Apex Central™ *as a Service*

版本：2019

Widget 和策略管理手冊

適用於企業的集中化安全防護管理

文件編號：APTM08533/181106

發行日期：2018 年 11 月

受美國專利保護，專利編號： 5,623,600；5,889,943；5,951,698；6,119,165

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

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

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

請至下列網站並給予您對此文件的評估意見：

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

目錄

序言

序言 vii
文件 viii
讀者 viii
文件慣例 ix
詞彙 x

部分 I：簡介

第 1 章：資訊中心

關於資訊中心 1-2
標籤和 Widget 1-2
作業中心 1-6
摘要標籤 1-14
DLP 事件調查標籤 1-25
Data Loss Prevention 標籤 1-28
符合性標籤 1-31
安全威脅偵測標籤 1-36
設定主動式雲端截毒技術設定 1-43

第 2 章：策略管理

策略管理 2-2
策略狀態 2-21

部分 II：Apex Central Widget

第 3 章：Apex Central 資訊中心 Widget

端點防護驗證 Widget 3-2
嘗試做出 C&C 回呼的主機 Widget 3-3
Apex Central 前幾名檔案型安全威脅 Widget 3-4
歷來唯一遭到入侵的主機 Widget 3-5
策略狀態 3-5
快速啟動 3-6

部分 III：Apex One 資訊中心 Widget

第 4 章：Apex One 資訊中心 Widget

前幾名封鎖的應用程式 4-2
前幾名違反的 Application Control 條件 4-2

部分 IV：Apex One Security Agent 策略管理

第 5 章：Security Agent 程式設定

其他服務設定 5-2
權限和其他設定 5-4
更新代理程式 5-15

第 6 章：Application Control 策略設定

應用程式控管 6-2

第 7 章：行為監控策略設定

行為監控 7-2
設定行為監控規則與例外 7-11

第 8 章：惡意程式防護策略設定

掃瞄方法類型 8-2
手動掃瞄 8-4
即時掃瞄 8-9
立即掃瞄 8-17
預約掃瞄 8-23
中毒處理行動 8-30
掃瞄例外支援 8-38

第 9 章：網頁信譽評等策略設定

網頁信譽評等 9-2
設定網頁信譽評等策略 9-2

第 10 章：未知安全威脅防護

Machine Learning 10-2
設定樣本提交設定 10-4
設定可疑連線設定 10-5

第 11 章：周邊設備存取控管策略設定

周邊設備存取控管 11-2
設定周邊設備存取控管設定 11-2

第 12 章：掃瞄例外清單

間諜程式/可能的資安威脅程式核可清單 12-2
信任的程式清單 12-2

第 13 章：Endpoint Sensor 策略設定

Endpoint Sensor 13-2
設定 Endpoint Sensor 設定 13-2

第 14 章：Vulnerability Protection 策略設定

Vulnerability Protection 14-2

設定 Vulnerability Protection 設定 14-2

部分 V：Apex One Server 策略管理

第 15 章：Apex One Server 策略設定

Application Control 伺服器設定 15-2

設定 Endpoint Sensor 伺服器設定 15-2

部分 VI：Apex One Data Loss Prevention 策略管理

第 16 章：Apex One Data Loss Prevention 策略設定

Data Loss Prevention (DLP) 16-2

設定 Data Loss Prevention 策略 16-3

第 17 章：Data Discovery Widget

前幾名偵測到的機密檔案策略 Widget 17-2

前幾名具有機密檔案的端點 Widget 17-3

前幾名 Data Discovery 範本相符項目 Widget 17-5

前幾名機密檔案 Widget 17-6

第 18 章：Apex One 資料發現策略設定

建立 Data Discovery 策略 18-2

部分 VII：Apex One (Mac) Widget 和策略

第 19 章：Apex One (Mac) Widget

關鍵效能指標 Widget 19-2

第 20 章：Trend Micro Apex One (Mac) 策略設定

掃瞄方法類型 20-2
掃瞄類型 20-6
用於掃瞄的快取設定 20-21
掃瞄例外 20-22
用戶端自我保護 20-26
用戶端更新 20-27
網站信譽評等服務 20-30
周邊設備存取控管 20-33
Endpoint Sensor 20-35
信任的程式清單 20-37
Machine Learning 設定 20-38

索引

索引 IN-1

序言

序言

歡迎使用《Trend Micro™ Apex Central™ as a Service Widget 與策略管理指南》。本文件說明如何在 Apex Central as a Service 中設定「資訊中心」Widget 和「策略管理」Widget。

本節涵蓋下列主題：

- 文件 第 viii 頁
- 讀者 第 viii 頁
- 文件慣例 第 ix 頁
- 詞彙 第 x 頁

文件

Apex Central as a Service 文件包含下列各項：

文件	說明
Readme 檔	包含已知問題清單，可能也包含「線上說明」或印刷文件中未提供的最新產品資訊
管理手冊	提供如何設定及管理 Apex Central as a Service 和受管理產品的詳細指示，以及說明 Apex Central as a Service 概念和功能的 PDF 文件
線上說明	以 WebHelp 格式編譯的 HTML 檔案，提供「相關指示」、使用建議和特定領域資訊。也可以從 Apex Central as a Service 主控台存取的「說明」
Widget 和策略管理手冊	說明如何在 Apex Central as a Service 中設定資訊中心 Widget 和策略管理設定的 PDF 文件
資料安全防護清單（僅第 1 章）	其中列出 Data Loss Prevention 的預先定義資料識別碼和範本的 PDF 文件
知識庫	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。若要存取知識庫，請前往下列網站：http://esupport.trendmicro.com/zh-tw/business/default.aspx

您可以從下列位置下載最新的 PDF 文件和 Readme 檔：

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

讀者

Apex Central as a Service 文件適用於下列使用者：

- Apex Central as a Service 管理員：負責安裝、設定及管理 Apex Central as a Service。這些使用者必須具備進階網路管理和伺服器管理知識。

- 受管理產品管理員：負責管理與 Apex Central as a Service 整合之 Trend Micro 產品的使用者。這些使用者必須具備進階網路管理和伺服器管理知識。

文件慣例

本文件會使用下列慣例。

表 1. 文件慣例

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

詞彙

下表提供 Apex Central as a Service 文件中使用的正式詞彙：

詞彙	說明
管理員（或 Apex Central as a Service 管理員）	管理 Apex Central as a Service 伺服器的人員
用戶端	安裝在端點上的受管理產品程式
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
Apex Central as a Service 主控台、Web 主控台或管理主控台	用於存取、設定及管理 Apex Central as a Service 的 Web-based 使用者介面 注意 整合式受管理產品的主控台是由受管理產品的名稱表示。例如，Apex One Web 主控台。
受管理端點	安裝了受管理產品用戶端的端點
受管理的產品	與 Apex Central as a Service 整合的 Trend Micro 產品
受管理的伺服器	安裝了受管理產品的端點
伺服器	安裝了 Apex Central as a Service 伺服器的端點
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
雙堆疊	同時具有 IPv4 和 IPv6 位址的實體。
單純 IPv4	僅具有 IPv4 位址的實體
單純 IPv6	僅具有 IPv6 位址的實體

部分 I

簡介

第 1 章

資訊中心

本節討論如何使用 Apex Central as a Service 資訊中心標籤和 Widget。

包含下列主題：

- 關於資訊中心 第 1-2 頁
- 標籤和 Widget 第 1-2 頁
- 作業中心 第 1-6 頁
- 摘要標籤 第 1-14 頁
- DLP 事件調查標籤 第 1-25 頁
- Data Loss Prevention 標籤 第 1-28 頁
- 符合性標籤 第 1-31 頁
- 安全威脅偵測標籤 第 1-36 頁
- 設定主動式雲端截毒技術設定 第 1-43 頁

關於資訊中心

當您開啟 Apex Central as a Service Web 主控台或按一下主功能表中的「資訊中心」時，會顯示「資訊中心」。每個 Apex Central as a Service 使用者帳號都具有一個完全獨立的資訊中心。對屬於特定使用者帳號的資訊中心所做的任何變更，均不會影響其他使用者帳號的資訊中心。

「資訊中心」包含下列項目：

- 標籤
- Widget

標籤和 Widget

Widget 是「資訊中心」的核心元件。Widget 提供有關各種安全相關事件的特定資訊。

Widget 顯示以下出處的資訊：

- Apex Central as a Service 資料庫
- 已註冊的受管理產品
- 趨勢科技主動式雲端截毒技術

標籤為 Widget 提供了容器。「資訊中心」最多支援 30 個標籤。

使用標籤

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

程序

1. 移至「資訊中心」。
2. 如果要新增標籤，請執行下列作業：
   a. 按一下「新增」圖示 (+)。

   b. 為新標籤輸入名稱。
3. 如果要重新命名標籤：
   a. 將滑鼠游標暫留在標籤名稱上，然後請點選向下箭號。

   b. 請點選「重新命名」，然後輸入新的標籤名稱。
4. 如果要變更標籤上各 Widget 的配置：
   a. 將滑鼠游標暫留在標籤名稱上，然後請點選向下箭號。
   b. 請點選「變更版面配置」。
   c. 在出現的畫面中選取新的配置。
   d. 按一下「儲存」。
5. 如果要刪除標籤：
   a. 將滑鼠游標暫留在標籤名稱上，然後請點選向下箭號。
   b. 請點選「刪除」並確認。
6. 如果要播放標籤投影片放映：
   a. 請點選標籤顯示右側的「設定」按鈕。

b. 啟動「標籤投影片放映」控制項。

c. 選取在切換到下一個標籤前，每個標籤顯示的時間長度。

使用 Widget

透過新增、移動、調整大小、重新命名和刪除項目等動作來管理 Widget。您也可以修改為 Widget 提供資料的產品。

程序

1. 移至「資訊中心」。
2. 請點選某個標籤。
3. 如果要新增 Widget：

a. 請點選標籤顯示右側的「設定」按鈕。

b. 請點選「新增 Widget」。

c. 選取要新增的 Widget。

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

d. 請點選「新增」。

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

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

6. 如果要重新命名 Widget：

a. 請點選設定圖示 (>)。

b. 輸入新標題。

c. 按一下「儲存」。

7. 如果要修改 Widget 的產品範圍，請執行下列作業：

a. 請點選設定圖示 (>)。

b. 按一下「範圍」欄位中的雙箭號按鈕 ( )。

c. （選用）按一下漏斗圖示 ( ) 來過濾並搜尋產品。

d. 選取為了 Widget 提供資料的產品，然後按一下「確定」。

e. 按一下「儲存」。

8. 如果要刪除 Widget，請點選刪除圖示 (>)。

作業中心

「作業中心」是一個特殊的標籤/Widget，可透過彙總您網路的符合性層級、嚴重安全威脅偵測和已停止的偵測等相關資料，來提供您的網路安全防護狀態的整體摘要。您也可以使用「作業中心」圖表，來快速識別整合式 Active Directory 結構中的高風險使用者和群組。

注意

如果要變更範例圖表資料，並根據您的公司網路來顯示網站或報告行，請啟動 Active Directory 整合或根據 IP 位址建立自訂網站。

按一下設定圖示 (>)，可變更標籤上顯示的下列資訊。

- 組織：指定組織的顯示名稱。
- Active Directory 分組：指定圖表中的節點代表 Active Directory 中的「網站」或「報告行」。
- 期間：指定圖表上所顯示資料的時間範圍。

符合性指標

「作業中心」標籤中的這個區段，提供防毒病毒碼符合性層級或您網路的 Data Loss Prevention 符合性層級的相關資訊。

當您的網路符合性層級變更時，符合性指標圖示的顏色會隨之變更，以反映在「Active Directory 和符合性設定」畫面中設定的門檻值。

預設檢視會顯示「防毒病毒碼符合性」指標的資訊。

注意

變更符合性指標會同時變更在「安全性作業」圖表中顯示的符合性層級資訊。

如果要變更顯示的符合性資訊，請在向下箭號圖示 ( ) 旁按一下已選取的符合性指標名稱，然後從下拉式清單中選取下列其中一個指標。

指標	說明
防毒病毒碼符合性	顯示下列資訊： • 採用可接受的「病毒碼」和「本機雲端病毒碼」版本的 Security Agent 百分比 • 在您的網路上，具有過期防毒病毒碼的端點總數 按一下「具有過期特徵碼的端點」的計數，可在「使用者/端點目錄」中檢視受影響端點的詳細資訊。

指標	說明
Data Loss Prevention 符合性	顯示下列資訊： • 已啟動 Data Loss Prevention 且具有可接受的安全威脅偵測項目數的 Security Agent 百分比 • 具有 Data Discovery 安全威脅偵測項目的端點總數 按一下「具有無法接受的安全威脅偵測項目的端點」的計數，可在「使用者/端點目錄」中檢視受影響端點的詳細資訊。

嚴重安全威脅

「作業中心」標籤的「嚴重安全威脅」區段會顯示您網路中的嚴重安全威脅偵測總數、受影響的使用者總數，以及受影響的重要使用者（以星號標示）數目。

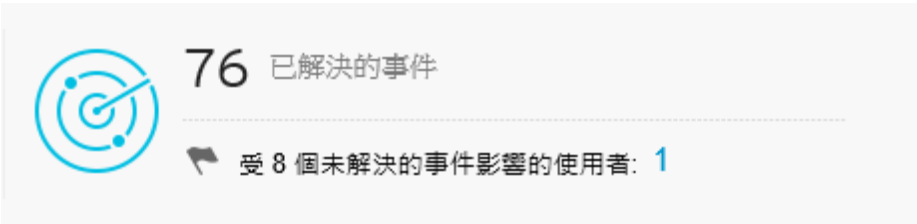
按一下受影響的使用者數目，可在「使用者/端點目錄」畫面上檢視其他詳細資訊。

嚴重安全威脅偵測包括下列安全威脅類型。

安全威脅類型	說明
C&C 回呼	嘗試和指令與控制項 (C&C) 伺服器進行通訊，以便傳送資訊、接收指示，以及下載其他惡意程式
已知的進階持續安全威脅 (APT)	攻擊者發起的入侵會具有侵犯性地追擊並入侵所選目標，通常隨著時間的推移執行一連串的失敗和成功的嘗試活動（並非孤立事件），以深入到目標網路內部

安全威脅類型	說明
橫向移動	搜尋目錄、電子郵件、管理伺服器和其他資產，以勘測出網路的內部結構，進而取得認證來存取這些系統，讓攻擊者得以在系統間跳轉
勒索軟體	除非使用者支付贖金，否則會阻止或限制使用者存取其系統的惡意程式
社交工程攻擊	利用文件（例如 PDF 檔案）中發現的安全弱點所進行的惡意程式或駭客攻擊
未知安全威脅	由 Deep Discovery Inspector、端點安全防護產品或其他具有沙盒虛擬平台的產品偵測到，且風險等級為「高」的可疑物件（IP 位址、網域、檔案 SHA-1 雜湊值、電子郵件訊息）
弱點攻擊	利用通常在程式和作業系統中發現的安全弱點所進行的惡意程式或駭客攻擊

已解決的事件



「作業中心」標籤的這個區段，會顯示您網路中已解決和未解決的事件總數。

按一下「受 __ 個未解決的事件影響的使用者」欄位的計數，可檢視您網路中受未解決事件影響之使用者的詳細資訊。

作業中心圖表

「作業中心」標籤上的圖表，會顯示您網路的嚴重安全威脅比率與符合性層級之間的關係。X 軸表示嚴重安全威脅與網站或報告行中端點總數的比率。Y 軸表示網站或報告行達到所選符合性指標的哪個符合性層級。您可以使用此資料來快速識別整合式 Active Directory 結構中的高風險使用者和群組。

注意

如果要變更範例圖表資料，並根據您的公司網路來顯示網站或報告行，請啟動 Active Directory 整合或根據 IP 位址建立自訂網站。

將滑鼠游標暫留在某個節點上，可檢視特定網站或報告行的符合性及嚴重安全威脅資訊。節點上的尾部表示指定時間範圍內安全狀態變更的方向。

- 按一下設定圖示 (>) 可變更節點所代表的「Active Directory 分組」（「網站」、「報告行」）。
- 您也可以使用「Active Directory 和符合性設定」畫面來自訂網站和報告行。

預設檢視會顯示您網路中所有節點過去 7 天的所選符合性指標資訊。

- 選取不同的符合性指標，會變更顯示的符合性資訊。
- 按一下設定圖示 (>) 可變更所顯示資料的「期間」。
- 按一下某個節點，即可在右側的摘要面板中檢視所選節點的詳細資訊。

作業中心詳細資料窗格

「作業中心」標籤上的詳細資料窗格，會顯示關於您網路中符合性層級、嚴重安全威脅偵測，以及已解決/未解決事件總數的更多詳細資訊。

預設檢視會顯示您網路中所有節點過去 7 天的所選符合性指標資訊。

- 選取不同的符合性指標，會變更顯示的符合性資訊。
- 按一下圖表上的某個節點，可僅顯示所選節點的資訊。
- 按一下設定圖示 (>) 可變更所顯示資料的「期間」。

表 1-1. 符合性資訊

指標	說明

防毒病毒碼符合性	顯示採用可接受的「病毒碼」和「本機雲端病毒碼」版本的 Security Agent 百分比
	
	您也可以檢視下列詳細資料：
	
	• 受管理的用戶端：已安裝 Security Agent 的端點數目
	  • 具有符合的病毒碼：採用可接受的「病毒碼」和「本機雲端病毒碼」版本的受管理用戶端數目
	  • 具有過期的病毒碼：未採用可接受的「病毒碼」和「本機雲端病毒碼」版本的受管理用戶端數目
	  • 離線 7 天：未與受管理產品伺服器進行通訊達到 7 天（或更多天）的受管理用戶端數目
	  • 例外：從符合性計算排除的使用者或端點數目
	• 未受管理的端點：未安裝 Security Agent 的端點數目
	
	展開類別並按一下計數，可檢視受影響端點的其他詳細資料。

Data Loss Prevention 符合性	顯示已啟動 Data Loss Prevention 且具有可接受的安全威脅偵測項目數的 Apex One 用戶端百分比
	
	您也可以檢視下列詳細資料：
	
	• 受管理的用戶端：已安裝啟動了 Data Loss Prevention 的 Security Agent 的端點數目
	  • 具有可接受的安全威脅偵測項目：具有可接受的安全威脅偵測項目數的受管理用戶端數目
	  • 具有無法接受的安全威脅偵測項目：超過可接受的安全威脅偵測項目數的受管理用戶端數目
	  • 離線 7 天：未與受管理產品伺服器進行通訊達到 7 天（或更多天）的受管理用戶端數目
	  • 例外：從符合性計算排除的使用者或端點數目
	• 未受管理的端點：未安裝啟動了 Data Loss Prevention 的 Security Agent 的端點數目
	
	展開類別並按一下計數，可檢視受影響端點的其他詳細資料。

表 1-2. 嚴重安全威脅

區段	說明
嚴重安全威脅	顯示在您網路中偵測到的嚴重安全威脅（依安全威脅類型）總數 列出所有會影響您網路的嚴重安全威脅類型 如需瞭解偵測的安全威脅類型，請執行下列操作： • 展開安全威脅類型以檢視偵測清單。 • 按一下某個偵測，即可在「安全威脅資訊」畫面上檢視其他詳細資料。
受影響的使用者	顯示受嚴重安全威脅影響的使用者總數 • 展開此區段可檢視受影響的使用者。 • 按一下某個受影響的使用者，即可在「使用者」資訊畫面上檢視其他詳細資料。
受影響的端點	顯示受嚴重安全威脅影響的端點總數 • 展開此區段可檢視受影響的端點。 • 按一下某個受影響的端點，即可在「端點」資訊畫面上檢視其他詳細資料。

表 1-3. 事件總數

資料	說明
事件總數	顯示偵測到的事件總數
已解決的事件	顯示您網路中已解決的事件數目
未解決的事件	顯示您網路中需要採取處理行動的未解決事件數目
受影響的使用者	顯示您網路中受未解決事件影響的使用者數目 按一下計數可檢視受影響使用者的詳細資料。

摘要標籤

「摘要」標籤包含一組預先定義的 Widget，這些 Widget 提供網路安全狀態的總覽。

注意

您可以新增、刪除或修改「摘要」標籤上顯示的 Widget。

可用的 Widget：

- 嚴重安全威脅
- 具有安全威脅的使用者
- 具有安全威脅的端點
- Apex Central 的前幾名安全威脅
- 產品連線狀態
- 產品元件狀態
- 勒索軟體防範

嚴重安全威脅 Widget

此 Widget 會顯示在您網路中偵測到的嚴重安全威脅類型的總數，以及受到每個安全威脅類型影響的「重要使用者」和「其他使用者」的數目。

使用「範圍」下拉式清單，選取顯示的資料時間範圍。

資料表會按嚴重性順序列出嚴重安全威脅類型。

- 按一下「重要使用者」或「其他使用者」欄中的數字，然後按一下您要檢視的使用者。

「安全威脅類型」欄會顯示下列安全威脅類型。

安全威脅類型	說明
C&C 回呼	嘗試和指令與控制項 (C&C) 伺服器進行通訊，以便傳送資訊、接收指示，以及下載其他惡意程式

安全威脅類型	說明
已知的進階持續安全威脅 (APT)	攻擊者發起的入侵會具有侵犯性地追擊並入侵所選目標，通常隨著時間的推移執行一連串的失敗和成功的嘗試活動（並非孤立事件），以深入到目標網路內部
橫向移動	搜尋目錄、電子郵件、管理伺服器和其他資產，以勘測出網路的內部結構，進而取得認證來存取這些系統，讓攻擊者得以在系統間跳轉
勒索軟體	除非使用者支付贖金，否則會阻止或限制使用者存取其系統的惡意程式
社交工程攻擊	利用文件（例如 PDF 檔案）中發現的安全弱點所進行的惡意程式或駭客攻擊
未知安全威脅	由 Deep Discovery Inspector、端點安全防護產品或其他具有沙盒虛擬平台的產品偵測到，且風險等級為「高」的可疑物件（IP 位址、網域、檔案 SHA-1 雜湊值、電子郵件訊息）
弱點攻擊	利用通常在程式和作業系統中發現的安全弱點所進行的惡意程式或駭客攻擊

具有安全威脅的使用者 Widget

此 Widget 會顯示具有安全威脅偵測項目之使用者的相關資訊。

使用「範圍」下拉式清單，選取顯示的資料時間範圍。

按一下「重要使用者」或「其他使用者」標籤，可在不同的檢視間切換。

資料表會先按嚴重安全威脅類型之嚴重性順序，再按使用者的安全威脅偵測數順序，列出受影響的使用者。

- 按一下您要檢視之使用者的「安全威脅」欄中的數字。

「最嚴重的安全威脅」欄會顯示下列安全威脅類型。

安全威脅類型	說明
C&C 回呼	嘗試和指令與控制項 (C&C) 伺服器進行通訊，以便傳送資訊、接收指示，以及下載其他惡意程式

安全威脅類型	說明
已知的進階持續安全威脅 (APT)	攻擊者發起的入侵會具有侵犯性地追擊並入侵所選目標，通常隨著時間的推移執行一連串的失敗和成功的嘗試活動（並非孤立事件），以深入到目標網路內部
橫向移動	搜尋目錄、電子郵件、管理伺服器和其他資產，以勘測出網路的內部結構，進而取得認證來存取這些系統，讓攻擊者得以在系統間跳轉
勒索軟體	除非使用者支付贖金，否則會阻止或限制使用者存取其系統的惡意程式
社交工程攻擊	利用文件（例如 PDF 檔案）中發現的安全弱點所進行的惡意程式或駭客攻擊
未知安全威脅	由 Deep Discovery Inspector、端點安全防護產品或其他具有沙盒虛擬平台的產品偵測到，且風險等級為「高」的可疑物件（IP 位址、網域、檔案 SHA-1 雜湊值、電子郵件訊息）
弱點攻擊	利用通常在程式和作業系統中發現的安全弱點所進行的惡意程式或駭客攻擊

具有安全威脅的端點 Widget

此 Widget 會顯示具有安全威脅偵測項目之端點的相關資訊。

使用「範圍」下拉式清單，選取顯示的資料時間範圍。

按一下「重要使用者」或「其他使用者」標籤，可在不同的檢視間切換。

資料表會先按嚴重安全威脅類型之嚴重性順序，再按使用者的安全威脅偵測數順序，列出受影響的使用者。

- 按一下您要檢視之使用者的「安全威脅」欄中的數字。

「最嚴重的安全威脅」欄會顯示下列安全威脅類型。

安全威脅類型	說明
C&C 回呼	嘗試和指令與控制項 (C&C) 伺服器進行通訊，以便傳送資訊、接收指示，以及下載其他惡意程式

安全威脅類型	說明
已知的進階持續安全威脅 (APT)	攻擊者發起的入侵會具有侵犯性地追擊並入侵所選目標，通常隨著時間的推移執行一連串的失敗和成功的嘗試活動（並非孤立事件），以深入到目標網路內部
橫向移動	搜尋目錄、電子郵件、管理伺服器和其他資產，以勘測出網路的內部結構，進而取得認證來存取這些系統，讓攻擊者得以在系統間跳轉
勒索軟體	除非使用者支付贖金，否則會阻止或限制使用者存取其系統的惡意程式
社交工程攻擊	利用文件（例如 PDF 檔案）中發現的安全弱點所進行的惡意程式或駭客攻擊
未知安全威脅	由 Deep Discovery Inspector、端點安全防護產品或其他具有沙盒虛擬平台的產品偵測到，且風險等級為「高」的可疑物件（IP 位址、網域、檔案 SHA-1 雜湊值、電子郵件訊息）
弱點攻擊	利用通常在程式和作業系統中發現的安全弱點所進行的惡意程式或駭客攻擊

Apex Central 的前幾名安全威脅 Widget

此 Widget 會顯示指定時間範圍內偵測到的惡意檔案和惡意 URL 的相關資訊。

按一下顯示圖示 ()，可選擇要以長條圖還是資料表顯示資料。

使用圖表/資料表上方的下拉式清單，可選取要顯示的安全威脅資料類型。

- 惡意檔案：根據偵測數目，排名在您的網路中偵測到的惡意檔案
- 惡意 URL：根據偵測數目，排名在您的網路中偵測到的惡意 URL

按一下長條、安全威脅名稱或偵測數目可開啟「記錄查詢」畫面，其中會顯示受影響端點的相關資訊、安全威脅詳細資訊，以及偵測計數。

預設檢視會顯示已登入的使用者帳號具有存取權限之所有受管理產品的前 10 名安全威脅。

- 按一下設定圖示 (> )，可編輯 Widget 標題、產品範圍或顯示的安全威脅數目。

產品元件狀態 Widget

此 Widget 會顯示您網路上受管理產品或端點的元件版本與合規狀態。使用此 Widget 可追蹤具有已過期元件的受管理產品或端點。

預設檢視會顯示受 Apex Central as a Service 管理之元件的最新版本，以及受管理產品的合規狀態。「特徵碼」和「引擎」區段一開始會先以最高的不合規率順序列出元件。您可以按一下「比率」欄來變更排序順序。

按一下「特徵碼」或「引擎」欄中的任何一個元件可檢視圓餅圖，其中顯示使用每個元件版本的受管理產品或端點的數目。

按一下「已過期/全部」欄中的計數，可檢視已過期受管理產品、所有受管理產品、已過期端點或所有端點上元件版本的相關資訊。

按一下設定圖示 (> )，設定下列選項：

注意

「摘要」標籤上不會顯示 Widget 的設定圖示 ()。

- 如果要修改 Widget 的產品範圍，請在「範圍」欄位中按一下雙箭頭按鈕 (>>)，然後選取提供資料的產品。
- 如果要編輯 Widget 中顯示的元件，請從「特徵碼」或「引擎」欄位中選取或清除元件。
- 如果要顯示受管理產品、端點或兩者的合規資訊，請指定「來源」。
- 如果要指定檢視受管理產品所報告之所有元件的資料，還是檢視僅由 Apex Central as a Service 管理之元件的資料，請選取「檢視」。

資料	說明
特徵碼	顯示特徵碼檔案、範本或垃圾郵件防護規則的名稱
引擎	顯示掃瞄引擎的名稱
最新版本	顯示下列資訊： • Apex Central as a Service 所下載元件的最新版本 • 可供下載之元件（由受管理產品報告）的最新版本
已過期/全部	顯示下列資訊： • 已過期：具有已過期元件的受管理產品或端點數目 按一下「已過期/全部」欄中的第一個計數，可檢視已過期受管理產品或端點上元件版本的相關資訊。 • 全部：採用此元件的受管理產品或端點的總數 按一下「已過期/全部」欄中的第二個計數，可檢視所有受管理產品或端點上元件版本的相關資訊。 注意 選取「兩者都有」做為「來源」時，才會顯示此欄。
分級	顯示具有已過期元件的受管理產品或端點的百分比 注意 選取「兩者都有」做為「來源」時，才會顯示此欄。

產品連線狀態 Widget

此 Widget 會顯示所有向 Apex Central as a Service 伺服器註冊的受管理產品的連線狀態。

預設檢視會列出已登入的使用者帳號具有存取權限之每個受管理產品的連線狀態和受管理伺服器名稱。

- 如果要變更產品範圍，請按一下設定圖示 (>)，然後選取新的「範圍」。
- 如果要檢視每個連線狀態的受管理產品總數的摘要，請按一下設定圖示 (>)，然後將「檢視」切換至「摘要」。

按一下「檢視詳細資料」，即可在「記錄查詢」畫面上檢視詳細資訊。

狀態	說明
作用中	表示產品服務正在執行中，並且已成功建立與 Apex Central as a Service 伺服器的通訊
離線	表示產品服務未執行，或無法建立與 Apex Central as a Service 伺服器的通訊

狀態	說明
異常	表示在使用者定義的用戶端通訊逾時間隔內，產品服務並未與 Apex Central as a Service 伺服器進行通訊

勒索軟體防範 Widget

此 Widget 提供指定時間範圍內，所有勒索軟體攻擊嘗試的總覽。

預設檢視會以摘要的形式顯示所有偵測到的勒索軟體，並根據感染通道將所有嘗試分類。

- 按一下勒索軟體偵測計數，可檢視其他詳細資料。

通道	說明
郵件	在電子郵件訊息或電子郵件附件中偵測到勒索軟體
網站	網頁信譽評等服務偵測到勒索軟體
網路流量	Apex One 可疑連線與 Deep Discovery Inspector 偵測到勒索軟體
雲端同步	雲端儲存上的 Cloud App Security 和 Office 365 伺服器（Exchange Online、SharePoint Online 和 OneDrive）偵測到勒索軟體，或 Apex One 在與雲端儲存同步的 Apex One 用戶端上的本機資料夾中偵測到勒索軟體
檔案	檔案信譽評等服務偵測到勒索軟體
行為	Apex One 行為監控偵測到勒索軟體

DLP 事件調查標籤

「DLP 事件調查」標籤所包含的 Widget 會根據事件狀態、嚴重性等級和受管理的使用者，顯示有關 DLP 事件的資訊。

下列是預先定義的 Widget：

- DLP 事件 (依嚴重性和狀態)
- DLP 事件趨勢 (依使用者)
- DLP 事件 (依使用者)

DLP 事件趨勢 (依使用者) Widget

此 Widget 會根據受管理的使用者檢查 DLP 事件數目的趨勢。可以依嚴重性等級過濾資料，或將資料過濾為只顯示指定時間範圍內特定使用者所觸發的事件總數。依預設，此 Widget 會顯示使用者之帳號權限所允許的所有受管理產品的資料。

使用「範圍」下拉式清單，選取顯示的資料時間範圍。

按一下圖形中的區段來開啟「事件資訊」畫面，並檢閱事件的摘要。

按一下 Widget 上的 Widget 設定圖示可存取其他設定。

設定	說明
標題	在欄位中為 Widget 指定一個有意義的新標題。
範圍	指定觸發 DLP 事件的時間範圍。
範圍	指定 Widget 顯示的資料範圍。 • 直接受管理的使用者 • 所有受管理的使用者：從直接受管理的使用者和直接受管理的使用者下屬處收集資料。
嚴重性	指定用於過濾資料的嚴重性等級。
要顯示的使用者	指定要顯示的受管理使用者數目。

按一下「儲存」以套用變更並更新 Widget 資料。

DLP 事件 (依嚴重性和狀態) Widget

此 Widget 會根據嚴重性等級和事件狀態檢查 DLP 事件數目。您可以依嚴重性等級過濾資料，也可以顯示新事件和高嚴重性事件的總數。依預設，此 Widget 會顯示使用者之帳號權限所允許的所有受管理產品的資料。

使用「範圍」下拉式清單，選取顯示的資料時間範圍。

按一下任何欄中的數字來開啟「事件資訊」畫面，並檢閱事件的摘要。

若要查看特定事件，請在「事件 ID」欄位中輸入 ID，然後按一下「搜尋」。

秘訣

每個事件都指派有一個 ID 號碼。按一下資料表連結、在「事件詳細資料已更新」事件通知，或在 Data Loss Prevention 記錄查詢結果中，都可以找到 ID 號碼。

按一下 Widget 上的 Widget 設定圖示可存取其他設定。

設定	說明
標題	在欄位中為 Widget 指定一個有意義的新標題。
範圍	指定觸發 DLP 事件的時間範圍。
範圍	指定 Widget 顯示的資料範圍。 • 直接受管理的使用者 • 所有受管理的使用者：從直接受管理的使用者和直接受管理的使用者下屬處收集資料
嚴重性	指定用於過濾資料的嚴重性等級。

按一下「儲存」以套用變更並更新 Widget 資料。

DLP 事件 (依使用者) Widget

此 Widget 會根據嚴重性等級和受管理的使用者檢查 DLP 事件數目。您可以依嚴重性等級過濾資料，也可以顯示特定使用者所觸發的新事件和高嚴重性事件總數。依預設，此 Widget 會顯示使用者之帳號權限所允許的所有受管理產品的資料。此 Widget 最多顯示 50 個使用者。

使用「範圍」下拉式清單，選取顯示的資料時間範圍。

按一下任何欄中的數字來開啟「事件資訊」畫面，並檢閱事件的摘要。

若要查看特定使用者，請在「使用者」欄位中輸入幾個字元，然後按一下「搜尋」。舉例來說，輸入 `ke` 會顯示含有 `ke` 的所有使用者名稱，例如 “Ken” 和 “Brooke” 。您也可以輸入網域和使用者名稱，例如 `domain1\chris`。

注意

使用者名稱不能包含下列字元：" [ ] : ; | = + * ? / \ < &> ,

網域名稱不能包含下列字元：\ * + = | : ; " ? < &> ,

按一下 Widget 上的 Widget 設定圖示可存取其他設定。

設定	說明
標題	在欄位中為 Widget 指定一個有意義的新標題。
範圍	指定觸發 DLP 事件的時間範圍。
範圍	指定 Widget 顯示的資料範圍。 • 直接受管理的使用者 • 所有受管理的使用者：從直接受管理的使用者和直接受管理的使用者下屬處收集資料。
嚴重性	指定用於過濾資料的嚴重性等級。
要顯示的使用者	指定要顯示的受管理使用者數目。

按一下「儲存」以套用變更並更新 Widget 資料。

Data Loss Prevention 標籤

「Data Loss Prevention」標籤所包含的 Widget 會顯示 DLP 事件、範本相符項目和事件來源的相關資訊。

下列是預先定義的 Widget：

- DLP 事件 (依通道)
- DLP 範本相符數
- 前幾名 DLP 事件來源
- DLP 違反的策略

DLP 事件 (依通道) Widget

此 Widget 會顯示 DLP 事件總數。可以依事件觸發所在通道的類型過濾資料。

使用「範圍」下拉式清單，選取顯示的資料時間範圍。

使用「通道」下拉式清單來過濾出事件觸發所在通道的類型。

此 Widget 會顯示 DLP 事件數目和通道佔事件總數的比率。此 Widget 會依下列項目顯示資料：

資料	說明
P2P	依「資料範圍」指定的任何受管理產品，顯示所有的對等式 DLP 事件
IM	依「資料範圍」指定的任何受管理產品，顯示所有即時傳訊 DLP 事件
網路郵件	依「資料範圍」指定的任何受管理產品，顯示所有網路郵件 DLP 事件
電子郵件	依「資料範圍」指定的任何受管理產品，顯示所有電子郵件 DLP 事件
Web 應用程式	依「資料範圍」指定的任何受管理產品，顯示所有 Web 應用程式 DLP 事件
其他	依「資料範圍」指定的任何受管理產品，顯示其餘的 DLP 事件

