道 IP 位址為準，還是以 OfficeScan 用戶端與 OfficeScan 伺服器或任何參考伺服器的連線狀態為準。

- 閘道 IP 和 MAC 位址：如果 OfficeScan 用戶端電腦的閘道 IP 位址符合您在「電腦位置」畫面指定的任一閘道 IP 位址，則該電腦的位置為「內部」。否則，電腦的位置就是「外部」。
- 用戶端連線狀態：如果 OfficeScan 用戶端可以連線至 OfficeScan 伺服器或 Intranet 上任何指定的參考伺服器，電腦位置就是「內部」。此外，如果企業網路外部的電腦可以與 OfficeScan 伺服器/參考伺服器建立連線，則該電腦的位置也是「內部」。如果上述條件都不符合，則電腦的位置就是外部。

設定位置設定

程序

1. 瀏覽至「用戶端電腦 > 電腦位置」。
2. 選擇位置是以「用戶端連線狀態」還是以「閘道 IP 與 MAC 位址」為準。
3. 如果選擇「用戶端連線狀態」，請決定是否要使用參考伺服器。

   如需詳細資訊，請參閱參考伺服器 第 13-26 頁。

   a. 如果您沒有指定參考伺服器，當發生下列事件時，OfficeScan 用戶端會檢查 OfficeScan 伺服器的連線狀態：

      - OfficeScan 用戶端從行動模式切換到一般（線上/離線）模式。
      - OfficeScan 用戶端從一種掃瞄方法切換到另一種掃瞄方法。如需詳細資訊，請參閱掃瞄方法 第 7-6 頁。
      - OfficeScan 用戶端偵測到電腦中的 IP 位址變更。
      - OfficeScan 用戶端重新啟動。
      - 伺服器開始連線驗證。如需詳細資訊，請參閱 OfficeScan 用戶端圖示 第 14-23 頁。
      - 網頁信譽評等位置條件在套用全域設定時變更。
      - 病毒爆發防範策略已經不再執行，而且已經恢復病毒爆發前的設定。

b. 如果您已經指定參考伺服器，則 OfficeScan 用戶端會先檢查 OfficeScan 伺服器的連線狀態，如果無法連線至 OfficeScan 伺服器，再檢查參考伺服器的連線狀態。OfficeScan 用戶端會在每個小時以及發生上述事件時檢查連線狀態。

4. 如果選擇「閘道 IP 與 MAC 位址」：

   a. 在提供的文字方塊中輸入閘道 IPv4/IPv6 位址。

   b. 輸入 MAC 位址。

   c. 按一下「新增」。

      如果您不是輸入 MAC 位址，OfficeScan 會包含所有屬於特定 IP 位址的 MAC 位址。

   d. 重覆步驟 a 到步驟 c，直到完成所有要新增的閘道 IP 位址。

   e. 使用「閘道設定匯入程式」工具匯入閘道設定清單。

      如需詳細資訊，請參閱閘道設定匯入程式 第 14-4 頁。

5. 按一下「儲存」。

閘道設定匯入程式

OfficeScan 會檢查電腦的位置以決定要使用的網頁信譽評等策略，以及要連線的主動式雲端截毒伺服器來源。OfficeScan 識別位置的其中一個方式，就是檢查電腦的閘道 IP 位址與 MAC 位址。

您可以在「電腦位置」畫面設定閘道設定，或使用「閘道設定匯入程式」工具將閘道設定清單匯入至「電腦位置」畫面。

使用閘道設定匯入程式

程序

1. 準備含有閘道設定清單的文字檔 (`.txt`)。在每一行中輸入 IPv4 或 IPv6 位址並選擇性地輸入 MAC 位址。

請以逗號分隔 IP 位址與 MAC 位址。項目的最大數值為 4096。

例如：

```
10.1.111.222,00:17:31:06:e6:e7

2001:0db7:85a3:0000:0000:8a2e:0370:7334

10.1.111.224,00:17:31:06:e6:e7
```

2. 在伺服器電腦上，移至<伺服器安裝資料夾>\PCCSRV\Admin\Utility\GatewaySettingsImporter，然後按兩下 GSImporter.exe。

注意

您無法從「終端機服務」執行「閘道設定匯入程式」工具。

---

3. 在「閘道設定匯入程式」畫面上，瀏覽至步驟 1 中所建立的檔案，然後按一下「匯入」。
4. 按一下「確定」。

   閘道設定會顯示在「電腦位置」畫面上，而且 OfficeScan 伺服器會將這些設定部署至 OfficeScan 用戶端。
5. 如果要刪除所有項目，請按一下「全部清除」。

   如果只需要刪除特定項目，請將它從「電腦位置」畫面移除。
6. 如果要將設定匯出至檔案，請按一下「全部匯出」，然後指定檔案名稱與類型。

OfficeScan 用戶端程式管理

下列主題討論管理和保護 OfficeScan 用戶端程式的方式：

- OfficeScan 用戶端服務 第 14-6 頁
- OfficeScan 用戶端服務重新啟動 第 14-10 頁
- 本機自我保護 第 14-11 頁

OfficeScan 用戶端服務

OfficeScan 用戶端會執行下列表格中所列的服務。您可以從 Microsoft 管理主控台檢視這些服務的狀態。

表 14-2. OfficeScan 用戶端服務

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 • OfficeScan 本機自我保護 注意 OfficeScan 本機自我保護可防止 OfficeScan 用戶端於服務啟動及執行時意外終止。
OfficeScan NT 防火牆 (TmPfw.exe)	OfficeScan 防火牆
OfficeScan 資料安全防護服務 (dsagent.exe)	• Data Loss Prevention • 周邊設備存取控管
OfficeScan NT 監聽程式 (tmlisten.exe)	OfficeScan 用戶端與 OfficeScan 伺服器間的通訊

服務	受控制的功能
OfficeScan NT Proxy 服務 (TmProxy.exe)	• 網頁信譽評等 • POP3 郵件掃瞄
OfficeScan NT 即時掃瞄 (ntrtscan.exe)	• 即時掃瞄 • 預約掃瞄 • 手動掃瞄/立即掃瞄

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)
- OfficeScan NT 防火牆 (TmPfw.exe)
- OfficeScan 資料安全防護服務 (dsagent.exe)

因此，在伺服器平台（Windows Server 2003、Windows Server 2008 和 Windows Server 2012）上，預設會關閉這些服務。如果要啟動這些服務：

- 持續監控系統效能，並在發現效能變差時採取必要的處理行動。
- 對於 TMBMSRV.exe，如果您將耗用大量系統資源的應用程式從「行為監控」策略排除，則可以啟動該服務。您可以使用效能調整工具來識別耗用大量系統資源的應用程式。如需詳細資訊，請參閱使用趨勢科技效能調整工具 第 14-9 頁。

對於桌上型電腦平台，只有在發現效能嚴重變差時才需要關閉那些服務。

從 Web 主控台啟動或關閉用戶端服務

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 對於執行 Windows XP、Vista、7 或 8 的 OfficeScan 用戶端：
   a. 在用戶端樹狀結構中，按一下根網域圖示（）以包含所有的用戶端，或選取特定網域或用戶端。

注意

當您選取根網域或特定網域時，設定只會套用到執行 Windows XP、Vista、7 或 8 的用戶端。設定不會套用到任何執行 Windows Server 平台的用戶端（即使它們是網域的一部分）。

b. 按一下「設定 > 其他服務設定」。

c. 選取或清除下列區段中的核取方塊：

- 未經授權的變更阻止服務
- 防火牆服務
- 資料安全防護服務

d. 按一下「儲存」將設定套用至網域。如果選取根網域圖示，請從下列選項中選擇：

- 套用至所有用戶端：將設定套用至所有現有的 Windows XP/Vista/7/8 用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
- 僅套用於未來網域：僅將設定套用至加入未來網域中的 Windows XP/Vista/7/8 用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

3. 對於執行 Windows Server 2003，Windows Server 2008 或 Windows Server 2012 的 OfficeScan 用戶端：

a. 選取用戶端樹狀結構中的用戶端。

b. 按一下「設定 > 其他服務設定」。

c. 選取或清除下列區段中的核取方塊：

- 未經授權的變更阻止服務
- 防火牆服務
- 資料安全防護服務

d. 按一下「儲存」。

使用趨勢科技效能調整工具

程序

1. 從下列位置下載「趨勢科技效能調整工具」：

   http://esupport.trendmicro.com/solution/zh-tw/1074941.aspx

2. 將 `TMPerfTool.exe` 從 `TMPerfTool.zip` 中解壓縮出來。

3. 將 `TMPerfTool.exe` 放在 <用戶端安裝資料夾> 中或 `TMBMCLI.dll` 所在的同一資料夾中。

4. 以滑鼠右鍵按一下 `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，然後按一下「確定」。

6. 按一下「分析」。

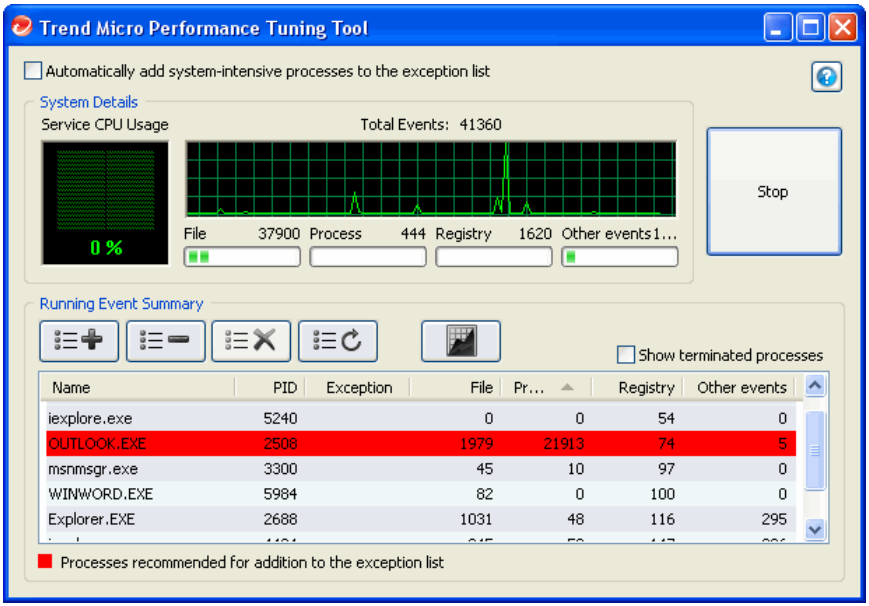


圖 14-1. 系統會反白顯示耗用大量系統資源的處理程序

此工具會開始監控 CPU 使用狀況與事件負載。系統會以紅色反白顯示耗用大量系統資源的處理程序。

7. 選取耗用大量系統資源的處理程序，然後按一下「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. 按一下「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，請參閱行為監控例外清單 第 8-5 頁。

OfficeScan 用戶端服務重新啟動

OfficeScan 會重新啟動意外停止回應的 OfficeScan 用戶端服務，以及不是由正常系統程序停止的用戶端服務。如需有關用戶端服務的詳細資訊，請參閱OfficeScan 用戶端服務 第 14-6 頁。

設定必要設定讓 OfficeScan 用戶端服務重新啟動。

設定服務重新啟動設定

程序

1. 瀏覽至「用戶端電腦 > 全域用戶端設定」。

2. 移至「OfficeScan 服務重新啟動」區段。
3. 選取「如果服務意外終止，則自動重新啟動 OfficeScan 用戶端服務」。
4. 設定下列項目：
   - 在 __ 分鐘之後重新啟動服務：指定 OfficeScan 重新啟動服務之前的等候時間（以分鐘為單位）。
   - 如果第一次嘗試重新啟動服務失敗，請重試 __ 次：指定嘗試重新啟動服務的重試次數上限。如果經過指定的重試次數上限之後服務仍為停止狀態，請手動重新啟動服務。
   - 在 __ 小時之後重設重新啟動失敗計數：如果嘗試重試的次數已達到上限後服務仍為停止狀態，OfficeScan 會等候特定的小時數，然後重設失敗計數。如果服務在經過指定的時數之後仍為停止狀態，則 OfficeScan 會重新啟動服務。

本機自我保護

使用 OfficeScan 本機自我保護，OfficeScan 用戶端便可保護正常運作所需的程序和其他資源。OfficeScan 本機自我保護可協助防止程式或實際的使用者關閉惡意程式防護功能。

OfficeScan 本機自我保護可提供下列選項：

- 保護 OfficeScan 用戶端服務 第 14-12 頁
- 保護 OfficeScan 用戶端安裝資料夾中的檔案 第 14-13 頁
- 保護 OfficeScan 用戶端登錄機碼 第 14-14 頁
- 保護 OfficeScan 用戶端程序 第 14-14 頁

設定 OfficeScan 本機自我保護設定

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。

2. 在用戶端樹狀結構中，按一下根網域圖示 () 或選取特定的網域或用戶端。
3. 按一下「設定 > 權限和其他設定」。
4. 按一下「其他設定」標籤，然後移至「本機自我保護」區段。
5. 啟動下列選項：
   - 保護 OfficeScan 用戶端服務 第 14-12 頁
   - 保護 OfficeScan 用戶端安裝資料夾中的檔案 第 14-13 頁
   - 保護 OfficeScan 用戶端登錄機碼 第 14-14 頁
   - 保護 OfficeScan 用戶端程序 第 14-14 頁

   
   注意
   在 Windows 伺服器平台上，預設會關閉登錄機碼和處理程序的安全防護。
6. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

保護 OfficeScan 用戶端服務

OfficeScan 會封鎖所有嘗試終止下列 OfficeScan 用戶端服務的動作：

- OfficeScan NT 監聽程式 (`TmListen.exe`)
- OfficeScan NT 即時掃瞄 (`NTRtScan.exe`)
- OfficeScan NT Proxy 服務 (`TmProxy.exe`)

- OfficeScan NT 防火牆 (`TmPfw.exe`)
- OfficeScan 資料安全防護服務 (`dsagent.exe`)
- 趨勢科技未經授權的變更阻止服務 (`TMBMSRV.exe`)

注意

如果啟動此選項，OfficeScan 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。

保護 OfficeScan 用戶端安裝資料夾中的檔案

為防止其他程式或使用者修改或刪除 OfficeScan 用戶端檔案，OfficeScan 會鎖定根目錄<用戶端安裝資料夾>中的下列檔案：

- 所有已經過數位簽署且副檔名為 `.exe`、`.dll` 和 `.sys` 的檔案
- 某些不具備數位簽章的檔案，包括：
  - `bspatch.exe`
  - `bzip2.exe`
  - `INETWH32.dll`
  - `libcurl.dll`
  - `libeay32.dll`
  - `libMsgUtilExt.mt.dll`
  - `msvcm80.dll`
  - `MSVCP60.DLL`
  - `msvcp80.dll`
  - `msvcr80.dll`
  - `OfceSCV.dll`

- OFCESCVPack.exe
- patchbld.dll
- patchw32.dll
- patchw64.dll
- PiReg.exe
- ssleay32.dll
- Tmeng.dll
- TMNotify.dll
- zlibwapi.dll

保護 OfficeScan 用戶端登錄機碼

OfficeScan 會封鎖所有嘗試在下列登錄機碼和子機碼修改、刪除或新增項目的動作：

- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TMCSS

保護 OfficeScan 用戶端程序

OfficeScan 會封鎖所有嘗試終止下列程序的動作：

- TmListen.exe:接收來自 OfficeScan 伺服器的指令與通知，並促進 OfficeScan 用戶端與伺服器之間的通訊。
- NTRtScan.exe:在 OfficeScan 用戶端執行即時、預約與手動掃瞄
- TmProxy.exe:先掃瞄網路流量，然後將網路流量傳遞至目標應用程式
- TmPfw.exe:提供封包層級防火牆、網路病毒掃瞄和入侵偵測功能

- 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
- DSAgent.exe:監控機密資料的傳輸並控制對裝置的存取權

OfficeScan 用戶端安全

透過從兩個安全設定中選取想要的選項，控制使用者對 OfficeScan 用戶端安裝目錄和登錄設定的存取權。

控制對 OfficeScan 用戶端安裝目錄和登錄機碼的存取權

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 或選取特定的網域或用戶端。
3. 按一下「設定 > 權限和其他設定」。
4. 按一下「其他設定」標籤，然後移至「用戶端安全設定」區段。
5. 從下列存取權限選取想要的設定：
   - 高：OfficeScan 用戶端安裝目錄會繼承 Program Files 資料夾的權限，而 OfficeScan 用戶端的登錄項目會繼承 HKLM\軟體 機碼的權限。針對大部分的 Active Directory 設定，這會自動將「一般」使用者（不具有管理員權限的使用者）的權限限制成唯讀。
   - 一般：此權限會將 OfficeScan 用戶端程式目錄與 OfficeScan 用戶端登錄項目的完整權限授與所有使用者（使用者群組 "Everyone"）。
6. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

- 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
- 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

OfficeScan 用戶端主控台存取限制

此設定可關閉從系統匣或 Windows「開始」功能表存取 OfficeScan 用戶端主控台的功能。使用者存取 OfficeScan 用戶端主控台的唯一方式是按一下 <用戶端安裝資料夾> 中的 `PccNT.exe`。設定此設定後，請重新載入 OfficeScan 用戶端讓設定生效。

此設定不會關閉 OfficeScan 用戶端。OfficeScan 用戶端會在背景中執行並持續提供安全威脅防護。

限制對 OfficeScan 用戶端主控台的存取

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 或選取特定的網域或用戶端。
3. 按一下「設定 > 權限和其他設定」。
4. 按一下「其他設定」標籤，然後移至「用戶端主控台存取限制」區段。
5. 選取「不允許使用者從系統匣或 Windows「開始」功能表存取用戶端主控台」。
6. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

- 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
- 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

OfficeScan 用戶端卸載

OfficeScan 用戶端卸載權限可讓使用者暫時停止 OfficeScan 用戶端，而且您可以指定暫時停止 OfficeScan 用戶端時是否需要密碼。

授與用戶端卸載權限

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 或選取特定網域或用戶端。
3. 按一下「設定 > 權限和其他設定」。
4. 在「權限」標籤上，移至「卸載」區段。
5. 如果要允許不需密碼就可卸載用戶端，請選取「允許使用者卸載 OfficeScan 用戶端」。
   - 如果要求必須輸入密碼，請選取「使用者需要密碼才能卸載 OfficeScan 用戶端」，然後輸入密碼並確認。
6. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。

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

OfficeScan 用戶端行動權限

如果用戶端與伺服器之間的事件干擾使用者的工作，您可以將 OfficeScan 用戶端行動權限授與特定使用者。例如，經常做簡報的使用者可以在開始簡報之前先啟動行動模式，以防止 OfficeScan 伺服器在該 OfficeScan 用戶端上部署 OfficeScan 用戶端設定和開始執行掃瞄。

當用戶端處於行動模式時：

- OfficeScan 用戶端不會傳送記錄檔到 OfficeScan 伺服器，即使伺服器與用戶端間有正常運作的連線也一樣。
- OfficeScan 伺服器不會在用戶端上開始執行工作，也不會將 OfficeScan 用戶端設定部署到用戶端，即使伺服器與用戶端間有正常運作的連線也一樣。
- 如果用戶端可以連線到其任何更新來源，OfficeScan 用戶端會更新元件。來源包含 OfficeScan 伺服器、更新代理程式或自訂更新來源。

  下列事件會觸發行動用戶端上的更新：

  - 使用者執行手動更新時。
  - 自動用戶端更新執行時。您可以關閉行動用戶端上的自動用戶端更新。如需詳細資訊，請參閱在行動用戶端關閉自動用戶端更新 第 14-19 頁。
  - 預約更新執行時。只有具有必要權限的用戶端可以執行預約更新。您可以隨時撤銷此權限。如需詳細資訊，請參閱在行動 OfficeScan 用戶端撤銷預約更新權限 第 14-20 頁。

授與用戶端行動權限

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 或選取特定網域或用戶端。
3. 按一下「設定 > 權限和其他設定」。
4. 在「權限」標籤上，移至「行動權限」區段。
5. 選取「啟動行動模式」。
6. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

在行動用戶端關閉自動用戶端更新

程序

1. 瀏覽至「更新 > 用戶端電腦 > 自動更新」。
2. 移至「事件觸發更新」區段。
3. 關閉「包括行動和離線用戶端」。

注意

如果關閉「在 OfficeScan 伺服器下載新元件之後，立即在用戶端開始元件更新」，系統會自動關閉此選項。

4. 按一下「儲存」。

在行動 OfficeScan 用戶端撤銷預約更新權限

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 或選取特定網域或用戶端。
3. 按一下「設定 > 權限和其他設定」。
4. 在「權限」標籤上，移至「元件更新權限」區段。
5. 清除「啟動預約更新」選項。
6. 按一下「儲存」。

Client Mover

如果網路上有多部 OfficeScan 伺服器，您可以使用 Client Mover 工具將 OfficeScan 用戶端從某一部 OfficeScan 伺服器轉移到另一部。將新的 OfficeScan 伺服器新增至網路之後，當您要將現有的 OfficeScan 用戶端轉移至新的伺服器時，這個工具會特別有用。

注意

兩部伺服器必須為相同語言的版本。如果您使用 Client Mover 將舊版 OfficeScan 用戶端移到最新版本的伺服器，則 OfficeScan 用戶端會自動升級。

使用此工具之前，請先確定您使用的帳號具有管理員權限。

執行 Client Mover

程序

1. 在 OfficeScan 伺服器上，移至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\IpXfer。
2. 將 IpXfer.exe 複製到 OfficeScan 用戶端電腦。如果 OfficeScan 用戶端電腦執行的是 x64 類型平台，請改為複製 IpXfer_x64.exe。
3. 在 OfficeScan 用戶端電腦上，開啟命令提示字元，然後瀏覽到放置複製的可執行檔案的資料夾。
4. 使用下列語法執行 Client Mover：

   <可執行檔檔案名稱> -s <伺服器名稱> -p <伺服器監聽通訊埠> -c <用戶端監聽通訊埠> -d <網域或網域階層>

   表 14-3. Client Mover 參數

參數	說明
<可執行檔檔案名稱>	IpXfer.exe 或 IpXfer_x64.exe
<伺服器名稱>	目標 OfficeScan 伺服器（OfficeScan 用戶端轉移後所在的伺服器）的名稱
<伺服器監聽通訊埠>	目標 OfficeScan 伺服器的監聽通訊埠（或信任的通訊埠）。如果要在 OfficeScan Web 主控台上檢視監聽通訊埠，請按一下主功能表中的「管理 > 連線設定」。
<用戶端監聽通訊埠>	OfficeScan 用戶端電腦用來與伺服器通訊的通訊埠號碼
<網域或網域階層>	用戶端將在其中分組的用戶端樹狀結構網域或子網域。網域階層應該指出子網域。

   範例：

```
ipXfer.exe -s Server01 -p 8080 -c 21112 -d Workgroup

ipXfer_x64.exe -s Server02 -p 8080 -c 21112 -d Workgroup
\Group01
```

5. 如果要確認 OfficeScan 用戶端現在是否從屬於另一部伺服器，請執行下列操作：

   a. 在 OfficeScan 用戶端電腦上，以滑鼠右鍵按一下系統匣中的 OfficeScan 用戶端程式圖示。

   b. 選取「OfficeScan 主控台」。

   c. 按一下功能表中的「說明」，然後選取「關於」。

   d. 在「伺服器名稱/通訊埠」欄位中，檢查 OfficeScan 用戶端要報告的 OfficeScan 伺服器。

   注意

   如果 OfficeScan 用戶端未出現在管理它的新 OfficeScan 伺服器的用戶端樹狀結構中，請重新啟動新伺服器的主服務 (`ofservice.exe`)。

離線 OfficeScan 用戶端

當您使用 OfficeScan 用戶端解除安裝程式移除電腦中的 OfficeScan 用戶端程式時，程式會自動通知伺服器。當伺服器收到此通知時，便會移除 OfficeScan 用戶端樹狀結構中的用戶端圖示，表示該用戶端已不存在。

不過，如果您使用其他方法移除 OfficeScan 用戶端（例如：重新格式化電腦硬碟或手動刪除 OfficeScan 用戶端檔案），OfficeScan 就無法得知 OfficeScan 用戶端已被移除，而會將 OfficeScan 用戶端顯示為離線。如果使用者長期卸載或關閉 OfficeScan 用戶端，伺服器也會將該 OfficeScan 用戶端顯示為離線。

如果要讓用戶端樹狀結構只顯示連線的用戶端，請設定讓 OfficeScan 自動從用戶端樹狀結構中移除離線用戶端。

自動移除離線用戶端

程序

1. 瀏覽至「管理 > 離線用戶端」。

2. 選取「啟動自動移除離線用戶端」。
3. 選取「在離線 __ 天後自動移除 OfficeScan 用戶端」。
4. 按一下「儲存」。

用戶端和伺服器間的連線

OfficeScan 用戶端必須持續維持與其上層伺服器之間的連線，才能及時更新元件、接收通知，以及套用組態變更。下列主題討論如何檢查 OfficeScan 用戶端的連線狀態和解決連線問題：

- 用戶端 IP 位址 第 5-8 頁
- OfficeScan 用戶端圖示 第 14-23 頁
- 驗證用戶端和伺服器間的連線 第 14-36 頁
- 連線驗證記錄檔 第 14-37 頁
- 無法連線到用戶端 第 14-38 頁

OfficeScan 用戶端圖示

系統匣中的 OfficeScan 用戶端圖示會提供視覺提示，指出 OfficeScan 用戶端目前的狀態，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 14-4. 如 OfficeScan 用戶端圖示中指出的 OfficeScan 用戶端狀態

用戶端狀態	說明	視覺提示
用戶端與 OfficeScan 伺服器之間的連線	線上用戶端已連線到 OfficeScan 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 OfficeScan 伺服器之間的連線。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。 用戶端即使已連線到網路，也可以變成離線狀態。如需此問題的詳細資訊，請參閱：OfficeScan 用戶端已連線到網路，但顯示為離線 第 14-34 頁。
	行動用戶端不一定能夠與 OfficeScan 伺服器彼此通訊。	圖示包含桌面與訊號符號。  背景顏色是藍色或紅色的陰影，視即時掃瞄服務的狀態而定。 如需有關行動用戶端的詳細資訊，請參閱OfficeScan 用戶端行動權限 第 14-18 頁。

用戶端狀態	說明	視覺提示
主動式雲端截毒伺服器來源的可用性	主動式雲端截毒技術伺服器來源包括主動式雲端截毒技術伺服器和趨勢科技主動式雲端截毒技術。 標準用戶端會連線到主動式雲端截毒伺服器來源進行網頁信譽評等查詢。 雲端掃瞄用戶端會連線到主動式雲端截毒伺服器來源進行掃瞄與網頁信譽評等查詢。	如果主動式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式雲端截毒伺服器來源，而用戶端嘗試與伺服器來源建立連線，則圖示會包含一個進度列。  如需此問題的詳細資訊，請參閱：主動式雲端截毒伺服器來源無法使用 第 14-35 頁。
		若為標準用戶端，當關閉用戶端上的網頁信譽評等時，將不會顯示核取記號或進度列。

用戶端狀態	說明	視覺提示
即時掃瞄服務狀態	OfficeScan 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。覆蓋兩層藍色陰影用來表示用戶端的掃瞄方法。 • 若為標準掃瞄：  • 若為雲端截毒掃瞄： 
		如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。 覆蓋兩層紅色陰影用來表示用戶端的掃瞄方法。 • 若為標準掃瞄：  • 若為雲端截毒掃瞄：  如需此問題的詳細資訊，請參閱：即時掃瞄服務已關閉或未正常運作 第 14-34 頁。
即時掃瞄狀態	即時掃瞄透過在建立、修改或擷取檔案時掃瞄看是否有安全威脅，以提供主動式安全防護。	如果啟動即時掃瞄，則不會有視覺提示。
		如果關閉即時掃瞄，整個圖示會圍繞著紅色圈圈並包含紅色的對角線。  如需此問題的詳細資訊，請參閱： • 即時掃瞄已關閉 第 14-34 頁 • 即時掃瞄已關閉，且 OfficeScan 用戶端正以行動模式執行 第 14-34 頁

用戶端狀態	說明	視覺提示
病毒碼更新狀態	用戶端必須定期更新病毒碼，以保護用戶端不受最新的安全威脅攻擊。	如果病毒碼是最新狀態或僅稍微過期，則不會有視覺提示。
		如果病毒碼嚴重過期，則圖示會包含一個驚嘆號。這表示病毒碼已有一段時間未更新。  如需有關如何更新用戶端的詳細資訊，請參閱 OfficeScan 用戶端更新 第 6-24 頁。

雲端截毒掃瞄圖示

當 OfficeScan 用戶端使用雲端截毒掃瞄時，會顯示下列任一圖示。

表 14-5. 雲端截毒掃瞄圖示

圖示	和 OfficeScan 伺服器之間的連線	主動式雲端截毒伺服器來源的可用性	即時掃瞄服務	即時掃瞄
	線上	可用	正常運作	已啟動
	線上	可用	正常運作	已關閉
	線上	可用	已關閉或未正常運作	已關閉或未正常運作
	線上	無法使用，重新連線至來源	正常運作	已啟動
	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

圖示	和 OfficeScan 伺服器之間的連線	主動式雲端截毒伺服器來源的可用性	即時掃瞄服務	即時掃瞄
	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
	行動模式	可用	正常運作	已啟動
	行動模式	可用	正常運作	已關閉
	行動模式	可用	已關閉或未正常運作	已關閉或未正常運作
	行動模式	無法使用，重新連線至來源	正常運作	已啟動
	行動模式	無法使用，重新連線至來源	正常運作	已關閉
	行動模式	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 OfficeScan 用戶端使用標準掃瞄時，會顯示下列任一圖示。

表 14-6. 標準掃瞄圖示

圖示	和 OfficeScan 伺服器之間的連線	由主動式雲端截毒伺服器來源所提供的網頁信譽評等服務	即時掃瞄服務	即時掃瞄	病毒碼
	線上	可用	正常運作	已啟動	最新狀態或稍微過期
	線上	無法使用，重新連線至來源	正常運作	已啟動	最新狀態或稍微過期
	線上	可用	正常運作	已啟動	嚴重過期
	線上	無法使用，重新連線至來源	正常運作	已啟動	嚴重過期
	線上	可用	正常運作	已關閉	最新狀態或稍微過期
	線上	無法使用，重新連線至來源	正常運作	已關閉	最新狀態或稍微過期
	線上	可用	正常運作	已關閉	嚴重過期
	線上	無法使用，重新連線至來源	正常運作	已關閉	嚴重過期
	線上	可用	已關閉或未正常運作	已關閉或未正常運作	最新狀態或稍微過期
	線上	無法使用，重新連線至來源	已關閉或未正常運作	已關閉或未正常運作	最新狀態或稍微過期
	線上	可用	已關閉或未正常運作	已關閉或未正常運作	嚴重過期

圖示	和 OfficeScan 伺服器之間的連線	由主動式雲端截毒伺服器來源所提供的網頁信譽評等服務	即時掃瞄服務	即時掃瞄	病毒碼
	線上	無法使用，重新連線至來源	已關閉或未正常運作	已關閉或未正常運作	嚴重過期
	離線	可用	正常運作	已啟動	最新狀態或稍微過期
	離線	無法使用，重新連線至來源	正常運作	已啟動	最新狀態或稍微過期
	離線	可用	正常運作	已啟動	嚴重過期
	離線	無法使用，重新連線至來源	正常運作	已啟動	嚴重過期
	離線	可用	正常運作	已關閉	最新狀態或稍微過期
	離線	無法使用，重新連線至來源	正常運作	已關閉	最新狀態或稍微過期
	離線	可用	正常運作	已關閉	嚴重過期
	離線	無法使用，重新連線至來源	正常運作	已關閉	嚴重過期
	離線	可用	已關閉或未正常運作	已關閉或未正常運作	最新狀態或稍微過期
	離線	無法使用，重新連線至來源	已關閉或未正常運作	已關閉或未正常運作	最新狀態或稍微過期
	離線	可用	已關閉或未正常運作	已關閉或未正常運作	嚴重過期
	離線	無法使用，重新連線至來源	已關閉或未正常運作	已關閉或未正常運作	嚴重過期

