Trend Micro Apex Central™

Patch 4

管理員指南

集中管理端點的安全

Trend Micro Incorporated / 趨勢科技股份有限公司保留變更此文件與此處提及之產品的權利，恕不另行通知。安裝及使用產品之前，請先閱讀 Readme 檔、版本資訊和/或適用的最新版文件。您可至 Trend Micro 網站取得上述資訊：

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

Trend Micro、Trend Micro t-ball 標誌、Trend Micro Apex Central、Trend Micro Apex One、Control Manager 和 OfficeScan 是 Trend Micro Incorporated / 趨勢科技股份有限公司 的商標或註冊商標。所有其他廠牌與產品名稱則為其個別擁有者的商標或註冊商標。

版權所有 © 2023。Trend Micro Incorporated / 趨勢科技股份有限公司。保留所有權利。

文件編號：APEM09683/230207

發行日期：2023 年 3 月

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

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

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

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

請至下列網站並給予您對此文件的評估意見：

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

隱私權資料和個人資料蒐集披露

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

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

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

趨勢科技所蒐集的資料將遵循趨勢科技隱私權注意事項中的規定：

https://www.trendmicro.com/privacy

目錄

序言

序言 xi
文件 xii
讀者 xiii
文件慣例 xiii
詞彙 xiv

部分 I：簡介

第 1 章：Apex Central 簡介

關於 Apex Central 1-2
新增功能 1-2
主要功能和優點 1-4
Apex Central 架構 1-6

部分 II：開始使用

第 2 章：Web 主控台

關於 Web 主控台 2-2
將 HTTPS 存取權指派給 Web 主控台 2-3
存取 Web 主控台 2-5
設定 Web 主控台設定值 2-7

第 3 章：資訊中心

關於資訊中心 3-2

標籤和 Widget 3-2
安全狀況標籤 3-6
摘要標籤 3-15
資料外洩防護標籤 3-25
符合性標籤 3-31
安全威脅統計資料標籤 3-36

第 4 章：帳號管理

使用者帳號 4-2
使用者角色 4-14

第 5 章：使用授權管理

Apex Central 啟動和使用授權資訊 5-2
受管理產品的啟動和註冊 5-3

第 6 章：Active Directory 和符合性設定

Active Directory 整合 6-2
符合性指標 6-6
端點和使用者分組 6-11

第 7 章：使用者/端點目錄

使用者/端點目錄 7-2
使用者詳細資料 7-3
端點詳細資料 7-9
Active Directory 詳細資料 7-18
受影響的使用者 7-18
使用進階搜尋 7-23
自訂標籤 (Tags) 和過濾器 7-27

部分 III：受管理產品整合

第 8 章：受管理產品註冊

受管理產品註冊方法 8-2
伺服器註冊 8-2
受管理產品的通訊 8-10

第 9 章：Security Agent 安裝

下載 Security Agent 安裝套件 9-2
Apex One Security Agent 系統需求 9-4
Apex One (Mac) Security Agent 安裝 9-25

第 10 章：產品目錄

產品目錄 10-2
檢視受管理產品狀態摘要 10-4
執行產品目錄的進階搜尋 10-5
執行受管理產品工作 10-7
設定受管理的產品設定 10-8
從產品目錄查詢記錄檔 10-9
目錄管理 10-10

第 11 章：元件更新

元件更新 11-2
設定預約更新設定 11-4
設定手動更新設定 11-8
設定用於元件/使用授權更新、雲端服務及 Syslog 轉送的 Proxy 伺服器設定 11-11

第 12 章：指令追蹤和產品通訊

指令追蹤 12-2

查詢及檢視指令 12-3

設定通訊逾時設定 12-4

部分 IV：策略

第 13 章：策略管理

策略管理 13-2

策略狀態 13-22

第 14 章：策略資源

Application Control 條件 14-2

資料外洩防護 14-14

入侵防護規則 14-31

周邊設備存取控管允許的裝置 14-35

部分 V：偵測

第 15 章：記錄檔

記錄查詢 15-2

查詢記錄檔 15-2

設定記錄檔彙整 15-12

設定 Syslog 轉送 15-13

刪除記錄檔 15-18

第 16 章：通知

事件通知 16-2

通知方法設定 16-3
聯絡人群組 16-6
進階安全威脅活動事件 16-9
內容策略違規事件 16-30
資料外洩防護事件 16-33
已知的安全威脅活動事件 16-42
網路存取控制事件 16-57
不尋常的產品行為事件 16-60
更新 16-67

第 17 章：報告

報告總覽 17-2
自訂範本 17-2
一次性報告 17-18
預約報告 17-22
設定報告維護 17-31
檢視我的報告 17-32

第 18 章：資料外洩防護事件

管理員工作 18-2
DLP 事件檢閱程序 18-6

部分 VI：安全威脅資訊與回應

第 19 章：連線的威脅防範

關於連線的威脅防範 19-2
功能需求 19-2
可疑物件清單管理 19-6

先發式可疑物件防護 19-19
連線的威脅防範產品整合 19-34

第 20 章：安全威脅調查

安全威脅調查總覽 20-2
歷史調查 20-3
即時調查 20-21
調查結果 20-30

第 21 章：Managed Detection and Response

Managed Detection and Response 總覽 21-2
追蹤 Managed Detection and Response 工作指令 21-15
查詢支援的目標 21-17
Managed Detection and Response 的安全威脅調查中心用戶端 21-19

第 22 章：可疑物件中樞和節點架構

可疑物件中樞和節點 Apex Central 伺服器 22-2
設定可疑物件中樞和節點 22-3
從中央 Apex Central 取消註冊可疑物件節點 22-4
組態設定注意事項 22-5

部分 VII：自動化中心

第 23 章：Apex Central 自動化中心

部分 VIII：工具和支援

第 24 章：管理資料庫

瞭解 Apex Central 資料庫 24-2

使用 SQL Server Management Studio 備份 db_ApexCentral .. 24-9

使用 SQL 指令壓縮 db_ApexCentral_Log.ldf 24-11

使用 SQL Server Management Studio 壓縮 db_ApexCentral_log.ldf 24-12

第 25 章：Apex Central 工具

關於 Apex Central 工具 25-2

使用用戶端移轉工具 (AgentMigrateTool.exe) 25-2

使用資料庫組態設定工具 (DBConfig.exe) 25-2

第 26 章：技術支援

疑難排解資源 26-2

聯絡趨勢科技 26-3

將可疑內容傳送到趨勢科技 26-4

其他資源 26-5

附錄

附錄 A：Apex Central 系統檢查清單

伺服器位址檢查清單 A-2

通訊埠檢查清單 A-3

Apex Central 慣例 A-3

核心處理程序和組態設定檔 A-4

通訊和監聽通訊埠 A-6

附錄 B：資料檢視

資料檢視：安全記錄檔 B-2
資料檢視：產品資訊 B-88

附錄 C：Token 變數

標準 Token 變數 C-2
進階安全威脅活動 Token 變數 C-2
攻擊發現 Token 變數 C-5
C&C 回呼 Token 變數 C-6
內容策略違規 Token 變數 C-8
資料外洩防護 Token 變數 C-9
已知的安全威脅活動 Token 變數 C-11
網路存取控制 Token 變數 C-13
Web 存取策略違規 Token 變數 C-14

附錄 D：IPv6 支援

Apex Central 伺服器需求 D-2
IPv6 支援限制 D-2
設定 IPv6 位址 D-2
顯示 IP 位址的畫面 D-3

附錄 E：MIB 檔案

使用 Apex Central MIB 檔案 E-2
使用 NVW Enforcer SNMPv2 MIB 檔案 E-2

附錄 F：Syslog 內容對應 — CEF

CEF 攻擊發現偵測記錄檔 F-3
CEF 行為監控記錄檔 F-9
CEF C&C 回呼記錄檔 F-14

CEF 內容安全記錄檔 F-19
CEF 資料外洩防護記錄檔 F-27
CEF 裝置存取控制記錄檔 F-35
CEF Endpoint Application Control 記錄檔 F-42
CEF 引擎更新狀態記錄檔 F-44
CEF 入侵防護記錄檔 F-46
CEF 受管理的產品登入/登出事件 F-49
CEF 網路內容檢測記錄檔 F-51
CEF 特徵碼更新狀態記錄檔 F-54
CEF Machine Learning 記錄檔 F-56
CEF 產品稽核事件 F-61
CEF 沙盒偵測記錄檔 F-63
CEF 間諜程式/可能的資安威脅程式記錄檔 F-66
CEF 可疑檔案記錄檔 F-74
CEF 病毒/惡意程式記錄檔 F-77
CEF Web 網頁安全記錄檔 F-82

索引

索引 IN-1

序言

序言

本文件介紹 Trend Micro Apex Central™，並討論使用資訊、受管理產品整合以及安全監控詳細資料。

本節涵蓋下列主題：

- 文件 第 xii 頁
- 讀者 第 xiii 頁
- 文件慣例 第 xiii 頁
- 詞彙 第 xiv 頁

文件

Apex Central 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
安裝和升級手冊	討論安裝 Apex Central 的需求與程序的 PDF 文件 注意 次要發行版本、Service Pack 和修補程式可能不提供《安裝和升級手冊》。
系統需求	討論安裝 Apex Central 的需求與程序的 PDF 文件
管理手冊	提供如何設定及管理 Apex Central 和受管理產品的詳細指示，以及說明 Apex Central 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 主控台存取的「說明」
Widget 和策略管理手冊	包含如何在 Apex Central 中對資訊中心 Widget 和策略管理進行設定的資訊說明 若要存取此手冊，請移至 https://docs.trendmicro.com/zh-tw/enterprise/trend-micro-apex-central-2019-widget-and-policy-management-guide/preface-(wpg)_001.aspx。
自動化中心	說明如何使用 Apex Central 自動化 API 的線上使用者手冊與參考：https://automation.trendmicro.com/apex-central/home
資料安全防護清單（僅第 1 章）	其中列出資料外洩防護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：https://success.trendmicro.com/tw/business-support

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-central.aspx

讀者

Apex Central 文件適用於下列使用者：

- Apex Central 管理員：負責安裝、設定及管理 Apex Central。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 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

慣例	說明
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 文件中使用的正式詞彙：

詞彙	說明
管理員（或 Apex Central 管理員）	管理 Apex Central 伺服器的人員
Security Agent	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 主控台、Web 主控台或管理主控台	用於存取、設定及管理 Apex Central 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 Security Agent 的端點
受管理的產品	與 Apex Central 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

詞彙	說明
伺服器	安裝了 Apex Central 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

Apex Central 簡介

本節介紹 Trend Micro Apex Central™，並提供其特性和功能的總覽。

包含下列主題：

- 關於 Apex Central 第 1-2 頁
- 新增功能 第 1-2 頁
- 主要功能和優點 第 1-4 頁
- Apex Central 架構 第 1-6 頁

關於 Apex Central

Trend Micro Apex Central™ 是一個 Web-based 主控台，可讓您在閘道、郵件伺服器、檔案伺服器和企業桌面層級上集中管理 Trend Micro 產品和服務。管理員可以使用策略管理功能，來設定產品設定並將其部署到受管理產品和端點。Apex Central Web-based 管理主控台提供單一監控點，來監控整個網路上的防毒和內容安全產品與服務。

Apex Central 可讓系統管理員監控感染、安全違規或病毒/惡意程式進入點等活動，並對這些活動進行報告。系統管理員可以在整個網路中下載並部署元件（例如：防毒病毒碼檔案、掃瞄引擎和垃圾郵件防護規則），以確保您擁有最新的安全防護。Apex Central 允許進行手動更新和預約更新，還允許您將產品視為群組或個體來設定和管理，以提升彈性。

新增功能

此版本的 Apex Central 包含下列新增和增強功能。

功能	說明
新平台	Apex Central 支援安裝於 Windows Server 2022。

表 1-1. 先前更新

功能	說明
事件通知	為防止將過多不必要的通知傳送給向收件者，已關閉下列事件通知設定（「偵測 > 通知 > 事件通知 > 進階安全威脅活動」）： • C&C 回呼警訊 • C&C 回呼病毒爆發警訊 • 關聯的事件偵測
其他進階安全威脅活動通知	Apex Central 支援針對行為監控違規和 Machine Learning 偵測發出「進階安全威脅活動」事件通知。

功能	說明
進階記錄策略最佳化	Apex One Vulnerability Protection 的「進階記錄策略」（策略 > 策略管理 > Apex One Security Agent > Vulnerability Protection 設定 > 網路引擎設定）預設使用「可設定狀態、片段與驗證器抑制」，以排除與片段和驗證器相關的事件。
並行作業階段限制	Apex Central 允許管理員禁止每個使用者帳號使用多個 Web 主控台作業階段。
嚴重事件稽核	Apex One 伺服器和 Security Agent 會蒐集與嚴重系統事件（移動 Security Agent、解除安裝 Security Agent、重設密碼）相關的 Windows 事件記錄檔，並將記錄檔傳送至 Apex Central 產品稽核事件記錄檔中。
資訊中心增強功能	• 「作業中心」標籤的名稱已變更為「安全狀況」；「安全威脅偵測」標籤的名稱已變更為「安全威脅統計資料」；先前位在「DLP 事件查詢」標籤的 Widget 已移至「資料外洩防護」標籤。 • 在「安全狀況」資訊中心標籤上切換「資料表」檢視，可在一個資料表中顯示圖表節點、嚴重安全威脅和防毒特徵碼符合性資訊。
增強的 API 整合	Apex Central 提供多個 API，用於將 CEF 格式的偵測記錄檔、產品稽核事件、Security Agent 病毒碼更新狀態或 Security Agent 引擎更新狀態轉送至 SIEM 伺服器。 如需詳細資訊，請參閱 https://automation.trendmicro.com/apex-central/home。
影響分析增強功能	執行影響分析時，「受影響的使用者」畫面會每 60 秒自動重新整理一次。
新的資訊中心 Widget	• 「快速調查」Widget 可讓您直接從資訊中心啟動歷史調查。 • 使用「攻擊發現偵測」Widget 可檢視 Endpoint Sensor「攻擊發現」功能所產生的偵測記錄檔。 「攻擊發現」記錄檔包含 MITRE™ 策略和技術資訊以及 Windows 反惡意程式碼掃瞄介面 (AMSI) 資料。 • 「前幾名受 IPS 事件影響的端點」、「最常見的 IPS 攻擊來源」和「最常見的 IPS 事件」Widget 可讓您對網路上的「入侵防護」事件一目瞭然。
密碼複雜度增強功能	• Apex Central 使用者帳號對密碼複雜度的要求較高。 • 「卸載並解除安裝 Security Agent」功能已納入增強的密碼複雜度要求，提供更強大的安全性。

功能	說明
還原策略繼承	「行為監控」、Machine Learning 和「信任的程式清單」等策略的增強功能提供策略繼承支援。
SQL Server 支援	Apex Central 支援 Microsoft SQL Server 2019 Cumulative Update 4 (CU4) 和 SQL Server Express CU4。
Syslog 增強功能	• Apex Central 允許您將「入侵防護」記錄檔和「產品稽核事件」記錄檔轉送至 Syslog 伺服器。 • 一般事件格式 (CEF) Syslog 會指出偵測到的嚴重安全威脅類型。
弱點修補	Apex Central 已修補跨網站程式檔 (XSS) 和 SQL 插入弱點。
Web 瀏覽器支援	Apex Central 支援 Microsoft Edge (Chromium)。

主要功能和優點

Apex Central 提供下列功能和優點。

功能	優點
Active Directory 整合	Apex Central 支援與多個 Active Directory 樹系整合，並且除了 Active Directory 使用者之外，還允許您匯入 Active Directory 群組。您還可以啟動 Active Directory 驗證，讓外部網路上的商業同盟合作夥伴的使用者或群組，安全地登入 Apex Central 主控台。
資訊中心	使用「資訊中心」標籤和 Widget，可全面洞悉受管理的產品和 Apex Central 資訊（包括安全威脅偵測、元件狀態、策略違規等）。
安全狀況	使用「安全狀況」標籤，可立即深入探索您網路中的防毒病毒碼和資料外洩防護符合狀態、嚴重安全威脅偵測，以及已解決和未解決的事件。
使用者/端點目錄	檢視 Apex Central 網路中所有使用者和端點及任何安全威脅偵測的詳細資訊。

功能	優點
產品目錄	在病毒/惡意程式爆發期間，系統管理員可以立即將組態設定修改部署到受管理產品，甚至會從 Apex Central Web 主控台執行手動掃瞄。
全域策略管理	系統管理員可以從單一管理主控台，使用策略來進行產品設定並將其部署到受管理產品和端點，以確保您組織的病毒/惡意程式和內容安全策略實施的一致性。
記錄檔	使用單一管理主控台可檢視所有已註冊受管理產品的彙總記錄檔，而不需要登入每一個個別產品主控台。
事件通知	將 Apex Central 設定為透過電子郵件傳送關於 Windows Syslog、SNMP Trap 或是您組織所使用的內部或產業標準應用程式的通知，讓管理員隨時掌握網路事件的動態。
報告	使用自訂或靜態範本建立全面的報告，以取得確保網路安全防護和安全性符合所需之可付諸行動的資訊。
元件更新	持續穩定下載及部署防毒病毒碼、垃圾郵件防護規則、掃瞄引擎，以及其他防毒或內容安全元件，協助您確保所有受管理產品都是最新的。
連線的威脅防範	Apex Central 整合了多種趨勢科技產品與解決方案，可協助您在目標式攻擊和進階安全威脅造成永久性損害之前進行偵測、分析及回應。
安全通訊基礎結構	Apex Central 使用奠基於 Secure Socket Layer (SSL) 通訊協定的通訊基礎結構，還會利用驗證來加密郵件。
以角色為基礎的管理	透過將特定的 Web 主控台權限指派給管理員，並只提供執行特定工作所需的工具和權限，來授與及控制 Apex Central Web 主控台的存取權。
指令追蹤	指令追蹤可讓您持續監控使用 Apex Central Web 主控台執行的指令（例如，防毒病毒碼更新和元件部署）是否成功完成。
使用授權管理	對受管理產品部署新的啟動碼，或重新啟動現有啟動碼。
Security Agent 安裝	直接從 Apex Central 主控台下載 Apex One 或 Apex One (Mac) 的 Security Agent 安裝套件。

功能	優點
雙因素驗證	「雙因素驗證」藉由要求使用者輸入 Google Authenticator 應用程式所產生的驗證碼以登入 Apex Central，為使用者帳號提供額外的安全性。
瀏覽器支援	此版本的 Apex Central 支援下列瀏覽器： • Microsoft™ Internet Explorer™ • Microsoft™ Edge™ • Microsoft™ Edge™ (Chromium) • Google™ Chrome™

Apex Central 架構

Trend Micro Apex Central™ 提供從一個集中位置控制 Trend Micro 產品和服務的方式。此應用程式可以簡化對於企業病毒/惡意程式及內容安全策略的管理。

下表說明 Apex Central 使用的元件。

元件	說明
Apex Central 伺服器	做為所有從用戶端收集之資料的存放區。Apex Central 伺服器提供下列功能： • SQL 資料庫，可儲存受管理產品的組態設定和記錄檔 Apex Central 使用 Microsoft SQL Server 資料庫 (db_ApexCentral.mdf) 來儲存記錄檔、受管理產品資訊、使用者帳號、網路環境和通知設定等資料。 • Web 伺服器，可代管 Apex Central Web 主控台 • 郵件用戶端，可透過電子郵件傳送事件通知 Apex Central 會將 Apex Central 網路上所發生事件的通知傳送給個別收件者或收件者群組。透過電子郵件、SNMP Trap、Syslog 或您組織用於傳送通知的內部/產業標準應用程式來傳送事件通知。 • 報告伺服器，可產生防毒和內容安全產品報告 Apex Central 報告是有關 Apex Central 網路中所發生安全威脅和內容安全事件的線上數字集合。
趨勢科技管理通訊協定	MCP 會處理 Apex Central 伺服器與支援新一代用戶端的受管理產品的互動。 MCP 代理程式隨受管理產品一起安裝，它使用單向/雙向通訊來與 Apex Central 進行通訊。MCP 代理程式會輪詢 Apex Central 是否有指令和更新。
Web 服務整合通訊	可讓 Apex Central 與受管理產品進行通訊的無用戶端整合模型
Web-based 管理主控台	可讓管理員從幾乎任何一台具有 Internet 連線和 Web 瀏覽器的電腦管理 Apex Central Apex Central 管理主控台是透過 Microsoft Internet Information Server (IIS) 在 Internet 上發佈，並且由 Apex Central 伺服器代管的 Web-based 主控台。它可讓您從任何使用相容 Web 瀏覽器的電腦管理 Apex Central 網路。
Widget 架構	可讓管理員建立自訂的資訊中心來監控 Apex Central 網路。

部分 II

開始使用

第 2 章

Web 主控台

本節討論如何存取及設定 Apex Central Web-based 管理主控台。

包含下列主題：

- 關於 Web 主控台 第 2-2 頁
- 將 HTTPS 存取權指派給 Web 主控台 第 2-3 頁
- 存取 Web 主控台 第 2-5 頁
- 設定 Web 主控台設定值 第 2-7 頁

關於 Web 主控台

Apex Central Web 主控台可針對所有受已向 Apex Central 伺服器註冊之趨勢科技產品保護的端點和使用者，提供集中式管理、監控，以及一目瞭然的安全狀態。主控台內有一組預設設定和預設值，您可根據這些安全需求和規定設定這些設定和值。Web 主控台可讓您從任何使用相容 Web 瀏覽器的電腦管理 Apex Central 網路。

注意

請以 1366 x 768 像素的螢幕解析度檢視 Web 主控台。

Apex Central 支援下列 Web 瀏覽器：

- Microsoft Internet Explorer™ 11
- Microsoft Edge™
- Microsoft Edge™ (Chromium)
- Google Chrome™

Web 主控台需求

資源	需求
處理器	300 MHz Intel™ Pentium™ 處理器或同級處理器
RAM	至少 128 MB
可用磁碟空間	至少 30 MB

資源	需求
瀏覽器	Microsoft Internet Explorer™ 11、Microsoft Edge™、Microsoft Edge™ (Chromium) 或 Google Chrome™ 重要 使用 Internet Explorer 存取 Apex Central Web 主控台時，請關閉「相容性檢視」。
其他	支援 1366 x 768 解析度（256 色）或以上的顯示器

將 HTTPS 存取權指派給 Web 主控台

在安裝 Apex Central 期間，您可以選擇使用哪個安全層級來存取管理主控台。使用 HTTP 連線的安全層級最低。使用 HTTPS 連線的安全性最高。如果在安裝期間選取安全性最低的連線，您可以在安裝完成後將存取層級變更為最安全的連線。

重要

- 您必須取得憑證並設定 Apex Central 虛擬目錄，然後才能開始向 Apex Central 伺服器傳送及從其接收加密或經過數位簽署的資訊。
- 下列程序說明如何從 Windows Server 2012 R2 安裝指派 HTTPS 存取權。

  如果您執行不同版本的 Windows Server，請參閱您的特定 Windows Server 安裝適用的 Microsoft 文件。

步驟

1. 從任何憑證提供者（例如 `Thawte.com` 或 `VeriSign.co`）取得「網站憑證」。
2. 登入 Apex Central 伺服器。
3. 移至「開始 > 系統管理工具 > Internet Information Services (IIS) 管理員」。

會出現「Internet Information Services (IIS) 管理員」畫面。

4. 從左側的「連線」窗格中選取伺服器名稱。
5. 從中間的「功能檢視」窗格中按兩下「伺服器憑證」。
6. 從右側的「動作」窗格中按一下「匯入...」。

   會出現「匯入憑證」畫面。
7. 匯入在步驟 1 中取得的網站憑證：
   a. 上傳憑證檔案。
   b. 指定憑證的密碼。
   c. 選取「憑證存放區」。
   d. 請點選「確定」。

      Windows Server 會匯入憑證檔案並關閉「匯入憑證」畫面。
8. 從左側的「連線」窗格中展開「站台」資料夾，然後選取在 Apex Central 安裝期間建立的「<網站>」。

注意

如果您在 Apex Central 安裝期間未指定自訂的「<網站>」名稱，則預設「<網站>」名稱為「預設網站」。

9. 以滑鼠右鍵按一下「<網站>」，然後選取「編輯繫結...」。

   會出現「站台繫結」畫面。
10. 設定站台繫結：
    a. 選取「https」類型，然後按一下「編輯...」。

秘訣

如果「站台繫結」清單中未出現「https」類型，請按一下「新增...」以手動新增「https」類型。

b. 從「SSL 憑證」下拉式清單中選取匯入的憑證檔案。

c. 請點選「確定」。

d. 請點選「關閉」。

11. 設定 SSL 設定：

a. 展開「<網站>」，然後選取「WebApp」虛擬目錄。

b. 從中間的「功能檢視」窗格中按兩下「SSL 設定」。

c. 選取「需要 SSL」。

d. 從右側的「動作」窗格中按一下「套用」。

會出現「警示」窗格，指出已成功儲存變更。

12. 請在以下位置指定 HTTPS 通訊埠號碼：

- 登錄機碼：

  `HKLM\Software\Wow6432Node\TrendMicro\TVCS\WebPort`

- 系統組態設定檔：

  在 `<Apex Central 安裝資料夾>\systemconfiguration.xml` 檔案中，找到 `m_uiWebServer_Https_Port` 並將值設定為 HTTPS 通訊埠號碼。

13. 重新啟動下列服務：

- Trend Micro Apex Central
- 趨勢科技管理基礎架構
- W3WP

存取 Web 主控台

從 Apex Central 伺服器或任何具有 Internet 存取權的端點和支援的 Web 瀏覽器登入 Apex Central 主控台。

注意

- 在同一個端點上，無法從多個瀏覽器使用相同的使用者帳號登入 Apex Central 管理主控台。
- 您可以在不同的端點上使用相同的使用者帳號登入 Apex Central 管理主控台。

步驟

1. 從本機或從遠端存取 Apex Central 管理主控台。
   - 如果要從本機存取主控台，請在 Apex Central 伺服器上移至「開始 > 程式集 > Trend Micro Apex Central > Trend Micro Apex Central」。
   - 如果要從遠端存取主控台，請開啟 Web 瀏覽器並前往下列位址：

     `http(s)://<主機名稱>/WebApp/login.html`

     其中 <主機名稱> 是完整的網域名稱 (FQDN)、IP 位址或 Apex Central 伺服器的伺服器名稱。

   會出現「登入」畫面。
2. 請提供登入認證。
   - 如果要使用 Apex Central 帳號認證登入，請輸入使用者名稱和密碼。
   - 如果要使用網域認證登入，請使用下列格式輸入網域和使用者名稱，然後輸入密碼。

     網域\使用者名稱

     注意

     使用網域認證登入需要整合式 Active Directory 結構。

     如需詳細資訊，請洽詢 Active Directory 管理員。
3. 按一下「登入」。

注意

如果您的管理員啟動了雙因素驗證，請遵循螢幕上的提示操作。

如需有關設定雙因素驗證的詳細資訊，請聯絡您的管理員。

4. （選用）使用網域認證登入時，可以按一下「使用網域認證登入」按鈕，將認證儲存起來供日後使用。

注意

僅當管理員已將 Apex Central 伺服器新增至 Active Directory 伺服器上的 Active Directory 網域時，才會顯示「使用網域認證登入」按鈕。

Apex Central 會提示您提供您的網域認證，並確認自動登入。下次存取主控台時，按一下「使用網域認證登入」即可自動登入。

5. 如果要從 Web 主控台登出，請移至 Web 主控台的右上角，然後按一下「<帳號名稱> > 登出」。

設定 Web 主控台設定值

請設定 Apex Central Web 主控台設定，以決定使用者存取 Web 主控台的方式，以及畫面重新整理的頻率。

步驟

1. 移至「管理 > 設定 > Web 主控台設定」。

   會出現「Web 主控台設定」畫面。

2. 設定必要的設定。

區段	設定
Web 主控台自動重新整理	選取「啟動自動重新整理」，可使 Apex Central 伺服器依照指定的時間間隔重新整理畫面資料 • 重新整理 Web 主控台，每隔：_ 秒：選取 Web 主控台重新整理畫面資料的頻率（以秒為單位）
Web 主控台逾時	選取「啟動自動登出 Web 主控台」，讓 Apex Central 伺服器依照指定的時間間隔將使用者登出 • 在經過 _ 分鐘後，自動登出 Web 主控台：：選取 Web 主控台在使用者閒置多長時間（以分鐘為單位）後自動將其登出
安全設定	選取「達到未成功的登入嘗試次數後，自動鎖定使用者帳號」，可使 Apex Central 伺服器鎖定未成功的登入嘗試達到指定次數的使用者帳號 • 連續未成功的嘗試次數：指定未成功的登入嘗試次數 • 帳號鎖定持續時間：指定鎖定使用者帳號的時間長度（以分鐘為單位）
並行作業階段限制	選取「按帳號強制執行一個作業階段」可禁止同一使用者帳號使用多個 Web 主控台登入作業階段

3. 按一下「儲存」。

第 3 章

資訊中心

本節討論如何使用 Apex Central 資訊中心標籤和 Widget。

包含下列主題：

- 關於資訊中心 第 3-2 頁
- 標籤和 Widget 第 3-2 頁
- 安全狀況標籤 第 3-6 頁
- 摘要標籤 第 3-15 頁
- 資料外洩防護標籤 第 3-25 頁
- 符合性標籤 第 3-31 頁
- 安全威脅統計資料標籤 第 3-36 頁

關於資訊中心

當您開啟 Apex Central 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 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 資料庫
- 已註冊的受管理產品

  如需詳細資訊，請參閱伺服器註冊 第 8-2 頁。

- 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。

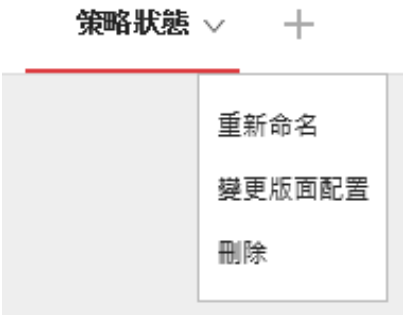
使用標籤

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。

步驟

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。

步驟

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

a. 請點選標籤顯示右側的「設定」按鈕。

b. 請點選「新增 Widget」。

c. 選取要新增的 Widget。

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

d. 請點選「新增」。

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

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

6. 如果要重新命名 Widget：

a. 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 (>)。

安全狀況標籤

「安全狀況」標籤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，提供網路安全防護狀態的整體摘要。您可以使用「安全狀況」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站台或回報層級，請啟動 Active Directory 整合或根據 IP 位址建立自訂網站。

如需詳細資訊，請參閱 Active Directory 和符合性設定 第 6-1 頁。

依預設，「安全狀況」標籤會切換至「圖表」檢視 ( )。如果要在資料表中顯示圖表節點、嚴重安全威脅和防毒特徵碼符合性資訊，請切換至「資料表」檢視 ( )。

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「站台」或「回報層級」。
- 要顯示的群組：選取處於最高風險之群組的前多少名
- 期間：指定圖表上所顯示資料的時間範圍。

符合性指標

「安全狀況」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資料外洩防護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「安全狀況」圖表中顯示的符合性層級資訊。

如需詳細資訊，請參閱安全狀況圖表 第 3-10 頁。

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 注意 Apex Central 支援 Security Agent 用於下列受管理產品： • Apex One • Worry Free Business Security Services 如需設定符合性指標設定的詳細資訊，請參閱設定防毒病毒碼符合性指標 第 6-7 頁。 • 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。 如需詳細資訊，請參閱使用者/端點目錄 第 7-2 頁。
資料外洩防護符合	顯示下列資訊： • 已啟動資料外洩防護且具有可接受的安全威脅偵測項目數的 Security Agent 百分比 如需設定符合性指標設定的詳細資訊，請參閱設定資料外洩防護符合指標 第 6-9 頁。 • 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。 如需詳細資訊，請參閱使用者/端點目錄 第 7-2 頁。

嚴重安全威脅

「安全狀況」標籤的「嚴重安全威脅」區段會顯示在您網路中偵測到的獨特嚴重安全威脅（依安全威脅類型）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。

如需有關定義重要使用者或端點的詳細資訊，請參閱使用者或端點重要性 第 7-34 頁。

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。

如需詳細資訊，請參閱使用者/端點目錄 第 7-2 頁。

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
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箱的產品偵測到，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

「安全狀況」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。

如需詳細資訊，請參閱使用者/端點目錄 第 7-1 頁。

安全狀況圖表

「安全狀況」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站台或回報層級中端點總數的比率。Y 軸表示站台或回報層級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站台或回報層級，請啟動 Active Directory 整合或根據 IP 位址建立自訂網站。

如需詳細資訊，請參閱 Active Directory 和符合性設定 第 6-1 頁。

將滑鼠游標暫留在某個節點上，可檢視特定站台或回報層級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」（「站台」、「回報層級」）。
- 您也可以使用「Active Directory 和符合性設定」畫面來自訂站台和回報層級。

  如需詳細資訊，請參閱端點和使用者分組 第 6-11 頁。

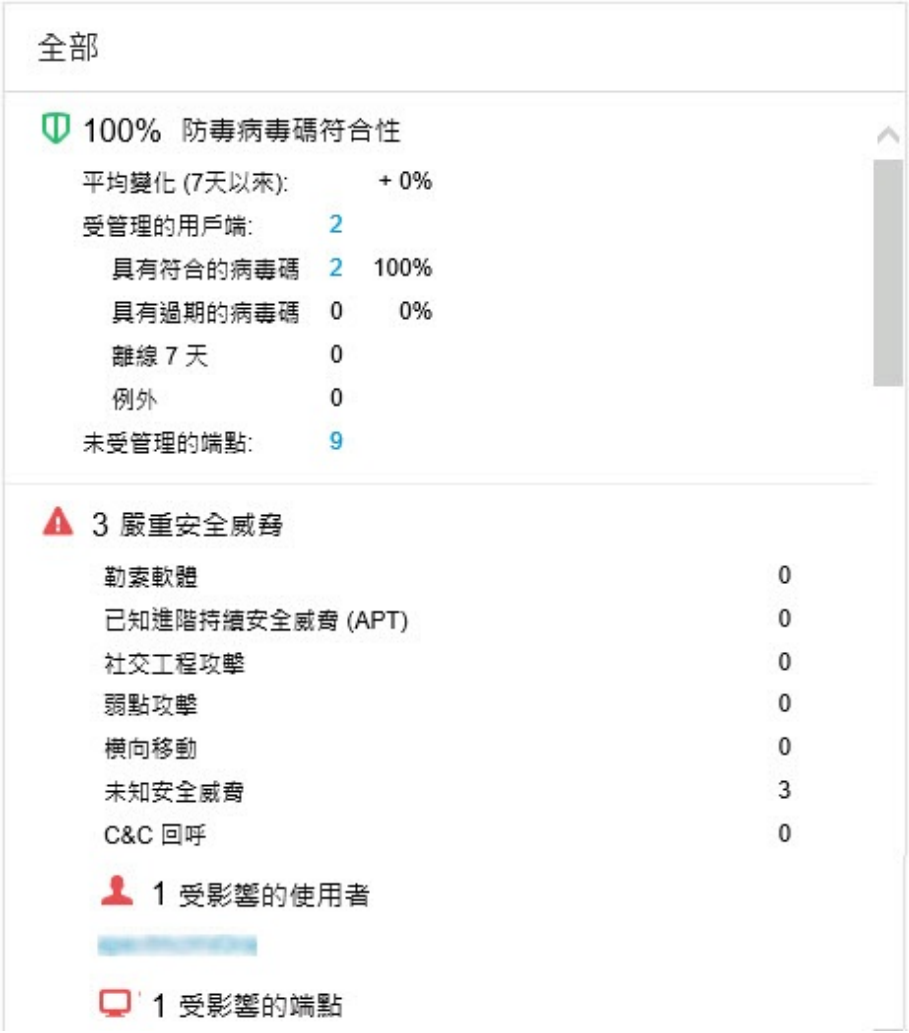
預設檢視會顯示您網路中所有節點過去 7 天的所選符合性指標資訊。

- 選取不同的符合性指標，會變更顯示的符合性資訊。

  如需詳細資訊，請參閱符合性指標 第 3-7 頁。

- 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。如需詳細資訊，請參閱安全狀況詳細資料窗格 第 3-12 頁。

安全狀況詳細資料窗格



「安全狀況」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。

  如需詳細資訊，請參閱符合性指標 第 3-7 頁。

- 按一下圖表上的某個節點，可僅顯示所選節點的資訊。

  如需詳細資訊，請參閱安全狀況圖表 第 3-10 頁。

- 按一下設定圖示 (>) 可變更所顯示資料的「期間」。

表 3-1. 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 Apex One 或 Worry-Free Business Security Services 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 Apex One 或 Worry-Free Business Security Services 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。
	如需詳細資訊，請參閱下列主題：
	• 設定防毒病毒碼符合性指標 第 6-7 頁
	• 使用者/端點目錄 第 7-1 頁

指標	說明

資料外洩防護符合	顯示已啟動資料外洩防護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 Apex One 或 Worry-Free Business Security Services 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 Apex One 或 Worry-Free Business Security Services 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。
	
	如需詳細資訊，請參閱下列主題：
	
	• 設定資料外洩防護符合指標 第 6-9 頁
	• 使用者/端點目錄 第 7-1 頁

表 3-2. 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獨特嚴重安全威脅（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。 如需詳細資訊，請參閱受影響的使用者 第 7-18 頁。

區段	說明
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。 如需詳細資訊，請參閱使用者所面臨的安全威脅 第 7-6 頁。
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。 如需詳細資訊，請參閱端點上的安全威脅 第 7-12 頁。

表 3-3. 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。 如需詳細資訊，請參閱使用者/端點目錄 第 7-1 頁。

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
- 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獨特嚴重安全威脅類型的總數，以及每個安全威脅類型的受影響使用者數目和安全威脅偵測數目。

按一下設定圖示 (>)，以變更預設「檢視」。

- 在「摘要」標籤或「自訂」標籤中，預設會選取「受影響的使用者」檢視。
- 在「安全威脅調查」標籤中，預設會選取「安全威脅偵測」檢視。

注意

- 此 Widget 會按嚴重性順序列出嚴重安全威脅類型。
- 個別使用者可能受到多個嚴重安全威脅類型的影響。

使用「範圍」下拉式清單，選取顯示的資料時間範圍。

圖 3-1. 受影響的使用者檢視

「受影響的使用者」檢視會顯示受每個安全威脅類型影響的「重要使用者」和「其他使用者」數目。

- 按一下「重要使用者」或「其他使用者」欄中的計數，然後按一下您要檢視的受影響使用者。

  如需詳細資訊，請參閱使用者所面臨的安全威脅 第 7-6 頁。

- 您可以在「使用者/端點目錄」畫面中定義重要使用者或端點。

  如需詳細資訊，請參閱使用者或端點重要性 第 7-34 頁。

圖 3-2. 安全威脅偵測檢視

「安全威脅偵測」檢視會顯示每個嚴重安全威脅類型的偵測數目。

- 按一下某個嚴重安全威脅類型，可檢視特定安全威脅偵測。
- 按一下特定安全威脅偵測的超連結，可檢視受影響使用者的詳細資料，並自動啟動「根本原因分析」以判定該安全威脅是否影響您網路中的其他端點。

  如需詳細資訊，請參閱受影響的使用者 第 7-18 頁。

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
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
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
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

安全威脅類型	說明
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
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
未知安全威脅	由 Deep Discovery Inspector、端點安全防護產品或其他具有沙箱的產品偵測到，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）
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

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。

- 如需有關定義重要使用者或端點的詳細資訊，請參閱使用者或端點重要性 第 7-34 頁。

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。

  如需詳細資訊，請參閱使用者所面臨的安全威脅 第 7-6 頁。

「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箱的產品偵測到，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「重要端點」或「其他端點」標籤，可在不同的檢視間切換。

- 如需有關定義重要使用者或端點的詳細資訊，請參閱使用者或端點重要性 第 7-34 頁。

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。

  如需詳細資訊，請參閱端點上的安全威脅 第 7-12 頁。

「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
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箱的產品偵測到，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 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 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 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 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。

- 如需詳細資訊，請參閱查詢記錄檔 第 15-2 頁。

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 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 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 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

通道	說明
行為	Apex One 行為監控偵測到勒索軟體

資料外洩防護標籤

「資料外洩防護」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。

預先定義的 Widget 包括：

- 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 (依傳輸管道)
- DLP 範本相符數
- 前幾名 DLP 事件來源
- DLP 違反的策略

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。

重要

此 Widget 僅顯示已指派了資料外洩防護 (DLP) 使用者角色的 Apex Central 使用者帳號資料。

如需有關檢閱 DLP 事件及設定 DLP 使用者角色的詳細資訊，請參閱 https://docs.trendmicro.com/en-us/enterprise/apex-central-online-help/dlp_incidents。

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。

重要

此 Widget 僅顯示已指派了資料外洩防護 (DLP) 使用者角色的 Apex Central 使用者帳號資料。

如需有關檢閱 DLP 事件及設定 DLP 使用者角色的詳細資訊，請參閱 https://docs.trendmicro.com/en-us/enterprise/apex-central-online-help/dlp_incidents。

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 資料外洩防護 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。

重要

此 Widget 僅顯示已指派了資料外洩防護 (DLP) 使用者角色的 Apex Central 使用者帳號資料。

如需有關檢閱 DLP 事件及設定 DLP 使用者角色的詳細資訊，請參閱 https://docs.trendmicro.com/en-us/enterprise/apex-central-online-help/dlp_incidents。

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。

設定	說明
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 (依傳輸管道) 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

資料	說明
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 會執行記錄查詢，以提供詳細資訊。

資料	說明
產品	向 Apex Central 註冊的受管理產品
版本	受管理產品的版本
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 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 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 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 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。

- 如需詳細資訊，請參閱查詢記錄檔 第 15-2 頁。

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 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 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 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 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」。

安全威脅統計資料標籤

「安全威脅統計資料」標籤所包含的 Widget 會顯示彙整的安全威脅偵測。

預先定義的 Widget 包括：

- 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
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

- 違規類型

資料	說明
行為監控	「資料範圍」指定之任何受管理產品偵測到的行為監控違規
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）
周邊設備存取控管	「資料範圍」指定之任何受管理產品偵測到的周邊設備存取控管違規
防火牆違規事件	「資料範圍」指定之任何受管理產品的防火牆違規
網路內容檢測	「資料範圍」指定之任何受管理產品偵測到的網路內容檢測違規
Machine Learning	「資料範圍」指定之任何受管理產品偵測到的 Machine Learning
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
可疑檔案	「資料範圍」指定之任何受管理產品偵測到的可疑檔案
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
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）

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
- 最近 7 天
- 最近 14 天
- 最近 30 天

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	受管理產品採取的處理行動或處理行動結果 注意 對於「Web 安全」安全威脅類型，不會顯示此欄

資料	說明
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 (%)	總偵測數中安全威脅所佔百分比

此 Widget 會顯示下列安全威脅類型的安全威脅偵測：

表 3-4. 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。
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。

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類型。

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

按一下設定圖示 (>)，可編輯 Widget 標題或產品範圍。

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

按一下「設定」圖示 (>)，可編輯下列項目：

- 標題：修改「C&C 回呼事件」Widget 的標題。
- 範圍：按一下 >> 並選取 Widget 用做來源的父伺服器。
- C&C 清單來源：選取「全球資訊」、「沙箱」或「使用者定義」做為 C&C 清單來源。
- 要顯示的項目：選取要在 Widget 中顯示的項目數。

按一下「儲存」以套用變更並結束。

第 4 章

帳號管理

本節討論如何建立及管理 Apex Central 使用者帳號和角色。

包含下列主題：

- 使用者帳號 第 4-2 頁
- 使用者角色 第 4-14 頁

使用者帳號

「使用者帳號」畫面提供先前針對 Apex Central 主控台設定的所有使用者帳號清單。您可以使用此畫面，設定每位使用者的使用者帳號和特定角色。

如需有關使用者角色的詳細資訊，請參閱使用者角色 第 4-14 頁。

下表列出「使用者帳號」畫面上提供的工作。

工作	說明
新增使用者帳號	按一下「新增」，設定新的使用者帳號或從整合式 Active Directory 結構匯入使用者或群組。 如需詳細資訊，請參閱新增使用者帳號 第 4-4 頁。 **注意** Apex Central 可讓您從整合式 Active Directory 結構建立使用者和群組的使用者帳號。 如需詳細資訊，請參閱 Active Directory 整合 第 6-2 頁。
刪除使用者帳號	選取現有帳號的「使用者/群組名稱」旁邊的核取方塊，然後按一下「刪除」來永久移除帳號。 **警告!** 帳號永久刪除時會從 Apex Central 伺服器移除所有先前設定的帳號資訊。
啟動雙因素驗證	按一下「啟動雙因素驗證」連結，要求使用者輸入 Google Authenticator 應用程式所產生的驗證碼，才能登入 Apex Central。 如需詳細資訊，請參閱啟動或關閉雙因素驗證 第 4-10 頁。
關閉雙因素驗證	按一下「關閉雙因素驗證」連結，只需使用有效的使用者帳號和密碼即可登入 Apex Central。 如需詳細資訊，請參閱啟動或關閉雙因素驗證 第 4-10 頁。
編輯使用者帳號	按一下使用者帳號的「使用者/群組名稱」來編輯使用者資訊。 如需詳細資訊，請參閱編輯使用者帳號 第 4-9 頁。

工作	說明
解除鎖定使用者帳號	按一下「已鎖定」欄中的「解除鎖定」按鈕，可解除鎖定連續未成功的登入嘗試次數超過指定次數的帳號。 如需詳細資訊，請參閱設定 Web 主控台設定值 第 2-7 頁。
啟動使用者帳號	按一下「啟動」欄中的 圖示，可啟動已關閉的帳號來登入 Apex Central 主控台。 **注意** 您也可以編輯帳號，來啟動已關閉的帳號。 如需詳細資訊，請參閱編輯使用者帳號 第 4-9 頁。
關閉使用者帳號	按一下「啟動」欄中的 圖示，可暫時禁止使用者登入 Apex Central 主控台。 **注意** • 您也可以編輯使用者帳號，來關閉該帳號。 如需詳細資訊，請參閱編輯使用者帳號 第 4-9 頁。 • Apex Central 無法關閉 Active Directory 使用者或群組的帳號。如果要關閉 Active Directory 帳號，您必須從 Active Directory 伺服器關閉帳號。 如需詳細資訊，請洽詢 Active Directory 管理員。

Root 帳號

Apex Central 允許您在安裝時指定 Root 帳號的名稱。Root 帳號可以檢視功能表中的所有功能、使用所有可用的服務及安裝用戶端。您無法刪除 Root 帳號。

Root 帳號也具有下列額外的權限：

- Root 帳號可以解除鎖定已鎖定的功能，方法是強制登出目前使用該功能的使用者。
- Root 帳號可以略過雙因素驗證。

注意

Apex Central 帳號只能登入 Apex Central，不能登入整個網路。Apex Central 使用者帳號與網路網域帳號不同。

新增使用者帳號

使用「使用者帳號」畫面建立 Apex Central 管理員的新使用者帳號，或從整合式 Active Directory 結構匯入使用者或群組。

重要

- 只有在安裝期間建立的 Root 帳號，或是指派了「管理員」或「管理員和 DLP 合規官」使用者角色的使用者帳號，可以在 Apex Central 上建立新使用者帳號。
- 從 Active Directory 結構匯入使用者或群組需要整合式 Active Directory 結構。

  如需詳細資訊，請參閱 Active Directory 整合 第 6-2 頁。
- 整合 Active Directory 結構可讓 Active Directory 使用者或群組使用「使用網域認證登入」按鈕登入 Apex Central，而不需要提供使用者名稱和密碼。

  如需詳細資訊，請參閱存取 Web 主控台 第 2-5 頁。

步驟

1. 移至「管理 > 帳號管理 > 使用者帳號」。

   會出現「使用者帳號」畫面。

2. 請點選「新增」。

   會出現「使用者帳號 > 步驟 1：使用者資訊」畫面。

3. 選取「啟動此帳號」，以在建立後啟動帳號。

注意

Apex Central 無法關閉 Active Directory 使用者或群組的帳號。如果要關閉 Active Directory 帳號，您必須從 Active Directory 伺服器關閉帳號。

如需詳細資訊，請洽詢 Active Directory 管理員。

4. 選取帳號類型。

- 如果要建立新的 Apex Central 使用者帳號，請執行下列作業：

  a. 選取「自訂帳號」。

  b. 設定下列必要的帳號資訊：

資訊	說明
使用者名稱	輸入使用者登入 Apex Central Web 主控台所需提供的帳號名稱。
完整名稱	輸入使用者的完整名稱。
密碼	輸入使用者登入 Apex Central Web 主控台所需提供的密碼。 **注意** 使用者可以在「我的帳號」畫面上變更密碼。 如需詳細資訊，請參閱檢視或編輯使用者帳號資訊 第 4-12 頁。
確認密碼	輸入「密碼」欄位中所提供的相同密碼。

資訊	說明
電子郵件信箱	輸入使用者接收通知的電子郵件信箱。 **注意** • Apex Central 透過電子郵件傳送報告和事件通知或在啟動雙因素驗證時，都需要填寫此欄位。 • 您也必須設定 SMTP 伺服器設定，才能使雙因素驗證正常運作，並可讓 Apex Central 透過電子郵件傳送報告和通知。 如需詳細資訊，請參閱設定 SMTP 伺服器設定 第 16-3 頁。

- 如果要從整合式 Active Directory 結構匯入使用者或群組，請執行下列作業：

  a. 選取「Active Directory 使用者或群組」。

  b. 使用下列項目搜尋 Active Directory 使用者或群組：

  - 使用者/群組名稱

    注意

    - 這是必填欄位。
    - 您可以運用星號 (*) 萬用字元，使用部分字串比對進行搜尋。

      例如，輸入 “tom *” 會搜尋名稱以 “tom” 開頭的所有使用者或群組。

  - 基準辨別名稱

  c. 請點選「搜尋」。

  在「搜尋結果」清單中會出現符合指定條件的 Active Directory 帳號。

d. 從「搜尋結果」清單中選取 Active Directory 使用者或群組，然後按一下 >。

在「選取的使用者/群組」清單中會出現選取的 Active Directory 使用者或群組。

重要

- Apex Central 會要求您先手動同步處理 Active Directory 資料，匯入的使用者或群組之後才能使用其 Active Directory 網域認證登入 Apex Central。

  如需詳細資訊，請參閱 Active Directory 整合 第 6-2 頁：

- 您不需要從移轉自舊版 Control Manager 的 Active Directory 結構手動同步處理 Active Directory 資料。來自移轉的 Active Directory 結構的使用者與群組在移轉完成後，即可登入 Apex Central。

5. 按「下一步」。

會出現「使用者帳號 > 步驟 2：存取控制」畫面。

6. 從「選取角色」下拉式清單中選取使用者角色。

注意

- 為使用者角色定義的存取權限之優先順序高於您針對個別使用者帳號所設定的受管理產品/資料夾存取權限。
- 「DLP 合規官」和「DLP 事件檢閱者」角色只適用於 Active Directory 使用者或群組。

  如需詳細資訊，請參閱使用者角色 第 4-14 頁。

7. 在「選取可存取的產品/資料夾」樹狀結構中，選取使用者在「產品目錄」結構中可存取的產品或資料夾。

注意

您可以限制使用者存取單一受管理產品，或允許其存取整個「 產品目錄」。指派資料夾的存取權可讓使用者存取所有子資料夾和受管理產品。

如需詳細資訊，請參閱受管理產品存取控制 第 4-8 頁。

8. 為使用者帳號指定受管理產品/資料夾存取權限。

注意

這些存取權限會決定使用者帳號可對受管理產品執行的處理行動。授與帳號的權限不能超過授與者的權限。

如需詳細資訊，請參閱受管理產品存取控制 第 4-8 頁。

9. 請點選「完成」。

在「使用者帳號」畫面上會出現新的使用者帳號。

受管理產品存取控制

您指定給所選受管理產品/資料夾的存取權限會決定使用者在「產品目錄」畫面上的可用控制項。例如，如果您只將「執行」存取權限指定給所選取的受管理產品/資料夾，那麼使用者只能使用「產品目錄」畫面上的「工作」按鈕。

注意

「產品目錄」畫面上的可用處理行動會根據使用者角色、受管理產品/資料夾的存取權限，以及您在「產品目錄」結構中選取的受管理產品/資料夾動態變更。

如需詳細資訊，請參閱產品目錄 第 10-2 頁。

您可以為可存取的受管理產品/資料夾指定下列一或多個存取權限。

存取權限	說明
執行	允許使用者帳號使用「產品目錄」畫面上的「工作」按鈕，對可存取資料夾中的受管理產品執行工作。 如需詳細資訊，請參閱執行受管理產品工作 第 10-7 頁。
設定	允許使用者帳號使用「產品目錄」畫面上的「設定」按鈕進行受管理產品設定，或從 Apex Central 登入受管理產品 Web 主控台 如需詳細資訊，請參閱設定受管理的產品設定 第 10-8 頁。
編輯目錄	允許使用者帳號使用「目錄管理」按鈕，在「產品目錄」結構中組織可存取的受管理產品或資料夾。 如需詳細資訊，請參閱目錄管理 第 10-10 頁。

注意

當管理員指定使用者可以存取哪些產品時，管理員也同時指定使用者可以從 Apex Central 存取哪些資訊。受影響的資訊如下：元件資訊、記錄檔、產品摘要資訊、安全資訊，以及可用於報告和記錄查詢的資訊。

例如：

Bob 和 Jane 都是 Apex One 管理員。他們兩人都擁有相同的使用者角色權限（兩人都可存取 Web 主控台中相同的功能表項目）。不過，Jane 負責監督所有 Apex One 伺服器的作業。Bob 則僅負責監督用來保護行銷部門桌上型電腦的 Apex One 伺服器運作。因此，他們兩人可在 Web 主控台中檢視的資訊非常不同。在登入之後，Bob 只會看到其 Apex Central 使用者帳號允許之 Apex One 伺服器（行銷部門的 Apex One 伺服器）的適當資訊。當 Jane 登入後，她會看到所有 Apex One 伺服器的資訊，因為其 Apex Central 使用者帳號授與她存取所有向 Apex Central 註冊之 Apex One 伺服器的權限。

編輯使用者帳號

使用「使用者帳號」畫面可對您有編輯權限的任何使用者帳號，編輯使用者資訊、使用者角色或受管理產品/資料夾存取權限。

重要

- 在安裝期間建立的 Root 帳號可以編輯 Apex Central 網路上的任何使用者帳號。指派有「管理員」或「管理員和 DLP 合規官」使用者角色的任何使用者帳號，都可以編輯 Apex Central 網路上除了 Root 帳號之外的所有其他使用者帳號。
- 使用者帳號的存取權限一旦修改，便會終止被修改帳號及被修改帳號所建立之所有帳號的所有 Apex Central 作業階段。
- 您無法變更現有帳號的使用者名稱。

步驟

1. 移至「管理 > 帳號管理 > 使用者帳號」。

   會出現「使用者帳號」畫面。

2. 按一下帳號的「使用者/群組名稱」來進行修改。

   會出現「使用者帳號 > 步驟 1：使用者資訊」畫面。

3. 如果要啟動或關閉帳號，請選取或取消選取「啟動此帳號」核取方塊。
4. 修改使用者資訊。
5. 按「下一步」。

   會出現「使用者帳號 > 步驟 2：存取控制」畫面。

6. 修改使用者角色、可存取的產品/資料夾或存取權限。
7. 按一下「完成」來套用變更。

啟動或關閉雙因素驗證

「雙因素驗證」藉由要求使用者輸入 Google Authenticator 應用程式所產生的驗證碼以登入 Apex Central，為使用者帳號提供額外的安全性。

重要

Apex Central 的雙因素驗證需要下列項目：

- 設定每個使用者帳號的電子郵件信箱

  如需詳細資訊，請參閱檢視或編輯使用者帳號資訊 第 4-12 頁。

- 設定用於傳送電子郵件通知的 SMTP 伺服器設定

  如需詳細資訊，請參閱設定 SMTP 伺服器設定 第 16-3 頁。

- 在每個使用者的行動裝置上下載並安裝 Google Authenticator 應用程式

注意

- <Root> 帳號一律可以略過雙因素驗證。
- 雖然 Google Authenticator 應用程式產生的驗證碼會每隔 30 秒變更一次，但使用者仍可以在最長 5 分鐘內使用先前產生的驗證碼登入 Apex Central。

步驟

1. 移至「管理 > 帳號管理 > 使用者帳號」。

   會出現「使用者帳號」畫面。

2. 如果要啟動雙因素驗證，請執行下列作業：

   a. 按一下「啟動雙因素驗證」。

      會出現確認對話方塊。

   b. 按一下「啟動」。

      - 「使用者帳號」畫面頂端會顯示一則警告訊息，提示您為所有使用者帳號設定電子郵件信箱。

        按一下此連結可檢視尚未設定電子郵件信箱的使用者。

      - 「新增使用者帳號」畫面上的電子郵件信箱欄位會變成必填欄位。

- 使用者必須輸入有效的使用者名稱和密碼，以及 Google Authenticator 應用程式產生的驗證碼，才能登入 Apex Central。

3. 如果要關閉雙因素驗證，請執行下列作業：

   a. 按一下「關閉雙因素驗證」。

      會出現確認對話方塊。

   b. 按一下「關閉」。

      只需要使用有效的使用者帳號和密碼，即可登入 Apex Central Web 主控台。

檢視或編輯使用者帳號資訊

使用「我的帳號」畫面可檢視或變更下列帳號資訊：您自己的使用者帳號或是您所建立的使用者帳號。

如需有關編輯指派給特定使用者帳號之使用者角色的資訊，請參閱編輯使用者帳號 第 4-9 頁。

步驟

1. 移至「管理 > 帳號管理 > 我的帳號」。

   會出現「我的帳號」畫面。

2. 設定下列帳號資訊：

資訊	說明
完整名稱	輸入使用者的完整名稱。 注意 這是必填欄位。

資訊	說明
密碼	輸入使用者登入 Apex Central Web 主控台所需提供的密碼。 注意 這是必填欄位。
確認密碼	輸入「密碼」欄位中所提供的相同密碼。 注意 這是必填欄位。
電子郵件信箱	輸入使用者接收通知的電子郵件信箱。 注意 • Apex Central 透過電子郵件傳送報告和事件通知或進行雙因素驗證時，都需要填寫此欄位。 如需有關雙因素驗證的詳細資訊，請參閱啟動或關閉雙因素驗證 第 4-10 頁。 • 為了使 Apex Central 透過電子郵件傳送報告和事件通知，您也必須進行 SMTP 伺服器設定。 如需詳細資訊，請參閱設定 SMTP 伺服器設定 第 16-3 頁。
電話號碼	輸入與使用者帳號相關聯的有線電話號碼。
行動電話號碼	輸入與使用者帳號相關聯的行動電話號碼。

3. 按一下「儲存」來套用變更。

使用者角色

「使用者角色」畫面提供您可指派給使用者帳號的所有預設使用者角色和所有自訂使用者角色的清單。使用者角色會定義使用者可以存取及控制 Apex Central Web 主控台的哪些區域。您可使用此畫面來建立及編輯自訂的 Apex Central 使用者角色。

重要

如果舊版 Apex Central 中的自訂使用者角色擁有「策略管理」功能表項目的權限，在升級至目前版本後，角色將擁有完全控制權限。您可將權限變更為「維護」或「唯讀」。如果從不含「策略管理」的 Apex Central 版本升級，除非您選擇修改角色設定，否則自訂使用者角色將無權管理或檢視「策略管理」功能。

注意

- 只有在安裝期間建立的 Root 帳號，或是指派了「管理員」或「管理員和 DLP 合規官」使用者角色的使用者帳號，可以建立新使用者帳號及指派使用者角色。
- 為使用者角色定義的存取權限之優先順序高於您針對個別使用者帳號所設定的受管理產品/資料夾存取權限。

  如需詳細資訊，請參閱受管理產品存取控制 第 4-8 頁。

下表列出「使用者角色」畫面上提供的工作。

工作	說明
新增使用者角色	按一下「新增」可建立新的自訂使用者角色。 如需詳細資訊，請參閱新增使用者角色 第 4-18 頁。

工作	說明
刪除使用者角色	選取某個自訂使用者角色的「名稱」旁的核取方塊，然後按一下「刪除」，可永久移除角色。 注意 您無法刪除 Trend Micro Apex Central™ 提供的任何預設使用者角色。
編輯使用者角色	按一下某個使用者角色的「名稱」，可編輯或檢視指派的存取權限。 如需詳細資訊，請參閱編輯使用者角色 第 4-19 頁。 注意 您無法編輯 Trend Micro Apex Central™ 提供的任何預設使用者角色。 如需有關預設使用者角色的詳細資訊，請參閱預設使用者角色 第 4-15 頁。

預設使用者角色

Apex Central 提供一些可指派給使用者帳號的預設使用者角色。使用者角色會定義使用者可以存取及控制 Apex Central Web 主控台的哪些區域。雖然您可以將某些存取權限新增至預設使用者角色，但無法從預設使用者角色移除任何預先定義的存取權限。

注意

只有在安裝期間建立的 Root 帳號，或是指派了「管理員」或「管理員和 DLP 合規官」使用者角色的使用者帳號，可以建立新使用者帳號及指派使用者角色。

如需有關新增或編輯自訂使用者角色的詳細資訊，請參閱下列主題：

- 新增使用者角色 第 4-18 頁
- 編輯使用者角色 第 4-19 頁

下表說明「使用者角色」畫面上提供的預設角色。

角色	說明
Administrator_and_DLP Compliance_Officer	• 可以執行所有功能表項目上的所有處理行動 • 可以監控、檢閱及調查任何 Active Directory 使用者觸發的 DLP 事件。
Administrator	• 可以執行所有功能表項目上的所有處理行動 • 無法監控、檢閱或調查任何 Active Directory 使用者觸發的 DLP 事件
DLP_Compliance_Officer	• 可以執行「資訊中心」上所有的處理行動 • 可以監控、檢閱及調查任何 Active Directory 使用者觸發的 DLP 事件。 注意 此使用者角色僅適用於 Active Directory 使用者或群組。
DLP_Incident_Reviewer	• 可以執行「資訊中心」上所有的處理行動 • 只能監控、檢閱及調查由向 DLP 事件檢閱者報告的 Active Directory 使用者觸發的 DLP 事件 注意 此使用者角色僅適用於 Active Directory 使用者或群組。 如需詳細資訊，請參閱下列主題： • 回報層級 第 6-13 頁 • 新增使用者帳號 第 4-4 頁

角色	說明
Operator	• 可以執行所有「資訊中心」和「目錄」功能表項目上的所有處理行動 • 可以執行記錄查詢、檢視其他使用者產生及傳送的報告，以及更新使用者帳號資訊 • 只能檢視「策略管理」畫面上的資訊 • 無法監控、檢閱或調查任何 Active Directory 使用者觸發的 DLP 事件
Power_User	• 可以執行所有「資訊中心」和「目錄」功能表項目上的所有處理行動 • 可以執行記錄查詢、維護記錄檔，以及產生並維護報告 • 只能檢視「策略管理」畫面上的資訊 • 無法監控、檢閱或調查任何 Active Directory 使用者觸發的 DLP 事件
Read-only_User	• 可以檢視所有功能表項目的資訊，以及更新使用者帳號資訊 • 可以執行「資訊中心」上所有的處理行動 • 可以執行記錄查詢、產生報告、建立自訂報告範本、搜尋目錄，以及建立並使用自訂標籤 (Tags)/過濾器來管理「使用者/端點目錄」樹狀結構 • 無法檢視其他使用者產生的報告
SSO_User	• 可以執行所有功能表項目上的所有處理行動 • 無法監控、檢閱或調查任何 Active Directory 使用者觸發的 DLP 事件 注意 預設會隱藏此使用者角色。
Threat_Investigator	• 可以調查受管理端點/伺服器上的安全威脅事件。

注意

舊版中的「Operator」和「Power_Users」角色，都不具有對「策略管理」功能表項目執行動作的權限。在升級至此版本後，這兩個角色將具有唯讀權限，且無法變更。

新增使用者角色

您可以使用「使用者角色」畫面來建立自訂使用者角色。

步驟

1. 移至「管理 > 帳號管理 > 使用者角色」。

   會出現「使用者角色」畫面。

2. 請點選「新增」。

   會出現「新增角色」畫面。

3. 在「角色資訊」區段中：

   a. 在「名稱」欄位中輸入唯一的使用者角色名稱。

   b. 在「說明」欄位中針對使用者角色提供有意義的說明。

      注意

      此說明會顯示在「使用者角色」清單中。提供有意義的說明，有助於管理員在使用者角色名稱無法完全表達使用者角色的用途時，快速識別使用者角色。

4. 在「功能表存取控制」區段中，選取使用者角色的可存取功能表項目。

5. 指定所選功能表項目的存取權限。

   - 完全控制，但不包括：選取此選項可允許使用者對可存取功能表項目執行所有可用的動作

- 建立、複製及匯入策略：選取此選項可防止使用者在「策略管理」畫面上建立、複製或匯入策略

  如需詳細資訊，請參閱策略管理 第 13-2 頁。

- 監控、檢閱及調查所有使用者觸發的 DLP 事件：選取此選項可防止使用者調查所有 Active Directory 使用者觸發的 DLP 事件

- 唯讀：選取此選項可僅允許使用者檢視在「功能表存取控制」區段中選取之功能表項目的資訊

6. 按一下「儲存」。

   新使用者角色會顯示在「使用者角色」畫面上。

編輯使用者角色

Apex Central 允許您修改自訂使用者角色的存取權限。

如需有關編輯指派給特定使用者帳號之使用者角色的資訊，請參閱編輯使用者帳號 第 4-9 頁。

注意

可存取功能表項目上顯示的受管理產品資訊會根據 Apex Central 管理員在個別使用者帳號中指定的受管理產品/目錄權限而定。

例如：

Bob 和 Jane 都是 Apex One 管理員。他們兩人都擁有相同的使用者角色權限（兩人都可存取 Web 主控台中相同的功能表項目）。不過，Jane 負責監督所有 Apex One 伺服器的作業。Bob 則僅負責監督用來保護行銷部門桌上型電腦的 Apex One 伺服器運作。因此，他們兩人可在 Web 主控台中檢視的資訊非常不同。在登入之後，Bob 只會看到其 Apex Central 使用者帳號允許之 Apex One 伺服器（行銷部門的 Apex One 伺服器）的適當資訊。當 Jane 登入後，她會看到所有 Apex One 伺服器的資訊，因為其 Apex Central 使用者帳號授與她存取所有向 Apex Central 註冊之 Apex One 伺服器的權限。

步驟

1. 移至「管理 > 帳號管理 > 使用者角色」。

   會出現「使用者角色」畫面。

2. 按一下使用者角色的「名稱」進行編輯。

   會出現「編輯角色」畫面。

3. 編輯使用者角色資訊。

4. 按一下「儲存」來套用變更。

第 5 章

使用授權管理

本節討論如何啟動或續訂 Apex Central 和受管理產品的產品使用授權。

包含下列主題：

- Apex Central 啟動和使用授權資訊 第 5-2 頁
- 受管理產品的啟動和註冊 第 5-3 頁

Apex Central 啟動和使用授權資訊

啟動 Apex Central 可讓您使用所有產品功能，包括下載更新的程式元件。

啟動 Apex Central

「使用授權管理」畫面可讓您在取得啟動碼後啟動 Apex Central（請向 Trend Micro 銷售代表或經銷商索取啟動碼）。

如果您已購買 Apex One Sandbox as a Service 的使用授權，則也可以從「使用授權管理」畫面啟動該使用授權。

重要

在啟動 Apex Central 後，請先登出後再登入 Apex Central Web 主控台，以使變更生效。

步驟

1. 移至「管理 > 使用授權管理 > Apex Central」。

   會出現「使用授權資訊」畫面，其中顯示目前的使用授權資訊。

2. 按一下「指定新啟動碼」連結。
3. 輸入您的啟動碼。
4. 按一下「啟動」。
5. 請先登出後再登入 Apex Central Web 主控台，以使變更生效。

檢視和更新 Apex Central 使用授權資訊

「使用授權管理」畫面顯示您目前的 Apex Central 使用授權資訊和啟動狀態。您可以從這個畫面存取 Trend Micro Customer Licensing Portal，以更新或續約您的使用授權。

如果您購買了 Apex One Sandbox as a Service 的使用授權，則「使用授權管理」畫面也會顯示使用授權資訊和啟動狀態。

步驟

1. 移至「管理 > 使用授權管理 > Apex Central」。

   會出現「使用授權資訊」畫面，其中顯示目前的使用授權資訊。

2. 如果要更新畫面以顯示最新的使用授權資訊，請執行下列作業：

   a. 按一下「更新使用授權資訊」。

   b. 請先登出後再登入 Apex Central Web 主控台，以使變更生效。

3. 如果要續訂您的使用授權，請執行下列作業：

   a. 按一下「指定新啟動碼」連結。

   b. 輸入您的啟動碼。

   c. 按一下「啟動」。

   d. 請先登出後再登入 Apex Central Web 主控台，以使變更生效。

4. 如果要在 Trend Micro Customer Licensing Portal 中檢視目前使用授權的相關資訊，請執行下列作業：

   a. 按一下「線上檢視」。

   b. 使用您的趨勢科技帳號和密碼登入 Customer Licensing Portal。

   c. 按一下「我的產品/服務」功能表標籤。

   d. 展開「產品/服務」類別，以檢視已註冊之趨勢科技產品的使用授權資訊。

受管理產品的啟動和註冊

如果要使用 Apex Central、受管理產品（例如 Apex One、ScanMail for Microsoft Exchange）及其他服務，您必須取得啟動碼並啟動軟體或服務。軟

體隨附授權碼。請使用該授權碼在 Trend Micro Customer Licensing Portal 網站線上註冊軟體並取得啟動碼。

當受管理產品向 Apex Central 註冊時，受管理產品會將其啟動碼新增至「使用授權管理」畫面上的受管理產品啟動碼清單中。管理員可將新的啟動碼新增至清單，並重新部署續訂的啟動碼。

使用授權管理詳細資料

下表說明在「使用授權管理」畫面（「管理 > 使用授權管理 > 受管理的產品」）中顯示的受管理產品使用授權資訊。

秘訣

您可以不勾選「隱藏已到期的啟動碼」核取方塊，即可檢視所有受管理產品的使用授權詳細資料。

欄名稱	說明
啟動碼	顯示受管理產品的啟動碼
注意	顯示啟動碼的其他資訊
已啟動的產品	顯示部署了啟動碼的受管理產品數目
使用授權狀態	顯示啟動碼的狀態： • 有效 • 已到期
類型	顯示啟動碼的類型： • 完整版：允許在維護合約期間完整使用產品（通常為 1 年） • 試用版：允許在試用期間完整使用產品（通常為 3 個月）
到期日	顯示啟動碼到期日期
授權計數	顯示啟動碼允許的授權數目

欄名稱	說明
線上檢視使用授權資訊	按一下連結可開啟您的預設 Web 瀏覽器，並前往 Trend Micro Customer Licensing Portal。 您可在此入口網站中管理趨勢科技企業帳號，其中包含內部部署產品的啟動碼，以及趨勢科技軟體即服務解決方案的產品授權。

受管理的產品使用授權資訊

按一下「使用授權管理」畫面（管理 > 使用授權管理 > 受管理的產品）上的「啟動碼」，即會顯示下列有關受管理產品/服務的使用授權資訊。

欄位	說明
啟動碼	用於啟動產品/服務之使用授權的代碼
狀態	使用授權狀態（例如「有效」）
類型	產品/服務的使用授權類型（例如「完整版」或「試用版」）
到期日	產品/服務使用授權的到期日
說明	啟動碼的使用者定義說明 • 在文字方塊中輸入說明，然後按一下「完成」以儲存變更。

啟動受管理的產品

使用「使用授權管理」畫面可啟動受管理的產品使用授權。啟動受管理的產品可讓您使用產品的所有功能，包括下載更新的程式元件。您可以在從產品套件取得啟動碼，或是向趨勢科技經銷商購買啟動碼之後，啟動受管理的產品。

步驟

1. 移至「管理 > 使用授權管理 > 受管理的產品」。

   會出現「使用授權管理」畫面。

2. 按一下「新增並部署」。

   會出現「新增及部署新使用授權 > 步驟 1：輸入啟動碼」畫面。

3. 在「新啟動碼」欄位中輸入您想要啟動之產品的啟動碼。

4. 按「下一步」。

   會出現「新增及部署新使用授權 > 步驟 2：選取目標」畫面。

   注意

   如果清單中未顯示任何產品，則選取的啟動碼不支援目前已向 Apex Central 註冊的任何產品。這可能表示受管理的產品不支援從 Apex Central 伺服器接收啟動碼。

5. 選取要部署啟動碼的受管理產品。

6. 按一下「部署」。

   會出現「使用授權管理」畫面，並會在資料表中列出新啟動碼。

   注意

   「使用授權管理」畫面頂端的快顯通知訊息會顯示啟動碼部署狀態。

   按一下訊息中的連結，可在「追蹤指令」畫面上檢視部署狀態詳細資料。

續約受管理的產品使用授權

Apex Central 可以從「使用授權管理」畫面將啟動碼部署或重新部署到已註冊的產品。

步驟

1. 移至「管理 > 使用授權管理 > 受管理的產品」。

   會出現「使用授權管理」畫面。

2. 從清單中選取啟動碼。
3. 按一下「重新部署」。

   會出現「重新部署使用授權」畫面。
4. 選取要部署啟動碼的產品。

   注意

   - 如果清單中未顯示任何產品，則選取的啟動碼不支援目前已向 Apex Central 註冊的任何產品。
   - 您必須選取至少一個產品，才能部署啟動碼。
5. 按一下「部署」。

   Apex Central 會將啟動碼部署到選取的產品。

第 6 章

Active Directory 和符合性設定

本節討論如何在 Apex Central 中設定 Active Directory 整合和符合性指標設定。

包含下列主題：

- Active Directory 整合 第 6-2 頁
- '符合性指標 第 6-6 頁
- 端點和使用者分組 第 6-11 頁

Active Directory 整合

將 Apex Central 與 Microsoft Active Directory 伺服器整合，可以：

- 讓管理員根據 Active Directory 使用者或群組建立用於 Web 主控台存取的使用者帳號。

  如需詳細資訊，請參閱新增使用者帳號 第 4-4 頁。

- 根據您現有的組織結構對應使用者/端點目錄，並將端點資訊（例如，安全威脅偵測和策略狀態）與 Active Directory 使用者資訊（例如，登入歷史記錄和聯絡詳細資料）整合。

  如需詳細資訊，請參閱使用者/端點目錄 第 7-2 頁。

- 使用 Active Directory 中的站台位置和報告行資訊，在「安全狀況」資訊中心標籤上更進一步全盤掌握您網路的安全防護狀態。

  如需詳細資訊，請參閱符合性指標 第 6-6 頁。

設定 Active Directory 連線設定

請指定連線設定，讓 Apex Central 從 Active Directory 伺服器同步處理端點和使用者資訊。

注意

Apex Central 支援與多個 Active Directory 樹系進行同步處理。每當新增 Active Directory 網域時，都會自動同步處理同一樹系中的所有網域。

如需有關樹系信任的詳細資訊，請聯絡您的 Active Directory 管理員。

步驟

1. 移至「管理 > 設定 > Active Directory 和符合性設定」。
2. 按一下「Active Directory 設定」標籤。

3. 選取「啟動 Active Directory 同步處理和驗證」。
4. 設定連線設定以存取 Active Directory 伺服器。

欄位	說明
伺服器位址	輸入 Active Directory 伺服器的 FQDN 或 IP 位址（IPv4 或 IPv6）。
使用者名稱	輸入用於存取 Active Directory 伺服器所需的網域名稱和使用者名稱。 範例格式為網域\使用者名稱
密碼	輸入用於存取 Active Directory 伺服器所需的密碼。

- 如果要新增其他 Active Directory 伺服器，請按一下新增圖示 (+)。
- 如果要刪除 Active Directory 伺服器，請按一下刪除圖示 (–)。

5. 從「同步處理頻率 (以小時為單位)」下拉式清單中，選取 Apex Central 與 Active Directory 伺服器同步處理資料的頻率。

注意

Active Directory 同步處理時間會根據 Active Directory 資料庫的大小和複雜度而有不同。有可能需要一個小時以上才會完成同步處理。

6. （選用）展開「進階設定」以設定「同步處理來源」或「連線模式」。
   a. 請選取下列其中一個同步處理來源：
      - 網域控制站：將多個樹系的所有網域與信任關係同步處理
      - 全域目錄：同步處理單一樹系的所有網域

重要

無法從具有預設設定的全域目錄同步處理 Apex Central 使用的一些資訊（例如，地理位置以及全域群組或網域本機群組中的使用者成員資格）。僅當您的網路策略禁止 Apex Central 連線至所有網域控制站時，才能選擇從全域目錄進行同步處理。

b. 選取下列其中一種連線模式：

- SSL

  重要

  如果要使用 SSL 連線，請將 Active Directory 憑證匯入到 Apex Central 伺服器。

- 非 SSL

7. （選用）按一下「測試連線」以測試伺服器連線。

   注意

   測試連線不會儲存 Active Directory 伺服器設定。

   Active Directory 伺服器連線狀態圖示（ 或 ）會顯示在伺服器位址前面。

8. 按一下「儲存」。

   Apex Central 會根據同步處理頻率，從 Active Directory 伺服器同步處理端點和使用者資訊。

9. （選用）藉由修改位於以下位置的 `ADSyncOUList.config` 組態設定檔，設定 Apex Central 要同步處理的 Active Directory 網域和 OU：

   `<Apex Central 安裝目錄>\ADSyncOUList.config`

10. （選用）按一下「立即同步處理」，以手動同步處理 Active Directory 資料。

    Active Directory 伺服器連線狀態圖示（ 或 ）會顯示在伺服器位址前面。

11. 如果要移除已同步處理的 Active Directory 伺服器，請執行下列作業：

    a. 不勾選「啟動 Active Directory 同步處理」核取方塊。

    b. 按一下「清除資料」，以從已移除 Active Directory 伺服器中清除 Apex Central 伺服器的資料。

Apex Central 會移除已同步處理的 Active Directory 伺服器。

注意

按一下「清除資料」會觸發每隔 2 分鐘執行一次的預約工作，該工作會從 Apex Central 資料庫清除已移除之 Active Directory 伺服器的所有資料。

Active Directory 同步處理疑難排解

Active Directory 同步處理讓 Apex Central 可以從 Active Directory 伺服器取得使用者資訊（例如站台和回報層級資訊）。

如果「資訊中心」畫面上顯示 Active Directory 相關錯誤，請參閱下表瞭解疑難排解解決方案。

問題	解決方案
使用者名稱或密碼錯誤	• 確保您指定了正確的帳號資訊。 • 確認使用者帳號有權存取 Active Directory 伺服器。 如需協助，請洽詢 Active Directory 管理員。
無法連線到 Active Directory 伺服器	• 確保您已設定正確的 Active Directory 伺服器連線設定。 如需詳細資訊，請參閱設定 Active Directory 連線設定 第 6-2 頁。 • 檢查 Active Directory 伺服器是否可用。 • 檢查網路連線和防火牆設定。 • 確保 Apex Central 和 Active Directory 伺服器都可以建立與對方的通訊。 如果要測試 Apex Central 與 Active Directory 伺服器之間的連線，請按一下「Active Directory 和符合性設定」畫面上的「測試連線」。

問題	解決方案
無法存取 Apex Central 資料庫	確保已連線到 Apex Central 資料庫。 如需詳細資訊，請參閱瞭解 Apex Central 資料庫 第 24-2 頁。

如果連線問題持續發生，請洽詢支援人員。

如需詳細資訊，請參閱技術支援 第 26-1 頁。

符合性指標

Apex Central 包含下列符合性指標，並且會根據指標設定及從 Active Directory 伺服器同步處理的使用者和端點資訊來執行符合性計算。您可以在「安全狀況」資訊中心標籤上，檢視符合性指標的資訊。

- 防毒特徵碼符合性：使用可接受的防毒病毒碼（「病毒碼」和「本機雲端病毒碼」）版本的受管理 Apex One Security Agent 百分比
- 資料外洩防護符合性：具有可接受的機密資料偵測事件數目的受管理 Apex One（支援 Data Discovery）和 Cloud App Security 用戶端百分比

下列程序總覽說明如何讓 Apex Central 執行符合性計算，並在「安全狀況」資訊中心標籤上顯示符合性資訊。

步驟

1. 連線至 Active Directory 伺服器，以同步處理使用者和端點資訊。

   如需詳細資訊，請參閱設定 Active Directory 連線設定 第 6-2 頁。

2. 設定符合性指標設定。

   如需詳細資訊，請參閱下列主題：

   - 設定防毒病毒碼符合性指標 第 6-7 頁
   - 設定資料外洩防護符合指標 第 6-9 頁

3. （選用）根據 Active Directory 站台和回報層級，自訂端點和使用者分組。

如需詳細資訊，請參閱端點和使用者分組 第 6-11 頁。

4. 移至「資訊中心」以檢視符合性資訊。

注意

如果要變更 Active Directory 分組或檢視您的受管理用戶端的 Data Discovery 符合性，請設定「安全狀況」標籤設定。

如需詳細資訊，請參閱下列主題：

- 安全狀況標籤 第 3-6 頁
- 使用 Widget 第 3-4 頁

設定防毒病毒碼符合性指標

您可以設定「防毒病毒碼符合性」指標的設定和例外，以在「安全狀況」標籤上顯示使用可接受的防毒病毒碼（「病毒碼」和「本機雲端病毒碼」）版本的受管理 Security Agent 百分比。

注意

Apex Central 支援 Security Agent 用於下列受管理產品：

- Apex One
- Worry Free Business Security Services

步驟

1. 移至「管理 > 設定 > Active Directory 和符合性設定」。
2. 按一下「符合性指標」標籤。
3. 按一下「防毒病毒碼符合性」。
4. 下表說明可用的組態設定選項。

欄	說明
可接受的特徵碼版本	為端點指定符合安全要求的特徵碼版本。
警訊指標	調整滑桿控制項來設定不同警訊層級的門檻值（合規用戶端的百分比）。

5. 在「例外清單」中，選取自訂標籤或過濾器，以將使用者或端點從符合性計算排除。

注意

- 例外清單會套用至所有 Apex Central 使用者。您只能根據您的權限新增或刪除例外，以修改對應的標籤和過濾器。
- 如需有關建立標籤或過濾器的詳細資訊，請參閱自訂標籤 (Tags) 和過濾器 第 7-27 頁。

a. 請點選「新增」。

會出現「新增例外」畫面。

b. 從「類型」下拉式清單中選取「使用者」或「端點」，以按照類型顯示可用的自訂過濾器和標籤；或者，選取「全部」以檢視所有項目。

注意

若要搜尋自訂過濾器或標籤，請在文字欄位中輸入名稱並按 Enter 鍵。

如需有關自訂標籤 (Tags) 或過濾器的詳細資訊，請參閱自訂標籤 (Tags) 和過濾器 第 7-27 頁。

c. 選取一或多個自訂標籤 (Tags) 或過濾器，然後按一下「新增」。

選取的項目會顯示在「例外清單」中。

d. 請點選「關閉」。

e. 按一下「儲存」。

f. 從「套用由以下人員新增的例外」下拉式清單中指定已新增的自訂標籤 (Tags) 或過濾器的範圍。

- 所有使用者帳號：排除任何使用者帳號所新增之自訂過濾器和標籤中指定的所有使用者與端點
- 僅已登入的帳號：僅排除目前登入的使用者帳號所新增之自訂過濾器和標籤中指定的使用者與端點

6. 按一下「儲存」。

設定資料外洩防護符合指標

您可以設定「資料外洩防護符合性」指標的設定和例外，以在「安全狀況」標籤上顯示具有可接受的機密資料偵測事件數目的受管理 Security Agent（支援 Data Discovery）百分比。

步驟

1. 移至「管理 > 設定 > Active Directory 和符合性設定」。
2. 按一下「符合性指標」標籤。
3. 按一下「資料外洩防護符合性」。
4. 下表說明可用的組態設定選項。

欄	說明
期間	指定所顯示資料的時間範圍。
可接受的安全威脅偵測數	輸入可接受的機密資料偵測事件數目。
警訊指標	調整滑桿控制項來設定不同警訊層級的門檻值（合規用戶端的百分比）。

5. 在「例外清單」中，選取自訂標籤或過濾器，以將使用者或端點從符合性計算排除。

注意

- 例外清單會套用至所有 Apex Central 使用者。您只能根據您的權限新增或刪除例外，以修改對應的標籤和過濾器。
- 如需有關建立標籤或過濾器的詳細資訊，請參閱自訂標籤 (Tags) 和過濾器 第 7-27 頁。

a. 請點選「新增」。

會出現「新增例外」畫面。

b. 從「類型」下拉式清單中選取「使用者」或「端點」，以按照類型顯示可用的自訂過濾器和標籤；或者，選取「全部」以檢視所有項目。

秘訣

若要搜尋自訂過濾器或標籤，請在文字欄位中輸入名稱並按 Enter 鍵。

如需有關自訂標籤 (Tags) 或過濾器的詳細資訊，請參閱自訂標籤 (Tags) 和過濾器 第 7-27 頁。

c. 選取一或多個自訂標籤 (Tags) 或過濾器，然後按一下「新增」。

選取的項目會顯示在「例外清單」中。

d. 請點選「關閉」。

e. 按一下「儲存」。

f. 從「套用由以下人員新增的例外」下拉式清單中指定已新增的自訂標籤 (Tags) 或過濾器的範圍。

- 所有使用者帳號：排除任何使用者帳號所新增之自訂過濾器和標籤中指定的所有使用者與端點
- 僅已登入的帳號：僅排除目前登入的使用者帳號所新增之自訂過濾器和標籤中指定的使用者與端點

6. 按一下「儲存」。

端點和使用者分組

Apex Central 可以根據下列資訊，將「安全狀況」標籤上的端點或使用者分組：

- 站台位置
- 回報層級管理員

依預設，Apex Central 會從 Active Directory 同步處理使用者或端點站台以及回報層級資訊。您可以設定自訂站台和回報層級群組來顯示符合性資訊。

站台

下表說明「站台」標籤上顯示的站台資訊。

表 6-1. 站台

欄	說明
顯示名稱	輸入在「安全狀況」Widget/標籤上顯示的名稱。 注意 依預設，「其他」群組包含不屬於任何站台的端點。
站台	從 Active Directory 同步處理的站台名稱

建立自訂站台

您可以建立自訂站台群組，來包含某個指定 IP 位址範圍內的端點或使用者。

步驟

1. 移至「管理 > 設定 > Active Directory 和符合性設定」。
2. 按一下「站台」標籤。

3. 按一下「新增自訂」。

   會出現「新增自訂站台」畫面。

4. 指定「顯示名稱」，此名稱用來識別「安全狀況」Widget/標籤上的群組。

5. 選取「節點顏色」，此顏色用來識別「安全狀況」Widget/標籤上的群組。

6. 6.指定自訂站台中包含之端點的 IPv4 或 IPv6 位址範圍

7. 按一下「儲存」。

   建立自訂站台後，可以執行下列作業：

   - 按一下「刪除自訂」，可刪除選取的自訂站台。
   - 按一下自訂站台名稱，可變更設定。

合併站台

您可以藉由合併兩個或更多個站台，來建立一個自訂站台。在合併已存在的站台之後，Apex Central 會從清單移除原始站台。

秘訣

Apex Central 使用實心點圖示 ( ) 表示合併的群組。

步驟

1. 移至「管理 > 設定 > Active Directory 和符合性設定」。
2. 按一下「站台」標籤。
3. 選取兩個或更多個站台。
4. 按一下「合併」。

   會出現「合併站台」畫面。

5. 指定「顯示名稱」，此名稱用來識別「安全狀況」Widget/標籤上的群組。
6. 選取「節點顏色」，此顏色用來識別「安全狀況」Widget/標籤上的群組。
7. 按一下「儲存」。

   在合併站台之後，您可以按一下「分割」來分割合併的站台。

回報層級

下表說明「回報層級」標籤上顯示的資訊。

表 6-2. 回報層級

資料	說明
回報層級	報告列層級會指示使用者在 Active Directory 中的管理階層層級。 從「回報層級」下拉式清單中選取層級數字，然後按一下「套用」來更新清單。
顯示名稱	在「安全狀況」標籤上顯示的名稱 秘訣 依預設，「其他」群組包含回報層級高於所選層級的所有管理員。
管理員	回報層級管理員 會從 Active Directory 伺服器同步處理此資訊。

建立自訂回報層級

您可以建立自訂回報層級，來將直接或間接向所選管理員報告的使用者分組。

步驟

1. 移至「管理 > 設定 > Active Directory 和符合性設定」。
2. 按一下「回報層級」標籤。
3. （選用）變更「回報層級」設定，然後按一下「套用」以更新清單。

   報告列層級會指示使用者在 Active Directory 中的管理階層層級。
4. 按一下「新增自訂」。

   會出現「新增自訂回報層級」畫面。
5. 指定「顯示名稱」，此名稱用來識別「安全狀況」Widget/標籤上的群組。
6. 從「使用者」清單中選取使用者，然後按一下圖示以新增至「選取的使用者」清單。

   注意

   如果要選取多個使用者，請按 Ctrl 鍵並按一下使用者名稱。
7. 按一下「儲存」。

   建立自訂回報層級後，可以執行下列作業：

   - 按一下「刪除自訂」，可刪除選取的自訂回報層級。
   - 按一下自訂群組名稱，可變更設定。

合併回報層級

您可以藉由合併兩個或更多個回報層級，來建立一個自訂回報層級。在合併已存在的回報層級之後，Apex Central 會從清單移除原始回報層級。

秘訣

Apex Central 使用實心點圖示 ( ) 表示合併的群組。

步驟

1. 移至「管理 > 設定 > Active Directory 和符合性設定」。
2. 按一下「回報層級」標籤。
3. 選取兩個或更多個回報層級。
4. 按一下「合併」。

   會出現「合併回報層級」畫面。
5. 指定「顯示名稱」，此名稱用來識別「安全狀況」Widget/標籤上的群組。
6. 按一下「儲存」。

   在合併回報層級之後，您可以按一下「分割」來分割合併的回報層級。

第 7 章

使用者/端點目錄

本節討論如何檢視有關 Apex Central 網路中所有使用者和端點的資訊。

包含下列主題：

- 使用者/端點目錄 第 7-2 頁
- 使用者詳細資料 第 7-3 頁
- 端點詳細資料 第 7-9 頁
- Active Directory 詳細資料 第 7-18 頁
- 受影響的使用者 第 7-18 頁
- 使用進階搜尋 第 7-23 頁
- 自訂標籤 (Tags) 和過濾器 第 7-27 頁

使用者/端點目錄

「使用者/端點目錄」畫面會顯示指定時間範圍內 Apex Central 網路中所有使用者和端點的相關資訊。

- 使用「端點」或「使用者」標籤下方的下拉式清單控制項，可以指定要顯示哪一段時間範圍內的資料，或在「表格式檢視」和「時間表檢視」之間切換。
- 按一下「匯出」將資料匯出為 *.csv 檔案或 *.png 影像。

> **注意**
>
> 「表格式檢視」僅支援將資料匯出為 *.csv 檔案。「時間表檢視」可以將資料匯出為 *.csv 檔案或 *.png 影像。匯出的 *.png 時間表影像只會顯示最多 30 個使用者或端點的資訊。

「使用者/端點」樹狀結構將資料組織成下列類別：

- 使用者：包含有關登入端點或屬於整合式 Active Directory 結構的任何使用者的資訊

  如需詳細資訊，請參閱使用者詳細資料 第 7-3 頁。
- 端點：包含有關將記錄檔傳送到 Apex Central 或屬於整合式 Active Directory 結構的任何端點的資訊

  如需詳細資訊，請參閱端點詳細資料 第 7-9 頁。
- Active Directory：顯示整合式 Active Directory 伺服器的組織單位

> **注意**
>
> Apex Central 支援與多個 Active Directory 樹系進行同步處理。每當新增 Active Directory 網域時，都會自動同步處理同一樹系中的所有網域。
>
> 如需有關樹系信任的詳細資訊，請聯絡您的 Active Directory 管理員。

您可以透過使用進階搜尋、標籤及過濾器，變更「使用者」和「端點」節點中顯示的預設資料。

如需詳細資訊，請參閱使用進階搜尋 第 7-23 頁和自訂標籤 (Tags) 和過濾器 第 7-27 頁。

使用者詳細資料

「使用者/端點目錄」畫面會顯示指定時間範圍內的使用者資訊。

- 使用「端點」或「使用者」標籤下方的下拉式清單控制項，可以指定要顯示哪一段時間範圍內的資料，或在「表格式檢視」和「時間表檢視」之間切換。
- 按一下「匯出」將資料匯出為 *.csv 檔案或 *.png 影像。

注意

「表格式檢視」僅支援將資料匯出為 *.csv 檔案。「時間表檢視」可以將資料匯出為 *.csv 檔案或 *.png 影像。匯出的 *.png 時間表影像只會顯示最多 30 個使用者或端點的資訊。

下表說明「使用者/端點目錄」畫面上「表格式檢視」中顯示的使用者資訊。

表 7-1. 在表格式檢視下的使用者詳細資料

欄	說明
	如果端點或使用者已被指派重要性標籤，Apex Central 會顯示一個黃色星狀圖示 ( ) 來指出重要性。 如需詳細資訊，請參閱使用者或端點重要性 第 7-34 頁。

欄	說明

使用者	Apex Central 可識別使用者並根據端點類型或透過與 Active Directory 的整合，將使用者與端點相關聯。
	• 伺服器和桌面平台：Apex Central 會將上次登入的使用者與端點關聯
	• 行動裝置：
	  • 如果 Active Directory 同步處理可以使用，Apex Central 會利用關聯的 Active Directory 帳號解析行動裝置的已註冊電子郵件信箱
	  • 如果 Active Directory 同步處理無法使用，Apex Central 會顯示行動裝置的已註冊電子郵件信箱
	按一下使用者名稱，可檢視聯絡詳細資料。
	如需詳細資訊，請參閱聯絡資訊 第 7-8 頁。
	注意
	「使用者 > 全部」節點會列出不同端點的所有本機使用者（不論其狀態是否重複）。可能存在名稱相同的重複使用者。Apex Central 會從受管理產品整合具有多個本機使用者的所有端點。

網域	• 如果 Active Directory 同步處理可以使用，此 Apex Central 會顯示使用者所屬的網域名稱。 • 如果 Active Directory 同步處理無法使用，則此 Apex Central 會顯示使用者是其最後一個登入人員的端點/主機名稱。
管理員	如果 Active Directory 同步處理可以使用，Apex Central 會顯示使用者的管理員 按一下「管理員」欄中的名稱，可檢視管理員的聯絡詳細資料。 如需詳細資訊，請參閱聯絡資訊 第 7-8 頁。
端點	目前與使用者關聯的端點數目（根據端點中的上次登入資訊） 按一下計數，可檢視資料表中的相關端點資訊。 如需詳細資訊，請參閱端點詳細資料 第 7-9 頁。

欄	說明
策略	目前與使用者關聯的策略數目（根據端點中的上次登入資訊） 按一下「策略」計數，可檢視使用者的相關策略資訊。 如需詳細資訊，請參閱策略狀態 第 7-8 頁。
安全威脅	在與使用者關聯的端點上發生的安全威脅總數 按一下「安全威脅」計數，可檢視使用者的相關安全威脅資訊。 如需詳細資訊，請參閱使用者所面臨的安全威脅 第 7-6 頁。 例如，如果 Henry 是最後一個登入端點 us-mkt-dev1 的使用者，而該端點回報 10 個病毒/惡意程式偵測和 2 個網頁違規，則 Henry 的「安全威脅」數目會顯示為 12 個。 注意 • 如果您的網路環境並未使用 Active Directory，將不會顯示閘道產品的下列偵測/違規：電子郵件內容違規、網路釣魚電子郵件，以及垃圾郵件。 • 端點產品（例如 Apex One）偵測到的安全威脅，會與端點的最後一個登入使用者關聯。閘道產品（例如 IWSVA）偵測到的安全威脅，會與觸發偵測的使用者關聯。

下表說明「使用者/端點目錄」畫面上「時間表檢視」中顯示的使用者資訊。

表 7-2. 在時間表檢視下的使用者詳細資料

欄	說明
使用者	Apex Central 可識別使用者並根據端點類型或透過與 Active Directory 的整合，將使用者與端點相關聯。
安全威脅	在與使用者關聯的端點上發生的安全威脅總數 按一下「安全威脅」計數，可檢視使用者的相關安全威脅資訊。 如需詳細資訊，請參閱使用者所面臨的安全威脅 第 7-6 頁。

欄	說明
<時間表>	時間表會指出每個使用者的安全威脅發生時間。 • 將滑鼠游標暫留在紅色警告圓點 ( ) 上，可檢視某個使用者在特定日期的嚴重安全威脅數目和所有安全威脅偵測項目總數。 • 將滑鼠游標暫留在實心紅點 ( ) 上，可檢視某個使用者在特定日期的非嚴重安全威脅偵測項目數目。 • 按一下紅點可檢視特定日期的相關安全威脅資訊。 如需詳細資訊，請參閱使用者所面臨的安全威脅 第 7-6 頁。

使用者所面臨的安全威脅

在「使用者」資訊畫面上的「安全威脅」標籤可讓您檢視在指派給所選使用者的端點上偵測到的所有安全威脅。

您可以從 Apex Central 主控台的「資訊中心 > 摘要」標籤上的下列 Widget 存取此畫面。

- 嚴重安全威脅：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。
- 具有安全威脅的使用者：按一下您要檢視的使用者的「威脅」欄中的數字。
- 具有安全威脅的端點：按一下您要檢視的端點的「威脅」欄中的數字。在「端點」資訊畫面上，按一下「一般資訊」標籤，然後按一下使用者名稱。