按一下「通道」欄中的連結或按一下圖形中的區段，會開啟顯示詳細資訊的畫面。

資料	說明
通道	DLP 事件觸發所在通道的類型
事件	觸發的 DLP 事件數目
百分比 (%)	DLP 事件佔事件總數的百分比

如果要變更此 Widget 顯示的資訊，請按一下 > 。在出現的對話方塊中，請按一下 >>，並選取此 Widget 用做其來源的父伺服器，來指定「範圍」。

DLP 範本相符數 Widget

此 Widget 會顯示您網路上的 DLP 事件類型。資料可依範本進行過濾。

使用「範圍」下拉式清單，選取顯示的資料時間範圍。

按一下「範本」欄中的連結或按一下圖形中的區段，會開啟顯示詳細資訊的畫面。

資料	說明
範本	DLP 事件所觸發的範本
事件	DLP 事件數目
百分比 (%)	DLP 事件佔事件總數的百分比

如果要變更此 Widget 顯示的資訊，請按一下 > 。在出現的對話方塊中，請按一下 >>，並選取此 Widget 用做其來源的父伺服器，來指定「範圍」。

前幾名 DLP 事件來源 Widget

此 Widget 會顯示網路上前幾名 DLP 事件來源的總數。這些資料包括使用者、電子郵件信箱、主機名稱和 IP 位址，這些內容可依事件來源進行過濾。

使用「範圍」下拉式清單，選取顯示的資料時間範圍。

使用「顯示」下拉式清單選取要顯示的資料。

DLP 違反的策略 Widget

此 Widget 會顯示 DLP 違反的策略。使用此 Widget 可以檢查 DLP 事件總數。依預設，會依事件數目排序資料。如果要依策略名稱排序資料，請按一下「策略」欄標題。

使用「範圍」下拉式清單，選取顯示的資料時間範圍。

按一下「事件」欄中的連結，會開啟顯示詳細資訊的畫面。

資料	說明
策略	DLP 事件觸發所在策略的名稱
事件	觸發的 DLP 事件數目

符合性標籤

「符合性」標籤包含幾個 Widget，用於顯示受管理產品或端點的元件或連線符合性的相關資訊。

下列是預先定義的 Widget：

- 產品應用程式符合性
- 產品元件狀態
- 產品連線狀態
- 用戶端連線狀態

產品應用程式符合性 Widget

此 Widget 會顯示受管理產品的產品版本、語言、Build 與更新狀態。這可以讓管理員快速分辨哪些受管理產品的應用程式為最新版本、哪些需要更新。

按一下顯示圖示 ()，可選擇要以長條圖還是資料表顯示資料。

按一下「最新」和「過期」欄中的計數，可開啟顯示詳細資訊的畫面。Apex Central as a Service 會執行記錄查詢，以提供詳細資訊。

資料	說明
產品	向 Apex Central as a Service 註冊的受管理產品
版本	受管理產品的版本

資料	說明
語言	受管理產品的語言版本
Build	受管理產品的 Build 號碼
最新	視為已更新的產品數目 編輯 Widget 以指定仍應視為最新的最低產品版本。 按一下計數來檢視有關產品的更多詳細資料。
過期	處於「過期」狀態的產品數目 按一下計數來檢視有關產品的更多詳細資料。
更新率 (%)	處於「最新」狀態的產品百分比

依預設，此 Widget 會顯示使用者之帳號權限所允許的所有受管理產品的資料。

指定橫條圖或資料表以顯示資料。資料預設以橫條圖顯示。

按一下「編輯」存取下列選項：

- 按一下「範圍 > 瀏覽」，指定要為 Widget 提供資料的產品。

  資料範圍可指定 Widget 使用哪些產品來顯示資料。這可能對此 Widget 顯示資訊的有用性有嚴重影響。

- 在「最新範圍」下拉式清單上，指定與最新 Build 之間差距幾個版本時仍應視為「最新」的產品版本數目。

按一下「儲存」以套用變更並結束。

產品元件狀態 Widget

此 Widget 會顯示您網路上受管理產品或端點的元件版本與合規狀態。使用此 Widget 可追蹤具有已過期元件的受管理產品或端點。

預設檢視會顯示受 Apex Central as a Service 管理之元件的最新版本，以及受管理產品的合規狀態。「特徵碼」和「引擎」區段一開始會先以最高的不合規率順序列出元件。您可以按一下「比率」欄來變更排序順序。

按一下「特徵碼」或「引擎」欄中的任何一個元件可檢視圓餅圖，其中顯示使用每個元件版本的受管理產品或端點的數目。

按一下「已過期/全部」欄中的計數，可檢視已過期受管理產品、所有受管理產品、已過期端點或所有端點上元件版本的相關資訊。

按一下設定圖示 (>)，設定下列選項：

注意

「摘要」標籤上不會顯示 Widget 的設定圖示 ( )。

- 如果要修改 Widget 的產品範圍，請在「範圍」欄位中按一下雙箭頭按鈕 ( )，然後選取提供資料的產品。
- 如果要編輯 Widget 中顯示的元件，請從「特徵碼」或「引擎」欄位中選取或清除元件。
- 如果要顯示受管理產品、端點或兩者的合規資訊，請指定「來源」。
- 如果要指定檢視受管理產品所報告之所有元件的資料，還是檢視僅由 Apex Central as a Service 管理之元件的資料，請選取「檢視」。

資料	說明
特徵碼	顯示特徵碼檔案、範本或垃圾郵件防護規則的名稱
引擎	顯示掃瞄引擎的名稱
最新版本	顯示下列資訊： • Apex Central as a Service 所下載元件的最新版本 • 可供下載之元件（由受管理產品報告）的最新版本

資料	說明
已過期/全部	顯示下列資訊： • 已過期：具有已過期元件的受管理產品或端點數目 按一下「已過期/全部」欄中的第一個計數，可檢視已過期受管理產品或端點上元件版本的相關資訊。 • 全部：採用此元件的受管理產品或端點的總數 按一下「已過期/全部」欄中的第二個計數，可檢視所有受管理產品或端點上元件版本的相關資訊。 注意 選取「兩者都有」做為「來源」時，才會顯示此欄。
分級	顯示具有已過期元件的受管理產品或端點的百分比 注意 選取「兩者都有」做為「來源」時，才會顯示此欄。

產品連線狀態 Widget

此 Widget 會顯示所有向 Apex Central as a Service 伺服器註冊的受管理產品的連線狀態。

預設檢視會列出已登入的使用者帳號具有存取權限之每個受管理產品的連線狀態和受管理伺服器名稱。

- 如果要變更產品範圍，請按一下設定圖示 (>)，然後選取新的「範圍」。
- 如果要檢視每個連線狀態的受管理產品總數的摘要，請按一下設定圖示 (>)，然後將「檢視」切換至「摘要」。

按一下「檢視詳細資料」，即可在「記錄查詢」畫面上檢視詳細資訊。

狀態	說明
作用中	表示產品服務正在執行中，並且已成功建立與 Apex Central as a Service 伺服器的通訊
離線	表示產品服務未執行，或無法建立與 Apex Central as a Service 伺服器的通訊
異常	表示在使用者定義的用戶端通訊逾時間隔內，產品服務並未與 Apex Central as a Service 伺服器進行通訊

用戶端連線狀態 Widget

此 Widget 會顯示用戶端與其父伺服器的連線狀態。會顯示下列受管理產品的用戶端：

- Endpoint Sensor
- Endpoint Encryption
- 趨勢科技行動安全防護
- 趨勢科技行動安全防護（適用於 Mac）
- Apex One
- Vulnerability Protection

- Worry-Free Business Security Services

依預設，此 Widget 會顯示使用者之帳號權限所允許的所有受管理產品的資料。

按一下「線上」、「離線」或「總數」欄中的值，可檢視詳細資訊。Apex Central as a Service 會執行記錄查詢以提供資訊。

資料	說明
伺服器	父伺服器
線上	連線到其父伺服器的用戶端
離線	中斷與其父伺服器連線的用戶端
總數	端點總數

如果要變更此 Widget 顯示的資訊，請按一下 ⋮ > 。在出現的對話方塊中，請按一下 >>，並選取此 Widget 用做其來源的父伺服器，來指定「範圍」。

安全威脅偵測標籤

「安全威脅偵測」標籤所包含的 Widget 會顯示彙整的安全威脅偵測。

下列是預先定義的 Widget：

- Apex Central 的前幾名安全威脅
- Apex Central 安全威脅統計資料
- 安全威脅偵測結果
- 偵測到的策略違規
- C&C 回呼事件

Apex Central 的前幾名安全威脅 Widget

此 Widget 會顯示指定時間範圍內偵測到的惡意檔案和惡意 URL 的相關資訊。

按一下顯示圖示 ( )，可選擇要以長條圖還是資料表顯示資料。

使用圖表/資料表上方的下拉式清單，可選取要顯示的安全威脅資料類型。

- 惡意檔案：根據偵測數目，排名在您的網路中偵測到的惡意檔案
- 惡意 URL：根據偵測數目，排名在您的網路中偵測到的惡意 URL

按一下長條、安全威脅名稱或偵測數目可開啟「記錄查詢」畫面，其中會顯示受影響端點的相關資訊、安全威脅詳細資訊，以及偵測計數。

預設檢視會顯示已登入的使用者帳號具有存取權限之所有受管理產品的前 10 名安全威脅。

- 按一下設定圖示 (>)，可編輯 Widget 標題、產品範圍或顯示的安全威脅數目。

Apex Central 安全威脅統計資料 Widget

此 Widget 會顯示您網路中的安全威脅偵測總數。可以按照安全威脅類型或您網路中偵測到安全威脅的位置來過濾資料。

- 產品類別

資料	說明
病毒/惡意程式	「資料範圍」指定之任何受管理產品偵測到的病毒/惡意程式
間諜程式/可能的資安威脅程式	「資料範圍」指定之任何受管理產品偵測到的間諜程式/可能的資安威脅程式
Web 安全	「資料範圍」指定之任何受管理產品偵測到的 Web 網頁安全違規（惡意 URL、封鎖的 URL）
內容違規	「資料範圍」指定之任何受管理產品偵測到的內容安全違規（垃圾郵件、封鎖的關鍵字和表示式）

- 安全威脅類型

資料	說明
檔案伺服器	「資料範圍」指定之任何受管理產品在檔案伺服器上偵測到的安全威脅
網路	「資料範圍」指定之任何受管理產品在您網路中偵測到的安全威脅
未知	無法識別的安全威脅
郵件	「資料範圍」指定之任何受管理產品在電子郵件伺服器上偵測到的安全威脅
桌上型電腦	「資料範圍」指定之任何受管理產品在桌上型電腦上偵測到的安全威脅
閘道	「資料範圍」指定之任何受管理產品在閘道上偵測到的安全威脅
Apex Central 伺服器	「資料範圍」指定之任何受管理產品在 Apex Central 伺服器上偵測到的安全威脅

注意

此 Widget 一次只會顯示一種資訊類型的資料。

按一下「偵測」欄中的連結，以開啟其中顯示詳細資訊的畫面。Apex Central 會執行記錄查詢，以提供詳細資訊。

資料	說明
類型	安全威脅的類型，或偵測到安全威脅的受管理產品
偵測數	偵測到的安全威脅數目
百分比 (%)	偵測到的安全威脅總數的安全威脅百分比

指定 Widget 所顯示資料的日期範圍：

- 今天
- 1 週
- 2 週
- 1 個月

指定 Widget 顯示資料的方式：

- 圓餅圖
- 長條圖
- 表格式
- 折線圖

依預設，此 Widget 會顯示使用者之帳號權限所允許的所有受管理產品的資料。

如果要變更此 Widget 顯示的資訊，請按一下 ⋮ > 。在出現的對話方塊中，請按一下 >> ，並選取此 Widget 用做其來源的父伺服器，來指定「範圍」。

安全威脅偵測結果 Widget

此 Widget 會顯示安全威脅偵測數目和安全威脅佔偵測總數的比率。此 Widget 一次只會顯示一種資訊類型的資料。按一下「偵測」欄中的連結，會開啟顯示詳細資訊的畫面。Apex Central 會執行記錄查詢，以提供詳細資訊。

資料	說明
結果	安全威脅的類型，或偵測到安全威脅的受管理產品 注意 對於「Web 安全」安全威脅類型，不會顯示此欄
策略/規則名稱	在「Web 安全」安全威脅類型下套用的策略/規則類型。 注意 對於其他列出的安全威脅類型，不會顯示此欄。
偵測	偵測到的安全威脅數目
百分比 (%)	偵測到的安全威脅總數的安全威脅百分比

此 Widget 會顯示下列安全威脅類型的安全威脅偵測：

表 1-4. 安全威脅類型

安全威脅類型	說明
病毒/惡意程式	依「資料範圍」指定的任何受管理產品，顯示對所有檔案採取的處理行動。範例：已清除、拒絕存取等。
間諜程式/可能的資安威脅程式	依「資料範圍」指定的任何受管理產品，顯示對所有檔案採取的處理行動。範例：成功、需要進一步處理行動等。
內容安全	依「資料範圍」指定的任何受管理產品，顯示對所有電子郵件訊息採取的處理行動。範例：已刪除、已清除附件中的巨集等。
Web 安全	依「資料範圍」指定的任何受管理產品，顯示使用策略封鎖的所有 Web 網頁安全違規。範例：檔案封鎖、檔案名稱等。

安全威脅類型	說明
網路病毒	依「資料範圍」指定的任何受管理產品，顯示對所有網路病毒採取的處理行動。

如果要變更此 Widget 顯示的資訊，請按一下 ⋮ > 。在出現的對話方塊中，請按一下 >>，並選取此 Widget 用做其來源的父伺服器，來指定「範圍」。

- 使用「標題」欄位修改「安全威脅偵測結果」Widget 的標題。
- 使用「安全威脅類型」下拉式清單指定安全威脅類型。

按一下「儲存」以套用變更並結束。

策略違規偵測 Widget

此 Widget 會顯示網路病毒牆執行器裝置的策略違規偵測。按一下「偵測」欄中的連結，會開啟顯示詳細資訊的畫面。Apex Central 會執行記錄查詢，以提供詳細資訊。

資料	說明
類型	將「服務違規」列為一種安全威脅類型
已更新	上次更新日期
偵測	網路病毒牆執行器裝置偵測到的服務違規數目

如果要變更此 Widget 顯示的資訊，請按一下 ⋮ > 。

- 使用「標題」欄位修改「策略違規偵測 」Widget 的標題。
- 在出現的對話方塊中，請按一下 >>，並選取此 Widget 用做其來源的父伺服器，來指定「範圍」。

注意

此 Widget 僅會顯示網路病毒牆執行器偵測到的策略違規。

按一下「儲存」以套用變更並結束。

C&C 回呼事件 Widget

此 Widget 會根據遭到入侵的主機或回呼位址來顯示 C&C 回呼嘗試次數。此 Widget 一次只會顯示一種資訊類型的資料。按一下任何資料表儲存格中的數字，可開啟「C&C 回呼事件」畫面，其中包含下列回呼摘要資料：

資料	說明
遭到入侵的主機	受影響的主機或電子郵件信箱
回呼位址	遭到入侵的主機嘗試對其回呼的 URL、IP 位址或電子郵件信箱
C&C 伺服器位置	C&C 伺服器所在的地區和國家
回呼嘗試次數	回呼位址與遭到入侵的主機之間的聯絡次數
最新回呼位址/遭到入侵的主機	上個回呼嘗試所登入到的 URL、IP 位址或電子郵件信箱
回呼位址/遭到入侵的主機（欄中顯示數目）	與回呼嘗試次數關聯之遭到入侵的主機或回呼位址數目
記錄者	記錄事件的受管理產品名稱

如果要變更此 Widget 顯示的資訊，請按一下 ⋮ > ⫶⫶。

- 使用「標題」欄位可修改「C&C 回呼事件」Widget 的標題。
- 在出現的對話方塊中，請按一下 >>，並選取此 Widget 用做其來源的父伺服器，來指定「範圍」。
- 使用「C&C 清單來源」下拉式清單可指定 C&C 來源。下拉式清單會列出「全球資訊」、「沙盒虛擬平台」和「使用者定義的」C&C 清單來源。
- 使用「要顯示的項目」下拉式清單可選取要在 Widget 中顯示的項目數。下拉式清單會列出最多前 50 個項目。

按一下「儲存」以套用變更並結束。

設定主動式雲端截毒技術設定

啟動 Trend Micro Smart Feedback 後，可將安全威脅資訊與趨勢科技主動式雲端截毒技術共享。這可讓 Trend Micro 迅速識別及處理新的安全威脅，從而為您的網路提供更好的安全防護。

注意

電子郵件信譽評等、檔案信譽評等和網站信譽評等服務，都是主動式雲端截毒技術的一部分。

程序

1. 移至「管理 > 設定 > 主動式雲端截毒技術設定」。

   會出現「主動式雲端截毒技術設定」畫面。

2. 選取「啟動 Trend Micro Smart Feedback 和主動式雲端截毒技術服務」。

3. 從「時間間隔」下拉式清單中，指定 Apex Central as a Service 將完全匿名的安全威脅資訊傳送給主動式雲端截毒技術的頻率。

4. （選用）從「您所屬產業」下拉式清單中，指定您公司所屬的產業。

5. 按一下「儲存」。

第 2 章

策略管理

本節包含有關如何在受管理產品和端點上執行策略管理的資訊。

包含下列主題：

- 策略管理 第 2-2 頁
- 策略狀態 第 2-21 頁

策略管理

策略管理可讓管理員從單一管理主控台在受管理產品和端點上實施產品設定。管理員可藉由選取目標並設定產品設定清單來建立策略。

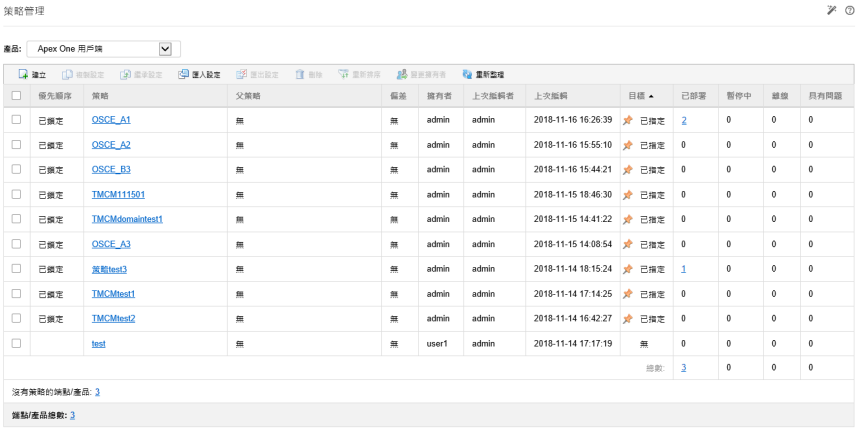
如果要在新的受管理產品或端點上執行策略管理，請將受管理產品從「新增實體」資料夾中移到「產品目錄」結構中的另一個資料夾。

建立新策略

程序

1. 移至「策略 > 策略管理」。

   會出現「策略管理」畫面。



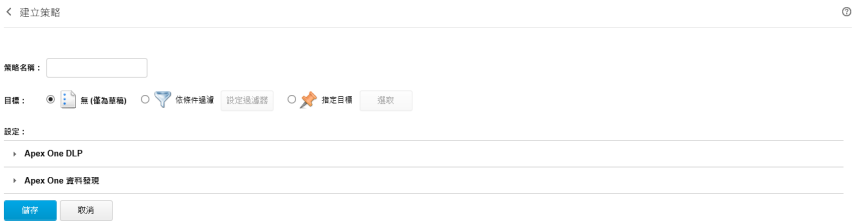
2. 從「產品」清單中選取產品設定的類型。

   畫面會重新整理，以顯示為所選受管理產品建立的策略。

   如需有關為特定受管理產品設定策略設定的詳細資訊，請參閱《Apex Central as a Service Widget 和策略管理手冊》。

3. 請點選「建立」。

   會出現「建立策略」畫面。



4. 輸入策略名稱。

5. 指定目標。

   Apex Central as a Service 會提供多種目標選取方法，這些方法會影響策略的運作方式。

   注意

   如果要包含受管理產品或端點做為目標，請確定受管理產品或端點的產品版本支援 Apex Central as a Service 中的策略管理。「策略範本設定」畫面（「策略 > 策略資源 > 策略範本設定」）包含受支援產品版本的相關資訊。

   策略清單會以下列順序排列策略目標：

   - 指定目標：使用此選項可選取特定端點或受管理的產品。
   - 依條件過濾：使用此選項可根據過濾條件自動配置端點。
   - 無 (僅為草稿)：使用此選項可將策略儲存為草稿，而不需要選擇任何目標。

6. 按一下受管理的產品功能，可展開功能並對其進行設定。重複此步驟以設定所有功能。

   - 每個功能都包含「說明」主題連結，提供功能和使用方式的說明。

- 對於某些產品設定，Apex Central as a Service 必須從受管理的產品取得特定設定選項。如果管理員針對某個策略選取多個目標，則 Apex Central as a Service 只會從第一個選取的目標取得設定選項。為了確保策略部署成功，請確定已跨多個目標同步處理產品設定。

- 如果您要為 Apex One 用戶端建立策略，而您想要將該用戶端做為未來子策略的父項，請對子策略設定可以繼承、自訂或延伸的設定。

  - 如需可繼承、自訂或延伸的 Apex One 用戶端設定清單，請參閱使用父策略設定 第 2-9 頁。

  - 如需有關建立子策略的詳細資訊，請參閱繼承策略設定 第 2-12 頁。

7. 按一下「部署」或「儲存」。

   如果按一下「部署」，Apex Central as a Service 將會開始部署。已部署的策略會顯示在「策略管理」畫面上的清單中。Apex Central as a Service 通常需要幾分鐘時間，來將策略部署到目標。

   按一下「策略管理」畫面上的「重新整理」，可在策略清單中更新狀態資訊。如果經過一段很長時間後，部署狀態依然是「暫停中」，這可能是目標有問題。請檢查 Apex Central as a Service 與目標之間是否已連線。另外，也請檢查目標是否正常運作。

   一旦 Apex Central as a Service 將策略部署到目標，則在策略中定義的設定會覆寫目標中的現有設定。Apex Central as a Service 會每隔 24 小時強制執行目標中的策略設定。雖然本機管理員可以從受管理的產品主控台變更設定，但每次 Apex Central as a Service 強制執行策略設定時都會覆寫這些變更。

   - Apex Central as a Service 會每隔 24 小時強制執行目標的策略設定。由於策略實施只會每隔 24 小時發生一次，因此如果本機管理員在實施期間之間透過受管理產品主控台進行變更，則目標中的產品設定可能會與策略設定不一致。

   - 部署到 IMSVA 伺服器的策略設定優先於目標伺服器上的現有設定，並不會覆寫它們。IMSVA 伺服器會將這些策略設定儲存在清單頂端。

   - 如果指派有 Apex Central as a Service 策略的 Apex One 用戶端已移至另一個 Apex One 網域，則用戶端設定將會暫時變更為由該 Apex One 網

域定義的設定。一旦 Apex Central as a Service 再次強制執行策略，用戶端設定就會符合策略設定。

依條件過濾

使用此選項可根據過濾條件自動配置端點。

此選項：

- 僅適用於下列受管理的產品：
  - Apex One
  - 企業版行動安全防護
  - Apex One (Mac)
- 使用過濾器，以便自動將目前與未來的目標指派給策略
- 有助於將標準設定部署到目標群組

管理員可以變更策略清單中過濾策略的優先順序。當管理員重新排序策略清單時，Apex Central as a Service 會根據目標條件和每個策略建立者的使用者角色，將目標重新指派到不同的過濾策略。

Apex Central as a Service 只能將沒有策略的端點指派到新的過濾策略。如果要重新配置已指派到過濾策略的端點，請在優先順序清單中，將另一個具有符合條件的過濾策略往上移動。

如需有關 Apex Central as a Service 如何將目標指派到過濾策略的詳細資訊，請參閱將端點指派給過濾策略 第 2-6 頁。

程序

1. 在「建立策略」畫面上，移至「目標」區段，並選取「依條件過濾」，然後按一下「設定過濾器」。

   會出現「依篩選條件」畫面。

2. 選取下列選項並定義條件。

條件	說明
比對關鍵字於	根據主機名稱或 Apex Central as a Service 顯示名稱定義關鍵字。 注意 對於單一關鍵字搜尋，Apex Central as a Service 會執行部分比對。您可以搜尋多個彼此以逗號分隔的關鍵字，但是 Apex Central as a Service 僅會針對每個提供的關鍵字，提供符合完整字串的項目。
IP 位址	定義 IP 位址的範圍，然後按一下「新增」。 注意 • 策略管理僅支援 IPv4 位址。 • 在新的受管理產品或端點向 Apex Central as a Service 註冊後，大約需要經過一小時，才能讓受管理產品或端點成為可供依 IP 位址搜尋。
作業系統	從下拉式清單中選取一或多個作業系統。
目錄	選取下列其中一個目錄並定義條件。 • 產品目錄：從「產品目錄」結構中選取資料夾 • Active Directory：從整合式 Active Directory 結構中選取組織單位 • Apex One 網域階層：輸入至少一個 Apex One 網域階層關鍵字

3. 按一下「儲存」。

   會重新載入「建立策略」畫面。

將端點指派給過濾策略

在新端點向 Apex Central as a Service 註冊後，它會從上到下執行整個清單中的過濾策略。當同時滿足下列兩個條件時，Apex Central as a Service 會將新端點指派給過濾策略：

- 新端點符合策略中的目標條件
- 策略建立者擁有管理新端點的權限

相同的處理行動會套用至已指派給策略的端點，但策略建立者稍後會刪除策略。

注意

對於剛剛向 Apex Central as a Service 註冊的端點，以及剛從已刪除的策略釋放的端點，會有停止端點配置的三分鐘寬限期。在這段期間內，這些端點將暫時不含任何策略。

如果端點不符合任何過濾策略中的目標條件，則端點不會與任何策略關聯。當下列處理行動發生時，Apex Central as a Service 會再次配置這些端點：

- 建立新的過濾策略
- 編輯過濾策略
- 重新排序過濾策略
- 每日端點配置預約時程

  Apex Central as a Service 會使用每日端點配置預約時程來確保端點指派給正確的策略。此處理行動會在每天下午 3:15 發生一次。當端點內容（例如：作業系統或 IP 位址）變更時，這些端點需要每日預約時程來將其重新指派給正確的策略。

  注意

  如果端點在每日端點配置預約時程期間處於離線狀態，這些端點的策略狀態會持續處於暫停中，直到端點上線為止。

當上述處理行動發生時，Apex Central as a Service 會根據下列條件來配置端點：

表 2-1. 過濾策略的端點配置

	新端點或已刪除策略的端點	沒有策略的端點	有策略的端點
建立新策略		●	

編輯策略	●	●	●
重新排序過濾策略	●	●	●
每日端點配置預約時程	●	●	●

指定策略目標

使用此選項可選取特定端點或受管理的產品。

此選項：

- 使用搜尋或瀏覽功能尋找特定目標，然後手動將這些目標指派給策略
- 如果管理員計劃僅將特定設定部署到某些目標，此選項非常有用
- 保持固定於策略清單的頂端，而且會優先於任何過濾策略

程序

1. 在「建立策略」畫面上，移至「目標」區段，並選取「指定目標」，然後按一下「選取」。

   會出現「指定目標」畫面。

2. 使用「搜尋」或「瀏覽」尋找目標。

   - 搜尋：使用下列搜尋條件來尋找端點或受管理的產品。搜尋結果會顯示符合所有選定條件的端點或受管理產品。
     - 比對關鍵字於：根據主機名稱或 Apex Central as a Service 顯示名稱定義關鍵字。
     - IP 位址：定義 IP 位址範圍，然後按一下「新增」。

注意

- 策略管理僅支援 IPv4 位址。
- 在新的受管理產品或端點向 Apex Central as a Service 註冊後，大約需要經過一小時，才能讓受管理產品或端點成為可供依 IP 位址搜尋。

  - 作業系統：從下拉式清單中選取一或多個作業系統。
- 瀏覽：瀏覽產品目錄或 Active Directory 來尋找要指派策略的端點或受管理產品。

3. 選取端點或受管理產品，然後按一下「新增選取的目標」。
4. 請等候「檢視處理行動清單」和「檢視結果」中的數字變更。
5. 請點選「確定」。

   會重新載入「建立策略」畫面。

使用父策略設定

為「Apex One 用戶端」建立父策略的 Apex Central as a Service 管理員，可以設定要繼承、自訂或延伸的特定策略設定。

注意

這些選項在其他受管理產品上無法使用。

- 繼承自父策略
  - 子策略管理員完全無法變更設定。Apex One 管理員可以從 Apex One server 主控台手動變更設定。不過，當 Apex Central as a Service 將策略部署到 Apex One server 時，設定會遭到覆寫。

    例如，Apex Central as a Service 管理員可以建立一個父策略，來執行從「手動掃瞄」中排除 PDF 檔案。
  - 對父策略設定所做的變更一律會對子策略執行。

- 如果父策略的權限從「繼承自父策略」變更為「可自訂」或「從父策略延伸」，則子策略管理員可以自訂或延伸目前的設定。對父策略設定所做的變更已經不再執行。

- 可自訂
  - 子策略可以不採用父策略中所設定的設定。

    例如，如果父策略的「預約掃瞄」每週執行一次但可自訂，則子策略管理員可將預約時程變更為每日一次。
  - 對父策略設定所做的變更永遠不會對子策略執行。
  - 如果父策略的權限從「可自訂」變更為「繼承自父策略」，則父策略的目前設定會覆寫子策略的設定。對父策略設定所做的變更一律會執行。

- 從父策略延伸
  - 子策略管理員可以對父策略中設定的項目進行新增。

    例如，如果父策略在「手動掃瞄」期間不掃瞄 20 個檔案名稱，則管理員可以再將 10 個安全且可信的檔案新增到子策略中。
  - 在父策略中移除或新增的項目也會在子策略中新增或移除。已移除的項目可以新增回子策略。
  - 如果父策略的權限從「從父策略延伸」變更為「繼承自父策略」，則會在子策略中移除與父策略不相符的項目。對父策略中的項目所做的變更一律會執行。

下表列出可以繼承、自訂或延伸的父策略設定。

設定與路徑	可用的選項		
	繼承自父策略	可自訂	從父策略延伸
掃瞄預約時程 「預約掃瞄設定」>「目標」標籤 >「預約」區段	●	●	

設定與路徑	可用的選項		
	繼承自父策略	可自訂	從父策略延伸
要掃瞄的副檔名 「手動掃瞄/即時掃瞄/立即掃瞄/預約掃瞄設定」>「目標」標籤 >「要掃瞄的檔案」區段 >「具有下列副檔名的檔案」選項	●		●
掃瞄例外清單（不掃瞄的目錄、檔案和副檔名） 「手動掃瞄/即時掃瞄/立即掃瞄/預約掃瞄設定」>「掃瞄例外」標籤	●		● 從掃瞄例外清單中選取「從父策略延伸」時，會展開此清單以顯示「子策略限制」區段，父策略建立者可以在此處指定子策略不能從掃瞄排除的項目。

複製策略設定

管理員可以從現有策略複製設定、使用相同設定建立新策略，以及將設定部署到不同端點或受管理產品。

注意

您不能複製「Apex One 用戶端」子策略的設定。如果要判斷「Apex One 用戶端」的策略是子策略還是父策略，請檢查「父策略」欄。如果策略是子策略，將會顯示可供點選的值，否則會顯示「無」。

程序

1. 移至「策略 > 策略管理」。

   會出現「策略管理」畫面。

2. 從「產品」清單中選取產品設定的類型。

畫面會重新整理，以顯示為所選受管理產品建立的策略。

3. 從清單中選取策略。
4. 按一下「複製設定」。

   會出現「複製並建立策略」畫面。
5. 在「策略名稱」欄位中，輸入策略的名稱。
6. 指派「目標」給策略。
7. （選用）視需要變更設定。
8. 按一下「部署」。

注意

- 按一下「部署」後，請等候兩分鐘，讓 Apex Central as a Service 將策略部署到目標。按一下「策略管理」畫面上的「重新整理」，可在策略清單中更新狀態資訊。
- Apex Central as a Service 會每隔 24 小時強制執行目標的策略設定。

繼承策略設定

藉由繼承現有父策略的設定，來建立新的子策略。子策略無法複製，也不能繼承其設定。

此工作需要用於 Apex One 用戶端的父策略。用於 Apex One 用戶端的父策略在「父策略」欄的底下會顯示值「無」。

程序

1. 移至「策略 > 策略管理」。

   會出現「策略管理」畫面。
2. 從「產品」清單中選取「Apex One 用戶端」。

畫面會重新整理，以顯示為所選受管理產品建立的策略。

3. 選取沒有本機管理設定的父策略。

4. 按一下「繼承設定」。

   會出現「繼承並建立策略」畫面。

5. 在「策略名稱」欄位中，輸入策略的名稱。

6. 指派「目標」給策略。

7. （選用）檢閱可自訂或延伸的設定，然後視需要做出變更。如需設定清單以進行檢閱，請參閱使用父策略設定 第 2-9 頁。

   注意

   如果在父策略上選取的選項是「繼承自父策略」，則無法自訂或延伸設定。

   例如：

   - 如果「預約掃瞄」設定是可自訂的，則您可以將預約時程從每週一次變更為每日一次。
   - 如果可延伸「即時掃瞄」的掃瞄例外清單，那麼您可以輸入您認為安全且可信的其他檔案名稱。建立子策略後，會將這些檔案名稱新增到掃瞄例外清單。

8. 按一下「部署」。

   注意

   - 按一下「部署」後，請等候兩分鐘，讓 Apex Central as a Service 將策略部署到目標。按一下「策略管理」畫面上的「重新整理」，可在策略清單中更新狀態資訊。
   - Apex Central as a Service 會每隔 24 小時強制執行目標的策略設定。

修改策略

管理員可以視需要修改策略目標和設定。Root 帳號擁有者可以修改清單中的每個策略，而其他帳號擁有者只能修改自己所建立的策略。修改策略後，Apex Central as a Service 會將策略部署到目標。

對於 Apex One 用戶端的父策略，如果您針對特定功能修改了目標及設定，所做的修改便會套用到所有子策略，並部署到各自的目標。父策略的某些設定支援權限，可用來控制允許對子策略進行哪些變更。對這些父策略權限的修改，也會套用到子策略，並部署到目標。如需支援權限的設定清單，請參閱使用父策略設定 第 2-9 頁。

例如：

- 如果您將掃瞄預約時程權限從「繼承自父策略」變更為「可自訂」，管理員便可以開始自訂其子策略的現有預約時程。
- 如果您將「手動掃瞄」副檔名權限從「從父策略延伸」變更為「繼承自父策略」，則管理員新增到子策略的任何副檔名將被移除。此外，管理員也無法再新增副檔名。

程序

1. 瀏覽至「策略 > 策略管理」。

   會出現「策略管理」畫面。

2. 從「產品」清單中選取產品設定的類型。

   畫面會重新整理，以顯示為所選受管理產品建立的策略。

3. 按一下「策略」欄中的策略名稱。

   會出現「編輯策略」畫面。

4. 修改策略。

   注意

   修改過濾策略中的過濾條件會影響目標配置。Apex Central as a Service 可能將部分目標重新指派到其他過濾策略，或將額外的目標新增到目前的策略。

5. 按一下「部署」。

   Apex Central as a Service 通常需要幾分鐘時間，來將策略部署到目標。按一下「策略管理」畫面上的「重新整理」，可在策略清單中更新狀態資訊。如果經過一段很長時間後，部署狀態依然是「暫停中」，這可能是目標有問題。請檢查 Apex Central as a Service 與目標之間是否已連線。另外，也請檢查目標是否正常運作。

   Apex Central as a Service 會每隔 24 小時強制執行目標的策略設定。

匯入和匯出策略

匯出策略進行備份，或匯入到同一版本的另一部 Apex Central as a Service 伺服器。

注意：

- Apex Central as a Service 只會匯出策略設定，但不會匯出策略目標。
- 父策略在匯出或匯入後，仍會保持為父策略。
- 子策略在匯出後會變成父策略。因此，子策略在匯入後會是父策略。
- 如果策略名稱與現有子策略相同，則 Apex Central as a Service 無法匯入該策略。如果現有策略並非子策略，則 Apex Central as a Service 會在匯入後覆寫該策略。

程序

1. 瀏覽至「策略 > 策略管理」。

   會出現「策略管理」畫面。

2. 從「產品」清單中選取產品設定的類型。

   畫面會重新整理，以顯示為所選受管理產品建立的策略。

3. 如果要匯出，請選取一或多個策略，並按一下「匯出設定」，然後儲存產生的策略檔案。

如果匯出單一策略，產生的檔案會使用副檔名 .cmpolicy。

如果匯出多個策略，產生的檔案會是一個壓縮 (.zip) 檔案，其中包含多個個別 .cmpolicy 檔案。如果您之後想要將這些檔案匯入到同一部或另一部伺服器，請務必先解壓縮個別檔案，因為系統不允許匯入壓縮檔。