圖示	和 OfficeScan 伺服器之間的連線	由主動式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
	行動模式	可用	正常運作	已啟動	最新狀態或稍微過期
	行動模式	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
	行動模式	可用	正常運作	已啟動	嚴重過期
	行動模式	無法使用，重新連線至來源	正常運作	已啟動	嚴重過期
	行動模式	可用	正常運作	已關閉	最新狀態或稍微過期
	行動模式	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
	行動模式	可用	正常運作	已關閉	嚴重過期
	行動模式	無法使用，重新連線至來源	正常運作	已關閉	嚴重過期
	行動模式	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
	行動模式	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
	行動模式	可用	已關閉或未正常運作	已關閉或未正常運作	嚴重過期
	行動模式	無法使用，重新連線至來源	已關閉或未正常運作	已關閉或未正常運作	嚴重過期
	線上	無 (已關閉用戶端上的網頁信譽評等功能)	正常運作	已啟動	最新狀態或稍微過期

圖示	和 OfficeScan 伺服器之間的連線	由主動式雲端截毒伺服器來源所提供的網頁信譽評等服務	即時掃瞄服務	即時掃瞄	病毒碼
	線上	無 (已關閉用戶端上的網頁信譽評等功能)	正常運作	已啟動	嚴重過期
	線上	無 (已關閉用戶端上的網頁信譽評等功能)	正常運作	已關閉	最新狀態或稍微過期
	線上	無 (已關閉用戶端上的網頁信譽評等功能)	正常運作	已關閉	嚴重過期
	線上	無 (已關閉用戶端上的網頁信譽評等功能)	已關閉或未正常運作	已關閉或未正常運作	最新狀態或稍微過期
	線上	無 (已關閉用戶端上的網頁信譽評等功能)	已關閉或未正常運作	已關閉或未正常運作	嚴重過期
	離線	無 (已關閉用戶端上的網頁信譽評等功能)	正常運作	已啟動	最新狀態或稍微過期
	離線	無 (已關閉用戶端上的網頁信譽評等功能)	正常運作	已啟動	嚴重過期
	離線	無 (已關閉用戶端上的網頁信譽評等功能)	正常運作	已關閉	最新狀態或稍微過期
	離線	無 (已關閉用戶端上的網頁信譽評等功能)	正常運作	已關閉	嚴重過期
	離線	無 (已關閉用戶端上的網頁信譽評等功能)	已關閉或未正常運作	已關閉或未正常運作	最新狀態或稍微過期

圖示	和 OfficeScan 伺服器之間的連線	由主動式雲端截毒伺服器來源所提供的網頁信譽評等服務	即時掃瞄服務	即時掃瞄	病毒碼
	離線	無 (已關閉用戶端上的網頁信譽評等功能)	已關閉或未正常運作	已關閉或未正常運作	嚴重過期
	行動模式	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
	行動模式	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
	行動模式	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
	行動模式	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
	行動模式	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
	行動模式	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

OfficeScan 用戶端圖示指示的問題的解決方案

如果 OfficeScan 用戶端圖示指出下列任何一種狀況，請執行必要的處理行動：

病毒碼檔案已有一段時間未更新

OfficeScan 用戶端使用者需要更新元件。從 Web 主控台的「更新 > 用戶端電腦 > 自動更新」中設定元件更新設定，或在「用戶端電腦 > 用戶端管理 > 設定 > 權限和其他設定 > 權限 > 元件更新權限中，授與使用者進行更新的權限。

即時掃瞄服務已關閉或未正常運作

如果「即時掃瞄服務」（OfficeScan NT 即時掃瞄）已關閉或未正常運作，使用者必須從 Microsoft 管理主控台手動啟動該服務。

即時掃瞄已關閉

從 Web 主控台啟動「即時掃瞄」（「用戶端電腦 > 用戶端管理 > 設定 > 掃瞄設定 > 即時掃瞄設定」）。

即時掃瞄已關閉，且 OfficeScan 用戶端正以行動模式執行

使用者必須先關閉行動模式。關閉行動模式之後，從 Web 主控台啟動「即時掃瞄」。

OfficeScan 用戶端已連線到網路，但顯示為離線

從 Web 主控台驗證連線（「用戶端電腦 > 連線驗證」），然後檢查連線驗證記錄檔（「記錄檔 > 用戶端電腦記錄檔 > 連線驗證」）。

如果驗證之後 OfficeScan 用戶端仍為離線狀態：

1. 如果伺服器和 OfficeScan 用戶端上的連線狀態都是離線，請檢查網路連線。
2. 如果 OfficeScan 用戶端上的連線狀態為離線，但在伺服器上顯示為線上狀態，表示伺服器的網域名稱可能已變更，而 OfficeScan 用戶端使用網域名稱連線到伺服器（如果在伺服器安裝期間選取了網域名稱）。請向 DNS 或 WINS 伺服器註冊 OfficeScan 伺服器的網域名稱，或是將網域名稱和 IP 資訊新增至用戶端電腦 `<Windows 資料夾>\system32\drivers\etc` 資料夾中的「hosts」檔案。

3. 如果 OfficeScan 用戶端上的連線狀態為線上，但伺服器上的連線狀態為離線，請檢查 OfficeScan 防火牆設定。防火牆可能會封鎖伺服器到用戶端的通訊，但是允許用戶端到伺服器的通訊。

4. 如果 OfficeScan 用戶端上的連線狀態為線上，但伺服器上的連線狀態為離線，表示 OfficeScan 用戶端的 IP 位址可能已變更，但其狀態並未反映在伺服器上（例如：重新載入用戶端時）。請嘗試重新部署 OfficeScan 用戶端。

主動式雲端截毒伺服器來源無法使用

如果用戶端和主動式雲端截毒伺服器來源間的連線中斷，請執行這些工作：

1. 在 Web 主控台上，移至「電腦位置」畫面（「用戶端電腦 > 電腦位置」），然後檢查下列電腦位置設定是否正確：
   - 參考伺服器和通訊埠號碼
   - 閘道 IP 位址
2. 在 Web 主控台上，移至「主動式雲端截毒技術來源」畫面（「主動式雲端截毒技術 > 主動式雲端截毒技術來源」），然後執行下列工作：
   a. 檢查標準或自訂來源清單上的「主動式雲端截毒技術伺服器」設定是否正確。
   b. 測試是否可以和伺服器建立連線。
   c. 設定來源清單之後，請按一下「通知所有用戶端」。
3. 檢查主動式雲端截毒技術伺服器和 OfficeScan 用戶端上的下列設定檔是否同步：
   - `sscfg.ini`
   - `ssnotify.ini`
4. 開啟「登錄編輯程式」，然後檢查用戶端是否已連線到企業網路。