- 歷來的安全威脅：根據偵測時間以及偵測是否發生於指派的端點或使用者帳號，提供用圖表示的安全威脅資訊。
  - 將滑鼠暫留在安全威脅圖示上（例如， ），可檢視有關該偵測的詳細資料。
  - 變更「縮放」值，可變更顯示的時間間隔。
  - 捲動切換圖表下方顯示的日期，可變更結束日期。
  - 按一下漏斗圖示 ( ) 並選取下列條件，然後使用「或」或「和」運算子建置進階過濾器，即可套用過濾器。
    - 安全威脅類型：從第二個下拉式清單中選取安全威脅類別
    - 安全威脅：輸入惡意程式名稱或可疑 URL、IP 位址或寄件者的電子郵件信箱
    - 安全威脅狀態：選取「已由產品解決」、「需要採取處理行動」或「已手動解決」
- 安全威脅詳細資訊：提供有關「歷來的安全威脅」圖表上顯示的安全威脅的更多詳細資訊
  - 按一下「安全威脅」欄中的值，可檢視「受影響的使用者」畫面。

    如需詳細資訊，請參閱受影響的使用者。
  - 按一下「詳細資料」」欄中的「檢視」連結，可檢視詳細資訊。
  - 按一下 「安全威脅狀態」欄中的旗標圖示 ()，可針對需要進行補救的安全威脅變更安全威脅狀態。

注意

針對安全威脅變更安全威脅狀態，實際上並無法解決該安全威脅。安全威脅狀態是一種案例處理工具，可協助管理員追蹤識別出的安全威脅，並指明安全威脅已解決，讓其他管理員知道。

安全威脅狀態	說明
已由產品解決 ( )	表示受管理產品已解決安全威脅 注意 您無法變更此安全威脅狀態。
需要採取處理行動 ( )	表示需要進行補救 按一下「需要採取處理行動」圖示 ( )，可將安全威脅狀態變更為「已手動解決」( )。
已手動解決 ( )	表示管理員已執行補救 按一下「已由產品解決」圖示 ( )，可將安全威脅狀態變更為「需要採取處理行動」( )。

策略狀態

「策略狀態」標籤顯示目標端點上已安裝的所有產品、指派的任何 Apex Central 策略，以及各個已安裝產品的目前策略狀態。

注意

Apex Central 可識別使用者並根據端點類型或透過與 Active Directory 的整合，將使用者與端點相關聯。

按一下「已指派的策略」名稱以檢視或編輯策略。

聯絡資訊

「聯絡資訊」畫面會顯示類似於 Active Directory 中項目的使用者詳細資料。

將聯絡資訊與 Active Directory 同步處理

Apex Central 會從 Active Directory 通用類別目錄 (GC) 同步處理資料。

步驟

1. 開啟 Microsoft Management Console (MMC)。
2. 新增嵌入式管理單元（Active Directory 架構）。
3. 在左側面板中，移至「屬性」。
4. 對下列各項啟動「複寫這個屬性到通用類別目錄」：
   - ProxyAddresses
   - department
   - homephone
   - PhysicalDeliveryOfficeName
   - telephoneNumber
   - title
5. 等待 Active Directory 複寫開始進行。

端點詳細資料

「使用者/端點目錄」畫面會顯示指定時間範圍內的端點資訊。

- 使用「端點」或「使用者」標籤下方的下拉式清單控制項，可以指定要顯示哪一段時間範圍內的資料，或在「表格式檢視」和「時間表檢視」之間切換。
- 按一下「匯出」將資料匯出為 `*.csv` 檔案或 `*.png` 影像。

注意

「表格式檢視」僅支援將資料匯出為 *.csv 檔案。「時間表檢視」可以將資料匯出為 *.csv 檔案或 *.png 影像。匯出的 *.png 時間表影像只會顯示最多 30 個使用者或端點的資訊。

下表說明「使用者/端點目錄」畫面上「表格式檢視」中顯示的使用者資訊。

欄	說明
	如果端點或使用者已被指派重要性標籤，Apex Central 會顯示一個黃色星狀圖示 ( ) 來指出重要性。 如需詳細資訊，請參閱使用者或端點重要性 第 7-34 頁。
端點	主機名稱或裝置名稱 按一下端點名稱來檢視「端點」畫面，此畫面會開啟到「策略狀態」標籤。 如需詳細資訊，請參閱策略狀態 第 7-14 頁。
IP 位址	端點的靜態或動態 IP 位址
類型	電腦或裝置類型：伺服器、桌上型電腦、筆記型電腦、行動裝置及其他
作業系統	電腦或裝置上執行的作業系統
端點伺服器	負責管理端點之伺服器的伺服器名稱和其上安裝的產品
使用者	最近登入和/或使用端點的使用者之名稱或電子郵件信箱 如需詳細資訊，請參閱聯絡資訊 第 7-8 頁。
安全威脅	在端點上發生的安全威脅總數 按一下「安全威脅」計數，可檢視端點的相關安全威脅資訊。 如需詳細資訊，請參閱端點上的安全威脅 第 7-12 頁。

下表說明「使用者/端點目錄」畫面上「時間表檢視」中顯示的端點資訊。

表 7-3. 在時間表檢視下的端點詳細資料

欄	說明
端點	主機名稱或裝置名稱 按一下端點名稱來檢視「端點」畫面，此畫面會開啟到「策略狀態」標籤。 如需詳細資訊，請參閱策略狀態 第 7-14 頁。 **注意** 如果端點已被指派「重要」標籤，Apex Central 會在端點名稱前面顯示一個黃色星狀圖示 ( )。 如需詳細資訊，請參閱使用者或端點重要性 第 7-34 頁。
安全威脅	在端點上發生的安全威脅總數 按一下「安全威脅」計數，可檢視端點的相關安全威脅資訊。 如需詳細資訊，請參閱端點上的安全威脅 第 7-12 頁。
<時間表>	時間表會指出每個端點的安全威脅發生時間。 • 將滑鼠游標暫留在紅色警告圓點 ( ) 上，可檢視某個端點在特定日期的嚴重安全威脅數目和所有安全威脅偵測項目總數。 • 將滑鼠游標暫留在實心紅點 ( ) 上，可檢視某個端點在特定日期的非嚴重安全威脅偵測項目數目。 如需詳細資訊，請參閱端點上的安全威脅 第 7-12 頁。

端點資訊

「端點」資訊畫面提供有關所選端點的更多詳細資訊。「端點」資訊畫面標題會顯示端點圖示 ( )，後接端點名稱。

按一下下列其中一個標籤，可檢視相關資訊。

- 威脅：顯示在所選端點上偵測到的所有安全威脅

  如需詳細資訊，請參閱端點上的安全威脅 第 7-12 頁。

- 策略狀態：顯示與所選端點相關聯的策略清單

  如需詳細資訊，請參閱策略狀態 第 7-14 頁。

- 注意事項：顯示有關所選端點的任何手動新增的注意事項

  如需詳細資訊，請參閱端點注意事項 第 7-15 頁。

- 一般資訊：顯示有關所選端點的基本資訊

  如需詳細資訊，請參閱端點的一般資訊 第 7-15 頁。

「端點」資訊畫面也可讓您使用「工作」功能表，對所選端點採取特定的處理行動。

- 指派標籤：使標籤與所選端點相關聯以做為搜尋之用

  如需詳細資訊，請參閱自訂標籤 (Tags) 第 7-29 頁。

- 隔離：限制端點對網路和 Internet 的存取權限

  如需詳細資訊，請參閱隔離端點 第 19-32 頁。

- 恢復：恢復對已離隔端點的網路存取權限

  如需詳細資訊，請參閱隔離端點 第 19-32 頁。

端點上的安全威脅

在「端點」資訊畫面上的「安全威脅」標籤可讓您檢視在特定端點上偵測到的所有安全威脅。

您可以從下列位置存取「端點」資訊畫面上的「安全威脅」標籤：

- 「具有安全威脅的端點」Widget：按一下「安全威脅」欄中的計數

  如需詳細資訊，請參閱具有安全威脅的端點 Widget 第 3-20 頁。

- 「端點詳細資料」畫面：按一下「安全威脅」欄中的計數

  如需詳細資訊，請參閱端點詳細資料 第 7-9 頁。

- 「安全威脅」畫面上的「受影響的使用者」標籤：按一下「主機名稱」欄中的端點名稱

  如需詳細資訊，請參閱受影響的使用者 第 7-18 頁。

- 工作：可讓您將「指派標籤」，或者 「隔離」或「恢復」與端點的連線。

  如需詳細資訊，請參閱隔離端點 第 19-32 頁。

- 歷來的安全威脅：根據偵測時間以及偵測是否發生於指派的端點或使用者帳號，提供用圖表示的安全威脅資訊。
  - 將滑鼠暫留在安全威脅圖示上（例如，）），可檢視有關該偵測的詳細資料。
  - 變更「縮放」值，可變更顯示的時間間隔。
  - 捲動切換圖表下方顯示的日期，可變更結束日期。
  - 按一下漏斗圖示 () 並選取下列條件，然後使用「或」或「和」運算子建置進階過濾器，即可套用過濾器。
    - 安全威脅類型：從第二個下拉式清單中選取安全威脅類別
    - 安全威脅：輸入惡意程式名稱或可疑 URL、IP 位址或寄件者的電子郵件信箱
    - 安全威脅狀態：選取「已由產品解決」、「需要採取處理行動」或「已手動解決」
- 安全威脅詳細資訊：提供有關「歷來的安全威脅」圖表上顯示的安全威脅的更多詳細資訊

- 按一下「安全威脅」欄中的值，可檢視「受影響的使用者」畫面。

  如需詳細資訊，請參閱受影響的使用者。

- 按一下「詳細資料」」欄中的「檢視」連結，可檢視詳細資訊。

- 按一下 「安全威脅狀態」欄中的旗標圖示 ( )，可針對需要進行補救的安全威脅變更安全威脅狀態。

注意

針對安全威脅變更安全威脅狀態，實際上並無法解決該安全威脅。安全威脅狀態是一種案例處理工具，可協助管理員追蹤識別出的安全威脅，並指明安全威脅已解決，讓其他管理員知道。

安全威脅狀態	說明
已由產品解決 ( )	表示受管理產品已解決安全威脅 **注意** 您無法變更此安全威脅狀態。
需要採取處理行動 ( )	表示需要進行補救 按一下「需要採取處理行動」圖示 ( )，可將安全威脅狀態變更為「已手動解決」( )。
已手動解決 ( )	表示管理員已執行補救 按一下「已由產品解決」圖示 ( )，可將安全威脅狀態變更為「需要採取處理行動」( )。

策略狀態

「策略狀態」標籤顯示目標端點上已安裝的所有產品、指派的任何 Apex Central 策略，以及各個已安裝產品的目前策略狀態。

按一下「已指派的策略」名稱以檢視或編輯策略。

端點注意事項

您可以手動將注意事項新增到端點，以協助追蹤特定端點上的問題和解決方案。例如，在您調查和解決安全威脅時，或是您在所有安全威脅已解決後即將恢復網路連線時，新增有關隔離端點的其他注意事項。

Apex Central 會自動新增對應於特定處理行動的下列注意事項：

- 「隔離」
- 「恢復」
- 「指派標籤 {標籤名稱}」
- 「移除標籤 {標籤名稱}」

如需詳細資訊，請參閱將自訂標籤 (Tags) 指派給使用者/端點 第 7-30 頁和隔離端點 第 19-32 頁。

端點的一般資訊

您可以檢視有關端點的下列資訊：

資訊	說明
IP 位址	端點的 IP 位址
類型	端點的類型（例如，筆記型電腦）
作業系統	端點上的作業系統

資訊	說明
使用者	與端點相關聯的使用者帳號 **注意** Apex Central 可識別使用者並根據端點類型或透過與 Active Directory 的整合，將使用者與端點相關聯。
網域	與端點相關聯的 Active Directory 網域

隔離端點

隔離有風險的端點，以執行調查並解決安全問題。解決所有問題後，立即恢復連線。

步驟

1. 移至「目錄 > 使用者/端點」。
2. 選取以檢視端點。
3. 按一下清單中某個端點的名稱。
4. 在出現的「端點」資訊畫面中，按一下「工作 > 隔離」。

   Apex Central 會因以下原因而關閉端點上的「隔離」選項：

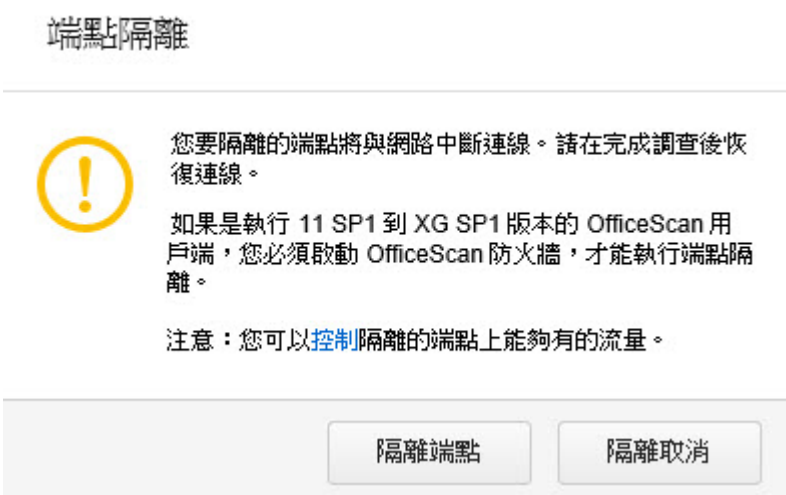
   - 端點上的用戶端執行不受支援的版本。
   - 用於登入 Apex Central 的使用者帳號沒有必要權限。
5. 「端點」資訊畫面頂端會顯示一則訊息，可讓您監控隔離狀態。隔離完成後，訊息會關閉，並在目標端點上顯示一則通知來通知使用者。

   如果隔離過程中發生問題，「端點 — {名稱}」畫面頂端的訊息會通知您發生問題。
6. 如果要檢視您的 Apex Central 網路中所有已隔離的端點，請在「使用者/端點目錄」樹狀結構中按一下「端點 > 過濾器 > 網路內容 > 已隔離」節點。

7. （選用）如果要為所有已隔離端點設定允許的輸入和輸出流量，請執行下列作業：

   如需預設趨勢科技通訊埠的清單，請參閱下載 Security Agent 安裝套件 第 9-2 頁。

   a. 在出現的畫面上，按一下備註中的「控制」超連結。



   b. 選取「控制已隔離端點的流量」。

   c. 展開「輸入流量」或「輸出流量」區段。

   d. 透過指定「通訊協定」、「IP 位址」和「目標通訊埠」，指定允許的流量。

      使用逗號分隔多個目標通訊埠。

   e. 按一下「目標通訊埠」資訊右側的 - 控制項，以新增多個輸入和輸出項目。

注意

修改允許的流量設定後，所有先前隔離的端點和稍後隔離的任何端點，都會套用輸入和輸出流量設定。

---

8. 在解決已隔離端點上的安全威脅後，請從下列位置恢復網路連線：
   - 「端點」資訊畫面：按一下「工作 > 恢復」。
   - 端點 > 過濾器 > 網路連線 > 已隔離：在資料表中選取端點列，然後按一下「工作 > 恢復網路連線」。
9. 畫面頂端會顯示一則訊息，可讓您監控恢復狀態。恢復完成後，訊息會關閉，並在目標端點上顯示一則通知來通知使用者。

   如果恢復過程中發生問題，畫面頂端的訊息會通知您發生問題。

Active Directory 詳細資料

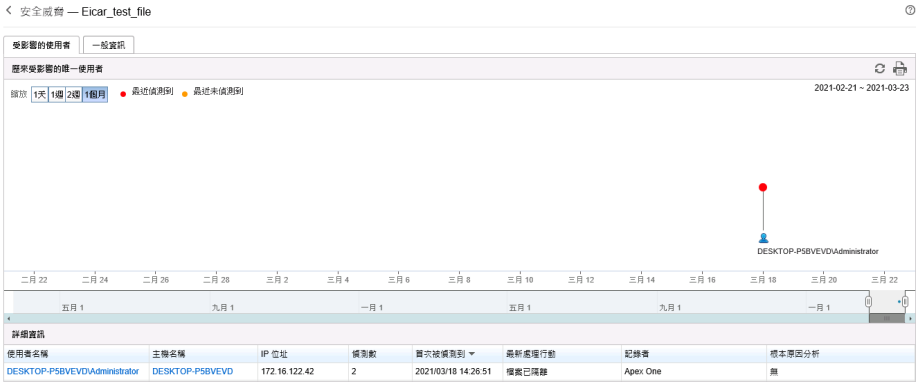
Active Directory 節點會顯示整合式 Active Directory 結構。檢視 Active Directory 節點中的組織單位時，清單將提供兩個標籤：

- 使用者：如需詳細資訊，請參閱使用者詳細資料 第 7-3 頁。
- 端點：如需詳細資訊，請參閱端點詳細資料 第 7-9 頁。

受影響的使用者

「安全威脅」畫面上的「受影響的使用者」標籤，可讓您檢視整個網路中被特定安全威脅鎖定為攻擊目標的使用者。

您可以在「使用者」或「端點」資訊畫面中，透過按一下資料表中的「安全威脅」名稱來存取「受影響的使用者」標籤。



- 歷來受影響的唯一使用者：以圖形顯示受安全威脅影響的使用者和偵測時間
  - 按一下「分析影響」可啟動「根本原因分析」，以判斷安全威脅是否已影響您網路上的其他端點。

    重要

    從「安全威脅資訊」畫面執行影響分析時，需要有效的 Apex One Endpoint Sensor 使用授權，並為適當的 Apex One Security Agent 或 Apex One (Mac) 策略啟動「啟動 Sensor」功能。

    如需詳細資訊，請參閱對受影響的使用者進行影響分析 第 7-20 頁。

  - 按一下「啟動回溯掃瞄」可掃瞄歷史 Web 存取記錄檔，確認在網路中是否存在回呼 C&C 伺服器的嘗試和其他相關活動。

重要

如果要從「安全威脅資訊」畫面執行執行「回溯掃瞄」，必須在 Apex Central 的「伺服器註冊畫面中新增至少一個 Deep Discovery Inspector 伺服器，並且在已註冊的 Deep Discovery Inspector 伺服器上啟動「回溯掃瞄」。

如需詳細資訊，請參閱對受影響的使用者執行回溯掃瞄 第 7-21 頁。

- 將滑鼠游標暫留在某個使用者圖示上，可檢視您環境中受此特定安全威脅影響的所有使用者，以及該安全威脅的偵測歷史記錄
  - 最近偵測到：在掃瞄期間發生的安全威脅偵測
  - 最近未偵測到：在對記錄檔資料進行影響分析期間發生的安全威脅偵測
- 變更「縮放」值，可變更顯示的時間間隔。
- 捲動切換圖表下方顯示的日期，可變更結束日期。

- 詳細資料：提供有關「歷來受影響的唯一使用者」圖形上顯示之安全威脅的更多詳細資訊
  - 按一下「使用者名稱」或「主機名稱」欄中的值，可檢視更多詳細資料。

    如需詳細資訊，請參閱使用者所面臨的安全威脅或端點上的安全威脅。

安全威脅的一般資訊

所顯示的資訊會隨接收自受管理產品的安全威脅類型和安全威脅相關資訊而有所不同。

對受影響的使用者進行影響分析

您可以從 Apex Central 的「安全威脅」畫面上的「受影響的使用者」標籤，對您環境中的安全威脅執行歷史影響分析。

Apex One Endpoint Sensor 會透過聯絡用戶端並對用戶端記錄檔執行歷史掃瞄，來分析您環境中可疑檔案、IP 位址和網域的影響，從而判斷可疑物件是否已影響您的環境一段時間而未被偵測到。

重要

若要執行影響分析，需要有效的 Apex One Endpoint Sensor 使用授權。請確保您的 Apex One Endpoint Sensor 使用授權有效，然後為適當的 Apex One Security Agent 或 Apex One (Mac) 策略啟動「啟動 Sensor」功能。

如需詳細資訊，請參閱《Apex Central Widget 和策略管理手冊》。

步驟

1. 在 Apex Central 主控台中，移至「資訊中心」。
2. 在「具有安全威脅的使用者」或「具有安全威脅的端點」Widget 中，按一下數字。
3. 在出現的畫面中，按一下「安全威脅詳細資訊」資料表中的「安全威脅」名稱。

   會出現「受影響的使用者」畫面。
4. 按一下「分析影響」。

   Endpoint Sensor 會掃瞄歷史網路流量和記錄檔中是否有任何的可疑物件偵測項目。

   如需詳細資訊，請參閱 Endpoint Sensor 中的歷史調查 第 19-16 頁。

對受影響的使用者執行回溯掃瞄

您可以從 Apex Central 的「安全威脅」畫面上的「受影響的使用者」標籤執行「回溯掃瞄」來掃瞄歷史 Web 存取記錄檔，確認在網路中是否存在回呼 C&C 伺服器的嘗試和其他相關活動。

Deep Discovery Inspector 會根據趨勢科技回溯掃瞄所收集的歷史網路流量資訊，來分析可疑 URL 的影響。

重要

如果要從「安全威脅資訊」畫面執行執行「回溯掃瞄」，必須在 Apex Central 的「伺服器註冊畫面中新增至少一個 Deep Discovery Inspector 伺服器，並且在已註冊的 Deep Discovery Inspector 伺服器上啟動「回溯掃瞄」。

如需詳細資訊，請參閱《Deep Discovery Inspector 管理手冊》。

步驟

1. 在 Apex Central 主控台中，移至「資訊中心」。
2. 在「具有安全威脅的使用者」或「具有安全威脅的端點」Widget 中，按一下數字。
3. 在出現的畫面中，按一下「安全威脅詳細資訊」資料表中的「安全威脅」名稱。

   會出現「受影響的使用者」畫面。
4. 按一下「啟動回溯掃瞄」

   Deep Discovery Inspector 會掃瞄歷史 Web 存取記錄檔，確認在網路中是否存在回呼 C&C 伺服器的嘗試和其他相關活動。

   如需詳細資訊，請參閱 Deep Discovery Inspector 中的回溯掃瞄 第 7-22 頁。

Deep Discovery Inspector 中的回溯掃瞄

回溯掃瞄是以雲端為基礎的服務，這項服務會掃瞄歷史 Web 存取記錄檔，確認在網路中是否存在回呼 C&C 伺服器的嘗試和其他相關活動。Web 存取記錄檔可能僅包括與 C&C 伺服器之間最近才發現的未偵測和解除封鎖連線。檢查這些記錄檔是鑑識調查的重要環節，這可以判斷您的網路是否受到攻擊的影響。

回溯掃瞄會將下列記錄檔資訊儲存在主動式雲端截毒技術中：

- Deep Discovery Inspector 所監控的端點 IP 位址

- 端點所存取的 URL
- Deep Discovery Inspector 的 GUID

回溯掃瞄會接著定期掃瞄儲存的記錄項目，以檢查是否存在回呼下列清單中 C&C 伺服器的嘗試：

- 趨勢科技全球資訊清單：趨勢科技從多個來源編譯清單，並評估每個 C&C 回呼位址的風險等級。C&C 清單會每天更新並傳送到已啟動的產品。
- 使用者定義的清單：回溯掃瞄也會掃瞄記錄檔，來比對您自己的 C&C 伺服器清單。位址必須儲存在文字檔案中。

重要

Deep Discovery Inspector 中「回溯掃瞄」畫面只會顯示有關使用趨勢科技全球資訊清單的掃瞄資訊。

使用進階搜尋

Apex Central 允許您使用部分字串比對來搜尋使用者或端點。您也可以使用布林運算子來過濾清單中顯示的使用者或端點。

步驟

1. 移至「目錄 > 使用者/端點」。

   會出現「使用者/端點目錄」畫面。

2. 按一下資料表上方的「進階」連結。
3. 在「搜尋」下拉式清單中，選取「使用者」或「端點」。

   第二個下拉式清單控制項中的搜尋條件會根據您的選取項目而動態變更。

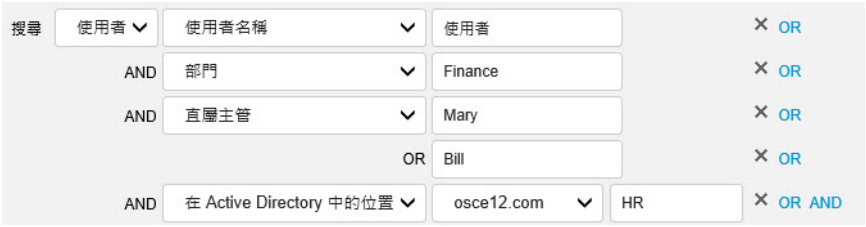
   如需詳細資訊，請參閱進階搜尋類別 第 7-25 頁。

4. 使用過濾器右側的布林運算子新增多個搜尋條件。

5. 使用過濾器右側的布林運算子新增多個搜尋條件。

   - OR：允許您針對指定的條件搜尋多個值。符合任一個值的所有記錄均會顯示。
   - AND：允許您選取新的搜尋條件。僅顯示既符合針對此條件指定的值，又符合所有其他選取的條件值的記錄。

   若要過濾 Active Directory 網域 "HR" 中財務部門裡 "Mary" 或 "Bill" 下屬中姓名包含 "ja" 的所有使用者，請指定下列條件：



6. 按一下下列其中一個項目，以顯示結果：

   - 搜尋：在清單中顯示搜尋結果，但不會儲存搜尋條件。
   - 另存為新的自訂過濾器：在清單中顯示搜尋結果，並提示您將搜尋條件儲存為自訂過濾器。自訂過濾器會顯示在「使用者/端點目錄」樹狀結構中的「使用者」或「端點」節點下方。

     如需詳細資訊，請參閱過濾器 第 7-31 頁。

7. （選用）使用「端點」或「使用者」標籤下方的下拉式清單控制項，可以指定要顯示哪一段時間範圍內的資料，或在「表格式檢視」和「時間表檢視」之間切換。

8. （選用）按一下「匯出」將資料匯出為 *.csv 檔案或 *.png 影像。

注意

- 「表格式檢視」僅支援將資料匯出為 *.csv 檔案。
- 「時間表檢視」可以將資料匯出為 *.csv 檔案或 *.png 影像。

進階搜尋類別

在執行進階搜尋時，請針對「使用者」和「端點」使用下列搜尋條件選項。

表 7-4. 使用者類別

類別	說明
使用者名稱	本機使用者或屬於 Active Directory 結構之人員的帳號名稱
直屬主管	使用者直屬主管的帳號名稱
在 Active Directory 中的位置	開始對其搜尋的組織單位
部門	在您的公司中，根據職務（例如，會計）或其他條件將使用者分組的部門名稱
Active Directory 群組	Active Directory 使用者和電腦帳號的集合，可將聯絡人和其他群組視為單一單位加以管理
安全威脅類型	從第三個下拉式清單中選取安全威脅類型
安全威脅	透過輸入惡意程式名稱、URL、IP 位址或寄件者電子郵件信箱，搜尋特定安全威脅
安全威脅狀態	「安全威脅」畫面上第一欄中的旗子圖示，指出下列補救狀態：已由產品解決、需要採取處理行動、已手動解決 如需詳細資訊，請參閱使用者所面臨的安全威脅 第 7-6 頁。
重要性	指派的重要性層級 如需詳細資訊，請參閱使用者或端點重要性 第 7-34 頁。
Active Directory 站台	從 Active Directory 同步處理的站台名稱 如需詳細資訊，請參閱端點和使用者分組 第 6-11 頁。
回報層級	從 Active Directory 同步處理的回報層級顯示名稱 如需詳細資訊，請參閱端點和使用者分組 第 6-11 頁。

表 7-5. 端點類別

類別	說明
端點名稱	端點的主機或裝置名稱
IP 位址	IPv4 位址範圍 注意 依 IPv4 網段搜尋需要特定範圍（開頭為首個八位元）。搜尋會傳回 IP 位址中包含此項目的所有端點。
端點類型	電腦或裝置類型：伺服器、桌上型電腦、筆記型電腦、行動裝置或其他
作業系統	端點上的作業系統類型
在 Active Directory 中的位置	開始對其搜尋的組織單位
安全威脅類型	從第三個下拉式清單中選取安全威脅類型
安全威脅	透過輸入惡意程式名稱、URL、IP 位址或寄件者電子郵件信箱，搜尋特定安全威脅
安全威脅狀態	「安全威脅」畫面上第一欄中的旗子圖示，指出下列補救狀態：已由產品解決、需要採取處理行動、已手動解決 如需詳細資訊，請參閱端點上的安全威脅 第 7-12 頁。
符合性	防毒特徵碼符合性或資料外洩防護符合狀態 如需詳細資訊，請參閱符合性指標 第 6-6 頁。
重要性	指派的重要性層級 如需詳細資訊，請參閱使用者或端點重要性 第 7-34 頁。
Active Directory 站台	從 Active Directory 同步處理的站台名稱 如需詳細資訊，請參閱端點和使用者分組 第 6-11 頁。
回報層級	從 Active Directory 同步處理的回報層級顯示名稱 如需詳細資訊，請參閱端點和使用者分組 第 6-11 頁。

類別	說明
安裝模式	Security Agent 安裝模式 如需詳細資訊，請參閱下載 Security Agent 安裝套件 第 9-2 頁。
服務	Security Agent 服務 如需詳細資訊，請參閱《Apex Central Widget 和策略管理手冊》。
Apex One 網域階層	端點在 Apex One 網域階層中的位置

自訂標籤 (Tags) 和過濾器

請根據您的網路和管理需求來使用標籤和過濾器。在使用標籤和過濾器時，Trend Micro 建議您考量下列事項：

- 根據您的 Active Directory 組織將使用者分組
- 根據端點的位置將端點分組
- 將具有類似內容或特性的使用者或端點分為一組

  例如：

  - 根據直接監督員關聯將使用者分組
  - 將使用相同作業系統的端點分為一組

注意

- 任何 Apex Central 使用者帳號只要在「使用者/端點目錄」中擁有建立或修改自訂標籤 (Tags)、過濾器或重要標籤的權限，就可以檢視或修改所有其他使用者帳號所建立的自訂標籤 (Tags)、過濾器或重要標籤。
- 在「使用者/端點目錄」畫面上編輯標籤、過濾器或重要性標籤時，也會一併修改記錄查詢和報告所用的對應標籤、過濾器或重要性標籤。例如，如果在「使用者/端點目錄」畫面上，將端點從自訂過濾器中移除，則使用該過濾器的記錄查詢和產生的報告將會排除已移除端點中的資料。
- Apex Central 會在 Active Directory 同步處理之後，自動將重要性指派給「網域管理員」（使用者）和「網域控制站」（端點）。
  - 目前的 Apex Central 版本僅支援每個整合式 Active Directory 網域有一位重要的「網域管理員」和一個重要的「網域控制站」。個別使用者帳號無法再為相同的「網域管理員」和「網域控制站」指派不同的「重要」標籤。
  - 如果在舊版 Apex Central 上，已存在不同使用者帳號針對「網域管理員」和「網域控制站」所建立的「重要」標籤，則現有的「網域管理員」和「網域控制站」將被刪除，並更換為每個整合式 Active Directory 網域有一位「網域管理員」和一個重要的「網域控制站」。

秘訣

- 在「使用者存取」記錄查詢資料檢視中，會提供與任何可用自訂標籤 (Tags) 或過濾器相關之任何使用者修改的詳細資訊。

  如需詳細資訊，請參閱下列主題：

  - 查詢記錄檔 第 15-2 頁
  - 使用者存取資訊 第 B-90 頁
- 透過指定相關聯的標籤、過濾器或重要標籤做為報告目標，針對已加標籤的使用者和端點產生自訂報告。

  如需詳細資訊，請參閱下列主題：

  - 建立一次性報告 第 17-19 頁
  - 新增預約報告 第 17-23 頁
  - 編輯預約報告 第 17-27 頁

自訂標籤 (Tags)

「自訂標籤 (Tags)」是您可手動關聯一或多個使用者/端點來將其分組的標籤。

- 依預設，Apex Central 不會指派標籤給任何使用者或端點。
- 您可以將多個自訂標籤 (Tags) 套用至多個使用者/端點。
- 任何 Apex Central 使用者帳號只要在「使用者/端點目錄」中擁有建立或修改自訂標籤 (Tags)、過濾器或重要標籤的權限，就可以檢視或修改所有其他使用者帳號所建立的自訂標籤 (Tags)、過濾器或重要標籤。

建立自訂標籤 (Tags)

注意

- 任何 Apex Central 使用者帳號只要在「使用者/端點目錄」中擁有建立或修改自訂標籤 (Tags)、過濾器或重要標籤的權限，就可以檢視或修改所有其他使用者帳號所建立的自訂標籤 (Tags)、過濾器或重要標籤。
- 在「使用者/端點目錄」畫面上編輯標籤、過濾器或重要性標籤時，也會一併修改記錄查詢和報告所用的對應標籤、過濾器或重要性標籤。例如，如果在「使用者/端點目錄」畫面上，將端點從自訂過濾器中移除，則使用該過濾器的記錄查詢和產生的報告將會排除已移除端點中的資料。

步驟

1. 移至「目錄 > 使用者/端點」。
2. 在樹狀結構中，展開「使用者」或「端點」下的「自訂標籤 (Tags)」節點。
3. 按一下「新增自訂標籤 (Tags)」。
4. 為標籤輸入描述性名稱，然後按 Enter 鍵或按一下 以儲存新標籤。

   標籤會出現在「使用者」或「端點」標籤清單中。

   建立自訂標籤 (Tags) 後，可以執行下列作業：

- 按一下任何自訂標籤 (Tags) 旁的 圖示，可編輯標籤名稱。
- 按一下任何自訂標籤 (Tags) 旁的 圖示，可刪除標籤。

將自訂標籤 (Tags) 指派給使用者/端點

注意

- 任何 Apex Central 使用者帳號只要在「使用者/端點目錄」中擁有建立或修改自訂標籤 (Tags)、過濾器或重要標籤的權限，就可以檢視或修改所有其他使用者帳號所建立的自訂標籤 (Tags)、過濾器或重要標籤。
- 在「使用者/端點目錄」畫面上編輯標籤、過濾器或重要性標籤時，也會一併修改記錄查詢和報告所用的對應標籤、過濾器或重要性標籤。例如，如果在「使用者/端點目錄」畫面上，將端點從自訂過濾器中移除，則使用該過濾器的記錄查詢和產生的報告將會排除已移除端點中的資料。

步驟

1. 移至「目錄 > 使用者/端點」。
2. 選取要檢視的「使用者」或「端點」，或是搜尋特定的使用者/端點。
3. 如果要將自訂標籤 (Tags) 與使用者/端點關聯，請執行下列作業：
   - 按一下使用者/端點列，然後按一下「工作 > 指派/移除自訂標籤 (Tags)」。
   - 以滑鼠右鍵按一下使用者/端點列，然後按一下「指派/移除自訂標籤 (Tags)」。
4. 在「指派/移除自訂標籤 (Tags)」對話方塊中，從清單中選取或清除必要標籤，然後按一下「儲存」。

   您可以透過從「自訂標籤 (Tags)」清單中選取標籤，然後檢查選取的使用者或端點是否正常顯示，來驗證標籤與選取的使用者或端點是否正確關聯。

過濾器

過濾器會自動對具有相同條件的使用者或端點進行分組。

- 您可以根據自訂標籤和過濾器，將「使用者」或「端點」分組或指派重要性。

  如需詳細資訊，請參閱建立自訂過濾器 第 7-33 頁和使用者或端點重要性 第 7-34 頁。

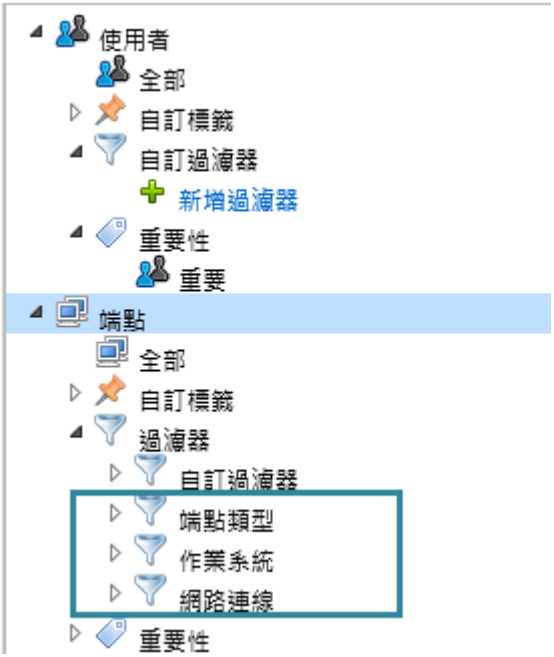
- 此外，「端點」樹狀結構也會根據預設過濾器將端點分組。

  如需詳細資訊，請參閱預設端點過濾器 第 7-32 頁。

- 任何 Apex Central 使用者帳號只要在「使用者/端點目錄」中擁有建立或修改自訂標籤 (Tags)、過濾器或重要標籤的權限，就可以檢視或修改所有其他使用者帳號所建立的自訂標籤 (Tags)、過濾器或重要標籤。

預設端點過濾器

依預設，「端點」樹狀結構會根據組織中典型的端點分組來提供預設過濾器。



展開其中一個預設過濾器，然後選取要顯示的端點類型。

如需有關資料表欄和其中所包含資料的詳細資訊，請參閱使用者詳細資料 第 7-3 頁。

下列是預設過濾器：

- 端點類型：伺服器、桌上型電腦、筆記型電腦、行動裝置和其他類型
- 作業系統：安裝於端點上的常見作業系統，包括 Windows、Mac OS、iOS、Android 和其他作業系統
- 網路連線：隔離的端點

注意

在檢視「已隔離」端點後，您可以按一下「工作 > 恢復網路連線」來停止隔離。

建立自訂過濾器

注意

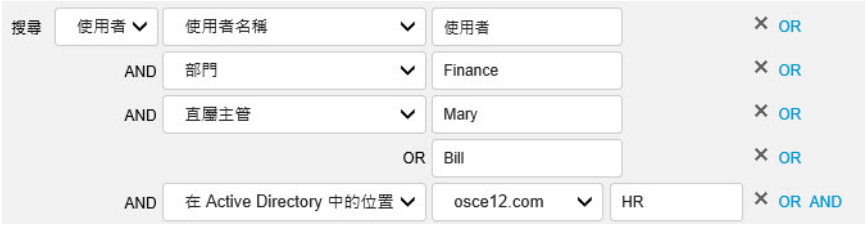
- 任何 Apex Central 使用者帳號只要在「使用者/端點目錄」中擁有建立或修改自訂標籤 (Tags)、過濾器或重要標籤的權限，就可以檢視或修改所有其他使用者帳號所建立的自訂標籤 (Tags)、過濾器或重要標籤。
- 在「使用者/端點目錄」畫面上編輯標籤、過濾器或重要性標籤時，也會一併修改記錄查詢和報告所用的對應標籤、過濾器或重要性標籤。例如，如果在「使用者/端點目錄」畫面上，將端點從自訂過濾器中移除，則使用該過濾器的記錄查詢和產生的報告將會排除已移除端點中的資料。

步驟

1. 移至「目錄 > 使用者/端點」。
2. 在樹狀結構中展開「自訂過濾器」節點。
   - 對於「使用者」，請展開「自訂過濾器」。
   - 對於「端點」，請展開「過濾器」，然後再展開「自訂過濾器」。
3. 按一下「新增過濾器」。

   資料表上方「搜尋」區域會變更，以允許您選取過濾條件。
4. 根據可用的條件過濾使用者或端點。

下列範例會過濾 Active Directory 網域 "HR" 中財務部門裡 "Mary" 或 "Bill" 下屬中姓名包含 "ja" 的所有使用者：



如需詳細資訊，請參閱進階搜尋類別 第 7-25 頁。

建立自訂過濾器後，可以執行下列作業：

- 按一下任何自訂過濾器旁的 圖示，可編輯過濾器名稱。
- 按一下任何自訂過濾器旁的 圖示，可更新布林表示式。
- 按一下任何自訂過濾器旁的 圖示，可刪除過濾器。

使用者或端點重要性

將重要性指派給使用者群組和端點群組，可讓您透過「資訊中心」畫面快速監控並回應攻擊這些目標的安全威脅。Apex Central 提供多個 Widget，為「重要」使用者與端點醒目提示安全威脅事件。您也許想要將較嚴格的策略套用到重要使用者或端點，並且持續監控其防護狀態。

您必須先指派自訂標籤，或是建立自訂過濾器，來識別重要使用者或端點。在識別網路上的重要使用者或端點後，即可指派「重要」標籤，以在「資訊中心」上提供更佳的可見性。

如需詳細資訊，請參閱自訂標籤 (Tags) 和過濾器 第 7-27 頁。

注意

- 手動將重要性指派給使用自訂標籤 (Tags) 和過濾器分組的使用者/端點。
- 任何 Apex Central 使用者帳號只要在「使用者/端點目錄」中擁有建立或修改自訂標籤 (Tags)、過濾器或重要標籤的權限，就可以檢視或修改所有其他使用者帳號所建立的自訂標籤 (Tags)、過濾器或重要標籤。
- 在「使用者/端點目錄」畫面上編輯標籤、過濾器或重要性標籤時，也會一併修改記錄查詢和報告所用的對應標籤、過濾器或重要性標籤。例如，如果在「使用者/端點目錄」畫面上，將端點從自訂過濾器中移除，則使用該過濾器的記錄查詢和產生的報告將會排除已移除端點中的資料。
- Apex Central 會在 Active Directory 同步處理之後，自動將重要性指派給「網域管理員」（使用者）和「網域控制站」（端點）。
  - 目前的 Apex Central 版本僅支援每個整合式 Active Directory 網域有一位重要的「網域管理員」和一個重要的「網域控制站」。個別使用者帳號無法再為相同的「網域管理員」和「網域控制站」指派不同的「重要」標籤。
  - 如果在舊版 Apex Central 上，已存在不同使用者帳號針對「網域管理員」和「網域控制站」所建立的「重要」標籤，則現有的「網域管理員」和「網域控制站」將被刪除，並更換為每個整合式 Active Directory 網域有一位「網域管理員」和一個重要的「網域控制站」。

步驟

1. 移至「目錄 > 使用者/端點」。
2. 展開樹狀結構中「使用者」或「端點」下的「重要性」節點。
3. 按一下「重要」，然後按一下「編輯」圖示 ( )。
4. 在顯示的畫面上：
   - 選取一或多個自訂標籤或自訂過濾器來指派重要性，然後按一下「儲存」。
   - 不勾選一或多個自訂標籤或自訂過濾器來移除重要性，然後按一下「儲存」。

   主畫面中的資料表會更新，並顯示符合自訂標籤或自訂過濾器的端點或使用者清單。

如需有關資料表欄和其中所包含資料的詳細資訊，請參閱使用者詳細資料 第 7-3 頁。

部分 III

受管理產品整合

第 8 章

受管理產品註冊

本節討論如何向 Apex Central 伺服器註冊受管理產品和伺服器。

包含下列主題：

- 受管理產品註冊方法 第 8-2 頁
- 伺服器註冊 第 8-2 頁
- 受管理產品的通訊 第 8-10 頁

受管理產品註冊方法

Apex Central 藉由使用下列其中一種方法，要求受管理產品向 Apex Central 伺服器註冊：

- Apex Central 管理主控台上的「伺服器註冊」畫面
- 受管理產品的管理主控台（透過 Apex Central MCP 代理程式）

伺服器註冊

「伺服器註冊」畫面（「管理 > 受管理的伺服器 > 伺服器註冊」）可讓您使用 Apex Central 管理主控台註冊、設定受管理產品，或取消註冊已向 Apex Central 註冊的受管理產品。

如需有關使用受管理產品 Web 主控台向 Apex Central 註冊之產品的詳細資訊，請參閱連線的威脅防範產品整合 第 19-34 頁。

使用「伺服器註冊」畫面執行下列工作。

工作	說明
新增受管理的伺服器	按一下「新增」，即可向 Apex Central 伺服器註冊受管理的產品。 如需詳細資訊，請參閱新增受管理的伺服器 第 8-4 頁。 注意 如果「新增」圖示已關閉，則受管理的產品會使用受管理產品主控台向 Apex Central 註冊。
編輯受管理的伺服器設定	按一下「處理行動」欄中的「編輯」圖示，修改受管理伺服器的組態設定。 如需詳細資訊，請參閱編輯受管理的伺服器 第 8-6 頁。

工作	說明
刪除受管理的伺服器	按一下「處理行動」欄中的「刪除」圖示，從 Apex Central 伺服器取消註冊受管理的伺服器。 如需詳細資訊，請參閱刪除受管理的伺服器 第 8-7 頁。
設定 Proxy 伺服器設定	按一下「Proxy 伺服器設定」，可設定受管理產品的 Proxy 伺服器設定。 如需詳細資訊，請參閱設定受管理產品的 Proxy 伺服器設定 第 8-8 頁。
設定雲端服務設定	按一下「雲端服務設定」來註冊、編輯或取消註冊雲端服務 如需詳細資訊，請參閱設定雲端服務設定 第 8-10 頁。
組織「產品目錄」結構中的受管理伺服器	按一下「目錄管理」來分組「產品目錄」結構中的受管理的產品或移至新位置 如需詳細資訊，請參閱管理產品目錄 第 10-12 頁。
以單一登入方式登入受管理產品主控台	按一下「伺服器」欄中的連結，即可以單一登入方式登入受管理產品主控台。 **秘訣** 您也可以從「產品目錄」畫面，以單一登入方式登入受管理產品主控台。 如需詳細資訊，請參閱產品目錄 第 10-2 頁。

注意

如需有關「伺服器註冊」畫面顯示的詳細資料的詳細資訊，請參閱受管理伺服器詳細資料 第 8-3 頁。

受管理伺服器詳細資料

下表說明「伺服器註冊」畫面顯示的資訊。

欄名稱	說明
伺服器	顯示受管理產品的伺服器名稱 注意 按一下使用 MCP 代理程式向 Apex Central 註冊之受管理產品的伺服器名稱，會將您重新導向到受管理產品主控台。
顯示名稱	顯示受管理產品的伺服器顯示名稱
產品	顯示受管理產品的名稱
連線類型	顯示受管理產品如何向 Apex Central 註冊 • 自動：受管理產品透過 MCP 代理程式向 Apex Central 註冊 。 如需詳細資訊，請參閱連線的威脅防範產品整合 第 19-34 頁。 • 手動：管理員使用「伺服器註冊」畫面註冊受管理產品。 如需詳細資訊，請參閱新增受管理的伺服器 第 8-4 頁。 • 雲端服務：受管理產品透過「雲端服務設定」進行註冊。 如需詳細資訊，請參閱設定雲端服務設定 第 8-10 頁。
上次報告	顯示 Apex Central 最近一次從受管理產品收到回應的日期和時間
沙箱	顯示受管理產品向其提交樣本的已註冊沙箱（如果有）
處理行動	• 編輯：按一下此圖示可更新伺服器資訊 如需詳細資訊，請參閱編輯受管理的伺服器 第 8-6 頁。 • 刪除：按一下此圖示可取消註冊受管理伺服器 如需詳細資訊，請參閱刪除受管理的伺服器 第 8-7 頁。

新增受管理的伺服器

使用「伺服器註冊」畫面，可以向 Apex Central 伺服器註冊受管理的伺服器。

注意

- 如果「新增」按鈕處於關閉狀態，則會使用受管理的產品管理主控台向 Apex Central 註冊產品。

  如需詳細資訊，請參閱連線的威脅防範產品整合 第 19-34 頁。

- 在對最近新增的受管理伺服器執行策略管理前，請先按一下「目錄管理」，然後將受管理的產品從「新實體」資料夾移至其他位置。

  如需詳細資訊，請參閱管理產品目錄 第 10-12 頁。

步驟

1. 移至「管理 > 受管理的伺服器 > 伺服器註冊」。

   會出現「伺服器註冊」畫面。

2. 從「伺服器類型」下拉式清單中選取產品。

   會出現已註冊受管理伺服器的清單。

3. 按一下資料表中的「新增」按鈕或「新增產品」連結。

   會出現「新增伺服器」畫面。

4. 指定下列伺服器資訊：

   - 伺服器：輸入 <受管理的產品> 伺服器名稱、FQDN 或 IPv4/IPv6 位址，以及通訊埠號碼（如果有的話）。

     重要

     伺服器位址必須以 `HTTP` 或 `HTTPS` 為開頭。

   - 顯示名稱：指定 <受管理的產品> 伺服器在 Apex Central 中顯示的名稱。

5. 如果登入受管理的伺服器需要驗證，請指定下列認證：

   - 使用者名稱：提供具有管理員權限的 <受管理的產品> 帳號的名稱。
   - 密碼：輸入所提供帳號的密碼。

重要

Apex Central 需要具有管理員權限的帳號，才能部署策略設定。

6. （選用）如果要使用 Proxy 伺服器，請選取「使用 Proxy 伺服器來連線」核取方塊。

   如需詳細資訊，請參閱設定受管理產品的 Proxy 伺服器設定 第 8-8 頁。

7. 如果要啟動樣本提交，請從「沙箱」下拉式清單中選取沙箱產品/服務。

重要

- 對於 Deep Security 和 Trend Micro Endpoint Sensor，您必須先新增受管理的伺服器，然後編輯伺服器來選取沙箱。
- 對於所有其他受管理的產品，您可以在第一次新增受管理的伺服器時選取沙箱。
- 如需詳細資訊，請參閱連線的威脅防範產品整合 第 19-34 頁。

8. 按一下「儲存」。

   最近新增的伺服器會顯示在已註冊的受管理伺服器清單中。

編輯受管理的伺服器

使用「伺服器註冊」畫面可編輯向 Apex Central 伺服器註冊的受管理伺服器資訊。

步驟

1. 移至「管理 > 受管理的伺服器 > 伺服器註冊」。

   會出現「伺服器註冊」畫面。

2. 從「伺服器類型」下拉式清單中選取產品。

   會出現已註冊受管理伺服器的清單。

3. 針對您想要編輯的受管理伺服器，按一下「處理行動」欄中的「編輯」圖示。

   會出現「編輯伺服器」畫面。

4. 編輯伺服器資訊。

   - 驗證：如果伺服器需要驗證才能登入，請提供使用者名稱和密碼。
   - 連線：選取「使用 Proxy 伺服器來連線」核取方塊，以使用設定的 Proxy 伺服器。

     如需詳細資訊，請參閱設定受管理產品的 Proxy 伺服器設定 第 8-8 頁。
   - 樣本提交：從「沙箱」下拉式清單中選取沙箱產品/服務。

     重要

     - 如果「沙箱」下拉式清單顯示「不支援」，則必須從受管理產品伺服器主控台（例如 Deep Discovery Inspector 主控台）設定沙箱產品/服務，而非從 Apex Central 進行設定。
     - 由節點 Apex Central 所管理的 Apex One 伺服器可以選取已向中樞 Apex Central 註冊的 Deep Discovery Analyzer 做為沙箱產品/服務。

     如需詳細資訊，請參閱連線的威脅防範產品整合 第 19-34 頁。

5. 按一下「儲存」。

刪除受管理的伺服器

可以使用「伺服器註冊」畫面，將受管理的伺服器從 Apex Central 取消註冊。

步驟

1. 移至「管理 > 受管理的伺服器 > 伺服器註冊」。

會出現「伺服器註冊」畫面。

2. 點選「目錄管理」。
3. 展開產品樹狀結構並選取要刪除的伺服器。
4. 請點選「刪除」。

   會出現確認畫面。
5. 請點選「確定」。

   所選伺服器即會從產品樹狀結構刪除。

> **注意**
>
> 在「伺服器註冊」畫面上刪除受管理的伺服器，並不會解除安裝伺服器程式或相關的用戶端。

6. 在伺服器的管理主控台上，移至產品註冊畫面，然後從 Apex Central 取消註冊伺服器。
7. 請點選「確定」。

設定受管理產品的 Proxy 伺服器設定

Apex Central 允許您使用 Proxy 伺服器來連線到內部網路中的受管理產品。在設定受管理產品的 Proxy 伺服器設定後，請啟動特定受管理伺服器的 Proxy 伺服器連線。

如需詳細資訊，請參閱編輯受管理的伺服器 第 8-6 頁。

> **重要**
>
> 您只能針對相同受管理產品類型的所有受管理伺服器使用一部 Proxy 伺服器。

步驟

1. 移至「管理 > 受管理的伺服器 > 伺服器註冊」。

   會出現「伺服器註冊」畫面。

2. 從「伺服器類型」下拉式清單中選取產品。

   會出現已註冊受管理伺服器的清單。

3. 按一下「Proxy 伺服器設定」。

   會出現「Proxy 伺服器設定」畫面。

4. 選取下列其中一個通訊協定：

   - HTTP
   - SOCKS 4
   - SOCKS 5

5. 指定下列欄位：

   - 伺服器：輸入 Proxy 伺服器的伺服器名稱、FQDN 或 IPv4 位址
   - 通訊埠：輸入 Proxy 伺服器用於用戶端連線的通訊埠號碼

6. 如果 Proxy 伺服器需要驗證，請指定下列認證：

   - 使用者名稱
   - 密碼

7. 按一下「儲存」。

8. 如果要啟動 Proxy 伺服器連線，請執行下列作業：

   a. 針對您想要編輯的受管理伺服器，按一下「處理行動」欄中的「編輯」圖示。

      會出現「編輯伺服器」畫面。

   b. 在「連線」區段中選取「使用 Proxy 伺服器來連線」核取方塊。

c. 按一下「儲存」。

設定雲端服務設定

您可以使用「伺服器註冊」畫面，將受管理的雲端服務向 Apex Central 註冊或取消註冊。

步驟

1. 移至「管理 > 受管理的伺服器 > 伺服器註冊」。

   會出現「伺服器註冊」畫面。

2. 按一下「雲端服務設定」。

   會出現「雲端服務設定」畫面。

3. 如果要註冊雲端服務，提供下列認證：

   - 帳號：輸入您用來在 Trend Micro Customer Licensing Portal (https://clp.trendmicro.com/) 中啟動雲端服務產品授權的使用者名稱。
   - 密碼：輸入雲端服務帳號的密碼。

4. 如果要取消註冊雲端服務，請按一下「停止使用 Apex Central 管理服務」，然後同意所有後續出現的提示。

5. 請點選「確定」。

受管理產品的通訊

Apex Central 使用安裝於受管理伺服器的管理通訊協定 (MCP) 代理程式與未透過 Apex Central 管理主控台向 Apex Central 伺服器註冊的受管理產品進行通訊。

MCP 代理程式會按固定的間隔傳送活動訊號以指出受管理產品運作正常，藉此與 Apex Central 伺服器進行通訊。

管理員可以設定用戶端通訊預約時程，來決定用戶端何時將活動訊號傳送到 Apex Central 伺服器。

重要

Apex Central 僅允許為透過 Apex Central 管理主控台向 Apex Central 伺服器註冊的受管理產品設定用戶端通訊預約時程。

修改預設用戶端通訊預約時程

Apex Central 使用預設的用戶端通訊預約時程與所有沒有自訂用戶端通訊預約時程的受管理產品進行通訊。

使用「設定通訊器預約時程」畫面，藉由按一下時段變更通訊狀態，來修改預設預約時程。

步驟

1. 移至「管理 > 受管理的伺服器 > 用戶端通訊預約時程」。

   會出現「用戶端通訊預約時程」畫面。

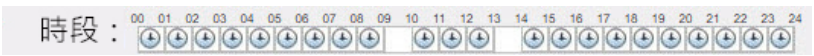
2. 在「通訊器」欄中，按一下「預設預約時程」。

   會出現「設定通訊器預約時程」。

3. 按一下時段來變更用戶端通訊狀態。

   - 將某個時段設定為「閒置」會建立連續的時間範圍，用戶端會在此時間範圍內將活動訊號傳送到 Apex Central 伺服器。

     例如，將時段 09 和 13 設定為「閒置」，會建立兩個連續時段的時間範圍。



- 您可以指定最多三個「預約」時段的連續時間範圍，用戶端會在此時間範圍內將活動訊號傳送到 Apex Central 伺服器。

4. 按一下「儲存」。

設定用戶端通訊預約時程

您可以在「設定通訊器預約時程」畫面上按一下某個時段來變更通訊狀態，即可自訂受管理產品的用戶端通訊預約時程。

重要

您只能為每一個受管理產品設定一個用戶端通訊預約時程。

步驟

1. 移至「管理 > 受管理的伺服器 > 用戶端通訊預約時程」。

   會出現「用戶端通訊預約時程」畫面。

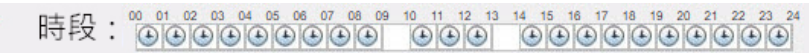
2. 在「通訊器」欄中，按一下要修改的受管理產品。

   會出現「設定通訊器預約時程」畫面。

3. 按一下某個時段以變更通訊狀態。

   - 將某個時段設定為「閒置」會建立連續的時間範圍，用戶端會在此時間範圍內將活動訊號傳送到 Apex Central 伺服器。

     例如，將時段 09 和 13 設定為「閒置」，會建立兩個連續時段的時間範圍。

   - 您可以指定最多三個「預約」時段的連續時間範圍，用戶端會在此時間範圍內將活動訊號傳送到 Apex Central 伺服器。

4. 按一下「儲存」。

設定受管理產品活動訊號間隔

「受管理產品活動訊號間隔」設定可決定用戶端傳送活動訊號給 Apex Central 伺服器的頻率。

使用「通訊逾時設定」畫面可定義受管理產品活動訊號間隔（以分鐘為單位）。

在設定受管理產品活動訊號間隔時，請考量下列事項：

- 「受管理產品活動訊號間隔」設定只會套用到使用 Apex Central 管理主控台向 Apex Central 伺服器註冊的受管理產品。
- 較長的活動訊號間隔會耗用較少頻寬，但在 Apex Central 更新通訊狀態之前發生的網路事件就會比較多。
- 較短的活動訊號間隔會耗用較多頻寬，但能提供您網路狀態更即時的概況。

步驟

1. 移至「管理 > 受管理的伺服器 > 通訊逾時設定」。

   會出現「通訊逾時設定」畫面。

2. 在「受管理產品活動訊號間隔」區段中，設定下列設定：

   - 報告受管理產品狀態，間隔為每：定義用戶端通訊活動訊號間隔

     有效值為 5 到 480 分鐘之間。

   - 在無通訊時間到達以下時間後，將狀態設定為異常：定義用戶端通訊逾時間隔

     有效值為 15 到 1440 分鐘之間。

重要

「在無通訊時間到達以下時間後，將狀態設定為異常」值必須至少是「報告受管理產品狀態，間隔為每」值的 3 倍。

3. 按一下「儲存」。

第 9 章

Security Agent 安裝

本章說明 Security Agent 的安裝需求和方法。

包含下列主題：

- 下載 Security Agent 安裝套件 第 9-2 頁
- Apex One Security Agent 系統需求 第 9-4 頁
- Apex One (Mac) Security Agent 安裝 第 9-25 頁

下載 Security Agent 安裝套件

使用「Security Agent 下載」畫面可以建立及下載 Apex One 或 Apex One (Mac) 的 Security Agent 安裝套件。您可以下載及安裝 Security Agent 安裝套件，也可以取得可傳送給使用者的 URL，讓他們將 Security Agent 安裝套件直接下載到目標端點上。

表 9-1. 安裝前組態設定

Security Agent	組態設定
Apex One	在安裝 Apex One Security Agent 之前： • 變更預設的 Apex One Security Agent 卸載和解除安裝密碼 • 確保端點可以透過通訊埠 80 和 443 進行通訊 • 確保端點可以存取 *.trendmicro.com • 設定 Apex One Security Agent Proxy 伺服器設定（如果需要）
Apex One (Mac)	在安裝 Apex One (Mac) Security Agent 之前： • 確保端點可以透過通訊埠 61617 和 8443 (SaaS) 進行通訊 • 確保端點可以存取 *.trendmicro.com • 設定 Apex One Security Agent Proxy 伺服器設定（如果需要）

如需有關在端點上安裝 Security Agent 之系統需求的詳細資訊，請參閱下列主題：

- Apex One Security Agent 系統需求 第 9-4 頁
- Apex One (Mac) Security Agent 系統需求 第 9-25 頁

步驟

1. 移至「管理 > Security Agent 下載」。
2. 選取作業系統。
   - Windows 64 位元：選取此選項可建立用於 Apex One Security Agent 的 64 位元 MSI 安裝套件

- Windows 32 位元：選取此選項可建立用於 Apex One Security Agent 的 32 位元 MSI 安裝套件
- Mac：選取此選項可建立用於 Apex One (Mac) Security Agent 的 ZIP 安裝套件

3. 對於「Windows 64 位元」或「Windows 32 位元」Apex One Security Agent，請選取「安裝模式」：
   - 完整功能集：安裝包含完整功能的標準 Apex One Security Agent
   - 共存：共存模式 Apex One Security Agent 提供有限的 Apex One 功能子集，但與執行任何端點安全防護軟體的任何受支援 Windows 端點相容。

   秘訣

   選取「共存」模式可允許目標端點使用協力廠商安全防護軟體。

4. 如果您有多部對應的受管理產品伺服器可用於所選安裝套件的類型，請使用「伺服器」下拉式清單選取 Security Agent 向其報告的伺服器。

   注意

   如果您僅有一部受管理產品伺服器，則只會顯示受管理產品伺服器名稱。

5. 按一下下列其中一個部署選項：
   - 下載：下載 Security Agent 安裝套件的複本，您可以從本機安裝，或稍後部署到目標端點
   - 取得下載連結：顯示可傳送給使用者的 URL，讓他們直接在目標端點上安裝 Security Agent

   注意

   對於 Apex One 伺服器，Apex One Security Agent 套件會套用「Security Agent 封裝工具」上次執行時產生的設定。

   如需詳細資訊，請參閱《Apex One 管理手冊》

Apex One Security Agent 系統需求

本節簡述所支援的 Windows 平台上進行全新安裝的 Apex One Security Agent 系統需求。

Windows 端點平台

Windows 7（32/64 位元）Service Pack 1 需求

項目	需求
版本 重要 需要 Service Pack 1。	• Home Basic • Home Premium • Ultimate • Professional • Enterprise • Professional for Embedded Systems • Ultimate for Embedded Systems • Thin PC
處理器	• 至少 1GHz（32 位元）/2GHz（64 位元）Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）

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

Windows 8.1（32/64 位元）需求

項目	需求
版本（不需要有 Service Pack）	• Standard • Pro • Enterprise
處理器	• 至少 1GHz（32 位元）/2GHz（64 位元）Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）

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

Windows 10（32/64 位元）需求

項目	需求
版本（不需要有 Service Pack）	• Home • Pro • 工作站專業版 • 教育版 • Enterprise
更新支援	• Windows 10 November 2021 Update (Windows 10 21H2) 和更早版本

項目	需求
處理器	• 至少 1GHz（32 位元）/2GHz（64 位元）Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）
可用磁碟空間	• 至少 1.5GB • 建議使用 2.0GB 注意 如果您要在 Security Agent 上啟動 Application Control、Endpoint Sensor、Vulnerability Protection 和資料安全防護，趨勢科技建議您將最低磁碟空間增加至 3.0 GB。
其他	• 支援 1024 x 768 解析度（256 色）或以上的顯示器 • 允許透過 Windows 防火牆（如果已啟動）進行印表機/檔案共用 • 啟動預設的本機 admin 注意 不支援 Windows UI。

Windows Server 平台

Windows Server 2008 R2（64 位元）平台

- Windows Server 2008 R2 第 9-8 頁
- Windows Storage Server 2008 R2 第 9-9 頁
- Windows HPC Server 2008 R2 第 9-10 頁

注意

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

表 9-2. Windows Server 2008 R2

項目	需求
版本（Service Pack 1）	• Standard • Enterprise • Datacenter • Web • Server Core
處理器	• 至少 1.4GHz 的 Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）

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

表 9-3. Windows Storage Server 2008 R2

項目	需求
版本（Service Pack 1）	• Basic • Standard • Enterprise • Workgroup
處理器	• 至少 1.4GHz 的 Intel Pentium 或同級處理器（建議使用 2GHz） • AMD™ 64 處理器 • Intel 64 處理器
RAM	• 最低 2 GB（專用於 Apex One） 具有 Endpoint Sensor 的 Apex One： • 最低 2 GB（專用於 Apex One）

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

表 9-4. Windows HPC Server 2008 R2

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

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

Windows MultiPoint Server 2010（64 位元）平台

注意

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

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

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

Windows MultiPoint Server 2011（64 位元）平台

注意

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

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

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

Windows Server 2012（64 位元）平台

- Windows Server 2012 第 9-14 頁
- Windows Server 2012 R2 第 9-15 頁
- Windows Storage Server 2012 第 9-16 頁
- Windows Storage Server 2012 R2 第 9-17 頁
- Windows MultiPoint Server 2012 第 9-18 頁
- Windows Server 2012 容錯移轉叢集 第 9-18 頁
- Windows Server 2012 R2 容錯移轉叢集 第 9-19 頁

注意

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

表 9-5. Windows Server 2012

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

表 9-6. Windows Server 2012 R2

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

表 9-7. Windows Storage Server 2012

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

表 9-8. Windows Storage Server 2012 R2

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

表 9-9. Windows MultiPoint Server 2012

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

表 9-10. Windows Server 2012 容錯移轉叢集

項目	需求
版本（不需要有 Service Pack）	• 無

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

表 9-11. Windows Server 2012 R2 容錯移轉叢集

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

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

Windows Server 2016（64 位元）平台

- Windows Server 2016 第 9-21 頁
- Windows Server 2016 容錯移轉叢集 第 9-22 頁
- Windows Storage Server 2016 第 9-22 頁

注意

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

表 9-12. Windows Server 2016

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

表 9-13. Windows Server 2016 容錯移轉叢集

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

表 9-14. Windows Storage Server 2016

項目	需求
版本（不需要有 Service Pack）	• Standard • Workgroup

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

Windows Server 2019（64 位元）平台

注意

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

表 9-15. Windows Server 2019

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

Apex One (Mac) Security Agent 安裝

本節說明 Apex One (Mac) Security Agent 的安裝需求和方法。

如需詳細資訊，請參閱 Apex One (Mac) 文件。

Apex One (Mac) Security Agent 系統需求

以下是在 Mac 端點上安裝 Security Agent 的需求。

表 9-16. Security Agent 安裝需求

資源	需求
作業系統	• macOS™ Catalina 10.15 • macOS™ Mojave 10.14 • macOS™ High Sierra 10.13 • macOS™ Sierra 10.12 • OS X™ El Capitan 10.11
硬體	• 處理器：Apple® M1、Apple® M2 或 Intel®Core™ 處理器 • RAM：至少 2GB • 可用磁碟空間：至少 512MB
伺服器與用戶端間通訊	• 8443 (SaaS) • 61617
其他	• *.trendmicro.com 的存取權 • 用於 Internet 連線的 Proxy 伺服器設定（如果需要）

第 10 章

產品目錄

本節討論如何檢視所有已向 Apex Central 伺服器註冊的受管理產品，以及「產品目錄」畫面上提供的工作相關資訊。

包含下列主題：

- 產品目錄 第 10-2 頁
- 檢視受管理產品狀態摘要 第 10-4 頁
- 執行產品目錄的進階搜尋 第 10-5 頁
- 執行受管理產品工作 第 10-7 頁
- 設定受管理的產品設定 第 10-8 頁
- 從產品目錄查詢記錄檔 第 10-9 頁
- 目錄管理 第 10-10 頁

產品目錄

「產品目錄」畫面會顯示所有已向 Apex Central 伺服器註冊的受管理產品伺服器的相關資訊。您可以使用這個畫面搜尋特定的受管理產品實體、檢視受管理伺服器狀態摘要、執行受管理產品工作、設定受管理的產品設定，或查詢受管理產品記錄檔。

秘訣

您也可以使用「記錄查詢」」畫面查詢受管理產品記錄檔。

如需詳細資訊，請參閱查詢記錄檔 第 15-2 頁。

「產品目錄」樹狀結構將受管理產品分門別類到下列預設資料夾中：

- <Root>：顯示 Apex Central 伺服器的名稱，並包含下列所有子資料夾
- 本機資料夾：包含「新增實體」資料夾與您所建立的任何自訂資料夾
- 新增實體：包含所有最近向 Apex Central 伺服器註冊的受管理產品
- 搜尋結果：包含所有符合基本或進階搜尋條件的受管理產品

注意

Apex Central 會從特殊字元（!、#、$、%、(、)、*、+、-、逗號、句號、+、?、@、[、]、^、_、{、|、} 和 ~）、數字（0 到 9）或字母字元（a/A 到 z/Z）開始以遞增順序列出所有資料夾（「新增實體」資料夾除外）。

「產品目錄」畫面使用圖示來表示受管理產品以及受管理產品的連線狀態。

如需有關「產品目錄」連線狀態圖示的詳細資訊，請參閱連線狀態圖示 第 10-4 頁。

下表列出「產品目錄」畫面上提供的工作。

工作	說明
檢視狀態摘要	在「產品目錄」中選取受管理產品項目以檢視狀態摘要。 如需詳細資訊，請參閱檢視受管理產品狀態摘要 第 10-4 頁。
尋找受管理產品實體	在「尋找實體」搜尋方塊中，使用部分字串比對搜尋受管理產品實體，然後按一下「搜尋」。符合搜尋條件的受管理產品實體會顯示在「搜尋結果」資料夾中。 如需有關執行進階搜尋的詳細資訊，請參閱執行受管理產品工作 第 10-7 頁。
設定受管理的產品設定	在「產品目錄」樹狀結構中選取受管理產品項目，然後從「設定」下拉式清單中選取選項。 如需詳細資訊，請參閱設定受管理的產品設定 第 10-8 頁。
執行受管理產品工作	在「產品目錄」樹狀結構中選取受管理產品項目，然後從「工作」下拉式清單中選取選項。 如需詳細資訊，請參閱執行受管理產品工作 第 10-7 頁。
查詢受管理產品記錄檔	在「產品目錄」中選取受管理產品項目，然後按一下「記錄檔」。 如需詳細資訊，請參閱從產品目錄查詢記錄檔 第 10-9 頁。
組織產品目錄結構	按一下「目錄管理」，建立新資料夾，或在「產品目錄」樹狀結構中移動或分組受管理產品實體。 如需詳細資訊，請參閱目錄管理 第 10-10 頁。
以單一登入方式登入受管理產品主控台	在「產品目錄」樹狀結構的對應資料夾中選取受管理產品伺服器圖示，然後按一下「設定 > <受管理的產品> 單一登入」。 秘訣 您也可以從「伺服器註冊」畫面，以單一登入方式登入受管理產品主控台。 如需詳細資訊，請參閱伺服器註冊 第 8-2 頁。

連線狀態圖示

「產品目錄」會使用下列圖示來指出 Apex Central 伺服器與已註冊的受管理產品之間的通訊狀態。

圖示	MCP 代理程式狀態	產品服務狀態
	執行中	執行中
	執行中	未執行
	通訊逾時 **注意** 在「通訊逾時設定」畫面上所設定的活動訊號間隔內，Apex Central 伺服器無法建立與受管理產品伺服器上 MCP 代理程式的通訊。	未知
	未執行 **注意** 在經過多次失敗嘗試後，根據「通訊逾時設定」畫面上所設定的條件，Apex Central 伺服器無法建立與受管理產品伺服器上 MCP 代理程式的通訊。	未執行

檢視受管理產品狀態摘要

Apex Central 可讓您使用「產品目錄」畫面檢視受管理產品和資料夾的狀態摘要。

秘訣

您也可以使用「資訊中心」上的「安全威脅偵測結果」Widget，檢視受管理產品狀態摘要。

步驟

1. 移至「目錄 > 產品」。

   會出現「產品目錄」畫面。

2. 在「產品目錄」樹狀結構中選取下列項目，以在工作區中顯示狀態摘要。

項目	說明
受管理的產品	選取此項目可檢視系統資訊和產品使用授權資訊
受管理產品資料夾	選取此項目可檢視防毒、間諜程式/可能的資安威脅程式、內容安全、Web 安全、網路病毒、違規狀態和元件狀態的摘要
受管理產品伺服器	在「產品目錄」樹狀結構中選取受管理產品伺服器，然後按一下「資料夾 > 產品檢視」，可顯示受管理產品伺服器上的所有網域
「產品目錄」樹狀結構中的網域	選取此項目可顯示屬於受管理產品伺服器上此網域的所有用戶端

注意

依預設，Apex Central 會顯示截至查詢日期的前七天資訊。

您可以從「期間」下拉式清單中選取「今天」、「最近 7 天」、「最近 14 天」或「最近 30 天」來變更摘要期間。

執行產品目錄的進階搜尋

Apex Central 可讓您使用部分字串比對，在「產品目錄」中搜尋受管理產品項目名稱、網域及端點。您也可以使用布林運算子，對資料夾物件執行進階搜尋來找出特定物件。

注意

執行搜尋後，任何的符合項目都會顯示在「產品目錄」樹狀結構之「搜尋結果」節點下的新資料夾中。

步驟

1. 移至「目錄 > 產品」。

   會出現「產品目錄」畫面。

2. 在「產品目錄」樹狀結構中選取要搜尋的資料夾。

   重要

   進階搜尋功能只會在所選取的資料夾與所有子資料夾中進行搜尋。您無法在「搜尋結果」資料夾中執行搜尋。

3. 按一下「進階搜尋」。

   會出現「進階搜尋」畫面。

4. 在「符合」下拉式清單中，從下列項目中選取：

   - 所有條件
   - 任何條件

5. 指定過濾條件。

   注意

   - 可用的條件、運算子及值會有所變更，具體取決於向 Apex Central 註冊的產品以及先前的過濾選取項目。
   - Apex Central 支援使用多達 20 個過濾條件來進行搜尋。

6. 如果要新增或移除搜尋條件，請按一下搜尋條件右側的按鈕。

7. 請點選「搜尋」。

符合搜尋條件的受管理產品會顯示在「產品目錄」樹狀結構中的「搜尋結果」資料夾中。

執行受管理產品工作

使用「工作」下拉式功能表，將工作發出到特定的受管理產品或受管理產品群組。

顯示的指令類型會隨選取的受管理產品而變更。部分一般工作包括：

- 部署元件
- 傳送掃瞄指令
- 同步處理用戶端

秘訣

從趨勢科技主動式更新伺服器，將最新的元件下載到 Apex Central 伺服器，然後再將更新部署到特定的受管理產品或受管理產品群組。

如需詳細資訊，請參閱設定手動更新設定 第 11-8 頁。

步驟

1. 移至「目錄 > 產品」。

   會出現「產品目錄」畫面。

2. 從「產品目錄」樹狀結構中選取受管理產品或資料夾。

   注意

   如果您選取了資料夾，Apex Central 會嘗試將選取的指令傳送到所選資料夾內包含的所有適用受管理產品。

3. 從「工作」下拉式功能表中，選取要執行的工作。

4. 如果要將指令傳送到受管理產品，請執行下列動作：
   - 部署指令：請按一下「立即部署」。
   - 掃瞄指令：
     a. 選取掃瞄指令。
     b. 選取受管理的產品。
     c. 按一下「傳送要求」。
5. 按一下「指令詳細資料」來監控工作進度，或按一下「確定」繼續進行其他工作。

設定受管理的產品設定

Apex Central 允許您透過登入受管理產品的 Web 主控台，或藉由在 Apex Central Web 主控台中將組態設定複製到目標電腦，來設定受管理的產品。

注意
如需有關設定受管理產品的其他資訊，請參閱受管理產品的文件。

步驟

1. 移至「目錄 > 產品」。

   會出現「產品目錄」畫面。
2. 從「產品目錄」樹狀結構中選取受管理的產品。
3. 從「設定」下拉式清單中，選取下列其中一項：

   注意
   視選取的受管理產品而定，「設定」下拉式功能表中的選項會有所不同。

- 組態設定複寫：將組態設定從選取的受管理產品複製到目標電腦
- 複製組態設定到整個資料夾：將組態設定複製到所選受管理產品的同一個資料夾中的所有其他受管理產品
- <受管理的產品> 單一登入：讓您使用您的 Apex Central 認證登入受管理的產品 Web 主控台
- 設定 <受管理的產品>：讓您登入受管理產品的 Web 主控台
  - 如果看到提示，請輸入您的使用者名稱和密碼以登入受管理產品的 Web 主控台。
  - 如果看到提示，請按一下「是」以進入受管理產品的 Web 主控台。

從產品目錄查詢記錄檔

Apex Central 可讓您從「產品目錄」樹狀結構中選取受管理產品或資料夾做為資訊來源，藉此從「產品目錄」畫面執行記錄查詢。

注意

從「產品目錄」查詢記錄檔時，Apex Central 會根據您在「產品目錄」畫面上選取的受管理產品伺服器或資料夾，預先選取產品範圍。

如需有關從「記錄查詢」畫面執行記錄查詢的詳細資訊，請參閱查詢記錄檔 第 15-2 頁。

步驟

1. 移至「目錄 > 產品」。

   會出現「產品目錄」畫面。

2. 從「產品目錄」樹狀結構中選取受管理產品或資料夾。

注意

選取的受管理產品或資料夾會決定記錄查詢的產品範圍。

3. 按一下「記錄檔」按鈕。

   會出現「記錄查詢」畫面。

4. 選取記錄類型，然後按一下「確定」。

5. 選取時間範圍，或指定自訂的日期範圍。

6. 如果要指定自訂的過濾條件，請執行下列作業：

   a. 按一下「顯示進階過濾器」。

   b. 選取「所有條件」或「任何條件」做為條件符合規則。

   c. 從「選取條件...」下拉式清單中選取過濾選項。

   d. 選取運算子並指定條件。

注意

Apex Central 支援使用多達 20 個自訂過濾條件來進行各個記錄查詢。

7. 請點選「搜尋」。

目錄管理

「目錄管理」畫面可讓您根據管理需求自訂「產品目錄」結構。若要存取「目錄管理」畫面，請按一下「產品目錄」畫面（目錄 > 產品）上的「目錄管理」按鈕。

根據地理、行政或產品特定用途，將受管理產品分組。下表結合了用於存取目錄中受管理產品或資料夾的不同存取權限，顯示建議的分組類型及各種類型的優缺點。

表 10-1. 產品分組比較

分組類型	優點	缺點
地理或行政	清除結構	相同的產品沒有分組組態設定
產品類型	有分組組態設定和狀態	存取權限可能不相符
結合兩者	分組組態設定和存取權限管理	複雜結構，可能不易於管理

謹慎計劃此結構，因為結構也會影響下列項目：

表 10-2. 結構的考量事項

注意事項	影響
使用者存取	建立使用者帳號時，Apex Central 會提示使用者可以存取的「產品目錄」區段。例如，授與根區段的存取權，會授與整個目錄的存取權。授與特定受管理產品的存取權，僅會授與該特定產品的存取權。
部署計劃	Apex Central 會根據「部署計劃」將更新元件（例如，病毒碼檔案、掃瞄引擎、垃圾郵件防護規則、程式更新）部署到產品。這些計劃會部署到「產品目錄」資料夾，而非個別產品。因此，結構良好的目錄會簡化收件者的指定。

如需詳細資訊，請參閱管理產品目錄 第 10-12 頁。

重要

使用者帳號具有根據「產品目錄」資料夾指派的特定存取權限。

- 變更「產品目錄」結構可能會影響 Apex Central 使用者可以存取受管理產品的方式。
- 您可以選取「在移動受管理產品/資料夾時，目前的使用者存取權限會保持不變」核取方塊，以防止在變更「產品目錄」結構時一併變更使用者存取範圍。

如需詳細資訊，請參閱使用者帳號 第 4-2 頁。

管理產品目錄

使用「目錄管理」畫面可組織您的「產品目錄」結構。

如需詳細資訊，請參閱目錄管理 第 10-10 頁。

重要

- Apex Central 透過使用一種功能鎖定機制，防止多位使用者在不知情的情況下同時進行變更。如果有另一位使用者已在使用「目錄管理」畫面，Apex Central 會通知您。如果您還是要變更「產品目錄」且可能會影響其他使用者的變更，請按一下「中斷」立即存取畫面。
- 變更「產品目錄」結構可能會影響 Apex Central 使用者可以存取受管理產品的方式。使用者帳號具有根據「產品目錄」資料夾指派的特定存取權限。

  如需詳細資訊，請參閱使用者帳號 第 4-2 頁。

步驟

1. 移至「目錄 > 產品」。

   會出現「產品目錄」畫面。

2. 按一下「目錄管理」按鈕。

   會出現「目錄管理」畫面。

3. 如果您要維持所有受管理產品的目前使用者存取權限，請啟動「在移動受管理產品/資料夾時，目前的使用者存取權限會保持不變」核取方塊。

   注意

   如果您關閉此選項，並將受管理產品移至新的位置，則受管理產品會繼承新資料夾位置的權限。

4. 如果要組織「產品目錄」，您可以執行下列工作：
   - 新增資料夾：在「本機資料夾」節點中建立新的自訂資料夾
   - 重新命名：重新命名現有的自訂資料夾

- 刪除：刪除現有的自訂資料夾

  注意

  Apex Central 無法刪除其中包含已註冊受管理產品的自訂資料夾。

- 移動受管理產品或資料夾：將受管理產品或資料夾拖放到新的位置

  重要

  您無法在「根」、「階層式資料夾」或「新增實體」資料夾中重新命名、刪除或新增產品或資料夾。

5. 按一下「返回」套用變更，並返回「產品目錄」畫面。

還原受管理產品

警告!

下列處理行動可能會從「產品目錄」中刪除受管理產品：

- 重新安裝 Apex Central 伺服器並選取「刪除現有的記錄，然後建立新資料庫」
- 使用另一個同名的資料庫取代損毀的 Apex Central 資料庫

使用下列三種方法之一，還原不小心從「產品目錄」中刪除的受管理產品。

步驟

- 在受管理產品伺服器上手動重新啟動 Apex Central MCP 代理程式服務。
- 等候 MCP 代理程式在 8 小時後自動向 Apex Central 伺服器重新註冊。
- 從受管理產品主控台手動將 MCP 代理程式向 Apex Central 伺服器重新註冊。

第 11 章

元件更新

本節討論如何在 Apex Central 中設定元件更新。

包含下列主題：

- 元件更新 第 11-2 頁
- 設定預約更新設定 第 11-4 頁
- 設定手動更新設定 第 11-8 頁
- 設定用於元件/使用授權更新、雲端服務及 Syslog 轉送的 Proxy 伺服器設定 第 11-11 頁

元件更新

Apex Central 伺服器會代管受管理產品用於保護您的網路免於遭受最新安全威脅的元件檔案。

請透過執行手動或預約更新，使這些元件保持在最新狀態。Apex Central 允許您執行下列工作：

- 從更新來源下載最新的元件版本
- 將更新的元件部署到受管理產品

元件清單

您可以在「預約更新」和「手動更新」畫面中檢視 Apex Central 伺服器上可用元件的清單。

下表說明「預約更新」和「手動更新」畫面中顯示的元件資訊。

欄位	說明
類別	顯示元件類別的名稱 按一下 ▸ 可顯示某個類別中的元件清單。
類型	顯示元件類型
目前版本	顯示 Apex Central 成功下載之元件的上個版本
上次下載	顯示 Apex Central 下載「目前版本」元件的時間
關聯的產品	顯示使用元件的受管理產品名稱或受管理產品數目 如果有多個受管理產品使用元件，請將滑鼠游標移到文字上方，即會顯示關聯的受管理產品清單。

更新來源

設定 Apex Central 伺服器從趨勢科技主動式更新伺服器或其他更新來源下載元件。如果 Apex Central 伺服器無法直接連線到趨勢科技主動式更新伺服器，或在網路中代管更新伺服器時，您可以指定其他更新來源。

依預設，Apex Central 會使用更安全的 HTTPS 連線方法，從趨勢科技主動式更新伺服器下載元件。

為了存取其他更新來源，Apex Central 支援遠端 UNC 驗證，這會從更新來源伺服器使用使用者帳號，以將資料夾共用給 Apex Central 來下載更新。

部署計劃

您可以使用部署計劃來指定 Apex Central 伺服器將更新元件部署到受管理產品的範圍和預約時程。

在 Apex Central 伺服器從更新來源下載新元件版本後，您可以設定 Apex Central 立即、於指定時間，或延遲一段時間後，將更新元件部署到受管理產品。

您可以設定 Apex Central 根據不同的部署預約時程，將更新元件部署到選取的受管理產品。

在建立部署預約時程時，請考量下列事項：

- 您只能針對每個部署預約時程選取一個資料夾或受管理產品。不過，您可以針對部署計劃指定多個預約時程。
- Apex Central 會根據下載的完成時間來排定部署計劃延遲，每個延遲彼此各自獨立。

  例如，假設您有三個資料夾要更新，更新間隔為 5 分鐘，則您可以指派第一個資料夾延遲 5 分鐘，然後將剩下的兩個資料夾分別設定為延遲 10 和 15 分鐘。

注意

如果您在部署計劃中未指定部署預約時程，則 Apex Central 會下載更新，但不會將更新元件部署到受管理產品。

新增部署預約時程

您可以設定部署預約時程，以便根據您指定的預約時程，將更新的元件部署到選取的受管理產品。

步驟

1. 存取「預約更新」或「手動更新」畫面。
2. 在「部署計劃」區段中，選取「為受管理產品定義其他部署計劃」。
3. 按一下「+ 新增」。

   會出現「新增預約時程」畫面。
4. 設定部署預約時程。
5. 在「受管理產品/資料夾」樹狀結構中，選取受管理的產品或產品資料夾。
6. 按一下「確定」以儲存設定。

   建立部署計劃後，您可以執行下列工作：

   - 按一下預約時程可編輯部署預約時程設定。
   - 按一下「刪除」可移除選取的部署預約時程。

設定預約更新設定

設定預約元件更新設定，可讓 Apex Central 伺服器在指定的預約時程從更新來源下載選取的元件

您也可以設定 Apex Central 根據部署計劃，將更新的元件部署到受管理產品。

注意

直接從 Control Manager 6.0 Service Pack 3 移轉到 Apex Central 會保留先前在「預約更新」畫面上針對「所有特徵碼檔案/清除範本，但不含 Deep Discovery 惡意程式病毒碼」所設定的「更新來源」、「下載預約」和「部署計劃」組態設定。

警告!

直接從 Control Manager 6.0 Service Pack 3 移轉到 Apex Central 會將「手動更新」和「預約更新」畫面上的「元件」組態設定重設為預設設定。

步驟

1. 移至「管理 > 更新 > 預約更新」。
2. 使用下拉式清單可過濾元件清單。您可以根據下列項目過濾元件清單：
   - 產品：從下拉式清單中選取一或多個受管理產品或所有趨勢科技產品，然後按一下「套用」
   - 類別：從下拉式清單中選取一或多個元件類別，然後按一下「套用」
   - 類型：從下拉式清單中選取一或多個元件類型，然後按一下「套用」
3. 在「元件」區段中，選取元件類別或展開類別來選取要更新的元件。

   如需詳細資訊，請參閱元件清單 第 11-2 頁。

   重要

   如果您選取「啟動智慧元件下載」核取方塊，Apex Central 會根據選取的元件類別自動選取所有元件。您無法選取個別元件進行更新。如果要選取個別元件，請不勾選此核取方塊。

   注意

   如果要將 Apex Central 網路流量降至最低，請關閉下載沒有對應受管理產品或服務的元件。

4. （選用）選取「啟動智慧元件下載」，可允許 Apex Central 根據選取的元件類別，從更新來源自動偵測並下載新元件。

注意

如果未啟動智慧元件下載功能，則 Apex Central 在預約或手動更新期間，只會下載元件清單中所選現有元件的更新。

5. 在「更新來源」區段中，選取下列其中一個選項，然後設定必要的設定：

   - 趨勢科技主動式更新伺服器：選取此選項可從官方趨勢科技主動式更新伺服器下載元件更新。
   - 其他更新來源：在文字欄位中輸入更新來源的 URL。按一下 + 圖示，最多可指定五個更新來源。

     如果需要驗證伺服器，請按一下「指定驗證認證」，然後輸入使用者名稱和密碼資訊。

     如需詳細資訊，請參閱更新來源 第 11-3 頁。

注意

如果 Apex Central 伺服器使用 Proxy 伺服器連線到更新來源，請在「Proxy 伺服器設定」畫面上設定 Proxy 伺服器設定。

如需詳細資訊，請參閱設定用於元件/使用授權更新、雲端服務及 Syslog 轉送的 Proxy 伺服器設定 第 11-11 頁。

6. 在「下載預約」區段中，選取「啟動預約下載」，然後指定元件下載預約。
7. 在「部署計劃」區段中，選取部署選項，然後設定必要的設定。

選項	說明
部署到所有選取的受管理產品	選取此選項，可根據下列其中一個預約，將更新的元件部署到選取的受管理產品： • 立即：Apex Central 在 Apex Central 完成下載新的元件版本後，會立即將更新的元件部署到受管理產品。 • 開始於：Apex Central 會於指定的開始時間，將更新的元件部署到受管理產品。 • 延遲：Apex Central 在等待指定的時間過後，會將更新的元件部署到受管理產品。
為受管理產品定義其他部署計劃	選取此選項，可設定指定受管理產品的部署預約時程。 執行下列其中一項作業： • 按一下「+ 新增」，可新增部署預約時程。 如需詳細資訊，請參閱新增部署預約時程 第 11-4 頁。 • 按一下預約時程可編輯部署預約時程設定。 • 按一下「刪除」可移除選取的部署預約時程。 注意 如果您沒有指定部署預約時程，Apex Central 會下載元件更新，但不會將更新的元件部署到受管理產品。
不要部署	如果您不想讓 Apex Central 自動將更新的元件部署到受管理產品，則選取此選項。 您可以手動將更新的元件部署到「產品」畫面上的受管理產品。 如需詳細資訊，請參閱執行受管理產品工作 第 10-7 頁。

8. 按一下「儲存」。

設定手動更新設定

您可以在 Apex Central 伺服器上啟動手動更新，以從更新來源下載選取的元件。

您也可以設定 Apex Central 根據部署計劃，將更新的元件部署到受管理產品。

警告!

