



7.0 TREND MICRO™ Control Manager

管理手冊

適用於企業的集中化安全防護管理

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/control-manager.aspx>

Trend Micro、Trend Micro t-ball 標誌、OfficeScan 和 Control Manager 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 © 2018。Trend Micro Incorporated / 趨勢科技股份有限公司。保留所有權利。

文件編號：CMTM78290/180614

發行日期：2018 年 4 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。在安裝或使用本產品前，請先閱讀此文件。

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

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

請至下列網站並給予您對此文件的評估意見：

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

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：Control Manager 簡介

關於 Control Manager	1-2
Control Manager 的新增功能 7.0	1-2
主要功能和優點	1-6
Control Manager 架構	1-8
主動式雲端截毒技術參與	1-9

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 Control Manager Web 主控台	2-3
存取 Web 主控台	2-4
設定 Web 主控台設定值	2-6
設定主動式雲端截毒技術設定	2-7

第 3 章：資訊中心

關於資訊中心	3-2
標籤和 Widget	3-2
作業中心	3-6
摘要標籤	3-16
DLP 事件調查標籤	3-29
Data Loss Prevention 標籤	3-32
符合性標籤	3-35
安全威脅偵測標籤	3-41

第 4 章：帳號管理

使用者帳號	4-2
使用者角色	4-13

第 5 章：使用授權管理

Control Manager 啟動和使用授權資訊	5-2
受管理產品的啟動和註冊	5-4

第 6 章：Active Directory 和符合性設定

Active Directory 整合	6-2
符合性指標	6-5
端點和使用者分組	6-10

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	7-10
Active Directory 詳細資料	7-16

受影響的使用者	7-17
使用進階搜尋	7-21
自訂標籤和過濾器	7-25

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
OfficeScan 用戶端安裝	9-4
OfficeScan SaaS 用戶端系統需求	9-22
Trend Micro Security (適用於 Mac) 用戶端安裝	9-47
Trend Micro Security (適用於 Mac) SaaS 用戶端安裝	9-52

第 10 章：產品目錄

產品目錄	10-2
檢視受管理產品狀態摘要	10-6
執行產品目錄的進階搜尋	10-7
執行受管理產品工作	10-8
設定受管理的產品設定	10-9
從產品目錄查詢記錄檔	10-10
目錄管理	10-12

第 11 章：策略管理

策略管理	11-2
Data Loss Prevention	11-23
策略狀態	11-39

第 12 章：元件更新

元件更新	12-2
設定預約更新設定	12-5
設定手動更新設定	12-8
設定用於元件和使用授權更新的 Proxy 伺服器設定	12-11

第 13 章：指令追蹤

指令追蹤	13-2
查詢及檢視指令	13-3
設定指令逾時設定	13-4

部分 IV：安全監控

第 14 章：記錄檔

記錄查詢	14-2
使用記錄查詢	14-2
設定記錄檔彙整	14-10
刪除記錄檔	14-11

第 15 章：通知

事件通知	15-2
通知方法設定	15-3
聯絡人群組	15-6

進階安全威脅活動事件	15-9
內容策略違規事件	15-26
Data Loss Prevention 事件	15-29
已知的安全威脅活動事件	15-38
網路存取控制事件	15-53
不尋常的產品行為事件	15-56
更新	15-63
第 16 章：報告	
報告總覽	16-2
自訂範本	16-2
一次性報告	16-18
預約報告	16-22
設定報告維護	16-31
檢視我的報告	16-31
第 17 章：連線的威脅防範	
關於連線的威脅防範	17-2
功能需求	17-2
可疑物件清單管理	17-7
先發式可疑物件防護	17-19
連線的威脅防範產品整合	17-26
第 18 章：Data Loss Prevention 事件	
管理員工作	18-2
DLP 事件檢閱程序	18-8

部分 V：工具和支援

第 19 章：管理資料庫

瞭解 Control Manager 資料庫	19-2
使用 SQL Server Management Studio 備份 db_ControlManager	19-8
使用 SQL 指令壓縮 db_ControlManager_Log.ldf	19-10
使用 SQL Server Management Studio 壓縮 db_ControlManager_log.ldf	19-11

第 20 章：Control Manager 工具

關於 Control Manager 工具	20-2
使用用戶端移轉工具 (AgentMigrateTool.exe)	20-2
使用資料庫組態設定工具 (DBConfig.exe)	20-2

第 21 章：可疑物件中樞和節點 Control Manager 架構

可疑物件中樞和節點 Control Manager 架構	21-2
設定可疑物件中樞和節點	21-3
從中樞 Control Manager 取消註冊可疑物件節點	21-4
組態設定注意事項	21-5

第 22 章：可疑物件清單匯出程式和匯入程式使用者手冊

可疑物件清單匯出程式和匯入程式使用者手冊	22-2
使用可疑物件清單匯出程式 (SuspiciousObjectExporter.exe)	22-2
使用 Control Manager 匯出沙盒虛擬平台例外清單	22-10
使用 Control Manager 匯出使用者定義的清單	22-11
使用可疑物件清單匯入程式 (ImportSOFromCSV.exe)	22-11
使用 Control Manager 匯入沙盒虛擬平台例外清單	22-13
使用 Control Manager 匯入使用者定義的清單	22-14

第 23 章：使用 LogForwarder 工具 (LogForwarder.exe)

簡介	23-2
----------	------

系統需求	23-3
限制	23-3
設定 LogForwarder 設定	23-4
開始與停止轉送記錄檔	23-6
第 24 章：可疑物件移轉工具使用手冊	
可疑物件移轉工具使用手冊	24-2
準備 Check Point 防火牆伺服器	24-2
準備驗證憑證組態設定檔	24-4
使用可疑物件移轉工具	24-8
使用可疑物件清單匯出程式 (SuspiciousObjectExporter.exe)	24-10
使用 Check Point Suspicious Activity Monitoring Client 工具	24-18
第 25 章：技術支援	
疑難排解資源	25-2
聯絡趨勢科技	25-3
將可疑內容傳送到趨勢科技	25-4
其他資源	25-5

附錄

附錄 A：Control Manager 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
Control Manager 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-85

附錄 C：Token 變數

關於 Token 變數	C-2
標準 Token 變數	C-3
進階安全威脅活動 Token 變數	C-3
C&C 回呼 Token 變數	C-4
內容策略違規 Token 變數	C-5
Web 存取安全違規 Token 變數	C-5
Data Loss Prevention Token 變數	C-6
已知的安全威脅活動 Token 變數	C-8
網路存取控制 Token 變數	C-10

附錄 D：IPv6 支援

Control Manager 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 Control Manager 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 Data Loss Prevention 記錄檔	F-3
CEF 行為監控記錄檔	F-9
CEF 裝置存取控制記錄檔	F-14
CEF 引擎更新狀態記錄檔	F-20

CEF Machine Learning 記錄檔	F-22
CEF 特徵碼更新狀態記錄檔	F-26
CEF 內容安全記錄檔	F-28
CEF 間諜程式/可能的資安威脅程式記錄檔	F-32
CEF 病毒/惡意程式記錄檔	F-40
CEF Web 網頁安全記錄檔	F-44
CEF C&C 回呼記錄檔	F-55
CEF 可疑檔案記錄檔	F-59
CEF 網路內容檢測記錄檔	F-61
CEF Endpoint Application Control 記錄檔	F-63
CEF 沙盒偵測記錄檔	F-65

索引

索引	IN-1
----------	------

序言

序言


本文件介紹 Trend Micro™ Control Manager™，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

Control Manager 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	<p>討論安裝 Control Manager 的需求與程序的 PDF 文件</p> <hr/> <p> 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》。</p>
系統需求	討論安裝 Control Manager 的需求與程序的 PDF 文件
管理手冊	提供如何設定及管理 Control Manager 和受管理產品的詳細指示，以及說明 Control Manager 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 Control Manager 主控台存取的「說明」
連線的威脅防範入門	說明如何使用 Control Manager 整合多種趨勢科技產品與解決方案，來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、分析及回應的 PDF 文件。
Widget 和策略管理手冊	說明如何在 Control Manager 中設定資訊中心 Widget 和策略管理設定的 PDF 文件
資料安全防護清單（僅第 1 章）	其中列出 Data Loss Prevention 的預先定義資料識別碼和範本的 PDF 文件
知識庫	提供問題解決方法和疑難排解資訊的線上資料庫。此資料庫提供有關產品已知問題的最新資訊。若要存取知識庫，請前往下列網站： http://esupport.trendmicro.com/zh-tw/business/default.aspx

您可以從下列位置下載最新的 PDF 文件和 Readme 檔：

<http://docs.trendmicro.com/zh-tw/enterprise/control-manager.aspx>

讀者

Control Manager 文件適用於下列使用者：



- Control Manager 管理員：負責安裝、設定及管理 Control Manager。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 Control Manager 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
<i>斜體</i>	參考其他文件
等寬	指令行範例、程式碼、Web URL、檔案名稱和程式輸出
瀏覽 > 路徑	可達到特定畫面的瀏覽路徑 例如，「檔案 > 儲存」代表請點選「檔案」，然後請點選介面上的「儲存」
 注意	組態設定注意事項
 秘訣	推薦或建議

慣例	說明
 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 Control Manager 文件中使用的正式詞彙：

詞彙	說明
管理員（或 Control Manager 管理員）	管理 Control Manager 伺服器的人員
用戶端	安裝在端點上的受管理產品程式
元件	負責針對安全威脅進行掃描、偵測和採取中毒處理行動
Control Manager 主控台、Web 主控台或管理主控台	用於存取、設定及管理 Control Manager 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，OfficeScan Web 主控台。
受管理端點	安裝了受管理產品用戶端的端點
受管理的產品	與 Control Manager 整合的 Trend Micro 產品
受管理的伺服器	安裝了受管理產品的端點
伺服器	安裝了 Control Manager 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

詞彙	說明
產品服務	透過 Microsoft Management Console (MMC) 所代管的 Control Manager 服務。
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

Control Manager 簡介

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

包含下列主題：

- [關於 Control Manager 第 1-2 頁](#)
- [Control Manager 的新增功能 7.0 第 1-2 頁](#)
- [主要功能和優點 第 1-6 頁](#)
- [Control Manager 架構 第 1-8 頁](#)
- [主動式雲端截毒技術參與 第 1-9 頁](#)

關於 Control Manager


Trend Micro™ Control Manager™ 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。Control Manager 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。


Control Manager 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、掃描引擎和垃圾郵件防護規則），以確保您擁有最新的安全防護。Control Manager 允許手動更新和預約更新。Control Manager 允許您將產品視為群組或個體來設定和管理，以提升彈性。

Control Manager 的新增功能 7.0


此版本的 Control Manager 包含下列新增和增強功能。

功能	說明
Active Directory 整合增強功能	此版本的 Control Manager 支援與多個 Active Directory 樹系整合，並且除了使用者之外，還允許您匯入 Active Directory 群組。 如需詳細資訊，請參閱 Active Directory 整合 第 6-2 頁 。
資訊中心增強功能	資訊中心經過重新設計，能夠讓您更清楚看到自己網路的安全防護狀態。
全新的「暫留時間」Widget	此 Widget 會根據安全威脅在受影響使用者的端點上存在的時間長度，提供前幾名嚴重安全威脅的總覽。
全新的「執行摘要」報告	全新的「執行摘要」報告範本可提供有關您網路中所有安全威脅偵測的廣泛情報，以及檢視可針對受影響使用者/端點或安全威脅偵測（依通道和產品）採取的處理行動總覽。

功能	說明
全新的「通知」功能表	<p>全新的「通知」功能表可讓您更輕鬆存取先前名為「事件中心」（現在已重新命名為「事件通知」）的畫面。全新的功能表還包含「通知方法設定」畫面（先前稱為「一般事件設定」）和「聯絡人群組」畫面（先前稱為「使用者群組」）。</p> <p>如需詳細資訊，請參閱通知方法設定 第 15-3 頁。</p>
全新的「唯讀」使用者角色	<p>您可以指派全新的「唯讀」使用者角色，輕鬆允許使用者帳號在 Control Manager 管理主控台中檢視資訊，但不將修改組態設定的存取權限授與使用者。</p>
全新的報告格式	<p>您現在可以使用下列格式來產生靜態報告：</p> <ul style="list-style-type: none"> • Microsoft Word 格式 (*.docx) • Microsoft Excel 格式 (*.xlsx) <hr/> <p> 注意</p> <ul style="list-style-type: none"> • 此版本的 Control Manager 不再支援 ActiveX 和 Crystal Report 格式。 • 如果您是從舊版 Control Manager 移轉，則您仍可在 Control Manager 7.0 中下載先前產生的 Crystal Reports。
作業中心	<p>使用「作業中心」標籤，可立即深入探索您網路中的防毒病毒碼和 Data Loss Prevention 符合性狀態、嚴重安全威脅偵測，以及已解決和未解決的事件。</p> <p>如需詳細資訊，請參閱作業中心 第 3-6 頁。</p>

功能	說明
平台和瀏覽器支援	<p>此版本的 Control Manager 支援下列項目：</p> <ul style="list-style-type: none"> • Microsoft™ Windows™ Server 2016 • Microsoft™ Internet Explorer™ 11 • Microsoft™ Edge™ • Google™ Chrome™ • Microsoft™ SQL Server™ 2016 <hr/> <p> 注意</p> <p>此版本的 Control Manager 不再支援下列項目：</p> <ul style="list-style-type: none"> • Microsoft™ Windows™ Server 2003 • Microsoft™ Internet Explorer™ 8、9 或 10 • Microsoft™ SQL Server™ 2005
策略管理增強功能	<p>您現在可以將策略指派給從多個已同步處理之 Active Directory 樹系的組織單位中選取的目標。</p> <p>為了防止網路管理出現空檔，您也可以指定某個使用者帳號做為策略的擁有者，即使該使用者帳號不具有指定目標的存取權限亦可。</p>
Security Agent 安裝	<p>直接從 Control Manager 主控台建立及下載 OfficeScan 或 Trend Micro Security (適用於 Mac) 的 Security Agent 安裝套件。</p>
簡化的記錄查詢	<p>先前名為「全新臨機操作查詢」和「儲存的臨機操作查詢」的兩個畫面，已整合為全新的「記錄查詢」畫面。增強的「記錄查詢」畫面採用全新設計，可讓您在單一畫面中，就能更輕鬆查詢記錄、執行進階搜尋、儲存和共用記錄查詢，以及匯出搜尋結果。</p>

功能	說明
可疑物件管理增強功能	<p>為了進一步提高對先前未知安全威脅的防護力，您現在可以使用「使用者定義的可疑物件」畫面來上傳可疑物件檔案，來協助已註冊的受管理產品偵測安全威脅，而不需要手動輸入檔案 SHA-1 雜湊值。</p> <p>除了可疑檔案、URL 和 IP 位址外，您現在也可在「物件」欄中展開可疑網域，以深入瞭解詳細資訊。</p> <p>在「物件」欄中展開可疑物件後，帶有星號的使用者或端點表示它們是「重要」使用者或端點，因此會顯示在「有風險的收件者」或「有風險的端點」清單的頂端。「最新處理行動結果」欄會顯示受管理產品最近採取的矯正性處理行動。您也可以按一下「最新處理行動結果」欄名稱來排序偵測清單，將需要進一步緩和的安全威脅顯示在頂端。</p> <p>為了簡化案例處理程序，先前獨立的「影響評估」和「緩和」標籤已整合為一個「影響評估與緩和」標籤。</p>
傳輸層安全性 1.2 支援	<p>此版本的 Control Manager 支援傳輸層安全性 (TLS) 1.2 通訊協定，可為您的網路通訊提供更強而有力的安全防護。</p>
雙因素驗證	<p>「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 Control Manager，為使用者帳號提供額外的安全性。</p> <p>如需詳細資訊，請參閱啟動或關閉雙因素驗證 第 4-10 頁。</p>
更新功能表增強功能與智慧元件下載	<p>重新設計的「更新」功能表，可讓您使用「預約更新」或「手動更新」畫面，更輕鬆地管理及部署元件更新。</p> <p>您還可以啟動智慧元件下載，讓 Control Manager 自動從更新來源偵測並下載所選元件類別中的新元件。</p>

功能	說明
使用者/端點目錄增強功能	<p>除了傳統的「表格式檢視」外，現在也可使用「時間表檢視」顯示使用者或端點資訊，讓您按照時間順序清楚列出安全威脅偵測的發生時間，並且更輕鬆地識別某段時間範圍內的特徵碼。</p> <p>您還可以將使用者/端點目錄中的資料匯出為 *.csv 檔案或 *.png 影像。</p> <hr/> <p> 注意</p> <p>「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。</p> <p>如需詳細資訊，請參閱使用者/端點目錄 第 7-2 頁。</p>

主要功能和優點

Control Manager 提供下列功能和優點。

功能	優點
作業中心	使用「作業中心」標籤，可立即深入探索您網路中的防毒病毒碼和 Data Loss Prevention 符合性狀態、嚴重安全威脅偵測，以及已解決和未解決的事件。
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 Control Manager 資訊（包括安全威脅偵測、元件狀態、策略違規等）。
使用者/端點目錄	檢視 Control Manager 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。
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 Control Manager Web 主控台執行手動掃描。

功能	優點
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 Control Manager 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	Control Manager 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	Control Manager 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 Control Manager 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 Control Manager 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 Control Manager 主控台建立及下載 OfficeScan 或 Trend Micro Security (適用於 Mac) 的 Security Agent 安裝套件。

Control Manager 架構

Trend Micro Control Manager 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 Control Manager 使用的元件。

元件	說明
Control Manager 伺服器	<p>做為所有從用戶端收集之資料的存放區。Control Manager 伺服器提供下列功能：</p> <ul style="list-style-type: none"> SQL 資料庫，可儲存受管理產品的組態設定和記錄檔 Control Manager 使用 Microsoft SQL Server 資料庫 (db_ControlManager.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 Control Manager Web 主控台 郵件用戶端，可透過電子郵件傳送事件通知 Control Manager 會將 Control Manager 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 Control Manager 報告是有關 Control Manager 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	<p>MCP 會處理 Control Manager 伺服器與支援新一代用戶端的受管理產品的互動。</p> <p>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 Control Manager 進行通訊。MCP 代理程式會輪詢 Control Manager 是否有指令和更新。</p>
Web 服務整合通訊	<p>可讓 Control Manager 與受管理產品進行通訊的無用戶端整合模型</p>

元件	說明
Web-based 管理主控台	<p>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 Control Manager</p> <p>Control Manager 管理主控台是透過 Microsoft Internet Information Server (IIS) 在 Internet 上發佈，並且由 Control Manager 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 Control Manager 網路。</p>
Widget 架構	可讓管理員建立自訂的資訊中心來監控 Control Manager 網路。

主動式雲端截毒技術參與

Trend Micro Smart Feedback 會持續收集並分析安全威脅資訊，以提供更好的安全防護。一旦加入 Trend Micro Smart Feedback，表示您同意趨勢科技從您的裝置收集資訊以協助識別新安全威脅。趨勢科技將從您的裝置收集如下資訊：

- 檔案總和檢查碼
- 存取的網址
- 檔案資訊，包括大小與路徑
- 執行檔名稱



秘訣

您不需要加入 Smart Feedback 仍可保護您的裝置。您隨時可以選擇參與或是退出此活動。趨勢科技建議您參與 Smart Feedback 以協助我們為所有趨勢科技客戶提供更完善的全方位保護機制。

如需主動式雲端截毒技術的詳細資訊，請造訪 <http://www.smartprotectionnetwork.com>。

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 Control Manager 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 Control Manager Web 主控台 第 2-3 頁](#)
- [存取 Web 主控台 第 2-4 頁](#)
- [設定 Web 主控台設定值 第 2-6 頁](#)
- [設定主動式雲端截毒技術設定 第 2-7 頁](#)

關於 Web 主控台

Control Manager Web 主控台可針對所有受已向 Control Manager 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 Control Manager 網路。




注意

請以 1366 x 768 像素的螢幕解析度檢視 Web 主控台。

Control Manager 支援下列 Web 瀏覽器：

- Microsoft Internet Explorer™ 11
- Microsoft Edge™
- 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
瀏覽器	Microsoft Internet Explorer™ 11、Microsoft Edge™ 或 Google Chrome™
	 重要 使用 Internet Explorer 或 Edge 存取 Control Manager Web 主控台時，請關閉「相容性檢視」。

資源	需求
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 Control Manager Web 主控台

在安裝 Control Manager 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 連線的安全性最低。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。

您必須取得憑證並設定 Control Manager 虛擬目錄，然後才能開始向 Control Manager 伺服器傳送及從其接收加密或經過數位簽署的資訊。

程序

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 Control Manager 伺服器。
3. 按一下「開始 > 程式集 > 系統管理工具 > 網際網路服務管理員」，以開啟 IIS Microsoft Management Console (MMC)。
4. 按一下 IIS 伺服器旁邊的 + 號，以展開虛擬站台清單。
5. 選取「預設網站」，然後以滑鼠右鍵按一下「內容」。
6. 在「預設網站內容」畫面上：
 - a. 按一下「目錄安全性」標籤。
 - b. 按一下「伺服器憑證」以使用新增憑證精靈建立伺服器憑證要求。
 - c. 按「下一步」。
 - d. 在「伺服器憑證方法」畫面中，選取「從金鑰管理員備份檔案匯入憑證」，然後按一下「下一步」。

- c. 輸入金鑰的「完整路徑」和「檔案名稱」（例如 cm_cert.key），然後按一下「下一步」。
 - f. 指定金鑰的「密碼」，然後按一下「下一步」。
 - g. 在「匯入憑證摘要」畫面上，按一下「下一步」以執行伺服器憑證，或按一下「上一步」以修改設定。
7. 按一下「確定」以套用「預設網站」伺服器憑證，並返回「預設網站」清單。
 8. 從「預設網站」清單中選取「Control Manager」虛擬目錄，然後以滑鼠右鍵按一下「內容」。
 9. 按一下「目錄安全性」標籤，然後按一下「安全通訊」下的「編輯」。會出現「安全通訊」視窗。
 10. 選取「需要安全通道 (SSL)」和「需要 128 位元加密」。
 11. 按一下「確定」以關閉「安全通訊」視窗。
 12. 按一下「確定」以套用變更並返回「預設網站」清單。

當您下次使用 HTTP 來存取 Web 主控台時，會顯示下列訊息：

您必須透過安全通道檢視此頁面。

存取 Web 主控台

從 Control Manager 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 Control Manager 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 Control Manager 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 Control Manager 管理主控台。

程序

1. 從本機或從遠端存取 Control Manager 管理主控台。
 - 如果要從本機存取主控台，請在 Control Manager 伺服器上移至「開始 > 程式集 > Trend Micro Control Manager > Trend Micro Control Manager」。
 - 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 Control Manager 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 Control Manager 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 Control Manager 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。

Control Manager 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，請執行下列其中一項：
 - 在 Web 主控台的右上角，按一下「<帳號名稱> > 登出」。
 - 同時按下 **CTRL** 和 **W** 鍵。

設定 Web 主控台設定值

請設定 Control Manager 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。

程序

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 Control Manager 伺服器依照指定的時間間隔重新整理畫面資料 <ul style="list-style-type: none"> • 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）

區段	設定
Web 主控台逾時	<p>選取「啟動自動登出 Web 主控台」，讓 Control Manager 伺服器依照指定的時間間隔將使用者登出</p> <ul style="list-style-type: none"> 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	<p>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 Control Manager 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</p> <ul style="list-style-type: none"> 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）

3. 按一下「儲存」。

設定主動式雲端截毒技術設定

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

有些 Widget 也需要啟動「主動式雲端截毒技術設定」，才能正常運作。這是因為 Widget 會直接從趨勢科技主動式雲端截毒技術接收其資料。



注意

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

程序

1. 移至「管理 > 設定 > 主動式雲端截毒技術設定」。

會出現「主動式雲端截毒技術設定」畫面。

2. 選取「啟動 Trend Micro Smart Feedback 和主動式雲端截毒技術服務」。
 3. 從「時間間隔」下拉式清單中，指定 Control Manager 將完全匿名的安全威脅資訊傳送給主動式雲端截毒技術的頻率。
 4. （選用）從「您所屬產業」下拉式清單中，指定您公司所屬的產業。
 5. 按一下「儲存」。
-

第 3 章

資訊中心

本節討論如何使用 Control Manager 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](#)
- [作業中心 第 3-6 頁](#)
- [摘要標籤 第 3-16 頁](#)
- [DLP 事件調查標籤 第 3-29 頁](#)
- [Data Loss Prevention 標籤 第 3-32 頁](#)
- [符合性標籤 第 3-35 頁](#)
- [安全威脅偵測標籤 第 3-41 頁](#)

關於資訊中心

當您開啟 Control Manager 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 Control Manager 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：

- Control Manager 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
如需詳細資訊，請參閱[設定主動式雲端截毒技術設定 第 2-7 頁](#)。

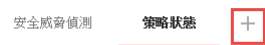
標籤為 Widget 提供了容器。「資訊中心」最多支援 30 個標籤。

使用標籤

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

程序

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



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



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



- b. 啟動「標籤投影片放映」控制項。
- c. 選取在切換到下一個標籤前，每個標籤顯示的時間長度。

使用 Widget



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

程序

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

- a. 請點選標籤顯示右側的「設定」按鈕。



- b. 請點選「新增 Widget」。
- c. 選取要新增的 Widget。
- 在 Widget 頂端的下拉式清單，選取類別以縮小選取範圍。
 - 使用畫面頂端的搜尋文字方塊可搜尋特定 Widget。
- d. 請點選「新增」。
4. 如果要將 Widget 移至同一個標籤上的新位置，請將 Widget 拖放至新位置。
5. 將滑鼠游標指向 Widget 的右邊緣，然後向左或向右移動游標，即可調整多欄標籤上的 Widget 大小。
6. 如果要重新命名 Widget：
- a. 請點選設定圖示 ( > )。
 - b. 輸入新標題。
 - c. 按一下「儲存」。
7. 如果要修改 Widget 的產品範圍，請執行下列作業：

- a. 請點選設定圖示 ()。
 - b. 按一下「範圍」欄位中的雙箭號按鈕 ()。
 - c. (選用) 按一下漏斗圖示 () 來過濾並搜尋產品。
 - d. 選取為了 Widget 提供資料的產品，然後按一下「確定」。
 - e. 按一下「儲存」。
8. 如果要刪除 Widget，請點選刪除圖示 ()。

作業中心





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

注意

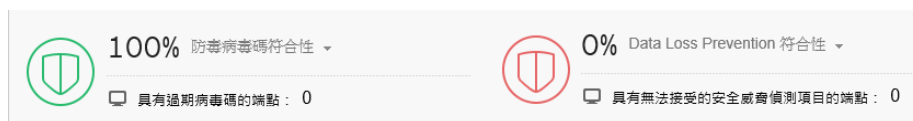
如果要變更範例圖表資料，並根據您的公司網路來顯示網站或報告行，請啟動 Active Directory 整合或根據 IP 位址建立自訂網站。

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

按一下設定圖示 ( > )，可變更標籤上顯示的下列資訊。

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

符合性指標



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

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


預設檢視會顯示「防毒病毒碼符合性」指標的資訊。



注意

變更符合性指標會同時變更在「安全性作業」圖表中顯示的符合性層級資訊。

如需詳細資訊，請參閱[作業中心圖表 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	<p>顯示下列資訊：</p> <ul style="list-style-type: none"> 採用可接受的「病毒碼」和「本機雲端病毒碼」版本的 OfficeScan 和 Worry-Free Business Security Services 用戶端百分比 <p>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 6-6 頁。</p> <ul style="list-style-type: none"> 在您的網路上，具有過期防毒病毒碼的端點總數 <p>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。</p> <p>如需詳細資訊，請參閱使用者/端點目錄 第 7-2 頁。</p>
Data Loss Prevention 符合性	<p>顯示下列資訊：</p> <ul style="list-style-type: none"> 已啟動 Data Loss Prevention 且具有可接受的安全威脅偵測項目數的 OfficeScan 用戶端百分比 <p>如需設定符合性指標設定的詳細資訊，請參閱設定 Data Loss Prevention 符合性指標 第 6-8 頁。</p> <ul style="list-style-type: none"> 具有 Data Discovery 安全威脅偵測項目的端點總數 <p>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。</p> <p>如需詳細資訊，請參閱使用者/端點目錄 第 7-2 頁。</p>

嚴重安全威脅



3 嚴重安全威脅



受影響的使用者: 2 (0*)

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

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 7-30 頁。

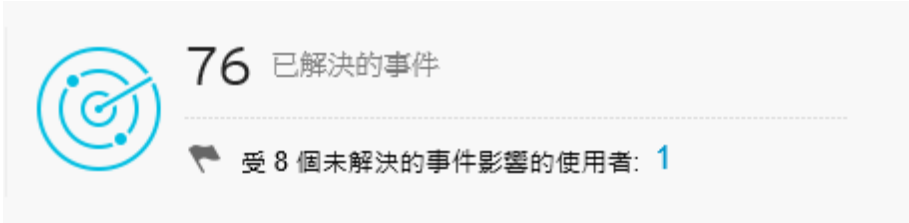
按一下受影響的使用者數目，可在「使用者/端點目錄」畫面上檢視其他詳細資訊。

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盒虛擬平台的產品偵測到，且風險等級為「高」的可疑物件（IP 位址、網域、檔案 SHA-1 雜湊值、電子郵件訊息）
弱點攻擊	利用通常在程式和作業系統中發現的安全弱點所進行的惡意程式或駭客攻擊

已解決的事件



「作業中心」標籤的這個區段，會顯示您網路中已解決和未解決的事件總數。按一下「受 __ 個未解決的事件影響的使用者」欄位的計數，可檢視您網路中受未解決事件影響之使用者的詳細資訊。

如需詳細資訊，請參閱[使用者/端點目錄 第 7-1 頁](#)。

作業中心圖表



「作業中心」標籤上的圖表，會顯示您網路的嚴重安全威脅比率與符合性層級之間的關係。X 軸表示嚴重安全威脅與網站或報告行中端點總數的比率。Y 軸

表示網站或報告行達到所選符合性指標的哪個符合性層級。您可以使用此資料來快速識別整合式 Active Directory 結構中的高風險使用者和群組。





注意

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



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

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

如需詳細資訊，請參閱 [端點和使用者分組](#) 第 6-10 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 [作業中心詳細資料窗格](#) 第 3-12 頁。

作業中心詳細資料窗格

全部

0% Data Loss Prevention 符合性

受管理的用戶端:	0	
具有可接受的安全威脅偵測項目	0	0%
具有無法接受的安全威脅偵測項目	0	0%
離線 7 天	0	
例外	0	
未受管理的端點:	16	

3 嚴重安全威脅

勒索軟體	2
已知的進階持續安全威脅 (APT)	1
社交工程攻擊	0
弱點攻擊	0
橫向移動	0
未知安全威脅	0
C&C 回呼	0

2 受影響的使用者

[Report WA_UserD](#)

[Report \ben](#)

2 受影響的端點

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

預設檢視會顯示您網路中所有節點過去 7 天的所選符合性指標資訊。



- 選取不同的符合性指標，會變更顯示的符合性資訊。
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[作業中心圖表 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	<p>顯示採用可接受的「病毒碼」和「本機雲端病毒碼」版本的 OfficeScan 和 Worry-Free Business Security Services 用戶端百分比</p> <p>您也可以檢視下列詳細資料：</p> <ul style="list-style-type: none"> • 受管理的用戶端：已安裝 OfficeScan 和 Worry-Free Business Security Services 用戶端的端點數目 <ul style="list-style-type: none"> • 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：未安裝的 OfficeScan 或 Worry-Free Business Security Services 用戶端的端點數目 <p>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。</p> <p>如需詳細資訊，請參閱下列主題：</p> <ul style="list-style-type: none"> • 設定防毒病毒碼符合性指標 第 6-6 頁 • 使用者/端點目錄 第 7-1 頁

指標	說明
<p>Data Loss Prevention 符合性</p>	<p>顯示已啟動 Data Loss Prevention 且具有可接受的安全威脅偵測項目數的 OfficeScan 用戶端百分比</p> <p>您也可以檢視下列詳細資料：</p> <ul style="list-style-type: none"> • 受管理的用戶端：已安裝啟動了 Data Loss Prevention 的 OfficeScan 用戶端的端點數目 <ul style="list-style-type: none"> • 具有可接受的安全威脅偵測項目：具有可接受的安全威脅偵測項目數的受管理用戶端數目 • 具有無法接受的安全威脅偵測項目：超過可接受的安全威脅偵測項目數的受管理用戶端數目 • 離線 7 天：未與受管理產品伺服器進行通訊達到 7 天（或更多天）的受管理用戶端數目 • 例外：從符合性計算排除的使用者或端點數目 • 未受管理的端點：未安裝啟動了 Data Loss Prevention 的 OfficeScan 用戶端的端點數目 <p>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。</p> <p>如需詳細資訊，請參閱下列主題：</p> <ul style="list-style-type: none"> • 設定 Data Loss Prevention 符合性指標 第 6-8 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
<p>嚴重安全威脅</p>	<p>顯示在您網路中偵測到的嚴重安全威脅總數</p> <p>列出所有會影響您網路的嚴重安全威脅類型</p> <p>如需瞭解偵測的安全威脅類型，請執行下列操作：</p> <ul style="list-style-type: none"> • 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。 <p>如需詳細資訊，請參閱受影響的使用者 第 7-17 頁。</p>

區段	說明
受影響的使用者	<p>顯示受嚴重安全威脅影響的使用者總數</p> <ul style="list-style-type: none"> 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。 <p>如需詳細資訊，請參閱使用者所面臨的安全威脅 第 7-6 頁。</p>
受影響的端點	<p>顯示受嚴重安全威脅影響的端點總數</p> <ul style="list-style-type: none"> 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。 <p>如需詳細資訊，請參閱端點上的安全威脅 第 7-13 頁。</p>

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	<p>顯示您網路中受未解決事件影響的使用者數目</p> <p>按一下計數可檢視受影響使用者的詳細資料。</p> <p>如需詳細資訊，請參閱使用者/端點目錄 第 7-1 頁。</p>

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
- Control Manager 的前幾名安全威脅
- 產品連線狀態
- 產品元件狀態

嚴重安全威脅 Widget

嚴重安全威脅 ⋮

上次重新整理時間: 2018/06/21 01:41:53

範圍: 2018/06/15 ~ 2018/06/21

2 嚴重安全威脅類型

安全威脅類型 ⓘ	重要使用者	其他使用者
勒索軟體	0	2
已知的進階持續安全威脅 (APT)	0	1
社交工程攻擊	0	0
弱點攻擊	0	0
橫向移動	0	0
未知安全威脅	0	0
C&C 回呼	0	0

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

- 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 7-30 頁](#)。

使用「範圍」下拉式清單，選取顯示的資料時間範圍。

資料表會按嚴重性順序列出嚴重安全威脅類型。

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

如需詳細資訊，請參閱[使用者所面臨的安全威脅 第 7-6 頁](#)。

「安全威脅類型」欄會顯示下列安全威脅類型。



注意

個別使用者可能受到多個嚴重安全威脅類型的影響。

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
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盒虛擬平台的產品偵測到，且風險等級為「高」的可疑物件（IP 位址、網域、檔案 SHA-1 雜湊值、電子郵件訊息）

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
受嚴重安全威脅影響的使用者總數	此列顯示的計數表示具有至少一個嚴重安全威脅偵測項目的「重要使用者」和「其他使用者」的總數。每個使用者可能受到多個嚴重安全威脅的影響。

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 7-30 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
已知的進階持續安全威脅 (APT)	攻擊者發起的人侵會具有侵犯性地追擊並入侵所選目標，通常隨著時間的推移執行一連串的失敗和成功的嘗試活動（並非孤立事件），以深入到目標網路內部
橫向移動	搜尋目錄、電子郵件、管理伺服器和其他資產，以勘測出網路的內部結構，進而取得認證來存取這些系統，讓攻擊者得以在系統間跳轉
勒索軟體	除非使用者支付贖金，否則會阻止或限制使用者存取其系統的惡意程式
社交工程攻擊	利用文件（例如 PDF 檔案）中發現的安全弱點所進行的惡意程式或駭客攻擊
未知安全威脅	由 Deep Discovery Inspector、端點安全防護產品或其他具有沙盒虛擬平台的產品偵測到，且風險等級為「高」的可疑物件（IP 位址、網域、檔案 SHA-1 雜湊值、電子郵件訊息）
弱點攻擊	利用通常在程式和作業系統中發現的安全弱點所進行的惡意程式或駭客攻擊

具有安全威脅的端點 Widget

具有安全威脅的端點

上次重新整理時間: 2018/06/21 01:47:32

範圍: 1週

2018/06/15 ~ 2018/06/21

0 重要端點

3 其他端點

主機名稱	IP 位址	安全威脅	最嚴重的安全威脅
Client01	110.1.0.1	46	勒索軟體
Client04	104.0.16.1	10	勒索軟體
WIN-H0F70G8T1MA	172.16.122.115	10	無

此 Widget 會顯示具有安全威脅偵測項目之端點的相關資訊。

使用「範圍」下拉式清單，選取顯示的資料時間範圍。

按一下「重要使用者」或「其他使用者」標籤，可在不同的檢視間切換。

- 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 7-30 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 7-13 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)	攻擊者發起的人侵會具有侵犯性地追擊並入侵所選目標，通常隨著時間的推移執行一連串的失敗和成功的嘗試活動（並非孤立事件），以深入到目標網路內部
橫向移動	搜尋目錄、電子郵件、管理伺服器和其他資產，以勘測出網路的內部結構，進而取得認證來存取這些系統，讓攻擊者得以在系統間跳轉
勒索軟體	除非使用者支付贖金，否則會阻止或限制使用者存取其系統的惡意程式
社交工程攻擊	利用文件（例如 PDF 檔案）中發現的安全弱點所進行的惡意程式或駭客攻擊
未知安全威脅	由 Deep Discovery Inspector、端點安全防護產品或其他具有沙盒虛擬平台的產品偵測到，且風險等級為「高」的可疑物件（IP 位址、網域、檔案 SHA-1 雜湊值、電子郵件訊息）
弱點攻擊	利用通常在程式和作業系統中發現的安全弱點所進行的惡意程式或駭客攻擊

Control Manager 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 ([圖表] [表格])，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 ([三點] > [齒輪])，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 Control Manager 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 Control Manager 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	顯示掃描引擎的名稱

資料	說明
最新版本	<p>顯示下列資訊：</p> <ul style="list-style-type: none"> • Control Manager 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	<p>顯示下列資訊：</p> <ul style="list-style-type: none"> • 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。 <hr/> <p> 注意 選取「兩者都有」做為「來源」時，才會顯示此欄。</p>
受管理的產品/全部	<ul style="list-style-type: none"> • 受管理的產品：具有已過期元件的受管理產品數目 按一下「受管理的產品/全部」欄中的第一個計數，可檢視已過期受管理產品上元件版本的相關資訊。 • 全部：採用此元件的受管理產品總數 按一下「受管理的產品/全部」欄中的第二個計數，可檢視所有受管理產品上元件版本的相關資訊。 <hr/> <p> 注意 選取「受管理的產品」做為「來源」時，才會顯示此欄。</p>

資料	說明
端點/全部	<ul style="list-style-type: none"> • 端點：具有已過期元件的端點數目 按一下「端點/全部」欄中的第一個計數，可檢視已過期端點上元件版本的相關資訊。 • 全部：採用此元件的端點總數 按一下「端點/全部」欄中的第二個計數，可檢視所有端點上元件版本的相關資訊。 <hr/> <p> 注意 選取「端點」做為「來源」時，才會顯示此欄。</p>
過期率	<p>顯示具有已過期元件的受管理產品或端點的百分比</p> <hr/> <p> 注意 選取「受管理的產品」或「端點」做為「來源」時，才會顯示此欄。</p>
分級	<p>顯示具有已過期元件的受管理產品或端點的百分比</p> <hr/> <p> 注意 選取「兩者都有」做為「來源」時，才會顯示此欄。</p>

產品連線狀態 Widget

The screenshot shows two views of the '產品連線狀態' (Product Connection Status) widget. The left view is a detailed list of products, and the right view is a summary table.

狀態	伺服器	產品
異常	IWSVA01	InterScan Web Security Virtual Appliance
異常	CAS01	Cloud App Security
異常	OSCE1	OfficeScan
異常	DDH1	Deep Discovery Inspector
異常	IWSVA1	InterScan Web Security Virtual Appliance
異常	SPNT1	ServerProtect for Windows
異常	SMEX1	ScanMail for Microsoft Exchange
異常	NVW1	Network VirusWall 2500 v2
異常	WFBS01	Worry Free Business Security Services
作用中	DDES01	Trend Micro Endpoint Sensor

狀態	產品
異常	16
連線	0
作用中	2

此 Widget 會顯示所有向 Control Manager 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[記錄查詢 第 14-2 頁](#)。

如需有關受管理產品通訊及連線狀態圖示的詳細資訊，請參閱下列主題：

- [受管理產品的通訊 第 8-10 頁](#)
- [連線狀態圖示 第 10-5 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 Control Manager 伺服器的通訊

狀態	說明
離線	表示產品服務未執行，或無法建立與 Control Manager 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 Control Manager 伺服器進行通訊 如需詳細資訊，請參閱 設定受管理產品活動訊號間隔 第 8-12 頁 。

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	OfficeScan 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 OfficeScan 在與雲端儲存同步的 OfficeScan 用戶端上的本機資料夾中偵測到勒索軟體
檔案	檔案信譽評等服務偵測到勒索軟體
行為	OfficeScan 行為監控偵測到勒索軟體

DLP 事件調查標籤

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

下列是預先定義的 Widget：

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

DLP 事件趨勢 (依使用者) Widget

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

使用「範圍」下拉式清單，選取顯示的資料時間範圍。

按一下圖形中的區段來開啟「事件資訊」畫面，並檢閱事件的摘要。

按一下 Widget 上的 Widget 設定圖示可存取其他設定。

設定	說明
標題	在欄位中為 Widget 指定一個有意義的新標題。
範圍	指定觸發 DLP 事件的時間範圍。
範圍	指定 Widget 顯示的資料範圍。 <ul style="list-style-type: none"> 直接受管理的使用者 所有受管理的使用者：從直接受管理的使用者和直接受管理的使用者下屬處收集資料。
嚴重性	指定用於過濾資料的嚴重性等級。
要顯示的使用者	指定要顯示的受管理使用者數目。

按一下「儲存」以套用變更並更新 **Widget** 資料。

DLP 事件 (依嚴重性和狀態) Widget

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

使用「範圍」下拉式清單，選取顯示的資料時間範圍。

按一下任何欄中的數字來開啟「事件資訊」畫面，並檢閱事件的摘要。

若要查看特定事件，請在「事件 ID」欄位中輸入 ID，然後按一下「搜尋」。



秘訣

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

按一下 Widget 上的 Widget 設定圖示可存取其他設定。

設定	說明
標題	在欄位中為 Widget 指定一個有意義的新標題。
範圍	指定觸發 DLP 事件的時間範圍。
範圍	指定 Widget 顯示的資料範圍。 <ul style="list-style-type: none"> 直接受管理的使用者 所有受管理的使用者：從直接受管理的使用者和直接受管理的使用者下屬處收集資料
嚴重性	指定用於過濾資料的嚴重性等級。

按一下「儲存」以套用變更並更新 **Widget** 資料。

DLP 事件 (依使用者) Widget

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

使用「範圍」下拉式清單，選取顯示的資料時間範圍。

按一下任何欄中的數字來開啟「事件資訊」畫面，並檢閱事件的摘要。

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



注意

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

網域名稱不能包含下列字元：\ * + = | ; " ? < & > ,

按一下 Widget 上的 Widget 設定圖示可存取其他設定。

設定	說明
標題	在欄位中為 Widget 指定一個有意義的新標題。
範圍	指定觸發 DLP 事件的時間範圍。
範圍	指定 Widget 顯示的資料範圍。 <ul style="list-style-type: none"> 直接受管理的使用者 所有受管理的使用者：從直接受管理的使用者和直接受管理的使用者下屬處收集資料。
嚴重性	指定用於過濾資料的嚴重性等級。
要顯示的使用者	指定要顯示的受管理使用者數目。

按一下「儲存」以套用變更並更新 **Widget** 資料。

Data Loss Prevention 標籤

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

下列是預先定義的 **Widget**：

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

DLP 事件 (依通道) **Widget**

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

使用「範圍」下拉式清單，選取顯示的資料時間範圍。




使用「通道」下拉式清單來過濾出事件觸發所在通道的類型。

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

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

按一下「通道」欄中的連結或按一下圖形中的區段，會開啟顯示詳細資訊的畫面。

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

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




DLP 範本相符數 Widget

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

使用「範圍」下拉式清單，選取顯示的資料時間範圍。

按一下「範本」欄中的連結或按一下圖形中的區段，會開啟顯示詳細資訊的畫面。

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

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

前幾名 DLP 事件來源 Widget

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

使用「範圍」下拉式清單，選取顯示的資料時間範圍。

使用「顯示」下拉式清單選取要顯示的資料。

DLP 違反的策略 Widget

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

使用「範圍」下拉式清單，選取顯示的資料時間範圍。

按一下「事件」欄中的連結，會開啟顯示詳細資訊的畫面。

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

符合性標籤



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

下列是預先定義的 Widget：

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

產品應用程式符合性 Widget

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

按一下顯示圖示 ( )，可選擇要以長條圖還是資料表顯示資料。

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

資料	說明
產品	向 Control Manager 註冊的受管理產品
版本	受管理產品的版本

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

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

指定橫條圖或資料表以顯示資料。資料預設以橫條圖顯示。

按一下「編輯」存取下列選項：

- 按一下「範圍 > 瀏覽」，指定要為 **Widget** 提供資料的產品。
資料範圍可指定 **Widget** 使用哪些產品來顯示資料。這可能對此 **Widget** 顯示資訊的有用性有嚴重影響。
- 在「最新範圍」下拉式清單上，指定與最新 **Build** 之間差距幾個版本時仍應視為「最新」的產品版本數目。

按一下「儲存」以套用變更並結束。

產品元件狀態 **Widget**

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

預設檢視會顯示受 **Control Manager** 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 Control Manager 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	顯示掃描引擎的名稱
最新版本	顯示下列資訊： <ul style="list-style-type: none"> • Control Manager 所下載元件的最新版本 • 可供下載之元件（由受管理產品報告）的最新版本

資料	說明
已過期/全部	<p>顯示下列資訊：</p> <ul style="list-style-type: none"> 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。 <hr/> <p> 注意 選取「兩者都有」做為「來源」時，才會顯示此欄。</p>
受管理的產品/全部	<ul style="list-style-type: none"> 受管理的產品：具有已過期元件的受管理產品數目 按一下「受管理的產品/全部」欄中的第一個計數，可檢視已過期受管理產品上元件版本的相關資訊。 全部：採用此元件的受管理產品總數 按一下「受管理的產品/全部」欄中的第二個計數，可檢視所有受管理產品上元件版本的相關資訊。 <hr/> <p> 注意 選取「受管理的產品」做為「來源」時，才會顯示此欄。</p>
端點/全部	<ul style="list-style-type: none"> 端點：具有已過期元件的端點數目 按一下「端點/全部」欄中的第一個計數，可檢視已過期端點上元件版本的相關資訊。 全部：採用此元件的端點總數 按一下「端點/全部」欄中的第二個計數，可檢視所有端點上元件版本的相關資訊。 <hr/> <p> 注意 選取「端點」做為「來源」時，才會顯示此欄。</p>


資料	說明
過期率	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「受管理的產品」或「端點」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

產品連線狀態			產品連線狀態	
上次重新監視時間：2016-06-29 15:55			上次重新監視時間：2016-06-29 15:56	
狀態	伺服器	產品	狀態	產品
 異常	RWSVA01	InterScan Web Security Virtual Appliance	 異常	16
 異常	CAS01	Cloud App Security	 連線	0
 異常	OSCE1	OfficeScan	 作用中	2
 異常	DDI1	Deep Discovery Inspector		
 異常	RWSVA1	InterScan Web Security Virtual Appliance		
 異常	SPNT1	ServerProtect for Windows		
 異常	SMEX1	ScanMail for Microsoft Exchange		
 異常	NVW1	Network VirusWall 2500 v2		
 異常	WFBSS01	Worry Free Business Security Services		
 作用中	DDES01	Trend Micro Endpoint Sensor		

此 Widget 會顯示所有向 Control Manager 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[記錄查詢 第 14-2 頁](#)。

如需有關受管理產品通訊及連線狀態圖示的詳細資訊，請參閱下列主題：

- [受管理產品的通訊 第 8-10 頁](#)
- [連線狀態圖示 第 10-5 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 Control Manager 伺服器的通訊
離線	表示產品服務未執行，或無法建立與 Control Manager 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 Control Manager 伺服器進行通訊 如需詳細資訊，請參閱 設定受管理產品活動訊號間隔 第 8-12 頁 。

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：




- Trend Micro 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）
- OfficeScan

- 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。Control Manager 會執行隨機操作查詢來提供資訊。

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

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

安全威脅偵測標籤

「安全威脅偵測」標籤所包含的 Widget 會顯示彙整的安全威脅偵測。

下列是預先定義的 Widget：

- Control Manager 的前幾名安全威脅
- Control Manager 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

Control Manager 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 ([Bar Chart] [Table])，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 ([More] > [Edit])，可編輯 Widget 標題、產品範圍或顯示的安全威脅數目。

Control Manager 安全威脅統計資料 Widget

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

- 產品類別

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

- 安全威脅類型

資料	說明
檔案伺服器	「資料範圍」指定之任何受管理產品在檔案伺服器上偵測到的安全威脅
網路	「資料範圍」指定之任何受管理產品在您網路中偵測到的安全威脅
未知	無法識別的安全威脅
郵件	「資料範圍」指定之任何受管理產品在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
Control Manager 伺服器	「資料範圍」指定之任何受管理產品在 Control Manager 伺服器上偵測到的安全威脅

**注意**

此 Widget 一次只會顯示一種資訊類型的資料。

按一下「偵測」欄中的連結，以開啟其中顯示詳細資訊的畫面。Control Manager 會執行隨機操作查詢，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	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：

- 24 小時
- 1 週
- 2 週
- 1 個月

指定 Widget 顯示資料的方式：


- 圓餅圖
- 長條圖
- 表格式
- 折線圖

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

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

安全威脅偵測結果 Widget

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




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

此 Widget 會顯示下列安全威脅類型的安全威脅偵測：

表 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。

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

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



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


按一下「儲存」以套用變更並結束。

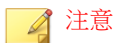
策略違規偵測 Widget

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

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

如果要變更此 Widget 顯示的資訊，請按一下  > 。

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



注意



此 Widget 僅會顯示網路病毒牆執行器偵測到的策略違規。


按一下「儲存」以套用變更並結束。

C&C 回呼事件 Widget

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

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

如果要變更此 Widget 顯示的資訊，請按一下  > 。

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

按一下「儲存」以套用變更並結束。

第 4 章

帳號管理

本節討論如何建立及管理 Control Manager 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 4-13 頁

使用者帳號

「使用者帳號」畫面提供先前針對 Control Manager 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 4-13 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	<p>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。</p> <p>如需詳細資訊，請參閱新增使用者帳號 第 4-4 頁。</p> <hr/> <p> 注意 Control Manager 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。</p> <p>如需詳細資訊，請參閱Active Directory 整合 第 6-2 頁。</p>
刪除使用者帳號	<p>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。</p> <hr/> <p> 警告! 永久刪除帳號會從 Control Manager 伺服器移除所有先前設定的帳號資訊。</p>
啟動雙因素驗證	<p>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 Control Manager。</p> <p>如需詳細資訊，請參閱啟動或關閉雙因素驗證 第 4-10 頁。</p>
關閉雙因素驗證	<p>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 Control Manager。</p> <p>如需詳細資訊，請參閱啟動或關閉雙因素驗證 第 4-10 頁。</p>