4. 如果要匯入，請按一下「匯入設定」，然後找到 .cmpolicy 檔案並載入。

   請一次匯入一個檔案。如果某個策略已存在於策略清單中，將會顯示提示訊息，詢問是否允許 Apex Central as a Service 覆寫現有策略。按一下「確定」以繼續。

   畫面會重新整理來納入匯入的策略。策略會顯示在清單的頂端。請視需要重新排序策略清單。

刪除策略

管理員可以從清單中移除策略。接著，如果與所刪除策略關聯的目標符合另一個策略的過濾條件，Apex Central as a Service 就會重新配置該目標。這些沒有相符項目的目標會變成不含策略的端點，並且會保留刪除之策略所定義的設定，除非受管理產品管理員修改設定。

Apex Central as a Service 僅允許策略建立者刪除自己的策略。不過，root 帳號可以刪除清單中的每個策略。

您不能刪除其設定已由現有子策略繼承的 Apex One 用戶端父策略。

程序

1. 移至「策略 > 策略管理」。

   會出現「策略管理」畫面。

2. 從「產品」清單中選取產品設定的類型。

   畫面會重新整理，以顯示為所選受管理產品建立的策略。

3. 選取要刪除的策略。

4. 請點選「刪除」。

   會出現確認畫面。

5. 請點選「確定」。

變更策略擁有者

預設的策略擁有者是建立策略的使用者帳號。您可以使用「策略管理」畫面，將策略擁有者變更為任何一個 Apex Central as a Service 使用者帳號。您也可以將策略擁有者變更為 Active Directory 群組，這麼做會將群組中的所有 Active Directory 使用者指定為策略的擁有者。

重要

如果您將策略擁有者變更為無權存取指定目標的使用者帳號，則新的擁有者可以修改策略設定，但無法檢視策略資料。

程序

1. 移至「策略 > 策略管理」。

   會出現「策略管理」畫面。

2. 選取一或多個要變更擁有者的策略。

3. 按一下「變更擁有者」。

   會出現「變更策略擁有者」畫面。

4. 從下拉式清單中選取使用者帳號。

5. 按一下「儲存」以變更擁有者。

   Apex Central as a Service 會傳送一封電子郵件通知給所有已被指派「管理員」角色的使用者帳號。

瞭解策略清單

此策略清單會顯示所有使用者建立的策略的資訊和狀態。在新端點向 Apex Central as a Service 註冊後，它會從上到下執行整個清單中的過濾策略。當同時滿足下列兩個條件時，Apex Central as a Service 會將新端點指派給過濾策略：

- 新端點符合策略的目標條件
- 策略建立者擁有管理新端點的權限

下表說明「策略管理」畫面上所顯示的策略清單欄。按一下欄可排序資料。

表 2-2. 策略清單

欄	說明
優先順序	顯示策略的優先順序 • Apex Central as a Service 會從最高到最低優先順序列出策略。 • 當管理員建立過濾策略時，Apex Central as a Service 會將新策略儲存成最低優先順序的策略。 • 指定策略的優先順序高於任何過濾策略，並且會保持放在清單的頂端。管理員無法重新排序指定策略。 • Apex Central as a Service 會將草稿策略放在清單的最下面。
策略	顯示策略的名稱
策略	僅當選取的產品為「Apex One 用戶端」時，才會顯示此欄。 如果策略是子策略（亦即會繼承其父策略的設定），此欄會顯示父策略的名稱。否則，會顯示「無」。
偏差	僅當選取的產品為「Apex One 用戶端」時，才會顯示此欄。 如果策略是子策略，則此欄會顯示策略已變更的設定數目，因此會與父策略的設定不一致。如果策略與其父策略之間的設定一致，則會顯示 0（零）。 如果策略不是子策略，會顯示「無」。

欄	說明
擁有者	顯示目前被指派有該策略的使用者 注意 預設擁有者為建立策略的使用者。 • 如果您將策略擁有者變更為無權存取指定目標的使用者帳號，則新的擁有者可以修改策略設定，但無法檢視策略資料。 • 您也可以將策略指派給 Active Directory 群組，藉此指派給多位擁有者。 如需詳細資訊，請參閱變更策略擁有者 第 2-17 頁。
上次編輯者	顯示上次編輯策略的使用者
上次編輯	顯示上次編輯策略的時間
目標	顯示管理員如何為策略選取目標。 • 已指定：使用瀏覽或搜尋功能，為策略選取特定目標。指定的策略會保持固定於策略清單的頂端，而且會優先於過濾策略。 • 已過濾：使用過濾器，以便自動將目前與未來的目標指派給策略。管理員可以重新排列過濾策略的優先順序。將滑鼠游標暫留在項目上，即可方便地檢視過濾條件，並視需要調整。 • 無：策略建立者將策略儲存為草稿，而未選取任何目標。
已部署	顯示已套用策略設定或具有未啟動的產品服務的目標數目 按一下數字可檢視策略狀態。
暫停中	顯示未套用策略設定的目標數目 按一下數字可檢視策略狀態。
離線	顯示具有離線用戶端的目標數目 按一下數字可檢視策略狀態。

欄	說明
具有問題	顯示因為策略部署不受支援、沒有策略組態設定、系統錯誤、端點與產品伺服器之間通訊錯誤、端點不受支援、從本機變更設定、產品服務已關閉或部署不完全，而未套用策略設定的目標數目 按一下數字可檢視策略狀態。

注意

「已部署」和「暫停中」欄中的數字只會反映管理員有管理權限的端點或受管理產品。

重新排序策略清單

管理員可以使用「重新排序」按鈕，變更過濾策略的順序。重新排列策略清單可能會影響目標配置。Apex Central as a Service 可能會重新指派部分目標給不同的過濾策略。

注意

- 指定的策略保留固定不變，始終優先於過濾策略。
- 此功能僅適用於管理 Apex One 設定。

程序

1. 移至「策略 > 策略管理」。

   會出現「策略管理」畫面。

2. 從「產品」清單中選取產品設定的類型。

   畫面會重新整理，以顯示為所選受管理產品建立的策略。

3. 按一下「重新排序」。

會出現「重新排序策略」畫面。

4. 重新排列「優先順序」欄的順序。
5. 按一下「儲存」。

注意

按一下「儲存」後，請稍候兩分鐘，讓 Apex Central as a Service 完成重新指派目標。按一下「策略管理」畫面上的「重新整理」，可在策略清單中更新狀態資訊。

策略狀態

策略狀態可讓管理員檢查 Apex Central as a Service 是否已成功將策略部署到目標。

如果要檢查策略部署狀態，請使用下列其中一種方法：

- 在「策略管理」畫面上，按一下策略清單中的數字。會出現「記錄查詢」畫面。

- 在資訊中心上，按一下「策略狀態」Widget 中的數字。會出現「記錄查詢」畫面。
- 執行記錄查詢

下表提供各個策略狀態的說明和建議：

表 2-3. 策略狀態

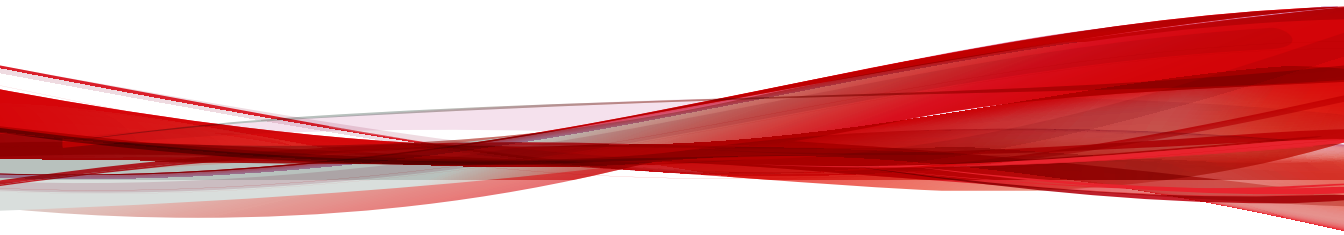
策略狀態	說明	建議
暫停中	Apex Central as a Service 正在處理策略。	請等候幾分鐘後再重新檢查狀態。
沒有策略	Apex Central as a Service 尚未將策略指派給此端點或受管理產品。	將策略指派給端點或受管理產品。
已部署	Apex Central as a Service 已成功部署策略。	無
端點無法連線到伺服器	• 端點未收到策略設定。 • 伺服器目前忙碌中。	• 檢查端點的連線狀態 • 將端點連線到公司網路 • 等候更新的策略狀態
產品設定不適用	受管理產品無法處理某些策略設定。	• 請確認策略設定 • 更新為最新策略範本版本 • 檢查受管理產品的設定 • 請確認「受管理的伺服器」畫面上的受管理產品 IP 位址 如果 IP 位址不正確，請取消註冊，然後重新將受管理產品註冊到 Apex Central as a Service。 • 請參閱受管理產品的《管理手冊》。
不支援的端點	端點不支援策略設定中指定的某些功能。	將用戶端升級到支援的版本。

策略狀態	說明	建議
已從本機變更設定	端點或受管理產品的某些設定不符合策略中指定的設定，因為受管理產品的管理員透過受管理產品主控台做了一些變更。	請於受管理產品主控台上確認設定。
未啟動的產品服務	受管理產品尚未啟動策略設定中所指定的部份服務。	請在受管理產品上啟動相關服務。
關閉的產品服務	未受管理產品已關閉策略設定中所指定的部份服務。	請在受管理產品上啟動相關服務。
已部分部署	Apex Central as a Service 已實施該策略設定的一部分。	請等候幾分鐘後再重新檢查狀態。
受 [Apex Central as a Service 伺服器名稱] 管理	另一個 Apex Central as a Service 目前正在管理受管理產品。	從「受管理的伺服器」清單中移除受管理產品，然後重新將受管理產品新增到清單。
使用者名稱或密碼無效	用於驗證的使用者名稱或密碼不正確。	請確認使用者名稱或密碼。
產品伺服器或驗證資訊無效	伺服器名稱或驗證資訊不正確。	請確認伺服器名稱和驗證資訊。
無法自動登入產品	Apex Central as a Service 無法使用單一登入功能來存取受管理產品。	• 檢查「產品目錄」中的單一登入功能 • 檢查 MCP 代理程式的連線狀態 • 在「受管理的伺服器」清單中，將伺服器的連線類型從「自動」變更為「手動」。
Web 伺服器組態設定錯誤	發生 Web 服務錯誤。	請檢查 IIS 組態設定。
產品通訊錯誤	無法存取產品主控台。	• 檢查是否能連線到受管理產品的 Web 主控台。 • 檢查受管理產品的設定。

策略狀態	說明	建議
無法連線到產品。	Apex Central as a Service 無法建立與受管理產品的連線。	• 檢查受管理產品的連線狀態。 • 檢查網路連線
不支援的產品版本	受管理產品版本不受支援。	將受管理產品升級到支援的版本。
網路組態設定錯誤	發生網路連線錯誤。	檢查網路連線。
系統錯誤。錯誤 ID：[錯誤 ID 號碼]。	發生系統錯誤。	請洽詢您的 Trend Micro 支援人員。

部分 II

Apex Central Widget



第 3 章

Apex Central 資訊中心 Widget

本節包含 Apex Central as a Service 資訊中心中支援的 Apex Central 特定 Widget 的說明主題。

包含下列主題：

- 端點防護驗證 Widget 第 3-2 頁
- 嘗試做出 C&C 回呼的主機 Widget 第 3-3 頁
- Apex Central 前幾名檔案型安全威脅 Widget 第 3-4 頁
- 歷來唯一遭到入侵的主機 Widget 第 3-5 頁
- 策略狀態 第 3-5 頁
- 快速啟動 第 3-6 頁

端點防護驗證 Widget

此 Widget 會顯示整合式 Active Directory 結構中端點的 Apex One 和 Deep Security 安全防護狀態。

重要

在使用此 Widget 之前：

- 請將 Apex One 用戶端樹狀結構與 Active Directory 樹狀結構同步處理。

  如需進一步的指示，請參閱 Apex One 文件。

- 移至「管理 > 設定 > 端點防護驗證」來啟動 Widget，並進行 Active Directory 伺服器、Apex One server 和 Deep Security 伺服器連線設定。

按一下「設定」圖示 (>)，可設定下列項目：

- Apex One server：按一下瀏覽按鈕 ( )，指定要為 Widget 提供資料的 Apex One server。
- Deep Security 伺服器： 按一下瀏覽按鈕 ( )，指定要為 Widget 提供資料的 Deep Security 伺服器。
- 欄：指定 Widget 要在資料表格中顯示的欄。

按一下 Active Directory 結構中的組織單位，可檢視下列資訊。

欄	說明
電腦	顯示端點名稱
Apex One	顯示端點是否受 Apex One 或 VDI 用戶端保護
Deep Security	顯示端點是否受 Deep Security 用戶端保護
實體主機	顯示虛擬端點所在的實體伺服器
特徵碼	顯示 Apex One 或 VDI 用戶端使用的特徵碼檔案版本
掃瞄引擎	顯示 Apex One 或 VDI 用戶端使用的掃瞄引擎版本

欄	說明
用戶端版本	顯示用戶端程式版本
Deep Security 資料檔	顯示使用中的 Deep Security 資料檔
伺服器名稱	顯示與端點連線的 Apex One 和/或 Deep Security 伺服器

嘗試做出 C&C 回呼的主機 Widget

此 Widget 會顯示唯一遭到入侵的主機總數，並依 C&C 清單來源將這些主機分組。

預設檢視會顯示當天的資料。

使用「範圍」下拉式清單，選取顯示的資料時間範圍。您可以檢視「今天」、「1 週」、「2 週」或「1 個月」的資料。

資料	說明
與全球資訊相符的主機	趨勢科技全球資訊網（包括主動式雲端截毒技術）所偵測到的 C&C 回呼。
與動態分析器相符的主機	動態分析器（包括沙盒虛擬平台與網路內容檢測引擎）所偵測到的 C&C 回呼。 分析器內建於 Deep Discovery Inspector 和 Apex One 之類的產品中。
與受管理產品中使用者定義的清單相符的主機	產品利用使用者定義清單所偵測到的 C&C 回呼。 Deep Discovery Inspector 中的「拒絕清單」就是使用者定義清單的一個例子。

Apex Central 前幾名檔案型安全威脅 Widget

此 Widget 會追蹤在整個網路的端點上偵測到的最常見惡意檔案的分佈，並以前 10/25/50（其中之一）名檔案型安全威脅（病毒和間諜程式/可能的資安威脅程式）顯示產品偵測分佈。

按一下圖形中的任何一個節點，可開啟其中顯示詳細資訊的畫面。Apex Central 會執行記錄查詢，以提供詳細資訊。

指定 Widget 所顯示資料的日期範圍：

- 今天
- 1 週
- 2 週
- 1 個月

指定 Widget 顯示的安全威脅。此 Widget 一次只會顯示一種檔案型安全威脅的資料。依預設，此 Widget 會顯示使用者之帳號權限所允許的所有受管理產品的資料。

按一下 Widget 上的 Widget 設定圖示可存取其他設定。

設定	說明
標題	在欄位中為 Widget 指定一個有意義的新標題。
範圍	指定 Widget 顯示的資料範圍。 此範圍決定 Widget 使用哪些產品來顯示資料。
前幾名安全威脅	指定要顯示的安全威脅數目。

按一下「儲存」以套用變更並更新 Widget 資料。

歷來唯一遭到入侵的主機 Widget

此 Widget 會顯示受管理的產品過去 30 天內所記錄的唯一遭到入侵的主機。

此 Widget 會將唯一遭到入侵的主機分組，並用圓圈顯示這些主機。圓圈的大小相對代表遭到入侵的主機數目。

- 小：1 到 5
- 中：6 到 10
- 大：11 或以上

將滑鼠游標移到電腦圖示或主機名稱上，可顯示其他遭到入侵的主機。

使用「回呼位址」下拉式清單可顯示曾嘗試回呼所選回呼位址的遭到入侵的主機。

注意

「回呼位址」下拉式清單包含前 25 名回呼位址。

此 Widget 只會顯示遭到入侵的主機對所選回呼位址的第一次回呼嘗試。

按一下「設定」圖示 (⋮ > ⫶)，來變更 Widget 用做來源的受管理產品。在出現的對話方塊中，按一下 >> 並選取用做來源的受管理產品，來指定「範圍」。

策略狀態

此 Widget 會顯示您各項策略的部署狀態。

按一下策略名稱或目標數目，會開啟一個新「記錄查詢」畫面來提供詳細資訊。

資料	說明
策略	顯示策略的名稱
部署狀態	顯示符合策略設定的目標百分比
已部署	顯示已套用策略設定或具有未啟動的產品服務的目標數目
暫停中	顯示未套用策略設定的目標數目 注意 如果未安裝 Hotfix 2575，則「暫停中」欄會包含具有離線用戶端的目標數目。
離線	顯示具有離線用戶端的目標數目 重要 此功能需要安裝 Hotfix 2575，否則「暫停中」欄會包含具有離線用戶端的目標數目，且不會顯示「離線」欄。
具有問題	顯示因為策略部署不受支援、沒有策略組態設定、系統錯誤、端點與產品伺服器之間通訊錯誤、端點不受支援、從本機變更設定、產品服務已關閉或部署不完全，而未套用策略設定的目標數目
沒有策略的端點/產品	顯示未套用任何策略的端點或受管理產品的數目
端點/產品總數	顯示管理員可以管理的端點或受管理產品的數目

快速啟動

此 Widget 會顯示「產品目錄」和「策略管理」的捷徑。

部分 III

Apex One 資訊中心 Widget

第 4 章

Apex One 資訊中心 Widget

本節說明 Apex Central as a Service 中可用的 Apex One 資訊中心 Widget。

包含下列主題：

- 前幾名封鎖的應用程式 第 4-2 頁
- 前幾名違反的 Application Control 條件 第 4-2 頁

前幾名封鎖的應用程式

此 Widget 提供在違反 Application Control 策略的應用程式當中，使用者最常嘗試存取的前幾名應用程式的總覽。

請使用「設定」按鈕來變更顯示的預設應用程式數目。

前幾名違反的 Application Control 條件

此 Widget 提供使用者在嘗試存取未經授權的應用程式時，最常觸發的前幾名 Application Control 條件的總覽。

請使用「設定」按鈕來變更顯示的預設相符項目數目。

部分 IV

Apex One Security Agent 策略管理

第 5 章

Security Agent 程式設定

本節說明如何管理端點上安裝的 Security Agent 程式。

包含下列主題：

- 其他服務設定 第 5-2 頁
- 權限和其他設定 第 5-4 頁
- 更新代理程式 第 5-15 頁

其他服務設定

Security Agent 程式需要您啟動其他一些服務，以使某些功能正常運作。下表說明可用的服務，以及需要每項服務的功能。

服務	說明	功能
未經授權的變更阻止服務 (TMBMSRV.exe)	規範應用程式行為及驗證程式的可信度	• Machine Learning • 行為監控 • 周邊設備存取控管 • 認證安全防護軟體服務 • 用戶端自我保護
防火牆服務 (TmPfw.exe)	規範網路連線存取權限	• Apex One 防火牆
可疑連線服務	為 C&C 回呼提供進階防護	• 使用者定義的 IP 核可和封鎖清單 • 全域 C&C IP 清單（網路內容檢測引擎） • 惡意程式網路特徵鑑別（關聯規則病毒碼）
資料安全防護服務 (dsagent.exe)	在端點上提供對於敏感資料的進階監控並限制裝置存取權	• Data Loss Prevention • 周邊設備存取控管（封鎖存取權）
進階防護服務 (TMCCSF.exe)	增強進階掃瞄與防護功能	• Machine Learning • 瀏覽器弱點攻擊防護 • 行為監控

設定其他的 Security Agent 服務

程序

1. 在下列區段中選取選項，以啟動「Windows 桌上型電腦」或「Windows Server 平台」上的必要服務：

   - 未經授權的變更阻止服務
     - 在 Windows Server 平台上，請選取「僅啟動 Security Agent 自我保護功能所需的服務」，以確保 Security Agent 程式受到保護而不會影響伺服器效能。

     重要

     選取「僅啟動 Security Agent 自我保護功能所需的服務」可確保與「行為監控」、「周邊設備存取控管」、Machine Learning（程序偵測）和「認證安全防護軟體服務」相關的服務都不會執行。如果您想要使用任何掃瞄功能，請勿啟動此功能。

   - 防火牆服務

     重要

     啟動或關閉服務會暫時中斷端點與網路的連線。請務必在非繁忙時段變更設定，以將連線中斷造成的影響降至最低。

   - 可疑連線服務
   - 資料安全防護服務

     重要

     啟動或關閉服務會暫時中斷端點與網路的連線。請務必在非繁忙時段變更設定，以將連線中斷造成的影響降至最低。

   - 進階防護服務

重要

啟動 Windows Server 平台上的其他服務可能會影響伺服器的效能。啟動 Windows Server 平台上的服務後，趨勢科技建議您監控伺服器一段時間，以確保效能未受影響。

權限和其他設定

設定 Security Agent 授與使用者可以設定個人化設定、顯示通知訊息和保護重要 Security Agent 檔案與服務的權限。

設定用戶端權限

程序

1. 請視需要進行設定。

區段	設定
單機模式	啟動單機模式：允許使用者在 Security Agent 上關閉下列功能，以避免 Security Agent 對系統效能造成負面影響： • Security Agent 不會從伺服器接受策略設定 • Security Agent 不會從伺服器開始掃瞄命令 • Security Agent 不會傳送記錄檔給伺服器 使用者可以在單機模式下的用戶端上，手動開始掃瞄和更新。
掃瞄	• 設定手動掃瞄：允許使用者在 Security Agent 主控台上設定「手動掃瞄」設定 • 設定即時掃瞄：允許使用者在 Security Agent 主控台上設定「即時掃瞄」設定 • 設定即預約瞄：允許使用者在 Security Agent 主控台上設定「預約掃瞄」設定

區段	設定
預約掃瞄	• 延後預約掃瞄：允許使用者在預約掃瞄開始之前延後掃瞄，或是將目前執行中的掃瞄停止一段指定的時間 注意 使用者只能將執行中的掃瞄停止一次。一旦掃瞄重新啟動，Security Agent 會重新掃瞄端點上的所有檔案。 • 略過及停止預約掃瞄：允許使用者略過或停止執行中的預約掃瞄一次 注意 使用者不能多次略過或停止「預約掃瞄」。即使在系統重新啟動後，「預約掃瞄」仍會根據下次預約時間繼續掃瞄。
防火牆	• 在 Security Agent 主控台上顯示防火牆設定：允許使用者在 Security Agent 主控台上進行「防火牆」設定 • 允許使用者啟動/關閉防火牆、入侵偵測系統和防火牆違規通知訊息：在 Security Agent 系統匣圖示上顯示「啟動/關閉防火牆」和「啟動/關閉 IDS 模式」功能表選項 注意 Apex One 防火牆使用狀態檢測、高效能網路病毒掃瞄和消除病毒，來保護網路上的用戶端和伺服器。如果您授與使用者啟動或關閉防火牆和其功能的權限，請警告他們不要長時間關閉防火牆，以避免端點遭受入侵和駭客攻擊。 • 允許 Security Agent 用戶端將防火牆記錄檔傳送到 Apex One server：將 Security Agent 設定為傳送防火牆記錄檔到伺服器，以便您分析網路流量
行為監控	在 Security Agent 主控台上顯示「行為監控」設定：允許使用者在 Security Agent 主控台上進行「行為監控」設定
信任的程式清單	在 Security Agent 主控台上顯示信任的程式清單：允許使用者在 Security Agent 主控台上設定「信任的程式清單」

區段	設定
郵件掃瞄	在 Security Agent 主控台上顯示「郵件掃瞄」設定：允許使用者在 Security Agent 主控台上進行「郵件掃瞄」設定 啟動此設定後，即時掃瞄就會偵測從郵件伺服器擷取的 POP3 電子郵件訊息，並對包含惡意安全威脅的電子郵件採取處理行動。
Proxy 設定	允許使用者設定 Proxy 設定：允許使用者在下列情況下只能使用由使用者設定的 Proxy 設定： • 當 Security Agent 執行「立即更新」時。 • 當使用者關閉（或 Security Agent 無法偵測）自動 Proxy 設定時。 警告! 如果使用者設定的 Proxy 設定不正確，會導致發生更新問題。允許使用者設定自己的 Proxy 設定時請特別小心。
元件更新	• 執行「立即更新」：在 Security Agent 系統匣圖示上顯示「立即更新」功能表選項 • 啟動/關閉預約更新：在 Security Agent 系統匣圖示上顯示「啟動/關閉預約更新」功能表選項 注意 管理員必須先在「其他設定」標籤上選取「啟動 Security Agent 的預約更新」設定，然後功能表項目才會顯示在 Security Agent 功能表上。

區段	設定
卸載並解除鎖定	Security Agent 卸載與解除鎖定權限可讓使用者暫時停止 Security Agent，或者不論是否擁有密碼都能取得進階 Web 主控台功能的存取權。 • 不需要密碼 • 需要密碼：輸入要求的密碼和確認密碼 注意 如果您選取「需要密碼」但不指定密碼，Apex Central as a Service 會套用下列預設密碼： • 對於內部部署 Apex One：在伺服器安裝期間提供的密碼 • 對於 Apex One as a Service：用於佈建主控台的帳號名稱
解除安裝	Security Agent 解除安裝權限允許使用者在本機端點上解除安裝 Security Agent 程式。 • 不需要密碼 • 需要密碼：輸入要求的密碼和確認密碼 注意 如果您選取「需要密碼」但不指定密碼，Apex Central as a Service 會套用下列預設密碼： • 對於內部部署 Apex One：在伺服器安裝期間提供的密碼 • 對於 Apex One as a Service：用於佈建主控台的帳號名稱

設定其他用戶端設定

程序

1. 請視需要進行設定。

區段	設定
共存模式轉換	將使用共存模式的 Security Agent 永久轉換成可完整運作的 Security Agent：啟動在「共存模式」下安裝之 Security Agent 的所有功能 重要 您無法復原此動作。將使用共存模式的 Security Agent 轉換成可完整運作的 Security Agent 之後，用戶端程式會嘗試解除安裝端點上任何不相容的協力廠商安全防護軟體。在轉換完成後，Apex One 會啟動與一般 Security Agent 功能相關的所有必要服務與功能。 如果需要在已轉換的端點上使用共存模式 Security Agent，必須先解除安裝 Security Agent 程式，然後再重新安裝共存模式 Security Agent。

更新設定	• Security Agent 會從趨勢科技主動式更新伺服器下載更新：將無法連線到指定更新來源的 Security Agent 設定為嘗試從趨勢科技主動式更新伺服器進行更新
	• 啟動 Security Agent 用戶端的預約更新：將所有 Security Agent 設定為依預設啟動預約更新
	• Security Agent 僅會更新下列元件：控制 Security Agent 執行元件更新的方式
	  • 所有元件（包括 Hotfix 和用戶端）：Security Agent 會更新所有元件
	  • 病毒碼檔案、引擎、驅動程式：Security Agent 不會升級 Security Agent 程式或部署 Hotfix
	  • 病毒碼檔案：Security Agent 不會升級 Security Agent 程式、部署 Hotfix 或更新引擎和驅動程式

區段	設定
網頁信譽評等設定	當網站被封鎖時顯示通知：每當封鎖違反網頁信譽評等策略的 URL 時，Security Agent 會顯示通知訊息
行為監控設定	當程式被封鎖時顯示通知：每當封鎖違反行為監控策略的程式時，Security Agent 會顯示通知訊息
C&C 聯絡人警訊設定	偵測到 C&C 回呼時顯示通知：每當偵測到 C&C 回呼時，Security Agent 會顯示通知訊息
中央隔離區恢復設定	還原隔離檔案時顯示通知：每當還原隔離的檔案時，Security Agent 會顯示通知訊息
Machine Learning 設定	偵測到安全威脅時顯示通知：每當 Machine Learning 偵測到未知安全威脅時，Security Agent 會顯示通知訊息
Security Agent 自我保護	• 保護 Security Agent 服務：防止使用者或應用程式終止 Security Agent 服務 • 保護 Security Agent 安裝資料夾中的檔案：防止使用者或者應用程式修改或刪除 Security Agent 安裝資料夾中的檔案 • 保護 Security Agent 登錄機碼：防止使用者或者應用程式修改、刪除或新增由 Security Agent 程式使用的登錄值 • 保護 Security Agent 程序：防止使用者或者應用程式終止 Security Agent 程序 如需詳細資訊，請參閱 Security Agent 自我保護 第 5-10 頁。
預約掃瞄設定	執行預約掃瞄之前顯示通知：在設定的預約掃瞄開始執行之前，Security Agent 會顯示通知訊息
用於掃瞄的快取設定	• 啟動數位簽章快取：將 Security Agent 設定為使用行為監控數位簽章特徵碼來排除不進行手動掃瞄、預約掃瞄和立即掃瞄的檔案 • 啟動依要求掃瞄快取：將 Security Agent 設定為保留本機依要求掃瞄快取，以便在手動掃瞄、預約掃瞄和立即掃瞄期間不掃瞄某些檔案，進而提升掃瞄效能 如需詳細資訊，請參閱用於掃瞄的快取設定 第 5-12 頁。
POP3 電子郵件掃瞄設定	掃瞄 POP3 電子郵件：在 Security Agent 上啟動 POP3 郵件掃瞄 如需詳細資訊，請參閱 POP3 郵件掃瞄 第 5-14 頁。

區段	設定
Security Agent 存取限制	不允許使用者從系統匣或 Windows「開始」功能表存取 Security Agent 主控台：不允許使用者使用系統匣或 Windows「開始」功能表存取 Security Agent 主控台 注意 此設定不會關閉 Security Agent。Security Agent 會在背景中執行並持續提供安全威脅防護。
重新啟動通知	當端點需要重新啟動以完成清除中毒檔案時顯示通知：當使用者需要重新啟動端點以完成清除中毒檔案時，Security Agent 會顯示通知

Security Agent 自我保護

使用 Security Agent 自我保護，Security Agent 可保護正常運作所需的程序和其他資源。Security Agent 自我保護可協助防止程式或實際的使用者嘗試關閉惡意程式防護功能。

保護 Security Agent 服務

Apex One 會封鎖所有嘗試來終止下列 Security Agent 服務：

- Apex One NT Listener (`TmListen.exe`)
- Apex One NT RealTime Scan (`NTRtScan.exe`)
- Apex One NT Proxy Service (`TmProxy.exe`)
- Apex One NT Firewall (`TmPfw.exe`)
- Trend Micro Apex One Data Protection Service (`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，Security Agent 可能會使得您無法在端點上成功地安裝協力廠商產品。如果遇到此問題，您可以先暫時關閉此選項，然後在安裝完協力廠商產品之後重新啟動此選項。

- Apex One Common Client Solution Framework (TmCCSF.exe)

保護 Security Agent 安裝資料夾中的檔案

為防止其他程式和使用者修改或刪除 Security Agent 檔案，Apex One 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 Security Agent 登錄機碼

Security Agent 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\Osprey
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\AMSP

保護 Security Agent 處理程序

Security Agent 會封鎖所有嘗試終止下表中處理程序的動作。

處理程序	說明
TmListen.exe	接收來自 Apex One 伺服器的指令與通知，並促進 Security Agent 與伺服器之間的通訊
NTRtScan.exe	在 Security Agent 上執行即時、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
PccNTMon.exe	此處理程序負責啟動 Security Agent 主控台
TmCCSF.exe	執行瀏覽器弱點攻擊防護和記憶體掃瞄

Security Agent 還會阻止在 Microsoft Software Restriction Policies (SRP) 中新增處理程序。Software Restriction Policies 會阻止在端點上執行列出的應用程式。如果要防止在 Software Restriction Policies 清單中新增 Security Agent 處理程序：

1. 啟動「保護 Security Agent 程序」。
2. 啟動「未經授權的變更阻止服務」。

用於掃瞄的快取設定

Security Agent 可以建置數位簽章和依要求掃瞄快取檔案以提高其掃瞄效能。執行依要求掃瞄時，Security Agent 會依次檢查數位簽章快取檔案和依要求掃瞄快

取檔案，以選擇要從掃瞄中排除的檔案。如果不掃瞄大量檔案，將會縮短掃瞄時間。

數位簽章快取

「手動掃瞄」、「預約掃瞄」與「立即掃瞄」期間均會使用數位簽章快取檔案。用戶端不會掃瞄簽章已新增到數位簽章快取檔案的檔案。

Security Agent 使用行為監控所用的數位簽章特徵碼，來建置數位簽章快取檔案。數位簽章特徵碼包含 Trend Micro 認為可信，因而可以不掃瞄的檔案清單。

注意

「行為監控」會在 Windows Server 平台上自動關閉。如果啟動數位簽章快取，這些平台上的 Security Agent 會下載要在快取中使用的數位簽章特徵碼，而不會下載其他行為監控元件。

用戶端會根據預約時程建置數位簽章快取檔案，該時程可從 Web 主控台進行設定。用戶端執行此操作的目的如下：

- 為建立上一快取檔案後加入系統的新檔案新增簽章
- 移除系統中已修改或已刪除檔案的簽章

在快取建置過程中，用戶端會檢查以下資料夾中的可信檔案，然後將這些檔案的簽章新增到數位簽章快取檔案：

- `%PROGRAMFILES%`
- `%WINDIR%`

快取建置程序不會影響端點的效能，因為用戶端在此程序中使用的系統資源非常少。用戶端還可以繼續進行由於某種原因（例如，主機電源關閉或無線端點的 AC 電源轉接器未插電時）而中斷的快取建置工作。

依要求掃瞄快取

在「手動掃瞄」、「預約掃瞄」和「立即掃瞄」期間使用依要求掃瞄快取檔案。Security Agent 不會掃瞄其快取已新增到依要求掃瞄快取檔案的檔案。

每次執行掃瞄時，Security Agent 都會檢查不存在安全威脅的檔案的內容。如果某個不存在安全威脅的檔案在一段時間（可設定該時間範圍）內未經修改，則 Security Agent 會將該檔案的快取新增到依要求掃瞄快取檔案。如果在下一次掃瞄時檔案的快取未到期，則不會掃瞄該檔案。

不存在威脅的檔案的快取會在一定天數（亦可設定該時段）內到期。如果在快取到期時或到期之後進行掃瞄，Security Agent 會移除已到期的快取並掃瞄檔案是否包含威脅。如果檔案不存在威脅且保持不變，則會將該檔案的快取新增回依需求掃瞄快取檔案。如果檔案不存在威脅但最近進行了修改，則不會新增相應的快取，並將在下次掃瞄時重新掃瞄該檔案。

不存在威脅的檔案的快取到期可防止從掃瞄中排除中毒檔案，如以下範例所示：

- 嚴重過期特徵碼檔案可能已將受感染、未修改的檔案視為不存在威脅。如果快取未到期，則中毒檔案會保存在系統中，直到該檔案修改並透過即時掃瞄偵測到。
- 如果修改了快取的檔案，且即時掃瞄在修改檔案期間不可用，則只有快取到期後，才能對修改的檔案掃瞄威脅。

新增到依需求掃瞄快取檔案的快取數取決於掃瞄類型及其掃瞄目標。例如，如果在「手動掃瞄」期間 Security Agent 只掃瞄了端點中 1,000 個檔案中的 200 個，則快取數可能會較少。

如果頻繁執行依需求掃瞄，則依需求掃瞄快取檔案的掃瞄時間會大大降低。在全部快取均未到期的掃瞄工作中，通常需要 12 分鐘的掃瞄可以降到 1 分鐘。降低檔案必須保持不變的天數和延長快取有效期限通常可以提高效能。由於檔案必須在相對較短的時間內保持不變，因此可以將更多的快取新增到快取檔案。快取還可能會保持較長的有效期，這意味著有更多的檔案跳過掃瞄。