直接從 Control Manager 6.0 Service Pack 3 移轉到 Apex Central 會將「手動更新」和「預約更新」畫面上的「元件」組態設定重設為預設設定。

步驟

1. 移至「管理 > 更新 > 手動更新」。
2. 使用下拉式清單可過濾元件清單。您可以根據下列項目過濾元件清單：
   - 產品：從下拉式清單中選取一或多個受管理產品或所有趨勢科技產品，然後按一下「套用」
   - 類別：從下拉式清單中選取一或多個元件類別，然後按一下「套用」
   - 類型：從下拉式清單中選取一或多個元件類型，然後按一下「套用」
3. 在「元件」區段中，選取元件類別或展開類別來選取要更新的元件。

   如需詳細資訊，請參閱元件清單 第 11-2 頁。

   重要

   如果您選取「啟動智慧元件下載」核取方塊，Apex Central 會根據選取的元件類別自動選取所有元件。您無法選取個別元件進行更新。如果要選取個別元件，請不勾選此核取方塊。

   注意

   如果要將 Apex Central 網路流量降至最低，請關閉下載沒有對應受管理產品或服務的元件。

4. （選用）選取「啟動智慧元件下載」，可允許 Apex Central 根據選取的元件類別，從更新來源自動偵測並下載新元件。

   注意

   如果未啟動智慧元件下載功能，則 Apex Central 在預約或手動更新期間，只會下載元件清單中所選現有元件的更新。

5. 在「更新來源」區段中，選取下列其中一個選項，然後設定必要的設定：

   - 趨勢科技主動式更新伺服器：選取此選項可從官方趨勢科技主動式更新伺服器下載元件更新。
   - 其他更新來源：在文字欄位中輸入更新來源的 URL。按一下 + 圖示，最多可指定五個更新來源。

     如果需要驗證伺服器，請按一下「指定驗證認證」，然後輸入使用者名稱和密碼資訊。

     如需詳細資訊，請參閱更新來源 第 11-3 頁。

   注意

   如果 Apex Central 伺服器使用 Proxy 伺服器連線到更新來源，請在「Proxy 伺服器設定」畫面上設定 Proxy 伺服器設定。

   如需詳細資訊，請參閱設定用於元件/使用授權更新、雲端服務及 Syslog 轉送的 Proxy 伺服器設定 第 11-11 頁。

6. 在「部署計劃」區段中，選取部署選項，然後設定必要的設定。

選項	說明
部署到所有選取的受管理產品	選取此選項，可根據下列其中一個預約，將更新的元件部署到選取的受管理產品： • 立即：Apex Central 在 Apex Central 完成下載新的元件版本後，會立即將更新的元件部署到受管理產品。 • 開始於：Apex Central 會於指定的開始時間，將更新的元件部署到受管理產品。 • 延遲：Apex Central 在等待指定的時間過後，會將更新的元件部署到受管理產品。
為受管理產品定義其他部署計劃	選取此選項，可設定指定受管理產品的部署預約時程。 執行下列其中一項作業： • 按一下「+ 新增」，可新增部署預約時程。 如需詳細資訊，請參閱新增部署預約時程 第 11-4 頁。 • 按一下預約時程可編輯部署預約時程設定。 • 按一下「刪除」可移除選取的部署預約時程。 注意 如果您沒有指定部署預約時程，Apex Central 會下載元件更新，但不會將更新的元件部署到受管理產品。
不要部署	如果您不想讓 Apex Central 自動將更新的元件部署到受管理產品，則選取此選項。 您可以手動將更新的元件部署到「產品」畫面上的受管理產品。 如需詳細資訊，請參閱執行受管理產品工作 第 10-7 頁。

7. 按一下「立即下載」。

   在「手動更新」畫面的頂端會顯示下載進度。

8. 如果要取消進行中的下載：

   • 按一下進度列中的「停止目前的更新」按鈕。

- 按一下「立即下載」按鈕，取消進行中的下載，並開始新的下載。

設定用於元件/使用授權更新、雲端服務及 Syslog 轉送的 Proxy 伺服器設定

Apex Central 允許您將 Proxy 伺服器用於元件/使用授權更新、雲端服務及 Syslog 轉送。

注意

如果您為伺服器選取了 SOCKS 通訊協定，則也可以將同一個 Proxy 伺服器用於 Syslog 轉送。Syslog 轉送不支援 HTTP 通訊協定 Proxy 伺服器。

如需詳細資訊，請參閱設定 Syslog 轉送 第 15-13 頁。

步驟

1. 移至「管理 > 設定 > Proxy 設定」。

   會出現「Proxy 設定」畫面。

2. 選取「將 Proxy 伺服器用於元件/使用授權更新、雲端服務、syslog 轉送，以及可疑物件中樞 Apex Central 伺服器連線」。

3. 選取通訊協定：

   注意

   Syslog 轉送不支援 HTTP Proxy 伺服器。如果要將 Proxy 伺服器用於 Syslog 轉送，請選取 SOCKS 通訊協定。

   - HTTP
   - SOCKS 4
   - SOCKS 5

4. 在「伺服器名稱或 IP 位址」欄位中輸入伺服器的主機名稱或 IP 位址。
5. 在「通訊埠」欄位中輸入通訊埠號碼。
6. 如果您的伺服器需要驗證，請輸入使用者名稱和密碼。
7. 按一下「儲存」。

第 12 章

指令追蹤和產品通訊

本節討論如何追蹤從 Apex Central 伺服器發出的指令。

包含下列主題：

- 指令追蹤 第 12-2 頁
- 查詢及檢視指令 第 12-3 頁
- 設定通訊逾時設定 第 12-4 頁

指令追蹤

「指令追蹤」畫面可提供傳送自 Apex Central 伺服器之所有先前發出指令的清單。您可以使用此畫面來監控您從 Apex Central 主控台向受管理產品發出之指令的狀態。例如，在發出「立即開始掃瞄」工作後，這個工作可能需要數分鐘才能完成，在此期間，您可以繼續執行其他工作，然後參考「指令追蹤」畫面來查詢及檢視已發出指令的狀態。

如需有關查詢及檢視指令的詳細資訊，請參閱查詢及檢視指令 第 12-3 頁。

下表說明「指令追蹤」畫面上顯示的指令資訊。

欄名稱	說明
已核發	Apex Central 伺服器向受管理產品發出指令的日期和時間
指令	Apex Central 伺服器所發出指令的類型
使用者	觸發指令的使用者名稱
成功	完成指令的受管理產品數目 按一下「成功」欄中的計數，可檢視有關指令的更多詳細資訊。 如需詳細資訊，請參閱指令詳細資料 第 12-3 頁。
未成功	無法執行指令的受管理產品數目 按一下「未成功」欄中的計數，可檢視有關指令的更多詳細資訊。 如需詳細資訊，請參閱指令詳細資料 第 12-3 頁。
進行中	目前正在執行指令的受管理產品數目 按一下「進行中」欄中的計數，可檢視有關指令的更多詳細資訊。 如需詳細資訊，請參閱指令詳細資料 第 12-3 頁。
全部	Apex Central 向其發出指令的受管理產品總數 按一下「全部」欄中的計數，可檢視有關指令的更多詳細資訊。 如需詳細資訊，請參閱指令詳細資料 第 12-3 頁。

查詢及檢視指令

使用「指令追蹤」畫面追蹤及檢視之前發出的指令。

步驟

1. 移至「管理 > 指令追蹤」。

   會出現「追蹤指令」畫面。

2. 如果要過濾指令清單，請指定下列項目：

   - 發出：指定受管理產品傳送指令的時間
   - 指令：選取要監控的指令
   - 使用者：提供用來傳送此指令的帳號名稱。

     秘訣

     將此欄位保留空白，將會查詢所有使用者發出的查詢指令。

   - 狀態：選取一或多個指令狀態，然後按一下「套用」。

3. 按一下「成功」、「未成功」、「進行中」或「全部」欄中的計數，以檢視詳細的指令資訊。

   會出現「指令詳細資料」畫面。

   如需詳細資訊，請參閱指令詳細資料 第 12-3 頁。

指令詳細資料

「指令詳細資料」畫面會顯示已發出之指令的下列相關資訊。

欄名稱	說明
上次回報	受管理產品上次傳送回應給 Apex Central 伺服器的日期和時間

欄名稱	說明
伺服器/實體	受管理產品伺服器的主機名稱
狀態	已發出指令的狀態
說明	指令狀態的其他詳細資料

注意

「指令詳細資料」畫面會每隔 30 秒重新整理一次。

設定通訊逾時設定

「受管理產品活動訊號間隔」設定可決定用戶端傳送活動訊號給 Apex Central 伺服器的頻率。

- 「受管理產品活動訊號間隔」設定只會套用到使用 Apex Central 管理主控台向 Apex Central 伺服器註冊的受管理產品。
- 較長的活動訊號間隔會耗用較少頻寬，但在 Apex Central 更新通訊狀態之前發生的網路事件就會比較多。
- 較短的活動訊號間隔會耗用較多頻寬，但能提供您網路狀態更即時的概況。

「指令逾時設定」可決定 Apex Central 嘗試將指令傳送到受管理的伺服器的時間。

步驟

1. 移至「管理 > 受管理的伺服器 > 通訊逾時設定」。

   會出現「通訊逾時設定」畫面。

2. 在「受管理產品活動訊號間隔」區段中，設定下列設定：

   - 報告受管理產品狀態，間隔為每：定義用戶端通訊活動訊號間隔

     有效值為 5 到 480 分鐘之間。

- 在無通訊時間到達以下時間後，將狀態設定為異常：定義用戶端通訊逾時間隔

  有效值為 15 到 1440 分鐘之間。

重要

「在無通訊時間到達以下時間後，將狀態設定為異常」值必須至少是「報告受管理產品狀態，間隔為每」值的 3 倍。

3. 在「指令逾時設定」區段中，選取下列其中一項：
   - 24 小時
   - 48 小時
   - 72 小時
4. 按一下「儲存」。

部分 IV

策略

第 13 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。

重要

每個受管理的產品皆提供不同的策略設定，您可對其進行設定並部署到策略目標。您可以在《*Apex Central Widget* 和策略管理手冊》中找到支援的受管理產品的完整清單及每個產品的策略設定。

您可以使用下列連結來下載手冊的 PDF 版本：

https://docs.trendmicro.com/en-us/enterprise/apex-central.aspx

您還可以使用下列連結來線上檢視手冊：

https://docs.trendmicro.com/en-us/enterprise/apex-central-widget-and-policy-management-guide/introduction.aspx

---

包含下列主題：

- 策略管理 第 13-2 頁
- 策略狀態 第 13-22 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

重要

每個受管理的產品皆提供不同的策略設定，您可對其進行設定並部署到策略目標。您可以在《Apex Central Widget 和策略管理手冊》中找到支援的受管理產品的完整清單及每個產品的策略設定。

您可以使用下列連結來下載手冊的 PDF 版本，或在線上檢視手冊：

https://docs.trendmicro.com/en-us/enterprise/apex-central.aspx

步驟

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 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 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。

   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。

     如需詳細資訊，請參閱指定策略目標 第 13-8 頁。

   - 依條件過濾：使用此選項可根據過濾條件自動配置端點。

     如需詳細資訊，請參閱依條件過濾 第 13-4 頁。

   - 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。

   如需有關策略清單的詳細資訊，請參閱瞭解策略清單 第 13-18 頁。

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 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 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 Security Agent 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 Security Agent 設定清單，請參閱使用父策略設定 第 13-9 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 13-12 頁。

7. 按一下「部署」或「儲存」。

如果按一下「部署」，Apex Central 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 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「等待中」，這可能是目標有問題。請檢查 Apex Central 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 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 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 強制執行策略設定時都會覆寫這些變更。

- Apex Central 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 策略的 Apex One Security Agent 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 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 (Mac)
  - Apex One 資料外洩防護

  - Apex One Security Agent
  - 企業版行動安全防護
  - Trend Micro Endpoint Application Control
- 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 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 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 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 13-6 頁。

步驟

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 顯示名稱定義關鍵字。 **注意** 對於單一關鍵字搜尋，Apex Central 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 僅會針對每個提供的關鍵字，提供符合完整字串的項目。

條件	說明
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 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 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 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 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 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 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等待中，直到端點上線為止。
- 如果端點的 Apex One 網域有所變更，Apex Central 將在 10 分鐘後部署更新的策略。

當上述處理行動發生時，Apex Central 會根據下列條件來配置端點：

表 13-1. 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

步驟

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 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 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。

  注意

  如果要設定 Active Directory，請參閱 Active Directory 整合 第 6-2 頁。

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 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 伺服器主控台手動變更設定。不過，當 Apex Central 將策略部署到 Apex One 伺服器時，設定會遭到覆寫。

    例如，Apex Central 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	●		● 注意 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」。

步驟

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 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 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」。

步驟

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 13-9 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 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 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 會將策略部署到目標。

重要

每個受管理的產品皆提供不同的策略設定，您可對其進行設定並部署到策略目標。您可以在《*Apex Central Widget* 和策略管理手冊》中找到支援的受管理產品的完整清單及每個產品的策略設定。

您可以使用下列連結來下載手冊的 PDF 版本，或在線上檢視手冊：

https://docs.trendmicro.com/en-us/enterprise/apex-central.aspx

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 13-9 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。

步驟

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 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 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「等待中」，這可能是目標有問題。請檢查 Apex Central 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 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，或匯入同一版本的另一部 Apex Central 伺服器。

注意

- Apex Central 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 無法匯入該策略。如果現有策略並非子策略，則 Apex Central 會在匯入後覆寫該策略。
- 如需詳細資訊，請參閱下列主題：
  - 建立新策略 第 13-2 頁
  - 繼承策略設定 第 13-12 頁

步驟

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. 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。
   - 如果匯出了單一策略，則所產生的檔案會使用副檔名 `*.cmpolicy`。
   - 如果匯出了多個策略，則所產生的檔案會是一個壓縮 (`*.zip`) 檔案，其中包含個別的 `.cmpolicy` 檔案。
4. 如果要匯入，請按一下「匯入設定」，然後找出並載入策略檔案。
   - 您可以匯入整個 `*.zip` 檔案或逐一匯入各 `*.cmpolicy` 檔案。
   - 如果某個策略已存在於策略清單中，則會出現確認提示，詢問您是否要覆寫現有策略。

     按一下「確定」以繼續。

   畫面會重新整理，並在清單的最前面顯示匯入的策略。

如需有關重新排序策略清單的詳細資訊，請參閱重新排序策略清單 第 13-21 頁。

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 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 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。

步驟

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 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。

步驟

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 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 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 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 13-2. 策略清單

欄	說明
優先順序	顯示策略的優先順序 • Apex Central 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 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 會將草稿策略放在清單的最下面。
策略	顯示策略的名稱
策略版本	僅當選取的產品為「Apex One Security Agent」時，才會顯示此欄。 顯示部署的最新策略版本 注意 有些目標可能未部署最新策略版本。如果要檢視特定目標上部署的目前版本，請按一下「已部署」欄中的數字。
策略	僅當選取的產品為「Apex One Security Agent」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 Security Agent」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 13-17 頁。
上次編輯者	顯示上次編輯策略的使用者
上次編輯	僅當選取的產品為「Apex One Security Agent」時，才會顯示此欄。 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。
等待中	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「等待中」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 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。

步驟

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 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 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 13-3. 策略狀態

策略狀態	說明	建議
等待中	Apex Central 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 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 已成功部署策略。	無

策略狀態	說明	建議
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。 • 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。
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。
未啟動的使用授權	受管理產品尚未啟動策略設定中所指定之部分服務的使用授權。	請從 Apex Central 主控台的「使用授權管理」畫面啟動相關服務的使用授權
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 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 伺服器名稱] 管理	另一個 Apex Central 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。

策略狀態	說明	建議
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 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。
無法連線到產品。	Apex Central 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。

第 14 章

策略資源

本節包含有關整合式產品/服務適用之策略資源的資訊。

重要

每個受管理的產品皆提供不同的策略設定，您可對其進行設定並部署到策略目標。您可以在《*Apex Central Widget* 和策略管理手冊》中找到支援的受管理產品的完整清單及每個產品的策略設定。

您可以使用下列連結來下載手冊的 PDF 版本，或在線上檢視手冊：

https://docs.trendmicro.com/en-us/enterprise/apex-central.aspx

包含下列主題：

- Application Control 條件 第 14-2 頁
- 資料外洩防護 第 14-14 頁
- 入侵防護規則 第 14-31 頁
- 周邊設備存取控管允許的裝置 第 14-35 頁

Application Control 條件

設定 Application Control 條件，以便您可以接著指派給 Security Agent 策略規則。您可以建立「允許」和「封鎖」條件，來限制使用者可在受保護的端點上執行或安裝的應用程式。您也可以建立評估條件來監控端點上執行的應用程式，然後根據使用結果縮小條件範圍。

重要

您必須先設定 Application Control 條件，然後再將 Application Control 策略部署到 Security Agent。

每個受管理的產品皆提供不同的策略設定，您可對其進行設定並部署到策略目標。您可以在《*Apex Central Widget* 和策略管理手冊》中找到支援的受管理產品的完整清單及每個產品的策略設定。

您可以使用下列連結來下載手冊的 PDF 版本，或在線上檢視手冊：

https://docs.trendmicro.com/en-us/enterprise/apex-central.aspx

下表列出「Application Control 條件」畫面上提供的工作。

工作	說明
新增條件	按一下「新增條件」下拉式按鈕，然後選取下列選項： • 允許：按一下以定義「允許」或「鎖定」條件 如需詳細資訊，請參閱定義允許的應用程式條件 第 14-4 頁。 • 封鎖：按一下以定義「封鎖」或「評估」條件 如需詳細資訊，請參閱定義封鎖的應用程式條件 第 14-6 頁。 • 複製：選取現有的條件，然後按一下「複製」，以根據現有的設定定義新條件 • 匯入：按一下以選取從相容的 Application Control 來源匯出的 ZIP 套件 **注意** 如果匯入的套件包含的條件名稱符合已存在的條件，則您可以選擇「覆寫」現有條件或「略過」匯入名稱重複的條件。
匯出條件	選取現有條件左側的核取方塊，然後按一下「匯出」，以將選取的條件儲存為 ZIP 套件 (<時間戳記>_iACRuleExport.zip)
刪除條件	選取現有條件左側的核取方塊，然後按一下「刪除」，從清單移除選取的條件。 **警告!** 如果您選取現有 Apex One Security Agent 策略所使用的條件，您必須確認是否要從所有受影響的 Security Agent 策略中刪除並移除該條件。您無法復原此動作。
修改條件	按一下「條件名稱」以修改條件設定 **注意** 下次當 Security Agent 連線到伺服器時，受影響的端點才會接收已修改的條件設定。

工作	說明
檢視策略關聯	按一下「目標策略」欄中的值，以顯示實施該條件之所有 Apex One Security Agent 策略的清單。 秘訣 按一下策略名稱可開啟新的瀏覽器標籤，您可以在此檢視或修改策略設定。

定義允許的應用程式條件

Application Control 讓您能夠定義條件來特別允許特定應用程式執行。您可以定義允許條件，以確保 Application Control 絕不會封鎖特定應用程式，您也可以建立允許在端點上執行的應用程式完整清單，然後將「鎖定」策略部署到端點。處於「鎖定」模式時，對於允許條件中未包含的任何應用程式，使用者都無法執行、存取或安裝。

如需有關「鎖定」策略的詳細資訊，請參閱《Application Control 策略設定》。

步驟

1. 移至「策略 > 策略資源 > Application Control 條件」。

   會出現「Application Control 條件」畫面。

2. 按一下「新增條件」，然後選取「允許」。

   會出現「允許條件設定」畫面。

3. 輸入條件的唯一「名稱」。

4. 為應用程式選取「信任權限」的層級。

權限	說明	使用範例
應用程式無法執行外部處理程序	應用程式無法存取任何外部處理程序或啟動任何其他應用程式	可在您要允許獨立應用程式在端點上執行，但要防止存取其他處理程序時使用 例如，此設定會允許 Microsoft Word 執行，但會防止嵌入式 OLE 物件執行。
應用程式可以執行其他處理程序	應用程式可以啟動外部處理程序以及使用者無法直接存取的應用程式	可在您要允許應用程式在端點上執行，同時仍允許存取所需的子處理程序或附加元件時使用。 例如，此設定會允許 Internet Explorer 執行，也允許 Internet Explorer 執行任何已安裝的嵌入程式。
可繼承的執行權限 (不建議)	應用程式可以安裝並啟動外部處理程序和應用程式，子應用程式也可以安裝並啟動外部處理程序和應用程式	可在您要允許安裝套件在端點上執行執時使用 「可繼承的執行權限 (不建議)」會允許安裝套件執行所有安裝工作，接著也會允許所安裝的應用程式執行所有必要的處理程序。

5. 選取用來識別應用程式的「比對方法」，然後進行必要的設定。

方法	說明
應用程式信譽評等清單	可讓您將此條件套用至趨勢科技已測試過且已指派安全評分的應用程式 如需詳細資訊，請參閱應用程式信譽評等清單 第 14-8 頁。
檔案路徑	可讓您將此條件套用至安裝在指定位置的任何應用程式 如需詳細資訊，請參閱檔案路徑 第 14-9 頁。
憑證	可讓您根據憑證有效性和憑證屬性，將此條件套用至應用程式 如需詳細資訊，請參閱憑證 第 14-12 頁。

方法	說明
雜湊值	可讓您根據 SHA-1 或 SHA-256 雜湊值，將此條件套用至應用程式 如需詳細資訊，請參閱雜湊值 第 14-13 頁。
灰色地帶軟體清單	可讓您在此條件中包含趨勢科技已測試過且發現可能有害的應用程式 「灰色地帶軟體清單」是「應用程式信譽評等清單」的子集，其包含在未正確使用下可能是惡意的應用程式。趨勢科技建議您封鎖或監控「灰色地帶軟體清單」中的應用程式，以確保您的網路保持安全狀態。

6. 按一下「儲存」。

定義封鎖的應用程式條件

Application Control 讓您能夠定義條件來特別封鎖特定應用程式，使其無法執行。您可以定義封鎖條件，以確保 Application Control 始終封鎖特定應用程式，您也可以建立「評估」條件來監控使用者所存取的應用程式。

步驟

1. 移至「策略 > 策略資源 > Application Control 條件」。

   會出現「Application Control 條件」畫面。

2. 按一下「新增條件」，然後選取「封鎖」。

   會出現「封鎖條件設定」畫面。

3. 輸入條件的唯一「名稱」。

4. 如果要建立監控規則，請選取「啟動評估模式」。

   注意

   Application Control 會記錄與評估條件相符的所有應用程式，但不會採取任何進一步的處理行動。Application Control 可讓應用程式正常執行。

5. 選取用來識別應用程式的「比對方法」，然後進行必要的設定。

方法	說明
應用程式信譽評等清單	可讓您將此條件套用至趨勢科技已測試過且已指派安全評分的應用程式 如需詳細資訊，請參閱應用程式信譽評等清單 第 14-8 頁。
檔案路徑	可讓您將此條件套用至安裝在指定位置的任何應用程式 如需詳細資訊，請參閱檔案路徑 第 14-9 頁。
憑證	可讓您根據憑證有效性和憑證屬性，將此條件套用至應用程式 如需詳細資訊，請參閱憑證 第 14-12 頁。
雜湊值	可讓您根據 SHA-1 或 SHA-256 雜湊值，將此條件套用至應用程式 如需詳細資訊，請參閱雜湊值 第 14-13 頁。
灰色地帶軟體清單	可讓您在此條件中包含趨勢科技已測試過且發現可能有害的應用程式 「灰色地帶軟體清單」是「應用程式信譽評等清單」的子集，其包含在未正確使用下可能是惡意的應用程式。趨勢科技建議您封鎖或監控「灰色地帶軟體清單」中的應用程式，以確保您的網路保持安全狀態。

6. 按一下「儲存」。

應用程式比對方法

Application Control 提供多種方法，用於識別要包含在允許和封鎖條件中的應用程式。

注意

Application Control 也提供灰色地帶軟體清單，您無法修改此清單。

「灰色地帶軟體清單」是「應用程式信譽評等清單」的子集，其包含在未正確使用下可能是惡意的應用程式。趨勢科技建議您封鎖或監控「灰色地帶軟體清單」中的應用程式，以確保您的網路保持安全狀態。

應用程式信譽評等清單

應用程式信譽評等清單是經過趨勢科技測試之應用程式的完整清單。這份清單包含桌上型電腦、伺服器和行動裝置的最熱門作業系統檔案、二進位檔案及應用程式。趨勢科技會定期更新此清單。

重要

請確保您已開啟「認證安全防護軟體病毒碼」的定期更新，以使用最新的應用程式資訊來保持最新狀態。

您可以輸入「供應商」或「應用程式」的名稱來搜尋應用程式。使用所提供的資料來選取應用程式。

資料	說明
應用程式	應用程式的名稱 **秘訣** 若要檢視每個應用程式版本的詳細資訊，請展開「應用程式信譽評等清單」。
AIR 評分	依據應用程式熱門程度和信譽評等的綜合性安全評分
全域使用量	應用程式的全球普遍程度 **秘訣** 按一下普遍程度可檢視應用程式使用率的區域性明細。

檔案路徑

您可以根據絕對路徑、儲存裝置類型和 Perl Compatible Regular Expressions (PCRE)，來設定 Application Control 明確以特定目錄位置做為目標。

選取是否按特定路徑或儲存裝置類型進行比對，並指定比對字串類型（「字串」或「正規運算式 (PCRE)」）。輸入套用至條件的檔案路徑。

注意

- 在指定「字串」類型比對時，Application Control 支援使用星號 (*) 萬用字元。星號字元可代表所指定字串位置的子目錄中的一或多個字元。
- Application Control 不支援使用環境變數來指定字串或正規運算式 (PCRE) 類型相符項目的檔案路徑。
- 您不能使用萬用字元來表示所選儲存位置的整個內容。
- 您可以指定最多 100 個檔案路徑。

表 14-1. 支援的儲存位置

儲存位置	環境變數	說明
特定路徑	無	僅套用至所指定精確路徑中的應用程式 注意 使用此位置類型時，Application Control 不會檢查裝置類型。
任何內建儲存	$FixedDrives	僅套用至位於指定路徑中並儲存在內部儲存裝置（內部硬碟）上的應用程式
任何本機儲存	$LocalDrives	僅套用至位於指定路徑中並儲存在非卸除式本機儲存裝置（內部或外部硬碟）上的應用程式
任何卸除式儲存	$RemovableDrives	僅套用至位於指定路徑中並儲存在卸除式儲存裝置（USB 儲存裝置、CD/DVD）上的應用程式
網路路徑	$RemoteDrives	僅套用至位於指定路徑中並儲存在共用網路資源上的應用程式

儲存位置	環境變數	說明
Program Files 資料夾	$ProgramFiles	僅套用至位於指定路徑中並儲存在 Program Files 資料夾（預設資料夾為 `C:\Program Files` 和 `C:\Program Files (x86)`）中的應用程式
系統磁碟區	$SystemDrive	僅套用至位於指定路徑中並儲存在預設 Windows 系統磁碟機中的應用程式

檔案路徑範例的使用

目標	允許規則	封鎖規則	結果
監控所有使用者的 Downloads 資料夾	-	1. 啟動評估模式 2. 任何本機儲存 3. 字串 4. `C:\Users\*\Downloads\*`	記錄對所有使用者的 Downloads 資料夾中應用程式的存取嘗試。 監控： • `C:\Users\john_doe\Downloads\start.exe` • `C:\Users\Administrator\Downloads\start.exe`

目標	允許規則	封鎖規則	結果
封鎖位於 `Program Files` 目錄之 `MyApps` 子資料夾內的全部資料夾中的所有應用程式	-	1. Program Files 資料夾 2. 字串 3. `\MyApps*`	封鎖： • `C:\Program Files(x86)\MyApps\start.exe` • `C:\Program Files\MyApps\start.exe` • `C:\Program Files(x86)\MyApps\bin\start.exe` 允許： • `C:\Program Files(x86)\start.exe`
允許位於 `Program Files` 目錄之 `MyApps` 子資料夾內的全部資料夾中的所有應用程式，但封鎖所有其他其應用程式/資料夾	1. Program Files 資料夾 2. 字串 3. `\MyApps*`	1. 任何本機儲存 2. 字串 3. `C:\Program Files\*` AND 1. 任何本機儲存 2. 字串 3. `C:\Program Files (x86)\*`	封鎖： • `C:\Program Files(x86)\start.exe` 允許： • `C:\Program Files(x86)\MyApps\start.exe` • `C:\Program Files\MyApps\start.exe` • `C:\Program Files(x86)\MyApps\bin\start.exe`

目標	允許規則	封鎖規則	結果
僅封鎖位於 `Program Files` 目錄之 `MyApps` 子資料夾內的應用程式，但允許所有其他其應用程式/資料夾	1. 允許 `MyApps` 目錄的子資料夾 a. Program Files 資料夾 b. 字串 c. `\MyApps\*\*`	1. Program Files 資料夾 2. 字串 3. `\MyApps\*`	封鎖： • `C:\Program Files(x86)\MyApps\start.exe` • `C:\Program Files\MyApps\start.exe` 允許： • `C:\Program Files(x86)\start.exe` • `C:\Program Files(x86)\MyApps\bin\start.exe`
封鎖任何資料夾的特定應用程式檔案名稱	-	1. 特定路徑 2. 正規運算式 (PCRE) 3. `.*\\(?i)test(?-i)\..*`	封鎖： • `C:\MyApps\test.exe` • `C:\Users\guet\AppData\Local\Temp\test.exe` • `C:\Program Files(x86)\MyApps\test.exe`

憑證

您可以將 Application Control 設定為依據憑證的「信任」層級明確鎖定包含特定憑證屬性的應用程式。

選取憑證的「信任」層級類型，然後指定所需的憑證「核發者」或「主旨」資訊。

注意

在指定憑證屬性時，Application Control 支援使用星號 (*) 萬用字元，但必須將萬用字元與其他字元合併使用，以限制指定範圍。例如，在任何欄位中，都不能只使用萬用字元。

下表說明不同的「信任」類型。

類型	說明
信任 (有效)	您必須在信任的憑證清單中已包含憑證，且憑證必須尚未過期
信任 (已到期)	您必須已在信任的憑證清單中新增憑證，但憑證已過期
不信任	憑證未知或您尚未將憑證新增至信任的憑證清單

注意

用於「允許」和「封鎖」條件的「信任」層級組合各有不同。

雜湊值

您可以將 Application Control 設定為使用 SHA-1 或 SHA-256 雜湊值格式來比對應用程式。您可以選擇手動指定雜湊值，也可以匯入所產生值的清單。

選取您的「輸入方法」，然後遵循畫面上的指示操作。

輸入方法	說明
手動	允許您手動指定最多 100 個雜湊值（和說明）

輸入方法	說明
匯入	允許您匯入 ZIP 套件，其中包含格式正確的雜湊值清單（採用 CSV 格式） 您可以選擇使用「雜湊產生器工具」，或使用「CSV 範例格式」手動建立 CSV 檔案。 **警告!** 您只能對每一組條件匯入一個檔案。當您嘗試匯入新的雜湊值清單到條件時，Application Control 會完全覆寫現有的值。 • 雜湊產生器工具：在您已安裝所有必要應用程式的目標端點上下載並執行此工具。此工具會自動建立有效的 ZIP 套件，其中包含在端點上發現的所有應用程式的雜湊值。 • CSV 範例格式：下載範例檔案，然後遵循指示正確填入雜湊值清單。完成清單後，請以 ZIP 格式壓縮檔案，然再匯入到一組條件中。 **重要** 雜湊值清單不能同時包含 SHA-1 和 SHA-256 格式。您必須建立不同的雜湊值檔案，讓每一種雜湊值格式擁有各自適用的 Application Control 條件。

資料外洩防護

資料外洩防護 (DLP) 可保護組織的機密與敏感資料（稱為數位資產），免遭受意外洩露和蓄意竊取。DLP 允許您：

- 識別要保護的數位資產
- 建立策略，以限制或防止透過常見通道（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

DLP 會根據策略中定義的一組規則來評估資料。策略會決定必須保護以防止未經授權傳輸的資料，以及 DLP 在偵測到傳輸活動時所要執行的處理行動。

重要

每個受管理的產品皆提供不同的策略設定，您可對其進行設定並部署到策略目標。您可以在《*Apex Central Widget* 和策略管理手冊》中找到支援的受管理產品的完整清單及每個產品的策略設定。

您可以使用下列連結來下載手冊的 PDF 版本，或在線上檢視手冊：

https://docs.trendmicro.com/en-us/enterprise/apex-central.aspx

資料識別碼類型

數位資產是組織必須保護以防止未經授權傳輸的檔案和資料。管理員可以透過下列資料識別碼定義數位資產：

- 表示式：具有特定結構的資料。

  如需詳細資訊，請參閱表示式 第 14-15 頁。

- 檔案屬性：檔案類型和檔案大小等檔案內容。

  如需詳細資訊，請參閱檔案屬性 第 14-20 頁。

- 關鍵字清單：特殊字詞或字組的清單。

  如需詳細資訊，請參閱關鍵字 第 14-22 頁。

注意

管理員無法刪除 DLP 範本正在使用的資料識別碼。請先刪除範本，再刪除資料識別碼。

表示式

表示式是具有特定結構的資料。例如，信用卡號碼通常有 16 位數字，而且其格式為 "nnnn-nnnn-nnnn-nnnn"，因此很適合透過表示式來偵測。

管理員可以使用已預先定義的表示式和自訂表示式。

如需詳細資訊，請參閱預先定義的表示式 第 14-16 頁和自訂表示式 第 14-16 頁。

預先定義的表示式

資料外洩防護隨附一組預先定義的表示式。您無法修改或刪除這些表示式。

資料外洩防護會使用病毒碼比對和數學方程式來驗證這些表示式。資料外洩防護將可能的機密資料與表示式進行比對之後，可能還會對資料進行其他的驗證檢查。

如需完整的預先定義表示式清單，請參閱「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。

檢視預先定義的表示式設定

注意

預先定義的表示式無法修改或刪除。

步驟

1. 移至「策略 > 策略資源 > DLP 資料識別碼」。
2. 請點選「表示式」標籤。
3. 請點選某個表示式名稱。
4. 在開啟的畫面中檢視設定。

自訂表示式

如果預先定義的表示式均不符合公司的需求，您可以建立自訂表示式。

表示式是功能強大的字串比對工具。建立表示式之前，請熟悉表示式語法。設計不良的表示式會嚴重影響效能。

建立表示式時：

- 請參閱預先定義的表示式，瞭解如何定義有效的表示式。例如，如果要建立包含日期的表示式，請參閱以「Date」為字首的表示式。
- 請注意，資料外洩防護遵循 Perl Compatible Regular Expressions (PCRE) 中定義的表示式格式。如需 PCRE 的詳細資訊，請造訪下列網站：

  http://www.pcre.org/
- 從簡單的表示式開始。如果表示式造成誤判，請予以修改；您也可以微調表示式以提高偵測的正確性。

建立表示式時，管理員有數種條件可供選擇。表示式必須符合選擇的條件，資料外洩防護才能將它套用到 DLP 策略。如需有關不同條件選項的詳細資訊，請參閱自訂表示式的條件 第 14-17 頁。

自訂表示式的條件

表 14-2. 自訂表示式的條件選項

條件	規則	範例
無	無	全部 — 來自「美國戶口普查局」的姓名 • 表示式：[^\w]([A-Z][a-z]{1,12}(\s?,\s?|[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]
特定字元	表示式必須包含您指定的字元。 此外，表示式中的字元數目必須介於下限到上限之間。	美國 — 美國銀行轉帳號碼 • 表示式：[^\d]([0123678]\d{8})[^\d] • 字元：0123456789 • 字元數目下限：9 • 字元數目上限：9

條件	規則	範例
字尾	字尾是指表示式的最後部分。字尾必須包含您指定的字元並包含特定數目的字元。 此外，表示式中的字元數目必須介於下限到上限之間。	全部 – 住家地址 • 表示式：\D(\d+\s[a-z.]+\s([a-z]+\s){0,2} (lane|ln|street|st|avenue|ave|road|rd|place|pl|drive|dr|circle| cr|court|ct|boulevard|blvd)\.?[0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\ s\d{5}(-\d{4})?)[^\d-] • 字尾字元：0123456789- • 字元數目：5 • 表示式中的字元數目下限：25 • 表示式中的字元數目上限：80
單一字元分隔符號	表示式必須要有兩個部分並用一個字元分隔。這個字元的長度必須是 1 個位元組。 此外，分隔符號左邊的字元數目必須介於下限到上限之間。分隔符號右邊的字元數目不能超過上限。	全部 – 電子郵件信箱 • 表示式：[^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] • 分隔符號：@ • 左邊字元數目下限：3 • 左邊字元數目上限：15 • 右邊字元數目上限：30

建立自訂表示式

步驟

1. 移至「策略 > 策略資源 > DLP 資料識別碼」。
2. 請點選「表示式」標籤。
3. 請點選「新增」。

   接著會顯示一個新畫面。
4. 輸入表示式的名稱。名稱的長度不能超過 100 個位元組，而且不能包含下列字元：

- > < * ^ | & ? \ /

5. 請輸入長度不超過 256 個位元組的說明。
6. 輸入顯示的資料。

   例如，如果要建立識別碼的表示式，請輸入範例識別碼。此資料僅供參考，而且不會顯示在產品的任何地方。

7. 選擇下列其中一個條件，並為選擇的條件配置其他設定（請參閱自訂表示式的條件 第 14-17 頁）：

   - 無
   - 特定字元
   - 字尾
   - 單一字元分隔符號

8. 針對實際資料測試表示式。

   例如，如果表示式會評估國碼，請在「測試資料」文字方塊中輸入有效的識別碼，請點選「測試」，然後檢查結果。

9. 如果您對結果感到滿意，請點選「儲存」。

注意

只在測試成功時才儲存設定。無法偵測到任何資料的表示式會浪費系統資源，而且可能會影響效能。

匯入自訂表示式

如果您有包含表示式且格式正確的 .dat 檔案，請使用此選項。您可以從目前正在存取的伺服器或其他伺服器匯出表示式，來產生該檔案。

步驟

1. 移至「策略 > 策略資源 > DLP 資料識別碼」。

2. 請點選「表示式」標籤。
3. 請點選「匯入」，然後尋找包含表示式的 .dat 檔案。
4. 請點選「開啟」。

   隨即顯示訊息，通知您是否匯入成功。如果要匯入的表示式已存在，系統將會略過該表示式。

檔案屬性

檔案屬性是檔案的特定內容。定義資料識別碼時，您可以使用兩種檔案屬性，亦即檔案類型和檔案大小。例如，某個軟體開發公司可能想要限制只能與研發部門（其成員負責開發和測試該軟體）共用該公司的軟體安裝程式。在此案例中，Apex Central 管理員可以建立一個策略，禁止將大小為 10 到 40 MB 的可執行檔案傳輸到 RD 以外的所有部門。

對於機密檔案而言，單獨使用檔案屬性不是很可靠。承上例，這樣可能也會封鎖其他部門共用的協力廠商軟體安裝程式。因此，Trend Micro 建議您將檔案屬性與其他 DLP 資料識別碼結合，以便提高偵測機密檔案的正確性。

如需完整的支援檔案類型清單，請參閱「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。

建立檔案屬性清單

步驟

1. 移至「策略 > 策略資源 > DLP 資料識別碼」。
2. 請點選「檔案屬性」標籤。
3. 請點選「新增」。

   接著會顯示一個新畫面。
4. 輸入檔案屬性清單的名稱。名稱的長度不能超過 100 個位元組，而且不能包含下列字元：

- > < * ^ | & ? \ /

5. 請輸入長度不超過 256 個位元組的說明。
6. 選取您偏好的真實檔案類型。
7. 如果您要包含的檔案類型並未列出，請選取「副檔名」，然後輸入檔案類型的副檔名。資料外洩防護會檢查具有指定副檔名的檔案，而不會檢查其真實檔案類型。指定副檔名的指導方針：
   - 每個副檔名必須以星號 (*) 為開頭，後接句點 (.)，然後是副檔名。星號是萬用字元，代表檔案的實際名稱。例如，`*.pol` 的相符項目有 `12345.pol` 和 `test.pol`。
   - 您可以在副檔名包含萬用字元。使用問號 (?) 代表單一字元，星號 (*) 代表兩個以上字元。請參閱下列範例：

     - `*.*m` 的相符項目有下列檔案：`ABC.dem`、`ABC.prm`、`ABC.sdcm`

     - `*.m*r` 的相符項目有下列檔案：`ABC.mgdr`、`ABC.mtp2r`、`ABC.mdmr`

     - `*.fm?` 的相符項目有下列檔案：`ABC.fme`、`ABC.fml`、`ABC.fmp`

   - 在副檔名的結尾加上星號時請務必小心，因為這可能會與部分檔案名稱及不相關的副檔名相符。例如：`*.do*` 的相符項目有 `abc.doctor_john.jpg` 和 `abc.donor12.pdf`。
   - 請使用分號 (;) 來分隔副檔名。分號後面不用加上空格。
8. 輸入檔案大小下限和上限（以位元組為單位）。這兩個檔案大小值必須是大於零的正整數。
9. 請點選「儲存」。

匯入檔案屬性清單

如果您有包含檔案屬性清單且格式正確的 `.dat` 檔案，請使用此選項。您可以從目前正在存取的伺服器或其他伺服器匯出檔案屬性清單，來產生該檔案。

步驟

1. 移至「策略 > 策略資源 > DLP 資料識別碼」。
2. 請點選「檔案屬性」標籤。
3. 請點選「匯入」，然後尋找包含檔案屬性清單的 .dat 檔案。
4. 請點選「開啟」。

   隨即顯示訊息，通知您是否匯入成功。如果要匯入的檔案屬性清單已存在，系統將會略過該清單。

關鍵字

關鍵字是特殊字詞或字組。您可以將相關關鍵字新增到關鍵字清單，以識別特定資料類型。例如，「診斷」、「血型」、「接種」和「醫師」是可能出現在診斷書中的關鍵字。如果要防止傳輸診斷書檔案，您可以在 DLP 策略中使用這些關鍵字，然後將資料外洩防護設定為封鎖包含這些關鍵字的檔案。

您可以結合常用字詞以構成有意義的關鍵字。例如，您可以結合 "end"、"read"、"if" 和 "at"，以構成可在原始碼中找到的關鍵字（例如："END-IF"、"END-READ" 和 "AT END"）。

您可以使用已預先定義的關鍵字清單或自訂關鍵字清單。如需詳細資訊，請參閱 預先定義的關鍵字清單 第 14-22 頁和自訂關鍵字清單 第 14-23 頁.

預先定義的關鍵字清單

資料外洩防護隨附一組預先定義的關鍵字清單。您無法修改或刪除這些關鍵字清單。每個清單都有自己的內建條件，可判斷該範本是否會觸發策略違規。

如需資料外洩防護中預先定義關鍵字清單的詳細資訊，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

關鍵字清單的運作方式

關鍵字條件的數目

每個關鍵字清單都包含一個條件，要求文件中必須有特定數目的關鍵字，清單才可觸發違規。

關鍵字數目條件包含下列值：

- 所有：清單中的關鍵字都必須出現在文件中。
- 任何：清單中的任一關鍵字必須出現在文件中。
- 特定數目：文件中至少要有指定數目的關鍵字。如果文件中的關鍵字數目比指定的數目多，則資料外洩防護會觸發違規。

距離條件

某些清單會包含「距離」條件以判定是否有違規情形。「距離」指的是某關鍵字的第一個字元和另一個關鍵的第一個字元之間的字元數。請考慮下列項目：

First Name:_John_ Last Name:_Smith_

此表單 — 名字、姓氏清單包含「距離」條件：五十 (50)，以及常用的表單欄位：「名字」和「姓氏」。以上述的範例而言，當「First Name」的「F」和「Last Name」的「L」之間的字元數為十八 (18) 時，資料外洩防護即會觸發違規。

對於不會觸發違規的項目範例，請考慮以下幾點：

The first name of our new employee from Switzerland is John. His last name is Smith.

在此範例中，「first name」的「f」和「last name」的「l」之間的字元數為六十一 (61)。已超過距離的門檻值，所以不會觸發違規。

自訂關鍵字清單

如果預先定義的關鍵字清單不符合您的需求，您可以建立自訂關鍵字清單。

設定關鍵字清單時，您可以選擇數種條件。關鍵字清單必須符合您選擇的條件，資料外洩防護才能將它套用到策略。為每個關鍵字清單選擇下列其中一個條件：

- 任何關鍵字
- 所有關鍵字
- 在 <x> 個字元內的所有關鍵字
- 關鍵字的結合評分超過門檻值

如需有關條件規則的詳細資訊，請參閱自訂關鍵字清單條件 第 14-24 頁。

自訂關鍵字清單條件

表 14-3. 關鍵字清單的條件

條件	規則
任何關鍵字	檔案至少必須包含關鍵字清單中的一個關鍵字。
所有關鍵字	檔案必須包含關鍵字清單中的所有關鍵字。
在 <x> 個字元內的所有關鍵字	檔案必須包含關鍵字清單中的所有關鍵字。此外，每個關鍵字組都必須在各自的 <x> 個字元內。 例如，您的 3 個關鍵字是 WEB、DISK 和 USB，而您指定的字元數是 20。 如果資料外洩防護依 DISK、WEB 和 USB 的順序偵測到所有這些關鍵字，則從「D」（在 DISK 中）到「W」（在 WEB 中）還有從「W」到「U」（在 USB 中），都最多只能相隔 20 個字元。 下列資料符合此條件：DISK####WEB############USB 下列資料不符合此條件：DISK******************WEB****USB（從「D」到「W」相隔 23 個字元） 決定字元數時請記住，此數字越小（例如 10）通常掃瞄時間就越短，但涵蓋的區域也相對較小。這可能會使得偵測到敏感資料的可能性降低，特別是對於大型檔案。此數字越大，涵蓋的區域也越大，但是掃瞄時間可能會比較長。

條件	規則
關鍵字的結合評分超過門檻值	檔案必須包含關鍵字清單中的一或多個關鍵字。如果只偵測到一個關鍵字，其評分必須高於門檻值。如果有多個關鍵字，其結合評分必須高於門檻值。 請為每個關鍵字指定介於 1 到 10 之間的評分。您應該為機密性較高的的字組或詞組（例如：對於人力資源部門的「調薪」）指定較高的評分。對於本身沒有太高權重的字組或詞組，則可以指定較低的評分。 設定門檻值時，請考慮您為關鍵字指定的評分。例如，如果您有五個關鍵字，而其中有三個關鍵字具有高優先順序，則門檻值可以等於或小於那三個高優先順序關鍵字的結合評分。這表示偵測到這三個關鍵字時就可以將該檔案視為機密檔案。

建立關鍵字清單

步驟

1. 移至「策略 > 策略資源 > DLP 資料識別碼」。
2. 請點選「關鍵字」標籤。
3. 請點選「新增」。

   接著會顯示一個新畫面。
4. 輸入關鍵字清單的名稱。名稱的長度不能超過 100 個位元組，而且不能包含下列字元：

   - > < * ^ | & ? \ /
5. 請輸入長度不超過 256 個位元組的說明。
6. 選擇下列其中一個條件，並為選擇的條件設定其他設定：

   - 任何關鍵字
   - 所有關鍵字
   - 在 <x> 個字元內的所有關鍵字
   - 關鍵字的結合評分超過門檻值

7. 手動將關鍵字新增到清單中：

   a. 輸入長度介於 3 到 40 個位元組之間的關鍵字，並指定是否區分大小寫。

   b. 請點選「新增」。

8. 如果要使用「匯入」選項來新增關鍵字：

   注意

   如果您有包含關鍵字且格式正確的 .csv 檔案，請使用此選項。您可以從目前正在存取的伺服器或其他伺服器匯出關鍵字，來產生該檔案。

   a. 請點選「匯入」，然後尋找包含關鍵字的 .csv 檔案。

   b. 請點選「開啟」。

      隨即顯示訊息，通知您是否匯入成功。如果要匯入的關鍵字已存在於該清單中，系統將會略過該關鍵字。

9. 如果要刪除某個關鍵字，請選取該關鍵字，然後請點選「刪除」。

10. 如果要匯出關鍵字：

    注意

    使用「匯出」功能來備份關鍵字或將它們匯入到另一台伺服器。將匯出關鍵字清單中的所有關鍵字。您無法匯出個別關鍵字。

    a. 請點選「匯出」。

    b. 將產生的 .csv 檔案儲存到想要的位置。

11. 請點選「儲存」。

匯入關鍵字清單

如果您有包含關鍵字清單且格式正確的 .dat 檔案，請使用此選項。您可以從目前正在存取的伺服器或其他伺服器匯出關鍵字清單，來產生該檔案。

步驟

1. 移至「策略 > 策略資源 > DLP 資料識別碼」。
2. 請點選「關鍵字」標籤。
3. 請點選「匯入」，然後尋找包含關鍵字清單的 .dat 檔案。
4. 請點選「開啟」。

   隨即顯示訊息，通知您是否匯入成功。如果要匯入的關鍵字清單已存在，系統將會略過該清單。

資料外洩防護範本

DLP 範本結合 DLP 資料識別碼與邏輯運算子 (And、Or、Except) 以形成條件陳述式。只有滿足特定條件陳述式的檔案或資料會受到 DLP 策略的管制。

例如，檔案必須是 Microsoft Word 檔案（檔案屬性）AND （且）必須包含特定法律詞彙（關鍵字）AND（且）必須包含 ID 號碼（表示式），才能受到「聘用合約」策略管制。此策略允許人力資源部門的員工透過列印方式傳輸檔案，以便將列印複本交由員工簽署。但禁止透過其他可能的通道（例如：電子郵件）傳輸。

如果您已經設定 DLP 資料識別碼，您也可以建立自己的範本。您也可以使用已預先定義的範本。如需詳細資訊，請參閱自訂的 DLP 範本 第 14-28 頁和預先定義的 DLP 範本 第 14-27 頁。

注意

您無法刪除目前正在「DLP 策略」中使用的範本。刪除範本之前，請先從策略移除範本。

預先定義的 DLP 範本

資料外洩防護隨附以下一組已預先定義的範本，供您視各種法規標準需求使用。您無法修改或刪除這些範本。

- GLBA:Gramm-Leach-Billey Act
- HIPAA：健康保險流通與責任法案
- PCI-DSS：支付卡產業資料安全標準
- SB-1386：美國參議院法案 1386
- US PII：美國的個人識別資訊

如需所有預先定義範本的用途，以及受保護的資料範本的詳細清單，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

自訂的 DLP 範本

如果您已經設定資料識別碼，請建立自己的範本。範本結合資料識別碼與邏輯運算子 (And、Or、Except) 以形成條件陳述式。

如需有關條件陳述式和邏輯運算子如何運作的詳細資訊和範例，請參閱條件陳述式和邏輯運算子 第 14-28 頁。

條件陳述式和邏輯運算子

資料外洩防護會從左到右評估條件陳述式。設定條件陳述式時，請小心使用邏輯運算子。使用不當會造成條件陳述式錯誤，而且有可能產生意想不到的後果。

請參閱下表中的範例。

表 14-4. 條件陳述式範例

條件陳述式	解譯和範例
[資料識別碼 1] 和 [資料識別碼 2] Except [資料識別碼 3]	檔案必須滿足 [資料識別碼 1] 和 [資料識別碼 2] 但不用滿足 [資料識別碼 3]。 例如： 檔案必須是 [Adobe PDF 文件] 而且必須包含 [電子郵件信箱]，但是不應該包含 [關鍵字清單中的所有關鍵字]。
[資料識別碼 1] 或 [資料識別碼 2]	檔案必須滿足 [資料識別碼 1] 或 [資料識別碼 2]。 例如： 檔案必須是 [Adobe PDF 文件] 或 [Microsoft Word 文件]。
Except [資料識別碼 1]	檔案必須不滿足 [資料識別碼 1]。 例如： 檔案不能是 [多媒體檔案]。

如表格中最後一個範例所示，如果檔案必須不能滿足陳述式中的所有資料識別碼，則條件陳述式中的第一個資料識別碼可以有「Except」運算子。不過，在大部分的情況下，第一個資料識別碼沒有運算子。

建立範本

步驟

1. 移至「策略 > 策略資源 > DLP 範本」。
2. 請點選「新增」。

   接著會顯示一個新畫面。
3. 輸入範本的名稱。名稱的長度不能超過 100 個位元組，而且不能包含下列字元：

   - > < * ^ | & ? \ /
4. 請輸入長度不超過 256 個位元組的說明。

5. 選取資料識別碼，然後請點選「新增」圖示。

   選取定義時：

   - 按住 CTRL 鍵，然後選取資料識別碼，就可以選取多個項目。
   - 如果想要使用特定定義，可以使用搜尋功能。您可以輸入完整或部分的資料識別碼名稱。
   - 每個範本最多可以包含 30 個資料識別碼。

6. 如果要建立新的表示式，請點選「表示式」，再請點選「新增表示式」。在顯示的畫面中，設定該表示式的設定。

7. 如果要建立新的檔案屬性清單，請點選「檔案屬性」，再請點選「新增檔案屬性」。在顯示的畫面中，設定該檔案屬性清單的設定。

8. 如果要建立新的關鍵字清單，請點選 「關鍵字」，再請點選 「新增關鍵字」。在顯示的畫面中，設定該關鍵字清單的設定。

9. 如果您選取表示式，請輸入出現次數，這是指資料外洩防護將表示式套用至策略之前，表示式必須出現的次數。

10. 為每個定義選擇邏輯運算子。

    注意

    設定條件陳述式時，請小心使用邏輯運算子。使用不當會造成條件陳述式錯誤，而且有可能產生意想不到的後果。如需正確用法範例，請參閱條件陳述式和邏輯運算子 第 14-28 頁。

11. 如果要從選取的識別碼清單中移除資料識別碼，請點選資源回收筒圖示。

12. 在「預覽」下方，檢查條件陳述式並視需要修改不適用的陳述式。

13. 請點選「儲存」。

匯入範本

如果您有包含範本且格式正確的 `.dat` 檔案，請使用此選項。您可以從目前正在存取的伺服器或其他伺服器匯出範本，來產生該檔案。

步驟

1. 移至「策略 > 策略資源 > DLP 範本」。
2. 請點選「匯入」，然後尋找包含範本的 .dat 檔案。
3. 請點選「開啟」。

   隨即顯示訊息，通知您是否匯入成功。如果要匯入的範本已存在，系統將會略過該範本。

入侵防護規則

「入侵防護規則」畫面顯示 Apex Central Vulnerability Protection 支援的入侵防護規則。入侵防護規則會檢查網路封包（和封包序列）的實際內容。根據入侵防護規則中的條件組，對這些封包執行各種處理行動。這些處理行動包括替換專門定義的或可疑的位元組序列，或是完全丟棄封包並重設連線。

- 若要過濾規則清單，請使用「搜尋」方塊來指定顯示在任何欄中的完整或部分字串。
- 若要依欄資料排序入侵防護規則的清單，請按一下欄標題。
- 若要檢視詳細的入侵防護規則內容，請按一下規則之「規則名稱」欄中的連結。
- 若要將來自一或多個來源端點的流量排除不進行 Vulnerability Protection 掃瞄，請按一下「設定例外」，並指定來源 IP 位址。

  注意

  您最多可將 100 個項目新增到例外清單。

注意

在手動或預約元件更新期間，Apex Central 會自動從 Apex One 伺服器匯入/更新入侵防護規則。

重要

每個受管理的產品皆提供不同的策略設定，您可對其進行設定並部署到策略目標。您可以在《*Apex Central Widget* 和策略管理手冊》中找到支援的受管理產品的完整清單及每個產品的策略設定。

您可以使用下列連結來下載手冊的 PDF 版本，或在線上檢視手冊：

https://docs.trendmicro.com/en-us/enterprise/apex-central.aspx

下表說明「入侵防護規則」畫面上顯示的規則資訊。

欄	說明
識別碼	入侵防護規則的唯一識別碼標籤
規則名稱	入侵防護規則的名稱
應用程式類型	此入侵防護規則所分組到的應用程式類型
嚴重性	趨勢科技指派給規則的嚴重性等級 **注意** 規則的嚴重性對規則的實作或套用方式並無影響。檢視「入侵防護規則」清單時，嚴重性等級非常適合當成排序條件使用。
模式	入侵防護模組使用的網路引擎偵測模式。按一下模式可對規則進行設定。
類型	偵測到的弱點類型： • 主動式：已知或未知（例如，零時差）弱點 • 弱點攻擊：已知弱點的已知弱點攻擊（通常為簽章型） • 弱點：可能存在一或多個弱點攻擊的弱點
CVE	MITRE 指派給弱點的常見弱點和漏洞 (CVE®) 識別碼 如需詳細資訊，請參閱 http://cve.mitre.org/。
Microsoft	Microsoft 指派給弱點的常見弱點和漏洞 (CVE®) 識別碼

欄	說明
CVSS 評分	根據美國國家弱點資料庫 (National Vulnerability Database) 對弱點進行測量得出的常見弱點評分系統 (CVSS) 嚴重性評分 如需詳細資訊，請參閱 http://nvd.nist.gov/cvss.cfm。
上次更新時間	規則上次修改的日期和時間

入侵防護規則內容

「入侵防護規則內容」畫面顯示有關特定入侵防護規則和弱點的詳細資訊。按一下「一般」標籤或「弱點」，可檢視有關規則的詳細資料。

下表說明「一般」標籤和「弱點」標籤上提供的資訊。

表 14-5. 一般資訊

資料	說明
識別碼	入侵防護規則的唯一識別碼標籤
名稱	入侵防護規則的名稱
說明	入侵防護規則的說明 注意 Apex One Vulnerability Protection 不支援單機版 Trend Micro Vulnerability Protection 上可用的組態設定選項。
應用程式類型	此入侵防護規則所分組到的應用程式類型
優先順序	入侵防護規則的優先順序層級。系統會先套用優先順序較高的規則，然後再套用優先順序較低的規則。

資料	說明
嚴重性	趨勢科技指派給規則的嚴重性等級 注意 規則的嚴重性對規則的實作或套用方式並無影響。檢視「入侵防護規則」清單時，嚴重性等級非常適合當成排序條件使用。
模式	入侵防護模組使用的網路引擎偵測模式。按一下模式可對規則進行設定。
類型	偵測到的弱點類型： • 主動式：已知或未知（例如，零時差）弱點 • 弱點攻擊：已知弱點的已知弱點攻擊（通常為簽章型） • 弱點：可能存在一或多個弱點攻擊的弱點
已核發	規則的發佈（而非下載）日期
上次更新時間	規則上次修改的日期和時間

表 14-6. 弱點資訊

資料	說明
嚴重性	弱點的嚴重性等級
CVSS 評分	根據美國國家弱點資料庫 (National Vulnerability Database) 對弱點進行測量得出的常見弱點評分系統 (CVSS) 嚴重性評分 如需詳細資訊，請參閱 http://nvd.nist.gov/cvss.cfm。
說明	弱點的說明
外部參考	我們提供外部參考的連結，可讓您瞭解有關弱點的詳細資訊

周邊設備存取控管允許的裝置

匯入或匯出適用於所有 Apex One Security Agent 策略目標的「周邊設備存取控管允許的裝置」清單。

注意

- 僅啟動「資料安全防護」的 Security Agent 可覆寫已新增至「周邊設備存取控管允許的裝置」清單中之裝置的「封鎖」或「讀取」處理行動。
- 「周邊設備存取控管允許的裝置」清單不適用於無「資料安全防護」的 Security Agent，以及「周邊設備存取控管」權限未設定為「封鎖」或「讀取」的 Security Agent。

項目	說明
匯入	選取格式正確的 CSV 檔案，其中包含您要在所有 Apex One Security Agent 端點上允許的所有裝置的清單。 重要 匯入新的清單時，會徹底覆寫先前的清單。若要保留現有清單，請先匯出清單後，再匯入新的 CSV 檔案。
上次匯入時間	伺服器匯入目前清單的日期/時間
允許的裝置總數	目前所套用清單中允許的裝置總數
匯出	以 CSV 格式匯出目前允許的清單

部分 V

偵測

第 15 章

記錄檔

本章說明如何存取 Apex Central 產生的記錄檔和向 Apex Central 註冊的受管理產品中的記錄檔。

包含下列主題：

- 記錄查詢 第 15-2 頁
- 查詢記錄檔 第 15-2 頁
- 設定記錄檔彙整 第 15-12 頁
- 設定 Syslog 轉送 第 15-13 頁
- 刪除記錄檔 第 15-18 頁

記錄查詢

Apex Central 可讓您查詢 Apex Central 資料庫中 Apex Central 產生的記錄檔和已註冊受管理產品中的記錄檔資料。

Apex Central 也讓您可以執行以下操作：

- 使用進階過濾器縮小記錄查詢搜尋結果的範圍。
- 設定記錄檔彙整設定，以降低受管理產品的記錄檔資料傳送到 Apex Central 伺服器時的網路流量。
- 請依類型手動刪除記錄項目，或設定自動刪除記錄。

查詢記錄檔

使用「記錄查詢」畫面查詢 Apex Central 產生的記錄檔和已註冊受管理產品中的記錄檔資料。您也可以使用進階自訂過濾器來縮小搜尋結果範圍、以 XML 或 CSV 格式匯出搜尋結果，或儲存記錄查詢搜尋條件並與其他 Apex Central 管理員共用。

注意

Apex Central 也允許您從「產品目錄」」畫面執行記錄查詢。

如需詳細資訊，請參閱從產品目錄查詢記錄檔 第 10-9 頁。

步驟

1. 移至「偵測 > 記錄檔 > 記錄查詢」。

   會出現「記錄查詢」畫面。

2. 指定記錄類型。

注意

記錄類型對應於 Apex Central 報告中使用的特定資料檢視。

如需有關記錄類型和資料檢視的詳細資訊，請參閱記錄檔名稱與資料檢視 第 15-6 頁。

a. 從第一個下拉式清單控制項中選取記錄類型。

b. 按一下「確定」以套用選取的記錄類型。

3. 如果要將搜尋結果過濾為來自特定受管理產品的資料，請執行下列作業：

a. 按一下第二個下拉式清單控制項。

b. 使用下列其中一個選項選取要查詢的目標：

- 目錄：可讓您從「產品目錄」結構找出受管理產品並加以選取
- 類型：可讓您選擇產品類型，然後從同類型的所有已註冊受管理產品清單中進行選取
- 標籤和過濾器：可讓您從使用者/端點目錄選取自訂標籤 (Tags)、過濾器或重要標籤來查詢特定端點

注意

- 您可以選取最多 10 個自訂標籤 (Tags)、過濾器或重要標籤來執行記錄查詢。
- 不能使用內含「符合性」、「重要」、「安全威脅類型」、「安全威脅」或「安全威脅狀態條件」資訊的自訂過濾器來執行記錄查詢。

c. 按一下「確定」以套用選取的目標。

4. 從「時間」下拉式清單控制項中選取時間範圍。

5. 如果要使用自訂條件過濾搜尋結果，請執行下列作業：

a. 按一下「顯示進階過濾器」。

b. 指定自訂過濾器的「符合」規則：

- 所有條件：資料必須符合所有指定的條件
- 任何條件：資料符合任一指定的條件即可

c. 在「選取條件...」下拉式清單中，選取要過濾的資料欄。

注意

「選取條件...」下拉式清單中的資料欄會根據您在第一個下拉式清單控制項中選取的記錄類型而動態變更。

如需有關資料欄的詳細資訊，請參閱記錄檔名稱與資料檢視 第 15-6 頁，並參考對應的資料檢視詳細資料。

顯示在第二個和第三個下拉式清單中的過濾條件會根據您選取的資料欄而動態變更。

d. 在第二個下拉式清單中，選取運算子。

e. 在第三個下拉式清單中，定義條件。

注意

Apex Central 支援使用多達 20 個自訂過濾條件來進行各個記錄查詢。

6. 請點選「搜尋」。

在「記錄查詢」畫面的資料表中會顯示搜尋結果。

注意

- 「產生時間」欄會顯示受管理產品首次偵測到安全威脅時，端點上的本機日期和時間。
- 「接收時間」欄會顯示 Apex Central 伺服器從受管理產品伺服器收到資料時，Apex Central 伺服器上的本機日期和時間。

7. （選用）按一下資料欄中的連結，可向下切入來瞭解詳細資訊。

8. （選用）在搜尋結果中自訂資料欄。

- 按一下「自訂欄」來新增或移除資料表中顯示的欄。

- 拖曳欄標題來重新排列欄的顯示順序。

9. （選用）匯出記錄查詢結果。

   a. 按一下「匯出到 CSV」或「匯出到 XML」。

      會出現「記錄查詢匯出頁面」畫面。

   b. 匯出完成後，開啟或儲存檔案。

10. （選用）儲存記錄查詢搜尋條件。

注意

- 儲存記錄查詢時，只會儲存查詢的搜尋條件。如果要儲存記錄查詢搜尋結果，請匯出結果或使用格線資料表建立報告。

  如需有關建立報告的詳細資訊，請參閱報告 第 17-1 頁。

- 已儲存的查詢會自動顯示給來自相同 Active Directory 群組的所有使用者。

- 已儲存的查詢旁邊的灰色「使用者」圖示 ( )，表示 Active Directory 群組之外的使用者共用該記錄查詢。將滑鼠游標暫留在這個圖示上，可以檢視共用查詢的使用者名稱。

---

   a. 按一下「儲存」按鈕 ( )。

   b. 指定已儲存查詢的名稱。

   c. 按一下「儲存」。

儲存記錄查詢後，您可以按一下「已儲存的查詢」按鈕 ( ) 檢視已儲存的查詢清單，然後執行下列處理行動。

- 按一下已儲存的查詢名稱，以執行記錄查詢。
- 按一下已儲存的查詢名稱旁邊的「共用」圖示 ( )，可與所有的 Apex Central 使用者共用記錄查詢。
- 按一下已儲存的查詢名稱旁邊的「停止共用」圖示 ( )，即可停止與所有 Apex Central 使用者共用記錄查詢。

- 按一下「刪除」圖示 (🗑) 可移除已儲存的查詢。

記錄檔名稱與資料檢視

Apex Central 記錄檔類型與自訂報告範本的特定資料檢視對應。您可以使用下列資料檢視，針對記錄查詢結果建立自訂報告範本。

如需詳細資訊，請參閱下列主題：

- 自訂範本 第 17-2 頁
- 資料檢視 第 B-1 頁

表 15-1. 安全記錄檔

記錄檔名稱	資料檢視	說明
系統事件：		
病毒/惡意程式	病毒/惡意程式詳細資訊	提供有關網路上病毒/惡意程式偵測的特定資訊，例如偵測到病毒/惡意程式的受管理產品、病毒/惡意程式的名稱，以及中毒端點的名稱 如需詳細資訊，請參閱病毒/惡意程式詳細資訊 第 B-68 頁。
間諜程式/可能的資安威脅程式	間諜程式/可能的資安威脅程式詳細資訊	提供有關網路上間諜程式/可能的資安威脅程式偵測的特定資訊，例如偵測到間諜程式/可能的資安威脅程式的受管理產品、間諜程式/可能的資安威脅程式的名稱，以及中毒端點的名稱 如需詳細資訊，請參閱間諜程式/可能的資安威脅程式詳細資訊 第 B-56 頁。
可疑檔案	可疑檔案詳細資訊	提供有關網路中偵測到的可疑檔案的特定資訊 如需詳細資訊，請參閱可疑檔案詳細資訊 第 B-5 頁。

記錄檔名稱	資料檢視	說明
行為監控	行為監控詳細資訊	提供有關網路上行為監控事件的特定資訊 如需詳細資訊，請參閱行為監控詳細資訊 第 B-45 頁。
完整性監控	完整性監控資訊	用來監控端點上發生的特定變更，例如已安裝的軟體、執行中的服務、程序、檔案、目錄、監聽通訊埠、登錄機碼和登錄值 如需詳細資訊，請參閱完整性監控資訊 第 B-50 頁。
Application Control	Application Control 違規詳細資訊	提供有關您網路中發生之 Application Control 違規的特定資訊（例如，違反的 Security Agent 策略和條件） 如需詳細資訊，請參閱 Application Control 違規詳細資訊 第 B-43 頁。
周邊設備存取控管	裝置存取控制資訊	提供有關網路上裝置存取控制事件的特定資訊 如需詳細資訊，請參閱裝置存取控制資訊 第 B-41 頁。
端點安全性符合	端點安全性符合詳細資訊	提供有關網路上端點安全性符合的特定資訊 如需詳細資訊，請參閱端點安全性符合詳細資訊 第 B-46 頁。
端點安全違規	端點安全違規詳細資訊	提供有關網路上端點安全違規的特定資訊 如需詳細資訊，請參閱端點安全違規詳細資訊 第 B-46 頁。
Machine Learning	Machine Learning 詳細資訊	提供有關 Machine Learning 偵測到的進階未知安全威脅的特定資訊 如需詳細資訊，請參閱 Machine Learning 詳細資訊 第 B-3 頁。

記錄檔名稱	資料檢視	說明
沙箱	沙箱偵測詳細資訊	提供有關沙箱偵測到的進階未知安全威脅的特定資訊 如需詳細資訊，請參閱沙箱偵測資訊 第 B-6 頁。
沙箱可疑物件	沙箱可疑物件影響詳細資訊	提供有關沙箱可疑物件之影響的詳細資訊 如需詳細資訊，請參閱沙箱可疑物件影響詳細資訊 第 B-7 頁。
攻擊發現	攻擊發現偵測資訊	提供有關攻擊發現所偵測到的安全威脅的一般資訊 如需詳細資訊，請參閱攻擊發現偵測資訊 第 B-9 頁。
灰色軟體偵測	灰色軟體偵測資訊	提供在您網路上偵測到的可能攻擊指標的詳細資訊 如需詳細資訊，請參閱灰色軟體偵測資訊 第 B-35 頁。
網路事件：		
垃圾郵件連線	垃圾郵件連線資訊	提供有關您網路中垃圾郵件來源的特定資訊（例如，偵測到垃圾郵件的受管理產品、受管理產品採取的特定處理行動，以及偵測到的垃圾郵件總數） 如需詳細資訊，請參閱垃圾郵件連線資訊 第 B-53 頁。
內容違規	內容違規詳細資訊	提供有關內含內容違規之電子郵件的特定資訊（例如，偵測到內容違規的受管理產品、電子郵件的寄件者和收件者、內容違規策略的名稱，以及偵測到的違規總數） 如需詳細資訊，請參閱內容違規詳細資訊 第 B-16 頁。

記錄檔名稱	資料檢視	說明
進階電子郵件安全威脅	進階電子郵件安全威脅	提供有關內含進階安全威脅之電子郵件的特定資訊（例如，異常行為、假資料或誤導資料、可疑和惡意行為特徵碼，以及表示系統遭到入侵但需要進一步調查以確認的字串） 如需詳細資訊，請參閱內含進階安全威脅的電子郵件訊息 第 B-17 頁。
網頁信譽評等	網頁信譽評等詳細資訊	提供有關網頁信譽評等服務所偵測到之應用程式活動的符合性資訊 如需詳細資訊，請參閱網站信譽評等服務詳細資訊 第 B-79 頁。
Web 違規	Web 違規偵測詳細資訊	提供有關網路上網頁違規偵測的特定資訊 如需詳細資訊，請參閱 Web 違規詳細資訊 第 B-81 頁。
防火牆違規事件	防火牆違規事件詳細資訊	提供有關您網路中防火牆違規的特定資訊（例如，偵測到違規的受管理產品、傳輸來源和傳輸目標，以及防火牆違規的總數） 如需詳細資訊，請參閱防火牆違規事件詳細資訊 第 B-47 頁。
網路內容檢測	網路內容檢測資訊	提供有關網路上網路內容違規的特定資訊 如需詳細資訊，請參閱網路內容檢測資訊 第 B-51 頁。
入侵防護	入侵防護詳細資訊	提供特定資訊來協助您及時防範已知和零時差攻擊、防禦 Web 應用程式弱點，以及找出存取網路的惡意軟體 如需詳細資訊，請參閱入侵防護詳細資訊 第 B-49 頁。
C&C 回呼	C&C 回呼詳細資訊	提供有關網路上偵測到的 C&C 回呼事件的特定資訊 如需詳細資訊，請參閱 C&C 回呼詳細資訊 第 B-2 頁。

記錄檔名稱	資料檢視	說明
可疑安全威脅	可疑安全威脅詳細資訊	提供有關網路上可疑安全威脅的特定資訊，例如：偵測到可疑安全威脅的受管理產品、有關來源與目標的特定資訊、網路上的可疑安全威脅總數 如需詳細資訊，請參閱可疑安全威脅詳細資訊 第 B-25 頁。
應用程式活動	詳細應用程式活動	顯示有關違反網路安全策略的應用程式活動的特定資訊 如需詳細資訊，請參閱詳細應用程式活動 第 B-41 頁。
自動威脅清除	自動威脅清除詳細資訊	提供有關網路上緩和伺服器為解決安全威脅所執行之工作的特定資訊 如需詳細資訊，請參閱緩和詳細資訊 第 B-24 頁。
威脅關聯偵測	威脅關聯偵測詳細資訊	提供有關安全威脅詳細分析及矯正建議的特定資訊 如需詳細資訊，請參閱關聯詳細資訊 第 B-23 頁。
資料安全防護事件：		
資料外洩防護	DLP 事件資訊	提供有關資料外洩防護偵測到的事件的特定資訊 如需詳細資訊，請參閱 DLP 事件資訊 第 B-20 頁。
Data Discovery	資料發現資料外洩防護偵測資訊	顯示有關 Data Discovery 偵測到的事件的特定資訊 如需詳細資訊，請參閱資料發現資料外洩防護偵測資訊 第 B-18 頁。

表 15-2. 產品資訊

記錄檔名稱	資料檢視	說明
受管理的產品：		

記錄檔名稱	資料檢視	說明
產品狀態	產品狀態資訊	提供有關已向 Apex Central 伺服器註冊之受管理產品的詳細資訊（例如，受管理產品的版本和 Build 號碼，以及受管理產品伺服器的作業系統） 如需詳細資訊，請參閱產品狀態資訊 第 B-102 頁。
產品事件	產品事件資訊	提供受管理產品事件的相關資訊（例如，受管理產品向 Apex Central 註冊、元件更新，以及啟動碼部署） 如需詳細資訊，請參閱產品事件資訊 第 B-102 頁。
產品稽核事件	產品稽核事件記錄檔	提供受管理產品稽核事件的相關資訊（例如，受管理產品主控台存取） 如需詳細資訊，請參閱產品稽核事件記錄檔 第 B-100 頁。
Apex Central：		
指令追蹤	指令追蹤資訊	提供 Apex Central 向受管理產品發出之指令的相關資訊（例如，Apex Central 發出進行元件更新或啟動碼部署之指令的日期和時間，以及指令的狀態） 如需詳細資訊，請參閱指令追蹤資訊 第 B-89 頁。
Apex Central 事件	Apex Central 事件資訊	提供 Apex Central 伺服器事件的相關資訊（例如，受管理產品向 Apex Central 註冊、元件更新，以及啟動碼部署） 如需詳細資訊，請參閱 Apex Central 事件資訊 第 B-88 頁。
未受管理的端點	未受管理的端點	提供所偵測到未安裝 Trend Micro Security Agent 之端點的相關資訊。 如需詳細資訊，請參閱未受管理的端點資訊 第 B-90 頁。

記錄檔名稱	資料檢視	說明
使用者存取	使用者存取資訊	提供 Apex Central 使用者存取權及使用者登入 Apex Central 時所執行活動的相關資訊 如需詳細資訊，請參閱使用者存取資訊 第 B-90 頁。
產品使用授權	產品使用授權詳細資訊	提供受管理產品或服務之啟動碼與使用授權狀態的相關資訊（例如，受管理產品的版本和使用授權到期日） 如需詳細資訊，請參閱產品使用授權詳細資訊 第 B-98 頁。

設定記錄檔彙整

記錄檔彙整可讓您僅將選取的資料從受管理產品傳送到 Apex Central 伺服器，來節省網路頻寬。

警告!

Apex Central 無法還原受管理產品未傳送到 Apex Central 伺服器的資料。

步驟

1. 移至「偵測 > 記錄檔 > 記錄檔彙整設定」。

   會出現「編輯記錄檔彙整規則」畫面。

2. 選取「啟動記錄檔彙整」。
3. 展開記錄檔類別。
4. 不勾選此核取方塊可停止將資料從受管理產品傳送到 Apex Central。
5. 按一下「儲存」。

設定 Syslog 轉送

使用「Syslog 設定」畫面來設定 Apex Central 將支援的記錄檔轉送到 Syslog 伺服器。

如需詳細資訊，請參閱下列主題：

- 關閉 Syslog 轉送 第 15-16 頁
- 支援的記錄類型和格式 第 15-17 頁

注意

- 如果您是從舊版 Control Manager 安裝移轉到 Apex Central，則 Apex Central 會自動匯入您先前使用 LogForwarder 工具（<Control Manager 安裝目錄>\LogForwarder.exe）所設定的 Syslog 轉送設定。
- 移轉到 Apex Central 之後，就無法再執行 LogForwarder 工具。

步驟

1. 移至「管理 > 設定 > Syslog 設定」。

   會出現「Syslog 設定」畫面。

2. 選取「啟動 Syslog 轉送」核取方塊。
3. 為接收所轉送 Syslog 的伺服器設定下列設定：
   - 伺服器位址：Syslog 伺服器 IP 位址或 FQDN
   - 通訊埠：Syslog 伺服器通訊埠號碼
   - 通訊協定：選取傳輸通訊協定

注意

如果選取「SSL/TLS」，Apex Central 預設會接受有效的自我簽署憑證。

- 如果伺服器憑證包含「主體替代名稱」，則「主體替代名稱」必須包含伺服器 FQDN 或 IP 位址。
- 若要獲得額外的安全防護，請使用有效的伺服器憑證或將伺服器憑證上傳到 Apex Central。

4. （選用）若要上傳伺服器憑證，請執行下列作業：

重要

- Apex Central 僅支援採用 .DER 或 .PEM 編碼的伺服器憑證（使用 X.509 格式）。

  如需詳細資訊，請參閱 https://support.ssl.com/Knowledgebase/Article/View/19/0/der-vs-crt-vs-cer-vs-pem-certificates-and-how-to-convert-them。
- Apex Central 僅支援上傳用於 SSL/TLS 傳輸的伺服器憑證。

a. 選取「使用伺服器憑證」核取方塊。

b. 按一下「選取」從電腦中選取伺服器憑證。

c. 按一下「開啟」。

Apex Central 會上傳選取的伺服器憑證。

5. （選用）若要使用 Proxy 伺服器來進行 Syslog 轉送，請選取「使用 SOCKS Proxy 伺服器」核取方塊。

重要

- Apex Central 僅支援透過 SOCKS 通訊協定 Proxy 伺服器（用於 SSL/TLS 或 TCP 傳輸）來進行 Syslog 轉送。
- Syslog 轉送不支援 HTTP Proxy 伺服器。如果要使用 Proxy 伺服器來進行 Syslog 轉送，請按一下「設定 Proxy 伺服器設定」，然後在「Proxy 伺服器設定」畫面上選取 SOCKS 通訊協定伺服器。

  如需詳細資訊，請參閱設定用於元件/使用授權更新、雲端服務及 Syslog 轉送的 Proxy 伺服器設定 第 11-11 頁。

Apex Central 會使用在「Proxy 伺服器設定」畫面（「管理 > 設定 > Proxy 伺服器設定」）上設定的 Proxy 伺服器來進行 Syslog 轉送。

6. 選取記錄檔格式：
   - CEF：記錄檔訊息會使用標準的「一般事件格式」(CEF)
   - Apex Central 格式：將 Syslog「設備」代碼設定為「Local0」，並將「嚴重性」代碼設定為「Notice」

   如需詳細資訊，請參閱支援的記錄類型和格式 第 15-17 頁。
7. 設定 Apex Central 轉送記錄檔的頻率。
8. 選取要轉送的記錄類型：
   a. 從「記錄類型」下拉式清單中選取記錄檔類別：

      注意

      您可以從多個記錄檔類別中選取記錄類型。

      - 安全記錄檔
      - 產品資訊

   b. 選取您要轉送之記錄檔的核取方塊。

      Apex Central 會在「記錄類型」下拉式清單旁顯示所選記錄類型的總數。

c. （選用）從「記錄類型」下拉式清單中選取其他記錄檔類別，即可選取要轉送的額外記錄類型。

9. （選用）按一下「測試連線」以測試伺服器連線。

注意

測試連線不會儲存 Syslog 伺服器設定。

Syslog 伺服器連線狀態會顯示在畫面頂端。

10. 按一下「儲存」。

- Apex Central 會開始將記錄檔轉送到設定的 Syslog 伺服器。
- 如果要監控記錄檔轉送狀態，請移至「管理 > 指令追蹤」，然後從「指令」下拉式清單中選取「轉送 Syslog」。

  如需詳細資訊，請參閱查詢及檢視指令 第 12-3 頁。

關閉 Syslog 轉送

使用「Syslog 設定」畫面來停止從 Apex Central 轉送記錄檔到 Syslog 伺服器。

步驟

1. 移至「管理 > 設定 > Syslog 設定」。

   會出現「Syslog 設定」畫面。

2. 不勾選「啟動 Syslog 轉送」核取方塊。

3. 按一下「儲存」。

   Apex Central 會停止將記錄檔轉送到設定的 Syslog 伺服器。

支援的記錄類型和格式

Apex Central 可以採用下列記錄格式將記錄檔轉送到 Syslog 伺服器：

- CEF：記錄檔訊息會使用標準的「一般事件格式」(CEF)
- Apex Central 格式：將 Syslog「設備」代碼設定為「Local0」，並將「嚴重性」代碼設定為「Notice」

下表列出每一種記錄類型支援的格式：

表 15-3. 安全記錄檔

記錄類型	CEF	Apex Central 格式
Application Control	是	否
攻擊發現	是	否
行為監控	是	是
C&C 回呼	是	否
內容違規	是	否
資料外洩防護	是	是
周邊設備存取控管	是	是
入侵防護	是	否
網路內容檢測	是	否
Machine Learning	是	否
間諜程式/可能的資安威脅程式	是	否
可疑檔案	是	否
沙箱	是	否
病毒/惡意程式	是	否
Web 違規	是	否

表 15-4. 產品資訊

記錄類型	CEF	APEX CENTRAL 格式
引擎更新狀態	是	是
受管理的產品登入/登出事件	是	是
產品稽核事件	是	否
病毒碼更新狀態	是	是

如需有關對應 CEF 與 Apex Central 格式之間 Syslog 內容的資訊，請參閱 Syslog 內容對應 — CEF 第 F-1 頁。

刪除記錄檔

使用「記錄檔維護」畫面可手動依類型刪除記錄項目，或是設定自動刪除記錄。

警告!

手動刪除記錄檔資料可能會影響報告的產生。

秘訣

Trend Micro 建議您將資料外洩防護記錄檔備份至您的 Security Information and Event Management (SIEM) 伺服器，並將記錄檔保留至少 2 年。

步驟

1. 移至「偵測 > 記錄檔 > 記錄檔維護」。

   會出現「記錄檔維護」畫面。

2. 如果要手動刪除記錄，請執行下列作業：

   a. 選取記錄類型的核取方塊。

b. 根據您要刪除的記錄項目類型，按一下對應列中的「全部刪除」。

接著會出現確認訊息。

c. 按一下「確定」，可刪除所選類型的所有記錄。

3. 如果要設定自動刪除記錄，請執行下列作業：

a. 選取記錄類型的核取方塊。

b. 在「記錄項目數上限」欄中，指定 Apex Central 保留的記錄數目上限。

注意

依預設，Apex Central 會保留最多 1,000,000 個記錄項目。

c. 在「清除偏移」欄中，指定當記錄數目達到「記錄項目數上限」欄中指定的數目時，Apex Central 所要刪除的記錄數目。

注意

依預設，清除偏移值是 1,000 個記錄項目。

d. 在「記錄保留時間上限」欄中，指定 Apex Central 自動刪除存在多長時間的記錄。

注意

依預設，記錄保留時間上限為 90 天。

e. 按一下「儲存」。

第 16 章

通知

本節討論如何傳送有關 Apex Central 網路上所發生事件的通知。

包含下列主題：

- 事件通知 第 16-2 頁
- 通知方法設定 第 16-3 頁
- 聯絡人群組 第 16-6 頁
- 進階安全威脅活動事件 第 16-9 頁
- 內容策略違規事件 第 16-30 頁
- 資料外洩防護事件 第 16-33 頁
- 已知的安全威脅活動事件 第 16-42 頁
- 網路存取控制事件 第 16-57 頁
- 不尋常的產品行為事件 第 16-60 頁
- 更新 第 16-67 頁

事件通知

Apex Central 可以通知收件者個人或群組有關受管理產品偵測到的事件。支援的通知方法包括電子郵件訊息、Windows 系統記錄檔通知、SMNP Trap、Ssyslog 訊息及觸發應用程式。

如需詳細資訊，請參閱通知方法設定 第 16-3 頁

使用「事件通知」畫面來啟動或關閉有關下列類別的事件通知。

事件類別	說明
進階安全威脅活動	提供有關進階和未知安全威脅的警告 如需詳細資訊，請參閱進階安全威脅活動事件 第 16-9 頁。
內容策略違規	提供有關電子郵件內容和 URL 安全策略違規的警告 如需詳細資訊，請參閱內容策略違規事件 第 16-30 頁。
資料外洩防護	提供有關資料外洩防護事件和範本相符項目的資訊 如需詳細資訊，請參閱資料外洩防護事件 第 16-33 頁。
已知的安全威脅活動	提供有關防毒受管理產品偵測到的病毒/間諜程式/可能的資安威脅程式的警告 如需詳細資訊，請參閱已知的安全威脅活動事件 第 16-42 頁。
網路存取控制	提供來自受管理網路病毒牆產品的警告 如需詳細資訊，請參閱網路存取控制事件 第 16-57 頁。
不尋常的產品行為	提供有關產品選項或服務啟動和停用的資訊 如需詳細資訊，請參閱不尋常的產品行為事件 第 16-60 頁。

事件類別	說明
更新	提供防毒和內容安全元件更新結果（成功或不成功） 如需詳細資訊，請參閱更新 第 16-67 頁。

通知方法設定

使用「通知方法設定」畫面可進行下列通知方法的設定。

方法	說明
電子郵件	設定「SMTP 伺服器設定」以傳送有關受管理產品所偵測到事件的電子郵件通知。 如需詳細資訊，請參閱設定 SMTP 伺服器設定 第 16-3 頁。
SNMP Trap	設定「SNMP Trap 設定」以傳送有關受管理產品所偵測到事件的 SNMP Trap 通知。 如需詳細資訊，請參閱設定 SNMP Trap 設定 第 16-4 頁。
Syslog	設定「Syslog 設定」，以將 Syslog 訊息傳送給選取的收件者或支援的協力廠商產品。 如需詳細資訊，請參閱設定 Syslog 設定 第 16-5 頁。
觸發應用程式	提供使用者認證以觸發組織所用的內部或產業標準應用程式來傳送通知。 如需詳細資訊，請參閱設定觸發應用程式設定 第 16-5 頁。

設定 SMTP 伺服器設定

Apex Central 允許您傳送電子郵件來向選取的收件者通知受管理產品偵測到的事件。

重要

您必須設定「SMTP 伺服器設定」，Apex Central 才能傳送電子郵件。

步驟

1. 移至「偵測 > 通知 > 通知方法」。

   會出現「通知方法」畫面。

2. 在「SMTP 伺服器設定」區段中，指定下列項目：

   a. 伺服器 FQDN 或 IP 位址：輸入有效的 FQDN、IPv4 或 IPv6 位址。

   b. 通訊埠：輸入 SMTP 伺服器的通訊埠號碼。

   c. 寄件者電子郵件信箱：輸入傳送事件通知的電子郵件信箱。

   d. 附件大小限制 (KB)：指定檔案附件大小上限（以 KB 為單位）。

3. 如果要使用延伸 SMTP (ESMTP)，請執行下列作業：

   a. 選取「啟動 ESMTP」。

   b. 指定使用者名稱和密碼。

   c. 從「驗證」下拉式清單中選取驗證方法。

4. 按一下「儲存」。

設定 SNMP Trap 設定

Apex Central 允許您傳送「簡易網路管理通訊協定」(SNMP) Trap 來向選取的收件者通知受管理產品偵測到的事件。

步驟

1. 移至「偵測 > 通知 > 通知方法」。

   會出現「通知方法」畫面。

2. 在「SNMP Trap 設定」區段中，指定下列項目：

   a. 社群名稱：輸入 SNMP 社群名稱。

b. 伺服器 IP 位址：輸入 SNMP 伺服器的 IPv4 或 IPv6 位址。

3. 按一下「儲存」。

設定 Syslog 設定

Apex Central 允許您傳送 Syslog 訊息來向選取的收件者通知受管理產品偵測到的事件。

您也可以將 Syslog 訊息直接傳輸至受支援的協力廠商產品。

步驟

1. 移至「偵測 > 通知 > 通知方法」。

   會出現「通知方法」畫面。

2. 在「Syslog 設定」區段中，指定下列項目：

   a. 伺服器 IP 位址：輸入 Syslog 伺服器的 IPv4 或 IPv6 位址。

   b. 通訊埠：Syslog 伺服器的通訊埠號碼。

   c. 設備：選取設備代碼。

   注意

   請使用新增圖示 (+) 新增多個 Syslog 伺服器。

3. 按一下「儲存」。

設定觸發應用程式設定

Apex Central 允許您使用內部或產業標準應用程式，來向選取的收件者通知受管理產品偵測到的事件。

例如，如果您的組織使用會執行 `net send` 指令的批次檔，則您可以使用「通知方法設定」畫面來提供具有必要權限之使用者帳號的認證。

重要

將觸發應用程式檔案儲存在 Apex Central 伺服器上的下列位置：

```
<Apex Central 安裝目錄>\Application\
```

步驟

1. 移至「偵測 > 通知 > 通知方法」。

   會出現「通知方法」畫面。

2. 在「觸發應用程式設定」區段中，選取「使用指定的使用者來觸發應用程式」。

3. 輸入具有觸發應用程式所需權限之帳號的使用者名稱和密碼。

4. 按一下「儲存」。

聯絡人群組

「聯絡人群組」畫面提供所有先前定義的聯絡人群組清單，可在指定報告和事件通知收件者時使用這份清單。您可以使用 Apex Central 聯絡人群組來傳送通知或報告給同一個群組中的所有收件者，而不需要逐一選取使用者帳號。

下表列出「聯絡人群組」畫面上提供的工作。

工作	說明
新增聯絡人群組	按一下「新增」可建立新的聯絡人群組。 如需詳細資訊，請參閱新增聯絡人群組 第 16-7 頁。

工作	說明
移除現有的聯絡人群組	選取現有的聯絡人群組，然後按一下「移除」。 警告! 刪除聯絡人群組會影響所有使用該群組的報告或通知。
編輯現有的聯絡人群組	按一下現有聯絡人群組的「名稱」，即可編輯收件者。 如需詳細資訊，請參閱編輯聯絡人群組 第 16-8 頁。

新增聯絡人群組

使用「新增群組」畫面可針對報告和事件通知建立新的聯絡人群組。

步驟

1. 移至「偵測 > 通知 > 聯絡人群組」

   會出現「聯絡人群組」畫面。

2. 請點選「新增」。

   會出現「新增群組」畫面。

3. 輸入聯絡人群組的名稱。

4. 指定聯絡人群組的收件者。

   - 在「可用的使用者帳號」清單中選取使用者帳號，然後按一下「>」。

     選取的使用者帳號會出現在「選取的使用者帳號」清單中。

     注意
     您也可以從整合式 Active Directory 結構中新增使用者和群組。
     如需詳細資訊，請參閱 Active Directory 整合 第 6-2 頁。

- 在「其他收件者」欄位中，輸入電子郵件信箱，然後按 Enter 鍵。

  最近新增的電子郵件信箱會顯示在「其他收件者」欄位下方。

  注意

  您一次只能新增一個電子郵件信箱。

5. 按一下「儲存」。

編輯聯絡人群組

使用「編輯群組」畫面可針對報告和事件通知建立新的聯絡人群組。

注意

您無法編輯現有聯絡人群組的「名稱」。

步驟

1. 移至「偵測 > 通知 > 聯絡人群組」

   會出現「聯絡人群組」畫面。

2. 按一下您要編輯的聯絡人群組的「名稱」。

   會出現「編輯群組」畫面。

3. 指定聯絡人群組的收件者。

   - 在「可用的使用者帳號」清單中選取使用者帳號，然後按一下「>」。

     選取的使用者帳號會出現在「選取的使用者帳號」清單中。

     注意

     您也可以從整合式 Active Directory 結構中新增使用者和群組。

     如需詳細資訊，請參閱 Active Directory 整合 第 6-2 頁。

- 在「其他收件者」欄位中，輸入電子郵件信箱，然後按 Enter 鍵。

  最近新增的電子郵件信箱會顯示在「其他收件者」欄位下方。

  注意

  您一次只能新增一個電子郵件信箱。

4. 按一下「儲存」。

進階安全威脅活動事件

使用「事件通知」畫面來啟動並設定您網路上偵測到的進階安全威脅活動通知。

攻擊發現偵測

設定下列事件通知，以在攻擊發現引擎偵測到進階安全威脅時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「進階安全威脅活動」。

   會出現事件清單。

3. 在「事件」欄中，按一下「攻擊發現偵測」。

   會出現「攻擊發現偵測」畫面。

4. 指定下列通知設定。

設定	說明
偵測類型	選取觸發事件通知的偵測風險等級。
期間	指定時間範圍。

5. 選取通知的收件者。
   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。
   b. 按一下 >。
      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。
6. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱攻擊發現 Token 變數 第 C-5 頁。

7. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
8. 按一下「儲存」。

行為監控違規

設定下列事件通知，以在偵測到「行為監控」違規時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。
   會出現「事件通知」畫面。
2. 按一下「進階安全威脅活動」。
   會出現事件清單。

3. 在「事件」欄中，按一下「行為監控違規」。

   會出現「行為監控違規」畫面。

4. 指定下列通知設定。

設定	說明
為每個偵測觸發警訊	選取以傳送每個偵測的事件通知。
指定套用於單一端點的警訊門檻值	選取以傳送僅符合指定條件之偵測的事件通知。 • 偵測：指定偵測數目 • 期間：指定以小時為單位的時間範圍

5. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

6. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱進階安全威脅活動 Token 變數 第 C-2 頁。

7. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。

8. 按一下「儲存」。

C&C 回呼警訊

設定下列事件通知，以在偵測到端點與已知 C&C 回呼位址之間的通訊時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「進階安全威脅活動」。

   會出現事件清單。

3. 在「事件」欄中，按一下「C&C 回呼警訊」。

   會出現「C&C 回呼警訊」畫面。

4. 指定下列通知設定。

設定	說明
C&C 清單來源	選取一或多個 C&C 清單來源。

5. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

6. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和 C&C 回呼 Token 變數 第 C-6 頁。
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和 C&C 回呼 Token 變數 第 C-6 頁。
Syslog	Apex Central 可以將 Syslog 導向至支援的協力廠商產品，包括 Cisco Security Monitoring, Analysis and Response (MARS)。

7. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
8. 按一下「儲存」。

C&C 回呼病毒爆發警訊

設定下列事件通知，以在偵測到多個端點與已知 C&C 回呼位址之間的通訊時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「進階安全威脅活動」。

   會出現事件清單。

3. 在「事件」欄中，按一下「C&C 回呼病毒爆發警訊」。

   會出現「C&C 回呼病毒爆發警訊」畫面。

4. 指定下列通知設定。

設定	說明
C&C 清單來源	選取一或多個 C&C 清單來源。
回呼嘗試次數	指定回呼嘗試次數。
遭到入侵的主機	指定遭到入侵的主機數目。
期間	指定時間範圍。

5. 選取通知的收件者。
   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。
   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。
6. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和 C&C 回呼 Token 變數 第 C-6 頁。

7. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
8. 按一下「儲存」。

關聯的事件偵測

設定下列事件通知，以在偵測到關聯的事件時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

會出現「事件通知」畫面。

2. 按一下「進階安全威脅活動」。

   會出現事件清單。

3. 在「事件」欄中，按一下「關聯的事件偵測」。

   會出現「關聯的事件偵測」畫面。

4. 指定下列通知設定。

設定	說明
附加 CSV 格式的記錄檔	選取以將內含有關偵測之記錄檔資料的 *.csv 檔案傳送給事件通知收件者。

5. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

6. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱進階安全威脅活動 Token 變數 第 C-2 頁。 **注意** 由於系統會從多個主機彙整資料，所以 `%hostIP%` 和 `%group%` Token 變數不適用於電子郵件通知。

7. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。

8. 按一下「儲存」。

內含進階安全威脅的電子郵件訊息

設定下列事件通知，以便在偵測到內含進階安全威脅的電子郵件訊息時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「進階安全威脅活動」。

   會出現事件清單。

3. 在「事件」欄中，按一下「內含進階安全威脅的電子郵件訊息」。

   會出現「內含進階安全威脅的電子郵件訊息」畫面。

4. 指定下列通知設定。

設定	說明
偵測	輸入受管理產品偵測到的安全威脅數目。
期間	指定時間範圍。
偵測類型	選取觸發事件通知的偵測風險等級。

5. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

6. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁。

7. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
8. 按一下「儲存」。

高風險沙箱偵測數

設定下列事件通知，以在沙箱偵測到高度可疑物件時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「進階安全威脅活動」。

   會出現事件清單。

3. 在「事件」欄中，按一下「高風險沙箱偵測」。

   會出現「高風險沙箱偵測」畫面。

4. 指定下列通知設定。

設定	說明
為每個偵測觸發警訊	選取以傳送每個偵測的事件通知。

設定	說明
指定套用於單一端點的警訊門檻值	選取以傳送僅符合指定條件之偵測的事件通知。 • 偵測：指定偵測數目 • 期間：指定以小時為單位的時間範圍
附加 CSV 格式的記錄檔	選取以將內含有關偵測之記錄檔資料的 *.csv 檔案傳送給事件通知收件者。

5. 選取通知的收件者。
   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。
   b. 按一下 >。
      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。
6. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和進階安全威脅活動 Token 變數 第 C-2 頁。

7. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
8. 按一下「儲存」。

高風險主機偵測

設定下列事件通知，以在網路上偵測到高風險主機時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「進階安全威脅活動」。

   會出現事件清單。

3. 在「事件」欄中，按一下「高風險主機偵測」。

   會出現「高風險主機偵測」畫面。

4. 指定下列通知設定。

設定	說明
為每個偵測觸發警訊	選取以傳送每個偵測的事件通知。
指定套用於單一端點的警訊門檻值	選取以傳送僅符合指定條件之偵測的事件通知。 • 偵測：指定偵測數目 • 期間：指定以小時為單位的時間範圍
附加 CSV 格式的記錄檔	選取以將內含有關偵測之記錄檔資料的 *.csv 檔案傳送給事件通知收件者。

5. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

6. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和進階安全威脅活動 Token 變數 第 C-2 頁。

7. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
8. 按一下「儲存」。

已知目標式攻擊行為

設定下列事件通知，以在網路上偵測到已知的目標式攻擊行為時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。
2. 按一下「進階安全威脅活動」。

   會出現事件清單。
3. 在「事件」欄中，按一下「已知目標式攻擊行為」。

   會出現「已知目標式攻擊行為」畫面。
4. 指定下列通知設定。

設定	說明
為每個偵測觸發警訊	選取以傳送每個偵測的事件通知。
指定套用於單一端點的警訊門檻值	選取以傳送僅符合指定條件之偵測的事件通知。 • 偵測：指定偵測數目 • 期間：指定以小時為單位的時間範圍

設定	說明
附加 CSV 格式的記錄檔	選取以將內含有關偵測之記錄檔資料的 *.csv 檔案傳送給事件通知收件者。

5. 選取通知的收件者。
   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。
   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。
6. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和進階安全威脅活動 Token 變數 第 C-2 頁。

7. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
8. 按一下「儲存」。

潛在文件弱點攻擊偵測

設定下列事件通知，以在網路上偵測到內含潛在弱點攻擊程式碼的文件時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「進階安全威脅活動」。

   會出現事件清單。

3. 在「事件」欄中，按一下「潛在文件弱點攻擊偵測」。

   會出現「潛在文件弱點攻擊偵測」畫面。

4. 指定下列通知設定。

設定	說明
為每個偵測觸發警訊	選取以傳送每個偵測的事件通知。
指定套用於單一端點的警訊門檻值	選取以傳送僅符合指定條件之偵測的事件通知。 • 偵測：指定偵測數目 • 期間：指定以小時為單位的時間範圍
附加 CSV 格式的記錄檔	選取以將內含有關偵測之記錄檔資料的 *.csv 檔案傳送給事件通知收件者。

5. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

6. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和進階安全威脅活動 Token 變數 第 C-2 頁。

7. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。

8. 按一下「儲存」。

Machine Learning 偵測

設定下列事件通知，以在趨勢科技 Machine Learning 偵測到新興的未知安全威脅時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「進階安全威脅活動」。

   會出現事件清單。

3. 在「事件」欄中，按一下「Machine Learning 偵測」。

   隨即顯示「Machine Learning 偵測」畫面。

4. 指定下列通知設定。

設定	說明
為每個偵測觸發警訊	選取以傳送每個偵測的事件通知。
指定套用於單一端點的警訊門檻值	選取以傳送僅符合指定條件之偵測的事件通知。 • 偵測：指定偵測數目 • 期間：指定以小時為單位的時間範圍

5. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

6. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱進階安全威脅活動 Token 變數 第 C-2 頁。

7. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
8. 按一下「儲存」。

Rootkit 或駭客工具偵測

設定下列事件通知，以在網路上偵測到 Rootkit 或駭客工具時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「進階安全威脅活動」。

   會出現事件清單。

3. 在「事件」欄中，按一下「Rootkit 或駭客工具偵測」。

   會出現「Rootkit 或駭客工具偵測」畫面。

4. 指定下列通知設定。

設定	說明
為每個偵測觸發警訊	選取以傳送每個偵測的事件通知。

設定	說明
指定套用於單一端點的警訊門檻值	選取以傳送僅符合指定條件之偵測的事件通知。 • 偵測：指定偵測數目 • 期間：指定以小時為單位的時間範圍
附加 CSV 格式的記錄檔	選取以將內含有關偵測之記錄檔資料的 *.csv 檔案傳送給事件通知收件者。

5. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

6. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和進階安全威脅活動 Token 變數 第 C-2 頁。

7. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。

8. 按一下「儲存」。

SHA-1 拒絕清單偵測

設定下列事件通知，以在網路上偵測到檔案內含的 SHA-1 值與「拒絕清單」中的物件相符時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「進階安全威脅活動」。

   會出現事件清單。

3. 在「事件」欄中，按一下「SHA-1 拒絕清單偵測」。

   會出現「SHA-1 拒絕清單偵測」畫面。

4. 指定下列通知設定。

設定	說明
為每個偵測觸發警訊	選取以傳送每個偵測的事件通知。
指定套用於單一端點的警訊門檻值	選取以傳送僅符合指定條件之偵測的事件通知。 • 偵測：指定偵測數目 • 期間：指定以小時為單位的時間範圍
附加 CSV 格式的記錄檔	選取以將內含有關偵測之記錄檔資料的 *.csv 檔案傳送給事件通知收件者。

5. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

6. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和進階安全威脅活動 Token 變數 第 C-2 頁。

7. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
8. 按一下「儲存」。

將有風險的收件者列入監視清單

設定下列事件通知，以在 Deep Discovery Email Inspector 偵測到有惡意或可疑電子郵件訊息或附件傳送給監視清單中的收件者時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「進階安全威脅活動」。

   會出現事件清單。

3. 在「事件」欄中，按一下「將有風險的收件者列入監視清單」。

   會出現「將有風險的收件者列入監視清單」畫面。

4. 指定下列通知設定。

條件	說明
電子郵件信箱監視清單	輸入要監控的電子郵件信箱。使用分號 (;) 分隔多個項目。
類型	選取觸發事件通知的偵測風險等級。

條件	說明
偵測	輸入受管理產品偵測到的安全威脅數目。
期間	指定偵測的時間範圍。

5. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

6. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和進階安全威脅活動 Token 變數 第 C-2 頁。

7. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。

8. 按一下「儲存」。

蠕蟲或檔案感染程式傳播偵測

設定下列事件通知，以在網路中偵測到蠕蟲或檔案感染程式特徵時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「進階安全威脅活動」。

   會出現事件清單。

3. 在「事件」欄中，按一下「蠕蟲或檔案感染程式傳播偵測」。

   會出現「蠕蟲或檔案感染程式傳播偵測」畫面。

4. 指定下列通知設定。

設定	說明
為每個偵測觸發警訊	選取以傳送每個偵測的事件通知。
指定警訊門檻值	選取以傳送僅符合指定條件之偵測的事件通知。 • 偵測：指定偵測數目 • 期間：指定以小時為單位的時間範圍
附加 CSV 格式的記錄檔	選取以將內含有關偵測之記錄檔資料的 *.csv 檔案傳送給事件通知收件者。

5. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

6. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和進階安全威脅活動 Token 變數 第 C-2 頁。

7. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。

8. 按一下「儲存」。

內容策略違規事件

使用「事件通知」畫面來啟動並設定您網路上偵測到的內容策略違規通知。

電子郵件政策違規

設定下列事件通知，以便在偵測到違反內容安全策略的電子郵件時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「內容違規策略」。

   會出現事件清單。

3. 在「事件」欄中，按一下「電子郵件政策違規」。

   會出現「電子郵件政策違規」畫面。

4. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

5. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和內容策略違規 Token 變數 第 C-8 頁。
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和內容策略違規 Token 變數 第 C-8 頁。
SNMP Trap	Apex Central 可將 SNMP Trap 通知儲存在 Management Information Bases (MIB) 中。如果要檢視 SNMP Trap 通知，請移至「通知 > 通知方法設定」，然後按一下「SNMP Trap 設定」下的「下載 MIB 檔案」。
觸發應用程式	將應用程式檔案的完整路徑和任何參數指定給指令。
Syslog	在 IP 網路中轉送記錄檔訊息的標準 Apex Central 可以將 Syslog 導向至支援的協力廠商產品，包括 Cisco Security Monitoring, Analysis and Response (MARS)。

6. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
7. 按一下「儲存」。

Web 存取安全違規

設定下列事件通知，以在由於違反安全策略而封鎖對 URL 的存取時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「內容違規策略」。

   會出現事件清單。

3. 在「事件」欄中，按一下「Web 存取安全違規」。

   會出現「Web 存取安全違規」畫面。

4. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

5. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和 Web 存取策略違規 Token 變數 第 C-14 頁。
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和 Web 存取策略違規 Token 變數 第 C-14 頁。
SNMP Trap	Apex Central 可將 SNMP Trap 通知儲存在 Management Information Bases (MIB) 中。如果要檢視 SNMP Trap 通知，請移至「通知 > 通知方法設定」，然後按一下「SNMP Trap 設定」下的「下載 MIB 檔案」。
觸發應用程式	將應用程式檔案的完整路徑和任何參數指定給指令。
Syslog	在 IP 網路中轉送記錄檔訊息的標準 Apex Central 可以將 Syslog 導向至支援的協力廠商產品，包括 Cisco Security Monitoring, Analysis and Response (MARS)。

6. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。

7. 按一下「儲存」。

資料外洩防護事件

使用「事件通知」畫面來啟動並設定您網路上偵測到的資料外洩防護事件通知。

事件詳細資料已更新

設定下列事件通知，以在事件詳細資料已更新時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「資料外洩防護」。

   會出現事件清單。

3. 在「事件」欄中，按一下「事件詳細資料已更新」。

   會出現「事件詳細資料已更新」畫面。

4. 指定通知事件詳細資料更新的條件：

條件	說明
事件詳細資料更新	選取事件詳細資料更新的類型。 • 已關閉 • 任何變更

條件	說明
依嚴重性層級過濾	選取下列一或多個風險等級。 • 高 • 中 • 低 • 資訊性 • 未定義

5. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和資料外洩防護 Token 變數 第 C-9 頁。

6. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
7. 按一下「儲存」。

預約事件摘要

設定下列事件通知，以將網路上發生 DLP 事件之摘要傳送給管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「資料外洩防護」。

   會出現事件清單。

3. 在「事件」欄中，按一下「預約事件摘要」。

   會出現「預約事件摘要」畫面。

4. 指定下列通知設定。

條件	說明
頻率	選取此選項會每日或每週接收通知。

附加事件詳細資料	選取此選項會將事件記錄附加到通知。
	• 選取 DLP 合規官會接收的內容：
	  • 來自所有受管理使用者的事件
	  • 僅來自直屬員工的事件
	注意
	DLP 事件檢閱者只接收來自直屬員工的事件
	• 選取記錄檔詳細資料的格式

5. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和資料外洩防護 Token 變數 第 C-9 頁。

6. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
7. 按一下「儲存」。

事件大幅增加

設定以下事件，以在整個預先定義的期間內，發生的 DLP 事件大幅增加時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「資料外洩防護」。

   會出現事件清單。

3. 在「事件」欄中，按一下「事件大幅增加」。

   會出現「事件大幅增加」畫面。

4. 指定下列通知設定。

設定	說明
每小時一次	指定每小時的事件數目。
每日一次	指定每日的事件數目。

5. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

6. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和資料外洩防護 Token 變數 第 C-9 頁。

7. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。

8. 按一下「儲存」。

由通道觸發的事件大幅增加

設定下列事件通知，以在整個預先定義的期間內，發生的由通道觸發的 DLP 事件大幅增加時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「資料外洩防護」。

   會出現事件清單。

3. 在「事件」欄中，按一下「由通道觸發的事件大幅增加」。

   會出現「由通道觸發的事件大幅增加」畫面。

4. 指定下列通知設定。

設定	說明
每小時一次	指定每小時的事件數目。
每日一次	指定每日的事件數目。

5. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

6. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和資料外洩防護 Token 變數 第 C-9 頁。

7. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
8. 按一下「儲存」。

由寄件者觸發的事件大幅增加

設定下列事件通知，以在整個預先定義的期間內，發生的由寄件者觸發的 DLP 事件大幅增加時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「資料外洩防護」。

   會出現事件清單。

3. 在「事件」欄中，按一下「由寄件者觸發的事件大幅增加」。

   會出現「由寄件者觸發的事件大幅增加」畫面。

4. 指定下列通知設定。

設定	說明
每小時一次	指定每小時的事件數目。
每日一次	指定每日的事件數目。

5. 選取通知的收件者。

a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

b. 按一下 >。

選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

6. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和資料外洩防護 Token 變數 第 C-9 頁。

7. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。

8. 按一下「儲存」。

由使用者觸發的事件大幅增加

設定下列事件通知，以在整個預先定義的期間內，發生的由使用者觸發的 DLP 事件大幅增加時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

會出現「事件通知」畫面。

2. 按一下「資料外洩防護」。

會出現事件清單。

3. 在「事件」欄中，按一下「由使用者觸發的事件大幅增加」。

會出現「由使用者觸發的事件大幅增加」畫面。

4. 指定下列通知設定。

設定	說明
每小時一次	指定每小時的事件數目。
每日一次	指定每日的事件數目。

5. 選取通知的收件者。
   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。
   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

6. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和資料外洩防護 Token 變數 第 C-9 頁。

7. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
8. 按一下「儲存」。

範本相符項目大幅增加

設定下列事件通知，以在整個預先定義的期間內，出現的 DLP 範本相符項目大幅增加時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「資料外洩防護」。

   會出現事件清單。

3. 在「事件」欄中，按一下「範本相符項目大幅增加」。

   會出現「範本相符項目大幅增加」畫面。

4. 指定下列通知設定。

設定	說明
每小時一次	指定每小時的事件數目。
每日一次	指定每日的事件數目。

5. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

6. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和資料外洩防護 Token 變數 第 C-9 頁。

7. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。

8. 按一下「儲存」。

已知的安全威脅活動事件

使用「事件通知」畫面來啟動並設定您網路上偵測到的已知安全威脅活動通知。

網路病毒警訊

設定下列事件通知，以在偵測到網路病毒時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「已知的安全威脅活動」。

   會出現事件清單。

3. 在「事件」欄中，按一下「網路病毒警訊」。

   會出現「網路病毒警訊」畫面。

4. 指定下列通知設定。

設定	說明
偵測	輸入受管理產品偵測到的安全威脅數目。
受影響的使用者/端點	指定受影響的使用者/端點數目。
期間	指定時間範圍。

5. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

6. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁、已知的安全威脅活動 Token 變數 第 C-11 頁和網路存取控制 Token 變數 第 C-13 頁。
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁、已知的安全威脅活動 Token 變數 第 C-11 頁和網路存取控制 Token 變數 第 C-13 頁。
SNMP Trap	Apex Central 可將 SNMP Trap 通知儲存在 Management Information Bases (MIB) 中。如果要檢視 SNMP Trap 通知，請移至「通知 > 通知方法設定」，然後按一下「SNMP Trap 設定」下的「下載 MIB 檔案」。
觸發應用程式	將應用程式檔案的完整路徑和任何參數指定給指令。
Syslog	Apex Central 可以將 Syslog 導向至支援的協力廠商產品，包括 Cisco Security Monitoring, Analysis and Response (MARS)。

7. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。

8. 按一下「儲存」。

特殊間諜程式/可能的資安威脅程式警訊

設定下列事件通知，以在偵測到受監控間諜程式/可能的資安威脅程式安全威脅清單中包含的間諜程式/可能的資安威脅程式時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「已知的安全威脅活動」。

   會出現事件清單。

3. 在「事件」欄中，按一下「特殊間諜程式/可能的資安威脅程式警訊」。

   會出現「特殊間諜程式/可能的資安威脅程式警訊」畫面。

4. 輸入要監控的間諜程式/可能的資安威脅程式名稱。

5. 指定下列通知設定。

設定	說明
期間	指定時間範圍。

6. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

7. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和已知的安全威脅活動 Token 變數 第 C-11 頁。

方法	說明
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和已知的安全威脅活動 Token 變數 第 C-11 頁。
觸發應用程式	將應用程式檔案的完整路徑和任何參數指定給指令。
Syslog	Apex Central 可以將 Syslog 導向至支援的協力廠商產品，包括 Cisco Security Monitoring, Analysis and Response (MARS)。

8. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
9. 按一下「儲存」。

特殊病毒警訊

設定下列事件通知，以在偵測到受監控病毒清單中包含的病毒時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。
2. 按一下「已知的安全威脅活動」。

   會出現事件清單。
3. 在「事件」欄中，按一下「特殊病毒警訊」。

   會出現「特殊病毒警訊」畫面。
4. 輸入要監控的病毒名稱。
5. 指定下列通知設定。

設定	說明
期間	指定時間範圍。

6. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

7. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁、已知的安全威脅活動 Token 變數 第 C-11 頁和網路存取控制 Token 變數 第 C-13 頁。
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁、已知的安全威脅活動 Token 變數 第 C-11 頁和網路存取控制 Token 變數 第 C-13 頁。
觸發應用程式	將應用程式檔案的完整路徑和任何參數指定給指令。
Syslog	Apex Central 可以將 Syslog 導向至支援的協力廠商產品，包括 Cisco Security Monitoring, Analysis and Response (MARS)。

8. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。

9. 按一下「儲存」。

發現間諜程式/可能的資安威脅程式 — 處理行動成功

設定下列事件通知，以在成功對偵測到的間諜程式/可能的資安威脅程式採取已設定的間諜程式/可能的資安威脅程式中毒處理行動時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「已知的安全威脅活動」。

   會出現事件清單。

3. 在「事件」欄中，按一下「發現間諜程式/可能的資安威脅程式 — 處理行動成功」。

   會出現「發現間諜程式/可能的資安威脅程式 — 處理行動成功」畫面。

4. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

5. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和已知的安全威脅活動 Token 變數 第 C-11 頁。

方法	說明
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和已知的安全威脅活動 Token 變數 第 C-11 頁。
SNMP Trap	Apex Central 可將 SNMP Trap 通知儲存在 Management Information Bases (MIB) 中。如果要檢視 SNMP Trap 通知，請移至「通知 > 通知方法設定」，然後按一下「SNMP Trap 設定」下的「下載 MIB 檔案」。
觸發應用程式	將應用程式檔案的完整路徑和任何參數指定給指令。
Syslog	Apex Central 可以將 Syslog 導向至支援的協力廠商產品，包括 Cisco Security Monitoring, Analysis and Response (MARS)。

6. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
7. 按一下「儲存」。

發現間諜程式/可能的資安威脅程式 – 需要進一步處理行動

設定下列事件通知，以在偵測到的間諜程式/可能的資安威脅程式需要採取進一步處理行動時通知管理員。

設定下列事件通知，以在未成功對偵測到的間諜程式/可能的資安威脅程式採取已設定的間諜程式/可能的資安威脅程式中毒處理行動時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「已知的安全威脅活動」。

   會出現事件清單。

3. 在「事件」欄中，按一下「發現間諜程式/可能的資安威脅程式 — 需要進一步處理行動」。

   會出現「發現間諜程式/可能的資安威脅程式 — 需要進一步處理行動」畫面。

4. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

5. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和已知的安全威脅活動 Token 變數 第 C-11 頁。
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和已知的安全威脅活動 Token 變數 第 C-11 頁。
SNMP Trap	Apex Central 可將 SNMP Trap 通知儲存在 Management Information Bases (MIB) 中。如果要檢視 SNMP Trap 通知，請移至「通知 > 通知方法設定」，然後按一下「SNMP Trap 設定」下的「下載 MIB 檔案」。
觸發應用程式	將應用程式檔案的完整路徑和任何參數指定給指令。
Syslog	Apex Central 可以將 Syslog 導向至支援的協力廠商產品，包括 Cisco Security Monitoring, Analysis and Response (MARS)。

6. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。

7. 按一下「儲存」。

發現病毒 — 第一個處理行動成功

設定下列事件通知，以在成功對偵測到的病毒採取第一個中毒處理行動時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「已知的安全威脅活動」。

   會出現事件清單。

3. 在「事件」欄中，按一下「發現病毒 — 第一個處理行動成功」。

   會出現「發現病毒 — 第一個處理行動成功」畫面。

4. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

5. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和已知的安全威脅活動 Token 變數 第 C-11 頁。
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和已知的安全威脅活動 Token 變數 第 C-11 頁。

方法	說明
SNMP Trap	Apex Central 可將 SNMP Trap 通知儲存在 Management Information Bases (MIB) 中。如果要檢視 SNMP Trap 通知，請移至「通知 > 通知方法設定」，然後按一下「SNMP Trap 設定」下的「下載 MIB 檔案」。
觸發應用程式	將應用程式檔案的完整路徑和任何參數指定給指令。
Syslog	Apex Central 可以將 Syslog 導向至支援的協力廠商產品，包括 Cisco Security Monitoring, Analysis and Response (MARS)。

6. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
7. 按一下「儲存」。

發現病毒 — 第一個處理行動未成功，第二個處理行動不可用

設定下列事件通知，以在針對偵測到的病毒所採取的第一個中毒處理行動未成功，而第二個處理行動不可用時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「已知的安全威脅活動」。

   會出現事件清單。

3. 在「事件」欄中，按一下「發現病毒 — 第一個處理行動未成功，第二個處理行動不可用」。

   會出現「發現病毒 — 第一個處理行動未成功，第二個處理行動不可用」畫面。

4. 選取通知的收件者。

a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

b. 按一下 >。

選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

5. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和已知的安全威脅活動 Token 變數 第 C-11 頁。
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和已知的安全威脅活動 Token 變數 第 C-11 頁。
SNMP Trap	Apex Central 可將 SNMP Trap 通知儲存在 Management Information Bases (MIB) 中。如果要檢視 SNMP Trap 通知，請移至「通知 > 通知方法設定」，然後按一下「SNMP Trap 設定」下的「下載 MIB 檔案」。
觸發應用程式	將應用程式檔案的完整路徑和任何參數指定給指令。
Syslog	Apex Central 可以將 Syslog 導向至支援的協力廠商產品，包括 Cisco Security Monitoring, Analysis and Response (MARS)。

6. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。

7. 按一下「儲存」。

發現病毒 — 第一個和第二個處理行動未成功

設定下列事件通知，以在針對偵測到的病毒所採取的第一個和第二個中毒處理行動都未成功時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「已知的安全威脅活動」。

   會出現事件清單。

3. 在「事件」欄中，按一下「發現病毒 — 第一個和第二個處理行動未成功」。

   會出現「發現病毒 — 第一個和第二個處理行動未成功」畫面。

4. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

5. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和已知的安全威脅活動 Token 變數 第 C-11 頁。
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和已知的安全威脅活動 Token 變數 第 C-11 頁。
SNMP Trap	Apex Central 可將 SNMP Trap 通知儲存在 Management Information Bases (MIB) 中。如果要檢視 SNMP Trap 通知，請移至「通知 > 通知方法設定」，然後按一下「SNMP Trap 設定」下的「下載 MIB 檔案」。

方法	說明
觸發應用程式	將應用程式檔案的完整路徑和任何參數指定給指令。
Syslog	Apex Central 可以將 Syslog 導向至支援的協力廠商產品，包括 Cisco Security Monitoring, Analysis and Response (MARS)。

6. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
7. 按一下「儲存」。

發現病毒 — 第二個處理行動成功

設定下列事件通知，以在成功對偵測到的病毒採取第二個中毒處理行動時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「已知的安全威脅活動」。

   會出現事件清單。

3. 在「事件」欄中，按一下「發現病毒 — 第二個處理行動成功」。

   會出現「發現病毒 — 第二個處理行動成功」畫面。

4. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

5. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和已知的安全威脅活動 Token 變數 第 C-11 頁。
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和已知的安全威脅活動 Token 變數 第 C-11 頁。
SNMP Trap	Apex Central 可將 SNMP Trap 通知儲存在 Management Information Bases (MIB) 中。如果要檢視 SNMP Trap 通知，請移至「通知 > 通知方法設定」，然後按一下「SNMP Trap 設定」下的「下載 MIB 檔案」。
觸發應用程式	將應用程式檔案的完整路徑和任何參數指定給指令。
Syslog	Apex Central 可以將 Syslog 導向至支援的協力廠商產品，包括 Cisco Security Monitoring, Analysis and Response (MARS)。

6. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
7. 按一下「儲存」。

病毒爆發警訊

設定下列事件通知，以在偵測到病毒爆發時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。
2. 按一下「已知的安全威脅活動」。

   會出現事件清單。

3. 在「事件」欄中，按一下「病毒爆發警訊」。

   會出現「病毒爆發警訊」畫面。

4. 指定下列通知設定。

設定	說明
偵測	輸入受管理產品偵測到的安全威脅數目。
受影響的使用者/端點	指定受影響的使用者/端點數目。
期間	指定時間範圍。

5. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

6. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和已知的安全威脅活動 Token 變數 第 C-11 頁。
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和已知的安全威脅活動 Token 變數 第 C-11 頁。
SNMP Trap	Apex Central 可將 SNMP Trap 通知儲存在 Management Information Bases (MIB) 中。如果要檢視 SNMP Trap 通知，請移至「通知 > 通知方法設定」，然後按一下「SNMP Trap 設定」下的「下載 MIB 檔案」。
觸發應用程式	將應用程式檔案的完整路徑和任何參數指定給指令。

方法	說明
Syslog	Apex Central 可以將 Syslog 導向至支援的協力廠商產品，包括 Cisco Security Monitoring, Analysis and Response (MARS)。

7. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
8. 按一下「儲存」。

網路存取控制事件

使用「事件通知」畫面來啟動並設定您網路上偵測到的網路病毒牆策略違規或潛在弱點攻擊通知。

網路病毒牆策略違規

設定下列事件通知，以在偵測到網路病毒牆策略違規時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「網路存取控制」。

   會出現事件清單。

3. 在「事件」欄中，按一下「網路病毒牆策略違規」。

   會出現網路病毒牆策略違規畫面。

4. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

b. 按一下 >。

選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

5. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁。
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁。
SNMP Trap	Apex Central 可將 SNMP Trap 通知儲存在 Management Information Bases (MIB) 中。如果要檢視 SNMP Trap 通知，請移至「通知 > 通知方法設定」，然後按一下「SNMP Trap 設定」下的「下載 MIB 檔案」。
觸發應用程式	將應用程式檔案的完整路徑和任何參數指定給指令。

6. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
7. 按一下「儲存」。

潛在弱點攻擊

設定下列事件通知，以在網路病毒牆偵測到潛在弱點攻擊時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「網路存取控制」。

會出現事件清單。

3. 在「事件」欄中，按一下「潛在弱點攻擊」。

   會出現「潛在弱點攻擊」畫面。

4. 指定下列通知設定。

設定	說明
偵測	指定網路病毒牆偵測到的潛在弱點攻擊量。
期間	指定時間範圍。
報告者	指定回報潛在弱點攻擊的網路病毒牆裝置數目。

5. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

6. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和網路存取控制 Token 變數 第 C-13 頁。
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁和網路存取控制 Token 變數 第 C-13 頁。
SNMP Trap	Apex Central 可將 SNMP Trap 通知儲存在 Management Information Bases (MIB) 中。如果要檢視 SNMP Trap 通知，請移至「通知 > 通知方法設定」，然後按一下「SNMP Trap 設定」下的「下載 MIB 檔案」。

方法	說明
觸發應用程式	將應用程式檔案的完整路徑和任何參數指定給指令。
Syslog	Apex Central 可以將 Syslog 導向至支援的協力廠商產品，包括 Cisco Security Monitoring, Analysis and Response (MARS)。

7. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
8. 按一下「儲存」。

不尋常的產品行為事件

使用「事件通知」畫面來啟動並設定您網路上偵測到的不尋常的產品行為通知。

無法連接受管理產品

設定下列事件通知，以在 Apex Central 與受管理的產品伺服器之間發生連線錯誤時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。
2. 按一下「不尋常的產品行為」。

   會出現事件清單。
3. 在「事件」欄中，按一下「無法連接受管理產品」。

   會出現「無法連接受管理產品」畫面。
4. 選取通知的收件者。

a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

b. 按一下 >。

選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

5. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁。

6. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。

7. 按一下「儲存」。

產品服務已啟動

設定下列事件通知，以在產品服務啟動時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

會出現「事件通知」畫面。

2. 按一下「不尋常的產品行為」。

會出現事件清單。

3. 在「事件」欄中，按一下「產品服務已啟動」。

會出現「產品服務已啟動」畫面。

4. 選取通知的收件者。

a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

b. 按一下 >。

選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

5. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁。
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁。
SNMP Trap	Apex Central 可將 SNMP Trap 通知儲存在 Management Information Bases (MIB) 中。如果要檢視 SNMP Trap 通知，請移至「通知 > 通知方法設定」，然後按一下「SNMP Trap 設定」下的「下載 MIB 檔案」。
觸發應用程式	將應用程式檔案的完整路徑和任何參數指定給指令。
Syslog	Apex Central 可以將 Syslog 導向至支援的協力廠商產品，包括 Cisco Security Monitoring, Analysis and Response (MARS)。

6. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。

7. 按一下「儲存」。

產品服務已停止

設定下列事件通知，以在產品服務停止時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 按一下「不尋常的產品行為」。

   會出現事件清單。

3. 在「事件」欄中，按一下「產品服務已停止」。

   會出現「產品服務已停止」畫面。

4. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

5. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁。
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁。
SNMP Trap	Apex Central 可將 SNMP Trap 通知儲存在 Management Information Bases (MIB) 中。如果要檢視 SNMP Trap 通知，請移至「通知 > 通知方法設定」，然後按一下「SNMP Trap 設定」下的「下載 MIB 檔案」。
觸發應用程式	將應用程式檔案的完整路徑和任何參數指定給指令。

方法	說明
Syslog	Apex Central 可以將 Syslog 導向至支援的協力廠商產品，包括 Cisco Security Monitoring, Analysis and Response (MARS)。

6. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
7. 按一下「儲存」。

即時掃瞄已關閉

設定下列事件通知，以在「即時掃瞄」關閉時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。
2. 按一下「不尋常的產品行為」。

   會出現事件清單。
3. 在「事件」欄中，按一下「即時掃瞄已關閉」。

   會出現「即時掃瞄已關閉」畫面。
4. 選取通知的收件者。
   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。
   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。
5. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁。
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁。
SNMP Trap	Apex Central 可將 SNMP Trap 通知儲存在 Management Information Bases (MIB) 中。如果要檢視 SNMP Trap 通知，請移至「通知 > 通知方法設定」，然後按一下「SNMP Trap 設定」下的「下載 MIB 檔案」。
觸發應用程式	將應用程式檔案的完整路徑和任何參數指定給指令。
Syslog	Apex Central 可以將 Syslog 導向至支援的協力廠商產品，包括 Cisco Security Monitoring, Analysis and Response (MARS)。

6. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
7. 按一下「儲存」。

即時掃瞄已啟動

設定下列事件通知，以在「即時掃瞄」啟動時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。
2. 按一下「不尋常的產品行為」。

   會出現事件清單。
3. 在「事件」欄中，按一下「即時掃瞄已啟動」。

會出現「即時掃瞄已啟動」畫面。

4. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

5. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁。
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁。
SNMP Trap	Apex Central 可將 SNMP Trap 通知儲存在 Management Information Bases (MIB) 中。如果要檢視 SNMP Trap 通知，請移至「通知 > 通知方法設定」，然後按一下「SNMP Trap 設定」下的「下載 MIB 檔案」。
觸發應用程式	將應用程式檔案的完整路徑和任何參數指定給指令。
Syslog	Apex Central 可以將 Syslog 導向至支援的協力廠商產品，包括 Cisco Security Monitoring, Analysis and Response (MARS)。

6. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。

7. 按一下「儲存」。

更新

使用「事件通知」畫面來啟動並設定元件更新狀態通知。

垃圾郵件防護規則更新成功

設定下列事件通知，以在垃圾郵件防護規則更新成功時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 請點選「更新」。

   會出現事件清單。

3. 在「事件」欄中，按一下「垃圾郵件防護規則更新成功」。

   會出現「垃圾郵件防護規則成功更新」畫面。

4. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

5. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁。

方法	說明
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁。
SNMP Trap	Apex Central 可將 SNMP Trap 通知儲存在 Management Information Bases (MIB) 中。如果要檢視 SNMP Trap 通知，請移至「通知 > 通知方法設定」，然後按一下「SNMP Trap 設定」下的「下載 MIB 檔案」。
觸發應用程式	將應用程式檔案的完整路徑和任何參數指定給指令。
Syslog	Apex Central 可以將 Syslog 導向至支援的協力廠商產品，包括 Cisco Security Monitoring, Analysis and Response (MARS)。

6. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
7. 按一下「儲存」。

垃圾郵件防護規則更新未成功

設定下列事件通知，以在垃圾郵件防護規則更新未成功時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。
2. 請點選「更新」。

   會出現事件清單。
3. 在「事件」欄中，按一下「垃圾郵件防護規則更新未成功」。

   會出現「垃圾郵件防護規則更新未成功」畫面。
4. 選取通知的收件者。

a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

b. 按一下 >。

選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

5. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁。
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁。
SNMP Trap	Apex Central 可將 SNMP Trap 通知儲存在 Management Information Bases (MIB) 中。如果要檢視 SNMP Trap 通知，請移至「通知 > 通知方法設定」，然後按一下「SNMP Trap 設定」下的「下載 MIB 檔案」。
觸發應用程式	將應用程式檔案的完整路徑和任何參數指定給指令。
Syslog	Apex Central 可以將 Syslog 導向至支援的協力廠商產品，包括 Cisco Security Monitoring, Analysis and Response (MARS)。

6. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。

7. 按一下「儲存」。

特徵碼檔案/清除範本更新成功

設定下列事件通知，以在特徵碼檔案或清除範本更新成功時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 請點選「更新」。

   會出現事件清單。

3. 在「事件」欄中，按一下「特徵碼檔案/清除範本更新成功」。

   會出現「特徵碼檔案/清除範本更新成功」畫面。

4. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

5. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁。
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁。
SNMP Trap	Apex Central 可將 SNMP Trap 通知儲存在 Management Information Bases (MIB) 中。如果要檢視 SNMP Trap 通知，請移至「通知 > 通知方法設定」，然後按一下「SNMP Trap 設定」下的「下載 MIB 檔案」。
觸發應用程式	將應用程式檔案的完整路徑和任何參數指定給指令。

方法	說明
Syslog	Apex Central 可以將 Syslog 導向至支援的協力廠商產品，包括 Cisco Security Monitoring, Analysis and Response (MARS)。

6. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
7. 按一下「儲存」。

特徵碼檔案/清除範本更新未成功

設定下列事件通知，以在特徵碼檔案或清除範本更新未成功時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 請點選「更新」。

   會出現事件清單。

3. 在「事件」欄中，按一下「特徵碼檔案/清除範本更新未成功」。

   會出現「特徵碼檔案/清除範本更新未成功」畫面。

4. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

5. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁。
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁。
SNMP Trap	Apex Central 可將 SNMP Trap 通知儲存在 Management Information Bases (MIB) 中。如果要檢視 SNMP Trap 通知，請移至「通知 > 通知方法設定」，然後按一下「SNMP Trap 設定」下的「下載 MIB 檔案」。
觸發應用程式	將應用程式檔案的完整路徑和任何參數指定給指令。
Syslog	Apex Central 可以將 Syslog 導向至支援的協力廠商產品，包括 Cisco Security Monitoring, Analysis and Response (MARS)。

6. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
7. 按一下「儲存」。

掃瞄引擎更新成功

設定下列事件通知，以在掃瞄引擎更新成功時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。
2. 請點選「更新」。

   會出現事件清單。
3. 在「事件」欄中，按一下「掃瞄引擎更新成功」。

會出現「掃瞄引擎更新成功」畫面。

4. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

5. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁。
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁。
SNMP Trap	Apex Central 可將 SNMP Trap 通知儲存在 Management Information Bases (MIB) 中。如果要檢視 SNMP Trap 通知，請移至「通知 > 通知方法設定」，然後按一下「SNMP Trap 設定」下的「下載 MIB 檔案」。
觸發應用程式	將應用程式檔案的完整路徑和任何參數指定給指令。
Syslog	Apex Central 可以將 Syslog 導向至支援的協力廠商產品，包括 Cisco Security Monitoring, Analysis and Response (MARS)。

6. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。

7. 按一下「儲存」。

掃瞄引擎更新未成功

設定下列事件通知，以在掃瞄引擎更新未成功時通知管理員。

步驟

1. 移至「偵測 > 通知 > 事件通知」。

   會出現「事件通知」畫面。

2. 請點選「更新」。

   會出現事件清單。

3. 在「事件」欄中，按一下「掃瞄引擎更新未成功」。

   會出現「掃瞄引擎更新未成功」畫面。

4. 選取通知的收件者。

   a. 從「可用的使用者和群組」清單中，選取聯絡人群組或使用者帳號。

   b. 按一下 >。

      選取的聯絡人群組或使用者帳號會出現在「選取的使用者和群組」清單中。

5. 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	如果要自訂電子郵件通知範本，請使用支援的 Token 變數或修改「主旨」和「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁。
Windows 事件記錄檔	如果要自訂通知範本，請使用支援的 Token 變數或修改「訊息」欄位中的文字。 如需詳細資訊，請參閱標準 Token 變數 第 C-2 頁。
SNMP Trap	Apex Central 可將 SNMP Trap 通知儲存在 Management Information Bases (MIB) 中。如果要檢視 SNMP Trap 通知，請移至「通知 > 通知方法設定」，然後按一下「SNMP Trap 設定」下的「下載 MIB 檔案」。
觸發應用程式	將應用程式檔案的完整路徑和任何參數指定給指令。

方法	說明
Syslog	Apex Central 可以將 Syslog 導向至支援的協力廠商產品，包括 Cisco Security Monitoring, Analysis and Response (MARS)。

6. 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
7. 按一下「儲存」。

第 17 章

報告

本節討論如何使用從所有受管理產品（已向 Apex Central 註冊）收集的資料，建立報告。

包含下列主題：

- 報告總覽 第 17-2 頁
- 自訂範本 第 17-2 頁
- 一次性報告 第 17-18 頁
- 預約報告 第 17-22 頁
- 設定報告維護 第 17-31 頁
- 檢視我的報告 第 17-32 頁

報告總覽

Apex Central 可讓您產生、下載及傳送整合所有已註冊受管理產品之資料的報告，而不需要登入多個產品主控台。

您可以使用 Apex Central 執行下列作業：

- 在需要時產生一次性報告。
- 新增預約報告，以根據使用者定義的預約時程，自動產生並傳送報告給指定收件者。
- 從資料檢視建立自訂報告範本，或使用預先定義的自訂範本和靜態範本。
- 針對已指派自訂標籤 (Tags)、過濾器或重要標籤的端點產生自訂報告。

自訂範本

「自訂範本」畫面提供所有可用自訂報告範本的清單。Apex Central 提供一些預先定義的自訂範本供您使用。您可以複製預先定義的範本來加以編輯，也可以透過選取並設定特定報告項目來建立新範本。

注意

自訂範本會使用與特定 Apex Central 記錄檔對應的資料檢視來定義報告資料的範圍。

如需詳細資訊，請參閱下列主題：

- 記錄檔名稱與資料檢視 第 15-6 頁
- 資料檢視 第 B-1 頁

下表列出「自訂範本」畫面上的可用工作。

工作	說明
新增自訂範本	按一下「新增」以建立新的自訂範本。 如需詳細資訊，請參閱新增或編輯自訂範本 第 17-3 頁。
刪除自訂範本	選取現有的範本，然後按一下「刪除」。
編輯自訂範本	按一下要編輯的現有範本的「名稱」。 如需詳細資訊，請參閱新增或編輯自訂範本 第 17-3 頁。
複製自訂範本	選取現有的範本，然後按一下「複製」。Apex Central 會使用下列命名方式，新增範本到清單中： <原始範本名稱> 的複本 如需詳細資訊，請參閱新增或編輯自訂範本 第 17-3 頁。
匯入自訂範本	按一下「匯入」，可將格式正確的 XML 報告範本匯入到 Apex Central。
匯出自訂範本	選取現有的範本，然後按一下「匯出」。Apex Central 會以 XML 格式匯出範本。

新增或編輯自訂範本

您可以建立自訂範本，以便使用多種格式來產生公司專用的報告。

步驟

1. 移至「偵測 > 報告 > 自訂範本」。

   會出現「自訂範本」畫面。

2. 新增、編輯或複製範本。

   - 如果要新增範本，請按一下「新增」。

     會出現「新增報告範本」畫面。

   - 如果要編輯現有範本，請按一下範本的「名稱」。

     會出現「編輯報告範本」畫面。

- 如果要製作現有範本的複本來做為新範本的基礎，請執行下列作業：

  a. 選取您要使用之範本「名稱」左側的核取方塊。

  b. 按一下「複製」。

     Apex Central 會使用下列命名方式，新增範本到清單中：

     <原始範本名稱> 的複本

  c. 按一下最近新增的範本「名稱」。

     會出現「編輯報告範本」畫面。

3. 指定範本的唯一「名稱」。
4. （選用）提供新範本的「說明」。
5. 使用「作用中面板」，將報告項目拖放到可用的「列」中，以設計報告的區段配置。

重要

每一列僅支援 3 個報告項目。

秘訣

如果未顯示「作用中面板」，請按一下「範本內容」旁的「顯示作用中面板」按鈕。

表 17-1. 報告項目

範本項目	說明
靜態文字	提供使用者定義內容的容器 注意 靜態文字內容最多可包含 4096 個字元。 如需詳細資訊，請參閱設定靜態文字報告項目 第 17-6 頁。

範本項目	說明
長條圖	插入可自訂的長條圖物件 如需詳細資訊，請參閱設定長條圖報告項目 第 17-7 頁。
折線圖	插入可自訂的折線圖物件 如需詳細資訊，請參閱設定折線圖報告項目 第 17-9 頁。
圓餅圖	插入可自訂的圓餅圖物件 如需詳細資訊，請參閱設定圓餅圖報告項目 第 17-12 頁。
動態資料表	插入可自訂的動態資料表/樞紐分析表物件 動態資料表中的資訊會在水平或垂直方向比較正好兩個資料欄位。 如需詳細資訊，請參閱設定動態資料表報告項目 第 17-14 頁。
格線資料表	插入可自訂的資料表物件 格線資料表中的資訊會與記錄查詢中顯示的資訊相同。 如需詳細資訊，請參閱設定格線資料表報告項目 第 17-17 頁。

6. 使用「在上方插入分頁」、「在上方插入列」、「在下方插入列」和「刪除此列」等按鈕，在您的報告中組織列和頁面的配置。

注意

新增至同一列的報告項目，會以您將項目新增到範本的順序並排顯示。這可讓您在同一行顯示多個圖表。如果您想在同一個頁面中的不同行顯示多個圖表，請插入新列，但不插入分頁。

圖 17-1. 可將靜態文字顯示在長條圖上方的自訂報告範本設定

7. 按一下「儲存」。

設定靜態文字報告項目

此工作假設您已新增「靜態文字」報告項目到自訂報告範本列。

如需詳細資訊，請參閱新增或編輯自訂範本 第 17-3 頁。

步驟

1. 在「靜態文字」報告項目中，按一下「編輯」。

   會出現「編輯靜態文字」畫面。

2. 在「名稱」欄位中，指定文字方塊項目的標題。
3. 在「訊息」欄位中，指定要在訊息內文中顯示的任何描述性文字。

   注意

   靜態文字內容最多可包含 4096 個字元。

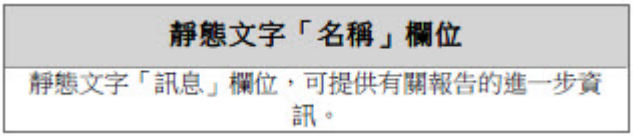


圖 17-2. 靜態文字報告輸出範例

4. 按一下「儲存」以返回「新增/編輯報告範本」畫面。

設定長條圖報告項目

此工作假設您已新增「長條圖」報告項目到自訂報告範本列。

如需詳細資訊，請參閱新增或編輯自訂範本 第 17-3 頁。

步驟

1. 在「長條圖」報告項目中，按一下「編輯」。

   會出現「編輯長條圖 > 步驟 1：資料檢視」畫面。

2. 從「資料檢視」目錄中選取您要顯示的報告資料類型。

如需詳細資訊，請參閱資料檢視 第 B-1 頁。

3. 按「下一步」>。

   會出現「步驟 2：設定查詢條件」畫面。

4. 如果要過濾顯示的資料，請選取「自訂條件」。

5. 指定自訂過濾器的「符合」規則。

   - 所有的條件：資料必須符合所有指定的條件。
   - 任何條件：資料符合任一指定的條件即可。

6. 指定過濾條件，每個條件都包含三個部分：

   - 資料類型：與資料檢視傳回的欄對應
   - 運算子：用來比對或排除資料類型值
   - 值：從下拉式清單控制項中選取條件，或在文字方塊中指定值

   注意

   會顯示哪些選項，視您選取的資料檢視及選取的資料類型和運算子而定。

   Apex Central 支援最多 20 個過濾器。

7. 請使用加號 (+) 和減號 (−) 控制項來新增或移除條件。

8. 按「下一步」>。

   會出現「步驟 3：指定設計」畫面。

9. 指定用做圖表標題的「名稱」。

10. 從「拖曳可用的欄位」清單中，將顯示的資料拖放到下列位置：

    - 資料欄位：指定圖表中出現的資料總數
    - 類別欄位：指定資料在圖表中的分隔方式
    - 系列欄位：定義要對比垂直和水平軸來製圖用做比較的資料類型

11. 在「資料內容」區段中，設定下列項目：

- 彙整依據：顯示資料的方法
  - 執行個體總數：包含資料中重複的結果
  - 唯一執行個體數目：僅顯示重複結果類型的一個執行個體

  例如，如果端點在資料中偵測到 5 個 “VirusA” 執行個體和 3 個 “VirusB” 執行個體，則圖形上的偵測計數會顯示下列值：
  - 執行個體總數 = 8（病毒偵測數，不論病毒名稱為何）
  - 唯一執行個體數目 = 2（唯一病毒類型，不論出現次數）

12. 在「類別內容」區段中，設定下列項目：
    - 指定圖表中水平軸上顯示的「標籤」名稱。
    - 選取「排序」順序和方向。
      - 彙整值：根據資料的計數值排序
      - 類別名稱：根據類別名稱的字母順序排序
    - 選取「過濾摘要結果」核取方塊，可過濾報告中顯示的資料。
      - 指定要顯示的項目數目上限。
      - 啟動「彙整剩餘項目」，可將所有剩餘資料歸類到「其他」類別。
13. 在「系列內容」區段中，指定顯示用於描述資料系列的「標籤名稱」。
14. 按一下「儲存」。

    會出現「新增/編輯報告範本」畫面，其中顯示已套用之更新的圖表設定。

設定折線圖報告項目

此工作假設您已新增「折線圖」報告項目到自訂報告範本列。

如需詳細資訊，請參閱新增或編輯自訂範本 第 17-3 頁。

步驟

1. 在「折線圖」報告項目中，按一下「編輯」。

   會出現「編輯折線圖 > 步驟 1：資料檢視」畫面。

2. 從「資料檢視」目錄中選取您要顯示的報告資料類型。

   如需詳細資訊，請參閱資料檢視 第 B-1 頁。

3. 按「下一步」>。

   會出現「步驟 2：設定查詢條件」畫面。

4. 如果要過濾顯示的資料，請選取「自訂條件」。

5. 指定自訂過濾器的「符合」規則。

   - 所有的條件：資料必須符合所有指定的條件。
   - 任何條件：資料符合任一指定的條件即可。

6. 指定過濾條件，每個條件都包含三個部分：

   - 資料類型：與資料檢視傳回的欄對應
   - 運算子：用來比對或排除資料類型值
   - 值：從下拉式清單控制項中選取條件，或在文字方塊中指定值

   注意

   會顯示哪些選項，視您選取的資料檢視及選取的資料類型和運算子而定。

   Apex Central 支援最多 20 個過濾器。

7. 請使用加號 (+) 和減號 (−) 控制項來新增或移除條件。

8. 按「下一步」>。

   會出現「步驟 3：指定設計」畫面。

9. 指定用做圖表標題的「名稱」。

10. 從「拖曳可用的欄位」清單中，將顯示的資料拖放到下列位置：
    - 資料欄位：定義圖表上垂直軸的資料值
    - 類別欄位：定義圖表上水平軸的資料值
    - 系列欄位：定義要對比垂直和水平軸來製圖用做比較的資料類型
11. 在「資料內容」區段中，設定下列項目：
    - 值標籤：圖表中垂直軸上顯示的標籤
    - 彙整依據：顯示資料的方法
        - 執行個體總數：包含資料中重複的結果
        - 唯一執行個體數目：僅顯示重複結果類型的一個執行個體

        例如，如果端點在資料中偵測到 5 個 “VirusA” 執行個體和 3 個 “VirusB” 執行個體，則圖形上的偵測計數會顯示下列值：
        - 執行個體總數 = 8（病毒偵測數，不論病毒名稱為何）
        - 唯一執行個體數目 = 2（唯一病毒類型，不論出現次數）
12. 在「類別內容」區段中，設定下列項目：
    - 指定圖表中水平軸上顯示的「標籤」名稱。
    - 選取「排序」順序和方向。
        - 彙整值：根據資料的計數值排序
        - 類別名稱：根據類別名稱的字母順序排序
    - 選取「過濾摘要結果」核取方塊，可過濾報告中顯示的資料。
        - 指定要顯示的項目數目上限。
        - 啟動「彙整剩餘項目」，可將所有剩餘資料歸類到「其他」類別。
13. 在「系列內容」區段中，指定顯示用於描述資料系列的「標籤名稱」。
14. 按一下「儲存」。

會出現「新增/編輯報告範本」畫面，其中顯示已套用之更新的圖表設定。

設定圓餅圖報告項目

此工作假設您已新增「圓餅圖」報告項目到自訂報告範本列。

如需詳細資訊，請參閱新增或編輯自訂範本 第 17-3 頁。

步驟

1. 在「圓餅圖」報告項目中，按一下「編輯」。

   會出現「編輯圓餅圖 > 步驟 1：資料檢視」畫面。

2. 從「資料檢視」目錄中選取您要顯示的報告資料類型。

   如需詳細資訊，請參閱資料檢視 第 B-1 頁。

3. 按「下一步」>。

   會出現「步驟 2：設定查詢條件」畫面。

4. 如果要過濾顯示的資料，請選取「自訂條件」。

5. 指定自訂過濾器的「符合」規則。

   - 所有的條件：資料必須符合所有指定的條件。
   - 任何條件：資料符合任一指定的條件即可。

6. 指定過濾條件，每個條件都包含三個部分：

   - 資料類型：與資料檢視傳回的欄對應
   - 運算子：用來比對或排除資料類型值
   - 值：從下拉式清單控制項中選取條件，或在文字方塊中指定值

注意

會顯示哪些選項，視您選取的資料檢視及選取的資料類型和運算子而定。

Apex Central 支援最多 20 個過濾器。

7. 請使用加號 (+) 和減號 (−) 控制項來新增或移除條件。
8. 按「下一步」>。

   會出現「步驟 3：指定設計」畫面。
9. 指定用做圖表標題的「名稱」。
10. 從「拖曳可用的欄位」清單中，將顯示的資料拖放到下列位置：
    - 資料欄位：指定圖表中出現的資料總數
    - 類別欄位：指定資料在圖表中的分隔方式
11. 在「資料內容」區段中，設定下列項目：
    - 彙整依據：顯示資料的方法
      - 執行個體總數：包含資料中重複的結果
      - 唯一執行個體數目：僅顯示重複結果類型的一個執行個體

      例如，如果端點在資料中偵測到 5 個 “VirusA” 執行個體和 3 個 “VirusB” 執行個體，則圖形上的偵測計數會顯示下列值：
      - 執行個體總數 = 8（病毒偵測數，不論病毒名稱為何）
      - 唯一執行個體數目 = 2（唯一病毒類型，不論出現次數）
12. 在「類別內容」區段中，設定下列項目：
    - 指定圖表中水平軸上顯示的「標籤」名稱。
    - 選取「排序」順序和方向。
      - 彙整值：根據資料的計數值排序
      - 類別名稱：根據類別名稱的字母順序排序

- 選取「過濾摘要結果」核取方塊，可過濾報告中顯示的資料。
  - 指定要顯示的項目數目上限。
  - 啟動「彙整剩餘項目」，可將所有剩餘資料歸類到「其他」類別。

13. 按一下「儲存」。

    會出現「新增/編輯報告範本」畫面，其中顯示已套用之更新的圖表設定。

設定動態資料表報告項目

此工作假設您已新增「動態資料表」報告項目到自訂報告範本列。

如需詳細資訊，請參閱新增或編輯自訂範本 第 17-3 頁。

步驟

1. 在「動態資料表」報告項目中，按一下「編輯」。

   會出現「編輯動態資料表 > 步驟 1：資料檢視」畫面。

2. 從「資料檢視」目錄中選取您要顯示的報告資料類型。

   如需詳細資訊，請參閱資料檢視 第 B-1 頁。

3. 按「下一步」>。

   會出現「步驟 2：設定查詢條件」畫面。

4. 如果要過濾顯示的資料，請選取「自訂條件」。

5. 指定自訂過濾器的「符合」規則。
   - 所有的條件：資料必須符合所有指定的條件。
   - 任何條件：資料符合任一指定的條件即可。

6. 指定過濾條件，每個條件都包含三個部分：

- 資料類型：與資料檢視傳回的欄對應
- 運算子：用來比對或排除資料類型值
- 值：從下拉式清單控制項中選取條件，或在文字方塊中指定值

注意

會顯示哪些選項，視您選取的資料檢視及選取的資料類型和運算子而定。

Apex Central 支援最多 20 個過濾器。

7. 請使用加號 (+) 和減號 (−) 控制項來新增或移除條件。
8. 按「下一步」>。

   會出現「步驟 3：指定設計」畫面。
9. 指定用做圖表標題的「名稱」。
10. 從「拖曳可用的欄位」清單中，將顯示的資料拖放到下列位置：
    - 列欄位：定義資料在資料表中的水平分隔方式
    - 欄欄位：定義資料在資料表中的垂直分隔方式
    - 資料欄位：定義為資料表中指定之「列欄位」或「欄欄位」顯示的資料值

重要

「動態資料表」報告項目只需要一個「資料欄位」，以及一個「列欄位」或一個「欄欄位」。

11. 在「資料內容」區段中，設定下列項目：
    - 資料欄位標題：資料欄位的標籤
    - 彙整依據：顯示資料的方法
      - 執行個體總數：包含資料中重複的結果
      - 唯一執行個體數目：僅顯示重複結果類型的一個執行個體

例如，如果端點在資料中偵測到 5 個 “VirusA” 執行個體和 3 個 “VirusB” 執行個體，則圖形上的偵測計數會顯示下列值：

- 執行個體總數 = 8（病毒偵測數，不論病毒名稱為何）
- 唯一執行個體數目 = 2（唯一病毒類型，不論出現次數）

12. 在「列內容」區段中，設定下列項目：
    - 指定「列標頭標題」。
    - 選取「排序」順序和方向。
        - 彙整值：根據資料的計數值排序
        - 標頭標題：根據類別名稱的字母順序排序
    - 選取「過濾摘要結果」核取方塊，可過濾報告中顯示的資料。
        - 指定要顯示的項目數目上限。
        - 啟動「彙整剩餘項目」，可將所有剩餘資料歸類到「其他」類別。
13. 在「欄內容」區段中，設定下列項目：
    - 指定「欄標頭標題」。
    - 選取「排序」順序和方向。
        - 彙整值：根據資料的計數值排序
        - 標頭標題：根據類別名稱的字母順序排序
    - 選取「過濾摘要結果」核取方塊，可過濾報告中顯示的資料。
        - 指定要顯示的項目數目上限。
        - 啟動「彙整剩餘項目」，可將所有剩餘資料歸類到「其他」類別。
14. 按一下「儲存」。

    會出現「新增/編輯報告範本」畫面，其中顯示已套用之更新的圖表設定。

設定格線資料表報告項目

此工作假設您已新增「格線資料表」報告項目到自訂報告範本列。

如需詳細資訊，請參閱新增或編輯自訂範本 第 17-3 頁。

步驟

1. 在「格線資料表」報告項目中，按一下「編輯」。

   會出現「編輯格線資料表 > 步驟 1：資料檢視」畫面。

2. 從「資料檢視」目錄中選取您要顯示的報告資料類型。

   如需詳細資訊，請參閱資料檢視 第 B-1 頁。

3. 按「下一步」>。

   會出現「步驟 2：設定查詢條件」畫面。

4. 如果要過濾顯示的資料，請選取「自訂條件」。

5. 指定自訂過濾器的「符合」規則。

   - 所有的條件：資料必須符合所有指定的條件。
   - 任何條件：資料符合任一指定的條件即可。

6. 指定過濾條件，每個條件都包含三個部分：

   - 資料類型：與資料檢視傳回的欄對應
   - 運算子：用來比對或排除資料類型值
   - 值：從下拉式清單控制項中選取條件，或在文字方塊中指定值

   注意

   會顯示哪些選項，視您選取的資料檢視及選取的資料類型和運算子而定。

   Apex Central 支援最多 20 個過濾器。

7. 請使用加號 (+) 和減號 (−) 控制項來新增或移除條件。

8. 按「下一步」>。

   會出現「步驟 3：指定設計」畫面。

9. 指定用做圖表標題的「名稱」。

10. 選取要在報告中顯示的資料欄位：

    注意

    依預設，Apex Central 會為指定的資料檢視選取所有欄位。

11. 選取「選取的欄位」的「排序」順序。

12. 選取「顯示數量」，以定義報告中包含的項目數目上限。

13. 按一下「儲存」。

    會出現「新增/編輯報告範本」畫面，其中顯示已套用之更新的圖表設定。

一次性報告

「一次性報告」畫面提供有關網路的所有先前產生的一次性報告清單。您可以使用此畫面建立新的一次性報告，並檢視先前產生的一次性報告。

下表列出「一次性報告」畫面上的可用工作。

工作	說明
新增一次性報告	按一下「新增」來建立新的一次性報告。 如需詳細資訊，請參閱建立一次性報告 第 17-19 頁。
刪除一次性報告	選取現有的一次性報告，然後按一下「刪除」。
轉寄一次性報告給電子郵件收件者	選取現有的一次性報告，然後按一下「轉寄」，將報告做為電子郵件附件傳送給指定的收件者。
檢視產生的一次性報告	按一下您要檢視的報告的「檢視」欄中的「檢視」連結。

工作	說明
檢視一次性報告資料檔	按一下先前產生的一次性報告的「名稱」，來檢視報告資料檔。 注意 您無法編輯先前產生的一次性報告資料檔。

建立一次性報告

使用「一次性報告」畫面來視需要產生報告。建立報告時，請指定要使用自訂範本還是靜態範本。

步驟

1. 移至「偵測 > 報告 > 一次性報告」。

   會出現「一次性報告」畫面。

2. 請點選「新增」。

   會出現「新增一次性報告 > 步驟 1：內容」畫面。

3. 在「名稱」欄位中輸入報告的名稱。

4. （選用）在「說明」欄位中輸入報告的說明。

5. 在「報告內容」區段中，選取下列其中一種範本類型：

   - 自訂範本：選取一或多個自訂報告範本。

     注意

     選取多個自訂範本會產生單一報告，其中顯示來自全部所選範本的已格式化資料。

     如需有關建立自訂報告範本的詳細資訊，請參閱新增或編輯自訂範本 第 17-3 頁。

- 靜態範本：選取 Trend Micro 所提供的一或多個靜態範本。
  a. 從「報告類別」下拉式清單中選取靜態範本。
  b. 選取要在報告中顯示的資料，然後指定所有對應的參數。

6. 選取報告產生格式。
   - 自訂範本報告格式：
     - Adobe PDF 格式 (*.pdf)
     - HTML 格式 (*.html)
     - XML 格式 (*.xml)
     - CSV 格式 (*.csv)
   - 靜態範本報告格式：
     - Adobe PDF 格式 (*.pdf)
     - Microsoft Word 格式 (*.docx)
     - Microsoft Excel 格式 (*.xlsx)
7. 按「下一步」。

   會出現「新增一次性報告 > 步驟 2：目標」畫面。
8. 使用下列其中一個檢視指定目標。
   - 產品目錄：選取提供報告資訊的受管理產品或其中包含受管理產品的資料夾。
   - 標籤和過濾器：最多選取 10 個包含使用者或端點的自訂標籤 (Tags)、過濾器或重要標籤，以提供報告資訊。

注意

- 「標籤和過濾器」檢視只適用於自訂報告範本。
- 使用者帳號所產生的報告僅包含端點中該使用者有權限檢視的資料。如果使用者帳號所選取的標籤、過濾器或重要性標籤包含使用者帳號沒有權限可檢視的端點，則產生的報告將會排除來自未經授權端點的資料。
- 在「使用者/端點目錄」畫面上編輯標籤、過濾器或重要性標籤時，也會一併修改記錄查詢和報告所用的對應標籤、過濾器或重要性標籤。例如，如果在「使用者/端點目錄」畫面上，將端點從自訂過濾器中移除，則使用該過濾器的記錄查詢和產生的報告將會排除已移除端點中的資料。

9. 如果報告包含來自網路病毒牆執行器裝置的資料，請指定產生報告的用戶端：
   - 所有用戶端：從所有網路病毒牆執行器裝置產生報告
   - IP 範圍：從特定的 IP 位址範圍產生報告
   - 網段：從特定的網路區段產生報告
10. 按「下一步」。

    會出現「新增一次性報告 > 步驟 3：時間範圍」畫面。
11. 指定報告的時間範圍。
12. 按「下一步」。

    會出現「新增一次性報告 > 步驟 4：郵件內容和收件者」畫面。
13. （選用）將報告做為電子郵件附件傳送給選取的收件者。
    a. 在「主旨」欄位中，輸入內含報告之電子郵件訊息的標題。
    b. 在「訊息」欄位中，輸入報告的相關說明。
    c. 選取「將報告做為電子郵件附件傳送」，將報告傳送給選取的收件者。
    d. 選取聯絡人群組或使用者帳號。

e. 按一下「>>」。

選取的聯絡人群組或使用者帳號會顯示在「收件者」清單中。

14. 請點選「完成」。

會出現「一次性報告」畫面，其中顯示最近新增的報告產生工作。

15. 如果要檢視產生的報告，請執行下列作業：

a. 按一下您要檢視之已產生報告的「檢視」欄中的「檢視」連結。

b. 開啟或儲存產生的報告檔案。

檢視一次性報告

使用「一次性報告」畫面，可檢視先前產生的一次性報告。

步驟

1. 移至「偵測 > 報告 > 一次性報告」。

會出現「一次性報告」畫面。

2. 按一下您要檢視之已產生報告的「檢視」欄中的「檢視」連結。
3. 開啟或儲存產生的報告檔案。

預約報告

「預約報告」畫面會列出根據使用者定義的預約時程自動產生的所有報告。您可以使用此畫面來檢視有關先前設定的預約報告的基本資訊、新增預約報告，以及啟動/關閉預約報告。

下表列出「預約報告」畫面上的可用工作。

工作	說明
新增預約報告資料檔	按一下「新增」建立新的預約報告資料檔。 如需詳細資訊，請參閱新增預約報告 第 17-23 頁。
編輯預約報告資料檔	按一下要編輯的現有預約報告資料檔的「名稱」。 如需詳細資訊，請參閱編輯預約報告 第 17-27 頁。
複製預約報告資料檔	選取一或多個現有預約報告資料檔，然後按一下「複製」，即可複製選取的資料檔。 按一下要編輯的已複製預約報告資料檔的「名稱」。 如需詳細資訊，請參閱編輯預約報告 第 17-27 頁。
刪除預約報告資料檔	選取現有的預約報告資料檔，然後按一下「刪除」。
檢視先前產生的預約報告	按一下您要檢視的報告的「歷史記錄」欄中的「檢視」連結。 如需詳細資訊，請參閱檢視預約報告 第 17-31 頁。
啟動或關閉預約報告	• 如果要關閉預約報告，請按一下「啟動」欄中的「已啟動」( ) 圖示。 • 如果要啟動預約報告，請按一下「啟動」欄中的「已關閉」( ) 圖示。 注意 依預設，會啟動最近新增的預約報告資料檔。

新增預約報告

使用「預約報告」畫面可按照使用者定義的預約時程自動產生報告。新增預約報告時，請指定要使用自訂範本還是靜態範本。

步驟

1. 移至「偵測 > 報告 > 預約報告」。

   會出現「預約報告」畫面。

2. 請點選「新增」。

   會出現「新增預約報告 > 步驟 1：內容」畫面。

3. 在「名稱」欄位中輸入報告的名稱。

4. （選用）在「說明」欄位中輸入報告的說明。

5. 在「報告內容」區段中，選取下列其中一種範本類型：

   - 自訂範本：選取一或多個自訂報告範本。

     注意

     選取多個自訂範本會產生單一報告，其中顯示來自全部所選範本的已格式化資料。

     如需有關建立自訂報告範本的詳細資訊，請參閱新增或編輯自訂範本 第 17-3 頁。

   - 靜態範本：選取 Trend Micro 所提供的一或多個靜態範本。

     a. 從「報告類別」下拉式清單中選取靜態範本。

     b. 選取要在報告中顯示的資料，然後指定所有對應的參數。

6. 選取報告產生格式。

   - 自訂範本報告格式：
     - Adobe PDF 格式 (*.pdf)
     - HTML 格式 (*.html)
     - XML 格式 (*.xml)
     - CSV 格式 (*.csv)
   - 靜態範本報告格式：
     - Adobe PDF 格式 (*.pdf)
     - Microsoft Word 格式 (*.docx)
     - Microsoft Excel 格式 (*.xlsx)

7. 按「下一步」。

   會出現「新增預約報告 > 步驟 2：目標」畫面。

8. 使用下列其中一個檢視指定目標。

   - 產品目錄：選取提供報告資訊的受管理產品或其中包含受管理產品的資料夾。
   - 標籤和過濾器：最多選取 10 個包含使用者或端點的自訂標籤 (Tags)、過濾器或重要標籤，以提供報告資訊。

   注意

   - 「標籤和過濾器」檢視只適用於自訂報告範本。
   - 使用者帳號所產生的報告僅包含端點中該使用者有權限檢視的資料。如果使用者帳號所選取的標籤、過濾器或重要性標籤包含使用者帳號沒有權限可檢視的端點，則產生的報告將會排除來自未經授權端點的資料。
   - 在「使用者/端點目錄」畫面上編輯標籤、過濾器或重要性標籤時，也會一併修改記錄查詢和報告所用的對應標籤、過濾器或重要性標籤。例如，如果在「使用者/端點目錄」畫面上，將端點從自訂過濾器中移除，則使用該過濾器的記錄查詢和產生的報告將會排除已移除端點中的資料。

9. 如果報告包含來自網路病毒牆執行器裝置的資料，請指定產生報告的用戶端：

   - 所有用戶端：從所有網路病毒牆執行器裝置產生報告
   - IP 範圍：從特定的 IP 位址範圍產生報告
   - 網段：從特定的網路區段產生報告

10. 按「下一步」。

    會出現「新增預約報告 > 步驟 3：頻率」畫面。

11. 指定產生報告的頻率：

    - 每 n 天一次：根據您的選擇，每隔 1 到 6 天產生一次報告。

- 每週一次：每週於指定日子產生一次報告。
- 兩週一次：每兩週於指定日子產生一次報告。
- 每月一次：每月於第 1 天、第 5 天、第 10 天、第 15 天、第 20 天、第 25 天或最後一天產生一次報告。

12. 指定資料範圍：
    - 報告包含一直到下方指定之「啟動預約」時間為止的資料：這表示報告可以包含最長達 23 個小時以上的資料。由於此選項對每週一次或每月一次報告的影響很小，因此產生的「每日一次」報告可包含幾乎整整兩天的資料，實際時間長度視「啟動預約」時間而定。
    - 報告包含一直到前一天 23:59:59 為止的資料：這表示報告的資料收集一到午夜就會立即停止。報告是一段精確的時間範圍（範例：「每日一次」報告是 24 小時），但不會包含絕對最新的資料。
13. 指定報告預約時程啟動時間：
    - 立即：報告預約時程會在啟動報告後立即啟動。
    - 「開始時間」：報告預約時程會在隨附欄位中指定的日期和時間啟動。

秘訣

按一下「年/月/日」欄位旁的行事曆圖示，可使用動態行事曆來指定日期範圍。

14. 按「下一步」。

    會出現「新增預約報告 > 步驟 4：郵件內容和收件者」畫面。

15. （選用）將報告做為電子郵件附件傳送給選取的收件者。
    a. 在「主旨」欄位中，輸入內含報告之電子郵件訊息的標題。
    b. 在「訊息」欄位中，輸入報告的相關說明。
    c. 選取「將報告做為電子郵件附件傳送」，將報告傳送給選取的收件者。

d. 選取聯絡人群組或使用者帳號。

e. 按一下「>>」。

選取的聯絡人群組或使用者帳號會顯示在「收件者」清單中。

16. 請點選「完成」。

會出現「預約報告」畫面，其中顯示最近新增的報告產生工作。

注意

依預設，Apex Central 會啟動最近新增的預約報告。

17. 如果要檢視產生的報告，請執行下列作業：

a. 按一下您要檢視之預約報告的「歷史記錄」欄中的「檢視」連結。

會出現「預約報告歷史記錄」畫面。

b. 按一下您要檢視之已產生報告的「檢視」欄中的「檢視」連結。

秘訣

如果預約報告尚未產生，請按一下「產生」按鈕，以根據預約報告設定建立快速報告。

c. 開啟或儲存產生的報告檔案。

編輯預約報告

使用「預約報告」畫面可按照使用者定義的預約時程自動產生報告。新增預約報告時，請指定要使用自訂範本還是靜態範本。

步驟

1. 移至「偵測 > 報告 > 預約報告」。

會出現「預約報告」畫面。

2. 按一下預約報告資料檔的「名稱」。

   會出現「編輯預約報告 > 步驟 1：內容」畫面。

3. 在「名稱」欄位中輸入報告的名稱。

4. （選用）在「說明」欄位中輸入報告的說明。

5. 在「報告內容」區段中，選取下列其中一種範本類型：

   - 自訂範本：選取一或多個自訂報告範本。

     注意

     選取多個自訂範本會產生單一報告，其中顯示來自全部所選範本的已格式化資料。

     如需有關建立自訂報告範本的詳細資訊，請參閱新增或編輯自訂範本 第 17-3 頁。

   - 靜態範本：選取 Trend Micro 所提供的一或多個靜態範本。

     a. 從「報告類別」下拉式清單中選取靜態範本。

     b. 選取要在報告中顯示的資料，然後指定所有對應的參數。

6. 選取報告產生格式。

   - 自訂範本報告格式：
     - Adobe PDF 格式 (*.pdf)
     - HTML 格式 (*.html)
     - XML 格式 (*.xml)
     - CSV 格式 (*.csv)
   - 靜態範本報告格式：
     - Adobe PDF 格式 (*.pdf)
     - Microsoft Word 格式 (*.docx)
     - Microsoft Excel 格式 (*.xlsx)

7. 按「下一步」。

   會出現「編輯預約報告 > 步驟 2：目標」畫面。

8. 使用下列其中一個檢視指定目標。

   - 產品目錄：選取提供報告資訊的受管理產品或其中包含受管理產品的資料夾。
   - 標籤和過濾器：最多選取 10 個包含使用者或端點的自訂標籤 (Tags)、過濾器或重要標籤，以提供報告資訊。

   注意

   - 「標籤和過濾器」檢視只適用於自訂報告範本。
   - 使用者帳號所產生的報告僅包含端點中該使用者有權限檢視的資料。如果使用者帳號所選取的標籤、過濾器或重要性標籤包含使用者帳號沒有權限可檢視的端點，則產生的報告將會排除來自未經授權端點的資料。
   - 在「使用者/端點目錄」畫面上編輯標籤、過濾器或重要性標籤時，也會一併修改記錄查詢和報告所用的對應標籤、過濾器或重要性標籤。例如，如果在「使用者/端點目錄」畫面上，將端點從自訂過濾器中移除，則使用該過濾器的記錄查詢和產生的報告將會排除已移除端點中的資料。

9. 如果報告包含來自網路病毒牆執行器裝置的資料，請指定產生報告的用戶端：

   - 所有用戶端：從所有網路病毒牆執行器裝置產生報告
   - IP 範圍：從特定的 IP 位址範圍產生報告
   - 網段：從特定的網路區段產生報告

10. 按「下一步」。

    會出現「編輯預約報告 > 步驟 3：頻率」畫面。

11. 指定產生報告的頻率：

    - 每 n 天一次：根據您的選擇，每隔 1 到 6 天產生一次報告。

- 每週一次：每週於指定日子產生一次報告。
- 兩週一次：每兩週於指定日子產生一次報告。
- 每月一次：每月於第 1 天、第 5 天、第 10 天、第 15 天、第 20 天、第 25 天或最後一天產生一次報告。

12. 指定資料範圍：
    - 報告包含一直到下方指定之「啟動預約」時間為止的資料：這表示報告可以包含最長達 23 個小時以上的資料。由於此選項對每週一次或每月一次報告的影響很小，因此產生的「每日一次」報告可包含幾乎整整兩天的資料，實際時間長度視「啟動預約」時間而定。
    - 報告包含一直到前一天 23:59:59 為止的資料：這表示報告的資料收集一到午夜就會立即停止。報告是一段精確的時間範圍（範例：「每日一次」報告是 24 小時），但不會包含絕對最新的資料。
13. 指定報告預約時程啟動時間：
    - 立即：報告預約時程會在啟動報告後立即啟動。
    - 「開始時間」：報告預約時程會在隨附欄位中指定的日期和時間啟動。

秘訣

按一下「年/月/日」欄位旁的行事曆圖示，可使用動態行事曆來指定日期範圍。

14. 按「下一步」。

    會出現「編輯預約報告 > 步驟 4：郵件內容和收件者」畫面。

15. （選用）將報告做為電子郵件附件傳送給選取的收件者。
    a. 在「主旨」欄位中，輸入內含報告之電子郵件訊息的標題。
    b. 在「訊息」欄位中，輸入報告的相關說明。
    c. 選取「將報告做為電子郵件附件傳送」，將報告傳送給選取的收件者。

d. 選取聯絡人群組或使用者帳號。

e. 按一下「>>」。

選取的聯絡人群組或使用者帳號會顯示在「收件者」清單中。

16. 請點選「完成」。

會出現「預約報告」畫面，其中顯示最近新增的報告產生工作。

檢視預約報告

使用「預約報告」畫面，可檢視先前產生的預約報告。

步驟

1. 移至「偵測 > 報告 > 預約報告」。

會出現「預約報告」畫面。

2. 按一下您要檢視之預約報告的「歷史記錄」欄中的「檢視」連結。

會出現「預約報告歷史記錄」畫面。

3. 按一下您要檢視之已產生報告的「檢視」欄中的「檢視」連結。

秘訣

如果預約報告尚未產生，請按一下「產生」按鈕，以根據預約報告設定建立快速報告。

4. 開啟或儲存產生的報告檔案。

設定報告維護

設定「報告維護」設定，可在達到報告數目上限時刪除報告。

步驟

1. 移至「偵測 > 報告 > 報告維護」。

   會出現「報告維護」畫面。

2. 指定要保留的一次性報告和預約報告的數目上限。

3. 按一下「儲存」。

檢視我的報告

「我的報告」畫面提供目前使用者所產生的所有報告清單。您也可以檢視與目前使用者同屬相同群組的其他使用者所產生的報告。

步驟

1. 移至「偵測 > 報告 > 我的報告」。

   會出現「我的報告」畫面。

2. 按一下您要檢視之已產生報告的「檢視」欄中的「檢視」連結。

3. 開啟或儲存產生的報告檔案。

第 18 章

資料外洩防護事件

Apex Central 提供可讓 DLP 合規官和事件檢閱者檢視及更新事件資訊的功能。

包含下列主題：

- 管理員工作 第 18-2 頁
- DLP 事件檢閱程序 第 18-6 頁

管理員工作

如果要啟動事件檢閱程序，Apex Central 管理員必須完成一些必要工作。下表列出所需工作和參考資料：

表 18-1. 管理員工作

工作	參考資料
在 Active Directory 中設定管理員資訊。	設定 Active Directory 使用者的管理員資訊 第 18-2 頁
設定 Active Directory 整合，以取得使用者資訊。	Active Directory 和符合性設定 第 6-1 頁
建立 DLP 事件查詢專用的使用者帳號。 您可以指派下列使用者角色來授與檢閱 DLP 事件的權限： • 管理員和 DLP 合規官 • DLP 合規官 • DLP 事件檢閱者 注意 「DLP 合規官」和「DLP 事件檢閱者」角色僅適用於 Active Directory 使用者。	• 瞭解 DLP 使用者角色 第 18-3 頁 • 預設使用者角色 第 4-15 頁 • 新增使用者帳號 第 4-4 頁
設定「預約事件摘要」和「事件詳細資料已更新」通知。	• 預約事件摘要 第 16-34 頁 • 事件詳細資料已更新 第 16-33 頁
匯出 DLP 記錄檔供稽核之用。	查詢記錄檔 第 15-2 頁

設定 Active Directory 使用者的管理員資訊

為方便管理員調查 DLP 事件，請設定每位 Active Directory 使用者的管理員資訊。

步驟

1. 開啟「Active Directory 使用者和電腦」主控台。按一下「開始 > 系統管理工具 > Active Directory 使用者和電腦」。

   會出現「Active Directory 使用者和電腦」主控台。

2. 按兩下使用者。

   會出現「<使用者> 內容」畫面。

3. 按一下「組織」標籤，然後按一下「變更...」。

   會出現「選取使用者或聯絡人」畫面。

4. 指定管理員資訊，然後按一下「確定」。

5. 如果要確認管理員與使用者的關係，請開啟管理員的「<使用者> 內容」畫面，接著按一下「組織」標籤，然後檢查「直屬員工」下方的使用者資訊。

瞭解 DLP 使用者角色

Apex Central 提供下列資料外洩防護 (DLP) 使用者角色：

- 管理員和 DLP 合規官
- DLP 合規官
- DLP 事件檢閱者

注意

您只能將「DLP 合規官」和「DLP 事件檢閱者」角色指派給 Active Directory 使用者帳號。

下表說明與 DLP 使用者角色相關的功能和特性：

功能	角色	說明
DLP 記錄檔	管理員和 DLP 合規官	• 檢視所有 Active Directory 使用者的 DLP 記錄檔資料 • 存取顯示 DLP 事件資訊的特定 Widget
	DLP 合規官 DLP 事件檢閱者	• 將存取限制為與直接受管理的使用者相關的 DLP 記錄檔 • 存取顯示 DLP 事件資訊的特定 Widget

事件範圍	管理員和 DLP 合規官
	DLP 合規官
		• 按一下下列任何「資料外洩防護」Widget 上的「設定」圖示 (>)，並選取「所有受管理的使用者」做為「範圍」，可檢視所有 Active Directory 使用者的 DLP 事件資料。
		  • 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)
		  注意
		  • 依預設，每個「資料外洩防護」Widget 的範圍只允許此角色檢視「直接受管理的使用者」的事件資料。
		  • 變更一個「資料外洩防護」Widget 的「範圍」不會影響任何其他 Widget 的範圍。
		• 在所有其他畫面上：
		  • 指派有「管理員和 DLP 合規官」角色的使用者帳號可以根據使用者帳號的產品範圍，檢視受管理產品回報的所有 Active Directory 使用者之資料。
		  • 「DLP 合規官」角色無法檢視任何資料

	DLP 事件檢閱者	檢視直接受管理的使用者的 DLP 事件資料

功能	角色	說明
功能表存取	管理員和 DLP 合規官 DLP 合規官 DLP 事件檢閱者	存取「資料外洩防護」標籤和下列 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) 如需詳細資訊，請參閱資料外洩防護標籤 第 3-25 頁。
預約事件摘要通知	管理員和 DLP 合規官 DLP 合規官 DLP 事件檢閱者	接收下列內容： • 每日或每週電子郵件通知 • 事件計數（依嚴重性層級）的摘要清單 • Apex Central Web 主控台的連結
事件詳細資料已更新通知	管理員和 DLP 合規官 DLP 合規官	收到事件狀態或備註發生變更的通知 注意 「DLP 事件檢閱者」角色不會收到此通知。

建立 DLP 稽核記錄檔

管理員可以使用記錄查詢來產生及匯出 DLP 稽核記錄檔。請按照查詢記錄檔 第 15-2 頁中所述程序來執行記錄查詢，並設定下列項目：

- 記錄類型：選取「使用者存取」
- 進階過濾器：將下列活動（「活動」）新增至自訂條件：
  - 下載 DLP 事件檔案
  - 更新 DLP 事件

DLP 事件檢閱程序

在 Apex Central 管理員完成必要工作後，檢閱者即可開始事件檢閱程序。下表列出工作和參考資料：

表 18-2. DLP 事件檢閱程序

工作	說明
接收預約事件摘要通知訊息	Apex Central 會每天或每週摘要列出並傳送電子郵件通知給事件檢閱者。
使用下列其中一種方法來檢閱有關事件的詳細資料： • 按一下訊息中提供的連結登入 Apex Central Web 主控台 • 開啟附件（如果有的話）	瞭解事件資訊清單 第 18-6 頁
更新事件狀態並提供備註	檢閱事件詳細資料 第 18-8 頁

瞭解事件資訊清單

「事件資訊」畫面顯示檢閱者可管理的事件清單。事件檢閱者可以使用此畫面執行下列作業：

- 檢視事件摘要
- 對事件採取處理行動
- 匯出事件詳細資料

表 18-3. 事件資訊清單

項目	說明
識別碼	唯一事件 ID

項目	說明
收到	Apex Central 收到事件資料的日期和時間 注意 收到來自受管理產品的 DLP 記錄檔後，Apex Central 需要 30 分鐘時間來處理記錄檔，之後事件檢閱者即可檢視資料。
嚴重性	事件的嚴重性層級 注意 Apex Central 一收到 DLP 事件並進行處理時，如果在受管理產品中發生變更，Apex Central 並不會更新嚴重性層級。
策略	觸發事件的 Apex Central 策略名稱 注意 如果事件觸發的 DLP 策略是在受管理產品中建立的，則此名稱會顯示為「無」。
使用者	觸發事件的使用者名稱
管理員	使用者的管理員名稱
狀態	事件的目前狀態 • 新增 • 調查中 • 已向上呈報 • 已關閉
處理行動	可用來管理事件的處理行動

檢閱事件詳細資料

按一下「事件資訊」畫面「處理行動」欄中的「編輯」圖示，會出現「事件詳細資料」畫面，其中顯示有關事件的詳細資訊。DLP 事件檢閱者可以使用此畫面更新事件狀態，並針對事件提供意見。

表 18-4. 事件詳細資料

項目	說明
識別碼	唯一事件 ID
狀態	使用此項目可更新事件的檢閱狀態。 可用的選項： • 新增 • 調查中 • 已向上呈報 • 已關閉
嚴重性	事件的嚴重性層級 **注意** Apex Central 一收到 DLP 事件並進行處理時，如果在受管理產品中發生變更，Apex Central 並不會更新嚴重性層級。
策略	觸發事件的 Apex Central 策略名稱 **注意** 如果事件觸發的 DLP 策略是在受管理產品中建立的，則此名稱會顯示為「無」。
規則	觸發事件所依據的規則名稱

項目	說明
收到	Apex Central 收到事件資料的日期和時間 注意 收到來自受管理產品的 DLP 記錄檔後，Apex Central 需要 30 分鐘時間來處理記錄檔，之後事件檢閱者即可檢視資料。
已產生	在受管理產品中發生事件的日期和時間
使用者	觸發事件的使用者名稱
管理員	使用者的管理員名稱
端點	來源主機名稱
IP 位址	來源 IP 位址
寄件者	來源電子郵件信箱
主旨	電子郵件訊息的主旨
收件者	目標電子郵件信箱
目標	包含數位資產的檔案預定目標或通道（如果沒有來源可用的話）
上次修改日期	資產上次修改的日期和時間
上次修改者	上次修改資產的使用者名稱
範本	觸發事件的範本名稱
檔案	觸發事件的檔案名稱或檔案連結 注意 在受管理產品中隔離檔案。
SHA-1	檔案的雜湊資訊
通道	傳輸發生所經由的通道
處理行動	對事件採取的處理行動

項目	說明
使用者理由	使用者所定義之允許使用者傳輸機密資料的理由
相符內容	觸發事件的數位資產
備註	使用者定義的事件相關注意事項

部分 VI

安全威脅資訊與回應

第 19 章

連線的威脅防範

本節討論如何在目標式攻擊和進階安全威脅造成永久性損害之前進行偵測、分析及回應。

包含下列主題：

- 關於連線的威脅防範 第 19-2 頁
- 功能需求 第 19-2 頁
- 可疑物件清單管理 第 19-6 頁
- 先發式可疑物件防護 第 19-19 頁
- 連線的威脅防範產品整合 第 19-34 頁

關於連線的威脅防範

Apex Central 整合了多種趨勢科技產品與解決方案，可協助您在目標式攻擊和進階安全威脅造成永久性損害之前進行偵測、分析及回應。

如需詳細資訊，請參閱連線的威脅防範產品整合。

功能需求

下表列出可與「連線的威脅防範」架構搭配使用的功能清單，以及整合彼此的必要產品和選用產品。

功能	必要產品	可選產品

安全威脅監控	• Apex Central
	• Deep Discovery Inspector 5.0（或更新版本）或下列其中一個沙箱產品：
	  • Apex One Sandbox as a Service
	  • Deep Discovery Analyzer
	重要
	若要評估記錄檔資料，將需要至少一個選用產品。
		• Apex One 2019 或 OfficeScan 11.0 SP1（或更新版本）
		• Apex One Endpoint Sensor
		• Cloud App Security 5.0（或更新版本）
		• Deep Security Manager 10.0（或更新版本）
		• InterScan Messaging Security Virtual Appliance 9.1（或更新版本）
		• InterScan Web Security Virtual Appliance 6.5 SP2 Patch 4（或更新版本）
		• ScanMail for Microsoft Exchange 12.5（或更新版本）
		• Trend Micro Endpoint Application Control 2.0 SP1（或更新版本）

功能	必要產品	可選產品

可疑物件清單同步處理
 	
如需詳細資訊，請參閱可疑物件清單 第 19-6 頁和連線的威脅防範產品整合 第 19-34 頁。
	• Apex Central
	• Deep Discovery Inspector 5.0（或更新版本）或下列其中一個沙箱產品：
	  • Apex One Sandbox as a Service
	  • Deep Discovery Analyzer
	
	重要
	若要進行可疑物件清單同步處理，將需要至少一個選用產品。
		• Apex One 2019 或 OfficeScan 11.0 SP1（或更新版本）
		• Cloud App Security 5.0（或更新版本）
		• Deep Discovery Director
		• Deep Security Manager 10.0（或更新版本）
		• InterScan Messaging Security Virtual Appliance 9.1（或更新版本）
		• InterScan Web Security Virtual Appliance 6.5 SP2 Patch 4（或更新版本）
		• 主動雲端截毒技術伺服器 3.3 Patch 2（或更新版本）
		• Trend Micro Endpoint Application Control 2.0 SP1（或更新版本）

功能	必要產品	可選產品

可疑物件樣本提交	• Deep Discovery Inspector 5.0（或更新版本）或下列其中一個沙箱產品：
	  • Apex One Sandbox as a Service
	  • Deep Discovery Analyzer
		• Apex One 2019 或 OfficeScan 11.0 SP1（或更新版本）
		• Apex One Endpoint Sensor
		• Deep Discovery Email Inspector 3.0（或更新版本）
		• Deep Security Manager 10.0（或更新版本）
		• InterScan Messaging Security Virtual Appliance 9.1（或更新版本）
		• InterScan Web Security Virtual Appliance 6.5 SP2 Patch 4（或更新版本）
		• ScanMail for Microsoft Exchange 12.5（或更新版本）

可疑物件管理	• Apex Central
	• Deep Discovery Inspector 5.0（或更新版本）或下列其中一個沙箱產品：
	  • Apex One Sandbox as a Service
	  • Deep Discovery Analyzer
		• Apex One 2019 或 OfficeScan 11.0 SP1（或更新版本）
		• Apex One Endpoint Sensor
		• Cloud App Security 5.0（或更新版本）
		• Deep Security Manager 10.0（或更新版本）
		• InterScan Messaging Security Virtual Appliance 9.1（或更新版本）
		• InterScan Web Security Virtual Appliance 6.5 SP2 Patch 4（或更新版本）
		• Trend Micro Endpoint Application Control 2.0 SP1（或更新版本）

功能	必要產品	可選產品
可疑物件中毒處理行動 如需詳細資訊，請參閱可疑物件中毒處理行動 第 19-9 頁。	• Apex Central	• Apex One 2019 或 OfficeScan 11.0 SP1（或更新版本） • Cloud App Security 5.0（或更新版本） • Deep Security Manager 10.0（或更新版本） • InterScan Messaging Security Virtual Appliance 9.1（或更新版本） • InterScan Web Security Virtual Appliance 6.5 SP2 Patch 4（或更新版本） • 主動雲端截毒技術伺服器 3.3 Patch 2（或更新版本） • Trend Micro Endpoint Application Control 2.0 SP1（或更新版本）
影響分析	• Apex Central • Apex One Endpoint Sensor 重要 若要在「受影響的使用者」畫面中執行影響分析，則還需要 Deep Discovery Inspector 5.0（或更新版本）。 如需詳細資訊，請參閱對受影響的使用者進行影響分析 第 7-20 頁。	• Deep Discovery Inspector 5.0（或更新版本）

功能	必要產品	可選產品
端點隔離 如需詳細資訊，請參閱隔離端點 第 19-32 頁。	• Apex Central • Apex One 2019 或 OfficeScan 11.0 SP1（或更新版本）	• Apex One Endpoint Sensor
IOC 管理	• Apex Central • Apex One Endpoint Sensor	• 無

可疑物件清單管理

Apex Central 可讓您在受管理產品中同步處理可疑物件清單，並建立使用者定義的清單和例外清單，以進一步控管可疑物件的擴散。您也可以設定支援的受管理產品在您的環境中偵測到可疑物件時，所要採取的特定處理行動。

Apex Central 會整合沙箱與使用者定義的可疑物件清單（不含例外），並將清單與整合的受管理產品同步處理。

如需可與 Apex Central 同步處理可疑物件清單的產品詳細資訊，請參閱功能需求 第 19-2 頁中的〈可疑物件清單同步處理〉。

可疑物件清單

Apex Central 會整合沙箱可疑物件清單，並在多個受管理產品中同步處理所有的可疑物件清單。每個受管理產品實作清單的方式視產品如何實作該功能而定。請參閱受管理產品的《管理手冊》，以取得有關產品如何使用和同步處理可疑物件清單的詳細資訊。

注意

管理員可以使用 Apex Central 主控台，設定對可疑物件所要採取的特定中毒處理行動。然後，您可以設定特定的受管理產品根據「可疑物件」清單設定執行處理行動。

如需詳細資訊，請參閱可疑物件中毒處理行動 第 19-9 頁。

清單類型	說明
沙箱可疑物件	與沙箱整合的受管理產品會提交可疑檔案或 URL 給沙箱來進行分析。如果沙箱判定物件是可能的安全威脅，則沙箱會將物件新增至「可疑物件」清單。沙箱接著會將清單傳送至其已註冊的 Apex Central 伺服器，來進行彙總和同步處理。 在 Apex Central 主控台上，移至「安全威脅資訊 > 沙箱可疑物件 > 物件」標籤，以檢視「沙箱可疑物件」清單。 如需詳細資訊，請參閱可疑物件偵測 第 19-14 頁。
沙箱可疑物件例外	Apex Central 管理員可以從沙箱可疑物件清單中選取認為安全的物件，然後將其新增到例外清單。 在 Apex Central 主控台上，移至「安全威脅資訊 > 沙箱可疑物件 > 例外」標籤，以檢視「沙箱可疑物件例外」清單。 Apex Central 會將例外清單傳送給訂閱此清單的沙箱（不含 Apex One Sandbox as a Service）。當沙箱偵測到可疑物件，而該物件列在例外清單中時，沙箱會將該物件視為「安全」，並且不會再次分析該物件。 如需詳細資訊，請參閱將例外新增到沙箱可疑物件清單 第 19-7 頁。
使用者定義的可疑物件	Apex Central 管理員可以在「安全威脅資訊 > 自訂情報 > 使用者定義的可疑物件」中，新增其認為可疑，但目前不在沙箱可疑物件清單中的物件。 如需詳細資訊，請參閱先發式可疑物件防護 第 19-19 頁。

將例外新增到沙箱可疑物件清單

Apex Central 允許您根據檔案 SHA-1、網域、IP 位址或 URL，將物件從「沙箱可疑物件」清單中排除。

重要

「使用者定義的可疑物件」清單的優先順序高於「沙箱可疑物件」清單。

步驟

1. 移至「安全威脅資訊 > 沙箱可疑物件」。

   會出現「沙箱可疑物件」畫面。

2. 按一下「例外」標籤。

3. 請點選「新增」。

4. 指定物件的「類型」。

   - 檔案：指定檔案的「檔案 SHA-1」雜湊值。
   - IP 位址：指定 IP 位址。
   - URL：指定 URL。
   - 網域：指定網域。

     Apex Central 允許您使用萬用字元 (*) 從沙箱可疑物件清單排除特定子網域或子目錄。

範例	說明
https://*.domain.com/	從「沙箱可疑物件」清單排除網域 “domain.com” 下子網域內的所有 URL **重要** 如果 URL 包含子目錄，則不會排除該 URL，即使該 URL 含有相符的子網域。例如，“https://abc.domain.com/abc” 不會被排除。
*.abc.domain.com	從沙箱可疑物件清單排除子網域 “abc” 的所有子網域

範例	說明
https:// *.domain.com/abc/*	從「沙箱可疑物件」清單排除網域 “domain.com” 下子網域內的所有 URL 以及子目錄 “abc” 的所有子目錄 重要 如果 URL 不包含子目錄 “abc” 內的子目錄，則該 URL 依然會被排除。例如，“https://abc.domain.com/abc” 會被排除。

5. （選用）指定「注意」，協助識別可疑物件。

6. 請點選「新增」。

   物件會顯示在「沙箱例外」清單中。訂閱了可疑物件清單的受管理產品，會在下次同步處理期間接收新的物件資訊。

可疑物件中毒處理行動

管理員可以使用 Apex Central 主控台，設定特定受管理產品在偵測到「沙箱可疑物件」清單或「使用者定義的可疑物件」清單中的特定可疑物件後，所要採取的中毒處理行動。

表 19-1. 中毒處理行動產品支援

產品	沙箱清單	使用者定義的清單
Apex One（任何版本）	對下列可疑物件類型執行處理行動： • 檔案：記錄、封鎖、隔離 • IP 位址：記錄、封鎖 • URL：記錄、封鎖 • 網域：記錄、封鎖	對下列可疑物件類型執行處理行動： • 檔案：記錄、封鎖、隔離 • 檔案 SHA-1：記錄、封鎖 • IP 位址：記錄、封鎖 • URL：記錄、封鎖 • 網域：記錄、封鎖

產品	沙箱清單	使用者定義的清單
OfficeScan XG SP1（或更新版本）	對下列可疑物件類型執行處理行動： • 檔案：記錄、封鎖、隔離 • IP 位址：記錄、封鎖 • URL：記錄、封鎖 • 網域：記錄、封鎖	對下列可疑物件類型執行處理行動： • 檔案：記錄、封鎖、隔離 • IP 位址：記錄、封鎖 • URL：記錄、封鎖 • 網域：記錄、封鎖
Deep Security Manager 10.0（或更新版本）	對下列可疑物件類型執行處理行動： • 檔案：記錄、封鎖、隔離 • URL：記錄、封鎖	對下列可疑物件類型執行處理行動： • 檔案：記錄、封鎖、隔離 • URL：記錄、封鎖
• Deep Discovery Inspector 5.0（或更新版本） • Deep Discovery Email Inspector 3.0（或更新版本）	同步處理下列可疑物件類型： • 檔案：不執行任何中毒處理行動 • IP 位址：不執行任何中毒處理行動 • URL：不執行任何中毒處理行動 • 網域：不執行任何中毒處理行動	同步處理下列可疑物件類型： • 檔案：不執行任何中毒處理行動 • IP 位址：不執行任何中毒處理行動 • URL：不執行任何中毒處理行動 • 網域：不執行任何中毒處理行動
InterScan Messaging Security Virtual Appliance 9.1（或更新版本）	對下列可疑物件類型執行處理行動： • 檔案：記錄、封鎖、隔離	對下列可疑物件類型執行處理行動： • 檔案：記錄、封鎖、隔離 • 檔案 SHA-1：記錄、封鎖、隔離

產品	沙箱清單	使用者定義的清單
InterScan Web Security Virtual Appliance 6.5 SP2 Patch 4（或更新版本）	對下列可疑物件類型執行處理行動： • 檔案：記錄、封鎖、隔離 • 檔案 SHA-1：記錄、封鎖、隔離 • IP 位址：記錄、封鎖 • URL：記錄、封鎖 • 網域：記錄、封鎖	對下列可疑物件類型執行處理行動： • 檔案：記錄、封鎖、隔離 • 檔案 SHA-1：記錄、封鎖、隔離 • IP 位址：記錄、封鎖 • URL：記錄、封鎖 • 網域：記錄、封鎖
Trend Micro Endpoint Application Control 2.0 SP1 Patch 1（或更新版本）	對下列可疑物件類型執行處理行動： • 檔案：記錄、封鎖、隔離	對下列可疑物件類型執行處理行動： • 檔案：記錄、封鎖、隔離 • 檔案 SHA-1：記錄、封鎖、隔離
Cloud App Security 5.0（或更新版本）	對下列可疑物件類型執行處理行動： • 檔案：記錄、封鎖、隔離 • URL：記錄、封鎖	對下列可疑物件類型執行處理行動： • 檔案：記錄、封鎖、隔離 • URL：記錄、封鎖

<table>
<tr><th>產品</th><th>沙箱清單</th><th>使用者定義的清單</th></tr>
<tr><td rowspan="2">主動雲端截毒技術伺服器 3.3 Patch 2（或更新版本）
OfficeScan 11.0 SP1（或更新版本）整合式主動雲端截毒技術伺服器
趨勢科技產品會將網頁信譽評等查詢傳送到支援的主動雲端截毒技術伺服器</td><td>受管理產品在網頁信譽評等查詢期間，會針對下列可疑物件類型執行處理行動：
URL：記錄、封鎖</td><td>受管理產品在網頁信譽評等查詢期間，會針對下列可疑物件類型執行處理行動：
URL：記錄、封鎖
重要
主動雲端截毒技術伺服器會將「使用者定義的可疑物件」清單中的所有 URL 分類為「高」風險。</td></tr>
<tr><td colspan="2">注意
只有特定的受管理產品可以對可疑 URL 物件直接執行 Apex Central 中設定的處理行動。其他受管理產品則會根據產品已設定的「網站信譽評等服務」設定，對可疑 URL 物件採取處理行動。

受管理產品上顯示的記錄檔可能不會包含可疑物件偵測的相關資訊。Apex Central 會解譯從受管理產品傳送的記錄檔，然後在 Apex Central 主控台上顯示可疑物件偵測。</td></tr>
</table>

設定派送設定

設定派送設定，可讓 Apex Central 整合沙箱和使用者定義的可疑物件（不包括例外），並傳送給特定的受管理產品。這些產品會同步處理並使用其中全部或部分物件。

Apex Central 還可將可疑 IP 位址和網域傳送至 TippingPoint。

注意

「派送設定」也允許您設定可疑物件中樞和節點 Apex Central 伺服器設定，來跨多部 Apex Central 伺服器同步處理可疑物件清單。

如需詳細資訊，請參閱可疑物件中樞和節點架構 第 22-1 頁。

步驟

1. 移至「安全威脅資訊 > 派送設定」。

   會出現「派送設定」畫面。

2. 如果要將可疑物件傳送至受管理的產品，請執行下列作業：

   a. 按一下「受管理的產品」標籤。

   b. 選取「傳送可疑物件至受管理的產品」核取方塊。

   c. 記下下列資訊，以便在受管產品中設定 Apex Central 做為沙箱來源時使用：

      - 服務 URL：Apex Central 的服務 URL
      - API 金鑰：用來將 Apex Central 識別為受管理產品的代碼

   d. 按一下「儲存」。

   e. 按一下「立即同步處理」。

3. 如果要將可疑物件傳送至 TippingPoint，請執行下列作業：

   a. 按一下「TippingPoint」標籤。

   b. 選取「傳送可疑物件 (只有 IP 位址和網域名稱) 至 TippingPoint」核取方塊。

      注意

      Apex Central 會傳送沙箱所分析的可疑 IP 位址和網域名稱。TippingPoint 會使用信譽評等過濾器來對整個信譽評等群組套用封鎖、允許或通知等處理行動。如需有關信譽評等過濾器的詳細資訊，請參閱您的 TippingPoint 文件。

   c. 指定下列項目：

      - 伺服器名稱：輸入用於 TippingPoint 部署的伺服器 URL 和通訊埠號碼。
      - 使用者名稱：輸入具有足夠權限可存取 TippingPoint 主控台之帳號的使用者名稱。

- 密碼：輸入帳號的密碼。

d. （選用）按一下「測試連線」，可確認連線。

e. 選取會觸發 Apex Central 將網域名稱或 IP 位址資訊傳送至 TippingPoint 的嚴重性層級。

- 僅有高：具有高嚴重性的 IP 位址和網域名稱
- 中和高：具有高和中嚴重性的 IP 位址和網域名稱
- 全部：具有高、中和低嚴重性的 IP 位址和網域名稱

f. 按一下「儲存」。

g. 按一下「立即同步處理」。

可疑物件偵測

您可以使用 Apex Central 主控台，以多種方式檢視在您環境中偵測到的可疑物件。如需以不同方式檢視偵測到的可疑物件之相關資訊，請參閱下列內容：

- 檢視有風險的端點和收件者 第 19-14 頁
- 分析沙箱可疑物件的影響 第 19-15 頁

注意

Apex Central 只能在環境中識別暴露於可疑物件的使用者或端點。您無法使用 Apex Central 主控台，對任何可疑物件採取任何直接處理行動。

檢視有風險的端點和收件者

Apex Central 會檢查網站信譽評等服務、URL 過濾、網路內容檢測，以及從所有受管理產品收到的基於規則的偵測記錄檔，然後將這些記錄檔與其可疑物件清單進行比較。

步驟

1. 移至「安全威脅資訊 > 沙箱可疑物件」。

   會出現「沙箱可疑物件」畫面。

2. 按一下「物件」標籤。

3. 展開您要檢視的「物件」左側的箭頭。

   - 「有風險的端點」清單會顯示所有仍受可疑物件影響的端點和使用者。
     - 對於「檔案」偵測，「最新處理行動結果」欄會顯示受管理產品回報的上一個處理行動結果。
     - 對於所有其他偵測類型，「最新處理行動結果」欄會顯示「無」。
   - 「有風險的收件者」清單會顯示所有仍受可疑物件影響的收件者。

分析沙箱可疑物件的影響

「沙箱可疑物件」畫面可讓您執行對您網路的影響分析。影響分析會使用 Endpoint Sensor 來聯絡用戶端並對用戶端記錄檔執行歷史掃瞄，以判斷可疑物件是否已影響您的環境一段時間而未被偵測到。

您也可以針對「自訂情報」畫面上使用者定義的可疑物件執行影響分析。

如需詳細資訊，請參閱對使用者定義的可疑物件的 IOC 進行影響分析和回應 第 19-30 頁。

重要

若要執行影響分析，需要有效的 Apex One Endpoint Sensor 使用授權。請確保您的 Apex One Endpoint Sensor 使用授權有效，然後為適當的 Apex One Security Agent 或 Apex One (Mac) 策略啟動「啟動 Sensor」功能。

如需詳細資訊，請參閱《Apex Central Widget 和策略管理手冊》。

步驟

1. 移至「安全威脅資訊 > 沙箱可疑物件」。

   會出現「沙箱可疑物件」畫面。

2. 按一下「物件」標籤。

3. 從清單中選取一或多個物件。

   注意

   Apex Central 不支援對 URL 物件進行影響分析。

4. 按一下「分析影響」。

   Endpoint Sensor 會聯絡用戶端，並評估用戶端記錄檔中是否有任何的可疑物件偵測項目。

   注意

   影響分析時間會視您的網路環境而有不同。

5. 展開您要檢視的「物件」左側的箭頭。

   - 「有風險的端點」清單會顯示所有仍受可疑物件影響的端點和使用者。
     - 對於「檔案」偵測，「最新處理行動結果」欄會顯示受管理產品回報的上一個處理行動結果。
     - 對於所有其他偵測類型，「最新處理行動結果」欄會顯示「無」。
   - 「有風險的收件者」清單會顯示所有仍受可疑物件影響的收件者。

Endpoint Sensor 中的歷史調查

歷史調查會根據指定的條件評估歷史事件和關聯分析。結果可以根本原因分析映射圖（顯示任何可疑活動的執行流程）的形式來檢視。這有助於分析涉及目標式攻擊的企業範圍事件鏈。

歷史調查使用下列物件類型來進行其調查：

- DNS 記錄
- IP 位址
- 檔案名稱
- 檔案路徑
- SHA-1 雜湊值
- MD5 雜湊值
- 使用者帳號

歷史調查會查詢包含端點歷史事件的標準化資料庫。相較於傳統記錄檔，這種方法使用的磁碟空間較少，耗用的資源也不多。

檢視處理程序

「正在處理程序」畫面提供環境中的可疑物件的生命週期總覽，以及可疑物件目前對使用者或端點的影響。

重要

需要有內含沙箱之產品或服務的額外使用授權，才能檢視處理程序。請確定您擁有以下至少一項產品的有效使用授權：

- Apex One Sandbox as a Service
- Deep Discovery Analyzer 6.5（或更新版本）
- Deep Discovery Email Inspector 3.5（或更新版本）
- Deep Discovery Inspector 5.0（或更新版本）