   機碼：

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp
   \CurrentVersion\iCRC Scan\Scan Server
   ```

- 如果 `LocationProfile=1`，表示 OfficeScan 用戶端已連線到網路，因此應該可以連線到主動式雲端截毒技術伺服器。
- 如果 `LocationProfile=2`，表示 OfficeScan 用戶端未連線到網路，而且應該連線到主動式雲端截毒技術。從 Internet Explorer 檢查 OfficeScan 用戶端電腦是否可以瀏覽 Internet 網頁。

5. 檢查用以連線到主動式雲端截毒技術和主動式雲端截毒技術伺服器的內部和外部 Proxy 伺服器設定。如需詳細資訊，請參閱 OfficeScan 用戶端的內部 Proxy 伺服器 第 14-42 頁和 OfficeScan 用戶端的外部 Proxy 伺服器 第 14-43 頁。

6. 若為標準用戶端，請確認 OfficeScan NT Proxy 服務 (`TmProxy.exe`) 正在執行中。如果此服務已停止，用戶端將無法連線到網頁信譽評等的主動式雲端截毒伺服器來源。

驗證用戶端和伺服器間的連線

用戶端和 OfficeScan 伺服器間的連線狀態會顯示在 OfficeScan Web 主控台的用戶端樹狀結構中。

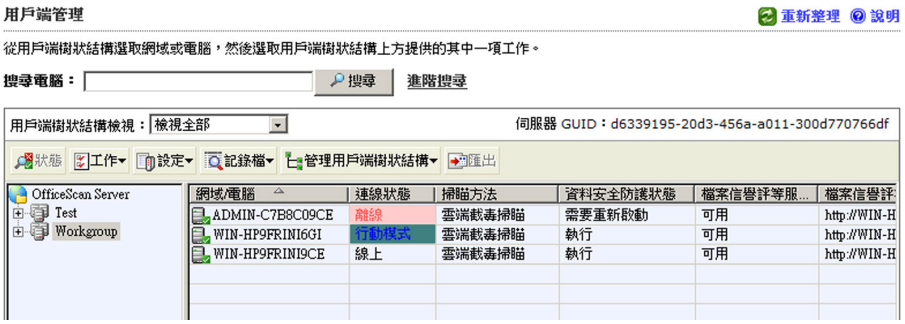


圖 14-2. 顯示用戶端與 OfficeScan 伺服器的連線狀態的用戶端樹狀結構

某些情況可能使用用戶端樹狀結構無法顯示正確的用戶端連線狀態。例如，如果您不小心拔除用戶端電腦的網路線，用戶端將無法通知伺服器其現為離線狀態。這個用戶端仍會在用戶端樹狀結構中顯示為線上。

手動驗證用戶端與伺服器間的連線，或讓 OfficeScan 執行預約驗證。您無法選取特定網域或用戶端，然後驗證其連線狀態。OfficeScan 會驗證其所有已註冊用戶端的連線狀態。

驗證用戶端與伺服器間的連線

程序

1. 瀏覽至「用戶端電腦 > 連線驗證」。
2. 如果要手動驗證用戶端與伺服器間的連線，請移至「手動驗證」標籤，然後按一下「立即驗證」。
3. 如果要自動驗證用戶端與伺服器間的連線，請移至「預約驗證」標籤。
   a. 選取「啟動預約驗證」。
   b. 選取驗證頻率和開始時間。
   c. 按一下「儲存」以儲存驗證預約時程。
4. 檢查用戶端樹狀結構，以驗證狀態或檢視連線驗證記錄檔。

連線驗證記錄檔

OfficeScan 會製作連線驗證記錄檔，讓您能夠判斷 OfficeScan 伺服器是否可與所有其註冊用戶端進行通訊。每當您從 Web 主控台驗證用戶端和伺服器間的連線時，OfficeScan 就會建立記錄項目。

如果要避免記錄檔佔去過多硬碟空間，請手動刪除記錄檔或設定記錄檔刪除預約時程。如需有關管理記錄檔的詳細資訊，請參閱記錄檔管理 第 13-31 頁。

檢視連線驗證記錄檔

程序

1. 瀏覽至「用戶端電腦 > 連線驗證」。
2. 檢查「狀態」欄位以檢視連線驗證結果。
3. 如果要將記錄檔儲存為逗號分隔值 (CSV) 檔案，請按一下「匯出到 CSV」。開啟檔案或將其儲存至特定位置。

無法連線到用戶端

位於無法連接的網路（例如：NAT 閘道後方的網路區段）上的 OfficeScan 用戶端通常會是離線，因為伺服器無法與這些用戶端建立直接連線。因此，伺服器無法通知這些用戶端執行下列動作：

- 下載最新的元件。
- 套用從 Web 主控台設定的用戶端設定。例如：當您從 Web 主控台變更「預約掃瞄」頻率時，伺服器將立即通知用戶端套用新設定。

因此，無法連線的用戶端無法及時執行這些工作。它們只能在起始與伺服器的連線時才能執行工作，例如下列情況：

- 用戶端在安裝後向伺服器註冊。
- 用戶端重新啟動或重新載入。此事件不會經常發生，而且通常需要使用者介入。
- 在用戶端上觸發手動或預約更新。此事件也不會經常發生。

只有在用戶端註冊、重新啟動或重新載入時，伺服器才會「得知」用戶端連線並將其視為處於線上狀態。不過，因為伺服器仍無法建立與用戶端的連線，因此伺服器會立即將狀態變更為離線。

OfficeScan 提供「活動訊號」和伺服器輪詢功能，可解決無法連接的用戶端的問題。使用這些功能時，伺服器會停止通知用戶端有關元件更新和設定變更的

資訊。伺服器反而會變成被動角色，隨時等候用戶端傳送活動訊號或起始輪詢。當伺服器偵測到這些事件時，便會將用戶端視為處於線上狀態。

注意

與活動訊號和伺服器輪詢無關的事件（例如：用戶端起始的手動用戶端更新和記錄檔傳送）不會觸發伺服器更新無法連線的用戶端的狀態。

活動訊號

OfficeScan 用戶端會傳送活動訊號訊息，以通知伺服器用戶端的連線仍正常運作。當伺服器收到活動訊號訊息時，便會將該用戶端視為處於線上狀態。在用戶端樹狀結構中，用戶端的狀態可以是下列其中一個值：

- 線上：表示一般線上用戶端
- 無法連接/線上：表示位在無法連接的網路中的線上用戶端

注意

當 OfficeScan 用戶端在傳送活動訊號訊息時，它不會更新元件或套用新設定。標準用戶端會在定期更新期間執行這些工作（請參閱 OfficeScan 用戶端更新 第 6-24 頁）。位在無法連接的網路中的用戶端會在伺服器輪詢期間執行這些工作。

活動訊號功能可解決位在無法連接的網路中的 OfficeScan 用戶端總是看起來像是離線的問題（即使用戶端可連線到伺服器）。

Web 主控台中有一個設定，可控制用戶端傳送活動訊號訊息的頻率。如果伺服器未收到活動訊號，它不會立即將用戶端視為處於離線狀態。另一個設定可控制沒有活動訊號多長時間之後，再將用戶端的狀態變更為：

- 離線：表示一般離線 OfficeScan 用戶端
- 無法連接/離線：表示位在無法連接的網路中的離線 OfficeScan 用戶端

選擇活動訊號設定時，務必在顯示最新用戶端 狀態資訊的需求和管理系統資源的需求之間取得平衡。預設設定能夠滿足大部分情況的需求。不過，當您自訂活動訊號設定時，請務必考慮下列幾點：

表 14-7. 活動訊號建議

活動訊號頻率	建議
長時間間隔活動訊號（60 分鐘以上）	活動訊號之間的時間間隔越長，伺服器在 Web 主控台上反映用戶端狀態之前可能發生的事件數目就越多。
短時間間隔活動訊號（60 分鐘以下）	短時間間隔可讓伺服器提供更即時的用戶端狀態，但會耗用較多頻寬。

伺服器輪詢

伺服器輪詢功能可解決無法連線的 OfficeScan 用戶端未及時接收元件更新和用戶端設定變更的通知的問題。此功能獨立於活動訊號功能。

使用伺服器輪詢功能時：

- OfficeScan 用戶端會定期自動起始與 OfficeScan 伺服器的連線。當伺服器偵測到發生輪詢時，就會將用戶端視為「無法連接/線上」。
- OfficeScan 用戶端會連線到其一或多個更新來源，以下載任何已更新的元件並套用新的用戶端設定。如果 OfficeScan 伺服器或「更新代理程式」是主要更新來源，用戶端會同時取得元件和新設定。如果來源不是 OfficeScan 伺服器或「更新代理程式」，用戶端只會取得已更新的元件，然後連線到 OfficeScan 伺服器或「更新代理程式」以取得新設定。

設定活動訊號和伺服器輪詢功能

程序

1. 瀏覽至「用戶端電腦 > 全域用戶端設定」，
2. 移至「無法連線的網路」區段。
3. 設定伺服器輪詢設定。

   如需有關伺服器輪詢的詳細資訊，請參閱 伺服器輪詢 第 14-40 頁。

   a. 如果 OfficeScan 伺服器同時具有 IPv4 和 IPv6 位址，您可以輸入 IPv4 位址範圍和 IPv6 字首和長度。

如果伺服器是純 IPv4，請輸入 IPv4 位址；如果伺服器是純 IPv6，請輸入 IPv6 字首和長度。

當用戶端的 IP 位址符合範圍中的某個 IP 位址時，用戶端會套用活動訊號和伺服器輪詢設定，而伺服器會將用戶端視為屬於無法連線的網路。

注意

具有 IPv4 位址的用戶端可連線到純 IPv4 或雙堆疊 OfficeScan 伺服器。

具有 IPv6 位址的用戶端可連線到純 IPv6 或雙堆疊 OfficeScan 伺服器。

雙堆疊用戶端可連線到雙堆疊、純 IPv4 或純 IPv6 OfficeScan 伺服器。

b. 在「用戶端每隔 __ 分鐘輪詢伺服器中是否有更新的元件與設定」中，指定伺服器輪詢頻率。請輸入介於 1 到 129600 分鐘之間的值。

秘訣

趨勢科技建議至少將伺服器輪詢頻率設定為活動訊號傳送頻率的三倍。

4. 設定活動訊號設定。

如需有關活動訊號功能的詳細資訊，請參閱活動訊號 第 14-39 頁。

a. 選取「允許用戶端將活動訊號傳送到伺服器」。

b. 選取「所有用戶端」或「僅限無法連線的網路中的用戶端」。

c. 在「用戶端傳送活動訊號的間隔：__ 分鐘」中，指定用戶端傳送活動訊號的頻率。請輸入介於 1 到 129600 分鐘之間的值。

d. 在「如果超過以下時間未收到用戶端傳送的活動訊號，則將它視為離線：__ 分鐘」中，指定 OfficeScan 伺服器在多久時間內未收到活動訊號就將用戶端視為離線。請輸入介於 1 到 129600 分鐘之間的值。

5. 按一下「儲存」。

OfficeScan 用戶端 Proxy 伺服器設定

設定 OfficeScan 用戶端，讓用戶端在連線到內部和外部伺服器時使用 Proxy 伺服器設定。

OfficeScan 用戶端的內部 Proxy 伺服器

OfficeScan 用戶端可以使用內部 Proxy 伺服器設定來連線到網路上的下列伺服器：

- OfficeScan 伺服器電腦

  此伺服器電腦裝載 OfficeScan 伺服器和整合式主動式雲端截毒技術伺服器。OfficeScan 用戶端會連線到 OfficeScan 伺服器以更新元件、取得組態設定，以及傳送記錄檔。OfficeScan 用戶端會連線到整合式主動式雲端截毒技術伺服器以傳送掃瞄查詢。

- 主動式雲端截毒技術伺服器

  主動式雲端截毒技術伺服器包含所有獨立式主動式雲端截毒技術伺服器和其他 OfficeScan 伺服器的整合式主動式雲端截毒技術伺服器。OfficeScan 用戶端會連線到伺服器以傳送掃瞄和網頁信譽評等查詢。

設定內部 Proxy 伺服器設定

程序

1. 瀏覽到「管理 > Proxy 伺服器設定」。
2. 按一下「內部 Proxy 伺服器」標籤。
3. 移至「用戶端與 OfficeScan 伺服器電腦之間的連線」區段。
   a. 選取「當用戶端連線至 OfficeScan 伺服器和整合式主動式雲端截毒技術伺服器時，使用下列 Proxy 伺服器設定」。
   b. 指定 Proxy 伺服器名稱或 IPv4/IPv6 位址，以及通訊埠號碼。

注意

如果您有 IPv4 和 IPv6 用戶端，請定雙堆疊 Proxy 伺服器（由它的主機名稱指出）。這是因為內部 Proxy 伺服器設定是全域設定。如果指定 IPv4 位址，IPv6 用戶端將無法連線到 Proxy 伺服器。同樣地，如果指定 IPv6 位址，IPv4 將無法連線到 Proxy 伺服器。

c. 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。

4. 移至「用戶端與獨立式主動式雲端截毒技術伺服器之間的連線」區段。

   a. 選取「當用戶端連線至獨立式主動式雲端截毒技術伺服器時，使用下列 Proxy 伺服器設定」。

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

   c. 如果 Proxy 伺服器需要驗證，請輸入使用者名稱和密碼，然後確認密碼。

5. 按一下「儲存」。

OfficeScan 用戶端的外部 Proxy 伺服器

OfficeScan 伺服器和 OfficeScan 用戶端可以使用外部 Proxy 伺服器設定來連線到趨勢科技所裝載的伺服器。此主題討論適用於用戶端的外部 Proxy 伺服器設定。如需適用於伺服器的外部 Proxy 伺服器設定，請參閱用於 OfficeScan 伺服器更新的 Proxy 第 6-16 頁。

OfficeScan 用戶端可以使用在 Internet Explorer 中設定的 Proxy 伺服器設定，連線到趨勢科技主動式雲端截毒技術。如果需要 Proxy 伺服器驗證，用戶端將會使用 Proxy 伺服器驗證憑證（使用者 ID 和密碼）。

設定 Proxy 伺服器驗證憑證

程序

1. 瀏覽到「管理 > Proxy 伺服器設定」。

2. 按一下「外部 Proxy 伺服器」標籤。
3. 移至「用戶端與趨勢科技伺服器之間的連線」區段。
4. 輸入 Proxy 伺服器驗證所需的使用者 ID 和密碼，然後確認密碼。支援下列 Proxy 伺服器驗證通訊協定：
   - 基本存取驗證
   - 摘要存取驗證
   - 整合的 Windows 驗證
5. 按一下「儲存」。

用戶端的 Proxy 伺服器設定權限

您可以授與用戶端使用者設定 Proxy 伺服器設定的權限。OOfficeScan 用戶端只會在下列情況中使用使用者設定的 Proxy 伺服器設定：

- 當 OfficeScan 用戶端執行「立即更新」時。
- 當使用者關閉（或 OfficeScan 用戶端無法偵測）自動 Proxy 伺服器設定時。如需詳細資訊，請參閱適用於 OfficeScan 用戶端的自動 Proxy 伺服器設定 第 14-45 頁。

警告!

如果使用者設定的 Proxy 伺服器設定不正確，會導致發生更新問題。允許使用者設定自己的 Proxy 伺服器設定時請特別小心。

授與 Proxy 伺服器設定權限

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。

2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 權限和其他設定」。
4. 在「權限」標籤上，移至「Proxy 伺服器設定權限」區段。
5. 選取「允許用戶端使用者設定 Proxy 伺服器設定」。
6. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

適用於 OfficeScan 用戶端的自動 Proxy 伺服器設定

手動設定 Proxy 伺服器設定對於許多終端使用者來說，可能是複雜的工作。使用自動 Proxy 伺服器設定可確保套用正確的 Proxy 伺服器設定，而不需使用者介入。

啟動此選項時，自動 Proxy 伺服器設定會是 OfficeScan 用戶端更新元件（透過自動更新或「立即更新」）時的主要 Proxy 伺服器設定。如需有關自動更新和「立即更新」的詳細資訊，請參閱 OfficeScan 用戶端更新方法 第 6-31 頁。

如果 OfficeScan 用戶端無法使用自動 Proxy 伺服器設定連線，具有設定 Proxy 伺服器設定權限的用戶端使用者可使用使用者設定的 Proxy 伺服器設定。否則，使用自動 Proxy 伺服器設定的連線將無法成功建立。

注意

不支援 Proxy 伺服器驗證。

設定自動 Proxy 伺服器設定

程序

1. 瀏覽至「用戶端電腦 > 全域用戶端設定」，
2. 移至「Proxy 伺服器組態設定」區段。
3. 如果您要讓 OfficeScan 依照 DHCP 或 DNS 自動偵測管理員設定的 Proxy 伺服器設定，請選取「自動偵測設定」。
4. 如果您要讓 OfficeScan 使用網路管理員設定的 Proxy 伺服器自動組態設定 (PAC) 程式檔來偵測適當的 Proxy 伺服器：
   a. 選取「使用自動組態設定程式檔」。
   b. 輸入 PAC 程式檔的位址。
5. 按一下「儲存」。

檢視 OfficeScan 用戶端資訊

「檢視狀態」畫面顯示有關 OfficeScan 用戶端的重要資訊，包括權限、用戶端軟體詳細資料及系統事件。

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「狀態」。
4. 展開用戶端電腦的名稱以檢視狀態資訊。如果您選取多個用戶端，請按一下「全部展開」以檢視所有選定用戶端的狀態資訊。

5. （選用）使用「重設」按鈕將安全威脅數量重設為零。

匯入和匯出用戶端設定

OfficeScan 可讓您將用戶端樹狀結構設定（由特定 OfficeScan 用戶端或網域所套用）匯出到檔案。接著，您可以匯入該檔案以將設定套用到其他用戶端和網域，或套用到具有相同版本的其他 OfficeScan 伺服器。

系統將匯出所有用戶端樹狀結構設定，「更新代理程式」設定除外。

匯出用戶端設定

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 匯出設定」。
4. 按一下任何連結，以檢視您所選取 OfficeScan 用戶端或網域的設定。
5. 按一下「匯出」以儲存設定。

   設定會存到 `.dat` 檔案中。
6. 按一下「儲存」，然後指定要儲存 `.dat` 檔案的位置。
7. 按一下「儲存」。

匯入用戶端設定

程序

1. 瀏覽至「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 匯入設定」。
4. 按一下「瀏覽」，在電腦上尋找 `.dat` 檔案，然後按一下「匯入」。

   「匯入設定」畫面就會出現，並顯示設定的摘要。
5. 按一下任何連結，以檢視要匯入的掃瞄設定或權限的詳細資訊。
6. 匯入設定。
   - 如果您是按一下根網域圖示，請選取「套用至所有網域」，然後按一下「套用到目標」。
   - 如果您是選取網域，請選取「套用至屬於選取之網域的所有電腦」，然後按一下「套用到目標」。
   - 如果您是選取多個用戶端，請按一下「套用到目標」。

安全性符合

使用「安全性符合」來判斷缺點、部署解決方案及維護安全基礎架構。這項功能有助於減少保護網路環境安全所需的時間，並讓組織在安全性和功能的需求之間取得平衡點。

實施適用於兩種電腦類型的安全性符合：

- 受管理：OfficeScan 用戶端受 OfficeScan 伺服器所管理的電腦。如需詳細資訊，請參閱適用於受管用戶端的安全性符合 第 14-49 頁。
- 未受管理：包括下列各項：

- OfficeScan 用戶端不是由 OfficeScan 伺服器所管理
- 未安裝 OfficeScan 用戶端的電腦
- OfficeScan 伺服器無法與其連線的電腦
- 無法驗證其安全狀態的電腦

如需詳細資訊，請參閱適用於未受管端點的安全性符合 第 14-60 頁。

適用於受管用戶端的安全性符合

「安全性符合」可產生「符合性報告」，以協助您評估 OfficeScan 伺服器所管理 OfficeScan 用戶端的安全狀態。「安全性符合」可視需要或根據預約產生報告。

您可以在「符合性報告」畫面上存取視需要和預約報告。該畫面包含下列標籤：

- 服務：使用此標籤來檢查用戶端服務是否正常運作。如需詳細資訊，請參閱服務 第 14-50 頁。
- 元件：使用此標籤來檢查 OfficeScan 用戶端是否有最新元件。如需詳細資訊，請參閱元件 第 14-51 頁。
- 掃瞄符合性：使用此標籤來檢查用戶端是否定期執行掃瞄。如需詳細資訊，請參閱掃瞄符合性 第 14-53 頁。
- 設定：使用此標籤來檢查用戶端設定是否與伺服器設定一致。如需詳細資訊，請參閱設定 第 14-55 頁。

注意

「元件」標籤可顯示執行最新和舊版產品的 OfficeScan 用戶端。對於其他標籤，只有執行 10.5、10.6 或更新版本的 OfficeScan 用戶端才會顯示。

有關符合性報告的注意事項

- 「安全性符合」會在產生「符合性報告」之前先查詢 OfficeScan 用戶端的連線狀態。它會在報告中包含線上和離線用戶端，但不會包含行動用戶端。
- 對於以角色為基礎的使用者帳號：
  - 每個 Web 主控台使用者帳號都有一組完全獨立的「符合性報告」設定。變更使用者帳號的「符合性報告」設定不會影響其他使用者帳號的設定。
  - 報告的範圍取決於使用者帳號的用戶端網域權限。例如，如果您將管理網域 A 和 B 的權限授與某個使用者帳號，該使用者帳號的報告只會顯示來自屬於網域 A 和 B 的用戶端的資料。

    如需有關使用者帳號的詳細資訊，請參閱以角色為基礎的管理 第 13-2 頁。

服務

「安全性符合」會檢查下列 OfficeScan 用戶端服務是否正常運作：

- 防毒
- 間諜程式防護
- 防火牆
- 網頁信譽評等
- 行為監控/周邊設備存取控管（亦稱為「趨勢科技未經授權的變更阻止服務」）
- 資料安全防護

不相容的用戶端在「符合報告」中至少會計算兩次。

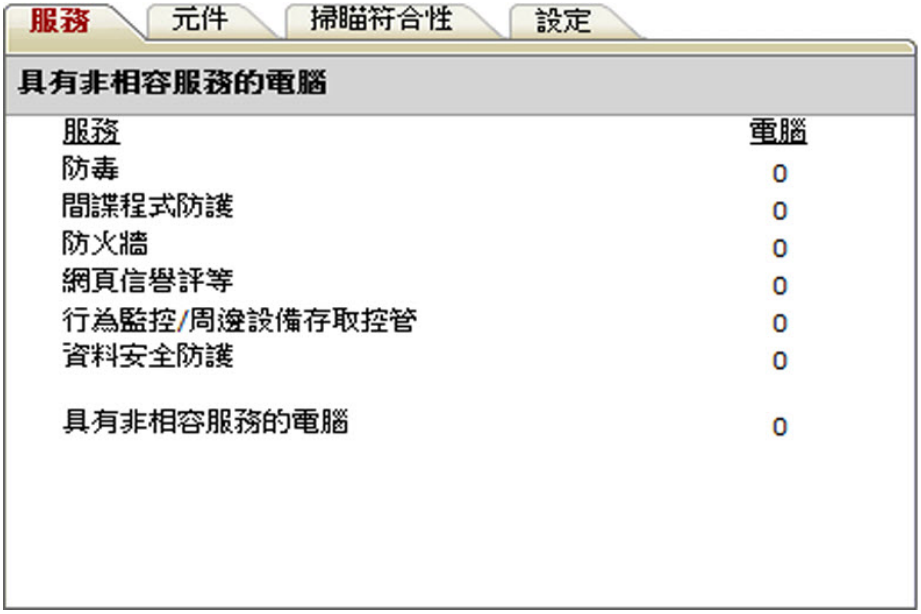


圖 14-3. 符合報告的「服務」標籤

- 在「服務異常的 Officescan 用戶端」類別中
- 在 OfficeScan 用戶端不相容的類別中。例如，如果某個 OfficeScan 用戶端的防毒服務未正常運作，該用戶端會在「防毒」類別中計算一次。如果多個服務未正常運作，該用戶端會在每個不相容的類別中都計算一次。

從 Web 主控台或 OfficeScan 用戶端電腦重新啟動未運作的服務。如果重新啟動服務之後，服務可以正常運作，下次評估時該用戶端就不會再顯示為不相容。

元件

「安全性符合」會判斷 OfficeScan 伺服器和 OfficeScan 用戶端之間的元件版本是否一致。不一致的情況通常發生在用戶端無法連線到伺服器以更新元件時。

如果用戶端是從其他來源（例如：趨勢科技主動式更新伺服器）取得更新，該用戶端的元件版本就可能比伺服器上的元件還要新。

「安全性符合」會檢查下列元件：

- 本機雲端病毒碼
- 病毒碼
- IntelliTrap 病毒碼
- IntelliTrap 例外病毒碼
- 病毒掃瞄引擎
- 間諜程式病毒碼
- 間諜程式主動式監控病毒碼
- 間諜程式掃瞄引擎
- 病毒清除範本
- 病毒清除引擎
- 一般防火牆病毒碼
- 一般防火牆驅動程式
- 行為監控驅動程式
- 行為監控核心服務
- 行為監控配置特徵碼
- 數位簽章特徵碼
- 策略實施特徵碼
- 行為監控偵測特徵碼
- 程式版本

不相容的用戶端在「符合報告」中至少會計算兩次。

圖 14-4. 符合報告的「元件」標籤

- 在「需要更新元件的 Officescan 用戶端」類別中
- 在用戶端不相容的類別中。例如，如果用戶端的「本機雲端病毒碼」版本與伺服器上的版本不一致，該用戶端會在「本機雲端病毒碼」類別中計算一次。如果多個元件版本不一致，該用戶端會在每個不相容的類別中都計算一次。

如果要解決元件版本不一致的問題，請更新用戶端或伺服器上的已過期元件。

掃瞄符合性

「安全性符合」會檢查「立即掃瞄」或「預約掃瞄」是否定期執行，以及這些掃瞄是否在合理的時間內完成。

注意

只有已在用戶端上啟動「預約掃瞄」時，「安全性符合」才會回報「預約掃瞄」狀態。

「安全性符合」會使用下列掃瞄符合性條件：

- 未執行「立即掃瞄」或「預約掃瞄」(x) 天：如果 OfficeScan 用戶端在指定天數內未執行過「立即掃瞄」或「預約掃瞄」，則會被判定為不相容。
- 「立即掃瞄」或「預約掃瞄」已超過 (x) 小時：如果 OfficeScan 用戶端上次執行「立即掃瞄」或「預約掃瞄」的持續時間已超過指定的時數，則會被判定為不相容。

不相容的用戶端在「符合報告」中至少會計算兩次。

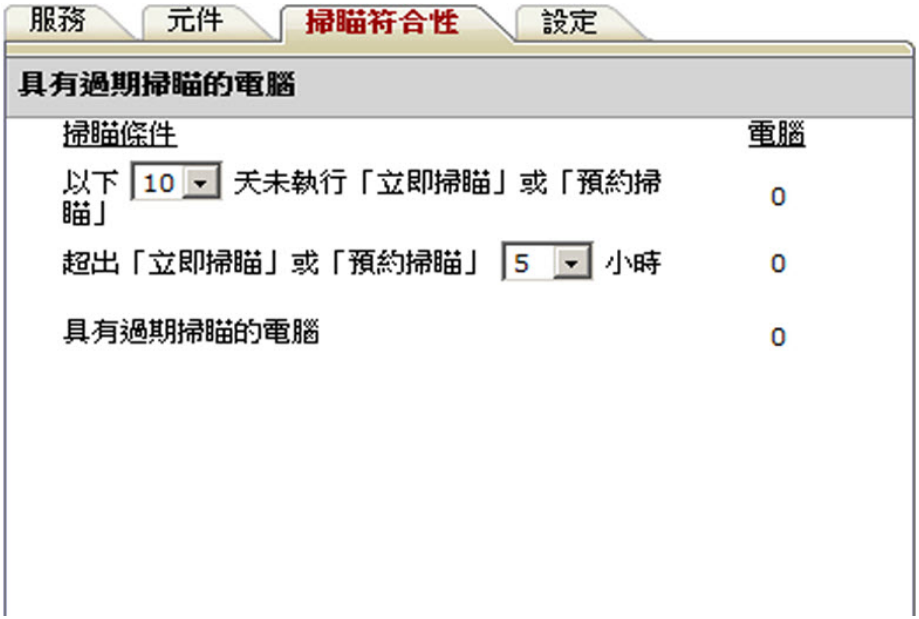


圖 14-5. 符合報告的「掃瞄符合性」標籤

- 在「動或預約掃瞄異常的 Officescan 用戶端」類別中

- 在用戶端不相容的類別中。例如，如果上次執行「預約掃瞄」的時間超過指定的時數，該用戶端會在「「立即掃瞄」或「預約掃瞄」已超過 <x> 小時」類別中計算一次。如果用戶端符合多個掃瞄符合性條件，它會在每個不相容的類別中都計算一次。

在尚未執行掃瞄工作或無法完成掃瞄的用戶端上，執行「立即掃瞄」或「預約掃瞄」。

設定

「安全性符合」會判斷用戶端是否與用戶端樹狀結構中的上層網域具有相同的設定。如果您將用戶端移到另一個套用不同設定的網域中，或如果具有特定權限的用戶端使用者在 OfficeScan 用戶端主控台上進行手動設定，設定可能會不一致。

OfficeScan 會驗證下列設定：

- 掃瞄方法
- 手動掃瞄設定
- 即時掃瞄設定
- 預約掃瞄設定
- 立即掃瞄設定
- 權限和其他設定
- 其他服務設定
- 網頁信譽評等
- 行為監控
- 周邊設備存取控管
- 間諜程式/可能的資安威脅程式核可清單
- Data Loss Prevention 設定

不相容的用戶端在「符合報告」中至少會計算兩次。

圖 14-6. 符合報告的「設定」標籤

- 在「與 Officescan 伺服器組態設定不一致的用戶端」類別中
- 在用戶端不相容的類別中。例如，如果用戶端中的掃瞄方法設定與其上層網域不一致，該用戶端會在「掃瞄方法」類別中計算一次。如果多個設定不一致，該用戶端會在每個不相容的類別中都計算一次。

如果要解決設定不一致的問題，請將網域設定套用到用戶端。

依要求執行的符合性報告

您可以視需要使用「安全性符合」來產生「符合報告」。報告可協助您評估 OfficeScan 伺服器所管理 OfficeScan 用戶端的安全狀態。

如需有關符合性報告的詳細資訊，請參閱適用於受管用戶端的安全性符合 第 14-49 頁。

產生視需要「符合性報告」

程序

1. 瀏覽至「安全性符合 > 符合性評估 > 符合性報告」。
2. 移至「用戶端樹狀結構範圍」區段。
3. 選取根網域或網域，然後按一下「評估」。
4. 檢視用戶端服務的「符合報告」。

   如需有關用戶端服務的詳細資訊，請參閱服務 第 14-50 頁。

   a. 按一下「服務」標籤。

   b. 在「服務異常的 Officescan 用戶端」下，檢查具有服務異常的用戶端數量。

   c. 按一下數字連結，以顯示用戶端樹狀結構中所有受影響的用戶端。

   d. 從查詢結果中選取用戶端。

   e. 按一下「重新啟動 OfficeScan 用戶端」以重新啟動服務。

   > **注意**
   >
   > 若重新執行評估後，用戶端仍顯示為不相容，請手動重新啟動用戶端電腦上的服務。

   f. 如果要將用戶端清單儲存到檔案，請按一下「匯出」。

5. 檢視用戶端元件的「符合報告」。

   如需有關用戶端元件的詳細資訊，請參閱元件 第 14-51 頁。

   a. 按一下「元件」標籤。

b. 在「需要更新元件的 Officescan 用戶端」下，檢查元件版本與伺服器上的版本不一致的用戶端數量。

c. 按一下數字連結，以顯示用戶端樹狀結構中所有受影響的用戶端。

注意

如果至少有一部用戶端擁有比 OfficeScan 伺服器新的元件，請手動更新 OfficeScan 伺服器。

d. 從查詢結果中選取用戶端。

e. 按一下「立即更新」以強制用戶端下載元件。

注意

- 為確保用戶端可升級用戶端程式，請關閉「用戶端電腦 > 用戶端管理 > 設定 > 權限和其他設定」中的「用戶端可更新元件，但不升級用戶端程式或部署 HotFix」選項。
- 重新啟動電腦（而不是按一下「立即更新」），可更新一般防火牆驅動程式。

f. 如果要將用戶端清單儲存到檔案，請按一下「匯出」。

6. 檢視掃瞄的「符合報告」。

如需有關掃瞄的詳細資訊，請參閱掃瞄符合性 第 14-53 頁。

a. 按一下「掃瞄符合性」標籤。

b. 在「手動或預約掃瞄異常的 Officescan 用戶端」下，設定下列選項：

- 用戶端未執行「立即掃瞄」或「預約掃瞄」的天數
- 「立即掃瞄」或「預約掃瞄」的執行時數

注意

如果超過該天數或時數，則將用戶端視為不符合。

c. 按一下「用戶端樹狀結構範圍」區段旁的「評估」。

d. 在「手動或預約掃瞄異常的 Officescan 用戶端」下，檢查符合掃瞄條件的用戶端數量。

e. 按一下數字連結，以顯示用戶端樹狀結構中所有受影響的用戶端。

f. 從查詢結果中選取用戶端。

g. 按一下「立即掃瞄」以在用戶端上開始執行「立即掃瞄」。

注意

為避免重複掃瞄，如果「立即掃瞄」的執行時間超過指定時數，將關閉「立即掃瞄」選項。

h. 如果要將用戶端清單儲存到檔案，請按一下「匯出」。

7. 檢視設定的「符合報告」。

如需有關設定的詳細資訊，請參閱設定 第 14-55 頁。

a. 按一下設定標籤。

b. 在「與 Officescan 伺服器組態設定不一致的用戶端」下，檢查設定與用戶端樹狀結構網域設定不一致的用戶端數量。

c. 按一下數字連結，以顯示用戶端樹狀結構中所有受影響的用戶端。

d. 從查詢結果中選取用戶端。

e. 按一下「套用網域設定」。

f. 如果要將用戶端清單儲存到檔案，請按一下「匯出」。

預約符合性報告

「安全性符合」可依預約產生「符合報告」。報告可協助您評估 OfficeScan 伺服器所管理 OfficeScan 用戶端的安全狀態。

如需有關符合性報告的詳細資訊，請參閱適用於受管用戶端的安全性符合 第 14-49 頁。

設定預約「符合性報告」的設定

程序

1. 瀏覽至「安全性符合 > 符合性評估 > 預約符合性報告」。
2. 選取「啟動預約報告」。
3. 指定報告的標題。
4. 選取下列其中一項或全部：
   - 服務 第 14-50 頁
   - 元件 第 14-51 頁
   - 掃瞄符合性 第 14-53 頁
   - 設定 第 14-55 頁
5. 指定將接收預約「符合性報告」相關通知的電子郵件信箱。

   注意

   設定電子郵件通知設定，以確保可成功地傳送電子郵件通知。如需詳細資訊，請參閱管理員通知設定 第 13-28 頁。

6. 指定預約時程。
7. 按一下「儲存」。

適用於未受管端點的安全性符合

「安全性符合」可查詢 OfficeScan 伺服器所屬網路中的未受管理端點。使用 Active Directory 和 IP 位址來查詢端點。

未受管理端點的安全狀態可以是下列任一種：

表 14-8. 未受管理端點的安全狀態

狀態	說明
受其他 OfficeScan 伺服器管理	電腦上安裝的 OfficeScan 用戶端由另一部 OfficeScan 伺服器管理。OfficeScan 用戶端已連線，並執行此版本 OfficeScan 或更舊的版本。
未安裝 OfficeScan 用戶端	電腦上未安裝 OfficeScan 用戶端。
無法連接	OfficeScan 伺服器無法連接該電腦並判斷其安全狀態。
無法解析的 Active Directory 評估	該電腦屬於 Active Directory 網域，但 OfficeScan 伺服器無法判斷其安全狀態。 注意 OfficeScan 伺服器資料庫包含伺服器所管理的用戶端清單。伺服器會在 Active Directory 中查詢電腦的 GUID，然後與儲存在資料庫中的 GUID 做比較。如果 GUID 不在資料庫中，便會將電腦歸類在「無法解析的 Active Directory 評估」類別下。

如果要執行安全性評估，請執行下列工作：

1. 定義查詢範圍。如需詳細資訊，請參閱定義 Active Directory/IP 位址範圍和查詢 第 14-61 頁。
2. 檢查查詢結果中未受保護的電腦。如需詳細資訊，請參閱檢視查詢結果 第 14-64 頁。
3. 安裝 OfficeScan 用戶端。如需詳細資訊，請參閱以安全性符合進行安裝 第 5-55 頁。
4. 設定預約查詢。如需詳細資訊，請參閱設定預約查詢評估 第 14-65 頁。

定義 Active Directory/IP 位址範圍和查詢

首次查詢時，請定義 Active Directory/IP 位址範圍，此範圍包含 OfficeScan 伺服器將依要求或定期查詢的 Active Directory 物件和 IP 位址。定義範圍之後，請啟動查詢程序。

注意

為定義 Active Directory 範圍，OfficeScan 必須先與 Active Directory 整合。如需有關整合的詳細資訊，請參閱 Active Directory 整合 第 2-26 頁。

程序

1. 瀏覽至「安全性符合 > 外部伺服器管理」。
2. 在「Active Directory/IP 位址範圍」區段中，按一下「定義」。接著會開啟一個新畫面。
3. 如果要定義 Active Directory 範圍：
   a. 移至「Active Directory 範圍」區段。
   b. 選取「使用依要求執行的評估」，執行即時查詢以獲得更準確的結果。關閉此選項會使得 OfficeScan 查詢資料庫，而非查詢每個 OfficeScan 用戶端。只查詢資料庫的速度比較快，但查詢結果比較不準確。
   c. 選取要查詢的物件。如果是首次查詢，請選取包含少於 1,000 個帳號的物件，然後記錄完成查詢所花的時間。使用此資料做為效能基準。
4. 如果要定義 IP 位址範圍：
   a. 移至「IP 位址範圍」區段。
   b. 選取「啟動 IP 位址範圍」。
   c. 指定 IP 位址範圍。按一下加號或減號按鈕以新增或刪除 IP 位址範圍。
   - 對於純 IPv4 OfficeScan 伺服器，請輸入 IPv4 位址範圍。
   - 對於純 IPv6 OfficeScan 伺服器，請輸入 IPv6 字首和長度。
   - 對於雙堆疊 OfficeScan 伺服器，請輸入 IPv4 位址範圍和（或）IPv6 字首和長度。

     IPv6 位址範圍的限制是 16 個位元，這與 IPv4 位址範圍的限制相同。因此，字首長度應該介於 112 到 128 之間。

表 14-9. IPv6 位址的字首長度和號碼

長度	IPv6 位址的號碼
128	2
124	16
120	256
116	4,096
112	65,536

5. 在「進階設定」下，指定 OfficeScan 伺服器用來與用戶端通訊的通訊埠。安裝 OfficeScan 伺服器期間，安裝程式會隨機產生通訊埠號碼。

   如果要檢視 OfficeScan 伺服器所使用的通訊埠，請移至「用戶端電腦 > 用戶端管理」，然後選取網域。通訊埠會顯示在「IP 位址」欄旁邊。趨勢科技建議您記下通訊埠號碼以備參考。

   a. 按一下「指定通訊埠」。

   b. 輸入通訊埠號碼，然後按一下「新增」。重複此步驟，直到新增所需的所有通訊埠號碼。

   c. 按一下「儲存」。

6. 如果要使用特定通訊埠號碼檢查電腦的連線，請選取「宣告無法與電腦連線，方法是檢查通訊埠 <x>」。如果無法建立連線，OfficeScan 會立即將該電腦視為無法連接。預設通訊埠號碼是 135。

   啟動此設定可加快查詢。無法建立與某部電腦的連線時，OfficeScan 伺服器不需要再執行所有其他連線驗證工作，就會將該電腦視為無法連接。

7. 如果要儲存範圍並啟動查詢，請按一下「儲存並重新評估」。如果只要儲存設定，請按一下「僅儲存」。「外部伺服器管理」畫面會顯示查詢的結果。

注意

查詢可能需要較長的時間才能完成，在查詢範圍較大時更是如此。請等到「外部伺服器管理」畫面顯示結果後，再執行另一次查詢。否則，目前的查詢作業階段會終止，而且查詢程序會重新啟動。

檢視查詢結果

查詢結果會出現在「安全狀態」區段下。未受管理的端點將具有下列其中一種狀態：

- 受其他 OfficeScan 伺服器管理
- 未安裝 OfficeScan 用戶端
- 無法連接
- 無法解析的 Active Directory 評估

建議的工作

1. 在「安全狀態」區段中，按一下數字連結以顯示所有受影響的電腦。
2. 使用搜尋和進階搜尋功能，搜尋並僅顯示符合搜尋條件的電腦。

   如果您使用進階搜尋功能，請指定下列項目：

   - IPv4 位址範圍
   - IPv6 字首和長度（字首應該介於 112 到 128 之間）
   - 電腦名稱
   - OfficeScan 伺服器名稱
   - Active Directory 樹狀結構
   - 安全狀態

   如果名稱不完整，OfficeScan 將不會傳回結果。如果不確定完整名稱，請使用萬用字元 (*)。

3. 如果要將電腦清單儲存到檔案，請按一下「匯出」。
4. 對於由另一部 OfficeScan 伺服器管理的 OfficeScan 用戶端，請使用 Client Mover 工具將這些 OfficeScan 用戶端變更為由目前的 OfficeScan 伺服器管理。如需有關此工具的詳細資訊，請參閱 Client Mover 第 14-20 頁。

設定預約查詢評估

設定 OfficeScan 伺服器定期查詢 Active Directory 和 IP 位址，以確保安全指導方針獲得實行。

程序

1. 瀏覽至「安全性符合 > 外部伺服器管理」。
2. 按一下用戶端樹狀結構頂端的「設定」。
3. 啟動預約查詢。
4. 指定預約時程。
5. 按一下「儲存」。

趨勢科技虛擬桌面支援

使用「趨勢科技虛擬桌面支援」最佳化虛擬桌面防護。此功能會調節位於單一虛擬伺服器上的 OfficeScan 用戶端工作。

在單一伺服器上執行多個桌面，以及依需求執行掃瞄或執行元件更新會耗用大量的系統資源。使用此功能可禁止用戶端同時執行掃瞄或更新元件。

例如，如果 VMware vCenter 伺服器有三個執行 OfficeScan 用戶端的虛擬桌面，OfficeScan 可以起始「立即掃瞄」並將更新同時部署到所有三個用戶端。「虛擬桌面支援」會辨識用戶端是否位於同一個實體伺服器。「虛擬桌面支援」允許先在第一個用戶端上執行工作，延後其他兩個用戶端上執行相同工作，直到第一個用戶端完成該工作為止。

您可以在下列平台上使用「虛擬桌面支援」：

- VMware vCenter™ (VMware View™)
- Citrix™ XenServer™ (Citrix XenDesktop™)
- Microsoft Hyper-V™ 伺服器

如需有關這些平台的詳細資訊，請參閱 VMware View、Citrix XenDesktop 或 Microsoft Hyper-V 網站。

使用「OfficeScan VDI 安裝前掃瞄範本產生工具」可最佳化依需求掃瞄或從基礎映像或模板映像中移除 GUID。

虛擬桌面支援安裝

「虛擬桌面支援」是 OfficeScan 內建的功能，但您必須另行為此功能取得使用授權。安裝 OfficeScan 伺服器之後，此功能就可用，但此功能無法運作。安裝此功能表示您必須從主動式更新伺服器（或自訂更新來源，如果已設定自訂更新來源）下載檔案。該檔案併入 OfficeScan 伺服器之後，您就可以註冊「虛擬桌面支援」以啟動其完整功能。您必須從 Plug-In Manager 執行安裝和註冊。

注意

純 IPv6 環境未完全支援「虛擬桌面支援」。如需詳細資訊，請參閱單純 IPv6 伺服器的限制 第 A-3 頁。

安裝虛擬桌面支援

程序

1. 開啟 OfficeScan Web 主控台，然後按一下主功能表中的「Plug-in Manager」。
2. 在「Plug-in Manager」畫面中，移至「趨勢科技虛擬桌面支援」區段，然後按一下「下載」。

   套件的大小會顯示在「下載」按鈕旁。

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

注意

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

3. 監控下載進度。下載期間您可以瀏覽其他畫面。

   如果在下載套件時遇到問題，請檢查 OfficeScan 產品主控台中的伺服器更新記錄檔。在主功能表上，按一下「記錄檔 > 伺服器更新記錄檔」。

   當 Plug-in Manager 下載該檔案之後，「虛擬桌面支援」會顯示在新畫面中。

   注意

   如果未顯示「虛擬桌面支援」，請參閱 Plug-In Manager 疑難排解 第 15-9 頁，以查知原因和解決方案。

4. 如果要立即安裝「虛擬桌面支援」，請按一下「立即安裝」。如果要稍後安裝：

   a. 按一下「稍後安裝」。

   b. 開啟「Plug-in Manager」畫面。

   c. 移至「趨勢科技虛擬桌面支援」區段，然後按一下「安裝」。

5. 閱讀授權合約，然後按一下「同意」表示您接受其中的條款。

   安裝便會開始。

6. 監控安裝進度。安裝之後，會顯示「虛擬桌面支援」的版本。

虛擬桌面支援使用授權

您可以從 Plug-In Manager 檢視、註冊和續約「虛擬桌面支援」使用授權。

請從趨勢科技取得啟動碼，然後用它來啟動「虛擬桌面支援」的完整功能。

註冊或續約「虛擬桌面支援」

程序

1. 開啟 OfficeScan Web 主控台，然後按一下主功能表中的「Plug-in Manager」。
2. 在 Plug-in Manager 畫面中，移至「趨勢科技虛擬桌面支援」區段，然後按一下「管理程式」。
3. 按一下「檢視使用授權資訊」。
4. 在開啟的「產品使用授權詳細資料」畫面中，按一下「新啟動碼」。
5. 在開啟的畫面中輸入「啟動碼」，然後按一下「儲存」。
6. 返回「產品使用授權詳細資料」畫面，按一下「更新資訊」重新整理該畫面，以便顯示新使用授權詳細資料和功能狀態。這個畫面也提供趨勢科技網站連結，按一下此連結即可檢視關於您的使用授權的詳細資訊。

檢視「虛擬桌面支援」的使用授權資訊

程序

1. 開啟 OfficeScan Web 主控台，並按一下主功能表中的 Plug-in Manager > [趨勢科技虛擬桌面支援] 管理程式。
2. 按一下「檢視使用授權資訊」。
3. 在開啟的畫面中檢視使用授權詳細資訊。

   「虛擬桌面支援使用授權詳細資料」區段提供下列資訊：

   - 狀態：顯示「已啟動」、「未啟動」或「已到期」。
   - 版本：顯示「完整版」或「試用版」。如果您同時擁有完整版和試用版，則會顯示的版本是「完整版」。

- 到期日：如果「虛擬桌面支援」有多個使用授權，會顯示最新的到期日。例如，如果使用授權到期日為 12/31/2010 和 06/30/2010，則會顯示 12/31/2010。
- 授權數目：顯示可使用「虛擬桌面支援」的 OfficeScan 用戶端數量。
- 啟動碼：顯示啟動碼

出現下列情況時顯示有關使用授權的提醒：

如果您有完整版使用授權：

- 在功能的寬限期內。寬限期視地區而定。請向您的趨勢科技銷售人員確認寬限期。
- 使用授權到期且經過寬限期以後。在這期間，您無法取得技術支援。

如果您有試用版使用授權

- 使用授權到期時。在這期間，您無法取得技術支援。

4. 按一下「線上檢視詳細的使用授權」，在趨勢科技網站上檢視您的使用授權相關資訊。
5. 如果要更新畫面以顯示最新的使用授權資訊，請按一下「更新資訊」。

虛擬伺服器連線

新增 VMware vCenter 4 (VMware View 4)、Citrix XenServer 5.5 (Citrix XenDesktop 4) 或 Microsoft Hyper-V 伺服器來最佳化依需求掃瞄或元件更新。OfficeScan 伺服器會與指定的虛擬伺服器通訊，以判定在相同實體伺服器上的 OfficeScan 用戶端。

新增伺服器連線

程序

1. 開啟 OfficeScan Web 主控台，並按一下主功能表中的 Plug-in Manager > [趨勢科技虛擬桌面支援] 管理程式。
2. 選取「VMware vCenter 伺服器」、「Citrix XenServer」、 或「Microsoft Hyper-V」。
3. 啟動與伺服器之間的連線。
4. 指定下列資訊：
   - 針對 VMware vCenter 和 Citrix XenServer 伺服器：
     - IP 位址
     - 通訊埠
     - 連線通訊協定（HTTP 或 HTTPS）
     - 使用者名稱
     - 密碼
   - 針對 Microsoft Hyper-V 伺服器：
     - 主機名稱或 IP 位址
     - 網域\使用者名稱

       注意
       登入帳號必須為管理員群組中的網域帳號
     - 密碼
5. 您可以視需要啟動 VMware vCenter 或 Citrix XenServer Proxy 伺服器連線。
   a. 指定 Proxy 伺服器名稱或 IP 位址，以及通訊埠。
   b. 如果 Proxy 伺服器需要驗證，請指定使用者名稱和密碼。

6. 按一下「測試連線」以驗證 OfficeScan 伺服器是否可成功連線至伺服器。

注意

如需疑難排解 Microsoft Hyper-V 連線的詳細資訊，請參閱 疑難排解 Microsoft Hyper-V 連線 第 14-72 頁。

7. 按一下「儲存」。

新增其他伺服器連線

程序

1. 開啟 OfficeScan Web 主控台，並按一下主功能表中的 Plug-in Manager > [趨勢科技虛擬桌面支援] 管理程式。
2. 按一下「新增 vCenter 連線」、「新增 XenServer 連線」或「新增 Hyper-V 連線」。
3. 重複以上步驟來提供適當的伺服器資訊。
4. 按一下「儲存」。

刪除連線設定

程序

1. 開啟 OfficeScan Web 主控台，並瀏覽至主功能表中的 Plug-in Manager > [趨勢科技虛擬桌面支援] 管理程式。
2. 按一下「刪除此連線」。
3. 按一下「確定」以確認刪除此設定。
4. 按一下「儲存」。

疑難排解 Microsoft Hyper-V 連線

Microsoft Hyper-V 連線會針對用戶端和伺服器間的通訊使用 Windows Management Instrumentation (WMI) 和 DCOM。防火牆策略可能會封鎖此通訊，而導致連線至 Hyper-V 伺服器失敗。

Hyper-V 伺服器監聽通訊埠會預設為通訊埠 135，然後會選擇一個隨機設定的通訊埠作為日後通訊之用。如果防火牆封鎖 WMI 傳輸或這兩個通訊埠的其中之一，則與伺服器的連線就會失敗。管理員可以修改防火牆策略，使與 Hyper-V 伺服器的通訊可以成功進行。

在進行下列防火牆修改前確認 IP 位址、網域\使用者名稱和密碼等所有連線設定皆正確。

允許透過 Windows 防火牆進行 WMI 通訊

程序

1. 在 Hyper-V 伺服器上，開啟「Windows 防火牆允許的程式」畫面。

   在 Windows 2008 R2 系統上，移至「控制面板 > 系統和安全 > Windows 防火牆 > 允許程式或功能透過 Windows 防火牆」。

2. 選取「Windows Management Instrumentation (WMI)」。

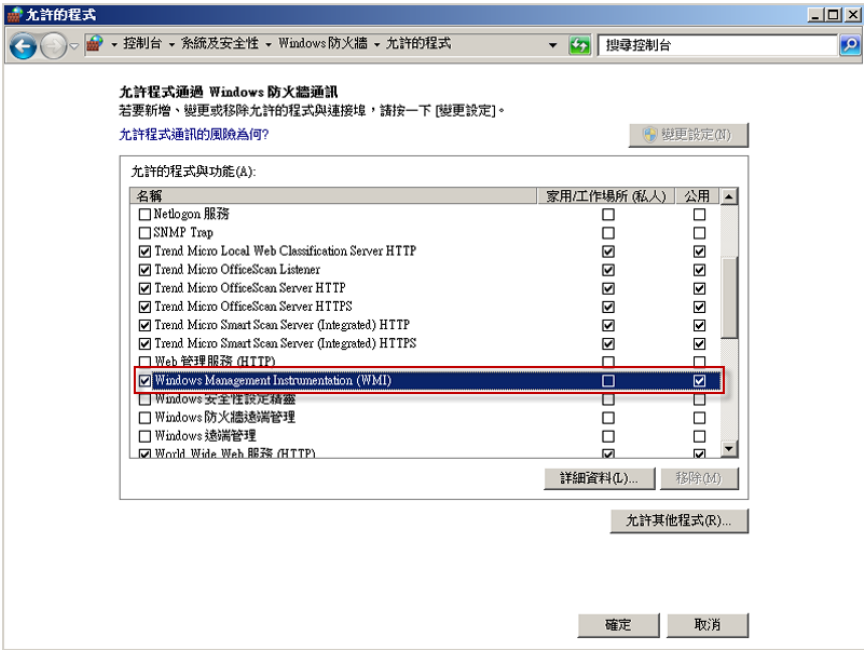


圖 14-7.「Windows 防火牆允許的程式」畫面

3. 按一下「儲存」。
4. 重新測試 Hyper-V 連線。

允許透過 Windows 防火牆或第三方防火牆開啟通訊埠通訊

程序

1. 在 Hyper-V 伺服器上確認防火牆允許透過通訊埠 135 進行通訊，並重新測試 Hyper-V 連線。

   如需開啟通訊埠的詳細資訊，請參閱您的防火牆文件。

2. 如果連線至 Hyper-V 伺服器失敗，則請設定 WMI 使用固定的通訊埠。

如需「*為 WMI 設定固定通訊埠*」，請參閱：

http://msdn.microsoft.com/en-us/library/windows/desktop/bb219447(v=vs.85).aspx

3. 開啟通訊埠 135 和新建立的固定通訊埠 (24158) 以透過防火牆進行通訊。
4. 重新測試 Hyper-V 連線。

VDI 安裝前掃瞄範本產生工具

使用「OfficeScan VDI 安裝前掃瞄範本產生工具」可最佳化依需求掃瞄或從基礎映像或模板映像中移除 GUID。此工具會掃瞄基礎或模板映像並認證該映像。掃瞄此映像的重複項時，OfficeScan 只會檢查發生變更的部分。這可確保縮短掃瞄時間。

秘訣

趨勢科技建議您在套用 Windows 更新或安裝新的應用程式後產生預先掃瞄範本。

建立安裝前掃瞄範本

程序

1. 在 OfficeScan 伺服器電腦上，瀏覽至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\TCacheGen。
2. 選擇 VDI 安裝前掃瞄範本產生工具的版本。下列是可以使用的版本：

表 14-10. VDI 安裝前掃瞄範本產生工具版本

檔案名稱	指示
TCacheGen.exe	如果您要直接在 32 位元平台上執行此工具，請選擇這個檔案。

檔案名稱	指示
TCacheGen_x64.exe	如果您要直接在 64 位元平台上執行此工具，請選擇這個檔案。
TCacheGenCli.exe	如果您要從 32 位元平台的命令列介面執行此工具，請選擇這個檔案。
TCacheGenCli_x64.exe	如果您要從 64 位元平台的命令列介面執行此工具，請選擇這個檔案。

3. 將您在上一個步驟中選擇之工具的版本複製到基礎映像的<用戶端安裝資料夾>。

4. 執行此工具。

   - 如果要直接執行工具：

     a. 按兩下 `TCacheGen.exe` 或 `TCacheGen_x64.exe`。

     b. 按一下「產生安裝前掃瞄範本」。

   - 如果要從命令列介面執行工具：

     a. 開啟命令提示字元，然後將目錄切換至<用戶端安裝資料夾>。

     b. 輸入下列命令：

     ```
     TCacheGenCli Generate_Template
     ```

     或者

     ```
     TcacheGenCli_x64 Generate_Template
     ```

注意

該工具會在產生安裝前掃瞄範本和移除 GUID 之前，先掃瞄映像是否有安全威脅。

產生安裝前掃瞄範本後，該工具會卸載 OfficeScan 用戶端。請勿重新載入 OfficeScan 用戶端。如果重新載入 OfficeScan 用戶端，則您需要再次建立安裝前掃瞄範本。

移除範本中的 GUID

程序

1. 在 OfficeScan 伺服器電腦上，瀏覽至 <伺服器安裝資料夾>\PCCSRV\Admin\Utility\TCacheGen。
2. 選擇 VDI 安裝前掃瞄範本產生工具的版本。下列是可以使用的版本：

   表 14-11. VDI 安裝前掃瞄範本產生工具版本

檔案名稱	指示
TCacheGen.exe	如果您要直接在 32 位元平台上執行此工具，請選擇這個檔案。
TCacheGen_x64.exe	如果您要直接在 64 位元平台上執行此工具，請選擇這個檔案。
TCacheGenCli.exe	如果您要從 32 位元平台的命令列介面執行此工具，請選擇這個檔案。
TCacheGenCli_x64.exe	如果您要從 64 位元平台的命令列介面執行此工具，請選擇這個檔案。

3. 將您在上一個步驟中選擇之工具的版本複製到基礎映像的<用戶端安裝資料夾>。
4. 執行此工具。
   - 如果要直接執行工具：
     a. 按兩下 TCacheGen.exe 或 TCacheGen_x64.exe。
     b. 按一下「移除範本中的 GUID」。
   - 如果要從命令列介面執行工具：
     a. 開啟命令提示字元，然後將目錄切換至<用戶端安裝資料夾>。
     b. 輸入下列命令：

        ```
        TCacheGenCli Remove GUID
        ```

        或者