工作	說明
編輯使用者帳號	<p>按一下使用者帳號的「使用者/群組名稱」來編輯使用者資訊。</p> <p>如需詳細資訊，請參閱編輯使用者帳號 第 4-9 頁。</p>
解除鎖定使用者帳號	<p>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。</p> <p>如需詳細資訊，請參閱設定 Web 主控台設定值 第 2-6 頁。</p>
啟動使用者帳號	<p>按一下「啟動」欄中的  圖示，可啟動已關閉的帳號登入 Control Manager 主控台。</p> <hr/> <p> 注意</p> <p>您也可以編輯帳號，來啟動已關閉的帳號。</p> <p>如需詳細資訊，請參閱編輯使用者帳號 第 4-9 頁。</p>
關閉使用者帳號	<p>按一下「啟動」欄中的  圖示，可暫時阻止使用者登入 Control Manager 主控台。</p> <hr/> <p> 注意</p> <ul style="list-style-type: none"> 您也可以編輯使用者帳號，來關閉該帳號。 <p>如需詳細資訊，請參閱編輯使用者帳號 第 4-9 頁。</p> <ul style="list-style-type: none"> Control Manager 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。 <p>如需詳細資訊，請洽詢 Active Directory 管理員。</p>

Root 帳號

Control Manager 在安裝時會建立 Root 帳號。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

Control Manager 帳號只能登入 Control Manager，不能登入整個網路。Control Manager 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 Control Manager 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 Root、「管理員」或「管理員和 DLP 合規官」帳號可以建立新使用者帳號。
 - 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 Control Manager，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 2-4 頁](#)。
-

程序

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**

Control Manager 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 Control Manager 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 Control Manager 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 Control Manager Web 主控台所需提供的密碼。 <div style="border: 1px solid black; padding: 5px;">  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。 </div>
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	<p>輸入使用者接收通知的電子郵件信箱。</p> <hr/> <p> 注意</p> <ul style="list-style-type: none"> • Control Manager 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 Control Manager 透過電子郵件傳送報告和通知。 <p>如需詳細資訊，請參閱設定 SMTP 伺服器設定 第 15-3 頁。</p>

- 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**

- Control Manager 7.0 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 Control Manager。
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 Control Manager 6.0 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 Control Manager。

-
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 4-13 頁](#)。

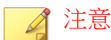
-
7. 在「選取可存取的產品/資料夾」樹狀結構中，選取使用者在「產品目錄」結構中可存取的產品或資料夾。

**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](#)。

- 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](#)。

- 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	<p>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。</p> <p>如需詳細資訊，請參閱執行受管理產品工作 第 10-8 頁。</p>
設定	<p>允許使用者帳號使用「產品目錄」畫面上的「設定」按鈕設定受管理產品設定或從 Control Manager 登入受管理產品 Web 主控台。</p> <p>如需詳細資訊，請參閱設定受管理的產品設定 第 10-9 頁。</p>

存取權限	說明
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 10-12 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 Control Manager 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 OfficeScan 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 負責監督所有的 OfficeScan 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 OfficeScan 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 Control Manager 使用者帳號允許之 OfficeScan 伺服器（行銷部門的 OfficeScan 伺服器）的適當資訊。當 Jane 登入後，她會看到所有 OfficeScan 伺服器的資訊，因為其 Control Manager 使用者帳號授與她存取所有向 Control Manager 註冊之 OfficeScan 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

- Root 帳號可以編輯 Control Manager 網路上的任何使用者帳號。指派有「管理員」或 DLP_Compliance_Officer 使用者角色的任何使用者帳號可以編輯 Control Manager 網路上的所有其他使用者帳號，但不包括 Root 帳號。
- 修改使用者帳號的存取權限，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 Control Manager 作業階段。
- 您無法變更現有帳號的使用者名稱。

程序

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 Control Manager，為使用者帳號提供額外的安全性。使用「使用者帳號」畫面可對所有 Control Manager 使用者帳號啟動或關閉雙因素驗證。



重要

Control Manager 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 15-3 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。
- 您無法從 Control Manager 主控台啟動 Trend Micro Customer Licensing Portal (CLP) 帳號的雙因素驗證。
如需詳細資訊，請參閱 Trend Micro Customer Licensing Portal 文件。
- 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 Control Manager。

程序

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 Control Manager。
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 Control Manager 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。

程序

- 移至「管理 > 帳號管理 > 我的帳號」。
會出現「我的帳號」畫面。
- 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。
密碼	輸入使用者登入 Control Manager Web 主控台所需提供的密碼。  注意 這是必填欄位。

資訊	說明
確認密碼	<p>輸入「密碼」欄位中所提供的相同密碼。</p> <hr/> <p> 注意 這是必填欄位。</p>
電子郵件信箱	<p>輸入使用者接收通知的電子郵件信箱。</p> <hr/> <p> 注意</p> <ul style="list-style-type: none"> • Control Manager 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 Control Manager 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 15-3 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 Control Manager 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 Control Manager 使用者角色。

**重要**

如果舊版 Control Manager 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 Control Manager 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 Root、管理員，以及管理員和 DLP 合規官帳號可以新增或編輯使用者角色。
- 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 4-17 頁 。
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。 <div data-bbox="428 993 481 1036" data-label="Image"></div> 注意 您無法刪除 Trend Micro Control Manager 提供的任何預設使用者角色。

工作	說明
編輯使用者角色	<p data-bbox="521 250 1161 305">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。</p> <p data-bbox="521 323 1040 349">如需詳細資訊，請參閱編輯使用者角色 第 4-19 頁。</p> <hr/> <p data-bbox="528 399 575 440"> 注意</p> <p data-bbox="585 436 1167 488">您無法編輯 Trend Micro Control Manager 提供的任何預設使用者角色。</p> <p data-bbox="585 506 1177 558">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。</p>

預設使用者角色

Control Manager 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 Control Manager 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 Root、「管理員」和「管理員和 DLP 合規官」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 4-17 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
管理員 (DLP 合規官)	<ul style="list-style-type: none"> • 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。
管理員	<ul style="list-style-type: none"> • 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 合規官	<ul style="list-style-type: none"> • 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。 <hr/> <p> 注意 此使用者角色僅適用於 Active Directory 使用者或群組。</p>
DLP 事件檢閱者	<ul style="list-style-type: none"> • 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 <hr/> <p> 注意 此使用者角色僅適用於 Active Directory 使用者或群組。</p> <hr/> <p>如需詳細資訊，請參閱下列主題：</p> <ul style="list-style-type: none"> • 報告行 第 6-12 頁 • 新增使用者帳號 第 4-4 頁
運算子	<ul style="list-style-type: none"> • 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 • 可以執行所有執行記錄查詢、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

角色	說明
進階使用者	<ul style="list-style-type: none"> • 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、產生並維護報告，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
唯讀使用者	<ul style="list-style-type: none"> • 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/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 使用者	<ul style="list-style-type: none"> • 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

舊版中的「操作員」和「進階使用者」角色，都不具有使用「策略管理」功能表項目的權限。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。

程序

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 11-2 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

Control Manager 可讓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的使用者角色資訊，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 Control Manager 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 OfficeScan 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 負責監督所有的 OfficeScan 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 OfficeScan 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 Control Manager 使用者帳號允許之 OfficeScan 伺服器（行銷部門的 OfficeScan 伺服器）的適當資訊。當 Jane 登入後，她會看到所有 OfficeScan 伺服器的資訊，因為其 Control Manager 使用者帳號授與她存取所有向 Control Manager 註冊之 OfficeScan 伺服器的權限。

程序

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 Control Manager 和受管理產品的產品使用授權。
包含下列主題：

- [Control Manager 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 5-4 頁](#)

Control Manager 啟動和使用授權資訊

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

啟動 Control Manager

在取得啟動碼後，您可以啟動 Control Manager（請向 Trend Micro 銷售人員或經銷商索取啟動碼）。



注意

不論是 Control Manager 標準版還是 Control Manager 進階版的使用授權金鑰，都允許您存取一組相同的功能。



重要

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

程序

1. 移至「管理 > 使用授權管理 > Control Manager」。
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 Control Manager Web 主控台，以使變更生效。
-

檢視和更新 Control Manager 使用授權資訊



注意

不論是 Control Manager 標準版還是 Control Manager 進階版的使用授權金鑰，都允許您存取一組相同的功能。

程序

1. 移至「管理 > 使用授權管理 > Control Manager」。
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 Control Manager 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 Control Manager 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「線上檢視使用授權資訊」。
 - 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 Control Manager 7.0、受管理產品（例如 OfficeScan、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 Control Manager 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
產品	顯示部署了啟動碼的受管理產品數目
狀態	顯示啟動碼的狀態： <ul style="list-style-type: none"> • 已啟動 • 已到期

欄名稱	說明
類型	顯示啟動碼的類型： <ul style="list-style-type: none"> 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
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。

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。

程序

- 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。
- 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。
- 在「新啟動碼」欄位中輸入您想要啟動之產品的啟動碼。
- 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。



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 Control Manager 註冊的任何產品。這可能表示受管理的產品不支援從 Control Manager 伺服器接收啟動碼。

5. 選取要部署啟動碼的受管理產品。

6. 請點選「完成」。

會出現「使用授權管理」畫面，其中資料表會列出新啟動碼。

續約受管理的產品使用授權

Control Manager 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。

程序

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. 按一下「儲存」。



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 Control Manager 註冊的任何產品。

第 6 章

Active Directory 和符合性設定

本節討論如何在 Control Manager 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 6-5 頁](#)
- [端點和使用者分組 第 6-10 頁](#)

Active Directory 整合

將 Control Manager 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「安全性作業」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 6-5 頁](#)。

設定 Active Directory 連線設定

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



注意

Control Manager 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。

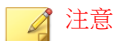
如需有關樹系信任的詳細資訊，請聯絡您的 Active Directory 管理員。



程序

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。

**注意**

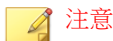
- 如果要新增其他 Active Directory 伺服器，請按一下新增圖示 ()。
- 如果要刪除 Active Directory 伺服器，請按一下刪除圖示 ()。

5. 從「同步處理，每」下拉式清單中，選取 Control Manager 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) 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。

7. 按一下「儲存」。

在設定並儲存 Active Directory 伺服器連線設定後，您可以執行下列工作：

- 按一下「立即同步處理」，以手動與 Active Directory 伺服器同步處理資料。

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

- 按一下「清除資料」，以手動從 Control Manager 資料庫清除已移除之 Active Directory 伺服器的資料。



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，該工作會從已移除的 Active Directory 伺服器清除所有資料。

Active Directory 同步處理疑難排解

Active Directory 同步處理讓 Control Manager 可以從 Active Directory 伺服器取得使用者資訊（例如站台和報告行資訊）。

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	<ul style="list-style-type: none">• 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。

問題	解決方案
無法連線到 Active Directory 伺服器	<ul style="list-style-type: none"> • 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 Control Manager 和 Active Directory 伺服器都可以建立與對方的通訊。 如果要測試 Control Manager 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」。
無法存取 Control Manager 資料庫	<p>確保已連線到 Control Manager 資料庫。</p> <p>如需詳細資訊，請參閱瞭解 Control Manager 資料庫 第 19-2 頁。</p>

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 25-1 頁](#)。

符合性指標

Control Manager 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「作業中心」資訊中心標籤上，檢視符合性指標的資訊。

- 防毒病毒碼符合性：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 OfficeScan 和 Worry-Free Business Security Services 用戶端百分比
- Data Loss Prevention 符合性：具有可接受的機密資料偵測事件數目的受管理 OfficeScan（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 Control Manager 執行符合性計算，並在「作業中心」資訊中心標籤上顯示符合性資訊。

程序

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 6-6 頁
 - [設定 Data Loss Prevention 符合性指標](#) 第 6-8 頁
3. （選用）根據 Active Directory 站台和報告行，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 6-10 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「作業中心」標籤設定。

如需詳細資訊，請參閱下列主題：

- [作業中心](#) 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「作業中心」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 OfficeScan 和 Worry-Free Business Security Services 用戶端百分比。

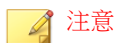
程序

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」。
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 Control Manager 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[自訂標籤和過濾器 第 7-25 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。
如需有關自訂標籤或過濾器的詳細資訊，請參閱[自訂標籤和過濾器 第 7-25 頁](#)。

- c. 選取一或多個自訂標籤或過濾器，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 Data Loss Prevention 符合性指標

您可以設定「Data Loss Prevention 符合性」指標的設定和例外，以在「作業中心」標籤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 OfficeScan（支援 Data Discovery）和 Cloud App Security 用戶端百分比。

程序

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「Data Loss Prevention」。
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。
門檻值	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 Control Manager 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[自訂標籤和過濾器 第 7-25 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。
如需有關自訂標籤或過濾器的詳細資訊，請參閱[自訂標籤和過濾器 第 7-25 頁](#)。

- c. 選取一或多個自訂標籤或過濾器，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

- 按一下「儲存」。

端點和使用者分組

Control Manager 可以根據下列資訊，將「安全性作業」標籤上的端點或使用者分組：


- 站台位置
- 報告行管理員

依預設，Control Manager 會從 Active Directory 同步處理使用者或端點站台以及報告行資訊。您可以設定自訂站台和報告行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	<p>在「執行安全狀況」Widget 上顯示的名稱</p> <hr/> <p> 注意 依預設，「其他」群組包含不屬於任何站台的端點。</p> <hr/>
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。

程序

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「執行安全狀況」Widget 上的群組。
5. 選取「節點顏色」，此顏色用來識別「執行安全狀況」Widget 上的群組。
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，Control Manager 會從清單移除原始站台。



秘訣

Control Manager 使用實心點圖示表示合併的群組。

程序

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「執行安全狀況」Widget 上的群組。
6. 選取「節點顏色」，此顏色用來識別「執行安全狀況」Widget 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。

報告行

下表說明「報告行」標籤上顯示的資訊。

表 6-2. 報告行

資料	說明
報告行層級	報告列層級會指示使用者在 Active Directory 中的管理階層層級。 從「報告行層級」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「執行安全狀況」資訊中心上顯示的名稱  注意 依預設，「其他」群組包含報告行層級高於所選層級的所有管理員。
管理員	報告行管理員 會從 Active Directory 伺服器同步處理此資訊。

建立自訂報告行

您可以建立自訂報告行，來將直接或間接向所選管理員報告的使用者分組。

程序

1. 移至「管理 > 設定 > Active Directory 和符合性設定」。
2. 按一下「報告行」標籤。
3. （選用）變更「報告行層級」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「新增自訂報告行」畫面。
5. 指定「顯示名稱」，此名稱用來識別「執行安全狀況」Widget 上的群組。
6. 選取「節點顏色」，此顏色用來識別「執行安全狀況」Widget 上的群組。
7. 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。

8. 按一下「儲存」。
建立自訂報告行後，可以執行下列作業：
 - 按一下「刪除自訂」，可刪除選取的自訂報告行。
 - 按一下自訂群組名稱，可變更設定。
-

合併報告行

您可以藉由合併兩個或更多個報告行，來建立一個自訂報告行。在合併已存在的報告行之後，Control Manager 會從清單移除原始報告行。



秘訣

Control Manager 使用實心點圖示表示合併的群組。

程序

1. 移至「管理 > 設定 > Active Directory 和符合性設定」。
 2. 按一下「報告行」標籤。
 3. 選取兩個或更多個報告行。
 4. 按一下「合併」。
會出現「合併報告行」畫面。
 5. 指定「顯示名稱」，此名稱用來識別「執行安全狀況」Widget 上的群組。
 6. 選取「節點顏色」，此顏色用來識別「執行安全狀況」Widget 上的群組。
 7. 按一下「儲存」。
在合併報告行之後，您可以按一下「分割」來分割合併的報告行。
-

第 7 章

使用者/端點目錄

本節討論如何檢視有關 Control Manager 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 7-10 頁](#)
- [Active Directory 詳細資料 第 7-16 頁](#)
- [受影響的使用者 第 7-17 頁](#)
- [使用進階搜尋 第 7-21 頁](#)
- [自訂標籤和過濾器 第 7-25 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 Control Manager 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。



「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 Control Manager 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 7-10 頁](#)。
- Active Directory：顯示整合式 Active Directory 伺服器的組織單位



Control Manager 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 7-21 頁和[自訂標籤和過濾器](#) 第 7-25 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。

使用者/端點目錄

搜尋 使用者 使用姓名編號電子郵件號碼 新增

使用者 (103)

1 個月 表格式檢視

使用者	網域	管理員	端點	端點	安全威脅
Administrator	LYNN-231283DDDE	無	1	0	0
Administrator	OSCE12	無	0	0	0
Administrator	WIN-H0F70G8T1MA	無	1	0	10
Alice	OSCE12	Terrence	0	0	0
ben	Report	無	1	0	84

- 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. 在表格格式檢視下的使用者詳細資料

欄	說明
	<p>如果端點或使用者已被指派重要性標籤，Control Manager 會顯示一個黃色星狀圖示 () 來指出重要性。</p> <p>如需詳細資訊，請參閱使用者或端點重要性 第 7-30 頁。</p>
使用者	<p>Control Manager 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。</p> <ul style="list-style-type: none"> • 伺服器 and 桌面平台：Control Manager 會將上次登入的使用者與端點關聯 • 行動裝置： <ul style="list-style-type: none"> • 如果 Active Directory 同步處理可以使用，Control Manager 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，Control Manager 會顯示行動裝置的已註冊電子郵件信箱 <p>按一下使用者名稱，可檢視聯絡詳細資料。</p> <p>如需詳細資訊，請參閱聯絡資訊 第 7-9 頁。</p> <hr/> <p> 注意</p> <p>「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。Control Manager 會從受管理產品整合具有多個本機使用者的所有端點。</p>
網域	<ul style="list-style-type: none"> • 如果 Active Directory 同步處理可以使用，此 Control Manager 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 Control Manager 會顯示使用者是其最後一個登入人員的端點/主機名稱。

欄	說明
管理員	<p>如果 Active Directory 同步處理可以使用，Control Manager 會顯示使用者的管理員</p> <p>按一下「管理員」欄中的名稱，可檢視管理員的聯絡詳細資料。</p> <p>如需詳細資訊，請參閱聯絡資訊 第 7-9 頁。</p>
端點	<p>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）</p> <p>按一下計數，可檢視資料表中的相關端點資訊。</p> <p>如需詳細資訊，請參閱端點詳細資料 第 7-10 頁。</p>
策略	<p>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）</p> <p>按一下「策略」計數，可檢視使用者的相關策略資訊。</p> <p>如需詳細資訊，請參閱策略狀態 第 7-8 頁。</p>
安全威脅	<p>在與使用者關聯的端點上發生的安全威脅總數</p> <p>按一下「安全威脅」計數，可檢視使用者的相關安全威脅資訊。</p> <p>如需詳細資訊，請參閱使用者所面臨的安全威脅 第 7-6 頁。</p> <p>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 個偵測到的病毒/惡意程式和 2 個網頁違規，則 Henry 的「安全威脅」數目會顯示為 12 個。</p> <hr/> <p> 注意</p> <ul style="list-style-type: none"> 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 OfficeScan）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	Control Manager 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 。
<時間表>	時間表會指出每個使用者的安全威脅發生時間。 <ul style="list-style-type: none"> 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 Control Manager 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。

< Administrator

安全威脅 業務狀態 聯絡資訊

端點的安全威脅

縮放 1天 1週 2週 1個月

2018-05-28 ~ 2018-06-27

WIN-HOF70G8T1MA



WIN-HOF70G8T1MA Administrator

五月 28 五月 30 六月 1 六月 3 六月 5 六月 7 六月 9 六月 11 六月 13 六月 15 六月 17 六月 19 六月 21 六月 23 六月 25 六月 27

四月 9 四月 23 五月 7 五月 21 六月 4 六月 18

安全威脅詳細資訊

安全威脅	類別	權監源位/電子郵件主	處理行動	端點	記錄者	時間	詳細資訊
7.zip.dll	應用程式邊境	7.zip	已封鎖	WIN-HOF70G8T1MA	Trend Micro Endpoint ...	2018/06/20 15:10:03	檢視
7zG.exe	應用程式邊境	7.zip	已封鎖	WIN-HOF70G8T1MA	Trend Micro Endpoint ...	2018/06/20 15:08:42	檢視
7z.exe	應用程式邊境	7.zip	已封鎖	WIN-HOF70G8T1MA	Trend Micro Endpoint ...	2018/06/20 15:08:34	檢視
7z.exe	應用程式邊境	7.zip	已封鎖	WIN-HOF70G8T1MA	Trend Micro Endpoint ...	2018/06/20 15:04:54	檢視
7zG.exe	應用程式邊境	7.zip	已封鎖	WIN-HOF70G8T1MA	Trend Micro Endpoint ...	2018/06/20 15:04:42	檢視
7zFM.exe	應用程式邊境	7.zip	已封鎖	WIN-HOF70G8T1MA	Trend Micro Endpoint ...	2018/06/20 15:04:35	檢視
7-zip.dll	應用程式邊境	7.zip	已封鎖	WIN-HOF70G8T1MA	Trend Micro Endpoint ...	2018/06/20 15:04:09	檢視

- 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 Control Manager 策略，以及各個已安裝產品的目前策略狀態。

**注意**

Control Manager 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。

聯絡資訊	
標題:	Engineer
部門:	Developer
辦公室:	Taipei
管理員:	[REDACTED]
辦公室號碼:	[REDACTED]
住家號碼:	[REDACTED]
電子郵件信箱:	ann@tr.com
網域:	OSCE12

將聯絡資訊與 Active Directory 同步處理

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

程序

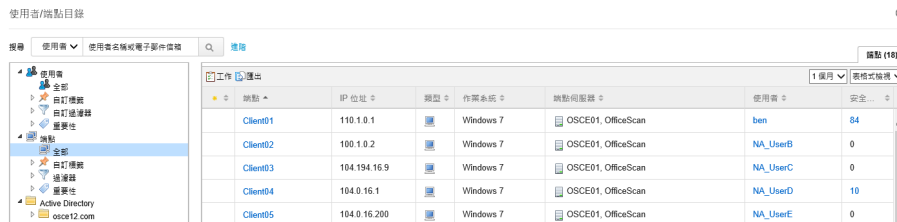
1. 開啟 Microsoft Management Console (MMC)。

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。

使用者/端點目錄



The screenshot shows a web interface for 'Users/Endpoints'. On the left is a navigation tree with categories like '全部', '自訂標籤', '屬性', and 'Active Directory'. The main area displays a table with columns: '端點', 'IP 位址', '類型', '作業系統', '端點伺服器', '使用者', and '安全...'. The table contains five rows of data for Client01 through Client05.



端點	IP 位址	類型	作業系統	端點伺服器	使用者	安全...
Client01	110.1.0.1	藍	Windows 7	OSCE01, OfficeScan	ben	84
Client02	100.1.0.2	藍	Windows 7	OSCE01, OfficeScan	NA_UserB	0
Client03	104.194.16.9	藍	Windows 7	OSCE01, OfficeScan	NA_UserC	0
Client04	104.0.16.1	藍	Windows 7	OSCE01, OfficeScan	NA_UserD	10
Client05	104.0.16.200	藍	Windows 7	OSCE01, OfficeScan	NA_UserE	0

- 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， Control Manager 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 7-30 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 7-15 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	在電腦或裝置上執行的作業系統：支援的 Windows 桌面/伺服器系統、 Mac OS 、 iOS 、 Android 、 Symbian 及 Windows Mobile
網域	如果已啟動 Active Directory 整合，這會對應到網域名稱
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 7-9 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 7-13 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	<p>主機名稱或裝置名稱</p> <p>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。</p> <p>如需詳細資訊，請參閱策略狀態 第 7-15 頁。</p>
安全威脅	<p>在端點上發生的安全威脅總數</p> <p>按一下「安全威脅」計數，可檢視端點的相關安全威脅資訊。</p> <p>如需詳細資訊，請參閱端點上的安全威脅 第 7-13 頁。</p>
<時間表>	<p>時間表會指出每個端點的安全威脅發生時間。</p> <ul style="list-style-type: none"> 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。 <p>如需詳細資訊，請參閱端點上的安全威脅 第 7-13 頁。</p>

端點 - [名稱] 資訊

「端點」畫面提供有關所選端點的更多詳細資訊。請按一下某個標籤來檢視相關資訊。

- 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 7-13 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 7-15 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 7-16 頁](#)。

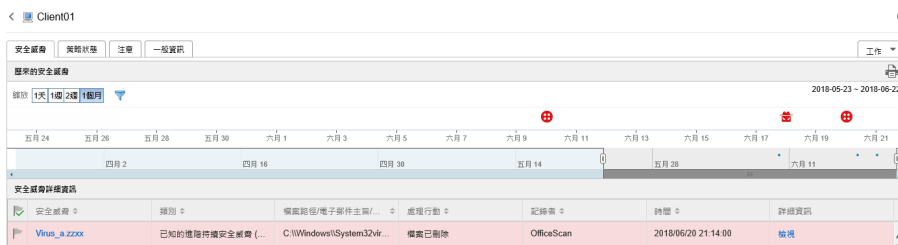
「端點」畫面也可讓您使用「工作」功能表，對所選端點採取特定的處理行動。

- 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 第 7-26 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 17-24 頁](#)。
- 恢復：恢復對已離隔端點的網路存取權限




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 Control Manager 主控台的「資訊中心 > 摘要」標籤或「受影響的使用者」畫面上的「具有安全威脅的端點」Widget 存取此畫面。



- 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[對受影響的使用者進行影響評估 第 7-19 頁](#)和[隔離端點 第 17-24 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 Control Manager 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。

Control Manager 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」

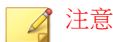
- 「指派標籤 {標籤名稱}」
- 「移除標籤 {標籤名稱}」

如需詳細資訊，請參閱[將自訂標籤指派給使用者/端點](#) 第 7-27 頁和[隔離端點](#) 第 17-24 頁。

端點的一般資訊

您可以檢視有關端點的下列資訊：

- IP 位址
- 類型
- 作業系統
- 使用者



Control Manager 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。

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 7-10 頁。

受影響的使用者

「安全威脅資訊」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」畫面上的「安全威脅」標籤中，透過按一下資料表中的安全威脅名稱來存取此畫面。



- 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「評估影響」可執行詳細的記錄檔分析，從而判斷安全威脅是否存在於端點上，但先前並未偵測到。



重要

如果要從「安全威脅資訊」畫面執行影響評估，需要將 Endpoint Sensor 1.5（或更新版本）和 Deep Discovery Inspector 3.8（或更新版本）向 Control Manager 註冊。

如需詳細資訊，請參閱[對受影響的使用者進行影響評估](#) 第 7-19 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評估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。

< 安全威脅 — PE_RAMNIT.DEN

受影響的使用者

一般資訊

名稱:	PE_RAMNIT.DEN
類型:	惡意程式
以下項目的變種:	RAMNIT 家庭
損害可能性:	■ 中
散佈可能性:	■ 低
最早引擎版本:	8.900
首次在全球發現:	2012/01/01 08:00:03
上次在全球發現:	2018/06/26 07:20:53
受影響最大的國家/地區:	Vietnam,India,Philippines

This File infector executes the dropped file(s). As a result, malicious routines of the dropped files are exhibited on the affected system.


[檢視 Threat Connect 的詳細資訊](#)

對受影響的使用者進行影響評估

在 Control Manager 的「受影響的使用者」畫面中，您可以對您環境中的安全威脅執行完整或部分歷史影響評估。

Deep Discovery Inspector 會根據趨勢科技回溯掃描所收集的歷史網路流量記錄資訊，來評估可疑 URL、IP 位址和網域的影響。

Endpoint Sensor 會透過聯絡用戶端並對用戶端記錄檔執行歷史掃描，來評估您環境中可疑檔案、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。

CONTROL MANAGER 版本	受管理的產品
<p>執行影響評估需要下列版本的 Control Manager :</p> <ul style="list-style-type: none"> Control Manager 7.0 (或更新版本) 	<p>Control Manager 需要至少下列其中一項產品，才能執行影響評估。</p> <ul style="list-style-type: none"> Endpoint Sensor 1.5 (或更新版本) Deep Discovery Inspector 3.8 (或更新版本) <hr/> <p> 重要 必須在 Deep Discovery Inspector 中啟動「回溯掃描」，才能執行影響評估。</p>

程序

1. 在 Control Manager 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。



秘訣

您可以使用「檔案路徑/電子郵件主旨/規則名稱」欄辨識可疑物件偵測項目。任何由「沙盒虛擬平台」或「使用者定義的」清單偵測到的項目，都屬於可疑物件。

會出現「受影響的使用者」畫面。

4. 按一下「評估影響」。

Deep Discovery Inspector 和 Endpoint Sensor (如果可用) 會掃描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 [Deep Discovery Inspector](#) 中的回溯掃描 第 7-21 頁和 [Endpoint Sensor](#) 中的回溯掃描 第 17-16 頁。

Deep Discovery Inspector 中的回溯掃描

回溯掃描是以雲端為基礎的服務，這項服務會掃描歷史 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。

回溯掃描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

回溯掃描會接著定期掃描儲存的記錄項目，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：回溯掃描也會掃描記錄檔，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「回溯掃描」畫面只會顯示有關使用趨勢科技全球資訊清單的掃描資訊。

使用進階搜尋

Control Manager 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。

程序

- 移至「目錄 > 使用者/端點」。
會出現「使用者/端點目錄」畫面。
- 按一下資料表上方的「進階」連結。
- 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 7-23 頁](#)。
- 使用過濾器右側的布林運算子新增多個搜尋條件。
- 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：

使用者/端點目錄

The screenshot shows a search interface for 'Users/Endpoints'. It features a search bar with a dropdown menu set to '使用者' (Users) and a text input field containing 'ja'. Below this, there are several filter rows:

- A row with 'AND' operator, a dropdown for '部門' (Department) set to 'Finance', and a text input field containing 'Mary'.
- A row with 'AND' operator, a dropdown for '直屬主管' (Direct Supervisor) set to 'Bill', and a text input field containing 'Mary'.
- A row with 'OR' operator, a dropdown for '在 Active Directory 中的位置' (Location in Active Directory) set to 'osce12.com', and a text input field containing 'HR'.

Each filter row has a small 'X' icon and the label 'OR' or 'AND' to the right, indicating the logical relationship between the filters.

- 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 7-27 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

類別	說明
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 7-30 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 6-10 頁。
報告行	從 Active Directory 同步處理的報告行顯示名稱 如需詳細資訊，請參閱 端點和使用者分組 第 6-10 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 位址中包含該項目的所有端點。
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	作業系統類型：Windows XP、Windows Vista、Windows 7、Windows 8、Windows 10、Windows 2000、Windows 2003、Windows 2008、Windows 2012、Windows 2016、Mac OS、iOS、Android、Symbian、Windows Mobile 或其他
在 Active Directory 中的位置	開始對其搜尋的組織單位

類別	說明
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 7-13 頁 。
符合性	防毒病毒碼符合性或 Data Loss Prevention 符合性狀態 如需詳細資訊，請參閱 符合性指標 第 6-5 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 7-30 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 6-10 頁 。
報告行	從 Active Directory 同步處理的報告行顯示名稱 如需詳細資訊，請參閱 端點和使用者分組 第 6-10 頁 。
安裝模式	OfficeScan 用戶端功能集（「完整功能集」或「共存」模式） 如需詳細資訊，請參閱 下載 Security Agent 安裝套件 第 9-2 頁 。

自訂標籤和過濾器

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



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：

- [記錄查詢 第 14-2 頁](#)
 - [使用者存取資訊 第 B-99 頁](#)
-

自訂標籤

「自訂標籤」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，Control Manager 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套用至多個使用者/端點。
- 所有有權存取「使用者/端點目錄」的使用者都可以建立及檢視自訂標籤，但只有建立自訂標籤的使用者可以刪除或修改標籤。



重要

在 Control Manager 安裝期間建立的管理員帳號擁有所有自訂標籤的完全控制權，因此可以刪除或修改任何使用者建立的標籤。

建立自訂標籤

程序

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」節點。

3. 按一下「新增自訂標籤」。
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。

建立自訂標籤後，可以執行下列作業：

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

將自訂標籤指派給使用者/端點

程序

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」。
 - 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」。
4. 在「指派/移除自訂標籤」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」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。

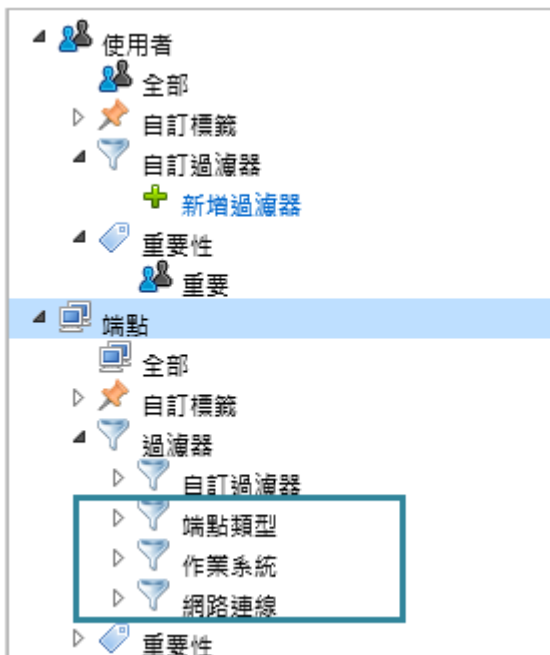
如需詳細資訊，請參閱[建立自訂過濾器](#) 第 7-29 頁和[使用者或端點重要性](#) 第 7-30 頁。

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 7-28 頁。

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：手動隔離的端點



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

程序

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 w12p.tcm.co 中的所有 Ja 使用者：

使用者/端點目錄

搜尋	使用者	使用者名稱	ja	×	OR	
	AND	部門	Finance	×	OR	
	AND	直屬主管	Mary	×	OR	
			OR	×	OR	
	AND	在 Active Directory 中的位置	osce12.com	HR	×	OR AND

如需詳細資訊，請參閱[進階搜尋類別](#) 第 7-23 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。Control Manager 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」上提供最佳的可見性。

如需詳細資訊，請參閱[自訂標籤和過濾器](#) 第 7-25 頁。

注意

- 依預設，系統會將重要性指派給「網域管理員」（使用者）和「網域控制站」（端點）。
- 手動將重要性指派給使用自訂標籤和過濾器分組的使用者/端點。
- 所有可以存取「使用者/端點目錄」的使用者都可以指派或移除重要性。

程序

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 Control Manager 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

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

- Control Manager 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 Control Manager 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 Control Manager 管理主控台註冊、設定受管理產品，或取消註冊已向 Control Manager 註冊的受管理產品。

如需有關使用受管理產品 Web 主控台向 Control Manager 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 17-26 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	<p>按一下「新增」，即可向 Control Manager 伺服器註冊受管理的產品。</p> <p>如需詳細資訊，請參閱新增受管理的伺服器 第 8-4 頁。</p> <hr/> <p> 注意</p> <p>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 Control Manager 註冊。</p>
編輯受管理的伺服器設定	<p>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。</p> <p>如需詳細資訊，請參閱編輯受管理的伺服器 第 8-6 頁。</p>


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 Control Manager 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 8-7 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 8-9 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 使用目錄管理 第 10-13 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 Control Manager 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。

欄名稱	說明
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	<p>顯示受管理產品如何向 Control Manager 註冊</p> <ul style="list-style-type: none"> 自動：受管理產品透過 MCP 代理程式向 Control Manager 註冊。 如需詳細資訊，請參閱連線的威脅防範產品整合 第 17-26 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 8-9 頁。
上次報告	顯示 Control Manager 最近一次從受管理產品收到回應的日期和時間
處理行動	<ul style="list-style-type: none"> 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 **Control Manager** 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 Control Manager 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 17-26 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[使用目錄管理 第 10-13 頁](#)。

程序

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）。
 - 顯示名稱：指定 Control Manager 中顯示的 <受管理的產品> 伺服器名稱。
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**

Control Manager 需要具有管理員權限的帳號，才能部署策略設定。

6. 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 8-7 頁](#)。

7. 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 Control Manager 伺服器註冊的受管理伺服器資訊。

程序

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 8-7 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 Control Manager 取消註冊。

程序

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. 按一下要移除之受管理伺服器的「處理行動」欄中的「刪除」圖示。
4. 請點選「確定」。

Control Manager 會將已刪除的伺服器取消註冊。



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。

設定受管理產品的 Proxy 伺服器設定

Control Manager 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。

程序

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 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 Control Manager 註冊或取消註冊。

程序

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://tm.login.trendmicro.com/simplesaml/saml2/idp/SSOService.php>) 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 Control Manager 管理服务」，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

Control Manager 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 Control Manager 管理主控台向 Control Manager 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 Control Manager 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 Control Manager 伺服器。



重要

Control Manager 僅允許為透過 Control Manager 管理主控台向 Control Manager 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

Control Manager 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。

程序

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. 按一下時段來變用戶端通訊狀態。

**注意**

- 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 Control Manager 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 Control Manager 伺服器。

4. 按一下「儲存」。

設定用戶端通訊預約時程

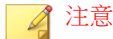
您可以在「設定通訊器預約時程」畫面上按一下某個時段來變更通訊狀態，即可自訂受管理產品的用戶端通訊預約時程。

**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。

程序

- 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。
- 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。
- 按一下某個時段以變更通訊狀態。

**注意**

- 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 Control Manager 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 Control Manager 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 Control Manager 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 Control Manager 管理主控台向 Control Manager 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 Control Manager 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情況。

程序

- 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」。
-

停止並重新啟動 Control Manager 服務

使用 Windows 的「服務」畫面來重新啟動下列任何 Control Manager 服務：

- 趨勢科技管理基礎架構
- Trend Micro Control Manager

**注意**

- 這些是 Windows 作業系統上在背景中執行的服務，並非是需要啟動碼的 Trend Micro 服務（例如，病毒爆發防範服務）。
 - 下列程序假設您在 Windows Server 2008 R2 上執行 Control Manager。
-

程序

1. 移至「開始 > 所有程式 > 系統管理工具 > 服務」。
會出現「服務」畫面。

2. 如果要停止 Control Manager 服務，請執行下列作業：
 - a. 以滑鼠右鍵按一下「<Control Manager 服務>」。
會出現快顯功能表。
 - b. 請點選「停止」。
 3. 如果要重新啟動 Control Manager 服務，請執行下列作業：
 - a. 以滑鼠右鍵按一下「<Control Manager 服務>」。
會出現快顯功能表。
 - b. 請點選「開始」。
-

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](#)
- [OfficeScan 用戶端安裝 第 9-4 頁](#)
- [OfficeScan SaaS 用戶端系統需求 第 9-22 頁](#)
- [Trend Micro Security \(適用於 Mac\) 用戶端安裝 第 9-47 頁](#)
- [Trend Micro Security \(適用於 Mac\) SaaS 用戶端安裝 第 9-52 頁](#)

下載 Security Agent 安裝套件

在「Security Agent 下載」畫面中，您可以從 Control Manager 主控台建立 OfficeScan 或 Trend Micro Security (適用於 Mac) 的 Security Agent 安裝套件。您可以使用此畫面從本機下載及安裝 Security Agent 套件，或是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。

表 9-1. 安裝前組態設定

SECURITY AGENT	組態設定
OfficeScan	<p>在安裝 OfficeScan 用戶端之前：</p> <ul style="list-style-type: none"> 變更預設的 OfficeScan 用戶端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 OfficeScan 用戶端 Proxy 伺服器設定（如果需要）
Trend Micro Security (適用於 Mac)	<p>在安裝 Trend Micro Security (適用於 Mac) 用戶端之前：</p> <ul style="list-style-type: none"> 確保端點可以透過通訊埠 61617 進行通訊 <hr/> <p> 注意 對於 Trend Micro Security (適用於 Mac) SaaS 用戶端，請確定端點可透過通訊埠 8443 進行通訊。</p> <hr/> <ul style="list-style-type: none"> 確保端點可以存取 *.trendmicro.com 設定 OfficeScan 用戶端 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：

- [OfficeScan 用戶端安裝 第 9-4 頁](#)
- [OfficeScan SaaS 用戶端系統需求 第 9-22 頁](#)
- [Trend Micro Security \(適用於 Mac\) 用戶端安裝 第 9-47 頁](#)
- [Trend Micro Security \(適用於 Mac\) SaaS 用戶端安裝 第 9-52 頁](#)

程序

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 OfficeScan 用戶端的 64 位元 MSI 安裝套件
 - Windows 32 位元：選取此選項可建立用於 OfficeScan 用戶端的 32 位元 MSI 安裝套件
 - Mac OS：選取此選項可建立用於 Trend Micro Security (適用於 Mac) 用戶端的 ZIP 安裝套件
3. 若要進行「OfficeScan 即服務」用戶端安裝，請選取「安裝模式」：
 - 完整功能集：安裝包含完整功能的標準 OfficeScan 用戶端
 - 共存：共存模式 OfficeScan 用戶端提供有限的 OfficeScan 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：
 - 下載用戶端：從管理產品伺服器下載 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 OfficeScan 伺服器，OfficeScan 用戶端套件會套用「用戶端封裝工具」上次執行時產生的設定。

如需詳細資訊，請參閱《OfficeScan 即服務管理手冊》。

OfficeScan 用戶端安裝

本部分簡述所支援的 Windows 平台上進行全新安裝的 OfficeScan 用戶端系統需求。

- [Windows 端點平台的全新安裝 第 9-4 頁](#)
- [Windows Embedded 系統平台的全新安裝 第 9-9 頁](#)
- [Windows Server 平台的全新安裝 第 9-13 頁](#)
- [更新代理程式 第 9-21 頁](#)

Windows 端點平台的全新安裝





重要

趨勢科技僅保證在 2019 年 1 月 30 日之前為 Windows XP 平台提供持續支援。若要在所有端點上繼續獲得最高層級的安全性，請準備移轉計劃。

作業系統		版本	SER VICE PAC K	處理器	RAM	可用 磁碟 空間	其他
Windows XP	32 位 元	Home	SP3	300MHz Intel Pentium 或同級處 理器 AMD™ 64 處理 器 Intel 64 處理器	至少 256MB (至少 100MB 專用 於 OfficeScan) 建議使用 512MB 的處 理器	至少 800M B 建議 使用 1GB 的處 理器	支援 1024 x 768 解析度 (256 色) 或 以上的顯示器 Microsoft Internet Explorer 8.0 或 9.0 (如果 執行 Web 安 裝) 關閉「簡易檔 案共用」 啟動遠端登錄 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
		Professio nal					
	Professio nal for Embed ded Systems						
	Tablet PC						
	64 位 元	Professio nal	SP2				

作業系統		版本	SERVICE PACK	處理器	RAM	可用磁碟空間	其他
Windows 7	32 位元/64 位元	Home Basic	含/不含 SP1	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	至少 1GB (32 位元) / 1.5GB (64 位元) (至少 100MB 專用於 OfficeScan) 建議使用 2 GB 的處理器	至少 800MB 建議使用 1GB 的處理器	支援 1024 x 768 解析度 (256 色) 或以上的顯示器 Microsoft Internet Explorer 8.0 或 9.0 (如果執行 Web 安裝) 關閉「簡易檔案共用」 啟動遠端登錄 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
		Home Premium					
		Ultimate					
		Professional					
		Enterprise					
		Professional for Embedded Systems					
		Ultimate for Embedded Systems					
Thin PC							

作業系統		版本	SERVICE PACK	處理器	RAM	可用磁碟空間	其他
Windows 8/8.1	32 位元/64 位元	Standard	無	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	至少 1GB (32 位元) / 1.5GB (64 位元) (至少 100MB 專用於 OfficeScan) 建議使用 2 GB 的處理器	至少 800MB 建議使用 1GB 的處理器	支援 1024 x 768 解析度 (256 色) 或以上的顯示器 Windows Internet Explorer 10.0 (如果要執行 Web 安裝) 啟動遠端登錄 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 <hr/>  注意 不支援 Windows UI。
		Pro					
		Enterprise					

作業系統		版本	SERVICE PACK	處理器	RAM	可用磁碟空間	其他
Windows 10	32 位元/64 位元	Home	無	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	至少 1GB (32 位元) / 2GB (64 位元) (至少 100MB 專用於 OfficeScan) 建議使用 2 GB 的處理器	至少 800MB 建議使用 1GB 的處理器	支援 1024 x 768 解析度 (256 色) 或以上的顯示器 Windows Internet Explorer 11.0 (如果要執行 Web 安裝) 啟動遠端登錄 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 <hr/>  注意 不支援 Windows UI。
		Pro					
		Education					
		Enterprise					

Windows Embedded 系統平台的全新安裝

作業系統		版本	SER VICE PAC K	處理器	RAM	可用磁碟空間	其他
Windows XP Embedded Standard	32 位元	無	SP1 / SP2 / SP3	300MHz Intel Pentium 或同級處理器	至少 256MB (至少 100MB 專用於 OfficeScan)	至少 800MB 建議使用 1GB 的處理器	支援 1024 x 768 解析度 (256 色) 或以上的顯示器 Microsoft Internet Explorer 8.0 或 9.0 (如果執行 Web 安裝) 關閉「簡易檔案共用」 啟動遠端登錄 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 Embedded Standard 2009	32 位元	無	無	AMD™ 64 處理器	建議使用 512MB 的處理器		
Windows Embedded POSReady 2009	32 位元	無	無				

作業系統		版本	SERVICE PACK	處理器	RAM	可用磁碟空間	其他
Windows Embedded POSReady 7	32 位元/64 位元	無	無	至少 1GHz (32 位元) / 2GHz (64 位元)	至少 1GB (32 位元) / 1.5GB (64 位元) (至少 100MB 專用於 OfficeScan)	至少 800MB 建議使用 1GB 的處理器	支援 1024 x 768 解析度 (256 色) 或以上的顯示器 Microsoft Internet Explorer 8.0 或 9.0 (如果執行 Web 安裝) 關閉「簡易檔案共用」 啟動遠端登錄 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 7 Embedded	32 位元/64 位元	Standard	SP1	Intel Pentium 或同級處理器 (建議使用 2GHz) AMD™ 64 處理器 Intel 64 處理器	建議使用 2 GB 的處理器		
		Professional					
		Ultimate					

作業系統		版本	SERVICE PACK	處理器	RAM	可用磁碟空間	其他
Windows 8 Embedded	32 位元/64 位元	Standard	無	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	至少 1GB (32 位元) / 1.5GB (64 位元) (至少 100MB 專用於 OfficeScan) 建議使用 2 GB 的處理器	至少 800MB 建議使用 1GB 的處理器	支援 1024 x 768 解析度 (256 色) 或以上的顯示器 Microsoft Internet Explorer 8.0 或 9.0 (如果執行 Web 安裝) 關閉「簡易檔案共用」 啟動遠端登錄 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
		Pro					
		Industry Enterprise					
		Industry Pro					

作業系統		版本	SERVICE PACK	處理器	RAM	可用磁碟空間	其他
Windows 8.1 Embedded	32 位元/64 位元	Pro	無	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	至少 1GB (32 位元) / 1.5GB (64 位元) (至少 100MB 專用於 OfficeScan) 建議使用 2 GB 的處理器	至少 800MB 建議使用 1GB 的處理器	支援 1024 x 768 解析度 (256 色) 或以上的顯示器 Microsoft Internet Explorer 8.0 或 9.0 (如果執行 Web 安裝) 關閉「簡易檔案共用」 啟動遠端登錄 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
		Industry Enterprise					
		Industry Pro					
Windows 10 IoT Embedded	32 位元/64 位元	Enterprise	無				

 注意

- OfficeScan 用戶端支援安裝有特定核心元件的 Windows Embedded 系統。如需 Windows Embedded 系統所需元件的詳細資訊，請參閱趨勢科技常見知識庫 (<http://esupport.trendmicro.com/solution/zh-TW/1105117.aspx>)。
- 由於 Windows Embedded 系統的複雜性，OfficeScan 可能無法支援所有選用的 Windows 元件。如果您在組合使用選用元件時發生不相容的情況，請聯絡您的技術支援小組。

Windows Server 平台的全新安裝



重要

趨勢科技僅保證在 2018 年 1 月 30 日之前為 Windows Server 2003 平台提供持續支援。若要在所有端點上繼續獲得最高層級的安全性，請準備移轉計劃。

作業系統		版本	SER VICE PAC K	處理器	RAM	可用磁碟空間	其他
Windows Server 2003	32 位 元/64 位元	Standar d	SP2	300MHz Intel Pentium 或同級 處理器 AMD™ 64 處理 器	至少 256MB (至 少 100MB 專用於 OfficeScan) 建議使用 512MB 的 處理器	至少 800MB 建議使用 1GB 的處理 器	支援 1024 x 768 解析度 (256 色) 或以上的顯 示器 Microsoft Internet Explorer 8.0 或 9.0 (如果執行 Web 安裝) 啟動遠端登 錄 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
		Enterpri se					
		Datacen ter					
		Web					
Windows Server 2003 R2		Standar d	SP2				
		Enterpri se					
		Datacen ter					
Windows Storage Server 2003		Basic	SP2				
		Standar d					
		Enterpri se					
		Workgro up					

作業系統		版本	SERVICE PACK	處理器	RAM	可用磁碟空間	其他
Windows Storage Server 2003 R2		Basic	SP2				
		Standard					
		Enterprise					
		Workgroup					
Windows Compute Cluster Server 2003 (主動/被動)		無	無				
Windows Server 2008	32 位元	Standard	SP2	至少 1GHz 的 Intel Pentium 或同級處理器 (建議使用 2GHz) AMD™ 64 處理器	至少 512MB (至少 100MB 專用於 OfficeScan) 建議使用 2 GB 的處理器	至少 800MB 建議使用 1GB 的處理器	支援 1024 x 768 解析度 (256 色) 或以上的顯示器 Microsoft Internet Explorer 8.0 或 9.0 (如果執行 Web 安裝) 啟動遠端登錄 允許透過 Windows 防火牆 (如果已啟動) 進行印表機/檔案共用
		Enterprise					
		Datacenter					
		Web					
		Server Core					
Windows Storage Server 2008		Basic	SP2	Intel 64 處理器			
Windows HPC		無	無				

作業系統		版本	SER VICE PAC K	處理器	RAM	可用磁碟空間	其他
Server 2008							啟動預設的本機 admin
Windows Server 2008 容錯移轉叢集（主動/被動）		無	無				
Windows Server 2008	64 位元	Standard	SP2	至少 1.4GHz 的 Intel Pentium 或同級處理器（建議使用 2GHz） AMD™ 64 處理器	至少 512MB（至少 100MB 專用於 OfficeScan）	至少 800MB 建議使用 1GB 的處理器	支援 1024 x 768 解析度（256 色）或以上的顯示器 Microsoft Internet Explorer 8.0 或 9.0（如果執行 Web 安裝） 啟動遠端登錄
		Enterprise					
		Datacenter					
		Web					
		Server Core					
Windows Server 2008 R2		Standard	SP1	Intel 64 處理器			允許透過 Windows 防火牆（如果已啟動）進行印表機/檔案共用
		Enterprise					
		Datacenter					
		Web					
		Server Core					
Windows Storage		Basic	SP2				啟動預設的本機 admin

作業系統		版本	SERVICE PACK	處理器	RAM	可用磁碟空間	其他
Server 2008		Standard					
		Enterprise					
		Workgroup					
Windows Storage Server 2008 R2		Basic	SP1				
		Standard					
		Enterprise					
		Workgroup					
Windows HPC Server 2008	64 位元	無	無	至少 1.4GHz 的 Intel Pentium 或同級處理器 (建議使用 2GHz)	至少 512MB (至少 100MB 專用於 OfficeScan)	至少 800MB 建議使用 1GB 的處理器	支援 1024 x 768 解析度 (256 色) 或以上的顯示器 Microsoft Internet Explorer 8.0 或 9.0 (如果執行 Web 安裝) 啟動遠端登錄 允許透過 Windows 防火牆 (如果已啟動) 進
Windows HPC Server 2008 R2		無	無				
Windows Server 2008 容錯移轉叢集 (主動/被動)		無	無				

