TREND MICRO™

3.2 趨勢科技™ 主動式雲端截毒技術伺服器 管理手冊

讓安全更具智慧

Endpoint Security

Messaging Security

Protected Cloud

Web Security

文件編號：APTM37774/170406

發行日期：2017 年 4 月

受美國專利保護，專利編號： 等待獲得專利中。

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，請參閱趨勢科技線上說明中心和/或趨勢科技常見問題集。

趨勢科技十分重視文件品質的提升。如果您對於本文件或其他趨勢科技文件有任何問題、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 v

關於趨勢科技 vi

產品文件 vi

讀者 vi

文件慣例 vii

第 1 章：簡介

主動式雲端截毒技術伺服器如何運作？ 1-2

新解決方案的必要性 1-2

主動式雲端截毒技術解決方案 1-2

本版本中的新功能 1-7

主要功能和優點 1-8

趨勢科技主動式雲端截毒技術 1-8

檔案信譽評等服務 1-9

網頁信譽評等服務 1-9

Smart Feedback 1-9

第 2 章：使用主動式雲端截毒技術伺服器

初始組態設定 2-2

使用產品主控台 2-6

存取產品主控台 2-7

使用主動式雲端截毒技術 2-7

使用信譽評等服務 2-8

設定使用者定義的 URL 2-10

設定可疑物件 2-11

啟動 Smart Feedback 2-13

更新 2-14
設定手動更新 2-14
設定預約更新 2-15
病毒碼檔案更新 2-15
程式檔案更新 2-15
設定更新來源 2-19
管理工作 2-19
SNMP 服務 2-19
Proxy 設定 2-23
支援 2-25
變更產品主控台密碼 2-26
匯入憑證 2-27
與趨勢科技產品和服務整合 2-27

第 3 章：監控主動式雲端截毒技術伺服器

使用摘要畫面 3-2
標籤 3-3
Widget 3-6
記錄檔 3-12
封鎖的 URL 3-13
更新記錄檔 3-14
信譽評等服務記錄檔 3-14
記錄檔維護 3-15
通知 3-16
電子郵件通知 3-16
SNMP Trap 通知 3-19

第 4 章：與 Trend Micro Control Manager 整合

趨勢科技 Control Manager 4-2
支援的 Control Manager 版本 4-2
本主動式雲端截毒技術伺服器版本中的 Control Manager 整合 4-2

第 5 章：技術支援

疑難排解資源 5-2
使用支援入口網站 5-2
安全威脅百科全書 5-2
聯絡趨勢科技 5-3
加速支援要求 5-4
將可疑內容傳送到趨勢科技 5-4
電子郵件信譽評等服務 5-4
檔案信譽評等服務 5-5
網頁信譽評等服務 5-5
其他資源 5-5
下載專區 5-5
文件意見反應 5-6

附錄 A：命令列介面 (CLI) 命令

索引

索引 IN-1

序言

序言

歡迎使用《主動式雲端截毒技術伺服器管理手冊》。本文件包含產品設定的相關資訊。

包含下列主題：

- 關於趨勢科技™ 第 vi 頁
- 產品文件 第 vi 頁
- 讀者 第 vi 頁
- 文件慣例 第 vii 頁

關於趨勢科技™

趨勢科技提供病毒防護、垃圾郵件防護以及內容過濾安全防護軟體與服務。趨勢科技可協助全球客戶遏止惡意程式碼傷害其電腦。

產品文件

主動式雲端截毒技術伺服器文件包含：

文件	說明
安裝和升級手冊	協助您進行安裝、升級和部署的規劃。
管理手冊	協助您設定所有產品設定。
線上說明	提供有關每個欄位以及如何透過使用者介面設定所有功能的詳細指示。
Readme 檔	包含其他文件中可能未提供的最新發表產品資訊。其中的主題包括功能的說明、安裝祕訣、已知問題和產品發行歷史記錄。

您可以在下列網址取得此文件：

http://downloadcenter.trendmicro.com/?regs=TW

讀者

主動式雲端截毒技術伺服器文件是專為 IT 管理員和系統管理員所撰寫。本文件假設讀者已具備深入的電腦網路知識。

本文件並不假設讀者具備任何病毒/惡意程式防範或垃圾郵件防範技術的知識。

文件慣例

《主動式雲端截毒技術伺服器使用者手冊》使用下列慣例。

表 1. 文件慣例

慣例	說明
全部大寫	頭字語、縮寫、特定的命令名稱和鍵盤上的按鍵
粗體	功能表和功能表命令、命令按鈕、標籤和選項
瀏覽 > 路徑	可達到特定畫面的瀏覽路徑 例如，「檔案 > 儲存」代表按一下「檔案」，然後按一下介面上的「儲存」
 注意	組態設定注意事項
 秘訣	推薦或建議
 警告!	重要的處理行動和組態設定選項

第 1 章

簡介

本章提供趨勢科技™ 主動式雲端截毒技術伺服器™功能的介紹和說明。

包含下列主題：

- 主動式雲端截毒技術伺服器如何運作？ 第 1-2 頁
- 本版本中的新功能 第 1-7 頁
- 主要功能和優點 第 1-8 頁
- 趨勢科技主動式雲端截毒技術 第 1-8 頁

主動式雲端截毒技術伺服器如何運作？

主動式雲端截毒技術伺服器是新一代的雲端進階防護解決方案。此解決方案的核心是進階的掃瞄架構，它會利用儲存在雲端的惡意程式防護簽章來進行掃瞄。

此解決方案會利用檔案信譽評等和網頁信譽評等技術來偵測安全威脅。此技術的運作方式是將先前儲存在端點上的大量惡意程式防護簽章和清單改由主動式雲端截毒技術伺服器處理。

透過這種方式，可以大幅減少不斷增加的端點簽章更新量對於系統和網路的影響。

新解決方案的必要性

在目前的 File-based 威脅處理方法中，保護端點所需的病毒碼（或定義）大多是經由預約方式傳遞。病毒碼是從趨勢科技分批傳遞至端點。端點上的病毒/惡意程式防護軟體在收到更新後，即會將這批針對新病毒/惡意程式威脅的病毒定義碼重新載入記憶體中。如果有新的病毒/惡意程式威脅出現，即需對此病毒碼再進行部分或全部更新，並重新載入到端點上，以確保持續防護。

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

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

主動式雲端截毒技術解決方案

雲端查詢程序使用兩種 Network-based 技術：

- 趨勢科技 主動雲端截毒技術™：具備全球規模的 Internet-based 基礎結構，可提供服務給無法直接存取其企業網路的使用者。
- 主動式雲端截毒技術伺服器：主動式雲端截毒技術伺服器存在於區域網路中。這是要讓可以存取其企業區域網路的使用者使用。這些伺服器的設計目標是供客戶在企業網路內執行作業，以最佳化效能。

注意

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

這兩種 Network-based 解決方案控管了大部分的病毒/惡意程式病毒碼定義和網頁信譽評分。趨勢科技主動雲端截毒技術和主動式雲端截毒技術伺服器會將這些定義提供給網路上的其他端點，以驗證是否有潛在的安全威脅。如果端點無法判斷檔案或 URL 是否有風險，則只會將查詢傳送至主動式雲端截毒技術伺服器。

端點會利用檔案信譽評等和網頁信譽評等技術，向主動式雲端截毒技術伺服器電腦執行查詢，以做為其正常系統防護活動的一部分。在此解決方案中，代理程式會將辨識資訊（由趨勢科技技術所決定）傳送至主動式雲端截毒技術伺服器電腦，以進行查詢。在使用檔案信譽評等技術時，代理程式絕對不會傳送整個檔案。而是會使用辨識資訊來判斷檔案的風險。

病毒碼檔案

主動雲端截毒技術病毒碼檔案用於檔案信譽評等服務和網頁信譽評等服務。趨勢科技會透過趨勢科技主動式更新伺服器發行這些病毒碼檔案。

下列為病毒碼檔案：

表 1-1. 主動式雲端截毒技術伺服器病毒碼檔案

信譽評等服務	病毒碼	詳細資訊
檔案信譽評等服務	雲端病毒碼	雲端查詢程序會將雲端病毒碼檔案和即時雲端查詢系統搭配使用。雲端查詢系統在驗證過程中，會向主動式雲端截毒技術伺服器驗證檔案、URL 和其他元件。主動式雲端截毒技術伺服器電腦會使用數種演算法，來達到使用最少網路頻寬的高效率程序。 雲端病毒碼會每小時自動更新。
網頁信譽評等服務	網頁封鎖病毒碼	使用網頁信譽評等服務的產品（如 OfficeScan 和 Deep Security）會透過向主動式雲端截毒技術伺服器傳送網頁信譽評等查詢，來根據網頁封鎖病毒碼驗證網站的信譽評等。這些產品會將從主動式雲端截毒技術來源收到的信譽評等資料與端點上實施的網頁信譽評等策略互相關聯。依據策略的不同，產品有可能允許或阻止存取網站。 注意 如需使用網頁信譽評等服務的產品清單，請參閱： 與趨勢科技產品和服務整合 第 2-27 頁

病毒碼更新程序

病毒碼更新是一種對於安全威脅的回應。主動雲端截毒技術和主動式雲端截毒技術伺服器電腦會從主動式更新伺服器下載雲端病毒碼檔案。支援主動式雲端截毒技術伺服器電腦的趨勢科技產品會從主動式更新伺服器下載本機雲端病毒碼。

位於內部網路中的端點則會從支援主動式雲端截毒技術伺服器電腦的趨勢科技產品下載本機雲端病毒碼檔案。外部端點位於內部網路之外，並且無法與主動

式雲端截毒技術伺服器電腦或支援主動式雲端截毒技術伺服器電腦的趨勢科技產品連線。

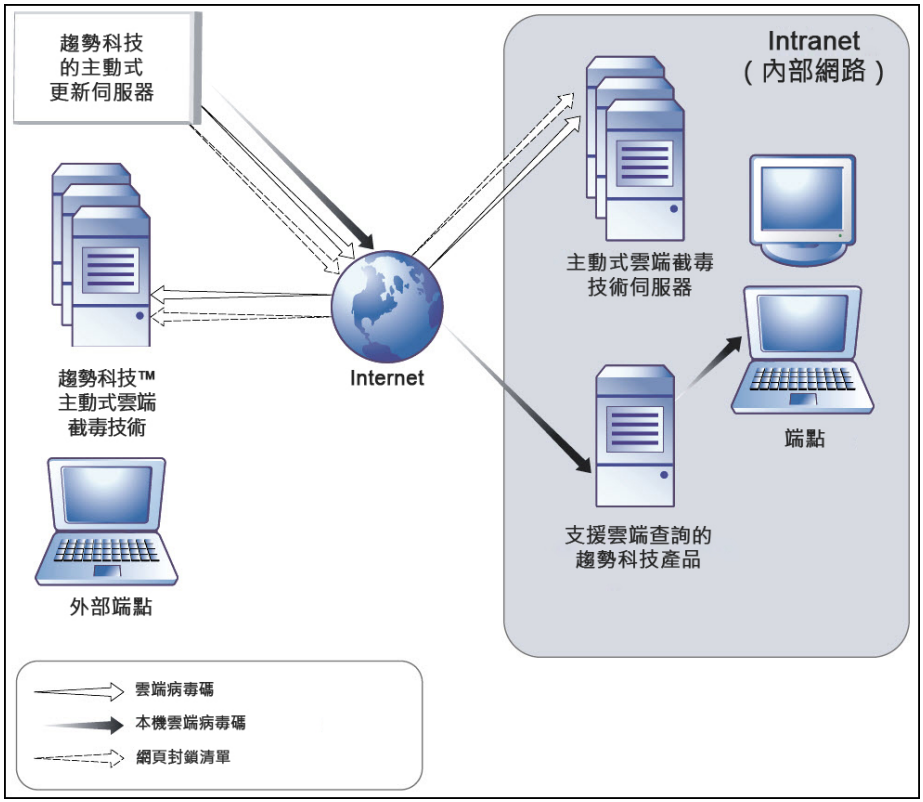


圖 1-1. 病毒碼更新程序

查詢程序

目前位於內部網路的端點會使用主動式雲端截毒技術伺服器電腦來查詢。目前不在內部網路的端點則可以連線到趨勢科技主動式雲端截毒技術來查詢。

雖然主動式雲端截毒技術伺服器電腦要有網路連線才能使用，但是無法使用網路連線的端點一樣能夠享受趨勢科技的技術。位於端點上的本機雲端病毒碼和掃瞄技術，可以保護無法存取網路連線的端點。