步驟

1. 移至「安全威脅資訊 > 沙箱可疑物件」。

2. 按一下特定可疑物件資料表的「正在處理程序」欄中的「檢視」連結。

   會出現「正在處理程序」畫面。

3. 按一下下列任何標籤，可檢視有關可疑物件的詳細資訊。

標籤	說明
樣本提交	顯示可疑物件的第一次和最近一次分析的相關資訊 Apex Central 與下列產品整合，使用沙箱分析其他受管理產品所提交的可疑物件： • Deep Discovery Analyzer 6.5（或更新版本） • Deep Discovery Email Inspector 3.5（或更新版本） • Deep Discovery Inspector 5.0（或更新版本） 注意 Apex One Sandbox as a Service 不提供「樣本提交」資訊。
分析	顯示沙箱對所提交物件的分析 沙箱會根據使系統面臨危險或損失的可能性來判定可疑物件的風險等級。支援的物件包括檔案（SHA-1 雜湊值）、IP 位址、網域和 URL。 注意 Apex One Sandbox as a Service 不提供「產品」、「產品主機名稱」或「產品 IP 位址」資訊。
發佈	顯示同步處理「可疑物件」清單」的所有產品和上次同步處理時間 Apex Central 會整合沙箱與使用者定義的可疑物件清單（不含例外），並將清單與整合的受管理產品同步處理。

標籤	說明
影響分析與緩和	顯示受可疑物件影響的所有端點和使用者 • 對於「檔案」偵測，「最新處理行動結果」欄會顯示受管理產品回報的上一個處理行動結果。 • 對於所有其他偵測類型，「最新處理行動結果」欄會顯示「無」。 按一下「根本原因分析」連結，可進一步調查物件如何影響使用者或端點。

先發式可疑物件防護

Apex Central 提供各種不同的方法來防範網路中無法識別的可疑物件。使用「使用者定義的可疑物件」清單，或是從 OpenIOC 或 STIX 檔案匯入指標，可以對外部來源所識別的可疑安全威脅採取積極的處理行動。

功能	說明
使用者定義的可疑物件清單	「使用者定義的可疑物件」清單可讓您定義已註冊沙箱在網路上未尚未偵測到的可疑檔案、檔案 SHA-1、IP 位址、URL 和網域物件。 支援的受管理產品如果訂閱了「可疑物件」清單，可以對清單中的物件採取處理行動，防止未知安全威脅的擴散。 如需詳細資訊，請參閱下列主題： • 將物件新增到使用者定義的可疑物件清單 第 19-20 頁 • 可疑物件中毒處理行動 第 19-9 頁 • 對使用者定義的可疑物件的 IOC 進行影響分析和回應 第 19-30 頁

功能	說明
STIX 檔案清單	STIX 檔案清單可讓您匯入 Structured Threat Import Expression (STIX) 檔案，然後將可疑檔案 SHA-1、IP 位址、URL 和網域物件解壓縮到「使用者定義的可疑物件」清單。 如需詳細資訊，請參閱下列主題： • 將 STIX 物件新增至「使用者定義的可疑物件」清單 第 19-22 頁 • 對使用者定義的可疑物件的 IOC 進行影響分析和回應 第 19-30 頁
OpenIOC 檔案清單	OpenIOC 檔案清單可讓您匯入 OpenIOC 檔案，然後將可疑檔案 SHA-1、IP 位址、URL 和網域物件解壓縮到「使用者定義的可疑物件」清單。 如需詳細資訊，請參閱下列主題： • 將 OpenIOC 物件新增至「使用者定義的可疑物件」清單 第 19-25 頁 • 對使用者定義的可疑物件的 IOC 進行影響分析和回應 第 19-30 頁

將物件新增到使用者定義的可疑物件清單

您可以將可疑物件新增到「使用者定義的可疑物件」清單，藉此保護您的網路，防範網路中尚未識別的物件。Apex Central 會為您提供選項，以根據檔案、檔案 SHA-1、網域、IP 位址或 URL 來新增物件。您也可以指定支援的趨勢科技產品在偵測到可疑物件後要執行的中毒處理行動。

如需詳細資訊，請參閱下列主題：

- 匯入使用者定義的可疑物件清單 第 19-22 頁
- 將 OpenIOC 物件新增至「使用者定義的可疑物件」清單 第 19-25 頁
- 將 STIX 物件新增至「使用者定義的可疑物件」清單 第 19-22 頁

步驟

1. 移至「安全威脅資訊 > 自訂情報」。

   會出現「自訂情報」畫面。

2. 按一下「使用者定義的可疑物件」標籤。

   會出現「使用者定義的可疑物件」清單。

3. 請點選「新增」。

4. 指定物件的「類型」。

   - 檔案：按一下「瀏覽」上傳可疑物件檔案。
   - 檔案：指定檔案的「檔案 SHA-1」雜湊值。
   - IP 位址：指定 IP 位址。
   - URL：指定 URL。
   - 網域：指定網域。

5. 指定支援的產品在偵測到物件後採取的「中毒處理行動」。

   - 記錄
   - 封鎖
   - 隔離

   注意

   此中毒處理行動僅適用於「檔案」或「檔案 SHA-1」物件。

6. （選用）指定「注意」，協助識別可疑物件。

7. （選用）指定到期日。

8. 請點選「新增」。

   物件會顯示在「使用者定義的可疑物件」清單中。訂閱了可疑物件清單的受管理產品，會在下次同步處理期間接收新的物件資訊。

匯入使用者定義的可疑物件清單

使用格式正確的 CSV 檔案，將多個可疑物件新增到「使用者定義的可疑物件」清單中。

步驟

1. 移至「安全威脅資訊 > 自訂情報」。

   會出現「自訂情報」畫面。

2. 按一下「使用者定義的可疑物件」標籤。

   會出現「使用者定義的可疑物件」清單。

3. 請點選「匯入」。

4. 選取內含可疑物件清單的 CSV 檔案。

   秘訣

   按一下「下載範例 CSV」連結以取得格式正確的範例 CSV 檔案，這個檔案包含有關建立使用者定義的可疑物件清單的詳細指示。

5. 請點選「匯入」。

   CSV 檔案中的物件會出現在「使用者定義的可疑物件」清單中。訂閱了可疑物件清單的受管理產品，會在下次同步處理期間接收新的物件資訊。

將 STIX 物件新增至「使用者定義的可疑物件」清單

從信任的外部來源（安全性論壇或其他 Deep Discovery Virtual Analyzer 產品）取得格式正確的 Structured Threat Information Expression (STIX) 檔案 (`*.xml`) 後，請將該檔案匯入 Apex Central，以解壓縮可疑檔案 SHA-1、IP 位址、URL 及網域物件到「使用者定義的可疑物件」清單。上傳檔案時，您也可以指定支援的趨勢科技產品在偵測到可疑物件後採取的中毒處理行動。

如需有關手動將可疑物件新增至「使用者定義的可疑物件」清單的詳細資訊，請參閱將物件新增到使用者定義的可疑物件清單 第 19-20 頁。

重要

Apex Central 僅支援上傳格式正確、含有 `*.xml` 副檔名，並且符合下列 STIX 和 Cybox 版本的 STIX 檔案：

- STIX 1.1
- STIX 1.1.1
- STIX 1.2
- Cybox 2.1

注意

匯入 STIX 檔案時，Apex Central 會自動將可疑物件解壓縮到「使用者定義的可疑物件」清單。

步驟

1. 移至「安全威脅資訊 > 自訂情報」。

   會出現「自訂情報」畫面。

2. 按一下「STIX」標籤。

   會出現 STIX 檔案清單。

3. （選用）如果要過濾檔案清單中顯示的檔案，請使用搜尋方塊，以指定「檔案名稱」、「簡短說明」或「來源新增者」欄中所包含的完整或部分字串。

4. 請點選「新增」。

   會出現「新增 STIX 的檔案」畫面。

5. 選取要上傳的 STIX 檔案 (`*.xml`)。

   a. 按一下「選取檔案...」。

   b. 選取一或多個要上傳的檔案。

注意

- 每個檔案的檔案大小上限為 10 MB。
- 同時上傳的檔案總數不能超過 200 個檔案。

c. 請點選「開啟」。

6. （選用）按一下「進階設定」以指定支援的產品在偵測到物件後採取的中毒處理行動。

注意

您也可以針對「使用者定義的可疑物件」清單上的可疑物件設定中毒處理行動。

如需詳細資訊，請參閱可疑物件中毒處理行動 第 19-9 頁。

7. 請點選「新增」。

Apex Central 會上傳所選取的 STIX 檔案，然後將可疑物件解壓縮到「使用者定義的可疑物件」清單。

- 如果要下載特定檔案的複本，請按一下「檔案名稱」欄中的連結。
- 如果要追蹤檔案解壓縮狀態，請使用「指令追蹤」畫面。

  如需詳細資訊，請參閱指令追蹤 第 12-2 頁。

- 如果要在已過濾的「使用者定義的可疑物件」清單檢視上檢視解壓縮後的可疑物件，請按一下「已解壓縮物件」欄中的計數。
- 如果要刪除檔案，請選取至少一個檔案的「檔案名稱」旁的核取方塊，然後按一下「刪除」。

注意

- 刪除檔案並不會將解壓縮後的可疑物件從「使用者定義的可疑物件」清單中移除。
- 在 Apex Central 完成解壓縮檔案中的可疑物件後，您才能刪除檔案。

將 OpenIOC 物件新增至「使用者定義的可疑物件」清單

您可以匯入格式正確的 OpenIOC 檔案 (`*.ioc`)，然後將可疑檔案 SHA-1、IP 位址、URL 及網域物件解壓縮到「使用者定義的可疑物件」清單，藉此保護您的網路，防範網路中尚未識別的物件。上傳檔案時，您可以指定受支援趨勢科技產品在偵測到可疑物件後要執行的中毒處理行動。上傳 OpenIOC 檔案後，您也可以選取上傳的檔案做為歷史調查或即時調查的評估條件。

如需有關手動將可疑物件直接新增至「使用者定義的可疑物件」清單的詳細資訊，請參閱將物件新增到使用者定義的可疑物件清單 第 19-20 頁。

重要

Apex Central 僅支援 OpenIOC 1.0。

注意

依預設，在完成 OpenIOC 檔案上傳時，Apex Central 會自動將可疑物件解壓縮到「使用者定義的可疑物件」清單。

或者，您可以選擇先上傳 OpenIOC 檔案，然後於檔案上傳完成後再手動解壓縮可疑物件。

步驟

1. 移至「安全威脅資訊 > 自訂情報」。

   會出現「自訂情報」畫面。

2. 按一下「OpenIOC」標籤。

   會出現 OpenIOC 檔案清單。

3. （選用）如果要過濾檔案清單中顯示的檔案，請使用搜尋方塊，以指定「檔案名稱」、「簡短說明」或「來源新增者」欄中所包含的完整或部分字串。

4. 請點選「新增」。

會出現「新增 OpenIOC 檔案」畫面。

5. 選取要上傳的 OpenIOC 檔案 (`*.ioc`)。

   a. 按一下「選取檔案...」。

   b. 選取一或多個要上傳的檔案。

   注意

   - 每個檔案的檔案大小上限為 10 MB。
   - 同時上傳的檔案總數不能超過 200 個檔案。
   - 在「使用者定義的可疑物件」清單中，每個可疑物件類型的物件數目上限不能超過針對各類型規定的 10,000 個物件。

     如果達到可疑物件類型的物件數目上限，該可疑物件類型的解壓縮工作將不會成功。

   c. 請點選「開啟」。

6. （選用）按一下「進階設定」來設定下列設定：

   - 如果要上傳檔案而不會自動解壓縮可疑物件，請不勾選「將檔案 SHA-1、IP 位址、URL 和網域物件解壓縮到使用者定義的可疑物件清單」核取方塊。

     注意

     如果您在上傳檔案時關閉了自動解壓縮功能，則您仍可以在檔案上傳完成後手動解壓縮物件。

   - 指定支援的產品在偵測到物件後要執行的中毒處理行動。

     注意

     您也可以針對「使用者定義的可疑物件」清單上的可疑物件設定中毒處理行動。

     如需詳細資訊，請參閱可疑物件中毒處理行動 第 19-9 頁。

7. 請點選「新增」。

秘訣

- 如果要追蹤檔案上傳狀態，請使用「使用者存取」記錄類型執行記錄查詢。

  如需詳細資訊，請參閱查詢記錄檔 第 15-2 頁。

- 如果要追蹤可疑物件解壓縮狀態，請使用「指令追蹤」畫面。

  如需詳細資訊，請參閱指令追蹤 第 12-2 頁。

Apex Central 會將所選取的 OpenIOC 檔案上傳至 OpenIOC 檔案清單。

注意

- 如果選取了預設設定，則 Apex Central 會自動將可疑物件解壓縮到「使用者定義的可疑物件」清單。
- OpenIOC 檔案清單中的「已解壓縮物件」欄會針對以下情況顯示「無」：
  - 上傳 OpenIOC 檔案而不自動解壓縮可疑物件。
  - Apex Central 無法從 OpenIOC 檔案中解壓縮可疑物件。

8. 如果要手動從上傳的 OpenIOC 檔案中解壓縮可疑物件，請執行下列作業：

   a. 選取所上傳檔案的「檔案名稱」旁的核取方塊。

   b. 按一下「解壓縮」。

      「已解壓縮物件」欄會顯示從 OpenIOC 檔案解壓縮到「使用者定義的可疑物件」清單的可疑物件數目。

      - 如果要下載特定檔案的複本，請按一下「檔案名稱」欄中的連結。
      - 如果要追蹤檔案解壓縮狀態，請使用「指令追蹤」畫面。

        如需詳細資訊，請參閱指令追蹤 第 12-2 頁。

      - 如果要在已過濾的「使用者定義的可疑物件」清單檢視上檢視解壓縮後的可疑物件，請按一下「已解壓縮物件」欄中的計數。

- 如果要刪除檔案，請選取至少一個檔案的「檔案名稱」旁的核取方塊，然後按一下「刪除」。

注意

- 刪除檔案並不會將解壓縮後的可疑物件從「使用者定義的可疑物件」清單中移除。
- 在 Apex Central 完成解壓縮檔案中的可疑物件後，您才能刪除檔案。

9. 如果要使用上傳的 OpenIOC 檔案做為評估條件來啟動安全威脅調查，請執行下列作業：

重要

- 若要執行安全威脅調查，需要有效的 Endpoint Sensor 使用授權。請確保您的 Endpoint Sensor 使用授權有效，或聯絡您的服務供應商來取得啟動碼。
- 在啟動您的 Endpoint Sensor 使用授權之後，請藉由在「策略管理」畫面上（「策略 > 策略管理」）建立 Apex One 用戶端策略或 Apex One (Mac) 策略，來啟動 Endpoint Sensor 功能。

  如需詳細資訊，請參閱《Apex Central Widget 和策略管理手冊》。

a. 選取所上傳檔案的「檔案名稱」旁的核取方塊。

b. 執行下列其中一種類型的安全威脅調查：

調查	說明
歷史調查	歷史調查會使用伺服器中繼資料，來識別可能需要進一步分析的候選端點。 將滑鼠游標暫留在「分析影響」按鈕上，然後按一下「歷史調查」。 注意 您也可以從「歷史調查」畫面（回應 > 歷史調查）執行歷史調查。 如需詳細資訊，請參閱使用使用者定義的條件進行歷史調查 第 20-5 頁。 如需有關用於歷史調查之伺服器中繼資料的特定資訊，請參閱 Endpoint Sensor 中繼資料 第 20-2 頁。
一次性調查	「一次性調查」是指隨需產生的即時調查，它會調查目前位於磁碟上的所有檔案和目前在記憶體中執行的所有程序。 將滑鼠游標暫留在「分析影響」按鈕上，然後移至「即時調查 > 一次性」。 注意 您也可以從「即時調查」畫面（「回應 > 即時調查）的「一次性調查」標籤執行一次性調查。 如需詳細資訊，請參閱一次性調查 第 20-24 頁。

調查	說明
預約調查	「預約調查」是指依指定時間間隔自動執行的即時調查。 將滑鼠游標暫留在「分析影響」按鈕上，然後移至「即時調查 > 預約」。 注意 您也可以從「即時調查」畫面（「回應 > 即時調查）的「預約調查」標籤執行預約調查。 如需詳細資訊，請參閱預約調查 第 20-26 頁。

對使用者定義的可疑物件的 IOC 進行影響分析和回應

將可疑物件或格式正確的 IOC（STIX 或 OpenIOC）檔案新增至 Apex Central 後，您可以選取特定檔案、檔案 SHA-1、IP 位址或網域物件，來執行影響分析，藉此判斷您的網路是否存在安全威脅，並採取緩和措施來防止安全威脅擴散到其他端點。

如需詳細資訊，請參閱下列主題：

- 匯入使用者定義的可疑物件清單 第 19-22 頁
- 將 OpenIOC 物件新增至「使用者定義的可疑物件」清單 第 19-25 頁
- 將 STIX 物件新增至「使用者定義的可疑物件」清單 第 19-22 頁

重要

- 若要執行影響分析，需要有效的 Apex One Endpoint Sensor 使用授權。請確保您的 Apex One Endpoint Sensor 使用授權有效，然後為適當的 Apex One Security Agent 或 Apex One (Mac) 策略啟動「啟動 Sensor」功能。

  如需詳細資訊，請參閱《Apex Central Widget 和策略管理手冊》。

- 如果要隔離端點，會要求您在目標端點上安裝 Apex One Security Agent。

步驟

1. 移至「安全威脅資訊 > 自訂情報」。

   會出現「自訂情報」畫面。

2. 按一下「使用者定義的可疑物件」標籤。

   會出現「使用者定義的可疑物件」清單。

3. 從清單中選取一或多個物件。

   注意

   Apex Central 不支援對 URL 物件進行影響分析。

4. 按一下「分析影響」。

   Endpoint Sensor 會聯絡用戶端，並評估用戶端記錄檔中是否有任何的可疑物件偵測項目。

   注意

   影響分析時間會視您的網路環境而有不同。

5. 展開您要檢視的「物件」左側的箭頭。

   - 「有風險的端點」清單會顯示所有仍受可疑物件影響的端點和使用者。
     - 對於「檔案」偵測，「最新處理行動結果」欄會顯示受管理產品回報的上一個處理行動結果。

- 對於所有其他偵測類型，「最新處理行動結果」欄會顯示「無」。

- 「有風險的收件者」清單會顯示所有仍受可疑物件影響的收件者。

隔離端點

隔離有風險的端點，以執行調查並解決安全問題。解決所有問題後，立即恢復連線。

重要

- 端點隔離需要有效的 Apex Central 使用授權。
- 如果是執行 11 SP1 到 XG SP1 版本的 OfficeScan 用戶端，您必須啟動 OfficeScan 防火牆，才能執行端點隔離。

步驟

1. 移至「目錄 > 使用者/端點」。
2. 選取以檢視端點。
3. 按一下清單中某個端點的名稱。
4. 在出現的「端點」資訊畫面中，按一下「工作 > 隔離」。

   Apex Central 會因以下原因而關閉端點上的「隔離」選項：

   - 端點上的用戶端執行不受支援的版本。
   - 用於登入 Apex Central 的使用者帳號沒有必要權限。
5. 「端點」資訊畫面頂端會顯示一則訊息，可讓您監控隔離狀態。隔離完成後，訊息會關閉，並在目標端點上顯示一則通知來通知使用者。

   如果隔離過程中發生問題，「端點 — {名稱}」畫面頂端的訊息會通知您發生問題。

6. 如果要檢視您的 Apex Central 網路中所有已隔離的端點，請在「使用者/端點目錄」樹狀結構中按一下「端點 > 過濾器 > 網路內容 > 已隔離」節點。

7. （選用）如果要為所有已隔離端點設定允許的輸入和輸出流量，請執行下列作業：

   a. 選取「控制已隔離端點的流量」。

   b. 展開「輸入流量」或「輸出流量」區段。

   c. 透過指定「通訊協定」、「IP 位址」和「目標通訊埠」，指定允許的流量。

      使用逗號分隔多個目標通訊埠。

   d. 按一下「目標通訊埠」資訊右側的 - 控制項，以新增多個輸入和輸出項目。

注意

修改允許的流量設定後，所有先前隔離的端點和稍後隔離的任何端點，都會套用輸入和輸出流量設定。

---

8. 在解決已隔離端點上的安全威脅後，請從下列位置恢復網路連線：

   - 「端點」資訊畫面：按一下「工作 > 恢復」。
   - 端點 > 過濾器 > 網路連線 > 已隔離：在資料表中選取端點列，然後按一下「工作 > 恢復網路連線」。

9. 畫面頂端會顯示一則訊息，可讓您監控恢復狀態。恢復完成後，訊息會關閉，並在目標端點上顯示一則通知來通知使用者。

   如果恢復過程中發生問題，畫面頂端的訊息會通知您發生問題。

連線的威脅防範產品整合

連線的威脅防範策略整合許多趨勢科技產品。下圖說明主要產品的互動方式。

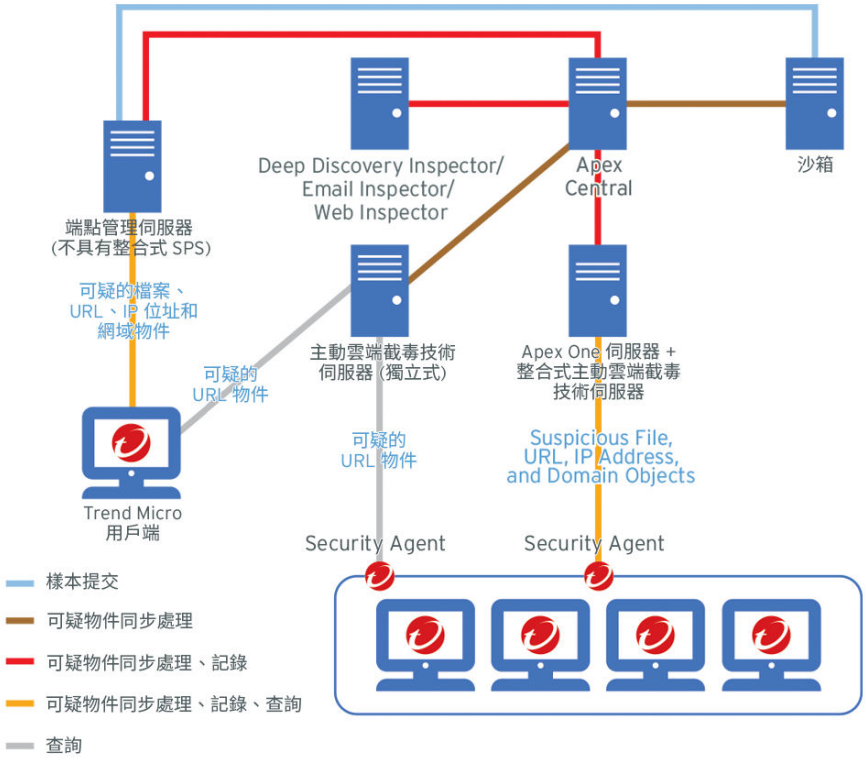


圖 19-1. 端點防護範例拓撲

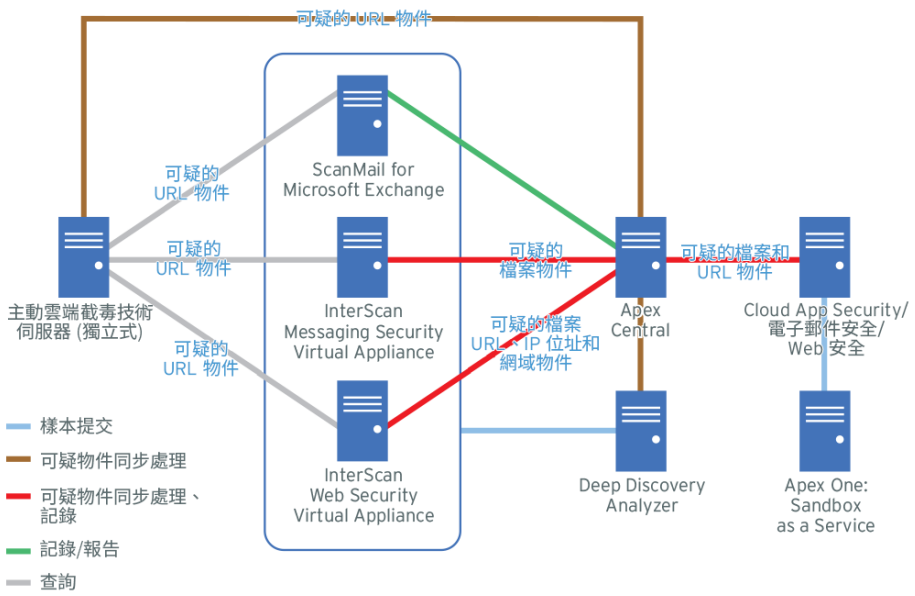


圖 19-2. 傳訊和網路安全範例拓撲

Apex Central 會透過記錄檔分析，並將偵測到的檔案與已同步處理的可疑物件清單進行比較，來進一步監控其他已註冊的趨勢科技產品。

如需每個主要產品的 Apex Central 註冊資訊和可疑物件清單同步處理資訊，請參閱下列內容：

Apex Central

需求	說明
產品版本	• Apex Central（任何版本） • Control Manager 7.0（或更新版本）

需求	說明
Apex Central 註冊	對於未透過 Apex Central 主控台向 Apex Central 註冊的產品，需要下列 Apex Central 註冊資訊： • 伺服器 FQDN 或 IP 位址 • 通訊埠：依預設，Apex Central 會使用 HTTP 通訊埠 80 或 HTTPS 通訊埠 443 對於使用 Apex Central 管理主控台進行註冊的產品，請移至「管理 > 受管理的伺服器 > 伺服器註冊」，接著從「伺服器類型」清單中選取產品，然後按一下「新增」。
可疑物件清單同步處理	對於不會自動將「可疑物件」清單與 Apex Central 同步處理的產品，需要下列 API 資訊： • API 金鑰：如果要取得 API 金鑰，請開啟 Apex Central 管理主控台並移至「安全威脅資訊 > 派送設定」。
整合式連線的威脅防範功能	• 安全威脅監控 • 可疑物件清單同步處理 • 可疑物件管理 • 影響分析 • 端點隔離 • IOC 管理

Apex One

需求	說明
產品版本	• Apex One 2019 • OfficeScan 11.0 SP1（或更新版本）

需求	說明
Apex Central 註冊	從 Apex One Web 主控台的「管理 > 設定 > Apex Central」 需要的 Apex Central 資訊： • 伺服器 FQDN 或 IP 位址 • 通訊埠：依預設，Apex Central 會使用 HTTP 通訊埠 80 或 HTTPS 通訊埠 443 如需詳細資訊，請參閱《Apex One 管理手冊》。
可疑物件清單同步處理	從 Apex One Web 主控台的「管理 > 設定 > 可疑物件清單」 需要的 Apex Central 資訊： • 無 注意 Apex One 會在 Apex Central 註冊期間自動從 Apex Central 伺服器取得所需的 API 金鑰資訊
整合式連線的威脅防範功能	• 安全威脅監控 • 可疑物件清單同步處理 • 可疑物件管理 • 端點隔離

Apex One Endpoint Sensor

需求	說明
啟動碼	需要額外的使用授權。請洽詢您的服務供應商來取得啟動碼。
啟動功能	從 Apex Central 管理主控台啟動 Endpoint Sensor。移至「策略 > 策略管理」，然後從「產品」下拉式清單中選取「Apex One Security Agent」來建立或修改策略。展開「Endpoint Sensor 設定」，然後選取「啟動 Endpoint Sensor」核取方塊。 如需詳細資訊，請參閱《Apex Central Widget 和策略管理手冊》。

需求	說明
可疑物件清單同步處理	Apex One Endpoint Sensor 不會與 Apex Central 同步處理「可疑物件」清單
整合式連線的威脅防範功能	• 安全威脅監控 • 可疑物件樣本提交 • 可疑物件管理 • 影響分析 • 端點隔離 • IOC 管理

Apex One Sandbox as a Service

需求	說明
啟動碼	需要額外的使用授權。請洽詢您的服務供應商來取得啟動碼。
Apex Central 註冊	從 Apex Central 管理主控台完成註冊。移至「管理 > 使用授權管理 > Apex Central」，然後在 「Apex One Sandbox as a Service」區段中按一下「指定新啟動碼」來提供及啟動「啟動碼」。
可疑物件清單同步處理	向 Apex Central 註冊後自動執行 依預設，「可疑物件」清單會每隔 10 分鐘與 Apex Central 伺服器同步處理一次。
整合式連線的威脅防範功能	• 安全威脅監控 • 可疑物件清單同步處理 • 可疑物件樣本提交 • 可疑物件管理

Cloud App Security

需求	說明
產品版本	5.0（或更新版本）
Apex Central 註冊	從 Apex Central 管理主控台完成註冊。移至「管理 > 受管理的伺服器 > 伺服器註冊」，接著從「伺服器類型」清單中選取產品，然後按一下「新增」。
可疑物件清單同步處理	如需詳細資訊，請參閱《Cloud App Security 線上說明》。
整合式連線的威脅防範功能	• 安全威脅監控 • 可疑物件清單同步處理 • 可疑物件管理 • 可疑物件中毒處理行動

Deep Discovery Analyzer

需求	說明
產品版本	6.5（或更新版本）
Apex Central 註冊	從 Apex Central 管理主控台完成註冊。移至「管理 > 受管理的伺服器 > 伺服器註冊」，接著從「伺服器類型」清單中選取產品，然後按一下「新增」。
可疑物件清單同步處理	向 Apex Central 註冊後自動執行 依預設，「可疑物件」清單會每隔 10 分鐘與 Apex Central 伺服器同步處理一次。
整合式連線的威脅防範功能	• 安全威脅監控 • 可疑物件清單同步處理 • 可疑物件樣本提交 • 可疑物件管理

Deep Discovery Director

需求	說明
產品版本	5.0（或更新版本）
Apex Central 註冊	從 Apex Central 管理主控台完成註冊。移至「管理 > 受管理的伺服器 > 伺服器註冊」，接著從「伺服器類型」清單中選取產品，然後按一下「新增」。
可疑物件清單同步處理	向 Apex Central 註冊後自動執行 依預設，「可疑物件」清單會每隔 10 分鐘與 Apex Central 伺服器同步處理一次。
整合式連線的威脅防範功能	• 安全威脅監控 • 可疑物件清單同步處理 • 可疑物件樣本提交 • 可疑物件管理

Deep Discovery Email Inspector

需求	說明
產品版本	3.5（或更新版本）
Apex Central 註冊	如需詳細資訊，請參閱《Deep Discovery Email Inspector 管理手冊》。
可疑物件清單同步處理	如需詳細資訊，請參閱《Deep Discovery Email Inspector 管理手冊》。
整合式連線的威脅防範功能	• 可疑物件清單同步處理 • 可疑物件樣本提交

Deep Discovery Inspector

需求	說明
產品版本	5.0（或更新版本）
Apex Central 註冊	從 Deep Discovery Inspector 管理主控台（「管理 > 整合的產品/服務 > Apex Central」） 需要的 Apex Central 資訊： • 伺服器 FQDN 或 IP 位址 • 通訊埠：依預設，Apex Central 會使用 HTTP 通訊埠 80 或 HTTPS 通訊埠 443 如需詳細資訊，請參閱《Deep Discovery Inspector 管理手冊》。
可疑物件清單同步處理	從 Deep Discovery Inspector 管理主控台（「管理 > 整合的產品/服務 > Apex Central」） 需要的 Apex Central 資訊： • API 金鑰：如果要取得 API 金鑰，請開啟 Apex Central 管理主控台並移至「安全威脅資訊 > 派送設定」。 如需詳細資訊，請參閱《Deep Discovery Inspector 管理手冊》。
整合式連線的威脅防範功能	• 安全威脅監控 • 可疑物件清單同步處理 • 可疑物件樣本提交 • 可疑物件管理

Deep Discovery Web Inspector

需求	說明
產品版本	2.5（或更新版本）

需求	說明
Apex Central 註冊	如需詳細資訊，請參閱《Deep Discovery Web Inspector 管理手冊》。
可疑物件清單同步處理	如需詳細資訊，請參閱《Deep Discovery Web Inspector 管理手冊》。
整合式連線的威脅防範功能	• 可疑物件清單同步處理 • 可疑物件樣本提交

Deep Security Manager

重要

Deep Security as a Service 不支援連線的威脅防範。只有 Deep Security Manager 內部部署伺服器支援「連線的威脅防範」功能。

需求	說明
產品版本	10.0（或更新版本）
Apex Central 註冊	從 Apex Central 管理主控台完成註冊。移至「管理 > 受管理的伺服器 > 伺服器註冊」，接著從「伺服器類型」清單中選取產品，然後按一下「新增」。
可疑物件清單同步處理	向 Apex Central 註冊後自動執行
整合式連線的威脅防範功能	• 安全威脅監控 • 可疑物件清單同步處理 • 可疑物件樣本提交 • 可疑物件管理 • 可疑物件中毒處理行動

Email Security

需求	說明
Apex Central 註冊	從 Apex Central 管理主控台完成註冊。移至「管理 > 受管理的伺服器 > 伺服器註冊」，接著從「伺服器類型」清單中選取產品，然後按一下「新增」。
可疑物件清單同步處理	如需詳細資訊，請參閱《Email Security 管理員主控台線上說明》。
整合式連線的威脅防範功能	• 安全威脅監控 • 可疑物件清單同步處理 • 可疑物件管理 • 可疑物件中毒處理行動

InterScan Messaging Security Virtual Appliance

需求	說明
產品版本	9.1（或更新版本）
Apex Central 註冊	如需詳細資訊，請參閱《InterScan Messaging Security Virtual Appliance 管理手冊》。
可疑物件清單同步處理	向 Apex Central 註冊後自動執行
整合式連線的威脅防範功能	• 安全威脅監控 • 可疑物件清單同步處理 • 可疑物件樣本提交 • 可疑物件管理 • 可疑物件中毒處理行動

InterScan Web Security Virtual Applicance

需求	說明
產品版本	6.5 SP2 Patch 4（或更新版本）
Apex Central 註冊	如需詳細資訊，請參閱《InterScan Web Security Virtual Appliance 管理手冊》。
可疑物件清單同步處理	如需詳細資訊，請參閱《InterScan Web Security Virtual Appliance 管理手冊》。
整合式連線的威脅防範功能	• 安全威脅監控 • 可疑物件清單同步處理 • 可疑物件樣本提交 • 可疑物件管理 • 可疑物件中毒處理行動

ScanMail for Microsoft Exchange

需求	說明
產品版本	12.5（或更新版本）
Apex Central 註冊	如需詳細資訊，請參閱《ScanMail for Microsoft Exchange 管理手冊》。
可疑物件清單同步處理	如需詳細資訊，請參閱《ScanMail for Microsoft Exchange 管理手冊》。
整合式連線的威脅防範功能	• 安全威脅監控 • 可疑物件樣本提交

主動雲端截毒技術伺服器

需求	說明
產品版本	3.3 Patch 2（或更新版本）
Apex Central 註冊	從 Apex Central 管理主控台完成註冊。移至「管理 > 受管理的伺服器 > 伺服器註冊」，接著從「伺服器類型」清單中選取產品，然後按一下「新增」。
可疑物件清單同步處理	從主動雲端截毒技術伺服器 Web 主控台中，移至「主動雲端截毒技術 > 可疑物件」。 「可疑物件」清單來源的必要詳細資訊： • 服務 URL • 通訊埠 如果清單來源是 Apex Central，則預設的通訊埠為 HTTP 通訊埠 80 或 HTTPS 通訊埠 443。 • API 金鑰：由伺服器管理員提供 如果清單來源是 Apex Central，則開啟 Apex Central 管理主控台並移至「管理 > 可疑物件 > 派送設定」。 **注意** 在主動雲端截毒技術伺服器 3.3 （或更新版本）中，Apex Central 會在註冊期間自動傳送必要的 API 金鑰資訊到主動雲端截毒技術伺服器。 如需詳細資訊，請參閱《主動雲端截毒技術伺服器管理手冊》。
整合式連線的威脅防範功能	• 可疑物件清單同步處理 • 可疑物件中毒處理行動

Endpoint Application Control

需求	說明
產品版本	2.0 SP1 Patch 1（或更新版本）
Apex Central 註冊	從 Apex Central 管理主控台完成註冊。移至「管理 > 受管理的伺服器 > 伺服器註冊」，接著從「伺服器類型」清單中選取產品，然後按一下「新增」。
可疑物件清單同步處理	向 Apex Central 註冊後自動執行
整合式連線的威脅防範功能	• 安全威脅監控 • 可疑物件清單同步處理 • 可疑物件管理

Web 安全

需求	說明
Apex Central 註冊	從 Apex Central 管理主控台完成註冊。移至「管理 > 受管理的伺服器 > 伺服器註冊」，接著從「伺服器類型」清單中選取產品，然後按一下「新增」。
可疑物件清單同步處理	如需詳細資訊，請參閱《Web 安全線上說明》。
整合式連線的威脅防範功能	• 安全威脅監控 • 可疑物件清單同步處理 • 可疑物件管理 • 可疑物件中毒處理行動

第 20 章

安全威脅調查

本節討論如何使用「安全威脅調查」執行調查並分析結果。

包含下列主題：

- 安全威脅調查總覽 第 20-2 頁
- 歷史調查 第 20-3 頁
- 即時調查 第 20-21 頁
- 調查結果 第 20-30 頁

安全威脅調查總覽

使用「安全威脅調查」可尋找網路中的可疑物件。

「安全威脅調查」可以關聯來自 Endpoint Sensor 和 Active Directory 的資訊，以顯示整個網路中的端點和使用者帳號的相關攻擊資訊。

如果網路是進行中的攻擊或 APT 的目標時，安全威脅調查可以：

- 評估目標式攻擊造成的損害範圍
- 提供有關攻擊到達和進展的資訊
- 協助規劃有效的安全事件回應

可供使用的安全威脅調查類型如下：

- 歷史調查可以快速識別出哪些可能的候選端點需要進一步分析。歷史調查會使用伺服器中繼資料來快速傳回結果。

  如需詳細資訊，請參閱歷史調查 第 20-3 頁。

- 即時調查會對目前的系統狀態執行調查。即時調查可設定為在特定期間執行，也支援透過使用 OpenIOC 和 YARA 規則來擴大條件組。

  如需詳細資訊，請參閱即時調查 第 20-21 頁。

Endpoint Sensor 中繼資料

中繼資料是指從端點收集再上傳至伺服器的資料。在歷史調查期間，Endpoint Sensor 會利用上述資料來識別受影響的端點。

如需詳細資訊，請參閱歷史調查 第 20-3 頁。

收集的中繼資料類型，視端點上安裝的作業系統而定。

表 20-1. 按作業系統的中繼資料

作業系統	中繼資料	
Windows	• 主機（名稱/IP 位址） • 使用者帳號 • 檔案名稱 • 檔案路徑 • 雜湊值（SHA-1、SHA-256 和 MD5）	• 登錄機碼 • 登錄資料 • 登錄名稱 • 指令行 • URL
macOS	• 主機（名稱/IP 位址） • 使用者帳號 • 檔案名稱 • URL	• 檔案路徑 • 雜湊值（SHA-1、SHA-256 和 MD5） • 指令行

注意

- URL 收集僅適用於處理回呼事件，並且只支援 HTTP 通訊協定。
- 使用「策略管理」畫面可進行中繼資料設定。
- 在歷史調查期間提供的資料是 Security Agent 資料的子集，並且僅包含有關高風險檔案類型的資訊。如果評估未傳回任何結果，則您可以執行即時調查。

歷史調查

歷史調查可以快速識別出哪些可能的候選端點需要進一步分析。歷史調查會使用伺服器中繼資料來快速傳回結果。

若要存取此畫面，請移至「回應 > 歷史調查」。

「歷史調查」畫面提供兩個標籤：

標籤	說明
評估	可以使用評估執行下列作業： • 評估安全威脅的普遍程度，以及安全威脅已在網路中存在多長時間。評估範圍涵蓋所有歷史資料。 • 使用簡單的條件判定安全威脅存在與否。評估僅支援一組有限的條件。 評估支援下列條件類型： • 使用者定義：指定或載入最多 10 個使用者定義的條件，或載入 C&C 回呼事件。 如需詳細資訊，請參閱使用者定義的條件支援的格式 第 20-9 頁。 • OpenIOC 檔案：使用 OpenIOC 規則定義調查條件。歷史調查會略過所有條件，並比對 OpenIOC 檔案中指定的任何指標。 如需詳細資訊，請參閱歷史調查支援的 IOC 指標 第 20-16 頁。 評估範圍涵蓋整個伺服器中繼資料，並且會在一找到相符項目時立即更新結果窗格。可能需要數分鐘才能完成對整個伺服器中繼資料的評估。 如需詳細資訊，請參閱使用使用者定義的條件進行歷史調查 第 20-5 頁。
根本原因分析結果	如果評估傳回相符項目，則管理員可產生根本原因分析來執行下列作業： • 列出所有與指定條件相關的物件 • 識別是否有任何相關物件值得注意 • 檢閱導致相符物件執行的一系列事件。 產生根本原因分析可能需要一些時間才能完成。使用「根本原因分析」標籤可監控工作進度。 如需詳細資訊，請參閱關聯分析 第 20-32 頁。

使用使用者定義的條件進行歷史調查

注意

如果要對目前的系統狀態執行調查，請使用「即時調查」。

如需詳細資訊，請參閱啟動一次性調查 第 20-22 頁。

步驟

1. 移至「回應 > 歷史調查」。
2. 按一下「使用者定義」。
3. 選取下列其中一個選項：
   - 符合所有條件：尋找符合所有指定條件的物件
   - 符合任何條件：尋找符合任一指定條件的物件
4. 按一下「新條件」，然後選取條件類型並指定有效的資訊。

   如需詳細資訊，請參閱使用者定義的條件支援的格式 第 20-9 頁。

   如果要管理條件，請執行下列作業：
   - 按一下「重設」以清除所有指定的條件。
   - 若要儲存條件供未來調查使用，請按一下 並指定條件名稱。

   注意

   歷史調查支援最多 10 個儲存的使用者定義的條件。

5. （選用）若要載入現有的使用者定義的條件，請按一下「選取條件」。
   a. 按一下「是」。

      注意

      套用現有條件會覆寫目前指定的任何條件。

b. 移至「已儲存的條件」標籤。

c. 選取條件。

如果要管理條件，請執行下列作業：

- 使用「上次使用」欄排序條件。
- 使用「刪除」圖示刪除已儲存的條件。

d. 按一下「新增已儲存的條件」。

6. （選用）若要載入 C&C 回呼事件，請按一下「選取條件」。

a. 按一下「是」。

注意

套用現有條件會覆寫目前指定的任何條件。

b. 移至「C&C 回呼事件」標籤。

c. 選取條件。

按一下「期間」以按指定的時間過濾 C&C 回呼事件。

d. 按一下「載入 C&C 回呼事件」。

注意

「記錄查詢」畫面提供有關 C&C 回呼事件的其他詳細資料，以供您在選取前需要檢閱時使用。若要移至「記錄查詢」畫面，請瀏覽至「偵測 > 記錄檔 > 記錄查詢」，然後依「網路事件 > C&C 回呼」進行過濾。

7. 按一下「評估」。

8. 在「結果」窗格中檢閱顯示的結果。

注意

- 留出一些時間供歷史調查執行。在中繼資料中發現相符物件，調查就會立即在結果表格尾端附加更多列。調查可能需要數分鐘才能完成。
- 在歷史調查期間提供的資料是 Security Agent 資料的子集，並且僅包含有關高風險檔案類型的資訊。如果評估未傳回任何結果，則您可以執行即時調查。

提供下列詳細資料：

欄名稱	說明
端點	包含相符物件的端點名稱 按一下可檢視有關端點的更多詳細資料。
狀態	端點的目前連線狀態
IP 位址	包含相符物件的端點 IP 位址 IP 位址是由網路指派
作業系統	端點所使用的作業系統
使用者	Security Agent 首次記錄相符物件時已登入的使用者之使用者名稱 按一下使用者名稱可檢視有關使用者的更多詳細資料。
管理伺服器	管理受影響端點的伺服器
首次發現	Security Agent 首次記錄相符物件時的日期和時間

欄名稱	說明
詳細資訊	按一下此圖示可開啟「比對詳細資料」畫面。 「比對詳細資料」畫面會顯示下列詳細資料： • 條件：評估中使用的條件 • 首次發現：Security Agent 首次記錄相符物件時的日期和時間 • CLI/登錄出現次數：在命令列或登錄項目中發現的相符項目數目 按一下值可顯示更多詳細資料。 • 分級：趨勢科技資訊所指派的分級 您可以在 Threat Connect 或 VirusTotal 中進一步檢查分級為「惡意」的物件。 • 受影響的端點：當分級為「惡意」時，代表在其中發現類似相符項目的端點數目 此計數僅計入過去 90 天內受影響的端點。
星號 (*)	表示某個端點已標記為「重要」

9. 識別並選取需要進一步處理行動的一或多個端點。

注意

歷史調查結果可能包含 macOS 端點。由於 macOS 端點沒有可用的處理行動，因此這些端點的核取方塊均處於關閉狀態。

處理行動	說明
產生根本原因分析	產生根本原因分析，以檢閱導致相符物件執行的一系列事件。 如需詳細資訊，請參閱從評估啟動根本原因分析 第 20-17 頁。

處理行動	說明
啟動即時調查	使用相同條件對目前系統狀態執行新調查。 **重要** 僅適用於安裝在 Windows 平台上的 Security Agent。 會出現「即時調查」畫面，並使用現有的條件啟動全新的一次性調查。 如果使用使用者定義的條件進行評估，「即時調查」僅會使用選取的端點做為條件 如需詳細資訊，請參閱啟動一次性調查 第 20-22 頁。
隔離端點	中斷所選端點與網路的連線。 **重要** 僅適用於安裝在 Windows 平台上的 Security Agent。 在解決已隔離端點上的安全威脅後，「目錄 > 使用者/端點」畫面上的下列位置會提供選項，讓您恢復已隔離端點的網路連線： • 端點 > 全部：按一下資料表中某個端點的名稱，然後在出現的畫面上按一下「工作 > 恢復」。 • 端點 > 過濾器 > 網路連線 > 已隔離：在資料表中選取端點列，然後按一下「工作 > 恢復網路連線」。

使用者定義的條件支援的格式

重要

如果您的環境同時管理 Apex One 內部部署和 Apex One as a Service Security Agent，則部分功能可能與 Apex One as a Service 有所不同。Apex One as a Service Security Agent 會繼續傳送資料到趨勢科技伺服器，但調查功能可能與 Apex Central as a Service 主控台不同。

類型	項目
使用者名稱 （僅完全相符）	指定 Active Directory 帳號或本機使用者的名稱 範例： • jane_smith 注意 僅使用本機使用者帳號名稱（<使用者名稱>）。不包含網域名稱。
檔案名稱 （僅完全相符）	指定完整檔案名稱 (包含副檔名) 範例： • filename.exe
檔案目錄 （僅完全相符；僅限內部部署）	指定不含檔案名稱的完整路徑 範例： • `c:\windows\system32\wbem\`
檔案雜湊值 （僅完全相符）	指定檔案的雜湊值。 範例： • `SHA-1: a2da9cda33ce378a21f54e9f03f6c0c9efba61fa` 注意 依預設，Endpoint Sensor 只會記錄 SHA-1 值。如果要使用 SHA-256 或 MD5 雜湊值，請更新用戶端策略以納入其他雜湊類型。

類型	項目
FQDN/IP 位址/主機名稱 （僅完全相符）	指定遠端端點 FQDN、IP 位址或主機名稱，以識別受調查端點所建立的網路連線 **注意** 不支援 IPv6 格式。 範例： • cncserver.com • maliciousssite.com • 192.168.0.1

登錄機碼
（支援部分比對）
 	
登錄值名稱
（支援部分比對）
 	
登錄值資料
（支援部分比對）
	指定完整或部分登錄機碼、值名稱或值資料
	
	注意
	• Trend Micro 只會記錄重要登錄位置的活動，以降低對端點資源的影響。
	如果調查不成功，而您想要進一步調查，請執行「即時調查」。
	• 請勿指定 SID 值做為登錄條件。調查不支援使用 SID 值做為自訂登錄條件。
	• 使用登錄資料做為調查條件的限制如下：
	  • 條件最多可包含 10 個項目。
	  • 每個項目必須至少有 2 個字元。
	  • 項目不能包含空格。

類型	項目
CLI 命令 （支援部分比對）	指定完整或部分命令列字串，然後按 Enter 鍵來新增項目。 **注意** 使用命令列做為調查條件的限制如下： • 條件最多可包含 10 個項目。 • 每個項目必須至少有 2 個字元。 • 項目不能包含空格。

使用 OpenIOC 檔案進行歷史調查

注意

如果要對目前的系統狀態執行調查，請使用「即時調查」。

如需詳細資訊，請參閱啟動一次性調查 第 20-22 頁。

步驟

1. 移至「回應 > 歷史調查」。
2. 按一下「OpenIOC 檔案」標籤。

注意

在歷史調查中使用 OpenIOC 檔案存在下列限制：

- 一次只能載入一個 OpenIOC 檔案。
- OpenIOC 檔案中指定的任何運算子都會變更為 `OR`。
- 唯一支援的條件為 `IS`。使用其他條件的項目會被忽略並會使用刪除線標示。
- 僅支援適用於所收集中繼資料的那些指標。使用不受支援之指標的項目會被忽略並使用刪除線標示。

如需詳細資訊，請參閱歷史調查支援的 IOC 指標 第 20-16 頁。

3. 如果要上傳新的 OpenIOC 檔案並使用它來進行調查，請執行下列作業：
   a. 按一下「上傳 OpenIOC 檔案」。
   b. 選取有效的 OpenIOC 檔案。
   c. 按一下「開啟」。
4. 如果要使用現有的 OpenIOC 檔案進行調查，請執行下列作業：
   a. 按一下「使用現有 OpenIOC 檔案」。
   b. 選取檔案。
   c. 按一下「套用」。
5. 按一下「評估」。
6. 在「結果」窗格中檢閱顯示的結果。

注意

- 留出一些時間供歷史調查執行。在中繼資料中發現相符物件，調查就會立即在結果表格尾端附加更多列。調查可能需要數分鐘才能完成。
- 將游標懸停在「端點」標籤上會顯示快顯視窗，其中顯示評估的進度。
- 在歷史調查期間提供的資料是 Security Agent 資料的子集，並且僅包含有關高風險檔案類型的資訊。如果評估未傳回任何結果，則您可以執行即時調查。

提供下列詳細資料：

欄名稱	說明
端點	包含相符物件的端點名稱 按一下可檢視有關端點的更多詳細資料。
狀態	端點的目前連線狀態
IP 位址	包含相符物件的端點 IP 位址 IP 位址是由網路指派
作業系統	端點所使用的作業系統
使用者	Security Agent 首次記錄相符物件時已登入的使用者之使用者名稱 按一下使用者名稱可檢視有關使用者的更多詳細資料。
管理伺服器	管理受影響端點的伺服器
首次發現	Security Agent 首次記錄相符物件時的日期和時間
詳細資訊	按一下此圖示可開啟「比對詳細資料」畫面。 「比對詳細資料」畫面會顯示下列詳細資料： • 條件：評估中使用的條件 • 首次發現：Security Agent 首次記錄相符物件時的日期和時間 • CLI/登錄出現次數：在命令列或登錄項目中發現的相符項目數目 按一下值可顯示更多詳細資料。 • 分級：趨勢科技資訊所指派的分級 您可以在 Threat Connect 或 VirusTotal 中進一步檢查分級為「惡意」的物件。 • 受影響的端點：當分級為「惡意」時，代表在其中發現類似相符項目的端點數目 此計數僅計入過去 90 天內受影響的端點。
星號 (*)	表示某個端點已標記為「重要」

7. 識別並選取需要進一步處理行動的一或多個端點。

注意

歷史調查結果可能包含 macOS 端點。由於 macOS 端點沒有可用的處理行動，因此這些端點的核取方塊均處於關閉狀態。

處理行動	說明
產生根本原因分析	產生根本原因分析，以檢閱導致相符物件執行的一系列事件。 如需詳細資訊，請參閱從評估啟動根本原因分析 第 20-17 頁。
啟動即時調查	使用相同條件對目前系統狀態執行新調查。 會出現「即時調查」畫面，並使用現有的條件啟動全新的一次性調查。 如果使用 OpenIOC 檔案進行評估，「即時調查」會同時使用目前的 OpenIOC 檔案及選取的端點做為條件 如需詳細資訊，請參閱啟動一次性調查 第 20-22 頁。
隔離端點	中斷所選端點與網路的連線。 注意 在解決已隔離端點上的安全威脅後，「目錄 > 使用者/端點」畫面上的下列位置會提供選項，讓您恢復已隔離端點的網路連線： • 端點 > 全部：按一下資料表中某個端點的名稱，然後在出現的畫面上按一下「工作 > 恢復」。 • 端點 > 過濾器 > 網路連線 > 已隔離：在資料表中選取端點列，然後按一下「工作 > 恢復網路連線」。

歷史調查支援的 IOC 指標

OpenIOC 檔案是包含一或多個入侵指標 (IOC) 的 XML 檔案。請確認 OpenIOC 檔案使用的指標項受所選調查類型支援。

下表列出調查支援的 IOC 指標。

表 20-2. 歷史調查支援的 IOC 指標

類別	項目	要求的條件
DNSENTRYITEM	HOST	IS
	RECORDDATA/HOST	IS
	RECORDDATA/IPV4ADDRESS	IS
FILEITEM	FILENAME	IS
	SHA1SUM	IS
	SHA2SUM	IS
	MD5SUM	IS
PORTITEM	LOCALIP	IS
	REMOTEIP	IS
PROCESSITEM	ARGUMENTS	CONTAINS
	NAME	IS
	SECTIONLIST/ MEMORYSECTION/SHA1SUM	IS
	SECTIONLIST/ MEMORYSECTION/ SHA256SUM	IS
	SECTIONLIST/ MEMORYSECTION/MD5SUM	IS

類別	項目	要求的條件
REGISTRYITEM	KEYPATH	CONTAINS
	VALUE	CONTAINS
	VALUENAME	CONTAINS
	USERNAME	IS

注意

選取此項目後，Endpoint Sensor 會顯示 OpenIOC 檔案的預覽。檢閱預覽可確認 OpenIOC 檔案是否包含支援的指標與條件。不受支援的組合採用刪除線這種格式，並在調查過程中被忽略。

從評估啟動根本原因分析

根本原因分析是一項調查工具，可顯示導致相符物件執行的一系列事件。

如果評估傳回相符項目，則管理員可產生根本原因分析來執行下列作業：

- 列出所有與指定條件相關的物件
- 識別是否有任何相關物件值得注意
- 檢閱導致相符物件執行的一系列事件。

產生根本原因分析可能需要一些時間才能完成。

步驟

1. 執行歷史調查。

   在「結果」窗格中檢閱顯示的結果。

   如需詳細資訊，請參閱使用使用者定義的條件進行歷史調查 第 20-5 頁。

2. 識別並選取一或多個端點，然後按一下「產生根本原因分析」。

3. 指定新的「根本原因分析」工作的名稱。
4. 檢閱顯示的條件。
   - 若要使用使用者定義的條件來進行評估，請使用 AND 或 OR 運算子結合多個條件來產生「根本原因分析」。
   - 若要使用 OpenIOC 檔案來進行評估，請使用目前的 OpenIOC 檔案中的指標做為條件來產生「根本原因分析」。
5. 檢閱目標端點。

   注意

   如果要從清單中移除端點，請按一下刪除圖示。

6. 指定期間。

   依預設，系統會對所有記錄的日期執行分析。
7. 按一下「產生」。
8. 移至「根本原因分析結果」標籤，可監控分析的進度。

   產生根本原因分析可能需要一些時間才能完成。

   如需詳細資訊，請參閱根本原因分析結果 第 20-19 頁。
9. 在工作完成後，按一下「工作」名稱。

注意

如果 Endpoint Sensor 因為下列原因而無法產生根本原因分析，則工作名稱不會顯示為連結：

- 目標端點的資料不足。

  請確認資料未被清除。如果用戶端資料庫達到資料庫大小上限，Endpoint Sensor 就會清除最舊的記錄檔，以釋放空間給新的事件項目。如果要避免發生此問題，請指定較大的用戶端資料庫大小。

- 調查找不到符合 OpenIOC 檔案中指定之所有條件的物件。

  評估會忽略 OpenIOC 檔案中的所有條件，以傳回初始結果。不過，「根本原因分析」工作會新增回一些條件做為調查的額外條件。因此，「根本原因分析」工作可能無法產生同時符合 OpenIOC 條件及其條件的結果。

10. 檢閱結果。

根本原因分析結果

若要監控「根本原因分析」工作的進度，請移至「回應 > 歷史調查」，然後按一下「根本原因分析結果」標籤。

如果評估傳回相符項目，則管理員可產生根本原因分析來執行下列作業：

- 列出所有與指定條件相關的物件
- 識別是否有任何相關物件值得注意
- 檢閱導致相符物件執行的一系列事件。

產生根本原因分析可能需要一些時間才能完成。

如需詳細資訊，請參閱從評估啟動根本原因分析 第 20-17 頁。

下表列出可供檢閱的調查詳細資料。

欄名稱	說明
狀態	「根本原因分析」工作的進度
名稱	「根本原因分析」工作的名稱 按一下可開啟「關聯分析」和「物件詳細資料」畫面。 如需詳細資訊，請參閱關聯分析 第 20-32 頁。 **注意** 如果 Endpoint Sensor 因為下列原因而無法產生根本原因分析，則工作名稱不會顯示為連結： • 目標端點的資料不足。 請確認資料未被清除。如果用戶端資料庫達到資料庫大小上限，Endpoint Sensor 就會清除最舊的記錄檔，以釋放空間給新的事件項目。如果要避免發生此問題，請指定較大的用戶端資料庫大小。 • 調查找不到符合 OpenIOC 檔案中指定之所有條件的物件。 評估會忽略 OpenIOC 檔案中的所有條件，以傳回初始結果。不過，「根本原因分析」工作會新增回一些條件做為調查的額外條件。因此，「根本原因分析」工作可能無法產生同時符合 OpenIOC 條件及其條件的結果。
條件	為「根本原因分析」工作指定的條件
相符物件	在端點中找到的相符物件數目 按一下值可檢視更多詳細資料。
星號 (*)	表示某個端點已標記為「重要」
端點	包含相符物件的端點名稱 按一下「端點」名稱可檢視有關端點的更多詳細資料。
IP 位址	包含相符物件的端點 IP 位址 IP 位址是由網路指派

欄名稱	說明
已啟動	「根本原因分析」工作的啟動日期和時間
已用	工作自啟動後經過的時間長度
建立者	建立工作的使用者

若要刪除「根本原因分析」工作，請在資料表中選取項目，然後按一下「刪除」。

即時調查

即時調查會對目前的系統狀態執行調查。即時調查可設定為在特定期間執行，也支援透過使用 OpenIOC 和 YARA 規則來擴大條件組。

重要

僅適用於安裝在 Windows 平台上的 Security Agent。

即時調查支援下列條件：

- OpenIOC 規則：使用 OpenIOC 規則掃瞄目前在磁碟上的所有檔案。

  注意

  選取此項目後，Endpoint Sensor 會顯示 OpenIOC 檔案的預覽。檢閱預覽可確認 OpenIOC 檔案是否包含支援的指標與條件。不受支援的組合採用刪除線這種格式，並在調查過程中被忽略。

  如需詳細資訊，請參閱即時調查支援的 IOC 指標 第 20-29 頁。

- YARA 規則：使用 YARA 規則掃瞄目前在記憶體中執行的所有程序。

注意

根本原因分析結果僅適用於 YARA 規則。

由於即時調查是針對目前的系統狀態執行的，而在此期間有些檔案和登錄項目可能已被鎖定或正在使用中。因此根本原因分析結果不適用於使用 OpenIOC 規則或登錄搜尋的調查。如果要使用 OpenIOC 規則或登錄資料來產生根本原因分析，請使用歷史調查。

如需詳細資訊，請參閱歷史調查 第 20-3 頁。

- 搜尋登錄：指定要對目標端點進行比對的登錄機碼、名稱和資料。

注意

僅會對下列根機碼下的登錄值執行調查：

- HKEY_CURRENT_USER
- HKEY_CLASSES_ROOT
- HKEY_LOCAL_MACHINE
- HKEY_USERS

管理員可以指定要執行的即時調查類型：

- 一次性調查僅會執行一次。調查一經建立就會立即執行。

  如需詳細資訊，請參閱啟動一次性調查 第 20-22 頁。

- 您可以將預約的調查設定為按照特定時間間隔自動執行。

  如需詳細資訊，請參閱啟動預約調查 第 20-25 頁。

即時調查需要一些時間才能完成。

啟動一次性調查

步驟

1. 移至「回應 > 即時調查」。

2. 按一下「一次性調查」標籤。
3. 按一下「新調查」。
4. 指定此調查的「名稱」。
5. 根據物件需要符合的規則選取「方法」：
   - 使用 OpenIOC 掃瞄磁碟檔案：磁碟上符合 OpenIOC 檔案所提供規則的物件

     注意

     選取此項目後，Endpoint Sensor 會顯示 OpenIOC 檔案的預覽。檢閱預覽可確認 OpenIOC 檔案是否包含支援的指標與條件。不受支援的組合採用刪除線這種格式，並在調查過程中被忽略。

     如需詳細資訊，請參閱即時調查支援的 IOC 指標 第 20-29 頁。

   - 使用 YARA 掃瞄記憶體中的程序：記憶體中目前符合 YARA 檔案所提供規則的物件
   - 搜尋登錄：符合使用者定義之條件的登錄機碼、名稱和資料
6. 按一下「選取端點」並指定要納入調查的端點。

   注意

   「目標端點」畫面可能不會顯示選取要進行調查的所有端點。
   - 使用者只能檢視已被授與足夠存取權限的端點。
   - 僅適用於安裝在 Windows 平台上的 Security Agent。
7. 按一下「啟動調查」。
8. 若要檢視一次性調查的結果並監控其進度，請執行下列作業：
   a. 移至「回應 > 即時調查」。
   b. 按一下「一次性調查」標籤。

   如需詳細資訊，請參閱一次性調查 第 20-24 頁。

一次性調查

一次性調查是只會執行一次的調查。

若要檢視一次性調查的結果並監控其進度，請移至「回應 > 即時調查」，然後按一下「一次性調查」標籤。

下列詳細資料可供檢閱。

欄	說明
狀態	調查的目前狀態
進度	調查的完成百分比
名稱	使用者定義的名稱，用於識別調查 按一下可檢視調查結果。
方法	調查所使用的方法
條件	• OpenIOC 或 YARA 規則檔案的檔案名稱 • 使用者定義的登錄值
相符端點	包含符合指定條件之物件的端點數目
目標端點	選取的要調查的端點總數 按一下可檢視有關所選端點的更多詳細資料。 **注意** 「目標端點」畫面可能不會顯示選取要進行調查的所有端點。使用者只能檢視已被授與足夠存取權限的端點。
已啟動	調查的啟動日期和時間
已用	調查自啟動後經過的時間長度
建立者	建立調查的使用者

按一下「新調查」以啟動新調查。

選取至少一個調查以啟動下列選項：

- 停止：取消調查。無法恢復已停止的調查。
- 刪除：停止調查，然後從清單中移除調查。無法復原已移除的調查。

啟動預約調查

步驟

1. 移至「回應 > 即時調查」。
2. 按一下「預約調查」標籤。
3. 按一下「新調查」。
4. 指定此調查的「名稱」。
5. 根據物件需要符合的規則選取「方法」：
   - 使用 OpenIOC 掃瞄磁碟檔案：磁碟上符合 OpenIOC 檔案所提供規則的物件

     注意

     選取此項目後，Endpoint Sensor 會顯示 OpenIOC 檔案的預覽。檢閱預覽可確認 OpenIOC 檔案是否包含支援的指標與條件。不受支援的組合採用刪除線這種格式，並在調查過程中被忽略。

     如需詳細資訊，請參閱即時調查支援的 IOC 指標 第 20-29 頁。
   - 使用 YARA 掃瞄記憶體中的程序：記憶體中目前符合 YARA 檔案所提供規則的物件
   - 搜尋登錄：符合使用者定義之條件的登錄機碼、名稱和資料
6. 按一下「選取端點」並指定要納入調查的端點。

注意

「目標端點」畫面可能不會顯示選取要進行調查的所有端點。

- 使用者只能檢視已被授與足夠存取權限的端點。
- 僅適用於安裝在 Windows 平台上的 Security Agent。

7. 指定此調查的預約時程。
   - 期間：指定調查的開始日期和結束日期。調查僅會在提供的日期範圍內執行。預設期間設定為一個月。
   - 頻率：指定在整個預約時程期間重複執行調查的頻率。預設頻率設定為「每日」的「08:00」。
8. 按一下「啟動調查」。
9. 如果要檢視預約調查的結果並監控其進度，請執行下列作業：
   a. 移至「回應 > 即時調查」。
   b. 按一下「預約調查」標籤。

      如需詳細資訊，請參閱預約調查 第 20-26 頁。
   c. 如果要檢視每個預約執行的詳細資料，請按一下調查名稱以開啟「預約調查歷史記錄」畫面。

      如需詳細資訊，請參閱檢閱預約調查歷史記錄 第 20-28 頁。

預約調查

預約調查是設定為在特定期間自動執行的調查。

若要檢視預約調查的結果並監控其進度，請移至「回應 > 即時調查」，然後按一下「預約調查」標籤。

下表列出可供檢閱的詳細資料。

欄	說明
啟動	調查的目前狀態
名稱	使用者定義的名稱，用於識別調查 按一下可開啟「預約工作歷史記錄」畫面。
方法	調查所使用的方法
條件	OpenIOC 檔案的檔案名稱 使用者定義的登錄值
目標端點	選取的要調查的端點總數 按一下可檢視有關所選端點的更多詳細資料。 **注意** 「目標端點」畫面可能不會顯示選取要進行調查的所有端點。使用者只能檢視已被授與足夠存取權限的端點。
頻率	調查在整個預約時程的重複執行頻率
最新調查	最新調查的啟動日期和時間
最新已用時間	最新調查自啟動後經過的時間長度
最新相符端點	包含符合最新調查的指定條件之物件的端點數目
建立者	建立調查的使用者

按一下「新調查」以啟動新調查。

按一下「刪除」可停止調查，然後從清單中移除調查。無法復原已移除的調查。

注意

如果刪除 OpenIOC 檔案，將會自動關閉任何使用已刪除的 OpenIOC 檔案的預約調查。

檢閱預約調查歷史記錄

使用「預約調查歷史記錄」畫面可檢視過去的預約，並監控執行中預約的進度。

步驟

1. 存取「預約調查歷史記錄」畫面：
   a. 移至「回應 > 即時調查」。
   b. 在「預約調查」標籤上，按一下「名稱」欄中的值。
2. 檢閱預約總覽中所列的詳細資料：
   - 工作名稱：提供給預約的名稱
   - 期間和頻率：顯示預約執行調查的時間和頻率。
   - 方法：預約每次執行時所用的條件。按一下可顯示完整條件。
   - 目標端點：按一下可檢視預約中所含端點的清單。
3. 檢閱預約每次執行時的調查詳細資料。

欄名稱	說明
狀態	調查的目前狀態
進度	調查的完成百分比
相符端點	包含符合指定條件之物件的端點數目 按一下可開啟「調查結果」畫面。
已啟動	調查的啟動日期和時間
已用	調查自啟動後經過的時間長度 對於已完成的調查，這是執行調查花費的總時間

4. 選取至少一個調查以啟動下列選項：
   - 停止：取消調查。無法恢復已停止的調查。

- 刪除：停止調查，然後從清單中移除調查。無法復原已移除的調查。

即時調查支援的 IOC 指標

OpenIOC 檔案是包含一或多個入侵指標 (IOC) 的 XML 檔案。請確認 OpenIOC 檔案使用的指標項受所選調查類型支援。

下表列出調查支援的 IOC 指標。

重要

選擇 IOC 檔案時，您必須確保 IOC 指標包含要比對的檔案位置 ("FileItem/FullPath" 或 "FileItem/FilePath")。

類別	項目	要求的條件	注意
FILEITEM	FULLPATH	IS	指完整的目錄路徑、檔案名稱和副檔名
	FILEPATH	IS、CONTAINS、STARTS-WITH、ENDS-WITH	支援部分比對
	FILENAME	IS、CONTAINS、STARTS-WITH、ENDS-WITH	支援部分比對
	MD5SUM	IS	
	SHA1SUM	IS	
	SHA256SUM	IS	
	SIZEINBYTES	IS	
	CREATED	GREATER-THAN、LESS-THAN	需要的格式（採用 UTC）：yyyy-mm-ddThh:mm:ss
	MODIFIED	GREATER-THAN、LESS-THAN	需要的格式（採用 UTC）：yyyy-mm-ddThh:mm:ss
	ACCESSED	GREATER-THAN、LESS-THAN	需要的格式（採用 UTC）：yyyy-mm-ddThh:mm:ss

注意

選取此項目後，Endpoint Sensor 會顯示 OpenIOC 檔案的預覽。檢閱預覽可確認 OpenIOC 檔案是否包含支援的指標與條件。不受支援的組合採用刪除線這種格式，並在調查過程中被忽略。

調查結果

使用「調查結果」畫面可取得調查結果的快速總覽。您可從下列位置存取此畫面：

- 在「一次性調查」標籤中，按一下調查「名稱」。

- 在「預約的調查」標籤中，按一下調查「名稱」，然後按一下「相符端點」欄中的值。

此畫面會顯示下列資訊：

- 其中顯示已分類為「相符、不相符、已排入佇列」或「已取消」之端點總數的環圈圖

  圖表左側提供總數摘要。隨著調查持續進行，會即時更新此摘要。

圖示	標籤	說明
	相符	包含相符物件的受調查端點數目
	沒有相符項目	未包含相符物件的受調查端點數目
	已排入佇列	仍要進行調查的端點數目。 當不再有已排入佇列的端點要進行調查時，調查就會完成。
	已取消	未調查的端點數目。 這可能是由於使用者取消、系統錯誤或端點逾時。

- 建立調查時所使用的參數。

  按一下「條件」可檢閱調查所使用的搜尋條件。

- 其中提供有關調查中所含每個端點的更多詳細資料的結果資料表。

  此資料表會根據調查狀態將端點分組為幾個標籤。此資料表會顯示下列詳細資料：

欄名稱	說明
星號 (*)	表示某個端點已標記為「重要」
端點	包含相符物件的端點名稱 按一下「端點」名稱可檢視有關端點的更多詳細資料。
IP 位址	包含相符物件的端點 IP 位址 IP 位址是由網路指派。

欄名稱	說明
作業系統	端點所使用的作業系統
使用者	Endpoint Sensor 用戶端首次記錄相符物件時已登入的使用者之使用者名稱 按一下使用者名稱可檢視有關使用者的更多詳細資料。
比對詳細資料	按一下可檢視比對的詳細資料。
根本原因分析	按一下可檢視「根本原因分析」畫面。 注意 根本原因分析結果僅適用於 YARA 規則。 由於即時調查是針對目前的系統狀態執行的，而在此期間有些檔案和登錄項目可能已被鎖定或正在使用中。因此根本原因分析結果不適用於使用 OpenIOC 規則或登錄搜尋的調查。如果要使用 OpenIOC 規則或登錄資料來產生根本原因分析，請使用歷史調查。 如需詳細資訊，請參閱從評估啟動根本原因分析 第 20-17 頁。
已用	自調查啟動後經過的時間長度。

關聯分析

「關聯分析」標籤會顯示「根本原因分析」，也會醒目提示可能有利於調查的其他資訊。

「安全威脅調查」可以關聯來自 Endpoint Sensor 和 Active Directory 的資訊，以顯示整個網路中的端點和使用者帳號的相關攻擊資訊。

資訊	說明
目標端點	顯示受調查之端點的詳細資訊 按一下端點名稱和使用者名稱可檢視詳細資訊。 按一下「隔離端點」以中斷端點與網路的連線。隔離期間，用戶端只能與伺服器通訊。 注意 在解決已隔離端點上的安全威脅後，「目錄 > 使用者/端點」畫面上的下列位置會提供選項，讓您恢復已隔離端點的網路連線： • 端點 > 全部：按一下資料表中某個端點的名稱，然後在出現的畫面上按一下「工作 > 恢復」。 • 端點 > 過濾器 > 網路連線 > 已隔離：在資料表中選取端點列，然後按一下「工作 > 恢復網路連線」。
首次發現的物件	關聯分析中疑似應負責建立所調查物件的第一個物件。 這通常是目標式攻擊的進入點。 將游標懸停在物件上，然後按一下 以在關聯分析中找到該物件。
相符物件	顯示物件或與調查條件相符的物件清單 將滑鼠游標暫留在物件上，然後按一下 以在「根本原因分析」中找到物件。
值得注意的物件	根據現有的趨勢科技情報，會醒目提示該關聯分析中可能有惡意的物件 計算的數值為關聯分析中獨特的值得注意的物件數目。 按一下以檢視值得注意的物件之清單。 將游標懸停在物件上，然後按一下 以在關聯分析中找到該物件。

資訊	說明
「根本原因分析」區域	顯示事件中涉及之物件的視覺分析 **注意** 如果關聯分析中的節點數目超過顯示上限，則只會顯示主要關聯分析。為避免發生這個問題，請縮小調查條件範圍。 按一下任何可用的節點以檢視有關所選物件的詳細資訊。 如需有關如何解讀關聯分析的詳細資訊，請參閱： • 物件詳細資料：資料檔標籤 第 20-34 頁 **注意** 「資料檔」標籤是所選物件沒有其他可用標籤時的預設檢視。 • 物件詳細資料：相關物件標籤 第 20-36 頁 • 瀏覽關聯分析 第 20-36 頁 • 根本原因分析圖示 第 20-37 頁

注意

如果要匯出資料，請按一下 並執行下列其中一項：

- 選取「關聯分析」可將所有根本原因鏈匯出為 .png 檔案。
- 選取「物件詳細資料」可將所有資料匯出為 CSV 檔案。

物件詳細資料：資料檔標籤

「資料檔」標籤顯示適用於所選物件類型的詳細資訊。

有些物件可能只會顯示一組有限的詳細資訊，或在執行時可能無法提供任何詳細資訊。

注意

您可以在 Threat Connect 或 VirusTotal 中進一步檢查分級為「惡意」的物件。

此標籤也可能會顯示「相符物件」和「值得注意的物件」的其他選項：

選項	說明
終止物件	只終止目標端點目前狀態下的所有執行中的執行個體 注意 此處理行動僅適用於未分級、惡意和可疑的「程序」類型物件。如果要確認指令是否成功，請移至「管理 > 指令追蹤」。
新增至可疑物件清單	只終止目標端點目前狀態下的所有執行中的執行個體，然後將物件新增至「使用者定義的可疑物件」清單。 注意 如果已啟動 Application Control，則符合已新增至「使用者定義的可疑物件」清單之物件的雜湊值的程序都不允在所有端點上執行。Endpoint Sensor 也會先終止「“程序”」類型物件後再將它們新增到清單，且 Application Control 會禁止其再次啟動。
新增至歷史調查清單	新增物件做為新歷史調查的條件 若要開始進行調查，請按一下「關聯分析」上方的「啟動歷史調查」按鈕。 注意 如果您決定不再想對「關聯分析」中的物件執行歷史調查，請按一下該物件，然後按一下「從歷史調查清單中移除」按鈕。 如需詳細資訊，請參閱使用使用者定義的條件進行歷史調查 第 20-5 頁。

物件詳細資料：相關物件標籤

「相關物件」標籤會顯示所選取物件的所有相依項目。

注意

「相關物件」標籤只會顯示「“程序”」物件的其他資訊。

這些物件是執行相符物件所需要的。此標籤會顯示下列詳細資料：

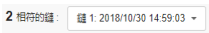
內容	說明
處理行動	此物件完成的處理行動
已記錄	記錄處理行動的日期和時間
分級	根據趨勢科技資訊指派給此物件的分級
受影響的端點	受影響的端點（如果有）
目標路徑	物件的目標目的地

您可以使用下列選項管理「相關物件」標籤：

- 此標籤提供可根據指定處理行動過濾物件的下拉式清單。按一下下拉式清單可檢視所有可用的處理行動。
- 按一下「顯示詳細資料」可檢視有關物件的更多詳細資料。

瀏覽關聯分析

若要瀏覽關聯分析，請按住並拖曳區域或使用可用的瀏覽圖示。

圖示	說明
	根本原因分析可包含一或多個相符的根本原因關聯分析。 按一下下拉式清單可檢視所選端點的其他關聯分析。

圖示	說明
啟動歷史調查	按一下可開始使用歷史調查清單中的物件進行歷史調查。 如果歷史調查清單中沒有任何物件，則此功能無法使用。 如果要啟動此功能，請在歷史調查清單中新增至少一個相符物件或值得注意的物件。
	按一下可進入全螢幕模式。 再按一下可退出全螢幕模式。
	按一下可放大或縮小。
	游標懸停時，可檢視顯示在關聯分析中的符號說明。 如需詳細資訊，請參閱根本原因分析圖示 第 20-37 頁。

根本原因分析圖示

關聯分析使用下列圖示顯示物件類型：

圖示	名稱	說明
	首次發現的物件	標示最常建立相符物件的物件

圖示	名稱	說明
	相符的條件	標示符合調查條件的物件
	正常物件	標示已經過驗證而不會造成安全威脅的物件 這些通常是常見的系統檔案。
	未分級的物件	標示尚未分級的物件
	可疑物件	標示顯露出與已知安全威脅有類似行為的物件
	惡意物件	標示與已知安全威脅相符的物件
	開機	會在系統啟動期間啟動的物件
	瀏覽器	能顯示網頁的物件，通常是網路瀏覽器
	電子郵件用戶端	可以傳送和接收電子郵件的物件，通常是電子郵件用戶端或伺服器
	檔案	為磁碟上檔案的物件
	網路	與網路連線或 Internet 相關的物件
	處理程序	為執行期間執行的處理程序的物件
	登錄	為登錄機碼、項目或資料的物件

圖示	名稱	說明
	事件	表示物件所完成的處理動作
	關聯	表示兩個物件之間的關係

物件詳細資料

「物件詳細資料」標籤顯示的資訊與「根本原因分析」標籤相同，但會以資料表形式顯示資訊。它還會將物件組織成下列標籤：

- 物件：涉及相符物件執行的物件，按其父程序分組。按一下 ▶ 可展開清單。
- 值得注意的事件：鏈中可能存在惡意的物件（根據現有的趨勢科技情報）
- 檔案事件：鏈中本身是檔案的物件
- 登錄事件：鏈中本身是登錄機碼、資料和項目的物件
- IP 位址/DNS 事件：本身是 IP 位址或 DNS 事件的物件

此資料表提供下列詳細資料：

欄名稱	說明
記錄的物件	所記錄物件的名稱 按一下物件名稱可檢視更多詳細資料。
PID	所記錄物件的程序 ID
已記錄	物件成為鏈中相關物件的日期和時間
活動	此物件完成的處理行動 按一下物件名稱可檢視更多詳細資料。

欄名稱	說明
物件信譽	根據趨勢科技資訊指派給此物件的分級 您可以在 Threat Connect 或 VirusTotal 中進一步檢查分級為「惡意」的物件。
受影響的端點	出現物件的端點數目 受影響的端點百分比（根據網路上的端點總數） 按一下值可檢視有關端點的更多詳細資料。

使用下列選項可管理資料表：

- 在所有標籤上的「記錄的物件」欄中選取至少一個物件，然後按一下「啟動歷史調查」以啟動另一項調查。
- 在「物件」標籤中，按一下過濾器圖示 ( )，可根據指定的條件過濾資料表。
- 在「檔案事件」標籤上，按一下「已記錄」和「物件信譽」欄，可排序資料表。

第 21 章

Managed Detection and Response

本章討論如何使用 Apex Central 主控台來設定 Managed Detection and Response 設定並管理調查工作。

包含下列主題：

- Managed Detection and Response 總覽 第 21-2 頁
- 追蹤 Managed Detection and Response 工作指令 第 21-15 頁
- 查詢支援的目標 第 21-17 頁
- Managed Detection and Response 的安全威脅調查中心用戶端 第 21-19 頁

Managed Detection and Response 總覽

在「Managed Detection and Response」畫面中，您可以從 Apex Central 主控台將 Managed Detection and Response 設定和調查工作部署到指定的目標。

秘訣

- 如果要檢視 Managed Detection and Response 工作指令的狀態，請使用「指令追蹤」畫面。

  如需詳細資訊，請參閱追蹤 Managed Detection and Response 工作指令 第 21-15 頁。

- 如果要進行進階搜尋來找出支援 Managed Detection and Response 服務的目標，請使用「使用者/端點目錄」畫面。

  如需詳細資訊，請參閱查詢支援的目標 第 21-17 頁。

使用「Managed Detection and Response」畫面可執行下列工作。

工作	說明
向安全威脅調查中心伺服器註冊	按一下「設定」標籤，可向安全威脅調查中心伺服器註冊 Apex Central。 Apex Central 與 Trend Micro 安全威脅調查中心整合，以啟動 Managed Detection and Response 功能。 如需詳細資訊，請參閱向安全威脅調查中心註冊 Apex Central 第 21-3 頁。
從安全威脅調查中心伺服器取消註冊	按一下「設定」標籤，可向安全威脅調查中心伺服器取消註冊 Apex Central。 如需詳細資訊，請參閱從安全威脅調查中心伺服器取消註冊 第 21-5 頁。

工作	說明
暫停或恢復 Managed Detection and Response 服務	按一下「設定」標籤，可暫停或恢復 Managed Detection and Response 服務。 **重要** 暫停 Managed Detection and Response 服務，就不會再收到新的調查工作，也會停止將記錄檔傳送到安全威脅調查中心伺服器。Apex Central 不會取消任何進行中的工作，結果仍會傳送到安全威脅調查中心伺服器。 如需詳細資訊，請參閱暫停或恢復 Managed Detection and Response 服務 第 21-6 頁。
核可或拒絕新的調查工作	按一下「等待中的工作」標籤，可核可或拒絕新的調查工作。 如需詳細資訊，請參閱核可或拒絕調查工作 第 21-6 頁。
追蹤已部署的調查工作	按一下「工作追蹤」標籤，可追蹤及檢視已核可或已拒絕的調查工作和指令。 如需詳細資訊，請參閱追蹤調查工作 第 21-11 頁。
檢視自動化的分析	按一下「自動化的分析」標籤，可檢視有關 Trend Micro 所收集之記錄檔資料的資訊，以進一步保護您的網路。 如需詳細資訊，請參閱檢視自動化的分析 第 21-14 頁。

向安全威脅調查中心註冊 Apex Central

Apex Central 與 Trend Micro 安全威脅調查中心整合，以啟動 Managed Detection and Response 功能。

重要

- Managed Detection and Response 功能需要購買服務計劃，才能取得有效的伺服器位址和公司 GUID。請聯絡 Trend Micro 銷售人員或經銷商來購買服務計劃。

步驟

1. 移至「回應 > Managed Detection and Response」。

   會出現「Managed Detection and Response」畫面。

2. 按一下「設定」標籤。

3. 指定下列資訊：

   - 伺服器位址：由 Trend Micro 銷售人員或經銷商提供的安全威脅調查中心伺服器位址
   - 公司 GUID：由 Trend Micro 銷售人員或經銷商提供的 Managed Detection and Response 服務 GUID

4. 為新的調查工作設定自動核准設定。

   注意

   - 如果啟動了自動核准，Apex Central 會傳送電子郵件通知，將自動核可的新調查工作通知收件者。
   - 如果關閉自動核准，則 Apex Central 會傳送所有新調查工作的電子郵件通知，以要求手動核准。

   - 選取「自動核可調查工作」核取方塊，以啟動自動核準新的調查工作。
   - 不勾選「自動核可調查工作」核取方塊，將會關閉自動核准新的調查工作。

5. （選用）設定通知收件者。

   注意

   - 您可以在「使用者帳號」畫面上（管理 > 帳號管理 > 使用者帳號）新增使用者帳號。
   - 您可以在「聯絡人群組」畫面上（偵測 > 通知 > 聯絡人群組）新增聯絡人群組。

- 如果要新增收件者，請從「可用的使用者和群組」清單中選取聯絡人，然後按一下「>」。

  選取的聯絡人會出現在「選取的使用者和群組」清單中。

- 如果要移除收件者，請從「選取的使用者和群組」清單中選取聯絡人，然後按一下「<」。

  選取的聯絡人會出現在「可用的使用者和群組」清單中。

6. 按一下「註冊」。

   - 「伺服器位址」欄位會顯示已註冊安全威脅調查中心伺服器的位址。
   - 「寄件者 ID」欄位會取代「公司 GUID」欄位，並顯示會從已註冊安全威脅調查中心伺服器接收調查工作的 Apex Central 伺服器的 GUID。

從安全威脅調查中心伺服器取消註冊

重要

取消註冊會自動關閉 Managed Detection and Response 服務。

步驟

1. 移至「回應 > Managed Detection and Response」。

   會出現「Managed Detection and Response」畫面。

2. 按一下「設定」標籤。
3. 按一下「取消註冊」。

   會出現確認對話方塊。

4. 按一下「取消註冊」。

   Managed Detection and Response 服務將會自動關閉。

暫停或恢復 Managed Detection and Response 服務

重要

暫停 Managed Detection and Response 服務，就不會再收到新的調查工作，也會停止將記錄檔傳送到安全威脅調查中心伺服器。Apex Central 不會取消任何進行中的工作，結果仍會傳送到安全威脅調查中心伺服器。

步驟

1. 移至「回應 > Managed Detection and Response」。

   會出現「Managed Detection and Response」畫面。

2. 按一下「設定」標籤。

3. 若要暫停 Managed Detection and Response 服務，請執行下列作業：

   a. 按一下「暫停服務」。

   b. 在出現的確認對話方塊中：

      - 按一下「暫停服務」可暫停 Managed Detection and Response 服務。
      - 按一下「取消」可返回「設定」畫面而不暫停 Managed Detection and Response 服務。

4. 若要恢復 Managed Detection and Response 服務，請按一下「恢復服務」。

   Apex Central 會恢復接收新的調查工作，並將記錄檔傳送到安全威脅調查中心伺服器。

核可或拒絕調查工作

「Managed Detection and Response」畫面上的「等待中的工作」標籤會顯示由安全威脅調查中心提交需要管理員手動核可的調查工作。您可以檢視特定工作的目標和指令、修改選取的目標，以及核可或拒絕選取的工作。

如需有關「Managed Detection and Response」畫面上顯示之安全威脅調查中心工作指令的詳細資訊，請參閱安全威脅調查中心工作指令 第 21-10 頁。

秘訣

如果要檢視 Managed Detection and Response 工作指令的狀態，請使用「指令追蹤」畫面。

如需詳細資訊，請參閱追蹤 Managed Detection and Response 工作指令 第 21-15 頁。

重要

- Apex Central 會在安全威脅調查中心提交後僅保留調查工作資訊 90 天。
- 依預設，如果新調查工作在 Apex Central 收到後的 72 小時內未被核可或拒絕，新調查工作將自動逾時。

  如需有關調查工作指令狀態的詳細資訊，請參閱安全威脅調查中心指令狀態 第 21-13 頁。

步驟

1. 移至「回應 > Managed Detection and Response」。

   會出現「Managed Detection and Response」畫面。

2. 按一下「等待中的工作」標籤。

   會出現一個資料表，並顯示調查工作清單，其中包含如下資訊：

欄	說明
工作說明	由安全威脅調查中心管理員手動指定的工作名稱
指令	用於部署到所選取目標的工作指令 如需有關「Managed Detection and Response」畫面上顯示之安全威脅調查中心工作指令的詳細資訊，請參閱安全威脅調查中心工作指令 第 21-10 頁。
目標	工作的目標數目

欄	說明
到期	在 Apex Central 伺服器上工作將到期的本機時間 **重要** 依預設，如果新調查工作在 Apex Central 收到後的 72 小時內未被核可或拒絕，新調查工作將自動逾時。 如需有關調查工作指令狀態的詳細資訊，請參閱安全威脅調查中心指令狀態 第 21-13 頁。

3. 若要檢視等待中工作的目標，請按一下「工作說明」欄位旁的向右箭號圖示 (▶)。

   會出現一個資料表並顯示下列詳細資料：

欄	說明
端點	目標端點的名稱
IP 位址	目標端點的 IP 位址
使用者	上次登入目標端點的使用者名稱
Endpoint Sensor 服務	Endpoint Sensor 服務在目標端點上的狀態 如需詳細資訊，請參閱 Endpoint Sensor 服務狀態 第 21-10 頁。 **重要** 為了讓 Apex Central 能將調查工作部署到指定的目標，必須在目標上啟動 Endpoint Sensor 服務。

4. 若要核可待進行的調查工作，請執行下列作業：

   a. 選取您要核可之每個工作名稱旁的核取方塊。

   注意
   選取工作的核取方塊時，會一併選取該工作的所有目標。

b. 按一下工作名稱旁的向右箭頭圖示 (▶)，以修改該工作的所選目標。

重要

為了讓 Apex Central 能將調查工作部署到指定的目標，必須在目標上啟動 Endpoint Sensor 服務。

- 選取要包含的目標旁邊的核取方塊。
- 請勿勾選要排除的目標旁邊的核取方塊。

c. 對每個等待中的工作，重複以上步驟。

d. 按一下「核可」。

已核可的工作會顯示在「工作追蹤」標籤中。

如需詳細資訊，請參閱追蹤調查工作 第 21-11 頁。

5. 若要拒絕待進行的調查工作，請執行下列作業：

a. 選取您要拒絕之每個工作名稱旁的核取方塊。

注意

選取工作的核取方塊時，會一併選取該工作的所有目標。

b. 按一下工作名稱旁的向右箭頭圖示 (▶)，以修改該工作的所選目標。

- 選取要包含的目標旁邊的核取方塊。
- 請勿勾選要排除的目標旁邊的核取方塊。

c. 對每個等待中的工作，重複以上步驟。

d. 按一下「拒絕」。

已拒絕的工作會顯示在「工作追蹤」標籤中。

如需詳細資訊，請參閱追蹤調查工作 第 21-11 頁。

安全威脅調查中心工作指令

下表說明 Apex Central 的「Managed Detection and Response」畫面上顯示的安全威脅調查中心工作指令。

指令名稱	說明
收集檔案範例	從目標端點收集可疑檔案的樣本，然後將樣本傳送到安全威脅調查中心
執行趨勢科技調查套件	在目標端點上部署並執行趨勢科技調查套件
執行進階安全威脅評估	在目標端點上部署並執行 Trend Micro Anti-Threat Toolkit
評估影響	對目標端點啟動影響評估
執行根本原因分析	藉由使用安全威脅調查中心管理員指定的條件，對目標端點啟動根本原因分析

Endpoint Sensor 服務狀態

下表說明「等待中的工作」標籤上「Endpoint Sensor 服務」欄中顯示的用戶端狀態。

狀態	說明
已啟動	目標端點已啟動 Endpoint Sensor 重要 為了讓 Apex Central 能將調查工作部署到指定的目標，必須在目標上啟動 Endpoint Sensor 服務。
已關閉	目標端點已關閉 Endpoint Sensor
不支援伺服器使用授權	Apex One 使用授權不支援 Endpoint Sensor 服務

狀態	說明
需要受支援的 Security Agent 版本	目標端點未安裝 Security Agent，或目標端點的伺服器版本不受支援

追蹤調查工作

使用「Managed Detection and Response」畫面上的「工作追蹤」標籤，可追蹤及檢視核可的或拒絕的調查工作和指令的狀態。

秘訣

如果要檢視 Managed Detection and Response 工作指令的狀態，請使用「指令追蹤」畫面。

如需詳細資訊，請參閱追蹤 Managed Detection and Response 工作指令 第 21-15 頁。

重要

Apex Central 會在安全威脅調查中心提交後僅保留調查工作資訊 90 天。

步驟

1. 移至「回應 > Managed Detection and Response」。

   會出現「Managed Detection and Response」畫面。

2. 按一下「工作追蹤」標籤。

   會出現一個資料表，並顯示調查工作清單，其中包含如下資訊：

欄	說明
工作說明	由安全威脅調查中心管理員手動指定的工作名稱

欄	說明
指令	用於部署到所選取目標的工作指令 如需詳細資訊，請參閱安全威脅調查中心工作指令 第 21-10 頁。
目標	工作的目標數目
工作狀態	調查工作的部署狀態 如需詳細資訊，請參閱安全威脅調查中心工作狀態 第 21-12 頁。
上次更新時間	在 Apex Central 伺服器上最近狀態更新的本機時間

3. 按一下工作說明旁的向右箭號圖示 (▶)，可檢視工作指令資訊。

   會出現一個資料表並顯示下列詳細資料：

欄	說明
指令狀態	工作指令的部署狀態 如需詳細資訊，請參閱安全威脅調查中心指令狀態 第 21-13 頁。
端點	目標端點的名稱
IP 位址	目標端點的 IP 位址
使用者	上次登入目標端點的使用者名稱
已核可/已拒絕	在 Apex Central 伺服器上管理員核可或拒絕工作時的本機時間
核可/拒絕者	核可或拒絕該工作的管理員的使用者帳號名稱
上次更新時間	在 Apex Central 伺服器上最近狀態更新的本機時間

安全威脅調查中心工作狀態

下表說明「Managed Detection and Response」畫面上「工作追蹤」標籤中顯示之安全威脅調查中心工作的狀態。

如需有關「Managed Detection and Response」畫面上顯示之安全威脅調查中心工作指令的詳細資訊，請參閱安全威脅調查中心工作指令 第 21-10 頁。

狀態	說明
進行中	情況包括： • 已核可該工作，但尚未部署到 Apex One 伺服器 • 該工作指令已部署到 Apex One 伺服器，但尚未在指定的目標上完成
已完成	Apex Central 管理員已核可或拒絕該工作，且該工作已在指定的目標上完成（無論是否成功） 如需詳細資訊，請參閱安全威脅調查中心指令狀態 第 21-13 頁。

安全威脅調查中心指令狀態

下表說明「工作追蹤」畫面上顯示的指令狀態。

狀態	說明
等待中的核可	Apex Central 管理員尚未核可或拒絕該工作
已拒絕	Apex Central 管理員已拒絕該工作
正在傳送指令	已核可該工作，且 Apex Central 正將工作指令傳送到指定的目標
進行中	該工作指令已部署到 Apex One 伺服器，但尚未在指定的目標上完成
正在上傳	受管理的產品正在上傳工作酬載
成功	在指定的目標上成功完成該工作指令
無法處理指令	在指定的目標上未成功完成該工作指令

狀態	說明
指令逾時	情況包括： • Apex Central 管理員在收到該工作的 72 小時內未核可該工作 • 受管理的產品無法在核可後的 9 天內完成該工作指令 • 該工作指令在 Apex One 伺服器上逾時
用戶端沒有回應	Apex One 伺服器無法建立與目標用戶端間的通訊
Endpoint Sensor 已關閉	目標端點已關閉 Endpoint Sensor
需要受支援的 Security Agent 版本	目標端點未安裝 Security Agent，或目標端點的伺服器版本不受支援
不支援伺服器使用授權	Apex One 使用授權不支援 Endpoint Sensor 服務

檢視自動化的分析

Trend Micro 會定期執行自動化的分析來收集記錄檔資料，以進一步保護您的網路。使用「自動化的分析」標籤可檢視有關 Trend Micro 收集之記錄檔的資訊。

重要

Apex Central 會在安全威脅調查中心提交後僅保留調查工作資訊 90 天。

步驟

1. 移至「回應 > Managed Detection and Response」。

   會出現「Managed Detection and Response」畫面。

2. 按一下「自動化的分析」標籤。

   會出現一個資料表並顯示下列詳細資料：

欄	說明
開始時間	自動化的分析工作啟動時的 Trend Micro 伺服器本機時間
結束時間	自動化的分析工作完成時的 Trend Micro 伺服器本機時間
狀態	自動化的分析工作的狀態
指令	自動化的分析工作的類型
目標	自動化的分析工作的目標端點名稱或數目

3. 按一下「目標」欄中的計數可檢視目標。

   會出現「目標」畫面，其中顯示受影響端點的清單。

追蹤 Managed Detection and Response 工作指令

使用「指令追蹤」畫面可查詢及檢視 Apex Central 伺服器發出之 Managed Detection and Response 工作指令的詳細資料。

如需有關「Managed Detection and Response」畫面上顯示之追蹤安全威脅調查中心工作指令的資訊，請參閱追蹤調查工作 第 21-11 頁。

步驟

1. 移至「管理 > 指令追蹤」。

   會出現「追蹤指令」畫面。

2. 如果要過濾指令清單，請指定下列項目：

   - 已發出：指定 Apex Central 何時傳送工作指令
   - 指令：選取指令類型

     Apex Central Managed Detection and Response 工作指令包含下列項目：

指令名稱	說明
將安全威脅調查中心設定部署到受管理的產品	用於將安全威脅調查中心設定部署到受管理產品的指令
將安全威脅調查中心工作部署到受管理的產品	用於將安全威脅調查中心工作部署到受管理產品的指令
續約安全威脅調查中心憑證	用於續約 Apex Central 伺服器上安全威脅調查中心憑證的指令 注意 安全威脅調查中心伺服器會自動部署工作，以在 Apex Central 伺服器上的安全威脅調查中心憑證到期日前的 30 天續約該憑證。
提取安全威脅調查中心工作	用於從安全威脅調查中心伺服器提取工作的指令 注意 只有工作指令不成功時，此指令才會顯示在「指令追蹤」畫面上。