作業系統	版本	SER VICE PAC K	處理器	RAM	可用磁碟空間	其他	
						行印表機/檔案共用 啟動預設的本機 admin	
Windows MultiPoint Server 2010	64 位 元	無	無	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	至少 512MB (至 少 100MB 專用於 OfficeScan)	至少 800MB 建議使用 1GB 的處理 器	支援 1024 x 768 解析度 (256 色) 或以上的顯 示器 Microsoft Internet Explorer 8.0 或 9.0 (如果執行 Web 安裝) 啟動遠端登 錄 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		Standar d	無				
Windows Server 2012	64 位 元	Standar d	無	至少 1.4GHz 的 Intel Pentium 或同級 處理器 (建議 使用 2GHz)	至少 512MB (至 少 100MB 專用於 OfficeScan)	至少 800MB 建議使用 1GB 的處理 器	支援 1024 x 768 解析度 (256 色) 或以上的顯 示器 Windows Internet Explorer 10.0 (如果
		Datacen ter					
		Server Core					

作業系統		版本	SERVICE PACK	處理器	RAM	可用磁碟空間	其他
Windows Server 2012 R2	Standard	無	AMD™ 64 處理器 Intel 64 處理器				要執行 Web 安裝) 啟動遠端登錄 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
	Datacenter						
	Server Core						
Windows Storage Server 2012	Standard	無					啟動預設的本機 admin
	Workgroup						
Windows Storage Server 2012 R2	Standard	無					 注意 不支援 Windows UI。
	Workgroup						
Windows MultiPoint Server 2012	Standard	無					
	Premium						
Windows Server 2012 容錯移轉叢集	無	無					
Windows Server 2012 R2 容錯移轉叢集	無	無			至少 512MB (至少 100MB 專用於 OfficeScan)		

作業系統	版本	SER VICE PAC K	處理器	RAM	可用磁碟空間	其他	
					建議使用 2 GB 的處理器		
Windows Server 2016	64 位元	Standard	無	至少 1.4GHz 的 Intel Pentium 或同級處理器 (建議使用 2GHz)	至少 512MB (至少 100MB 專用於 OfficeScan) 建議使用 2 GB 的處理器	至少 800MB 建議使用 1GB 的處理器	支援 1024 x 768 解析度 (256 色) 或以上的顯示器 Windows Internet Explorer 11.0 (如果要執行 Web 安裝) 啟動遠端登錄 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
		Datacenter					
Windows Server 2016 容錯移轉叢集		Server Core	無	AMD™ 64 處理器 Intel 64 處理器			
		無					
Windows Storage	64 位元	Standard	無	至少 1.4GHz 的 Intel	至少 512MB (至少 100MB)	至少 800MB	支援 1024 x 768 解析度 (256 色)



注意

不支援 Windows UI。

作業系統		版本	SER VICE PAC K	處理器	RAM	可用磁碟空 間	其他
Server 2016		Workgro up		Pentium 或同級 處理器 (建議 使用 2GHz) AMD™ 64 處理 器 Intel 64 處理器	專用於 OfficeScan) 建議使用 2 GB 的處理 器	建議使用 1GB 的處理 器	或以上的顯 示器 Windows Internet Explorer 11.0 (如果 要執行 Web 安裝) 啟動遠端登 錄 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 Wind ows UI。
Windows Server , 1706 版	64 位 元	Server Core	無	至少 1.4GHz 的 Intel Pentium 或同級 處理器 (建議 使用 2GHz)	至少 512MB (至 少 100MB 專用於 OfficeScan) 建議使用 2 GB 的處理 器	至少 800MB 建議使用 1GB 的處理 器	支援 1024 x 768 解析度 (256 色) 或以上的顯 示器 Windows Internet Explorer 11.0 (如果

作業系統		版本	SER VICE PAC K	處理器	RAM	可用磁碟空間	其他
				AMD™ 64 處理器 Intel 64 處理器			要執行 Web 安裝) 啟動遠端登 錄 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 <hr/>  注意 不支 援 Wind ows UI。

**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。

更新代理程式

資源	需求
處理器	800MHz Intel Pentium 處理器或同級處理器

資源	需求
RAM	512MB (1GB 用於執行 Windows Vista 的更新代理程式) 建議 1GB 或更多 (1.5GB 或更多用於執行 Windows Vista 的更新代理程式)
可用磁碟空間	至少 700MB 至少 1GB (如果更新代理程式部署 HotFix 和 OfficeScan 用戶端)
顯示器	支援 1024 x 768 解析度 (256 色) 或以上的顯示器

OfficeScan SaaS 用戶端系統需求

本部分簡述所支援的 Windows 平台上進行全新安裝的 OfficeScan SaaS 用戶端系統需求。

Windows 端點平台的全新安裝


Windows 7 (32/64 位元) 需求

項目	需求
版本 (含/不含 SP1)	<ul style="list-style-type: none"> • Home Basic • Home Premium • Ultimate • Professional • Enterprise • Professional for Embedded Systems • Ultimate for Embedded Systems • Thin PC

項目	需求
處理器	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 至少 1GB (32 位元) / 1.5GB (64 位元) (至少 100MB 專用於 OfficeScan) 建議使用 2 GB 的處理器
可用磁碟空間	<ul style="list-style-type: none"> 至少 800MB 建議使用 1GB 的處理器
其他	<ul style="list-style-type: none"> 支援 1024 x 768 解析度 (256 色) 或以上的顯示器 Microsoft Internet Explorer 8.0 或 9.0 (如果執行 Web 安裝) 關閉「簡易檔案共用」 啟動遠端登錄 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 8/8.1 (32/64 位元) 需求

項目	需求
版本 (不需要有 Service Pack)	<ul style="list-style-type: none"> Standard Pro Enterprise

項目	需求
處理器	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 至少 1GB (32 位元) / 1.5GB (64 位元) (至少 100MB 專用於 OfficeScan) 建議使用 2 GB 的處理器
可用磁碟空間	<ul style="list-style-type: none"> 至少 800MB 建議使用 1GB 的處理器
其他	<ul style="list-style-type: none"> 支援 1024 x 768 解析度 (256 色) 或以上的顯示器 Windows Internet Explorer 10.0 (如果要執行 Web 安裝) 啟動遠端登錄 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 <hr/> <p> 注意 不支援 Windows UI。</p>

Windows 10 (32/64 位元) 需求

項目	需求
版本 (不需要有 Service Pack)	<ul style="list-style-type: none"> Home Pro Education Enterprise

項目	需求
更新支援	<ul style="list-style-type: none"> • Anniversary Update • Creators Update • Fall Creators Update
處理器	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 至少 1GB (32 位元) /2GB (64 位元) (至少 100MB 專用於 OfficeScan) • 建議使用 2 GB 的處理器
可用磁碟空間	<ul style="list-style-type: none"> • 至少 800MB • 建議使用 1GB 的處理器
其他	<ul style="list-style-type: none"> • 支援 1024 x 768 解析度 (256 色) 或以上的顯示器 • Windows Internet Explorer 11.0 (如果要執行 Web 安裝) • 啟動遠端登錄 • 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 <hr/> <p> 注意 不支援 Windows UI。</p>

Windows Server 平台的全新安裝

Windows Server 2008（32 位元）平台

- [Windows Server 2008 第 9-26 頁](#)
- [Windows Storage Server 2008 第 9-27 頁](#)
- [Windows HPC Server 2008 第 9-28 頁](#)
- [Windows Server 2008 容錯移轉叢集（主動/被動） 第 9-28 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

項目	需求
版本（Service Pack 2）	<ul style="list-style-type: none"> • Standard • Enterprise • Datacenter • Web • Server Core
處理器	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 至少 512MB（至少 100MB 專用於 OfficeScan） • 建議使用 2 GB 的處理器
可用磁碟空間	<ul style="list-style-type: none"> • 至少 800MB • 建議使用 1GB 的處理器

項目	需求
其他	<ul style="list-style-type: none"> • 支援 1024 x 768 解析度 (256 色) 或以上的顯示器 • Microsoft Internet Explorer 8.0 或 9.0 (如果執行 Web 安裝) • 啟動遠端登錄 • 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

項目	需求
版本 (Service Pack 2)	<ul style="list-style-type: none"> • Basic
處理器	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 至少 512MB (至少 100MB 專用於 OfficeScan) • 建議使用 2 GB 的處理器
可用磁碟空間	<ul style="list-style-type: none"> • 至少 800MB • 建議使用 1GB 的處理器
其他	<ul style="list-style-type: none"> • 支援 1024 x 768 解析度 (256 色) 或以上的顯示器 • Microsoft Internet Explorer 8.0 或 9.0 (如果執行 Web 安裝) • 啟動遠端登錄 • 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

項目	需求
版本 (Service Pack 2)	<ul style="list-style-type: none"> Basic
處理器	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 至少 512MB (至少 100MB 專用於 OfficeScan) 建議使用 2 GB 的處理器
可用磁碟空間	<ul style="list-style-type: none"> 至少 800MB 建議使用 1GB 的處理器
其他	<ul style="list-style-type: none"> 支援 1024 x 768 解析度 (256 色) 或以上的顯示器 Microsoft Internet Explorer 8.0 或 9.0 (如果執行 Web 安裝) 啟動遠端登錄 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 9-5. Windows Server 2008 容錯移轉叢集 (主動/被動)

項目	需求
版本 (不需要有 Service Pack)	<ul style="list-style-type: none"> 無
處理器	<ul style="list-style-type: none"> 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

項目	需求
RAM	<ul style="list-style-type: none"> 至少 512MB (至少 100MB 專用於 OfficeScan) 建議使用 2 GB 的處理器
可用磁碟空間	<ul style="list-style-type: none"> 至少 800MB 建議使用 1GB 的處理器
其他	<ul style="list-style-type: none"> 支援 1024 x 768 解析度 (256 色) 或以上的顯示器 Microsoft Internet Explorer 8.0 或 9.0 (如果執行 Web 安裝) 啟動遠端登錄 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 2008 (64 位元) 平台

- [Windows Server 2008 第 9-30 頁](#)
- [Windows Server 2008 R2 第 9-31 頁](#)
- [Windows Storage Server 2008 第 9-31 頁](#)
- [Windows Storage Server 2008 R2 第 9-32 頁](#)
- [Windows HPC Server 2008 第 9-33 頁](#)
- [Windows HPC Server 2008 R2 第 9-34 頁](#)
- [Windows Server 2008 容錯移轉叢集 \(主動/被動\) 第 9-34 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 9-6. Windows Server 2008

項目	需求
版本 (Service Pack 2)	<ul style="list-style-type: none">• Standard• Enterprise• Datacenter• Web• Server Core
處理器	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 至少 512MB (至少 100MB 專用於 OfficeScan)
可用磁碟空間	<ul style="list-style-type: none">• 至少 800MB• 建議使用 1GB 的處理器
其他	<ul style="list-style-type: none">• 支援 1024 x 768 解析度 (256 色) 或以上的顯示器• Microsoft Internet Explorer 8.0 或 9.0 (如果執行 Web 安裝)• 啟動遠端登錄• 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 9-7. Windows Server 2008 R2

項目	需求
版本 (Service Pack 1)	<ul style="list-style-type: none"> • Standard • Enterprise • Datacenter • Web • Server Core
處理器	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 至少 512MB (至少 100MB 專用於 OfficeScan)
可用磁碟空間	<ul style="list-style-type: none"> • 至少 800MB • 建議使用 1GB 的處理器
其他	<ul style="list-style-type: none"> • 支援 1024 x 768 解析度 (256 色) 或以上的顯示器 • Microsoft Internet Explorer 8.0 或 9.0 (如果執行 Web 安裝) • 啟動遠端登錄 • 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 9-8. Windows Storage Server 2008

項目	需求
版本 (Service Pack 2)	<ul style="list-style-type: none"> • Basic • Standard • Enterprise • Workgroup

項目	需求
處理器	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 至少 512MB（至少 100MB 專用於 OfficeScan）
可用磁碟空間	<ul style="list-style-type: none"> 至少 800MB 建議使用 1GB 的處理器
其他	<ul style="list-style-type: none"> 支援 1024 x 768 解析度（256 色）或以上的顯示器 Microsoft Internet Explorer 8.0 或 9.0（如果執行 Web 安裝） 啟動遠端登錄 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 9-9. Windows Storage Server 2008 R2

項目	需求
版本（Service Pack 1）	<ul style="list-style-type: none"> Basic Standard Enterprise Workgroup
處理器	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 至少 512MB（至少 100MB 專用於 OfficeScan）

項目	需求
可用磁碟空間	<ul style="list-style-type: none"> 至少 800MB 建議使用 1GB 的處理器
其他	<ul style="list-style-type: none"> 支援 1024 x 768 解析度 (256 色) 或以上的顯示器 Microsoft Internet Explorer 8.0 或 9.0 (如果執行 Web 安裝) 啟動遠端登錄 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 9-10. Windows HPC Server 2008

項目	需求
版本 (不需要有 Service Pack)	<ul style="list-style-type: none"> 無
處理器	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 至少 512MB (至少 100MB 專用於 OfficeScan)
可用磁碟空間	<ul style="list-style-type: none"> 至少 800MB 建議使用 1GB 的處理器
其他	<ul style="list-style-type: none"> 支援 1024 x 768 解析度 (256 色) 或以上的顯示器 Microsoft Internet Explorer 8.0 或 9.0 (如果執行 Web 安裝) 啟動遠端登錄 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 9-11. Windows HPC Server 2008 R2

項目	需求
版本（不需要有 Service Pack）	<ul style="list-style-type: none"> 無
處理器	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 至少 512MB（至少 100MB 專用於 OfficeScan）
可用磁碟空間	<ul style="list-style-type: none"> 至少 800MB 建議使用 1GB 的處理器
其他	<ul style="list-style-type: none"> 支援 1024 x 768 解析度（256 色）或以上的顯示器 Microsoft Internet Explorer 8.0 或 9.0（如果執行 Web 安裝） 啟動遠端登錄 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 9-12. Windows Server 2008 容錯移轉叢集（主動/被動）

項目	需求
版本（不需要有 Service Pack）	<ul style="list-style-type: none"> 無
處理器	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 至少 512MB（至少 100MB 專用於 OfficeScan）

項目	需求
可用磁碟空間	<ul style="list-style-type: none"> • 至少 800MB • 建議使用 1GB 的處理器
其他	<ul style="list-style-type: none"> • 支援 1024 x 768 解析度 (256 色) 或以上的顯示器 • Microsoft Internet Explorer 8.0 或 9.0 (如果執行 Web 安裝) • 啟動遠端登錄 • 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)	<ul style="list-style-type: none"> • 無
處理器	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 至少 512MB (至少 100MB 專用於 OfficeScan)
可用磁碟空間	<ul style="list-style-type: none"> • 至少 800MB • 建議使用 1GB 的處理器

項目	需求
其他	<ul style="list-style-type: none"> • 支援 1024 x 768 解析度 (256 色) 或以上的顯示器 • Microsoft Internet Explorer 8.0 或 9.0 (如果執行 Web 安裝) • 啟動遠端登錄 • 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)	<ul style="list-style-type: none"> • Standard • Premium
處理器	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 至少 512MB (至少 100MB 專用於 OfficeScan)
可用磁碟空間	<ul style="list-style-type: none"> • 至少 800MB • 建議使用 1GB 的處理器

項目	需求
其他	<ul style="list-style-type: none"> • 支援 1024 x 768 解析度 (256 色) 或以上的顯示器 • Microsoft Internet Explorer 8.0 或 9.0 (如果執行 Web 安裝) • 啟動遠端登錄 • 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 9-37 頁](#)
- [Windows Server 2012 R2 第 9-38 頁](#)
- [Windows Storage Server 2012 第 9-39 頁](#)
- [Windows Storage Server 2012 R2 第 9-40 頁](#)
- [Windows MultiPoint Server 2012 第 9-41 頁](#)
- [Windows Server 2012 容錯移轉叢集 第 9-42 頁](#)
- [Windows Server 2012 R2 容錯移轉叢集 第 9-43 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 9-13. Windows Server 2012

項目	需求
版本 (不需要有 Service Pack)	<ul style="list-style-type: none"> • Standard • Datacenter • Server Core

項目	需求
處理器	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 至少 512MB（至少 100MB 專用於 OfficeScan）
可用磁碟空間	<ul style="list-style-type: none"> 至少 800MB 建議使用 1GB 的處理器
其他	<ul style="list-style-type: none"> 支援 1024 x 768 解析度（256 色）或以上的顯示器 Windows Internet Explorer 10.0（如果要執行 Web 安裝） 啟動遠端登錄 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 <hr/> <p> 注意 不支援 Windows UI。</p>

表 9-14. Windows Server 2012 R2

項目	需求
版本（不需要有 Service Pack）	<ul style="list-style-type: none"> Standard Datacenter Server Core
處理器	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 至少 512MB（至少 100MB 專用於 OfficeScan）


項目	需求
可用磁碟空間	<ul style="list-style-type: none"> • 至少 800MB • 建議使用 1GB 的處理器
其他	<ul style="list-style-type: none"> • 支援 1024 x 768 解析度 (256 色) 或以上的顯示器 • Windows Internet Explorer 10.0 (如果要執行 Web 安裝) • 啟動遠端登錄 • 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 <hr/> <p> 注意 不支援 Windows UI。</p>

表 9-15. Windows Storage Server 2012

項目	需求
版本 (不需要有 Service Pack)	<ul style="list-style-type: none"> • Standard • Workgroup
處理器	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 至少 512MB (至少 100MB 專用於 OfficeScan)
可用磁碟空間	<ul style="list-style-type: none"> • 至少 800MB • 建議使用 1GB 的處理器

項目	需求
其他	<ul style="list-style-type: none"> • 支援 1024 x 768 解析度 (256 色) 或以上的顯示器 • Windows Internet Explorer 10.0 (如果要執行 Web 安裝) • 啟動遠端登錄 • 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 <hr/> <p> 注意 不支援 Windows UI。</p>

表 9-16. Windows Storage Server 2012 R2

項目	需求
版本 (不需要有 Service Pack)	<ul style="list-style-type: none"> • Standard • Workgroup
處理器	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 至少 512MB (至少 100MB 專用於 OfficeScan)
可用磁碟空間	<ul style="list-style-type: none"> • 至少 800MB • 建議使用 1GB 的處理器

項目	需求
其他	<ul style="list-style-type: none"> • 支援 1024 x 768 解析度 (256 色) 或以上的顯示器 • Windows Internet Explorer 10.0 (如果要執行 Web 安裝) • 啟動遠端登錄 • 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 <hr/> <p> 注意 不支援 Windows UI。</p>

表 9-17. Windows MultiPoint Server 2012

項目	需求
版本 (不需要有 Service Pack)	<ul style="list-style-type: none"> • Standard • Premium
處理器	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 至少 512MB (至少 100MB 專用於 OfficeScan)
可用磁碟空間	<ul style="list-style-type: none"> • 至少 800MB • 建議使用 1GB 的處理器

項目	需求
其他	<ul style="list-style-type: none"> • 支援 1024 x 768 解析度 (256 色) 或以上的顯示器 • Windows Internet Explorer 10.0 (如果要執行 Web 安裝) • 啟動遠端登錄 • 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 <hr/> <p> 注意 不支援 Windows UI。</p>

表 9-18. Windows Server 2012 容錯移轉叢集

項目	需求
版本 (不需要有 Service Pack)	<ul style="list-style-type: none"> • 無
處理器	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 至少 512MB (至少 100MB 專用於 OfficeScan)
可用磁碟空間	<ul style="list-style-type: none"> • 至少 800MB • 建議使用 1GB 的處理器

項目	需求
其他	<ul style="list-style-type: none"> • 支援 1024 x 768 解析度 (256 色) 或以上的顯示器 • Windows Internet Explorer 10.0 (如果要執行 Web 安裝) • 啟動遠端登錄 • 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 <hr/> <p> 注意 不支援 Windows UI。</p>

表 9-19. Windows Server 2012 R2 容錯移轉叢集

項目	需求
版本 (不需要有 Service Pack)	<ul style="list-style-type: none"> • 無
處理器	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 至少 512MB (至少 100MB 專用於 OfficeScan) • 建議使用 2 GB 的處理器
可用磁碟空間	<ul style="list-style-type: none"> • 至少 800MB • 建議使用 1GB 的處理器

項目	需求
其他	<ul style="list-style-type: none"> • 支援 1024 x 768 解析度 (256 色) 或以上的顯示器 • Windows Internet Explorer 10.0 (如果要執行 Web 安裝) • 啟動遠端登錄 • 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 <hr/> <p> 注意 不支援 Windows UI。</p>

Windows Server 2016 (64 位元) 平台

- [Windows Server 2016 第 9-44 頁](#)
- [Windows Server 2016 容錯移轉叢集 第 9-45 頁](#)
- [Windows Storage Server 2016 第 9-46 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 9-20. Windows Server 2016

項目	需求
版本 (不需要有 Service Pack)	<ul style="list-style-type: none"> • Standard • Datacenter • Server Core

項目	需求
處理器	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 至少 512MB（至少 100MB 專用於 OfficeScan） 建議使用 2 GB 的處理器
可用磁碟空間	<ul style="list-style-type: none"> 至少 800MB 建議使用 1GB 的處理器
其他	<ul style="list-style-type: none"> 支援 1024 x 768 解析度（256 色）或以上的顯示器 Windows Internet Explorer 11.0（如果要執行 Web 安裝） 啟動遠端登錄 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 <hr/> <p> 注意 不支援 Windows UI。</p>

表 9-21. Windows Server 2016 容錯移轉叢集

項目	需求
版本（不需要有 Service Pack）	<ul style="list-style-type: none"> 無
處理器	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 至少 512MB (至少 100MB 專用於 OfficeScan) 建議使用 2 GB 的處理器
可用磁碟空間	<ul style="list-style-type: none"> 至少 800MB 建議使用 1GB 的處理器
其他	<ul style="list-style-type: none"> 支援 1024 x 768 解析度 (256 色) 或以上的顯示器 Windows Internet Explorer 11.0 (如果要執行 Web 安裝) 啟動遠端登錄 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 <hr/> <p> 注意 不支援 Windows UI。</p>

表 9-22. Windows Storage Server 2016

項目	需求
版本 (不需要有 Service Pack)	<ul style="list-style-type: none"> Standard Workgroup
處理器	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 至少 512MB (至少 100MB 專用於 OfficeScan) 建議使用 2 GB 的處理器
可用磁碟空間	<ul style="list-style-type: none"> 至少 800MB 建議使用 1GB 的處理器

項目	需求
其他	<ul style="list-style-type: none"> • 支援 1024 x 768 解析度 (256 色) 或以上的顯示器 • Windows Internet Explorer 11.0 (如果要執行 Web 安裝) • 啟動遠端登錄 • 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 <hr/> <div style="display: flex; align-items: center;">  注意 不支援 Windows UI。 </div>

Trend Micro Security (適用於 Mac) 用戶端安裝

本節說明 Trend Micro Security (適用於 Mac) 用戶端的安裝需求和方法。
 如需詳細資訊，請參閱 Trend Micro Security (適用於 Mac) 文件。

用戶端安裝需求

下列是在端點上安裝 Trend Micro Security (適用於 Mac) 用戶端的需求。

表 9-23. 用戶端安裝需求

資源	需求
作業系統	<ul style="list-style-type: none"> • macOS™ High Sierra 10.13 • macOS™ Sierra 10.12 • OS X™ El Capitan 10.11 • OS X™ Yosemite 10.10 或更新版本 • OS X™ Mavericks 10.9 或更新版本 • OS X™ Mountain Lion 10.8.3 或更新版本 • OS X™ Lion 10.7.5 或更新版本（僅限 64 位元）
硬體	<ul style="list-style-type: none"> • 處理器：Intel® Core™ 處理器 • RAM：至少 512MB • 可用磁碟空間：至少 300MB
通訊埠	61617
其他	<ul style="list-style-type: none"> • *.trendmicro.com 的存取權 • 用於 Internet 連線的 Proxy 伺服器設定（如果需要）

**注意**

此產品版本不再支援 Mac OS X Snow Leopard™ 10.6.8 或更早版本。如果有用戶端安裝在 Mac OS X Snow Leopard 上，則不要升級用戶端，並確定是否有 Trend Micro Security（適用於 Mac）2.0 SP1 伺服器可以管理這些用戶端。

用戶端安裝方法和安裝檔案

您可以使用下列其中一種方法來安裝 Trend Micro Security（適用於 Mac）用戶端：

- 在端點上啟動安裝套件 (tmsminstall.zip)，於單一端點上安裝
- 從 Apple Remote Desktop 啟動安裝套件 (tmsminstall.mpkg.zip)，在數個端點上安裝

- 透過部署內含 Trend Micro Security (適用於 Mac) 用戶端的作業系統映像，在多個端點上安裝。在安裝完成後，Trend Micro Security (適用於 Mac) 用戶端會自動向 Trend Micro Security (適用於 Mac) 伺服器註冊。

從 Trend Micro Security (適用於 Mac) 伺服器取得所需的用戶端安裝套件，然後將其複製到端點。

有許多方法可以取得套件：

- 在 Trend Micro Security (適用於 Mac) Web 主控台中，瀏覽至「用戶端 > 用戶端安裝檔案」，然後按一下「用戶端安裝檔案」下方的連結。



注意

此畫面上也有提供用戶端解除安裝套件的連結。您可以使用這些套件來將用戶端程式從端點移除。請根據您要移除的用戶端程式版本選擇對應的套件。

如需解除安裝 Trend Micro Security (適用於 Mac) 用戶端的相關資訊，請參閱 [用戶端解除安裝 第 9-51 頁](#)。

-
- 瀏覽至 <伺服器安裝資料夾>TSM_HTML\ActiveUpdate\ClientInstall\。
 - 從 Control Manager Web 主控台

用戶端安裝後

程序

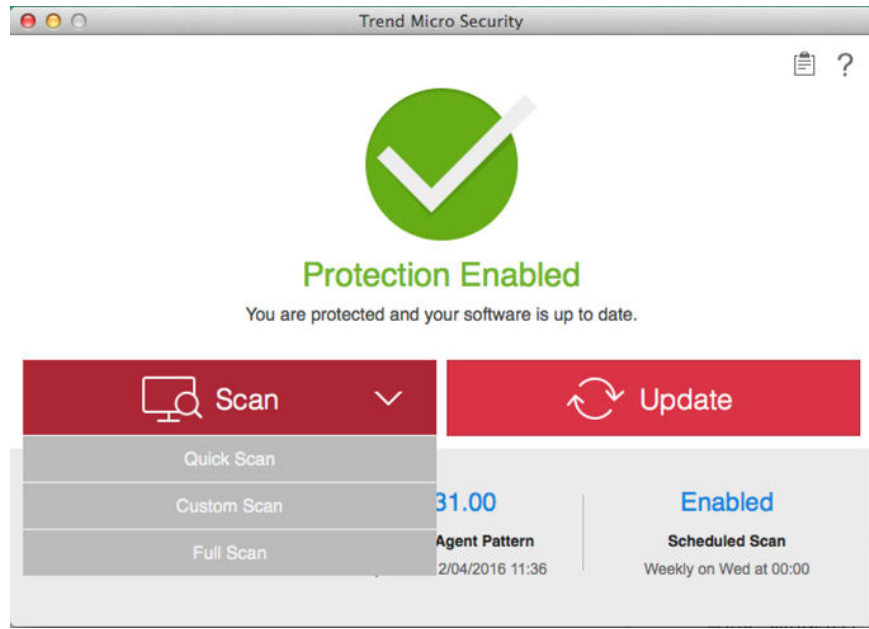
1. 請驗證下列項目：
 - 端點的功能表列上顯示了 Trend Micro Security (適用於 Mac) 用戶端圖示 (🛡️)。
 - 在 <用戶端安裝資料夾> 下可找到 Trend Micro Security (適用於 Mac) 用戶端檔案。
 - 用戶端出現在 Web 主控台的用戶端樹狀結構中。如果要存取用戶端樹狀結構，請按一下主功能表上的「用戶端管理」。

2. 在用戶端主控台上按一下「更新」，以更新 Trend Micro Security (適用於 Mac)。用戶端會從 Trend Micro Security (適用於 Mac) 伺服器下載元件。



如果用戶端無法連線到伺服器，則用戶端會直接從趨勢科技主動式更新伺服器下載。必須有 Internet 連線，才能連線到主動式更新伺服器。

3. 在端點上啟動手動掃描。



接下來需執行的動作

在安裝完成後，如果用戶端出現問題，請嘗試解除安裝用戶端後再重新安裝。

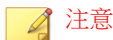
用戶端解除安裝

請僅在用戶端程式發生問題時將程式解除安裝，但之後應立即重新安裝，讓端點能夠持續防禦安全威脅。

程序

1. 從 Trend Micro Security (適用於 Mac) 伺服器取得用戶端解除安裝套件 (tmsmuninstall.zip)。在 Trend Micro Security (適用於 Mac) Web 主控台中，瀏覽至「用戶端 > 用戶端安裝檔案」，然後按一下「用戶端解除安裝檔案」下方的連結。

2. 將套件複製到端點上並加以啟動。
3. 填寫「名稱」和「密碼」欄位，以開始執行解除安裝程序。



注意

指定端點上具有管理權限之帳號的名稱和密碼。

4. 如果解除安裝成功，請按一下「關閉」以完成解除安裝程序。
-

接下來需執行的動作

將用戶端從伺服器取消註冊。

1. 在 Web 主控台中，按一下「用戶端管理」，然後選取已解除安裝的用戶端。
2. 按一下「管理用戶端樹狀結構 > 移除群組/用戶端」。

Trend Micro Security (適用於 Mac) SaaS 用戶端安裝

本節說明 Trend Micro Security (適用於 Mac) SaaS 用戶端的安裝需求和方法。

如需詳細資訊，請參閱 Trend Micro Security (適用於 Mac) 文件。

Trend Micro Security (適用於 Mac) SaaS 用戶端系統需求

下列是在端點上安裝 Trend Micro Security (適用於 Mac) SaaS 用戶端的需求。

表 9-24. 用戶端安裝需求

資源	需求
作業系統	<ul style="list-style-type: none"> • macOS™ High Sierra 10.13 • macOS™ Sierra 10.12 • OS X™ El Capitan 10.11 • OS X™ Yosemite 10.10 或更新版本 • OS X™ Mavericks 10.9 或更新版本 • OS X™ Mountain Lion 10.8.3 或更新版本 • OS X™ Lion 10.7.5 或更新版本（僅限 64 位元）
硬體	<ul style="list-style-type: none"> • 處理器：Intel® Core™ 處理器 • RAM：至少 512MB • 可用磁碟空間：至少 300MB
通訊埠	8443
其他	<ul style="list-style-type: none"> • *.trendmicro.com 的存取權 • 用於 Internet 連線的 Proxy 伺服器設定（如果需要）

Trend Micro Security（適用於 Mac）SaaS 用戶端安裝方法



注意

在安裝 Trend Micro Security（適用於 Mac）SaaS 用戶端之前：

- 確保用戶端端點可以透過通訊埠 8443 與伺服器進行通訊
- 確保端點可以存取 *.trendmicro.com
- 設定用戶端 Proxy 伺服器設定（如果需要）


從 Control Manager 取得必要的用戶端安裝套件。

您可以使用下列其中一種方法來安裝 Trend Micro Security (適用於 Mac) 用戶端：

- 在端點上啟動安裝套件 (tmsminstall.zip)，於單一端點上安裝
- 從 Apple Remote Desktop 啟動安裝套件 (tmsminstall.mpkg.zip)，在數個端點上安裝
- 透過部署內含 Trend Micro Security (適用於 Mac) 用戶端的作業系統映像，在多個端點上安裝。在安裝完成後，Trend Micro Security (適用於 Mac) 用戶端會自動向 Trend Micro Security (適用於 Mac) 伺服器註冊。

Trend Micro Security (適用於 Mac) SaaS 用戶端安裝後

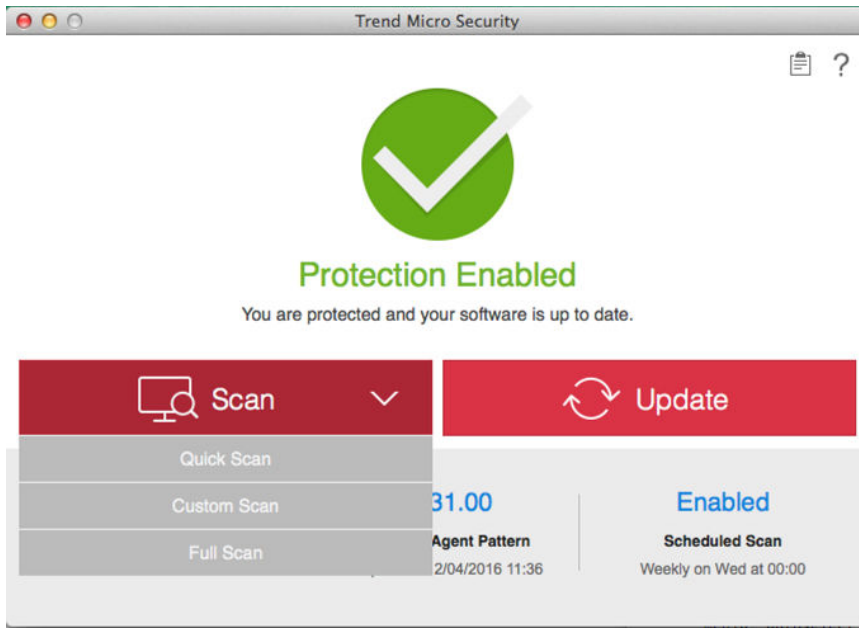
程序

1. 請驗證下列項目：
 - 端點的功能表列上顯示了 Trend Micro Security (適用於 Mac) 用戶端圖示 。
 - 在 <用戶端安裝資料夾> 下可找到 Trend Micro Security (適用於 Mac) 用戶端檔案。
 - 用戶端出現在 Web 主控台的用戶端樹狀結構中。如果要存取用戶端樹狀結構，請按一下主功能表上的「用戶端管理」。
2. 在用戶端主控台上按一下「更新」，以更新 Trend Micro Security (適用於 Mac)。用戶端會從 Trend Micro Security (適用於 Mac) 伺服器下載元件。



如果用戶端無法連線到伺服器，則用戶端會直接從趨勢科技主動式更新伺服器下載。必須有 Internet 連線，才能連線到主動式更新伺服器。

3. 在端點上啟動手動掃描。



接下來需執行的動作

在安裝完成後，如果用戶端出現問題，請嘗試解除安裝用戶端後再重新安裝。

第 10 章

產品目錄

本節討論如何檢視所有已向 Control Manager 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 10-6 頁](#)
- [執行產品目錄的進階搜尋 第 10-7 頁](#)
- [執行受管理產品工作 第 10-8 頁](#)
- [設定受管理的產品設定 第 10-9 頁](#)
- [從產品目錄查詢記錄檔 第 10-10 頁](#)
- [目錄管理 第 10-12 頁](#)

產品目錄

「產品目錄」畫面顯示所有已向 Control Manager 伺服器註冊的管理通訊協定 (MCP) 產品伺服器相關資訊。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[使用記錄查詢 第 14-2 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 Control Manager 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 Control Manager 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

Control Manager 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」圖示的詳細資訊，請參閱下列主題：

- [受管理產品的圖示 第 10-3 頁](#)
- [連線狀態圖示 第 10-5 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 10-6 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 10-8 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 10-9 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 10-8 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 10-10 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 10-12 頁 。

受管理產品的圖示

「產品目錄」使用下列圖示來代表已向 Control Manager 伺服器註冊的受管理產品。

圖示	說明
	Hosted Email Security
	Housecall

圖示	說明
	Intrusion Defense Firewall 網域
	InterScan eManager
	InterScan VirusWall NT
	InterScan VirusWall Unix
	InterScan WebProtect
	InterScan Web Security as a Service
	網路病毒牆
	OfficeScan Corporate Edition
	OfficeScan Corporate Edition 網域
	合作夥伴安全整合
	ScanMail for Microsoft Exchange
	ScanMail for Microsoft Exchange 叢集
	ServerProtect Information Server for NetWare
	ServerProtect Information Server for Windows
	ServerProtect Information Server for Windows 網域
	ServerProtect for NetWare (一般伺服器)
	ServerProtect for Windows (一般伺服器)
	ServerProtect for Windows 網域

圖示	說明
	Control Manager 階層式伺服器
	Endpoint Encryption
	Endpoint Encryption 網域
	Worry-Free Business Security Services
	Worry-Free Business Security Services 網域

連線狀態圖示

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

如需詳細資訊，請參閱[受管理產品的通訊](#) 第 8-10 頁。

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 仍在嘗試建立通訊	未知
	未執行  注意 重新嘗試未成功超過 3 次， 無法建立通訊	未執行

檢視受管理產品狀態摘要

Control Manager 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。

程序

- 移至「目錄 > 產品」。
會出現「產品目錄」畫面。
- 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，Control Manager 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

Control Manager 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。

程序

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 Control Manager 註冊的產品以及先前的過濾選取項目。
 - Control Manager 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 Control Manager 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 12-8 頁。

程序

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，Control Manager 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

Control Manager 允許您透過登入受管理產品的 Web 主控台，或藉由在 Control Manager 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。

程序

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：



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：讓您使用您的網域認證登入受管理產品的 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

Control Manager 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。



從「產品目錄」查詢記錄檔時，Control Manager 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[記錄查詢](#) 第 14-2 頁。

程序

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」。

記錄檔查詢

記錄檔查詢

< 返回 病毒/惡意程式偵測 指定的產品

安全記錄檔

系統事件

- 病毒/惡意程式偵測
- 間諜程式/可能的資安威脅程式偵測
- 可疑檔案偵測
- 行為監控違規
- 完整性監控
- Endpoint Application Control 違規
- 周邊設備存取控管違規
- 端點安全性符合
- 端點安全違規

確定 取消

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**

Control Manager 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。

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， Control Manager 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	Control Manager 會根據「部署計劃」將更新元件（例如，病毒碼檔案、掃描引擎、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。

**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 **Control Manager** 使用者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](#)。

使用目錄管理

使用「目錄管理」畫面可組織您的「產品目錄」結構。

Control Manager 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，**Control Manager** 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。

**重要**

變更「產品目錄」結構可能會影響 **Control Manager** 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](#)。

程序

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



警告!

如果您刪除包含受管理產品的自訂資料夾，Control Manager 便會從 Control Manager 伺服器自動取消註冊受管理產品。

- 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



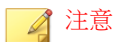
重要

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

Control Manager 可讓您還原不小心從「產品目錄」中刪除的受管理產品。



下列處理行動也可能會從「產品目錄」中刪除受管理產品:

- 重新安裝 Control Manager 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 Control Manager 資料庫
-

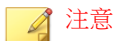
程序

1. 重新啟動受管理產品伺服器上的 Control Manager 服務。



如需詳細資訊，請參閱[停止並重新啟動 Control Manager 服務](#) 第 8-13 頁。

2. 等待用戶端自行重新註冊。



依預設，舊版的 Control Manager 代理程式會每隔八個小時驗證其與伺服器的連線。如果代理程式偵測到其記錄已被刪除，便會自動自行重新註冊。

3. 手動將 MCP 代理程式重新註冊到 Control Manager 伺服器
-

第 11 章

策略管理

本節包含有關如何在受管理產品和端點上執行策略管理的資訊。

包含下列主題：

- [策略管理 第 11-2 頁](#)
- [Data Loss Prevention 第 11-23 頁](#)
- [策略狀態 第 11-39 頁](#)

策略管理

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

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

建立新策略

程序

1. 移至「策略 > 策略管理」。
會出現「策略管理」畫面。



2. 從「產品」清單中選取產品設定的類型。
畫面會重新整理，以顯示為所選受管理產品建立的策略。
如需有關為特定受管理產品設定策略設定的詳細資訊，請參閱《Control Manager 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。

Control Manager 會提供多種目標選取方法，這些方法會影響策略的運作方式。

**注意**

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

策略清單會以下列順序排列策略目標：

- 指定目標：使用此選項可選取特定端點或受管理的產品。
如需詳細資訊，請參閱[指定策略目標 第 11-8 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 11-4 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 11-17 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，Control Manager 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 Control Manager 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 OfficeScan 用戶端建立策略，而您想要將該用戶端做為未來子策略的父項，請對子策略設定可以繼承、自訂或延伸的設定。
 - 如需可繼承、自訂或延伸的 OfficeScan 用戶端設定清單，請參閱[使用父策略設定 第 11-9 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 11-12 頁](#)。

7. 按一下「部署」或「儲存」。

如果按一下「部署」，Control Manager 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。Control Manager 通常需要幾分鐘時間，來將策略部署到目標。

按一下「策略管理」畫面上的「重新整理」，可在策略清單中更新狀態資訊。如果經過一段很長時間後，部署狀態依然是「暫停中」，這可能是目標有問題。請檢查 Control Manager 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 Control Manager 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。Control Manager 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 Control Manager 強制執行策略設定時都會覆寫這些變更。

- Control Manager 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 Control Manager 策略的 OfficeScan 用戶端已移至另一個 OfficeScan 網域，則用戶端設定將會暫時變更為由該 OfficeScan 網域定義的設定。一旦 Control Manager 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：
 - OfficeScan

- 企業版行動安全防護
- Trend Micro Security (適用於 Mac)
- 使用過濾器，以便自動將目前與未來的目標指派給策略
- 有助於將標準設定部署到目標群組

管理員可以變更策略清單中過濾策略的優先順序。當管理員重新排序策略清單時，Control Manager 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。

Control Manager 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 Control Manager 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 11-6 頁](#)。

程序

1. 在「建立策略」畫面上，移至「目標」區段，並選取「依條件過濾」，然後按一下「設定過濾器」。
會出現「依篩選條件」畫面。
2. 選取下列選項並定義條件。

條件	說明
比對關鍵字於	<p>根據主機名稱或 Control Manager 顯示名稱定義關鍵字。</p> <hr/> <p> 注意 對於單一關鍵字搜尋，Control Manager 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 Control Manager 僅會針對每個提供的關鍵字，提供符合完整字串的項目。</p>

條件	說明
IP 位址	<p>定義 IP 位址的範圍，然後按一下「新增」。</p> <hr/> <p> 注意</p> <ul style="list-style-type: none"> 策略管理僅支援 IPv4 位址。 在新的受管理產品或端點向 Control Manager 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	<p>選取下列其中一個目錄並定義條件。</p> <ul style="list-style-type: none"> 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 OfficeScan 網域階層：輸入至少一個 OfficeScan 網域階層關鍵字

3. 按一下「儲存」。

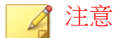
會重新載入「建立策略」畫面。

將端點指派給過濾策略

在新端點向 Control Manager 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，Control Manager 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 Control Manager 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，Control Manager 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

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

**注意**

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

當上述處理行動發生時，Control Manager 會根據下列條件來配置端點：

表 11-1. 過濾策略的端點配置

	新端點或已刪除策略的端點	沒有策略的端點	有策略的端點
建立新策略		●	
編輯策略	●	●	●
重新排序過濾策略	●	●	●
每日端點配置預約時程	●	●	●

指定策略目標

使用此選項可選取特定端點或受管理的產品。

此選項：

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

程序

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

會出現「指定目標」畫面。

2. 使用「搜尋」或「瀏覽」尋找目標。
 - 搜尋：使用下列搜尋條件來尋找端點或受管理的產品。搜尋結果會顯示符合所有選定條件的端點或受管理產品。
 - 比對關鍵字於：根據主機名稱或 Control Manager 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 Control Manager 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

Control Manager 管理員建立 OfficeScan 用戶端的父策略時，可以設定要繼承、自訂或延伸策略的特定設定。

**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。OfficeScan 管理員可以從 OfficeScan 伺服器主控台手動變更設定。不過，當 Control Manager 將策略部署到 OfficeScan 伺服器時，設定會遭到覆寫。

例如，Control Manager 管理員可以建立一個父策略，來執行從「手動掃描」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	●	●	
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	●		●

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
掃描例外清單（不掃描的目錄、檔案和副檔名） 「手動掃描/即時掃描/立即掃描/預約掃描設定」>「掃描例外」標籤	●		● 從掃描例外清單中選取「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描排除的項目。

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

程序

1. 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. 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」。



- 按一下「部署」後，請等候兩分鐘，讓 Control Manager 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。
 - Control Manager 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 OfficeScan 用戶端的父策略。用於 OfficeScan 用戶端的父策略在「父策略」欄的底下會顯示值「無」。

程序

1. 移至「策略 > 策略管理」。
會出現「策略管理」畫面。
2. 從「產品」清單中選取「OfficeScan 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 11-9 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「預約掃描」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「即時掃描」的掃描例外清單，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描例外清單。
8. 按一下「部署」。

**注意**

- 按一下「部署」後，請等候兩分鐘，讓 Control Manager 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。
- Control Manager 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，Control Manager 會將策略部署到目標。

對於 OfficeScan 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 11-9 頁。

例如：

- 如果您將掃描預約時程權限從「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「手動掃描」副檔名權限從「從父策略延伸」變更為「繼承自父策略」，則管理員新增到子策略的任何副檔名將被移除。此外，管理員也無法再新增副檔名。

程序

1. 瀏覽至「策略 > 策略管理」。
會出現「策略管理」畫面。
2. 從「產品」清單中選取產品設定的類型。
畫面會重新整理，以顯示為所選受管理產品建立的策略。
3. 按一下「策略」欄中的策略名稱。
會出現「編輯策略」畫面。
4. 修改策略。



注意

修改過濾策略中的過濾條件會影響目標配置。Control Manager 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」。

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

Control Manager 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 Control Manager 伺服器。



注意

- Control Manager 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 Control Manager 無法匯入該策略。如果現有策略並非子策略，則 Control Manager 會在匯入後覆寫該策略。

程序

1. 移至「策略 > 策略管理」。
會出現「策略管理」畫面。
2. 從「產品」清單中選取產品設定的類型。
畫面會重新整理，以顯示為所選受管理產品建立的策略。
3. 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 11-20 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，Control Manager 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。

Control Manager 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 OfficeScan 用戶端父策略。

程序

1. 瀏覽至「策略 > 策略管理」。
會出現「策略管理」畫面。
 2. 從「產品」清單中選取產品設定的類型。
畫面會重新整理，以顯示為所選受管理產品建立的策略。
 3. 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 Control Manager 使用者帳號。您也可以將策略擁有者變更為 Active Directory 群組，這麼做會將群組中的所有 Active Directory 使用者指定為策略的擁有者。



重要

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

程序

1. 移至「策略 > 策略管理」。
會出現「策略管理」畫面。
2. 選取一或多個要變更擁有者的策略。
3. 按一下「變更擁有者」。
會出現「變更策略擁有者」畫面。
4. 從下拉式清單中選取使用者帳號。
5. 按一下「儲存」以變更擁有者。

Control Manager 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 Control Manager 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，Control Manager 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 11-2. 策略清單

欄	說明
優先順序	<p>顯示策略的優先順序。</p> <ul style="list-style-type: none"> • Control Manager 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，Control Manager 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。 • Control Manager 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	<p>如果選取的產品為「OfficeScan 用戶端」時，才會顯示此欄。</p> <p>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」。</p>
偏差	<p>如果選取的產品為「OfficeScan 用戶端」時，才會顯示此欄。</p> <p>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）。</p> <p>如果策略不是子策略，會顯示「無」。</p>
目標	<p>顯示管理員如何為策略選取目標。</p> <ul style="list-style-type: none"> • 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。

欄	說明
已部署	<p>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</p> <p>按一下數字可檢視策略狀態。</p>
暫停中	<p>顯示未套用策略設定的目標數目</p> <hr/> <p> 注意</p> <p>如果未安裝 Hotfix 2575，則「暫停中」欄會包含具有離線用戶的目標數目。</p> <hr/> <p>按一下數字可檢視策略狀態。</p>
離線	<p>顯示具有離線用戶的目標數目</p> <hr/> <p> 重要</p> <p>此功能需要安裝 Hotfix 2575，否則「暫停中」欄會包含具有離線用戶的目標數目，且不會顯示「離線」欄。</p> <hr/> <p>按一下數字可檢視策略狀態。</p>
具有問題	<p>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</p> <p>按一下數字可檢視策略狀態。</p>
擁有者	<p>顯示目前被指派有該策略的使用者</p> <hr/> <p> 注意</p> <p>預設擁有者為建立策略的使用者。</p> <ul style="list-style-type: none"> • 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。 <p>如需詳細資訊，請參閱變更策略擁有者 第 11-17 頁。</p>

欄	說明
上次編輯者	顯示上次編輯策略的使用者

**注意**

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

重新排序策略清單

管理員可以使用「重新排序」按鈕，變更過濾策略的順序。重新排列策略清單可能會影響目標配置。Control Manager 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 OfficeScan 設定。

程序

1. 瀏覽至「策略 > 策略管理」。
會出現「策略管理」畫面。
2. 從「產品」清單中選取產品設定的類型。
畫面會重新整理，以顯示為所選受管理產品建立的策略。
3. 按一下「重新排序」。

會出現「重新排序策略」畫面。

重新排序策略
✕

⚠ 重排策略的優先順序可能會影響端點配置。端點可能會被重新指派給其他策略。 ✕

優先順序	策略	已指派的目標	目標	建立者
1 ▼	Standard	5	已過濾	root
2 ▼	Standard 2	0	已過濾	root

儲存

取消

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 Control Manager 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。

更新策略範本

「策略範本設定」畫面會列出管理員可加以啟動或升級的下列元件：

- 策略管理架構：整體策略結構
- 產品支援：受管理產品和端點的設定範本



注意

如果要檢查哪些產品版本支援策略管理，請將滑鼠游標移至「範本版本」欄中的資訊圖示上。

程序

1. 下載最新的「Control Manager Widget 集區和策略範本 (適用於 Control Manager 6.0 和更新版本)」元件。

如需有關如何下載 Control Manager 元件的詳細資訊，請參閱[元件更新 第 12-2 頁](#)。

「資訊中心」和「策略管理」畫面頂端會顯示一個藍色通知。

2. 在任一個畫面上，按一下通知方塊中的「立即更新」。
3. 完成更新時，請按一下「確定」。

畫面會重新整理，此時會出現登入畫面。

4. 登入 Web 主控台。
5. 移至「策略 > 策略資源 > 策略範本設定」。

會出現「策略範本設定」畫面。

6. 按一下「策略架構」列中的「更新 <版本號碼>」。
7. 如果要新增策略範本，請按一下「處理行動」欄中的「啟動」。

接著，管理員可以從「策略管理」畫面上的「產品」清單中選取新的設定範本。

8. 如果要更新現有範本，請按一下「處理行動」欄中的「更新 <版本號碼 >」。



注意

如果要查看有關更新的詳細資訊，請按一下「處理行動」欄中的「詳細資料」。

一旦更新完成，管理員可以透過編輯現有策略來檢查已更新的功能。在「設定」區段下，新功能標題旁會顯示一則紅色訊息。

Data Loss Prevention

Data Loss Prevention (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。

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 11-24 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 11-28 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 11-30 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 11-24 頁](#)和[自訂表示式 第 11-25 頁](#)。

預先定義的表示式

Data Loss Prevention 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。

Data Loss Prevention 會使用病毒碼比對和數學方程式來驗證這些表示式。Data Loss Prevention 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。

程序

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，Data Loss Prevention 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，Data Loss Prevention 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 11-25 頁。

自訂表示式的條件

表 11-3. 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 <ul style="list-style-type: none"> • 表示式：<code>[^\w]([A-Z][a-z]{1,12})(\s?,\s?[\s]\s([A-Z])\s[A-Z][a-z]{1,12})[^\w]</code>

條件	規則	範例
特定字元	<p>表示式必須包含您指定的字元。</p> <p>此外，表示式中的字元數目必須介於下限到上限之間。</p>	<p>美國 — 美國銀行轉帳號碼</p> <ul style="list-style-type: none"> 表示式：<code>[^d]{0123678}d{8}[^d]</code> 字元：0123456789 字元數目下限：9 字元數目上限：9
字尾	<p>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。</p> <p>此外，表示式中的字元數目必須介於下限到上限之間。</p>	<p>全部 — 住家地址</p> <ul style="list-style-type: none"> 表示式：<code>\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-]</code> 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	<p>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。</p> <p>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。</p>	<p>全部 — 電子郵件信箱</p> <ul style="list-style-type: none"> 表示式：<code>[^w.]{1,20}@[a-z0-9]{2,20}[.][a-z]{2,5}[a-z.]{0,10}[^w.]</code> 分隔符號：@ 左邊字元數目下限：3 左邊字元數目上限：15 右邊字元數目上限：30

建立自訂表示式

程序

- 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 11-25 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。

程序

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，Control Manager 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

程序

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。Data Loss Prevention 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。

程序

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 Data Loss Prevention 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 11-31 頁](#) 和 [自訂關鍵字清單 第 11-32 頁](#)。

預先定義的關鍵字清單

Data Loss Prevention 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 Data Loss Prevention 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 Data Loss Prevention 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，Data Loss Prevention 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，Data Loss Prevention 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 11-32 頁。

自訂關鍵字清單條件

表 11-4. 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。

條件	規則
<p>在 <x> 個字元內的所有關鍵字</p>	<p>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。</p> <p>例如，您的 3 個關鍵字是 WEB、DISK 和 USB，而您指定的字元數是 20。</p> <p>如果 Data Loss Prevention 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。</p> <p>下列資料符合此條件：DISK####WEB#####USB</p> <p>下列資料不符合此條件：DISK*****WEB****USB（從「D」到「W」相隔 23 個字元）</p> <p>決定字元數時請記住，此數字越小（例如 10）通常掃描時間就越短，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，但是掃描時間可能會比較長。</p>
<p>關鍵字的結合評分超過門檻值</p>	<p>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。</p> <p>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。</p> <p>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低於那三個高優先順序關鍵字的結合評分。這表示偵測到這三個關鍵字時就可以將該檔案視為機密檔案。</p>

建立關鍵字清單

程序

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。

程序

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。

Data Loss Prevention 範本

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

例如，檔案必須是 Microsoft Word 檔案（檔案屬性）AND（且）必須包含特定法律詞彙（關鍵字）AND（且）必須包含 ID 號碼（表示式），才能受到「聘用合約」策略管制。此策略允許人力資源部門的員工透過列印方式傳輸檔案，

以便將列印複本交由員工簽署。但禁止透過其他可能的通道（例如：電子郵件）傳輸。

如果您已經設定 DLP 資料識別碼，您也可以建立自己的範本。您也可以使用已預先定義的範本。如需詳細資訊，請參閱自訂的 DLP 範本 第 11-36 頁和預先定義的 DLP 範本 第 11-36 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

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

如需所有預先定義範本的目的，以及受保護的資料範本的詳細清單，請參閱「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 11-37 頁。

條件陳述式和邏輯運算子

Data Loss Prevention 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 11-5. 條件陳述式範例

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

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

建立範本

程序

- 移至「策略 > 策略資源 > DLP 範本」。
- 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 Data Loss Prevention 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 11-37 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。

程序

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。

策略狀態

策略狀態可讓管理員檢查 Control Manager 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 11-6. 策略狀態

策略狀態	說明	建議
暫停中	Control Manager 正在處理策略。	請等候幾分鐘後再重新檢查狀態。
沒有策略	Control Manager 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	Control Manager 已成功部署策略。	無
端點無法連線到伺服器	<ul style="list-style-type: none"> 端點未收到策略設定。 伺服器目前忙碌中。 	<ul style="list-style-type: none"> 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。	<ul style="list-style-type: none"> 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 <p>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 Control Manager。</p> <ul style="list-style-type: none"> 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。
未啟動的產品服務	受管理產品尚未啟動策略設定中所指定的部份服務。	請在受管理產品上啟動相關服務。
關閉的產品服務	未受管理產品已關閉策略設定中所指定的部份服務。	請在受管理產品上啟動相關服務。

策略狀態	說明	建議
已部分部署	Control Manager 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 [Control Manager 伺服器名稱] 管理	另一個 Control Manager 目前正在管理受管理產品。	從「受管理的伺服器」清單中移除受管理產品，然後重新將受管理產品新增到清單。
使用者名稱或密碼無效	用於驗證的使用者名稱或密碼不正確。	請確認使用者名稱或密碼。
產品伺服器或驗證資訊無效	伺服器名稱或驗證資訊不正確。	請確認伺服器名稱和驗證資訊。
無法自動登入產品	Control Manager 無法使用單一登入功能來存取受管理產品。	<ul style="list-style-type: none"> 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。	<ul style="list-style-type: none"> 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。	Control Manager 無法建立與受管理產品的連線。	<ul style="list-style-type: none"> 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 12 章

元件更新

本節討論如何在 Control Manager 中設定元件更新。

包含下列主題：

- [元件更新 第 12-2 頁](#)
- [設定預約更新設定 第 12-5 頁](#)
- [設定手動更新設定 第 12-8 頁](#)
- [設定用於元件和使用授權更新的 Proxy 伺服器設定 第 12-11 頁](#)

元件更新

Control Manager 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。Control Manager 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 Control Manager 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 Control Manager 成功下載之元件的上個版本
上次下載	顯示 Control Manager 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 Control Manager 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 Control Manager 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，Control Manager 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或其他更新來源下載元件。

為了存取其他更新來源，Control Manager 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 Control Manager 來下載更新。

部署計劃

您可以使用部署計劃來指定 Control Manager 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 Control Manager 伺服器從更新來源下載新元件版本後，您可以設定 Control Manager 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。

若要進行更精細的元件更新管理，您可以設定 Control Manager 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。
- Control Manager 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 Control Manager 會下載更新，但不會將更新元件部署到受管理產品。
- 您可以設定受管理產品可以與 Control Manager 用戶端進行通訊並下載元件的時間。

如需詳細資訊，請參閱[設定用戶端通訊預約時程](#) 第 8-11 頁。

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。

程序

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 Control Manager 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 Control Manager 根據部署計劃，將更新的元件部署到受管理產品。



注意

移轉到 Control Manager 7.0 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」與「部署計劃」組態設定。



警告!