```
TcacheGenCli_x64 Remove GUID
```

全域用戶端設定

OfficeScan 會套用全域用戶端設定到所有用戶端，或者只套用到具有特定權限的用戶端。

程序

1. 瀏覽至「用戶端電腦 > 全域用戶端設定」。
2. 設定下列設定：

表 14-12. 全域用戶端設定

設定	關係
掃瞄設定	全域掃瞄設定 第 7-62 頁
預約掃瞄設定	全域掃瞄設定 第 7-62 頁
病毒/惡意程式記錄檔頻寬設定	全域掃瞄設定 第 7-62 頁
防火牆設定	全域防火牆設定 第 12-23 頁
防火牆記錄檔數	全域防火牆設定 第 12-23 頁
行為監控設定	行為監控 第 8-2 頁
更新	作為 OfficeScan 用戶端更新來源的主動式更新伺服器 第 6-30 頁
保留磁碟空間	為 OfficeScan 用戶端更新設定保留磁碟空間 第 6-41 頁
無法連接的網路	無法連線到用戶端 第 14-38 頁
警訊設定	配置 OfficeScan 用戶端更新通知 第 6-43 頁

設定	關係
OfficeScan 服務重新啟動	OfficeScan 用戶端服務重新啟動 第 14-10 頁
Proxy 伺服器組態設定	適用於 OfficeScan 用戶端的自動 Proxy 伺服器設定 第 14-45 頁
偏好的 IP 位址	用戶端 IP 位址 第 5-8 頁

3. 按一下「儲存」。

設定用戶端權限及其他設定

授與使用者修改特定設定並在 OfficeScan 用戶端上執行高等級工作的權限。

注意

防毒設定僅會在啟動 OfficeScan 防毒功能之後才會顯示。

秘訣

如果要在整個組織中執行統一的設定和策略，請僅授與使用者有限的權限。

程序

1. 瀏覽至「 用戶端電腦 > 用戶端管理 」或「用戶端電腦 > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 ( ) 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「設定 > 權限和其他設定」。
4. 在「權限」標籤上，設定下列使用者權限：

表 14-13. 用戶端權限

用戶端權限	關係
行動權限	OfficeScan 用戶端行動權限 第 14-18 頁
掃瞄權限	掃瞄類型權限 第 7-48 頁
預約掃瞄權限	預約掃瞄權限和其他設定 第 7-51 頁
防火牆權限	防火牆權限 第 12-21 頁
行為監控權限	行為監控權限 第 8-8 頁
郵件掃瞄權限	郵件掃瞄權限和其他設定 第 7-57 頁
工具箱權限	授與使用者檢視工具箱標籤的權限 第 17-6 頁
Proxy 伺服器設定權限	用戶端的 Proxy 伺服器設定權限 第 14-44 頁
元件更新權限	OfficeScan 用戶端的更新權限和其他設定 第 6-39 頁
解除安裝	授與 OfficeScan 用戶端解除安裝權限 第 5-66 頁
卸載	授與用戶端卸載權限 第 14-17 頁

5. 按一下「其他設定」標籤並設定下列設定：

表 14-14. 其他用戶端設定

設定	關係
更新設定	OfficeScan 用戶端的更新權限和其他設定 第 6-39 頁
網頁信譽評等設定	用戶端使用者的網路安全威脅通知 第 11-9 頁
行為監控設定	行為監控權限 第 8-8 頁
本機自我保護	本機自我保護 第 14-11 頁
用於掃瞄的快取設定	用於掃瞄的快取設定 第 7-59 頁

設定	關係
預約掃瞄設定	授與預約掃瞄權限並顯示權限通知 第 7-52 頁
用戶端安全設定	OfficeScan 用戶端安全 第 14-15 頁
POP3 電子郵件掃瞄設定	授與郵件掃瞄權限和啟動 POP3 郵件掃瞄 第 7-59 頁
用戶端主控台存取限制	OfficeScan 用戶端主控台存取限制 第 14-16 頁
重新啟動通知	OfficeScan 用戶端使用者的安全威脅通知 第 7-76 頁

6. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

部分 IV

提供其他防護

第 15 章

使用 Plug-In Manager

本章討論如何設定 Plug-In Manager，並提供透過 Plug-In Manager 提供之嵌入程式解決方案的總覽。

本章內容：

關於 Plug-In Manager

OfficeScan 包括一個名為 Plug-In Manager 的架構，可以將新的解決方案整合到既有的 OfficeScan 環境。為有效簡化這些解決方案的管理，Plug-In Manager 以 Widget 的形式提供解決方案的概覽資料。

注意

當前沒有任何嵌入解決方案支援 IPv6。伺服器可下載這些解決方案，但無法將其部署到純 IPv6 OfficeScan 用戶端或純 IPv6 主機。

Plug-In Manager 提供了兩種類型的解決方案：

- 本機 OfficeScan 功能

  有些本機 OfficeScan 功能會單獨授權，並透過 Plug-In Manager 啟用。在本版本中，有兩種功能屬於此類別，名稱分別是趨勢科技虛擬桌面支援和 OfficeScan 資料安全防護。

- Plug-in 程式

  Plug-in 程式不屬於 OfficeScan 程式。這些程式具有其自己的授權，且主要透過其自己的管理主控台（可從 OfficeScan Web 主控台內存取）進行管理。嵌入程式的範例包括 Intrusion Defense Firewall、Trend Micro Security（適用於 Mac）以及趨勢科技手機防護精靈。

本文件提供了 Plug-in 程式安裝和管理的一般概述，並討論了 Widget 中可用的 Plug-in 資料。如需設定和管理程式的詳細資訊，請參閱特定 Plug-in 程式的文件。

用戶端代理程式和用戶端 Plug-in Manager

一些嵌入程式（如 Intrusion Defense Firewall）具有安裝在 Windows 作業系統中的用戶端代理程式。您可以透過以程序名稱 `CNTAoSMgr.exe` 執行的用戶端 Plug-in Manager 管理用戶端代理程式。

CNTAoSMgr.exe 會隨 OfficeScan 用戶端一起安裝，兩者的系統需求相同。對 CNTAoSMgr.exe 唯一的其他需求是 Microsoft XML Parser (MSXML) 3.0 版或更新版本。

注意

其他的用戶端代理程式不會安裝在 Windows 作業系統中，因此無法從用戶端 Plug-in Manager 進行管理。Trend Micro Security（適用於 Mac）用戶端和趨勢科技手機防護精靈的行動裝置代理程式是這些代理程式的範例。

Widget

使用 Widget 可檢視已部署的各個嵌入程式解決方案的概覽資料。OfficeScan 伺服器的「摘要」管理平台上提供了 Widget。一個名為 OfficeScan 和 Plug-ins 混搭 的特殊 Widget 會將 OfficeScan 用戶端和 Plug-in 解決方案中的資料結合，然後將資料顯示在用戶端樹狀結構中。

本管理手冊概述了 Widget 以及支援 Widget 的解決方案。

Plug-In Manager 安裝

在先前的 Plug-In Manager 版本中，Plug-In Manager 安裝套件會從趨勢科技主動式更新伺服器中下載，然後安裝在裝載 OfficeScan 伺服器的電腦上。在此版本中，安裝套件包含在 OfficeScan 伺服器安裝套件中。

剛接觸 OfficeScan 的新使用者在執行安裝套件並完成安裝之後，會同時安裝 OfficeScan 伺服器和 Plug-In Manager。升級至此 OfficeScan 版本且之前已使用 Plug-In Manager 的使用者需要先停止 Plug-In Manager 服務，然後再執行安裝套件。

執行安裝後的工作

在安裝 Plug-In Manager 之後請執行以下操作：

程序

1. 透過在 OfficeScan Web 主控台的主畫面上按一下 Plug-In Manager 來存取 Plug-in Manager Web 主控台。
2. 管理嵌入程式解決方案。
3. 存取 OfficeScan Web 主控台上的「摘要」資訊平台以管理用於嵌入程式解決方案的 Widget。

本機 OfficeScan 功能管理

本機 OfficeScan 功能會隨 OfficeScan 一起安裝，並從 Plug-In Manager 啟用。有些功能（如趨勢科技虛擬桌面支援）是從 Plug-In Manager 管理的，而有些功能（如 OfficeScan 資料安全防護）則從 OfficeScan Web 主控台進行管理。

管理嵌入程式

OfficeScan 的嵌入程式獨立安裝和啟動。每個嵌入程式均提供自己的主控台來進行產品管理。可以從 OfficeScan Web 主控台存取管理主控台。

Plug-in 程式安裝

嵌入程式會顯示在 Plug-In Manager 主控台上。可以使用主控台下載、安裝及管理該程式。Plug-in Manager 從趨勢科技主動式更新伺服器或自訂更新來源（如果已正確設定）下載嵌入程式的安裝套件。必須有 Internet 連線，才能從主動式更新伺服器下載套件。

當 Plug-In Manager 下載安裝套件或開始安裝時，Plug-In Manager 會暫時關閉其他的嵌入程式功能，例如下載、安裝和升級。

Plug-In Manager 不支援從 Trend Micro Control Manager 的單一登入功能進行嵌入程式安裝或管理。

安裝嵌入程式

程序

1. 開啟 OfficeScan Web 主控台，然後按一下主功能表中的「Plug-in Manager」。
2. 在 Plug-in Manager 畫面中，移到嵌入程式區段，然後按一下「下載」。嵌入程式套件的大小會顯示在「下載」按鈕旁邊。Plug-in Manager 將下載套件儲存到<伺服器安裝資料夾>\PCCSRV\Download\Product
3. 監控下載進度。下載期間您可以瀏覽其他畫面。

圖 15-1. 嵌入程式的下載進度

Plug-in Manager 下載套件之後，嵌入程式就會顯示在新畫面中。

注意

如果在下載套件時遇到問題，請檢查 OfficeScan 產品主控台中的伺服器更新記錄檔。在主功能表上，按一下「記錄檔 > 伺服器更新記錄檔」。

4. 按一下「立即安裝」或「稍後安裝」。
   - 如果按下了「立即安裝」，請查看安裝進度。
   - 如果按下了「稍後安裝」，請存取「Plug-in Manager」畫面，移至嵌入程式區段，按一下「安裝」，然後查看安裝進度。

安裝後，將顯示目前嵌入程式的版本。然後，即可開始管理嵌入程式。

Plug-in 程式管理

從嵌入程式的管理主控台（可透過 OfficeScan Web 主控台存取）進行設定並執行與程式相關的工作。工作包括啟用程式並將其用戶端代理程式部署到端點。如需設定和管理程式的詳細資訊，請參閱特定 plug-in 程式的文件。

管理嵌入程式

程序

1. 開啟 OfficeScan Web 主控台，然後按一下「Plug-in Manager」。
2. 在「Plug-in Manager」畫面中，移至嵌入程式區段，然後按一下「管理程式」。

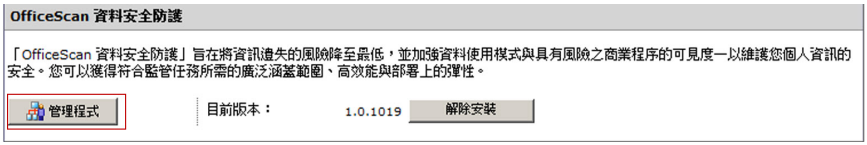


圖 15-2. Plug-in 程式的「管理程式」按鈕

Plug-in 程式更新

安裝的新版本嵌入程式會顯示在 Plug-In Manager 主控台上。您可以在主控台上下載升級套件，然後升級該程式。Plug-In Manager 會從趨勢科技主動式更新伺服器或自訂更新來源（如果已正確設定）下載套件。必須有 Internet 連線，才能從主動式更新伺服器下載套件。

當 Plug-In Manager 下載安裝套件或開始升級時，Plug-In Manager 會暫時關閉其他的嵌入程式功能，例如下載、安裝和升級。

Plug-In Manager 不支援從 Trend Micro Control Manager 的單一登入功能進行嵌入程式升級。

升級嵌入程式

程序

1. 開啟 OfficeScan Web 主控台，然後按一下主功能表中的「Plug-in Manager」。
2. 在 Plug-in Manager 畫面中，移到嵌入程式區段，然後按一下「下載」。升級套件的大小會顯示在「下載」按鈕旁。
3. 監控下載進度。在下載期間，您可瀏覽其他畫面，而不會影響升級作業。

注意

如果在下載套件時發生問題，請檢查 OfficeScan Web 主控台中的伺服器更新記錄檔。在主功能表上，按一下記錄檔 > 伺服器更新記錄檔。

4. Plug-In Manager 下載套件後，會顯示一個新畫面。
5. 按一下「立即升級」或「稍後升級」。
   - 如果按下了「立即升級」，請查看升級進度。
   - 如果按下了「稍後升級」，請存取「Plug-in Manager」畫面，移至嵌入程式區段，按一下「升級」，然後查看升級進度。

升級後，Plug-In Manager 服務可能需要重新啟動，這會導致「Plug-In Manager」畫面暫時不可用。該畫面可用時，將顯示目前嵌入程式版本。

Plug-in 程式解除安裝

有多種方法可解除安裝 Plug-in 程式。

- 從 Plug-In Manager 主控台解除安裝嵌入程式。

- 解除安裝 OfficeScan 伺服器同時也會解除安裝 Plug-In Manager 和所有伺服器嵌入程式。如需有關解除安裝 OfficeScan 伺服器的指示，請參閱*《OfficeScan 安裝和升級手冊》*。

對於具有用戶端代理程式的嵌入程式：

- 請參閱嵌入程式的文件，以查看解除安裝嵌入程式是否也將解除安裝用戶端代理程式。
- 對於安裝在已安裝 OfficeScan 用戶端的電腦上的用戶端代理程式，解除安裝 OfficeScan 用戶端也將解除安裝用戶端代理程式和用戶端 Plug-in Manager (`CNTAoSMgr.exe`)。

從 Plug-In Manager 主控台解除嵌入程式

程序

1. 開啟 OfficeScan Web 主控台，然後按一下主功能表中的「Plug-in Manager」。
2. 在「Plug-in Manager」畫面中，移至嵌入程式區段，然後按一下「管理程式」。

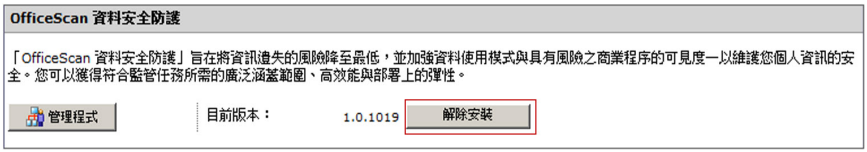


圖 15-3. 嵌入程式的「解除安裝」按鈕

3. 監控解除安裝進度。解除安裝期間您可以瀏覽其他畫面。
4. 解除安裝之後，請重新整理 Plug-in Manager 畫面。Plug-in 程式再次可供安裝。

解除安裝 Plug-In Manager

解除安裝 OfficeScan 伺服器同時也會解除安裝 Plug-In Manager 和所有伺服器嵌入程式。如需有關解除安裝 OfficeScan 伺服器的指示，請參閱*《OfficeScan 安裝和升級手冊》*。

Plug-In Manager 疑難排解

檢查 OfficeScan 伺服器和 OfficeScanPlug-In Manager 的用戶端偵錯記錄，以及嵌入程式偵錯資訊。

Plug-in 程式不顯示在 Plug-in Manager 主控台上

可供下載和安裝的嵌入程式可能會因以下原因而無法顯示在 Plug-In Manager 主控台上：

程序

1. Plug-In Manager 仍在下載嵌入程式。如果程式的套件大小較大，可能要花些時間。請時時檢查畫面，以查看 Plug-in 程式是否有顯示。

   注意

   如果 Plug-In Manager 無法下載嵌入程式，則會在 24 個小時後自動重新下載。如果要手動觸發 Plug-In Manager 下載嵌入程式，請重新啟動 OfficeScan Plug-In Manager 服務。

2. 伺服器電腦無法連線到 Internet。如果伺服器電腦是透過 Proxy 伺服器連線到 Internet，請確定是否能夠使用 Proxy 伺服器設定建立 Internet 連線。

3. OfficeScan 更新來源不是主動式更新伺服器。在 OfficeScan Web 主控台中，移至「更新 > 伺服器 > 更新來源」，然後檢查更新來源。如果更新來源不是主動式更新伺服器，您會有下列選擇：

   - 選取主動式更新伺服器做為更新來源。

- 如果選取「其他更新來源」，請先在「其他」更新來源清單中選取第一個項目做為更新來源，並且確認它可以成功連線到主動式更新伺服器。Plug-In Manager 僅支援清單中的第一個項目。
- 如果選取「包含目前檔案副本的 Intranet 位置」，請確定 Intranet 中的電腦也能連線到主動式更新伺服器。

用戶端代理程式安裝和顯示問題

由於以下原因，安裝嵌入程式的用戶端代理程式可能會失敗，或代理程式可能無法顯示在 OfficeScan 用戶端主控台上：

程序

1. 用戶端 Plug-in Manager (`CNTAosMgr.exe`) 未執行。在 OfficeScan 用戶端電腦上，開啟 Windows 工作管理員並執行 `CNTAosMgr.exe` 處理程序。
2. 未將用戶端代理程式的安裝套件下載至`<用戶端安裝資料夾>\AU_Data\AU_Temp\{xxx}AU_Down\Product` 中的 OfficeScan 用戶端電腦資料夾。請檢查位於 `\AU_Data\AU_Log\` 中的 `Tmudump.txt` 以瞭解下載失敗原因。

   注意

   如果成功安裝代理程式，則 `<用戶端安裝資料夾>\AOSSvcInfo.xml` 中包含代理程式資訊。
3. 代理程式安裝失敗或需要進一步動作。可從嵌入程式的管理主控台檢查安裝狀態，並執行作業，如在安裝後重新啟動 OfficeScan 用戶端電腦或在安裝前安裝必需的作業系統 Patch。

不支援 Apache Web Server 版本

Plug-In Manager 會使用 Internet Server Application Programming Interface (ISAPI) 處理部分的 Web 要求。ISAPI 和 Apache Web Server 2.0.56 版到 2.0.59 版及 2.2.3 版到 2.2.4 版不相容。

如果 Apache Web Server 執行任何不相容的版本，您可以將其取代為 2.0.63 版，也就是 OfficeScan 和 Plug-In Manager 所使用的版本。此版本也與 ISAPI 相容。

程序

1. 將 OfficeScan 伺服器升級至目前版本。
2. 備份下列位於<伺服器安裝資料夾>中 Apache2 資料夾的檔案：
   - `httpd.conf`
   - `httpd.conf.tmbackup`
   - `httpd.default.conf`
3. 從「新增/移除程式」畫面解除安裝不相容的 Apache Web Server 版本。
4. 安裝 Apache Web Server 2.0.63。
   a. 從<伺服器安裝資料夾>`\Admin\Utility\Apache` 啟動 apache.msi。
   b. 在「伺服器資訊」畫面中，輸入必要的資料。
   c. 在「目標資料夾」畫面中，按一下「變更」並瀏覽到 `<OfficeScan` 伺服器安裝資料夾> 來變更目標資料夾。
   d. 完成安裝。
5. 將備份檔案複製回 Apache2 資料夾。
6. 重新啟動 Apache Web Server 服務。

如果 Internet Explorer 上的「自動組態設定程式檔設定」重新導向到 Proxy 伺服器，則用戶端代理程式無法啟動

由於用戶端代理程式啟動命令重新導向到 Proxy 伺服器，因此用戶端 Plug-in Manager (`CNTAosMgr.exe`) 無法啟動該代理程式。這個問題只有在 Proxy 伺服器設定將使用者的 HTTP 傳輸重新導向至 127.0.0.1 時才會發生。

如果要解決該問題，請使用定義明確的 Proxy 伺服器策略。例如，勿將 HTTP 傳輸重新導向至 127.0.0.1。

如果您需要使用控制 127.0.0.1 HTTP 要求的 Proxy 伺服器組態設定，請執行下列工作。

程序

1. 在 OfficeScan Web 主控台上設定 OfficeScan 防火牆設定值。

   注意

   只有在 OfficeScan 用戶端啟動 OfficeScan 防火牆時，才執行這個步驟。

   a. 在 Web 主控台上，移至「用戶端電腦 > 防火牆 > 策略」，然後按一下「編輯例外範本」。

   b. 在「編輯例外範本」畫面，按一下「新增」。

   c. 使用下列資訊：

      - 名稱：您偏好的名稱
      - 處理行動：允許網路流量
      - 方向：入站
      - 通訊協定：TCP
      - 通訊埠：介於 5000 和 49151 之間的通訊埠號碼

d. IP 位址：選取「 單一 IP 位址 」並指定您的 Proxy 伺服器 IP 位址（建議選項）或選取「 所有 IP 位址 」。

e. 按一下「儲存」。

f. 返回「編輯例外範本」畫面，按一下「儲存並且套用到現有策略」。

g. 移至「用戶端電腦 > 防火牆 > 資料檔」，然後按一下「指定資料檔給用戶端」。

如果沒有防火牆資料檔，按一下「新增」即可建立。使用下列設定：

- 名稱：您偏好的名稱
- 說明：您偏好的說明
- 策略：所有存取策略

儲存新的資料檔之後，按一下「指定資料檔給用戶端」。

2. 修改 `ofcscan.ini` 檔案。

a. 使用文字編輯器開啟 <伺服器安裝資料夾> 中的 `ofcscan.ini` 檔案。

b. 搜尋 **`[Global Setting]`**，然後將 `FWPortNum=21212` 新增到下一行。將「21212」變更為您在上述步驟 c 中指定的通訊埠號碼。

例如：

```
[Global Setting]