安裝在端點上的代理程式會先對端點執行掃瞄。如果代理程式無法判斷檔案或 URL 的風險，則代理程式會將查詢傳送到主動式雲端截毒技術伺服器以驗證該風險。

表 1-2. 保護行為會根據是否能存取內部網路而定

位置	病毒碼檔案和查詢行為
存取內部網路	• 病毒碼檔案：端點會從支援主動式雲端截毒技術伺服器電腦的趨勢科技產品下載本機雲端病毒碼檔案。 • 查詢：端點連線到主動式雲端截毒技術伺服器以進行查詢。
無法存取內部網路	• 病毒碼檔案：端點除非可以連線到支援主動式雲端截毒技術伺服器電腦的趨勢科技產品，否則無法下載最新的本機雲端病毒碼檔案。 • 查詢：端點可以使用本機資源（例如：本機雲端病毒碼檔案）來掃瞄檔案。

進階過濾技術可讓代理程式「快取」查詢結果。此舉可改進掃瞄效能，而且不需要多次傳送相同的查詢到主動式雲端截毒技術伺服器電腦。

代理程式若是無法在本機確認檔案的風險，並且在嘗試數次之後仍無法連線到任何主動式雲端截毒技術伺服器電腦，就會將檔案標記為待驗證，並暫時允許存取檔案。當與主動式雲端截毒技術伺服器之間的連線恢復時，便會重新掃瞄所有已標示的檔案。接著，會對已確認為網路之安全威脅的檔案執行適當的中毒處理行動。

秘訣

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

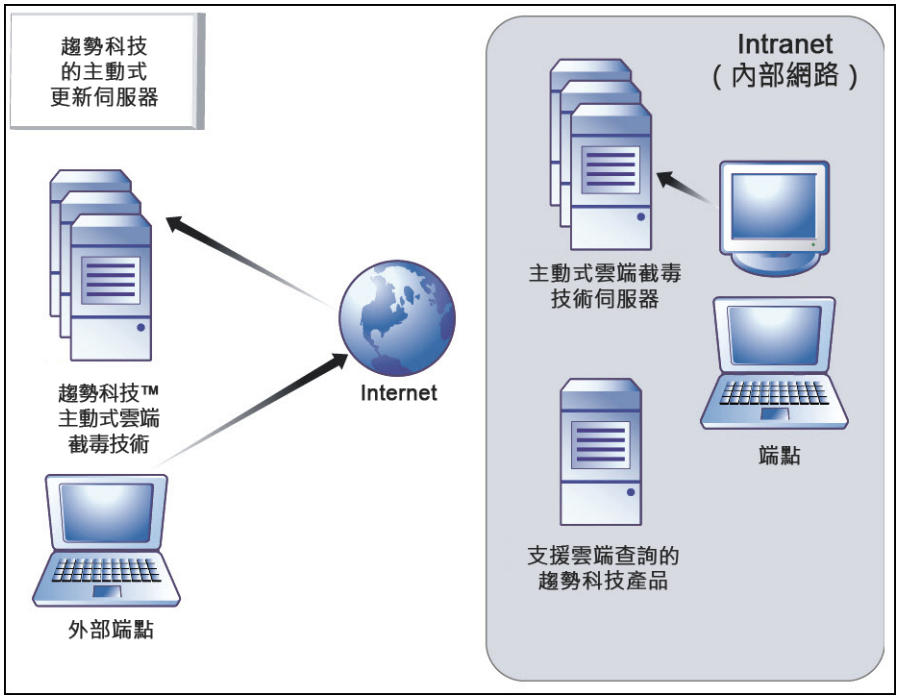


圖 1-2. 查詢程序

本版本中的新功能

主動式雲端截毒技術伺服器包含下列新功能及加強功能：

表 1-3. 第 3.2 版新增功能

功能	說明
CentOS 7.3	主動式雲端截毒技術伺服器已將作業系統更新為 CentOS 7.3。

主要功能和優點

主動式雲端截毒技術伺服器提供下列功能及優點：

- 檔案信譽評等技術
  - 企業網路將具有更大的優勢可應付激增的安全威脅。
  - 抵禦新興威脅所需的總「防護前置時間」大幅減少。
  - 工作站上核心記憶體的耗用量大幅減少，而且隨時間增加的量非常小。
  - 使系統管理更有效率並簡化管理。大量的病毒定義碼更新只需傳遞到一部伺服器，不必傳遞到許多工作站。這可減少要在許多工作站上進行病毒碼更新而帶來的大幅影響。
  - 抵禦 Web-based 和混合式攻擊。
  - 阻止病毒/惡意程式、特洛伊木馬程式、電腦蠕蟲，以及這些安全威脅的新變體。
  - 偵測及移除間諜程式/可能的資安威脅程式（包括隱藏的 Rootkit）。
- 網頁信譽評等技術
  - 抵禦 Web-based 和混合式攻擊。
  - 重視隱私權的客戶不必擔心網頁信譽評等向主動式雲端截毒技術進行查詢時會暴露他們的機密資訊。
  - 主動式雲端截毒技術伺服器回應查詢的時間比主動式雲端截毒技術更短。
  - 在您的網路上安裝主動式雲端截毒技術伺服器可減少閘道頻寬負載。

趨勢科技主動式雲端截毒技術

趨勢科技™主動雲端截毒技術™是新一代的雲端用戶端內容安全基礎結構，旨在保護客戶不受安全威脅和網路安全威脅的侵襲。此解決方案同時提供本機和託

管解決方案，不論使用者正處於網路上、在家中或路上都可提供保護，方法是使用輕量型代理程式來存取電子郵件、網頁和檔案信譽評等技術以及安全威脅資料庫的獨一無二雲端相互關聯性。隨著存取這個網路的產品、服務和使用者越來越多，客戶受到的保護會自動更新和強化，從而為其使用者建立了一個即時的守望相助系統防護服務。

檔案信譽評等服務

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

網頁信譽評等服務

透過全世界其中一個最大的網域信譽評等資料庫，趨勢科技網頁信譽評等技術依據諸如網站的存在時間長短、位置變更記錄，以及透過惡意程式行為分析所發現的可疑活動指標等因素來指定信譽評等，以追蹤 Web 網域的可信度。然後它就會繼續掃瞄網站，並阻擋使用者存取中毒的網站。網頁信譽評等功能有助於確認使用者存取的是安全網頁，且不含任何網路安全威脅，例如惡意程式、間諜程式，以及專門在誘騙使用者提供個人資訊的網路釣魚詐騙手法。為了提高準確度並減少誤判的情形，趨勢科技網頁信譽評等技術會為網站內的特定網頁或連結指定信譽評分，而不是將整個網站進行分類或封鎖，因為通常合法網站只有部分受到駭客入侵，而信譽評等會隨著時間動態變更。

網頁信譽評等功能有助於確認使用者存取的是安全網頁，且不含任何網路安全威脅，例如惡意程式、間諜程式，以及專門在誘騙使用者提供個人資訊的網路釣魚詐騙手法。網頁信譽評等會根據網頁的信譽評等分級來決定是否加以封鎖。當網頁信譽評等啟動時，可讓使用者注意不要去存取惡意 URL。

Smart Feedback

趨勢科技™ Smart Feedback 提供趨勢科技產品之間不間斷的通訊，以及本公司全年無休的安全威脅研究中心和技術。若是單一客戶在執行例行信譽檢查時發

現任何新的安全威脅，就會自動更新所有趨勢科技的安全威脅資料庫，以避免其他客戶受到該安全威脅的攻擊。趨勢科技藉由持續處理透過廣大全球客戶和合作夥伴網路收集的安全威脅資訊，提供自動的即時防護以抵禦最新的安全威脅侵襲，同時提供更佳的協同安全防護，就像是自動化的守望相助系統，動員整個社群來保護其中的每個人。因為安全威脅資訊是根據通訊來源的信譽評等而非特定通訊內容來收集，所以客戶個人或商業資訊的隱私一律會受到保護。

第 2 章

使用主動式雲端截毒技術伺服器

本章提供主動式雲端截毒技術伺服器的組態設定資訊。

包含下列主題：

- 初始組態設定 第 2-2 頁
- 使用產品主控台 第 2-6 頁
- 使用主動式雲端截毒技術 第 2-7 頁
- 更新 第 2-14 頁
- 管理工作 第 2-19 頁
- 變更產品主控台密碼 第 2-26 頁
- 匯入憑證 第 2-27 頁
- 與趨勢科技產品和服務整合 第 2-27 頁

初始組態設定

安裝後請執行下列工作。

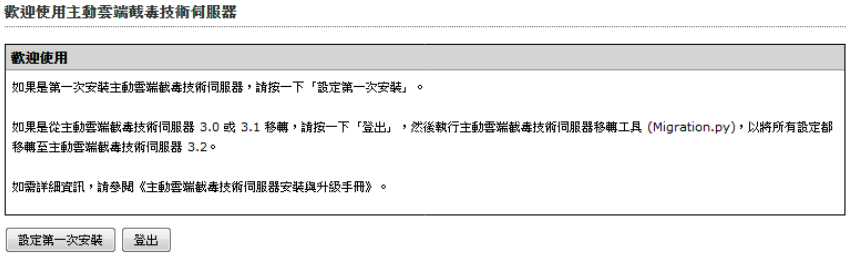
重要

如果是從主動式雲端截毒技術伺服器 3.0 或 3.1 移轉，請先執行主動式雲端截毒技術伺服器移轉工具 (Migration.py) 將您所有設定移轉至主動式雲端截毒技術伺服器 3.2，然後再繼續。

程序

1. 登入 Web 主控台。

   「歡迎使用」畫面隨即出現。



2. 按一下「設定第一次安裝」。

   第一次安裝精靈隨即出現。

3. 選取「啟動檔案信譽評等服務」核取方塊，以使用檔案信譽評等。

4. 按「下一頁」。

   「網頁信譽評等服務」畫面隨即出現。

5. 選取「啟動網頁信譽評等服務」核取方塊，以啟動網頁信譽評等。

6. （選用）過濾器優先順序設定可讓您指定 URL 查詢適用的過濾順序。

7. 按「下一頁」。

「Smart Feedback」畫面隨即出現。

8. 選取以使用 Smart Feedback，協助趨勢科技針對新的安全威脅更快提供解決方案。

9. 按「下一頁」。

   「Proxy 設定」畫面隨即出現。

10. 如果您的網路使用 Proxy 伺服器，請指定 Proxy 設定。

11. 按一下「完成」，以完成主動式雲端截毒技術伺服器清單的初始組態設定。

    Web 主控台的「摘要」畫面隨即顯示。

> **注意**
>
> 主動式雲端截毒技術伺服器將會在初始組態設定之後，自動更新病毒碼檔案。

使用產品主控台

產品主控台包含下列元素：

- 主功能表：提供「摘要」、「主動式雲端截毒技術」、「更新」、「記錄檔」和「管理」畫面的連結。
- 工作區：檢視摘要資訊和元件狀態、設定選項、更新元件和執行管理工作。