移轉到 Control Manager 7.0 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。

程序

1. 移至「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 12-2 頁](#)。



重要

如果您選取「啟動智慧元件下載」核取方塊，Control Manager 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 Control Manager 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 Control Manager 根據選取的元件類別，從更新來源自動偵測並下載新元件。

當您選取這個選項時，Control Manager 也會下載所選類別中所有現有元件的更新。



注意

如果未啟動智慧元件下載功能，則 Control Manager 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 12-3 頁](#)。




注意

如果 Control Manager 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[設定用於元件和使用授權更新的 Proxy 伺服器設定 第 12-11 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	<p>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：</p> <ul style="list-style-type: none"> • 立即：Control Manager 在 Control Manager 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：Control Manager 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：Control Manager 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	<p>選取此選項，可設定指定受管理產品的部署預約時程。</p> <p>執行下列其中一項作業：</p> <ul style="list-style-type: none"> • 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 12-4 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。 <hr/> <p> 注意 如果您沒有指定部署預約時程，Control Manager 會下載元件更新，但不會將更新的元件部署到受管理產品。</p>
不要部署	<p>如果您不想讓 Control Manager 自動將更新的元件部署到受管理產品，則選取此選項。</p> <p>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。</p> <p>如需詳細資訊，請參閱執行受管理產品工作 第 10-8 頁。</p>

8. 按一下「儲存」。

設定手動更新設定

您可以在 Control Manager 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 Control Manager 根據部署計劃，將更新的元件部署到受管理產品。



警告!

移轉到 Control Manager 7.0 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。

程序

1. 移至「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 12-2 頁](#)。



重要

如果您選取「啟動智慧元件下載」核取方塊，Control Manager 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 Control Manager 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 Control Manager 根據選取的元件類別，從更新來源自動偵測並下載新元件。

當您選取這個選項時，Control Manager 也會下載所選類別中所有現有元件的更新。

**注意**

如果未啟動智慧元件下載功能，則 Control Manager 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 12-3 頁](#)。

**注意**

如果 Control Manager 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[設定用於元件和使用授權更新的 Proxy 伺服器設定 第 12-11 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	<p>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：</p> <ul style="list-style-type: none"> • 立即：Control Manager 在 Control Manager 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：Control Manager 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：Control Manager 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	<p>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：</p> <ul style="list-style-type: none"> • 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 12-4 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。 <hr/> <p> 注意 如果您沒有指定部署預約時程，Control Manager 會下載元件更新，但不會將更新的元件部署到受管理產品。</p>
不要部署	<p>如果您不想讓 Control Manager 自動將更新的元件部署到受管理產品，則選取此選項。</p> <p>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。</p> <p>如需詳細資訊，請參閱執行受管理產品工作 第 10-8 頁。</p>

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。
-

設定用於元件和使用授權更新的 Proxy 伺服器設定

Control Manager 允許您使用 Proxy 伺服器來進行元件下載和使用授權更新。

程序

1. 移至「管理 > 設定 > Proxy 伺服器設定」。
會出現「連線設定」畫面。
 2. 選取「將 Proxy 伺服器用於元件/使用授權更新及雲端服務連線」。
 3. 選取通訊協定：
 - 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 13 章

指令追蹤

本節討論如何追蹤從 Control Manager 伺服器發出的指令。

包含下列主題：

- [指令追蹤 第 13-2 頁](#)
- [查詢及檢視指令 第 13-3 頁](#)
- [設定指令逾時設定 第 13-4 頁](#)

指令追蹤

「指令追蹤」畫面可提供傳送自 Control Manager 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 Control Manager 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 13-3 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	Control Manager 伺服器向受管理產品發出指令的日期和時間
指令	Control Manager 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 13-3 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 13-3 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 13-3 頁 。
全部	Control Manager 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 13-3 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。

程序

- 移至「管理 > 指令追蹤」。
會出現「追蹤指令」畫面。
- 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」。
- 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 13-3 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 Control Manager 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。

設定指令逾時設定

使用「通訊逾時設定」畫面可設定指令逾時設定。當指令逾時，Control Manager 會停止嘗試執行發出的指令。

程序

1. 移至「管理 > 設定 > 通訊逾時設定」。
會出現「通訊逾時設定」畫面。
2. 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
3. 按一下「儲存」。

部分 IV

安全監控



第 14 章

記錄檔

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

包含下列主題：

- [記錄查詢 第 14-2 頁](#)
- [使用記錄查詢 第 14-2 頁](#)
- [設定記錄檔彙整 第 14-10 頁](#)
- [刪除記錄檔 第 14-11 頁](#)

記錄查詢

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

Control Manager 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 Control Manager 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。

使用記錄查詢

使用「記錄查詢」畫面查詢 Control Manager 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 Control Manager 管理員共用。



注意

Control Manager 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 10-10 頁。

程序

1. 移至「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 Control Manager 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[記錄查詢資料檢視](#) 第 14-5 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找出受管理產品並加以選取：
 - 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
 - c. 選取特定的受管理產品或產品類型。
 - d. 按一下「確定」以套用選取的受管理產品或產品類型。
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[記錄查詢資料檢視 第 14-5 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


Control Manager 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。
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 16-1 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 Control Manager 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 Control Manager 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。

記錄查詢資料檢視

Control Manager 記錄檔類型與報告中使用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。

表 14-1. 安全記錄檔

記錄類型	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-6 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-19 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-71 頁 。
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-43 頁 。
完整性監控	完整性監控資訊	用來監控電腦上特定區域是否發生變更，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-47 頁 。
Endpoint Application Control 違規	Endpoint Application Control 違規詳細資訊	提供有關網路上海端點應用程式違規的特定資訊，例如違反的策略和規則名稱 如需詳細資訊，請參閱 Endpoint Application Control 違規詳細資訊 第 B-45 頁 。

記錄類型	資料檢視	說明
周邊設備存取控管違規	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-44 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-40 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-39 頁 。
Machine Learning 詳細資訊	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-72 頁 。
沙盒虛擬平台偵測數	沙盒虛擬平台偵測詳細資訊	提供有關沙盒虛擬平台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 沙盒虛擬平台偵測資訊 第 B-73 頁 。
網路事件：		
垃圾郵件連線	垃圾郵件連線資訊	提供有關網路上垃圾郵件來源的特定資訊 如需詳細資訊，請參閱 垃圾郵件連線資訊 第 B-36 頁 。
內容違規	內容違規詳細資訊	提供有關網路上內容違規的特定資訊 如需詳細資訊，請參閱 內容違規詳細資訊 第 B-30 頁 。
內含進階安全威脅的電子郵件訊息	內含進階安全威脅的電子郵件訊息	提供有關內含可疑和惡意行為特徵碼的電子郵件訊息的特定資訊 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-32 頁 。

記錄類型	資料檢視	說明
網站信譽評等服務	網站信譽評等服務詳細資訊	提供有關網頁信譽評等服務偵測到的策略或規則違規的安全威脅資訊 如需詳細資訊，請參閱 網站信譽評等服務詳細資訊 第 B-55 頁 。
Web 違規	Web 違規詳細資訊	提供有關網路上 Web 違規的特定資訊 如需詳細資訊，請參閱 Web 違規詳細資訊 第 B-53 頁 。
防火牆違規事件	防火牆違規事件詳細資訊	提供有關網路上防火牆違規事件的特定資訊 如需詳細資訊，請參閱 防火牆違規事件詳細資訊 第 B-37 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-38 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-46 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-69 頁 。
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-64 頁 。

記錄類型	資料檢視	說明
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。
緩和	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 如需詳細資訊，請參閱 緩和詳細資訊 第 B-68 頁。
關聯	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 如需詳細資訊，請參閱 關聯詳細資訊 第 B-69 頁。
資料安全防護事件：		
Data Loss Prevention	DLP 事件資訊	顯示有關 Data Loss Prevention 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-81 頁。
Data Discovery	資料發現 Data Loss Prevention 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 Data Loss Prevention 偵測資訊 第 B-84 頁。

表 14-2. 產品資訊

記錄類型	資料檢視	說明
受管理的產品：		
產品狀態	產品狀態資訊	顯示有關已註冊於 Control Manager 伺服器之受管理產品的特定資訊 如需詳細資訊，請參閱 產品狀態資訊 第 B-89 頁。

記錄類型	資料檢視	說明
產品事件	產品事件資訊	顯示有關受管理產品事件的特定資訊 如需詳細資訊，請參閱 產品事件資訊 第 B-91 頁。
產品稽核事件	產品稽核事件記錄檔	顯示與受管理產品相關的稽核資訊 如需詳細資訊，請參閱 產品稽核事件記錄檔 第 B-92 頁。
Control Manager :		
指令追蹤	指令追蹤資訊	顯示有關向受管理產品發出的指令的特定資訊 如需詳細資訊，請參閱 指令追蹤資訊 第 B-100 頁。
Control Manager 事件	Control Manager 事件資訊	顯示有關 Control Manager 伺服器事件的特定資訊 如需詳細資訊，請參閱 Control Manager 事件資訊 第 B-100 頁。
使用者存取	使用者存取資訊	顯示 Control Manager 使用者存取權和使用者登入 Control Manager 時所執行的活動 如需詳細資訊，請參閱 使用者存取資訊 第 B-99 頁。
產品使用授權	產品使用授權詳細資訊	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資訊 如需詳細資訊，請參閱 產品使用授權詳細資訊 第 B-87 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 Control Manager 伺服器，來節省網路頻寬。

**警告!**

Control Manager 無法還原受管理產品未傳送到 Control Manager 伺服器的資料。

程序

1. 移至「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 Control Manager。
5. 按一下「儲存」。

刪除記錄檔

您可以使用「記錄檔維護」畫面，來手動依類型刪除記錄項目，或是設定自動刪除記錄。

**秘訣**

Trend Micro 建議您將 Data Loss Prevention 記錄檔備份至 Security Information and Event Management (SIEM)，並保留至少 2 年。

程序

1. 移至「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. 按一下對應列中的「全部刪除」。
接著會出現警告訊息。
 - 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 Control Manager 保留的記錄數目上限。



注意

依預設，Control Manager 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，Control Manager 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 Control Manager 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 15 章

通知

本節討論如何傳送有關 Control Manager 網路上所發生事件的通知。
包含下列主題：

- [事件通知](#) 第 15-2 頁
- [通知方法設定](#) 第 15-3 頁
- [聯絡人群組](#) 第 15-6 頁
- [進階安全威脅活動事件](#) 第 15-9 頁
- [內容策略違規事件](#) 第 15-26 頁
- [Data Loss Prevention 事件](#) 第 15-29 頁
- [已知的安全威脅活動事件](#) 第 15-38 頁
- [網路存取控制事件](#) 第 15-53 頁
- [不尋常的產品行為事件](#) 第 15-56 頁
- [更新](#) 第 15-63 頁

事件通知

Control Manager 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、Syslog 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 15-3 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 15-9 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 15-26 頁 。
Data Loss Prevention	提供有關 Data Loss Prevention 事件和範本相符項目的資訊 如需詳細資訊，請參閱 Data Loss Prevention 事件 第 15-29 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 15-38 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 15-53 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 15-56 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 15-63 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 15-3 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 15-4 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 15-5 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 15-6 頁。

設定 SMTP 伺服器設定

Control Manager 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」，Control Manager 才能傳送電子郵件。

程序

1. 移至「通知 > 通知方法設定」
會出現「通知方法設定」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

Control Manager 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。

程序

1. 移至「通知 > 通知方法設定」
會出現「通知方法設定」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

Control Manager 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。

程序

1. 移至「通知 > 通知方法設定」
會出現「通知方法設定」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

Control Manager 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。

程序


1. 移至「通知 > 通知方法設定」
會出現「通知方法設定」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 Control Manager 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 15-7 頁。

工作	說明
移除現有的聯絡人群組	<p>選取現有的聯絡人群組，然後按一下「移除」。</p> <hr/> <p> 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。</p> <hr/>
編輯現有的聯絡人群組	<p>按一下現有聯絡人群組的「名稱」，即可編輯收件者。</p> <p>如需詳細資訊，請參閱編輯聯絡人群組 第 15-8 頁。</p>

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。

程序

- 移至「通知 > 聯絡人群組」
會出現「聯絡人群組」畫面。
- 請點選「新增」。
會出現「新增群組」畫面。
- 輸入聯絡人群組的名稱。
- 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」。

程序

1. 移至「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。



您一次只能新增一個電子郵件信箱。

- 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。

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。

程序

- 移至「通知 > 事件通知」。
會出現「事件通知」畫面。
- 按一下「進階安全威脅活動」。
會出現事件清單。
- 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。
- 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。
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	<p>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。</p> <p>如需詳細資訊，請參閱標準 Token 變數 第 C-3 頁和進階安全威脅活動 Token 變數 第 C-3 頁。</p>

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。

程序

1. 移至「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-3 頁和 C&C 回呼 Token 變數 第 C-4 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-3 頁和 C&C 回呼 Token 變數 第 C-4 頁。

方法	說明
Syslog	Control Manager 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。

程序

1. 移至「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	<p>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。</p> <p>如需詳細資訊，請參閱標準 Token 變數 第 C-3 頁 和 C&C 回呼 Token 變數 第 C-4 頁。</p>

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。

程序

1. 移至「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-3 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。

程序

1. 移至「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-3 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」。

高風險沙盒虛擬平台偵測數

設定下列事件通知，以在沙盒虛擬平台偵測到高度可疑物件時通知管理員。

程序

1. 移至「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「高風險沙盒虛擬平台偵測」。
會出現「高風險沙盒虛擬平台偵測」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。 <ul style="list-style-type: none"> • 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	<p>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。</p> <p>如需詳細資訊，請參閱標準 Token 變數 第 C-3 頁和進階安全威脅活動 Token 變數 第 C-3 頁。</p>

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。

程序

1. 移至「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。

設定	說明
指定套用於單一端點的警訊門檻值	<p>選取以傳送僅符合指定條件之偵測的事件通知。</p> <ul style="list-style-type: none"> 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	<p>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。</p> <p>如需詳細資訊，請參閱標準 Token 變數 第 C-3 頁和進階安全威脅活動 Token 變數 第 C-3 頁。</p>

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。

程序

1. 移至「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。 <ul style="list-style-type: none"> • 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	<p>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。</p> <p>如需詳細資訊，請參閱標準 Token 變數 第 C-3 頁和進階安全威脅活動 Token 變數 第 C-3 頁。</p>

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。

程序

1. 移至「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。

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。 <ul style="list-style-type: none"> 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-3 頁 和進階安全威脅活動 Token 變數 第 C-3 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。

程序

1. 移至「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。
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。 <ul style="list-style-type: none"> • 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	<p>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。</p> <p>如需詳細資訊，請參閱標準 Token 變數 第 C-3 頁和進階安全威脅活動 Token 變數 第 C-3 頁。</p>

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。

程序

1. 移至「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。

設定	說明
指定套用於單一端點的警訊門檻值	<p>選取以傳送僅符合指定條件之偵測的事件通知。</p> <ul style="list-style-type: none"> 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	<p>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。</p> <p>如需詳細資訊，請參閱標準 Token 變數 第 C-3 頁和進階安全威脅活動 Token 變數 第 C-3 頁。</p>

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。

程序

1. 移至「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。 <ul style="list-style-type: none"> • 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	<p>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。</p> <p>如需詳細資訊，請參閱標準 Token 變數 第 C-3 頁和進階安全威脅活動 Token 變數 第 C-3 頁。</p>

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。

程序

1. 移至「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-3 頁和內容策略違規 Token 變數 第 C-5 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-3 頁和內容策略違規 Token 變數 第 C-5 頁。
SNMP Trap	Control Manager 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 Control Manager 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。

程序

1. 移至「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-3 頁 和 Web 存取安全違規 Token 變數 第 C-5 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-3 頁 和 Web 存取安全違規 Token 變數 第 C-5 頁 。
SNMP Trap	Control Manager 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	在 IP 網路中轉送記錄檔訊息的標準 Control Manager 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」。

Data Loss Prevention 事件

使用「事件通知」畫面來啟動並設定您網路上偵測到的 Data Loss Prevention 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。

程序

1. 移至「通知 > 事件通知」。
會出現「事件通知」畫面。
2. 按一下「Data Loss Prevention」。
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。 <ul style="list-style-type: none"> 已關閉 任何變更
依嚴重性層級過濾	選取下列一或多個風險等級。 <ul style="list-style-type: none"> 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-3 頁和 Data Loss Prevention Token 變數 第 C-6 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。

程序

- 移至「通知 > 事件通知」。
會出現「事件通知」畫面。

2. 按一下「Data Loss Prevention」。
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	<p>選取此選項會將事件記錄附加到通知。</p> <ul style="list-style-type: none"> • 選取 DLP 合規官會接收的內容： <ul style="list-style-type: none"> • 來自所有受管理使用者的事件 • 僅來自直屬員工的事件 <hr/> <p> 注意 DLP 事件檢閱者只接收來自直屬員工的事件</p> <hr/> <ul style="list-style-type: none"> • 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	<p>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。</p> <p>如需詳細資訊，請參閱標準 Token 變數 第 C-3 頁和 Data Loss Prevention Token 變數 第 C-6 頁。</p>

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。

程序

1. 移至「通知 > 事件通知」。
會出現「事件通知」畫面。
2. 按一下「Data Loss Prevention」。
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	<p>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。</p> <p>如需詳細資訊，請參閱標準 Token 變數 第 C-3 頁和 Data Loss Prevention Token 變數 第 C-6 頁。</p>

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。

程序

1. 移至「通知 > 事件通知」。
會出現「事件通知」畫面。
2. 按一下「Data Loss Prevention」。
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-3 頁和 Data Loss Prevention 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」。

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。

程序

1. 移至「通知 > 事件通知」。
會出現「事件通知」畫面。
2. 按一下「Data Loss Prevention」。
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。

- 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。

- 選取通知的收件者。
 - 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。
 - 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。
- 啟動下列一或多個通知方法。

方法	說明
電子郵件訊息	<p>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。</p> <p>如需詳細資訊，請參閱標準 Token 變數 第 C-3 頁和 Data Loss Prevention Token 變數 第 C-6 頁。</p>

- 如果要測試收件者是否可以接收事件通知，請按一下「測試」。
- 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。

程序

- 移至「通知 > 事件通知」。

會出現「事件通知」畫面。

2. 按一下「Data Loss Prevention」。

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-3 頁和 Data Loss Prevention 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」。

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。

程序

1. 移至「通知 > 事件通知」。
會出現「事件通知」畫面。
2. 按一下「Data Loss Prevention」。
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-3 頁和 Data Loss Prevention 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」。

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。

程序

1. 移至「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	<p>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。</p> <p>如需詳細資訊，請參閱標準 Token 變數 第 C-3 頁、已知的安全威脅活動 Token 變數 第 C-8 頁和網路存取控制 Token 變數 第 C-10 頁。</p>
Windows 事件記錄檔	<p>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。</p> <p>如需詳細資訊，請參閱標準 Token 變數 第 C-3 頁、已知的安全威脅活動 Token 變數 第 C-8 頁和網路存取控制 Token 變數 第 C-10 頁。</p>
SNMP Trap	Control Manager 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	Control Manager 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。

程序

1. 移至「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-3 頁 和已知的安全威脅活動 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-3 頁 和已知的安全威脅活動 Token 變數 第 C-8 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	Control Manager 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。

程序

- 移至「通知 > 事件通知」。
會出現「事件通知」畫面。
- 按一下「已知的安全威脅活動」。
會出現事件清單。
- 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	<p>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。</p> <p>如需詳細資訊，請參閱標準 Token 變數 第 C-3 頁、已知的安全威脅活動 Token 變數 第 C-8 頁和網路存取控制 Token 變數 第 C-10 頁。</p>
Windows 事件記錄檔	<p>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。</p> <p>如需詳細資訊，請參閱標準 Token 變數 第 C-3 頁、已知的安全威脅活動 Token 變數 第 C-8 頁和網路存取控制 Token 變數 第 C-10 頁。</p>
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	Control Manager 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。

程序

1. 移至「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	<p>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。</p> <p>如需詳細資訊，請參閱標準 Token 變數 第 C-3 頁和已知的安全威脅活動 Token 變數 第 C-8 頁。</p>

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-3 頁和已知的安全威脅活動 Token 變數 第 C-8 頁。
SNMP Trap	Control Manager 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	Control Manager 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。

程序

1. 移至「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-3 頁和已知的安全威脅活動 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-3 頁和已知的安全威脅活動 Token 變數 第 C-8 頁。
SNMP Trap	Control Manager 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	Control Manager 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。

程序

1. 移至「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	<p>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。</p> <p>如需詳細資訊，請參閱標準 Token 變數 第 C-3 頁和已知的安全威脅活動 Token 變數 第 C-8 頁。</p>
Windows 事件記錄檔	<p>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。</p> <p>如需詳細資訊，請參閱標準 Token 變數 第 C-3 頁和已知的安全威脅活動 Token 變數 第 C-8 頁。</p>

方法	說明
SNMP Trap	Control Manager 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	Control Manager 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。

程序

1. 移至「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-3 頁和已知的安全威脅活動 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-3 頁和已知的安全威脅活動 Token 變數 第 C-8 頁。
SNMP Trap	Control Manager 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	Control Manager 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。

程序

1. 移至「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-3 頁和已知的安全威脅活動 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-3 頁和已知的安全威脅活動 Token 變數 第 C-8 頁。
SNMP Trap	Control Manager 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	Control Manager 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。

程序

1. 移至「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	<p>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。</p> <p>如需詳細資訊，請參閱標準 Token 變數 第 C-3 頁 和已知的安全威脅活動 Token 變數 第 C-8 頁。</p>
Windows 事件記錄檔	<p>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。</p> <p>如需詳細資訊，請參閱標準 Token 變數 第 C-3 頁 和已知的安全威脅活動 Token 變數 第 C-8 頁。</p>
SNMP Trap	Control Manager 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	Control Manager 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。

程序

1. 移至「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-3 頁和已知的安全威脅活動 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-3 頁和已知的安全威脅活動 Token 變數 第 C-8 頁。
SNMP Trap	Control Manager 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	Control Manager 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。

程序

1. 移至「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-3 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-3 頁。
SNMP Trap	Control Manager 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。

程序

- 移至「通知 > 事件通知」。
會出現「事件通知」畫面。
- 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-3 頁 和 網路存取控制 Token 變數 第 C-10 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-3 頁 和 網路存取控制 Token 變數 第 C-10 頁 。
SNMP Trap	Control Manager 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	Control Manager 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 Control Manager 與受管理產品伺服器之間發生連線錯誤時通知管理員。

程序

1. 移至「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-3 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。

程序

1. 移至「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-3 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-3 頁。
SNMP Trap	Control Manager 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	Control Manager 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。

程序

1. 移至「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-3 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-3 頁。
SNMP Trap	Control Manager 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	Control Manager 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」。

即時掃描已關閉

設定下列事件通知，以在「即時掃描」關閉時通知管理員。

程序

1. 移至「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「即時掃描已關閉」。
會出現「即時掃描已關閉」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-3 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-3 頁。
SNMP Trap	Control Manager 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	Control Manager 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。

程序

1. 移至「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「即時掃描已啟動」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-3 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-3 頁。
SNMP Trap	Control Manager 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	Control Manager 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。

程序

1. 移至「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-3 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-3 頁。
SNMP Trap	Control Manager 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	Control Manager 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。

程序

1. 移至「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-3 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-3 頁。
SNMP Trap	Control Manager 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	Control Manager 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。

程序

1. 移至「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-3 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-3 頁 。
SNMP Trap	Control Manager 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	Control Manager 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。

程序

1. 移至「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-3 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-3 頁。
SNMP Trap	Control Manager 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	Control Manager 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」。

掃描引擎更新成功

設定下列事件通知，以在掃描引擎更新成功時通知管理員。

程序

1. 移至「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「掃描引擎更新成功」。

會出現「掃描引擎更新成功」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-3 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-3 頁 。
SNMP Trap	Control Manager 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	Control Manager 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」。

掃描引擎更新未成功

設定下列事件通知，以在掃描引擎更新未成功時通知管理員。

程序

1. 移至「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「掃描引擎更新未成功」。
會出現「掃描引擎更新未成功」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-3 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-3 頁。
SNMP Trap	Control Manager 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	Control Manager 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 16 章

報告

本節討論如何使用從所有受管理產品（已向 Control Manager 註冊）收集的資料，建立報告。

包含下列主題：

- [報告總覽 第 16-2 頁](#)
- [自訂範本 第 16-2 頁](#)
- [一次性報告 第 16-18 頁](#)
- [預約報告 第 16-22 頁](#)
- [設定報告維護 第 16-31 頁](#)
- [檢視我的報告 第 16-31 頁](#)

報告總覽

Control Manager 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 Control Manager 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。

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。Control Manager 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

自訂範本會使用資料檢視來定義報告資料的範圍。

如需有關報告資料檢視的詳細資訊，請參閱[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 16-3 頁 。
刪除自訂範本	選取現有的範本，然後按一下「刪除」。

工作	說明
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 16-3 頁 。
複製自訂範本	選取現有的範本，然後按一下「複製」。Control Manager 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 16-3 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 Control Manager。
匯出自訂範本	選取現有的範本，然後按一下「匯出」。Control Manager 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。

程序

1. 移至「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」。

Control Manager 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 16-1. 報告項目

範本項目	說明
靜態文字	<p>提供使用者定義內容的容器</p> <hr/> <p> 注意 靜態文字內容最多可包含 4096 個字元。</p> <hr/> <p>如需詳細資訊，請參閱設定靜態文字報告項目 第 16-6 頁。</p>
長條圖	<p>插入可自訂的長條圖物件</p> <p>如需詳細資訊，請參閱設定長條圖報告項目 第 16-7 頁。</p>

範本項目	說明
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 16-9 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 16-12 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 16-14 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 16-17 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。

新增報告範本

範本內容 顯示作用中面板

名稱：

說明：

在上方插入分頁 在上方插入列

靜態文字 編輯 刪除

ABCabc
未命名

刪除此列 在下方插入列

在上方插入分頁 在上方插入列

長條圖 編輯 刪除

未命名

刪除此列 在下方插入列

儲存 取消

圖 16-1. 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 16-3 頁。

程序

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。

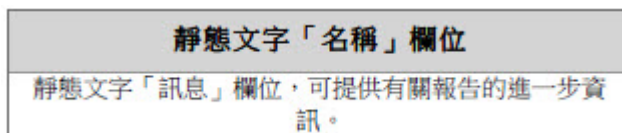


圖 16-2. 靜態文字報告輸出範例

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 16-3 頁。

程序

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。

Control Manager 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 16-3 頁。

程序

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



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。
Control Manager 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 16-3 頁](#)。

程序

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。

Control Manager 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 16-3 頁](#)。

程序

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。

Control Manager 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 16-3 頁](#)。

程序

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。

Control Manager 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，Control Manager 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 16-19 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。
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。 <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  注意 您無法編輯先前產生的一次性報告資料檔。 </div>

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。

程序

- 移至「報告 > 一次性報告」。
會出現「一次性報告」畫面。
- 請點選「新增」。
會出現「新增一次性報告 > 步驟 1：內容」畫面。
- 在「名稱」欄位中輸入報告的名稱。
- （選用）在「說明」欄位中輸入報告的說明。
- 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 16-3 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。



注意

- 此版本的 Control Manager 不再支援 ActiveX 和 Crystal Report 格式。
 - 如果您是從舊版 Control Manager 移轉，則您仍可在 Control Manager 7.0 中下載先前產生的 Crystal Reports。
-

- 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. 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。
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。

程序



1. 移至「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 16-23 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 16-27 頁 。

工作	說明
複製預約報告資料檔	<p>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。</p> <p>按一下要編輯的已複製預約報告資料檔的「名稱」。</p> <p>如需詳細資訊，請參閱編輯預約報告 第 16-27 頁。</p>
刪除預約報告資料檔	<p>選取現有的預約報告資料檔，然後按一下「刪除」。</p>
檢視先前產生的預約報告	<p>按一下您要檢視的報告的「歷史記錄」欄中的「檢視」連結。</p> <p>如需詳細資訊，請參閱檢視預約報告 第 16-30 頁。</p>
啟動或關閉預約報告	<ul style="list-style-type: none"> • 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。 <hr/> <p> 注意 依預設，會啟動最近新增的預約報告資料檔。</p>

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。

程序

1. 移至「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 16-3 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。



注意

此版本的 Control Manager 不再支援 ActiveX 和 Crystal Report 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. 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。
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，Control Manager 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。

程序

1. 移至「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 16-3 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。



此版本的 Control Manager 不再支援 ActiveX 和 Crystal Report 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. 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。
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。

程序

1. 移至「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。

程序

1. 移至「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。

程序

1. 移至「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 17 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 17-2 頁](#)
- [功能需求 第 17-2 頁](#)
- [可疑物件清單管理 第 17-7 頁](#)
- [先發式可疑物件防護 第 17-19 頁](#)
- [連線的威脅防範產品整合 第 17-26 頁](#)

關於連線的威脅防範

Control Manager 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	<ul style="list-style-type: none"> Control Manager 7.0 (或更新版本) Deep Discovery Inspector 3.8 (或更新版本) 或 Deep Discovery Analyzer 5.1 (或更新版本) <hr/>  注意 若要評估記錄檔資料，將需要至少一個選用產品。	<ul style="list-style-type: none"> OfficeScan 11.0 SP1 (或更新版本) Deep Security 10.0 (或更新版本) Endpoint Sensor 1.5 (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 2 (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) Cloud App Security 5.0 (或更新版本)

功能	必要產品	可選產品
<p>可疑物件清單同步處理</p> <p>如需詳細資訊，請參閱可疑物件清單 第 17-7 頁和連線的威脅防範產品整合 第 17-26 頁。</p>	<ul style="list-style-type: none"> • Control Manager 7.0（或更新版本） • Deep Discovery Inspector 3.8（或更新版本）或 Deep Discovery Analyzer 5.1（或更新版本） <hr/> <p> 注意 若要進行同步處理，將需要至少一個選用產品。</p>	<ul style="list-style-type: none"> • 主動式雲端截毒技術伺服器 3.0 Patch 1（或更新版本） • OfficeScan 11.0 SP1（或更新版本） • Deep Security 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 2（或更新版本） • Trend Micro Endpoint Application Control 2.0 SP1（或更新版本） • Cloud App Security 5.0（或更新版本）

功能	必要產品	可選產品
可疑物件樣本提交	<ul style="list-style-type: none">• Deep Discovery Inspector 3.8 (或更新版本) 或 Deep Discovery Analyzer 5.1 (或更新版本)	<ul style="list-style-type: none">• Deep Security 10.0 (或更新版本)• OfficeScan 11.0 SP1 (或更新版本)• Endpoint Sensor 1.5 (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 2 (或更新版本)• ScanMail for Microsoft Exchange 12.5 (或更新版本)• Deep Discovery Email Inspector 3.0 (或更新版本)

功能	必要產品	可選產品
可疑物件管理	<ul style="list-style-type: none">• Control Manager 7.0 (或更新版本)• Deep Discovery Inspector 3.8 (或更新版本) 或 Deep Discovery Analyzer 5.1 (或更新版本)	<ul style="list-style-type: none">• OfficeScan 11.0 SP1 (或更新版本)• Deep Security 10.0 (或更新版本)• Endpoint Sensor 1.5 (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 2 (或更新版本)• Trend Micro Endpoint Application Control 2.0 SP1 (或更新版本)• Cloud App Security 5.0 (或更新版本)

功能	必要產品	可選產品
<p>可疑物件中毒處理行動</p> <p>如需詳細資訊，請參閱可疑物件中毒處理行動第 17-10 頁。</p>	<ul style="list-style-type: none"> Control Manager 7.0 (或更新版本) 	<ul style="list-style-type: none"> 主動式雲端載毒技術伺服器 3.0 Patch 1 (或更新版本) OfficeScan 11.0 SP1 (或更新版本) Deep Security 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 2 (或更新版本) Trend Micro Endpoint Application Control 2.0 SP1 (或更新版本) Cloud App Security 5.0 (或更新版本)
影響評估	<ul style="list-style-type: none"> Control Manager 7.0 (或更新版本) Endpoint Sensor 1.5 (或更新版本) 	<ul style="list-style-type: none"> 無
<p>端點隔離</p> <p>如需詳細資訊，請參閱隔離端點第 17-24 頁。</p>	<ul style="list-style-type: none"> Control Manager 7.0 (或更新版本) OfficeScan 11.0 SP1 (或更新版本) 	<ul style="list-style-type: none"> Endpoint Sensor 1.5 (或更新版本)
IOC 管理	<ul style="list-style-type: none"> Control Manager 7.0 (或更新版本) Endpoint Sensor 1.5 (或更新版本) 	<ul style="list-style-type: none"> 無

可疑物件清單管理

Control Manager 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。

Control Manager 會整合沙盒虛擬平台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 Control Manager 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 17-2 頁](#)中的〈可疑物件清單同步處理〉。

可疑物件清單

Control Manager 會整合沙盒虛擬平台可疑物件清單，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 Control Manager 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 17-10 頁](#)。

清單類型	說明
沙盒虛擬平台可疑物件	<p>與沙盒虛擬平台整合的受管理產品會提交可疑檔案或 URL 給沙盒虛擬平台來進行分析。如果沙盒虛擬平台判定物件是可能的安全威脅，則沙盒虛擬平台會將物件新增至「可疑物件」清單。沙盒虛擬平台接著會將清單傳送至其已註冊的 Control Manager 伺服器，來進行彙總和同步處理。</p> <p>在 Control Manager 主控台中，移至「管理 > 可疑物件 > 沙盒虛擬平台物件 > 物件」標籤，以檢視「沙盒虛擬平台可疑物件」清單。</p>
沙盒虛擬平台可疑物件例外	<p>Control Manager 管理員可以從沙盒虛擬平台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。</p> <p>在 Control Manager 主控台上，移至「管理 > 可疑物件 > 沙盒虛擬平台物件 > 例外」標籤，來檢視沙盒虛擬平台可疑物件例外。</p> <p>Control Manager 會將例外清單傳送給訂閱此清單的沙盒虛擬平台。當沙盒虛擬平台偵測到可疑物件，而該物件列在例外清單中時，沙盒虛擬平台會將該物件視為「安全」，並且不會再次分析該物件。</p> <p>如需詳細資訊，請參閱將例外新增到沙盒虛擬平台可疑物件清單 第 17-8 頁。</p>
使用者定義的可疑物件	<p>Control Manager 管理員可以在「管理 > 可疑物件 > 使用者定義的物件」中，新增其認為可疑，但目前不在沙盒虛擬平台可疑物件清單中的物件。</p> <p>如需詳細資訊，請參閱先發式可疑物件防護 第 17-19 頁。</p>

將例外新增到沙盒虛擬平台可疑物件清單

Control Manager 允許您根據檔案 SHA-1、網域、IP 位址或 URL，將物件從「沙盒虛擬平台可疑物件」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「沙盒虛擬平台可疑物件」清單。

程序

1. 移至「管理 > 可疑物件 > 沙盒虛擬平台物件」。
會出現「沙盒虛擬平台可疑物件」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 SHA-1：指定檔案的 SHA-1 雜湊值。
 - IP 位址：指定 IP 位址。
 - URL：指定 URL。
 - 網域：指定網域。

Control Manager 允許您使用萬用字元 (*) 從沙盒虛擬平台可疑物件清單排除特定子網域或子目錄。

範例	說明
<code>https://*.domain.com/</code>	從沙盒虛擬平台可疑物件清單排除網域 “domain.com” 的所有子網域
<code>*.abc.domain.com</code>	從沙盒虛擬平台可疑物件清單排除子網域 “abc” 的所有子網域
<code>https://*.domain.com/abc/*</code>	從沙盒虛擬平台可疑物件清單排除網域 “domain.com” 的所有子網域和子目錄 “abc” 的子目錄

5. (選用) 指定「便利貼」，協助識別可疑物件。
6. 請點選「新增」。

物件會顯示在「沙盒虛擬平台例外」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 Control Manager 主控台，設定特定受管理產品在偵測到「沙盒虛擬平台可疑物件」清單或「使用者定義的可疑物件」清單中的特定可疑物件時，所要採取的中毒處理行動。

表 17-1. 中毒處理行動產品支援

產品	沙盒虛擬平台清單	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： <ul style="list-style-type: none"> • 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： <ul style="list-style-type: none"> • 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 10.0 (或更新版本)	對下列可疑物件類型執行處理行動： <ul style="list-style-type: none"> • 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： <ul style="list-style-type: none"> • 檔案：記錄、封鎖、隔離 • URL：記錄、封鎖
<ul style="list-style-type: none"> • 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： <ul style="list-style-type: none"> • 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： <ul style="list-style-type: none"> • 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

產品	沙盒虛擬平台清單	使用者定義的清單
InterScan Messaging Security Virtual Appliance 9.1 (或更新版本)	<p>對下列可疑物件類型執行處理行動：</p> <ul style="list-style-type: none"> 檔案：記錄、封鎖、隔離 	<p>對下列可疑物件類型執行處理行動：</p> <ul style="list-style-type: none"> 檔案：記錄、封鎖、隔離 檔案 SHA-1：記錄、封鎖、隔離
InterScan Web Security Virtual Appliance 6.5 Patch 2 (或更新版本)	<p>對下列可疑物件類型執行處理行動：</p> <ul style="list-style-type: none"> 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 	<p>對下列可疑物件類型執行處理行動：</p> <ul style="list-style-type: none"> 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)	<p>對下列可疑物件類型執行處理行動：</p> <ul style="list-style-type: none"> 檔案：記錄、封鎖、隔離 	<p>對下列可疑物件類型執行處理行動：</p> <ul style="list-style-type: none"> 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)	<p>對下列可疑物件類型執行處理行動：</p> <ul style="list-style-type: none"> 檔案：記錄、封鎖、隔離 URL：記錄、封鎖 	<p>對下列可疑物件類型執行處理行動：</p> <ul style="list-style-type: none"> 檔案：記錄、封鎖、隔離 URL：記錄、封鎖

產品	沙盒虛擬平台清單	使用者定義的清單
<ul style="list-style-type: none"> 主動式雲端截毒技術伺服器 3.0 Patch 1 (或更新版本) OfficeScan 11.0 SP1 (或更新版本) 整合式主動式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式雲端截毒技術伺服器 	<p>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：</p> <ul style="list-style-type: none"> URL：記錄、封鎖 	<p>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：</p> <ul style="list-style-type: none"> URL：記錄、封鎖 <hr/> <p> 重要 主動式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。</p> <hr/> <p> 注意 只有特定的受管理產品可以對可疑 URL 物件直接執行 Control Manager 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。</p> <p>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。Control Manager 會解譯從受管理產品傳送的記錄檔，然後在 Control Manager 主控台上顯示可疑物件偵測。</p>

設定預設設定

設定預設設定，可讓 Control Manager 整合沙盒虛擬平台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。

Control Manager 還可將可疑 IP 位址和網域傳送至 TippingPoint。

程序

- 移至「管理 > 可疑物件 > 預設設定」。
會出現「預設設定」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 Control Manager 做為沙盒虛擬平台來源時使用：
 - 服務 URL：Control Manager 的服務 URL
 - API 金鑰：用來將 Control Manager 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. 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**

Control Manager 會傳送 Deep Discovery Inspector 和 Deep Discovery Analyzer 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。

- b. 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。
- c. (選用) 按一下「測試連線」，可確認連線。
- d. 選取會觸發 Control Manager 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
4. 按一下「儲存」。
 5. 按一下「立即同步處理」。
-

可疑物件偵測

您可以使用 Control Manager 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 17-14 頁](#)
 - [使用 Endpoint Sensor 評估影響 第 17-16 頁](#)
-




注意

Control Manager 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 Control Manager 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

Control Manager 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。


必要產品	可選產品
<ul style="list-style-type: none"> Control Manager 7.0 (或更新版本) 至少一個選用產品 	<ul style="list-style-type: none"> 使用 Control Manager 管理的趨勢科技產品 Endpoint Sensor 1.5 (或更新版本) <hr/> <p> 重要</p> <ul style="list-style-type: none"> Endpoint Sensor 1.5 僅提供與「檔案」和「IP 位址」可疑物件類型相關的資訊。 Endpoint Sensor 1.6 (或更新版本) 會提供與「檔案」、「IP 位址」和「網域」可疑物件類型相關的資訊。

程序

- 在 Control Manager 主控台中，移至「管理 > 可疑物件 > 沙盒虛擬平台物件」。
- 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。

使用 Endpoint Sensor 評估影響

Endpoint Sensor 會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。

必要產品	可選產品
<ul style="list-style-type: none"> • Control Manager 7.0 (或更新版本) • Endpoint Sensor 1.5 (或更新版本) <hr/> <p> 重要</p> <ul style="list-style-type: none"> • Endpoint Sensor 1.5 僅提供與「檔案」和「IP 位址」可疑物件類型相關的資訊。 • Endpoint Sensor 1.6 (或更新版本) 會提供與「檔案」、「IP 位址」和「網域」可疑物件類型相關的資訊。 	<ul style="list-style-type: none"> • 無

程序

1. 在 Control Manager 主控台中，移至「管理 > 可疑物件 > 沙盒虛擬平台物件」。
2. 選取您要評估之「物件」旁的核取方塊。
3. 按一下「評估影響」。

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。

Endpoint Sensor 中的回溯掃瞄

回溯掃瞄會根據指定的搜尋條件，調查歷史事件及其活動鏈。結果可以思考映射圖（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。


回溯掃描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

回溯掃描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。

必要產品	可選產品
<ul style="list-style-type: none"> Control Manager 7.0 (或更新版本) Deep Discovery Inspector 3.8 (或更新版本) 或 Deep Discovery Analyzer 5.1 (或更新版本) 需要至少一個選用產品，才能檢視「影響評估」與「緩和」資料 	<ul style="list-style-type: none"> 使用 Control Manager 管理的趨勢科技產品 Endpoint Sensor 1.5 (或更新版本) <hr/> <p> 重要</p> <ul style="list-style-type: none"> Endpoint Sensor 1.5 僅提供與「檔案」和「IP 位址」可疑物件類型相關的資訊。 Endpoint Sensor 1.6 (或更新版本) 會提供與「檔案」、「IP 位址」和「網域」可疑物件類型相關的資訊。

程序

1. 在 Control Manager 主控台中，移至「管理 > 可疑物件 > 沙盒虛擬平台物件」。
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	<p>顯示可疑物件的第一次和最近一次分析的相關資訊</p> <p>Control Manager 與下列產品整合，使用沙盒虛擬平台分析其他受管理產品所提交的可疑物件：</p> <ul style="list-style-type: none"> Deep Discovery Analyzer 5.1 (或更新版本) Deep Discovery Endpoint Inspector 3.0 (或更新版本) Deep Discovery Inspector 3.8 (或更新版本)

標籤	說明
分析	<p>顯示沙盒虛擬平台對所提交物件的分析</p> <p>沙盒虛擬平台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。</p>
發佈	<p>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</p> <p>Control Manager 會整合沙盒虛擬平台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。</p>
影響評估與緩和	<p>顯示受可疑物件影響的所有端點和使用者</p> <ul style="list-style-type: none"> • 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」。 <p>按一下「可疑活動」連結，可進一步調查物件如何影響使用者或端點。</p>

先發式可疑物件防護

Control Manager 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，或是匯入「入侵指標 (IOC)」，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	<p>「使用者定義的可疑物件」清單可讓您定義已註冊沙盒虛擬平台在網路上尚未偵測到的可疑檔案、IP 位址、URL 和網域物件。</p> <p>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。</p> <p>將物件新增到使用者定義的可疑物件清單 第 17-20 頁</p> <p>可疑物件中毒處理行動 第 17-10 頁</p>
入侵指標	<p>匯入 IOC 檔案以便對網路上的端點執行深度的歷史分析，進而判斷安全威脅是否已經影響到您的環境。</p> <p>對 IOC 執行影響評估時，需要有關端點歷來行為的詳細記錄檔資訊。只有已安裝 Endpoint Sensor 1.5（或更新版本）的端點才能收集執行這種詳細分析類型所需的必要記錄檔資訊。</p> <p>透過整合 OfficeScan 11.0 SP1（或更新版本）用戶端，您可以隔離受影響的端點，以防止端點上識別的安全威脅進一步擴散。</p> <p>對 IOC 進行影響評估和回應 第 17-22 頁</p>

將物件新增到使用者定義的可疑物件清單

您可以透過將可疑物件新增到「使用者定義的可疑物件」清單，保護您的網路免受尚未識別之物件的侵襲。Control Manager 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（不包括網域物件）後採取的中毒處理行動。

程序

- 移至「管理 > 可疑物件 > 使用者定義的物件」。
 - 會出現「使用者定義的可疑物件」畫面。
 - 請點選「新增」。
 - 指定物件的「類型」。
- 檔案：按一下「瀏覽」上傳可疑物件檔案。

- 檔案 SHA-1：指定檔案的 SHA-1 雜湊值。
 - IP 位址：指定 IP 位址。
 - URL：指定 URL。
 - 網域：指定網域。
4. 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**

此選項僅適用於「檔案」或「檔案 SHA-1」物件。

5. （選用）指定「便利貼」，協助識別可疑物件。
6. 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。

程序

1. 移至「管理 > 可疑物件 > 使用者定義的物件」。
會出現「使用者定義的可疑物件」畫面。
2. 請點選「匯入」。

3. 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。

4. 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。

對 IOC 進行影響評估和回應

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 IOC 檔案後，請將檔案匯入至 Control Manager，以判斷您的網路中是否存在安全威脅並採取緩和措施，以防止安全威脅散佈到其他端點。



重要

- 如果要對外部 IOC 資料進行影響評估，必須將 Endpoint Sensor 1.5（或更新版本）向 Control Manager 註冊並安裝在目標端點上。
 - 如果要隔離端點，必須在目標端點上安裝 OfficeScan 11.0 SP1（或更新版本）用戶端並啟動 OfficeScan 防火牆。
-

程序

1. 移至「管理 > 入侵指標」。
會出現「入侵指標 (IOC)」畫面。
2. 請點選「新增」。
3. 選取您要用做調查來源的 IOC 檔案。
4. 按一下「上傳」。
會出現一個畫面，其中列出檔案中包含的受支援指標。