如果很少執行依需求掃瞄，則可以關閉依需求掃瞄快取，因為快取會在下一次執行掃瞄時到期。

POP3 郵件掃瞄

當 Security Agent 具有郵件掃瞄權限時，Security Agent 主控台會顯示「郵件掃瞄」選項。「郵件掃瞄」選項會顯示 POP3 郵件掃瞄。

下表說明 POP3 郵件掃瞄程式。

表 5-1. 郵件掃瞄程式

詳細資訊	說明
用途	掃瞄 POP3 電子郵件訊息中是否有病毒/惡意程式
先決條件	• 必須先由管理員從 Web 主控台將其啟動，然後使用者才能使用該程式 注意 您必須啟動「在 Security Agent 主控台上顯示「郵件掃瞄」設定」權限，才能啟動 POP3 郵件掃瞄。 如需詳細資訊，請參閱設定用戶端權限 第 5-4 頁。 • 您可以從 Security Agent 主控台設定針對病毒/惡意程式的處理行動，但無法從 Web 主控台進行設定
支援的掃瞄類型	即時掃瞄 從 POP3 郵件伺服器擷取電子郵件時，便會執行掃瞄。
掃瞄結果	• 有關掃瞄完成後偵測到的安全威脅的資訊 • 未在 Security Agent 主控台的「記錄檔」畫面中記錄的掃瞄結果 • 未傳送到伺服器的掃瞄結果

更新代理程式

如果要將部署元件、網域設定或用戶端程式和 HotFix 的工作分發到 Security Agent，請將某些 Security Agent 指定為更新代理程式或其他 Security Agent 的更新來源。這樣能協助您確保 Security Agent 準時收到更新，而不會將大量網路流量導向至 Apex One server。

如果網路依位置區分為不同網段，而且各網段之間的網路連結出現高傳輸負載，請在每個位置至少指定一個「更新代理程式」。

注意

指定從某個更新代理程式更新元件的 Security Agent 僅會從該更新代理程式收到更新的元件和設定。所有 Security Agent 仍會向 Apex One 伺服器報告其狀態。

將 Security Agent 指定為「更新代理程式」

程序

1. 選取「更新代理程式」可以共用的項目。
   - 元件更新
   - 網域設定
   - Security Agent 程式和 Hotfix

第 6 章

Application Control 策略設定

本節討論如何在 Security Agent 上設定 Application Control 策略。

包含下列主題：

- 應用程式控管 第 6-2 頁
- 設定 Application Control 設定（用戶端） 第 6-2 頁

應用程式控管

Application Control 讓您能夠控制哪些使用者可在一些端點上存取特定的應用程式。您可以選擇建立整體的端點型策略，如果已整合 Active Directory，那麼您可以按端點建立非常精細的使用者型策略。

在您確定策略的範圍後，可以建立應用程式相符條件，來定義要允許、封鎖或監控哪些應用程式。有經驗的使用者可以建立「鎖定」條件，藉此僅允許信任的應用程式執行，並封鎖規則明確不允許的所有應用程式。

設定 Application Control 設定（用戶端）

在設定 Application Control 策略之前，請確保您會先定義所有必要的 Application Control 條件。Application Control 策略需要使用預先設定的條件，該條件定義您要在端點上或要針對特定使用者「允許」或「封鎖」哪些應用程式。

如需詳細資訊，請參閱：

程序

1. 選取「啟動 Application Control」。
2. 在「使用者定義的規則」區段中，根據已登入的使用者帳號，將規則指派至端點。

   重要

   - 僅當您擁有整合式 Active Directory 時，才能使用使用者型 Application Control。如果您沒有 Active Directory 整合，則只能將條件指派至預設的「所有使用者帳號」規則。
   - 您無法刪除預設的「所有使用者帳號」規則。

   a. 新增規則或修改現有規則。

- 如果要新增規則，請按一下「指派規則」。
- 如果要修改現有規則，請按一下資料表中「使用者帳號」欄的值。

會出現「指派規則」畫面。

b. 指定您要套用特定 Application Control 條件的「使用者帳號」。

重要

- 僅當您擁有整合式 Active Directory 時，才能使用使用者型 Application Control。如果您沒有 Active Directory 整合，則只能將規則指派至預設的「所有使用者帳號」規則。
- 每個規則只能指派 30 個使用者或群組。如果您需要將更多的使用者數目指派給策略，請建立其他規則。

---

c. 按一下條件的「名稱」，將所需的條件移至「選取的條件」資料表。

d. 按一下「儲存」。

注意

如果要變更規則的「優先順序」，請選取並拖曳規則到清單中的不同位置。Application Control 會將第一個相符規則套用至多個規則中所包含的使用者。

---

3. 在「其他處理行動」區段中，指定使用者嘗試執行的應用程式未符合任何「使用者定義的規則」條件時，Application Control 所要執行的處理行動。

- 允許：所有其他應用程式都能執行：Application Control 對未符合任何「使用者定義的規則」條件的應用程式中不採取任何處理行動。選擇使用 Application Control 封鎖或監控應用程式使用率的時機。
- 鎖定：封鎖所有未在上次資產清單掃瞄期間識別出來的應用程式：在端點收到此指令後，Application Control 會採取下列處理行動：

  a. Application Control 掃瞄端點，並建立完整的應用程式資產清單。

  b. Application Control「鎖定」端點，而且不允許存取：

  - 明確不符合「使用者定義的規則」資料表中定義之「允許」條件的所有應用程式

- 明確不符合「使用者定義的規則」資料表中定義之評估條件的所有應用程式
- 在特定端點的資產清單掃瞄結果中找不到的任何應用程式

- 排除來自趨勢科技所信任供應商的應用程式：選取此選項可自動允許趨勢科技安全威脅專家已判斷為來自所信任供應商的所有應用程式

4. 在「用戶端通知」區段中，選取「在有應用程式遭封鎖時顯示通知」可在 Application Control 封鎖應用程式時在端點上顯示通知。

5. 在「記錄檔維護」區段中，指定端點應保留記錄檔資料的天數上限。

重要

請記得先「部署」或「儲存」您的 Apex One Security Agent 策略，再離開此畫面。如果您沒有儲存整個策略，將會遺失所有變更。

第 7 章

行為監控策略設定

本節說明如何在 Security Agent 中設定行為監控策略。

包含下列主題：

- 行為監控 第 7-2 頁
- 設定行為監控規則與例外 第 7-11 頁

行為監控

行為監控會不斷地監控端點上的作業系統或已安裝軟體是否發生了異常修改。行為監控透過惡意程式行為封鎖和事件監控來保護端點。這兩個功能搭配使用者已設定的例外清單和認證安全防護軟體服務更是相得益彰。

重要

依預設，「行為監控」在所有版本的 Windows Server 平台上 j 均是關閉的。

惡意程式行為封鎖

惡意程式行為封鎖能夠提供多一層的必要安全威脅防護，以封鎖存在惡意行為的程式。它會觀察一段時間內的系統事件。當程式執行不同的動作組合或動作序列時，惡意程式行為封鎖會偵測已知的惡意行為並封鎖關聯程式。使用此功能可確保以更高等級來抵禦全新、未知和新興的安全威脅。

惡意程式行為監控會提供以下威脅程度掃瞄選項：

- 「已知安全威脅」：封鎖與已知惡意程式安全威脅相關聯的行為
- 「已知和潛在威脅」：封鎖與已知威脅相關聯的行為並對可能是惡意的行為採取處理行動

在已啟動通知的情況下，封鎖某個程式後，Security Agent 會在端點上顯示通知。

勒索軟體防護

「勒索軟體防護」會阻止「勒索軟體」安全威脅未經授權即修改或加密用戶端上的檔案。勒索軟體是一種惡意軟體，會限制存取檔案，並要求付錢才能恢復受影響的檔案。

Apex One 提供下列方法，保護您的環境不受勒索軟體安全威脅的侵害。

注意

若要減少 Security Agent 將安全的程序偵測為惡意程式的機會，請確保用戶端具有 Internet 存取，以使用 Trend Micro 伺服器執行其他驗證程序。

選項	說明
保護文件以防止未經授權的加密或修改	您可以設定行為監控偵測可能代表勒索軟體攻擊的特定事件序列。在「行為監控」比對以下所有條件後，Security Agent 就會終止並嘗試隔離惡意程式： 1. 某個未被識別安全的程序嘗試在一段時間內修改、刪除或重新命名三個檔案。 2. 程序嘗試修改受保護的副檔名類型 此外，啟動「自動備份可疑程式變更的檔案」，可為端點上要加密的檔案建立副本。完成加密程序後，如果 Apex One 偵測到勒索軟體安全威脅，Apex One 會提示使用者恢復受影響的檔案，而無須承受任何資料遺失之苦。 注意 自動檔案備份需要用戶端端點上至少有 100 MB 的磁碟空間，而且僅會備份大小小於 10 MB 的檔案。 用戶端端點上的備份資料夾位置為：<用戶端安裝資料夾>\CCSF\module\DRE\data。 警告! 如果未啟動「自動備份可疑程式變更的檔案」，Apex One 無法復原受勒索軟體安全威脅影響的最初檔案。
封鎖常與勒索軟體相關的程序	勒索軟體通常會先將可執行檔分發到端點上的特定位置，然後再嘗試綁架檔案。封鎖從這些位置啟動的程序，有助於讓勒索軟體無法綁架檔案。

選項	說明
啟動程式檢測，以偵測並封鎖遭到入侵的可執行檔	程式檢測會監控程序並執行 API 攔截，藉以判斷某個程式是否存在非預期的行為。雖然此程序可提高對遭到入侵的可執行檔的整體偵測率，卻可能會導致系統效能降低。 秘訣 如果您在「要封鎖的安全威脅」下拉式清單中選取「已知和潛在安全威脅」，程式檢測會提供增強的安全性。

弱點攻擊防護

弱點攻擊防護會與程式檢測搭配運作，藉以監控程式的行為，並偵測可能代表攻擊者已攻擊程式弱點的異常行為。偵測到異常行為後，「行為監控」就會終止程式程序。

重要

若要使用「弱點攻擊防護」，您必須選取「啟動程式檢測，以偵測並封鎖遭到入侵的可執行檔」。

新發現的程式防護

「行為監控」與「網頁信譽評等服務」和「即時掃瞄」搭配使用時，可驗證經由 Web 通道、電子郵件應用程式或 Microsoft Office 巨集指令碼下載的檔案的普遍程度。偵測到「新發現」的檔案後，管理員可選擇在執行檔案之前提示使用者。Trend Micro 會根據偵測到檔案的次數或是檔案存在的時間長度（由主動雲端截毒技術判定），決定是否將程式分類為新發現的程式。

「行為監控」會掃瞄每個通道的下列檔案類型：

- Web (HTTP/HTTPS)：掃瞄 `.exe` 檔案。
- 電子郵件應用程式：掃瞄 `.exe` 檔案以及未加密的 `.zip` 和 `.rar` 檔案中的壓縮 `.exe` 檔案。

注意

- 管理員必須啟動用戶端上的「網頁信譽評等服務」以允許 Security Agent 掃瞄 HTTP 或 HTTPS 流量，然後才能顯示此提示。
- Security Agent 會在執行程序期間比對透過電子郵件應用程式下載的檔案名稱。如果檔案名稱已變更，使用者就不會收到提示。

事件監控

事件監控提供了一種更為通用的方法來抵禦未授權軟體和惡意程式攻擊。它會在系統區域中監控某些事件，允許管理員調整觸發此類事件的程式。如果您的特定系統保護需求高於惡意程式行為封鎖提供的需求，請使用事件監控。

以下表格為監控系統事件清單。

表 7-1. 監控的系統事件

事件	說明
重複的系統檔案	許多惡意程式會使用 Windows 系統檔案所使用的檔案名稱，來建立本身或其他惡意程式的副本。這樣做通常是為了覆寫或取代系統檔案、規避偵測，或讓使用者不敢隨意刪除惡意檔案。
Hosts 檔案修改	Hosts 檔案可將網域名稱對應到 IP 位址。許多惡意程式皆有能力修改主機檔案，而使網路瀏覽器重新導向至中毒、不存在或偽造的網站。
可疑行為	可疑行為是合法程式很少執行的特定動作或一系列動作。使用有可疑行為的程式時應小心謹慎。
新 Internet Explorer 嵌入程式	間諜程式/可能的資安威脅程式通常會安裝不必要的 Internet Explorer 嵌入程式，包括工具列和瀏覽器協助物件。
Internet Explorer 設定的修改	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。
安全策略修改	修改「Windows 安全策略」可允許不必要的應用程式執行及變更系統設定。

事件	說明
程式庫插入	許多惡意程式都會設定 Windows，以讓所有應用程式自動載入程式庫 (DLL)。這樣可讓 DLL 中的惡意常式在每次應用程式啟動時執行。
Shell 的修改	許多惡意程式都會修改 Windows Shell 設定，以將本身與特定檔案類型關聯。此常式可讓惡意程式在使用者於「Windows 檔案總管」中開啟關聯的檔案時自動啟動。變更 Windows Shell 設定也可以讓惡意程式追蹤所使用的程式，以及隨著合法應用程式啟動。
新服務	Windows 服務是具有特殊功能的處理程序，通常以完整的系統管理權限在背景連續執行。惡意程式有時會將本身安裝為服務，以維持隱藏狀態。
系統檔案修改	特定 Windows 系統檔案決定系統行為，包括啟動程式和螢幕保護裝置設定。許多惡意程式都會修改系統檔案，以在系統啟動時自動啟動並控制系統行為。
防火牆策略的修改	「Windows 防火牆策略」決定可存取網路的應用程式、開放用於通訊的通訊埠，以及可與電腦通訊的 IP 位址。許多惡意程式都會修改策略，以允許本身存取網路和 Internet。
系統程序的修改	許多惡意程式會在內建 Windows 處理程序中執行各種動作。這些動作可能包含終止或修改執行中的處理程序。
新啟動程式	惡意應用程式通常會在 Windows 登錄中新增或修改自動啟動項目，以在每次電腦啟動時自動啟動。

當事件監控偵測到監控的系統事件時，它會執行針對此事件所設定的處理行動。

以下表格列出的是管理員在監控系統事件上可採取的行動。

表 7-2. 監控的系統事件的處理行動

處理行動	說明
存取	Security Agent 一律允許與事件相關聯的程式執行，並且會記錄事件以供評估。 這是對所有監控的系統事件的預設處理行動。 注意 這個選項不支援 64 位元系統的程式庫植入（DLL 植入）事件。
允許	Security Agent 一律允許與事件相關聯的程式執行。
需要時詢問	Security Agent 會提示使用者允許或拒絕與事件相關聯的程式執行，並將該程式新增到例外清單。 如果使用者在特定的時間內未回應，Security Agent 會自動允許此程式執行。預設時間為 30 秒。 注意 這個選項不支援 64 位元系統的程式庫植入（DLL 植入）事件。
拒絕	Security Agent 一律封鎖與事件相關聯的程式執行，並且會記錄事件。 在已啟動通知的情況下，封鎖某個程式後，Security Agent 會在端點上顯示通知。

行為監控例外清單

行為監控例外清單包含 Security Agent 未使用行為監控加以監控的程式。

- 核可的程式：Security Agent 會讓「核可的程式」清單中的所有程式通過行為監控掃瞄。

注意

雖然行為監控不會對已新增至「核可的程式」清單的程式採取處理行動，但其他掃瞄功能（例如，檔案型掃瞄）仍會先掃瞄程式再允許程式程行。

- 封鎖的程式：Security Agent 會封鎖「封鎖的程式」清單中的所有程式。若要設定「封鎖的程式」清單，請啟動「事件監控」。

從 Web 主控台設定例外清單。您也可以授與使用者權限，讓他們可以從 Security Agent 主控台設定自己的例外清單。

如需詳細資訊，請參閱設定用戶端權限 第 5-4 頁。

例外清單萬用字元支援

在定義檔案路徑、檔案名稱和副檔名等例外類型時，行為監控核可清單支援使用萬用字元。請使用下表來正確格式化例外清單，以確保 Apex One 不掃瞄正確的檔案和資料夾。

支援的萬用字元：

- 星號 (*)：代表任意字元或一串字元
- 問號 (?)：代表單一字元

重要

行為監控核可清單不支援使用萬用字元來取代系統磁碟機代號或 UNC 位址。

例外類型	萬用字元用法	相符	不相符
目錄	`C:\*` 排除指定磁碟機中的所有檔案和資料夾	• `C:\sample.exe` • `C:\folder\test.doc`	• `D:\sample.exe` • `E:\folder\test.doc`

例外類型	萬用字元用法	相符	不相符
特定資料夾層下的特定檔案	`C:\*\Sample.exe` 僅在 `Sample.exe` 檔案位於 `C:\` 目錄下的任何子資料夾內時才排除此檔案	• `C:\files\Sample.exe` • `C:\temp\files\Sample.exe`	• `C:\sample.exe`
UNC 路徑	`\\<UNC path>\*\Sample.exe` 僅在 `Sample.exe` 檔案位於指定 UNC 路徑下的任何子資料夾內時才排除此檔案	• `\\<UNC path>\files\Sample.exe` • `\\<UNC path>\temp\files\Sample.exe`	• `R:\files\Sample.exe` 原因：不支援對應磁碟機。 • `\\<UNC path>\Sample.exe` 原因：檔案並未存在於 UNC 路徑下的子資料夾內。
檔案名稱和副檔名	`C:\*.*` 排除 `C:\` 目錄下所有資料夾和子資料夾內具有副檔名的所有檔案	• `C:\Sample.exe` • `C:\temp\Sample.exe` • `C:\test.doc`	• `D:\sample.exe` • `C:\Sample` **注意** `C:\Sample` 沒有副檔名，因此會被排除而不掃瞄。

例外類型	萬用字元用法	相符	不相符
檔案名稱	`C:\*.exe` 排除 C:\ 目錄下所有資料夾和子資料夾內副檔名為 .exe 的所有檔案	• C:\Sample.exe • C:\temp\test.exe	• C:\Sample.doc • C:\temp\test.bat • C:\Sample **注意** C:\Sample 沒有副檔名，因此會被排除而不掃瞄。
副檔名	`C:\Sample.*` 排除 C:\ 目錄下名稱為 Sample（副檔名不限）的檔案。	• C:\Sample.exe	• C:\Sample1.doc • C:\temp\Sample.bat • C:\Sample **注意** C:\Sample 沒有副檔名，因此會被排除而不掃瞄。
特定目錄結構中的檔案	`C:\*\*\Sample.exe` 排除位於 C:\ 目錄下第二層子資料夾或任何更下層子資料夾內所有檔案名稱和副檔名為 Sample.exe 的檔案	• C:\files\temp\Sample.exe • C:\files\temp\test\Sample.exe	• C:\Sample.exe • C:\temp\Sample.exe • C:\files\temp\Sample.doc

例外類型	萬用字元用法	相符	不相符
複雜的路徑或檔案名稱	`C:\Sam*e??.exe` 排除其名稱滿足下列條件的所有檔案： • 以字元 "Sam" 為開頭 • 檔案名稱的倒數第三個字元必須是 "e" • 檔案名稱開頭的 "Sam" 字串與結尾的 "e??" 字串之間必須至少有 1 個字元 • 副檔名之前與檔案名稱中的 "e" 之後必須有正好 2 個字元 • 副檔名是 .exe 如果檔案符合所有要求的條件且位於 C:\ 目錄中，「行為監控」就會排除這些檔案而不掃瞄。	• C:\Sample12.exe • C:\SamSamSample12.exe	• C:\SaSmple12.exe 原因：不是以 "Sam" 為開頭 • C:\SamSamSam12.exe 原因：倒數第三個字元不是 "e" • C:\Same12.exe 原因：開頭的 "Sam" 字串與倒數第三個字元 "e" 之間未包含任何其他字元 • C:\Sample1.exe 原因：副檔名之前與 "e" 之後未包含 2 個字元 • C:\Sample12.doc 原因：副檔名不正確

設定行為監控規則與例外

設定行為監控策略以保護端點抵禦勒索軟體、弱點攻擊和新興的安全威脅。使用事件監控功能可評估或封鎖常與惡意程式安全威脅相關的行為。

注意

依預設，「行為監控」在所有版本的 Windows Server 平台上 j 均是關閉的。

程序

1. 在「惡意程式行為封鎖」區段中：

   a. 選取「啟動惡意程式行為封鎖」，然後指定要封鎖的安全威脅類型：

      - 已知安全威脅：封鎖與已知惡意程式安全威脅相關聯的行為
      - 已知和潛在安全威脅：封鎖與已知威脅相關聯的行為，並對可能是惡意的行為採取處理行動

   b. 選取您要啟用以抵禦勒索軟體安全威脅的勒索軟體防護功能。

      - 保護文件以防止未經授權的加密或修改：阻止潛在的勒索軟體安全威脅加密或修改文件內容
        - 自動備份與恢復遭可疑程式變更的檔案：在偵測到勒索軟體安全威脅時，為端點上要加密的檔案建立備份複本，以防任何資料遺失

        注意

        自動檔案備份需要用戶端端點上至少有 100 MB 的磁碟空間，而且僅會備份大小小於 10 MB 的檔案。

      - 封鎖常與勒索軟體相關的處理程序：在加密和修改文件之前，封鎖與已知勒索軟體安全威脅相關的處理程序
      - 啟動程式檢測，以偵測並封鎖遭到入侵的可執行檔：程式檢測可監控處理程序並執行 API 攔截，以判斷程式是否表現出非預期的行為。雖然此程序可提高對遭到入侵的可執行檔的整體偵測率，卻可能會導致系統效能降低。

        秘訣

        如果您在「要封鎖的安全威脅」下拉式清單中選取「已知和潛在安全威脅」，程式檢測會提供增強的安全性。

      如需詳細資訊，請參閱勒索軟體防護 第 7-2 頁。

   c. 在「弱點攻擊防護」下，啟動「如果程式展現出與弱點攻擊有關的異常行為，請將其終止」，以防範可能遭到攻擊的程式。

注意

若要使用「弱點攻擊防護」，您必須選取「啟動程式檢測，以偵測並封鎖遭到入侵的可執行檔」。

如需詳細資訊，請參閱弱點攻擊防護 第 7-4 頁。

重要

弱點攻擊防護與即時掃瞄 (隔離在記憶體中偵測到的惡意程式變體) 搭配使用時，可增強防禦無檔案攻擊的能力。

如需詳細資訊，請參閱即時掃瞄：「目標」標籤 第 8-11 頁。

2. 在「新發現的程式」區段中，啟動「監控經由 Web 或電子郵件應用程式通道下載之新發現的程式」，然後選取要在執行所下載的程式之前先「提示使用者」，還是讓 Apex One 僅記錄偵測。

3. 在「事件監控」區段中：

   a. 選取「啟動事件監控」。

   b. 請點選「指定詳細設定」以選取要監控的事件類型。

   c. 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 7-5 頁。

4. 請點選「例外」標籤以設定例外清單。

   a. 在「輸入完整的程式路徑」下，輸入要核可或封鎖的程式完整路徑。

      請以半形分號 (;) 來分隔多個項目。

   b. 請點選「新增到例外清單」或「新增到封鎖清單」。

   c. 如果要從清單中移除封鎖的或核可的程式，請點選程式旁的垃圾桶圖示 ( )。

注意

Apex One 最多可接受合併總計 1024 個核可的程式和封鎖的程式。

第 8 章

惡意程式防護策略設定

本節說明如何在 Security Agent 中設定惡意程式防護掃瞄。

包含下列主題：

- 掃瞄方法類型 第 8-2 頁
- 手動掃瞄 第 8-4 頁
- 即時掃瞄 第 8-9 頁
- 立即掃瞄 第 8-17 頁
- 預約掃瞄 第 8-23 頁
- 中毒處理行動 第 8-30 頁
- 掃瞄例外支援 第 8-38 頁

掃瞄方法類型

Security Agent 可以使用兩種掃瞄方法中的其中一種來掃瞄是否有安全威脅。掃瞄方法包括雲端截毒掃瞄和標準掃瞄。

- 雲端截毒掃瞄

  使用雲端截毒掃瞄的 Security Agent 在本文件中稱為雲端截毒掃瞄用戶端。雲端截毒掃瞄用戶端將受益於檔案信譽評等服務提供的本機掃瞄和雲端查詢。

- 標準掃瞄

  不使用雲端截毒掃瞄的 用戶端稱為標準掃瞄用戶端。標準掃瞄用戶端會將所有 Security Agent 元件儲存在端點上，並在本機掃瞄所有檔案。

切換掃瞄方法指導方針

下表列出切換 Security Agent 使用的掃瞄方法前應瞭解的一些考量事項。

表 8-1. 切換到雲端截毒掃瞄時的注意事項

注意事項	詳細資訊
產品使用授權	確定已啟動新掃瞄方法需要的所有使用授權。
Apex One 伺服器	確保用戶端可連線到 Apex One 伺服器。Apex One 只會通知已上線的用戶端切換掃瞄方法。離線用戶端在上線後，才會接獲通知。單機用戶端會在上線後接獲通知，或者用戶端若有預約更新權限，則會在執行預約更新時接獲通知。 此外，需確認 Apex One 伺服器具有最新的元件，以確保 Security Agent 可以從伺服器下載正確的病毒碼。
要切換的 Security Agent 數目	一次切換少量的 Security Agent，可確保有效利用 Apex One server 與主動式雲端截毒技術伺服器資源。當 Security Agent 變更掃瞄方法的同時，這些伺服器可以執行其他重要工作。

注意事項	詳細資訊
時機	切換掃瞄方法時，Security Agent 必需下載適用於新掃描方法的完整版必要病毒碼檔案。 建議您在離峰時段進行切換，以便將對網路頻寬的影響及對使用者日常作業的干擾降到最低。趨勢科技建議您在轉換程序進行期間關閉 Security Agent 中的「立即更新」功能。
IPv6 支援 重要 僅適用於向內部部署 Apex One server 報告的 Security Agent。	雲端截毒掃瞄用戶端會將掃瞄查詢傳送至主動雲端截毒技術來源。 純 IPv6 雲端截毒掃瞄用戶端無法將查詢直接傳送到純 IPv4 來源，例如： • 主動雲端截毒技術伺服器 2.0（整合式或獨立式） 注意 主動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 雲端截毒掃瞄用戶端無法將查詢傳送至純 IPv6 主動雲端截毒技術伺服器。 如果要使雲端截毒掃瞄用戶端連線到來源，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。
主動雲端截毒技術服務 重要 僅適用於向內部部署 Apex One server 報告的 Security Agent。	如果要將 Security Agent 從標準掃瞄切換到雲端截毒掃瞄，請確定已設定「主動雲端截毒技術服務」。

手動掃瞄

「手動掃瞄」是依需求掃瞄，會在使用者於 Security Agent 主控台上執行掃瞄後立即啟動。完成掃瞄所需的時間，視要掃瞄的檔案數目和 Security Agent 端點的硬體資源而定。

請設定「手動掃瞄」設定，並將其套用至一或多個用戶端與網域，或套用至伺服器管理的所有用戶端。

設定手動掃瞄設定

請使用下列標籤來設定「手動掃瞄」設定：

- 手動掃瞄：「目標」標籤 第 8-4 頁
- 手動掃瞄：「處理行動」標籤 第 8-6 頁
- 手動掃瞄：「掃瞄例外」標籤 第 8-8 頁

手動掃瞄：「目標」標籤

程序

1. 在「要掃瞄的檔案」區段中，從下列項目中選取：
   - 所有可掃瞄的檔案：包括所有可掃瞄的檔案。無法掃瞄的檔案為受密碼保護的檔案、加密檔案、或超過使用者定義的掃瞄限制範圍的檔案。

     注意

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

   - IntelliScan 所掃瞄的檔案類型：根據真實檔案型態掃瞄檔案。

- 具有下列副檔名的檔案（使用逗號來分隔項目）：根據副檔名手動指定要掃瞄的檔案。請使用逗號分隔多個項目。

注意

設定上層策略時，指定其他使用者設定子策略的方式。

- 從上層策略繼承：子策略必須使用在上層策略中設定的設定
- 從上層策略延伸：子策略可以將其他設定附加至從上層策略繼承的設定

2. 在「掃瞄設定」區段中，設定必要設定。

設定	說明
掃瞄隱藏資料夾	允許 Security Agent 偵測端點上的隱藏資料夾，然後加以掃瞄
掃瞄網路磁碟機	掃瞄實際位於其他端點，但對應至本機端點的目錄
掃瞄壓縮檔	掃瞄封存檔中指定的壓縮層數  注意 掃瞄更多層有可能偵測到深藏在壓縮封存檔中的惡意程式，但這麼做可能影響系統效能。
掃瞄 OLE 物件	掃瞄檔案中指定的「物件連結與嵌入」(OLE) 層數 在 OLE 檔案中偵測到弱點攻擊程式碼：OLE 弱點攻擊偵測會檢查 Microsoft Office 檔案中是否有弱點攻擊程式碼，主動識別惡意程式。  注意 指定的層數同時適用於「掃瞄 OLE 物件」和「在 OLE 檔案中偵測到弱點攻擊程式碼」選項。
掃瞄開機區	掃瞄端點上硬碟的開機磁區是否有病毒/惡意程式

3. 在「CPU 使用率」區段中，從下列項目中選取：

- 高：掃瞄之間不暫停

- 中：如果 CPU 耗用大於 50% 便在檔案掃瞄間暫停；如果小於 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

手動掃瞄：「處理行動」標籤

程序

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

        如需詳細資訊，請參閱主動式處理行動 第 8-31 頁。

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

        如需詳細資訊，請參閱自訂中毒處理行動 第 8-32 頁。

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

      建立檔案的備份複本，可供您在需要時恢復檔案的原始版本。

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

- 隔離目錄：Security Agent 會將所有隔離檔案的加密複本傳送到指定的位置

如需詳細資訊，請參閱隔離目錄 第 8-33 頁。

d. 在「損害清除及復原服務」區段中，設定下列項目：

- 清除類型
  - 標準清除：Security Agent 會在標準清除期間執行下列任何處理行動：
    - 偵測並移除活動的特洛伊木馬程式
    - 終結特洛伊木馬程式所建立的處理程序
    - 修復特洛伊木馬程式修改的系統檔案
    - 刪除特洛伊木馬程式遺留的檔案和應用程式
  - 進階清除：除了標準清除處理行動外，Security Agent 還會遏止詐欺安全軟體（亦稱為 FakeAV）及某些 Rootkit 變體的活動。
- 偵測到可能的病毒/惡意程式時執行清除：針對可能的惡意程式安全威脅執行設定的清除類型

注意

只有對可能的病毒/惡意程式的處理行動不是「暫不處理」也不是「拒絕存取」時，才能選取該選項。

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

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

注意

在清除間諜程式/可能的資安威脅程式後，Security Agent 會備份間諜程式/可能的資安威脅程式資料，如果您認為可安全存取這些間諜程式/可能的資安威脅程式，便可恢復這些資料。

- 暫不處理：記錄偵測事件，但允許程式執行

手動掃瞄：「掃瞄例外」標籤

程序

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

      如需詳細資訊，請參閱趨勢科技產品目錄例外 第 8-38 頁。

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

   c. 輸入不掃瞄的目錄路徑，然後點選 + 按鈕。

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

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

        如需詳細資訊，請參閱萬用字元例外 第 8-39 頁。

3. 在「掃瞄例外清單（檔案）」區段中，設定必要設定。
   a. 設定上層策略時，指定其他使用者設定子策略的方式。
      - 從上層策略繼承：子策略必須使用在上層策略中設定的設定
      - 從上層策略延伸：子策略可以將其他設定附加至從上層策略繼承的設定

b. 輸入不掃瞄的檔案名稱或加上完整目錄路徑的檔案名稱，然後點選 + 按鈕。

注意

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

  如需詳細資訊，請參閱萬用字元例外 第 8-39 頁。

4. 在「掃瞄例外清單（副檔名）」區段中，設定必要設定。

   a. 設定上層策略時，指定其他使用者設定子策略的方式。

   - 從上層策略繼承：子策略必須使用在上層策略中設定的設定
   - 從上層策略延伸：子策略可以將其他設定附加至從上層策略繼承的設定

   b. 選取或輸入不掃瞄的副檔名，然後點選「新增 >」按鈕。

注意

- 您最多可以指定 256 個不掃瞄的副檔名。
- 若為「手動掃瞄」、「預約掃瞄」與「立即掃瞄」，請使用問號 (?)（用於取代單一字元）或星號 (*)（用於取代多個字元）做為萬用字元。例如，如果您不要掃瞄副檔名以 D 開頭的所有檔案（例如 DOC、DOT 或 DAT），請輸入 `D*` 或 `D??`。

即時掃瞄

「即時掃瞄」會一直持續進行。每當接收、開啟、下載、複製或修改檔案時，「即時掃瞄」即會掃瞄檔案是否存在安全威脅。如果 Security Agent 未偵測到安全威脅，則使用者可以繼續存取檔案。如果 Security Agent 偵測到安全威脅或可能的病毒/惡意程式，則會顯示一則通知訊息，指出中毒檔案的名稱和具體的安全威脅。

即時掃瞄會保留一個持續的掃瞄快取，每次 Security Agent 啟動時都會重新載入該掃瞄快取。Security Agent 會追蹤在卸載 Security Agent 後對檔案或資料夾進行的所有變更，並將這些檔案從快取移除。

設定即時掃瞄設定

程序

1. 選取下列選項：
   - 啟動病毒/惡意程式掃瞄
   - 啟動間諜程式/可能的資安威脅程式掃瞄

   注意

   必須先啟動病毒/惡意程式掃瞄，然後才能啟動間諜程式/可能的資安威脅程式掃瞄。在病毒爆發期間，Security Agent 會自動啟動即時掃瞄，並且在病毒爆發結束之前，您都無法關閉掃瞄功能。即時掃瞄可防止病毒修改或刪除端點上的檔案和資料夾。

2. 設定「目標」設定。

   如需詳細資訊，請參閱即時掃瞄：「目標」標籤 第 8-11 頁。

3. 設定「處理行動」設定。

   如需詳細資訊，請參閱即時掃瞄：「處理行動」標籤 第 8-13 頁。

4. 設定「掃瞄例外」設定。

   如需詳細資訊，請參閱即時掃瞄：「掃瞄例外」標籤 第 8-15 頁。

即時掃瞄：「目標」標籤

程序

1. 在「使用者對檔案執行的活動」區段中，從「執行下列動作時掃瞄檔案」下拉式清單中選取會觸發掃瞄的檔案作業。
   - 建立/修改和擷取時：掃瞄端點上已建立、已修改或已開啟的所有檔案
   - 建立/修改時：掃瞄端點上已建立或已修改的所有檔案
   - 擷取時：掃瞄端點上已開啟的所有檔案
2. 在「要掃瞄的檔案」區段中，從下列項目中選取：
   - 所有可掃瞄的檔案：包括所有可掃瞄的檔案。無法掃瞄的檔案為受密碼保護的檔案、加密檔案、或超過使用者定義的掃瞄限制範圍的檔案。

     注意

     此選項提供了可能的最高安全性。但是，掃瞄每個檔案是一件即費時又耗資源的事，而且在某些情況下可能會太過累贅。因此，您可以限制用戶端在掃瞄中包含的檔案數量。
   - IntelliScan 所掃瞄的檔案類型：根據真實檔案型態掃瞄檔案。
   - 具有下列副檔名的檔案（使用逗號來分隔項目）：根據副檔名手動指定要掃瞄的檔案。請使用逗號分隔多個項目。

     注意

     設定上層策略時，指定其他使用者設定子策略的方式。
     - 從上層策略繼承：子策略必須使用在上層策略中設定的設定
     - 從上層策略延伸：子策略可以將其他設定附加至從上層策略繼承的設定
3. 在「掃瞄設定」區段中，設定必要設定。

設定	說明
關機期間掃瞄軟碟機	關機期間掃瞄軟碟機
掃瞄網路磁碟機	掃瞄實際位於其他端點，但對應至本機端點的目錄
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
在插入卸除式儲存裝置之後掃瞄其中所有檔案	在每次使用者插入 USB 儲存裝置時，自動掃瞄其所有檔案
隔離在記憶體中偵測到的惡意程式變體	「行為監控」會掃瞄系統記憶體中是否有可疑處理程序，而「即時掃瞄」會對應處理程序並掃瞄其中是否有惡意程式安全威脅。如果發現惡意程式安全威脅，「即時掃瞄」會隔離處理程序和（或）檔案。 注意 記憶體掃瞄會與行為監控中的弱點攻擊防護搭配運作，以針對無檔案型態攻擊提供增強的防護。 如需詳細資訊，請參閱設定行為監控規則與例外 第 7-11 頁。
掃瞄壓縮檔	掃瞄封存檔中指定的壓縮層數 注意 掃瞄更多層有可能偵測到深藏在壓縮封存檔中的惡意程式，但這麼做可能影響系統效能。

設定	說明
掃瞄 OLE 物件	掃瞄檔案中指定的「物件連結與嵌入」(OLE) 層數 在 OLE 檔案中偵測到弱點攻擊程式碼：OLE 弱點攻擊偵測會檢查 Microsoft Office 檔案中是否有弱點攻擊程式碼，主動識別惡意程式。 注意 指定的層數同時適用於「掃瞄 OLE 物件」和「在 OLE 檔案中偵測到弱點攻擊程式碼」選項。
啟動 IntelliTrap	偵測壓縮檔中是否含有 Bot 之類的惡意程式碼
對經由 Web 與電子郵件通道下載的檔案啟動 CVE 弱點攻擊掃瞄	根據常見弱點和漏洞 (CVE) 系統，封鎖會嘗試攻擊市售產品已知弱點的程序