- 使用者：提供用來傳送此指令的使用者帳號名稱

  秘訣
  將此欄位保留空白，將會查詢所有使用者發出的查詢指令。

- 狀態：選取一或多個指令狀態，然後按一下「套用」。

3. 按一下「成功」、「未成功」、「進行中」或「全部」欄中的計數，以檢視詳細的指令資訊。

   會出現「指令詳細資料」畫面。

   如需詳細資訊，請參閱指令詳細資料 第 12-3 頁。

指令詳細資料

「指令詳細資料」畫面會顯示已發出之指令的下列相關資訊。

欄名稱	說明
上次回報	受管理產品上次傳送回應給 Apex Central 伺服器的日期和時間
伺服器/實體	受管理產品伺服器的主機名稱
狀態	已發出指令的狀態
說明	指令狀態的其他詳細資料

注意

「指令詳細資料」畫面會每隔 30 秒重新整理一次。

查詢支援的目標

使用「使用者/端點目錄」畫面可針對支援 Managed Detection and Response 服務的目標執行進階搜尋。

步驟

1. 移至「目錄 > 使用者/端點」。

   會出現「使用者/端點目錄」畫面。

2. 按一下資料表上方的「進階」連結。

3. 在「搜尋」下拉式清單控制項中，選取「端點」。

   第二個下拉式清單控制項中的搜尋條件會根據您的選取項目而動態變更。

4. 在第二個下拉式清單控制項中，選取「服務」。

   第三個下拉式清單控制項和第四個下拉式清單控制項隨即出現。

5. 在第三個下拉式清單控制項中，選取「Endpoint Sensor」。
6. 在第四個下拉式清單控制項中，選取用戶端狀態：
   - 已啟動：搜尋已啟動 Endpoint Sensor 服務的端點
   - 已關閉：搜尋已關閉 Endpoint Sensor 服務的端點
7. 使用過濾器右側的布林運算子新增多個搜尋條件。
   - OR：允許您針對指定的條件搜尋多個值。符合任一個值的所有記錄均會顯示。
   - AND：允許您選取新的搜尋條件。僅顯示既符合針對此條件指定的值，又符合所有其他選取的條件值的記錄。
8. 按一下下列其中一個項目，以顯示結果：
   - 搜尋：在清單中顯示搜尋結果，但不會儲存搜尋條件。
   - 另存為新的自訂過濾器：在清單中顯示搜尋結果，並提示您將搜尋條件儲存為自訂過濾器。自訂過濾器會顯示在「使用者/端點目錄」樹狀結構中的「端點」節點下方。
9. （選用）使用「端點」標籤下方的下拉式清單控制項，可以指定要顯示哪一段時間範圍內的資料，或在「表格式檢視」和「表格式檢視」之間切換。
10. （選用）按一下「匯出」將資料匯出為 `*.csv` 檔案或 `*.png` 影像。

注意

- 「表格式檢視」僅支援將資料匯出為 `*.csv` 檔案。
- 「時間表檢視」可以將資料匯出為 `*.csv` 檔案或 `*.png` 影像。

Managed Detection and Response 的安全威脅調查中心用戶端

Managed Detection and Response 的安全威脅調查中心用戶端會自動將下列資訊從 Apex Central 伺服器傳送到安全威脅調查中心伺服器。

資料類型	說明
Apex Central 偵測記錄檔	包含與向 Apex Central 伺服器註冊的受管理產品所偵測到的系統事件、網路事件及資料安全防護事件相關的記錄檔
Apex Central 資訊	包含 Apex Central 伺服器資訊
受管理產品資訊	包含有關向 Apex Central 伺服器註冊之趨勢科技產品的資訊
受管理的端點資訊	包含有關由向 Apex Central 伺服器註冊之趨勢科技產品管理的端點的資訊

第 22 章

可疑物件中樞和節點架構

本節提供管理員在跨多部 Apex Central 伺服器同步處理可疑物件清單所需的材料。

包含下列主題：

- 可疑物件中樞和節點 Apex Central 伺服器 第 22-2 頁
- 設定可疑物件中樞和節點 第 22-3 頁
- 從中央 Apex Central 取消註冊可疑物件節點 第 22-4 頁
- 組態設定注意事項 第 22-5 頁

可疑物件中樞和節點 Apex Central 伺服器

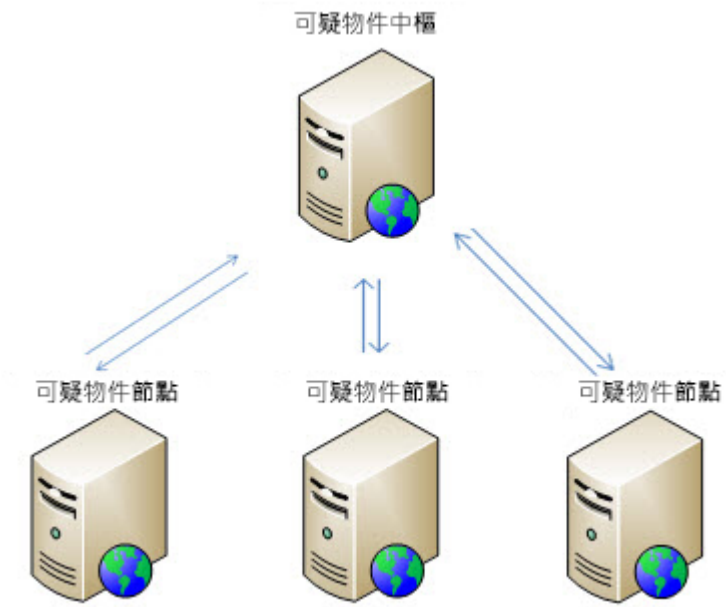
Trend Micro Apex Central™ 可疑物件中樞和節點架構可讓您跨多部 Apex Central 伺服器同步處理可疑物件清單。中央 Apex Central 伺服器上的可疑物件清單會整合來自以下位置的可疑物件清單：所有節點 Apex Central 伺服器，以及任何其他已註冊到任何這些伺服器的受管理產品；然後將這些清單部署回節點 Apex Central 伺服器。

管理員必須先設定可疑物件中央 Apex Central 伺服器，然後根據環境指派其他 Apex Central 伺服器做為可疑物件節點伺服器。Trend Micro Deep Discovery 產品可以註冊到可疑物件中樞或任何可疑物件節點 Apex Central 伺服器。這種架構會要求您透過可疑物件中央 Apex Central 伺服器主控台設定所有可疑物件處理行動。

重要

您必須透過可疑物件中央 Apex Central 對可疑物件清單執行所有作業，以確保所有節點 Apex Central 伺服器保持正確同步處理狀態。

透過可疑物件節點 Apex Central 對可疑物件執行的中毒處理行動，可能不會同步處理到所有連線的伺服器。



設定可疑物件中樞和節點

步驟

1. 登入可疑物件中央 Apex Central 伺服器主控台。
2. 移至「安全威脅資訊 > 派送設定」。

   會出現「派送設定」畫面。
3. 按一下「受管理的產品」標籤，然後複製（記下）下列設定：
   - 服務 URL
   - API 金鑰
4. 登入可疑物件節點 Apex Central 伺服器主控台。

5. 移至「安全威脅資訊 > 派送設定」。

   會出現「派送設定」畫面。

6. 在「中央 Apex Central」標籤中，提供從可疑物件中央 Apex Central 複製的下列設定：

   - 服務 URL
   - API 金鑰

7. （選用）選取「使用 Proxy 伺服器」核取方塊，以透過 Proxy 伺服器連線至中樞 Apex Central。

   注意

   若要設定或修改 Proxy 伺服器設定，請按一下「設定 Proxy 伺服器設定」。

8. 按一下「註冊」。

   會出現確認對話方塊，其中訊息指出伺服器已正確向中樞 Apex Central 註冊。

9. 對每一部可疑物件節點 Apex Central 伺服器重複上述程序。

10. 如果要設定預設同步處理間隔，請執行下列作業：

    a. 從「同步處理間隔」下拉式清單中選取時間範圍。

    b. 按一下「儲存」。

從中央 Apex Central 取消註冊可疑物件節點

注意

在取消註冊節點 Apex Central 伺服器後，所有先前同步處理的物件會留存在節點 Apex Central 伺服器可疑物件清單中。

步驟

1. 登入可疑物件節點 Apex Central 伺服器主控台。
2. 移至「安全威脅資訊 > 派送設定」。

   會出現「派送設定」畫面。
3. 在「中央 Apex Central 設定」區段中，按一下「取消註冊」。

   會出現確認對話方塊，並顯示訊息指出伺服器已從中央 Apex Central 正確取消註冊伺服器。
4. 如果您將可疑物件中樞和節點部署完全停止，請針對每部可疑物件節點 Apex Central 伺服器重複此程序。

組態設定注意事項

在成功設定可疑物件中樞並註冊可疑物件節點 Apex Central 伺服器後，請注意下列組態設定資訊。

注意

在取消註冊節點 Apex Central 伺服器後，所有先前同步處理的物件會留存在節點 Apex Central 伺服器可疑物件清單中。

組態設定	中央 APEX CENTRAL	節點 APEX CENTRAL
同步處理間隔	無	5 分鐘（預設值）

<table>
<tr><th>組態設定</th><th>中央 APEX CENTRAL</th><th>節點 APEX CENTRAL</th></tr>
<tr><td rowspan="2">可疑物件清單同步處理</td><td>從中央 Apex Central 到節點：
沙箱清單
使用者定義的清單</td><td>從節點 Apex Central 到中樞：
沙箱清單</td></tr>
<tr><td colspan="2">注意
中央 Apex Central 伺服器不會將「使用者定義」清單或「例外」清單中「注意事項」欄的資料傳送到節點 Apex Central 伺服器。
在同步處理清單時，「使用者定義」清單的優先順序高於「沙箱」清單。
如果您在下次同步處理前，將某個物件同時新增到中央 Apex Central 上的「使用者定義」清單和「沙箱」清單，則中央 Apex Central 伺服器會將這兩種清單部署到節點 Apex Central 伺服器。
如果節點 Apex Central 沙箱清單中的某個物件也存在於中央 Apex Central 使用者定義清單中，則在下次同步處理期間，節點 Apex Central 沙箱清單的可疑物件風險等級會變更為「高」。</td></tr>
<tr><td>設定可疑物件設定</td><td>建議使用

透過中央 Apex Central 設定可疑物件，可確保已註冊的節點 Apex Central 伺服器彼此一致。</td><td>無</td></tr>
</table>

部分 VII

自動化中心

第 23 章

Apex Central 自動化中心

Apex Central 提供 RESTful API，讓您能夠存取特定產品功能。您可以使用這些 API 將第三方解決方案與 Apex Central 整合、蒐集並共用可疑物件資訊，以及自動執行調查和管理工作。

如需詳細資訊，請參閱 https://automation.trendmicro.com/apex-central/home。

部分 VIII

工具和支援

第 24 章

管理資料庫

此區段顯示管理員管理 Apex Central 網路所需的材料。

包含下列主題：

- 瞭解 Apex Central 資料庫 第 24-2 頁
- 使用 SQL Server Management Studio 備份 db_ApexCentral 第 24-9 頁
- 使用 SQL 指令壓縮 db_ApexCentral_Log.ldf 第 24-11 頁
- 使用 SQL Server Management Studio 壓縮 db_ApexCentral_log.ldf 第 24-12 頁

瞭解 Apex Central 資料庫

Apex Central 使用 Microsoft SQL Server 資料庫 (db_ApexCentral.mdf) 來儲存記錄檔所包含的資料、通訊器預約時程、受管理產品和子伺服器資訊、使用者帳號、網路環境及通知設定。

Apex Central 伺服器使用系統 DSN ODBC 連線建立資料庫連線。Apex Central 安裝會產生此連線，以及用於存取 db_ApexCentral.mdf 的 ID 和密碼。預設 ID 為 sa。Apex Central 會對密碼加密。

如果要獲得最大的 SQL Server 安全防護，請為用來管理 db_ApexCentral 的所有 SQL 帳號設定下列最低權限：

- dbcreator（針對伺服器角色）
- db_owner 角色（針對 db_ApexCentral）

受管理產品的記錄檔會造成資料庫日益龐大。受管理產品會傳送各種記錄類型到 Apex Central。

下表列出每一種記錄類型的記錄檔計數與資料庫大小。

表 24-1. 記錄檔計數和資料庫大小

記錄類型	記錄檔計數	資料庫大小 (MB)
病毒	100,000	150
	500,000	750
	1,000,000	1,500
間諜程式/可能的資安威脅程式	100,000	150
	500,000	750
	1,000,000	1,500
Web 安全	100,000	150
	500,000	750
	1,000,000	1,500

記錄類型	記錄檔計數	資料庫大小 (MB)
行為監控	100,000	120
	500,000	600
	1,000,000	1,200
資料外洩防護	100,000	300
	500,000	1,500
	1,000,000	3,000
檔案雜湊偵測	100,000	180
	500,000	900
	1,000,000	1,800
攻擊發現	100,000	1,200
	500,000	6,000
	1,000,000	12,000
入侵防護	100,000	70
	500,000	350
	1,000,000	700
Application Control	100,000	200
	500,000	1,000
	1,000,000	2,000

儲存記錄檔所需的資料庫空間可以根據記錄檔的類型和數量計算出來。例如：

- Apex One 受管理產品每天會傳送 20,000 個病毒記錄檔和 10,000 個 Web 安全記錄檔到 Apex Central。
- Apex Central 會保留這兩種記錄檔類型 90 天。

病毒記錄檔和 Web 安全記錄檔所需的資料庫空間分別是 1.2 GB 和 1 GB。不過，也可能需要額外空間供記錄檔摘要或其他功能使用。

由於 Apex Central 資料庫在可擴充資料庫（即 SQL Server）上執行，因此理論上的限制是硬體可處理的容量。Trend Micro 已測試過多達 2,000,000 個項目。如果資料庫伺服器的效能過度運用或達到其上限，則 Web 主控台可能會發生連線逾時。

秘訣

Trend Micro 建議您針對資料庫成長配置大量的緩衝空間，並監控資料庫來協助準確測量資料庫大小。

瞭解 db_ApexCentral 資料表

如果要存取 Apex Central 資料庫中的所有資料表，請使用 Microsoft Access 專案 (*.adp/*.ade) 或 Microsoft SQL Management Studio。

注意

未經趨勢科技客服部門的指示，請勿使用任何 SQL 工具來新增、刪除或修改記錄。

Apex Central 資料庫由下列資料表所組成：

表 24-2. 使用者/端點目錄資料表

目錄管理資料表	說明
tb_WebSecurityLog	儲存來自產品的 Web 存取違規記錄檔
tb_SecurityLog	儲存接收自 ScanMail 和 InterScan Messaging 產品的內容違規記錄檔
tb_LogGeneral	儲存來自網路型產品（例如 Deep Discovery Inspector）的網路封包掃瞄記錄檔
tb_LogDataLossPrevention	儲存從產品傳送/接收自產品的資料外洩防護相關記錄檔

目錄管理資料表	說明
tb_AV*Log * 對應到病毒、事件、StatusEngineInfo 和 StatusPatternInfo	儲存產品記錄檔 病毒資料表儲存產品所偵測到的病毒/惡意程式事件記錄檔。其他資料表則儲存產品狀態記錄檔，以及病毒碼和引擎版本、更新和部署時間、未處理的病毒計數。
tb_SpywareLog	儲存產品所偵測到的惡意間諜程式資訊
tb_PersonalFirewallLog	儲存來自 OfficeScan 的個人防火牆偵測記錄檔
tb_LogBehaviorMonitor	儲存 Officescan 所偵測到的惡意系統行為事件
tb_Network_Content_Inspection_Engine_Log	儲存來自 OfficeScan 的已封鎖 C&C 伺服器連線嘗試記錄檔
tb_FileHashDetectionLog	儲存來自受管理產品的可疑檔案偵測記錄檔
tb_LogIntrusionPrevention	儲存來自 Deep Security 和 Vulnerability Protection 的入侵防護記錄檔
tb_MachineLearning_Detection_Log	儲存來自 OfficeScan 的 Machine Learning 偵測記錄檔
tb_ApplicationControlEvent	儲存來自 Endpoint Application Control 的 Endpoint Application Control 違規記錄檔
tb_SandboxDetectionlog	儲存來自受管理產品的沙箱偵測記錄檔

表 24-3. 目錄管理資料表

目錄管理資料表	說明
CDSM_Entity	儲存受管理產品資訊
CDSM_Agent	儲存通訊器資訊
CDSM_Registry	儲存登錄資訊
CDSM_UserLog	儲存有關誰存取 Web 主控台、存取哪些選項，以及使用者何時存取 Web 主控台等資訊；這有助於稽核 Web 主控台存取
CDSM_SystemEventlog	儲存內部處理程序產生的系統記錄檔

表 24-4. 伺服器指令控制器資料表

伺服器指令控制器資料表	說明
tb_TVCSCommandList	儲存受管理產品指令
tb_TVCSCommandTaskQueue	儲存向受管理產品發出的指令
tb_CommandTracking	儲存指令狀態
tb_CommandItemTracking	儲存詳細的指令狀態
tb_ProcessInfo	儲存 `MsgReceiver.exe`、`CmdProcessor.exe`、`LogReceiver.exe`、`LogRetriever.exe` 等的相關資訊。
tb_LoginUserSessionData	儲存使用者登入作業階段控制
tb_ManualDownload	儲存手動下載資訊
tb_ScheduleDownload	儲存預約下載資訊

表 24-5. 受管理產品資料表

受管理產品資料表	說明
tb_EntityInfo	儲存受管理產品資訊

表 24-6. 記錄檔資料表

記錄檔資料表	說明
tb_TempLog	儲存產品記錄檔的原始資料
tb_AV*Log	儲存產品記錄檔 * 對應到 Virus、Event、Status、PEInfo、WebSecurity。 這些資料表儲存產品狀態記錄檔，以及病毒碼和引擎版本、更新和部署時間、未處理的病毒計數。
tb_InValidLog	儲存無法識別的記錄檔資訊

記錄檔資料表	說明
• tb_TotalWebSecurityCount • tb_TotalVirusCount • tb_TotalSecurityCount • tb_TopTenSource • tb_TopTenDestination • tb_TopTenVirus	儲存狀態摘要和報告的病毒摘要資訊
tb_LogPurgePolicy	儲存清除記錄檔設定
tb_LogPurgeCounter	儲存清除記錄檔計數器
• tb_InstanceForVirusOutbreak • tb_InstanceForSpecialVirus • tb_InstanceForVirusOutbreak	儲存警訊通知中使用的記錄檔執行個體

表 24-7. 通知資料表

通知資料表	說明
• tb_Alert_NTF_JobList • tb_Event_NTF_JobList	儲存通知佇列清單
tb_EventNotificationFilter	儲存事件中心組態設定

通知資料表	說明
• tb_SendEMailNotification • tb_SendSNMPTrapNotification • tb_SendWindowsNTEventLogNotification • tb_LaunchAProgramNotification • tb_SendSysLogNotification	儲存通知方法設定
tb_VirusOutBreakPolicy	儲存病毒爆發期間使用的規則
tb_SpecialVirusPolicy	儲存使用者指定的病毒名稱
• tb_VirusOutbreakAccumulate • tb_SpecialVirusAccumulate	儲存病毒計數器資訊
• tb_UGNtfRelation • tb_NtfUserGROUP • tb_GroupAndUserRelation	儲存使用者和群組通知設定

表 24-8. 報告資料表

報告資料表	說明
• tb_ReportScheduleTask • tb_ReportTaskQueue	儲存及處理報告產生工作
tb_ReportItemTracking	儲存報告範本檔案目錄

表 24-9. 病毒碼和引擎部署資料表

病毒碼和引擎部署資料表	說明
• tb_DeploymentPlans • tb_DeploymentPlansTF	儲存部署計劃資訊
tb_DeploymentPlanTasks	儲存部署工作佇列
tb_DeployNowJobList	儲存進行中的部署計劃狀態
tb_DeployCommandTracking	儲存部署指令追蹤資訊
tb_DeploymentPlanTargets	儲存套用了部署指令的受管理產品資訊

使用 SQL Server Management Studio 備份 db_ApexCentral

使用 SQL Server 時，請使用 SQL Server Management Studio 來備份 Apex Central 資料庫。

注意

Trend Micro 建議您定期備份 Apex Central 資料庫。在修改 Apex Central 資料庫（例如，新增或安裝受管理的產品）之前，請務必先進行備份。

步驟

1. 在 Apex Central 伺服器中，按一下「開始 > 所有程式 > Microsoft SQL Server <版本> > SQL Server Management Studio」。

   <版本> 是 SQL Server Management Studio 的版本。

2. 在功能表列中，按一下「檢視 > 物件總管」。在「物件總管」面板中，按兩下「<主機\執行個體名稱>」，然後按兩下「資料庫」。

   <主機\執行個體名稱> 是 SQL Server 主機名稱和 SQL 執行個體名稱。

3. 以滑鼠右鍵按一下「db_ApexCentral」，然後按一下「工作 > 備份」。
4. 在「備份組」下方，提供「名稱」和「說明」。
5. 在「來源 > 備份類型」下方，選取「完整」。
6. 在「目的地」下方，按一下「新增」以指定備份檔案目的地。
7. 當顯示「備份作業已成功完成」訊息時，請按一下「確定」。

使用 SQL Server Management Studio 還原備份 db_ApexCentral

使用 SQL Server Management Studio 還原備份 Apex Central 資料庫。

步驟

1. 停止 Apex Central。
2. 按一下「開始 > 程式集 > 系統管理工具 > 服務」以開啟「服務」畫面。
3. 以滑鼠右鍵按一下「<Apex Central Service>」，然後按一下「停止」。
4. 按一下「程式集 > SQL Server Management Studio」來存取 SQL Server Management Studio。
5. 在主控台上，按一下「SQL 伺服器群組 > {SQL server} > 資料庫」。

   {SQL server} 是 SQL Server 主機名稱。
6. 以滑鼠右鍵按一下「db_ApexCentral > 所有工作 > 還原資料庫...」。
7. 在「還原資料庫」畫面上，選取要還原的資料庫。
8. 按一下「確定」來啟動還原程序。
9. 出現「還原資料庫 '{Apex Central database"}' 已成功完成」的訊息時，按一下「確定」。
10. 按一下「開始 > 程式集 > 系統管理工具 > 服務」以開啟「服務」畫面。

11. 以滑鼠右鍵按一下「<Apex Central Service>」，然後按一下「重新啟動」。
12. 啟動 Apex Central。

使用 SQL 指令壓縮 db_ApexCentral_Log.ldf

步驟

1. 請使用 SQL Server Management Studio 備份 Apex Central 資料庫。
2. 從可用的資料庫中，選取 db_ApexCentral 資料庫。
3. 執行下列 SQL 程式檔：

```
DBCC shrinkfile('db_ApexCentral_log', 10)
```

4. 確認 db_ApexCentral_Log.LDF 的大小小於 10 MB。

   如果 db_ApexCentral_Log.LDF 的大小並未減少，請使用下列 SQL 指令來識別所使用的資料庫復原模式：

```
SELECT name as DatabaseName, DATABASEPROPERTYEX(name, 'Reco
very') as RecoveryMode FROM master.dbo.sysdatabases where n
ame='db_ApexCentral'
```

   如果資料庫復原模式為 FULL，請執行下列 SQL 程序檔：

```
-- Truncate the log by changing the database recovery model
 to SIMPLE.
ALTER DATABASE db_ApexCentral
SET RECOVERY SIMPLE;
GO
-- Shrink the truncated log file to 10 MB.
DBCC SHRINKFILE (db_ApexCentral_Log, 10);
GO
-- Reset the database recovery model.
ALTER DATABASE db_ApexCentral
```

```
SET RECOVERY FULL;
GO
```

如需壓縮 SQL 資料庫和 SQL 指令的詳細資訊，請參閱《Microsoft SQL Server 管理》文件。

使用 SQL Server Management Studio 壓縮 db_ApexCentral_log.ldf

Apex Central 資料庫的交易記錄檔是 …\data\db_ApexCentral_log.LDF。SQL Server 在其正常作業過程中會產生交易記錄。

db_ApexCentral_log.LDF 包含使用 db_ApexCentral.mdf 的所有受管理產品交易。

依預設，交易記錄檔在 SQL Server 組態設定上沒有任何檔案大小限制。這會導致可用的磁碟空間耗盡。

在 Microsoft SQL Server 2008（或更新版本）上壓縮 db_ApexCentral_log.ldf 檔案大小

步驟

1. 請使用 SQL Server Management Studio 備份 Apex Central 資料庫。
2. 清除交易記錄。
3. 在 SQL Server 上，按一下「程式集 > SQL Server Management Studio」，來開啟 SQL Server Management Studio。
4. 選取 SQL Server，並在出現提示時指定驗證認證。
5. 以滑鼠右鍵按一下 db_ApexCentral，然後選取「內容」。

   會出現「內容」對話方塊。

6. 按一下「選項」。

   會出現「選項」工作區。

7. 從「復原模式:」清單中選取「簡易」。

8. 請點選「確定」。

第 25 章

Apex Central 工具

本節討論如何使用多個 Apex Central 組態設定工具。

包含下列主題：

- 關於 Apex Central 工具 第 25-2 頁
- 使用用戶端移轉工具 (AgentMigrateTool.exe) 第 25-2 頁
- 使用資料庫組態設定工具 (DBConfig.exe) 第 25-2 頁

關於 Apex Central 工具

Apex Central 提供多種工具，可協助您處理特定的組態設定工作。Apex Central 的大多數工具存放在下列位置：

```
<Apex Central 安裝目錄>\WebUI\download\tools\
```

使用用戶端移轉工具 (AgentMigrateTool.exe)

Apex Central 所提供的用戶端移轉工具可以用來移轉受另一部 Apex Central 伺服器管理的用戶端。

注意

此用戶端移轉工具支援以 Windows 與 Linux 為基礎的用戶端移轉。

步驟

1. 使用「管理員」帳號登入目標伺服器。

   重要

   只有「管理員」帳號具有足夠權限來執行此用戶端移轉工具。

2. 從下列位置執行 `AgentMigrateTool.exe`：`<Apex Central 安裝目錄>\`

使用資料庫組態設定工具 (DBConfig.exe)

`DBConfig.exe` 工具可讓使用者變更用於 Apex Central 資料庫的使用者帳號、密碼和資料庫名稱。

此工具提供下列選項：

- DBName：資料庫名稱
- DBAccount：資料庫帳號
- DBPassword：資料庫密碼
- Mode：資料庫驗證模式（「SQL Server 驗證」或「Windows 驗證」）

注意

預設資料庫驗證模式為「SQL Server 驗證」模式。不過，設定進行 Windows 驗證時，將需要「Windows 驗證」模式。

步驟

1. 在 Apex Central 伺服器上開啟指令提示字元。
2. 使用下列指令找出包含 `DBConfig.exe` 檔案的目錄：

   ```
   cd <Apex Central 安裝目錄>\DBConfig
   ```

3. 輸入 `dbconfig` 並按 `Enter` 鍵。

   會出現 DBConfig 工具介面。

4. 指定您要修改的設定：
   - 範例 1：`DBConfig -DBName="db_your_database>" -DBAccount="sqlAct" -DBPassword="sqlPwd" -Mode="SQL"`
   - 範例 2：`DBConfig -DBName="db_your_database>" -DBAccount="winAct" -DBPassword="winPwd" -Mode="WA"`
   - 範例 3：`DBConfig -DBName="db_your_database>" -DBPassword="sqlPwd"`

第 26 章

技術支援

瞭解下列主題：

- 疑難排解資源 第 26-2 頁
- 聯絡趨勢科技 第 26-3 頁
- 將可疑內容傳送到趨勢科技 第 26-4 頁
- 其他資源 第 26-5 頁

疑難排解資源

聯絡技術支援之前，請考慮造訪下列趨勢科技線上資源。

使用支援入口網站

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

步驟

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

   秘訣

   若要線上提交支援案例，請造訪下列 URL：

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

   趨勢科技支援工程師會在 24 小時或更短時間內調查案例並對其進行回應。

安全威脅百科全書

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

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

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

聯絡趨勢科技

可以透過電話或電子郵件聯絡趨勢科技代表：

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

- 全球客戶服務據點：

  https://www.trendmicro.com/us/about-us/contact/index.html
- 趨勢科技產品文件：

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

加速支援要求

為了提高解決問題的速度，現已提供下列資訊：

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

將可疑內容傳送到趨勢科技

有多個選項可供將可疑內容傳送到趨勢科技，以便進一步分析。

電子郵件信譽評等服務

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

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

請參閱下列「常見問題集」項目，將訊息範例傳送給趨勢科技：

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

檔案信譽評等服務

收集系統資訊並將可疑檔案內容提交到趨勢科技：

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

記錄案例編號以供追蹤。

網頁信譽評等服務

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

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

如果指定的分級不正確，請傳送重新分類要求到趨勢科技。

其他資源

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

下載專區

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

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

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

文件意見反應

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

附錄

附錄

附錄 A

Apex Central 系統檢查清單

請使用本節的檢查清單來記錄相關系統資訊做為參考。

包含下列主題：

- 伺服器位址檢查清單 第 A-2 頁
- 通訊埠檢查清單 第 A-3 頁
- Apex Central 慣例 第 A-3 頁
- 核心處理程序和組態設定檔 第 A-4 頁
- 通訊和監聽通訊埠 第 A-6 頁

伺服器位址檢查清單

在安裝過程中，以及在設定 Apex Central 伺服器的過程中，您都必須提供下列伺服器位址資訊，以便使用您的網路。請記下此處的資訊以方便參考。

表 A-1. 伺服器位址檢查清單

需要的資訊	範例	您的值
Apex Central 伺服器資訊		
IP 位址	10.1.104.255	
完整的網域名稱 (FQDN)	server.company.com	
NetBIOS（主機）名稱	yourserver	
Web 伺服器資訊		
IP 位址	10.1.104.225	
完整的網域名稱 (FQDN)	server.company.com	
NetBIOS（主機）名稱	yourserver	
以 SQL 為基礎的 Apex Central 資料庫資訊		
IP 位址	10.1.104.225	
完整的網域名稱 (FQDN)	server.company.com	
NetBIOS（主機）名稱	sqlserver	
用於下載元件的 Proxy 伺服器		
IP 位址	10.1.174.225	
完整的網域名稱 (FQDN)	proxy.company.com	
NetBIOS（主機）名稱	proxyserver	
SMTP 伺服器資訊（選用，用於電子郵件通知）		
IP 位址	10.1.123.225	

需要的資訊	範例	您的值
完整的網域名稱 (FQDN)	mail.company.com	
NetBIOS（主機）名稱	mailserver	
SNMP Trap 資訊（選用，用於 SNMP Trap 通知）		
社群名稱	trendmicro	
IP 位址	10.1.194.225	
Syslog 伺服器資訊（選用，用於 Syslog 通知）		
IP 位址	10.1.194.225	
伺服器通訊埠	514	

通訊埠檢查清單

Apex Central 使用下列通訊埠執行所指示的用途。

通訊埠	範例	您的值
SMTP	25	
Proxy	8088	
Web 主控台和更新/部署元件	80	

Apex Central 慣例

請參閱下列適用於 Apex Central 安裝或 Web 主控台組態設定的慣例。

- 使用者名稱
  - 最大長度：32 個字元

- 允許的字元：A-Z、a-z、0-9、-、_、.、$

- 資料夾名稱
  - 最大長度：32 個字元
  - 不允許的字元：/、>、&、"、%、^、=

注意

對於 Apex Central 伺服器主機名稱，安裝程式支援伺服器使用底線 ("_") 做為伺服器名稱的一部分。

核心處理程序和組態設定檔

Apex Central 會以 XML 格式儲存系統組態設定和暫存檔案。

下表說明 Apex Central 所使用的組態設定檔和處理程序。

表 A-2. Apex Central 組態設定檔

組態設定檔	說明
AuthInfo.ini	此組態設定檔包含有關私密金鑰檔案名稱、公開金鑰檔案名稱、憑證檔案名稱、私密金鑰的加密複雜密碼，以及主機識別碼和通訊埠等資訊。
aucfg.ini	主動式更新組態設定檔
TVCS_Cert.pem	SSL 驗證使用的憑證
TVCS_Pri.pem	SSL 使用的私密金鑰
TVCS_Pub.pem	SSL 使用的公開公鑰
ProcessManager.xml	由 ProcessManager.exe 使用
CmdProcessorEventHandler.xml	由 CmdProcessor.exe 使用
DMRegisterinfo.xml	由 CasProcessor.exe 使用

組態設定檔	說明
DataSource.xml	儲存 Apex Central 處理程序的連線參數
SystemConfiguration.xml	Apex Central 系統組態設定檔
agent.ini	MCP 代理程式檔案

表 A-3. Apex Central 核心處理程序

程序	說明
ProcessManager.exe	啟動和停止其他 Apex Central 核心處理程序
CmdProcessor.exe	傳送 XML 指令（由其他處理程序定義格式）給受管理產品，來處理產品註冊、傳送警訊、執行預約工作及套用病毒爆發防範策略
LogReceiver.exe	接收受管理產品的記錄檔和訊息。從 Control Manager 7.0 開始，LogReceiver.exe 只會處理來自 Trend Micro Damage Control Services 和「趨勢科技安全弱點評估」的記錄檔
LogProcessor.exe	從受管理產品接收記錄檔，以及從受管理產品接收實體資訊
LogRetriever.exe	擷取並儲存 Apex Central 資料庫中的記錄檔
ReportServer.exe	產生 Apex Central 報告
MsgReceiver.exe	從 Apex Central 伺服器和受管理產品接收訊息
CasProcessor.exe	允許 Apex Central 伺服器管理其他 Apex Central 伺服器
inetinfo.exe	Microsoft Internet Information Service 處理程序
cm.exe	管理 dmserver.exe 和 mrf.exe
dmserver.exe	提供 Apex Central Web 主控台登入頁面，以及管理「產品目錄」（Apex Central 端）
sCloudProcessor.NET.exe	可要求 Apex Central Web 主控台或其他處理程序提供核發者的工作識別碼，以查詢狀態、查詢結果及取消要求；由「使用者/端點目錄」使用

通訊和監聽通訊埠

下列是預設的 Apex Central 通訊和監聽通訊埠。

服務	服務通訊埠
ProcessManager.exe	20501
CmdProcessor.exe	20101
comdProcessor.NET.exe	21003
LogReceiver.exe	20201
LogProcessor.exe	21001
LogRetriever.exe	20301
ReportServer.exe	20601
MsgReceiver.exe	20001
CasProcessor.exe	20801
sCloudProcessor.NET.exe	21002

附錄 B

資料檢視

本節說明 Apex Central 支援可用於自訂報告範本和記錄查詢的資料檢視。

包含下列主題：

- 資料檢視：安全記錄檔 第 B-2 頁
- 資料檢視：產品資訊 第 B-88 頁

資料檢視：安全記錄檔

顯示受管理產品所偵測的安全威脅相關資訊：病毒、間諜程式/可能的資安威脅程式、網路釣魚網站等。

進階安全威脅資訊

顯示受管理產品在您網路中偵測到的進階持續安全威脅和目標式攻擊的摘要和詳細資料。

C&C 回呼詳細資訊

提供有關網路上偵測到的 C&C 回呼事件的特定資訊

表 B-1. C&C 回呼詳細資訊資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
遭到入侵的主機	嘗試做出回呼的 IP 位址、主機名稱或電子郵件信箱
回呼位址	遭到入侵的主機嘗試從其或對其做出回呼的物件
C&C 清單來源	辨識 C&C 伺服器的 C&C 清單來源 • C&C IP 清單 • 全球資訊清單 • 使用者定義的 IP 清單 • 沙箱清單
網路群組	受管理產品（例如 Deep Discovery Inspector）的管理員所定義的受監控網路群組

資料	說明
C&C 風險等級	趨勢科技指派給事件的風險等級： • 高：已知是惡意的，或涉及高嚴重性連線 • 中：信譽評等服務尚未掌握其情況的 IP 位址/網域/URL • 低：信譽評等服務指出以前曾涉及入侵或垃圾郵件活動
C&C 伺服器位置	C&C 伺服器所在的地區和國家
首次監控到	趨勢科技首次偵測到回呼位址的日期和時間
上次活動	遭到入侵的主機上次聯絡回呼位址的日期和時間
惡意程式系列	與回呼位址關聯的惡意程式名稱
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
產品項目	Apex Central 中受管理產品伺服器的顯示名稱

Machine Learning 詳細資訊

提供有關 Machine Learning 偵測到的進階未知安全威脅的特定資訊

表 B-2. Machine Learning 詳細資訊

資料	說明
偵測時間	受管理產品伺服器或 Security Agent 偵測到安全威脅的日期和時間
收到	Apex Central 從受管理產品接收資料的日期和時間
產品實體/端點	根據相關的來源： • Apex Central 中受管理產品伺服器的顯示名稱 • 端點的名稱或 IP 位址

資料	說明
產品/端點 IP	根據相關的來源： • 受管理產品伺服器的 IP 位址 • 端點的 IP 位址
產品	受管理產品或服務的名稱
伺服器	Apex Central 中受管理產品伺服器的顯示名稱
可能的安全威脅類型	Machine Learning 在將分析結果與其他已知的安全威脅相比較後，所發現檔案中最可能包含的安全威脅類型
安全威脅	安全威脅的名稱
登入使用者	事件發生當時已登入的使用者名稱
類型	觸發偵測的物件類型（「檔案」或「程序」）
檔案路徑	執行程序的檔案物件路徑或程式路徑
檔案建立時間	檔案物件的建立日期和時間
父程序	觸發所偵測到程序的程序
程序指令	執行所偵測到程序的指令
程序擁有者	觸發所偵測到程序的使用者名稱
端點感染通道	安全威脅源自的通道
感染來源	安全威脅的來源
安全威脅可能性	檔案/程序符合惡意程式模型的程度
處理行動結果	受管理產品採取的處理行動結果
主旨	觸發偵測的電子郵件主旨
傳送時間	電子郵件傳送到郵件伺服器的日期和時間
寄件者	觸發偵測的電子郵件寄件者
收件者	觸發偵測的電子郵件收件者

資料	說明
雲端服務供應商	雲端服務供應商的名稱

可疑檔案詳細資訊

提供有關網路中偵測到的可疑檔案的特定資訊

表 B-3. 可疑檔案詳細資訊資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已偵測	受管理產品偵測到安全威脅的日期和時間
端點	端點的名稱
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
產品項目	Apex Central 中受管理產品伺服器的顯示名稱
端點 IP 位址	端點的 IP 位址
端點主機名稱	端點的主機名稱
檔案類型	檔案物件的類型
檔案 SHA-1	檔案物件的 SHA-1 雜湊值
檔案路徑	執行程序的檔案物件路徑或程式路徑
C&C 清單來源	辨識 C&C 伺服器的 C&C 清單來源 • C&C IP 清單 • 全球資訊清單 • 使用者定義的 IP 清單 • 沙箱清單
處理行動	受管理產品採取的處理行動

資料	說明
掃瞄類型	報告事件的掃瞄類型（例如，即時掃瞄、預約掃瞄、手動掃瞄）
已建立	檔案物件的建立日期和時間
已修改	檔案物件上次修改的日期和時間

沙箱偵測資訊

提供有關沙箱偵測到的進階未知安全威脅的特定資訊

表 B-4. 沙箱偵測資訊

資料	說明
已產生	受管理產品產生資料的日期和時間
收到	Apex Central 從受管理產品接收資料的日期和時間
產品	受管理產品或服務的名稱
伺服器名稱	伺服器的名稱
主機	主機的名稱
項目通道	感染通道
來源	安全威脅的來源
目標	安全威脅的目標位置
程序名稱	觸發偵測的程序名稱
SHA1	觸發偵測的檔案物件 SHA-1 雜湊值
類型	觸發偵測的物件類型（「檔案」或「程序」）
檔案名稱	觸發偵測的檔案物件名稱
檔案類型	觸發偵測的檔案物件類型
URL	觸發偵測的 URL 物件

資料	說明
提交規則	沙箱所提交的規則
提交時間	沙箱提交規則的日期和時間
完成時間	沙箱完成分析的日期和時間
安全威脅	安全威脅的名稱
風險等級	沙箱指派的風險等級
安全威脅類別	安全威脅的類型
最嚴重的安全威脅	依嚴重性等級排名之最嚴重的安全威脅
雲端服務供應商	雲端服務供應商的名稱

沙箱可疑物件影響詳細資訊

提供有關沙箱可疑物件之影響的詳細資訊

資料	說明
類型	可疑物件的類型
物件	可疑物件的名稱
中毒處理行動	偵測到可疑物件的受管理產品所執行的中毒處理行動（例如記錄、封鎖）
風險等級	安全威脅的風險等級
到期	為可疑物件設定的到期日期和時間
第一次提交時間	受管理產品第一次將可疑物件提交到沙箱的日期和時間
第一次提交產品名稱	第一次將可疑物件提交到沙箱的受管理產品的名稱
第一次提交主機名稱	第一次將可疑物件提交到沙箱的受管理伺服器的顯示名稱
第一次提交 IP 位址	第一次將可疑物件提交到沙箱的受管理伺服器的 IP 位址
第一次提交檔案名稱	受管理產品第一次提交到沙箱的可疑物件的檔案名稱

資料	說明
第一次提交檔案類型	受管理產品第一次提交到沙箱的可疑物件的檔案類型
第一次提交來源	受管理產品第一次提交到沙箱的可疑物件的來源
第一次提交目標	受管理產品第一次提交到沙箱的可疑物件的目標
最近一次提交時間	受管理產品最近一次將可疑物件提交到沙箱的日期和時間
最近一次提交產品名稱	最近一次將可疑物件提交到沙箱的受管理產品的名稱
最近一次提交主機名稱	最近一次將可疑物件提交到沙箱的受管理產品的顯示名稱
最近一次提交 IP 位址	最近一次將可疑物件提交到沙箱的受管理伺服器的 IP 位址
最近一次提交檔案名稱	受管理產品最近一次提交到沙箱的可疑物件的檔案名稱
最近一次提交檔案類型	受管理產品最近一次提交到沙箱的可疑物件的檔案類型
最近一次提交檔案 SHA-1	受管理產品最近一次提交到沙箱的可疑物件的檔案 SHA-1
最近一次提交偵測名稱	受管理產品最近一次提交到沙箱的可疑物件的偵測名稱
最近一次提交來源	受管理產品最近一次提交到沙箱的可疑物件的來源
最近一次提交目標	受管理產品最近一次提交到沙箱的可疑物件的目標
端點網域名稱	觸發偵測的端點網域名稱
端點主機名稱	觸發偵測的端點顯示名稱
端點使用者網域名稱	偵測時登入端點的使用者網域名稱
端點使用者網域帳號	偵測時登入端點的使用者網域帳號
端點使用者名稱	事件發生當時已登入的使用者名稱
端點 IP 位址	端點的 IP 位址

資料	說明
端點第一次發現時間	在端點上第一次偵測到可疑物件的日期和時間
端點第一個產品偵測	在端點上第一次偵測到可疑物件的受管理產品的名稱
端點第一個採取的處理行動	受管理產品在端點上所採取的第一個處理行動
端點上次發現時間	在端點上最近一次偵測到可疑物件的日期和時間
端點上一個產品偵測	在端點上最近一次偵測到可疑物件的受管理產品的名稱
端點上一個採取的處理行動	受管理產品在端點上所採取的上一個處理行動
端點上一個處理行動結果	受管理產品在端點上所採取的上一個處理行動的結果

攻擊發現偵測

顯示「攻擊發現」所提供的資訊。

攻擊發現偵測資訊

提供有關攻擊發現所偵測到的安全威脅的一般資訊

表 B-5. 攻擊發現偵測資訊

資料	說明
已產生	受管理產品產生資料的日期和時間
收到	Apex Central 從受管理產品接收資料的日期和時間
端點	端點的名稱
產品	受管理產品或服務的名稱
管理伺服器實體	端點向其回報之 Apex Central 中受管理產品伺服器的顯示名稱

資料	說明
產品版本	受管理產品的版本
策略	已偵測到 MITRE ATT&CK™ 策略 如需詳細資訊，請參閱 https://attack.mitre.org/tactics/enterprise/。
技術	已偵測到 MITRE ATT&CK™ 技術 如需詳細資訊，請參閱 https://attack.mitre.org/techniques/enterprise/。
端點 IP	端點的 IP 位址
風險等級	「攻擊發現」指派的風險等級
病毒碼版本	偵測類型的「攻擊發現」病毒碼號碼
規則 ID	偵測規則的序號
規則名稱	指定「攻擊發現」偵測哪些行為的規則
相關物件	偵測數目 按一下計數可檢視其他詳細資料。 如需詳細資訊，請參閱詳細的攻擊發現偵測資訊 第 B-10 頁。
產生時間 (本機時間)	「攻擊發現」偵測到安全威脅的時間（以用戶端的本機時區為準） 此時間會以 UTC 時差顯示。
執行個體 ID	指派給事件的偵測 ID 具有相同執行個體 ID 的項目屬於同一事件。

詳細的攻擊發現偵測資訊

提供有關攻擊發現所偵測到的安全威脅的一般資訊

表 B-6. 詳細的攻擊發現偵測資訊

資料	說明
物件值	受偵測到的安全威脅攻擊的目標物件名稱
物件類型	受偵測到的安全威脅攻擊的目標物件類型
首次記錄	「攻擊發現」第一次記錄安全威脅偵測的時間
檔案目錄	受偵測到的安全威脅攻擊的目標物件目錄
程序 ID	程序的 PID
CLI 指令	觸發安全威脅偵測的程序指令
簽署單位	憑證簽署單位
使用者網域	偵測到的使用者帳號的網域名稱
使用者名稱	與物件關聯的帳號名稱
模擬使用者名稱	安全威脅模擬的使用者名稱
驗證 ID	指派給登入作業階段的本機唯一識別碼
完整性層級	指派給登入使用者的保護或存取層級
檔案 SHA-1	物件檔案的 SHA-1 雜湊值
檔案 SHA-256	物件檔案的 SHA-256 雜湊值
檔案 MD5	物件檔案的 MD5 雜湊值
普查分級	趨勢科技安全威脅專家根據所記錄的檔案歷史記錄判定的分級
檔案安全擁有者	檔案內容中指明的檔案目前擁有者
檔案安全擁有者網域	檔案內容中指明的檔案目前擁有者網域
檔案安全上一任擁有者	檔案內容中指明的檔案上一任擁有者
檔案安全上一任擁有者網域	檔案內容中指明的檔案上一任擁有者網域
登錄機碼	安全威脅存取的登錄機碼

資料	說明
登錄值名稱	安全威脅存取的登錄值名稱
登錄值資料	安全威脅存取的登錄值資料
AMSI 應用程式名稱	與安全威脅關聯的應用程式名稱或程式檔語言
AMSI 應用程式完整路徑	與安全威脅關聯的應用程式完整路徑
AMSI 應用程式版本	與安全威脅關聯的應用程式版本
AMSI 程式檔來源	程式檔來源的檔案名稱和副檔名
AMSI 程式檔內容	程式檔的內容
AMSI 程式檔來源 SHA-1	程式檔來源的 SHA-1 雜湊值
AMSI 程式檔來源 SHA-256	程式檔來源的 SHA-256 雜湊值
來源 IP 位址	偵測到的安全威脅的來源 IP 位址
來源 IP 位址通訊埠	偵測到的安全威脅的來源 IP 位址通訊埠號碼
目標 IP 位址	安全威脅存取的 IP 位址
目標 IP 位址通訊埠	安全威脅存取的 IP 通訊埠號碼
目標 URL	安全威脅存取的 URL
目標網域	安全威脅存取的網域名稱
WMI 事件	與安全威脅關聯的 WMI 事件資訊
Windows 事件來源	Windows 事件記錄檔中指明的用來記錄事件的軟體名稱
Windows 事件記錄檔內容	觸發偵測的 Windows 事件記錄檔內容
驗證權限名稱	安全威脅竄改的授權權限名稱
驗證權限屬性	安全威脅竄改的授權權限屬性
驗證權限全部關閉	安全威脅竄改的「授權權限全部關閉」的狀態

內容違規資訊

顯示有關受管理產品在網路上偵測到的禁止內容的摘要和詳細資料。

內容違規處理行動/結果摘要

提供受管理產品對內容違規採取的處理行動摘要。範例：受管理產品對內容違規採取的處理行動，以及受所採取處理行動影響的電子郵件數目

表 B-7. 內容違規處理行動/結果摘要資料檢視

資料	說明
處理行動	顯示受管理產品對違反內容策略之電子郵件採取的處理行動類型。 範例：已轉寄、已清除附件中的巨集、已刪除
策略違規偵測計數	顯示受管理產品對其採取指定處理行動的違規數目。

歷來內容違規偵測摘要

提供一段時間（每天一次、每週一次、每月一次）內的內容違規偵測摘要。範例：收集摘要資料的時間和日期、受內容違規影響的端點數目、唯一內容違規總數，以及網路上的內容違規總數

表 B-8. 歷來內容違規偵測摘要資料檢視

資料	說明
日期/時間	顯示資料摘要發生的時間。
唯一策略	顯示受管理產品偵測到違反的唯一策略數目。 範例：受管理產品在 1 部電腦上偵測到相同策略的 10 個違規執行個體。 偵測數 = 10

資料	說明
唯一寄件者/使用者	顯示所傳送內容違反了受管理產品策略的唯一電子郵件信箱或使用者數目。 範例：受管理產品偵測到來自 3 部電腦之相同策略的 10 個違規執行個體。 唯一寄件者/使用者 = 3
唯一收件者	顯示所接收內容違反了受管理產品策略的唯一電子郵件收件者數目。 範例：受管理產品在 2 部電腦上偵測到相同策略的 10 個違規執行個體。 唯一收件者 = 2
偵測	顯示受管理產品偵測到的策略違規總數。 範例：受管理產品在 1 部電腦上偵測到相同策略的 10 個違規執行個體。 偵測數 = 10

內容違規策略摘要

提供特定策略引發之內容違規偵測的摘要。範例：違反的策略名稱、偵測到內容違規的過濾器類型、網路中的內容違規總數

表 B-9. 內容違規策略摘要資料檢視

資料	說明
策略	顯示端點違反的策略名稱。
過濾器類型	顯示觸發違規的過濾器類型。範例：內容過濾器、網路釣魚過濾器、URL 信譽評等過濾器

資料	說明
唯一寄件者/使用者	顯示所傳送內容違反了受管理產品策略的唯一電子郵件信箱或使用者數目。 範例：受管理產品偵測到來自 3 部電腦之相同策略的 10 個違規執行個體。 唯一寄件者/使用者 = 3
唯一收件者	顯示所接收內容違反了受管理產品策略的唯一電子郵件收件者數目。 範例：受管理產品在 2 部電腦上偵測到相同策略的 10 個違規執行個體。 唯一收件者 = 2
偵測	顯示受管理產品偵測到的策略違規總數。 範例：受管理產品在 1 部電腦上偵測到相同策略的 10 個違規執行個體。 偵測數 = 10

內容違規寄件者摘要

提供特定寄件者引發之內容違規偵測的摘要。範例：內容寄件者的名稱、唯一內容違規數目、網路中的內容違規總數

表 B-10. 內容違規寄件者摘要資料檢視

資料	說明
寄件者/使用者	顯示所傳送內容違反了受管理產品策略的電子郵件信箱或使用者。
偵測	顯示受管理產品偵測到的策略違規總數。 範例：受管理產品在 1 部電腦上偵測到相同策略的 10 個違規執行個體。 偵測數 = 10

資料	說明
唯一收件者	顯示所接收內容違反了受管理產品策略的唯一電子郵件收件者數目。 範例：受管理產品在 2 部電腦上偵測到相同策略的 10 個違規執行個體。 唯一收件者 = 2
唯一策略	顯示受管理產品偵測到違反的唯一策略數目。 範例：受管理產品在 1 部電腦上偵測到相同策略的 10 個違規執行個體。 偵測數 = 10

內容違規詳細資訊

提供有關內含內容違規之電子郵件的特定資訊（例如，偵測到內容違規的受管理產品、電子郵件的寄件者和收件者、內容違規策略的名稱，以及偵測到的違規總數）

表 B-11. 內容違規詳細資訊資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
產品項目	Apex Central 中受管理產品伺服器的顯示名稱
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
收件者	所接收內容違反了受管理產品策略的電子郵件收件者
寄件者/使用者	所傳送內容違反了受管理產品策略的電子郵件信箱或使用者
主旨	違反了策略之電子郵件的主旨行內容
策略	電子郵件違反的策略名稱

資料	說明
策略設定	電子郵件違反的策略設定
檔案位置	違反策略的檔案位置
檔案	違反策略的檔案名稱
URL	違反指定策略的 URL
風險等級	趨勢科技對您網路的風險評估 範例：高安全性、低安全性、中等安全性
過濾器類型	偵測到電子郵件違規的過濾器類型 範例：內容過濾器、大小過濾器、附件過濾器
子過濾器類型	偵測到電子郵件違規的子過濾器類型
過濾器處理行動	偵測過濾器對違反策略之電子郵件採取的處理行動 範例：清除、隔離、清除巨集
過濾器處理行動結果	偵測到違規之過濾器所採取處理行動的結果
處理行動	受管理產品採取的處理行動 範例：傳送、清除巨集、轉寄
偵測	偵測總數

內含進階安全威脅的電子郵件訊息

提供有關內含進階安全威脅之電子郵件的特定資訊（例如，異常行為、假資料或誤導資料、可疑和惡意行為特徵碼，以及表示系統遭到入侵但需要進一步調查以確認的字串）

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
產品項目	Apex Central 中受管理產品伺服器的顯示名稱

資料	說明
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
收件者	觸發偵測的電子郵件收件者
寄件者	觸發偵測的電子郵件寄件者
主旨	觸發偵測的電子郵件主旨
附件計數	電子郵件附件的數目
附件	電子郵件附件的名稱
附件類型	電子郵件附件的類型
處理行動	受管理產品採取的處理行動 範例：傳送、清除巨集、隔離
安全威脅類型	安全威脅的類型
安全威脅名稱	安全威脅的名稱
風險等級	調查後的電子郵件風險等級
來源 IP	最接近電子郵件寄件者的郵件傳輸用戶端 (MTA) IP 位址
訊息 ID	由管理員設定的唯一郵件 ID
連結計數	電子郵件中的連結數目
連結	電子郵件中的連結清單

資料發現資訊

顯示 Data Discovery 偵測的相關資訊。

資料發現資料外洩防護偵測資訊

顯示有關 Data Discovery 偵測到的事件的特定資訊

表 B-12. 資料發現資料外洩防護偵測資訊

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
規則	觸發偵測的規則名稱
端點	端點的名稱或 IP 位址
網域	受管理產品所屬的網域
使用者	事件發生當時已登入的使用者名稱
使用者網域	使用者所屬的網域名稱
檔案路徑	包含數位資產的位置完整路徑或通道（如果沒有來源可用的話）
檔案	安全威脅存取的檔案物件名稱
範本	事件觸發的確切規則名稱和範本
處理行動	受管理產品採取的處理行動
詳細資訊	其他資訊（例如，使用者為了繼續傳輸機密資料所提供的原因）

資料發現端點資訊

表 B-13. 資料發現端點資訊

資料	說明
已產生	顯示受管理產品產生記錄檔資料的時間。
端點	顯示資料外洩防護偵測到傳輸的電腦的 IP 位址或主機名稱。
裝置類別	顯示裝置類別的名稱（與 Windows 裝置管理員中顯示的一樣）。
裝置顯示名稱	顯示裝置的顯示名稱（與 Windows 裝置管理員中顯示的一樣）。
供應商	顯示提供裝置的公司名稱。

資料外洩防護資訊

顯示從受管理產品收集之 DLP 事件、範本相符項目和事件來源的相關資訊。

DLP 事件資訊

提供有關資料外洩防護偵測到的事件的特定資訊

表 B-14. DLP 事件資訊

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
事件 ID	事件的識別碼
嚴重性	事件的嚴重性等級
狀態	事件的偵測狀態
管理員	部門的管理員名稱
部門	部門的名稱
策略	觸發偵測的策略
產品項目/端點	端點的名稱
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
產品/端點 IP	根據相關的來源： • 受管理產品伺服器的 IP 位址 • 端點的 IP 位址
產品/端點 MAC	根據相關的來源： • 受管理產品伺服器的 MAC 位址 • Security Agent 端點的 MAC 位址

資料	說明
管理伺服器	端點向其回報之 Apex Central 中受管理產品伺服器的顯示名稱
端點	已安裝用戶端（例如 Apex One 用戶端）之電腦的 IP 位址或主機名稱
事件來源 (AD 顯示名稱)	事件來源的 Active Directory 顯示名稱
事件來源 (AD 帳號)	事件來源的 Active Directory 帳號名稱
事件來源 (寄件者)	來源電子郵件信箱
網站	觸發事件的網站 URL
收件者	目標電子郵件信箱
主旨	電子郵件的主旨
檔案位置	檔案的位置和名稱
檔案	觸發事件的檔案名稱
檔案/資料大小	觸發事件的檔案大小或資料大小
規則	事件所觸發的規則名稱
範本	在其中觸發範本相符項目的範本名稱
通道	透過其傳輸數位資產的實體
目標	傳輸的目標
處理行動	受管理產品採取的處理行動
事件	事件數目
雲端服務供應商	雲端服務供應商的名稱

DLP 範本相符項目資訊

表 B-15. DLP 範本相符項目資訊

資料	說明
識別碼	顯示記錄的唯一 ID。
收到	顯示受管理產品收到事件資訊的時間。
已產生	顯示觸發事件的時間。
產品實體/端點	此資料欄顯示下列其中一項： • 受管理產品的實體顯示名稱。Apex Central 使用受管理產品的實體顯示名稱識別受管理產品。 • 已安裝用戶端（例如 Apex One 用戶端）之電腦的 IP 位址或主機名稱。
產品	顯示受管理產品的名稱。範例：Apex One、ScanMail for Microsoft Exchange
產品/端點 IP	此資料欄顯示下列其中一項： • 安裝了受管理產品的伺服器 IP 位址。 • 已安裝用戶端（例如 Apex One 用戶端）之電腦的 IP 位址。
產品/端點 MAC	此資料欄顯示下列其中一項： • 安裝了受管理產品的伺服器 MAC 位址。 • 已安裝用戶端（例如 Apex One 用戶端）之電腦的 MAC 位址。
管理伺服器	顯示受管理產品（端點會向此產品註冊）的實體顯示名稱。Apex Central 使用受管理產品的實體顯示名稱識別受管理產品。
端點	顯示已安裝用戶端（例如 Apex One 用戶端）之電腦的 IP 位址或主機名稱。
事件來源 (使用者)	顯示登入的使用者名稱。
收件者	顯示目標電子郵件信箱。
主旨	顯示電子郵件訊息的主旨。

資料	說明
檔案位置	顯示檔案的位置和名稱。
檔案	顯示觸發事件的檔案名稱。
規則	顯示由事件觸發的規則名稱。
範本	顯示在其中觸發範本相符項目的範本名稱。
通道	顯示透過其傳輸數位資產的實體。

Deep Discovery 資訊

顯示有關受管理產品在網路上偵測到的可疑活動的摘要和詳細資料。

關聯詳細資訊

提供有關安全威脅詳細分析及矯正建議的特定資訊

表 B-16. 關聯詳細資訊資料檢視

資料	說明
已產生	受管理產品產生資料的日期和時間
IP 位址	端點的 IP 位址
網路群組	受監控的網路群組
通訊協定	受管理產品從其偵測到安全威脅的廣泛通訊協定群組
安全威脅類型	安全威脅的類型 範例：病毒、間諜程式/可能的資安威脅程式、詐騙
嚴重性	事件的嚴重性等級
偵測	偵測的類型（根據關聯規則）
詳細資訊	與偵測相關的備註或註解

資料	說明
MAC 位址	端點的 MAC 位址
主機名稱	端點的名稱
關聯規則 ID	關聯規則的規則 ID

緩和詳細資訊

提供有關網路上緩和伺服器為解決安全威脅所執行之工作的特定資訊

表 B-17. 緩和詳細資訊資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
緩和實體	Apex Central 中受管理產品伺服器的顯示名稱
產品	受管理產品或服務的名稱
端點 IP	端點的 IP 位址
端點	端點的名稱
資料來源	會產生安全威脅事件資訊的 Deep Discovery 產品或工作
資料來源主機	會產生安全威脅事件資訊之 Deep Discovery 產品的主機名稱
安全威脅事件	緩和伺服器記錄的安全威脅相關事件 如需詳細資訊，請參閱 http://docs.trendmicro.com/all/ent/tms/v2.6/en-us/tmtm_2.6_olh/help/info/threat_event_logs.htm。
緩和狀態	安全威脅事件（依狀態群組） 如需詳細資訊，請參閱 http://docs.trendmicro.com/all/ent/tms/v2.6/en-us/tmtm_2.6_olh/help/info/threat_event_logs.htm。

資料	說明
緩和詳細資料	有關安全威脅事件的緩和詳細資料 如需詳細資訊，請參閱 http://docs.trendmicro.com/all/ent/tms/v2.6/en-us/tmtm_2.6_olh/help/info/mitigation_status.htm。
偵測	偵測總數
詳細資訊	有關安全威脅的詳細資料

可疑安全威脅詳細資訊

提供有關網路上可疑安全威脅的特定資訊，例如：偵測到可疑安全威脅的受管理產品、有關來源與目標的特定資訊、網路上的可疑安全威脅總數

表 B-18. 可疑安全威脅詳細資訊資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
產品項目	Apex Central 中受管理產品伺服器的顯示名稱
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
緩和主機	緩和伺服器的主機名稱（例如，網路病毒牆執行器或 Threat Mitigator）
流量/連線	傳輸的方向
通訊協定群組	受管理產品從其偵測到安全威脅的廣泛通訊協定群組 範例：FTP、HTTP、P2P
通訊協定	受管理產品從其偵測到可疑安全威脅的通訊協定 範例：ARP、BitTorrent
目標 IP 位址	安全威脅存取的 IP 位址

資料	說明
目標主機	安全威脅存取的端點顯示名稱
目標通訊埠	安全威脅存取的 IP 通訊埠號碼
目標 MAC 位址	安全威脅存取的 MAC 位址
目標作業系統	安全威脅存取的端點作業系統
目標使用者 <x>	用來登入目標主機的名稱 <x> 是使用者名稱
登入 (目標使用者 <x>)	登入時間戳記 <x> 代表登入次數和特定的時間戳記
來源 IP 位址	偵測到的安全威脅的來源 IP 位址
來源主機名稱	安全威脅起源所在的端點名稱
來源通訊埠	偵測到的安全威脅的來源 IP 位址通訊埠號碼
來源 MAC 位址	偵測到的安全威脅的來源 MAC 位址
來源作業系統	安全威脅起源所在的端點作業系統
來源使用者 <x>	用來登入目標來源主機的名稱 <x> 是使用者名稱
登入 (來源使用者 <x>)	來源上的登入時間戳記 <x> 代表登入次數和特定的時間戳記
來源網域	安全威脅起源所在的端點網域
安全威脅類型	安全威脅的類型 範例：病毒、間諜程式/可能的資安威脅程式、詐騙
策略/規則名稱	觸發偵測的策略或規則
收件者	觸發偵測的傳輸收件者
寄件者	觸發偵測的傳輸寄件者

資料	說明
主旨	觸發偵測的電子郵件主旨
附件檔案名稱	附件的檔案名稱和副檔名
附件檔案類型	附件的檔案類型
附件 SHA-1	附件的 SHA-1 雜湊值
URL	視為可疑安全威脅的 URL
使用者	受管理產品偵測到安全威脅時已登入目標的使用者名稱
IM/IRC 使用者	Deep Discovery Inspector 偵測到違規時登入的即時通訊或 IRC 使用者名稱。
瀏覽器/FTP 用戶端	可疑安全威脅起源所在的 Web 瀏覽器或 FTP 端點。
檔案	執行程序的檔案物件或程式的名稱
壓縮檔中的檔案	壓縮封存檔中受影響的檔案物件名稱
封存檔 SHA-1	封存檔物件的 SHA-1 雜湊值
封存檔檔案類型	封存檔物件的類型
共用資料夾	顯示可疑安全威脅是否源自共用資料夾
SHA-1	檔案物件的 SHA-1 雜湊值
緩和處理行動	緩和伺服器採取的處理行動 範例：檔案已清除、檔案已丟棄、檔案已刪除
緩和結果	緩和伺服器採取的處理行動結果
來源 IP 群組	可疑安全威脅起源所在的來源 IP 位址群組
來源網路區域	可疑安全威脅起源所在的來源網路區域
端點群組	受可疑安全威脅影響之端點的 IP 位址群組
端點網路區域	受可疑安全威脅影響之端點的網路區域

資料	說明
偵測	偵測總數 範例：受管理產品在 1 部電腦上偵測到相同類型的 10 個違規執行個體。 偵測數 = 10
C&C 清單來源	辨識 C&C 伺服器的 C&C 清單來源 • C&C IP 清單 • 全球資訊清單 • 使用者定義的 IP 清單 • 沙箱清單
C&C 風險等級	C&C 回呼的風險等級
備註	事件的其他相關資訊
C&C 伺服器	C&C 伺服器的名稱、URL 或 IP 位址
C&C 伺服器類型	C&C 伺服器的類型
惡意程式類型	惡意程式的類型

可疑安全威脅整體摘要

提供有關您網路上可疑安全威脅的特定資訊。範例：違反的策略/規則、有關來源與目標的摘要資訊、網路上的可疑安全威脅總數

表 B-19. 可疑安全威脅整體摘要資料檢視

資料	說明
策略/規則名稱	顯示違反的策略/規則名稱。
通訊協定	顯示違規是透過哪個通訊協定發生的。 範例：HTTP、FTP、SMTP

資料	說明
唯一端點	顯示受可疑安全威脅影響的唯一電腦數目。 範例：受管理產品在 2 部電腦上偵測到相同類型的 10 個可疑安全威脅執行個體。 唯一端點 = 2
唯一來源	顯示可疑安全威脅起源所在的唯一來源數目。 範例：受管理產品從 3 部電腦上偵測到相同類型的 10 個可疑安全威脅執行個體。 唯一來源 = 3
唯一收件者	顯示所接收內容違反了受管理產品可疑安全威脅策略的唯一電子郵件訊息收件者數目。 範例：受管理產品在 2 部電腦上偵測到相同策略的 10 個可疑安全威脅違規執行個體。 唯一收件者 = 2
唯一寄件者	顯示所傳送內容違反了受管理產品可疑安全威脅策略的唯一電子郵件訊息寄件者數目。 範例：受管理產品偵測到來自 3 部電腦的相同策略之 10 個可疑安全威脅違規執行個體。 唯一寄件者 = 3
偵測	顯示受管理產品偵測到的策略/規則違規總數。 範例：受管理產品在 1 部電腦上偵測到相同類型的 10 個違規執行個體。 偵測數等於 10。
緩和	顯示網路病毒牆執行器裝置或 Trend Micro™ Threat Mitigator™ 對其採取處理行動的端點數目。
已清除的端點	顯示 Trend Micro Threat Mitigator 清除的端點總數。
清除端點率 (%)	顯示 Trend Micro Threat Mitigator 清除的端點佔偵測總數的百分比。

可疑來源摘要

提供從特定來源偵測到的可疑安全威脅摘要。範例：來源的名稱、有關目標與規則/違規的摘要資訊、網路上的可疑安全威脅總數

表 B-20. 可疑來源摘要資料檢視

資料	說明
來源 IP	顯示可疑安全威脅起源所在的來源 IP 位址。
唯一策略/規則	顯示來源電腦違反的唯一策略/規則數目。 範例：受管理產品在 2 部電腦上偵測到相同策略的 10 個策略違規執行個體。 唯一策略/規則 = 1
唯一端點	顯示受可疑安全威脅影響的唯一電腦數目。 範例：受管理產品在 2 部電腦上偵測到相同類型的 10 個可疑安全威脅執行個體。 唯一端點 = 2
偵測	顯示受管理產品偵測到的策略/規則違規總數。 範例：受管理產品在 1 部電腦上偵測到相同類型的 10 個違規執行個體。 偵測數 = 10

風險最高的可疑端點摘要

提供偵測到最可疑安全威脅的端點摘要。範例：目標的名稱、有關來源與規則/違規的摘要資訊、網路上的可疑安全威脅總數

表 B-21. 風險最高的可疑安全威脅端點摘要資料檢視

資料	說明
端點 IP	顯示受可疑安全威脅影響的電腦 IP 位址。

資料	說明
唯一策略/規則	顯示來源電腦違反的唯一策略/規則數目。 範例：受管理產品在 2 部電腦上偵測到相同策略的 10 個策略違規執行個體。 唯一策略/規則 = 1
唯一來源	顯示可疑安全威脅起源所在的唯一來源數目。 範例：受管理產品從 3 部電腦上偵測到相同類型的 10 個可疑安全威脅執行個體。 唯一來源 = 3
偵測	顯示受管理產品偵測到的策略/規則違規總數。 範例：受管理產品在 1 部電腦上偵測到相同類型的 10 個違規執行個體。 偵測數 = 10

風險最高的可疑收件者摘要

提供偵測到最可疑安全威脅的收件者摘要。範例：收件者的名稱、有關寄件者與規則/違規的摘要資訊、網路上的可疑安全威脅總數

表 B-22. 風險最高的可疑收件者摘要資料檢視

資料	說明
收件者	顯示受可疑安全威脅影響的收件者電子郵件信箱。
唯一策略/規則	顯示來源電腦違反的唯一策略/規則數目。 範例：受管理產品在 2 部電腦上偵測到相同策略的 10 個策略違規執行個體。 唯一策略/規則 = 1

資料	說明
唯一寄件者	顯示所傳送內容違反了受管理產品可疑安全威脅策略的唯一電子郵件訊息寄件者數目。 範例：受管理產品偵測到來自 3 部電腦的相同策略之 10 個可疑安全威脅違規執行個體。 唯一寄件者 = 3
偵測	顯示受管理產品偵測到的策略/規則違規總數。 範例：受管理產品在 1 部電腦上偵測到相同類型的 10 個違規執行個體。 偵測數 = 10

可疑寄件者摘要

提供從特定寄件者偵測到的可疑安全威脅摘要。範例：寄件者的名稱、有關收件者與規則/違規的摘要資訊、網路上的可疑安全威脅總數

表 B-23. 可疑寄件者摘要資料檢視

資料	說明
寄件者	顯示策略/規則違規來源的電子郵件信箱。
唯一策略/規則	顯示來源電腦違反的唯一策略/規則數目。 範例：受管理產品在 2 部電腦上偵測到相同策略的 10 個策略違規執行個體。 唯一策略/規則 = 1
唯一收件者	顯示所接收內容違反了受管理產品可疑安全威脅策略的唯一電子郵件訊息收件者數目。 範例：受管理產品在 2 部電腦上偵測到相同策略的 10 個可疑安全威脅違規執行個體。 唯一收件者 = 2

資料	說明
偵測	顯示受管理產品偵測到的策略/規則違規總數。 範例：受管理產品在 1 部電腦上偵測到相同類型的 10 個違規執行個體。 偵測數 = 10

可疑安全威脅通訊協定偵測摘要

提供針對特定通訊協定偵測到的可疑安全威脅摘要。範例：通訊協定的名稱、有關來源與目標的摘要資訊、網路上的可疑安全威脅總數

表 B-24. 可疑安全威脅通訊協定偵測摘要資料檢視

資料	說明
通訊協定	顯示發生可疑安全威脅的通訊協定名稱。範例：HTTP、FTP、SMTP
唯一策略/規則	顯示來源電腦違反的唯一策略/規則數目。 範例：受管理產品在 2 部電腦上偵測到相同策略的 10 個策略違規執行個體。 唯一策略/規則 = 1
唯一端點	顯示受可疑安全威脅影響的唯一電腦數目。 範例：受管理產品在 2 部電腦上偵測到相同類型的 10 個可疑安全威脅執行個體。 唯一端點 = 2
唯一來源	顯示可疑安全威脅起源所在的唯一來源數目。 範例：受管理產品從 3 部電腦上偵測到相同類型的 10 個可疑安全威脅執行個體。 唯一來源 = 3

資料	說明
唯一收件者	顯示所接收內容違反了受管理產品可疑安全威脅策略的唯一電子郵件訊息收件者數目。 範例：受管理產品在 2 部電腦上偵測到相同策略的 10 個可疑安全威脅違規執行個體。 唯一收件者 = 2
唯一寄件者	顯示所傳送內容違反了受管理產品可疑安全威脅策略的唯一電子郵件訊息寄件者數目。 範例：受管理產品偵測到來自 3 部電腦的相同策略之 10 個可疑安全威脅違規執行個體。 唯一寄件者 = 3
偵測	顯示受管理產品偵測到的策略/規則違規總數。 範例：受管理產品在 1 部電腦上偵測到相同類型的 10 個違規執行個體。 偵測數 = 10

歷來可疑安全威脅偵測摘要

提供一段時間（每日一次、每週一次、每月一次）內的可疑安全威脅偵測摘要。範例：摘要資料的收集時間和日期、有關來源與目標的摘要資訊、網路上的可疑安全威脅總數

表 B-25. 歷來可疑安全威脅偵測摘要資料檢視

資料	說明
日期/時間	顯示資料摘要發生的時間。
唯一策略/規則	顯示來源電腦違反的唯一策略/規則數目。 範例：受管理產品在 2 部電腦上偵測到相同策略的 10 個策略違規執行個體。 唯一策略/規則 = 1

資料	說明
唯一端點	顯示受可疑安全威脅影響的唯一電腦數目。 範例：受管理產品在 2 部電腦上偵測到相同類型的 10 個可疑安全威脅執行個體。 唯一端點 = 2
唯一來源	顯示可疑安全威脅起源所在的唯一來源數目。 範例：受管理產品從 3 部電腦上偵測到相同類型的 10 個可疑安全威脅執行個體。 唯一來源 = 3
唯一收件者	顯示所接收內容違反了受管理產品可疑安全威脅策略的唯一電子郵件訊息收件者數目。 範例：受管理產品在 2 部電腦上偵測到相同策略的 10 個可疑安全威脅違規執行個體。 唯一收件者 = 2
唯一寄件者	顯示所傳送內容違反了受管理產品可疑安全威脅策略的唯一電子郵件訊息寄件者數目。 範例：受管理產品偵測到來自 3 部電腦的相同策略之 10 個可疑安全威脅違規執行個體。 唯一寄件者 = 3
偵測	顯示受管理產品偵測到的策略/規則違規總數。 範例：受管理產品在 1 部電腦上偵測到相同類型的 10 個違規執行個體。 偵測數 = 10

灰色軟體偵測資訊

提供在您網路上偵測到的可能攻擊指標的詳細資訊

表 B-26. 灰色軟體偵測資訊資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
端點	端點的名稱
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
管理伺服器實體	端點向其回報之 Apex Central 中受管理產品伺服器的顯示名稱
偵測類型	灰色軟體偵測的類型
規則	觸發偵測的策略或規則
詳細資訊	JSON 物件，其中包含有關偵測的其他資訊
策略	已偵測到 MITRE ATT&CK™ 策略 如需詳細資訊，請參閱 https://attack.mitre.org/tactics/enterprise/。
技術	已偵測到 MITRE ATT&CK™ 技術 如需詳細資訊，請參閱 https://attack.mitre.org/techniques/enterprise/。

整體安全威脅資訊

顯示有關網路整體安全威脅局勢的摘要和統計資料。

網路防護分界資訊

顯示會影響整個網路的安全威脅全面總覽資訊。範例：受管理產品的網路防護類型（閘道、電子郵件）、安全威脅類型、受影響的端點數目

表 B-27. 網路防護分界資訊資料檢視

資料	說明
產品類別	顯示受管理產品所屬的類別。 範例：桌面產品、郵件伺服器產品、網路產品
產品	顯示受管理產品的名稱。 範例：Apex One、ScanMail for Microsoft Exchange
安全威脅類別	顯示受管理產品偵測到的安全威脅廣泛類別。 範例：防毒、間諜程式防護、網路釣魚防護
唯一端點	顯示受安全威脅/違規影響的唯一電腦數目。 範例：Apex One 在 2 部電腦上偵測到相同病毒的 10 個病毒執行個體。 唯一端點 = 2
唯一來源	顯示安全威脅/違規起源所在的唯一電腦數目。 範例：Apex One 在 2 部電腦上偵測到來自 3 個來源之相同病毒的 10 個病毒執行個體。 唯一來源 = 3
偵測	顯示受管理產品偵測到的安全威脅/違規總數。 範例：Apex One 在 1 部電腦上偵測到相同病毒的 10 個病毒執行個體。 偵測數 = 10

網路安全威脅分析資訊

顯示影響桌上型電腦的整體安全威脅資訊。範例：安全威脅數目、安全威脅偵測總數、受影響端點數目

表 B-28. 網路安全威脅分析資訊資料檢視

資料	說明
安全威脅類別	顯示受管理產品偵測到的安全威脅廣泛類別。 範例：防毒、間諜程式防護、網路釣魚防護
安全威脅	顯示受管理產品偵測到的安全威脅的名稱。
項目類型	顯示受管理產品偵測到的安全威脅的進入點。 範例：在檔案、HTTP、Windows Live Messenger (MSN) 中發現病毒
唯一端點	顯示受安全威脅/違規影響的唯一電腦數目。 範例：Apex One 在 2 部電腦上偵測到相同病毒的 10 個病毒執行個體。 唯一端點 = 2
唯一來源	顯示安全威脅/違規起源所在的唯一電腦數目。 範例：Apex One 在 2 部電腦上偵測到來自 3 個來源之相同病毒的 10 個病毒執行個體。 唯一來源 = 3
偵測	顯示受管理產品偵測到的安全威脅/違規總數。 範例：Apex One 在 1 部電腦上偵測到相同病毒的 10 個病毒執行個體。 偵測數 = 10

安全威脅端點分析資訊

顯示以受影響端點為焦點的資訊。範例：端點的名稱、安全威脅進入網路的各種方式、受影響的端點數目

表 B-29. 安全威脅端點分析資訊資料檢視

資料	說明
端點	顯示受安全威脅/違規影響的電腦名稱。

資料	說明
安全威脅類別	顯示受管理產品偵測到的安全威脅廣泛類別。 範例：防毒、間諜程式防護、網路釣魚防護
安全威脅名稱	顯示受管理產品偵測到的安全威脅的名稱。
偵測	顯示受管理產品偵測到的安全威脅/違規總數。 範例：Apex One 在 1 部電腦上偵測到相同病毒的 10 個病毒執行個體。 偵測數 = 10
已偵測	顯示上次在受安全威脅/違規影響的電腦上偵測到安全威脅/違規的時間和日期。

安全威脅項目分析資訊

顯示以安全威脅進入點為焦點的資訊。範例：受管理產品的網路安全防護類型（閘道、電子郵件、桌面）、安全威脅的名稱、上次安全威脅偵測的時間

表 B-30. 安全威脅項目分析資訊資料檢視

資料	說明
項目類型	顯示受管理產品偵測到的安全威脅進入點。 範例：在檔案中發現病毒、FTP、檔案傳輸
產品	顯示偵測到安全威脅的受管理產品名稱。 範例：Apex One、ScanMail for Microsoft Exchange
安全威脅類別	顯示受管理產品偵測到的安全威脅具體類別。 範例：防毒、間諜程式防護、內容過濾
唯一端點	顯示受安全威脅/違規影響的唯一電腦數目。 範例：Apex One 在 2 部電腦上偵測到相同病毒的 10 個病毒執行個體。 唯一端點 = 2

資料	說明
唯一來源	顯示安全威脅/違規起源所在的唯一電腦數目。 範例：Apex One 在 2 部電腦上偵測到來自 3 個來源之相同病毒的 10 個病毒執行個體。 唯一來源 = 3
偵測	顯示受管理產品偵測到的安全威脅/違規總數。 範例：Apex One 在 1 部電腦上偵測到相同病毒的 10 個病毒執行個體。 偵測數 = 10

安全威脅來源分析資訊

顯示以安全威脅來源為焦點的資訊。範例：安全威脅來源的名稱、安全威脅進入網路的各種方式、受影響的端點數目

表 B-31. 安全威脅來源分析資訊資料檢視

資料	說明
來源主機	顯示導致安全威脅/違規產生的電腦名稱。
安全威脅類別	顯示受管理產品偵測到的安全威脅廣泛類別。 範例：防毒、間諜程式防護、網路釣魚防護
安全威脅	顯示受管理產品偵測到的安全威脅的名稱。
偵測	顯示受管理產品偵測到的安全威脅/違規總數。 範例：Apex One 在 1 部電腦上偵測到相同病毒的 10 個病毒執行個體。 偵測數 = 10
已偵測	顯示上次在受安全威脅/違規影響的電腦上偵測到安全威脅/違規的時間和日期。

策略/規則違規資訊

顯示有關受管理產品在網路上偵測到之策略/規則違規的摘要和詳細資料。

裝置存取控制資訊

提供有關您網路上與裝置存取控制相關事件的特定資訊。

表 B-32. 裝置存取控制資訊資料檢視

資料	說明
收到	顯示 Apex Central 從受管理產品收到資料的時間
已產生	顯示受管理產品產生資料的時間
產品實體/端點	此資料欄顯示下列其中一項： • 受管理產品的實體顯示名稱。Apex Central 使用受管理產品的實體顯示名稱識別受管理產品。 • 已安裝用戶端（例如 Apex One 用戶端）之電腦的 IP 位址或主機名稱
產品	顯示受管理產品的名稱 範例：Apex One
目標程序	顯示違規將其做為目標的程序
檔案名稱	顯示檔案的名稱
裝置類型	顯示所存取的裝置類型
權限	顯示權限類型
使用者	顯示受管理產品偵測到事件時登入到端點的使用者名稱

詳細應用程式活動

顯示有關違反網路安全策略的應用程式活動的特定資訊

表 B-33. 詳細應用程式活動資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
產品項目	Apex Central 中受管理產品伺服器的顯示名稱
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
VLAN ID	可疑安全威脅起源所在的來源 VLAN ID (VID)
偵測者	偵測到可疑安全威脅的過濾器、掃瞄引擎或受管理產品
流量/連線	網路流量的方向，或網路上可疑安全威脅起源所在的位置
通訊協定群組	受管理產品從其偵測到可疑安全威脅的廣泛通訊協定群組 範例：FTP、HTTP、P2P
通訊協定	受管理產品從其偵測到可疑安全威脅的通訊協定 範例：ARP、Bearshare、BitTorrent
說明	趨勢科技針對事件提供的詳細說明
端點主機	符合策略/規則之電腦的主機名稱
來源 IP	可疑安全威脅起源所在的來源 IP 位址
來源 MAC	可疑安全威脅起源所在的來源 MAC 位址
來源通訊埠	可疑安全威脅起源所在的來源通訊埠號碼
來源 IP 群組	違規起源所在的來源 IP 位址群組
來源網路區域	違規起源所在的來源網路區域
端點 IP	受可疑安全威脅影響之端點的 IP 位址
端點通訊埠	受可疑安全威脅影響之端點的通訊埠號碼
端點 MAC	受可疑安全威脅影響之端點的 MAC 位址

資料	說明
端點群組	受可疑安全威脅影響之端點的 IP 位址群組
端點網路區域	受可疑安全威脅影響之端點的網路區域
偵測	偵測總數 範例：Apex One 在 1 部電腦上偵測到相同病毒的 10 個病毒執行個體。 偵測數 = 10
安全威脅類型	受管理產品偵測到的安全威脅的特定類型
偵測嚴重性	事件的嚴重性層級
IP 位址 (關注的)	目標端點（來源或目標）的 IP 位址 如果資料交換是在網路內部進行的，則關注的 IP 是來源 IP 位址。如果流量是外部流量，則關注的 IP 是目標 IP 位址。
IP 位址 (對等)	與關注的 IP 相對的 IP 位址 例如，如果關注的 IP 是來源 IP 位址，則對等 IP 就是目標 IP 位址。
相符的已歸類事件	符合同一彙整規則的記錄檔計數
彙整的相符已歸類事件	符合同一規則的已彙整記錄檔計數
網路群組	群組的名稱
主機嚴重性	主機嚴重性
記錄 ID	記錄 ID

Application Control 違規詳細資訊

提供有關您網路中發生之 Application Control 違規的特定資訊（例如，違反的 Security Agent 策略和條件）

表 B-34. Application Control 違規詳細資訊資料檢視

資料	說明
已產生	受管理產品產生資料的日期和時間
收到	Apex Central 從受管理產品接收資料的日期和時間
使用者名稱	事件發生當時已登入的使用者名稱
端點	端點的名稱
處理行動	受管理產品採取的處理行動
檔案	執行程序的檔案物件或程式的名稱
處理程序	檔案物件執行的程序
策略	Apex Central 或受管理產品主控台套用的策略名稱
條件	應用程式使用率的規則名稱
比對方法	允許條件或封鎖條件中用於識別應用程式的方法
版本	認證安全防護軟體病毒碼版本
雜湊類型	使用的雜湊演算法類型
雜湊值	檔案物件的雜湊值
憑證簽署單位	憑證的核發者
伺服器	端點向其回報之 Apex Central 中受管理產品伺服器的顯示名稱
連線狀態	端點與受管理產品伺服器之間連線的狀態
端點 IP 位址	端點的 IP 位址
指令	發出的指令
程序擁有者	發出指令之帳號的使用者名稱
應用程式	檔案物件所屬的應用程式名稱
相符的檔案路徑	檔案物件的目錄位置
偵測	偵測總數

資料	說明
檔案上次修改時間	檔案物件上次修改的日期和時間

行為監控詳細資訊

提供有關網路上與行為監控相關之事件的特定資訊。

表 B-35. 行為監控詳細資訊資料檢視

資料	說明
從實體收到的時間	顯示 Apex Central 從受管理產品收到資料的時間
在實體產生的時間	顯示受管理產品產生資料的時間
主機	顯示所存取電腦的 IP 位址或主機名稱
風險等級	顯示趨勢科技對您網路的風險評估
記錄類型	顯示觸發違規的記錄類型
策略	顯示違規所觸發的策略名稱
主旨	顯示特定檔案（包括其目錄）
事件類型	顯示違規類型
目標	顯示事件類型指定的路徑或目錄
處理行動	顯示受管理產品採取的處理行動
作業	顯示讀取/寫入或執行作業
端點	顯示遭到攻擊之電腦的主機名稱
端點 IP	顯示遭到攻擊之電腦的 IP 位址
端點感染通道	顯示安全威脅源自的通道
雲端服務供應商	顯示雲端服務供應商的名稱

端點安全性符合詳細資訊

提供有關網路上端點安全性符合的特定資訊

表 B-36. 端點安全性符合詳細資訊資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
產品項目	Apex Central 中受管理產品伺服器的顯示名稱
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
端點	符合策略/規則之電腦的主機名稱
端點 IP	符合策略/規則之電腦的 IP 位址
端點 MAC	符合策略/規則之電腦的 MAC 位址
策略/規則名稱	合規的策略/規則名稱
服務	符合策略/規則的服務/程式名稱
使用者	事件發生當時已登入的使用者名稱
說明	趨勢科技針對事件提供的詳細說明
偵測	偵測總數 範例：Apex One 在 1 部電腦上偵測到相同病毒的 10 個病毒執行個體。 偵測數 = 10

端點安全違規詳細資訊

提供有關網路上端點安全違規的特定資訊

表 B-37. 端點安全違規詳細資訊資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
產品項目	Apex Central 中受管理產品伺服器的顯示名稱
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
端點	端點的名稱
端點 IP	端點的 IP 位址
端點 MAC	端點的 MAC 位址
策略/規則名稱	觸發偵測的策略/規則名稱
服務	觸發偵測的服務/程式名稱
使用者	事件發生當時已登入的使用者名稱
強制性處理行動	策略/規則強制執行的處理行動
矯正性處理行動	可協助停止違規所引發之酬載的處理行動
說明	趨勢科技針對事件提供的詳細說明
偵測	偵測總數 範例：Apex One 在 1 部電腦上偵測到 10 個同一類型的安全違規。 偵測數 = 10

防火牆違規事件詳細資訊

提供有關您網路中防火牆違規的特定資訊（例如，偵測到違規的受管理產品、傳輸來源和傳輸目標，以及防火牆違規的總數）

表 B-38. 防火牆違規詳細資訊資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
產品項目/端點	根據相關的來源： • Apex Central 中受管理產品伺服器的顯示名稱 • 端點的名稱或 IP 位址
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
事件類型	觸發偵測的事件類型 範例：入侵、策略違規
風險等級	趨勢科技對您網路的風險評估 範例：高安全性、低安全性、中等安全性
流量/連線	傳輸的方向
通訊協定	入侵使用的通訊協定 範例：HTTP、SMTP、FTP
來源通訊埠	偵測到的安全威脅的來源 IP 位址通訊埠號碼
來源 IP	偵測到的安全威脅的來源 IP 位址
目標通訊埠	偵測到的安全威脅所存取的通訊埠號碼
目標 IP	偵測到的安全威脅所存取的端點 IP 位址
目標程序	違規將其做為目標的程序
說明	趨勢科技針對事件提供的詳細說明
處理行動	受管理產品採取的處理行動 範例：檔案已清除、檔案已隔離、檔案暫不處理

資料	說明
偵測	偵測總數 範例：受管理產品在 1 部電腦上偵測到相同類型的 10 個違規執行個體 偵測數 = 10

入侵防護詳細資訊

提供特定資訊來協助您及時防範已知和零時差攻擊、防禦 Web 應用程式弱點，以及找出存取網路的惡意軟體

資料	說明
已產生	受管理產品產生資料的日期和時間
收到	Apex Central 從受管理產品接收資料的日期和時間
伺服器	受管理產品伺服器的顯示名稱
產品項目/端點	端點的名稱或 IP 位址
受影響的 IP 位址	受安全威脅影響之端點的 IP 位址
原因/規則	事件觸發的入侵防護規則
模式	入侵防護模組所使用的網路引擎偵測模式
處理行動	受管理產品採取的處理行動
應用程式類型	與事件所觸發之入侵防護規則關聯的「應用程式類型」
攻擊來源	偵測到的安全威脅的來源
來源 IP 位址	偵測到的安全威脅的來源 IP 位址
來源 MAC 位址	偵測到的安全威脅的來源 MAC 位址
來源通訊埠	偵測到的安全威脅的來源通訊埠
目標 IP 位址	安全威脅存取的 IP 位址

資料	說明
目標 MAC 位址	安全威脅存取的 MAC 位址
目標通訊埠	安全威脅存取的通訊埠號碼
MAC 位址（關注的）	根據網路流量的方向： • 輸入網路流量的「來源 MAC 位址」 • 輸出網路流量的「目標 MAC 位址」
通訊協定	安全威脅進入網路所用的通訊協定
方向	傳輸的方向
優先順序	偵測的重要性（根據單機版 Vulnerability Protection 所採用的排名系統）
嚴重性	事件的嚴重性等級

完整性監控資訊

用來監控端點上發生的特定變更，例如已安裝的軟體、執行中的服務、程序、檔案、目錄、監聽通訊埠、登錄機碼和登錄值

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
伺服器	受管理產品伺服器的主機名稱
變更	完整性規則偵測到的變更
使用者	事件發生當時已登入的使用者名稱
處理程序	事件起源所在的程序
類型	登錄機碼的類型
機碼	登錄機碼

資料	說明
排名	完整性排名
嚴重性	事件的嚴重性等級

網路內容檢測資訊

提供有關網路上網路內容違規的特定資訊

表 B-39. 網路內容檢測資訊資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
產品/端點 IP	根據相關的來源： • Apex Central 中受管理產品伺服器的顯示名稱 • 端點的名稱或 IP 位址
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
傳輸方向	傳輸的方向
本機 IP 位址	Security Agent 端點的 IP 位址
本機 IP 位址通訊埠	Security Agent 端點的 IP 位址通訊埠號碼
遠端 IP 位址	外部端點的 IP 位址
遠端 IP 位址通訊埠	外部端點的 IP 位址通訊埠號碼
遠端網域	與偵測關聯的網域名稱
處理程序	嘗試聯絡時所使用的程序 (路徑\應用程式名稱)
處理行動	受管理產品採取的處理行動
特徵碼類型	與偵測關聯的特徵碼類型

資料	說明
安全威脅名稱	安全威脅的名稱

垃圾郵件違規資訊

顯示有關受管理產品在網路上偵測到垃圾郵件的摘要和詳細資料。

垃圾郵件詳細資訊

提供有關您網路中垃圾郵件違規的特定資訊（例如，偵測到內容違規的受管理產品、違反的特定策略名稱，以及網路中垃圾郵件違規的總數）

表 B-40. 垃圾郵件詳細資訊資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
產品項目	Apex Central 中受管理產品伺服器的顯示名稱
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
收件者	觸發偵測的電子郵件收件者
寄件者	觸發偵測的電子郵件寄件者
主旨	觸發偵測的電子郵件主旨
策略	觸發偵測的策略
處理行動	受管理產品採取的處理行動

資料	說明
偵測	偵測總數 範例：受管理產品在 1 個端點上偵測到相同垃圾郵件的 10 個違規執行個體。 偵測數 = 10

垃圾郵件違規整體摘要

提供網路上垃圾郵件違規的摘要

資料	說明
收件者網域	受垃圾郵件影響的收件者網域
唯一收件者	顯示從指定網域收到垃圾郵件的唯一收件者數目。 範例：受管理產品在 3 部電腦上偵測到來自相同網域之垃圾郵件的 10 個違規執行個體。 唯一收件者 = 3
偵測	顯示受管理產品偵測到的垃圾郵件違規總數。 範例：受管理產品在 1 部電腦上偵測到相同垃圾郵件的 10 個違規執行個體。 偵測數 = 10

垃圾郵件連線資訊

提供有關您網路中垃圾郵件來源的特定資訊（例如，偵測到垃圾郵件的受管理產品、受管理產品採取的特定處理行動，以及偵測到的垃圾郵件總數）

表 B-41. 垃圾郵件連線資訊資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間

資料	說明
已產生	受管理產品產生資料的日期和時間
產品項目	Apex Central 中受管理產品伺服器的顯示名稱
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
來源 IP	偵測到的安全威脅的來源 IP 位址
過濾器類型	偵測到事件的過濾器類型
處理行動	受管理產品採取的處理行動 範例：中斷連線、略過連線
偵測	偵測總數 範例：Apex One 在 1 部電腦上偵測到相同垃圾郵件的 10 個違規執行個體。 偵測數 = 10

歷來垃圾郵件偵測摘要

提供一段時間（每日一次、每週一次、每月一次）內的垃圾郵件偵測摘要。範例：收集摘要資料的時間和日期、受垃圾郵件影響的端點數目、網路上垃圾郵件違規總數

表 B-42. 歷來垃圾郵件偵測摘要資料檢視

資料	說明
摘要時間	顯示資料摘要發生的時間。
唯一收件者網域	顯示受垃圾郵件影響的唯一收件者網域總數。 範例：受管理產品從 1 個收件者網域的 2 個網域中偵測到相同垃圾郵件的 10 個違規執行個體。 唯一收件者網域 = 1

資料	說明
唯一收件者	顯示從指定網域收到垃圾郵件的唯一收件者數目。 範例：受管理產品在 3 部電腦上偵測到來自相同網域之垃圾郵件的 10 個違規執行個體。 唯一收件者 = 3
偵測	顯示受管理產品偵測到的垃圾郵件違規總數。 範例：受管理產品在 1 部電腦上偵測到相同垃圾郵件的 10 個違規執行個體。 偵測數 = 10

垃圾郵件收件者摘要

提供特定端點上的垃圾郵件違規摘要。範例：端點的名稱、端點上病毒/惡意程式執行個體總數

表 B-43. 垃圾郵件收件者摘要資料檢視

資料	說明
收件者	顯示收到垃圾郵件的收件者名稱。
偵測	顯示受管理產品偵測到的垃圾郵件違規總數。 範例：受管理產品在 1 部電腦上偵測到相同垃圾郵件的 10 個違規執行個體。 偵測數 = 10

間諜程式/可能的資安威脅程式資訊

顯示有關受管理產品在網路上偵測到間諜程式/可能的資安威脅程式的摘要和詳細資料。

間諜程式/可能的資安威脅程式詳細資訊

提供有關網路上間諜程式/可能的資安威脅程式偵測的特定資訊，例如偵測到間諜程式/可能的資安威脅程式的受管理產品、間諜程式/可能的資安威脅程式的名稱，以及中毒端點的名稱

表 B-44. 間諜程式/可能的資安威脅程式詳細資訊資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
產品項目/端點	根據相關的來源： • Apex Central 中受管理產品伺服器的顯示名稱 • 端點的名稱或 IP 位址
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
產品/端點 IP	根據相關的來源： • 受管理產品伺服器的 IP 位址 • 端點的 IP 位址
產品/端點 MAC	根據相關的來源： • 受管理產品伺服器的 MAC 位址 • Security Agent 端點的 MAC 位址
管理伺服器實體	端點向其回報之 Apex Central 中受管理產品伺服器的顯示名稱
間諜程式/可能的資安威脅程式	安全威脅的名稱
端點	端點的名稱或 IP 位址
來源主機	安全威脅起源所在的端點 IP 位址或名稱
使用者	事件發生當時已登入的使用者名稱

資料	說明
結果	受管理產品採取的處理行動結果 範例：成功、需要進一步的處理行動
處理行動	受管理產品採取的處理行動 範例：檔案已清除、檔案已隔離、檔案已刪除
偵測	偵測總數 範例：Apex One 在 1 部電腦上偵測到相同的間諜程式/可能的資安威脅程式的 10 個間諜程式/可能的資安威脅程式執行個體。 偵測數 = 10
項目類型	安全威脅的進入點
詳細資訊	顯示特定偵測的其他相關資訊的連結
端點感染通道	安全威脅源自的通道
Apex One 網域階層	Security Agent 所屬的用戶端樹狀結構網域或子網域
網域	端點向其回報之受管理產品伺服器的網域
作業系統	端點上的作業系統
雲端服務供應商	雲端服務供應商的名稱