5. 如果要啟動調查，請從清單中選取 IOC 檔案，然後按一下「評估影響」。會出現「立即調查」畫面。
6. 從「目標端點」下拉列表中選取「全部」或「特定」，然後輸入要調查的端點名稱或 IP 位址。
使用新行來新增多個端點名稱或 IP 位址。
7. 按一下「立即調查」。

**注意**

執行調查可能需要一些時間才能完成。在「進度」欄中監控調查進度。

8. 評估完成後，按一下「有風險」欄中的數字可檢視更多詳細資料，或對受影響的端點採取處理行動。

**注意**

「暫停中/有問題」欄會顯示評估尚未完成的端點數目。例如，在端點重新連線到網路之前，無法開始對端點進行評估。

會出現「入侵指標 > 有風險的端點」畫面。

9. 如果要防止可疑物件在您的網路中散佈，請按一下「處理行動」欄中的「隔離」，以停止受影響端點上的網路流量。

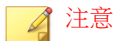
**重要**

如果要隔離端點，必須在目標端點上安裝 OfficeScan 11.0 SP1（或更新版本）用戶端並啟動 OfficeScan 防火牆。

10. 按一下「修改允許的流量」按鈕，可以選擇性地設定所有已隔離端點的允許輸入和輸出流量。
 - 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。

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。

必要產品	可選產品
<ul style="list-style-type: none"> • Control Manager 7.0 (或更新版本) • OfficeScan 11.0 SP1 (或更新版本) <hr/> <div style="display: flex; align-items: center;"> <p>重要 如果要隔離端點，必須在目標端點上安裝 OfficeScan 用戶端並啟動 OfficeScan 防火牆。</p> </div>	<ul style="list-style-type: none"> • Endpoint Sensor 1.5 (或更新版本)

程序

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. 在顯示的「端點 — {名稱}」畫面中，按一下「工作 > 隔離」。

Control Manager 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 Control Manager 的使用者帳號沒有必要權限。
5. 「端點 — {名稱}」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 Control Manager 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 > 網路連線 > 已隔離」節點。
 7. 按一下「修改允許的流量」按鈕，可以選擇性地設定所有已隔離端點的允許輸入和輸出流量。
 - 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 — {名稱}：按一下「工作 > 還原」。
 - 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「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。

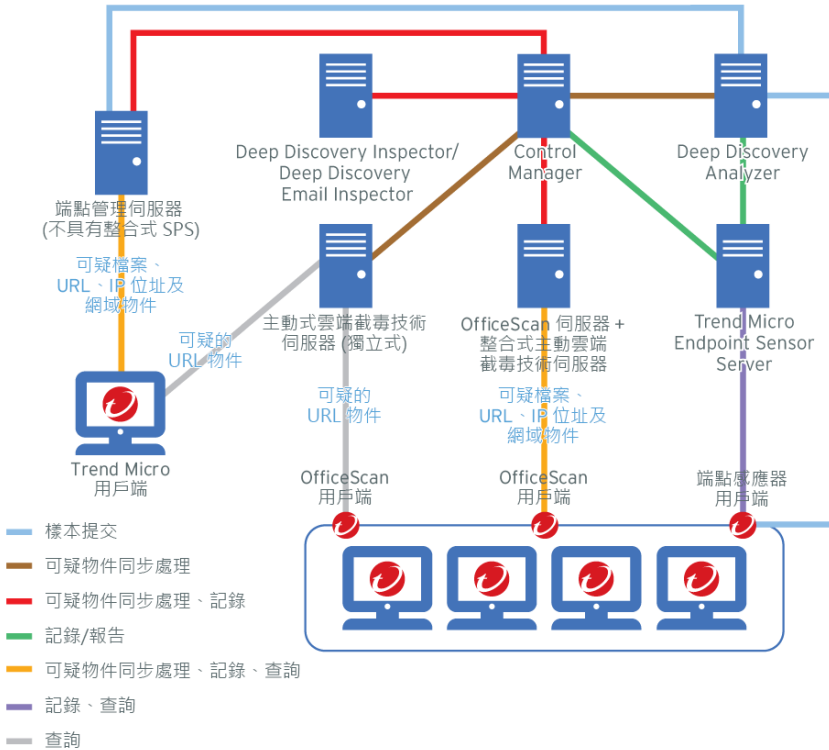


圖 17-1. 端點防護

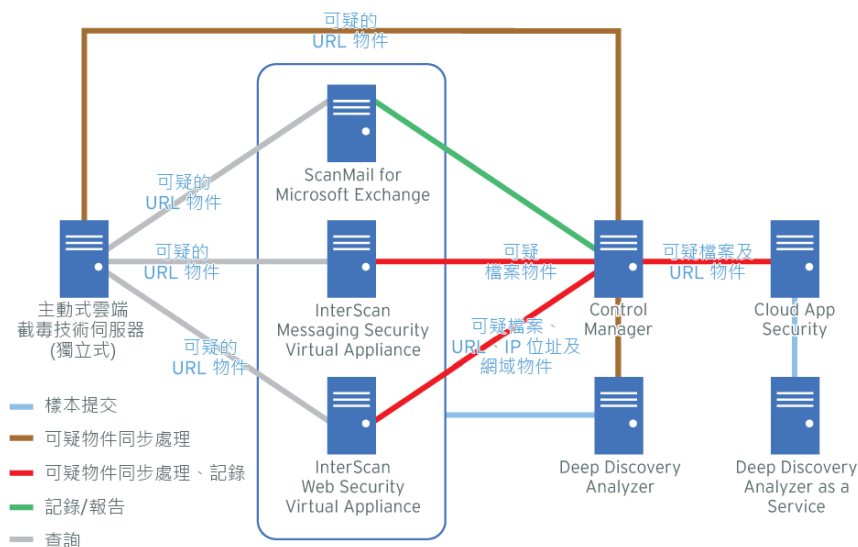


圖 17-2. 傳訊和網路安全

Control Manager 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 Control Manager 註冊資訊和可疑物件清單同步處理資訊，請參閱下列內容：

- [Control Manager 第 17-28 頁](#)
- [Deep Discovery Analyzer 第 17-29 頁](#)
- [Trend Micro Endpoint Sensor 第 17-30 頁](#)
- [Deep Discovery Inspector 第 17-30 頁](#)
- [Deep Security 第 17-31 頁](#)
- [OfficeScan 第 17-32 頁](#)

- [主動式雲端截毒技術伺服器 第 17-33 頁](#)
- [InterScan Messaging Security Virtual Appliance 第 17-34 頁](#)
- [InterScan Web Security Virtual Appliance 第 17-35 頁](#)
- [ScanMail for Microsoft Exchange 第 17-36 頁](#)
- [Trend Micro Endpoint Application Control 第 17-36 頁](#)
- [Deep Discovery Email Inspector 第 17-37 頁](#)
- [Cloud App Security 第 17-37 頁](#)

Control Manager

需求	說明
產品版本	7.0 (或更新版本)
Control Manager 註冊資訊	<p>對於未透過 Control Manager 主控台向 Control Manager 註冊的產品，需要下列 Control Manager 註冊資訊：</p> <ul style="list-style-type: none"> • 伺服器 FQDN 或 IP 位址 • 通訊埠：依預設，Control Manager 會使用 HTTP 通訊埠 80 或 HTTPS 通訊埠 443 <p>對於使用 Control Manager 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」。</p>
可疑物件清單同步處理	<p>對於不會自動將「可疑物件」清單與 Control Manager 同步處理的產品，需要下列 API 資訊：</p> <ul style="list-style-type: none"> • API 金鑰：如果要取得 API 金鑰，請開啟 Control Manager 管理主控台並移至「管理 > 可疑物件 > 預設設定」。

需求	說明
整合式連線的威脅防範功能	<ul style="list-style-type: none"> • 安全威脅監控 • 可疑物件清單同步處理 • 可疑物件管理 • 影響評估 • 端點隔離 • IOC 管理

Deep Discovery Analyzer

需求	說明
產品版本	5.1 (或更新版本)
Control Manager 註冊	從 Control Manager 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」，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 Control Manager 註冊後自動執行 依預設，「可疑物件」清單會每隔 10 分鐘與 Control Manager 伺服器同步處理一次。
整合式連線的威脅防範功能	<ul style="list-style-type: none"> • 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

Trend Micro Endpoint Sensor



注意

- 先前名為 Deep Discovery Endpoint Sensor（1.5 版和較早版本）。
- Endpoint Sensor 不支援可疑物件清單同步處理。

需求	說明
產品版本	1.5（或更新版本）
Control Manager 註冊	從 Control Manager 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」，從「伺服器類型」清單中選取產品，然後按一下「新增」。
整合式連線的威脅防範功能	<ul style="list-style-type: none"> • 安全威脅監控 • 可疑物件樣本提交 • 可疑物件管理 • 影響評估 • 端點隔離 • IOC 管理

Deep Discovery Inspector

需求	說明
產品版本	3.8（或更新版本）

需求	說明
Control Manager 註冊	<p>從 Deep Discovery Inspector 管理主控台（「管理 > 整合的產品/服務 > Control Manager」）</p> <p>需要的 Control Manager 資訊：</p> <ul style="list-style-type: none"> • 伺服器 FQDN 或 IP 位址 • 通訊埠：依預設，Control Manager 會使用 HTTP 通訊埠 80 或 HTTPS 通訊埠 443 <p>如需詳細資訊，請參閱《Deep Discovery Inspector 管理手冊》。</p>
可疑物件清單同步處理	<p>從 Deep Discovery Inspector 管理主控台（「管理 > 整合的產品/服務 > Control Manager」）</p> <p>需要的 Control Manager 資訊：</p> <ul style="list-style-type: none"> • API 金鑰：如果要取得 API 金鑰，請開啟 Control Manager 管理主控台並移至「管理 > 可疑物件 > 預設設定」。 <p>如需詳細資訊，請參閱《Deep Discovery Inspector 管理手冊》。</p>
整合式連線的威脅防範功能	<ul style="list-style-type: none"> • 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 Security

需求	說明
產品版本	10.0（或更新版本）
Control Manager 註冊	從 Control Manager 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」，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 Control Manager 註冊後自動執行

需求	說明
整合式連線的威脅防範功能	<ul style="list-style-type: none"> 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

OfficeScan

需求	說明
產品版本	11.0 SP1 (或更新版本)
Control Manager 註冊	<p>從 OfficeScan Web 主控台的「管理 > 設定 > Control Manager」</p> <p>需要的 Control Manager 資訊：</p> <ul style="list-style-type: none"> 伺服器 FQDN 或 IP 位址 通訊埠：依預設，Control Manager 會使用 HTTP 通訊埠 80 或 HTTPS 通訊埠 443 <p>如需詳細資訊，請參閱《OfficeScan 管理手冊》。</p>
可疑物件清單同步處理	<p>從 OfficeScan Web 主控台的「管理 > 設定 > 可疑物件清單」</p> <p>需要的 Control Manager 資訊：</p> <ul style="list-style-type: none"> 無 <hr/> <p> 注意</p> <p>OfficeScan 會在 Control Manager 註冊期間自動從 Control Manager 伺服器取得所需的 API 金鑰資訊</p>

需求	說明
整合式連線的威脅防範功能	<ul style="list-style-type: none"> 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

主動式雲端截毒技術伺服器

需求	說明
產品版本	3.0 Patch 1 (或更新版本)
Control Manager 註冊	從 Control Manager 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」，從「伺服器類型」清單中選取產品，然後按一下「新增」。

需求	說明
可疑物件清單同步處理	<p>從主動式雲端截毒技術伺服器 Web 主控台：</p> <ul style="list-style-type: none"> 在主動式雲端截毒技術伺服器 3.0 Patch 1 中，請移至「主動式雲端截毒技術 > C&C 聯絡人警訊」 在主動式雲端截毒技術伺服器 3.0 Patch 2（或更新版本）中，移至「主動式雲端截毒技術 > 可疑物件」 <p>「可疑物件」清單來源的必要詳細資訊：</p> <ul style="list-style-type: none"> 服務 URL 通訊埠 <p>如果清單來源是 Control Manager，則預設的通訊埠為 HTTP 通訊埠 80 或 HTTPS 通訊埠 443。</p> <ul style="list-style-type: none"> API 金鑰：由伺服器管理員提供 <p>如果清單來源是 Control Manager，則開啟 Control Manager 管理主控台並移至「管理 > 可疑物件 > 預設設定」。</p> <hr/> <p> 注意</p> <p>在主動式雲端截毒技術伺服器 3.3（或更新版本）中，Control Manager 會在註冊期間自動傳送必要的 API 金鑰資訊到主動式雲端截毒技術伺服器。</p> <hr/> <p>如需詳細資訊，請參閱《主動式雲端截毒技術伺服器管理手冊》。</p>
整合式連線的威脅防範功能	<ul style="list-style-type: none"> 可疑物件清單同步處理 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）

需求	說明
Control Manager 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 Control Manager 註冊後自動執行
整合式連線的威脅防範功能	<ul style="list-style-type: none"> • 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 Appliance

需求	說明
產品版本	6.5 SP2 Patch 2 (或更新版本)
Control Manager 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	<ul style="list-style-type: none"> • 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)
Control Manager 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	<ul style="list-style-type: none"> 安全威脅監控 可疑物件樣本提交

Trend Micro Endpoint Application Control

需求	說明
產品版本	2.0 SP1 Patch 1 (或更新版本)
Control Manager 註冊	從 Control Manager 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」，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 Control Manager 註冊後自動執行
整合式連線的威脅防範功能	<ul style="list-style-type: none"> 安全威脅監控 可疑物件清單同步處理 可疑物件管理

Deep Discovery Email Inspector

需求	說明
產品版本	3.0 (或更新版本)
Control Manager 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	<ul style="list-style-type: none"> 可疑物件清單同步處理 可疑物件樣本提交

Cloud App Security

需求	說明
產品版本	5.0 (或更新版本)
Control Manager 註冊	從 Control Manager 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」，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 管理手冊》。
整合式連線的威脅防範功能	<ul style="list-style-type: none"> 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 18 章

Data Loss Prevention 事件

Control Manager 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 18-8 頁](#)

管理員工作

如果要啟動事件檢閱程序，Control Manager 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
<p>建立 DLP 事件調查專用的使用者帳號。您可以指派下列使用者角色來授與檢閱 DLP 事件的權限：</p> <ul style="list-style-type: none"> • 管理員和 DLP 合規官 • DLP 合規官 • DLP 事件檢閱者 <hr/> <p> 注意 「DLP 合規官」和「DLP 事件檢閱者」角色僅適用於 Active Directory 使用者。</p>	<ul style="list-style-type: none"> • 瞭解 DLP 使用者角色 第 18-5 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。	<ul style="list-style-type: none"> • 預約事件摘要 第 15-30 頁 • 事件詳細資料已更新 第 15-29 頁
匯出 DLP 記錄檔供稽核之用。	使用記錄查詢 第 14-2 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。

程序

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。

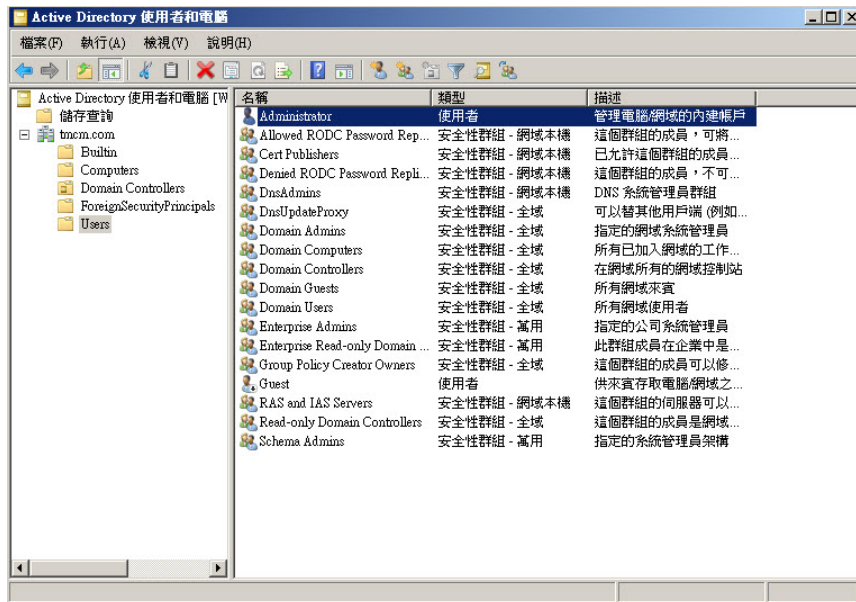


圖 18-1. Active Directory 使用者和電腦主控台

2. 按兩下使用者。

會出現「<使用者> 內容」畫面。

Administrator 內容

撥入 環境 工作階段 遠端控制 終端機服務設定檔 COM+

一般 位址 帳戶 設定檔 電話 組織 隸屬於

職稱(J):

部門(D):

公司(C):

主管

姓名(N):

變更(H)... 內容(P) 清除(L)

屬下(E):

確定 取消 套用(A) 說明

圖 18-2. 「<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。

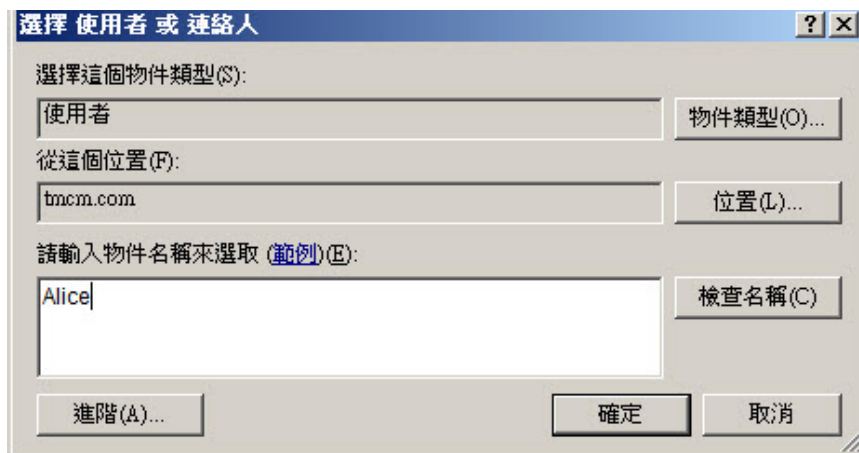


圖 18-3. 「選取使用者或聯絡人」畫面

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

Control Manager 提供下列 Data Loss Prevention (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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 將存取限制為與直接受管理的使用者相關的 DLP 記錄檔
	DLP 事件檢閱者	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 按一下下列任何「DLP 事件調查」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。 <ul style="list-style-type: none"> 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) <hr/> <p> 注意</p> <ul style="list-style-type: none"> 依預設，每個「DLP 事件調查」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「DLP 事件調查」Widget 的「範圍」不會影響任何其他 Widget 的範圍。 <hr/> <ul style="list-style-type: none"> 在所有其他畫面上： <ul style="list-style-type: none"> 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 合規官	
	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	存取「DLP 事件調查」標籤和下列 Widget： <ul style="list-style-type: none"> • 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 DLP 事件調查標籤 第 3-29 頁 。
	DLP 合規官	
	DLP 事件檢閱者	
預約事件摘要通知	管理員和 DLP 合規官	接收下列內容： <ul style="list-style-type: none"> • 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 • Control Manager Web 主控台的連結
	DLP 合規官	
	DLP 事件檢閱者	
事件詳細資料已更新通知	管理員和 DLP 合規官	收到事件狀態或備註發生變更的通知 <hr/> <div style="display: flex; align-items: center;">  注意 </div> 「DLP 事件檢閱者」角色不會收到此通知。
	DLP 合規官	

建立 DLP 稽核記錄檔

管理員可以使用臨機操作查詢來產生及匯出 DLP 稽核記錄檔。請按照[使用記錄查詢 第 14-2 頁](#)中所述程序來執行記錄查詢，並設定下列項目：

- 資料範圍：選取「Control Manager」
- 資料檢視：選取「使用者存取資訊」
- 查詢條件：將下列活動新增至「自訂」條件：
 - 刪除 DLP 記錄檔
 - 刪除存取記錄檔
 - 下載 DLP 事件檔案

- 啟動存取記錄檔維護
- 啟動 DLP 記錄檔維護
- 關閉存取記錄檔維護
- 關閉 DLP 記錄檔維護
- 更新 DLP 事件
- 變更 DLP 記錄檔維護設定
- 更新存取記錄檔維護設定

DLP 事件檢閱程序

在 Control Manager 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	Control Manager 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： <ul style="list-style-type: none"> • 按一下訊息中提供的連結登入 Control Manager Web 主控台 • 開啟附件（如果有的話） 	瞭解事件資訊清單 第 18-8 頁
更新事件狀態並提供備註	檢閱事件詳細資料 第 18-10 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
收到	<p>Control Manager 收到事件資料的日期和時間</p> <hr/> <p> 注意 收到來自受管理產品的 DLP 記錄檔後，Control Manager 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。</p>
嚴重性	<p>事件的嚴重性層級</p> <hr/> <p> 注意 Control Manager 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，Control Manager 並不會更新嚴重性層級。</p>
策略	<p>觸發事件的 Control Manager 策略名稱</p> <hr/> <p> 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」。</p>
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




項目	說明
狀態	事件的目前狀態 <ul style="list-style-type: none"> • 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： <ul style="list-style-type: none"> • 新增 • 調查中 • 已向上呈報 • 已關閉

項目	說明
嚴重性	<p>事件的嚴重性層級</p> <hr/> <p> 注意 Control Manager 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，Control Manager 並不會更新嚴重性層級。</p>
策略	<p>觸發事件的 Control Manager 策略名稱</p> <hr/> <p> 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」。</p>
規則	觸發事件所依據的規則名稱
收到	<p>Control Manager 收到事件資料的日期和時間</p> <hr/> <p> 注意 收到來自受管理產品的 DLP 記錄檔後，Control Manager 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。</p>
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
寄件者	來源電子郵件信箱
收件者	目標電子郵件信箱
端點	來源主機名稱
IP	來源 IP 位址
範本	觸發事件的範本名稱
相符內容	觸發事件的數位資產

項目	說明
檔案	觸發事件的檔案名稱或檔案連結 <hr/>  注意 在受管理產品中隔離檔案。 <hr/>
SHA-1	檔案的雜湊資訊
主旨	電子郵件訊息的主旨
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
使用者理由	當管理員允許使用者傳輸機密資料時，用戶端使用者提供的理由
備註	使用者定義的事件相關注意事項

部分 V

工具和支援



第 19 章

管理資料庫

此區段顯示管理員管理 Control Manager 網路所需的材料。

包含下列主題：

- [瞭解 Control Manager 資料庫 第 19-2 頁](#)
- [使用 SQL Server Management Studio 備份 db_ControlManager 第 19-8 頁](#)
- [使用 SQL 指令壓縮 db_ControlManager_Log.ldf 第 19-10 頁](#)
- [使用 SQL Server Management Studio 壓縮 db_ControlManager_log.ldf 第 19-11 頁](#)

瞭解 Control Manager 資料庫

Control Manager 使用 Microsoft SQL Server 資料庫 (db_ControlManager.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。

Control Manager 伺服器使用系統 DSN ODBC 連線建立資料庫連線。Control Manager 安裝會產生此連線，以及用於存取 db_ControlManager.mdf 的 ID 和密碼。預設 ID 為 sa。Control Manager 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_ControlManager 的所有 SQL 帳號設定下列最低權限：

- dbcreator (針對伺服器角色)
- db_owner (針對 db_ControlManager 角色)

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檔類型到 Control Manager。趨勢科技會測量下列常見記錄檔類型的資料庫大小：

- 病毒記錄檔
- 間諜程式記錄檔
- Web 安全記錄檔
- 內容安全記錄檔

請參閱下表，以取得資料庫的大小：

表 19-1. 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	156
	500,000	667
	1,000,000	1,191

記錄類型	記錄檔計數	資料庫大小 (MB)
間諜程式	100,000	156
	500,000	770
	1,000,000	1,570
內容安全	100,000	121
	500,000	543
	1,000,000	1,263
Web 安全	100,000	99
	500,000	562
	1,000,000	1,106

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：

- OfficeScan 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 Control Manager。
- Control Manager 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 Control Manager 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_ControlManager 資料表

如果要存取 Control Manager 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。

Control Manager 資料庫由下列資料表所組成：

表 19-2. 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）的網路封包掃描記錄檔
tb_LogDataLossPrevention	儲存從產品傳送/接收自產品的 Data Loss Prevention 相關記錄檔
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

目錄管理資料表	說明
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盒虛擬平台偵測記錄檔

表 19-3. 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 19-4. 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

伺服器指令控制器資料表	說明
tb_ManualDownload	儲存手動下載資訊
tb_ScheduleDownload	儲存預約下載資訊

表 19-5. 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 19-6. 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
<ul style="list-style-type: none"> • 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

記錄檔資料表	說明
<ul style="list-style-type: none"> • tb_InstanceForVirusOutbreak • tb_InstanceForSpecialVirus • tb_InstanceForVirusOutbreak 	儲存警訊通知中使用的記錄檔執行個體

表 19-7. 通知資料表

通知資料表	說明
<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • tb_VirusOutbreakAccumulate • tb_SpecialVirusAccumulate 	儲存病毒計數器資訊

通知資料表	說明
<ul style="list-style-type: none"> • tb_UGNtfRelation • tb_NtfUserGROUP • tb_GroupAndUserRelation 	儲存使用者和群組通知設定

表 19-8. 報告資料表

報告資料表	說明
<ul style="list-style-type: none"> • 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 19-9. 病毒碼和引擎部署資料表

病毒碼和引擎部署資料表	說明
<ul style="list-style-type: none"> • 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_ControlManager

使用 SQL Server 時，請使用 SQL Server Management Studio 來備份 Control Manager 資料庫。

**注意**

Trend Micro 建議您定期備份 Control Manager 資料庫。在修改 Control Manager 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。

程序

1. 在 Control Manager 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_ControlManager」，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_ControlManager

使用 SQL Server Management Studio 還原備份 Control Manager 資料庫。

程序

1. 停止 Control Manager。
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「<Control Manager 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_ControlManager > 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 '{Control Manager 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「<Control Manager service>」，然後按一下「重新啟動」。
 12. 啟動 Control Manager。
-

使用 SQL 指令壓縮 db_ControlManager_Log.ldf

程序

1. 請使用 SQL Server Management Studio 備份 Control Manager 資料庫。
2. 從可用的資料庫中，選取 db_ControlManager 資料庫。
3. 執行下列 SQL 程式檔：

```
DBCC shrinkfile('db_ControlManager_log', 10)
```


4. 確認 db_ControlManager_Log.LDF 的大小小於 10 MB。

如果 db_ControlManager_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, 'Recovery') as RecoveryMode FROM master.dbo.sysdatabases where name='db_ControlManager'
```

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_ControlManager
SET RECOVERY SIMPLE;
GO
-- Shrink the truncated log file to 10 MB.
DBCC SHRINKFILE (db_ControlManager_Log, 10);
GO
-- Reset the database recovery model.
ALTER DATABASE db_ControlManager
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_ControlManager_log.ldf

Control Manager 資料庫的交易記錄檔是 ...\\data \\db_ControlManager_log.LDF。SQL Server 在其正常作業過程中會產生交易記錄。

db_ControlManager_log.LDF 包含使用 db_ControlManager.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_ControlManager_log.ldf 檔案大小

程序

1. 請使用 SQL Server Management Studio 備份 Control Manager 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 Windows 驗證。
 5. 以滑鼠右鍵按一下 db_ControlManager，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」。
 9. 檢查 db_ControlManager_log.ldf 檔案大小。大小應該是 10 MB。
-

第 20 章

Control Manager 工具

本節討論如何使用多個 Control Manager 組態設定工具。

包含下列主題：

- [關於 Control Manager 工具 第 20-2 頁](#)
- [使用用戶端移轉工具 \(AgentMigrateTool.exe\) 第 20-2 頁](#)
- [使用資料庫組態設定工具 \(DBConfig.exe\) 第 20-2 頁](#)

關於 Control Manager 工具

Control Manager 提供多種工具，可協助您處理特定的組態設定工作。Control Manager 的大多數工具存放在下列位置：

<Control Manager 安裝目錄>\WebUI\download\tools\

使用用戶端移轉工具 (AgentMigrateTool.exe)

Control Manager 7.0 所提供的用戶端移轉工具可以用來移轉受 Control Manager 6.0 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。

程序

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：<Control Manager 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為 Control Manager 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。

程序

1. 在 Control Manager 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 <Control Manager 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 21 章

可疑物件中樞和節點 Control Manager 架構

本節提供管理員在跨多部 Control Manager 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 Control Manager 架構 第 21-2 頁](#)
- [設定可疑物件中樞和節點 第 21-3 頁](#)
- [從中樞 Control Manager 取消註冊可疑物件節點 第 21-4 頁](#)
- [組態設定注意事項 第 21-5 頁](#)

可疑物件中樞和節點 Control Manager 架構

Trend Micro Control Manager™ 可疑物件中樞和節點架構可讓您跨多部 Control Manager 伺服器同步處理可疑物件清單。中樞 Control Manager 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 Control Manager 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 Control Manager 伺服器。

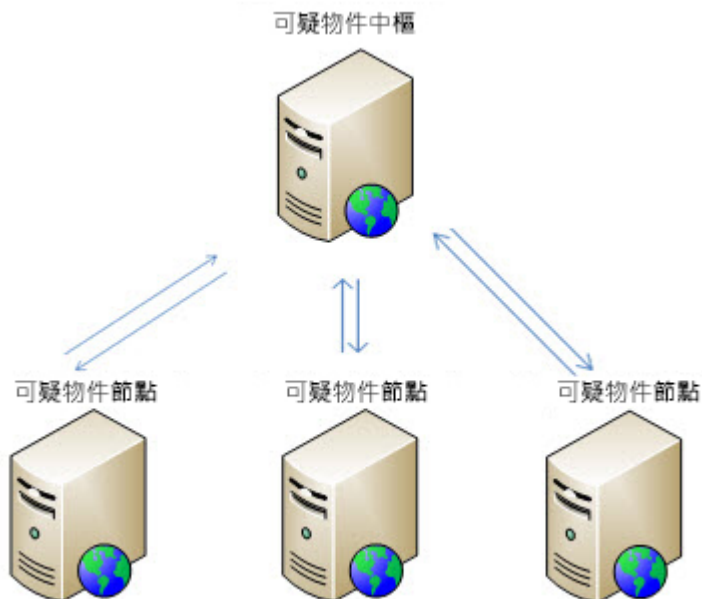
管理員必須先設定可疑物件中樞 Control Manager 伺服器，然後根據環境指派其他 Control Manager 伺服器做為可疑物件節點伺服器。Trend Micro Deep Discovery 產品可以註冊到可疑物件中樞或任何可疑物件節點 Control Manager 伺服器。這種架構會要求您透過可疑物件中樞 Control Manager 伺服器主控台設定所有可疑物件處理行動。



重要

您必須透過可疑物件中樞 Control Manager 對可疑物件清單執行所有作業，以確保所有節點 Control Manager 伺服器保持正確同步處理狀態。

透過可疑物件節點 Control Manager 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

程序

1. 登入可疑物件中樞 Control Manager 伺服器主控台。
2. 移至「管理 > 可疑物件 > 預設設定」。
會出現「預設設定」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 Control Manager 伺服器主控台。
 5. 移至「管理 > 可疑物件 > 預設設定」。
會出現「預設設定」畫面。
 6. 在「中樞 Control Manager」標籤中，提供從可疑物件中樞 Control Manager 複製的下列設定：
 - 服務 URL
 - API 金鑰
 7. 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 Control Manager 註冊。
 8. 對每一部可疑物件節點 Control Manager 伺服器重複上述程序。
 9. 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」。
-

從中樞 Control Manager 取消註冊可疑物件節點



注意

在取消註冊節點 Control Manager 伺服器後，所有先前同步處理的物件會留存在節點 Control Manager 伺服器可疑物件清單中。

程序

1. 登入可疑物件節點 Control Manager 伺服器主控台。

2. 移至「管理 > 可疑物件 > 預設設定」。
3. 在「中樞 Control Manager 設定」區段中，按一下「取消註冊」。

會出現確認對話方塊，並顯示訊息指出從中樞 Control Manager 伺服器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 Control Manager 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 Control Manager 伺服器後，請注意下列組態設定資訊。



注意

在取消註冊節點 Control Manager 伺服器後，所有先前同步處理的物件會留存在節點 Control Manager 伺服器可疑物件清單中。

組態設定	中樞 CONTROL MANAGER	節點 CONTROL MANAGER
同步處理間隔	無	5 分鐘（預設值）

組態設定	中樞 CONTROL MANAGER	節點 CONTROL MANAGER
可疑物件清單同步處理	從中樞 Control Manager 到節點： <ul style="list-style-type: none"> • 沙盒虛擬平台清單 • 使用者定義的清單 	從節點 Control Manager 到中樞： <ul style="list-style-type: none"> • 沙盒虛擬平台清單
<div style="border: 1px solid black; padding: 10px;"> <div style="display: flex; align-items: flex-start;">  <div style="margin-left: 5px;"> <p>注意</p> <ul style="list-style-type: none"> • 中樞 Control Manager 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 Control Manager 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「沙盒虛擬平台」清單。 <ul style="list-style-type: none"> • 如果您在下次同步處理前，將某個物件同時新增到中樞 Control Manager 上的「使用者定義」清單和「沙盒虛擬平台」清單，則中樞 Control Manager 伺服器會將這兩種清單部署到節點 Control Manager 伺服器。 • 如果節點 Control Manager 沙盒虛擬平台清單中的某個物件也存在於中樞 Control Manager 使用者定義清單中，則在下次同步處理期間，節點 Control Manager 沙盒虛擬平台清單的可疑物件風險等級會變更為「高」。 • 如果要自動同步處理移轉的 Control Manager 6.0 安裝的「例外」清單，需要在移轉前於 Control Manager 6.0 伺服器上啟動可疑物件中樞和節點 Control Manager 架構。 • Control Manager 7.0 安裝會保留移轉的 Control Manager 6.0 安裝的可疑物件中樞和節點架構。 • 如果要在移轉前於 Control Manager 6.0 伺服器上啟動可疑物件中樞和節點 Control Manager 架構，請在 SystemConfiguration.xml 檔案中找到 m_iTmcmSoDist_ForceSyncWhitelist 標籤，並將值變更為 1。 </div> </div> </div>		

組態設定	中樞 CONTROL MANAGER	節點 CONTROL MANAGER
設定可疑物件設定	建議使用 透過中樞 Control Manager 設定可疑物件，可確保已註冊的節點 Control Manager 伺服器彼此一致。	不建議使用  重要 為了確保節點 Control Manager 伺服器上的所有可疑物件清單維持同步狀態，請勿透過節點 Control Manager 伺服器主控台對可疑物件清單執行任何處理行動（例如，「新增」物件或使物件「到期」）。

第 22 章

可疑物件清單匯出程式和匯入程式使用者手冊

本節討論如何使用 Control Manager 可疑物件清單匯出程式 (SuspiciousObjectExporter.exe) 和匯入程式 (ImportSOFromCSV.exe) 工具。

包含下列主題：

- [可疑物件清單匯出程式和匯入程式使用者手冊 第 22-2 頁](#)
- [使用可疑物件清單匯出程式 \(SuspiciousObjectExporter.exe\) 第 22-2 頁](#)
- [使用 Control Manager 匯出沙盒虛擬平台例外清單 第 22-10 頁](#)
- [使用 Control Manager 匯出使用者定義的清單 第 22-11 頁](#)
- [使用可疑物件清單匯入程式 \(ImportSOFromCSV.exe\) 第 22-11 頁](#)
- [使用 Control Manager 匯入沙盒虛擬平台例外清單 第 22-13 頁](#)
- [使用 Control Manager 匯入使用者定義的清單 第 22-14 頁](#)

可疑物件清單匯出程式和匯入程式使用者手冊

Trend Micro Control Manager™ 可疑物件清單匯出程式和匯入程式工具可讓您匯出及匯入 Control Manager 可疑物件清單，而不需要登入 Control Manager 管理主控台。

- 可疑物件清單匯出程式：從 Control Manager 伺服器匯出多種檔案格式的可疑物件清單。
- 可疑物件清單匯入程式：將格式正確的逗號分隔值 (CSV) 可疑物件資料匯入 Control Manager。

使用匯出程式和匯入程式工具，可以在多部 Control Manager 伺服器中和支援的協力廠商應用程式中，同步處理可疑物件資料，藉此增強防禦未知和新興安全威脅的能力。

使用可疑物件清單匯出程式 (SuspiciousObjectExporter.exe)

使用「可疑物件清單匯出程式」工具 (SuspiciousObjectExporter.exe)，可匯出多種檔案格式的 Control Manager 可疑物件清單。依預設，「可疑物件清單匯出程式」工具會匯出 XML 格式的可疑物件資料。

如需如何變更輸出檔案格式的詳細資訊，請參閱[修改組態設定檔 第 22-5 頁](#)。



重要

「可疑物件清單匯出程式工具」需要 Control Manager 7.0（或更新版本）。

如果要下載最新的安裝套件，請參閱 http://downloadcenter.trendmicro.com/index.php?regs=tw&clk=result_page&clkval=drop_list&prodid=7。

程序

1. 在 Control Manager 伺服器上開啟指令提示字元。
2. 使用下列指令找出包含 SuspiciousObjectExporter.exe 檔案的目錄：

```
cd <Control Manager 安裝目錄>\SOTools
```


3. 使用下列指令執行 SuspiciousObjectExporter.exe：




```
SuspiciousObjectExporter.exe [/s <Start ID> /e <End ID>]
[/f <y | n>] [/d]
```




注意

執行 SuspiciousObjectExporter.exe 且未使用任何參數時，會顯示使用情形詳細資料，並提示您提供 <Start ID> 和 <End ID> 的值。

參數	說明	範例
/s <Start ID>	<p>表示要匯出的第一個物件的 ID</p> <hr/> <p> 注意</p> <ul style="list-style-type: none"> • 會要求您指定 /e <End ID> 值 • 指定值 0 表示清單的開頭 	<ul style="list-style-type: none"> • SuspiciousObjectExporter.exe /s 0 /e 0 在匯出過程中，會匯出所有可疑物件並鎖定指令行介面 • SuspiciousObjectExporter.exe /s 3 /e 8 在匯出過程中，會匯出從 ID 3 開始到 ID 8 的可疑物件並鎖定指令行介面 • SuspiciousObjectExporter.exe /s 0 /e 4 在匯出過程中，會匯出從清單開頭開始到 ID 4 的可疑物件並鎖定指令行介面

參數	說明	範例
<code>/e <End ID></code>	<p>表示要匯出的最後一個物件的 ID</p> <hr/> <p> 注意</p> <ul style="list-style-type: none"> 會要求您指定 <code>/s <Start ID></code> 值 指定值 <code>0</code> 表示清單的結尾 	<ul style="list-style-type: none"> <code>SuspiciousObjectExporter.exe /s 0 /e 0</code> 在匯出過程中，會匯出所有可疑物件並鎖定指令行介面 <code>SuspiciousObjectExporter.exe /s 3 /e 8</code> 在匯出過程中，會匯出從 ID 3 開始到 ID 8 的可疑物件並鎖定指令行介面 <code>SuspiciousObjectExporter.exe /s 4 /e 0</code> 在匯出過程中，會匯出從 ID 4 開始到清單結尾的可疑物件並鎖定指令行介面
<code>/f <y n></code>	<p>指定在匯出過程中是否要鎖定指令行介面</p> <hr/> <p> 注意</p> <p>選用參數；如果未指定，預設值為 "yes"</p> <hr/> <p> 重要</p> <p>您必須在使用 <code>SuspiciousObjectExporter.exe</code> 工具、PowerShell 程序檔或 Windows 工作排程器中的批次程式檔預約自動匯出時，於「新增引數(可省略)」欄位中指定下列參數。</p> <p><code>/f n</code></p>	<ul style="list-style-type: none"> <code>SuspiciousObjectExporter.exe /f y</code> 在匯出過程中，會匯出所有可疑物件並鎖定指令行介面 <code>SuspiciousObjectExporter.exe /s 0 /e 0 /f y</code> 在匯出過程中，會匯出所有可疑物件並鎖定指令行介面 <code>SuspiciousObjectExporter.exe /f n</code> 在匯出過程中，會匯出所有可疑物件並解除鎖定指令行介面

參數	說明	範例
/d	用於啟動偵錯模式  注意 選用參數，通常由支援人員用於識別錯誤	SuspiciousObjectExporter.exe /d 匯出所有可疑物件與其他偵錯記錄檔

4. 如果要檢視匯出的可疑物件清單，請移至 <目前的目錄>\SOTools\ 目錄，然後開啟 SuspiciousObjectList.xml 檔案。

**注意**

如果您遵循此程序，則 <目前的目錄> 指的是 <Control Manager 安裝目錄>。

5. 如果要檢視所有匯出記錄檔，請移至 <目前的目錄>\SOTools\ 目錄，然後開啟 ExportRecord.txt 檔案。

**注意**

如果您遵循此程序，則 <目前的目錄> 指的是 <Control Manager 安裝目錄>。

修改組態設定檔

如果要變更「可疑物件清單匯入程式」的預設組態設定，請移至 <Control Manager 安裝目錄>\SOTools 目錄並修改 SuspiciousObjectExporter.exe.config 檔案。

**秘訣**

Trend Micro 建議您先建立組態設定檔的備份，再進行任何修改。

機碼	說明	範例
outputRootFolderPath 位置： <appSettings>	表示 SuspiciousObjectExporter.exe 工具的工作目錄	<ul style="list-style-type: none"> <code><add key="outputRootFolderPath" value="."/></code> 此工具使用 SuspiciousObjectExporter.exe 程式所在的目錄來處理清單 <code><add key="outputRootFolderPath" value="C:\Program Files (x86)\Trend Micro\Control Manager"/></code> 此工具使用指定的目錄 (C:\Program Files (x86)\Trend Micro\Control Manager) 來處理清單
outputFolderName 位置： <appSettings>	表示匯出的可疑物件清單檔案的輸出目錄	<ul style="list-style-type: none"> <code><add key="outputFolderName" value="SOTools"/></code> 將檔案匯出到 <outputRootFolderPath>\SOTools 目錄 <code><add key="outputFolderName" value="SOList"/></code> 將檔案匯出到 <outputRootFolderPath>\SOList 目錄

機碼	說明	範例
styleSheetFile 位置： <appSettings>	表示工具套用到匯出的清單的樣式表	<ul style="list-style-type: none"> <li data-bbox="659 256 1185 354"> <p>• <add key="styleSheetFile" value=""/></p> <p>將 XML 格式的所有清單匯出為 outputFile 機碼所指定的 *.txt 或 *.xml 檔案</p> <li data-bbox="659 370 1185 521"> <p>• <add key="styleSheetFile" value="ExportCSV.xslt"/></p> <p>用於匯出「沙盒虛擬平台可疑物件」清單、「使用者定義的可疑物件」清單或含有限欄子集的「例外」清單（採用 CSV 格式）</p> <hr/> <p> 重要</p> <p>選取 ExportCSV.xslt 樣式表後，您可以不再設定此工具匯出的欄。此工具只會匯出樣式表中指定的欄。</p> <hr/> <li data-bbox="659 716 1185 808"> <p>• <add key="styleSheetFile" value="ExportSTIX.xslt"/></p> <p>用來匯出所有 STIX 格式的可疑物件清單</p> <li data-bbox="659 829 1185 922"> <p>• <add key="styleSheetFile" value="ExportCPL.xslt"/></p> <p>用來匯出所有 CPL 格式的可疑物件清單</p> <hr/> <p> 重要</p> <p>如果您指定樣式表，則必須將 defaultSampleTemplates 機碼設定為相同的值。</p> <hr/>

機碼	說明	範例
outputFile 位置： <appSettings>	表示匯出的可疑物件清單檔案的檔案名稱和副檔名 指定新的副檔名可變更輸出檔案格式	<ul style="list-style-type: none"> <code><add key="outputFile" value="SuspiciousObjectList.xml"/></code> 將可疑物件清單匯出為名為 SuspiciousObjectList.xml 的 *.xml 檔案 <code><add key="outputFile" value="SuspiciousObjectList.txt"/></code> 將可疑物件清單匯出為名為 SuspiciousObjectList.txt 的 *.txt 檔案
defaultSampleTemplates 位置： <appSettings>	表示工具套用到匯出的清單的樣式表來源檔案	<ul style="list-style-type: none"> <code><add key="defaultSampleTemplates" value="ExportCSV.xslt"/></code> 找出指定的樣式表檔案 <hr/> <p> 重要 指定的值必須符合指定給 styleSheetFile 或 defaultSampleTemplates 機碼的值。</p> <hr/> <p> 注意 預設值為 "ExportCPL.xslt ExportSTIX.xslt ExportCSV.xslt"。</p>
<suspiciousObjectColumns> 位置： <soDataColumnSettings>	表示所選清單上的資料欄 設定 isEnable="true" 可匯出指定的資料欄	<ul style="list-style-type: none"> <code><add id="1" name="SeqID" isEnable="true"/></add></code> 從所選清單匯出 "SeqID" 資料欄 <code><add id="1" name="MD5Key" isEnable="false"/></add></code> 從所選清單明確排除 "MD5Key" 資料欄 <hr/> <p> 重要 如果您指定了 ExportCSV.xslt 樣式表，此工具只會匯出樣式表中指定的欄。</p>

機碼	說明	範例
<p><suspiciousObjectTypeList></p> <p>位置： <soTypeSettings></p>	<p>表示要從所選清單匯出的物件類型</p> <p>設定 isEnabled="true" 可匯出指定的物件類型</p>	<ul style="list-style-type: none"> • <add value="0" description="IP" isEnabled="true"></add> 從所選清單匯出所有 IP 位址類型物件 • <add value="1" description="Domain" isEnabled="false"></add> 從匯出的清單明確排除所有「網域」物件
<p><suspiciousObjectSourceType></p> <p>位置： <soTypeSettings></p>	<p>表示可疑物件來源類型</p> <p>設定 isEnabled="true" 可匯出指定的物件類型</p>	<ul style="list-style-type: none"> • <add value="0" description="SourceType" isEnabled="true"/> 選取「沙盒虛擬平台可疑物件」清單 • <add value="1" description="SourceType" isEnabled="true"/> 選取「使用者定義的可疑物件」清單 • <add value="2" description="SourceType" isEnabled="true"/> 選取「沙盒虛擬平台例外」清單 <hr/> <p> 重要</p> <ul style="list-style-type: none"> • 如果您指定了 ExportCSV.xslt 樣式表，並選取「沙盒虛擬平台可疑物件」清單或「使用者定義的可疑物件」清單，則此工具會匯出下列欄：物件、類型、掃描預先過濾器、注意事項和中毒處理行動。 • 如果您指定了 ExportCSV.xslt 樣式表，並選取「沙盒虛擬平台例外」清單，此工具會匯出下列欄：物件、類型、掃描預先過濾器和注意事項。

使用 Control Manager 匯出沙盒虛擬平台例外清單



重要

Control Manager 僅支援以 CSV 格式匯出「沙盒虛擬平台可疑物件例外」清單。

程序

1. 移至「管理 > 可疑物件 > 沙盒虛擬平台物件」。
會出現「沙盒虛擬平台可疑物件」畫面。
 2. 按一下「例外」標籤。
 3. 按一下「全部匯出」。
會出現進度畫面。
 4. 匯出完成後，按一下「下載」。
確認方塊便會出現。
 5. 按一下「儲存」。
會出現「另存新檔」畫面。
 6. （選用）指定新的位置或檔案名稱。
 7. 按一下「儲存」。
-

使用 Control Manager 匯出使用者定義的清單



重要

Control Manager 僅支援以 CSV 格式匯出「使用者定義的可疑物件」清單。

程序

1. 移至「管理 > 可疑物件 > 使用者定義的物件」
會出現「使用者定義的可疑物件」畫面。
2. 按一下「全部匯出」。
會出現進度畫面。
3. 匯出完成後，按一下「下載」。
確認方塊便會出現。
4. 按一下「儲存」。
會出現「另存新檔」畫面。
5. （選用）指定新的位置或檔案名稱。
6. 按一下「儲存」。

使用可疑物件清單匯入程式 (ImportSOFromCSV.exe)

使用「可疑物件清單匯入程式」工具 (ImportSOFromCSV.exe) 可將格式正確的可疑物件資料 *.csv 檔案匯入 Control Manager。

**重要**

「可疑物件清單匯入程式工具」需要 Control Manager 7.0（或更新版本）。

如果要下載最新的 Control Manager 安裝套件，請參閱 http://downloadcenter.trendmicro.com/index.php?regs=tw&clk=result_page&clkval=drop_list&prodid=7。

程序

1. 在 Control Manager 伺服器上開啟指令提示字元。
2. 使用下列指令找出包含 ImportSOFromCSV.exe 檔案的目錄：