FWPortNum=5000
```

c. 儲存檔案。

3. 在 Web 主控台上，移至「用戶端電腦 > 全域用戶端設定」，然後按一下「 儲存 」。

系統、更新模組或 Plug-in Manager 程式中發生錯誤，且錯誤訊息提供特定錯誤碼

Plug-In Manager 將在錯誤訊息中顯示以下任何錯誤碼。如果您在參考下表中提供的解決方案後無法解決問題，請聯絡您的經銷商。

表 15-1. Plug-In Manager 錯誤碼

錯誤碼	訊息、原因和解決方案
001	Plug-In Manager 程式中發生錯誤。 查詢更新工作進度時，Plug-In Manager 更新模組無回應。模組或命令處理常式可能尚未初始化。 重新啟動 OfficeScan Plug-In Manager 服務，然後重新執行此工作。
002	發生系統錯誤。 Plug-In Manager 更新模組無法開啟登錄機碼 `SOFTWARE\TrendMicro\OfficeScan\service\AoS`，因為該機碼已被刪除。 執行下列步驟： 1. 開啟登錄編輯程式，然後瀏覽到 `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service\AoS\OSCE_Addon_Service_CompList_Version`。將值重設為 1.0.1000。 2. 重新啟動 OfficeScan Plug-In Manager 服務。 3. 下載/解除安裝嵌入程式。

錯誤碼	訊息、原因和解決方案
028	發生更新錯誤。 可能原因： • Plug-In Manager 更新模組無法下載嵌入程式。確認網路連線正常，然後再試一次。 • 由於 AU Patch 代理程式傳回錯誤，因此 Plug-In Manager 更新模組無法安裝嵌入程式。AU Patch 代理程式是一種程式，可以啟動新 Plug-in 程式的安裝作業。如需錯誤的確切原因，請檢查 `\PCCSRV\Web\Service\AU_Data\AU_Log` 中的主動式更新模組偵錯記錄檔 `TmuDump.txt`。 執行下列步驟： 1. 開啟登錄編輯程式，然後瀏覽到 `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service\AoS\OSCE_Addon_Service_CompList_Version`。將值重設為 1.0.1000。 2. 刪除此嵌入程式登錄機碼 `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_ADDON_xxxx`。 3. 重新啟動 OfficeScan Plug-In Manager 服務。 4. 下載並安裝嵌入程式。
170	發生系統錯誤。 Plug-In Manager 更新模組目前正在處理另一項作業，因此無法處理輸入作業。 請稍後執行此工作。
202	Plug-In Manager 程式中發生錯誤。 Plug-In Manager 程式無法處理正在 Web 主控台上執行的工作。 如果程式有升級可用，請重新整理 Web 主控台或升級 Plug-In Manager。
203	Plug-In Manager 程式中發生錯誤。 嘗試與 Plug-In Manager 後端服務通訊時，Plug-In Manager 程式發生處理程序間通訊 (IPC) 錯誤。 重新啟動 OfficeScan Plug-In Manager 服務，然後重新執行此工作。

錯誤碼	訊息、原因和解決方案
其他錯誤碼	發生系統錯誤。 下載新的嵌入程式時，Plug-In Manager 將檢查主動式更新伺服器中的嵌入程式清單。Plug-In Manager 無法取得此清單。 執行下列步驟： 1. 開啟登錄編輯程式，然後瀏覽到 `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service\AoS\OSCE_Addon_Service_CompList_Version`。將值重設為 `1.0.1000`。 2. 重新啟動 OfficeScan Plug-In Manager 服務。 3. 下載並安裝嵌入程式。

第 16 章

使用 Policy Server for Cisco NAC

本章包含安裝和設定策略伺服器 for Cisco NAC 的基本指示。如需有關設定和管理 Cisco Secure ACS 伺服器和其他 Cisco 產品的詳細資訊，請參閱下列網站提供的最新 Cisco 文件：

http://www.cisco.com/univercd/home/home.htm

本章內容：

關於 Policy Server for Cisco NAC

Trend Micro Policy Server for Cisco Network Admission Control (NAC) 會評估 OfficeScan 用戶端上的防毒元件狀態。策略伺服器組態設定選項可讓您進行一些設定以便在有風險的用戶端上執行中毒處理行動，讓這些用戶端符合組織的安全計畫。

這些中毒處理行動包括下列項目：

- 指示 OfficeScan 用戶端電腦更新其 OfficeScan 用戶端元件
- 啟動即時掃瞄
- 執行立即掃瞄
- 在 OfficeScan 用戶端電腦上顯示通知訊息，以通知使用者發生防毒策略違規

如需有關 Cisco NAC 技術的其他資訊，請瀏覽 Cisco 網站，網址為：

http://www.cisco.com/go/nac

元件和術語

下列是您要瞭解和使用 Policy Server for Cisco NAC 時所需熟悉的各種元件和重要術語清單。

元件

下列是趨勢科技在執行 Policy Server for Cisco NAC 時的必要元件：

表 16-1. 策略伺服器 for Cisco NAC 元件

元件	說明
Cisco Trust Agent (CTA)	安裝在用戶端電腦上的程式，可讓電腦與其他 Cisco NAC 元件進行通訊
OfficeScan 用戶端電腦	安裝了 OfficeScan 用戶端程式的電腦。如果要使用 Cisco NAC，OfficeScan 用戶端電腦也必須有 Cisco Trust Agent。
網路存取裝置	支援 Cisco NAC 功能的網路裝置。支援的「網路存取裝置」包括各種 Cisco 路由器、防火牆和無線網路存取點，以及具有「終端機存取控制器存取控制系統」(TACACS+) 或「遠端撥號使用者服務」(RADIUS) 通訊協定的協力廠商裝置。 如需支援的裝置清單，請參閱支援的平台和需求 第 16-19 頁。
Cisco Secure Access Control Server (ACS)	透過「網路存取裝置」從用戶端接收 OfficeScan 用戶端防毒資料，並將它傳送至外部使用者資料庫進行評估的伺服器。稍後在此程序中，ACS 伺服器還會將評估結果（其中可能包括 OfficeScan 用戶端的指示）傳送至「網路存取裝置」。
策略伺服器	接收和評估 OfficeScan 用戶端防毒資料的程式。執行評估之後，策略伺服器會決定 OfficeScan 用戶端應執行的中毒處理行動，然後通知 OfficeScan 用戶端執行這些中毒處理行動。
OfficeScan 伺服器	會向策略伺服器回報目前的「病毒碼」和「病毒掃瞄引擎」版本，策略伺服器會使用這項資訊評估 OfficeScan 用戶端的防毒狀態。

術語

熟悉下列與 Policy Server for Cisco NAC 相關的術語：

表 16-2. Policy Server for Cisco NAC 術語

術語	定義
安全狀況	防毒軟體在 OfficeScan 用戶端上的呈現方式和現狀。在此實作中，安全狀況是指用戶端電腦上是否有 OfficeScan 用戶端程式、特定 OfficeScan 用戶端設定的狀態，以及「病毒掃瞄引擎」和「病毒碼」是否為最新狀態。

術語	定義
狀況 Token	策略伺服器在 OfficeScan 用戶端驗證之後所建立。它包括通知 OfficeScan 用戶端執行一組指定的中毒處理行動（例如：啟動「即時掃瞄」或更新防毒元件）的資訊。
用戶端驗證	評估用戶端安全狀況並將狀況 Token 傳回至 OfficeScan 用戶端的程序
策略伺服器規則	包含策略伺服器用來衡量 OfficeScan 用戶端安全狀況的可設定條件的指導方針。規則還會包含安全狀況資訊符合條件時，OfficeScan 用戶端和策略伺服器應執行的中毒處理行動（如需詳細資訊，請參閱策略伺服器策略和規則 第 16-9 頁）。
策略伺服器策略	策略伺服器對照以衡量 OfficeScan 用戶端安全狀況的一組規則。策略還包含與策略相關聯規則中的條件不符合安全狀況時，OfficeScan 用戶端和策略伺服器應執行的中毒處理行動（如需詳細資訊，請參閱策略伺服器策略和規則 第 16-9 頁）。
驗證、授權和計算 (AAA)	說明三種主要服務，用來控制使用者 OfficeScan 用戶端對電腦資源的存取。驗證是指識別用戶端，通常是藉由使用者輸入使用者名稱和密碼的方式。授權是指使用者所擁有發出特定命令的權限。計算是指一種在作業階段期間用來計算資源的方法，通常會保存在記錄檔中。Cisco Secure Access Control Server (ACS) 即為 Cisco 的 AAA 伺服器實作。
憑證授權單位 (CA)	一種授權，位於散佈數位憑證的網路上，其目的在於執行驗證和保護電腦和（或）伺服器之間連線的安全。
數位憑證	基於安全用途的附件。最常見的是，憑證在伺服器（例如：Web 伺服器）上驗證用戶端，且包含下列各項：使用者身分資訊、公開金鑰（用於加密）和憑證授權單位 (CA) 的數位簽章，以確認憑證有效。
遠端驗證撥號使用者服務 (RADIUS)	需要用戶端輸入使用者名稱和密碼的驗證系統。Cisco Secure ACS 伺服器支援 RADIUS。
終端機存取控制器存取控制系統 (TACACS+)	透過 AAA 命令啟動的安全通訊協定，用於驗證使用者用戶端。Cisco ACS 伺服器支援 TACACS+。

Cisco NAC 架構

下圖說明基本 Cisco NAC 架構。

圖 16-1. 基本 Cisco NAC 架構

此圖中的 OfficeScan 用戶端已安裝 CTA，而且只能透過支援 Cisco NAC 的「網路存取裝置」存取網路。「網路存取裝置」位於用戶端和其他 Cisco NAC 元件之間。

注意

您的網路架構可能會根據 Proxy 伺服器、路由器或防火牆的呈現方式而有所不同。

用戶端驗證流程

OfficeScan 用戶端驗證是指評估 OfficeScan 用戶端的安全狀況，並且在策略伺服器認為用戶端有風險時，傳回指示給 OfficeScan 用戶端執行的程序。策略伺服器會使用可設定的規則和策略驗證 OfficeScan 用戶端。

下列是 OfficeScan 用戶端嘗試存取網路時所發生的事件流程：

1. Cisco「網路存取裝置」會在用戶端嘗試存取網路時要求用戶端的安全狀況，藉此開始進行驗證流程。
2. 「網路存取裝置」之後會將安全狀況傳送到 ACS 伺服器。
3. ACS 伺服器會將安全狀況傳送到策略伺服器，使其執行評估。
4. 在另一項處理程序中，策略伺服器會定期輪詢 OfficeScan 伺服器中的「病毒碼」和「病毒掃瞄引擎」版本資訊，以使其資料維持最新狀態。然後它會使用您設定的策略將這項資訊和 OfficeScan 用戶端安全狀況資料進行比較。
5. 接著，策略伺服器會建立狀況 Token 並將其傳回 OfficeScan 用戶端。

6. OfficeScan 用戶端會執行狀況 Token 中設定的處理行動。

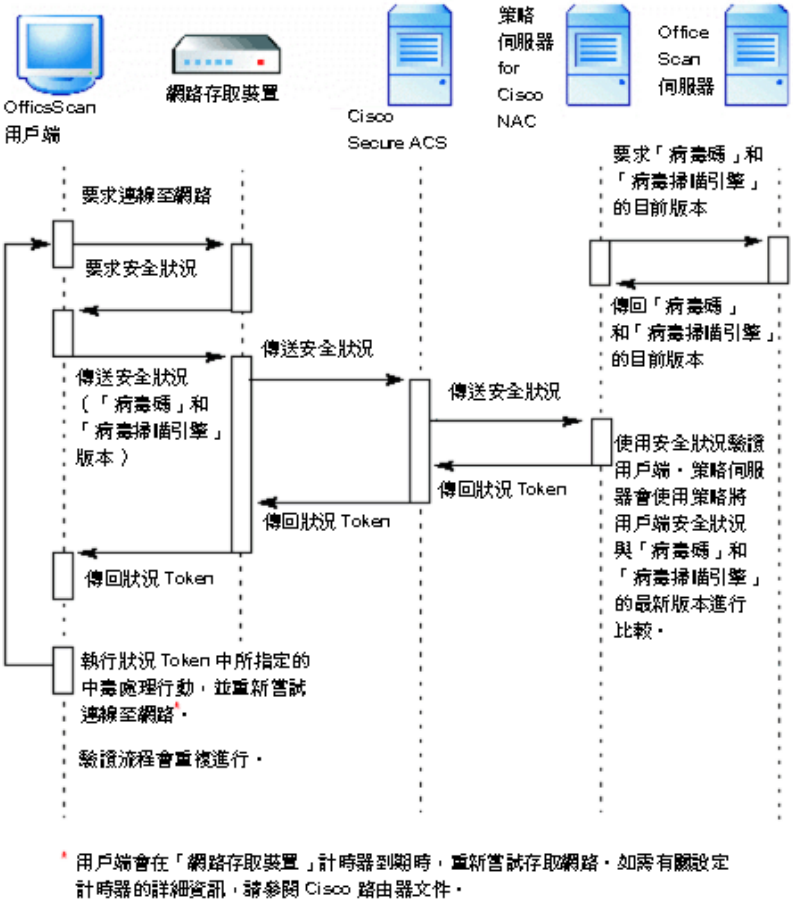


圖 16-2. 網路存取驗證流程

策略伺服器

策略伺服器負責評估 OfficeScan 用戶端的安全狀況，並建立狀況 Token。它會將安全狀況與從 OfficeScan 用戶端為其成員的 OfficeScan 伺服器接收的最新版「病毒碼」和「病毒掃瞄引擎」進行比較。也會將狀況 Token 傳回 Cisco Secure ACS 伺服器，然後伺服器會將其從 Cisco「網路存取裝置」傳送到 OfficeScan 用戶端。

在單一網路上安裝其他策略伺服器可以增進大量用戶端同時嘗試存取網路時的效能，這些策略伺服器也可在某部策略伺服器故障時做為備份使用。如果一個網路上有多部 OfficeScan 伺服器，策略伺服器會處理所有已向其註冊的 OfficeScan 伺服器的要求。同樣地，多部策略伺服器可處理已向所有策略伺服器註冊的單一 OfficeScan 伺服器的要求。下圖說明多部 OfficeScan 伺服器與策略伺服器之間的關係。

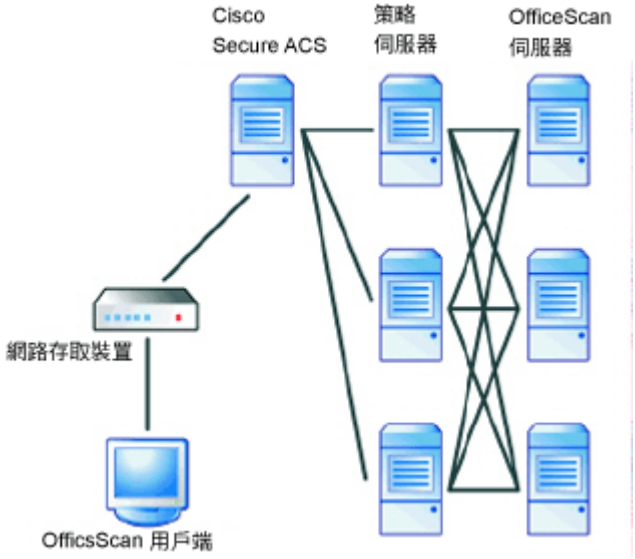


圖 16-3. 多部策略伺服器/OfficeScan 伺服器之間的關係

您也可以在與安裝 OfficeScan 伺服器相同的電腦上安裝策略伺服器。

策略伺服器策略和規則

策略伺服器會使用可設定的規則和策略協助您執行組織的安全指導方針。

規則包括策略伺服器用來與 OfficeScan 用戶端安全狀況比較的特定條件。如果用戶端安全狀況符合您在規則中設定的條件，則用戶端和伺服器會執行您在規則中指定的中毒處理行動（請參閱策略伺服器和 OfficeScan 用戶端處理行動 第 16-10 頁）。

策略包括一或多個規則。請同時針對病毒爆發模式和一般模式，為網路上每一部註冊的 OfficeScan 伺服器各指定一個策略（如需有關網路模式的詳細資訊，請參閱安全威脅爆發 第 7-89 頁）。

如果 OfficeScan 用戶端安全狀況符合屬於策略的規則中的條件，則 OfficeScan 用戶端會執行您在規則中設定的中毒處理行動。不過，如果 OfficeScan 用戶端安全狀況不符合與策略相關聯的任何規則中的任何條件，您仍然可以在策略中配置 OfficeScan 用戶端和伺服器要執行的預設處理行動（請參閱策略伺服器和 OfficeScan 用戶端處理行動 第 16-10 頁）。

秘訣

如果要讓 OfficeScan 網域中特定 OfficeScan 用戶端的病毒爆發和一般模式策略有別於同一個網域中的其他 OfficeScan 用戶端，趨勢科技建議您重建網域，將具有相似需求的 OfficeScan 用戶端分成一組（請參閱 OfficeScan 網域 第 2-42 頁）。

規則撰寫

規則包括安全狀況條件、與 OfficeScan 用戶端相關聯的預設回應以及 OfficeScan 用戶端和策略伺服器執行的處理行動。

安全狀況條件

規則包括下列安全狀況條件：

- 用戶端電腦狀態：OfficeScan 用戶端電腦是否為開機狀態
- 用戶端即時掃瞄狀態：「即時掃瞄」已啟動或關閉
- 用戶端掃瞄引擎版本現狀：「病毒掃瞄引擎」是否為最新

- 用戶端病毒碼檔案狀態：「病毒碼」的新舊狀態。策略伺服器會藉由檢查下列其中一個項目來判斷病毒碼狀態：
  - 「病毒碼」的版本號碼是否比策略伺服器的版本號碼還舊
  - 「病毒碼」是否在驗證前幾天推出

規則的預設回應

回應可協助您瞭解發生 OfficeScan 用戶端驗證時，網路上 OfficeScan 用戶端的狀況。回應會出現在策略伺服器用戶端驗證記錄檔中，並且對應狀況 Token。請從下列預設回應中選擇：

- 正常：OfficeScan 用戶端電腦符合安全策略而且未中毒。
- 檢查：OfficeScan 用戶端需要更新其防毒元件。
- 中毒：OfficeScan 用戶端電腦已中毒或是有中毒的風險。
- 轉換：OfficeScan 用戶端電腦為開機狀態。
- 隔離：OfficeScan 用戶端電腦可能中毒的風險相當高且需要隔離。
- 未知：其他任何狀況

注意

您無法新增、刪除或修改回應。

策略伺服器和 OfficeScan 用戶端處理行動

如果 OfficeScan 用戶端安全狀況符合規則條件，策略伺服器可在策略伺服器用戶端驗證記錄中建立項目（如需詳細資訊，請參閱 用戶端驗證記錄檔 第 16-40 頁）。

如果 OfficeScan 用戶端安全狀況符合規則條件，則 OfficeScan 用戶端可執行下列中毒處理行動：

- 啟動用戶端「即時掃瞄」，讓 OfficeScan 用戶端能夠掃瞄所有開啟或儲存的檔案（如需詳細資訊，請參閱即時掃瞄 第 7-13 頁）

- 更新所有 OfficeScan 元件（如需詳細資訊，請參閱 OfficeScan 元件和程式 第 6-2 頁）
- 在啟動「即時掃瞄」或更新之後掃瞄 OfficeScan 用戶端（「立即掃瞄」）
- 在 OfficeScan 用戶端電腦上顯示通知訊息

預設規則

策略伺服器提供預設規則，讓您擁有進行設定的基礎。這些規則涵蓋常用和建議的安全狀況和中毒處理行動。下列為預設提供的規則：

表 16-3. 預設規則

規則名稱	比對條件	符合條件時回應	伺服器中毒處理行動	OFFICESCAN 用戶端處理行動
正常	「即時掃瞄」狀態已啟動，且「病毒掃瞄引擎」和「病毒碼」為最新狀態。	正常	無	無

規則名稱	比對條件	符合條件時回應	伺服器中毒處理行動	OfficeScan 用戶端處理行動
檢查	「病毒碼」版本至少應比 OfficeScan 用戶端所註冊的 OfficeScan 伺服器早一個版本。	檢查	在用戶端驗證記錄檔中建立項目	• 更新元件 • 啟動「即時掃瞄」或更新之後在 OfficeScan 用戶端上執行自動「立即清除」 • 在 OfficeScan 用戶端電腦上顯示通知訊息 秘訣 如果您使用此規則，請使用自動部署。此有助於確保 OfficeScan 用戶端在 OfficeScan 下載新元件之後立即收到最新的「病毒碼」。
轉換	OfficeScan 用戶端電腦為開機狀態。	轉換	無	無
隔離	「病毒碼」版本至少應比 OfficeScan 用戶端所註冊的 OfficeScan 伺服器早五個版本。	隔離	在用戶端驗證記錄檔中建立項目	• 更新元件 • 啟動「即時掃瞄」或更新之後在 OfficeScan 用戶端上執行自動「立即清除」和「立即掃瞄」 • 在 OfficeScan 用戶端電腦上顯示通知訊息
未受到防毒保護	「即時掃瞄」狀態為已關閉。	中毒	在用戶端驗證記錄檔中建立項目	• 啟動 OfficeScan 用戶端即時掃瞄 • 在 OfficeScan 用戶端電腦上顯示通知訊息

策略撰寫

策略包括任何數目的規則和預設回應與中毒處理行動。

- 規則執行

  策略伺服器會依照特定順序執行規則，如此您就能設定規則的優先順序。您可以變更規則的順序、新增規則和移除策略中現有的規則。

- 策略的預設回應

  如同規則一般，策略包括預設回應，可協助您瞭解發生用戶端驗證時，網路上 OfficeScan 用戶端的狀況。不過，預設回應只有在用戶端安全狀況「不」符合策略中的任何規則時，才會與用戶端相關聯。

  策略的回應與規則的回應相同（如需回應的清單，請參閱規則的預設回應 第 16-10 頁）。

- 策略伺服器和 OfficeScan 用戶端處理行動

  策略伺服器將 OfficeScan 用戶端狀態資訊放入與策略相關聯的每一條規則中，以迫使用戶端遵循規則。規則是根據 Web 主控台上指定的使用中規則由上往下套用。如果 OfficeScan 用戶端狀態符合任何一條規則，OfficeScan 用戶端會部署與規則對應的處理行動。如果沒有相符的規則，便套用預設的規則，而用戶端會部署與預設規則對應的中毒處理行動。

  預設的病毒爆發模式策略會使用「正常」規則評估 OfficeScan 用戶端，讓所有與此規則不相符的 OfficeScan 用戶端針對「中毒」回應立刻執行中毒處理行動。

  預設一般模式策略會使用所有非「正常」規則（轉換、未受到防毒保護、隔離、檢查）評估 OfficeScan 用戶端，將所有與這些規則不相符的 OfficeScan 用戶端歸類為「正常」，並針對「正常」規則套用中毒處理行動。

預設策略

策略伺服器提供預設策略，讓您擁有進行設定的基礎。可使用的策略有兩個，一個用於一般模式，另一個用於病毒爆發模式。

表 16-4. 預設策略

策略名稱	說明
預設一般模式策略	• 與策略相關聯的預設規則：轉換、未受到防毒保護、隔離和檢查 • 沒有符合的規則時回應：正常 • 伺服器中毒處理行動：無 • OfficeScan 用戶端處理行動：無

預設病毒爆發模式策略	• 與策略相關聯的預設規則：正常
	• 沒有符合的規則時回應：中毒
	• 伺服器中毒處理行動：在用戶端驗證記錄檔中建立項目
	• OfficeScan 用戶端處理行動：
	  • 啟動用戶端即時掃瞄
	  • 更新元件
	  • 啟動「即時掃瞄」或更新之後在 OfficeScan 用戶端上執行「立即掃瞄」
	  • 在 OfficeScan 用戶端電腦上顯示通知訊息

同步處理

定期同步處理策略伺服器和已註冊的 OfficeScan 伺服器可讓「病毒碼」、「病毒掃瞄引擎」和伺服器病毒爆發狀態（一般模式或病毒爆發模式）的策略伺服器版本與 OfficeScan 伺服器上的版本一樣新。請使用下列方法執行同步處理：

- 手動：隨時在「摘要」畫面上執行同步處理（請參閱策略伺服器摘要資訊 第 16-38 頁）。
- 依預約：設定同步處理預約時程（請參閱管理工作 第 16-41 頁）。

憑證

Cisco NAC 技術使用下列數位憑證建立各種元件之間的成功通訊：

表 16-5. Cisco NAC 憑證

憑證	說明
ACS 憑證	會在 ACS 伺服器和「憑證授權單位」(CA) 伺服器之間建立信任的通訊。「憑證授權單位」伺服器會在您將 ACS 憑證儲存在 ACS 伺服器上之前，先簽署 ACS 憑證。
CA 憑證	會在 Cisco ACS 伺服器上驗證 OfficeScan 用戶端。OfficeScan 伺服器會將 CA 憑證同時部署至 ACS 伺服器和 OfficeScan 用戶端（使用 Cisco Trust Agent 封裝）。
策略伺服器 SSL 憑證	會建立策略伺服器和 ACS 伺服器之間的安全 HTTPS 通訊。策略伺服器安裝程式會自動在安裝策略伺服器期間產生策略伺服器 SSL 憑證。 策略伺服器 SSL 憑證為選用。不過，請使用它來確保只有加密的資料會在策略伺服器和 ACS 伺服器之間傳輸。

下圖說明建立和部署 ACS 與 CA 憑證所包含的步驟：

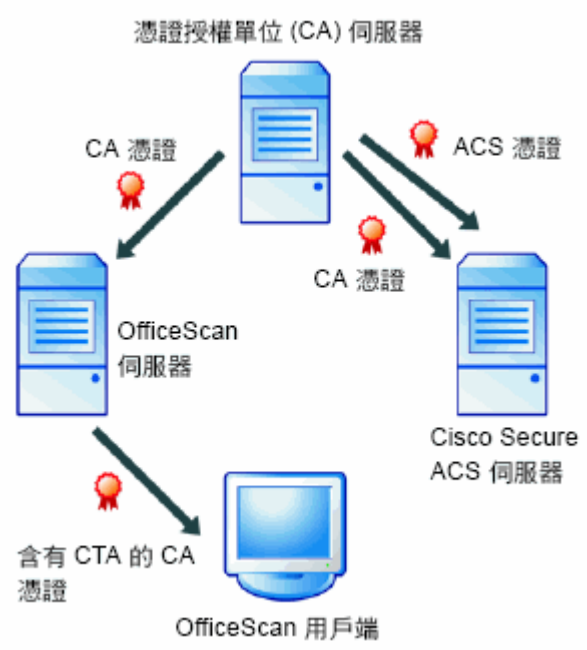


圖 16-4. 建立和部署 ACS 與 CA 憑證

1. 在 ACS 伺服器發出憑證簽署要求至 CA 伺服器之後，CA 就會發出憑證（稱為「ACS 憑證」），然後 ACS 憑證就會安裝到 ACS 伺服器上。如需詳細資訊，請參閱 Cisco Secure ACS 伺服器登記 第 16-22 頁。
2. CA 憑證會從 CA 伺服器匯出，並且安裝到 ACS 伺服器上。如需詳細資訊，請參閱安裝 CA 憑證 第 16-22 頁。
3. OfficeScan 伺服器上會儲存一份相同的 CA 憑證副本。
4. OfficeScan 伺服器會將 CA 憑證部署至含有 CTA 的 OfficeScan 用戶端。如需詳細資訊，請參閱 Cisco Trust Agent 部署 第 16-25 頁。

CA 憑證

已安裝 CTA 的 OfficeScan 用戶端會先向 ACS 伺服器驗證，再傳送用戶端安全狀況。有數種方法可用於驗證（如需詳細資訊，請參閱 Cisco Secure ACS 文件）。例如，您可能已使用 Windows Active Directory 針對 Cisco Secure ACS 啟動電腦驗證，其可設為自動在 Active Directory 中新增電腦時產生終端使用者用戶端憑證。如需詳細資訊，請參閱 Microsoft 知識庫文章 313407，標題為「HOW TO:Create Automatic Certificate Requests with Group Policy in Windows」。

如果是本身具有「憑證授權單位」(CA) 伺服器，但其終端使用者用戶端尚未具有憑證的使用者，OfficeScan 提供了一種分發根憑證給 OfficeScan 用戶端的機制。請在安裝 OfficeScan 期間或從 OfficeScan Web 主控台分發憑證。OfficeScan 會在部署 Cisco Trust Agent 到 OfficeScan 用戶端時分發憑證（請參閱 Cisco Trust Agent 部署 第 16-25 頁）。

注意

如果您已從「憑證授權單位」取得憑證，或是已產生自己的憑證並將其分發到終端使用者 OfficeScan 用戶端，則不需要再次進行這項動作。

將憑證分發到 OfficeScan 用戶端前，請先向 CA 伺服器登記 ACS 伺服器，然後備妥憑證（如需詳細資訊，請參閱 Cisco Secure ACS 伺服器登記 第 16-22 頁）。

策略伺服器系統需求

安裝策略伺服器前，請檢查電腦是否符合下列需求：

表 16-6. 策略伺服器系統需求

硬體/軟體	需求
作業系統	• Windows 2000 Professional（Service Pack 4） • Windows 2000 Server（Service Pack 4） • Windows 2000 Advanced Server（Service Pack 4） • Windows XP Professional（Service Pack 3 或更新版本），32 位元和 64 位元 • Windows Server 2003（Standard 和 Enterprise Edition）（Service Pack 2 或更新版本），32 位元和 64 位元
硬體	• 300MHz Intel Pentium 處理器或同級處理器 • 128MB RAM • 300MB 可用磁碟空間 • 支援 800 x 600 解析度（256 色）或以上的顯示器
Web 伺服器	• Microsoft Internet Information Server (IIS) 5.0 版或 6.0 版 • Apache Web Server 2.0 或更新版本（僅適用於 Windows 2000/XP/Server 2003）
Web 主控台	如果要使用 OfficeScan 伺服器 Web 主控台，則需求如下： • 133MHz Intel Pentium 處理器或同級處理器 • 64MB RAM • 30MB 可用磁碟空間 • 支援 800 x 600 解析度（256 色）或以上的顯示器 • Microsoft Internet Explorer 5.5 或更新版本

Cisco Trust Agent (CTA) 需求

將 Cisco Trust Agent 部署到用戶端電腦前，請先檢查電腦是否符合下列需求：

注意

Cisco Trust Agent 不支援 IPv6。您不能將這個代理程式部署到單純 IPv6 端點。

表 16-7. Cisco Trust Agent (CTA) 需求

硬體/軟體	需求
作業系統	• Windows 2000 Professional 和 Server（Service Pack 4） • Windows XP Professional（Service Pack 3 或更新版本），32 位元 • Windows Server 2003（Standard 和 Enterprise Edition）（Service Pack 2 或更新版本），32 位元
硬體	• 200MHz 單一或多個 Intel Pentium 處理器 • 128MB RAM（適用於 Windows 2000） • 256MB RAM（適用於 Windows XP 和 Windows Server 2003） • 5MB 可用磁碟空間（建議 20MB）
其他	• Windows Installer 2.0 或更新版本

支援的平台和需求

下列平台支援 Cisco NAC 功能：

表 16-8. 支援的平台和需求

支援的平台	機型	IOS 映像	最低記憶體/快閃記憶體
路由器			
Cisco 830、870 系列	831, 836, 837	IOS 12.3(8) 或更新版本	48MB/8MB

支援的平台	機型	IOS 映像	最低記憶體/快閃記憶體
Cisco 1700 系列	1701, 1711, 1712, 1721, 1751, 1751-V, 1760	IOS 12.3(8) 或更新版本	64MB/16MB
Cisco 1800 系列	1841	IOS 12.3(8) 或更新版本	128MB/32MB
Cisco 2600 系列	2600XM, 2691	IOS 12.3(8) 或更新版本	96MB/32MB
Cisco 2800 系列	2801, 2811, 2821, 2851	IOS 12.3(8) 或更新版本	128MB/64MB
Cisco 3600 系列	3640/3640A、3660-ENT 系列	IOS 12.3(8) 或更新版本	48MB/16MB
Cisco 3700 系列	3745, 3725	IOS 12.3(8) 或更新版本	128MB/32MB
Cisco 3800 系列	3845, 3825	IOS 12.3(8) 或更新版本	256MB/64MB
Cisco 7200 系列	720x, 75xx	IOS 12.3(8) 或更新版本	128MB/48MB
VPN 集訊器			
Cisco VPN 3000 系列	3005 - 3080	V4.7 或更新版本	無
交換器			
Cisco Catalyst 2900	2950, 2970	IOS 12.1(22)EA5	無
Cisco Catalyst 3x00	3550, 3560, 3750	IOS 12.2(25)SEC	無
Cisco Catalyst 4x00	Supervisor 2+ 或更新版本	IOS 12.2(25)EWA	無
Cisco Catalyst 6500	6503、6509、Supervisor 2 或更新版本	CatOS 8.5 或更新版本	Sup2 - 128MB、Sup32 - 256MB、Sup720 - 512MB

支援的平台	機型	IOS 映像	最低記憶體/快閃記憶體
無線網路存取點			
Cisco AP1200 系列	1230	無	無

策略伺服器 for NAC 部署

下列程序僅供參考，而且會隨 Microsoft 和（或）Cisco 介面的更新而變更。

在執行任何工作之前，請先確認網路上的「網路存取裝置」是否支援 Cisco NAC（請參閱支援的平台和需求 第 16-19 頁）。如需安裝和組態設定指示，請參閱裝置文件。同時，請在網路上安裝 ACS 伺服器。如需指示，請參閱 Cisco Secure ACS 文件。

1. 將 OfficeScan 伺服器安裝在網路上（請參閱《*安裝和升級手冊*》）。
2. 在要讓策略伺服器評估其防毒保護的所有用戶端上安裝 OfficeScan 用戶端程式。
3. 登記 Cisco Secure ACS 伺服器。在 ACS 伺服器和「憑證授權單位」(CA) 伺服器之間建立信任關係，作法是讓 ACS 伺服器發出憑證簽章要求，然後將 CA 簽章的憑證（稱為「ACS 憑證」）儲存到 ACS 伺服器上（如需詳細資訊，請參閱 Cisco Secure ACS 伺服器登記 第 16-22 頁）。
4. 將 CA 憑證匯出至 ACS 伺服器，然後在 OfficeScan 伺服器上儲存副本。這個步驟只有在您尚未將憑證部署至用戶端和 ACS 伺服器時才需要（請參閱 安裝 CA 憑證 第 16-22 頁）。
5. 將 Cisco Trust Agent 和 CA 憑證部署到所有 OfficeScan 用戶端，讓用戶端能夠提交安全狀況資訊給策略伺服器（請參閱 Cisco Trust Agent 部署 第 16-25 頁）。
6. 安裝策略伺服器 for Cisco NAC 以處理來自 ACS 伺服器的要求（請參閱安裝 Policy Server for Cisco NAC 第 16-29 頁）。
7. 將 SSL 憑證從策略伺服器匯出到 Cisco ACS 伺服器，在兩部伺服器之間建立安全 SSL 通訊（請參閱安裝 Policy Server for Cisco NAC 第 16-29 頁）。

8. 設定 ACS 伺服器將狀況驗證要求轉送到策略伺服器（請參閱 ACS 伺服器組態設定 第 16-35 頁）。

9. 設定策略伺服器 for NAC。建立和修改策略伺服器規則與策略，以執行組織的 OfficeScan 用戶端安全策略（請參閱 Policy Server for Cisco NAC 組態設定 第 16-36 頁）。

Cisco Secure ACS 伺服器登記

向「憑證授權單位」(CA) 伺服器登記 Cisco Secure ACS 伺服器，以便在兩部伺服器之間建立信任關係。下列程序適用於執行 Windows「憑證授權單位」伺服器的使用者，以便管理網路上的憑證。如果您使用的是其他 CA 應用程式或服務，請參閱廠商文件；如需有關如何登記憑證的指示，請參閱 ACS 伺服器文件。

安裝 CA 憑證

OfficeScan 用戶端會先向 ACS 伺服器驗證，再傳送安全狀況資料。要有 CA 憑證才能進行這項驗證。首先，將 CA 憑證從 CA 伺服器同時匯出到 ACS 伺服器和 OfficeScan 伺服器，然後建立 CTA 代理程式部署套件。該套件包括 CA 憑證（請參閱 CA 憑證 第 16-17 頁和 Cisco Trust Agent 部署 第 16-25 頁）。

執行下列動作，以便匯出並安裝 CA 憑證：

- 從「憑證授權單位」伺服器匯出 CA 憑證
- 將其安裝在 Cisco Secure ACS 伺服器上
- 在 OfficeScan 伺服器上儲存副本

注意

下列程序適用於執行 Windows「憑證授權單位」伺服器的使用者，以便管理網路上的憑證。如果您使用的是其他「憑證授權單位」應用程式或服務，請參閱廠商文件。

匯出並安裝 CA 憑證進行分發

程序

1. 從「憑證授權單位」(CA) 伺服器匯出憑證：
   a. 在 CA 伺服器上，按一下「開始 > 執行」。

      會開啟「執行」畫面。

   b. 在「開啟」方塊中輸入 mmc，

      會開啟新的管理主控台畫面。

   c. 按一下「 檔案 > 新增/移除嵌入式管理單元。

      會出現「新增/移除嵌入式管理單元」畫面。

   d. 按一下「憑證」，然後按一下「新增」，

      會開啟「憑證嵌入式管理單元」畫面。

   e. 按一下「電腦帳戶」，然後按一下「下一步」，

      會開啟「選擇電腦」畫面。

   f. 按一下「本機電腦」，然後按一下「完成」。

   g. 按一下「關閉」以關閉「新增獨立嵌入式管理單元」畫面。

   h. 按一下「確定」以關閉「新增/移除嵌入式管理單元」畫面。

   i. 在主控台樹狀結構檢視中，按一下「憑證 > 信任的根憑證授權 > 憑證」。

   j. 從清單中選取要分發到用戶端和 ACS 伺服器的憑證。

   k. 按一下「動作 > 所有工作 > 匯出...」。

      會開啟「憑證匯出精靈」。

   l. 按「下一步」。

   m. 按一下「DER 編碼二位元 x.509」，然後按一下「下一步」。

n. 輸入檔案名稱並瀏覽至要匯出憑證到其中的目錄。

o. 按「下一步」。

p. 按一下「完成。

會顯示確認視窗。

q. 按一下「確定」。

2. 將憑證安裝在 Cisco Secure ACS 上。

a. 按一下「系統組態設定 > ACS 憑證安裝 > ACS 憑證授權單位安裝」。

b. 在「CA 憑證檔案」欄位中輸入憑證的完整路徑和檔案名稱。

c. 按一下「提交」。 Cisco Secure ACS 會提示您重新啟動服務。

d. 按一下「系統組態設定 > 服務控制」。

e. 按一下「重新啟動」，Cisco Secure ACS 便會重新啟動。

f. 按一下「系統組態設定 > ACS 憑證管理 > 編輯憑證信任清單」。會出現「編輯憑證信任清單」畫面。

g. 選取對應到您在步驟 b 所匯入憑證的核取方塊，然後按一下「提交」，Cisco Secure ACS 會提示您重新啟動服務。

h. 按一下「系統組態設定 > 服務控制」。

i. 按一下「重新啟動」，Cisco Secure ACS 便會重新啟動。

3. 將憑證（.cer 檔）複製到 OfficeScan 伺服器電腦，以便您能夠將其部署到含有 CTA 的用戶端（如需詳細資訊，請參閱）。

注意

請將憑證儲存到本機磁碟機上，而不是儲存到網路磁碟機上。

Cisco Trust Agent 部署

Cisco Trust Agent (CTA) 是裝載在 OfficeScan 伺服器內並且會安裝到用戶端的程式，它會讓 OfficeScan 用戶端向 Cisco ACS 報告防毒資訊。

注意

Cisco Trust Agent 不支援 IPv6。您不能將這個代理程式部署到純 IPv6 端點。

在安裝 OfficeScan 伺服器期間部署 CTA

如果您在安裝 OfficeScan 伺服器前已備妥 CA 憑證，便可以在安裝 OfficeScan 伺服器時部署 CTA。部署 CTA 的選項位於安裝程式的「安裝其他 OfficeScan 程式」畫面。如需有關安裝 OfficeScan 伺服器的指示，請參閱*《安裝和升級手冊》*。

程序

1. 在「安裝其他 OfficeScan 程式」畫面中，選取「Cisco Trust Agent for Cisco NAC」。
2. 如果您已將憑證分發到 Cisco Secure NAC 終端使用者用戶端，請按一下「下一步」，否則請執行下列步驟以分發憑證。
   a. 按一下「匯入憑證」。
   b. 找出並選取備妥的憑證檔案，然後按一下「確定」。

      如需有關備妥憑證檔案的詳細資訊，請參閱安裝 CA 憑證 第 16-22 頁。
   c. 按「下一步」。
3. 繼續安裝 OfficeScan 伺服器。

從 OfficeScan Web 主控台部署 CTA

如果您未在伺服器安裝期間選取這個選項以安裝/升級 CTA，仍可以從 Web 主控台執行這項操作。在安裝/升級 CTA 之前，請先部署 OfficeScan 用戶端憑證至用戶端。

注意

「憑證授權單位」(CA) 伺服器會產生用戶端憑證檔案。請向趨勢科技的銷售人員要求憑證檔案。

當您準備安裝/升級時，請在「Cisco NAC > 代理程式管理」中檢查要安裝的 CTA 版本，然後在「Cisco NAC > 代理程式部署」中將 CTA 安裝到 OfficeScan 用戶端。「代理程式部署」畫面還可讓您選擇解除安裝 CTA。

請先在執行 Windows 2000/XP 的 OfficeScan 用戶端上安裝 Windows Installer 2.0 for NT 4.0，再部署 CTA。

匯入用戶端憑證

用戶端（或 CA）憑證會在 Cisco ACS 伺服器驗證使用者 OfficeScan 用戶端。OfficeScan 伺服器會將 CA 憑證與 Cisco Trust Agent (CTA) 部署至 OfficeScan 用戶端。因此，請先將憑證匯入至 OfficeScan 伺服器，然後再部署 CTA。

程序

1. 開啟 OfficeScan 伺服器的 Web 主控台，然後按一下「Cisco NAC > 用戶端憑證」。
2. 輸入憑證的確切檔案路徑。
3. 輸入儲存在伺服器上已備妥的 CA 憑證的完整路徑和檔案名稱（例如：`C:\CiscoNAC\certificate.cer`)。如需有關備妥 CA 憑證的詳細資訊，請參閱安裝 CA 憑證 第 16-22 頁。
4. 按一下「匯入」。

如果要清除欄位，請按一下「重設」。

Cisco Trust Agent 版本

在將 CTA 安裝到用戶端之前，請檢查要安裝的 CTA 版本（Cisco Trust Agent 或 Cisco Trust Agent Supplicant）。這兩個版本間唯一的不同是 Supplicant 套件提供電腦和終端使用者第 2 層驗證。

如果 Cisco NAC Access Control Server (ACS) 是 4.0 或更新版本，請將用戶端上的 Cisco Trust Agent 升級至 2.0 或更新版本。

檢查 CTA 版本

程序

1. 開啟 OfficeScan 伺服器的 Web 主控台，然後按一下「Cisco NAC > 代理程式管理」。
2. 按一下「使用 <CTA 版本>」。

   OfficeScan 伺服器會開始使用新版本。

手動取代 CTA 套件

如果要使用特定版本，請手動取代 OfficeScan 伺服器上的 CTA 套件。

程序

1. 在您要使用的 CTA 版本中，將 CTA `.msi` 檔案複製到下列其中一個資料夾：
   - <伺服器安裝資料夾>`\PCCSRV\Admin\Utility\CTA\CTA-Package`
   - <伺服器安裝資料夾>`\PCCSRV\Admin\Utility\CTA\ CTA-Supplicant-Package`
2. 將下列檔案複製到 <伺服器安裝資料夾>`\ PCCSRV\Admin\Utility\CTA \PosturePlugin`：`TmabPP.dll`、`tmabpp.inf` 和 `TmAbPpAct.exe`。

3. 在 Web 主控台中，移至「Cisco NAC > 代理程式管理」，然後按一下「使用 <CTA 版本>」。

升級代理程式後，這些檔案會壓縮為 PostureAgent.zip 做為 CTA 部署套件，此壓縮檔會放在 <伺服器安裝資料夾>\PCCSRV\download\Product 下。

部署 Cisco Trust Agent

部署 Cisco Trust Agent，讓 OfficeScan 用戶端可以向 Cisco ACS 回報防毒資訊。

程序

1. 瀏覽至「Cisco NAC > 代理程式管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 () 以包含所有的用戶端，或選取特定網域或用戶端。
3. 按一下「部署代理程式」。
4. 如果您安裝 OfficeScan 伺服器時不接受「Cisco 授權合約」中的條款，這時會出現使用授權資訊。請閱讀授權合約，然後按一下「是」同意接受條款。
5. 選取「安裝/升級 Cisco Trust Agent。
6. （選用）選取「解除安裝 OfficeScan 用戶端時，也解除安裝 Cisco Trust Agent」。

   注意

   您也可以使用此畫面來解除安裝或保留用戶端上的 CTA 狀態。

   保留 CTA 狀態表示如果已安裝 CTA，則防止在安裝時覆寫該 CTA。除非您正在執行升級或確定從未在任何所選用戶端上安裝過 CTA 時，您可能會想要使用此選項，否則，伺服器會重新安裝 CTA，而您的設定將會遺失。

7. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：

- 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
- 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

注意

如果您在按一下「安裝 Cisco Trust Agent」時，要在其中部署代理程式的 OfficeScan 用戶端為離線狀態，則 OfficeScan 會自動在 OfficeScan 用戶端上線時完成工作要求。

Cisco Trust Agent 安裝驗證

將 CTA 部署到用戶端後，請檢視 OfficeScan 用戶端樹狀結構以確認安裝成功。用戶端樹狀結構包含標題為「Cisco Trust Agent」的欄位，這個欄位會在「更新」、「檢視全部」或「防毒」檢視中出現。成功安裝的 CTA 包含 CTA 程式的版本號碼。

此外，請確認用戶端電腦上正在執行下列程序：

- `ctapsd.exe`
- `ctaEoU.exe`
- `ctatransapt.exe`
- `ctalogd.exe`

安裝 Policy Server for Cisco NAC

有兩種方式可以安裝策略伺服器：

- 位於企業版 DVD 上的策略伺服器安裝程式
- OfficeScan 伺服器的主安裝程式（這個程式會在同一部電腦上同時安裝 OfficeScan 伺服器和策略伺服器）

注意

主安裝程式會在 IIS 或 Apache Web Server 上同時安裝 OfficeScan 伺服器和策略伺服器 Web 主控台。如果安裝程式在系統上找不到 Apache 伺服器，或者安裝的現有 Apache 伺服器不是 2.0 版，則安裝程式會自動安裝 Apache 2.0 版。

ACS 伺服器、策略伺服器和 OfficeScan 伺服器必須位於同一個網路區段，才能確保通訊有效。

安裝 Apache Web Server 前，如需升級、Patch 和安全問題的最新資訊，請參閱 Apache 網站：

http://www.apache.org

使用策略伺服器安裝程式安裝策略伺服器

程序

1. 登入您要安裝 Policy Server for Cisco NAC 的電腦。
2. 在 Enterprise CD 上找出 Policy Server for Cisco NAC 安裝程式套件。
3. 按兩下 `setup.exe` 以執行安裝程式。
4. 請遵循安裝指示。

您可以將策略伺服器安裝到 OfficeScan 伺服器電腦。

從 OfficeScan 伺服器的主安裝程式安裝 Cisco NAC 的策略伺服器

程序

1. 在 OfficeScan 伺服器主安裝程式的「安裝其他 OfficeScan 程式」畫面中，選取「Policy Server for Cisco NAC」。
2. 按「下一步」。

3. 繼續安裝 OfficeScan 伺服器，直到出現 Trend Micro Policy Server for Cisco NAC 的「歡迎」畫面。

4. 按「下一步」。

   會出現「Policy Server for Cisco NAC 授權合約」畫面。

5. 請閱讀這份合約，然後按一下「是」繼續。

   會出現「選擇安裝的位置」畫面。

6. 請按一下「瀏覽...」並選取安裝策略伺服器的新位置，視需要修改預設的目標位置。

7. 按「下一步」。

   會出現「Web 伺服器」畫面。

8. 請選擇策略伺服器的 Web 伺服器：

   - IIS 伺服器：按一下以安裝在現有的 IIS Web 伺服器安裝上
   - Apache 2.0 Web 伺服器：按一下以安裝在 Apache 2.0 Web 伺服器上

9. 按「下一步」。

   會出現「Web 伺服器設定」畫面。

10. 請設定下列資訊：

    a. 如果您選擇在一部 IIS 伺服器上安裝策略伺服器，請選擇下列其中一項：

       - IIS 預設網站：按一下以安裝為 IIS 預設網站
       - IIS 虛擬網站：按一下以安裝為 IIS 虛擬網站

    b. 在「通訊埠」旁，輸入做為伺服器監聽通訊埠的通訊埠。

       當策略伺服器和 OfficeScan 伺服器位於同一部電腦上且使用同一部 Web 伺服器時，通訊埠號碼如下所示：

       - 預設網站上的 Apache Web Server/IIS Web 伺服器：策略伺服器和 OfficeScan 伺服器的通訊埠相同。

- 都位於虛擬網站的 IIS Web 伺服器上：策略伺服器的預設監聽通訊埠是 8081，而 SSL 通訊埠則是 4344。OfficeScan 伺服器的預設監聽通訊埠是 8080，而 SSL 通訊埠則為 4343。

c. 如果您選擇將策略伺服器安裝在 IIS 伺服器上，則可以使用 Secured Socket Layer (SSL)。輸入 SSL 通訊埠號碼和您要讓 SSL 憑證保持有效的年數（預設值為 3 年）。

如果您啟動 SSL，則此通訊埠號碼將會做為伺服器的監聽通訊埠。策略伺服器的位址如下：

- `http://<Policy Server name>:<port number>`
- `https://<策略伺服器名稱>:<通訊埠號碼>` (如果您啟動 SSL)

11. 按「下一步」。
12. 指定策略伺服器主控台密碼，然後按「下一步」。
13. 指定 ACS 伺服器驗證密碼，然後按「下一步」。
14. 檢視安裝設定。如果同意這些設定，請按「下一步」開始安裝。否則，按一下「上一步」移至上一個畫面。
15. 安裝完成後，請按一下 「完成」。

OfficeScan 伺服器主安裝程式會繼續執行剩餘的 OfficeScan 伺服器安裝。

策略伺服器 SSL 憑證準備作業

如果要在 ACS 伺服器和策略伺服器之間建立安全 SSL 連線，請備妥專門搭配 SSL 使用的憑證。安裝程式會自動產生 SSL 憑證。

準備 IIS 策略伺服器 SSL 憑證

程序

1. 從 MMC 上的「憑證存放區」匯出憑證。

a. 在策略伺服器上，按一下「開始 > 執行」。

會開啟「執行」畫面。

b. 在「開啟」方塊中輸入 mmc，

會開啟新的管理主控台畫面。

c. 按一下「 主控台 > 新增/移除嵌入式管理單元。

會出現「新增/移除嵌入式管理單元」畫面。

d. 按一下「新增」。

會出現「新增獨立嵌入式管理單元」畫面。

e. 按一下「憑證」，然後按一下「新增」，

會開啟「憑證嵌入式管理單元」畫面。

f. 按一下「電腦帳戶」，然後按一下「下一步」，

會開啟「選擇電腦」畫面。

g. 按一下「本機電腦」，然後按一下「完成」。

h. 按一下「關閉」以關閉「新增獨立嵌入式管理單元」畫面。

i. 按一下「確定」以關閉「新增/移除嵌入式管理單元」畫面。

j. 在主控台樹狀結構檢視中，按一下「憑證（本機電腦） > 信任的根憑證授權 > 憑證」。

k. 從清單中選取憑證。

注意

按兩下憑證並選取「內容」，查看憑證指模。指模應該與位於 IIS 主控台的憑證指模相同。

如果要確認指模是否相同，請開啟 IIS 主控台並以滑鼠右鍵按一下「虛擬網站」或「預設網站」（視您安裝策略伺服器的網站而定），然後選取「內容」。按一下「目錄安全性」，然後按一下「檢視憑證」以檢視憑證指模等憑證詳細資訊。

l. 按一下「動作 > 所有工作 > 匯出...」。會開啟「憑證匯出精靈」。

m. 按「下一步」。

n. 按一下「DER 編碼二位元 x.509」或「Base 64 編碼 X.509」，然後按一下「下一步」。

o. 輸入檔案名稱並瀏覽至要匯出憑證到其中的目錄。

p. 按「下一步」。

q. 按一下「完成」，會顯示確認視窗。

r. 按一下「確定」。

2. 將憑證安裝在 Cisco Secure ACS 上。

a. 在 ACS Web 主控台上，按一下「系統組態設定 > ACS 憑證安裝 > ACS 憑證授權單位安裝」。

b. 在「CA 憑證檔案」欄位中輸入憑證的完整路徑和檔案名稱。

c. 按一下「提交」。 Cisco Secure ACS 會提示您重新啟動服務。

d. 按一下「系統組態設定 > 服務控制」。

e. 按一下「重新啟動」，Cisco Secure ACS 便會重新啟動。

準備 Apache 策略伺服器 SSL 憑證

程序

1. 從 MMC 上的「憑證存放區」匯出憑證。

a. 取得 `server.cer` 憑證檔案。這個檔案位置會視您先安裝的是 OfficeScan 伺服器還是策略伺服器而定：

- 如果您先安裝 OfficeScan 伺服器再安裝策略伺服器，則該檔案位於下列目錄：<伺服器安裝資料夾 >`\PCCSRV\Private\certificate`

- 如果您先安裝策略伺服器再安裝 OfficeScan 伺服器，則該檔案位於下列目錄：<伺服器安裝資料夾>\PolicyServer\Private\certificate

b. 將憑證檔案複製到 ACS 伺服器。

2. 將憑證安裝在 Cisco Secure ACS 上。

a. 在 ACS Web 主控台上，按一下「系統組態設定 > ACS 憑證安裝 > ACS 憑證授權單位安裝」。

b. 在「CA 憑證檔案」欄位中輸入憑證的完整路徑和檔案名稱。

c. 按一下「提交」。

Cisco Secure ACS 會提示您重新啟動服務。

d. 按一下「系統組態設定 > 服務控制」。

e. 按一下「重新啟動」，

Cisco Secure ACS 便會重新啟動。

ACS 伺服器組態設定

如果要允許 Cisco Secure ACS 傳送驗證要求到 Policy Server for Cisco NAC，請在「外部策略」中新增 Policy Server for Cisco NAC，讓外部使用者資料庫用來進行驗證。如需有關如何在新外部策略中新增策略伺服器的指示，請參閱 ACS 伺服器文件。

注意

將 ACS 伺服器設為執行封鎖用戶端對網路的存取等工作。這些 ACS 功能不在執行 Trend Micro Policy Server for Cisco NAC 的討論範圍內，所以沒有在本文件中提供。如需有關設定其他 ACS 功能的詳細資訊，請參閱 ACS 文件。

Policy Server for Cisco NAC 組態設定

安裝 OfficeScan 和策略伺服器並部署 OfficeScan 用戶端和 Cisco Trust Agent 後，請設定 Policy Server for Cisco NAC。如果要設定策略伺服器，請移至「Cisco NAC > 策略伺服器」並按一下策略伺服器連結，從 OfficeScan Web 主控台存取策略伺服器 Web 主控台。

本節說明下列各方面的策略伺服器組態設定：

- 從 OfficeScan 設定策略伺服器 第 16-36 頁說明如何在 OfficeScan Web 主控台上管理策略伺服器。
- 策略伺服器摘要資訊 第 16-38 頁為您說明如何在網路上取得策略伺服器總覽。
- 策略伺服器註冊 第 16-39 頁是設定策略伺服器的第一個步驟。
- 規則 第 16-39 頁為您說明如何建立並編輯組成策略的規則。
- 策略 第 16-40 頁為您說明如何建立並編輯最終決定策略伺服器衡量用戶端安全狀況的方式。
- 用戶端驗證記錄檔 第 16-40 頁為您全盤說明如何使用記錄檔來瞭解網路上用戶端的安全狀況狀態。
- 用戶端記錄檔維護 第 16-40 頁提供關於如何維護用戶端驗證記錄檔大小的總覽。
- 管理工作 第 16-41 頁說明如何變更策略伺服器密碼並設定同步處理的預約時程。

從 OfficeScan 設定策略伺服器

設定策略伺服器的第一個步驟是將已安裝的策略伺服器新增至 OfficeScan 伺服器，如此可讓您從 OfficeScan Web 主控台開啟策略伺服器 Web 主控台。

從 OfficeScan 新增策略伺服器

程序

1. 在 OfficeScan Web 主控台的主功能表上，按一下「Cisco NAC > 策略伺服器」。

   會出現「策略伺服器管理」畫面，其中顯示所有策略伺服器的清單。

2. 按一下「新增」。

   「Policy Server」畫面便會顯示。

3. 輸入完整的策略伺服器位址，以及伺服器用來進行 HTTPS 通訊的通訊埠號碼（例如：`https://policy-server:4343/`）。同時輸入選擇性的伺服器說明。

4. 輸入登入策略伺服器 Web 主控台時要使用的密碼，然後確認密碼。

5. 按一下「新增」。

從 OfficeScan 刪除策略伺服器

程序

1. 在 OfficeScan Web 主控台的主功能表上，按一下「Cisco NAC > 策略伺服器」。

   會出現「策略伺服器管理」畫面，其中顯示所有策略伺服器的清單。

2. 選取要刪除的策略伺服器旁邊的核取方塊。

3. 按一下「刪除」。

注意

如果要驗證網路上的所有用戶端，請將所有 OfficeScan 伺服器新增到至少一部策略伺服器。

策略伺服器摘要資訊

「摘要」畫面包含有關策略伺服器的資訊，包括策略和規則的組態設定、用戶端驗證記錄檔和已向策略伺服器註冊的 OfficeScan 伺服器。

Policy Server for Cisco NAC 的 IP 位址和通訊埠號碼會出現在「摘要」畫面的頂端。

「組態設定摘要」表會顯示已向策略伺服器註冊的 OfficeScan 伺服器數目、策略伺服器策略和組成策略的規則。

檢視和修改策略伺服器的「組態設定摘要」詳細資料

程序

1. 在 OfficeScan Web 主控台的主功能表上，按一下「Cisco NAC > 策略伺服器」。

   會出現「策略伺服器管理」畫面，其中顯示所有策略伺服器的清單。

2. 按一下要檢視其詳細資訊的策略伺服器的伺服器名稱，

   會出現「摘要」畫面，其中顯示「組態設定摘要」表。

3. 按一下您要檢視其組態設定的項目旁的連結：

   - 註冊的 OfficeScan 伺服器：目前位於網路上的 OfficeScan 伺服器
   - 策略：註冊的 OfficeScan 伺服器可使用的策略伺服器策略
   - 規則：組成策略的策略伺服器規則

秘訣

如果您希望網路上的多部策略伺服器使用相同的設定，包括相同的規則和策略，請從其中一部伺服器匯出設定，然後將設定匯入另一部伺服器中。趨勢科技建議您在網路上的所有策略伺服器上設定相同的設定，以維持防毒策略的一致性。

使用註冊的 OfficeScan 伺服器將策略伺服器同步化

程序

1. 在摘要畫面中，按一下「與 OfficeScan 同步處理」。會出現「摘要－同步處理結果」畫面，其中顯示下列唯讀資訊：
   - OfficeScan 伺服器名稱：註冊的 OfficeScan 伺服器的主機名稱或 IP 位址和通訊埠號碼
   - 同步處理結果：指出同步處理是否成功
   - 上次同步處理日期：上次成功同步處理的日期

如需有關同步處理的詳細資訊，請參閱同步處理 第 16-14 頁。

策略伺服器註冊

請至少向一部 OfficeScan 伺服器註冊策略伺服器，讓策略伺服器可以取得「病毒碼」和「病毒掃瞄引擎」版本資訊。如需有關 OfficeScan 伺服器在驗證程序中所扮演角色的資訊，請參閱用戶端驗證流程 第 16-6 頁。

注意

如果要讓策略伺服器驗證網路上的所有用戶端，請將所有 OfficeScan 伺服器新增到至少一部策略伺服器。

從 OfficeScan 伺服器畫面中新增 OfficeScan 伺服器或編輯現有伺服器的設定，您可以移至策略伺服器 Web 主控台並按一下「組態設定 > OfficeScan 伺服器」，藉此存取該畫面。

規則

規則是策略的基礎並且會組成策略。根據下一個步驟的策略伺服器組態設定來設定規則。如需詳細資訊，請參閱規則撰寫 第 16-9 頁。

如果要存取 Cisco ACS 規則的 Web 主控台畫面，請移至策略伺服器 Web 主控台並按一下主功能表上的「組態設定 > 規則」。

策略

在設定新規則或確認預設規則適合您的安全執行需求之後，請設定註冊的 OfficeScan 伺服器可使用的策略。如需詳細資訊，請參閱策略撰寫 第 16-13 頁。

新增 Cisco NAC 策略或編輯現有策略以決定目前執行的規則，並且在用戶端安全狀況不符合任何規則時，針對用戶端採取處理行動。

如果要存取 Cisco ACS 策略的 Web 主控台畫面，請移至策略伺服器 Web 主控台並按一下主功能表上的「組態設定 > 策略」。

用戶端驗證記錄檔

使用用戶端驗證記錄檔檢視在策略伺服器上驗證用戶端時的詳細資訊。驗證會在 ACS 伺服器擷取用戶端安全狀況資料並將其傳送到策略伺服器時發生，而策略伺服器會將該資料與策略和規則比較（請參閱用戶端驗證流程 第 16-6 頁）。

注意

如果要在新增或編輯新規則或策略時產生用戶端驗證記錄檔，請選取「伺服器端中毒處理行動」下的核取方塊。

如果要存取 Cisco ACS 記錄檔的 Web 主控台畫面，請移至策略伺服器 Web 主控台並按一下主功能表上的「記錄檔 > 檢視用戶端驗證記錄檔」。

用戶端記錄檔維護

策略伺服器會在用戶端驗證記錄檔達指定大小時封存這些檔案，也可在記錄檔累積到指定數目後加以刪除。按一下策略伺服器 Web 主控台上的「記錄檔 > 記錄檔維護」，指定策略伺服器維護用戶端驗證記錄檔的方式。

管理工作

在策略伺服器上執行下列管理工作：

- 變更密碼：變更新增策略伺服器時設定的密碼（請參閱從 OfficeScan 設定策略伺服器 第 16-36 頁）
- 設定同步處理預約時程：策略伺服器必須定期取得 OfficeScan 伺服器上「病毒碼」和「病毒掃瞄引擎」的版本，以便評估 OfficeScan 用戶端安全狀況。因此，您無法啟動或關閉預約同步處理。依預設，策略伺服器每五分鐘會與 OfficeScan 伺服器同步處理一次（如需詳細資訊，請參閱同步處理 第 16-14 頁）。

注意

可以在「摘要」畫面上隨時手動同步處理策略伺服器與 OfficeScan 伺服器（請參閱策略伺服器摘要資訊 第 16-38 頁）。

如果要存取 Cisco ACS 管理工作的 Web 主控台畫面，請移至策略伺服器 Web 主控台並按一下主功能表上的「管理」。

第 17 章

設定 OfficeScan 與協力廠商軟體

本章說明 OfficeScan 與協力廠商軟體的整合。

本章內容：

Check Point 架構和組態設定總覽

您可以使用「開放式安全平台」(OPSEC) 架構中的「安全組態驗證」(SCV) 將 OfficeScan 安裝與 Check Point™ SecureClient™ 整合。閱讀本節之前，請先參閱 Check Point SecureClient OPSEC 文件。您可以在下列網址找到 OPSEC 文件：

http://www.opsec.com

Check Point SecureClient 能夠使用「安全組態驗證」(SCV) 檢查，確認連線至網路之電腦的安全組態。SCV 檢查是一組定義已安全設定的用戶端系統的條件。協力廠商軟體可以與 Check Point SecureClient 溝通這些條件的值。接著 Check Point SecureClient 會將這些條件與 SCV 檔中的條件進行比較，以判斷用戶端是否安全。

SCV 檢查會定期執行，以確保只有安全設定的系統才能連線到網路。

SecureClient 會使用策略伺服器將 SCV 檢查傳送至所有在系統上註冊的用戶端。管理員會使用 SCV 編輯程式在策略伺服器上設定 SCV 檢查。

「SCV 編輯程式」是 Check Point 提供的工具，可讓您修改 SCV 檔以便傳送至用戶端安裝。如果要執行「SCV 編輯程式」，請在策略伺服器上尋找並執行 `SCVeditor.exe` 檔。在 SCV 編輯程式中，開啟 `C:\FW1\NG\Conf` 資料夾中的 `local.scv` 檔（如果安裝路徑與預設不同，請將 `C:\FW1` 取代為 Check Point 防火牆的安裝路徑）。

如需使用「SCV 編輯程式」開啟和修改 `SCV` 檔的特定指示，請參閱 OfficeScan 整合 第 17-2 頁。

OfficeScan 整合

OfficeScan 用戶端會定期傳送「病毒碼」號碼與「病毒掃瞄引擎」號碼至 SecureClient 進行驗證。然後，SecureClient 會將這些值與用戶端 `local.scv` 檔中的值進行比較。

如果您在文字編輯器中開啟 `local.scv` 檔，則顯示如下：