功能表	說明
摘要	在您新增 Widget 後，顯示有關主動式雲端截毒技術伺服器電腦、流量和偵測次數的自訂資訊。
主動式雲端截毒技術	提供設定信譽評等服務、使用者定義的 URL、可疑物件和 Smart Feedback 的選項。
更新	提供設定預約更新、手動程式更新、程式套件上傳和更新來源的選項。
記錄檔	提供查詢記錄檔和記錄檔維護的選項。
管理	提供用於設定 SNMP 服務、通知、代理伺服器設定，以及收集診斷資訊以進行疑難排解的選項。

存取產品主控台

登入 Web 主控台之後，初始畫面會顯示主動式雲端截毒技術伺服器電腦的狀態摘要。

程序

1. 安裝之後，開啟 Web 瀏覽器，並輸入初始 CLI 標題上顯示的 URL。
2. 輸入 `admin` 做為使用者名稱，並在對應欄位中輸入密碼。
3. 按一下「登入」。

使用主動式雲端截毒技術

這個版本的主動式雲端截毒技術伺服器包含檔案信譽評等服務和網頁信譽評等服務。

使用信譽評等服務

從產品主控台啟動「信譽評等服務」，以允許其他趨勢科技產品使用「主動式雲端截毒技術」。

啟動檔案信譽評等服務

啟動檔案信譽評等服務，以支援來自端點的查詢。

程序

1. 移至「主動式雲端截毒技術 > 信譽評等服務」，然後移至「檔案信譽評等」標籤。

2. 選取「啟動檔案信譽評等服務」核取方塊。

3. 按一下「儲存」。

   「伺服器位址」現在可供其他支援主動式雲端截毒技術伺服器電腦的趨勢科技產品用來進行檔案信譽評等查詢。

啟動網頁信譽評等服務

啟動網頁信譽評等服務，以支援來自端點的 URL 查詢。以下是此畫面提供的選項。

- 啟動網頁信譽評等服務：選取以支援來自端點的網頁信譽評等查詢。
- 伺服器位址：由其他趨勢科技產品用來進行網頁信譽評等查詢。
- 過濾器優先順序：選取以指定過濾 URL 時的優先順序。

程序

1. 移至「主動式雲端截毒技術 > 信譽評等服務」，然後按一下「網頁信譽評等」標籤。
2. 選取「啟動網頁信譽評等服務」核取方塊。
3. （選用）指定過濾 URL 時使用者定義的許可及封鎖的 URL 的優先順序。例如，如果「使用者定義的封鎖的 URL」具有第一優先順序，則「使用者定義的許可的 URL」將列為第二優先順序。

4. 按一下「儲存」。

「伺服器位址」現在可供其他支援主動式雲端截毒技術伺服器的趨勢科技產品用來進行網頁信譽評等查詢。

設定使用者定義的 URL

使用者定義的 URL 可讓您指定您自己的許可的 URL 和（或）封鎖的 URL。這會用於網頁信譽評等。以下是此畫面提供的選項。

- 搜尋規則：選取此選項，可在規則清單中搜尋某個字串。
- 測試 URL：選取此選項，可搜尋 URL 會觸發的規則。URL 的開頭必須是 `http://` 或 `https://`。

程序

1. 移至「主動式雲端截毒技術 > 使用者定義的 URL」。
2. 在「搜尋條件」下方，按一下「新增」。

   「新增規則」畫面隨即顯示。

3. 選取「啟動這項規則」核取方塊。

4. 選取下列其中一項：

   - URL:指定 URL 並套用至所有 URL 的子網站或只套用至某個網頁。
   - 含關鍵字的 URL：指定字串並使用一般表示式。

   按一下「測試」，以檢視將此規則套用至 Web 存取記錄檔中最常見的 20 個 URL，以及前一天前 100 個 URL 的結果。

5. 選取下列其中一項：

   - 所有用戶端：套用至所有用戶端。
   - 指定範圍：套用至某個範圍的 IP 位址、網域名稱和電腦名稱。

   
   注意

   此項同時支援 IPv4 和 IPv6 位址。

6. 按一下「核可」或「封鎖」。
7. 按一下「儲存」。

匯入使用者定義的 URL

使用此畫面可從另一台主動式雲端截毒技術伺服器匯入使用者定義的 URL。以下是此畫面提供的選項。

- 瀏覽：按一下以從您的電腦選取 `.csv` 檔案。
- 上傳：按一下以上傳選取的 `.csv` 檔案。
- 取消：按一下可回到上一個畫面。

設定可疑物件

可疑物件是指在提交的範例中發現的已知惡意或可能含有惡意的 IP 位址、網域、URL 或 SHA-1 值。

主動式雲端截毒技術伺服器可以訂閱下列來源，來同步處理可疑物件：

表 2-1. 主動式雲端截毒技術伺服器可疑物件來源

來源	可疑物件類型	說明
Deep Discovery Analyzer • 沙盒虛擬平台	URL	沙盒虛擬平台是一種用於分析可疑檔案的雲端虛擬環境。沙盒影像允許在模擬網路上端點的環境中觀察檔案行為，不會帶來任何危害網路的風險。 受管產品中的沙盒虛擬平台會追蹤並分析提交的範例。沙盒虛擬平台會將可能讓系統曝露於危險或損失的可疑物件加上旗標。
Control Manager 整合的可疑物件 • Control Manager 之使用者定義的可疑物件 • 沙盒虛擬平台可疑物件	URL	Deep Discovery Analyzer 會傳送可疑物件清單給 Control Manager。 Control Manager 管理員可以新增他們認為可疑，但目前不在沙盒虛擬平台可疑物件清單中的物件。使用者定義的可疑物件之優先順序高於沙盒虛擬平台可疑物件。 Control Manager 會整合可疑物件以及對物件採取的中毒處理行動，然後將它們散發到主動式雲端截毒技術伺服器。

在訂閱之後，主動式雲端截毒技術伺服器會轉送：

- 可疑的 URL 資訊到會傳送網頁信譽評等查詢的趨勢科技產品（如 OfficeScan 代理程式、ScanMail 和 Deep Security）
- 針對可疑的 URL 所採取的處理行動到會傳送網頁信譽評等查詢的 OfficeScan 代理程式。

注意

如需 Control Manager 如何管理可疑物件的相關資訊，請參閱： http://docs.trendmicro.com/en-us/enterprise/control-manager-60-service-pack-3/whats_new_6sp3/suspicious_object_supported_products.aspx

程序

1. 移至「主動式雲端截毒技術 > 可疑物件」。
2. 輸入可疑物件「來源」的 FQDN 或 IP 位址。
3. 輸入可疑物件來源所取得的「API 金鑰」。
4. 選用：按一下「測試連線」，驗證伺服器名稱、IP 位址及 API 金鑰均有效且來源可用。
5. 按一下「訂閱」。
6. 若要立即同步處理可疑物件，請選取「同步處理並啟動可疑物件」，然後按一下「立即同步處理」。

   注意

   只有主動式雲端截毒技術伺服器成功連線至來源時，此選項才可用。

7. 按一下「儲存」。

啟動 Smart Feedback

Trend Micro Smart Feedback 會與趨勢科技主動雲端截毒技術分享匿名的安全威脅資訊，讓趨勢科技可以迅速識別和處理新的安全威脅。您可以隨時透過這個主控台關閉智慧回報系統。

程序

1. 移至「主動式雲端截毒技術 > Smart Feedback」。

   注意

   請先確定主動式雲端截毒技術伺服器具有 Internet 連線，然後再啟動 Smart Feedback。

2. 選取「啟動 Trend Micro Smart Feedback」。

3. 選取您的產業。
4. 按一下「儲存」。

更新

主動式雲端截毒技術伺服器需要使用最新的病毒碼檔案和元件，才能發揮最大效用。趨勢科技每小時會發行新版的雲端病毒碼檔案。

秘訣

趨勢科技建議您在安裝之後立即更新元件。

設定手動更新

手動更新病毒碼的步驟：

程序

1. 移至「更新」。

2. 按一下下拉式清單中的「病毒碼」或「程式」。
3. 按一下「立即更新」或「立即儲存和更新」，以立即套用更新。

設定預約更新

執行預約更新的步驟：

程序

1. 移至「更新」。
2. 按一下下拉式清單中的「病毒碼」或「程式」。
3. 指定更新預約時程。
4. 按一下「儲存」。

病毒碼檔案更新

更新病毒碼檔案，有助於確保查詢會套用最新資訊。以下是此畫面提供的選項：

- 啟動預約更新：選取以設定每小時或每 15 分鐘自動更新一次。
- 立即更新：按一下以立即更新所有病毒碼檔案。

程式檔案更新

更新到產品程式的最新版本可運用產品加強功能。以下是此畫面提供的選項。

- 作業系統：選取以更新作業系統元件。
- 主動式雲端截毒技術伺服器：選取以更新產品伺服器程式檔案。

- Widget 元件：選取以更新 Widget。
- 啟動預約更新：選取以在每天或每週的特定時間更新程式檔案。
- 僅下載：選取以下載更新，並收到程式檔案更新提示。
- 下載之後自動更新：選取以在下載之後將所有更新套用至產品，而不論是否需要重新啟動或重新開機。
- 請勿自動更新需要重新啟動或重新開機的程式：選取以下載所有更新，並且只安裝不需要重新啟動或重新開機的程式。
- 上傳：按一下以上傳和更新適用於主動式雲端截毒技術伺服器的程式檔案。
- 瀏覽：按一下以尋找程式套件。
- 立即儲存和更新：按一下以套用所有設定並立即執行更新。

有三種方法可以更新程式檔案：預約更新、手動更新以及上傳元件。

啟動預約更新

程序

1. 移至「更新 > 程式」。
2. 選取「啟動預約更新」並選取更新預約時程。

3. 選取下列其中一個更新方法：

    - 僅下載：選取此核取方塊，以下載程式檔案，但不加以安裝。當有程式檔案更新可供安裝時，Web 產品主控台上即會出現訊息。
    - 下載之後自動更新：選取此核取方塊，以在下載程式檔案更新之後自動加以安裝。
        - 請勿自動更新需要重新啟動或重新開機的程式：選取此核取方塊，以在更新需要重新啟動或重新開機時，在 Web 產品主控台上顯示提示。系統將會自動安裝不需要重新啟動或重新開機的程式更新。

4. 按一下「儲存」。

執行手動更新

程序

1. 移至「更新 > 程式」。
2. 選取下列其中一個更新方法：

    - 僅下載：選取此核取方塊，以下載程式檔案，但不加以安裝。當有程式檔案更新可供安裝時，Web 產品主控台上即會出現訊息。
    - 下載之後自動更新：選取此核取方塊，以在下載程式檔案更新之後自動加以安裝。
        - 請勿自動更新需要重新啟動或重新開機的程式：選取此核取方塊，以在更新需要重新啟動或重新開機時，在 Web 產品主控台上顯示提示。系統將會自動安裝不需要重新啟動或重新開機的程式更新。

3. 按一下「立即儲存和更新」。

上傳檔案以執行手動更新

程序

1. 移至「更新 > 程式」。

   重要

   在繼續之前，請確定主動式雲端截毒技術伺服器未在執行更新。如果您必須更新程式或元件，請先停用預約元件更新，然後再繼續。

2. 在「上傳元件」下，按一下「瀏覽...」，以找出需要執行手動程式更新的程式檔案。

   注意

   找出您從趨勢科技網站下載或從趨勢科技取得的程式檔案。

3. 找到該檔案，然後按一下「開啟」。

4. 按一下「上傳」。

   注意

   如果已停用預約掃瞄來更新程式或元件，請在上傳和更新之後重新啟用該掃瞄。

可用的程式檔案

使用此畫面來更新可用的程式檔案。以下是此畫面提供的選項。

- <核取方塊>：選取要更新的可用程式檔案旁邊的核取方塊。
- 立即更新：按一下以更新選定程式檔案。

設定更新來源

使用此畫面來指定檔案信譽評等和網頁信譽評等的更新來源。預設更新來源為趨勢科技的主動式更新伺服器。以下是此畫面提供的選項。

- 趨勢科技的主動式更新伺服器：選取以從趨勢科技的主動式更新伺服器下載更新。
- 其他更新來源：選取以指定諸如 趨勢科技 Control Manager 的更新來源。