```
cd <Control Manager 安裝目錄>
```

3. 使用下列指令執行 ImportSOFromCSV.exe：

```
ImportSOFromCSV.exe "<完整路徑>" {UserDefinedSO |  
ExceptionSO}
```

說明：

- <完整路徑>：表示格式正確的 CSV 檔案的目錄和檔案名稱
- {UserDefinedSO}：表示包含「使用者定義的可疑物件」清單資料的檔案
- {ExceptionSO}：表示包含「沙盒虛擬平台例外」清單資料的檔案

例如：

- SuspiciousObjectImporter.exe "c:\Program Files (x86)\Trend Micro\Control Manager\importExceptionSample.csv" ExceptionSO

會將 c:\Program Files (x86)\Trend Micro\Control Manager 目錄中的 importExceptionSample.csv 檔案匯入 Control Manager 中的沙盒虛擬平台例外清單

使用 Control Manager 匯入沙盒虛擬平台例外清單



重要

Control Manager 僅支援匯入格式正確的沙盒虛擬平台例外清單資料 *.csv 檔案。

程序

1. 移至「管理 > 可疑物件 > 沙盒虛擬平台物件」
會出現「沙盒虛擬平台可疑物件」畫面。
2. 按一下「例外」標籤。
3. 請點選「匯入」。
會出現「匯入例外」畫面。
4. 按一下「瀏覽...」，然後選取包含例外清單資料的 *.csv 檔案。



秘訣

按一下「下載範例 CSV」連結，可取得一個格式正確且附有詳細指示的 *.csv 檔案範例。

5. 請點選「開啟」。
6. 請點選「匯入」。
會關閉「匯入例外」畫面，而匯入的例外會出現在「沙盒虛擬平台可疑物件例外」清單中。

使用 Control Manager 匯入使用者定義的清單



重要

Control Manager 僅支援匯入格式正確的使用者定義可疑物件資料 *.csv 檔案。

程序

1. 移至「管理 > 可疑物件 > 使用者定義的物件」
會出現「使用者定義的可疑物件」畫面。
2. 請點選「匯入」。
會出現「匯入使用者定義的清單」畫面。
3. 按一下「瀏覽...」，然後選取包含使用者定義的可疑物件資料的 *.csv 檔案。



秘訣

按一下「下載範例 CSV」連結，可取得一個格式正確且附有詳細指示的 *.csv 檔案範例。

4. 請點選「開啟」。
 5. 請點選「匯入」。
會關閉「匯入使用者定義的清單」畫面，而匯入的物件會出現在「使用者定義的可疑物件」清單中。
-

第 23 章

使用 LogForwarder 工具 (LogForwarder.exe)

本節討論如何使用 Control Manager LogForwarder 工具。

包含下列主題：

- [簡介 第 23-2 頁](#)
- [系統需求 第 23-3 頁](#)
- [限制 第 23-3 頁](#)
- [設定 LogForwarder 設定 第 23-4 頁](#)
- [開始與停止轉送記錄檔 第 23-6 頁](#)

簡介

LogForwarder 工具 (LogForwarder.exe) 是新一代的 DataExportTool，可採用下列格式將 Control Manager 資料庫中的多種產品記錄檔傳送到 Syslog 伺服器：

- 一般事件格式 (CEF)
- Control Manager 記錄格式



重要

- Trend Micro Control Manager 7.0 不再支援 DataExport 工具。
管理員必須使用新的 LogForwarder 工具 (LogForwarder.exe)。
- LogForwarder 工具僅支援 UDP 通訊協定。

LogForwarder 工具支援新的記錄類型，包括「網路內容檢測」記錄、「可疑檔案」記錄及「C&C 回呼」記錄。管理員也可以設定此工具，使其在 Control Manager 伺服器的背景程序中執行。

表 23-1. 支援的記錄類型格式

記錄類型	CEF 記錄格式支援	CONTROL MANAGER 記錄格 式支援
行為監控	是	是
C&C 回呼	是	否
Data Loss Prevention	是	是
裝置存取控制	是	是
引擎更新狀態	是	是
可疑檔案	是	否
網路內容檢測	是	否
病毒/惡意程式	是	否

記錄類型	CEF 記錄格式支援	CONTROL MANAGER 記錄格式支援
特徵碼更新狀態	是	是
內容安全	是	否
間諜程式/可能的資安威脅程式	是	否
Web 安全	是	否
Machine Learning	是	否

系統需求

LogForwarder 工具需要 Trend Micro Control Manager 7.0。



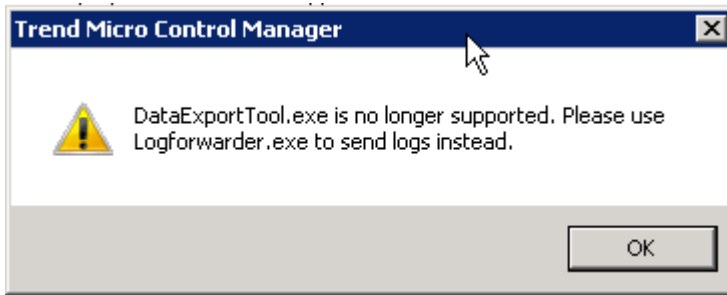
重要

LogForwarder 工具僅支援 UDP 通訊協定。

限制

Trend Micro Control Manager 7.0 不再支援 DataExportTool.exe 工具。

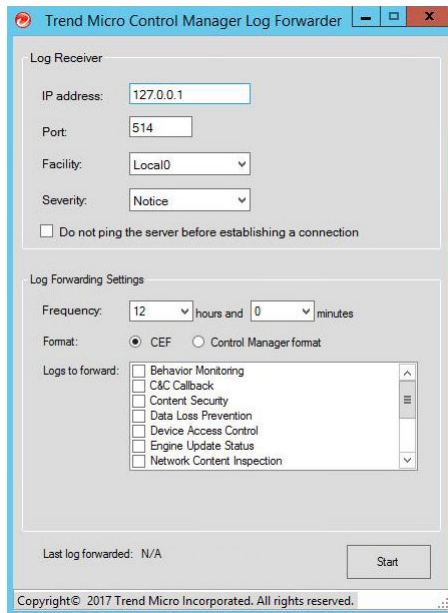
- Control Manager 7.0 的全新安裝不提供 DataExportTool.exe 工具。
- 從舊版移轉到 Control Manager 7.0 後，若嘗試執行 DataExportTool.exe 工具，會出現下列警告訊息：



設定 LogForwarder 設定

程序

1. 移至 Control Manager 安裝目錄。
依預設，安裝目錄是 C:\Program Files (x86)\Trend Micro\Control Manager。
2. 使用管理員權限（「以系統管理員身分執行」）執行 LogForwarder.exe 檔案，以開啟 LogForwarder 主控台。



3. 設定「記錄檔收件者」設定。

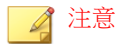
- IP 位址：Syslog 伺服器 IP 位址
- 通訊埠：Syslog 伺服器通訊埠號碼
- 設備：Syslog 訊息的設備代碼



注意

此設定僅適用於 Control Manager 格式的記錄檔。

- 嚴重性：Syslog 訊息的嚴重性層級



注意

此設定僅適用於 Control Manager 格式的記錄檔。

- (選用) 在建立連線前不用 Ping 伺服器：選取此選項可傳送 Syslog 訊息，而不需要先 Ping 目標伺服器

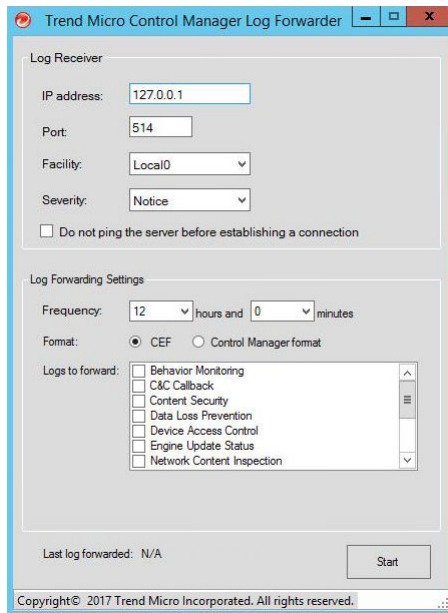
4. 設定「記錄檔轉寄設定」。
 - 頻率：此工具傳送記錄檔的頻率
 - 格式：選取使用 CEF 還是 Control Manager 記錄格式
 - 要轉寄的記錄：選取要轉寄給 Control Manager 的記錄類型
-

開始與停止轉送記錄檔

程序

1. 移至 Control Manager 安裝目錄。

依預設，安裝目錄是 C:\Program Files (x86)\Trend Micro\Control Manager。
2. 使用管理員權限（「以系統管理員身分執行」）執行 LogForwarder.exe 檔案，以開啟 LogForwarder 主控台。



3. 請執行下列其中一個處理行動：
- 如果要開始轉送記錄檔，請執行下列作業：
 - a. 請點選「開始」。

**注意**

如果 Control Manager 服務尚未啟動，便會出現訊息提示您稍待片刻，讓服務完成重新啟動。

- b. 確認您要開始轉送記錄檔。

**注意**

開始轉送記錄檔會重新啟動 Control Manager 服務，並關閉 LogForwarder 主控台。在 Control Manager 服務成功重新啟動後，該工具會持續在背景中執行，直到使用者重新開啟 LogForwarder 主控台並按一下「停止」。

- 如果要停止轉送記錄檔，請執行下列作業：
 - a. 請點選「停止」。



注意

如果 Control Manager 服務尚未啟動，便會出現訊息提示您稍待片刻，讓服務完成重新啟動。

- b. 確認您要停止轉送記錄檔。



注意

停止轉送記錄檔會重新啟動 Control Manager 服務。在 Control Manager 服務成功重新啟動後，該工具便不再於背景中執行。

第 24 章

可疑物件移轉工具使用手冊

本節提供管理員使用 Control Manager 可疑物件移轉工具所需的材料。

包含下列主題：

- [可疑物件移轉工具使用手冊 第 24-2 頁](#)
- [準備 Check Point 防火牆伺服器 第 24-2 頁](#)
- [準備驗證憑證組態設定檔 第 24-4 頁](#)
- [使用可疑物件移轉工具 第 24-8 頁](#)
- [使用可疑物件清單匯出程式 \(SuspiciousObjectExporter.exe\) 第 22-2 頁](#)
- [使用 Check Point Suspicious Activity Monitoring Client 工具 第 24-18 頁](#)

可疑物件移轉工具使用手冊

「趨勢科技可疑物件移轉工具」可讓您將可疑物件資料從 Control Manager 伺服器移轉到協力廠商應用程式，而不需要手動匯出、格式化及匯入個別的 Control Manager 可疑物件清單。

本使用手冊說明如何將「可疑物件移轉工具」與「趨勢科技可疑物件清單匯出程式」和 Check Point Suspicious Activity Monitoring (SAM) Client 工具搭配使用。

- 可疑物件移轉工具：以循環方式執行「可疑物件清單匯出程式」工具和 Check Point SAM Client。
- 可疑物件清單匯出程式：從 Control Manager 伺服器匯出多種檔案格式的可疑物件清單。
- Check Point SAM Client：將可疑物件資料正確格式化，然後匯入 Check Point 伺服器。

如果要手動將個別 Control Manager 可疑物件清單移轉到 Check Point 伺服器，您也可以使用「可疑物件清單匯出程式」和 Check Point SAM Client 工具，而不執行「可疑物件移轉工具」。

準備 Check Point 防火牆伺服器



注意

下列程序假設您使用 Check Point Firewall R77.20 搭配 Gaia OS 和 SmartDashboard R77.20。



重要

您必須先備妥 Check Point 防火牆伺服器，再準備驗證憑證組態設定檔。

程序

1. 設定 Check Point Suspicious Activity Monitoring (SAM) 伺服器通訊埠，以進行 Check Point Open Platform for Security (OPSEC) 通訊。

- a. 在專家模式下登入 Check Point 防火牆伺服器。
- b. 使用下列指令找出 `fwopsec.conf` 檔案，然後在 VI 編輯器中開啟此檔案：

```
vi /var/opt/CPsuite-R77/fw1/conf/fwopsec.conf
```

- c. 找出 `sam_server auth_port`，並將通訊埠號碼變更為 "18181"。

```
sam_server auth_port 18181
```

- d. 找出 `sam_server port`，並將通訊埠號碼變更為 "18180"。

```
sam_server port 18180
```

- e. 按 **ESC** 鍵使 VI 編輯器回到指令模式。

- f. 使用下列指令來儲存變更：

```
:wq
```

- g. 使用下列指令，將伺服器關機並重新啟動：

```
shutdown -r -h 0
```

2. 登入 Check Point SmartDashboard 主控台。
3. 允許 `FW1_sam` 和 `FW1_ica_pull` 服務通過 Check Point 防火牆。
 - a. 在「Firewall」標籤上，按一下「Policy」。
 - b. 按一下「Add Rule at the Top」。
 - c. 在最近建立的規則的「Service」欄中，按一下 (+) 圖示，然後從下拉式清單中選取「FW1_sam」。
 - d. 以滑鼠右鍵按一下最近建立的規則的「Action」欄，然後將內容設定為「Accept」。
 - e. 按一下「Add Rule at the Top」。
 - f. 在最近建立的規則的「Service」欄中，按一下 (+) 圖示，然後從下拉式清單中選取「FW1_ica_pull」。
 - g. 以滑鼠右鍵按一下最近建立的規則的「Action」欄，然後將內容設定為「Accept」。

- h. 按一下「Install Policy」。
4. 建立 OPSEC 應用程式和單次密碼。
 - a. 移至「Manage > Servers and OPSEC Applications」。
 - b. 按一下「New」並從下拉式功能表中選取「OPSEC Application」。
 - c. 指定下列項目：
 - Name：輸入 OPSEC 應用程式的名稱
 - Host：從下拉式清單中選取 Check Point 防火牆伺服器
 - d. 在「Client Entities」區段中選取「SAM」。
 - e. 按一下「Communication」。
 - f. 建立並確認單次密碼。
 - g. 按一下「Initialize」。
會出現確認對話方塊。
 - h. 請點選「關閉」。
 - i. 請點選「確定」。
-

準備驗證憑證組態設定檔



注意

- 下列程序假設您使用 Control Manager 7.0 伺服器來準備驗證憑證組態設定檔。
- 「可疑物件移轉工具」需要 Control Manager 7.0（或更新版本）。

如果要下載最新的 Control Manager 安裝套件，請參閱 http://downloadcenter.trendmicro.com/index.php?regs=tw&clk=result_page&clkval=drop_list&prodid=7。

**重要**

您必須先備妥 Check Point 防火牆伺服器，再準備驗證憑證組態設定檔。

如需詳細資訊，請參閱[準備 Check Point 防火牆伺服器 第 24-2 頁](#)。

程序

1. 在 Control Manager 伺服器上開啟指令提示字元。
2. 請備妥來自 Check Point 防火牆伺服器安全內部通訊 (SIC) 憑證。
 - a. 執行下列指令：

```
opsec_pull_cert -h <host> -n <object> -p <password> -o  
<path>
```

說明：

- -h <host>：表示 Check Point 防火牆伺服器的 IP 位址
- -n <object>：表示您在 Check Point SmartDashboard 主控台中建立的 OPSEC 應用程式名稱

如需詳細資訊，請參閱[準備 Check Point 防火牆伺服器 第 24-2 頁](#)。

- -p <password>：表示指定的 OPSEC 應用程式的單次密碼
- -o <path>：表示輸出 opsec.p12 憑證檔案的完整路徑

Opsec_pull_cert 指令會傳回 **full entity sic name**，格式如下：

```
CN=*,O=*
```

- b. 複製 opsec_pull_cert 指令所傳回的 **full entity sic name**。
 - c. 將 opsec.p12 檔案移至 <Control Manager 安裝目錄>\SOTools 目錄中。
3. 移至 <Control Manager 安裝目錄>\SOTools 目錄，並找出 sam.conf 檔案。

4. 使用文字編輯器開啟 `sam.conf` 檔案，然後參照下表修改所需的機碼。

機碼	說明	範例
<code>sam_server auth_type</code>	表示驗證方法	<code>sam_server auth_type sslca</code>
<code>sam_server ip</code>	表示 Check Point 防火牆伺服器的 IP 位址	<code>sam_server ip 192.168.127.130</code>
<code>sam_server auth_port</code>	表示 Check Point 防火牆伺服器上的 OPSEC 通訊埠	<code>sam_server auth_port 18181</code>
 重要 您必須提供 <code>fwosec.conf</code> 檔案中設定的相同 <code>sam_server auth_port</code> 號碼。		
<code>sam_server opsec_entity_sic_name</code>	表示 Check Point 防火牆伺服器 SIC 名稱	<code>sam_server opsec_entity_sic_name "cn=cp_mgmt,o=gw-1e9412..7ny9dn"</code>
<code>opsec_sic_name</code>	表示 <code>opsec_pull_cert</code> 指令所傳回的 SIC 名稱	<code>opsec_sic_name "CN=CMtest,O=gw-1e9412..7ny9dn"</code>
 重要 您必須提供 <code>opsec_pull_cert</code> 指令所傳回的確切 full entity sic name 。		
<code>opsec_sslca_file</code>	表示驗證憑證檔案的檔案名稱	<code>opsec_sslca_file opsec.p12</code>
<code>opsec_sic_policy_file</code>	表示 SIC 策略檔案的檔案名稱	<code>opsec_sic_policy_file sic_policy.ini</code>

5. 移至 <Control Manager 安裝目錄>\SOTools 目錄，並找出 `Customized.config` 檔案。
6. 使用文字編輯器開啟 `Customized.config` 檔案，然後參照下表修改所需的機碼。

機碼	說明	範例
寄件者 位置： <SOMigration Tool>	將值變更為 "CKP_SAM_Client.exe"	<add key="Sender" value="CKP_SAM_Client.exe" />
引數 位置： <SOMigration Tool>	將值變更為 "-t <timeout> -g <fw-ip> -c <conf_path> -A notify any <IP_address>" 說明： <ul style="list-style-type: none"> -t <timeout>：表示 Check Point 伺服器在可疑 物件到期之前等待的時間量 (以秒為單位) -c <conf_path>：表示 sam.conf 檔案的相對路徑 -g <fw-ip>：表示 Check Point 防火牆伺服器的 IPv4 位址 -A notify any <IP_address>：要求 Check Point 防火牆伺服器 通知有效的 IPv4 位址 	<add key="Arguments" value="-t 600 -g 192.168.127.130 -c sam.conf -A notify any 10.10.10.10" />
 注意 如需使用 Check Point sam_client_action 引數的詳細資訊，請參閱 Check Point 防火牆伺服器文件。		
outputFolderName 位置： <OutputSettings>	將值變更為 "Check_Point"	<add key="outputFolderName" value="Check_Point" />

機碼	說明	範例
outputFile 位置： <OutputSettings>	將值變更為 "SuspiciousObjectList.xml"	<add key="outputFile" value="SuspiciousObjectList.xml" />
description="IP" 位置： <suspiciousObjectTypeList>	設定 isEnabled="true"	<add value="0" description="IP" isEnabled="true"
description="SourceType" 位置： <suspiciousObjectSourceType>	將值變更為 "0"	<add value="0" description="SourceType" isEnabled="true"
name="Entity" 位置： <suspiciousObjectColumns>	設定 isEnabled="true"	<add id="3" name="Entity" isEnabled="true"

使用可疑物件移轉工具

使用「可疑物件移轉工具」可以匯出所有的 Control Manager 可疑物件清單，並將格式正確的可疑物件資料匯入 Check Point 伺服器。

**注意**

如果要手動將個別 Control Manager 可疑物件清單移轉到 Check Point 伺服器，您可以使用「可疑物件清單匯出程式」和 Check Point SAM Client 工具，而不執行「可疑物件移轉工具」。

如需詳細資訊，請參閱[使用 Check Point Suspicious Activity Monitoring Client 工具](#) 第 24-18 頁。

**重要**

使用「可疑物件移轉工具」之前，您必須：

- 準備 Check Point 防火牆伺服器
如需詳細資訊，請參閱[準備 Check Point 防火牆伺服器](#) 第 24-2 頁。
- 準備驗證組態設定檔
如需詳細資訊，請參閱[準備驗證憑證組態設定檔](#) 第 24-4 頁。

程序

1. 登入 Control Manager 伺服器。
2. 開啟命令提示字元。
3. 使用下列指令找出包含 SOMigrationTool.exe 檔案的目錄：

```
cd <Control Manager 安裝目錄>\SOTools
```
4. 使用下列指令執行 SOMigrationTool.exe：

```
SOMigrationTool Check_Point
```

指令的總執行時間即會顯示，這表示可疑物件資料移轉成功。
5. 如果要檢視 Check Point 防火牆伺服器上匯入的可疑物件資料，請執行下列作業：
 - a. 登入 Check Point SmartView Monitor 主控台。
 - b. 移至「Tools > Suspicious Activity Rules」。

會出現「Enforced Suspicious Activity Rules」畫面，並顯示匯入的可疑物件資料。

使用可疑物件清單匯出程式 (SuspiciousObjectExporter.exe)

使用「可疑物件清單匯出程式」工具 (SuspiciousObjectExporter.exe)，可匯出多種檔案格式的 Control Manager 可疑物件清單。依預設，「可疑物件清單匯出程式」工具會匯出 XML 格式的可疑物件資料。

如需如何變更輸出檔案格式的詳細資訊，請參閱[修改組態設定檔 第 22-5 頁](#)。



重要

「可疑物件清單匯出程式工具」需要 Control Manager 7.0（或更新版本）。

如果要下載最新的安裝套件，請參閱 http://downloadcenter.trendmicro.com/index.php?regs=tw&clk=result_page&clkval=drop_list&prodid=7。

程序

1. 在 Control Manager 伺服器上開啟指令提示字元。
2. 使用下列指令找出包含 SuspiciousObjectExporter.exe 檔案的目錄：

```
cd <Control Manager 安裝目錄>\SOTools
```



3. 使用下列指令執行 SuspiciousObjectExporter.exe：




```
SuspiciousObjectExporter.exe [/s <Start ID> /e <End ID>]  
[/f <y | n>] [/d]
```



注意

執行 SuspiciousObjectExporter.exe 且未使用任何參數時，會顯示使用情形詳細資料，並提示您提供 <Start ID> 和 <End ID> 的值。

參數	說明	範例
<code>/s <Start ID></code>	<p>表示要匯出的第一個物件的 ID</p> <hr/> <p> 注意</p> <ul style="list-style-type: none"> 會要求您指定 <code>/e <End ID></code> 值 指定值 <code>0</code> 表示清單的開頭 	<ul style="list-style-type: none"> <code>SuspiciousObjectExporter.exe /s 0 /e 0</code> 在匯出過程中，會匯出所有可疑物件並鎖定指令行介面 <code>SuspiciousObjectExporter.exe /s 3 /e 8</code> 在匯出過程中，會匯出從 ID 3 開始到 ID 8 的可疑物件並鎖定指令行介面 <code>SuspiciousObjectExporter.exe /s 0 /e 4</code> 在匯出過程中，會匯出從清單開頭開始到 ID 4 的可疑物件並鎖定指令行介面
<code>/e <End ID></code>	<p>表示要匯出的最後一個物件的 ID</p> <hr/> <p> 注意</p> <ul style="list-style-type: none"> 會要求您指定 <code>/s <Start ID></code> 值 指定值 <code>0</code> 表示清單的結尾 	<ul style="list-style-type: none"> <code>SuspiciousObjectExporter.exe /s 0 /e 0</code> 在匯出過程中，會匯出所有可疑物件並鎖定指令行介面 <code>SuspiciousObjectExporter.exe /s 3 /e 8</code> 在匯出過程中，會匯出從 ID 3 開始到 ID 8 的可疑物件並鎖定指令行介面 <code>SuspiciousObjectExporter.exe /s 4 /e 0</code> 在匯出過程中，會匯出從 ID 4 開始到清單結尾的可疑物件並鎖定指令行介面

參數	說明	範例
/f <y n>	<p>指定在匯出過程中是否要鎖定指令行介面</p> <hr/> <p> 注意 選用參數；如果未指定，預設值為 "yes"</p> <hr/> <p> 重要 您必須在使用 SuspiciousObjectExporter.exe 工具、PowerShell 程序檔或 Windows 工作排程器中的批次程式檔預約自動匯出時，於「新增引數 (可省略)」欄位中指定下列參數。</p> <p>/f n</p>	<ul style="list-style-type: none"> SuspiciousObjectExporter.exe /f y 在匯出過程中，會匯出所有可疑物件並鎖定指令行介面 SuspiciousObjectExporter.exe /s 0 /e 0 /f y 在匯出過程中，會匯出所有可疑物件並鎖定指令行介面 SuspiciousObjectExporter.exe /f n 在匯出過程中，會匯出所有可疑物件並解除鎖定指令行介面
/d	<p>用於啟動偵錯模式</p> <hr/> <p> 注意 選用參數，通常由支援人員用於識別錯誤</p>	<p>SuspiciousObjectExporter.exe /d</p> <p>匯出所有可疑物件與其他偵錯記錄檔</p>

4. 如果要檢視匯出的可疑物件清單，請移至 <目前的目錄>\SOTools\ 目錄，然後開啟 SuspiciousObjectList.xml 檔案。



如果您遵循此程序，則 <目前的目錄> 指的是 <Control Manager 安裝目錄>。

5. 如果要檢視所有匯出記錄檔，請移至 <目前的目錄>\SOTools\ 目錄，然後開啟 ExportRecord.txt 檔案。

**注意**

如果您遵循此程序，則 <目前的目錄> 指的是 <Control Manager 安裝目錄>。

修改組態設定檔

如果要變更「可疑物件清單匯入程式」的預設組態設定，請移至 <Control Manager 安裝目錄>\SOTools 目錄並修改 SuspiciousObjectExporter.exe.config 檔案。

**秘訣**

Trend Micro 建議您先建立組態設定檔的備份，再進行任何修改。

機碼	說明	範例
outputRootFolderPath 位置： <appSettings>	表示 SuspiciousObjectExporter.exe 工具的工作目錄	<ul style="list-style-type: none"> <code><add key="outputRootFolderPath" value="." /></code> 此工具使用 SuspiciousObjectExporter.exe 程式所在的目錄來處理清單 <code><add key="outputRootFolderPath" value="C:\Program Files (x86)\Trend Micro\Control Manager" /></code> 此工具使用指定的目錄 (C:\Program Files (x86) \Trend Micro\Control Manager) 來處理清單

機碼	說明	範例
outputFolderName 位置： <appSettings>	表示匯出的可疑物件清單檔案的輸出目錄	<ul style="list-style-type: none">• <add key="outputFolderName" value="SOTools"/> 將檔案匯出到 <outputRootFolderPath> \SOTools 目錄• <add key="outputFolderName" value="SOList"/> 將檔案匯出到 <outputRootFolderPath> \SOList 目錄

機碼	說明	範例
styleSheetFile 位置： <appSettings>	表示工具套用到匯出的清單的樣式表	<ul style="list-style-type: none"> <li data-bbox="659 256 1192 354"> <p>• <add key="styleSheetFile" value=""/></p> <p>將 XML 格式的所有清單匯出為 outputFile 機碼所指定的 *.txt 或 *.xml 檔案</p> <li data-bbox="659 370 1192 521"> <p>• <add key="styleSheetFile" value="ExportCSV.xslt"/></p> <p>用於匯出「沙盒虛擬平台可疑物件」清單、「使用者定義的可疑物件」清單或含有限欄子集的「例外」清單（採用 CSV 格式）</p> <hr/> <p> 重要</p> <p>選取 ExportCSV.xslt 樣式表後，您可以不再設定此工具匯出的欄。此工具只會匯出樣式表中指定的欄。</p> <hr/> <li data-bbox="659 716 1192 808"> <p>• <add key="styleSheetFile" value="ExportSTIX.xslt"/></p> <p>用來匯出所有 STIX 格式的可疑物件清單</p> <li data-bbox="659 829 1192 922"> <p>• <add key="styleSheetFile" value="ExportCPL.xslt"/></p> <p>用來匯出所有 CPL 格式的可疑物件清單</p> <hr/> <p> 重要</p> <p>如果您指定樣式表，則必須將 defaultSampleTemplates 機碼設定為相同的值。</p> <hr/>

機碼	說明	範例
outputFile 位置： <appSettings>	表示匯出的可疑物件清單檔案的檔案名稱和副檔名 指定新的副檔名可變更輸出檔案格式	<ul style="list-style-type: none"> <code><add key="outputFile" value="SuspiciousObjectList.xml"/></code> 將可疑物件清單匯出為名為 SuspiciousObjectList.xml 的 *.xml 檔案 <code><add key="outputFile" value="SuspiciousObjectList.txt"/></code> 將可疑物件清單匯出為名為 SuspiciousObjectList.txt 的 *.txt 檔案
defaultSampleTemplates 位置： <appSettings>	表示工具套用到匯出的清單的樣式表來源檔案	<ul style="list-style-type: none"> <code><add key="defaultSampleTemplates" value="ExportCSV.xslt"/></code> 找出指定的樣式表檔案 <hr/> <p> 重要 指定的值必須符合指定給 styleSheetFile 或 defaultSampleTemplates 機碼的值。</p> <hr/> <p> 注意 預設值為 "ExportCPL.xslt ExportSTIX.xslt ExportCSV.xslt"。</p>
<suspiciousObjectColumns> 位置： <soDataColumnSettings>	表示所選清單上的資料欄 設定 isEnable="true" 可匯出指定的資料欄	<ul style="list-style-type: none"> <code><add id="1" name="SeqID" isEnable="true"></add></code> 從所選清單匯出 "SeqID" 資料欄 <code><add id="1" name="MD5Key" isEnable="false"></add></code> 從所選清單明確排除 "MD5Key" 資料欄 <hr/> <p> 重要 如果您指定了 ExportCSV.xslt 樣式表，此工具只會匯出樣式表中指定的欄。</p>

機碼	說明	範例
<p><suspiciousObjectTypeList></p> <p>位置： <soTypeSettings></p>	<p>表示要從所選清單匯出的物件類型</p> <p>設定 isEnabled="true" 可匯出指定的物件類型</p>	<ul style="list-style-type: none"> • <add value="0" description="IP" isEnabled="true"></add> 從所選清單匯出所有 IP 位址類型物件 • <add value="1" description="Domain" isEnabled="false"></add> 從匯出的清單明確排除所有「網域」物件
<p><suspiciousObjectSourceType></p> <p>位置： <soTypeSettings></p>	<p>表示可疑物件來源類型</p> <p>設定 isEnabled="true" 可匯出指定的物件類型</p>	<ul style="list-style-type: none"> • <add value="0" description="SourceType" isEnabled="true"/> 選取「沙盒虛擬平台可疑物件」清單 • <add value="1" description="SourceType" isEnabled="true"/> 選取「使用者定義的可疑物件」清單 • <add value="2" description="SourceType" isEnabled="true"/> 選取「沙盒虛擬平台例外」清單 <hr/> <p> 重要</p> <ul style="list-style-type: none"> • 如果您指定了 ExportCSV.xslt 樣式表，並選取「沙盒虛擬平台可疑物件」清單或「使用者定義的可疑物件」清單，則此工具會匯出下列欄：物件、類型、掃描預先過濾器、注意事項和中毒處理行動。 • 如果您指定了 ExportCSV.xslt 樣式表，並選取「沙盒虛擬平台例外」清單，此工具會匯出下列欄：物件、類型、掃描預先過濾器和注意事項。

使用 Check Point Suspicious Activity Monitoring Client 工具



注意

下列程序假設您使用 Check Point 提供的 CKP_SAM_Client.exe 工具，將可疑物件資料匯入 Check Point 防火牆伺服器。



重要

使用 Check Point SAM Client 工具之前，您必須：

- 準備 Check Point 防火牆伺服器
如需詳細資訊，請參閱[準備 Check Point 防火牆伺服器](#) 第 24-2 頁。
- 準備驗證組態設定檔
如需詳細資訊，請參閱[準備驗證憑證組態設定檔](#) 第 24-4 頁。
- 使用「可疑物件清單匯出程式」工具匯出 Control Manager 可疑物件清單
如需詳細資訊，請參閱[使用可疑物件清單匯出程式 \(SuspiciousObjectExporter.exe\)](#) 第 22-2 頁。

程序

1. 登入 Control Manager 伺服器。
2. 開啟命令提示字元。
3. 使用下列指令找出包含 CKP_SAM_Client.exe 檔案的目錄：