```
(SCVObject

:SCVNames (
```

```
: (OfceSCV

:type (plugin)

:parameters (

:CheckType (OfceVersionCheck)

:LatestPatternVersion (701)

:LatestEngineVersion (7.1)

:PatternCompareOp (">=")

:EngineCompareOp (">=")

)

)

)

:SCVPolicy (

: (OfceSCV)

)

:SCVGlobalParams (

:block_connections_on_unverified (true)

:scv_policy_timeout_hours (24)

)

)
```

本範例中，如果病毒碼檔案版本為 701 或更新版本，而且掃瞄引擎號碼為 7.1 或更新版本，則 SCV 檢查將允許透過防火牆連線。如果掃瞄引擎或病毒碼檔案的版本較舊，則會封鎖所有透過 Check Point 防火牆的連線。請使用「SCV 編輯程式」在策略伺服器上修改 `local.scv` 檔中的這些值。

注意

Check Point 不會自動更新 SCV 檔中病毒碼檔案和掃瞄引擎的版本號碼。只要 OfficeScan 更新掃瞄引擎或病毒碼檔案，您就需要手動變更 `local.scv` 檔中的條件值，以便維持最新狀態。如果您未更新掃瞄引擎和病毒碼版本，Check Point 將授權給來自使用舊版病毒碼檔案或掃瞄引擎的用戶端傳輸，因而增加新病毒入侵系統的可能性。

設定 OfficeScan 的「安全組態驗證」檔案

如果要修改 `local.scv` 檔，您必須下載並執行「SCV 編輯程式」(`SCVeditor.exe`)。

程序

1. 從 Check Point 下載網站下載 `SCVeditor.exe`。

   「SCV 編輯程式」為 OPSEC SDK 套件的一部分。

2. 在策略伺服器上執行 `SCVeditor.exe`，

   會開啟「SCV 編輯程式」主控台。

3. 展開「產品」資料夾並選取「`user_policy_scv`」。

4. 按一下「編輯 > 產品 > 修改」，然後在「修改」方塊中輸入 `OfceSCV`。按一下「確定」。

   注意

   如果 `local.scv` 檔已包含其他協力廠商軟體的產品策略，請按一下「編輯 > 產品 > 新增」，然後在「新增」方塊中輸入 `OfceSCV` 建立新策略。

5. 按一下「編輯 > 參數 > 新增」，然後在對應的方塊中輸入「名稱」和「值」來新增參數。

   下表列出參數名稱和值。參數名稱和值有區分大小寫。請依照表格所列順序輸入。

表 17-1. SCV 檔案參數的名稱和值

名稱	值
CheckType	OfceVersionCheck
LatestPatternVersion	<目前的病毒碼檔案號碼>
LatestEngineVersion	<目前的掃瞄引擎號碼>
LatestPatternDate	<目前的病毒碼檔案發行日期>
PatternCompareOp	>=
EngineCompareOp	>=
PatternMismatchMessage	
EngineMismatchMessage	

輸入最新的病毒碼檔案號碼和掃瞄引擎號碼，取代大括號內的文字。您可以按一下 OfficeScan Web 主控台主功能表上的「更新 &升級」，來檢視用戶端最新的病毒碼和掃瞄引擎版本。 病毒碼版本號碼會出現在代表受保護的 OfficeScan 用戶端百分比的圓形圖右側。

6. 選取「封鎖未驗證 SCV 上的連線」。
7. 按一下「編輯 > 產品 > 執行」。
8. 按一下「檔案｜ > 產生策略檔案」，建立該檔案。選取現有的 `local.scv` 檔將它覆寫。

安裝 SecureClient 支援模組

如果使用者從「虛擬私人網路」(VPN) 連線到辦公室網路，而且其電腦上同時安裝了 Check Point SecureClient 和 OfficeScan 用戶端，請指示他們安裝 SecureClient 支援。這個模組可讓 SecureClient 在 VPN 用戶端上執行 SCV 檢查，確保只有經過安全設定的系統才能連線到網路。使用者可以檢查系統匣上的 () 圖示來確認其電腦是否有安裝 Check Point SecureClient。使用者也可以檢

查 Windows 的「新增/移除程式」畫面中是否有名為「Check Point SecureClient」的項目。

使用者會從 OfficeScan 用戶端主控台的「工具箱」標籤啟動安裝。只有在使用者擁有必要的權限，且 OfficeScan 用戶端電腦的作業系統是 Windows XP 或 Windows Server 2003 時，才會顯示此標籤。

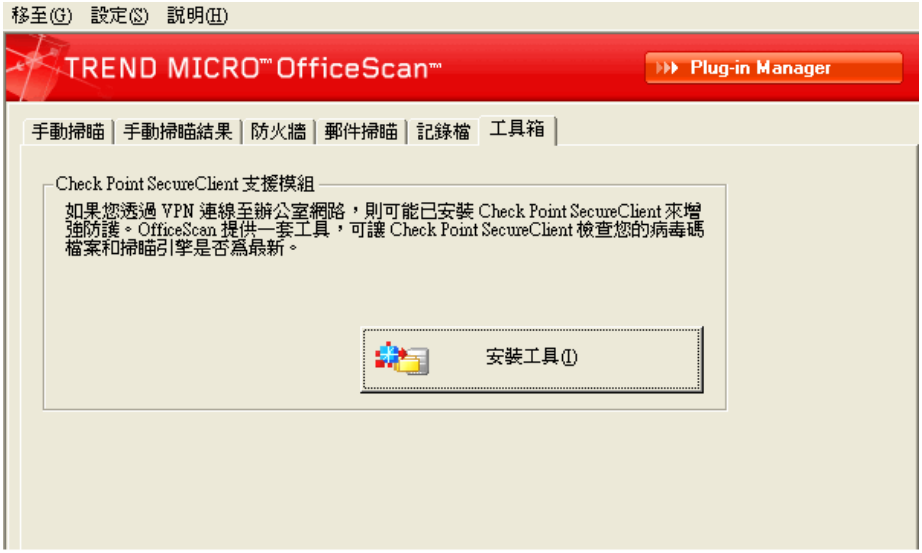


圖 17-1. OfficeScan 用戶端主控台上的「工具箱」標籤

授與使用者檢視工具箱標籤的權限

程序

1. 瀏覽至「用戶端電腦｜ > 用戶端管理」。
2. 在用戶端樹狀結構中，按一下根網域圖示 ( ) 以包含所有的用戶端，或選取特定網域或用戶端。

注意

「Check Point SecureClient 支援」不支援 IPv6。您不能將此模組部署到單純 IPv6 端點。

3. 按一下「設定 > 權限和其他設定」。
4. 在「使用權限」標籤中，移至「工具箱權限」區段。
5. 選取「顯示用戶端主控台上的「工具箱」標籤，並允許使用者安裝「Check Point SecureClient 支援模組」」。
6. 如果在用戶端樹狀結構中選取網域或用戶端，請按一下「儲存」。如果按下了根網域圖示，則從下列選項進行選擇：
   - 套用至所有用戶端：將設定套用至所有現有的用戶端，並套用至任何加入現有/未來網域中的新用戶端。未來網域是指在您設定這些設定時尚未建立的網域。
   - 僅套用於未來網域：僅將設定套用至加入未來網域中的用戶端。這個選項不會將設定套用到加入現有網域中的新用戶端。

安裝 SecureClient 支援模組

程序

1. 開啟 OfficeScan 用戶端主控台。
2. 按一下「工具箱」標籤。
3. 在「Check Point SecureClient 支援」下，按一下「安裝工具」，

   會出現確認畫面。
4. 按一下「是」。

   OfficeScan 用戶端會連線到伺服器並下載模組。下載完成時，OfficeScan 會顯示訊息。

5. 按一下「確定」。

第 18 章

取得說明

本章說明如何疑難排解您可能會遇到的問題，以及如何與客服人員聯絡。

本章內容：

疑難排解資源

本節提供一份資源清單，可讓您用來對 OfficeScan 伺服器和 OfficeScan 用戶端問題進行疑難排解。

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 OfficeScan 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。

在 OfficeScan 支援的所有平台上執行此工具。如果要取得這項工具和相關文件，請聯絡您的經銷商。

趨勢科技效能調整工具

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

如需詳細資訊，請參閱 http://esupport.trendmicro.com/solution/zh-tw/1074941.aspx。

OfficeScan 伺服器記錄檔

除了 Web 主控台上提供的記錄檔之外，您還可以使用其他類型的記錄檔（例如：偵錯記錄檔）來解決產品問題。

警告!

偵錯記錄檔可能會影響伺服器的效能，並且消耗大量的磁碟空間。務必僅在必要時啟動偵錯記錄，並且在不需要偵錯資料時立即關閉。如果您需要節省磁碟空間，請移除記錄檔。

使用 LogServer.exe 的伺服器偵錯記錄檔

使用 `LogServer.exe` 來收集下列項目的偵錯記錄檔：

- OfficeScan 伺服器基本記錄檔
- Trend Micro Vulnerability Scanner
- Active Directory 整合記錄檔
- 用戶端分組記錄檔
- 安全性符合記錄檔
- 以角色為基礎的管理
- 雲端截毒掃瞄
- 策略伺服器

正在啟動偵錯記錄

程序

1. 登入 Web 主控台。
2. 在 Web 主控台的標題上，按一下「OfficeScan」中的第一個「O」。
3. 指定偵錯記錄檔設定。
4. 按一下「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`。

正在關閉偵錯記錄

程序

1. 登入 Web 主控台。
2. 在 Web 主控台的標題上，按一下「OfficeScan」中的第一個「O」。
3. 清除「啟動偵錯記錄檔」。
4. 按一下「儲存」。

正在啟動伺服器安裝和升級的偵錯記錄

請先啟動偵錯記錄，再執行下列工作：

- 先解除安裝伺服器，然後再安裝一次。
- 將 OfficeScan 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電腦上啟動，而不會在遠端電腦上啟動）。

程序

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