程序

1. 移至「更新 > 來源」，然後選取「檔案信譽評等」標籤或「網頁信譽評等」標籤。
2. 選取「趨勢科技的主動式更新伺服器」，或選取「其他更新來源」並輸入 URL。
3. 按一下「儲存」。

管理工作

管理工作可讓您設定 SNMP 服務設定、通知、代理伺服器設定或下載診斷資訊。

SNMP 服務

主動式雲端截毒技術伺服器支援 SNMP，以在監控產品方面提供更大的靈活性。進行設定，並透過「SNMP 服務」畫面下載 Management Information Base (MIB) 檔案。以下是此畫面提供的選項。

- 啟動 SNMP 服務：選取以使用 SNMP。
- 社群名稱：指定 SNMP 社群名稱。

- 啟動 IP 限制：選取以啟動 IP 位址限制。

> **注意**
>
> IP 限制不支援無類別網域間路由 (CIDR)。您可以啟動 IP 位址限制，防止他人未經授權存取 SNMP 服務。

- IP 位址：指定 IP 位址以便使用 SNMP 服務監控健全狀態。
- 子網路遮罩：指定網路遮罩，以定義使用 SNMP 服務來監控電腦狀態所需的 IP 位址範圍。
- 主動式雲端截毒技術伺服器 MIB：按一下以下載主動式雲端截毒技術伺服器 MIB 檔案。
- 儲存：按一下以保留設定。
- 取消：按一下以捨棄變更。

設定 SNMP 服務

設定 SNMP 服務設定，以允許 SNMP 管理系統監控主動式雲端截毒技術伺服器的狀態。

程序

1. 移至「管理 > SNMP 服務」。

2. 選取「啟動 SNMP 服務」核取方塊。
3. 指定「社群名稱」。
4. 選取「啟動 IP 限制」核取方塊，防止他人未經授權存取 SNMP 服務。

注意

IP 限制不支援無類別網域間路由 (CIDR)。

5. 指定 IP 位址。
6. 指定子網路遮罩。
7. 按一下「儲存」。

下載 MIB 檔案

從 Web 主控台下載 MIB 檔案，以使用 SNMP 服務。

程序

1. 移至「管理 > SNMP 服務」。
2. 按一下「主動式雲端截毒技術伺服器 MIB」以下載 MIB 檔案。確認視窗隨即顯示。
3. 按一下「儲存」。

   「另存新檔」畫面隨即顯示。
4. 指定儲存位置。
5. 按一下「儲存」。

主動式雲端截毒技術伺服器 MIB

下表提供主動式雲端截毒技術伺服器 MIB 的說明。

物件名稱	物件識別碼 (OID)	說明
Trend-MIB:: TBLVersion	1.3.6.1.4.1.6101.1.2.1.1	傳回目前的「雲端病毒碼」版本。
Trend-MIB:: TBLLastSuccessfulUpdate	1.3.6.1.4.1.6101.1.2.1.2	傳回上次成功更新雲端病毒碼的日期與時間。
Trend-MIB:: LastUpdateError	1.3.6.1.4.1.6101.1.2.1.3	傳回上次更新雲端病毒碼的狀態。 • 0: 上次更新病毒碼成功。 • <錯誤碼>：上次更新病毒碼不成功。
Trend-MIB:: LastUpdateErrorMessage	1.3.6.1.4.1.6101.1.2.1.4	如果上次更新雲端病毒碼失敗，則會傳回錯誤訊息。
Trend-MIB:: WCSVersion	1.3.6.1.4.1.6101.1.2.1.5	傳回目前的網頁封鎖病毒碼版本。
Trend-MIB:: WCSLastSuccessfulUpdate	1.3.6.1.4.1.6101.1.2.1.6	傳回上次成功更新網頁封鎖病毒碼的日期與時間。
Trend-MIB:: WCSLastUpdateError	1.3.6.1.4.1.6101.1.2.1.7	傳回上次更新網頁封鎖病毒碼的狀態。 • 0: 上次更新病毒碼成功。 • <錯誤碼>：上次更新病毒碼不成功。
Trend-MIB:: WCSLastUpdateErrorMessage	1.3.6.1.4.1.6101.1.2.1.8	如果上次更新網頁封鎖病毒碼失敗，則會傳回錯誤訊息。
Trend-MIB:: LastVerifyError	1.3.6.1.4.1.6101.1.2.2.2	傳回檔案信譽評等查詢的狀態。 • 0: 檔案信譽評等查詢已如預期般運作。 • <錯誤碼>：檔案信譽評等查詢未如預期般運作。

物件名稱	物件識別碼 (OID)	說明
Trend-MIB:: WCSLastVerifyError	1.3.6.1.4.1.6101.1.2.2.3	傳回網頁信譽評等查詢的狀態。 • 0: 網頁信譽評等查詢已如預期般運作。 • <錯誤碼>：網頁信譽評等查詢未如預期般運作。
Trend-MIB:: LastVerifyErrorMessage	1.3.6.1.4.1.6101.1.2.2.4	如果檔案信譽評等查詢的上一個健全狀態為失敗，將會傳回錯誤訊息。
Trend-MIB:: WCSLastVerifyErrorMessage	1.3.6.1.4.1.6101.1.2.2.5	如果網頁信譽評等查詢的上一個健全狀態為失敗，將會傳回錯誤訊息。

支援的 MIB

下表提供其他支援 MIB 的說明。

物件名稱	物件識別碼 (OID)	說明
SNMP MIB-2 系統	1.3.6.1.2.1.1	系統群組包含與項目所在之系統相關的資訊。此群組中的物件對於故障管理和組態管理而言很實用。請參閱 IETF RFC 1213。
SNMP MIB-2 介面	1.3.6.1.2.1.2	介面物件群組包含網路裝置上每個介面的相關資訊。此群組提供故障管理、組態管理、效能管理及帳號管理的實用資訊。請參閱 IETF RFC 2863。

Proxy 設定

如果您在網路中使用 Proxy 伺服器，請設定 Proxy 設定。以下是此畫面提供的選項。

- 使用 Proxy 伺服器：選取您的網路是否使用 Proxy 伺服器。
- HTTP：選取您的 Proxy 伺服器是否使用 HTTP 做為 Proxy 伺服器通訊協定。

- SOCKS5：選取您的 Proxy 伺服器是否使用 SOCKS5 做為 Proxy 伺服器通訊協定。
- 伺服器名稱或 IP 位址：輸入 Proxy 伺服器名稱或 IP 位址。
- 通訊埠：輸入通訊埠號碼。
- 使用者 ID：如果您的 Proxy 伺服器需要驗證，請輸入 Proxy 伺服器的使用者 ID。
- 密碼：如果您的 Proxy 伺服器需要驗證，請輸入 Proxy 伺服器的密碼。

設定 Proxy 設定

程序

1. 移至「管理 > Proxy 設定」。

2. 選取「使用 Proxy 伺服器來進行更新」核取方塊。
3. 選取「HTTP」或「SOCKS5」 做為 Proxy 伺服器通訊協定。

注意

主動式雲端截毒技術伺服器不再支援 SOCKS4 Proxy 伺服器組態設定。

4. 輸入伺服器名稱或 IP 位址。
5. 輸入通訊埠號碼。
6. 如果您的 Proxy 伺服器需要憑證，請輸入「使用者 ID」和「密碼」。
7. 按一下「儲存」。

支援

使用 Web 主控台來下載診斷資訊，以進行疑難排解和支援。

按一下「開始」以開始收集診斷資訊。

下載取得支援所需的系統資訊

程序

1. 移至「管理 > 支援」。
2. 按一下「開始」。

   下載進度畫面隨即出現。
3. 在出現已下載檔案的提示時，按一下「儲存」。
4. 指定位置和檔案名稱。
5. 按一下「儲存」。

變更產品主控台密碼

產品主控台密碼是保護主動式雲端截毒技術伺服器免於受到未經授權變更的主要方式。如需更安全的環境，請定期變更主控台密碼，並使用難以猜測的密碼。可以透過命令列介面 (CLI) 變更 admin 帳號密碼。從 CLI 使用 "configure password" 命令來進行變更。

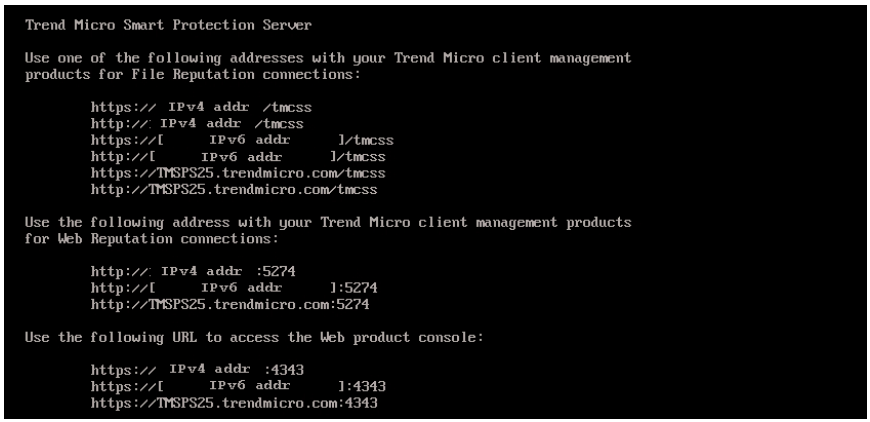
秘訣

如果要設計一個安全的密碼，請考慮下列作法：

- 同時包含字母和數字。
- 避免在（任何語言的）字典中找得到的單字。
- 故意拼錯單字。
- 使用片語或組合字。
- 使用大小寫字母的組合。
- 使用符號。

程序

1. 使用 admin 帳號登入 CLI 主控台。



2. 輸入下列命令以啟動管理命令：

   ```
   enable
   ```

3. 輸入下列命令：

   ```
   configure password admin
   ```

4. 輸入新密碼。

5. 再輸入一次新密碼以確認該密碼。

匯入憑證

為了安全起見，本主動式雲端截毒技術伺服器版本可讓管理員重新產生或匯入伺服器憑證。

程序

1. 移至「管理 > 憑證」。

   目前的「伺服器憑證資訊」隨即顯示。

2. 按一下「取代目前的憑證」。

3. 按一下「瀏覽...」選取要上傳的有效憑證。此憑證必須是 .pem 檔案。

4. 按「下一步」。

5. 檢查新憑證的詳細資料，然後按一下「完成」。稍候幾秒，讓憑證匯入。

與趨勢科技產品和服務整合

主動式雲端截毒技術伺服器與下列各表格中列出的趨勢科技產品和服務整合。請參閱整合產品線上說明中的相關章節，以瞭解整合詳細資訊。

表 2-2. 檔案信譽評等服務

使用的元件	元件來源	整合的產品和最低支援版本	第一個主動式雲端截毒技術伺服器版本
雲端病毒碼 注意 雲端病毒碼可與安裝在整合產品上的本機雲端病毒碼搭配運作。	• 趨勢科技主動式更新伺服器（預設） • 支援使用 HTTP 或 HTTPS 作為其他更新來源	• OfficeScan 10 • Core Protection Module 10.5 • Deep Security 7.5 • InterScan Messaging Security Virtual Appliance 9.1 • InterScan Web Security Virtual Appliance 6.5 SP1 • ScanMail for Microsoft Exchange 10 SP1 • PortalProtect 2.1 for SharePoint 2.1 • Threat Mitigator 2.5 • Worry-Free Business Security 6.0	1.0
主動式雲端截毒技術服務 Proxy 伺服器（用於社群檔案信譽評等）	無（內建）	• Deep Discovery Email Inspector 2.5 • Deep Discovery Inspector 3.8 SP2 • Deep Discovery Analyzer 5.5 SP1 • OfficeScan XG	3.0 Patch 2