```
cd <Control Manager 安裝目錄>/SOTools
```

4. 使用下列指令執行 CKP_SAM_Client.exe：

```
CKP_SAM_Client.exe -t <timeout> -g <fw-ip> -c <conf_path> -  
A notify any <IP_address>
```

說明：

- `-t <timeout>`：表示 Check Point 伺服器在可疑物件到期之前等待的時間量（以秒為單位）
- `-c <conf_path>`：表示 `sam.conf` 檔案的相對路徑
- `-g <fw-ip>`：表示 Check Point 防火牆伺服器的 IPv4 位址
- `-A notify any <IP_address>`：要求 Check Point 防火牆伺服器通知有效的 IPv4 位址

**注意**

- 在不使用任何引數的情況下執行 `CKP_SAM_Client.exe`，會顯示工具的使用情形詳細資料。
- 如需 Check Point `sam_client_action` 引數的詳細資訊，請參閱 Check Point 防火牆伺服器文件。

`CKP_SAM_Client.exe` 工具會指出已成功完成要求。

5. 如果要檢視 Check Point 防火牆伺服器上匯入的可疑物件資料，請執行下列作業：
 - a. 登入 Check Point SmartView Monitor 主控台。
 - b. 移至「Tools > Suspicious Activity Rules」。

會出現「Enforced Suspicious Activity Rules」畫面，並顯示匯入的可疑物件資料。

第 25 章

技術支援

瞭解下列主題：

- [疑難排解資源](#) 第 25-2 頁
- [聯絡趨勢科技](#) 第 25-3 頁
- [將可疑內容傳送到趨勢科技](#) 第 25-4 頁
- [其他資源](#) 第 25-5 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。

程序

1. 移至 <http://esupport.trendmicro.com/zh-tw/default.aspx>。
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://esupport.trendmicro.com/zh-tw/srf/twbizmain.aspx>

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政策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 <http://about-threats.trendmicro.com/threatencyclopedia.aspx?language=tw&tab=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	http://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：
<http://www.trendmicro.com/us/about-us/contact/index.html>
- 與台灣趨勢科技聯絡：
<http://www.trendmicro.tw/tw/about-us/contact/index.html>
- 趨勢科技產品文件：
<http://docs.trendmicro.com/zh-tw/home.aspx>

加速支援要求

為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
- 安裝的代理程式版本
- 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，以將其包含在全域例外清單中：

<https://ers.trendmicro.com/>

請參閱下列「常見問題集」項目，將訊息範例傳送給趨勢科技：

<http://esupport.trendmicro.com/solution/zh-TW/1112106.aspx>

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：

<http://esupport.trendmicro.com/solution/zh-tw/1059565.aspx>

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）：

<http://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：

<http://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。

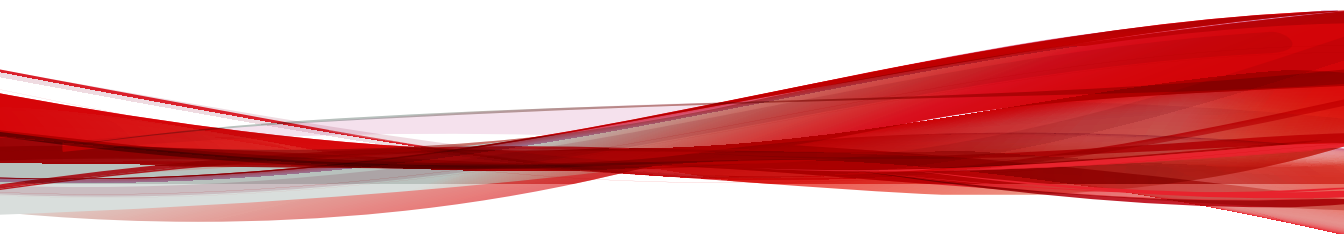
文件意見反應

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

docs@trendmicro.com 聯絡我們。

附錄

附錄



附錄 A

Control Manager 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](#)
- [Control Manager 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 Control Manager 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
Control Manager 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 Control Manager 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

Control Manager 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	
防火牆、「轉送」通訊埠 (選用; 在 Control Manager 代理程式安裝期間使用)	224	

Control Manager 慣例

請參閱下列適用於 Control Manager 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：40 個字元
 - 不允許的字元：/ > & "

**注意**

對於 Control Manager 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

Control Manager 會以 XML 格式儲存系統組態設定和暫存檔案。

下表說明 Control Manager 所使用的組態設定檔和處理程序。

表 A-2. Control Manager 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

組態設定檔	說明
CmdProcessorEventHandler.xml	由 CmdProcessor.exe 使用
DMRegisterinfo.xml	由 CasProcessor.exe 使用
DataSource.xml	儲存 Control Manager 處理程序的連線參數
SystemConfiguration.xml	Control Manager 系統組態設定檔
agent.ini	MCP 代理程式檔案

表 A-3. Control Manager 處理程序

程序	說明
ProcessManager.exe	啟動和停止其他 Control Manager 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 3.0 Service Pack 4 開始，LogReceiver.exe 只會處理來自 Trend Micro Damage Control Services 和「趨勢科技弱點評估」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 Control Manager 資料庫中的記錄檔
ReportServer.exe	產生 Control Manager 報告
MsgReceiver.exe	從 Control Manager 伺服器 and 受管理產品接收訊息
CasProcessor.exe	允許 Control Manager 伺服器管理其他 Control Manager 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 Control Manager Web 主控台登入頁面，以及管理「產品目錄」（Control Manager 端）

程序	說明
sCloudProcessor.NET.exe	可要求 Control Manager 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 Control Manager 通訊和監聽通訊埠。

服務	服務通訊埠
ProcessManager.exe	20501
CmdProcessor.exe	20101
cmdProcessor.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 Control Manager 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-85 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。

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-1. 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：OfficeScan 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：OfficeScan 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

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：OfficeScan 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-2. 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：OfficeScan 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：OfficeScan 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：OfficeScan 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

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-3. 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：OfficeScan 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：OfficeScan 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
偵測	顯示受管理產品偵測到的病毒/惡意程式總數。 範例：OfficeScan 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-4. 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：OfficeScan 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：OfficeScan 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：OfficeScan 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	顯示偵測到病毒/惡意程式的唯一端點數目。 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/惡意程式詳細資訊

此資料檢視提供有關您網路上病毒/惡意程式執行個體的特定資訊。範例：偵測到病毒/惡意程式的受管理產品、病毒/惡意程式的名稱、具有病毒/惡意程式的端點名稱

表 B-5. 病毒/惡意程式詳細資訊資料檢視

資料	說明
收到	顯示 Control Manager 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： <ul style="list-style-type: none"> 受管理產品的實體顯示名稱。Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。 已安裝用戶端（例如 OfficeScan 用戶端）的電腦 IP 位址或主機名稱。
產品	顯示受管理產品的名稱。 範例：OfficeScan、ScanMail for Microsoft Exchange

資料	說明
產品/端點 IP	此資料欄顯示下列其中一項： <ul style="list-style-type: none"> 安裝了受管理產品的伺服器 IP 位址。 已安裝用戶端（例如 OfficeScan 用戶端）的電腦 IP 位址。
產品/端點 MAC	此資料欄顯示下列其中一項： <ul style="list-style-type: none"> 安裝了受管理產品的伺服器 MAC 位址。 已安裝用戶端（例如 OfficeScan 用戶端）的電腦 MAC 位址。
管理伺服器實體	顯示受管理產品伺服器（端點會向此伺服器註冊）的實體顯示名稱。
網域	顯示受管理產品伺服器（端點會向此伺服器註冊）的網域。
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
端點感染通道	安全威脅源自的通道
端點	顯示受病毒/惡意程式影響的電腦 IP 位址或主機名稱。
來源主機	顯示病毒/惡意程式起源所在的電腦 IP 位址或主機名稱。
使用者	顯示受管理產品偵測到病毒/惡意程式時登入端點電腦的使用者名稱。
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
偵測	顯示受管理產品偵測到的病毒/惡意程式總數。 範例：OfficeScan 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

資料	說明
項目類型	顯示受管理產品偵測到的病毒/惡意程式的進入點。 範例：在檔案、HTTP、Windows Live Messenger (MSN) 中發現病毒
詳細資訊	僅用於臨機操作查詢。顯示有關選取項目的詳細資訊。 在臨機操作查詢中，此欄會以加上底線的方式顯示選取項目。按一下加上底線的選取項目將會顯示有關選取項目的詳細資訊。 範例：主機詳細資料、網路詳細資料、HTTP/FTP 詳細資料
OfficeScan 網域階層	顯示 OfficeScan 網域階層的路徑。
部門	顯示端點所屬的部門名稱
作業系統	顯示在端點上執行的作業系統
特徵碼/規則	顯示觸發偵測的特徵碼或規則
特徵碼/規則版本	顯示觸發偵測的特徵碼或規則版本
雲端服務供應商	顯示雲端服務供應商的名稱

端點病毒/惡意程式資訊

提供有關端點上發現的病毒/惡意程式執行個體的特定資訊。範例：偵測到病毒/惡意程式的受管理產品、偵測到病毒/惡意程式的掃描類型、端點上偵測到病毒/惡意程式的檔案路徑

表 B-6. 端點病毒/惡意程式資訊資料檢視

資料	說明
收到	顯示 Control Manager 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。

資料	說明
產品實體/端點	此資料欄顯示下列其中一項： <ul style="list-style-type: none"> • 受管理產品的實體顯示名稱。Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。 • 已安裝用戶端（例如 OfficeScan 用戶端）的電腦 IP 位址或主機名稱。
產品/端點 IP	此資料欄顯示下列其中一項： <ul style="list-style-type: none"> • 安裝了受管理產品的伺服器 IP 位址。 • 已安裝用戶端（例如 OfficeScan 用戶端）的電腦 IP 位址。
產品	顯示受管理產品的名稱。 範例： OfficeScan 、 ScanMail for Microsoft Exchange
管理伺服器實體	顯示受管理產品伺服器（端點會向此伺服器註冊）的實體顯示名稱。
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
端點	顯示受病毒/惡意程式影響的電腦名稱。
使用者	顯示受管理產品偵測到病毒/惡意程式時登入端點電腦的使用者名稱。
掃描類型	顯示受管理產品用來偵測病毒/惡意程式的掃描類型。範例：即時、預約、手動
檔案	顯示受管理產品偵測到受病毒/惡意程式影響的檔案名稱。
檔案路徑	顯示受管理產品在端點電腦上偵測到病毒/惡意程式的檔案路徑。
壓縮檔中的檔案	顯示壓縮檔中的中毒檔案/病毒/惡意程式名稱。
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

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：OfficeScan 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	顯示雲端服務供應商的名稱

Web 病毒/惡意程式資訊

提供有關 HTTP 或 FTP 流量中發現的 Web 病毒/惡意程式執行個體的特定資訊。範例：偵測到病毒/惡意程式的受管理產品、病毒/惡意程式發生所在位置的傳輸方向、下載病毒/惡意程式的 Internet 瀏覽器或 FTP 端點。

表 B-7. Web 病毒/惡意程式資訊資料檢視

資料	說明
收到	顯示 Control Manager 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： <ul style="list-style-type: none"> 受管理產品的實體顯示名稱。Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。 已安裝用戶端（例如 OfficeScan 用戶端）的電腦 IP 位址或主機名稱。
產品	顯示受管理產品的名稱。 範例：OfficeScan、ScanMail for Microsoft Exchange
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
端點	顯示受管理產品偵測到存在 Web 病毒/惡意程式的電腦的 IP 位址或主機名稱。

資料	說明
來源 URL	顯示 Web 病毒/惡意程式起源所在 Web/FTP 站台的 URL。
使用者	顯示受管理產品偵測到病毒/惡意程式時登入端點電腦的使用者名稱。
流量/連線	顯示病毒/惡意程式進入的方向。
瀏覽器/FTP 用戶端	顯示 Web 病毒/惡意程式起源所在的 Internet 瀏覽器或 FTP 端點。
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
偵測	顯示受管理產品偵測到的病毒/惡意程式總數。 範例：OfficeScan 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	顯示雲端服務供應商的名稱

電子郵件病毒/惡意程式資訊

提供有關電子郵件訊息中發現的病毒/惡意程式執行個體的特定資訊。範例：偵測到病毒/惡意程式的受管理產品、電子郵件訊息的主旨行內容、包含病毒/惡意程式的電子郵件訊息寄件者

表 B-8. 電子郵件病毒/惡意程式資訊資料檢視

資料	說明
收到	顯示 Control Manager 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。
產品項目	顯示受管理產品的實體顯示名稱。Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。

資料	說明
產品	顯示受管理產品的名稱。 範例：OfficeScan、ScanMail for Microsoft Exchange
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
收件者	顯示包含病毒/惡意程式的電子郵件訊息收件者。
寄件者	顯示包含病毒/惡意程式的電子郵件訊息寄件者。
使用者	顯示受管理產品偵測到病毒/惡意程式時登入端點電腦的使用者名稱。
主旨	顯示包含病毒/惡意程式的電子郵件訊息主旨行內容。
檔案	顯示受管理產品偵測到受病毒/惡意程式影響的檔案名稱。
壓縮檔中的檔案	顯示壓縮檔中的中毒檔案/病毒/惡意程式名稱。
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
偵測	顯示受管理產品偵測到的病毒/惡意程式總數。 範例：OfficeScan 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	顯示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。範例：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、有關病毒/惡意程式的來源與目標特定資訊

表 B-9. 網路病毒/惡意程式資訊資料檢視

資料	說明
收到	顯示 Control Manager 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： <ul style="list-style-type: none"> 受管理產品的實體顯示名稱。Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。 已安裝用戶端（例如 OfficeScan 用戶端）的電腦 IP 位址或主機名稱。
產品	顯示受管理產品的名稱。 範例：OfficeScan、ScanMail for Microsoft Exchange
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
端點	顯示受病毒/惡意程式影響的電腦的 IP 位址/主機名稱。
來源主機	顯示病毒/惡意程式起源所在的電腦 IP 位址或主機名稱。
使用者	顯示受管理產品偵測到病毒/惡意程式時登入端點電腦的使用者名稱。
流量/連線	顯示病毒/惡意程式進入的方向。
通訊協定	顯示病毒/惡意程式進入網路所用的通訊協定。 範例：HTTP、SMTP、FTP
端點電腦	顯示受病毒/惡意程式影響的電腦的名稱。
端點通訊埠	顯示受病毒/惡意程式影響的電腦的通訊埠號碼。
端點 MAC	顯示受病毒/惡意程式影響的電腦的 MAC 位址。
來源電腦	顯示病毒/惡意程式起源所在的電腦的電腦名稱。
來源通訊埠	顯示病毒/惡意程式起源所在的電腦的通訊埠號碼。
來源 MAC	顯示病毒/惡意程式起源所在的電腦的 MAC 位址。

資料	說明
檔案	顯示受管理產品偵測到受病毒/惡意程式影響的檔案名稱。
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
偵測	顯示受管理產品偵測到的病毒/惡意程式總數。 範例：OfficeScan 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	顯示雲端服務供應商的名稱

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-10. 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。

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。 OfficeScan 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： OfficeScan 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-11. 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。
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： OfficeScan 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 個課程式/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： OfficeScan 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：OfficeScan 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

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-12. 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：OfficeScan 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：OfficeScan 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：OfficeScan 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）內の間諜程式/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-13. 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。
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：OfficeScan 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：OfficeScan 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：OfficeScan 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：OfficeScan 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-14. 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
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：OfficeScan 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：OfficeScan 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：OfficeScan 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詳細資訊

提供有關您網路上的間諜程式/可能的資安威脅程式執行個體的特定資訊。範例：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、具有間諜程式/可能的資安威脅程式的端點名稱

表 B-15. 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	顯示 Control Manager 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： <ul style="list-style-type: none"> 受管理產品的實體顯示名稱。Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品 已安裝用戶端（例如 OfficeScan 用戶端）且受間諜程式/可能的資安威脅程式影響的電腦 IP 位址或主機名稱
產品	顯示受管理產品的名稱。範例： OfficeScan 、 ScanMail for Microsoft Exchange
產品/端點 IP	此資料欄顯示下列其中一項： <ul style="list-style-type: none"> 安裝了受管理產品的伺服器 IP 位址 已安裝用戶端（例如 OfficeScan 用戶端）且受間諜程式/可能的資安威脅程式影響的電腦 IP 位址
產品/端點 MAC	此資料欄顯示下列其中一項： <ul style="list-style-type: none"> 安裝了受管理產品的伺服器 MAC 位址 已安裝用戶端（例如 OfficeScan 用戶端）且受間諜程式/可能的資安威脅程式影響的電腦 MAC 位址
管理伺服器實體	顯示受管理產品伺服器（端點會向此伺服器註冊）的實體顯示名稱
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
端點	顯示受間諜程式/可能的資安威脅程式影響的電腦 IP 位址或主機名稱

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 IP 位址或主機名稱
使用者	顯示受管理產品偵測到間諜程式/可能的資安威脅程式時登入端點電腦的使用者名稱
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
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
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：OfficeScan 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	顯示受管理產品偵測到的間諜程式/可能的資安威脅程式的進入點。 範例：在檔案、HTTP、Windows Live Messenger (MSN) 中發現病毒
詳細資訊	僅用於記錄查詢。顯示有關選取項目的詳細資訊。 在記錄查詢中，此欄會以加上底線的方式顯示選取項目。按一下加上底線的選取項目將會顯示有關選取項目的詳細資訊。 範例：主機詳細資料、網路詳細資料、HTTP/FTP 詳細資料
端點感染通道	顯示安全威脅源自的通道
OfficeScan 網域階層	顯示 OfficeScan 用戶端所屬的用戶端樹狀結構網域或子網域
網域	顯示該端點所屬網域的名稱
作業系統	顯示在端點上執行的作業系統
雲端服務供應商	顯示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

提供有關端點上發現的間諜程式/可能的資安威脅程式執行個體的特定資訊。
 範例：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描類型、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-16. 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	顯示 Control Manager 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： <ul style="list-style-type: none"> 受管理產品的實體顯示名稱。Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品 已安裝用戶端（例如 OfficeScan 用戶端）且受間諜程式/可能的資安威脅程式影響的電腦 IP 位址或主機名稱
產品/端點 IP	此資料欄顯示下列其中一項： <ul style="list-style-type: none"> 安裝了受管理產品的伺服器 IP 位址 已安裝用戶端（例如 OfficeScan 用戶端）且受間諜程式/可能的資安威脅程式影響的電腦 IP 位址
產品	顯示受管理產品的名稱 範例：OfficeScan、ScanMail for Microsoft Exchange
管理伺服器實體	顯示受管理產品伺服器（端點會向此伺服器註冊）的實體顯示名稱
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
端點	顯示受間諜程式/可能的資安威脅程式影響的電腦 IP 位址或主機名稱
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 IP 位址或主機名稱

資料	說明
使用者	顯示受管理產品偵測到間諜程式/可能的資安威脅程式時登入端點電腦的使用者名稱
掃描類型	顯示受管理產品用來偵測間諜程式/可能的資安威脅程式的掃描類型 範例：即時、預約、手動
資源	顯示受影響的特定資源 範例：application.exe、H Key Local Machine\SOFTWARE\ACME
資源類型	顯示受間諜程式/可能的資安威脅程式影響的資源類型 範例：登錄、記憶體資源
安全威脅類型	顯示受管理產品偵測到的間諜程式/可能的資安威脅程式特定類型 範例：廣告軟體、COOKIE、對等式應用程式
風險等級	顯示趨勢科技針對間諜程式/可能的資安威脅程式對您網路造成的風險所定義的風險等級。 範例：高安全性、中等安全性、低安全性
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
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
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
雲端服務供應商	顯示雲端服務供應商的名稱

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。範例：偵測到間諜程式/可能的資安威脅程式的受管理產品、間

課程式/可能的資安威脅程式發生所在位置的傳輸方向、下載間課程式/可能的資安威脅程式的 Internet 瀏覽器或 FTP 端點

表 B-17. Web 間課程式/可能的資安威脅程式資料檢視

資料	說明
收到	顯示 Control Manager 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： <ul style="list-style-type: none"> 受管理產品的實體顯示名稱。Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品 已安裝用戶端（例如 OfficeScan 用戶端）且受間課程式/可能的資安威脅程式影響的電腦 IP 位址或主機名稱
產品	顯示受管理產品的名稱 範例：OfficeScan、ScanMail for Microsoft Exchange
間課程式/可能的資安威脅程式	顯示受管理產品偵測到的間課程式/可能的資安威脅程式名稱
IP	顯示受管理產品偵測到存在間課程式/可能的資安威脅程式的電腦的 IP 位址
來源 URL	顯示間課程式/可能的資安威脅程式起源所在 Web/FTP 站台的 URL
流量/連線	顯示間課程式/可能的資安威脅程式進入的方向。
瀏覽器/FTP 用戶端	顯示間課程式/可能的資安威脅程式起源所在的 Internet 瀏覽器或 FTP 端點
使用者	顯示受管理產品偵測到間課程式/可能的資安威脅程式時登入端點電腦的使用者名稱
結果	顯示受管理產品對間課程式/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
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：OfficeScan 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	顯示雲端服務供應商的名稱

電子郵件間諜程式/可能的資安威脅程式

提供有關電子郵件訊息中發現的間諜程式/可能的資安威脅程式執行個體的特定資訊。範例：偵測到間諜程式/可能的資安威脅程式的受管理產品、電子郵件訊息的主旨行內容、包含間諜程式/可能的資安威脅程式的電子郵件訊息寄件者

表 B-18. 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	顯示 Control Manager 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
產品項目	顯示受管理產品的實體顯示名稱。Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品
產品	顯示受管理產品的名稱 範例：OfficeScan、ScanMail for Microsoft Exchange
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
收件者	顯示包含間諜程式/可能的資安威脅程式的電子郵件訊息收件者
寄件者	顯示包含間諜程式/可能的資安威脅程式的電子郵件訊息寄件者

資料	說明
使用者	顯示受管理產品偵測到間諜程式/可能的資安威脅程式時登入端點電腦的使用者名稱
主旨	顯示包含間諜程式/可能的資安威脅程式的電子郵件訊息的主旨行內容
檔案	顯示受管理產品偵測到受間諜程式/可能的資安威脅程式影響的檔案名稱
壓縮檔中的檔案	顯示存在於壓縮檔中的間諜程式/可能的資安威脅程式的檔案名稱
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
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
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：OfficeScan 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	顯示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。範例：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、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-19. 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	顯示 Control Manager 從受管理產品收到資料的時間

資料	說明
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： <ul style="list-style-type: none"> 受管理產品的實體顯示名稱。Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。 已安裝用戶端（例如 OfficeScan 用戶端）且受間諜程式/可能的資安威脅程式影響的電腦 IP 位址或主機名稱。
產品	顯示受管理產品的名稱 範例：OfficeScan、ScanMail for Microsoft Exchange
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
流量/連線	顯示間諜程式/可能的資安威脅程式進入的方向。
通訊協定	顯示間諜程式/可能的資安威脅程式進入網路所用的通訊協定 範例：HTTP、SMTP、FTP
端點 IP	顯示受間諜程式/可能的資安威脅程式影響的電腦的 IP 位址
端點	顯示受間諜程式/可能的資安威脅程式影響的電腦 IP 位址或主機名稱
端點通訊埠	顯示受間諜程式/可能的資安威脅程式影響的電腦的通訊埠號碼
端點 MAC	顯示受間諜程式/可能的資安威脅程式影響的電腦的 MAC 位址
來源 IP	顯示間諜程式/可能的資安威脅程式起源所在的電腦的 IP 位址
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的主機名稱
來源通訊埠	顯示間諜程式/可能的資安威脅程式起源所在的電腦的通訊埠號碼
來源 MAC	顯示間諜程式/可能的資安威脅程式起源所在的電腦的 MAC 位址
使用者	顯示受管理產品偵測到間諜程式/可能的資安威脅程式時登入端點電腦的使用者名稱
檔案	顯示受管理產品偵測到受間諜程式/可能的資安威脅程式影響的檔案名稱

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
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
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：OfficeScan 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	顯示雲端服務供應商的名稱

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-20. 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-21. 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

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-22. 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
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

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
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-23. 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。

內容違規詳細資訊

提供有關網路上內容違規的特定資訊。範例：偵測到內容違規的受管理產品、違反的特定策略名稱、網路上的內容違規總數

表 B-24. 內容違規詳細資訊資料檢視

資料	說明
收到	顯示 Control Manager 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。
產品項目	顯示受管理產品的實體顯示名稱。 Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。
產品	顯示受管理產品的名稱。範例： OfficeScan 、 ScanMail for Microsoft Exchange
收件者	顯示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	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。
主旨	顯示違反策略之電子郵件的主旨行內容。
策略	顯示電子郵件違反的策略名稱。
策略設定	顯示電子郵件違反的策略設定。
檔案位置	顯示違反策略的檔案位置。
檔案	顯示違反策略的檔案名稱。
URL	顯示違反指定策略的 URL。
風險等級	顯示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	顯示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	顯示偵測到電子郵件違規的子過濾器類型。
過濾器處理行動	顯示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	顯示偵測到電子郵件違規之過濾器的處理行動結果。

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：傳送、清除巨集、轉寄
偵測	顯示受管理產品偵測到的策略違規總數。

內含進階安全威脅的電子郵件訊息

顯示內含惡意和可疑行為的所有電子郵件訊息。可疑行為包括異常行為、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	顯示 Control Manager 從受管理產品收到資料的時間。
產品項目	顯示受管理產品的實體顯示名稱。 Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。
產品	顯示受管理產品的名稱。範例： OfficeScan 、 ScanMail for Microsoft Exchange
收件者	顯示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	顯示傳送違反受管理產品策略內容的電子郵件信箱。
主旨	顯示違反策略之電子郵件的主旨行內容。
附件計數	附件數目
附件	附件名稱
附件類型	附件類型
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：傳送、清除巨集、隔離
安全威脅類型	安全威脅類型
安全威脅名稱	安全威脅名稱

資料	說明
風險等級	調查後的電子郵件訊息風險等級
來源 IP	最接近電子郵件寄件者的 MTA IP 位址
訊息 ID	由管理員設定的唯一訊息 ID
連結計數	訊息中的連結數目
連結	連結清單

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-25. 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

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-26. 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
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

資料	說明
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

垃圾郵件詳細資訊

提供有關網路上垃圾郵件違規的特定資訊。範例：偵測到內容違規的受管理產品、違反的特定策略名稱、網路上的垃圾郵件違規總數

表 B-27. 垃圾郵件詳細資訊資料檢視

資料	說明
收到	顯示 Control Manager 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。
產品項目	顯示受管理產品的實體顯示名稱。 Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。
產品	顯示受管理產品的名稱。 範例：OfficeScan、ScanMail for Microsoft Exchange
收件者	顯示內含垃圾郵件之電子郵件的收件者。
寄件者	顯示內含垃圾郵件之電子郵件的寄件者。
主旨	顯示內含垃圾郵件之電子郵件的主旨行內容。
策略	顯示電子郵件違反的策略名稱。
處理行動	顯示受管理產品對在電子郵件中發現的垃圾郵件採取的處理行動類型。 範例：傳送、轉寄、清除巨集

資料	說明
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

提供有關網路上垃圾郵件來源的特定資訊。範例：偵測到垃圾郵件違規的受管理產品、受管理產品對垃圾郵件違規採取的特定處理行動、網路上的垃圾郵件違規總數

表 B-28. 垃圾郵件連線資訊資料檢視

資料	說明
收到	顯示 Control Manager 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。
產品項目	顯示受管理產品的實體顯示名稱。Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。
產品	顯示受管理產品的名稱。 範例：OfficeScan、ScanMail for Microsoft Exchange
來源 IP	顯示垃圾郵件起源所在的郵件伺服器 IP 位址。
過濾器類型	顯示偵測到電子郵件違規的過濾器類型。 範例：即時 Blackhole 清單 (RBL+)、快速 IP 清單 (QIL)
處理行動	顯示受管理產品為防止垃圾郵件進入郵件伺服器而對垃圾郵件採取的處理行動類型。 範例：中斷連線、略過連線

資料	說明
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

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。

防火牆違規事件詳細資訊

提供有關網路上防火牆違規的特定資訊。範例：偵測到防火牆違規的受管理產品、有關來源和目標的特定資訊、網路上的防火牆違規總數

表 B-29. 防火牆違規詳細資訊資料檢視

資料	說明
收到	顯示 Control Manager 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： <ul style="list-style-type: none"> 受管理產品的實體顯示名稱。Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品 已安裝用戶端（例如 OfficeScan 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：OfficeScan、ScanMail for Microsoft Exchange
事件類型	顯示觸發違規的事件類型。範例：入侵、策略違規

資料	說明
風險等級	顯示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	顯示違規項目的方向
通訊協定	顯示入侵使用的通訊協定 範例：HTTP、SMTP、FTP
來源 IP	顯示嘗試入侵您網路之電腦的 IP 位址
端點通訊埠	顯示遭到攻擊之電腦的通訊埠號碼
端點 IP	顯示遭到攻擊之電腦的 IP 位址
目標應用程式	顯示入侵鎖定的目標應用程式
說明	趨勢科技針對事件提供的詳細說明
處理行動	顯示受管理產品對策略違規採取的處理行動類型 範例：檔案已清除、檔案已隔離、檔案暫不處理
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

網路內容檢測資訊

此資料檢視提供有關網路上網路內容違規的特定資訊。

表 B-30. 網路內容檢測資訊資料檢視

資料	說明
收到	顯示 Control Manager 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

資料	說明
產品實體/端點	此資料欄顯示下列其中一項： <ul style="list-style-type: none"> 受管理產品的實體顯示名稱。Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品 已安裝用戶端（例如 OfficeScan 用戶端）的電腦 IP 位址或主機名稱
產品	顯示受管理產品的名稱 範例：OfficeScan、ScanMail for Microsoft Exchange
流量/連線	顯示違規項目的方向
端點 IP	顯示遭到攻擊之電腦的 IP 位址
端點通訊埠	顯示遭到攻擊之電腦的通訊埠號碼
目標 IP	顯示網路上可能的目標電腦的 IP 位址
目標網域	顯示網路上可能的目標電腦的網域
目標程序	顯示違規將其做為目標的程序
處理行動	顯示受管理產品對策略違規採取的處理行動類型
特徵碼類型	顯示符合違規的特徵碼類型

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-31. 端點安全違規詳細資訊資料檢視

資料	說明
收到	顯示 Control Manager 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。
產品項目	顯示受管理產品的實體顯示名稱。 Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。

資料	說明
產品	顯示受管理產品的名稱。 範例：OfficeScan、ScanMail for Microsoft Exchange
端點	顯示符合策略/規則之電腦的主機名稱。
端點 IP	顯示符合策略/規則之電腦的 IP 位址。
端點 MAC	顯示符合策略/規則之電腦的 MAC 位址。
策略/規則名稱	顯示合規的策略/規則名稱。
服務	顯示符合策略/規則的服務/程式名稱。
使用者	顯示受管理產品偵測到策略/規則合規時已登入端點的使用者名稱。
強制性處理行動	顯示策略/規則強制執行的處理行動。
矯正性處理行動	顯示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	顯示受管理產品偵測到的策略/規則合規總數。 範例：受管理產品在 1 部電腦上偵測到相同類型的 10 個合規執行個體。 偵測數 = 10

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執行個體的特定資訊。範例：偵測到安全性符合的受管理產品、合規的特定策略名稱、網路上的安全性符合總數

表 B-32. 端點安全性符合詳細資訊資料檢視

資料	說明
收到	顯示 Control Manager 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。

資料	說明
產品項目	顯示受管理產品的實體顯示名稱。 Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。
產品	顯示受管理產品的名稱。 範例：OfficeScan、ScanMail for Microsoft Exchange
端點	顯示符合策略/規則之電腦的主機名稱。
端點 IP	顯示符合策略/規則之電腦的 IP 位址。
端點 MAC	顯示符合策略/規則之電腦的 MAC 位址。
策略/規則名稱	顯示合規的策略/規則名稱。
服務	顯示符合策略/規則的服務/程式名稱。
使用者	顯示受管理產品偵測到策略/規則合規時已登入端點的使用者名稱。
說明	趨勢科技針對事件提供的詳細說明。
偵測	顯示受管理產品偵測到的策略/規則合規總數。 範例：受管理產品在 1 部電腦上偵測到相同類型的 10 個合規執行個體。 偵測數 = 10

詳細應用程式活動

顯示有關您網路上應用程式活動的整體資訊。範例：偵測到安全性符合的受管理產品、合規的特定策略名稱、網路上的安全性符合總數

表 B-33. 詳細應用程式活動資料檢視

資料	說明
收到	Control Manager 從受管理產品收到資料的時間。
已產生	受管理產品產生資料的時間。

資料	說明
產品項目	受管理產品的實體顯示名稱。Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。
產品	受管理產品的名稱。 範例：OfficeScan、ScanMail for Microsoft Exchange
VLAN ID	顯示可疑安全威脅起源所在的來源 VLAN ID (VID)。
偵測者	顯示偵測到可疑安全威脅的過濾器、掃描引擎或受管理產品。
流量/連線	顯示網路流量的方向，或網路上可疑安全威脅起源所在的位置。
通訊協定群組	顯示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	顯示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	顯示符合策略/規則之電腦的主機名稱。
來源 IP	顯示可疑安全威脅起源所在的來源 IP 位址。
來源 MAC	顯示可疑安全威脅起源所在的來源 MAC 位址。
來源通訊埠	顯示可疑安全威脅起源所在的來源通訊埠號碼。
來源 IP 群組	顯示違規起源所在的來源 IP 位址群組。
來源網路區域	顯示違規起源所在的來源網路區域。
端點 IP	顯示受可疑安全威脅影響之端點的 IP 位址。
端點通訊埠	顯示受可疑安全威脅影響之端點的通訊埠號碼。
端點 MAC	顯示受可疑安全威脅影響之端點的 MAC 位址。
端點群組	顯示受可疑安全威脅影響之端點的 IP 位址群組。
端點網路區域	顯示受可疑安全威脅影響之端點的網路區域。

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
安全威脅類型	顯示受管理產品偵測到的特定類型安全威脅。
偵測嚴重性	顯示事件的嚴重性層級。
IP 位址 (關注的)	顯示目標端點 (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)	顯示與關注的 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	顯示符合同一彙整規則的記錄檔計數。
彙整的相符已歸類事件	顯示符合同一規則的已彙整記錄檔計數。
網路群組	顯示群組的名稱。
主機嚴重性	顯示主機嚴重性。
記錄 ID	顯示記錄 ID。

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-34. 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 Control Manager 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

資料	說明
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

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-35. 裝置存取控制資訊資料檢視

資料	說明
收到	顯示 Control Manager 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

資料	說明
產品實體/端點	此資料欄顯示下列其中一項： <ul style="list-style-type: none"> 受管理產品的實體顯示名稱。Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品 已安裝用戶端（例如 OfficeScan 用戶端）的電腦 IP 位址或主機名稱
產品	顯示受管理產品的名稱 範例： OfficeScan
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

Endpoint Application Control 違規詳細資訊

提供有關網路上應用程式違規的特定資訊。例如：違反的策略和規則名稱、有關端點和應用程式的特定資訊

表 B-36. Endpoint Application Control 違規詳細資訊資料檢視

資料	說明
收到	顯示 Control Manager 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。
使用者名稱	顯示使用者帳號的名稱。
端點	顯示受影響的電腦的主機名稱。
處理行動	顯示處理行動類型：允許、封鎖、鎖定。
應用程式	顯示會觸發規則的應用程式名稱。

資料	說明
版本	顯示版本資訊。
策略	顯示 Trend Micro™ Endpoint Application Control™ 策略的名稱。
規則	顯示應用程式使用率的規則名稱。
伺服器	顯示 Endpoint Application Control 伺服器的主機名稱。
連線狀態	顯示所連線到的特定 Endpoint Application Control 伺服器的狀態。
端點 IP 位址	顯示符合策略/規則之電腦的 IP 位址。
SHA-1	顯示檔案簽章。
指令	顯示所發出指令的類型。
程序擁有者	顯示發出指令之帳號的使用者名稱。

入侵防護詳細資訊

使用此資訊可即時抵禦已知的攻擊和零時差攻擊、防範 Web 應用程式弱點，以及識別會存取網路的惡意軟體。

資料	說明
收到	顯示 Control Manager 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。
伺服器	顯示受管理產品伺服器的主機名稱。
來源 IP	入侵來源的 IP 位址
來源 MAC	入侵來源的 MAC 位址
來源通訊埠	入侵來源的通訊埠號碼
目標 IP	入侵目標的 IP 位址
目標 MAC	入侵目標的 MAC 位址

資料	說明
目標通訊埠	入侵目標的通訊埠號碼
MAC (關注的)	顯示目標端點（來源或目標）的 MAC 位址。如果入侵是在網路內部發生的，則關注的 MAC 是來源 MAC 位址。如果流量是外部流量，則關注的 IP 是目標 MAC 位址。
模式	內聯或分流
處理行動	顯示受管理產品對入侵採取的處理行動類型。 範例：防範、偵測
方向	通訊方向
排名	入侵排名
嚴重性	入侵嚴重性
通訊協定	入侵期間使用的通訊協定
應用程式	易受攻擊的應用程式
原因	拒絕封包的原因

完整性監控資訊

使用資訊來監控電腦上特定區域是否發生變更，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	顯示 Control Manager 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
伺服器	顯示受管理產品伺服器的主機名稱
變更	電腦變更
使用者	登入電腦的使用者

資料	說明
處理程序	已變更的程序
類型	登錄機碼的類型
機碼	登錄機碼
排名	完整性排名
嚴重性	變更的嚴重性

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。

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-37. 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

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-38. 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
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 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-39. 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

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-40. 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

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-41. 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

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-42. 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 違規詳細資訊

此資料檢視提供有關您網路上 Web 違規的特定資訊。例如，偵測到 Web 違規的受管理產品、違規的特定策略名稱或網路上的 Web 違規總數。

表 B-43. Web 違規詳細資訊資料檢視

資料	說明
收到	顯示 Control Manager 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。
管理伺服器實體	顯示管理產品項目的伺服器實體顯示名稱。
產品項目	顯示受管理產品的實體顯示名稱。Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。
產品	顯示受管理產品的名稱。 範例：OfficeScan、ScanMail for Microsoft Exchange

資料	說明
流量/連線	顯示違規項目的方向。
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
URL	顯示違反 Web 策略的 URL 名稱。
使用者/IP	顯示違反策略的端點使用者或 IP 位址。
使用者群組	顯示違反策略的使用者的使用者群組。
端點	顯示違反策略的端點 IP 位址。
端點主機	顯示違反策略的端點 IP 位址或主機名稱。
產品主機	顯示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	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
封鎖規則	顯示阻止存取違規 URL 的封鎖規則。 範例：URL 封鎖
策略	顯示 URL 違反的策略名稱。
檔案	顯示違反策略的檔案名稱。
處理程序	顯示違反策略的程序名稱。
網頁信譽評等分級	顯示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	顯示受管理產品對策略違規採取的處理行動類型。 範例：暫不處理、封鎖
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

網站信譽評等服務詳細資訊

顯示有關您網路上應用程式活動的整體資訊。範例：偵測到安全性符合的受管理產品、符合的特定策略名稱、網路上的安全性符合總數

表 B-44. 網站信譽評等服務詳細資訊資料檢視

資料	說明
收到	Control Manager 從受管理產品收到資料的時間。
已產生	受管理產品產生資料的時間。
產品項目	受管理產品的實體顯示名稱。 Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。
產品	受管理產品的名稱。 範例：OfficeScan、ScanMail for Microsoft Exchange
VLAN ID	顯示可疑安全威脅起源所在的來源 VLAN ID (VID)。
偵測者	顯示偵測到可疑安全威脅的過濾器、掃描引擎或受管理產品。
流量/連線	顯示網路流量的方向，或網路上可疑安全威脅起源所在的位置。
通訊協定群組	顯示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	顯示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	顯示符合策略/規則之電腦的主機名稱。
來源 IP	顯示可疑安全威脅起源所在的來源 IP 位址。
來源 MAC	顯示可疑安全威脅起源所在的來源 MAC 位址。
來源通訊埠	顯示可疑安全威脅起源所在的來源通訊埠號碼。
來源 IP 群組	顯示可疑安全威脅起源所在的來源 IP 位址群組。
來源網路區域	顯示可疑安全威脅起源所在的來源網路區域。

資料	說明
端點 IP	顯示受可疑安全威脅影響之端點的 IP 位址。
端點通訊埠	顯示受可疑安全威脅影響之端點的通訊埠號碼。
端點 MAC	顯示受可疑安全威脅影響之端點的 MAC 位址。
端點群組	顯示受可疑安全威脅影響之端點的 IP 位址群組。
端點網路區域	顯示受可疑安全威脅影響之端點的網路區域。
策略/規則名稱	顯示可疑安全威脅所違反的策略/規則。
URL	顯示視為可疑安全威脅的 URL。
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
C&C 清單來源	顯示辨識 C&C 伺服器的 C&C 清單來源。
C&C 風險等級	顯示 C&C 伺服器的風險等級。
安全威脅類型	顯示受管理產品偵測到的特定類型安全威脅。
偵測嚴重性	顯示事件的嚴重性層級。
IP 位址 (關注的)	顯示目標端點 (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)	顯示與關注的 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	顯示符合同一彙整規則的記錄檔計數。
彙整的相符已歸類事件	顯示符合同一規則的已彙整記錄檔計數。
網路群組	顯示群組的名稱。

資料	說明
主機嚴重性	顯示主機嚴重性。
記錄 ID	顯示記錄 ID。
攻擊階段	顯示攻擊發生階段。
備註	顯示攻擊的相關說明。
C&C 伺服器	顯示 C&C 伺服器的名稱、URL 或 IP 位址。
C&C 伺服器類型	顯示伺服器類型。
寄件者	顯示傳輸起源所在的寄件者位址。
收件者	顯示傳輸的目標位址。
主旨	顯示包含 Web URL 的電子郵件訊息主旨行。

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。

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-45. 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	<p>顯示受可疑安全威脅影響的唯一電腦數目。</p> <p>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。</p> <p>唯一端點 = 2</p>
唯一來源	<p>顯示可疑安全威脅起源所在的唯一來源數目。</p> <p>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。</p> <p>唯一來源 = 3</p>
唯一收件者	<p>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。</p> <p>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。</p> <p>唯一收件者 = 2</p>
唯一寄件者	<p>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。</p> <p>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。</p> <p>唯一寄件者 = 3</p>
偵測	<p>顯示受管理產品偵測到的策略/規則違規總數。</p> <p>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。</p> <p>偵測數等於 10。</p>
緩和	<p>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。</p>
已清除的端點	<p>顯示 Trend Micro Threat Mitigator 清除的端點總數。</p>
清除端點率 (%)	<p>顯示 Trend Micro Threat Mitigator 清除的端點佔偵測總數的百分比。</p>

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-46. 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-47. 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-48. 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-49. 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-50. 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-51. 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	<p>顯示受可疑安全威脅影響的唯一電腦數目。</p> <p>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。</p> <p>唯一端點 = 2</p>
唯一來源	<p>顯示可疑安全威脅起源所在的唯一來源數目。</p> <p>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。</p> <p>唯一來源 = 3</p>
唯一收件者	<p>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。</p> <p>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。</p> <p>唯一收件者 = 2</p>
唯一寄件者	<p>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。</p> <p>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。</p> <p>唯一寄件者 = 3</p>
偵測	<p>顯示受管理產品偵測到的策略/規則違規總數。</p> <p>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。</p> <p>偵測數 = 10</p>

可疑安全威脅詳細資訊

提供有關您網路上可疑安全威脅的特定資訊。範例：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-52. 可疑安全威脅詳細資訊資料檢視

資料	說明
收到	顯示 Control Manager 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。
產品項目	顯示受管理產品的實體顯示名稱。 Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。
產品	顯示受管理產品的名稱。範例： OfficeScan 、 ScanMail for Microsoft Exchange
緩和主機	顯示緩和伺服器的主機名稱（網路病毒牆執行器或 Threat Mitigator ）
流量/連線	顯示網路流量的方向，或網路上可疑安全威脅起源所在的位置。
通訊協定群組	顯示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	顯示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
目標 IP 位址	顯示受可疑安全威脅影響之端點的 IP 位址。
目標主機	顯示受可疑安全威脅影響之端點的主機名稱。
目標通訊埠	顯示受可疑安全威脅影響之端點的通訊埠號碼。
目標 MAC 位址	顯示受可疑安全威脅影響之端點的 MAC 位址。
目標作業系統	顯示在目標主機上執行的作業系統。
目標使用者 <x>	顯示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>)	顯示登入時間戳記。 <x> 代表登入次數和特定的時間戳記。
來源 IP 位址	顯示可疑安全威脅起源所在的來源 IP 位址。
來源主機名稱	顯示可疑安全威脅起源所在的來源主機名稱。

資料	說明
來源通訊埠	顯示可疑安全威脅起源所在的來源通訊埠號碼。
來源 MAC 位址	顯示可疑安全威脅起源所在的來源 MAC 位址。
來源作業系統	顯示在目標來源主機上執行的作業系統。
來源使用者 <x>	顯示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>)	顯示在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	顯示可疑安全威脅起源所在的來源網域。
安全威脅類型	顯示受管理產品偵測到的特定類型安全威脅。 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	顯示可疑安全威脅所違反的策略/規則。
收件者	顯示可疑安全威脅的收件者。
寄件者	顯示可疑安全威脅的寄件者。
主旨	顯示包含間諜程式/可能的資安威脅程式的電子郵件的主旨行內容。
附件檔案名稱	顯示附件的檔案和副檔名名稱。
附件檔案類型	顯示附件的檔案類型。
附件 SHA-1	顯示附件的 SHA-1 雜湊。
URL	顯示視為可疑安全威脅的 URL。
使用者	顯示受管理產品偵測到可疑安全威脅時登入目標的使用者名稱。
IM/IRC 使用者	顯示 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	顯示可疑安全威脅起源所在的 Internet 瀏覽器或 FTP 端點。
檔案	顯示可疑檔案的名稱。
壓縮檔中的檔案	顯示可疑安全威脅是否源自壓縮檔。

資料	說明
封存檔 SHA-1	顯示封存檔的 SHA-1 雜湊。
封存檔檔案類型	顯示封存檔的類型。
共用資料夾	顯示可疑安全威脅是否源自共用資料夾。
SHA-1	顯示 SHA-1 雜湊。
緩和處理行動	顯示緩和伺服器對可疑安全威脅採取的處理行動。 範例：檔案已清除、檔案已丟棄、檔案已刪除
緩和結果	顯示緩和伺服器對可疑安全威脅採取的處理行動結果。
來源 IP 群組	顯示可疑安全威脅起源所在的來源 IP 位址群組。
來源網路區域	顯示可疑安全威脅起源所在的來源網路區域。
端點群組	顯示受可疑安全威脅影響之端點的 IP 位址群組。
端點網路區域	顯示受可疑安全威脅影響之端點的網路區域。
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
C&C 清單來源	其中包含回呼位址的清單名稱 <ul style="list-style-type: none"> 全球資訊（趨勢科技全球資訊網，包括主動式雲端截毒技術） 受管理產品中的沙盒虛擬平台 在受管理產品中設定的使用者定義 C&C 清單
C&C 風險等級	回呼的嚴重性等級
備註	顯示攻擊的相關說明。
C&C 伺服器	顯示 C&C 伺服器的名稱、URL 或 IP 位址。
C&C 伺服器類型	顯示伺服器類型。
惡意程式類型	顯示惡意程式類型。

緩和詳細資訊

提供有關緩和伺服器為解決您網路上安全威脅所執行之工作的特定資訊。

表 B-53. 緩和詳細資訊資料檢視

資料	說明
收到	顯示 Control Manager 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。
緩和實體	顯示緩和伺服器（網路病毒牆執行器或 Threat Mitigator ）的實體顯示名稱
產品	顯示受管理產品的名稱。範例： OfficeScan 、 ScanMail for Microsoft Exchange
端點 IP	顯示受安全威脅影響之端點的 IP 位址。
端點	顯示受安全威脅影響之端點的主機名稱。
資料來源	顯示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	顯示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	顯示緩和伺服器記錄的安全威脅相關事件。請參閱下列參考資料： 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	顯示安全威脅事件（依狀態群組）。請參閱下列參考資料： http://docs.trendmicro.com/all/ent/tms/v2.6/en-us/tmtm_2.6_olh/help/info/threat_event_logs.htm
緩和詳細資料	顯示安全威脅事件的詳細資料。請參閱下列參考資料： http://docs.trendmicro.com/all/ent/tms/v2.6/en-us/tmtm_2.6_olh/start.htm#help/info/mitigation_status.htm
偵測	顯示受管理產品偵測到的安全威脅總數。
詳細資訊	顯示安全威脅的詳細資料。

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-54. 關聯詳細資訊資料檢視

資料	說明
已產生	顯示受管理產品產生資料的時間。
IP 位址	顯示受可疑安全威脅影響之端點的 IP 位址。
網路群組	顯示受監控的網路群組。
通訊協定	顯示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。
安全威脅類型	顯示受管理產品偵測到的特定類型安全威脅。 範例：病毒、間諜程式/可能的資安威脅程式、詐騙
嚴重性	顯示主機嚴重性。
偵測	顯示偵測類型（根據關聯規則）
詳細資訊	顯示與偵測相關的備註或註解。
MAC 位址	顯示受可疑安全威脅影響之端點的 MAC 位址。
主機名稱	顯示受可疑安全威脅影響之端點的主機名稱。
關聯規則 ID	顯示規則 ID。

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

提供有關從網路偵測到的 C&C 回呼事件的特定資訊。

表 B-55. C&C 回呼詳細資訊資料檢視

資料	說明
收到	顯示 Control Manager 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。
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	包含 C&C 位址的清單之來源 <ul style="list-style-type: none"> • 全球資訊（趨勢科技全球資訊網，包括主動式雲端截毒技術） • 受管理產品中的分析器（沙盒虛擬平台和網路內容檢測引擎） • Control Manager 和受管理產品（例如 Deep Discovery Inspector）中所設定之使用者定義的 C&C 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
C&C 風險等級	<ul style="list-style-type: none"> • 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	顯示受管理產品的名稱。範例： OfficeScan 、 ScanMail for Microsoft Exchange
產品項目	顯示受管理產品的實體顯示名稱。 Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。

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-56. 可疑檔案詳細資訊資料檢視

資料	說明
收到	顯示 Control Manager 從受管理產品收到資料的時間。
已偵測	顯示受管理產品偵測到可疑物件的時間
端點	發現可疑物件所在的端點。
產品	顯示受管理產品的名稱。範例： OfficeScan 、 ScanMail for Microsoft Exchange
產品項目	顯示受管理產品的實體顯示名稱。 Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。
端點 IP 位址	端點 IP 位址
端點主機名稱	端點的主機名稱
檔案類型	可疑物件的檔案類型
檔案 SHA-1	可疑物件的 SHA-1 雜湊值
檔案路徑	可疑物件的檔案路徑和名稱
C&C 清單來源	包含 C&C 位址的清單之來源 <ul style="list-style-type: none"> 全球資訊（趨勢科技全球資訊網，包括主動式雲端截毒技術） 受管理產品（沙盒虛擬平台或網路內容檢測引擎關聯規則）中的分析器 Control Manager 和受管理產品（例如 Deep Discovery Inspector）中所設定之使用者定義的 C&C 清單
處理行動	解決可疑物件的處理行動
掃描類型	偵測可疑物件的掃描類型
已建立	顯示在端點中建立可疑物件的時間
已修改	顯示在端點中修改可疑物件的時間

Machine Learning 詳細資訊

此資料檢視提供有關 Machine Learning 偵測到的進階未知安全威脅的特定資訊。

表 B-57. Machine Learning 詳細資訊

資料	說明
偵測時間	顯示 Machine Learning 偵測到安全威脅的時間
收到	顯示 Control Manager 從受管理產品收到資料的時間
產品實體/端點	顯示下列其中一項： <ul style="list-style-type: none"> 受管理產品的實體顯示名稱 已安裝用戶端（例如 OfficeScan 用戶端）之端點的 IP 位址或主機名稱
產品/端點 IP	顯示下列其中一項： <ul style="list-style-type: none"> 受管理產品伺服器的 IP 位址 已安裝用戶端的端點 IP 位址
產品	顯示受管理產品的名稱
伺服器	顯示受管理產品伺服器的主機名稱
可能的安全威脅類型	指出 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	Machine Learning 引擎判斷出的安全威脅名稱
登入使用者	顯示受管理產品偵測到安全威脅時已登入端點的使用者名稱
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	顯示所偵測到物件的檔案建立時間
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

資料	說明
程序擁有者	顯示與所偵測到程序關聯的使用者名稱
端點感染通道	安全威脅源自的通道
感染來源	顯示安全威脅的來源
安全威脅可能性	指出檔案/程序符合惡意程式模型的程度
處理行動結果	採取處理行動的結果
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

沙盒虛擬平台偵測資訊

此資料檢視提供有關沙盒虛擬平台偵測到的進階未知安全威脅的特定資訊。

表 B-58. 沙盒虛擬平台偵測資訊

資料	說明
已產生	顯示受管理產品偵測到安全威脅的時間
收到	顯示 Control Manager 從受管理產品收到資料的時間
產品	顯示受管理產品的名稱
伺服器名稱	顯示伺服器的名稱
主機	顯示主機的名稱
項目通道	顯示感染通道
來源	顯示安全威脅的來源
目標	顯示安全威脅的目標位置

資料	說明
程序名稱	觸發偵測的程序名稱
SHA1	觸發偵測的檔案 SHA-1 雜湊
類型	顯示觸發偵測的物件類型（「檔案」或「程序」）
檔案名稱	顯示觸發偵測的檔案名稱
檔案類型	顯示觸發偵測的檔案類型
URL	顯示觸發偵測的 URL
提交規則	顯示沙盒虛擬平台所提交的規則
提交時間	顯示沙盒虛擬平台提交規則的時間
完成時間	顯示沙盒虛擬平台完成分析的時間
安全威脅	沙盒虛擬平台所判斷出的安全威脅名稱
風險等級	顯示沙盒虛擬平台指派的風險等級
安全威脅類別	顯示安全威脅類型
最嚴重的安全威脅	表示依嚴重性等級排名之最嚴重的安全威脅

沙盒虛擬平台可疑物件影響詳細資訊

此資料檢視提供有關沙盒虛擬平台可疑物件之影響的詳細資訊。

資料	說明
類型	偵測到的可疑物件的安全威脅類型
物件	偵測到的可疑物件的類型
中毒處理行動	偵測到可疑物件的受管理產品所採取的中毒處理行動
風險等級	偵測到的可疑物件的風險等級
到期	為可疑物件設定的到期時間

資料	說明
第一次提交時間	受管理產品第一次將可疑物件提交到沙盒虛擬平台的時間
第一次提交產品名稱	第一次將可疑物件提交到沙盒虛擬平台的受管理產品
第一次提交主機名稱	第一次將可疑物件提交到沙盒虛擬平台的受管理伺服器的主機名稱
第一次提交 IP 位址	第一次將可疑物件提交到沙盒虛擬平台的受管理伺服器的 IP 位址
第一次提交檔案名稱	受管理產品第一次提交到沙盒虛擬平台的可疑物件的檔案名稱
第一次提交來源	受管理產品第一次提交到沙盒虛擬平台的可疑物件的來源
第一次提交目標	受管理產品第一次提交到沙盒虛擬平台的可疑物件的目標
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盒虛擬平台的時間
最近一次提交產品名稱	最近一次將可疑物件提交到沙盒虛擬平台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盒虛擬平台的受管理產品的主機名稱
最近一次提交 IP 位址	最近一次將可疑物件提交到沙盒虛擬平台的受管理伺服器的 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盒虛擬平台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盒虛擬平台的可疑物件的檔案類型
最近一次提交來源	受管理產品最近一次提交到沙盒虛擬平台的可疑物件的來源
最近一次提交目標	受管理產品最近一次提交到沙盒虛擬平台的可疑物件的目標
端點網域名稱	觸發偵測的端點網域名稱
端點主機名稱	觸發偵測的端點主機名稱
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	登入觸發偵測的端點的使用者名稱

資料	說明
端點 IP 位址	觸發偵測的端點 IP 位址
端點第一次發現時間	在端點上第一次偵測到可疑物件的時間
端點第一個產品偵測	受管理產品在端點上第一次偵測到可疑物件的時間
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時間
端點上一個產品偵測	受管理產品在端點上最近一次偵測到可疑物件的時間
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

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-59. 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。

資料	說明
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：OfficeScan 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：OfficeScan 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：OfficeScan 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-60. 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：OfficeScan、ScanMail for Microsoft Exchange

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
唯一端點	顯示受安全威脅/違規影響的唯一電腦數目。 範例：OfficeScan 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：OfficeScan 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：OfficeScan 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-61. 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：OfficeScan、ScanMail for Microsoft Exchange

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：OfficeScan 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：OfficeScan 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：OfficeScan 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-62. 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。

資料	說明
偵測	顯示受管理產品偵測到的安全威脅/違規總數。 範例：OfficeScan 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-63. 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。
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：OfficeScan 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。

Data Loss Prevention 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

此資料檢視提供有關 Data Loss Prevention (DLP) 事件的資訊。

表 B-64. DLP 事件資訊

資料	說明
收到	顯示 Control Manager 收到記錄檔的時間
已產生	顯示在受管理產品中產生記錄檔資料的時間
事件 ID	顯示事件的識別碼
嚴重性	顯示事件的嚴重性等級
狀態	顯示事件的偵測狀態
管理員	顯示部門的管理員名稱
部門	顯示部門名稱
策略	顯示已違反的策略
產品實體/端點	此資料欄顯示下列其中一項： <ul style="list-style-type: none"> 受管理產品的實體顯示名稱。Control Manager 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 OfficeScan 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：OfficeScan、ScanMail for Microsoft Exchange
產品/端點 IP	此資料欄顯示下列其中一項： <ul style="list-style-type: none"> 安裝了受管理產品的伺服器 IP 位址 已安裝用戶端（例如 OfficeScan 用戶端）的電腦 IP 位址

資料	說明
產品/端點 MAC	此資料欄顯示下列其中一項： <ul style="list-style-type: none"> 安裝了受管理產品的伺服器 MAC 位址 已安裝用戶端（例如 OfficeScan 用戶端）的電腦 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。Control Manager 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 OfficeScan 用戶端）的電腦 IP 位址或主機名稱
事件來源 (AD 顯示名稱)	顯示事件來源的 Active Directory 顯示名稱
事件來源 (AD 帳號)	顯示事件來源的 Active Directory 帳號名稱
事件來源 (寄件者)	顯示來源電子郵件信箱
網站	顯示觸發事件的網站 URL
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
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
檔案/資料大小	顯示觸發事件的檔案大小或資料大小
規則	顯示事件所觸發的規則名稱
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
目標	顯示目標
處理行動	顯示對事件採取的處理行動
事件	顯示事件數目
雲端服務供應商	顯示雲端服務供應商的名稱

DLP 範本相符項目資訊

表 B-65. 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： <ul style="list-style-type: none"> 受管理產品的實體顯示名稱。Control Manager 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 OfficeScan 用戶端）的電腦 IP 位址或主機名稱。
產品	顯示受管理產品的名稱。範例：OfficeScan、ScanMail for Microsoft Exchange
產品/端點 IP	此資料欄顯示下列其中一項： <ul style="list-style-type: none"> 安裝了受管理產品的伺服器 IP 位址。 已安裝用戶端（例如 OfficeScan 用戶端）的電腦 IP 位址。
產品/端點 MAC	此資料欄顯示下列其中一項： <ul style="list-style-type: none"> 安裝了受管理產品的伺服器 MAC 位址。 已安裝用戶端（例如 OfficeScan 用戶端）的電腦 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。Control Manager 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 OfficeScan 用戶端）的電腦 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。

資料發現資訊

顯示資料發現資訊的相關資訊。

資料發現 Data Loss Prevention 偵測資訊

表 B-66. 資料發現 Data Loss Prevention 偵測資訊

資料	說明
收到	顯示 Control Manager 收到記錄檔的時間。
已產生	顯示受管理產品產生記錄檔資料的時間。
規則	顯示由事件觸發的規則名稱。
端點	顯示 Data Loss Prevention 偵測到傳輸的電腦的 IP 位址或主機名稱。
網域	顯示受管理產品所屬的網域。
使用者	顯示開始執行活動的使用者名稱。
使用者網域	顯示使用者所屬的網域名稱。
檔案路徑	顯示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	顯示完整檔案名稱。

資料	說明
範本	顯示事件觸發的確切規則名稱和範本。
處理行動	顯示對傳輸採取的處理行動。
詳細資訊	顯示其他資訊，例如，使用者為了繼續傳輸機密資料所提供的理由。

資料發現端點資訊

表 B-67. 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 Data Loss Prevention 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。

資料檢視：產品資訊

顯示 **Control Manager**、受管理的產品、元件及使用授權的相關資訊。

使用授權資訊

顯示有關 **Control Manager** 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-68. 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。Control Manager 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：OfficeScan、ScanMail for Microsoft Exchange
產品版本	顯示受管理產品的版本號碼。範例：OfficeScan - 10.0、Control Manager - 5.0
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。

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-69. 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。

資料	說明
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。

產品使用授權詳細資訊

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資訊。範例：受管理產品資訊、試用版或完整版產品、使用授權到期日

表 B-70. 產品使用授權詳細資訊資料檢視

資料	說明
產品項目	顯示受管理產品的實體顯示名稱。 Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。
產品	顯示受管理產品的名稱。範例：OfficeScan、ScanMail for Microsoft Exchange
產品版本	顯示受管理產品的版本號碼。範例：OfficeScan- 10.0、Control Manager- 5.0
受管理服务	顯示受管理服務的名稱。範例：網站信譽評等服務
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
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
啟動碼	顯示受管理產品的啟動碼。
使用授權到期日	顯示受管理產品的使用授權到期日。

資料	說明
授權數目	顯示啟動碼允許的授權數目。
說明	顯示啟動碼的說明。

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。

產品發佈摘要

顯示有關已註冊於 Control Manager 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-71. 產品發佈摘要資料檢視

資料	說明
已向 Control Manager 註冊	顯示受管理產品註冊所在的 Control Manager 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：OfficeScan、ScanMail for Microsoft Exchange
產品版本	顯示受管理產品的版本號碼。範例：OfficeScan- 10.0、Control Manager- 5.0
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。

產品狀態資訊

顯示有關已註冊於 Control Manager 之受管理產品的詳細資訊。範例：受管理產品版本和 Build 號碼、作業系統

表 B-72. 產品狀態資訊資料檢視

資料	說明
產品實體/端點	此資料欄顯示下列其中一項： <ul style="list-style-type: none"> 受管理產品的實體顯示名稱。Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。 已安裝用戶端（例如 OfficeScan 用戶端）的電腦 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： <ul style="list-style-type: none"> 安裝了受管理產品的伺服器主機名稱。 已安裝用戶端（例如 OfficeScan 用戶端）的電腦主機名稱。
產品/端點 IP	此資料欄顯示下列其中一項： <ul style="list-style-type: none"> 安裝了受管理產品的伺服器 IP 位址。 已安裝用戶端（例如 OfficeScan 用戶端）的電腦 IP 位址。
產品/端點 MAC	此資料欄顯示下列其中一項： <ul style="list-style-type: none"> 安裝了受管理產品的伺服器 MAC 位址。 已安裝用戶端（例如 OfficeScan 用戶端）的電腦 MAC 位址。
管理 Control Manager 實體	顯示 Control Manager 伺服器（受管理產品會向此伺服器註冊）的實體顯示名稱。
管理伺服器實體	顯示受管理產品（端點會向此產品註冊）的實體顯示名稱。Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。
網域	顯示受管理產品所屬的網域。

資料	說明
連線狀態	此資料欄顯示下列其中一項： <ul style="list-style-type: none"> 受管理產品與 Control Manager 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 (OfficeScan) 的連線狀態。範例：正常、異常、離線
特徵碼狀態	顯示受管理產品或具有用戶端（例如 OfficeScan 用戶端）的電腦所使用的特徵碼檔案/規則的狀態。範例：最新、過期
引擎狀態	顯示受管理產品或具有用戶端（例如 OfficeScan 用戶端）的電腦所使用的掃描引擎的狀態。範例：最新、過期
產品	顯示受管理產品的名稱。範例： OfficeScan 、 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： OfficeScan- 10.0 、 Control Manager- 5.0
產品 Build	顯示受管理產品的 Build 號碼。此資訊顯示在產品的「關於」畫面上。範例：版本： 5.0 (Build 1219)
產品角色	顯示受管理產品或裝有用戶端（例如 OfficeScan 用戶端）的電腦在網路環境中的角色。範例：伺服器
作業系統	顯示安裝了受管理產品/用戶端的電腦作業系統。
作業系統版本	顯示安裝了受管理產品/用戶端的電腦作業系統版本號碼。
作業系統 Service Pack	顯示安裝了受管理產品/用戶端的電腦作業系統 Service Pack 號碼。
更新代理程式	如果代理程式為「更新代理程式」
上次預約掃描	上次預約掃描的日期和時間
上次手動掃描	上次手動掃描的日期和時間
上次立即掃描	上次立即掃描的日期和時間
即時掃描	如果即時掃描已啟動
防火牆	如果防火牆已啟動

資料	說明
特徵碼/規則部署狀態	顯示特徵碼/規則的部署狀態
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	顯示掃描引擎部署狀態
引擎部署	掃描引擎部署的日期和時間
使用者	顯示上次登入受管理產品伺服器端點的使用者名稱

產品事件資訊

顯示受管理產品事件的相關資訊。範例：向 Control Manager 註冊的受管理產品、元件更新、啟動碼部署

表 B-73. 產品事件資訊資料檢視

資料	說明
收到	顯示 Control Manager 接收受管理產品事件相關資料的時間。
已產生	顯示受管理產品產生事件相關資料的時間。
產品項目	顯示受管理產品的實體顯示名稱。Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。
產品	顯示受管理產品的名稱。範例：OfficeScan、ScanMail for Microsoft Exchange
產品版本	顯示受管理產品的版本號碼。範例：OfficeScan- 10.0、Control Manager- 5.0
事件嚴重性	顯示事件的嚴重性。範例：資訊、嚴重、警告
事件類型	顯示發生的事件類型。範例：發現下載型病毒、檔案封鎖、還原
指令狀態	顯示指令的狀態。範例：成功、未成功、進行中
說明	顯示受管理產品針對事件提供的說明。

產品稽核事件記錄檔

顯示與受管理產品相關的稽核資訊。例如，稽核管理主控台存取。

表 B-74. 產品稽核事件記錄檔資料檢視

資料	說明
收到	顯示 Control Manager 接收受管理產品事件相關資料的時間。
已產生	顯示受管理產品產生事件相關資料的時間。
主機	顯示下列其中一項： <ul style="list-style-type: none"> 安裝了受管理產品的伺服器主機名稱。 顯示已安裝引擎（例如 OfficeScan 用戶端）的電腦主機名稱。
使用者	顯示帳號資訊。
事件類別	顯示所發生事件的類別。範例：管理主控台存取
事件層級	顯示事件的嚴重性。
事件說明	顯示受管理產品針對事件提供的說明。

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。

引擎狀態

顯示有關受管理產品使用的掃描引擎的詳細資訊。範例：掃描引擎名稱、最新的掃描引擎部署時間，以及哪些受管理產品使用該掃描引擎

表 B-75. 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： <ul style="list-style-type: none"> 受管理產品的實體顯示名稱。Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。 已安裝用戶端（例如 OfficeScan 用戶端）的電腦 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： <ul style="list-style-type: none"> 安裝了受管理產品的伺服器主機名稱。 已安裝用戶端（例如 OfficeScan 用戶端）的電腦 IP 位址。
產品/端點 IP	此資料欄顯示下列其中一項： <ul style="list-style-type: none"> 安裝了受管理產品的伺服器 IP 位址。 已安裝用戶端（例如 OfficeScan 用戶端）的電腦 IP 位址。
連線狀態	此資料欄顯示下列其中一項： <ul style="list-style-type: none"> 受管理產品與 Control Manager 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 (OfficeScan) 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： OfficeScan 、 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： OfficeScan- 10.0 、 Control Manager- 5.0
產品角色	顯示受管理產品或裝有用戶端（例如 OfficeScan 用戶端）的電腦在網路環境中的角色。範例：伺服器
引擎	顯示掃描引擎的名稱。範例：垃圾郵件防護引擎 (Windows)、病毒掃描引擎 IA 64 位元掃描引擎
引擎版本	顯示掃描引擎的版本。範例：垃圾郵件防護引擎 (Windows)： 3.000.1153 、病毒掃描引擎 IA 64 位元掃描引擎： 8.000.1008
引擎狀態	顯示掃描引擎的目前狀態。範例：最新、過期

資料	說明
引擎已更新	顯示最新掃描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-76. 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： <ul style="list-style-type: none"> 受管理產品的實體顯示名稱。Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。 已安裝用戶端（例如 OfficeScan 用戶端）的電腦 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： <ul style="list-style-type: none"> 安裝了受管理產品的伺服器主機名稱。 已安裝用戶端（例如 OfficeScan 用戶端）的電腦 IP 位址。
產品/端點 IP	此資料欄顯示下列其中一項： <ul style="list-style-type: none"> 安裝了受管理產品的伺服器 IP 位址。 已安裝用戶端（例如 OfficeScan 用戶端）的電腦 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： <ul style="list-style-type: none"> 受管理產品與 Control Manager 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 (OfficeScan) 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： OfficeScan 、 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： OfficeScan- 10.0 、 Control Manager- 5.0
產品角色	顯示受管理產品或裝有用戶端（例如 OfficeScan 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。
OfficeScan 網域階層	顯示 OfficeScan 網域階層的路徑。

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，以及掃描引擎部署狀態

表 B-77. 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。 Control Manager 會使用受管理產品的實體顯示名稱來識別受管理產品。

資料	說明
產品	顯示受管理產品的名稱。範例：OfficeScan、ScanMail for Microsoft Exchange
產品版本	顯示受管理產品的版本號碼。範例：OfficeScan- 10.0、Control Manager- 5.0
連線狀態	顯示受管理產品與 Control Manager 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	顯示掃描引擎的目前狀態。範例：最新、過期
引擎部署狀態	顯示最新掃描更新的部署狀態。範例：成功、未成功、進行中
引擎部署	顯示最新掃描引擎部署到受管理產品或端點的時間。

掃描引擎狀態摘要

顯示有關受管理產品使用的掃描引擎的摘要資訊。範例：掃描引擎名稱、掃描引擎比率以及過期掃描引擎數目

表 B-78. 引擎狀態摘要資料檢視

資料	說明
引擎	顯示掃描引擎的名稱。範例：垃圾郵件防護引擎 (Windows)、病毒掃描引擎 IA 64 位元掃描引擎
版本	顯示掃描引擎的版本。範例：垃圾郵件防護引擎 (Windows)：3.000.1153、病毒掃描引擎 IA 64 位元掃描引擎：8.000.1008
最新	顯示具有最新掃描引擎的受管理產品數目。
過期	顯示具有過期掃描引擎的受管理產品數目。

資料	說明
更新率 (%)	顯示具有最新掃描引擎的受管理產品百分比。這包括會傳回「無」做為值的掃描引擎。

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-79. 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
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

資料	說明
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

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/掃描引擎的摘要資訊。

表 B-80. 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의網域名稱。
端點	顯示已安裝用戶端（例如 OfficeScan 用戶端）的電腦主機名稱。
特徵碼過期	顯示具有過期特徵碼檔案的受管理產品數目。
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	顯示具有過期掃描引擎的受管理產品數目。
引擎更新率 (%)	顯示具有最新掃描引擎的受管理產品百分比。這包括會傳回 n/a 做為值的掃描引擎。

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-81. 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

資料	說明
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

Control Manager 資訊

顯示 Control Manager 使用者存取、指令追蹤資訊及 Control Manager 伺服器事件的相關資訊。

使用者存取資訊

此資料檢視會顯示 Control Manager 使用者存取，以及使用者登入 Control Manager 期間所執行的活動。

表 B-82. 使用者存取資訊資料檢視

資料	說明
日期/時間	顯示活動開始的時間
使用者	顯示起始活動的使用者名稱
Active Directory 群組	顯示 Active Directory 群組的名稱
使用者角色	顯示指派給此帳號的 Control Manager 使用者角色名稱
帳號類型	顯示 Control Manager 管理員指派給使用者的帳號類型。例如： Root 、進階使用者或操作員
帳號類型說明	顯示帳號類型的說明。對於預設帳號類型，此說明來自 Control Manager，對於自訂帳號類型，此說明來自使用者定義的說明

資料	說明
活動	顯示使用者對 Control Manager 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	顯示活動的結果
說明	顯示活動的說明（如果有說明的話）

Control Manager 事件資訊

顯示與 Control Manager 伺服器事件相關的資訊。範例：向 Control Manager 註冊的受管理產品、元件更新、啟動碼部署

表 B-83. Control Manager 事件資訊資料檢視

資料	說明
日期/時間	顯示事件發生的時間。
事件類型	顯示發生的事件類型。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	顯示事件的結果。範例：成功、未成功
說明	顯示活動的說明（如果有的話）。

指令追蹤資訊

顯示 Control Manager 傳送給受管理產品之指令的相關資訊。範例：向 Control Manager 註冊的受管理產品、元件更新、啟動碼部署

表 B-84. 指令追蹤資訊資料檢視

資料	說明
日期/時間	顯示指令發出者發出指令的時間。
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

資料	說明
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
使用者	顯示發出指令的使用者。
狀態更新	顯示對所選 Control Manager 的所有指令執行最新狀態檢查的時間。
成功	顯示成功的指令數目。
未成功	顯示不成功的指令數目。
進行中	顯示仍在進行中的指令數目。
全部	顯示指令的總數（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 **Control Manager** 註冊的受管理產品、元件更新、啟動碼部署

表 B-85. 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 Control Manager 的所有指令執行最新狀態檢查的時間。

資料	說明
結果詳細資料說明	顯示 Control Manager 為事件提供的說明。

附錄 C

Token 變數

本節說明 Control Manager 支援的可用於自訂事件通知訊息的 Token 變數。
包含下列主題：

- [關於 Token 變數 第 C-2 頁](#)
- [標準 Token 變數 第 C-3 頁](#)
- [進階安全威脅活動 Token 變數 第 C-3 頁](#)
- [C&C 回呼 Token 變數 第 C-4 頁](#)
- [內容策略違規 Token 變數 第 C-5 頁](#)
- [Web 存取安全違規 Token 變數 第 C-5 頁](#)
- [Data Loss Prevention Token 變數 第 C-6 頁](#)
- [已知的安全威脅活動 Token 變數 第 C-8 頁](#)
- [網路存取控制 Token 變數 第 C-10 頁](#)

關於 Token 變數

使用 Token 變數，代表「主旨」和「訊息」欄位中的資料來自訂事件通知。

Control Manager 支援下列事件通知的 Token 變數。

事件類別	說明
標準版	套用至所有事件通知的 Token 變數 如需詳細資訊，請參閱 標準 Token 變數 第 C-3 頁 。
進階安全威脅活動	套用至「進階安全威脅活動」事件通知的 Token 變數 如需詳細資訊，請參閱 進階安全威脅活動 Token 變數 第 C-3 頁 。
C&C 回呼	套用至「C&C 回呼」事件通知的 Token 變數 如需詳細資訊，請參閱 C&C 回呼 Token 變數 第 C-4 頁 。
內容策略違規	套用至「C&C 回呼」事件通知的 Token 變數 如需詳細資訊，請參閱 內容策略違規 Token 變數 第 C-5 頁 。
Web 存取安全	套用至「Web 存取安全」事件通知的 Token 變數 如需詳細資訊，請參閱 Web 存取安全違規 Token 變數 第 C-5 頁 。
Data Loss Prevention	套用至 Data Loss Prevention 事件通知的 Token 變數 如需詳細資訊，請參閱 Data Loss Prevention Token 變數 第 C-6 頁 。
已知的安全威脅活動	套用至「已知的安全威脅活動」事件通知的 Token 變數 如需詳細資訊，請參閱 已知的安全威脅活動 Token 變數 第 C-8 頁 。
網路存取控制	套用至「網路存取控制」事件通知的 Token 變數 如需詳細資訊，請參閱 網路存取控制 Token 變數 第 C-10 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。

變數	說明
%cmserver%	Control Manager 伺服器名稱
%computer%	偵測到事件發生所在電腦的網路名稱
%entity%	事件發生所在的受管理產品的「產品目錄」路徑
%event%	觸發通知的事件
%pname%	受管理產品名稱
%pver%	受管理產品版本
%time%	事件發生的時間 (hh: mm)
%vloginuser%	間諜程式記錄檔中自訂事件的登入使用者資訊
%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

進階安全威脅活動 Token 變數

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%	<p>根據傳輸方向，%hostIP% 是由 Deep Discovery Inspector 決定的 IP 位址：</p> <ul style="list-style-type: none"> 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%	開始時間
%END_TIME%	<p>結束時間</p> <p>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，Control Manager 會計算這些記錄檔。如果符合警訊條件，Control Manager 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。</p>
%detections%	<p>偵測數目</p> <p>例如：</p> <p>事件：高風險沙盒虛擬平台偵測</p> <p>IP 位址：%hostIP%</p> <p>主機名稱：%computer%</p> <p>群組：%group%</p> <p>時間範圍：%START_TIME% - %END_TIME%</p> <p>偵測：%detections%</p>

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。

變數	說明
%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
%CnC_LIST_SRC%	其中包含回呼位址的清單名稱
%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。

變數	說明
%subject%	電子郵件通知的主目標頭
%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

Web 存取安全違規 Token 變數

下表說明用於自訂 Web 存取安全違規事件通知訊息的 Token 變數。

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

Data Loss Prevention Token 變數

變數	說明
DLP 變數： 由「預約事件摘要」和「事件詳細資料已更新」事件使用	
%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
%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

變數	說明
%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_ALLOW_NUM%	由所有受管理的使用者觸發的低嚴重性事件總數
%DLP_INCIDENT_ALINFO_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%	Control Manager 策略名稱 <div style="border: 1px solid black; padding: 5px; margin: 5px 0;">  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，Control Manager 策略名稱會顯示為「無」。 </div>
%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_NUMBER%	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

變數	說明
%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

變數	說明
病毒變數：由警訊或病毒爆發防範服務事件通知所使用	
%device_ip%	中毒端點的 IP 位址
%egnver%	<ul style="list-style-type: none"> 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」。
%ptnver%	<ul style="list-style-type: none"> 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」。

變數	說明
%scanmethod%	特定病毒處理行動的掃描方法。此 Token 僅適用於下列警訊： <ul style="list-style-type: none"> • 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%	<ul style="list-style-type: none"> • 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%	<ul style="list-style-type: none"> • 病毒計數。 • 由病毒爆發警訊所使用。
%vdest%	<ul style="list-style-type: none"> • 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%	<ul style="list-style-type: none"> • 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。

變數	說明
特殊變數：由網路病毒牆執行器已完成工作相關事件所使用	
%action%	網路病毒牆執行器對網路病毒的處理行動（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。

附錄 D

IPv6 支援

本附錄包含有關 Control Manager 中 IPv6 支援範圍的資訊。
包含下列主題：

- [Control Manager 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](#)

Control Manager 伺服器需求

在 Control Manager 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	Control Manager 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	Control Manager 不支援包含 % 字元的 IPv6 伺服器位址。
Control Manager 報告	下列靜態報告不支援 IPv6 位址： <ul style="list-style-type: none"> 策略違規報告 服務違規報告
Control Manager 功能	下列功能不支援 IPv6 位址： <ul style="list-style-type: none"> 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。

- Control Manager 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
```