即時掃瞄：「處理行動」標籤

程序

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

        如需詳細資訊，請參閱主動式處理行動 第 8-31 頁。
        - 自訂可能的病毒/惡意程式的處理行動：選取並指定 Security Agent 針對可能的惡意程式安全威脅採取的處理行動
      - 對所有的病毒/惡意程式類型使用相同的處理行動：指定 Security Agent 針對所有惡意程式安全威脅採取相同的處理行動
      - 對每個病毒/惡意程式類型使用特定的處理行動：指定 Security Agent 針對特定安全威脅採取的處理行動

如需詳細資訊，請參閱自訂中毒處理行動 第 8-32 頁。

b. 選取要向使用者顯示的通知類型。

- 偵測到病毒/惡意程式時顯示通知：選取此選項可在偵測到惡意程式時，顯示通知告知 Security Agent 使用者
- 偵測到可能的病毒/惡意程式時顯示通知：選取此選項可在偵測到可能的惡意程式時，顯示通知告知 Security Agent 使用者

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

建立檔案的備份複本，可供您在需要時恢復檔案的原始版本。

d. 指定隔離目錄的位置。

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

如需詳細資訊，請參閱隔離目錄 第 8-33 頁。

e. 在「損害清除及復原服務」區段中，設定下列項目：

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

> **注意**
>
> 只有對可能的病毒/惡意程式的處理行動不是「暫不處理」也不是「拒絕存取」時，才能選取該選項。

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

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

注意

在清除間諜程式/可能的資安威脅程式後，Security Agent 會備份間諜程式/可能的資安威脅程式資料，如果您認為可安全存取這些間諜程式/可能的資安威脅程式，便可恢復這些資料。

- 拒絕存取：不允許使用者開啟或複製間諜程式或可能的資安威脅程式元件
- 偵測到間諜程式/可能的資安威脅程式時，在端點上顯示通知：選取此選項可在偵測到間諜程式/可能的資安威脅程式時，顯示通知告知 Security Agent 使用者

即時掃瞄：「掃瞄例外」標籤

程序

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

      如需詳細資訊，請參閱趨勢科技產品目錄例外 第 8-38 頁。

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

   c. 輸入不掃瞄的目錄路徑，然後點選 + 按鈕。

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

注意

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

  如需詳細資訊，請參閱萬用字元例外 第 8-39 頁。

3. 在「掃瞄例外清單（檔案）」區段中，設定必要設定。
   a. 設定上層策略時，指定其他使用者設定子策略的方式。
      - 從上層策略繼承：子策略必須使用在上層策略中設定的設定
      - 從上層策略延伸：子策略可以將其他設定附加至從上層策略繼承的設定
   b. 輸入不掃瞄的檔案名稱或加上完整目錄路徑的檔案名稱，然後點選 + 按鈕。

注意

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

  如需詳細資訊，請參閱萬用字元例外 第 8-39 頁。

4. 在「掃瞄例外清單（副檔名）」區段中，設定必要設定。
   a. 設定上層策略時，指定其他使用者設定子策略的方式。
      - 從上層策略繼承：子策略必須使用在上層策略中設定的設定
      - 從上層策略延伸：子策略可以將其他設定附加至從上層策略繼承的設定
   b. 選取或輸入不掃瞄的副檔名，然後點選「新增 >」按鈕。

注意

- 您最多可以指定 256 個不掃瞄的副檔名。
- 「即時掃瞄」不支援使用萬用字元來設定副檔名例外。

立即掃瞄

「立即掃瞄」由管理員透過 Web 主控台從遠端開始，可以將一或多個 Security Agent 端點做為目標。

請設定「手動掃瞄」設定，並將其套用至一或多個 Security Agent 與網域，或套用至伺服器管理的所有 Security Agent。

進行立即掃瞄設定

程序

1. 選取下列選項：
   - 啟動病毒/惡意程式掃瞄
   - 啟動間諜程式/可能的資安威脅程式掃瞄

   注意

   必須先啟動病毒/惡意程式掃瞄，然後才能啟動間諜程式/可能的資安威脅程式掃瞄。

2. 設定「目標」設定。

   如需詳細資訊，請參閱立即掃瞄：「目標」標籤 第 8-18 頁。

3. 設定「處理行動」設定。

   如需詳細資訊，請參閱立即掃瞄：「處理行動」標籤 第 8-19 頁。

4. 設定「掃瞄例外」設定。

   如需詳細資訊，請參閱立即掃瞄：「掃瞄例外」標籤 第 8-21 頁。

立即掃瞄：「目標」標籤

程序

1. 在「要掃瞄的檔案」區段中，從下列項目中選取：

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

     注意

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

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

     注意

     設定上層策略時，指定其他使用者設定子策略的方式。

     - 從上層策略繼承：子策略必須使用在上層策略中設定的設定
     - 從上層策略延伸：子策略可以將其他設定附加至從上層策略繼承的設定

2. 在「掃瞄設定」區段中，設定必要設定。

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

3. 在「CPU 使用率」區段中，從下列項目中選取：
   - 高：掃瞄之間不暫停
   - 中：如果 CPU 耗用大於 50% 便在檔案掃瞄間暫停；如果小於 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

立即掃瞄：「處理行動」標籤

程序

1. 在「病毒/惡意程式」區段中，設定必要設定。
   a. 選取 Security Agent 在偵測到安全威脅後採取的處理行動類型。

- 使用主動式處理行動：選取此選項可使用一套預先設定的中毒處理行動，來處理病毒/惡意程式

  如需詳細資訊，請參閱主動式處理行動 第 8-31 頁。

  - 自訂可能的病毒/惡意程式的處理行動：選取並指定 Security Agent 針對可能的惡意程式安全威脅採取的處理行動

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

  如需詳細資訊，請參閱自訂中毒處理行動 第 8-32 頁。

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

   建立檔案的備份複本，可供您在需要時恢復檔案的原始版本。

c. 指定隔離目錄的位置。

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

   如需詳細資訊，請參閱隔離目錄 第 8-33 頁。

d. 在「損害清除及復原服務」區段中，設定下列項目：

   - 清除類型
     - 標準清除：Security Agent 會在標準清除期間執行下列任何處理行動：
       - 偵測並移除活動的特洛伊木馬程式
       - 終結特洛伊木馬程式所建立的處理程序
       - 修復特洛伊木馬程式修改的系統檔案

- 刪除特洛伊木馬程式遺留的檔案和應用程式
- 進階清除：除了標準清除處理行動外，Security Agent 還會遏止詐欺安全軟體（亦稱為 FakeAV）及某些 Rootkit 變體的活動。

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

注意

只有對可能的病毒/惡意程式的處理行動不是「暫不處理」也不是「拒絕存取」時，才能選取該選項。

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

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

注意

在清除間諜程式/可能的資安威脅程式後，Security Agent 會備份間諜程式/可能的資安威脅程式資料，如果您認為可安全存取這些間諜程式/可能的資安威脅程式，便可恢復這些資料。

- 暫不處理：記錄偵測事件，但允許程式執行

立即掃瞄：「掃瞄例外」標籤

程序

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

   如需詳細資訊，請參閱趨勢科技產品目錄例外 第 8-38 頁。

b. 設定上層策略時，指定其他使用者設定子策略的方式。

- 從上層策略繼承：子策略必須使用在上層策略中設定的設定
- 從上層策略延伸：子策略可以將其他設定附加至從上層策略繼承的設定

c. 輸入不掃瞄的目錄路徑，然後點選 + 按鈕。

Security Agent 不會掃瞄位於指定目錄（和子目錄）中的檔案。

注意

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

如需詳細資訊，請參閱萬用字元例外 第 8-39 頁。

3. 在「掃瞄例外清單（檔案）」區段中，設定必要設定。

a. 設定上層策略時，指定其他使用者設定子策略的方式。

- 從上層策略繼承：子策略必須使用在上層策略中設定的設定
- 從上層策略延伸：子策略可以將其他設定附加至從上層策略繼承的設定

b. 輸入不掃瞄的檔案名稱或加上完整目錄路徑的檔案名稱，然後點選 + 按鈕。

注意

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

如需詳細資訊，請參閱萬用字元例外 第 8-39 頁。

4. 在「掃瞄例外清單（副檔名）」區段中，設定必要設定。

a. 設定上層策略時，指定其他使用者設定子策略的方式。

- 從上層策略繼承：子策略必須使用在上層策略中設定的設定

- 從上層策略延伸：子策略可以將其他設定附加至從上層策略繼承的設定

b. 選取或輸入不掃瞄的副檔名，然後點選「新增 >」按鈕。

注意

- 您最多可以指定 256 個不掃瞄的副檔名。
- 若為「手動掃瞄」、「預約掃瞄」與「立即掃瞄」，請使用問號 (?)（用於取代單一字元）或星號 (*)（用於取代多個字元）做為萬用字元。例如，如果您不要掃瞄副檔名以 D 開頭的所有檔案（例如 DOC、DOT 或 DAT），請輸入 `D*` 或 `D??`。

預約掃瞄

「預約掃瞄」會在指定的日期與時間自動執行。使用「預約掃瞄」，可針對用戶端自動執行例行掃瞄，並提高掃瞄管理效率。

請設定「預約掃瞄」設定，並將其套用至一或多個用戶端與網域，或套用至伺服器管理的所有用戶端。

設定預約掃瞄設定

程序

1. 選取下列選項：
   - 啟動病毒/惡意程式掃瞄
   - 啟動間諜程式/可能的資安威脅程式掃瞄

注意

必須先啟動病毒/惡意程式掃瞄，然後才能啟動間諜程式/可能的資安威脅程式掃瞄。

2. 設定「目標」設定。

   如需詳細資訊，請參閱預約掃瞄：「目標」標籤 第 8-24 頁。

3. 設定「處理行動」設定。

   如需詳細資訊，請參閱預約掃瞄：「處理行動」標籤 第 8-26 頁。

4. 設定「掃瞄例外」設定。

   如需詳細資訊，請參閱預約掃瞄：「掃瞄例外」標籤 第 8-28 頁。

預約掃瞄：「目標」標籤

程序

1. 在「預約」區段中，指定「預約掃瞄」頻率：
   - 每日一次：每天於指定時間掃瞄一次
   - 每週一次，每 <day_of_week>：每週於指定日子的指定時間掃瞄一次
   - 每月一次，於 <number>：每月於指定日子的指定時間掃瞄一次
   - 每月一次，於 <ordinal> <day_of_week>：每月於指定工作日的指定時間掃瞄一次

重要

如果選取的日子不存在於指定的月份（例如，2 月沒有第 “30” 天），「預約掃瞄」會在該月的最後一天執行。

注意

設定上層策略時，指定其他使用者設定子策略的方式。

- 從上層策略繼承：子策略必須使用在上層策略中設定的設定
- 可自訂：其他管理員可以將子策略設定為不同於上層策略設定。

2. 在「要掃瞄的檔案」區段中，從下列項目中選取：

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

     注意

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

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

     注意

     設定上層策略時，指定其他使用者設定子策略的方式。

     - 從上層策略繼承：子策略必須使用在上層策略中設定的設定
     - 從上層策略延伸：子策略可以將其他設定附加至從上層策略繼承的設定

3. 在「掃瞄設定」區段中，設定必要設定。

設定	說明
掃瞄壓縮檔	掃瞄封存檔中指定的壓縮層數 **注意** 掃瞄更多層有可能偵測到深藏在壓縮封存檔中的惡意程式，但這麼做可能影響系統效能。

設定	說明
掃瞄 OLE 物件	掃瞄檔案中指定的「物件連結與嵌入」(OLE) 層數 在 OLE 檔案中偵測到弱點攻擊程式碼：OLE 弱點攻擊偵測會檢查 Microsoft Office 檔案中是否有弱點攻擊程式碼，主動識別惡意程式。 注意 指定的層數同時適用於「掃瞄 OLE 物件」和「在 OLE 檔案中偵測到弱點攻擊程式碼」選項。
掃瞄開機區	掃瞄端點上硬碟的開機磁區是否有病毒/惡意程式

4. 在「CPU 使用率」區段中，從下列項目中選取：
   - 高：掃瞄之間不暫停
   - 中：如果 CPU 耗用大於 50% 便在檔案掃瞄間暫停；如果小於 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

預約掃瞄：「處理行動」標籤

程序

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

        如需詳細資訊，請參閱主動式處理行動 第 8-31 頁。
      - 自訂可能的病毒/惡意程式的處理行動：選取並指定 Security Agent 針對可能的惡意程式安全威脅採取的處理行動

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

  如需詳細資訊，請參閱自訂中毒處理行動 第 8-32 頁。

b. 選取要向使用者顯示的通知類型。

- 偵測到病毒/惡意程式時顯示通知：選取此選項可在偵測到惡意程式時，顯示通知告知 Security Agent 使用者
- 偵測到可能的病毒/惡意程式時顯示通知：選取此選項可在偵測到可能的惡意程式時，顯示通知告知 Security Agent 使用者

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

建立檔案的備份複本，可供您在需要時恢復檔案的原始版本。

d. 指定隔離目錄的位置。

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

如需詳細資訊，請參閱隔離目錄 第 8-33 頁。

e. 在「損害清除及復原服務」區段中，設定下列項目：

- 清除類型
  - 標準清除：Security Agent 會在標準清除期間執行下列任何處理行動：
    - 偵測並移除活動的特洛伊木馬程式
    - 終結特洛伊木馬程式所建立的處理程序
    - 修復特洛伊木馬程式修改的系統檔案

- 刪除特洛伊木馬程式遺留的檔案和應用程式

- 進階清除：除了標準清除處理行動外，Security Agent 還會遏止詐欺安全軟體（亦稱為 FakeAV）及某些 Rootkit 變體的活動。

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

注意

只有對可能的病毒/惡意程式的處理行動不是「暫不處理」也不是「拒絕存取」時，才能選取該選項。

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

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

注意

在清除間諜程式/可能的資安威脅程式後，Security Agent 會備份間諜程式/可能的資安威脅程式資料，如果您認為可安全存取這些間諜程式/可能的資安威脅程式，便可恢復這些資料。

- 暫不處理：記錄偵測事件，但允許程式執行

- 偵測到間諜程式/可能的資安威脅程式時，在端點上顯示通知：選取此選項可在偵測到間諜程式/可能的資安威脅程式時，顯示通知告知 Security Agent 使用者

預約掃瞄：「掃瞄例外」標籤

程序

1. 選取「啟動掃瞄例外」。

2. 在「掃瞄例外清單（目錄）」區段中，設定必要設定。

   a. 選取「不掃瞄趨勢科技產品的安裝目錄」可自動排除與其他趨勢科技產品相關聯的目錄。

      如需詳細資訊，請參閱趨勢科技產品目錄例外 第 8-38 頁。

   b. 設定上層策略時，指定其他使用者設定子策略的方式。

      - 從上層策略繼承：子策略必須使用在上層策略中設定的設定
      - 從上層策略延伸：子策略可以將其他設定附加至從上層策略繼承的設定

   c. 輸入不掃瞄的目錄路徑，然後點選 + 按鈕。

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

      注意

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

        如需詳細資訊，請參閱萬用字元例外 第 8-39 頁。

3. 在「掃瞄例外清單（檔案）」區段中，設定必要設定。

   a. 設定上層策略時，指定其他使用者設定子策略的方式。

      - 從上層策略繼承：子策略必須使用在上層策略中設定的設定
      - 從上層策略延伸：子策略可以將其他設定附加至從上層策略繼承的設定

   b. 輸入不掃瞄的檔案名稱或加上完整目錄路徑的檔案名稱，然後點選 + 按鈕。

      注意

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

        如需詳細資訊，請參閱萬用字元例外 第 8-39 頁。

4. 在「掃瞄例外清單（副檔名）」區段中，設定必要設定。

   a. 設定上層策略時，指定其他使用者設定子策略的方式。

      - 從上層策略繼承：子策略必須使用在上層策略中設定的設定
      - 從上層策略延伸：子策略可以將其他設定附加至從上層策略繼承的設定

   b. 選取或輸入不掃瞄的副檔名，然後點選「新增 >」按鈕。

      注意

      - 您最多可以指定 256 個不掃瞄的副檔名。
      - 若為「手動掃瞄」、「預約掃瞄」與「立即掃瞄」，請使用問號 (?)（用於取代單一字元）或星號 (*)（用於取代多個字元）做為萬用字元。例如，如果您不要掃瞄副檔名以 D 開頭的所有檔案（例如 DOC、DOT 或 DAT），請輸入 `D*` 或 `D??`。

中毒處理行動

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

重要

某些檔案無法清除。

如需詳細資訊，請參閱：

- 主動式處理行動 第 8-31 頁
- 自訂中毒處理行動 第 8-32 頁
- 無法清除病毒的檔案 第 8-35 頁

主動式處理行動

不同類型的病毒/惡意程式需要不同的中毒處理行動。自訂中毒處理行動需要有病毒/惡意程式的知識，並且可能會是冗長而乏味的工作。Security Agent 使用「主動式處理行動」來因應這些問題。

「主動式處理行動」是一套預先設定的中毒處理行動，可以處理病毒/惡意程式。如果您不熟悉中毒處理行動，或是不確定何種中毒處理行動適合那一種特定的病毒/惡意程式，趨勢科技建議您使用「主動式處理行動」。

使用「主動式處理行動」具有以下優點：

- 「主動式處理行動」會使用趨勢科技建議的中毒處理行動。您不需要耗費時間來設定中毒處理行動。
- 病毒撰寫者會不斷變更病毒/惡意程式攻擊端點的方式。更新「主動式處理行動」設定以抵禦最新威脅和最新的病毒/惡意程式攻擊方法。

下表說明「主動式處理行動」處理每種類型病毒/惡意程式的方式。

表 8-2. 趨勢科技建議的病毒/惡意程式中毒處理行動

病毒/惡意程式類型	即時掃瞄		手動掃瞄/預約掃瞄	
	第一個中毒處理行動	第二個中毒處理行動	第一個中毒處理行動	第二個中毒處理行動
CVE 弱點攻擊	通過	無	無	無
惡作劇	隔離	無	隔離	無
特洛伊木馬程式	隔離	無	隔離	無
病毒	清除	隔離	清除	隔離
測試病毒	拒絕存取	無	暫不處理	無
封裝程式	隔離	無	隔離	無
其他	清除	隔離	清除	隔離

病毒/惡意程式類型	即時掃瞄		手動掃瞄/預約掃瞄	
	第一個中毒處理行動	第二個中毒處理行動	第一個中毒處理行動	第二個中毒處理行動
可能的惡意程式	拒絕存取或使用者設定的處理行動	無	暫不處理或使用者設定的處理行動	無

注意

- 對於可能的病毒/惡意程式，即時掃瞄期間的預設中毒處理行動是「拒絕存取」，而手動掃瞄和預約掃瞄期間的預設中毒處理行動是「暫不處理」。如果這些不是您的偏好處理行動，可以將其變更為「隔離」、「刪除」或「重新命名」。
- 有些檔案無法清除。
- 進行間諜程式/可能的資安威脅程式掃瞄時，無法使用主動式處理行動。

自訂中毒處理行動

處理行動	說明
刪除	刪除中毒檔案。
隔離	重新命名中毒檔案，然後將其移至端點上的暫時隔離目錄。 Security Agent 會將已隔離的檔案傳送到指定的隔離目錄（預設位於管理伺服器上）。 Security Agent 會將傳送至此目錄的隔離檔案加密。 如需詳細資訊，請參閱隔離目錄 第 8-33 頁。

處理行動	說明
清除	先清除中毒檔案，才允許完整存取該檔案。 如果無法清除檔案，Security Agent 會執行第二個中毒處理行動，可能是下列其中一個中毒處理行動：「隔離」、「刪除」、「重新命名」與「暫不處理」。 系統可對所有類型的安全威脅（但不包括可能的病毒/惡意程式）執行此中毒處理行動。 注意 某些檔案無法清除。如需詳細資訊，請參閱無法清除病毒的檔案 第 8-35 頁。
重新命名	將中毒檔案的副檔名變更為 `vir`。使用者一開始無法開啟重新命名的檔案，但是如果使檔案與特定的應用程式產生關聯，就可以開啟該檔案。 開啟重新命名的中毒檔案時，可能會執行病毒/惡意程式。
通過	不對偵測到的安全威脅執行任何處理行動，但是在記錄檔中記錄偵測到的安全威脅。
拒絕存取	當 Security Agent 偵測到嘗試開啟或執行中毒檔案時，會立即阻止該操作。 使用者可以手動刪除中毒的檔案。

隔離目錄

如果針對中毒檔案的處理行動為「隔離」，則 Security Agent 會加密該檔案，並將其移至 <用戶端安裝資料夾>\SUSPECT 下的暫時隔離資料夾，然後將檔案傳送至指定的隔離目錄。

注意

您可以在日後需要存取加密的隔離檔案時加以恢復。

接受位於 Apex One server 電腦上的預設隔離目錄。此目錄採用 URL 格式，並且包含伺服器的主機名稱或 IP 位址。

- 如果伺服器同時管理 IPv4 和 IPv6 用戶端，請使用主機名稱，以便所有 Security Agent 都可以將隔離檔案傳送到伺服器。
- 如果伺服器只具有 IPv4 位址，或只透過其 IPv4 位址進行識別，則只有純 IPv4 和雙堆疊 Security Agent 可以將隔離檔案傳送到伺服器。
- 如果伺服器只具有 IPv6 位址，或只透過其 IPv6 位址進行識別，則只有純 IPv6 和雙堆疊 Security Agent 可以將隔離檔案傳送到伺服器。

您也可以輸入 URL、UNC 路徑或絕對檔案路徑格式的位置來指定替代的隔離目錄。Security Agent 應該可以連線到此替代目錄。例如，如果替代目錄將接收來自雙堆疊和純 IPv6 Security Agent 的隔離檔案，此目錄應具有 IPv6 位址。Trend Micro 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 8-3. 隔離目錄

隔離目錄	接受的格式	範例	注意
管理伺服器電腦上的目錄	URL	`http://<osceserver>`	這是預設的目錄。 進行此目錄的設定，如隔離資料夾的大小等。
	UNC 路徑	`\\<osceserver>\ofcscan\Virus`	
其他 Apex One server 電腦上的目錄（若您在網路上有其他 Apex One server）	URL	`http://<osceserver2>`	確定 Security Agent 可連線到此目錄。如果您指定不正確的目錄，Security Agent 會將隔離的檔案保留在 SUSPECT 資料夾中，直到指定正確的隔離目錄為止。在伺服器的病毒/惡意程式記錄檔中，掃瞄結果為「無法將隔離檔案傳送到指定的隔離資料夾」。 如果您使用 UNC 路徑，請確定是否可讓「Everyone」群組共享隔離目錄資料夾，並指定讀取和寫入權限給這個群組。
	UNC 路徑	`\\<osceserver2>\ofcscan\Virus`	
網路上的其他端點	UNC 路徑	`\\<computer_name>\temp`	
Security Agent 上的其他目錄	絕對路徑	`C:\temp`	

無法清除病毒的檔案

「病毒掃瞄引擎」無法清除下列檔案：

表 8-4. 無法清除的檔案解決方案

無法清除的檔案	說明和解決方案
感染特洛伊木馬程式的檔案	特洛伊木馬程式是一種會執行無法預期或未經授權（惡意）動作的程式，例如：顯示訊息、刪除檔案、或將磁碟格式化。特洛伊木馬程式不會感染檔案，因此不需要清除。 解決方案：「損害清除及復原引擎」和「損害清除及復原範本」會移除特洛伊木馬程式。
感染蠕蟲的檔案	蠕蟲是一種自含程式（或一組程式集），可將本身的功能或程式碼的一部分散佈到其他端點系統。這種病毒通常透過網路連線或電子郵件的附件散播。由於蠕蟲是自含程式，因此無法清除。 解決方案：Trend Micro 建議您刪除蠕蟲。
防寫的中毒檔案	解決方案：移除防寫，以允許清除檔案。
密碼保護的檔案	受密碼保護的檔案，包括受密碼保護的壓縮檔或受密碼保護的 Microsoft Office 檔案。 解決方案：移除密碼保護，以允許清除檔案。
備份檔案	副檔名為 RB0~RB9 的檔案是中毒檔案的備份副本。清除程序會建立中毒檔案的備份，以防病毒/惡意程式在清除期間損害檔案。 解決方案：如果成功清除中毒檔案，您便不需要保留其備份複本。如果端點運作正常，就可以將備份檔案刪除。
資源回收筒內的中毒檔案	因為系統正在執行，所以系統可能不允許移除「資源回收筒」內的中毒檔案。
	1. 以管理員權限登入端點。 2. 關閉所有執行中的應用程式，防止應用程式鎖定檔案而使 Windows 無法刪除該檔案。 3. 開啟命令提示字元。 4. 輸入下列指令以刪除檔案： `del /s \$Recycle.Bin\*`

無法清除的檔案	說明和解決方案
	5. 檢查檔案是否已移除。
Windows Temp 資料夾或 Internet Explorer 暫存資料夾內的中毒檔案	因為端點會使用 Windows Temp 資料夾或 Internet Explorer 暫存資料夾中的中毒檔案，所以系統不允許清除這些檔案。要清除的檔案可能是 Windows 作業所需的暫存檔。

	1. 以管理員權限登入端點。
	2. 關閉所有執行中的應用程式，防止應用程式鎖定檔案而使 Windows 無法刪除該檔案。
	3. 如果中毒檔案位於 Windows Temp 資料夾中：
	a. 開啟命令提示字元。
	b. 輸入下列指令以刪除檔案：
	`del /s \Windows\Temp\*`
	c. 在標準模式下重新啟動端點。
	4. 如果中毒檔案位於 Internet Explorer 暫存資料夾中：
	a. 開啟命令提示字元並移至 Internet Explorer Temp 資料夾。
	• Windows 7：`%LocalAppData%\Microsoft\Windows\Temporary Internet Files`
	• Windows 8/8.1：`%LocalAppData%\Microsoft\Windows\INetCache`
	• Windows 10：`%LocalAppData%\Microsoft\Windows\INetCache\IE`
	b. 輸入下列指令以刪除檔案：
	`del /s .\*`
	最後一個指令會刪除 Internet Explorer 暫存資料夾中所有的檔案。
	c. 在標準模式下重新啟動端點。

使用不支援的壓縮格式壓縮的檔案。	解決方案：解壓縮檔案。

無法清除的檔案	說明和解決方案
鎖住的檔案，或是目前正在執行的檔案。	解決方案：解除鎖定檔案或等候檔案執行完畢。
毀損的檔案。	解決方案：刪除檔案。

感染特洛伊木馬程式的檔案

特洛伊木馬程式是一種會執行無法預期或未經授權（通常為惡意性質）動作（例如：顯示訊息、刪除檔案、或將磁碟格式化）的程式。特洛伊木馬程式不會感染檔案，因此沒有必要清除。

解決方案：Security Agent 會使用「損害清除及復原引擎」和「損害清除及復原範本」移除特洛伊木馬程式。

感染蠕蟲的檔案

蠕蟲是一種自含程式（或程式集），可以將本身具有功能性的複製體或其片段散佈到其他端點系統。這種病毒通常透過網路連線或電子郵件的附件散播。因為檔案屬於自含程式，所以無法清除蠕蟲。

解決方案：Trend Micro 建議刪除蠕蟲。

防寫的中毒檔案

解決方案：移除防寫，讓 Security Agent 清除檔案。

受密碼保護的檔案

包括受密碼保護的壓縮檔或受密碼保護的 Microsoft Office 檔案。

解決方案：移除密碼安全防護，以允許 Security Agent 清除這些檔案。

備份檔案

副檔名為 RB0~RB9 的檔案是中毒檔案的備份副本。Security Agent 會建立中毒檔案的備份，以防病毒/惡意程式在清除期間損害檔案。

解決方案：如果 Security Agent 成功清除中毒檔案，您便不需要保留備份複本。如果端點運作正常，就可以將備份檔案刪除。

掃瞄例外支援

在將目錄和檔案名稱從惡意程式防護掃瞄中排除時，請參閱下列支援資訊：

- 趨勢科技產品目錄例外 第 8-38 頁
- 萬用字元例外 第 8-39 頁

趨勢科技產品目錄例外

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

- <伺服器安裝資料夾>
- IM 安全性
- InterScan eManager 3.5x
- InterScan Web Security Suite
- InterScan Web Protect
- InterScan FTP VirusWall
- InterScan Web VirusWall
- InterScan NSAPI Plug-in
- InterScan E-mail VirusWall

- ScanMail eManager™ 3.11、5.1、5.11、5.12
- ScanMail for Lotus Notes™ eManager NT
- ScanMail™ for Microsoft Exchange

萬用字元例外

檔案和目錄的掃瞄例外清單支援使用萬用字元。使用「?」字元取代一個字元，使用「*」取代多個字元。

請謹慎使用萬用字元。用錯字元可能會排除不適當的檔案或目錄。例如，新增 C:* 至「掃瞄例外清單 (檔案)」將會不掃瞄整個 C:\ 磁碟機。

表 8-5. 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:\ 目錄中的所有 .txt 檔案	C:\ 目錄中的所有其他檔案類型
[]	不支援	不支援

第 9 章

網頁信譽評等策略設定

本節說明如何在 Security Agent 中設定網頁信譽評等策略。

包含下列主題：

- 網頁信譽評等 第 9-2 頁
- 設定網頁信譽評等策略 第 9-2 頁

網頁信譽評等

網頁信譽評等技術會依據諸如網站的存在時間長短、位置變更記錄，以及透過惡意程式行為分析所發現的可疑活動指標等因素來指定信譽評等評分，以追蹤 Web 網域的可信度。趨勢科技會持續分析網站並更新網頁信譽評等評分，以防止使用者存取潛在的惡意內容。

當使用者嘗試存取某個網站時，Security Agent 會查詢主動雲端截毒技術來源，以判斷網站內容的風險等級。Security Agent 中設定好的「網頁信譽評等」策略會決定是否允許使用者存取網站。

「網頁信譽評等」允許您將您認為安全或危險的網站新增到核可清單或封鎖清單。對於已新增到這些清單中的網站，Security Agent 不會查詢其網頁信譽評等評分，而是自動允許或封鎖存取。

設定網頁信譽評等策略

如果您已經設定 Proxy 伺服器來處理組織中的 HTTP 通訊，而且必須經過驗證才能存取 Web，請指定 Proxy 伺服器驗證憑證。

程序

1. 請點選「外部用戶端」標籤以設定外部用戶端的策略，或請點選「內部用戶端」標籤以設定內部用戶端的策略。
2. 在「請在下列作業系統啟動網頁信譽評等」下方，選取要保護的 Windows 平台類型（「Windows 桌上型電腦平台」和「Windows Server 平台」）。

   秘訣

   如果您已經使用含有網頁信譽評等功能的 Trend Micro 產品（例如 InterScan Web Security Virtual Appliance），Trend Micro 建議您對內部用戶端關閉網頁信譽評等。

3. 選取「啟動評估模式」。

注意

處於評估模式時，Security Agent 會允許存取所有網站。如果存取的任何網站違反所設定的「安全層級」設定，Security Agent 會記錄此事件。評估模式可讓您監控網站存取，以便在主動封鎖使用者存取之前評估網站的安全性。在您評估存取記錄檔之後，您可以將信任的網站新增到「核可的 URL 清單」中，然後再關閉評估模式。

4. 選取「檢查 HTTPS URL」。

重要

HTTPS URL 掃瞄也支援 HTTP/2 通訊協定。您必須針對不同的瀏覽器設定某些必要設定，網頁信譽評等才能檢查 HTTPS 或 HTTP/2 URL。

如需詳細資訊，請參閱 HTTPS URL 掃瞄支援 第 9-6 頁。

5. 選取「只掃瞄通用 HTTP 通訊埠」以限制網頁信譽評等僅掃瞄通過通訊埠 80、81 和 8080 的流量。依預設，網頁信譽評等會掃瞄通過全部通訊埠的所有流量。

注意

在 Windows 7、8、8.1、10 或 Windows Server 2008 R2、2012 或更新版本的平台上不受支援。

6. 請針對內部 Security Agent 選取「傳送查詢至主動雲端截毒技術伺服器」（如果您希望 Security Agent 將網頁信譽評等查詢傳送至主動雲端截毒技術伺服器）。

   - 如果您啟動此選項：
     - 用戶端會參考主動雲端截毒技術伺服器來源清單，判斷應該將查詢傳送至哪些主動雲端截毒技術伺服器。
     - 請確定主動雲端截毒技術伺服器呈運行狀態。如果主動雲端截毒技術伺服器全都無法使用，用戶端便不會將查詢傳送至主動雲端截毒技術。其餘的用戶端網頁信譽評等資料來源為核可和封鎖的 URL 清單。
     - 用戶端不會封鎖未測試的網站。主動雲端截毒技術伺服器不會儲存這些網站的網頁信譽評等資料。

- 如果您關閉此選項：
  - 用戶端會將網頁信譽評等查詢傳送至主動雲端截毒技術。端點必須連線至 Internet 才能成功傳送查詢。
  - 如果您選取「封鎖尚未經由趨勢科技測試的網頁」選項，用戶端會封鎖未測試網站。

注意

您只能將內部的內部部署 Security Agent 設定為將網頁信譽評等查詢傳送至本機的主動雲端截毒技術伺服器。

7. 選取可用的網頁信譽評等安全層級：「高」、「中」或「低」

注意

安全層級決定網頁信譽評等會允許還是封鎖對 URL 的存取。例如，如果您將安全層級設定為「低」，網頁信譽評等只會封鎖已知為網路安全威脅的 URL。設定較高的安全層級可提高網路安全威脅偵測率，但誤判的可能性也會提高。

8. 如果您關閉了「傳送查詢至主動雲端截毒技術伺服器」選項，您可以選取「封鎖尚未經由趨勢科技測試的網頁」。

注意

雖然 Trend Micro 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。

9. 選取「封鎖包含惡意程式檔的網頁」以識別網路瀏覽器弱點攻擊和惡意程式檔，並避免使用這些威脅入侵網路瀏覽器。

   網頁信譽評等同時利用瀏覽器弱點攻擊防護特徵碼和程式檔分析器病毒碼，在系統受到入侵之前識別並封鎖網頁。

重要

- 「瀏覽器弱點攻擊防護」功能僅在 Internet Explorer 7.0 及更新版本中受支援。
- 瀏覽器弱點攻擊防護功能需要您啟動「進階防護服務」。

10. 設定核可和封鎖的清單。

注意

核可清單優先於封鎖的清單。當 URL 與核可清單中的項目相符時，用戶端會一律允許存取該 URL，即使該 URL 列在封鎖清單中也一樣。

a. 選取「啟動核可/封鎖清單」。

b. 輸入 URL。

您可在 URL 中的任何位置加入萬用字元 (*)。

例如：

- 輸入 `www.trendmicro.com/*` 表示網頁信譽評等核可 Trend Micro 網站中的所有網頁。
- 輸入 `*.trendmicro.com/*` 表示網頁信譽評等核可 `trendmicro.com` 的任何子網域中的所有網頁。

您可以輸入包含 IP 位址的 URL。如果 URL 包含 IPv6 位址，請使用括號將位址括起來。

c. 請點選「新增到核可清單」或「新增到封鎖清單」。

重要

網頁信譽評等不會對核可及封鎖清單中的位址執行任何掃瞄。

11. 如果要送出網頁信譽評等的意見反應，請點選「重新評估 URL」下提供的 URL。系統會在瀏覽器視窗中開啟趨勢科技網頁信譽評等查詢系統。

12. 選取是否允許 Security Agent 將網頁信譽評等記錄檔傳送至伺服器。如果您想分析網頁信譽評等封鎖的 URL，並針對您認為可以安全存取的 URL 採取合適的處理行動，請允許用戶端傳送記錄檔。

HTTPS URL 掃瞄支援

HTTPS 通訊使用憑證來識別 Web 伺服器。它會將資料加密以防止盜取及竊聽。雖然使用 HTTPS 存取網站的安全性較高，但仍存在風險。即使網站具有有效的憑證，一旦遭到入侵，便會裝載惡意程式並竊取個人資訊。此外，由於憑證相當容易取得，很輕易就能架設使用 HTTPS 的惡意 Web 伺服器。