表 2-3. 網頁信譽評等服務

使用的元件	元件來源	整合的產品和最低支援版本	第一個主動式雲端截毒技術伺服器版本
網頁封鎖病毒碼	• 趨勢科技主動式更新伺服器（預設） • 其他支援的更新來源	• OfficeScan 10.5 • Core Protection Module 10.5 • Deep Discovery Inspector 2.6 • Deep Security 7.5 • ScanMail for Microsoft Exchange 10.0 SP1 • ScanMail for Lotus Domino 5.6 • PortalProtect 2.1 • Trend Micro Security (適用於 Mac) 2.0	2.0
許可/封鎖的 URL	無 （清單直接在主動式雲端截毒技術伺服器主控台上設定）		2.0
可疑的 URL	• Control Manager 6.0 SP2 • Deep Discovery Analyzer 5.0		2.6 Patch 1
加強的可疑 URL	• Control Manager 6.0 SP3	• OfficeScan 11 SP1	3.0 Patch 1
主動式雲端截毒技術服務 Proxy 伺服器（用於 Web 檢查服務）	無（內建）	• Deep Discovery Email Inspector 2.5 • Deep Discovery Inspector 3.8 SP2 • Deep Discovery Analyzer 5.5 SP1	3.0 Patch 2

表 2-4. 行動應用程式信譽評等服務

使用的元件	元件來源	整合的產品和最低支援版本	第一個主動式雲端截毒技術伺服器版本
主動式雲端截毒技術服務 Proxy 伺服器	無（內建）	• Deep Discovery Email Inspector 2.5 • Deep Discovery Inspector 3.8 SP2 • Deep Discovery Analyzer 5.5 SP1	3.0 Patch 2

表 2-5. 認證安全防護軟體服務

使用的元件	元件來源	整合的產品和最低支援版本	第一個主動式雲端截毒技術伺服器版本
主動式雲端截毒技術服務 Proxy 伺服器	無（內建）	• Deep Discovery Email Inspector 2.5 • Deep Discovery Inspector 3.8 SP2 • Deep Discovery Analyzer 5.5 SP1	3.0 Patch 2

表 2-6. 預測性機器學習

使用的元件	元件來源	整合的產品和最低支援版本	第一個主動式雲端截毒技術伺服器版本
主動式雲端截毒技術服務 Proxy 伺服器	無（內建）	• OfficeScan XG	3.1

注意

主動式雲端截毒技術服務 Proxy 伺服器會將來自整合產品的查詢要求重新導向到主動式雲端截毒技術進行進一步分析。

第 3 章

監控主動式雲端截毒技術伺服器

使用記錄檔以及含 Widget 的「摘要」畫面來監控主動式雲端截毒技術伺服器。

包含下列主題：

- 使用摘要畫面 第 3-2 頁
- 記錄檔 第 3-12 頁
- 通知 第 3-16 頁

使用摘要畫面

「摘要」畫面可以顯示有關主動式雲端截毒技術伺服器電腦、流量和偵測次數的自訂資訊。

主動式雲端截毒技術伺服器針對檔案信譽評等服務連線同時支援 HTTP 和 HTTPS 通訊協定，針對網頁信譽評等服務連線支援 HTTP 通訊協定。HTTPS 可提供較安全的連線，而 HTTP 使用的頻寬較少。主動式雲端截毒技術伺服器位址會顯示於命令列介面 (CLI) 主控台標題上。

「摘要」畫面包含下列使用者介面元素：

- 伺服器可見度：按一下以將伺服器新增至「伺服器可見度」清單中，或者為連到「伺服器可見度」清單中之伺服器的連線，設定 Proxy 伺服器設定。在所有 Widget 中編輯伺服器資訊的方式都相同。

注意

「主動式雲端截毒技術伺服器位址」會與管理端點的趨勢科技產品一起使用。「伺服器位址」會用於設定端點對主動式雲端截毒技術伺服器電腦的連線。

- 標籤為 Widget 提供了容器。如需詳細資訊，請參閱標籤 第 3-3 頁。
- Widget 是管理平台的核心元件。如需詳細資訊，請參閱Widget 第 3-6 頁。

標籤

標籤為 Widget 提供了容器。「摘要」畫面上的每個標籤都能保留多達 20 個 Widget。「摘要」畫面本身最多支援 30 個標籤。

標籤工作

下表會列出所有與標籤相關的工作：

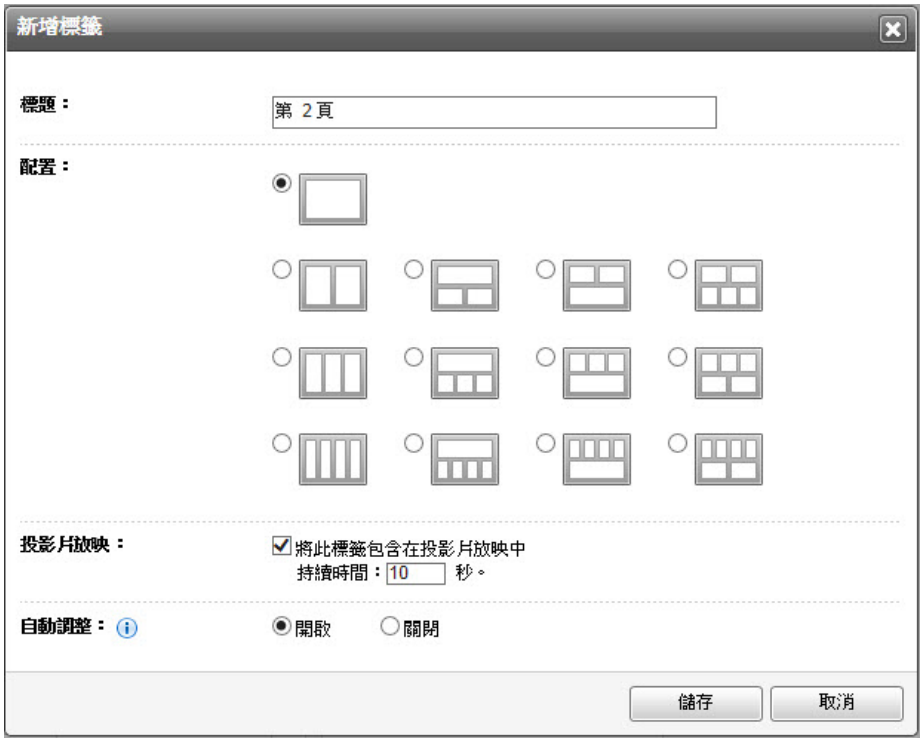
工作	步驟
新增標籤	按一下「摘要」畫面頂端的加號圖示 (+)。「新增標籤」視窗隨即顯示。如需有關此視窗的詳細資訊，請參閱「新增標籤」視窗 第 3-4 頁。
編輯標籤設定	按一下「標籤設定」。類似於「新增標籤」視窗的視窗會開啟，您可以在其中編輯設定。

工作	步驟
播放標籤投影片放映	按一下「播放標籤投影片放映」。已選取標籤中的資訊會變更，與投影片放映類似。
移動標籤	使用拖放功能變更標籤的位置。
刪除標籤	按一下標籤標題旁邊的刪除圖示 ( )。刪除標籤也會刪除標籤中的全部 Widget。

「新增標籤」視窗

當您在「摘要」畫面中新增標籤時，會開啟「新增標籤」視窗。

此視窗包含下列選項：



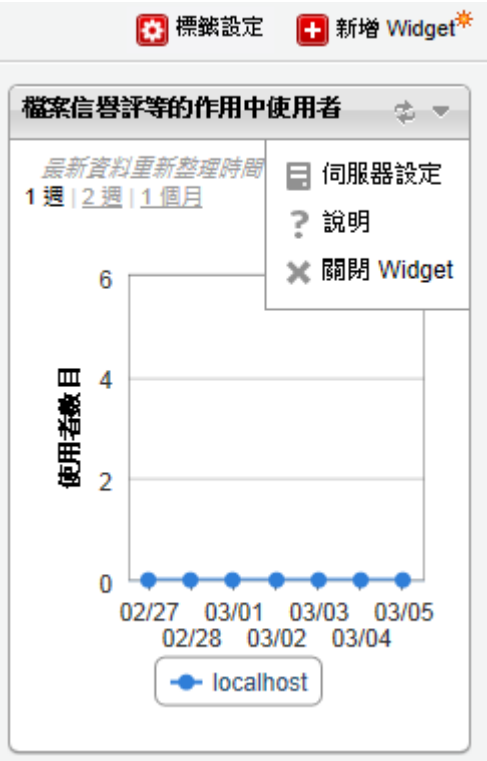
選項	步驟
標題	輸入標籤的名稱。
配置	從可用的配置中選擇。
投影片放映	已選取標籤中的資訊會變更，與投影片放映類似。如果啟用此選項，則可以選擇希望出現在投影片放映中的標籤，還可以控制投影片放映的速度。
自動調整	自動調整會將 Widget 調整為方塊的大小。

Widget

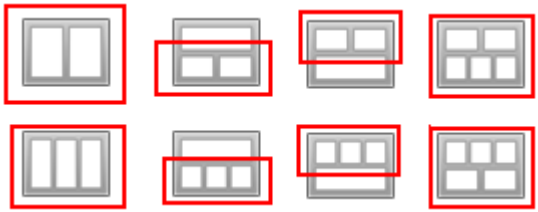
Widget 可讓您自訂要在「摘要」畫面上顯示的資訊。您可以在 Web 主控台中新增 Widget。您可以拖放 Widget 以自訂其顯示順序。您可以使用「程式更新」畫面，下載和更新可用的 Widget 套件。更新 Widget 套件之後，即可從「摘要」畫面新增 Widget。

Widget 工作

下表會顯示與 Widget 相關的工作：



工作	步驟
新增 Widget	開啟標籤，然後按一下標籤右上角的「新增 Widget」。「新增 Widget」畫面隨即顯示。
重新整理 Widget 資料	按一下重新整理圖示 ( )。
設定伺服器設定	按一下三角形圖示 ( )，然後再按「伺服器設定」( )，以包含 Widget 使之可以從伺服器取得資訊，或排除 Widget 使之無法從伺服器取得資訊。您也可以按一下「檢查伺服器可見度」從「伺服器可見度」清單新增伺服器，或是設定 Proxy 伺服器設定，以建立與「伺服器可見度」清單中伺服器的連線。
檢視說明	按一下三角形圖示 ( )，然後按一下「說明」( )。
刪除 Widget	按一下三角形圖示 ( )，然後按一下「關閉 Widget」( )。此處理行動可從包含 Widget 的標籤將此 Widget 移除，而不是從包含它的其他標籤移除，或是從「新增 Widget」畫面的 Widget 清單移除。
移動 Widget	使用拖放功能將 Widget 移動到標籤內的不同位置。

工作	步驟
調整 Widget 的大小	若要調整 Widget 的大小，請將游標指向 Widget 的右邊緣。當您看到粗的垂直線和箭頭（如下列影像所示）時，請按住游標並將游標移到左側或右側。  只有多欄標籤上的 Widget 可以調整大小。這些標籤可能具有下列任何一個配置，而且反白顯示的區段包含可調整大小的 Widget。 

可用的 Widget

本發行版本提供以下 Widget。

即時狀態

使用即時狀態 Widget 可監控主動式雲端截毒技術伺服器的狀態。

注意

當「摘要」畫面上顯示此 Widget 時，產品主控台作業階段將不會到期。「電腦狀態」每分鐘都會更新一次，這表示因為會持續傳送要求到伺服器，因此作業階段將不會到期。但是，如果目前顯示的標籤並未包含此 Widget，則作業階段仍然會到期。