端點間諜程式/可能的資安威脅程式

提供有關其中偵測到間諜程式/可能的資安威脅程式之端點的特定資訊（例如，偵測到間諜程式/可能的資安威脅程式的受管理產品、偵測到間諜程式/可能的資安威脅程式的掃瞄類型，以及端點上偵測到間諜程式/可能的資安威脅程式的檔案路徑）

表 B-45. 端點間諜程式/可能的資安威脅程式資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間

資料	說明
已產生	受管理產品產生資料的日期和時間
產品項目/端點	根據相關的來源： • Apex Central 中受管理產品伺服器的顯示名稱 • Security Agent 端點的名稱或 IP 位址
產品/端點 IP	根據相關的來源： • 受管理產品伺服器的 IP 位址 • 端點的 IP 位址
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
管理伺服器實體	端點向其回報之 Apex Central 中受管理產品伺服器的顯示名稱
間諜程式/可能的資安威脅程式	安全威脅的名稱
端點	安全威脅存取的端點 IP 位址或名稱
來源主機	安全威脅起源所在的端點 IP 位址或名稱
使用者	事件發生當時已登入的使用者名稱
掃瞄類型	報告事件的掃瞄類型（例如，即時掃瞄、預約掃瞄、手動掃瞄）
資源	受安全威脅影響的特定資源 範例：`application.exe`、`H Key Local Machine\SOFTWARE\ACME`
資源類型	受安全威脅影響的資源類型 範例：登錄、記憶體資源
安全威脅類型	安全威脅的類型 範例：廣告軟體、COOKIE、對等式應用程式
風險等級	安全威脅的風險等級 範例：高安全性、中等安全性、低安全性

資料	說明
結果	受管理產品採取的處理行動結果 範例：成功、需要進一步的處理行動
處理行動	受管理產品採取的處理行動 範例：檔案已清除、檔案已隔離、檔案已刪除
偵測	偵測總數
雲端服務供應商	雲端服務供應商的名稱

端點間諜程式/可能的資安威脅程式摘要

提供特定端點的間諜程式/可能的資安威脅程式偵測摘要。範例：端點名稱、端點上的特定間諜程式/可能的資安威脅程式執行個體數目、網路上的間諜程式/可能的資安威脅程式執行個體總數

表 B-46. 端點間諜程式/可能的資安威脅程式摘要資料檢視

資料	說明
端點	顯示受間諜程式/可能的資安威脅程式影響的電腦主機名稱或 IP 位址。
唯一來源	顯示間諜程式/可能的資安威脅程式起源所在的唯一來源數目。 範例：Apex One 偵測到源自 2 個感染來源的相同間諜程式/可能的資安威脅程式之 10 個間諜程式/可能的資安威脅程式執行個體。 唯一來源 = 2
唯一偵測	顯示受管理產品偵測到的唯一間諜程式/可能的資安威脅程式數目。 範例：Apex One 在 1 部電腦上偵測到相同的間諜程式/可能的資安威脅程式的 10 個間諜程式/可能的資安威脅程式執行個體。 唯一偵測 = 1

資料	說明
偵測	顯示受管理產品偵測到的間諜程式/可能的資安威脅程式總數。 範例：Apex One 在 1 部電腦上偵測到相同的間諜程式/可能的資安威脅程式的 10 個間諜程式/可能的資安威脅程式執行個體。 偵測數 = 10

電子郵件間諜程式/可能的資安威脅程式

提供有關其中偵測到間諜程式/可能的資安威脅程式之電子郵件的特定資訊（例如，偵測到間諜程式/可能的資安威脅程式的受管理產品、電子郵件的主旨行內容，以及內含間諜程式/可能的資安威脅程式之電子郵件的寄件者）

表 B-47. 電子郵件間諜程式/可能的資安威脅程式資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
產品項目	Apex Central 中受管理產品伺服器的顯示名稱
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
間諜程式/可能的資安威脅程式	安全威脅的名稱
收件者	觸發偵測的電子郵件收件者
寄件者	觸發偵測的電子郵件寄件者
使用者	事件發生當時已登入的使用者名稱
主旨	觸發偵測的電子郵件主旨
檔案	安全威脅存取的檔案物件名稱
壓縮檔中的檔案	壓縮封存檔中受影響的檔案物件名稱

資料	說明
結果	受管理產品採取的處理行動結果 範例：成功、需要進一步的處理行動
處理行動	受管理產品採取的處理行動 範例：檔案已清除、檔案已隔離、檔案已刪除
偵測	偵測總數 範例：Apex One 在 1 部電腦上偵測到相同的間諜程式/可能的資安威脅程式的 10 個間諜程式/可能的資安威脅程式執行個體。 偵測數 = 10
雲端服務供應商	雲端服務供應商的名稱

網路間諜程式/可能的資安威脅程式

提供有關網路流量中發現的間諜程式/可能的資安威脅程式執行個體的特定資訊（例如，偵測到間諜程式/可能的資安威脅程式的受管理產品、間諜程式/可能的資安威脅程式進入您網路所用的通訊協定，以及有關間諜程式/可能的資安威脅程式的來源與目標特定資訊）

表 B-48. 網路間諜程式/可能的資安威脅程式資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
產品實體/端點	根據相關的來源： • Apex Central 中受管理產品伺服器的顯示名稱 • Security Agent 端點的名稱或 IP 位址
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange

資料	說明
間諜程式/可能的資安威脅程式	安全威脅的名稱
流量/連線	傳輸的方向
通訊協定	安全威脅進入網路所用的通訊協定 範例：HTTP、SMTP、FTP
端點 IP	安全威脅存取的 IP 位址
端點	安全威脅存取的端點 IP 位址或名稱
端點通訊埠	安全威脅存取的 IP 通訊埠號碼
端點 MAC	安全威脅存取的 MAC 位址
來源 IP	偵測到的安全威脅的來源 IP 位址
來源主機	安全威脅起源所在的端點 IP 位址或名稱
來源通訊埠	偵測到的安全威脅的來源 IP 位址通訊埠號碼
來源 MAC	偵測到的安全威脅的來源 MAC 位址
使用者	事件發生當時已登入的使用者名稱
檔案	安全威脅存取的檔案物件名稱
結果	受管理產品採取的處理行動結果 範例：成功、需要進一步的處理行動
處理行動	受管理產品採取的處理行動 範例：檔案已清除、檔案已隔離、檔案已刪除
偵測	偵測總數 範例：Apex One 在 1 部電腦上偵測到相同的間諜程式/可能的資安威脅程式的 10 個間諜程式/可能的資安威脅程式執行個體。 偵測數 = 10
雲端服務供應商	雲端服務供應商的名稱

間諜程式/可能的資安威脅程式整體摘要

提供有關間諜程式/可能的資安威脅程式偵測的整體特定摘要。範例：間諜程式/可能的資安威脅程式的名稱、受間諜程式/可能的資安威脅程式影響的端點數目、網路上間諜程式/可能的資安威脅程式執行個體總數

表 B-49. 間諜程式/可能的資安威脅程式整體摘要資料檢視

資料	說明
間諜程式/可能的資安威脅程式	顯示受管理產品偵測到的間諜程式/可能的資安威脅程式名稱。
唯一端點	顯示受間諜程式/可能的資安威脅程式影響的唯一電腦數目。 Apex One 在 3 部不同的電腦上偵測到相同的間諜程式/可能的資安威脅程式的 10 個間諜程式/可能的資安威脅程式執行個體。 唯一端點 = 3
唯一來源	顯示間諜程式/可能的資安威脅程式起源所在的唯一來源數目。 範例：Apex One 偵測到源自 2 個感染來源的相同間諜程式/可能的資安威脅程式之 10 個間諜程式/可能的資安威脅程式執行個體。 唯一來源 = 2
偵測	顯示受管理產品偵測到的間諜程式/可能的資安威脅程式總數。

間諜程式/可能的資安威脅程式處理行動/結果摘要

顯示受管理產品對間諜程式/可能的資安威脅程式採取的處理行動摘要。範例：對間諜程式/可能的資安威脅程式採取的特定處理行動、採取的處理行動結果、網路上的間諜程式/可能的資安威脅程式執行個體總數

表 B-50. 間諜程式/可能的資安威脅程式處理行動/結果摘要資料檢視

資料	說明
結果	顯示受管理產品對間諜程式/可能的資安威脅程式採取的處理行動結果。 範例：成功、需要進一步的處理行動

資料	說明
處理行動	顯示受管理產品對間諜程式/可能的資安威脅程式採取的處理行動類型。 範例：檔案已清除、檔案已隔離、檔案已刪除
唯一端點	顯示受間諜程式/可能的資安威脅程式影響的唯一電腦數目。 範例：Apex One 在 3 部不同的電腦上偵測到相同的間諜程式/可能的資安威脅程式的 10 個諜程式/可能的資安威脅程式執行個體。 唯一端點 = 3
唯一來源	顯示間諜程式/可能的資安威脅程式起源所在的唯一來源數目。 範例：Apex One 偵測到源自 2 個感染來源的相同間諜程式/可能的資安威脅程式之 10 個間諜程式/可能的資安威脅程式執行個體。 唯一來源 = 2
偵測	顯示受管理產品偵測到的間諜程式/可能的資安威脅程式總數。 範例：Apex One 在 1 部電腦上偵測到相同的間諜程式/可能的資安威脅程式的 10 個間諜程式/可能的資安威脅程式執行個體。 偵測數 = 10

歷來間諜程式/可能的資安威脅程式偵測摘要

提供一段時間（每日一次、每週一次、每月一次）內的間諜程式/可能的資安威脅程式偵測摘要。範例：收集摘要資料的時間和日期、受間諜程式/可能的資安威脅程式影響的端點數目、網路上的間諜程式/可能的資安威脅程式執行個體總數

表 B-51. 歷來間諜程式/可能的資安威脅程式偵測摘要資料檢視

資料	說明
日期/時間	顯示資料摘要發生的時間。

資料	說明
唯一偵測	顯示受管理產品偵測到的唯一間諜程式/可能的資安威脅程式數目。 範例：Apex One 在 1 部電腦上偵測到相同的間諜程式/可能的資安威脅程式的 10 個間諜程式/可能的資安威脅程式執行個體。 唯一偵測 = 1
唯一端點	顯示受間諜程式/可能的資安威脅程式影響的唯一電腦數目。 範例：Apex One 在 3 部不同的電腦上偵測到相同的間諜程式/可能的資安威脅程式的 10 個諜程式/可能的資安威脅程式執行個體。 唯一端點 = 3
唯一來源	顯示間諜程式/可能的資安威脅程式起源所在的唯一來源數目。 範例：Apex One 偵測到源自 2 個感染來源的相同間諜程式/可能的資安威脅程式之 10 個間諜程式/可能的資安威脅程式執行個體。 唯一來源 = 2
偵測	顯示受管理產品偵測到的間諜程式/可能的資安威脅程式總數。 範例：Apex One 在 1 部電腦上偵測到相同的間諜程式/可能的資安威脅程式的 10 個間諜程式/可能的資安威脅程式執行個體。 偵測數 = 10

間諜程式/可能的資安威脅程式來源摘要

提供病毒爆發來源的間諜程式/可能的資安威脅程式偵測摘要。範例：來源電腦名稱、來自來源電腦的特定間諜程式/可能的資安威脅程式執行個體數目、網路上的特定間諜程式/可能的資安威脅程式執行個體總數

表 B-52. 間諜程式/可能的資安威脅程式來源摘要資料檢視

資料	說明
來源主機	顯示間諜程式/可能的資安威脅程式起源所在的電腦名稱。

資料	說明
唯一端點	顯示受間諜程式/可能的資安威脅程式影響的唯一電腦數目。 範例：Apex One 在 3 部不同的電腦上偵測到相同的間諜程式/可能的資安威脅程式的 10 個諜程式/可能的資安威脅程式執行個體。 唯一端點 = 3
唯一偵測	顯示受管理產品偵測到的唯一間諜程式/可能的資安威脅程式數目。 範例：Apex One 在 1 部電腦上偵測到相同的間諜程式/可能的資安威脅程式的 10 個間諜程式/可能的資安威脅程式執行個體。 唯一偵測 = 1
偵測	顯示受管理產品偵測到的間諜程式/可能的資安威脅程式總數。 範例：Apex One 在 1 部電腦上偵測到相同的間諜程式/可能的資安威脅程式的 10 個間諜程式/可能的資安威脅程式執行個體。 偵測數 = 10

Web 間諜程式/可能的資安威脅程式

提供有關 HTTP 或 FTP 流量中發現的間諜程式/可能的資安威脅程式執行個體的特定資訊（例如，偵測到間諜程式/可能的資安威脅程式的受管理產品、間諜程式/可能的資安威脅程式發生所在位置的傳輸方向，以及下載間諜程式/可能的資安威脅程式的 Web 瀏覽器或 FTP 用戶端）

表 B-53. Web 間諜程式/可能的資安威脅程式資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
產品實體/端點	根據相關的來源： • Apex Central 中受管理產品伺服器的顯示名稱 • Security Agent 端點的名稱或 IP 位址

資料	說明
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
間諜程式/可能的資安威脅程式	安全威脅的名稱
IP	端點的 IP 位址
來源 URL	安全威脅起源所在的 Web/FTP 站台的 URL
流量/連線	傳輸的方向
瀏覽器/FTP 用戶端	安全威脅存取的 Web 瀏覽器或 FTP 用戶端
使用者	事件發生當時已登入的使用者名稱
結果	受管理產品採取的處理行動結果 範例：成功、需要進一步的處理行動
處理行動	受管理產品採取的處理行動 範例：檔案已清除、檔案已隔離、檔案已刪除
偵測	偵測總數 範例：Apex One 在 1 部電腦上偵測到相同的間諜程式/可能的資安威脅程式的 10 個間諜程式/可能的資安威脅程式執行個體。 偵測數 = 10
雲端服務供應商	雲端服務供應商的名稱

病毒/惡意程式資訊

顯示有關受管理產品在網路上偵測到的病毒/惡意程式的摘要和詳細資料。

病毒/惡意程式詳細資訊

提供有關網路上病毒/惡意程式偵測的特定資訊，例如偵測到病毒/惡意程式的受管理產品、病毒/惡意程式的名稱，以及中毒端點的名稱

表 B-54. 病毒/惡意程式詳細資訊資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
產品項目/端點	根據相關的來源： • Apex Central 中受管理產品伺服器的顯示名稱 • 端點的名稱或 IP 位址
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
產品/端點 IP	根據相關的來源： • 受管理產品伺服器的 IP 位址 • 端點的 IP 位址
產品/端點 MAC	根據相關的來源： • 受管理產品伺服器的 MAC 位址 • Security Agent 端點的 MAC 位址
管理伺服器實體	端點向其回報之 Apex Central 中受管理產品伺服器的顯示名稱
網域	端點向其回報之受管理產品伺服器的網域
病毒/惡意程式	安全威脅的名稱
端點感染通道	安全威脅源自的通道
端點	端點的名稱或 IP 位址
來源主機	安全威脅起源所在的端點 IP 位址或名稱
使用者	事件發生當時已登入的使用者名稱

資料	說明
結果	受管理產品採取的處理行動結果
處理行動	受管理產品採取的處理行動
偵測	偵測總數 範例：Apex One 在 1 部電腦上偵測到相同病毒的 10 個病毒執行個體。 偵測數 = 10
項目類型	安全威脅的進入點
詳細資訊	顯示特定偵測的其他相關資訊的連結
Apex One 網域階層	Security Agent 所屬的用戶端樹狀結構網域或子網域
部門	端點所屬的 Active Directory 部門
作業系統	端點上的作業系統
特徵碼/規則	觸發偵測的特徵碼或規則
特徵碼/規則版本	觸發偵測的特徵碼或規則的版本
雲端服務供應商	雲端服務供應商的名稱
檔案	執行程序的檔案物件或程式的名稱
檔案路徑	執行程序的檔案物件路徑或程式路徑

端點病毒/惡意程式資訊

提供有關其中偵測到病毒/惡意程式之端點的特定資訊（例如，偵測到病毒/惡意程式的受管理產品、偵測到病毒/惡意程式的掃瞄類型，以及端點上偵測到病毒/惡意程式的檔案路徑）

表 B-55. 端點病毒/惡意程式資訊資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間

資料	說明
已產生	受管理產品產生資料的日期和時間
產品實體/端點	根據相關的來源： • Apex Central 中受管理產品伺服器的顯示名稱 • Security Agent 端點的名稱或 IP 位址
產品/端點 IP	根據相關的來源： • 受管理產品伺服器的 IP 位址 • Security Agent 端點的 IP 位址
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
管理伺服器實體	端點向其回報之 Apex Central 中受管理產品伺服器的顯示名稱
病毒/惡意程式	安全威脅的名稱 範例：NIMDA、BLASTER、I_LOVE_YOU.EXE
端點	端點的名稱
使用者	事件發生當時已登入的使用者名稱
掃瞄類型	報告事件的掃瞄類型（例如，即時掃瞄、預約掃瞄、手動掃瞄）
檔案	安全威脅存取的檔案物件名稱
檔案路徑	安全威脅存取的檔案物件路徑
壓縮檔中的檔案	壓縮封存檔中受影響的檔案物件名稱
結果	受管理產品採取的處理行動結果 範例：成功、需要進一步的處理行動
處理行動	受管理產品採取的處理行動 範例：檔案已清除、檔案已隔離、檔案已刪除

資料	說明
偵測	偵測總數 範例：Apex One 在 1 部電腦上偵測到相同病毒的 10 個病毒執行個體。 偵測數 = 10
雲端服務供應商	雲端服務供應商的名稱

電子郵件病毒/惡意程式資訊

提供有關其中偵測到病毒/惡意程式之電子郵件的特定資訊（例如，偵測到病毒/惡意程式的受管理產品、電子郵件的主旨行內容，以及內含病毒/惡意程式之電子郵件的寄件者）

表 B-56. 電子郵件病毒/惡意程式資訊資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
產品項目	Apex Central 中受管理產品伺服器的顯示名稱
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
病毒/惡意程式	安全威脅的名稱 範例：`NIMDA`、`BLASTER`、`I_LOVE_YOU.EXE`
收件者	觸發偵測的電子郵件收件者
寄件者	觸發偵測的電子郵件寄件者
使用者	事件發生當時已登入的使用者名稱
主旨	觸發偵測的電子郵件主旨
檔案	安全威脅存取的檔案物件名稱

資料	說明
壓縮檔中的檔案	壓縮封存檔中受影響的檔案物件名稱
結果	受管理產品採取的處理行動結果 範例：成功、需要進一步的處理行動
處理行動	受管理產品採取的處理行動 範例：檔案已清除、檔案已隔離、檔案已刪除
偵測	偵測總數 範例：Apex One 在 1 部電腦上偵測到相同病毒的 10 個病毒執行個體。 偵測數 = 10
雲端服務供應商	雲端服務供應商的名稱

網路病毒/惡意程式資訊

提供有關網路流量中發現的病毒/惡意程式執行個體的特定資訊（例如，偵測到病毒/惡意程式的受管理產品、病毒/惡意程式進入您網路所用的通訊協定，以及有關病毒/惡意程式的來源與目標特定資訊）

表 B-57. 網路病毒/惡意程式資訊資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
產品項目/端點	根據相關的來源： • Apex Central 中受管理產品伺服器的顯示名稱 • 端點的名稱或 IP 位址
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange

資料	說明
病毒/惡意程式	安全威脅的名稱 範例：NIMDA、BLASTER、I_LOVE_YOU.EXE
端點	安全威脅存取的端點 IP 位址或名稱
來源主機	安全威脅起源所在的端點 IP 位址或名稱
使用者	事件發生當時已登入的使用者名稱
流量/連線	傳輸的方向
通訊協定	安全威脅進入網路所用的通訊協定 範例：HTTP、SMTP、FTP
端點電腦	安全威脅存取的端點 IP 位址或名稱
端點通訊埠	安全威脅存取的 IP 通訊埠號碼
端點 MAC	安全威脅存取的 MAC 位址
來源電腦	安全威脅起源所在的端點 IP 位址或名稱
來源通訊埠	偵測到的安全威脅的來源 IP 位址通訊埠號碼
來源 MAC	偵測到的安全威脅的來源 MAC 位址
檔案	安全威脅存取的檔案物件名稱
結果	受管理產品採取的處理行動結果 範例：成功、需要進一步的處理行動
處理行動	受管理產品採取的處理行動 範例：檔案已清除、檔案已隔離、檔案已刪除
偵測	偵測總數 範例：Apex One 在 1 部電腦上偵測到相同病毒的 10 個病毒執行個體。 偵測數 = 10
雲端服務供應商	雲端服務供應商的名稱

病毒/惡意程式整體摘要

提供有關病毒/惡意程式偵測的整體特定摘要。範例：病毒/惡意程式的名稱、受病毒影響的端點數目、網路上病毒執行個體總數

表 B-58. 病毒/惡意程式整體摘要資料檢視

資料	說明
病毒/惡意程式	顯示受管理產品偵測到的病毒/惡意程式名稱。 範例：NIMDA、BLASTER、I_LOVE_YOU.EXE
唯一端點	顯示受病毒/惡意程式影響的唯一電腦數目。 範例：Apex One 在 3 部不同的電腦上偵測到相同病毒的 10 個病毒執行個體。 唯一端點 = 3
唯一來源	顯示病毒/惡意程式起源所在的唯一感染來源數目。 範例：Apex One 偵測到源自 2 個感染來源的相同病毒的 10 個病毒執行個體。 唯一來源 = 2
偵測	顯示受管理產品偵測到的病毒/惡意程式總數。 範例：Apex One 在 1 部電腦上偵測到相同病毒的 10 個病毒執行個體。 偵測數 = 10

病毒/惡意程式處理行動/結果摘要

提供受管理產品對病毒/惡意程式採取的處理行動摘要。範例：對病毒/惡意程式採取的特定處理行動、採取的處理行動結果、網路上的病毒/惡意程式執行個體總數

表 B-59. 病毒/惡意程式處理行動/結果摘要資料檢視

資料	說明
結果	顯示受管理產品對病毒/惡意程式採取的處理行動結果。 範例：成功、需要進一步的處理行動
處理行動	顯示受管理產品對病毒/惡意程式採取的處理行動類型。 範例：檔案已清除、檔案已隔離、檔案已刪除
唯一端點	顯示受病毒/惡意程式影響的唯一電腦數目。 範例：Apex One 在 3 部不同的電腦上偵測到相同病毒的 10 個病毒執行個體。 唯一端點 = 3
唯一來源	顯示病毒/惡意程式起源所在的唯一感染來源數目。 範例：Apex One 偵測到源自 2 個感染來源的相同病毒的 10 個病毒執行個體。 唯一來源 = 2
偵測	顯示受管理產品偵測到的病毒/惡意程式總數。範例：Apex One 在 1 部電腦上偵測到相同病毒的 10 個病毒執行個體。 偵測數 = 10

歷來病毒/惡意程式偵測摘要

提供一段時間內的病毒/惡意程式偵測摘要

資料	說明
日期/時間	顯示資料摘要發生的時間。
唯一偵測	顯示唯一病毒/惡意程式偵測數目。 範例：受管理產品在 2 個端點上偵測到相同病毒。 唯一偵測 = 1

資料	說明
唯一端點	顯示病毒/惡意程式偵測的唯一端點數目。 範例：受管理產品在 4 個端點上偵測到病毒。 唯一端點 = 4
唯一來源	顯示病毒/惡意程式的唯一來源數目。 範例：受管理產品從兩個不同來源偵測到 10 個病毒。 唯一來源 = 2
偵測	顯示受管理產品偵測到的病毒/惡意程式總數。 範例：受管理產品在 1 部電腦上偵測到 10 個病毒/惡意程式。 偵測數 = 10

病毒/惡意程式端點摘要

提供特定端點的病毒/惡意程式偵測摘要。範例：端點名稱、端點上的特定病毒/惡意程式執行個體數目、網路上的病毒/惡意程式執行個體總數

表 B-60. 病毒/惡意程式端點摘要資料檢視

資料	說明
端點	顯示受病毒/惡意程式影響的電腦 IP 位址或主機名稱。
唯一來源	顯示病毒/惡意程式起源所在的唯一感染來源數目。 範例：Apex One 偵測到源自 2 個感染來源的相同病毒的 10 個病毒執行個體。 唯一來源 = 2
唯一偵測	顯示受管理產品偵測到的唯一病毒/惡意程式數目。 範例：Apex One 在 1 部電腦上偵測到相同病毒的 10 個病毒執行個體。 唯一偵測 = 1

資料	說明
偵測	顯示受管理產品偵測到的病毒/惡意程式總數。 範例：Apex One 在 1 部電腦上偵測到相同病毒的 10 個病毒執行個體。 偵測數 = 10

病毒/惡意程式來源摘要

提供病毒爆發來源的病毒/惡意程式偵測摘要。範例：來源電腦名稱、來自來源電腦的特定病毒/惡意程式執行個體數目、網路上的病毒/惡意程式執行個體總數

表 B-61. 病毒/惡意程式來源摘要資料檢視

資料	說明
來源主機	顯示病毒/惡意程式起源所在的電腦的 IP 位址或主機名稱
唯一端點	顯示受病毒/惡意程式影響的唯一電腦數目 範例：Apex One 在 3 部不同的電腦上偵測到相同病毒的 10 個病毒執行個體 唯一偵測 = 3
唯一偵測	顯示受管理產品偵測到的唯一病毒/惡意程式數目 範例：Apex One 在 1 部電腦上偵測到相同病毒的 10 個病毒執行個體 偵測數 = 10
偵測	顯示受管理產品偵測到的病毒/惡意程式總數 範例：Apex One 在 1 部電腦上偵測到相同病毒的 10 個病毒執行個體 偵測數 = 10
部門	顯示端點所屬的部門名稱

Web 病毒/惡意程式資訊

提供有關 HTTP 或 FTP 流量中發現的病毒/惡意程式執行個體的特定資訊（例如，偵測到病毒/惡意程式的受管理產品、傳輸方向，以及下載病毒/惡意程式的 Web 瀏覽器或 FTP 用戶端）

表 B-62. Web 病毒/惡意程式資訊資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
產品項目/端點	根據相關的來源： • Apex Central 中受管理產品伺服器的顯示名稱 • 端點的名稱或 IP 位址
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
病毒/惡意程式	安全威脅的名稱 範例：`NIMDA`、`BLASTER`、`I_LOVE_YOU.EXE`
端點	安全威脅存取的端點 IP 位址或名稱
來源 URL	安全威脅起源所在的 Web/FTP 站台的 URL
使用者	事件發生當時已登入的使用者名稱
流量/連線	傳輸的方向
瀏覽器/FTP 用戶端	安全威脅存取的 Web 瀏覽器或 FTP 用戶端
結果	受管理產品採取的處理行動結果
處理行動	受管理產品採取的處理行動

資料	說明
偵測	偵測總數 範例：Apex One 在 1 部電腦上偵測到相同病毒的 10 個病毒執行個體。 偵測數 = 10
雲端服務供應商	雲端服務供應商的名稱

Web 違規/信譽評等資訊

顯示有關受管理產品在網路上偵測到 Internet 違規的摘要和詳細資料。

網站信譽評等服務詳細資訊

提供有關網頁信譽評等服務所偵測到之應用程式活動的符合性資訊

表 B-63. 網站信譽評等服務詳細資訊資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
產品項目	Apex Central 中受管理產品伺服器的顯示名稱
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
VLAN ID	可疑安全威脅起源所在的來源 VLAN ID (VID)
偵測者	偵測到安全威脅的過濾器、掃瞄引擎或受管理產品
流量/連線	傳輸的方向
通訊協定群組	受管理產品從其偵測到可疑安全威脅的廣泛通訊協定群組 範例：FTP、HTTP、P2P

資料	說明
通訊協定	受管理產品從其偵測到可疑安全威脅的通訊協定 範例：ARP、BitTorrent
說明	趨勢科技針對事件提供的詳細說明
端點	符合策略/規則之電腦的主機名稱
來源 IP	偵測到的安全威脅的來源 IP 位址
來源 MAC	偵測到的安全威脅的來源 MAC 位址
來源通訊埠	偵測到的安全威脅的來源 IP 位址通訊埠號碼
來源 IP 群組	可疑安全威脅起源所在的來源 IP 位址群組
來源網路區域	可疑安全威脅起源所在的來源網路區域
端點 IP	受可疑安全威脅影響之端點的 IP 位址
端點通訊埠	受可疑安全威脅影響之端點的通訊埠號碼
端點 MAC	受可疑安全威脅影響之端點的 MAC 位址
端點群組	受可疑安全威脅影響之端點的 IP 位址群組
端點網路區域	受可疑安全威脅影響之端點的網路區域
策略/規則名稱	觸發偵測的策略或規則
URL	觸發偵測的 URL 物件
偵測	偵測總數 範例：受管理產品在 1 部電腦上偵測到相同類型的 10 個違規。 偵測數 = 10
C&C 清單來源	辨識 C&C 伺服器的 C&C 清單來源
C&C 風險等級	C&C 伺服器的風險等級
安全威脅類型	安全威脅的類型
偵測嚴重性	事件的嚴重性等級

資料	說明
IP 位址 (關注的)	目標端點（來源或目標）的 IP 位址 如果資料交換是在網路內部進行的，則關注的 IP 是來源 IP 位址。如果流量是外部流量，則關注的 IP 是目標 IP 位址。
IP 位址 (對等)	與關注的 IP 相對的 IP 位址 例如，如果關注的 IP 是來源 IP 位址，則對等 IP 就是目標 IP 位址。
相符的已歸類事件	符合同一彙整規則的記錄檔計數
彙整的相符已歸類事件	符合同一規則的已彙整記錄檔計數
網路群組	群組的名稱
主機嚴重性	主機嚴重性
記錄 ID	記錄 ID
攻擊階段	攻擊發生階段
備註	事件的其他相關資訊
C&C 伺服器	C&C 伺服器的名稱、URL 或 IP 位址
C&C 伺服器類型	C&C 伺服器的類型
寄件者	觸發偵測的傳輸寄件者
收件者	觸發偵測的傳輸收件者
主旨	內含 Web URL 之電子郵件的主旨

Web 違規詳細資訊

提供有關網路上網頁違規偵測的特定資訊

表 B-64. Web 違規詳細資訊資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
管理伺服器實體	端點向其回報之 Apex Central 中受管理產品伺服器的顯示名稱
產品項目	Apex Central 中受管理產品伺服器的顯示名稱
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
流量/連線	傳輸的方向
通訊協定	違規是透過哪個通訊協定發生的 範例：HTTP、FTP、SMTP
URL	觸發偵測的 URL 物件
使用者/IP	違反策略的端點使用者或 IP 位址
使用者群組	違反策略之使用者的使用者群組
端點	違反策略的端點 IP 位址
端點主機	違反策略的端點 IP 位址或主機名稱
產品主機	偵測到違規的受管理產品 IP 位址或主機名稱
過濾/封鎖類型	阻止存取違規 URL 的過濾/封鎖類型 範例：URL 封鎖、URL 過濾、網頁封鎖
封鎖規則	阻止存取違規 URL 的封鎖規則 範例：URL 封鎖
策略	觸發偵測的策略
檔案	違反策略的檔案名稱
處理程序	違反策略的程序名稱

資料	說明
網頁信譽評等分級	根據趨勢科技分析的網站相對安全性（以百分比表示）
處理行動	受管理產品採取的處理行動 範例：暫不處理、封鎖
偵測	偵測總數 範例：受管理產品在 1 部電腦上偵測到相同 URL 的 10 個違規執行個體。 偵測數 = 10

Web 違規整體摘要

提供特定策略的 Web 違規摘要。範例：違反的策略名稱、用於阻止存取 URL 的過濾/封鎖類型、網路上的 Web 違規總數

表 B-65. Web 違規整體摘要資料檢視

資料	說明
策略	顯示 URL 違反的策略名稱。
過濾/封鎖類型	顯示阻止存取違規 URL 的過濾/封鎖類型。 範例：URL 封鎖、URL 過濾、網頁封鎖
唯一端點	顯示違反指定策略的唯一端點數目。 範例：受管理產品在 4 部電腦上偵測到相同 URL 的 10 個違規執行個體。 唯一端點 = 4
唯一 URL	顯示違反指定策略的唯一 URL 數目。 範例：受管理產品在 1 部電腦上偵測到相同 URL 的 10 個違規執行個體。 唯一 URL = 1

資料	說明
偵測	顯示受管理產品偵測到的 Web 違規總數。 範例：受管理產品在 1 部電腦上偵測到相同 URL 的 10 個違規執行個體。 偵測數 = 10

歷來 Web 違規偵測摘要

提供一段時間（每日一次、每週一次、每月一次）內的 Web 違規偵測摘要。範例：收集摘要資料的時間和日期、違規的端點數目、網路上的 Web 違規總數

表 B-66. 歷來 Web 違規偵測摘要資料檢視

資料	說明
日期/時間	顯示資料摘要發生的時間。
唯一策略	顯示違反的策略數目。 範例：受管理產品在 2 部電腦上偵測到相同策略的 10 個策略違規執行個體。 唯一策略 = 1
唯一端點	顯示違反指定策略的唯一端點數目。 範例：受管理產品在 4 部電腦上偵測到相同 URL 的 10 個違規執行個體。 唯一端點 = 4
唯一 URL	顯示違反指定策略的唯一 URL 數目。 範例：受管理產品在 1 部電腦上偵測到相同 URL 的 10 個違規執行個體。 唯一 URL = 1

資料	說明
偵測	顯示受管理產品偵測到的 Web 違規總數。 範例：受管理產品在 1 部電腦上偵測到相同 URL 的 10 個違規執行個體。 偵測數 = 10

Web 違規偵測摘要

提供一段時間（每日一次、每週一次、每月一次）內的 Web 違規偵測摘要。範例：收集摘要資料的時間和日期、違規的端點數目、網路上的 Web 違規總數

表 B-67. Web 違規偵測摘要資料檢視

資料	說明
唯一策略	顯示違反的策略數目。 範例：受管理產品在 2 部電腦上偵測到相同策略的 10 個策略違規執行個體。 唯一策略 = 1
唯一端點	顯示違反指定策略的唯一端點數目。 範例：受管理產品在 4 部電腦上偵測到相同 URL 的 10 個違規執行個體。 唯一端點 = 4
唯一 URL	顯示違反指定策略的唯一 URL 數目。 範例：受管理產品在 1 部電腦上偵測到相同 URL 的 10 個違規執行個體。 唯一 URL = 1

資料	說明
唯一使用者/IP	顯示違反指定策略的唯一使用者數目或端點 IP 位址數目。 範例：受管理產品偵測到來自一位使用者的相同 URL 的 10 個違規執行個體。 唯一使用者/IP = 1
唯一使用者群組	顯示違反指定策略的唯一使用者群組數目。 範例：受管理產品偵測到來自一個使用者群組的相同 URL 的 10 個違規執行個體。 唯一使用者群組 = 1
偵測	顯示受管理產品偵測到的 Web 違規總數。 範例：受管理產品在 1 部電腦上偵測到相同 URL 的 10 個違規執行個體。 偵測數 = 10

Web 違規端點摘要

提供特定端點的 Web 違規偵測摘要。範例：違規端點的 IP 位址、違反的策略數目、網路上的 Web 違規總數

表 B-68. Web 違規端點摘要資料檢視

資料	說明
端點	顯示違反 Web 策略的端點 IP 位址或主機名稱。
唯一策略	顯示違反的策略數目。 範例：受管理產品在 2 部電腦上偵測到相同策略的 10 個策略違規執行個體。 唯一策略 = 1

資料	說明
唯一 URL	顯示違反指定策略的唯一 URL 數目。 範例：受管理產品在 1 部電腦上偵測到相同 URL 的 10 個違規執行個體。 唯一 URL = 1
偵測	顯示受管理產品偵測到的 Web 違規總數。 範例：受管理產品在 1 部電腦上偵測到相同 URL 的 10 個違規執行個體。 偵測數 = 10

Web 違規過濾器/封鎖類型摘要

提供受管理產品對 Web 違規採取的處理行動摘要。範例：用於阻止存取 URL 的過濾器/封鎖類型、網路上的 Web 違規總數

表 B-69. Web 違規過濾器/封鎖類型摘要資料檢視

資料	說明
封鎖類別	顯示阻止存取違規 URL 的廣泛過濾器/封鎖類型。 範例：URL 封鎖、URL 過濾、間諜程式防護
過濾/封鎖類型	顯示阻止存取違規 URL 的特定過濾器/封鎖類型。 範例：URL 封鎖、URL 過濾、病毒/惡意程式
偵測	顯示受管理產品偵測到的 Web 違規總數。 範例：受管理產品在 1 部電腦上偵測到相同 URL 的 10 個違規執行個體。 偵測數 = 10

Web 違規 URL 摘要

提供特定 URL 的 Web 違規偵測摘要。範例：造成 Web 違規的 URL 名稱、用於阻止存取 URL 的過濾器/封鎖類型、網路上的 Web 違規總數

表 B-70. Web 違規 URL 摘要資料檢視

資料	說明
URL	顯示違反 Web 策略的 URL。
過濾/封鎖類型	顯示阻止存取違規 URL 的過濾/封鎖類型。 範例：URL 封鎖、URL 過濾、網頁封鎖
唯一端點	顯示違反指定策略的唯一端點數目。 範例：受管理產品在 4 部電腦上偵測到相同 URL 的 10 個違規執行個體。 唯一端點 = 4
偵測	顯示受管理產品偵測到的 Web 違規總數。 範例：受管理產品在 1 部電腦上偵測到相同 URL 的 10 個違規執行個體。 偵測數 = 10

資料檢視：產品資訊

顯示 Apex Central、受管理的產品、元件及使用授權的相關資訊。

Apex Central 資訊

顯示 Apex Central 使用者存取、「指令追蹤」資訊及 Apex Central 伺服器事件的相關資訊。

Apex Central 事件資訊

提供 Apex Central 伺服器事件的相關資訊（例如，受管理產品向 Apex Central 註冊、元件更新，以及啟動碼部署）

表 B-71. Apex Central 事件資訊資料檢視

資料	說明
日期/時間	事件發生的時間
事件類型	發生的事件類型（範例：通知 TMI 用戶端、伺服器通知使用者、報告服務通知使用者）
結果	事件的結果（範例：成功、未成功）
說明	活動的說明（如果有的話）

指令追蹤資訊

提供 Apex Central 向受管理產品發出之指令的相關資訊（例如，Apex Central 發出進行元件更新或啟動碼部署之指令的日期和時間，以及指令的狀態）

表 B-72. 指令追蹤資訊資料檢視

資料	說明
日期/時間	指令發出者發出指令的時間
指令類型	所發出指令的類型（範例：預約更新、啟動碼部署）
指令參數	與指令相關的特定資訊（範例：特定特徵碼檔案名稱、特定啟動碼）
使用者	發出指令的使用者
狀態更新	對所選 Apex Central 的所有指令執行最新狀態檢查的時間
成功	成功的指令數目
未成功	未成功的指令數目
進行中	仍在進行中的指令數目
全部	指令的總數（成功 + 未成功 + 進行中）

指令追蹤詳細資訊

顯示與指令相關的詳細資訊。範例：向 Apex Central 註冊的受管理產品、元件更新、啟動碼部署

表 B-73. 指令追蹤詳細資訊資料檢視

資料	說明
日期/時間	顯示發出指令的時間。
指令類型	顯示所發出指令的類型。範例：預約更新、啟動碼部署
指令參數	顯示與指令相關的特定資訊。範例：特定特徵碼檔案名稱、特定啟動碼
產品項目	顯示向其發出指令的受管理產品。
使用者	顯示發出指令的使用者。
指令狀態	顯示指令的狀態：成功、未成功、進行中
狀態更新	顯示對所選 Apex Central 的所有指令執行最新狀態檢查的時間。
結果詳細資料說明	顯示 Apex Central 為事件提供的說明。

未受管理的端點資訊

提供所偵測到未安裝 Trend Micro Security Agent 之端點的相關資訊。

表 B-74. 未受管理的端點資訊資料檢視

資料	說明
端點	端點的名稱

使用者存取資訊

提供 Apex Central 使用者存取權及使用者登入 Apex Central 時所執行活動的相關資訊

表 B-75. 使用者存取資訊資料檢視

資料	說明
日期/時間	活動的啟動日期和時間
使用者	起始活動的使用者名稱
Active Directory 群組	Active Directory 群組的名稱
使用者角色	Apex Central 中指派給使用者帳號的使用者角色
活動	使用者對 Apex Central 所執行的活動（範例：登入、編輯使用者帳號、新增部署計劃）
結果	活動的結果
說明	活動的說明（如果有的話）
角色說明	指派給使用者帳號之使用者角色的說明

元件資訊

顯示有關受管理產品元件是已過期還是最新，以及元件部署的狀態資訊、詳細資訊和摘要資訊。

端點特徵碼/引擎狀態摘要

顯示有關受管理產品使用的特徵碼檔案/掃瞄引擎的摘要資訊。

表 B-76. 端點特徵碼/引擎狀態摘要

資料	說明
產品主機	顯示安裝了受管理產品的伺服器主機名稱。
網域	顯示主機的網域名稱。
端點	顯示已安裝用戶端（例如 Apex One 用戶端）之電腦的主機名稱。
特徵碼過期	顯示具有過期特徵碼檔案的受管理產品數目。

資料	說明
特徵碼更新率 (%)	顯示具有最新特徵碼檔案的受管理產品百分比。這包括會傳回 n/a 做為值的特徵碼檔案。
引擎過期	顯示具有過期掃瞄引擎的受管理產品數目。
引擎更新率 (%)	顯示具有最新掃瞄引擎的受管理產品百分比。這包括會傳回 n/a 做為值的掃瞄引擎。

端點特徵碼/規則更新狀態摘要

此資料檢視會顯示有關特徵碼或規則的更新狀態摘要資訊。

表 B-77. 端點特徵碼/規則更新狀態摘要資料檢視

資料	說明
特徵碼/規則	顯示特徵碼或規則的名稱
特徵碼/規則狀態	指出目前的特徵碼或規則版本是否為最新版本
特徵碼/規則版本	顯示特徵碼或規則的版本
特徵碼/規則已更新	指出特徵碼或規則是否已成功更新
端點計數	顯示使用目前特徵碼或規則版本的端點數目
端點總數	顯示使用特徵碼或規則的端點總數
比率 (%)	顯示使用目前特徵碼或規則版本的端點百分比

引擎狀態

顯示有關受管理產品使用的掃瞄引擎的詳細資訊。範例：掃瞄引擎名稱、最新的掃瞄引擎部署時間，以及哪些受管理產品使用該掃瞄引擎

表 B-78. 引擎狀態資料檢視

資料	說明
產品實體/端點	此資料欄顯示下列其中一項： • 受管理產品的實體顯示名稱。Apex Central 使用受管理產品的實體顯示名稱識別受管理產品。 • 已安裝用戶端（例如 Apex One 用戶端）之電腦的 IP 位址或主機名稱。
產品主機/端點	此資料欄顯示下列其中一項： • 安裝了受管理產品的伺服器主機名稱。 • 已安裝用戶端（例如 Apex One 用戶端）之電腦的 IP 位址。
產品/端點 IP	此資料欄顯示下列其中一項： • 安裝了受管理產品的伺服器 IP 位址。 • 已安裝用戶端（例如 Apex One 用戶端）之電腦的 IP 位址。
連線狀態	此資料欄顯示下列其中一項： • 受管理產品與 Apex Central 之間的連線狀態。範例：正常、異常、離線 • 端點用戶端與受管理產品 (Apex One) 的連線狀態。範例：正常、異常、離線
產品	顯示受管理產品的名稱。範例：Apex One、ScanMail for Microsoft Exchange
產品版本	顯示受管理產品或受管理產品用戶端的版本號碼。範例：Apex One 2019、Apex Central 2019
產品角色	顯示受管理產品或具有用戶端（例如 Apex One 用戶端）的電腦在網路環境中的角色。範例：伺服器
引擎	顯示掃瞄引擎的名稱。範例：垃圾郵件防護引擎 (Windows)、病毒掃瞄引擎 IA 64 位元掃瞄引擎
引擎版本	顯示掃瞄引擎的版本。範例：垃圾郵件防護引擎 (Windows)：3.000.1153、病毒掃瞄引擎 IA 64 位元掃瞄引擎：8.000.1008
引擎狀態	顯示掃瞄引擎的目前狀態。範例：最新、過期

資料	說明
引擎已更新	顯示最新掃瞄引擎部署到受管理產品或端點的時間。

特徵碼/規則狀態

顯示有關受管理產品使用的特徵碼檔案/規則的詳細資訊。範例：特徵碼檔案/規則名稱、最新特徵碼檔案/規則部署的時間，以及哪些受管理產品使用特徵碼檔案/規則

表 B-79. 特徵碼/規則狀態資料檢視

資料	說明
產品實體/端點	此資料欄顯示下列其中一項： • 受管理產品的實體顯示名稱。Apex Central 使用受管理產品的實體顯示名稱識別受管理產品。 • 已安裝用戶端（例如 Apex One 用戶端）之電腦的 IP 位址或主機名稱。
作業系統	此資料欄會顯示安裝了受管理產品的伺服器作業系統。
產品主機/端點	此資料欄顯示下列其中一項： • 安裝了受管理產品的伺服器主機名稱。 • 已安裝用戶端（例如 Apex One 用戶端）之電腦的 IP 位址。
產品/端點 IP	此資料欄顯示下列其中一項： • 安裝了受管理產品的伺服器 IP 位址。 • 已安裝用戶端（例如 Apex One 用戶端）之電腦的 IP 位址。
更新代理程式	此資料欄會顯示受管理產品的更新代理程式。
網域	此資料欄會顯示安裝了受管理產品的伺服器網域。
管理伺服器實體顯示名稱	此資料欄會顯示管理伺服器實體顯示名稱。

資料	說明
連線狀態	此資料欄顯示下列其中一項： • 受管理產品與 Apex Central 之間的連線狀態。範例：正常、異常、離線 • 端點用戶端與受管理產品 (Apex One) 的連線狀態。範例：正常、異常、離線
產品	顯示受管理產品的名稱。範例：Apex One、ScanMail for Microsoft Exchange
產品版本	顯示受管理產品或受管理產品用戶端的版本號碼。範例：Apex One 2019、Apex Central 2019
產品角色	顯示受管理產品或具有用戶端（例如 Apex One 用戶端）的電腦在網路環境中的角色。範例：伺服器
特徵碼/規則	顯示特徵碼檔案或規則的名稱。範例：病毒碼檔案、垃圾郵件防護病毒碼
特徵碼/規則版本	顯示特徵碼或規則的版本。範例：病毒碼檔案：3.203.00、垃圾郵件防護病毒碼：14256
特徵碼/規則狀態	顯示特徵碼檔案/規則的目前狀態。範例：最新、過期
特徵碼/規則已更新	顯示最新特徵碼檔案/規則部署到受管理產品或端點的時間。
Apex One 網域階層	顯示 Apex One 網域階層的路徑。

特徵碼檔案/規則狀態摘要

顯示有關受管理產品使用的特徵碼檔案/規則的摘要資訊。範例：特徵碼檔案/規則名稱、特徵碼檔案/規則更新率，以及過期特徵碼檔案/規則數目

表 B-80. 特徵碼檔案/規則狀態摘要資料檢視

資料	說明
特徵碼檔案/規則	顯示特徵碼檔案或規則的名稱。範例：病毒碼檔案、垃圾郵件防護病毒碼

資料	說明
版本	顯示特徵碼或規則的版本。範例：病毒碼檔案：3.203.00、垃圾郵件防護病毒碼：14256
最新	顯示具有最新特徵碼檔案或規則的受管理產品百分比。
過期	顯示具有過期特徵碼檔案或規則的受管理產品數目。
更新率 (%)	顯示具有最新特徵碼檔案/規則的受管理產品百分比。這包括會傳回 n/a 做為值的特徵碼檔案/規則。
前 1 個版本的比率 (%)	顯示所含特徵碼檔案/規則為前 1 個版本的受管理產品百分比
前 2 個版本的比率 (%)	顯示所含特徵碼檔案/規則為前 2 個版本的受管理產品百分比
前 3 個版本的比率 (%)	顯示所含特徵碼檔案/規則為前 3 個版本的受管理產品百分比
前 4 個版本的比率 (%)	顯示所含特徵碼檔案/規則為前 4 個版本的受管理產品百分比
前 5 個版本的比率 (%)	顯示所含特徵碼檔案/規則為前 5 個版本的受管理產品百分比
前 6 個或更舊版本的比率 (%)	顯示所含特徵碼檔案/規則為前 6 個或更舊版本的受管理產品百分比

產品元件部署

顯示有關受管理產品使用的元件的詳細資訊。範例：特徵碼檔案/規則名稱、特徵碼檔案/規則版本號碼，以及掃瞄引擎部署狀態

表 B-81. 產品元件部署資料檢視

資料	說明
產品項目	顯示受管理產品的實體顯示名稱。Apex Central 使用受管理產品的實體顯示名稱識別受管理產品。

資料	說明
產品	顯示受管理產品的名稱。範例：Apex One、ScanMail for Microsoft Exchange
產品版本	顯示受管理產品的版本號碼。範例：Apex One 2019、Apex Central 2019
連線狀態	顯示受管理產品與 Apex Central 伺服器之間或受管理產品與其端點之間的連線狀態。
特徵碼/規則狀態	顯示特徵碼檔案/規則的目前狀態。範例：最新、過期
特徵碼/規則部署狀態	顯示最新特徵碼檔案/規則更新的部署狀態。範例：成功、未成功、進行中
特徵碼/規則部署	顯示最新特徵碼檔案/規則部署到受管理產品或端點的時間。
引擎狀態	顯示掃瞄引擎的目前狀態。範例：最新、過期
引擎部署狀態	顯示最新掃瞄更新的部署狀態。範例：成功、未成功、進行中
引擎部署	顯示最新掃瞄引擎部署到受管理產品或端點的時間。

掃瞄引擎狀態摘要

顯示有關受管理產品使用的掃瞄引擎的摘要資訊。範例：掃瞄引擎名稱、掃瞄引擎比率以及過期掃瞄引擎數目

表 B-82. 引擎狀態摘要資料檢視

資料	說明
引擎	顯示掃瞄引擎的名稱。範例：垃圾郵件防護引擎 (Windows)、病毒掃瞄引擎 IA 64 位元掃瞄引擎
版本	顯示掃瞄引擎的版本。範例：垃圾郵件防護引擎 (Windows)：3.000.1153、病毒掃瞄引擎 IA 64 位元掃瞄引擎：8.000.1008
最新	顯示具有最新掃瞄引擎的受管理產品數目。
過期	顯示具有過期掃瞄引擎的受管理產品數目。

資料	說明
更新率 (%)	顯示具有最新掃瞄引擎的受管理產品百分比。這包括會傳回「無」做為值的掃瞄引擎。

使用授權資訊

顯示有關 Apex Central 和受管理產品使用授權資訊的狀態資訊、詳細資訊與摘要資訊。

產品使用授權詳細資訊

提供受管理產品或服務之啟動碼與使用授權狀態的相關資訊（例如，受管理產品的版本和使用授權到期日）

表 B-83. 產品使用授權詳細資訊資料檢視

資料	說明
產品項目	Apex Central 中受管理產品伺服器的顯示名稱
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
產品版本	受管理產品或服務的版本
受管理服務	受管理服務的名稱 範例：網站信譽評等服務
使用授權狀態	受管理產品的使用授權狀態 範例：已啟動、已到期、在寬限期內
產品類型	啟動碼提供的受管理產品類型 範例：試用版、完整版
啟動碼	受管理產品或服務的啟動碼

資料	說明
使用授權到期日	受管理產品的使用授權到期日
授權數目	啟動碼允許的授權數目
說明	啟動碼的說明

產品使用授權資訊摘要

顯示有關啟動碼的資訊，以及使用該啟動碼的受管理產品相關詳細資訊。範例：啟動碼所允許的授權計數、試用或完整產品版本、關於啟動碼的使用者定義說明

表 B-84. 產品使用授權資訊摘要資料檢視

資料	說明
啟動碼	顯示受管理產品的啟動碼。
使用者定義的說明	顯示有關啟動碼的使用者定義說明。
產品/服務	顯示使用該啟動碼的受管理產品或服務數目。
使用授權狀態	顯示受管理產品的使用授權狀態。範例：已啟動、已到期、在寬限期內
產品類型	顯示啟動碼提供的受管理產品類型。範例：試用版、完整版
使用授權到期日	顯示受管理產品的使用授權到期日。
授權數目	顯示啟動碼允許的授權數目。

產品使用授權狀態

顯示有關受管理產品的詳細資訊，以及受管理產品所使用啟動碼的相關資訊。範例：受管理產品資訊、啟動碼是否處於作用中狀態、啟動碼所啟動的受管理產品數目

表 B-85. 產品使用授權狀態資料檢視

資料	說明
產品項目	顯示受管理產品的實體顯示名稱。Apex Central 使用受管理產品的實體顯示名稱識別受管理產品。
產品	顯示受管理產品的名稱。範例：Apex One、ScanMail for Microsoft Exchange
產品版本	顯示受管理產品的版本號碼。範例：Apex One 2019、Apex Central 2019
服務	顯示在受管理產品服務的名稱。範例：病毒爆發防範服務
使用授權狀態	顯示受管理產品的使用授權狀態。範例：已啟動、已到期、在寬限期內
啟動碼	顯示受管理產品的啟動碼。
啟動碼	顯示受管理產品所使用啟動碼的數目。
使用授權到期日	顯示受管理產品的使用授權到期日。

受管理產品資訊

顯示有關受管理產品或受管理產品端點的狀態資訊、詳細資訊和摘要資訊。

產品稽核事件記錄檔

提供受管理產品稽核事件的相關資訊（例如，受管理產品主控台存取）

表 B-86. 產品稽核事件記錄檔資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間

資料	說明
主機	根據相關的來源： • 受管理產品伺服器的顯示名稱 • Security Agent 端點的顯示名稱
使用者	事件發生當時已登入的使用者名稱
事件類別	事件的類型 範例：管理主控台存取
事件層級	事件的嚴重性等級
事件說明	事件的說明

產品發佈摘要

顯示有關已向 Apex Central 註冊之受管理產品的摘要資訊。範例：受管理產品名稱、版本號碼、受管理產品數目

表 B-87. 產品發佈摘要資料檢視

資料	說明
已向 Apex Central 註冊	顯示受管理產品向其註冊的 Apex Central 伺服器。
產品類別	顯示受管理產品的安全威脅防護類別。範例：伺服器型產品、桌面（電腦和行動裝置）產品 注意 桌面產品包括行動裝置解決方案。
產品	顯示受管理產品的名稱。範例：Apex One、ScanMail for Microsoft Exchange
產品版本	顯示受管理產品的版本號碼。範例：Apex One 2019、Apex Central 2019

資料	說明
產品角色	顯示受管理產品在網路環境中具有的角色。範例：伺服器、用戶端
產品	顯示網路包含的特定受管理產品總數。

產品事件資訊

提供受管理產品事件的相關資訊（例如，受管理產品向 Apex Central 註冊、元件更新，以及啟動碼部署）

表 B-88. 產品事件資訊資料檢視

資料	說明
收到	Apex Central 從受管理產品接收資料的日期和時間
已產生	受管理產品產生資料的日期和時間
產品項目	Apex Central 中受管理產品伺服器的顯示名稱
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
產品版本	受管理產品或服務的版本
事件嚴重性	事件的嚴重性等級
事件類型	事件的類型 範例：發現下載型病毒、檔案封鎖、還原
指令狀態	指令的狀態 範例：成功、未成功、進行中
說明	事件的說明

產品狀態資訊

提供有關已向 Apex Central 伺服器註冊之受管理產品的詳細資訊（例如，受管理產品的版本和 Build 號碼，以及受管理產品伺服器的作業系統）

表 B-89. 產品狀態資訊資料檢視

資料	說明
產品實體/端點	根據相關的來源： • Apex Central 中受管理產品伺服器的顯示名稱 • Security Agent 端點的名稱或 IP 位址
產品主機/端點	根據相關的來源： • 受管理產品伺服器的顯示名稱 • Security Agent 端點的顯示名稱
產品/端點 IP	根據相關的來源： • 受管理產品伺服器的 IP 位址 • Security Agent 端點的 IP 位址
產品/端點 MAC	根據相關的來源： • 受管理產品伺服器的 MAC 位址 • Security Agent 端點的 MAC 位址
管理 Apex Central 實體	Apex Central 伺服器（受管理產品伺服器會向此伺服器回報）的顯示名稱
管理伺服器實體	端點向其回報之 Apex Central 中受管理產品伺服器的顯示名稱
網域	受管理產品所屬的網域
連線狀態	根據相關的來源： • 受管理產品伺服器與 Apex Central 之間連線的狀態（範例：正常、異常、離線） • Security Agent 端點與受管理產品伺服器之間連線的狀態（範例：正常、異常、離線）
資料安全防護狀態	Security Agent 的資料外洩防護狀態 範例：已安裝、未安裝
特徵碼狀態	受管理產品或 Security Agent 所用特徵碼檔案/規則的狀態 範例：最新、過期

資料	說明
引擎狀態	受管理產品或 Security Agent 所用掃瞄引擎的狀態 範例：最新、過期
產品	受管理產品或服務的名稱 範例：Apex One、ScanMail for Microsoft Exchange
產品版本	受管理產品或服務的版本
Endpoint Sensor 版本	Endpoint Sensor 的版本
Application Control 版本	Application Control 的版本
Vulnerability Protection 版本	Vulnerability Protection 的版本
產品 Build	受管理產品的 Build 號碼
產品角色	受管理產品伺服器或 Security Agent 端點在網路環境中所具有的角色。（範例：伺服器）
作業系統	受管理產品伺服器或 Security Agent 端點的作業系統
作業系統版本	受管理產品伺服器或 Security Agent 端點的作業系統版本
作業系統 Service Pack	受管理產品伺服器或 Security Agent 端點的作業系統 Service Pack 號碼
更新代理程式	如果 Security Agent 為「更新代理程式」
上次預約掃瞄	上次預約掃瞄的日期和時間
上次手動掃瞄	上次手動掃瞄的日期和時間
上次立即掃瞄	上次立即掃瞄處理行動的日期和時間
即時掃瞄	如果即時掃瞄已啟動
防火牆	如果防火牆已啟動
特徵碼/規則部署狀態	特徵碼/規則的部署狀態

資料	說明
特徵碼/規則部署	特徵碼/規則部署的日期和時間
引擎部署狀態	掃瞄引擎部署狀態
引擎部署	掃瞄引擎部署的日期和時間
登入使用者	最後一個登入受管理端點之使用者的下層登入名稱 (NetBIOS_Domain\User_Name)
上次啟動	Security Agent 上次開始執行的日期和時間
離線時間	Security Agent 上次進入離線狀態的日期和時間
使用者名稱	事件發生當時已登入的使用者名稱

附錄 C

Token 變數

本節說明 Apex Central 支援的可用於自訂事件通知訊息的 Token 變數。

包含下列主題：

- 標準 Token 變數 第 C-2 頁
- 進階安全威脅活動 Token 變數 第 C-2 頁
- 攻擊發現 Token 變數 第 C-5 頁
- C&C 回呼 Token 變數 第 C-6 頁
- 內容策略違規 Token 變數 第 C-8 頁
- 資料外洩防護 Token 變數 第 C-9 頁
- 已知的安全威脅活動 Token 變數 第 C-11 頁
- 網路存取控制 Token 變數 第 C-13 頁
- Web 存取策略違規 Token 變數 第 C-14 頁

標準 Token 變數

下表說明用於自訂所有事件通知訊息的 Token 變數。

注意

部分事件通知支援其他 Token 變數。如需特定事件通知支援的 Token 變數完整清單，請參閱特定事件通知的通知方法資訊。

變數	說明
%cmserver%	Apex Central 伺服器名稱
%computer%	端點的名稱
%entity%	Apex Central 中受管理產品伺服器的顯示名稱
%event%	偵測到的事件
%pname%	受管理產品的名稱
%pver%	受管理產品的版本
%time%	事件發生的時間 (hh: mm)
%vloginuser%	事件發生當時已登入的使用者名稱
%act%	受管理產品採取的處理行動。範例：檔案已清除、檔案已刪除、檔案已隔離

進階安全威脅活動 Token 變數

注意

如需所有事件通知支援的標準 Token 變數清單，請參閱標準 Token 變數 第 C-2 頁。

下表說明用於自訂進階安全威脅活動事件通知訊息的 Token 變數。

變數	說明
%hostIP%	根據傳輸方向，%hostIP% 是由 Deep Discovery Inspector 決定的 IP 位址： • 輸出流量（內部流量傳輸到外部網路）：%hostIP% 是網路（來源）中端點的 IP 位址 • 網路內部流量：%hostIP% 是網路中端點的 IP 位址 • 網路中端點的外部流量：%hostIP% 是網路中端點的 IP 位址 • 網路外部流量：%hostIP% 是網路外部端點的 IP 位址
%group%	子網路的名稱
%START_TIME%	偵測期間的開始日期和時間 注意 通知條件決定開始時間和結束時間的指定時間範圍。
%END_TIME%	偵測期間的結束日期和時間 定義時間範圍間隔的開始和結束時間。在特定間隔期間收到記錄檔時，Apex Central 會計算這些記錄檔。如果符合警訊條件，Apex Central 會重視記錄檔。%START_TIME% 是間隔的開始時間，%END_TIME% 是間隔的結束時間。間隔長度由警訊設定中的期間門檻值決定。 注意 通知條件決定開始時間和結束時間的指定時間範圍。

變數	說明
%detections%	偵測數目 例如： 事件：高風險沙箱偵測 IP 位址：%hostIP% 主機名稱：%computer% 群組：%group% 時間範圍：%START_TIME% - %END_TIME% 偵測：%detections%

下表說明用於自訂行為監控違規與 Machine Learning 偵測之事件通知訊息的 Token 變數。

變數	說明
%hostIP%	根據傳輸方向，%hostIP% 是由 Deep Discovery Inspector 決定的 IP 位址： • 輸出流量（內部流量傳輸到外部網路）：%hostIP% 是網路（來源）中端點的 IP 位址 • 網路內部流量：%hostIP% 是網路中端點的 IP 位址 • 網路中端點的外部流量：%hostIP% 是網路中端點的 IP 位址 • 網路外部流量：%hostIP% 是網路外部端點的 IP 位址
%START_TIME%	偵測期間的開始日期和時間 注意 通知條件決定開始時間和結束時間的指定時間範圍。

變數	說明
%END_TIME%	偵測期間的結束日期和時間 定義時間範圍間隔的開始和結束時間。在特定間隔期間收到記錄檔時，Apex Central 會計算這些記錄檔。如果符合警訊條件，Apex Central 會重視記錄檔。%START_TIME% 是間隔的開始時間，%END_TIME% 是間隔的結束時間。間隔長度由警訊設定中的期間門檻值決定。 **注意** 通知條件決定開始時間和結束時間的指定時間範圍。
%detections%	偵測數目 例如： 事件：高風險沙箱偵測 IP 位址：%hostIP% 主機名稱：%computer% 群組：%group% 時間範圍：%START_TIME% - %END_TIME% 偵測：%detections%
%domain%	目標在 Apex One 網域階層中的根網域
%hierarchy%	目標在 Apex One 網域階層中的完整路徑
%BM_policy%	行為監控策略識別碼
%risklevel%	事件的風險等級
%target%	事件的目標

攻擊發現 Token 變數

下表說明用於自訂「攻擊發現」事件通知訊息的 Token 變數。

變數	說明
%cmserver%	Apex Central 伺服器名稱
%computer%	端點的名稱
%entity%	Apex Central 中受管理產品伺服器的顯示名稱
%event%	偵測到的事件
%pname%	受管理產品的名稱
%pver%	受管理產品的版本
%time%	事件發生的時間 (hh: mm)
%vloginuser%	事件發生當時已登入的使用者名稱
%act%	受管理產品採取的處理行動。範例：檔案已清除、檔案已刪除、檔案已隔離
%actresult%	受管理產品採取的處理行動結果。範例：成功、需要進一步的處理行動
%highrisk_detection%	指定期間的高風險偵測的數目
%highrisk_detection_endpoint%	指定期間具有高風險偵測的端點數目
%mediumrisk_detection%	指定期間的中度風險偵測的數目
%mediumrisk_detection_endpoint%	指定期間具有中度風險偵測的端點數目
%start_time%	偵測期間的開始日期和時間
%end_time%	偵測期間的結束日期和時間

C&C 回呼 Token 變數

下表說明用於自訂 C&C 回呼事件通知訊息的 Token 變數。

注意

如需所有事件通知支援的標準 Token 變數清單，請參閱標準 Token 變數 第 C-2 頁。

變數	說明
%CnC_LIST_SRC%	其中包含回呼位址的清單名稱
%CNC_PD_NAME%	傳送記錄檔的受管理產品伺服器的產品 ID
%CNC_PD_VERSION%	傳送記錄檔的受管理產品伺服器的版本
%CNC_PD_NODE%	傳送記錄檔的受管理產品伺服器的端點名稱
%CNC_PD_IP%	傳送記錄檔的受管理產品伺服器的 IP 位址
%CNC_EVTTIME%	記錄檔的產生時間
%CNC_AGENTNAME%	偵測到回呼的 Security Agent 端點名稱
%CNC_AGENTIP%	偵測到回呼的 Security Agent 端點 IP 位址
%CNC_AGENTDOMAIN%	偵測到回呼的 Security Agent 端點所屬的 Apex One 網域
%CNC_POLICY_RULE%	偵測到回呼的策略名稱或規則 ID
%CNC_ACTION%	安全記錄檔、個人防火牆、NCIE 記錄檔或 Web 安全記錄檔的處理行動結果
%CNC_EMAIL_SENDER%	與回呼關聯的電子郵件寄件者
%CNC_EMAIL_SUBJECT%	與回呼關聯的電子郵件主旨
%CNC_RISKLEVEL%	與 C&C 伺服器關聯的惡意程式群組風險等級
%CNC_DETECT_SOURCE%	定義偵測規則的 C&C 清單
%CNC_CHANNEL%	指示目標格式的類型 ID

變數	說明
%CNC_URL%	端點嘗試連線的遠端 URL
%CNC_URL_CATEGORY%	端點嘗試連線的站台 URL 類別
%CNC_IP_PORT%	C&C 伺服器 IP 位址和通訊埠
%CNC_EMAIL_REPT%	與回呼關聯的電子郵件收件者
%CNC_FIRST_SEEN%	C&C 伺服器的第一個已知偵測
%CNC_LAST_SEEN%	C&C 伺服器的最後一個已知偵測
%CNC_LOCATION%	C&C 伺服器的國碼
%CNC_MALEWARE_FAMILY%	與 C&C 偵測關聯的惡意程式系列
%CNC_ATTACK_GROUP%	C&C 群組清單
%CNC_PROCESS_NAME%	與 C&C 偵測關聯的程序名稱
%CALLBACK_ADDR%	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
%COMPR_HOST%	受影響的主機或電子郵件信箱
%CALLBACK_NUM%	回呼位址與遭到入侵的主機之間的聯絡次數
%COMPR_HOST_NUM%	牽涉病毒爆發的遭到入侵的主機數目
%CALLBACK_ADDR_NUM%	牽涉病毒爆發的回呼位址數目

內容策略違規 Token 變數

下表說明用於自訂內容策略違規事件通知訊息的 Token 變數。

注意

如需所有事件通知支援的標準 Token 變數清單，請參閱標準 Token 變數 第 C-2 頁。

變數	說明
%subject%	電子郵件通知的主旨標頭
%sender%	寄件者的電子郵件信箱
%recipient%	收件者的電子郵件信箱
%filtername%	違反的內容過濾規則/策略名稱
%filteract%%	過濾器套用的處理行動
%msgact%	套用至郵件的處理行動

資料外洩防護 Token 變數

下表說明用於自訂「資料外洩防護」事件通知訊息的 Token 變數。

注意

如需所有事件通知支援的標準 Token 變數清單，請參閱標準 Token 變數 第 C-2 頁。

變數	說明
%DLP_INCIDENT_TOTAL_NUM%	由直接受管理的使用者觸發的事件總數
%DLP_INCIDENT_HIGH_NUM%	由直接受管理的使用者觸發的高嚴重性事件總數
%DLP_INCIDENT_MED_NUM%	由直接受管理的使用者觸發的中嚴重性事件總數

變數	說明
%DLP_INCIDENT_LOW_NUM%	由直接受管理的使用者觸發的低嚴重性事件總數
%DLP_INCIDENT_INFO_NUM%	由直接受管理的使用者觸發的資訊性事件總數
%DLP_INCIDENT_UNDEFINED_NUM%	由直接受管理的使用者觸發之未定義的嚴重性事件總數
%DLP_INCIDENT_ALLTOTAL_NUM%	由所有受管理的使用者觸發的事件總數
%DLP_INCIDENT_ALLHIGH_NUM%	由所有受管理的使用者觸發的高嚴重性事件總數
%DLP_INCIDENT_ALLMED_NUM%	由所有受管理的使用者觸發的中嚴重性事件總數
%DLP_INCIDENT_ALLLOW_NUM%	由所有受管理的使用者觸發的低嚴重性事件總數
%DLP_INCIDENT_ALLINFO_NUM%	由所有受管理的使用者觸發的資訊性事件總數
%DLP_INCIDENT_ALLUNDEFINED_NUM%	由所有受管理的使用者觸發之未定義的嚴重性事件總數
%DLP_START_TIME%	報告期間的開始日期和時間
%DLP_END_TIME%	報告期間的結束日期和時間
%weblink%	使用此連結可檢視通知訊息中所列事件資訊的詳細資料
%INCIDENTID%	事件 ID 號碼
%SEVERITY%	事件嚴重性層級
%POLICY%	Apex Central 策略名稱 **注意** 對於觸發了在受管理產品主控台上所建立的 DLP 策略之事件，Apex Central 策略名稱會顯示為「無」。

變數	說明
%ACCOUNT%	使用者名稱
%OLD_STATUS%	修改前的事件狀態
%NEW_STATUS%	修改後的事件狀態
%LATEST_COMMENT%	關於此事件的最新備註
%DLP_VIOLATION_NUM%	與 DLP 策略相符的違規數目
%DLP_THRESHOLD%	違規數目，達到此數目就必須觸發以指出策略違規大幅增加
%DLP_TEMPLATE%	與事件大幅增加相符的範本
%DLP_USER_NAME%	與觸發了 DLP 策略違規之端點相關聯的使用者名稱
%DLP_SENDER%	觸發了 DLP 策略違規的郵件寄件者
%DLP_CHANNEL%	觸發了 DLP 策略違規的事件通道
%STATUS_CHANGE_TIME%	事件詳細資料已更新

已知的安全威脅活動 Token 變數

下表說明用於自訂「已知的安全威脅活動」或「病毒爆發防範服務」事件通知訊息的 Token 變數。

注意

如需所有事件通知支援的標準 Token 變數清單，請參閱標準 Token 變數 第 C-2 頁。

變數	說明
%device_ip%	中毒端點的 IP 位址

變數	說明
%egnver%	• 掃瞄引擎版本 • 由警訊事件類別以及「已收到主動式病毒爆發防範策略」通知和「病毒爆發防範模式已啟動」通知所使用。對於警訊事件類別的通知類型，此變數指的是受管理產品伺服器上目前已安裝的掃瞄引擎版本。 • 對於「已收到主動式病毒爆發防範策略」通知和「病毒爆發防範模式已啟動」通知，此變數指的是所需的「病毒爆發防範策略」。
%hierarchy%	• 端點在 Apex One 網域階層中的位置 • 由警訊事件類別所使用
%ptnver%	• 病毒碼版本 • 由警訊事件類別以及「已收到主動式病毒爆發防範策略」通知和「病毒爆發防範服務已啟動」通知所使用。對於警訊事件類別的通知類型，此變數指的是受管理產品伺服器上目前已安裝的病毒碼版本。 • 對於「已收到主動式病毒爆發防範策略」通知和「病毒爆發防範服務已啟動」通知，此變數指的是所需的「病毒爆發防範策略」。
%scanmethod%	特定病毒處理行動的掃瞄方法。此 Token 僅適用於下列警訊： • 發現病毒 — 第一個處理行動未成功，第二個處理行動不可用 • 發現病毒 — 第一個和第二個處理行動未成功 • 發現病毒 — 第一個處理行動成功 • 發現病毒 — 第二個處理行動成功
%threat_info%	• 由病毒爆發防範策略所提供的病毒/惡意程式安全威脅資訊 • 由「已收到主動式病毒爆發防範策略」和「病毒爆發防範服務已啟動」所使用
%vcnt%	• 病毒計數。 • 由病毒爆發警訊所使用。

變數	說明
%vdest%	• 病毒/惡意程式的目標。 • 範例： 電子郵件偵測：%vdest% 是預期收件者 以主機為基礎/端點偵測：%vdest% 是端點 IP 位址或主機名稱 • 由警訊事件類別所使用
%vfile%	中毒檔案名稱。由警訊事件類別所使用。
%vfilepath%	中毒檔案目錄。由警訊事件類別所使用。
%vname%	病毒或惡意程式名稱。由警訊事件類別所使用。
%vsrc%	• 病毒/惡意程式的起源或感染來源。 • 例如，如果防毒受管理產品在電子郵件訊息中偵測到病毒/惡意程式時，訊息寄件者會取得 %vsrc% 的值。 • 由警訊事件類別以及網路病毒警訊通知類型所使用。

網路存取控制 Token 變數

下表說明用於自訂網路存取控制事件通知訊息的 Token 變數。

注意

如需所有事件通知支援的標準 Token 變數清單，請參閱標準 Token 變數 第 C-2 頁。

變數	說明
%action%	網路病毒牆執行器對網路病毒採取的處理行動（暫不處理、丟棄或隔離）
%description%	由潛在弱點攻擊偵測到的事件所使用的錯誤說明

Web 存取策略違規 Token 變數

下表說明用於自訂「Web 存取策略違規」事件通知訊息的 Token 變數。

注意

如需所有事件通知支援的標準 Token 變數清單，請參閱標準 Token 變數 第 C-2 頁。

變數	說明
%url%	有疑問的 URL
%vdestip%	目標 URL 的 IP 位址
%blockrule%	違反的規則名稱
%blocktype%	套用到 URL 的處理行動

附錄 D

IPv6 支援

本附錄包含有關 Apex Central 中 IPv6 支援範圍的資訊。

包含下列主題：

- Apex Central 伺服器需求 第 D-2 頁
- IPv6 支援限制 第 D-2 頁
- 設定 IPv6 位址 第 D-2 頁
- 顯示 IP 位址的畫面 第 D-3 頁

Apex Central 伺服器需求

在 Apex Central 伺服器上安裝並啟動 IPv6 堆疊之後，會自動啟動 IPv6 支援。

注意

Trend Micro 假設讀者熟悉 IPv6 概念及設定支援 IPv6 定址之網路的相關工作。

IPv6 支援限制

下表列出 IPv6 支援的限制：

項目	限制
雙 IP 堆疊	Apex Central 僅支援雙 IP 堆疊。如果移除 IPv4 堆疊，IPv6 支援可能無法正常運作。
IPv4 回送介面	需要 IPv4 回送介面。如果要驗證 TCP/IP 軟體是否正常運作，請 ping `127.0.0.1`。
IPv6 位址格式	Apex Central 不支援包含 % 字元的 IPv6 伺服器位址。
Apex Central 報告	下列靜態報告不支援 IPv6 位址： • 策略違規報告 • 服務違規報告
Apex Central 功能	下列功能不支援 IPv6 位址： • 進階記錄查詢的 IP 位址範圍 • 可疑物件記錄的 IPv6 位址標準化

設定 IPv6 位址

透過 Web 主控台可設定 IPv6 位址。下面是一些組態設定準則。

- Apex Central 可接受標準的 IPv6 位址表示法。

  例如：

  `2001:0db7:85a3:0000:0000:8a2e:0370:7334`

  `2001:db7:85a3:0:0:8a2e:370:7334`

  `2001:db7:85a3::8a2e:370:7334`

  `::ffff:192.0.2.128`

- Apex Central 也可接受連結-本機 IPv6 位址，例如：

  fe80::210:5aff:feaa:20a2

  警告!

  指定連結-本機 IPv6 位址時應謹慎小心，因為即使 Apex Central 可以接受這類位址，但它可能在某些情況下無法如預期般運作。例如，如果更新來源位於其他網路區段且可由其連結-本機 IPv6 位址所辨識，Apex Central 就無法從該來源進行更新。

- IPv6 位址是 URL 的一部分時，請使用方括號 ([]) 將位址括起來。

顯示 IP 位址的畫面

IP 位址會顯示下列畫面上：

- 產品目錄
- 記錄查詢結果
- 伺服器註冊
- 資訊中心 Widget

附錄 E

MIB 檔案

本節討論該 Apex Central 支援的管理資訊庫 (MIB) 檔案。

包含下列主題：

- 使用 Apex Central MIB 檔案 第 E-2 頁
- 使用 NVW Enforcer SNMPv2 MIB 檔案 第 E-2 頁

使用 Apex Central MIB 檔案

從下列連結下載 Apex Central MIB 檔案，並使用支援 SNMP 通訊協定的應用程式，將檔案解壓縮並匯入。

https://CM_IP:CM_Port/TVCSDownload/tools/ApexCentral_mib.zip

使用 NVW Enforcer SNMPv2 MIB 檔案

從下列連結下載 NVW Enforcer SNMPv2 MIB 檔案，並使用支援 SNMP 通訊協定的應用程式，將檔案解壓縮並匯入。

- https://CM_IP:CM_Port/TVCSDownload/tools/nvw2_mib2.zip

附錄 F

Syslog 內容對應 — CEF

下表提供 Apex Central 記錄檔輸出與 CEF Syslog 類型之間的 Syslog 內容對應關係。

包含下列主題：

- CEF 攻擊發現偵測記錄檔 第 F-3 頁
- CEF 行為監控記錄檔 第 F-9 頁
- CEF C&C 回呼記錄檔 第 F-14 頁
- CEF 內容安全記錄檔 第 F-19 頁
- CEF 資料外洩防護記錄檔 第 F-27 頁
- CEF 裝置存取控制記錄檔 第 F-35 頁
- CEF Endpoint Application Control 記錄檔 第 F-42 頁
- CEF 引擎更新狀態記錄檔 第 F-44 頁
- CEF 入侵防護記錄檔 第 F-46 頁
- CEF 受管理的產品登入/登出事件 第 F-49 頁
- CEF 網路內容檢測記錄檔 第 F-51 頁
- CEF 特徵碼更新狀態記錄檔 第 F-54 頁

- CEF Machine Learning 記錄檔 第 F-56 頁
- CEF 產品稽核事件 第 F-61 頁
- CEF 沙盒偵測記錄檔 第 F-63 頁
- CEF 間諜程式/可能的資安威脅程式記錄檔 第 F-66 頁
- CEF 可疑檔案記錄檔 第 F-74 頁
- CEF 病毒/惡意程式記錄檔 第 F-77 頁
- CEF Web 網頁安全記錄檔 第 F-82 頁

CEF 攻擊發現偵測記錄檔

注意

如果一個攻擊發現偵測記錄檔所關聯的物件超過 4 個，Apex Central 只會轉送前 4 個物件。

CEF 索引鍵	說明	值
標頭 (logVer)	CEF 格式版本	CEF:0
標頭 (vendor)	裝置供應商	趨勢科技
標頭 (pname)	裝置產品	Apex Central
標頭 (pver)	裝置版本	2019
標頭 (eventid)	事件 ID	700220
標頭 (eventName)	記錄檔名稱	攻擊發現偵測
標頭 (severity)	嚴重性	3
deviceExternalId	識別碼	範例：38
rt	事件觸發時間 (UTC)	範例：“2018 年 3 月 22 日 08:23:23 GMT +00:00”
dhost	端點主機名稱	範例：ApexOneClient01
dst	用戶端 IPv4 位址	範例：10.0.8.20
C6a3	用戶端 IPv6 位址	範例：fd96:7521:9502:6:b5b0:b2b5:4173:3f5d
duser	使用者名稱	範例：Admin004
customerExternalID	執行個體 ID	範例：8c1e2d8f-a03b-47ea-aef8-5aeab99ea697
cn1Label	"cn1" 欄位的對應標籤	SLF_RiskLevel

CEF 索引鍵	說明	值
cn1	風險等級	範例：0 • 0：未知 • 100：低度風險 • 500：中度風險 • 1000：高度風險
cn2Label	"cn2" 欄位的對應標籤	SLF_PatternNumber
cn2	病毒碼號碼	範例：30.1012.00
cs1Label	"cs1" 欄位的對應標籤	SLF_RuleID
cs1	規則 ID	範例：powershell invoke expression
cat	類別 ID	範例：point of entry
cs2Label	"cs2" 欄位的對應標籤	SLF_ADEObjectGroup_Info_1

CEF 索引鍵	說明	值

cs2	攻擊發現物件資訊	例如：
		
		process - powershell.exe - {
		"META_FILE_MD5" :
		"9393f60b1739074eb17c5f4dddefe239",
		"META_FILE_NAME" :
		"powershell.exe",
		"META_FILE_SHA1" :
		"887ce4a295c163791b60fc23d285e6d84f28ee4c",
		"META_FILE_SHA2" :
		"de96a6e50044335375dc1ac238336066889d9ffc7d73628ef4fe1b1b160ab32c",
		"META_PATH" :
		"c:\\windows\\system32\\windowspowershell\\v1.0\\",
		"META_PROCESS_CMD" :
		["powershell cmd "],
		"META_PROCESS_PID" : 7132,
		"META_SIGNER" :
		"microsoft windows",
		"META_SIGNER_VALIDATION" :
		true,
		"META_USER_USER_NAME" :
		"Administrator",
		"META_USER_USER_SERVERNAME" :
		"Host",
		"OID" : 1
		}

cs3Label	"cs3" 欄位的對應標籤	SLF_ADEObjectGroup_Info_2

CEF 索引鍵	說明	值

cs3	攻擊發現物件資訊	例如：
		
		process - powershell.exe - {
		"META_FILE_MD5" :
		"9393f60b1739074eb17c5f4dddefe239",
		"META_FILE_NAME" :
		"powershell.exe",
		"META_FILE_SHA1" :
		"887ce4a295c163791b60fc23d285e6d84f28ee4c",
		"META_FILE_SHA2" :
		"de96a6e50044335375dc1ac238336066889d9ffc7d73628ef4fe1b1b160ab32c",
		"META_PATH" :
		"c:\\windows\\system32\\windowspowershell\\v1.0\\",
		"META_PROCESS_CMD" :
		["powershell cmd "],
		"META_PROCESS_PID" : 7132,
		"META_SIGNER" :
		"microsoft windows",
		"META_SIGNER_VALIDATION" :
		true,
		"META_USER_USER_NAME" :
		"Administrator",
		"META_USER_USER_SERVERNAME" :
		"Host",
		"OID" : 1
		}

cs4Label	"cs4" 欄位的對應標籤	SLF_ADEObjectGroup_Info_3

CEF 索引鍵	說明	值

cs4	攻擊發現物件資訊	例如：
		
		process - powershell.exe - {
		"META_FILE_MD5" :
		"9393f60b1739074eb17c5f4dddefe239",
		"META_FILE_NAME" :
		"powershell.exe",
		"META_FILE_SHA1" :
		"887ce4a295c163791b60fc23d285e6d84f28ee4c",
		"META_FILE_SHA2" :
		"de96a6e50044335375dc1ac238336066889d9ffc7d73628ef4fe1b1b160ab32c",
		"META_PATH" :
		"c:\\windows\\system32\\windowspowershell\\v1.0\\",
		"META_PROCESS_CMD" :
		["powershell cmd "],
		"META_PROCESS_PID" : 7132,
		"META_SIGNER" :
		"microsoft windows",
		"META_SIGNER_VALIDATION" :
		true,
		"META_USER_USER_NAME" :
		"Administrator",
		"META_USER_USER_SERVERNAME" :
		"Host",
		"OID" : 1
		}

cs5Label	"cs5" 欄位的對應標籤	SLF_ADEObjectGroup_Info_4

CEF 索引鍵	說明	值

cs5	攻擊發現物件資訊	例如：
		<pre>process - powershell.exe - {
		"META_FILE_MD5" :
		"9393f60b1739074eb17c5f4ddd
		efe239",
		"META_FILE_NAME" :
		"powershell.exe",
		"META_FILE_SHA1" :
		"887ce4a295c163791b60fc23d2
		85e6d84f28ee4c",
		"META_FILE_SHA2" :
		"de96a6e50044335375dc1ac238
		336066889d9ffc7d73628ef4fe
		1b1b160ab32c",
		"META_PATH" :
		"c:\\windows\\system32\\wi
		ndowspowershell\\v1.0\\",
		"META_PROCESS_CMD" :
		["powershell cmd "],
		"META_PROCESS_PID" : 7132,
		"META_SIGNER" :
		"microsoft windows",
		"META_SIGNER_VALIDATION" :
		true,
		"META_USER_USER_NAME" :
		"Administrator",
		"META_USER_USER_SERVERNAME" :
		"Host",
		"OID" : 1
		}</pre>

deviceNtDomain	Active Directory 網域	範例：APEXTMCM
dntdom	Apex One 網域階層	範例：OSCEDomain1
TMCMLogDetected Host	發生記錄事件的端點名稱	範例：MachineHostName
TMCMLogDetected IP	發生記錄事件的 IP 位址	範例：10.1.2.3
ApexCentralHost	Apex Central 主機名稱	範例：TW-CHRIS-W2019

CEF 索引鍵	說明	值
devicePayloadId	唯一訊息 GUID	範例：1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform	端點作業系統	範例：Windows 7 6.1 (Build 7601) Service Pack 1

記錄檔範例：

```
CEF:0|Trend Micro|Apex Central|2019|700211|Attack Discovery
Detections|3|deviceExternalId=5 rt=Jan 17 2019 03:38:06 GMT+
00:00 dhost=VCAC-Window-331 dst=10.201.86.150 customerExtern
alID=8c1e2d8f-a03b-47ea-aef8-5aeab99ea697 cn1Label=SLF_RiskL
evel cn1=0 cn2Label=SLF_PatternNumber cn2=30.1012.00 cs1Labe
l=SLF_RuleID cs1=powershell invoke expression cat=point of e
ntry cs2Label=SLF_ADEObjectGroup_Info_1 cs2=process - code9.
exe - {USER: administrator09} deviceNtDomain=APEXTMCM dntdom
=OSCEDomain1 TMCMLogDetectedHost=VCAC-Window-331 TMCMLogDete
ctedIP=10.201.86.150 ApexCentralHost=TW-CHRIS-W2019devicePay
loadId=1C00290C0360-9CDE11EB-D4B8-F51F-C697 TMCMdevicePlatfo
rm=Windows 7 6.1 (Build 7601) Service Pack 1
```

CEF 行為監控記錄檔

CEF 索引鍵	說明	值
標頭 (logVer)	CEF 格式版本	CEF:0
標頭 (vendor)	產品供應商	Trend Micro
標頭 (pname)	產品名稱	Apex Central
標頭 (pver)	產品版本	2019
標頭 (eventid)	行為監控策略識別碼	BM:1000
標頭 (eventName)	記錄檔名稱	行為監控
標頭 (severity)	嚴重性	3

CEF 索引鍵	說明	值
rt	事件觸發時間 (UTC)	範例：“2018 年 3 月 22 日 08:23:23 GMT+00:00”
dvchost	主機名稱	範例：localhost
cs2Label	cs2 欄位的對應標籤	策略
cs2	策略類型	• 遭到入侵的可執行檔 • 新的啟動程式 • 主機檔案的修改 • 程式庫植入 • 新增 Internet Explorer 嵌入程式 • Internet Explorer 設定的修改 • Shell 的修改 • 新增服務 • 安全策略修改 • 防火牆策略的修改 • 系統檔案的修改 • 重複的系統檔案 • 分層服務提供器 • 系統程序的修改 • 可疑行為 • 新發現的程式 • 未經授權的檔案加密 • 安全威脅行為分析 • 使用者定義的策略
sproc	事件的目標	範例：C:\\Windows\\SysWOW64\\rundll32.exe

CEF 索引鍵	說明	值
cs3Label	cs3 欄位的對應標籤	Event_Type
cs3	事件類型	• 程序 • 處理影像 • 登錄 • 檔案系統 • 驅動程式 • SDT • 系統 API • 使用者模式 • 弱點攻擊 • 全部
cs4Label	cs4 欄位的對應標籤	作業
cs4	事件目標所執行的作業	• 建立程序 • 開啟 • 終止 • 刪除 • 寫入 • 存取 • 建立檔案 • 關閉 • 執行 • 啟動 • 弱點攻擊 • 未處理的作業
cs5Label	cs5 欄位的對應標籤	Risk_Level

CEF 索引鍵	說明	值
cs5	風險等級	範例：1 • 0：低 • 1：高
TMCMLogTarget	目標主機	範例：HKCU\\Software\ \Microsoft\\Windows\ \CurrentVersion\\Run\\COM+
act	轉譯的處理行動	• 允許 • 詢問 • 拒絕 • 終止 • 唯讀 • 唯讀/唯寫 • 唯讀/僅能執行 • 意見反應 • 清除 • 未知 • 評估 • 已終止。檔案已還原。 • 已終止。有些檔案未還原。 • 已終止。檔案未還原。 • 已終止。重新啟動結果：檔案已還原。 • 已終止：重新啟動結果：部分檔案未還原。 • 已終止：重新啟動結果：檔案未還原。
shost	來源主機（端點）	範例：shost1

CEF 索引鍵	說明	值
src	來源主機 IP 位址	範例："10.0.147.105"
deviceFacility	產品	範例：Apex One
原因	嚴重安全威脅類型	範例：E • A：已知的進階持續安全威脅 (APT) • B：社交工程攻擊 • C：弱點攻擊 • D：橫向移動 • E：未知安全威脅 • F：C&C 回呼 • G：勒索軟體
deviceNtDomain	Active Directory 網域	範例：APEXTMCM
dntdom	Apex One 網域階層	範例：OSCEDomain1
TMCMLogDetectedHost	發生記錄事件的端點名稱	範例：MachineHostName
TMCMLogDetectedIP	發生記錄事件的 IP 位址	範例：10.1.2.3
ApexCentralHost	Apex Central 主機名稱	範例：TW-CHRIS-W2019
devicePayloadId	唯一訊息 GUID	範例：1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform	端點作業系統	範例：Windows 7 6.1 (Build 7601) Service Pack 1

記錄檔範例：

```
CEF:0|Trend Micro|Apex Central|2019|BM:1000|Behavior Monitor
ing|3|rt=Sep 20 2019 01:02:03 GMT+00:00 dvchost=localhost cs
5Label=Risk_Level cs5=1 cs2Label=Policy cs2=Threat Behavior
Analysis sproc=subject cs3Label=Event_Type cs3=File system
TMCMLogTarget=HKCU\\Software\\Microsoft\\Windows\\CurrentVer
```

```
sion\\Run\\COM+ act=Ask cs4Label=Operation cs4=Create Proces
s shost=shost1 src=10.0.76.40 deviceFacility=Apex One reason
=G deviceNtDomain=APEXTMCM dntdom=OSCEDomain1 TMCMLogDetecte
dHost=shost1 TMCMLogDetectedIP=10.0.76.40 ApexCentralHost=TW
-CHRIS-W2019 devicePayloadId=1C00290C0360-9CDE11EB-D4B8-F51F
-C697 TMCMdevicePlatform=Windows 7 6.1 (Build 7601) Service
Pack 1
```

CEF C&C 回呼記錄檔

CEF 索引鍵	說明	值
標頭 (logVer)	CEF 格式版本	CEF:0
標頭 (vendor)	裝置供應商	Trend Micro
標頭 (pname)	裝置產品	Apex Central
標頭 (pver)	裝置版本	2019
標頭 (eventid)	CnC：處理行動	CnC：封鎖
標頭 (eventName)	名稱	CnC 回呼
標頭 (severity)	嚴重性	3
deviceExternalId	識別碼	範例：12
cat	記錄類型	範例：1756
deviceFacility	產品	範例：Apex One
cs2Label	cs2 欄位的對應標籤	範例：El_ProductVersion
cs2	產品版本	範例：11.0
rt	事件觸發時間 (UTC)	範例：“2018 年 3 月 22 日 08:23:23 GMT+00:00”
shost	端點主機名稱	範例：ApexOneClient01
src	端點 IPv4 位址	範例：10.201.86.187

CEF 索引鍵	說明	值
c6a2Label	c6a2 欄位的對應標籤	範例：SLF_ClientIP
c6a2	端點 IPv6 位址	範例：2620:101:4003:7a0:fd4b:52ed:53bd:ae3d
cs3Label	cs3 欄位的對應標籤	範例：SLF_DomainName
cs3	網域名稱	範例：DOMAIN1
cs4Label	cs4 欄位的對應標籤	範例：SLF_PolicyName
cs4	策略名稱	範例：網頁信譽評等服務資料庫中的 C&C 伺服器 URL — HTTP（要求）
act	處理行動	範例：封鎖 • 0：未知 • 1：暫不處理 • 2：封鎖 • 3：監控 • 4：刪除 • 5：隔離 • 6：警告 • 7：警告並繼續 • 8：覆寫
cn1Label	cn1 欄位的對應標籤	範例：SLF_CCCA_RiskLevel

CEF 索引鍵	說明	值
cn1	C&C 風險等級	範例：1 • 0：SLF_CCCA_RISKLEVEL_UNKNOWN • 1：SLF_CCCA_RISKLEVEL_LOW • 2：SLF_CCCA_RISKLEVEL_MEDIUM • 3：SLF_CCCA_RISKLEVEL_HIGH
cn2Label	cn2 欄位的對應標籤	範例：SLF_CCCA_DetectionSource
cn2	C&C 清單來源	範例：1 • 0：SLF_CCCA_GLOBAL_LIST • 1：SLF_CCCA_CUSTOM_LIST • 2：SLF_CCCA_CUSTOM_LIST_USER_DEFINED
cn3Label	cn3 欄位的對應標籤	範例：SLF_CCCA_DetectionFormat
cn3	回呼位址格式	範例：1 • 0：IP • 1：IP • 2：HTTP • 3：SMTP
要求	URL	範例：http://CC13.jojo.com
deviceCustomDate1Label	deviceCustomDate1 欄位的對應標籤	範例：SLF_FirstSeen

CEF 索引鍵	說明	值
deviceCustomDate1	首次監控到回呼嘗試的 UTC 時間	範例：2017 年 10 月 10 日 16:58:03 GMT+ 00:00
deviceCustomDate2Label	deviceCustomDate2 欄位的對應標籤	範例：SLF_LastSeen
deviceCustomDate2	上次監控到回呼嘗試的 UTC 時間	範例：2017 年 10 月 11 日 10:58:03 GMT+ 00:00
cs5Label	cs5 欄位的對應標籤	範例：CnCDestination
cs5	回呼 URL 位址	範例：http://CC13.jojo.com
dst	回呼 IPv4 位址	範例：10.201.86.195
c6a3Label	c6a3 欄位的對應標籤	範例：CnCDestination
c6a3	回呼 IPv6 位址	範例：fe80::38ca:cd15:443c:40bb%11
deviceProcessName	程序名稱	範例：C:\\Program Files (x86)\\Internet Explorer\\iexplore.exe
dvchost	主機名稱	範例："localhost"
deviceNtDomain	Active Directory 網域	範例：APEXTMCM
dntdom	Apex One 網域階層	範例：OSCEDomain1
TMCMLogDetectedHost	發生記錄事件的端點名稱	範例：MachineHostName
TMCMLogDetectedIP	發生記錄事件的 IP 位址	範例：10.1.2.3
ApexCentralHost	Apex Central 主機名稱	範例：TW-CHRIS-W2019
devicePayloadId	唯一訊息 GUID	範例：1C00290C0360-9CDE11EB-D4B8-F51F-C697

CEF 索引鍵	說明	值
deviceDirection	網路流量方向	範例：0 值的意義會隨 “cat” 欄位值而異。 如果 “cat” 欄位值為 1756、1707 或 1733： • 0：未知 • 1：輸入 • 2：輸出 如果 “cat” 欄位值為 1739、1741 或 1723： • 0：輸出 • 1：輸入 • 2：未知 如果 “cat” 欄位值為 1705、1735 或 1775： • -1：未知 • 0：外寄電子郵件 • 1：內送電子郵件 • 2：內部電子郵件
TMCMdevicePlatform	端點作業系統	範例：Windows 7 6.1 (Build 7601) Service Pack 1

記錄檔範例：

```
CEF:0|Trend Micro|Apex Central|2019|CnC:Block|CnC Callback
|3|deviceExternalId=12 rt=Oct 11 2017 06:34:09 GMT+00:00 cat
=1756 deviceFacility=Apex One cs2Label=EI_ProductVersion cs2
=11.0 shost=ApexOneClient01 src=10.201.86.187 cs3Label=SLF_D
omainName cs3=DOMAIN act=Block cn1Label=SLF_CCCA_RiskLevel c
n1=1 cn2Label=SLF_CCCA_DetectionSource cn2=1 cn3Label=SLF_CC
CA_DestinationFormat cn3=1 dst=10.201.86.195 deviceProcessNa
me=C:\\Program Files (x86)\\Internet Explorer\\iexplore.exe
```

```
deviceNtDomain=APEXTMCM dntdom=OSCEDomain1 dvchost=localhost
TMCMLogDetectedHost=ApexOneClient01 TMCMLogDetectedIP=10.201
.86.187 ApexCentralHost=TW-CHRIS-W2019 devicePayloadId=1C002
90C0360-9CDE11EB-D4B8-F51F-C697 deviceDirection=0 TMCMdevice
Platform=Windows 7 6.1 (Build 7601) Service Pack 1
```

CEF 內容安全記錄檔

CEF 索引鍵	說明	值
標頭 (logVer)	CEF 格式版本	CEF:0
標頭 (vendor)	裝置供應商	Trend Micro
標頭 (pname)	裝置產品	Apex Central
標頭 (pver)	裝置產品版本	2019
標頭 (eventid)	MS：過濾器處理行動	MS:Clean
標頭 (eventName)	策略名稱	策略
標頭 (severity)	嚴重性	3
cnt	偵測數目	範例：10
dhost	列出所有收件者	範例：employee_a1@Acompany.com;employee_a2@Acompany.com
duser	其中一個收件者	範例：employee_a1@Acompany.com
act	過濾器處理行動	範例：Clean 如需詳細資訊，請參閱過濾器處理行動對應資料表 第 F-24 頁。
cs1Label	cs1 欄位的對應標籤	範例：Policy_Settings
cs1	策略設定	範例：Default_policy