重要

Internet Explorer 的 HTTPS 掃瞄僅支援以桌面模式運作的 Windows 8、Windows 8.1 或 Windows 2012 平台。

啟動 HTTPS URL 檢查，以減少接觸雖使用 HTTPS 卻已遭到入侵或惡意的網站。網頁信譽評等可以監控下列瀏覽器上的 HTTPS 流量：

表 9-1. 支援 HTTPS 流量的瀏覽器

瀏覽器	版本	先決條件
Microsoft Internet Explorer	8.x	最新版本
	9.x	使用者必須在瀏覽器快顯視窗中啟動 `Trend Micro Osprey Plugin Class` 附加元件。
	10.x	
	11.x	
Mozilla Firefox	3.5 或更新版本	無
Chrome	最新版本	
Microsoft Edge	最新版本	

如需有關針對網頁信譽評等設定 Internet Explorer 設定的詳細資訊，請參閱下列常見問題集文章：

- http://esupport.trendmicro.com/solution/zh-tw/1060643.aspx
- http://esupport.trendmicro.com/solution/zh-tw/1095350.aspx

第 10 章

未知安全威脅防護

本節說明如何設定 Security Agent 來偵測及防禦先前未識別、已知或不常見的安全威脅。

包含下列主題：

- Machine Learning 第 10-2 頁
- 設定樣本提交設定 第 10-4 頁
- 設定可疑連線設定 第 10-5 頁

Machine Learning

趨勢科技 Machine Learning 採用進階機器學習技術來關聯安全威脅資訊，並執行深度檔案分析來偵測新興的未知安全威脅，這透過數位 DNA 指紋、API 對應和其他檔案特徵來實現。Machine Learning 還會對未知或不太普遍的處理程序執行行為分析，以確定是否有新興或未知安全威脅正企圖讓您的網路中毒。

Machine Learning 是一個功能強大的工具，可協助保護您的環境，使其免遭不明安全威脅和零時差攻擊。

偵測類型	說明
檔案	Security Agent 在偵測到未知或不常見的檔案之後，會使用進階安全威脅掃瞄引擎 (ATSE) 掃瞄該檔案，以便擷取檔案特徵，然後將報告傳送給裝載於趨勢科技主動式雲端截毒技術上的 Machine Learning 引擎。透過使用惡意程式模擬，Machine Learning 將範例與惡意程式模型進行比較、指定概率分數，並確定檔案可能包含的惡意程式類型。 如果正常運作的 Internet 連線無法使用，Machine Learning 會自動切換至本機模式來提供不間斷的未知安全威脅防護，以抵禦可攜式可執行檔安全威脅。 視您對 Machine Learning 進行的設定而定，Security Agent 可能會嘗試「隔離」受影響的檔案，以防安全威脅繼續擴散到您的整個網路。

偵測類型	說明
處理程序	Security Agent 在偵測到未知或不常見的程序之後，會使用關聯式智慧型引擎監控該程序，然後將行為報告傳送給 Machine Learning 引擎。透過使用行為惡意程式塑型，Machine Learning 將處理程序行為與模型進行比較、指定概率分數，並確定處理程序可能正在執行的惡意程式類型。 程序偵測也會監控程式檔執行。如果關聯式智慧型引擎偵測到可疑程式檔執行，Machine Learning 會採取設定的處理行動。 Machine Learning 會對下列類型的程式檔執行程式檔封鎖： • cscript • jar • powershell • vbs • wscript 視您對 Machine Learning 進行的設定而定，Security Agent 可能會「終止」受影響的程序或程式檔，然後嘗試清除執行該程序或程式檔的檔案。

設定 Machine Learning 設定

注意

若要使用「Machine Learning」，您必須啟動下列服務：

- 未經授權的變更阻止
- 進階防護服務

程序

1. 選取「啟動 Machine Learning」。
2. 在「偵測設定」下，選取偵測的類型以及「Machine Learning」採取的相關處理行動。

偵測類型	處理行動
檔案	• 隔離： 選取此項，即會自動依「Machine Learning」分析結果，將展現惡意程式相關特徵的檔案隔離 • 僅記錄檔： 選取此項，即會掃瞄未知檔案並記錄「Machine Learning」分析結果，以供內部進一步調查安全威脅
處理程序	• 終止：選取此項，即會自動依「Machine Learning」分析結果，將展現惡意程式相關行為的程序或程式檔終止 重要 「Machine Learning」會嘗試將已執行惡意程序或程式檔的檔案清除。如果清除處理行動不成功，Machine Learning 會將受影響的檔案隔離。 • 僅記錄檔：選取此項，即會掃瞄未知程序或程式檔並記錄「Machine Learning」分析結果，以供內部進一步調查安全威脅

3. 在「例外」下，設定全域的「Machine Learning」檔案例外，以防止所有用戶端將某個檔案偵測為惡意檔案。

   a. 請點選「新增檔案雜湊」。

      會出現「將檔案新增到例外清單」畫面。

   b. 指定要從掃瞄中排除的檔案 SHA-1 雜湊值。

   c. （選擇性）提供附註來解釋當成例外的原因，或是說明與雜湊值相關聯的檔案名稱。

   d. 按一下「新增」。

      Machine Learning 便會將檔案雜湊新增到「例外」清單。

設定樣本提交設定

您可以將 Security Agent 設定為在發現檔案物件可能包含先前未曾識別出的安全威脅時，將檔案物件提交給沙盒虛擬平台做進一步分析。沙盒虛擬平台在評估

物件之後，如果發現物件包含未知的安全威脅，就會將物件新增至沙盒虛擬平台的可疑物件清單，然後將清單分發給整個網路中的其他 Security Agent。

可疑檔案包括下列任何項目：

- 未經趨勢科技判定的程式（經由支援的 Web 瀏覽器或電子郵件通道下載）
- 啟發式引擎偵測到的可疑程序（經由支援的 Web 瀏覽器或電子郵件通道下載）
- 卸除式儲存裝置中較少見的自動執行程式

重要

Security Agent 可以提交變更的樣本檔大小，視您使用的沙盒虛擬平台的類型而定。如果使用的是 Deep Discovery Analyzer 伺服器，樣本檔的大小可達 50 MB。如果使用的是 Deep Discovery Analyzer as a Service 附加元件，樣本檔的大小可達 60 MB。

程序

1. 選取「啟動將可疑檔案提交到沙盒虛擬平台」。

設定可疑連線設定

Security Agent 可以記錄並封鎖端點與全域 C&C IP 清單中的位址之間建立的所有連線。您還可以記錄（同時也可存取）使用者定義的封鎖 IP 清單中設定的 IP 位址。

Security Agent 也可以監控可能由僵屍網路或其他惡意程式威脅產生的連線。偵測到惡意程式威脅後，Security Agent 可嘗試清除感染。

程序

1. 啟動「偵測對全域 C&C IP 清單中的位址進行的網路連線」設定，來監控對趨勢科技已確認之 C&C 伺服器進行的連線，然後選取「僅記錄」或「封鎖」連線。

- 如果要允許用戶端連線到使用者定義的封鎖 IP 清單中的位址，請啟動「記錄並允許存取使用者定義的封鎖 IP 清單位址」設定。

注意

您必須先啟動網路連線記錄，然後 Security Agent 才能允許存取使用者定義的封鎖 IP 清單中的位址。

2. 啟動「使用惡意程式網路特徵鑑別來偵測連線」設定，然後選取「僅記錄」或「封鎖」連線。

- 如果要允許 Security Agent 嘗試清除與 C&C 伺服器建立的連線，請啟動「偵測到 C&C 回呼時清除可疑連線」設定。Security Agent 會使用 GeneriClean 清除惡意程式威脅，並終止與 C&C 伺服器的連線。

注意

您必須先啟動「使用惡意程式網路特徵鑑別的記錄檔連線」，Security Agent 才能嘗試清除與封包結構比對偵測到的 C&C 伺服器之間建立的連線。

第 11 章

周邊設備存取控管策略設定

本節說明如何在 Security Agent 中設定周邊設備存取控管策略。

包含下列主題：

- 周邊設備存取控管 第 11-2 頁
- 設定周邊設備存取控管設定 第 11-2 頁

周邊設備存取控管

周邊設備存取控管會規範對連線到電腦的外部儲存裝置與網路資源的存取。周邊設備存取控管有助於防止資料遺失與外洩，並且可與檔案掃瞄搭配使用，以協助防禦安全威脅。

您可以設定內部和外部用戶端的周邊設備存取控管策略。管理員通常會針對外部用戶端設定較嚴格的策略。

Apex Central as a Service 同時提供端點型和使用者型周邊設備存取控管策略組態設定。

設定周邊設備存取控管設定

程序

1. 選取「啟動周邊設備存取控管」。
   - 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。
2. 新增或編輯周邊設備存取控管規則：
   - 對於使用者型規則：
     - 如果要建立以 Active Directory 使用者或群組帳號為基礎的規則，請點選「新增」。
     - 如果要編輯以 Active Directory 使用者或群組帳號為基礎的規則，請點選「使用者帳號」欄中的連結。

重要

必須將 Active Directory 與 Apex Central as a Service 整合，使用者型周邊設備存取控管規則才可供使用。

- 如果要編輯預設的端點型規則，請執行下列步驟：
  - 請點選「使用者帳號」欄中的「所有使用者（預設值）」連結。

    注意

    您無法刪除預設的端點型規則。

會出現「周邊設備存取控管規則」畫面。

3. 在「使用者帳號」區段中，輸入並選取要套用規則的 Active Directory 使用者或群組帳號。

   注意

   在編輯預設的「所有使用者（預設值）」端點型規則時，您無法指定使用者或組群帳號。

4. 在「儲存裝置」區段中：

   a. 為每個儲存裝置選取權限。

      重要

      - 只有已啟動「資料安全防護」的 Security Agent 可執行「封鎖」處理行動。如果您將策略部署至尚未啟動「資料安全防護」的 Security Agent，則 Apex One 會套用下拉式方塊中設定的處理行動。
      - Apex One 會自動套用在「允許的 USB 清單」中為任何 USB 裝置設定的存取權限，即使未啟動「資料安全防護」也一樣。

      如需有關權限的詳細資訊，請參閱裝置的權限 第 11-5 頁。

      如果您選擇限制任何儲存裝置的存取權，將會出現「允許的程式」按鈕。對於「USB 儲存裝置」，如果您選取了「封鎖（資料安全防護）」，將會出現「允許的 USB 裝置」按鈕。

   b. （選用）請點選「允許的程式」來設定周邊設備存取控管不會對任何裝置類型限制存取權的程式清單。

      會出現「允許的程式」畫面。

i. 輸入周邊設備存取控管允許使用者存取之程式的完整路徑或受信任的數位簽章提供者資訊。

注意

- 如果指定數位簽章提供者，周邊設備存取控管只會允許由發行者簽署的程式「執行」。

  如需詳細資訊，請參閱指定數位簽章提供者 第 11-8 頁。

- 如果指定程式的完整路徑，周邊設備存取控管允許的程式清單支援使用萬用字元。

  如需詳細資訊，請參閱周邊設備存取控管允許的程式清單的萬用字元支援 第 11-7 頁。

---

ii. 請點選「新增」。

程式的完整路徑或受信任的數位簽章提供者資訊會顯示在清單中。

iii. 選取允許程式「執行」還是「讀取/寫入」。

iv. 請點選「確定」。

c. （選用）請點選「允許的 USB 裝置」來設定周邊設備存取控管不會將其封鎖的 USB 裝置清單。

會出現「允許的 USB 裝置」畫面。

i. 在清單中輸入裝置廠商、型號和序號 ID。

ii. 如果要新增更多裝置，請點選加號 (+) 圖示。

iii. 在「權限」下拉式清單中，指定周邊設備存取控管允許使用者存取指定 USB 裝置的存取權層級。

iv. 請點選「確定」。

d. 選取「封鎖 USB 儲存裝置的自動執行功能」以防止儲存在 USB 裝置中的程式自動執行。

e. 選取「當 Apex One 偵測到未經授權的裝置存取時，會在端點上顯示通知訊息」以在周邊設備存取控管限制存取裝置時通知使用者。

5. 對於已安裝資料安全防護功能的 Security Agent，請選取「允許」或「封鎖」存取「行動裝置」和「非儲存裝置」下方所列的裝置。

6. 請點選「確定」。

注意

周邊設備存取控管會自動向所有使用者型規則指派高於預設端點型規則的優先順序（「所有使用者（預設值）」）。

7. （選用）管理周邊設備存取控管規則清單。

   - 優先順序：請點選箭頭以變更使用者型規則的優先順序。
   - 複製：選取規則，點選「複製」，然後修改規則內容。
   - 刪除：選取規則，然後點選「刪除」以從清單永久移除規則。

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 11-1. 儲存裝置的周邊設備存取控管權限

權限	裝置上的檔案	輸入的檔案
完整存取權	允許的作業：複製、移動、開啟、儲存、刪除、執行	允許的作業：儲存、移動、複製 這表示檔案可以儲存、移動與複製到裝置上。

權限	裝置上的檔案	輸入的檔案
修改	允許的作業：複製、移動、開啟、儲存、刪除 禁止的作業：執行	允許的作業：儲存、移動、複製
讀取和執行	允許的作業：複製、開啟、執行 允許的作業：儲存、移動、刪除	禁止的作業：儲存、移動、複製
讀取	允許的作業：複製、開啟 禁止的作業：儲存、移動、刪除、執行	禁止的作業：儲存、移動、複製
僅列出裝置內容	禁止的作業：所有作業 向使用者顯示裝置與其包含的檔案（例如，從 Windows 檔案總管）。	禁止的作業：儲存、移動、複製
封鎖 （安裝資料安全防護後即可使用）	禁止的作業：所有作業 不向使用者顯示裝置與其包含的檔案（例如，從 Windows 檔案總管）。	禁止的作業：儲存、移動、複製

檔案型掃瞄可彌補裝置權限之不足，甚至加以覆寫。例如，如果權限允許開啟檔案，但 Security Agent 偵測到檔案已感染惡意程式，則會對該檔案執行特定的中毒處理行動，以消除惡意程式。如果中毒處理行動為「清除」，檔案將會在清除後開啟。但是，如果中毒處理行動為「刪除」，則會刪除檔案。

下表列出受資料安全防護管理之行動和非儲存裝置的權限。

表 11-2. 行動和非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
允許	允許的作業：複製、移動、開啟、儲存、刪除、執行	允許的作業：儲存、移動、複製 這表示檔案可以儲存、移動與複製到裝置上。

權限	裝置上的檔案	輸入的檔案
封鎖	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

秘訣

資料安全防護的周邊設備存取控管功能支援所有的 64 位元平台。如果要在 Security Agent 不支援的系統上監控未經授權的變更阻止，請將裝置權限設定為「封鎖」，以限制這些裝置的存取權。

周邊設備存取控管允許的程式清單的萬用字元支援

程式路徑和名稱的長度上限為 259 個字元，並且只能包含英數字元 (A-Z、a-z、0-9)。您不能只指定程式名稱。

您可以使用萬用字元取代磁碟機代號和程式名稱。使用問號 (?) 代表單一字元資料（例如：磁碟機代號）。使用星號 (*) 代表多字元資料（例如：程式名稱）。

注意

您不能使用萬用字元代表資料夾名稱。必須指定資料夾的確實名稱。

下列是正確使用萬用字元的範例：

表 11-3. 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

範例	符合的資料
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 11-4. 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	

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，在程式上請點選滑鼠右鍵並選取「內容」）來取得數位簽章提供者。

第 12 章

掃瞄例外清單

本節說明如何設定適用於多個掃描功能的掃瞄例外清單。

包含下列主題：

- 間諜程式/可能的資安威脅程式核可清單 第 12-2 頁
- 信任的程式清單 第 12-2 頁

間諜程式/可能的資安威脅程式核可清單

Security Agent 會提供「核可的」間諜程式/可能的資安威脅程式清單，其中包含您不希望被視為間諜程式/可能的資安威脅程式的檔案或應用程式。在掃瞄期間偵測到特定的間諜程式/可能的資安威脅程式時，Security Agent 會檢查核可清單，如果在核可清單中找到相符項目，則不會執行任何處理行動。

請將核可清單套用至一或多個 Security Agent 與網域，或套用至伺服器管理的所有 Security Agent。將核可清單套用至所有的掃瞄類型，表示在「手動掃瞄」、「即時掃瞄」、「預約掃瞄」與「立即掃瞄」期間，都將使用相同的核可清單。

管理間諜程式/可能的資安威脅程式核可清單

程序

1. 在「間諜程式/可能的資安威脅程式名稱」表格中，選取間諜程式/可能的資安威脅程式名稱。如果要選取多個名稱，請按住 CTRL 鍵並進行選取。
   - 您也可以在「搜尋」欄位中輸入關鍵字，然後點選「搜尋」。表格會以符合關鍵字的名稱重新整理。
2. 請點選「新增」。

   名稱會移至「核可清單」表格中。
3. 如果要從核可清單移除名稱，請選取名稱並請點選「移除」。如果要選取多個名稱，請按住 CTRL 鍵並進行選取。

信任的程式清單

在「即時掃瞄」和「行為監控掃瞄」期間，您可以將 Security Agent 設定為不掃瞄信任的處理程序。將程式新增到「信任的程式清單」後，Security Agent 不再對由該程式開始的程式或任何處理程序執行「即時掃瞄」。將信任的程式新增到「信任的程式清單」，以提升端點上的掃瞄效能。

注意

您可以將符合下列要求的檔案新增到「信任的程式」清單中：

- 檔案位於 Windows 系統目錄以外的位置。
- 檔案擁有有效的數位簽章。

將程式新增到「信任的程式清單」後，Security Agent 會自動從下列掃瞄中排除該程式：

- 即時掃瞄檔案檢查
- 行為監控
- 即時掃瞄處理程序掃瞄

設定信任的程式清單

信任的程式清單不包括程式以及程式從即時掃瞄和行為監控掃瞄呼叫的所有子程序。

程序

1. 輸入要從清單中排除之程式的完整程式路徑。
2. 請點選「新增到信任的程式清單」。
3. 如果要從清單中移除程式，請點選「刪除」圖示。

第 13 章

Endpoint Sensor 策略設定

本節討論如何在 Security Agent 中設定 Endpoint Sensor 策略。

包含下列主題：

- Endpoint Sensor 第 13-2 頁
- 設定 Endpoint Sensor 設定 第 13-2 頁

Endpoint Sensor

Endpoint Sensor 是功能強大的監控和調查工具，用於識別安全威脅是否存在、其位置以及進入點。透過使用詳細的系統事件記錄和歷史分析，您可以執行初步調查來探索隱藏在您整個網路中的安全威脅，並找出所有受影響的端點。產生根本原因分析報告可瞭解安全威脅進入端點之後惡意程式的性質及活動。

您也可以過使用共用的 IOC 檔案和 YARA 規則來執行詳細調查。詳細調查會對端點進行深入的即時搜尋，以找出先前未識別的安全威脅，以及可能的「進階持續安全威脅」攻擊。

設定 Endpoint Sensor 設定

重要

Endpoint Sensor 功能需要特殊的使用授權。將 Endpoint Sensor 策略部署到端點之前，請確保您擁有正確的使用授權。如需有關如何取得使用授權的詳細資訊，請洽詢您的支援供應商。

程序

1. 選取「啟動 Endpoint Sensor」。
2. 選取「啟動事件記錄」，以開始收集用戶端端點上的系統事件記錄檔。

   執行調查時，Endpoint Sensor 會使用詳細的事件記錄檔來識別有風險的端點。識別出受影響的 Windows 端點後，您可以執行深入的根本原因分析，以更好地瞭解可能的攻擊媒介。

選項	說明
資料庫大小上限	指定 Endpoint Sensor 將事件記錄檔儲存到端點時可使用的資料庫大小上限。一旦用戶端資料庫達到這個大小上限，Endpoint Sensor 就會清除最舊的記錄檔，以釋放空間給新的事件項目。

選項	說明
傳送一小部分的記錄檔資料來執行初步評估	傳送到伺服器的資訊由中繼資料組成（例如，端點上的網域、檔案或程序）。在初步評估期間，Endpoint Sensor 會利用上述資料來識別受影響的端點。 • 上傳頻率：指定用戶端將中繼資料上傳至 Apex Central 伺服器的頻率。 注意 視網路而定，上傳太過頻繁可能會影響網路效能。
啟動「攻擊發現」以在端點上偵測已知的攻擊指標	「攻擊發現」會根據攻擊指標 (IoA) 行為來使用趨勢科技安全威脅資訊。在偵測到已知的 IoA 之後，「攻擊發現」便會記錄該偵測。

第 14 章

Vulnerability Protection 策略設定

本節討論如何在 Security Agent 中設定 Vulnerability Protection 策略。

包含下列主題：

- Vulnerability Protection 第 14-2 頁
- 設定 Vulnerability Protection 設定 第 14-2 頁

Vulnerability Protection

藉由與 Vulnerability Protection 整合，可透過在官方修補程式正式發佈之前自動執行虛擬修補程式的應用程式，來保護 Apex One 使用者。趨勢科技會根據您的網路效能和安全優先順序，來為受保護的端點提供建議的入侵防護規則。

設定 Vulnerability Protection 設定

程序

1. 選取「啟動 Vulnerability Protection」。
2. 設定入侵防護設定：
   a. 按一下「入侵防護設定」標籤。
   b. 選取下列其中一個模式：
      - 效能優先：使用入侵防護規則的子集可節省網路資源
      - 安全性優先：使用整組的入侵防護規則，但需要使用額外的網路資源
   c. （選用）選取檢視以依狀態過濾入侵防護規則的清單。

檢視	說明
全部	顯示所有入侵防護規則
由模式定義 (已啟動)	僅顯示所選取模式啟動的入侵防護規則
由模式定義 (已關閉)	僅顯示所選取模式關閉的入侵防護規則
已啟動	顯示所有已啟動的入侵防護規則
已關閉	顯示所有已關閉的入侵防護規則

d. 藉由從「狀態」下拉式清單控制項中選取來修改規則的狀態。

- 由模式定義 (已啟動)：選取的優先模式預設會啟動對應的規則。選取此選項以套用優先模式所定義的規則狀態。
- 由模式定義 (已關閉)：選取的優先模式預設會關閉對應的規則。選取此選項以套用優先模式所定義的規則狀態。
- 已啟動：選取此選項可啟動規則。
- 已關閉：選取此選項可關閉規則。

3. 設定網路引擎設定：

a. 按一下「網路引擎設定」標籤。

b. 選取「網路引擎偵測模式」。

- 內嵌：即時封包串流直接透過 Vulnerability Protection 網路引擎傳遞。在封包繼續進行通訊協定堆疊之前，會將所有規則套用至網路流量。
- TAP (僅偵測)：從主要串流複製並轉向即時封包串流。

c. 進行下列設定：

設定	說明
「已建立」逾時	在關閉連線前保持「已建立」狀態的時間。
LAST_ACK 逾時	在關閉連線前保持 LAST-ACK 狀態的時間。
冷啟動逾時	允許在啟動可設定狀態機制之前建立可能屬於連線的非 SYN 封包的時間長度。
UDP 逾時	UDP 連線的持續時間上限。
TCP 連線數目上限	同時 TCP 連線數目上限。
UDP 連線數目上限	同時 UDP 連線數目上限。
暫不處理狀態碼	此選項可讓您暫不處理特定類型的事件。您最多可以指定暫不處理三個事件。

設定	說明
進階記錄策略	您可以選取下列設定： • 略過：不過濾事件。會覆寫「暫不處理狀態碼」設定（如上）和其他進階設定，但不會覆寫 Apex One server 上定義的記錄設定。 • 預設：如果引擎處於 TAP 模式，將會切換至「TAP 模式」，如果引擎處於內嵌模式，則切換至「正常」。 • 正常：記錄「已丟棄重新傳輸」除外的所有事件。 • 回溯相容性模式：僅限支援用途。 • 詳細資訊模式：與「正常」相同，但會包括已丟棄重新傳輸。 • 可設定狀態與正規化抑制：暫不處理已丟棄重新傳輸、缺少連線、無效的旗標、無效的序列、無效的 ACK、來路不明的 UDP、來路不明的 ICMP、不符合允許的策略。 • 可設定狀態、正規化與片段抑制：暫不處理「可設定狀態與正規化抑制」暫不處理的所有項目，以及與片段相關的事件。 • 可設定狀態、片段與驗證器抑制：暫不處理「可設定狀態、正規化與片段抑制」暫不處理的所有項目，以及與驗證器相關的事件。 • TAP 模式：暫不處理已丟棄重新傳輸、缺少連線、無效的旗標、無效的序列、無效的 ACK、ACK 重新傳輸上限、已關閉連線上的封包。 如需「可設定狀態與正規化抑制」、「可設定狀態、正規化與片段抑制」、「可設定狀態、片段與驗證器抑制」和「TAP 模式」暫不處理之事件的更完整清單，請參閱進階記錄策略模式 第 14-5 頁。

4. 按一下「儲存」以套用設定。

進階記錄策略模式

下表列出在四個較為複雜的「進階記錄策略」模式下暫不處理的事件類型。

模式	暫不處理的事件
可設定狀態與正規化抑制	缺少連線 無效的旗標 無效的序列 無效的 ACK 來路不明的 UDP 來路不明的 ICMP 不符合允許的策略 已丟棄重新傳輸

模式	暫不處理的事件
可設定狀態、正規化與片段抑制	缺少連線 無效的旗標 無效的序列 無效的 ACK 來路不明的 UDP 來路不明的 ICMP 不符合允許的策略 CE 旗標 無效的 IP 無效的 IP 資料包長度 分段 無效的片段偏移 第一個片段太小 片段超出界限 片段偏移太小 IPv6 封包 輸入連線數目上限 輸出連線數目上限 傳送的 SYN 已達上限 使用授權已到期 IP 版本未知 無效的封包資訊 ACK 重新傳輸上限 已關閉連線上的封包 已丟棄重新傳輸

模式	暫不處理的事件
可設定狀態、片段與驗證器抑制	缺少連線 無效的旗標 無效的序列 無效的 ACK 來路不明的 UDP 來路不明的 ICMP 不符合允許的策略 CE 旗標 無效的 IP 無效的 IP 資料包長度 分段 無效的片段偏移 第一個片段太小 片段超出界限 片段偏移太小 IPv6 封包 輸入連線數目上限 輸出連線數目上限 傳送的 SYN 已達上限 使用授權已到期 IP 版本未知 無效的封包資訊 無效的資料偏移 無 IP 標頭 無法讀取的乙太網路標頭 未定義 來源與目標 IP 相同 無效的 TCP 標頭長度 無法讀取的通訊協定標頭 無法讀取的 IPv4 標頭 未知的 IP 版本

模式	暫不處理的事件
TAP 模式	缺少連線 無效的旗標 無效的序列 無效的 ACK ACK 重新傳輸上限 已關閉連線上的封包 已丟棄重新傳輸

部分 V

Apex One Server 策略管理

第 15 章

Apex One Server 策略設定

本節說明如何管理 Apex One Server 策略設定。

包含下列主題：

- Application Control 伺服器設定 第 15-2 頁
- 設定 Endpoint Sensor 伺服器設定 第 15-2 頁

Application Control 伺服器設定

Application Control 會按每個受管理的伺服器環境維護偵測資料庫。設定 Application Control 記錄檔資料在受管理的伺服器上保留的最大天數。

設定 Endpoint Sensor 伺服器設定

重要

Endpoint Sensor 功能需要特殊的使用授權。將 Endpoint Sensor 策略部署到端點之前，請確保您擁有正確的使用授權。如需有關如何取得使用授權的詳細資訊，請洽詢您的支援供應商。

程序

1. 建立或編輯策略。
   a. 若要建立策略，請按一下「建立」。
   b. 若要編輯策略，請按一下「策略」欄中的策略名稱。
2. 移至「Apex One Server 設定」，然後設定「Endpoint Sensor 設定」。

選項	說明
中繼資料儲存空間上限	指定允許的中繼資料儲存空間大小上限。請指定介於 1024 到 4096 GB 之間的大小。預設儲存空間大小為 1024 GB。一旦中繼資料儲存空間達到此大小，伺服器就會清除舊記錄來容納新記錄。

3. 按一下「部署」或「儲存」。

部分 VI

Apex One Data Loss Prevention 策略管理

第 16 章

Apex One Data Loss Prevention 策略設定

本節說明如何為 Security Agent 設定 Data Loss Prevention 策略。

包含下列主題：

- Data Loss Prevention (DLP) 第 16-2 頁
- 設定 Data Loss Prevention 策略 第 16-3 頁

Data Loss Prevention (DLP)

傳統的安全解決方案著重於防止外部安全威脅入侵網路。在現今的安全環境中，這麼做卻只能有一半的效果。資料遭到侵害的情況相當普遍，這會將組織的機密與敏感資料（稱為數位資產）暴露給外部未經授權的人員。資料遭到侵害可能是因為內部員工出錯或大意、資料外包、電腦設備遭竊或隨意放置、或惡意的攻擊所造成的。

資料外洩會導致：

- 品牌商譽受損
- 客戶對公司的信任度降低
- 為了進行補救措施而投入不必要的成本，以及因不遵守法規而須支付罰金
- 因智慧財產被盜，錯失商機和收益

隨著資料外洩情況越來越普遍以及因此而帶來的損害，許多公司現在都將數位資產保護視為安全措施的關鍵要素。

「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。

設定 Data Loss Prevention 策略

程序

1. 請點選「外部用戶端」標籤以設定外部用戶端的策略，或請點選「內部用戶端」標籤以設定內部用戶端的策略。

   注意

   如果您尚未設定用戶端位置設定，請進行設定。用戶端會使用這些位置設定來確定要套用的正確 Data Loss Prevention 策略。

2. 選取「啟動 Data Loss Prevention」。
3. 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。
4. 請在「規則」標籤上管理 Data Loss Prevention 套用至策略的規則。

工作	說明
新增規則	請點選「新增」以建立套用至策略的規則。 如需詳細資訊，請參閱設定 Data Loss Prevention 規則 第 16-4 頁。
複製現有的規則設定	選取現有的規則，然後點選「複製」以開啟「Data Loss Prevention 策略設定」畫面。視需要修改規則設定。

工作	說明
刪除現有的規則	選取現有的規則，然後點選「刪除」以從清單移除規則。
修改現有的規則	請點選現有規則的「規則」名稱以修改設定。
啟動/關閉現有的規則	請點選「啟動」欄下方的按鈕，以啟動或關閉某項策略的規則。

注意

一個策略最多可包含 40 個規則。

5. 請點選「例外」標籤，然後配置任何必要的例外設定。

   如需詳細資訊，請參閱 Data Loss Prevention 例外 第 16-12 頁。

設定 Data Loss Prevention 規則

注意

Data Loss Prevention 會按優先順序處理規則和範本。如果規則設定為「暫不處理」，Data Loss Prevention 會處理清單中的下一個規則。如果規則設定為「封鎖」或「使用者理由」，Data Loss Prevention 會封鎖或接受使用者處理行動，不會進一步處理該規則/範本。

程序

1. 選取啟動這項規則。
2. 指定此規則的名稱。

   配置下列範本設定：

3. 請點選「範本」標籤。
4. 從「可用的範本」清單中選取範本，然後請點選「新增」。

選取範本時：

- 請點選範本名稱來反白顯示名稱，藉此選取多個項目。
- 如果想要使用特定範本，可以使用搜尋功能。您可以輸入完整或部分的範本名稱。

注意

每個規則最多可以包含 200 個範本。

配置下列通道設定：

5. 請點選「通道」標籤。
6. 選取規則的通道。

   如需有關通道的詳細資訊，請參閱網路通道 第 16-6 頁和系統和應用程式通道 第 16-8 頁。

7. 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 16-6 頁。

8. 如果您已選取「電子郵件用戶端」，請執行下列操作：
   a. 請點選「例外」。
   b. 指定受監控和不受監控的內部電子郵件網域。

      如需有關受監控與不受監控的電子郵件網域的詳細資訊，請參閱電子郵件用戶端 第 16-7 頁。

9. 如果您已選取「卸除式儲存」，請執行下列操作：
   a. 請點選「例外」。
   b. 新增按照廠商識別的不受監控卸除式儲存裝置。裝置型號和序號 ID 是選用的。

USB 裝置的核可清單支援使用星號 (*) 萬用字元。以星號 (*) 取代任何欄位，以包含符合其他欄位要求的所有裝置。

例如，[vendor]-[model]-* 會將指定廠商和指定型號類型的所有 USB 裝置置於核可清單中，而不論序號 ID 為何。

c. 如果要新增更多裝置，請點選加號 (+) 圖示。

配置下列處理行動設定：

10. 請點選「處理行動」標籤。
11. 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 16-9 頁。
12. 配置「範本」、「通道」和「處理行動」設定之後，請點選「儲存」。

網路通道的傳輸範圍和目標

傳輸範圍和目標會定義 Data Loss Prevention 必須監控之網路通道上的資料傳輸。對於應監控的傳輸，Data Loss Prevention 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，Data Loss Prevention 不會檢查其中是否有資料識別碼，且會立即允許該傳輸。

網路通道

Data Loss Prevention 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，Data Loss Prevention 會檢查您必須設定的傳輸範圍。根據您選取的範圍，Data Loss Prevention 會監控所有資料傳輸或只監控區域網路 (LAN) 外部的傳輸。

電子郵件用戶端

Data Loss Prevention 會監控透過各種電子郵件用戶端傳輸的電子郵件。Data Loss Prevention 會檢查電子郵件的主旨、內文和附件是否包含資料識別碼。如需支援的電子郵件用戶端清單，請參閱「資料安全防護清單」文件，網址為：

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

當使用者嘗試傳送電子郵件時，就會予以監控。如果電子郵件包含資料識別碼，Data Loss Prevention 會允許或封鎖該電子郵件。

您可以定義不受監控的內部電子郵件網域和受監控的子網域。

- 不受監控的電子郵件網域：Data Loss Prevention 會立即允許傳送到不受監控網域的電子郵件傳輸。

  注意

  資料傳輸至不受監控的電子郵件網域及受監控的電子郵件子網域（中毒處理行動是「監控」）與允許傳輸的是類似的。唯一不同之處是 Data Loss Prevention 不會記錄不受監控的電子郵件網域的傳輸，但永遠會記錄受監控的電子郵件子網域的傳輸。

- 受監控的電子郵件子網域：當 Data Loss Prevention 偵測到傳輸至受監控子網域的電子郵件時，它會檢查策略的處理行動。然後根據處理行動決定允許或封鎖傳輸。

  注意

  如果您選取電子郵件用戶端作為監控的通道，則電子郵件必須符合其受監控的策略。相反，傳送到受監控電子郵件子網域的電子郵件會自動受到監控，無論其是否符合策略。

使用下列任一格式指定網域，並以逗號分隔多個網域：

- X400 格式，例如 /O=Trend/OU=USA, /O=Trend/OU=China
- 電子郵件網域，例如 `example.com`

對於透過 SMTP 通訊協定傳送的電子郵件，Data Loss Prevention 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
3. 不受監控的電子郵件網域
4. 受監控的電子郵件子網域

這表示如果電子郵件是傳送到受監控目標清單中的 SMTP 伺服器，則電子郵件會受到監控。如果 SMTP 伺服器不在受監控目標清單中，則 Data Loss Prevention 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，Data Loss Prevention 只會檢查下列清單：

1. 不受監控的電子郵件網域
2. 受監控的電子郵件子網域

系統和應用程式通道

Data Loss Prevention 可以監控下列系統和應用程式通道：

- 雲端儲存服務
- 資料錄製器 (CD/DVD)
- 對等式應用程式
- PGP 加密
- 印表機
- 卸除式儲存
- 同步處理軟體 (ActiveSync)

- Windows 剪貼簿

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. 在內部部署 Apex One 伺服器電腦上，移至 <伺服器安裝資料夾>\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）

Data Loss Prevention 處理行動

當 Data Loss Prevention 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 16-1. Data Loss Prevention 處理行動

處理行動	說明
處理行動	
暫不處理	Data Loss Prevention 允許傳輸並會記錄傳輸。
封鎖	Data Loss Prevention 封鎖傳輸並會記錄傳輸。
其他處理行動	
通知用戶端使用者	Data Loss Prevention 會顯示通知訊息告知傳輸資料的使用者，並告知資料已傳送或已封鎖。
記錄資料	無論主要處理行動為何，Data Loss Prevention 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，Trend Micro 強烈建議您只針對高度機密資訊選擇此選項。