```
[debug]

debuglevel=9

debuglog=c:\LogServer\ofcdebug.log

debugLevel_new=D

debugSplitSize=10485760

debugSplitPeriod=12

debugRemoveAfterSplit=1
```

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

安裝記錄檔

- 本機安裝/升級記錄檔

  檔案名稱：OFCMAS.LOG

  位置：%windir%

- 遠端安裝/升級記錄檔
  - 在您啟動安裝程式的電腦上：

    檔案名稱：ofcmasr.log

    位置：%windir%

- 在目標電腦上：

  檔案名稱：`OFCMAS.LOG`

  位置：`%windir%`

Active Directory 記錄檔

- 檔案名稱：`ofcdebug.log`
- 檔案名稱：`ofcserver.ini`

  位置：<伺服器安裝資料夾>`\PCCSRV\Private\`
- 檔案名稱：
  - `dbADScope.cdx`
  - `dbADScope.dbf`
  - `dbADPredefinedScope.cdx`
  - `dbADPredefinedScope.dbf`
  - `dbCredential.cdx`
  - `dbCredential.dbf`

  位置：<伺服器安裝資料夾>`\PCCSRV\HTTPDB\`

以角色為基礎的管理記錄檔

如果要取得詳細的以角色為基礎的管理資訊，請執行下列其中一項作業：

- 執行 Trend Micro Case Diagnostics Tool。如需相關資訊，請參閱 Case Diagnostic Tool 第 18-2 頁。
- 收集下列記錄檔：
  - <伺服器安裝資料夾>`\PCCSRV\Private\AuthorStore` 資料夾中的所有檔案。

- OfficeScan 伺服器記錄檔 第 18-3 頁

OfficeScan 用戶端分組記錄檔

- 檔案名稱：ofcdebug.log
- 檔案名稱：ofcserver.ini

  位置：<伺服器安裝資料夾>\PCCSRV\Private\
- 檔案名稱：SortingRule.xml

  位置：<伺服器安裝資料夾>\PCCSRV\Private\SortingRuleStore\
- 檔案名稱：
  - dbADScope.cdx
  - dbADScope.dbf

  位置：<伺服器安裝資料夾>\HTTPDB\

元件更新記錄檔

檔案名稱：TmuDump.txt

位置：<伺服器安裝資料夾>\PCCSRV\Web\Service\AU_Data\AU_Log

正在取得詳細的伺服器更新資訊

程序

1. 建立名為 aucfg.ini 的檔案，其中包含下列內容：

```
[Debug]
level=-1
[Downloader]
```

```
ProxyCache=0
```

2. 將檔案儲存到 <伺服器安裝資料夾>\PCCSRV\Web\Service。
3. 重新啟動「OfficeScan 主服務」。

正在停止收集詳細的伺服器更新資訊

程序

1. 刪除 aucfg.ini。
2. 重新啟動「OfficeScan 主服務」。

Apache 伺服器記錄檔

檔案名稱：

- install.log
- error.log
- access.log

位置：<伺服器安裝資料夾>\PCCSRV\Apache2

Client Packager 記錄檔

正在啟動建立 Client Packager 的記錄

程序

1. 在<伺服器安裝資料夾>\PCCSRV\Admin\Utility\ClientPackager 中修改 ClnExtor.ini，如下所示：

```
[Common]
```

DebugMode=1

2. 檢查 C:\ 中的 ClnPack.log。

正在關閉建立 Client Packager 的記錄

程序

1. 開啟 ClnExtor.ini。
2. 將「DebugMode」值從 1 變更為 0。

安全符合性報告記錄檔

如果要取得詳細的「安全性符合」資訊，請收集下列檔案：

- 檔案名稱：RBAUserProfile.ini

  位置：<伺服器安裝資料夾>\PCCSRV\Private\AuthorStore\

- 在 <伺服器安裝資料夾>\PCCSRV\Log\Security Compliance Report 資料夾中的所有檔案。
- OfficeScan 伺服器記錄檔 第 18-3 頁

外部伺服器管理記錄檔

- 檔案名稱：ofcdebug.log
- 檔案名稱：ofcserver.ini

  位置：<伺服器安裝資料夾>\PCCSRV\Private\

- 在 <伺服器安裝資料夾>\PCCSRV\Log\Outside Server Management Report\ 資料夾中的所有檔案。
- 檔案名稱：

- dbADScope.cdx
- dbADScope.dbf
- dbClientInfo.cdx
- dbclientInfo.dbf

位置：<伺服器安裝資料夾>\HTTPDB\

周邊設備存取控管例外記錄檔

如果要取得詳細的「周邊設備存取控管例外」資訊，請收集下列檔案：

- 檔案名稱：ofcscan.ini

  位置：<伺服器安裝資料夾>\
- 檔案名稱：dbClientExtra.dbf

  位置：<伺服器安裝資料夾>\HTTPDB\
- 來自 OfficeScan Web 主控台的「周邊設備存取控管例外」清單。

網頁信譽評等記錄檔

檔案名稱：diagnostic.log

位置：<伺服器安裝資料夾>\PCCSRV\LWCS\

ServerProtect 一般伺服器移轉工具記錄檔

正在開啟「ServerProtect 一般伺服器移轉工具」的偵錯記錄

程序

1. 建立名為 ofcdebug.ini 的檔案，其中包含下列內容：

```
[Debug]

DebugLog=C:\ofcdebug.log

DebugLevel=9
```

2. 將檔案儲存到 C:\。
3. 檢查 C:\ 中的 ofcdebug.log。

注意

若要關閉偵錯記錄，請刪除 ofcdebug.ini 檔案。

VSEncrypt 記錄檔

OfficeScan 會自動在使用者帳號的暫存資料夾中建立偵錯記錄檔 (VSEncrypt.log)。例如，C:\Documents and Settings\<使用者名稱>\Local Settings\Temp。

Control Manager MCP 代理程式記錄檔

對 <伺服器安裝資料夾>\PCCSRV\CMAgent 資料夾中的檔案進行偵錯

- Agent.ini
- Product.ini
- 「Control Manager 設定」網頁擷取畫面
- ProductUI.zip

正在啟動 MCP 代理程式的偵錯記錄

程序

1. 修改 <伺服器安裝資料夾>\PCCSRV\CmAgent 中的 product.ini，如下所示：

```
[Debug]

debugmode = 3

debuglevel= 3

debugtype = 0

debugsize = 10000

debuglog = C:\CMAgent_debug.log
```

2. 從 Microsoft 管理主控台重新啟動 OfficeScan Control Manager 代理程式服務。
3. 檢查 `C:\` 中的 `CMAgent_debug.log`。

正在關閉 MCP 代理程式的偵錯記錄

程序

1. 開啟 `product.ini` 並刪除下列內容：

```
debugmode = 3

debuglevel= 3

debugtype = 0

debugsize = 10000

debuglog = C:\CMAgent_debug.log
```

2. 重新啟動 OfficeScan Control Manager 服務。

病毒掃瞄引擎記錄檔

正在啟動病毒掃瞄引擎用戶端的偵錯記錄

程序

1. 開啟「登錄編輯程式」(regedit.exe)。
2. 移至 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMFilter\Parameters。
3. 將「DebugLogFlags」的值變更為「00003eff」。
4. 執行引導您掃瞄所遭遇問題的步驟。
5. 檢查 %windir% 中的 TMFilter.log。

注意

將「DebugLogFlags」的值恢復為「00000000」以關閉偵錯記錄

病毒/惡意程式記錄檔

檔案名稱：

- dbVirusLog.dbf
- dbVirusLog.cdx

位置：<伺服器安裝資料夾>\PCCSRV\HTTPDB\

間諜程式/可能的資安威脅程式記錄檔

檔案名稱：

- dbSpywareLog.dbf
- dbSpywareLog.cdx

位置：<伺服器安裝資料夾>\PCCSRV\HTTPDB\

病毒爆發記錄檔

目前的防火牆違規病毒爆發記錄檔

檔案名稱：Cfw_Outbreak_Current.log

位置：<伺服器安裝資料夾>\PCCSRV\Log\

上次防火牆違規病毒爆發記錄檔

檔案名稱：Cfw_Outbreak_Last.log

位置：<伺服器安裝資料夾>\PCCSRV\Log\

目前的病毒/惡意程式爆發記錄檔

檔案名稱：Outbreak_Current.log

位置：<伺服器安裝資料夾>\PCCSRV\Log\

上次病毒/惡意程式爆發記錄檔

檔案名稱：Outbreak_Last.log

位置：<伺服器安裝資料夾>\PCCSRV\Log\

目前的間諜程式/可能的資安威脅程式爆發記錄檔

檔案名稱：Spyware_Outbreak_Current.log

位置：<伺服器安裝資料夾>\PCCSRV\Log\

上次間諜程式/可能的資安威脅程式爆發記錄檔

檔案名稱：Spyware_Outbreak_Last.log

位置：<伺服器安裝資料夾>\PCCSRV\Log\

虛擬桌面支援記錄檔

- 檔案名稱：vdi_list.ini

  位置：<伺服器安裝資料夾>\PCCSRV\TEMP\

- 檔案名稱：vdi.ini

  位置：<伺服器安裝資料夾>\PCCSRV\Private\

- 檔案名稱：ofcdebug.txt

  位置：<伺服器安裝資料夾>\PCCSRV\

如果要產生 ofcdebug.txt，請啟動偵錯記錄。如需啟動偵錯記錄的指示，請參閱正在啟動偵錯記錄 第 18-4 頁。

OfficeScan 用戶端記錄檔

可以使用 OfficeScan 用戶端記錄檔（例如：偵錯記錄檔）對 OfficeScan 用戶端問題進行疑難排解。

警告!

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

使用 LogServer.exe 的 OfficeScan 用戶端偵錯記錄檔

正在啟動 OfficeScan 用戶端的偵錯記錄

程序

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:\`。

   注意

   `LogServer.exe` 會自動在每次 OfficeScan 用戶端電腦啟動時執行。指示使用者「不要」關閉電腦啟動時開啟的 LogServer.exe 命令視窗，因為這會提示 OfficeScan 停止偵錯記錄功能。如果使用者關閉命令視窗，可以執行位於 <用戶端安裝資料夾> 的 `LogServer.exe` 以再次啟動偵錯記錄功能。

3. 在每部 OfficeScan 用戶端電腦上，檢查 C:\ 中的 ofcdebug.log。

注意

透過刪除 `ofcdebug.ini` 即可關閉 OfficeScan 用戶端的偵錯記錄功能。

全新安裝記錄檔

檔案名稱：OFCNT.LOG

位置：

- %windir%（適用於所有 MSI 套件以外的安裝方法）
- %temp%（適用於 MSI 套件安裝方法）

升級/HotFix 記錄檔

檔案名稱：upgrade_yyyymmddhhmmss.log

位置：<用戶端安裝資料夾>

損害清除及復原服務記錄檔

正在啟動「損害清除及復原服務」的偵錯記錄

程序

1. 開啟 <用戶端安裝資料夾> 中的 TSC.ini。
2. 修改下列這行的內容：

   DebugInfoLevel=3

3. 檢查 <用戶端安裝資料夾>\debug 中的 TSCDebug.log。

正在關閉「損害清除及復原服務」的偵錯記錄

開啟 TSC.ini 並將「DebugInfoLevel」值從 3 變更為 0。

清除記錄檔

檔案名稱：Conn_YYYYMMDD.log

位置：<用戶端安裝資料夾>\report\

郵件掃瞄記錄檔

檔案名稱：SmolDbg.txt

位置：<用戶端安裝資料夾>

主動式更新記錄檔

- 檔案名稱：Update.ini

  位置：<用戶端安裝資料夾>

- 檔案名稱：TmuDump.txt

  位置：<用戶端安裝資料夾>\AU_Log\

OfficeScan 用戶端連線記錄檔

檔案名稱：Conn_YYYYMMDD.log

位置：<用戶端安裝資料夾>\ConnLog

OfficeScan 用戶端更新記錄檔

檔案名稱：Tmudump.txt

位置：<用戶端安裝資料夾>\AU_Data\AU_Log

取得 OfficeScan 用戶端詳細的更新資訊

程序

1. 建立名為 `aucfg.ini` 的檔案，其中包含下列內容：

   ```
   [Debug]

   level=-1

   [Downloader]

   ProxyCache=0
   ```

2. 將檔案儲存到 <用戶端安裝資料夾>。
3. 重新載入 OfficeScan 用戶端。

注意

刪除 `aucfg.ini` 檔案並且重新載入 OfficeScan 用戶端以停止收集詳細的用戶端更新資訊。

病毒爆發防範記錄檔

檔案名稱：`OPPLogs.log`

位置：<用戶端安裝資料夾>`\OppLog`

病毒爆發防護恢復記錄檔

檔案名稱：

- `TmOPP.ini`
- `TmOPPRestore.ini`

位置：<用戶端安裝資料夾>\

OfficeScan 防火牆記錄檔

在 Windows Vista/Server 2008/7/Server 2012/8 電腦上啟動一般防火牆驅動程式的偵錯記錄

程序

1. 修改下列登錄值：

登錄機碼	值
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmwfp\Parameters	類型：DWORD 值 (REG_DWORD) 名稱：DebugCtrl 值：0x00001111
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmlwf\Parameters	類型：DWORD 值 (REG_DWORD) 名稱：DebugCtrl 值：0x00001111

2. 重新啟動電腦。
3. 檢查 C:\ 中的 wfp_log.txt 和 lwf_log.txt。

正在 Windows XP 和 Windows Server 2003 電腦上啟動一般防火牆驅動程式的偵錯記錄

程序

1. 將下列資料新增至 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmcfw\Parameters：
   - 類型：DWORD 值 (REG_DWORD)
   - 名稱：DebugCtrl
   - 值：0x00001111

2. 重新啟動電腦。
3. 檢查 C:\ 中的 cfw_log.txt。

正在關閉一般防火牆驅動程式的偵錯記錄（所有作業系統）

程序

1. 刪除登錄機碼中的 DebugCtrl。
2. 重新啟動電腦。

正在啟動 OfficeScan NT 防火牆服務的偵錯記錄

程序

1. 按照下列方式編輯 <用戶端安裝資料夾> 中的 TmPfw.ini：

```
[ServiceSession]
Enable=1
```

2. 重新載入用戶端。
3. 檢查 C:\temp 中的 ddmmyyyy_NSC_TmPfw.log。

正在關閉 OfficeScan NT 防火牆服務的偵錯記錄

程序

1. 開啟 TmPfw.ini，並將「Enable」值從 1 變更為 0。
2. 重新載入 OfficeScan 用戶端。

網頁信譽評等和 POP3 郵件掃瞄記錄檔

正在啟動網頁信譽評等服務和 POP3 郵件掃瞄功能的除錯記錄

程序

1. 編輯位於 <用戶端安裝資料夾>中的 `TmProxy.ini`，如下所示：

   ```
   [ServiceSession]

   Enable=1

   LogFolder=C:\temp
   ```

2. 重新載入 OfficeScan 用戶端。

3. 檢查 `C:\temp` 中的 `ddmmyyyy_NSC_TmProxy.log`。

正在關閉網頁信譽評等服務和 POP3 郵件掃瞄功能的除錯記錄

程序

1. 開啟 `TmProxy.ini`，並將「`Enable`」值從 1 變更為 0。

2. 重新載入 OfficeScan 用戶端。

周邊設備存取控管例外清單記錄檔

檔案名稱：`DAC_ELIST`

位置：<用戶端安裝資料夾>\

資料安全防護偵錯記錄檔

啟動資料安全防護模組的偵錯記錄功能

程序

1. 從支援供應商處取得 `logger.cfg` 檔案。
2. 將下列資料新增至 `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\DlpLite`：
   - 類型：字串
   - 名稱：`debugcfg`
   - 值：`C:\Log\logger.cfg`
3. 在 `C:\ directory` 目錄中建立名為 “「Log」” 的資料夾。
4. 將 `logger.cfg` 複製到 “Log” 資料夾。
5. 從 Web 主控台部署「Data Loss Prevention」和「周邊設備存取控管」設定，以開始收集記錄檔。

注意

透過刪除登錄機碼中的 `debugcfg`，然後重新啟動電腦，以關閉資料安全防護模組的偵錯記錄功能。

Windows 事件記錄檔

Windows 事件檢視器會記錄成功發生的應用程式事件，例如登入或變更帳號設定。

程序

1. 執行下列其中一項作業：

- 按一下「開始 > 控制台 > 效能與維護 > 系統管理工具 > 電腦管理」。
- 開啟包含事件檢視器嵌入式管理單元的 MMC。

2. 按一下「事件檢視器」。

傳輸驅動程式介面 (TDI) 記錄檔

正在啟動 TDI 的偵錯記錄

程序

1. 將下列資料新增至 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\tmtdi\Parameters`：

參數	值
機碼 1	類型：`DWORD 值 (REG_DWORD)` 名稱：偵錯 值：`1111 (十六進位)`
機碼 2	類型：字串值 `(REG_SZ)` 名稱：`LogFile` 值：`C:\tmtdi.log`

2. 重新啟動電腦。
3. 檢查 `C:\` 中的 `tmtdi.log`。

注意

在登錄機碼刪除「`Debug`」和「`LogFile`」然後重新開機以關閉 TDI 的偵錯記錄。

聯絡客戶服務部門

趨勢科技提供所有已註冊使用者為期一年的技術支援、病毒碼下載和程式更新，之後您則必須購買更新維護。如果需要協助或有任何問題，請隨時與我們聯絡。也歡迎您提供寶貴的意見。

全球客戶服務據點：

http://www.trendmicro.com/support

趨勢科技產品文件：

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

聯絡資訊

在美國，您可以透過電話、傳真或電子郵件聯絡趨勢科技銷售人員：

Trend Micro, Inc. 10101 North De Anza Blvd., Cupertino, CA 95014

免付費電話：+1 (800) 228-5651 (業務) 語音電話：+1 (408) 257-1500 (主要) 傳真： +1 (408) 257-2003

網址：www.trendmicro.com

電子郵件：support@trendmicro.com

加速支援要求

當您聯絡趨勢科技時，為加速解決您的問題，請務必備妥下列詳細資料：

- Microsoft Windows 和 Service Pack 版本
- 網路類型
- 電腦廠牌、型號和任何其他已連接到您電腦的硬體
- 您電腦的記憶體大小和可用硬碟空間

- 安裝環境的詳細說明
- 任何所出現錯誤訊息的確切文字
- 問題模擬的步驟

趨勢科技常見問題集

趨勢科技網站的「趨勢科技常見問題集」提供最新的產品問題解答。如果在產品文件中找不到解答，您也可以使用「常見問題集」送出問題。「常見問題集」的網址如下：

http://www.trendmicro.com.tw/solutionbank/corporate/default.asp

趨勢科技會持續更新「常見問題集」的內容，並每日新增解決方案。不過，如果您找不到解答，可在電子郵件中描述問題，並將其直接傳送給趨勢科技的支援工程師，工程師會調查問題並儘速回應。

TrendLabs

TrendLabs^{SM} 是趨勢科技的全球防毒研究與支援中心。TrendLabs 位於三大洲，延攬了超過 250 位研究人員和工程師，全天候為您和趨勢科技客戶提供服務與支援。

您可以信賴下列的售後服務：

- 一般病毒碼更新，更新所有已知的「監管中」和「非監管中」的電腦病毒和惡意程式碼
- 緊急病毒爆發支援
- 傳送電子郵件給防毒工程師
- 常見問題集，技術支援問題的趨勢科技線上資料庫

TrendLabs 已獲 ISO 9002 國際品質認證。

安全資訊中心

趨勢科技網站提供了完整的安全資訊：

- 目前「擴散中」或作用中的病毒和惡意機動程式碼清單
- 電腦病毒惡作劇
- Internet 安全威脅諮詢
- 病毒週報
- 病毒百科全書（其中包括已知的病毒和惡意可攜式程式碼的名稱與癥狀的完整清單）
- 詞彙表
- http://www.trendmicro.com/vinfo/zh-tw

文件意見反應

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或建議，請移至下列網站：

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

附錄 A

OfficeScan 的 IPv6 支援

本附錄的適用對象是打算在支援 IPv6 定址的環境中部署 OfficeScan 的使用者。本附錄包含有關 OfficeScan 中 IPv6 支援範圍的資訊。

趨勢科技假設讀者熟悉 IPv6 概念及設定支援 IPv6 定址之網路的相關工作。

適用於 OfficeScan 伺服器和用戶端的 IPv6 支援

從此 10.6 版開始，OfficeScan 可支援 IPv6。先前的 OfficeScan 版本不支援 IPv6 定址。安裝或升級符合 IPv6 需求的 OfficeScan 伺服器和 OfficeScan 用戶端之後，會自動啟動 IPv6 支援。

OfficeScan 伺服器需求

OfficeScan 伺服器的 IPv6 需求如下：

- 伺服器必須安裝在 Windows Server 2008 或 Windows Server 2012 上，不能安裝在 Windows Server 2003 上，因為該作業系統無法完全支援 IPv6 定址。
- 伺服器必須使用 IIS Web 伺服器。Apache Web Server 不支援 IPv6 定址。
- 如果伺服器將管理 IPv4 和 IPv6 OfficeScan 用戶端，則必須同時具有 IPv4 和 IPv6 位址，且必須由其主機名稱加以識別。如果伺服器是由其 IPv4 位址所識別，則 IPv6 OfficeScan 用戶端無法連線到該伺服器。如果純 IPv4 用戶端連線到由其 IPv6 位址所識別的伺服器，則會發生相同的問題。
- 如果伺服器將只會管理 IPv6 用戶端，則最低需求為一個 IPv6 位址。伺服器可由其主機名稱或 IPv6 位址加以識別。當伺服器由其主機名稱所識別時，會偏好使用其「完整合格的網域名稱 (FQDN)」。這是因為在純 IPv6 環境中，WINS 伺服器無法將主機名稱轉換為其對應的 IPv6 位址。

> **注意**
>
> 只有在執行伺服器的本機安裝時，才能指定 FQDN。遠端安裝不支援這項作業。

OfficeScan 用戶端需求

OfficeScan 用戶端必須安裝在以下系統上：

- Windows 7
- Windows Server 2008
- Windows Vista
- Windows 8
- Windows Server 2012

請勿將其安裝在 Windows Server 2003 和 Windows XP 上，因為這些作業系統無法完全支援 IPv6 定址。

OfficeScan 用戶端最好同時具有 IPv4 和 IPv6 位址，因為與它連線的一些實體僅支援 IPv4 定址。

單純 IPv6 伺服器的限制

下表列出 OfficeScan 伺服器僅具有 IPv6 位址時所存在的限制。

表 A-1. 單純 IPv6 伺服器的限制

項目	限制
用戶端管理	純 IPv6 伺服器無法執行以下操作： • 將 OfficeScan 用戶端部署到純 IPv4 端點。 • 管理純 IPv4 OfficeScan 用戶端。
更新和集中式管理	純 IPv6 伺服器無法從純 IPv4 更新來源更新，例如： • 趨勢科技主動式更新伺服器 • Control Manager 5.5 • Control Manager 5.0 注意 Control Manager 自 5.5 SP1 版起才開始支援 IPv6。 • 任何純 IPv4 自訂更新來源

項目	限制
產品註冊、啟動和續約	純 IPv6 伺服器無法連線到趨勢科技線上註冊伺服器註冊產品、取得使用授權和啟動/續約使用授權。
Proxy 伺服器連線	純 IPv6 伺服器無法透過純 IPv4 Proxy 伺服器進行連線。
嵌入程式解決方案	純 IPv6 伺服器會包含 Plug-In Manager，但無法將任何嵌入程式解決方案部署到： • 純 IPv4 OfficeScan 用戶端或純 IPv4 主機（因為無法直接連線） • 純 IPv6 OfficeScan 用戶端或純 IPv6 主機（因為嵌入程式解決方案都不支援 IPv6）。

透過設定可在 IPv4 和 IPv6 位址之間進行轉換的雙堆疊 Proxy 伺服器（例如 DeleGate），可以克服上述大部分的限制。將 Proxy 伺服器置於 OfficeScan 伺服器以及它所連線或服務的實體之間。

純 IPv6 OfficeScan 用戶端的限制

下表列出 OfficeScan 用戶端僅具有 IPv6 位址時所存在的限制。

表 A-2. 純 IPv6 OfficeScan 用戶端限制

項目	限制
上層 OfficeScan 伺服器	純 IPv4 OfficeScan 伺服器無法管理純 IPv6 OfficeScan 用戶端。
更新	純 IPv6 OfficeScan 用戶端無法從純 IPv4 更新來源更新，例如： • 趨勢科技主動式更新伺服器 • 純 IPv4 OfficeScan 伺服器 • 純 IPv4 更新代理程式 • 任何純 IPv4 自訂更新來源

項目	限制
掃瞄查詢、網頁信譽評等查詢以及 Smart Feedback	純 IPv6 OfficeScan 用戶端無法傳送查詢到主動式雲端截毒技術伺服器來源，例如： • 主動式雲端截毒技術伺服器 2.0（整合式或獨立式） 注意 主動式雲端截毒技術伺服器自 2.5 版開始會支援 IPv6。 • 趨勢科技主動式雲端截毒技術（也用於 Smart Feedback）
軟體安全	純 IPv6 OfficeScan 用戶端無法連線到趨勢科技裝載的認證安全防護軟體服務。
嵌入程式解決方案	純 IPv6 OfficeScan 用戶端無法安裝嵌入程式解決方案，因為所有 Plug-in 解決方案都不支援 IPv6。
程式	由於以下程式不支援 IPv6，因此純 IPv6 OfficeScan 用戶端無法安裝它們： • Cisco Trust Agent • Check Point SecureClient 支援
Proxy 伺服器連線	純 IPv6 OfficeScan 用戶端無法透過純 IPv4 Proxy 伺服器進行連線。

透過設定可在 IPv4 和 IPv6 位址之間進行轉換的雙堆疊 Proxy 伺服器（例如 DeleGate），可以克服上述大部分的限制。將 Proxy 伺服器置於 OfficeScan 用戶端與它們連線的實體之間。

設定 IPv6 位址

透過 Web 主控台可設定 IPv6 位址或 IPv6 位址範圍。下面是一些組態設定準則。

- OfficeScan 接受標準的 IPv6 位址表示法。

例如：