表 3-1. Widget 資料

資料	說明
服務	由主動式雲端截毒技術伺服器提供的服務。
通訊協定	這會顯示服務所支援的通訊協定。檔案信譽評等支援 HTTP 和 HTTPS 通訊協定。網頁信譽評等支援 HTTP。HTTPS 提供較為安全的連線，而 HTTP 則使用較少的頻寬。
主機	檔案信譽評等和網頁信譽評等服務位址。這些位址和支援主動式雲端截毒技術伺服器電腦的趨勢科技產品搭配使用。這些位址會用於設定與主動式雲端截毒技術伺服器電腦的連線。
電腦狀態	「健全狀況狀態」下會顯示下列項目： • 檔案信譽評等查詢：顯示檔案信譽評等是否如預期般運作。 • 網頁信譽評等查詢：顯示網頁信譽評等是否如預期般運作。 • 主動式更新：顯示主動式更新是否已如預期般運作。 • 平均 CPU 負載：顯示過去 1、5 和 15 分鐘由核心所產生的電腦平均負載。 • 可用記憶體：顯示電腦上可用的實體記憶體。 • 交換磁碟使用率：顯示交換磁碟使用率。 • 可用空間：顯示電腦上目前可用的磁碟空間。

檔案信譽評等的作用中使用者

作用中使用者 Widget 會顯示對主動式雲端截毒技術伺服器進行檔案信譽評等查詢的使用者數目。每部獨特的用戶端電腦都會視為一個作用中使用者。

注意

此 Widget 會以 2-D 圖表顯示資訊，而且每小時會更新一次，或是隨時按一下重新整理圖示 () 來更新資料。

表 3-2. Widget 資料

資料	說明
使用者	傳送查詢給主動式雲端截毒技術伺服器電腦的使用者數目。
日期/時間	查詢的日期。

檔案信譽評等的 HTTP 流量報告

HTTP 流量報告 Widget 會顯示用戶端向主動式雲端截毒技術伺服器傳送的檔案信譽評等查詢所產生的網路總流量（以 KB 為單位）。此 Widget 中的資訊會每小時更新一次。您也可以隨時按一下重新整理圖示 () 來更新資料。

表 3-3. Widget 資料

資料	說明
流量 (KB)	查詢所產生的網路流量。
日期/時間	查詢的日期。

前 10 部針對檔案信譽評等封鎖的電腦

此 Widget 會顯示在主動式雲端截毒技術伺服器從檔案信譽評等查詢收到已知病毒之後，歸類為中毒電腦的前 10 部中毒最多電腦的 IP 位址。此 Widget 中的資訊會以表格顯示，其中包含電腦 IP 位址和每部電腦上的偵測總數。此 Widget 中的資訊會每小時更新一次，或是可以隨時按一下重新整理圖示 () 來更新資料。

使用此 Widget 可追蹤您網路上中毒數量最多的電腦。

注意

如果您在此 Widget 中啟動多部主動式雲端截毒技術伺服器，此 Widget 會計算所選主動式雲端截毒技術伺服器上的偵測總數，並以清單顯示來自所選主動式雲端截毒技術伺服器電腦的前 10 部中毒最多的電腦。

表 3-4. Widget 資料

資料	說明
IP	電腦的 IP 位址。
偵測	此電腦所偵測到的安全威脅數目。

網頁信譽評等的作用中使用者

作用中使用者 Widget 會顯示對主動式雲端截毒技術伺服器進行網頁信譽評等查詢的使用者數目。每部獨特的用戶端電腦都會視為一個作用中使用者。

注意

此 Widget 會以 2-D 圖表顯示資訊，而且每 5 分鐘會更新一次，或是隨時按一下重新整理圖示 () 來更新資料。

表 3-5. Widget 資料

資料	說明
使用者	傳送查詢給主動式雲端截毒技術伺服器電腦的使用者數目。
日期/時間	查詢的日期。

網頁信譽評等的 HTTP 流量報告

HTTP 流量報告 Widget 會顯示用戶端向主動式雲端截毒技術伺服器傳送的網頁信譽評等查詢所產生的網路總流量（以 KB 為單位）。此 Widget 中的資訊會每小時更新一次。您也可以隨時按一下重新整理圖示 () 來更新資料。

表 3-6. Widget 資料

資料	說明
流量 (KB)	查詢所產生的網路流量。
日期/時間	查詢的日期。

前 10 部針對網頁信譽評等封鎖的電腦

此 Widget 會顯示在主動式雲端截毒技術伺服器收到要進行網頁信譽評等查詢的 URL 之後，歸類為遭封鎖電腦的前 10 部最常遭到封鎖電腦的 IP 位址。此 Widget 中的資訊會以表格顯示，其中包含電腦 IP 位址和每部電腦上的遭封鎖 URL 總數。此 Widget 中的資訊會每天更新一次，或是可以隨時按一下重新整理圖示 ( ) 來更新資料。

使用此 Widget 可追蹤您網路上存取封鎖網站數量最多的電腦。

注意

如果您在此 Widget 中啟動多部主動式雲端截毒技術伺服器，此 Widget 會計算所選主動式雲端截毒技術伺服器上的偵測總數，並以清單顯示來自所選主動式雲端截毒技術伺服器電腦的前 10 部最常遭到封鎖的電腦。

表 3-7. Widget 資料

資料	說明
IP	電腦的 IP 位址。
偵測	來自此電腦的遭封鎖 URL 數目。

記錄檔

使用記錄檔來監控主動式雲端截毒技術伺服器的狀態。如果要檢視記錄檔資訊，可執行查詢。

封鎖的 URL

「封鎖的 URL」畫面會顯示傳回惡意結果的網頁信譽評等查詢相關資訊。

以下是此畫面提供的選項。

- 關鍵字：指定要在搜尋 URL 時使用的關鍵字。
- 日期範圍：選取日期範圍。
- 來源：選取一或多個來源以顯示對應的記錄檔。
  - 使用者定義的封鎖的 URL：顯示與主動式雲端截毒技術伺服器使用者定義的封鎖的 URL 相符之封鎖的 URL。
  - 網頁封鎖病毒碼：顯示與網頁封鎖病毒碼中項目相符的封鎖的 URL。
  - C&C URL 符合：顯示與以下來源中項目相符的封鎖的 URL：
    - Control Manager 之使用者定義的可疑物件：Control Manager 中使用者定義的可疑物件的子集
    - 沙盒虛擬平台：啟用沙盒虛擬平台的產品（如 Deep Discovery Advisor、Deep Discovery Analyzer 和 Control Manager）中可疑物件的子集
    - 網頁封鎖特徵碼中的全球資訊：趨勢科技主動式雲端截毒技術會從世界各地的來源彙整出「全球資訊」清單，並評估每個 C&C 回呼位址的風險等級。網頁信譽評等服務會將「全球資訊」清單搭配惡意網站信譽評分使用，以針對進階的安全威脅提供更強的安全防護。網頁信譽評等安全層級則會根據指定的風險等級，決定要對惡意網站或 C&C 伺服器採取的處理行動。

以下是此畫面顯示的詳細資訊：

- 日期和時間：所封鎖 URL 事件的日期和時間。
- URL:封鎖的 URL。
- 顯示記錄檔：顯示有關封鎖的 URL 的來源資訊。
- 用戶端 GUID：嘗試存取所封鎖 URL 的電腦 GUID。

- 伺服器 GUID：支援主動式雲端截毒技術伺服器電腦的趨勢科技產品之 GUID。
- 用戶端 IP：嘗試存取所封鎖 URL 的電腦 IP 位址。
- 電腦：嘗試存取所封鎖 URL 的電腦名稱。
- 產品項目：偵測到 URL 的趨勢科技產品。

更新記錄檔

「更新記錄檔」畫面會顯示病毒碼或程式檔案更新的資訊。以下是此畫面提供的選項。

- 日期範圍：選取更新發生的日期範圍。
- 類型：選取要顯示的更新類型。

記錄檔詳細資料：

- 日期和時間：更新伺服器的日期和時間。
- 元件名稱：已更新的元件。
- 結果：可能為成功或不成功。
- 說明：說明更新事件。
- 更新方式：顯示標準掃瞄或雲端截毒掃瞄。

信譽評等服務記錄檔

「信譽評等服務記錄檔」畫面會顯示網頁信譽評等和檔案信譽評等的服務狀態資訊。以下是此畫面提供的選項。

- 服務：指定服務。
- 結果：指定結果類型。

- 日期範圍：選取日期範圍。

記錄檔詳細資料：

- 日期和時間：信譽評等服務檢查「檔案信譽評等」或「網頁信譽評等」之服務狀態的日期和時間。
- 服務：此服務可能是「網頁信譽評等」或「檔案信譽評等」。
- 結果：可能為成功或不成功。
- 說明：說明「網頁信譽評等」或「檔案信譽評等」的服務狀態。

記錄檔維護

維護記錄檔，以刪除不再需要的記錄檔。以下是此畫面提供的選項。

- 病毒碼更新記錄檔：選取以清除病毒碼更新記錄檔項目。
- 程式更新記錄檔：選取以清除更新記錄檔項目。
- 封鎖的 URL：選取以清除 URL 查詢項目。
- 信譽評等服務記錄檔：選取以清除信譽評等服務事件項目。
- 刪除所有記錄檔：選取以刪除所有記錄檔。
- 清除早於下列天數的記錄檔：選取以清除較舊的記錄檔。
- 啟動預約清除：選取以預約自動清除。

程序

1. 移至「記錄檔 > 記錄檔維護」。
2. 選取要清除的記錄檔類型。
3. 選取以刪除所有記錄檔或早於指定天數的記錄檔。
4. 選取清除預約時程，或按一下「立即清除」。

5. 按一下「儲存」。

通知

您可以將主動式雲端截毒技術伺服器設為當服務或更新的狀態變更時，傳送電子郵件或「簡易網路管理通訊協定」(SNMP) Trap 通知給指定的人員。

電子郵件通知

設定電子郵件通知設定，以便在服務或更新的狀態變更時，透過電子郵件通知管理員。以下是此畫面提供的選項。

- SMTP 伺服器：輸入 SMTP 伺服器 IP 位址。
- 通訊埠號碼：輸入 SMTP 伺服器通訊埠號碼。
- 寄件人：輸入要在電子郵件通知寄件人欄位中使用的電子郵件信箱。
- 服務：選取以在「檔案信譽評等」、「網頁信譽評等」和「病毒碼更新」的狀態變更時傳送通知。
- 收件人：輸入要將此事件的通知傳送到的一或多個電子郵件信箱。
- 主旨：輸入此事件的新主旨或使用預設主旨文字。
- 訊息：輸入此事件的新訊息或使用預設訊息文字。
- 檔案信譽評等狀態變更：選取以傳送狀態變更的通知，然後指定此通知的收件人。
- 網頁信譽評等狀態變更：選取以傳送狀態變更的通知，然後指定此通知的收件人。
- 病毒碼更新狀態變更：選取以傳送狀態變更的通知，然後指定此通知的收件人。
- 更新：選取以針對所有程式相關的通知傳送通知。

- 程式更新下載不成功：選取以在程式更新下載失敗時傳送通知，然後指定此通知的收件人。
- 有程式更新可供使用：選取以在有需要確認的程式更新可供使用時傳送通知，然後指定此通知的收件人。
- 程式更新狀態：選取以傳送程式已更新的通知，然後指定此通知的收件人。
- 程式更新已重新啟動主動式雲端截毒技術伺服器或相關服務：選取以在程式更新程序已重新啟動主動式雲端截毒技術伺服器或相關服務時傳送通知，然後指定此通知的收件人。
- 預設訊息：按一下以將「主旨」和「訊息」欄位還原成趨勢科技的預設文字。