處理行動	說明
使用指定的金鑰/密碼加密支援的通道 (只有在安裝「端點加密」的情況下才能使用) **注意** 此選項僅適用於「卸除式儲存」和「雲端儲存」服務通道且只有在選取「暫不處理」處理行動的情況下才能使用。	如果 Trend Micro Endpoint Encryption 隨 Security Agent 一起安裝，則 Data Loss Prevention 可自動加密檔案，然後允許使用者將這些檔案傳送到其他位置。如果未安裝「端點加密」，Data Loss Prevention 會對檔案執行「封鎖」處理行動。 選擇以下其中一個加密金鑰或固定式密碼： • 使用者金鑰：亦稱為「本機金鑰」，該金鑰對每個使用者是唯一的，會限制建立加密檔案的使用者存取該檔案。 • 共用金鑰：該金鑰指的是「群組金鑰」或「企業金鑰」，端點加密管理員會使用 PolicyServer MMC 設定該類型。 • 固定式密碼：使用者會使用畫面上的提示字元手動提供固定式密碼。「端點加密」會建立一個自動解壓縮套件，使用者可在提供解密密碼後存取任一端點。 **重要** • 目標端點必須安裝了「端點加密」且使用者必須登入「端點加密」才能加密資料。 • 位於 USB 裝置上的加密檔案，會在使用者嘗試解密檔案時接受 Data Loss Prevention 掃瞄。解密 USB 裝置上含有機密資料的檔案時，會觸發 USB 加密通訊協定，使系統要求對機密資料加密 (再次)。如果要防止 Data Loss Prevention 嘗試「重新加密」資料，請將已加密的檔案移至本機磁碟機，然後再嘗試存取資料。 • Data Loss Prevention 會在使用網頁用戶端時阻止將檔案上傳到雲端儲存的嘗試。手動加密檔案，然後使用網頁用戶端上傳檔案。

處理行動	說明
使用者理由 注意 僅在選取「封鎖」處理行動之後，才可以使用該選項。	Data Loss Prevention 會在執行「封鎖」處理行動之前提示使用者。透過提供敏感資料安全通過的原因，使用者可選取覆寫「封鎖」處理行動。可用的理由有： • 這是已建立的商業程序的一部分。 • 我的管理員已核可資料傳輸。 • 該檔案中的資料不是保密的。 • 其他：使用者在提供的文字欄位中提供了替代說明。

Data Loss Prevention 例外

DLP 例外會套用到整個策略，包括策略內定義的所有規則。Data Loss Prevention 會在掃瞄數位資產之前，先將例外設定套用到所有傳輸。如果傳輸符合其中一項例外規則，Data Loss Prevention 會根據例外類型立即允許或掃瞄傳輸。

定義不受監控和受監控的目標

根據「通道」標籤上設定的傳輸範圍，定義不受監控的和受監控的目標。如需如何定義所有傳輸的不受監控的和受監控的目標詳細資訊，請參閱傳輸範圍：所有傳輸 第 16-13 頁。如需如何定義僅限區域網路外部的傳輸的不受監控的和受監控的目標詳細資訊，請參閱傳輸範圍：僅限區域網路外部的傳輸 第 16-14 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，Data Loss Prevention 僅支援無類別網域間路由 (CIDR) 類型的通訊埠。這表示您只能輸入 32 之類的數字，而不能輸入 255.255.255.0。

2. 如果要以特定通道作為目標，請包含這些通道的預設或公司定義的通訊埠號碼。例如，通訊埠 21 通常用於 FTP 傳輸、通訊埠 80 用於 HTTP、通訊埠 443 用於 HTTPS。使用分號分隔目標與通訊埠號碼。
3. 您也可以包含通訊埠範圍。如果要包含所有通訊埠，請忽略通訊埠範圍。

   具有通訊埠號碼和通訊埠範圍的目標範例：

   - 10.1.1.1:80
   - host:5-20
   - host.domain.com:20
   - 10.1.1.1/32:20
4. 使用逗點分隔多個目標。

傳輸範圍：所有傳輸

Data Loss Prevention 會監控主機電腦外部傳輸的資料。

注意

Trend Micro 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：Data Loss Prevention 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 Data Loss Prevention 不會記錄不受監控的目標的傳輸，但永遠會記錄受監控的目標的傳輸。

- 受監控的目標：這些是不受監控的目標之中應監控的特定目標。受監控的目標是：
  - 選用的，如果您已定義不受監控的目標。
  - 不可設定的，如果您沒有定義不受監控的目標。

例如：

下列 IP 位址已指定給貴公司的法律部門：

- `10.201.168.1` 到 `10.201.168.25`

您正在建立策略，用於監控傳送「就業證明」給除了法律部門全職員工以外所有員工的傳輸。如果要這麼做，您可以選取「所有傳輸」作為傳輸範圍，接著：

選項	步驟
選項 1	1. 將 `10.201.168.1-10.201.168.25` 新增到不受監控的目標。 2. 將法律部門兼職員工的 IP 位址新增到受監控的目標。假設有 3 個 IP 位址 — `10.201.168.21-10.201.168.23`。
選項 2	將法律部門全職員工的 IP 位址新增到非受監控的目標： • `10.201.168.1-10.201.168.20` • `10.201.168.24-10.201.168.25`

如需有關定義受監控與不受監控的目標的指導方針，請參閱定義不受監控和受監控的目標 第 16-12 頁。

傳輸範圍：僅限區域網路外部的傳輸

Data Loss Prevention 會監控傳輸到區域網路 (LAN) 外部任何目標的資料。

注意

趨勢科技建議您為內部用戶端選擇此範圍。

「網路」是指公司或區域網路。這包括目前網路（端點和網路遮罩的 IP 位址）及下列標準私人 IP 位址：

- 類別 A：10.0.0.0 到 10.255.255.255
- 類別 B：172.16.0.0 到 172.31.255.255
- 類別 C：192.168.0.0 到 192.168.255.255

如果您選取此傳輸範圍，則可以定義下列項目：

- 不受監控的目標：定義位於 LAN 外部且您認為安全因而不應監控的目標。

注意

資料傳輸至不受監控的目標及受監控的目標（中毒處理行動是「監控」）與允許傳輸的是類似的。唯一不同之處是 Data Loss Prevention 不會記錄不受監控的目標的傳輸，但永遠會記錄受監控的目標的傳輸。

- 受監控的目標：定義位於 LAN 內部的您想要監控的目標。

如需有關定義受監控與不受監控的目標的指導方針，請參閱定義不受監控和受監控的目標 第 16-12 頁。

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，Data Loss Prevention 會使壓縮檔遵循下列規則：

- 解壓縮檔大小超過：__ MB (1-512MB)
- 壓縮層的數目超過：__ (1-20)
- 要掃瞄的檔案數超過：__ (1-2000)

第 17 章

Data Discovery Widget

本節包含 Apex Central as a Service 中支援的所有 Data Discovery 資訊中心 Widget 的說明主題。

包含下列主題：

- 前幾名偵測到的機密檔案策略 Widget 第 17-2 頁
- 前幾名具有機密檔案的端點 Widget 第 17-3 頁
- 前幾名 Data Discovery 範本相符項目 Widget 第 17-5 頁
- 前幾名機密檔案 Widget 第 17-6 頁

前幾名偵測到的機密檔案策略 Widget

此 Widget 會顯示有關 Data Discovery 策略違規偵測和觸發規則的機密檔案資訊。

注意

依預設，此 Widget 會顯示使用者帳號有權檢視的所有受管理產品的資料。

使用「範圍」下拉式清單，選取顯示的資料時間範圍。

- 如果要指定自訂時間範圍或時間間隔，請按一下設定圖示 (>)，然後針對「範圍」選取「自訂」。

使用「規則」下拉式清單可指定觸發偵測的規則。

- 如果要指定顯示的規則數目，請按一下設定圖示 (>)，然後從「要顯示的規則」下拉式清單中選取。
- 如果要彙整剩餘的資料，請按一下設定圖示 (>)，然後選取「將剩餘資料顯示為「其他」」。

按一下顯示圖示 ( )，可選擇要以資料表、長條圖、圓餅圖還是折線圖來顯示資料。

預設檢視會以資料表顯示下列資訊。

欄名稱	說明
規則名稱	顯示機密檔案所觸發的規則。
偵測	顯示規則被觸發的次數 按一下「偵測」欄名稱可依偵測數排序資料表。 按一下數字即可檢視有關偵測的詳細資訊（偵測的發生時間、偵測到的機密檔案）。
百分比	將規則被觸發的次數顯示為偵測總數的百分比

按一下「偵測」欄中的數字，或按一下圖表區段，可檢視詳細資訊。

資料	說明
收到	Apex Central 接收資料的時間和日期
已產生	偵測的發生時間和日期
規則	觸發的規則
端點	觸發規則的端點
網域	觸發規則的網域
使用者	觸發規則的使用者
使用者網域	使用者所屬的網域
檔案路徑	機密檔案的檔案路徑
檔案	機密檔案的名稱
範本	規則所屬的範本
處理行動	對機密檔案採取的處理行動

前幾名具有機密檔案的端點 Widget

此 Widget 會顯示有關所含機密檔案觸發 Data Discovery 策略違規偵測的端點資訊。

注意

依預設，此 Widget 會顯示使用者帳號有權檢視的所有受管理產品的資料。

使用「範圍」下拉式清單，選取顯示的資料時間範圍。

- 如果要指定自訂時間範圍或時間間隔，請按一下設定圖示 (>)，然後針對「範圍」選取「自訂」。

使用「規則」下拉式清單可指定觸發偵測的規則。

- 如果要指定顯示的範本數目，請按一下「設定」圖示 (>)，然後從「要顯示的端點」下拉式清單中選取。
- 如果要彙整剩餘的資料，請按一下設定圖示 (>)，然後選取「將剩餘資料顯示為「其他」」。

按一下顯示圖示 ()，可選擇要以資料表、長條圖還是圓餅圖來顯示資料。

預設檢視會以資料表顯示下列資訊。

欄名稱	說明
端點	顯示所含機密檔案觸發規則的端點
偵測	顯示規則被觸發的次數 按一下「偵測」欄名稱可依偵測數排序資料表。
百分比	將規則被觸發的次數顯示為偵測總數的百分比

按一下「偵測」欄中的數字，或按一下圖表區段，可檢視詳細資訊。

資料	說明
收到	Apex Central 接收資料的時間和日期
已產生	偵測的發生時間和日期
規則	觸發的規則
端點	觸發規則的端點
網域	觸發規則的網域
使用者	觸發規則的使用者
使用者網域	使用者所屬的網域
檔案路徑	機密檔案的檔案路徑
檔案	機密檔案的名稱
範本	規則所屬的範本

資料	說明
處理行動	對機密檔案採取的處理行動

前幾名 Data Discovery 範本相符項目 Widget

此 Widget 會顯示有關歷來前幾名 Data Discovery 範本策略違規的資訊。

注意

依預設，此 Widget 會顯示使用者帳號有權檢視的所有受管理產品的資料。

使用「範圍」下拉式清單，選取顯示的資料時間範圍。

- 如果要指定自訂時間範圍或時間間隔，請按一下設定圖示 (>)，然後針對「範圍」選取「自訂」。

使用「規則」下拉式清單可指定觸發偵測的規則。

- 如果要指定顯示的範本數目，請按一下「設定」圖示 (>)，然後從「要顯示的範本」下拉式清單中選取。
- 如果要彙整剩餘的資料，請按一下設定圖示 (>)，然後選取「將剩餘資料顯示為「其他」」。

按一下顯示圖示 ( )，可選擇要以資料表、長條圖還是圓餅圖來顯示資料。

預設檢視會以資料表顯示下列資訊。

欄名稱	說明
範本	顯示機密檔案所觸發的範本

欄名稱	說明
偵測	顯示觸發範本的次數 按一下「偵測」欄名稱可依偵測數排序資料表。
百分比	顯示觸發範本的次數佔偵測總數的百分比

按一下「偵測」欄中的數字，或按一下圖表區段，可檢視詳細資訊。

資料	說明
收到	Apex Central 接收資料的時間和日期
已產生	偵測的發生時間和日期
規則	觸發的規則
端點	觸發規則的端點
網域	觸發規則的網域
使用者	觸發規則的使用者
使用者網域	使用者所屬的網域
檔案路徑	機密檔案的檔案路徑
檔案	機密檔案的名稱
範本	規則所屬的範本
處理行動	對機密檔案採取的處理行動

前幾名機密檔案 Widget

此 Widget 會顯示有關歷來觸發 Data Discovery 策略違規的前幾名機密檔案資訊。

注意

依預設，此 Widget 會顯示使用者帳號有權檢視的所有受管理產品的資料。

使用「範圍」下拉式清單，選取顯示的資料時間範圍。

- 如果要指定自訂時間範圍或時間間隔，請按一下設定圖示 (>)，然後針對「範圍」選取「自訂」。

使用「規則」下拉式清單可指定觸發偵測的規則。

- 如果要指定顯示的偵測數目，請按一下「設定」圖示 (>)，然後從「要顯示的機密檔案」下拉式清單中選取。
- 如果要彙整剩餘的資料，請按一下設定圖示 (>)，然後選取「將剩餘資料顯示為「其他」」。

按一下顯示圖示 ( )，可選擇要以資料表、長條圖還是圓餅圖來顯示資料。

預設檢視會以資料表顯示下列資訊。

欄名稱	說明
檔案	顯示可能洩漏的機密檔案
偵測	顯示機密檔案可能洩漏的次數 按一下「偵測」欄名稱可依偵測數排序資料表。
百分比	顯示機密檔案可能洩漏的次數佔偵測總數的百分比

按一下「偵測」欄中的數字，或按一下圖表區段，可檢視詳細資訊。

資料	說明
收到	Apex Central 接收資料的時間和日期
已產生	偵測的發生時間和日期
規則	觸發的規則
端點	觸發規則的端點
網域	觸發規則的網域
使用者	觸發規則的使用者

資料	說明
使用者網域	使用者所屬的網域
檔案路徑	機密檔案的檔案路徑
檔案	機密檔案的名稱
範本	規則所屬的範本
處理行動	對機密檔案採取的處理行動

第 18 章

Apex One 資料發現策略設定

本節討論如何在 Apex Central 中設定 Apex One 資料發現策略設定。

包含下列主題：

- 建立 Data Discovery 策略 第 18-2 頁

建立 Data Discovery 策略

Data Discovery 會搜尋資料庫、端點和文件管理系統，以確認是否存在敏感資訊。Data Discovery Widget 可顯示 Data Loss Prevention 是否符合企業策略。管理員可以使用 Data Discovery 策略和 Widget，來對其網路執行矯正性處理行動。

注意

對端點磁碟或目錄執行完整掃瞄時，使用者可能會感覺系統速度明顯變慢。

程序

1. 選取「啟動 Data Discovery」。
2. 請點選「新增」。

   會出現「資料發現策略設定」畫面。
3. 選取啟動這項規則。
4. 指定此規則的名稱。
5. 設定目標資料夾設定：
   a. 按一下「目標資料夾」標籤。

      注意

      根資料夾不能是 Windows 共用資料夾或卸除式裝置（USB 裝置或 DVD）。

   b. 在「檔案路徑」區段中，指定檔案的掃瞄位置。

注意

Data Discovery 不會掃瞄位於下列目錄的 autoexec.bat 檔案：

- \Documents and Settings*\Application Data\
- \Documents and Settings*\Local Settings\
- \Documents and Settings*\Cookies\
- \Program Files\
- \Windows\
- \Winnt\
- \Users*\AppData\
- \ProgramData\

c. 在「檔案類型例外」區段中，指定掃瞄例外。

- 掃瞄：指定要掃瞄的特定檔案或檔案類型。
- 不掃瞄：指定 Data Discovery 不掃瞄的特定檔案、檔案類型或資料夾。

注意

- Data Discovery 支援下列萬用字元：
  - *：替換 * 前後的任何字元和所有字元
  - ?：替換單一字元或單一雙位元字元
- 使用直立線符號 (|) 分隔多個項目並使用以下格式：
  - 檔案：*.<副檔名>（範例：*.exe|*.doc）
  - 資料夾：指定檔案路徑（範例：*\Test*|C:\My-Docs\）

配置下列範本設定：

6. 配置下列範本設定：

a. 請點選「範本」標籤。

b. 從「可用的範本」清單中選取範本，然後請點選「新增」。

選取範本時：

- 請點選範本名稱來反白顯示名稱，藉此選取多個項目。
- 如果想要使用特定範本，可以使用搜尋功能。您可以輸入完整或部分的範本名稱。

注意

- 每個規則最多可以包含 500 個範本。
- 如果「可用的範本」清單中沒有您偏好的範本，請移至「策略 > 策略資源 > DLP 範本」，然後建立新範本。

7. 配置下列處理行動設定：

a. 請點選「處理行動」標籤。

b. 選取「監控」以記錄偵測項目來進行分析。

c. （選用）選取「加密」以使用下列其中一種方法來加密機密檔案：

- 使用者金鑰
- 群組金鑰
- 加密密碼：加密密碼是所有 Apex One server 的全域密碼。按一下「建立加密密碼」以設定密碼。

8. 設定預約掃瞄：

a. 按一下「預約」標籤。

b. 指定掃瞄頻率。

c. 指定掃瞄開始時間。

9. 按一下「儲存」以套用設定。

部分 VII

Apex One (Mac) Widget 和策略

第 19 章

Apex One (Mac) Widget

本節包含有關 Apex Central as a Service 中支援的 Apex One (Mac) 資訊中心 Widget 的說明主題。

包含下列主題：

- 關鍵效能指標 Widget 第 19-2 頁

關鍵效能指標 Widget

在「Apex Central as a Service 資訊中心」畫面上，使用此 Widget 可根據選取的條件顯示 Apex One (Mac) 關鍵效能指標 (KPI)。

如需有關如何將 Widget 新增至「資訊中心」畫面的資訊，請參閱 Apex Central as a Service 文件。

秘訣

依預設，此 Widget 會將發生 15 次的事件標示為「重要」( )，將發生 30 次的事件標示為「嚴重」( )。或者，也可以藉由自訂事件門檻值，將事件標示為「重要」或「嚴重」。

設定關鍵效能指標

在 Apex Central as a Service 的「資訊中心」上，存取「Apex One (Mac) 關鍵效能指標」Widget，以執行與下列指標相關的工作。

表 19-1. KPI Widget 指標工作

工作	步驟
新增指標	1. 按一下「新增指標」。會出現「新增指標」畫面。 2. 從「名稱」下拉式清單中選取選項，並選擇性地自訂設定。 3. 按一下「儲存」。
編輯指標	1. 按一下清單中的指標。會出現「編輯指標」畫面。 2. 自訂設定。 3. 按一下「儲存」。

工作	步驟
刪除指標。	1. 按一下清單中的指標。會出現「編輯指標」畫面。 2. 請點選「刪除」。 3. 請點選「確定」。
設定事件門檻值設定	1. 在「新增指標」或「編輯指標」畫面上，選取「達到下列門檻值時啟動警訊」。 2. 輸入每個事件類型的事件發生次數下限。 3. 按一下「儲存」。 注意 如果下列兩項條件同時成立，則「出現次數」欄中顯示「重要」或「嚴重」圖示： • 符合此指標的事件出現次數等於或高於門檻值。 • 已選取「達到下列門檻值時啟動警訊」。

設定 Widget 設定

在「Apex Central as a Service 資訊中心」畫面上，從 Widget 右上方的功能表中選取「Widget 設定」以執行下列工作：

表 19-2. KPI Widget 設定

工作	步驟
編輯 Widget 標題	在文字欄位中輸入 Widget 標題。

工作	步驟
設定每日更新時間	從下拉式清單中，選取每天要產生 Widget 資料的時刻。 秘訣 如果要手動重新整理 Widget 資料，請按一下「重新整理」( ) 圖示。

第 20 章

Trend Micro Apex One (Mac) 策略設定

本節討論如何在 Apex Central 中設定 Trend Micro Apex One (Mac) 策略設定。

包含下列主題：

- 掃瞄方法類型 第 20-2 頁
- 掃瞄類型 第 20-6 頁
- 用於掃瞄的快取設定 第 20-21 頁
- 掃瞄例外 第 20-22 頁
- 用戶端自我保護 第 20-26 頁
- 用戶端更新 第 20-27 頁
- 網站信譽評等服務 第 20-30 頁
- 周邊設備存取控管 第 20-33 頁
- Endpoint Sensor 第 20-35 頁
- 信任的程式清單 第 20-37 頁
- Machine Learning 設定 第 20-38 頁

掃瞄方法類型

Apex One (Mac) Security Agent 可使用兩種掃瞄方法中的其中一種來掃瞄是否有安全威脅。掃瞄方法包括雲端截毒掃瞄和傳統掃瞄。

- 雲端截毒掃瞄

  使用雲端截毒掃瞄的代理程式在本文件中稱為「雲端截毒掃瞄代理程式」。雲端截毒掃瞄代理程式將受益於檔案信譽評等服務提供的本機掃瞄和雲端查詢。

  這是預設的掃瞄方法類型。

- 傳統掃瞄

  未使用雲端截毒掃瞄的代理程式稱為「標準掃瞄代理程式」。標準掃瞄代理程式會將所有 Apex One (Mac) 元件儲存在用戶端端點上，並在本機掃瞄所有檔案。

掃瞄方法比較

下表提供這兩種掃瞄方法的比較：

表 20-1. 傳統掃瞄和雲端截毒掃瞄的比較

比較基準	傳統掃瞄	雲端截毒掃瞄
掃瞄行為	標準掃瞄代理程式會在本機端點上執行掃瞄。	• 雲端截毒掃瞄代理程式會在本機端點上執行掃瞄。 • 如果 Security Agent 在掃瞄期間無法判斷檔案的風險，則 Security Agent 會將掃瞄查詢傳送到主動式雲端截毒技術來源來確認該風險。 • Security Agent 會「快取」掃瞄查詢結果，以提升掃瞄效能。

比較基準	傳統掃瞄	雲端截毒掃瞄
元件使用中且已更新	所有元件（「Mac 自動邏輯分析病毒碼」和「本機雲端病毒碼」除外）在更新來源都可用。	所有元件（「病毒碼」和「間諜程式主動式監控病毒碼」除外）在更新來源都可用。
傳統更新來源	Apex One (Mac) 伺服器	Apex One (Mac) 伺服器

從雲端截毒掃瞄切換至傳統掃瞄

下表提供將用戶端切換到傳統掃瞄時的其他考量事項。

表 20-2. 切換到傳統掃瞄時的考量事項

注意事項	詳細資訊
要切換的用戶端數目	一次切換少量的 Security Agent，可確保有效利用 Apex One (Mac) 伺服器與主動式雲端截毒技術伺服器資源。當 Security Agent 變更其掃瞄方法的同時，這些伺服器可以執行其他重要工作。
時機	切換回傳統掃瞄時，Security Agent 可能會從 Apex One (Mac) 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掃瞄代理程式。 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 Security Agent 預約要從伺服器進行更新時，執行切換作業。

注意事項	詳細資訊
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。切換至傳統掃瞄時，您可以： • 建立新的群組，並指派傳統掃瞄為其掃瞄方法。任何移至此群組的 Security Agent，都會使用傳統掃瞄。當您移動 Security Agent 時，請啟動「將新群組的設定套用至選取的用戶端」設定。 • 選取群組並加以設定，使其使用傳統掃瞄。屬於該群組的雲端截毒掃瞄代理程式將會切換到傳統掃瞄。 • 從群組中選取一或多個雲端截毒掃瞄代理程式，然後將其切換到傳統掃瞄。 注意 如果群組的掃瞄方法有任何變更，都將覆寫您為個別 Security Agent 設定的掃瞄方法。

從傳統掃瞄切換至雲端截毒掃瞄

如果要將用戶端從傳統掃瞄切換到雲端截毒掃瞄，請確保已在 Apex One server 上設定「主動式雲端截毒技術服務」。如需詳細資訊，請參閱 Apex One 文件。

下表提供將用戶端切換至雲端截毒掃瞄時的其他考量事項。

表 20-3. 切換到雲端截毒掃瞄時的注意事項

注意事項	詳細資訊
產品使用授權	如果要使用雲端截毒掃瞄，請確保您已在 Apex One server 上啟動下列服務的使用授權，且這些使用授權尚未到期： • 防毒 • 網站信譽評等服務和間諜程式防護

注意事項	詳細資訊
Apex One (Mac) 伺服器	確定用戶端可連線到 Apex One (Mac) 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，或者用戶端若有預約更新權限，則會在執行預約更新時接獲通知。
要切換的用戶端數目	一次切換相對少量的用戶端，可確保有效利用 Apex One (Mac) 伺服器資源。當用戶端變更其掃瞄方法時，Apex One (Mac) 伺服器可以執行其他重要工作。
時機	首次切換至雲端截毒掃瞄時，用戶端必須從 Apex One (Mac) 伺服器下載完整版的 Mac 自動邏輯分析病毒碼和本機雲端病毒碼。雲端病毒碼僅適用於雲端截毒掃瞄代理程式。 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 Security Agent 預約要從伺服器進行更新時，執行切換作業。
用戶端樹狀結構設定	掃瞄方法是一項可在根、群組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： • 建立新的群組，並將雲端截毒掃瞄指派為其掃瞄方法。任何移至此群組的用戶端，都會使用雲端截毒掃瞄。當您移動用戶端時，請啟動「將新群組的設定套用至選取的用戶端」設定。 • 選取群組並加以設定，使其使用雲端截毒掃瞄。屬於該群組的標準掃瞄代理程式將會切換至雲端截毒掃瞄。 • 從群組中選取一或多個標準掃瞄代理程式，然後將其切換至雲端截毒掃瞄。 注意 如果群組的掃瞄方法有任何變更，都將覆寫您為個別 Security Agent 設定的掃瞄方法。

注意事項	詳細資訊
IPv6 支援	雲端截毒掃瞄代理程式會將掃瞄查詢傳送至主動雲端截毒技術來源。 純 IPv6 雲端截毒掃瞄用戶端無法將查詢直接傳送到純 IPv4 來源，例如： • 主動式雲端截毒技術伺服器 3.0（整合式或獨立式） • 趨勢科技主動式雲端截毒技術 同樣，純 IPv4 雲端截毒掃瞄用戶端無法將查詢傳送至純 IPv6 主動式雲端截毒技術伺服器。 如果要使雲端截毒掃瞄代理程式連線到來源，需提供可以轉換 IP 位址的雙堆疊 Proxy 伺服器（如 DeleGate）。

掃瞄類型

Apex One (Mac) 提供下列掃瞄類型，來保護端點不受安全威脅侵害：

掃瞄類型	說明
即時掃瞄	每當接收、開啟、下載、複製或修改檔案時，自動掃瞄端點上的檔案 請參閱即時掃瞄 第 20-6 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 請參閱手動掃瞄 第 20-11 頁。
預約掃瞄	根據管理員所設定的預約時程，自動掃瞄端點上的檔案 請參閱預約掃瞄 第 20-15 頁。
立即掃瞄	由管理員啟動的掃瞄，掃瞄一或多個目標端點上的檔案

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 Apex One (Mac) 未偵測到

安全威脅，檔案會保留在其位置，供使用者繼續存取。如果 Apex One (Mac) 偵測到安全威脅，則顯示一則通知訊息，指出中毒檔案的名稱和具體的安全威脅風險。

請設定「即時掃瞄」設定，並將其套用至一或多個用戶端與群組，或套用至伺服器管理的所有 Security Agent。

設定即時掃瞄設定

程序

1. 選取核取方塊以啟動「即時掃瞄」。
2. 按一下「目標」標籤，以進行檔案活動和掃瞄設定。

   如需詳細資訊，請參閱即時掃瞄：「目標」標籤 第 20-7 頁。
3. 按一下「處理行動」標籤，以設定 Apex One (Mac) 對偵測到的安全威脅所執行的中毒處理行動。

   如需詳細資訊，請參閱即時掃瞄：「處理行動」標籤 第 20-8 頁。

即時掃瞄：「目標」標籤

程序

1. 在「使用者對檔案執行的活動」下，選擇對檔案執行哪些活動時會觸發「即時掃瞄」。您可以選取下列選項：
   - 在建立/修改檔案時掃瞄：掃瞄引入端點的新檔案（例如，在下載檔案後），或掃瞄所修改的檔案
   - 在擷取/執行檔案時掃瞄：在檔案開啟時掃瞄
   - 在建立/修改和擷取/執行檔案時掃瞄
   - 在建立/修改/執行檔案時掃瞄

例如，若選取第三個選項，會對下載至端點的新檔案進行掃瞄；若未偵測到安全威脅，則會保留在其目前位置上。當使用者開啟檔案，或使用者修改檔案後要進行儲存前，將會掃瞄該檔案。

2. 在「掃瞄設定」下，選取下列一或多個選項：

   - 掃瞄壓縮檔：掃瞄封存檔中的個別檔案

     如需詳細資訊，請參閱支援的壓縮檔類型 第 20-9 頁。

   - 掃瞄網路磁碟機：掃瞄實際位於其他端點，但對應至本機端點的目錄

即時掃瞄：「處理行動」標籤

在「處理行動」標籤中，設定 Apex One (Mac) 對偵測到的安全威脅所執行的中毒處理行動。

程序

1. 在「處理行動」下，指定中毒處理行動。

選項	說明
使用主動式處理行動	「主動式處理行動」是一套預先設定的中毒處理行動，可以處理各種類型的安全威脅。如果不確定某個特定安全威脅類型適合採用哪種中毒處理行動，趨勢科技建議您使用「主動式處理行動」。 「主動式處理行動」設定會在特徵碼檔案中持續更新，以保護端點抵禦最新的安全威脅和最新的攻擊方法。

選項	說明
對所有安全風險類型都使用相同的處理行動	如果您要對「可能的病毒/惡意程式」以外的所有安全威脅類型執行相同的處理行動，請選取此選項。對於「可能的病毒/惡意程式」，處理行動一律為「暫不處理」。 若您選擇「清除」做為第一個處理行動，請選取清除未成功時 Apex One (Mac) 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。 如需有關中毒處理行動的詳細資訊，請參閱中毒處理行動 第 20-10 頁。

2. 選取「偵測到病毒/惡意程式時，在用戶端端點上顯示通知訊息」，可讓 Apex One (Mac) 在即時掃瞄期間偵測到安全威脅時顯示通知訊息。

支援的壓縮檔類型

Apex One (Mac) 支援下列壓縮類型。

副檔名	類型
.zip	由 Pkzip 建立的封存檔
.rar	由 RAR 建立的封存檔
.tar	由 Tar 建立的封存檔
.arj	ARJ 壓縮的封存檔
.hqx	BINHEX
.gz；.gzip	Gnu ZIP
.Z	LZW/壓縮的 16 位元
.bin	MacBinary
.cab	Microsoft 封包檔
Microsoft 壓縮/MSCOMP	

副檔名	類型
.eml；.mht	MIME
.td0	Teledisk 格式
.bz2	Unix BZ2 Bzip 壓縮檔
.uu	UUEncode
.ace	WinAce

中毒處理行動

指定特定掃瞄類型偵測到安全威脅時，Apex One (Mac) 執行的處理行動。

Apex One (Mac) 執行的處理行動視偵測到安全威脅的掃瞄類型而定。例如，當 Apex One (Mac) 在手動掃瞄（掃瞄類型）期間偵測到安全威脅，將會清除（處理行動）中毒檔案。

下列是 Apex One (Mac) 可以針對安全威脅執行的處理行動：

中毒處理行動	詳細資訊
刪除	Apex One (Mac) 從端點移除中毒檔案。
隔離	Apex One (Mac) 重新命名中毒檔案，再將其移至端點上的隔離目錄中，此目錄位於 <用戶端安裝資料夾>/common/lib/vsapi/quarantine。 進入隔離目錄後，Apex One (Mac) 可以根據使用者指定的處理行動，對隔離的檔案執行另一個處理行動。Apex One (Mac) 可以刪除、清除或恢復該檔案。恢復檔案意味著將檔案移回其原始位置而不執行任何處理行動。使用者可以恢復實際上無害的檔案。清除檔案意味著從隔離的檔案中移除安全威脅，如果清除成功，就將檔案移至原始位置。
清除	Apex One (Mac) 從中毒檔案中移除安全威脅，然後再允許使用者存取該檔案。 如果無法清除檔案，Apex One (Mac) 會執行第二個處理行動，可能是下列其中一個處理行動：「隔離」、「刪除」與「暫不處理」。如果要設定第二個處理行動，請瀏覽至「用戶端管理 > 設定 > {掃瞄類型}」，然後按一下「處理行動」標籤。

中毒處理行動	詳細資訊
暫不處理	Apex One (Mac) 對中毒檔案不執行任何處理行動，但會將偵測到的安全威脅記錄在記錄檔中。檔案會留在其所在的位置。 Apex One (Mac) 對感染有「可能的病毒/惡意程式」類型的檔案一律執行「暫不處理」，以減輕誤判情況。如果進一步的分析確認可能的病毒/惡意程式確實是安全威脅，將會發行新的病毒碼，讓 Apex One (Mac) 可以執行適當的中毒處理行動。如果可能的病毒/惡意程式實際上是無害時，系統將不會再偵測。 例如：Apex One (Mac) 偵測到名為 "123.pdf" 的檔案含有 "x_probable_virus"，並在偵測時不執行任何處理行動。接著趨勢科技確認 "x_probable_virus" 是一種特洛伊木馬程式，並發行新的病毒碼版本。在載入新的病毒碼後，Apex One (Mac) 會將 "x_probable_virus" 偵測為特洛伊木馬程式，如果對這類程式的處理行動是「刪除」，那麼就會刪除 "123.pdf"。

手動掃瞄

「手動掃瞄」是依需求掃瞄，會在使用者於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端點的硬體資源而定。

請設定「手動掃瞄」設定，並將其套用至一或多個用戶端與群組，或套用至伺服器管理的所有用戶端。

設定手動掃瞄設定

程序

1. 按一下「目標」標籤，以進行一般掃瞄和 CPU 使用率設定。

   如需詳細資訊，請參閱手動掃瞄：「目標」標籤 第 20-12 頁。

2. 按一下「處理行動」標籤，以設定 Apex One (Mac) 對偵測到的安全威脅所執行的中毒處理行動。

   如需詳細資訊，請參閱手動掃瞄：「處理行動」標籤 第 20-13 頁。

手動掃瞄：「目標」標籤

程序

1. 在「要掃瞄的檔案」區段中，從下列項目中選取：

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

     注意

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

   - 僅掃瞄 Mach-O 檔案：僅掃瞄端點上的 Mach-O 檔案。Apex One (Mac) Security Agent 不會掃瞄其他檔案類型是否有惡意程式。

2. 在「掃瞄設定」下，選取下列一或多個選項：

   - 掃瞄壓縮檔：掃瞄封存檔中的個別檔案

     如需詳細資訊，請參閱支援的壓縮檔類型 第 20-9 頁。

   - 掃瞄網路磁碟機：掃瞄實際位於其他端點，但對應至本機端點的目錄

   - 掃瞄 Time Machine：僅掃瞄 Time Machine 磁碟機中的檔案

     注意

     在針對「手動掃瞄」和「預約掃瞄」啟動「掃瞄 Time Machine」選項後，由於 Mac OS 的權限限制，Apex One (Mac) 只會偵測惡意程式安全威脅，而不採取任何處理行動（清除、隔離或刪除）。在產品記錄檔中，設定的中毒處理行動會顯示為未成功。

3. 在「掃瞄設定」區段中，設定必要設定。

   - 高：掃瞄之間不暫停

- 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

手動掃瞄：「處理行動」標籤

在「處理行動」標籤中，設定 Apex One (Mac) 對偵測到的安全威脅所執行的中毒處理行動。

選項	說明
使用主動式處理行動	「主動式處理行動」是一套預先設定的中毒處理行動，可以處理各種類型的安全威脅。如果不確定某個特定安全威脅類型適合採用哪種中毒處理行動，趨勢科技建議您使用「主動式處理行動」。 「主動式處理行動」設定會在特徵碼檔案中持續更新，以保護端點抵禦最新的安全威脅和最新的攻擊方法。
對所有安全風險類型都使用相同的處理行動	如果您要對「可能的病毒/惡意程式」以外的所有安全威脅類型執行相同的處理行動，請選取此選項。對於「可能的病毒/惡意程式」，處理行動一律為「暫不處理」。 若您選擇「清除」做為第一個處理行動，請選取清除未成功時 Apex One (Mac) 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。 如需有關中毒處理行動的詳細資訊，請參閱中毒處理行動 第 20-10 頁。

支援的壓縮檔類型

Apex One (Mac) 支援下列壓縮類型。

副檔名	類型
.zip	由 Pkzip 建立的封存檔

副檔名	類型
.rar	由 RAR 建立的封存檔
.tar	由 Tar 建立的封存檔
.arj	ARJ 壓縮的封存檔
.hqx	BINHEX
.gz；.gzip	Gnu ZIP
.Z	LZW/壓縮的 16 位元
.bin	MacBinary
.cab	Microsoft 封包檔
Microsoft 壓縮/MSCOMP	
.eml；.mht	MIME
.td0	Teledisk 格式
.bz2	Unix BZ2 Bzip 壓縮檔
.uu	UUEncode
.ace	WinAce