```
2001:0db7:85a3:0000:0000:8a2e:0370:7334
```

```
2001:db7:85a3:0:0:8a2e:370:7334
```

```
2001:db7:85a3::8a2e:370:7334
```

```
::ffff:192.0.2.128
```

- OfficeScan 也接受連結-本機 IPv6 位址，例如：

```
fe80::210:5aff:feaa:20a2
```

警告!

指定連結-本機 IPv6 位址時應謹慎小心，因為即使 OfficeScan 可以接受這類位址，但它可能在某些情況下無法如預期般運作。例如，如果更新來源位於其他網路區段且由可其連結-本機 IPv6 位址所辨識，OfficeScan 用戶端就無法從該來源進行更新。

- IPv6 位址是 URL 的一部分時，請使用方括號 ([]) 將位址括起來。
- 對於 IPv6 位址範圍，通常需要輸入字首和字首長度。對於需要伺服器查詢 IP 位址的組態，會套用字首長度限制，以防止伺服器查詢大量 IP 位址時可能出現效能問題。例如，對於外部伺服器管理功能，字首長度只能介於 112（65,536 個 IP 位址）和 128（2 個 IP 位址）之間。
- 涉及 IPv6 位址或位址範圍的某些設定會部署到 OfficeScan 用戶端，但是 OfficeScan 用戶端會略過這些設定。例如，如果設定了主動式雲端截毒技術伺服器來源清單，其中包括可由其 IPv6 位址辨識的主動式雲端截毒技術伺服器，則純 IPv4 OfficeScan 用戶端會略過該伺服器並連線到其他主動式雲端截毒技術伺服器來源。

顯示 IP 位址的畫面

本主題將列舉 Web 主控台中顯示 IP 位址的位置。

- 用戶端樹狀結構

無論何時顯示用戶端樹狀結構，純 IPv6 OfficeScan 用戶端的 IPv6 位址都會顯示在「IP 位址」欄下方。對於雙堆疊 OfficeScan 用戶端，如果它們使用自己的 IPv6 位址向伺服器註冊，則會顯示它們的 IPv6 位址。

注意

雙堆疊 OfficeScan 用戶端向伺服器註冊時使用的 IP 位址可透過用戶端電腦 > 全域用戶端設定 > 偏好的 IP 位址進行控制。

將用戶端樹狀結構設定匯出至檔案時，IPv6 位址也會顯示在匯出檔案中。

- 用戶端狀態

  瀏覽至「用戶端電腦 > 用戶端管理」 > 狀態時，可取得詳細的用戶端資訊。在這個畫面中，會看到純 IPv6 OfficeScan 用戶端的 IPv6 位址以及使用自己的 IPv6 位址向伺服器註冊的雙堆疊 OfficeScan 用戶端的 IPv6 位址。

- 記錄檔

  雙堆疊用戶端和純 IPv6 OfficeScan 用戶端的 IPv6 位址會顯示在以下記錄檔中：

  - 病毒/惡意程式記錄檔
  - 間諜程式/可能的資安威脅程式記錄檔
  - 防火牆記錄檔
  - 連線驗證記錄檔

- Control Manager 主控台

  下表列出哪些 OfficeScan 伺服器和 OfficeScan 用戶端的 IP 位址會顯示在 Control Manager 主控台上。

表 A-3. 顯示在 Control Manager 主控台上的 OfficeScan 伺服器和 OfficeScan 用戶端 IP 位址

OfficeScan	Control Manager 版本		
	5.5 SP1	5.5	5.0
雙堆疊伺服器	IPv4 和 IPv6	IPv4	IPv4
純 IPv4 伺服器	IPv4	IPv4	IPv4
純 IPv6 伺服器	IPv6	不支援	不支援
雙堆疊 OfficeScan 用戶端	OfficeScan 用戶端向 OfficeScan 伺服器註冊所使用的 IP 位址	OfficeScan 用戶端向 OfficeScan 伺服器註冊所使用的 IP 位址	OfficeScan 用戶端向 OfficeScan 伺服器註冊所使用的 IP 位址
純 IPv4 OfficeScan 用戶端	IPv4	IPv4	IPv4
純 IPv6 OfficeScan 用戶端	IPv6	IPv6	IPv6

附錄 B

Windows Server Core 2008/2012 支援

本附錄討論 Windows Server Core 2008/2012 的 OfficeScan 支援。

Windows Server Core 2008/2012 支援

Windows Server Core 2008/2012 是 Windows Server 2008/2012 的「最小」安裝。在 Server Core 中：

- 許多 Windows Server 2008/2012 選項和功能都已移除。
- 伺服器是執行極精簡的核心作業系統。
- 工作大部分都必須從命令列介面執行。
- 作業系統只執行少數服務，而且在啟動期間只需要少量資源。

OfficeScan 用戶端支援 Server Core。本節包含有關 Server Core 支援的資訊。

OfficeScan 伺服器不支援 Server Core。

Windows Server Core 安裝方法

不支援下列安裝方法或只支援部分安裝方法：

- Web 安裝網頁：因為 Server Core 沒有 Internet Explorer，所以不支援這種方法。
- Trend Micro Vulnerability Scanner：Vulnerability Scanner 工具無法在 Server Core 本機上執行。請從 OfficeScan 伺服器或另一部電腦執行此工具。

下列是支援的安裝方法：

- 遠端安裝。如需詳細資訊，請參閱從 OfficeScan Web 主控台遠端安裝 第 5-17 頁。
- Login Script Setup
- 用戶端封裝程式

使用 Login Script Setup 安裝 OfficeScan 用戶端

程序

1. 開啟命令提示字元。
2. 輸入下列命令以對應 AutoPcc.exe 檔案的位置：

   ```
   net use <對應磁碟機代號> \\<OfficeScan 伺服器主機名稱或 IP 位址>\ofcscan
   ```

   例如：

   ```
   net use P:\\10.1.1.1\ofcscan
   ```

   隨即顯示訊息，通知您 AutoPcc.exe 的位置是否對應成功。
3. 輸入對應的磁碟機代號及冒號，以切換至 AutoPcc.exe 的位置。例如：

   ```
   P:
   ```
4. 輸入下列命令以啟動安裝：

   ```
   AutoPcc.exe
   ```

下列影像顯示命令提示字元中的命令和結果。

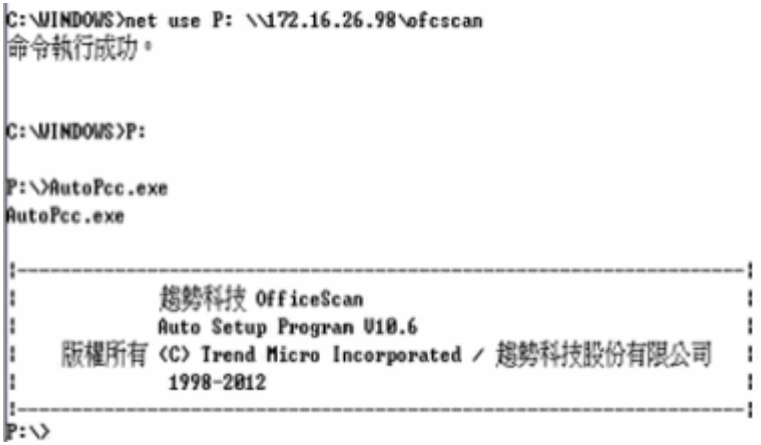


圖 B-1. 命令提示字元顯示如何使用 Login Script Setup 安裝 OfficeScan 用戶端

使用 OfficeScan 用戶端套件安裝 OfficeScan 用戶端

程序

1. 建立套件。

   如需詳細資訊，請參閱以用戶端封裝程式安裝 第 5-21 頁。

2. 開啟命令提示字元。

3. 輸入下列命令以對應 OfficeScan 用戶端套件的位置：

   ```
   net use <對應磁碟機代號> \\<用戶端套件的位置>
   ```

   例如：

   ```
   net use P:\\10.1.1.1\Package
   ```

隨即顯示訊息，通知您 OfficeScan 用戶端套件的位置是否對應成功。

4. 輸入對應的磁碟機代號及冒號，以切換至 OfficeScan 用戶端套件的位置。例如：

   ```
   P:
   ```

5. 輸入下列命令，將 OfficeScan 用戶端套件複製到 Server Core 電腦上的本機目錄：

   ```
   copy <套件檔案名稱> <Server Core 電腦上要複製套件的目錄>
   ```

   例如：

   ```
   複製 officescan.msi C:\Client Package
   ```

   隨即顯示訊息，通知您 OfficeScan 用戶端套件是否複製成功。

6. 切換至本機目錄。例如：

   ```
   C:
   ```

   ```
   cd C:\Client Package
   ```

7. 輸入套件檔案名稱以啟動安裝。例如：

   ```
   officescan.msi
   ```

下列影像顯示命令提示字元中的命令和結果。

圖 B-2. 命令提示字元顯示如何使用用戶端套件安裝 OfficeScan 用戶端

Windows Server Core 上的 OfficeScan 用戶端功能

Windows Server 2008/2012 上可用的大部分 OfficeScan 用戶端功能在 Server Core 上都可用。唯一不支援的功能是「行動模式」。

如需 Windows Server 2008/2012 上可用功能的清單，請參閱 OfficeScan 用戶端功能 第 5-3 頁。

您只能從命令列介面存取 OfficeScan 用戶端主控台。

注意

有些 OfficeScan 用戶端主控台畫面會包括「說明」按鈕，只要按一下這個按鈕，就會開啟內容感應式、以 HTML 為架構的說明。由於 Windows Server Core 2008/2012 沒有瀏覽器，因此這個說明無法供使用者使用。如果要查看「說明」，使用者必須安裝瀏覽器。

Windows Server Core 命令

從命令列介面執行命令，以啟動 OfficeScan 用戶端主控台和其他 OfficeScan 用戶端工作。

如果要執行命令，請瀏覽到 `PccNTMon.exe` 所在位置。此處理程序負責啟動 OfficeScan 用戶端主控台。此處理程序位於 <用戶端安裝資料夾> 下。

下表列出可用命令。

表 B-1. Windows Server Core 命令

命令	處理行動
`pccntmon`	開啟 OfficeScan 用戶端主控台
`pccnt`	
`pccnt <磁碟機或資料夾路徑>`	掃瞄指定的磁碟機或資料夾是否有安全威脅 指導方針： • 如果資料夾路徑包含空格，請以引號括住整個路徑。 • 不支援掃瞄個別檔案。 正確的命令： • `pccnt C:\` • `pccnt D:\Files` • `pccnt "C:\Documents and Settings"` 不正確的命令： • `pccnt C:\Documents and Settings` • `pccnt D:\Files\example.doc`
`pccntmon -r`	開啟「即時監控」
`pccntmon -v`	開啟顯示用戶端元件與其版本清單的畫面

命令	處理行動
`pccntmon -u`	開啟已啟動「立即更新」（用戶端手動更新）的畫面 如果「立即更新」無法啟動，下列訊息會顯示在命令提示字元中： 已關閉或未正常運作
`pccntmon -n`	開啟可在其中指定用戶端卸載密碼的快顯視窗 如果不需要密碼就可以卸載 OfficeScan 用戶端，即會開始卸載 OfficeScan 用戶端。 如果要重新載入 OfficeScan 用戶端，請輸入下列命令： `pccntmon`
`pccntmon -m`	開啟可在其中指定 OfficeScan 用戶端解除安裝密碼的快顯視窗 如果不需要密碼就可以解除安裝 OfficeScan 用戶端，即會開始解除安裝 OfficeScan 用戶端。

命令	處理行動

`pccntmon -c`	在命令列中顯示下列資訊：
	• 掃瞄方法
	  • 雲端截毒掃瞄
	  • 標準掃瞄
	• 病毒碼狀態
	  • 已更新
	  • 已過期
	• 即時掃瞄服務
	  • 正常運作
	  • 已關閉或未正常運作
	• 用戶端狀態
	  • 線上
	  • 行動模式
	  • 離線
	• 網頁信譽評等服務
	  • 可用
	  • 正在重新連線
	• 檔案信譽評等服務
	  • 可用
	  • 正在重新連線

`pccntmon -h`	顯示所有可用的命令

附錄 C

Windows 8 和 Windows Server 2012 支援

本附錄討論 Windows 8 和 Windows Server 2012 的 OfficeScan 支援。

關於 Windows 8 和 Windows Server 2012

Windows 8 和 Windows Server 2012 為使用者提供兩種作業模式：桌面模式和 Windows UI 模式。桌面模式與傳統 Windows「開始」畫面類似。

Windows UI 為使用者提供全新的使用者界面體驗，與 Windows Phone 所用的使用者界面類似。新功能包括捲軸觸控式螢幕界面、磚和快顯通知。

表 C-1. 磚和快顯通知

控制	說明
磚	磚類似於舊版 Windows 所用的桌面圖示。使用者按一下或點選某個磚就能啟動與此磚關聯的應用程式。 動態磚可為使用者提供動態更新的應用程式特定資訊。應用程式可將資訊張貼到磚（即使應用程式未執行）
快顯通知	快顯通知類似於快顯訊息。這些通知會隨時提供應用程式執行時所發生事件的資訊。不論 Windows 是否正處於桌面模式、顯示鎖定畫面或是執行其他的應用程式，快顯通知都會顯示在前景。 **注意** 視應用程式而定，快顯通知可能不會在所有畫面上或每個模式中顯示。

以 Windows UI 模式執行的 OfficeScan

下表說明 OfficeScan 如何在 Windows UI 模式下支援磚和快顯通知。

表 C-2. 磚和快顯通知的 OfficeScan 支援

控制	OfficeScan 支援
磚	OfficeScan 為使用者提供可連至 OfficeScan 用戶端程式的磚。使用者按一下磚時，Windows 會切換至桌面模式並顯示 OfficeScan 用戶端程式。 注意 OfficeScan 不支援動態磚。
快顯通知	OfficeScan 提供下列快顯通知： • 偵測到可疑程式 • 預約掃瞄 • 已解決安全威脅 • 需要重新啟動電腦 • 偵測到 USB 儲存裝置 • 偵測到病毒爆發 注意 OfficeScan 只會在 Windows UI 模式下顯示快顯通知。

啟動快顯通知

使用者可以透過修改 OfficeScan 用戶端電腦上的「電腦設定」來選擇接收快顯通知。OfficeScan 需要使用者啟動快顯通知。

程序

1. 將滑鼠游標移至畫面的右下角以顯示「快速鍵」列。
2. 按一下「設定 > 變更電腦設定」。

   會出現「電腦設定」畫面。

3. 按一下「通知」。
4. 在「通知」區段下，將下列設定設定為「開啟」：
   - 顯示應用程式通知
   - 在鎖定畫面上顯示應用程式通知（選用）
   - 播放通知音效（選用）

Internet Explorer 10

Internet Explorer (IE) 10 是 Windows 8 和 Windows Server 2012 的預設瀏覽器。Internet Explorer 10 有兩個不同版本：一個適用於 Windows UI，另一個適用於桌面模式。

Windows UI 適用的 Internet Explorer 10 提供無嵌入程式的瀏覽體驗。用於網頁瀏覽的嵌入程式以前沒有成熟的統一標準可供遵循，因此這些嵌入程式採用的程式碼的品質並不穩定。嵌入程式還需要使用更多的系統資源，這會增加感染惡意程式的風險。

Microsoft 開發了適用於 Windows UI 的 Internet Explorer 10，遵循全新的標準式技術，可取代以往使用的嵌入程式解決方案。下表列出 Internet Explorer 10 用以取代舊嵌入程式技術的新技術。

表 C-3. 標準式技術與嵌入程式的比較

功能	World Wide Web (W3C) 標準技術	嵌入程式同等功能範例
視訊和音訊	HTML5 視訊和音訊	• Flash • Apple QuickTime • Silverlight

功能	WORLD WIDE WEB (W3C) 標準技術	嵌入程式同等功能範例
圖形	• HTML5 畫布 • 可縮放向量圖形 (SVG) • 階層式樣式表層級 3 (CSS3) 轉換和動畫 • CSS 變形	• Flash • Apple QuickTime • Silverlight • Java Applet
離線儲存	• Web 儲存 • 檔案 API • IndexedDB • 應用程式快取 API	• Flash • Java Applet • Google Gears
網路通訊、資源共享、檔案上傳	• HTML Web 傳訊 • 跨源資源共享 (CORS)	• Flash • Java Applet

Microsoft 也開發了專用於桌面模式的嵌入程式相容 Internet Explorer 10 版本。如果以 Windows UI 模式執行的使用者瀏覽了需要使用其他嵌入程式的網站，Internet Explorer 10 將會顯示一則通知，提示使用者切換至桌面模式。進入桌面模式後，使用者就可以檢視需要使用或安裝協力廠商嵌入程式的網站。

Internet Explorer 10 中的 OfficeScan 功能支援

使用者用於運作 Windows 8 或 Windows Server 2012 的模式種類，會影響所用的 Internet Explorer 10 版本以及不同 OfficeScan 功能所提供的支援層級。下表列出桌面模式和 Windows UI 模式下不同 OfficeScan 功能的支援層級。

注意

未列出的功能表示在這兩種 Windows 作業模式中提供完整支援。

表 C-4. UI 模式支援的 OfficeScan 功能

功能	桌面模式	WINDOWS UI
Web 伺服器主控台	完整支援	不支援
網頁信譽評等	完整支援	部分支援 • HTTPS 掃瞄已關閉
防火牆	完整支援	部分支援 • 應用程式過濾已關閉

附錄 D

詞彙

此術語包含提供關於一般參考用電腦用詞詞彙表，如趨勢科技產品和技術。

ActiveUpdate

「主動式更新」是許多趨勢科技產品的通用功能。只要連線到趨勢科技更新網站，您就能透過 Internet 使用「主動式更新」下載最新的病毒碼檔案、掃瞄引擎、程式和其他趨勢科技元件檔案。

Compressed File（壓縮檔）

單一的檔案，其中包含一或多個個別檔案和資訊，可由適當的程式進行解壓縮（例如：WinZip）。

Cookie

這是一種用於儲存 Internet 使用者相關資訊（例如：名稱、偏好設定和喜好）的機制，Web 瀏覽器會儲存 Cookie 供後續使用。當您下次存取您的瀏覽器擁有其 Cookie 的網站時，瀏覽器會將 Cookie 傳送至 Web 伺服器，Web 伺服器便會使用 Cookie 中的資訊為您呈現自訂的網頁。例如，當您進入網站時，歡迎頁面上可能會顯示您的名稱。

Denial of Service Attack（拒絕服務攻擊）

「拒絕服務」(DoS) 攻擊是指對電腦或網路發動可導致「服務」（即網路連線）中斷的攻擊。DoS 攻擊通常會佔用大量網路頻寬，或是使系統資源（例如：電腦的記憶體）超載。

DHCP

「動態主機控制通訊協定」(DHCP) 是一種可將動態 IP 位址指定給網路裝置的通訊協定。透過動態定址，裝置每次連線到網路時都會有不同的 IP 位址。在

某些系統中，裝置的 IP 位址甚至可以在連線狀態下變更。DHCP 也支援混合使用靜態與動態 IP 位址。

DNS

「網域名稱系統」(DNS) 是一種通用的資料查詢服務，主要用於將 Internet 中的主機名稱轉譯為 IP 位址。

DNS 用戶端向 DNS 伺服器要求主機名稱與位址資料的程序，稱之為解析。使用基本 DNS 設定時，伺服器會執行預設解析。例如，假設有遠端伺服器向其他伺服器查詢目前區域中某部機器的資料。遠端伺服器中的用戶端軟體會查詢解析程式，而解析程式會透過其資料庫檔案回覆要求。

網域名稱

系統完整名稱包含本機主機名稱和網域名稱，例如：`tellsitall.com`。網域名稱必須足以判斷 Internet 上任何主機的唯一 Internet 位址。此程序（稱為「名稱解析」）使用「網域名稱系統」(DNS)。

Dynamic IP Address（動態 IP 位址）

動態 IP 位址是指 DHCP 伺服器指定的 IP 位址。電腦的 MAC 位址將維持不變，不過 DHCP 伺服器會根據可用性指定新的 IP 位址給電腦。

ESMTP

「加強版簡易郵件傳輸通訊協定」(ESMTP) 包含安全性、驗證與其他裝置，可節省頻寬並保護伺服器。

End User License Agreement（使用者授權合約）

「使用者授權合約」也稱為 EULA，是軟體發行者和軟體使用者之間的合法契約。通常會簡述對使用者的限制，如果使用者要拒絕合約，安裝時不要按「我接受」。當然，按一下「我不接受」將會結束軟體產品的安裝。

許多使用者會在安裝某些免費軟體時顯示的 EULA 上按一下「我接受」，而不小心就同意在其電腦上安裝間諜軟體和其他類型的可能的資安威脅程式。

False Positive（誤判）

安全軟體若將某個檔案錯誤偵測為中毒，就是誤判。

FTP

「檔案傳輸通訊協定」(FTP) 是一種標準通訊協定，用於透過 Internet 將檔案從伺服器傳輸到用戶端。如需詳細資訊，請參閱「網路工作群組 RFC 959」。

GeneriClean

GeneriClean（也就是所謂的參考清除）是一種即使沒有病毒清除元件也能夠清除病毒/惡意程式的新技術。GeneriClean 可使用偵測到的檔案為基礎，來確定偵測到的檔案是否在記憶體中有對應的程序/服務和登錄項目，然後一併刪除它們。

Hot Fix

Hotfix 是針對單一客戶回報的問題的因應措施或解決方案。HotFix 是針對特定問題，所以不會對所有客戶發行。Windows HotFix 包括安裝程式，而非 Windows HotFix 則不包括（通常您需要停止程式精靈、複製檔案以覆寫安裝中的對應檔案，然後重新啟動精靈）。

依預設，OfficeScan 用戶端可安裝 HotFix。如果不要 OfficeScan 用戶端安裝 HotFix，可移至「用戶端電腦 > 用戶端管理」，然後按一下「設定 > 權限和其他設定 > 其他設定」標籤，在 Web 主控台中變更用戶端更新設定。

如果無法在 OfficeScan 伺服器上部署 HotFix，請使用 Touch Tool 變更 HotFix 的時間戳記。這會讓 OfficeScan 將這個 HotFix 解譯為新的 HotFix，使伺服器自動再次嘗試部署這個 HotFix。如需此工具的詳細資訊，請參閱執行用於 OfficeScan 用戶端 Hotfix 的 Touch Tool 第 6-45 頁。

HTTP

「超文字傳輸通訊協定」(HTTP) 是標準的通訊協定，用於透過 Internet 將網頁（包括圖片和多媒體內容）從伺服器傳輸至用戶端。

HTTPS

使用安全套接字層 (SSL) 的超文件傳輸通訊協定。HTTPS 是由 HTTP 演變而來的安全版 HTTP，用於處理安全交易。

ICMP

有時候，閘道或目的主機會使用「Internet 控制訊息通訊協定」(ICMP) 與來源主機進行通訊（例如，為了回報處理資料包時發生的錯誤）。ICMP 會使用基本的 IP 支援做為較高階的通訊協定，不過 ICMP 實際上是整合的 IP 通訊埠，

並且由每個 IP 模組實作。ICMP 訊息會在數種情況下傳送：例如，資料包無法到達目的地時、閘道沒有轉送資料包的緩衝容量時，以及閘道可以指示主機以較短的路由進行傳輸時。「網際網路通訊協定」的設計並非絕對可靠。這些控制訊息的目的在於提供通訊環境中相關問題的意見反應，而非讓 IP 變得可靠。

IntelliScan

IntelliScan 是辨識要掃瞄的檔案的方法。對於可執行檔（例如：`.exe`），真實的檔案類型取決於檔案內容。針對非執行檔（例如 `.txt`），則根據檔案標頭判斷真實檔案型態。

使用 IntelliScan 具有以下優點：

- 效能最佳化：由於 IntelliScan 使用最少的系統資源，所以不會影響用戶端上的應用程式。
- 縮短掃瞄時間：由於「智慧型掃瞄」採用真實檔案型態辨識，因此只掃瞄容易受到感染的檔案。因此會比掃瞄所有檔案所花的掃瞄時間少很多。

IntelliTrap

病毒撰寫者通常會使用即時壓縮演算法騙過病毒過濾機制。IntelliTrap 透過封鎖即時壓縮可執行檔並將其與其他惡意程式特徵比對，以降低這類病毒進入網路的風險。由於 IntelliTrap 會將這類檔案識別為安全威脅，而且可能會錯誤地封鎖安全的檔案，因此建議您在啟動 IntelliTrap 時隔離（不刪除或清除）檔案。如果使用者定期交換即時壓縮可執行檔，請關閉 IntelliTrap。

IntelliTrap 使用下列元件：

- 病毒掃瞄引擎
- IntelliTrap 病毒碼
- IntelliTrap 例外病毒碼

IP

「網際網路通訊協定 (IP) 可將資料區塊（稱為資料包）從來源傳輸至目的地，而來源和目的地都是以固定長度位址來識別的主機。」(RFC 791)

Java File（Java 檔案）

Java 是由 Sun Microsystems 所開發的通用程式設計語言。Java 檔案中包含 Java 程式碼。Java 提供適用於多種平台的 Java Applet 格式，支援 Internet 的程式設計。Applet 是一種以 Java 程式設計語言撰寫的程式，可納入 HTML 頁面中。當您使用支援 Java 技術的瀏覽器來檢視包含 Applet 的頁面時，Applet 會將其程式碼傳輸至您的電腦，讓瀏覽器的 Java 虛擬機器執行該 Applet。

LDAP

「輕量型目錄存取通訊協定」(LDAP) 是一種應用程式通訊協定，用於查詢及修改透過 TCP/IP 執行的目錄服務。

Listening Port（監聽通訊埠）

監聽通訊埠可用於處理用戶端連線要求，以便進行資料交換。

MCP Agent（MCP 代理程式）

趨勢科技「管理通訊協定」(MCP) 是趨勢科技推出的新一代受管理產品的代理程式。MCP 取代了 Trend Micro Management Infrastructure (TMI)，成為 Control Manager 與 OfficeScan 進行通訊的方式。MCP 擁有數項新功能：

- 減少網路負載和套件大小

- 支援 NAT 和防火牆穿透
- 支援 HTTPS
- 單向和雙向通訊支援
- 支援單一登入 (SSO)
- 叢集節點支援

Mixed Threat Attack（混合式安全威脅攻擊）

混合式安全威脅攻擊會利用企業網路中的多個進入點與弱點，如「Nimda」或「Code Red」安全威脅。

NAT

「網路位址轉譯」(Network Address Translation) 是將安全 IP 位址從位址集區轉譯至暫時、外部、已登錄 IP 位址的標準。這會讓具有私人指定之 IP 位址的信任網路取得 Internet 的存取權。這也表示您無須針對網路中的每部機器取得已登錄的 IP 位址。

NetBIOS

「網路基本輸入輸出系統」(NetBIOS) 是一種應用程式介面 (API)，可將網路功能之類的功能新增至磁碟作業系統 (DOS) 的基本輸入/輸出系統 (BIOS)。

One-way Communication（單向通訊）

NAT 穿透在現實網路環境中成為越來越嚴重的問題。為了解決這個問題，MCP 使用單向通訊。單向通訊讓 MCP 代理程式可開始與伺服器的連線，且可從伺服器輪詢命令。每個要求都是 CGI 類命令查詢或記錄檔傳輸。為了減少對網路的影響，MCP 代理程式會盡量將連線保持在可用和開啟狀態。後續要求則會使用現有開啟中的連線。如果連線中斷，所有與相同主機間的 SSL 連線就能從作業階段 ID 快取記憶體中獲益，因為此快取記憶體可大幅縮短重新連線的時間。

Patch

Patch 是一組 HotFix 和安全修補程式，可解決多種程式問題。趨勢科技會定期提供 Patch。Windows Patch 包括安裝程式，而非 Windows Patch 一般則有安裝程式檔。

Phish Attack（網路釣魚攻擊）

網路釣魚是一種快速發展的欺詐形式，藉由模仿合法網站來詐騙網路使用者洩漏私人資訊。

通常，未起疑心的使用者會收到乍似緊急 (且看似真實) 的電子郵件，告訴他們帳號有問題，必須立即修正才能避免帳號停用。電子郵件中會包括某個網站的 URL，看起來就和真的一模一樣（要複製合法電子郵件和合法網站很簡單），然後會變更所謂的後端，也就是指已收集資料的接收者。

電子郵件會告訴使用者要登入該網站，並且確認某些帳號資訊。駭客會收到使用者提供的資料（例如：登入名稱、密碼、信用卡號或身分證字號）。

網路釣魚的欺詐方式速度快、廉價，而且易於久存。對於施展這種方式的罪犯而言，同樣也十分有利可圖。網路釣魚就連電腦高手也很難偵測，而且執法單位也難以追蹤。更糟的是，幾乎不可能判刑。

如果您發現任何疑似釣魚網站的網站，請回報給趨勢科技。

Ping

Ping 是一種將 ICMP Echo 要求傳送至 IP 位址並等候回應的公用程式。Ping 公用程式可以判斷使用指定 IP 位址的電腦是否為線上狀態。

POP3

「郵件通訊協定 3」(POP3) 是一種標準通訊協定，用於儲存電子郵件訊息以及將其從伺服器傳輸至用戶端電子郵件應用程式。

Proxy 伺服器

Proxy 伺服器是一種可接受具有特殊字首之 URL 的 World Wide Web 伺服器，用來從本機快取或遠端伺服器提取文件，然後將 URL 傳回給要求端。

RPC

「遠端程序呼叫」(RPC) 是一種網路通訊協定，可讓執行於某部主機上的電腦程式在另一部主機上執行程式碼。

安全修補程式

安全修補程式著重於安全問題，適合對所有客戶進行部署。Windows 安全修補程式包括安裝程式，而非 Windows Patch 一般則有安裝程式檔。

Service Pack

Service Pack 是重要到足以成為產品升級的 HotFix、Patch 和功能加強的合併整合。Windows 和非 Windows Service Pack 都包括安裝程式和安裝程式檔。

SMTP

「簡易郵件傳輸通訊協定」(SMTP) 是一種標準通訊協定，用於透過 Internet 在不同的伺服器之間傳送電子郵件訊息，或是將電子郵件訊息從用戶端傳送至伺服器。

SNMP

「簡易網路管理通訊協定」(SNMP) 是一種通訊協定，可支援監控連接到網路的裝置上應得到管理注意的狀況。

SNMP Trap

SNMP Trap 是一種將通知傳送給使用管理主控台（支援這種通訊協定）的網路管理員的方式。

OfficeScan 可以將通知儲存在 Management Information Bases (MIB) 中。您可以使用 MIB 瀏覽器來檢視 SNMP Trap 通知。

SOCKS 4

SOCKS 4 是 Proxy 伺服器用來在內部網路或 LAN 的用戶端與 LAN 外部的電腦或伺服器之間建立連線的 TCP 通訊協定。SOCKS 4 通訊協定會提出連線要求、設定 Proxy 迴路，並在 OSI 模型的應用程式層轉送資料。

SSL

Secure Socket Layer (SSL) 由 Netscape 所設計的通訊協定，可提供應用程式通訊協定（如 HTTP、Telnet 或 FTP）與 TCP/IP 之間的分層資料安全性。此安全通訊協定可為 TCP/IP 連線提供資料加密、伺服器驗證、訊息完整性與選用的用戶端驗證。

SSL Certificate（SSL 憑證）

此數位憑證可建立安全的 HTTPS 通訊。

TCP

「傳輸控制通訊協定」(TCP) 是一種連線導向、端對端的可靠通訊協定，用於配合支援多個網路應用程式的分層通訊協定階層架構。TCP 會依賴 IP 資料包來完成位址解析。如需詳細資訊，請參閱 DARPA Internet Program RFC 793。

Telnet

Telnet 是藉由建立「網路虛擬終端機」，而在 TCP 上聯繫終端機裝置的標準方法。如需詳細資訊，請參閱「網路工作群組 RFC 854」。

Trojan Port（特洛伊木馬程式通訊埠）

特洛伊木馬程式通訊埠通常是特洛伊木馬程式連線到電腦所使用的通訊埠。在病毒爆發期間，OfficeScan 會封鎖下列可能遭特洛伊木馬程式利用的通訊埠號碼。

表 D-1. 特洛伊木馬程式通訊埠

通訊埠號碼	特洛伊木馬程式	通訊埠號碼	特洛伊木馬程式
23432	Asylum	31338	Net Spy
31337	Back Orifice	31339	Net Spy
18006	Back Orifice 2000	139	Nuker
12349	Bionet	44444	Prosiak
6667	Bionet	8012	Ptakks
80	Codered	7597	Qaz
21	DarkFTP	4000	RA
3150	Deep Throat	666	Ripper
2140	Deep Throat	1026	RSM
10048	Delf	64666	RSM
23	EliteWrap	22222	Rux
6969	GateCrash	11000	Senna Spy
7626	Gdoor	113	Shiver
10100	Gift	1001	Silencer
21544	Girl Friend	3131	SubSari
7777	GodMsg	1243	Sub Seven
6267	GW Girl	6711	Sub Seven
25	Jesrto	6776	Sub Seven

通訊埠號碼	特洛伊木馬程式	通訊埠號碼	特洛伊木馬程式
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	Net Bus	12345	Valvo line
7300	Net Spy	1234	Valvo line

Trusted Port（信任的通訊埠）

伺服器和 OfficeScan 用戶端使用信任的通訊埠與彼此通訊。

如果您在病毒爆發後封鎖信任的通訊埠，然後將網路設定恢復正常，OfficeScan 用戶端將不會立即繼續與伺服器通訊。在到達您在「病毒爆發防範設定」畫面中指定的時數後，才會恢復用戶端與伺服器之間的通訊。

OfficeScan 會使用 HTTP 通訊埠（預設為 8080）做為伺服器上信任的通訊埠。在安裝期間，您可以輸入其他通訊埠號碼。如果要封鎖這個信任的通訊埠和 OfficeScan 用戶端上信任的通訊埠，請選取「封鎖通訊埠」畫面上的「封鎖信任的通訊埠」核取方塊。

主安裝程式會在安裝期間隨機產生 OfficeScan 用戶端信任的通訊埠。

判斷信任的通訊埠

程序

1. 存取 <伺服器安裝資料夾>\PCCSRV。
2. 使用記事本等文字編輯器開啟 ofcscan.ini 檔案。
3. 如果是伺服器信任的通訊埠，請搜尋字串 "Master_DomainPort"，然後查看其值。

   例如，如果字串顯示為 Master_DomainPort=80，這表示伺服器上信任的通訊埠為第 80 號通訊埠。

4. 如果是用戶端信任的通訊埠，請搜尋字串 "Client_LocalServer_Port"，然後查看其值。

   例如，如果字串顯示為 `Client_LocalServer_Port=41375`，這表示用戶端上信任的通訊埠為第 41375 號通訊埠。

Two-way Communication（雙向通訊）

雙向通訊是單向通訊的替代方案。雙向通訊是以單向通訊為基礎，但還多了接收伺服器通知的 HTTP-based 通道，可改善 MCP 代理程式即時傳遞和處理來自伺服器的命令。

UDP

「使用者資料包通訊協定」(UDP) 是搭配 IP 使用的無連線通訊協定，可讓應用程式傳送訊息至其他程式。如需詳細資訊，請參閱 DARPA Internet Program RFC 768。

Uncleanable File（無法清除的檔案）

「病毒掃瞄引擎」無法清除下列檔案：

- 感染特洛伊木馬程式的檔案
- 感染蠕蟲的檔案
- 防寫的中毒檔案
- 密碼保護的檔案
- 備份檔案
- 資源回收筒內的中毒檔案

- Windows Temp 資料夾或 Internet Explorer 暫存資料夾內的中毒檔案

感染特洛伊木馬程式的檔案

特洛伊木馬程式是一種會執行無法預期或未經授權（通常為惡意性質）動作（例如：顯示訊息、刪除檔案、或將磁碟格式化）的程式。特洛伊木馬程式不會感染檔案，因此沒有必要清除。

解決方案： OfficeScan 會使用「病毒清除引擎」和「病毒清除範本」移除特洛伊木馬程式。

感染蠕蟲的檔案

電腦蠕蟲是一種自含程式（或程式集），可以將本身具有功能性的複製體或其片段散佈到其他電腦系統。這種病毒通常透過網路連線或電子郵件的附件散播。因為檔案屬於自含程式，所以無法清除蠕蟲。

解決方案： 趨勢科技建議刪除蠕蟲。

防寫的中毒檔案

解決方案： 移除防寫，讓 OfficeScan 清除檔案。

受密碼保護的檔案

包括受密碼保護的壓縮檔或受密碼保護的 Microsoft Office 檔案。

解決方案： 移除密碼保護，讓 OfficeScan 清除這些檔案。

備份檔案

副檔名為 RB0~RB9 的檔案是中毒檔案的備份副本。OfficeScan 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 OfficeScan 成功清除中毒檔案，您便不需要保留備份副本。如果電腦運作正常，您可以刪除備份檔案。

索引

六畫

二十三畫