CEF 索引鍵	說明	值
cs2Label	cs2 欄位的對應標籤	範例：Product_Version
cs2	產品版本	範例：11
cs3Label	cs3 欄位的對應標籤	範例：Filter_Type
cs3	過濾器類型	範例：URL reputation filter • 0：未知 • 1：ContentFilter • 2：AttachmentFilter • 3：StandardFilter • 4：SizeFilter • 5：DisclaimerMgr • 6：SpamFilter • 7：OPP • 8：ImportFilter • 9：PhishingFilter • 10：UrlReputationFilter
cs4Label	cs4 欄位的對應標籤	範例：CLF_ReasonCode
cs4	原因代碼	範例：存取
cs5Label	cs5 欄位的對應標籤	範例：CLF_ReasonCodeSource
cs5	原因代碼來源	範例：Web
cs6Label	cs6 欄位的對應標籤	範例：Action_on_Message

CEF 索引鍵	說明	值
cs6	處理行動	範例：3 • 0：未知 • 1：無 • 2：傳送 • 3：刪除 • 4：隔離 • 5：延後 • 6：轉寄 • 7：取代 • 8：封存 • 100：清除巨集 • 101：暫不處理
cat	記錄類型	範例：1705
dvchost	端點主機名稱	範例：ApexOneClient01
rt	事件觸發時間 (UTC)	範例：“2018 年 3 月 22 日 08:23:23 GMT+00:00”
cn1Label	cn1 欄位的對應標籤	範例：Severity
cn1	嚴重性代碼	範例：2 • 0：未知 • 1：資訊 • 2：警告 • 3：錯誤 • 4：嚴重
TMCMLogSeverity	嚴重性說明	第二個掃瞄引擎
cn2Label	cn2 欄位的對應標籤	Filter_Action_Result

CEF 索引鍵	說明	值
cn2	過濾器處理行動結果	範例：21 如需詳細資訊，請參閱過濾器處理行動結果對應資料表 第 F-25 頁。
deviceExternalId	識別碼	範例：5
fname	檔案	範例：RERERW~42w.exe
msg	主旨	範例：開啟這封電子郵件就有機會獲得免費手機
shost	列出所有違規的寄件者/使用者	範例："bear" <bear@abc.mail.com>;"yumi" <yumi@abc.mail.com>
suser	其中一個違規的寄件者/使用者	範例："bear" <bear@abc.mail.com>
deviceFacility	產品	範例：Deep Discovery Email Inspector
src	電子郵件寄件者 IP 位址	範例：10.206.155.122
filepath	可疑檔案位置	範例：https://ca91-1.testurl.com:443
要求	可疑的 URL	範例：https://ca91-1.testurl.com:443

CEF 索引鍵	說明	值
原因	嚴重安全威脅類型	範例：E • A：已知的進階持續安全威脅 (APT) • B：社交工程攻擊 • C：弱點攻擊 • D：橫向移動 • E：未知安全威脅 • F：C&C 回呼 • G：勒索軟體
ApexCentralHost	Apex Central 主機名稱	範例：TW-CHRIS-W2019
devicePayloadId	唯一訊息 GUID	範例：1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform	端點作業系統	範例：Windows 7 6.1 (Build 7601) Service Pack 1

記錄檔範例：

```
CEF:0|Trend Micro|Apex Central|2019|MS:Clean|This is a policy
name|3|deviceExternalId=90045 rt=Sep 17 2018 01:27:42 GMT+00
:00 dhost=user@test.com duser=user@test.com act=Clean cs1Label
=Policy_Settings cs1=This is policy content cs2Label=CLF_Produ
ctVersion cs2=3.2 cs3Label=Filter_Type cs3=URL reputation filt
er cs5Label=CLF_ReasonCodeSource cs5=20 cs6Label=Action_on_Mes
sage cs6=0 cat=1705 dvchost=ApexOneClient01 cn1Label=Severity
cn1=2 TMCMLogSeverity=Second scan engine fname=NE_AEP.1550
msg=plain_qp_no8_av1u_NE_AEP.1550 shost=user2@test.com suser=
user2@test.com cn2Label=Filter_Action_Result cn2=21 deviceFaci
lity=Deep Discovery Email Inspector src=10.206.155.122 reason=
B,G ApexCentralHost=TW-CHRIS-W2019 devicePayloadId=1C00290C036
0-9CDE11EB-D4B8-F51F-C697 TMCMdevicePlatform=Windows 7 6.1 (B
uild 7601) Service Pack 1
```

過濾器處理行動對應資料表

值	說明
0	未知
1	無
2	清除
3	刪除
4	移動
5	重新命名
6	暫不處理/記錄
7	清除巨集
8	丟棄
9	隔離
10	插入/取代
11	封存
12	加上戳記
13	封鎖
14	重新導向郵件以供核准
81	加密
90	偵測
257	重設

過濾器處理行動結果對應資料表

值	說明
0	未知
1	無
21	檔案已清除
22	檔案已刪除
23	檔案已隔離
24	檔案已重新命名
25	檔案暫不處理
26	無法清除檔案。暫不處理
27	無法清除檔案。已刪除
28	無法清除檔案。已重新命名
29	無法清除檔案。已隔離
30	檔案已清除巨集
31	無法清除檔案。已清除巨集
32	檔案已取代
33	檔案已丟棄
34	檔案已封存
35	檔案已成功封鎖
36	檔案已成功隔離
37	檔案已成功加上戳記
38	檔案已上傳
39	無法清除檔案。已隔離

值	說明
40	無法清除檔案。暫不處理
41	拒絕存取
42	無處理行動
43	成功將系統重新開機
44	清除間諜程式/可能的資安威脅程式對系統有不良影響
45	成功手動停止掃瞄
46	成功重新導向郵件以供核准
81	已加密
121	無法清除檔案
122	無法刪除檔案
123	無法隔離檔案
124	無法重新命名檔案
125	無法暫不處理檔案
126	無法清除或暫不處理檔案
127	無法清除或刪除檔案
128	無法清除或重新命名檔案
129	無法清除或隔離檔案
130	無法清除檔案中的巨集
131	無法清除檔案或檔案中的巨集
132	無法取代檔案
133	無法丟棄檔案
134	無法封存檔案
135	無法封鎖檔案

值	說明
136	無法隔離檔案
137	無法在檔案中加上戳記
138	無法上傳檔案
139	無法清除或隔離檔案
140	無法清除或暫不處理檔案
141	無法拒絕存取
142	無法執行處理行動
143	需要採取處理行動 — 請重新啟動端點以完成安全威脅清除
145	無法手動停止掃瞄
146	無法重新導向郵件以供核准
201	需要採取處理行動 — 請執行完整系統掃瞄
202	需要採取處理行動 — 請使用 Apex One 工具箱中的 "Rescue Disk" 工具來移除此安全威脅。如果此問題持續發生，請洽詢支援人員
203	需要採取處理行動 — 請使用 Apex One 工具箱中的 "Rootkit Buster" 工具來移除此安全威脅。如果此問題持續發生，請洽詢支援人員
204	需要採取處理行動 — 請使用 Apex One 工具箱中的 "Clean Boot" 工具來移除此安全威脅。如果此問題持續發生，請洽詢支援人員

CEF 資料外洩防護記錄檔

CEF 索引鍵	說明	值
標頭 (logVer)	CEF 格式版本	CEF:0
標頭 (vendor)	裝置供應商	Trend Micro
標頭 (pname)	裝置產品	Apex Central

CEF 索引鍵	說明	值
標頭 (pver)	裝置版本	2019
標頭 (eventid)	事件 ID	700106
標頭 (eventName)	記錄檔名稱	資料外洩防護
標頭 (severity)	嚴重性	3
cs1Label	cs1 欄位的對應標籤	策略 GUID
cs1	策略 GUID	範例： FAF492CF-164C-4672-9A79-F1AB9CB288A3
cn1Label	cn1 欄位的對應標籤	產品
cn1	產品類型值	範例：15
rt	事件觸發時間 (UTC)	範例：“2018 年 3 月 22 日 08:23:23 GMT+00:00”
src	來源主機 IP 位址	範例：10.0.57.160
smac	來源主機 MAC 位址	範例：74-27-00-0C-65-E7
shost	來源主機名稱	範例：shost1
cs4Label	cs4 欄位的對應標籤	Incident_Source_(AD_Account)
cs4	違規的使用者名稱	範例：Trend
suser	電子郵件寄件者	範例：sender@example.com
要求	存取的 URL	範例：https://example.com/api/content
duser	以逗號 (,) 分隔的收件者清單	範例： user1@example.com;user2@example.com;
msg	主旨	範例：Sample,20171017

CEF 索引鍵	說明	值
filepath	檔案路徑	範例：D:\\Windows Live Mail\\Storage Folders\\Imported Fo e52\\Local Folders\\Sent Items\\Archive Aft de1\\Clients,Adv 22b\\\
fname	觸發器檔案名稱	範例：2B43363A-000000A4.eml
fsize	檔案大小（以位元組為單位）	範例：3
cs5Label	cs5 欄位的對應標籤	規則
cs5	規則名稱	範例：SAMPLE RULE SET
cs6Label	cs6 欄位的對應標籤	範本
cs6	範本名稱	範例：Apex One policy
cn3Label	cn3 欄位的對應標籤	通道
cn3	通道類型	範例：3 如需詳細資訊，請參閱通道對應資料表 第 F-32 頁。
cn2Label	cn2 欄位的對應標籤	處理行動
cn2	處理行動結果	範例：4 如需詳細資訊，請參閱處理行動結果對應資料表 第 F-31 頁。
cs2Label	cs2 欄位的對應標籤	策略
cs2	策略名稱	範例：OfficeScan
cs3Label	cs3 欄位的對應標籤	產品實體/端點
cs3	端點主機名稱	範例：Sample_Host
dvchost	伺服器主機名稱	範例：localhost
deviceFacility	產品名稱	範例：Apex One
deviceNtDomain	Active Directory 網域	範例：APEXTMCM

CEF 索引鍵	說明	值
dntdom	Apex One 網域階層	範例：OSCEDomain1
externalId	事件的記錄 ID	範例：101
cfp1Label	cfp1Label 欄位的對應標籤	ForensicFileAvailable
cfp1	指出是否可以下載鑑識檔案	• 0：無法下載檔案 • 1：可以下載檔案
TMCMLogDetectedHost	發生記錄事件的端點名稱	範例：MachineHostName
TMCMLogDetectedIP	發生記錄事件的 IP 位址	範例：10.1.2.3
ApexCentralHost	Apex Central 主機名稱	範例：TW-CHRIS-W2019
devicePayloadId	唯一訊息 GUID	範例：1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform	端點作業系統	範例：Windows 7 6.1 (Build 7601) Service Pack 1

記錄檔範例：

```
CEF:0|Trend Micro|Apex Central|2019|700106|Data Loss Prevent
ion|3|cs3Label=Product_Entity/Endpoint cs3=Sample_Host dvc
host=Sampledvchost cs2Label=Policy cs2=N/A cn1Label=Product
cn1=15 rt=Oct 13 2017 02:54:04 GMT+00:00 src=10.0.9.34 smac=
34-E6-D7-84-BC-7F shost=shost1 cs4Label=Incident_Source_(AD_
Account) cs4=12467 filePath=D:\\2. DRIVER\\drivers WIN7\\Dri
vers\\DP_CardReader_14032.7z\\O2Micro\\FORCED\\6x86\\ fname=
O2MDFvst.INF cs5Label=Rule cs5=SAMPLE RULE SET cs6Label=Temp
late cs6=Apex One policy cn3Label=Channel cn3=0 cn2Label=Act
ion cn2=4 deviceFacility=Apex One deviceNtDomain=APEXTMCM dn
tdom=OSCEDomain1 externalId=101 cfp1Label=ForensicFileAvaila
ble cfp1=0 dvchost=localhost TMCMLogDetectedHost=ApexOneClie
nt01 TMCMLogDetectedIP=10.201.86.187 ApexCentralHost=TW-CHRI
S-W2019 devicePayloadId=1C00290C0360-9CDE11EB-D4B8-F51F-C697
 TMCMdevicePlatform=Windows 7 6.1 (Build 7601) Service Pack
 1
```

處理行動結果對應資料表

值	說明
-1	無法使用
0	已封鎖
1	已刪除
2	已傳送
3	已記錄
4	暫不處理
5	已隔離
6	已取代
7	已封存
8	已封存 (僅郵件內文)
9	已隔離 (僅郵件內文)
10	暫不處理 (僅郵件內文)
11	已加密
12	已警示 (端點)
13	已警示 (伺服器)
14	資料已錄製
15	使用者有正當理由
16	已遞交
17	已改變收件者
18	密件已複製
19	已延後傳送

值	說明
20	已加上戳記
21	附件已刪除
22	主旨已加標籤
23	X 標頭已加標籤
24	已解密
25	已重新加密
26	已加標籤（郵件）
27	已加密（使用者金鑰）
28	已加密（群組金鑰）
29	已移動
30	暫不處理 (已加密)
31	暫不處理 (使用者有正當理由)
32	已封鎖 (未安裝 Endpoint Encryption)
33	已封鎖 (使用者有正當理由)
34	已封鎖 (已登出 Endpoint Encryption)
35	已封鎖 (Endpoint Encryption 錯誤)
36	Web 上傳

通道對應資料表

值	說明
65535	無法使用
0	卸除式儲存

值	說明
1	SMB
2	電子郵件
3	IM
4	FTP
5	HTTP
6	HTTPS
7	PGP
8	資料錄製器
9	印表機
10	剪貼簿
11	同步處理
12	P2P
13	網路郵件
14	文件管理
15	雲端儲存
121	SMTP 電子郵件
122	Exchange 用戶端郵件
123	Lotus Note 電子郵件
130	網路郵件 (Yahoo!Mail)
131	網路郵件 (Hotmail)
132	網路郵件 (Gmail)
133	網路郵件 (AOL Mail)
140	IM (MSN)

值	說明
141	IM (AIM)
142	IM (Yahoo Messenger)
143	IM (Skype)
191	P2P (BitTorrent)
192	P2P (EMule)
193	P2P (Winny)
194	P2P (HTCSYN)
195	P2P (iTunes)
196	雲端儲存 (DropBox)
197	雲端儲存 (Box)
198	雲端儲存 (Google Drive)
199	雲端儲存 (OneDrive)
200	雲端儲存 (SugarSync)
201	雲端儲存 (Hightail)
202	IM (QQ)
203	網路郵件（其他）
204	雲端儲存 (Evernote)
211	文件管理 (SharePoint)

CEF 裝置存取控制記錄檔

CEF 索引鍵	說明	值
標頭 (logVer)	CEF 格式版本	CEF:0
標頭 (vendor)	裝置供應商	Trend Micro
標頭 (pname)	裝置產品	Apex Central
標頭 (pver)	裝置版本	2019
標頭 (eventid)	事件 ID	700107
標頭 (eventName)	記錄檔名稱	裝置存取控制
標頭 (severity)	嚴重性	3
rt	事件觸發時間 (UTC)	範例：“2018 年 3 月 22 日 08:23:23 GMT+00:00”
cs1Label	cs1 欄位的對應標籤	產品實體/端點
cs1	伺服器主機名稱	範例：Sample_Host
shost	來源主機名稱	範例：shost1
duser	使用者名稱	範例：testserver\\administrator
dvchost	目標主機名稱	範例：localhost
cn1Label	cn1 欄位的對應標籤	產品
cn1	產品識別碼	範例：Apex One 如需詳細資訊，請參閱產品識別碼對應資料表 第 F-37 頁。
sproc	目標程序	範例：C:\\Windows\\explorer.exe
fname	檔案名稱	範例：F:\\Autorun.inf
cn2Label	cn2 欄位的對應標籤	Device_Type

CEF 索引鍵	說明	值
cn2	裝置類型	範例：0 • 0：USB 儲存裝置 • 1：非儲存 USB • 2：CD/DVD • 3：磁碟片 • 4：網路磁碟機
cn3Label	cn3 欄位的對應標籤	權限
cn3	權限	範例：3 • 0：修改 • 1：讀取和執行 • 2：讀取 • 3：僅列出裝置內容 • 4：封鎖
deviceFacility	產品	範例：Apex One
deviceNtDomain	Active Directory 網域	範例：APEXTMCM
dntdom	Apex One 網域階層	範例：OSCEDomain1
TMCMLogDetectedHost	發生記錄事件的端點名稱	範例：MachineHostName
TMCMLogDetectedIP	發生記錄事件的 IP 位址	範例：10.1.2.3
ApexCentralHost	Apex Central 主機名稱	範例：TW-CHRIS-W2019
devicePayloadId	唯一訊息 GUID	範例：1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform	端點作業系統	範例：Windows 7 6.1 (Build 7601) Service Pack 1

記錄檔範例：

```
CEF:0|Trend Micro|Apex Central|2019|700107|Device Access C
ontrol|3|rt=Aug 16 2017 04:49:15 GMT+00:00 cs1Label=Product_
Entity/Endpoint cs1=Sample_Host shost=shost1 dvchost=localho
st cn1Label=Product cn1=15 sproc=C:\\Windows\\explorer.exe f
name=F:\\Autorun.inf cn2Label=Device_Type cn2=0 cn3Label=Per
mission cn3=3 deviceFacility=Apex One deviceNtDomain=APEXTMC
M dntdom=OSCEDomain1 TMCMLogDetectedHost=shost1 TMCMLogDetec
tedIP=10.0.76.40 ApexCentralHost=TW-CHRIS-W2019 devicePayloa
dId=1C00290C0360-9CDE11EB-D4B8-F51F-C697 TMCMdevicePlatform
=Windows 7 6.1 (Build 7601) Service Pack 1
```

產品識別碼對應資料表

值	說明
0	未知產品
1	ScanMail for ccMail
2	ScanMail for Lotus Domino
3	ScanMail for Microsoft Exchange
4	ScanMail for Microsoft Mail
5	ScanMail for OpenMail
6	保留 1
7	保留 2
8	保留 3
9	保留 4
10	InterScan WebProtect
11	保留 5
12	保留 6
13	保留 7

值	說明
14	PC-cillin 企業版
15	Apex One
16	Apex One for Microsoft SBS
18	ServerProtect for Windows
19	ServerProtect for Windows (SOHO)
20	Apex Central
21	通用
22	InterScan VirusWall for Unix
23	InterScan VirusWall for Windows
24	MOCA
25	GoldenGate
26	主動式更新
27	IS_Y2K_SCANNER
28	Y2K VIRUS TECH SUPPORT SRV
30	HouseCall
31	PC-cillin ISP 伺服器
32	PC-cillin ISP 用戶端
33	eManager for ScanMail Exchange
34	InterScan Messaging Security Suite for Windows
35	InterScan Messaging Security Suite for UNIX
36	PortalProtect
37	GateLock Corporate Edition
38	防火牆管理 (NetScreen)

值	說明
39	InterScan Web Security Suite for Solaris
40	InterScan Web Security Suite for Windows NT
41	Nokia Message Protector
42	InterScan Web Security Suite for Linux
43	InterScan Web Security Suite for Appliance
44	InterScan Messaging Security Appliance
45	InterScan for Small and Medium Business for Windows NT
46	InterScan Web Security Virtual Appliance
47	InterScan Messaging Security Virtual Appliance
50	InterScan Gateway Security Appliance
51	ServerProtect for Linux
52	ServerProtect for EMC
53	ServerProtect for NetApp
56	子 Apex Central 伺服器
60	損害清除及復原服務
65	Golden Gate for NT
66	網路病毒牆 1200
67	網路病毒牆 MIPS
68	網路病毒牆 2500
69	網路病毒牆 2500 v2
70	安全弱點評估
71	網路病毒牆執行器 1200
72	網路病毒牆執行器

值	說明
73	網路病毒牆執行器
75	Trend Micro Threat Mitigator
85	間諜程式防護企業版
87	Trend Micro InterScan for Cisco CSC SSM-20
88	Trend Micro InterScan for Cisco CSC SSM-10
90	IM 安全性
95	InterScan VirusWall
96	InterScan VirusWall for Linux
100	Control Manager Agent
200	eDoctor 伺服器
300	eDoctor 用戶端
132	InterScan Messaging Security Suite for Solaris
120	Threat Discovery Appliance
131	適用於 Linux 的資料庫安全防護
151	Total Discovery Mitigation Server
154	Deep Discovery Inspector
155	ScanMail for IBM Domino
156	Deep Discovery Email Inspector
1000	InterScan eManager
1001	InterScan AppletTrap
1002	InterScan VirusWall Java
1003	IS_SEMAIL
1004	InterScan WebProtect for ICAP

值	說明
10001	NEC StarOffice
20001	Dr. Soloman 防毒
20002	Inoculan
20003	Norton Anti-Virus
20004	Sophos Sweep
20005	Intel LANProtect
20006	McAfee Virus Scan
20007	FProt
21000	其他協力廠商產品
31001	Apex One (Mac)
31002	Trend Micro Endpoint Encryption
31003	Trend Micro Endpoint Application Control
31004	Trend Micro Deep Security
31006	Vulnerability Protection
31005	趨勢科技行動安全防護
31007	趨勢科技 Safe Mobile Workforce
31008	Deep Discovery Analyzer
31009	Trend Micro Endpoint Sensor
31012	Deep Discovery Web Inspector
31101	Trend Micro Email Security
31102	Worry Free Business Security Services
31103	Trend Micro Web Security
31104	Cloud App Security

值	說明
55555	示範產品

CEF Endpoint Application Control 記錄檔

CEF 索引鍵	說明	值
標頭 (logVer)	CEF 格式版本	CEF:0
標頭 (vendor)	裝置供應商	Trend Micro
標頭 (pname)	裝置產品	Apex Central
標頭 (pver)	裝置版本	2019
標頭 (eventid)	裝置事件類別識別碼	• 0：允許 • 1：封鎖 • 2：鎖定
標頭 (eventName)	事件名稱	Endpoint Application Control 違規資訊
標頭 (severity)	嚴重性	3
deviceExternalId	識別碼	範例：39
rt	事件觸發時間 (UTC)	範例：“2018 年 3 月 22 日 08:23:23 GMT+00:00”
dvchost	電腦名稱	範例：localhost
shost	用戶端主機名稱	範例：shost1
cs1	產品伺服器特徵碼版本	範例：1297
suser	用戶端使用者名稱	範例：TREND\User
cs2	用戶端 IPv4 位址	範例：10.0.17.6

CEF 索引鍵	說明	值
c6a3	用戶端 IPv6 位址	範例：fe80::38ca:cd15:443c:40bb%11
cn1	用戶端狀態	• 1：正在重建資料庫 • 2：線上 • 3：離線
filehash	應用程式檔案 SHA-1 雜湊	範例：D6712CAE5EC821F910E14945153AE7871AA536CA
fname	應用程式檔案名稱	範例：notepad.exe
cs3	應用程式程序指令行	範例：notepad.exe
duser	使用者名稱	範例：Admin004
cs4	規則名稱	範例：SAMPLE RULE SET
cs5	策略名稱	範例：SAMPLE POLICY
act	策略處理行動	• 0：已允許 • 1：已封鎖 • 2：報告為允許 • 3：報告為封鎖
deviceFacility	產品名稱	範例：Trend Micro Endpoint Application Control
deviceNtDomain	Active Directory 網域	範例：APEXTMCM
dntdom	Apex One 網域階層	範例：OSCEDomain1
ApexCentralHost	Apex Central 主機名稱	範例：TW-CHRIS-W2019
devicePayloadId	唯一訊息 GUID	範例：1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform	端點作業系統	範例：Windows 7 6.1 (Build 7601) Service Pack 1

記錄檔範例：

```
CEF:0|Trend Micro|Apex Central|2019|EAC:1|Endpoint Applica
tion Control Violation Information|3|deviceExternalId=39 rt=
Jun 27 2012 03:14:03 GMT+00:00 cs1Label=Version cs1=1.299.00
 suser=TMCM\\QA cs2Label=ApplicationControlEvent_ClientIPAdd
ress_V4 cs2=0.0.0.0 cn1Label=Connection_Status cn1=0 fileHas
h=c0869b72C5606D22D92A6AC986686BB87485A25b fname=P2P_TEST.ex
e cs3Label=Command cs3=C:\\P2P_TEST.exe duser=QA cs4Label=Ru
le cs4=Test cs5Label=Policy cs5=TestPolicy act=Blocked devic
eFacility=Trend Micro Endpoint Application Control deviceNtD
omain=APEXTMCM dntdom=OSCEDomain1 ApexCentralHost=TW-CHRIS-
W2019 devicePayloadId=1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform=Windows 7 6.1 (Build 7601) Service Pack
1
```

CEF 引擎更新狀態記錄檔

CEF 索引鍵	說明	值
標頭 (logVer)	CEF 格式版本	CEF:0
標頭 (vendor)	產品供應商	Trend Micro
標頭 (pname)	產品名稱	Apex Central
標頭 (pver)	產品版本	2019
標頭 (eventid)	事件 ID	800102
標頭 (eventName)	記錄檔名稱	引擎更新狀態
標頭 (severity)	嚴重性	3
rt	事件觸發時間 (UTC)	範例：“2018 年 3 月 22 日 08:23:23 GMT+00:00”
shost	產品實體/端點	範例：shost1
cs2Label	cs2 欄位的對應標籤	產品/端點 IP

CEF 索引鍵	說明	值
cs2	產品/端點 IP	範例：10.0.17.6
cn1Label	cn1 欄位的對應標籤	連線狀態
cn1	連線狀態	範例：100 • 0：無法連線 • 1：作用中 • 2：離線 • 100：產品作用中 • 101：產品離線，但用戶端作用中 • 102：行動
cn2Label	cn2 欄位的對應標籤	引擎
cn2	引擎	範例：4096
cn5Label	cn5 欄位的對應標籤	引擎版本
cs5	引擎版本	範例：9.950.1006
cn3Level	cn3 欄位的對應標籤	引擎狀態
cn3	引擎狀態	範例：1 • 1：最新 • 2：過期
cs6Label	cs6 欄位的對應標籤	AUComponent_Type
cs6	主動式更新元件類型	範例：1 • 1：引擎
deviceFacility	受管理產品名稱	範例：Apex One
msg	引擎類型顯示名稱	範例："病毒掃瞄引擎 DLL (Windows 2000/NT，32 位元)"
deviceNtDomain	Active Directory 網域	範例：APEXTMCM

CEF 索引鍵	說明	值
dntdom	Apex One 網域階層	範例：OSCEDomain1
ApexCentralHost	Apex Central 主機名稱	範例：TW-CHRIS-W2019
devicePayloadId	唯一訊息 GUID	範例：1C00290C0360-9CDE11EB-D4B8-F51F-C697

記錄檔範例：

```
CEF:0|Trend Micro|Apex Central|2019|800102|Engine Update S
tatus|3|rt=Apr 20 2017 12:04:34 GMT+00:00 shost=shost1 cs2La
bel=Product/Endpoint_IP cs2=10.0.17.6 cn1Label=Connection_St
atus cn1=100 cn2Label=Engine cn2=4096 cs5Label=Engine_Versio
n cs5=9.950.1006 cn3Label=Engine_Status cn3=1 cs6Label=AUCom
ponent_Type cs6=1 deviceFacility=Apex One deviceNtDomain=APE
XTMCM dntdom=OSCEDomain1
```

CEF 入侵防護記錄檔

CEF 索引鍵	說明	值
標頭 (logVer)	CEF 格式版本	CEF:0
標頭 (vendor)	產品供應商	Trend Micro
標頭 (pname)	產品名稱	Apex Central
標頭 (pver)	產品版本	2019
標頭 (eventid)	事件 ID	
標頭 (eventName)	記錄檔名稱	
標頭 (severity)	嚴重性	3
dvchost	受管理端點的顯示名稱	範例：localhost
rt	記錄檔產生時間 (UTC)	範例：2017 年 11 月 15 日 08:43:57 GMT+ 00:00

CEF 索引鍵	說明	值
src	來源 IPv4 位址	範例：10.1.152.12
c6a2Label	"c6a2" 欄位的對應標籤	SLF_SourceIPv6
c6a2	來源 IPv6 位址	"2001:b011:1004:325b:8db7:6ca9:8fc5:321a"
smac	來源 MAC 位址	範例："18:31:BF:4F:30:DD"
spt	來源通訊埠	範例：60886
dst	目標 IPv4 位址	範例：10.1.153.151
c6a3Label	"c6a3" 欄位的對應標籤	SLF_DestinationIPv6
c6a3	目標 IPv6 位址	範例："2001:b011:1004:325b:8db7:6ca9:8fc5:654a"
dmac	目標主機 MAC 位址	範例："D0:17:C2:95:ED:71"
dpt	目標通訊埠	範例：139
cn2Label	"cn2" 欄位的對應標籤	SLF_IsDetectionOnly
cn2	指出系統是否處於「僅偵測」模式	範例：0 • 0 或 NULL = 否 • 1 = 是
act	處理行動	範例："LOG" SLF_ACTION 對應： • 0 = 未知 • 3 = 刪除 • 6 = 記錄 • 10 = 插入/取代 • 13 = 封鎖 • 257 = 重設

CEF 索引鍵	說明	值
deviceDirection	輸入或輸出方向	範例："Apex One"
cn3Label	"cn3" 欄位的對應標籤	SLF_Rank
cn3	事件的權重優先順序	範例：3 從嚴重性 x 資產值計算得出
cn4Label	"cn4" 欄位的對應標籤	SLF_SeverityCode
cn4	系統定義的事件嚴重性值	範例：1 • 1 = 低 • 2 = 中 • 3 = 高 • 4 = 嚴重
proto	遭入侵的網路通訊協定	範例：10009 • 28 = ICMP • 46 = ICMPv6 • 10003 = TCP • 10004 = UDP • 10005 = IGMP • 10006 = GGP • 10007 = PUP • 10008 = IDP • 10009 = ND • 10010 = RAW
cs2Label	"cs2" 欄位的對應標籤	SLF_ConnectionType
cs2	網路應用程式名稱	範例："DCERPC Services"
cn1Label	"cn1" 欄位的對應標籤	SLF_RuleID

CEF 索引鍵	說明	值
cn1	檢查規則的 ID	範例：1005448
cs1Label	"cs1" 欄位的對應標籤	SLF_RuleContent
cs1	規則 ID 和說明的字串常值	範例："1005448 - SMB Null Session Detected - 1"
cnt	彙整計數	範例：1
deviceNtDomain	Active Directory 網域	範例：APEXTMCM
dntdom	Apex One 網域階層	範例：OSCEDomain1

記錄檔範例：

```
CEF:0|Trend Micro|Apex Central|2019|Log|1009549 - Detected T
erminal Services (RDP) Server Traffic - 1 (ATT&CK T1015,T104
3,T1076,T1048,T1032,T1071)|3|rt=Apr 20 2020 03:33:20 GMT+00:
00 dvchost=OSCEClient23 deviceFacility=Apex One act=Log,src=
10.1.1.9 dst=80.1.1.9 smac=54-BF-64-84-7F-09 spt=89 dmac=54-
BF-64-84-7F-19 dpt=449 cn2Label=SLF_IsDetectionOnly cn2=0 de
viceDirection=Inbound cn3Label=SLF_Rank cn3=1 cn4Label=SLF_S
everityCode cn4=1 proto=10009 cs2Label=SLF_ConnectionType cs
2=N/A cn1Label=SLF_RuleID cn1=1009549 cs1Label=SLF_RuleConte
nt cs1=1009549 - Detected Terminal Services (RDP) Server Tra
ffic - 1 (ATT&CK T1015,T1043,T1076,T1048,T1032,T1071) cnt=1
deviceNtDomain=APEXTMCM dntdom=OSCEDomain1
```

CEF 受管理的產品登入/登出事件

CEF 索引鍵	說明	值
標頭 (logVer)	CEF 格式版本	CEF:0
標頭 (vendor)	裝置供應商	Trend Micro
標頭 (pname)	裝置產品	Apex Central

CEF 索引鍵	說明	值
標頭 (pver)	裝置版本	2019
標頭 (eventid)	事件 ID	700211
標頭 (eventName)	記錄檔名稱	受管理的產品登入/登出事件
標頭 (severity)	嚴重性	3
deviceExternalId	識別碼	範例：38
deviceFacility	產品名稱	範例：ScanMail for Microsoft Exchange
cs1Label	cs1 欄位的對應標籤	Product_Version
cs1	產品版本	範例：14
cn1Label	cn1 欄位的對應標籤	Command_Status
cn1	指令狀態	範例：110
msg	詳細的事件資訊	範例：Sample Message
shost	產品伺服器名稱	範例：SMEX01

記錄檔範例：

```
CEF:0|Trend Micro|Apex Central|2019|700211|Managed Product L
ogon/Logoff Events|3|deviceExternalId=11 shost=SMEX01 device
Facility=ScanMail for Microsoft Exchange cs1Label=Product_Ve
rsion cs1=14 cn1Label=Command_Status cn1=110 msg=A user with
 the Administrator role(s) has logged on.Detail Information
:UserName:TEST2013\\administrator,IP address:10.204.166.127,
EventType:Log in/out,SourceType:SMEX UI.#015
```

CEF 網路內容檢測記錄檔

CEF 索引鍵	說明	值
標頭 (logVer)	CEF 格式版本	CEF:0
標頭 (vendor)	裝置供應商	Trend Micro
標頭 (pname)	裝置產品	Apex Central
標頭 (pver)	裝置版本	2019
標頭 (eventid)	NCIE：處理行動	NCIE：暫不處理
標頭 (eventName)	名稱	可疑連線
標頭 (severity)	嚴重性	3
deviceExternalId	識別碼	範例：1
cat	記錄類型	範例：1756
deviceFacility	產品	範例：Apex One
rt	事件觸發時間 (UTC)	範例：“2018 年 3 月 22 日 08:23:23 GMT+00:00”
deviceProcessName	處理程序	範例：C:\\Windows\\system32\\svchost-1.exe
src	本機 IPv4 位址	範例：10.201.86.152
c6a2Label	c6a2 欄位的對應標籤	範例：SLF_SourceIP
c6a2	本機 IPv6 位址	範例：2620:101:4003:7a0:fd4b:52ed:53bd:ae3d
spt	本機 IP 位址通訊埠	範例：54594
dst	遠端 IPv4 位址	範例：10.69.81.64
c6a3Label	c6a3 欄位的對應標籤	範例：SLF_DestinationIP

CEF 索引鍵	說明	值
c6a3	遠端 IPv6 位址	範例：fe80::38ca:cd15:443c:40bb%11
dpt	遠端 IP 位址通訊埠	範例：80
act	處理行動	範例：暫不處理 • 0：未知 • 1：暫不處理 • 2：封鎖 • 3：監控 • 4：刪除 • 5：隔離 • 6：警告 • 7：警告並繼續 • 8：覆寫
deviceDirection	傳輸方向	範例：輸入 • 0：無 • 1：輸入 • 2：輸出
cn1Label	cn1 欄位的對應標籤	範例：SLF_PatternType
cn1	特徵碼類型	範例：2 • 0：全域 C&C 特徵碼 • 1：關聯規則 • 2：使用者定義的封鎖清單
cs2Label	cs2 欄位的對應標籤	範例：NCIE_ThreatName
cs2	安全威脅名稱	範例：Malicious_identified_CnC_querying_on_UDP_detected

CEF 索引鍵	說明	值
原因	嚴重安全威脅類型	範例：E • A：已知的進階持續安全威脅 (APT) • B：社交工程攻擊 • C：弱點攻擊 • D：橫向移動 • E：未知安全威脅 • F：C&C 回呼 • G：勒索軟體
dvchost	主機名稱	範例："localhost"
deviceNtDomain	Active Directory 網域	範例：APEXTMCM
dntdom	Apex One 網域階層	範例：OSCEDomain1
TMCMLogDetectedHost	發生記錄事件的端點名稱	範例：MachineHostName
TMCMLogDetectedIP	發生記錄事件的 IP 位址	範例：10.1.2.3
ApexCentralHost	Apex Central 主機名稱	範例：TW-CHRIS-W2019
devicePayloadId	唯一訊息 GUID	範例：1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform	端點作業系統	範例：Windows 7 6.1 (Build 7601) Service Pack 1

記錄檔範例：

```
CEF:0|Trend Micro|Apex Central|2019|NCIE:Pass|Suspicious
Connection|3|deviceExternalId=1 rt=Oct 11 2017 06:34:06 GMT+0
0:00 cat=1756 deviceFacility=Apex One deviceProcessName=C:\\W
indows\\system32\\svchost-1.exe act=Pass src=10.201.86.152 ds
t=10.69.81.64 spt=54594 dpt=80 deviceDirection=None cn1Label=
SLF_PatternType cn1=2 cs2Label=NCIE_ThreatName cs2=Malicious_
identified_CnC_querying_on_UDP_detected reason=F deviceNtDoma
```

```
in=APEXTMCM dntdom=OSCEDomain1 dvchost=shost1 TMCMLogDetected
Host=shost1 TMCMLogDetectedIP=10.1.2.3ApexCentralHost=TW-CHRI
S-W2019 devicePayloadId=1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform=Windows 7 6.1 (Build 7601) Service Pack 1
```

CEF 特徵碼更新狀態記錄檔

CEF 索引鍵	說明	值
標頭 (logVer)	CEF 格式版本	CEF:0
標頭 (vendor)	產品供應商	Trend Micro
標頭 (pname)	產品名稱	Apex Central
標頭 (pver)	產品版本	2019
標頭 (eventid)	事件 ID	800101
標頭 (eventName)	記錄檔名稱	特徵碼更新狀態
標頭 (severity)	嚴重性	3
rt	事件觸發時間 (UTC)	範例：“2018 年 3 月 22 日 08:23:23 GMT+00:00”
shost	產品實體/端點	範例：shost1
cs1Label	cs1 欄位的對應標籤	作業系統
cs1	作業系統	範例：Windows 7
cs2Label	cs2 欄位的對應標籤	產品/端點 IP
cs2	產品/端點 IP	範例：10.0.7.20
cs3Label	cs3 欄位的對應標籤	更新代理程式
cs3	更新代理程式	範例：0
cs4Label	cs4 欄位的對應標籤	網域

CEF 索引鍵	說明	值
cs4	網域	範例：預設
cn1Label	cn1 欄位的對應標籤	連線狀態
cn1	連線狀態	範例：100 • 0：無法連線 • 1：作用中 • 2：離線 • 100：產品作用中 • 101：產品離線，但用戶端作用中 • 102：行動
cn2Label	cn2 欄位的對應標籤	特徵碼/規則
cn2	特徵碼/規則	範例：2048
cs5Label	cs5 欄位的對應標籤	特徵碼/規則版本
cs5	特徵碼/規則版本	範例：1548
cn3Label	cn3 欄位的對應標籤	特徵碼/規則狀態
cn3	特徵碼/規則狀態	範例：1 • 1：最新 • 2：前 1 個版本 • 3：前 2 個版本 • 4：前 3 個版本 • 5：前 4 個版本 • 6：前 5 個版本 • 7：前 6 個或更舊版本
cs6Label	cs6 欄位的對應標籤	AUComponent_Type

CEF 索引鍵	說明	值
cs6	主動式更新元件類型	範例：2 • 2：特徵碼
deviceFacility	受管理產品名稱	範例：Apex One
msg	病毒碼類型顯示名稱	範例："Virus Pattern"
deviceNtDomain	Active Directory 網域	範例：APEXTMCM
dntdom	Apex One 網域階層	範例：OSCEDomain1
ApexCentralHost	Apex Central 主機名稱	範例：TW-CHRIS-W2019
devicePayloadId	唯一訊息 GUID	範例：1C00290C0360-9CDE11EB-D4B8-F51F-C697

記錄檔範例：

```
CEF:0|Trend Micro|Apex Central|2019|800101|Pattern Update
Status|3|rt=Nov 02 2017 12:46:44 GMT+00:00 shost=shost1 cs1L
abel=Operating_System cs1=Windows 7  cs2Label=Product/Endpoi
nt_IP cs2=10.0.7.20 cs3Label=Update_Agent cs3=0 cs4Label=Dom
ain cs4=Default cn1Label=Connection_Status cn1=100 cn2Label=
Pattern/Rule cn2=2048 cs5Label=Pattern/Rule_Version cs5=1548
 cn3Label=Pattern/Rule_Status cn3=1 cs6Label=AUComponent_Typ
e cs6=2 deviceFacility=Apex One deviceNtDomain=APEXTMCM dntd
om=OSCEDomain1
```

CEF Machine Learning 記錄檔

CEF 索引鍵	說明	值
標頭 (logVer)	CEF 格式版本	CEF:0
標頭 (vendor)	產品供應商	Trend Micro
標頭 (pname)	產品名稱	Apex Central

CEF 索引鍵	說明	值
標頭 (pver)	產品版本	2019
標頭 (eventid)	PML：處理行動結果	PML：檔案已清除
標頭 (eventName)	偵測名稱	virusa
標頭 (severity)	嚴重性	3
rt	事件觸發時間 (UTC)	範例：“2018 年 3 月 22 日 08:23:23 GMT+00:00”
dvchost	產品伺服器	範例：Sample_Host
cn1Label	cn1 欄位的對應標籤	ThreatType
cn1	可能的安全威脅類型	範例：35143 如需詳細資訊，請參閱安全威脅類型對應資料表 第 F-60 頁。
cs2Label	cs2 欄位的對應標籤	DetectionName
cs2	安全威脅	範例：Troj.Win32.TRX.XXPE002FF017
shost	中毒端點	範例：10.0.0.1
suser	登入使用者	範例：TREND\\User
cn2Label	cn2 欄位的對應標籤	DetectionType
cn2	偵測類型	範例：0 • 0：檔案 • 1：程序
filePath	檔案路徑	範例：D:\\
fname	檔案名稱	範例：ALCORMP.EXE
deviceCustomDate1	檔案建立時間	範例：2017-04-26 05:53:27.000
sproc	系統程序	範例：notepad.exe

CEF 索引鍵	說明	值
cn4Label	cn4 欄位的對應標籤	ProcessCommandLine
cs4	程序指令	範例：notepad.exe
duser	程序擁有者	範例：user1
app	感染通道	範例：10 • 0：未知 • 1：本機磁碟機 • 2：網路磁碟機 • 3：自動執行檔案 • 10：Web • 11：電子郵件 • 999：本機或網路磁碟機
cs3Label	cs3 欄位的對應標籤	InfectionLocation
cs3	感染來源	範例：http://10.0.0.1/
dst	產品/端點 IPv4 位址	範例：10.0.17.6
c6a3Label	c6a3 欄位的對應標籤	產品/端點 IP
c6a3	產品/端點 IPv6 位址	範例： fd66:5168:9882:6:b5b0:b2b5:4173:3f5d
cn3Label	cn3 欄位的對應標籤	Confidence
cn3	安全威脅可能性	範例：82
act	處理行動結果	範例：21 如需詳細資訊，請參閱處理行動對應資料表 第 F-69 頁。
filehash	檔案 SHA-1	範例： 52c17c785b45ee961f68fb17744276076f383085

CEF 索引鍵	說明	值
dhost	產品實體/端點	範例：dhost1
deviceExternalId	記錄序號	範例：100
deviceFacility	產品	範例：Apex One
原因	嚴重安全威脅類型	範例：E • A：已知的進階持續安全威脅 (APT) • B：社交工程攻擊 • C：弱點攻擊 • D：橫向移動 • E：未知安全威脅 • F：C&C 回呼 • G：勒索軟體
deviceNtDomain	Active Directory 網域	範例：APEXTMCM
dntdom	Apex One 網域階層	範例：OSCEDomain1
TMCMLogDetectedHost	發生記錄事件的端點名稱	範例：MachineHostName
TMCMLogDetectedIP	發生記錄事件的 IP 位址	範例：10.1.2.3
ApexCentralHost	Apex Central 主機名稱	範例：TW-CHRIS-W2019
devicePayloadId	唯一訊息 GUID	範例：1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform	端點作業系統	範例：Windows 7 6.1 (Build 7601) Service Pack 1

記錄檔範例：

```
CEF:0|Trend Micro|Apex Central|2019|PML:File cleaned|Detecti
on01|3|deviceExternalId=1 rt=Dec 01 2018 16:01:00 GMT+00:00
deviceFacility=15 dvchost=OSCE01 cn1Label=ThreatType cn1=1 c
s2Label=DetectionName cs2=Detection01 shost=10.0.0.1 suser=S
```

```
ample_Domain\\Sample_User cn2Label=DetectionType cn2=0 fileP
ath=C:\\test01\\aaa.exe fname=aaa.exe deviceCustomDate1Label
=FileCreationDate deviceCustomDate1=Dec 02 2018 00:01:00 GMT
+00:00 sproc=notepad.exe cs4Label=ProcessCommandLine cs4=not
epad.exe -test duser=admin01 app=1 cs3Label=InfectionLocatio
n cs3=https://10.1.1.1 dst=80.1.1.1 cn3Label=Confidence cn3=
81 act=21 fileHash=177750B65A21A9043105FD0820B85B58CF148A01
dhost=OSCEClient11 reason=E deviceNtDomain=APEXTMCM dntdom=O
SCEDomain1 TMCMLogDetectedHost=OSCEClient11 TMCMLogDetectedI
P=80.1.1.1 ApexCentralHost=TW-CHRIS-W2019 devicePayloadId=1C
00290C0360-9CDE11EB-D4B8-F51F-C697 TMCMdevicePlatform=Windo
ws 7 6.1 (Build 7601) Service Pack 1
```

安全威脅類型對應資料表

值	說明
35140	廣告軟體
35141	後門程式
35142	瀏覽器修改程式
35143	DDoS
35144	惡意撥號程式
35145	弱點攻擊
35146	駭客工具
35147	惡作劇程式
35148	可能不想要的應用程式
35149	勒索軟體
35150	Rootkit
35151	間諜程式
35152	特洛伊木馬程式

值	說明
35153	特洛伊木馬程式點擊程式
35154	特洛伊木馬程式下載程式
35155	特洛伊木馬病毒植入程式
35156	特洛伊木馬程式 Proxy
35157	特洛伊木馬程式間諜程式
35158	檔案感染程式
35159	蠕蟲
35160	開機

CEF 產品稽核事件

CEF 索引鍵	說明	值
標頭 (logVer)	CEF 格式版本	CEF:0
標頭 (vendor)	產品供應商	Trend Micro
標頭 (pname)	產品名稱	Apex Central
標頭 (pver)	產品版本	2019
標頭 (eventid)	事件 ID	1745
標頭 (eventName)	記錄檔名稱	產品稽核事件
標頭 (severity)	嚴重性	3
cat	記錄類型	1745
deviceFacility	受管理的產品	範例：Apex One
dvchost	受管理端點的顯示名稱	範例：localhost

CEF 索引鍵	說明	值
rt	事件觸發時間 (UTC)	範例：“2018 年 3 月 22 日 08:23:23 GMT+00:00”
cn1Label	cn1 欄位的對應標籤	SLF_CategoryID
cn1	類別 ID	範例：536,870,912
cn2Label	"cn2" 欄位的對應標籤	SLF_SeverityLevel
cn2	嚴重性層級	範例：4 • 1 = 錯誤 • 2 = 警告 • 4 = 資訊 • 16 = 故障稽核
suser	遭遇事件發生的使用者名稱	範例："administrator"
deviceNtDomain	Active Directory 網域	範例：APEXTMCM
dntdom	Apex One 網域階層	範例：OSCEDomain1
ApexCentralHost	Apex Central 主機名稱	範例：TW-CHRIS-W2019
devicePayloadId	唯一訊息 GUID	範例：1C00290C0360-9CDE11EB-D4B8-F51F-C697

記錄檔範例：

```
CEF:0|Trend Micro|Apex Central|2019|Delete|1009490 - Block A
dministrative Share - 1 (ATT&CK T1077,T1105)|3|rt=Apr 20 202
0 03:33:15 GMT+00:00 dvchost=OSCEClient22 deviceFacility=Ape
x One act=Delete, src=10.1.1.8 dst=80.1.1.8 smac=54-BF-64-84
-7F-08 spt=88 dmac=54-BF-64-84-7F-18 dpt=448 cn2Label=SLF_Is
DetectionOnly cn2=1 deviceDirection=Outbound cn3Label=SLF_Ra
nk cn3=100 cn4Label=SLF_SeverityCode cn4=4 proto=10008 cs2La
bel=SLF_ConnectionType cs2=Suspicious Client Application Act
ivity cn1Label=SLF_RuleID cn1=1009490 cs1Label=SLF_RuleConte
nt cs1=1009490 - Block Administrative Share - 1 (ATT&CK T107
7,T1105) cnt=1 deviceNtDomain=APEXTMCM dntdom=OSCEDomain1
```

CEF 沙盒偵測記錄檔

注意

沙盒偵測記錄檔在 Apex Central 主控台上稱為「沙箱偵測」。

CEF 索引鍵	說明	值
標頭 (logVer)	CEF 格式版本	CEF:0
標頭 (vendor)	裝置供應商	Trend Micro
標頭 (pname)	裝置產品	Apex Central
標頭 (pver)	裝置版本	2019
標頭 (eventid)	裝置事件類別識別碼	VAD
標頭 (eventName)	事件名稱	沙箱偵測名稱
標頭 (severity)	嚴重性	3
deviceExternalId	識別碼	範例：2
rt	事件觸發時間 (UTC)	範例：“2018 年 3 月 22 日 08:23:23 GMT+00:00”
deviceFacility	產品	範例：Apex One
dvchost	伺服器名稱	範例：OSCE01
dhost	端點名稱	範例：Isolate-ClientA
dst	端點 IPv4 位址	範例：10.0.17.6
c6a3	端點 IPv6 位址	範例：fe80::38ca:cd15:443c:40bb%11
app	項目通道	範例：0 如需詳細資訊，請參閱通訊協定對應資料表 第 F-89 頁
sourceServiceName	來源	範例：Test1@tmcm.extbeta.com

CEF 索引鍵	說明	值
destinationServiceName	目標	範例：Test2@tmcm.extbeta.com;Test3@tmcm.extbeta.com
sproc	程序名稱	範例：VA
fileHash	檔案 SHA-1 雜湊	範例：D6712CAE5EC821F910E14945153AE7871AA536CA
fname	檔案名稱	範例：C:\\\\QA_Log.zip
要求	URL	範例：http://127.1.1.1
cs1	沙箱所判斷出的安全威脅名稱	範例：VAN_RANSOMWARE.umxxhelloransom_abc
cn1	顯示沙箱指派的風險等級	範例：0 • 0：無風險 • 1：低度風險 • 2：中度風險 • 3：高度風險 • 9999：未知
cs2	顯示安全威脅類型	範例：Anti-security, self-preservation

CEF 索引鍵	說明	值
cs3	雲端儲存供應商	範例：Google Drive • Dropbox • Box • Google 雲端硬碟 • Microsoft OneDrive • SugarSync • Hightail • Evernote • Microsoft Exchange Online • Microsoft SharePoint Online • 未知 • 無
原因	嚴重安全威脅類型	範例：E • A：已知的進階持續安全威脅 (APT) • B：社交工程攻擊 • C：弱點攻擊 • D：橫向移動 • E：未知安全威脅 • F：C&C 回呼 • G：勒索軟體
deviceNtDomain	Active Directory 網域	範例：APEXTMCM
dntdom	Apex One 網域階層	範例：OSCEDomain1
TMCMLogDetectedHost	發生記錄事件的端點名稱	範例：MachineHostName
TMCMLogDetectedIP	發生記錄事件的 IP 位址	範例：10.1.2.3

CEF 索引鍵	說明	值
ApexCentralHost	Apex Central 主機名稱	範例：TW-CHRIS-W2019
devicePayloadId	唯一訊息 GUID	範例：1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform	端點作業系統	範例：Windows 7 6.1 (Build 7601) Service Pack 1

記錄檔範例：

```
CEF: 0|Trend Micro|Apex Central|2019|VAD|VAN_RANSOMWARE.um
xxhelloransom_abc|3|deviceExternalId=2 rt=Mar 22 2018 08:23:
23 GMT+00:00 deviceFacility=Apex One dvchost=OSCE01 dhost=
Isolate-ClientA dst=0.0.0.0 app=1 sourceServiceNameTest1@tre
nd.com.tw destinationServiceName=Test2@tmcm.extbeta.com;Test
3@tmcm.extbeta.com sproc=VA fileHash=3395856CE81F2B7382DEE72
602F798B642F14140 fname=C:\\\\QA_Log.zip request=http://127.
1.1.1 cs1Label=Security_Threat cs1=VAN_RANSOMWARE.umxxhellor
ansom_abc cn1Label=Risk_Level cn1=0 cs2Label=Threat_Categori
es cs2=Anti-security, self-preservation cs3Label=Cloud_Servi
ce_Vendor cs3=Google Drive reason=E deviceNtDomain=APEXTMCM
dntdom=OSCEDomain1 TMCMLogDetectedHost=OSCEClient TMCMLogDe
tectedIP=0.0.0.0 ApexCentralHost=TW-CHRIS-W2019 devicePaylo
adId=1C00290C0360-9CDE11EB-D4B8-F51F-C697 TMCMdevicePlatfor
m=Windows 7 6.1 (Build 7601) Service Pack 1
```

CEF 間諜程式/可能的資安威脅程式記錄檔

CEF 索引鍵	說明	值
標頭 (logVer)	CEF 格式版本	CEF:0
標頭 (vendor)	裝置供應商	Trend Micro
標頭 (pname)	裝置產品	Apex Central
標頭 (pver)	裝置版本	2019

CEF 索引鍵	說明	值
標頭 (eventid)	裝置事件類別識別碼	偵測到間諜程式
標頭 (eventName)	事件名稱	偵測到間諜程式
標頭 (severity)	嚴重性	3
cnt	偵測數目	範例：10
rt	事件觸發時間 (UTC)	範例：“2018 年 3 月 22 日 08:23:23 GMT+00:00”
cn1Label	cn1 欄位的對應標籤	範例：特徵碼類型
cn1	特徵碼類型	範例：1073741840
cs1Label	cs1 欄位的對應標籤	範例：病毒名稱
cs1	間諜程式/可能的資安威脅程式	範例：ADW_OPENCANDY
cs2Label	cs2 欄位的對應標籤	範例：引擎版本
cs2	引擎版本	範例：6.2.3027
cs5Label	cs5 欄位的對應標籤	範例：處理行動結果
cs5	處理行動	範例：成功將系統重新開機 如需詳細資訊，請參閱處理行動對應資料表 第 F-69 頁。
cs6Label	cs6 欄位的對應標籤	範例：特徵碼版本
cs6	特徵碼版本	範例：1297
cat	記錄類型	範例：1727
dvchost	端點主機名稱	範例：ApexOneClient01
deviceExternalId	識別碼	範例：3
fname	資源	範例：F:\\Malware\\psas\\rsrc2.bin
filePath	資源	範例：F:\\Malware\\psas\\rsrc2.bin

CEF 索引鍵	說明	值
dhost	端點主機名稱	範例：ApexOneClient01
dst	端點 IPv4 位址	範例：50.8.1.1
c6a3Label	c6a3 欄位的對應標籤	範例：SLP_DestinationIP
c6a3	端點 IPv6 位址	範例：fe80::38ca:cd15:443c:40bb%11
fileHash	檔案 SHA-1	範例：D6712CAE5EC821F910E14945153AE7871AA536CA
deviceFacility	產品	範例：Apex One
duser	使用者名稱	範例：Admin004
cn2Label	cn2 欄位的對應標籤	範例：Scan_Type
cn2	掃瞄類型	範例：立即掃瞄 如需詳細資訊，請參閱間諜程式/可能的資安威脅程式掃瞄類型對應資料表 第 F-72 頁。
cn3Label	cn3 欄位的對應標籤	範例：Security_Threat_Type
cn3	安全威脅類型	範例：廣告軟體 如需詳細資訊，請參閱間諜程式/可能的資安威脅程式風險類型對應資料表 第 F-73 頁。
deviceNtDomain	Active Directory 網域	範例：APEXTMCM
dntdom	Apex One 網域階層	範例：OSCEDomain1
TMCMLogDetectedHost	發生記錄事件的端點名稱	範例：MachineHostName
TMCMLogDetectedIP	發生記錄事件的 IP 位址	範例：10.1.2.3
ApexCentralHost	Apex Central 主機名稱	範例：TW-CHRIS-W2019

CEF 索引鍵	說明	值
devicePayloadId	唯一訊息 GUID	範例：1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform	端點作業系統	範例：Windows 7 6.1 (Build 7601) Service Pack 1

記錄檔範例：

```
CEF:0|Trend Micro|Apex Central|2019|Spyware Detected|Spywa
re Detected|3|deviceExternalId=3 rt=Oct 06 2017 08:39:46 GMT
+00:00 cnt=1 dhost=ApexOneClient01 cn1Label=PatternType cn1=
1073741840 cs1Label=VirusName cs1=ADW_OPENCANDY cs2Label=Eng
ineVersion cs2=6.2.3027 cs5Label=ActionResult cs5=Reboot sys
tem successfully cs6Label=PatternVersion cs6=1297 cat=1727 d
vchost=ApexOneClient01 fname=F:\\Malware\\psas\\rsrc2.bin fi
lePath=F:\\Malware\\psas\\rsrc2.bin dst=50.8.1.1 deviceFacil
ity=Apex One deviceNtDomain=APEXTMCM dntdom=OSCEDomain1 TMCM
LogDetectedHost=ApexOneClient01 TMCMLogDetectedIP=50.8.1.1
ApexCentralHost=TW-CHRIS-W2019 devicePayloadId=1C00290C0360-
9CDE11EB-D4B8-F51F-C697 TMCMdevicePlatform=Windows 7 6.1 (Bu
ild 7601) Service Pack 1
```

處理行動對應資料表

值	說明
0	未知
1	無
21	檔案已清除
22	檔案已刪除
23	檔案已隔離
24	檔案已重新命名

值	說明
25	檔案暫不處理
26	無法清除檔案。暫不處理
27	無法清除檔案。檔案已刪除
28	無法清除檔案。檔案已重新命名
29	無法清除檔案。檔案已隔離
31	無法清除檔案。檔案已刪除
32	檔案已取代
34	檔案已封存
35	已成功封鎖
36	已成功隔離
37	已成功將其他資訊新增到電子郵件內文
38	檔案已上傳
39	無法清除檔案。檔案已隔離
40	無法清除檔案。暫不處理
41	拒絕存取
42	無處理行動
43	系統已重新啟動
44	清除間諜程式/可能的資安威脅程式對系統有不良影響
45	已成功手動停止掃瞄
46	已成功重新導向郵件以供核准
81	已加密
121	無法清除檔案
122	無法刪除檔案

值	說明
123	無法隔離檔案
124	無法重新命名檔案
125	無法暫不處理檔案
126	無法清除或暫不處理檔案
127	無法清除或刪除檔案
128	無法清除或重新命名檔案
129	無法清除或隔離檔案
130	無法刪除附件
131	無法清除或刪除附件
132	下列其中一項： • 無法取代檔案內容 • 附件名稱與一項內容規則相符，因此變更了附件名稱
134	無法封存檔案
135	無法封鎖檔案
136	無法隔離檔案
137	無法將其他資訊新增到電子郵件內文
138	無法上傳檔案
139	無法清除或隔離檔案
140	無法清除或暫不處理檔案
141	無法拒絕存取
142	無法執行無處理行動
143	需要採取處理行動 — 請重新啟動端點以完成安全威脅清除
144	未定義

值	說明
145	無法手動停止掃瞄
146	無法重新導向郵件以供核准
201	需要採取處理行動 — 請執行完整系統掃瞄
202	需要採取處理行動 — 請使用 OfficeScan 中的 "Rescue Disk" 工具
203	需要採取處理行動 — 請使用 OfficeScan 工具箱中的 "Rootkit Buster" 工具來移除此安全威脅。如果此問題持續發生，請洽詢支援人員
204	需要採取處理行動 — 請使用 OfficeScan 工具箱中的 "Clean Boot" 工具來移除此安全威脅。如果此問題持續發生，請洽詢支援人員

間諜程式/可能的資安威脅程式掃瞄類型對應資料表

值	說明
0	未知
1	無
11	即時掃瞄
12	手動掃瞄
13	預約掃瞄
14	即時郵件掃瞄
15	即時資料庫掃瞄
16	立即掃瞄
17	卡掃瞄
18	損害清除及復原服務
19	儲存裝置掃瞄

間諜程式/可能的資安威脅程式風險類型對應資料表

值	說明
0	未知
1	追蹤軟體
2	廣告軟體
3	Cookie
4	惡意撥號程式
5	低安全性
6	一般
7	按鍵記錄程式
8	特洛伊木馬程式
9	可疑
10	綁架軟體
11	寄生蟲
12	瀏覽器輔助工具 (BHO)
13	LSP
15	URL 捷徑
16	對等式應用程式
17	蠕蟲
19	下載程式
20	病毒
21	EULAware
22	變種

值	說明
23	中等安全性
24	高安全性
25	安全弱點評估

CEF 可疑檔案記錄檔

CEF 索引鍵	說明	值
標頭 (logVer)	CEF 格式版本	CEF:0
標頭 (vendor)	裝置供應商	Trend Micro
標頭 (pname)	裝置產品	Apex Central
標頭 (pver)	裝置版本	2019
標頭 (eventid)	FH：處理行動	FH：記錄
標頭 (eventName)	名稱	可疑檔案
標頭 (severity)	嚴重性	3
deviceExternalId	識別碼	範例：1
cat	記錄類型	範例：1766
deviceFacility	產品	範例：Apex One
cn1Label	cn1 欄位的對應標籤	範例：SLF_ProductVersion
cn1	產品版本	範例：11
rt	事件觸發時間 (UTC)	範例：“2018 年 3 月 22 日 08:23:23 GMT+00:00”
dst	端點 IPv4 位址	範例：10.201.86.151
c6a3Label	c6a3 欄位的對應標籤	範例：端點 IPv6 位址

CEF 索引鍵	說明	值
c6a3	端點 IPv6 位址	範例：2620:101:4003:7a0:fd4b:52ed:53bd:ae3d
dhost	端點主機名稱	範例：APEX-ONE-CLIENT-1
cs2Label	cs2 欄位的對應標籤	範例：SLF_TrueFileType
cs2	檔案類型	範例：文字
fileHash	檔案 SHA-1	範例：D6712CAE5EC821F910E14945153AE7871AA536CA
cs3Label	cs3 欄位的對應標籤	範例：SLF_FileSource
cs3	檔案路徑	範例：C:\\Users\\Administrator\\Desktop\\BT-SHA1-SAMPLE\\BT-SHA1-SAMPLE\\017545113A434757C5F0F13095DBBF138BD76A40;0x36D572AE
cn2Label	cn2 欄位的對應標籤	範例：SLF_SourceType
cn2	C&C 清單來源	範例：0 • 0：沙盒 • 1：使用者定義
act	處理行動	範例：記錄 • 1：記錄 • 2：封鎖 • 3：隔離
cn3Label	cn3 欄位的對應標籤	範例：SLF_ScanType

CEF 索引鍵	說明	值
cn3	掃瞄類型	範例：1 • 1：預約掃瞄 • 2：手動掃瞄 • 3：立即掃瞄 • 4：即時掃瞄
原因	嚴重安全威脅類型	範例：E • A：已知的進階持續安全威脅 (APT) • B：社交工程攻擊 • C：弱點攻擊 • D：橫向移動 • E：未知安全威脅 • F：C&C 回呼 • G：勒索軟體
deviceNtDomain	Active Directory 網域	範例：APEXTMCM
dntdom	Apex One 網域階層	範例：OSCEDomain1
TMCMLogDetectedHost	發生記錄事件的端點名稱	範例：MachineHostName
TMCMLogDetectedIP	發生記錄事件的 IP 位址	範例：10.1.2.3
ApexCentralHost	Apex Central 主機名稱	範例：TW-CHRIS-W2019
devicePayloadId	唯一訊息 GUID	範例：1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform	端點作業系統	範例：Windows 7 6.1 (Build 7601) Service Pack 1

記錄檔範例：

```
CEF:0|Trend Micro|Apex Central|2019|FH:Log|Suspicious File
s|3|deviceExternalId=1 rt=Nov 15 2016 02:47:21 GMT+00:00 cat
=1766 deviceFacility=Apex One cn1Label=SLF_ProductVersion cn
1=11 dst=10.201.86.151 dhost=APEX-ONE-CLIENT-1 cs2Label=SLF_
TrueFileType cs2=SLF_TrueFileType fileHash=D6712CAE5EC821F91
0E14945153AE7871AA536CA cs3Label=SLF_FileSource cs3=C:\\User
s\\Administrator\\Desktop\\BT-SHA1-SAMPLE\\BT-SHA1-SAMPLE\\0
17545113A434757C5F0F13095DBBF138BD76A40;0x36D572AE cn2Label=
SLF_SourceType cn2=0 act=Log cn3Label=SLF_ScanType cn3=1 rea
son=E deviceNtDomain=APEXTMCM dntdom=OSCEDomain1 TMCMLogDete
ctedHost=APEX-ONE-CLIENT-1 TMCMLogDetectedIP=10.201.86.151
ApexCentralHost=TW-CHRIS-W2019 devicePayloadId=1C00290C0360-
9CDE11EB-D4B8-F51F-C697 TMCMdevicePlatform=Windows 7 6.1 (Bu
ild 7601) Service Pack 1
```

CEF 病毒/惡意程式記錄檔

CEF 索引鍵	說明	值
標頭 (logVer)	CEF 格式版本	CEF:0
標頭 (vendor)	裝置供應商	Trend Micro
標頭 (pname)	裝置產品	Apex Central
標頭 (pver)	裝置版本	2019
標頭 (eventid)	AV：處理行動	AV：檔案已重新命名
標頭 (eventName)	病毒/惡意程式名稱	JS_EXPLOIT.SMDN
標頭 (severity)	嚴重性	3
cnt	偵測	範例：10
dhost	端點	範例：ApexOneClient01
duser	使用者	範例：Admin004

CEF 索引鍵	說明	值
act	處理行動	範例：檔案已重新命名 如需詳細資訊，請參閱處理行動對應資料表 第 F-69 頁。
rt	記錄檔產生時間 (UTC)	範例：2017 年 10 月 6 日 08:39:46 GMT+ 00:00
cn1Label	cn1 欄位的對應標籤	範例：VLF_PatternNumber
cn1	特徵碼/規則版本	範例：920500
cn2Label	cn2 欄位的對應標籤	範例：VLF_SecondAction
cn2	第二個處理行動	範例：3 如需詳細資訊，請參閱第二個處理行動對應資料表 第 F-81 頁。
cs1Label	cs1 欄位的對應標籤	範例：VLF_FunctionCode
cs1	掃瞄類型	範例：手動掃瞄 • 0：未知 • 1：無 • 11：即時掃瞄 • 12：手動掃瞄 • 13：預約掃瞄 • 16：立即掃瞄 • 17：卡掃瞄 • 18：損害清除及復原服務 • 19：儲存裝置掃瞄
cs2Label	cs2 欄位的對應標籤	範例：VLF_EngineVersion
cs2	引擎版本	範例：9.500.1005
cs3Label	cs3 欄位的對應標籤	範例：CLF_ProductVersion

CEF 索引鍵	說明	值
cs3	產品版本	範例：11
cs4Label	cs4 欄位的對應標籤	範例：CLF_ReasonCode
cs4	原因代碼	範例：病毒記錄檔
cs5Label	cs5 欄位的對應標籤	範例：VLF_FirstActionResult
cs5	第一個處理行動結果	範例：無法清除檔案 如需詳細資訊，請參閱處理行動對應資料表 第 F-69 頁。
cs6Label	cs6 欄位的對應標籤	範例：第二個處理行動結果
cs6	第二個處理行動結果	範例：無法清除檔案。“”暫不處理 如需詳細資訊，請參閱處理行動對應資料表 第 F-69 頁。
cat	記錄類型	範例：1703
dvchost	產品伺服器名稱	範例：ApexOneServer01
cn3Label	cn3 欄位的對應標籤	範例：CLF_SeverityCode
cn3	嚴重性代碼	範例：2 • 0：未知 • 1：資訊 • 2：警告 • 3：錯誤 • 4：嚴重
deviceExternalId	識別碼	範例：3
fname	檔案	範例：FakeMalwareRebootDel.exe

CEF 索引鍵	說明	值
filePath	檔案路徑	範例：C:\\Users\\ADMINI~1\\AppData\\Local\\Temp\\Rar$DR01.046\\
msg	壓縮檔中的檔案	範例：BMAC Schedule of Events.xls
shost	來源主機、UNC 或電子郵件信箱 **注意** 系統可能不會將此金鑰納入在記錄檔中。	範例：“xxx@test.com”
dst	端點 IPv4 位址	範例：50.8.1.1
c6a3Label	c6a3 欄位的對應標籤	範例：SLP_DestinationIP
c6a3	端點 IPv6 位址	範例：fe80::38ca:cd15:443c:40bb%11
fileHash	檔案 SHA-1	範例：D6712CAE5EC821F910E14945153AE7871AA536CA
deviceFacility	產品	範例：Apex One
原因	嚴重安全威脅類型	範例：E • A：已知的進階持續安全威脅 (APT) • B：社交工程攻擊 • C：弱點攻擊 • D：橫向移動 • E：未知安全威脅 • F：C&C 回呼 • G：勒索軟體
deviceNtDomain	Active Directory 網域	範例：APEXTMCM

CEF 索引鍵	說明	值
dntdom	Apex One 網域階層	範例：OSCEDomain1

記錄檔範例：

```
CEF:0|Trend Micro|Apex Central|2019|AV:File renamed|JS_EXP
LOIT.SMDN|3|deviceExternalId=104 rt=Feb 18 2016 14:34:00 G
MT+00:00 cnt=1 dhost=ApexOneClient01 duser=Admin004 act=Fi
le renamed cn1Label=VLF_PatternNumber cn1=920500 cn2Label=
VLF_SecondAction cn2=3 cs1Label=VLF_FunctionCode cs1=Manua
l Scan cs2Label=VLF_EngineVersion cs2=9.500.1005 cs3Label=
CLF_ProductVersion cs3=10.6 cs4Label=CLF_ReasonCode cs4=vi
rus log cs5Label=VLF_FirstActionResult cs5=File renamed cs
6Label=VLF_SecondActionResult cs6=N/A cat=1703 dvchost=Ape
xOneServer01 cn3Label=CLF_ServerityCode cn3=2 fname=0348C6
93056617D34FC5B5BAB4643885FEE5FEDF;0xD5D56AC2 filePath=C:\
\Users\\Administrator\\Desktop\\trend_test_virus\\Trojans\
\ msg=BMAC Schedule of Events.xls shost=xxx@test.com dst=1
0.201.129.24 devic eFacility=Apex One reason=B deviceNtDom
ain=APEXTMCM dntdom=O SCEDomain1 ApexCentralHost=TW-CHRIS-
W2019 devicePayloadId=1C00290C0360-9CDE11EB-D4B8-F51F-C697
```

第二個處理行動對應資料表

值	說明
0	未知
1	無
2	清除
3	刪除
4	移動
5	重新命名
6	暫不處理/記錄

值	說明
7	清除巨集
8	丟棄
9	隔離
10	插入/取代
11	封存
12	加上戳記
13	封鎖
14	重新導向郵件以供核准
81	已加密
90	偵測
257	重設

CEF Web 網頁安全記錄檔

CEF 索引鍵	說明	值
標頭 (logVer)	CEF 格式版本	CEF:0
標頭 (vendor)	裝置供應商	Trend Micro
標頭 (pname)	裝置產品	Apex Central
標頭 (pver)	裝置版本	2019
標頭 (eventid)	WB：過濾/封鎖類型	WB：1
標頭 (eventName)	封鎖規則或過濾/封鎖類型	5
標頭 (severity)	嚴重性	3

CEF 索引鍵	說明	值
app	通訊協定	範例：3 如需詳細資訊，請參閱通訊協定對應資料表 第 F-89 頁。
cnt	偵測	範例：10
dpt	伺服器通訊埠	範例：80
act	處理行動	範例：0 • 0：未知 • 1：暫不處理 • 2：封鎖 • 3：監控 • 4：刪除 • 5：隔離 • 6：警告 • 7：警告並繼續 • 8：覆寫
rt	事件觸發時間 (UTC)	範例：“2018 年 3 月 22 日 08:23:23 GMT+00:00”
src	端點 IPv4 位址	範例：10.1.128.34
c6a2Label	c6a2 欄位的對應標籤	範例：SLF_SourceIP
c6a2	端點 IPv6 位址	範例：2620:101:4003:7a0:fd4b:52ed:53bd:ae3d
cs1Label	cs1 欄位的對應標籤	範例：SLF_PolicyName
cs1	策略	範例：外部使用者策略
cs4Label	cs4 欄位的對應標籤	範例：CLF_ReasonCode
cs4	原因代碼	範例：存取

CEF 索引鍵	說明	值
cs5Label	cs5 欄位的對應標籤	範例：CLF_ReasonCodeSource
cs5	原因代碼來源	範例：Web
deviceDirection	流量/連線	範例：2 • 0：無 • 1：輸入 • 2：輸出
cat	過濾/封鎖類型	範例：7 如需詳細資訊，請參閱過濾/封鎖類型對應資料表 第 F-86 頁。
dvchost	端點主機名稱	範例：ApexOneClient08
cn1Label	cn1 欄位的對應標籤	範例：CLF_SeverityCode
cn1	嚴重性代碼	範例：0 • 0：未知 • 1：資訊 • 2：警告 • 3：錯誤 • 4：嚴重
deviceExternalId	識別碼	範例：38
fname	檔案	範例：test.txt
要求	URL	範例：http://www.violetsoft.net/counter/insert.php?dbserver\=db1&c_pcode\=25&c_pid\=funpop1&c_kind\=4&c_mac\=FE-ED-BE-EF-0C-E1
deviceFacility	產品	範例：Apex One
duser	使用者名稱	範例：Admin004

CEF 索引鍵	說明	值
shost	用戶端主機名稱	範例：ABC-HOST-WKS12
cs2Label	cs2 欄位的對應標籤	範例：Blocking_Rule
cs2	封鎖規則	範例：內容過濾器
deviceProcessName	程序名稱	範例：C:\\Windows\ \system32\ \svchost-1.exe
cn3Label	cn3 欄位的對應標籤	範例：ReputationScore
cn3	信譽評等評分	範例：49
dst	伺服器 IP 位址	範例：10.69.81.64
cn2Label	cn2 欄位的對應標籤	範例：SLF_SeverityLevel
cn2	嚴重性層級	範例：100 • 100：高 • 300：中高 • 500：中度 • 700：中低 • 900：低
原因	嚴重安全威脅類型	範例：E • A：已知的進階持續安全威脅 (APT) • B：社交工程攻擊 • C：弱點攻擊 • D：橫向移動 • E：未知安全威脅 • F：C&C 回呼 • G：勒索軟體
deviceNtDomain	Active Directory 網域	範例：APEXTMCM

CEF 索引鍵	說明	值
dntdom	Apex One 網域階層	範例：OSCEDomain1
TMCMLogDetectedHost	發生記錄事件的端點名稱	範例：MachineHostName
TMCMLogDetectedIP	發生記錄事件的 IP 位址	範例：10.1.2.3
ApexCentralHost	Apex Central 主機名稱	範例：TW-CHRIS-W2019
devicePayloadId	唯一訊息 GUID	範例：1C00290C0360-9CDE11EB-D4B8-F51F-C697
TMCMdevicePlatform	端點作業系統	範例：Windows 7 6.1 (Build 7601) Service Pack 1

記錄檔範例：

```
CEF:0|Trend Micro|Apex Central|2019|WB:7|7|3|deviceExterna
lId=38 rt=Nov 15 2017 08:43:57 GMT+00:00 app=17 cntLabel=Agg
regatedCount cnt=1 dpt=80 act=1 src=10.1.128.46 cs1Label=SLF
_PolicyName cs1=External User Policy deviceDirection=2 cat=7
 dvchost=ApexOneClient08 fname=test.txt request=http://www.v
ioletsoft.net/counter/insert.php?dbserver\=db1&c_pcode\=25&c
_pid\=funpop1&c_kind\=4&c_mac\=FE-ED-BE-EF-0C-E1 deviceFacil
ity=Apex One shost=ABC-HOST-WKS12 reason=G deviceNtDomain=AP
EXTMCM dntdom=OSCEDomain1 TMCMLogDetectedHost=ABC-HOST-WKS12
TMCMLogDetectedIP=10.1.128.46 ApexCentralHost=TW-CHRIS-W2019
devicePayloadId=1C00290C0360-9CDE11EB-D4B8-F51F-C697 TMCMdev
icePlatform=Windows 7 6.1 (Build 7601) Service Pack 1
```

過濾/封鎖類型對應資料表

值	說明
0	未知
1	檔案名稱

值	說明
2	網路郵件網站
3	Web 伺服器
4	URL 特徵碼
5	Java/VB 程序檔
6	真實檔案類型
7	使用者定義
8	伺服器定義
9	Web 策略
11	網路釣魚
12	網路釣魚/間諜程式/可能的資安威脅程式
13	網路釣魚/病毒/惡意程式共犯
14	網路釣魚/偽造簽章
15	網路釣魚/惡意媒介
16	網路釣魚/惡意 Applet
17	網路釣魚信譽評等
20	IP 轉譯策略
21	Java 掃瞄策略
22	惡意行動程式碼策略
31	網址嫁接
32	URL 封鎖
33	URL 過濾
34	用戶端 IP 封鎖
35	目標通訊埠封鎖

值	說明
36	網站信譽評等服務
41	不支援的檔案類型
42	超過檔案總數上限
43	超過檔案大小上限
44	超過解壓縮層數上限
45	超過解壓縮時間範圍
46	超過壓縮比率上限
47	密碼保護的檔案
48	受限制的間諜程式/可能的資安威脅程式類型
60	字串特徵碼
70	HTTP 檢測
-1	病毒/惡意程式
-2	間諜程式/可能的資安威脅程式
-3	網路病毒
-4	IntelliTrap
-5	可疑病毒/惡意程式
-6	可疑間諜程式/可能的資安威脅程式
-7	詐騙
-8	可疑行為

通訊協定對應資料表

值	說明
0	未知
1	SMTP
2	POP3
3	IRC
4	DNS 回應
5	HTTP
6	FTP
7	TFTP
8	SMB
9	Windows Live Messenger (MSN)
10	AIM
11	Yahoo!Messenger
12	Gmail
13	Yahoo!郵件
14	Windows Live Hotmail
15	RDP
16	DHCP
17	Telnet
18	LDAP
19	檔案傳輸
20	SSH

值	說明
21	Dameware
22	VNC
23	Cisco Telnet
24	Kerberos
25	DCE RPC
26	SQL
27	pcAnywhere
28	ICMP
29	SNMP
30	病毒碼 TCP
31	病毒碼 UDP
32	HTTPS
33	SMB2
34	MMS
35	IMAP4
36	RADIUS
37	Radmin
38	FTP_Response
48	RTSP/RTP-UDP
49	RTSP/RTP-TCP
50	RTSP/RDT-UDP
51	RTSP/RDT-TCP
52	WMSP

值	說明
53	SHOUTCast
54	RTMP
68	DNS 要求
256	BitTorrent
257	Kazaa
258	Limewire
259	Bearshare
260	Bluester
261	Edonkey Emule
262	Edonkey2000
263	Filezilla
264	Guncleus
265	Gnutella
266	Winny
267	Napster
268	Morpheus
269	Napster
270	Shareaza
271	WinMX
272	Mldonkey
273	Direct Connect
274	Soulseek
275	OpenAP

值	說明
276	Kuro
277	Imesh
278	Skype
279	Google Talk
317	Cabos
318	Zultrax
319	Foxy
320	eDonkey
321	Ares
322	Miranda
323	Kceasy
324	MoodAmp
325	Deepnet Explorer
326	FreeWire
327	Gimme
328	GnucDNA GWebCache
329	Jubster
330	MyNapster
331	Nova GWebCache
332	Swapper GWebCache
333	Xnap
334	Xolox
335	Ppstream

值	說明
640	AIM Express
641	Chikka SMS Messenger
642	eBuddy
643	ICQ2Go
644	ILoveIM Web Messenger
645	IMUnitive
646	Mabber
647	Meebo
648	Yahoo!Web Messenger
848	SIP2
1024	GPass
10001	IP
10002	ARP
10003	TCP
10004	UDP
10005	IGMP
60	ORACLE
44	MySQL
520	MSSQL
337	Postgres
41	ICMPv6
10006	GGP
10007	PUP

值	說明
10008	IDP
10009	ND
10010	RAW

索引

符號

「使用網域認證登入」按鈕, 2-7

A

Active Directory
- 手動同步處理, 6-2
- 同步處理頻率, 6-2
- 回報層級, 6-13
- 站台, 6-11
- 連線問題疑難排解, 6-5
- 連線設定, 6-2
- 整合, 6-2

Apex Central, 1-2, 1-7
- MCP, 1-7
- SQL 資料庫, 1-7
- Web-based 管理主控台, 1-7
- Web 伺服器, 1-7
- Web 服務整合, 1-7
- Widget 架構, 1-7
- 使用授權資訊, 5-2
- 受管理的產品, 10-2
- 啟動, 5-2
- 產品目錄, 10-2
- 報告伺服器, 1-7
- 郵件伺服器, 1-7
- 資料庫資料表, 24-4
- 關於, 1-2

Apex Central 伺服器
- Web 主控台, 2-2, 2-3

Apex One
- Security Agent, 9-2

Apex One (Mac)
- Security Agent, 9-2

C

CEF syslog 對應
- C&C 回呼, F-14
- Endpoint Application Control, F-42
- Machine Learning, F-56
- Web 安全, F-82
- 入侵防護記錄檔, F-46
- 內容安全, F-19
- 引擎更新狀態, F-44
- 可疑檔案, F-74
- 行為監控, F-9
- 攻擊發現偵測, F-3
- 沙盒偵測記錄檔, F-63
- 沙箱, F-63
- 受管理的產品登入/登出事件, F-49
- 特徵碼更新狀態, F-54
- 病毒/惡意程式, F-77
- 產品稽核事件, F-61
- 間諜程式/可能的資安威脅程式, F-66
- 裝置存取控制, F-35
- 資料外洩防護, F-27
- 網路內容檢測, F-51

Control Manager, 1-1
- 通知, 16-3
- 關於, 1-1

D

DBConfig 工具, 25-2

DLP, 14-14

DLP 事件檢閱者, 18-6
- 事件資訊清單, 18-6

M

Managed Detection and Response
- 工作追蹤, 21-12

安全威脅調查中心工作, 21-10
自動化的分析, 21-14
指令追蹤, 21-15
等待中的工作, 21-6
Managed Detection and Response 服務
暫停, 21-3, 21-6
繼續, 21-3, 21-6
Managed Detection and Response 的安全威脅調查中心用戶端, 21-19
MCP, 1-7
MIB 檔案
Apex Central, E-2
NVW Enforcer SNMPv2, E-2

P

PCRE, 14-17
Perl Compatible Regular Expressions, 14-17
Proxy 伺服器設定
Syslog 轉送, 11-11
元件更新, 11-11
使用授權更新, 11-11
受管理的伺服器清單, 8-8

S

Security Agent, 9-5
Apex One, 9-2
Apex One (Mac), 9-2
Windows 10, 9-6
Windows 7, 9-4
Windows 8.1, 9-5
Windows HPC Server 2008 R2, 9-10
Windows MultiPoint Server 2010, 9-11
Windows MultiPoint Server 2011, 9-12
Windows MultiPoint Server 2012, 9-18
Windows Server 2008 R2, 9-8
Windows Server 2012, 9-14
Windows Server 2012 R2, 9-15
Windows Server 2012 容錯移轉叢集, 9-18, 9-19
Windows Server 2016, 9-21
Windows Server 2016 容錯移轉叢集, 9-22
Windows Server 2019, 9-24
Windows Storage Server 2008 R2, 9-9
Windows Storage Server 2012, 9-16
Windows Storage Server 2012 R2, 9-17
Windows Storage Server 2016, 9-22
下載, 9-2
Small Network Management Protocol
請參閱 SNMP, 16-3
SNMP, 16-3
SSO, 8-3, 10-3
Syslog 設定, 15-17
設定, 15-13, 15-16
Syslog 轉送, 15-17
Proxy 伺服器設定, 11-11
啟動, 15-13
關閉, 15-16

U

users
編輯帳號, 4-9

W

Web 主控台, 2-2, 2-3
登出, 2-7
Widget, 3-2

wildcards（萬用字元）, 14-21
檔案屬性, 14-21
Windows 10, 9-6
Windows 7, 9-4
Windows 8.1, 9-5
Windows HPC Server 2008 R2, 9-10
Windows MultiPoint Server 2010, 9-11
Windows MultiPoint Server 2011, 9-12
Windows MultiPoint Server 2012, 9-18
Windows Server 2008 R2, 9-8
Windows Server 2012, 9-14
Windows Server 2012 R2, 9-15
Windows Server 2012 容錯移轉叢集, 9-18, 9-19
Windows Server 2016, 9-21
Windows Server 2016 容錯移轉叢集, 9-22
Windows Server 2019, 9-24
Windows Storage Server 2008 R2, 9-9
Windows Storage Server 2012, 9-16
Windows Storage Server 2012 R2, 9-17
Windows Storage Server 2016, 9-22

一畫

一次性報告, 17-18
檢視, 17-22

三畫

工作
安全威脅調查中心, 21-10
拒絕, 21-11
核可, 21-11
工作追蹤, 21-11
工具
Apex Central MIB 檔案, E-2
DBConfig 工具, 25-2
NVW Enforcer SNMPv2 MIB 檔案, E-2
用戶端移轉工具, 25-2

四畫

元件更新, 11-2, 11-8
Proxy 伺服器設定, 11-11
更新通知, 11-3
部署計劃, 11-3
部署預約時程, 11-3
預約, 11-4
元件更新通知, 11-3
元件清單, 11-2
手動元件更新, 11-8
手動更新
元件, 11-2
支援
更快地解決問題, 26-3
支援的目標
查詢, 21-17
文件, xii
文件意見反應, 26-5

五畫

用戶端
安全威脅調查中心, 21-19
用戶端移轉工具, 25-2
目標, 13-20
已部署, 13-20
依條件過濾, 13-3
具有問題, 13-21
等待中, 13-20
瀏覽, 13-9
離線, 13-20
目錄管理, 10-10, 10-12

六畫

回報層級, 6-13

合併, 6-14
建立自訂, 6-13
檢視, 6-13
存取權限, 4-8
安全威脅
使用者, 7-6
端點, 7-12
安全威脅狀態, 7-7, 7-14
安全威脅統計資料標籤, 3-36
安全威脅詳細資訊
安全威脅狀態, 7-7, 7-14
安全威脅調查中心
工作狀態, 21-12
工作指令, 21-10
用戶端, 21-19
指令狀態, 21-13
註冊, 21-2, 21-3
有問題的目標, 13-21
自訂表示式, 14-16–14-19
條件, 14-17, 14-18
匯入, 14-19
自訂範本, 14-28, 17-2
建立, 14-29
匯入, 14-30
自訂關鍵字, 14-23
條件, 14-24, 14-25
匯入, 14-26
自動化的分析, 21-14

七畫

伺服器
位址檢查清單, A-2
伺服器位址檢查清單, A-2
伺服器註冊, 8-2
方法, 8-2
刪除, 8-7
雲端服務設定, 8-10
新增, 8-4
編輯, 8-6
刪除
使用者帳號, 4-2
記錄檔, 15-18
刪除受管理的伺服器, 8-7
刪除策略, 13-17
我的帳號, 4-12
我的報告, 17-32
更新, 11-2
元件, 11-2
元件清單, 11-2
手動, 11-8
防毒病毒碼, 6-6
防毒病毒碼符合性
指標設定, 6-7

八畫

事件詳細資料已更新通知, 18-5
事件資訊清單, 18-6
依條件過濾, 13-3
使用者
刪除帳號, 4-2
啟動帳號, 4-3
關閉帳號, 4-3
使用者/端點目錄, 21-17
使用者詳細資料, 7-3
進階搜尋, 7-23, 21-17
進階搜尋類別, 7-25
匯出資料, 7-24, 21-18
端點詳細資料, 7-9
標籤和過濾器, 7-27
使用者分組, 6-11
使用者角色, 4-14
新增, 4-18
預設使用者角色, 4-15
編輯, 4-19

使用者帳號
存取權限, 4-8
刪除, 4-2
使用者角色, 4-14
啟動, 4-3
新增, 4-4
解除鎖定, 4-3
編輯, 4-9
瞭解, 4-2
關閉, 4-3
使用者詳細資料, 7-3
表格式檢視, 7-3
時間表檢視, 7-3
使用授權更新
Proxy 伺服器設定, 11-11
使用授權資訊, 5-2
檢視, 5-2
續約, 5-2
使用授權管理, 5-2
受管理的產品, 5-4
詳細資料, 5-4
使用網域認證登入, 2-6
取消註冊
受管理的伺服器, 8-7
受管理的伺服器, 8-2
取消註冊, 8-7
註冊, 8-4
編輯伺服器, 8-6
受管理的伺服器清單
設定 Proxy 伺服器設定, 8-8
受管理的產品, 10-2
使用授權管理, 5-4
啟動, 5-3, 5-5
設定, 10-8
部署元件, 10-7
發出工作, 10-7
註冊, 5-3, 5-6
檢視記錄檔, 10-9
拒絕工作, 21-6
拒絕的工作, 21-11

九畫
表示式, 14-15
自訂, 14-16, 14-19
條件, 14-17, 14-18
預先定義, 14-16
表格式檢視
使用者詳細資料, 7-3
端點詳細資料, 7-9

八畫
長條圖, 17-7

九畫
建立
稽核記錄檔, 18-5
建立策略, 13-2, 13-15
設定, 13-3
複製設定, 13-11
指令追蹤, 12-2
Managed Detection and Response, 21-15
指令詳細資料, 12-3, 21-17
查詢, 12-3
檢視, 12-3
指令詳細資料, 12-3, 21-17
指定目標
瀏覽, 13-9
指定策略, 13-3
優先順序, 13-8
查詢
支援的目標, 21-17
調查工作指令, 21-15

重新排序策略, 13-21

十畫
時間表檢視
使用者詳細資料, 7-3
端點詳細資料, 7-9
核可工作, 21-6
核可的工作, 21-11
案例處理, 7-7, 7-14
站台, 6-11
合併, 6-12
建立自訂, 6-11
檢視, 6-11

十二畫
草稿策略, 13-3

十畫
記錄查詢, 15-2
記錄檔, 15-1, 15-2
刪除, 15-18
查詢, 15-2
設定記錄檔彙整, 15-12
記錄檔維護, 15-18

十一畫
帳號
我的帳號, 4-12
帳號管理
使用者角色
預設使用者角色, 4-15
編輯, 4-19
啟動
Apex Central, 5-2
Syslog 轉送, 15-13
使用者帳號, 4-3
受管理的產品, 5-3, 5-5
啟動碼, 5-2
條件
自訂表示式, 14-17, 14-18
關鍵字, 14-24, 14-25
條件陳述式, 14-28
產品目錄, 10-2
工作, 10-2
受管理的產品, 10-2
管理, 10-10, 10-12
產品範圍
Widget, 3-5
符合性指標, 6-6
符合性標籤, 3-31
設定
存取權限, 4-8
受管理的產品, 10-8
記錄檔彙整, 15-12
設定 Proxy 伺服器設定
受管理的伺服器清單, 8-8
通知, 16-3
事件詳細資料已更新, 18-5
設定, 16-3
預約事件摘要, 18-5
通知和報告
聯絡人群組
新增, 16-7
編輯, 16-8
通訊埠
檢查清單, A-3
部署的目標, 13-20
部署計劃, 11-3

十二畫
單一登入
伺服器註冊, 8-3
產品目錄, 10-3
報告
一次性報告, 17-18, 17-19

自訂報告範本
新增, 17-3
自訂範本, 17-2, 17-3
長條圖, 17-7
圓餅圖, 17-12
刪除, 17-31
我的報告, 17-32
格式, 17-20, 17-24, 17-28
自訂範本, 17-20, 17-24, 17-28
靜態範本, 17-20, 17-24, 17-28
預約報告, 17-22, 17-23, 17-27
範本, 15-6, 17-3
檢視
預約報告, 17-31
檢視報告
一次性報告, 17-22
報告維護, 17-31
報告範本
自訂, 17-3
登入, 2-6
從本機, 2-6
從遠端, 2-6
登出, 2-7
等待中的工作, 21-6
等待中的目標, 13-20
策略
刪除, 13-17
建立, 13-2, 13-15
重新排序, 13-21
編輯, 13-14
策略目標, 13-20
策略清單, 13-6, 13-18
策略設定
複製, 13-11
策略管理, 13-2
DLP, 14-14
目標, 13-20
有問題的目標, 13-21
刪除策略, 13-17
建立策略, 13-2, 13-15
指定策略, 13-3
重新排序策略, 13-21
草稿策略, 13-3
設定, 13-3
部署的目標, 13-20
等待中的目標, 13-20
策略清單, 13-6, 13-18
策略優先順序, 13-8, 13-19
編輯策略, 13-14
複製策略設定, 13-11
擁有者, 13-20
瞭解, 13-2
離線目標, 13-20
變更擁有者, 13-17
策略優先順序, 13-19
策略類型
指定, 13-3
重新排序策略, 13-21
草稿, 13-3
策略優先順序, 13-19
註冊
安全威脅調查中心, 21-2, 21-3
受管理的伺服器, 8-4
受管理的產品, 5-3, 5-6
詞彙, xiv
進階搜尋
使用者/端點目錄, 7-23, 21-17
雲端服務組態設定, 8-10

十三畫

匯出
DLP 事件詳細資料, 18-6
圓餅圖, 17-12

新增
Active Directory 使用者, 4-4
Active Directory 群組, 4-4
使用者帳號, 4-4
受管理的伺服器, 8-4
解除鎖定
使用者帳號, 4-3
資料外洩防護, 14-15
DLP 合規官, 18-3
DLP 事件檢閱者, 18-3
事件查詢, 18-1, 18-6
DLP 合規官, 18-3
DLP 事件檢閱者, 18-3
通知, 18-5
匯出事件詳細資料, 18-6
管理員工作, 18-2
稽核記錄檔, 18-5
事件資訊清單, 18-6
表示式, 14-15–14-19
符合性指標, 6-6
資料識別碼, 14-15
範本, 14-27–14-30
檔案屬性, 14-20, 14-21
關鍵字, 14-22–14-26
資料外洩防護 (DLP), 14-14
資料外洩防護符合
指標設定, 6-9
資料庫資料表, 24-4
資料檢視
安全威脅資訊, B-2
產品資訊, B-88
資料識別碼, 14-15
表示式, 14-15
檔案屬性, 14-15
關鍵字, 14-15
資訊中心
Widget, 3-2
修改產品範圍, 3-5
移動, 3-4
新增, 3-4
標籤, 3-2
刪除, 3-4
投影片放映, 3-2
重新命名, 3-2
新增, 3-2
摘要, 3-15
過濾策略
重新排序, 13-21
電子郵件, 16-3
預先定義的表示式, 14-16
檢視, 14-16
預先定義的範本, 14-27
預先定義的關鍵字
距離, 14-23
關鍵字的數目, 14-23
預約更新, 11-4
元件, 11-2
預約事件摘要通知, 18-5
預約報告, 17-22
檢視, 17-31
預設使用者角色, 4-15

十四畫

摘要標籤, 3-15
端點分組, 6-11
端點詳細資料, 7-9
表格式檢視, 7-9
時間表檢視, 7-9
管理
Managed Detection and Response, 21-2
刪除受管理的伺服器, 8-7
受管理的伺服器, 8-2

停止管理雲端服務, 8-10
雲端服務設定, 8-10
新增受管理的伺服器, 8-4
編輯受管理的伺服器, 8-6

十五畫

暫停
Managed Detection and Response, 21-3, 21-6
標籤, 3-2
Widget, 3-2
安全威脅統計資料, 3-36
符合性, 3-31
摘要, 3-15
標籤和過濾器, 7-27
稽核記錄檔, 18-5
範本, 14-27–14-30
自訂, 14-28–14-30
自訂報告, 17-3
條件陳述式, 14-28
預先定義, 14-27
邏輯運算子, 14-28
編輯
使用者角色, 4-19
使用者帳號, 4-9
編輯受管理的伺服器, 8-6
編輯策略, 13-14
複製策略設定, 13-11
調查 DLP 事件, 18-1, 18-6
DLP 合規官, 18-3
DLP 事件檢閱者, 18-3
事件資訊清單, 18-6
通知, 18-5
匯出事件詳細資料, 18-6
管理員工作, 18-2
稽核記錄檔, 18-5
調查工作
拒絕, 21-6
狀態, 21-12
核可, 21-6
追蹤, 21-11

十六畫

選取目標
依條件過濾, 13-3

十七畫

檔案屬性, 14-15, 14-20, 14-21
wildcards（萬用字元）, 14-21
建立, 14-21
匯入, 14-21
檢查清單
伺服器位址, A-2
通訊埠, A-3
檢視
自動化的分析, 21-14
受管理產品記錄檔, 10-9
檢閱 DLP 事件, 18-6
事件資訊清單, 18-6
瞭解
使用者帳號, 4-2
聯絡人群組, 16-6
移除, 16-6
新增, 16-6, 16-7
編輯, 16-8

十八畫

瀏覽目標, 13-9

十九畫

離線目標, 13-20

十八畫

雙因素驗證, 2-6, 2-7, 4-10

十九畫
關閉
Syslog 轉送, 15-16
使用者帳號, 4-3
關鍵字, 14-15, 14-22
自訂, 14-23–14-26
預先定義, 14-22, 14-23

二十畫
繼續
Managed Detection and Response, 21-3, 21-6
觸發應用程式, 16-3

二十三畫
邏輯運算子, 14-28

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: APTM09699/230316