中毒處理行動

指定特定掃瞄類型偵測到安全威脅時，Apex One (Mac) 執行的處理行動。

Apex One (Mac) 執行的處理行動視偵測到安全威脅的掃瞄類型而定。例如，當 Apex One (Mac) 在手動掃瞄（掃瞄類型）期間偵測到安全威脅，將會清除（處理行動）中毒檔案。

下列是 Apex One (Mac) 可以針對安全威脅執行的處理行動：

中毒處理行動	詳細資訊
刪除	Apex One (Mac) 從端點移除中毒檔案。

中毒處理行動	詳細資訊
隔離	Apex One (Mac) 重新命名中毒檔案，再將其移至端點上的隔離目錄中，此目錄位於 <用戶端安裝資料夾>/common/lib/vsapi/quarantine。 進入隔離目錄後，Apex One (Mac) 可以根據使用者指定的處理行動，對隔離的檔案執行另一個處理行動。Apex One (Mac) 可以刪除、清除或恢復該檔案。恢復檔案意味著將檔案移回其原始位置而不執行任何處理行動。使用者可以恢復實際上無害的檔案。清除檔案意味著從隔離的檔案中移除安全威脅，如果清除成功，就將檔案移至原始位置。
清除	Apex One (Mac) 從中毒檔案中移除安全威脅，然後再允許使用者存取該檔案。 如果無法清除檔案，Apex One (Mac) 會執行第二個處理行動，可能是下列其中一個處理行動：「隔離」、「刪除」與「暫不處理」。如果要設定第二個處理行動，請瀏覽至「用戶端管理 > 設定 > {掃瞄類型}」，然後按一下「處理行動」標籤。
暫不處理	Apex One (Mac) 對中毒檔案不執行任何處理行動，但會將偵測到的安全威脅記錄在記錄檔中。檔案會留在其所在的位置。 Apex One (Mac) 對感染有「可能的病毒/惡意程式」類型的檔案一律執行「暫不處理」，以減輕誤判情況。如果進一步的分析確認可能的病毒/惡意程式確實是安全威脅，將會發行新的病毒碼，讓 Apex One (Mac) 可以執行適當的中毒處理行動。如果可能的病毒/惡意程式實際上是無害時，系統將不會再偵測。 例如：Apex One (Mac) 偵測到名為 "123.pdf" 的檔案含有 "x_probable_virus"，並在偵測時不執行任何處理行動。接著趨勢科技確認 "x_probable_virus" 是一種特洛伊木馬程式，並發行新的病毒碼版本。在載入新的病毒碼後，Apex One (Mac) 會將 "x_probable_virus" 偵測為特洛伊木馬程式，如果對這類程式的處理行動是「刪除」，那麼就會刪除 "123.pdf"。

預約掃瞄

「預約掃瞄」會在指定的日期與時間自動執行。使用「預約掃瞄」，可對用戶端自動執行例行掃瞄，並提高掃瞄管理效率。

請設定「預約掃瞄」設定，並將其套用至一或多個用戶端與群組，或套用至伺服器管理的所有用戶端。

設定預約掃瞄設定

程序

1. 選取核取方塊以啟動「預約掃瞄」。
2. 按一下「目標」標籤，以設定一般掃瞄和 CPU 使用率設定，以及掃瞄預約時程。

   如需詳細資訊，請參閱預約掃瞄：「目標」標籤 第 20-16 頁。
3. 按一下「處理行動」標籤，以設定 Apex One (Mac) 對偵測到的安全威脅所執行的中毒處理行動。

   如需詳細資訊，請參閱預約掃瞄：「處理行動」標籤 第 20-17 頁。

預約掃瞄：「目標」標籤

程序

1. 在「預約」下，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，如果選取 29 日、30 日或 31 日，但該月沒有此日期，則 Apex One (Mac) 會在該月最後一天執行「預約掃瞄」。
2. 在「要掃瞄的檔案」區段中，從下列項目中選取：

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

注意

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

- 智慧型掃瞄所掃瞄的檔案類型：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。
- 指定路徑或完整路徑：手動指定要掃瞄的檔案或目錄。例如：`/Shared/Files/mytext.txt` 或 `/Shared/Files`。

3. 在「掃瞄設定」下，選取下列一或多個選項：
   - 掃瞄壓縮檔：掃瞄封存檔中的個別檔案

     如需詳細資訊，請參閱支援的壓縮檔類型 第 20-9 頁。
   - 掃瞄 Time Machine：僅掃瞄 Time Machine 磁碟機中的檔案

注意

在針對「手動掃瞄」和「預約掃瞄」啟動「掃瞄 Time Machine」選項後，由於 Mac OS 的權限限制，Apex One (Mac) 只會偵測惡意程式安全威脅，而不採取任何處理行動（清除、隔離或刪除）。在產品記錄檔中，設定的中毒處理行動會顯示為未成功。

4. 在「掃瞄設定」區段中，設定必要設定。
   - 高：掃瞄之間不暫停
   - 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

預約掃瞄：「處理行動」標籤

在「處理行動」標籤中，設定 Apex One (Mac) 對偵測到的安全威脅所執行的中毒處理行動。

程序

1. 在「處理行動」下，指定中毒處理行動。

選項	說明
使用主動式處理行動	「主動式處理行動」是一套預先設定的中毒處理行動，可以處理各種類型的安全威脅。如果不確定某個特定安全威脅類型適合採用哪種中毒處理行動，趨勢科技建議您使用「主動式處理行動」。 「主動式處理行動」設定會在特徵碼檔案中持續更新，以保護端點抵禦最新的安全威脅和最新的攻擊方法。
對所有安全風險類型都使用相同的處理行動	如果您要對「可能的病毒/惡意程式」以外的所有安全威脅類型執行相同的處理行動，請選取此選項。對於「可能的病毒/惡意程式」，處理行動一律為「暫不處理」。 若您選擇「清除」做為第一個處理行動，請選取清除未成功時 Apex One (Mac) 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。 如需有關中毒處理行動的詳細資訊，請參閱中毒處理行動 第 20-10 頁。

2. 在「預約掃瞄權限」下，指定使用者是否可延後或略過預約掃瞄。

權限	說明
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。 設定對應於下列項目的時數和分鐘數： • 延後時間長度上限 • 掃瞄重新開始之前應該經過的時間長度上限
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

3. 在「預約掃瞄設定」下，指定通知和電池電量設定。

設定	說明
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」前數分鐘會在端點上顯示通知訊息。這時使用者會收到有關掃瞄預約時程（日期與時間）及其「預約掃瞄」權限（例如：延後、略過，或是停止預約掃瞄）的通知。 設定顯示通知訊息的時機（以分鐘為單位）。
當掃瞄時間超過 __ 小時又 __ 分鐘時，自動停止預約掃瞄	用戶端會在超過指定的時間長度而掃瞄尚未完成時停止掃瞄。若在掃瞄期間偵測到任何安全威脅，用戶端會立即通知使用者。
無線端點的電池電力剩餘時間若少於 __ %，而且已拔掉 AC 電源轉接器，則略過「預約掃瞄」	如果 Apex One (Mac) 偵測到無線端點的電池電力不足，並且其 AC 電源轉接器並未連接至任何電源時，則會略過「預約掃瞄」。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。若掃瞄進行時電池電力不足，則此掃瞄並不會終止。

支援的壓縮檔類型

Apex One (Mac) 支援下列壓縮類型。

副檔名	類型
.zip	由 Pkzip 建立的封存檔
.rar	由 RAR 建立的封存檔
.tar	由 Tar 建立的封存檔
.arj	ARJ 壓縮的封存檔
.hqx	BINHEX
.gz；.gzip	Gnu ZIP
.Z	LZW/壓縮的 16 位元
.bin	MacBinary
.cab	Microsoft 封包檔
Microsoft 壓縮/MSCOMP	
.eml；.mht	MIME
.td0	Teledisk 格式
.bz2	Unix BZ2 Bzip 壓縮檔
.uu	UUEncode
.ace	WinAce

中毒處理行動

指定特定掃瞄類型偵測到安全威脅時，Apex One (Mac) 執行的處理行動。

Apex One (Mac) 執行的處理行動視偵測到安全威脅的掃瞄類型而定。例如，當 Apex One (Mac) 在手動掃瞄（掃瞄類型）期間偵測到安全威脅，將會清除（處理行動）中毒檔案。

下列是 Apex One (Mac) 可以針對安全威脅執行的處理行動：

中毒處理行動	詳細資訊
刪除	Apex One (Mac) 從端點移除中毒檔案。
隔離	Apex One (Mac) 重新命名中毒檔案，再將其移至端點上的隔離目錄中，此目錄位於 <用戶端安裝資料夾>/common/lib/vsapi/quarantine。 進入隔離目錄後，Apex One (Mac) 可以根據使用者指定的處理行動，對隔離的檔案執行另一個處理行動。Apex One (Mac) 可以刪除、清除或恢復該檔案。恢復檔案意味著將檔案移回其原始位置而不執行任何處理行動。使用者可以恢復實際上無害的檔案。清除檔案意味著從隔離的檔案中移除安全威脅，如果清除成功，就將檔案移至原始位置。
清除	Apex One (Mac) 從中毒檔案中移除安全威脅，然後再允許使用者存取該檔案。 如果無法清除檔案，Apex One (Mac) 會執行第二個處理行動，可能是下列其中一個處理行動：「隔離」、「刪除」與「暫不處理」。如果要設定第二個處理行動，請瀏覽至「用戶端管理 > 設定 > {掃瞄類型}」，然後按一下「處理行動」標籤。
暫不處理	Apex One (Mac) 對中毒檔案不執行任何處理行動，但會將偵測到的安全威脅記錄在記錄檔中。檔案會留在其所在的位置。 Apex One (Mac) 對感染有「可能的病毒/惡意程式」類型的檔案一律執行「暫不處理」，以減輕誤判情況。如果進一步的分析確認可能的病毒/惡意程式確實是安全威脅，將會發行新的病毒碼，讓 Apex One (Mac) 可以執行適當的中毒處理行動。如果可能的病毒/惡意程式實際上是無害時，系統將不會再偵測。 例如：Apex One (Mac) 偵測到名為 "123.pdf" 的檔案含有 "x_probable_virus"，並在偵測時不執行任何處理行動。接著趨勢科技確認 "x_probable_virus" 是一種特洛伊木馬程式，並發行新的病毒碼版本。在載入新的病毒碼後，Apex One (Mac) 會將 "x_probable_virus" 偵測為特洛伊木馬程式，如果對這類程式的處理行動是「刪除」，那麼就會刪除 "123.pdf"。

用於掃瞄的快取設定

每次掃瞄執行時，用戶端都會檢查已修改的檔案快取，以查明檔案自上次用戶端啟動後是否有所修改。

- 如果某個檔案已被修改，則用戶端會掃瞄該檔案，並將其新增至已掃瞄的檔案快取中。
- 如果某個檔案未被修改，則用戶端會檢查該檔案是否在已掃瞄的檔案快取中。
    - 如果檔案在已掃瞄的檔案快取中，則用戶端會略過掃瞄該檔案。
    - 如果檔案不在已掃瞄的檔案快取中，則用戶端會檢查核可的檔案快取。

    注意

    核可的檔案快取包含 Apex One (Mac) 認為可信的檔案。這些可信的檔案均經過連續幾版病毒碼的掃瞄，且每次掃瞄後都被宣告不存在安全威脅，或為長期維持未修改狀態且不存在安全威脅的檔案。

    - 如果檔案在核可的檔案快取中，則用戶端會略過掃瞄該檔案。
    - 如果檔案不在核可的檔案快取中，則用戶端會掃瞄該檔案，並將其新增至已掃瞄的檔案快取中。

每當掃瞄引擎或病毒碼更新之後，會清除全部或部分快取。

如果掃瞄頻繁執行，且大量檔案與快取相符，會大幅縮短掃瞄時間。

如果掃瞄不常執行，請關閉快取，以使每次掃瞄都檢查檔案是否存在安全威脅。

掃瞄例外

設定掃瞄例外可提高掃瞄效能，並略過掃瞄已知無害的檔案。當特定的掃瞄類型執行時，Apex One (Mac) 會檢查掃瞄例外清單，來判斷不掃瞄端點上的哪些檔案。

掃瞄例外清單	詳細資訊
檔案	符合下列情況時，Apex One (Mac) 不會掃瞄檔案： • 檔案位於掃瞄例外清單中指定的目錄路徑底下 • 檔案符合掃瞄例外清單中指定的完整檔案路徑（目錄路徑和檔案名稱）
副檔名	如果檔案的副檔名符合此例外清單中包含的任何副檔名，Apex One (Mac) 便不會掃瞄該檔案。

設定掃瞄例外清單

如需有關掃瞄例外清單的詳細資訊，請參閱掃瞄例外 第 20-22 頁。

程序

1. 選取核取方塊以啟動掃瞄例外。
2. 如果要設定「掃瞄例外清單 (檔案)」，請執行下列作業：
   a. 輸入完整檔案路徑或目錄路徑，然後按一下「新增」。

      提醒：

      - 不能只輸入檔案名稱。
      - 您最多可以指定 64 個路徑。如需範例，請參閱下表。

路徑	詳細資訊	範例

完整檔案路徑	排除端點上的特定檔案	• 範例 1：
		`/file.log`
		• 範例 2：
		`/System/file.log`

路徑	詳細資訊	範例

目錄路徑	排除位於特定資料夾及其所有子資料夾中的所有檔案	• 範例 1：
		`/System/`
		不予掃瞄的檔案範例：
		• `/System/file.log`
		• `/System/Library/file.log`
		要掃瞄的檔案範例：
		• `/Applications/file.log`
		• 範例 2：
		`/System/Library`
		不予掃瞄的檔案範例：
		• `/System/Library/file.log`
		• `/System/Library/Filters/file.log`
		要掃瞄的檔案範例：
		• `/System/file.log`

- 使用星號萬用字元 (*) 取代資料夾名稱。

  如需範例，請參閱下表。

路徑	萬用字元用法範例
完整檔案路徑	`/Users/Mac/*/file.log` 不予掃瞄的檔案範例： • `/Users/Mac/Desktop/file.log` • `/Users/Mac/Movies/file.log` 要掃瞄的檔案範例： • `/Users/file.log` • `/Users/Mac/file.log`

目錄路徑	• 範例 1：
	`/Users/Mac/*`
	不予掃瞄的檔案範例：
	• `/Users/Mac/doc.html`
	• `/Users/Mac/Documents/doc.html`
	• `/Users/Mac/Documents/Pics/pic.jpg`
	要掃瞄的檔案範例：
	• `/Users/doc.html`
	• 範例 2：
	`/*/Components`
	不予掃瞄的檔案範例：
	• `/Users/Components/file.log`
	• `/System/Components/file.log`
	要掃瞄的檔案範例：
	• `/file.log`
	• `/Users/file.log`
	• `/System/Files/file.log`

- 不支援部分比對資料夾名稱。例如，不能輸入 `/Users/*user/temp` 來排除名稱以 user 為結尾之資料夾（例如 end_user 或 new_user）中的檔案。

b. 如果要刪除某個路徑，請選取該路徑，然後按一下「移除」。

3. 如果要設定「掃瞄例外清單 (副檔名)」，請執行下列作業：

a. 輸入不含句點 (.) 的副檔名，然後按一下「新增」。例如，輸入 `pdf`。您最多可以指定 64 個副檔名。

b. 如果要刪除某個副檔名，請選取該副檔名，然後按一下「移除」。

用戶端自我保護

用戶端自我保護功能可防止其他程式、甚至可防止使用者修改或刪除 Security Agent 所使用的檔案。

當您啟動「保護用戶端所用的檔案」，且 Security Agent 正在端點上執行時，Apex One (Mac) 會鎖定下列檔案和資料夾：

- /Library/Application Support/TrendMicro/common
- /Library/Application Support/TrendMicro/Kext
- /Library/Application Support/TrendMicro/TmccMac
- /Library/Application Support/TrendMicro/TmccUpdate
- /Library/Application Support/TrendMicro/Plug-in
- /Library/Application Support/TrendMicro/Tools
- /Library/LaunchDaemons/com.trendmicro.icore.*
- /Library/LaunchDaemons/com.trendmicro.tmsm.plugin.plist
- /Library/LaunchDaemons/com.trendmicro.tmsm.launcher.plist
- /Application/TrendMicroSecurity.app

注意

Apex One (Mac) 允許您在 /Library/Application Support/TrendMicro/Tools 資料夾中新增檔案，但無法將這些檔案從此資料夾中刪除。

用戶端更新

為確保 Security Agent 能夠持續抵禦最新安全威脅，請定期更新代理程式元件。當元件嚴重過期或每當病毒爆發時，也請更新 Security Agent。如果 Security Agent 長期無法從 Apex One (Mac) 伺服器或主動式更新伺服器進行更新，元件就會嚴重過期。

用戶端更新方法

有許多方法可以更新用戶端。

更新方式	說明
管理員啟動的手動更新	從下列 Web 主控台畫面啟動更新： • 「用戶端管理」畫面。 • 「摘要」畫面。
自動更新	• 在伺服器完成更新後，伺服器會立即通知 Security Agent 進行更新。 • 系統會根據您設定的預約時程執行更新。您可以設定一個預約時程，此預約時程會套用至一或多個 Security Agent 和網域，或是套用至伺服器管理的所有 Security Agent。 如需詳細資訊，請參閱設定用戶端更新設定 第 20-29 頁。
使用者啟動的手動更新	使用者在其端點上啟動更新。

用戶端更新來源

依預設，Security Agent 會從 Apex One (Mac) 伺服器下載元件。除了元件之外，Security Agent 還會在從 Apex One (Mac) 伺服器更新時接收組態設定檔。Security Agent 需要使用這些組態設定檔來套用新設定。每一次您在 Web 主控台上修改 Apex One (Mac) 設定時，組態設定檔都會變更。

在更新 Security Agent 之前，請檢查 Apex One (Mac) 伺服器是否有最新元件。

如果 Apex One (Mac) 伺服器無法使用，請將一個、多個或全部 Security Agent 設定為從趨勢科技主動式更新伺服器下載。

如需詳細資訊，請參閱設定用戶端更新設定 第 20-29 頁。

注意

如果用戶端只有 IPv6 位址，請閱讀純 IPv6 用戶端的限制 第 20-28 頁中有關用戶端更新的 IPv6 限制。

用戶端更新注意事項與提醒

- Security Agent 可以在更新期間使用 Proxy 伺服器設定。請在 Security Agent 主控台中設定 Proxy 伺服器設定。
- 在更新期間，端點的功能表列上的 Security Agent 圖示會指出產品正在進行更新。如果 Security Agent 程式有升級可用，Security Agent 會先進行更新，然後升級至最新的程式版本或 Build。在更新完成之前，使用者無法從主控台執行任何工作。
- 請存取「摘要」畫面，以檢查所有 Security Agent 是否均已更新。

純 IPv6 用戶端的限制

下表列出 Security Agent 只有 IPv6 位址時所存在的限制。

表 20-4. 純 IPv6 用戶端的限制

項目	限制
父伺服器	純 IPv4 用戶端無法由純 IPv6 伺服器管理。
更新	純 IPv6 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 Apex One (Mac) 伺服器

項目	限制
網頁信譽評等查詢	純 IPv6 用戶端無法將網頁信譽評等查詢傳送到趨勢科技主動式雲端截毒技術。
Proxy 伺服器連線	純 IPv6 用戶端無法透過純 IPv4 Proxy 伺服器進行連線。
部署用戶端	Apple Remote Desktop 無法將用戶端部署到純 IPv6 端點，因為這些端點永遠顯示為離線。

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。請將 Proxy 伺服器置於用戶端與它們連線的實體之間。

設定用戶端更新設定

如需用戶端更新的詳細說明，請參閱用戶端更新 第 20-27 頁。

程序

1. 選取「用戶端無法連線至 Apex One (Mac) 伺服器時，從趨勢科技主動式更新伺服器下載更新」，可允許用戶端從趨勢科技主動式更新伺服器下載更新。

   注意

   如果 Security Agent 只具有 IPv6 位址，請閱讀純 IPv6 用戶端的限制 第 20-28 頁以瞭解用戶端更新的 IPv6 限制。

2. 選取「用戶端可更新元件，但無法升級用戶端程式或安裝 HotFix」，可允許繼續更新元件，但會阻止用戶端升級。

3. 若要設定預約更新，請完成下列步驟：

   a. 選取「啟動預約更新」。

   b. 設定預約時程。

   c. 如果您選取「每日一次」或「每週一次」，請指定更新時間，以及 Apex One (Mac) 伺服器會通知 Security Agent 更新元件的時間範圍。例

如，如果開始時間為中午 12 點且時間範圍為 2 小時，則伺服器會在中午 12 點到下午 2 點之間隨機通知所有線上 Security Agent 來更新元件。這個設定可以避免所有線上 Security Agent 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流量。

網站信譽評等服務

網站信譽評等服務技術會依據諸如網站的存在時間長短、位置變更記錄，以及透過惡意程式行為分析所發現的可疑活動指標等因素來指定信譽評等評分，以追蹤 Web 網域的可信度。然後它就會繼續掃瞄網站，並阻擋使用者存取中毒的網站。

用戶端會將查詢傳送到主動雲端截毒技術來源，來判斷使用者正在嘗試存取之網站的信譽。網站的信譽和端點上實施的特定網頁信譽評等策略相關聯。根據使用中的策略而定，用戶端會封鎖或允許對網站的存取。

注意

此功能支援 2014 年 4 月之後發行的最新 Safari™、Mozilla™、Firefox™ 和 Google Chrome™ 瀏覽器。

設定網頁信譽評等設定

網站信譽評等服務設定中的策略會指定 Apex One (Mac) 是否要封鎖還是允許對網站的存取。為了判定應使用的適當策略，Apex One (Mac) 會檢查用戶端的位置。如果用戶端可以連線至 Apex One (Mac) 伺服器，則用戶端的位置是「內部」。否則，用戶端的位置就是「外部」。

程序

1. 如果要設定外部 Security Agent 的策略，請執行下列作業：
   a. 按一下「外部用戶端」標籤。

b. 選取「啟動網頁信譽評等策略」。

啟動此策略後，外部 Security Agent 會將網頁信譽評等查詢傳送至主動式雲端截毒技術。

注意

如果用戶端只具有 IPv6 位址，請閱讀純 IPv6 用戶端的限制 第 20-28 頁以瞭解網頁信譽評等查詢的 IPv6 限制。

c. 選取可用的網站信譽評等服務安全層級：「高」、「中」或「低」

注意

由安全層級來決定 Apex One (Mac) 是允許還是封鎖對 URL 的存取。例如，如果您將安全層級設定為「低」，Apex One (Mac) 只會封鎖已知為網頁威脅的 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。

d. 如果要送出網站信譽評等服務的意見反應，請按一下所提供的 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。

2. 如果要設定內部 Security Agent 的策略，請執行下列作業：

a. 按一下「內部用戶端」標籤。

b. 選取「啟動網頁信譽評等策略」。

啟動此策略後，內部 Security Agent 會將網頁信譽評等查詢傳送至以下項目：

- 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。
- 主動式雲端截毒技術，如果關閉了「傳送查詢至主動式雲端截毒技術伺服器」選項。

注意

如果用戶端只具有 IPv6 位址，請閱讀純 IPv6 用戶端的限制 第 20-28 頁以瞭解網頁信譽評等查詢的 IPv6 限制。

c. 如果您希望內部 Security Agent 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，Security Agent 會參考 Apex One Security Agent 所用的同一個主動式雲端截毒技術來源清單，來判定應該將查詢傳送至哪些主動式雲端截毒技術伺服器。
   - 如果您關閉此選項時，Security Agent 會將網頁信譽評等查詢傳送至主動式雲端截毒技術。端點必須連線至 Internet 才能成功傳送查詢。

d. 選取可用的網站信譽評等服務安全層級：「高」、「中」或「低」

注意

由安全層級來決定 Apex One (Mac) 是允許還是封鎖對 URL 的存取。例如，如果您將安全層級設定為「低」，Apex One (Mac) 只會封鎖已知為網頁威脅的 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。

Security Agent 不會封鎖未測試的網站，不論其安全層級為何。

e. 如果要送出網站信譽評等服務的意見反應，請按一下所提供的 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。

f. 選取是否允許 Security Agent 將網頁信譽評等記錄檔傳送至伺服器。如果您想分析 Apex One (Mac) 所封鎖的 URL，並針對您認為可以安全存取的 URL 採取合適的處理行動，請允許 Security Agent 傳送記錄檔。

設定核可和封鎖的 URL 清單

將您認為安全或危險的網站新增到核可清單或封鎖清單。Apex One (Mac) 在偵測到對任何這些網站的存取時，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來源。

程序

1. 存取 Apex One (Mac) Web 主控台。
2. 瀏覽至「用戶端 > 全域用戶端設定 > 網站信譽評等服務核可/封鎖的 URL 清單」。
3. 在文字方塊中指定 URL。您可在 URL 中的任何位置加入萬用字元 (*)。

   範例：

   - `www.trendmicro.com/*` 表示 www.trendmicro.com domain 網域中的所有網頁。
   - `*.trendmicro.com/*` 表示 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，請使用方括號括住該位址。
4. 請點選「新增到核可清單」或「新增到封鎖清單」。
5. 如果要刪除某個項目，請從「檢視」下拉式清單中選取一個選項，然後按一下 URL 旁的圖示。
6. 按一下「部署」。

周邊設備存取控管

「周邊設備存取控管」會規範對連線到端點的外部儲存裝置與網路資源的存取。周邊設備存取控管有助於防止資料遺失與外洩，並且可與檔案掃瞄搭配使用，以協助防禦安全威脅。

您可以設定內部和外部用戶端的周邊設備存取控管策略。管理員通常會針對外部用戶端設定較嚴格的策略。

策略是用戶端樹狀結構中精細的設定。您可以針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。

設定周邊設備存取控管設定

程序

1. 請點選「外部用戶端」標籤以設定外部用戶端的設定，或請點選「內部用戶端」標籤以設定內部用戶端的設定。
2. 選取「啟動周邊設備存取控管」。
3. 在「裝置」下，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 20-34 頁。
4. （選用）如果 USB 儲存裝置的權限為「封鎖」，您可以在「USB 儲存裝置核可清單」下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。

   a. 輸入裝置廠商。

   b. 輸入裝置型號和序號 ID。

   c. 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 20-34 頁。

   注意

   核可清單上的 USB 儲存裝置必須擁有比「裝置」區段中 USB 儲存裝置的權限設定更高的權限層級。
5. 在「通知」下，選取「偵測到新裝置時，於用戶端端點上顯示通知訊息」選項，以在新儲存裝置連線至端點時顯示通知。該通知會指出新儲存裝置的存取權限。
6. 按一下「部署」。

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、SD 卡、網路磁碟機和 Thunderbolt SATA 儲存裝置。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 20-5. 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。
唯讀	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
封鎖	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 Finder）。	禁止的作業：儲存、移動、複製

注意

唯讀權限不適用於網路磁碟機。

Endpoint Sensor

Endpoint Sensor 是功能強大的監控和調查工具，用於識別安全威脅是否存在、其位置以及進入點。透過使用詳細的系統事件記錄和歷史分析，您可以執行初步調查來探索隱藏在您整個網路中的安全威脅，並找出所有受影響的端點。產生根本原因分析報告可瞭解安全威脅進入端點之後惡意程式的性質及活動。

您也可以過使用共用的 IOC 檔案和 YARA 規則來執行詳細調查。詳細調查會對端點進行深入的即時搜尋，以找出先前未識別的安全威脅，以及可能的「進階持續安全威脅」攻擊。

設定 Endpoint Sensor 設定

重要

Endpoint Sensor 功能需要特殊的使用授權。將 Endpoint Sensor 策略部署到端點之前，請確保您擁有正確的使用授權。如需有關如何取得使用授權的詳細資訊，請洽詢您的支援供應商。

程序

1. 選取「啟動 Endpoint Sensor」。
2. 選取「啟動事件記錄」，以開始收集用戶端端點上的系統事件記錄檔。

   執行調查時，Endpoint Sensor 會使用詳細的事件記錄檔來識別有風險的端點。識別出受影響的 Windows 端點後，您可以執行深入的根本原因分析，以更好地瞭解可能的攻擊媒介。

選項	說明
資料庫大小上限	指定 Endpoint Sensor 將事件記錄檔儲存到端點時可使用的資料庫大小上限。一旦用戶端資料庫達到這個大小上限，Endpoint Sensor 就會清除最舊的記錄檔，以釋放空間給新的事件項目。

選項	說明
傳送一小部分的記錄檔資料來執行初步評估	傳送到伺服器的資訊由中繼資料組成（例如，端點上的網域、檔案或程序）。在初步評估期間，Endpoint Sensor 會利用上述資料來識別受影響的端點。 • 上傳頻率：指定用戶端將中繼資料上傳至 Apex Central 伺服器的頻率。 注意 視網路而定，上傳太過頻繁可能會影響網路效能。
啟動「攻擊發現」以在端點上偵測已知的攻擊指標	「攻擊發現」會根據攻擊指標 (IoA) 行為來使用趨勢科技安全威脅資訊。在偵測到已知的 IoA 之後，「攻擊發現」便會記錄該偵測。

信任的程式清單

在「即時掃瞄」和事件記錄期間，您可以將 Security Agent 設定為不掃瞄信任的程序。將程式新增到「信任的程式清單」後，Security Agent 不再對由該程式啟動的程式或任何程序執行「即時掃瞄」和事件記錄。將信任的程式新增到「信任的程式清單」，以提升端點上的掃瞄效能。

注意

如果符合下列需求，則您可以將檔案新增到「信任的程式清單」中：

- 檔案位於系統目錄以外的位置。
- 檔案擁有有效的數位簽章。

將程式新增到「信任的程式清單」後，Security Agent 會自動從下列作業中排除該程式：

- 即時掃瞄檔案檢查

- 即時掃瞄處理程序掃瞄
- 事件記錄

設定信任的程式清單

「信任的程式清單」不包括程式以及程式從即時掃瞄呼叫的所有子程序。

程序

1. 輸入要從清單中排除之程式的完整程式路徑。
2. 按一下「+ 新增」。
3. 如果要從清單中移除程式，請點選「刪除」圖示。

Machine Learning 設定

趨勢科技 Machine Learning 採用進階機器學習技術來關聯安全威脅資訊，並執行深度檔案分析來偵測新興的未知安全威脅，這透過數位 DNA 指紋、API 對應和其他檔案特徵來實現。Machine Learning 還會對未知或不太普遍的處理程序執行行為分析，以確定是否有新興或未知安全威脅正企圖讓您的網路中毒。

Machine Learning 是一個功能強大的工具，可協助保護您的環境，使其免遭不明安全威脅和零時差攻擊。

若要啟動此功能，請選取「啟動 Machine Learning」。

索引

D

Data Discovery, 18-2
    建立策略, 18-2
Data Loss Prevention, 16-2
    系統和應用程式通道, 16-8
    處理行動, 16-9
    解壓縮規則, 16-15
    網路通道, 16-6, 16-7, 16-12 – 16-14
DSP, 11-8

I

IPv6 支援
    限制, 20-28

S

Security Agent
    處理程序, 5-12
    登錄機碼, 5-11
    檔案, 5-11

W

Widget, 1-2
wildcards（萬用字元）
    周邊設備存取控管, 11-7, 11-8

四畫

不受監控的目標, 16-13, 16-15
不受監控的電子郵件網域, 16-7
元件
    在更新代理程式上, 5-15
手動掃瞄, 8-4
文件, viii

五畫

主動式處理行動, 8-31
用戶端自我保護, 5-10
用於掃瞄的快取設定, 5-12
目標, 2-19
    已部署, 2-19
    依條件過濾, 2-3
    具有問題, 2-20
    暫停中, 2-19
    瀏覽, 2-9
    離線, 2-19
立即掃瞄, 8-17

六畫

安全威脅偵測標籤, 1-36
有問題的目標, 2-20
行為監控
    系統事件的處理行動, 7-6
    例外清單, 7-7

七畫

刪除策略, 2-16
即時掃瞄, 8-9
更新
    更新代理程式, 5-15
更新代理程式, 5-15
系統和應用程式通道, 16-8

八畫

事件監控, 7-5
依要求掃瞄快取, 5-13
依條件過濾, 2-3
例外清單, 7-7
    行為監控, 7-7
受監控的目標, 16-14, 16-15
受監控的電子郵件子網域, 16-7
周邊設備存取控管, 11-2, 11-5, 11-7, 11-8, 20-33, 20-34

wildcards（萬用字元）, 11-7, 11-8
需求, 11-2
數位簽章提供者, 11-8
儲存裝置, 11-5, 20-34
權限, 11-5, 11-7, 20-34
程式路徑和名稱, 11-7

九畫

封鎖的程式清單, 7-7
建立策略, 2-2, 2-15
設定, 2-3
複製設定, 2-11
指定目標
瀏覽, 2-9
指定策略, 2-3
優先順序, 2-8
重新排序策略, 2-20

十畫

核可的程式清單, 7-7
核可清單, 12-2

十二畫

草稿策略, 2-3

十一畫

掃瞄方法
切換掃瞄方法, 8-2
雲端截毒掃瞄, 8-2
標準掃瞄, 8-2
掃瞄快取, 5-12
掃瞄例外, 8-39
掃瞄類型, 20-6
產品範圍
Widget, 1-5
符合性標籤, 1-31

九畫

處理行動
Data Loss Prevention, 16-9

十一畫

部署的目標, 2-19

十二畫

惡意程式行為封鎖, 7-2
策略
Data Discovery, 18-2
刪除, 2-16
建立, 2-2, 2-15
重新排序, 2-20
編輯, 2-14
策略目標, 2-19
策略清單, 2-6, 2-18
策略設定
複製, 2-11
策略管理, 2-1, 2-2
目標, 2-19
有問題的目標, 2-20
刪除策略, 2-16
建立策略, 2-2, 2-15
指定策略, 2-3
重新排序策略, 2-20
草稿策略, 2-3
設定, 2-3
部署的目標, 2-19
策略清單, 2-6, 2-18
策略優先順序, 2-8, 2-18
暫停中的目標, 2-19
編輯策略, 2-14
複製策略設定, 2-11
擁有者, 2-19
瞭解, 2-2
離線目標, 2-19

變更擁有者, 2-17
策略優先順序, 2-18
策略類型
指定, 2-3
重新排序策略, 2-20
草稿, 2-3
策略優先順序, 2-18
詞彙, x

十一畫
郵件掃瞄, 5-14

十二畫
間諜程式/可能的資安威脅程式掃瞄
核可清單, 12-2
雲端截毒掃瞄, 20-2, 20-3
從傳統掃瞄切換過來, 20-3

十三畫
傳統掃瞄, 20-2, 20-3
切換至雲端截毒掃瞄, 20-3
裝置清單工具, 16-9
解除安裝
使用解除安裝程式, 5-7
解壓縮規則, 16-15
資料安全防護, 16-2
資訊中心
Widget, 1-2
修改產品範圍, 1-5
移動, 1-4
新增, 1-4
標籤, 1-2
刪除, 1-3
投影片放映, 1-2
重新命名, 1-2
新增, 1-2
摘要, 1-14
過濾策略
重新排序, 2-20
隔離目錄, 8-33
電子郵件網域, 16-7
預約掃瞄, 8-23

十四畫
摘要標籤, 1-14
監控的系統事件, 7-5
監控的系統事件的處理行動, 7-6
網頁信譽評等, 9-2
網站信譽評等服務, 20-30
網路通道, 16-6, 16-7, 16-12 – 16-14
不受監控的目標, 16-12
受監控的目標, 16-12
傳輸範圍
外部傳輸, 16-14
所有傳輸, 16-13
傳輸範圍和目標, 16-6
電子郵件用戶端, 16-7

十五畫
數位簽章快取, 5-13
數位簽章特徵碼, 5-13
數位簽章提供者, 11-8
指定, 11-8
暫停中的目標, 2-19
標籤, 1-2
Widget, 1-2
安全威脅偵測, 1-36
符合性, 1-31
摘要, 1-14
編輯策略, 2-14
複製策略設定, 2-11

十六畫
選取目標

依條件過濾, 2-3

十八畫
儲存裝置
權限, 11-5, 20-34

十七畫
壓縮檔
解壓縮規則, 16-15

十八畫
瀏覽目標, 2-9

十九畫
離線目標, 2-19

二十二畫
權限
卸載權限, 5-7
程式路徑和名稱, 11-7
郵件掃瞄權限, 5-14
儲存裝置, 11-5, 20-34

TREND MICRO™

趨勢科技股份有限公司
台北市敦化南路二段 198 號 8 樓
電話：(886) 2-23789666　傳真：(886) 2-23780993　info@trendmicro.com

www.trendmicro.com

Item Code: APTM08533/181106