設定電子郵件通知

程序

1. 移至「管理 > 通知」，然後前往「電子郵件」標籤。

電子郵件通知適用的標籤隨即出現。

2. 選取「服務」核取方塊，以接受所有服務之狀態變更的電子郵件通知，或是從顯示的選項選取特定服務：

   - 檔案信譽評等狀態變更：選取以傳送狀態變更的通知，然後指定收件人、主旨和訊息。
   - 網頁信譽評等狀態變更：選取以傳送狀態變更的通知，然後指定收件人、主旨和訊息。
   - 病毒碼更新狀態變更：選取以傳送狀態變更的通知，然後指定收件人、主旨和訊息。

3. 選取「更新」核取方塊，或選取下列其中一個項目：

- 程式更新下載不成功：選取以傳送此事件的通知，然後指定收件人、主旨和訊息。
- 有程式更新可供使用：選取以傳送此事件的通知，然後指定收件人、主旨和訊息。
- 程式更新狀態：選取以傳送此事件的通知，然後指定收件人、主旨和訊息。
- 程式更新已重新啟動主動式雲端截毒技術伺服器或相關服務：選取以傳送此事件的通知，然後指定收件人、主旨和訊息。

4. 在「SMTP 伺服器」欄位中輸入 SMTP 伺服器 IP 位址。
5. 輸入 SMTP 通訊埠號碼。
6. 在「寄件人」欄位中，輸入電子郵件信箱。所有的電子郵件通知都會在電子郵件的「寄件人」欄位中顯示此信箱。
7. 按一下「儲存」。

SNMP Trap 通知

設定「簡易網路管理通訊協定」(SNMP) 通知設定，以便在服務或更新的狀態變更時，透過 SNMP Trap 通知管理員。以下是此畫面提供的選項。

- 伺服器 IP 位址：指定 SNMP Trap 收件人 IP 位址。
- 社群名稱：指定 SNMP 社群名稱。
- 服務：選取以在「檔案信譽評等」、「網頁信譽評等」和「病毒碼更新」的狀態變更時傳送 SNMP 通知。
- 訊息：輸入此事件的新訊息或使用預設訊息文字。
- 檔案信譽評等狀態變更：選取以傳送狀態變更的通知。
- 網頁信譽評等狀態變更：選取以傳送狀態變更的通知。
- 病毒碼更新狀態變更：選取以傳送狀態變更的通知。

- 預設訊息：按一下以將「訊息」欄位還原成趨勢科技的預設文字。

設定 SNMP Trap 通知

設定「簡易網路管理通訊協定」(SNMP) 通知設定，以便在服務或更新的狀態變更時，透過 SNMP Trap 通知管理員。

程序

1. 移至「管理 > 通知」，然後前往「SNMP」標籤。

   SNMP Trap 通知適用的標籤隨即出現。

2. 選取「服務」核取方塊，或選取下列其中一個核取方塊：

   - 檔案信譽評等狀態變更：選取以傳送狀態變更的通知，然後指定收件人、主旨和訊息。
   - 網頁信譽評等狀態變更：選取以傳送狀態變更的通知，然後指定收件人、主旨和訊息。

- 病毒碼更新狀態變更：選取以傳送狀態變更的通知，然後指定收件人、主旨和訊息。

3. 輸入 SNMP Trap 伺服器 IP 位址。
4. 輸入 SNMP 社群名稱。
5. 按一下「儲存」。

第 4 章

與 Trend Micro™ Control Manager™ 整合

主動式雲端截毒技術伺服器與 Control Manager 整合。

包含下列主題：

- 趨勢科技 Control Manager 第 4-2 頁
- 支援的 Control Manager 版本 第 4-2 頁
- 本主動式雲端截毒技術伺服器版本中的 Control Manager 整合 第 4-2 頁

趨勢科技 Control Manager

趨勢科技 Control Manager™ 是一個集中式管理主控台，可管理位於閘道、郵件伺服器、檔案伺服器和企業桌面層級的趨勢科技產品和服務。Control Manager 的 Web-based 管理主控台為整個網路中的受管產品和服務提供單一監控點。

Control Manager 可讓系統管理員監控和回報各種活動，例如病毒感染、安全違規或病毒進入點。系統管理員可下載元件並將其部署到整個網路中，有助於確保防護的一致性並保持在最新狀態。Control Manager 允許手動和預先排程的更新，並可依群組或逐一設定和管理產品，更富靈活彈性。

支援的 Control Manager 版本

本主動式雲端截毒技術伺服器版本支援下列 Control Manager 版本。

功能	CONTROL MANAGER 版本	
	6.0 SP3	6.0 SP2 或舊版
同步處理可疑物件和動作	是	否
使用 Control Manager 作為替代更新來源	是	是

注意

主動式雲端截毒技術伺服器只能透過單純 IPv4 或雙重堆疊網路連線到 Control Manager。

本主動式雲端截毒技術伺服器版本中的 Control Manager 整合

本主動式雲端截毒技術伺服器版本包含下列功能：

表 4-1. 與 Control Manager 整合

功能	說明
同步處理可疑物件和動作	1. Control Manager 會整合可疑物件和掃瞄動作，然後將這些資訊轉送到主動式雲端截毒技術伺服器。 2. 主動式雲端截毒技術伺服器會將可疑的 URL 和動作轉送到 Office Scan 代理程式。針對傳送網頁信譽評等查詢的產品 (例如 Portal Protect 和 Deep Security)，主動式雲端截毒技術伺服器則只會轉送可疑的 URL。 注意 如需 Control Manager 如何管理可疑物件的詳細資訊，請參閱 http://docs.trendmicro.com/all/ent/tmcm/v6.0-sp3/en-us/tmcm_6.0_sp3_ctd_primer/ctd_primer.pdf
Control Manager 作為替代更新來源	如果主動式雲端截毒技術伺服器沒有 Internet 連線，Control Manager 可充當更新來源。

第 5 章

技術支援

瞭解下列主題：

- 疑難排解資源 第 5-2 頁
- 聯絡趨勢科技 第 5-3 頁
- 將可疑內容傳送到趨勢科技 第 5-4 頁
- 其他資源 第 5-5 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策略的產品來抵禦此複雜惡意程式。安全威脅百科全書提供了多種混合性安全威脅的名稱和癥狀的完整清單，包括已知惡意程式、垃圾郵件、惡意 URL 和已知弱點。

移至 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	PC-cillin 用戶服務專線 Tel: 886-2-2378-3666 企業授權用戶技術專線 Tel: 886-2-2377-2323 其他聯絡資訊 Tel: (886) 2-23789666
網站	http://www.trendmicro.com.tw
電子郵件信箱	http://www.trend.com.tw/corpmail/

- 全球客戶服務據點：

  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

為了提高解決問題的速度，現已提供下列資訊：

- 問題模擬的步驟
- 裝置或網路資訊
- 電腦品牌、型號以及連接的任何其他硬體或裝置
- 記憶體大小和可用硬碟空間
- 作業系統和 Service Pack 版本
- 安裝的 Agent 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 A

命令列介面 (CLI) 命令

本節說明產品中可用來執行監控、偵錯、疑難排解和組態設定工作的命令列介面 (CLI) 命令。使用您的 admin 帳號透過虛擬機器登入 CLI。CLI 命令可讓管理員執行組態設定工作以及偵錯和疑難排解功能。CLI 介面還提供了其他用於監控重要資源和功能的命令。若要存取 CLI 介面，您必須擁有管理員帳號和密碼。

命令	語法	說明
`certificate regen self-sign`	`certificate regen self-sign <Issued_to> <Issued_by> <Validity>`	重新產生自我簽署憑證。 <Issued_to>:憑證接收者的一般名稱或 CN <Issued_by>:憑證核發者的一般名稱或 CN <Validity>:憑證的有效天數
`certificate update CA`	`certificate update CA`	下載最新的 CA 組合檔
`configure date`	`configure date <date> <time>`	設定日期並儲存到 CMOS `date` DATE_FIELD [DATE_FIELD] `time` TIME_FIELD [TIME_FIELD]

命令	語法	說明
`configure dns ipv4`	`configure dns ipv4 <dns1> [dns2]`	設定 IPv4 DNS 設定 `dns1` IPv4_ADDR 主要 DNS 伺服器 `dns2` IPv4_ADDR 次要 DNS 伺服器 []
`configure dns ipv6`	`configure dns ipv6 <dns1> [dns2]`	設定 IPv6 DNS 設定 `dns1` IPv6_ADDR 主要 DNS 伺服器 `dns2` IPv6_ADDR 次要 DNS 伺服器 []
`configure hostname`	`configure hostname <hostname>`	設定主機名稱 `hostname` HOSTNAME 主機名稱或 FQDN
`configure ipv4 dhcp`	`configure ipv4 dhcp [vlan]`	將預設乙太網路介面設為使用 DHCP `vlan` VLAN_ID VLan ID [1-4094]，預設無 VLan： [0]
`configure ipv4 static`	`configure ipv4 static <ip> <mask> <gateway> [vlan]`	將預設乙太網路介面設為使用靜態 IPv4 設定 `vlan` VLAN_ID VLan ID [1-4094]，預設無 VLan： [0]
`configure ipv6 auto`	`configure ipv6 auto [vlan]`	將預設乙太網路介面設為使用自動鄰居搜索 IPv6 設定 `vlan` VLAN_ID VLan ID [1-4094]，預設無 VLan： [0]
`configure ipv6 dhcp`	`configure ipv6 dhcp [vlan]`	將預設乙太網路介面設為使用動態 IPv6 設定 (DHCPv6) `vlan` VLAN_ID VLan ID [1-4094]，預設無 VLan： [0]
`configure ipv6 static`	`configure ipv6 static <v6ip> <v6mask> <v6gate> [vlan]`	將預設乙太網路介面設為使用靜態 IPv6 設定 `vlan` VLAN_ID VLan ID [1-4094]，預設無 VLan： [0]

命令	語法	說明
configure locale de_DE	configure locale de_DE	將系統地區設定設為德文
configure locale en_US	configure locale en_US	將系統地區設定設為英文
configure locale es_ES	configure locale es_ES	將系統地區設定設為西班牙文
configure locale fr_FR	configure locale fr_FR	將系統地區設定設為法文
configure locale it_IT	configure locale it_IT	將系統地區設定設為義大利文
configure locale ja_JP	configure locale ja_JP	將系統地區設定設為日文
configure locale ko_KR	configure locale ko_KR	將系統地區設定設為韓文
configure locale ru_RU	configure locale ru_RU	將系統地區設定設為俄文
configure locale zh_CN	configure locale zh_CN	將系統地區設定設為中文（簡體）
configure locale zh_TW	configure locale zh_TW	將系統地區設定設為中文（繁體）
configure ntp	configure ntp <ip or FQDN>	設定 NTP 伺服器
configure port	configure port <frs_http_port> <frs_https_port> <wrs_http_port>	變更檔案信譽評等服務及網頁信譽評等服務的服務通訊埠。
configure password	configure password <user>	設定帳號密碼 user USER 您要變更其密碼的使用者名稱。使用者可以是 'admin'、'root' 或是主動式雲端截毒技術伺服器之 Administrator 群組中的任何使用者。

命令	語法	說明
configure proxy-service	configure proxy-service <wis_url> <cfr_url> <grid_url> <mars_url>	修改趨勢科技全域防護服務 URL。 <wis_url>:Web 檢查服務 URL <cfr_url>:社群檔案信譽評等 URL <grid_url>:正常檔案和資訊資料庫 URL <mars_url>:行動應用程式信譽評等服務 URL
configure service	configure service inter-face <ifname>	設定預設伺服器設定
configure timezone Africa Cairo	configure timezone Africa Cairo	將時區設為「非洲/開羅」位置。
configure timezone Africa Harare	configure timezone Africa Harare	將時區設為「非洲/哈拉雷」位置。
configure timezone Africa Nairobi	configure timezone Africa Nairobi	將時區設為「非洲/奈洛比」位置。
configure timezone America Anchorage	configure timezone America Anchorage	將時區設為「美洲/安克拉治」位置。
configure timezone America Bogota	configure timezone America Bogota	將時區設為「美洲/波哥大」位置。
configure timezone America Buenos_Aires	configure timezone America Buenos_Aires	將時區設為「美洲/布宜諾斯艾利斯」位置。
configure timezone America Caracas	configure timezone America Caracas	將時區設為「美洲/卡拉卡斯」位置。