- Control Manager 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 Control Manager 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，Control Manager 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 Control Manager 支援的管理資訊庫 (MIB) 檔案。
包含下列主題：

- [使用 Control Manager MIB 檔案 第 E-2 頁](#)
- [使用 NVW Enforcer SNMPv2 MIB 檔案 第 E-2 頁](#)

使用 Control Manager MIB 檔案

從下列連結下載 Control Manager 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/cm2_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 Control Manager 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 Data Loss Prevention 記錄檔 第 F-3 頁
- CEF 行為監控記錄檔 第 F-9 頁
- CEF 裝置存取控制記錄檔 第 F-14 頁
- CEF 引擎更新狀態記錄檔 第 F-20 頁
- CEF Machine Learning 記錄檔 第 F-22 頁
- CEF 特徵碼更新狀態記錄檔 第 F-26 頁
- CEF 內容安全記錄檔 第 F-28 頁
- CEF 間諜程式/可能的資安威脅程式記錄檔 第 F-32 頁
- CEF 病毒/惡意程式記錄檔 第 F-40 頁
- CEF Web 網頁安全記錄檔 第 F-44 頁
- CEF C&C 回呼記錄檔 第 F-55 頁
- CEF 可疑檔案記錄檔 第 F-59 頁

- [CEF 網路內容檢測記錄檔 第 F-61 頁](#)

CEF Data Loss Prevention 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	Control Manager
標頭 (pver)	裝置版本	7.0
標頭 (eventid)	事件 ID	700106
標頭 (eventName)	記錄檔名稱	Data Loss Prevention
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	記錄檔產生時間 (UTC)	範例：2017 年 2 月 14 日 11:14:08 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

CEF 索引鍵	說明	值
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
filepath	檔案路徑	範例：D:\\Windows Live Mail\\Storage Folders\\Imported Folder52\\Local Folders\\Sent Items\\Archive Aft de1\\Clients,Adv22b\\
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：PSG 策略
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-7 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-5 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

CEF 索引鍵	說明	值
cs3	端點主機名稱	範例：Sample_OSCE
dvchost	伺服器主機名稱	範例：localhost
deviceFacility	產品名稱	範例：OfficeScan

記錄檔範例：

```
CEF:0|Trend Micro|Control Manager|7.0|700106|Data Loss Prevention|3|cs3Label=Product_Entity/Endpoint cs3=Sample_OSCE 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=PSG Policy cn3Label=Channel cn3=0 cn2Label=Action c
n2=4 deviceFacility=OfficeScan
```

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

值	說明
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
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

值	說明
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
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

值	說明
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)
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)

值	說明
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 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)	裝置供應商	Trend Micro
標頭 (pname)	裝置產品	Control Manager
標頭 (pver)	裝置版本	7.0
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
rt	記錄檔產生時間 (UTC)	範例：2017 年 2 月 14 日 11:14:08 GMT+00:00
dvchost	主機名稱	範例：localhost
cn1Label	cn1 欄位的對應標籤	風險等級

CEF 索引鍵	說明	值
cn1	風險等級	<ul style="list-style-type: none"> • 0：低 • 1：高
cs2Label	cs2 欄位的對應標籤	策略識別碼
cs2	策略識別碼	<ul style="list-style-type: none"> • 0：遭到入侵的可執行檔 • 1：新增啟動程式 • 2：主機檔案的修改 • 3：程式庫植入 • 4：新增 Internet Explorer 嵌入程式 • 5：Internet Explorer 設定的修改 • 6：Shell 的修改 • 7：新增服務 • 8：安全策略的修改 • 9：防火牆策略的修改 • 10：系統檔案的修改 • 11：重複的系統檔案 • 13：分層服務提供者 • 14：系統程序的修改 • 16：可疑行為 • 100：新發現的程式 • 200：未經授權的檔案加密 • 1000：安全威脅行為分析 • 9999：使用者定義的策略
sproc	Aegis 主體	範例：C:\\Windows\\ \\SysWOW64\\rundll32.exe

CEF 索引鍵	說明	值
cn2Label	cn2 欄位的對應標籤	事件類型
cn2	事件類型	<ul style="list-style-type: none"> • 1：程序 • 2：處理影像 • 4：登錄 • 8：檔案系統 • 16：驅動程式 • 32：SDT • 64：系統 API • 128：使用者模式 • 2048：弱點攻擊 • 65535：全部
cs1Label	cs1 欄位的對應標籤	目標
cs1	目標主機	範例：HKCU\Software\Microsoft\Windows\CurrentVersion\Run\COM+

CEF 索引鍵	說明	值
act	轉譯的處理行動	<ul style="list-style-type: none"> • 0：允許 • 1：詢問 • 2：拒絕 • 3：終止 • 4：唯讀 • 5：唯讀/唯寫 • 6：唯讀/僅能執行 • 7：反饋 • 8：清除 • 1002：未知 • 1003：評估 • 1004：已終止。檔案已還原。 • 1005：已終止。有些檔案未還原。 • 1006：已終止。檔案未還原。 • 1007：已終止。重新啟動結果：檔案已還原。 • 1008：已終止。重新啟動結果：有些檔案未還原。 • 1009：已終止。重新啟動結果：檔案未還原。
cn3Label	cn3 欄位的對應標籤	TranslatedAegisOperation

CEF 索引鍵	說明	值
cn3	轉譯的 Aegis 物件的作業	<ul style="list-style-type: none"> • 101：建立程序 • 102：開啟 • 103：終止 • 104：終止 • 301：刪除 • 302：寫入 • 303：存取 • 401：建立檔案 • 402：關閉 • 403：執行 • 501：啟動 • 601：弱點攻擊 • 9999：未處理的作業
shost	來源主機（端點）	範例：shost1
src	來源主機 IP 位址	範例："10.0.147.105"
deviceFacility	產品	範例：OfficeScan

記錄檔範例：

```
CEF:0|Trend Micro|Control Manager|7.0|BM:1000|Behavior Monitoring|3|rt=Aug 16 2017 05:00:40 GMT+00:00 dvchost=localhost
cn1Label=Risk_Level cn1=1 cs2Label=Policy cs2=1000 sproc=C:\
\Windows\SysWOW64\rundll32.exe cn2Label=Event_Type cn2=4 c
s1Label=Target cs1=HKCU\Software\Microsoft\Windows\Curre
ntVersion\Run\COM+ act=3 cn3Label=Operation cn3=302 shost=
shost1 src=10.0.76.40 deviceFacility=OfficeScan
```

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	Control Manager
標頭 (pver)	裝置版本	7.0
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	記錄檔產生時間 (UTC)	範例：2017 年 2 月 14 日 11:14:08 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_OSCE
shost	來源主機名稱	範例：shost1
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：OfficeScan 如需詳細資訊，請參閱 產品識別碼對應資料表 第 F-15 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	裝置類型

CEF 索引鍵	說明	值
cn2	裝置類型	範例：0 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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：OfficeScan

記錄檔範例：

```
CEF:0|Trend Micro|Control Manager|7.0|700107|Device Access C
ontrol|3|rt=Aug 16 2017 04:49:15 GMT+00:00 cs1Label=Product_
Entity/Endpoint cs1=Sample_OSCE 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=OfficeScan
```

產品識別碼對應資料表

值	說明
0	未知產品

値	説明
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
14	PC-cillin 企業版
15	OfficeScan
16	OfficeScan for Microsoft SBS
18	ServerProtect for Windows
19	ServerProtect for Windows (SOHO)
20	Control Manager 伺服器
21	通用
22	InterScan VirusWall for Unix
23	InterScan VirusWall for Windows
24	MOCA

值	說明
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)
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

值	說明
51	ServerProtect for Linux
52	ServerProtect for EMC
53	ServerProtect for NetApp
56	Control Manager 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	弱點評估
71	網路病毒牆執行器 1200
72	網路病毒牆執行器
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

值	說明
300	eDoctor 用戶端
1000	InterScan eManager
1001	InterScan AppletTrap
1002	InterScan VirusWall Java
1003	IS_SEMAIL
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
31004	Trend Micro Deep Security
31005	趨勢科技行動安全防護
31003	Trend Micro Endpoint Application Control
1004	InterScan WebProtect for ICAP
10001	NEC StarOffice
20001	Dr. Soloman 防毒
20002	Inoculan
20003	Norton Anti-Virus
20004	Sophos Sweep
20005	Intel LANProtect
20006	McAfee Virus Scan

值	說明
20007	FProt
21000	其他協力廠商產品
55555	示範產品
31104	Cloud App Security
31008	Deep Discovery Analyzer
31009	Trend Micro Endpoint Sensor
31101	Hosted Email Security
31006	Vulnerability Protection
31103	InterScan Web Security as a Service
31001	Trend Micro Security (適用於 Mac)
31002	Trend Micro Endpoint Encryption
31007	趨勢科技 Safe Mobile Workforce
31102	Worry Free Business Security Services

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)	裝置供應商	Trend Micro
標頭 (pname)	裝置產品	Control Manager
標頭 (pver)	裝置版本	7.0
標頭 (eventid)	事件 ID	800102

CEF 索引鍵	說明	值
標頭 (eventName)	記錄檔名稱	引擎更新狀態
標頭 (severity)	嚴重性	3
rt	記錄檔產生時間 (UTC)	範例：2017 年 4 月 20 日 12:04:34 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
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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 0：未使用 • 1：使用中
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：1 • 1：引擎
deviceFacility	產品名稱	範例：OfficeScan

記錄檔範例：

```
CEF:0|Trend Micro|Control Manager|7.0|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=OfficeScan . [0]
```

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)	裝置供應商	Trend Micro
標頭 (pname)	裝置產品	Control Manager
標頭 (pver)	裝置版本	7.0
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	偵測時間 (UTC)	範例：2017 年 2 月 14 日 11:14:08 GMT+00:00
dvchost	產品伺服器	範例：Sample_OSCE
cn1Label	cn1 欄位的對應標籤	可能的安全威脅類型

CEF 索引鍵	說明	值
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-25 頁。
cs2Label	cs2 欄位的對應標籤	安全威脅
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	類型
cn2	偵測類型	範例：0 <ul style="list-style-type: none"> • 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
cn4Label	cn4 欄位的對應標籤	程序指令
cs4	程序指令	範例：notepad.exe
duser	程序擁有者	範例：user1

CEF 索引鍵	說明	值
app	感染通道	範例：10 <ul style="list-style-type: none"> • 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	感染來源
cs3	感染來源	範例：http://10.0.0.1/
dst	產品/端點 IP	範例：10.0.35.49
c6a3Label	c6a3 欄位的對應標籤	產品/端點 IP
c6a3	產品/端點 IP	範例：10.0.17.6
cn3Label	cn3 欄位的對應標籤	安全威脅可能性
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 處理行動結果對應資料表 第 F-5 頁。
filehash	檔案 SHA-1	範例： 52c17c785b45ee961f68fb1774 4276076f383085
dhost	產品實體/端點	範例：dhost1
deviceExternalId	記錄序號	範例：100
deviceFacility	產品	範例：OfficeScan

記錄檔範例：

```
CEF:0|Trend Micro|Control Manager|7.0|PML:File cleaned|virus
a|3|deviceFacility=1 cs2Label=DetectionName cs2=virusa suser
=Sample-OSCE\Administrator cn2Label=DetectionType cn2=0 fil
ePath=C:\\WindowsFILENAME deviceCustomDate1Label=FileCreatio
nDate deviceCustomDate1=Nov 03 2016 08:58:03 GMT+00:00 sproc
=notepad.exe cs4Label=ProcessCommandLine cs4=notepad.exe -te
st duser=admin app=2 cs3Label=InfectionLocation cs3=http://1
0.0.0.1/ dst=10.0.174.28 cn3Label=Confidence cn3=82 act=21
```

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
35153	特洛伊木馬程式點擊程式
35154	特洛伊木馬程式下載程式

值	說明
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 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)	裝置供應商	Trend Micro
標頭 (pname)	裝置產品	Control Manager
標頭 (pver)	裝置版本	7.0
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	記錄檔產生時間 (UTC)	範例：2017 年 11 月 2 日 12:46:44 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

CEF 索引鍵	說明	值
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
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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 0：未使用 • 1：使用中
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	產品	範例：OfficeScan

記錄檔範例：

```
CEF:0|Trend Micro|Control Manager|7.0|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=OfficeScan . [0]
```

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	Control Manager
標頭 (pver)	裝置版本	7.0
標頭 (eventid)	MS：過濾器處理行動	MS：1
標頭 (eventName)	策略名稱	策略
標頭 (severity)	嚴重性	3
cnt	偵測數目	範例：10

CEF 索引鍵	說明	值
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：2 <ul style="list-style-type: none"> • 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
cs1Label	cs1 欄位的對應標籤	範例：SL_PolicyContent
cs1	策略設定	範例：Default_policy
cs2Label	cs2 欄位的對應標籤	範例：CLF_ProductVersion
cs2	產品版本	範例：11
cs3Label	cs3 欄位的對應標籤	範例：SL_FilterType

CEF 索引鍵	說明	值
cs3	過濾器類型	範例：2 <ul style="list-style-type: none">• 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：SL_MessageAction

CEF 索引鍵	說明	值
cs6	處理行動	範例：3 <ul style="list-style-type: none"> • 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：OSCEClient01
rt	記錄檔產生時間 (UTC)	範例：2017 年 11 月 15 日 08:45:57 GMT+ 00:00
cn1Label	cn1 欄位的對應標籤	範例：CLF_SeverityCode
cn1	嚴重性代碼	範例：0 <ul style="list-style-type: none"> • 0：未知 • 1：資訊 • 2：警告 • 3：錯誤 • 4：嚴重
deviceExternalId	識別碼	範例：5
fname	檔案	範例：RERERW~42w.exe

CEF 索引鍵	說明	值
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：OfficeScan

記錄檔範例：

```
CEF:0|Trend Micro|Control Manager|7.0|MS:5|This is a policy
name|3|deviceExternalId=6 rt=Nov 15 2017 08:46:23 GMT+00:00
cntLabel=AggregatedCount cnt=1 dhost=employee_a1@Acompany.co
m;employee_a2@Acompany.com duser=employee_a1@Acompany.com ac
t=5 cs1Label=SL_PolicyContent cs1=Default_policy cs2Label=CL
F_ProductVersion cs2=5.6 cs3Label=SL_FilterType cs3=5 cs4Lab
el=CLF_ReasonCode cs4=access violation cs5Label=CLF_ReasonCo
deSource cs5=20 cs6Label=SL_MessageAction cs6=5 cat=1705 dvc
host=OSCEClient01 cn1Label=CLF_ServerityCode cn1=0 fname=2_f
ile_D2AF1F1DB8857744AFFD6C85BDEF86FBEDCE5C35 msg=Open this e
mail to win a free phone shost=bear@abc.mail.com;yumi@abc.ma
il.com suser=bear@abc.mail.com deviceFacility=OfficeScan
```

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	Control Manager
標頭 (pver)	裝置版本	7.0

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	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：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-35 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：OSCEClient01
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：OSCEClient01
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： D6712CAE5EC821F910E1494 5153AE7871AA536CA
deviceFacility	產品	範例：OfficeScan
duser	使用者名稱	範例：Admin004
cn2Label	cn2 欄位的對應標籤	範例：Scan_Type
cn2	掃描類型	範例：立即掃描 如需詳細資訊，請參閱 間諜程式/可能的資安威脅程式掃描類型對應資料表 第 F-38 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-38 頁。

記錄檔範例：

```
CEF:0|Trend Micro|Control Manager|7.0|Spyware Detected|Spyware Detected|3|deviceExternalId=3 rt=Oct 06 2017 08:39:46 GMT+00:00 cnt=1 dhost=OSCEClient01 cn1Label=PatternType cn1=1073741840 cs1Label=VirusName cs1=ADW_OPENCANDY cs2Label=Engine Version cs2=6.2.3027 cs5Label=ActionResult cs5=Reboot system successfully cs6Label=PatternVersion cs6=1297 cat=1727 dvhost=OSCEClient01 fname=F:\Malware\psas\rsrc2.bin filePath
```

```
=F:\\Malware\\psas\\rsrc2.bin dst=50.8.1.1 deviceFacility=OfficeScan
```

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
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	檔案已丟棄
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	已成功封鎖
36	已成功隔離

值	說明
37	已成功加上戳記
38	檔案已上傳
39	無法清除檔案。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	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	已成功手動停止掃描
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
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

值	說明
133	無法丟棄檔案
134	無法封存檔案
135	無法封鎖檔案
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
145	無法手動停止掃描
146	無法重新導向郵件以供核准
201	需要採取處理行動 — 請執行完整系統掃描
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

值	說明
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
23	中等安全性
24	高安全性
25	弱點評估

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	Control Manager
標頭 (pver)	裝置版本	7.0
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：OSCEClient01
duser	使用者	範例：Admin004
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-35 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-43 頁 。
cs1Label	cs1 欄位的對應標籤	範例：VLF_FunctionCode

CEF 索引鍵	說明	值
cs1	掃瞄類型	範例：手動掃瞄 <ul style="list-style-type: none"> • 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
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-35 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-35 頁 。

CEF 索引鍵	說明	值
cat	記錄類型	範例：1703
dvchost	端點主機名稱	範例：OSCEClient01
cn3Label	cn3 欄位的對應標籤	範例：CLF_SeverityCode
cn3	嚴重性代碼	範例：2 <ul style="list-style-type: none"> • 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
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	範例：ABC-OSCE-WKS12
suser	來源主機	範例：ABC-OSCE-WKS12
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

CEF 索引鍵	說明	值
deviceFacility	產品名稱	範例：OfficeScan

記錄檔範例：

```
CEF:0|Trend Micro|Control Manager|7.0|AV:File renamed|JS_EXP
LOIT.SMDN|3|deviceExternalId=104 rt=Feb 18 2016 14:34:00 GMT
+00:00 cnt=1 dhost=OSCE_Client-4 duser=Admin004 act=File ren
amed cn1Label=VLF_PatternNumber cn1=920500 cn2Label=VLF_Seco
ndAction cn2=3 cs1Label=VLF_FunctionCode cs1=Manual Scan cs2
Label=VLF_EngineVersion cs2=9.500.1005 cs3Label=CLF_ProductV
ersion cs3=10.6 cs4Label=CLF_ReasonCode cs4=virus log cs5Lab
el=VLF_FirstActionResult cs5=File renamed cs6Label=VLF_Secon
dActionResult cs6=N/A cat=1703 dvchost=OSCEClient04 cn3Label
=CLF_ServerityCode cn3=2 fname=0348C693056617D34FC5B5BAB4643
885FEE5FEDF;0xD5D56AC2 filePath=C:\\Users\\Administrator\\De
sktop\\trend_test_virus\\Trojans\\ msg=BMAC Schedule of Even
ts.xls shost=ABC-OSCE-WKS12 suser=ABC-OSCE-WKS12 dst=10.201.
129.24 deviceFacility=OfficeScan
```

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
7	清除巨集

值	說明
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	Control Manager
標頭 (pver)	裝置版本	7.0
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-50 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 <ul style="list-style-type: none"> • 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	記錄檔產生時間 (UTC)	範例：2017 年 11 月 15 日 08:43:57 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 <ul style="list-style-type: none"> • 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-48 頁 。
dvchost	端點主機名稱	範例：OSCEClient08
cn1Label	cn1 欄位的對應標籤	範例：CLF_SeverityCode
cn1	嚴重性代碼	範例：0 <ul style="list-style-type: none"> • 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：OfficeScan

CEF 索引鍵	說明	值
duser	使用者名稱	範例：Admin004
shost	用戶端主機名稱	範例：ABC-OSCE-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：0 <ul style="list-style-type: none"> • 0：未知 • 1：資訊 • 2：警告 • 3：錯誤 • 4：嚴重

記錄檔範例：

```
CEF:0|Trend Micro|Control Manager|7.0|WB:7|7|3|deviceExternalId=38 rt=Nov 15 2017 08:43:57 GMT+00:00 app=17 cntLabel=AggregatedCount cnt=1 dpt=80 act=1 src=10.1.128.46 cs1Label=SLF_PolicyName cs1=External User Policy deviceDirection=2 cat=7 dvchost=OSCEClient08 fname=test.txt request=http://www.violentsoft.net/counter/insert.php?dbserver=db1&c_pcode=25&c_pid=funpop1&c_kind=4&c_mac=FE-ED-BE-EF-0C-E1 deviceFacility=OfficeScan
```

過濾/封鎖類型對應資料表

值	說明
0	未知
1	檔案名稱
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

值	說明
32	URL 封鎖
33	URL 過濾
34	用戶端 IP 封鎖
35	目標通訊埠封鎖
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	受限制の間諜程式/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

値	説明
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

値	説明
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

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	Control Manager
標頭 (pver)	裝置版本	7.0
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：OfficeScan
cs2Label	cs2 欄位的對應標籤	範例：EI_ProductVersion
cs2	產品版本	範例：11.0
rt	記錄檔產生時間 (UTC)	範例：2017 年 10 月 11 日 06:34:09 GMT+ 00:00
shost	端點主機名稱	範例：OSCEClient01
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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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

CEF 索引鍵	說明	值
cn3	回呼位址格式	範例：1 <ul style="list-style-type: none"> • 0：IP • 1：IP • 2：HTTP • 3：SMTP
要求	URL	範例：http://CC13.joyo.com
deviceCustomDate1 Label	deviceCustomDate1 欄位的對應標籤	範例：SLF_FirstSeen
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
deviceCustomDate2 Label	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.joyo.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

記錄檔範例：

```
CEF:0|Trend Micro|Control Manager|7.0|CnC:Block|CnC Callback
|3|deviceExternalId=12 rt=Oct 11 2017 06:34:09 GMT+00:00 cat
=1756 deviceFacility=OfficeScan cs2Label=EI_ProductVersion c
s2=11.0 shost=OSCEClient01 src=10.201.86.187 cs3Label=SLF_Do
mainName cs3=DOMAIN act=Block cn1Label=SLF_CCCA_RiskLevel cn
```

```
1=1 cn2Label=SLF_CCCA_DetectionSource cn2=1 cn3Label=SLF_CCC
A_DestinationFormat cn3=1 dst=10.201.86.195 deviceProcessNam
e=C:\\Program Files (x86)\\Internet Explorer\\iexplore.exe
```

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	Control Manager
標頭 (pver)	裝置版本	7.0
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	產品名稱	範例：OfficeScan
cn1Label	cn1 欄位的對應標籤	範例：SLF_ProductVersion
cn1	產品版本	範例：11
rt	偵測時間	範例：2017 年 11 月 15 日 02:47:21 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
c6a3	端點 IPv6 位址	範例：2620:101:4003:7a0:fd4b: 52ed:53bd:ae3d

CEF 索引鍵	說明	值
dhost	端點主機名稱	範例：OSCE-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： D6712CAE5EC821F910E1494 5153AE7871AA536CA
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\\ \\017545113A434757C5F0F130 95DBBF138BD76A40;0x36D57 2AE
cn2Label	cn2 欄位的對應標籤	範例：SLF_SourceType
cn2	C&C 清單來源	範例：0 <ul style="list-style-type: none"> • 0：沙盒 • 1：使用者定義
act	處理行動	範例：記錄 <ul style="list-style-type: none"> • 1：記錄 • 2：封鎖 • 3：隔離
cn3Label	cn3 欄位的對應標籤	範例：SLF_ScanType
cn3	掃描類型	範例：1 <ul style="list-style-type: none"> • 1：預約掃描 • 2：手動掃描 • 3：立即掃描 • 4：即時掃描

記錄檔範例：

```
CEF:0|Trend Micro|Control Manager|7.0|FH:Log|Suspicious File
s|3|deviceExternalId=1 rt=Nov 15 2016 02:47:21 GMT+00:00 cat
=1766 deviceFacility=OfficeScan cn1Label=SLF_ProductVersion
cn1=11 dst=10.201.86.151 dhost=OSCE-CLIENT-1 cs2Label=SLF_Tr
ueFileType cs2=SLF_TrueFileType fileHash=D6712CAE5EC821F910E
14945153AE7871AA536CA cs3Label=SLF_FileSource cs3=C:\\Users\\
Administrator\\Desktop\\BT-SHA1-SAMPLE\\BT-SHA1-SAMPLE\\017
545113A434757C5F0F13095DBBF138BD76A40;0x36D572AE cn2Label=SL
F_SourceType cn2=0 act=Log cn3Label=SLF_ScanType cn3=1
```

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	Control Manager
標頭 (pver)	裝置版本	7.0
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	產品名稱	範例：OfficeScan
rt	記錄檔產生時間 (UTC)	範例：2017 年 10 月 11 日 06:34:06 GMT+ 00:00
deviceProcessName	目標程序	範例：C:\\Windows\\system32\\svchost-1.exe

CEF 索引鍵	說明	值
src	來源 IPv4 位址	範例：10.201.86.152
c6a2Label	c6a2 欄位的對應標籤	範例：SLF_SourceIP
c6a2	來源 IPv6 位址	範例：2620:101:4003:7a0:fd4b:52ed:53bd:ae3d
spt	來源通訊埠	範例：54594
dst	目標 IPv4 位址	範例：10.69.81.64
c6a3Label	c6a3 欄位的對應標籤	範例：SLF_DestinationIP
c6a3	目標 IPv6 位址	範例：fe80::38ca:cd15:443c:40bb%11
dpt	目標通訊埠	範例：80
act	處理行動	範例：暫不處理 <ul style="list-style-type: none"> • 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	流量/連線	範例：輸入 <ul style="list-style-type: none"> • 0：無 • 1：輸入 • 2：輸出
cn1Label	cn1 欄位的對應標籤	範例：SLF_PatternType

CEF 索引鍵	說明	值
cn1	特徵碼類型	範例：2 <ul style="list-style-type: none"> • 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

記錄檔範例：

```
CEF:0|Trend Micro|Control Manager|7.0|NCIE:Pass|Suspicious Connection|3|deviceExternalId=1 rt=Oct 11 2017 06:34:06 GMT+00:00 cat=1756 deviceFacility=OfficeScan deviceProcessName=C:\\Windows\\system32\\svchost-1.exe act=Pass src=10.201.86.152 dst=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
```

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	Control Manager
標頭 (pver)	裝置版本	7.0

CEF 索引鍵	說明	值
標頭 (eventid)	裝置事件類別識別碼	<ul style="list-style-type: none"> • 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	記錄檔產生時間 (UTC)	範例：2017 年 2 月 14 日 11:14:08 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
c6a3	用戶端 IPv6 位址	範例：fe80::38ca:cd15:443c: 40bb%11
cn1	用戶端狀態	<ul style="list-style-type: none"> • 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： D6712CAE5EC821F910E1494 5153AE7871AA536CA
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

CEF 索引鍵	說明	值
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	<ul style="list-style-type: none"> • 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

記錄檔範例：

```
CEF:0|Trend Micro|Control Manager|7.0|EAC:1|Endpoint Application 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_ClientIPAddress_V4 cs2=0.0.0.0 cn1Label=Connection_Status cn1=0 fileHash=c0869b72C5606D22D92A6AC986686BB87485A25b fname=P2P_TEST.exe cs3Label=Command cs3=C:\\P2P_TEST.exe duser=QA cs4Label=Rule cs4=Test cs5Label=Policy cs5=TestPolicy act=Blocked deviceFacility=Trend Micro Endpoint Application Control
```

CEF 沙盒偵測記錄檔

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	Control Manager
標頭 (pver)	裝置版本	7.0

CEF 索引鍵	說明	值
標頭 (eventid)	裝置事件類別識別碼	VAD
標頭 (eventName)	事件名稱	沙盒偵測名稱
標頭 (severity)	嚴重性	3
deviceExternalId	識別碼	範例：2
rt	記錄檔產生時間 (UTC)	範例：2018 年 3 月 22 日 08:23:23 GMT+00:00
deviceFacility	產品類型	範例：OfficeScan
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：1
sourceServiceName	來源	範例： Test1@tmcm.extbeta.com
destinationServiceName	目標	範例： Test2@tmcm.extbeta.com;Test 3@tmcm.extbeta.com
sproc	程序名稱	範例：VA
fileHash	檔案 SHA-1 雜湊	範例： D6712CAE5EC821F910E1494 5153AE7871AA536CA
fname	檔案名稱	範例：C:\\\\QA_Log.zip
要求	URL	範例：http://127.1.1.1
cs1	沙盒偵測記錄檔偵測名稱	範例： VAN_RANSOMWARE.umxxhell oransom_abc

CEF 索引鍵	說明	值
cn1	沙盒偵測記錄檔風險等級	範例：0
cs2	沙盒偵測記錄檔安全威脅類別	範例：Anti-security, self-preservation
cs3	雲端儲存供應商	範例：N/A #015

記錄檔範例：

```
CEF: 0|Trend Micro|Control Manager|7.0|VAD|VAN_RANSOMWARE.um
xxhelloransom_abc|3|deviceExternalId=2 rt=Mar 22 2018 08:23:
23 GMT+00:00 deviceFacility=OfficeScan 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=N/A #015
```


索引

符號

「使用網域認證登入」按鈕, 2-5

A

Active Directory

- 手動同步處理, 6-2
- 同步處理頻率, 6-2
- 站台, 6-10
- 連線問題疑難排解, 6-4
- 連線設定, 6-2
- 報告行, 6-12
- 整合, 6-2

C

CEF syslog 對應

- C&C 回呼, F-55
- Data Loss Prevention, F-3
- Endpoint Application Control, F-63
- Machine Learning, F-22
- Web 安全, F-44
- 內容安全, F-28
- 引擎更新狀態, F-20
- 可疑檔案, F-59
- 行為監控, F-9
- 沙盒偵測記錄檔, F-65
- 特徵碼更新狀態, F-26
- 病毒/惡意程式, F-40
- 間諜程式/可能的資安威脅程式, F-32
- 裝置存取控制, F-14
- 網路內容檢測, F-61

Control Manager, 1-1, 1-2, 1-8

- MCP, 1-8
- SQL 資料庫, 1-8
- Web-based 管理主控台, 1-9

- Web 伺服器, 1-8
- Web 服務整合, 1-8
- Widget 架構, 1-9
- 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
- 通知, 15-3
- 報告伺服器, 1-8
- 郵件伺服器, 1-8
- 資料庫資料表, 19-4
- 關於, 1-1, 1-2

Control Manager 伺服器

- Web 主控台, 2-2, 2-3

D

DataExportTool, 23-3

Data Loss Prevention, 11-23

- DLP 合規官, 18-5
- DLP 事件檢閱者, 18-5
- 事件資訊清單, 18-8
- 事件調查, 18-1, 18-8
 - DLP 合規官, 18-5
 - DLP 事件檢閱者, 18-5
 - 通知, 18-7
 - 匯出事件詳細資料, 18-8
 - 管理員工作, 18-2
 - 稽核記錄檔, 18-7

表示式, 11-24 - 11-26, 11-28

- 符合性指標, 6-5
- 資料識別碼, 11-23
- 範本, 11-35 - 11-37, 11-39
- 檔案屬性, 11-28 - 11-30
- 關鍵字, 11-30 - 11-33, 11-35

Data Loss Prevention (DLP), 11-23

Data Loss Prevention 符合性

指標設定, 6-8

DBConfig 工具, 20-2

DLP, 11-23

DLP 事件檢閱者, 18-8

事件資訊清單, 18-8

L

LogForwarder 工具

系統需求, 23-3

限制, 23-3

停止, 23-6

設定, 23-4

開始, 23-6

簡介, 23-2

M

MCP, 1-8

MIB 檔案

Control Manager, E-2

NVW Enforcer SNMPv2, E-2

O

OfficeScan

Security Agent, 9-2

OfficeScan 用戶端

Windows 10, 9-8, 9-24

Windows 10 IoT Embedded, 9-12

Windows 7, 9-6, 9-22

Windows 7 Embedded, 9-10

Windows 8, 9-7, 9-23

Windows 8.1, 9-7, 9-23

Windows 8.1 Embedded, 9-12

Windows 8 Embedded, 9-11

Windows Compute Cluster Server

2003, 9-14

Windows Embedded POSReady 2009,
9-9

Windows Embedded POSReady 7, 9-10

Windows Embedded Standard 2009,
9-9

Windows HPC Server 2008, 9-14, 9-16,
9-28, 9-33

Windows HPC Server 2008 R2, 9-16,
9-34

Windows MultiPoint Server 2010, 9-17,
9-35

Windows MultiPoint Server 2011, 9-17,
9-36

Windows MultiPoint Server 2012, 9-18,
9-41

Windows Server , 1706 版, 9-20

Windows Server 2003, 9-13

Windows Server 2003 R2, 9-13

Windows Server 2008, 9-14, 9-15, 9-26,
9-30

Windows Server 2008 R2, 9-15, 9-31

Windows Server 2008 容錯移轉叢集,
9-15, 9-16, 9-28, 9-34

Windows Server 2012, 9-17, 9-37

Windows Server 2012 R2, 9-18, 9-38

Windows Server 2012 R2 容錯移轉叢集,
9-18

Windows Server 2012 容錯移轉叢集,
9-18, 9-42, 9-43

Windows Server 2016, 9-19, 9-44

Windows Server 2016 容錯移轉叢集,
9-19, 9-45

Windows Storage Server 2003, 9-13

Windows Storage Server 2003 R2, 9-14

Windows Storage Server 2008, 9-14,
9-15, 9-27, 9-31

- Windows Storage Server 2008 R2, 9-16, 9-32
 - Windows Storage Server 2012, 9-18, 9-39
 - Windows Storage Server 2012 R2, 9-18, 9-40
 - Windows Storage Server 2016, 9-19, 9-46
 - Windows XP, 9-5
 - Windows XP Embedded Standard, 9-9
 - 更新代理程式, 9-21, 9-22
- P**
- PCRE, 11-25
 - Perl Compatible Regular Expressions, 11-25
 - Proxy 伺服器設定
 - 元件更新, 12-11
 - 使用授權更新, 12-11
 - 受管理的伺服器清單, 8-7
- S**
- Security Agent
 - OfficeScan, 9-2
 - Trend Micro Security (適用於 Mac), 9-2
 - 下載, 9-2
 - Small Network Management Protocol
 - 請參閱 SNMP, 15-3
 - SNMP, 15-3
- T**
- Trend Micro Security (適用於 Mac)
 - Security Agent, 9-2
- W**
- Web 主控台, 2-2, 2-3
 - 登出, 2-6
 - Widget, 3-2
 - wildcards (萬用字元), 11-29
 - 檔案屬性, 11-29
 - Windows 10, 9-8, 9-24
 - Windows 10 IoT Embedded, 9-12
 - Windows 7, 9-6, 9-22
 - Windows 7 Embedded, 9-10
 - Windows 8, 9-7, 9-23
 - Windows 8.1, 9-7, 9-23
 - Windows 8.1 Embedded, 9-12
 - Windows 8 Embedded, 9-11
 - Windows Compute Cluster Server 2003, 9-14
 - Windows Embedded POSReady 2009, 9-9
 - Windows Embedded POSReady 7, 9-10
 - Windows Embedded Standard 2009, 9-9
 - Windows HPC Server 2008, 9-14, 9-16, 9-28, 9-33
 - Windows HPC Server 2008 R2, 9-16, 9-34
 - Windows MultiPoint Server 2010, 9-17, 9-35
 - Windows MultiPoint Server 2011, 9-17, 9-36
 - Windows MultiPoint Server 2012, 9-18, 9-41
 - Windows Server , 1706 版, 9-20
 - Windows Server 2003, 9-13
 - Windows Server 2003 R2, 9-13
 - Windows Server 2008, 9-14, 9-15, 9-26, 9-30
 - Windows Server 2008 R2, 9-15, 9-31
 - Windows Server 2008 容錯移轉叢集, 9-15, 9-16, 9-28, 9-34
 - Windows Server 2012, 9-17, 9-37
 - Windows Server 2012 R2, 9-18, 9-38
 - Windows Server 2012 R2 容錯移轉叢集, 9-18
 - Windows Server 2012 容錯移轉叢集, 9-18, 9-42, 9-43
 - Windows Server 2016, 9-19, 9-44
 - Windows Server 2016 容錯移轉叢集, 9-19, 9-45
 - Windows Storage Server 2003, 9-13
 - Windows Storage Server 2003 R2, 9-14

Windows Storage Server 2008, 9-14, 9-15, 9-27, 9-31

Windows Storage Server 2008 R2, 9-16, 9-32

Windows Storage Server 2012, 9-18, 9-39

Windows Storage Server 2012 R2, 9-18, 9-40

Windows Storage Server 2016, 9-19, 9-46

Windows XP, 9-5

Windows XP Embedded Standard, 9-9

一畫

一次性報告, 16-18

檢視, 16-22

三畫

工具

Control Manager MIB 檔案, E-2

DBConfig 工具, 20-2

NVW Enforcer SNMPv2 MIB 檔案,

E-2

用戶端移轉工具, 20-2

四畫

元件更新, 12-2, 12-8

Proxy 伺服器設定, 12-11

更新通知, 12-3

部署計劃, 12-3

部署預約時程, 12-3

預約, 12-5

元件更新通知, 12-3

元件清單, 12-2

升級策略範本, 11-21

手動元件更新, 12-8

手動更新

元件, 12-2

支援

更快地解決問題, 25-4

文件, xii

文件意見反應, 25-6

五畫

用戶端移轉工具, 20-2

目標, 11-18

已部署, 11-19

依條件過濾, 11-3

具有問題, 11-19

暫停中, 11-19

瀏覽, 11-8

離線, 11-19

六畫

存取權限, 4-8

安全威脅

使用者, 7-6

端點, 7-13

安全威脅狀態, 7-8, 7-14

安全威脅偵測標籤, 3-41

安全威脅詳細資訊

安全威脅狀態, 7-8, 7-14

有問題的目標, 11-19

自訂表示式, 11-25, 11-26, 11-28

條件, 11-25, 11-26

匯入, 11-28

自訂範本, 11-36, 16-2

建立, 11-37

匯入, 11-39

自訂關鍵字, 11-32

條件, 11-32, 11-33

匯入, 11-35

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, 8-9
- 新增, 8-4
- 編輯, 8-6
- 刪除
 - 使用者帳號, 4-2
 - 記錄檔, 14-11
- 刪除受管理的伺服器, 8-7
- 刪除策略, 11-16
- 我的帳號, 4-12
- 我的報告, 16-31
- 更新, 12-2
 - 元件, 12-2
 - 元件清單, 12-2
 - 手動, 12-8
- 更新代理程式, 9-21, 9-22
- 系統需求, 23-3
- 防毒病毒碼, 6-5
- 防毒病毒碼符合性
 - 指標設定, 6-6
- 八畫**
- 事件詳細資料已更新通知, 18-7
- 事件資訊清單, 18-8
- 依條件過濾, 11-3
- 使用者
 - 刪除帳號, 4-2
 - 啟動帳號, 4-3
 - 編輯帳號, 4-9
 - 關閉帳號, 4-3
- 使用者/端點目錄
 - 使用者詳細資料, 7-3
 - 進階搜尋, 7-21
 - 進階搜尋類別, 7-23
 - 匯出資料, 7-23
 - 端點詳細資料, 7-10
- 使用者分組, 6-10
- 使用者角色, 4-13
 - 新增, 4-17
 - 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, 4-13
 - 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, 12-11
- 使用授權資訊, 5-2
- 使用授權管理
 - 受管理的產品, 5-4
 - 詳細資料, 5-4
- 使用網域認證登入, 2-5
- 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, 8-7
- 受管理的產品, 10-2
 - 使用授權管理, 5-4
 - 啟動, 5-4, 5-5

- 設定, 10-9
- 部署元件, 10-8
- 發出工作, 10-8
- 註冊, 5-4, 5-6
- 檢視記錄檔, 10-10

九畫

- 表示式, 11-23, 11-24
 - 自訂, 11-25, 11-28
 - 條件, 11-25, 11-26
 - 預先定義, 11-24
- 表格式檢視
 - 使用者詳細資料, 7-3
 - 端點詳細資料, 7-10

八畫

- 長條圖, 16-7

九畫

- 建立
 - 稽核記錄檔, 18-7
- 建立策略, 11-2, 11-15
 - 設定, 11-3
 - 複製設定, 11-11
- 指令追蹤, 13-2
 - 指令詳細資料, 13-3
 - 查詢, 13-3
 - 檢視, 13-3
- 指令詳細資料, 13-3
- 指定目標
 - 瀏覽, 11-8
- 指定策略, 11-3
 - 優先順序, 11-8
- 重新排序策略, 11-20

十畫

- 時間表檢視
 - 使用者詳細資料, 7-3

- 端點詳細資料, 7-10
- 案例處理, 7-8, 7-14
- 站台, 6-10
 - 合併, 6-11
 - 建立自訂, 6-10
 - 檢視, 6-10

十二畫

- 草稿策略, 11-3

十畫

- 記錄查詢, 14-2
- 記錄檔, 14-1, 14-2
 - 刪除, 14-11
 - 查詢, 14-2
 - 設定記錄檔彙整, 14-10

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

- Control Manager, 5-2
- 使用者帳號, 4-3
- 受管理的產品, 5-4, 5-5

- 啟動碼, 5-2

條件

- 自訂表示式, 11-25, 11-26
- 關鍵字, 11-32, 11-33
- 條件陳述式, 11-37
- 產品目錄, 10-2
 - 工作, 10-2
 - 受管理的產品, 10-2
- 產品範圍

- Widget, 3-5
- 符合性指標, 6-5
- 符合性標籤, 3-35
- 設定
 - 存取權限, 4-8
 - 受管理的產品, 10-9
 - 記錄檔彙整, 14-10
- 設定 Proxy 伺服器設定
 - 受管理的伺服器清單, 8-7
- 通知, 15-3
 - 事件詳細資料已更新, 18-7
 - 設定, 15-3
 - 預約事件摘要, 18-7
- 通知和報告
 - 聯絡人群組
 - 新增, 15-7
 - 編輯, 15-8
- 通訊埠
 - 檢查清單, A-3
- 部署的目標, 11-19
- 部署計劃, 12-3
- 十二畫**
- 報告
 - 一次性報告, 16-18, 16-19
 - 自訂報告範本
 - 新增, 16-3
 - 自訂範本, 16-2, 16-3
 - 長條圖, 16-7
 - 圓餅圖, 16-12
 - 刪除, 16-31
 - 我的報告, 16-31
 - 格式, 16-20, 16-24, 16-28
 - 自訂範本, 16-20, 16-24, 16-28
 - 靜態範本, 16-20, 16-24, 16-28
 - 預約報告, 16-22, 16-23, 16-27
 - 範本, 16-3
- 檢視
 - 預約報告, 16-30
- 檢視報告
 - 一次性報告, 16-22
- 報告行, 6-12
 - 合併, 6-13
 - 建立自訂, 6-12
 - 檢視, 6-12
- 報告維護, 16-31
- 報告範本
 - 自訂, 16-3
- 登入, 2-5
 - 從本機, 2-5
 - 從遠端, 2-5
- 登出, 2-6
- 策略
 - 刪除, 11-16
 - 建立, 11-2, 11-15
 - 重新排序, 11-20
 - 編輯, 11-13
- 策略目標, 11-18
- 策略清單, 11-6, 11-17
- 策略設定
 - 複製, 11-11
- 策略管理, 11-1, 11-2
 - DLP, 11-23
 - 升級策略範本, 11-21
 - 目標, 11-18
 - 有問題的目標, 11-19
- 刪除策略, 11-16
- 建立策略, 11-2, 11-15
- 指定策略, 11-3
- 重新排序策略, 11-20
- 草稿策略, 11-3
- 設定, 11-3
- 部署的目標, 11-19

- 策略清單, 11-6, 11-17
- 策略優先順序, 11-8, 11-18
- 暫停中的目標, 11-19
- 編輯策略, 11-13
- 複製策略設定, 11-11
- 擁有者, 11-19
- 瞭解, 11-2
- 離線目標, 11-19
- 變更擁有者, 11-17
- 策略範本, 11-21
- 策略優先順序, 11-18
- 策略類型
 - 指定, 11-3
 - 重新排序策略, 11-20
 - 草稿, 11-3
 - 策略優先順序, 11-18
- 註冊
 - 受管理的伺服器, 8-4
 - 受管理的產品, 5-4, 5-6
- 詞彙, xiv
- 進階搜尋
 - 使用者/端點目錄, 7-21
- 雲端服務組態設定, 8-9

十三畫

- 匯出
 - DLP 事件詳細資料, 18-8
- 圓餅圖, 16-12
- 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
- 資料庫資料表, 19-4
- 資料檢視

- 安全威脅資訊, B-2
- 產品資訊, B-85
- 資料識別碼, 11-23
- 表示式, 11-23
- 檔案屬性, 11-23
- 關鍵字, 11-23
- 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, 3-3
 - 投影片放映, 3-2
 - 重新命名, 3-2
 - 新增, 3-2
 - 摘要, 3-16

過濾策略

- 重新排序, 11-20
- 電子郵件, 15-3
- 預先定義的表示式, 11-24
 - 檢視, 11-24
- 預先定義的範本, 11-36
- 預先定義的關鍵字
 - 距離, 11-31
 - 關鍵字的數目, 11-31
- 預約更新, 12-5
 - 元件, 12-2
- 預約事件摘要通知, 18-7
- 預約報告, 16-22
 - 檢視, 16-30
- 預設使用者角色, 4-15

十四畫

- 摘要標籤, 3-16
- 端點分組, 6-10
- 端點詳細資料, 7-10

表格式檢視, 7-10
 時間表檢視, 7-10

管理

- 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, 8-9
- 雲端服務設定, 8-9
- 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

暫停中的目標, 11-19

標籤, 3-2

- Widget, 3-2
- 安全威脅偵測, 3-41
- 符合性, 3-35
- 摘要, 3-16

稽核記錄檔, 18-7

範本, 11-35 - 11-37, 11-39

- 自訂, 11-36, 11-37, 11-39
- 自訂報告, 16-3
- 條件陳述式, 11-37
- 預先定義, 11-36
- 邏輯運算子, 11-37

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, 11-13

複製策略設定, 11-11

調查 DLP 事件, 18-1, 18-8

- DLP 合規官, 18-5
- DLP 事件檢閱者, 18-5
- 事件資訊清單, 18-8
- 通知, 18-7
- 匯出事件詳細資料, 18-8
- 管理員工作, 18-2

稽核記錄檔, 18-7

十六畫

選取目標

- 依條件過濾, 11-3

十七畫

檔案屬性, 11-23, 11-28 - 11-30

- wildcards (萬用字元), 11-29
- 建立, 11-29
- 匯入, 11-30

檢查清單

- 伺服器位址, A-2
- 通訊埠, A-3

檢視

- 受管理產品記錄檔, 10-10

檢閱 DLP 事件, 18-8

- 事件資訊清單, 18-8

瞭解

使用者帳號, 4-2

聯絡人群組, 15-6

移除, 15-6

新增, 15-6, 15-7

編輯, 15-8

十八畫

瀏覽目標, 11-8

十九畫

離線目標, 11-19

十八畫

雙因素驗證, 2-5, 4-10

十九畫

關閉

使用者帳號, 4-3

關鍵字, 11-23, 11-30

自訂, 11-32, 11-33, 11-35

預先定義, 11-31

二十畫

觸發應用程式, 15-3

二十三畫

邏輯運算子, 11-37



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: CMTM78290/180614