命令	語法	說明
configure timezone America Chicago	configure timezone America Chicago	將時區設為「美洲/芝加哥」位置。
configure timezone America Chihuahua	configure timezone America Chihuahua	將時區設為「美洲/奇瓦瓦」位置。
configure timezone America Denver	configure timezone America Denver	將時區設為「美洲/丹佛」位置。
configure timezone America Godthab	configure timezone America Godthab	將時區設為「美洲/哥特哈布」位置。
configure timezone America Lima	configure timezone America Lima	將時區設為「美洲/利馬」位置。
configure timezone America Los_Angeles	configure timezone America Los_Angeles	將時區設為「美洲/洛杉磯」位置。
configure timezone America Mexico_City	configure timezone America Mexico_City	將時區設為「美洲/墨西哥市」位置。
configure timezone America New_York	configure timezone America New_York	將時區設為「美洲/紐約」位置。
configure timezone America Noronha	configure timezone America Noronha	將時區設為「美洲/諾若尼亞」位置。

命令	語法	說明
configure timezone America Phoenix	configure timezone America Phoenix	將時區設為「美洲/鳳凰城」位置。
configure timezone America Santiago	configure timezone America Santiago	將時區設為「美洲/聖地牙哥」位置。
configure timezone America St_Johns	configure timezone America St_Johns	將時區設為「美洲/聖約翰斯」位置。
configure timezone America Tegucigalpa	configure timezone America Tegucigalpa	將時區設為「美洲/德古西加巴」位置。
configure timezone Asia Almaty	configure timezone Asia Almaty	將時區設為「亞洲/阿馬提」位置。
configure timezone Asia Baghdad	configure timezone Asia Baghdad	將時區設為「亞洲/巴格達」位置。
configure timezone Asia Baku	configure timezone Asia Baku	將時區設為「亞洲/巴庫」位置。
configure timezone Asia Bangkok	configure timezone Asia Bangkok	將時區設為「亞洲/曼谷」位置。
configure timezone Asia Calcutta	configure timezone Asia Calcutta	將時區設為「亞洲/加爾各答」位置。
configure timezone Asia Colombo	configure timezone Asia Colombo	將時區設為「亞洲/可倫坡」位置。

命令	語法	說明
configure timezone Asia Dhaka	configure timezone Asia Dhaka	將時區設為「亞洲/達卡」位置。
configure timezone Asia Hong_Kong	configure timezone Asia Hong_Kong	將時區設為「亞洲/香港」位置。
configure timezone Asia Irkutsk	configure timezone Asia Irkutsk	將時區設為「亞洲/伊爾庫次克」位置。
configure timezone Asia Jerusalem	configure timezone Asia Jerusalem	將時區設為「亞洲/耶路撒冷」位置。
configure timezone Asia Kabul	configure timezone Asia Kabul	將時區設為「亞洲/喀布爾」位置。
configure timezone Asia Karachi	configure timezone Asia Karachi	將時區設為「亞洲/喀拉蚩」位置。
configure timezone Asia Katmandu	configure timezone Asia Katmandu	將時區設為「亞洲/加德滿都」位置。
configure timezone Asia Krasnoyarsk	configure timezone Asia Krasnoyarsk	將時區設為「亞洲/克拉斯諾亞爾斯克」位置。
configure timezone Asia Kuala_Lumpur	configure timezone Asia Kuala_Lumpur	將時區設為「亞洲/吉隆坡」位置。
configure timezone Asia Kuwait	configure timezone Asia Kuwait	將時區設為「亞洲/科威特」位置。
configure timezone Asia Magadan	configure timezone Asia Magadan	將時區設為「亞洲/馬加丹」位置。

命令	語法	說明
configure timezone Asia Manila	configure timezone Asia Manila	將時區設為「亞洲/馬尼拉」位置。
configure timezone Asia Muscat	configure timezone Asia Muscat	將時區設為「亞洲/馬斯喀特」位置。
configure timezone Asia Rangoon	configure timezone Asia Rangoon	將時區設為「亞洲/仰光」位置。
configure timezone Asia Seoul	configure timezone Asia Seoul	將時區設為「亞洲/首爾」位置。
configure timezone Asia Shanghai	configure timezone Asia Shanghai	將時區設為「亞洲/上海」位置。
configure timezone Asia Singapore	configure timezone Asia Singapore	將時區設為「亞洲/新加坡」位置。
configure timezone Asia Taipei	configure timezone Asia Taipei	將時區設為「亞洲/台北」位置。
configure timezone Asia Tehran	configure timezone Asia Tehran	將時區設為「亞洲/德黑蘭」位置。
configure timezone Asia Tokyo	configure timezone Asia Tokyo	將時區設為「亞洲/東京」位置。
configure timezone Asia Yakutsk	configure timezone Asia Yakutsk	將時區設為「亞洲/亞庫茲克」位置。

命令	語法	說明
configure timezone Atlantic Azores	configure timezone Atlantic Azores	將時區設為「大西洋/亞速爾群島」位置。
configure timezone Australia Adelaide	configure timezone Australia Adelaide	將時區設為「澳洲/阿德雷德」位置。
configure timezone Australia Brisbane	configure timezone Australia Brisbane	將時區設為「澳洲/布里斯本」位置。
configure timezone Australia Darwin	configure timezone Australia Darwin	將時區設為「澳洲/達爾文」位置。
configure timezone Australia Hobart	configure timezone Australia Hobart	將時區設為「澳洲/霍巴特」位置。
configure timezone Australia Melbourne	configure timezone Australia Melbourne	將時區設為「澳洲/墨爾本」位置。
configure timezone Australia Perth	configure timezone Australia Perth	將時區設為「澳洲/伯斯」位置。
configure timezone Europe Amsterdam	configure timezone Europe Amsterdam	將時區設為「歐洲/阿姆斯特丹」位置。
configure timezone Europe Athens	configure timezone Europe Athens	將時區設為「歐洲/雅典」位置。

命令	語法	說明
configure timezone Europe Belgrade	configure timezone Europe Belgrade	將時區設為「歐洲/貝爾格勒」位置。
configure timezone Europe Berlin	configure timezone Europe Berlin	將時區設為「歐洲/柏林」位置。
configure timezone Europe Brussels	configure timezone Europe Brussels	將時區設為「歐洲/布魯塞爾」位置。
configure timezone Europe Bucharest	configure timezone Europe Bucharest	將時區設為「歐洲/布加勒斯特」位置。
configure timezone Europe Dublin	configure timezone Europe Dublin	將時區設為「歐洲/都柏林」位置。
configure timezone Europe Moscow	configure timezone Europe Moscow	將時區設為「歐洲/莫斯科」位置。
configure timezone Europe Paris	configure timezone Europe Paris	將時區設為「歐洲/巴黎」位置。
configure timezone Pacific Auckland	configure timezone Pacific Auckland	將時區設為「太平洋/奧克蘭」位置。
configure timezone Pacific Fiji	configure timezone Pacific Fiji	將時區設為「太平洋/斐濟」位置。
configure timezone Pacific Guam	configure timezone Pacific Guam	將時區設為「太平洋/關島」位置。

命令	語法	說明
configure timezone Pacific Honolulu	configure timezone Pacific Honolulu	將時區設為「太平洋/檀香山」位置。
configure timezone Pacific Kwajalein	configure timezone Pacific Kwajalein	將時區設為「太平洋/瓜加林島」位置。
configure timezone Pacific Midway	configure timezone Pacific Midway	將時區設為「太平洋/中途島」位置。
configure timezone US Alaska	configure timezone US Alaska	將時區設為「美國/阿拉斯加」位置。
configure timezone US Arizona	configure timezone US Arizona	將時區設為「美國/亞利桑那」位置。
configure timezone US Central	configure timezone US Central	將時區設為「美國/中部」位置。
configure timezone US East-Indiana	configure timezone US East-Indiana	將時區設為「美國/東印地安那」位置。
configure timezone US Eastern	configure timezone US Eastern	將時區設為「美國/東部」位置。
configure timezone US Hawaii	configure timezone US Hawaii	將時區設為「美國/夏威夷」位置。
configure timezone US Mountain	configure timezone US Mountain	將時區設為「美國/山區」位置。

命令	語法	說明
`configure timezone US Pacific`	`configure timezone US Pacific`	將時區設為「美國/太平洋」位置。
`disable adhoc-query`	`disable adhoc-query`	關閉 Web 存取記錄檔
`disable ssh`	`disable ssh`	關閉 sshd 精靈
`enable`	`enable`	啟動管理命令
`enable adhoc-query`	`enable adhoc-query`	啟動 Web 存取記錄檔
`enable ssh`	`enable ssh`	啟動 sshd 精靈
`exit`	`exit`	結束作業階段
說明	說明	顯示 CLI 語法的總覽。
`history`	`history [limit]`	顯示目前作業階段的命令列歷史記錄 `limit` 指定要顯示的 CLI 命令數目。範例：指定 [`limit`] 為 “5” 表示顯示 5 個 CLI 命令。
`reboot`	`reboot [time]`	在經過指定的延遲時間之後或立即重新啟動這部電腦 `time` UNIT 要等多久再重新啟動這部電腦 [0] 的時間（以分鐘為單位）
`show date`	`show date`	顯示目前的日期/時間
`show hostname`	`show hostname`	顯示網路主機名稱
`show interfaces`	`show interfaces`	顯示網路介面資訊
`show ipv4 address`	`show ipv4 address`	顯示網路 IPv4 位址
`show ipv4 dns`	`show ipv4 dns`	顯示網路 IPv4 DNS 伺服器

命令	語法	說明
show ipv4 gateway	show ipv4 gateway	顯示網路 IPv4 閘道
show ipv4 route	show ipv4 route	顯示網路 IPv4 路由表
show ipv4 type	show ipv4 type	顯示網路 IPv4 設定類型（dhcp/靜態）
show ipv6 address	show ipv6 address	顯示網路 IPv6 位址
show ipv6 dns	show ipv6 dns	顯示網路 IPv6 DNS 伺服器
show ipv6 gateway	show ipv6 gateway	顯示網路 IPv6 閘道
show ipv6 route	show ipv6 route	顯示網路 IPv6 路由表
show ipv6 type	show ipv6 type	顯示網路 IPv6 設定類型（自動/dhcp/靜態）
show timezone	show timezone	顯示網路時區
show uptime	show uptime	顯示目前系統正常執行時間
show url management	show url management	顯示 Web 管理主控台 URL
show url FileReputationService	show url FileReputationService	顯示檔案信譽評等服務的端點連線位址
show url WebReputationService	show url WebReputationService	顯示網頁信譽評等服務的端點連線位址
shutdown	shutdown [time]	在經過指定的延遲之後或立即關閉這部電腦 time UNIT 要等多久再關閉這部電腦 [0] 的時間（以分鐘為單位）

索引

C

Control Manager
- 與主動式雲端截毒技術伺服器整合, 4-2

Control Manager 之使用者定義的可疑物件, 2-12

W

Widget, 3-6

四畫

支援
- 更快地解決問題, 5-4

文件意見反應, 5-6

文件慣例, vii

五畫

主動式雲端截毒技術, 1-3

主動式雲端截毒技術伺服器, 1-3

七畫

沙盒虛擬平台, 2-12

十二畫

雲端病毒碼, 1-4

十四畫

摘要畫面
- Widget, 3-6
- 標籤, 3-3

網頁封鎖病毒碼, 1-4

十五畫

標籤, 3-3

十七畫

趨勢科技
- 關於, vi

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: APTM37774/170406